

Digital Forensics in the Cloud: Encrypted Data Evidence Tracking

ZHUANG TIAN, BSc (Hons)

a thesis submitted to the graduate faculty of design and creative technologies
Auckland University of Technology
in partial fulfilment of the
requirements for the degree of
Master of Forensic Information Technology

School of Computer and Mathematical Sciences

Auckland, New Zealand
2014

Declaration

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the qualification of any other degree or diploma of a University or other institution of higher learning, except where due acknowledgement is made in the acknowledgements.

.....

Zhuang Tian

Acknowledgements

This thesis was completed at the Faculty of Design and Creative Technologies in the school of Computing and Mathematical Sciences at Auckland University of Technology, New Zealand. While conducting the research project I received support from many people in one way or another, without whose support, this thesis would not have been completed in its present form. It is my pleasure to take this opportunity to thank all of you, without the intention or possibility to be complete. I would like to apologize to those who I did not mention by name here; however, I highly value your kind support.

Firstly, I would like to deeply thank my thesis supervisor Prof. Brian Cusack for the exceptional support given during the thesis project. He provided me with the freedom to explore research directions and to choose the routes that I wanted to investigate. Dr. Cusack's encouragement, excellent guidance, creative suggestions, and critical comments have greatly contributed to this thesis. Dr. Cusack, I would like to thank you very much for your daily supervision. Moreover, he provided me ongoing inspiration, without which the finalised copy of this thesis would not have been achieved. I enjoyed our discussions and had learned a great deal from you.

Also, I would like to thank my program leader Dr. Alastair Aisbet and MFIT Lab Instructor, Thomas Laurenson, Junewon Park and Ammann Roman for their mentorships, who gave endless efforts to organise the critical research environment much needed for this project. In addition, we would like to thank my fellow MFIT students, especially Yao Lu, Ting Ting Goh and Wei Li, who provided stimulating discussions, challenging questions, peer encouragement and many exciting debates in our chosen area of Digital Forensic research, and side interests in cloud data encryption topics.

Similarly, I would like to express my deep appreciation to all of the lecturers who gave me knowledge as well as taught me the concepts during the lectures of MFIT. I would like to thank my thesis proof readers, who gave feedback on communication improvement.

Finally, I would also like to express my sincere thanks to my late father, (Dayang Tian), my mother, Suping Zhang, my parents-in-law Fuchang Huang and Shenli Yin,

whose continual support, encouragement, love, praying for my progress and for teaching me the values in life that brought me where I am today. I greatly appreciate my wife, Rui Huang. She persistently supported me throughout my master's study. Without her, I could have never undertaken the program. Even when I was struggling with the direction of my life, she consistently encouraged me and helped me be confident over and over again.

Abstract

Cloud computing is an emerging model that separates application and information resources from the underlying infrastructure, and the mechanisms used to deliver them. The elastic nature, cost effective price and convenient connectivity make the cloud become more and more attractive as a storage medium for digital forensic investigators. The increasing volumes of data are also a driver for investigators use of a cloud for storing evidence and performing analysis. However, because of the distributed nature of the cloud (Cruz, & Atkison, 2011, p.306), data stored in the cloud may likely be divided into smaller chunks and placed at different data centres all over the globe. Moreover, the dynamic and remote nature of the cloud, make data relocating from data centre to data centre. Hence, data may be constantly compressed and resized. Thus, it is possible that data may be lost during the transmission; or compromised by attacks in the cloud. Furthermore, redundant storage in multiple jurisdictions (Yan, 2011, p.612) and the lack of transparent real-time information about where data is stored introduces judicial issues and further complications for investigations. Virtualisation also impacts on the privacy of other users (Dahbur, & Mohammad, 2011, p.2) of the cloud. To maintain information security, organisations can encrypt data before storing them in the Cloud; and then decrypt after retrieving the data from the Cloud.

The key challenges that a digital investigator is facing before committing to the cloud, is how to ensure that the security of evidence data will be maintained; and privacy will be protected in order to fulfil digital forensic investigation principles. Although solutions such as Hou, Uehara, Yiu, & Hui (2011, p.378) have been proposed to use homomorphic encryption to protect innocent evidence data from being exposed; they are, however, more suited in a relatively static database environment, and the feasibility and performance of such solutions in a public cloud are still yet to be studied and evaluated.

To maintain information security, organisations can encrypt data before storing them in the Cloud; and decrypt after retrieving the data from the Cloud. The research will identify, analyse and evaluate whether or not modern encryption algorithms can be

used in providing data security and persevering privacy for digital forensic investigation evidence data stored in the cloud.

To conduct the proposed research, a trial system was created in a lab controlled environment to simulate commercial situations where data will be relocated and distributed. The normal operation of the trial system was documented as the semi-trusted Storage-as-a-service cloud, in which stored digital forensic investigation data were scattered. Hence, the integrity, confidentiality and availability of digital forensic investigation data were stressed. Then experimental data generated during the research were collected and analysed, in order to test the robustness and performances of selected encryption tools.

The methodology used in a simulated environment was based on descriptive methods in which the case scenario of simulated attack on the cloud by redistributing encrypted sample file data from one storage medium to another. To investigate the robustness and performances of selected encryption tools, a customized cloud simulation were created using VMware. The descriptive mythology allowed the elaboration of precise details relevant to the research question.

The purpose of the main research question was to evaluate whether or not modern encryption algorithms can be used in providing security and preserve privacy for digital forensic investigation evidence data stored in the cloud. Consequently, the court evidence admissibility requirement was met according to digital forensic investigation principles and guidelines. The significant findings were found that the selected encryption tools were able to provide security for evidence data in the cloud at a sufficient level. Moreover, the encryption tools examined had reasonably good performance in the cloud. Though, AxCrypt had the overall best performance in terms of security features and data compression result resilience.

To conclude, the research conducted confirms that modern encryption algorithms are able to maintain security and preserve privacy for digital forensic investigation evidence data stored in the cloud. Moreover, using modern encryption algorithms ensures that evidence data do meet confidentiality, availability, privacy preserving, chain-of-custody and eventually court admissibility requirements. Ultimately, digital forensic investigator compliance principles are fulfilled.

Table of Contents

Declaration	ii
Acknowledgement.....	iii
Abstract	v
Table of Contents	vii
List of Tables.....	xiv
List of Figures	xv
Abbreviations	xvii

Chapter One: Introduction

1.0 BACKGROUND	1
1.1 CONCEPTS OF THE CLOUD.....	1
1.2 OBSTACLES IN THE CLOUD	3
1.3 MOTIVATION	6
1.4 STRUCTURE OF DISSERTATION.....	8

Chapter Two: Literature Review

2.0 INTRODUCTION	11
2.1 HISTORY OF THE CLOUD COMPUTING	13
2.1.1 The 1950s	13
2.1.2 The 1960 – 1990s	14
2.1.3 The 1990s	14
2.1.4 from 2000 to Date.....	15
2.2 CONCEPTS OF THE CLOUD COMPUTINGS.....	16
2.2.1 Definition of the Cloud Computing.....	16
2.2.2 Characteristics of the Cloud Computing	18
2.2.3 Service Models of the Cloud Computing	21
2.2.4 The Cloud Computing Deployment Models	24
2.2.5 The Cloud Computing Architecture	26
2.3 EXAMPLES OF THE CLOUD TECHNOLOGY.....	27
2.3.1 Amazon EC2	29

2.3.2 Microsoft Azure	29
2.3.3 Google App Engine	30
2.4 OBSTACLES IN THE CLOUD RELATING TO DIGITAL FORENSIC INVESTIGATION	30
2.4.1 Digital Forensic	31
2.4.1.1 Acquisition.....	32
2.4.1.2 Extraction.....	33
2.4.1.3 Analysis	33
2.4.1.4 Reporting	34
2.4.1.5 Preservation of Evidence and Chain of Custody	35
2.4.2 Challenges of Digital Forensic in the Cloud Environnement.....	35
2.4.2.1 The Cloud Governance	36
2.4.2.2 The Cloud Security	37
2.5 MODERN DATA ENCRYPTITON ALGORITHMS.....	41
2.5.1 Symmetric and Asymmetric Encryptions.....	41
2.5.2 DES & 3DES.....	43
2.5.3 AES	45
2.5.4 Free Encryption Tools	46
2.5.4.1 GNU Privacy Guard.....	46
2.5.4.2 TrueCrypt.....	48
2.5.4.3 AESCrypt.....	49
2.5.4.4 AxCrypt	50
2.5.4.4 AESTool	51
2.6 SUMMARY OF PROBLEMS AND ISSUES	52
2.7 CONCLUSION.....	53

Chapter Three: Research Methodology

3.0 INTRODUCTION	55
3.1 REVIEW OF SIMILAR STUDIES	55
3.1.1 Storing Forensic Investigation Evidence Data in the Cloud	56
3.1.2 The Cloud Security and Privacy Issues.....	57
3.1.3 Modern Encryption Techniques Used to Enhance Data Security in the Cloud.....	59

3.2 THE RESEARCH QUESTIONS AND HYPOTHESES.....	61
3.3 THE RESEARCH MODEL.....	64
3.3.1 Research Phases	65
3.3.2 Research Design Architecture.....	68
3.3.3 Research Components.....	69
3.4 DATA REQUIREMENTS.....	70
3.4.1 Data Generation	70
3.4.2 Data Collection	71
3.4.3 Data Processing.....	72
3.4.4 Data Analysis	73
3.4.5 Data Presentation	74
3.4.6 Data Map.....	75
3.5 LIMITATIONS	77
3.6 CONCLUSION.....	79

Chapter Four: Research Findings

4.0 INTRODUCTION	81
4.1 VARIATIONS IN DATA REQUIREMENTS	81
4.1.1 System Design	82
4.1.2 Data Generation	83
4.1.3 Data Collection	83
4.1.4 Data Processing, Analysis and Presentation	85
4.2 INITIAL TESTING FINDINGS.....	85
4.2.1 Phase One: Testing of Selected Encryption Tools.....	85
4.2.1.1 Phase One Experiment Process.....	86
4.2.1.2 Phase One Experiment Findings	87
4.2.2 Phase Two: Testing of Encryption Tools on Single VM (VM1)	95
4.2.2.1 Phase Two Experiment Process	95
4.2.2.2 Phase Two Experiment Findings	96
4.3 STABILISED TESTING FINDINGS	97
4.3.1 Phase Three: Testing of Encryption Tools on Double VMs	97
4.3.1.1 Phase Three Experiment Process	97
4.3.1.2 Phase Three Experiment Findings	98

4.3.2 Phase Four: Testing of Encryption Tools on Circled VMs.....	100
4.3.2.1 Phase Four Experiment Process.....	100
4.3.2.2 Phase Four Experiment Findings	101
4.4 CONCLUSION.....	102

Chapter Five: Research Discussion

5.0 INTRODUCTION	103
5.1 EVIDENCE FOR RESEARACH QUESTION ANSWERS	104
5.1.1 Main Research Question and Associated Hypothesis.....	104
5.1.2 Secondary Research Question and Associated Hypothesis	107
5.2 DISCUSSION	112
5.2.1 Discussion of Testing Phases.....	113
5.2.2 Discussion of Selected Encryption Tools	115
5.2.3 Discussion of Testing Environment.....	117
5.3 RECOMMENDATIONS	118
5.4 CONCLUSION.....	119

Chapter Six: Conclusion

6.0 INTRODUCTION	120
6.1 LIMITATIONS OF RESEARCH.....	122
6.2 FUTURE RESEARCH	124

REFERENCES	126
-------------------------	-----

APPENDICES	139
-------------------------	-----

Appendix 1: Screenshot of “Original Data”	139
Appendix 2: Table of “Original Data”	141
Appendix 3: Screenshot of AESCrypt “Encrypted Data” on Desktop.....	142
Appendix 4: Table of AESCrypt “Encrypted Data” on Desktop	144

Appendix 5: Table of AESCrypt “Recovered Data” from Desktop	145
Appendix 6: Screenshot of AxCrypt “Encrypted Data” on Desktop	146
Appendix 7: Table of AxCrypt “Encrypted Data” on Desktop.....	148
Appendix 8: Table of AxCrypt “Recovered Data” from Desktop	149
Appendix 9: Screenshot of AESTool “Encrypted Data” on Desktop	150
Appendix 10: Table of AESTool “Encrypted Data” on Desktop	152
Appendix 11: Table of AESTool “Recovered Data” from Desktop	153
Appendix 12: Table of AESCrypt “Stored Data” on VM1 (Single VM Environment)..	154
Appendix 13: Table of AESCrypt “Retrieved Data” from VM1 (Single VM Environment)	155
Appendix 14: Table of AESCrypt “Recovered Data” from VM1 (Single VM Environment)	156
Appendix 15: Table of AxCrypt “Stored Data” on VM1 (Single VM Environment)	157
Appendix 16: Table of AxCrypt “Retrieved Data” from VM1 (Single VM Environment)	158
Appendix 17: Table of AxCrypt “Recovered Data” from VM1 (Single VM Environment)	159
Appendix 18: Table of AESTool “Stored Data” on VM1 (Single VM Environment) ...	160
Appendix 19: Table of AESTool “Retrieved Data” from VM1 (Single VM Environment)	161
Appendix 20: Table of AESTool “Recovered Data” from VM1 (Single VM Environment)	162
Appendix 21: Table of AESCrypt “Stored Data” on VM1 (Double VMs Environment)	163
Appendix 22: Table of AESCrypt “Stored Data” on VM2 (Double VMs Environment)	164
Appendix 23: Table of AESCrypt “Retrieved Data” from VM2 (Double VMs Environment)	165
Appendix 24: Table of AESCrypt “Recovered Data” from VM2 (Double VMs Environment)	166
Appendix 25: Table of AxCrypt “Stored Data” on VM1 (Double VMs Environment) .	167
Appendix 26: Table of AxCrypt “Stored Data” on VM2 (Double VMs Environment) .	168
Appendix 27: Table of AxCrypt “Retrieved Data” from VM2 (Double VMs Environment)	169

Appendix 28: Table of AxCrypt “Recovered Data” from VM2 (Double VM Environment)	170
Appendix 29: Table of AESTool “Stored Data” on VM1 (Double VMs Environment)	171
Appendix 30: Table of AESTool “Stored Data” on VM2 (Double VMs Environment)	172
Appendix 31: Table of AESTool “Retrieved Data” from VM2 (Double VMs Environment)	173
Appendix 32: Table of AESCrypt “Recovered Data” from VM2 (Double VMs Environment)	174
Appendix 33: Table of AESCrypt “Stored Data” on VM1 (Circled VMs Environment)	175
Appendix 34: Table of AESCrypt “Stored Data” on VM2 (Circled VMs Environment)	176
Appendix 35: Table of AESCrypt “Stored Data” Copied on VM1 from VM2 (Circled VMs Environment)	177
Appendix 36: Table of AESCrypt “Retrieved Data” from VM1 (Circled VMs Environment)	178
Appendix 37: Table of AESCrypt “Recovered Data” from VM1 (Circled VMs Environment)	179
Appendix 38: Table of AxCrypt “Stored Data” on VM1 (Circled VMs Environment)	180
Appendix 39: Table of AxCrypt “Stored Data” on VM2 (Circled VMs Environment)	181
Appendix 40: Table of AxCrypt “Stored Data” Copied on VM1 from VM2 (Circled VMs Environment)	182
Appendix 41: Table of AxCrypt “Retrieved Data” from VM1 (Circled VMs Environment)	183
Appendix 42: Table of AxCrypt “Recovered Data” from VM1 (Circled VMs Environment)	184
Appendix 43: Table of AESTool “Stored Data” on VM1 (Circled VMs Environment)	185
Appendix 44: Table of AESTool “Stored Data” on VM2 (Circled VMs Environment)	186

Appendix 45: Table of AESTool “Stored Data” Copied on VM1 from VM2 (Circled VMs Environment)	187
Appendix 46: Table of AESTool “Retrieved Data” from VM1 (Circled VMs Environment)	188
Appendix 47: Table of AESTool “Recovered Data” from VM1 (Circled VMs Environment)	189
Appendix 48: Table of Computer Profile Summary	190

List of Tables

Table 2.1: Examples of the Cloud Computing Services & Comparison	27
Table 2.2: Table of GnuPG Characteristics	47
Table 3.1: Common Data Encryption Algorithms Used in the Cloud	59
Table 3.2: NIST Statistical Tests	61
Table 3.3: Main Research Question and Associated Hypothesis	62
Table 3.4: Secondary Research Questions	63
Table 3.5: Secondary Research Questions Associated Hypotheses	63
Table 4.1: The “Secrete Key” Used for the First 10 Sample Files by AESCrypt and AxCrypt	86
Table 4.2: The “Secrete Key” Used for the First 10 Sample Files by AESTool	87
Table 4.3: Timestamps of the Original Sample Files and AESCrypt Encrypted Files	88
Table 4.4: Timestamps of AESCrypt Encrypted Files and Recovered Files	88
Table 4.5: File Sizes of AESCrypt Encrypted Files and Original Sample Files	89
Table 4.6: Timestamps of the Original Files and AxCrypt Encrypted Files	91
Table 4.7: Timestamps of AxCrypt Encrypted Files and Recovered Files	91
Table 4.8: File Sizes Comparison of AxCrypt and AESCrypt Encrypted Files	92
Table 4.9: the Selected Encryption Tools Features Comparison	95
Table 5.1: Main Research Question and Tested Hypothesis	105
Table 5.2: Secondary Research Question 1 and Tested Hypothesis	107
Table 5.3: Secondary Research Question 2 and Tested Hypothesis	108
Table 5.4: Secondary Research Question 3 and Tested Hypothesis	110

List of Figures

Figure 2.1: Brief History of the Cloud Computing	16
Figure 2.2: The Cloud Computing Concept Map	17
Figure 2.3: Three Service Models of the Cloud Computing	21
Figure 2.4: Type 1 & Type 2 Hypervisors	23
Figure 2.5: The Cloud Computing Types	24
Figure 2.6: The Cloud Computing Sample Architecture	26
Figure 2.7: Digital Forensic Lifecycle	31
Figure 2.8: Simplified Model of Symmetric Encryption	42
Figure 2.9 Simplified Model of Asymmetric Encryption	43
Figure 2.10: DES Encryption and Decryption Model	44
Figure 2.11: 3DES Encryption and Decryption Model	44
Figure 2.12: AES Encryption and Decryption Model	45
Figure 2.13: TrueCrypt GUI Main Window	48
Figure 2.14: AESCrypt Simple User Options	50
Figure 2.15: AESTool Simple GUI Window	51
Figure 3.1: Proposed Data Security Model in the Cloud	60
Figure 3.2: Theoretical Research Model	66
Figure 3.3: The Proposed Research Architecture Design	68
Figure 3.4: Research Data Map	76
Figure 4.1: Variation of System Design	82
Figure 4.2: Error Message of Not Entering AESCrypt Secrete Key	89
Figure 4.3: Error Message of Entering Incorrect AESCrypt Secrete Key	90
Figure 4.4: AxCrypt Error Message of Incorrect Secrete Key	92
Figure 4.5: AxCrypt Error Message of Encrypting an Opening File	93
Figure 4.6: AxCrypt Encrypting and Shredding Process	93
Figure 4.7: AxCrypt Verifying and Decrypting Process	94
Figure 4.8: AESTool Error Message of Incorrect Secrete Key	94
Figure 4.9: AxCrypt Encrypted Files Copied to VM1	96
Figure 4.10: The Selected Encryption Tools Successful Decryption Rate in Single VM Environment	96
Figure 4.11: System Clock Comparison of VM1 and VM2	98

Figure 4.12: Screenshot of AxCrypt Encrypted Files' Timestamps on Desktop	99
Figure 4.13: The Selected Encryption Tools Successful Decryption Rate in Double VMs Environment	100
Figure 4.14: The Selected Encryption Tools Successful Decryption Rate in Circled VMs Environment	101

Abbreviations

API	Application Program Interface
AES	Advanced Encryption Standard
AMT	Amazon Mechanical Turk
AT&T	American Telephone & Telegraph
AWS	Amazon Web Services
CIA	Central Intelligence Agency
CLR	Common Language Runtime
CPU	Central Processing Unit
DEA	Data Encryption Algorithm
DEC	Digital Equipment Corporation
DES	Data Encryption Standard
3DES	Triple Data Encryption Standard
DSA	Digital Signature Algorithm
EC2	Amazon Elastic Computer Cloud
FIPS	Federal Information Processing Standard
GCSB	Government Communication Security Bureau
GFS	Google File System
GPL	General Public Licences
GUI	Graphical User Interface
HD	Hard Drive
HMAC	Hash Message Authentication Code
IaaS	Infrastructure-as-a-service
IBM	International Business Machines Corporation
IDEA	International Data Encryption Algorithm
IS	Information System
ISA	Instruction Set Architecture
IT	Information Technology
MD	Message Digest
MIT	Massachusetts Institute of Technology

NIJ	National Institute of Justice
NIST	National Institute of Standards and Technology
OS	Operating System
Paas	Platform-as-a-service
PC	Personal Computer
PRNG	Pseudorandom Number Generator
RC 4	Rivest Cipher 4
RC 6	Rivest Cipher 6
RIPEMD	RACE Integrity Primitives Evaluation Message Digest
RSA	Rivest, Shamir and Adleman Encryption Algorithm
RAM	Random Access Memory
S3	Simple Storage Service
Saas	Software-as-a-service
SHA	Secure Hash Algorithm
SLA	Service Level Agreement
SQL	Structured Query Language
SSL	Secure Sockets Layer
TB	Terabytes
TICS	Telecommunication Interception Capability and Security
UCB	University of California, Berkeley
UCSD	University of California, San Diego
US	United States
USB	Universal Serial Bus
VM	Virtual Machine
VMM	Virtual Machine Manager
VPN	Virtual Private Network
Xaas	X-as-a-service

Chapter One

INTRODUCTION

1.0 BACKGROUND

This thesis concerns the cloud and the issues and problems that arise when an investigator may use cloud storage for forensic evidence files. Consequently in this introduction chapter the cloud is reviewed in section 1 to identify problems for secure data storage and retrieval. In section 2 the research motivation and methods are introduced; and section 3 provides the structure outline for the thesis.

1.1 CONCEPTS OF THE CLOUD

In recent years, the concepts and implementations of contemporary distributed information technology infrastructures have been developing in the area of cloud computing. Vendors offer resources, software and information provided to computers and other digital devices as utility to the end users in distant locations. Users can access these services and information through the internet. Consequently, a new field of study has been rapidly emerging for the use of the cloud computing architecture layers and the functionality of the distinct services offered to end users.

Mohamed (2012, p.2) points out that the cloud computing refers to use the networked information system infrastructure including both hardware and software, and its capability to provide services in the resources on-demand environment. In the cloud, a company rents on another company's computer systems to perform the work. The rented space in the cloud can be in a globally connected data centre with many other companies where the user network entry point can be at any point on the internet. Data in the cloud environment can be replicated to any data centre in the world that is owned and operated by the cloud vendors. The cloud vendors have their own series of policies,

security systems, hardware and software packages that are independent of what an end user company is doing in the cloud space.

Yu (2010, p.1) believes that along with this new paradigm, various business models are developed. They can be described using “X-as-a-service”, where “X” could be hardware, software and data storage. Getov (2012, p.373) categorises cloud computing in three services, which are software-as-a-service (SaaS), platform-as-a-service (PaaS) and infrastructure-as-a-service (IaaS). Yu (2010) argues that the most popular examples are: Amazon’s Elastic Compute Cloud (EC2) and Simple Storage Service (S3), Google App Engine and Microsoft.

- SaaS: In this cloud service model, vendors install, operate, maintain and update user required applications. The user does not need to manage the underlying structures on which the applications are running.
- PaaS: In this model, vendors provide platforms such as OS, programming language execution environment, data centre, web and mail servers with virus scanning and monitoring services as well as anti-spam services.
- IaaS: This is the most basic cloud service model. Providers offer services for computers and infrastructures such as storage, firewall and network system.

Additionally, National Institute of Standards and Technology (NIST) defines the following deployment models for the cloud computing:

- Public cloud: the service made available to the public or/and other organisations. The users can access to the cloud using publicly accessible web browser interface.
- Private cloud: the service only provided to a single organisation. Only members of the organisation can have accesses to the cloud.
- Community cloud: shared infrastructure for specific community.

- Hybrid cloud: this type of cloud environment is composed by two or more cloud deployment models.

(Mohamed & Abdelkader, 2012, p.12)

The cloud computing provides users with scalable resources in the pay-as-you-use fashion at relatively low price. The concept of the cloud computing enables its users to set up their applications and infrastructures more conveniently, hence to improve its management and maintenance. It also allows users to more rapidly and easily to adjust their resources to meet fluctuating and unpredictable requirements.

“65% companies in Europe and North American have made relatively serious commitments to the cloud services according to a 05 December survey of 3,500 businesses released 05 December 2011 by Computer Sciences Corp” (Fogarty, 2012).

Comparing to build their own information system (IS), organisations and individuals can make significant savings by migrate their data into the cloud. With the development of the cloud computing technologies, it is easy to imagine that in the foreseeable future, more users will commit to the cloud. Additionally, Lillard (2010, p.22) suggests that the cloud computing model can also be very useful for digital forensic by allowing storage of very large log files on a storage instance or in a very large database for easy data retrieval and discovery.

1.2 OBSTACLES IN THE CLOUD

However, as promising as it is, cloud computing is also facing many challenges. Since a public cloud is hosted, operated and managed by a cloud vendor, thus it goes beyond the control of the end users. Therefore, digital forensic investigators need to evaluate the risks associated with their evidence data in a cloud vendor for storage or for investigation. Yet, Wan, Liu & Deng (2012, p.743) have pointed out that the cloud vendor is normally a commercial enterprise, which cannot be fully trusted. Digital data

represents crucial evidence to any digital forensic investigation. Disclosure and/or a contamination of such data will seriously compromise any investigation.

Also, evidence data in the cloud environment can be replicated to any data centre in many countries that is owned and operated by the cloud vendors. However, these countries may not necessarily have equivalent legislations regarding data privacy and protection. In such a case, digital forensic investigators may wonder: where will the evidence data be stored? In which countries will the infrastructure be located? What are the security regulations in those countries? Is the evidence data going to be stored in a single physical place (Getov, 2012), or distributed across different sites? More generally, do the evidence data storage, extraction and analysis comply with integrity, preservation, confidentiality and court admissibility requirements during a digital forensics investigation lifecycle?

Moreover, the complication of the inter-linkage layers between the cloud vendors and the digital forensic investigators can provide a fertile ground for hackers and criminals who want to hack into systems for their own purpose. Amazon and Google have had a variety of massive data security incidents in the cloud environment. Researchers (Wang, Zhu & Zhang, 2012, p.151) have stated that in 2009, S3 was interrupted twice respectively in February and July. It led to websites that were lying on a single network storage service to freeze.

Additionally, this can provide grounds for an attacker using the same cloud environment as the investigator, since it is relatively cheap to rent a space in the cloud environment. For example, Amazon's S3 data storage service (Yu, 2010) just charges monthly fee of US\$0.12 to US\$0.15 per gigabyte. Researchers (Ristenpart, Tromer, Shacham & Savage, 2009, p.199) from University of California, San Diego (UCSD) and Massachusetts Institute of Technology (MIT) conducted side attack experiments on EC2. This experiment was based on the assumption that even though attackers and victims used two isolated virtual machines in the same cloud environment, however the fact of both of them share the same physical resources allowed the attack to become possible. The experiment produced a 40% success rate to mount side attacks on EC2.

This experiment shows some alarming results. Firstly, attackers only need to invest very little to conduct attacks in the cloud environment. Secondly, it is possible to

achieve such attack. Since this experiment only utilised standard customer abilities, and it did not require the cloud provider to disclose specific details of infrastructure or assignment policies it is easy to do. Thirdly, though the experiment was conducted on EC2, however it could be generalised on other cloud environments, such as Azure and S3. Overall, it indicates that the tangible dangers exist while deploying sensitive tasks in the cloud.

Meacham & Shasha (2012, p.633) believe that another data security concern with the cloud is that the only assurance of evidence data protection are the word of the cloud vendor, the legal and the business incentives for the vendor not to leak or abuse information. Even if the digital forensic investigator trusts the vendor and the vendor is truly scrupulous and motivated to protect the evidence data, there is still the danger of malicious or sloppy individuals within the vendor's organisation, or some sort of large-scale data breach. These events get into the news with alarming frequency and demonstrate the risk materialising.

Stolfo, Salem & Keromytis (2012, p.125) point out that in 2009, a Twitter employee's account was hacked. More than 310 of the company's documents were stolen, some of them such as financial projections and executive meeting notes containing highly confidential information. At the same time, large numbers of users' accounts were illegally accessed. A frightening number of accounts and services related to Twitter and its employees, such as Gmail, Google Apps, GoDaddy, MobileMe, AT&T, Amazon, Hotmail, Paypal and iTunes were either directly or indirectly affected. Even though the particular attack was launched by an outsider; however it would have been much easier if the attacker was a malicious insider.

Given the above obstacles, the main concerns for the digital forensic investigators when using the cloud, are the cloud governance and security in general, evidence data integrity and preservation specifically.

To overcome these challenges, Hu & Klein (2009, p.735) argue that encryption on evidence data is a feasible technical solution. Using encryption to protect data is nothing new. Wang, et al (2012) state that various encryption algorithms such as DES, 3DES, AES and RSA, have existed for more than a decade. Weis & Alves-Foss (2011, p.49) believe that with substantial amount of evidence data being stored, encryption

seems like the perfect security solution. In fact, it has been now commonly accepted that data encryption in the cloud environment is a good way to mitigate security concerns over evidence data integrity, preservation and confidentiality by the cloud. Indeed, with the possession of the secret key for decryption, digital forensic investigators can still get control of their evidence data regardless where the evidence data may be stored physically. Better yet, (Yang & Zhang (2011, p.145) suggest that data encryption can also help to overcome other concerns such as regulatory compliance and geographic restriction, in the sense that the encrypted data by no means useful without the decryption capability.

1.3 MOTIVATION

Section 1.1 identified and briefly discussed the background to the chosen research area of digital forensic evidence data storage in the cloud environment. In order to understand the reasoning for the chosen research areas, the motivations of the writer will be presented and discussed ranging from the popularity of the cloud computing to the lack of adequate data protection security measures in the cloud environment to ensure data integrity for a digital forensic investigation.

The rapid growth in capacity of storage devices is increasingly challenging digital forensic investigators due to the limited time to create a forensic image of a disk, or process all the data found. Garfinkel (2010) argues that the use of the cloud environments will inevitably exacerbate the problem of data storage and analysis. One solution digital forensic investigators could rely on is the use of the cloud environment for storing evidence and performing analysis. The idea of using the cloud to host a “forensic service” used to conduct investigations has already been proposed by studies such as (Ruan, Carthy, Kechadi & Crosbie, 2011, p.58; Taylor, Haggerty, Gresty & Hegarty, 2010, p.304). Several issues arose and are yet to be addressed including for example, the forensically stable transfer of evidence from the source of the investigation to the cloud storage, and the management of the chain of custody for evidence. Furthermore, those studies have not considered in detail the virtualised nature of clouds, which is likely to have a significant impact on forensic investigations beyond the cloud security.

Moreover, once digital forensic investigators store the evidence data in the cloud environment, the digital data are likely to be scattered in the hard drives, and in different data centres in different countries. Hence, it presents a great challenge to digital forensic investigators as to maintain evidence data storage, extraction and analysis complying with integrity, preservation, confidentiality and court admissibility requirements during digital forensics investigation lifecycle. The following questions are essential to answer before a digital investigator fully commits to storage in the cloud environment.

- Can modern encryption algorithms provide reliability to retain data integrity in the cloud?
- With the investigator not having complete control of the storage, how can the investigator be sure that evidence is not in the process of being altered in the cloud at that moment in time?
- How to protect the privacy of data during investigation?

To ensure that the cloud can be used to deliver forensic investigations, there are still many open issues to be studied, including confidentiality, privacy, integrity and auditability. Some related issues which can be studied in this research include:

- The ability to ensure the evidence is unaltered when transferred to and from as well as when stored in the cloud.
- The ability to ensure the evidence is secure from unauthorized access and maintains the chain of custody.
- The ability to control access to the evidence stored in the cloud, and to ensure that other users of the cloud do not have access to the material.

In summary, the proceeding discussion illustrates the demand for advancement of knowledge in the realm of ensuring evidence data integrity in the cloud environment during digital forensic lifecycle, in order to meet court admissibility requirements. The

research motivations include the increasing popularity of the cloud computing, potential security issues and absolute evidence data integrity requirement during digital forensic investigations. At present greatly limited knowledge of requirements and controls need testing and the robustness of data encryption algorithms in the environment proven. In conclusion, in an optimistic view, the cloud computing provides a bright and promising future for digital forensic investigators to take advantages of. Yet at the same time many unanswered questions remain.

The central focus of the proposed research is to set up a cloud simulation environment and to test a set of well-known encryption algorithms to evaluate the effectiveness and robustness to protect integrity, preservation, confidentiality and court admissibility of evidence data during a digital forensic lifecycle against unauthorised access. In addition, the evaluation will show areas where improvement can be made.

1.4 STRUCTURE OF DISSERTATION

This thesis will be structured in a logical sequence to communicate the research conducted. The formalities section presents an abstract of the thesis, acknowledgements and a table of contents. Additionally, a list of figures and a list of tables are presented as well as a listing of the abbreviations used in the thesis.

Chapter One provides an introduction to the project. The chosen topic area and associated background is put forward including an outline of the cloud computing technologies. A background to the processes and principles of digital forensics is also discussed. The motivations for the project identify the need for the proposed research and investigation in the chosen research area.

Chapter Two provides an extensive review and discussion of the available literature for the topic area in order to build a thorough understanding of the current state of knowledge. The history and the concept of the cloud computing provides an overview of the technology being investigated is followed by a discussion of the security challenges and associated attacks. The process of digital forensics is presented with specific association to the cloud computing storage and potential contamination of evidence data. Modern data encryption algorithms are also covered from the perspective of use in data protection. In closing, the problems and issues surrounding digital forensic

evidence data storage in the cloud demonstrate specific aspects and emphasis on which to focus the research.

The research methodology for the project is critically evaluated in Chapter Three. First, several published similar studies are reviewed in order to be informed on previous research methodologies, as well as to highlight specific ways research is done in this area. The research questions are then developed from the preceding literature discussed in Chapter Two, and the related similar studies. Each question is also accompanied by a hypothesis; a proposed explanation made on the basis of theoretical information and the gathered knowledge. The research questions provide a guide for the thesis and establish the research requirements needed to determine a resolution for each of the proposed questions. Next, the research model is proposed which outlines four specific phases of research testing divided into Phase One and Two for initial testing; and Phase Three and Four for stabilised testing. The system architecture, the necessary components, the software and the hardware requirements are also discussed to provide information regarding to the proposed system design. The data requirements of the research model are then investigated, outlining the data generation, collection, analysis and reporting methodologies that are required for each of the testing phases. The expected outcomes of each phase of research testing are then outlined. The Chapter concludes with a consideration of the limitations of the proposed research methodology and the scope of the testing to be conducted.

Chapter Four reports the findings for each of the research testing phases. First, the variations of the previously proposed data requirements are identified. The subsequent modifications are then applied to the proposed methods. The reported findings are then divided into initial and stabilised testing, with the corresponding four separate phases of testing followed by the analysis of the data gathered. Summing up, the significant and analysed results from the research testing are finally presented in graphical form to visually display the results.

Chapter Five is a discussion of the research findings. To start with, the research questions developed earlier are revisited and arguments made for and against the associated hypotheses are tabled so that a synopsis of the learnt information and results achieved from the testing phases can be viewed. The research findings are then

examined at length. Each phase of testing is discussed, as well as an extensive evaluation of the system design developed and implemented for the research testing. Finally, recommendations are suggested based on the outcomes which were discovered during the conducted research.

Chapter Six concludes the thesis and recommends further topics for study. A conclusion of the research project is presented, stating the most important findings that were achieved and discussing the capabilities of the proposed and tested system design. Limitations of the research are outlined and discussed to identify limitations in the research conducted and findings discovered. Finally, potential future research areas involving using encryption algorithms to protect evidence data integrity during the digital forensic investigation lifecycle in the cloud environment; complete the chapter.

The appendices at the end of the thesis provide additional information regarding the findings; including a full set of collected data from testing and used desktop specifications.

Chapter Two

LITERATURE REVIEW

2.0 INTRODUCTION

In recent years, the concepts and implementations of contemporary distributed information technology infrastructures have been developing in the area of cloud computing. Vendors offer resources, software and information provided to computers and other digital devices as utility to the end users at distant locations. Users can access these services and information through the internet. Consequently, a new field of study has been rapidly merged on the basis of the cloud computing architecture layers with distinct functions offered to users. Lillard, (2010) suggests that the cloud computing can be thought of a simple rental of computer space in another company's data centre.

The origin of the term “*cloud computing*” is unclear. However, the expression of “*cloud*” is commonly used in science to describe a large agglomeration of objects that visually appear from a distance as a cloud, and depict any set of things whose details are not inspected further in a given context. Traditionally, the term of “*cloud*” is used in the following contexts:

- Meteorology: a weather cloud is an agglomeration.
- Mathematics: a large number of points in a coordinate system is mathematics is seen a point cloud.
- Astronomy: stars that appear grouped together in the sky are known as nebula (Latin for mist or cloud), such as the Milky Way.
- Physics: the indeterminate position of electrons around an atomic kernel appears like a cloud to a distant observer.

In analogy to the above expressions, the “*cloud*” was used as a metaphor for the internet and a standardised cloud-like shape was used to denote a network on telephony

schematics. Later it was used to represent the internet in computer network diagrams. Gibbs (2013, p.10) believes that the symbol of cloud was used to represent the internet as early as 1996, in which servers were the shown connected to, but external to the cloud symbol.

The cloud computing provides users with scalable resources in the pay-as-you-use fashion at relatively low price. The concept of the cloud computing enables its users to set up their applications and infrastructures more conveniently, hence to improve its management and maintenance. It also allows users to more rapidly and easily to adjust their resources to meet fluctuating and unpredictable requirements.

“65% companies in Europe and North American have made relatively serious commitments to the cloud services according to a 05 December survey of 3,500 businesses released 05 December 2011 by Computer Sciences Corp” (Fogarty. 2012).

Comparing to build their own IS, organisations and individuals can make significant savings by migrate their data into the cloud. With the development of the cloud computing technologies, it is easy to imagine that in the foreseeable future, more users will commit to the cloud. Additionally (Lillard, 2010), the cloud computing model can also be useful for digital forensics by allowing storage of very large log files on a storage instance or in a very large database for easy data retrieval and discovery.

However, the cloud computing does not only come with benefits. Since a public cloud is hosted, operated and managed by a cloud vendor, thus it goes beyond the control of the users. Therefore, the digital forensic investigators need to give up their evidence data to the cloud vendor for storage or investigation. Yet the cloud vendor is normally a commercial enterprise, which cannot be fully trusted (Wan, et al, 2012). Digital data represent crucial evidence to any digital forensics investigation. Disclosure and/or contamination of such data will seriously compromise any investigation.

To overcome these challenges, encryption on evidence data is a feasible technical solution (Hu & Klein, 2009). Using encryption to protect data is nothing new. Various encryption algorithms such as, DES, 3DES, AES & RSA have existed for more

than a decade (Wang, et al, 2012). With substantial amount of evidence data being stored, encryption seems like the perfect security solution (Weis & Alves-Foss, 2011).

The research objective of Chapter 2 is to critically review the current literature relevant to the three study areas which were introduced in Chapter One, namely the cloud computing, data encryption algorithms and digital forensic principles. First of all, it is vital to understand all aspects of the cloud computing technology, the concepts, architecture, deployment models, potential threats and attacks. The link is then made to the second topic, that of implications for digital forensic investigators committing to the cloud computing and the need for encryption algorithms to maintain the evidence data integrity in order to meet court admissibility requirements.

The literature review will not only serve as a fact-finding undertaking, but will also identify where prospective problems and issues exist from which to derive potential research questions. Chapter 2 is structure into seven main sections. Section 2.1 introduces the history of the cloud computing. Section 2.2 explains the concepts of the cloud computing. Section 2.3 discusses some of popular cloud services. Section 2.4 studies some of obstacles in the cloud computing relating to digital forensic investigation. Section 2.5 introduces a set of modern encryption algorithms. Section 2.6 summaries the problems and issues relating to evidence data protection in the cloud environment during a digital forensic lifecycle. Section 2.7 forms the foundation of the research needed in the area of evidence data encryption in the cloud environment.

2.1 HISTORY OF THE CLOUD COMPUTING

The following sub sections review different historical epochs of cloud development.

2.1.1 The 1950s

The underlying concept of cloud computing dates back to the 1950s, when large scale mainframe computers became available in academia and corporations, accessible via thin clients/terminal computers, since they were used mainly for communication purposes, and had no internal processing capacities. In order to make more efficient use of costly mainframes, a practice evolved that allowed multiple users to share both the physical access to the computer from multiple terminals as well as to share the CPU time. This eliminated periods of inactivity on the mainframe and allowed for a greater

return on the investment. (Christopher, 1959, p.336) The practice of sharing CPU time on a mainframe became known in the industry as time-sharing. During the middle of 70s, it was popularly known as Remote Job Entry (RJE) process, which was mostly associated with IBM and DEC mainframes (Garfinkel, 2011, p.64).

2.1.2 The 1960s – 1990s

In 1960s, McCarthy suggested that “*computation may someday be organised as a public utility*”. In his book, Parkhill (1966, p.156) compared the future computer system as an electricity grid, and thoroughly explained the use of public, private, government and community forms, which contained the most of characteristics of today’s cloud computing concepts.

Other scholars (Rayan, Merchant & Falvey, 2011, p.7) have shown that the concept of cloud computing originated in the 1950s, when scientist Grosch (1958), postulated that the entire world would operate on dumb terminals powered by about 15 large data centres. Due to expense of these powerful computers, many organisations as well as individuals could avail themselves of computing capability through time sharing. Also, he predicted that several corporations, such as IBM, Tymshare and Dial Data could market time sharing as a commercial venture.

2.1.3 The 1990s

In the 1990s, the internet began to grow rapidly (Hwang, Chuang, Hsu & Wu, 2011, p.2), and the increasingly sophisticated network infrastructure and bandwidth dramatically enhanced the stability of various application services available to users through the internet. Telecommunication companies, which previously provide dedicated point-to-point data circuits, began offering virtual private network (VPN) services with cost efficient quality of service. By switching traffic as they saw fit to balance server usages, they could manage the overall network bandwidth more efficiently. Thus, they began to use the cloud symbol to denote the demarcation point between what the vendors were responsible for and what users were responsible for, thus marking the beginning of cloud computing network services.

One of the first milestones for the cloud computing was the launch of Salesforce.com in 1999. It pioneered the concept of delivering enterprise applications

via a simple website. The services firm (Salesforce, 2011) paved the way for both specialist and mainstream software firms to deliver applications over the internet. Hence, the cloud computing extends this boundary to cover servers (Yadav, Jain & Fisal, 2012, p.114) as well as the network infrastructure.

2.1.4 from 2000 to Date

After the dot-com bubble, Amazon played a key role in all the development of the cloud computing by modernising their data centres, which like the most of other computer networks, were using as little as 10% of their processing power at any one time, just to leave enough room for occasional spikes. So, in 2002 Amazon Web Services (AWS) was launched. It provided a suite of cloud services, such as storage, computation and even human intelligence through Amazon Mechanical Turk (AMT).

Having found that the new cloud architecture resulted in significant internal efficiency improvements that could add new features faster and more efficiently, Amazon initiated a new product development effort to provide the cloud computing to external customers. In 2006, Amazon expanded its cloud services. First it launched EC2, which provides a commercial web service that allows small companies and individuals to rent computers on which to run their own computer applications. Later a web based data storage service – S3 was introduced. This offered the pay-as-you-go cloud model (Bloomberg Business Week, 2006; Brooks, 2010) to both users and the industry as a whole. Now, such a model has become the standard cloud computing business model.

In 2009, Google Apps (Google, 2013) was launched. It allows people to create and store documents entirely in the cloud. On 01 February 2010, Microsoft Windows released its cloud computing platform (Windows Azure, 2013) – Azure for building, deploying and managing applications and services through a global network of Microsoft managed data centres. It provides both Paas and Iaas. On 01 March 2011, IBM announced its SmartCloud (IBM, 2011) framework to support Smarter Planet, which is a crucial component of the Smarter Computing foundation.

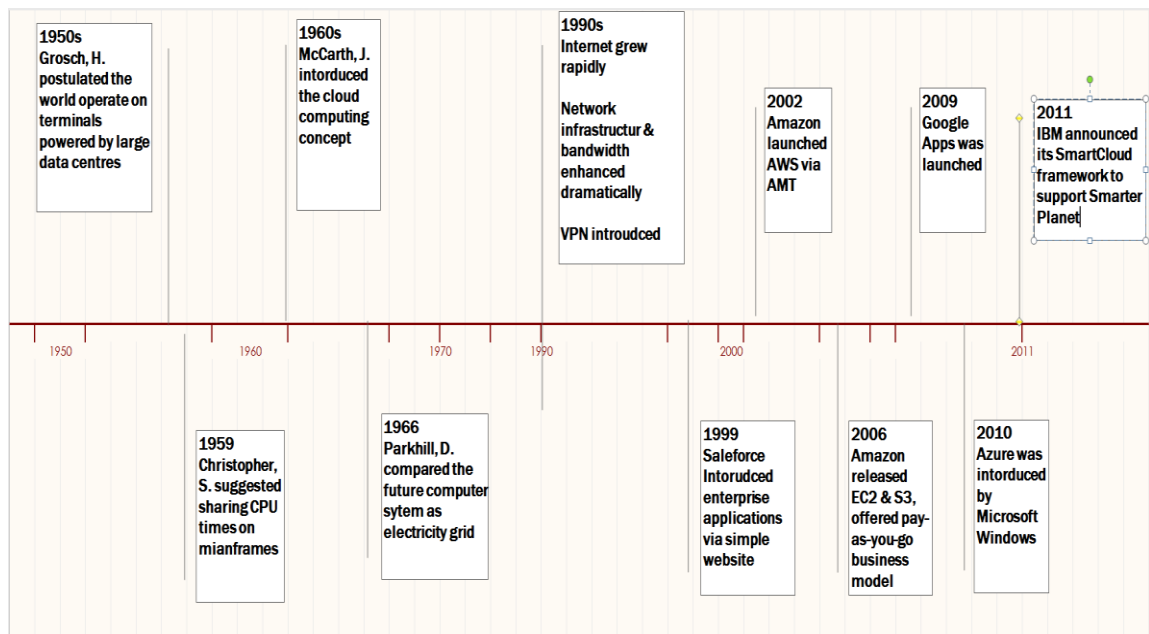


Figure 2.1: Brief History of the Cloud Computing.

2.2 CONCEPTS OF THE CLOUD COMPUTING

The previous section briefly discussed the history of cloud computing development, and some of current cloud computing services. However, some people may even wonder what exactly the cloud computing is, since these services do have some similarities, and at the same time are differentiated by functions and features. In this section, the researcher will discuss the concept of the cloud computing in much detail. Section 2.1.2.1 discusses the definition of cloud computing. Section 2.1.2.2 looks at some of characteristics of the cloud computing. Section 2.1.2.3 explains services models of the cloud computing. Section 2.1.2.4 introduces the cloud computing deployment model. Finally, Section 2.1.2.5 briefly discusses some of the cloud computing architecture types.

2.2.1 Definition of the Cloud Computing

Huang & Liao (2012, p.142) believe that the cloud computing is a large scale distributed computing paradigm. Somani, Lakhani & Mundra (2010, p.211) argue that it is often difficult to define the cloud computing. Bracci, Corradi & Foschini (2012, p.812) point out that According to National Institute of Standards and Technology (NIST), the

definition of the cloud computing is model for enabling convenient, on-demand network access to a shared pool of configurable computing resources, including networks, servers, storage, application and services that can be rapidly acquired, provisioned and released with minimal management effort or services provider interaction.

Hwang, et al (2011) state that as a concept, the cloud computing's primary significance lies in allowing the end users to access computation resources through the internet. Some scholars (Baker, Buyya & Laforenza, 2002, p.1437) have found that the cloud computing was similar to grid computing. Yet some (Yeo, Venugopal, Chu & Buyya, 2010, p.1466) also find similarities to utilities such as water and electrical power, hence refer to it as utility computing. Since the use of resources can be independently adjusted, Kandukuri, Paturi & Rakshit (2009, p.517) believe that it is also sometimes referred to as autonomic computing. Figure 2.2 shows the concept of the cloud computing map.

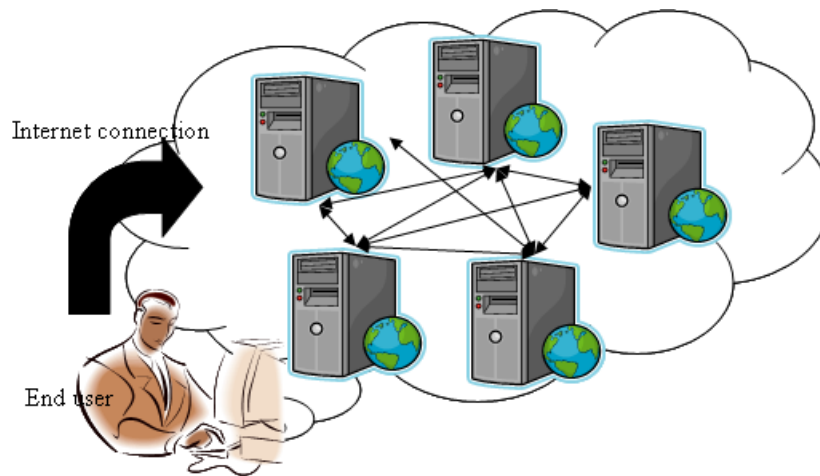


Figure 2.2: The cloud Computing Concept Map.

Source: (Hwang, et al, p.1)

After making thorough comparisons on scholarly definitions of the cloud computing, Vaquero, Roderio-Merino, Caceres & Lindner (2009, p.599) suggested the cloud computing could be defined as the integration of virtual resources according to user requirements, flexibly combining resources including hardware, development platforms and various applications to create services.

2.2.2 Characteristics of the Cloud Computing

Some researchers (Mohamed, et al, 2012; Gibbs, 2013) have summarised the following characteristics of the cloud computing:

- Self-provisioning of resource: users have ability to re-provision technological infrastructure resources.
- Application programming interface (API) accessibility to software: it enables machines to interact with cloud software in the same way as the user interface facilitates interaction between users and computers.
- Pay-as-you-go: users only need to pay for the resources that they actually use and the period that they use. Hence, cost is claimed to be reduced. Also, Subramania (2009) points out that in a public delivery model, capital expenditure is converted to operational expenditure. Its main purpose is to lower barriers to entry, since infrastructure is typically provided by a vendor, and does not need to be purchased or infrequent intensive computing tasks. For example, both Yu (2010) & Lillard (2010) state that Amazon's S3 data storage service just charges monthly fee of US\$0.12 to US\$0.15 per gigabyte. The e-FISCAL project's state of the art repository (Gibbs, 2013) contains several articles looking into cost aspects in more details. Most of them concluded that costs savings depend on the type of services provided and the type of infrastructure available in-house.
- Device and location independency: users only need the internet and web browsers to access systems regardless of their location or what device they using, such as users can access iCloud using PC, iphone as well as ipad.
- Virtualisation: it allows multiple operating systems (OS) and applications run concurrently on a host computer. Popek & Goldberg (1974, p.412) argued that virtualisation presented to the guest OS a virtual operating platform and managed the execution of the guest OS.

- Multi-tenancy: the cloud computing is built on a business model, where resources and costs are shared by a large pool of users. Thus, it allows that
 - Centralised infrastructure in locations with lower cost, such as real estate and electricity.
 - Increased peak load capacity. Users do not need to engineer for the highest possible load levels.
 - He, Guo, Ghanem & Guo (2012, p.574) believe that improved utilisation and efficiency for systems that are often only 10-20% utilised.

- Reliability (King, 2008): if multiple redundant sites are used, then reliability can be improved. Thus, it makes well designed cloud computing envrioning for business continuity and disaster recovery.

- Massive scalability (He, Guo, Ghanem & Guo, 2012, p.15): the cloud computing provides the ability to scale to tens of thousands of systems, massive storage spaces as well as bandwidth.

- Elasticity (He, et al, 2012): users can rapidly increase and decrease their computing resources as needed.

- Performance: Vendors constantly monitor the cloud environment performance. Katsaros, Kousiouris, Gogouvitis, Kyriazis, Menychtas & Varvarigou (2012, p.1029) suggest that performace of the cloud is a set of consistent and loosely grouped architectures are constructed using web services as the system interface.

- Security: certain security features can be improved (Hu & Klein, 2009; Huang & Liao, 2012; Bracci, et al, 2012) due to the centralised data and security focused resources. However, strong concerns about loss of control over certain sensitive data, and the lack of security for stored kernel, Generally speaking, the cloud computing security is often as good as or even better than other traditional systems. This is partially because vendors are able to devote resources to solve

security issues that many customers cannot afford. However, the complexity of security is greatly increased when data is distributed over a wider area or greater number of devices and in multi-tenant systems that are being shared by unrelated users. Additionally, some researchers (Li, Yu, Cao & Lou, 2011, p.383; Deng, Petkovic, Nalin & Baroni, 2011, p.549) point out that user's access to security audit logs may be difficult if it is not impossible.

- Maintenance: depending on type of services that users acquire, the cloud computing maintenance is much easier than a traditional information system, and it can be access from different sites.

In their report, Mell & Grance (2011) stated that NIST also identified five essential characteristics of the cloud computing:

- On-demand self-service: a consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service vendor.
- Broad network access: capabilities are available over the network and access through standard mechanisms that promote use by heterogeneous thin or thick client platforms, such as mobile phones, tablets, laptops and workstations.
- Resource pooling: the vendor's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.
- Rapid elasticity: capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear unlimited and can be appropriated in any quantity at any time.

- **Measured service:** the cloud computing automatically control and optimise resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service, such as storage, processing, bandwidth and active user accounts. Resource usage can be monitored, controlled and reported, providing transparency for both the vendor and consumer of the utilised service.

2.2.3 Service Models of the Cloud Computing

Both Yu (2010) and Mohamed (2012, p.2) believe that since Amazon EC2 & S3 established pay-as-you-go fashion at relatively low price, X-as-a-service business model has become the standard industry business model. The “X” can be hardware, software, data storage, security, communication and monitoring. This has commonly accepted that the cloud computing have three services model (Getov, 2012; Gibbs, 2013; Hu & Klein, 2009; Huang & Liao, 2012; Hwang, et al, 2011; Kulkarni, Gambhir, Patil & Dongare, 2012, p.548; Mohamed, et al, 2012; Weis & Alves-Foss, 2011; Yu, 2010): Iaas, Paas and Saas.

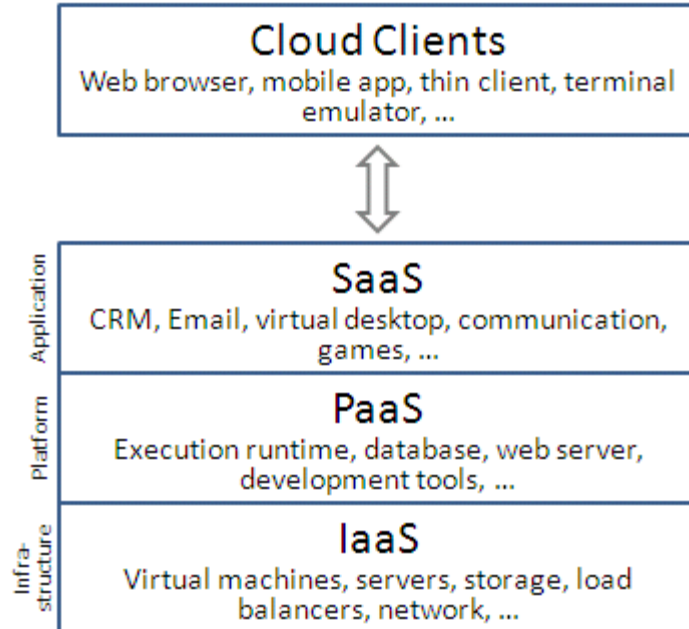


Figure 2.3: Three Service Models of the Cloud Computing.

Source: (Gibbs, 2013, p.11)

IaaS refers to Infrastructure-as-a-service, which is the most basic cloud service model. Vendors offer services for computers and infrastructures such as storage, firewall and network system, or more often as virtual machines and other resources. These resources are provided on requests from the vendors' large pools installed in data centres including IP addresses as well as configurations of dedicated virtual private networks (VPN) through the Internet for the wide area connectivity. To use their applications, users can install their application software and operating system images on the computers. In this model, the cloud users have the sole responsibilities to patch and maintain their operating system and application software. In fact, IaaS refers not to a machine that does all the work, but simply to a facility given to businesses that offers users the leverage of extra storage space in servers and data centres.

Examples of IaaS include Amazon CloudFormation and underlying services (Gibbs, 2013; Lillard, 2010; Armbrust, Fox, Griffith, Joseph, Katz; Konwinski, Lee, Patterson, Rabikin, Stoica & Zaharia, 2009, p.2) such as Amazon EC2, Rackspace Cloud, Google Compute Engine and RightScale.

In order to accommodate requirement of running different operating systems and applications on the same resource pools concurrently in a cloud environment, it needs to have a technology to support such operations. This is done using a hypervisor.

“Hypervisor is also called virtual machine manager (VMM). It allows multiple operating systems run concurrently on a host computer. VMM presents to the guest operating systems a virtual operating platform and manages the execution of the guest operating systems. Hence, it enables multiple of a variety of operating systems share the virtualised hardware resources.” (Popek & Goldberg, 1974)

VMM is an interface of a specific cloud computing IaaS functionality. Popek & Goldberg (1974) classified two types of VMM:

- Type 1 (Native, Bare Metal) VMMs run directly on the host's hardware to control the hardware and to manage guest operating system. A guest operating

system thus runs on another level above the VMM. This model represents the classic implementation of virtual machine architectures.

- Type 2 (Hosted) VMMs run within a conventional operating system environment. With the VMM layer as a distinct second software level, guest operating system run at the third level above the hardware.

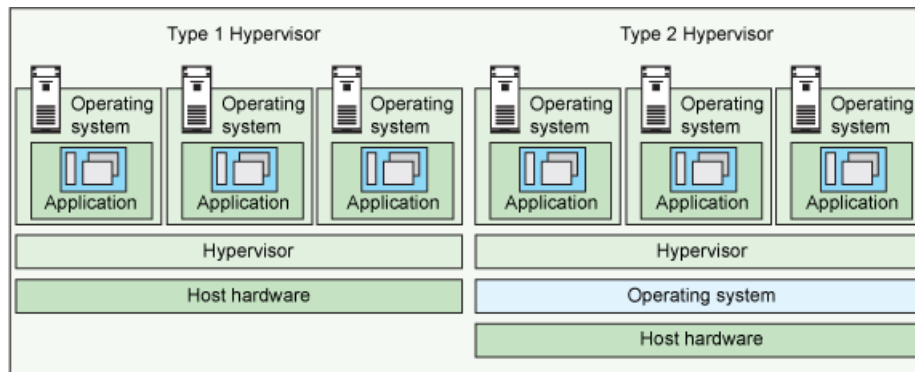


Figure 2.4: Type 1 & Type 2 Hypervisors.

Source: (Tholeti, 2011, p.3)

Paas refers to Platform-as-a-service. In this model, vendors provide platforms such as OS, programming language execution environment, data centre, web and mail servers with virus scanning and monitoring services as well as anti-spam services. This model could benefit developers to set up a required software environment on the cloud without the need to buy and manage expensive and complicated underlying hardware and software layers. Gibbs (2013), Lillard (2010) and Armbrust, et al (2009) have listed examples of Paas, which included Amazon Elastic Beanstalk, Heroku, EngineYard, Google App Engine and Microsoft Azure.

Saas refers to Software-as-a-service. Hamdaqa, Livogiannis, & Tahvildari (2011, p.98) argue that in this cloud service model, vendors install, operate, maintain and update user required applications. Users can access the software from cloud clients. They do not need to manage the underlying structures on which the applications are running. This can reduce the overhead to install and manage the applications on the users' computers. Therefore, it simplifies maintenance and support requirements. The

cloud replicates user processing data onto multiple virtual machines (VM) at run time. This allows the cloud to meet multiple users' needs concurrently.

Load balancers distribute the work over the set of virtual machines. This process is inconspicuous to the users who see only a single access point. To accommodate a large number of users, cloud applications can be multi-tenant. That is, any machine serves more one cloud user organisation. It is commonly referred to special types of cloud based application software with a similar naming convention, such as desktop-as-a-service, business-process-as-a-service and communication-as-a-service. . Gibbs (2013), Lillard (2010) and Armbrust, et al (2009) have listed examples of Saas, which included Google Apps, Quickbooks Online and Salesforce.com.

2.2.4 The Cloud Computing Deployment Models

Generally speaking, the cloud computing is categorised four types of deployment models, which are public cloud, community cloud, private cloud and hybrid cloud suggested by (Getov, 2012; Gibbs, 2013; Hu & Klein, 2009; Huang & Liao, 2012; Hwang, et al, 2011; Kulkarni, et al, 2012, p.548; Mohamed, et al, 2012; Weis & Alves-Foss, 2011; Yu, 2010).

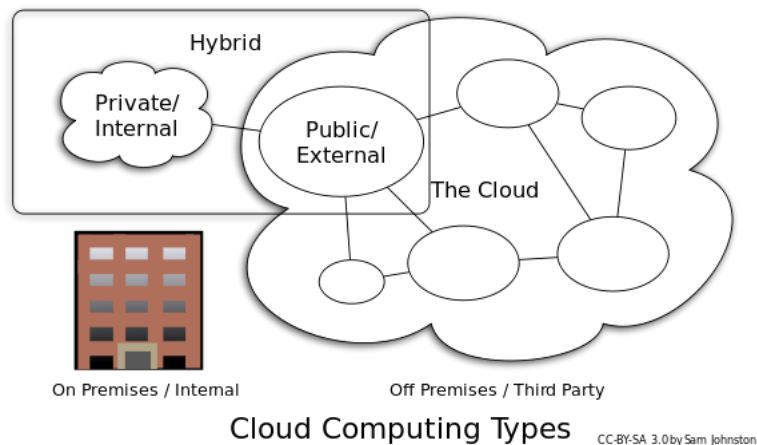


Figure 2.5: The Cloud Computing Types.

Source: (Gibbs, 2013, p.13)

In public cloud, software, hardware and other information system resources are made available to the general public by a vendor. Usually, these services are free or offered on a pay-as-you-go model. Gens (2008) believes that generally, public cloud service vendors such as Microsoft, Google and IBM own and manage the infrastructure. The only access medium is the internet. Direct connectivity is not offered.

In their report Mell & Grance (2011) stated that private cloud was cloud infrastructure operated solely for a single organisation. It is either managed internally or by a third-party, as well as hosted either internally or externally. Undertaking a private cloud project requires a significant level and degree of engagement to virtualise the business environment, and it will require the organisation to re-evaluate decisions about existing resources. When it is done right, it can have a positive impact on a business. However, if every one of the steps in the project raises security issues, which must be addressed in order to avoid serious vulnerabilities

The private clouds have attracted criticism because users “*still have to buy, build, and manage them*” (Foley, J., 2008), and thus do not benefit from less hands-on management. Essentially “*(lacking) the economic model that makes cloud computing such an intriguing concept*” (Haff, 2009; Murraray, 2009).

Community cloud shares infrastructure between several organisations (Mell & Grance, 2011) from a specific community with common concerns, such as security, compliance and jurisdiction. Similar to private cloud, it can be managed either internally or by a third-party, and host either internally or externally. The costs are shared among the fewer users comparing with the public cloud, but more than the private cloud. Hence, only some of the cost savings potentials of the cloud computing are realised.

Hybrid cloud is a composition of two or more clouds (Mell & Grance, 2011) that remain unique entities but are bound together, offering the benefits of multiple deployment models. Taylor & Metzler (2010) believe that such composition expands deployment options for cloud services, allowing IT organisations to use public cloud computing resources to meet temporary needs. This capability enables hybrid clouds to employ cloud bursting (Mell & Grance, 2011) for scaling across clouds. The cloud bursting is an application deployment model in which an application runs in a private cloud or data centre and “*bursts*” to a public cloud when the demand for computing

capacity increases. Rouse (2011) defines that a primary advantage of the cloud bursting and a hybrid cloud model is that an organisation only pays for extra computing resources when they are needed.

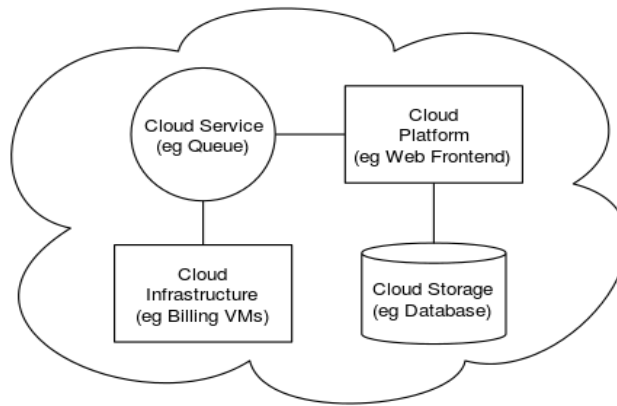


Figure 2.6: The Cloud Computing Sample Architecture.

Source: (Gibbs, 2013, p.14)

Vizard (2012) suggests that the cloud bursting enables data centres to create an in-house IT infrastructure that supports average workloads, and use cloud resources from public or private clouds, during spikes in processing demands.

By utilising hybrid cloud architecture, companies and individuals are able to obtain degrees of fault tolerance combined with locally immediate usability without dependency on the internet connectivity. A hybrid cloud architecture requires both on-premises resources and remote server based cloud infrastructure. Hybrid clouds lack the flexibility (Stevens, 2011), security and certainty of in-house applications. A hybrid cloud provides the flexibility of in house applications with the fault tolerance and scalability of cloud based services.

2.2.5 The Cloud Computing Architecture

Cloud architecture defined by Varia (2008) is such that the systems architecture of the software systems involved in the delivery of cloud computing, typically involves multiple cloud components communicating with each other over a loose coupling

mechanism, such as a messaging queue. Elastic provision implies intelligence in the use of tight or loose coupling as applied to mechanisms such as these and others.




The definition of inter-cloud suggested by Bernstein, Ludvigson, Sankar, & Diamond (2009, p.328) as well as Davis (2009) is an inter-connected global “cloud of clouds”, and an extension of the internet “network of networks” on which it is based.

2.3 EXAMPLES OF THE CLOUD TECHNOLOGY

In the previous sections, the researcher mentioned some popular cloud computing examples, such as Amazon EC2, Microsoft Azure and Google App Engine. In this section, the researcher will have a closer look at those examples.

Researchers (Armbrust, et al, 2009) from University of California at Berkeley (UCB) conducted experiments to compare those of popular cloud computing services from the point of virtualised resources in order to ensure scalability and high availability.

Table 2.1: Examples of the Cloud Computing Services & Comparison

	 EC2	 Windows Azure	 Google App Engine
Computation Model (VM)	<ul style="list-style-type: none"> • X86 Instruction Set Architecture (ISA) via Xen VM • Computation elasticity allows scalability, but developer must build the machinery or third party VAR, such as RightScale must 	<ul style="list-style-type: none"> • Microsoft Common Language Runtime (CLR) VM • Common intermediate form executed in managed environment • Machines are provisioned based 	<ul style="list-style-type: none"> • Predefined application structure and framework • Programmer provided “handlers” written in Python, all persistent state stored in MegaStore (outside Python code) • Automatic scaling up and down of

	provide it	on declarative description (e.g. which “role” can be replicated); automatic load balancing	computation and storage <ul style="list-style-type: none"> • Network and server failover • All consistent with 3-tier web app structure
Storage Model	<ul style="list-style-type: none"> • Range of models from block store to augmented key/blob store • Automatic scaling varies from no scaling or sharing to fully automatic (S3) depending on which model used • Consistency guarantees vary widely depending on which model used • APIs vary from standardised to proprietary 	<ul style="list-style-type: none"> • SQL Data Services (restricted view of SQL Server) • Azure storage service 	<ul style="list-style-type: none"> • MegaStore/BigTable
Networking Model	<ul style="list-style-type: none"> • Declarative specification of IP level topology • Internal placement details concealed • Security Groups 	<ul style="list-style-type: none"> • Automatic based on programmer’s declarative descriptions of app components (roles) 	<ul style="list-style-type: none"> • Fixed topology to accommodate 3-tier web app structure • Scaling up and down is automatic and programmer invisible

	enable restricting which nodes may communicate <ul style="list-style-type: none"> • Availability zones provide abstraction of independent network failure • Elastic IP addresses provide persistently routable network name 		
--	---	--	--

Source: (Armbrust, et al, 2009)

2.3.1 Amazon EC2

On 25 August 2006, Amazon launched EC service. EC2 is a central part of Amazon’s cloud computing platform. It allows users to rent virtual computers on which to run their own computer applications. Also, EC2 provides scalable deployment of applications by offering a web service through which a user can boot an Amazon Machine Image to create a virtual machine, which Amazon calls an “*instance*”, containing any software desired. A user can create, launch and terminate server instances as needed, paying by the hour for active servers, hence the term of “*elastic*”. EC2 provides users with control over the geographical location of instances that allows for latency optimization and high levels of redundancy (Brooks, 2010; Gibbs, 2013, LaMonica, 2008; Tajadod, Batten & Govinda, 2012, p.539; Armbrust, et al, 2009; Mohamed, et al; 2012).

2.3.2 Microsoft Azure

On 01 February 2010, Microsoft Windows released its cloud computing platform – Azure for building, deploying and managing applications and services through a global network of Microsoft managed data centres. It provides both Paas and Iaas as well as

many different programming languages, tools and frameworks, including both Microsoft specific and third-party software and systems (Window Azure, 2013; Gibbs, 2013; Lillard, 2010; Armbrust, et al, 2009; Mohamed, et al, 2012; Tajadod, 2012).

2.3.3 Google App Engine

In 2009, Google Apps (Google, 2013) was launched. It is a Paas cloud computing platform for developing and hosting web application in Google managed data centres, and allows people to create and store documents entirely in the cloud. Applications are such as sandboxed and run across multiple servers (Google, 2013). Google App Engine offers automatic scaling (Sanderson, 2009, p. 57; Gibbs, 2013; Lillard, 2013; Ambrust, et al, 2009; Mohamed, et al, 2012) for web applications – as the number of requests increases for an application, App Engine automatically allocates more resources for the web application to handle the additional demand.

2.4 OBSTACLES IN THE CLOUD RELATING TO DIGITAL FORENSIC INVESTIGATION

Comparing to build their own IS, organisations and individuals can make significant savings by migrate their data into the cloud. With the development of the cloud computing technologies, it is easy to imagine that in the foreseeable future, more users will commit to the cloud. Moreover, Lillard (2010) argues that the cloud computing model can also be very useful for digital forensics by allowing storage of very large log files on a storage instance or in a very large database for easy data retrieval and discovery.

However, as promising as it is, cloud computing is also facing many challenges. Wan, et al (2012) point out that since a public cloud is hosted, operated and managed by a cloud vendor, thus it goes beyond the control of the users. Therefore, digital forensic investigators need to give up their evidence data to the cloud vendor for storage or investigation. Yet the cloud vendor is normally a commercial enterprise, which cannot be fully trusted. Digital data represents crucial evidence to any digital forensics investigation. Disclosure and/or contamination of such data will seriously compromise any investigation.

2.4.1 Digital Forensic

Further discussion of the challenges regarding storing evidence data in the cloud environment during digital forensic lifecycle, requires definition of what digital forensics is, and what characterises and requirements are. According to Cusack (2012) digital forensics involves obtaining and analysing digital information as evidence in civil, criminal or administrative cases. The tasks of digital forensic include recovering data that users have hidden or deleted, which can be used as incriminating or exculpatory evidence. Digital forensics includes the follow areas:

- Network forensics: it yields information about how perpetrator or an attacker gained access to a network.
- Data discovery: it recovers information that was deleted by mistake or lost during a power surge or server crash. Before conducting data recovery, investigators know exactly what data they are looking for.
- Disaster recovery: it uses digital forensics techniques to retrieve information that clients have lost.

There are four different stages during digital forensics investigation lifecycle (Cusack, 2012), which are acquisition, extraction, analysis and reporting.

Phase 1	Phase 2	Phase 3	Phase 4
Acquisition	Extraction	Analysis	Reporting
<- -- Preservation of Evidence -- ->			
<- -- Chain of Custody -- ->			

Figure 2.7: Digital Forensic Lifecycle.

Source: (Cusack, 2012)

2.4.1.1 Acquisition

Britz (2009, p.297) suggests that acquisition can be defined as the method of copying data from one media to another on a bit level, ensuring the transfer of every bit from the original media is copied in an exact representation on the storage media being used without altering the original data. The term refers both to the collection of evidentiary forensic images as well as those data pertinent to the case gathered from any digital device in support of an investigation.

Acquisition processes includes collection of volatile network, memory and system state information; and collection of non-victim server and network application logs to include intrusion detection system logs and network streams. Once volatile evidence has been considered and obtained, evidence data will be acquired using the following steps: identify and document digital devices that need to be acquired and document hardware configuration and physical properties.

During the acquisition phase, every reasonable effort should be taken to minimize modifications to the system. Especially prior to any forensic acquisition, where feasible, a write blocker should be employed; evidentiary logs and other logical digital evidence should be handled in the same manner as forensic image, especially with regard to integrity checking.

Acquisitions can be performed through a variety of methods. A few examples include: through the use of a 'single-use Device,' such as a handheld imaging tool, via a network monitoring device, or via the simple act of obtaining logs from intrusion detection systems. Both Britz (2009) and Cusack (2012) argue that proper acquisition is the cornerstone of digital forensic investigation. Improperly acquired evidence can lead to the alteration, damage or destruction of data. Every effort must be made to acquire with minimal invasiveness and impact on the target system.

Documentation of any process used to gather digital evidence must be thorough and provide a detailed description of all steps taken, software used and changes made to any running digital device. The ultimate goal of the forensic acquisition is to ensure that investigators have identical image of the original evidence to work from. The primary reason for working from the copy of the original images is that investigators will never be able to reproduce that information if the original is altered or changed. This can have

a significant impact if the information is requested by the defence attorney in a legal proceeding.

