Recovery of Forensic Artefacts from a Smart Home IoT Ecosystem

M A Hannan Bin Azhar and Samuel Benjamin Louis Bate
School of Engineering, Technology and Design
Canterbury Christ Church University
Canterbury, United Kingdom
Email: hannan.azhar@canterbury.ac.uk; sblbate@gmail.com

Abstract— **This paper reports an investigation into a modern smart-environment ecosystem comprising of multiple Internet of Things devices: Amazon Echo, Nest Indoor Camera and Philips Hue smart-bulb. As of yet, there is still little to no documentation, nor established methodology for the examination, acquisition and documentation of evidentiary artefacts from a smart-environment. Much of the research still remains individual to each device and does not incorporate the "melting pot" reality of most smart-environments. The methodology outlined in this paper was artefact-centric, and was purposely designed to facilitate the creation, discovery and documentation of network-native, cloud-native and device-native artefacts. Whilst not all aspects of the investigation were successful, a strong groundwork of documentation of the artefacts present on each of the smart-devices examined has been compiled, so as to inform and lay the foundations for future studies on this area of research.**

Keywords- Internet of Things Forensics; Internet of Things ecosystem forensics; Digital forensics; Smart Home; Internet of Things; Amazon Alexa; Nest Camera; Smart-Bulb.

I. INTRODUCTION

It has been forecasted that by 2022 smart-homes will number half a billion equating to 22.5% of households globally [1], with Internet connected devices numbering as many as 100 billion [2] by 2020. Increasingly these smart-devices have been used to automate our daily lives from scheduling of alarms that coincides with the level of lighting in the bedroom to become a hub for the social media or to order goods and services in a quick and convenient manner. However, with the ever-growing importance and reliance placed on these devices, the security and privacy concerns, widely reported [3][4] from these devices, cannot be ignored. Personal data, such as addresses, contact details and banking information are all stored in some manner by these devices, and can be recalled by the device at any given time to process a command contextually relevant to that information. The inherent weakness of these devices due to their lack of dedicated defense leaves them susceptible to outside unauthorised access by attackers, as seen by the rise of botnet Distributed Denial-of-Service (DDoS) attacks, most notably in the Mirai botnet, wherein devices were hijacked, enslaved and utilised to cause chaos and damage on a widespread scale [3]. Thus, criminals are targeting these devices to commit a new form of burglary, which necessitates the need for forensic investigation of home Internet of Things (IoT) devices with aim to recover potential wealth of evidence by the law enforcement agencies [4]. There are generally three areas of interest to a digital forensic investigator when examining a device for artefacts of evidentiary value, specifically how and when the device might have communicated or otherwise logged an event. These three categories of interest are communications or events specific to the device itself, known as device native artefacts; communications made across a shared network, known as network native artefacts and communications between the device and a service via the cloud, known as cloud-native artefacts [5]. Even though some authors reported extraction of artefacts from smart IoT devices [5][6][7], there is lack of research reporting investigation of a smart eco-system connecting a wide range of devices. Ecosystems created by a range of interconnected devices can be complex due to their heterogeneous nature [5]. The results presented in this paper will demonstrate retrieval and interpretation of numerous network, cloud native and device specific artefacts taken from a smart-environment consisting of a range of devices, specifically by including a smart bulb, Philips Hue smart-bulb [8], which was not explored before. Other IoT devices in the smart environment were Amazon Echo [9], a Nest Indoor Security Camera [10] and an Android smartphone [11].

The remainder of the paper will be organised as follows: Section 2 of this paper reviews existing work on forensic investigations of Smart IoT devices. A brief explanation on the methodology used will be discussed in Section 3. Results and analysis will be reported in Sections 4 and 5. Finally, Section 6 concludes the paper.

