IoT Forensics: Amazon Echo as a Use Case

Shancang Li, Kim-Kwang Raymond Choo *Senior Member, IEEE,* Qindong Sun, William J. Buchanan, and Jiuxin Cao

Abstract—Internet of Things (IoT) are increasingly common in our society, and can be found in civilian settings as well as sensitive applications such as battlefields and national security. Given the potential of these devices to be targeted by attackers, they are a valuable source in digital forensic investigations. In addition, incriminating evidence may be stored on an IoT device (e.g. Amazon Echo in a home environment and Fitbit worn by the victim or an accused person). In comparison to IoT security and privacy literature, IoT forensics is relatively under-studied. IoT forensics is also challenging in practice, particularly due to the complexity, diversity, and heterogeneity of IoT devices and ecosystems. In this paper, we present an IoT based forensic model that supports the identification, acquisition, analysis, and presentation of potential artifacts of forensic interest from IoT devices and the underpinning infrastructure. Specifically, we use the popular Amazon Echo as a use case to demonstrate how our proposed model can be used to guide forensics analysis of IoT devices.

Index Terms—Digital Forensics, Internet of Things, IoT Forensic Model, IoT Forensics, Amazon Echo Forensics

1 Introduction

In an Internet of Things (IoT) setting, the number of smart devices connected to the Internet can range from a few to billions. Such devices are often able to sense their environment (e.g. temperature, humidity and wind speed), as well as interconnecting and communicating with each other [1], [2], [3]. According to Juniper research [4], more than 20.4 billion smart devices will be connected to IoT by the year 2020, generating approximately £134 billion annually by 2022 for the IoT cyber security industry. This is telling of the IoT trend in our society, which is also evident by IoT being extended to sectors such as battlefields and military (e.g. Internet of Battlefield Things and Internet of Military Things)[1].

In 2017, it was reported that users of Bose headphones were being spied upon without their consent [5]. Specifically, a plaintiff filed a complaint against Bose for their Bose Connect application, which allegedly collected data on the music and audio books their users listened to, and sent the collected information to a third-party data miner (Segment.io). In the same year, Vizio [6], a Smart TV manufacturer, was also allegedly monitoring over 11 million smart TVs, where user data were being sent to other third parties without user consent [6]. Specifically, it was alleged that the manufacturer monitored the pixels displayed on the TV screen and matched these to movies stored on a database. This technique is known as automatic content recognition (ACR). Vizio was subsequently fined a total of USD2.2 Million by the US Federal Trade Commission, and was also ordered not to track their users [6]. In addition, the organization was ordered to delete all their existing data relating to this incident (e.g. near-by access point details, postal codes, and the Internet protocol address (IP Address) of the local network, and implement a privacy policy [7].

In general, an IoT system consists of a (large) number of IoT devices, IoT infrastructures, services and applications, and interface to other applications or services, which can be organized into four layers as shown in Figure 1 [8]:

1) Sensing layer, which includes sensing devices to sense and acquire information, such as smart sensors, radio-frequency identification (RFID), and client components of IoT;
2) Network layer, which is the infrastructure to support connectivity to Internet and other devices;
3) Service layer, which provides and manages services to users or other applications; and
4) Application-interface layer, which provides interface to users or other services.

It can be expected that the increasing popularity and pervasivenesss of IoT devices will make such devices more attractive to attackers, seeking to compromise our systems or exfiltrate our data, and gain a competitive advantage. In other words, any IoT device such as a 3D printer, a smart switch or a smart bulb in a smart home environment can potentially be compromised to gain access to the smart devices or the user's personal data [1], [3], [9], [10]. In 2016, for example, distributed denial of service (DDoS) attacks targeting the Domain Name System (DNS) provider, Dyn, was carried out by a botnet comprising a large number of 2.5 million compromised IoT devices (e.g. IP camera, smart printers, and home WiFi gateway) [2], [11]. In the past two years, a large number of vulnerability scans targeting IoT devices have also been reported. For example in a recent study [12], the authors examined more than 1 TB of passive measurement data collected from a /8 network telescope (of IoT devices), in correlation with 400 GB of

- *S. Li is with the Department of Computer Science and Creative Technologies, University of the West of England, Bristol BS16 1QY, UK. E-mail: shancang.li@uwe.ac.uk*
- *K.-K. R. Choo is with the Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX 78249, USA E-mail: raymond.choo@fulbrightmail.org*
- *Qindong Sun and Li are with the Department of Computer Science at Xi'an University of Technology, Xi'an 710048, China E-mail: sqd@xaut.edu.cn*
- *William J. Buchanan is with the School of Computing, Edinburgh Napier University, Edinburgh EH10 5DT, UK E-mail: w.buchanan@napier.ac.uk.*
- *Jiuxin Cao is with the School of Computer Science and Engineering, Southeast University, Nanjing, China E-mail: jx.cao@seu.edu.cn.*

[1] https://www.arl.army.mil/www/default.cfm?page=3050 (last accessed February 12th, 2019)

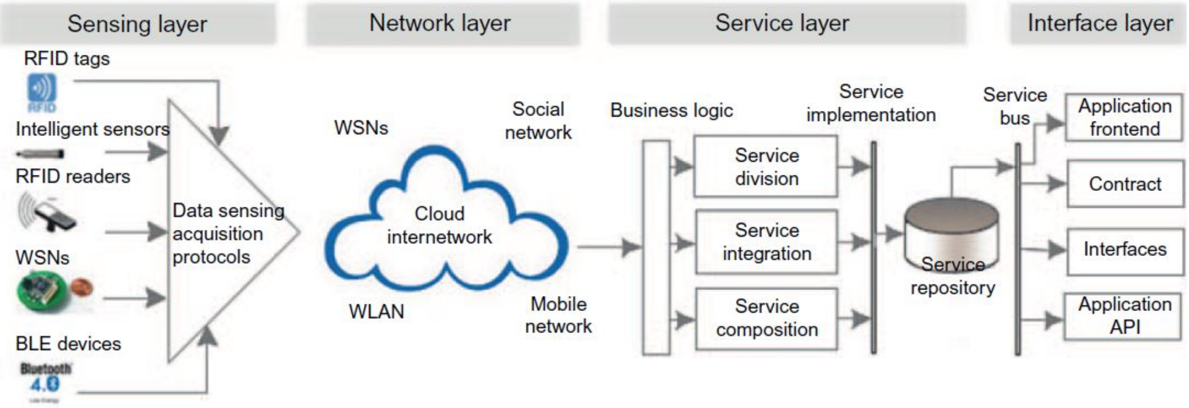


Fig. 1. General IoT Architecture

information from the Shodan service. Based on their findings, the authors were able to classify the "inferred IoT devices based on their hosting sector type (financial, education, manufacturing, etc.) and most abused IoT manufacturers" [13]. They also identified more than 120,000 Internet-scale exploited IoT devices, including in critical infrastructure sectors, as well as inferring "140 large-scale IoT-centric probing campaigns; a sample of which includes a worldwide distributed campaign where close to 40% of its population includes video surveillance cameras from Dahua, and another very large inferred coordinated campaign consisting of more than 50,000 IoT devices". These findings echoed findings such as those of [14], in the sense that a large number of today's IoT devices are insecure. This is not surprising due to the challenges in designing efficient security and privacy solutions. In other words, security and privacy solutions designed for IoT devices will have to take into consideration the interoperability and complex ecosystems, as well as the computational limitations in IoT devices.

Hence, IoT devices are likely to be sources of evidence in a cyber security investigation (e.g. investigation of a DDoS attack) [15]. Unlike conventional digital forensics (e.g. mobile device forensics), the diversity in IoT devices (e.g. 3D printers, roadside units in a smart transportation system, smart healthcare devices in a hospital, and smart military uniforms) and the different evidence and privacy regulations compound the challenges of such investigations [16]. Some of these challenges are as follows:

- *Identification*: identification of potential evidence in IoT environment can be challenging, particularly if the investigators are not familiar with the types of IoT devices present as well as the underpinning infrastructure;
- *Preservation*: once the potential source of evidence is identified, then the question is how can we acquire and preserve the evidence from the IoT devices, companion application, IoT services, networks in the IoT infrastructure, and so on, in a forensically sound manner; and
- *Analysis*: depending on the format that the evidence is acquired, analysis of the acquired evidence may be challenging. We also have to ensure that the analysis takes into consideration data provenance and the interaction between IoT and cloud servers that facilitate the aggregation and processing of data from the IoT.

The following major contributions are presented in this paper:

1) We propose an IoT based forensic analysis model, which supports the identification, acquisition, analysis, and presentation of potential artifacts of forensic interest from IoT devices and the underpinning infrastructure;
2) We address IoT devices forensic investigation processes from the forensic perspective, in which each IoT devices are expected to provide important forensic artifacts;
3) We analyse forensic artifacts retrieved from the popular Amazon Echo as a use case to demonstrate how our proposed model can be used to guide forensics analysis of IoT devices.

