Forensic Analysis of Amazon Alexa Echo Dot 4th Generation

Damilola Oladimeji
Dept. of Computer Science
Sam Houston State University
Huntsville, Texas, US
dko011@shsu.edu

Bing Zhou
Dept. of Computer Science
Sam Houston State University
Huntsville, Texas, US
bxz003@shsu.edu

2022 IEEE International Conference on Big Data (Big Data) | 978-1-6654-8045-1/22/$31.00 ©2022 IEEE | DOI: 10.1109/BigData55660.2022.10020328

***Abstract*—Internet of Things devices such as Amazon Alexa have grown in popularity over the years due to the ease it gives to its' user. As a result of the common occurrence of crimes taking place at homes, especially violent crimes there is a high possibility of the presence of an Alexa when a criminal investigation occurs; thus, forensic investigations on these devices are required to assess the evidential value to forensic examiners. This paper focused on the carrying out a forensic investigation of Amazon Alexa Echo Dot 4th generation on the software and the cloud level. This paper shows how forensic artifacts could be obtained from the Alexa application on an iPhone and an Android smartphone, as well as adapted and described an open source tool that can be used to collect evidence from an Amazon Alexa Echo Dot 4th generation at the cloud level.**

***Index Terms*—Alexa, Amazon Echo, Alexa Forensics, Internet of Things, IoT forensics, Alexa app**

I. Introduction

The use of Internet of Things (IoT) devices has recently increased dramatically. Many of these gadgets may be credited to the smart home idea, which is meant to give ease in day-to-day tasks. As a result, they tend to capture and occasionally keep a large amount of personal data about their customers. This data frequently not only identifies the person directly, but also their daily schedules and behaviors. Critical data may even be analyzed, stored, and communicated in the case of wearable smart devices.

According to research, the global market for IoT is set to grow to 657 billion dollars by 2025 [1]. The rise in popularity of IoT devices have also resulted in the growing number of homes that incorporate digital connectivity with voice interaction. Smart fridges, smart door locks, virtual personal assistant, wearable smart devices are some examples of these devices.

With IOT devices such as virtual personal assistants being able to connect the user to smart homes and make schedule actions based on voice commands, they are more prominent than ever. These devices can control appliances in homes such as lights, TV, door locks, and entertainment systems. It is projected that almost every home will have these kinds of devices, thereby increasing the chances of the presence of these devices in crime scenes [2].

One of the most popular smart speakers currently in use today is the Amazon Alexa echo device. As the popularity of the Amazon Echo grows, concerns about user privacy have arisen. Concerns were expressed when the Echo was released regarding whether it was always listening in on conversations and other activities in one's home. Is the data being captured if it is constantly on? If so, how is this data being used? Amazon answered these concerns by detailing how the gadget works. .

These speakers have smart assistants/ Intelligent Personal Assistant (IPA) that take input from users' speech, convert it to text, apply natural language processing (NLP) to this text, act, and then respond as an informative voice message [3]. This complicated task of translating voice is not usually performed locally but is instead sent to the proprietary server for processing [5].

In the case of Amazon Alexa, the gadget listens for the word "Alexa" to be said, which triggers it to begin recording and processing. As a result, Alexa must continually record audio to pick up the instruction and send it to the Amazon cloud for processing [3] [4]. The device is controlled and administered via Companion Clients (laptops with web browsers, mobile devices with the Amazon Alexa App) with direct access to the cloud server [5].

Bloomberg recently reported [6] that Amazon workers have access to customer speech recordings and listen to them to enhance Alexa's voice recognition algorithm. The Echo, according to Amazon, is constantly on and listening, but only for select key phrases like wake and Alexa. Alexa does not pay attention to or record what is spoken around it if these key phrases are not utilized.

A major obstacle that may arise to forensic analyst is the acquisition of the vital data processed by these devices, this is because they are all closed source with Amazon refusing to divulge how they handle the information. Recently, evidence gathered by smart speakers like Alexa and Google Assistant has been substantial and reasonable in a variety of criminal cases [1] [5]. In 2015, Arkansas state police intended to solve a murder case using Amazon Echo data. Several times, it was been claimed that Amazon refused to grant law enforcement authorities access to their servers until the suspect himself opted to submit the data [5].

978-1-6654-8045-1/22/$31.00 ©2022 IEEE

This paper focused on the forensic examination of the IPA known as Alexa used on the Echo Dot 4th generation developed by Amazon. The goal of this paper was to determine the amount of tangible information that is processed and stored by the Echo Dot 4th generation device. This study seeks to address the following questions:

- What forensic artifacts may be retrieved from the Amazon Echo's applications on smartphones (Android and iOS)?
- What forensic cloud artifacts may be retrieved from the Amazon Echo device?
- Can the results of this study provide insights into an effective open source tool that digital forensic investigators can use to analyze cloud services such as Amazon's cloud service (AWS)?
- Where is evidence saved in the Alexa file system?

The rest of this paper is arranged as follows. Section II describes the background and relevant work on Alexa. Section III outlines the Alexa system model and overview of the gadget.In section IV, we detail the methodology adopted in this research as well as the experimentation study and acquisition. Section V discusses the analysis and results of the experimentation carried out. Section VI gives a brief discussion of artefacts found as well as their relevance. Section VII summarizes the conclusion, limitation and future work.

II. Background and Relevant Works

A. Amazon Echo Dot Ecosystem

The first Echo was made available to select Amazon members in 2014, with the business expanding its availability to general consumers the following year. According to reports, when Jeff Bezos realized that getting latency down to a more conversational level was the key to voice assistants, he directed the Alexa team to reduce latency to one second something that had never been done with voice assistants before (the team's goal had been to get latency to an all-time low of two seconds). When they achieved that target, the first Echo was ready for sale [7].

Amazon then saw that some consumers desired a smart speaker that was smaller and more portable than the Echo, and that could be used up close. The Echo Dot has all of the same Alexa functions as the Echo but is housed in a much smaller, cube speaker.

The Echo Dot's first generation was introduced in spring 2016 and was particularly built for smaller settings than the original Echo. In the fall of 2016, Amazon released the 2nd-generation Echo Dot. This version added the ability for Echo Dots to collaborate for shared sound and saw a price decrease. The third-generation Echo Dot was released in 2018. It now featured a fabric cover and a more rounded design, like previous Echos, but that was the end of the alterations. Around the same time, Amazon began selling Echo Dots designed exclusively for children. A new Echo Dot was announced in 2020, radically revolutionizing the range. The new model was a scaled-down replica of the orb-like 4th-generation Echo. The analysis of the Alexa Amazon 4th generation will work for previous generations as this is the most recent currently available in the market.

