Manual IoT Forensics of a Samsung Gear S3 Frontier Smartwatch

Seila Becirovic
Faculty of Electrical Engineering
University of Sarajevo
Sarajevo, Bosnia and Herzegovina
sbecirovic1@etf.unsa.ba

Sasa Mrdovic
Faculty of Electrical Engineering
University of Sarajevo
Sarajevo, Bosnia and Herzegovina
sasa.mrdovic@etf.unsa.ba

***Abstract*—Internet of Things (IoT) devices such as Samsung Gear S3 Frontier smartwatch are great sources of potential digital evidence, due to their constant daily use. The main aim of this paper is to analyze the capabilities and limitations of IoT forensics of a Samsung Gear S3 Frontier smartwatch. Main concepts of IoT forensics, a summary of the current and future research progress and challenges, is given. A scenario of watch events during 3 hours of usage was recorded, which forensic analysis had to restore. Manual extraction and analysis of data, along with the detailed look at the discovered relevant files, and achieved results are presented. The primary contribution of this paper consists of a detailed approach to a particular smartwatch forensic, which supports future forensic investigations.**

***Keywords*—Internet of Things, IoT forensics, Security, Digital forensics, Smartwatch forensics, Samsung Gear S3 Frontier**

I. Introduction

Future of the Internet is composed of numerous connected devices, that provide different types of services to customers. As a result of this rapid growth of devices and connectivity, a network paradigm known as the Internet of Things (IoT) emerged. IoT represents new technologies that make life easier. Health and fitness applications, smart house management, agriculture, transport, storage, education, security are examples of IoT usages.

IoT, like any other system, needs a way to analyze things that happened within a system. Performing such analysis is known as forensics. IoT forensics is a rather new area of research with a lot of opportunities and open issues. It provides an abundance of forensic data that might be more difficult to obtain than in standard digital forensics.

In this paper, the focus is on the device level forensics of Samsung Gear S3 Frontier smartwatch. Although IoT forensics also includes cloud and network forensics, they are not considered here due to limited space. Practical challenges of device level analysis are presented, with the process of gathering and examining data, and evidence reviewing.

The paper is structured as follows: Second section gives a short overview of IoT forensics. Section III reviews prior work in the area of IoT forensics. The fourth section presents a scenario of events and methods of obtaining relevant data and relevant files for analysis. Section V discusses found evidence, along with the resulting timeline. Finally, the last section discusses future research and concludes the paper.

II. IoT Forensics

In [1], authors define IoT forensics as following: “IoT forensics is an especial branch of digital forensics, where the identification, collection, organization, and presentation processes deal with the IoT infrastructures to establish the facts about a criminal incident.” IoT forensics represents a combination of three digital forensics schemes:

- Device level forensics analyzes local memory of IoT devices, which is the focus of this paper.
- Network forensics analyzes network logs in search of different (IoT) data sources.
- Cloud forensics analyzes (IoT) data stored in the cloud.

IoT forensics can be divided into the following categories, as given in [2]: forensics phases, enablers, networks, sources of evidence, investigation modes, forensics models, forensics layers, forensics tools, and forensics data processing. Each category consists of different parts of IoT forensics.

IoT brings a lot of opportunities and issues in forensic analysis, that open a new chapter in digital forensics. Differences between IoT and traditional digital forensics are given in [3], and are as follows:

- *Evidence sources* - IoT has more types of sources since almost everything will be a possible source.
- *Number of devices* - The total number of IoT devices will be much bigger than a number of traditional devices and that translates to a number of devices in any particular investigation.
- *Types of evidence* - Unlike mostly standardized documents and file formats in traditional digital forensics, in IoT any and all formats are possible.
- *Quantity of data and evidence* - Due to a larger number of devices, amount of data in IoT could be in thousands of times more.
- *Types of networks and protocols* - Traditional networks are overwhelmingly TCP/IP over Ethernet, WiFi or mobile, but IoT still has a variety of networks and protocols in use like RFID, Zigbee, Z-Wawe, NFC, LoRa, to mention a few.
- *Network boundaries* - In IoT, boundary lines are becoming blurry and it is hard to distinguish one relevant network from the others.

- *What to seize* - In IoT, it is difficult to identify all possible sources of evidence and then select the most relevant ones.

