The Journal of Supercomputing (2023) 79:973–997
https://doi.org/10.1007/s11227-022-04639-5

Digital forensic analysis of intelligent and smart IoT devices

Minju Kim[1] · Yeonghun Shin[1] · Wooyeon Jo[2] · Taeshik Shon[1,3]

Accepted: 30 May 2022 / Published online: 20 July 2022

Abstract
AI is combined with various devices to provide improved performance. IoT devices combined with AI are called smart IoT. Smart IoT devices can be controlled using wearable devices. Wearable devices such as smartwatches and smartbands generate personal information through sensors to provide a range of services to users. As the generated data are preserved in the storage of the wearable device, getting access to these data from the device can prove useful in criminal investigations. We, therefore, propose a forensic model based on direct connections using wireless or interfaces beyond indirect forensics for wearable devices. The forensic model was derived based on the ecosystem of wearable devices and was divided into logical and physical forensic methods. To confirm the applicability of the forensic model, we applied it to wearable devices from Samsung, Apple, and Garmin. Our results demonstrate that the proposed forensic model can be successfully used to derive artifacts.

Keywords Digital forensics · Wearable ecosystem · Smartwatch · Smartband

1 Introduction

With the development of new technologies, existing technologies were combined with new technologies and developed into other new technologies. The emergence of new technologies has led to the development of various security technologies [1–4]. One of the most used new technologies is artificial intelligence. Artificial intelligence is combined with various devices to provide improved performance

The datasets generated during and/or analysed during the current study are not available due to the privacy, so data sharing is not applicable.

✉ Taeshik Shon
tsshon@ajou.ac.kr

[1] Department of AI Convergence network, Ajou University, Suwon, Korea

[2] Department of Computer Engineering, Ajou University, Suwon, Korea

[3] Department of Cyber Security, Ajou University, Suwon, Korea

and customized services [5]. Various devices such as refrigerators, air conditioners, and surveillance systems have been combined with AI [6]. Devices combined with AI are also called smart IoT. Smart IoT devices can be controlled using wearable devices. A wearable device may be used to control the temperature of the air conditioner or to turn on/off a light switch. Not only that, it can send notifications to the wearable device when an intrusion into the surveillance system is detected.

Wearable devices, such as smartwatches and smartbands, are worn close to and/or on the body to collect information about the environment around the user and body changes using sensors. Wearable devices not only provide health-related data such as heart rate and physical activity, but also notification services such as phone calls, text messages. Moreover, with the continuous improvement in the quantity as well as quality of services provided by wearable devices, the number of users of wearable devices has significantly increased. In addition, the International Data Corporation has predicted that the sales of wearable devices will reach 489.1 million units by 2023 [7].

Wearable devices provide a range of different services to users through a continuous data exchange with a paired device or cloud server. Most of the data of the cloud server are stored in the internal storage of the wearable device. Therefore, if these data stored in the device's internal storage can be obtained, the time and cost involved in requesting user data from the manufacturer during a criminal investigation can be substantially reduced. Alternatively, the accuracy of the investigation can be increased by cross-analyzing the data provided by the manufacturer and the data stored in the wearable device.

Recently, digital forensic research has expanded into new environments, such as internet of things (IoT), artificial intelligence (AI) speakers [8–12]. However, as wearable devices get more and more miniaturized, it will become challenging to use them in existing forensic techniques. Furthermore, considering the present times where multiple wearable devices with more and better functions are introduced every year, if the forensic methods of existing research are applied to the latest wearable devices, the results of the previous research will be different. The latest wearable devices use the embedded subscriber identity module (eSIM) to communicate with the cloud server alone, which allows it to acquire more data than wearable devices paired with only smartphones.

Most of the research on existing wearable devices has been carried out indirectly for forensics using paired devices [13–19]. Indirect forensics using paired devices synchronized with the wearable device acquire data about a wearable device stored on a smartphone or PC. Owing to this synchronization, indirect forensics using paired devices have more limited data than direct forensics using wearable devices. Because manufacturers of different wearable devices use different operating systems (OS), and each device has a different data storage structure, applying the existing research on the latest wearable devices is not practical. Therefore, we propose an ecosystem of wearable devices for the forensics of

wearable devices. In this study, we mainly performed direct forensics on wearable devices. The contributions of this study are as follows:

1. A wearable device ecosystem was derived to apply digital forensics based on the identification of major interfaces and connection configurations of smart watches and smartbands.
2. A forensic model divided into logical and physical forensic methods have been proposed based on the wearable device ecosystem. Logical forensics methods include analyses using PC connections and internal storage of paired devices, physical forensics include analyses through the printed circuit board (PCB) service port, PCB debugging port, and chip-off.
3. To verify the forensic model, it was applied to wearable devices of major manufacturers, and the related artifacts were acquired and analyzed.

2 Related work

2.1 Wearable device forensics

Becirovic et al. [20] performed forensic analysis on Samsung Gear S3 Frontier devices. Data were acquired by accessing the shell of the wearable device using a Wi-Fi. Only short message service (SMS) and messenger usage data were acquired. Gregorio et al. [21] performed forensics on three types of smartwatches based on a real-time OS. The Joint Test Action Group (JTAG) was used to acquire user data in the internal storage of smartwatch. In the study by Odom et al., data from smartphones paired with the Samsung Galaxy Gear S3 Frontier and Apple Watch Series 3 devices were acquired [22]. Data extraction of Galaxy Gear S3 Frontier was performed using the Universal Forensic Extraction Device 4PC of Cellebrite, and the Apple Watch Series 3 was connected to a PC through an iBUS S2, and Xcode was used to extract the data. However, they used an existing data acquisition program. Most of the research on wearable devices is used paired smartphone, and thus, it is difficult to know whether the personal information of the user remains in the wearable device. Wearable devices are being released from various manufacturers, but the amount of research being conducted is insufficient.

2.2 Internet of things forensics

Jo et al. [23] conducted a digital forensic study on an AI speaker ecosystem that has an environment similar to that of wearable devices. In this study, five analysis methods were proposed by dividing them into three forensic areas. The research by Shin et al. which was conducted as a follow-up study to that by Jo et al. proposed five methods of injecting a certificate into an AI speaker to analyze the encrypted traffic between the AI speaker and the cloud [24]. The encrypted traffic of the AI speakers was analyzed through the ball grid array rework of the NAND flash memory with the certificate injection. Shancang et al. [25] presented an IoT-based forensic model

that supports the identification, acquisition, and analysis of forensic artifacts in IoT devices and infrastructure. The proposed model is a forensic approach based on the Amazon Echo AI speaker as an example. The wearable device is worn on the body of the user, and its position can be changed. Conversely, the AI speaker ecosystem has a fixed position. Therefore, the types of acquisition artifacts expected will be different. Because wearable devices are miniaturized, there is a limit to the application of the existing IoT forensic techniques.

