Forensic Analysis of the August Smart Device Ecosystem

Shinelle Hutchinson
Department of Computer and Information Technology
Purdue University
West Lafayette, IN, 47907
hutchi50@purdue.edu

Umit Karabiyik
Department of Computer and Information Technology
Purdue University
West Lafayette, IN, 47907
umit@purdue.edu

***Abstract*—Smart Homes are becoming increasingly popular with homeowners investing in new internet-connected technologies, from smart plugs to smart appliances. One particular area where homeowners use smart devices is at the front door, as they install smart doorbells and smart locks. In this paper, we embark on an investigative journey into the August smart device ecosystem, specifically looking at the interaction between the August Smart Doorbell Pro and the August Smart Lock Pro, with their controlling app, August Home. We aim to determine what type of data forensic investigators may be able to recover about these devices and their use. We also explore how these devices interact with each other, noting any privacy issues that may be discovered. We found that a wealth of forensic data could be recovered, particularly from rooted Android devices and jailbroken iPhone devices. Information about the owner of the smart device, guests who were given access to the devices, device interactions, and pictures taken by the doorbell camera, were all recoverable in plaintext. Our results also show that user's GPS coordinates associated with the lock's Auto-Unlock feature were recovered only from a rooted Android device.**

***Index Terms*—Forensic Investigation, Internet of Things (IOT), IoT Forensics, Mobile Forensics, Privacy, Smart Home**

I. Introduction

Internet of Things (IoT) devices are being made to generate, interact, and share data with each other. However, there is an important question to ask: How well do these devices maintain or protect user data or privacy during their operations? One of the most popular smart devices homeowners now employ is the smart doorbell camera. According to recent statistics in [1], the global smart doorbell market size will grow by 2.63 billion USD during 2019-2023. These devices allow users to see who is at their front door without having to open the door physically. It also sends alerts to users when motion is detected, provides 2-way communication, and some even record the moments leading up to a motion detection event.

Another popular IoT device being used together with the doorbell camera is a smart lock. These devices allow users to lock or unlock their door with the tap of a button, or just by entering or leaving a set perimeter around the lock (i.e., geofence). These smart devices make homeowners' lives more convenient, but at what potential cost to user privacy. At the time of this writing, there has been no previous research into the August smart device ecosystem, although there is other work available on individual August products [2].

In this paper, we investigate the August Smart Doorbell Cam Pro and August Smart Lock Pro, focusing on their controlling application (app), called August Home, that is used to interact with these devices. We investigate this app on both Android and Apple iOS devices to determine what forensically relevant information can be acquired. More precisely, we determine what information can be recovered from the app, that can help investigators during an investigation. We also investigate how these devices interact with each other and identify what data is being shared, particularly any privacy concerns that result from their interactions. We provide our methodology in detail and discuss the challenges faced during our study. These results will be beneficial for forensic investigators who may encounter these and similar devices during an investigation. We also highlight relevant data that could be useful and identify where this data can be found.

The rest of this paper is organized as follows. Section II provides background information on IoT forensics and Smart Home devices. In Section III we detail the methodology followed in this study while in Section IV we present our findings. In Section V we discuss the relevance of our findings and lastly, we conclude our work in Section VI.

II. Literature Review

In this section, we highlight some of the previous related literature that we have studied. There have been several forensic frameworks proposed for IoT Forensics, and some of them are highlighted here.

Goudbeek et al. developed a 7-phase investigation framework for the smart home environment and evaluated its utility using three case studies in [3]. The authors also explored the types of potential evidential data in a smart home environment and how to go about acquiring such data. They were able to determine a range of artifacts that could be recovered from IoT devices. The authors also showed that potential evidentiary data could be in the central unit, in a microprocessor close to the sensor, in a cloud solution, or with a third-party service provider [3].

In [4], Meffert et al. emphasized many complications that IoT devices introduce, including the lack of standardization

978-1-7281-5628-6/20/$31.00 ©2020 IEEE

among devices, the different communication protocols that these devices use and the fact that some of these devices use Real-Time Operating Systems (RTOS) which does not store much, if any, data. To help bridge the gap due to these challenges, the authors proposed a generalized framework called Forensic State Acquisition from Internet of Things, to collect state data from IoT devices.

