DFRWS

Welcome pwn: Almond smart home hub forensics

a.* removed for peer review

a

b

c

d

Abstract

Many home interactive sensors and networked devices are being branded as “Internet of Things” or IoT devices. Such disparate gadgets often have little in common other than that they all communicate using similar protocols. The emergence of devices known as “smart home hubs” allow for such hardware to be controlled by non-technical users providing inexpensive home security and other home automation functions. To the cyber analyst, these smart environments can be a boon to digital forensics; information such as interactions with the devices, sensors registering motion, temperature or moisture levels in different rooms all tend to be collected in one location rather than into separate locations. This paper presents the research work conducted on one such smart home hub environment, the Securifi Almond+, and provides guidance for forensic data acquisition and analysis of artefacts pertaining to user interaction across the hub, the iPhone/Android companion app and the local & Cloud web interfaces.

Keywords: Internet of things; extraction; smart sensor; smart home hub; iOS; android; cloud;

1. Introduction

The rapid expansion of internet enabled devices has lead to the realization of the “Internet of Things” (IoT) as first mentioned by Kevin Ashton in 1999 (Ashton, 2009). These devices have expanded the interaction between humans and technology, but also increased the risk and impact of possible vulnerabilities in devices or their implementation. IoT devices are advancing at a considerable rate. Currently there is estimated to be more than 6.4 billion IoT devices connected, and the number is expected to reach a total of 8.4 billion connected IoT devices in 2017 (Gartner, 2017), other estimates suggest this rising to 30.7 billion devices in 2020 and estimated to increase to 75.4 billion in 2025 (Columbus, 2016). The volume and variety of IoT devices presents a challenge to the digital forensics examiner. One particular market for IoT devices in is developing the ‘Smart Home’ as evidenced in the USA where the real estate market is adapting a “Smart Home” policy and is trying to sell more and more houses that have IoT devices installed (Paxton, 2017). Smart homes use a variety of devices, integrated to provide intelligent features, enabling security, automation and energy conservation.

The degree of human interaction with these systems suggests that they have the potential to provide a significant amount of information to a digital forensics investigation. Currently there is limited information available offering forensic investigators an insight into what information of interest is stored on the vast range of devices, or how to acquire data in a forensically sound fashion. This paper seeks to provide a greater insight into the types of information available in-Home Automation Smart Hubs that may be of value to law enforcement agencies in those territories where these devices are available.

The rest of this paper is organised as follows. Related work describes similar forensic examinations on other smart hub devices, Almond ecosystem presents our experiment configuration and introduces features of the device, forensic challenges identifies issues faced during the course of investigation, investigative methodology describes the process taken to identify artefacts, data extraction details how an investigator may extract artefacts from devices in the

* Corresponding author. Tel.: +0-000-000-0000; fax: +0-000-000-0000.
E-mail address: removed@removed.rem.

Almond environment, artefacts of forensic importance identify locations where evidence of note may be found, recommendations for the forensic examiner provides a summary of data extraction and analysis, and conclusions and future work provides a summary of the research presented in this paper and thoughts for continuing examination.

2. Related Work

There are a number of challenges presented by IoT devices in terms of extracting, accessing, interpreting and verifying the data. This is because devices have widely varying functionality, often a customised operating system and may use one or more, of a number wireless network transmission protocols. This is now a significant area of research with effort focused on the analysis and data acquisition from popular IoT devices (e.g. Meffert et al, 2017 and Oriwoh et al, 2013). The complexity, variety and distribution of IoT devices, which are by their nature part of the infrastructure, may cause significant problems. As a digital forensic analyst getting access to the systems can be a separate challenge altogether. However, in many cases, it may be unnecessary to access the actual IoT device as this may hold very limited information. What may prove to be of more forensic value would be any system used to integrate IoT or similar devices to provide control (Sutherland 2015). Typically, domestic systems are connected via some form of hub or centralised service to facilitate a 'Smart Home'. The integration of these devices has already raised security concerns (Plachkinova, Vo, Alluhaidan, 2016). Generally, the forensic analysis of Smart Hubs has been limited. The following section describes work carried out to date on three such systems; Amazon Alexa, Apple HomeKit and Google OnHub\Google Home.