The Amazon Echo is a line of intelligent virtual assistant devices that come in a variety of sizes and configurations. However, at their heart, they all have a microphone and a speaker and interface with the Amazon Alexa speech service, allowing the user to manage it with voice commands [4].

To start a task using one's voice, the gadget must first be triggered or woken up. This is done by saying wake word: Alexa. When the gadget is awake, it listens for a query or a command. The gadget also starts recording what is spoken after the wake word. The speech clip is then transferred to an Amazon server, where it is processed and returned to the user. Responses often consist of the user's request being fulfilled, such as playing a music or reading the news. On occasion, for clarification purposes, may respectfully query the user with a question (e.g., what time?)

To begin more sophisticated operations, the user must utilize the Amazon Alexa app, which is available for a number of platforms and devices. A user may use the app to add things to their shopping carts or to-do lists, to start, pause, shuffle, and stop music, to set alarms and timers, and to manage smart home devices. This is very useful while traveling away from home. For example, while on vacation, one may use the Alexa app to turn on/off lights or check if a door is closed. A user may also control device settings like as location services and Wi-Fi networks via the app.

Whatever method is used to start tasks, all activities are synchronised with the Alexa app. This means that voice-controlled inquiries and orders sent to the Echo or Echo Dot will appear in the Alexa app, and modifications made in the Alexa app will also be synchronized to the Echo or Echo Dot. Essentially, if an Echo or Echo Dot is used in combination with the Alexa app, they will remain in sync [8].

It was necessary to thoroughly study the architecture of Amazon Alexa in order to carry out forensic study on the target IOT device. As previously stated, the Amazon Echo manages an interface for interacting with the cloud-based service, Alexa. Cloud-based operations, such as Echo and Alexa, constitute a typical operating technique of IoT devices because most are inextricably linked to cloud services in order to provide interoperability with companion clients and compatible devices for user convenience.

The Amazon Alexa ecosystem is made up of numerous components; Fig. 1 depicts the main flow of Alexa activities. First, the user initiates communication with the smart speaker by saying "Alexa,.." followed by the order. The Amazon Cloud service (AWS) then executes and archives such commands. This cloud service handles functions such as authentication, data management, logging, and connection to external compatible devices. The Alexa app on the system (phone, tablet, or laptop) is another crucial component of the Alexa ecosystem. The app provides an interface for the user too view things such as a to-do list, shopping list, alerts, and so on.Additionally, Alexa may be enhanced by connecting to suitable IoT devices and adding skills (third-party apps) for incorporating diverse applications.

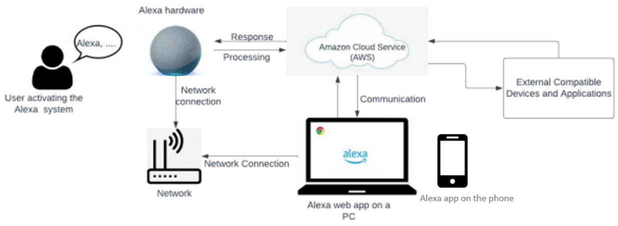


Fig. 1. Amazon Alexa Ecosystem

B. Relevant Works

Research have been conducted on the digital forensic analysis of IOT, which has been widely used in the investigation of Alexa. The validity of data processing from the device to the Alexa cloud services has been brought into doubt since the release of the first Echo smart speaker, and research has been performed to help investigations into digital forensics of Alexa-enabled devices.

Zawoad and Hassan, stated that IOT devices should be analysed in three levels (cloud, network and device) [9], additionally, Li et al., discovered that forensics on Alexa could be performed on three different levels (device level, network level, and cloud level), but many challenges were encountered when attempting to perform IoT forensics due to the complexity of these levels in relation to the device and their relationship with one another [10]. Kebande et al. proposed a framework to conduct Digital forensic on IOT devices which also discusses the three layers Cloud forensics, Network forensics and Device level forensics [11].

Chung et al. [12], who discovered and explained that companion apps on companion clients (laptops, smartphones) include many client-centric artifacts that may be utilized as evidence on Alexa and proposed the Cloud-based Forensic Toolkit (CIFT). While [12] focused on the identification of evidence from Alexa on the cloud and device level, Jessica hyde [13] and Brain Moran carried out forensic investigation on Alexa utilizing both software and hardware forensics approaches in attempt to gather as much information from their Alexa app as possible, including using previously discussed methods.

Recent research studies have recommended investigating cloud-native forensics in IOT devices in order to overcome the basic restriction that vast volumes of data are still not saved in storage devices or are only stored in ephemeral caches. Vassil et al., for example, used APIs enabled by cloud services to develop forensic methodologies on native artifacts of Google Drive, Microsoft OneDrive, Dropbox, and Box. As a result, they were able to put cloud drive acquisition mechanisms in place [14] [15].

On the other hand, Yildirim et al. [2] , Tristan et al., [16] and Engelhardt [17] carried out research on smart speakers using Google home and Alexa as case studies to identify the location of evidence on both devices as well as comparing the quantity of evidence found.

Youn et al. [1] updated the CIFT created by [12] for use on all Alexa Echo Show devices, and they claim to be making the program open source, although progress is still being carried out. Other research so far on Alexa focused on identifying exactly the information being stored on Alexa either from the cloud or the device level [4] [18], [19].

This paper focused on the carrying out a forensic investigation of Amazon Alexa Echo dot 4 th generation on the software and the cloud level. This paper differs from the reviewed literature in that, unlike Youn et al. [1] and Chung et al. [12] that carried out analysis on the cloud level of the Amazon Alexa device, the tool used to carry out this acquisition method is not yet publicly available. This paper emphasizes and examines the tool used in sections III and IV, which is available to the public but difficult to locate and it proposes a methodology on carrying out analysis on the software and cloud level of the Amazon Alexa Echo dot 4th generation device.

III. System Model

This section comprehensively presents the forensic components in the Alexa system model. In this system, we assume the Alexa has been found in a criminal scene and is to be investigated upon by digital forensic analyst to discover the forensic evidence it could proffer in a legally sound manner. This system model highlights the components to be examined in the Alexa Amazon ecosystem.

