

블루투스로 연결된 스마트폰과 자동차 인포테인먼트 시스템에서의 시간 조작 탐지

조민혁, 이산, 정지현, 김선재, 조성제

WDSC 2024

2024.08.20

INDEX

01

서론 & 배경지식

02

시간 조작 탐지 기법

03

실험 환경 및 실험 방법

04

로그 수집 및 로그 분석

05

결론 및 향후 연구

01

서론 & 배경 지식

서론

❖ 디지털 포렌식

- ✓ “정보의 무결성을 보존하고 데이터에 대한 엄격한 보관 체계를 유지하면서 데이터를 식별, 수집, 검사 및 분석하는 데 과학적 방법을 적용 하는 것” – NIST SP 800-86



❖ 안티 포렌식

- ✓ “데이터를 은폐 또는 파괴하여 접근하지 못하도록 하는 기술” – NIST SP 800-86



❖ 타임 스탬프

- ✓ “디지털 포렌식 분석에 있어서 가장 기본적이면서 중요한 정보”
- ✓ “범죄자는 타임스탬프를 조작하여 포렌식 수사를 어렵게 할 수 있다”



❖ 본 논문의 필요성

- ✓ 블루투스 연결 환경에서 양 기기의 시간 정보 다를 때 블루투스 및 시스템 로그에 어떤 영향을 미치는 지에 대한 연구가 수행된 적이 없다
- ✓ 포렌식 수사에서 시간 정보가 다른 상황에서 어떤 시간대로 결정하여 수사를 진행해야 하는지에 대한 연구가 수행된 적이 없다

❖ 본 논문의 목표

- ✓ 차량과 스마트폰 간 블루투스 연결 환경에서의 시간 조작 진행
- ✓ 각 기기에서 시간 조작 됐을 시 로그 데이터의 타임스탬프가 상이하게 기록되어 발생
- ✓ 블루투스 로그 분석 및 시스템 로그 분석을 통한 시간 조작 탐지 기법 제시

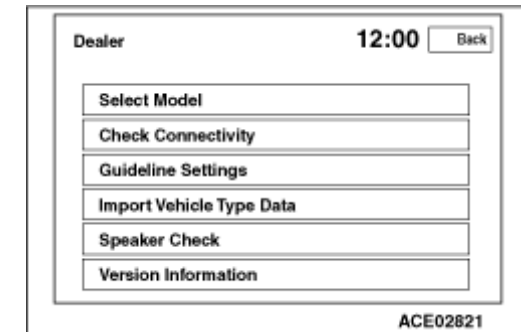
배경 지식

❖ 딜러 모드

- ✓ 차량 AVN 시스템의 시크릿 기능 -> 특정 방법을 통해 접근 가능
- ✓ 해당 모드에 접근하여 히든 메뉴를 통한 SW 업데이트, 차량 시스템 진단 정보, 로그 수집 가능

