The investigative significance of digital artefacts discovered in forensic images of household IoT devices using open-source software

KUNEV, Dimitar, JANARTHANAN, Tharmini and ZARGARI, Shahrzad <http://orcid.org/0000-0001-6511-7646>

The Investigative Significance of Digital Artefacts Discovered in Forensic Images of Household IoT Devices Using Open-source Software

Dimitar Kunev[1], Tharmini Janarthanan[2], Shahrzad Zargari[2]
University of Warwick[1], Sheffield Hallam University[2]
United Kingdom

Abstract

As the IoT technology grows, forensic practitioners more often come across IoT devices that present significant challenges to their investigations. IoT devices lack any standardisation in design and security. As a result, the devices can be incredibly different to one another either by running other operating systems or using various data formats and network protocols. IoT devices also use Real-Time operating systems that only store data when used, creating challenges in the data acquisition stage and the analysis stage. The structure of the wider IoT environment also presents jurisdiction and data location challenges, such as identifying who owns the data and how to preserve its integrity. The forensic investigation in the IoT environment involves a combination of cloud forensics, network forensics, and device forensics where there is a lack of a systematic framework for investigation as well as suitable forensic tools.

In this study, a comprehensive analysis of IoT datasets published by NIST was conducted to discover the evidential significance of data stored in these IoT devices in order to assist forensic practitioners in their investigations. Two open-source tools (Autopsy and bulk_extractor) were used in this research. Their performance was evaluated. A triage method was proposed to help investigators identify the most forensically valuable IoT devices in a crime scene. The proposal prioritised devices that contained the most significant evidence, which can be used as a starting point in any investigation.

Keywords: digital forensics, IoT, Autopsy, bulk_extractor, VTO Labs, forensic investigation

1. Introduction

The Internet of Things (IoT) is defined as the network capability built into objects and devices that allow them to connect to the Internet and send and receive data [1]. In the last few years, there has been an exponential increase in the amount of IoT devices and technologies being applied to various contexts in modern society. IoT technologies have become embedded into people's everyday lives through smart home devices and appliances as they, together with smart wearable devices, comprise 63% of all connected devices worldwide [2]. As a result of their ubiquity, IoT devices are described as powerful and rich sources of evidential data used in digital forensic investigations [3].

This paper aims to contribute to the knowledge of IoT forensics examination by analysing the existing IoT device datasets to ascertain the number of digital artefacts that can be discovered. This research compares the employed tools in the study and evaluates their performance. An IoT device triage and prioritisation method have been proposed based on the research findings to assist digital forensic practitioners in IoT investigations.

Section 2 of this paper outlines the challenges presented by IoT devices in the traditional digital forensic field. Next, it looks at the current IoT forensic frameworks in response to the challenges, highlighting areas for improvement. Section 3 explains the research methodology and introduces the IoT device datasets that have been used as the basis for this research. Section 4 looks at the research findings, evaluates and compares the tools' performance before finally proposing an IoT device triage and prioritisation model. The last section outlines the conclusion and describes the impact of this study.

2. Related Work

This section presents the landscape of current research into IoT forensics. It discusses the identified challenges IoT devices pose to the current digital forensic method. Subsequently, it outlines the various

DOI: 10.20533/ijicr.2042.4655.2021.0133

proposed frameworks and methods identified in the literature.

2.1. Challenges in IoT forensics

The nature of IoT environments presents obstacles in almost every step of the digital forensic investigation [4]. These challenges are further discussed in detail below.

2.1.1. Evidence Location. In traditional digital forensics, it is easier to locate and determine which devices are compromised and can be a source of evidential forensic data. In contrast, IoT forensics is challenging due to the range and characteristics of IoT devices. For example, a modern smart home can have up to 17 different potential sources of evidence, including smart appliances, smart meters, smart hubs, personal assistants, and various wearables [5]. Furthermore, the dynamic nature of the IoT environment with devices constantly exiting and entering a given network either automatically or due to the user physically moving them results in blurring boundaries. The devices move through different networks, complicating the process of determining case boundaries [6].

2.1.2. Data acquisition. In the acquisition stage, a forensic image is made of all the data on a device, which can serve as the basis for any future investigations to preserve the original device's data integrity [7]. The use of a large amount of internet traffic in an IoT environment necessitates creating a forensic image of the network data, which is often challenging due to the use of encryption protocols by some of these IoT devices when transmitting data [4]. Some data might be stored in a third-party cloud service providers across countries with different laws and regulations. It raises jurisdiction issues regarding who owns the data generated from IoT devices and the limitation of physical accessibility to the data for investigation purposes.

The volatile nature of IoT devices also poses a challenge to the data acquisition phase. It is due to the resource-limited design and continuous operations of IoT devices whereby data might only exist for a short amount of time before being completely overwritten because of a lack of storage space [4], [5], [6]. Some of these IoT devices use Real-Time Operating Systems (RTOS), which do not use local storage and only record data during operation [8]. Therefore, creating a forensic image from RTOS devices must be done while the device is operating, which contradicts ACPO principles [7].