The authors utilized the power of openHAB [5] to serve as their Forensic State Acquisition Controller (FSAC). All of the test IoT devices (door sensor, motion sensor, thermostat) were connected to the FSAC. The authors performed various experiments using each sensor (open door/close door/activate motion sensor) and collected the necessary state data from openHAB log files. This framework is unable to collect stored data on IoT devices or their controllers (e.g., smartphone app), nor is it able to recover deleted data. Our research goes beyond just investigating the state data from IoT devices as we analyze both the Android and iOS apps for the August devices as well as the interconnected relationship between both devices.

Previous researches have investigated the privacy of IoT devices. In particular, Apthorpe et al. [6] and Dorai et al. [7] were both able to show significant privacy leakage from popular IoT devices. In [6], the researchers investigated several IoT devices' network traffic to determine if any privacy leakage occurred. They found that although all the traffic was encrypted, there were spikes in network traffic for the devices that corresponded to when the user interacted with the devices. The authors recognized this as a privacy leakage issue as the network spikes indicate when a user is actively using the IoT device. A similar methodology would be followed during our experiments to investigate the network traffic of the August IoT devices.

Apthorpe et al. in [7] investigated a single brand of IoT devices they termed, the Nest Ecosystem, and simultaneously proposed a tool, the Forensic Evidence Acquisition and Analysis System (FEAAS). FEAAS automates the forensic analysis process of IoT data from iOS devices and provides inferences about user actions. The authors did not investigate the interaction between Nest devices as we intend to do during our research on the August ecosystem. We believe this investigation would hold pertinent evidentiary data that investigators can leverage during a case.

In other research, Chung et al. [8] investigated the Amazon Alexa ecosystem by analyzing two Amazon Echo Dot devices using their proof-of-concept tool, Cloud-based IoT Forensic Toolkit (CIFT). CIFT combines cloud-native forensics with client-side forensics to extract potential evidentiary data from Amazon Echo devices via the cloud, Android, and iOS apps and Chrome web browser [8]. Articles [7] and [8] are similar in that they both investigate IoT devices by looking at their client apps and web browser cache. However, authors in [8] go a step further to also investigate the cloud data for the respective devices. Although this research is related to our work, in that we will be investigating both the Android and iOS apps related to August IoT devices, IoT cloud forensics is outside the scope of our current research.

Ho et al. in [2] noted that there was limited research into the security implications of smart devices and the many new ways they allow user interactions. In addressing this issue, the authors investigated five smart locks, one of which was from August. Each lock was subjected to two categories of attacks: state consistency attacks and unwanted unlocking. In regard to the August lock, the researchers showed that this lock was vulnerable to both attacks. According to the results presented in [2], the August lock can allow someone whose access was recently revoked, to unlock the lock still if their smartphone with the August Home app was not connected to the Internet. This unwarranted behavior occurred because the lock needs to connect through the user's smartphone Internet connection in order to get server updates, including revocation list updates. They also showed how the August lock is susceptible to unwanted unlocking. In line with this research, we investigate our August Smart Lock Pro to determine if a guest user can maintain access to the lock even after having their access revoked by the lock's owner.

Authors in [9] identified some of the security challenges within IoT environments as Authentication, Authorization, and Privacy as well as some of the forensic challenges, including evidence identification, collection and preservation, and evidence analysis and correlation. These issues have been explored by several other researchers including [3], [4] and [6].

A. Smart Locks

Smart locks require three basic components to work: a physical lock device, a smartphone app, and access to a web server. Once these are all available, a user can interact with the lock through the app. In order to interact with the August Smart Lock Pro, users need to establish a Bluetooth connection with the smart lock or a WiFi connection. The August smart lock can use WiFi if it's synced to the August Doorbell Pro, or the user has the August Connect WiFi Bridge setup. A WiFi connection then allows users to interact with the smart lock remotely from virtually anywhere in the world. As of April 2020, August is yet to release its new 'WiFi Smart Lock' which does not require additional hardware to access the Internet.

The August Smart Lock Pro (1) allows users to unlock/lock the device through the app, (2) provides logging of lock interactions, (3) allows for auto-unlocking through the use of a geofence, (4) has auto-lock capabilities, and (5) provides users the ability to grant virtual keys to friends or guests so they can interact with the lock without the owner needing to be physically available. All these features add to the convenience afforded to homeowners and make these devices more appealing.

B. Smart Doorbells

Smart doorbells are internet-connected camera devices that afford homeowners the luxury of 'answering' their front door without having to open the door manually. The August Smart Doorbell device, specifically, allows users to view live streams

of the doorbell camera, record video, alerts the user to motion events, and when paired with its corresponding smart lock, allows the user to operate the lock during a doorbell call, all from the August app.