2.1. Amazon Alexa

The Amazon Alexa system is a combination of specific hardware (Echo and Echo Dot) and the cloud based Alexa personal assistant. The considerable popularity of the Amazon Alexa System has led to some community efforts exploring the analysis of the device including the hardware (The Unofficial Amazon Echo User Forum, 2016). An analysis by the Leahy Center for Digital Investigation in 2016 provided some insight regarding performing a forensic analysis on the Amazon Alexa, via third party devices. This report explains techniques for data collection and data extraction. The greatest challenge they encountered was third-party device integration with

Figure 1: Top - Almond+ touchscreen, Right - iPhone app, Bottom - Cloud web interface

the Echo. The data collection using such devices and their companion applications was found to be generating possible discrepancies in the data. Chung et al. (2017), considered the Alexa ecosystem and proposed a possible toolkit to support forensic analysis. The toolkit "*tries to acquire (download) cloud-native artifacts from the server using the unofficial APIs…*". A challenge experienced by the authors in the past is unofficial APIs are subject to change without warning which could then require re-engineering of code, that is if the functionality is still available. Hyde and Moran (2017) describe both destructive and non-destructive methods of accessing the Amazon hardware to extract evidence.

2.2. Apple HomeKit

The Apple system uses the iCloud keychain to retain information on devices and other information. The Apple system requires an Apple iOS device or Apple TV to remain in the home to act as a hub for external access (Apple, 2017a). Apple are releasing the HomePod in December 2017. The Homepod appears to be limited in capacity acting only as a speaker (Apple, 2017b). The Apple system is likely to pose a problem for in depth investigations due to the way that it is structured.

2.3. Google OnHub and Google Home

Google Home provides a similar service to that of Alexa with access to various Google services and Google assistant. It is capable of running on either the Android or Apple iOS Operating Systems. Launched in 2017 it can interface with a number of IoT devices,

there is however very limited information on forensic best practice with this system. Another possible device the investigator might encounter is the Google OnHub which takes a different approach than that adopted by Amazon, as rather than an additional device, the OnHub is intended to replace the home router with one system that can interface with Smart / IoT devices.

3. Almond ecosystem

The Almond+ is a smart home hub that integrates the functionality of a router with the ability to control and respond to IoT sensors and devices. It has the ability to work with or without Internet connectivity (Securifi, 2017). It is more akin to devices such as Google's OnHub than Amazon's Echo in that it is designed to replace an existing router. The device also provides the facility to be setup as a repeater or an access point. The Almond+ supports two protocols, namely Zigbee (Zigbee Alliance 2017) and z-Wave (Z-Wave Alliance 2017) and has the ability to work with or without Internet connectivity (Securifi, 2017).

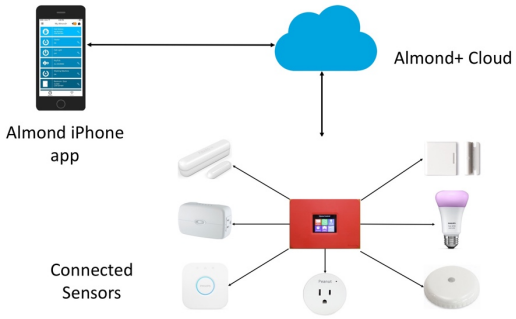

Figure 2: Almond+ Environment Setup

The following sensors were connected to the Almond+ for the experiment (Figure 2):

1. Three Philips Hue Lamps via a Philips Hue Bridge - changes colour, dimming, on/off
2. Jasco Dimmer Plug, 3-pronged dimmer device
3. Securifi Peanut Plug, on/off power device
4. Fibaro Door/Temperature Sensor, two-components
5. NYCE Motion/Temperature/Humidity Sensor, positioned on ceiling
6. Two NYCE Door Sensors, alternative device to Fibaro

There are four ways for a user to interact with the Almond ecosystem, via the hardware itself, a companion app on iOS or Android, and through Cloud or local web interfaces.

3.1. Via the touchscreen

The Almond+ provides an interactive touch screen to the user (Figure 1). The interface on the Almond+ provides a myriad of information to the user like: settings, adding and controlling sensors, weather, list of users, firewall, security and sharing features.

3.2. Via the companion app

The smart app for the Almond+ is available for iOS and Android (Figure 1). The app provides a lot more information than the web interface and is able to connect locally (LAN) or via cloud to the Almond+ router. In local mode, the environment does not need Internet connectivity to work. The cloud connectivity feature provides the user facility to monitor and control the smart sensors connected to the Almond+ remotely. The cloud connectivity also provides the history for the sensor activity. It sends a notification when a sensor is triggered and its current state. It also maintains a log of the sensors activity in the app. We found no perceivable difference between the companion app for iOS and Android.

3.3. Via the Cloud web interface

The web interface appears to not be as complete as the Almond+ touchscreen software or companion apps. This provides a view of the current status of sensors and which network devices have connected (Figure 1).

