2022 IEEE/ACIS 20th International Conference on Software Engineering Research, Management and Applications (SERA) | 978-1-6654-8350-6/22/$31.00 ©2022 IEEE | DOI: 10.1109/SERA54885.2022.9806735

Towards Internet of Things (IoT) Forensics Analysis on Intelligent Robot Vacuum Systems

Honghe Zhou*, Lin Deng*, Weifeng Xu†, Wei Yu*, Josh Dehlinger*, and Suranjan Chakraborty*
* Department of Computer and Information Sciences
Towson University, Maryland, USA
Emails: hzhou4@students.towson.edu, {ldeng, wyu, jdehlinger, schakraborty}@towson.edu
†School of Criminal Justice
University of Baltimore, Maryland, USA
Email: wxu@ubalt.edu

***Abstract*—With the rapid advancement of information technology, the Internet of Things (IoT) has significantly impacted people's daily life. IoT devices not only bring comfort and convenience to every aspect of the world, but also appear to be a new target of cybercrimes. Thus, IoT forensics becomes a critical step in forensics investigation. Intelligent robot vacuums are one of the most popular IoT devices. As robot vacuums can connect to the Internet and be operated through mobile apps, a large amount of data may be stored and transmitted among the vacuums, mobile apps, and the network. The data may include the history of the robot's operation, network and user credentials, and layouts of the floor plan of a house. From the perspective of digital forensics, these data can be critical while collecting necessary evidence, investigating suspects and victims, and reconstructing crime scenes. To this end, this paper makes an initial attempt to conduct a digital forensic analysis on intelligent robot vacuum systems. Specifically, this paper retrieves and analyzes a robot vacuum's operation log, the installation details of the robot vacuum's control system, and the usage record of the application from the memory of a smartphone.**

***Index Terms*—Internet of Things, Digital Forensics, IoT Forensics**

I. Introduction

The Internet of Things (IoT) refers to the seamless connection and data transfer of various devices, such as sensors, mobile phones, smart appliances, and vehicles, that are ubiquitous around people, and connected through the Internet [1]. The Internet and wireless network infrastructure has penetrated all cyber-physical system devices, resulting in an interconnected digital world consisting of portable and tiny mobile and IoT devices, such as smartphones, smartwatches, Amazon Echo devices, and even drones, which can support a variety of smart-world applications [2], [3]. The number of IoT devices exceeded 25 billion by the end of 2020 [4], and this number is expected to surpass 50 billion by the end of 2050 [5]. With IoT, billions of devices can be connected and share collected data simultaneously [6]. With the advance in cloud/edge computing and data analytics techniques, efficient and intelligent monitoring and control of cyber-physical systems can be supported [7], [8].

IoT offers numerous benefits not only to system operators, but also to consumers. A wide variety of connected devices and low-cost sensors make it possible to gather information from our environment, thereby making it possible to improve our standard of living [9]. These smart IoT devices are already being used in a variety of areas such as energy, transportation, healthcare, smart cities, and manufacturing, among others [10]. For example, drones can accurately deliver a variety of goods to customers quickly based on information from the IoT, achieving time and resource savings. Also, wearable devices such as smartwatches and health trackers can record information about a user's physical conditions at any time. They can make suggestions on users' living habits based on their physical information and even send alerts when users are in emergency.

While IoT makes people's day-to-day lives more convenient and dynamic, it also creates more opportunities for malicious actors to attack in ways that directly impact people. In other words, IoT has become a new target of cybercrimes and can dramatically affect several smart-world systems [2], [11], [12]. A report from Symantec indicates that many new cybercrime cases, such as ransomware, malicious attacks, fraud, node tampering, SQL injections, and phishing, involve the usage of various IoT devices or applications [13]. For example, IoT ransomware can target vulnerabilities in IoT devices to carry out ransomware attacks that can be harmful to the finances of a large number of organizations. Similarly, SQL injection enables hackers to gain access to IoT devices and obtain large amounts of data illegally.

Unlike traditional digital forensics methods, IoT forensics brings new challenges to forensics investigators, educators, and researchers. First, when a user uses IoT devices, a lot of information about the user may be transmitted or stored in a virtual environment. Such information, if not appropriately protected, can very likely become the target of cybercriminals. Second, IoT devices generate, use, and store various types of personal and sensitive data. How to balance the use of data and privacy/security risk has been an unsolved issue. These data are heterogeneous, as this information can be logs, usernames, passwords, emails, messages, etc. Additionally, the operating systems of IoT devices are heterogeneous too, ranging from Android, Linux, iOS, to embedded systems. Third, these various forms of IoT data can be stored in different locations (e.g., remote servers, cloud, or local devices). This makes it

978-1-6654-8350-6/22/$31.00 ©2022 IEEE
SERA 2022, May 25-27, 2022, Las Vegas, USA

challenging to gather sufficient evidence related to cybercrimes in a timely and comprehensive manner [14].