II. LITERATURE REVIEW

Apthorpe et al. [7] conducted their investigation upon a "melting pot" [12] smart-environment, utilising a Nest Camera, a Sense Sleep Monitor, and a WeMo Switch smart-plug. Their investigation was conducted from the perspective of a passive observer to a network, such as a system administrator or an Internet Service Provider (ISP). During the experiment, they found that using a packet sniffing software they were able to reliably obtain evidence of the presence and activity of these devices on the network, namely through communications between the devices and their respective companies' domains. They noted that the Sense Sleep Monitor, through its communications with those domains, left a tangible trail of artefacts that an observer to the system would easily be able to identify and subsequently discover the wearers activity [7]. Sleeping patterns were also able to be identified, such as times the wearer would go to bed and wake up in the morning, or during the night.

Chung et al. [5] were also able to identify cloud-native artefacts produced by the Amazon Echo during its usage due to its reliance on Internet services throughout its operation

 ISBN: 978-1-61208-743-6

which they could access through unofficial Application Programming Interfaces (APIs) [13]. Another online source, Piette [14], has extensively documented the APIs for the Amazon Echo, which are integral to the daily operation of the device and could potentially hold valuable evidence to a digital forensic investigation. It is possible to view a user's data that is stored in the cloud through these APIs, and each piece of user data is assigned as a "card" by Amazon for storage. Organisation of user data by Amazon means it is easy to search through these artefacts to locate user data, and discern the time and date of actions performed by the user, as well as the type of actions performed. However, these cards do not last usually more than a few days [14] and this severely limits their evidentiary potential as there is only a matter of hours for an investigator to discover them before the artefacts are lost forever.

As with Chung et al. [5], Dorai et al. [6] similarly were able to find client-native artefacts present in their investigation of a Nest device smart-environment with a focus on Internet Protocol (IP) enabled security cameras. A vast number of artefacts were retrieved that provided evidence of the Nest companion app having been used on a device. As reported by Dorai et al. [6], whilst artefacts of evidentiary value could be retrieved, the detection algorithm employed by the IP camera devices, unless fine-tuned by the owner, produces a great number of false-positives as well as false-negatives through either reporting events. As such, the artefacts produced by the operation of the device should be examined in conjunction with other sources of evidence where possible, so as to validate that neither a false-positive, nor false-negative, occurred. Ji et al. [15] corroborated these findings in their own investigation into IP cameras and in developing a tool named HomeSpy, and were able to monitor the network and cloud-native artefacts produced by such devices, proving that monitoring of these artefacts bears a great evidentiary value to the investigators.

III. METHODOLOGY

The study detailed in this paper analyses a smart environment consisting of an Amazon Echo [9], a Philips Hue smart-bulb [8], a Nest Indoor Security Camera [10] and an Android smartphone [11]. The Android Operating System (OS) was selected for its market dominance [16], representing a higher likelihood of its involvement in a crime-scene. The environment in which the testing took place was designed to emulate a smart-home ecosystem, with the devices all set-up and connected to a home network, as shown in Figure 1. At the center of the ecosystem was the router and hub that connected the devices across the network and Internet, either through Wi-Fi or a wired connection. The Philips Hue system uses a hub, so there is no direct communication between the smart phone and the smart light bulbs, as the commands to the bulb goes through the hub via the Zigbee protocol. As all the traffic was broadcasted over the network, by connecting an observation machine via a wired ethernet to the hub allows capturing and analysis of packets for the examination.

The smartphone was used within the environment, as a controller for the devices, to simulate a user's interaction within the smart-home. In addition to controlling the devices via the smartphone, If This Then That (IFTTT) [17] application was used to create interactions between smart-devices, known as 'recipes', in which an action on one triggers another. Using the mobile to control the devices, and the IFTTT to link their interactions with one another, evidentiary artefacts were created on the smartphones, the devices, the network and cloud with the aim to be retrieved and examined. As shown in Figure 1, listed beneath the Cloud, Android mobile and Laptop are the tools, utilities, applications and other possible locations where evidence might be produced during the experiment. Due to the nature of the experiment, a private network was used to limit the amount of unwanted traffic occurring across it, which would otherwise potentially obscure the examination of artefacts transmitted.