2.1.3. Evidence preservation. An essential part of forensics is maintaining a chain of custody as it is used to maintain the integrity and repeatability of the produced evidence. Maintaining a chain of custody in an IoT environment poses a challenge to forensic investigators due to various networks with different jurisdictions. Evidence must be gathered from several remote servers, and it can be in multiple other formats [4].

2.1.4. Examination process. One of the biggest problems faced during forensic analysis of IoT devices is the heterogenous nature, which utilises various formats, operating systems, network protocols, and hardware [6]. The highly varied device format requires different tools and techniques to access, extract and make sense of the existing data in IoT devices [6]. As such, the effectiveness of traditional forensic software when analysing IoT devices has been questioned. While they might be able to provide forensic carving of the data found on lightweight devices with RTOS, they would still struggle with its interpretation across multiple available formats [5]. Al-Sadi et al. [9] proposed using open-source forensic tools such as Autopsy, Wireshark, Nmap and bulk_extractor for analysing all aspects of the IoT environment as their open-source nature allow digital forensic investigators to modify the source codes if needed. This demonstrates that different tools are often required to investigate IoT devices.

Further, IoT devices produce a huge volume of data, posing a challenge to digital forensic investigators to adequately examine these data, complete the investigation, and produce evidence in court within a short time frame. In certain circumstances, the forensic value of this huge amount of data is often minimal. Some of these IoT devices simply provide periodic information about changes to their environment, thus providing little more than circumstantial evidence [4].

2.2. Current IoT forensic frameworks

Various IoT digital forensic frameworks, models, and processes have been proposed to respond to the outlined IoT forensic challenges and serve as a guide for gathering, examining, and analysing digital forensic data from the IoT environment [5]. They range from frameworks designed to tackle challenges related to specific steps of the digital forensic investigation process to frameworks based on examining particular IoT devices. This includes identifying and prioritising evidence sources in the IoT environment [10] and models proposing proactive solutions by implementing a central evidence

DOI: 10.20533/ijicr.2042.4655.2021.0133

repository that passively collects evidential IoT data [11].

Conversely, research focusing on examining IoT devices such as smart TVs and IoT hubs have discovered that most evidential data such as account names, device settings and time zone information was found on the mobile device acting as the endpoint of the IoT environment under the form of SQLite databases [12], [13]. The methods and software that have been used to identify and extract these forensic data vary considerably. However, many of these examinations have been carried out under lab environments that allow for complete control of variables that differ significantly from the ideal IoT environment set up [3].

3. Methodology

This section aims to outline the methodology used in conducting this research. It provides an overview and characteristics of the examined IoT image datasets. Next, it covers the forensic tools used, explains why they were chosen, and explains the digital forensic methods employed.

3.1. IoT datasets

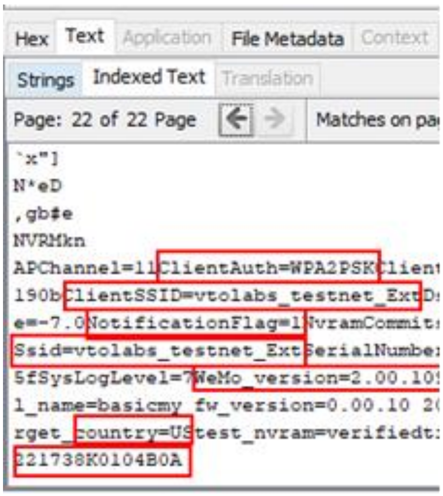
This study analyses a publicly available database of forensic images of IoT devices published by VTO Labs [14]. There was a clear literature gap surrounding the VTO Labs IoT datasets as only two sources were identified that had examined some of the datasets. The first work was the Zena Forensics blog which discussed four images in four separate blog posts, namely the Samsung Refrigerator, LG TV, Android TV and Roomba images [15], [16], [17], [18]. The other was a paper by [19] that examined the Eufy Floodlight camera image and the Kasa Smart Light bulb image. Overall, both studies discovered a good amount of evidential data about each device and explained how the data was gathered.

During this study, several issues with the IoT datasets from VTO Labs were identified. Firstly, it was not clear about the method used to acquire the forensic images of these devices. The website mentioned that: "The data has been acquired using digital forensic techniques to extract data from the data storage areas on the devices and their affiliated systems" however, the techniques and tools used were not elaborated on [14]. Previous research conducted on Smart TV forensic analysis showed that the storage card had to be separated from the TV's motherboard to produce a forensic image of the storage device [20]. Thus, the forensic integrity of these datasets cannot be verified.