In this paper, we address the issue of IoT forensics and introduce an approach to conducting digital forensic analysis on intelligent robot vacuums, a unique type of IoT device used by many people but rarely investigated by forensic professionals. As one of the most widely used IoT devices in smart homes and buildings, the global market for the intelligent robot vacuum is expected to reach 60.9 million units by 2027 [15]. As most intelligent robot vacuums can be operated through mobile apps, the vacuums may transmit and store data in the phone's memory. Once a crime has been committed, these data can be very helpful in forensic investigation.

To this end, in this paper, we carry out a pilot study investigating the iRobot system for the retrieval of digital forensics information. We introduce in detail the forensics tools that we used and the evidence obtained from the study. In summary, the contributions of this paper are listed as follows:

- The design of a digital forensic approach that carries on the investigation of IoT devices.
- A pilot study of forensic analysis on intelligent robot vacuums, which is a representative IoT device.

The rest of this paper is organized as follows. Section II provides the background of digital forensics and IoT forensics. Section III gives an overview of related research. Section IV describes our IoT forensics in detail. Section V provides the results of our IoT forensic analysis. Finally, Section VI discusses the future work and concludes the paper.

II. Background

Digital forensics refers to the identification, search, seizure, preservation, and investigation of digital evidence on various types of electronic devices [16]. It is a branch of traditional forensic science. As crimes increase, real-world digital forensic investigation is a complex and systematic process. Digital evidence is scattered among different forms of artifacts, such as the operating system's registry, device memory, service logs, emails, etc. The steps of identification, collection, recovery, analysis, and preservation of digital evidence constitute the Forensics Investigation Life Cycle [17], [18].

The purpose of IoT forensics is similar to the one of digital forensics, that is, to identify and extract digital information in a legal and forensically reasonable way [19]. In addition to collecting forensic data from specific IoT devices or sensors, forensic data can be collected from networks and the applications that control the devices. Thus, IoT forensics includes three digital forensics schemes: network forensics, application level forensics, and device level forensics. Fig. 1 shows the overall workflow of IoT forensics. A comprehensive IoT forensics analysis requires the investigation of all three schemes, because different levels of forensics contribute to different evidence. For example, network logs and traffics can be obtained through network forensics; user credentials and usage events are retrieved by application level forensics; disk images are extracted using device-level (i.e., hardware) forensics.

III. Related Work

Recently, researchers have shown significant interest in investigating IoT forensics and proposing new approaches. An example is the vehicle information system that controls various types of vehicles, receives alerts from sensors, and facilitates communication from drivers. The vehicle information system is critical to IoT forensics, because it stores a large amount of data related to users, such as vehicle navigation history, call history, contact list, pictures, videos, and so on [20]. Professionals can use such information to identify responsible individuals for traffic accidents or cyber-attacks. In addition, in case of an accident, forensic professionals can check the sensor records. To solve the forensics problems related to the autonomous vehicle, Feng *et al.* [21] proposed a new digital forensics model for Smart City Automated Vehicles after investigating and analyzing the threats and various criminal cases faced by the automated vehicle. This study identifies possible attack vectors and digital evidence collection points in intelligent autonomous vehicles, providing guidance for future research in this field [21]. Likewise, Hossain *et al.* [22] proposed a framework to investigate criminal cases for the Internet of Vehicles systems. The framework can safely collect and store evidence and ensure the integrity of stored evidence [22].

Other areas of interest have been smart home systems. These systems consist of sensors and actuators designed to improve residents' comfort and convenience, often without manual control [19]. The smart home enables owners to remotely monitor and control housing conditions. It also helps with building maintenance and security. In smart home systems, air conditioning, heating systems, refrigerators, electric lights, and so on can be controlled through the Internet. Such systems, like the smart speaker developed by Amazon, the Amazon Echo can become a potential source of digital evidence, because of its widely used and always-on mode of operation [23]. Alexa is a smart virtual assistant that controls Amazon Echo. Chung *et al.* [23] proposed an approach combining cloud-native and client-centric forensics for the Amazon Alexa ecosystem. Their method combines cloud-side and client-side forensics, which overcomes the limitations of separate cloud forensics that require permissions and pose difficulties in obtaining deleted data in the past [23]. Likewise, Li *et al.* [24] proposed an IoT forensics analysis model and demonstrated the IoT forensic analysis on Amazon Echos. Their study revealed the availability of data in Amazon Echo. The model supports the identification, acquisition, analysis, and presentation of forensic useful information from IoT devices and infrastructure [24]. While for our research subject, robot vacuums, Luckhurst [25] explained the importance of robot vacuum forensics from the perspective of DNA acquisition. The paper of Luckhurst [25] shows that investigators can detect a small amount of DNA invisible to naked eyes, through robot vacuums' filters and brushes.