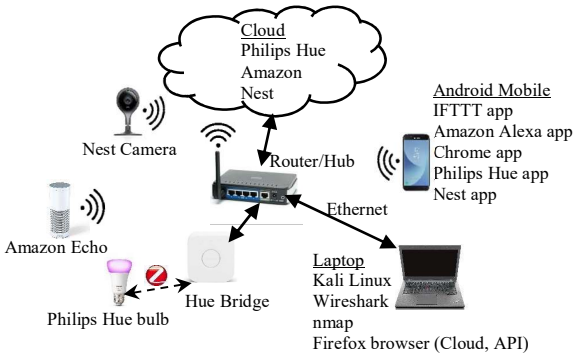

Figure 1. A Smart-Home ecosystem.

The examination of the devices was structured in several stages, each taking its own form and artefact-centric. The main objective of the investigation was not to apportion guilt for a crime committed within a smart-environment, but to provide an overview for what artefacts are generated by smart-devices during their daily usage. First and foremost was the passive observation of the devices whilst in use, as in Apthorpe et al. [7], to observe and record network-native artefacts, such as communications instigated by the devices to external services and IP addresses during their usage. This observation was conducted with the network traffic analysis software Wireshark [18] running on a laptop with Kali Linux [19], an OS used in forensic investigations, which comes with many useful utilities and tools pre-installed.

The next stage of the investigation was concerned with the discovery and documentation of cloud-based artefacts generated during the devices' usage. To investigate these artefacts, several methods were used. Firstly, unofficial APIs for the Amazon Echo [14] were used to allow access to the available data stored by the device in the cloud. Secondly, the user accounts of the smart-devices were accessed to investigate any cloud-native artefacts that might be discoverable through the user account portals of each of the device's respective websites.

The final stage of the investigation involved port-scanning of the devices used to see if any ports were open on them that might allow remote access to the onboard storage of the devices. For this, the 'nmap' utility (on Kali Linux) was used with the 'aggressive' flag, which offers a wider range of

 ISBN: 978-1-61208-743-6

information about the device in addition to the visible ports. The aggressive scan allowed the probing of OS detection (-O), version scanning (-sV), script scanning (-sC) and traceroute (--traceroute) on the devices in addition to any open ports that might be exploited to gain access to the devices. The ACPO good practice guidelines [20] state in the first and second principles that in the recovery of data of evidentiary value, the data should not be altered in any way, and if it is, this must be explained and justified. These principles also extend to the physical modification of a device to gain access to data upon it, such as removing an exterior casing from an Amazon Echo to access the on-board storage device, that was otherwise inaccessible. This paper's research strictly adhered to these principles, and as such, no physical modification of the evidence took place.

IV. Results of Network-native and Device Specific Artefacts

This section reports the artefacts discovered during the passive observation of the network and while using the port scanning to gain remote access to the devices. The results are presented for both network-native and device-specific artefacts.

A. Amazon Echo

Network-native artefacts were observed during the usage of the Amazon Echo device in the form of communications created by the device, directed to Internet Protocol version 4 (IPv4) addresses related to Amazon and official third-party advertisement organisations related to Amazon. Upon asking the Amazon Alexa "Alexa, what is the time?" a communication was observed with the Internet Protocol version 4 (IPv4) address "13.32.69.70" (Figure 2), which was identified as a UK based Amazon address using the 'whois' lookup tool included with Kali Linux's terminal. In addition to the UK address, contact was also made with a US address also associated with Amazon. As can be noted in Figure 2, IP addresses similar to "13.32.69.70" were communicated with during the operation; however, these are similarly registered to Amazon Technologies with a range of IP addresses having been reserved and registered for communications purposes.

No.	Time	Source	Destination	Protocol	Length	Info
28	8.000699319	Sagemcom_93:fa:54	Spanning-tree-(for-...	STP	60	Conf. Root = 6144
29	8.258183015	192.168.1.136	13.32.69.70	TLSv1.2	112	Application Data
30	8.258245334	192.168.1.136	13.32.65.90	TLSv1.2	112	Application Data
31	8.258312163	192.168.1.136	54.172.140.249	TLSv1.2	112	Application Data
32	8.258343202	192.168.1.136	13.32.65.90	TLSv1.2	112	Application Data
33	8.258391497	192.168.1.136	54.172.140.249	TLSv1.2	112	Application Data
34	8.266213385	13.32.69.70	192.168.1.136	TLSv1.2	112	Application Data
35	8.266273061	192.168.1.136	13.32.69.70	TCP	66	41166 → 443 [ACK]
36	8.266851925	13.32.65.90	192.168.1.136	TLSv1.2	112	Application Data
37	8.266886588	192.168.1.136	13.32.65.90	TCP	66	57698 → 443 [ACK]
38	8.270303936	13.32.65.90	192.168.1.136	TLSv1.2	112	Application Data