In addition, several VTO IoT datasets contained only images of the device's storage space. In contrast, others included an accompanying mobile image which was assumed to have acted as the controller. Two of the datasets appeared to be duplicates of one another, while the dataset for the Philips Hue Bridge was unavailable at the time of the study. The Vizio TV image is linked to an empty Google drive folder. In contrast, some of the datasets contained two or more forensic images of the same data. For example, in the iRobot690 Roomba dataset, there were two .bin image files, one called "RoombaDump.bin" and the other "RoombaDump2.bin". It is unknown why this was the case and whether both images were derived using the same method. As a result, out of the 16 datasets, only 9 could be examined.

3.2. Employed forensic tools

In this research, two open-source tools (Autopsy and bulk_extractor) were used to analyse the forensic images from the VTO IoT datasets. Both tools were identified as one of the most appropriate tools to examine IoT devices (end sensor devices and application layer devices) [9]. Therefore, the two tools were selected to analyse the VTO IoT datasets as many of these datasets contained an image of the end device and the mobile device used as a controller. Once all the images are examined using both tools, the results will be manually scanned following the conventional digital forensic process. In Autopsy, this will be achieved using the software's keyword search engine and forensic carving capabilities. In contrast, in bulk_extractor, this will be achieved through a manual investigation of all the data that the software managed to carve out.



```
`x"]
N*eD
,gb#e
NVRMkn
APChannel=11ClientAuth=WPA2PSKClient
190bClientSSID=vtolabs_testnet_ExtD:
e=-7.0NotificationFlag=1NvramCommit:
Ssid=vtolabs_testnet_ExtSerialNumbe:
5fSysLogLevel=7WeMo_version=2.00.10
1_name=basicmy fw_version=0.00.10 2(
rget_country=UStest_nvram=verifiedt:
221738K0104B0A
```

Figure 1. Illustrates the indexed text method used

DOI: 10.20533/ijicr.2042.4655.2021.0133

Additionally, as Autopsy did not recognise some forensic images' file systems, therefore a manual examination of the indexed text found by Autopsy was performed. This method was derived from Epifani's way of examining the Roomba iRobot690 image [18].

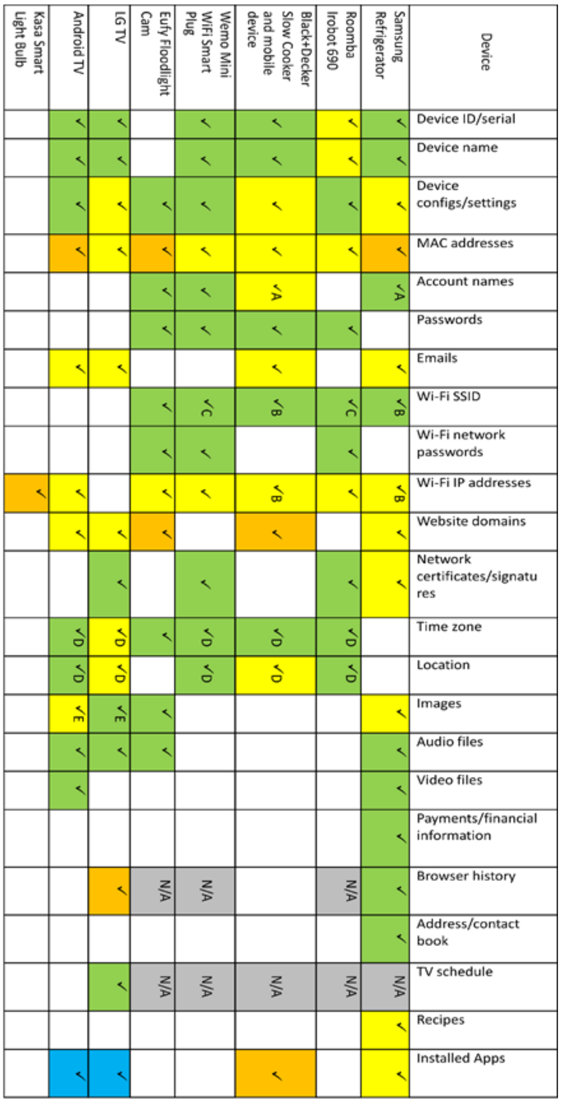
4. Findings

Section 4 covers the digital artefacts discovered on the device images as a result of the examination carried out. It presents an overview and description of the discovered data from each device. Further, it evaluates the effectiveness of the two open-source tools used in this examination and proposes an IoT device triage and prioritisation method based on the findings.