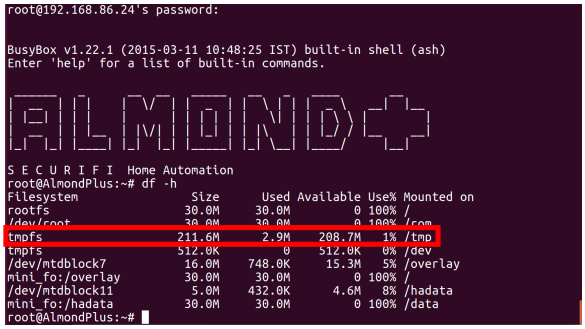

Figure 3: Default mount points - /tmp contains valuable data but resides in RAM

3.4. Via the local web interface

The hub provides a local web-based interface which may be accessed by visiting the IP address on the local network (in our setup this was achieved by

visiting http://10.10.10.254). It is similar in look and feel to the Cloud web interface but is only accessible on the local connection.

4. Forensic challenges

During the course of the research, a number of barriers to successfully examine forensically the system were identified. No discernable removable media could be found in any of the hardware in the sample environment, neither in the IoT devices themselves nor in the smart hub. The Almond+ contains 512MB of RAM and flash memory. The flash memory tends to be used for core operating system files; a temporary filesystem stored in volatile memory contains sensor data. It is of critical importance to note that, if the smart hub is rebooted or powered off, valuable digital evidence will be irretrievably lost. As may be seen in Figure 3, almost half of the available RAM is dedicated to `/tmp` which contains a considerable number of artefacts (211.6M of 512M total).

A popular mechanism for accessing remote systems is SSH, which is enabled by default on the cabled LAN connections only; user configuration is required to enable it over Wi-Fi (Lars, 2014). The SSH server is provided by Dropbear v0.52, released in 2008 (Johnson, 2017). When connected to via a modern SSH client, the client responds that it is unable to negotiate a secure connection with the host; no matching key-exchange methods are found. Dropbear offers diffie-hellman-group1-sha1 which requires forcing legacy options to connect, guidance is available in OpenSSH (2017).

Some devices can be controlled by multiple smart systems. With an Amazon Echo device connected to the sample environment the authors were able to control the Hue lightbulbs with voice commands. Even though the Hue bridge was connected as a smart device to the Almond+, any changes made with the Echo did not result in any artefacts being generated on the Smart home hub. Only changes made either directly on the Almond+ or via the companion app whilst in Cloud connectivity mode resulted in observational evidence on the device. The companion app in local mode provided current status and interaction, but no update to the logs. The companion smartphone app activity can be found on the Almond+ in the `CloudDaemon.log` file which maintains the records for the commands sent via the app. The work by Chung et al. (2012), should be referenced if an Amazon Echo is found in the target environment.

Unfortunately for the forensic investigator, it has become more difficult to obtain files from Apple devices in recent iOS versions with fewer files from applications being included in iTunes backups for offline analysis. The iTunes sync functionality is so important to iOS forensics, even a clean install of Cellebrite Physical Analyzer v.6.3.2 states that iTunes must be installed for extraction from certain iOS devices. The reader is urged to reference the summary of iOS8-11 in Afonin (2017). Significant files from the companion app are not readily accessible; analysts may need to either manually hand-scroll through information on the app itself or risk jailbreaking the device to obtain the data.

5. Investigative methodology

Post Almond+ setup, the smart devices were added in a sequential manner. Every sensor was individually connected to the Almond+ to see what changes were being made in the log files. After examining the modifications made by a sensor the device was removed from the Almond+ and the router was setup for the next sensor. This allowed us to identify generic logs which stored all actions, and specific logs unique to certain devices.

After recording the readings for every sensor individually the Almond+ was reset and all the sensors were connected to it. Then the logs were monitored to see what was being recorded on the Almond+ when the sensors were interacted with via the on-screen interface, the smart app and the Cloud/web interface. The logs were cross referenced to observe how, if any, changes occurred and to determine the results of the user's actions.

NIST (2014) (Guidelines on mobile device forensics) were referenced before attempting the following course of action. We assessed the implications of performing a Pangu jailbreak (Pangu, 2016) on an iPhone 5s running iOS 9.3.2. Comparisons were made between data extracted from 1) a backup made using iTunes first a non-jailbroken device, 2) a backup made using iTunes with a jailbroken device and 3) manual extraction using Cydia file browsing apps. We found there wasn't a difference in the quality of the extraction between 1. and 2., but 3. provided additional files of importance. As we had the ability to jailbreak and were able to confirm that Pangu on an iPhone 5s running 9.3.2 did not alter the companion app files, we chose to proceed with this method to obtain more data. Other jailbreak

tools should be assessed in a similar function to confirm the implications of the jailbreak process upon the quality of the extraction.

6. Data extraction

There are stark differences between extraction methods for devices in the Almond ecosystem, each is discussed in turn below.