Figure 2. IPv4 address related to Amazon.

```
root@kali:~# nmap -A 192.168.1.127
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-03 10:26 UTC
Nmap scan report for amazon-65cc37160.lan (192.168.1.127)
Host is up (0.0078s latency).
All 1000 scanned ports on amazon-65cc37160.lan (192.168.1.127) are filtered (959) or closed (41)
MAC Address: CC:F7:35:6B:03:DF (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   7.79 ms amazon-65cc37160.lan (192.168.1.127)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.56 seconds
```

Figure 3. Port scan of the Amazon Alexa.

The aggressive port scanning of Amazon Alexa revealed that it was largely locked down (Figure 3). This is to be expected of Amazon Echo, which handles sensitive personal information, such as the user's full name and email address. Due to the closed ports, displayed during the scan in Figure 3, there were no access points to enter the device's on-board storage remotely.

B. Nest Indoor Security Camera

In order to create network-native artefacts from the Nest camera, live streaming of the camera's feed and its ability to play audio, recorded from the mobile controller's microphone, were used; however, no artefacts were visible across the network.

```
root@kali:~# nmap -A 192.168.1.126
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-03 10:19 UTC
Nmap scan report for udhcp-1-19-3-18-b4-30-69-65-31.lan (192.168.1.126)
Host is up (0.014s latency).
All 1000 scanned ports on udhcp-1-19-3-18-b4-30-69-65-31.lan (192.168.1.126) are closed
MAC Address: 18:B4:30:69:65:31 (Nest Labs)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   13.70 ms udhcp-1-19-3-18-b4-30-69-65-31.lan (192.168.1.126)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.85 seconds
```

Figure 4. Port scan of the Nest camera.

Aggressive scanning of the camera revealed that all 1000 scanned ports were closed, as shown in Figure 4. This indicates that the device received the querying packets sent during the scan and responded with a packet, indicating there was no service active or listening on that port [21]. As with the Amazon Echo, the lack of discovered open ports meant that there was no way to remotely access the device's on-board storage.

C. Philips Hue smart-bulbs and bridge

With regards to the Philips Hue smart-bulb, using the 'nmap' utility, the Philips Hue smart-bulb bridge was identified, as evidenced by Figure 5.

```
root@kali:~# nmap -A 192.168.1.123
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-03 10:22 UTC
Nmap scan report for Philips-hue.lan (192.168.1.123)
Host is up (0.00044s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE  VERSION
80/tcp   open  http     nginx
|_http-server-header: nginx
|_http-title: hue personal wireless lighting
443/tcp  open  ssl/http nginx
|_http-server-header: nginx
|_http-title: hue personal wireless lighting
| ssl-cert: Subject: commonName=001788fffe70c23e/organizationName=Philips Hue/countryName=NL
| Not valid before: 2017-01-01T00:00:00
|_Not valid after:  2038-01-01T00:00:00
8080/tcp open  http     Web-Based Enterprise Management CIM serverOpenPegasus WBEM httpd
|_http-title: Site doesn't have a title.
MAC Address: 00:17:88:70:C2:3E (Philips Lighting BV)
Device type: specialized
Running: Philips embedded, Linux
OS CPE: cpe:/o:linux:linux_kernel
OS details: Philips Hue Bridge 2.0 (Linux)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.44 ms Philips-hue.lan (192.168.1.123)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 116.18 seconds
```

Figure 5. Port scan of Philips Hue smart-bulb bridge.

