International Journal of Advanced Science and Technology
Vol.117 (2018), pp.129-138
http://dx.doi.org/10.14257/ijast.2018.117.11

Preemptive Cyber Response Strategy and IoT Forensic Evidence

Jin-young Song[1] and Dea-woo Park[2*]

*[12]Hoseo Graduate School of Venture, Hoseo University, Seoul,
(06724), South Korea
[1]jedisong2083@gmail.com, [2*]prof_pdw@naver.com*

Abstract

With the development of IoT technology, the use of IoT terminals connected with smart phones is increasing. At the same time, security incidents are occurring. IoT security incidents can be linked to risk at both a personal and national level through social disruption and cyberterrorism. In this study, we analyze the security infringement environment in an IoT smart watch device. We extract forensic evidence from the watch, using a hashing function to verify data integrity, and create a forensic report to be used as legal evidence of a cyber attack point of origin. Finally, we suggest that IoT smart terminals are infiltration targets and that preventive measures and accountability should be adopted in order to form a preemptive response to attacks as part of national cyber security.

Keywords: *Cybersecurity, National cybersecurity, Cyber-attack, Preemptive response, IoT Forensic*

1. Introduction

Due to recent developments in information communication and IT technologies, household electrical appliances, mobile devices and wearable devices analyze and process data via wired / wireless communication without human control [1].

In South Korea, there were 7.7 DDoS attacks in 2009, 3.4 DDoS attacks in 2011, and the NH Agricultural Bank was brought to a standstill. Along with the JoongAng Ilbo incident in 2012, the spread of smartphones has led to phishing, pharming, and smishing attacks. In December 2014, about 25 million pieces of information were leaked from a hacker attack on KHNP (suspected to have originated in North Korea); there was a ransomware attack in 2015, and Interpark was attacked in May 2016. In August 2016, North Korean hackers hacked the Defense Integrated Data Center (DIDC), which was known to have captured PC viruses and confidential data from the Defense Ministry [2].

In the development of IoT, various data are collected and processed to provide a better environment for users in daily life [3]. From 2012, the spread of smartphones has caused phishing, pharming, and smishing attacks. With the development of IoT (Internet of Things) technology in 2017, IoT terminals in cooperation with smartphones are utilized. However, with the increase in IoT terminal equipment and technology development, many difficulties have arisen in securing and analyzing evidence for digital forensic investigation. For example, IoT smart watche devices have many different operating systems (Android, iOS, Tizen *etc.*,) and manufacturers for each device, and the method for accessing and analysing system internals is different. Nevertheless, the reason for the need for digital forensics in IoT terminals is that these devices can provide evidence and clues that can be used to prove criminal activity.

Received (April 16, 2018), Review Result (June 2, 2018), Accepted (June 10, 2018)

[*] Corresponding Author

ISSN: 2005-4238 IJAST
Copyright ⓒ 2018 SERSC Australia

For example, in the United States in 2015, heart rate data was extracted from a smart watch and the exact time of a physical attack was determined from the point of time at which the heart rate peaked. In other words, the various kinds of information held in a smart watch (heart rate, daily activity, GPS location etc.) can be extracted, secured and used in legal proceedings [4].

In this study, we show how to acquire smartwatch data and forensic evidence as an example of how IoT devices can be used as statutory evidence. Forensic extraction of attack data for IoT smart watch devices is important for determining the point of origin of an APT (Advanced Persistent Threat) cyber terrorism attack. We propose data extraction and digital forensics as part of a preemptive cyberterrorism countermeasure strategy.

2. Related Works

2.1. Android Wear

Android's Wear OS is a Google Android operating system designed for wearable devices such as smart watches. Wear OS pairs wearable devices with an Android smartphone, enabling bidirectional data transmission. The current version of Android Wear is 2.8, which will work with Android version 7.0 or higher [5].

Android Wear can support Bluetooth, Wi-Fi, and various functions and applications via LTE. Many hardware manufacturers, such as Samsung and LG, are producing a variety of smart wearable devices based on Android's Wear OS. The user can control the smartphone using Android Wear. For example, it is possible to access music, voice call, message transmission, location information and fitness management functions.

2.2. Android Debug Bridge

(ADB) Android Debug Bridge is a terminal tool that can communicate with Emulator Instances and Android Devices. This tool provides a Unix shell on a connected computer which can be used to execute various commands on an Android device; commands include functions to install and debug applications on the Android device. This tool has the following three features [6].

1) You can invoke the Android device client from the terminal by running the ADB command. 2) When executing commands on the computer, the daemons that run are executed as background processes inside each Android device. 3) The server that manages the communication between the client and the daemon runs in the background of the computer.

