Forensic Analysis for AI Speaker with Display Echo Show 2nd Generation as a Case Study

Min-A Youn, Yirang Lim, Kangyoun Seo, Hyunji Chung*, Sangjin Lee*

DFRC, Korea University, 02841, Anam-dong, Seongbuk-gu, Seoul, Korea

Abstract

As the Internet of Things (IoT) era arrives, many Internet-connected devices are being released, and their use is increasing. One of these, the AI speaker, is designed to augment user convenience by using voice recognition. The best-known products are the Amazon Echo family, including Echo and Echo Dot and more recently, Echo Show with display. An AI speaker with display provides diverse functions such as surfing the Internet, taking pictures, making voice or video calls, and controlling smart home devices. To do this, Alexa cloud servers store a variety of configuration values and historical logs, and users can manage their own cloud-native data through interfaces (e.g., Web sites or mobile apps). For this reason, AI speakers with smart display are similar to PCs or smartphones, which can be very profitable from a digital forensic perspective. This paper focuses on detailed research on the second generation of Echo Show. The first step was to collect forensic artifacts stored inside the product by teardown, identifying eMMC flash memory chips and performing chip-off on Echo Show. Alexa app-related artifacts used on smartphones and how to automatically acquire data from the Alexa cloud were also investigated. From three sources including Echo Show, a companion client (smartphone), and the Alexa cloud, it was possible to acquire user credentials, traces of photos, records of watching videos, log files, and Internet histories with timestamp. The second step was to identify the possibility of inferring new information by correlating artifacts collected from different sources. Integrative analysis enables investigators to track suspect activity across digital devices. Third, this paper introduces an updated version of Cloud-based IoT Forensic Toolkit (CIFT) to support digital investigation of Echo Show. Based on the technical findings, this study proposes a digital forensic framework for a smart speaker with a display that can play an important role as a digital witness at a crime scene. Until now, there has been no multilevel approach to acquisition and analysis of Echo Show data in the field of digital forensics. Therefore, this study makes a contribution to the digital forensic community.

Keywords: Digital forensics, IoT forensics, Amazon Echo Show forensics, Chip-off, Client-centric artifact, Cloud-native artifact, Integrated analysis, Digital forensic framework.

1. Introduction

The global market of Internet of things (IoT) is expected to grow to 657 billion U.S. dollars in size by the end of 2025 (Research., 2018). Various types of IoT devices, such as home cameras, AI speakers, smart door locks, smart refrigerators, and smart cars, are already used frequently in people's daily lives (Thomas, 2019). In homes, business place, cars, or on the body, IoT devices make life simpler and better. One of the reasons IoT technology can be incorporated into life is because users can interact with digital devices with voice.

However, interacting only with voices approaches a limitation on continuous communication. In order to solve this problem, a speaker equipped with a display (it is called smart display) has recently been released, and the number of users is rapidly increasing (Marketsandmarkets, 2019). Unlike the AI speaker, the smart display, especially Echo Show Family, is equipped with a display and a touch pad, and a camera can be used to take pictures or videos, user can surf the Internet through a web browser, and make video calls. As the interface for interacting with the user is diversified, various types of digital traces remain as the smart display provides a function similar with a smartphone or a PC. Therefore, it can be viewed as a digital forensic analysis target.

Amazon's Echo Show 2nd generation, the highest-selling

*Corresponding author

Email addresses: mina_youn@korea.ac.kr (Min-A Youn), yirang0329@korea.ac.kr (Yirang Lim), crmsnmercury@gmail.com (Kangyoun Seo), localchung@korea.ac.kr (Hyunji Chung*), sangjin@korea.ac.kr (Sangjin Lee*)

smart displays in the United States, is our research target in this paper (Kinsella, 2019). Like the real-world case, during the digital forensic investigation, the Echo family devices was used as witnesses or witnesses to crime cases (David, 2019). To support digital investigation, some researchers have researched digital forensic techniques and procedures for the Echo family. They dealt with the entire ecosystem around Echo Dot and proposed a framework that classifies various layers to collect data in the environment (Chung et al., 2017).

Based on the framework proposed by Chung et al. (2017), this study identifies the ecosystem consisting of display speakers and actually collected data from the smart display itself, the smartphone, and the cloud. In particular, user generated data was collected with a hardware approach (chip off) that was not performed in the previous study. It also collects smartphone apps that work with smart displays and data stored in the cloud. We explain how to estimate user behavior through correlation analysis between data collected from three different sources (Echo Show, smartphone, Alexa cloud). Based on the technical findings, we propose digital forensic framework for investigating display-type AI speakers. This study is significant because techniques and framework can be applied to other IoT devices as well.

The rest of the paper is organized as follows. Section 2 describes background information and related studies on Alexa family devices. Section 3 explains how to acquire digital evidence from multiple resources such as Echo Show device, smartphone, and cloud. Section 4 presents forensically meaningful artifacts related to Echo Show. In addition, we will upload a script for automatically collecting Alexa cloud native artifacts. Section 5 explains integrative analysis of forensic artifacts from multiple sources. Section 6 proposes a generalized digital forensic framework for smart display. Finally, Section 7 concludes this paper.

2. Backgrounds

Section 2 gives some background knowledge of the Amazon Echo Show and previous research related to the Amazon Echo family of devices. 2.4 presents research direction affected by related works.