The aggressive scanning revealed that the Philips Hue smart-bulb bridge had three open ports, these ports were for "http" and "ssl/http" services. Moreover device-native artefacts were present in the scan of the Philips Hue smart-bulb bridge in Figure 5, specifically in the form of details of the Linux-based OS, Philips Hue Bridge 2.0, the device was

operating on. The webserver listening on the port 80 of the bridge carry an inherently weak form of security due to the way it allows user to control the bulbs [22]. Given that a malware or an attacker can see the history of devices previously connected to the local area network using the 'arp' command, access to the bulb can be easily gained through the hashing of a whitelisted Media Access Control (MAC) address.

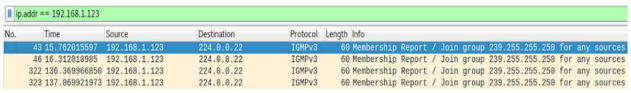

Figure 6. Wireshark observation of smart-bulb bridge.

Controlling the device using the Philips Hue smart-phone application, the bulbs were turned on and off several times in an attempt to simulate an attack of hacking and controlling of the smart bulbs, causing them to flash. It was observed via the Wireshark's report, as shown in Figure 6, that the device left traces of the activity on the network by making several "Membership Report/Join group" requests during the event. The significance of these artefacts would be that to an investigator, midway through such an attack there would be clear evidence of its occurrence upon the network.

D. Artefacts from Multiple Devices

IFTTT was used in the experiment to connect multiple devices to observe how they interact with one another on a network level. The application allows users to make 'recipes', which are essentially if/then statements. In the case of the experiment, the setup was that when the Amazon Echo's timer ended, the Philips Hue smart-bulbs would flash on and off.

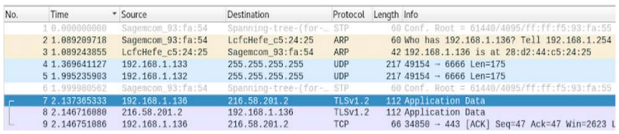

Figure 7. Wireshark observation of IFTTT ecosystem.

Figure 7 shows a Wireshark observation of the Echo's timer reaching zero, triggering the Philips Hue smart-bulbs to flash on and off. As can be seen in the final three events, application data is detected originating from the Philips Hue smart-bulb bridge, which contacts the IP address "216.58.201.2". A simple 'whois' lookup of this IP reveals this to be a Google registered IP address.

With regards to the network-native artefacts, it is worth noting that the Amazon Echo proved to be the 'loudest' device on the network, generating a mass of network-native artefacts, while communicating not only with servers owned by Amazon but with the third-parties for the purpose of advertisement. It appeared that a single command invoked on the Amazon Echo generated more traffic and network-native artefacts than that of when the rest of the devices were put together.

V. Results of Cloud-Native Artefacts

This section reports the artefacts discovered in the cloud storage generated by each device while they were used in the smart environment. Results are categorised by each device type.

A. Amazon Echo

There were many recorded examples of cloud-native artefacts created in the usage of the Amazon Alexa device, of which seven separate categories of artefacts could be observed. The artefact categories were as follows: customer status, authentication, bluetooth, music account details, provider capabilities, third party consent and devices listed to the Amazon account. It primarily concerns the initial setup of the user's Amazon Account with that device with flags, such as "countryOfResidenceSet", "eulaAcceptance" and "preferredMarketplaceSet".


```
{"authenticated":true,"canAccessPrimeMusicContent":false,
,"customerEmail":"sb1082forensic@gmail.com","customerId":
 "A1UPCFISGWVC05","customerName":"sb1082 forensic"}
```


Figure 8. Alexa Authentication Artefact.

Figure 8 displays the Authentication artefact. This artefact seems to concern whether or not the user's account is authenticated ("authenticated:true"), presumably via a confirmation email following sign-up as well as other information specific to the user's account, such as their email address, name and Amazon ID. Additionally, the status of the user is also listed (whether or not they have Amazon Prime membership) labelled as "canAccessPrimeMusicContent".


```
forensic","primeStatus":false,"service":"AUDIBLE"}
[{"associated":true,"customerId":"A1UPCFISGWVC05",
  "email":"sb1082forensic@gmail.com",
  "firstName":"sb1082 forensic"
 "primeStatus":false,"service":"CLOUD_PLAYER"}]
 forensic","primeStatus":false,"service":"TUNE_IN"}]
```


Figure 9. Alexa Music account detail.