2.3. Digital Forensics

Digital forensics refers to the procedures related to the preparation of a report in the preliminary stages of an investigation. These procedures include the acquisition of the main items of information, the transfer and storage of evidence, and the analysis of the evidence before submitting to a judicial agency [7]. This represents a breakthrough in that it provides evidence and clues that were not available in the past. Digital Forensics has become a key element in cybercriminal tracking and investigation as hackers and cybercriminals leave a variety of electronic evidence in the operating system, applications, memory, *etc.*, of computers, e-mail, and IoT devices [8].

Copyright ⓒ 2018 SERSC Australia

2.4. Digital Forensic Tool

The digital forensic tool is a tool developed to aid investigation. Domestic investigative agencies use tools that integrate a series of processes, such as collection, analysis, and reporting of evidence [9].

Typically, Guidance Software's EnCase and AccessData's FTK Imager are used. Domestically developed tools include Final Data's Final Forensics and the Prosecution Agency’s EE (Digital Evidence Analysis System for computer forensics) [10] [11].

3. Forensic Evidence for Preemptive Cyber Response Strategy

An act of cyberterrorism is a case where at least 2 cybercrimes simultaneously occur through an information and communication network infrastructure. These crimes may include stealing, distorting or propagating national and social infrastructure information involving national security. This information may include foreign affairs, national defense, unification, administration, social living and personal safety information, and may involve infringement, information draining, misusing the rights thereof, operating illegal websites, and corrupting and deleting the information.

In particular, since recent smartphones contain important personal information, cyber-attacks against smart watches connected with IoT are increasing. A user who fails to respond to these cyber-attacks on a proactive basis will become subject to the crisis of online cyber terrorism and cyber warfare

3.1. Extraction Scenario of Cyber-attack Evidence

In this thesis, we propose a method of extracting call logs, letters and images from an LG G Watch Urbane smart watch. The smart watch is paired with a Samsung Galaxy S6 smartphone. Smartphone images, messages, call logs, etc. are linked with the smart watch. The smart watch is connected to a computer for analysis. The computer is used to access the smart watch adb shell in order to extract smart watch data. The smart watch secures administrator privileges via routing in the absence of administrator authorization.

After establishing administrator access privileges, internal data is transferred from the smart watch to the computer for analysis. The transmitted internal data is analyzed using a forensic tool.

3.2. Evidence Extraction Scenario

The following environment was used to extract data from the smart watch.

Table 1. Test Environment

Tool	Function	Major features
Samsung Notebook Always 9	PC Analysis	Windows 10, Android SDK
Samsung Galaxy S6	Test SmartPhone	Android X
LG G Watch Urbane	Test SmartWatch	Android Wear 2.0
SuperSU, TWRP	Root	Root and Custom Rom

In order to access the smart watch adb shell, the PC must be connected to the watch. The LG G Watch Urbane Smart Watch does not have its own USB port and can not be directly physically connected. USB connection is possible through the watch’s charger when it is connected to the watch.