2.4.1.2 Extraction

Data that is acquired should be examined using a combination of automated and manual methods to assess and extract data of particular interest for the specific situation while preserving the integrity of the data.

Britz (2209) and Cusack (2012) define that extraction is performed on a forensic copy, extracted data from deleted, hidden, password protected data email including deleted email; data from reformatted or repartitioned hard drives; data from unallocated and slack space; file created, modified and last accessed times; web sites visited and files transferred.

2.4.1.3 Analysis

The result of the extraction should be analysed (Britz, 2009; Cusack, 2012), using well-documented methods and techniques, to derive useful information that address the questions that were the impetus for the collection and extraction. This involves finding who did the alleged action, what allegedly happened, where and why and finding out how it all lines up to point to a conclusion.

Analysis of digital evidence should be conducted on working copies of evidentiary data. Analysis can be conducted on the following layers:

- Physical: this layer applies to any physical item the can be seen or held. It can apply to computer systems, removable media; device description, manufacturer, model, serial number, property control number or other unique identifiers.
- Media management: this layer applies to the data storage capabilities of the device: size of available storage, number of storage volumes on the device; type of storage volume; record the partition or volume table or map and correlate number and size of volumes with available storage. File system describes the way files or other data records are stored on a disk. File system are most commonly managed by a computer operating system: type, label, size, allocated block size and version.

- Application layer: analysing at this layer is completely dependent upon the supporting facts and focus of investigation, support request and type of device being analysed. The following should be identified and reported as applicable: operating system and version, and/or firmware for some electronic storage devices; common operating system configuration settings. This will largely depend on the needs of the investigation; identification of extracted data, meta-data and hashes.

2.4.1.4 Reporting

The result of the analysis should be reported. Items to be reported may include: a description of the actions employed; an explanation of how tools and procedures were selected; a determination of any other actions that should be performed, such as forensic examination of additional data source, securing identified vulnerabilities, and improving existing security controls; and recommendations for improvements to policies, guidelines, procedures, tools and other aspects of the forensic process.

Context includes background and general information on the case, analysis overview and suspected role of the system being examined. Scope includes underlying search authority, specific parameters requested by investigator; item analysed including particularly identify items examined or acquired; system clock, time zone settings and system overview; and general procedures followed.

A Summary of findings should within both the context of the underlying investigation and the scope of the forensic exam, provide the requestor a succinct description of what potentially relevant data was discovered. Detailed findings include complete evidentiary file. A Report must be written with the target audience in mind. In those cases where technical material is included and definitions are not clear, terms should be defined.

The goal of reporting is to accurately describe the details of an incident. Therefore, it is essential to be:

- Understandable to decision makers
- Able to withstand a barrage of legal scrutiny

- Ambiguous and not open to misinterpretation
- Easily reference; contain all information required to explain investigators' conclusions
- Offering valid conclusions, opinions or recommendations when needed and be created in a timely manner.

Any conclusions from the examination of evidence should clearly be distinguished from the results of tests and examinations. Any limitations to the results and conclusions should be explained. Opinions should be expressed in simple, precise and unambiguous terms. Reports must be signed only by the examiner that has carried out the work.

2.4.1.5 Preservation of Evidence and Chain of Custody

Preservation refers to keeping things from being altered. Ideally, the original copy that investigators make or copies stay unchanged. Any other work is done on a copy of a copy that can be verified as unchanged.

Chain of custody is a legal term that refers to the ability to guarantee the identity and integrity of the specimen from collection through to reporting of the test results. Its purpose is maintaining credible protection of evidence in custody. It is essentially important to keep the chain of custody in place to ensure that a forensic lifecycle reflects how the investigation was conducted, and to avoid the risk of mishandling evidence.

Hence, a proper chain of custody procedure should always be strictly observed. This includes a thorough documentation of sources of data, the use of “write-blocking” devices to ensure no data changes take place inadvertently, initial forensic screening of disk drives for relevant data and making bit-for-bit copies of hard drives.

Also, the chain of custody ensures that digital fingerprints match up at all stages of investigation, and that documentation of all evidence including photography and serial numbers of inventory of all evidence artefacts as well as maintaining case logs for all evidence related activities is performed.

2.4.2 Challenges of Digital Forensic in the Cloud Environment

From the above discussion, it shows that maintaining evidence data integrity is absolute paramount in digital forensic investigators. Therefore, the main challenge that digital

forensics is facing in the cloud environment is how to main evidence data integrity in each phase of digital forensic lifecycle, in order to meet court admissibility requirements. In the author's opinion the main challenge is composed by two obstacles, namely the cloud governance and security.

2.4.2.1 The Cloud Governance

Once evidence data have been stored in the cloud environment, they can be replicated to any data centre in many countries that is owned and operated by the cloud vendors. However, these countries may not necessarily have equivalent legislations regarding data privacy protection.

In October 2013, Google, Microsoft, Facebook and Yahoo have written to New Zealand Communications Minister Amy Adams (One News, 15 October 2013) urging New Zealand Government not to pass the Telecommunications Interception Capability and Security (TICS) Bill (One News, 13 July 2013).

The TICS bill is companion legislation to New Zealand Government Communications Security Bureau Law (Young, 2013; Wong, 2013), which allows certain information to be provided to the New Zealand Police, Defence Force and the Security Intelligence Service. The TICS bill will oblige telecommunications firms to provide assistance to the Government Communication Security Bureau (GCSB) in intercepting and decrypting communications. It will also force them to follow the GCSB's instructions on network security.

The companies said in the letter that the bill could oblige any "blogging platform, social network, email service or other online forum", anywhere in the world, to provide assistance to GCSB. However, this can cause conflict with those companies' privacy and confidentiality obligations in other countries. According to The United States of America privacy laws (Solove & Schwartz, 2011, p.168; Social Security), U.S. companies are not allowed ever to pass customers' information directly to another country's intelligence services. The four firms said internet companies could be forced to choose between breaking New Zealand law, breaking the law in their own home countries, or withdrawing their services from New Zealand.

Another problem with the cloud governance is data security ambiguity. In May 2010, CA Technologies and the Ponemon Institute jointly released the Security of Cloud

Computing Users study, involving 642 U.S. and 283 European the cloud computing users. According to their Chart 11 (Tajadod, et al, 2012), only 32% of the users and 32% the vendors believe the cloud vendor should be responsible for ensuring the security of cloud services. However, 69% of vendors believe the users as most responsible for security, while only 35% of users believe they are most responsible for ensuring security.

These differences of opinion between the users and the vendors about who is responsible for securing the cloud mean that organisations may be over relying on their cloud vendors to provide safe cloud computing environment.

In such a case, digital forensic investigators may wonder: where will the evidence data be stored? In which countries will the infrastructure be located? What are the security regulations in those countries? Is the evidence data going to be stored in a single physical place (Getov, 2012) or distributed across different sites? More generally, do the evidence data storage, extraction and analysis comply with integrity, preservation, confidentiality and court admissibility requirements during digital forensics investigation lifecycle?

2.4.2.2 The Cloud Security

Also, the complication of the inter-linkage between the cloud vendors and the digital forensic investigators can provide a fertile ground for hackers and criminals who want to hack into systems for their own purpose. Amazon and Google have disclosed a variety of massive data security incidents in the cloud environment. Wang, Zhu & Zhang (2012, p.150) point out that in 2009, S3 was interrupted twice respectively in February and July. It led websites that laying on a single network storage services to paralysis.

Additionally, the cloud computing can provide ground for an attacker using the same cloud environment as well, since it is relatively cheap to rent a space in the cloud environment. For example, Amazon's S3 data storage service just charges monthly fee of US\$0.12 to US\$0.15 per gigabyte (Yu, 2010). Researchers (Ristenpart, et al, 2009) from University of California, San Diego (UCSD) and Massachusetts Institute of Technology (MIT), conducted side attack experiment on EC2. This experiment was based on the assumption that even though attacker and victim used two isolated virtual machines in the same cloud environment, however the fact of both of them share the

same physical resources allowed the attack had become possible. The experiment produced a 40% success rate to mount side attacks on EC2.

This experiment has shown some alarming results. Firstly, attackers only need to invest very little to conduct attacks in the cloud environment. Secondly, it is possible to achieve such an attack. Since this experiment only utilised standard customer abilities, and it did not require the cloud provider to disclose specific details of infrastructure or assignment policies. Thirdly, though the experiment was conducted on EC2, however it could be generalised from other cloud environments, such as Azure and S3. Overall, it indicates that the tangible dangers exist while deploying sensitive tasks in the cloud.

Malware and rootkits are also able to install themselves as VMMs below the cloud operating system, which can make them effectively hiding from anti-virus software, since they can intercept the OS operations without being detected. Once malware infects the cloud, in order to maintain its residence, it has to either:

- Pretend to be a legitimate program in order to get control and avoid being detected by an auditing program; or
- Actively remaining in the memory space.

In his article “Malware and Cloud Jacking”, Jon Shende (2010) states that

“It can then use this access to infinite computing power and storage to compute values needed by the verification authority on the infected system thereby avoiding detection and possible moving undetected throughout any array of networks; wreaking undetected havoc as it processes data.”

There are two types of known attacks on the hypervisor which are hyper jacking and VM escape. Hyper jacking (McKay, 2011) means VMM stack jacking. It involves an attacker inserting a rogue VMM. It assumes that it is difficult to detect the insertion for any operation systems running on the VMM. It can allow attack gain potential control of

any VMs on the physical machine. Examples of such malwares are Blue Pill, SubVirt and Vitriol.

One method of hyper jacking is to overwrite page files on disk which contains paged out kernel code. This can be achieved by forcing kernel to be paged out by allocating large amounts of memory. It searches for an unused driver in page file and replaces its dispatch function with shell code. It then causes the driver to be executed, thus it enables shell code to download the rest of the malware.

Interaction between VM and VMM presents a potential of the cloud attack vulnerability. Normally VMs are encapsulated and isolated in the cloud. The operating systems running inside VMs do not interact with the parent VMM. Plankers (2007) defines that the process of breaking out and interacting with the VMM is called VM escape. Once an attacker gains access to the VMM, subsequently the attacker can gain control over every other VMs running on the cloud.

“If a virtual system is compromised by an attacker and via set software system is able to totally bypass the hypervisor or virtual layer, it is quite possible to get access to the host machine and by this root privileges. For instance a vulnerability vmnat.exe was identified in VMware Workstation, which could be exploited by remote attackers to execute arbitrary commands.” (Shende, 2010)

Shende has argued that such exploitation can cause the cloud to execute arbitrary code in certain circumstances due to the weak security configurations. However, Kostya Kortchinsky (2009) developed Immunity’s Canvas commercial penetration testing tool v6.47 including Cloudburst attack module, shows it is not the case. The Cloudburst is able to exploit VMware vulnerability in VMware Workstation. This module can exploit vulnerability discovery, let attackers get access to the system and eventually corrupt its memory. The test showed that VMware 6.5.0 and 6.5.1 were affected as well as all host OS including Linux. This was achieved by allowing the guest VM to execute malicious code on the host then tunnel a connection to it.

“On a 64-bit Intel x86 architecture with virtualization extensions, there are 56 reasons for VM exits, and this forms the large attack surface which is the basis of the security threat.” (Szefer, Keller, Lee & Rexford, 2011, p.401). Each VM escape can cause VMM code to run. When the guest OS executes some operations causing escape, the VMM intervenes in order to maintain system’s abstraction. The experiment conducted by Szefer, et al (2011) illustrates that different VM escape and subsequent VMM support can be caused by different events. *“Each VM escape can be treated as a communication channel since VM implicitly or explicitly sends information to VMM. So VMM can handle the event”* (Szefer, et al, 2011, p.411). The potential danger of VM escape is to create a window of opportunity for malware VM to attack VMM, such as by exploiting how VMM handles a certain situation.

Another data security concern (Meacham & Shasha, 2012) with the cloud is that the only assurance of evidence data protection are the word of the cloud vendor, and the legal and the business incentives for the vendor not to leak or abuse information. Even if the digital forensic investigators trust the vendor is truly scrupulous and motivated to protect the evidence data, there is still the danger of malicious or sloppy individuals within the vendor’s organisation, or some sort of large-scale data breach that currently make the news with alarming frequency.

Stolfo, Salem & Keromytis (2012) point out that in 2009, a Twitter employee’s account was hacked. More than 310 of the company’s documents were stolen, some of them such as financial projections and executive meeting notes containing highly confidential information. At the same time, large numbers of users’ accounts were illegally accessed. A frightening number of accounts and services related to Twitter and its employees, such as Gmail, Google Apps, GoDaddy, MobileMe, AT&T, Amazon, Hotmail, Paypal and iTunes were either directly or indirectly affected. Even though the particular attack was launched by an outsider; however it would have been much easier if the attacker was a malicious insider.

Given the above obstacles, one can understand the main concerns of the digital forensic investigators to commit data to the cloud. The main concerns are the cloud governance and security in general, evidence data integrity and preservation in specifically.

2.5 MODERN DATA ENCRYPTION ALGORITHMS

To overcome these challenges, Hu & Klein (2009) argue that encryption on evidence data is a feasible technical solution. Using encryption to protect data is nothing new. Wang, et al (2012) state that various encryption algorithms such as, DES, 3DES, AES & RSA have existed for more than a decade. Weis & Alves-Foss (2011) believe that with substantial amount of evidence data being stored, encryption seems like the perfect security solution. In fact, it has been now commonly accepted that data encryption in the cloud environment is a good way to mitigate security concerns over evidence data integrity, preservation and confidentiality by the cloud. Indeed, with the possession of the secret key for decryption, digital forensic investigators are entitled to still get control of their evidence data regardless where the evidence data may be stored physically. Better yet, (Yang & Zhang (2011) suggest that data encryption can also help to overcome other concerns such as regulatory compliance and geographic restriction, in the sense that the encrypted data by no means useful without the decryption capability.

2.5.1 Symmetric and Asymmetric Encryptions

Common data encryption methods include symmetric and asymmetric cryptography algorithms. Symmetric encryption (Stallings, 2011, p.33) is used to conceal the contents of blocks or streams of data of any size, including messages, files, encryption keys and password. Examples of symmetric cryptography algorithms (Hwang, et al, 2011) are Triple Data Encryption Standard (3DES) which is used in the W.S. Federal Information Processing Standard's (FIPS) 46-3, and 197 Advanced Encryption Standard (AES). A typical symmetric cryptography algorithm has five ingredients:

- Plaintext: this the original intelligible message or data that is fed into the algorithm as input
- Encryption algorithm: the encryption algorithm performs various substitutions and transformations on the plaintext
- Secret key: The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will

produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key

- Decryption algorithm: this is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext

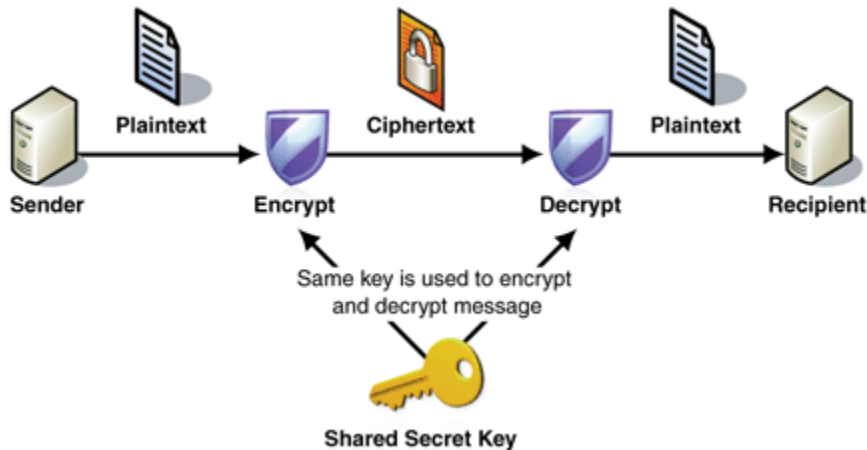


Figure 2.8: Simplified Model of Symmetric Encryption.

Source: (Microsoft, 2005)

On the other hand, asymmetric encryption is also called “public key encryption”. It has two different keys (Hwang, et al, 2011) “*public key*” and “*private key*”. The “*public key*” is used to encryption; and the “*private key*” is used to decryption. Example is such as RSA. Generally, asymmetric encryption (Stallings, 2011) is used to conceal small blocks of data, such as encryption keys and hash function values, which are used in digital signatures. A typical asymmetric cryptography algorithm has the following ingredients:

- Plaintext: this is the readable message or data that is fed into the algorithm as input
- Encryption algorithm: the encryption algorithm performs various transformations on the plaintext

- **Public and private key:** this is a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption. The exact transformations performed by the algorithm depend on the public or private key that is provided as input
- **Ciphertext:** this is the scrambled message produced as output. It depends on the plaintext and the key. For a given message, two different keys will produce two different ciphertexts
- **The Decryption algorithm:** this algorithm accepts the ciphertext and the matching key and produces the original plaintext

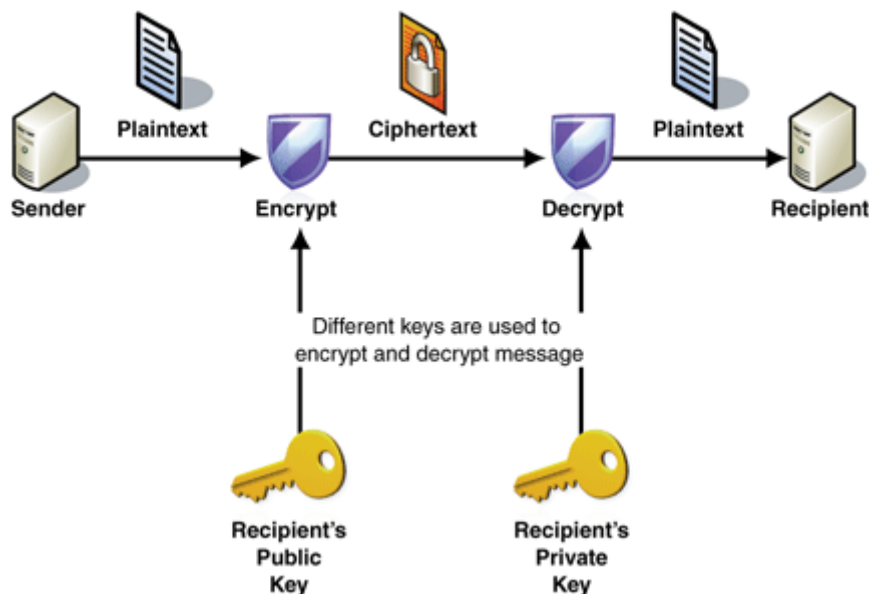


Figure 2.9: Simplified Model of Asymmetric Encryption.

Source: (Microsoft, 2005)

2.5.2 DES & 3DES

Stallings (2011) suggests that DES is the most widely used encryption scheme adopted in 1977 by the NIST, as FIPS 46. Moreover, Hwang, et al (2011) explain that the algorithm itself is referred to as the Data Encryption Algorithm (DEA). For DES, data are encrypted in 64-bit blocks using a 56-bit key. The algorithm transforms 64-bit input

in a series of steps into a 64-bit output. The same steps, with the same key, are used to reverse the encryption.

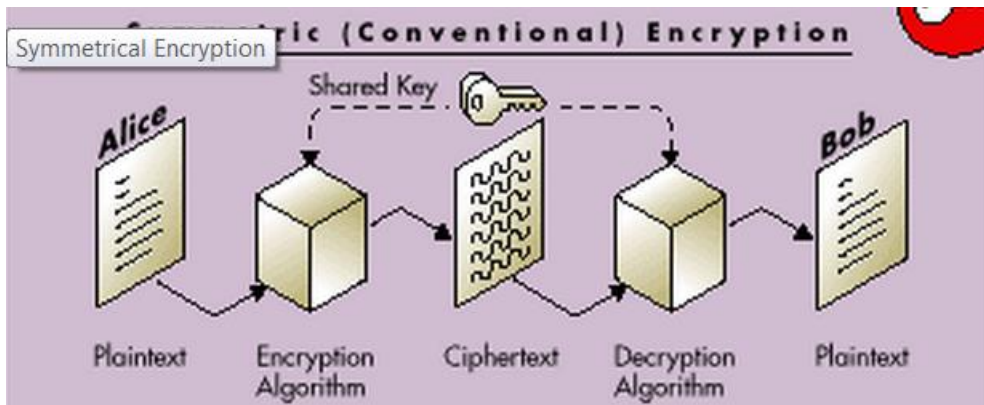


Figure 2.10: DES Encryption and Decryption Model.

Source: (Smart Card Basics, 2010)

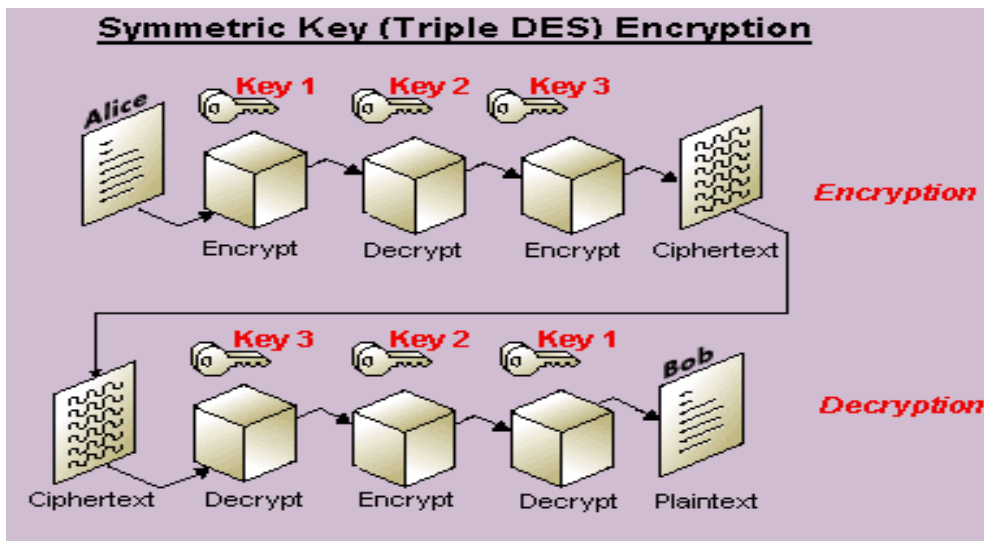


Figure 2.11: 3DES Encryption and Decryption Model.

Source: (Smart Card Basics, 2010)

Stallings (2011) stated that the original DES was generally sufficient when that algorithm was designed. However, the availability of increasing computational power, made brute-force attacks feasible. In 1988, the Electronic Frontier Foundation, using a specially developed computer called the DES Cracker, managed to break DES in less than 3 days. The cost of the machine was under US\$250,000. Additionally (Tropical

Software), it has been shown that for a cost of one million dollars, a dedicated hardware device can be built that could search all possible DES keys in about 3.5 hours.

3DES was the answer to many of the shortcomings of DES. 3DES provides a relatively simple method of increasing the key size of DES to protect against brute-force attacks, without the need to design a completely new block cipher algorithm.

2.5.3 AES

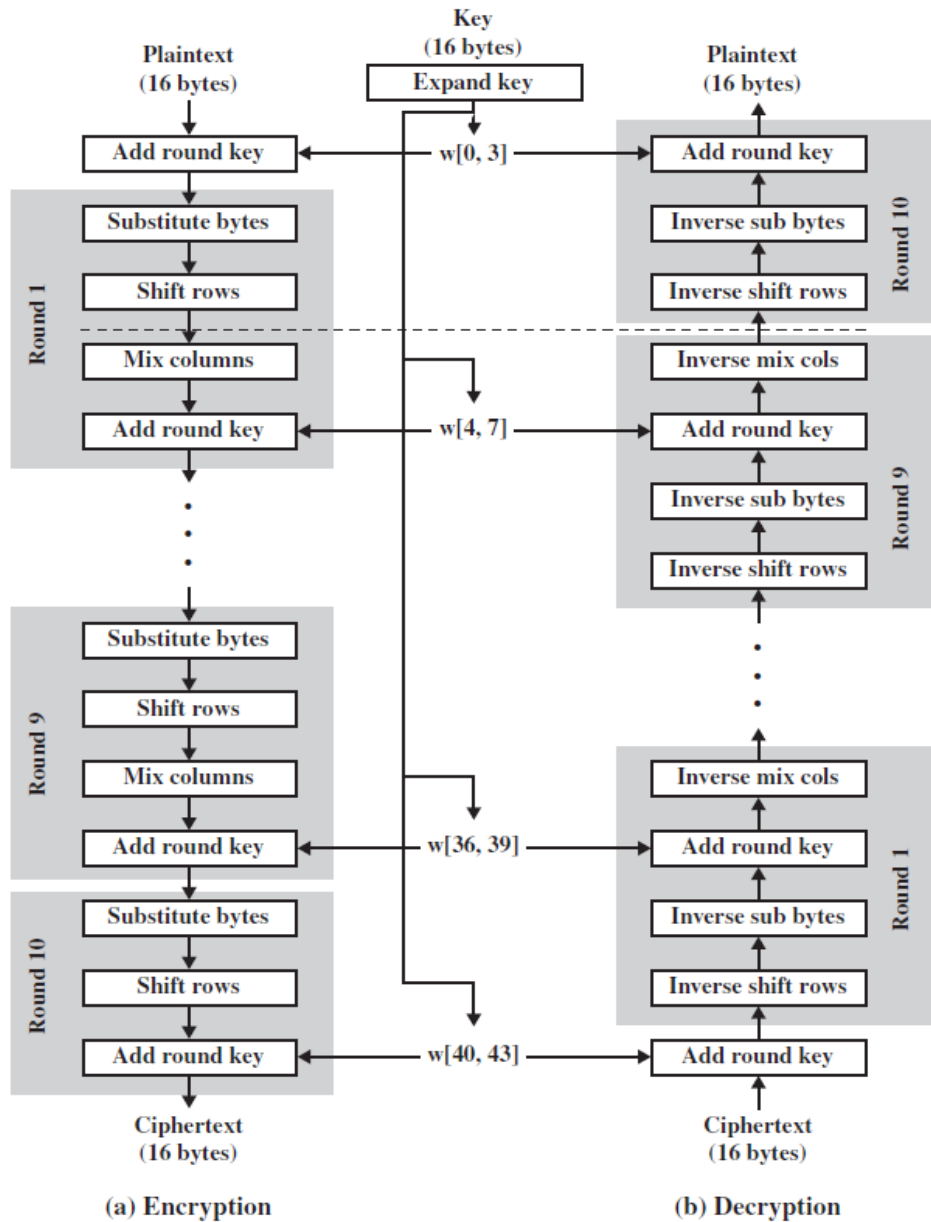


Figure 2.12: AES Encryption and Decryption Model.

Source: (Stallings, 2011, p.154)

In 2001, AES is published by NIST to replace DES. Like DES and 3DES, it is also a symmetric block cipher. AES is based on a design principle known as substitution and permutation network. It is fast in both software and hardware (Schneier, Kelsey, Whiting, Wagner, Hall, Ferguson, Kohno & Stay, 2000). The cipher takes a plaintext block size of 128 bits. The key length can be 128, 192 or 256 bits. The algorithm (Stallings, 2011; Schneier, et al, 2000) is referred to as AES-128, AES-192 or AES-256 depending on the key length.

The input to the encryption and decryption algorithms is a single 128-bit block. This block is depicted as a 4×4 square matrix of bytes. This block is copied into the state array, which is modified at each stage of encryption or decryption. After the final stage, state is copied to an output matrix.

2.5.4 Free Encryption Tools

Encryption software is software, which is specially designed for the main purpose of performing encryption and decryption functions on a particular data files on hard drives and removable media, email message or the packets sent over computer networks. File encryption is type of encryption performed on data storage medium, where individual files/directories are encrypted by encryption software. The encryption software executes a particular encryption algorithm. It aims to encrypt data in the way it cannot be recovered without decryption key. Thus, the overall data security is ensured. File encryption is an important part of today's information system security. There are many free downloadable encryption software available on the Internet. According to,

There are many free downloadable encryption software available on the Internet. According to, Ramesh Natarajan (2013), the top five best free file encryption software for windows are: GNU Privacy Guard, Truecrypt, AxCrypt, 7-zip and AESCrypt. GNU Privacy Guard, Truecrypt, AxCrypt and AESCrypt are encryption tools, whereas 7-zip is a compression tool.

2.5.4.1 GNU Privacy Guard

GNU Privacy Guard (GnuPG, 2013) is open source command-line free file encryption software developed under GNU free software project. It was initially developed by

Werner Koch, and released on 07 September 1999 for Version 1.0.0. Later, it was included as part of OpenPGP project.

GnuPG is hybrid encryption software. It uses combination of symmetric-key cryptographic algorithms for speed, as well as asymmetric-key cryptographic algorithms for ease of secure key exchange. Typically, it uses recipient's public to encrypt a session key which is used only once. It encrypts messages using asymmetric-key pairs individually generated by users. The resulting public keys may be exchanged with other users in a various ways, such as the Internet key servers. The extreme caution should be taken during key exchange process.

Table 2.2: Table of GnuPG Characteristics.

<i>Asymmetric Algorithm:</i> RSA, ElGamal, DSA
<i>Symmetric Algorithm:</i> IDEA (from version 1.4.13/2.0.20) 3DES, CAST5, Blowfish, AES-128, AES-192, AES-256, Twofish, Camellia-128, Camellia-192, Camellia-256 (from version 1.4.10/2.0.12)
<i>Hash:</i> MD5, SHA-1, RIPEMD-160, SHA-256, SHA384, SHA512, SHA-224
<i>Compression:</i> uncompressed, ZIP, ZLIB, BZIP2

In order to prevent identify spoofing by corrupting public key to “own” identity correspondence. Also, it is possible to use encrypted digital signature to a message. Thus, the integrity of message is maintained, and the sender can be verified. According to GnuPG, it supports the following algorithms listed in Table 2.2.

The first and greatest limitation is considered in GnuPG, is that GnuPg is a command-line based system. It is not written as an API, which can be incorporated into other software. Thus, it requires users to familiar with command type environment, which many users are lack these days. Hence, it is clear that because of its characteristics, it is not suitable for encrypt digital forensic investigation evidence data in the cloud environment. Therefore, for the purpose this research, the author considers that GnuPG is not used for the experiment.

2.5.4.2 TrueCrypt

TrueCrypt (TrueCrypt, 2014) is also open source encryption software. It is considered very powerful, flexible and highly effective in providing real time encryption. Real time encryption allows the encrypted data file accessible immediately after the key is provided. It seems that the entire volume is typically mounted as if it were a physical drive, which makes the file just as accessible as any unencrypted ones. TrueCrypt can create a virtual encrypted disk within a file or certain size of data storage under Microsoft Windows, OS X and Linux. In addition, Natarajan (2013) points out that it supports parallelized encryption for multi-core system and pipeline read/write operations under Microsoft Windows.

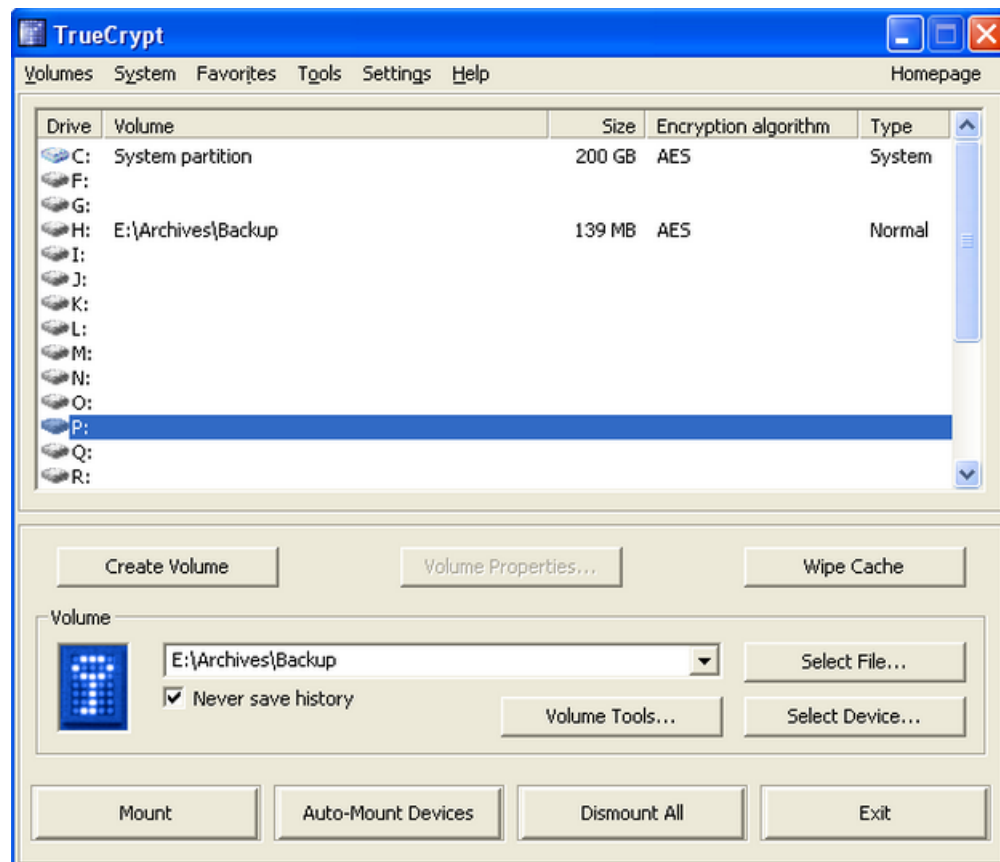


Figure 2.13: TrueCrypt GUI Main Window.

It uses “volumes” to contain the encrypted data (Gizmo's, 2013) at rest as well as when it is accessed. Each volume contains its own file system. Firstly, users mount the volume

as a file system drive that uses its own drive letter. Then, users can read, change or add to the encrypted content of the volume when it is mounted. The encryption key is required to mount the volume. Individual encryption algorithms supported by TrueCrypt are AES, Serpent and Twofish. Additionally, five different combinations of cascaded algorithms are available: AES-Twofish, AES-Twofish-Serpent, Serpent-AES, Serpent-Twofish-AES and Twofish-Serpent. The hash functions used by TrueCrypt are RIPEMD-160, SHA-512 and Whirlpool. Figure 2.13 shows TrueCrypt graphic user interface (GUI) main window.

Despite its popularity, flexibility and efficiency, there are some concerns have been sought in TrueCrypt over the years. TrueCrypt supports a concept called plausible deniability (TrueCrypt, 2014), by allowing a single “hidden volume” to be created within another volume. The concept of plausible deniability (Wikipedia, 2013) is originated from the Central Intelligence Agency (CIA) in the early 1960s to describe the withholding of information from senior officials in order to protect them from the public. In cryptography, it means that the Windows versions of TrueCrypt have the ability to create and run a hidden encrypted operating system whose existence may be denied. However, in order to maintain the data security, TrueCrypt does not change the files size and timestamp by default after they are retrieved or modified. Consequently, when the files are stored in the cloud environment, the files will not be backed up due to their non-changed file sizes and timestamps. Thus, in order to back up the files properly, the users have to manually change the timestamps. On the other hand, some cloud backup services such as DropBox, do check that hash value of the volume files. If they are changed, a new copy of the volume file will be stored.

Researchers (Halderman, Schoen, Heninger, Clarkson, Paul, Calandrino, Feldman, Appelbaum, & Felten) have found another security concern with TrueCrypt which was that it stored encryption keys in RAM. On an ordinary personal computer, the DRAM will maintain its contents for several seconds after power is cut. Thus, it will create an opportunity for attackers to recover the key.

2.5.4.3 AESCrypt

Like the aforementioned encryption software, AES Crypt is also free open source encryption tool. It uses AES-256 cryptographic algorithm to encrypt and decrypt data

files (AES Crypt, 2014), and run independently from the operating systems, on which it is installed. Similar to AxCrypt, AES Crypt is incredible simple to use. Unlike the most encryption software, it does not have program window. To encrypt or decrypt data files, users can just right click the files and select AES Crypt item, and enter the password. A new encrypted or decrypted version of the file is created. Since the original file is not purged, AES Crypt is best used for situations (Gizmo's, 2013) where users need to upload, email or otherwise move the encrypted files. However, to prevent the unencrypted version of files to be accessed by unauthorised parties, the files must be erased. Otherwise, the data security can be breached. Figure 2.14 demonstrates AESCrypt simple user options

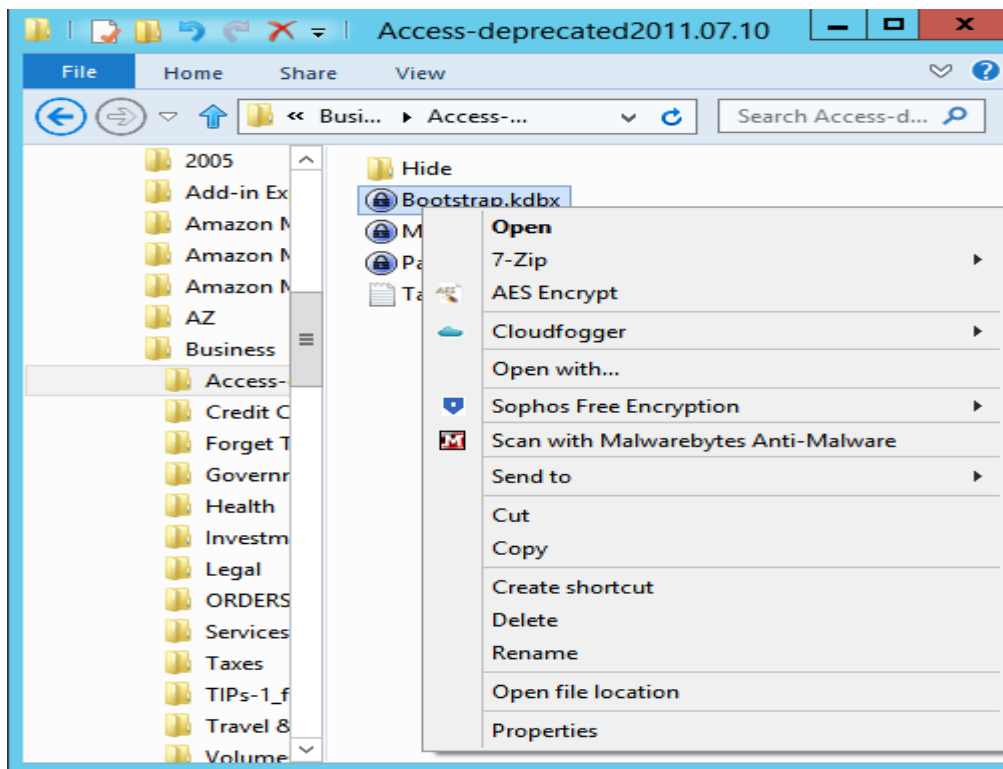


Figure 2.14: AESCrypt Simple User Options.

2.5.4.4 AxCrypt

AxCrypt is a free open source developed by Axantum Software. It uses AES-128 cryptographic algorithm (Natarajan, 2013) to encrypt and decrypt data files. It creates an archive that contains additional metadata along with the encrypted data file. The original

file is deleted after encryption. It is a very simple program. To encrypt data files, users can just right click the files and select “encrypt”. Simply double –clicking an encrypted file, users can edit or view it with the program of choice. Closing the files, they are automatically re-encrypted. Self-decrypting files are also supported, removing the need to install AxCrypt to decrypt. It is best known to support data files store on the cloud environment (Axantum, 2013), such as Dropbox, Live Mesh, SkyDrive, Box.net and more.

2.5.4.5 AESTool

AESTool (Cryptool) is excellent open source e-learning cryptographic software. It implements AES encryption algorithm. Originally, it is developed as part of Cryptool projected started in 1998 by German companies and universities. The current version of AESTool is 2.5.1. Because it uses unique features to illustrate AES cryptographic concepts; hence, it has received several awards, such as Germany Land of Ideas 2008, European Information Security Award 2004, IT Security Award NRW 2004 and TeleTrust Special Award 2004. So far, there are no documentations explicitly explain which AES algorithm that AESTool implements; yet the maximum key length only allows 64-bits hexadecimal digitals. Since, it is only an e-learning tool for education and training purpose; therefore it uses simply GUI window, and provides basic encryption and decryption functions. Figure 2.15 shows AESTool simple GUI window.

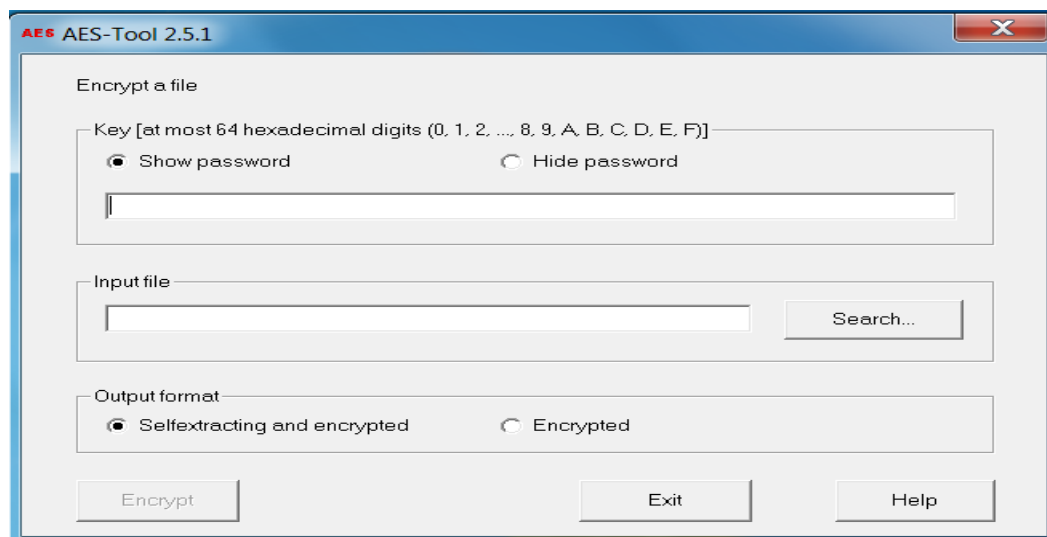


Figure 2.15: AESTool Simple GUI Window.

2.6 SUMMARY OF PROBLEMS AND ISSUES

From the literature reviewed there have been a number of issues presented that are specific in the realm of storing evidence data during digital forensic lifecycle. The apparent problems and issues discovered will be outlined in order to identify important aspects of the chosen research area where further research is needed.

The rapid growth in capacity of storage devices is increasingly challenging digital forensic investigators due to the limited time to create a forensic image of a disk, or process all of the data found. The use of the cloud environments will inevitably exacerbate the problem (Garfinkel, 2010) of data storage and analysis. One solution digital forensic investigators could rely on is the use of the cloud environment for storing evidence and performing analysis. The idea of using the cloud to host a “forensic service” used to conduct investigations has already been proposed by studies such as Ruan, et al (2011) & Taylor, et al (2010). Several issues rose and yet to be addressed include for example, the forensically sound transfer of evidence from the source of the investigation to the cloud storage, and the management of the chain of custody for evidence. Furthermore, those studies have not considered in detail the virtualised nature of clouds, which is likely to have a significant impact on forensic investigations beyond the cloud security.

Moreover, once digital forensic investigators store the evidence data in the cloud environment, the digital data are likely to be scattered in the hard drives, even in different data centres in different countries. Hence, it presents a great challenge to digital forensic investigators that how to maintain evidence data storage, extraction and analysis complying with integrity, preservation, confidentiality and court admissibility requirements during digital forensics investigation lifecycle. The following questions are essentially important to investigate before digital investigator is fully committing to the cloud environment.

- Are data encryption schemes robust enough in the cloud environment?
- With the investigator not having complete control of the storage, how can the investigator be sure that evidence is not in the process of being altered in the cloud at that moment in time?

- How to protect the privacy of innocent data during investigation?

To ensure that the cloud can be used to deliver forensic investigations, there are still many open issues to be studied, including confidentiality, privacy, integrity and auditability. Some related issues which can be studied in this research include:

- The ability to ensure the evidence is unaltered when transferred to and from as well as when stored in the cloud.
- The ability to ensure the evidence is secure from unauthorized access and the chain of custody is maintained.
- The ability to control access to the evidence stored in the cloud, and ensuring other users of the cloud do not have access to the material.

The discussed problems and issues demonstrate the need for further research to be undertaken in the field of digital forensics in storing evidence data in the cloud environment.

2.7 CONCLUSION

The literature review conducted in Chapter 2 provides an overview of the current state of knowledge and of the context of the thesis. It first established the history and concepts of the cloud computing followed by a review of comparisons of popular the cloud services, its obstacles existed in governance and security aspects. The process of digital forensics and investigation provided fundamental knowledge to then lead on to a review of the potential challenges, when digital forensic investigators store the evidence data in the cloud environment. A set of modern data encryption algorithms was examined to establish the potential of protecting evidence data in the cloud environment with them.

The problems and issues apparent in using encryption algorithms to protect evidence data in the cloud were also identified as a basis for forming research questions.

The literature review discussed, therefore, introduces specific areas where there is a definite need for further research. In particular, the security issues which have been raised and apparent misuse of the cloud environment further support the perceived need to conduct such an investigation. The current state of knowledge is also identified as crucial factors that will assist in the design perspectives and development of a feasible research methodology. It has therefore, been determined that the proposed research will focus on advancing the body of knowledge surrounding evidence data integrity in the cloud. Specifically, the research will aim to test effectiveness and the robustness of the proposed data encryption algorithms to provide further information about the feasibility of storing evidence data in the cloud.

Chapter 3 will therefore firstly undertake a review of similar studies relevant to the chosen area of research and together with the literature knowledge, the main research question and associated sub-questions will be derived. Undoubtedly, there will be limitations to the proposed project but any potential restriction will be identified early at the pre-testing stage of the project so as to negate or explain any foreseen negative impacts in the results. The justifications for a research project have been established.

Chapter 3

RESEARCH METHODOLOGY

3.0 INTRODUCTION

In Chapter 3, the main research objectives are to formulate a research question and develop an appropriate methodology establishing a framework for the proposed research. The cloud computing technology provides compelling cost effectiveness and substantial space for digital forensic data evidence storage. There are a number of issues that surround the topic of maintaining evidence data integrity and meeting court admissibility requirements. The literature reviewed shows that an investigation in the field of data encryption trails would be of value.

A number of similar studies in the chosen research field will first be sourced and fully evaluated in Section 3.1 so as to learn from the experience of other researchers working within the same area of study. In conjunction with the reading from Chapter 2, these additional facts will be pivotal to forming the research question for answering and hypothesis to be tested. Section 3.2 will outline the main research question and secondary questions with associated hypotheses based on all of the gathered information.

Section 3.3 and 3.4 concentrate on establishing a practicable research model of the proposed system architecture and the associated hardware and software requirements. The data requirements in Section 3.4 will outline the generation, collection, analysis and reporting methodologies needed to conduct the research. Finally, the expected outcomes will be named in Section 3.5 and in Section 3.6 the limitations of the research will be discussed to identify early restrictions that may apply to the project.

3.1 REVIEW OF SIMILAR STUDIES

In order to develop the methodology for this research, three research studies have been sourced and reviewed. There are a number of references to help that were identified in

Chapter 2 with regard to facilitating the storing of digital forensic evidence in the cloud environment. The following research studies have been selected for relevance and similarity to the chosen research area, methodology proposed and detailed information regarding storing digital forensic evidence data in the cloud environment.

The first study by Garfinkel (2010) who predicts that today's golden age of digital forensics is quickly coming to an end due the lack of efficient compatible data analysis software and decryption tools, limited storage for evidence data processing and storing and the inadequate training. He also examines current forensic research directions and argues that to move forward the international digital forensic community needs to adopt standardized, modular approaches for data representation and forensic processing. The second study by Mahamood (2011) outlines security and confidentiality issues in relate to the cloud users' data in terms of its location, relocation, availability and security. Further, he evaluates several methods to improve data security and confidentiality in the cloud. The third study by Mohamed, et al. (2012) evaluates eight selected modern encryption algorithms on both desktop computers and the Amazon EC2 Micro Instance cloud computing environment to maintain data security. This evaluation was preformed according to randomness tests by using NIST statistical testing in the cloud environment.

3.1.1 Storing Forensic Investigation Evidence Data in the Cloud

In his article, Garfinkel (2010) points out that one of major challenges that today's digital forensic investigators are facing is growing concern of limited storage for relatively massive evidence data processing and storing. He argues that because of "The growing size of storage devices means that there is frequently insufficient time to create a forensic image of a subject device, or to process all of the data once it is found." Moreover, the vast size of today's storage devices means that time-honoured and court-approved techniques for conducting investigations are becoming slower and more expensive. For example, a 2TB hard drive can be purchased for \$120 but takes more than 7 hours to image. Not to mention that, the cloud users can easily rent large data storage at a very cheap cost. Consequently, systems and individuals of interest can have more storage than the police crime lab responsible for performing digital investigation forensic analysis.

Yet, on the other hand, digital forensic investigators could also enjoy the benefits of the cloud computing such as elastic, large data storage and pay-as-you-need. Perhaps, the digital forensic investigator can utilise the cloud as a perfect potential medium for storing and processing digital forensic investigation evidence data. Thus, it allows digital forensic investigators have sufficient storage for storing and processing evidence data as much as needed, and as long as it is required in cost-effectively manner.

3.1.2 The Cloud Security and Privacy Issues

Mahamood (2011) argues that the cloud offers a benefit of a high degree of data mobility, which allows the users to access their data with much freedom without being restricted by the locations. Yet, as a double-edged sword, it also has certain disadvantages. For example, when an enterprise has some sensitive data that is kept on a storage device in the cloud, they may want to know where it is being stored. Moreover, they may even wish to specify a preferred location, for example data to be kept in New Zealand. Thus, it requires a contractual agreement between the cloud vendor and the users that data should be stay in a particular location or reside on a given known server. The problem is that consumers are, sometimes, not aware of the implication of this and thus no such contract is agreed beforehand. Even though, the cloud vendor should take responsibility to ensure the security of system and provide robust authentication to safeguard the users' data; the users are ultimately responsible for the security and integrity of their own data (Kandukuri, et al, 2009).

Another issue is the data relocation. Initially, data is stored at an appropriate location decided by the cloud vendor. However, it is often moved from one place to another affected by the bandwidth efficiencies, cost provision and high capacity of the Internet access. Yet, the users do not always know the exact location where their data is stored. Most of time, it is not a problem to the average user. On the other hand, digital forensic investigators need to take extra precautions regarding to the data relocation, since it may cause more potential risk for the evidence.

In addition, cross border data distribution can also happen for the same reasons. This can lead to additional legal risks due to different countries having varying policies, regulations and legislation. The implication is that data protected by legislation in one country may not have the same, or even similar, protection in another country. For

example, the European Union and the United States of America have different privacy policies (Jaeger, Crimes, Lin, & Simmons, 2008, p.12). Their data protection laws are based on the assumption that the location and responsibility of data is known and understood. Law enforcement agencies in the United States of America have regulatory power to demand access to any data stored on any computer within the USA under USA Patriot Act 2001, the Foreign Intelligence Surveillance Act (FISA amendments act, 2008), the Electronic Communications Privacy Act 1986, the Privacy Act 1974 and the Homeland Security Act 2002.

Data availability is another challenge that the digital forensic investigator is facing while storing and processing evidence data in the cloud environment. Normally, the users' data is stored in chunks on different servers often residing on different locations or in different clouds. In this case, data availability becomes a major legitimate issue as the availability of interruptible and seamless provision becomes relatively difficult. Such issue can be exemplified by the outages suffered by Google's Gmail service in February, March and May 2009 (BBC News, 2009). In the subsequent service agreement for its Premier Apps range of products which also covers Gmail, Google promised that customer data availability will be least 99.9% of the time in any calendar month at the time (Google, 2009).

As noted in Section 2.4.2.2, data security risks and related issues are already big (Chen & Zhao, 2012; Jaeger., et al., 2008; Popović & Hocenski, 2010). When data mobility is at a high level then the risks and issues increase many folds, especially when data is transferred amongst different countries with different regulatory framework. High levels of data relocation have a negative implication for data security and data protection as well as data availability. The essential question with reference to security of evidence data residing in the cloud is: how to ensure security of data that is at risk. Mahamood (2012), points out that although the users know the location of data and there in no data mobility, there still are questions relating to its security and confidentiality of it. The obvious answer suggests that data should be encrypted.

He further argues that unfortunately data encryption is not always possible. For example, if data in the cloud is being processed by a SaaS or PaaS application, such as Salesforce.com or Google Apps, then encryption may not be suitable as this may prevent

indexing or searching of data. If this happens then availability and access of data will become problematic. Thus, he suggests that new methodologies should be developed, and more work needs to be done.

3.1.3 Modern Encryption Techniques Used to Enhance Data Security in the Cloud

Mohamed et al. (2012), point out that there are three types of data in the cloud. The first one is data in transit – data being transmitted. The second one is data at rest – storage data. Finally, the last one is data in processing – processing data. Hence, they raised two fundamental questions regarding data security, which are where the data is and who has access. According to the researchers, the most cloud vendors use three types of encryption algorithms to maintain the data security, which are listed in Table 3.1.

Table 3.1 Common Data Encryption Algorithms Used in the Cloud.

Storage	Processing	Transmission
<i>Symmetric encryption</i>	<i>Holomorphic encryption</i>	<i>Secret socket layer (SSL) encryption</i>
AES, DES, 3DES, Blowfish, ...	RSA, ElGamal, ...	SSL1.0, SSL3.0, SSL, 3.1, SSL 3.2, ...

Mohamed, et al. (2012) further propose three-layer system structure model, in which each layer performs its own duty to ensure the data security in the cloud. The first layer is responsible for user authentication. The second layer is responsible for the users' data encryption, and protects the privacy of users through a certain way by using one symmetric encryption algorithms. Additionally, it allows protection from the users. The third layer is used for fast recovery of the users' data, which depends on the speed of decryption algorithms. The design structure model is shown in the Figure 3.1.

To evaluate how well modern encryption algorithms can enhance data security in the cloud environment, the researchers (Mohamed, et al., 2012) conducted randomness NIST statistical testing (listed in Table 3.2) using eight selected modern encryption algorithms (RC4, RC6, AES, DES, 3DES, MARS, Two-Fish and Blowfish) on both desktop computers and Amazon EC2 Micro Instance cloud computing environment.

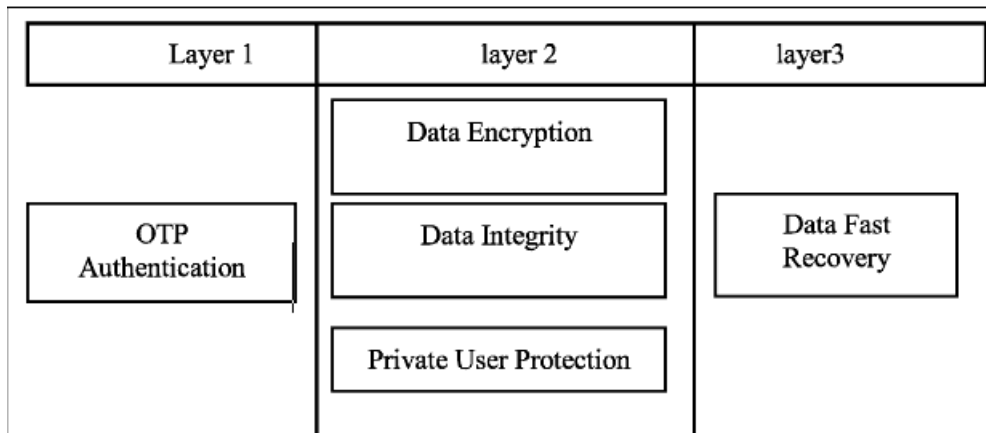


Figure 3.1: Proposed Data Security Model in the Cloud.

To do the experiments, the researchers developed the program that implements the methodology in Java language. They then launched the program on Amazon EC2 windows Micro Instance to generate 128 plain stream sequences as PRNG, each sequence is 7,929,856 bits in length and key stream of 128 bits. The researchers then applied encryption algorithms to get cipher text, which produced 128 sequences for each eight encryption algorithm. Finally, they connected to Amazon EC2 Ubuntu Linux Micro instance, run NIST statistical tests for each sequence to eight encryption algorithms. Micro instance of this Amazon EC2 family can provide a small amount of consistent CPU resources and allow burst CPU capacity when additional cycles are available. They are well suited for lower throughput applications and web sites that consume significant compute cycles periodically. The similar tests were also conducted on a desktop. The procedure was followed as in the cloud except that all the work was run in a traditional desktop.

The results showed no strong indications of statistical weakness for eight modern encryption algorithms in both environments. Yet, some differences existed between algorithms. In Amazon EC2, the evaluation of RC6, AES, DES and Blowfish were slightly better than other encryption algorithms. Overall, AES is a suitable algorithm for the Amazon EC2 environment; but Blowfish and DES are more suitable when the users focus is on the time use of the encryption method.

Table 3.2: NIST Statistical Tests.

Number	Statistical Test	User Input Parameter
1	Approximate Entropy	M = 10
2	Block Frequency	M = 128
3	Cusum-Forward	None
4	Cusum-Reverse	None
5	Spectral DFT	None
6	Frequency	None
7	Linear Complexity	M = 500
8	Long Runs of Ones	None
9	Non-overlapping Templates	M = 9, B = 000000001
10	Overlapping Templates	M = 9
11	Random Excursions	X = +1
12	Random Excursion Variant	X = -1
13	Rank	None
14	Runs	None
15	Serial	M = 16
16	Universal	None

Based on the experiments, it was concluded that when the users take precedence of performance of the algorithm over data security, the best choice of algorithms are Blowfish, DES or AES, since they take the least time to encrypt data than others and ensure that data retrieve faster. On the other hand, when the users take precedence of data security over performance of the algorithm, the best choice of algorithm is AES. Therefore, AES is the best encryption algorithm to ensure the high data security with fast performance in Amazon EC2.

3.2 THE RESEARCH QUESTIONS AND HYPOTHESES

The literature review (Chapter 2) has provided a foundation of written knowledge regarding the chosen research area of using modern symmetric encryption algorithms to enhance security and preserve privacy for digital forensic investigation evidence data stored in the cloud. A vast diversity of literature has been covered ranging from the cloud technology to modern encryption algorithms including the cloud characteristics,

data governance, distribution, relocation, and security and privacy concerns. The process of digital forensics was then examined and specific literature reviewed regarding digital forensics lifecycle. Finally, the various modern encryption algorithms theoretical designs were discussed. Additionally, the proceeding review of similar research studies (Section 3.1) has given a varying background into the use of modern encryption algorithms to enhance security for digital forensic investigation evidence data stored in the cloud. Specifically, the studies also provided an insight of the implementation of such ideas in the cloud. All of these studies have provided further information into the realm of preserving digital forensic investigation evidence data confidentiality, availability and court admissibility in the cloud.

The development of a research question was constructed based on the literature reviewed in Chapter 2, and the review of similar research studies in Section 3.1. The literature shows that the use of modern encryption algorithms is a potential mechanism to enhance security and preserve privacy for digital forensic investigation evidence stored in the cloud to meet court admissible requirements. However, there are still a number of issues that surround the topic of using modern encryption algorithms to maintain evidence data security and preserve its privacy during digital forensic investigation lifecycles to meet court admissibility requirements, once it is stored in the cloud. These issues are that the ability to ensure the evidence data is unaltered when transferred to and from as well as when stored in the cloud. The ability to ensure the evidence data is secure from unauthorized access and maintains the chain of custody. Finally, the ability to control access to the evidence stored in the cloud, and to ensure other users of the cloud do not have access to this material.

Table 3.3: Main Research Question and Associated Hypothesis.

Main Question: Can modern encryption algorithms be used to preserve evidence data privacy during digital forensic investigation lifecycle to meet court admissibility requirements, once it is stored in the cloud?
Asserted Main Hypothesis: That a system designed to apply modern encryption algorithms can maintain and preserve privacy on the evidence data to meet forensic investigation principles, when the data is stored in the cloud.

Table 3.3 displays the main research question and the associated hypothesis which has been developed from the information discussed thus far.

Furthermore, a number of related secondary questions have also been developed. The secondary questions have been devised in order to set out and answer various linked components of the main research question and are set out in Table 3.4.

Table 3.4: Secondary Research Questions.

<i>Secondary Question 1:</i> Can modern encryption algorithms provide reliability to retain data integrity in the cloud?
<i>Secondary Question 2:</i> With the investigators not having complete control of the storage, how can the investigator be sure that evidence data is not in the process of being altered in the cloud at that moment in time?
<i>Secondary Question 3:</i> How can the privacy of innocent data be protected during investigation?

Hypotheses have also been developed for each of the secondary questions which have been proposed. Because of the difficulty in composing a succinct hypothesis for each secondary question, a brief synopsis has been given to articulate the reasoning behind each of the informed hypotheses. Table 3.5 displays the hypotheses for each of the secondary research questions presented in Table 3.4.

Table 3.5: Secondary Research Questions Associated Hypotheses.

<p>Hypothesis 1:</p> <p>Modern encryption algorithms have been approved its reliability in retaining data integrity in single computer environment as well as centralised and distributed computer network systems. Thus, they are also robust enough in the cloud environment.</p>
<p>Hypothesis 2:</p> <p>Each time when digital forensic investigators storing and retrieving evidence data store in the cloud, the encryption software can update the most recent timestamp and</p>

hash function checksum assigned uniquely to each evidence data file after being accessed. The investigators can use these parameters to check against the last updates to ensure evidence data is not in the process of being altered in the cloud at that moment in time.

Hypothesis 3:

Modern encryption algorithms have been approved to be very effective and efficient to maintain high level data security. Therefore, they can also be used to protect the privacy of innocent data during investigation.

In order to attempt to answer the proposed research questions, validate the asserted hypotheses and conduct research testing in an organised manner a data map was developed. Figure 3.4 presents the research data map outlining the main research question, secondary research questions and the links to the associated research testing phases. Additionally, each testing phase is also linked to the associated point of data collection achieved from testing. Finally, the findings gathered from the research testing phases and related data collected will be used in determining the asserted hypotheses.

3.3 THE RESEARCH MODEL

The research design will define the approach that has been selected for this research. The aim of this research is to *investigate whether or not modern encryption algorithms are reliable to maintain a high level security and preserve privacy for digital forensic investigation evidence data stored in the cloud*. A theoretical research model is proposed using a design science approach in order to establish a framework for the research to be conducted. A descriptive methodology (Kothari, 2004, p.3) will be used to conduct fact-finding enquiries to establish the state of affairs in the proposed research area. From this the system architecture and the components needed to construct the system design will be derived.

A design science approach will be adapted to from the system design. Simon (1981) describes design science as a statement of “how things ought to be” and a “theory for design and action” (pp.132-133). Design theory gives explicit prescriptions (guidelines or principles) for constructing an artefact (Gregor, 2002, p.14). Design

science lies in acquired knowledge that can be used to design artefacts (in this case, to investigate the robustness of modern encryption algorithms used to preserve and maintain a high level security and privacy for digital forensic investigation evidence data stored in the cloud) and a prescription for a generic class of a problem (Van Aken, 2004). The intention of the research is to *use modern encryption algorithms to enhance security and privacy of digital forensic investigation evidence data stored in the cloud*. The goal is to *attempt to encrypted the digital forensic investigaiton evidence date using modern encryption algorithms before stored in the cloud to preserve its privacy, confidentiality and security to meet digital forensic investigation principles and practices*. It is proposed that three popular free opensource mordern encryption software (TrueCrypt, AxCrypt and AESCrypt) be installed and reviewed to determine the capabilities of the model and its ability to provide high level security and privacy for digital forensic investigation evidence data stored in the cloud. The installed software will encrypt acquired and extracted digital forensic investigation evidence data before it is stored in the cloud. The software will then decrypt the evidence data after digital forensic investigator retrieves it from the cloud before conducting analysis. Thus, it will maintain the preservation of evidence.

A descriptive methodology entails outlining the system design relating to the architecture and components needed implement it into a practical system. The software and hardware components and associated configurations will also be described and discussed in order present a proposal for the intended system.

3.3.1 Research Phases

The proposed theoretical research model described consists of four phases illustrated in Figure 3.2

Initial testing will be conducted on the proposed system which may necessitate the system to be modified several times in response to learning. Outcomes from initial testing will also allow the author to discover how the each software encrypts and decrypts different types of data files, existing features, advantages and disadvantages.

Initial testing will involve two phases. Phase One involves testing and evaluating of the encryption software in a desktop environment. Understanding the features of encryption software is crucial to the research. The features such as password generating

and storing, file timestamp update and hash function checksum, are the essential factors to ensure the research will meet the estimated outcomes. To properly evaluate the encryption software, firstly the data files will be encrypted and decrypted individually so that will mirror a real world case as closely as possible as well as providing a known baseline for analysis. Part of Phase One will be to follow proper acquisition procedures to ensure that handling of the device does not impact the results of the evaluation. Secondly, the entire sample files will be encrypted and decrypted using the same software to evaluate its performances. Individual software will be evaluated against the known data on the device to compare their strengths and weakness.

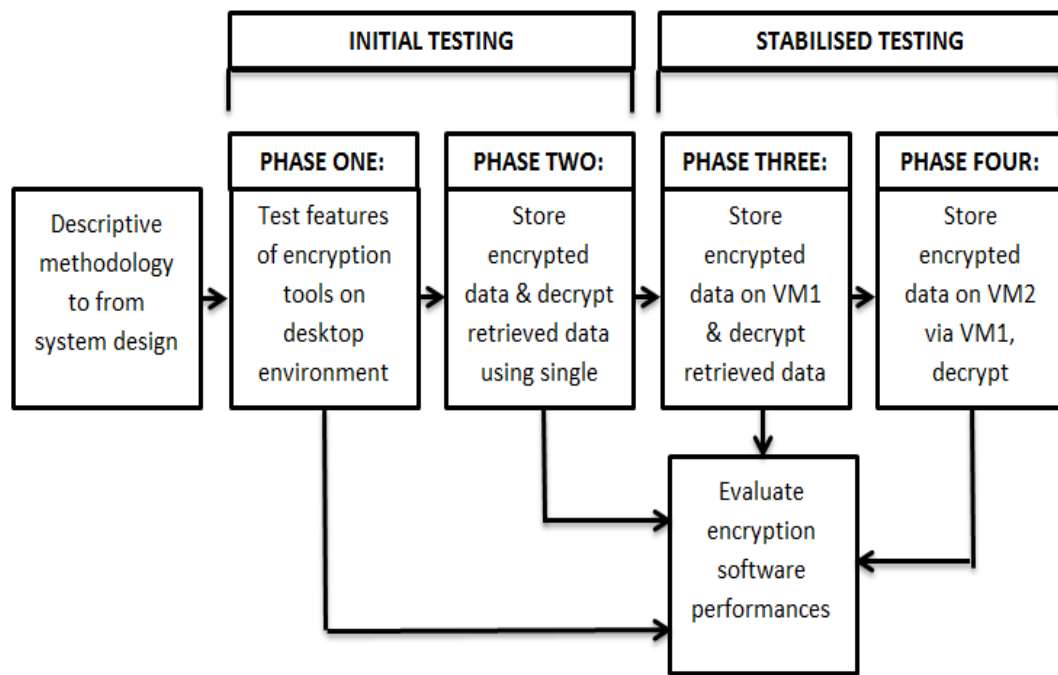


Figure 3.2: Theoretical Research Model.

Initial testing will involve two phases. Phase One involves testing and evaluating of the encryption software in a desktop environment. Understanding the features of encryption software is crucial to the research. The features such as password generating and storing, file timestamp update and hash function checksum, are the essential factors to ensure the research will meet the estimated outcomes. To properly evaluate the encryption

software, firstly the data files will be encrypted and decrypted individually so that will mirror a real world case as closely as possible as well as providing a known baseline for analysis. Part of Phase One will be to follow proper acquisition procedures to ensure that handling of the device does not impact the results of the evaluation. Secondly, the entire sample files will be encrypted and decrypted using the same software to evaluate its performances. Individual software will be evaluated against the known data on the device to compare their strengths and weakness.

Phase Two of initial testing requires Phase One to be complete. It involves the testing and evaluating of the encryption software in single virtual machine environment. All sample data files will be encrypted by each of the selected encryption tools and stored into one virtual machine. Later, they will be retrieved from the same virtual machine, and decrypted using same encryption software. Thus, all the selected encryption software will be tested and evaluated in a single virtual machine environment.

After the proposed system design is stabilised, further testing will conducted to review the ability of modern encryption software in maintaining high level security and privacy of digital forensic investigation evidence data stored in the cloud. The ultimate goal is to investigate whether or not the modern encryption algorithms will be robust enough to provide a high level of security for the evidence data in the cloud to meet digital forensic investigation compliance requirements. Therefore, the testing at the end of the initial stage is not the limit of the research. The tests are to inform different solutions to any identified problem areas encountered thus far.

Stabilised testing also involves two phases. Phase Three involves encrypting all sample data files using each of the selected encryption tools on desktop and stored into one virtual machine. Later, they will be retrieved from the other virtual machine, and decrypted using same encryption software. This test emulates the scenario where data is stored, distributed, relocated and attacked in the cloud. This Phase will evaluate whether or not the security and privacy of data will be still preserved in the cloud.

Phase Four of testing will involve encrypting all sample data files using each of the chosen encryption tools and stored on VM1. Later, they will be copied to VM2 from VM1. Then the sample files will be retrieved and decrypted after being copied back

from VM2 to VM1 (VM1 → VM2 → VM1). Thus, the robustness and performances of the modern encryption algorithms will be evaluated against the cloud environment.

3.3.2 Research Design Architecture

The proposed research architecture will closely follow previous theoretical and practical solution discussed in the selected similar studies (Section 3.1). In order to answer the main research question, it requires modern encryption tools to be installed and cloud simulation needs to be setup. Figure 3.3 displays the proposed research architecture design.

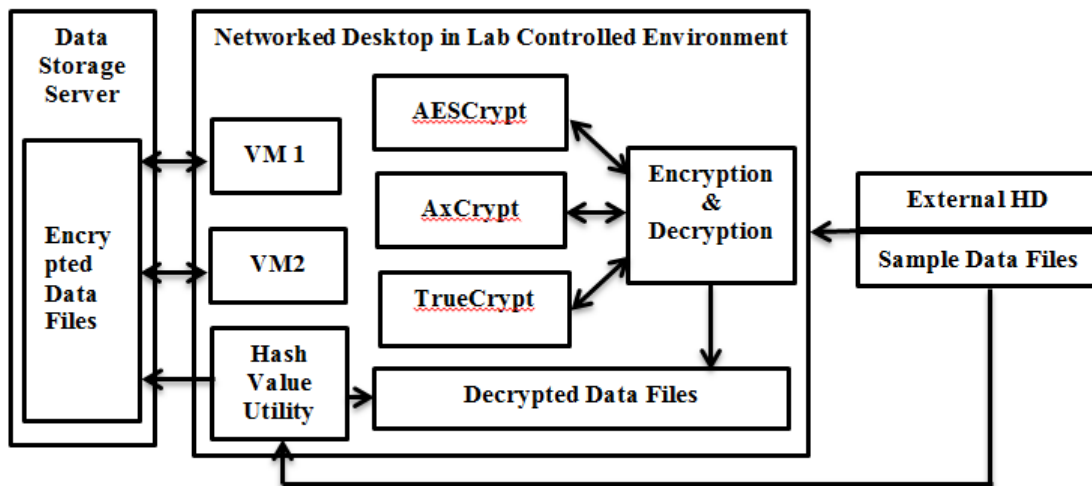


Figure 3.3: The Proposed Research Architecture Design.

From the above figure, the sample files are saved on a clean external hard drive (HD). It represents digital forensic investigation evidence data imaged to external data storage. The external hard drive is then attached to a networked desktop in lab controlled environment. Three selected encryption tools (AESCrypt, AxCrypt and TrueCrypt) which are also installed on the same desktop. Furthermore, a hash value utility (MD5 & SHA Checksum Utility) is installed on the desktop. The utility will calculate a hash value checksum for the every original sample data file, encrypted data file as well as the decrypted data files, in order to verify the integrity of data files. In additional, two virtual machines (VM1 & VM2) are setup on the desktop, which are transferring data between the desktop and data storage server. This simulates the cloud environment.

Firstly, the original sample data file is uploaded to the desktop from the external hard drive. The hash value utility calculates MD5 and SHA-1 hash values for each file. The encryption tools then encrypt the data files. Again, the hash value utility is used to calculate hash values for each encrypted data files. The encrypted files are stored on data storage server via VM1. Later, the encrypted files are retrieved from the data storage server through same virtual machine to the desktop. The hash value utility is used to calculate hash values for the retrieved data files. Then the selected encryption tools decrypt the files. The recovered data files are loaded to the desktop. Finally, the hash value utility is used to calculate hash values for the recovered data files. If either hash values of the original sample data files are same as the hash values of the recovered data files, or the hash values of the encrypted data files are same as the hash values of retrieved data files; the researcher then can say the sample data files have not been altered. Otherwise, the researcher can say the sample data files have been altered.

3.3.3 Research Components

The research testing will involve two main components, namely software components and hardware components. As discussed in Section 3.3.2, the software components include sample data files, three encryption tools, hash value utility and two virtual machines. The sample data files consists of 35 various file types representing data acquired and extracted during a single digital forensic investigation. These data files include 3 Encase files, 5 Microsoft Excel files, 11 JPEG image files, 5 PDF files, 5 Text Document files, 5 Microsoft Word Document files and 1 JPG carved file.

The three encryption tools tested in the proposed research are AESCrypt, AxCrypt and TrueCrypt (as reviewed in Chapter 2). The hash value utility used in this research is MD5 & SHA Checksum Utility. It is a small freeware utility which has the simple function of generating hash values. Thus, it allows users to verify the integrity of a file by calculating its MD5, SHA-1, SHA-256 and SHA-512 signatures, as the name implies. It provides comprehensive features which are compatible to Windows 7 operating system both 32 bits and 64 bits.

Finally, the two virtual machines installed are created using VMware Workstation 9 (VMware, 2014). It enables users to set up multiple virtual machines and use them simultaneously along with the actual machine. Each virtual machine can execute its own

operating system, such as Microsoft Windows, Linux and Unix. As such, VMware Workstation 9 allows one physical machine to run multiple operating systems simultaneously.