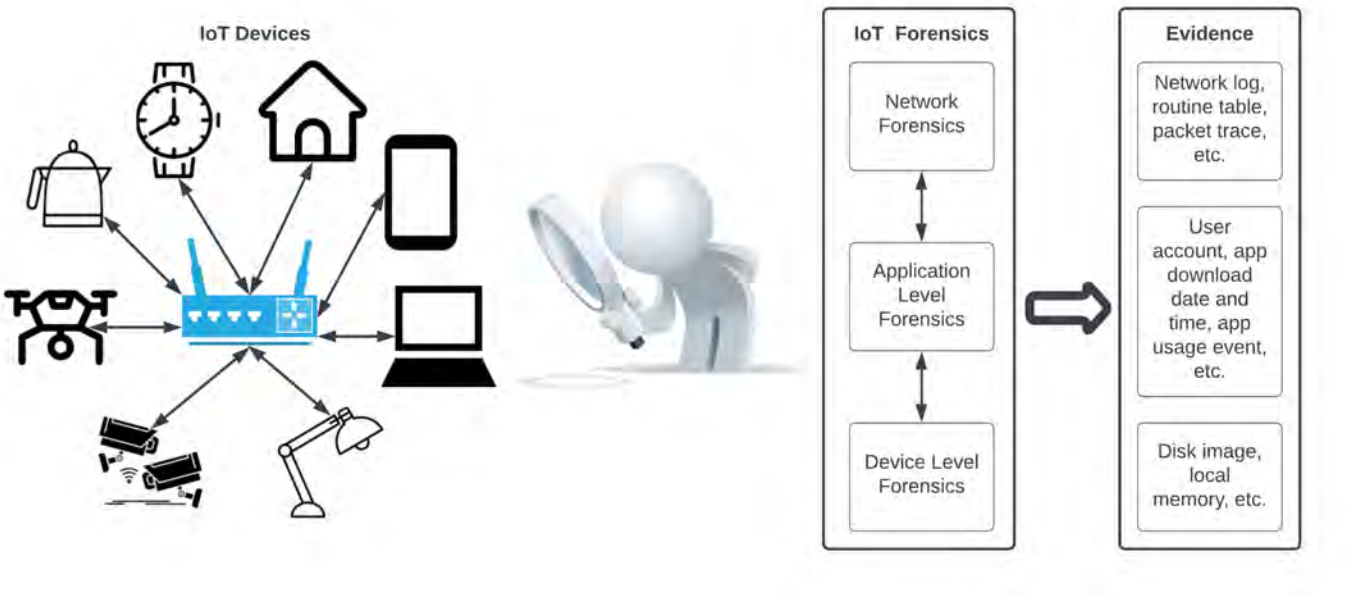

Fig. 1. Workflow of IoT Forensics

As a part of the smart home and building, intelligent robot vacuum systems are the focus of this paper regarding IoT forensics because they can record and transmit sensitive data, such as house information and the house owner's living habits.

IV. IoT Forensics Approach

This section introduces the general approach used for the forensic analysis on intelligent robot vacuum systems. In particular, we begin with the introduction of basic tools and then present the detailed steps of the IoT forensic analysis at the application level.

A. Basic Tools

Magisk: Magisk [26] is a suite of open-source software for customizing Android, supporting Android devices later than Android OS 5.0. Its features include a built-in graphical management interface, root access, startup scripts, SELinux patches, boot-time authentication, and forcible encryption removal. Magisk enables developers to modify "/system" and "/vendor" partitions and modify the Android operating system and other software functions.

Blueline Factory Image: The factory image is a binary image file that allows users to restore their device's original factory firmware [27]. And blueline is the codename of Google Pixel3 [27]. We use the Google Factory Image downloaded from the official website. The image needs to correspond to the phone's Android security update date and build number.

Team Win Recovery Project (TWRP): TWRP [28] is an open-source customizable recovery image for Android devices. It enables users to install custom software and ROMs on Android devices that are not supported by inventory recovery images. It supports wiping, backing up, restoring, and mounting partitions, such as user data, cache, and internal storage. TWRP also facilitates file transfer and management.

Android Debug Bridge (adb): The adb [29] is a command-line tool that allows users to communicate with devices. The adb command simplifies operations on the device such as installing and debugging apps. It also provides access to the Unix shell, which allows users to run various commands on Android devices.

Kali Linux Operating System: Kali Linux [30] is an open-source, Debian-based Linux operating system distribution featuring advanced penetration testing and security auditing. Kali Linux contains hundreds of tools targeted toward various information security tasks. We use Kali as the platform for our analysis of the data obtained from the iRobot Home app.

B. IoT Forensic Analysis at the Application Level

The first step of the analysis at the application level is to root the phone. Android users by default only have regular user privileges. "Root" is the process that allows Android users to gain restricted control over Android devices. The Android system is written based on the modified version of the Linux kernel. Therefore, root operations on Android devices gain similar administrative privileges to those on Linux operating systems. To root an Android phone, it is firstly required to use the Bootloader to unlock the phone. And then, with the help of the Magisk app and adb tool, a custom ROM (i.e., the blueline image) is installed. After that, the user is elevated to obtain root privileges of the phone. It is recommended to use tools such as Root Checker [31] to verify the root status. Fig. 2 shows the status of root access after checking.