2.1. Research motivation

We focused on Amazon Echo Show. With Alexa as a voice-activated assistant, the Echo Show is capable of doing various things, such as managing to-do lists, playing music, setting alarms, searching information, even taking pictures, making video calls, and streaming video. From a viewpoint of digital forensics, this is very similar to a laptop or tablet PC. For this reason, the Echo Show was selected as our research target for studying digital forensic approaches inside the IoT world.

2.2. Amazon Echo Show

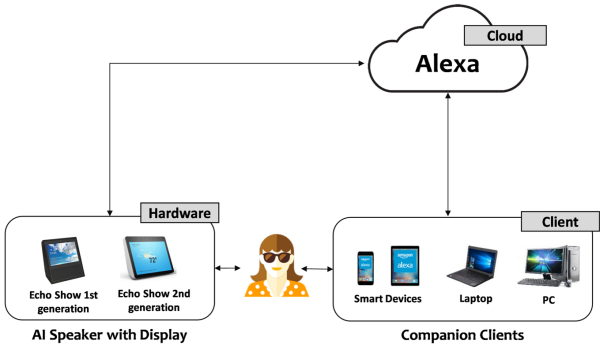

Figure 1: Amazon Echo Show Ecosystem

1) Overall ecosystem: The Echo Show with the Alexa Voice Service consists of a huge ecosystem, as shown in Figure 1. When using the Echo Show, the main components of the ecosystem, such as the Echo Show device, companion clients (smartphone/PC), and the Alexa cloud are connected to each other like an organ system. After setting up the Echo Show, the user can install the Alexa app on a smartphone to check the data generated by the device. All data is stored on the Alexa cloud.

2) Device installation: When starting the Echo Show for the first time, the user can connect to the account directly through the screen. This is different from the voice speaker which requires use of a smartphone.

3) Echo Show features: The Echo Show provides users with basic voice commands and can connect with smartphones and control other IoT devices, as with other Echo products. Device-specific features are web browsing, video calling, photo/video recording, streaming video content, shopping for products with visual search, and using Alexa Skills for Echo Show.

2.3. Amazon Echo family forensics

2.3.1. Hardware-based approach

Table 1 shows previous research about how to physically acquire digital data from the Amazon Echo family.

Table 1. Physical data acquisition for the Amazon Echo family

Type	Target device	Previous research
JTAG	Echo 1st	Clinton et al. (2016)
ISP Pin out	Echo Dot 1st, Echo 1st	Hyde and Moran (2017)
Debug pad	Echo 1st	Barnes (2017)
ADB	Echo Show 1st, Echo Dot 2nd	Vanderpot (2019)
Chip-off	Echo Dot 2nd, Echo Dot 3rd	Pawlaszczyk et al. (2019)

Data were collected from the Echo family of devices using a hardware-based approach. The devices were disassembled and checked for different types of interfaces (e.g., USB ports, debug pads, JTAG ports). If an interface was present, the device was connected to a PC and the data copied using appropriate equipment. If there was no interface, data were collected by physically removing the flash memory chip.

2.3.2. *Companion client-based approach*

Chung et al. (2017) have collected and analyzed the artifacts remaining on the user's device when using the Alexa application on Android and iOS. They have confirmed that they can get information about tokens and to-do and shopping lists. Engelhardt (2019) conducted a study on the second generation of Echo Dot connected with the Amazon Alexa App, which included Alexa-related artifacts such as the date and time the user added to the to-do or shopping list, voice commands as text, and Customer ID. They analyzed the user's behavior in detail (Engelhardt, 2019). Another study explained relevant settings in 'ADB', such as the encryption method for Alexa and whether backup was possible (Olufohunsi, 2020).

2.3.3. *Cloud-based approach*

The Echo family of devices uses the Alexa Voice Service (AVS). All data are stored in the Alexa cloud while the device is running (Rawes, 2019). There are ways to utilize APIs provided by service providers or informal APIs discovered through network analysis to collect data stored in the cloud. First of all, Roussev et al. (2016) suggested in their study, the method of collecting evidence for four cloud services using the official API, and also described the 'kumodd' tool to automate it. The Chung et al. (2017) study suggested a method and tool (CIFT) to automatically collect data stored in Alexa. They applied the method suggested by Roussev et al. (2016) to the Alexa cloud.

2.4. *Main points of our research*

As described above, there have been no studies on smart displays such as the Echo Show. In detail, the three main points of our study are as follows: First, we explored hardware-based approach as well as smartphone and cloud-based approach. Using a chip-off or JTAG techniques, we were able to collect important user-related data such as Amazon credentials (including password), log files and cache files to track user behavior, etc. By integrating and analyzing data stored in three sources, we obtained more precise information about user behaviors and user interests. Based on technical findings, this paper proposed digital forensic framework that reflects the characteristics of smart displays which is a variant of a multi-level forensic approach proposed by Chung (2018).

3. Data Acquisition from Three Sources

This section describes how to collect user data from the main components that make up the Alexa ecosystem. We obtained user data from three sources: hardware, client, and cloud, as shown in Figure 1.

The data stored in Echo Show is acquired from hardware chipsets. We identified 153 Ball BGA flash memory by performing teardown on Echo Show devices (see Figure 2).