III. Methodology

This study follows the forensic investigation model suggested by the National Institute of Standards and Technology (NIST) for extracting and examining the images from the devices [10]. Three smartphone devices were used in this study, an iPhone 7 running iOS 12 and two Samsung S7's running Android 7.0 (Nougat) and Android 8.0 (Oreo). These devices were chosen because they represent a large percentage of the global user base who may be interested in the results of this study. These devices are also proven to be jailbroken or rooted without significant challenges.

Jailbreaking/Rooting a device is the process in which the operating system is changed in such a way as to give users more access to the file system. This process changes the state of the device and should be used only when absolutely necessary [11].

The forensic software tools used for the acquisition of these devices include Magnet ACQUIRE (Version 2.21.0.18374), Magnet AXIOM (Version 3.7.0.1679), and MSAB XRY (Version 7.12.0, Build: 25665). AXIOM and XRY are both widely used in law enforcement investigations. We used BulkExtractor (Version 1.5.2) [12] to carve files out of the Magnet ACQUIRE image since ACQUIRE performs a physical acquisition of the device. This means that the image created would be a bit-by-bit copy of the device and lacks a file system structure. Alternatively, Magnet AXIOM and XRY both perform logical acquisitions when making an image. This means that the data is accessed by the Android file system [13]. Wireshark (Version 3.0) and an Alfa network adapter (Model # AWUS1900) were used to acquire the network traffic generated from the IoT devices and smartphones.

Extraction and analysis of the phone images were performed on a Dell Optiplex 7060 computer running Windows 10 Education (Version 1809) 64-bit Build 17763.805 with 16 GB of RAM memory and an Intel(R) Core(TM) i7-8700 processor.

A. Lab Setup

To conduct this study, we set up our own mini-smart home which included a TP-Link Archer AC1900 router, an Alfa AWUS1900 network adapter which allowed us to capture all traffic passing through the network, three smartphones (an iPhone 7 and two Samsung Galaxy S7 devices) and the August Smart Lock Pro (Model# ASL-03,AC-R1) and the August Smart Doorbell Pro (Serial# D2GXY00198) IoT devices.

B. Data Population

In preparation for device population in this study, new iCloud and Google accounts were created and the smartphones were then populated as follows:

- Factory reset each device to defaults.
- Signed into the new iCloud, and two Google accounts on the iPhone and Galaxy S7's, respectively.
- Acquired each devices' baseline image using Magnet AXIOM Process.
- Populated each device with data, as necessary, using the NIST guidelines for mobile device population [10].
  - Installed the August Home app from the App Store and the Google Play Store.
  - Created two (2) August accounts through the app, one used on the Galaxy S7 (Nougat), and the other on the iPhone 7.
  - Used each smartphone to interact with the August IoT devices.
- Collected network traffic while using each device.
- Performed the second acquisition of both devices.
- Rooted the Galaxy S7 (Nougat).
- Jailbroke the iPhone 7.
- Performed a full acquisition of all three devices.
- Examined all images using Magnet AXIOM Examiner and MSAB XRY.

The NIST guidelines for mobile device data population [10] was utilized for the initial population of user data on each smartphone. We set up the August Smart Doorbell and Smart Lock in our lab and interacted with both devices using the August Home app on the smartphones. We considered different interactions for our investigation, which are described below. During each interaction, we captured the network traffic that was generated.

1) Smart Lock Pro Interaction: We created an August account, signed into the August Home app, and performed initial setup procedures for the smart lock by following the on-screen instructions. Once the smart lock was successfully paired with the smartphone, we used the app to do the following:

- Unlocked and locked the smart lock.
- Enabled Auto-Lock feature to work after 30 seconds.
- Enabled and used Auto-Unlock feature.
- Granted virtual key to second Galaxy S7 (Oreo) device (S7Friend).
- Used S7Friend to unlock/lock the smart lock.
- Revoked virtual key from S7Friend and tried interacting with smart lock.

2) Smart Doorbell Pro Interaction: After interacting with the smart lock, we added a new device, the doorbell, and performed the initial setup by following the on-screen instructions. Once the doorbell was successfully paired with the smartphone and WiFi, we used the app to do the following:

- Enabled and tested the motion detection feature.
- Rang the doorbell and answered the call on the app.
- Viewed the live stream of the doorbell.
- Granted virtual key to second Samsung Galaxy S7 device (S7Friend) to access doorbell.
- Used S7Friend to view doorbell video stream and answer when doorbell rang.