3 Digital forensic model for wearable devices

In this study, we derived an ecosystem for wearable devices to acquire user data stored in the internal storage of wearable devices, as shown in Fig. 1, based on the main interface and connection configuration of the wearable devices.

The main components of the proposed ecosystem comprised wearable devices, smartphones, and PCs. A wearable device can be used by pairing with a smartphone. Bluetooth is used for pairing smartphones. When the wearable device is paired with a smartphone, communication with the cloud is performed indirectly through the smartphone. However, most of the latest wearable devices support Wi-Fi and LTE connection. Therefore, the wearable device can communicate directly with the cloud server without pairing with a smartphone. Some wearable devices may connect to a PC using USB and then transfer files to the wearable device. Alternatively, it may be possible to connect to a PC using Wi-Fi. In other words, there is a possibility that wearable devices store user personal information in the internal storage of the wearable device by pairing with another device. There are components for device operation on the PCB of wearable devices, such as the processor and memory. The PCB also has a debugging port and a service port. The debugging port is created by

Fig. 1 Wearable device ecosystem and ecosystem-based wearable device forensic model

the manufacturer for product debugging, such as JTAG and Universal asynchronous receiver/transmitter (UART), and the service port is a port created to check the normal booting of the wearable device during the manufacturing process.

The forensic model of wearable devices was constructed using logical forensic and physical forensic methods based on the main interfaces and connection configurations identified in the ecosystem of wearable devices. Logical forensics include PC connection, internal storage of paired devices, and physical forensics include PCB service port, PCB debugging port, and chip-off. Forensics on data stored in the wearable device through connection with PC or forensics on data stored in the paired mobile device are defined as logical forensics. In the case of using the wearable device PCB, it was defined as physical forensics.

3.1 Logical forensics

3.1.1 PC connections

Because most wearable devices support wired/wireless connections with a PC, forensics for acquiring data stored in the wearable devices may be performed through connection with the PC. It can be performed through a wired connection using a USB provided by the manufacturer or a wireless connection using Wi-Fi. A wired PC connection using USB uses USB with Ground, Data+, Data−, and Power pins. If USB does not have Data+ and Data− pins for data transmission, data transmission is impossible. Most of the latest wearable devices support Wi-Fi networks. To connect the wearable device and the PC using Wi-Fi, the Wi-Fi created in the PC must be connected to the wearable device.

For wearable device forensics using the PC Connection, most forensic performers have user authority, and hence, rooting is sometimes required to acquire the entire data. There are two common rooting methods. The first is using the recovery mode. This method installs the SU binary in internal storage to obtain administrator privileges. The second method obtains administrator privileges by installing the SU binary inside the device by using the vulnerabilities of the wearable devices or the OS. In both methods, it must be connected to a PC. The method of obtaining administrator privileges by rooting depends on the OS.

3.1.2 Internal storage of paired devices

Wearable devices continuously exchange data through communication with a paired device or cloud server. Information about the user is stored in the internal storage of smartphone and PC as well as wearable device. The internal storage of paired devices method is an indirect forensic method that forensics a wearable device using data stored in the internal storage of a paired device during a communication process.

A method of using data stored in a smartphone paired with a wearable device is to extract and analyze smartphone data to acquire only wearable device data stored during communication. In order to forensic the internal storage of a paired

smartphone, access to smartphone data is required, so obtaining administrator privileges of the smartphone must be preceded. Forensics using a paired device is performed only when direct forensic methods cannot be performed.

3.2 Physical forensics

3.2.1 PCB service port

Some wearable devices cannot connect to a PC. In some cases, a service port, which is an interface that can be connected to a PC, is implemented on the PCB of a wearable device that check normal booting during the manufacturing process. In most cases, the service port of the PCB can be connected to a PC by soldering. Some wearable devices have a BUS that can be connected to the interface of the PCB or can connect the wearable device and the PC using the USB provided by the manufacturer. Even if there is no additional connection interface, it can be connected to a PC by soldering a standard wire to the service port.

3.2.2 PCB debugging port

In some cases, the PCB of the wearable device implements not only a service port but also a debugging port, such as JTAG and UART, which is an interface for debugging. The debugging port can be used to extract data stored inside the device or to acquire a full dump image. When performing forensics using JTAG and UART ports, it is possible to acquire all data stored in the device because administrator privileges are not required [15, 21]. In the PCB debugging port of this paper, only the JTAG and UART debugging ports are analyzed to confirm the applicability of the forensic model.

3.2.3 Chip-off

Chip-off is performed as the last option when forensics at the S/W or H/W level are difficult. Chip-off is a method of acquiring data by physically acquiring NAND flash from the PCB of a wearable device. Chip-off requires a high level of understanding of various hardware and equipment. The NAND flash acquired through chip-off can be mounted on a PC, and data can be acquired in the form of a raw image [24].

Most of the NAND flash in the latest wearable devices is implemented in system-on-a-chip (SoC). In SoC, all blocks such as processor core and memory are implemented with a single chip, and even if chip-off is possible, it is difficult to obtain data by specifying NAND flash. However, some wearable devices use a separate embedded multimedia card (eMMC) as a NAND flash. When implemented in the form of a proprietary eMMC, it is possible to acquire data in the internal storage of wearable devices by chip-off. If the wearable device image obtained by chip-off uses Ext4 as the file system, even the deleted data can be acquired [26]. We applied the forensic model proposed in Sect. 4 to actual wearable devices and analyzed the artifacts based on the acquired data.

4 Practice for forensic model

Because wearable devices have different interfaces, we confirm the applicability of the proposed forensic model for wearable devices from Samsung, Apple, and Garmin with high penetration in 2020 and 2021 [27]. Three types of Samsung smartwatches, three types of Apple smartwatches, and one type of Garmin smartband were used in the forensic model application experiment.

4.1 Samsung smartwatches

The Samsung smartwatch used in the forensic model application experiment is Galaxy Watch 3 (LTE, Bluetooth), Galaxy Active 2 (Bluetooth), and Galaxy Watch 1 (Bluetooth). Table 1 shows the specifications of the Samsung smartwatch used in the forensic model application experiment. Three types of Samsung smartwatches can use Bluetooth and Wi-Fi communication. In addition, all three devices use eSIM to communicate with the cloud server without pairing with a smartphone. Therefore, we conducted an additional experiment on the Galaxy Watch 3 LTE to derive the difference between data stored in devices that cannot communicate with cellular communication and those that use cellular communication. As a result of the experiment, the applicability of the forensic model to three Samsung smartwatches, the same results and artifacts were derived. Therefore, only the experimental process for the Galaxy Watch 3 was described.