Copyright ⓒ 2018 SERSC Australia

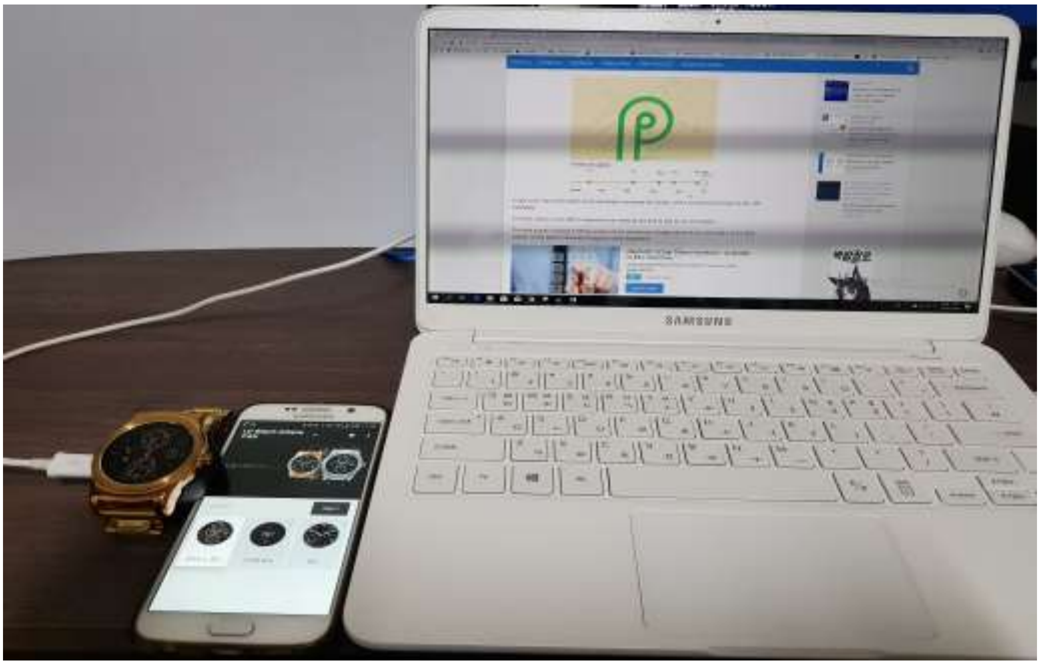


Figure 1. Test Environment

3.3. Evidence Extraction Scenario

USB debugging is enabled on the LG G Watch Urbane in order to obtain administrator privileges on the smart watch.

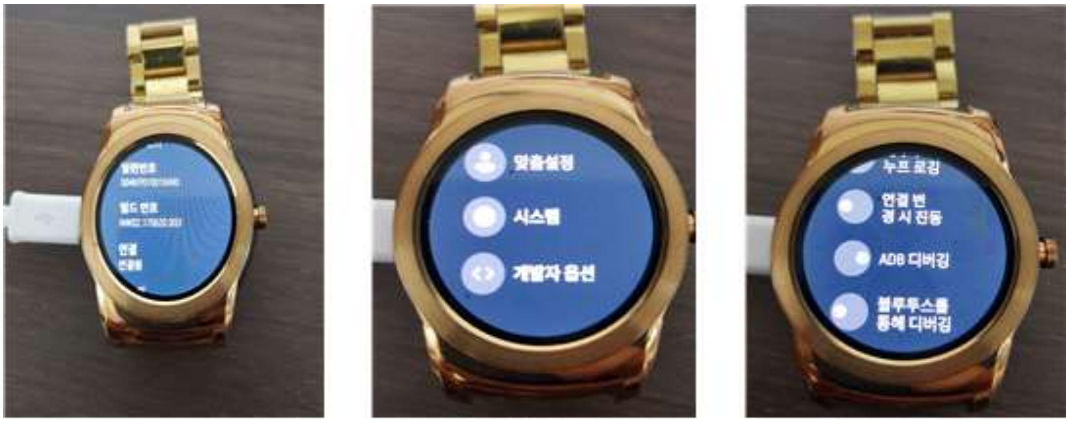
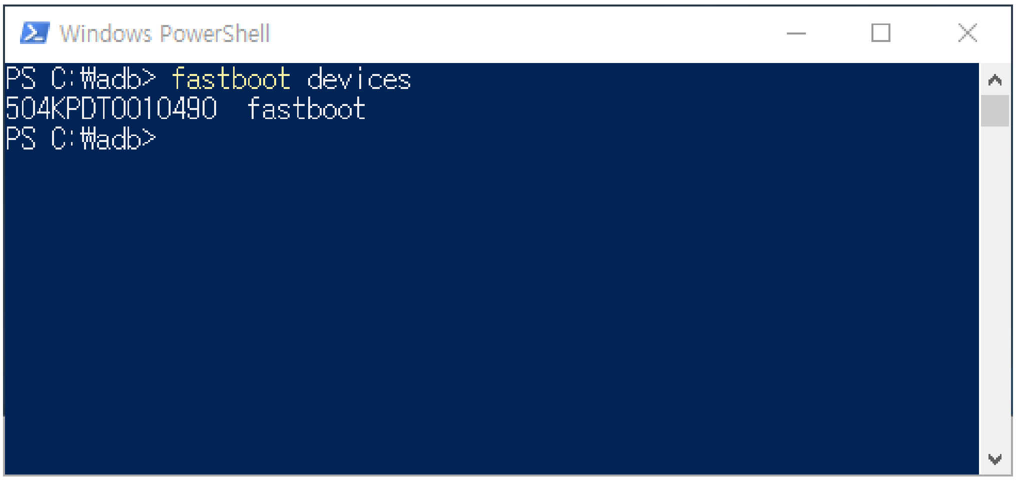


Figure 2. Smart Watch USB Debugging

In the smart watch settings software information section, the build number is pressed 7 to 8 times in order to enter developer mode. Entering developer mode activates USB debugging.