As illustrated in Figure 3.3, the hardware component for the experiment include external hard drive and networked desktop in lab controlled environment. The external hard drive is HDPC-CU manufactured by I-O Data. It is a standard portable external hard drive, supports Windows 7, both 32 bits and 64 bits operating systems using USB2.0 as interface. The desktop uses Windows 7 Professional Edition 32 bits and 64 bits operating systems.

3.4 DATA REQUIREMENTS

During the proposed testing phases there are a number of requirements for different aspects of data handling. It has been established that three free open source encryption software and two virtual machines will be installed in a laboratory testing environment. The clean external hard drive contains sample data files will be added to the testing environment. To evaluate the robustness and performance of modern encryption algorithms, various tests will be conducted where data is actively generated in the testing environment. The data that is collected will then be analysed and the results reported in Chapter 4.

The data requirements that need to be addressed in the research testing phases fall into five main categories: generation, collection, processing, analysis and presentation. Each of five data requirement categories will be discussed to ensure viable data is generated, distributed, reported and analysed correctly.

3.4.1 Data Generation

The process of data generation is an important aspect in the proposed research testing. In order to evaluate the robustness and performances of modern encryption algorithms used to maintain data security and privacy in the cloud, data must be generated using correct methods so as to provide accurate results. All four phases of research testing require data generation to evaluate the encryption algorithms in the simulation of the cloud environment.

There are several sources of data that are required for the proposed research including control data, encrypted data, recovered data and the documented journal on the investigation. Control data is the sample evidence that is generated based on the fictitious scenarios, where are to portray as closely as possible a real world event. The control data is to be recorded into a table as the known or expected facts and will later be used as a comparative baseline for the data collected during the experiment to verify if the encrypted files are altered or access by unauthorised person.

The second and third requirements for data are the encrypted and recovered data. Before the decryption, the data is to be retrieved from the cloud simulation environment where the scenario is performed. Once all the required data are gathered, a comparative analysis with the control data will be conducted with the aim of answering the sub-questions and ultimately the main research question. The step by step investigation processes conducted on the experimental case scenarios will also be recorded in journal form to ensure that the steps are repeatable.

3.4.2 Data Collection

The process and methods of data collection is an exceptionally crucial part of the data requirements. That data that is generated by the previously described methods (see Section 3.4.1) is subsequently collected in various log files.

The first data to be collected are the controlled data from Phase One. These data include Directory Name, File Name, Date Modified, Data Type, File Size, MD5 and SHA-1, SHA-256 and SHA-512 which will be served as baseline data to compare the results generated from the later research. The pre-test results can be collected from the directory window and MD5 & SHA Checksum Utility.

The second data to be collected after the data files are encrypted using three encryption software (TrueCrypt, AESCrypt and AxCrypt), are Directory Name (if can be encrypted), File Name, Date Modified, Data Type, File Size, MD5 and SHA-1, SHA-256, SHA-512, Drive Name from where the files and directory selected, Encryption Software, Encryption Algorithm, Timestamp, Passwords generated for encryption.

The encrypted files and directory will be stored on a virtual machine in the simulation of the cloud environment. Thus, data types collected from this phase are similar to pre-test data types. Later, the files and directory will be relocated and retrieved from another

virtual machine. Eventually, they will be decrypted on desktop to see whether or not the encryption algorithms will be robust enough to preserve sample files integrity, security and privacy. This pre-test data will be able to ascertain which encryption software and file type can or cannot be resist data relocation and distribution in the cloud.

Recovered data is collected after being decrypted using the same encryption software. Decrypted data can be used to determine what happened, when it happened, how it happened and why it happened. In order to collect the recovered data, case scenario activities depicted in Section 3.3.1 will be simulated on the experimental machine in the lab environment. During this process, the simulated activities on the experimental machine will be recorded. The variables that will be collected during this collection process are essentially same as encrypted data. All the information will be recorded in table form.

Each step of the research and which tools are used will be reported in journal format. The information documented in the journal is vital, as it records all the procedures undertaken in the research. This is to ensure that the procedures are repeatable and are able to reproduce similar results as well as to recommend an effective method for similar environments.

3.4.3 Data Processing

As aforementioned in Section 3.4.1, there will be four types of data that are needed to be collected all together: control data, encrypted data and recovered data. All the collected data will be processed in a tabular form by using an Excel spreadsheet. This is to ensure that the collected data can be evaluated in an effective and concise way.

Control data is processed in a lab environment using one computer freshly installed with the Windows 7 (Professional Edition) operating system. Also, two virtual machines will be created on the same computer, where one machine is used to store the sample files; the other one is used to retrieve the sample files. Thus, it creates a simulation environment to represent data relocation and distribution in the cloud. All the files and directory retrieved and decrypted will be saved on the desktop without changing the names. Each activity, all sample files created and tools used in the scenario will be recorded. Subsequently, these control data will be used for comparative analysis with the decrypted data.

Digital evidence is fragile: *“it can be altered, damaged, or destroyed easily by improper handling or examination”* (National Institute of Justice, 2004, p.11). To preserve and ensure the integrity of the evidence data, all sample files are processed with hash values before encryption and after decryption. When both values match, it is assumed that nothing has been altered while the data files are stored in the cloud simulation. Thus, it confirms the reliability of evaluated encryption tools. In addition, all sample files are assigned with a timestamp whenever it is accessed. When the sample files recovered from decryption, if the two timestamps are the same, it is assumed that no unauthorised access has occurred while the data files are stored in the cloud simulation. Thus, it confirms the evaluated encryption tools preserve the sample file data integrity.

The journal documenting events during the research is an important set of data that can be used to recommend the best practices for investigation procedures for encrypt evidence data stored in the cloud. The documented steps of the research in the journal will be transferred into a simple and comprehensive flow chart diagram for easy interpretation.

3.4.4 Data Analysis

The data analysis of this proposed research is divided into three parts. First is the analysis of the pre-test results conducted in Phase One. This is to analyse the selected free open source encryption tools’ capability and features that provide data security and privacy on various common digital forensic investigation data file formats such as Encase, Microsoft Excel, JPEG, PDF, Text Document, Microsoft Word Document and JPG. The second part of data analysis is the sample evidence data encrypted, retrieved and decrypted in the cloud simulation as mentioned in Section 3.3.1. Thirdly, a comparative analysis will be performed on the findings from the decrypted data and the control data.

The pre-test results analysis is based on the results produced by the encryption and decryption performed on the sample evidence files at a lab control desktop environment. From the test results collected, the three encryption tools are compared in terms of the features that provide encryption and decryption functions, the formats that can be encrypted, and whether or not the encryption algorithms can maintain a high level of security and preserve privacy of the sample files. Therefore, from analysis of the pre-

test results, encryption software features and sample data file formats, which can be encrypted and decrypted, are tested and verified.

The second part of the analysis is to analyse data generated from the sample evidence data being encrypted, retrieved and decrypted in the cloud simulation in Phase Two, Three and Four of the experiment. This part of analysis is to evaluate whether or not the selected encryption software are robust enough to resist data relocation and distribution; and subsequently maintains a high level security and preserves privacy of sample evidence files stored in the cloud simulation, respectively. This part of analysis consists of “timestamp analysis, file size analysis, encryption algorithms analysis and hash value analysis. The results from these selected analyses will be able to help digital forensic investigators determine the integrity and confidentiality of the sample files.

The third part of the analysis is a comparative analysis between the control data and the recovered data. The objective of this analysis is to determine whether the use of selected encryption tools are efficient to provide high level security and privacy for the sample evidence stored in the cloud simulation. If the results show positive outcomes that data privacy and security can be enhanced by using the selected encryption tools, then it will ultimately answer the asserted main research hypothesis: *“That a system designed to apply modern encryption algorithms can maintain and preserve high level security and privacy on the evidence data to meet forensic investigation principles, when the data is stored in the cloud.”*

3.4.5 Data Presentations

The data analysis will provide the most value if the results are presented in an appropriate and effective manner. The test data collected in Phase One of the experiment will be presented in a tabular form listing of Encryption software, Encryption/Decryption Algorithms, File Name, Date modified, Data Type, File Size, and Hash Values before and after being encrypted and decrypted. Finally the successful encryption/decryption product will be indicated with a year or not. Remarks will also be recorded if there is any additional relevant information from the observation.

Encrypted and recovered data will be presented mostly in table form generated by encryption and decryption functions performed on the sample data files. As mentioned earlier, control data is also called the known or expected data. Therefore during the

process of encrypting → storing → retrieving → decrypting analysis in the cloud simulation, if the expected data are recovered by the encryption software, then the relevant data will be exported into a table in Excel. These data will be collected until the end of the experiment. If expected files are found, then they will be recorded into the comparative analysis table as found, or partly found, and how they were found. Steps taken along the process will also be recorded as a journal to complete documentation. Finally, a recommendation for an effective guideline for evaluating selected encryption software will be established from the documentation and presented in an easy-to-understand flow chart diagram.

3.4.6 Data Map

A data map was developed to summarise the research requirements. Figure 3.4 presents the research data map outlining the main research question, secondary research questions and the links to the associated research testing phases. Additionally, all the connections and links are provided for referencing.

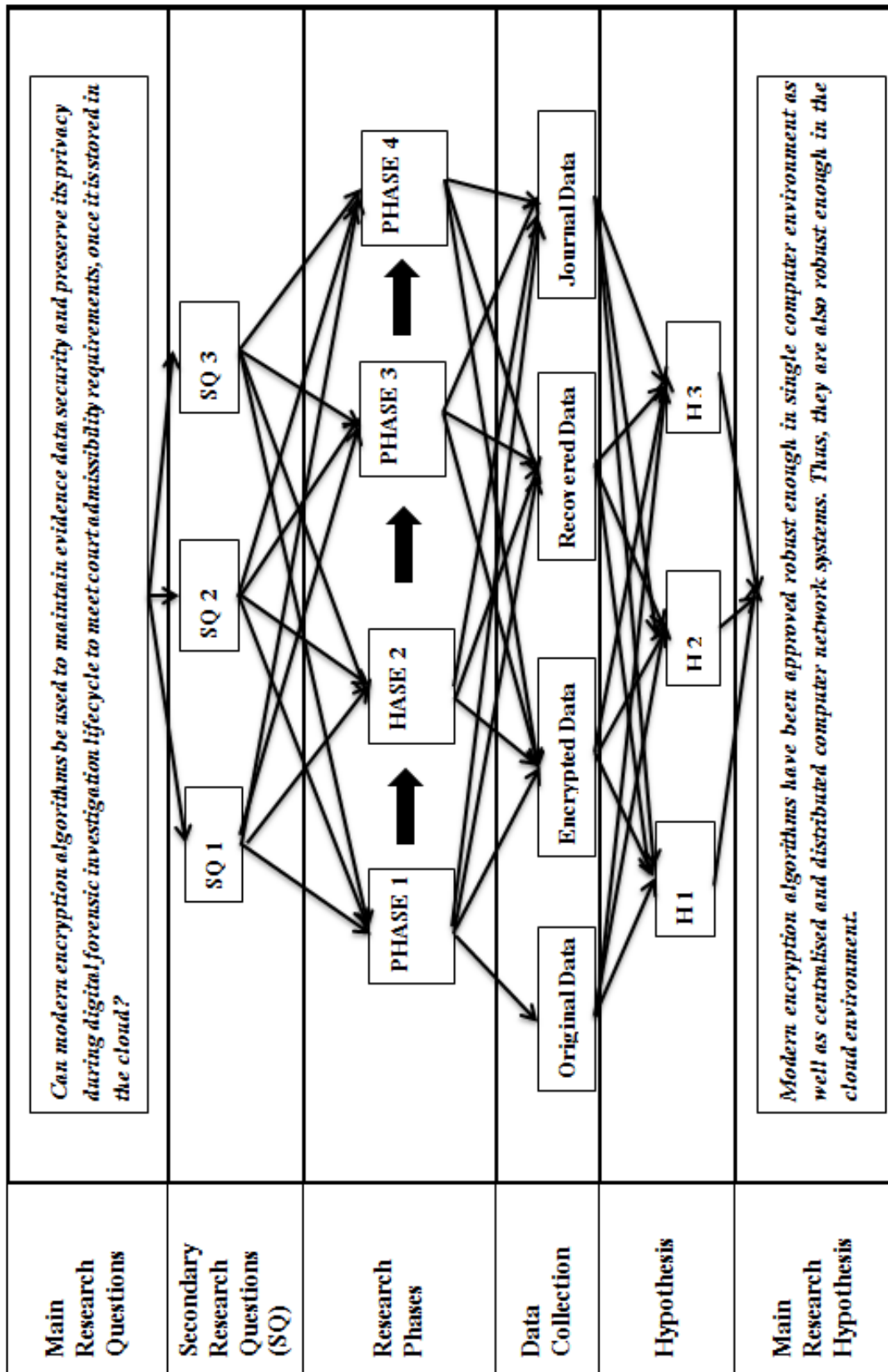


Figure 3.4: Research Data Map.

3.5 LIMITATIONS

The research methodology that has been proposed poses a number of limitations which will be outlined and discussed so that constraints in the proposed research may be recognised. It is important to identify such limitations in order to correctly evaluate the results obtained and to determine if, or where further areas of research are needed in the scope of using modern encryption algorithms to maintain a high level data security and preserve privacy of digital forensic investigation evidence data stored in the cloud environment.

The first main limitation of the propose research is that there are numerous modern encryption algorithms such as discussed in Section 2.5. Each uses different encryption and decryption techniques. Moreover, even the tools implementing the same encryption algorithm can have different features. For example, both AxCrypt and AESCrypt use AES encryption algorithm; however not only AxCrypt can encrypt single files, but also directories. On the other hand, AESCrypt can only encrypt individual files. . Furthermore, AESCrypt uses 256-bits key length, and AxCrypt uses 128-bits key length. In addition, all the selected encryption tools in this experiment use symmetric encryption technique, which means that both the encryption key and decryption key are the same. As aforementioned in Section 2.5, there is also asymmetric encryption technique, where encryption key and decryption key are not necessarily same. For the simplicity of the research, no asymmetric encryption software is selected.

Consequently, due to the limit resources, not all available encryption algorithms and tools can be tested in this research. In the author's opinion, it is possible that there exist far more comprehensive and robust encryption tools, which allow evidence data securely stored in the cloud to meet digital forensic investigation data preservation and confidentiality principles. Hence, the findings of the experiment cannot be generalised to other encryption tools, which are similar to the ones used in the proposed experiment. These encryption tools are selected because of their popularity, simplicity and comprehension (as discussed in chapter 2). Another reason the software selected is that

they are all free and open source. The digital forensic investigator can have the freedom to customise the tools to meet specific needs.

Secondly, the cloud simulation set up for the experiment is installed on a single networked desktop in a lab controlled environment. Two virtual machines are created and imaged on the same desktop using VMware. The operating system for the desktop is Windows 7 Professional Edition. The selected encryption tools are compatible to the operating system. However, the research method used in this experiment may be different with other operating systems like Mac or Linux. These platforms may have different file systems or structures as compared to the Windows 7.

Furthermore, the experiment is conducted on the cloud simulation. In the real world case, data distribution, relocation, compression and resizing policies in the cloud are far more complicated than the laboratory environment. In addition, different cloud vendors may use different methods and functions to implement these policies. One encryption tool performing well on one cloud, may not necessarily work on others. For example, the most representative storage service for infrastructure-oriented clouds is Amazon S3 (Carpen-Amarie, 2011, p.2077). It uses open source cloud paradigm – Hadoop, to meet the needs of data-intensive applications (Amazon). The framework takes care of splitting the data, scheduling the tasks and executing them in parallel on multiple machines. In this context, specialized distributed file systems have been proposed to deal with specific access patterns that require support for highly concurrent and fine-grained access to data. Yet, Google relies on Google File System (GFS) to provide fault tolerance by constant monitoring and automatic replication of data; whereas S3 has only limited support for data re-replication and load balancing along the storage nodes. Both GFS and Hadoop allow data management and locality transparent to users to tasks at runtime (Ghoshal & Ramakrishnan, 2012, p.1096).

Thirdly, for the sake of simplicity, the author assumes that the transmission links amongst the workstation and the virtual machines are secure. Additionally, there is not data lost during the transmission. However, in real world situation, the transmission links amongst workstations, the cloud data centres and servers are facing constant threats. Data may be lost or compromised during the transmitting stage. Hence,

asymmetric encryption algorithm such as RSA should be used to ensure evidence data is secured while being transmitted.

Fourthly, there is also a limitation on secret key storage and access control. All of the three encryption tools require secret key when performing encryption and decryption. TrueCrypt allows users to choose their own secret key or use the ones generated by the software. However, AxCrypt allows users to select a secret key from a file. Yet, AESCrypt only allows enter a secret key and confirm the key by re-entering it. No matter how the key are generated, it has to be stored somewhere. Hence, it presents a problem about secret key management and access control. In the real case scenario, secret key management and who has access to it are very complicated matters. This does not even include management for (public, private) key pair may be used in asymmetric encryption algorithm to ensure data security while evidence data are being transmitted. Hence, key management and access control have provided rich grounds for further research on information security in their own right. In this research, the author simply assumes that the secret key is stored securely.

3.6 CONCLUSION

Chapter 3 focused on developing the research methodology to conduct testing in the chosen research area of evaluating modern encryption algorithms in terms of providing high level data security and privacy preserving for evidence data stored in the cloud, in order to meet digital forensic investigation compliance principles.

Similar previous studies were presented by other researchers were also studied to aid in the development of testing methodologies. The additional information gained from the review of similar studies, coupled with the comprehensive literature review in Chapter 2, was used to develop the research questions, as well as the predicted hypotheses for each question. The proposed research model was then outlined, providing a logical progression of testing phases to be conducted. A descriptive methodology was employed to form the proposed research design, consisting of the design architecture and components. Furthermore, the proposed data requirements and limitations of the proposed research methodology were detailed and discussed.

Chapter 3 has thus presented an overview of the chosen research methodology. The research data map (see Figure 3.4) provided a graphical chart of the main and secondary research questions, linking each question to a specific phase of testing and the associated data collection point. The proposed phases of testing presented in Figure 3.2 outlines the phases of research testing needed to address the research questions. The model provides the goals of each phase of testing, involving implementing the system design in a testing environment. Following each separate phase of testing the associated data will be gathered and evaluated. Chapter 4 is now to report the findings of the experiments that were defined in this chapter.

Chapter Four

RESEARCH FINDINGS

4.0 INTRODUCTION

Chapter 3 has formulated the research questions based on the problems and issues pertinent to maintain a high level of security and privacy for preserving digital forensic investigation evidence data stored in the cloud. From this, the research methodology was then established. Furthermore, relevant studies from previous research were selected for review and guided the proposed research methodology. The research question, sub-questions as well as the research hypotheses were then derived for the selected problem and issues that were identified in the literature review in Chapter 2. The data requirements for the experimentation were presented and the limitations of the proposed research discussed.

Chapter 4 however is to report the findings of the research phases defined in Chapter 3. Any variations between the outlined methodologies and the actual experimentation will be discussed in Section 4.1. Then, in order to clearly articulate the research findings, various techniques will be used. The outcomes from each independent but consecutive four phases of testing will be reported and analysed to evaluate the purposed research design. The findings from data collection, data processing and data analysis will be presented in Section 4.2, 4.3 and 4.4. The summarised data from each phase will be presented in tabled format in Section 4.2 (initial testing findings) and Section 4.3 (stabilised testing findings). Section 4.4 concludes the chapter.

4.1 VARIATIONS IN DATA REQUIREMENTS

A number of variations to the originally proposed research methodology in data requirements (Section 3.4) have been made. It is important to identify these variations prior to the reporting of the findings from the research testing phases. Any differences

between the proposed methodology and the final methodology used during the testing phase of the research are therefore set out in the following sub sections.

4.1.1 System Design

During the course of performing the research testing phases, a number of challenges aroused which subsequently prompted changes being made in the proposed techniques for system design. During the Phase One of initial testing, the author discovered that the use of TrueCrypt as the encryption tool to maintain the data security and privacy in the cloud environment had presented a problems.

In order to encrypt individual files, TrueCrypt requires users to create a virtual volume where the encrypted files will be stored. The virtual volume is entirely encrypted and behaves like a real disk. When a user opens a file stored on a TrueCrype volume, for example, in media player, the file will be automatically decrypted to RAM on-the-fly while it is being read. Thus, after the original sample files being encrypted by TrueCrypt, the encrypted files will be stored on virtual disk of the testing desktop environment. This contradicts to the goal of the purposed research.

To overcome such problem, the author used AESTool instead. As discussed in Section 2, AESTool also uses a simple GUI window to allow users encrypting and decrypting files. Yet, users have the option of where the encrypted files can be stored. Thus, Figure 4.1 shows the variation of system design.

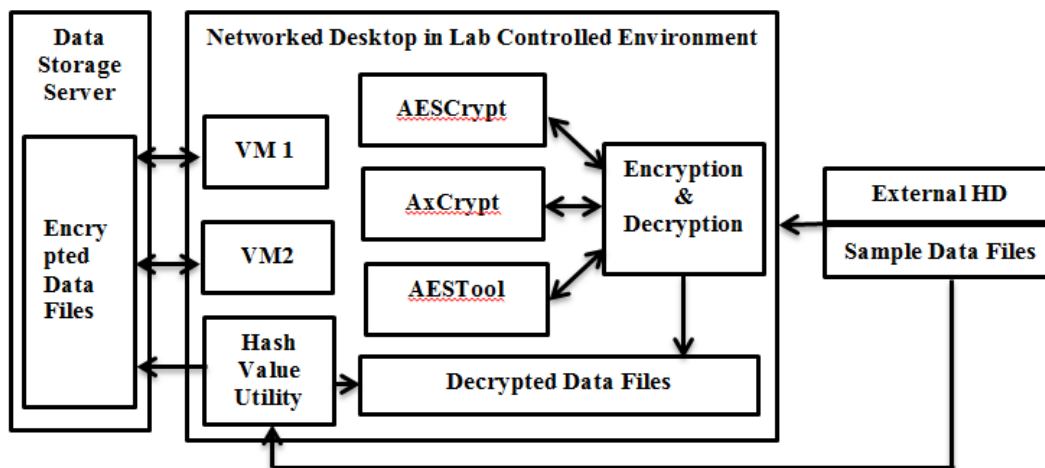


Figure 4.1: Variation of System Design.

4.1.2 Data Generation

In data generation, there are also several changes made. During the proposed experiment, the author discovered that there were more data sources required to steer the research to its original direction. Instead of having control data, encrypted data, recovered data and the documented journal on the investigation discussed in Section 3.4.1, the author used new data sources to evaluate the robustness and performances of the selected encryption tools used to maintain data security and privacy in the cloud simulation as accurately and precisely as possible. The data sources used in the experiment are that original data, encrypted data, stored data, retrieved data, recovered data and the documented journal on the investigation.

Original data is the sample evidence that is generated based on the fictitious scenarios. The second requirement for data is the encrypted data. It is generated after the selected encryption tool is used to perform encryption on the sample files. Both the original data and encrypted data are to be recorded into a table as the known or expected facts and will later be used as a comparative baseline for the data collected during the experiment to verify if the encrypted files are altered or access by an unauthorised person. The third requirement for data is stored data. Once, the encrypted files are stored on virtual machines, the stored data are produced. Before the decryption, the encrypted sample files are to be retrieved from the cloud simulation environment where the scenario is performed. Hence, retrieved data are created. Finally, the recovered data are generated after the sample files are decrypted using the same encryption tool. Once all the required data are gathered, a comparative analysis with the original data and original data will be conducted with the aim of answering the sub-questions and ultimately the main research question.

4.1.3 Data Collection

Collection of the data differed slightly from the process outlined in Section 3.4.2 due to the software restriction. The hash value utility used in this experiment – MD5 & SHA Checksum Utility could only calculate MD5 and SHA values for samples files but not the directory. Therefore, Directory Names are not used. Subsequently, the directory which contains sample files were neither encrypted nor decrypted in this experiment.

Secondly, the author believed that the use of both of MD5 value and SHA-1 value are sufficient to verify the integrity of the sample files. Since MD5 has a 128 bit hash so a brute force attack to find a collision requires at most 2^{128} applications of MD5, and 2^{64} by the birthday paradox. On the other hand, SHA-1 collision probability requires 2^{69} hash operation (Wang, Yin & Yu, 2005, p.17-36). Therefore, the author believed that the collision probability for both MD5 and SHA-1 is very small. Hence, it is omitted.

Thirdly, instead of using “Password” to represent encryption/decryption key used by each encryption tools when performing encryption and decryption; it is believed the use of “Secret Key” would be more precisely to reflect the meaning of encryption/decryption key.

Thus, the first data to be collected are the original data from Phase One. These data include File Name, Type, Size, Timestamp, MD5 Value and SHA-1 Value which will be served as baseline data to compare the results generated from the later research. The original data results can be collected from the directory window and MD5 and the SHA Checksum Utility.

Also, the second data to be collected from Phase One after the data files were encrypted using three encryption software (AESCrypt, AxCrypt and AESTool), are File Name, Type, Size, Timestamp, MD5 Value, SHA-1 Value, Successful Encryption, Secret Key and Algorithm.

The encrypted files will be stored on a virtual machine in the simulation of the cloud environment. Thus, data types collected from this phase are including File Name, Type, Size and Timestamp. Later, the encrypted files will be relocated and retrieved from another virtual machine. Hence, the data types collected after being retrieved from the virtual machines are File Name, Type, Size, Timestamp, MD5 Value and SHA-1 Value. Eventually, they will be decrypted on desktop to see whether or not the encryption algorithms will be robust enough to preserve sample files integrity, security and privacy. This original data will be able to ascertain which encryption software and file type can or cannot be resist data relocation and distribution in the cloud. Therefore, the data types collected from this stage are that File Name, Type, Size, Timestamp, MD5 Value, SHA-1 Value, Successful Decryption, Secret Key and Algorithm.

4.1.4 Data Processing, Analysis and Presentation

There were no major changes to data processing, analysis and presentation as per Section 3.4.3, 3.4.4 and 3.4.5. However, some screen shots of data analysis were added for completeness.

4.2 INITIAL TESTING FINDINGS

Initial testing of the project was proposed as it was anticipated that difficulties may occur in the implementation of the hardware and software configurations to be used during the research testing phase. The main goal of initial testing was to assess the implementation of the proposed system design of the selected encryption tools and their robustness and performances in the cloud simulation. In order to ultimately evaluate the capabilities of the selected encryption tools, it was essential firstly to perform initial testing on the lab controlled desktop environment. Following this, the encryption tools were then subjected to a range of testing to ensure its robustness and performances on the single desktop environment, such as successful rate of encrypting and decrypting sample files.

Once the initial testing of the existing system had been shown to be in order, Phase Two of initial testing, this time incorporating a single virtual machine was then conducted. Data generated using the same methodologies to the initial testing on the single desktop. Different features and functionalities of the selected encryption tools were examined and tested to develop a stabilised design, which could be used and relied on, for the final stage of the research testing.

4.2.1 Phase One: Testing of Selected Encryption Tools

Phase One is the initial stage of the purposed experiment. Once the selected encryption tools were installed on the desktop, their features and performances were examined in order to establish clear understanding about their capabilities. Also, “Encryption Data” and “Decryption Data” were collected at this stage. Together with “Original Data”, they served as baseline to be compared with data collected at later phases of the experiment. Section 4.2.1 discusses the tests conducted on Phase One of the experiment; and findings derived from the collected as well as any observations during the tests.

4.2.1.1 Phase One Experiment Process

Phase One, the first stage of initial testing involved encrypting and decrypting the sample files using the selected encryption tools on a single desktop environment. The total of 35 sample files were created and stored on an external hard drive. MD5 & SHA Checksum Utility was then used to calculate hash values for these files. The Original data were generated when files were created. Later, they were copied to a table. Appendix 1 and 2 show screenshots and tabled “Original Data”.

Each of the selected encryption tools was used to encrypt the sample files. The “Secret Key” used for AESCrypt and AxCrypt encryption and decryption functions were such that it contained 10 strings of 9 letters in alphabetical order padded with one Arabic numbers from 1 to 9 in ascending order starting with 1. The first eight letters were lower case. The ninth was upper case. For example, the “Secret Key” used to encrypt and decrypt “Encase File Sample 1.Ex01”, which is the first sample file, was that “abcdefghI1”. The “Secret Key” used to encrypt and decrypt “Encase File Sample 2.ex01”, which is the second sample file, was that “jklmonpgR2”. Table 4.1 shows the “Secret Key” used for the first 10 sample files by AESCrypt and AxCrypt.

Table 4.1: The “Secret Key” Used for the First 10 Sample Files by AESCrypt and AxCrypt.

File Name	Secrete Key
Encase File Sample 1.Ex01	abcdefghI1
Encase File Sample 2.ex01	jklmnopqR2
Encase File Sample 3.E01	stuvwxyzA3
Excel Sample File 1.xls	bcdefghiJ4
Excel Sample File 2.xls	klmnopqrS5
Excel Sample File 3.xls	tuvwxyzab6
Excel Sample File 4.xls	cdefghijK7
Excel Sample File 5.xls	lmnopqrsT8
Graphic Image Sample 1.jpg	uvwxyzabC9
Graphic Image Sample 2.jpg	defghijkL1
Graphic Image Sample 3.jpg	mnopqrstU2

On the other hand, the maximum key length that AESTool allows, is only 64 bit hexadecimal digit. Hence, for the simplicity of the experiment the all “Secret Key” used

to encrypt and decrypted sample files by AESTool, are the same, which is “ABCDEF1”, demonstrated by Table 4.2. The same “Secret key” was used for encryption and decryption for each sample files throughout the experiment.

Table 4.2: The “Secret Key” Used for the First 10 Sample Files by AESTool.

File Name	Secrete Key
Encase File Sample 1.Ex01	ABCDEF1
Encase File Sample 2.ex01	ABCDEF1
Encase File Sample 3.E01	ABCDEF1
Excel Sample File 1.xls	ABCDEF1
Excel Sample File 2.xls	ABCDEF1
Excel Sample File 3.xls	ABCDEF1
Excel Sample File 4.xls	ABCDEF1
Excel Sample File 5.xls	ABCDEF1
Graphic Image Sample 1.jpg	ABCDEF1
Graphic Image Sample 2.jpg	ABCDEF1
Graphic Image Sample 3.jpg	ABCDEF1

The “Encrypted Data” were collected and copied into a tabular form. After being successfully encrypted by each selected encryption tools, the sample files were decrypted by the same encryption tool. The “Decrypted Data” hence were created and used to check against the “Original Data”, in order to evaluate the performance of all the selected encryption tools. Appendices 3 to 11 show screenshots and tabled “Encrypted Data” and “Decrypted Data” for each encryption tool used, respectively.

4.2.1.2 Phase One Experiment Findings

The results (please refer to Appendices 3 to 11) from Phase One, showed several findings. Firstly, AEScript was able to encrypt and decrypt all sample files. That is both successful encryption and decryption rates are 100 per cent regardless of file type. This can be verified by comparing MD5 values and SHA-1values of the original sample files and the recovered files decrypted using AEScript.

Secondly, each time when AEScript was used to encrypt or decrypt files, the timestamp of the file was changed, as showed in Table 4.3 and 4.4.

Table 4.3: Timestamps of the Original Sample Files and AESCrypt Encrypted Files.

File Name	Timestamp	Timestamp	File Name
Encase File Sample 1.Ex01	29/06/2011 10:29 a.m.	13/02/2014 02:56 p.m.	Encase File Sample 1.Ex01.aes
Encase File Sample 2.ex01	28/11/2012 03:06 p.m.	13/02/2014 02:58 p.m.	Encase File Sample 2.ex01.aes
Encase File Sample 3.E01	04/04/2013 08:48 p.m.	13/02/2014 02:59 p.m.	Encase File Sample 3.E01.aes
Excel Sample File 1.xls	16/05/2013 08:41 a.m.	13/02/2014 03:22 p.m.	Excel Sample File 1.xls.aes
Excel Sample File 2.xls	17/06/2005 11:38 a.m.	13/02/2014 03:22 p.m.	Excel Sample File 2.xls.aes
Excel Sample File 3.xls	17/06/2005 11:39 a.m.	13/02/2014 03:23 p.m.	Excel Sample File 3.xls.aes
Excel Sample File 4.xls	17/06/2005 11:40 a.m.	13/02/2014 03:23 p.m.	Excel Sample File 4.xls.aes
Excel Sample File 5.xls	17/06/2005 11:41 a.m.	13/02/2014 03:23 p.m.	Excel Sample File 5.xls.aes
Graphic Image Sample 1.jpg	08/02/2008 03:44 p.m.	13/02/2014 03:24 p.m.	Graphic Image Sample 1.jpg.aes
Graphic Image Sample 2.jpg	22/01/2014 11:12 a.m.	13/02/2014 03:24 p.m.	Graphic Image Sample 2.jpg.aes
Graphic Image Sample 3.jpg	22/01/2014 11:13 a.m.	13/02/2014 03:25 p.m.	Graphic Image Sample 3.jpg.aes

Table 4.4: Timestamps of AESCrypt Encrypted Files and Recovered Files.

File Name	Timestamp	Timestamp	File Name
Encase File Sample 1.Ex01.aes	13/02/2014 02:56 p.m.	13/02/2014 05:14 p.m.	Encase File Sample 1.Ex01
Encase File Sample 2.ex01.aes	13/02/2014 02:58 p.m.	13/02/2014 05:32 p.m.	Encase File Sample 2.ex01
Encase File Sample 3.E01.aes	13/02/2014 02:59 p.m.	13/02/2014 05:33 p.m.	Encase File Sample 3.E01
Excel Sample File 1.xls.aes	13/02/2014 03:22 p.m.	13/02/2014 05:33 p.m.	Excel Sample File 1.xls
Excel Sample File 2.xls.aes	13/02/2014 03:22 p.m.	13/02/2014 05:33 p.m.	Excel Sample File 2.xls
Excel Sample File 3.xls.aes	13/02/2014 03:23 p.m.	13/02/2014 05:34 p.m.	Excel Sample File 3.xls
Excel Sample File 4.xls.aes	13/02/2014 03:23 p.m.	13/02/2014 05:34 p.m.	Excel Sample File 4.xls
Excel Sample File 5.xls.aes	13/02/2014 03:23 p.m.	13/02/2014 05:34 p.m.	Excel Sample File 5.xls
Graphic Image Sample 1.jpg.aes	13/02/2014 03:24 p.m.	13/02/2014 05:35 p.m.	Graphic Image Sample 1.jpg
Graphic Image Sample 2.jpg.aes	13/02/2014 03:24 p.m.	13/02/2014 05:35 p.m.	Graphic Image Sample 2.jpg
Graphic Image Sample 3.jpg.aes	13/02/2014 03:25 p.m.	13/02/2014 05:35 p.m.	Graphic Image Sample 3.jpg

Thirdly, when AESCrypt encrypting the sample files, it only add very small amount meta- data to the original files. The sizes of encrypted files almost had no changes at all comparing to the original files. Table 4.5 illustrates this.

Table 4.5: File Sizes of AESCrypt Encrypted Files and Original Sample Files.

Encase File Sample 1.Ex01	849,671 KB	849,672 KB	Encase File Sample 1.Ex01.aes
Encase File Sample 2.ex01	879,889 KB	879,890 KB	Encase File Sample 2.ex01.aes
Encase File Sample 3.E01	556 KB	556 KB	Encase File Sample 3.E01.aes
Excel Sample File 1.xls	36 KB	36 KB	Excel Sample File 1.xls.aes
Excel Sample File 2.xls	148 KB	149 KB	Excel Sample File 2.xls.aes
Excel Sample File 3.xls	69 KB	69 KB	Excel Sample File 3.xls.aes
Excel Sample File 4.xls	189 KB	190 KB	Excel Sample File 4.xls.aes
Excel Sample File 5.xls	89 KB	89 KB	Excel Sample File 5.xls.aes
Graphic Image Sample 1.jpg	31 KB	31 KB	Graphic Image Sample 1.jpg.aes
Graphic Image Sample 2.jpg	16 KB	16 KB	Graphic Image Sample 2.jpg.aes
Graphic Image Sample 3.jpg	10 KB	10 KB	Graphic Image Sample 3.jpg.aes
Graphic Image Sample 4.jpg	8 KB	8 KB	Graphic Image Sample 4.jpg.aes
Graphic Image Sample 5.jpg	17 KB	17 KB	Graphic Image Sample 5.jpg.aes
Graphic Image Sample 6.jpg	57 KB	58 KB	Graphic Image Sample 6.jpg.aes

Fourthly, AESCrypt was able to perform basic access control security functions. Such that user could not open the encrypted files without entering correct secret key. Figure 4.2 shows an error message when user trying to open a file encrypted by AESCrypt without entering secret key. Figure 4.3 shows an error message when user trying to open a file encrypted by AESCrypt with incorrect secret key.

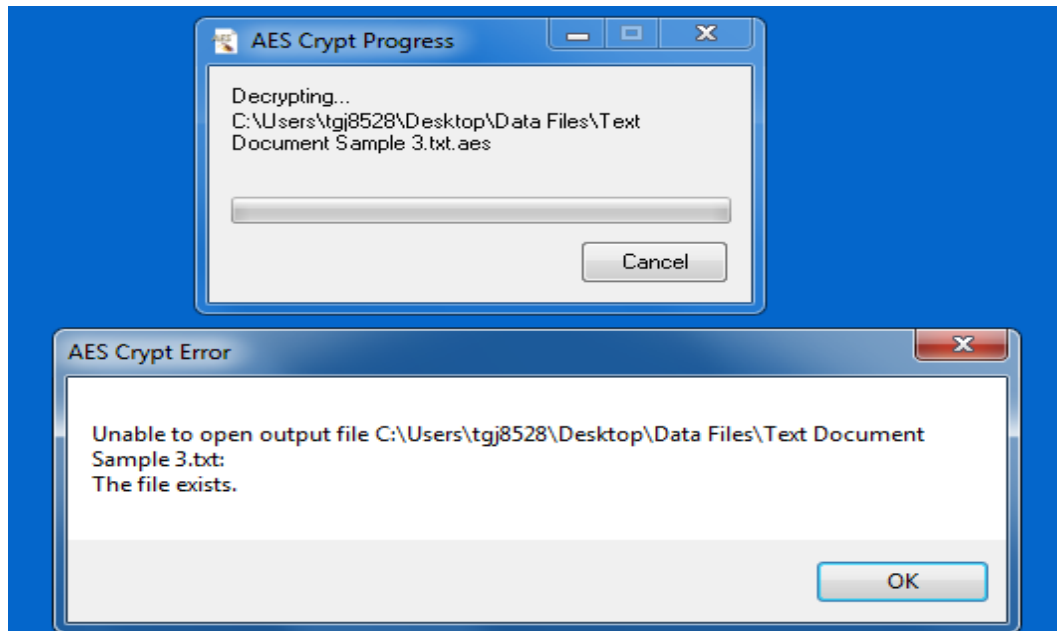


Figure 4.2: Error Message Of Not Entering AESCrypt Secret Key.

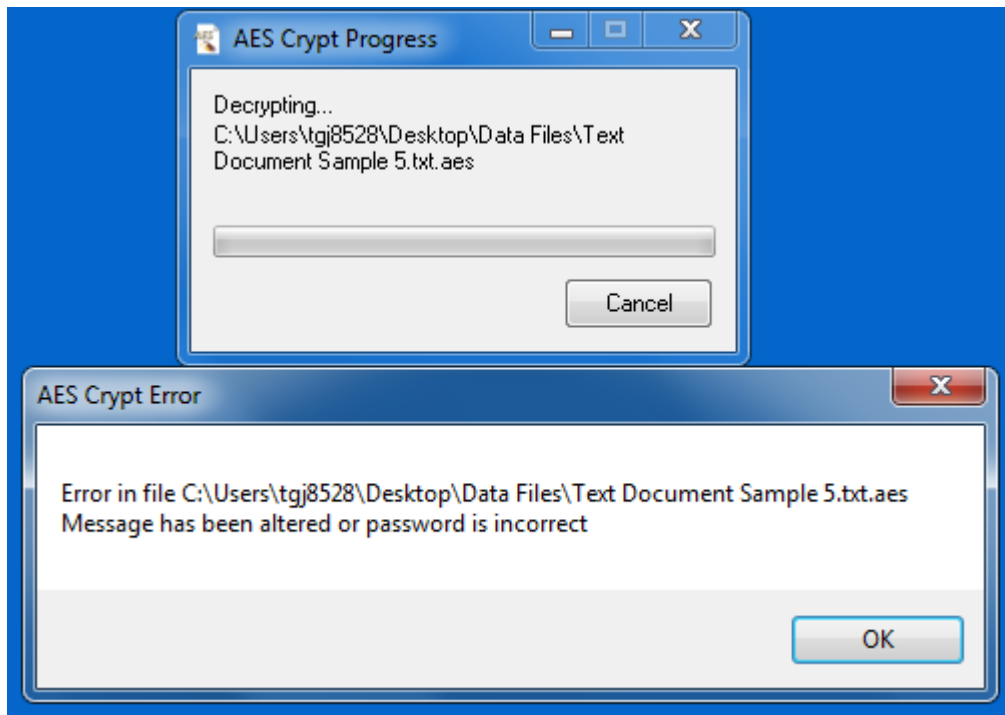


Figure 4.3: Error Message of Entering Incorrect AESCrypt Secret Key.

Fifthly, when AESCrypt performed encryption/decryption on an original sample file, the file remained unchanged; an encrypted/decrypted version of the file was created instead. The advantage of such feature is that it ensures the sample evidence files are untouched. Hence, it preserves data integrity. The disadvantage is that, once the original sample is encrypted and then decrypted by AESCrypt, the duplicated copy will occur. Hence, it may require users extra resources to manage duplicated copy with cautions. Otherwise, evidence data files may be tampered; or chain-of-custody may be compromised. Consequently, data confidentiality and availability may be breached.

Similar to AESCrypt, AxCrypt was also able to encrypt and decrypt all the sample files 100 per cent. However, in contrast, AxCrypt only altered the timestamp when it encrypted the original sample file; since it was time when the encrypted files were created. Yet, when the files were decrypted, the timestamps of the recovered files were same as the timestamps of the original files. This can be showed in Table 4.6 and 4.7. Such feature enables digital forensic investigator to keep track of when evidence

data is access last time and when the evidence data is encrypted. Subsequently, it allows digital forensic investigators to meet chain-of-custody requirement.

Table 4.6: Timestamps of the Original Sample Files and AxCrypt Encrypted Files.

File Name	Timestamp	Timestamp	File Name
Encase File Sample 1.Ex01	29/06/2011 10:29 a.m.	13/02/2014 06:59 p.m.	Encase File Sample 1-Ex01.axx
Encase File Sample 2.ex01	28/11/2012 03:06 p.m.	13/02/2014 07:00 p.m.	Encase File Sample 2-ex01.axx
Encase File Sample 3.E01	04/04/2013 08:48 p.m.	13/02/2014 07:00 p.m.	Encase File Sample 3-E01.axx
Excel Sample File 1.xls	16/05/2013 08:41 a.m.	13/02/2014 07:01 p.m.	Excel Sample File 1-xls.axx
Excel Sample File 2.xls	17/06/2005 11:38 a.m.	13/02/2014 07:01 p.m.	Excel Sample File 2-xls.axx
Excel Sample File 3.xls	17/06/2005 11:39 a.m.	13/02/2014 07:02 p.m.	Excel Sample File 3-xls.axx
Excel Sample File 4.xls	17/06/2005 11:40 a.m.	13/02/2014 07:02 p.m.	Excel Sample File 4-xls.axx
Excel Sample File 5.xls	17/06/2005 11:41 a.m.	13/02/2014 07:02 p.m.	Excel Sample File 5-xls.axx
Graphic Image Sample 1.jpg	08/02/2008 03:44 p.m.	13/02/2014 07:03 p.m.	Graphic Image Sample 1-jpg.axx
Graphic Image Sample 2.jpg	22/01/2014 11:12 a.m.	13/02/2014 07:03 p.m.	Graphic Image Sample 2-jpg.axx
Graphic Image Sample 3.jpg	22/01/2014 11:13 a.m.	13/02/2014 07:03 p.m.	Graphic Image Sample 3-jpg.axx

Table 4.7: Timestamps of AxCrypt Encrypted Files and Recovered Files.

File Name	Timestamp	Timestamp	File Name
Encase File Sample 1.Ex01	29/06/2011 10:29 a.m.	13/02/2014 06:59 p.m.	Encase File Sample 1-Ex01.axx
Encase File Sample 2.ex01	28/11/2012 03:06 p.m.	13/02/2014 07:00 p.m.	Encase File Sample 2-ex01.axx
Encase File Sample 3.E01	04/04/2013 08:48 p.m.	13/02/2014 07:00 p.m.	Encase File Sample 3-E01.axx
Excel Sample File 1.xls	16/05/2013 08:41 a.m.	13/02/2014 07:01 p.m.	Excel Sample File 1-xls.axx
Excel Sample File 2.xls	17/06/2005 11:38 a.m.	13/02/2014 07:01 p.m.	Excel Sample File 2-xls.axx
Excel Sample File 3.xls	17/06/2005 11:39 a.m.	13/02/2014 07:02 p.m.	Excel Sample File 3-xls.axx
Excel Sample File 4.xls	17/06/2005 11:40 a.m.	13/02/2014 07:02 p.m.	Excel Sample File 4-xls.axx
Excel Sample File 5.xls	17/06/2005 11:41 a.m.	13/02/2014 07:02 p.m.	Excel Sample File 5-xls.axx
Graphic Image Sample 1.jpg	08/02/2008 03:44 p.m.	13/02/2014 07:03 p.m.	Graphic Image Sample 1-jpg.axx
Graphic Image Sample 2.jpg	22/01/2014 11:12 a.m.	13/02/2014 07:03 p.m.	Graphic Image Sample 2-jpg.axx
Graphic Image Sample 3.jpg	22/01/2014 11:13 a.m.	13/02/2014 07:03 p.m.	Graphic Image Sample 3-jpg.axx

Unlike AESCrypt adding meta-data to the encrypted files, when performing encryption, AxCrypt also compressed the data files. The sizes of Encase files were slightly increased. The amount of increase data was same as the file encrypted by AESCrypt. The sizes of JPG, PNG and PDF files were remaining unchanged. Comparing with the original sample files, the size of Microsoft Excel and Word Document files were dramatically reduced. Even the sizes of Text Document files did not change, and files

sizes was same as the file sizes encrypted by AESCrypt; but in the author's opinion that it may due to the fact that the sample of Text Document files have relatively small size. Therefore, it was unable to show the differences of sizes after the files being encrypted and compressed by AxCrypt. Thus, it showed that AxCrypt had better compression results than AESCrypt. This can be illustrated by Table 4.8.

Table 4.8: File Sizes Comparison of AxCrypt and AESCrypt Encrypted Files

File Name	Size	Size	File Name
Encase File Sample 1-Ex01.axx	849,672 KB	849,672 KB	Encase File Sample 1.Ex01.aes
Encase File Sample 2-ex01.axx	879,890 KB	879,890 KB	Encase File Sample 2.ex01.aes
Encase File Sample 3-E01.axx	556 KB	556 KB	Encase File Sample 3.E01.aes
Excel Sample File 1-xls.axx	9 KB	36 KB	Excel Sample File 1.xls.aes
Excel Sample File 2-xls.axx	32 KB	149 KB	Excel Sample File 2.xls.aes
Excel Sample File 3-xls.axx	20 KB	69 KB	Excel Sample File 3.xls.aes
Excel Sample File 4-xls.axx	29 KB	190 KB	Excel Sample File 4.xls.aes
Excel Sample File 5-xls.axx	17 KB	89 KB	Excel Sample File 5.xls.aes
Word Document Sample 1-doc.axx	6 KB	22 KB	Word Document Sample 1.doc.aes
Word Document Sample 2-doc.axx	6 KB	22 KB	Word Document Sample 2.doc.aes
Word Document Sample 3-doc.axx	6 KB	22 KB	Word Document Sample 3.doc.aes
Word Document Sample 4-doc.axx	6 KB	22 KB	Word Document Sample 4.doc.aes
Word Document Sample 5-doc.axx	6 KB	22 KB	Word Document Sample 5.doc.aes

In addition, AxCrypt was also able to perform basic security functions to ensure data confidentiality. Figure 4.4 shows an error message when incorrect secret key used when unauthorised person trying to open a file encrypted by AxCrypt.

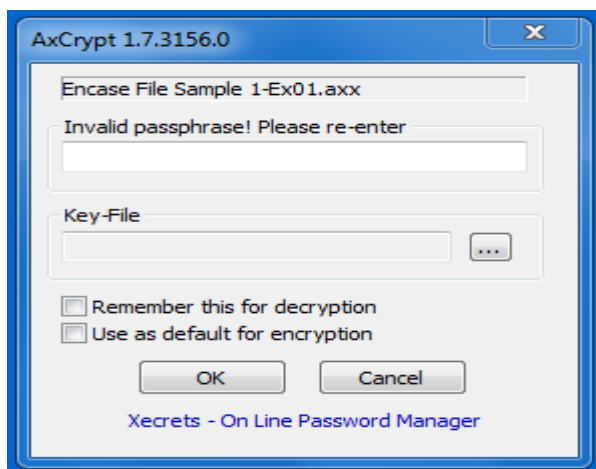


Figure 4.4: AxCrypt Error Message of Incorrect Secret Key.

Another AxCrypt feature is that it cannot perform encryption function on an open file. It may seem very trivial. However, it maintains the integrity of evidence data to allow digital investigators to meet chain-of-custody requirement. Figure 4.5 shows the error message.

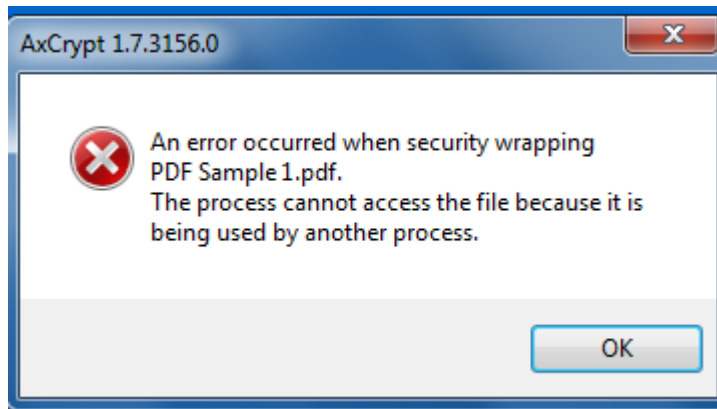


Figure 4.5: AxCrypt Error Message of Encrypting an Opening File.

After finishing encrypting file, by default AxCrypt will erase the original file. Comparing with AESCrypt, the advantage of such feature is that there will no duplicated copies occur. Hence, it does not require extra resources to manage duplicated copy with cautions. Evidence data files will not be tampered. Nor chain-of-custody will be compromised. Consequently, data confidentiality and availability may be ensured. On the other hand, in order to preserve evidence data, it requires a digital forensic investigator to make an extra copy of the original evidence data.

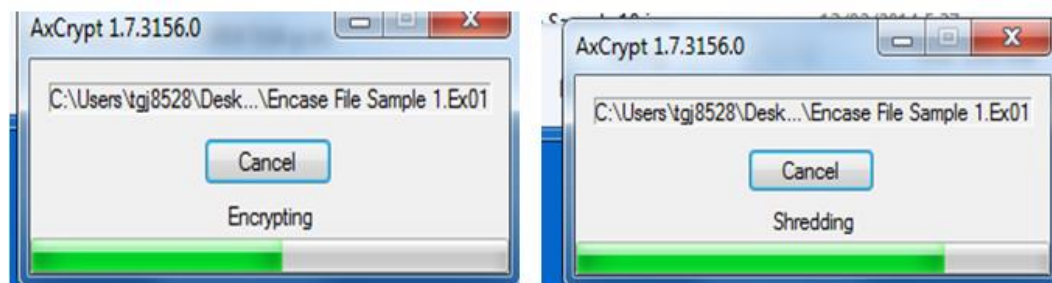


Figure 4.6: AxCrypt Encrypting and Shredding Process.

Another great feature of AxCrypt discovered by the author during Phase One of the experiment was that before AxCrypt decrypted the files, it performed file integrity check by calculating and verifying HMAC hash value of the encrypted files. Thus, extra method was used to ensure the data security and privacy preserving. This is demonstrated in Figure 4.7.

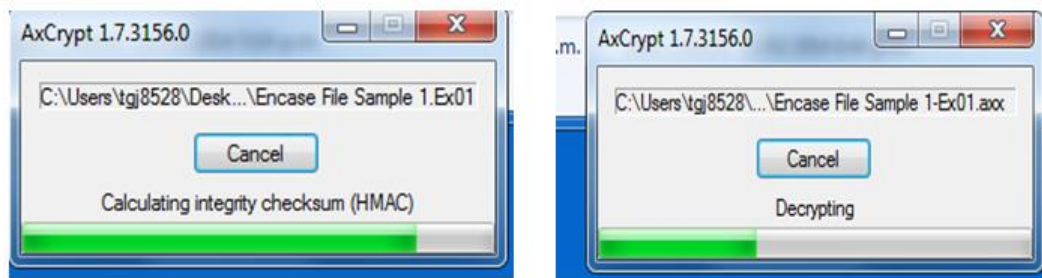


Figure 4.7: AxCrypt Verifying and Decrypting Process.

Like both of AESCrypt and AxCrypt, AESTool was also able to encrypt and decrypt all the sample files 100 per cent. Also, same as AESCrypt, each time when AESTool used to encrypt or decrypt files, the timestamp of the file was altered. Unlike AESCrypt and AxCrypt, after being encrypted by AESTool, the file sizes were increased dramatically (please refer to Appendix 4, 7 and 10). Though AESTool is a relatively simple encryption tool, it is still able to provide basic security function, showed in Figure 4.8.

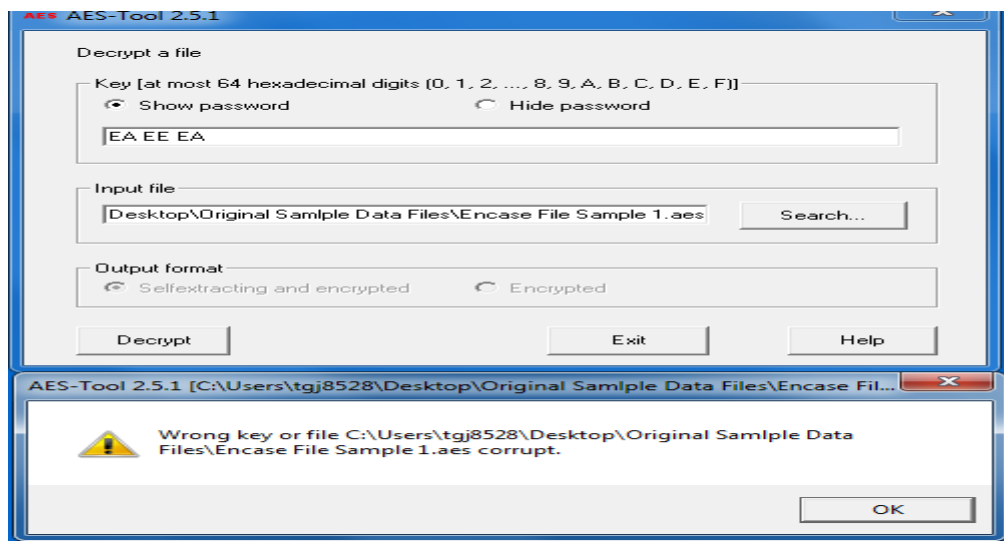


Figure 4.8: AESTool Error Message of Incorrect Secret Key.

Table 4.9: the Selected Encryption Tools Features Comparison.

Tools	Data Compression	Duplicated Copies	File Shredding	Timestamp Changing	Key Strength	Decryption Verification
AESCrypt	Average	Yes	No	Yes	Strong	No
AxCrypt	Good	No	Yes	No	Strong	Yes
AESTool	Bad	Yes	No	Yes	Average	No

From the above table, it is concluded that AxCrypt has the overall best performance results and provides the best security features amongst all the selected encryption tools.

4.2.2 Phase Two: Testing of Encryption Tools on Single VM (VM1)

After the initial evaluation conducted on the selected encryption tools on Phase One, a single virtual machine was created and added to the existing system. The purpose of adding a single virtual machine was to evaluate the robustness and performance of the selected encryption tools in a lab controlled cloud simulation environment, ultimately to answer asserted main research question.

4.2.2.1 Phase Two Experiment Process

Followed the proposed research model in 3.3.1, each of encrypted files created in Phase One by the selected encryption tools, were copied to the file directory in VM1 which had a remote connection with the desktop used in the experiment. Thus, “Stored Data” were created. This is showed in Figure 4.9.

Later, the files stored on VM1 were retrieved back to the desktop. Hence, “Retrieved Data” were generated. Accordingly, the encryption tools were used once again to decrypt the files. “Recovered Data” were produced.

In order to precisely and accurately evaluate robustness and performance of selected encryption tools, there were several comparisons made, such as “Encrypted Data” was compared with “Retrieved Data”; and “Original Data was compared with “Recovered Data”.

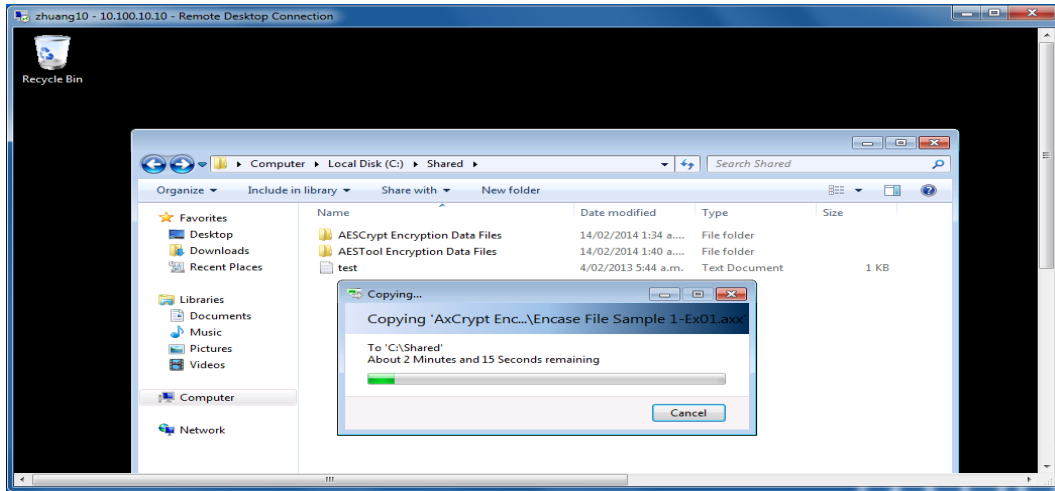


Figure 4.9: AxCrypt Encrypted Files Copied to VM1.

4.2.2.2 Phase Two Experiment Findings

The collected data (please refer to Appendix 12-20) generated from Phase Two, showed that all the selected encryption tools were able to recovered all the encrypted files respectively, without losing any data when encrypted files were stored and retrieved from a single virtual machine environment. Hence, it shows that all the selected encryption tools are reliable to provide high level data security and privacy preserving for digital forensic investigation evidence data stored on and retrieved from a single virtual machine of the cloud simulation environment. It is shown in Figure 4.10.

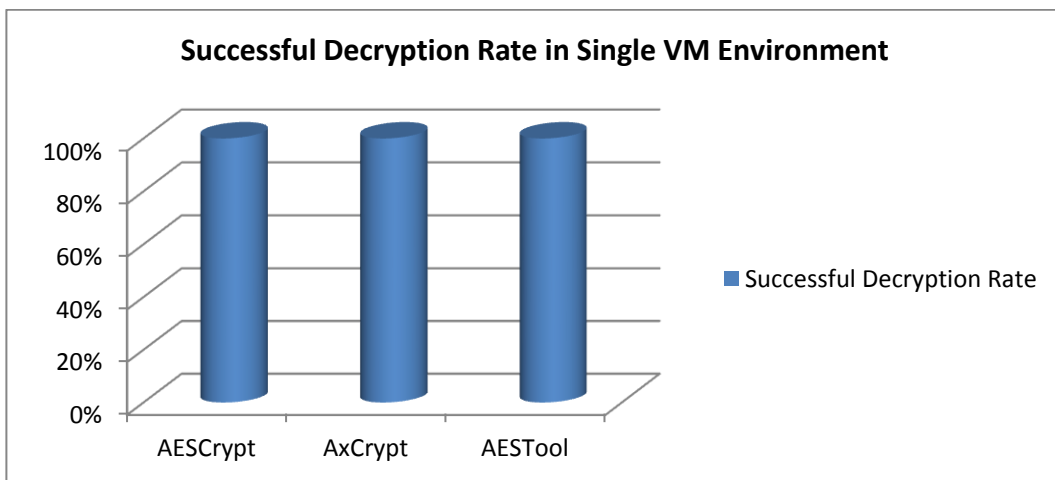


Figure 4.10: The Selected Encryption Tools Successful Decryption Rate in Single VM Environment.

4.3 STABILISED TESTING FINDINGS

Initial testing during Phase One and Phase Two revealed a number of conclusions from the data analysis and provided reasonable grounds on which to base the final stabilised research design of the proposed study. The implementation and subsequent testing of the stabilised virtual environment of the cloud simulation is now outlined in the following sections. Firstly, in Phase Three, two virtual machines were used to evaluate robustness and performances of the selected encryption tools. The testing methodologies were again drawn from initial testing results and analysis. Finally, in Phase Four, the more complicated testing scenarios were developed. The selected encryption tools were evaluated according to their robustness and performances against data relocation and distribution in the cloud simulation

4.3.1 Phase Three: Testing of Encryption Tools on Double VMs

In Phase Three another virtual machine was created and added to the existing testing environment. The extra element allowed the author to test the robustness and performances of the selected encryption tools against data relocation and distribution in simple setup of the cloud simulation environment.

4.3.1.1 Phase Three Experiment Process

Following the proposed research model in 3.3.1, each of encrypted files created in Phase One by the selected encryption tools, were copied to file directory in VM1 which had remote connection with the desktop used in the experiment. Thus, “Stored Data” on VM1 were created. The encrypted files were copied to VM2, which also had remote connection with the desktop. Hence, “Store Data” on VM2 were generated. Later, these files were retrieved back to the desktop from VM2. Subsequently, “Retrieved Data” were produced. Finally, the selected encryption tools were used to decrypt the retrieved files. If it was successful, then the files were recovered. Hence, “Recovered Data” were originated.

After the data generated from this phase, were collected and copied to tabular form, several comparisons were made, such as “Stored Data” on VM1 and VM2; “Encrypted Data” was compared with “Retrieved Data” from VM2; and “Original Data” was compared with “Recovered Data” for each selected encryption tool, respectively.

4.3.1.2 Phase Three Experiment Findings

First the results showed that the system clocks of two VMs had one hour elapse. The system clock on VM2 is one hour before VM1, showed in Figure 4.11. VM1's system clock was same as the desktop's, illustrated in Figure 4.12. Hence, the timestamps of encrypted files stored on VM2 was one hour before the timestamps of encrypted files stored on VM1 and on desktop.

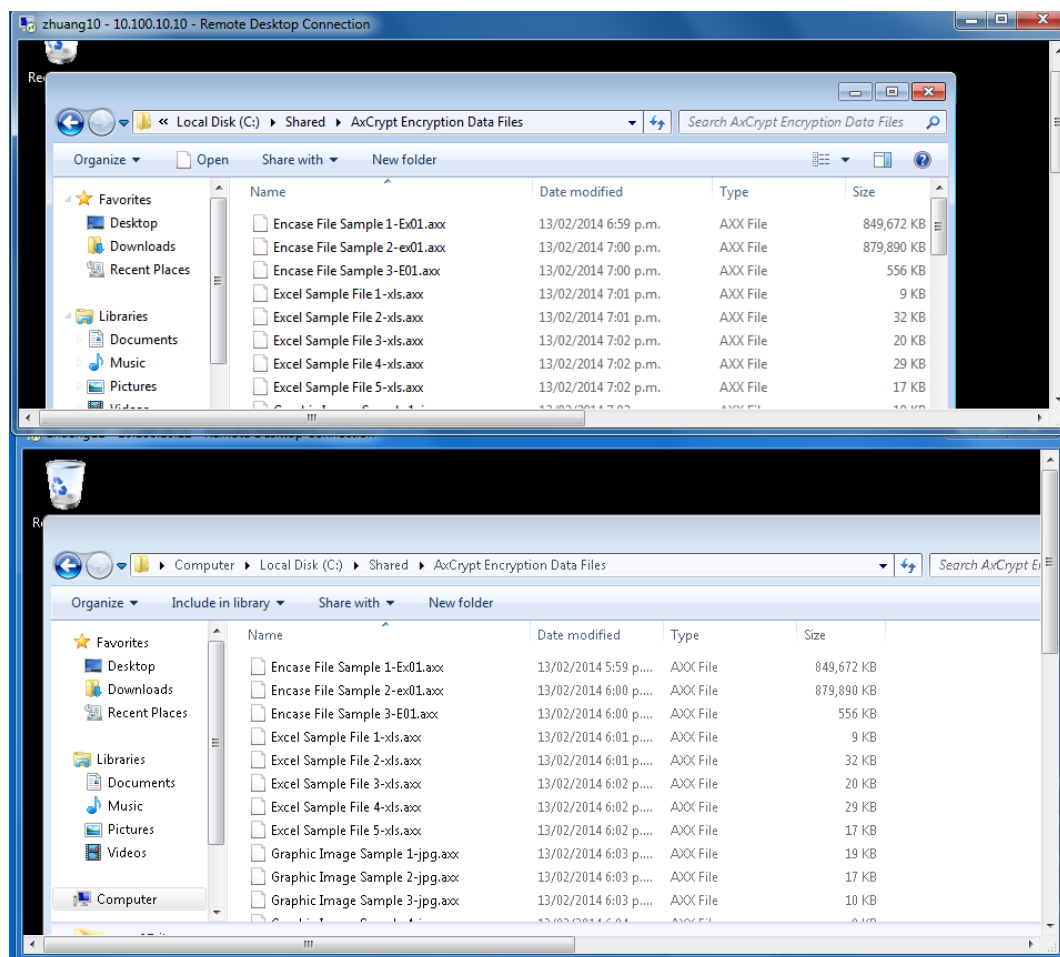
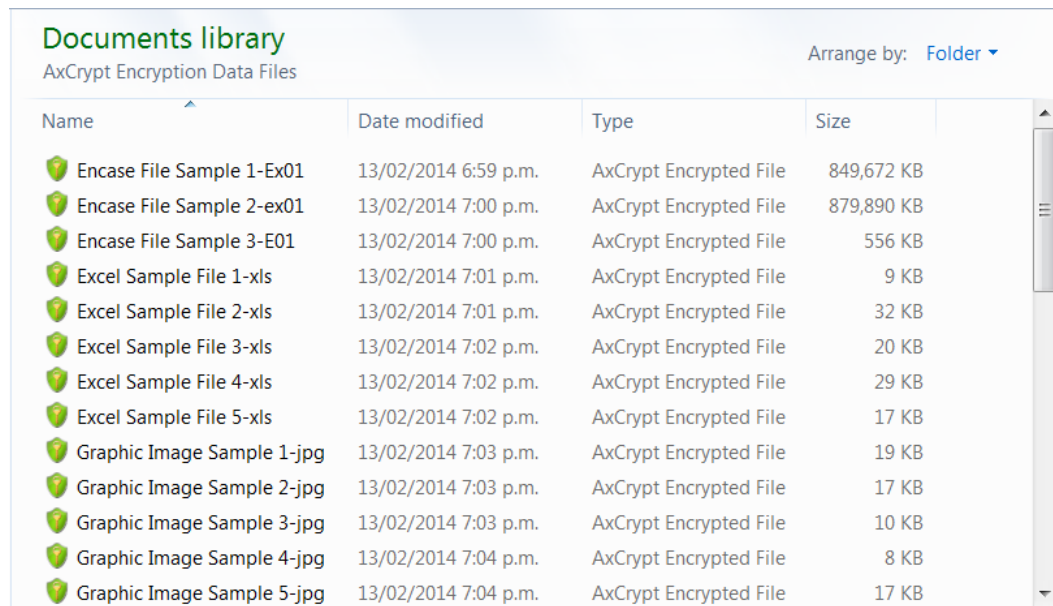


Figure 4.11: System Clock Comparison of VM1 and VM2.

However, when the encrypted files were fetched from VM2 to the desktop, the timestamps of the encrypted files were changed back to the original timestamps of when the encrypted files were created on the desktop (please refer to Appendix 6, 7 and 27). Even in this case, the examples used are the files encrypted by AxCrypt; yet it applies to

all the files encrypted by AESCrypt and AESTool in the experiment (please refer to Appendix 3, 4 and 23 for the files encrypted by AESCrypt as well as Appendix 9, 10 and 31 for the files encrypted by AESTool, respectively).



Name	Date modified	Type	Size
Encase File Sample 1-Ex01	13/02/2014 6:59 p.m.	AxCrypt Encrypted File	849,672 KB
Encase File Sample 2-ex01	13/02/2014 7:00 p.m.	AxCrypt Encrypted File	879,890 KB
Encase File Sample 3-E01	13/02/2014 7:00 p.m.	AxCrypt Encrypted File	556 KB
Excel Sample File 1-xls	13/02/2014 7:01 p.m.	AxCrypt Encrypted File	9 KB
Excel Sample File 2-xls	13/02/2014 7:01 p.m.	AxCrypt Encrypted File	32 KB
Excel Sample File 3-xls	13/02/2014 7:02 p.m.	AxCrypt Encrypted File	20 KB
Excel Sample File 4-xls	13/02/2014 7:02 p.m.	AxCrypt Encrypted File	29 KB
Excel Sample File 5-xls	13/02/2014 7:02 p.m.	AxCrypt Encrypted File	17 KB
Graphic Image Sample 1-jpg	13/02/2014 7:03 p.m.	AxCrypt Encrypted File	19 KB
Graphic Image Sample 2-jpg	13/02/2014 7:03 p.m.	AxCrypt Encrypted File	17 KB
Graphic Image Sample 3-jpg	13/02/2014 7:03 p.m.	AxCrypt Encrypted File	10 KB
Graphic Image Sample 4-jpg	13/02/2014 7:04 p.m.	AxCrypt Encrypted File	8 KB
Graphic Image Sample 5-jpg	13/02/2014 7:04 p.m.	AxCrypt Encrypted File	17 KB

Figure 4.12: Screenshot of AxCrypt Encrypted Files' Timestamps on Desktop.

Such a dilemma will make a digital investigator to unsure whether or not the differences of the file timestamps shown on the cloud and the file timestamps from the last access, are due to the cloud environment setup; or unauthorised access actually occurred. Therefore, it is important for digital forensic investigator and the cloud vendor to ensure the system clocks of the cloud and workstation are exactly same. This can be done by explicitly including this requirement in service level agreement (SLA) when signing contract with the cloud vendor.

Another finding is that file type and size remained unchanged when the encrypted file was relocated and distributed between VM1 and VM2. Hence, we can conclude that there was no data compression occurred during data relocation and distribution between the two VMs.

The collected data (please refer to Appendices 12 to 20) generated from Phase Three, showed that all the selected encryption tools were able to recovered all the encrypted files respectively, without losing any data when the encrypted files were

stored on VM1 and retrieved from VM2. Hence, it shows in Figure 4.13 that all the selected encryption tools are reliable to retain data integrity against data relocation and distribution between two virtual machines of the cloud simulation environment.

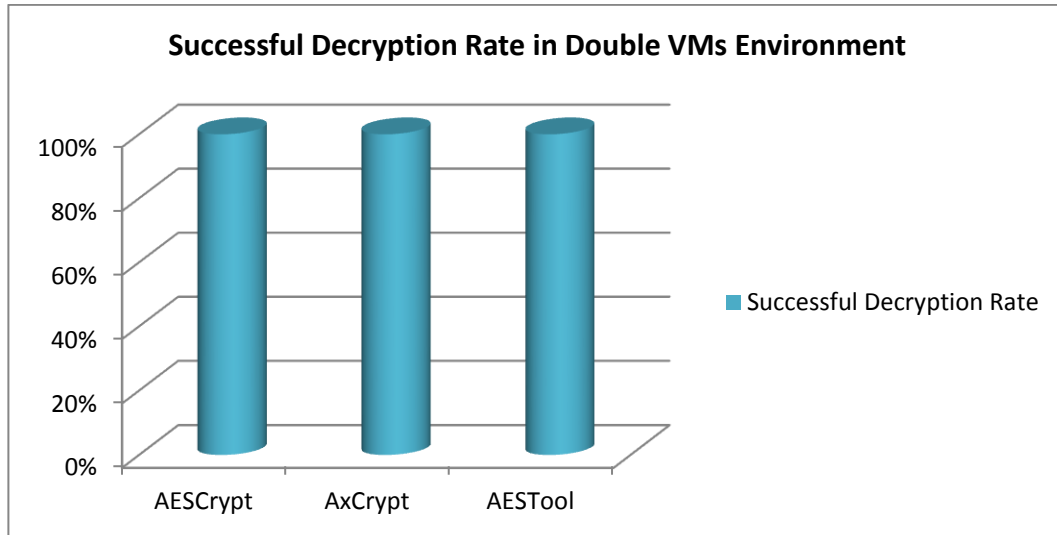


Figure 4.13: The Selected Encryption Tools Successful Decryption Rate in Double VMs Environment.

4.3.2 Phase Four: Testing of Encryption Tools on Circled VMs

Phase Four involved testing the reliability and performances of selected encryption tools on a more complicated level against data relocation and distribution in the cloud simulation environment formed by the two virtual machines.

4.3.2.1 Phase Four Experiment Process

As discussed in 3.3.1, each of encrypted files created in Phase One by the selected encryption tools, were copied to VM1 which had remote connection with the desktop used in the experiment. Thus, "Stored Data" on VM1 were created. The encrypted files were then copied to VM2, which also had remote connection with the desktop. Hence, "Store Data" on VM2 were generated. Again, the encrypted files stored on VM2 were copied back to VM1. Later, these files were retrieved back to the desktop from VM1. Subsequently, "Retrieved Data" were produced. Finally, the selected encryption tools

were used to decrypt the retrieved files. If it was successful, then the files were recovered. Hence, “Recovered Data” were originated.

