A Forensic Analysis of Home Automation Devices (FAHAD) Model: Kasa Smart Light Bulb and Eufy Floodlight Camera as Case Studies

Fahad E. Salamh[1]

Abstract

The adoption of Internet of Things (IoT) devices is rapidly increasing with the advancement of network technology, these devices carry sensitive data that require adherence to minimum security practices. The adoption of smart devices to migrate homeowners from traditional homes to smart homes has been noticeable. These smart devices share value with and are of potential interest to digital forensic investigators, as well. Therefore, in this paper we conduct a comprehensive security and forensic analysis to contribute to both fields—targeting a security enhancement of the selected IoT devices and assisting the current IoT forensics approaches. Our work follows several techniques such as forensic analysis of identifiable information, including connected devices and sensor data. Furthermore, we perform security assessment exploring insecure communication protocols, plain text credentials, and sensitive information. This will include reverse engineering some binary files and manual analysis techniques. The analysis includes a data-set of home automation devices provided by the VTO labs: (1) the eufy floodlight camera, and (2) the Kasa smart light bulb. The main goal of the technical experiment in this research is to support the proposed model.

Notes for Practice

- The proposed model follows multi-faceted approach, targeting both responding to an incident and clarifying investigative techniques in the absence of some connected devices such smartphones.

- It has been observed that if an investigator determines that timeline-related and user-identifiable evidence is important, along with absence of the remote-control device (e.g., smartphone or smart hub), a non-traditional digital forensic technique should be adopted—along with validating the outcome of the examination.

- The case study has led us to the discovery that eufy Floodlight Camera stores the password and other credentials in plain text, as well as an access to the filesystem, which contains sensitive data.

- It has been observed that IoT devices share a large volume of data, which require an incident response mindset when investigating smart devices.

Corresponding author [1] Email: fsalamh@purdue.edu Address: Department of Computer and Information Technology, Purdue University, West Lafayette, USA ORCID ID: 0000-0001-7076-2543

1. Introduction

The Internet of Things (IoT) has powered many fields today as it boosts the economy by adding convenience to the customer experience (Mattern & Floerkemeier, 2010; Satoh, 2012; Evans, 2011). By 2020, there will be about twenty billion IoT-connected devices in the world (Hung, 2017). From automobiles to smart homes, the modern style of homes will deploy IoT devices to automate home-based tasks. These tasks include devices such as light bulbs, security cameras, coffee machines, etc. Today, there are a number of IoT devices that carry large volumes of data, which poses challenges to the traditional digital

forensic processes, and creates additional attack vectors for adversaries to exploit. In this paper, we address security forensics challenges related to smart devices. The contributions of this paper are:

- A technical analysis of two smart devices.
- Proposal of an investigative model for forensic analysis of home automation devices that follows a non-traditional digital forensics approach.

This paper is structured as follows: In Section 2, we will discuss previous studies regarding IoT security and forensics. Section 3 will explore the methodology used in this paper, and Section 4 will demonstrate the technical experiment as a proof of concept (POC) that supports the proposed model. Lastly, we will conclude with directions for future research in Section 5.

2. Literature Review

Applying digital forensics tools and techniques to IoT devices might not always work (Watson & Dehghantanha, 2016). These smart devices share a large volume of data and follow a cheap design and technology, which both increase the chances of complexity. Also, the increased number of available IoT devices and the migration from a normal home to a smart home requires investigators to have updated knowledgeable of these technologies.

Recently, these devices have been a target for bad actors, who have been performing denial-of-service (DoS) attacks, installing ransomware, and spying on the privacy of others (Yaqoob et al., 2017; Azmoodeh, Dehghantanha, Conti, & Choo, 2018; S. R. Zahra & Chishti, 2019; A. Zahra & Shah, 2017). There are several components that must be secure, such as the used communication protocols, services, controllers, and endpoints (Alrawi, Lever, Antonakakis, & Monrose, 2019). Most IoT devices rely on cloud-based connect and are controlled either via mobile device or a smart hub. These components are targeted by malicious actors for several reasons. One is to initiate a reconnaissance attack for information gathering, and two is to target the user privacy for financial gain. However, another interesting reason might be data tampering with digital evidence.