4.1.1 PC Connection

Because Samsung Galaxy Watch 3 does not have DATA + and DATA pins in the USB provided by the manufacturer, it is impossible to connect it to a PC using USB. However, because the Samsung Galaxy Watch 3 is capable of network communication using Wi-Fi, we confirm the applicability of the wireless PC connection method of the forensic model in the Samsung smartwatch. For the PC connection experiment using Wi-Fi of Galaxy Watch 3 (LTE, Bluetooth), the mobile hotspot function of the PC was used. Because the Galaxy Watch 3 Bluetooth model communicates with the cloud server through the paired smartphone, it was paired with the Galaxy S9 + device. After PC connection using Wi-Fi, a smart development bridge (SDB) was used to acquire data, and firmware was flashed using Odin v3.13.3 to acquire administrator privileges.

For the PC connection using Wi-Fi, the Samsung smartwatch was connected to the Wi-Fi created on the PC in the normal booting state. A Samsung smartwatch connected to a PC can use the SDB after enabling USB debugging. SDB is a development bridge for Tizen OS developed by Samsung and has the similar function as the Android Development Bridge (ADB) for Android. This allowed us to access the Galaxy Watch 3 shell from a PC on the same Wi-Fi network. The internal storage data of the Galaxy Watch 3 were acquired through the SDB shell. By analyzing the acquired data, we were able to acquire various artifacts, such as:

Table 1 Samsung smartwatches spec used in experiment

	Samsung galaxy watch 3	Samsung galaxy active 2	Samsung galaxy watch 1
Processor	Samsung Exynos 9 Series SiP	Samsung Exynos 9 Series SiP	Samsung Exynos 9 Series SoC
Memory	1 GB LPDDR4X SDRAM, 8 GB eMMC	768 MB LPDDR4X SDRAM, 4 GB eMMC	768 MB LPDDR4X SDRAM, 4 GB eMMC
OS	Tizen 5.5	Tizen 5.5	Tizen 4.0
Communication	Wi-Fi 1/3/4, bluetooth 5.0, NFC	Wi-Fi 1/3/4, bluetooth 5.0, NFC	Wi-Fi 1/3/4, bluetooth 4.2, NFC

1. Paired device and wearable device information
2. Call history and text messages
3. Voice assistant raw file
4. Personal health data

Data acquisition through a PC connection does not acquire all data in the internal storage of Samsung Galaxy Watch 3 because a forensic model is applied with user authority. Therefore, the administrator privileges of Galaxy Watch 3 were acquired. To obtain administrator privileges on the Galaxy Watch 3, custom firmware or custom recovery must be flashed. Since there is no firmware that includes administrator privileges for Samsung smartwatches so far, we created a firmware with administrator privileges by injecting the SU binary into the stock firmware, which is the original firmware. The custom firmware with administrator privileges was flashed using Odin, but it did not boot normally. The phrase '_FOTA_BODY_FINALISING_NUPDATE_' is shown in Fig. 2. This indicates that Galaxy Watch 3 performs an integrity check during booting. If the integrity of the device is compromised, the firmware over-the-air (FOTA) protocol is automatically executed and the original firmware is flashed over a wireless connection.

4.1.2 PCB service port

To confirm the applicability of the physical forensic methods of the forensic model in the Samsung smartwatch, the interface and memory chip of the PCB were analyzed. The PCB of Galaxy Watch 3 is shown in Fig. 3. There are unmarked ports along with the processor and memory chip on the PCB of the Galaxy Watch 3. The six ports were estimated to be service ports [28]. As the experiment was conducted using a Bluetooth model, the Galaxy Watch 3 was paired with Galaxy S9+. The service port was connected to the PC using a standard wire. As shown in Fig. 4, the service port of Galaxy Watch 3 was soldered and connected to the PC. As a result, it was impossible to recognize the Galaxy Watch 3 in the PC in the normal booting

Fig. 2 Screen of Galaxy watch 3 after flashing custom firmware using Odin

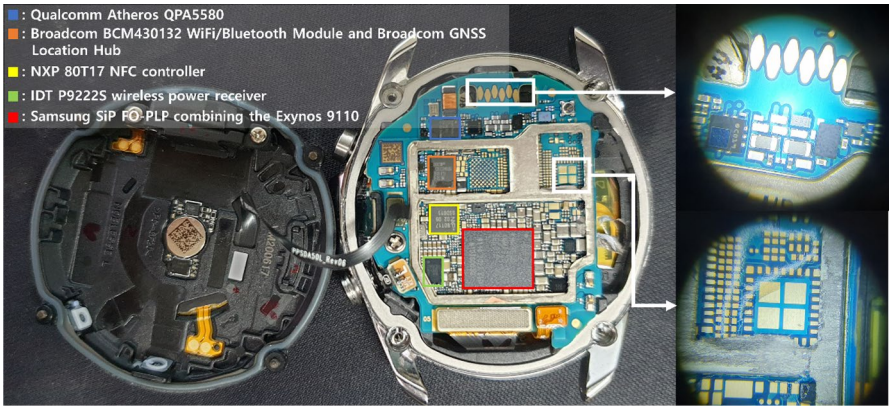


Fig. 3 PCB of Galaxy watch 3—on the right is an enlarged view of the unmarked port on the PCB

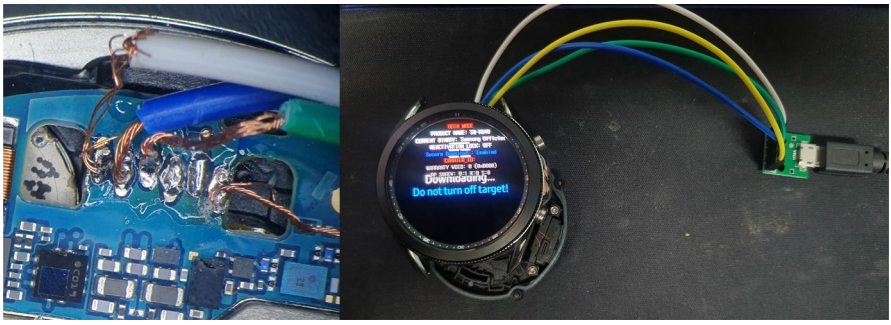
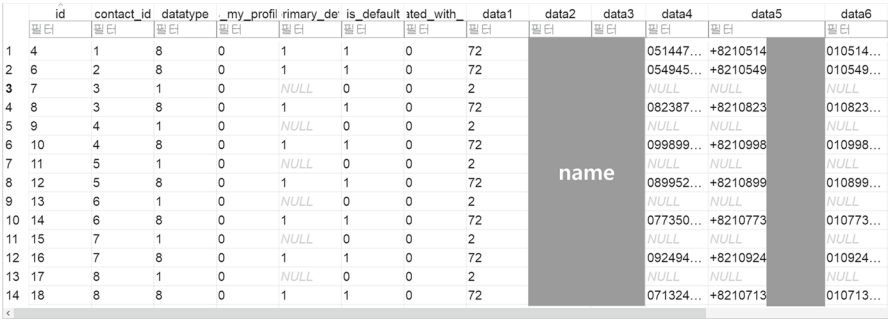


Fig. 4 Soldering to Galaxy watch 3 PCB service port using standard wire

state, but in the download mode, it was possible to recognize it in the PC. It was possible to enter the download mode, so we focused on trying to acquire administrator privileges in the PCB service port. The result of trying to acquire administrator privileges when connecting wirelessly from the PC connection method and the result of obtaining administrator privileges when connecting with PC using PCB Service Port were the same. It is presumed that the same results were obtained because there was only a difference between the PC and the wired/wireless connection.