- Revoked virtual key from S7Friend and tried interacting with doorbell.

3) Smart Doorbell and Smart Lock Interaction: In this final interaction, we synced the smart lock to be used with the doorbell camera and performed the following actions:

- Rang the doorbell and answered the call form the app.
- While on call, locked/unlocked the smart lock directly.

C. Acquisition

We opted to forensically image each smartphone device at three critical points: (1) the baseline image, (2) the image after interacting with the devices under investigation, and (3) another image taken after rooting/jailbreaking the device.

With the iPhone 7, we acquired all three images with Magnet AXIOM. Before taking the last image, we jailbroke the device using Chimera [14] app. One of the Galaxy S7 devices (S7Friend) was already rooted before being used in this study, and we acquired its images using MSAB XRY. The base image and unrooted image for the Galaxy S7 device (S7Owner) were also acquired using Magnet AXIOM. However, after getting this second image, Magnet's recovery image was not automatically taken off the device after the acquisition and left the device inoperable. We were able to root this Galaxy S7 using Samsung's ODIN tool [15] and a custom binary file from TWRP [16]. Once the device was rooted, we acquired it with MSAB XRY and Magnet ACQUIRE. Jailbreaking/Rooting the devices gave us full access to each phone's file system, where we expected to recover even more relevant data.

From the rooted acquisition of the Galaxy S7 devices, August data was found in the */data/data/com.august.luna* folder while on the jailbroken iPhone, the August data was found under the application ID folder *DA89397F-ADBB-44C5-93D2-11ED6FD2A9E4* and the app package name *com.august.iossapp*.

IV. Results

After analyzing each device image, we recovered a considerable amount of forensically relevant data. In this section, we present our results in detail.

Table I provides a summary of artifacts that can be recovered from each device. User Data includes name, e-mail address, phone number, and associated August ID for each August profile. User GPS Data refers specifically to GPS coordinates associated with the user's movements while Device Information includes any interactions made with the August devices, including actions like lock/unlock events, auto-unlock events, doorbell call events, and motion detection events. Plaintext passwords were not recoverable from any device while user GPS data was only recoverable from a rooted Android.

A. Android

During our analysis, we were unable to recover user data from the unrooted Android image. However, information about how the user interacted with the August Home app was recovered from the *usage_stats.txt* file. This file details when a specific app Activity (screen) was shown to the user and when it was put in the background. Additionally, the 20 most recent SQL queries that were run for each database within the August Home app was recovered from the *dbinfo.txt* file. The locations of these files are shown in Table II.

The rooted Android images contained a wealth of relevant data (see Table III), such as user profile information, which includes user's full name, e-mail address, phone number, August ID, profile picture and house picture. This information is found in the log files and the *ModelDatabase.db* file in the MSAB XRY image and the *json.txt* file in the Magnet ACQUIRE image. The *json.txt* file contained hyperlinked URLs for the doorbell pictures that were taken due to a motion detection event. Examples of these recovered pictures are shown in Fig. 1. However, the URLs stopped working after about two months. Fig. 2 shows an example of the event logs kept in the *ModelDatabase.db* database. The *ModelDatabase.db* file also holds information regarding the August devices associated with the August account and device interaction data. August provides an Auto-Unlock feature that uses a geofence to determine when to unlock the August Smart Lock automatically. If this feature is utilized, the user's GPS location data will be found in the *LocationDatabase.db* file. Cached image data from the Doorbell Camera was also recovered from the *image_manager_disk_cache* folder on the MSAB XRY image and from the *json.txt* from the Magnet ACQUIRE image.

Specifically, the S7Friend guest device contained additional data within the *RemoteLogQueue.db* file which stores data related to how the S7Friend user interacted with the August devices. During our experiments, we connected the S7Friend device to WiFi and revoked its access (from the Galaxy S7 Owner phone) to the smart lock and smart doorbell. S7Friend was still able to interact with the August devices for a brief period (under 10 seconds) before access to the devices was denied.

B. iOS

Unlike the unrooted Android image, the non-jailbroken iPhone image reveals more relevant data. Information about the August devices attached to the logged-in account was found in the *entities.plist* file. Information that is related to the Auto-Unlock feature use was found in the *group.com.august.general-cross-process.plist* file. However, unlike in Android, this log does not contain actual GPS coordinates. Instead, it shows when the Auto-Unlock feature was enabled, when the owner left the home geofence area and returned, and when Auto-Unlock succeeded in unlocking the August Smart lock. Pictures that are taken by the doorbell camera were also recovered during our analysis. However, this was only possible because the user downloaded the picture from the August Home app onto their smartphone device, after a motion detection event. Table IV shows the location of all relevant information on the non-jailbroken iPhone image.