❖ 블루투스 로그

- ✓ 블루투스 통신과 관련된 다양한 이벤트와 상태 변화를 기록한 파일
- ✓ 'root' 권한 존재하지 않을 시 해당 로그에 접근 불가



배경 지식

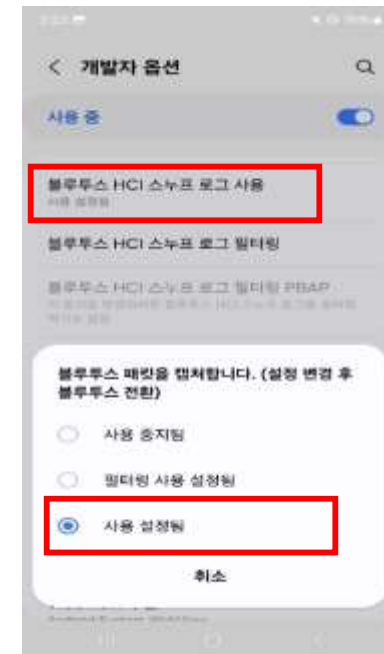
❖ 시스템 로그

- ✓ OS와 APP의 동작을 기록한 파일
- ✓ 기기의 전반적인 활동 기록



❖ 블루투스 HCI 스냅 로그

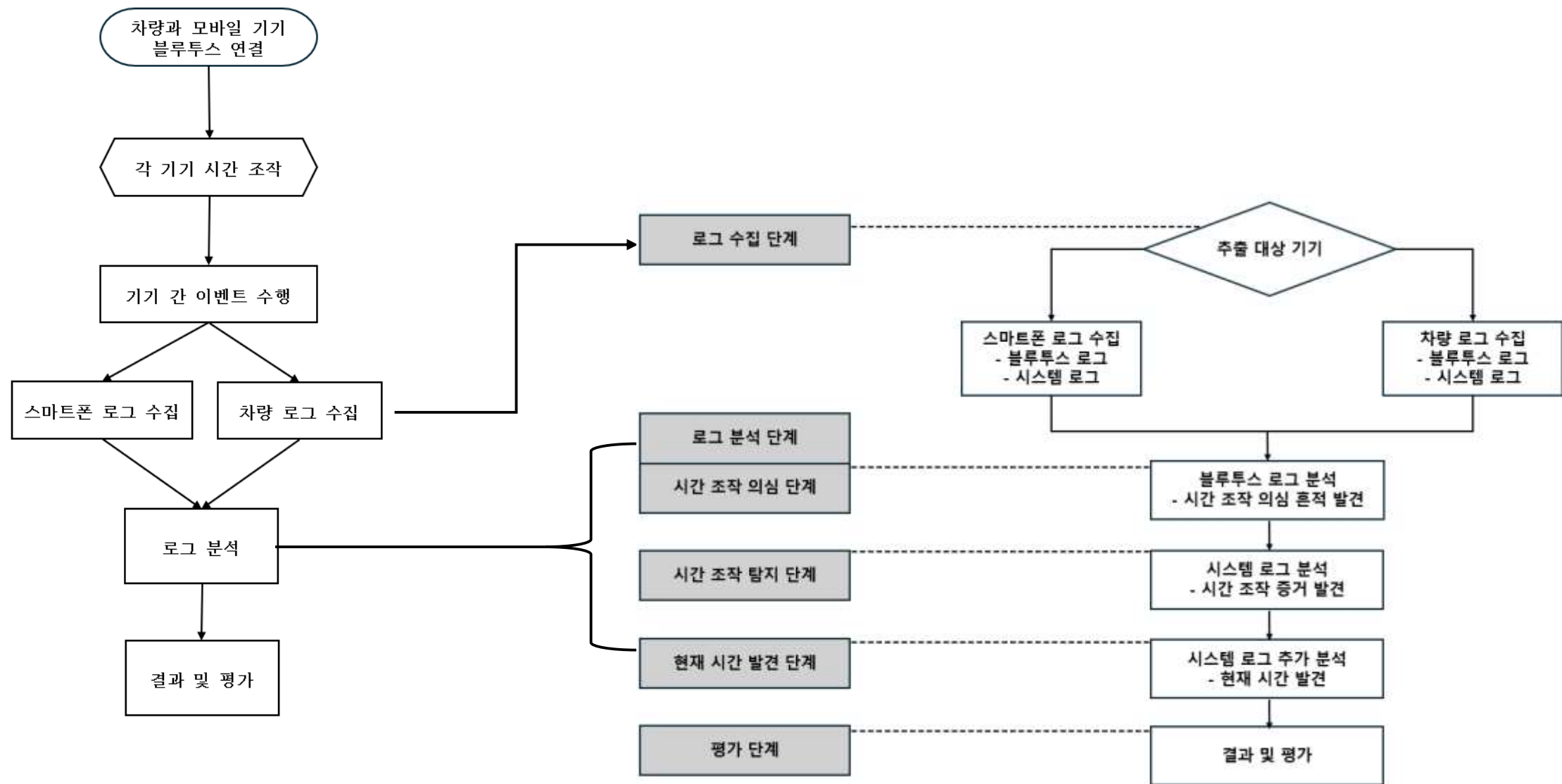
- ✓ 루팅되지 않은 기기는 블루투스 로그에 접근할 수 없기에 해당 기능으로 극복
- ✓ 블루투스 연결 상태 및 데이터 전송 상태 분석 가능
- ✓ 단, 해당 기능 사용하기 위해서는 개발자 옵션을 통한 활성화 필요