A. Amazon Alexa Forensic system Model

Alexa's skill set governs the replies provided by the Amazon Echo or Echo Dot, as well as the ability to begin tasks and make adjustments via the Amazon Alexa app. Alexa, like people, has a set of skills or competencies that allow it to execute jobs. These talents, however, are generated by developers and must be activated by the user in order to operate. As a result, Alexa can only comply with and work inside the skill set that has been built and enabled for its use. If a skill does not exist or has not been activated, Alexa will be unable to perform the user's request.

Amazon's Alexa Voice Service, which powers the Echo and Echo Dot, now has over 10,000 skills available [20]. Each of these skills, which range in topic from food to gaming to sports, enables users to build a more personalized experience according to their requirements and interests. The Alexa app allows users to enable skills. They may do this online, in the Amazon Alexa Skills Store, or by asking the Echo Dot. Once activated, users may access skills by saying a predefined set of words or phrases, such as Alexa, set my alarm. If the gadget recognizes the user, their query or command will be replied.

Furthermore, most of this data, if not all of it, is critical to the performance of the Amazon Echo and is required for the continuing advancement of the Alexa Voice Service. For example, in order for some skills, such as Audible, to function, the device needs have access to the user's Audible account in order to get information such as settings, preferences, stations, and playlists. This data is then saved in the cloud and made available for use the next time the user invokes the Audible ability. This stored data enables the gadget to reply to a request not just efficiently but also effectively [8].

The collection of data also improves Alexa's ability for speech recognition. Built with artificial intelligence capable of natural learning, recordings of inquiries and other requests made by Amazon Echo users assist Alexa in developing a better comprehension of linguistic variations such as accents and dialects [21].

As Amazon Alexa is an IoT device, which implies that aside from the specific IoT device (Alexa hardware) or sensor, forensic data might be collected from the internal network (e.g., a firewall or a router) or the cloud [22]. Hence, Alexa Forensics can be classified into four parts: Device level, Software level, IoT forensics, network forensics, and cloud forensics. Fig. 2 below shows the components to target when carrying out a forensic analysis on an Amazon Alexa Echo Dot device.

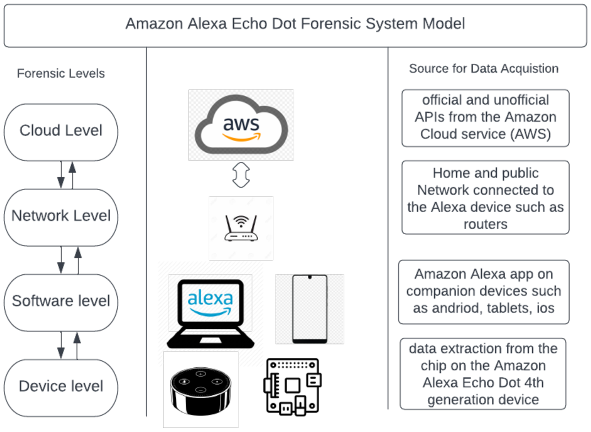

Amazon Alexa Echo Dot Forensic System Model
Forensic Levels
Cloud Level
Network Level
Software level
Device level
aws
alexa
Source for Data Acquistion
official and unofficial APIs from the Amazon Cloud service (AWS)
Home and public Network connected to the Alexa device such as routers
Amazon Alexa app on companion devices such as andriod, tablets, ios
data extraction from the chip on the Amazon Alexa Echo Dot 4th generation device

Fig. 2. Forensic System Model for Amazon Alexa

B. National Institute of Standards and Technology (NIST) Forensic Steps for Digital devices

When investigating a crime, the investigator must follow and refer to device or information technology forensics rules. Although specific procedures, processes, and controls may be retained by nations, organizations, and individual investigators, standardization is intended to result in the adoption of comparable, if not identical, approaches globally. This makes it easy to analyze, integrate, and contrast the findings of such investigations, even when they are conducted by different persons or groups and may span jurisdictions [23].

An integrated application of forensics standards has several advantages, including comprehensiveness and an improvement in the quality of forensic investigations. Forensic investigators can profit from introducing one forensic standard before the other, or from applying both forensic standards concurrently.

The key benefits of integrating the execution of these forensic standards include reliability, cheaper investigative costs, reduced time required for forensic inquiry, and elimination of needless duplication.

In order to ensure the data collected, analysed and reported on is forensically sound, it is important to follow certain standard forensic steps. The U.S. National Institute of Standards and Technology (NIST) forensic procedures were adopted for this investigation. Although this system is used commonly for digital forensic, rather than IOT forensics especially due to the multi-tenant nature of the cloud. However, this research divided the forensic examination into two levels and adapted this steps.

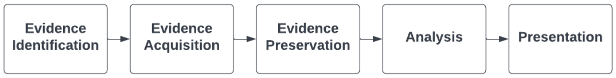


Fig. 3. U.S. National Institute of Standards and Technology (NIST) Forensic Steps for Digital devices

IV. Methodology

The primary purpose of this study was to carry out forensic analysis on a smart speaker using the Amazon Echo Dot 4^{th} generation device as a case study. The aim is to ascertain if the data acquired from these smart speakers have significant evidential value to digital forensic examiners. This section discusses the methods utilized in this study.

As discussed earlier, when conducting an IoT forensic investigation, in this case, Alexa, we must investigate evidence sources other than the actual IoT devices, such as the sensor, network, service, and interface layers (see Fig. 1). The components focused for this particular research are the software and cloud layers which are highlighted in the flowchart below.

The flowchart shows the aspects of the Amazon ecosystem system focused on for this research and shows steps taken to collect and analyze data found 1) online at https://alexa.amazon.com/, 2) in the Alexa app's folder structure, and 3) in the Android and iOS device's cache.

IoT forensics, like traditional digital forensics, relies mostly on four stages: 1) identification; 2) acquisition; 3)preservation; 4) analysis; and 5) presentation [24]. These stages were followed to get forensically sound evidence from the Alexa smart speaker and they briefly discussed below.

Evidence Identification During the identification step, the emphasis was on the IoT device (Amazon echo dot) and any connected infrastructure (e.g., routers).This study methods for data collection was determined by the data used to populate the IOT speakers. The categories of data have been divided into groups to aid in the analysis and assessment of the data collected.This is depicted is Table 1.