6.1. Almond+ smart home hub

According to Securifi, 2014, default SSH access is only available via LAN. At the time of writing, the latest firmware is `AP2-R090-L009-W016-ZW016-ZB005`. We have found that whether SSH is enabled or disabled in the interface, SSH continues to be accessible via Wi-Fi. Enabling the repeater mode functionality greyed out all the WAN access settings, but SSH via WIFI continued to work. The only way we have been able to remove SSH access was to connect via SSH and kill the SSH process manually.

Given the issues mentioned in section forensic challenges regarding the version of the SSH server (dropbear), we had to use the following command to log into the hub with a default username and password of root/root:

```
ssh -oKexAlgorithms=+diffie-
    hellman-group1-sha1 root@<IP>
```

After gaining access to the file system we proceeded with an empirical investigation of the filesystem for artefacts that would be of use to an investigation. This process led to identifying `/tmp` as containing most files of significance.

The Almond+ supports USB 3.0. We used a USB drive formatted appropriately to transfer files. The bitstream and resulting captures were hashed using the built-in "`md5sum`" to ensure standard forensic practice was followed. The following command was used to make the capture:

```
tar -czvf - /tmp/ | tee
/mnt/usb/usb_name/time_date.tar.gz md5sum >
/mnt/usb/usb_name/time_date.ar.gz.md5
```

Furthermore, it is possible to forensically image the raw devices in a similar fashion. Using the following command, we were able to pull the flash memory directly via ssh and create hashes of the bitstream and resulting image file.

```
ssh root@192.168.86.24
"dd if=/dev/mtdblock7" | tee mtdblock7.dd |
md5sum > mtdblock7.dd.md5
```

Given the system is active, imaging the flash memory twice will likely result in different hashes. Therefore, the importance of hashing the bitstream and the resulting image simultaneously is of paramount importance. If the md5 of the dd image and the text file match, the image has been created correctly.

We identified 14 separate mtdblock devices on the Almond+ and used the Linux tool `file` to attempt identification. A summary of these may be seen in Table 1.

Table 1. mtdblock datatypes reported by "`file`"

mtdblock #	Linux `file` command output
0,2,3,10,12,13	data
1	DOS executable (COM)
4,6	squashfs filesystem, little endian, version 4.0
5	u-boot legacy uImage, Linux-2.6.36, Linux/ARM, OS Kernel Image (Not compressed)
7,9	Linux jffs2 filesystem data little endian
8,11	ISO-8859 text, with very long lines, with no line terminators

Attempts to extract or mount the mtdblock images were not particularly successful; typically, this generated the following error "`jffs2: compression type 0x08 not available`". It is possible that the vendor used a non-standard compression algorithm, LZARI (type 0x08), as a way to discourage hackers from interfering with the equipment. We went as far as recompiling the Linux kernel on our Ubuntu workstation to enable all JFFS2 related options, but still received the same errors.

6.2. iPhone companion app

As previously mentioned in the section 'Challenges to the Investigator', obtaining raw files from iDevices is becoming progressively difficult with each iOS iteration. The process of hand-scrolling with suitable video recording equipment, albeit tedious, will extract the same useful information as can be seen in the raw files obtained via the jailbreaking method.

The tools iFile and Filza were used on an iPhone 5s jailbroken with Pangu (2016) on iOS 9.3.2 to locate and extract the Almond+ companion app data for further analysis. Filza conveniently provides the human-readable names of apps located in the iPhone.

Table 2: Summary of forensically important locations

Source	Location	Significance
Securifi Almond+	`/tmp/connected_home.log`	Entries created when smart devices are used on Almond+
Securifi Almond+	`/tmp/association.log`	Identified when smart device is added to hub
Securifi Almond+	`/tmp/CloudDaemon.log`	Detailed log of data sent/received from Cloud
Securifi Almond+	`/tmp/autoip.json`	Almond+ geographical information and weather data
iPhone App	`<root>/Documents/toolkit_deviclogs.db`	Record of all network devices (dis)associating with Almond+
iPhone App	`<root>/Documents/toolkit_notifications.db`	Record of all smart devices which have alerts explicitly set
iPhone App	`<root>/Library/Caches/Snapshots/com.securifi.almond/*@2x.png`	Screenshot of most recent user-interaction in app
Cloud/web	`connect.securifi.com`	Current Wi-Fi settings, list of all networked devices (highlights connected), firmware version

`/private/var/mobile/Containers/Data/Application`
Once the Almond folder is located, it may be compressed and transferred to a workstation for analysis of the SQLite files. All such files analysed using DB Browser for SQLite v.3.10.1 (DBBrowser, 2017).

6.3. Web interfaces – Cloud and local

The Cloud web interface for the Almond+ may be accessed at `connect.securifi.com`. An analyst may take screenshots or save the webpage to disk to extract information.

