Digital Investigation 26 (2018) S38–S46

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

DFRWS 2018 USA — Proceedings of the Eighteenth Annual DFRWS USA

Welcome pwn: Almond smart home hub forensics

Akshay Awasthi [a], Huw O.L. Read [a, b, *], Konstantinos Xynos [c, b], Iain Sutherland [b, d]

[a] Norwich University, Northfield, VT, USA
[b] Noroff University College, Elvagata 2a, Kristiansand, Norway
[c] DarkMatter LLC, Dubai, United Arab Emirates
[d] Security Research Institute, Edith Cowan University, Perth, Australia

Keywords:
Internet of things
Extraction
Smart sensor
Smart home hub
iOS
Android
Cloud

A B S T R A C T

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 central location rather than separate ones. 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 applications and the local & cloud-based web interfaces.

1. Introduction

The rapid expansion of internet enabled devices has lead to the realization of the “Internet of Things” (IoT) as first mentioned by 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 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 houses that have IoT devices installed (Paxton, 2017). Smart homes use a variety of devices, integrated to provide intelligent features such as providing 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: Section 2 describes similar forensic examinations on other smart hub devices, section 3 presents our experiment configuration and introduces features of the device, section 4 identifies issues faced during the course of investigation, section 5 describes the process taken to identify artefacts, section 6 details how an investigator may extract artefacts from devices in the Almond environment, section 7 identify locations where evidence of note may be found, section 8 provides a summary of data extraction and analysis, and finally, section 9 provides a summary of the research presented in this paper and thoughts for continuing the 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

* Corresponding author. Norwich University, Northfield, VT, USA.
E-mail address: hread@norwich.edu (H.O.L. Read).

https://doi.org/10.1016/j.diin.2018.04.014

wireless network transmission protocols. This is now a significant area of concern with research efforts focused on the analysis and data extraction 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 an infrastructure, may cause significant problems. Simply gaining physical access to the systems can be a separate challenge altogether for the analyst. However, in many cases, there is little of forensic value on the devices themselves. What may prove to be of greater importance is accessing any system used to integrate IoT devices providing centralised control (Sutherland et al., 2015). Typically, domestic systems are connected via some form of hub or central service to facilitate a "Smart Home". The integration of these devices has already raised security concerns (Plachkinova et al., 2016). Generally, the forensic analysis of Smart Hubs thus far has been limited. The following section describes related work carried out to date on three such systems; Amazon Alexa, Apple HomeKit and Google OnHub or 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 (dj_skully, 2016). An analysis by the LCDI (2016) provided some insight regarding performing a forensic analysis on the Amazon Alexa, via third party devices. The report explains techniques for data collection and data extraction. The greatest challenge they encountered was third-party device integration with 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; it *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 revising 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 and requires an Apple iOS device or Apple TV to remain in the home to act as a hub for external access (Apple, 2017a). Apple released the HomePod in early 2018, which appears to be limited in capacity acting as a speaker and an interface to Siri and HomeKit devices (Apple, 2017b). Given Apple's public stance on encryption and working with law enforcement (Cook, 2016), the challenge of extracting forensic data from the Home environment will likely be of particular interest to digital forensic researchers.

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 (Google, 2017) which takes a different approach than that adopted by Amazon. Rather than becoming an additional device on the network, 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 Googles 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 IoT protocols, namely Zigbee and Z-Wave. Fig. 1 demonstrates how the following sensors were connected to the Almond + environment for the experiment:

- Three Philips Hue Lamps via a Philips Hue Bridge - changes colour, dimming, on/off
- Jasco Dimmer Plug, 3-pronged dimmer device
- Securifi Peanut Plug, on/off power device
- Fibaro Door/Temperature Sensor, two-components
- NYCE Motion/Temperature/Humidity Sensor, positioned on ceiling
- Two NYCE Door Sensors, alternative 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 as depicted in Fig. 2. The interface on the Almond + provides a myriad of information to the user: 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 (Fig. 2) and both have a consistent look and feel. The app provides 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.