Issues and opportunities, mentioned in [1] - [6], that IoT forensics bring can be summarized as following:

- In IoT environments, data can be found in different locations, outside of user control. Data are usually in the cloud, on remote and unknown location. Finding the exact location of data is troublesome and a challenging. Data can be found outside of the country, mixed with data from multiple users. Analysis of such data might be against the laws and regulations in that country. Standardized techniques for analysis of data in multiple locations are required.
- Big Data are the results of numerous IoT devices. Identifying evidence in such large quantities of data and sources is a problem. However, a large number of available information increases the chances of finding evidence. Issues of scalability and requirements for new algorithms arise.
- Lack of standardization and various devices with different software, hardware, and applications, are the sources of complexity in IoT. Different devices require prior knowledge of the device and different tools to access data and gather evidence.
- Due to the vulnerability of IoT devices to cyberattacks and usage in malicious purposes, disabling the device without destruction is necessary. It is important to mention the limited availability of evidence on the devices, due to the smaller storage, and overwriting of data.
- Even though IoT devices help users in everyday activity, lack of forensics solutions for maintaining a level of user privacy is troubling. Understanding of context, integration of privacy can encourage individuals to cooperate with law enforcement agencies.

III. State of the Art

Due to the rise of IoT devices in everyday life, research on IoT forensics is continuously conducted. In order to discuss the current state of research, papers on IoT forensics of a smart home, smart car and smartphone/smartwatch devices are considered.

A. Smart home

Smart IoT devices at home play an important part in detecting movement and sound. Analysis of them can prove the location of suspects. In [7], authors analyzed smart lights as a case study. They show a great amount of obtained data.

In [4] researches present the design of FEMS (Forensics Edge Management System), that provides autonomous security and forensic services in the smart home environment.

Authors of [8] discuss practical issues of forensic analysis in homes. They suggest a combination of cloud forensics with device forensics. They analyzed Amazon Alexa device. In order to acquire data, they designed CIFT (Cloud-based IoT Forensic Toolkit), that automates data acquisition.

In [9] data collection and analysis are done after the IoT attack. Sensors, Sen.se and Samsung hub were used. Authors suggest a model for determining implications of acquired data, with a goal of creating mobility in IoT forensics.

B. Smart car

Internet of Vehicles (IoV) represents a system that enables information sharing between a car and its sensors. It brings different opportunities and challenges to digital forensics.
In [10] framework Trust-IoV is suggested. It makes data collection and evidence preservation easier, as well as maintaining a chain of responsibility.

Authors of [11] present a mobile application called DiaLOG, that supports digital forensics. It enables connection with vehicles to authorized devices, as well as collects action and provides integrity and data protection for forensic investigations.

C. Smartphone/smartwatch

In [12] forensic analysis of social network applications on smartphones was performed. Analysis of two BlackBerrys, two iPhones, and Android phone was done. The goal was to determine which data from applications is present on devices. It is notable to mention that Android and iPhones saved significant data, while BlackBerrys did not.

Authors of [6] display a case study of Apple smartwatch. Logical data acquisition through the iPhone, as well as manual data acquisition from the smartwatch, were done.

In [13] preliminary forensic analysis of two popular smartwatches Samsung Gear 2 Neo and LG G were performed. Collecting data from rooted devices was explained well as a methodology for it.

IV. Case study

Samsung Gear S3 Frontier is a smartwatch with Tizen operating system. Aforementioned is a Linux kernel-based operating system developed by the Tizen Association, one of Samsungs partners. Applications on this operating system use SQLite databases to store data.

Prior to the forensic analysis of the device, a sequence of actual events was executed and recorded as a “scenario”. The scenario containing the exact time, event, and user activity, is shown in table I. A goal of the forensic analysis is to find data that confirm the scenario and to discover what else is on the device.

Assumptions about the device:

- The device is not locked with a pin or a pattern;
- The device is not rooted;
- The device is connected with the phone’s user account;
- The device is connected to the phone with Bluetooth;
- Data from the device are synchronized with the phone;
- Following applications can create notifications: Samsung Health, Calls, Gmail, Facebook, Messenger, Viber, Instagram, WhatsApp, Telegram and MapMyRun;
- Wireless and GPS are on, on both devices;
- MapMyRun application is installed on both devices, to determine third-party software’s data accessibility.

TABLE I
SCENARIO

Time	Event	Activity
19:13	Start	Watch is paired with phone
19:13	MapMyRun started	/
19:25	Facebook Messenger	Notification removed
19:26	Call	Answered
19:32	Facebook Messenger	Notification removed
19:55	Facebook Messenger	Notification removed
19:57	Facebook Messenger	Notification removed
19:58	Facebook Messenger	Notification removed
20:30	Facebook Messenger	Notification removed
20:35	MapMyRun paused	/
21:21	WhatsApp	Notification removed
21:50	Facebook Messenger	Notification remains
21:50	Facebook Messenger	Notification remains
21:50	SMS	Notification remains
22:18	End	Watch is in Flight mode

A. Data Acquisition

As soon as the device was taken for analysis, to protect the integrity of data, Flight mode was turned on, which effectively turned WiFi, Bluetooth, and NFC off. Tizen SDK (software development kit) and SDB (smart development bridge) were installed, to perform acquisition and analysis.