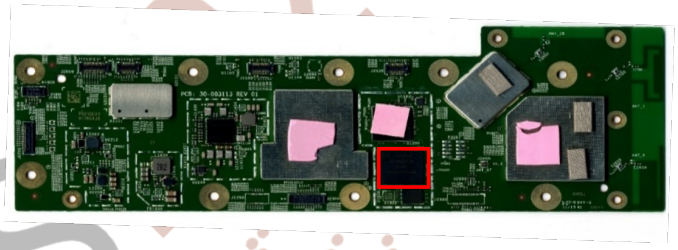

Figure 2: Hardware Platform (Echo Show 2nd generation)

The flash memory used in our target is SANDISK SDINBDG48G 8GB 3.3v. We collected data from the flash memory chip by using a standard socket and a tool named Easy JTAG (see Figure 3). As a result, we found that the structure of the Echo Show 2*nd* generation consisted of 13 partitions and operated on FireOS 5.5.3.1, which is based on Android SDK Level 22 (Lollipop). The relevant partition (specifically, the user data partition) is the '*android_data*' partition, which uses an Ext4 filesystem.

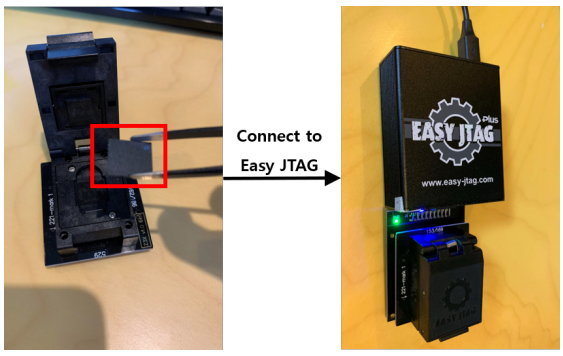

Figure 3: Reading Flash Memory Chip with Easy JTAG

Note that identifying Alexa application is essential to analyze the track of app usage from the smartphone connected to the Echo Show. The Echo Show operates 'Amazon Alexa (package name : com.amazon.dee.app)' in the Android system. We applied two methodologies from prior work, which use rooting

the smartphone (Jo et al., 2019) and the ADB protocol (Scrivens and Lin, 2017).

Finally, because of the importance of collecting all available data from the speaker, we obtained the cloud data using the API provided by Amazon together with the given user account. This data included the remaining information from the speaker (Orr and Sanchez, 2018). Note that the API can be figured out by inspecting network traffic over a proxy (Jo et al., 2019) or checking cache files from the smartphone (Chung et al., 2017).

4. Forensic Artifact Analysis

In this section, we describe forensic artifacts from the three sources explained in Section 3 (Echo Show, smartphone, and cloud). Section 4.1 explains how we evaluated *android_data*, on which the track of user activity is saved. Since *android_data* is formatted as an Ext4 filesystem, we adopted the well-known method of analyzing the filesystem (Fairbanks, 2012). In Sections 4.2 and 4.3, we describe related artifacts from Alexa, the smartphone, and the cloud.

All artifacts we describe are divided into three categories: *Account*, *System*, and *Activity*. *Account* includes information about the user account (i.e., user name or nickname), and *System* contains system log files. We define *Activity* as follows: surfing the Internet, reading e-mails, watching videos on the display, taking pictures or videos with a camera, talking with Echo Show, using the shopping or ToDo lists, and installing Skill apps. The detailed paths and information for all artifacts are described in Appendix A.

4.1. Echo Show 2nd generation artifacts

In this subsection, we illustrate how we collected the artifacts categorized by the three types (*Account*, *System*, *Activity*) from the Echo Show.

Note that it is necessary to distinguish between user accounts and system accounts before analyzing. Echo Show uses the user's nickname located in `accounts.db` and `0.xml` to build up settings. The `accounts.db` file includes two types of account, the one the user has set up and that the system has set up. The user account is identified as `name` in `0.xml`.

Regardless of the user's intention, the Echo Show, like other devices, leaves numerous kinds of logs. Among these logs, the `amazon_main`, `main`, `radio`, and `system` logs included tracks of users. The filename of the log, `Log.(log_type)#number#UNIX timestamps.txt.zip`, indicates the last modification time. In the files, the timestamps are recorded in the format 'mm-dd hh:mm:ss' (UTC +00:00), and contexts contain data from the last few days. A keyword 'WakeWord Detected' gives information about the time the user called the wakeup word, and the track of camera usage is identified as 'camera.StickerShotActivity'. Detailed log file is as shown in Figure 4.

Echo Show also contains forensically meaningful artifacts related to user activities. We identified the Internet browser history, including email account information and the content of emails. The ID of the Alexa account was automatically saved by default when logged in to the Silk Browser (Amazon, 2020). Additionally, we undertook password decoding by using Chrome Login Data Decrypt[1] and, as a result, we acquired an actual email address and password. After watching videos by using voice command or touching the screen of the device, we analyzed the `cache` files using the method described in previous work by Horsman (2018). The video generated from our streaming service targets, YouTube and Dailymotion on the website, was restored by reassembling the `cache`. The pictures Echo Show taken were not found; however, the history of shooting photos and videos was extracted from a database. The database contains the creation timestamp of the media files (UNIX timestamps), and the filename, size, hash value, and path of stored media files. The region was considered to the timestamp format when interpreting the time information because media files are stored using local or UTC time. In the case of pictures, the actual time taken is stored in the filename.

4.2. Smartphone artifacts

We collected artifacts about the user account from numerous files. Initially, the Alexa application was used to connect the Echo Show with the Amazon account. Information related to the account, such as name and e-mail address, is found in `service.identity.xml`. The account and the first time the smartphone was connected are found in `Web Data`. In `QuotaManger`, we found the number of times the user logged in and the last time the user was logged in.

Skills for the Echo Show can be downloaded and used through the Alexa application. This is similar to installing applications from Google Play or the App Store on a smartphone. The list of installed skills is identified by checking the icons in the `cache` and `xml` on the smartphone.