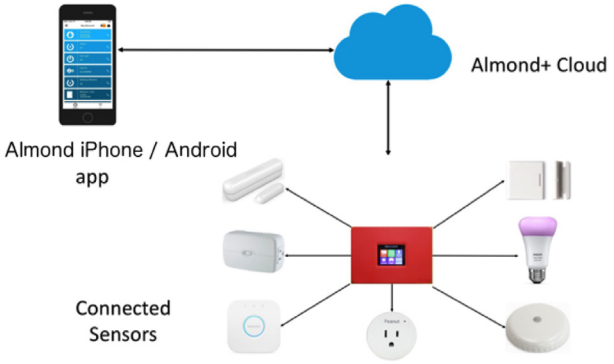

Fig. 1. Almond+ Environment Setup.

Fig. 2. Top Almond+ touchscreen, Right - companion app, Bottom–Cloud interface.

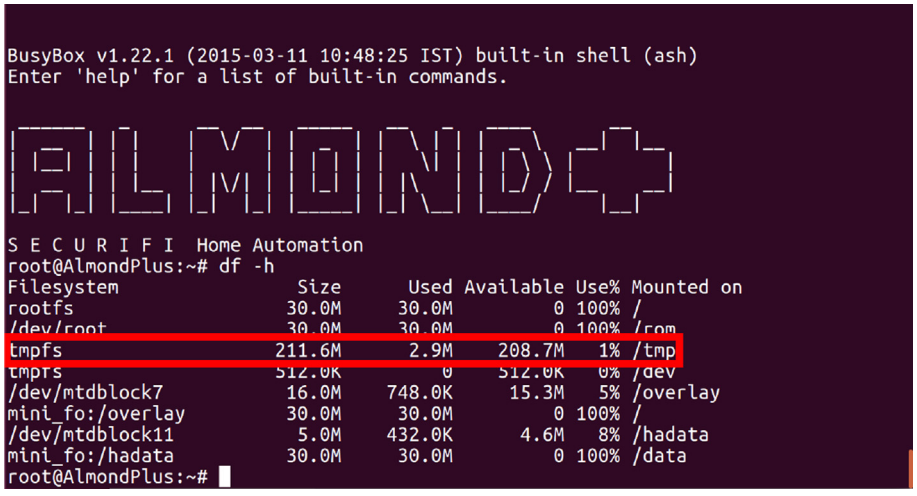

Fig. 3. Default mount points -/tmp contains valuable data but resides in RAM.

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 only subtle differences between the companion app for iOS and Android; the structure of the SQL databases were slightly different though the data was largely the same (Fig. 4).

3.3. Via the cloud-based 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 (Fig. 2).

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.

	id	external_id	mac	users	date_bucket	time	data	deviceid	devicename	devicetype	ue_in	_index	indexvalue	viewed	notiCat
		Filter	Filter		Filter	Filter		...	Filter	Filter	Fil...		Filter		...
1	1	50faf990-9...	25117...		1504843200.0	1504928296.872		26	Microsoft Ipcl26IMicrosoft just Left Almond-aab8	500	0	NULL	Microsoft just Left Almond-aab8	1	0
2	2	15f1b970-9...	25117...		1504843200.0	1504897703.559		26	Microsoft Ipcl26IMicrosoft rejoined Almond-aab8	500	0	NULL	Microsoft rejoined Almond-aab8	1	0
3	3	4f6d0970-9...	25117...		1504756800.0	1504814048.138		26	Microsoft Ipcl26IMicrosoft just Left Almond-aab8	500	0	NULL	Microsoft just Left Almond-aab8	1	0
4	4	08ecb7c0-9...	25117...		1504756800.0	1504798897.467		26	Microsoft Ipcl26IMicrosoft rejoined Almond-aab8	500	0	NULL	Microsoft rejoined Almond-aab8	1	0
5	5	e3962080-...	25117...		1504584000.0	1504647651.967		26	Microsoft Ipcl26IMicrosoft just Left Almond-aab8	500	0	NULL	Microsoft just Left Almond-aab8	1	0