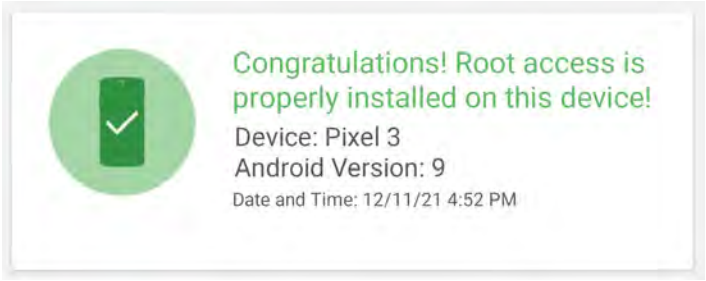

Fig. 2. The Status of Root Access

As the second step, after the preparation, we are able to conduct forensics investigation at the application level of the controlling app of intelligent robot vacuum systems. It is recommended to investigate various directories and data forms, including settings, user information, logs, network credentials, operations of the robot vacuum, clean schedules, etc.

In the third step, we need to retrieve all the data stored in the internal memory of the phone. To achieve this, installing customized recovery TWRP on the phone is a prerequisite, so that the adb commands (used for exporting data) can obtain the root privilege. We use the "adb reboot bootloader" command to enter in bootloader mode of the phone. Furthermore, we use the "fastboot boot (*The storage location of TWRP image file*)" command to enter the TWRP recover mode from bootloader mode.

As the last step, under TWRP recovery mode, we use the "adb pull" command to retrieve all the data from the phone's internal memory to the Kali system. Within the Kali system, we can use forensics tools to search and analyze useful information from the data. After screening and analyzing these data, the useful information is summarized and used as evidence.

V. IoT Forensic Pilot Study and Results

To evaluate the feasibility of conducting IoT forensics on intelligent robot vacuum systems, we conduct a pilot study at the application level forensics and report the results in this section.

A. Evaluation Subject

1) Google Pixel 3 smartphone: Pixel 3 is an Android smartphone released by Google. The Android version we used is Android 9.

2) Roomba j7+ robot vacuum: The Roomba j7+ robot vacuum is one of the iRobot company's latest robot vacuum products. We choose Roomba j7+ as the experimental subject because it can be controlled through a mobile app and store user-related data and settings. Fig. 3 [32] shows a picture of the j7+ robot vacuum.

3) iRobot Home Application: The iRobot Home application [33] is developed by iRobot company to control their company's robot vacuums. Fig. 4 [34] shows screenshots of the app. Its functions include turning on and off the robot vacuum, drawing the structure of a house, identifying and capturing photos of objects in a room, and scheduling robot vacuums to clean.

Fig. 3. iRobot Roomba j7+ Robot Vacuum [32]

B. Results of the Pilot Study

In the following, we show the results of the pilot forensics study on the application level of the iRobot intelligent vacuum system.

1) App Installation Date and Time: The installation date and time are stored in a fixed location on the phone. The location is "*data/data/com.android.vending/databases/localappstate.db*". This information is stored in the database in the form of a timestamp. It is shown in Fig. 5. As seen in the figure, "1637767340897" is the last time we downloaded the iRobot Home App from the Google Play store. Timestamp "1637767340897" is equivalent to "Wednesday, 24 Nov. 2021, 10:22:20 AM EST".

2) App Version Number: The version number of most apps is stored in a database called *gass* in the phone's internal memory. The location of *gass* database is "*data/data/com.google.android.gms/databases/gass.db*". The version number of the iRobot Home App is shown in Fig. 6. The "6.1.0" in Fig. 6 is the version number of the iRobot Home app we download from google play.

3) App Usage Events: From usage events, we can simply analyze what users are doing with the app at any given moment. The usage events are stored in the "*usagestats*" folder. Its location is "*/data/system/usagestats*". Usually, the system collects the data over 4 different intervals, daily, weekly, monthly, and yearly, and separates the data into different timestamp named folders. Because the raw data is stored as an XML file, which is difficult to analyze, we use the Android-Usagestats-XML-Protobuf parse tool [35] to aggregate the usage data in the different files together. It is a parser that acquires information from an XML file in the *usagestats* folder