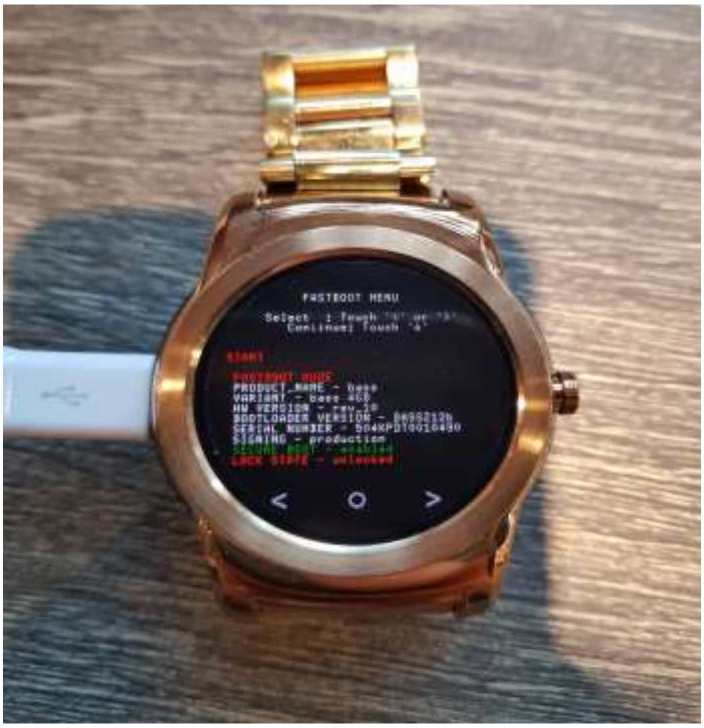
Copyright © 2018 SERSC Australia



```
PS C:₩adb> fastboot devices
504KPDT0010490  fastboot
PS C:₩adb>
```

Figure 3. Fastboot Devices

We locate the adb.exe and fastboot.exe files in the Android SDK folder, then run the terminal.



```
FASTBOOT MENU

Select : Touch [illegible]
Continue: Touch [illegible]

START

FASTBOOT MODE
PRODUCT_NAME - bass
VARIANT - bass 4GB
HW VERSION - rev_10
BOOTLOADER VERSION - [illegible]
SERIAL NUMBER - 504KPDT0010490
SIGNING - production
SECURE BOOT - enabled
LOCK STATE - unlocked
```

Figure 4. Smart Watch Fastboot Devices Mode

We execute the ADB ‘devices’ command to check the connection status of the LG G Watch Urbane Smart Watch.

We enter the ADB ‘reboot bootloader’ command to run the smart watch boot loader. After running the boot loader, we run ‘unlock’ to install the custom ROM. The custom ROM's TWRP performs various tasks such as backup and SuperSU installation.

To upload the TWRP image file to the LG G Watch Urbane smart watch, we enter the following command:

ADB push .\twrp-3.2.1-0-bass.img

After upload is completed, we use fastboot to access TWRP with custom ROM:

```
fastboot boot .\twrp-3.2.1-0-bass.img
```

When accessing TWRP with custom ROM, the following screen will be output in the LG G Watch Urbane Smart Watch.