Researchers in the paper by (Mundt, Dahn,¨ & Glock, 2014) have conducted an experiment to interfere with IoT devices targeting the behavior of people, while (Awasthi, Read, Xynos, & Sutherland, 2018) presented forensic data acquisition of a smart home hub environment. A conceptual model was developed by (Plachkinova, Vo, & Alluhaidan, 2016) demonstrating security and privacy issues related to smart home devices. The authors included device risks, infrastructure vulnerabilities, privacy violations, and remote breaches in their model. Moreover, research questions regarding the type of data that can be recovered from smart home devices and best practices in collecting and analyzing these devices, were raised by (Hutchinson, Yoon, Shantaram, & Karabiyik, n.d.). This work mainly focuses on studying a standard approach that can be adopted by cyber forensic investigators. An interesting piece of work by (Servida & Casey, 2019) has contributed by extending the current extraction and analysis approaches; however, we argue that the understanding of each process in terms of traditional digital forensics has to be enhanced to minimize the current challenges related to IoT forensics. Therefore, we work on enhancing all processes together considering the fact that IoT devices carry numerous metadata, which require some reconstruction techniques.

Alternatively, a comprehensive analysis of IoT devices (e.g., Google Nest Hub, Google Duo, TP-Link, and Samsung SmartThings) have been performed with identifying relative forensic evidence by employing the association between several factors (Kim, Park, Lee, & Kim, 2020). In addition, researchers have proposed a workflow pertained to smart home forensic investigating, which includes multiple stages (e., experiment, acquisition, analysis, and application). Each stage holds a specific function related to the functions of smart home devices. A generic IoT forensic model has been proposed by (Li, Choo, Sun, Buchanan, & Cao, 2019) as a result of analyzing Amazon Echo considering multiple crime scenarios. The presented model categorized IoT crime scenarios into three classifications IoT as tool, IoT as target, and IoT as witness emphasizing on several elements within the traditional digital forensics process. In the identification phase, researchers suggested a comprehensive list of items related to the identification of IoT devices in a crime scene. For instance, identifying all connected networks and internal/external access points. On the other side, research by (Karabiyik & Akkaya, 2019) has discussed challenges and potential evidence sources in IoT. The categorized expected sources of evidence in IoT fall into several logs of data (i.e., network, web, cloud, and sensor), which mostly require some reconstruction of these recovered metadata.

3. Methodology

The selected methodology of this research is based on several techniques such as reverse analysis, forensic examination, and manual carving analysis. These analyses will be performed using firmware extraction tool Binwalk created in 2010 by ReFirm Lab *(refirm, n.d.),* digital forensics platform Autopsy led by Brian Carrier, and strings command.
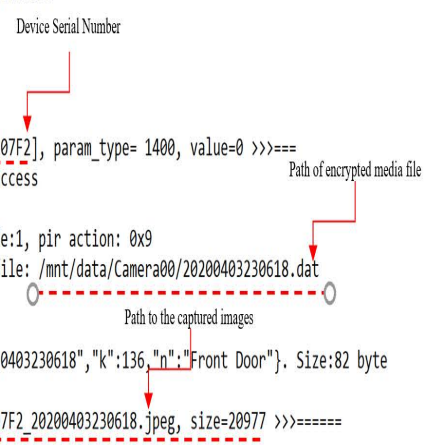
Figure 1. Identifiable information recovered from log.

The theoretical philosophy in this work discusses the differences between traditional and non-traditional digital forensics. Both Figures 6 and 7 illustrate the process of digital evidence. When it comes to the traditional technique, there should not be any reconstruction required to transform metadata to data and then to information that can be logged and reported as a piece of digital evidence. This is because most emerging technology devices share a large volume of data and rely on different communication protocols. Also, some of these devices have different hardware, software, and sensors. An investigator needs to be knowledgeable enough to respond to such an incident, and perform the reconstruction safely without compromising the integrity of data. The acquisition of the selected IoT devices was based on the device architecture and data storage. In the Forensic Analysis of Home Automation Devices Model 4.4, we go through the traditional digital forensics procedures (i.e., identification, preservation, analysis, presentation, and documentation); however, the design and architecture of IoT devices pose some limitations to the analysis phase, where not all digital evidence is accessible on certain tools. Therefore, we perform the analysis on two different software tools to report any limitations.