Figure 9 displays some of the artefacts from the registered account's music details. Information, such as the customer's identity, personal information and their prime membership status can be seen identified here. Moreover, associated services that can be accessed such as "AUDIBLE", "CLOUD_PLAYER", and "TUNE_IN" are listed here. Amongst other artefacts recovered were Alexa's Bluetooth, Provider Capabilities and Device artefacts. This concerns the Bluetooth connectivity of the Amazon Echo, and details the device's serial number and the software version operating on the device. Provider Capabilities detail what control applications, such as "AUDIBLE" can have over the Alexa device, such as "bookmarkSong" as well as the capability to use the search functions ("canSearchForStationByArtist") on the device. Device artefact lists the Alexa device associated with a user's Amazon account and contains information regarding the name of the device (""accountName"") as well as services that might be run from the device including "TIMERS_AND_ALARMS", "VOLUME_SETTING" and "VOICE_TRAINING".

 ISBN: 978-1-61208-743-6

B. *Nest Indoor Security Camera*

Numerous cloud-native artefacts were observed during the experimentation period due to Nest's reliance on an always-online connection to the Internet to allow the device to communicate with the Nest's servers. Cloud-native artefacts for Nest Camera consisted of hours of raw video footage saved to the cloud storage, which is viewable both through the Nest companion application and website. In addition to the raw hours of footage from the camera, the device also flags when movement is detected within the frame and is able to recognise when a person enters the frame and bookmarks that footage (as 'Events') for viewing at a later time.

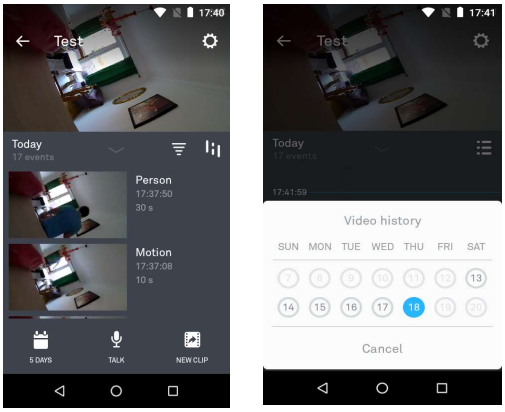

Figure 10. Nest Application on Android.

Figure 10 is a screenshot of the Nest application on Android, viewing the cloud-native 'events' artefacts. As can be seen, the service is able to distinguish between motion and people within a scene, which it stores for review by the owner. It also shows the wider number of cloud-native artefacts available to be viewed, which are raw footage recordings from previous days. It was also found that with the Nest Aware membership, up to 30 days of raw footage recorded from the user's Nest device can be saved to Nest's servers for viewing at a later time.

C. *Philips Hue smart-bulb*

Interestingly, it appears that the Philips Hue smart-bulb and its associated bridge remain permanently linked to any previous accounts and applications authorised upon them, by any previous owner. Therefore, the new owner of the bulb would have access to personal information, such as names and email addresses of the previous owner. These artefacts can be accessed by any account associated with the bridge, as evidenced by the screen-capture in Figure 11, where a previous owner's name and email address have been blackened out. Similarly, trace of one of the author's personal email address, sblbate@gmail.com, was also found, as it was used in a prior installation of the Hue Bridge.

Retrieval of personal data associated with previous owners would constitute a data breach under the General Data Protection Regulation (GDPR), as both names and email addresses are deemed personal data according to the GDPR guidelines [23]. Even though, finding a suspect's details, as a possible previous user of the device, can be of great interest to an investigator, it should be noted that removing an associated account with the bridge is relatively simple task; as such, anti-forensics measures could be employed by a suspect by deleting their account or unlinking their account from the bridge.