It is not recommended to interact with the local web interface, as can be seen in section Artefacts of forensic importance, mere browsing can cause updates to several files of evidential significance.

7. Artefacts of forensic importance

Across the Almond environment, several areas can provide evidence of value to the forensic investigator. Depending on the interface, varying levels of detail may be obtained.

Table 2 summarises important locations found across the Almond+ and its companion applications.

7.1. Residing on the Almond+

After performing an extraction as detailed in the data extraction section of this paper, the following files were identified as containing artefacts of forensic significance.

`/tmp/connected_home.log` – Entries are generated when a user interacts with the smart devices located within the "Connected Sensors" section of the Almond+ touchscreen interface. Interactions with the companion app or Cloud do not appear in this log. Connected sensors are identified using numerical values (Appendix A) that are assigned by the Almond+. In order to identify which sensor is associated with which device, the examiner will need to cross-reference the value with the "association" log file. The sample in Appendix A shows the commands executed for the Peanut Plug smart switch.

`/tmp/association.log` - This file keeps records of when a smart device is added to the hub. Each entry begins with a line indicating "`association Started`" proceeded by further detail about the protocol (zigbee or z-Wave), the manufacturer, and the assigned numerical value for the device. As can be seen in the Appendix A, the Peanut Plug "`sensor got Associated 5` [sic]".

`/tmp/CloudDaemon.log` – Provides a detailed history of data being sent to Cloud storage. All actions may be categorised by their `CommandType`, which appears as both XML and JSON entries. The following types were identified as being of particular interest:

`24` and `25` - Contain Wi-Fi SSID and password in plaintext
`DynamicDeviceList` - Smart devices and sensor values
`DynamicSceneList` - Scenes assigned to smart devices
`DynamicClientList` - Network devices, whether or not active
`DynamicIndexUpdated` - Smart device state changes
`RouterSummary` - Router settings, uptime, SSID, IP
`GetWirelessSettings` - SSID, mode, channel, encryption type, location
`AlmondProperties` – Centigrade usage, URL, preferred Internet check URL

`/tmp/autoip.json` – Contains geographical information about the Almond+ and the local weather summary. Information obtained via geographical lookup of IP address therefore VPN usage may provide weather patterns from different physical locations. Available information includes: timezone,

	id	external_id	mac	users	date_bucket	time	data	deviceid	devicename	devicetype	value_index	value_indexname	indexvalue	viewed	notiCat
		Filter	Filter		Filter	Filter		Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1	50faf990-9510...	251176217062072		1504843200.0	1504928296.8...		26	Microsoft lpcl26Microsoft just Left Almond-aab8	500	0	NULL	Microsoft just Left Almond-aab8	1	0
2	2	15f1b970-94c...	251176217062072		1504843200.0	1504897703.5...		26	Microsoft lpcl26Microsoft rejoined Almond-aab8	500	0	NULL	Microsoft rejoined Almond-aab8	1	0
3	3	4f6d0970-940...	251176217062072		1504756800.0	1504814048.1...		26	Microsoft lpcl26Microsoft just Left Almond-aab8	500	0	NULL	Microsoft just Left Almond-aab8	1	0
4	4	08ecb7c0-93e...	251176217062072		1504756800.0	1504798897.4...		26	Microsoft lpcl26Microsoft rejoined Almond-aab8	500	0	NULL	Microsoft rejoined Almond-aab8	1	0
5	5	e3962080-928...	251176217062072		1504584000.0	1504647651.9...		26	Microsoft lpcl26Microsoft just Left Almond-aab8	500	0	NULL	Microsoft just Left Almond-aab8	1	0

	id	external_id	mac	users	date_bucket	time	data	deviceid	devicename	devicetype	value_index	value_indexname	indexvalue	viewed	notiCat
	...	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
25	25	497888f0-aab8...	25117621706...		1507262400.0	1507309414.0		15	motion sensor	60	1	NULL	true	1	0
26	26	b4cc2650-aab5...	25117621706...		1507262400.0	1507308305.0		16	hr nyce	12	1	STATE	false	1	0
27	27	ab4fb6a0-aab5-...	25117621706...		1507262400.0	1507308289.0		16	hr nyce	12	1	STATE	true	1	0
28	28	8638cbb0-aaae...	25117621706...		1507262400.0	1507305221.0		15	motion sensor	60	6	HUMIDITY	45	1	0
29	29	33fc8ab0-aac4-...	25117621706...		1507262400.0	1507314532.0		14	Peanut Plug	50	1	SWITCH BINARY	true	1	0
30	30	3691db90-aac...	25117621706...		1507262400.0	1507314536.0		14	Peanut Plug	50	1	SWITCH BINARY	false	1	0
31	31	43167040-aac...	25117621706...		1507262400.0	1507315416.0		15	motion sensor	60	6	HUMIDITY	48	1	0
32	32	90592510-aac...	25117621706...		1507262400.0	1507315116.0		15	motion sensor	60	6	HUMIDITY	49	1	0
33	33	8f7aabf0-aac5-...	25117621706...		1507262400.0	1507315115.0		15	motion sensor	60	5	TEMPERATURE	71.2	1	0

Figure 4: Extracted from companion app. Top - toolkit_devicelogs.db, Bottom - toolkit_notifications.db

city, state, country, longitude, latitude, weather conditions.