4.1. Overview of data

Based on the examined devices, the Samsung Refrigerator was the one that contained the most information. This was due to the image's file system being the only one that was recognised by Autopsy, allowing for the folder and partition structure of the device to be viewed and analysed. The following datasets which yielded the most information were the LG TV and the Slow Cooker with its mobile device image. The data found on each dataset was different, with the LG TV providing more Audio/Visual data, while the mobile device image in the Slow Cooker dataset provided much more device configuration information together with password names and account numbers. The subsequent datasets were the Android TV box and the WeMo Wi-Fi smart plug in the order of information discovered. Once again, although similar in volume, the information in both devices varied significantly with the TV image containing Audio/Visual and image data, which the Wi-Fi plug image lacked due to its design. Conversely, the WeMo plug, like the Slow cooker dataset, contained information regarding accounts, Wi-Fi SSID and both account and Wi-Fi passwords, none found on the Android TV box. The following image by information discovered was the Eufy Floodlight camera. The camera image provided diverse data, including Audio/Visual files, account, password information, and device configuration data but did not contain any device identification data. This was followed by the iRobot 690 Roomba, which yielded a surprising amount of information for such a device. The device with the least amount of data discovered was the Kasa Smart Light bulb, for which only IP addresses were obtained using bulk_extractor. Information such as Device IDs, names, and configuration settings was found in almost all devices, except for the Kasa Smart Light Bulb.

Table 1. An overview of discovered data on each device according to which tool discovered it



Kasa Smart Light Bulb	Android TV	LG TV	Eufy Floodlight Cam	Wemo Mini WiFi Smart Plug	Black+Decker Slow Cooker and mobile device	Roomba Irobot 690	Samsung Refrigerator	Device
	🟩 ✓	🟩 ✓		🟩 ✓	🟩 ✓	🟨 ✓	🟩 ✓	Device ID/serial
	🟩 ✓	🟩 ✓		🟩 ✓	🟩 ✓	🟨 ✓	🟩 ✓	Device name
	🟩 ✓	🟨 ✓	🟩 ✓	🟩 ✓	🟨 ✓	🟩 ✓	🟨 ✓	Device configs/settings
	🟧 ✓	🟨 ✓	🟧 ✓	🟨 ✓	🟨 ✓	🟨 ✓	🟧 ✓	MAC addresses
			🟩 ✓	🟩 ✓	🟨 ✓A		🟩 ✓A	Account names
			🟩 ✓	🟩 ✓	🟩 ✓	🟩 ✓		Passwords
	🟨 ✓	🟨 ✓			🟨 ✓		🟨 ✓	Emails
			🟩 ✓	🟩 ✓C	🟩 ✓B	🟩 ✓C	🟩 ✓B	Wi-Fi SSID
			🟩 ✓	🟩 ✓		🟩 ✓		Wi-Fi network passwords
🟧 ✓	🟨 ✓		🟨 ✓	🟨 ✓	🟨 ✓B	🟨 ✓	🟨 ✓B	Wi-Fi IP addresses
	🟨 ✓	🟨 ✓	🟧 ✓		🟧 ✓		🟨 ✓	Website domains
		🟩 ✓		🟩 ✓		🟩 ✓	🟨 ✓	Network certificates/signatures
	🟩 ✓D	🟨 ✓D	🟩 ✓	🟩 ✓D	🟩 ✓D	🟩 ✓D		Time zone
	🟩 ✓D	🟨 ✓D		🟩 ✓D	🟨 ✓D	🟩 ✓D		Location
	🟨 ✓E	🟩 ✓E	🟩 ✓				🟨 ✓	Images
	🟩 ✓	🟩 ✓	🟩 ✓				🟩 ✓	Audio files
	🟩 ✓						🟩 ✓	Video files
							🟩 ✓	Payments/financial information
		🟧 ✓	N/A	N/A		N/A	🟩 ✓	Browser history
							🟩 ✓	Address/contact book
		🟩 ✓	N/A	N/A	N/A	N/A	N/A	TV schedule
							🟨 ✓	Recipes
	🟦 ✓	🟦 ✓			🟧 ✓		🟨 ✓	Installed Apps

A significant amount of information was discovered for the mobile device in the Slow Cooker dataset in a carved .txt file which displayed that the device in question was an iPad 5.1 running iOS 10.3.2. Information about the operating systems of other devices was also identified within the LG TV running the Linux-based WebOS, which was created explicitly for use in LG products. Similarly, the Samsung Refrigerator ran TizenOS, a Linux-based OS made specifically for running Samsung products. The Samsung Refrigerator also contained SQLite files that outlined the privileges with which specific core processes ran and a "usage.db" file that kept track of electricity usage by the device and could indicate

DOI: 10.20533/ijicr.2042.4655.2021.0133

when the refrigerator was on or off. Information about email addresses was found in some of the devices, but this ultimately yielded little data of forensic value as most of the emails were discovered in either open-source licensing or support documents.

Network data was also discovered for the bulk of the devices. The Eufy floodlight camera was found to store its Wi-Fi SSIDs and passwords in plain text with the Wi-Fi network "NETGEAR05" having the password "12345678". Moreover, the same was true for the iRobot 690 Roomba, where the Wi-Fi network "vtolabs_testnet" with its password "findthedata" was also stored in plain text. Information about visited domains and browser history was also discovered in the devices' images that supported it. The Samsung Refrigerator contained an SQL file called "browser-history.db", which showcased the device's browser history. Bulk_extractor discovered cookies present on the LG TV image that could be used to reconstruct the device's internet history as at least one of them was tied to YouTube advertisements indicating the site had been visited. TV channels and schedule information were discovered in two .json files in the LG TV image, which contained data relating to the airtime of certain shows and gave a brief description of their premise. This can potentially aid forensic investigators in establishing a timeline of events.