After the data collected from this phase, were copied to tabular form, several comparisons were made, such as “Stored Data” on VM1 and VM2; “Encrypted Data” was compared with “Retrieved Data” from VM1; and “Original Data was compared with “Recovered Data” for each selected encryption tools, accordingly.

4.3.2.2 Phase Four Experiment Findings

The collected data (please refer to Appendix 33-47) originated from Phase Four, showed several results. First, that all the selected encryption tools were able to recover all the encrypted files respectively, without losing any data when encrypted files were stored on VM1, relocated to VM2, copied back to VM1 and retrieved from VM1. This can be verified by comparing the MD5 value and SHA-1 value of recovered files and the original files (please refer to Appendix 2, 37, 42 and 47 for each encryption tools). Hence, it shows that in Figure 4.14 all the selected encryption tools are reliable enough against data relocation and distribution between two virtual machines of the cloud simulation environment.

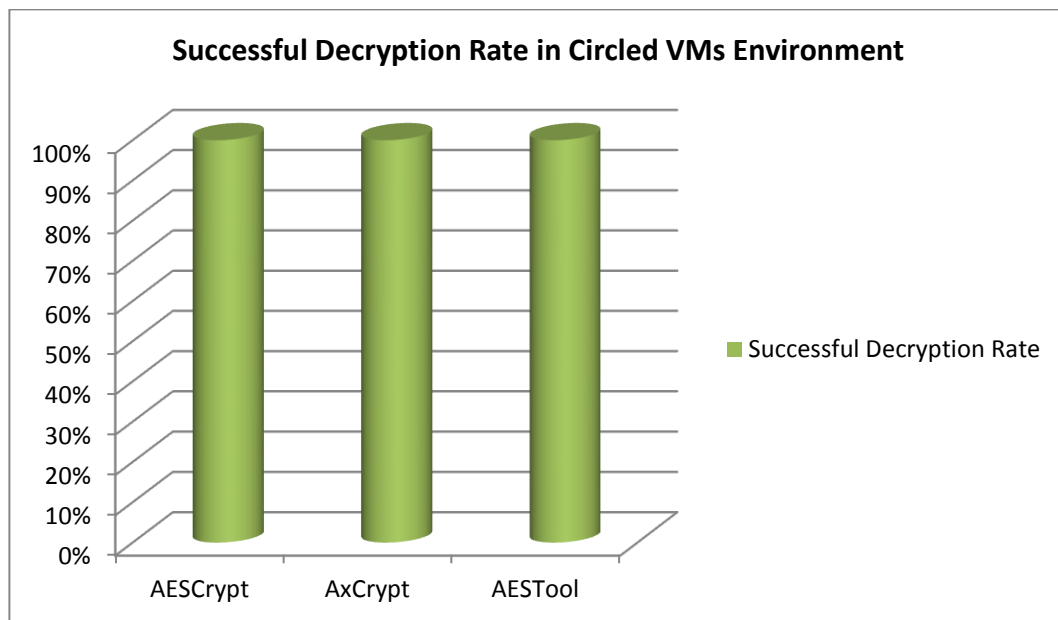


Figure 4.14: The Selected Encryption Tools Successful Decryption Rate in Circled VMs Environment.

The results also showed that encrypted files remained unchanged through the data relocation and distribution process of the experiment. Thus, it shows that the proposed system does not alter the stored files. The virtual environment of the cloud simulation behaves just like a local storage. Thus, the hypotheses suggested in Section 3.2 are proved to be correct.

4.4 CONCLUSION

Chapter 4 has covered the reporting, analysing and presentation of the research findings discovered during the research testing phases. Variations to the originally proposed research system design (Section 3.3) and data requirements (Section 3.4) were outlined and discussed in order to clarify specific changes made to the proposed testing methodology. Initial testing was then conducted. The selected encryption tools were evaluated on a single networked desktop in a laboratory controlled environment (Phase One), followed by the implementation a single virtual machine to simulate the cloud environment. Again, the selected encryption tools were tested under such environment (Phase Two). Initial testing discovered that the selected encryption tools were sufficient to preserve data integrity for digital forensic investigation evidence data stored in single virtual machine cloud simulation environment. The recovery rate of all the selected encryption tools for decrypting the encrypted files stored on single virtual machine was 100 per cent. Stabilised testing was next undertaken (Phase Three and Phase Four) involving relocating, distributing the encrypted files between two virtual machines and retrieved back to desktop.

Key findings included that all the selected encryption tools were reliable enough to provide high data security and privacy preserving for the sample files stored on the cloud simulation environment against data relocation and distribution. Yet, the collected data showed that AxCrypt had the best security features and performance results overall. The findings showed the hypotheses suggested in Section 3.2 to be correct. Ultimately, they answered the main and sub research questions.

Chapter Five

RESEARCH DISCUSSION

5.0 INTRODUCTION

Chapter 4 reported the significant findings achieved from each phase of research testing. The purpose of proposing a research methodology and then performing the various different phases of testing was to investigate the robustness and performances of the selected encryption tools to provide a high level data security and to preserve data privacy for digital forensic investigation evidence data stored in the cloud. Chapter Five will now form a discussion of the research findings for each testing phase so the significance of the results can be evaluated relating to and in association with the discipline area. Furthermore, the findings will be linked to the discussion to provide assurance when evaluating the research methodology, results achieved and conclusions drawn.

To begin, Section 5.1 will present the previously developed research questions (Section 3.2) in a tabled format. Each question will be answered and discussed in terms of the asserted hypotheses. Arguments will be made for and against the hypotheses and a summary made of the outcome. Following the tabulated questions, the findings of the research will then be discussed in detail in Section 5.2. The reason is to thoroughly evaluate the results, the purposed research design and why the results are important for the growth of knowledge in the realm of using encryption software to maintain data security and preserve privacy of digital forensic investigation evidence data stored in the cloud. In Section 5.3, the knowledge gained from the research conducted will be used to develop recommendations to further promote using modern algorithms to provide data security for the evidence data stored in the cloud environment. The chapter concludes with Section 5.4 in which the knowledge gained from the research conducted will be used to develop recommendations from the writer outlining the best practices and testing

methodologies to further promote using encryption software to protect evidence data stored in the cloud.

5.1 EVIDENCE FOR RESEARCH QUESTION ANSWERS

The main question and the following sub-questions were developed from both the literature review (Chapter 2) and the study of similar research cases (Section 3.1). The research questions will now be set out and answered in a table format. The table will be headed by each question asked, followed by the hypothesis as first outlined in the research methodology (Section 3.2). The asserted hypothesis given is a brief theoretical explanation using the knowledge gathered from the literature reviewed at the outset of the research project. The table will then present both the arguments for and the arguments against the hypotheses made, based on the findings of the research testing phases and technical knowledge learnt. The arguments for, will be those that find in support of, or prove the hypothesis, while arguments against, will refute or disprove the offered hypothesis. Reference will be made to specific findings to substantiate the statements providing rational reasoning for each argument. At the end of each table, a brief summary of the research questions and tested hypothesis will be given in order to accept, reject or be found as indeterminate based on the findings achieved.

5.1.1 Main Research Question and Associated Hypothesis

The main research question was developed to provide a specific goal for the research testing phases and to concentrate testing on a particular area. The main research question was: *Can encryption algorithms be used to preserve its privacy during digital forensic investigation lifecycle to meet court admissibility requirements, once it is stored in the cloud?*

In order to answer the proposed research question several phases of testing were proposed and conducted. The cloud simulation was created and subjected to various testing to determine the robustness and performances of selected encryption tools in providing data security and privacy preserving for digital forensic investigation evidence data stored on the cloud.

Table 5.1 displays the main research question, the associated hypothesis, arguments for and against are made and a summary of the tested hypothesis is given.

Table 5.1: Main Research Question and Tested Hypothesis.

<p>Main Question: <i>Can modern encryption algorithms be used to preserve its privacy during the digital forensic investigation lifecycle to meet court admissibility requirements, once it is stored in the cloud?</i></p>	
<p>Main Hypothesis:</p> <p>That a system designed to apply modern encryption algorithms can maintain and preserve privacy on the evidence data to meet forensic investigation principles, when the data is stored in the cloud.</p>	
<p>ARGUMENT FOR:</p> <p>The selected encryption tools were able to provide data security and privacy preserving for the sample files on the cloud simulation.</p> <p>All the selected encryption tools have security feature to prevent unauthorised access of encrypted files.</p> <p>All encryption tools implement AES algorithm, which has been approved to be secure (see Section 2.5).</p> <p>Once the sample files were encrypted by the selected files, they were passed to the cloud virtual simulation. The files were then relocated and</p>	<p>ARGUMENT AGAINST:</p> <p>The purposed research design was a relatively simple cloud simulation. It did not truly reflect the complicity of the real cloud in terms of data relocation, distribution and compression.</p> <p>All encryption algorithms are subject to brute-force attack.</p> <p>The encryption tools were not tested against attacks occurred in the cloud such as side channel attack (see Section 2.4.2.2 & Section 3.1).</p> <p>The transmission links amongst the desktop and VMs were assumed safe.</p>

<p>distributed in the simulation. After the encrypted files were retrieved, the encryption tools were able to recover all the encrypted files.</p> <p>A related study showed that modern encryption algorithms were able to provide high level data security in the real cloud environment (see Section 3.1).</p>	<p>The encryption tools were not tested against man-in-middle attack.</p> <p>Further researches are still needed to draw an absolute conclusion.</p>
<p>SUMMARY:</p> <p>The results showed that selected encryption tools were able to provided data security and privacy preserving for the sample files on the proposed cloud simulation. There were still a number of potential issues of the purposed research design and architecture as well as the software used to implement the system design. Though the simulation was relatively simple, nonetheless it has been shown that modern encryption algorithms were able to provide a high level data security in the real cloud environment (see Section 3.1). The data collected data from the experiment provided a positive outcome. Though the encryption tools were not tested against attacks in the cloud and transmission. However, AxCrypt did verify the integrity of encrypted file before decrypting them. Thus, it gave assurance on the genuineness of encrypted files. Furthermore, a hash value utility was used to verify integrity of files at each step of the experiment. Thus, the arguments made for and against prove the hypothesis to be accepted.</p>	
<p>ANSWER:</p> <p>Yes, encryption algorithms can be used to preserve its privacy during a digital forensic investigation lifecycle to meet court admissibility requirements, once it is stored in the cloud.</p>	

5.1.2 Secondary Research Questions and Associated Hypotheses

A total of 3 secondary research questions were also developed to assist in supporting or answering in different components needed to answer the main research question.

Tables 5.2, 5.3 and 5.4 display the secondary research questions, from question one to three respectively. Each table also presents the associated hypothesis, the arguments for and against the hypothesis, a summary of points discussed and the significance of the research outcome for each question. A statement of position accepting, rejecting or deeming the hypothesis indeterminate is also given for each question.

Table 5.2: Secondary Question 1 and Tested Hypothesis.

Secondary Question 1: <i>Can modern encryption algorithms provide reliability to retain data integrity in the cloud?</i>	
Hypothesis 1: Modern encryption algorithms have been approved its reliability in retaining data integrity in single computer environment as well as centralised and distributed computer network systems. Thus, they are also robust enough in the cloud environment.	
ARGUMENT FOR: After being encrypted by the selected encryption tools, all the original files were stored on the proposed cloud virtual simulation environment. Various data relocation and distribution scenarios were examined. After being retrieved from the simulation, the selected encryption tools were able to recover the original	ARGUMENT AGAINST: The cloud simulation used in the experiment was fairly simple comparing to the real cloud environment in terms of data relocation, distribution and compression. The encryption tools were not tested against attacks occurred in the cloud

files.	such as side channel attack (see Section 2.4.2.2 & Section 3.1).
A related study showed that modern encryption algorithms were robust enough to provide high level data security in the real cloud environment (see Section 3.1).	<p>The transmission links amongst the desktop and VMs were assumed safe. The encryption tools were not tested against man-in-middle attack.</p> <p>Further researches are still needed to draw an absolute conclusion.</p>
<p>SUMMARY:</p> <p>The data collected during the experiment showed that selected encryption tools were robust enough to provided data security and privacy preserving for the sample files on the proposed cloud simulation. There were still a number of potential issues of the purposed research design and architecture as well as the software used to implement the system design. Though the simulation was relatively simple, nonetheless it has been shown that modern encryption algorithms were robust enough to provide a high level data security in the real cloud environment (see Section 3.1). The experiment results showed a positive confirmation. Therefore, the arguments made for and against prove the hypothesis to be accepted.</p>	
<p>ANSWER:</p> <p>Yes, modern encryption algorithms are robust enough in the cloud.</p>	

Table 5.3: Secondary Question 2 and Tested Hypothesis.

<i>Secondary Question 2: With the investigators not having complete control of the storage, how can the investigator be sure that evidence data is not in the process of being altered in the cloud at that moment in time?</i>
Hypothesis 2:

<p>Each time when digital forensic investigators storing and retrieving evidence data store in the cloud, the encryption software can update the most recent timestamp and hash function checksum assigned uniquely to each evidence data file after being accessed. The investigators can use these parameters to check against the last updates to ensure evidence data is not in the process of being altered in the cloud at that moment in time.</p>	
<p>ARGUMENT FOR:</p> <p>Each time when AEScrypt and AESTool used to encrypt or decrypt files, the timestamp of the file was changed.</p> <p>AxCrypt only altered timestamp when it encrypted the original sample file; since it was time when the encrypted files were created. Yet, when the files were decrypted, the timestamps of the recovered files were same as the timestamps of the original files.</p> <p>Before AxCrypt decrypted the files, it performed file integrity check by calculating and verifying HMAC hash value of the encrypted files.</p> <p>Hash value utility was used to verify integrity of all the files at each step of the experiment.</p> <p>Even all hash functions are subject to</p>	<p>ARGUMENT AGAINST:</p> <p>The system clocks of two VMs had one hour elapse. The system clock on VM2 is one hour before VM1. Also, VM1's system clock was same as the desktop. Such a dilemma will make a digital investigator unsure whether or not the differences of the file timestamps shown on the cloud and the file timestamps from the last access, are due to the cloud environment setup; or unauthorised access actually occurred.</p> <p>All hash functions are subject to brute-force attack.</p>

brute-force attack, but the collision probability is relatively small. Hence, can be omitted.	
<p>SUMMARY:</p> <p>When files encrypted or decrypted by AESCrypt and AESTool, new timestamps were created. On the other hand, when file was encrypted by AxCrypt, new timestamps were created. Yet, when encrypted files were decrypted, the timestamps of recovered files were same as the original files'. When VM's system clock was same as the desktop, digital forensic investigators could rely on checking timestamps of files to track the access of evidence data stored on the cloud simulation. However, When VM's system clock was not same as the desktop, digital forensic investigators could not rely on checking timestamps of files to track the access of evidence data stored on the cloud simulation. Thus, when such dilemma occurs, a hash value utility was used to verify integrity of files at each step of the experiment. Thus, digital investigators can be sure that evidence data is not in the process of being altered in the cloud at that moment in time. The experiment results verified the hypothesis. Therefore, the arguments made for and against prove the hypothesis to be accepted.</p>	
<p>ANSWER:</p> <p>Each time when digital forensic investigators storing and retrieving evidence data store in the cloud, the encryption software can update the most recent timestamp and hash function checksum assigned uniquely to each evidence data file after being accessed. The investigators can use these parameters to check against the last updates to ensure evidence data is not in the process of being altered in the cloud at that moment in time.</p>	

Table 5.4: Secondary Question 3 and Tested Hypothesis.

Secondary Question 3: <i>How to protect the privacy of innocent data during</i>
--

<i>investigation?</i>	
Hypothesis 3: Modern encryption algorithms have been approved to be very effective and efficient to maintain high level data security. Therefore, they can also be used to protect the privacy of innocent data during investigation.	
ARGUMENT FOR: <p>The selected encryption tools were able to provide data security and privacy preserving for the sample files on the cloud simulation.</p> <p>All the selected encryption tools have security feature to prevent unauthorised access of encrypted files.</p> <p>Once the sample files were encrypted by the selected files, they were passed to the cloud virtual simulation. The files were then relocated and distributed in the simulation. After the encrypted files were retrieved, the encryption tools were able to recover all the encrypted files.</p> <p>All encryption tools implement AES algorithm, which has been approved to be secure (see Section 2.5).</p> <p>A related study showed that modern</p>	ARGUMENT AGAINST: <p>The purposed research design was a relatively simple cloud simulation. It did not truly reflect the complicity of the real cloud in terms of data relocation, distribution and compression.</p> <p>The encryption tools were not tested against attacks occurred in the cloud such as side channel attack (see Section 2.4.2.2 & Section 3.1).</p> <p>The transmission links amongst the desktop and VMs were assumed safe. The encryption tools were not tested against man-in-middle attack.</p> <p>All encryption algorithms are subject to brute-force attack.</p> <p>Further researches are still needed to draw an absolute conclusion.</p>

encryption algorithms were able to provide high level data security in the real cloud environment (see Section 3.1).	
<p>SUMMARY:</p> <p>The results showed that selected encryption tools were able to provide data security and privacy preserving for the sample files on the proposed cloud simulation. There were still a number of potential issues of the purposed research design and architecture as well as the software used to implement the system design. Though the simulation was relatively simple, nonetheless it has been shown that modern encryption algorithms were able to provide high level data security in the real cloud environment (see Section 3.1). The data collected data from the experiment provided a positive outcome. Though the encryption tools were not tested against attacks in the cloud and transmission. However, AxCrypt did verify the integrity of encrypted file before decrypting them. Thus, it gave assurance on the genuineness of encrypted files. Furthermore, a hash value utility was used to verify integrity of files at each step of the experiment. Thus, the arguments made for and against prove the hypothesis to be accepted.</p>	
<p>ANSWER:</p> <p>Modern encryption algorithms have been approved to be very effective and efficient to maintain a high level data security. Therefore, they can also be used to protect the privacy of innocent data during investigation.</p>	

5.2 DISCUSSION

The research findings have been reported, analysed and presented in Chapter 4. Section 5.2 will now discuss and comment on each of the four phases of research testing and the significances of those result. Each phase of testing will be discussed based on the importance of the findings in terms of answering the various research questions. This

section will be concluded with recommendations regarding the ability of the selected encryption tools to provide data security and privacy preserving for the evidence data that is stored in the cloud.

5.2.1 Discussion of Testing Phases

The research testing was divided into initial and stabilised testing, comprised of four separate testing phases, each with specific goals. The discussion of key points from the research testing phases will be conducted in order to identify and highlight the important findings. Reference will be made to specific outcomes of interest discovered during testing as well as the research questions which were addressed by each significant test conducted.

Phase One of the research testing was critical in setting the stage for the investigation of the main research question. The selected encryption tools were first installed to a desktop in a laboratory controlled environment and subjected to various initial testing requirements. Although the testing conducted in Phase One did not directly answer the research questions, the results obtained proved that the selected encryption tools was able to provide encryption on all the sample files regardless their file types. Also, they were able to successfully recover the encrypted files, respectively. Furthermore, all the selected encryption tools had security feature to prevent access to the encrypted files when an unauthorised person used incorrect secret keys (please refer to Section 4.2.1.2). The initial evaluation on the selected encryption tools was satisfactory. Thus, the selected encryption tools gave digital forensic investigators the confidence that these tools might have great possibility to provide a high level data security and privacy preserving for evidence data stored in the cloud. Hence, the hypothesis was subjected to further experimental testing.

Phase Two of the research testing involved the implementation and subsequent testing of the selected encryption tools in the cloud simulation of a single virtual machine environment. The encrypted files from Phase One were stored on and retrieved from the simulation through the virtual machine. Once they were fetched back to the desktop, the encryption tools were used to recover the sample files. As outlined in the findings (Section 4.2.2). The proposed system design and architecture prescribed by the proposed research model (Section 3.3) provided a foundation on which to implement the

cloud simulation. During the implementation and testing, the selected encryption tools were discovered to be sufficient and highly reliable to provide data security and privacy preserving for the sample files in terms of robustness and performances.

The findings provided valuable insight into the capabilities of the selected encryption tools of providing data security and privacy preserving on the cloud simulation of single virtual machine. Therefore, the main research question and sub-questions could ably be partially explained from the findings discovered. However, to fully answer the main research question and sub-questions, more tests needed to be conducted. As expected, the selected encryption tools performed accordingly as the main hypothesis and sub-hypotheses suggested in Section 3.2.

Though the selected encryption tools gave the overall satisfactory result, a slight dilemma occurred. Whenever AESCrypt and AESTool were used to encrypt and decrypt files, duplicated copies were created. Therefore, it presented a problem to the digital forensic investigator of how to manage the original files and duplicated copies as well as be able to track the most updated version of files in order to meet chain-of-custody, data integrity and subsequently evidence court admissible requirements. On the other hand, when AxCrypt performed encryption on the sample files; once the encrypted files were created, the original files were shredded. The sample files were able to be recovered, once the encrypted files were decrypted successfully. Hence, a digital forensic investigator did not have to worry about how to manage duplicated copies of the original files.

Phase Three of research testing involved implementing additional virtual machine to the simulation. Hence, the simulation contained two virtual machines, namely VM1 and VM2 respectively. The files encrypted on Phase One were once again stored on the simulation through VM1. In order to symbolise data relocation and distribution, the encrypted files were then copied to VM2 from VM1. Finally, there were retrieved back to the desktop from VM2.

Overall the selected encryption tools performed well at the satisfactory level. After the encrypted files were passed between the two virtual machines on the simulation, and retrieved back to the desktop, each of selected encryption tools were able to fully recover the original files without compromising data integrity. Thus, it

further proved what the main hypothesis and sub-hypotheses suggested in Section 3.2; and gave confirmation of the main research questions and sub-questions.

However, a slight issue occurred during the Phase Three. VM1 and VM2 as well as VM2 and the desktop did not have synchronised system clocks. More specifically, the system clock of VM2 was an hour faster than the system clock on VM1 and desktop. The dilemma is that when the cloud does not have synchronised system clock with workstation, it makes digital investigator unsure of whether or not the differences of the file timestamps shown on the cloud and the file timestamps shown on the workstation are caused by the cloud, or an unauthorised access actually occurred.

Phase Four was the final and most important testing phase and a culmination of the learnt outcomes of earlier phases of testing. Various data relocation and distribution scenarios were examined and subsequent evaluation of the selected encryption tools in terms of robustness and performances were conducted. The findings of Phase Four have earlier been reported in Section 4.3.2 and presented in Figure 4.14. Phase Four aided in answering the main research question as well as secondary question 3 and 4. The findings showed the robustness and satisfactory performances of the selected encryption tools to provide a high level data security and privacy preserving in the cloud simulation.

During the each phase of the experiment, the collected data were closely examined and evaluated in order to accurately capture changes that sample files made at each stage of every phase. The results generated by analysing the collected data, were sufficient and used to answer the main question and sub-questions.

5.2.2 Discussion of Selected Encryption Tools

The main research question addressed during the projected focussed on using modern encryption algorithms in providing high level data security and privacy preserving for digital forensics investigation evidence data store in the cloud. Therefore, it is prudent to discuss the robustness and performances of selected encryption tools which were tested during the project. Each testing phase provided findings and further understanding of the capabilities of the selected encryption tools.

Firstly, all the selected encryption tools were able to provide data security and preserve privacy for the sample files at satisfactory level in the cloud simulation. They

were able to encrypt all the sample files regardless their types, as well as to recover the sample files 100 per cent by performing decryption on the encrypted files.

The results showed that encrypted files were able to resist various data relocation and distribution scenarios examined in the experiment. Hence, the sample files' data security was maintained and privacy preserved by the selected encryption tools.

Furthermore, they all have security features to prevent unauthorised access to the encrypted files. However, during the experiment, only AxCrypt performed file integrity check by calculating and verifying HMAC hash value of the encrypted files.

Moreover, whenever AESCrypt and AESTool were used to encrypt and decrypt files, duplicated copies were created. Thus, digital forensic investigators need further resources to manage the original files and duplicated copies as well as be able to track the most updated version of files in order to meet chain-of-custody, data integrity and subsequently evidence court admissible requirements. On the other hand, when AxCrypt performed encryption on the sample files; once the encrypted files were created, the original files were shredded. The sample files were able to be recovered, once the encrypted files were decrypted successfully. Hence, a digital forensic investigator did not have to worry about how to manage duplicated copies of the original files.

In addition, even all the encryption tools implement AES encryption algorithms, yet AESCrypt has maximum key length of 256 bits. AxCrypt has maximum key length of 128 bits. However, AESTool has maximum key length of 64 bits with restriction of only hexadecimal digits used. The key length is a strong factor affecting the overall performance of an encryption algorithm in terms of resisting from brute-force attack and probability attack. Since, the key length is only 64 bits with restriction of only hexadecimal digits (0, 1, 2, ..., 8, 9, A, B, C, D, E, F). The possibility of AESTool being compromised is increased dramatically. Thus, AESTool has the worst key strength comparing with AESCrypt and AxCrypt.

Also instead of compressing sample files when performing encryption, AESTool added roughly 320K bits extra data on each of the original sample files (please refer to Appendix 1, 2, 9 and 10). In total, the entire data set of sample files were increased roughly 10.93Mbits ($320\text{Kbits} \times 35 = 11200\text{Kbits}$). Thus, it significantly increased the overall encrypted file's data sizes. Conversely, AxCrypt was able to reduced data size

when performing encryption on the sample files (please refer to Appendix 1, 2, 6 and 7). Especially that it gave excellent compression performance results on file types of Microsoft Excel and Window Documents. Finally, when performing encryptions, AESCrypt almost made no changes on the sample files. Only Encase files sizes were increased slightly. Table 4.8 shows the overall comparisons of the selected encryption tools. In the writer's opinion, AxCrypt has the overall best performance results.

5.2.3 Discussion of Testing Environment

Through the research process, various case scenarios were developed and examined in evaluating the robustness and performances of the selected encryption tools on the cloud simulation. The following section will discuss the simulation environment used during the experiment.

The experimental environment was set up to be as close as possible to the real world cloud environment. At Phase Two of the experiment, only one virtual machine was installed on a network desktop at laboratory controlled environment to simulate the cloud. At Phase Three and Four of the experiment, an additional virtual machine was added to the simulation. The virtual machines were created using VMware Workstation 9. It enables users to set up multiple virtual machines and use them simultaneously along with the actual machine. Each virtual machine can execute its own operating system, such as Microsoft Windows, Linux and Unix. As such, VMware Workstation 9 allows one physical machine to run multiple operating systems simultaneously. The encrypted files were relocated and distributed between the two virtual machines. As discussed in Section 3.5, in the real world case, data distribution, relocation, compression and resizing policies in the cloud are far more complicated than the laboratory environment. In addition, different cloud vendors may use different methods and functions to implement these policies.

In addition, the operating system for the desktop is Windows 7 Professional Edition (please refer to Appendix 48). The selected encryption tools are compatible to the operating system. However, the research method used in this experiment may be different with other operating systems like Mac or Linux. These platforms may have different file systems or structures. Thus, it may produce different research results.

5.3 RECOMMENDATIONS

The chosen area for research was derived from the literature review in Chapter 2. The main research questions and sub-questions were formed. Subsequently, the asserted main hypothesis and sub-hypotheses were found by the further review of related studies in Section 3.1. The planned experiment was conducted in order to answer the main and sub-research questions. This research followed the logical orders of scientific research, as discussed in Section 3.3. The purpose of this research is to evaluate whether or not modern encryption algorithms can maintain data security and preserve privacy of digital forensic investigation evidence data stored in the cloud.

The data collected during each phase of the experiment, have shown that the robustness and performances of all the selected encryption tools were at a satisfactory level, in terms of providing data security and preserving privacy against data relocation and distribution in the cloud simulation. However, AxCrypt had the overall best performances in terms of providing excellent data security features, file verifications and file compression. Based on the experimental results, the author recommends AxCrypt to be used to maintain a high level data security and integrity for evidence data stored on the cloud.

The research design also had some limitations (please refer to Section 3.5) and this leads to further possible research related to the research question. The author suggests that more realistic testing scenarios should be included in the future studies. Firstly, instead of testing the selected encryption tools on a cloud simulation, researchers can test the selected tools in a real cloud, such as EC2, Microsoft Azure and Google+. Thus, the results will be more persuasive. Moreover, the encryption tools should be evaluated by attacks on the cloud and transmission links, such as side channel attack, brute-force attack and man-in-middle attack. Thus, the encryption tools will be examined under more complication situations. Finally, not all encryption tools have the same features. Therefore, the author suggests that more encryption tools should be included and compared, in order to give a digital forensic investigator a much broad choice in selecting encryption tools according to specific tasks and purposes.

5.4 CONCLUSION

Chapter 5 has developed a discussion of the findings from the research testing which was reported, analysed and presented in Chapter 4. The research questions proposed in the research methodology (Section 3.2) have been answered and discussed in terms of the previously asserted hypotheses, and a conclusion reached regarding the validity of the predicted hypotheses. The findings achieved during the various testing phases were discussed and the selected encryption tools evaluated based on the robustness and performances in maintaining data security and preserving privacy of sample files in the cloud simulation, as well as the potential issues that may hinder the performances of the purposed research design.

The main research question of the project was centred on the robustness and performances of modern encryption algorithms in providing data security and privacy preserving for digital forensic investigation evidence data stored on the cloud. Subsequently, a research model was formed (Section 3.3) and a research design prescribed. During research testing the selected encryption tools and virtual machines were installed and evaluated, a stabilised design was formed, and testing scenarios were developed and examined to determine the robustness and performances of selected encryption tools. The findings discovered that the selected encryption tools were able to maintain data security and preserve privacy at an overall satisfactory level in the cloud simulation.

Chapter 6 concludes the thesis project and presents a summary of the research conducted and the significant results that have been discovered. Limitations to the research will be outlined to determine specific areas of research that were hindered in some form. In closing, other prospective fields of research within the discipline area will be discussed to highlight the many potential avenues open to future research.

Chapter Six

CONCLUSION

6.0 INTRODUCTION

Chapter Six presents the final conclusion of the thesis and the research conducted. Therefore, a summary of the research findings (Chapter 4), and subsequent review of the discussion of the findings (Chapter 5) is made. The chapter then concludes giving a synopsis of the limitations of the research but also identifies exciting avenues for potential future research within the chosen topic area.

The robustness and performances of encryption tools in the cloud was chosen area to be investigated. The popularity and current wide use of the cloud technology is unprecedented; however, this also co-occurs with the trend of increasingly widespread illegal practices involving crime. The very nature of the technology medium gives rise to potential security issues as well data preservation, integrity and governance problems in terms of storing digital forensic investigation evidence data in the cloud. Due to current problems of insufficient guidelines and procedures surrounding the process of using encryption algorithms to reinforce data security for the evidence data stored in the cloud, the chosen field of research focussed on evaluating the robustness and performances of three AES encryption tools to aid providing a high level data security and privacy preservation in the cloud.

Subsequent to a critical review of academic literature, and the analysis of similar research studies, a main research question was formed to provide a research goal. The aim was to design a cloud simulation using virtual machines installed on a networked desktop in a laboratory controlled environment to evaluate the robustness and performances of chosen encryption tools which implement AES encryption algorithms in terms of providing data security and preserving privacy. The overall findings showed

that the selected encryption tools were capable of providing data security and preserving data privacy at a satisfactory level in the cloud simulation.

Chapter 4 reported the findings from the proposed research phases. The findings were then analysed and subsequently presented. The phases involved initial and then stabilised testing. They will be briefly discussed in order to conclude the results that were discovered. Initial testing was undertaken in order to assess preliminary results and any early problems encountered so that the groundwork to develop a stabilised design was researched. Initial testing included Phase One and Phase Two of research model. Phase One involved installing the selected encryption tools to the desktop. Sample files were encrypted and decrypted using the selected encryption tools.

The results obtained proved that the selected encryption tools were able to provide encryption on all the sample files regardless their file types. Also, they were able to successfully recover the encrypted files, respectively. Furthermore, all the selected encryption tools had security features to prevent access to the encrypted files when an unauthorised person used incorrect secret keys (please refer to Section 4.2.1.2). These findings showed that the selected encryption tools were operating accordingly and correctly. Also, they provided baseline levels of performances to use in the later testing phases.

Phase Two then installed a virtual machine on the desktop to simulate the cloud environment. The encrypted files from Phase One were stored on and retrieved from the simulation through the virtual machine. Once they were fetched back to the desktop, the encryption tools were used to recover the sample files. The findings and analysis of the collected data discovered that the chosen encryption tools were capable of providing data security and preserving data privacy against data relocation and distribution for the sample files on the cloud simulation with a single virtual machine.

Stabilised testing was then conducted, comprising of research Phases Three and Four. Phase Three required using the knowledge gained from initial testing and installing an additional virtual machine to the simulation. The chosen encryption tools were once again examined and evaluated. Findings discovered that the selected encryption tools were capable of providing a satisfactory level of data security and preserving data privacy against data relocation and distribution for the sample files on

the cloud simulation. However, AxCrypt had the best performance results in terms of security features, and encryption file verification using hash values and data compression. Furthermore, the findings from Phases Two and Three reinforce that digital forensic principles are able to be maintained by AxCrypt. Thus evidence data preserving, confidentiality, availability, court admissibility and chain-of-custody are achieved.

Similar to Phase Three, the final stage of testing, Phase Four, involved relocating and distributing the encrypted files between the virtual machines, and retrieved back to the desktop. The findings from Phase Four illustrated that the selected encryption tools were capable to provide satisfactory levels of data security and preserved data privacy against data relocation and distribution for the sample files stored on the cloud simulation.

To sum up, each phase of testing provided findings to aid in answering the main research question and the associated hypothesis. The findings discovered that the selected encryption tools were robust and performed at a satisfactory level in providing data security and preserving data privacy against data relocation and distribution in the cloud simulation. However, there are still a number of potential issues regarding to the robustness and performances of selected encryption tools on the real cloud, including attack resisting capability, data compression and resizing. Therefore, in answer to the main research question, the selected encryption tools are able to preserve data privacy for digital investigation evidence data stored in the cloud. Yet, they are still required for future research to address the discovered shortcomings.

Finally, the knowledge gained was used to outline recommendations to promote using modern encryption algorithms to provide data security and privacy preserving for evidence data stored in the cloud. The recommendations include using AxCrypt to provide security and preserve privacy for evidence data stored in the cloud as well as the improvements for the future studies.

6.1 LIMITATIONS OF RESEARCH

The earlier identified limitations of the research methodology (Section 3.5) were outlined at the pre-testing stage of the proposed research, based on the defined research

model and projected system design. Those limitations that continue to be important after conducting the testing phases will be briefly reiterated. Then, limitations identified from the research findings and subsequent research discussion presented in Chapter 4 and 5 will be discussed.

A number of previously discussed limitations (Section 3.5) are still apparent, and remain a factor to the research conducted and findings achieved. Firstly, there were only three AES encryption tools were selected for the purposed research. In fact, there are numerous modern encryption algorithms that exist as discussed in Section 2.5. Each uses different encryption and decryption techniques. Moreover, even the tools implementing same encryption algorithm can have different features as showed in our experimental results.

Secondly, the experiment was conducted on a cloud simulation; and only two virtual machines were used. In the real world case, data distribution, relocation, compression and resizing policies in the cloud are far more complicated than the laboratory environment. In addition, different cloud vendors may use different methods and functions to implement these policies. One encryption tool performing well on one cloud, may not necessarily work on others. However, due to limited resources, the real clouds were not used in this experiment.

Thirdly, for the sake of simplicity, the author assumed that the transmission links amongst the workstation and the virtual machines were secure. Additionally, there was not data lost during the transmission. However, in a real world situation, the cloud is facing constant threats that data may be lost or compromised. Attacks such as brute-force, side-channel and man-in-middle were not recreated in this experiment. Thus, the conclusions drawn from the experimental results are limited to the proposed research model.

Fourthly, in this research, the author assumed that all the encryption keys were safe from attacker. However, in the real world, the encryption keys need to be properly managed, and access control policies should be developed and enforced. However, key management and access controls have provided rich grounds for research on information security in their own right. In this research, the author simply assumes that the secret key is stored securely.

There were also limitations as a result of the encryption software used during testing. Firstly, only open source encryption tools were used. The writer feels that the major downside is that these tools only provide relatively simple security features to protect encrypted files from unauthorised access. Yet, they may not be able to stand with more sophisticated attacks using supercomputers (Biryukov, & Grobshädl, 2010, p.221; GrobsBogdanov, Khovratovich & Rechberger, 2011, p.344).

Another software limitation was the lack of development that could have been made to the open source tools used. Since the source code of all tools used (AESCrypt, AxCrypt and AESTool) are released under various GNU General Public Licences (GPL), the source code is available for modification provided that certain licence specifications are met. These tools could have benefited from the addition of digital forensic functionality. However, no additions were attempted due to the defined scope of the conducted research and it not being a part of the project brief.

6.2 FUTURE RESEARCH

The research conducted during the project has provided additional insight to the chosen topic area of using modern encryption algorithms to provide security and preserve privacy for digital forensic investigation evidence data stored in the cloud. The project also highlighted a number of aspects for further research to provide security and preserve privacy for digital forensic investigation using the cloud as data storage medium.

A major area to target for future study relates to capabilities of modern encryption algorithms in providing data security and preserving privacy. The robustness and performances of the encryption algorithm against data relocation, distribution, compression and resizing, need to be investigated to a greater extent. For example, will modern encryption algorithms still be sufficient when an encrypted data file is divided into small parts and each of which is stored at different data centres. When a block cypher is used, will each small part still be encrypted while being distributed in the cloud; or can the block cypher only encrypt the data file as a whole? Moreover, when encrypted data file are stored in the cloud, they may face data compression and resizing.

Will the encryption algorithm still be able to provide security and preserve privacy when the encrypted data file is compressed and resized by the cloud?

In this research, for simplicity, the author assumed the transmission links amongst the workstation and the virtual machines were secure. Additionally, there was not data lost during the transmission. However, in a real world situation, the cloud is facing constant threats that data may be lost or compromised. Therefore, the second significant area for future research is that the encryption tools should be evaluated in a combination of asymmetric encryption such as RSA against attacks on the cloud and transmission links, such as side channel attacks, brute-force attacks and man-in-middle attacks. Thus, the encryption tools will be examined under more complication situations. Thus, evidence data security and privacy can be further improved and preserved, since RSA uses (public key, private key) pair to prevent a man-in-middle attack, and verify the integrity of encrypted data files instead of a hash utility being used each time when encrypted files are retrieved from the cloud.

The third significant area for future research is encryption key management and access control. In this research, the author assumed that all the encryption keys were safe from an attacker. However, in the real world, the encryption keys need to be properly managed, and access control policies should be developed and enforced. Only by doing so, digital forensic investigation evidence data can truly meet data confidentiality, availability, privacy preserving, chain-of-custody and eventually court admissibility requirements. Ultimately, digital forensic investigator compliance principles are fulfilled.

REFERENCES

- AES Crypt. (2014). *AES Crypt*. Retrieved from AES Crypt: <http://www.aescrypt.com/>
- Amazon. (n.d.). *Amazon elastic MapReduce (Amazon EMR)*. Retrieved from Amazon: <http://aws.amazon.com/elasticmapreduce/>
- Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R.H., Konwinski, A., Lee, G., Patterson, D.V., Rabikin, A., Stoica, I. & Zaharia, M. (2009). *Above the clouds: A berkeley view of cloud computing*. Berkeley: University of California at Berkeley.
- Axantum. (2013). *AxCrypt - password protect files with strong encryption*. Retrieved from Axantum: <http://flvranner.com/d/fileconverter.php>
- Baker, M., Buyya, R. & Laforenza, D. (2002). Grids and grid technologies for wide-area distributed computing. *International Journal of Software: Practice and Experience*, 32. 1437-1466.
- BBC News. (2009, September 02). *Engineer error knocks out Gmail*. Retrieved from BBC News: <http://news.bbc.co.uk/2/hi/technology/8232971.stm>
- Bernstein, D., Ludvigson, E., Sankar, K. & Diamond. (2009). Blueprint for the intercloud - protocols and formats for cloud computing interoperability. *Fourth International Conference on Internet and Web Applications and Services*, 328-336. Venice: IEEE.
- Biryukov, A. & Grobshädl, J. (2012). Cryptanalysis of the full AES using GPU-like special-purpose hardware. *Fundamenta Informaticae - Cryptology in Progress: 10th Central European Conference on Cryptology, Będlewo Poland, 2010*, 114 (3-4), 221-237.
- Bloomberg Business Week. (2006, November 12). *Jeff bezos' risky bet*. Retrieved from Bloomberg Business Week: <http://www.businessweek.com/stories/2006-11-12/jeff-bezos-risky-bet>

- Bogdanov, A., Khovratovich, D. & Rechberger, C. (2011). Biclique cryptanalysis of the full AES. *17th International Conference on the Theory and Application of Cryptology and Information Security*, 344-371. Seoul: Springer Berlin Heidelberg.
- Bracci, F., Corradi, A. & Foschini, L. (2012). Database security management for healthcare saas in the amazon aws cloud. *IEEE Symposium on Computers and Communications*, 812-819. Cappadocia: IEEE.
- Britz, M.T. (2009). *Computer forensics and cyber crime: An introduction 2nd edition*. Upper Saddle River: Pearson Education Inc.
- Brooks, C. (2010, July 17). *Amazon's early efforts at cloud computing? Partly accidental*. Retrieved from IT Knowledge Exchange: <http://itknowledgeexchange.techtarget.com/cloud-computing/amazons-early-efforts-at-cloud-computing-partly-accidental/>
- Carpen-Amarie, A. (2011). Towards a self-adaptive data mangement system for cloud enviornment. *2011 IEEE International Parallel & Distributed Processing Symposium* (pp. 2077-2080). Shanghai: IEEE.
- Chen, D. & Zhao, H. (2012). Data security and privacy protection issues in cloud computing. *2012 International Conference on Computer Science and Electronics Engineering (ICCSEE), 1*. 647-651. Hangzhou: IEEE.
- Christopher, S. (1959). Time sharing in large fast computers. *International Conference on Information Processing*, 336-341. Paris: UNESCO.
- Cruz, J.C.F. & Atkison, T. (2011). Digital forensics on a virtual machine. *The 49th Annual Southeast Regional Conference*, 326-327. New York: ACM.
- Cusack, B. (2012). *Cyber crime and IT governance*. Auckland: Auckland University of Technology.
- Cryptool. (n.d.). *About CrypTool 1*. Retrieved from Cryptool: <http://www.cryptool.org/en/cryptool1-en>

- Dahbur, K. & Mohammad, B. (2011). The anti-forensics challenge. *The 2011 International Conference on Intelligent Semantic Web-services and Applications*, 1-7. Amman: ACM.
- Davis, L. (2009, February 15). *Vint certf: Despite its age, the internet is still filled with problems*. Retrieved from Read Write: http://readwrite.com/2009/02/15/vint_cerf_despite_its_age_the#awesm=~olpTW7pGZ0vc4e
- Deng, M., Petkovic, M., Nalin, M. & Baroni, I. (2011). A home healthcare system in the cloud - addressing security and privacy challenges. *2011 IEEE 4th International Conference on Cloud Computing*, 549-556. Washington: IEEE.
- Firat, M. (2007, October 28). *Securing data in .net*. Retrieved from Code project: <http://www.codeproject.com/Articles/21076/Securing-Data-in-NET>
- Fogarty, K. (2012, January 05). *Malware that stole 45,000 Facebook logins highlights security hole from cloud*. Retrieved from IT World: <http://www.itworld.com/security/238079/malware-stole-45000-facebook-logins-highlights-security-hole-cloud>
- Foley, J. (2008, August 09). *Private clouds take shape*. Retrieved from Information Week: <http://www.informationweek.com/services/business/private-clouds-take-shape/209904474>
- Garfinkel, S.L. (2011, October 03). *The cloud imperative*. Retrieved from Technology Review (MIT): <http://www.technologyreview.com/news/425623/the-cloud-imperative/>
- Garfinkel, S.L. (2010). Digital forensics research: The next 10 years. *Digital investigation: The International Journal of Digital Forensics & Incident Response*, 7. 64-73.
- Gens, F. (2008, September 23). *Defining "cloud services" and "cloud computing"*. Retrieved from IDC Exchange: <http://blogs.idc.com/ie/?p=190>

- Getov, V. (2012). Security as a service in smart clouds - opportunities and concerns. *2012 IEEE 36th International Conference on Computer Software and Applications*, 373 - 379. Swissotel Grand Efes: IEEE Computer Society.
- Ghoshal, D. & Ramakrishnan, L. (2012). FRIEDA: Flexible robust intelligent elastic data management in cloud environment. *2012 SC Companion: High Performance Computing, Networking, Storage and Analysis (SCC)* (1096-1105). Salt Lake City: IEEE.
- Gibbs, S. (2013). Cloud computing. *International Journal of Innovative Research in Engineering & Science*, 1(1).10-17.
- Gizmo's. (2013, April 25). *Best free encrypted virtual drive utility*. Retrieved from Gizmo's: <http://www.techsupportalert.com/best-free-encrypted-virtual-drive-utility.htm>
- GnuPG. (2013, December 30). *The GNU Privacy Guard*. Retrieved from GnuPG: <http://www.gnupg.org/>
- Goldberg, R. P. (February 1973). Architectural Principles for Virtual Computer System. *Harvard University*, 22-26.
- Google. (2009). *Google apps service level agreement*. Retrieved from Google: <http://www.google.com/apps/intl/en/terms/sla.html>
- Google. (2013, October 15). *Google app engine*. Retrieved from Google Developers: <https://developers.google.com/appengine/docs/python/?csw=1>
- Google. (2013, September). *Our history in depth*. Retrieved from Google: <http://www.google.co.nz/about/company/history/>
- Gregor, S. (2002). Design theory in information systems. *Australian Journal of Information Systems*, 14-22.
- Haff, G. (2009, January 27). *Just don't call them private clouds*. Retrieved from Cnet: http://news.cnet.com/8301-13556_3-10150841-61.html
- Halderman, J.A., Schoen, S.D., Heninger, N., Clarkson, W., Paul, W., Calandrino, J.A. Feldman, A.J. Appelbaum, J. & Felten, E.W. (n.d.). *Lest we remember: Cold*

boot attacks on encryption keys. Retrieved from Usenix:
https://www.usenix.org/legacy/event/sec08/tech/full_papers/halderman/halderman_html/

- Hamdaqa, M., Livogiannis, T., & Tahvildari, L. (2011). A reference model for developing cloud applications. *1st International Conference on Cloud Computing and Services Science*, 98-103. Noordwijkerhout: Scite Press.
- He, S., Guo, L., Ghanem, M. & Guo, Y. (2012). Improving resource utilisation in the cloud environment using multivariate probabilistic models. *2012 IEEE 5th International Conference on Cloud Computing*, 574-581. Honolulu: IEEE.
- He, S., Guo, L., Ghanem, M., Guo, Y. & Han, R. (2012). Elastic applicaiton container: A lightweight approach for cloud resource provisioning. *2012 IEEE 26th International Conference on Advanced Information Networking and Applications*, 15-22. Fukuoka: IEEE.
- Hou, S., Uehara, T., Yiu, S.M. & Hui, L.C.K. (2011). Privacy preserving confidential forensic investigation for shared or remote servers. *Seventh International Intelligent Information Hiding and Multimedia Signal Processing Conference*, 378-383. Dalian: IEEE.
- Hu, J. & Klein, A. (2009). A benchmark of transparent data encryption for migration of web applications in the cloud. *8th IEEE International Conference on Dependable, Autonomic and Secure Computing*, 735-740. Chengdu: IEEE.
- Huang, J.Y. & Liao I.E. (2012). A searchable encryption scheme for outsourcing cloud storage. *2012 IEEE International Conference on Communication, Network and Satellite*, 142-146. Bali: IEEE.
- Hwang, J.J., Chuang, H.K., Hsu, Y.C. & Wu, H. (2011). A business model for cloud computing based on a separate encryption and decryption serviec. *2011 International Conference on Information Science and Applications*, 1-7. Jeju Island: IEEE.

- IBM. (2011, March 01). *IBM smarter computing blog*. Retrieved from IBM: https://www-304.ibm.com/connections/blogs/IBMSmarterSystems/date/201102?lang=en_us
- Jaeger, P.T., Crimes, J.M., Lin, J. & Simmons, S. (2008). Cloud computing and information policy: Computing in a policy cloud? *Journal of Information Technology & Politics*, 3.
- Kandukuri, B.R., Paturi, V.R. & Rakshit, A. (2009). Cloud security issues. *The 2009 IEEE International Conference on Services Computing*, 517-520. Bangalore: IEEE.
- Katsaros, G., Kousiouris, G., Gogouvitis, S.V., Kyriazis, D., Menychtas, A. & Varvarigou, T. (2012). A self-adaptive hierarchical monitoring mechanism for clouds. *Journal of Systems and Software*, 85(5). 1029-1041.
- King, R. (2008, August 04). *Cloud computing: Small companies take flight*. Retrieved from Bloomberg Business Week: <http://www.businessweek.com/stories/2008-08-04/cloud-computing-small-companies-take-flightbusinessweek-business-news-stock-market-and-financial-advice>
- Kortchinsky, K. (2009, June 29). *Cloudburst vmware guest to host escape story*. Retrieved from <http://www.blackhat.com:> http://www.google.co.nz/url?sa=t&rct=j&q=vm%20escape&source=web&cd=10&sqi=2&ved=0CG4QFjAJ&url=http%3A%2F%2Fwww.blackhat.com%2Fpresentations%2Fbh-usa-09%2FKORTCHINSKY%2FBHUSA09-Kortchinsky-Cloudburst-SLIDES.pdf&ei=DUyPT6-4KayaiAeM8un9Aw&usg=AFQjCNFvYG_NuT_
- Kothari, C.R. (2004). *Research Methodology: Methods and Techniques*. Delhi, India: New Age International Ltd.
- Kulkarni, G., Gambhir, J., Patil, T. & Dongare, A. (2012). A security aspects in cloud computing. *2012 IEEE 3rd International Conference on Software Engineering and Service Science*, 547-550. Beijing: IEEE.

- LaMonica, M. (2008, March 27). *Amazon web services adds 'resiliency' to ec2 compute service*. Retrieved from Cnet: http://news.cnet.com/8301-10784_3-9904091-7.html
- Li, M., Yu, S., Cao, N. & Lou, W. (2011). Authorized private keyword search over encrypted data in cloud computing. *2011 31st International Conference on Distributed Computing Systems*, 383-392. Minneapolis: IEEE.
- Lillard, T.V. (2010). *Digital forensics for network, internet, and cloud computing: A forensic evidence guide for moving targets and data*. Burlington: Syngress Publishing .
- National Institute of Justice. (2004, April 03). *NIJ: Special report - Forensic examination of digital evidence: A guide for law enforcement*. Retrieved from National Institute of Justice: <https://www.ncjrs.gov/pdffiles1/nij/199408.pdf>
- Mahmood, Z. (2011). Data location and security issues in cloud computing. *2011 International Conference on Emerging Intelligent Data and Web Technologies (EIDWT)*, 49-54. Tirana: IEEE.
- Marty, R. (2011). Cloud application logging for forensics. *The 2011 ACM Symposium on Applied Computing*, 178-184. New York: ACM.
- McKay, D. (2011, February 03). *A deep dive into hyperjacking*. Retrieved from Security Week: <http://www.securityweek.com/deep-dive-hyperjacking>
- Meacham, A. & Shasha, D. (2012). JustMyFriends: full SQL, full transactional amenities, and access privacy. *The 2012 ACM Sigmod International Conference on Mangement of Data*, 633-636. Scottsdale: ACM.
- Mell, P. & Grance, T. (2011). *The NIST definition of cloud computing (draft)*. Gaithersburg: National Institute of Standards and Technology.
- Microsoft. (2005, December). *Data confidentiality*. Retrieved from Microsoft: <http://msdn.microsoft.com/en-us/library/ff650720.aspx>

- Mohamed, E.M. (2012). Randomness testing of modern encryption techniques in cloud environment. *The 8th International Conference on Informatics and Systems*, 1-6. Cairo: Cairo University.
- Mohamed, E.M. & Abdelkader, H.S. (2012). Enhanced data security model for cloud computing. *8th International Conference on Informatics and Systems (INFOS)*, 12-17. Cairo: IEEE.
- Murray, A.C. (2009, January 09). *There's no such thing as a private cloud*. Retrieved from Information Week: <http://www.informationweek.com/cloud-computing/theres-no-such-thing-as-a-private-cloud/229207922>
- Natarajan, R. (2013, July 10). *Top 5 best free file encryption software for windows*. Retrieved from top 5 freeware: <http://www.top5freeware.com/file-encryption-software-for-windows>
- National Institute of Justice. (2004). *NIJ:Special Report - Forensic examination of digital evidence: A guide for law enforcement*. Retrieved from <https://www.ncjrs.gov/pdffiles1/nij/199408.pdf>
- One News. (2013, October 15). *Internet giants urge govt to drop spy bill*. Retrieved from TVNZ: <http://tvnz.co.nz/technology-news/internet-giants-urge-govt-drop-spy-bill-5648436>
- One News. (2013, July 13). *Microsoft raises concerns about spy laws*. Retrieved from TVNZ: <http://tvnz.co.nz/politics-news/microsoft-raises-concerns-spy-laws-5523956>
- Parkhill, D. (1966). *The challenge of the computer utility*. Boston: Addison-Wesley.
- Plankers, B. (2007, September 22). *What is VM Escape?* Retrieved from The Lone Systadmin: <http://lonesysadmin.net/2007/09/22/what-is-vm-escape/>
- Popek, G.J. & Goldberg, R.P. (1974). Formal requirements for virtualizable third generation architectures. *Communications of the ACM*, 17(7). 412-421.
- Popović, K. & Hocenski Ž. (2010). Cloud computing security issues and challenges. *The 33rd International Convention for Information and Communication*

- Technologies, Electronics and Microelectronics (MIPRO)*, 344-349. Opatija: IEEE.
- Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. (2009). Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. *The 16th ACM Conference on Computer and Communication Security*, 199-212. Chicago, Illinois, USA: ACM.
- Rouse, M. (2011, May 31). *Cloud bursting*. Retrieved from Search Cloud Computing : <http://searchcloudcomputing.techtarget.com/definition/cloud-bursting>
- Ruan, K., Carthy, J., Kechadi, T. & Crosbie, M. (2011). *Cloud forensics: An overview 7th edition*. Dublin: Centre for Cybercrime Investigation, University College Dublin. Retrieved from Centre for Cybercrime Investigation, University College Dublin.
- Ryan, P.S., Merchant, R. & Falvey, S. (2011). Regulation of the cloud in india. *Journal of Internet Law*, 15(4). 7-21.
- Salesforce. (2011). *A complete history of cloud computing*. Retrieved from Salesforce: <http://www.salesforce.com/uk/socialsuccess/cloud-computing/the-complete-history-of-cloud-computing.jsp>
- Sanderson, D. (2009). *Programming google app engine: build and run scalable web apps on google's infrastructure*. Sebastopol: O'reilly Media.
- Schneier, B., Kelsey, J., Whiting, D., Wagner, D., Hall, C., Ferguson, N., Kohno, T. & Stay, M. (2000). *The twofish team's final comments on aes selection*. San Jose: Counterpane Internet Security Inc.
- Shende, J. (2010, September 26). *Malware and Cloud Jacking*. Retrieved from Cloud Computing Journal: <http://cloudcomputing.sys-con.com/node/1543359>
- Simon, H.A. (1981). *The sciences of the artefact (2nd edition)*. Cambridge: MIT Press.
- Smart Card Basics. (2010). *Smart card security, part 2*. Retrieved from Smart Card Basics: http://www.smartcardbasics.com/smart-card-security_2.html#cryptography

- Social Security. (n.d.). *The privacy act and the freedom of information act*. Retrieved from Social Security: <http://www.ssa.gov/privacyact.htm>
- Solove, D.J. & Schwartz, P.M. (2011). *Privacy, information, and technology, third edition*. New York: Aspen Publishers.
- Somani, U., Lakhani, K. & Mundra, M. (2010). Implementing digital signature with rsa encryption algorithm to enhance the data security of cloud in cloud computing. *1st International Conference on Parallel, Distributed and Grid Computing*, 211-216. Solan: IEEE.
- Stallings, W. (2011). *Cryptography and network security: Principles and practice fifth edition*. Upper Saddle River: Pearson Education Inc.
- Stevens, A. (2011, June 29). *When hybrid clouds are a mixed blessing: Aiming for the best of the both worlds*. Retrieved from The Register: http://www.theregister.co.uk/2011/06/29/hybrid_cloud/
- Stolfo, S.J., Salem, M.B. & Keromytis, A.D. (2012). Fog computing: Mitigating insider data theft attacks in the cloud. *2012 IEEE Symposium on Security and Privacy Workshops*, 125-128. San Francisco: IEEE.
- Subramania, K. (2009, February 12). *Recession is good for cloud computing - microsoft agrees*. Retrieved from Cloud Ave: <http://www.cloudave.com/2425/recession-is-good-for-cloud-computing-microsoft-agrees/>
- Szefer, J., Keller, E., Lee, R.B., & Rexford, J. (October 2011). Eliminating the hypervisor attack surface for a more secure cloud. *The 18th ACM Conference on Computer and Communications Security*, 401-412. Chicago: ACM.
- Tajadod, G., Batten, L. & Govinda, K. (2012). Microsoft and Amazon: A comparison of approaches to cloud security. *2012 IEEE 4th International Conference on Cloud Computing Technology and Science*, 539-544. Taipei: IEEE.
- Taylor, M., Haggerty, J., Gresty, D. & Hegarty, R. (2010). Digital evidence in cloud computing systems. *Computer Law & Security Review*, 26(3). 304-308.





























- Taylor, S. & Metzler, J. (2010, August 23). *Cloud computing: Reality vs. fiction*. Retrieved from Network world: <http://www.networkworld.com/newsletters/frame/2010/082310wan1.html>
- Tholeti, B.P. (2011). *Hypervisors, virtualization, and the cloud: Learn about hypervisors, system virtualization, and how it works in a cloud environment*. New York: IBM Corporation.
- Tropical Software. (n.d.). *Triple DES encryption*. Retrieved from Tropical Software: <http://www.tropsoft.com/strongenc/des3.html>
- TrueCrypt. (2014). *Introduction*. Retrieved from TrueCrypt: <http://www.truecrypt.org/docs/>
- Van Aken, J. (2004). Management research based on the paradigm of the design sciences: The quest for field-tested and grounded technological rules. *Journal of Management Studies*, 41(2). 219-246.
- Vaquero, L.M., Roderio-Merino, J. & Caceres, J. (2009). A break in the clouds: Towards a cloud definition. *ACM SIGCOMM Computer Communication Review*, 25(6). 599-616.
- Varia, J. (2008, July 15). *Building grepthe web in the cloud, part 1: Cloud architectures*. Retrieved from Amazon Web Services: http://aws.amazon.com/articles/1632?_encoding=UTF8&jiveRedirect=1
- Vizard, M. (2012, June 21). *How cloudbursting "rightsizes" the data center*. Retrieved from Slashdot: <http://slashdot.org/topic/datacenter/how-cloudbursting-rightsizes-the-data-center/>
- VMware. (2014, January 24). *VMware Workstation zealot*. Retrieved from VMware : <http://blogs.vmware.com/workstation/>
- Wan, Z., Liu, J. & Deng, R.H. (2012). HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing. *IEEE Transactions on Information Forensics and Security*, 7(2). 743-754.





























- Wang, M., Zhu, G. & Zhang, X. (2012). General survey on massive data encryption. *2012 8th International Conference on Computing Technology and Information Management (ICCM), 1*. 150-155. Seoul: IEEE.
- Wang, X., Yin, Y.L. & Yu, H. (2005). Finding collisions in the full SHA-1. *25th Annual International Cryptology Conference*, 17-36. Santa Barbara: Springer Berlin Heidelberg.
- Weis, J. & Alves-Foss, J. (2011). Securing database as a service: Issues and compromises. *IEEE Security & Privacy*, 9(6). 49-55.
- Wikipedia. (2013, November 09). *Plausible deniability*. Retrieved from Wikipedia: http://en.wikipedia.org/wiki/Plausible_deniability
- Windows Azure. (2013). *Cloud services*. Retrieved from Windows Azure: <http://www.windowsazure.com/en-us/documentation/services/cloud-services/>
- Wong, S. (2013, August 21). *GCSB bill becomes law*. Retrieved from 3News: <http://www.3news.co.nz/GCSB-Bill-becomes-law/tabid/1607/articleID/310009/Default.aspx>
- Yadav, S., Jain, R. & Faisal, M. (2012). The energy consumptions for the betterment of computing and social environments of cloud computing. *International Journal of Latest Trends in Engineering and Technology*, 1(3). 114-122.
- Yan, C. (2011). Cybercrime forensic system in cloud computing. *2011 International Conference on Image Analysis and Signal Processing*, 612-615. Hubei: IEEE.
- Yang, Y. & Zhang, Y. (2011). A generic scheme for secure data sharing in cloud. *40th International Conference on Parallel Processing Workshops*, 145-153. Taipei: IEEE.
- Yeo, C.S., Venugopal, S., Chu, X. & Buyya, R. (2010). Autonomic metered pricing for a utility computing service. *Future Generation Computer System*, 26(8). 1437-1466.

- Young, A. (2013, August 21). *GCSB bill passes after final reading*. Retrieved from The New Zealand Herald: http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11112152
- Yu, S. W. (2010). Achieving secure, scalable, and fine-grained data access control in cloud computing. *IEEE Infocom 2010*, 1-9. San Diego: IEEE.
- Zafarullah, Z., Anwar, F. & Anwar, Z. (2011). Digital forensics for eucalyptus. *Frontiers of Information Technology*, 110-116.

APPENDICES

Appendix 1: Screenshot of “Original Data”



























Documents library Original Sample Data Files				
Name	Date modified	Type	Size	
 Encase File Sample 1Ex01	29/06/2011 10:29 a.m.	EX01 File	849,671 KB	
 Encase File Sample 2ex01	28/11/2012 3:06 p.m.	EX01 File	879,889 KB	
 Encase File Sample 3.E01	4/04/2013 8:48 p.m.	E01 File	556 KB	
 Excel Sample File 1	22/01/2014 2:14 p.m.	Microsoft Excel 97-2003 Worksheet	36 KB	
 Excel Sample File 2	22/01/2014 2:16 p.m.	Microsoft Excel 97-2003 Worksheet	148 KB	
 Excel Sample File 3	22/01/2014 2:16 p.m.	Microsoft Excel 97-2003 Worksheet	69 KB	
 Excel Sample File 4	22/01/2014 2:16 p.m.	Microsoft Excel 97-2003 Worksheet	189 KB	
 Excel Sample File 5	22/01/2014 2:16 p.m.	Microsoft Excel 97-2003 Worksheet	89 KB	
 Graphic Image Sample 1	22/01/2014 11:10 a.m.	JPEG image	31 KB	
 Graphic Image Sample 2	22/01/2014 11:12 a.m.	JPEG image	16 KB	
 Graphic Image Sample 3	22/01/2014 11:13 a.m.	JPEG image	10 KB	
 Graphic Image Sample 4	22/01/2014 11:13 a.m.	JPEG image	8 KB	
 Graphic Image Sample 5	22/01/2014 11:14 a.m.	JPEG image	17 KB	
 Graphic Image Sample 6	12/07/2005 1:14 a.m.	JPEG image	57 KB	
 Graphic Image Sample 7	3/09/2006 12:20 p.m.	JPEG image	2,001 KB	
 Graphic Image Sample 8	18/03/2009 9:06 a.m.	JPEG image	2,063 KB	
 Graphic Image Sample 9	10/01/2010 12:08 p.m.	JPEG image	155 KB	
 Graphic Image Sample 10	15/05/2012 3:43 p.m.	JPEG image	143 KB	
 Graphic Image Sample 11	21/11/1999 4:48 p.m.	JPEG image	50 KB	
 JPG Carved File Sample 1	9/05/2012 4:53 p.m.	PNG image	3 KB	
 PDF Sample 1	7/05/2011 2:15 p.m.	Adobe Acrobat Document	12,466 KB	
 PDF Sample 2	7/05/2011 2:28 p.m.	Adobe Acrobat Document	78,432 KB	
 PDF Sample 3	7/05/2011 2:17 p.m.	Adobe Acrobat Document	25,897 KB	
 PDF Sample 4	7/05/2011 1:11 p.m.	Adobe Acrobat Document	20,379 KB	
 PDF Sample 5	7/05/2011 1:11 p.m.	Adobe Acrobat Document	24,144 KB	
 Text Document Sample 1	22/01/2014 11:58 a.m.	Text Document	1 KB	
 Text Document Sample 2	22/01/2014 11:59 a.m.	Text Document	1 KB	
 Text Document Sample 3	22/01/2014 11:59 a.m.	Text Document	1 KB	





























Documents library				
Original Sample Data Files				
Name	Date modified	Type	Size	
 Excel Sample File 5	22/01/2014 2:16 p.m.	Microsoft Excel 97-2003 Worksheet	89 KB	
 Graphic Image Sample 1	22/01/2014 11:10 a.m.	JPEG image	31 KB	
 Graphic Image Sample 2	22/01/2014 11:12 a.m.	JPEG image	16 KB	
 Graphic Image Sample 3	22/01/2014 11:13 a.m.	JPEG image	10 KB	
 Graphic Image Sample 4	22/01/2014 11:13 a.m.	JPEG image	8 KB	
 Graphic Image Sample 5	22/01/2014 11:14 a.m.	JPEG image	17 KB	
 Graphic Image Sample 6	12/07/2005 1:14 a.m.	JPEG image	57 KB	
 Graphic Image Sample 7	3/09/2006 12:20 p.m.	JPEG image	2,001 KB	
 Graphic Image Sample 8	18/03/2009 9:06 a.m.	JPEG image	2,063 KB	
 Graphic Image Sample 9	10/01/2010 12:08 p.m.	JPEG image	155 KB	
 Graphic Image Sample 10	15/05/2012 3:43 p.m.	JPEG image	143 KB	
 Graphic Image Sample 11	21/11/1999 4:48 p.m.	JPEG image	50 KB	
 JPG Carved File Sample 1	9/05/2012 4:53 p.m.	PNG image	3 KB	
 PDF Sample 1	7/05/2011 2:15 p.m.	Adobe Acrobat Document	12,466 KB	
 PDF Sample 2	7/05/2011 2:28 p.m.	Adobe Acrobat Document	78,432 KB	
 PDF Sample 3	7/05/2011 2:17 p.m.	Adobe Acrobat Document	25,897 KB	
 PDF Sample 4	7/05/2011 1:11 p.m.	Adobe Acrobat Document	20,379 KB	
 PDF Sample 5	7/05/2011 1:11 p.m.	Adobe Acrobat Document	24,144 KB	
 Text Document Sample 1	22/01/2014 11:58 a.m.	Text Document	1 KB	
 Text Document Sample 2	22/01/2014 11:59 a.m.	Text Document	1 KB	
 Text Document Sample 3	22/01/2014 11:59 a.m.	Text Document	1 KB	
 Text Document Sample 4	22/01/2014 12:00 p.m.	Text Document	1 KB	
 Text Document Sample 5	22/01/2014 12:01 p.m.	Text Document	1 KB	
 Word Document Sample 1	22/01/2014 11:53 a.m.	Microsoft Word 97 - 2003 Document	22 KB	
 Word Document Sample 2	22/01/2014 11:53 a.m.	Microsoft Word 97 - 2003 Document	22 KB	
 Word Document Sample 3	22/01/2014 11:53 a.m.	Microsoft Word 97 - 2003 Document	22 KB	
 Word Document Sample 4	22/01/2014 11:54 a.m.	Microsoft Word 97 - 2003 Document	22 KB	
 Word Document Sample 5	22/01/2014 12:02 p.m.	Microsoft Word 97 - 2003 Document	22 KB	

Appendix 2: Table of “Original Data”

File Name	Type	Size	Timestamp	MD5 Value	SHA-1 Value
Encase File Sample 1E.x01	EnCase Evidence File	849,671 KB	29/06/2011 10:29 a.m.	5999BCEA0E97DA53375F2808FD1A4526	4EC9BE57076FA5E C23E07F05431E E0CF5AACAED9
Encase File Sample 2.ex01	EnCase Evidence File	879,889 KB	29/11/2012 03:06 p.m.	372D42D80233238B93E4187F12561DFB0	401A423CCE D930B9A146CC0BF56B75E33C0D358F
Encase File Sample 3.E01	EnCase Evidence File	556 KB	04/04/2013 08:48 p.m.	0186AACA9D373208279C8CB264C5023	BA2AA4CDB1A2CEB76DE6340761ED484574830B2EC
Excel Sample File 1.xls	Microsoft Excel 97-2003 Worksheet	36 KB	16/05/2013 08:41 a.m.	2C93B8B2A00CD51721B52B0FA1F3D0CF	AB3BC97CA8BCD50426A69178DE57C808289B2680
Excel Sample File 2.xls	Microsoft Excel 97-2003 Worksheet	148 KB	17/06/2005 11:38 a.m.	5637DFCA6A639B7178E B8A2017F47FF	10ADA707D929954072E2F5FE E4276F5D12E1844A
Excel Sample File 3.xls	Microsoft Excel 97-2003 Worksheet	69 KB	17/06/2005 11:39 a.m.	B1A2A3D0F54ADC27658D0A529D1962E5	21C77E DC4B640E C A6CE 1705C34E 3168D8123BCA4
Excel Sample File 4.xls	Microsoft Excel 97-2003 Worksheet	189 KB	17/06/2005 11:40 a.m.	C2193FB63A055364FCE86B1D352E DDE4	CDEF A95E 16B52F960199D9B4E 30773FF3080AC18
Excel Sample File 5.xls	Microsoft Excel 97-2003 Worksheet	89 KB	17/06/2005 11:41 a.m.	0A5FDA78D8389EB21C71BF92AD92C8D2	159BFB06D3F78987B5B1CF0A7B2449D8259157167
Graphic Image Sample 1.jpg	JPG File	31 KB	09/02/2008 03:44 p.m.	90DB7408078168B787AEB48B2C36D65A	4A973E 2C6D04D6BFBFB027C0A4CBA906E ABD460C
Graphic Image Sample 2.jpg	JPG File	16 KB	22/01/2014 11:12 a.m.	8CFB106B0AAC1017A741628751D376D0	C7228E 06BA1D9681C01844620A8AE 6CDF4C8269E
Graphic Image Sample 3.jpg	JPG File	10 KB	22/01/2014 11:13 a.m.	AA74E2E36B10DFF9B0D0CDE6B0F86AC3	0F60F38CE587A4DF0C996F8DA867AF11D255B1C
Graphic Image Sample 4.jpg	JPG File	8 KB	22/01/2014 11:13 a.m.	CC15388B2B0FC873F980FD51B63484D5	31895F A91D7F353D0D301BE 790053B891F4FFDAB
Graphic Image Sample 5.jpg	JPG File	17 KB	22/01/2014 11:14 a.m.	0A5FDA78D8389EB21C71BF92AD92C8D2	159BFB06D3F78987B5B1CF0A7B2449D8259157167
Graphic Image Sample 6.jpg	JPG File	57 KB	12/07/2005 01:14 a.m.	D2F1C6CAB6E06FAA2DE A02D7DAF2972	A3550E 9285239F679CA1592845B314D3BAFC8D59
Graphic Image Sample 7.JPG	JPG File	2,001 KB	03/09/2009 12:20 p.m.	E9E03E7CBDE53C1EAC4344AD566F48CC	0534321762701F94876FBCAC0B29DCCD1D3B5C55E
Graphic Image Sample 8.JPG	JPG File	2,063 KB	18/03/2009 09:06 a.m.	FA502616408B9197E262B6B96DEBF4332	9F55BF953D9239E4099D A978B1A08AB573081DDC
Graphic Image Sample 9.jpg	JPG File	155 KB	10/01/2010 12:08 p.m.	270657AAD1307324B356C2E876E594CA	349A534440B5715A3F256C0234B5F9BD866B745D
Graphic Image Sample 10.jpg	JPG File	143 KB	15/05/2012 03:43 p.m.	0688D1447E15A18A026EF25653147B61	8E66F89D10554B5BEEFDD02AA54D578FD2C57993A
Graphic Image Sample 11.jpg	JPG File	50 KB	21/11/1999 04:48 p.m.	8223359587404E0E1664A430B1786AD5	FC829D3A74FE9EB8873D85FE9B303A3A3C04FB782
JPG Carved File Sample 1.PNG	PNG File	3 KB	09/05/2011 04:53 p.m.	091523D1688262C765B3E270BC2641DF	A59252A8A8E BD282F70A56831BCB259D2A775DD3
PDF Sample 1.pdf	Adobe Acrobat Document	12,468 KB	07/05/2011 02:15 p.m.	D51CEFF64DB58FF6B1093A00C81F510F4	70FEE205ABBB6443641AA77E2A8D07BAADC39853F
PDF Sample 2.pdf	Adobe Acrobat Document	78,432 KB	07/05/2011 02:28 p.m.	9B10CF0E41BFF7E0DC4BCC196A5D4BC7	43109E07612ECAC6ADC9AAAB68B281136BAE548A9
PDF Sample 3.pdf	Adobe Acrobat Document	25,897 KB	07/05/2011 02:17 p.m.	8707ABB772EC57C81863D8A56E8579D5	FT725A9C766F78E17903385BDB06C352F9027A77
PDF Sample 4.pdf	Adobe Acrobat Document	20,379 KB	07/05/2011 01:11 p.m.	6E6F8EF9F1ABC66B41538F54641F9045	D6DED70991389788200C3B3704A59131A6E5116D
PDF Sample 5.pdf	Adobe Acrobat Document	24,144 KB	07/05/2011 01:11 p.m.	F0FBC1DA0477F2908EDC34AE189583DA	5160219A2646F482DEEF85DE969C0B842E2B5D0F
Text Document Sample 1.txt	Text Document	1 KB	22/01/2014 11:58 a.m.	B298224BE195B42EADC5EE391070714F	FD4D719ABFC610F724E A15E CDD55A7B6AE959E6D
Text Document Sample 2.txt	Text Document	1 KB	22/01/2014 11:59 a.m.	05CC0EF79F3AB824BCE14FC39062E897	C4B98B25050AEB6DE918A796B5C30EBDEF1496497
Text Document Sample 3.txt	Text Document	1 KB	22/01/2014 11:59 a.m.	98737ABB9C24FE151ADC37720C687C54	7D1049242610314B744192D1E A100777988166BC
Text Document Sample 4.txt	Text Document	1 KB	22/01/2014 12:00 p.m.	834E5BE18C0240D4FAEBB1BCE7205AF	8E15948E0D32F441E34D2C3ADE031475461C24DD
Text Document Sample 5.txt	Text Document	1 KB	22/01/2014 12:01 p.m.	F85B250C718103BE3FDECA1E8318EA20	3DCC79410AC0C69797F A89DDE1A2E20DCBF26AEO
Word Document Sample 1.doc	Microsoft 97-2003 Document	22 KB	22/01/2014 11:53 a.m.	263B834BDD0CD5B73BE2AD2BF446DF38	8293FCSA29F753799E12AFB67420584D307C5298
Word Document Sample 2.doc	Microsoft 97-2003 Document	22 KB	22/01/2014 11:53 a.m.	880289FA77E3BA443C3E3182D0842A2D	BDAA4AFCD8791C204E4A8F127BB77848A57B1AD91
Word Document Sample 3.doc	Microsoft 97-2003 Document	22 KB	22/01/2014 11:53 a.m.	CB689F8791B45AFAFF974B6D03C77F771	CFB870AC35086593F44E8D135455124D9095DAE1
Word Document Sample 4.doc	Microsoft 97-2003 Document	22 KB	22/01/2014 11:54 a.m.	C381FAA0CCFBC1E873879E7F327A0E07	8705FDDA0D773DCA0654BCB9CB1BDE7A3F8D8B1C
Word Document Sample 5.doc	Microsoft 97-2003 Document	22 KB	22/01/2014 12:02 p.m.	AD5136F7FA8B1223145C7FE0CADC0AD	7C33F7254E5D28887E0BA17FA451A61FB0C1E547