1) Evidence Acquisition : Due to the numerous forms of data storage and their locations, this study used two alternative ways to obtain and evaluate the data. The initial approach was

TABLE I
CATEGORIZATION OF DATA FOR COLLECTION

Category	Description
Alexa Data	Metadata about the device such as the name, serial number, make.
Network Information	Data about the internet connectivity such as Router details, IP and MAC information.
User data	Data that contains information about the user, interactions between the user and the device, lists, calendars, remainders.
Application Data	Data that identifies the software residing on the mobile phones such as user login details, and the details of the interactions between the app and the cloud and smart speaker.

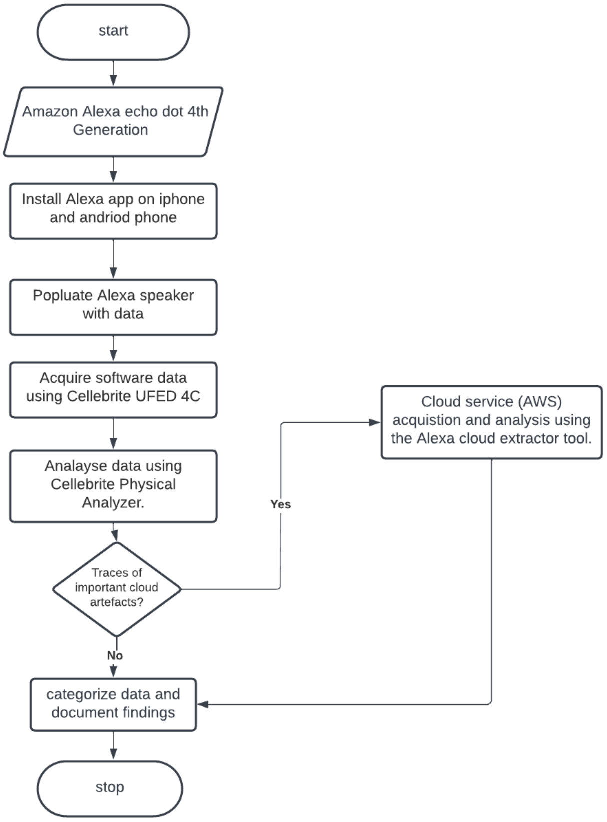

start
Amazon Alexa echo dot 4th Generation
Install Alexa app on iphone and andriod phone
Popluate Alexa speaker with data
Acquire software data using Cellebrite UFED 4C
Analayse data using Cellebrite Physical Analyzer.
Traces of important cloud artefacts?
Yes
Cloud service (AWS) acquistion and analysis using the Alexa cloud extractor tool.
No
categorize data and document findings
stop

Fig. 4. Flowchart of the experiment

manual extraction, which is described as ”capturing information brought up on a mobile device screen when using the user interface” in the Guidelines on Mobile Device Forensics [25]. Except for the use of a digital camera for note taking, manual extraction takes place without the use of forensic instruments. To see the contents of a mobile device, an investigator just uses the screen or keyboard [8].

The second approach was logical backup extraction, a more contemporary way of obtaining and evaluating evidence, has various advantages, the most notable of which is that it is forensically sound. The integrity of the data is preserved since it is not altered throughout the backup or analysis processes. Furthermore, logical backup extraction gives an additional method for recovering data from a device if the device is lost or destroyed. The analysis and extraction is discussed in detail in the next section titled Experimental setup & results.

2) Evidence Preservation: Preservation entails isolating, safeguarding, and preserving the status of physical and digital evidence. It entails halting or prohibiting any acts that might jeopardize the collection of digital information [26]. After acquisition of evidence, It was critical to take safeguards after acquiring evidence to verify that the evidence analyzed and reported were not corrupted. To achieve this, after acquisition, a hash of the evidence was taken and during analysis, that hash was used to check the integrity of the evidence folder analysed.

3) Evidence Analysis: To be able to interpret data collected and analyzed meaningfully, we must be familiar with the smart speaker’s native artifacts and file system. Amazon echo uses SQLite databases and web cache files that contain relevant information, such as accounts and interactions with Alexa, in relation to Amazon Echo. Hence, it is required to locate app data artifacts saved within laptop and use them to improve the outcomes of cloud-native forensics. Furthermore, because client-centric (app data) artifacts such as local databases and cache files are inextricably linked to cloud-side data, it is vital to first comprehend raw cloud data. Amazon echo uses SQLite databases and web cache files that contain relevant information, such as accounts and interactions with Alexa, in relation to Amazon Echo. During the examination of collected evidence, it was helpful to take note of the storage format in the SQLite database and the web cache files. By doing so, the information was be interpreted correctly.

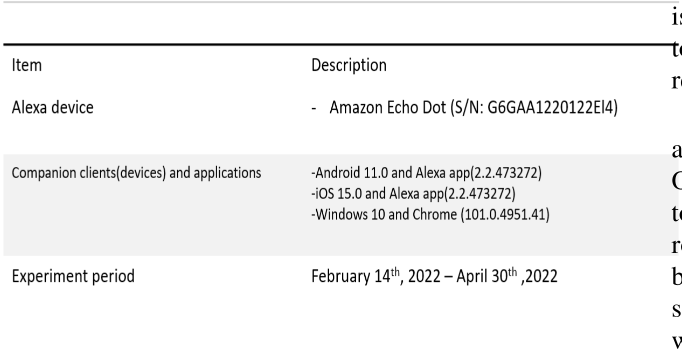
4) Presentation: The reporting process creates a complete record of all procedures done and conclusions reached during the case inquiry. This includes the use of forensic tools and procedures to ensure that the final report is consistent with the data supplied. This requires creating a report explaining the examination procedure and important facts gathered from the entire inquiry. This stage is what this paper aims to achieve.

A. *Experimental setup*

In this study, simulated user data was loaded into a sample Echo device, the dummy single user account that was be created for this experiment was called ***Test1*** Lab. The first phase of the study began on February 14, 2022 with the installation of an Amazon Echo Dot (4th Generation) in a shared space of a single person home. The Echo Dot was used by all three people in a single-family home for 10 weeks and 5 days. During this period, the Echo Dot was never turned off or silenced. This configuration supplied the Echo Dot with a regular yet standard stream of data to gather in the form of voice commands.

The experimental research environment also included two phones an Android and an iOS with the Component client app (Amazon Alexa app) downloaded and installed on them, all hardware devices (Alexa device and phones) were connected to the same wireless network.