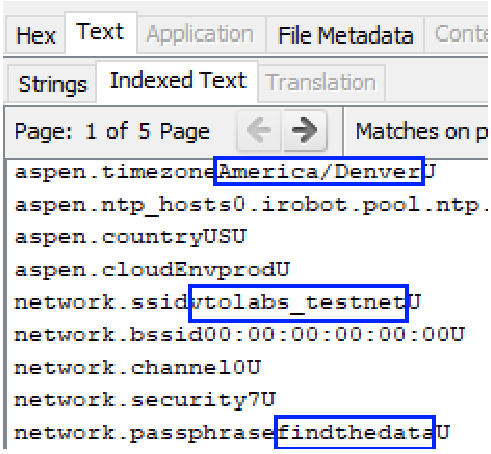
Account name and password information for each device were more scattered but yielded some interesting findings. For example, the Eufy Floodlight camera was discovered to store its usernames and passwords in a plain .txt file. This is a known vulnerability in IoT devices where usernames and passwords are either hard coded with default values or are stored in an unencrypted manner [2].

```
[user]
user1                              = admin
pwd1                               = admin
user2                              = opt
pwd2                               = opt
user3                              = guest
pwd3                               = guest
```

Figure 2. Usernames and passwords found on the Eufy floodlight camera image

Finally, information about the installed applications was discovered in the Samsung refrigerator and the mobile device in the Slow Cooker dataset. For the refrigerator, this information was present in the "appdb. db" file, which identified the following applications – Spotify, AccuWeather, FoodMinder and Pandora. The mobile device in the Slow Cooker dataset was discovered to have applications typical for the iOS environment, such as Safari, iTunes, iBooks, and the application for controlling the Slow Cooker.

Some devices were found to contain the same username – "connectedkitchenvto@gmail.com". They are marked as "A" in Table 1. The two devices also shared similar Wi-Fi addresses and networks marked as "B" in Table 1. The Roomba image and the WeMo Wi-Fi smart plug contained the same Wi-Fi network name amongst their data – "vtolabs_testnet", marked as "C" in Table 1. Moreover, time zone and location data were discovered for almost all devices, and all of them featured variations of US, Denver, UTC-7 and UTC-6, marked as "D" in Table 1. Finally, the two Smart TV images were found to have access to the same popular channels and services – YouTube, Netflix and ESPN, marked as "E" in Table 1.



```
aspen.timezoneAmerica/DenverU
aspen.ntp_hosts0.irobot.pool.ntp.
aspen.countryUSU
aspen.cloudEnvprodU
network.ssidvtolabs_testnetU
network.bssid00:00:00:00:00:00U
network.channel0U
network.security7U
network.passphrasefindthedataU
```

Figure 3. Timezone, network SSID and password information found on the iRobot 690 Roomba image

4.2. Evaluation of the tools

This section compares the results of the two tools used to examine the VTO Labs datasets. Additionally, they were also compared with the licensed X-Ways Forensics software which was used in previous research to examine some of the images from VTO Labs [15], [16], [17], [18]. The study assesses each tool's strengths and weaknesses and compares their performance to established forensic software to determine their viability as alternatives.

4.2.1. Comparison of Autopsy and bulk_extractor. While similar in their application, Autopsy and bulk_extractor feature fundamental differences in their design. As such, a comparison between the two tools will be helpful to researchers and practitioners in helping them to decide which tool to utilise. This was achieved through categorising and dividing the digital artefacts discovered according to whether Autopsy, bulk_extractor or both found them. This can be seen

DOI: 10.20533/ijicr.2042.4655.2021.0133

in Table 1 where artefacts discovered only by Autopsy are coloured green, artefacts discovered only by bulk_extractor are coloured in orange and artefacts found by both tools are coloured in yellow. The sections marked in blue are digital artefacts found by neither tool but were discovered by previous research of the VTO Labs database.

Based on this, the different characteristics of both tools were analysed regarding the type of evidential data found and the type of forensic image each tool was best at examining. Additionally, the findings of the better performing tool were compared to the conclusions produced by the professional forensic software X-ways forensics, which Epifani used in his examinations of four of the IoT devices [15], [16], [17], [18].

It is important to note that while Autopsy and bulk_extractor serve the same purpose, they function very differently. Autopsy is an open-source forensic platform that relies on powerful built-in keyword search functions and file signature identifiers to identify data and produce forensic images. It also features a developed Graphical user interface (GUI), virtualising the image environment and partitions. On the other hand, bulk_extractor has much simpler features without a GUI interface and is solely focused on its ability to extract features such as emails, IP addresses and website domains. Bulk_extractor presents these findings in .txt files in a raw string form and in a histogram, showing the number of times the data was found in the image. Most digital artefacts were found using Autopsy with bulk_extractor managing to find a smaller but evidentially significant part. The overlapping data found by both tools are presented in Table 2.