The history of the user's conversations with the Echo Show is located in `RKStorage1` and `DataStore.db`. The first file contains records of the alarm/timer and part of the conversations with the speaker. We can guess the user's behavior from the contexts in which conversations, URLs, and timestamps

[1] `https://github.com/priyankchheda/chrome_password_grabber`

Log Type	Time	Activity	Detail
System	07-29 9:22:16	ECS_ECWakeWordEventProvider	WakeWord Detected.
	07-29 9:30:02	ECS_ECWakeWordEventProvider	WakeWord Detected.
	07-29 9:55:33	ECS_ECWakeWordEventProvider	WakeWord Detected.
	07-30 1:50:51	ECS_ECWakeWordEventProvider	WakeWord Detected.
	07-30 6:11:08	ECS_ECWakeWordEventProvider	WakeWord Detected.
Event	07-30 6:11:11	am_create_activity	[0,646188014,148,com.amazon.zordon/.camera.StickerShotActivity,NULL,NULL,NULL,276856832]
	07-30 6:11:12	am_activity_launch_time	[0,646188014,com.amazon.zordon/.camera.StickerShotActivity,1696,1696]
	07-30 6:11:50	am_destroy_activity	[0,646188014,148,com.amazon.zordon/.camera.StickerShotActivity,finish-imm]
	07-30 6:11:50	am_failed_to_pause	[0,646188014,com.amazon.zordon/.camera.StickerShotActivity,(none)]
	07-30 6:11:50	am_finish_activity	[0,646188014,148,com.amazon.zordon/.camera.StickerShotActivity,app-request]
	07-30 6:11:11	am_focused_activity	[0,com.amazon.zordon/.camera.StickerShotActivity]
	07-30 6:11:50	am_on_paused_called	[0,com.amazon.zordon.camera.StickerShotActivity]
	07-30 6:11:12	am_on_resume_called	[0,com.amazon.zordon.camera.StickerShotActivity]
	07-30 6:11:50	am_pause_activity	[0,646188014,com.amazon.zordon/.camera.StickerShotActivity]
	07-30 6:11:11	am_restart_activity	[0,646188014,148,com.amazon.zordon/.camera.StickerShotActivity]
	07-30 6:11:51	sf_frame_dur	[com.amazon.zordon/com.amazon.zordon.camera.StickerShotActivity,484,570,60,2,2,0,0]

Figure 4: Detailed Log extracted from Echo Show

appear. The conversations are divided into CardID, in *deviceOwnerCustomerId#timestamp#deviceType#SerialNumber* format. There is also evidence that `cache` includes the images from the conversation. The image files provided by Alexa as a reply are left as files with internal signature 'JFIF' among 'cnt' extension files. The second file contains the ToDo and shopping lists, and matches that found in previous work (Chung et al., 2017).

4.3. Alexa cloud artifacts

The acquisition of cloud-native artifacts from the Alexa is very important. Forensic artifacts stored in the Alexa cloud are similar to the findings of previous research (Chung et al., 2017). There have been some changes to existing APIs, and there are additional APIs based on additional features available only in Echo Show, e.g., photo. The results of the updated APIs are shown in Appendix A. We added a module for Echo Show and we will upload with the source of CIFT.

5. Comprehensive Integrated Analysis

Forensic artifacts generated from cloud-based IoT devices are distributed and stored in digital devices and the cloud. In particular, actual data is stored in the cloud server. In this case, the same type of artifacts may be duplicated in several places, but different types of artifacts may be distributed and stored like pieces of a puzzle. In the latter case, new information can be found by collecting and analyzing data from multiple sources. Section 5 describes how to correlate artifacts from the multiple sources described in Section 4.

Table 2. Correlation between multiple sources

Multiple sources	Alexa Cloud	Companion clients
Echo Show	5.1 (UC), 5.2.1 (UB), 5.3.1 (UI)	5.2.2 (UB)
Companion clients	5.3.2 (UI), 5.3.3 (UI)	-

5.1. User credentials (UC)

Echo Show & Alexa cloud: If you log in through the Silk browser on the Echo Show, user account information remains on the device. The investigator can use this information to gain access to the Alexa cloud. A user account is required to access the cloud service and acquire the data.

5.2. User behavior (UB)

5.2.1. Taking photos

Echo Show & Alexa cloud: Photos or videos taken on the Echo Show are stored in the Alexa cloud. Artifacts from the Echo Show device contain only the date and hash values of the photos, so it is difficult to see what photos have been taken. By combining the data from the Echo Show with the data stored in the cloud, the investigator can see what photos have been taken and when they were taken.

5.2.2. Connecting a smartphone with Echo Show

Echo Show & companion clients A User can connect and use multiple Echo family devices with one Alexa account. As the smartphone manages the conversation history by using a CardID, specific echo device can be identified as the CardID. The SerialNumber of the CardID can be stored in a digital artifact obtained from the Echo device. This allows the investigator to identify which Echo device has connected to the user's companion client device.

5.3. User interests (UI)

5.3.1. Searching shopping items

Echo Show & Alexa cloud: Information about products that were searched for while shopping is stored as text in the Alexa cloud. Photos of the product remain on the Echo Show device

in `cache` data. With this information, the investigator can know which products the user wanted to shop for. This is similar to analyzing keywords and details that users searched for through a web browser when investigating a PC or smartphone.