4.1.3 PCB debugging port

The four ports in the lower right square shown in Fig. 3 were not marked on the PCB, so it was impossible to estimate which port they were, but it is estimated that they were not debugging ports. For detailed analysis, X-ray or CT scans were required. As there are no other ports, there was no debugging port in Samsung Galaxy Watch 3.



	id	contact_id	datatype	_my_profil	rimary_de	is_default	ated_with_	data1	data2	data3	data4	data5	data6
	필터	필터	필터	필터	필터	필터	필터	필터	필터	필터	필터	필터	필터
1	4	1	8	0	1	1	0	72			051447…	+8210514	010514…
2	6	2	8	0	1	1	0	72			054945…	+8210549	010549…
3	7	3	1	0	NULL	0	0	2			NULL	NULL	NULL
4	8	3	8	0	1	1	0	72			082387…	+8210823	010823…
5	9	4	1	0	NULL	0	0	2			NULL	NULL	NULL
6	10	4	8	0	1	1	0	72			099899…	+8210998	010998…
7	11	5	1	0	NULL	0	0	2			NULL	NULL	NULL
8	12	5	8	0	1	1	0	72			089952…	+8210899	010899…
9	13	6	1	0	NULL	0	0	2			NULL	NULL	NULL
10	14	6	8	0	1	1	0	72			077350…	+8210773	010773…
11	15	7	1	0	NULL	0	0	2			NULL	NULL	NULL
12	16	7	8	0	1	1	0	72			092494…	+8210924	010924…
13	17	8	1	0	NULL	0	0	2			NULL	NULL	NULL
14	18	8	8	0	1	1	0	72			071324…	+8210713	010713…

Fig. 5 Contact information stored in '.contacts-svc.db'

	id	number	umber_typ	normal_num	clean_num	minmatch	sim_id	person_id	log_type	log_time
	필터	필터	필터	필터	필터	필터	필터	필터	필터	필터
505	2207	010824…	72	+8210824	010824…	0824	1	892	2	160695…
506	2222	010660…	72	+8210660	010660…	0660	1	867	2	160697…
507	2225	010660…	72	+8210660	010660…	0660	3	867	1	160697…
508	2226	010660…	72	+8210660	010660…	0660	3	867	6	160697…
509	2227	010660…	72	+8210660	010660…	0660	1	867	6	160697…
510	2228	114	NULL	+82114	114	114	1	NULL	101	160697…
511	2229	114	NULL	+82114	114	114	1	NULL	101	160697…
512	2230	114	NULL	+82114	114	114	1	NULL	101	160697…
513	2231	010660…	72	+8210660	010660…	0660	3	867	6	160697…
514	2232	010660…	72	+8210660	010660…	0660	1	867	6	160697…
515	2233	010660…	72	+8210660	010660…	0660	3	867	1	160697…

Fig. 6 List of call log stored in '.contacts-svc.db'

4.1.4 Chip-off

The chips marked red in Fig. 3 are the Samsung Exynos 9110 SiP of the Galaxy Watch 3. Because system-in-a-package (SiP) implements several blocks as individual chips and then combines them into a single package, it is difficult to separate the NAND flash. Therefore, it was impossible to perform a chip-off.

The Samsung smartwatches were able to acquire data through the PC connection method by applying the proposed forensic model. The total artifacts are listed in Table 5 in Appendix. In the '.contacts-svc.db' file, as shown in Figs. 5 and 6, we could confirm the contacts stored in the smartphone paired with the smartwatch and call history. In the case of sending a text message, as shown in Fig. 7, it was possible to see the message exchanged as text stored in the '.msg-consumer-server.db' file. When speech-to-text (STT) was used, such as sending a message by voice, the raw data of the voice message were stored in the 'stt_pcmdump' folder. In the folder, data that the user commanded by voice were stored, but only the last command could be obtained. In addition, various

Fig. 7 Message log stored in '.msg-consumer-server.db'

user artifacts, such as media files, and health data, were acquired. However, in the case of health data, analysis was not possible because the contents were encrypted. Devices using LTE were able to acquire additional carrier information, eSIM ID, and phone number assigned to the wearable device.

4.2 Apple smartwatches

Apple Watch Series 5 (GPS + Cellular) and Apple Watch Series 3 (GPS/GPS + Cellular) are used for forensic model applicability experiments for Apple smartwatches. The specifications of the Apple devices for the forensic model applicability experiment are listed in Table 2. All three devices are possible Wi-Fi, so a PC connection method can be attempted. As a result of the experiment, the applicability of the forensic model to three apple smartwatches, the same results, and the same artifacts were derived. Therefore, only the experimental process for Apple Watch Series 5 GPS + Cellular and Apple Watch Series 3 GPS + Cellular was described.

4.2.1 PC connection

Apple Watch Series 5 cannot be connected to a PC using USB because the USB provided by the manufacturer does not have DATA + and DATA pins. However, because Apple Watch Series 5 is capable of network communication using Wi-Fi, the PC connection method using Wi-Fi is possible. To wirelessly connect the Apple Watch Series 5 to the PC, the Wi-Fi network created by the Internet sharing function of MacBook was connected to the Apple smartwatch. Access to Apple Watch Series 5 data over a wireless PC connection was attempted via the Apple Filing Protocol (AFP). Apple smartwatches with watchOS were not accessible, as AFP only supports connections to devices running macOS.