In this paper we present an IoT forensic model (see Section 3) and demonstrate how it can be used to guide the investigation of IoT devices, using Amazon Echo as a case study in Section 4. In the next section, we will briefly discuss related literature.

2 Related Literature

In recent years, IoT forensic has attracted attention from the forensic community [17], [18], [19], [20], for example in wearable devices [21], smart vehicles [22], smart home devices [23], and so on. Approaches may vary between the nature and type of digital forensic investigation. For example, at the IoT network layer, network forensics tools or methods are generally applied. We refer interested readers to the work of *Caviglion et al.* [24], who reviewed popular digital techniques in network forensics, reverse engineering, and so on, as well as the prevalent data storage formats and files systems. Key challenges were also briefly discussed. In another related work [18], the authors categorized IoT forensics into three zones: IoT zone, network zone, and cloud zone, where each zone consists of different areas and forensics analysis activities.

In [25], the authors presented an automated forensic management system (FEMS) that was designed to collect data from a three-layered architecture, namely: perception, network, and application layers. However, in dynamic IoT networks, it is difficult for FEMS to investigate all states of the IoT devices. *Zawoad et al.* proposed a forensic-aware IoT (FAIoT) model, which allows the collected evidence to be stored in a secure evidence repository server [14]. In [19], Orlando *et al.* described the methods to investigate the device's hardware and the relevant system (e.g. operating system, boot loader, remote installation and communication system). In addition, a detailed security measurement for IoT devices was provided. In [26], a general IoT forensics framework was proposed, comprising a forensic state acquisition (FSAIoT), and a centralized forensic state Acquisition (FSAC) to classify the evidence acquisition of IoT devices into three modes (i.e. controller to IoT devices, controller to cloud, and controller to controller) [27].

There have also been research efforts in smart home devices and the forensic of such devices. For example, Amazon Echo is increasingly used as the voice controller hub of smart sensors and devices, which plays a centric role in bridging different smart home devices and the amazon cloud server. The Amazon Echo is activated by wake words like ‘Alexa’, but must also constantly listen for the wake-up command, and clearly this is a potential evidence source [20], [23], [28]. For example, Chung *et al.* [29] explained how companion clients (i.e. devices used to send and capture commands and responses from intelligent home assistants, such as Alexa) can also be a source of evidence.

A number of device fingerprinting techniques have also been developed, which can be used for the investigation of IoT devices. For example, sensor pattern noise (SPN) can be used to identify the source device that has acquired a digital image or video, and this is relevant for the investigation of IoT devices that have a image or video acquisition capability (e.g. unmanned aerial vehicles). In SPN based image forensic analysis, as the most dominant part of SPN the photo response non-uniformity (PRNU) noise can be extracted from an image to build image fingerprint and camera fingerprint, which has been widely used in image origin identification and image forgery detection. Flicker forensics can also allow an investigator to identify an IoT device by analyzing the flicker signal and associate the parameters with some internal characteristics of the particular device [30].

In the next section, we will address our IoT forensic model.

3 Proposed IoT Forensic Model

When we conduct an IoT forensic investigation, we have to consider the sources of evidence other than the actual IoT devices, for example, the sensing, network, service and interface layers (see Figure 1).

Similar to conventional digital forensics, IoT forensics mainly consists of the following four stages: *identification, preservation, analysis, and presentation* [31].

1) In the identification stage, the focus should be on IoT devices (e.g. sensors and intelligent home assistants such as Amazon Echo), and any related infrastructure (e.g. routers).
2) In the preservation stage, we may require specialized / customized tools to acquire data from (proprietary) hardware and applications.
3) In the analysis stage, customized forensic tools may be required to analyze data from certain devices, other than the typical commercial forensic tools (e.g. EnCase and FTK). Both EnCase and FTK are commonly used forensics tools that can be used in digital security, security investigation, and e-discovery.
4) In the presentation stage, forensic investigators will need to detail the findings and be able to articulate the analysis, findings and their implications in a court of law. Meanwhile, the evidence items should be presented with their original format.

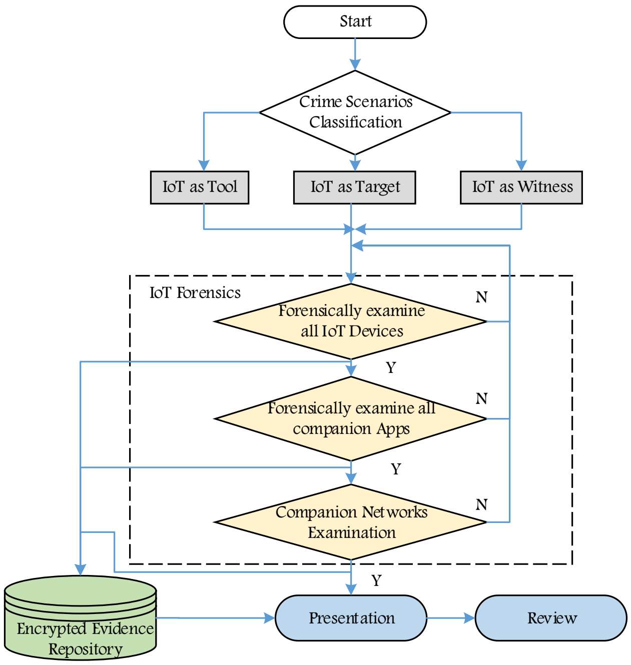

Start
Crime Scenarios Classification
IoT as Tool
IoT as Target
IoT as Witness
IoT Forensics
Forensically examine all IoT Devices
N
Y
Forensically examine all companion Apps
N
Y
Companion Networks Examination
N
Y
Encrypted Evidence Repository
Presentation
Review

Fig. 2. Proposed IoT Forensic Model

Building on the typical four-stage digital forensic process, we present an IoT forensic model – see Figure 2. Specifically, our model starts from an *offense classification* stage, where the roles of IoT are classified into *IoT as a target, IoT as a tool*, and *IoT as a witness*. Then, each related device and the companion apps are examined using the above four-stage process. In addition, all acquired forensic artifacts are stored in an encrypted evidence repository.

3.1 Offense Classification

Due to the diversity of devices and heterogeneity of networks in an IoT setting, it can be challenging to identify all sources of evidence and collect all relevant forensic artifacts in a timely fashion, especially if third parties or remote servers (e.g., websites and cloud servers) are involved. Firstly, to effectively identify the devices for an investigation, it is important to consider the nature of the offense (e.g. a serious and organized crime type will generally mean that more resources should be spent on the case), data acquisition methods, and relevant laws (e.g. what are the elements of proof) and regulations. In general, the IoT-related crimes can be group into three classes [32]:

(1) IoT device as a target (e.g. cyberattacks where vulnerabilities in IoT devices are exploited). IoT devices, particularly inexpensive devices, are likely to be resource limited in terms of computation capabilities, storage space, and power supply. Thus, it is challenging, or impractical, to install security solutions / packages on such devices, which make them an easy target for cyber attacks.

(2) IoT device as a tool, IoT devices can be used by forensic investigators as tools to identify, collect, analyse, or even present evidences in digital investigation. For example, a compromised IoT device is been used to facilitate other malicious activities such as a botnet attack.

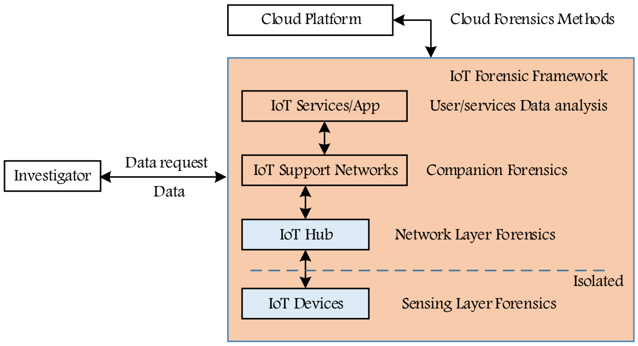


Fig. 3. IoT device identification procedure

(3) IoT device as a witness (e.g. data stored in the IoT device can directly implicate an individual accused of a crime), in which IoT devices are able to identify, collect, and preserve evidential data for forensic investigation. One prominent example involved the Amazon Echo, where an Arkansas man was accused of killing his friend. The prosecutor then sought recordings from the defendant's Amazon Echo to be used as evidence [33]. IoT as a witness will likely happen again in the future frequently because IoT devices are now an integral part of our daily life.

Figure 3 shows the workflow of IoT device identification, in which an IoT device will be examined using the appropriate approach.

3.2 IoT Device Identification

In this stage, we seek to answer the following questions:

- What was/were available at the event/crime scene or a remote site?
- Who and what was/were there when the event/crime occurred?
- What are the constraints in collecting the required evidence?
- What is the minimum set of evidence required to support the elements of proof for this specific offense?

A six-step IoT device identification method is presented in Figure 4.