5.3.2. Conversations with Alexa

Companion clients & Alexa cloud: When Alexa answers the user's question, the conversation with Alexa is stored as text in the cloud. In addition, images related to search keywords were retrieved from cache files extracted from the smartphone. By combining the conversation from the cloud with the cache files extracted from the smartphone, the investigator can find photos related to information that the user has searched for. The information that the user searched for can potentially be used to make inferences about content and subjects of interest.

5.3.3. Streaming services

Companion clients & Alexa cloud: When the user watches a video with a streaming web-based service, cached files can be stored inside the Echo Show. By reassembling cached files into a single playable video file, the investigator knows what types of video the user was watching on the Echo Show. Furthermore, it is possible to infer what subjects the user is interested in, as well as their age and gender.

6. Digital Forensic Framework for Smart Display

6.1. Digital forensic framework for smart display

We propose a digital forensic framework for smart displays as shown in Figure 5.

An investigator identifies the suspect's smart displays and companion clients such as a smartphone or PC (local side). In the case of smart displays, the investigator identifies the model and product number. If the device has a USB port, the investigator tries to plug into the USB port and collect its data. If there is no port, disassembling or teardown and chip-off are required for data collection. Once data acquisition is successful, the examiner can find the traces that connect with other devices. If there are artifacts related to other devices that have been linked with the smart display, the investigator can identify the smartphone or PC and collect data using traditional forensic techniques. If there are traces of artifacts related to smart displays, the artifacts from the smart displays and companion clients can be integratively analyzed.

The next step is to obtain user credentials to access the cloud. Credentials can remain on the device when the user signs in with a browser on smart displays like Echo Show. In addition, account information can be obtained from companion clients using memory-based forensic techniques or cookie hijacking. If gathering user credentials is successful, the investigator can access the cloud and try to acquire cloud-native artifacts.

After acquiring forensically meaningful artifacts from smart displays, companion clients, and the cloud through the process of identification, acquisition, and analysis, it is possible to perform an integrative analysis combining artifacts from three different sources. With correlation analysis, the investigator can find the most accurate evidence for tracking user behavior. In some cases, it might not be possible to obtain data from all three sources; for example, if the smart display device was not seized, data were wiped from the smartphone, all data were deleted in the cloud, and so on. In this case, the investigator can analyze each artifact separately.

6.2. Case study

6.2 introduces a hypothetical forensic case related to Echo Show and describes an investigation of the case using the forensic attributes described in the previous.

The party began at 6 pm on March 10, 2020 at John's house. While the party was going on, Lisa, who went upstairs, found her friend Tommy lying dead upstairs. The police to investigate it began investigating John's house. John and Lisa were accused of murder. The investigator looked closely at the Echo Show placed on the shelf upstairs near where Tommy was found, as it may have evidence of the case. Echo Show confirmed that it was a second-generation, sealed the device after shutting down the power, and additionally seized the suspect's smartphone.

First, through smartphone analysis, traces of using Alexa were found from John and Lisa's smartphones. In order to confirm which smartphone the Echo Show has been linked to, it was decided to deeply analyze the Echo Show device. After disassembling the device, chip-off was performed by identifying a flash memory chip. By reading the chip with Easy JTAG, digital data could be collected from the device. Data from the Echo Show began to be generated on February 19th. First of all, it was confirmed that the serial number included in the CardID extracted from John's smartphone and the device number of the Echo Show were the same. This means that the seized Echo Show was used by John in conjunction with a smartphone. In addition, John's Amazon account ID and password could be obtained through a trace that was logged in through the Silk Browser on February 19th. Forensic artifacts related to the Echo Show were visually presented as shown in Figure 6, which helps to analyze efficiently.

As shown in Figure 6, from February 25, John searched for words such as insurance receipts and insurance companies by