Connecting Samsung Gear S3 Frontier to the local machine is done using WiFi connection. Local WiFi network that was used for the connection was protected and not connected to the Internet, to prevent data alteration. It is possible to have WiFi or any other connection on, and others off in Flight mode, if each is turned on separately, without turning the Flight mode off.

On the device, the Debugging mode was turned on, and WiFi set in *Always on* mode. After determining the device's IP address, establishing a connection was done using Tizen Device Manager or SDB commands given in [12]. In this analysis, SDB commands were used to connect and to gather data, due to the ability to transfer hidden files and folder, which is not available when using Tizen Device Manager. Standard connection port is 26101.

The device was not rooted, so many folders and files with root privileges were not available. Given that, creating a forensic image was also not possible. SDB commands do not copy file history or owner's information.

Analysis of Tizen filesystem structure resulted in determining the two directories that are the most significant for this type of analysis: */home* and */opt*. They contain data and software specific for the watch user.

In order to acquire data, the bash script was written, which generated a cryptographic hash of all the files on the device and saved them in a file. Afterward, it copied all the files to the local machine using the SDB command. A cryptographic hash of copied files was generated as well and saved into a separate file. Differences between hash files were generated. They showed that some files weren't copied from the device to the local machine.

B. Analysis

After copying all the files, the analysis was performed. All significant files and paths to them, as well as the data that can be found in them, are given in table II. It turns out that identical copies of significant files in */home* folder exist in */opt/usr/home* folder. Therefore, for future research, analysis of */opt* folder only would be enough.

Analysis of important files can be summarized as follows:

- *.account.db* - is a SQLite database that contains data about connected Samsung account and the identifying e-mail address.
- *.CompanionInfo.db* - shows data, such as device model and operating system, about paired device.
- *.contacts-svc.db* - contains following data: contact list, phone numbers and call history in tables *contacts,phone_lookup, phonelogs* respectively. Contact images, if exist, can be found in */home/owner/apps_rw/com.samsung.w_contacts2/data/*
- *.context-app-history* - contains data about the applications' usage. Relevant tables include *Log_AppLaunch* and *Log_BatteryUsagePerApp*. First table contains data about the time when application was first started and application ID. Second table contains application ID, time of starting and time of stopping the application.
- *.context-sensor-recorder.db* - shows measurements form sensors: Pedometer and Pressure. Table *SensorPedometerRecord* containts data about number of steps (walking/running), traversed distance and spent calories. Timestamp and air pressure measurements can be found in *SensorPressureRecord* table.
- *.wnoti-service.db* - contains data about previous and current notifications in tables *asset* and *data* respectively. Only time and date, and path to notification icon are shown for previous notifications, while unremoved notifications show application, sender, path to the notification icon and content of notification. Icons, if exist, can be found in */opt/usr/data/wnoti/*. It is noted, that notification icons are in wrong file format, instead of having a .png extension they have a .jpg extension. Further analysis of icons, showed that shape of the icon corresponds to different application. Square shaped notifications are connected to Facebook and Telegram, circle shaped to WhatsApp and Instagram, and squircle shaped to Viber.
- *.shealth.db* - is an encrypted database and all its data is available through direct device usage.
- *.SuveyLog.db* - shows all of the information about application usage and usage of aplications' features, and device state in tables *use_app_survey, use_app_feature_survey* and *report_app_status_survey* respectively.
- *GPS and LBS logs* - do not show any significant information about the location, however they indicate that LBS and GPS are active and communicate with applications that require the data.
- *Database of a third-party software* - MapMyRun

TABLE II
IMPORTANT FILES

Path	File	Data
/opt/dbspace/5001/	.account.db	Connected account data
/opt/usr/dbspace/	.CompanionInfo.db	Database for paired device
/home/owner/.applications/dbspace/privacy/ /opt/usr/home/owner/.applications/dbspace/privacy/	.contacts-svc.db	Databases for contacts, phone calls etc.
/home/owner/.applications/dbspace/ /opt/usr/home/owner/.applications/dbspace/	.context-app-history.db	Application use data
/opt/dbspace/	.context-sensor-recorder.db	Sensor data (pedometer, pressure)
/opt/usr/dbspace/	.wnoti-service.db	Notification and icon paths database
/opt/usr/apps/com.samsung.shealth_gear/data/ /home/owner/apps_rw/com.samsung.shealth_gear/data/	.shealth.db	Samsung Health database - encrypted
/opt/usr/data/samsung-log-service/	.SurveyLog.db	Database for state changes
/opt/usr/data/wnoti/	/	Notification icons for applications and contacts
/opt/usr/apps/com.samsung.w-contacts2/data/ /home/owner/apps_rw/com.samsung.w_contacts2/data/	/	Contact photos
/opt/usr/data/location/	dump_gps.log dump_lbs_consumer.log	GPS and LBS logs
/opt/usr/home/owner/apps_rw/2x0Qp1z5oN/data /home/owner/apps_rw/2x0Qp1z5oN/data/	UAdatabase.db	Third-party software database