(a) iOS: toolkit_devicelogs.db - Log of networked devices joining and leaving network

	id	external_id	mac	users	date_bucket	time	data	deviceid	devicename	devicetype	alue_inde	value_indexname	indexvalue	viewed	notiCat
		Filter	Filter		Filter	Filter		...	Filter	Fil...	Fil...	Filter	Filter		F...
1	1	722f239...	251176...		1507176000.0	1507253218.0		14	Peanut Plug	50	1	SWITCH BINARY	false	1	0
2	2	5f8304a0...	251176...		1507176000.0	1507253187.0		14	Peanut Plug	50	1	SWITCH BINARY	true	1	0
3	3	e9c0e61...	251176...		1507262400.0	1507298086.0		15	motion sensor	60	6	HUMIDITY	44	1	0
4	4	f6e69990...	251176...		1507262400.0	1507297249.0		15	motion sensor	60	6	HUMIDITY	45	1	0
5	5	4425a4e...	251176...		1507262400.0	1507296949.0		15	motion sensor	60	6	HUMIDITY	46	1	0

(b) iOS: toolkit_notifications.db - Log of state changes for IoT devices

	msg_id	_mac	_dev_id	_dev_type	_index	_index_value	_index_name	_message	_time_stamp	_read	_type	_name
	Filter	Filter	F...	Filter		Filter	Filter	Filter	Filter		F...	Filter
38	0:1520904168529409%dd7a782019394df3	251176217062072	13	2	1	100	SWITCH MUL...	dimmer plug is dimmed to 100%	1520904166000	1	0	dimmer plug
39	0:1520904173502467%dd7a782019451cb7	251176217062072	13	2	1	37	SWITCH MUL...	dimmer plug is dimmed to 37%	1520904171000	1	0	dimmer plug
40	0:1520904178123694%dd7a782029ebe786	251176217062072	14	50	1	true	SWITCH BINARY	Peanut Plug is turned On	1520904176000	1	0	Peanut Plug
41	0:1520904181740695%dd7a782029ed5b67	251176217062072	14	50	1	false	SWITCH BINARY	Peanut Plug is turned Off	1520904179000	1	0	Peanut Plug
42	0:1520904290430903%dd7a7820046b03a9	251176217062072	10	48	2	false	SWITCH BINARY	lamp 1 is turned Off	1520904288000	0	0	lamp 1

(c) Android: notifications.db - Networked devices connecting to network and log of state changes

Fig. 4. SQLite files of forensic significance extracted from iPhone (Top, Centre) and Android (Bottom) apps.

4. Forensic challenges

During the course of the research, a number of barriers were identified that could impede a successful forensic examination. No discernible 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 512 MB 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 Fig. 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; user configuration is required to enable it over Wi-Fi (Lars, 2014a). SSH can permit remote access, filesystem extraction (sftp) and, in combination with other tools like dd remote imaging is also possible. An investigation into the potential for SSH as a data-access and data-extraction mechanism will be explored later in the paper.

There are several devices supported by the Almond + that can also be controlled by other "smart" devices; for example, the Philips Hue lightbulbs are compatible with the Amazon Echo device. Understanding whether there is any synchronisation between different controller-devices will be of interest to the forensic examiner.

Unfortunately for the examiner, it has become more difficult to obtain data from Apple devices in recent iOS versions with fewer files from applications 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 refer to the summary of iOS8-11 in Afonin (2017) for general iOS challenges to forensic analysis. Significant files from the companion app are not easily accessible in iOS; analysts may need to either manually hand-scroll through information on the app itself or risk jailbreaking the device to obtain the data. Similarly, depending upon the state of forensic tools, the Android version of the Almond app may have extraction issues related to permissions.

5. Investigative methods

In order to create the IoT-enabled environment, a number of sequential steps were completed to assess the impact of different devices (IoT, other controller-devices) and whether any artefacts of importance to forensic examiners could be discovered.

