Effects of Timestamp Manipulation in a Car Audio Video Navigation System Connected to a Smartphone via Bluetooth: A Preliminary Study

Min-hyuk Cho, Sun-jae Kim, Seong-je Cho

Computer Security & OS Lab, Dankook University

ICNGC 2024

2024.11.21

INDEX

01 Introduction & Background

02 Process of Detecting Timestamp Manipulation

03 Experimentation and Evaluation

04 Related Work

05 Conclusion & Future Work

01 Introduction & Background

Introduction

✓ Digital Forensics?

- "**Applying scientific methods** to identify, collect, examine, and analyze data while maintaining a rigorous security system to **ensure the integrity of information.**" – NIST SP 800-86

✓ Anti Forensics?

- "Techniques designed to **conceal** or **destroy data** to prevent access." – NIST SP 800-86

✓ Timestamp?

- "Information indicating when (hour, minute, second) a log was created."
- "**A fundamental and critical piece of information** in digital forensic analysis."

→ "Criminals can manipulate timestamps to hinder forensic investigations."

Introduction

✓ Objectives

- **To conduct experiments on time manipulation** in a Bluetooth-connected environment between a vehicle and a smartphone.
- To observe discrepancies in timestamp records in log data **when time manipulation occurs on vehicle.**
- To propose a method for detecting time manipulation through the **analysis of Bluetooth and system logs.**

✓ Motivation & Contributions

- **No research** has been conducted on how discrepancies in time information between two devices impact Bluetooth and system logs in a **Bluetooth-connected environment.**
- **No research** has yet addressed which time zone should be used for analysis when time information differs between devices in forensic investigations.

Background

✓ System Logs

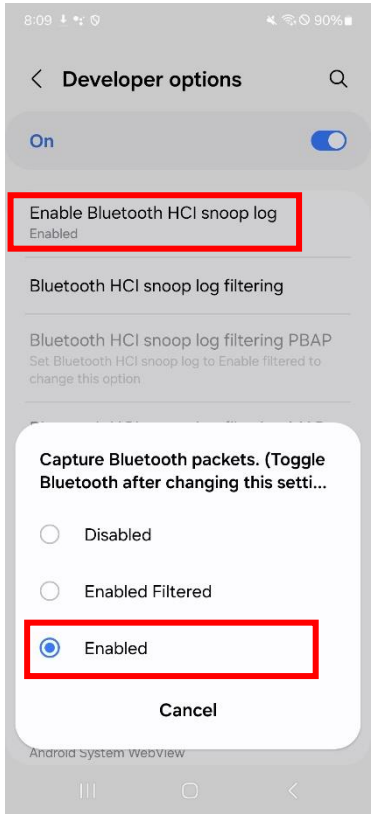
- Files that record the events of OS and applications.

✓ Bluetooth Logs

- Files that record various events and state changes related to Bluetooth communication.
- Access to these logs is restricted without 'root' privileges.

✓ Bluetooth HCI Snoop Log

- Overcomes the inability to access Bluetooth logs on non-rooted devices by using this feature.
- Enables analysis of Bluetooth connection status and data transfer status.
- However, this feature must be enabled through Developer Options.