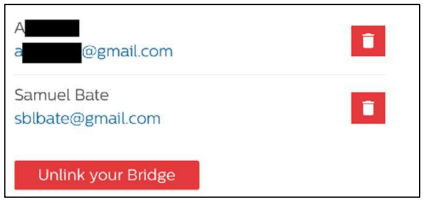

Figure 11. Philips Hue's Other users Artefacts.

Product ID	hb70c23eacb1b45a	Ethernet MAC Addr..	00:17:88:70:c2:3e
Model	BSB002	Internal IP Address	192.168.1.123
Firmware version	1931140050	Netmask	255.255.255.0
ID	001788fffe70c23e	Gateway	192.168.1.254

Figure 12. Philips Device specific artefacts on Cloud.

Figure 12 demonstrates example artefacts unique to the Philips Hue Bridge device captured from the Philips Hue website. In this case, it is possible to view the device's MAC address, its firmware version and unique identity. In addition to this, it is also possible to view the IP address and Gateway currently associated with the bridge. Further investigation on artefacts revealed that naming of the application "hue_ios_app#A**********'s iPhone" demonstrate that the application includes the host device's name set by the user, which can provide further evidence of which device the application was used on.

VI. CONCLUSIONS AND FUTURE WORK

This paper reports a large number of artefacts from various devices, especially by using a smart bulb in the ecosystem, with the IFTTT application used in the experiment to connect multiple devices to observe how they interact with one another. Even though the recovery of the device-native artefacts were limited due to the closure of any port for the remote access, numerous artefacts were discovered and documented on a network and cloud level; which includes personal details, logged video footage, and details of previous owners. These artefacts, when applied to a real-world investigation, have significant importance to identifying the implied ownership of the devices through personal information tied to these devices and stored on cloud servers. It is interesting to note that they all contain a great degree of personal information that would provide strong evidence to an investigator seeking to prove the identity of the owner. In the case of the Amazon Echo, its extensive documentation of a wide range of personal information was documented, e.g. email addresses, full names and agreements made including End User License Agreements (EULAs), authorisations for third-party music and streaming services, etc.

Nest (like Amazon) had a wealth of cloud-native artefacts available for viewing to an investigator. Though, where it did

 ISBN: 978-1-61208-743-6

not have much in the way of addresses and names, it did offer up to five days of recorded footage. This footage came complete with periods of interest, automatically flagged up for quick and convenient viewing, further categorised into alerts caused by a person in the frame and identified motion.

The Philips Hue smart-bulb and bridge continued the trend of storing large swathes of personal data in its cloud-native artefacts, tying accounts used in the past to the Philips Hue bridge and, in a sense, merging them together. As covered in the literature review, IoT devices typically are lacking when it comes to security, and the Philips Hue bridge seems to be no exception to this. It not only stores personal information but collates multiple users of a unique device into one shared hub, in which any user can view the information of others.

Whilst there was not a specific focus upon testing anti-forensics measures, anti-forensics must form a core component of any future research, building upon the foundation that this study provides. Moreover, to broaden the scope of the study, a wider range of mobile platforms including iOS should be explored to see what client-native artefacts can be recovered from Apple's Operating System and hardware, and to compare the differences, if any, between Android and iOS. Furthermore, future research should endeavour to develop an IoT specific forensic tool, so that majority of the investigation in this paper can be automated, enabling quicker retrieval of artefacts from the smart home ecosystem.

REFERENCES

[1] R. De Renesse, *Smart Home Devices Forecast Report: 2017-22 | Ovum Link, Ovum.informa.com*. [Online]. Available from: https://ovum.informa.com/resources/product-content/smart-home-devices-forecast-report-201722 (Accessed: 7-Aug-2019)

[2] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context Aware Computing for The Internet of Things: A Survey", IEEE Communications Surveys & Tutorials, vol. 16(1), pp. 414-454, 2014, doi: 10.1109/surv.2013.042313.00197.

[3] Z. Whittaker, *Mirai botnet attackers are trying to knock an entire country offline*, *ZDNet*. [Online]. Available from: https://www.zdnet.com/article/mirai-botnet-attack-briefly-knocked-an-entire-country-offline/ (Accessed: 7-Aug-2019).