1. Initial assessments of Almond + logs via an empirical investigation
   - IoT device introduced to Almond + ecosystem
   - Home hub log files examined and observations recorded
   - IoT device removed, to reduce noise on network
2. Almond + touchscreen assessment
   - Update configuration for an IoT device
   - Record observations in Almond + logs
3. Companion app assessment
   - Install Almond by Securifi app on iPhone and Android
   - Interact with devices via app, note time
   - Interact with devices via other mechanisms e.g. Cloud
   - Record observations in Almond + logs and handsets
4. Local network and Cloud assessment
5. Alternative controller-device implications (Amazon Echo)

Post Almond + setup, the smart devices were added sequentially. Sensors were 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 each 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 users actions.

Amazon Echo device was used on the same network to control the Philips Hue lights that were also connected to the Almond+. The logs were examined to evaluate if either any purposeful synchronisation took place between controller-devices, or if any such device was able to observe the controlling instructions provided by another.

NIST 800-101 Guidelines on Mobile Device Forensics (Ayers et al., 2014) was 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 with a non-jailbroken device, 2) a backup made using iTunes with a jailbroken device, 3) manual extraction using Cydia file browsing apps and 4) Cellebrite UFED Touch2 filesystem extraction. We found there wasn't a difference in the quality of the extraction between 1. 2. and 4. 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.

A similar process was conducted on the Android device (a Sony Xperia Z1 Compact running Android 5.1.1. 1) extraction from stock 5.1.1 via the android debug bridge (adb), 2) the backup feature from the Sony Xperia Companion software (1.9.2), 3) extraction after rooting, 4) using forensic hardware (Cellebrite UFED Touch 2, firmware 6.1.2). Only methods 3 and 4 allowed the extraction of the filesystem. Of these, method 4 was used as it is an established method of data 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 Lars (2014b), default SSH access is only available via LAN. At the time of writing, the firmware revision is AP2-R090-L009-W016- ZW016-ZB005. We have identified 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 WI-FI 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.

The SSH server is provided by Dropbear v0.52, released in 2008 (Johnson, 2017) and with 3 known vulnerabilities. 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. We had to use the following command to login to 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/id/time_date.tar.gz | md5sum >
/mnt/usb/id/time_date.tar.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@<ip_address>
“dd if = /dev/mtdblock7” | tee block7.dd
| md5sum > block7.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 tools `file` & `binwalk` to attempt identification. A summary of these may be seen in Table 1.

The squashfs file system can be easily extracted by using squashfs tools, which in Ubuntu can be found in the package `squashfs-tools`.

Attempts to extract or mount the individual mtdblock images identified as JFFS2 were not particularly successful; the mounting process generated the following error `jffs2: compression type 0x08 not available`.

This can be seen by attempting to mount the drive with the following set of commands:

```
$modprobe -r mtdram
$modprobe mtdram total_size = 18000
$dd if = block7.dd of = /dev/mtdblock0
$mount -t jffs2/dev/mtdblock0/mnt/testDrive
$dmesg | tail
```

First, we ensure that mtdram is unloaded and then load it again with the correct size of the device when executing `modprobe`. This requires the analyst to check the file size of the image that will be loaded (e.g., block7.dd), this is then provided as a value in `total_size`. The image file is then dd'ed to the device (e.g.,/dev/mtdblock0) and it is then mounted. `dmesg` can be consulted for any messages or errors.

It is hypothesised that the compression type (i.e., LZARI, type 0x08) is one that is not supported by modern implementations of jffs2 and was only included in the kernel of this particular system. There are a number of things that a forensic analyst could do. One of these could be to attempt to boot up the system using QEMU and navigate it from there. Another is to find the implementation of the compression and decompression used and implement it in `jffs2dump`.

6.2. Companion app

As previously mentioned in Forensic challenges, obtaining raw files from Apple devices 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.

Table 1
mtdblock datatypes reported by `file` & `binwalk`

mtdblock#	Linux `file` & `binwalk` command output
0,2,3,9,10,12,13	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)
7,11	Linux jffs2 filesystem data little endian
8	ISO-8859 text, with very long lines, with no line terminators

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.