4. Findings

The analysis follows two approaches here. Firstly, we perform a forensic analysis of each smart device acquired by the VTO lab, and secondly, we conduct a security assessment to report any issues.

4.1. Forensic Analysis of Eufy Floodlight Camera (EFC)

The forensic image of the eufy Floodlight Camera (EFC) device was acquired from the embedded Multi-Media Controller (eMMC) for data storage purposes. Loading the forensic image to Autopsy 4.16.0 reconstructed 585 files with data that was reassembled from the unallocated space of the memory. To break this down, we explored and investigated the 585 files based on their file format, and found that there were 11 images, 14 audios, 6 archives, 0 databases, 110 text, 69 (Executable and Linkable Forma) ELF executables, and 256 octet-streams, respectively. The **eMMC** has a built-in controller that stores chunk of data when deleted. The analysis led us to the discovery of artifacts stored in text files in the following format *fxxxxxxx*, where 'x's represent a randomly generated number.

- Logs pertained to internal and external WiFi connections, and WiFi Received Signal Strength Indicator (RSSI).
- Timestamps of all connections including setup.
- Information related to system size (free and used).
- A peer-to-peer (P2P) network connection reporting each detection with the value *10142*.
- Lights and motion sensors status with timestamps, with an event *ID = 355*.
- The camera type, which is *Hisi*. The parameter *hisi_camera_wifi_data_Assignment* with an ID of *788* and *794* identifies the wifi name, and bssid, respectively. For instance, in our analysis we discovered that the wifi name is *NETGEAR05* and the bssis is *10:da:43:6f:67:28*.
- The serial number of the connected mobile device.
- File path of stored video streams and pictures.