[4] E. Casey, "Smart home forensics", Digital Investigation, vol. 13, pp. A1-A2, 2015, doi: 10.1016/j.diin.2015.05.017.

[5] H. Chung, J. Park, and S. Lee, "Digital forensic approaches for Amazon Alexa ecosystem", Digital Investigation, vol. 22, pp. 15-25, 2017, doi: 10.1016/j.diin.2017.06.010.

[6] 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 Proc. of the 13th Int. Conf. on Availability, Reliability and Security, USA, Article 49, 10 pages, 2018, doi: https://doi.org/10.1145/3230833.3232814.

[7] N. Apthorpe, D. Reisman, and N. Feamster, "A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic", 2017, doi: arXiv:1705.06805.

[8] Philips Hue, *Hue White ambiance Starter kit E27*, [Online]. Available from: https://www.philips.co.uk/c-p/8718696728925/hue-white-ambiance-starter-kit-e27/specifications (Accessed: 7-Aug-2019).

[9] Amazon Echo, *Echo Plus (1st Gen) – With built-in smart home hub (White)*, [Online]. Available from: https://www.amazon.co.uk/Echo-Plus-With-Built-In-Smart-Home-Hub-Black/dp/B01J4IYBI0?th=1 (Accessed: 7-Aug-2019).

[10] Google Nest, *Google Nest Cam Indoor*. [Online]. Available from: https://store.google.com/gb/product/nest_cam_specs (Accessed: 7-Aug-2019).

[11] Android Phone, *Samsung Galaxy J3 (2016)*. [Online]. Available from: https://deviceguides.vodafone.co.uk/samsung/galaxy-j3-2016-android-5-1-1/specifications/ (Accessed: 7-Aug-2019).

[12] I. Vujačić, I. Ognjanović, and R. Šendelj, "SM@RT Home Personal Security and Digital Forensic Issues", The Eight Int. Conf. on Business Information Security, Serbia, October 2016.

[13] Analytic Physics, *Accessing Amazon Echo Data with JavaScript*, [Online]. Available from: http://analyticphysics.com/Diversions/Accessing%20Amazon%20Echo%20Data%20with%20JavaScript.htm (Accessed: 7-Aug-2019).

[14] O. Piette, *The Amazon Echo API,* [Online]. Available from: https://www.piettes.com/the-amazon-echo-api/ (Accessed: 7-Aug-2019).

[15] X. Ji, Y. Cheng, W. Xu and X. Zhou, "User Presence Inference via Encrypted Traffic of Wireless Camera in Smart Homes", Security and Communication Networks, pp. 1-10. 2018, doi: 10.1155/2018/3980371.

[16] Device Atlas, *Android v iOS market share 2019*, [Online]. Available from: https://deviceatlas.com/blog/android-v-ios-market-share (Accessed: 7-Aug-2019)

[17] IFTTT App, [Online]. Available from: https://ifttt.com/ (Accessed: 7-Aug-2019).

[18] Wireshark Website, [Online]. Available from: https://www.wireshark.org/ (Accessed: 7-Aug-2019).

[19] Kali Linux, [Online]. Available from: https://www.kali.org (Accessed: 7-Aug-2019)

[20] ACPO, *ACPO Good Practice Guide for Digital Evidence*, [Online]. Available from: https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf (Accessed: 7-Aug-2019)

[21] J. Williams, *Port Scanning 101: What It Is, What It Does, Why Hackers Love It, And Why You Will Too,* [Online]. Available from: https://blog.ipswitch.com/port-scanning-101-what-it-is-what-it-does (Accessed: 7-Aug-2019)

[22] N. Dhanjani, *Hacking Lightbulbs: Security evaluations of the Philips Hue Personal Wireless lighting system,* [Online]. Available from: https://www.dhanjani.com/docs/Hacking%20Lighbulbs%20Hue%20Dhanjani%202013.pdf (Accessed: 7-Aug-2019)

[23] GDPR, *GDPR Regulation,* [Online]. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (Accessed: 7-Aug-2019)

 ISBN: 978-1-61208-743-6