- Define device space, to identify the devices relating to the specific case;
- Establish the device lifecycle, to identify the time span for the device examination;
- Establish access, to identify the accessibility of the devices, including *confidentiality, authentication, authorization*, and so on;
- Define data categories, to define the data category that the device can provide;
- Network access control, to identify the connectivity of the networks relating to the device and isolate the device from the connections;
- Identify the access to devices, this stage summarizes previous steps and establish the availability of the device for investigators.

Despite the diversity of IoT device manufacturers, IoT devices share some similar features and capability. In general, an

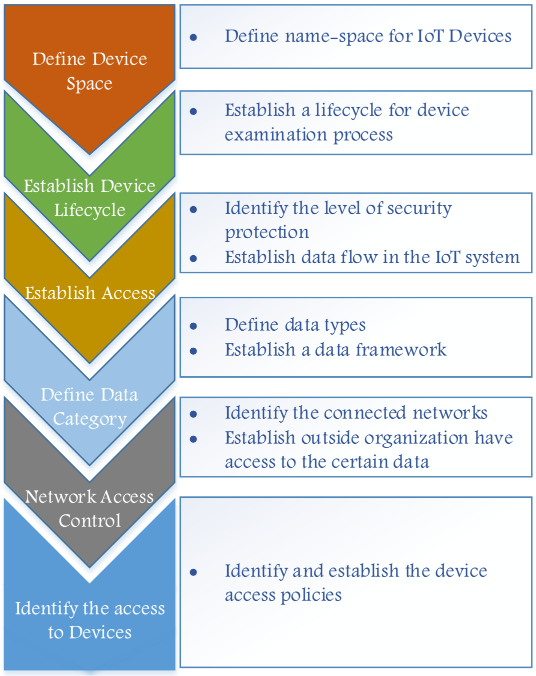

Define Device Space
Define name-space for IoT Devices
Establish Device Lifecycle
Establish a lifecycle for device examination process
Establish Access
Identify the level of security protection
Establish data flow in the IoT system
Define Data Category
Define data types
Establish a data framework
Network Access Control
Identify the connected networks
Establish outside organization have access to the certain data
Identify the access to Devices
Identify and establish the device access policies

Fig. 4. IoT device identification

IoT device consists of a processer or micro-controller, read-only memory (ROM), random access memory (RAM), communication module (Bluetooth, Wireless, Zigbee, *etc.*), and data input/output interfaces. To record the collected or generated data, an IoT device may be equipped with built-in secure digital (SD) memory to support removable memory. Software features of an IoT device include operating systems (some simple IoT devices may only run very simple code without an operating system), middleware, file system, and applications. Many IoT devices do not have a specific file system and in this case, the investigator may need undertake further research, for example how to leverage the application software development kit (SDK) to obtain more information.

Conventional digital forensic tools, such as DD, EnCase, FTK Imager, and SIFT, may also be useful in some cases. In IoT forensics, the data extraction tools/methods can be classified into five levels, namely: manual, logical, hex dumping/JTAG, chip-off, and micro-read [34]. For IoT devices that are not supported by existing forensic tools, the investigator could also consider seeking the cooperation of the device owner, reviewing seized material, seeking the assistance of the service provider (e.g. Amazon in the case of Amazon Echo), and so on.

3.3 Evidence Preservation

Tables 1 and 2 show the potential avenues for data preservation, and in this paper we will focus on memory forensics. Specifically, we will focus on (1) extracting data from the memory of a target IoT device; and (2) analyzing the physical memory data (from RAM), page file (or SWAP space) data, etc. Swap space denotes areas on disk used for interchanging contents between main ram and secondary memory, in linux swap is an actual disk partition and in windows machine, the swap space is a pagefile. In

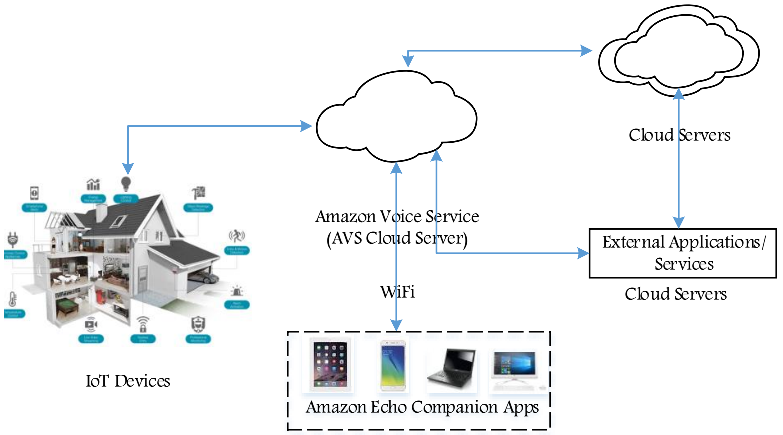


Fig. 5. General IoT Forensic Analysis

TABLE 1
Example of Hardware Characterization for IoT Devices

Hardware Features	Capabilities	Evidence Sources
Processor	48MHz to 2 GHz	Cache
Microcontroller	Less than 52MHz	RAM and FLASH
Memory	5MB to 128GB	Chip Memory and
Card slots	MicroSD, MicroSD	SD-based Card
Display	LCD to HD	–
Camera	Still, Video	DF/SD Card, ex-Memory
Interfaces	SPI, I2C	built-in RAM/SRAM
JTAG	JTAG Scanner	–
Input Interface	RS232 to Keyboards	–
Voice Input	Voice recognition	EEPROM, ex-storage
Positioning	GPS receiver	External storage
Wireless	IrDA, BT, WiFi, NFC	–
Battery	Li-Ion Polymer	–

TABLE 2
Example of Software Characterization for IoT Devices

Software Features	Capabilities	Evidence Sources
OS	Closed	Android, iOS,etc.
Secure coding	Programming language	RAM and FS
Logs	Events logs, data logs	FS, ex-storage
PIM	Calendar, List	FS, storage
Applications	application data	Cache, RAM, FS, ex-S
Data type	Application-based	Cache, RAM, FS, ex-S
Call	Logs	File systems
Data Processing	depends	Cache, RAM, FS, ex-S
Email	Applications	RAM and FS
Protocols	Communication	Cache, RAM, FS, ex-S
Web	Web browser	Cache, RAM, FS, ex-S
Web	Network services	Cache, RAM, FS, ex-S

digital forensics, Swap file is a rich source of key evidence items, including passwords, sensitive data, encryption keys, etc.

Live memory evidence extraction is another major issue in IoT forensic preservation. In resource-constrained IoT devices (e.g. limited computation, storage, energy supply, etc.), volatile memory extraction can often be conducted to extract key evidence stored in the RAM or an ongoing communication session [35]. A number of memory acquisition tools have been developed in the literature, such as the Android based memory subsystem (ashmem) [36], *Android low memory killer* [37], and *memory grab* [38].

However, there are still challenges in live memory acquisition. For example, the *memory protect unit* (MPU) technology only allows specific instructions or code to access the memory. This prevents the forensic investigator from accessing the memory. In addition, anti-forensics (AF) techniques including activities to overwrite data and metadata compound the challenges of memory acquisition. For example, TimeStomp[2] can be used to overwrite NTFS `create, modify, access, and change` timestamps [39].

Also, while a number of tools have been developed for live memory acquisition from computers and laptops (e.g. *Winen, dd, dumpit.exe, winhex, nigilant32, memoryze, readline*), there are limited tools designed for IoT devices.

3.4 IoT Forensic Analysis and Presentation

IoT forensic analysis can be scenario- and device-specific, since IoT systems can have different configurations and settings. For example, in a smart home system as shown in Figure 5, the devices involved may differ from an industry IoT (IIoT) systems. The general approach can include attempts to reconstruct the IoT crime/event scenes. The findings of the analysis also need to be documented and presented, for example to the jury, prosecutors and judges.

4 Amazon Echo (Pi) Forensics

Amazon Echo is a popular intelligent home assistant or ‘smart home’ IoT hub, which takes voice commands from the users to control itself and other connected IoT devices/sensors (*e.g.* smart lights, smart kettles, smart locks, smart thermostats, and smart doors) [40]. Using the voice recognition technology (i.e. Alexa in the case of Amazon Echo), users can interact with the connected IoT devices using their voice. Clearly, the devices require some sort of Internet connection (*e.g.* WiFi) [20].

[2] https://www.offensive-security.com/metasploit-unleashed/timestomp/, last accessed June 20th, 2018

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2019.2906946, IEEE Internet of Things Journal

In a prior work involving the analysis of Amazon Echo [29], it was reported that the user's history data and interactions with Alexa are stored in the SQLite database and web cache files. The authors analyzed two Amazon Echo Dots, with Android 4.4.2 + Alexa app, iOS 10.1.1 + Alexa app, OS X 10.10.5 + Chrome and Windows 10 + Chrome. For the network analysis, it was determined that most of the communications were encrypted and the JSON format was used for passing parameters. The authors' analysis of the communications revealed undocumented API calls to RESTful Web services. In other words, there are seven categories of data on the device, namely: account, customer setting, Alexa-associated devices, skills and behaviours of user, user activity, and *etc*. The researchers found that most of the data contain UNIX timestamps, which could be used to create timeline of activities within an investigation [29]. Within this applications, the utterance API could be used to download voice files [41].