After jailbreaking the iPhone 7, more detailed log files and cached data were recovered. All relevant data were found under the *private\var\mobile\Containers\Data*

TABLE I
SUMMARY OF RECOVERABLE AUGUST ARTIFACTS

Artifact	Android		IOS	
	Unrooted	Rooted	Non-Jailbroken	Jailbroken
User Data	NO	**YES**	NO	**YES**
User Password	NO	NO	NO	NO
User GPS Data	NO	**YES**	NO	NO
Device Interactions	NO	**YES**	**YES***	**YES**
Doorbell Camera Pictures	NO	**YES**	**YES***	**YES**

*Limited amount of data recovered.

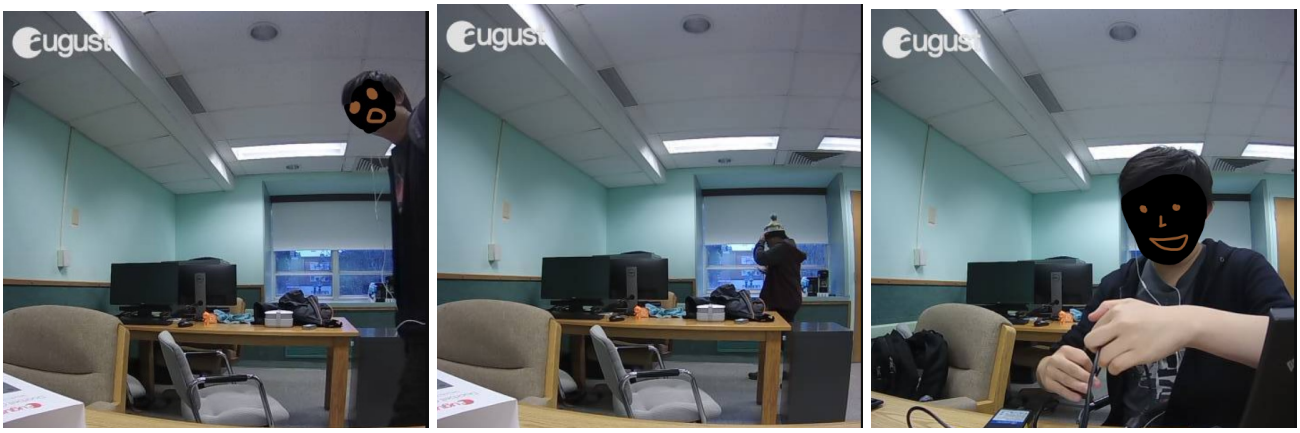

Fig. 1. Pictures of automatically uploaded doorbell pictures due to motion detection event.