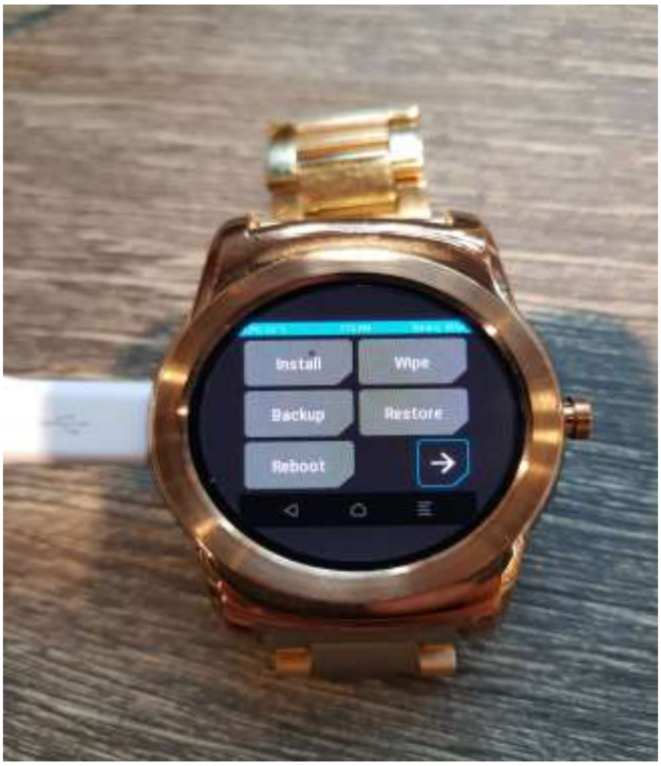


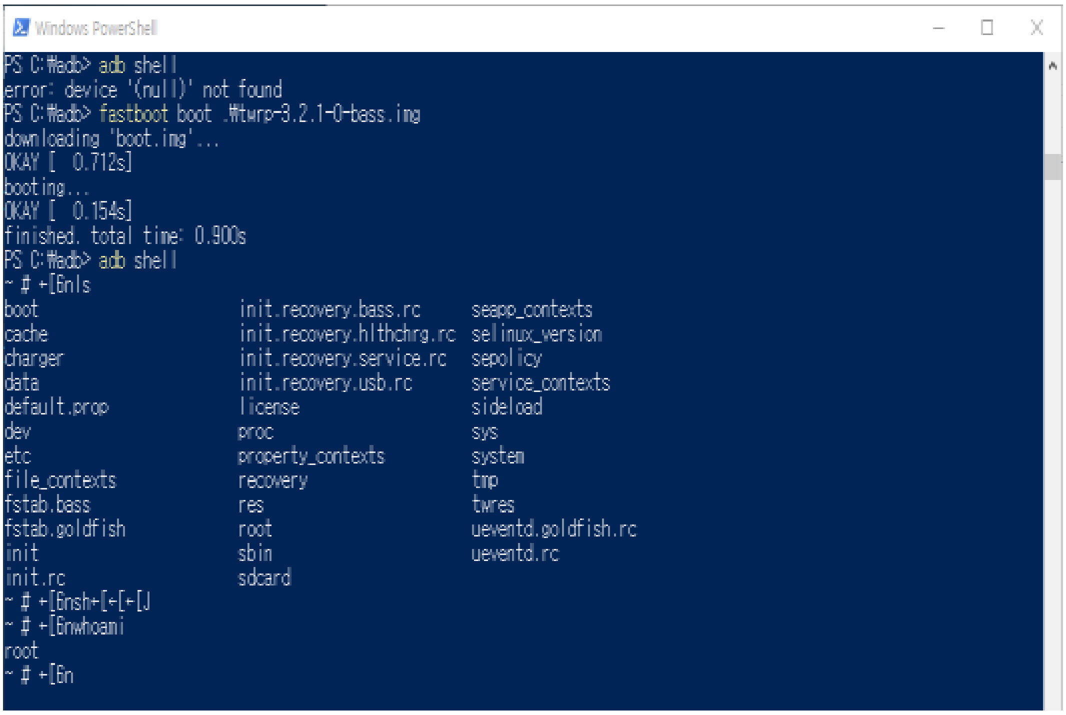
Figure 5. Smart Watch Custom ROM Mode

After entering TWRP, we install SuperSU to obtain root authority. We install the SuperSU.zip file from the install - install zip menu on the TWRP menu.

```
ADB push SuperSU.zip /sdcard/
```

In LG G Watch Urbane Terminal mode, you can see that the shell has root privileges. In order to view and modify internal data from Android, it is necessary to have root privileges, without which it is not possible to extract and view data.

When root privileges are acquired, it is possible to prepare an environment where the internal data of the LG G Watch Urbane Smart Watch can be secured as follows.

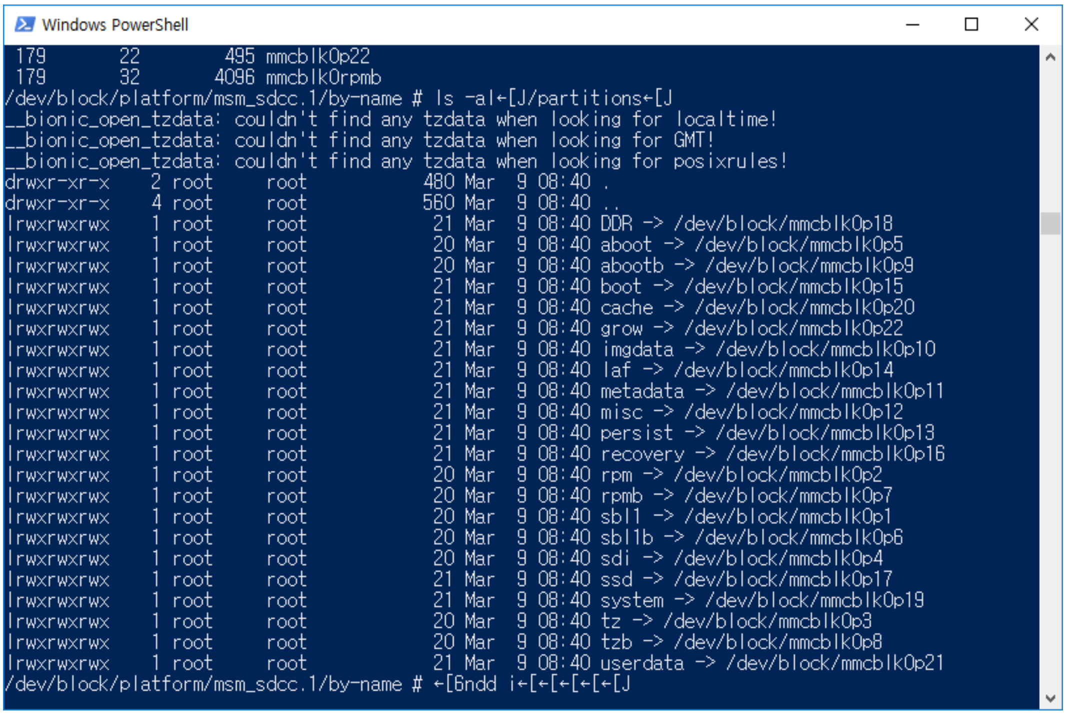


```
PS C:\adb> adb shell
error: device '(null)' not found
PS C:\adb> fastboot boot .\twrp-3.2.1-0-bass.img
downloading 'boot.img'...
OKAY [  0.712s]
booting...
OKAY [  0.154s]
finished. total time: 0.900s
PS C:\adb> adb shell
~ # ←[6nls
boot                       init.recovery.bass.rc      seapp_contexts
cache                      init.recovery.hlthchrg.rc  selinux_version
charger                    init.recovery.service.rc   sepolicy
data                       init.recovery.usb.rc       service_contexts
default.prop               license                    sideload
dev                        proc                       sys
etc                        property_contexts          system
file_contexts              recovery                   tmp
fstab.bass                 res                        twres
fstab.goldfish             root                       ueventd.goldfish.rc
init                       sbin                       ueventd.rc
init.rc                    sdcard
~ # ←[6nsh←[←[←[J
~ # ←[6nwhoami
root
~ # ←[6n
```