Appendix 3: Screenshot of AESCrypt “Encrypted Data” on Desktop

Documents library AESCrypt Encryption Data Files			
Name	Date modified	Type	Size
 Encase File Sample 1.Ex01	13/02/2014 2:56 p.m.	AES Crypt Encrypted Data File	849,672 KB
 Encase File Sample 2.ex01	13/02/2014 2:58 p.m.	AES Crypt Encrypted Data File	879,890 KB
 Encase File Sample 3.E01	13/02/2014 2:59 p.m.	AES Crypt Encrypted Data File	556 KB
 Excel Sample File 1.xls	13/02/2014 3:22 p.m.	AES Crypt Encrypted Data File	36 KB
 Excel Sample File 2.xls	13/02/2014 3:22 p.m.	AES Crypt Encrypted Data File	149 KB
 Excel Sample File 3.xls	13/02/2014 3:23 p.m.	AES Crypt Encrypted Data File	69 KB
 Excel Sample File 4.xls	13/02/2014 3:23 p.m.	AES Crypt Encrypted Data File	190 KB
 Excel Sample File 5.xls	13/02/2014 3:23 p.m.	AES Crypt Encrypted Data File	89 KB
 Graphic Image Sample 1.jpg	13/02/2014 3:24 p.m.	AES Crypt Encrypted Data File	31 KB
 Graphic Image Sample 2.jpg	13/02/2014 3:24 p.m.	AES Crypt Encrypted Data File	16 KB
 Graphic Image Sample 3.jpg	13/02/2014 3:25 p.m.	AES Crypt Encrypted Data File	10 KB
 Graphic Image Sample 4.jpg	13/02/2014 3:25 p.m.	AES Crypt Encrypted Data File	8 KB
 Graphic Image Sample 5.jpg	13/02/2014 3:25 p.m.	AES Crypt Encrypted Data File	17 KB
 Graphic Image Sample 6.jpg	13/02/2014 3:26 p.m.	AES Crypt Encrypted Data File	58 KB
 Graphic Image Sample 7.JPG	13/02/2014 3:26 p.m.	AES Crypt Encrypted Data File	2,001 KB
 Graphic Image Sample 8.JPG	13/02/2014 3:26 p.m.	AES Crypt Encrypted Data File	2,063 KB
 Graphic Image Sample 9.jpg	13/02/2014 3:27 p.m.	AES Crypt Encrypted Data File	155 KB
 Graphic Image Sample 10.jpg	13/02/2014 3:27 p.m.	AES Crypt Encrypted Data File	143 KB
 Graphic Image Sample 11.jpg	13/02/2014 3:28 p.m.	AES Crypt Encrypted Data File	50 KB
 JPG Carved File Sample 1.PNG	13/02/2014 3:28 p.m.	AES Crypt Encrypted Data File	4 KB
 PDF Sample 1.pdf	13/02/2014 3:29 p.m.	AES Crypt Encrypted Data File	12,466 KB
 PDF Sample 2.pdf	13/02/2014 3:30 p.m.	AES Crypt Encrypted Data File	78,432 KB
 PDF Sample 3.pdf	13/02/2014 3:30 p.m.	AES Crypt Encrypted Data File	25,897 KB
 PDF Sample 4.pdf	13/02/2014 3:31 p.m.	AES Crypt Encrypted Data File	20,379 KB
 PDF Sample 5.pdf	13/02/2014 3:32 p.m.	AES Crypt Encrypted Data File	24,145 KB
 Text Document Sample 1.txt	13/02/2014 3:32 p.m.	AES Crypt Encrypted Data File	1 KB

Documents library			
AESCrypt Encryption Data Files			
Name	Date modified	Type	Size
 Excel Sample File 5.xls	13/02/2014 3:23 p.m.	AES Crypt Encrypted Data File	89 KB
 Graphic Image Sample 1.jpg	13/02/2014 3:24 p.m.	AES Crypt Encrypted Data File	31 KB
 Graphic Image Sample 2.jpg	13/02/2014 3:24 p.m.	AES Crypt Encrypted Data File	16 KB
 Graphic Image Sample 3.jpg	13/02/2014 3:25 p.m.	AES Crypt Encrypted Data File	10 KB
 Graphic Image Sample 4.jpg	13/02/2014 3:25 p.m.	AES Crypt Encrypted Data File	8 KB
 Graphic Image Sample 5.jpg	13/02/2014 3:25 p.m.	AES Crypt Encrypted Data File	17 KB
 Graphic Image Sample 6.jpg	13/02/2014 3:26 p.m.	AES Crypt Encrypted Data File	58 KB
 Graphic Image Sample 7.JPG	13/02/2014 3:26 p.m.	AES Crypt Encrypted Data File	2,001 KB
 Graphic Image Sample 8.JPG	13/02/2014 3:26 p.m.	AES Crypt Encrypted Data File	2,063 KB
 Graphic Image Sample 9.jpg	13/02/2014 3:27 p.m.	AES Crypt Encrypted Data File	155 KB
 Graphic Image Sample 10.jpg	13/02/2014 3:27 p.m.	AES Crypt Encrypted Data File	143 KB
 Graphic Image Sample 11.jpg	13/02/2014 3:28 p.m.	AES Crypt Encrypted Data File	50 KB
 JPG Carved File Sample 1.PNG	13/02/2014 3:28 p.m.	AES Crypt Encrypted Data File	4 KB
 PDF Sample 1.pdf	13/02/2014 3:29 p.m.	AES Crypt Encrypted Data File	12,466 KB
 PDF Sample 2.pdf	13/02/2014 3:30 p.m.	AES Crypt Encrypted Data File	78,432 KB
 PDF Sample 3.pdf	13/02/2014 3:30 p.m.	AES Crypt Encrypted Data File	25,897 KB
 PDF Sample 4.pdf	13/02/2014 3:31 p.m.	AES Crypt Encrypted Data File	20,379 KB
 PDF Sample 5.pdf	13/02/2014 3:32 p.m.	AES Crypt Encrypted Data File	24,145 KB
 Text Document Sample 1.txt	13/02/2014 3:32 p.m.	AES Crypt Encrypted Data File	1 KB
 Text Document Sample 2.txt	13/02/2014 3:32 p.m.	AES Crypt Encrypted Data File	1 KB
 Text Document Sample 3.txt	13/02/2014 3:33 p.m.	AES Crypt Encrypted Data File	1 KB
 Text Document Sample 4.txt	13/02/2014 3:33 p.m.	AES Crypt Encrypted Data File	1 KB
 Text Document Sample 5.txt	13/02/2014 3:33 p.m.	AES Crypt Encrypted Data File	1 KB
 Word Document Sample 1.doc	13/02/2014 3:34 p.m.	AES Crypt Encrypted Data File	22 KB
 Word Document Sample 2.doc	13/02/2014 3:34 p.m.	AES Crypt Encrypted Data File	22 KB
 Word Document Sample 3.doc	13/02/2014 3:34 p.m.	AES Crypt Encrypted Data File	22 KB
 Word Document Sample 4.doc	13/02/2014 3:35 p.m.	AES Crypt Encrypted Data File	22 KB
 Word Document Sample 5.doc	13/02/2014 3:35 p.m.	AES Crypt Encrypted Data File	22 KB





























Appendix 4: Table of AESCrypt “Encrypted Data” on Desktop





















File Name	Type	Size	Timestamp	MD5 Value	SHA-1 Value	Successful Encryption	Secret Key	Algorithm
Encase File Sample 1.txt.aes	AES Crypt Encrypted Data File	849,672 KB	13/02/2014 02:56 p.m.	32EC01C90320092E68810FF6D6AE59D4	58165990DE55AE34A7C4FBEA0A91DAD21739F80	Yes	abcdehgh1	AES-256
Encase File Sample 2.txt.aes	AES Crypt Encrypted Data File	879,890 KB	13/02/2014 02:58 p.m.	8E541E6F1F1B4069E7F98B275C4F302	E227CA0FCC37B5C54CE71AA01F85228B093976E6	Yes	ijklmnopqR2	AES-256
Encase File Sample 3.txt.aes	AES Crypt Encrypted Data File	556 KB	13/02/2014 02:59 p.m.	1848D059A309A9525B3768976658B1	238369DA8C80B06E6C0B4FD0F062226E9FAA6020B	Yes	stuvwxyzA3	AES-256
Excel Sample File 1.xls.aes	AES Crypt Encrypted Data File	36 KB	13/02/2014 03:22 p.m.	2441D6C7AAAC9C42615A51EE9F85BEC	39477E7DAF659249A772172199389403353033	Yes	bcdelghiu4	AES-256
Excel Sample File 2.xls.aes	AES Crypt Encrypted Data File	149 KB	13/02/2014 03:22 p.m.	7818D3947862D802D97C038BA5D073C	20CA5CAF88223C942ED0671D1CC2C2345A60B06A	Yes	klmnopqrs5	AES-256
Excel Sample File 3.xls.aes	AES Crypt Encrypted Data File	69 KB	13/02/2014 03:23 p.m.	70287434E93C0C74435DE6DE1D1E8063	E28244A5B34A7811E1AA88367259FA04E36DD8	Yes	tuvwxyzab6	AES-256
Excel Sample File 4.xls.aes	AES Crypt Encrypted Data File	190 KB	13/02/2014 03:23 p.m.	330FA3E367766E83E4F0210D0875A808	B65DDAF4B6F03BA4A4A94E785FA2CA7283F16E	Yes	cdefghijk7	AES-256
Excel Sample File 5.xls.aes	AES Crypt Encrypted Data File	89 KB	13/02/2014 03:23 p.m.	F96852326A962060CAE68EA1A6F36A16	0159C6D1C578E0975C797CE0DAD06F5EDDA08B3A	Yes	lmnopqrst8	AES-256
Graphic Image Sample 1.jpg.aes	AES Crypt Encrypted Data File	31 KB	13/02/2014 03:24 p.m.	561A308F41A545706964EDED41AAE43	C0246AE926664E25F407A868632928C02E3CF2A	Yes	uvwxyzabc9	AES-256
Graphic Image Sample 2.jpg.aes	AES Crypt Encrypted Data File	16 KB	13/02/2014 03:24 p.m.	AB540B51677876001C3E9F6A7B19E8A8	FB4704915C1C1845F1A3819E8BD8FE663AF0723D	Yes	defghijkl1	AES-256
Graphic Image Sample 3.jpg.aes	AES Crypt Encrypted Data File	10 KB	13/02/2014 03:25 p.m.	428DCA0488C7F1415357CA6D27DF354	9A85A447FB59878C12A66B134848FA83197380C6	Yes	mnopqrstU2	AES-256
Graphic Image Sample 4.jpg.aes	AES Crypt Encrypted Data File	8 KB	13/02/2014 03:25 p.m.	330FA3E367766E83E4F0210D0875A808	B65DDAF4B6F03BA4A4A94E785FA2CA7283F16E	Yes	vwxyzabcD3	AES-256
Graphic Image Sample 5.jpg.aes	AES Crypt Encrypted Data File	17 KB	13/02/2014 03:25 p.m.	D86DFB82807D1B237523777EC5B737A1	A940416A3505AA2F60C151CAEC88EC08F6450772	Yes	efghijklM4	AES-256
Graphic Image Sample 6.jpg.aes	AES Crypt Encrypted Data File	58 KB	13/02/2014 03:26 p.m.	98A7DD3866483DF7259E7A25A10ACF3C	FBAB8332F0F4F8B8E5D28C8EACB77EE80912A39A8	Yes	nopqrstuV5	AES-256
Graphic Image Sample 7.JPG.aes	AES Crypt Encrypted Data File	2,001 KB	13/02/2014 03:26 p.m.	200F6B047832C4B63891F87EFAAD60A	133A610D08C0C09068854D0CF6625D51B5026905F	Yes	vwxyzabcE6	AES-256
Graphic Image Sample 8.JPG.aes	AES Crypt Encrypted Data File	2,063 KB	13/02/2014 03:26 p.m.	7E92DE2680841770A49EDD25431E08B8	C0C6AE5B80CD34DEFEB80E240F9A0B871E1C6C688	Yes	ghijklmnN7	AES-256
Graphic Image Sample 9.jpg.aes	AES Crypt Encrypted Data File	155 KB	13/02/2014 03:27 p.m.	058858E218AC08311C76E98271B8B48	3CD73088279055F0B7EBA157D5C5269FAFECAC9	Yes	opqrstuW8	AES-256
Graphic Image Sample 10.jpg.aes	AES Crypt Encrypted Data File	143 KB	13/02/2014 03:27 p.m.	621E9571D6848C05508AD1B7EAE7A8	7E052FC2FD167033837614E0B7F843B24F4F89A4B391	Yes	wxyzabcdeF9	AES-256
Graphic Image Sample 11.jpg.aes	AES Crypt Encrypted Data File	50 KB	13/02/2014 03:28 p.m.	FA2D595AC9BE2DF97B24F2F6887D4986	11016A41DC749AE51F8D3BA381A2F4F89A4B391	Yes	ghijklmnO1	AES-256
JPG Carved File Sample 1.PNG.aes	AES Crypt Encrypted Data File	4 KB	13/02/2014 03:28 p.m.	A0079238163E8EC9F8CEC68A3A17635	9C251158E6A0C1D47E6ACA7DC3673F3FC10CF9	Yes	pqrstuV2	AES-256
PDF Sample 1.pdf.aes	AES Crypt Encrypted Data File	12,466 KB	13/02/2014 03:29 p.m.	76198067F4CD7D48F45398134566EA4	74874E5AFAE93840613A481D8892E6585A7C0F80B	Yes	wxyzabcdeE3	AES-256
PDF Sample 2.pdf.aes	AES Crypt Encrypted Data File	78,432 KB	13/02/2014 03:30 p.m.	604B1B45B11400988A223CBA2811D12D	80780E05CF72032A697E46A8519498F2494DDCB	Yes	ghijklmnN4	AES-256
PDF Sample 3.pdf.aes	AES Crypt Encrypted Data File	25,897 KB	13/02/2014 03:30 p.m.	D893883FD0E0A051A04FDC896D38C1EB	332BD16ED24F819D5D8E853DAC960555C83F773A	Yes	opqrstuW5	AES-256
PDF Sample 4.pdf.aes	AES Crypt Encrypted Data File	20,379 KB	13/02/2014 03:31 p.m.	63BA757116C591245962C8C0C2A4D5A	CC38171630485E6816A45D13FC3E8833F263C1B	Yes	xyzabcdeF6	AES-256
PDF Sample 5.pdf.aes	AES Crypt Encrypted Data File	24,145 KB	13/02/2014 03:31 p.m.	0ED1D782870CA72F873A71946EE51F	5E1BA748A8F5A3CFB2767FE2AD89D99128DA600	Yes	ghijklmnO7	AES-256
Text Document Sample 1.txt.aes	AES Crypt Encrypted Data File	1 KB	13/02/2014 03:32 p.m.	C46616CF749CF7D0A2480251D00801D	C91F91BC3EBE316FF857D7D50E6356FF18197D2	Yes	pqrstuV8	AES-256
Text Document Sample 2.txt.aes	AES Crypt Encrypted Data File	1 KB	13/02/2014 03:32 p.m.	177F88208103369AFA0F70C89660CFF9	24C74C1641979753E0D6A44970732C318953EF10	Yes	uvwxyzabC9	AES-256
Text Document Sample 3.txt.aes	AES Crypt Encrypted Data File	1 KB	13/02/2014 03:33 p.m.	4946AC7F9940112F3AF48148004F07	30B635CEDE09A9F306282122D706F44695DEEB1	Yes	defghijkL1	AES-256
Text Document Sample 4.txt.aes	AES Crypt Encrypted Data File	1 KB	13/02/2014 03:33 p.m.	24564974AD1607715E1E59C3D3B6A82	78E359910940698C858D0A97257840F92858A716	Yes	mnopqrstU2	AES-256
Text Document Sample 5.txt.aes	AES Crypt Encrypted Data File	1 KB	13/02/2014 03:33 p.m.	FE3EC1D80D99A0A788E25D00CE7F1E6	FE4AC9A604C51248833543E22888952C062D7C60	Yes	wxyzabcD3	AES-256
Word Document Sample 1.doc.aes	AES Crypt Encrypted Data File	22 KB	13/02/2014 03:34 p.m.	600940D4BF157607298D284624432D0	7695755075C92E4AC2F0268E3174C0E53EED	Yes	efghijklM4	AES-256
Word Document Sample 2.doc.aes	AES Crypt Encrypted Data File	22 KB	13/02/2014 03:34 p.m.	8C26CE352A33889F88D4F179809505	A66DC2618AC09041D5C4509AD3289AD48F14364	Yes	nopqrstuV5	AES-256
Word Document Sample 3.doc.aes	AES Crypt Encrypted Data File	22 KB	13/02/2014 03:34 p.m.	1B7DCE84C475E1B19CADC04618A65C46	D81CF0E6739723FC3E544A5F21B161F7A0EC084	Yes	wxyzabcdeE6	AES-256
Word Document Sample 4.doc.aes	AES Crypt Encrypted Data File	22 KB	13/02/2014 03:35 p.m.	AF385C0A05DE95EBD0C21D382D11E88	291640737F1D44A2158B014A2D16E971AE34D30	Yes	ghijklmnO7	AES-256
Word Document Sample 5.doc.aes	AES Crypt Encrypted Data File	22 KB	13/02/2014 03:35 p.m.	EC191DF55D701B5A4ECC48381E27086F	251E1C5786DCC042CC06F39B030608D74769CC0A	Yes	pqrstuW8	AES-256

Appendix 5: Table of AESCrypt “Recovered Data” from Desktop

File Name	Type	Size	Timestamp	MD5 Value	SHA-1 Value	Successful Decryption	Secret Key	Algorithm
Encase File Sample 1.E01	Encase Evidence File	849,671 KB	13/02/2014 05:14 p.m.	5999BCEA0E97D45375F2808D144526	4EC0B8E57076FA5C23E07F05431EE0CF5AACAE09	Yes	abcdefghi1	AES-256
Encase File Sample 2.e01	Encase Evidence File	879,889 KB	13/02/2014 05:32 p.m.	372D0A28032238993E4197F12561DF80	401A423CCE09309B146CC0BF56B75E33C0D358F	Yes	klmnopqr2	AES-256
Encase File Sample 3.E01	Encase Evidence File	556 KB	13/02/2014 05:33 p.m.	01186A4A909373208279C8C8264C5023	B42AA4C0B1A2C76D6F6340761B0484574830B2EC	Yes	stuvwxyzA3	AES-256
Excel Sample File 1.xls	Microsoft Excel 97-2003 Worksheet	36 KB	13/02/2014 05:33 p.m.	2C938882A40CD51721B52B0FA1F3DDCF	A83BC97CA88C050A26A691780E57C808289B2680	Yes	bcdefghij4	AES-256
Excel Sample File 2.xls	Microsoft Excel 97-2003 Worksheet	148 KB	13/02/2014 05:33 p.m.	5637DFC46A639B7176E86A2017147FF	10A0A707D929954072E2F5FE4276F5D12E1844A	Yes	klmnopq55	AES-256
Excel Sample File 3.xls	Microsoft Excel 97-2003 Worksheet	69 KB	13/02/2014 05:34 p.m.	81A2A3D1F54A0C27658D0A529D1962E5	21C77ED4B640EAC6CE1705C4E37316808123BC4A	Yes	tuwxyzab6	AES-256
Excel Sample File 4.xls	Microsoft Excel 97-2003 Worksheet	189 KB	13/02/2014 05:34 p.m.	C2193F863A055364FCE86B1D352ED0E4	C0DFA95E168527960199098AE30773FF3080AC18	Yes	cdefghijk7	AES-256
Excel Sample File 5.xls	Microsoft Excel 97-2003 Worksheet	89 KB	13/02/2014 05:34 p.m.	045FDA78D8389EB21C71BF92AD92C802	1598FB060D3F7897B58CF0A782449D8259157167	Yes	lmnopqrst8	AES-256
Graphic Image Sample 1.jpg	JPG File	31 KB	13/02/2014 05:35 p.m.	9DD8B7408078168B78AEB4882C36D65A	4A973E2C6D04D68BFBD27C0A4CB4906EABD460C	Yes	uvwxyzabc9	AES-256
Graphic Image Sample 2.jpg	JPG File	16 KB	13/02/2014 05:35 p.m.	8CFB106804AC1017A741628751D376D0	C7228E068A1D9681C01844620A8AEC6F4C8269E	Yes	defghijkl1	AES-256
Graphic Image Sample 3.jpg	JPG File	10 KB	13/02/2014 05:35 p.m.	AA7AE2E36810DF98C0CD6E8CF696AC3	0F60F38CFE587A4D0FC096F80A867AF11D25581C	Yes	mnopqrstU2	AES-256
Graphic Image Sample 4.jpg	JPG File	8 KB	13/02/2014 05:36 p.m.	CC1538882B0FC873F980F51863484D5	31895FA91D7F533D00301BE79003588931F4FD48	Yes	vwxyzabcD3	AES-256
Graphic Image Sample 5.jpg	JPG File	17 KB	13/02/2014 05:36 p.m.	045FDA78D8389EB21C71BF92AD92C802	1598FB060D3F7897B58CF0A782449D8259157167	Yes	efghijklm4	AES-256
Graphic Image Sample 6.jpg	JPG File	57 KB	13/02/2014 05:36 p.m.	D2F1C6CA86E06FAA2DE402D7DAF2972	A3550E9285239F679CA15928458314D38AFC8D59	Yes	nopqrstuv5	AES-256
Graphic Image Sample 7.JPG	JPG File	2,001 KB	13/02/2014 05:37 p.m.	E9E08F7C8D5F3C1EAC4344A056648CC	0534321762701F94876F8C40B29D0CD1D385C55E	Yes	vwxyzabcde6	AES-256
Graphic Image Sample 8.JPG	JPG File	2,063 KB	13/02/2014 05:37 p.m.	FA50261640889197E2628686808F4332	9F558F95309239E4099DA97881A08A8573081DDC	Yes	ghijklmno7	AES-256
Graphic Image Sample 9.jpg	JPG File	155 KB	13/02/2014 05:37 p.m.	270657AAD13079248356C2E8761594CA	349A5344A085715A3F256C023485F98D8668745D	Yes	opqrstuvw8	AES-256
Graphic Image Sample 10.jpg	JPG File	143 KB	13/02/2014 05:37 p.m.	0685D1447E15A18A026F25853147B61	8E6F89D10554858E8F0D2AA54D578F02C57993A	Yes	wxyzabcdef9	AES-256
Graphic Image Sample 11.jpg	JPG File	50 KB	13/02/2014 05:38 p.m.	8223339567404E0E1664A43081786A05	FC829D3A74FE9E8879D8F59B303A3CAF87B2	Yes	ghijklmno1	AES-256
JPG Carved File Sample 1.PNG	PNG File	3 KB	13/02/2014 05:38 p.m.	09152D1688262C765382708C2641DF	AS9252A8A6EBD282F70A568831BC8259D2A775D03	Yes	pqrstuv2	AES-256
PDF Sample 1.pdf	Adobe Acrobat Document	12,466 KB	13/02/2014 05:38 p.m.	D51CEFF64D58F681093A00C81F510F4	70FEE205A8B6443641AA77E2A8D07BAADC39833F	Yes	vwxyzabcde3	AES-256
PDF Sample 2.pdf	Adobe Acrobat Document	78,432 KB	13/02/2014 05:39 p.m.	9810C0E41BFF7E0DC4BC196A5D4BC7	43109E07612E2CAC6ADC9A8688281136B8A548A9	Yes	efghijklmN4	AES-256
PDF Sample 3.pdf	Adobe Acrobat Document	25,897 KB	13/02/2014 05:40 p.m.	8707A8B772E5C7C81863D8A56EB579D5	F1725A9C766F78E17903385BDB086C352F9027A77	Yes	opqrstuvw5	AES-256
PDF Sample 4.pdf	Adobe Acrobat Document	20,379 KB	13/02/2014 05:40 p.m.	6E68EF9F1A8C6684538F54641F9045	D60ED70991389788200C38370A459131A6E5116D	Yes	xyzabcdef6	AES-256
PDF Sample 5.pdf	Adobe Acrobat Document	24,144 KB	13/02/2014 05:40 p.m.	F0FBC1D4077F2908EDC34AE189583DA	5160219A26487482D0EEFF85D0E99C08842E285D0F	Yes	ghijklmno7	AES-256
Text Document Sample 1.txt	Text Document	1 KB	13/02/2014 05:41 p.m.	B298248E1958A2EADCE5CE391710714F	FD40713ABFC61077A4E15ECC055A76A6E99916D	Yes	pqrstuv8	AES-256
Text Document Sample 2.txt	Text Document	1 KB	13/02/2014 05:41 p.m.	05CC0F79FA88248CE14FC3962E897	C48668250504E86D0E918A7985C30E80EFF496497	Yes	uvwxyzabc9	AES-256
Text Document Sample 3.txt	Text Document	1 KB	13/02/2014 05:42 p.m.	98737A8B9C24FE151ADC97720C687C54	7D1049242613314B744192D1E1A100779881668C	Yes	defghijkl1	AES-256
Text Document Sample 4.txt	Text Document	1 KB	13/02/2014 05:48 p.m.	834E59E13C02404FC1AE8B1BC72054F	8B15948E0D32F441E34D2C3ADE031475461C24DD	Yes	mnopqrstU2	AES-256
Text Document Sample 5.txt	Text Document	1 KB	13/02/2014 05:49 p.m.	F659230C7181038E3FDECA1E8318EA20	3DC794104C0C69797FA69DFAE2A20DC8F26AE0	Yes	vwxyzabcD3	AES-256
Word Document Sample 1.doc	Microsoft 97-2003 Document	22 KB	13/02/2014 05:50 p.m.	26388348D0CD58738E2AD2B4460F38	8293FC6A29F73799E12AF6742D584D307C5298	Yes	efghijklm4	AES-256
Word Document Sample 2.doc	Microsoft 97-2003 Document	22 KB	13/02/2014 05:50 p.m.	880288FA773B443C3E31820D842A2D	BDA44AF4C8791C204E4A8F127B87848A57B1AD91	Yes	nopqrstuv5	AES-256
Word Document Sample 3.doc	Microsoft 97-2003 Document	22 KB	13/02/2014 05:50 p.m.	C688978791B45A4F97486D03C77F771	CFB870AC35086593744E6D13545512AD9095DAE1	Yes	wxyzabcde6	AES-256
Word Document Sample 4.doc	Microsoft 97-2003 Document	22 KB	13/02/2014 05:50 p.m.	C381FA40CCFBC1873879E7F37A0E07	8705FDDA0D773DCA0654BC09CB1B0E7A3F8D881C	Yes	efghijklmO7	AES-256
Word Document Sample 5.doc	Microsoft 97-2003 Document	22 KB	13/02/2014 05:50 p.m.	A0B513677FA881223145C7FE0C4C0A0D	7C39F7254E5D28887D08A17F451A61F80C1E547	Yes	pqrstuvw8	AES-256

Appendix 6: Screenshot of AxCrypt “Encrypted Data” on Desktop

Documents library AxCrypt Encryption Data Files				
Name	Date modified	Type	Size	
 Encase File Sample 1-Ex01	13/02/2014 6:59 p.m.	AxCrypt Encrypted File	849,672 KB	
 Encase File Sample 2-ex01	13/02/2014 7:00 p.m.	AxCrypt Encrypted File	879,890 KB	
 Encase File Sample 3-E01	13/02/2014 7:00 p.m.	AxCrypt Encrypted File	556 KB	
 Excel Sample File 1-xls	13/02/2014 7:01 p.m.	AxCrypt Encrypted File	9 KB	
 Excel Sample File 2-xls	13/02/2014 7:01 p.m.	AxCrypt Encrypted File	32 KB	
 Excel Sample File 3-xls	13/02/2014 7:02 p.m.	AxCrypt Encrypted File	20 KB	
 Excel Sample File 4-xls	13/02/2014 7:02 p.m.	AxCrypt Encrypted File	29 KB	
 Excel Sample File 5-xls	13/02/2014 7:02 p.m.	AxCrypt Encrypted File	17 KB	
 Graphic Image Sample 1-jpg	13/02/2014 7:03 p.m.	AxCrypt Encrypted File	19 KB	
 Graphic Image Sample 2-jpg	13/02/2014 7:03 p.m.	AxCrypt Encrypted File	17 KB	
 Graphic Image Sample 3-jpg	13/02/2014 7:03 p.m.	AxCrypt Encrypted File	10 KB	
 Graphic Image Sample 4-jpg	13/02/2014 7:04 p.m.	AxCrypt Encrypted File	8 KB	
 Graphic Image Sample 5-jpg	13/02/2014 7:04 p.m.	AxCrypt Encrypted File	17 KB	
 Graphic Image Sample 6-jpg	13/02/2014 7:04 p.m.	AxCrypt Encrypted File	58 KB	
 Graphic Image Sample 7-JPG	13/02/2014 7:05 p.m.	AxCrypt Encrypted File	2,001 KB	
 Graphic Image Sample 8-JPG	13/02/2014 7:05 p.m.	AxCrypt Encrypted File	2,063 KB	
 Graphic Image Sample 9-jpg	13/02/2014 7:05 p.m.	AxCrypt Encrypted File	155 KB	
 Graphic Image Sample 10-jpg	13/02/2014 7:06 p.m.	AxCrypt Encrypted File	143 KB	
 Graphic Image Sample 11-jpg	13/02/2014 7:06 p.m.	AxCrypt Encrypted File	50 KB	
 JPG Carved File Sample 1-PNG	13/02/2014 7:06 p.m.	AxCrypt Encrypted File	4 KB	
 PDF Sample 1-pdf	13/02/2014 7:49 p.m.	AxCrypt Encrypted File	12,466 KB	
 PDF Sample 2-pdf	13/02/2014 7:50 p.m.	AxCrypt Encrypted File	68,437 KB	
 PDF Sample 3-pdf	13/02/2014 7:50 p.m.	AxCrypt Encrypted File	25,897 KB	
 PDF Sample 4-pdf	13/02/2014 7:51 p.m.	AxCrypt Encrypted File	20,379 KB	
 PDF Sample 5-pdf	13/02/2014 7:51 p.m.	AxCrypt Encrypted File	24,145 KB	
 Text Document Sample 1-txt	13/02/2014 7:08 p.m.	AxCrypt Encrypted File	1 KB	
 Text Document Sample 2-txt	13/02/2014 7:08 p.m.	AxCrypt Encrypted File	1 KB	
 Text Document Sample 3-txt	13/02/2014 7:08 p.m.	AxCrypt Encrypted File	1 KB	

Documents library				
AxCrypt Encryption Data Files				
Name	Date modified	Type	Size	
 Excel Sample File 5-xls	13/02/2014 7:02 p.m.	AxCrypt Encrypted File	17 KB	
 Graphic Image Sample 1-jpg	13/02/2014 7:03 p.m.	AxCrypt Encrypted File	19 KB	
 Graphic Image Sample 2-jpg	13/02/2014 7:03 p.m.	AxCrypt Encrypted File	17 KB	
 Graphic Image Sample 3-jpg	13/02/2014 7:03 p.m.	AxCrypt Encrypted File	10 KB	
 Graphic Image Sample 4-jpg	13/02/2014 7:04 p.m.	AxCrypt Encrypted File	8 KB	
 Graphic Image Sample 5-jpg	13/02/2014 7:04 p.m.	AxCrypt Encrypted File	17 KB	
 Graphic Image Sample 6-jpg	13/02/2014 7:04 p.m.	AxCrypt Encrypted File	58 KB	
 Graphic Image Sample 7-JPG	13/02/2014 7:05 p.m.	AxCrypt Encrypted File	2,001 KB	
 Graphic Image Sample 8-JPG	13/02/2014 7:05 p.m.	AxCrypt Encrypted File	2,063 KB	
 Graphic Image Sample 9-jpg	13/02/2014 7:05 p.m.	AxCrypt Encrypted File	155 KB	
 Graphic Image Sample 10-jpg	13/02/2014 7:06 p.m.	AxCrypt Encrypted File	143 KB	
 Graphic Image Sample 11-jpg	13/02/2014 7:06 p.m.	AxCrypt Encrypted File	50 KB	
 JPG Carved File Sample 1-PNG	13/02/2014 7:06 p.m.	AxCrypt Encrypted File	4 KB	
 PDF Sample 1-pdf	13/02/2014 7:49 p.m.	AxCrypt Encrypted File	12,466 KB	
 PDF Sample 2-pdf	13/02/2014 7:50 p.m.	AxCrypt Encrypted File	68,437 KB	
 PDF Sample 3-pdf	13/02/2014 7:50 p.m.	AxCrypt Encrypted File	25,897 KB	
 PDF Sample 4-pdf	13/02/2014 7:51 p.m.	AxCrypt Encrypted File	20,379 KB	
 PDF Sample 5-pdf	13/02/2014 7:51 p.m.	AxCrypt Encrypted File	24,145 KB	
 Text Document Sample 1-txt	13/02/2014 7:08 p.m.	AxCrypt Encrypted File	1 KB	
 Text Document Sample 2-txt	13/02/2014 7:08 p.m.	AxCrypt Encrypted File	1 KB	
Text Document Sample 3-txt	13/02/2014 7:08 p.m.	AxCrypt Encrypted File	1 KB	
Text Document Sample 4-txt	13/02/2014 7:09 p.m.	AxCrypt Encrypted File	1 KB	
Text Document Sample 5-txt	13/02/2014 7:09 p.m.	AxCrypt Encrypted File	1 KB	
Word Document Sample 1-doc	13/02/2014 7:10 p.m.	AxCrypt Encrypted File	6 KB	
Word Document Sample 2-doc	13/02/2014 7:10 p.m.	AxCrypt Encrypted File	6 KB	
Word Document Sample 3-doc	13/02/2014 7:10 p.m.	AxCrypt Encrypted File	6 KB	
Word Document Sample 4-doc	13/02/2014 7:10 p.m.	AxCrypt Encrypted File	6 KB	
Word Document Sample 5-doc	13/02/2014 7:11 p.m.	AxCrypt Encrypted File	6 KB	

Appendix 7: Table of AxCrypt “Encrypted Data” on Desktop

File Name	Type	Size	Timestamp	MD5 Value	SHA-1 Value	Successful Decryption	Secret Key	Algorithm
Erase File Sample 1-Ex01.axx	AxCrypt Encrypted File	849,672 KB	13/02/2014 06:59 p.m.	E66461D4805E2F31DD060675FD2841E9	AA2D084705908666C2DC047FA01B4C5DCA1815A4	Yes	abcdefgh1	AES-128
Erase File Sample 2-ex01.axx	AxCrypt Encrypted File	879,890 KB	13/02/2014 07:00 p.m.	B1003F33735C9F978831C7FE05E06D5350	0FA1F43D454C5CF2C8C596306138E80CC38C10	Yes	ijklmnopR2	AES-128
Erase File Sample 3-Ex01.axx	AxCrypt Encrypted File	556 KB	13/02/2014 07:00 p.m.	5D04D4D360DEA077277EFC05E40AA2E0F	7C16E8999FEB0041B04D12238283193C58083039	Yes	stuvwxyzA3	AES-128
Excel Sample File 1-xls.axx	AxCrypt Encrypted File	9 KB	13/02/2014 07:01 p.m.	C65C2736963FAF9A0DC08F2CAE0B3C4F5	57A2A538BE04E488315C3EB6806CA805F5D89506	Yes	bcdefghu4	AES-128
Excel Sample File 2-xls.axx	AxCrypt Encrypted File	32 KB	13/02/2014 07:01 p.m.	66130ED3A0908E59DFBFCB2C6F292ADC	A693E40C7D2407F8871988FFA8F67934FE5F83D0	Yes	klmnopqrs5	AES-128
Excel Sample File 3-xls.axx	AxCrypt Encrypted File	20 KB	13/02/2014 07:02 p.m.	5606346700F31986E5A08385ED54802F	D2FF481D9C0E493434D8C6C49FF4582C8888AC6	Yes	tuvwxyzab6	AES-128
Excel Sample File 4-xls.axx	AxCrypt Encrypted File	29 KB	13/02/2014 07:02 p.m.	EE0B9A1900846E1D3E0B817E1C205014	5009927550FF823EDC1CB3573FAFA1918D9363AC	Yes	cdefghijk7	AES-128
Excel Sample File 5-xls.axx	AxCrypt Encrypted File	17 KB	13/02/2014 07:02 p.m.	A8C4D7AE1F8126678380666399146366	F23404126AFF9B58E1A1DE3F78CDA3307AD63439	Yes	lmnopqrst8	AES-128
Graphic Image Sample 1-jpg.axx	AxCrypt Encrypted File	19 KB	13/02/2014 07:03 p.m.	6C84D9B14E33FF72D7AAD868D48F676C	C1678CA897E1359A8414D8BDE5E82A8D6C19B33C	Yes	uvwxyzabc9	AES-128
Graphic Image Sample 2-jpg.axx	AxCrypt Encrypted File	17 KB	13/02/2014 07:03 p.m.	7165530F346708FE79856505EEF712A8	81107D1DFFDEA59F7B12ACFC83087D0C49E853B	Yes	defghijkl1	AES-128
Graphic Image Sample 3-jpg.axx	AxCrypt Encrypted File	10 KB	13/02/2014 07:03 p.m.	9131988A562E8381856D8049035E3513	2AC4F8E37699754F370C47C86300C5A9F2FE48	Yes	mnoqrstui2	AES-128
Graphic Image Sample 4-jpg.axx	AxCrypt Encrypted File	8 KB	13/02/2014 07:04 p.m.	3F0F4E90FE56313FC45FD1B242C3034A	75EBED4DC3537FA2314E3FC517626DC42D34878	Yes	vwxyzabcD3	AES-128
Graphic Image Sample 5-jpg.axx	AxCrypt Encrypted File	17 KB	13/02/2014 07:04 p.m.	306F8A7B4597DC449A428E2995FEA950	D820BA4EA36B56CF04687F1F287C862D8316315F8	Yes	efghijklM4	AES-128
Graphic Image Sample 6-jpg.axx	AxCrypt Encrypted File	58 KB	13/02/2014 07:04 p.m.	569A61D966FD88E42E0E22AFC6DCE6A6A	4A41F28A51A42CB88CF9481D8585A36FA88AEC5	Yes	nopqrstuV5	AES-128
Graphic Image Sample 7-jpg.axx	AxCrypt Encrypted File	2,001 KB	13/02/2014 07:05 p.m.	34F08FDA5250F135D70A511681B0366C	53201208588E80A4625FB5C73FD9659758A0D885	Yes	wyzabcde6	AES-128
Graphic Image Sample 8-jpg.axx	AxCrypt Encrypted File	2,063 KB	13/02/2014 07:05 p.m.	EDF98C380D5197888F910508C9986F	24D8FD388C55A998990209A1E200FE5D441484F	Yes	fghijklmN7	AES-128
Graphic Image Sample 9-jpg.axx	AxCrypt Encrypted File	155 KB	13/02/2014 07:05 p.m.	A8F753046143441CC26A22968F73C6C7	B886337390180CFF7FEC9CA2C9A0A4F046927E3	Yes	opqrstuVW8	AES-128
Graphic Image Sample 10-jpg.axx	AxCrypt Encrypted File	143 KB	13/02/2014 07:06 p.m.	047A8AF66FD6410E31EEF043C6FC695	F5F5B08E779C1D94E47C4D133E58D9D200D5D4C	Yes	wyzabcdeF9	AES-128
Graphic Image Sample 11-jpg.axx	AxCrypt Encrypted File	50 KB	13/02/2014 07:06 p.m.	C5DD0D6C3F71A870E2830C28808F54AFC	076AA5A2E2D617018F9EB8FC28319C37DE804742	Yes	ghijklmnO1	AES-128
JPG Canned File Sample 1-PNG.axx	AxCrypt Encrypted File	4 KB	13/02/2014 07:06 p.m.	EC62EC8849175C5C4D9A54007R2B2606	F6C9C9C1G3457DA02938124A98C5028A8D575B1A	Yes	pqrstuV2	AES-128
PDF Sample 1-pdf.axx	AxCrypt Encrypted File	12,466 KB	13/02/2014 07:49 p.m.	68C5F8229EFAA0609AACFCAE669D35B	2361F2036FE741E6F30D8A568940809451B0857C	Yes	wyzabcdeE3	AES-128
PDF Sample 2-pdf.axx	AxCrypt Encrypted File	68,437 KB	13/02/2014 07:50 p.m.	8D0F51C3D0221A47C46712210646066	EDE5B780EA36AE4DC465A5D2806A0D0F42793883A	Yes	fghijklmN4	AES-128
PDF Sample 3-pdf.axx	AxCrypt Encrypted File	25,897 KB	13/02/2014 07:50 p.m.	4F5E98A2D6ED1A88A59A94AF0BFC9724	B4194AC96C275E82B866263F1AD6A7E7F6C5ADA1	Yes	opqrstuVW5	AES-128
PDF Sample 4-pdf.axx	AxCrypt Encrypted File	20,379 KB	13/02/2014 07:51 p.m.	399068439918C6C6A1C5D0D8082056358	7D91466FA98D7B1FC10D9F9A58950D8F9A28BE1	Yes	xyzabcdeF6	AES-128
PDF Sample 5-pdf.axx	AxCrypt Encrypted File	24,145 KB	13/02/2014 07:51 p.m.	C836F8A33EAE7A0686DFC99628EEF1BF	0A2408D5F1557E083D896DA3D5E7F089207D596	Yes	ghijklmnO7	AES-128
Text Document Sample 1-txt.axx	AxCrypt Encrypted File	1 KB	13/02/2014 07:08 p.m.	4F081272B5D0DADF8F698E6981879870	44E651252585E59095516AF42689DAAD284571788	Yes	pqrstuV8	AES-128
Text Document Sample 2-txt.axx	AxCrypt Encrypted File	1 KB	13/02/2014 07:08 p.m.	2B64ED74822789AECF811E05C87F8A48	78D62C59246A341E7E7FE69E9C8287F56A3649F	Yes	uvwxyzabc9	AES-128
Text Document Sample 3-txt.axx	AxCrypt Encrypted File	1 KB	13/02/2014 07:08 p.m.	BF09A6A2E60F305D9222B5A595978303	C979884C3FC17082EAD3A98D173C4E715E4572FF	Yes	defghijkL1	AES-128
Text Document Sample 4-txt.axx	AxCrypt Encrypted File	1 KB	13/02/2014 07:09 p.m.	3F0F4E90FE56313FC45FD1B242C3034A	75EBED4DC3537FA2314E3FC517626DC42D34878	Yes	mnoqrstui2	AES-128
Text Document Sample 5-txt.axx	AxCrypt Encrypted File	1 KB	13/02/2014 07:09 p.m.	B3809C366E815897D8C4B861880B08380D	1A792FF7F64A91B71E167E828F3CD5844F20CF16E	Yes	wyzabcD3	AES-128
Word Document Sample 1-doc.axx	AxCrypt Encrypted File	6 KB	13/02/2014 07:10 p.m.	64AD950330A02EA09990FB135220C910	A76F17E91AF19D57A61CF388C091D683FF5FE699	Yes	efghijklM4	AES-128
Word Document Sample 2-doc.axx	AxCrypt Encrypted File	6 KB	13/02/2014 07:10 p.m.	71A9D5948155A97880D77A8807F40B8CA	CA1619C935A3A54558FB279E455EEF4D6216FC41D	Yes	nopqrstuV5	AES-128
Word Document Sample 3-doc.axx	AxCrypt Encrypted File	6 KB	13/02/2014 07:10 p.m.	0695DDF32D989606453D0C30808E7B3F	08B8D7D7580ED067499AFAE41997A8BFD7452D6FB	Yes	wyzabcdeE6	AES-128
Word Document Sample 4-doc.axx	AxCrypt Encrypted File	6 KB	13/02/2014 07:10 p.m.	4377772E6E7752037179F99423CE91B	98C8F6B856A3751D88941AADC9CA006D0404	Yes	fghijklmnO7	AES-128
Word Document Sample 5-doc.axx	AxCrypt Encrypted File	6 KB	13/02/2014 07:11 p.m.	D0624D0C2C1F8973C44B48D7F891E56	C63F7699C8676DE0880FF8C4A00AA45CCF5A31F	Yes	pqrstuVW8	AES-128

Appendix 8: Table of AxCrypt “Recovered Data” from Desktop

File Name	Type	Size	Timestamp	MD5 Value	SHA-1 Value	Successful Decryption	Secret Key
Encase File Sample 1.Ex01	Encase Evidence File	849,671 KB	29/06/2011 10:29 a.m.	59998CEA0E97DA53375F2088FD14526	4EC9BE57076FA5EC23E07F05A31EFC0F5AACAE9D	Yes	abcdeghl1
Encase File Sample 2.ex01	Encase Evidence File	879,889 KB	28/11/2012 03:06 p.m.	372D42D80233289893E4187F12561DFB0	401A423CED930B9A146CC0BF56B7E33C0D358F	Yes	klmnopqr2
Encase File Sample 3.E01	Encase Evidence File	556 KB	04/04/2013 08:48 p.m.	01186AA4C9D92720879C9C82645C023	B42A44ACDB1A2C876D0F6340761BD484574830B2EC	Yes	stuvwxyzA3
Excel Sample File 1.xls	Microsoft Excel 97-2003 Worksheet	36 KB	16/05/2013 08:41 a.m.	2C938882A40C51721B5280FA1F30DCF	A838C97CA88CD50426A69178D557C808289B2680	Yes	bodeghil4
Excel Sample File 2.xls	Microsoft Excel 97-2003 Worksheet	148 KB	17/06/2005 11:38 a.m.	5637DFC46A639B7176EB66A2017147FF	10A0A707D929954072E2F5FE42765D12E184AA	Yes	klmnopqS5
Excel Sample File 3.xls	Microsoft Excel 97-2003 Worksheet	69 KB	17/06/2005 11:39 a.m.	B1A2A3D1F54A0C27658D0A529D1962E5	21C77EDC4B640C46CE1705C34E3168D81238CA4	Yes	tuwxyzab6
Excel Sample File 4.xls	Microsoft Excel 97-2003 Worksheet	189 KB	17/06/2005 11:40 a.m.	C2193FB63A055364FCF8681D352EDD64	CDEF495E168527960199D9B4E30773FF3080AC18	Yes	cdefghijk7
Excel Sample File 5.xls	Microsoft Excel 97-2003 Worksheet	89 KB	17/06/2005 11:41 a.m.	0A5FDA78D8389EB21C718F92A092C8D2	1598FB06D3F78987B5BCFA7B2449D8259157167	Yes	lmnopqrst8
Graphic Image Sample 1.jpg	JPG File	31 KB	08/02/2008 03:44 p.m.	9DD874080781688787AEB4882C36D65A	44973E2C6D04D68FB8D27C0A4CB490EABD460C	Yes	uvwxyzabc9
Graphic Image Sample 2.jpg	JPG File	16 KB	22/04/2014 11:12 a.m.	8CFB10680A4C1017A741628751D376D0	C7228E06BA1D9681C01844620A8AECDFAC8269E	Yes	defghijkl1
Graphic Image Sample 3.jpg	JPG File	10 KB	22/04/2014 11:13 a.m.	A474E2E36810DF98C0CDE68CF696AC3	0F60F38CFE587A4DFC96F8D867AF11D25581C	Yes	mnoqrstU2
Graphic Image Sample 4.jpg	JPG File	8 KB	22/04/2014 11:13 a.m.	CC1538882B0FC737980FD51B63484D5	31895FA91D7E353D0D3018E7900538891F4FDBA8	Yes	vwxyzabcD3
Graphic Image Sample 5.jpg	JPG File	17 KB	22/04/2014 11:14 a.m.	0A5FDA78D8389EB21C718F92A092C8D2	1598FB06D3F78987B5BCFA7B2449D8259157167	Yes	efghijklM4
Graphic Image Sample 6.jpg	JPG File	57 KB	12/07/2005 01:14 a.m.	D2F1C6CA86E06FAA2DEA02D7DAF2972	A3550E9285239F679CA1592845B314D3BAFC8D59	Yes	noqrstuv5
Graphic Image Sample 7.JPG	JPG File	2,001 KB	03/09/2009 12:20 p.m.	E9F03E7C8DDE33C1EAC4344AD566F48CC	0534321762701F94876FBCAC0829DCD1D385C55E	Yes	wxyzabcde6
Graphic Image Sample 8.JPG	JPG File	2,063 KB	18/03/2009 09:06 a.m.	FAS0261640889197E262B696D8F4332	9F55BF953D9239E4099D9A97881A084B573081DDC	Yes	fgghijklmN7
Graphic Image Sample 9.jpg	JPG File	155 KB	10/04/2010 12:08 p.m.	270657A4D13079248356C2E876E594CA	349A534440B5715A3F256C0234B5F9D08668745D	Yes	opqrstuvw8
Graphic Image Sample 10.jpg	JPG File	143 KB	15/05/2012 03:43 p.m.	0685D1447E15A18A026EF25B53147861	8E65F89D10554858E5FD02AA54D78FD2C57993A	Yes	wyzabcdef9
Graphic Image Sample 11.jpg	JPG File	50 KB	21/11/1999 04:48 p.m.	8223359567404E0E16644430B1786A05	FC829D3A74FE9E8879D85FE983034A3C04FB782	Yes	ghijklmnO1
JPG Carved File Sample 1.PNG	PNG File	3 KB	09/05/2012 04:53 p.m.	091523D16882626C765387708C2641DF	A5925A8AE8D282F70A568318CB259D2A775D0D3	Yes	pqrstuv2
PDF Sample 1.pdf	Adobe Acrobat Document	12,466 KB	07/05/2011 02:15 p.m.	D51CF6F4D58F681093A00C81F510F4	70FEE205AB86443641AA77E2A8D07BAA0C39853F	Yes	wxyzabcde3
PDF Sample 2.pdf	Adobe Acrobat Document	78,432 KB	07/05/2011 02:28 p.m.	9810CF0E41BF7E0DC48CC196A5D48C7	43109E07612EAC6AD9AA8688281136B48548A9	Yes	fgghijklmN4
PDF Sample 3.pdf	Adobe Acrobat Document	25,897 KB	07/05/2011 02:17 p.m.	8707AB8772E5C7C81863D8A56E8579D5	F1725A9C766F78E179033858D06C352F9027A77	Yes	opqrstuvw5
PDF Sample 4.pdf	Adobe Acrobat Document	20,379 KB	07/05/2011 01:11 p.m.	6E6F8EF9F1ABC66841538F54641F9045	D6DED70991389788200C3B370A459131A6E5116D	Yes	xyzabcdef6
PDF Sample 5.pdf	Adobe Acrobat Document	24,144 KB	07/05/2011 01:11 p.m.	F0FBC1DA0477F2908EDC34AE189583DA	5160219A26487482DEF85DE969C08842E285D0F	Yes	ghijklmnO7
Text Document Sample 1.txt	Text Document	1 KB	22/04/2014 11:58 a.m.	B298224BE195B42EAD0C5EE391170714F	FD4D713ABFC610F724EA15FC055A786A6E9596D	Yes	pqrstuv8
Text Document Sample 2.txt	Text Document	1 KB	22/04/2014 11:59 a.m.	05C0E7F9F3A8824BCE14FC39062E897	C4B96B25050AEB6D938A79B5C30E0DFF1496497	Yes	uvwxyzabc9
Text Document Sample 3.txt	Text Document	1 KB	22/04/2014 11:59 a.m.	98737A8B9C24FE151A0C97720C687C54	7D1049242613314874419D1EA100779881668C	Yes	defghijkl1
Text Document Sample 4.txt	Text Document	1 KB	22/04/2014 12:00 p.m.	834E5BE13C0240D4FAEB8B1BC672054F	8815948E0032F441E34D02C3A0E031475461C24DD	Yes	mnoqrstU2
Text Document Sample 5.txt	Text Document	1 KB	22/04/2014 12:01 p.m.	F85B250C718103BE3FDECA1E8318EA20	30CC794104C0CC69797F69DDE1A2E20C8F26AE0	Yes	wxyzabcD3
Word Document Sample 1.doc	Microsoft 97-2003 Document	22 KB	22/04/2014 11:53 a.m.	26388348D00C58F738E2A02BF4460F38	8293FC6A29F737939F12AF667420584D307C5298	Yes	efghijklM4
Word Document Sample 2.doc	Microsoft 97-2003 Document	22 KB	22/04/2014 11:53 a.m.	880288FA7E3B4443C3E18210084242D	8DAAA4FC8791C204E48F127B8748457B1AD91	Yes	noqrstuv5
Word Document Sample 3.doc	Microsoft 97-2003 Document	22 KB	22/04/2014 11:53 a.m.	C8699F8791B45A4F97466DD3C77F771	CF870AC35086593F4E6D13545512409095DAE1	Yes	wxyzabcde6
Word Document Sample 4.doc	Microsoft 97-2003 Document	22 KB	22/04/2014 11:54 a.m.	C381FA0CCFBC1E873879E7F327A0E07	8705FDDA0D773DC40E548CB9C1BD7E7AF8D8B1C	Yes	fgghijklmnO7
Word Document Sample 5.doc	Microsoft 97-2003 Document	22 KB	22/04/2014 12:02 p.m.	ADB136F7FA8B122345C7FED0ADC0AD	7C33F7254EE5D28887E0BA17451A61F80C1E547	Yes	pqrstuvw8

Appendix 9: Screenshot of AESTool “Encrypted Data” on Desktop

Documents library AESTool Encryption Data Files				
Name	Date modified	Type	Size	
AES Encase File Sample 1	13/02/2014 11:29 p.m.	Application	850,013 KB	
AES Encase File Sample 2	13/02/2014 11:35 p.m.	Application	880,231 KB	
AES Encase File Sample 3	13/02/2014 11:35 p.m.	Application	898 KB	
AES Excel Sample File 1	13/02/2014 11:35 p.m.	Application	378 KB	
AES Excel Sample File 2	13/02/2014 11:36 p.m.	Application	490 KB	
AES Excel Sample File 3	13/02/2014 11:36 p.m.	Application	411 KB	
AES Excel Sample File 4	13/02/2014 11:37 p.m.	Application	531 KB	
AES Excel Sample File 5	13/02/2014 11:37 p.m.	Application	431 KB	
AES Graphic Image Sample 1	13/02/2014 11:37 p.m.	Application	373 KB	
AES Graphic Image Sample 2	13/02/2014 11:38 p.m.	Application	358 KB	
AES Graphic Image Sample 3	13/02/2014 11:38 p.m.	Application	351 KB	
AES Graphic Image Sample 4	13/02/2014 11:38 p.m.	Application	349 KB	
AES Graphic Image Sample 5	13/02/2014 11:39 p.m.	Application	358 KB	
AES Graphic Image Sample 6	13/02/2014 11:39 p.m.	Application	399 KB	
AES Graphic Image Sample 7	13/02/2014 11:39 p.m.	Application	2,342 KB	
AES Graphic Image Sample 8	13/02/2014 11:39 p.m.	Application	2,404 KB	
AES Graphic Image Sample 9	13/02/2014 11:40 p.m.	Application	497 KB	
AES Graphic Image Sample 10	13/02/2014 11:40 p.m.	Application	485 KB	
AES Graphic Image Sample 11	13/02/2014 11:40 p.m.	Application	391 KB	
AES JPG Carved File Sample 1	13/02/2014 11:41 p.m.	Application	345 KB	
AES PDF Sample 1	13/02/2014 11:41 p.m.	Application	12,808 KB	
AES PDF Sample 2	13/02/2014 11:41 p.m.	Application	78,773 KB	
AES PDF Sample 3	13/02/2014 11:41 p.m.	Application	26,238 KB	
AES PDF Sample 4	13/02/2014 11:42 p.m.	Application	20,720 KB	
AES PDF Sample 5	13/02/2014 11:42 p.m.	Application	24,486 KB	
AES Text Document Sample 1	13/02/2014 11:42 p.m.	Application	342 KB	
AES Text Document Sample 2	13/02/2014 11:43 p.m.	Application	342 KB	
AES Text Document Sample 3	13/02/2014 11:43 p.m.	Application	342 KB	

Documents library				
AESTool Encryption Data Files				
Name	Date modified	Type	Size	
AES Excel Sample File 5	13/02/2014 11:37 p.m.	Application	431 KB	
AES Graphic Image Sample 1	13/02/2014 11:37 p.m.	Application	373 KB	
AES Graphic Image Sample 2	13/02/2014 11:38 p.m.	Application	358 KB	
AES Graphic Image Sample 3	13/02/2014 11:38 p.m.	Application	351 KB	
AES Graphic Image Sample 4	13/02/2014 11:38 p.m.	Application	349 KB	
AES Graphic Image Sample 5	13/02/2014 11:39 p.m.	Application	358 KB	
AES Graphic Image Sample 6	13/02/2014 11:39 p.m.	Application	399 KB	
AES Graphic Image Sample 7	13/02/2014 11:39 p.m.	Application	2,342 KB	
AES Graphic Image Sample 8	13/02/2014 11:39 p.m.	Application	2,404 KB	
AES Graphic Image Sample 9	13/02/2014 11:40 p.m.	Application	497 KB	
AES Graphic Image Sample 10	13/02/2014 11:40 p.m.	Application	485 KB	
AES Graphic Image Sample 11	13/02/2014 11:40 p.m.	Application	391 KB	
AES JPG Carved File Sample 1	13/02/2014 11:41 p.m.	Application	345 KB	
AES PDF Sample 1	13/02/2014 11:41 p.m.	Application	12,808 KB	
AES PDF Sample 2	13/02/2014 11:41 p.m.	Application	78,773 KB	
AES PDF Sample 3	13/02/2014 11:41 p.m.	Application	26,238 KB	
AES PDF Sample 4	13/02/2014 11:42 p.m.	Application	20,720 KB	
AES PDF Sample 5	13/02/2014 11:42 p.m.	Application	24,486 KB	
AES Text Document Sample 1	13/02/2014 11:42 p.m.	Application	342 KB	
AES Text Document Sample 2	13/02/2014 11:43 p.m.	Application	342 KB	
AES Text Document Sample 3	13/02/2014 11:43 p.m.	Application	342 KB	
AES Text Document Sample 4	13/02/2014 11:43 p.m.	Application	342 KB	
AES Text Document Sample 5	13/02/2014 11:43 p.m.	Application	342 KB	
AES Word Document Sample 1	13/02/2014 11:43 p.m.	Application	364 KB	
AES Word Document Sample 2	13/02/2014 11:44 p.m.	Application	364 KB	
AES Word Document Sample 3	13/02/2014 11:44 p.m.	Application	364 KB	
AES Word Document Sample 4	13/02/2014 11:44 p.m.	Application	364 KB	
AES Word Document Sample 5	13/02/2014 11:44 p.m.	Application	364 KB	

Appendix 10: Table of AESTool “Encrypted Data” on Desktop

File Name	Type	Size	Timestamp	MD5 Value	SHA-1 Value	Successful Encryption	Secret Key	Algorithm
Encase File Sample 1.exe	Application	850,013 KB	13/02/2014 11:29 p.m.	A1F96B13E979168E3019F7C722560253	AB42310D7B71F6EA54A8FE3E735C032798D95EE	Yes	ABCDEF1	AES-64
Encase File Sample 2.exe	Application	880,231 KB	13/02/2014 11:35 p.m.	996B9B8D3A2FBOACEA1FEF51828581B80	9552D0A98C9C5437E8AFB680CC621BFC93667D	Yes	ABCDEF1	AES-64
Encase File Sample 3.exe	Application	898 KB	13/02/2014 11:35 p.m.	014212168F51089F421D4E691F78124E	8533A84B7231F0C3C76904CFB9C6014B21C6DFB7	Yes	ABCDEF1	AES-64
Excel Sample File 1.exe	Application	378 KB	13/02/2014 11:35 p.m.	00CF104B7F44186BDC090F6F1BE1D54	7CC3D2112D0D317837D578E16AC75C170A9F2178	Yes	ABCDEF1	AES-64
Excel Sample File 2.exe	Application	490 KB	13/02/2014 11:36 p.m.	AAE560C7AD0EED45A0D7B21807973C2550	7B0077169D98A222718269366EF57A36976E1D	Yes	ABCDEF1	AES-64
Excel Sample File 3.exe	Application	411 KB	13/02/2014 11:36 p.m.	BF307088D01E5F56613B5202DA513317	AA96B788555F1732E25899F450328B16F415693	Yes	ABCDEF1	AES-64
Excel Sample File 4.exe	Application	531 KB	13/02/2014 11:37 p.m.	25ED898FE891E958CF3E22FFD51DF4E4	8C548D87BF8C8C545382C1F3B8A3307339FAA9D	Yes	ABCDEF1	AES-64
Excel Sample File 5.exe	Application	431 KB	13/02/2014 11:37 p.m.	508B45D5C913A78191921FCDAAFAA08	D3A4E0F78F8FFD1240D87A9C7FA99CDB053E17FE	Yes	ABCDEF1	AES-64
Graphic Image Sample 1.exe	Application	373 KB	13/02/2014 11:37 p.m.	C8E4C0328100B8186F926D9F1E439A03	9D61DF08F66E02F3EC9433807AAC5967015EE2E	Yes	ABCDEF1	AES-64
Graphic Image Sample 2.exe	Application	358 KB	13/02/2014 11:38 p.m.	3C3AD4EAD198DAFCA9D979615C88144D	C20D6E63A23F8EB3A1516A1716674FC26B78807	Yes	ABCDEF1	AES-64
Graphic Image Sample 3.exe	Application	351 KB	13/02/2014 11:38 p.m.	1D21EAD057C30F3E701D6D7276B88A0BC	1D8C3883AD302F5D30A08FBCD1FEB38F9F2F05	Yes	ABCDEF1	AES-64
Graphic Image Sample 4.exe	Application	349 KB	13/02/2014 11:38 p.m.	1681B7F497C075951AC18E12456E4424	3E83DCD58E8EB29A1432DD117F2C28C5D5A776B	Yes	ABCDEF1	AES-64
Graphic Image Sample 5.exe	Application	358 KB	13/02/2014 11:38 p.m.	A07FE5F835966E4852DA8D3D4E541BC	A9126477A4B2DAF81BD2598EB269A8FC8103FE1	Yes	ABCDEF1	AES-64
Graphic Image Sample 6.exe	Application	399 KB	13/02/2014 11:39 p.m.	5A19FC612248B648F81C37C981E5161A	2A0D5C3CEC60C0588623FE7283B725F8113A37E	Yes	ABCDEF1	AES-64
Graphic Image Sample 7.exe	Application	2,342 KB	13/02/2014 11:39 p.m.	767D519E9AB1BAC9B9696A1412FB4E44	02B84DD499D1F14F27466E7162903DE7C7673BFC	Yes	ABCDEF1	AES-64
Graphic Image Sample 8.exe	Application	2,404 KB	13/02/2014 11:39 p.m.	881C91DC63276836A60BDBE14D85C71	8CFF1CC5F49F34A527C5645D0D682E111C83DC3F	Yes	ABCDEF1	AES-64
Graphic Image Sample 9.exe	Application	497 KB	13/02/2014 11:39 p.m.	2785DE0A7224C620E038F83A5C81C16	CA850B8C93CD88DEA0DE6C727C84D37CE44D2F9	Yes	ABCDEF1	AES-64
Graphic Image Sample 10.exe	Application	485 KB	13/02/2014 11:40 p.m.	4C0FAFEA1BDCD92594E928087CFE1897	6FCA05013D197948C908882FD383121AAA29541D	Yes	ABCDEF1	AES-64
Graphic Image Sample 11.exe	Application	391 KB	13/02/2014 11:40 p.m.	31C4650CA1C4836FA8F3A710AA242C	D0717D815684687CA9680D56C36375452392947	Yes	ABCDEF1	AES-64
JPG Carved File Sample 1.exe	Application	345 KB	13/02/2014 11:40 p.m.	93DDE41DC614D0D8C81FC1BA30617316	27E2B0C867EF44ED172665D8989DA40F2329837C	Yes	ABCDEF1	AES-64
PDF Sample 1.pdf.exe	Application	12,808 KB	13/02/2014 11:41 p.m.	84D337AE2266CE0810AE337A1DEC8B89	5E70B2554407667428AA9CDB11EECA24C1BB360E	Yes	ABCDEF1	AES-64
PDF Sample 2.pdf.exe	Application	78,773 KB	13/02/2014 11:41 p.m.	9AC84AFE1BF90DFB8899190C3BF856AC	6A2A20147DCC502E57F5C72A6EC5D3C36F80D75	Yes	ABCDEF1	AES-64
PDF Sample 3.pdf.exe	Application	26,238 KB	13/02/2014 11:41 p.m.	82E0C172BA53572ADA81E8AE999F6443	84A850EA17DCB33FBAA0A982573515838BE6F4B4D3	Yes	ABCDEF1	AES-64
PDF Sample 4.pdf.exe	Application	20,720 KB	13/02/2014 11:41 p.m.	2AE9F73C06D1D8C480C7A1FBCA4F0A92	CD568C45036158663422819DA98269A0E0C88A33	Yes	ABCDEF1	AES-64
PDF Sample 5.pdf.exe	Application	24,486 KB	13/02/2014 11:42 p.m.	271198DD04E60A2706AA294CED8FB2CE	4A4753577D098545DA79D227E8D79FEDF516621F	Yes	ABCDEF1	AES-64
Text Document Sample 1.exe	Application	342 KB	13/02/2014 11:42 p.m.	1D558F13377877303A8CFFC29345513	3822EC157A8FD1188706DFEF48FE15CBDC650868	Yes	ABCDEF1	AES-64
Text Document Sample 2.exe	Application	342 KB	13/02/2014 11:42 p.m.	03C6657F56FDDA0A20CA39E16CDAB64FC	C27896D1320E1892FA889BA8286178EC182691B7	Yes	ABCDEF1	AES-64
Text Document Sample 3.exe	Application	342 KB	13/02/2014 11:43 p.m.	83A3A2837E74F33A99DA6F9808384CCD	48C064AE32317CD43C3FA8FC0D068841E75285E	Yes	ABCDEF1	AES-64
Text Document Sample 4.exe	Application	342 KB	13/02/2014 11:43 p.m.	852ABCA3816EAC21972D59DF98080C96	4520606A71C0825672532281084C434F97964463	Yes	ABCDEF1	AES-64
Text Document Sample 5.exe	Application	342 KB	13/02/2014 11:43 p.m.	AC180CA7A6G6AAEC5C3A363316F4C69	8CB434AE37A3C050A104ADC61ED161C96202007D	Yes	ABCDEF1	AES-64
Word Document Sample 1.exe	Application	364 KB	13/02/2014 11:43 p.m.	B4078169F58FAA31E08491FF32DD1D0F	16F8A1A778689CAE3E0FF2BF9F7B5884A5DC1CFF	Yes	ABCDEF1	AES-64
Word Document Sample 2.exe	Application	364 KB	13/02/2014 11:44 p.m.	252D48A0A2EE9FAE55C1FABE6493C8A0	54C80820F8837B9961600673E2C7E613F5E56D75	Yes	ABCDEF1	AES-64
Word Document Sample 3.exe	Application	364 KB	13/02/2014 11:44 p.m.	AA55ADA0AC03315FB2591E18011D2D0F1	B9F912D9A9B76D1540E409B289FC2C868851A222	Yes	ABCDEF1	AES-64
Word Document Sample 4.exe	Application	364 KB	13/02/2014 11:44 p.m.	F5790A28DA430F80668FC2C3276E13	94D45E6A2D645240C7D5B2615A31E785DE1AE02D	Yes	ABCDEF1	AES-64
Word Document Sample 5.exe	Application	364 KB	13/02/2014 11:44 p.m.	1A8F3FD825F6FB43388EAEADDDF223E83	88FB93DD0AA2986526F790AF44CF9222AAD4B48A9	Yes	ABCDEF1	AES-64

Appendix 11: Table of AESTool “Recovered Data” from Desktop

File Name	Type	Size	Timestamp	MD5 Value	SHA-1 Value	Successful Decryption	Secret Key
Encase File Sample 1.Ex01	Encase Evidence File	849,671 KB	14/02/2014 12:31 a.m.	59998CFA0E97DA5337F52808FD1A4526	4EC98E57076FA5EC23E07F05A31EE0CF5ACAAED9	Yes	ABCODEF1
Encase File Sample 2.ex01	Encase Evidence File	879,889 KB	14/02/2014 01:00 a.m.	372DA2D8022328893E4187F75162D1FB0	401A423CCED93089A146CC08F56873E33C0D358F	Yes	ABCODEF1
Encase File Sample 3.E01	Encase Evidence File	556 KB	14/02/2014 12:51 a.m.	011864AC490373208279C8C8264C5023	842AA4CD81A2CB76DE6340761BD4845748082EC	Yes	ABCODEF1
Excel Sample File 1.xls	Microsoft Excel 97-2003 Worksheet	36 KB	14/02/2014 12:51 a.m.	2C938882A40C051721B52B0FA1F3DDCF	A938C97CA88CD50A26A69178057C80828982680	Yes	ABCODEF1
Excel Sample File 2.xls	Microsoft Excel 97-2003 Worksheet	148 KB	14/02/2014 12:52 a.m.	5637DFC46A03897176E86A20171F47FF	10A0A707D9299540727E2F5FE4E34E31680D81238C44	Yes	ABCODEF1
Excel Sample File 3.xls	Microsoft Excel 97-2003 Worksheet	69 KB	14/02/2014 12:52 a.m.	B1A2A3D1F54A0C27658D0A529D1962E5	21C77EDC48640CA6CE1705C34E31680D81238C44	Yes	ABCODEF1
Excel Sample File 4.xls	Microsoft Excel 97-2003 Worksheet	189 KB	14/02/2014 12:52 a.m.	C2193FB63A055364FCE8681D352EDDE4	CDEF495E16852F960199D9984E3073FF3080AC18	Yes	ABCODEF1
Excel Sample File 5.xls	Microsoft Excel 97-2003 Worksheet	89 KB	14/02/2014 12:52 a.m.	0A5FDA7808389EB21C71B92AD92C8D2	1598FB06D3F78987B5BCE0A7B2449D8259157167	Yes	ABCODEF1
Graphic Image Sample 1.jpg	JPG File	31 KB	14/02/2014 12:52 a.m.	90DB7408078168B787AEB4882C36D65A	4A973E2C6D04D68FBFB027C0A4CB4906EABD460C	Yes	ABCODEF1
Graphic Image Sample 2.jpg	JPG File	16 KB	14/02/2014 12:53 a.m.	8CFB10680A4C1017A741628751D376D0	C7228F0B8A1D9681C01844620A8AEACDF4C8269E	Yes	ABCODEF1
Graphic Image Sample 3.jpg	JPG File	10 KB	14/02/2014 12:53 a.m.	A474E2E36810DF98BC0CDE68CF696AC3	0F60F38CE587A4D0FC996F8DA867A11D255B1C	Yes	ABCODEF1
Graphic Image Sample 4.jpg	JPG File	8 KB	14/02/2014 12:53 a.m.	CC153888280FC873F980FD51863484D5	31895FA91D7F353D0D3018E7900538891F4FFDAB	Yes	ABCODEF1
Graphic Image Sample 5.jpg	JPG File	17 KB	14/02/2014 12:54 a.m.	0A5FDA7808389EB21C71B92AD92C8D2	1598FB06D3F78987B5BCE0A7B2449D8259157167	Yes	ABCODEF1
Graphic Image Sample 6.jpg	JPG File	57 KB	14/02/2014 12:54 a.m.	D2F1C6CA96E06FAA2DE407D7DAF2972	A3550E9285239F679CA1592845B31403BAFC8D59	Yes	ABCODEF1
Graphic Image Sample 7.JPG	JPG File	2,001 KB	14/02/2014 12:55 a.m.	E9E03E7CBDE53C1EAC4344AD566F48CC	0534321762701F94876FBCAC0829D01D3385C55E	Yes	ABCODEF1
Graphic Image Sample 8.JPG	JPG File	2,063 KB	14/02/2014 12:55 a.m.	FA502616A0889197E26286896D8F4332	9F558F953D9239E4099DA97881A0848573081DDC	Yes	ABCODEF1
Graphic Image Sample 9.jpg	JPG File	155 KB	14/02/2014 12:55 a.m.	270657A4D1307924B356C2E876E594CA	349A5344A085715A3F256C023485F98D8668745D	Yes	ABCODEF1
Graphic Image Sample 10.jpg	JPG File	143 KB	14/02/2014 12:56 a.m.	0685D1447E1A518A026FF25B53147B61	8E65F89D10554858EEFD02AA54D578FD2C57993A	Yes	ABCODEF1
Graphic Image Sample 11.jpg	JPG File	50 KB	14/02/2014 12:56 a.m.	8223355957404E0E166A43081786A05	FC829D3A74FE9F88879D85FE98303A4C04FB782	Yes	ABCODEF1
JPG Carved File Sample 1.PNG	PNG File	3 KB	14/02/2014 12:56 a.m.	091523D16882626C76538270B8C2641DF	A5925A8A6EBD282F70A568318C8259D2A775D03	Yes	ABCODEF1
PDF Sample 1.pdf	Adobe Acrobat Document	12,466 KB	14/02/2014 12:56 a.m.	D51CF64D858FF6B1093A00C81F510F4	70FEE205AB86443641A77E2A8D07BAA0C39853F	Yes	ABCODEF1
PDF Sample 2.pdf	Adobe Acrobat Document	78,432 KB	14/02/2014 12:57 a.m.	9810CF0E41BFF7E0DC48CC196A5D48C7	43109E07612ECACGAD9AAB688B2811368A8548A9	Yes	ABCODEF1
PDF Sample 3.pdf	Adobe Acrobat Document	25,897 KB	14/02/2014 12:57 a.m.	8707A8B772EC57C81863D8A56EB579D5	F1725A9C766F78E17903385BDB06C352F9027A77	Yes	ABCODEF1
PDF Sample 4.pdf	Adobe Acrobat Document	20,379 KB	14/02/2014 12:57 a.m.	6E6F8EF91A8C66B41538F54641F9045	D6DED70991389788200C38370A59131A6E5116D	Yes	ABCODEF1
PDF Sample 5.pdf	Adobe Acrobat Document	24,144 KB	14/02/2014 12:57 a.m.	F0FBC1DA0A77F2908EDC34AE189583DA	5160219A2648F482DEF85DE969C08842E285D0F	Yes	ABCODEF1
Text Document Sample 1.txt	Text Document	1 KB	14/02/2014 12:57 a.m.	B2982248E195842EADCE5E391170714F	FD4D713A8FC610F72AE1A3ECCD55A786AE9956D	Yes	ABCODEF1
Text Document Sample 2.txt	Text Document	1 KB	14/02/2014 12:58 a.m.	05C0DEF79F3AB8248CE14FC39062E897	C4B96B25050A8E6DE91A79B5C30EB0EF1496497	Yes	ABCODEF1
Text Document Sample 3.txt	Text Document	1 KB	14/02/2014 12:58 a.m.	98737AB89C24FE151AD9C97720C687C54	7D1049242613148744192D1EA10077988166BC	Yes	ABCODEF1
Text Document Sample 4.txt	Text Document	1 KB	14/02/2014 12:58 a.m.	834E59E13C0240D4F1AEB81BCE7205AF	88159A8E0D32F441E34D2C34DE031475461C24DD	Yes	ABCODEF1
Text Document Sample 5.txt	Text Document	1 KB	14/02/2014 12:58 a.m.	F85B25C07181038E3FDECA1E8318EA20	3DC79410AC0C6979FA69DDE1A2E20C8F26AE0	Yes	ABCODEF1
Word Document Sample 1.doc	Microsoft 97-2003 Document	22 KB	14/02/2014 12:58 a.m.	263B83480CD58F738E2AD2BFA46DF38	8293FC6A29F753799E12AFB67420584D307C5298	Yes	ABCODEF1
Word Document Sample 2.doc	Microsoft 97-2003 Document	22 KB	14/02/2014 12:59 a.m.	880288FA7E38A443C3E31820D842A2D	BDAAAF8C891C204E4A8F127B8778A8457B1AD91	Yes	ABCODEF1
Word Document Sample 3.doc	Microsoft 97-2003 Document	22 KB	14/02/2014 12:59 a.m.	CB689F9791B45AAFF97486D03C77F771	CFB870AC35086593FA4E6D135455124D9095DAE1	Yes	ABCODEF1
Word Document Sample 4.doc	Microsoft 97-2003 Document	22 KB	14/02/2014 12:59 a.m.	C381FA0CCF8C1E8738797F372A0E07	8705FDAD0773DCA06548CB9C81BD7E7A9F8D881C	Yes	ABCODEF1
Word Document Sample 5.doc	Microsoft 97-2003 Document	22 KB	14/02/2014 12:59 a.m.	AD85136F7A88123145C7FE0ACDC0AD	7C3F7254EE5D28887F0BA17F451A61F80C1E547	Yes	ABCODEF1