	houseID	rawJson	timestamp
1	9ea93fdc-3313-4464-812d-2ff49545fcf6	{"entities":{"device":"b5ec217cee0f","callingUser":"deleted","otherUser":"deleted","house":"9ea93fdc-3313-4464-812d-2ff49545fcf6","activity":"5dd5b9d8b...	1574287828182
2	9ea93fdc-3313-4464-812d-2ff49545fcf6	{"entities":{"device":"DD73C2F5A6B8413BA008573D06E301A6","callingUser":"1e78f404-2b8c-4bb4-b897-623be69f5fef","otherUser":"deleted","house":"9ea93fdc-3313-4464-812d-2ff49545fcf6","activity":"5dd5b9cbae7b240008ce3648"},"house":{"...	1574287819038
3	9ea93fdc-3313-4464-812d-2ff49545fcf6	{"entities":{"device":"DD73C2F5A6B8413BA008573D06E301A6","callingUser":"1e78f404-2b8c-4bb4-b897-623be69f5fef","otherUser":"deleted","house":"9ea93fdc-3313-4464-812d-2ff49545fcf6","activity":"5dd5b9b520ab5700089c020b"},"house":{...	1574287797216
4	9ea93fdc-3313-4464-812d-2ff49545fcf6	{"entities":{"device":"b5ec217cee0f","callingUser":"deleted","otherUser":"deleted","house":"9ea93fdc-3313-4464-812d-2ff49545fcf6","activity":"5dd5b9d0b...	1574287778611
5	9ea93fdc-3313-4464-812d-2ff49545fcf6	{"entities":{"device":"DD73C2F5A6B8413BA008573D06E301A6","callingUser":"1e78f404-2b8c-4bb4-b897-623be69f5fef","otherUser":"deleted","house":"9ea93fdc-3313-4464-812d-2ff49545fcf6","activity":"5dd5b989ce214c00084f032b"},"house":{"...	1574287753686
6	9ea93fdc-3313-4464-812d-2ff49545fcf6	{"entities":{"device":"b5ec217cee0f","callingUser":"deleted","otherUser":"deleted","house":"9ea93fdc-3313-4464-812d-2ff49545fcf6","activity":"5dd5b9881...	1574287752500
7	9ea93fdc-3313-4464-812d-2ff49545fcf6	{"entities":{"device":"DD73C2F5A6B8413BA008573D06E301A6","callingUser":"1e78f404-2b8c-4bb4-b897-623be69f5fef","otherUser":"deleted","house":"9ea93fdc-3313-4464-812d-2ff49545fcf6","activity":"5dd5b980ae7b240008ce1f64"},"house":{"...	1574287744219
8	9ea93fdc-3313-4464-812d-2ff49545fcf6	{"entities":{"device":"DD73C2F5A6B8413BA008573D06E301A6","callingUser":"manuallock","otherUser":"deleted","house":"9ea93fdc-3313-4464-812d-2ff49...	1574287736000
9	9ea93fdc-3313-4464-812d-2ff49545fcf6	{"entities":{"device":"DD73C2F5A6B8413BA008573D06E301A6","callingUser":"1e78f404-2b8c-4bb4-b897-623be69f5fef","otherUser":"deleted","house":"9ea93fdc-3313-4464-812d-2ff49545fcf6","activity":"5dd5b9770ae8ac0008a192bd"},"house":{"...	1574287735751
10	9ea93fdc-3313-4464-812d-2ff49545fcf6	{"entities":{"device":"b5ec217cee0f","callingUser":"deleted","otherUser":"deleted","house":"9ea93fdc-3313-4464-812d-2ff49545fcf6","activity":"5dd5b958b...	1574287700131
11	9ea93fdc-3313-4464-812d-2ff49545fcf6	{"entities":{"device":"b5ec217cee0f","callingUser":"deleted","otherUser":"deleted","house":"9ea93fdc-3313-4464-812d-2ff49545fcf6","activity":"5dd5b91cb...	1574287634766

Fig. 2. Device Interactions log on Android showing details of the actions that were taken along with timestamps.

TABLE II
LOCATION OF AUGUST ARTIFACTS ON UNROOTED ANDROID

Artifact	Location
Database Commands	imagefile.zip\Live Data\Dumpsys Data\dbinfo.txt
Application Usage	imagefile.zip\Live Data\usage_stats.txt

Application\app_id folder. The *Cache.db* database contains information about the August Home app and some user interactions, including the random codes sent to the user's e-mail and phone number when the user logs in to the app. This database also holds records of offline keys for the user so he/she can interact with the August devices without a WiFi or mobile data connection. Table V shows the location of relevant information on the jailbroken iPhone image, while Fig. 3 shows the format used to store the event log data. In Fig. 3, we highlighted some of the relevant data an investigator can get from the logs, such as:

1) The action that occurred: here the action was someone

TABLE III
LOCATION OF AUGUST ARTIFACTS ON ROOTED ANDROID (UNDER *imagefile.zip* FOLDER)

Artifact	Location	
	MSAB XRY Image	**Magnet ACQUIRE Image**
User Data	/data/data/com.august.luna/databases/ModelDatabase.db	/imagefile/json.txt
	/data/data/com.august.luna/files/logs	
User GPS Data	/data/data/com.august.luna/databases/LocationDatabase.db	N/A
Device Interactions	/data/data/com.august.luna/databases/ModelDatabase.db	/imagefile/json.txt
	/data/data/com.august.luna/files/logs	
Doorbell Images	/data/data/com.august.luna/cache/image_manager_disk_cache	/imagefile/json.txt

TABLE IV
LOCATION OF AUGUST ARTIFACTS ON NON-JAILBROKEN IOS

Artifact	Location
Devices Info	AppDomainGroup-group.com.august.today\Library\Preferences\ group.com.august.today.plist
	\AppDomain-com.august.iossapp\Documents\entities.plist
Auto-Unlock Log	\AppDomainGroup-group.com.august.general-cross-process\ Library\Preferences\group.com.august.general-cross-process.plist
Doorbell Images	PhotoData\Thumbnails\V2\DCIM\100APPLE*
	PhotoData\Metadata\DCIM\100APPLE\filename