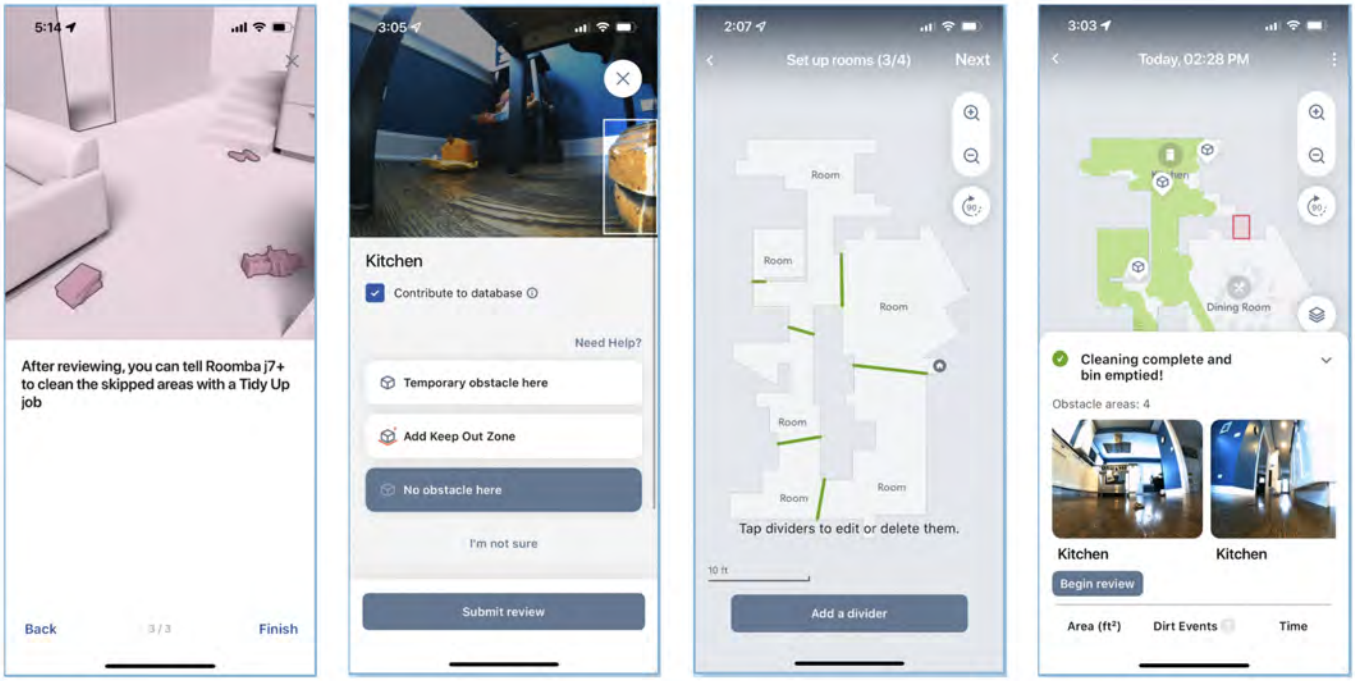

Fig. 4. The iRobot Home App [34]

```
┌──(root💀kali)-[/home/kali/iRobot]
└─# sqlite3 'com.android.vending/databases/localappstate.db'
SQLite version 3.34.1 2021-01-20 14:10:07
Enter ".help" for usage hints.
sqlite> select  package_name,  first_download_ms, title from appstate where lower(title) like '%iRobot%';
com.irobot.home|1637767340897|iRobot Home
sqlite>
```

Fig. 5. Installation Date and Time of the iRobot Home App

and puts it into an SQLite database for easy queries. Fig. 7 shows a part of the raw data retrieved in the study. It records the time stamp when the iRobot app is used by the user, package name, class, as well as the usage type and other information. The parsed data is shown in Fig. 8. In this figure, we transfer timestamps into the format of date and time. Also, in the raw data, the usage type is recorded as the integer value. For a more intuitive view, we convert them into text types. In Fig. 8, the usage events "*MOVE_TO_FOREGROUND*" and "*MOVE_TO_BACKGROUND*" of different activities represent the switch between interfaces. In most cases, when the user clicks a button, the app switches to another interface. Therefore, these usage event records enable us to analyze the user's behavior at a specific time frame.

4) The Clean Schedule of Robot Vacuums: The clean schedule is stored in the *irobot_home* log file in the phone. Its location is "*/data/data/com.irobot.home/files/logs/irobot_home.log*". This log file records the clean schedule in terms of hour, minute, and day of the week. The clean schedule of the robot vacuum is shown in Fig. 9. The figure shows that the user currently has two clean schedule settings: *"day": [1, 2, 5], "hour": 9, "min": 0* and *"day": [1, 3, 5], "hour": 2, "min": 0*. The first cleaning schedule is Monday, Tuesday, and Friday at 9 AM. The second cleaning schedule is Monday, Wednesday, and Friday at 2 AM. From this file, forensics investigators can learn when and on what date the robot is scheduled to clean the house. Also, from this information, forensics can analyze users' daily routines to a certain extent.

5) User Credentials and Network Information: The user account and network information are stored in the app's XML file. Its location is "*/data/data/com.irobot.home/shared_prefs/APP.xml*". Fig. 10 shows an example log file. From this file, we can locate the username, Wi-Fi name, local network address, and MAC address. The user account and network information are very important evidence. By analyzing the information, forensics investigators can learn the user's real identity and where the robot is connected to the Internet, which is the user's residence.

VI. Final Remarks

While enjoying the comfort and convenience brought by IoT devices, people start to see an increased number of