02 Process of Detecting Timestamp Manipulation

Process of Detecting Timestamp Manipulation

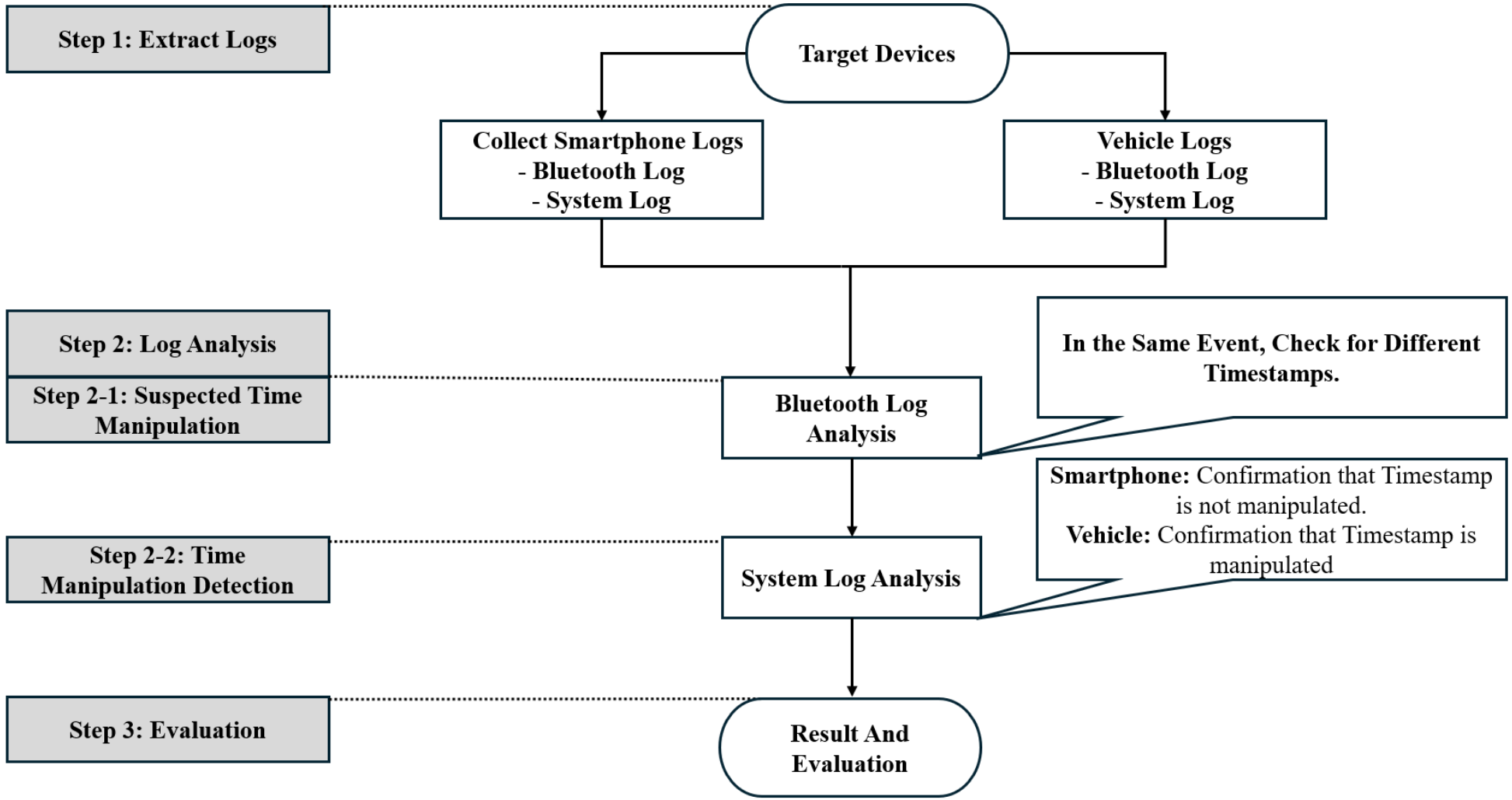


Fig 1. Process of Detecting Timestamp Manipulation on an AVN system

Process of Detecting Timestamp Manipulation: Data Collection Step

STEP 1) Log extraction (Logical Extraction)

✓ **Mobile phone**(Samsung Galaxy S21)

➢ **adb bugreport**

```
PS C:\Users\cgumg> adb bugreport s21_bugreport.zip
/data/user_de/0/com.android.shell/files/bugreports/dumpsta...le pulled, 0 skipped. 37.3 MB/s (21102152 bytes in 0.539s)
Bug report copied to s21_bugreport.zip
```

✓ **AVN** (Hyundai Avante AVN by Mobis)

➢ **Engineering mode**
- Hidden feature that provides a menu for logically extracting logs

➢ "**Copy image to USB**" menu

Process of Detecting Timestamp Manipulation: Data Analysis Step

STEP 2) Log Analysis

STEP 2-1) The first sub-step where time manipulation is suspected

- First, analyze the Bluetooth log, as communication has occurred through the Bluetooth connection.
- During this process, if logs for the same event have different timestamps, **suspect time manipulation.**

STEP 2-2) The second sub-step for detecting time manipulation

- Next, analyze the system log for a more detailed investigation.
- **Detect time manipulation** by identifying time manipulation log messages on the manipulated device and confirming the absence of such messages on the unmanipulated device.