*Only recoverable if previously downloaded from August Home app by user.

rang the doorbell.
2) The start and end times of the action in Epoch format.
3) The August ID of the user who answered the doorbell call via the August Home app.


```
:{"houseID":"fd08dd90-261e-43fd-
ba90-57e44af00b3a","houseName":"Ezio&apos;sLabHouse"},"dateTime":
1573850282426,"action":"doorbell_call_initiated","deviceName":"Ez
ioLabDoorbell","deviceID":"0764ad1a8148","deviceType":"doorbell",
"callingUser":{"UserID":"deleted","FirstName":"Unknown","LastName
":"User","UserName":"deleteduser","PhoneNo":"deleted"},"otherUser
":{"UserID":"deleted","FirstName":"Unknown","LastName":"User","Us
erName":"deleteduser","PhoneNo":"deleted"},"info":{"ended":157385
0293134,"started":1573850282426,"callID":"B9B07881-
DFB4-41FA-90CF-26F51A942E55","image":"https://res.cloudinary.com/
august-
com/image/upload/v1573850284/s4qh3ovlllk7ofknsulo.jpg","imageWidt
h":480,"imageHeight":640,"dvrID":"50f47258-47db-4efc-98e2-0beca62
56870","hasSubscription":false,"videoAvailable":true,"mobileCallS
tats":[],"users":{"answered_user":"e5ab9a6d-37ff-4fe8-95b0-
c65c0cf1b3f0","initiated_user":"e5ab9a6d-37ff-4fe8-95b0-
```


Fig. 3. Log generated on iOS due to doorbell being pressed. The highlighted parts show the action that was done, the start and end times of the action, and which user did the action.

During our experiments, we connected the S7Friend device to WiFi and revoked its access (from the iPhone 7 phone) to the smart lock and smart doorbell. Regarding the smart lock, the S7Friend device was immediately unable to interact with the smart lock. Alternatively, with the Smart Doorbell, the S7Friend device was still able to interact with the devices for a short period (under 10 seconds) before access to the devices was denied.

C. Network Traffic

After an in-depth analysis of the captured network data, we were unable to identify any sensitive information in plaintext. All August network traffic related to the devices' operations were encrypted with Transmission Control Protocol (TCP) or Transport Layer Security (TLS) v1.2 on both Android and iOS devices.

V. DISCUSSION

As our results in this study testify, forensically relevant artifacts can be recovered from both iOS and Android devices. Although there are slight variations in the type and format of the recovered data on both operating systems, forensic investigators would still be able to piece together a timeline of users' events. Such data would be pertinent in helping verify or disprove a suspect's alibi or aid in package theft investigations, for example.

We identified several privacy concerns during this investigative study. Firstly, the owner's full name, latitude and longitude of the smart lock, and device interactions can be found on guests' smartphone devices. Assuming the smart lock is installed on a door within the owner's home, someone could obtain the exact location of the house if the guest's phone is obtained, either illegally or without first being wiped. Secondly, pictures associated with doorbell motion detection events were found on the guest device. Once motion detection is enabled on the doorbell camera, any detection event would be sent to all users who currently have access to the camera. This could be a privacy violation if the owner does not set up guest access correctly or forgets to revoke guest access to the device.

Similar to [2], the guest device in our study was able to maintain a brief window of interaction with the August devices after having its access revoked by the device owner. However, the length of time with continued access is considerably less than in [2] and could be due to the network latency rather than improper device design.

When investigators are faced with these devices during a case, it helps to know just what data they should expect to find. Investigators must first determine the level of access they require from their suspect device: either rooted/jailbroken or not, and either an Android or iOS smartphone device. Once

TABLE V
LOCATION OF AUGUST ARTIFACTS ON JAILBROKEN IOS (UNDER PRIVATE\VAR\MOBILE\CONTAINERS\DATA\APPLICATION\DA89397F-ADBB-44C5-93D2-11ED6FD2A9E4)

Artifacts	Location
User Data	\Library\Caches\Logs
	\Library\Caches\com.august.iossapp\nscache\Cache.db
Device Interactions	\Library\Caches\Logs
	\Library\Caches\com.august.iossapp\nscache\fsCachedData
	\Library\Caches\com.august.iossapp\nscache\Cache.db
Doorbell Images	\Library\Caches\com.august.iossapp\nscache\fsCachedData

this is determined, the investigator should select a suitable imaging tool for their device.