Table 2 Apple smartwatches spec used in experiment

	Apple watch series 5 GPS + cellular	Apple watch series 3 GPS + cellular	Apple watch series 3 GPS
Processor	Apple S5 SiP, apple W3	Apple S3 SiP	Apple S3 SiP
Memory	1 GB LPDDR SDRAM, 32 GB	768 MB LPDDR3 SDRAM, 16 GB	768 MB LPDDR3 SDRAM, 8 GB
OS	watchOS 7.1	watchOS 7.1	watchOS 7.1
Communication	Wi-Fi 802.11b/g/n, bluetooth 5.0, NFC	Wi-Fi 802.11b/g/n, bluetooth 4.2, NFC	Wi-Fi 802.11b/g/n, bluetooth 4.2, NFC

4.2.2 Internal storage of paired devices

The Apple Watch Series 5 obtained only some data through direct forensic techniques. Therefore, Apple Watch Series 5 performed indirect forensic techniques to acquire wearable device data from the internal storage of paired devices of a paired smartphone. In order to experiment with the internal storage of paired devices, it is necessary to acquire administrator privileges for Apple smartphones in advance. To acquire administrator privileges for iPhone 7, checkraln, UNetbootin, and PuTTY were used to acquire administrator privileges for Apple smartphones. A PC using Windows 10 was used to acquire the internal storage data of an Apple smartphone.

The data of the smartphone paired with the Apple smartwatch were acquired by accessing the internal shell of the smartphone with administrator privileges. By analyzing the acquired smartphone data, only data directly related to Apple Watch Series 5 were extracted, and we were able to acquire various artifacts such as:

1. Smartwatch Bluetooth and Media Access Control (MAC) information
2. Apps installed on smartwatch
3. Mail account registered in the mail app
4. Contacts
5. Media directories and files list

Fig. 8 PCB of Apple watch series 3 (GPS + Cellular)

4.2.3 PCB service port

We analyzed the PCB of Apple Watch Series 3 (GPS + Cellular) and confirmed whether the physical forensic techniques of the forensic model can be applied to Apple smartwatches. The PCB of the Apple Watch Series 3 (GPS + Cellular) is shown in Fig. 8. Although the service port of the Apple smartwatch is not visible on the PCB, the hidden service port can be seen by removing the rubber stopper on the outside of the Apple smartwatch. To connect the Apple smartwatch with the PC, the iBUS developed by MFC TEAM was connected to the service port. After connecting the Apple smartwatch to the PC, the data were acquired using Xcode and the media data list was obtained by modifying the libimobiledevice open-source code [29]. For the PCB service port method, a list of media files was confirmed.

4.2.4 PCB debugging port

There are unmarked ports along with a microcontroller unit (MCU) on the PCB of Apple Watch Series 3 (GPS + Cellular). However, it was inferred that these ports were not related to JTAG or UART. For detailed analysis, X-ray or CT scans were required. Therefore, it was difficult to forensics through the PCB debugging port of Apple smartwatch.

4.2.5 Chip-off

Figure 8 shows the chip on the PCB of the Apple Watch Series 3 (GPS + Cellular). The PCB of Apple Watch Series 3 (GPS + Cellular) includes STMicro ST33G1M2 MCU, etc. Because the MCU is similar to the SoC, separating the NAND flash is difficult. Therefore, it was impossible to perform a chip-off.

```
[i] Successfully paired: 00008006-001434140147002E
[i] Validated paring with device 00008006-001434140147002E
[i] service 'com.apple.afc' has been started at port 49933
[i] Starting walking Apple Watch's directory...
  [Found] directory '/Downloads'
  [Found] directory '/Photos'
  [Found] directory '/Recordings'
  [Found] file '/Recordings/Recordings.db'
  [Found] directory '/Recordings/ckAssetFiles'
  [Found] directory '/Recordings/.Recordings_SUPPORT'
  [Found] directory '/Recordings/.Recordings_SUPPORT/_EXTERNAL_DATA'
  [Found] directory '/Recordings/.Recordings_SUPPORT/_FBF'
  [Found] directory '/Recordings/.CloudRecordings_SUPPORT'
  [Found] directory '/Recordings/.CloudRecordings_SUPPORT/_EXTERNAL_DATA'
  [Found] directory '/Recordings/.CloudRecordings_SUPPORT/_FBF'
  [Found] file '/Recordings/Recordings.db-shm'
  [Found] file '/Recordings/CloudRecordings.db-shm'
  [Found] file '/Recordings/CloudRecordings.db-wal'
  [Found] file '/Recordings/Recordings.db-wal'
  [Found] file '/Recordings/CloudRecordings.db'
  [Found] directory '/DCIM'
  [Found] directory '/DCIM/100APPLE'
  [Found] file '/DCIM/100APPLE/IMG_0017.JPG'
  [Found] file '/DCIM/100APPLE/IMG_0003.JPG'
  [Found] file '/DCIM/100APPLE/IMG_0082.MOV'
  [Found] file '/DCIM/100APPLE/IMG_0002.JPG'
  [Found] file '/DCIM/100APPLE/IMG_0016.JPG'
```

Fig. 9 List of media data stored on Apple Watch Series 5 (GPS + Cellular)

Apple smartwatches were able to apply a forensic model using the internal storage of paired devices and the PCB service port method. All acquired artifacts are listed in Table 6 of Appendix. Using the internal storage of the paired devices method, we were able to confirm the list of media files and their extensions stored in the Apple smartwatch. As shown in Fig. 9, a list of media files and directories existing under directories such as DCIM, downloads, and photos can be seen. If there is a file name with a timestamp among media files, the time that the user uses the smartwatch can be inferred by using the timestamp written on the file name.

4.3 Garmin smartband

Garmin Vivosport, a smartband released in 2019, was used to experiment the applicability of the forensic model to Garmin wearable devices. Table 3 lists the specifications of Garmin Vivosport. Smartbands have fewer features than smartwatches. Smartwatches are capable of network communication through Wi-Fi or eSIM, but smartbands are used by pairing with smartphones using Bluetooth. The Vivosport communicates with the cloud server by pairing with a smartphone via Bluetooth.