Table 2. Data found by both tools on the devices from the VTO Labs dataset

Device	Data found by both tools
Samsung Refrigerator	Emails, IP Addresses, Website domains, Digital certificates, Images, Device Settings, Recipes, Installed Apps,
Roomba Irobot 690	Device name, Device ID, IP addresses
Black+Decker Slow Cooker and mobile device	Device settings, MAC addresses, Account names, Emails, IP addresses, Location
Wemo Mini Wi-Fi Smart Plug	MAC addresses, IP addresses
Eufy Floodlight Cam	IP Addresses
LG TV	Device settings, MAC addresses, Emails, Website domains, Time zone, Location
Android TV box	Emails, IP Addresses, Website domains, Images
Kasa Smart Light bulb	None

As can be seen from Table 2, the most common digital artefacts found by both tools were IP addresses (6), followed by E-mails (4), with MAC addresses and website domains being third (3). This result was due to bulk_extractor's specific extraction algorithm focused mainly on network data. Crucially, bulk_extractor extracted data that was not found using Autopsy, which is presented in Table 3.

Nonetheless, despite the strong results of bulk_extractor regarding network data present on the images, Autopsy was better at discovering every other type of data overall. It is noticeable that the design, interface, and functionality of Autopsy is more similar to X-Ways forensics. Therefore, it will be more suitable to compare Autopsy with X-Ways rather than bulk_extractor.

Table 3. Data found only by bulk_extractor

Device	Data found only by bulk_extractor
Samsung Refrigerator	MAC addresses
Black+Decker Slow Cooker and mobile device	Website domains, Installed apps
Eufy Floodlight Cam	MAC addresses, Website domains
LG TV	Browser history
Android TV box	MAC addresses
Kasa Smart Light Bulb	IP addresses

4.2.2. Comparison of Autopsy and X-Ways Forensics. X-Ways Forensics managed to recognise the file systems of the Samsung Refrigerator, LG TV and Android TV box showing the partitions in the devices [15], [16], [17]. This is significant as Autopsy only managed to recognise the file system of the Samsung refrigerator image. The iRobot 690 image was the only image that was not recognised by X-Ways [18]. It is essential to mention that the installed applications on both Smart TV images were found by X-Ways Forensics, not by Autopsy nor bulk_extractor [16], [17]. On the other hand, there were two .pdf files discovered by Autopsy in the Samsung Refrigerator image, which were not presented in [15]. The two .pdf files were of a payment-by-wire transaction carried out using the banking site "chase.com" and contained the date of the transaction and the amount paid.

4.3. IoT device triage proposal

This section focuses on providing insight into which devices should be prioritised in a hypothetical IoT forensics investigation based on the data obtained from examining the VTO Labs datasets.

4.3.1. Information discovered on devices regarding other devices. As each IoT device forms an active part of a large and interconnected IoT environment, they often store information regarding the environment that can be used to reconstruct it. Information about other devices was found in 3 of the datasets – the Samsung Refrigerator, the Slow Cooker mobile device and the LG TV.

Table 4. Information found about other devices

Device	Number of connected devices	Type of connected devices
Samsung Refrigerator	3	3x Mobile phones
Mobile Device that was included with Slow Cooker	1	1x Slow Cooker + a big list of multiple others*
LG TV	1	Remote Control

The Samsung Refrigerator contained a database file that had information about connected devices. This file contained data about four devices, one of which was the refrigerator itself, and the other three were mobile phone devices – two Samsung G930V and one Google Pixel 2. Additionally, while the refrigerator and the mobile device from the Slow cooker dataset contained the exact account name ("connectedkitchenvto@gmail.com"), no data about the mobile device was found in the refrigerator image as the mobile device in the Slow Cooker dataset was an iPad 5.1.

The LG TV image contained a single connected device in the form of an LGE MR18 remote control. This information was discovered in a carved .ini file that included a timestamp, MAC address for the device, process ID number, and the encryption key for the remote control. Finally, the mobile device from the Slow Cooker dataset contained information about multiple connected devices. This information was discovered in carved .txt files from the device and revealed a large amount of data related to other devices, which at some points were connected to the iPad. Among these devices was the Slow Cooker, which was in the dataset, but other devices such as "Smart Curtain", "Gas Water Heater", "Hob" and more importantly "Refrigerator", "Smart plug" and "Smart Lighting" were also discovered. The latter three might represent devices from the VTO Lab datasets, with "Refrigerator" being the Samsung Refrigerator which, as mentioned before, contained the exact account name as the iPad, "Smart Plug" being the WeMo Wi-Fi Smart plug and "Smart Lighting" can either be the Kasa Smart Light bulb image or the Hue Light bulb.