The location of the client artefacts depends on the access method being used, such as for SQLite databases on iOS and Android, and within Chrome caches for OS X and Windows 10. A summary of these locations is presented in Table 3.

On Android device, the SQLite files are contained in $map\_data\_storage.db$ (token information for the current user, and is deleted when the user signs out) and *DataStore.db*. For iOS device, there is a single file named LocalData.sqlite. While the Android analysis was fairly easy, the iTunes backup protocol had to be used in iOS analysis. The chrome access data was found stored in the data-block-files, which could be possible to rebuild Alexa-related caches into the first HTTP headers, and cached data. This could be useful for determining user behaviors as the stored things (*e.g.* user clicks) can lead to calls to Alexa APIs [41], [42].

In IoT forensics, analyzing embedded files and data with firmware images is an effective way. By connecting the `UART` port in Echo, the boot debug messages can be output to a terminal. In our research, we determine that Echo uses `u-boot` as its boot loader, which is a popular open source bootloader and a number of commands/tools can be used to extract information in the firmware. In this paper, we use the `Alexa Pi` to build an `Echo` over Raspberry Pi Version B, which uses similar firmware with Amazon Echo. In our experiment, we analyze the Alexa Pi over Ubuntu (16.04), the companion app installed on an iPad 4 (iOS 12), and the Alexa Voice Server (AVS).

We first use `u-boot` to output the firmware in Alexa Pi, which results in three Encase images (see Figure 6).

4.1 Data Type

We then analyze the data type created, transmitted, processed, and stored on the IoT devices. For an Amazon Echo and the AVS service, we determine that the following (see also Figure 7):

- Device related data include device name, device group, serial number, hardware data, timezone, region, *etc.*
- Connectivity includes connection address, WiFi: Gateway IP, IP, media access control address (MAC address), Server address, Bluetooth address, *etc.*
- User data include data related to the IoT device, such as username/password, language, calenders, and email.
- Application data include Host name, Client version, ProductID, ClientID, ClientSecret, Device Reg name, Bearer token, registered user, *etc.*
- Other data include communication data, specific protocol type, *etc.*

4.2 Alexa Pi Data Acquisition

1) Data acquired from the companion app include device related information, account, and network, as shown in Figure 8. For each IoT device, more detailed data can be extracted using both logical and physical methods, including device name, wifi, device register, serial number, and MAC address. In addition, information such as language and location can also be extracted directly after further analyzing the app.

The bootloader's command line interface allows raw access to part of the memory areas and Flash integrated circuit (IC). When processing the `bootloader` message via the universal asynchronous receiver/transmitter (UART) port, an investigator can obtain the location of the kernel image and scout the firmware by using the u-boot command-line interface (CLI). In further examination of the file system in the firmware, Debian system information can also extracted as shown in Figure 9.

We use *Zenmap* to locate the IP address as: `192.168.0.10` and MAC address `AC:63:BE:78:98:D6` of an Echo via a ping scan. In more complex investigations, we can also use port pings to find all ports open on the devices. By checking the IP address and MAC address, the investigator can identify other IoT devices that need to be examined.

Through the UART, we can dump the firmware to an image file. In this investigation, it is very difficult to solder the UART to the USB ports. Fortunately, in [44], an Echo image is provided that can be loaded via a raspberry pi, which works fine as an Echo device. We investigate the images on the Raspberry Pi, which contains the information that an Echo has.

Some information to identify the device can be found by investigating the firmware. Amazon requires each Amazon Echo device to provide the productID (also known as Device Type ID), ClientID, and ClientSecret in order to use AVS, as shown in Figure 10. The Echo firmware contains several files within the root folder, for example in the automated_install.sh file.

4.3 Examination and Analysis

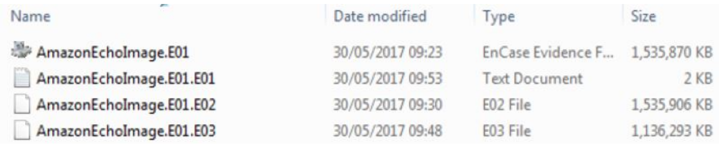
The two devices' information are shown in Figure 12. For each device, information such as device name, wireless connections, device register, serial number, and MAC address are located and analyzed. For example, the `Setting` section stored within the `Alexa` app contains information that can be used to identify the IoT device. In other words, the investigator can extract the device name, the Wi-Fi that the IoT device had previously connected to, Bluetooth connection information, and paired device. The 'device is registered to' information may also be used to identify the owner of the Echo, for example in collaboration with Amazon. Meanwhile both serial number and MAC address can be used to identify the Echo and other connected devices.

Echo uses an address set in the Alexa companion app, where the location information is used to provide weather forecasting and location-based services. Analysis of location information acquired from companion devices (e.g. Google Maps, Find your device, and weather) can also be corroborated with other analysis.

The location data extracted from settings shows the whereabouts of the user. It also provides the geolocation data (e.g. address, postcode) that the user was searching for. However, during the analysis, the investigator also needs to check the history to get more context of the search request.

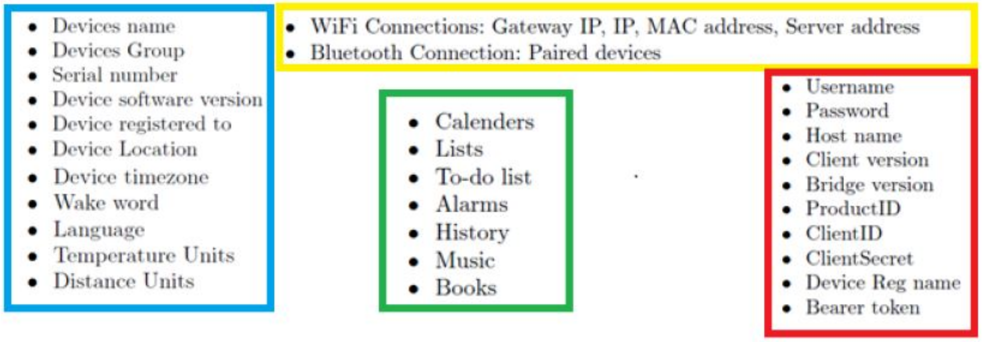
TABLE 3
Location of client artefacts [29]

OS	Application	Path	Format	Description
Android 4.4.2	Alexa 1.24.11760	/data/data/com.amazon.dee.app/databases/map_data_storage.db /data/data/com.amazon.dee.app/databases/DataStore.db /data/data/com.amazon.dee.app/app_webview/Cache/*	SQLite SQLite WebView cache	Tokens of an active user Todo and shopping list Cached native artificats
iOS 10.1.1	Alexa 1.24.11760	[iTunes backup]/com.amazon.echo/Documents/LocalData.sqlite	SQLite	Todo and shopping list
OS X 10.10.5	Chrome 55.0.2883.87	/Library/Cache/Google/Chrome/Default/Cache	Chrome cache	Cached native artifacts
Windows 10	Chrome 55.0.2883.87	%UserProfile%/AppData/Local/Google/Chrome/User Data/Default/Cache/	Chrome cache	Cached native artifacts



Name	Date modified	Type	Size
AmazonEchoImage.E01	30/05/2017 09:23	EnCase Evidence F...	1,535,870 KB
AmazonEchoImage.E01.E01	30/05/2017 09:53	Text Document	2 KB
AmazonEchoImage.E01.E02	30/05/2017 09:30	E02 File	1,535,906 KB
AmazonEchoImage.E01.E03	30/05/2017 09:48	E03 File	1,136,293 KB

Fig. 6. Alexa Pi firmware images created using Encase 7.0



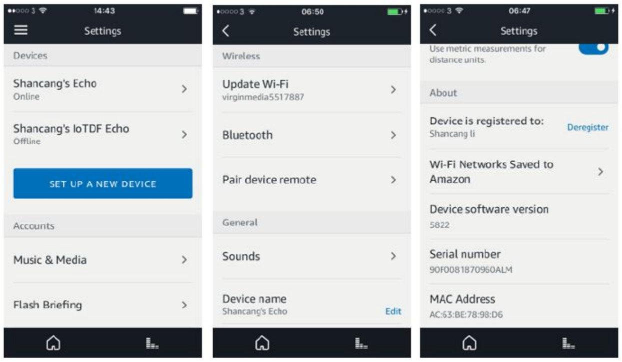
- Devices name
- Devices Group
- Serial number
- Device software version
- Device registered to
- Device Location
- Device timezone
- Wake word
- Language
- Temperature Units
- Distance Units

- WiFi Connections: Gateway IP, IP, MAC address, Server address
- Bluetooth Connection: Paired devices

- Calenders
- Lists
- To-do list
- Alarms
- History
- Music
- Books

- Username
- Password
- Host name
- Client version
- Bridge version
- ProductID
- ClientID
- ClientSecret
- Device Reg name
- Bearer token

Fig. 7. Data type related to Amazon Echo



Devices

Shancang's Echo
Online

Shancang's IoTDF Echo
Offline

Accounts

Music & Media

Flash Briefing

Wireless

Update Wi-Fi
virginmedia5517887

Bluetooth

Pair device remote

General

Sounds

Device name
Shancang's Echo
Edit

Use metric measurements for distance units.