Figure 6a. Smart Watch ADB Shell

3.4. Extract Data from Smart Watch

In order to extract the user data from the watch, we browse to the directory containing ‘userdata’.



```
 179        22         495 mmcblk0p22
 179        32        4096 mmcblk0rpmb
/dev/block/platform/msm_sdcc.1/by-name # ls -al←[J/partitions←[J
__bionic_open_tzdata: couldn't find any tzdata when looking for localtime!
__bionic_open_tzdata: couldn't find any tzdata when looking for GMT!
__bionic_open_tzdata: couldn't find any tzdata when looking for posixrules!
drwxr-xr-x    2 root     root             480 Mar  9 08:40 .
drwxr-xr-x    4 root     root             560 Mar  9 08:40 ..
lrwxrwxrwx    1 root     root              21 Mar  9 08:40 DDR -> /dev/block/mmcblk0p18
lrwxrwxrwx    1 root     root              20 Mar  9 08:40 aboot -> /dev/block/mmcblk0p5
lrwxrwxrwx    1 root     root              20 Mar  9 08:40 abootb -> /dev/block/mmcblk0p9
lrwxrwxrwx    1 root     root              21 Mar  9 08:40 boot -> /dev/block/mmcblk0p15
lrwxrwxrwx    1 root     root              21 Mar  9 08:40 cache -> /dev/block/mmcblk0p20
lrwxrwxrwx    1 root     root              21 Mar  9 08:40 grow -> /dev/block/mmcblk0p22
lrwxrwxrwx    1 root     root              21 Mar  9 08:40 imgdata -> /dev/block/mmcblk0p10
lrwxrwxrwx    1 root     root              21 Mar  9 08:40 laf -> /dev/block/mmcblk0p14
lrwxrwxrwx    1 root     root              21 Mar  9 08:40 metadata -> /dev/block/mmcblk0p11
lrwxrwxrwx    1 root     root              21 Mar  9 08:40 misc -> /dev/block/mmcblk0p12
lrwxrwxrwx    1 root     root              21 Mar  9 08:40 persist -> /dev/block/mmcblk0p13
lrwxrwxrwx    1 root     root              21 Mar  9 08:40 recovery -> /dev/block/mmcblk0p16
lrwxrwxrwx    1 root     root              20 Mar  9 08:40 rpm -> /dev/block/mmcblk0p2
lrwxrwxrwx    1 root     root              20 Mar  9 08:40 rpmb -> /dev/block/mmcblk0p7
lrwxrwxrwx    1 root     root              20 Mar  9 08:40 sbl1 -> /dev/block/mmcblk0p1
lrwxrwxrwx    1 root     root              20 Mar  9 08:40 sbl1b -> /dev/block/mmcblk0p6
lrwxrwxrwx    1 root     root              20 Mar  9 08:40 sdi -> /dev/block/mmcblk0p4
lrwxrwxrwx    1 root     root              21 Mar  9 08:40 ssd -> /dev/block/mmcblk0p17
lrwxrwxrwx    1 root     root              21 Mar  9 08:40 system -> /dev/block/mmcblk0p19
lrwxrwxrwx    1 root     root              20 Mar  9 08:40 tz -> /dev/block/mmcblk0p3
lrwxrwxrwx    1 root     root              20 Mar  9 08:40 tzb -> /dev/block/mmcblk0p8
lrwxrwxrwx    1 root     root              21 Mar  9 08:40 userdata -> /dev/block/mmcblk0p21
/dev/block/platform/msm_sdcc.1/by-name # ←[6ndd i←[←[←[←[J
```

Figure 6b. Smart Watch ADB Shell

When browsing the /dev/block/platform/msm_Sdcc.1/by-name folder, we can confirm that userdata is linked with / dev / block / mmcblk 0p21.