4.3.2. Evaluation of the results. Previous research identified that much of the information about specific IoT objects were found in the mobile devices, which comprised the final application layer of the IoT environment [12], [13]. This was supported by the forensic examinations carried out in this work, particularly a large amount of information gathered from the mobile device image included in the Slow Cooker dataset. In addition, one study stated that due to the constantly changing nature of the IoT environment, gathering data from a specific device might not be possible as the device might not be available or not contain any data [10]. As such, the paper proposed that if a device is unavailable, data about it can still be obtained from other devices which had previously connected to it as they would contain trace data [10]. Findings from the research carried out in this work supported this notion. A straightforward example was the discovery of trace data about an LGE MR18 remote control on the LG TV. This device was not featured in the original VTO Labs IoT datasets. Similar information was discovered about other connected devices that were not part of the VTO Labs IoT datasets in the Samsung Refrigerator image and the mobile device image in the Slow Cooker dataset.

4.3.3. IoT device triage and prioritisation. Based on the findings in the previous section, the following IoT device triage and prioritisation model is proposed:

1. The priority should be given to the seizure of mobile devices in an IoT investigation. This is because they would have the most information regarding the IoT environment and the connected devices, including the mobile applications. This makes them the ideal starting point following the NBT framework [10].
2. Next, large household appliances such as Smart TVs, smart Refrigerators and any other smart devices that offer more advanced capabilities than standard IoT devices should be prioritised for forensic seizure and examination. These types of devices were found

DOI: 10.20533/ijicr.2042.4655.2021.0133

to contain the most comprehensive data and the most varied data. They also included information about other devices connected to them, thus proving to be a valuable source of device traces according to the NBT model [10].

3. The next priority is given to any other IoT devices in order of their perceived capabilities. Devices in this category are a step-down from the previous multi- capability smart objects. Still, they offer more functionality than a simple end sensor device with a network connection such as a smart light bulb. The Eufy Floodlight camera, the WeMo Wi-Fi Smart Plug and the Roomba iRobot 690 are some examples of this category. These devices contained a good amount of forensic information but did not have the NBT capabilities that the previous devices offered, reducing their seizure priority [10].

4. Finally, the most simple and basic smart objects should be seized and examined last, like those that only have a sensor. Examples include the smart light bulb images from the VTO Labs datasets, which contained almost no real forensic information apart from a couple of IP addresses.

5. Conclusion

We examined a wide range of IoT device images published in the VTO Labs IoT databases, ranging from simple resource-limited end sensor devices like the Kasa smart light bulb to powerful and complex appliances like the Smart TV images and the Samsung Refrigerator image. This paper has identified the type of digital artefacts found on each device. Digital forensic investigators can use these findings to identify the potential evidential value of similar IoT devices during their investigations, thus saving time and resources.

Moreover, this study compared the effectiveness of three different forensic tools – bulk_extractor, Autopsy and X-Ways, supplying forensic examiners with a guide on the pros and cons of each tool. Autopsy was also compared to the paid forensic software of X-Ways Forensics used in previous research on four images in the VTO Labs IoT dataset. Autopsy managed to reproduce much of the data found by X-Ways with only minor exceptions, thus demonstrating the viability of open-source forensic tools as alternatives to established software.

Lastly, this paper has developed an IoT device triage guide based on synthesising the previously proposed IoT forensics frameworks and the data discovered in this study. Applying the NBT concept and Last-on-Scene algorithm, a triage order for IoT devices was proposed based on the number of digital artefacts found for each device and the information contained by the device about other devices and its larger IoT environment. This can guide digital forensic investigators when assessing potential sources of digital evidence and their significance in a crime scene or during a criminal investigation.

There is potential for further work in this area. Unlike VTO's drone set, which has been examined in multiple papers, their IoT datasets have only been featured in the two papers identified in this research. Thus, there is ample opportunity to examine this dataset using one of the multitudes of other paid or open-source forensic tools such as Magnet AXIOM, Guymager, FTK Imager, and SIFT. This will help reaffirm or reject the findings of previous studies and compare the effectiveness of the forensic tools to one another.

Additionally, the forensic images examined in this paper were static. Any information about network features and architectures was only presumed using the forensic images' available digital artefacts. Further research can potentially focus on setting up a controlled laboratory environment with several devices connected to a large IoT network. This network can then be examined in a live environment to ascertain a more detailed view of the exact data sent and transmitted by these devices to one another.

6. References

[1] Merriam-Webster, "Internet of Things," *Merriam-Webster,* 2021. https://www.merriam-webster.com/dictionary/Internet%20of%20Things, (Access Date: 8 May 2021).

[2] J. Malan, J. Eager, E. Lale-Demoz, G. C. Ranghieri and M. Brady, *Framing the Nature and Scale of Cyber Security Vulnerabilities within the Current Consumer Internet of Things (IoT) Landscape*, Centre for Strategy & Evaluation Services, 2020.