Process of Detecting Timestamp Manipulation: Evaluation Step

STEP 3) Evaluation & Verification

- Finally, perform an evaluation based on the log analysis results.
- Identify the time zone to use as a reference in Forensics investigations.

03 Experimentation and Evaluation

Experimental Environment

✓ Experimental Devices

TABLE 2. SPECIFICATION OF TARGET AVN SYSTEM AND ANDROID PHONE

Car AVN	
Vehicle Model	Hyundai Avante
AVN Manufacturer	Hyundai Mobis
Operating System	Android 4.4.2(KitKat)
Kernel Version	Linux 3.18.24-tcc
Smartphone	
Mobile Device Model	Galaxy S21
Manufacturer	Samsung
Operating System	Android 14
Kernel Version	Linux 5.4.242-27760517-abG991NKSU4FWK7

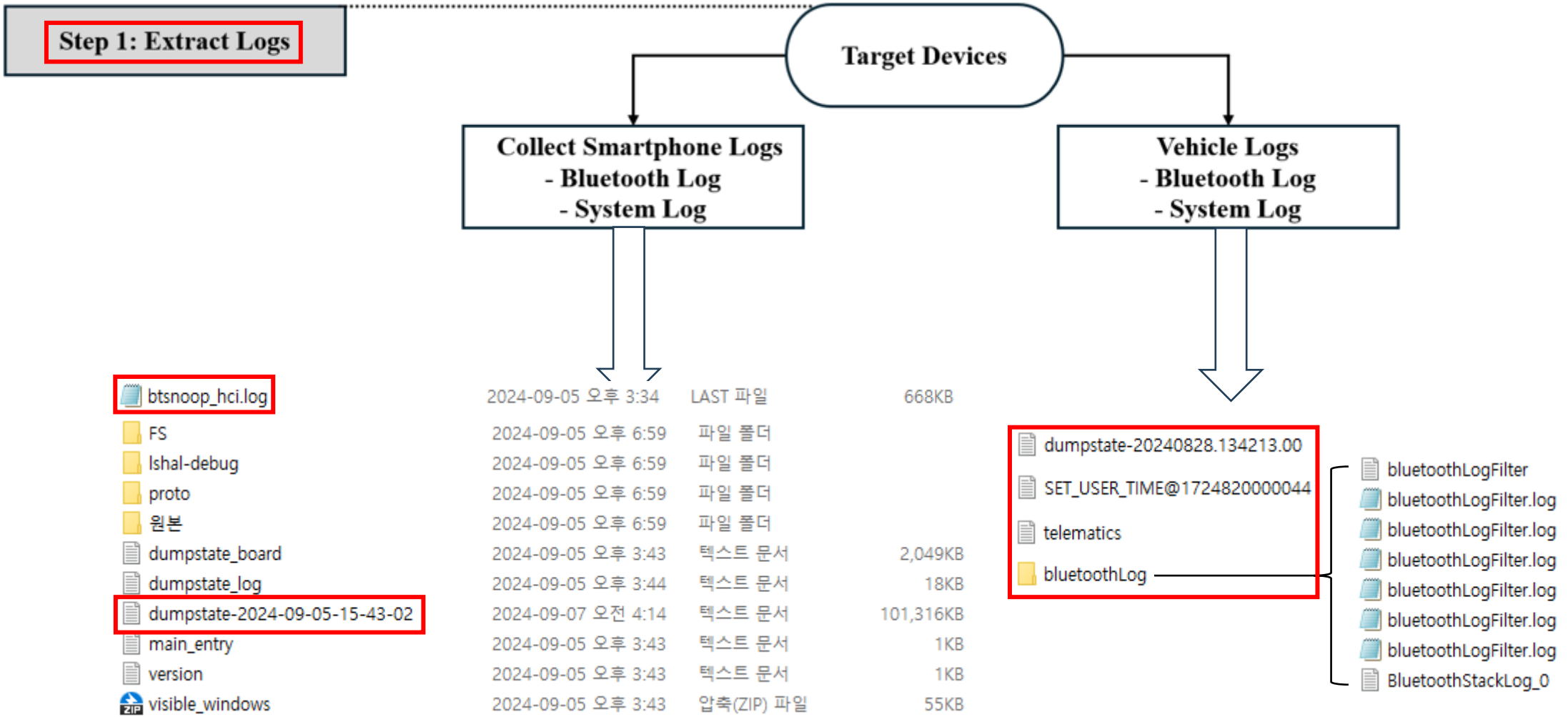
Experimental Method – Event Sequences based on a Scenario