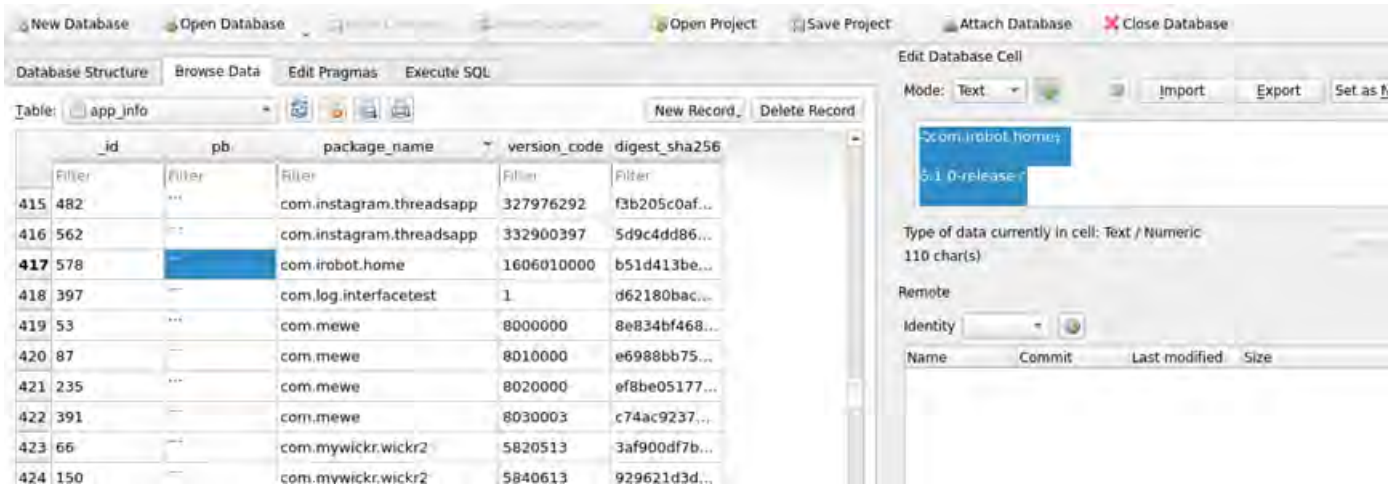

Fig. 6. Version Number of the iRobot Home App

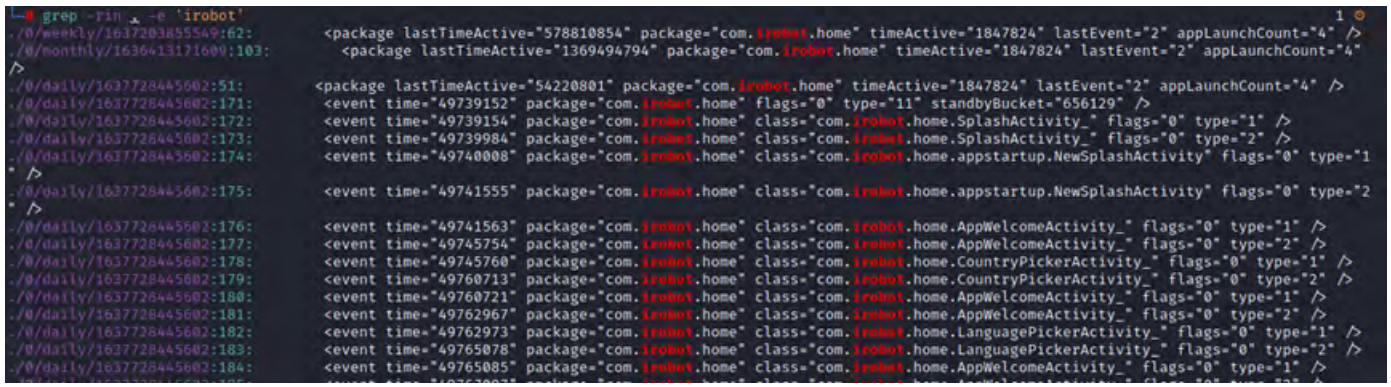

Fig. 7. Raw Data of Usage Events

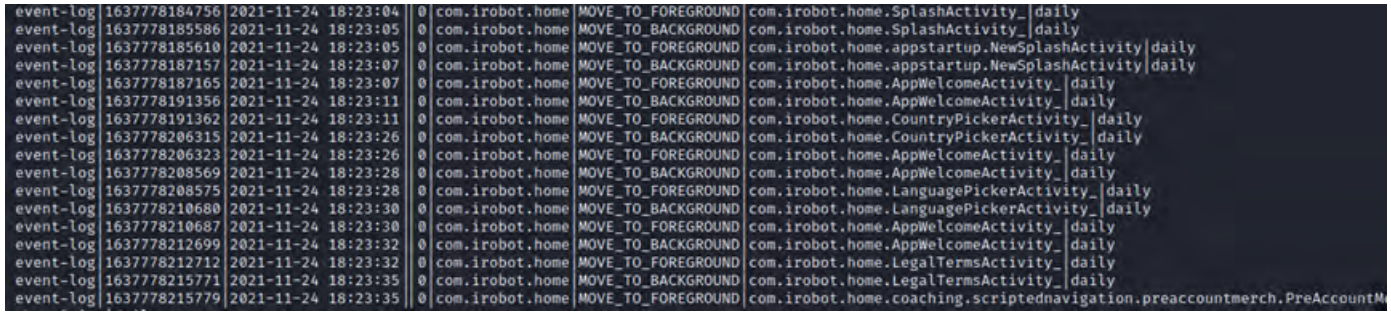

Fig. 8. The Parsed Data of Usage Events

cybercrimes targeting or leveraging IoT devices. IoT forensics becomes a crucial step in investigating suspects, reconstructing crime scenes, and collecting critical evidence. In this paper, we have designed an approach to conduct IoT forensics on intelligent robot vacuum systems, and performed a pilot forensics study at the application level of the iRobot smart vacuum and its app. Via extensive experiments, we have demonstrated the feasibility of retrieving sensitive information such as usage events, clean schedule set by the user, user account number and network information, etc.