If the suspect device is an Android device, one must be sure to examine the *ModelDatabase.db* file to determine August IDs for users and the IoT devices as well as some event data related to device interactions. Moreover, examiners can recover the user's GPS coordinates from the *LocationDatabase.db* file, provided the user enabled the smart lock's Auto-Unlock feature. Investigators should also examine the cached doorbell pictures in the *\cache\image_manager_disk_cache* folder and the log files in the *\files\logs* folder. If user location data is not required, an unrooted image may be sufficient. This image should provide other worthwhile data such as August device interactions, pictures taken by the smart doorbell camera, and August user data.

On the other hand, if dealing with an iOS suspect device, all germane August data would be under the *Caches* folder. Investigators should check the *Cache.db* file first to determine relevant August IDs associated with the user. Once this is known, traversing the log files from the *\Caches\Logs* and *\com.august.iossapp\nscache\fsCachedData* folders should be simple.

VI. CONCLUSION

Smart lock and smart doorbell camera use are on the rise and thus necessitates the need to know what forensically relevant data could be found regarding these devices. In this study, we examined the August Smart Lock Pro and August Smart Doorbell Pro and identified several forensically relevant artifacts that forensic investigators may be interested in during an investigation. Information about the owner, guests, allowed to use the devices, the house the devices are used in, device interactions, downloaded and cached images from the doorbell are all recoverable on iOS and Android devices, albeit in varying degrees. Exact user GPS data is only recoverable from a rooted Android device provided the user is using the smart lock's Auto-Unlock feature. The network traffic for these devices is well protected as communications occur using TCP and TLS.

Extending this investigation to include other smart lock and smart doorbell pairings and their interactions with popular Hubs like Google Home, Amazon Alexa, and Samsung SmartThings, on newer smartphone devices would be a possible future direction for this current work. Including the Smart Hubs would align more closely with how these devices are used in the real-world as it allows for the use of voice commands to interact with these IoT devices.

REFERENCES

[1] "Global smart doorbell market 2019-2023," Nov 2019. [Online]. Available: https://www.technavio.com/report/global-smart-doorbell-market-industry-analysis

[2] G. Ho, D. Leung, D. Leung, P. Mishra, A. Hosseini, D. Wagner, and D. Wagner, "Smart locks: Lessons for securing commodity internet of things devices," May 2016. [Online]. Available: https://dl.acm.org/citation.cfm?id=2897886

[3] A. Goudbeek, K.-K. R. Choo, and N.-A. Le-Khac, "A forensic investigation framework for smart home environment," IEEE, pp. 1446–1451, 2018.

[4] C. Meffert, D. Clark, I. Baggili, and F. Breitinger, "Forensic state acquisition from internet of things (fsaiot): A general framework and practical approach for iot forensics through iot device state acquisition," ACM, p. 56, 2017.

[5] openHAB, "empowering the smart home," 2020, last Accessed: 2/6/2020. [Online]. Available: https://www.openhab.org/

[6] N. Apthorpe, D. Reisman, and N. Feamster, "A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic," 2017.

[7] G. Dorai, S. Houshmand, and I. Baggili, "I know what you did last summer: your smart home internet of things and your iphone forensically ratting you out," ACM, p. 49, 2018.

[8] H. Chung, J. Park, and S. Lee, "Digital forensic approaches for amazon alexa ecosystem," pp. S15–S25, 2017.

[9] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of things security and forensics: Challenges and opportunities," 2018.

[10] "Nist," 2019. [Online]. Available: https://www.nist.gov/system/files/documents/2017/05/09/mobile_device_data _population_setup_guide.pdf

[11] J. Bays and U. Karabiyik, "Forensic analysis of third party location applications in android and ios," 2019.

[12] "Bulk extractor," 2019. [Online]. Available: http://downloads.digitalcorpora.org/downloads/bulk_extractor

[13] P. Feng, Q. Li, P. Zhang, and Z. Chen, "Logical acquisition method based on data migration for android mobile devices," pp. 55–62, 2018.

[14] "Chimera." [Online]. Available: https://chimera.sh/

[15] S. Odin, "Download Samsung Odin 3.12.3," 2020, last Accessed: 2/6/2020. [Online]. Available: https://odindownload.com/SamsungOdin/

[16] "Twrp for herolte." [Online]. Available: https://dl.twrp.me/herolte