Importantly, the smart cam stores all videos and pictures on the mobile app in the following format `\mnt\data\camera00\year month day\220731.dat.` The file extension indicates that these videos were stored in an encrypted format. Also, the log files include the P2P connection activity, showing remote address, local area network (LAN), and wireless local area network (WLAN) IP addresses. These metadata aid an investigator when linking supportive information with data acquired from the mobile device. Conducting a forensic analysis on the mobile app is out of the scope of this research, as our concern here is to walk through the digital investigation process of smart devices—not mobile apps. The process of mobile app forensics should not be challenging and might not be of interest to the investigators. The analyzed logs pro-vide extensive information related to integrity and validity of recorded media files by the smart cam. It is very important to ensure that these data have not been tempered with and they are accurate should they be presented in court. When a snapshot is taken by the smart cam, the logs show the full path of the image including the device serial number as follows `/mnt/data/video/T8420H01194807F2_20200403230525.jpeg`. When motion is detected, the assigned ID number is `131076`. This connectivity is based on cloud storage and network; therefore, the logs might include IP addresses relevant to the cloud storage device.

```
2020-04-03 23:06:19.160 [INFO][local_storage_interface.c:pir_trigger_handle_by_channel:1569] - camera: 0, waiting stream...
2020-04-03 23:06:19.167 [INFO][local_storage_interface.c:write_prebuf_record_file:1686] - prebuf frame 1 frame_num=15,16, timestamp=1585976774154
2020-04-03 23:06:19.175 [INFO][local_storage_interface.c:write_prebuf_record_file:1686] - prebuf frame 2 frame_num=15,16, timestamp=1585976775155
2020-04-03 23:06:19.196 [INFO][local_storage_interface.c:write_prebuf_record_file:1686] - prebuf frame 3 frame_num=15,15, timestamp=1585976776155
2020-04-03 23:06:19.228 [INFO][local_storage_interface.c:write_prebuf_record_file:1686] - prebuf frame 4 frame_num=15,16, timestamp=1585976777155
2020-04-03 23:06:19.242 [INFO][local_storage_interface.c:write_prebuf_record_file:1686] - prebuf frame 0 frame_num=15,16, timestamp=1585976778155
2020-04-03 23:06:19.261 [INFO][local_storage_interface.c:write_prebuf_record_file:1868] - prebuf frame num:75 620959, time:5 1585976774154
2020-04-03 23:06:19.262 [INFO][local_storage_interface.c:zx_storage_write_thread:2464] - start upload snapshot use msq.
2020-04-03 23:06:19.262 [INFO][floodlight_interface.c:zx_storage_push_thread:10632] - async process type: 0, /mnt/data/Camera00/20200403230618.dat
2020-04-03 23:06:19.264 [INFO][cloud_storage_interface.c:zx_putdata_aws_s3:841] - ****** put[20977]:/mnt/data/video/T8420H01194807F2_20200403230618.jpeg to aws s3 start ******
2020-04-03 23:06:19.551 [INFO][as_interface.c:zx_http_push_msg:6521] - ========= http push msg success, err.code=0 ========
2020-04-03 23:06:20.073 [INFO][as_interface.c:zx_hub_uptoken_request_ex:4109] - ======<<< err.code=0 >>>======
2020-04-03 23:06:20.233 [INFO][ppcs_interface.c:zx_p2p_listen:8973] - PPCS_Listen, ret -3
2020-04-03 23:06:20.234 [INFO][ppcs_interface.c:zx_get_p2p_connect_num:1708] - cur p2p remain connect number: 0( -1 -1 -1 -1 )
2020-04-03 23:06:20.740 [INFO][ppcs_interface.c:zx_p2p_listen:8971] - ppcs listen ...
2020-04-03 23:06:20.746 [INFO][floodlight_interface.c:zx_hisi_write_drop_caches_only:2193] - put_to_aws lock busy, ret = 16
2020-04-03 23:06:20.825 [INFO][local_storage_interface.c:zx_storage_write_thread:2481] - camera_0, frame_num=101
2020-04-03 23:06:20.819 [INFO][cloud_storage_interface.c:zx_putdata_aws_s3:996] - ****** put:/mnt/data/video/T8420H01194807F2_20200403230618.jpeg success, filesize:20977******
2020-04-03 23:06:20.833 [INFO][local_storage_interface.c:zx_put_snapshot:5148] - snapshot: put data snapshot jpeg aws s3 ok, use time 1569.
2020-04-03 23:06:27.026 [INFO][local_storage_interface.c:zx_storage_write_thread:2680] - end_time=1585976787019,start_time=1585976774154,now_time=1585976787025
2020-04-03 23:06:27.027 [INFO][local_storage_interface.c:zx_storage_write_thread:2681] - camera: 0, record end, record time: 12871ms, frame_num:194
2020-04-03 23:06:27.067 [INFO][local_storage_interface.c:zx_upload_record:4980] - upload hub history record start...storage_type=1
2020-04-03 23:06:27.068 [INFO][led_interface.c:zx_led_debug_print:183] - set led, record set white led off
2020-04-03 23:06:27.080 [INFO][led_interface.c:zx_set_led_automatically:355] - set led white on, network connectted, bind ok.
2020-04-03 23:06:27.081 [INFO][local_storage_interface.c:close_local_fp_by_channel:1993] - close file: /mnt/data/Camera00/20200403230618.dat
2020-04-03 23:06:27.082 [INFO][local_storage_interface.c:zx_storage_write_thread:2680] - sem wait...
2020-04-03 23:06:28.341 [INFO][as_interface.c:zx_upload_hub_history_record:3289] - code=0 file:/mnt/data/Camera00/20200403230618.dat
2020-04-03 23:06:28.348 [INFO][local_storage_interface.c:zx_upload_record:5031] - upload hub history record ok, file [/mnt/data/Camera00/20200403230618.dat][].
2020-04-03 23:06:35.413 [INFO][floodlight_interface.c:zx_fd_network_detection:10142] - internet ip:73.14.136.205
```