For future research, as shown in Fig. 1, IoT forensics includes network forensics, application level forensics, and device level forensics. This paper conducts the pilot study only at the application level. We believe that a further investigation on the other two levels would lead to more comprehensive outcomes, such as the structural layout of houses scanned by robot vacuums, cached image files, etc. Therefore, we plan to investigate at the network level and device level, such as leveraging network traffic analysis tools to intercept network data packets and read the data packets in real-time [36].

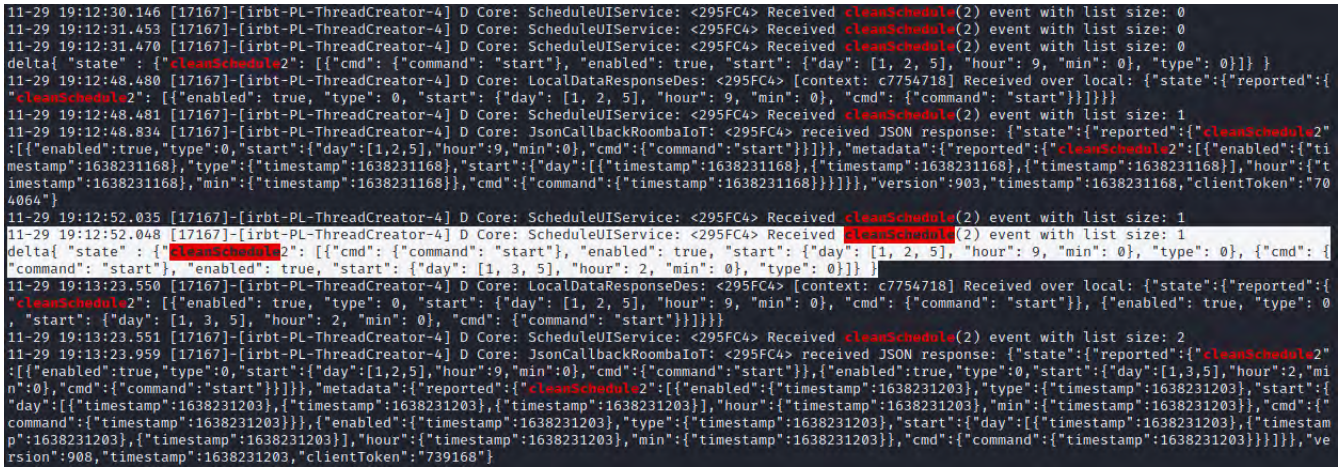

Fig. 9. The Clean Schedule of The Robot Vacuum

Fig. 10. The User Account and Network Information

We also plan to use traffic analysis tools to capture the package uploaded by the mobile phone through the network, to find the house structure drawing. At the device level, we aim to conduct a forensics study in firmware/hardware (e.g., attempting to retrieve data stored in the hardware).

Acknowledgment

This work is supported in part by the U.S. Department of Justice under 2019-DF-BX-K001. Deng is supported as a Jess and Mildred Fisher Endowed Professor of Computer and Information Sciences from the Fisher College of Science and Mathematics at Towson University. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the agency.

References

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128610001568

[2] X. Liu, C. Qian, W. G. Hatcher, H. Xu, W. Liao, and W. Yu, "Secure internet of things (iot)-based smart-world critical infrastructures: Survey, case study and research opportunities," *IEEE Access*, vol. 7, pp. 79 523–79 544, 2019.

[3] F. Liang, C. Qian, W. G. Hatcher, and W. Yu, "Search engine for the internet of things: Lessons from web search, vision, and opportunities," *IEEE Access*, vol. 7, pp. 104 673–104 691, 2019.

[4] R. S. Sinha, Y. Wei, and S.-H. Hwang, "A survey on lpwa technology: Lora and nb-iot," *Ict Express*, vol. 3, no. 1, pp. 14–21, 2017.

[5] A. Musaddiq, Y. B. Zikria, O. Hahm, H. Yu, A. K. Bashir, and S. W. Kim, "A survey on resource management in iot operating systems," *IEEE Access*, vol. 6, pp. 8459–8482, 2018.

[6] H. F. Atlam, A. Alenezi, M. O. Alassafi, and G. B. Wills, "Blockchain with internet of things: Benefits, challenges, and future directions." *International Journal of Intelligent Systems & Applications*, vol. 10, no. 6, 2018.

[7] M. Mohammadi, A. Al-Fuqaha, S. Sorour, and M. Guizani, "Deep learning for iot big data and streaming analytics: A survey," *IEEE Communications Surveys Tutorials*, vol. 20, no. 4, pp. 2923–2960, 2018.

[8] W. G. Hatcher and W. Yu, "A survey of deep learning: Platforms, applications and emerging research trends," *IEEE Access*, vol. 6, pp. 24 411–24 432, 2018.

[9] H. F. Atlam, A. Alenezi, A. Alharthi, R. J. Walters, and G. B. Wills, "Integration of cloud computing with internet of things: challenges and open issues," in *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE*

Smart Data (SmartData). IEEE, 2017, pp. 670–675.