Appendix 12: Table of AESCrypt “Stored Data” on VM1 (Single VM Environment)

File Name	Type	Size	Timestamp
Encase File Sample 1.Ex01.aes	AES File	849,672 KB	13/02/2014 02:56 PM
Encase File Sample 2.ex01.aes	AES File	879,890 KB	13/02/2014 02:58 PM
Encase File Sample 3.E01.aes	AES File	556 KB	13/02/2014 02:59 PM
Excel Sample File 1.xls.aes	AES File	36 KB	13/02/2014 03:22 PM
Excel Sample File 2.xls.aes	AES File	149 KB	13/02/2014 03:22 PM
Excel Sample File 3.xls.aes	AES File	69 KB	13/02/2014 03:23 PM
Excel Sample File 4.xls.aes	AES File	190 KB	13/02/2014 03:23 PM
Excel Sample File 5.xls.aes	AES File	89 KB	13/02/2014 03:23 PM
Graphic Image Sample 1.jpg.aes	AES File	31 KB	13/02/2014 03:24 PM
Graphic Image Sample 2.jpg.aes	AES File	16 KB	13/02/2014 03:24 PM
Graphic Image Sample 3.jpg.aes	AES File	10 KB	13/02/2014 03:25 PM
Graphic Image Sample 4.jpg.aes	AES File	8 KB	13/02/2014 03:25 PM
Graphic Image Sample 5.jpg.aes	AES File	17 KB	13/02/2014 03:25 PM
Graphic Image Sample 6.jpg.aes	AES File	58 KB	13/02/2014 03:26 PM
Graphic Image Sample 7.JPG.aes	AES File	2,001 KB	13/02/2014 03:26 PM
Graphic Image Sample 8.JPG.aes	AES File	2,063 KB	13/02/2014 03:26 PM
Graphic Image Sample 9.jpg.aes	AES File	155 KB	13/02/2014 03:27 PM
Graphic Image Sample 10.jpg.aes	AES File	143 KB	13/02/2014 03:27 PM
Graphic Image Sample 11.jpg.aes	AES File	50 KB	13/02/2014 03:28 PM
JPG Carved File Sample 1.PNG.aes	AES File	4 KB	13/02/2014 03:28 PM
PDF Sample 1.pdf.aes	AES File	12,466 KB	13/02/2014 03:29 PM
PDF Sample 2.pdf.aes	AES File	78,432KB	13/02/2014 03:30 PM
PDF Sample 3.pdf.aes	AES File	25,897 KB	13/02/2014 03:30 PM
PDF Sample 4.pdf.aes	AES File	20,379 KB	13/02/2014 03:31 PM
PDF Sample 5.pdf.aes	AES File	24,145 KB	13/02/2014 03:32 PM
Text Document Sample 1.txt.aes	AES File	1 KB	13/02/2014 03:32 PM
Text Document Sample 2.txt.aes	AES File	1 KB	13/02/2014 03:32 PM
Text Document Sample 3.txt.aes	AES File	1 KB	13/02/2014 03:33 PM
Text Document Sample 4.txt.aes	AES File	1 KB	13/02/2014 03:33 PM
Text Document Sample 5.txt.aes	AES File	1 KB	13/02/2014 03:33 PM
Word Document Sample 1.doc.aes	AES File	22 KB	13/02/2014 03:34 PM
Word Document Sample 2.doc.aes	AES File	22 KB	13/02/2014 03:34 PM
Word Document Sample 3.doc.aes	AES File	22 KB	13/02/2014 03:34 PM
Word Document Sample 4.doc.aes	AES File	22 KB	13/02/2014 03:35 PM
Word Document Sample 5.doc.aes	AES File	22 KB	13/02/2014 03:35 PM

Appendix 13: Table of AESCrypt “Retrieved Data” from VM1 (Single VM Environment)

File Name	Type	Size	Timestamp	MD5 Value	SHA-1 Value
Encase File Sample 1.Ex01.aes	AES Tool Files	849,672 KB	13/02/2014 02:56 PM	32EC01C9D3200922E68810FF6DEA59D4	58165999DE55AEB3A47CAFBED4910AD21739FB0
Encase File Sample 2.ex01.aes	AES Tool Files	879,890 KB	13/02/2014 02:58 PM	8E541E6F1F1B4069E7748B275CC4F302	E227CADFCC37B5C54CE71AAAE85228D93976E6
Encase File Sample 3.E01.aes	AES Tool Files	556 KB	13/02/2014 02:59 PM	1848D059A3809A952B37F68978658B1	238369DA8C806E6CB4FD4DF062226EF9AAB6D20B
Excel Sample File 1.xls.aes	AES Tool Files	36 KB	13/02/2014 03:22 PM	2441D6C7AAAC9C42615A51E9F858EC	39477EE7DAFF659249AF772717199389403353033
Excel Sample File 2.xls.aes	AES Tool Files	149 KB	13/02/2014 03:22 PM	7B1BD3947862D802E97C0388A50D37CC	20CA5CAFA88223CE942ED0671D1C2C2345460806A
Excel Sample File 3.xls.aes	AES Tool Files	69 KB	13/02/2014 03:23 PM	702B743AE93CD74A3505DE60E1D1E8063	E282445834A77B11E1AA88367259FAE04E36DD8
Excel Sample File 4.xls.aes	AES Tool Files	190 KB	13/02/2014 03:23 PM	330FA3E367766EB3E4F0210DD875AB08	B650DAFA4B6F03BA4A94FE7B5FA2C1A7283F16E
Excel Sample File 5.xls.aes	AES Tool Files	89 KB	13/02/2014 03:23 PM	F96852326A962060CAE68EA1A6F36A16	0159C6D1C578E0975C797CED0AD6F5FDDAB08B3A
Graphic Image Sample 1.jpg.aes	AES Tool Files	31 KB	13/02/2014 03:24 PM	561A308F41A5AF5706964EDED41A4EA3	C0246AE926664E25F407AB6863292BC02EF3CF2A
Graphic Image Sample 2.jpg.aes	AES Tool Files	16 KB	13/02/2014 03:24 PM	AB540851677B76001C3E9F6A7B19E8A8	FB4704915C1C1845F1A3819EB8DEFE663AF0723D
Graphic Image Sample 3.jpg.aes	AES Tool Files	10 KB	13/02/2014 03:25 PM	428DCA04B8C7F7415357C7A6D27DF354	9AB5AA47F859B78C12A66B134848FA83197380C6
Graphic Image Sample 4.jpg.aes	AES Tool Files	8 KB	13/02/2014 03:25 PM	330FA3E367766EB3E4F0210DD875AB08	B650DAFA4B6F03BA4A94FE7B5FA2C1A7283F16E
Graphic Image Sample 5.jpg.aes	AES Tool Files	17 KB	13/02/2014 03:25 PM	D86DFB82B07D1B237523F77EC58737A1	A840416A3505AA2F60C151CAEC88EC08F6450772
Graphic Image Sample 6.jpg.aes	AES Tool Files	58 KB	13/02/2014 03:26 PM	98A7DD38664B3DF7259E7A25410ACF3C	FBAB8332F0FF48BE5D2BCBEACB77EE80912A39A8
Graphic Image Sample 7.JPG.aes	AES Tool Files	2,001 KB	13/02/2014 03:26 PM	200F6BD417832C4B63B91F87EFA4D60A	133A610D08C009068854DC0F6625D51B50269D5F
Graphic Image Sample 8.JPG.aes	AES Tool Files	2,063 KB	13/02/2014 03:26 PM	7E92DE26808417704A9ED2D5431E088B	C0C64E5BD0CD34DDEB80E240E9ADBB71E1C6C688
Graphic Image Sample 9.jpg.aes	AES Tool Files	155 KB	13/02/2014 03:27 PM	05B858E218AC08311C76E9827187B848	3CD73088279D55F0B7EBA157D5C9269E48FECCA9
Graphic Image Sample 10.jpg.aes	AES Tool Files	143 KB	13/02/2014 03:27 PM	621E9571D6BA8CE050BADA1B7EAAE7A8	7E052FC2D16703B3B7614E0B7F843DD2DD5CA6B
Graphic Image Sample 11.jpg.aes	AES Tool Files	50 KB	13/02/2014 03:28 PM	FA2D595AC9BE2DF97824F2F6887D4986	11016A41DC749AE51F8D3BA381A24FDB9A4B391
JPG Carved File Sample 1.PNG.aes	AES Tool Files	4 KB	13/02/2014 03:28 PM	A007923B163EEBC9FBCE68A3A17635	9C251158E6A0C1D447E6CACAD7DC3673EFC10C0F9
PDF Sample 1.pdf.aes	AES Tool Files	12,466 KB	13/02/2014 03:29 PM	76198067F4CDFD4B8F453981345666EA4	74874E5AFE93840613A481D8892E6585A7C0F80B
PDF Sample 2.pdf.aes	AES Tool Files	78,432KB	13/02/2014 03:30 PM	6D4B1B45B11400988A223CBA2811D12D	B0780ED5CF720332A697EA6A8519498F2494DCB
PDF Sample 3.pdf.aes	AES Tool Files	25,897 KB	13/02/2014 03:30 PM	D893B83FD0E0A051A0AFDC896D3BC1E8	332BD16ED24F81905DBE853DAC96D555C83F773A
PDF Sample 4.pdf.aes	AES Tool Files	20,379 KB	13/02/2014 03:31 PM	63BA757116C5912459622C8CDC2AAD5A	CC3817163D485E6816AA5D13FC3E85833F263C1B
PDF Sample 5.pdf.aes	AES Tool Files	24,145 KB	13/02/2014 03:32 PM	0ED1DE782B70CA72F873AE71946EE51F	5E1BA748ABF5A3CFB27672FE2AD89D9912BDA60D
Text Document Sample 1.txt.aes	AES Tool Files	1 KB	13/02/2014 03:32 PM	C46616ECF749CF7D0A2480251D0080D1D	C91F91BC3EBE316FF857D7D500E6356EF18197D2
Text Document Sample 2.txt.aes	AES Tool Files	1 KB	13/02/2014 03:32 PM	177F88208103369A8F07FC8696DCCFE9	24C7AC16419797533E0D6A4970732C318953EF10
Text Document Sample 3.txt.aes	AES Tool Files	1 KB	13/02/2014 03:33 PM	4946AC17E98AD112FF3AF4A814B004FD7	30B635CEDED9A9F303628122D706FD44695DEEB1
Text Document Sample 4.txt.aes	AES Tool Files	1 KB	13/02/2014 03:33 PM	2456A974AD1607175E1E59C3DE386AB2	78E359910940699C88580A97257B40F9285BA716
Text Document Sample 5.txt.aes	AES Tool Files	1 KB	13/02/2014 03:33 PM	FE3E2C1D8D59FA04788E25DD0CCE71E6	FEAAC9A604C51248833543E22888952CD62DC760
Word Document Sample 1.doc.aes	AES Tool Files	22 KB	13/02/2014 03:34 PM	66094DDAFB15760F7298D284624A32D0	7695750275CE92E4AC2FD2696E3174CBE53EECD
Word Document Sample 2.doc.aes	AES Tool Files	22 KB	13/02/2014 03:34 PM	BE26CE532A33E88F9F88DAF179809D55	AEGCE2618AC09D41D5C45D9AD3289ADA8F14364
Word Document Sample 3.doc.aes	AES Tool Files	22 KB	13/02/2014 03:34 PM	1B7DC8EACAF75B19CADCD4618A65C46	D81CF0E6739723FC3E54A452EB1F617A0CE084
Word Document Sample 4.doc.aes	AES Tool Files	22 KB	13/02/2014 03:35 PM	AF385C0A05DE958EBDC12D382D111E88	291640737F1D44A2158BD14A2D16E9F71AE34D30
Word Document Sample 5.doc.aes	AES Tool Files	22 KB	13/02/2014 03:35 PM	EC191DF5FD701B5AAEC48381E27086F	251E2C5786DC0C42CC86F39BD306D8D74769CE0A

Appendix 14: Table of AESCrypt “Recovered Data” from VM1 (Single VM Environment)

File Name	Type	Size	Timestamp	MD5 Value	SHA-1 Value	Successful Decryption	Secret Key	Algorithm
Encase File Sample 1.Ex01	Encase Evidence File	849,672 KB	14/02/2014 03:56 AM	5999BCEA0E97D5A3375F2808FD1A4526	4EC9B85706F56C23E07F05A31EE0CF5AACAD9	Yes	abcdeffghi1	AES-256
Encase File Sample 2.ex01	Encase Evidence File	879,890 KB	14/02/2014 04:00 AM	377D0A2D80D3238893E4187F12561DFB0	401A423CCE9D930B9A146CC0B56B75C33C0D358F	Yes	ijklmnopq82	AES-256
Encase File Sample 3.E01	Encase Evidence File	556 KB	14/02/2014 04:01 AM	01186AA4CA9D373208279C8C8264C50D3	B42AA4CDB1A2C876D6E6340761BD48A574830B2FC	Yes	stuvwxyzab3	AES-256
Excel Sample File 1.xls	Microsoft Excel 97-2003 Worksheet	36 KB	14/02/2014 04:01 AM	2C9388B2A40CD51721B5280FA1F3DDCF	A83BC97CA88CD504264691780E37C808289B2680	Yes	bcdefghiu4	AES-256
Excel Sample File 2.xls	Microsoft Excel 97-2003 Worksheet	149 KB	14/02/2014 04:02 AM	5637DFC46A639B7176E86A20171E47FF	21C77EDC486A0EC46CE1705C34E3168D81238C44	Yes	klmnopq55	AES-256
Excel Sample File 3.xls	Microsoft Excel 97-2003 Worksheet	69 KB	14/02/2014 04:02 AM	B1A2A3D1F54A0C2765800A529D196E5	ZUC77EDC486A0EC46CE1705C34E3168D81238C44	Yes	tuwxyzab6	AES-256
Excel Sample File 4.xls	Microsoft Excel 97-2003 Worksheet	190 KB	14/02/2014 04:02 AM	C2193FB63A055364FCE8681D352ED0E4	C0EFA951E68527960199D9B4E3073F3080AC18	Yes	cdefghijk7	AES-256
Excel Sample File 5.xls	Microsoft Excel 97-2003 Worksheet	89 KB	14/02/2014 04:03 AM	0A5FDA78D3839EB21C71B9F2A097C8D2	1598FB06D3F78987B58C70A7B24A9D8259157167	Yes	lmnopqrst8	AES-256
Graphic Image Sample 1.jpg	JPG File	31 KB	14/02/2014 04:03 AM	9D0B74080781688787AEB4882C36D65A	44973E2C6D0A068BFB0D7C0A4CB4906EABD460C	Yes	uvwxyzabc9	AES-256
Graphic Image Sample 2.jpg	JPG File	16 KB	14/02/2014 04:03 AM	8CFB106B0A4C1017A741628751D376D0	C7228E068A1D9681C01844620A9AE6CDF4C8269E	Yes	defghijkl1	AES-256
Graphic Image Sample 3.jpg	JPG File	10 KB	14/02/2014 04:03 AM	AA74E2E36810DF9B9C0CDE68CF696AC3	0F60F38CFE587ADF0C9596F8D4867AF1D255B1C	Yes	mnopqrst2	AES-256
Graphic Image Sample 4.jpg	JPG File	8 KB	14/02/2014 04:04 AM	CC15388B280FC873F980FD51B63484D5	31895FA91D7F353D0D3018F790D538891F4FDDAB	Yes	vwxyzabc3	AES-256
Graphic Image Sample 5.jpg	JPG File	17 KB	14/02/2014 04:04 AM	0A5FDA78D3839EB21C71B9F2A097C8D2	1598FB06D3F78987B58C70A7B24A9D8259157167	Yes	efghijklm4	AES-256
Graphic Image Sample 6.jpg	JPG File	58 KB	14/02/2014 04:04 AM	D2F1C6CA6E0FAA2DEA02D7DAF2972	A3550E9285239F679CA1592845831403BAFC8D59	Yes	nopqrstuv5	AES-256
Graphic Image Sample 7.JPG	JPG File	2,001 KB	14/02/2014 04:04 AM	E9033E7C8DE53C1EAC4344AD566F48CC	0534321762701F94876F8CAC0B29D0C01D385C55E	Yes	wxyzabcde6	AES-256
Graphic Image Sample 8.JPG	JPG File	2,063 KB	14/02/2014 04:05 AM	FA50261640889197E2626B96D8BF4332	9F558F953D9239F4099D9A978B1A08AB573081DDC	Yes	ghijklmn7	AES-256
Graphic Image Sample 9.jpg	JPG File	155 KB	14/02/2014 04:05 AM	270657A0D1307924B356C2E876E594CA	349A5344A0B5715A3F256C032485F9808668745D	Yes	opqrstuvw8	AES-256
Graphic Image Sample 10.jpg	JPG File	143 KB	14/02/2014 04:05 AM	0685D1447E15A18A026F2F5853347861	865F589D10554858EEFFD02AA54D578FD0C57993A	Yes	wxyzabcde9	AES-256
Graphic Image Sample 11.jpg	JPG File	50 KB	14/02/2014 04:06 AM	822335956740460E16644A30B1786A05	FC829D3A74FE9E88879D85FF9830A3A3C04FB782	Yes	ghijklmn01	AES-256
JPG Carved File Sample 1.PNG	PNG File	4 KB	14/02/2014 04:06 AM	091523D16882626C76538270BC2641DF	A59252A8A6EBD282F70A56831BCB259D2A775D03	Yes	pqrstuv2	AES-256
PDF Sample 1.pdf	Adobe Acrobat Document	12,466 KB	14/02/2014 04:06 AM	D51CFE4D858FF681093A00C81F510F4	70FEE205AB86443641AA77E2A8D07BAAD0C39853F	Yes	wxyzabcde3	AES-256
PDF Sample 2.pdf	Adobe Acrobat Document	78,432 KB	14/02/2014 04:06 AM	9810CF0E418FF7E0DC24BCC196A5D4BC7	43109E07612ECAC6AD9AAB6882811368AB548A9	Yes	ghijklmn4	AES-256
PDF Sample 3.pdf	Adobe Acrobat Document	25,897 KB	14/02/2014 04:07 AM	8707A8B772E5C7C81863D8A56E8579D5	F1725A9C766F78E17903385B0B06C352F9027A77	Yes	opqrstuvw5	AES-256
PDF Sample 4.pdf	Adobe Acrobat Document	20,379 KB	14/02/2014 04:07 AM	6E6F8EF9FA8C66841538F54641F9045	D60ED70991389788200C383704A59131A6E5116D	Yes	xyzabcde6	AES-256
PDF Sample 5.pdf	Adobe Acrobat Document	24,145 KB	14/02/2014 04:07 AM	F0FBC1DA0477F2908DC34AE189583DA	5160219A2648F482DEFF8F5D9F969C08842E85D0F	Yes	ghijklmn07	AES-256
Text Document Sample 1.txt	Text Document	1 KB	14/02/2014 04:08 AM	B29824BE195842EADCC3EEF931170714F	FD40713A8FC0107724E1A15CC055A7B6A4E959E6D	Yes	pqrstuv8	AES-256
Text Document Sample 2.txt	Text Document	1 KB	14/02/2014 04:08 AM	05C0FE79F3A88248CE14FC9062E897	C489682305046FB6D9F18A7983C0F8D0E7496497	Yes	uvwxyzabc9	AES-256
Text Document Sample 3.txt	Text Document	1 KB	14/02/2014 04:08 AM	98737AB89C24FE151AD937720C687C54	7D1049242613314874419201E1A100777988168C	Yes	defghijkl1	AES-256
Text Document Sample 4.txt	Text Document	1 KB	14/02/2014 04:08 AM	834E5BE13C0240D4FAEB81BCF7205AF	8815948E0D32F44E1E34D0C3ADE031475461C24DD	Yes	mnopqrst2	AES-256
Text Document Sample 5.txt	Text Document	1 KB	14/02/2014 04:09 AM	F85B250C7181038C3FDECA1E8318FA20	30DC7940AC0C69797F69DDE1A2E2DDCB26A40	Yes	vwxyzabc3	AES-256
Word Document Sample 1.doc	Microsoft Word 97-2003 Document	22 KB	14/02/2014 04:09 AM	2638B34BD0C0D58F738E2A02BF46D0F38	8293FC6A29F73799E12AFB67420584D307C5238	Yes	efghijklm4	AES-256
Word Document Sample 2.doc	Microsoft Word 97-2003 Document	22 KB	14/02/2014 04:09 AM	880288FA7E384443C131820D8A2A2D	B0A4A4FC8791C204E4A8F1278877948A57B1A091	Yes	nopqrstuv5	AES-256
Word Document Sample 3.doc	Microsoft Word 97-2003 Document	22 KB	14/02/2014 04:10 AM	C8689F8791845A4F97486DD03C77F71	CF870AC35086593446D1354512490905DAE1	Yes	wxyzabcde6	AES-256
Word Document Sample 4.doc	Microsoft Word 97-2003 Document	22 KB	14/02/2014 04:10 AM	C381FA0CCFCB1E873879F7327A0E07	8705FDDA0D773DCA06548C09C1BDE7A3F80881C	Yes	ghijklmn07	AES-256
Word Document Sample 5.doc	Microsoft Word 97-2003 Document	22 KB	14/02/2014 04:10 AM	AD85136F7A881223145C7FE0CAD0C0AD	7C33F7254FE5028887C0B17F451A61F80C1E547	Yes	pqrstuvw8	AES-256

Appendix 15: Table of AxCrypt “Stored Data” on VM1 (Single VM Environment)

File Name	Type	Size	Timestamp
Encase File Sample 1-Ex01.axx	AXX File	849,672 KB	13/02/2014 06:59 PM
Encase File Sample 2-ex01.axx	AXX File	879,890 KB	13/02/2014 07:00 PM
Encase File Sample 3-E01.axx	AXX File	556 KB	13/02/2014 07:00 PM
Excel Sample File 1-xls.axx	AXX File	9 KB	13/02/2014 07:01 PM
Excel Sample File 2-xls.axx	AXX File	32 KB	13/02/2014 07:01 PM
Excel Sample File 3-xls.axx	AXX File	20 KB	13/02/2014 07:02 PM
Excel Sample File 4-xls.axx	AXX File	29 KB	13/02/2014 07:02 PM
Excel Sample File 5-xls.axx	AXX File	17 KB	13/02/2014 07:02 PM
Graphic Image Sample 1-jpg.axx	AXX File	19 KB	13/02/2014 07:03 PM
Graphic Image Sample 2-jpg.axx	AXX File	17 KB	13/02/2014 07:03 PM
Graphic Image Sample 3-jpg.axx	AXX File	10 KB	13/02/2014 07:03 PM
Graphic Image Sample 4-jpg.axx	AXX File	8 KB	13/02/2014 07:04 PM
Graphic Image Sample 5-jpg.axx	AXX File	17 KB	13/02/2014 07:04 PM
Graphic Image Sample 6-jpg.axx	AXX File	58 KB	13/02/2014 07:04 PM
Graphic Image Sample 7-JPG.axx	AXX File	2,001 KB	13/02/2014 07:05 PM
Graphic Image Sample 8-JPG.axx	AXX File	2,063 KB	13/02/2014 07:05 PM
Graphic Image Sample 9-jpg.axx	AXX File	155 KB	13/02/2014 07:05 PM
Graphic Image Sample 10-jpg.axx	AXX File	143 KB	13/02/2014 07:06 PM
Graphic Image Sample 11-jpg.axx	AXX File	50 KB	13/02/2014 07:06 PM
JPG Carved File Sample 1-PNG.axx	AXX File	4 KB	13/02/2014 07:06 PM
PDF Sample 1-pdf.axx	AXX File	12,466 KB	13/02/2014 07:49 PM
PDF Sample 2-pdf.axx	AXX File	68,437KB	13/02/2014 07:50 PM
PDF Sample 3-pdf.axx	AXX File	25,897 KB	13/02/2014 07:50 PM
PDF Sample 4-pdf.axx	AXX File	20,379 KB	13/02/2014 07:51 PM
PDF Sample 5-pdf.axx	AXX File	24,145 KB	13/02/2014 07:51 PM
Text Document Sample 1-txt.axx	AXX File	1 KB	13/02/2014 07:08 PM
Text Document Sample 2-txt.axx	AXX File	1 KB	13/02/2014 07:08 PM
Text Document Sample 3-txt.axx	AXX File	1 KB	13/02/2014 07:08 PM
Text Document Sample 4-txt.axx	AXX File	1 KB	13/02/2014 07:09 PM
Text Document Sample 5-txt.axx	AXX File	1 KB	13/02/2014 07:09 PM
Word Document Sample 1-doc.axx	AXX File	6 KB	13/02/2014 07:10 PM
Word Document Sample 2-doc.axx	AXX File	6 KB	13/02/2014 07:10 PM
Word Document Sample 3-doc.axx	AXX File	6 KB	13/02/2014 07:10 PM
Word Document Sample 4-doc.axx	AXX File	6 KB	13/02/2014 07:10 PM
Word Document Sample 5-doc.axx	AXX File	6 KB	13/02/2014 07:11 PM

Appendix 16: Table of AxCrypt “Retrieved Data” from VM1 (Single VM Environment)

File Name	Type	Size	Timestamp	MD5 Value	SHA-1 Value
Encase File Sample 1-Ex01.axx	AxCrypt Encrypted File	849,672 KB	13/02/2014 06:59 PM	E66461D4885E2F31DD6D6751FD2B41E9	AA2DBB847B59886E6C2DCB47FA01B4C5DCA1815A4
Encase File Sample 2-ex01.axx	AxCrypt Encrypted File	879,890 KB	13/02/2014 07:00 PM	B1003F33735C9F78831C7E0E5DE65350	0FA1F430445CA5CF2C8C596306138E8DCC3BC10
Encase File Sample 3-E01.axx	AxCrypt Encrypted File	556 KB	13/02/2014 07:00 PM	5D4D4D360DEA07274EFC854DA2AE06F	7C16E8F99EB8041BC4D122382823183C58083D39
Excel Sample File 1-xls.axx	AxCrypt Encrypted File	9 KB	13/02/2014 07:01 PM	C65C27369663AF9A90DC89E2AE0B3C4F5	57A2AA538EB4E4A88315C3EB6806C48D5E5D89506
Excel Sample File 2-xls.axx	AxCrypt Encrypted File	32 KB	13/02/2014 07:01 PM	66130E5AC908E58FDBCF82C6F292ADC	A69E340C7D240F8B71988FFABF67D934FE5F83D0
Excel Sample File 3-xls.axx	AxCrypt Encrypted File	20 KB	13/02/2014 07:02 PM	5606346700F319B6E5A08385ED54802F	D2FF4B1D9CDE493434DB8C49FF4582C8888B4C6
Excel Sample File 4-xls.axx	AxCrypt Encrypted File	29 KB	13/02/2014 07:02 PM	EE089A190D8E46E1D3EDB17E1C205014	5009927550FF823EDC1CB3573FFAF1918D9363AC
Excel Sample File 5-xls.axx	AxCrypt Encrypted File	17 KB	13/02/2014 07:02 PM	A8C4D7AE1F812667838D666399146366	F23400126AFF985BE1A1DE3F78CD43307AD63439
Graphic Image Sample 1-jpg.axx	AxCrypt Encrypted File	19 KB	13/02/2014 07:03 PM	6C84D9814E33FF72D7AAD868D4BF676C	C1678CAB97E1359A8414DBDE5E82A8D6C198C33C
Graphic Image Sample 2-jpg.axx	AxCrypt Encrypted File	17 KB	13/02/2014 07:03 PM	7165530F346708FE29856505EEF712A8	81107D1DEFDEAE59F7B12ACFFCB3087D0C49E8538
Graphic Image Sample 3-jpg.axx	AxCrypt Encrypted File	10 KB	13/02/2014 07:03 PM	91319B8A562E8381856D8049035E3513	2AC4F8E376999754F370C47C86300C5A9FF2EF4B
Graphic Image Sample 4-jpg.axx	AxCrypt Encrypted File	8 KB	13/02/2014 07:04 PM	3F0F4E90EF56313FCA5FD1B242C3034A	75EBED4DC3537FA23F4E3FC517626DC422D34878
Graphic Image Sample 5-jpg.axx	AxCrypt Encrypted File	17 KB	13/02/2014 07:04 PM	306F847B8A597DC449AA2B2E2995FEA950	D820B8AE436856CF046B7F1F282C862D8316315F8
Graphic Image Sample 6-jpg.axx	AxCrypt Encrypted File	58 KB	13/02/2014 07:04 PM	569A61D96FD88E42E0E22AFC6DC6E6A6A	4A41F28A51A42CB88CF9481D85B5A36F4884EAC5
Graphic Image Sample 7-jpg.axx	AxCrypt Encrypted File	2,001 KB	13/02/2014 07:05 PM	34F08FDA5250F135D70A511681BD366C	5320120858EB0A4625FB5C73FD965975BA0DBB5
Graphic Image Sample 8-JPG.axx	AxCrypt Encrypted File	2,063 KB	13/02/2014 07:05 PM	EDF98C380D5197B88BF910508CC9986F	24DBFD388C55A998902C9EA1E200F5EDA41484F
Graphic Image Sample 9-jpg.axx	AxCrypt Encrypted File	155 KB	13/02/2014 07:05 PM	A8F2530461434411C326A22988F73C6C7	BBB6337390180CFF7FCE9CA2C9A0AE4F046927E3
Graphic Image Sample 10-jpg.axx	AxCrypt Encrypted File	143 KB	13/02/2014 07:06 PM	047A84FF66FD6410E31E1FE043C6FC695	EF58CB8E779C1D94E47C4D133F58D92D200D5D4C
Graphic Image Sample 11-jpg.axx	AxCrypt Encrypted File	50 KB	13/02/2014 07:06 PM	C5DD66C3F71A8702E830C28808F5A4FC	076AA52AE2D617018F9EB8FC28319C37DEB04742
JPG Carved File Sample 1-PNG.axx	AxCrypt Encrypted File	4 KB	13/02/2014 07:06 PM	EC62EC88A9175C5CC4D9A5407B2606	F6C9C9C163457DA0293B124A98C5028ABD575B1A
PDF Sample 1-pdf.axx	AxCrypt Encrypted File	12,466 KB	13/02/2014 07:49 PM	68C5F8229EEA0609ACFFCAE669D35B	2361F2036FE741E6F30D8A56B940809451B0857C
PDF Sample 2-pdf.axx	AxCrypt Encrypted File	68,437KB	13/02/2014 07:50 PM	8DF51C3D0221A47CC467122106466066	EDE5B7B0EA26AE4D6465A5D2806AD0F42793B83A
PDF Sample 3-pdf.axx	AxCrypt Encrypted File	25,897 KB	13/02/2014 07:50 PM	4F5E98A2D6ED1A8BA59A94AF0BFC9724	B4194AC96C275E82B866263F1AD6A7EF6C65ADA1
PDF Sample 4-pdf.axx	AxCrypt Encrypted File	20,379 KB	13/02/2014 07:51 PM	39906B439918C6C6A1C50D0882056358	7D91466FD498D7B1FC10DF69A58950D8F9A2B8E1
PDF Sample 5-pdf.axx	AxCrypt Encrypted File	24,145 KB	13/02/2014 07:51 PM	C836F8A33EAE7A0686DFC9962BEFF1BF	0A2408D5F1557E0983D896DA3D5E7F089207D596
Text Document Sample 1-txt.axx	AxCrypt Encrypted File	1 KB	13/02/2014 07:08 PM	4F08127285D0DADF8F69BF6981879870	44E651252585E9D95516AFA2689DAAD284571788
Text Document Sample 2-txt.axx	AxCrypt Encrypted File	1 KB	13/02/2014 07:08 PM	2B64ED7482278AECF811E05C87F84A8	78D62C59246A341E7EF69E9C2887F256A3649F
Text Document Sample 3-txt.axx	AxCrypt Encrypted File	1 KB	13/02/2014 07:08 PM	BF09A6A2EE0F3057D92228F5A5978303	C979B84C5F0C17082EDA98D173C4E715E4572FF
Text Document Sample 4-txt.axx	AxCrypt Encrypted File	1 KB	13/02/2014 07:09 PM	3F0F4E90EF56313FCA5FD1B242C3034A	75EBED4DC3537FA23F4E3FC517626DC422D34878
Text Document Sample 5-txt.axx	AxCrypt Encrypted File	1 KB	13/02/2014 07:09 PM	B3B09CCB8EB15897DC4886188D80380D	1A792F7764A91B71E67E828F3CD584F20CF16E
Word Document Sample 1-doc.axx	AxCrypt Encrypted File	6 KB	13/02/2014 07:10 PM	6A4D950330A82EA09309F8135220C910	A76F17E91AF19D57A61CF388C091D683FF5FE699
Word Document Sample 2-doc.axx	AxCrypt Encrypted File	6 KB	13/02/2014 07:10 PM	71A9DF948155A8780D77A88D7E4088CA	CA1619CC9353A54558FB279E455EEF3D6216FC41D
Word Document Sample 3-doc.axx	AxCrypt Encrypted File	6 KB	13/02/2014 07:10 PM	0695DDF321DB99606453DC05808E7B3F	08BD87D7580ED067499AFE41997A88FD7452D6FB
Word Document Sample 4-doc.axx	AxCrypt Encrypted File	6 KB	13/02/2014 07:10 PM	437772E6E77520371792F99423CE91B	98CC8F6B5856A3751D88941AADCD9CA006D04D4
Word Document Sample 5-doc.axx	AxCrypt Encrypted File	6 KB	13/02/2014 07:11 PM	D0624DC02C1F8973C44B4BDF7F891E56	C63F7699C8676DE0B80FF8C4A00A445C5F5A31F

Appendix 17: Table of AxCrypt “Recovered Data” from VM1 (Single VM Environment)

File Name	Type	Size	Timestamp	MDS Value	SHA-1 Value	Successful Decryption	Secret Key	Algorithm
Encase File Sample 1.Ex01	Encase Evidence File	849,671 KB	29/06/2011 10:29 AM	59998CE40E97DA5337F2808F0145426	4FC0B5E7076FA5E3C23E07F05431EFC0F54ACAD9	Yes	abcdefgh11	AES-128
Encase File Sample 2.ex01	Encase Evidence File	879,889 KB	28/11/2012 03:06 PM	372DA2D8032328893E4187F12561DF80	4014423CED9809A146C0BF568F5E3C0D358F	Yes	ijklmnopR2	AES-128
Encase File Sample 3.E01	Encase Evidence File	556 KB	04/05/2013 08:48 PM	011864AC909373208279C8B264C5023	8424AA4C0B1A2C976DE6340761BD484574830B2EC	Yes	stuvwxyzA3	AES-128
Excel Sample File 1.xls	Microsoft Excel 97-2003 Worksheet	36 KB	16/05/2013 08:41 AM	2C98882A40C0D5172185280FA1F3D0CF	A83B0C97CA98C0D0426469178057C08828982680	Yes	bcd efghijA4	AES-128
Excel Sample File 2.xls	Microsoft Excel 97-2003 Worksheet	148 KB	17/06/2005 11:38 AM	56370FC46A63987176B6A20171E47FF	10A0A707092959047E275FE4E4275F5D12E1844A	Yes	klmnopqS5	AES-128
Excel Sample File 3.xls	Microsoft Excel 97-2003 Worksheet	69 KB	17/06/2005 11:39 AM	91A2A3D1F5440C276580A529D1962E5	21C77EDC4B60FCAC6C1705C4E3168081238CA4	Yes	tuvwxyzA6	AES-128
Excel Sample File 4.xls	Microsoft Excel 97-2003 Worksheet	189 KB	17/06/2005 11:40 AM	C2193FB63A055364FC8681D3521DDE4	CDEF495E16852796D190984E4073F3F080AC18	Yes	cdefghijk7	AES-128
Excel Sample File 5.xls	Microsoft Excel 97-2003 Worksheet	89 KB	17/06/2005 11:41 AM	0A5FD478D03389EB21C71BF92A093C802	159BF80603F7897B58CF0A78244908259157167	Yes	lmnopqrst8	AES-128
Graphic Image Sample 1.jpg	JPG File	31 KB	08/02/2008 03:44 PM	9DD8740807816887874EB48B2C36D65A	44973E2C6D0A0D6BF8B27C0A4C94906EABD460C	Yes	uvwxyzabc9	AES-128
Graphic Image Sample 2.jpg	JPG File	16 KB	22/01/2014 11:12 AM	8CFB10680A4C10174741628751D376D0	C7228E06841D9681C0184620A84E6CD4C8269E	Yes	defghijkl1	AES-128
Graphic Image Sample 3.jpg	JPG File	10 KB	22/01/2014 11:13 AM	A474E2E36810DF98C0CDE68CF696AC3	0F60F38CFE587A4DFC996F8D4867A711D25581C	Yes	mnopqrstU2	AES-128
Graphic Image Sample 4.jpg	JPG File	8 KB	22/01/2014 11:13 AM	CC153888280FC873F980FD518G3484D5	31895FA91D7F533D0D3018E7900538891F4FFDAB	Yes	vwxyzabcD3	AES-128
Graphic Image Sample 5.jpg	JPG File	17 KB	22/01/2014 11:14 AM	0A5FD478D03389EB21C71BF92A093C802	159BF80603F7897B58CF0A78244908259157167	Yes	efghijklM4	AES-128
Graphic Image Sample 6.jpg	JPG File	57 KB	12/07/2005 01:14 AM	D2F1C6C486606FAA2DEA02D7DAF2972	A3550E92852396679CA1592845B314038AFCD059	Yes	nopqrstuv5	AES-128
Graphic Image Sample 7.JPG	JPG File	2,001 KB	03/09/2009 12:20 PM	E9E08E7C80E53CEAC4344AD56648CC	0534321762701F94876FBAC0B29DCD1D385C55E	Yes	wxyzabcde6	AES-128
Graphic Image Sample 8.JPG	JPG File	2,063 KB	18/03/2009 09:06 AM	FA50261640889197E26286896D8F4332	9F558F953D9239E4099DA97881A08A573081DDC	Yes	efghijkmn7	AES-128
Graphic Image Sample 9.jpg	JPG File	155 KB	10/01/2010 12:08 PM	270527AAD13079248356C2E876E594CA	349A5344A0B571543756C0234B5F9B8668B745D	Yes	opqrstuvw8	AES-128
Graphic Image Sample 10.jpg	JPG File	143 KB	15/05/2012 03:43 PM	0685D1447E15A184026EF25B53147861	8E65F89D10554839E8FFD02A450578FD2C57993A	Yes	wxyzabcde9	AES-128
Graphic Image Sample 11.jpg	JPG File	50 KB	21/11/1999 04:48 PM	82223359567404E0E166A4A3081786AD5	FC829D3A747F9EB887908F5983034A3C04FB782	Yes	ghijklmnO1	AES-128
JPG Carved File Sample 1.PNG	PNG File	3 KB	09/05/2012 04:53 PM	09152D1688262C76538270B2C641DF	A59252A846EBD282F70A568318CB25902A775D03	Yes	pqrstuv2	AES-128
PDF Sample 1.pdf	Adobe Acrobat Document	12,466 KB	07/05/2011 02:15 PM	D51CF64D858F681093A00C81F510F4	70FEE205A8B6443641AA77EA8D078AADC39853F	Yes	wxyzabcde3	AES-128
PDF Sample 2.pdf	Adobe Acrobat Document	78,432 KB	07/05/2011 02:28 PM	9B1DCFD41BFF7E10DC4B8C196A5D48C7	43109E07612EACAC6AD09A48688281136BA8548A9	Yes	efghijkmn4	AES-128
PDF Sample 3.pdf	Adobe Acrobat Document	25,897 KB	07/05/2011 02:17 PM	8707A88777EC57C81863D8A56EB57905	F1725A9C766F78E1790338B8D806C352F9027A77	Yes	opqrstuvw5	AES-128
PDF Sample 4.pdf	Adobe Acrobat Document	20,379 KB	07/05/2011 01:11 PM	6E6F8E9F1ABCC6841538F54641F9045	D6DEFD70991389788200C38370A59131A6E5116D	Yes	wxyzabcde6	AES-128
PDF Sample 5.pdf	Adobe Acrobat Document	24,144 KB	07/05/2011 01:11 PM	F0FBC1DA0477F2908EDC34AE189583DA	S160219A2648F482DEEF85D3C969C08842E2B5D0F	Yes	ghijklmnO7	AES-128
Text Document Sample 1.txt	Text Document	1 KB	22/01/2014 11:58 AM	B2982248E195B42EADCE5EE391170714F	FD40713ABFC610F72AE15EC055A7B6AE958E6D	Yes	pqrstuv8	AES-128
Text Document Sample 2.txt	Text Document	1 KB	22/01/2014 11:59 AM	05CC0E7F9F3A88248C2E14FC93062E897	C4896B25050A5E680E918A79B5C3E1BDEF1096497	Yes	uvwxyzabc9	AES-128
Text Document Sample 3.txt	Text Document	1 KB	22/01/2014 11:59 AM	98737AB89C24FE15EAD0C97720C687C54	7D1049242633148744192D1EA100779881668C	Yes	defghijkl1	AES-128
Text Document Sample 4.txt	Text Document	1 KB	22/01/2014 12:00 PM	834E59E13C0240D4FAE8B18C7205AF	8B1594810D93F4A1E3402C3AD4031475461C24DD	Yes	mnopqrstU2	AES-128
Text Document Sample 5.txt	Text Document	1 KB	22/01/2014 12:01 PM	F85B250C7181038E3FDCAE18318EA20	3DC79410A0C0C69797A690DE1A2E2C8F26A640	Yes	wxyzabcD3	AES-128
Word Document Sample 1.doc	Microsoft 97-2003 Document	22 KB	22/01/2014 11:53 AM	26388348DC058F738C2AD0F446D0F38	8293FC6A29753799E12AF6674203840307C5298	Yes	efghijkM4	AES-128
Word Document Sample 2.doc	Microsoft 97-2003 Document	22 KB	22/01/2014 11:53 AM	880288FA7F3B4A43C3E3183D0842A2D	BD4A44FC891C204E448F1278877848A5781A091	Yes	nopqrstuv5	AES-128
Word Document Sample 3.doc	Microsoft 97-2003 Document	22 KB	22/01/2014 11:53 AM	C8689F8791B45AFAF97486D03C77F771	CF8870AC35086593F44E6013545524D090950AE1	Yes	wxyzabcde6	AES-128
Word Document Sample 4.doc	Microsoft 97-2003 Document	22 KB	22/01/2014 11:54 AM	C381FA0CCFBC1E873879E7F937A0E07	8705FDD40D773DCA06546CB9C81B0E7A3F80881C	Yes	efghijkmnO7	AES-128
Word Document Sample 5.doc	Microsoft 97-2003 Document	22 KB	22/01/2014 12:02 PM	ADB513677F4881223145C7FE0CA0C0AD	7C33F7254E4E5D28887E0BA17F451A61FB0C1E547	Yes	pqrstuvw8	AES-128

Appendix 18: Table of AESCrypt “Stored Data” on VM1 (Single VM Environment)

File Name	Type	Size	Timestamp
AES Encase File Sample 1	Application	850,013 KB	13/02/2014 11:29 PM
AES Encase File Sample 2	Application	880,231 KB	13/02/2014 11:35 PM
AES Encase File Sample 3	Application	898 KB	13/02/2014 11:35 PM
AES Excel Sample File 1	Application	378 KB	13/02/2014 11:35 PM
AES Excel Sample File 2	Application	490 KB	13/02/2014 11:36 PM
AES Excel Sample File 3	Application	411 KB	13/02/2014 11:36 PM
AES Excel Sample File 4	Application	531 KB	13/02/2014 11:37 PM
AES Excel Sample File 5	Application	431 KB	13/02/2014 11:37 PM
AES Graphic Image Sample 1	Application	373 KB	13/02/2014 11:37 PM
AES Graphic Image Sample 2	Application	358 KB	13/02/2014 11:38 PM
AES Graphic Image Sample 3	Application	351 KB	13/02/2014 11:38 PM
AES Graphic Image Sample 4	Application	349 KB	13/02/2014 11:38 PM
AES Graphic Image Sample 5	Application	358 KB	13/02/2014 11:38 PM
AES Graphic Image Sample 6	Application	399 KB	13/02/2014 11:39 PM
AES Graphic Image Sample 7	Application	2,342 KB	13/02/2014 11:39 PM
AES Graphic Image Sample 8	Application	2,404 KB	13/02/2014 11:39 PM
AES Graphic Image Sample 9	Application	497 KB	13/02/2014 11:39 PM
AES Graphic Image Sample 10	Application	485 KB	13/02/2014 11:40 PM
AES Graphic Image Sample 11	Application	391 KB	13/02/2014 11:40 PM
AES JPG Carved File Sample 1	Application	345 KB	13/02/2014 11:40 PM
AES PDF Sample 1.pdf	Application	12,808 KB	13/02/2014 11:41 PM
AES PDF Sample 2.pdf	Application	78,773 KB	13/02/2014 11:41 PM
AES PDF Sample 3.pdf	Application	26,238 KB	13/02/2014 11:41 PM
AES PDF Sample 4.pdf	Application	20,720 KB	13/02/2014 11:41 PM
AES PDF Sample 5.pdf	Application	24,486 KB	13/02/2014 11:42 PM
AES Text Document Sample 1	Application	342 KB	13/02/2014 11:42 PM
AES Text Document Sample 2	Application	342 KB	13/02/2014 11:42 PM
AES Text Document Sample 3	Application	342 KB	13/02/2014 11:43 PM
AES Text Document Sample 4	Application	342 KB	13/02/2014 11:43 PM
AES Text Document Sample 5	Application	342 KB	13/02/2014 11:43 PM
AES Word Document Sample 1	Application	364 KB	13/02/2014 11:43 PM
AES Word Document Sample 2	Application	364 KB	13/02/2014 11:44 PM
AES Word Document Sample 3	Application	364 KB	13/02/2014 11:44 PM
AES Word Document Sample 4	Application	364 KB	13/02/2014 11:44 PM
AES Word Document Sample 5	Application	364 KB	13/02/2014 11:44 PM

Appendix 19: Table of AESTool “Retrieved Data” from VM1 (Single VM Environment)

File Name	Type	Size	Timestamp	MD5 Value	SHA-1 Value
Encase File Sample 1.exe	Application	850,013 KB	13/02/2014 11:29 PM	A1F96B13E979168E3019F7C722560253	A842310D7B7F16E4A54A8FE3E735C032798D95EE
Encase File Sample 2.exe	Application	880,231 KB	13/02/2014 11:35 PM	996B9B3DA2F80ACEA1FEC51828581B80	9552D0A98CC9C5437E8AAAFB680C621BFC93E6F7D
Encase File Sample 3.exe	Application	898 KB	13/02/2014 11:35 PM	01421216BF51089F421D4E691F78124E	8533A8487231F0C3C76904CFB9C6014B21C6DFB7
Excel Sample File 1.exe	Application	378 KB	13/02/2014 11:35 PM	00CF104B7F44186BD0C090F6F1BE1D54	7CC302D112D0D317837D578E16AC75C17049F2178
Excel Sample File 2.exe	Application	490 KB	13/02/2014 11:36 PM	AAE560C7ADEEDA54D7B21807973C2550	780077169D98A22271826936B6EFF57A36976E1D
Excel Sample File 3.exe	Application	411 KB	13/02/2014 11:36 PM	BF307088D001E5F56613852D2DA513317	AA96B7B8555F1732E25B994F45032BB16F415693
Excel Sample File 4.exe	Application	531 KB	13/02/2014 11:37 PM	25ED89BEF8B91E958CF3E22FDF51DF4E4	8C548D878FCBEC5453822C1F3B843307339FAA9D
Excel Sample File 5.exe	Application	431 KB	13/02/2014 11:37 PM	50B845D5C913A778191921FCDAAFA408	D3A4E0F78F8FFD124DDDB7A9C7FA99CDBD53E17FE
Graphic Image Sample 1.exe	Application	373 KB	13/02/2014 11:37 PM	C8E4C0328100B8186F9D97961EA39403	9D61DF08F66E02F3ECB433807AACCS967015EE2E
Graphic Image Sample 2.exe	Application	358 KB	13/02/2014 11:38 PM	3C3AD4EAD19BDAFCA9D979615C88144D	20D06F63A23F8EB3A1516A171667F4FC26B78807
Graphic Image Sample 3.exe	Application	351 KB	13/02/2014 11:38 PM	1D21EAD57C30F3E701D6D7276888ADBC	1D8C3883AD302F5D30AD8F8CCD1FEB38F9F2F05
Graphic Image Sample 4.exe	Application	349 KB	13/02/2014 11:38 PM	1681B7F497C075951AC1BE12456EA424	3E83DCD58E8EB29A1432DD117F2C28C5D52A776B
Graphic Image Sample 5.exe	Application	358 KB	13/02/2014 11:38 PM	A07EF50F835966E4852DABD3D4E541BC	A9126477A482DAFB18D2598EB269A8EC8103FE1
Graphic Image Sample 6.exe	Application	399 KB	13/02/2014 11:39 PM	5A19FC6122488648F81C37C981E5161A	2A0D5C3CEC60C05588623FE7283B725FB113A37E
Graphic Image Sample 7.exe	Application	2,342 KB	13/02/2014 11:39 PM	767D519E9A81BAC9B9696A1412FB4E44	02B84DD499D1F14F27466E7162903DE7C7673BEC
Graphic Image Sample 8.exe	Application	2,404 KB	13/02/2014 11:39 PM	881C91DC63276836A6DBD8E145D85C71	8CFF1CC5F49F34A527C56455DD682E111C83DC3F
Graphic Image Sample 9.exe	Application	497 KB	13/02/2014 11:39 PM	2785DE0A7224C620E038F83A5C81C16	C485DBC93CD88DEA0DE6CC727C84D37CE4E44D2F9
Graphic Image Sample 10.exe	Application	485 KB	13/02/2014 11:40 PM	4C0FAFEA18CD92594E922B087CFE1897	6FCA05013D197948C9088B2FD383121AAA29541D
Graphic Image Sample 11.exe	Application	391 KB	13/02/2014 11:40 PM	31C4650CA14C836FAFBF3A3710AA242C	D0717DB15684687CA696D056C363754552392947
JPG Carved File Sample 1.exe	Application	345 KB	13/02/2014 11:40 PM	93DE41DC614D0D8CB1FC1BA30617316	27E2B0C867EF44ED172665D8989D40E2329837C
PDF Sample 1.pdf.exe	Application	12,808 KB	13/02/2014 11:41 PM	84D337AE2266ECEE0810AE337A1DEC8B9	5E70B2554407667428AA9CDB11E1CA24C1BB360E
PDF Sample 2.pdf.exe	Application	78,773 KB	13/02/2014 11:41 PM	9AC84FE18F900DFB8899190C38FB56AC	6A2A20147DC502E57E5C72A6EC5CD3C36F80D75
PDF Sample 3.pdf.exe	Application	26,238 KB	13/02/2014 11:41 PM	82E0C1728A53572ADA81E8AE939F6A43	84AB50EA17DCB33FBA0A98257351583BE6F4B4D3
PDF Sample 4.pdf.exe	Application	20,720 KB	13/02/2014 11:41 PM	2AE9F73C06D1D8C480C7A1FBCAFE0A92	CD568C450361586E3422819DA98269A0E0C88A33
PDF Sample 5.pdf.exe	Application	24,486 KB	13/02/2014 11:42 PM	271198DD04E60A2706AA294CEDE8FB2CE	444753577DD98545DA79D227E8079FE9DF516621F
Text Document Sample 1.exe	Application	342 KB	13/02/2014 11:42 PM	1D55BF133737877303A8CFFC29345513	3822EC157ABFD118B706DFF48FE15CB6580B68
Text Document Sample 2.exe	Application	342 KB	13/02/2014 11:42 PM	03C6657F56FD0A420CA39E16CDA684FC	C27896D1320E1892FA889B8A2B6178EC182691B7
Text Document Sample 3.exe	Application	342 KB	13/02/2014 11:43 PM	AA65ADAC03315FB2591E18011D2D0F1	B9F912D9A9876D154C0EA9B289FC26868851A222
Text Document Sample 4.exe	Application	342 KB	13/02/2014 11:43 PM	2AE9F73C06D1D8C480C7A1FBCAFE0A92	CD568C450361586E3422819DA98269A0E0C88A33
Text Document Sample 5.exe	Application	342 KB	13/02/2014 11:43 PM	A1C80CA7A6GAACEF5C3AE363316F4C69	8CBA3A4E37A3C050A104ADC61ED161C96202007D
Word Document Sample 1.exe	Application	364 KB	13/02/2014 11:43 PM	B4078169F5BF8A31E0B491FFE3DD1D0F	16E8A1A778689CAE3E0FF2BF9E7B5884A5DC1CFF
Word Document Sample 2.exe	Application	364 KB	13/02/2014 11:44 PM	252D48A0A2EE9FAE55C1FABE6493C8A0	54C80820F8837B961600673E2C7E613F5E56D75
Word Document Sample 3.exe	Application	364 KB	13/02/2014 11:44 PM	AA65ADAC03315FB2591E18011D2D0F1	B9F912D9A9876D154C0EA9B289FC26868851A222
Word Document Sample 4.exe	Application	364 KB	13/02/2014 11:44 PM	F5790A28DA3D8F0668FCCCE3276E13	94D45E6A2D645240C7D582615A31E785DE1AE02D
Word Document Sample 5.exe	Application	364 KB	13/02/2014 11:44 PM	1A8F3FD825F6FB43388EAEDDDF223E83	88FB3DD0A2986526F3790AF44CF9222AAD848A9

Appendix 20: Table of AESTool “Recovered Data” from VM1 (Single VM Environment)

File Name	Type	Size	Timestamp	MDS Value	SHA-1 Value	Successful Decryption	Secret Key	Algorithm
Encase File Sample 1.Ex01	Encase Evidence File	849,671 KB	14/02/2014 06:23 AM	5998CEA0E9D7A53375F2808FD1A4526	4FC9B857076FA5EC23E07F05431EFC0F5AACAED9	Yes	ABCDFFF1	AES-64
Encase File Sample 2.Ex01	Encase Evidence File	879,889 KB	14/02/2014 06:23 AM	372DA2D08023238893E4187F12561DFB0	401AA23CCE930B9A146CC0B56B75E33C0D58F	Yes	ABCDFFF1	AES-64
Encase File Sample 3.Ex01	Encase Evidence File	556 KB	14/02/2014 06:23 AM	011864AC49D373208798C8C26AC3023	B42AA4CDBA1A2C976DEF63A0761BD484574830B27C	Yes	ABCDFFF1	AES-64
Excel Sample File 1.xls	Microsoft Excel 97-2003 Worksheet	36 KB	14/02/2014 06:23 AM	2C9388B2A40CD51721B52B0FA1F3DDCF	A83BC97C48B0C50426A691780557C808289B2680	Yes	ABCDFFF1	AES-64
Excel Sample File 2.xls	Microsoft Excel 97-2003 Worksheet	148 KB	14/02/2014 06:23 AM	5637DFC46A63987176E8B6A20171477F	10A0A707D9295954072E25FE4E47055D12E1844A	Yes	ABCDFFF1	AES-64
Excel Sample File 3.xls	Microsoft Excel 97-2003 Worksheet	69 KB	14/02/2014 06:23 AM	B1A2A3D1F5A40C276580D4529D1962E5	21C77EDC4B640ECAC6E1705C4E316808123BC44	Yes	ABCDFFF1	AES-64
Excel Sample File 4.xls	Microsoft Excel 97-2003 Worksheet	189 KB	14/02/2014 06:23 AM	C2193FB63A055364FC8681D352EDDE4	C0EFA95E16B52960199D984E30773F3080AC18	Yes	ABCDFFF1	AES-64
Excel Sample File 5.xls	Microsoft Excel 97-2003 Worksheet	89 KB	14/02/2014 06:23 AM	0A5FDA78D8389FB21C71B92AD92C8D2	1598FB06D3F7897858CFA0A7B344908259157167	Yes	ABCDFFF1	AES-64
Graphic Image Sample 1.jpg	JPG File	31 KB	14/02/2014 06:23 AM	9DD974080781688787AE9A882C36065A	449732CGD04068FEBD7C04C9A906EABD460C	Yes	ABCDFFF1	AES-64
Graphic Image Sample 2.jpg	JPG File	16 KB	14/02/2014 06:23 AM	8CFB106800A4C1017A741628751D376D0	C7228E06BA1D9681C0184620A84E6CD4C8269E	Yes	ABCDFFF1	AES-64
Graphic Image Sample 3.jpg	JPG File	10 KB	14/02/2014 06:23 AM	AA74E2E36810DF99BC0CDE68CF696AC3	0F60F38CFE587A4DFC996F8DA867AF11D25581C	Yes	ABCDFFF1	AES-64
Graphic Image Sample 4.jpg	JPG File	8 KB	14/02/2014 06:23 AM	CC15388B80FC873F980FD51B63484D5	31895FA91D7F533D0D3018E7905388914FFDAB	Yes	ABCDFFF1	AES-64
Graphic Image Sample 5.jpg	JPG File	17 KB	14/02/2014 06:23 AM	1A5525BC59F37DDA42A2916E645458013	A9F560E8FC196A1AAE0A56907EEF78A0D5EBD	Yes	ABCDFFF1	AES-64
Graphic Image Sample 6.jpg	JPG File	57 KB	14/02/2014 06:23 AM	D2F1C6CAB6E06FAA2DEA02D7DAF2972	A355019285239F679CA1592845B314D38AFC8D59	Yes	ABCDFFF1	AES-64
Graphic Image Sample 7.JPG	JPG File	2,001 KB	14/02/2014 06:23 AM	E9E03E7CBDE53C1EAC4344AD566F48C	0534321762701F94876F8CA10829DCD1D3B5C55E	Yes	ABCDFFF1	AES-64
Graphic Image Sample 8.JPG	JPG File	2,063 KB	14/02/2014 06:23 AM	FAS0261640889197E26266908F4332	9F558F953D9239F4099DA97881A08A8573081DDC	Yes	ABCDFFF1	AES-64
Graphic Image Sample 9.jpg	JPG File	155 KB	14/02/2014 06:23 AM	270657AD13079248356C2E876E594CA	349A534440B5715A3F256C023485F98D8668745D	Yes	ABCDFFF1	AES-64
Graphic Image Sample 10.jpg	JPG File	143 KB	14/02/2014 06:23 AM	068501447E15A184026E25B33147B61	8E65F89D1055485BEFFD0A450578FD2C7993A	Yes	ABCDFFF1	AES-64
Graphic Image Sample 11.jpg	JPG File	50 KB	14/02/2014 06:23 AM	8223359567404E1664A430B1786AD5	FC829D3A747FEBE8879D8F983034A3C04FB782	Yes	ABCDFFF1	AES-64
JPG Carved File Sample 1.PNG	PNG File	3 KB	14/02/2014 06:23 AM	091523D16882626C7653B2708C2641DF	A59252A8A6EBD282F70A56831B3C259D2A775D03	Yes	ABCDFFF1	AES-64
PDF Sample 1.pdf	Adobe Acrobat Document	12,466 KB	14/02/2014 06:23 AM	D51CFE4D858FF681093A00C81F510F4	70FEE205A8B643641AA77E2A8D07BAAD39853F	Yes	ABCDFFF1	AES-64
PDF Sample 2.pdf	Adobe Acrobat Document	78,432 KB	14/02/2014 06:23 AM	9810CFE418FF7E0DC48CC196A5D48C7	43109E07612ECAC6AD9AAB68B281136B8A548A9	Yes	ABCDFFF1	AES-64
PDF Sample 3.pdf	Adobe Acrobat Document	25,897 KB	14/02/2014 06:23 AM	8707A8B72EC57C81863D8A56E8579D5	F1725A9C76678E179033858D806C3529027A77	Yes	ABCDFFF1	AES-64
PDF Sample 4.pdf	Adobe Acrobat Document	20,379 KB	14/02/2014 06:23 AM	6E6F8E9F1A8C66841538F54641F9A5	D60ED70991389788200C3B370A59131A6E5116D	Yes	ABCDFFF1	AES-64
PDF Sample 5.pdf	Adobe Acrobat Document	24,144 KB	14/02/2014 06:23 AM	F0FBC1D0A477F2908E2ADCE5EE39117074F	5160219A2648482DEEF85D596908B9A2E2B5D0F	Yes	ABCDFFF1	AES-64
Text Document Sample 1.txt	Text Document	1 KB	14/02/2014 06:23 AM	B298248E1958A4E2ADCE5EE39117074F	FD40713A8FC610F72AE15ECC055A766AE959E6D	Yes	ABCDFFF1	AES-64
Text Document Sample 2.txt	Text Document	1 KB	14/02/2014 06:23 AM	05CC0E79F3A8248CE14FC39062E897	C4896825050AEB060918A79B5C3BEDEF1496497	Yes	ABCDFFF1	AES-64
Text Document Sample 3.txt	Text Document	1 KB	14/02/2014 06:23 AM	98737AB89C24FE151AD09720C687C54	7D10492426133148744191D7E1A100779881668C	Yes	ABCDFFF1	AES-64
Text Document Sample 4.txt	Text Document	1 KB	14/02/2014 06:23 AM	834E59E13C040D4F1AE8B18C72054F	8815948E0D32441E3402C3A4D031475461C24DD	Yes	ABCDFFF1	AES-64
Text Document Sample 5.txt	Text Document	1 KB	14/02/2014 06:23 AM	F8582507C181038E3FDECA1E8318E420	3DC79410AC0C69797F4690DE1A2E200C8F26A60	Yes	ABCDFFF1	AES-64
Word Document Sample 1.doc	Microsoft 97-2003 Document	22 KB	14/02/2014 06:30 AM	26388348D0C058F738E2AD2B446F0F38	8293FC6A29F753799E12AF8674205840307C5298	Yes	ABCDFFF1	AES-64
Word Document Sample 2.doc	Microsoft 97-2003 Document	22 KB	14/02/2014 06:30 AM	880288A7E3B4443C3E31320D842A2D	B0A4A4FC8791C204E448F12778784845781AD91	Yes	ABCDFFF1	AES-64
Word Document Sample 3.doc	Microsoft 97-2003 Document	22 KB	14/02/2014 06:30 AM	C689F8791B45A4F94866D3C77F771	CF8870AC35086593F44E60135455124D9095DAE1	Yes	ABCDFFF1	AES-64
Word Document Sample 4.doc	Microsoft 97-2003 Document	22 KB	14/02/2014 06:30 AM	C381FA0CCFCB1E873879F7527A0E07	8705FD4D0D773DCA0548CB9C81BD7A3F8D881C	Yes	ABCDFFF1	AES-64
Word Document Sample 5.doc	Microsoft 97-2003 Document	22 KB	14/02/2014 06:30 AM	AD851367FA881223145C7E0CADC0AD	7C33F7254FE5D28887E0B417451461F90C1E547	Yes	ABCDFFF1	AES-64

Appendix 21: Table of AESCrypt “Stored Data” on VM1 (Double VMs Environment)

File Name	Type	Size	Timestamp
Encase File Sample 1.Ex01.aes	AES File	849,672 KB	13/02/2014 02:56 PM
Encase File Sample 2.ex01.aes	AES File	879,890 KB	13/02/2014 02:58 PM
Encase File Sample 3.E01.aes	AES File	556 KB	13/02/2014 02:59 PM
Excel Sample File 1.xls.aes	AES File	36 KB	13/02/2014 03:22 PM
Excel Sample File 2.xls.aes	AES File	149 KB	13/02/2014 03:22 PM
Excel Sample File 3.xls.aes	AES File	69 KB	13/02/2014 03:23 PM
Excel Sample File 4.xls.aes	AES File	190 KB	13/02/2014 03:23 PM
Excel Sample File 5.xls.aes	AES File	89 KB	13/02/2014 03:23 PM
Graphic Image Sample 1.jpg.aes	AES File	31 KB	13/02/2014 03:24 PM
Graphic Image Sample 2.jpg.aes	AES File	16 KB	13/02/2014 03:24 PM
Graphic Image Sample 3.jpg.aes	AES File	10 KB	13/02/2014 03:25 PM
Graphic Image Sample 4.jpg.aes	AES File	8 KB	13/02/2014 03:25 PM
Graphic Image Sample 5.jpg.aes	AES File	17 KB	13/02/2014 03:25 PM
Graphic Image Sample 6.jpg.aes	AES File	58 KB	13/02/2014 03:26 PM
Graphic Image Sample 7.JPG.aes	AES File	2,001 KB	13/02/2014 03:26 PM
Graphic Image Sample 8.JPG.aes	AES File	2,063 KB	13/02/2014 03:26 PM
Graphic Image Sample 9.jpg.aes	AES File	155 KB	13/02/2014 03:27 PM
Graphic Image Sample 10.jpg.aes	AES File	143 KB	13/02/2014 03:27 PM
Graphic Image Sample 11.jpg.aes	AES File	50 KB	13/02/2014 03:28 PM
JPG Carved File Sample 1.PNG.aes	AES File	4 KB	13/02/2014 03:28 PM
PDF Sample 1.pdf.aes	AES File	12,466 KB	13/02/2014 03:29 PM
PDF Sample 2.pdf.aes	AES File	78,432KB	13/02/2014 03:30 PM
PDF Sample 3.pdf.aes	AES File	25,897 KB	13/02/2014 03:30 PM
PDF Sample 4.pdf.aes	AES File	20,379 KB	13/02/2014 03:31 PM
PDF Sample 5.pdf.aes	AES File	24,145 KB	13/02/2014 03:32 PM
Text Document Sample 1.txt.aes	AES File	1 KB	13/02/2014 03:32 PM
Text Document Sample 2.txt.aes	AES File	1 KB	13/02/2014 03:32 PM
Text Document Sample 3.txt.aes	AES File	1 KB	13/02/2014 03:33 PM
Text Document Sample 4.txt.aes	AES File	1 KB	13/02/2014 03:33 PM
Text Document Sample 5.txt.aes	AES File	1 KB	13/02/2014 03:33 PM
Word Document Sample 1.doc.aes	AES File	22 KB	13/02/2014 03:34 PM
Word Document Sample 2.doc.aes	AES File	22 KB	13/02/2014 03:34 PM
Word Document Sample 3.doc.aes	AES File	22 KB	13/02/2014 03:34 PM
Word Document Sample 4.doc.aes	AES File	22 KB	13/02/2014 03:35 PM
Word Document Sample 5.doc.aes	AES File	22 KB	13/02/2014 03:35 PM

Appendix 22: Table of AESCrypt “Stored Data” on VM2 (Double VMs Environment)

File Name	Type	Size	Timestamp
Encase File Sample 1.Ex01.aes	AES File	849,672 KB	13/02/2014 01:56 PM
Encase File Sample 2.ex01.aes	AES File	879,890 KB	13/02/2014 01:58 PM
Encase File Sample 3.E01.aes	AES File	556 KB	13/02/2014 01:59 PM
Excel Sample File 1.xls.aes	AES File	36 KB	13/02/2014 02:22 PM
Excel Sample File 2.xls.aes	AES File	149 KB	13/02/2014 02:22 PM
Excel Sample File 3.xls.aes	AES File	69 KB	13/02/2014 02:23 PM
Excel Sample File 4.xls.aes	AES File	190 KB	13/02/2014 02:23 PM
Excel Sample File 5.xls.aes	AES File	89 KB	13/02/2014 02:23 PM
Graphic Image Sample 1.jpg.aes	AES File	31 KB	13/02/2014 02:24 PM
Graphic Image Sample 2.jpg.aes	AES File	16 KB	13/02/2014 02:24 PM
Graphic Image Sample 3.jpg.aes	AES File	10 KB	13/02/2014 02:25 PM
Graphic Image Sample 4.jpg.aes	AES File	8 KB	13/02/2014 02:25 PM
Graphic Image Sample 5.jpg.aes	AES File	17 KB	13/02/2014 02:25 PM
Graphic Image Sample 6.jpg.aes	AES File	58 KB	13/02/2014 02:26 PM
Graphic Image Sample 7.JPG.aes	AES File	2,001 KB	13/02/2014 02:26 PM
Graphic Image Sample 8.JPG.aes	AES File	2,063 KB	13/02/2014 02:26 PM
Graphic Image Sample 9.jpg.aes	AES File	155 KB	13/02/2014 02:27 PM
Graphic Image Sample 10.jpg.aes	AES File	143 KB	13/02/2014 02:27 PM
Graphic Image Sample 11.jpg.aes	AES File	50 KB	13/02/2014 02:28 PM
JPG Carved File Sample 1.PNG.aes	AES File	4 KB	13/02/2014 02:28 PM
PDF Sample 1.pdf.aes	AES File	12,466 KB	13/02/2014 02:29 PM
PDF Sample 2.pdf.aes	AES File	78,432KB	13/02/2014 02:30 PM
PDF Sample 3.pdf.aes	AES File	25,897 KB	13/02/2014 02:30 PM
PDF Sample 4.pdf.aes	AES File	20,379 KB	13/02/2014 02:31 PM
PDF Sample 5.pdf.aes	AES File	24,145 KB	13/02/2014 02:32 PM
Text Document Sample 1.txt.aes	AES File	1 KB	13/02/2014 02:32 PM
Text Document Sample 2.txt.aes	AES File	1 KB	13/02/2014 02:32 PM
Text Document Sample 3.txt.aes	AES File	1 KB	13/02/2014 02:33 PM
Text Document Sample 4.txt.aes	AES File	1 KB	13/02/2014 02:33 PM
Text Document Sample 5.txt.aes	AES File	1 KB	13/02/2014 02:33 PM
Word Document Sample 1.doc.aes	AES File	22 KB	13/02/2014 02:34 PM
Word Document Sample 2.doc.aes	AES File	22 KB	13/02/2014 02:34 PM
Word Document Sample 3.doc.aes	AES File	22 KB	13/02/2014 02:34 PM
Word Document Sample 4.doc.aes	AES File	22 KB	13/02/2014 02:35 PM
Word Document Sample 5.doc.aes	AES File	22 KB	13/02/2014 02:35 PM

Appendix 23: Table of AESCrypt “Retrieved Data” from VM2 (Double VMs Environment)