Retrieving data from the Android device (a Sony Xperia Z1 Compact running Android 5.1.1) was more straightforward; a Cellebrite UFED Touch 2 (firmware 6.1.0.140) provided a complete filesystem extraction including the Almond + app data. Once the Almond + folder is located, it may be copied to a workstation for analysis of the SQLite files. All such files were analysed using DB Browser for SQLite v.3.10.1 (sqlitebrowser, 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 7, 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 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*- ContainWi-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, 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/NestServer.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 companion app

Common to both Android and iOS, 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, on both Google and Apple operating systems. It should be reiterated that the iOS files retrieved from an iPhone were done so by jailbreaking the device as described in the Investigative methodology. The Almond + companion app, "Almond by Securifi" in both the Apple app and Google play stores, contains the following files of significance:

`<root>/Documents/toolkit_devicelogs.db`

iOS - Network devices (e.g. tablets, computers) are logged joining and leaving the network. With reference to Fig. 4a, two timestamps are available per event, both stored as GMT. `date_bucket` indicates the date (time is always set at midnight) and `time` which provides the full date and time. The `indexvalue` states when a new networked device was connected, `A new device <device_name>just joined Almond-aab8` (not seen in Fig. 4a), rejoined, or left. The `devicename` appears to be an amalgamation of both the device's name and a copy of the `indexvalue`. It is unknown if this repetition is deliberate.

`<root>/Documents/toolkit_notifications.db`

iOS - State changes for smart devices (i.e. IoT) are recorded in this file. The database structure is the same as that observed in `toolkit_devicelogs.db`. Timestamps are again stored in GMT. `devicename` contains either a default or a value set by the user identifying the IoT devices by name. `indexvalue` contains quite a varied set of values, based on the `devicetype`. The `value_indexname` is populated with an indicator of what state change triggered the event. For example in Fig. 4b, `devicetype` 60, a motion sensor with a built-in humidity sensor, has two

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/tool-kit_devicelogs.db	Record of all network devices (dis)associating with Almond+
iPhone App	<root>/Documents/tool-kit_notifications.db	Record of all smart devices which have alerts explicitly set
iPhone App	<root>/Library/Caches/Sna-pshots/com.securifi.al-mond/*@2x.png	Screenshot of most recent user-interaction in app
Android App	/data/data/com.securi-fi.almondplus/databases/not-ifications.db	Record of smart devices which have alerts explicitly set and network devices (dis)associating with Almond+
Cloud/Web	connect.securifi.com	Current Wi-Fi settings, list of all networked devices (highlights connected), firmware version

`value_indexname` entries associated with it, HUMIDITY and a NULL entry. The `indexvalue` for HUMIDITY provides the percentage value when the humidity in the room changes, the NULL entry indicates whether motion has been detected (true/false values).

`<root>/Library/Caches/Snapshots/com.securifi.almond/*@2x.png` (* represents an 8-4-4-4-12 alphanumeric string) iOS - 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.

`<root>/databases/notifications.db`

Android - An amalgamation of both iOS SQLite databases compiled in one file. Though the database contains the same information as its iOS counterpart, it is structured differently. Fig. 4c has a single `_time_stamp` value in GMT which provides full date and time information (unlike `data_bucket` above). The `_index_name`, `_name` and `_index_value` are equivalencies of the following iOS values `value_indexname`, `devicename` and `indexvalue`. The value `_message` appears unique to the Android app, it provides a high-level textual description of the event. The information can be derived from using other values but could be for convenience. For example, row 39 in Fig. 4c shows a dimmer plug registered a SWITCH MULTILEVEL value of 37. The `_message` indicates *dimmer plug is dimmed to 37%*.

It should be noted that both the Android and iOS companion apps contain a "View Device History" option for both smart (i.e. Zigbee and Z-Wave) and network (i.e. PC with Wi-Fi) devices. The available "history" for smart sensors is obtainable via the Alerts timeline. This information appears to be streamed from the Cloud as it did not appear to exist in local database files. However, when the companion app is reinstalled and an existing ID is used, this prior history can be streamed from the Cloud service and may be seen again.

7.3. Residing on the cloud 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. We were able to retrieve individual sensor data, presented as a timeline and 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.