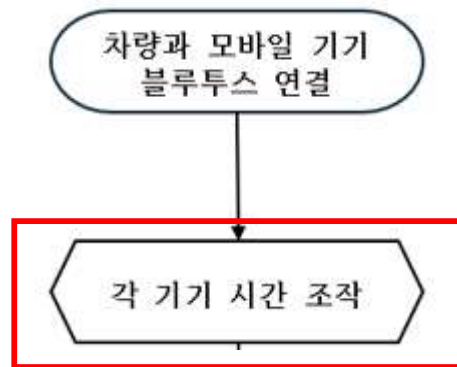
02

시간 조작 탐지 기법

시간 조작 탐지 기법



시간 조작 탐지 기법 – 시간 조작 경우의 수



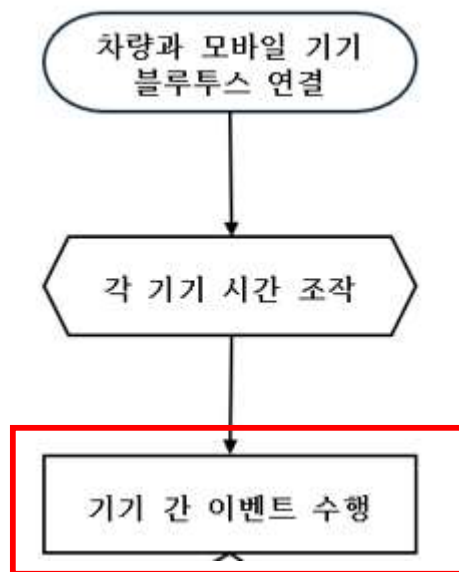
[표 1]. 시간 조작 경우의 수

기기	차량 AVN	모바일 기기
시간 조작	과거	과거
		현재
		미래
	현재	과거
		현재
		미래
	미래	과거
		현재
		미래

- 각 기기의 시간 조작의 경우의 수 – 총 9가지 존재

- 본 논문에서는 과거-과거의 CASE로 실험 진행

시간 조작 탐지 기법 - 블루투스 연결 환경 이벤트 목록



[표 2]. 블루투스 연결 환경 이벤트 목록

수행 가능한 이벤트 종류
통화 이벤트
음악 이벤트
내비게이션 이벤트
메시지 이벤트

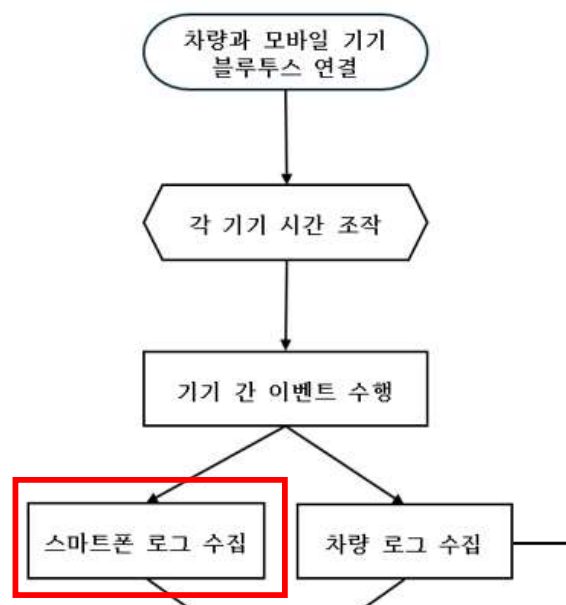
- 본 논문에서는 통화, 음악 이벤트 수행

시간 조작 탐지 기법 - 스마트폰 로그 수집



- Android 스마트폰은 **ADB**를 통하여 로그 수집 가능
- '설정->일반->개발자 옵션->USB 디버깅' 활성화 필요

시간 조작 탐지 기법 - 스마트폰 로그 수집



[표 3]. ADB 로그 추출 명령어

명령어
logcat
bugreport

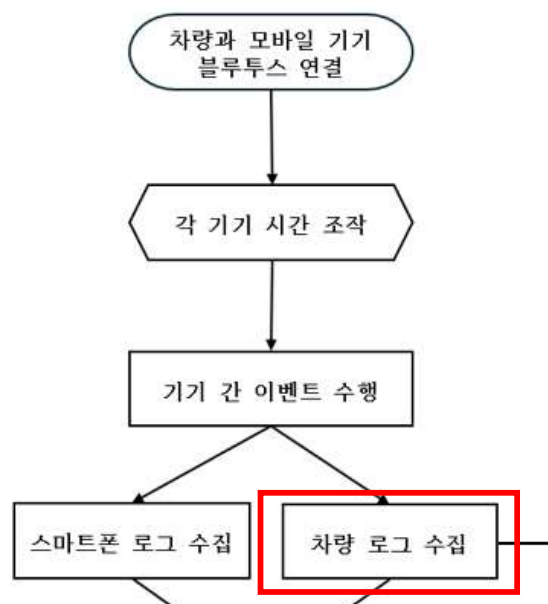
- logcat : 부팅 시점 이후로 로그 추출 가능 (휘발성 로그)

➔ 즉, 기기의 전원이 꺼진다면 로그가 모두 사라짐