File Name	Type	Size	Timestamp	MDS Value	SHA-1 Value
Encase File Sample 1.Ex01.aes	AES Tool Files	849,672 KB	13/02/2014 02:55 PM	32EC01C9D3200922E68810FE6DEA59D4	58165999DE5AEB3A47CAFBEAD4910AD21739FB0
Encase File Sample 2.ex01.aes	AES Tool Files	879,890 KB	13/02/2014 02:58 PM	8E541E6F1F1B4069E774B8275CC4F302	E227CADFC3785C54CE71AA0AE822B8D93976E6
Encase File Sample 3.E01.aes	AES Tool Files	556 KB	13/02/2014 02:59 PM	1848D059A3809A9525B37E6897B658B1	238369DA8CB086CE6CB4FD4DF062226EF9AAB6D20B
Excel Sample File 1.xls.aes	AES Tool Files	36 KB	13/02/2014 03:22 PM	2441D6C7AAAC9C4615A51E9F9E85BEC	39477EE7DAF659249AF727172199389403353033
Excel Sample File 2.xls.aes	AES Tool Files	149 KB	13/02/2014 03:22 PM	7B18D3947862D8D2E97C038BA50D37CC	20CA5CAF88223CE942ED0671D1C2C2345460B06A
Excel Sample File 3.xls.aes	AES Tool Files	69 KB	13/02/2014 03:23 PM	702B743AE93CDC74A35DE6DE1D1E8063	E2824445B34477B11E1AA88367259FAE04E36DD8
Excel Sample File 4.xls.aes	AES Tool Files	190 KB	13/02/2014 03:23 PM	330FA3E367766EB3E4F0210D0875AB08	B650DAFA4B6F03BA4AA94FE7B5FA2C1A7283F16E
Excel Sample File 5.xls.aes	AES Tool Files	89 KB	13/02/2014 03:23 PM	F96852326A962060CAE68EA1A6F36A16	0159C6D1C578E0975C797CED0AD6F5FDDA808B3A
Graphic Image Sample 1.jpg.aes	AES Tool Files	31 KB	13/02/2014 03:24 PM	561A308F41A5AF5706964EDED41A4EA3	C0246AE926664E25F407AB6863292BC02EF3CF2A
Graphic Image Sample 2.jpg.aes	AES Tool Files	16 KB	13/02/2014 03:24 PM	AB540B51677B76001C3E9F6A7B19E8A8	FB4704915C1C1845F1A3819EBBDEFE663AF0723D
Graphic Image Sample 3.jpg.aes	AES Tool Files	10 KB	13/02/2014 03:25 PM	428DCA048B87F7415357C7A6D27DF354	9AB5AA47F859878C12A668134848FA83197380C6
Graphic Image Sample 4.jpg.aes	AES Tool Files	8 KB	13/02/2014 03:25 PM	330FA3E367766EB3E4F0210D0875AB08	B650DAFA4B6F03BA4AA94FE7B5FA2C1A7283F16E
Graphic Image Sample 5.jpg.aes	AES Tool Files	17 KB	13/02/2014 03:25 PM	D86DF82B07D1B2375237F7EC5B737A1	A840416A305AA2F60C151CAE88EC0BF6450772
Graphic Image Sample 6.jpg.aes	AES Tool Files	58 KB	13/02/2014 03:26 PM	98A7DD38664B3DF7259E7A25410ACF3C	FBAB8332F0FF4BBE5D2BCBEACB77E80912A39A8
Graphic Image Sample 7.JPG.aes	AES Tool Files	2,001 KB	13/02/2014 03:26 PM	200F6BD417832CA4863B91F87EFA4D60A	133A610D08C009068854DC0F6625D51B50269D5F
Graphic Image Sample 8.JPG.aes	AES Tool Files	2,063 KB	13/02/2014 03:26 PM	7E92DE26B0841770A49EDD25431E08B8	C0C64E58DCD34DEEB80E240E9ADBB71E1C6C6B8
Graphic Image Sample 9.jpg.aes	AES Tool Files	155 KB	13/02/2014 03:27 PM	05B85E218AC08311C76E9827187B8A8	3CD73088279D55F0B7EBA157D5C9269E48FECCA9
Graphic Image Sample 10.jpg.aes	AES Tool Files	143 KB	13/02/2014 03:27 PM	621E9571D6BA8CE0550BAD1B7E4E7AB	7E052FC2DF167033B37614E0B7F843DD2DD5CA6B
Graphic Image Sample 11.jpg.aes	AES Tool Files	50 KB	13/02/2014 03:28 PM	FA2D595AC98E2DF97B24F2F6887D4986	11016A41DC749AE51F8D3BA381A2F4FDB9A4B391
JPG Carved File Sample 1.PNG.aes	AES Tool Files	4 KB	13/02/2014 03:28 PM	A007923B163EEBCC9FBCEC68A3A17635	9C251158E6A0C1D447E6CACA7DC3673EFC10C0F9
PDF Sample 1.pdf.aes	AES Tool Files	12,466 KB	13/02/2014 03:29 PM	76198067F4CDFD488F4539B134566EA4	74874E5AFE938A0613A481D8B92E6585A7C0F80B
PDF Sample 2.pdf.aes	AES Tool Files	78,432KB	13/02/2014 03:30 PM	6D4B1B45B11400988A4233CBA2811D12D	B0780ED5CF720332A697EA6AB519498F2494DDCB
PDF Sample 3.pdf.aes	AES Tool Files	25,897 KB	13/02/2014 03:30 PM	D893B83FDD0E0A051A0AFDC896D38C1EB	332BD16ED24F81905DBE853DAC96D555C83F773A
PDF Sample 4.pdf.aes	AES Tool Files	20,379 KB	13/02/2014 03:31 PM	63BA757116C5912459622C8DC2AAD5A	CC3B17163D485E6816AA5D13FC3E85833F263C1B
PDF Sample 5.pdf.aes	AES Tool Files	24,145 KB	13/02/2014 03:32 PM	0ED1DE782B70CA72F873AE71946EE51F	5E1BA748ABF5A3CFB27672FE2AD89D0912BDA60D
Text Document Sample 1.txt.aes	AES Tool Files	1 KB	13/02/2014 03:32 PM	C46616FC749CF7D0A2480251D008D1D	C91F91BC3EBE316FF857D7D500E6356F18197D2
Text Document Sample 2.txt.aes	AES Tool Files	1 KB	13/02/2014 03:32 PM	177F8B208103369AFB07F8C966DCCFE9	24C74C164197533FE0D6A4970732C318953EF10
Text Document Sample 3.txt.aes	AES Tool Files	1 KB	13/02/2014 03:33 PM	4946AC17E98AD112FF3AFA814B004FD7	30B635CEDED9AF303628122D706FD44695DEEB1
Text Document Sample 4.txt.aes	AES Tool Files	1 KB	13/02/2014 03:33 PM	2456A974AD1607175E1E59C3DE3B6AB2	78E359910940699C8B58DA97257B40F92B5BA716
Text Document Sample 5.txt.aes	AES Tool Files	1 KB	13/02/2014 03:33 PM	FE3E2C1D8D059FA04788E25D00CE71E6	FEAAC9A604C51248833543E22888952CD62DC760
Word Document Sample 1.doc.aes	AES Tool Files	22 KB	13/02/2014 03:34 PM	66094DDAFB15760F729B284624A32D0	76957550275CE92E4AC2FD2696E3174CBE53EED
Word Document Sample 2.doc.aes	AES Tool Files	22 KB	13/02/2014 03:34 PM	BE26CE532A33E88F9F88DAF179B09505	AE6CDE2618AC09D41D5C45D9AD3289ADA8F14364
Word Document Sample 3.doc.aes	AES Tool Files	22 KB	13/02/2014 03:34 PM	1B7DCE8ACAF75EB19CADCD4618A65C46	D81CF0E6739723FC3E54A45F2EB1F61F7A0CE084
Word Document Sample 4.doc.aes	AES Tool Files	22 KB	13/02/2014 03:35 PM	AF385C0A05DE958EBDC12D382D111E8B	291640737F1D44A2158BD14A2D16E9F71AE34D30
Word Document Sample 5.doc.aes	AES Tool Files	22 KB	13/02/2014 03:35 PM	EC191DFF5D701B5AEECC48381E27086F	251E2C5786DC0C42CC86F39BD306D8D74769CE0A

Appendix 24: Table of AESCrypt “Recovered Data” from VM2 (Double VMs Environment)

File Name	Type	Size	Timestamp	MD5 Value	SHA-1 Value	Successful Decryption	Secret Key	Algorithm
Encase File Sample 1.Ex01	Encase Evidence File	849,672 KB	14/02/2014 09:34 AM	5999BCAE0E97DA53275F2808FD1A4526	4FC9B657076F6A5C23E07F04531EE0CFC5A4CAED9	Yes	abcdeghi1	AES-256
Encase File Sample 2.ex01	Encase Evidence File	879,890 KB	14/02/2014 09:34 AM	372D42D80232388995E4187F1256DFB0	401AA323CED93099A146CC08F56B75E33CD0358F	Yes	ijklmnopR2	AES-256
Encase File Sample 3.E01	Encase Evidence File	556 KB	14/02/2014 09:34 AM	01186AAC490373208279C8C6A5C023	B42AAACDB1A2CB76D6340761BD484574B3082EC	Yes	stuvwxyz43	AES-256
Excel Sample File 1.xls	Microsoft Excel 97-2003 Worksheet	36 KB	14/02/2014 09:35 AM	2C9388B2A40C05172185280FA1F3D0CF	AB3BC97CA88CD50A26A69178057C808289B2680	Yes	bcdefghi4	AES-256
Excel Sample File 2.xls	Microsoft Excel 97-2003 Worksheet	149 KB	14/02/2014 09:35 AM	5637DFCA6A63987176B6A2017147FF	10A0A707D929954072E2F5FE42765D12E1844A	Yes	klmnopqr55	AES-256
Excel Sample File 3.xls	Microsoft Excel 97-2003 Worksheet	69 KB	14/02/2014 09:35 AM	81A2A3D1F54A0C27F58D0A529D1962E5	21C77EDC4B6A0ECAF6C1705C34E316808123BCA4	Yes	tuvwxyzab6	AES-256
Excel Sample File 4.xls	Microsoft Excel 97-2003 Worksheet	190 KB	14/02/2014 09:36 AM	C2103P663A055364FC1E8681D352EDDE4	C0EFA95E16852F960199D9984E30773FF3080AC18	Yes	cdefghijk7	AES-256
Excel Sample File 5.xls	Microsoft Excel 97-2003 Worksheet	89 KB	14/02/2014 09:36 AM	0A5FDA78D8389E821C71B9F2A092C802	1598FB0603F78987B58CF0A782449D8259157167	Yes	lmnopqrst8	AES-256
Graphic Image Sample 1.jpg	JPG File	31 KB	14/02/2014 09:36 AM	9DDB74080781688787AEB488C36D65A	44973E2C6D0406BF8BD27C0A4CB4906EABD460C	Yes	uvwxyzabc9	AES-256
Graphic Image Sample 2.jpg	JPG File	16 KB	14/02/2014 09:36 AM	8CFB10680A4C1017A741628751D376D0	C7228E068A1D9681C01844620A8AECDF4C8269E	Yes	defghijkl1	AES-256
Graphic Image Sample 3.jpg	JPG File	10 KB	14/02/2014 09:36 AM	AA74E2E36810DF9B8C0CD68CF696AC3	0F60F38CFE587A4D70C996F8DA887AF11D25581C	Yes	mnpqrstuv2	AES-256
Graphic Image Sample 4.jpg	JPG File	8 KB	14/02/2014 09:37 AM	CC15388B2B0FC873F980FD5186348A05	31895FA91D7F353D0D301BE7900338891F4FFDAB	Yes	vwxyzabc03	AES-256
Graphic Image Sample 5.jpg	JPG File	17 KB	14/02/2014 09:37 AM	0A5FDA78D8389E821C71B9F2A092C802	1598FB0603F78987B58CF0A782449D8259157167	Yes	efghijklm4	AES-256
Graphic Image Sample 6.jpg	JPG File	58 KB	14/02/2014 09:37 AM	D2F7C6CA86E06FAA2DEA02D7DAF2972	A3550E9285239F679CA15929458314D3BAFC0D59	Yes	nopqrstuV5	AES-256
Graphic Image Sample 7.JPG	JPG File	2,001 KB	14/02/2014 09:37 AM	E9E03E7C8D5E3C1EAC344AD566F48CC	0534321762701F94876F8CAC0B29D0CD3B5C55E	Yes	wxyzabcde6	AES-256
Graphic Image Sample 8.JPG	JPG File	2,063 KB	14/02/2014 09:38 AM	FA50261640889197E2628689608F4332	9F558P95309239E4099DA97881A0848573081D0C	Yes	fg hijklmN7	AES-256
Graphic Image Sample 9.jpg	JPG File	155 KB	14/02/2014 09:38 AM	270657AAD13079248336C2E876E59ACA	349A534440B5715A3F256C02348BF9B08668745D	Yes	opqrstuVW8	AES-256
Graphic Image Sample 10.jpg	JPG File	143 KB	14/02/2014 09:38 AM	0685D1447E15A18A026EF75853147861	8665F89D1054858EEFD02A54D578FD2C57993A	Yes	wxyzabcde9	AES-256
Graphic Image Sample 11.jpg	JPG File	50 KB	14/02/2014 09:38 AM	822353567A04E1E66A4430B1786A05	FC829D3A74FE0E8879D85F9830343C04F8782	Yes	ghijklmno1	AES-256
JPG Carved File Sample 1.PNG	PNG File	4 KB	14/02/2014 09:38 AM	091523D16882626C765382708C2641DF	A59252A8A6EBD282F70A568318C259D2A775D03	Yes	pqrstuV2	AES-256
PDF Sample 1.pdf	Adobe Acrobat Document	12,466 KB	14/02/2014 09:39 AM	D51CEFF6D858FF681093A00C81F510F4	70FE205AB86443641AA77E2A9D07BAAD39853F	Yes	wxyzabcde3	AES-256
PDF Sample 2.pdf	Adobe Acrobat Document	78,432 KB	14/02/2014 09:39 AM	9810CFDE41BFF7E0DC48CC196A5D48C7	43109E07612ECAC6ADCA9A8688281136BA8548A9	Yes	fg hijklmN4	AES-256
PDF Sample 3.pdf	Adobe Acrobat Document	25,897 KB	14/02/2014 09:39 AM	8707A8B772EC57C81863D8A56EB579D5	F1725A9C766F78E179033858DB0C352F902A77	Yes	opqrstuW5	AES-256
PDF Sample 4.pdf	Adobe Acrobat Document	20,379 KB	14/02/2014 09:39 AM	6E6F8EF9F1A8C66B41538F54641F9045	D60ED70991389788200C3B370A459131A6E51160	Yes	xyzabcdeF6	AES-256
PDF Sample 5.pdf	Adobe Acrobat Document	24,145 KB	14/02/2014 09:40 AM	F0FBC1D0A77F2908EAC344E189383DA	5160219A2648482DEFF85D5E969C084A2E285D0F	Yes	ghijklmno7	AES-256
Text Document Sample 1.txt	Text Document	1 KB	14/02/2014 09:40 AM	B29824BE195842EADCE5E391170714F	FD40713A8FC6107724EA155C055A78A6A959E6D	Yes	pqrstuV8	AES-256
Text Document Sample 2.txt	Text Document	1 KB	14/02/2014 09:40 AM	05C0E4F79FA88248CE14FC93062E897	C4896B2950A0EB60E938A79B5C30EB0EFF496497	Yes	uvwxyzabc9	AES-256
Text Document Sample 3.txt	Text Document	1 KB	14/02/2014 09:40 AM	98737A889C24FE1515AD9C97720C687C54	7D1049242613314B744192D1EA00779881666C	Yes	defghijkl1	AES-256
Text Document Sample 4.txt	Text Document	1 KB	14/02/2014 09:40 AM	834E58E13C0240D4F1AEB818C7203AF	8B15948E032F441E34D2C3ADCF031475461C24D0	Yes	mnpqrstu2	AES-256
Text Document Sample 5.txt	Text Document	1 KB	14/02/2014 09:41 AM	F85250C7181038E3FDECA1E8318EA20	30CC79410AC0C69797F469D0E1A2E20DC8F264E0	Yes	vwxyzabcD3	AES-256
Word Document Sample 1.doc	Microsoft 97-2003 Document	22 KB	14/02/2014 09:41 AM	26388348D0CD58F738E2AD28F4460F38	8293FC6A29F753799E12AF867420584D307C5298	Yes	efghijklM4	AES-256
Word Document Sample 2.doc	Microsoft 97-2003 Document	22 KB	14/02/2014 09:41 AM	880288FA7F3BAA43C3E31820D842D	B0A4A4FC8791C204E4A8127B877848457B1AD91	Yes	nopqrstuV5	AES-256
Word Document Sample 3.doc	Microsoft 97-2003 Document	22 KB	14/02/2014 09:41 AM	C6898791B45AA4F974B6D03C77F771	CF870AC35086593446E0135455124D9095DAE1	Yes	wxyzabcde6	AES-256
Word Document Sample 4.doc	Microsoft 97-2003 Document	22 KB	14/02/2014 09:41 AM	C381FA40CCFCB1873879E7F37A0E07	8705FDDAD0773DCA06548C09CB1B0E7A3F808B1C	Yes	ghijklmno7	AES-256
Word Document Sample 5.doc	Microsoft 97-2003 Document	22 KB	14/02/2014 09:41 AM	ADB51367F7A8B1223145C7FE0CA0C0AD	7C337254E5E5D28887E08A17F451A61F80C1E547	Yes	pqrstuwx8	AES-256

Appendix 25: Table of AxCrypt “Stored Data” on VM1 (Double VMs Environment)

File Name	Type	Size	Timestamp
Encase File Sample 1-Ex01.axx	AXX File	849,672 KB	13/02/2014 06:59 PM
Encase File Sample 2-ex01.axx	AXX File	879,890 KB	13/02/2014 07:00 PM
Encase File Sample 3-E01.axx	AXX File	556 KB	13/02/2014 07:00 PM
Excel Sample File 1-xls.axx	AXX File	9 KB	13/02/2014 07:01 PM
Excel Sample File 2-xls.axx	AXX File	32 KB	13/02/2014 07:01 PM
Excel Sample File 3-xls.axx	AXX File	20 KB	13/02/2014 07:02 PM
Excel Sample File 4-xls.axx	AXX File	29 KB	13/02/2014 07:02 PM
Excel Sample File 5-xls.axx	AXX File	17 KB	13/02/2014 07:02 PM
Graphic Image Sample 1-jpg.axx	AXX File	19 KB	13/02/2014 07:03 PM
Graphic Image Sample 2-jpg.axx	AXX File	17 KB	13/02/2014 07:03 PM
Graphic Image Sample 3-jpg.axx	AXX File	10 KB	13/02/2014 07:03 PM
Graphic Image Sample 4-jpg.axx	AXX File	8 KB	13/02/2014 07:04 PM
Graphic Image Sample 5-jpg.axx	AXX File	17 KB	13/02/2014 07:04 PM
Graphic Image Sample 6-jpg.axx	AXX File	58 KB	13/02/2014 07:04 PM
Graphic Image Sample 7-JPG.axx	AXX File	2,001 KB	13/02/2014 07:05 PM
Graphic Image Sample 8-JPG.axx	AXX File	2,063 KB	13/02/2014 07:05 PM
Graphic Image Sample 9-jpg.axx	AXX File	155 KB	13/02/2014 07:05 PM
Graphic Image Sample 10-jpg.axx	AXX File	143 KB	13/02/2014 07:06 PM
Graphic Image Sample 11-jpg.axx	AXX File	50 KB	13/02/2014 07:06 PM
JPG Carved File Sample 1-PNG.axx	AXX File	4 KB	13/02/2014 07:06 PM
PDF Sample 1-pdf.axx	AXX File	12,466 KB	13/02/2014 07:49 PM
PDF Sample 2-pdf.axx	AXX File	68,437KB	13/02/2014 07:50 PM
PDF Sample 3-pdf.axx	AXX File	25,897 KB	13/02/2014 07:50 PM
PDF Sample 4-pdf.axx	AXX File	20,379 KB	13/02/2014 07:51 PM
PDF Sample 5-pdf.axx	AXX File	24,145 KB	13/02/2014 07:51 PM
Text Document Sample 1-txt.axx	AXX File	1 KB	13/02/2014 07:08 PM
Text Document Sample 2-txt.axx	AXX File	1 KB	13/02/2014 07:08 PM
Text Document Sample 3-txt.axx	AXX File	1 KB	13/02/2014 07:08 PM
Text Document Sample 4-txt.axx	AXX File	1 KB	13/02/2014 07:09 PM
Text Document Sample 5-txt.axx	AXX File	1 KB	13/02/2014 07:09 PM
Word Document Sample 1-doc.axx	AXX File	6 KB	13/02/2014 07:10 PM
Word Document Sample 2-doc.axx	AXX File	6 KB	13/02/2014 07:10 PM
Word Document Sample 3-doc.axx	AXX File	6 KB	13/02/2014 07:10 PM
Word Document Sample 4-doc.axx	AXX File	6 KB	13/02/2014 07:10 PM
Word Document Sample 5-doc.axx	AXX File	6 KB	13/02/2014 07:11 PM

Appendix 26: Table of AxCrypt “Stored Data” on VM2 (Double VMs Environment)

File Name	Type	Size	Timestamp
Encase File Sample 1-Ex01.axx	AXX File	849,672 KB	13/02/2014 05:59 PM
Encase File Sample 2-ex01.axx	AXX File	879,890 KB	13/02/2014 06:00 PM
Encase File Sample 3-E01.axx	AXX File	556 KB	13/02/2014 06:00 PM
Excel Sample File 1-xls.axx	AXX File	9 KB	13/02/2014 06:01 PM
Excel Sample File 2-xls.axx	AXX File	32 KB	13/02/2014 06:01 PM
Excel Sample File 3-xls.axx	AXX File	20 KB	13/02/2014 06:02 PM
Excel Sample File 4-xls.axx	AXX File	29 KB	13/02/2014 06:02 PM
Excel Sample File 5-xls.axx	AXX File	17 KB	13/02/2014 06:02 PM
Graphic Image Sample 1-jpg.axx	AXX File	19 KB	13/02/2014 06:03 PM
Graphic Image Sample 2-jpg.axx	AXX File	17 KB	13/02/2014 06:03 PM
Graphic Image Sample 3-jpg.axx	AXX File	10 KB	13/02/2014 06:03 PM
Graphic Image Sample 4-jpg.axx	AXX File	8 KB	13/02/2014 06:04 PM
Graphic Image Sample 5-jpg.axx	AXX File	17 KB	13/02/2014 06:04 PM
Graphic Image Sample 6-jpg.axx	AXX File	58 KB	13/02/2014 06:04 PM
Graphic Image Sample 7-JPG.axx	AXX File	2,001 KB	13/02/2014 06:05 PM
Graphic Image Sample 8-JPG.axx	AXX File	2,063 KB	13/02/2014 06:05 PM
Graphic Image Sample 9-jpg.axx	AXX File	155 KB	13/02/2014 06:05 PM
Graphic Image Sample 10-jpg.axx	AXX File	143 KB	13/02/2014 06:06 PM
Graphic Image Sample 11-jpg.axx	AXX File	50 KB	13/02/2014 06:06 PM
JPG Carved File Sample 1-PNG.axx	AXX File	4 KB	13/02/2014 06:06 PM
PDF Sample 1-pdf.axx	AXX File	12,466 KB	13/02/2014 06:49 PM
PDF Sample 2-pdf.axx	AXX File	68,437KB	13/02/2014 06:50 PM
PDF Sample 3-pdf.axx	AXX File	25,897 KB	13/02/2014 06:50 PM
PDF Sample 4-pdf.axx	AXX File	20,379 KB	13/02/2014 06:51 PM
PDF Sample 5-pdf.axx	AXX File	24,145 KB	13/02/2014 06:51 PM
Text Document Sample 1-txt.axx	AXX File	1 KB	13/02/2014 06:08 PM
Text Document Sample 2-txt.axx	AXX File	1 KB	13/02/2014 06:08 PM
Text Document Sample 3-txt.axx	AXX File	1 KB	13/02/2014 06:08 PM
Text Document Sample 4-txt.axx	AXX File	1 KB	13/02/2014 06:09 PM
Text Document Sample 5-txt.axx	AXX File	1 KB	13/02/2014 06:09 PM
Word Document Sample 1-doc.axx	AXX File	6 KB	13/02/2014 06:10 PM
Word Document Sample 2-doc.axx	AXX File	6 KB	13/02/2014 06:10 PM
Word Document Sample 3-doc.axx	AXX File	6 KB	13/02/2014 06:10 PM
Word Document Sample 4-doc.axx	AXX File	6 KB	13/02/2014 06:10 PM

Appendix 27: Table of AxCrypt “Retrieved Data” from VM2 (Double VMs Environment)

File Name	Type	Size	Timestamp	MD5 Value	SHA-1 Value
Encase File Sample 1-Ex01.axx	AxCrypt Encrypted File	849,672 KB	13/02/2014 06:59 PM	E66461D4885E2F31DD6D6751FD2B41E9	AA2D8B47B59886E6C2DCB47FA01B4C5DCA1815A4
Encase File Sample 2-ex01.axx	AxCrypt Encrypted File	879,890 KB	13/02/2014 07:00 PM	B1003F33735CF978831C7EE08ED65350	0FA1F43D445AC5CF2C8C596306138E8DCC3BC10
Encase File Sample 3-E01.axx	AxCrypt Encrypted File	556 KB	13/02/2014 07:00 PM	5D4D4D0360DEA07274FCF854DAA2E06F	7C16E8F99EB8041BC4D1D22382823183C5B083D39
Excel Sample File 1-xls.axx	AxCrypt Encrypted File	9 KB	13/02/2014 07:01 PM	C6527369663AF9A90DC89E2AE083C4F5	572AA538EB4EA88315C3EB6806C48D5E5D89506
Excel Sample File 2-xls.axx	AxCrypt Encrypted File	32 KB	13/02/2014 07:01 PM	66130F5EAC908E58FDB8CFB2C6F292ADC	A69E340C7D240F8871988FFABF67D934F5F83D0
Excel Sample File 3-xls.axx	AxCrypt Encrypted File	20 KB	13/02/2014 07:02 PM	5606346700F319B8E5A08385ED54802F	D2FF4B1D9CDE493434DBCB49FF4582C8888B4C6
Excel Sample File 4-xls.axx	AxCrypt Encrypted File	29 KB	13/02/2014 07:02 PM	EE089A190D8E46E1D3EDB17E1C205014	5009927550FF823EDC1CB3573FAF1918D9363AC
Excel Sample File 5-xls.axx	AxCrypt Encrypted File	17 KB	13/02/2014 07:02 PM	A8C4D7AE1F812667838D666399146366	F23400126AFF985BE1A1DE3F78CD43307AD63439
Graphic Image Sample 1-jpg.axx	AxCrypt Encrypted File	19 KB	13/02/2014 07:03 PM	6C84D9B14E33FF72D7AA0B68D4BF676C	C1678CAB97E1359A8414DBDE5E82A8D6C19BC33C
Graphic Image Sample 2-jpg.axx	AxCrypt Encrypted File	17 KB	13/02/2014 07:03 PM	7165530F346708EF29856505EEF712A8	81107D1DEFEDEA59F7B12ACFCB3087D0C49E853B
Graphic Image Sample 3-jpg.axx	AxCrypt Encrypted File	10 KB	13/02/2014 07:03 PM	91319B88A562E8381856D8049035E3513	2AC4F8E376999754F370C47C86300C5A9F2F4B
Graphic Image Sample 4-jpg.axx	AxCrypt Encrypted File	8 KB	13/02/2014 07:04 PM	3F0F4E90EF563133CA5FD1B242C3034A	75EBED4DC3537FA23F4E3FC517626DC422D34878
Graphic Image Sample 5-jpg.axx	AxCrypt Encrypted File	17 KB	13/02/2014 07:04 PM	306F8A7BA597DC449AA28E2995FEA950	D820BAFA36856CF046B7F1F282C862D8316315F8
Graphic Image Sample 6-jpg.axx	AxCrypt Encrypted File	58 KB	13/02/2014 07:04 PM	569A61D96FDB8E42E0E22AFC6DCE6A6A	AA41F28A51A42C888CF9481D8585A36F4884EAC5
Graphic Image Sample 7-jpg.axx	AxCrypt Encrypted File	2,001 KB	13/02/2014 07:05 PM	34F08FDA3250F135D70A511681BD366C	53201208588E80A4625FB5C73FD965975BA0DB85
Graphic Image Sample 8-jpg.axx	AxCrypt Encrypted File	2,063 KB	13/02/2014 07:05 PM	EDF98E380D51978888F910508C9986F	24D8FD388C55A9989902C9A1E200FE5D4A1484F
Graphic Image Sample 9-jpg.axx	AxCrypt Encrypted File	155 KB	13/02/2014 07:05 PM	A8F253046143441CC26A22968F73C6C7	8B86337390180CFF7EC9CA2C9A0AE4F046927E3
Graphic Image Sample 10-jpg.axx	AxCrypt Encrypted File	143 KB	13/02/2014 07:06 PM	047A84FE66FD6410E31FE0403C6FC695	EF58C8E779C1D94E47C4D133CE58D92D200D5D4C
Graphic Image Sample 11-jpg.axx	AxCrypt Encrypted File	50 KB	13/02/2014 07:06 PM	C5DD06C3F71A8702E830C28808F54AFC	076AA52A2C2D617018F9EB8FC28319C37DEB04742
JPG Carved File Sample 1-PNG.axx	AxCrypt Encrypted File	4 KB	13/02/2014 07:06 PM	EC62EC8849175C5CC4D9A5407B2B2606	F6C9C9C163457DA02938124A98C5028ABD575B1A
PDF Sample 1-pdf.axx	AxCrypt Encrypted File	12,466 KB	13/02/2014 07:49 PM	6B C5F8229FEA06094ACFFCAE669D35B	2361F2036FE741E6F30D8A56894080945180857C
PDF Sample 2-pdf.axx	AxCrypt Encrypted File	68,437KB	13/02/2014 07:50 PM	8DF51C3D0221A47CC467122106466066	EDE5B7B0EA26AE4D6465A5D2806AD0F42793883A
PDF Sample 3-pdf.axx	AxCrypt Encrypted File	25,897 KB	13/02/2014 07:50 PM	4F5E98A2D6ED1A8BA59A94AF0BFC9724	B4194AC96C275E82B866263F1AD6A7EF6C65ADA1
PDF Sample 4-pdf.axx	AxCrypt Encrypted File	20,379 KB	13/02/2014 07:51 PM	39906B439918C6C6A1C5D0D0882056358	7D91466FD498D7B1FC10DF69A58950D8F9A2BBE1
PDF Sample 5-pdf.axx	AxCrypt Encrypted File	24,145 KB	13/02/2014 07:51 PM	C836F8A33EAE7A0686DFC99628EEF18F	0A2408D5F1557E0983D896DA3D5E7F089207D596
Text Document Sample 1-txt.axx	AxCrypt Encrypted File	1 KB	13/02/2014 07:08 PM	4F081272B5D0DAD8F698E6981879870	44E651252585E9D95516AFA2689DAAD284571788
Text Document Sample 2-txt.axx	AxCrypt Encrypted File	1 KB	13/02/2014 07:08 PM	2B64ED74822789AECF81E05C87F84A8	78D62C59246A341E7E7FE69E9C2887F256A3649F
Text Document Sample 3-txt.axx	AxCrypt Encrypted File	1 KB	13/02/2014 07:08 PM	BF09AGA2EE0F3057D9222B5F5A5978303	C979884C5F0C17082EDA398D173C4E715E4572FF
Text Document Sample 4-txt.axx	AxCrypt Encrypted File	1 KB	13/02/2014 07:09 PM	3F0F4E90EF563133CA5FD1B242C3034A	75EBED4DC3537FA23F4E3FC517626DC422D34878
Text Document Sample 5-txt.axx	AxCrypt Encrypted File	1 KB	13/02/2014 07:09 PM	B3B09CC6BEB15897DC4886188D80380D	1A792FF764A91B71EE67E828F3CD5844F20CF16E
Word Document Sample 1-doc.axx	AxCrypt Encrypted File	6 KB	13/02/2014 07:10 PM	6A4D950330A82EA09390FB135220C910	A76F17E91AF19057A61CF388C091D683FF5FE699
Word Document Sample 2-doc.axx	AxCrypt Encrypted File	6 KB	13/02/2014 07:10 PM	71A9D9E948155A8780D77A8807E408BCA	CA1619CC953A54558FB279EA55EEFFD6216FC41D
Word Document Sample 3-doc.axx	AxCrypt Encrypted File	6 KB	13/02/2014 07:10 PM	0695DDF321DB98E06453DC05B08E7B3F	08B087D758DE067499AFE41997A88FD7452D6FB
Word Document Sample 4-doc.axx	AxCrypt Encrypted File	6 KB	13/02/2014 07:10 PM	437777E67F520371792F99423CE91B	98CC8F685856A3751D88941AADCDC9CA006DF04D4
Word Document Sample 5-doc.axx	AxCrypt Encrypted File	6 KB	13/02/2014 07:11 PM	D0624DC02CF8973C44B48DF7F891E56	C63F7699C8676DE0B80F8C4A00A445CC5F5A31F

Appendix 28: Table of AxCrypt “Recovered Data” from VM2 (Double VMs Environment)

File Name	Type	Size	Timestamp	MD5 Value	SHA-1 Value	Successful Decryption	Secret Key	Algorithm
Encase File Sample 1.Ex01	EnCase Evidence File	849,671 KB	29/06/2011 10:29 AM	59999CEAE097DA53375F280FD1A4526	4EC98E57076FA5EC23E07F05431EE0C5AACAD9	Yes	abcde1gh1	AES-128
Encase File Sample 2.ex01	EnCase Evidence File	879,889 KB	28/11/2012 03:06 PM	372D42D8023238895E4187F12561DFB0	407AA23CCEDE93089A146CC0BF56875E33C0D358F	Yes	klmnopqr2	AES-128
Encase File Sample 3.E01	EnCase Evidence File	556 KB	04/04/2013 08:48 PM	01186AAC9D373208279C8CB264C5023	842AA4CDB1A2CB76DCE6340761BD48547483082EC	Yes	stuvwxy243	AES-128
Excel Sample File 1.xls	Microsoft Excel 97-2003 Worksheet	36 KB	16/05/2013 08:41 PM	2C938882AA00C51721B52807A1F3DDCF	A838C97CA08BC350256A69178DE57C808289B2680	Yes	bcde1ghu4	AES-128
Excel Sample File 2.xls	Microsoft Excel 97-2003 Worksheet	148 KB	17/06/2005 11:38 AM	5637DFCA6A63987176E86A20171F47FF	10A0A707D929954072E75FE4E276F5D12E184AA	Yes	klmnopqr55	AES-128
Excel Sample File 3.xls	Microsoft Excel 97-2003 Worksheet	69 KB	17/06/2005 11:39 AM	81A2A3D1F544AC2C7658D05A29D1962E5	21C77EDCA8640EACAGCE1709C34E3168D81238C44	Yes	tuvwxyzab6	AES-128
Excel Sample File 4.xls	Microsoft Excel 97-2003 Worksheet	189 KB	17/06/2005 11:40 AM	C219F963A0553648CE6881D352EDEE4	CDEF495E16852F960199D9B4E330773FF3080AC18	Yes	cde1ghijk7	AES-128
Excel Sample File 5.xls	Microsoft Excel 97-2003 Worksheet	89 KB	17/06/2005 11:41 AM	0A5FDA78D8389EB2C771BF92A092C8D2	1599F806D3F78987B58CF0A7B2449D8259157167	Yes	lmnopqr58	AES-128
Graphic Image Sample 1.jpg	JPG File	31 KB	08/02/2008 03:44 PM	9DD874080781688787AE184882C36D65A	44973E2CG04D68FBFB027C0A4CB4906ABD460C	Yes	uvwxyzabc9	AES-128
Graphic Image Sample 2.jpg	JPG File	16 KB	22/01/2014 11:12 AM	8CF8106B04AC1037A74761C8275D376D0	C7228E068A1D9681C0184462DA9AE6CDFC8289E	Yes	defghijkL1	AES-128
Graphic Image Sample 3.jpg	JPG File	10 KB	22/01/2014 11:13 AM	AA7AE3E36810DF9B8C0DCDE68CF696AC3	0F0F3FCFE587A4D0FC9366F8D8A867AF1A125581C	Yes	mnopqrstU2	AES-128
Graphic Image Sample 4.jpg	JPG File	8 KB	22/01/2014 11:13 AM	CC1538882B0FC873F980FD518G3484D5	31895FA91D7F353D0D3018F7900538891F4FDBAB	Yes	vwxyzabcD3	AES-128
Graphic Image Sample 5.jpg	JPG File	17 KB	22/01/2014 11:14 AM	0A5FDA78D8389EB2C771BF92A092C8D2	1599F806D3F78987B58CF0A7B2449D8259157167	Yes	efghijkM4	AES-128
Graphic Image Sample 6.jpg	JPG File	57 KB	12/07/2005 01:14 AM	D2F1CGCAABE86FAA2DEA02D7DAF2972	A3550F9285239F679CA15928458314D38AF8D59	Yes	nopqrstuV5	AES-128
Graphic Image Sample 7.JPG	JPG File	2,001 KB	03/09/2009 12:20 PM	E9E03E70BD553CE1EAC4344A0566F48CC	0534321762701F94876F8CA08290C01D385C55E	Yes	vwxyzabcE6	AES-128
Graphic Image Sample 8.JPG	JPG File	2,063 KB	18/03/2009 09:06 AM	FA50261640889197E26286960BDF4332	9F558F95309239FA0990A978B1A0848573081DDC	Yes	fghijkmN7	AES-128
Graphic Image Sample 9.jpg	JPG File	155 KB	10/01/2010 12:08 PM	270657A0D13079248356C2E876E594CA	349A54440B5715A3F256C02348F9808668745D	Yes	opqrstuW8	AES-128
Graphic Image Sample 10.jpg	JPG File	143 KB	15/05/2012 03:43 PM	068SD1447E15A18A026FEF25853147B61	8E65F98D10554858FEFD02A54D578FD325993A	Yes	wxyzabcE9	AES-128
Graphic Image Sample 11.jpg	JPG File	50 KB	21/11/1999 04:48 PM	822339567404DE1E16644A3081786A05	FC929D3A74FE9E8879085FE9383048AC04FB782	Yes	ghijkmNO1	AES-128
PGP Carved File Sample 1.PNG	PNG File	3 KB	09/05/2012 04:53 PM	091523D16882626C765382708C2641DF	A59252A846E8D28F70A5688318CB3259D2175D03	Yes	pqrstuV2	AES-128
PDF Sample 1.pdf	Adobe Acrobat Document	12,466 KB	07/05/2011 02:15 PM	D51CEFE6D858FF681093A00C81F510F4	70FE205A8B6443641AA77E2A80D7BADC439853F	Yes	vwxyzabcE3	AES-128
PDF Sample 2.pdf	Adobe Acrobat Document	78,432 KB	07/05/2011 02:28 PM	9810CF0E41BFF7E10DC48C196A5D48C7	43109E07612ECAACAD9AA06882813368A854849	Yes	fghijkmN4	AES-128
PDF Sample 3.pdf	Adobe Acrobat Document	25,897 KB	07/05/2011 02:17 PM	8707A8B772CE7C818638A56E8579D5	F1725A9C766F78E179033858D80C635F9027A77	Yes	opqrstuW5	AES-128
PDF Sample 4.pdf	Adobe Acrobat Document	20,379 KB	07/05/2011 01:11 PM	6E68E19F1A8C66841538F54641F9045	D6DE07091389788200C383704A59131A6E5116D	Yes	xyzabcE6	AES-128
PDF Sample 5.pdf	Adobe Acrobat Document	24,144 KB	07/05/2011 01:11 PM	F0FBC1D4047727908EDC34AE189583DA	5160719A246487482DEF8D5F969C0884E2B5D0F	Yes	ghijkmNO7	AES-128
Text Document Sample 1.txt	Text Document	1 KB	22/01/2014 11:58 AM	8293824BE195842EAC05EE39170714F	FD4D713A8FC610F724EA15ECCD55A7B64E93966D	Yes	pqrstuV8	AES-128
Text Document Sample 2.txt	Text Document	1 KB	22/01/2014 11:59 AM	98737A8B9C244FE15AD9C97720C687C54	C4B96825050AE86D9E918A79B5C30E0BEF1496497	Yes	uvwxyzabc9	AES-128
Text Document Sample 3.txt	Text Document	1 KB	22/01/2014 11:59 AM	98737A8B9C244FE15AD9C97720C687C54	7D10492426133148744192D1EAU00779881668C	Yes	defghijkL1	AES-128
Text Document Sample 4.txt	Text Document	1 KB	22/01/2014 12:00 PM	834E5BE13C024004FAEEB1BC7E205AF	8815948E0D32F441E34D2C3AD0E03175461C24DD	Yes	mnopqrstu2	AES-128
Text Document Sample 5.txt	Text Document	1 KB	22/01/2014 12:01 PM	F85B250C718103BCE3FDECA1E8318FA20	3DC79410AC0C6979FA69DDE1A2E2D0CB26AE0	Yes	vwxyzabcD3	AES-128
Word Document Sample 1.doc	Microsoft 97-2003 Document	22 KB	22/01/2014 11:53 AM	2638834BD0DC05B8738E2AD28B446D938	8293FC629F75799E12AF8674D0584D307C5298	Yes	efghijkM4	AES-128
Word Document Sample 2.doc	Microsoft 97-2003 Document	22 KB	22/01/2014 11:53 AM	880288FAF7E3B4A43C3E3182D08A2A2D	8DAA44FCF791C204E4A8F127B877948A57B1AD91	Yes	nopqrstuV5	AES-128
Word Document Sample 3.doc	Microsoft 97-2003 Document	22 KB	22/01/2014 11:53 AM	C6B898791045A4AF974B6D03C777771	CF8870AC35086593F44E6D13C4551A2D9095DAE1	Yes	vwxyzabcE6	AES-128
Word Document Sample 4.doc	Microsoft 97-2003 Document	22 KB	22/01/2014 11:54 AM	C381FA0CCFCB1E8738797E737A0E07	8705FDDA0D773DC0A56548C89CBDE7AF6E808B1C	Yes	fghijkmNO7	AES-128
Word Document Sample 5.doc	Microsoft 97-2003 Document	22 KB	22/01/2014 12:02 PM	A0B5136F7E4881223145C7FE0ACDDAD	7C33F734E5D28887E0BA17451A61FB0C1E547	Yes	pqrstuwwx8	AES-128

Appendix 29: Table of AESTool “Stored Data” on VM1 (Double VMs Environment)

File Name	Type	Size	Timestamp
AES Encase File Sample 1	Application	850,013 KB	13/02/2014 11:29 PM
AES Encase File Sample 2	Application	880,231 KB	13/02/2014 11:35 PM
AES Encase File Sample 3	Application	898 KB	13/02/2014 11:35 PM
AES Excel Sample File 1	Application	378 KB	13/02/2014 11:35 PM
AES Excel Sample File 2	Application	490 KB	13/02/2014 11:36 PM
AES Excel Sample File 3	Application	411 KB	13/02/2014 11:36 PM
AES Excel Sample File 4	Application	531 KB	13/02/2014 11:37 PM
AES Excel Sample File 5	Application	431 KB	13/02/2014 11:37 PM
AES Graphic Image Sample 1	Application	373 KB	13/02/2014 11:37 PM
AES Graphic Image Sample 2	Application	358 KB	13/02/2014 11:38 PM
AES Graphic Image Sample 3	Application	351 KB	13/02/2014 11:38 PM
AES Graphic Image Sample 4	Application	349 KB	13/02/2014 11:38 PM
AES Graphic Image Sample 5	Application	358 KB	13/02/2014 11:38 PM
AES Graphic Image Sample 6	Application	399 KB	13/02/2014 11:39 PM
AES Graphic Image Sample 7	Application	2,342 KB	13/02/2014 11:39 PM
AES Graphic Image Sample 8	Application	2,404 KB	13/02/2014 11:39 PM
AES Graphic Image Sample 9	Application	497 KB	13/02/2014 11:39 PM
AES Graphic Image Sample 10	Application	485 KB	13/02/2014 11:40 PM
AES Graphic Image Sample 11	Application	391 KB	13/02/2014 11:40 PM
AES JPG Carved File Sample 1	Application	345 KB	13/02/2014 11:40 PM
AES PDF Sample 1.pdf	Application	12,808 KB	13/02/2014 11:41 PM
AES PDF Sample 2.pdf	Application	78,773 KB	13/02/2014 11:41 PM
AES PDF Sample 3.pdf	Application	26,238 KB	13/02/2014 11:41 PM
AES PDF Sample 4.pdf	Application	20,720 KB	13/02/2014 11:41 PM
AES PDF Sample 5.pdf	Application	24,486 KB	13/02/2014 11:42 PM
AES Text Document Sample 1	Application	342 KB	13/02/2014 11:42 PM
AES Text Document Sample 2	Application	342 KB	13/02/2014 11:42 PM
AES Text Document Sample 3	Application	342 KB	13/02/2014 11:43 PM
AES Text Document Sample 4	Application	342 KB	13/02/2014 11:43 PM
AES Text Document Sample 5	Application	342 KB	13/02/2014 11:43 PM
AES Word Document Sample 1	Application	364 KB	13/02/2014 11:43 PM
AES Word Document Sample 2	Application	364 KB	13/02/2014 11:44 PM
AES Word Document Sample 3	Application	364 KB	13/02/2014 11:44 PM
AES Word Document Sample 4	Application	364 KB	13/02/2014 11:44 PM
AES Word Document Sample 5	Application	364 KB	13/02/2014 11:44 PM

Appendix 30: Table of AESTool “Stored Data” on VM2 (Double VMs Environment)

File Name	Type	Size	Timestamp
AES Encase File Sample 1	Application	850,013 KB	13/02/2014 10:29 PM
AES Encase File Sample 2	Application	880,231 KB	13/02/2014 10:35 PM
AES Encase File Sample 3	Application	898 KB	13/02/2014 10:35 PM
AES Excel Sample File 1	Application	378 KB	13/02/2014 10:35 PM
AES Excel Sample File 2	Application	490 KB	13/02/2014 10:36 PM
AES Excel Sample File 3	Application	411 KB	13/02/2014 10:36 PM
AES Excel Sample File 4	Application	531 KB	13/02/2014 10:37 PM
AES Excel Sample File 5	Application	431 KB	13/02/2014 10:37 PM
AES Graphic Image Sample 1	Application	373 KB	13/02/2014 10:37 PM
AES Graphic Image Sample 2	Application	358 KB	13/02/2014 10:38 PM
AES Graphic Image Sample 3	Application	351 KB	13/02/2014 10:38 PM
AES Graphic Image Sample 4	Application	349 KB	13/02/2014 10:38 PM
AES Graphic Image Sample 5	Application	358 KB	13/02/2014 10:38 PM
AES Graphic Image Sample 6	Application	399 KB	13/02/2014 10:39 PM
AES Graphic Image Sample 7	Application	2,342 KB	13/02/2014 10:39 PM
AES Graphic Image Sample 8	Application	2,404 KB	13/02/2014 10:39 PM
AES Graphic Image Sample 9	Application	497 KB	13/02/2014 10:39 PM
AES Graphic Image Sample 10	Application	485 KB	13/02/2014 10:40 PM
AES Graphic Image Sample 11	Application	391 KB	13/02/2014 10:40 PM
AES JPG Carved File Sample 1	Application	345 KB	13/02/2014 10:40 PM
AES PDF Sample 1.pdf	Application	12,808 KB	13/02/2014 10:41 PM
AES PDF Sample 2.pdf	Application	78,773 KB	13/02/2014 10:41 PM
AES PDF Sample 3.pdf	Application	26,238 KB	13/02/2014 10:41 PM
AES PDF Sample 4.pdf	Application	20,720 KB	13/02/2014 10:41 PM
AES PDF Sample 5.pdf	Application	24,486 KB	13/02/2014 10:42 PM
AES Text Document Sample 1	Application	342 KB	13/02/2014 10:42 PM
AES Text Document Sample 2	Application	342 KB	13/02/2014 10:42 PM
AES Text Document Sample 3	Application	342 KB	13/02/2014 10:43 PM
AES Text Document Sample 4	Application	342 KB	13/02/2014 10:43 PM
AES Text Document Sample 5	Application	342 KB	13/02/2014 10:43 PM
AES Word Document Sample 1	Application	364 KB	13/02/2014 10:43 PM
AES Word Document Sample 2	Application	364 KB	13/02/2014 10:44 PM
AES Word Document Sample 3	Application	364 KB	13/02/2014 10:44 PM
AES Word Document Sample 4	Application	364 KB	13/02/2014 10:44 PM
AES Word Document Sample 5	Application	364 KB	13/02/2014 10:44 PM

Appendix 31: Table of AESTool “Retrieved Data” from VM2 (Double VMs Environment)

File Name	Type	Size	Timestamp	MD5 Value	SHA-1 Value
Encase File Sample 1.exe	Application	850,013 KB	13/02/2014 11:29 PM	A1F96B13E979168E3019F7C722560253	AB42310D7B71F6E4A54A8FE3E735C032798D95EE
Encase File Sample 2.exe	Application	880,231 KB	13/02/2014 11:35 PM	996B9B3DA2FB0ACEA1FEC5828581B80	9552D0A98CC9C5437E8AABF860C621BFC93E6F7D
Encase File Sample 3.exe	Application	898 KB	13/02/2014 11:35 PM	01421216B8F510B9F421D4E691F78124E	8533A84B7231F0C3C76904CFB9C6014B21C6DFB7
Excel Sample File 1.exe	Application	378 KB	13/02/2014 11:35 PM	00CF104B7F441868DC090F6FE1BE1D54	7CC3D2112D0D3217837D578E16AC75C17049F2178
Excel Sample File 2.exe	Application	490 KB	13/02/2014 11:36 PM	AAE56C7ADEEDA54D7B21807973C2550	7B0077169D98A227182693686EFF57A36976E1D
Excel Sample File 3.exe	Application	411 KB	13/02/2014 11:36 PM	BF307088D01E5F56613B52D2DA513317	AA96B788555F1732E258994F450328B16F415693
Excel Sample File 4.exe	Application	531 KB	13/02/2014 11:37 PM	25ED89BE8B91E958CF3E22FFD51DF4E4	8C548D87BFCBEC5453822C1F38843307339EAA9D
Excel Sample File 5.exe	Application	431 KB	13/02/2014 11:37 PM	50B845D5C913A778191921FCDAAFA08	D3A4E0F78F8FD124DDB7A9C7FA99CDBD53E17FE
Graphic Image Sample 1.exe	Application	373 KB	13/02/2014 11:37 PM	C8E4C03281008B8186F926D9F1EA39403	9D61DF08F66E02F3ECB433807AAC5967015EE2E
Graphic Image Sample 2.exe	Application	358 KB	13/02/2014 11:38 PM	3C3AD4EAD198DAFCA9D979615C8B144D	C20D6E63A23F8EB3A1516A171667F4FC2687B807
Graphic Image Sample 3.exe	Application	351 KB	13/02/2014 11:38 PM	1D21EAD57C30F3E701D6D7276B88ADBC	1DBCC883AD302F5D30AD8FBCCD1FEB38FF9F2F05
Graphic Image Sample 4.exe	Application	349 KB	13/02/2014 11:38 PM	16B1B7F497C075951AC1BE12456EA424	3E83DCD58E8EB29A1432DD117F2C28C5D52A7768
Graphic Image Sample 5.exe	Application	358 KB	13/02/2014 11:38 PM	A07EF50F835966E4852DAD8D3D4E541BC	A9126477A4B2DAF81BD2598EB269A8EC8103FFE1
Graphic Image Sample 6.exe	Application	399 KB	13/02/2014 11:39 PM	5A19FC6122488B648F81C37C981E5161A	2A0D5C3CEC60C05588623FE7283B725FB113A37E
Graphic Image Sample 7.exe	Application	2,342 KB	13/02/2014 11:39 PM	767D519E9A81BAC989696A1412FB4E44	02B84DD499D1F14F27466E7162903DE7C76738EC
Graphic Image Sample 8.exe	Application	2,404 KB	13/02/2014 11:39 PM	881C91DC63276836A60B8D8E145D85C71	8CFFCC5F49F34A527C56455DD682E111C83DC3F
Graphic Image Sample 9.exe	Application	497 KB	13/02/2014 11:39 PM	2785DE0A7224C620EE038F83A5C81C16	CAS8DBCC93CD88DEA0DE6CC727C84D37CEE44D2F9
Graphic Image Sample 10.exe	Application	485 KB	13/02/2014 11:40 PM	4C0FAFEA1BCD92594E922B087C7FE1897	6FC405013D197948C9088B2F383121AAA29541D
Graphic Image Sample 11.exe	Application	391 KB	13/02/2014 11:40 PM	31C4650C41C4836FAFBFA3710AA242C	D0717DB15684687CA696D056C363754552392947
JPG Carved File Sample 1.exe	Application	345 KB	13/02/2014 11:40 PM	93DEE41DC614DD0D8C81FC1BA30617316	2727B0C867FE44ED172665D8989DA40E2329837C
PDF Sample 1.pdf.exe	Application	12,808 KB	13/02/2014 11:41 PM	84D337AE2266ECEE0810AE337A1DEC8B9	5E70B2554407667428AA9CDB11EECA24C18B360E
PDF Sample 2.pdf.exe	Application	78,773 KB	13/02/2014 11:41 PM	9AC84AFE1BF90DFB8899190C3BFB56AC	6A2A20147DCC502E57E5C72A6E5CD3C36F80D75
PDF Sample 3.pdf.exe	Application	26,238 KB	13/02/2014 11:41 PM	82E0C172BA53572ADA81E8AE939F6A43	84AB50EA17DCB833FBA0A982573515838E6F4B4D3
PDF Sample 4.pdf.exe	Application	20,720 KB	13/02/2014 11:41 PM	2AE9F73C06D1D8C480C7A1FBCAFE0A92	CD568C4503615B6E3422819DA98269A0E0C88A33
PDF Sample 5.pdf.exe	Application	24,486 KB	13/02/2014 11:42 PM	271198DD04E60A2706AA294CED8FB2CE	4A4753577DD98545DA79D227E8D79FDF516621F
Text Document Sample 1.exe	Application	342 KB	13/02/2014 11:42 PM	1D55BF133737877303A8CFC29345513	3B22EC157ABFD118B706DDEF48FE15C8D65B0B68
Text Document Sample 2.exe	Application	342 KB	13/02/2014 11:42 PM	03C6657F5FDF004A20CA39E16CDA684FC	C27896D1320E1892FA889BA82B6178EC182691B7
Text Document Sample 3.exe	Application	342 KB	13/02/2014 11:43 PM	AA655ADAC03315FB2591E18011D2D0F1	B9F912D9A9B76D154C0EA9B2B9FC26868851A222
Text Document Sample 4.exe	Application	342 KB	13/02/2014 11:43 PM	2AE9F73C06D1D8C480C7A1FBCAFE0A92	CD568C4503615B6E3422819DA98269A0E0C88A33
Text Document Sample 5.exe	Application	342 KB	13/02/2014 11:43 PM	A1C80CA7A6C6AAEC5C3AE363316F4C69	8CBA3A4E37A3C050A104ADCG1ED161C96202007D
Word Document Sample 1.exe	Application	364 KB	13/02/2014 11:43 PM	B4078169F5BFAA31E0B491FFE3DD1D0F	16E8A1A778689CAE3E0FF2BF9E7B5888A5DC1CFF
Word Document Sample 2.exe	Application	364 KB	13/02/2014 11:44 PM	252D48A0A2E9F4E55C1FABE6493C8A0	54C08020F8837B9961600673E2C7E613F5E56D75
Word Document Sample 3.exe	Application	364 KB	13/02/2014 11:44 PM	AA655ADAC03315FB2591E18011D2D0F1	B9F912D9A9B76D154C0EA9B2B9FC26868851A222
Word Document Sample 4.exe	Application	364 KB	13/02/2014 11:44 PM	F5790A28DAA3DF80668FCCE23276E13	94D45E6A2D645240C7D582615A31E785DE1AE02D
Word Document Sample 5.exe	Application	364 KB	13/02/2014 11:44 PM	1A8F3D825F6B4F3388EAEADD2F23EB3	88FFB3DD0A2986526F3790AF44CF9222AADB48A9

Appendix 32: Table of AESTool “Recovered Data” from VM2 (Double VMs Environment)

File Name	Type	Size	Timestamp	MDS Value	SHA-1 Value	Successful Decryption	Secret Key	Algorithm
Encase File Sample 1.ex01	Encase Evidence File	849,671 KB	14/02/2014 02:21 PM	5999BCAE0E97D53375F2808FD1A4526	4EC9B5E7076FA5EC23E07D05431E0CFC5ACAE9D	Yes	ABCEDEF1	AES-64
Encase File Sample 2.ex01	Encase Evidence File	879,889 KB	14/02/2014 02:22 PM	372D42D8022328893E4A187F12561DFB0	401A423CCED930B9A146C08F56B7533C0D358F	Yes	ABCEDEF1	AES-64
Encase File Sample 3.ex01	Encase Evidence File	556 KB	14/02/2014 02:22 PM	01186ACAC490373208279C8C8264C5023	B42A4ACD81A2C876D0E6340761BD48457A830B2EC	Yes	ABCEDEF1	AES-64
Excel Sample File 1.xls	Microsoft Excel 97-2003 Worksheet	36 KB	14/02/2014 02:23 PM	2C938882A40C051771B52B0FA1F3DDCF	A83BC97CA88CD50A26A69178D5F2C808289B2680	Yes	ABCEDEF1	AES-64
Excel Sample File 2.xls	Microsoft Excel 97-2003 Worksheet	148 KB	14/02/2014 02:23 PM	5637DFCA6A639B716E66A20171E47FF	10A04707D9299540772E2F5FE42765D012E184AA	Yes	ABCEDEF1	AES-64
Excel Sample File 3.xls	Microsoft Excel 97-2003 Worksheet	69 KB	14/02/2014 02:23 PM	B1A2A3D1F54A0C72658D0D529D196E5	21C77FEDC4B6A0FCAC6CE1705C343168D81238CA4	Yes	ABCEDEF1	AES-64
Excel Sample File 4.xls	Microsoft Excel 97-2003 Worksheet	189 KB	14/02/2014 02:23 PM	C2193F663A055364FCE6881D352E D0E4	CDFA95E16852F960199D984E30773F3080AC18	Yes	ABCEDEF1	AES-64
Excel Sample File 5.xls	Microsoft Excel 97-2003 Worksheet	89 KB	14/02/2014 02:23 PM	0A5FDA7808389EB21C718F92A093C8D2	159BF800D3F78987B5BCF0A7B2A49D8259157167	Yes	ABCEDEF1	AES-64
Graphic image Sample 1.jpg	JPG File	31 KB	14/02/2014 02:23 PM	9DD674080781688787AEB4882C36D65A	4A973E2C6D04D668FBFB027C0A4CB4906EABD460C	Yes	ABCEDEF1	AES-64
Graphic image Sample 2.jpg	JPG File	16 KB	14/02/2014 02:24 PM	8CFB10680A4C1017A744628751D376D0	C7228E068A1D9681C01844620A9AE6C0F4C8269E	Yes	ABCEDEF1	AES-64
Graphic image Sample 3.jpg	JPG File	10 KB	14/02/2014 02:24 PM	AA74E2E368100FF98C0CD668CF696AC3	0F60F38CFE587A0DFC9C916F8D0A867AF1D25581C	Yes	ABCEDEF1	AES-64
Graphic image Sample 4.jpg	JPG File	8 KB	14/02/2014 02:24 PM	CC153888280FC873F980FD51B63484D5	31895FA91D7F33D003018F7900538891F4FFDAB	Yes	ABCEDEF1	AES-64
Graphic image Sample 5.jpg	JPG File	17 KB	14/02/2014 02:24 PM	1A55258C59F37D0ADA2916645458013	A9F560E8F3C196AA1AAE0456907EE7BA00D5BD	Yes	ABCEDEF1	AES-64
Graphic image Sample 6.jpg	JPG File	57 KB	14/02/2014 02:24 PM	D2F1C6CAB6E06FAA42DEA02D7DAF2972	A3550E928529F679C15928458314D3BAFC8D59	Yes	ABCEDEF1	AES-64
Graphic image Sample 7.JPG	JPG File	2,001 KB	14/02/2014 02:24 PM	E9E03E7C8DE531EAC4344AD566F48CC	0534321762071F94876FBCAC0B29D0C1D385C55E	Yes	ABCEDEF1	AES-64
Graphic image Sample 8.JPG	JPG File	2,063 KB	14/02/2014 02:25 PM	FA50261640889197E262686960BF4332	9F558F953D939E4099D0A97881A08A8573081DDC	Yes	ABCEDEF1	AES-64
Graphic image Sample 9.jpg	JPG File	155 KB	14/02/2014 02:25 PM	270657A0D1307924B356C2E876E594CA	349A53444085715A3F256C0234B5F980866B745D	Yes	ABCEDEF1	AES-64
Graphic image Sample 10.jpg	JPG File	143 KB	14/02/2014 02:25 PM	0685D1447E15A18A026F23B53147861	8E65F8D10554B5BEEFDD02A54D578FD2C57993A	Yes	ABCEDEF1	AES-64
Graphic image Sample 11.jpg	JPG File	50 KB	14/02/2014 02:25 PM	8223359567404E0E1664A43081786A05	FC829D3A74F9E88879D8F5F8B3034A5C04FB782	Yes	ABCEDEF1	AES-64
JPG Carved File Sample 1.PNG	PNG File	3 KB	14/02/2014 02:25 PM	091523D168262627653B2708C2641DF	AS9252A8A6E8D282F70A56831BC8259D2A775D03	Yes	ABCEDEF1	AES-64
PDF Sample 1.pdf	Adobe Acrobat Document	12,466 KB	14/02/2014 02:25 PM	D51CE64D0B58F681093A00C81F510F4	70FEE205A8B643641AA77E2A8D07BAAD C39853F	Yes	ABCEDEF1	AES-64
PDF Sample 2.pdf	Adobe Acrobat Document	78,432 KB	14/02/2014 02:26 PM	9810CF0E41BFF7E0DC48C196A5D4BC7	43109E07612EAC6AD C9AAB6882811368AB548A9	Yes	ABCEDEF1	AES-64
PDF Sample 3.pdf	Adobe Acrobat Document	25,897 KB	14/02/2014 02:26 PM	8707AB8772EC57C81863D8A56EB579D5	F1725A9C766F78E17903385B0B06C352F9027A77	Yes	ABCEDEF1	AES-64
PDF Sample 4.pdf	Adobe Acrobat Document	20,379 KB	14/02/2014 02:26 PM	6E6F8E9F1A8C66841538F54641F9045	D60ED70991389788200C383704A59131A6E5116D	Yes	ABCEDEF1	AES-64
PDF Sample 5.pdf	Adobe Acrobat Document	24,144 KB	14/02/2014 02:26 PM	F0FBC1DA0477F2908EDC34AC189583DA	5160219A2648F482DEF85D5F969C08842E285D0F	Yes	ABCEDEF1	AES-64
Text Document Sample 1.txt	Text Document	1 KB	14/02/2014 02:26 PM	B2982248E195842EADCC5EE391170714F	FD4D713ABFC610F724EA15ECDD55A786A6E95916D	Yes	ABCEDEF1	AES-64
Text Document Sample 2.txt	Text Document	1 KB	14/02/2014 02:26 PM	05C0EF79F3A88248CE14FC39062E897	C496B25050AE660E918A798C3C0F8DEF1496497	Yes	ABCEDEF1	AES-64
Text Document Sample 3.txt	Text Document	1 KB	14/02/2014 02:27 PM	98737A889C24FE151AD C97720C687C54	7D10492426133148744192D1EA100779881668C	Yes	ABCEDEF1	AES-64
Text Document Sample 4.txt	Text Document	1 KB	14/02/2014 02:27 PM	834E58F13C0240D4F1AEB818C7205AF	8815948E0D37441E34D7C3A0E031475461C24DD	Yes	ABCEDEF1	AES-64
Text Document Sample 5.txt	Text Document	1 KB	14/02/2014 02:28 PM	F85B25C07181038E3FDCAC1A8318EA20	3DC779410AC0C6979FA69DDE1A2E2D0C8F26AE0	Yes	ABCEDEF1	AES-64
Word Document Sample 1.doc	Microsoft 97-2003 Document	22 KB	14/02/2014 02:28 PM	2638834B0C0C58F738E2AD2BF46D0F38	8293FC6A29F753799E12AFB6742D584D307C5298	Yes	ABCEDEF1	AES-64
Word Document Sample 2.doc	Microsoft 97-2003 Document	22 KB	14/02/2014 02:28 PM	880288FA7E384443C31820D8A2A2D	BD44A4FC8791C204E4A8F127B877848A57B1AD91	Yes	ABCEDEF1	AES-64
Word Document Sample 3.doc	Microsoft 97-2003 Document	22 KB	14/02/2014 02:28 PM	C6809F791D45A4FF97A86D03C77F771	CF8B70AC35086593F44E6D135455124D9095DAE1	Yes	ABCEDEF1	AES-64
Word Document Sample 4.doc	Microsoft 97-2003 Document	22 KB	14/02/2014 02:28 PM	C381FA0CCF9C1873879F7F327A0E07	8705FDDA0D773DC0A0654B09CB1BDE7A3F8D881C	Yes	ABCEDEF1	AES-64
Word Document Sample 5.doc	Microsoft 97-2003 Document	22 KB	14/02/2014 02:28 PM	AD85136F7F4881223145C7F0CADC0AD	7C3F7254E5ED28887E0B417F45A61F80C1E547	Yes	ABCEDEF1	AES-64

Appendix 33: Table of AESCrypt “Stored Data” on VM1 (Circled VMs Environment)

File Name	Type	Size	Timestamp
Encase File Sample 1.Ex01.aes	AES File	849,672 KB	13/02/2014 02:56 PM
Encase File Sample 2.ex01.aes	AES File	879,890 KB	13/02/2014 02:58 PM
Encase File Sample 3.E01.aes	AES File	556 KB	13/02/2014 02:59 PM
Excel Sample File 1.xls.aes	AES File	36 KB	13/02/2014 03:22 PM
Excel Sample File 2.xls.aes	AES File	149 KB	13/02/2014 03:22 PM
Excel Sample File 3.xls.aes	AES File	69 KB	13/02/2014 03:23 PM
Excel Sample File 4.xls.aes	AES File	190 KB	13/02/2014 03:23 PM
Excel Sample File 5.xls.aes	AES File	89 KB	13/02/2014 03:23 PM
Graphic Image Sample 1.jpg.aes	AES File	31 KB	13/02/2014 03:24 PM
Graphic Image Sample 2.jpg.aes	AES File	16 KB	13/02/2014 03:24 PM
Graphic Image Sample 3.jpg.aes	AES File	10 KB	13/02/2014 03:25 PM
Graphic Image Sample 4.jpg.aes	AES File	8 KB	13/02/2014 03:25 PM
Graphic Image Sample 5.jpg.aes	AES File	17 KB	13/02/2014 03:25 PM
Graphic Image Sample 6.jpg.aes	AES File	58 KB	13/02/2014 03:26 PM
Graphic Image Sample 7.JPG.aes	AES File	2,001 KB	13/02/2014 03:26 PM
Graphic Image Sample 8.JPG.aes	AES File	2,063 KB	13/02/2014 03:26 PM
Graphic Image Sample 9.jpg.aes	AES File	155 KB	13/02/2014 03:27 PM
Graphic Image Sample 10.jpg.aes	AES File	143 KB	13/02/2014 03:27 PM
Graphic Image Sample 11.jpg.aes	AES File	50 KB	13/02/2014 03:28 PM
JPG Carved File Sample 1.PNG.aes	AES File	4 KB	13/02/2014 03:28 PM
PDF Sample 1.pdf.aes	AES File	12,466 KB	13/02/2014 03:29 PM
PDF Sample 2.pdf.aes	AES File	78,432KB	13/02/2014 03:30 PM
PDF Sample 3.pdf.aes	AES File	25,897 KB	13/02/2014 03:30 PM
PDF Sample 4.pdf.aes	AES File	20,379 KB	13/02/2014 03:31 PM
PDF Sample 5.pdf.aes	AES File	24,145 KB	13/02/2014 03:32 PM
Text Document Sample 1.txt.aes	AES File	1 KB	13/02/2014 03:32 PM
Text Document Sample 2.txt.aes	AES File	1 KB	13/02/2014 03:32 PM
Text Document Sample 3.txt.aes	AES File	1 KB	13/02/2014 03:33 PM
Text Document Sample 4.txt.aes	AES File	1 KB	13/02/2014 03:33 PM
Text Document Sample 5.txt.aes	AES File	1 KB	13/02/2014 03:33 PM
Word Document Sample 1.doc.aes	AES File	22 KB	13/02/2014 03:34 PM
Word Document Sample 2.doc.aes	AES File	22 KB	13/02/2014 03:34 PM
Word Document Sample 3.doc.aes	AES File	22 KB	13/02/2014 03:34 PM
Word Document Sample 4.doc.aes	AES File	22 KB	13/02/2014 03:35 PM

Appendix 34: Table of AESCrypt “Stored Data” on VM2 (Circled VMs Environment)

File Name	Type	Size	Timestamp
Encase File Sample 1.Ex01.aes	AES File	849,672 KB	13/02/2014 01:56 PM
Encase File Sample 2.ex01.aes	AES File	879,890 KB	13/02/2014 01:58 PM
Encase File Sample 3.E01.aes	AES File	556 KB	13/02/2014 01:59 PM
Excel Sample File 1.xls.aes	AES File	36 KB	13/02/2014 02:22 PM
Excel Sample File 2.xls.aes	AES File	149 KB	13/02/2014 02:22 PM
Excel Sample File 3.xls.aes	AES File	69 KB	13/02/2014 02:23 PM
Excel Sample File 4.xls.aes	AES File	190 KB	13/02/2014 02:23 PM
Excel Sample File 5.xls.aes	AES File	89 KB	13/02/2014 02:23 PM
Graphic Image Sample 1.jpg.aes	AES File	31 KB	13/02/2014 02:24 PM
Graphic Image Sample 2.jpg.aes	AES File	16 KB	13/02/2014 02:24 PM
Graphic Image Sample 3.jpg.aes	AES File	10 KB	13/02/2014 02:25 PM
Graphic Image Sample 4.jpg.aes	AES File	8 KB	13/02/2014 02:25 PM
Graphic Image Sample 5.jpg.aes	AES File	17 KB	13/02/2014 02:25 PM
Graphic Image Sample 6.jpg.aes	AES File	58 KB	13/02/2014 02:26 PM
Graphic Image Sample 7.JPG.aes	AES File	2,001 KB	13/02/2014 02:26 PM
Graphic Image Sample 8.JPG.aes	AES File	2,063 KB	13/02/2014 02:26 PM
Graphic Image Sample 9.jpg.aes	AES File	155 KB	13/02/2014 02:27 PM
Graphic Image Sample 10.jpg.aes	AES File	143 KB	13/02/2014 02:27 PM
Graphic Image Sample 11.jpg.aes	AES File	50 KB	13/02/2014 02:28 PM
JPG Carved File Sample 1.PNG.aes	AES File	4 KB	13/02/2014 02:28 PM
PDF Sample 1.pdf.aes	AES File	12,466 KB	13/02/2014 02:29 PM
PDF Sample 2.pdf.aes	AES File	78,432KB	13/02/2014 02:30 PM
PDF Sample 3.pdf.aes	AES File	25,897 KB	13/02/2014 02:30 PM
PDF Sample 4.pdf.aes	AES File	20,379 KB	13/02/2014 02:31 PM
PDF Sample 5.pdf.aes	AES File	24,145 KB	13/02/2014 02:32 PM
Text Document Sample 1.txt.aes	AES File	1 KB	13/02/2014 02:32 PM
Text Document Sample 2.txt.aes	AES File	1 KB	13/02/2014 02:32 PM
Text Document Sample 3.txt.aes	AES File	1 KB	13/02/2014 02:33 PM
Text Document Sample 4.txt.aes	AES File	1 KB	13/02/2014 02:33 PM
Text Document Sample 5.txt.aes	AES File	1 KB	13/02/2014 02:33 PM
Word Document Sample 1.doc.aes	AES File	22 KB	13/02/2014 02:34 PM
Word Document Sample 2.doc.aes	AES File	22 KB	13/02/2014 02:34 PM
Word Document Sample 3.doc.aes	AES File	22 KB	13/02/2014 02:34 PM
Word Document Sample 4.doc.aes	AES File	22 KB	13/02/2014 02:35 PM
Word Document Sample 5.doc.aes	AES File	22 KB	13/02/2014 02:35 PM

**Appendix 35: Table of AESCrypt “Stored Data” Copied on VM1 from VM2
(Circled VMs Environment)**

File Name	Type	Size	Timestamp
Encase File Sample 1.Ex01.aes	AES File	849,672 KB	13/02/2014 02:56 PM
Encase File Sample 2.ex01.aes	AES File	879,890 KB	13/02/2014 02:58 PM
Encase File Sample 3.E01.aes	AES File	556 KB	13/02/2014 02:59 PM
Excel Sample File 1.xls.aes	AES File	36 KB	13/02/2014 03:22 PM
Excel Sample File 2.xls.aes	AES File	149 KB	13/02/2014 03:22 PM
Excel Sample File 3.xls.aes	AES File	69 KB	13/02/2014 03:23 PM
Excel Sample File 4.xls.aes	AES File	190 KB	13/02/2014 03:23 PM
Excel Sample File 5.xls.aes	AES File	89 KB	13/02/2014 03:23 PM
Graphic Image Sample 1.jpg.aes	AES File	31 KB	13/02/2014 03:24 PM
Graphic Image Sample 2.jpg.aes	AES File	16 KB	13/02/2014 03:24 PM
Graphic Image Sample 3.jpg.aes	AES File	10 KB	13/02/2014 03:25 PM
Graphic Image Sample 4.jpg.aes	AES File	8 KB	13/02/2014 03:25 PM
Graphic Image Sample 5.jpg.aes	AES File	17 KB	13/02/2014 03:25 PM
Graphic Image Sample 6.jpg.aes	AES File	58 KB	13/02/2014 03:26 PM
Graphic Image Sample 7.JPG.aes	AES File	2,001 KB	13/02/2014 03:26 PM
Graphic Image Sample 8.JPG.aes	AES File	2,063 KB	13/02/2014 03:26 PM
Graphic Image Sample 9.jpg.aes	AES File	155 KB	13/02/2014 03:27 PM
Graphic Image Sample 10.jpg.aes	AES File	143 KB	13/02/2014 03:27 PM
Graphic Image Sample 11.jpg.aes	AES File	50 KB	13/02/2014 03:28 PM
JPG Carved File Sample 1.PNG.aes	AES File	4 KB	13/02/2014 03:28 PM
PDF Sample 1.pdf.aes	AES File	12,466 KB	13/02/2014 03:29 PM
PDF Sample 2.pdf.aes	AES File	78,432KB	13/02/2014 03:30 PM
PDF Sample 3.pdf.aes	AES File	25,897 KB	13/02/2014 03:30 PM
PDF Sample 4.pdf.aes	AES File	20,379 KB	13/02/2014 03:31 PM
PDF Sample 5.pdf.aes	AES File	24,145 KB	13/02/2014 03:32 PM
Text Document Sample 1.txt.aes	AES File	1 KB	13/02/2014 03:32 PM
Text Document Sample 2.txt.aes	AES File	1 KB	13/02/2014 03:32 PM
Text Document Sample 3.txt.aes	AES File	1 KB	13/02/2014 03:33 PM
Text Document Sample 4.txt.aes	AES File	1 KB	13/02/2014 03:33 PM
Text Document Sample 5.txt.aes	AES File	1 KB	13/02/2014 03:33 PM
Word Document Sample 1.doc.aes	AES File	22 KB	13/02/2014 03:34 PM
Word Document Sample 2.doc.aes	AES File	22 KB	13/02/2014 03:34 PM
Word Document Sample 3.doc.aes	AES File	22 KB	13/02/2014 03:34 PM
Word Document Sample 4.doc.aes	AES File	22 KB	13/02/2014 03:35 PM
Word Document Sample 5.doc.aes	AES File	22 KB	13/02/2014 03:35 PM