About

Device is registered to:
Shancang li
Deregister

Wi-Fi Networks Saved to Amazon

Device software version
5822

Serial number
90F0081870960ALM

MAC Address
AC:63:BE:78:98:D6

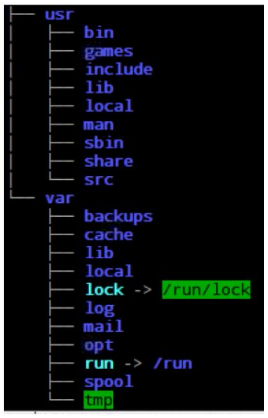
Fig. 8. Data extracted from the companion app (partially)

Amazon Echo is also capable of storing private conversations in the home, or other non-verbal indications that can identify who is present in the home (e.g. based on audible cues). However, in this stage we are only able to identify the recordings streamed by Echo from the user's home activated by the wake words. The text-transferred recordings are stored on both Amazon Alexa Server and Alexa companion app.

The device time zone is key to identifying data with an associated timestamp. In our further examination of the firmware, the device time zone can be used to validate the access/modify/creation time of files like .wavtemp. The wake word and language are also key to analyzing the history. Since the default wake word is Alexa, the investigator can also find the user-defined wake word, if any.

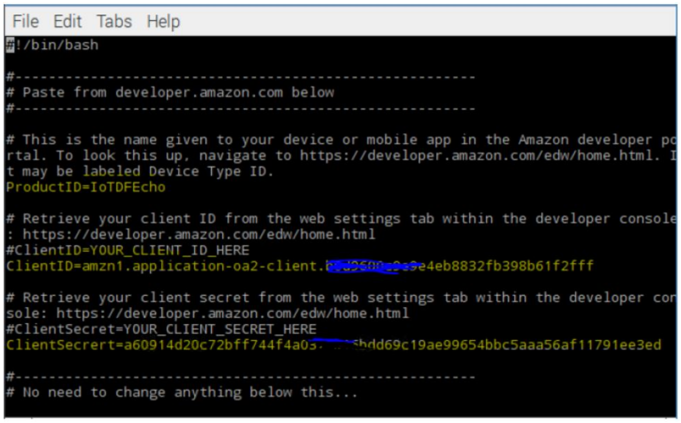
When examining the companion app and the firmware, we also located 5163 audio files (e.g. stop.mp3 and error.mp3), which can indicate the last operating time of the device (see Figure 11).

Figure 11 also shows the keyword search results. In this example, keywords such as amazon, echo and mac were used and 288, 206, and 144 results were found respectively. There are also 1584 potential email addresses located, which may contain the user accounts or potential passwords for logging to the AVS. In fact, we locate the login id with the corresponding password that can be used to login to the AVS, as shown in Figure 12. To further analyze the services that Echo provides, network forensics tools can be used to scan the open ports and potential services. In our examination, we use `Zenmap` with



```
├── usr
│   ├── bin
│   ├── games
│   ├── include
│   ├── lib
│   ├── local
│   ├── man
│   ├── sbin
│   ├── share
│   └── src
└── var
    ├── backups
    ├── cache
    ├── lib
    ├── local
    ├── lock -> /run/lock
    ├── log
    ├── mail
    ├── opt
    ├── run -> /run
    ├── spool
    └── tmp
```

Fig. 9. Alexa Pi firmware file system



```
#!/bin/bash

#---------------------------------------------------------
# Paste from developer.amazon.com below
#---------------------------------------------------------

# This is the name given to your device or mobile app in the Amazon developer po
rtal. To look this up, navigate to https://developer.amazon.com/edw/home.html. I
t may be labeled Device Type ID.
ProductID=IoTDFEcho

# Retrieve your client ID from the web settings tab within the developer console
: https://developer.amazon.com/edw/home.html
#ClientID=YOUR_CLIENT_ID_HERE
ClientID=amzn1.application-oa2-client.[redacted]e4eb8832fb398b61f2fff

# Retrieve your client secret from the web settings tab within the developer con
sole: https://developer.amazon.com/edw/home.html
#ClientSecret=YOUR_CLIENT_SECRET_HERE
ClientSecrert=a60914d20c72bff744f4a03[redacted]dd69c19ae99654bbc5aaa56af11791ee3ed

#---------------------------------------------------------
# No need to change anything below this...
```

Fig. 10. Alexa Pi configuration for AVS

command {`nmap -T4 -A -v 192.168.0.10`} to scan the ports. We note that ports `80, 5200, 515, 427, 10001, 631, and 9100` are open. These open ports can be useful in analyzing the connection behaviors of Echo and can be used to trace the behaviors of the user. Using command {`nmap -sV -T4 -F 192.168.0.10`}, we found the services provided by Echo, including `http, svrloc, printer, ipp, jetdirect, et al.` Two additional services were also found using service fingerprints. One of the findings is shown in Figure 13.

Findings from the analysis of different devices, etc) are then pieced together.

5 Conclusion

IoT forensics will be increasingly important, as more devices around us are connected to the Internet or some form of networks (*e.g.* a private home or office network). In other words, evidence can be collected from IoT devices, internal network, applications, some external (cloud) server, and/or other components of the IoT ecosystem. This complicates the challenge in the timely identification of potential evidential sources and acquisition of evidence. Thus, in this paper, we presented an IoT forensic analysis model and demonstrated how it can be used to guide the investigation of an Amazon Echo.

We also identified a number of potential research opportunities in IoT forensics, such as the following:

1) Timely identification of potential evidential sources and acquisition of evidence (as discussed above).
2) The data type / format and its lifespan may vary between different IoT devices and systems, and the dynamic nature of some IoT devices and systems may necessitate live forensics. Hence, we have to ensure that the tools and processed used in the acquisition of such data are forensically sound.
3) As IoT applications may be delivered as services in the cloud platform, evidence can be distributed across different cloud servers that are probably in a foreign jurisdiction. Hence, there is a need to design appropriate tools that could facilitate (remote) data acquisition, as well as working with policy makers to draft legislation to facilitate such remote data acquisition to ensure evidence admissibility.
4) We also need to design tools or techniques that allow us to address the large storage requirement associated with the search space.
5) We need to keep pace with emerging and new IoT devices and other components in the IoT ecosystem, for example in terms of our forensic capabilities and to overcome anti-forensic measures.
6) The need to design forensically-friendly / ready IoT systems (a concept coined as forensic-by-design in [43], [45], [46], [47], [48], [49]), in order to facilitate the identification and secure storage of data of forensic interest that will be made available for a forensic investigation.

Acknowledgment

The research presented in this paper is supported in part by the National Natural Science Foundation ($No.:61571360$), Shaanxi Science & Technology Co-ordination & Innovation Project ($No.:$ $2016KTZDGY05-09$), and the Innovation Project of Shaanxi Provincial Department of Education ($No.:17JF023$).

References

[1] S. Li and L. Da Xu, "Security in enabling technologies," *Securing the Internet of Things*, pp. 23–109, 2017.

[2] M. Mangia, F. Pareschi, R. Rovatti, and G. Setti, "Low-cost security of iot sensor nodes with rakeness-based compressed sensing: Statistical and known-plaintext attacks," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 2, pp. 327–340, Feb 2018.

[3] J. Pawlick and Q. Zhu, "Strategic trust in cloud-enabled cyber-physical systems with an application to glucose control," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 12, pp. 2906–2919, Dec 2017.

[4] A. Nieto, R. Roman, and J. Lopez, "Digital witness: Safeguarding digital evidence by using secure architectures in personal devices," *IEEE Network*, vol. 30, no. 6, pp. 34–41, November 2016.