TABLE 3. EVENT SCENARIO

Time	Event	Description
15:23	Bluetooth Connect	Enabling “Bluetooth HCI Snoop Log” on Android smartphone
15:24	Network Time Off	Turn off only vehicle’s network time
15:41	Manipulate Vehicle Time	2024/09/05, 15:41 -> 2024/08/25, 13:40
15:41	Calling Event	Calling to ‘01049232198’
15:43	Music Event	Title: A Collection of 2000s hit
15:44	Log Dump	Smartphone: adb bugreport Vehicle: Copy Image to USB

- ✓ Perform only Car AVN’s time manipulation after Bluetooth connection
- ✓ Execute predefined events in a Bluetooth-connected environment and then extract the logs.

Data Extraction STEP: Log Extraction



Data Analysis STEP (1/2): Discovering Signs of Time Manipulation

Smartphone		
Timestamp	*Event Type*	*Log Message*
2024-09-05 15:41:59	Calling	Sent +CLCC: 1,1,0,0,0,"01049232198",129
2024-09-05 15:42:14	Music	Sent Vendor dependent: Stable – GetElementAttributes – Title: "A Collection of 2000s hit"

Vehicle's AVN		
Timestamp	*Event Type*	*Log Message*
08-28 13:41:06	Music	MobisAvrcpControllerService [BTAD] title: A Collection of 2000s hit, artist:, album:, playingTime:12345000

"Bluetooth log analysis results indicate that time manipulation can be suspected when different timestamps appear for the same event."

Data Analysis STEP (2/2): Detecting Time Manipulation

Step 2-2: Time Manipulation Detection

System Log Analysis

Smartphone: Confirmation that Timestamp is not manipulated.
Vehicle: Confirmation that Timestamp is manipulated

Smartphone		
File Name	***Timestamp***	***Log Message***
dumpstate-2024-09-05-15-43-02.txt	09-05 15:40:19	automatic time enabled

Vehicle's AVN		
File Name	***Timestamp***	***Log Message***
telematics.txt	08-28 13:40:00	Action : android.intent.action.TIME_SET
SET_USER_TIME@ 1724820000044	-	millis: 1724820000000 offset: [new] - 698480811 [isUsetTimeSet] true

We can confirm that no time manipulation occurred on the smartphone through the message indicating that the automatic time setting was enabled in the system log analysis.

However, the system log analysis of the vehicle shows that the timestamp was manipulated, as the TIME_SET and isUsetTimeSet were set to true at the time the timestamp was altered.

Experimental Results and Evaluation

- Finally, Verifying that the smartphone's time remains unmanipulated enables us to identify **the appropriate time zone** to use as a reference in **forensic investigations.**

- Additionally, by analyzing the **SET_USER_TIME** entry in the vehicle's system log, where **millis: 1724820000000** and **offset: [new] -698480811**, we can adjust the time using these values, resulting in a current time that matches the smartphone's timestamp. This allows us to determine the **accurate current time.**

04 Related Work

Related Work

- ✓ **[8] Oh et al.** identified limitations in journal-based methods for detecting timestamp manipulation in NTFS and proposed a new algorithm that demonstrated improved performance. – NTFS

- ✓ **[9] Kaart et al.** addressed time manipulation in Android forensics, emphasizing validation with reference devices. They proposed a simple detection method and examined the impact of time synchronization settings. – Android