4.3.1 PC connection

The Garmin Vivosport USB provided by the manufacturer has GROUND, DATA+, DATA−, and POWER pins. Therefore, a wired PC connection using USB is possible. A Samsung Galaxy S10 was paired with Vivosport to communicate with the cloud server. After connecting to a PC, the data were analyzed using the FTK Imager v4.3.0.18. Unlike other wearable devices, Garmin Vivosport was classified as a disk drive when connected to a USB, so all data could be acquired without administrator privileges. By analyzing the acquired data, we were able to acquire various artifacts, such as:

1. User body information (weight, gender, height)
2. Heart rate log
3. Exercise log
4. PC Connection log

Table 3 Garmin smartband spec used in experiment

	Vivosport
Processor	MAX32620L, nRF52832
Memory	10 MB
OS	SW v4.00
Communication	Bluetooth smart and ANT+

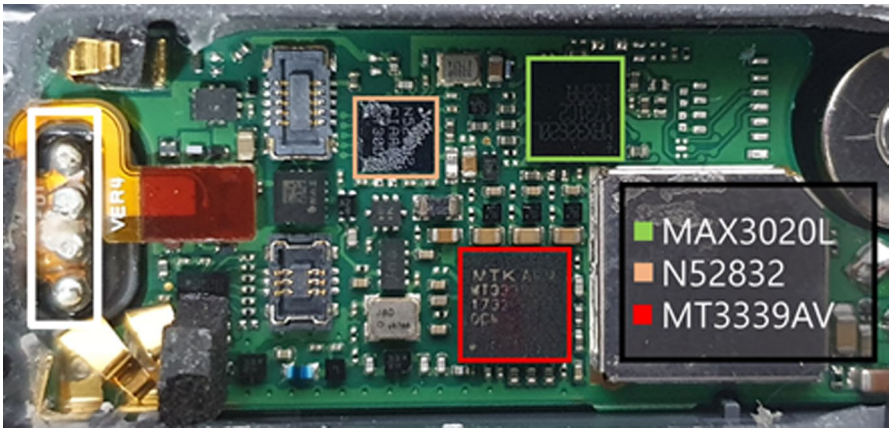


Fig. 10 PCB of Garmin Vivosport

4.3.2 PCB service port

The PCB of Garmin Vivosport is shown in Fig. 10; there were four ports. The USB provided by Garmin has GROUND, DATA +, DATA −, and POWER pins, and the USB connection location and port location were the same. Therefore, it is assumed that connecting GROUND, DATA +, DATA −, and POWER pins to the port is the same as connecting the USB. As a result, it is estimated that the Garmin Vivosport PCB Service Port result is the same as the PC connection result.

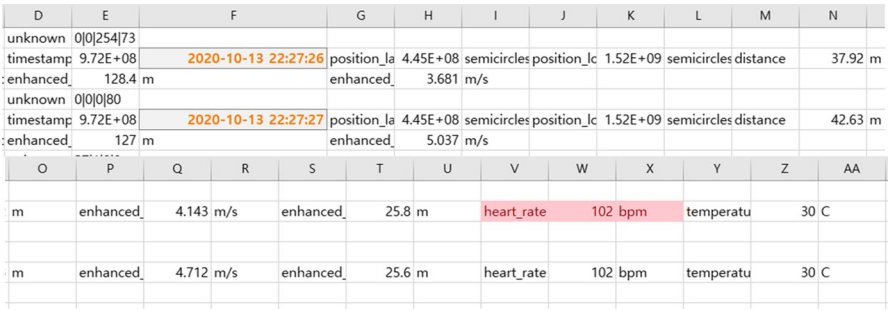
4.3.3 PCB debugging port

Figure 10 shows a PCB of Vivosport, and there was no port available for the JTAG and UART connections.

4.3.4 Chip-off

Compared with smartwatches, smartbands have a smaller PCB size and provide only relatively limited functions. Therefore, flash memory chips that can extract data from a smartband are rare. As shown in Fig. 10, the chips on the PCB of Garmin Vivosport are MAX3020L, N52832, etc. Both MAX3020L and N52832 ARM chips have a flash memory capacity that is significantly less than 10 MB. It was assumed that a separate memory chip was present on the board. However, the size of the remaining chips was small, even with a microscope, and thus, it was impossible to confirm.

Garmin Vivosport was able to acquire internal smartband storage data by applying the proposed forensic model. When connected to a PC via USB, it was possible to access all the data of the smartband without acquiring administrator privileges.



D	E	F	G	H	I	J	K	L	M	N
unknown	0|0|254|73									
timestamp	9.72E+08	2020-10-13 22:27:26	position_la	4.45E+08	semicircles	position_lo	1.52E+09	semicircles	distance	37.92 m
enhanced_	128.4 m		enhanced_	3.681	m/s					
unknown	0|0|0|80									
timestamp	9.72E+08	2020-10-13 22:27:27	position_la	4.45E+08	semicircles	position_lo	1.52E+09	semicircles	distance	42.63 m
enhanced_	127 m		enhanced_	5.037	m/s					

O	P	Q	R	S	T	U	V	W	X	Y	Z	AA
m	enhanced_	4.143	m/s	enhanced_	25.8	m	heart_rate	102	bpm	temperatu	30	C
m	enhanced_	4.712	m/s	enhanced_	25.6	m	heart_rate	102	bpm	temperatu	30	C

Fig. 11 FIT exercise log file saved in '/GARMIN/ACTIVITY/

Artifacts obtained from Garmin Vivosport are shown in Table 7 of Appendix. All data were saved as flexible and interoperable data transfer (FIT) files with the exception of connection records. Garmin devices manage almost all data through FIT files, and Garmin provides a FIT file conversion tool through the official developer website [30]. Figure 11 shows the conversion of the FIT exercise log file into a CSV file using the program on the official website. The files included a timestamp, heart rate, body temperature, and distance exercised. The position coordinates could be confirmed using the position_lat and position_lon values stored in the file in the '/GARMIN/ACTIVITY/' directory. Because the Garmin smartband can forensically acquire basic user information, health information, and even location information, meaningful artifacts can be acquired when acquiring a Garmin wearable device in an actual investigation.

5 Discussion

To construct a forensic model of wearable devices, an ecosystem of wearable devices was derived by identifying the major interfaces and connection configurations. Table 4 shows the results of applying the forensic model to the wearable devices. 'Forensic methods can be tried on the wearable device, and user artifacts can be acquired' is the '●' symbol, 'Forensic methods can be tried on the wearable device, but user artifacts cannot be acquired' is the '◑' symbol, 'Did not attempt to apply the forensic method to the wearable device' is the '-' symbol, and 'Attempted to apply the forensic method to the wearable device, but could not apply it' is the 'X' symbol.

When the proposed forensic model was applied to Samsung smartwatches, even without root authority, most user artifacts such as device information, SNS notifications, contacts, health could be acquired through the PC connection method. However, because the health data are user-sensitive, health data are encrypted, and thus, detailed analysis cannot be performed. When the STT function was used, the raw data commanded by the user were saved, but only the last command could be obtained. An additional experiment was performed on a device using LTE, showing

Table 4 Results of Applying the Forensic Model to Wearable Devices

	Device	Forensic model					
		PC connection (user authority)	PC connection (root privileges)	Internal storage of paired device	PCB service port	PCB debugging port	Chip-off
Smart watch	Samsung galaxy watch 3	●	◑	–	◑	X	X
	Samsung galaxy active 2	●	◑	–	◑	X	X
	Samsung galaxy watch 1	●	◑	–	◑	X	X
	Apple watch series 5 (GPS + cellular)	X	–	●	●	X	X
	Apple watch series 3 (GPS + cellular)	X	–	●	●	X	X
	Apple watch series 3 (GPS)	X	–	●	●	X	X
Smartband	GarminVivosport	●	–	–	–	X	X

●: Forensic methods can be tried on the wearable device, and user artifacts can be acquired

◑: Forensic methods can be tried on the wearable device, but user artifacts cannot be acquired

-: Did not attempt to apply the forensic method to the wearable device

X: Attempted to apply the forensic method to the wearable device, but could not apply it

the difference in the ability to obtain carrier information, eSIM ID, and mobile phone number assigned to the wearable device.