[3] F. Servida and E. Casey, "IoT forensic challenges and opportunities for digital traces," *Digital Investigation,* vol. 28**,** Supplement, pp. S22-S29, April, 2019. doi:https://doi.org/10.1016/j.diin.2019.01.012.

[4] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis and E. K. Markakis, "A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues," in *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1191-1221, Secondquarter 2020, doi: 10.1109/COMST.2019.2962586.

[5] M. Chernyshev, S. Zeadally, Z. Baig and A. Woodward, "Internet of Things Forensics: The Need, Process Models, and Open Issues," in *IT Professional*, vol. 20, no. 3, pp. 40-49, May./Jun. 2018, doi: 10.1109/MITP.2018.032501747.

[6] J. Hou, Y. Li, J. Yu and W. Shi, "A Survey on Digital Forensics in Internet of Things," in *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 1-15, Jan. 2020, doi: 10.1109/JIOT.2019.2940713.

[7] Association of Chief Police Officers, "*ACPO Good Practice Guide for Digital Evidence*," Association of Chief Police Officers, 2012.

[8] C. Meffert, C. Devon, 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," *ARES '17: Proceedings of the 12th* International *Conference on Availability, Reliability and Security*, Article no. 56, pp. 1-11, April, 2017. doi: https://doi.org/10.1145/3098954.3104 053.

[9] M. B. Al-Sadi, L. Chen and R. J. Haddad, "Internet of Things Digital Forensic Investigation Using Open Source Gears," *SoutheastCon 2018*, 2018, pp. 1-5, doi: 10.1109/SECON.2018.8479042.

[10] E. Oriwoh, D. Jazani, G. Epiphaniou and P. Sant, "Internet of Things Forensics: Challenges and approaches," *9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing*, 2013, pp. 608-615, doi: 10.4108/icst.collaboratecom.2013. 254159.

[11] S. Zawoad and R. Hasan, "FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things," *2015 IEEE International Conference on Services Computing*, 2015, pp. 279-284, doi: 10.1109/SCC.2015.46.

[12] S. Li, K. R. Choo, Q. Sun, W. J. Buchanan and J. Cao, "IoT Forensics: Amazon Echo as a Use Case," in *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6487-6497, Aug. 2019, doi: 10.1109/JIOT.2019.2906946.

[13] G. Dorai, S. Houshmand and I. Baggili, "I Know What You Did Last Summer: Your Smart Home Internet of Things and Your iPhone Forensically Ratting You Out," in *Proceedings of the 13th International Conference on Availability, Reliability and Security (ARES 2018),* 2018, pp. 1-10, doi: https://doi.org/10.1145/3230833.3232814.

[14] VTO Labs, "IoT Forensics," *VTO Labs,* 2021. https://www.vtolabs.com/iot-forensics, (Access Date: 5 May 2021).

[15] M. Epifani, "A journey into IoT Forensics - Episode 1 - Analysis of a Samsung Refrigerator (aka thanks VTO Labs for sharing!)," *Zena Forensics, 2020.* https://blog.digital-forensics.it/2020/12/a-journey-into-iot-forensics-episode-1.html, (Access Date: 4 June 2021).

[16] M. Epifani, "A journey into IoT Forensics - Episode 2 - Analysis of an LG Television (aka thanks VTO Labs for sharing!)," *Zena Forensics,* 2020. https://blog.digital-forensics.it/2020/12/a-journey-into-iot-forensics-episode-2.html, (Access Date: 5 June 2021).

[17] M. Epifani, "A journey into IoT Forensics - Episode 3 - Analysis of an Ematic Android TV OS Box (aka thanks VTO Labs for sharing!)," *Zena Forensics,* 2020. https://blog.digital- forensics.it/2020/12/a-journey-into-iot-forensics-episode-3.html, (Access Date: 5 June 2021).

[18] M. Epifani, "A journey into IoT Forensics - Episode 4 - Analysis of an iRobot Roomba 690 (aka thanks VTO Labs for sharing!)," *Zena Forensics,* 2020. https://blog.digital-forensics.it/2020/12/a-journey-into-iot-forensics-episode-4.html, (Access Date: 5 June 2021).

[19] F. Salamh, "A Forensic Analysis of Home Automation Devices (FAHAD) Model: Kasa Smart Light Bulb and Eufy Floodlight Camera as Case Studies," in *International Journal of Cyber Forensics and Advanced Threat* Investigations, vol. 1, no. 1-3, pp. 18-26, Dec. 2020, doi: https://doi.org/10.46386/ijcfati.v1i1-3.16.

[20] A. Boztas, A.R.J. Riethoven, and M. Roeloffs, "Smart TV forensics: Digital traces on televisions," in *Digital Investigation*, vol. 12, sup. 1, pp. S72-S80, March 2015, doi: https://doi.org/10.1016/j.diin.2015.01.012.

DOI: 10.20533/ijicr.2042.4655.2021.0133