[10] A. Alenezi, H. Atlam, R. Alsagri, M. Alassafi, and G. Wills, "Iot forensics: A state-of-the-art review, callenges and future directions." SCITEPRESS - Science and Technology Publications, 2019. [Online]. Available: http://hdl.handle.net/10545/624925

[11] W. Zhou, Y. Jia, Y. Yao, L. Zhu, L. Guan, Y. Mao, P. Liu, and Y. Zhang, "Discovering and understanding the security hazards in the interactions between IoT devices, mobile apps, and clouds on smart home platforms," in *28th USENIX Security Symposium (USENIX Security 19)*. Santa Clara, CA: USENIX Association, Aug. 2019, pp. 1133–1150. [Online]. Available: https://www.usenix.org/conference/usenixsecurity19/presentation/zhou

[12] S. Soltan, P. Mittal, and H. V. Poor, "BlackIoT: IoT botnet of high wattage devices can disrupt the power grid," in *27th USENIX Security Symposium (USENIX Security 18)*. Baltimore, MD: USENIX Association, Aug. 2018, pp. 15–32. [Online]. Available: https://www.usenix.org/conference/usenixsecurity18/presentation/soltan

[13] P. Wood, B. Nahorney, K. Chandrasekar, S. Wallace, and K. Haley, "Symantec global internet security threat report," *White Paper, Symantec Enterprise Security*, vol. 21, 2016.

[14] A. MacDermott, T. Baker, and Q. Shi, "Iot forensics: Challenges for the ioa era," in *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 2018, pp. 1–5.

[15] M. M. R. P. Ltd., *Robotic Vacuum Cleaner Market by Type, Distribution Channel, Operation Price Range Application - Global Forecast to 2028*, 2021.

[16] D. P. Joseph and J. Norman, *An Analysis of Digital Forensics in Cyber Security: AICC 2018*, 01 2019, pp. 701–708.

[17] J. Cosic and Z. Cosic, "Chain of custody and life cycle of digital evidence," *Computer technology and application*, vol. 3, no. 2, 2012.

[18] J. Patel, "Forensic investigation life cycle (filc) using 6 'r'policy for digital evidence collection and legal prosecution," *Int. J. Emerg. Trends Technol.*, vol. 2, no. 1, pp. 129–132, 2013.

[19] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, "A survey on the internet of things (iot) forensics: Challenges, approaches, and open issues," *IEEE Communications Surveys Tutorials*, vol. 22, no. 2, pp. 1191–1221, 2020.

[20] J. Toldinas, A. Venčkauskas, Š. Grigaliūnas, R. Damaševičius, and V. Jusas, "Suitability of the digital forensic tools for investigation of cyber crime in the internet of things and services," *RCITD. RCITD*, 2015.

[32] (2022) Roomba® j series robot vacuums. [Online]. Available: https://www.irobot.com/roomba/j-series

[21] X. Feng, E. S. Dawam, and S. Amin, "A new digital forensics model of smart city automated vehicles," in *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. IEEE, 2017, pp. 274–279.

[22] M. M. Hossain, R. Hasan, S. Zawoad *et al.*, "Trust-iov: A trustworthy forensic investigation framework for the internet of vehicles (iov)." in *ICIOT*, 2017, pp. 25–32.

[23] H. Chung, J. Park, and S. Lee, "Digital forensic approaches for amazon alexa ecosystem," *Digital Investigation*, vol. 22, pp. S15–S25, 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1742287617301974

[24] S. Li, K.-K. R. Choo, Q. Sun, W. J. Buchanan, and J. Cao, "Iot forensics: Amazon echo as a use case," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6487–6497, 2019.

[25] P. Luckhurst, "Robotic vacuum evidence recovery for low yield samples overlooked post investigation," Ph.D. dissertation, Murdoch University, 2019.

[26] (2022) Magisk: The magic mask for android. [Online]. Available: https://github.com/topjohnwu/Magisk

[27] (2022) Factory images for nexus and pixel devices. [Online]. Available: https://developers.google.com/android/images#blueline

[28] (2022) Teamwin - twrp. [Online]. Available: https://twrp.me/about/

[29] (2022) Android debug bridge (adb). [Online]. Available: https://developer.android.com/studio/command-line/adb

[30] (2022) What is kali linux? [Online]. Available: https://www.kali.org/docs/introduction/what-is-kali-linux/

[31] (2022) Root checker. [Online]. Available: https://root-checker.en.uptodown.com/android

[33] (2022) irobot home app. [Online]. Available: https://www.irobot.com/irobot-home-app

[34] (2022) irobot roomba j7+ review — tom's guide. [Online]. Available: https://teknosignal.com/irobot-roomba-j7-review-toms-guide/

[35] (2019) Android usagestats xml parser. [Online]. Available: https://abrignoni.blogspot.com/2019/02/android-usagestats-xml-parser.html

[36] A. Orebaugh, G. Ramirez, and J. Beale, *Wireshark & Ethereal network protocol analyzer toolkit*. Elsevier, 2006.