Finally, there are other files worth analysing depending on the smart sensors in use. For example, given its name, `/tmp/NestSever.log` is likely to contain details about events generated by Nest thermostats; we did not have a sample device at the time of writing to confirm residual artefacts.

7.2. Residing on the iPhone companion app

The app provides two methods of interfacing with Almond, via Cloud connectivity or through local (LAN) connectivity. The local connectivity option provides similar features when connected via the Cloud but it neither records device history nor sensor actions.

As discussed in Zdziarski 2008, "[t]he iPhone makes heavy use of database files to store information". Though the reference is nearly a decade old at the time of writing, the statement is relevant considering the plethora of apps storing data in SQLite database formats. The Almond+ companion app, "Almond by Securifi" in the Apple app store, contains the following files of significance:

`<root>/Documents/toolkit_devicelogs.db` - Network devices (e.g. tablets, computers) are logged joining and leaving the network. UNIX timestamps and device dames are available.

`<root>/Documents/toolkit_notifications.db` - State changes for smart devices (i.e. IoT) are recorded in this file. States (key "*indexvalue*") are dependent upon the type of sensor, the "*value_indexname"* may be cross-examined for further information. E.g. the *indexvalue* of 71.2 doesn't indicate much until we use *value_indexname* to discover these units are in *TEMPERATURE* and not another value such as *HUMIDITY*.

`<root>/Library/Caches/Snapshots/com.securifi.almond/*@2x.png` (* represents an 8-4-4-4-12 alphanumeric string) - This image file provides a snapshot of whatever the user last viewed on the application. Both the content and the filename are updated whenever the application loses focus.

Figure 4 displays information contained within the two database files mentioned above. It should be noted that the companion app contains a "View Device History" option for both smart (e.g. sensors) and network (e.g. PC with Wi-Fi) devices. However, at the time of writing, the authors were not able to obtain any history for smart devices using v.3.4.3 of the app, only for network devices. The available "history" for smart sensors is obtainable via the Alerts timeline. Furthermore, when the companion app is reinstalled and an existing ID is used, this prior history is downloaded from the Cloud service and may be again seen.

7.3. Residing on the Cloud web interface

At the time of writing, this interface is neither as developed as the companion app nor the native Almond+ interface; both the "Rules" and "Advanced Features" provide messages stating that these features are unavailable. Despite multiple attempts, we were also unable to retrieve any sensor data even though the companion app worked. We were able to obtain a list containing current wireless settings, network devices (name, Mac and IP only) and the software version. The "View Device History" option seen in the companion app was absent, but the list does indicate which devices are currently connected to the hub.

8. Recommendations for the forensic examiner

The following suggestions are made to those who encounter such devices during an examination:

1. Investigate the Almond+ first; it is the most volatile. Do not reboot or reset, evidence resides in a volatile `tmpfs` type filesystem.
2. Do not touch the screen. Investigators may be tempted to view the "Connected Sensors" but this will generate events in `/tmp/connected_home.log`
3. Connect to Wi-Fi (if password available) or LAN on Almond+.
4. Connect via SSH using method described in section 'Data Extraction'.
5. Create a backup of the data as described in section 6 using a memory stick and hashing.
6. Analyse files highlighted in Fig. 4. from Almond+ according to section 6 'Artefacts of Forensic Importance'.

If the Almond+ companion app is available on a phone/tablet, there are two paths an analyst may traverse but both should be performed only after standard procedures (NIST, 2014) are considered:

1. Ensure device data is copied using standard operating procedures
2. If device is iOS-based and jailbreaking is an option, evaluate impact of jailbreak to be able to defend actions in a court of law
3. Install Filza or iFile from the Cydia App Store onto device, manually extract data described in section data extraction.
4. Analyse files highlighted in Table 2.
5. If jailbreaking is not an option, start video recorder and record the actions
6. Perform hand-scroll of Almond+ companion app
    a. Bell icon - provides timeline of alerts (for those explicitly setup by user)
    b. Devices icon - "View History" provides presence-based (i.e. within range) artefacts (note - only useful with Cloud connectivity enabled)

If Cloud/web interface password is known:

1. Login at https://connect.securifi.com
2. Obtain router and device sensor by using print screens and/or saving web pages.