database, *.UAdatabase*, is not encrypted and showed data about user recorded workouts (sensor measurments, aggregated data). Notable tables include *Aggregates* and *Measurement*.

V. RESULTS

An analysis is highly dependent on gathering data in due time. The watch has limited memory, and it overwrites previous data with its daily use. Putting it in Flight mode and not using it, or rather turning it off, should be the first step upon watch acquirement for forensic analysis. In that way, it is possible to guarantee no outside data tampering.

After the analysis of the aforementioned files, a timeline of events was created. The timeline is given in table III. In the table, we see the time of the event and the event. Continuous user activity is merged into one row. As can be seen from the table, it was possible to reconstruct all the events in the scenario. More details were obtained than initially noted in the scenario. In order to confirm some of the cases, data from multiple databases were used.

Data about user actions, such as wrist movement, watch rotation and swipe on the watch were recorded. From this data, information about the exact time of watch usage can be determined. Different watch states, connected or not, are also recorded.

Table *use_app_feature* of .SurveyLog.db was used to determine which application created the notification. To determine the image of the sender, path from *asset* table of .wnoti-service.db was used. Notifications that were removed from the watch display, do not contain saved content, while those that are still on the watch do. Notification content, along with the name of the sender, can be found in *data* table of .wnoti-service.db.

Heart rate data are not available through Samsung Health application, despite the logs, that contain the time when it was measured. Database of MapMyRun application, reveals heart rate data, during active workout state. Using the SurveyLog.db, it is possible to discover notifications from Samsung Health application, concerning some form of activity or movement.

GPS and LBS logs do not contain usable information about the exact locations of the watch. Using data about air pressure measurements, with information about temperature and air pressure on sea level, the altitude of the watch can be determined. In the beginning, a slow rise of air pressure and the number of steps indicate that the user climbed down from a certain height of $610m$ to $510m$. During the last minutes, air pressure dropped suddenly, the number of steps was smaller, so a conclusion was drawn, that the user used some form of transportation.

During the analysis, all scenario points were proven. Generally speaking, acquired watch data contained information on watch usage. It was possible to determine when the user moved their wrist up or down, how he rotated the watch gear and which applications he used. Notifications that were still available on the watch itself could be found along with the time and date of the notification. If acquired in due time, records of previous notifications, in terms of timestamp, application, icon, though not available through the watch interface, were still available. Full phone logs were available, as they were regularly synced with the connected phone. Measurements from the pedometer and air pressure sensors were available for analysis. Using that data we could determine the walking distances, that the user traveled. The exact locations of the watch could not be determined, even though the LBS and GPS logs were available. Usage of third-party software that requires maps, if not encrypted, might provide such information. Using Samsung Health alerts that appeared on the watch, we could determine a type of activity user engaged in. Even though heart rate records or exact workouts were not available from the encrypted Samsung Health database, third-party applications' databases might not be encrypted, and they might store that data. Direct manipulation of the watch shows Samsung Health data. Data about the connected phone, user account were available, as well as all saved images, music and user files on the watch. Status of applications and the short-term history of watch states were available to examine. In conclusion, forensic analysis of a smartwatch can provide crucial evidence for investigations.

TABLE III
TIMELINE

Time	Event
19:12	Bluetooth and WiFi connection
19:13	Activity started on MapMyRun application
19:13-22:13	Air pressure rises from 941 to 952.
19:13-19:42	1663 steps 1402.24 m Min HR: 92 bpm Max HR: 164 bpm Avg HR: 122 bpm
19:26	Facebook notification
19:26	Call Duration: 19 s
19:27	Google notification
19:32	Facebook notification
19:55-20:10	47 steps 31.58 m Min HR: 70 bpm Max HR: 106 bpm Avg HR: 83 bpm
19:56	Facebook notification
19:57	Facebook notification
19:58	Facebook notification
19:59	Telegram notification
20:30	Facebook notification
20:30	Silent mode on
20:35	Activity paused on MapMyRun application
20:35-22:18	4913 steps 3199 m
20:39	Weather notification
21:09	Some sort of exercise
21:22	Whatsapp notification
21:50	SMS notification
21:50	Facebook notification
21:50	Facebook notification
20:13-22:17	Air pressure drop from 952 to 942.
22:10	Movement: 10∼20 m
22:17	Flight mode

VI. Conclusion and future development

In this paper, manual IoT forensics of a Samsung Gear S3 Frontier smartwatch was performed. Issues concerning the IoT forensics were explained. Available data and reconstructed sequence of events were presented, using manual IoT forensics of a smartwatch.