Timestamps of video recordings

Upload IP address

Figure 2. Logs of uploading and streaming activities

```
0x00000000: 5B 77 69 66  69 5D 0A 73  73 69 64 20  3D 20 4E 45   [wifi].ssid = NE
0x00000010: 54 47 45 41  52 30 35 0A  6B 65 79 20  3D 20 31 32   TGEAR05.key = 12
0x00000020: 33 34 35 36  37 38 0A 0A  5B 6E 65 74  77 6F 72 6B   345678..[network
0x00000030: 5D 0A 64 68  63 70 20 3D  20 6F 66 66  0A 69 70 20   ].dhcp = off.ip
0x00000040: 3D 20 31 39  32 2E 31 36  38 2E 30 2E  38 38 0A 6E   = 192.168.0.88.n
0x00000050: 65 74 6D 61  73 6B 20 3D  20 32 35 35  2E 32 35 35   etmask = 255.255
0x00000060: 2E 32 35 35  2E 30 0A 67  61 74 65 77  61 79 20 3D   .255.0.gateway =
0x00000070: 20 31 39 32  2E 31 36 38  2E 30 2E 31  0A 0A 5B 66    192.168.0.1..[f
0x00000080: 61 63 74 6F  72 79 5D 0A  66 6F 63 75  73 20 3D 20   actory].focus =
0x00000090: 30 0A 69 70  65 72 66 20  3D 20 30 0A  61 67 69 6E   0.iperf = 0.agin
0x000000a0: 67 20 3D 20  31 0A 0A 5B  63 75 74 5D  0A 70 65 72   g = 1..[cut].per
0x000000b0: 6F 69 64 20  3D 20 31 35  0A 0A                      oid = 15..
```

Figure 3. Connected WiFi and password (plain text)

Figure 4. Decompressed system files

Figure 5. Recovery of encoded geolocation data.

4.2. Security and Reverse Engineering Analysis

Using Binwalk, we extracted the binary file stored in the unallocated space, revealing data such as security certificates and system configuration.

We were able to recover the password in plain text format from several paths. One of them was the unallocated space recovered from the wpa supplicant configuration file. The password was *12345678* under the *etc/wpa_suplicant* folder

4.3. Forensic Anlysis of the Kasa Smart Light Bulb

The chip-off data recovery does not hold any invaluable data that can be beneficial for the investigation. The mobile app analysis has led us to the discovery of a database file called **iot.db** that has five tables including accounts, devices, locations, scenes, and device groups, respectively. The following list discusses the data that this database carries:

- Accounts: device ID, creation time, updated time, email, password, token, refresh token, first and last names
- Devices: device ID, creation time, updated time, IP address, software and hardware versions, cloud status, and RSSI
- Locations: device ID, account ID, creation time, updated time, timezone, latitude, longitude, and home settings
- Scenes: device ID, account ID, image URL, and usage count
- Device ID, account ID, creation time, updated time, and type

Due to the limitation of data population, the analysis revealed that only the location table holds data. For instance, the latitude and longitude of the IoT device stored in base64 format **XVZJ9gJ60LooZlDzd/o1eA==**, when decoding the base64 value, we got **39.7392** (See Figure 5).

4.4. Forensic Analysis of Home Automation Devices (FAHAD) Model

The proposed model follows multi-faceted approach, targeting both responding to an incident and clarifying investigative techniques in the absence of some connected devices such smartphones. Sometimes an investigator investigates an incident that has many missing elements; therefore, this model concentrates on these types of incidents to update the current IoT forensic procedures. To this end, we emphasize the importance of setting up strong credentials when creating usernames and passwords for these devices, as bad actors might be able to sniff the network capture and brute force login to the device and gain access to the system. These behaviors might also lead to tampering with evidence data leaving, false or no traces of the attempts. Moreover, the integrity of recorded videos should match the logs we illustrated in this research. An investigator should verify the logs of all streamed data. When it comes to devices such as the smart light bulb, a good amount of information can be

ISSN xxxx-xxxx (online). The International Journal of Cyber Forensics and Advanced Threat Investigations under a Creative Commons License, Attribution - NonCommercial-International 4.0 License (CC BY-NC 4.0)