9. Conclusions and future work

The continued growth in the volume and variety of IoT devices will result in an increasing amount of information being available for forensic analysis. In particular, the increase in the domestic use of IoT or 'smart devices' will likely generate a need for forensic analysis. Systems used to integrate IoT devices, i.e. the 'smart home hub' are likely to provide a useful single source of forensic artefacts relating to a user's interaction within an environment. The Almond+ ecosystem has a series of local- and cloud-based logs that are available for analysis. Information is also available from a companion application that provides some evidence of connected network devices and user activity.

The Almond+, like the Amazon Alexa service, has the potential to impact on an investigation as the information in the device may have some considerable forensic value as it can indicate interaction with the device at a certain time and date. For this reason, future work should include the possibility of developing a more generalised forensic guide for home hubs.

It should be possible to develop a forensics tool to analyse the information present on the Almond+ and to correlate the data between the different logs to provide a historical pattern of activity observed by the devices. Other future work will examine more destructive methods of analysis including data recovery via chip off or JTAG methods to obtain additional information. Further research in JFFS2 image mounting may allow for other forensic artefacts to be retrieved, such as deleted files via file carving or regex searching.

Acknowledgements

This research was supported by work funded from the Provost Chase Scholarship Initiatives at Norwich University.

References

Afonin, O., (2017) "New Security Measures in iOS 11 and Their Forensic Implications", Elcomsoft Blog, Sept, 2017. https://web.archive.org/web/20171008051714/https://blog.elcomsoft.com/2017/09/new-security-measures-in-ios-11-and-their-forensic-implications/ Last accessed: 8/10/2017

Apple, (2017a), "Apple HomeKit", https://developer.apple.com/homekit/ Last accessed: 8/10/2017

Apple, (2017b) "Apple HomePod" https://www.apple.com/homepod/ Last accessed: 8/10/2017

Ashton, K., (2009) "That 'Internet of Things' Thing", Jun. 22, 2009 online article, Last accessed: 8/10/2017.

Chung et al., 2012 Chung, H., Jungheum, P., Lee, S., "Digital forensic approaches for Amazon Alexa ecosystem", Proceedings of the Seventeenth Annual Digital Forensic Research Workshop USA, Vol. 22, Aug. 2017, pp. S15-S25.

Columbus, L., (2016), "Roundup Of Internet Of Things Forecasts And Market Estimates, 2016", https://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/ Nov, 27, 2016, Last accessed: 8/10/2017

DBBrowser, (2017) "DB Browser for SQLite, 'The official home of the DB Browser for SQLite'", https://web.archive.org/web/20171007172653/http://sqlitebrowser.org/ Last accessed: 7/10/2017

Gartner, (2017), "Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016", http://www.gartner.com/newsroom/id/3598917 Last accessed: 5/10/2017

Google Onhub, https://on.google.com/hub/ Last accessed: 8/10/2017

Hyde, J., and Moran B., (2017) "Alexa are you Skynet?", 2017

https://www.sans.org/summit-archives/file/summit-archive-1498230402.pdf Sans Summit, Last accessed: 8/10/2017

Johnson, 2017 Johnson, M., Dropbear Changelog, https://web.archive.org/web/20170828170840/https://matt.ucc.asn.au/dropbear/CHANGES Last accessed: 5/10/2017

Lars, 2014 User "Lars", https://wiki.securifi.com/index.php?title=Console_port_-_Almond%2B_2014

Leahy Center for Digital Investigation (2016) Amazon Echo Forensics, Leahy Center for Digital Investigation, Champlain College, USA, https://lcdiblog.champlain.edu/2016/05/28/amazon-echo-final-report/ Last accessed:8/10/2017.

Meffert, C., Clark, D., Baggili, I., and Breitinger, F., (2017) "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 (ARES '17). ACM, New York, NY, USA, Article 56, 11 pages. DOI: https://doi.org/10.1145/3098954.3104053

NIST 2014 Ayers, R., Brothers, S., Jansen, W., "Guidelines on Mobile Device Forensics", NIST Special Publication 800-101, May, 2014, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf Last accessed: 8/10/2017.

OpenSSH, 2017 OpenSSH Legacy Options, http://www.openssh.com/legacy.html https://web.archive.org/web/20170827101553/https://www.openssh.com/legacy.html Last accessed: 5/10/2017

Oriwoh, E., Jazani, D., Epiphaniou, G., and Sant, P., (2013), "Internet of Things Forensics: Challenges and approaches," 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing, Austin, TX, 2013, pp. 608-615. doi: 10.4108/icst.collaboratecom.2013.254159

Paetz, C., (2013) "Z-Wave Basics, Remote Control in Smart Homes", Amazon.co.uk Marston Gate.