Copyright ⓒ 2018 SERSC Australia

The ‘userdata’ folder contains data generated by using the smart watch, such as application installations, phone and messaging data, health information and multimedia files. In order to collect digital evidence, userdata must be extracted.

The data is extracted and transferred to the PC using the Linux ‘dd’ command:

```
dd if=/dev/block/mmcblk0p21 of=/sdcard/userdata.dd bs=4k
```

We now analyze the image file transferred to the PC using the file analysis tool.

3.5. Data Analysis

We use an image file analysis tool to analyze the image file of the data transferred from the LG G Watch Urbane Smart Watch.

In this project, we used open source software rather than proprietary. Autopsy was used for detailed classification of imaging files, and database information was read using SQL lite for database files.

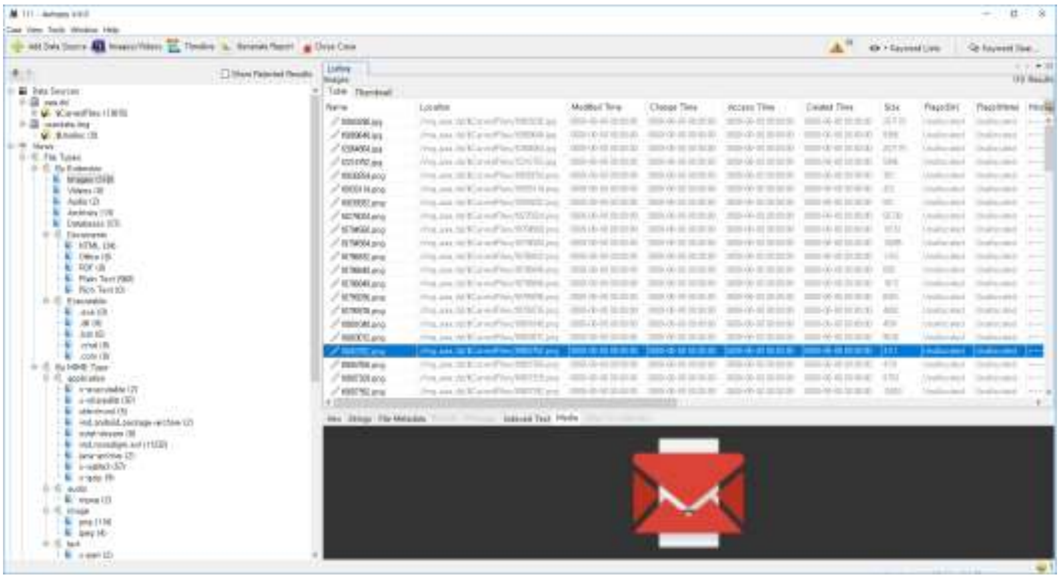


Figure 7. Imaging Data Analysis Tool

The analysis categorizes images, text messages, e-mail addresses, heart rate, and multimedia files in the LG G Watch Urbane smart watch's internal memory. It was possible to visually check the data of each application's database and of the smartphone.

However, some DB files were encrypted, and it was not possible to identify them just by looking. This may be a result of the Android security policy encrypting sensitive data in order to suppress the leakage of personal information through hacking.

Copyright ⓒ 2018 SERSC Australia

3.6. Preemptive Cyber Response Strategy on Cyber-Attack Origin

It is difficult to discern the origin of cyber-attacks in organized APT attacks made by states and governments, and to obtain hard evidence confirming the origin. APT attacks from North Korea and overseas are carried out systematically over long periods of time. Long, systematic attacks are made on IoT Smart terminals which are remote from the final targets that play an important role in national cybersecurity. The recently developed IoT Smart terminal is a good means of infiltration and can be used as a link to the ultimate target of the attack.

Forensic extraction of attack data from IoT terminals is important for discerning the origin of attacks. Ultimately, prevention of IoT Smart terminal attacks and the distribution of responsibilities will be a necessary part of national cyber security. Smart terminals may even be used as sentinels as part of a preemptive response strategy to protect national cyber security.

Of course, in order to identify the analysis data for detecting the cyber-attack origin, Network Forensic and System Forensic technologies must be supported.