5

retrieved from these devices in order to clarify many clues related to a crime—for instance, connected device ID, timestamps, and account ID. These might lead to a better understanding of who is controlling these devices at home, and provide a meaningful trace of their activities. At the same time, the security of these devices is very important, and it seems to be neglected by individuals and manufacturers. The eufy Floodlight Camera has the password and other credentials in plain text, as well as an access to the file system, which contains sensitive data. Factors of IoT devices influencing traditional digital forensics have been discussed in the paper by Yaqoob et al. (Yaqoob, Hashem, Ahmed, Kazmi, & Hong, 2019). In our study, we encountered some of these factors (i.e., limited visibility, short survival period, and lack of logs). A framework was proposed by Kim et al. (Kim et al., 2020) that demonstrates phases of smart home forensic investigation. In this work, we propose a non-traditional model 8 that demystifies important processes during identification, examination, and presentation of smart home forensic investigation. The app of Kasa cam contains thumbnails that can be preserved from the following path /cache/image manager disk cache/32bytes hex value.0 (Kim et al., 2020). Also, the authors claimed that the Android app stores an XML file that contains information such as device ID, device model, locations, accounts, and hardware and software versions. In our work, we conduct our analysis on the iOS app, which contains similar artifacts such as the iot.db database file, but the app stores information in a group.tplink.Kasa.plist file. A discussion on IoT features and architecture pertained to security, cybercrime, and digital forensics enhance the overall application of smart things (Atlam, Alenezi, Alassafi, Alshdadi, & Wills, 2020).
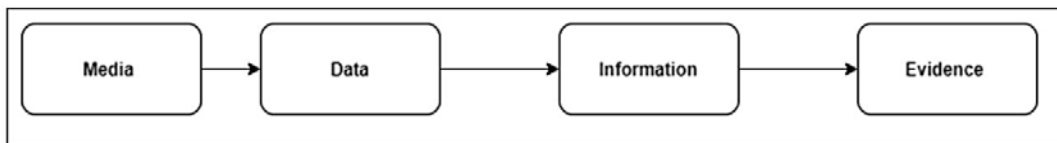

Figure 6. A traditional process of digital evidence.

The proposed model in figure 8 emphasizes the importance of a non-traditional approach in responding to cybercrimes related to home automated devices. Basically, the model begins with a process that distinguishes traditional versus non-traditional methods. For instance, if an investigator determines that timeline-related and user-identifiable evidence is important, along with absence of the remote control device (e.g., smartphone or smart hub), a non-traditional digital forensic technique should be adopted—along with validating the outcome of the examination. Moreover, sometimes the examination process encounters an encrypted piece of data, which requires an investigator to seek available decoding techniques. Therefore, each process of the non-traditional approach is slightly different from the known processes of digital forensics. For instance, identification and acquisition processes might pose a challenge to an investigator, leading to failure in acquiring the data. It is crucial to identify all possible connected devices, chips, and electronic sensors, and to be able to select the correct acquisition methodology. The analysis process is completely different from what is currently known. We insist on the need for an incident response mindset when investigating smart devices. As mentioned earlier, these devices share a large volume of data, and a traditional investigation will not result in a good conclusion. Today, these devices might be hacked and tampered with; therefore, the accurate digital evidence should answer all of the six key questions (who, when, why, where, what, and how). For an investigator to be able to answer these questions, it is not similar to the examination of computer forensics. Thus, one needs to be able to manually carve data and analyze available logs to be correlated with other events (i.e., sensor and system logs). Finally, the validation process ensures that the investigation followed accurate procedures and met the digital forensics and data integrity standards.
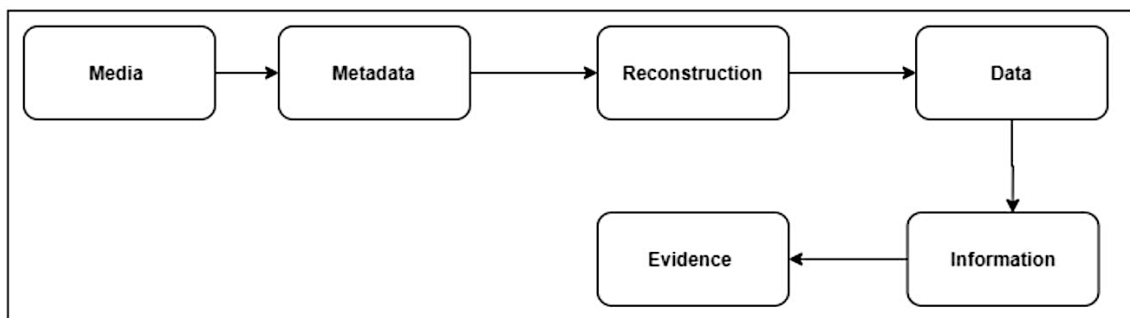