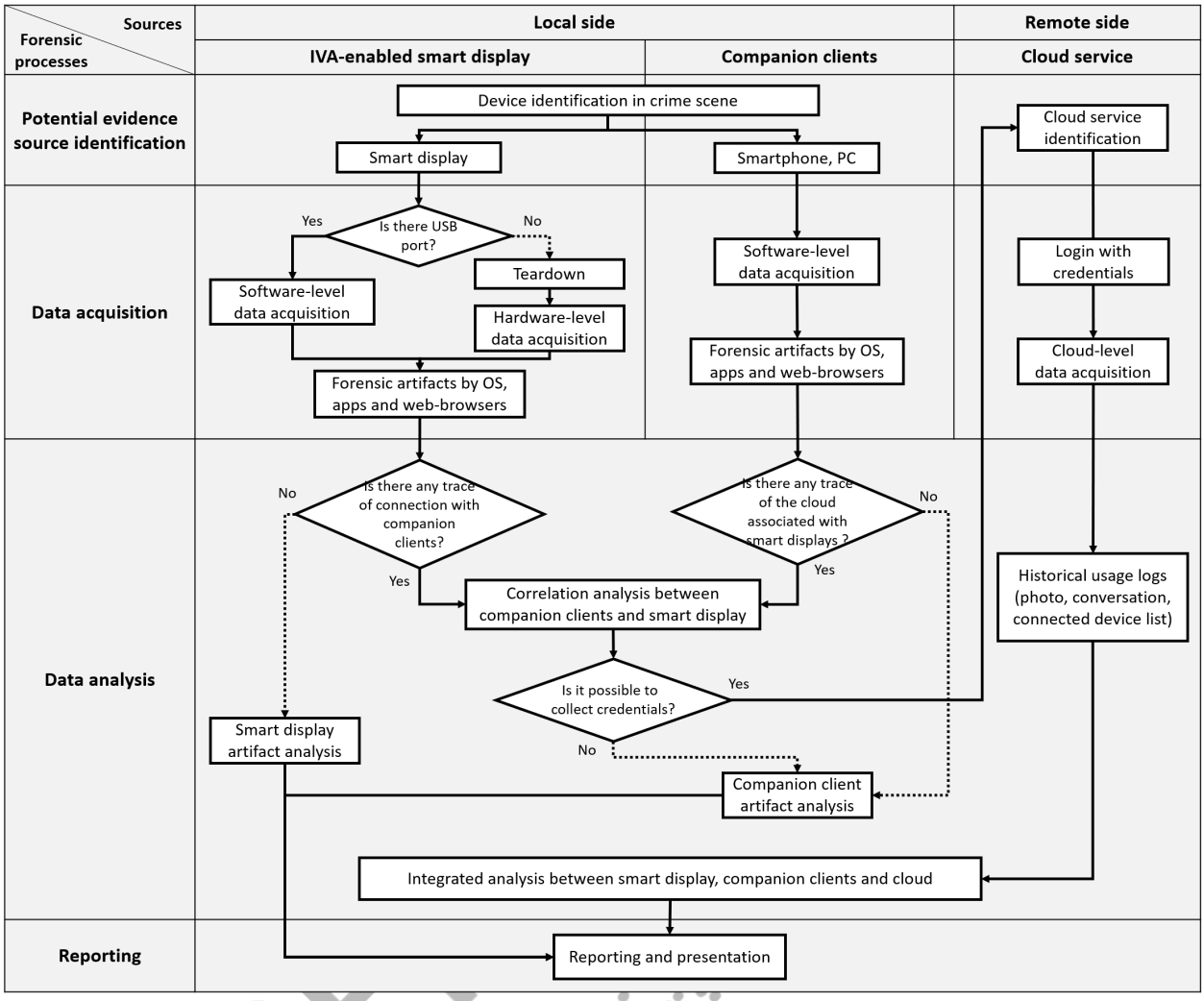

Figure 5: Digital Forensic Framework for Smart Displays

voice command, and confirmed that he searched for antidepressants/drugs through Amazon shopping. With conclusive evidence, it was decided to focus on whether John and Tommy had problems related to insurance or money. The investigation revealed that both of them had a conflict over money, which led to John's deliberate murder of Tommy on the day he invited Tommy and other friends home. Coincidentally, when the investigator checked the photos taken at the Echo Show by accessing the Alexa Cloud, they found that there were several photos in the trash, and that whenever they had a party, Tommy didn't. This scenario showed that the Echo Show could be used to find clues to the incident using all of the connected devices and evidence stored in the cloud. In real cases, these techniques and methodologies could help with investigation.

7. Conclusion

The market for IoT devices is expanding rapidly day by day and becoming more popular. When using IoT devices, people's actions and conversations are can be stored in the cloud server. In this situation, IoT generated data and user generated data play important role in digital evidence. In particular, as smart displays are equipped with touch pads and cameras, voice and video information is accumulating, which is likely to be a report of digital evidence. In this paper, we studied the second generation of Amazon Echo Show focusing on chip-off and JTAG data extraction (hardware-level approach), data acquisition from smart phone (software-level approach), and cloud data collection (cloud-level approach). In addition, the user's behavior was estimated by performing correlation analysis between data collected from multiple sources including Echo Show, smartphone and cloud. Based on the technical