Furthermore, the smart home skills the user will refer to while using Alexa was created on the Alexa skills kit website. These skills, like any other device function, are triggered by the wake word "Alex" followed by the user's voice command, which might be anything from turning on the light/TV to setting Alexa to guard mode while the user is away from home and even locking the front doors with Smart locks. The category of data targeted for this experiment will include account information, devices connected to the Alexa smart speaker, skills in operation on that device, user activities and finally the voice recordings of the user. Taking all these categories into consideration ensured the robustness and the copiousness of the data collected and investigated upon. The components are outlined in fig. 5 below.



Item	Description
Alexa device	- Amazon Echo Dot (S/N: G6GAA1220122El4)
Companion clients(devices) and applications	-Android 11.0 and Alexa app(2.2.473272) -iOS 15.0 and Alexa app(2.2.473272) -Windows 10 and Chrome (101.0.4951.41)
Experiment period	February 14th, 2022 – April 30th ,2022

Fig. 5. Components of Experimental setup

B. *Acquisition stage*

After the experimental environment has been set up and the device used as the case study has been populated with data as required, the next step was to extract the data used to populate the device. Data was extracted in two phases:

- Software Level: that is acquiring data from the companion app installed on the smartphones
- Cloud Level: acquiring the Amazon cloud data for this particular user ***Test1***.

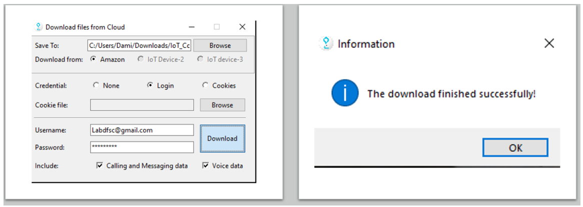
Fig. 4 highlights the steps adopted to acquire and analyse data in this research. The advantage of this proposed design is that it employs an agile analysis method that consider s the most crucial features to be investigated for forensic inquiry. This design provided a mechanism to identify the location of stored data on the Alexa echo dot 4th generation device targeted locations for this research.

1. **Software Phase Acquisition:** Data was extracted from the companion app installed on the Android and iOS . The tool used to acquire data from the smartphone was Cellebrite UFED 4PC. This tool is a commercial software that allows for the full system extractions from both iOS and Android devices. The data extracted was parsed through the Cellebrite Pyhsical Analyzer for analysis separately for the iOS device and Android device. Fig. 4 shows the acquired data from the Android smartphone used in this experiment. For this research, we performed a logical backup acquisition on the Android device and an full system acquisition for the iOS device.

2. **Cloud Phase Acquisition:** Since the device's bulk processing and storage is done on the cloud, the next phase was to retrieve data from the cloud. Echos Smart Speakers utilize the Alexa Voice Service (AVS) to store and process data from the running device. Usually, communications between the user and Alexa hardware is established via an internet connection with the Amazon cloud service (AWS) by entering the registered users' user ID and password. The purpose of extraction in this step is to assess whether critical artifacts such as user accounts, audio recordings, Wi-Fi settings, and card data can be recovered after analysis.

The open source tool used to acquire data from the cloud is called the Alexa Cloud extractor tool [27]. It is important to note that code of this tool had to be modified to suite this research. The tool can be seen in Fig 6 below.

The tool runs on python and requires dependencies such as selenium and Mozilla Firefox driver to run successfully. Once the interface on the extraction system is accessed, the tool requires a valid userID and password to utilize the login route to extract data from the cloud, or a cookies file may be uploaded as well. After download is complete, it gives a successful message and one can navigate to the storage path where the cloud data is stored. This results were returned in .json files and voice data were returned in .wav format.



Download files from Cloud

Save To: C:/Users/Dami/Downloads/IoT_Cc
Download from: ● Amazon ○ IoT Device-2 ○ IoT device-3
Credential: ○ None ● Login ○ Cookies
Cookie file:
Username: Labdfsc@gmail.com
Password: *********
Include: ☑ Calling and Messaging data ☑ Voice data

Information

The download finished successfully!

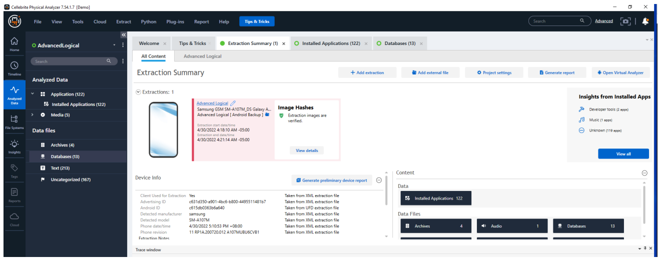
Fig. 6. Cloud extractor Tool

V. Results

This section shows the discusses the processes taken and tools used to acquire data from the Alexa device and the subsequent discoveries after investigating the acquired image.

A. *Analysis Procedure*

1) Analysis of the image of the Alexa app from the Android phone: From the acquisition phase, the full system extraction was parsed through the Cellebrite Physical analyzer for analysis. After going through each folder location shown in analysis tool, we located the location of the Alexa app on the Android device.

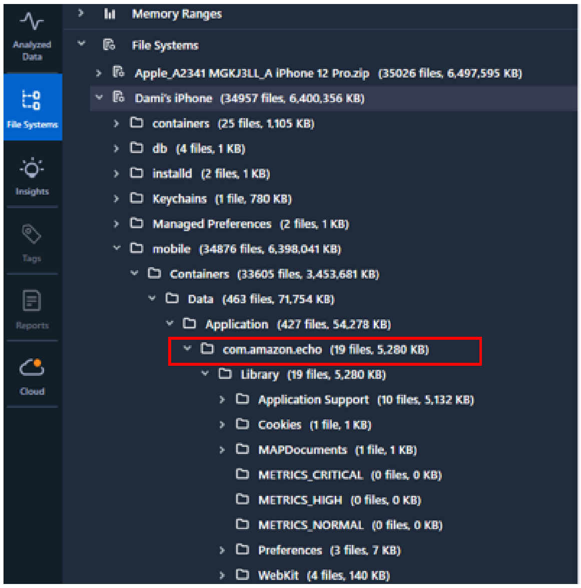


Client Used for Extraction	Yes	Taken from XML extraction file
Advertising ID	c631d350-a901-4bc6-b800-4495511481b7	Taken from XML extraction file
Android ID	c615db0363b6a640	Taken from UFD extraction file
Detected manufacturer	samsung	Taken from XML extraction file
Detected model	SM-A107M	Taken from XML extraction file
Phone date/time	4/30/2022 5:10:53 PM +08:00	Taken from XML extraction file
Phone revision	11 RP1A.200720.012 A107MUBU6CVB1	Taken from XML extraction file
Extraction Notes		

Fig. 7. Analysis of the Andriod phone on Cellebrite Physical analyzer

Fig. 7 reveals the information about Alexa storage on the Android phone that was examined. The directory gotten from the android device relating the to the app can be found in the ***data.amazon.dee.app.framework.AlexaApplication***.