7.4. Observations with the Amazon Echo

As mentioned in Forensic challenges, some devices can be controlled by multiple smart hubs. 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+ (via ethernet), any changes made to the state of the Hue lights with the Echo did not result in any artefacts generated on the Almond + ecosystem. Only changes made either directly on the Almond + or via the companion app while in Cloud connectivity mode resulted in observational evidence on the Almond + 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. (2017), should be referenced if an Amazon Echo is found in the target environment for further extraction opportunities.

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 6.
5. Create a backup of the data as described in section 6 a memory stick and hash the extracted data.
6. Analyse files highlighted in Table 2 from Almond + according to section 7.

   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 (Ayers et al., 2014) are considered:

1. Ensure device data is copied using standard operating procedures
2. Assess ability of forensic imaging tools (the authors used Cellebrite's UFED Touch 2 for the Android device) to extract data from device.
3. 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
4. Install Filza or iFile from the Cydia App Store onto device, manually extract data described in section 6.
5. Analyse files highlighted in Table 2.

6. If jailbreaking (iOS) or rooting (Android) are not an option, start video recorder and begin capture.
7. Perform hand-scroll of Almond+ companion app paying particular attention to any Alerts - once viewed their status will change to "seen".
   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 the Cloud password is known:

1. Login at `https://connect.securifi.com`
2. Obtain router and device sensor via print screen and/or saving web pages.

9. Conclusions and future work

The research work presented in this paper focused on one of the many different hubs coming to market providing a merging of networks in the home/SOHO environment. The combination of controlling both IoT enabled sensors and home network access from a single interface provides convenience and, in combination with always on, Cloud access, accessibility. The Almond+ ecosystem (including the home hub, iOS/Android companion apps and the Cloud environment) were examined to provide forensic examiners encountering such a device with a method of extraction and analysis. Furthermore, much like any significant changes to technology, the lessons that can be learned from initial adopters can further an analyst's understanding of the broader implications of the technology.

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 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 considerable forensic value as it can indicate interaction with the environment at a certain time and date. Observed changes such as humidity, temperature and motion are more passive in their approach. Other changes such as dimming lights, changing room colours and turning wall sockets on and off are more active requiring direct command. The data gathered from an Almond + system could provide a rich, if textual, picture of events leading up to a crime scene.

During the course of this research several observations were noted that could impact on a user's security and privacy. Default root passwords (which can be viewed in the SecuriFi wiki (Lars, 2014b)) should be changed before the hubs leave the manufacturer as is the case with many router vendors; stickers with a unique code attached to the device for example. The severity would also be lessened by checking the shipping configuration of such devices; as mentioned in Data extraction, the firmware version we assessed had root-accessible SSH access enabled over WiFi by default regardless of what the GUI interface indicated.

Future work should include the analysis of other, similarly marketed home hubs to produce more generalised forensic guide that would work across a range of devices. Furthermore, it would be desirable 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.