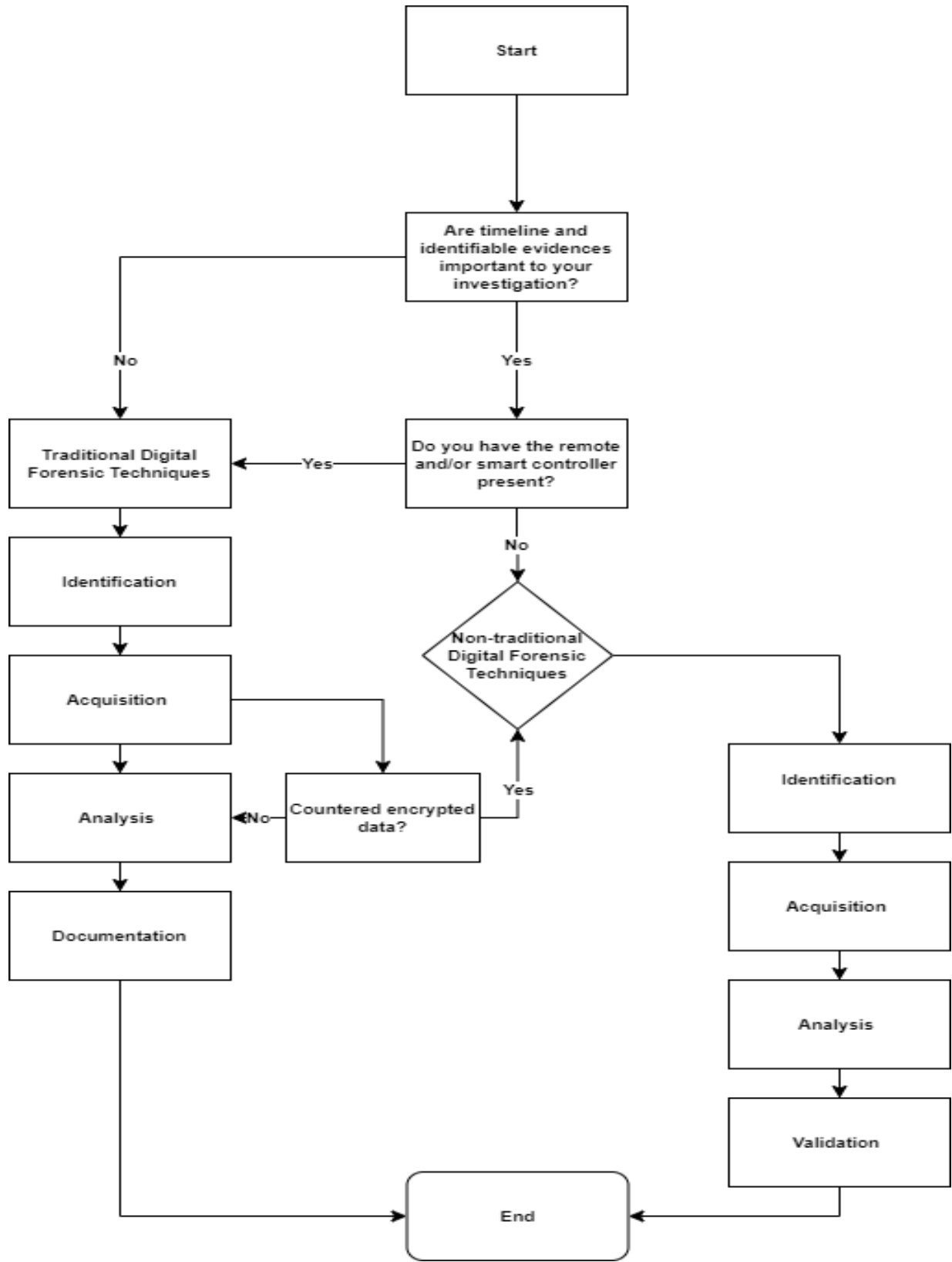**Figure 7.** A non-traditional process of digital evidence.

Figure 8. Forensic analysis of home automation devices model.

5. Conclusion

This research analyzed two smart devices targeting a generalized model that can be applied to other IoT devices. The model concentrates on non-traditional techniques, and all phases of the model were supported by the conducted technical experiment. This model does not cover the security aspect of IoT devices; therefore, we plan to include incident response and variance attack vectors into the model for future work.