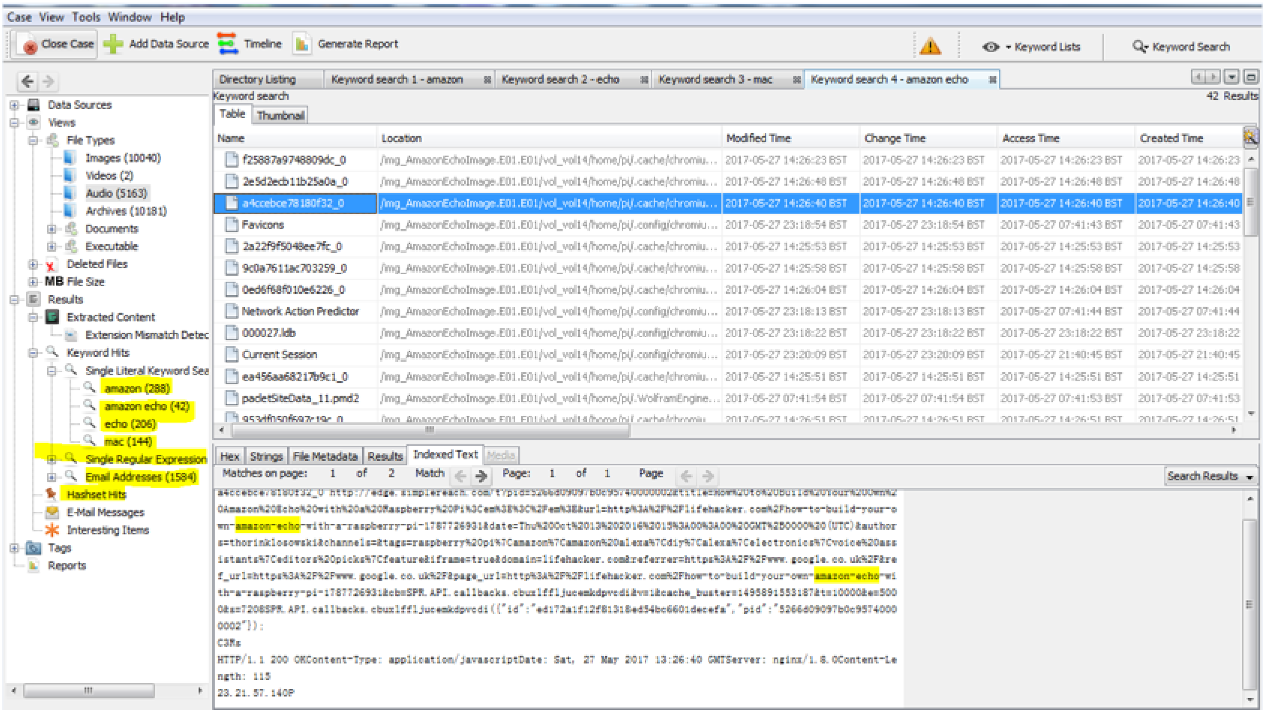
[5] H. Tsukayama. (2017) Bose headphones have been spying on customers, lawsuit claims. [Online]. Available: https://www.smh.com.au/technology/bose-20170420-gvo8pq.html

[6] J. Kastrenakes. (2017) Most smart tvs are tracking you vizio just got caught. [Online]. Available: https://www.theverge.com/2017/2/7/14527360/vizio-smart-tv-tracking-settlement-disable-settings

[7] Y. Ma, Y. Wu, J. Li, and J. Ge, "Apcn: A scalable architecture for balancing accountability and privacy in large-scale content-based networks," *Information Sciences*, 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0020025519300659

[8] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," *Industrial Informatics, IEEE Transactions on*, vol. 10, no. 4, pp. 2233–2243, 2014.

[9] Q. Do, B. Martini, and K.-K. R. Choo, "Cyber-physical systems information gathering: A smart home case study," *Computer Networks*, vol. 138, pp. 1–12, 2018.



Name	Location	Modified Time	Change Time	Access Time	Created Time
f25887a9748809dc_0	/img_AmazonEchoImage.E01.E01/vol_vol14/home/pi/.cache/chromiu...	2017-05-27 14:26:23 BST	2017-05-27 14:26:23 BST	2017-05-27 14:26:23 BST	2017-05-27 14:26:23
2e5d2ecb11b25a0a_0	/img_AmazonEchoImage.E01.E01/vol_vol14/home/pi/.cache/chromiu...	2017-05-27 14:26:48 BST	2017-05-27 14:26:48 BST	2017-05-27 14:26:48 BST	2017-05-27 14:26:48
a4ccebce78180f32_0	/img_AmazonEchoImage.E01.E01/vol_vol14/home/pi/.cache/chromiu...	2017-05-27 14:26:40 BST	2017-05-27 14:26:40 BST	2017-05-27 14:26:40 BST	2017-05-27 14:26:40
Favicons	/img_AmazonEchoImage.E01.E01/vol_vol14/home/pi/.config/chromiu...	2017-05-27 23:18:54 BST	2017-05-27 23:18:54 BST	2017-05-27 07:41:43 BST	2017-05-27 07:41:43
2a22f9f5048ee7fc_0	/img_AmazonEchoImage.E01.E01/vol_vol14/home/pi/.cache/chromiu...	2017-05-27 14:25:53 BST	2017-05-27 14:25:53 BST	2017-05-27 14:25:53 BST	2017-05-27 14:25:53
9c0a7611ac703259_0	/img_AmazonEchoImage.E01.E01/vol_vol14/home/pi/.cache/chromiu...	2017-05-27 14:25:58 BST	2017-05-27 14:25:58 BST	2017-05-27 14:25:58 BST	2017-05-27 14:25:58
0ed6f68f010e6226_0	/img_AmazonEchoImage.E01.E01/vol_vol14/home/pi/.cache/chromiu...	2017-05-27 14:26:04 BST	2017-05-27 14:26:04 BST	2017-05-27 14:26:04 BST	2017-05-27 14:26:04
Network Action Predictor	/img_AmazonEchoImage.E01.E01/vol_vol14/home/pi/.config/chromiu...	2017-05-27 23:18:13 BST	2017-05-27 23:18:13 BST	2017-05-27 07:41:44 BST	2017-05-27 07:41:44
000027.ldb	/img_AmazonEchoImage.E01.E01/vol_vol14/home/pi/.config/chromiu...	2017-05-27 23:18:22 BST	2017-05-27 23:18:22 BST	2017-05-27 23:18:22 BST	2017-05-27 23:18:22
Current Session	/img_AmazonEchoImage.E01.E01/vol_vol14/home/pi/.config/chromiu...	2017-05-27 23:20:09 BST	2017-05-27 23:20:09 BST	2017-05-27 21:40:45 BST	2017-05-27 21:40:45
ea456aa68217b9c1_0	/img_AmazonEchoImage.E01.E01/vol_vol14/home/pi/.cache/chromiu...	2017-05-27 14:25:51 BST	2017-05-27 14:25:51 BST	2017-05-27 14:25:51 BST	2017-05-27 14:25:51
padetSiteData_11.pmd2	/img_AmazonEchoImage.E01.E01/vol_vol14/home/pi/.WolframEngine...	2017-05-27 07:41:54 BST	2017-05-27 07:41:54 BST	2017-05-27 07:41:53 BST	2017-05-27 07:41:53
953df050f697c19c_0	/img_AmazonEchoImage.E01.E01/vol_vol14/home/pi/.cache/chromiu...	2017-05-27 14:26:51 BST	2017-05-27 14:26:51 BST	2017-05-27 14:26:51 BST	2017-05-27 14:26:51

```
a4ccebce78180f32_0 http://edge.simplereach.com/t?pid=5266d09097b0c9574000002&title=How%20to%20Build%20Your%20Own%2
0Amazon%20Echo%20with%20a%20Raspberry%20Pi%3Cem%3E%3C%2Fem%3E&url=http%3A%2F%2Flifehacker.com%2Fhow-to-build-your-o
wn-amazon-echo-with-a-raspberry-pi-1787726931&date=Thu%20Oct%2013%202016%2015%3A00%3A00%20GMT%2B0000%20(UTC)&author
s=thorinklosowski&channels=&tags=raspberry%20pi%7Camazon%7Camazon%20alexa%7Cdiy%7Calexa%7Celectronics%7Cvoice%20ass
istants%7Ceditors%20picks%7Cfeature&iframe=true&domain=lifehacker.com&referrer=https%3A%2F%2Fwww.google.co.uk%2F&re
f_url=https%3A%2F%2Fwww.google.co.uk%2F&page_url=http%3A%2F%2Flifehacker.com%2Fhow-to-build-your-own-amazon-echo-wi
th-a-raspberry-pi-1787726931&cb=SPR.API.callbacks.cbuxlffljucemkdpvcdi&v=1&cache_buster=1495891553187&t=10000&e=500
0&s=7208SPR.API.callbacks.cbuxlffljucemkdpvcdi({"id":"ed172a1f12f81318ed54bc6601decefa","pid":"5266d09097b0c9574000
0002"});
C3Rs
HTTP/1.1 200 OKContent-Type: application/javascriptDate: Sat, 27 May 2017 13:26:40 GMTServer: nginx/1.8.0Content-Le
ngth: 115
23.21.57.140P
```

Fig. 11. Firmware analysis using Autopsy

[10] Q. Do, B. Martini, and K. K. R. Choo, “A data exfiltration and remote exploitation attack on consumer 3d printers,” *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 10, pp. 2174–2186, Oct 2016.