Acknowledgements

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

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
```

References

Afonin, O., 2017. New Security Measures in Ios 11 and Their Forensic Implications (Online; accessed 8-October-2017). https://blog.elcomsoft.com/2017/09/new-security-measures-in-ios-11-and-their-forensic-implications/.

Apple, 2017a. Apple Homekit (Online; accessed 8-October-2017). https://developer.apple.com/homekit/.

Apple, 2017b. Apple Homepod (Online; accessed 8-October-2017). https://www.apple.com/homepod/.

Ashton, K., 2009. That 'internet of Things' Thing (Online; accessed 8-October-2017). http://www.rfidjournal.com/articles/view?4986.

Ayers, R., Brothers, S., Jansen, W., 2014. Nist Special Publication 800-101 Revision 1: Guidelines on Mobile Device Forensics. https://doi.org/10.6028/NIST.SP.800-101r1.

Chung, H., Park, J., Lee, S., 2017. Digital forensic approaches for amazon alexa ecosystem. Digit. Invest. 22, S15–S25.

Columbus, L., 2016. Roundup of internet of things forecasts and market estimates, 2016 (Online; accessed 8-October-2017). https://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#33963d40292d.

Cook, T., 2016. A Message to Our Customers; the Need for Encryption (Online; accessed 26-March-2018). https://www.apple.com/customer-letter/.

dj_skully, 2016. Understanding the Uart/jtag/pinouts on the Amazon Echo (Online; accessed 5-October-2017). http://www.echotalk.org/index.php?topic=443.0.

Gartner, 2017. Gartner Says 8.4 Billion Connected "things" Will Be in Use in 2017, up 31 Percent from 2016 (Online; accessed 5-October-2017). https://www.gartner.com/newsroom/id/3598917.

Google, 2017. Onhub (Online; accessed 8-October-2017). https://on.google.com/hub/.

Hyde, J., Moran, B., 2017. Alexa, Are You Skynet? (Online; accessed 8-October-2017)]. https://www.sans.org/summit-archives/file/summit-archive-1498230402.pdf.

Johnson, M., 2017. Dropbear Changelog (Online; accessed 5-October-201). https://matt.ucc.asn.au/dropbear/CHANGES.

Lars, 2014a. Console Port - Almond+ 2014 (Online; accessed 5-October-2017). https://wiki.securifi.com/index.php?title=Console_port\-\Almond\%2B\2014.

Lars, 2014b. Ssh Access - Almond+ 2014 (Online; accessed 5-October-2017). https://wiki.securifi.com/index.php?title=SSH\Access\-\Almond\%2B\2014.

LCDI, 2016. Amazon Echo Forensics (Online; accessed 5-October-2017). https://lcdiblog.champlain.edu/wp-content/uploads/sites/11/2016/05/EDITED_Amazon_Echo_Report-1.pdf.

Meffert, C., Clark, D., Baggili, I., 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, ACM, New York, NY, USA, p. 56, 1–56:11.

OpenSSH. Openssh Legacy Options, n.d. (Online; accessed 5-October-2017). https://www.openssh.com/legacy.html.

Oriwoh, E., Jazani, D., Epiphaniou, G., Sant, P., 2013. Internet of things forensics: challenges and approaches. In: 9th IEEE International Conference on Collaborative computing: networking, Applications and Worksharing, pp. 608–615.

Pangu, 2016. Pangu Jailbreak (Online; accessed 5-October-2017). http://en.pangu.io/.

Paxton, M., 2017. Smart Homes in the u.S. Becoming More Common, but Still Face Challenges (Online; accessed 5-October-2017). https://marketintelligence.spglobal.com/blog/smart-homes-in-the-u-s-becoming-more-common-but-still-face-challenges.

Plachkinova, M., Vo, A., Alluhaidan, A., 2016. Emerging trends in smart home security, privacy, and digital forensics. In: 22nd Americas Conference on Information Systems, AMCIS 2016, San Diego, CA, USA, August 11-14, 2016.

Securifi, 2017. Whats New? (Online; accessed 5-October-2017). https://www.securifi.com/whatsnew.

sqlitebrowser, 2017. Db Browser for Sqlite: the Official Home of the Db Browser for Sqlite (Online; accessed 7-October-2017). http://sqlitebrowser.org/.

Sutherland, I., Spyridopoulos, T., Read, H., Jones, A., Sutherland, G., Burgess, M., 2015. Applying the acpo guidelines to building automation systems. In: Tryfonas, T., Askoxylakis, I. (Eds.), Human Aspects of Information Security, Privacy, and Trust. Springer International Publishing, Cham, pp. 684–692.

Z-Wave,,. The Internet of Things Is Powered by Z-wave. Alliance Overview, n.d. (Online; accessed 6-October-2017). https://z-wavealliance.org/z-wave-alliance-overview/.

Zdziarski, J., 2008. IPhone Forensics: Recovering Evidence, Personal Data, and Corporate Assets. O'Reilly Media.

Zigbee,,. The Zigbee Alliance Creates Iot Standards that Help Control Your World, n.d. (Online; accessed 6-October-2017). http://www.zigbee.org/zigbeealliance/.