Declaration of Conflicting Interest

Funding

Acknowledgments

References

Alrawi, O., Lever, C., Antonakakis, M., & Monrose, F. (2019). Sok: Security evaluation of home-based iot deployments. In 2019 IEEE symposium on security and privacy (sp) (pp. 1362-1380). doi:10.1109/SP.2019.00013

Atlam, H. F., Alenezi, A., Alassafi, M. O., Alshdadi, A. A., & Wills, G. B. (2020). Security, cybercrime, and digital forensics for IoT. In Principles of internet of things (IoT) ecosystem: Insight paradigm (pp. 551-577). Springer. doi:10.1007/978-3-030-33596-0_22

Awasthi, A., Read, H. O., Xynos, K., & Sutherland, I. (2018). Welcome pwn: Almond smart home hub forensics. Digital Investigation, 26, S38-S46. doi:10.1016/j.diin.2018.04.014

Azmoodeh, A., Dehghantanha, A., Conti, M., & Choo, K.-K. R. (2018). Detecting crypto-ransomware in IoT networks based on energy consumption footprint. Journal of Ambient Intelligence and Humanized Computing, 9(4), 1141-1152. doi:10.1007/s12652-017-0558-5

Evans, D. (2011). The internet of things: How the next evolution of the internet is changing everything. CISCO white paper, 1(2011), 1-11.

Hung, M. (2017). Leading the IoT, Gartner Insights on how to lead in a connected world. Gartner Research, 1-29.

Hutchinson, S., Yoon, Y. H., Shantaram, N., & Karabiyik, U. (n.d.). Internet of things forensics in smart homes: Design, implementation, and analysis of smart home laboratory.

Karabiyik, U., & Akkaya, K. (2019). Digital forensics for IoT and WSNS. In Mission-oriented sensor networks and systems: Art and science (pp. 171-207). Springer. doi:10.1007/978-3-319-92384-0_6

Kim, S., Park, M., Lee, S., & Kim, J. (2020). Smart home forensics-data analysis of IoT devices. Electronics, 9(8), 1215. doi:10.3390/electronics9081215

Li, S., Choo, K.-K. R., Sun, Q., Buchanan, W. J., & Cao, J. (2019). Iot forensics: Amazon Echo as a use case. IEEE Internet of Things Journal, 6(4), 6487-6497. doi:10.1109/JIOT.2019.2906946

Mattern, F., & Floerkemeier, C. (2010). From the internet of computers to the internet of things. in From active data management to event-based systems and more (pp. 242-259). Springer. doi:10.1007/978-3-642-17226-7_15

Mundt, T., Dähn, A., & Glock, H. W. (2014). Forensic analysis of home automation systems. In 7th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs 2014).

Plachkinova, M., Vo, A., & Alluhaidan, A. (2016). Emerging trends in smart home security, privacy, and digital forensics.

Satoh, K. (2012). Ieee proof. IEEE vEhIcular tEchnology magazInE.

Servida, F., & Casey, E. (2019). IoT forensic challenges and opportunities for digital traces. Digital Investigation, 28, S22-S29. doi:10.1016/j.diin.2019.01.012

Watson, S., & Dehghantanha, A. (2016). Digital forensics: the missing piece of the internet of things promise. Computer Fraud & Security, 2016(6), 5-8. doi:10.1016/S1361-3723(15)30045-2

Yaqoob, I., Ahmed, E., ur Rehman, M. H., Ahmed, A. I. A., Al-garadi, M. A., Imran, M., & Guizani, M. (2017). The rise of ransomware and emerging security challenges in the internet of things. Computer Networks, 129, 444-458. doi:10.1016/j.comnet.2017.09.003

Yaqoob, I., Hashem, I. A. T., Ahmed, A., Kazmi, S. A., & Hong, C. S. (2019). Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges. Future Generation Computer Systems, 92, 265-275. doi:10.1016/j.future.2018.09.058

Zahra, A., & Shah, M. A. (2017). Iot based ransomware growth rate evaluation and detection using command and control blacklisting. In 2017 23rd international conference on automation and computing (icac) (pp. 1-6). doi:10.23919/IConAC.2017.8082013

Zahra, S. R., & Chishti, M. A. (2019). Ransomware and internet of things: A new security nightmare. In 2019 9th international conference on cloud computing, data science & engineering (confluence) (pp. 551-555). doi:10.1109/CONFLUENCE.2019.8776926