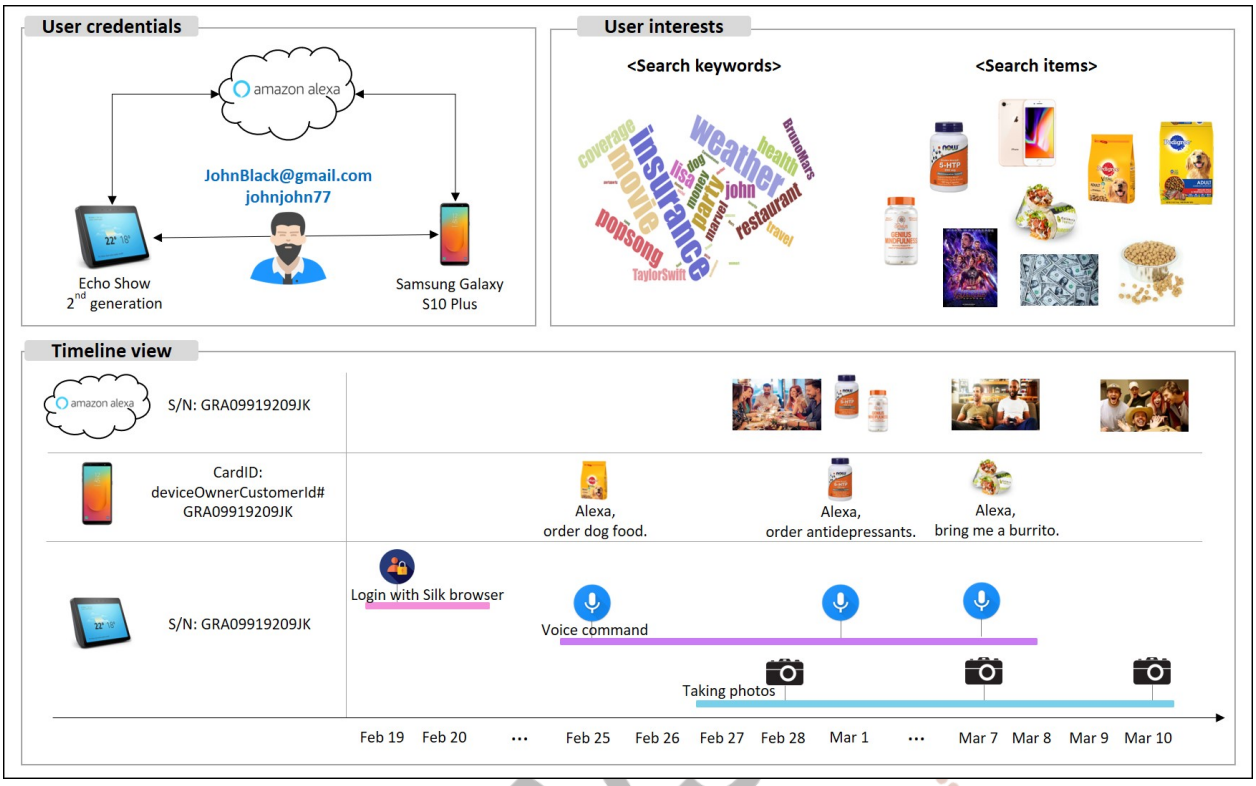

Figure 6: Visual Presentation of Echo Show Artifacts from Three Sources

findings, we proposed digital forensic framework for smart displays, which has a forensic significance in that it can be applied equally to other smart displays.

Acknowledgement

This work was supported by Institute of Information Communications Technology Planning Evaluation(IITP) grant funded by the Korea government(MSIT) (No.2018-0-01000, Development of Digital Forensic Integration Platform)

References

Amazon, 2020. Amazon silk developer guide.

Barnes, M., 2017. Alexa, are you listening. MWR Labs.

Chung, H., 2018. Digital forensic system for intelligent virtual assistant ecosystems. Dissertation, 34,73.

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. The Citadel, The Military College of South Carolina.

David, M., 2019. The role of home devices in police investigations. https://www.policeone.com/police-products/investigation/computer-digital-forensics/articles/the-role-of-home-devices-in-police-investigations-fvgBU0PswYW3Jhvm/.

Engelhardt, S., 2019. Smart speaker forensics.

Fairbanks, K. D., 2012. An analysis of ext4 for digital forensics. Digital investigation 9, S118–S130.

Horsman, G., 2018. Reconstructing streamed video content: A case study on youtube and facebook live stream content in the chrome web browser cache. Digital Investigation 26, S30–S37.

Hyde, J., Moran, B., 2017. Alexa, are you skynet. SANS Digital Forensics and Incident Response Summit.

Jo, W., Shin, Y., Kim, H., Yoo, D., Kim, D., Kang, C., Jin, J., Oh, J., Na, B., Shon, T., 2019. Digital forensic practices and methodologies for ai speaker ecosystems. Digital Investigation 29, S80–S93.

Kinsella, B., 2019. U.s. smart display user base grew 558percent in 2018 and more than doubled in second half of the year, amazon holds two-thirds market share. https://voicebot.ai/2019/03/07/u-s-smart-display-user-base-grew-558-in-2018-and-more-than-doubled-in-second-half-of-the-year-amazon-holds-two-thirds-market-share/.

Marketsandmarkets, 2019. Smart display market by smart home display (voice-controlled, appliance), smart display mirror (automotive-rearview side-view, retail, home), smart signage (retail hospitality, sports entertainment), components, and geography - global forecast to 20. https://www.marketsandmarkets.com/Market-Reports/global-smart-display-market-50180485.html.

Olufohunsi, T., 01 2020. Alexa forensics.

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.

Pawlaszczyk, D., Friese, J., Hummert, C., 2019. "alexa, tell me…"-a forensic examination of the amazon echo dot 3 rd generation.

Rawes, E., . K. W., 2019. What exactly is alexa? where does she come from? how does she work? https://www.digitaltrends.com/home/what-is-amazons-alexa-and-what-can-it-do/.

Research., Z. M., 2018. Iot devices market by device type (processor, sensor, connectivity ic and others) for building and home automation, energy and utilities, manufacturing, connected logistics, bfsi, transportation, connected health and others): Global industry analysis, siz.

Roussev, V., Barreto, A., Ahmed, I., 2016. Forensic acquisition of cloud drives. arXiv preprint arXiv:1603.06542.

Scrivens, N., Lin, X., 2017. Android digital forensics: data, extraction and analysis. In: Proceedings of the ACM Turing 50th Celebration Conference-China. pp. 1–10.

Thomas, M., 2019. These 24 internet of things examples and applications show the power of iot in everyday life. https://builtin.com/internet-things/iot-examples.

Vanderpot, A., 2019. Echo dot v2. https://github.com/echohacking/wiki/wiki/Echo-Dot-v2: https://github.com/echohacking/wiki.wiki.git.