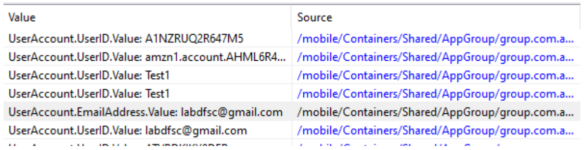
2) Analysis of the image of the Alexa app from the iOS phone: The analysis of the iPhone image acquired was parsed through Celebrite Physical analyzer. The bulk of the files relating to Alexa on the iPhone device was stored in the directory labelled ***com.amazon.echo***.Fig. 8 shows the this directory had 19 files and a it had a size of 5,280KB.



```
> Memory Ranges
v File Systems
  > Apple_A2341 MGKJ3LL_A iPhone 12 Pro.zip (35026 files, 6,497,595 KB)
  v Dami's iPhone (34957 files, 6,400,356 KB)
    > containers (25 files, 1,105 KB)
    > db (4 files, 1 KB)
    > installd (2 files, 1 KB)
    > Keychains (1 file, 780 KB)
    > Managed Preferences (2 files, 1 KB)
    v mobile (34876 files, 6,398,041 KB)
      v Containers (33605 files, 3,453,681 KB)
        v Data (463 files, 71,754 KB)
          v Application (427 files, 54,278 KB)
            v com.amazon.echo (19 files, 5,280 KB)
              v Library (19 files, 5,280 KB)
                > Application Support (10 files, 5,132 KB)
                > Cookies (1 file, 1 KB)
                > MAPDocuments (1 file, 1 KB)
                  METRICS_CRITICAL (0 files, 0 KB)
                  METRICS_HIGH (0 files, 0 KB)
                  METRICS_NORMAL (0 files, 0 KB)
                > Preferences (3 files, 7 KB)
                > WebKit (4 files, 140 KB)
```

Fig. 8. Location of the Alexa app on the iPhone device

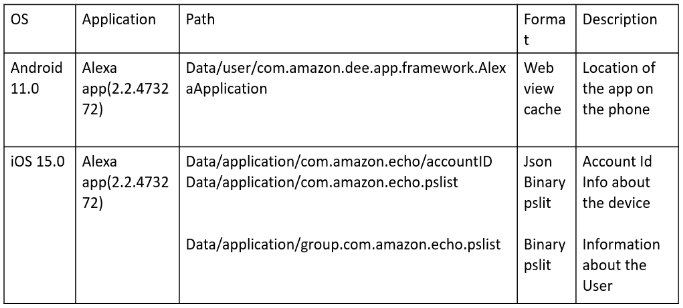
The iPhone analysis produced more result than the Android device, from the analysis of the iPhone image acquired, we found information such as the hashed password, phone number registered user, User ID as well as the cookies files relating the the Alexa app on the iPhone device. We also encountered some encrypted .json files from our analysis, this files were linked to the account ID and local storage Db on the SQLite database. The date and time are presented in Unix format. This information is really crucial. The app will only contain all information if it has been correctly synced to the present state. For the first time, information about the user other than the userID was available in the file service.identity.xml. The user name and email address used to create the Amazon account are saved here. The latter, in particular, is critical to the effective operation of the cloud analysis. This is depicted in Fig. 9.



Value	Source
UserAccount.UserID.Value: A1NZRUQ2R647M5	/mobile/Containers/Shared/AppGroup/group.com.a...
UserAccount.UserID.Value: amzn1.account.AHML6R4...	/mobile/Containers/Shared/AppGroup/group.com.a...
UserAccount.UserID.Value: Test1	/mobile/Containers/Shared/AppGroup/group.com.a...
UserAccount.UserID.Value: Test1	/mobile/Containers/Shared/AppGroup/group.com.a...
UserAccount.EmailAddress.Value: labdfsc@gmail.com	/mobile/Containers/Shared/AppGroup/group.com.a...
UserAccount.UserID.Value: labdfsc@gmail.com	/mobile/Containers/Shared/AppGroup/group.com.a...

Fig. 9. Location of the information about user

Fig. 10 shows the directories that had information about the Alexa app on both the iPhone and the Android device. This shows the location this information was stored, the details stored, and the format in which they were saved on each of the device analyzed.



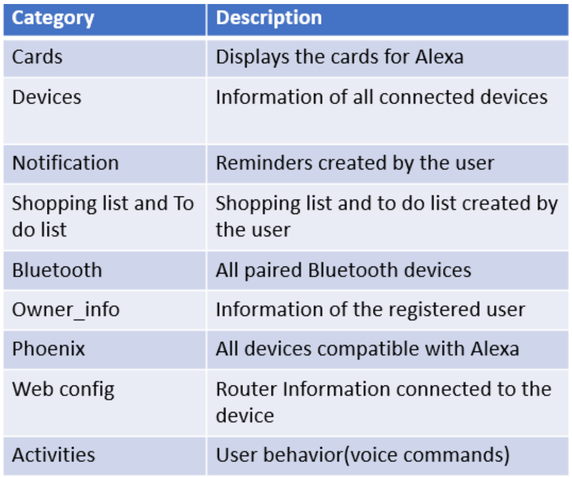
OS	Application	Path	Forma t	Description
Android 11.0	Alexa app(2.2.4732 72)	Data/user/com.amazon.dee.app.framework.Alex aApplication	Web view cache	Location of the app on the phone
iOS 15.0	Alexa app(2.2.4732 72)	Data/application/com.amazon.echo/accountID Data/application/com.amazon.echo.pslist	Json Binary pslit	Account Id Info about the device
		Data/application/group.com.amazon.echo.pslist	Binary pslit	Information about the User

Fig. 10. Directory of the artifacts found on the iPhone and Android Device

3) Analysis of the Cloud Data from Alexa: From the Alexa Cloud Extraction Tool, the cloud data gotten from Alexa were in .json file format and the voice data gotten were in .wav file format. The table below shows a list of the categories acquired using the tool. This tool uses unofficial Amazon APIs to access and download the cloud data.

The cloud data provided the most information to investigators. It was no doubt that the information discovered on the cloud level were significantly greater and more useful because bulk processing and storage id carried out on the cloud.