[11] K. P. Trommler. (2018) Know your enemy: What happens behind the scenes in a ddos attack. [Online]. Available: https://blog.paessler.com/types-of-ddos-attacks

[12] M. S. Pour, E. Bou-Harb, K. Varma, N. Neshenko, D. Pados, and K.-K. R. Choo, “Comprehending the IoT cyber threat landscape: A data dimensionality reduction technique to infer and characterize internet-scale IoT probing campaigns,” *Digital Investigation*, 2019.

[13] S. Li, S. Zhao, Y. Yuan, Q. Sun, and K. Zhang, “Dynamic security risk evaluation via hybrid bayesian risk graph in cyber-physical social systems,” *IEEE Transactions on Computational Social Systems*, vol. 5, no. 4, pp. 1133–1141, Dec 2018.

[14] 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*, June 2015, pp. 279–284.

[15] S. Alabdulsalam, K. Schaefer, T. Kechadi, and N.-A. Le-Khac, “Internet of things forensics: Challenges and case study,” *arXiv preprint arXiv:1801.10391*, 2018.

[16] A. MacDermott, T. Baker, and Q. Shi, “Iot forensics: Challenges for the ioa era,” in *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, Feb 2018, pp. 1–5.

[17] E. Oriwoh, D. Jazani, G. Epiphaniou, and P. Sant, “Internet of things forensics: Challenges and approaches,” in *Collaborative Computing: Networking, Applications and Worksharing (Collaboratecom), 2013 9th International Conference Conference on*. IEEE, 2013, pp. 608–615.

[18] B. Copos, K. Levitt, M. Bishop, and J. Rowe, “Is anybody home? inferring activity from smart home network traffic,” in *Security and Privacy Workshops (SPW), 2016 IEEE*. IEEE, 2016, pp. 245–251.

[19] O. Arias, J. Wurm, K. Hoang, and Y. Jin, “Privacy and security in internet of things and wearable devices,” *IEEE Transactions on Multi-Scale Computing Systems*, vol. 1, no. 2, pp. 99–109, April 2015.

[20] W. W. Gibbs, “Build your own amazon echo - turn a pi into a voice controlled gadget,” *IEEE Spectrum*, vol. 54, no. 5, pp. 20–21, May 2017.

[21] Q. Do, B. Martini, and K.-K. R. Choo, “Is the data on your wearable device secure? an android wear smartwatch case study,” *Software: Practice and Experience*, vol. 47, no. 3, pp. 391–403, 2017.

[22] N.-A. Le-Khac, D. Jacobs, J. Nijhoff, K. Bertens, and K.-K. R. Choo, “Smart vehicle forensics: Challenges and case study,” *Future Generation Computer Systems*, 2019.

[23] N.-A. L.-K. Arnoud Goudbeek, Kim-Kwang Raymond Choo, “A forensic investigation framework for smart home environment,” in *In Proceedings of 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2018)*. IEEE, 2018, pp. 1446–1451.

[24] L. Caviglione, S. Wendzel, and W. Mazurczyk, “The future of digital forensics: Challenges and the road ahead,” *IEEE Security Privacy*, vol. 15, no. 6, pp. 12–17, November 2017.

[25] E. Oriwoh and P. Sant, “The forensics edge management system: A concept and design,” in *2013 IEEE 10th International Conference on Ubiquitous Intelligence and Computing and 2013 IEEE 10th International Conference on Autonomic and Trusted Computing*, Dec 2013, pp. 544–550.

[26] C. Meffert, D. Clark, I. Baggili, and F. Breitinger, “Forensic state acquisition from internet of things (fsaiot): A general framework and practical approach for iot forensics through iot device state acquisition,” in *Proceedings of the 12th International Conference on Availability, Reliability and Security*. ACM, 2017, p. 56.

[27] A. Nieto, R. Rios, and J. Lopez, “Iot-forensics meets privacy: towards cooperative digital investigations,” *Sensors*, vol. 18, no. 2, p. 492, 2018.

[28] N. Chavez. (2017) Arkansas judge drops murder charge in amazon echo case. [Online]. Available: https://edition.cnn.com/2017/11/30/us/amazon-echo-arkansas-murder-case-dismissed/index.html

[29] H. Chung, J. Park, and S. Lee, “Digital forensic approaches for amazon alexa ecosystem,” *Digital Investigation*, vol. 22, pp. S15 – S25, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1742287617301974

[30] C. S. Community. (2017) What is iot forensics and how is it different from digital forensics? [Online]. Available: https://securitycommunity.tcs.com/infosecsoapbox/articles/2018/02/27/what-iot-forensics-and-how-it-different-digital-forensics

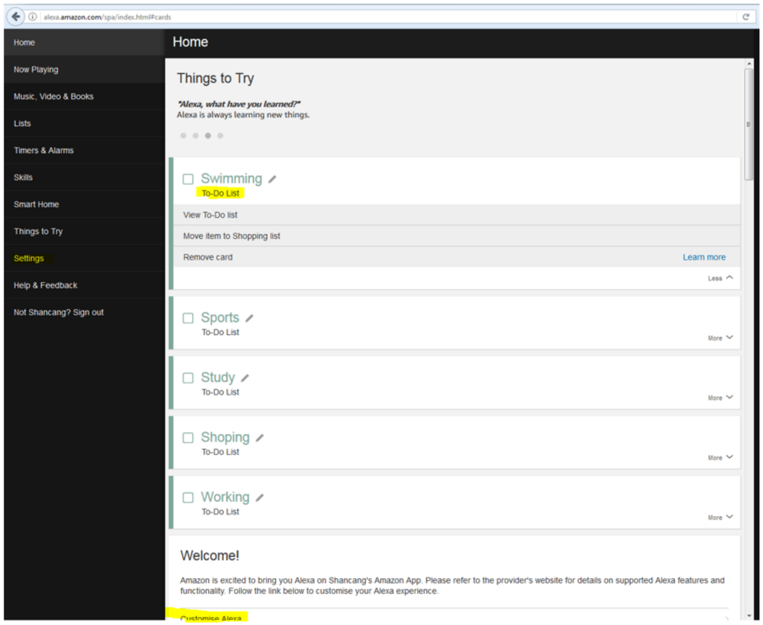
[31] R. Hegarty, D. J. Lamb, and A. Attwood, “Digital evidence challenges in the internet of things.” in *INC*, 2014, pp. 163–172.

[32] U. Salama. (2017) Investigating iot crime in the age of connected devices. [Online]. Available: https://securityintelligence.com/investigating-iot-crime-in-the-age-of-connected-devices/

[33] E. C. McLaughlin, “Suspect oks amazon to hand over echo recordings in murder case,” 2017.

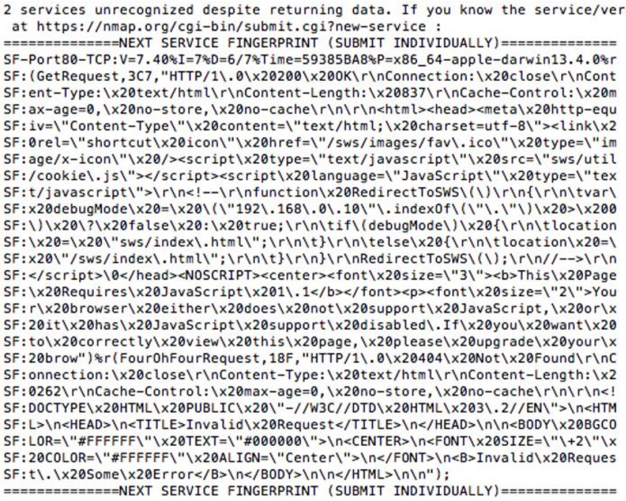
[34] R. A. S. B. W. Jansen, R. Ayers, and S. Brothers, “Guidelines on mobile device forensics,” *NIST Special Publication*, pp. 800–101, 2014.

[35] V. L. Thing, K.-Y. Ng, and E.-C. Chang, “Live memory forensics of mobile phones,” *digital investigation*, vol. 7, pp. S74–S82, 2010.



Amazon is excited to bring you Alexa on Shancang's Amazon App. Please refer to the provider's website for details on supported Alexa features and functionality. Follow the link below to customise your Alexa experience.