Appendix A. Forensically Meaningful Artifacts

Category	Sub Category		Source: Echo Show (1)	Source: Client (2)	Source: Cloud (3)	Format		Path	Details	
Account	Account ID		O	O	O*	1	SQLite	../data/com.amazon.zordon/databases/{AccountID}.mixtape.db	Account ID	Common ID created by Amazon
						2	xml	[data]/data/../shared_prefs		
							SQLite	../databases/DataStore.db(base64 encoded)		
	Nickname		O	O	O*		SQLite	../system/users/0/accounts.db	name	Nickname
						1	Xml	../system/users/0/0.xml	Name	Nickname
									lastLoggedIn	Last logged in time (UNIX timestamps)
									type	Account type
						2	Xml	[data]/data/../shared_prefs/*	Name	User nickname
									lastName	User's lastname
									firstName	User's firstname
									phoneNumber	User's phone number
									Email	Email address
	Contacts		X	X	O	3	Json	https://alexa-mobile-service-na-preview.amazon.com/users/ amzn1.comms.id.person.amzn1~{accountID}/contacts	"name":{ "firstName":"username", "lastName":"username" }, "numbers":{ "number":"user number", (User's cell phone number) "type":"Type of number" (e.g., Mobile) }	
System	WiFi		O	X	O*	1	txt	../misc/wifi/wpa_supplicant.conf	Ssid	Wifi name
									Psk	Password (plain text)
									Last_connect_time	Last connected time (UNIX timestamps)
	System Log		O	X	X	1	Log	../system/dropbox	Type	System, Events, etc,.
									Date	Logging time (UTC+00:00)
									Activity	Activity name
									Detail Activity	Detailed activity
Activity	Skill		X	O	X	2	Cache	../cache/image_cache/v2_olsl100.1	Skill Icons	
							ZIP	../cache/image_cache/HereMapCache/###/resource.db		
	Brow-ser	History	O	X	X	1	SQLite	../data/com.amazon.cloud9/app_amazon_webview/amazon_webview	Name	Account for E-mail
		Video					Cache	../data/com.amazon.alexa.webmediaplayer.fireos/cache/ org.chromium.android_webview	Watched video	
								../data/com.amazon.alexa.youtube.app/cache/org.chromium.android_webview		
								../data/com.amazon.cloud9/cache/Cache		
								../data/com.amazon.knightwebview/cache/org.chromium.android_webview		
								../data/org.mozilla.connect.firefox/ cache/org.chromium.android_webview		

Category	Sub Category		Source: Echo Show (1)	Source: Client (2)	Source: Cloud (3)	Format		Path	Details	
Activity	Camera		O	X	O	1	SQLite	../data/com.amazon.zordon.databases/amzn1.account.{accountID}.mixtape.db	Node Id	Unique ID for each picture
									Created_date / Modified_date/ Content_sort_date	The time of the photograph taken (UNIX timestamps)
									Content_date / Image_date_time/ Video_date_time	The time of the photograph taken (UNIX timestamps with local time)
									Name(Image/Video)	Photo_booth_single_shot YYYY-MM-DD_hh-mm-ss-mi.jpg/ Photo_booth_video{timestamp}.mp4
									Content_md5	Md5 for media file
							Cache	../data/com.amazon.glorialist/cache/Picasso-cache	The part of photograph	
						3	jpg	https://www.amazon.com/photos/all	Actual Pictures/Videos	
								https://www.amazon.com/photos/all/gallery/{node_id}		
	Conver-sation	Etc	X	O	O	2	SQLite	../databases/RKStorage1	Time	Conversation time (UNIX timestamps)
									Text	The context recognized by Alexa
									Url	Voice file URLs
							Cache	../cache/image_cache/v2_olsl100.1	The part of pictures showed by Echo Show	
		Text Message				3	Json	https://alexa-mobile-service-na-preview.amazon.com/users/ amzn1.comms.id.person.amzn1~{accountID}/conversations	”conversationId”:”Id for conversation”, ”participants”:[”amzn1.comms.id.person.amzn1~{accountID}”, “payload”:{ ”text”:”{Text Message}.”, ”templateId”:”sysmsg_welcome_cobo”	
		Voice Message						https://alexa-mobile-service-na-preview.amazon.com/users/ amzn1.comms.id.person.amzn1~{accountID}/conversations/ {conversationID}/messages?count=100&sort=asc	”conversationId”: ”Id for conversation”, ”clientMessageId”: ”client message”, ”time”: ”2019-11-28T11:29:35.571Z(No Local Time)”, ”sender”: ”amzn1.comms.id.person.amzn1~{accountID}”, ”type”: ”message/audio”, ”payload”: { ”mediaId”: ”An Identification for media”, ”transcript”: ”Hello hello”}	
	Shopping /ToDo		O	O	O	1	Cache	../data/com.amazon.ava.shopping.android/cache/Picasso-cache	The part of shopping images	
						2	SQLite	../databases/DataStore.db	Time	Conversation time (UNIX timestamps)
									value	Lists of shopping/to-do
						3	Json	https://alexa.amazon.com/api/namedLists	”createdDateTime”: 1572244688494, ”customerId”: ” AV1FD2ZFZ7KZN ”, ”itemId”:”{Shoppinglist itemId} ”type”: ”SOPPING_LIST”,}, { ”createdDateTime”: 1572244688494, ”customerId”: ” AV1FD2ZFZ7KZN ”, ”itemId”:”{todolist itemId} ”type”: ”TO_DO”	
								https://alexa.amazon.com/api/namedLists/{Shoppinglist itemId}/ items?startTime=&endTime=&completed=&listIds={Shoppinglist itemId} =&_={time}+1	”createdDateTime”: 1562808512888, ”listId”:{Shoppinglist ietemId}, ”updatedDateTime”:1562808512888, ”value”:”{name}” ex)haircut	
								https://alexa.amazon.com/api/namedLists/{Todolist itemId}/items? startTime=&endTime=&completed=&listIds={Todolist itemId}=&_={time}+2	”createdDateTime”: 1562808512888, ”listId”:{todolist ietemId}, ”updatedDateTime”:1562808512888, ”value”:”{name}” ex)haircut	

* means that we did not mark this artifact because it is the same as the 2017 study Chung et al. (2017).