From the data seen in the Fig. 10, we were able to significant information such as the user activities, the information about the user, web configuration such as the router name and password, the user to do list and shopping list, address of the user, information about the Alexa hardware (such as serial



Category	Description
Cards	Displays the cards for Alexa
Devices	Information of all connected devices
Notification	Reminders created by the user
Shopping list and To do list	Shopping list and to do list created by the user
Bluetooth	All paired Bluetooth devices
Owner_info	Information of the registered user
Phoenix	All devices compatible with Alexa
Web config	Router Information connected to the device
Activities	User behavior(voice commands)

Fig. 11. Categories of Cloud Data acquired

number, device type, device name and model), notifications, as well as behavior and habits of the user.

Each folder in the Fig. 11 had .json file in them containing crucial information about the either user, the device , the network configuration, external devices and many more significant information.

One of the most intriguing discoveries we made was the vast volume of data with timestamps. JSON data obtained by APIs such as cards, activities, media, alerts, phoenix, and todos had values with UNIX timestamps. This may give evidence that allows the reconstruction of user activity using a time zone provided by the device-preference API. There were additional fascinating data obtained by cards, activities, and todos that included the back half of a URL containing a user's voice recording on the cloud. As a result, if necessary, the voice file may be downloaded using the utterance API.

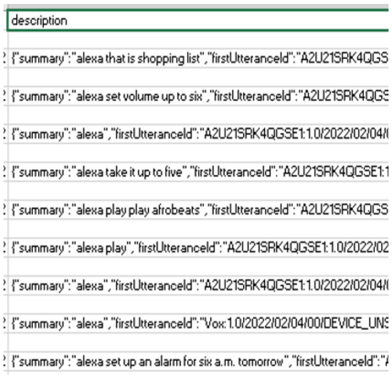
The cloud analysis enabled us to collect user-specific data, device-specific data, and network-specific information. Because the device serial number and user information are saved simultaneously, the device information is especially useful for uniquely assigning a device to the user. The most crucial, however, are the audio recordings maintained in the user's account. These can give information on a certain time period as well as actions taken during that moment. Based on an examination of background noise, it is most likely able to get information about the people present in that environment at the time of the recording. Fig. 12 shows a sample of a .json file from the activities folder, we can see the recordings of the users voice data in plain text.

In Fig, 13, the router information is stored in plain text in the web_config.json file. This leaves the user's network connect vulnerable to attacks as well as exposes the user's personal network information.

B. Summary of Analysis

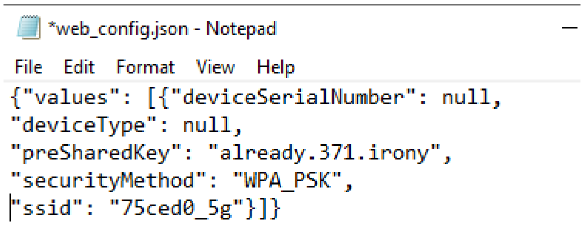
Upon carrying out examinations on the two phases of Alexa, a set of results were drawn and discussed in this research. The Android smartphone did not yield much information about the Alexa app, which might be attributed to the acquisition technique utilized or the fact that the OS on the phone was the most recent version at the time of writing this article. The iOS device, on the other hand, produced more substantial results that investigators may use to link the user to a device; it is also conceivable, however difficult, to obtain the user ID and password for use in the cloud extractor tool. The Alexa cloud extractor tool helped immensely by being an open source tool for retrieving user-related information from the cloud. The main disadvantage is that access to this tool requires a valid userID and password. This may cause a problem for forensic examiners, but the cookies file might also be used to obtain information from the cloud.

From the experiments carried out, we identified that the Amazon Echo captures a lot of data as an interactive gadget that is compatible with other Alexa-enabled devices and third-party services and comes with an app. The data type varies and includes the following: skills that a user has enabled, voice recordings of inquiries or requests made directly by the user in relation to the Echo dot, Alexa app requests and modifications, amazon Alexa's responses,Amazon subscription information, such as payment methods and delivery and billing addresses, information obtained from third-party services, such as account that is associated



```
description
{"summary":"alexa that is shopping list","firstUtteranceId":"A2U21SRK4QGS
{"summary":"alexa set volume up to six","firstUtteranceId":"A2U21SRK4QGS
{"summary":"alexa","firstUtteranceId":"A2U21SRK4QGSE1:1.0/2022/02/04/
{"summary":"alexa take it up to five","firstUtteranceId":"A2U21SRK4QGSE1:1
{"summary":"alexa play play afrobeats","firstUtteranceId":"A2U21SRK4QGS
{"summary":"alexa play","firstUtteranceId":"A2U21SRK4QGSE1:1.0/2022/02
{"summary":"alexa","firstUtteranceId":"A2U21SRK4QGSE1:1.0/2022/02/04/
{"summary":"alexa","firstUtteranceId":"Vox:1.0/2022/02/04/00/DEVICE_UNS
{"summary":"alexa set up an alarm for six a.m. tomorrow","firstUtteranceId":"
```

Fig. 12. Sample of stored audio commands retrieved from the cloud



```
{"values": [{"deviceSerialNumber": null,
"deviceType": null,
"preSharedKey": "already.371.irony",
"securityMethod": "WPA_PSK",
"ssid": "75ced0_5g"}]}
```

Fig. 13. Router name and password in plain text

VI. Discussion

This research was carried out by comparing the methodologies and processes employed to established relevant literature about IOT forensic investigation.

The findings of this investigation appear to indicate that the Amazon Echo does indeed contain data of evidential significance.The data acquired by the gadget, which ranges from timestamps to recordings, has the potential to help law enforcement expand their investigation.

The need for answers to these questions sparked the launch of an examination.

- What forensic artifacts may be retrieved from the Amazon Echo's applications on smartphones (Android and iOS)?
- What forensic cloud artifacts may be retrieved from the Amazon Echo device?
- Can the results of this study provide insights into an effective open source tool that digital forensic investigators can use to analyze cloud services such as Amazon's cloud service (AWS)?
- Where is evidence saved in the Alexa file system?

This study conducted a forensic examination on the Alexa ecosystem, concentrating on the software and cloud layers of the smart speaker system, resulting in the retrieval of a massive quantity of data for analysis. From this data, tangible forensics evidence were identified both from the mobile devices and cloud artifacts, appropriate tools for the acquisition and analysis of data for repeatability were discussed, and the location of file in the Alexa fie system was identified.