4. Conclusion

In this thesis, we have studied the preemptive response strategy for cyber-attacker origin for national cybersecurity. Forensic extraction of attack data in IoT Smart Watch terminals is important for understanding the attack point of origin. Ultimately, prevention of IoT Smart terminal attacks and the distribution of responsibilities will be a necessary part of national cyber security. Smart terminals may even be used as sentinels as part of a preemptive response strategy to protect national cyber security.

We demonstrated a method of extracting evidence from an LG G Watch Urbane smart watch, which is based on Android Wear OS. We set up an environment for obtaining evidence from the IoT terminal using ADB debugging in Android Wear OS, Bluetooth debugging and ADB in the Android SDK to access the internal memory of the smart watch. Imaging work was carried out to verify the data integrity after transferring the internal memory of the Smart Watch terminal. We conducted IoT terminal forensics to obtain evidential material from the smart watch terminal.

In the future, we will study how to decrypt the encrypted Information file in the cloud for cybersecurity.

Acknowledgments

This research was supported by the Academic Research Fund of Hoseo University in 2017 (No. 2017-0043).

References

[1] J. S. Yang and J. Y. Kim, “Case study analysis of wearable devices in the new media”, Journal of the Institute of Design and Culture of Korea, vol. 20, no. 2, **(2014)**, pp. 354-364.

[2] D. G. Gim, D. Y. Jeon and C. S. Lee, “A study on digital forensic process model of wireless router”, Digital Forensics Research, vol. 11, no. 1, **(2017)**, pp. 17-35.

[3] Hur and Kyeong, “A Hierarchical MAC Protocol for QoS Support in Wireless Wearable Computer Systems”, The Korean Institute of Information and Communication Engineering, vol. 11, no. 1, **(2014)**, pp. 14-18.

[4] I. H. Youn and J. H. Youn, “Navigator Lookout Activity Classification Using Wearable Accelerometers”, The Korean Institute of Information and Communication Engineering, vol. 15, no. 3, **(2017)**, pp. 182-186.
H. V. Jansen, N. R. Tas and J. W. Berenschot, “Encyclopedia of Nanoscience and Nanotechnology”, Edited H. S. Nalwa, American Scientific Publishers, Los Angeles, vol. 5, **(2004)**, pp. 163-275.

[5] D. Igebo and S. Bakudeo, “Mobile phone seizure search Prove consistency of standard procedure and forensic”, Korean Telecommunications Association Transactions, vol. 33, no. 6, **(2008)**, pp. 512-519.

[6] K. H. Kim and S. Bakudeo, “Study on a method to prove consistency in mobile forensics”, Korean Computer Informatics Journal, vol. 15, no. 1, **(2007)**. pp. 37-46.

[7] S. W. Sin. “Verification of the reliability of the evidence analysis tool for digital forensics”, Journal of Information Protection Society, vol. 21, no. 3, **(2011)**, pp. 165-176.

[8] K. B. Yun, “Forensic document of Android and Windows Mobile smartphone searched for houses”, Korean Institute of Information and Communications Technology Transactions, vol. 17, no. 2, **(2013)**, pp. 323-331.

[9] J. C. Lee, “Priority scheduling of digital evidence in forensics”, Korean Institute of Information and Communications Technology Transactions, vol. 17, no. 9, **(2013)**, pp. 2055-2062.

[10] F. Johnson, “XML based IoT simulation system”, Korean Institute of Information and Communications Technology Transactions, vol. 11, no. 1, **(2016)**, pp. 663-668.

[11] J. T. Kim, H. B. Jung and D. W. Han, “Research on the trend of lightweight IoT device platform”, Korean Information Technology Association Journal, vol. 13, no. 2, **(2015)**, pp. 1-8.

Authors

Jin-young Song is a Ph.D. student at the Hoseo Graduate School of Venture. Song majored in information security at university and majored in digital forensics and hacking in his master's degree. His interests are cyber-warfare, digital forensics, and hacking. Currently, he is an expert in national cybersecurity.

Dea-woo Park is an Associate Professor in the Hoseo Graduate School of Venture at Hoseo University in South Korea. Professor Park conducts research in Cybersecurity, Hacking Forensics and Convergence of Information Communication Technology in HFICT Lab at Hoseo Graduate School. Professor Park received the B.S. degree in computer science from Soongsil University in 1995 and the M.S. degree in 1998. He received the Ph.D. degree from the computer science department of Soongsil University in 2004. He has also been appointed Secretary General of the Forum of National Cybersecurity Policy, Chair of the Korea Information Security Forum, and Vice-Chairman of the Korean Institute of Information Security & Cryptology, the Korea Information and Communications Society, and the Korea Digital Forensic Society.

Copyright ⓒ 2018 SERSC Australia