When the forensic model was applied to Apple smartwatches, artifacts such as smartwatch information, email and contacts were acquired through internal storage of the paired device method. When the internal storage of the paired devices method is performed, there is a limitation in that the smartphone must be jailbroken.

When this forensic model was applied to Garmin smartband, unlike other wearable devices, the Garmin smartband was recognized as a disk drive when connected to a PC, and thus, it was able to acquire all data without the administrator privileges such as user information, exercise records.

By applying this forensic model to wearable devices, it is possible to acquire artifacts in all devices. However, because of the miniaturization of the PCB of the wearable devices, the debugging port could not be identified, and the NAND flash chip did not exist alone, making chip-off impossible in all devices. In addition, some manufacturers encrypt sensitive information about users, making data analysis impossible.

Deriving an ecosystem for wearable devices and applying a forensic model means a variety of devices that can be used in the actual investigation process. The forensics of wearable devices are significant because they can reduce the time and cost of requesting user data from the manufacturer during the investigation process and can perform cross-analysis with the data received from the manufacturer. It is also significant that it is possible to obtain accurate user health information that is not measured by a smartphone.

6 Conclusion

We constructed a forensic model focused on direct forensics for wearable devices, and user-related artifacts were identified by applying it to actual wearable devices. To construct the proposed forensic model, an ecosystem of wearable devices was derived by identifying the major interfaces and connection configurations of wearable devices. Because the applicable forensic methods differ depending on the wearable device, the forensic model was derived by dividing the forensic model into logical and physical forensic methods based on the ecosystem of the wearable devices. The proposed forensic model was applied to Samsung, Apple, and Garmin wearable devices to the confirm its applicability. Meaningful data such as call and text message history, voice assistant records, media files, reminders, and health records were obtained with user privileges when using Samsung smartwatches. However, because the health data were encrypted, we could not analyze them. Furthermore, data about e-mail accounts, installed apps, Bluetooth, and smartwatch MAC addresses were obtained using a forensic smartphone paired with Apple smartwatches. The Garmin smartband was recognized as a disk drive when using the PC connection method, and all data such as user information, exercise record, and heart rate were acquired without obtaining administrator privilege. Our results demonstrate that significant artifacts could be acquired in all the wearable devices used in the experiment.

Table 5 Artifacts obtained as a result of applying a forensic model to the Galaxy watch 3, Galaxy active 2, Galaxy watch 1

Type	Path	File name	Artifact
Device information	/opt/usr/home/owner/apps_rw/com.samsung.w-manager-service/data/	WearbleStatus.xml	Device Type, version, number(LTE)
Connected smartphone information	/opt/usr/home/owner/apps_rw/com.samsung.w-manager-service/data/	HostStatus.xml	Device Type, number(LTE)
	/opt/usr/home/owner/media/Downloads/.bt_dump/	*.log	Device Type
	/opt/dbspace/5001/	.account.db	Samsung account
Connected Bluetooth information	/opt/dbspace/	.Bluetooth_device.db	Connected time, Bluetooth address
Media file	/opt/usr/home/owner/.application/dbspace/	.media.db	Storage path, file size
	/opt/usr/home/owner/media/*/	*	Media file
wnoti	/opt/usr/dbspace/	.wnoti-service.db	Storage path, reminder time
	/opt/usr/data/wnoti/	*	Photo
Text message	/opt/usr/home/owner/apps_rw/com.samsung.message/data/dbspace/	.msg-consumer-server.db	SMS content, phone number
Voice message	/opt/usr/data/voice/stt/	stt_pcmdump	raw data of voice message
Contacts	/opt/usr/home/owner/.applications/dbspace/privacy	.contacts-svc.db	Name, phone call list, phone number
Reminder	/opt/usr/home/owner/apps_rw/com.samsung.w-reminder/data/	.reminder.db	Reminder content, setting time
Calender	/opt/usr/home/owner/apps_rw/com.samsung.w-calendar2/data/	.calendar_onsumer.db	Calender content, setting time
Alarm	/opt/usr/home/owner/apps_rw/com.samsung.alarm-solis/data/	.alarm.db	Alarm content, setting time
Location	/opt/usr/home/owner/apps_rw/.shared/com.samsung.weather/data/db/	.weather.db	Address
App usage log	/opt/dbspace/	.battery-monitor.db	App usage time
	/opt/usr/home/owner/.application/dbspace/	.context-app-history.db	App usage time
Blood pressure sensor	/tmp/	pressure_event.log	Measurement time, sensor value
	/opt/dbspace/	.context-sensor-recorder.db	Measurement time, sensor value
CMC log	/opt/usr/home/owner/apps_rw/com.samsung.cmc/data/	cmc_ulog	CMC usage time

Table 5 (continued)

Type	Path	File name	Artifact
Samsung health	/opt/usr/home/owner/apps_rw/com.samsung.shealth_gear/data/	.shealth.db	Encrypted
	/opt/usr/home/owner/apps_rw/com.samsung.shealth_gear/data/logfiles/	*	
	/opt/usr/home/owner/apps_rw/com.samsung.health.samd.bp/data/	health.samd.db	
		health.samd.ecg.db	
User credential	/opt/usr/home/owner/apps_rw/com.samsung.tizen.samsung-account/data/	samsungaccount.db	AuthToken, UserID
Filesystem	/etc./	fstab	Filesystem type
Certificate	/opt/share/cert-svc/dbspace/	certs-meta.db	Certificate list
eSIM	/opt/usr/data/esim/	esim_log	Carrier information
	/opt/usr/home/owner/.applications/dbspace/privacy/	.contacts-svc.db	eSIM ID(LTE)

In future studies, we intend to decrypt the encrypted health data acquired from

Table 6 Artifacts obtained as a result of applying a forensic model to the Apple Watch Series 5 (GPS + Cellular), Apple Watch Series 3 (GPS + Cellular/GPS)