Data from the experiments were acquired and preserved in a forensically sound manner, the methods and procedure used for analysis were also clearly documented. After the analysis phase was carried out, results were drawn up to show significant information.

It is possible to retrieve tangible information from the unofficial amazon API at https://alexa.amazon.com as it contains unparsed data from the Echo's to-do and shopping lists. Parsing the same database during examination of the Amazon Echo companion app and it was discovered that the same information is still available with the current version of the app and Echo. As stated in the result earlier, JSON files were retrieved and found to contain plain text files of the connected devices, remainders set by the user, shopping list and to do list, user id as well as router information.

VII. Conclusion

Smart speakers are already being utilized in many homes, which has led to the question of whether they might be of benefit in the event that they are discovered at a crime scene. It is vital to understand how to analyze this device in such a scenario in order to determine the significance of the information it may provide to digital forensic examiners.

This paper focused on the carrying out a forensic investigation of Amazon Alexa Echo Dot 4$^{\text{th}}$ generation on the software and the cloud level. The purpose of this study was to create a replicable methodology that allows for the identification of forensic artifacts that could be obtained from the application on an iPhone and an Android smartphone, as well as to identify an open source tool that forensic examiners may use to collect evidence from this device's cloud level. This research successfully found an open source tool and explained in detail the location of sensitive data on Alexa's file system on the software level and the cloud level.

The voice recordings will be analyzed in the future to discover if the Alexa device has recordings without the wake word "Alexa" and categorise the kind of information the device records without the wake word. Another future work is to carry out hardware-level analysis on the device itself.

References

[1] M.-A. Youn, Y. Lim, K. Seo, H. Chung, and S. Lee, "Forensic analysis for ai speaker with display echo show 2nd generation as a case study," *Forensic Science International: Digital Investigation*, vol. 38, p. 301130, 2021.

[2] İ. Yıldırım, E. Bostancı, and M. S. Güzel, "Forensic analysis with anti-forensic case studies on amazon alexa and google assistant build-in smart home speakers," in *2019 4th International Conference on Computer Science and Engineering (UBMK)*. IEEE, 2019, pp. 1–3.

[3] I. Yildirim and M. ErkanBostanci, "Forensic analysis of amazon alexa and google assistant built-in smart speakers."

[4] C. Krueger and S. McKeown, "Using amazon alexa apis as a source of digital evidence," in *2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*. IEEE, 2020, pp. 1–8.

[5] D. Pawlaszczyk, J. Friese, and C. Hummert, "Alexa, tell me-a forensic examination of the amazon echo dot 3 rd generation," *International Journal of Computer Sciences and Engineering*, vol. 7, no. 11, pp. 20–29, 2019.

[6] M. Day, G. Turner, and N. Drozdiak, "Amazon workers are listening to what you tell alexa. bloomberg," 2019.

[7] T. Lacoma, "The history of all the amazon echo devices," Oct 2021. [Online]. Available: https://www.digitaltrends.com/home/history-of-amazon-echo/

[8] D. A. Orr and L. Sanchez, "Alexa, did you get that? determining the evidentiary value of data stored by the amazon® echo." *Digit. Investig.*, vol. 24, pp. 72–78, 2018.

[9] S. Zawoad and R. Hasan, "Faiot: Towards building a forensics aware eco system for the internet of things," in *2015 IEEE International Conference on Services Computing*. IEEE, 2015, pp. 279–284.

[10] S. Li, K.-K. R. Choo, Q. Sun, W. J. Buchanan, and J. Cao, "Iot forensics: Amazon echo as a use case," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6487–6497, 2019.

[11] V. R. Kebande and I. Ray, "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)*. IEEE, 2016, pp. 356–362.

[12] H. Chung, J. Park, and S. Lee, "Digital forensic approaches for amazon alexa ecosystem," *Digital investigation*, vol. 22, pp. S15–S25, 2017.

[13] J. Hyde and B. Moran, "Alexa, are you skynet," *SANS Digital Forensics and Incident Response Summit*, 2017.

[14] V. Roussev and S. McCulley, "Forensic analysis of cloud-native artifacts," *Digital Investigation*, vol. 16, pp. S104–S113, 2016.

[15] V. Roussev, A. Barreto, and I. Ahmed, "Api-based forensic acquisition of cloud drives," in *IFIP International Conference on Digital Forensics*. Springer, 2016, pp. 213–235.

[16] S. Tristan, S. Sharma, and R. Gonzalez, "Alexa/google home forensics," in *Digital Forensic Education*. Springer, 2020, pp. 101–121.

[17] S. Engelhardt, "Smart speaker forensics," 2019.

[18] N. N. Loideain and R. Adams, "From alexa to siri and the gdpr: the gendering of virtual personal assistants and the role of data protection impact assessments," *Computer Law & Security Review*, vol. 36, p. 105366, 2020.

[19] J. T. Rajewski, "Internet of things forensics," *A Presentation at Enfuse*, 2016.

[20] M. E. Stucke and A. Ezrachi, "How digital assistants can harm our economy, privacy, and democracy," *Berkeley Technology Law Journal*, vol. 32, no. 3, pp. 1239–1300, 2017.

[21] A. Pfeifle, "Alexa, what should we do about privacy: Protecting privacy for users of voice-activated devices," *Wash. L. Rev.*, vol. 93, p. 421, 2018.

[22] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, “A survey on the internet of things (iot) forensics: challenges, approaches, and open issues,” *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1191–1221, 2020.

[23] A. Ajijola, P. Zavarsky, and R. Ruhl, “A review and comparative evaluation of forensics guidelines of nist sp 800-101 rev. 1: 2014 and iso/iec 27037: 2012,” in *World Congress on Internet Security (WorldCIS-2014)*. IEEE, 2014, pp. 66–73.

[24] R. Hegarty, D. J. Lamb, A. Attwood *et al.*, “Digital evidence challenges in the internet of things.” in *INC*, 2014, pp. 163–172.

[25] R. Ayers, S. Brothers, and W. Jansen, “Guidelines on mobile device forensics (draft),” *NIST Special Publication*, vol. 800, p. 101, 2013.

[26] R. Kaur and A. Kaur, “Digital forensics,” *International Journal of Computer Applications*, vol. 50, no. 5, 2012.

[27] LIFSHallym, “Iot$_{c}ode_{a}lexaclouddataextractor.''[Online].Available: https://github.com/LIFSHallym/$