Detailed examination of data acquisition shows the issues of data collection through SDB in a non-rooted watch. Analysis of available data can be used to prove certain user actions and behavior. If the watch was synced with a phone, additional pieces of information are available to the investigator, concerning the user, calls and social networks. Data acquired through smartwatch analysis was proven to be valuable in forensic investigations.

Further examination of smartwatches, concerning rooted or locked watch is required. Besides that, analysis of malicious software and its effects and traces on watch requires further development.

Generated watch data, in cases of careless data storing with high chances of security breaches, can be used by a malicious third party and sold to unscrupulous organizations. Data about user behavior, if breached, can affect health insurance policies and costs. Due to the availability of data during a forensic examination, the question of extracting necessary data without jeopardizing complete user privacy is still open. There is a need for defining privacy levels for IoT forensics.

Due to the rise of smartwatches available to users and different types of applications available for free download or purchase, it is crucial for an investigator to have a clear vision of where to look for viable information.

References

[1] S. Zawoad, and R. Zagib, “Faiot: Towards building a forensics aware eco system for the internet of things,” in 2015 IEEE International Conference on Services Computing, pp. 279-284, June 2015.

[2] I. Yaqoob, I. A. T. Hasheem, A. Ahmed, S. A. Kazmi and C.S. Hong, “Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges,” in Future Generation Computer Systems, vol. 92, pp. 265-275, 2019.

[3] E. Oriwoh, D. Jazani, G. Epiphaniou and P. Sant, “Internet of things forensics: Challenges and approaches,” in 9th IEEE International Conference on Collaborative computing: networking, Applications and Worksharing, pp. 608-615, October 2013.

[4] E. Oriwoh and P. Sant, “The forensics edge management system: A concept and design,” in 2013 IEEE 10th International Conference on Ubiquitous Intelligence and Computing and 2013 IEEE 10th International Conference on Autonomic and Trusted Computing, pp. 544-550, December 2013.

[5] N. H. N. Zulkipli, A. Alenezi and G. B. Wills, “ IoT Forensic: Bridging the Challenges in Digital Forensic and the Internet of Things,” in International Conference on Internet of Things, Big Data and Security, vol. 2, pp. 315-324, April 2017.

[6] S. Alabdulsalam, K. Schaefer, T. Kechadi and N. A. Le-Khac, “Internet of Things ForensicsChallenges and a Case Study,” in IFIP International Conference on Digital Forensics, pp. 35-48, January 2018.

[7] Q. Do, B. Martini and K. K. R. Choo, “Cyber-physical systems information gathering: A smart home case study,” in Computer Networks, vol. 138, pp. 1-12, 2018.

[8] H. Chung, J. Park and S. Lee, “Digital forensic approaches for Amazon Alexa ecosystem,” in Digital Investigation, vol. 22, pp. S15-S25, 2017.

[9] K. S. Rahman, M. Bishop and A. Holt, “Internet of Things mobility forensics,”, in de Proceedings of the 2016 Information Security Research and Education (INSuRE), 2016.

[10] M. M. Hossain, R. Hasan and S. Zawoad, “Trust-IoV: A Trustworthy Forensic Investigation Framework for the Internet of Vehicles (IoV),” in ICIOT, pp. 25-32, June 2017.

[11] H. Mansor, K. Markantonakis, R. N. Akram, K. Mayes and I. Gurulian, “Log your car: The non-invasive vehicle forensics,” in 2016 IEEE Trustcom/BigDataSE/ISPA, pp. 974-982, August 2016.

[12] N. Al Mutawa,I. Baggili and A. Marrington, “Forensic analysis of social networking applications on mobile devices,” in Digital Investigation, vol. 9, pp. S24-S33, 2012.

[13] I. Baggili, J. Oduro, K. Anthony, F. Breitinger and G. McGee, “Watch what you wear: preliminary forensic analysis of smart watches”, in 2015 10th International Conference on Availability, Reliability and Security, pp. 303-311, August 2015.