Appendix 36: Table of AESCrypt “Retrieved Data” from VM1 (Circled VMs Environment)

File Name	Type	Size	Timestamp	MD5 Value	SHA-1 Value
Encase File Sample 1.Ex01.aes	AES Tool Files	849,672 KB	13/02/2014 02:56 PM	32EC01C9D3200922E68810FE6DEA59D4	58165999DE5AE3B34A7CABFEAD4910AD21739FB0
Encase File Sample 2.Ex01.aes	AES Tool Files	879,890 KB	13/02/2014 02:58 PM	8E541E6F1F1B4069E774B8275CC4F302	E227CADFC37B5C54CE71AA0E85228D93976E6
Encase File Sample 3.Ex01.aes	AES Tool Files	556 KB	13/02/2014 02:59 PM	1848D059A3809A9525B37E6897B65BB1	238369DA8C806E6CB4FD4D0F62226EF9AAB6D20B
Excel Sample File 1.Xls.aes	AES Tool Files	36 KB	13/02/2014 03:22 PM	2441D6C7A4A9C942615A51FEF9F85BEC	39477EE7DAF659249AF727172199389403353033
Excel Sample File 2.Xls.aes	AES Tool Files	149 KB	13/02/2014 03:22 PM	7B1BD3947862D8D2E97C03BBASD0D7CC	20CA5CAF88223CE942ED0671D1C2C2345460806A
Excel Sample File 3.Xls.aes	AES Tool Files	69 KB	13/02/2014 03:23 PM	702B743AE93CDC74A35DE6DE1D1E8063	E2824445B34A77B11E1AA88367259FAE04E36D8
Excel Sample File 4.Xls.aes	AES Tool Files	190 KB	13/02/2014 03:23 PM	330FA3E367766EB3E4F0210DD875AB08	B650DAFA4B6F038A4AA94FE7B5FA2C1A7283F16E
Excel Sample File 5.Xls.aes	AES Tool Files	89 KB	13/02/2014 03:23 PM	F96852326A962060CAE68EA1A6F36A16	0159C6D1C578E0975C797CE0AD6F5FDDA808B3A
Graphic Image Sample 1.jpg.aes	AES Tool Files	31 KB	13/02/2014 03:24 PM	561A308E41A5AF5706964EDE041A4EA3	C0246AE92666AE25F407AB6863292B0C02EF3CF2A
Graphic Image Sample 2.jpg.aes	AES Tool Files	16 KB	13/02/2014 03:24 PM	A8540B51677B76001C3E9F6A7B19E8A8	FB4704915C1C1845F1A3819EBBDEF663AF0723D
Graphic Image Sample 3.jpg.aes	AES Tool Files	10 KB	13/02/2014 03:25 PM	428DCA048BC7F7415357C7A6D27DF354	9A85AA47FB59B78C12A66B134848F8A3197380C6
Graphic Image Sample 4.jpg.aes	AES Tool Files	8 KB	13/02/2014 03:25 PM	330FA3E367766EB3E4F0210DD875AB08	B650DAFA4B6F038A4AA94FE7B5FA2C1A7283F16E
Graphic Image Sample 5.jpg.aes	AES Tool Files	17 KB	13/02/2014 03:25 PM	D86DF882B07D1B237523F77EC5B737A1	A840416A3505AA2F60C151CAF88E0BF6450772
Graphic Image Sample 6.jpg.aes	AES Tool Files	58 KB	13/02/2014 03:26 PM	98A7DD3866483DF7259E7A25410ACF3C	FBAB8332F0FF4B8E5D2BCBEACB77EE80912A39A8
Graphic Image Sample 7.JPG.aes	AES Tool Files	2,001 KB	13/02/2014 03:26 PM	200F6BD417832C4B63B91F87EFA4D60A	133A610D08C009068854DC0F6625D51B50269D5F
Graphic Image Sample 8.JPG.aes	AES Tool Files	2,063 KB	13/02/2014 03:26 PM	7E92DE2680847170A49EDD25431E08B8	C0C64E58D0CD34DEEB80E240E9ADBB71E1C6C688
Graphic Image Sample 9.jpg.aes	AES Tool Files	155 KB	13/02/2014 03:27 PM	05B858E218AC08311C76E9B27187B848	3CD73088279D55F0B7EBA157D5C9269E48FECCA9
Graphic Image Sample 10.jpg.aes	AES Tool Files	143 KB	13/02/2014 03:27 PM	621E9571D68A8CE05508AD1B7EA4E7AB	7E052FC2DF167033837614E0B7F843DD2DD5CA6B
Graphic Image Sample 11.jpg.aes	AES Tool Files	50 KB	13/02/2014 03:28 PM	FA2D595AC9E2DF97824F2F6887D4986	11016A41DC749AE51F8D3BA381A2F4FD89A48391
JPG Carved File Sample 1.PNG.aes	AES Tool Files	4 KB	13/02/2014 03:28 PM	A007923B163EBC9FBC6C8A3A17635	9C251158E6A0C1D447E6ACAC7DC3673EFC10C0F9
PDF Sample 1.pdf.aes	AES Tool Files	12,466 KB	13/02/2014 03:29 PM	76198067F4CDFD488F4539B134566EA4	74874E5AF93B40613A481D8892E6585A7C0F80B
PDF Sample 2.pdf.aes	AES Tool Files	78,432 KB	13/02/2014 03:30 PM	6D4B1B45B11400988A223CBA2811D12D	B0780E05CF720332A697E7A6AB519498F2494DDCB
PDF Sample 3.pdf.aes	AES Tool Files	25,897 KB	13/02/2014 03:30 PM	D893883FD0E0A051A0AFDC896D3BC1EB	332BD16ED24F81905DBE853DACA96D555C83F73A
PDF Sample 4.pdf.aes	AES Tool Files	20,379 KB	13/02/2014 03:31 PM	638A757116C5912459622C8CDC2AAD5A	CC3B17163D485E6816AA5D13FC3E85833F263C1B
PDF Sample 5.pdf.aes	AES Tool Files	24,145 KB	13/02/2014 03:32 PM	0ED1DE782B70CA72F873AE71946EE51F	5E1BA748ABF5A3CFB27672FE2AD89D9912BDA60D
Text Document Sample 1.txt.aes	AES Tool Files	1 KB	13/02/2014 03:32 PM	C46616EC7749CF7D0A2480251D008D1D	C91F91BC3EBE316FF857D7D500E6356F18197D2
Text Document Sample 2.txt.aes	AES Tool Files	1 KB	13/02/2014 03:32 PM	177F88208103369AFB07FC8966DCCFE9	24C74C16419797533E0D6A4970732C318953EF10
Text Document Sample 3.txt.aes	AES Tool Files	1 KB	13/02/2014 03:33 PM	4946AC17E98AD112FF3AFA8148004FD7	308635CEDE09A9F30362812D706FD4695DEEB1
Text Document Sample 4.txt.aes	AES Tool Files	1 KB	13/02/2014 03:33 PM	2456A974AD1607175E1F59C3DE386AB2	78E359910940699C8858D9757B40F9285BA716
Text Document Sample 5.txt.aes	AES Tool Files	1 KB	13/02/2014 03:33 PM	FE3E2C1D8059FA04788E25DD0CE7F1E6	FEAC9A604C51248833543E22888952CD62DC760
Word Document Sample 1.doc.aes	AES Tool Files	22 KB	13/02/2014 03:34 PM	66094DDAFB15760F729BD284624A32D0	76957550275CE92E4AC2FD2696E3174CBE53EED
Word Document Sample 2.doc.aes	AES Tool Files	22 KB	13/02/2014 03:34 PM	BE26CE532A33E8F89F88DAF179B095D5	AE6CDE2618AC09D41D5C45D9AD3289ADA8F14364
Word Document Sample 3.doc.aes	AES Tool Files	22 KB	13/02/2014 03:34 PM	1B7DC8ACAF75EB19CADCD4618A65C46	D81CF016739723FC3E54A45F2EB1F61F7A0CE084
Word Document Sample 4.doc.aes	AES Tool Files	22 KB	13/02/2014 03:35 PM	AF385C0A05DE95BEBC12D382D111E8B	291640737F1D44A2158BD14A2D16E9F71AE34D30
Word Document Sample 5.doc.aes	AES Tool Files	22 KB	13/02/2014 03:35 PM	EC191DF5F701B5AAECC48381E27086F	251E2C5786DC0C42CC86F39BD306D8D74769CE0A

Appendix 37: Table of AESCrypt “Recovered Data” from VM1 (Circled VMs Environment)

File Name	Type	Size	Timestamp	MD5 Value	SHA-1 Value	Successful Decryption	Secret Key	Algorithm
Encase File Sample 1.1x01	Encase Evidence File	849,672 KB	14/02/2014 04:36 PM	59998CEA0E97D45337F532808D1A4526	4FC9B5E7076FAEC23E07F05431EE0C5A4CAD9	Yes	abcdeghi1	AES-256
Encase File Sample 2.1x01	Encase Evidence File	879,890 KB	14/02/2014 04:37 PM	377D4D2080232388935E4187712561DF80	401A423CCE9D93089A146C0B8F56875E33C0D358F	Yes	ijklmnopq2	AES-256
Encase File Sample 3.1x01	Encase Evidence File	556 KB	14/02/2014 04:37 PM	01186A4AC9A09373208279C8C6264C5023	842A44ACD81A2CB76DE6340761DD484574830B2EC	Yes	stuvwxyzA3	AES-256
Excel Sample File 1.xls	Microsoft Excel 97-2003 Worksheet	36 KB	14/02/2014 04:35 PM	C2C938882A4ACD51721B52B0FA1F3DDCF	A838C97C88C0D50426468179D5E7C80828982680	Yes	bcddefghi4	AES-256
Excel Sample File 2.xls	Microsoft Excel 97-2003 Worksheet	149 KB	14/02/2014 04:36 PM	5637DFC46A64698776E68A20171474FF	10A0A707D939954072E7F5EE42765F0D12E184A	Yes	klmnopq55	AES-256
Excel Sample File 3.xls	Microsoft Excel 97-2003 Worksheet	69 KB	14/02/2014 04:36 PM	81A2A3D3D1F54A0C276580A0529D1962E5	21C77EDC4B640CEAC6CE1705C34E3168081238C44	Yes	tuvwxyzab6	AES-256
Excel Sample File 4.xls	Microsoft Excel 97-2003 Worksheet	190 KB	14/02/2014 04:36 PM	C2193FB63A055364FC8681D352ED0E4	CDFA95EE16B52F960199D984E30773F3080AC18	Yes	cdefghijk7	AES-256
Excel Sample File 5.xls	Microsoft Excel 97-2003 Worksheet	89 KB	14/02/2014 04:36 PM	0A5FDA78D8389EB21C71BF92AD92C8D2	1598FB06D3F78987858CF0A7B2449D8259157167	Yes	lmnopqst8	AES-256
Graphic Image Sample 1.jpg	JPG File	31 KB	14/02/2014 04:37 PM	9DDB74080781688787AE84882C36D65A	44973E2C6D0AD66BF8FB027C04AC84906EABD460C	Yes	uvwxyzabc9	AES-256
Graphic Image Sample 2.jpg	JPG File	16 KB	14/02/2014 04:37 PM	8CFB10680A4AC1017A741628751D376D0	C7228E068A1D9681C01844620A8A6E6CDF4C8269E	Yes	defghijkl1	AES-256
Graphic Image Sample 3.jpg	JPG File	10 KB	14/02/2014 04:37 PM	AA74E2E36810DF9B9C0CDE68CF696AC3	0F60F38CF587A4DF0C9968D0A867AF11025581C	Yes	mnpqrstuv2	AES-256
Graphic Image Sample 4.jpg	JPG File	8 KB	14/02/2014 04:37 PM	CC15388B2B0CF37F980F051863484D5	31895FA91D7F353D0D3018E7900538891F4FDDA8	Yes	wxyzabc03	AES-256
Graphic Image Sample 5.jpg	JPG File	17 KB	14/02/2014 04:37 PM	0A5FDA78D8389EB21C71BF92AD92C8D2	1598FB06D3F78987858CF0A7B2449D8259157167	Yes	efghijklm4	AES-256
Graphic Image Sample 6.jpg	JPG File	58 KB	14/02/2014 04:38 PM	D2F1C6C486E06FAA2DEA02D70A4F2972	A3550E9285239F679CA15928458314D38AFCD59	Yes	nopqrstuv5	AES-256
Graphic Image Sample 7.jpg	JPG File	2,001 KB	14/02/2014 04:38 PM	E9E03E7C8D5E53C1EAC4344AD566F48C	0534321762701F948766FCAC0829DC1D385C55E	Yes	wxyzabcde6	AES-256
Graphic Image Sample 8.jpg	JPG File	2,063 KB	14/02/2014 04:38 PM	FAS0261640889197E2626696D8F4332	9F55BF953D9239E4099D9A78B1A08A8573081DDC	Yes	efghijklm7	AES-256
Graphic Image Sample 9.jpg	JPG File	155 KB	14/02/2014 04:38 PM	270657AAD13079248356C2E876E594CA	349A534440B5715A3F256C023485F98D668745D	Yes	opqrstuvw8	AES-256
Graphic Image Sample 10.jpg	JPG File	143 KB	14/02/2014 04:38 PM	0685D1447E15A18A026EF25853147861	8E65F89D0554B5BEEFD02AA54D578FD2C57993A	Yes	wyzabcdef9	AES-256
Graphic Image Sample 11.jpg	JPG File	50 KB	14/02/2014 04:39 PM	8223359567404E0E1664A43081786AD5	FC82903A74FE9E8879D85FE983034A3C04F8782	Yes	ghijklm01	AES-256
JPG Carved File Sample 1.PNG	PNG File	4 KB	14/02/2014 04:39 PM	091523D16883626C76538270BC2641DF	A59252A8A6B8D282F70A568318C8259D2A75D03	Yes	pqrstuv2	AES-256
PDF Sample 1.pdf	Adobe Acrobat Document	12,466 KB	14/02/2014 04:39 PM	D51CF64D858F681093A00C81F510F4	70FEE205A8B6443641A477E2A8D07BA0C39853F	Yes	wyzabcde3	AES-256
PDF Sample 2.pdf	Adobe Acrobat Document	78,432 KB	14/02/2014 04:39 PM	9810CF0E41BF7FED0C4BC196A5D48C7	43108E07612EAC6A0C9A4B6882811368A8568A9	Yes	efghijklm4	AES-256
PDF Sample 3.pdf	Adobe Acrobat Document	25,897 KB	14/02/2014 04:39 PM	8707A8B772EC57C81863D8A56E8579D5	F1725A9C766F78E7903385B0B06C352F9027A77	Yes	opqrstuvw5	AES-256
PDF Sample 4.pdf	Adobe Acrobat Document	20,379 KB	14/02/2014 04:39 PM	6E6F8E9F1ABC66841538F54641F90A5	D6DE7099138788200C38370A459131A65116D	Yes	xyzabcdef6	AES-256
PDF Sample 5.pdf	Adobe Acrobat Document	24,145 KB	14/02/2014 04:40 PM	F0FBC1DA0477F2908DC34AE189583DA	D6DE7099138788200C38370A459131A65116D	Yes	ghijklm07	AES-256
Text Document Sample 1.txt	Text Document	1 KB	14/02/2014 04:40 PM	B2882248E1958A2EADCE5EE391170714F	5160219A2648482DEE85D5E969C08842E85D0F	Yes	efghijklm8	AES-256
Text Document Sample 2.txt	Text Document	1 KB	14/02/2014 04:40 PM	05CC0FE79F3A88248C14FC39062E897	FD4D713ABFC610F72AE415EC0D55A7B6A859596D	Yes	pqrstuv8	AES-256
Text Document Sample 3.txt	Text Document	1 KB	14/02/2014 04:40 PM	98737AB89C24FE151AD09720C687C54	C489682505A0E86DE918A7985C30EBDEF1A96A97	Yes	wxyzabc9	AES-256
Text Document Sample 4.txt	Text Document	1 KB	14/02/2014 04:40 PM	834E5BE13C02404D4F1AE8B1BC7205AF	7D10492426133148744192D1EA100779881608C	Yes	defghijkl1	AES-256
Text Document Sample 5.txt	Text Document	1 KB	14/02/2014 04:40 PM	F85B250C7181038E3FDECA1E831BEA20	8815948E0D32F441E3402C3A0E031475461C24D0	Yes	mnpqrstuv2	AES-256
Word Document Sample 1.doc	Microsoft 97-2003 Document	22 KB	14/02/2014 04:41 PM	263883480C0D58738E2AD28F4460F38	30CC79410A0C69797FA69D0E1A2E200CBF26A40	Yes	wxyzabc03	AES-256
Word Document Sample 2.doc	Microsoft 97-2003 Document	22 KB	14/02/2014 04:41 PM	880288FA7E3B4A443CE31820D842A2D	8293FC6A29F753799E12AF6742058407C5298	Yes	efghijklm4	AES-256
Word Document Sample 3.doc	Microsoft 97-2003 Document	22 KB	14/02/2014 04:41 PM	C86897891B45A4FA9F486D03C7F7771	BD0AA4FC8791C20AE4A8F12B877848A781A091	Yes	nopqrstuv5	AES-256
Word Document Sample 4.doc	Microsoft 97-2003 Document	22 KB	14/02/2014 04:41 PM	C381FAA0CCFCFC1E873879E7F327A0E07	CF8870AC35086593F44E6D135455124D9095DAE1	Yes	wyzabcdef6	AES-256
Word Document Sample 5.doc	Microsoft 97-2003 Document	22 KB	14/02/2014 04:41 PM	AD8513677FA881223145C7F6C0AC0A04D	8705FDDA0D7730CA06548C89C91BD7A380881C	Yes	efghijklm07	AES-256
					7C33F7254E5D2887E0B47F451A61F80C1E547	Yes	pqrstuvw8	AES-256

Appendix 38: Table of AxCrypt “Stored Data” on VM1 (Circled VMs Environment)

File Name	Type	Size	Timestamp
Encase File Sample 1-Ex01.axx	AXX File	849,672 KB	13/02/2014 06:59 PM
Encase File Sample 2-ex01.axx	AXX File	879,890 KB	13/02/2014 07:00 PM
Encase File Sample 3-E01.axx	AXX File	556 KB	13/02/2014 07:00 PM
Excel Sample File 1-xls.axx	AXX File	9 KB	13/02/2014 07:01 PM
Excel Sample File 2-xls.axx	AXX File	32 KB	13/02/2014 07:01 PM
Excel Sample File 3-xls.axx	AXX File	20 KB	13/02/2014 07:02 PM
Excel Sample File 4-xls.axx	AXX File	29 KB	13/02/2014 07:02 PM
Excel Sample File 5-xls.axx	AXX File	17 KB	13/02/2014 07:02 PM
Graphic Image Sample 1-jpg.axx	AXX File	19 KB	13/02/2014 07:03 PM
Graphic Image Sample 2-jpg.axx	AXX File	17 KB	13/02/2014 07:03 PM
Graphic Image Sample 3-jpg.axx	AXX File	10 KB	13/02/2014 07:03 PM
Graphic Image Sample 4-jpg.axx	AXX File	8 KB	13/02/2014 07:04 PM
Graphic Image Sample 5-jpg.axx	AXX File	17 KB	13/02/2014 07:04 PM
Graphic Image Sample 6-jpg.axx	AXX File	58 KB	13/02/2014 07:04 PM
Graphic Image Sample 7-JPG.axx	AXX File	2,001 KB	13/02/2014 07:05 PM
Graphic Image Sample 8-JPG.axx	AXX File	2,063 KB	13/02/2014 07:05 PM
Graphic Image Sample 9-jpg.axx	AXX File	155 KB	13/02/2014 07:05 PM
Graphic Image Sample 10-jpg.axx	AXX File	143 KB	13/02/2014 07:06 PM
Graphic Image Sample 11-jpg.axx	AXX File	50 KB	13/02/2014 07:06 PM
JPG Carved File Sample 1-PNG.axx	AXX File	4 KB	13/02/2014 07:06 PM
PDF Sample 1-pdf.axx	AXX File	12,466 KB	13/02/2014 07:49 PM
PDF Sample 2-pdf.axx	AXX File	68,437KB	13/02/2014 07:50 PM
PDF Sample 3-pdf.axx	AXX File	25,897 KB	13/02/2014 07:50 PM
PDF Sample 4-pdf.axx	AXX File	20,379 KB	13/02/2014 07:51 PM
PDF Sample 5-pdf.axx	AXX File	24,145 KB	13/02/2014 07:51 PM
Text Document Sample 1-txt.axx	AXX File	1 KB	13/02/2014 07:08 PM
Text Document Sample 2-txt.axx	AXX File	1 KB	13/02/2014 07:08 PM
Text Document Sample 3-txt.axx	AXX File	1 KB	13/02/2014 07:08 PM
Text Document Sample 4-txt.axx	AXX File	1 KB	13/02/2014 07:09 PM
Text Document Sample 5-txt.axx	AXX File	1 KB	13/02/2014 07:09 PM
Word Document Sample 1-doc.axx	AXX File	6 KB	13/02/2014 07:10 PM
Word Document Sample 2-doc.axx	AXX File	6 KB	13/02/2014 07:10 PM
Word Document Sample 3-doc.axx	AXX File	6 KB	13/02/2014 07:10 PM
Word Document Sample 4-doc.axx	AXX File	6 KB	13/02/2014 07:10 PM
Word Document Sample 5-doc.axx	AXX File	6 KB	13/02/2014 07:11 PM

Appendix 39: Table of AxCrypt “Stored Data” on VM2 (Circled VMs Environment)

File Name	Type	Size	Timestamp
Encase File Sample 1-Ex01.axx	AXX File	849,672 KB	13/02/2014 05:59 PM
Encase File Sample 2-ex01.axx	AXX File	879,890 KB	13/02/2014 06:00 PM
Encase File Sample 3-E01.axx	AXX File	556 KB	13/02/2014 06:00 PM
Excel Sample File 1-xls.axx	AXX File	9 KB	13/02/2014 06:01 PM
Excel Sample File 2-xls.axx	AXX File	32 KB	13/02/2014 06:01 PM
Excel Sample File 3-xls.axx	AXX File	20 KB	13/02/2014 06:02 PM
Excel Sample File 4-xls.axx	AXX File	29 KB	13/02/2014 06:02 PM
Excel Sample File 5-xls.axx	AXX File	17 KB	13/02/2014 06:02 PM
Graphic Image Sample 1-jpg.axx	AXX File	19 KB	13/02/2014 06:03 PM
Graphic Image Sample 2-jpg.axx	AXX File	17 KB	13/02/2014 06:03 PM
Graphic Image Sample 3-jpg.axx	AXX File	10 KB	13/02/2014 06:03 PM
Graphic Image Sample 4-jpg.axx	AXX File	8 KB	13/02/2014 06:04 PM
Graphic Image Sample 5-jpg.axx	AXX File	17 KB	13/02/2014 06:04 PM
Graphic Image Sample 6-jpg.axx	AXX File	58 KB	13/02/2014 06:04 PM
Graphic Image Sample 7-JPG.axx	AXX File	2,001 KB	13/02/2014 06:05 PM
Graphic Image Sample 8-JPG.axx	AXX File	2,063 KB	13/02/2014 06:05 PM
Graphic Image Sample 9-jpg.axx	AXX File	155 KB	13/02/2014 06:05 PM
Graphic Image Sample 10-jpg.axx	AXX File	143 KB	13/02/2014 06:06 PM
Graphic Image Sample 11-jpg.axx	AXX File	50 KB	13/02/2014 06:06 PM
JPG Carved File Sample 1-PNG.axx	AXX File	4 KB	13/02/2014 06:06 PM
PDF Sample 1-pdf.axx	AXX File	12,466 KB	13/02/2014 06:49 PM
PDF Sample 2-pdf.axx	AXX File	68,437KB	13/02/2014 06:50 PM
PDF Sample 3-pdf.axx	AXX File	25,897 KB	13/02/2014 06:50 PM
PDF Sample 4-pdf.axx	AXX File	20,379 KB	13/02/2014 06:51 PM
PDF Sample 5-pdf.axx	AXX File	24,145 KB	13/02/2014 06:51 PM
Text Document Sample 1-txt.axx	AXX File	1 KB	13/02/2014 06:08 PM
Text Document Sample 2-txt.axx	AXX File	1 KB	13/02/2014 06:08 PM
Text Document Sample 3-txt.axx	AXX File	1 KB	13/02/2014 06:08 PM
Text Document Sample 4-txt.axx	AXX File	1 KB	13/02/2014 06:09 PM
Text Document Sample 5-txt.axx	AXX File	1 KB	13/02/2014 06:09 PM
Word Document Sample 1-doc.axx	AXX File	6 KB	13/02/2014 06:10 PM
Word Document Sample 2-doc.axx	AXX File	6 KB	13/02/2014 06:10 PM
Word Document Sample 3-doc.axx	AXX File	6 KB	13/02/2014 06:10 PM
Word Document Sample 4-doc.axx	AXX File	6 KB	13/02/2014 06:10 PM
Word Document Sample 5-doc.axx	AXX File	6 KB	13/02/2014 06:11 PM

Appendix 40: Table of AxCrypt “Stored Data” Copied on VM1 from VM2 (Circled VMs Environment)

File Name	Type	Size	Timestamp
Encase File Sample 1-Ex01.axx	AXX File	849,672 KB	13/02/2014 06:59 PM
Encase File Sample 2-ex01.axx	AXX File	879,890 KB	13/02/2014 07:00 PM
Encase File Sample 3-E01.axx	AXX File	556 KB	13/02/2014 07:00 PM
Excel Sample File 1-xls.axx	AXX File	9 KB	13/02/2014 07:01 PM
Excel Sample File 2-xls.axx	AXX File	32 KB	13/02/2014 07:01 PM
Excel Sample File 3-xls.axx	AXX File	20 KB	13/02/2014 07:02 PM
Excel Sample File 4-xls.axx	AXX File	29 KB	13/02/2014 07:02 PM
Excel Sample File 5-xls.axx	AXX File	17 KB	13/02/2014 07:02 PM
Graphic Image Sample 1-jpg.axx	AXX File	19 KB	13/02/2014 07:03 PM
Graphic Image Sample 2-jpg.axx	AXX File	17 KB	13/02/2014 07:03 PM
Graphic Image Sample 3-jpg.axx	AXX File	10 KB	13/02/2014 07:03 PM
Graphic Image Sample 4-jpg.axx	AXX File	8 KB	13/02/2014 07:04 PM
Graphic Image Sample 5-jpg.axx	AXX File	17 KB	13/02/2014 07:04 PM
Graphic Image Sample 6-jpg.axx	AXX File	58 KB	13/02/2014 07:04 PM
Graphic Image Sample 7-JPG.axx	AXX File	2,001 KB	13/02/2014 07:05 PM
Graphic Image Sample 8-JPG.axx	AXX File	2,063 KB	13/02/2014 07:05 PM
Graphic Image Sample 9-jpg.axx	AXX File	155 KB	13/02/2014 07:05 PM
Graphic Image Sample 10-jpg.axx	AXX File	143 KB	13/02/2014 07:06 PM
Graphic Image Sample 11-jpg.axx	AXX File	50 KB	13/02/2014 07:06 PM
JPG Carved File Sample 1-PNG.axx	AXX File	4 KB	13/02/2014 07:06 PM
PDF Sample 1-pdf.axx	AXX File	12,466 KB	13/02/2014 07:49 PM
PDF Sample 2-pdf.axx	AXX File	68,437KB	13/02/2014 07:50 PM
PDF Sample 3-pdf.axx	AXX File	25,897 KB	13/02/2014 07:50 PM
PDF Sample 4-pdf.axx	AXX File	20,379 KB	13/02/2014 07:51 PM
PDF Sample 5-pdf.axx	AXX File	24,145 KB	13/02/2014 07:51 PM
Text Document Sample 1-txt.axx	AXX File	1 KB	13/02/2014 07:08 PM
Text Document Sample 2-txt.axx	AXX File	1 KB	13/02/2014 07:08 PM
Text Document Sample 3-txt.axx	AXX File	1 KB	13/02/2014 07:08 PM
Text Document Sample 4-txt.axx	AXX File	1 KB	13/02/2014 07:08 PM
Text Document Sample 5-txt.axx	AXX File	1 KB	13/02/2014 07:09 PM
Word Document Sample 1-doc.axx	AXX File	6 KB	13/02/2014 07:10 PM
Word Document Sample 2-doc.axx	AXX File	6 KB	13/02/2014 07:10 PM
Word Document Sample 3-doc.axx	AXX File	6 KB	13/02/2014 07:10 PM
Word Document Sample 4-doc.axx	AXX File	6 KB	13/02/2014 07:10 PM
Word Document Sample 5-doc.axx	AXX File	6 KB	13/02/2014 07:11 PM

Appendix 41: Table of AxCrypt “Retrieved Data” from VM1 (Circled VMs Environment)

File Name	Type	Size	Timestamp	MD5 Value	SHA-1 Value
Encase File Sample 1-Ex01.axx	AxCrypt Encrypted File	849,672 KB	13/02/2014 06:59 PM	E66461D4885E2F31DD06D6751FD2841E9	AA2DB847B59886EC2DCB47FA01B4C5DCA1815A4
Encase File Sample 2-ex01.axx	AxCrypt Encrypted File	879,890 KB	13/02/2014 07:00 PM	B1003F33735CF978831C7EE05ED65350	0FA1F430D445CAC5CF2C8C596306138E8DCC3BC10
Encase File Sample 3-E01.axx	AxCrypt Encrypted File	556 KB	13/02/2014 07:00 PM	5D4D4D3600DEA07274EF6C854DA2AE06F	7C16E8F99FEB0418C4D122382823183C58083D39
Excel Sample File 1-Xls.axx	AxCrypt Encrypted File	9 KB	13/02/2014 07:01 PM	C65C27369663AF900DC89E2AE0B3C4F5	57A2AA538E84E88315C3EB6806C48D5E5D89506
Excel Sample File 2-Xls.axx	AxCrypt Encrypted File	32 KB	13/02/2014 07:01 PM	66130E5D5AC908E58FD8CB2C6F292ADC	A691340C7D240F8871988FFABF67D934FE5F83D0
Excel Sample File 3-Xls.axx	AxCrypt Encrypted File	20 KB	13/02/2014 07:02 PM	5606346700F31986E5A08385ED54802F	D2FF4B1D9CE493434DBCB49F4582C88884C6
Excel Sample File 4-Xls.axx	AxCrypt Encrypted File	29 KB	13/02/2014 07:02 PM	EE089A190D8E46E1D3EDB17E1C205014	5009927550FF823EDC1CB3573FFAF1918D9363AC
Excel Sample File 5-Xls.axx	AxCrypt Encrypted File	17 KB	13/02/2014 07:02 PM	A8C4D7AE1F812667838D666399146366	F23400126AFF9B58E1A1DE3F78CD43307AD63439
Graphic Image Sample 1-jpg.axx	AxCrypt Encrypted File	19 KB	13/02/2014 07:03 PM	6C84D9814E33FF7D77AAD868D48F676C	C1678CA897E1359A8414D80E5E82A806C198C33C
Graphic Image Sample 2-jpg.axx	AxCrypt Encrypted File	17 KB	13/02/2014 07:03 PM	7165530F346708EF29856505EEF712A8	81107D1DEFDEA59F7B12ACFFC83087D0C49E853B
Graphic Image Sample 3-jpg.axx	AxCrypt Encrypted File	10 KB	13/02/2014 07:03 PM	9131988A562E8381856D804903E3513	2AC4F8E376999754F370C47C86300C5A9FF2EF4B
Graphic Image Sample 4-jpg.axx	AxCrypt Encrypted File	8 KB	13/02/2014 07:04 PM	3F0F4E90EF56313FCASF5D1B242C3034A	75EBED4DC337FA23F4E3FC517626DC422D34878
Graphic Image Sample 5-jpg.axx	AxCrypt Encrypted File	17 KB	13/02/2014 07:04 PM	306F8A78A5970C449AA2BE2995FEA950	D8208AE36856CF04687F1F282C862D8316315F8
Graphic Image Sample 6-jpg.axx	AxCrypt Encrypted File	58 KB	13/02/2014 07:04 PM	569A61D96FDB88E42E0E20A2F6C6DCE6A6A	4A41F28A51A42CBB8CF9481D85BA36F4884EAC5
Graphic Image Sample 7-JPG.axx	AxCrypt Encrypted File	2,001 KB	13/02/2014 07:05 PM	34F08FDA5250F135D70A511681BD366C	53201208588EB0A4625FB5C73FD965975BA0DBB5
Graphic Image Sample 8-JPG.axx	AxCrypt Encrypted File	2,063 KB	13/02/2014 07:05 PM	EDF98E380D5197B88F910508CC9986F	24DBFD388C55A9989902C9EA1E200FE5DA41484F
Graphic Image Sample 9-jpg.axx	AxCrypt Encrypted File	155 KB	13/02/2014 07:05 PM	A8F253046143441CC26A22968F73C67	8BB6337390180CFF7E9CA2C9A0AE4F046927E3
Graphic Image Sample 10-jpg.axx	AxCrypt Encrypted File	143 KB	13/02/2014 07:06 PM	0478A4FE66FD6410E31E1FE043C6F6C95	EF5B CB8E79C1D94E47C4D133F58D92D200D5D4C
Graphic Image Sample 11-jpg.axx	AxCrypt Encrypted File	50 KB	13/02/2014 07:06 PM	C5DD66C37F1AB702E830C28808F54AFC	076AA52AE2D617018F9EB8FC28319C37DEB04742
JPG Carved File Sample 1-PNG.axx	AxCrypt Encrypted File	4 KB	13/02/2014 07:06 PM	EC62EC8849175C5CC4D9A5407B282606	F6C9C9C163457DA0293B124A98C5028A8D575B1A
PDF Sample 1-pdf.axx	AxCrypt Encrypted File	12,466 KB	13/02/2014 07:49 PM	68C5F8229EEA40609ACFFCAE669D35B	2361F2036FE741E6F30D8A568940809451B0857C
PDF Sample 2-pdf.axx	AxCrypt Encrypted File	68,437KB	13/02/2014 07:50 PM	8DF51C3D0221A47CC467122106466066	EDE5B7B0EA26AE4D6465A5D2806AD0F42793883A
PDF Sample 3-pdf.axx	AxCrypt Encrypted File	25,897 KB	13/02/2014 07:50 PM	4F5E98A2D6ED1A8BA59A94AF0BF9C724	B4194AC96C275E828866263F1AD6A7EF6C65ADA1
PDF Sample 4-pdf.axx	AxCrypt Encrypted File	20,379 KB	13/02/2014 07:51 PM	399068439918C6C6A1C50D0882056358	7D91466FD498D7B1FC10DF69A58950D8F9A28BE1
PDF Sample 5-pdf.axx	AxCrypt Encrypted File	24,145 KB	13/02/2014 07:51 PM	C836F8A33EAE7A0686D6FC9628EF1BF	0A2408D5F1557E0983D896DA3D5E7F089207D596
Text Document Sample 1-txt.axx	AxCrypt Encrypted File	1 KB	13/02/2014 07:08 PM	4F08127285D00ADF8698E6981879870	44E651252585E9D95516AFA2689DAAD284571788
Text Document Sample 2-txt.axx	AxCrypt Encrypted File	1 KB	13/02/2014 07:08 PM	2B64ED74822789AECF811E05C87F84A8	78D62C59246A341E7FEFE69E9C28B7F256A3649F
Text Document Sample 3-txt.axx	AxCrypt Encrypted File	1 KB	13/02/2014 07:08 PM	BF09A6A2EE0F3057D92228F5A5978303	C979B84C5F0C17082EDA398D173C4E715E4572FF
Text Document Sample 4-txt.axx	AxCrypt Encrypted File	1 KB	13/02/2014 07:09 PM	3F0F4E90EF56313FCASF5D1B242C3034A	75EBED4DC337FA23F4E3FC517626DC422D34878
Text Document Sample 5-txt.axx	AxCrypt Encrypted File	1 KB	13/02/2014 07:09 PM	B3B09C CB6EB15897DC48861880B0380D	1A792FF764A91B71EE67E7E28F3CD5844F20CF16E
World Document Sample 1-doc.axx	AxCrypt Encrypted File	6 KB	13/02/2014 07:10 PM	64AD950330A82EA09309FB135220C910	A76F17E91AF19D57A61CF388C091D683FF5FE699
World Document Sample 2-doc.axx	AxCrypt Encrypted File	6 KB	13/02/2014 07:10 PM	71A9DE948155A8780D77A88D7E4088CA	CA1619C9C953A54558FB279EA55EEF3D6216FC41D
World Document Sample 3-doc.axx	AxCrypt Encrypted File	6 KB	13/02/2014 07:10 PM	0695DDF321D8960E06453DC05080E7B3F	08BD87D758DE067499AFE41997A88FD7452D6FB
World Document Sample 4-doc.axx	AxCrypt Encrypted File	6 KB	13/02/2014 07:10 PM	4377772E6E77520371792F99423CE91B	98CC8F65856A3751D88941AADC9CA006DF04D4
World Document Sample 5-doc.axx	AxCrypt Encrypted File	6 KB	13/02/2014 07:11 PM	D0624DC02C1F8973C44B48D7F891E56	C63F7699C8676DE0B80FF8C4A00AA45CC5F5A31F

Appendix 42: Table of AxCrypt “Recovered Data” from VM1 (Circled VMs Environment)

File Name	Type	Size	Timestamp	MD5 Value	SHA-1 Value	Successful/Decryption	Secret Key	Algorithm
Encase File Sample 1.1x01	Encase Evidence File	849,671 KB	29/06/2011 10:29 AM	5999CEA0E97D45375F2808FD14A526	4EC9B65707FA5FC23E07F05A31EE0C5ACAE9D	Yes	abcdeh11	AES-128
Encase File Sample 2.1x01	Encase Evidence File	879,889 KB	28/11/2012 03:06 PM	372D42D8023238935E41871256D7B0	401A423CE9D089A146CC0B85687533C0D358F	Yes	ijklmnopqR2	AES-128
Encase File Sample 3.1x01	Encase Evidence File	556 KB	04/04/2013 08:48 PM	01186A4AC9D372208279C8C826A5C023	842A44AC0B1A2CB876DE6A40761BD0A857483082EC	Yes	stuvwxyzA3	AES-128
Excel Sample File 1.xls	Microsoft Excel 97-2003 Worksheet	36 KB	16/05/2013 08:41 AM	C2938882A40DC05172105280FA1F3DDCF	A83BC97C8B0C50426A69179D57C808289B2680	Yes	bcddefghiU4	AES-128
Excel Sample File 2.xls	Microsoft Excel 97-2003 Worksheet	148 KB	17/06/2005 11:38 AM	5637DFC464698776E86A20071F147FF	10A0A707092995A072E7F5FE42765F012E184A	Yes	klmnopqS5	AES-128
Excel Sample File 3.xls	Microsoft Excel 97-2003 Worksheet	69 KB	17/06/2005 11:39 AM	B1A2A3D1F54A0C276580DA0529D1962E5	21C77EDC4B640ECAC6E1705C34E3168081238CA4	Yes	tuwxyzab6	AES-128
Excel Sample File 4.xls	Microsoft Excel 97-2003 Worksheet	189 KB	17/06/2005 11:40 AM	C2193FB63A055564FC8688D1352ED0E4	C0FEA95E16B57F960199099A4E30773F3080AC18	Yes	cdefghijk7	AES-128
Excel Sample File 5.xls	Microsoft Excel 97-2003 Worksheet	89 KB	17/06/2005 11:41 AM	0A5FDA78D8389F821C71BF92A092C802	1598FB6D03F78987B58CF0A7B24A9D8259157167	Yes	lmnopqrsT8	AES-128
Graphic Image Sample 1.jpg	JPG File	31 KB	08/02/2008 03:44 PM	90D87408781688787AE84887C36D65A	44973E2C6D04D66FBFB027C04AC8A906EABD460C	Yes	uvwxyzabC9	AES-128
Graphic Image Sample 2.jpg	JPG File	16 KB	22/01/2014 11:12 AM	8CFB10680A4C1017A141628751D37600	C7228E068A1D9681C01844620A486C6C4C8269E	Yes	defghijkl1	AES-128
Graphic Image Sample 3.jpg	JPG File	10 KB	22/01/2014 11:13 AM	A474E2E36810DF99C0CDE68CF696AC3	0F60F38CFE587ADDFC996F80A867AF11D25581C	Yes	mnopqrstu2	AES-128
Graphic Image Sample 4.jpg	JPG File	8 KB	22/01/2014 11:13 AM	CC153888280FC873F980FDS186348A0D5	31895FA91D7F353D003D018E7900538891F4FDFAB	Yes	vwxyzabcD3	AES-128
Graphic Image Sample 5.jpg	JPG File	17 KB	22/01/2014 11:14 AM	0A5FDA78D8389F821C71BF92A092C802	1598FB6D03F78987B58CF0A7B24A9D8259157167	Yes	efghijklmM4	AES-128
Graphic Image Sample 6.jpg	JPG File	57 KB	12/07/2005 01:14 AM	D2F1C6C4B6E06FAA2DEA02D7DAF2972	A9350E9285239F679CA15928458314D38AFC8D59	Yes	nopqrstuV5	AES-128
Graphic Image Sample 7.jpg	JPG File	2,001 KB	03/09/2009 12:20 PM	E9E03E7C8DE53C1EAC434A4D566F48CC	0534321762701F94876FBCAC0B29DCD1D385C55E	Yes	vwxyzabcF6	AES-128
Graphic Image Sample 8.jpg	JPG File	2,063 KB	18/03/2009 09:06 AM	FAS0261640889197E2626B696D8F4332	9F55BF953D9239E4099D9A7881A08A9573081DDC	Yes	ghijklmnN7	AES-128
Graphic Image Sample 9.jpg	JPG File	155 KB	10/01/2010 12:08 PM	270657A4D13079248356C2E876E594CA	349A534440B5715A3F2560234B59808668745D	Yes	opqrstuVW8	AES-128
Graphic Image Sample 10.jpg	JPG File	143 KB	15/05/2012 03:43 PM	0685D1447E15A38A024EF25B83147B61	8E65F89D10554B58E8EED0A454D578FD327993A	Yes	vwxyzabcF9	AES-128
Graphic Image Sample 11.jpg	JPG File	50 KB	21/11/1999 04:48 PM	822335956740E1E664A3081786A0D5	FC829D3A74FE9EB8879085FE983034A3C04FB782	Yes	ghijklmnO1	AES-128
JPG Carved File Sample 1.PNG	PNG File	3 KB	09/05/2012 04:53 PM	091523D16882626C765382708C2641DF	A59252A8A68D282F70A5688318C8259D2A775D03	Yes	pqrstuV2	AES-128
PDF Sample 1.pdf	Adobe Acrobat Document	12,466 KB	07/05/2011 02:15 PM	D51CF64D858F681099A00C81F510F4	70FE205A8B643641A477E2A8D078A0C39853F	Yes	vwxyzabcE3	AES-128
PDF Sample 2.pdf	Adobe Acrobat Document	78,492 KB	07/05/2011 02:28 PM	9810CF0E41B8FFED0C48C196A5D48C7	43109E0762ECAC6ACD9A4B6882811368A548A9	Yes	ghijklmnM4	AES-128
PDF Sample 3.pdf	Adobe Acrobat Document	25,897 KB	07/05/2011 02:17 PM	8707A88772E57C81863D8A5E8E579D5	F1725A9C766F78E17903385B0806C352F902A77	Yes	opqrstuWV5	AES-128
PDF Sample 4.pdf	Adobe Acrobat Document	20,379 KB	07/05/2011 01:11 PM	6E6F8E9F1A8C6684158F546A1F90A5	D6D6ED70991389788200C38370A459131A6E5116D	Yes	xyzabcdeF6	AES-128
PDF Sample 5.pdf	Adobe Acrobat Document	24,144 KB	07/05/2011 01:11 PM	F0FBC1D0A077F2808EDC34AE189583DA	5160219A26A8482DEE85DE969C084028B5D0F	Yes	ghijklmnO7	AES-128
Text Document Sample 1.txt	Text Document	1 KB	22/01/2014 11:58 AM	B2982248E19582A2EADCC5EE391710714F	FD40713A0FC610F7A7E2A415EC0C55A7B64E9596D	Yes	pqrstuV8	AES-128
Text Document Sample 2.txt	Text Document	1 KB	22/01/2014 11:59 AM	05CC0E79F3A8B24BC14FC39062E897	CAB98B25050AE8B6D918A79B83C0E0EDF1496A97	Yes	uvwxyzabC9	AES-128
Text Document Sample 3.txt	Text Document	1 KB	22/01/2014 11:59 AM	98737A899C24FE151A0C9720C687C54	7D1049242613314874419D1EA10077988166BC	Yes	defghijkL1	AES-128
Text Document Sample 4.txt	Text Document	1 KB	22/01/2014 12:00 PM	834E58E13C0240D4F1AEB81BC7205AF	8815948ED032F441E3402C3A0E031475461C24DD	Yes	mnopqrstu2	AES-128
Text Document Sample 5.txt	Text Document	1 KB	22/01/2014 12:01 PM	F85B250C718103B83FDECA1E8318EA20	3DCC79410A0C069797A8BDD1EA2E20CBF26AE0	Yes	vwxyzabC3	AES-128
Word Document Sample 1.doc	Microsoft 97-2003 Document	22 KB	22/01/2014 11:53 AM	26388348D0C58F7387E2AD28F4460F38	8293F6A29F757399E12F8674205840307C5298	Yes	efghijklM4	AES-128
Word Document Sample 2.doc	Microsoft 97-2003 Document	22 KB	22/01/2014 11:53 AM	880288A7E738A44C3E318200842A2D	8DAAA4FC8791C204E4A8F127887948A5781A091	Yes	nopqrstuV5	AES-128
Word Document Sample 3.doc	Microsoft 97-2003 Document	22 KB	22/01/2014 11:53 AM	C8689F87918A54AF94746D03C77F771	CF8870AC35086593F44E6D135455124D0909D4E1	Yes	vwxyzabC6	AES-128
Word Document Sample 4.doc	Microsoft 97-2003 Document	22 KB	22/01/2014 11:54 AM	C381FAACCFC81E873879F7327A0E07	8705FDAD007730CA0548ACB9CB1BDE7A3F8D881C	Yes	ghijklmnO7	AES-128
Word Document Sample 5.doc	Microsoft 97-2003 Document	22 KB	22/01/2014 12:02 PM	AD85136F7FA881223145C7FE0CADC0AD	7C33F7254E5D28887E08417451A61F80C1E547	Yes	pqrstuWV8	AES-128

Appendix 43: Table of AESTool “Stored Data” on VM1 (Circled VMs Environment)

File Name	Type	Size	Timestamp
AES Encase File Sample 1	Application	850,013 KB	13/02/2014 11:29 PM
AES Encase File Sample 2	Application	880,231 KB	13/02/2014 11:35 PM
AES Encase File Sample 3	Application	898 KB	13/02/2014 11:35 PM
AES Excel Sample File 1	Application	378 KB	13/02/2014 11:35 PM
AES Excel Sample File 2	Application	490 KB	13/02/2014 11:36 PM
AES Excel Sample File 3	Application	411 KB	13/02/2014 11:36 PM
AES Excel Sample File 4	Application	531 KB	13/02/2014 11:37 PM
AES Excel Sample File 5	Application	431 KB	13/02/2014 11:37 PM
AES Graphic Image Sample 1	Application	373 KB	13/02/2014 11:37 PM
AES Graphic Image Sample 2	Application	358 KB	13/02/2014 11:38 PM
AES Graphic Image Sample 3	Application	351 KB	13/02/2014 11:38 PM
AES Graphic Image Sample 4	Application	349 KB	13/02/2014 11:38 PM
AES Graphic Image Sample 5	Application	358 KB	13/02/2014 11:38 PM
AES Graphic Image Sample 6	Application	399 KB	13/02/2014 11:39 PM
AES Graphic Image Sample 7	Application	2,342 KB	13/02/2014 11:39 PM
AES Graphic Image Sample 8	Application	2,404 KB	13/02/2014 11:39 PM
AES Graphic Image Sample 9	Application	497 KB	13/02/2014 11:39 PM
AES Graphic Image Sample 10	Application	485 KB	13/02/2014 11:40 PM
AES Graphic Image Sample 11	Application	391 KB	13/02/2014 11:40 PM
AES JPG Carved File Sample 1	Application	345 KB	13/02/2014 11:40 PM
AES PDF Sample 1.pdf	Application	12,808 KB	13/02/2014 11:41 PM
AES PDF Sample 2.pdf	Application	78,773 KB	13/02/2014 11:41 PM
AES PDF Sample 3.pdf	Application	26,238 KB	13/02/2014 11:41 PM
AES PDF Sample 4.pdf	Application	20,720 KB	13/02/2014 11:41 PM
AES PDF Sample 5.pdf	Application	24,486 KB	13/02/2014 11:42 PM
AES Text Document Sample 1	Application	342 KB	13/02/2014 11:42 PM
AES Text Document Sample 2	Application	342 KB	13/02/2014 11:42 PM
AES Text Document Sample 3	Application	342 KB	13/02/2014 11:43 PM
AES Text Document Sample 4	Application	342 KB	13/02/2014 11:43 PM
AES Text Document Sample 5	Application	342 KB	13/02/2014 11:43 PM
AES Word Document Sample 1	Application	364 KB	13/02/2014 11:43 PM
AES Word Document Sample 2	Application	364 KB	13/02/2014 11:44 PM
AES Word Document Sample 3	Application	364 KB	13/02/2014 11:44 PM
AES Word Document Sample 4	Application	364 KB	13/02/2014 11:44 PM
AES Word Document Sample 5	Application	364 KB	13/02/2014 11:44 PM

Appendix 44: Table of AESTool “Stored Data” on VM2 (Circled VMs Environment)

File Name	Type	Size
AES Encase File Sample 1	Application	850,013 KB
AES Encase File Sample 2	Application	880,231 KB
AES Encase File Sample 3	Application	898 KB
AES Excel Sample File 1	Application	378 KB
AES Excel Sample File 2	Application	490 KB
AES Excel Sample File 3	Application	411 KB
AES Excel Sample File 4	Application	531 KB
AES Excel Sample File 5	Application	431 KB
AES Graphic Image Sample 1	Application	373 KB
AES Graphic Image Sample 2	Application	358 KB
AES Graphic Image Sample 3	Application	351 KB
AES Graphic Image Sample 4	Application	349 KB
AES Graphic Image Sample 5	Application	358 KB
AES Graphic Image Sample 6	Application	399 KB
AES Graphic Image Sample 7	Application	2,342 KB
AES Graphic Image Sample 8	Application	2,404 KB
AES Graphic Image Sample 9	Application	497 KB
AES Graphic Image Sample 10	Application	485 KB
AES Graphic Image Sample 11	Application	391 KB
AES JPG Carved File Sample 1	Application	345 KB
AES PDF Sample 1.pdf	Application	12,808 KB
AES PDF Sample 2.pdf	Application	78,773 KB
AES PDF Sample 3.pdf	Application	26,238 KB
AES PDF Sample 4.pdf	Application	20,720 KB
AES PDF Sample 5.pdf	Application	24,486 KB
AES Text Document Sample 1	Application	342 KB
AES Text Document Sample 2	Application	342 KB
AES Text Document Sample 3	Application	342 KB
AES Text Document Sample 4	Application	342 KB
AES Text Document Sample 5	Application	342 KB
AES Word Document Sample 1	Application	364 KB
AES Word Document Sample 2	Application	364 KB
AES Word Document Sample 3	Application	364 KB
AES Word Document Sample 4	Application	364 KB
AES Word Document Sample 5	Application	364 KB

Appendix 45: Table of AESTool “Stored Data” Copied on VM1 from VM2 (Circled VMs Environment)

File Name	Type	Size
AES Encase File Sample 1	Application	850,013 KB
AES Encase File Sample 2	Application	880,231 KB
AES Encase File Sample 3	Application	898 KB
AES Excel Sample File 1	Application	378 KB
AES Excel Sample File 2	Application	490 KB
AES Excel Sample File 3	Application	411 KB
AES Excel Sample File 4	Application	531 KB
AES Excel Sample File 5	Application	431 KB
AES Graphic Image Sample 1	Application	373 KB
AES Graphic Image Sample 2	Application	358 KB
AES Graphic Image Sample 3	Application	351 KB
AES Graphic Image Sample 4	Application	349 KB
AES Graphic Image Sample 5	Application	358 KB
AES Graphic Image Sample 6	Application	399 KB
AES Graphic Image Sample 7	Application	2,342 KB
AES Graphic Image Sample 8	Application	2,404 KB
AES Graphic Image Sample 9	Application	497 KB
AES Graphic Image Sample 10	Application	485 KB
AES Graphic Image Sample 11	Application	391 KB
AES JPG Carved File Sample 1	Application	345 KB
AES PDF Sample 1.pdf	Application	12,808 KB
AES PDF Sample 2.pdf	Application	78,773 KB
AES PDF Sample 3.pdf	Application	26,238 KB
AES PDF Sample 4.pdf	Application	20,720 KB
AES PDF Sample 5.pdf	Application	24,486 KB
AES Text Document Sample 1	Application	342 KB
AES Text Document Sample 2	Application	342 KB
AES Text Document Sample 3	Application	342 KB
AES Text Document Sample 4	Application	342 KB
AES Text Document Sample 5	Application	342 KB
AES Word Document Sample 1	Application	364 KB
AES Word Document Sample 2	Application	364 KB
AES Word Document Sample 3	Application	364 KB
AES Word Document Sample 4	Application	364 KB
AES Word Document Sample 5	Application	364 KB

Appendix 46: Table of AESTool “Retrieved Data” from VM1 (Circled VMs Environment)

File Name	Type	Size	Timestamp	MD5 Value	SHA-1 Value
Encase File Sample 1.exe	Application	850,013 KB	13/02/2014 11:29 PM	A1F96B13E979168E3019F7C722560253	AB42310D7B71F6EA454A8FE3E735C032798D95EE
Encase File Sample 2.exe	Application	880,231 KB	13/02/2014 11:35 PM	99689B3DA2F80ACEA1FEC51828581B80	9552DOA98C9C5437E8AAFB680C621BFC93E6F7D
Encase File Sample 3.exe	Application	898 KB	13/02/2014 11:35 PM	014212168F5109B9F421D4E691F78124E	8533A84B7231F0C376904CFB9C6014B21C6DFB7
Excel Sample File 1.exe	Application	378 KB	13/02/2014 11:35 PM	00CF104B7F4418680C090F6E1BE1D54	7CC3D2112D00317837D578E16AC75C17049F2178
Excel Sample File 2.exe	Application	490 KB	13/02/2014 11:36 PM	AAE560C7ADDEADA54D7821807973C2550	7B0077169D98A2227182693686EF57A36976E1D
Excel Sample File 3.exe	Application	411 KB	13/02/2014 11:36 PM	BF307088D01E5F56613852D2DA513317	AA96B788555F1732E25B994F450328B16F415693
Excel Sample File 4.exe	Application	531 KB	13/02/2014 11:37 PM	25ED898EEB91E958CF3E227FD51DF4E4	8C548D878FCBE5C53822C1F3B843307339EA9D
Excel Sample File 5.exe	Application	431 KB	13/02/2014 11:37 PM	50BB45D5C913A778191921FCDAAFA08	D3A4E0F78F8FD124DD87A9C7FA99CDBD53E17FE
Graphic Image Sample 1.exe	Application	373 KB	13/02/2014 11:37 PM	C8E4C0328100B8186F926D9F1EA39403	9D61DF08F66E02F3ECB433807AAC5967015EE2E
Graphic Image Sample 2.exe	Application	358 KB	13/02/2014 11:38 PM	3C3AD4EAD19BDAFCA9D979615C88144D	C20D6E63A23F8EB3A1516A171667F4FC26B7B807
Graphic Image Sample 3.exe	Application	351 KB	13/02/2014 11:38 PM	1D21EAD57C30F3E701D6D7276888AD8C	1DB3C83AD302F5D30AD8FBCD1FEB38FF9F2F05
Graphic Image Sample 4.exe	Application	349 KB	13/02/2014 11:38 PM	16B1B7F497C075951AC1BE12456EA424	3E83DCD58E8EB29A1432DD117F2C28C5D52A7768
Graphic Image Sample 5.exe	Application	358 KB	13/02/2014 11:38 PM	A07EF50F835966E4857DABD3D4E541BC	A9126477A4B2DAFB18D2598EB269A8EC8103FFE1
Graphic Image Sample 6.exe	Application	399 KB	13/02/2014 11:39 PM	5A19FC6122488648F81C37C981E5161A	2A0D5C3CEC60C05588623FE72838725FB113A37E
Graphic Image Sample 7.exe	Application	2,342 KB	13/02/2014 11:39 PM	767D519E9AB1AC9B9696A1412FB4E44	02B84DD499D1F14F7466E7162903DE7C7673BEC
Graphic Image Sample 8.exe	Application	2,404 KB	13/02/2014 11:39 PM	881C91DC63276836A6DBD8E145D8C71	8CFF1CC5F49F34A527C56455DD682E111C83DC3F
Graphic Image Sample 9.exe	Application	497 KB	13/02/2014 11:39 PM	2785DE0A7224C620EE038F8A5C81C16	CA85DB8C93CD88DEA0DE6CC727C84D37CCE44D2F9
Graphic Image Sample 10.exe	Application	485 KB	13/02/2014 11:40 PM	4C0FAFEA1BCD92594E9228087CFE1897	6FCA05013D197948C9088B2F383121AAA29541D
Graphic Image Sample 11.exe	Application	391 KB	13/02/2014 11:40 PM	31C4650C41C4836FAFB3A3710AA242C	D0717D815684687CA696D056C363754552392947
JPG Carved File Sample 1.exe	Application	345 KB	13/02/2014 11:40 PM	93DEE41DC614D008C81FC1BA30617316	27E2B0C867EF44ED172665D8989DA40E2329837C
PDF Sample 1.pdf.exe	Application	12,808 KB	13/02/2014 11:41 PM	84D337AE2266ECE0810AE337A1DEC889	5E70B2554407667428AA9CDB11EECA24C1BB360E
PDF Sample 2.pdf.exe	Application	78,773 KB	13/02/2014 11:41 PM	9AC84AFE1BF90DFB8899190C3BF856AC	6A2A20147DC502E57E5C72A6EC5CD3C36F80D75
PDF Sample 3.pdf.exe	Application	26,238 KB	13/02/2014 11:41 PM	82E0C172BA53572ADA81E8AE939F6A43	84AB50EA17DCB33FBA0A982573515838E6F4B4D3
PDF Sample 4.pdf.exe	Application	20,720 KB	13/02/2014 11:41 PM	2AE9F73C06D1D8C480C7A1FBCAFE0A92	CD568C450361586E3422819DA98269A0E0C88A33
PDF Sample 5.pdf.exe	Application	24,486 KB	13/02/2014 11:42 PM	271198DD04E60A2706AA294CE8FB2CE	4A4753577DD98545DA79D227E8D79FDF516621F
Text Document Sample 1.exe	Application	342 KB	13/02/2014 11:42 PM	1D558F133737877303AC8FFC29345513	3822EC157A8FD118B706DFF48FE15C8D6580868
Text Document Sample 2.exe	Application	342 KB	13/02/2014 11:42 PM	03C6657F56FD04A20CA39E16CDA684FC	C27896D1320E1892FA889BA82B6178EC182691B7
Text Document Sample 3.exe	Application	342 KB	13/02/2014 11:43 PM	AA655ADAC03315FB2591E18011D2D0F1	B9F912D9A9B76D154C0EA98289FC26868851A222
Text Document Sample 4.exe	Application	342 KB	13/02/2014 11:43 PM	2AE9F73C06D1D8C480C7A1FBCAFE0A92	CD568C450361586E3422819DA98269A0E0C88A33
Text Document Sample 5.exe	Application	342 KB	13/02/2014 11:43 PM	A1C90CA7A6C6AAEC5E3AC363316F4C69	8CBA3A4E37A3C050A104ADC61ED161C96202007D
Word Document Sample 1.exe	Application	364 KB	13/02/2014 11:43 PM	B4078169F5BFAA31E08491FFE3DD1D0F	16E8A1A778689CAE3E0FF2BF9E7B588445DC1CFF
Word Document Sample 2.exe	Application	364 KB	13/02/2014 11:44 PM	252D48A0A2EE9F4E55C1FABE6493C8A0	54C80820F8837B9961600673E2C71613F5E56D75
Word Document Sample 3.exe	Application	364 KB	13/02/2014 11:44 PM	AA655ADAC03315FB2591E18011D2D0F1	B9F912D9A9B76D154C0EA98289FC26868851A222
Word Document Sample 4.exe	Application	364 KB	13/02/2014 11:44 PM	F5790A28DA3DF80668FCC2E3276E13	94D456A2D645240C7D5B2615A31E785DE1AE02D
Word Document Sample 5.exe	Application	364 KB	13/02/2014 11:44 PM	1A8F3FD825F6FB43388AEADDDF223EB3	8BFB3DD0A2986526F3790AF44CF9222AADB48A9

Appendix 47: Table of AESTool “Recovered Data” from VM1 (Circled VMs Environment)

File Name	Type	Size	Timestamp	MD5 Value	SHA-1 Value	Successful Decryption	Secret Key	Algorithm
Encase File Sample 1.ex01	Encase Evidence File	849,671 KB	14/02/2014 05:07 PM	5999BCFA0E9D70A5375F2808ED1A4526	4FC9B5E7076FA5EC23207F05431E0CF54ACAE99	Yes	ABCDFF1	AES-64
Encase File Sample 2.ex01	Encase Evidence File	879,889 KB	14/02/2014 05:07 PM	372DA2D8023238893E41B7E125561DF80	401A423CCED9309B9A1A6C0B1F56875E3C0D358F	Yes	ABCDFF1	AES-64
Encase File Sample 3.ex01	Encase Evidence File	556 KB	14/02/2014 05:07 PM	01186AAC49D373208279C8C9264C5023	842A4ACD081A2CB76D6E63407618D4857483082EC	Yes	ABCDFF1	AES-64
Excel Sample File 1.xls	Microsoft Excel 97-2003 Worksheet	36 KB	14/02/2014 05:08 PM	2C938882A40C051721B52B0FA1F3D0CF	A838C97C488CD50A26A69178D57C8028982680	Yes	ABCDFF1	AES-64
Excel Sample File 2.xls	Microsoft Excel 97-2003 Worksheet	148 KB	14/02/2014 05:08 PM	5637DFC46A6998776E86A2071147FF	10A0A707D9299594072E275FE4E72F65D12E1844A	Yes	ABCDFF1	AES-64
Excel Sample File 3.xls	Microsoft Excel 97-2003 Worksheet	69 KB	14/02/2014 05:08 PM	B1A2A3D1F54A0C276580A0529D962E5	21C77EDC486A0CA6CE1705C54E3373FF3080AC18	Yes	ABCDFF1	AES-64
Excel Sample File 4.xls	Microsoft Excel 97-2003 Worksheet	189 KB	14/02/2014 05:08 PM	C2193FB63A055364FC8681D352ED0E4	C0FEA95E16852F96019D994E30773FF3080AC18	Yes	ABCDFF1	AES-64
Excel Sample File 5.xls	Microsoft Excel 97-2003 Worksheet	89 KB	14/02/2014 05:08 PM	0A5EFA78D8389F821C71BF92A0D92C802	1598F806D3F78987B5BCF0A78249D8259157167	Yes	ABCDFF1	AES-64
Graphic Image Sample 1.jpg	JPG File	31 KB	14/02/2014 05:08 PM	9D0B74080781688787AE94882C36D65A	44973E2C6D04D68FB8D27C0A4CB9405EABD460C	Yes	ABCDFF1	AES-64
Graphic Image Sample 2.jpg	JPG File	16 KB	14/02/2014 05:09 PM	8CFB10680A4C107A7A1628751D37600	C728E068A1D9681C01844620A8AEGCDF4C8269E	Yes	ABCDFF1	AES-64
Graphic Image Sample 3.jpg	JPG File	10 KB	14/02/2014 05:09 PM	A474E2E36810DF9B8C0CDE68CF696AC3	0F60F38CE587A0DFC996F8D4867AF11D2581C	Yes	ABCDFF1	AES-64
Graphic Image Sample 4.jpg	JPG File	8 KB	14/02/2014 05:09 PM	CC153888180FC973F980FD51B63484D5	31895FA91D7F353D0D3018E7900538891F4FDDAB	Yes	ABCDFF1	AES-64
Graphic Image Sample 5.jpg	JPG File	17 KB	14/02/2014 05:09 PM	1A55258C59F37DADA2916E645458013	A9F56E8F3C196A41AE0A56907EEF78A0D5EBD	Yes	ABCDFF1	AES-64
Graphic Image Sample 6.jpg	JPG File	57 KB	14/02/2014 05:09 PM	D2F1C6CAB6E06FAA4DEA02D7DAF2972	A3550F9285239F679CA13928458314D3B4FC0D59	Yes	ABCDFF1	AES-64
Graphic Image Sample 7.jpg	JPG File	2,001 KB	14/02/2014 05:09 PM	E9E0E7C8DE53CEAC4344AD566F48CC	0534321762701F9487FBCAC0B29D0C1D385C55E	Yes	ABCDFF1	AES-64
Graphic Image Sample 8.jpg	JPG File	2,063 KB	14/02/2014 05:09 PM	FAS061640889197E262B68960B84332	9F558F953D9239E4099DA978B1A0848573081DDC	Yes	ABCDFF1	AES-64
Graphic Image Sample 9.jpg	JPG File	155 KB	14/02/2014 05:10 PM	270657AAD13079248356C2E876E59ACA	349A53444085715A3F25C02348C5F9808668745D	Yes	ABCDFF1	AES-64
Graphic Image Sample 10.jpg	JPG File	143 KB	14/02/2014 05:10 PM	0685014A7E15A18A026E25B53147B61	8E65F801055483BEEFDD02A54D578F02C57995A	Yes	ABCDFF1	AES-64
Graphic Image Sample 11.jpg	JPG File	50 KB	14/02/2014 05:10 PM	822335956740AE0E1664A3081786A05	FC82303A74FE9E88879085F9B303A3C04F9782	Yes	ABCDFF1	AES-64
JPG Carved File Sample 1.PNG	PNG File	3 KB	14/02/2014 05:10 PM	091523D16882626C76538270B2641DF	AS9252A8A6E8D28F70A568318C9259D2A7F5D03	Yes	ABCDFF1	AES-64
PDF Sample 1.pdf	Adobe Acrobat Document	12,466 KB	14/02/2014 05:10 PM	D51CEFF4D858F681093A00C81F510F4	70FEE206A8B64A3641AA77E2A8D07BAAC39853F	Yes	ABCDFF1	AES-64
PDF Sample 2.pdf	Adobe Acrobat Document	78,432 KB	14/02/2014 05:10 PM	9810CFE41BFF7E0D4BCCC196A5D4BC7	43109E07612EACAGAD9AA868281136BA8548A9	Yes	ABCDFF1	AES-64
PDF Sample 3.pdf	Adobe Acrobat Document	25,897 KB	14/02/2014 05:10 PM	8707AB8772E5C7381863D8A5E8B579D5	F1725A9C76678E179033858D806C352F902A77	Yes	ABCDFF1	AES-64
PDF Sample 4.pdf	Adobe Acrobat Document	20,379 KB	14/02/2014 05:11 PM	6E6F8E9F1A8C66841538F54641F90A5	D6DE07099138978820C38370A59131AE5116D	Yes	ABCDFF1	AES-64
PDF Sample 5.pdf	Adobe Acrobat Document	24,144 KB	14/02/2014 05:11 PM	F0FBC1D0A077F2908EC34AE188583DA	5160219A2648F48DEF85D9E968C08A42E2B500F	Yes	ABCDFF1	AES-64
Text Document Sample 1.txt	Text Document	1 KB	14/02/2014 05:11 PM	B238248E195842EAD0C5EE93170714F	FD40713A8FC610F724EA15CC05A78A6A95966D	Yes	ABCDFF1	AES-64
Text Document Sample 2.txt	Text Document	1 KB	14/02/2014 05:11 PM	05C0DE79F3A88248C14FC3966E2897	C4896825050AE60E918A798C3E80E0FF496497	Yes	ABCDFF1	AES-64
Text Document Sample 3.txt	Text Document	1 KB	14/02/2014 05:11 PM	9873AB89C24FE151AD0C9720C687C54	7D1049242613314B7449201EA100779881668C	Yes	ABCDFF1	AES-64
Text Document Sample 4.txt	Text Document	1 KB	14/02/2014 05:11 PM	834E58E13C0A4D04F1AE8B18C7205AF	8815948E0D32F44E434D2C3A0F031475461C24D0	Yes	ABCDFF1	AES-64
Text Document Sample 5.txt	Text Document	1 KB	14/02/2014 05:11 PM	F858250C7181038E3FDCAF8318E420	30C79410AC06979FA690DF1A2E20C8F264E0	Yes	ABCDFF1	AES-64
Word Document Sample 1.doc	Microsoft 97-2003 Document	22 KB	14/02/2014 05:12 PM	26388348D0C058F7382AD28446D6F38	8293FC6A29F75799E12AF86724D5840307C5298	Yes	ABCDFF1	AES-64
Word Document Sample 2.doc	Microsoft 97-2003 Document	22 KB	14/02/2014 05:12 PM	880288FA7E38A44C3E318208A2A2D	B0A4A4FC8791C20A4E48F1278B7848A57B1A091	Yes	ABCDFF1	AES-64
Word Document Sample 3.doc	Microsoft 97-2003 Document	22 KB	14/02/2014 05:12 PM	C6889F9791B454AF974B6D03C77F771	CF870AC35086593F44E6D135451AD9095DAE1	Yes	ABCDFF1	AES-64
Word Document Sample 4.doc	Microsoft 97-2003 Document	22 KB	14/02/2014 05:12 PM	C381FA0CCFC81E873879E7F327A0E07	8705FDA0D773DC406548C8B9C81B0E7A3F8D8B1C	Yes	ABCDFF1	AES-64
Word Document Sample 5.doc	Microsoft 97-2003 Document	22 KB	14/02/2014 05:12 PM	AD85136F7FA881223145C7FE0CADC0AD	7C337354E5D28887E0BA17F451A01F00C1E547	Yes	ABCDFF1	AES-64

Appendix 48: Table of Computer Profile Summary

Computer Name	WT304-009wcw (in AUTUNI)
Operating System	Windows 7 Enterprise (x64) Service Pack 1 (build 7601) Install Language: English (United States) System Locale: English (New Zealand) Installed: 22/02/2013 9:43:08 a.m.
System Model	AUT University AUTOPTCZ68 AUT University AUTOPTCZ68 Asset Tag: 12-0202-0094 Enclosure Type: Desktop
Processor	3.10 gigahertz Intel Core i5-2400 256 kilobyte primary memory cache 1024 kilobyte secondary memory cache 6144 kilobyte tertiary memory cache 64-bit ready Multi-core (4 total) Not hyper-threaded
Main Circuit Board	Board: Intel Corporation DZ68DB AAG27985-104 Serial Number: BTDB212002S3 Bus Clock: 100 megahertz BIOS: Intel Corp. DBZ6810H.86A.0042.2012.0518.1812 05/18/2012
Drives	500.11 Gigabytes Usable Hard Drive Capacity 266.01 Gigabytes Hard Drive Free Space ELBY CLONEDRIVE SCSI CdRom Device [Optical drive] Optiarc DVD RW AD-7280S [Optical drive] WDC WD5000AAKX-00ERMA0 [Hard drive] (500.11 GB) -- drive 0, s/n WD-WMC2E0002411, rev 15.01H15, SMART Status: Healthy
Memory Modules (RAM)	8100 Megabytes Usable Installed Memory

Slot 'DIMM3' is Empty			
Slot 'DIMM1' has 4096 MB (serial number 8B287A06)			
Slot 'DIMM4' is Empty			
Slot 'DIMM2' has 4096 MB (serial number 8B288606)			
Local Volumes	c: (NTFS on drive 0) *	262.14	52.83
		GB	GB free
	d: (NTFS on drive 0)	237.96	213.18
		GB	GB free
* Operating System is installed on c:			
Controllers	Intel(R) Desktop/Workstation/Server Express Chipset		
	SATA AHCI Controller		
Display	Intel(R) HD Graphics [Display adapter]		
	Philips 225B [Monitor] (21.7"vis, s/n DL51142355697, October 2011)		
Multimedia	Intel(R) Display Audio		
	Realtek High Definition Audio		
Bus Adaptors	Virtual CloneDrive		
	Intel(R) 6 Series/C200 Series Chipset Family USB Enhanced Host Controller - 1C26		
	Intel(R) 6 Series/C200 Series Chipset Family USB Enhanced Host Controller - 1C2D		
	Renesas Electronics USB 3.0 Host Controller		
	Renesas Electronics USB 3.0 Root Hub		
Virus Protection	ESET NOD32 Antivirus Version		
	4.2.76.0		
	Realtime File Scanning On		