- ✓ **[10] Pieterse et al.** developed the Authenticity Framework for Android Timestamps (AFAT) to detect timestamp manipulation, focusing on file system changes and database inconsistencies. This framework is crucial for maintaining evidence integrity and countering anti-forensic techniques in digital investigations. - Android

05 Conclusion & Future work

Conclusion & Future Work

- **Conclusion**
  - A new method for detecting time manipulation where an AVN was connected to a smartphone.
  - Suspected time manipulation through Bluetooth logs.
  - Detected time manipulation through system logs and identify the time zone to use as a reference in investigations.
    - This time manipulation detection process is expected to enable more efficient investigations

- **Future Work**
  - To develop a method to extract Bluetooth logs even when the Bluetooth HCI Snoop Log feature is disabled
  - To generalize the method by conducting additional verification across various scenarios and devices

References

1. André Årnes, “Digital Forensics: An Academic Introduction.” John Wiley & Sons Inc, Hoboken, NJ, 2018.
2. Gyu-Sang Cho, “Digital Forensic Analysis of Times tamp Change Tools: An Anti-Forensics Perspective.” Korean Society of Computer Information Conference, 07 a, Pages.391-392, 2019.
3. D. -i. Jang, G. -J. Ahn, H. Hwang, and K. Kim, "Understanding Anti-forensic Techniques with Timestamp Manipulation (Invited Paper)," 2016 IEEE 17th International Conference on Information Reuse and Integration (IRI), Pittsburgh, PA, USA, pp. 609-614, 2016.
4. Jewan Bang, Byeongyeong Yoo, and Sangjin Lee, "Analysis of changes in file time attributes with file manipulation", Digital Investigation, Volume 7, Issues 3–4, Pages 135-144, 2011.
5. Automotive Electronics Magazine, “Smart car's infotainment service and smartphone connection technology,” https://www.autoelectronics.co.kr/article/articleView.asp?idx=933.
6. R. Nusser and R. M. Pelz, "Bluetooth-based wireless connectivity in an automotive environment," Vehicular Technology Conference Fall 2000. IEEE VTS Fall VT C2000. 52nd Vehicular Technology Conference (Cat. N o. 00CH37152), Vol. 4, pp.1935-1942, 2000.
7. H.I Kang, M.S Park, S.J Cho, and J.H Jung, “Using Logs of an Android-based Audio Video Navigation System for a Timeline Analysis in Vehicle Digital Forensics.” Papers of the Korea Information Society 2023 Comprehensive Computer Science Conference, 1,259-1,261. 2023.
8. J. Oh, S. Lee, and H. Hwang, "Forensic Detection of Timestamp Manipulation for Digital Forensic Investigation," in IEEE Access, vol. 12, pp. 72544-72565, 2024.
9. M. Kaart and S. Laraghy, “Android forensics: Interpretation of timestamps,” in Digital Investigation, Volume 11, Issue 3, Pages 234-247, 2014.
10. H. Pieterse, M. S. Olivier, and R. P. van Heerden, "Playing hide-and-seek: Detecting the manipulation of Android Timestamps," *2015 Information Security for South Africa (ISSA)*, Johannesburg, South Africa, pp. 1-8, 2015.
11. https://source.android.com/docs/core/tests/debug/read-bug-reports?hl=ko#event-log.
12. Aya Fukami, Saugata Ghose, Yixin Luo, Yu Cai, and Onur Mutlu, “Improving the reliability of chip-off forensic analysis of NAND flash memory devices, Digital Investigation,” Volume 20, Supplement, Pages S1-S11, 2017.
13. V. Ndatinya, “Network forensics analysis using Wireshark”, International Journal of Security and Networks(USN), Vol.10, No. 2, 2015.

Acknowledgement

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science and ICT (no. 2021R1A2C2012574), and by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by Korea government (MSIT) (No.1711170476, Development of Collection and Integrated Analysis Methods of Automotive Inter/Intra System Artifacts through Construction of Event-based experimental system).

Thanks !

Q&A

Min-Hyuk-Cho
cgumgek8@dankook.ac.kr