Type	Path	File name	Artifact
Bluetooth information	/User/Library/DeviceRegistry.state/	historySecureProperties.plist	Bluetooth MAC address
MAC information	/User/Library/DeviceRegistry.state/	historySecureProperties.plist	Smartwatch MAC address
Smartwatch name	/User/Library/Health/	healthdb.sqlite	User setting name
Installed app list	/User/Library/DeviceRegistry/F79AD633-912E-4E6B-B3FD-D830AFF1BA96/com.apple.private.nanoresourcegrabber/received/	*	Installed app
Mail address	/User/Library/DeviceRegistry/F79AD633-912E-4E6B-B3FD-D830AFF1BA96/NanoMail/	registry.sqlite	Email account registered in the mail app
Contacts	/User/Library/DeviceRegistry/F79AD633-912E-4E6B-B3FD-D830AFF1BA96/AddressBook/	ABSABShadow.db	Number of saved contacts
Media file list	/DCIM /Photos /Recordings /Downloads	*	Media directories and files list

Samsung wearable devices and extract media files from Apple wearable devices based on the media file list acquired from Apple wearable devices. In addition, we

Table 7 Artifacts obtained as a result of applying a forensic model to the Garmin Vivosport

Type	Path	File name	Artifact
Exercise log	/GARMIN/ACTIVITY/	*.FIT	timestamp, heart bpm, activity_type, distance
Heart rate log	/GARMIN/MONITOR/	*.FIT	timestamp, heart rate
	/GARMIN/SLEEP/	*.FIT	timestamp, heart rate
Connection log	/GARMIN/EVENTLOGS/	*.txt	timestamp, PC connect times
Setting log	/GARMIN/SETTINGS/	SETTINGS.FIT	weight, gender, height, language,

plan to conduct research on the latest Samsung wearable device released in August 2021, which uses the Wear OS.

Appendix

See Table 5.
See Table 6.
See Table 7.

Acknowledgements This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT & Future Planning (NRF-2018R1D1A1B07043349). This research was supported by Energy Cloud R&D Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT (NRF-2019M3F2A1073385)

References

1. Kim S, Jo W, Shon T (2020) APAD: autoencoder-based payload anomaly detection for industrial IoE. Appl Soft Comput 88:106017
2. Kwon S, Yoo H, Shon T (2020) IEEE 1815.1-based power system security with bidirectional RNN-based network anomalous attack detection for cyber-physical system. IEEE Access 8:77572–77586
3. Kim H, Kim S, Jo W, Kim KH, Shon T (2021) Unknown payload anomaly detection based on format and field semantics inference in cyber-physical infrastructure systems. IEEE Access 9:75542–75552
4. Jiang F, Fu Y, Gupta BB, Liang Y, Rho S, Lou F, Tian Z (2018) Deep learning based multi-channel intelligent attack detection for data security. IEEE transact Sustai Comput 5(2):204–212
5. Rathore MM, Ahmad A, Paul A, Rho S (2016) Urban planning and building smart cities based on the internet of things using big data analytics. Comput Netw 101:63–80
6. Muhammad K, Ahmad J, Mehmood I, Rho S, Baik SW (2018) Convolutional neural networks based fire detection in surveillance videos. IEEE Access 6:18174–18183
7. Patently, IDC sees growth in wearables through to 2023 with apple watch leading the way, 2019.06. Accessed 29 Jan 2021 https://www.patentlyapple.com/patently-apple/
8. Lu Y, Li DX (2018) Internet of Things (IoT) cybersecurity research: A review of current research topics. IEEE Internet Things J 6(2):2103–2115

9. Hou J et al (2019) A survey on digital forensics in internet of things. IEEE Internet Things J 7(1):1–15
10. Al H, Haifa et al. (2020) State of the art in digital forensics for small scale digital devices. In: 2020 11th International Conference on Information and Communication Systems (ICICS). IEEE
11. Yang SJ et al (2017) Live acquisition of main memory data from android smartphones and smartwatches. Dig Investig 23:50–62
12. Siboni S et al (2016) Advanced security testbed framework for wearable IoT devices. ACM Transact on Internet Technol (TOIT) 16(4):1–25
13. Rughani PH, Dahiya M (2015) Analysis of android smart watch artifacts. Int J Sci Eng Res 6(8):920–930
14. Al-Sharrah, Manal, Ayed S, Imtiaz A. (2018) Watch your smartwatch. In: 2018 International Conference on Computing Sciences and Engineering (ICCSE). IEEE
15. Cyr, Britt, et al. (2014) Security analysis of wearable fitness devices (fitbit). Massachusetts Inst Technol 1
16. Ibrahim B et al. (2015) Watch what you wear: preliminary forensic analysis of smart watches. In: 2015 10th International Conference on Availability, Reliability and Security. IEEE
17. Dorai G, Shiva H, Sudhir A (2020) Data extraction and forensic analysis for smartphone paired wearables and IoT devices. In: Proceedings of the 53rd Hawaii International Conference on System Sciences
18. Kang S, Soram K, Jongsung K (2020) Forensic analysis for IoT fitness trackers and its application. Peer-to-Peer Netw Appl 13(2):564–573
19. MacDermott, Á ine, et al. (2019) Forensic analysis of wearable devices: fitbit, garmin and HETP watches. In: 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS). IEEE
20. Becirovic S, Sasa M (2019) Manual IoT forensics of a samsung gear S3 Frontier smartwatch. In: 2019 International Conference on Software, Telecommunications and Computer Networks (SoftCOM). IEEE
21. Gregorio J, Alarcos B, Gardel A (2019) Forensic analysis of nucleus RTOS on MTK smartwatches. Digital Investig 29:55–66
22. Odom NR et al (2019) Forensic inspection of sensitive user data and artifacts from smartwatch wearable devices. J Forensic Sci 64(6):1673–1686
23. Jo W et al (2019) Digital forensic practices and methodologies for AI speaker ecosystems. Digital Investig 29:S80–S93
24. Shin Y et al (2020) Certificate injection-based encrypted traffic forensics in AI speaker ecosystem. Forensic Sci Int Digital Investig 33:301010
25. Li S et al (2019) IoT forensics: amazon echo as a use case. IEEE Internet Things J 6(4):6487–6497
26. Lee S et al (2019) ExtSFR: scalable file recovery framework based on an Ext file system. Multimed Tools Appl 79:1–19
27. Counterpoint, Global smartwatch market revenue up 20% in H1 2020, Led by Apple, Garmin & Huawei, 2020.08. Accessed 29 Jan 2021, https://www.counterpointresearch.com/global-smartwatch-market-revenue-h1-2020/
28. XDA Developers, Accessed 14 Apr 2021 https://forum.xdadevelopers.com/t/galaxy-watch-active-2-44mm-sm-r820-odinstuck.4009587/#post-81471105
29. Libmobiledevice, Accessed 29 Jan 2021 https://github.com/libimobiledevice
30. Garmin Developer, Accessed 29 Jan 2021 https://developer.garmin.com/fit/overview/