Pangu, 2017 "Pangu Jailbreak", http://en.pangu.io/ Jul., 28, 2016. Last accessed: 8/10/2017

Paxton, M., (2017) "Smart Homes In The U.S. Becoming More Common, But Still Face Challenges" https://marketintelligence.spglobal.com/blog/smart-homes-in-the-u-s-becoming-more-common-but-still-face-challenges Jun., 14, 2017, Last accessed: 5/10/2017

Plachkinova M., Vo A., Alluhaidan A., (2016) Emerging Trends in Smart Home Security, Privacy, and Digital Forensics , Twenty-second Americas Conference on Information Systems, San Diego, 2016

Securifi, 2017 Securifi, "Whats New?", https://web.archive.org/web/20171005175712/https://www.securifi.com/whatsnew Last accessed: 5/10/2017

Securifi, 2014 Securifi, "SSH Access Almond+ 2014", https://web.archive.org/web/20171007234518/https://wiki.securifi.com/index.php?title=SSH_Access_-_Almond%2B_2014 Last accessed: 7/10/2017

Sutherland I., Spyridopoulos, T., Read, H., Jones, Sutherland G., Burgess M., (2015) Applying the ACPO guidelines to Building Automation Systems, HCI International 2015 Conference, Los Angeles USA.

The Unofficial Amazon Echo User Forum (2016) Understanding the UART/JTAG/Pinouts on the Amazon Echo http://www.echotalk.org/index.php?topic=443.0

Zdziarski, 2008 Zdziarski, J., "iPhone Forensics: Recovering Evidence, Personal Data, and Corporate Assets", O'Reilly Media, Sept 2008, pp70-74.

Zigbee Alliance 2017, http://www.zigbee.org/zigbeealliance/ Last accessed: 5/10/2017

Z-Wave Alliance 2017 https://z-wavealliance.org/ Last accessed: 7/10/2017

Appendix A. Almond+ file excerpts

/tmp/connected_home.log

```
[2017-10-4 18:4:40.94243]  {INFO}   SecurifiSmartSwitch  5 initial state On ActivePower: 0.000W
       Current: 0.000A Voltage: 0.000V
[2017-10-4 18:4:41.67981]  {INFO}   Device 5 index 1 is set to false value
[2017-10-4 18:4:42.61290]  {INFO}   Close button pressed
[2017-10-4 18:4:42.78809]  {INFO}   home mode matched
[2017-10-4 18:35:37.37573] {PRINT}  Received ClientLeft event
[2017-10-5 16:40:44.34214] {INFO}   SecurifiSmartSwitch  5 initial state Off ActivePower:
       0.000W Current: 0.000A Voltage: 0.000V
[2017-10-5 16:40:45.04513] {INFO}   Device 5 index 1 is set to true value
[2017-10-5 16:43:6.57517]  {PRINT}  Received ClientUpdated event
[2017-10-5 16:43:8.02169]  {PRINT}  Received ClientJoined event
```

/tmp/association.log

```
[2017-10-3 15:24:11.02826] {INFO} <====== association Started========>
[2017-10-3 15:24:19.78916] {PRINT}readarea
[2017-10-3 15:24:19.86888] {INFO} Sending Association command to zwave_server and zigbee_server
[2017-10-3 15:24:21.06685] {INFO} device joined status 1 1
[2017-10-3 15:24:21.06702] {INFO} Sending cancel command to zwave_server
[2017-10-3 15:24:21.12212] {INFO} Device got added (Zigbee)
[2017-10-3 15:24:28.10500] {INFO} device joined status 6 6
[2017-10-3 15:24:31.13461] {INFO} Getting Sensor info (Zigbee)
[2017-10-3 15:24:49.74244] {INFO} device joined status 10 10
[2017-10-3 15:24:49.74326] {INFO} collecting info of zigbee device
[2017-10-3 15:24:49.74344] {INFO} M_name Securifi Ltd. and manufrId 1002 and Imagetype 5ec0
[2017-10-3 15:24:49.74358] {INFO} Manu name Securifi Ltd.
[2017-10-3 15:24:49.74368] {INFO} No. of clusters found:2 and indexes:5 zonetype:0
[2017-10-3 15:24:49.74382] {INFO} Peanut Plug #5
[2017-10-3 15:24:49.97652] {INFO} Sensor got Associated (Zigbee)
[2017-10-3 15:24:49.97671] {INFO} Sensor got Associated 5 name Peanut Plug #5 (Zigbee)
[2017-10-3 15:25:21.84711] {INFO} Peanut Plug
[2017-10-3 15:25:21.84743] {INFO} Sending Packet to HaServer Success
[2017-10-3 15:25:21.84763] {INFO} Sending Packet to Haserver Success
```