Fig. 12. AVS website logged using the found login id and pwd from firmware



```
2 services unrecognized despite returning data. If you know the service/version,
 at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=7.40%I=7%D=6/7%Time=59385BA8%P=x86_64-apple-darwin13.4.0%r
SF:(GetRequest,3C7,"HTTP/1\.0\x20200\x20OK\r\nConnection:\x20close\r\nCont
SF:ent-Type:\x20text/html\r\nContent-Length:\x20837\r\nCache-Control:\x20m
SF:ax-age=0,\x20no-store,\x20no-cache\r\n\r\n<html><head><meta\x20http-equ
SF:iv=\"Content-Type\"\x20content=\"text/html;\x20charset=utf-8\"><link\x2
SF:0rel=\"shortcut\x20icon\"\x20href=\"/sws/images/fav\.ico\"\x20type=\"im
SF:age/x-icon\"\x20/><script\x20type=\"text/javascript\"\x20src=\"sws/util
SF:/cookie\.js\"></script><script\x20language=\"JavaScript\"\x20type=\"tex
SF:t/javascript\">\r\n<!--\r\nfunction\x20RedirectToSWS\(\)\r\n{\r\n\tvar\
SF:x20debugMode\x20=\x20\(\"192\.168\.0\.10\"\.indexOf\(\"\.\"\)\x20>\x200
SF:\)\x20\?\x20false\x20:\x20true;\r\n\tif\(debugMode\)\x20{\r\n\tlocation
SF:\x20=\x20\"sws/index\.html\";\r\n\t}\r\n\telse\x20{\r\n\tlocation\x20=\
SF:x20\"/sws/index\.html\";\r\n\t}\r\n}\r\nRedirectToSWS\(\);\r\n//-->\r\n
SF:</script>\0</head><NOSCRIPT><center><font\x20size=\"3\"><b>This\x20Page
SF:\x20Requires\x20JavaScript\x201\.1</b></font><p><font\x20size=\"2\">You
SF:r\x20browser\x20either\x20does\x20not\x20support\x20JavaScript,\x20or\x
SF:20it\x20has\x20JavaScript\x20support\x20disabled\.If\x20you\x20want\x20
SF:to\x20correctly\x20view\x20this\x20page,\x20please\x20upgrade\x20your\x
SF:20brow")%r(FourOhFourRequest,18F,"HTTP/1\.0\x20404\x20Not\x20Found\r\nC
SF:onnection:\x20close\r\nContent-Type:\x20text/html\r\nContent-Length:\x2
SF:0262\r\nCache-Control:\x20max-age=0,\x20no-store,\x20no-cache\r\n\r\n<!
SF:DOCTYPE\x20HTML\x20PUBLIC\x20\"-//W3C//DTD\x20HTML\x203\.2//EN\">\n<HTM
SF:L>\n<HEAD>\n<TITLE>Invalid\x20Request</TITLE>\n</HEAD>\n\n<BODY\x20BGCO
SF:LOR=\"#FFFFFF\"\x20TEXT=\"#000000\">\n<CENTER>\n<FONT\x20SIZE=\"\+2\"\x
SF:20COLOR=\"#FFFFFF\"\x20ALIGN=\"Center\">\n</FONT>\n<B>Invalid\x20Reques
SF:t\.\x20Some\x20Error</B>\n</BODY>\n\n</HTML>\n\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
```

Fig. 13. Unrecognized services found in the images

[36] S. Smalley and T. M. R2X, "The case for se android," *Linux Security Summit*, 2011.

[37] H. T. Al-Rayes, "Studying main differences between android & linux operating systems," *International Journal of Electrical & Computer Sciences IJECS-IJENS*, vol. 12, no. 05, 2012.

[38] J. T. Sylve, "Android memory capture and applications for security and privacy," 2011.

[39] D. Kirkpatrick. (2017) Gartner: Global wearables sales to grow 17 percent this year. [Online]. Available: https://www.marketingdive.com/news/gartner-global-wearables-sales-to-grow-17-this-year/503480/

[40] S. Li, L. Da Xu, and S. Zhao, "5g internet of things: A survey," *Journal of Industrial Information Integration*, 2018.

[41] B. Buchanan. (2017) The new digital investigator: Interrogating alexa. [Online]. Available: https://www.linkedin.com/pulse/new-digitial-investigator-interogating-alexa-buchanan-obe-phd-fbcs/

[42] S. Li, G. Oikonomou, T. Tryfonas, T. M. Chen, and L. D. Xu, "A distributed consensus algorithm for decision making in service-oriented internet of things," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 1461–1468, May 2014.

[43] W. Miao, G. Min, Y. Wu, H. Huang, Z. Zhao, H. Wang, and C. Luo, "Stochastic performance analysis of network function virtualization in future internet," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 3, pp. 613–626, March 2019.

[44] G. Bourne". (2016) I built my own amazon echo with a raspberry pi: Alexaberry. [Online]. Available: https://dzone.com/articles/i-built-my-own-amazon-echo-alexa-with-a-raspberry

[45] N. H. A. Rahman, W. B. Glisson, Y. Yang, and K. R. Choo, "Forensic-by-design framework for cyber-physical cloud systems," *IEEE Cloud Computing*, vol. 3, no. 1, pp. 50–59, 2016.

[46] N. H. A. Rahman, N. D. W. Cahyani, and K. R. Choo, "Cloud incident handling and forensic-by-design: cloud storage as a case study," *Concurrency and Computation: Practice and Experience*, vol. 29, no. 14, 2017.

[47] G. Grispos, W. B. Glisson, and K. R. Choo, "Medical cyber-physical systems development: A forensics-driven approach," in *Proceedings of the Second IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies, CHASE 2017, Philadelphia, PA, USA, July 17-19, 2017*, 2017, pp. 108–113.

[48] S. Li, L. D. Xu, and X. Wang, "Compressed sensing signal and data acquisition in wireless sensor networks and internet of things," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 4, pp. 2177–2186, Nov 2013.

[49] S. Li, S. Zhao, P. Yang, P. Andriotis, L. Xu, and Q. Sun, "Distributed consensus algorithm for events detection in cyber physical systems," *IEEE Internet of Things Journal*, pp. 1–1, 2019.

Shancang Li received the B.Sc. and M.Sc. degrees in mechanics engineering and the Ph.D. degree in computer science from Xi'an Jiaotong University, Xi'an, China, in 2001, 2004, and 2008, respectively. He is currently a senior lecturer with department of computer science and creative technologies at University of the West of England, Bristol, UK. His current research interests include digital forensics for emerging technologies, cyber security, IoT security, data privacy-preserving, Internet of Things, Blockchain technology, and the lightweight cryptography in resource constrained devices. He has authored over 60 papers published in high profile journals and conferences. Dr. Li is the Associate Editor of IEEE Access and Journal of Industrial Information Integration. He is a member of the British Computer Society.

Kim-Kwang Raymond Choo (SM'15) received the Ph.D. in Information Security in 2006 from Queensland University of Technology, Australia. He currently holds the Cloud Technology Endowed Professorship at The University of Texas at San Antonio (UTSA). In 2016, he was named the Cybersecurity Educator of the Year - APAC (Cybersecurity Excellence Awards are produced in cooperation with the Information Security Community on LinkedIn), and in 2015 he and his team won the Digital Forensics Research Challenge organized by Germanys University of Erlangen-Nuremberg. He is the recipient of the 2018 UTSA College of Business Col. Jean Piccione and Lt. Col. Philip Piccione Endowed Research Award for Tenured Faculty, IEEE TrustCom 2018 and ESORICS 2015 Best Paper Awards, 2014 Highly Commended Award by the Australia New Zealand Policing Advisory Agency, Fulbright Scholarship in 2009, 2008 Australia Day Achievement Medallion, and British Computer Societys Wilkes Award in 2008. He is also a Fellow of the Australian Computer Society, and Co-Chair of IEEE Multimedia Communications Technical Committees Digital Rights Management for Multimedia Interest Group.

Qindong Sun received his Ph.D. degree in School of Electronic and Information Engineering from the Xian Jiaotong University, China. He is currently the professor at the Department of Computer Science and Engineering of Xian University of Technology.

His research interests include network security, online social networks, digital forensics, cyber security, and internet of things (IoT). He is a member of China Computer Federation (CCF).

William J. Buchanan is a Professor in the School of Computing at Edinburgh Napier University, and a Fellow of the BCS and the IET. He was appointed an Officer of the Order of the British Empire (OBE) in the 2017 Birthday Honours for services to cyber security. In 2018 he received an Outstanding Contribution to Knowledge Exchange at the Scottish Knowledge Exchange Awards. One of his most recent achievements is the creation of a Blockchain Identify Lab and which is one of the first of its type in the world, and has significant industry funding.

Currently he leads the Centre for Distributed Computing, Networks, and Security at Edinburgh Napier University and The Cyber Academy (http://thecyberacademy.org). His main research focus is around information sharing, IoT, e-Health, threat analysis, cryptography, and triage within digital forensics. This has led to several World-wide patents, and in three highly successful spin-out companies: Zonefox (zonefox.com); Symphonic Software

Jiuxin Cao received his PhD. degree in computer science in 2003 from Xi'an Jiaotong University, China. He is currently a professor in the School of Cyber Science and Engineering at Southeast University in China. Currently he is leading the Jiangsu Key Laboratory of Computer Networking Technology as director. His current research interests include cyber security, location based services, online social network, etc. He is a senior member of China Computer Federation (CCF).