- Bugreport : logcat의 로그 데이터를 포함 한 상위 로그 데이터 추출 가능 (비휘발성 로그 + 휘발성 로그)

* 본 논문에서는 bugreport 명령어를 통하여 로그 수집을 함

시간 조작 탐지 기법 - 차량 로그 수집



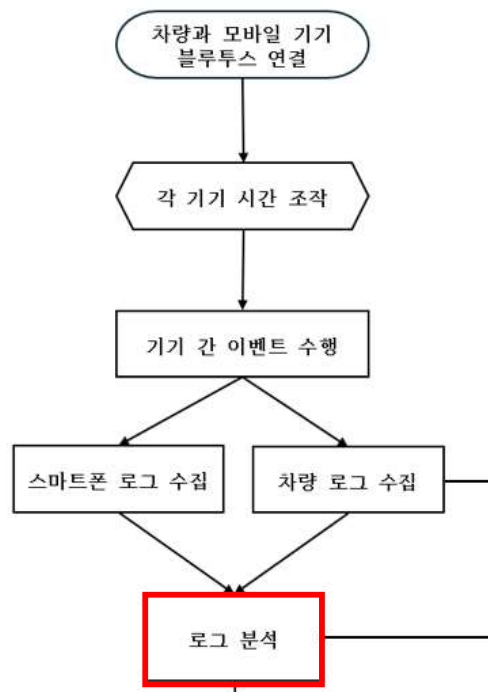
[표 4]. 차량 로그 추출 방법

로그 추출 방법
Chip-off
Copy image to USB

- Chip-off : 메모리칩을 물리적으로 제거하여 로그 데이터 추출
→ 즉, 메모리칩 손상 가능성 존재
- Copy image to USB : 차량 AVN의 딜러 모드에 접근하여 로그 데이터 추출

* 본 논문에서는 'Copy image to USB' 방식으로 로그 추출

시간 조작 탐지 기법 - 로그 분석



[표 5]. 시간 관련 키워드

시간 관련 키워드	
TimeChange	DateSet
TimeSet	UsetTime
DateChange	UsetDate

❖ 로그 데이터 분석 방식

- ‘수정된 날짜’ 태그를 확인하여 해당 조작 날짜 타임스탬프로 생성된 로그 파일 위주로 분석
- 블루투스로 통신하였기에 ‘블루투스 로그’도 분석
- 시간 관련 키워드를 통하여 분석
- 시간 관련 키워드의 로그 메시지가 존재하지 않는다면 조작된 타임스탬프 전후로 로그 데이터 분석

03

실험 환경 및 실험 방법

[표 6]. 대상 AVN 시스템 및 모바일 기기

AVN	
차종	Hyundai Avante
AVN 제조사	Hyundai Mobis
운영체제	Android 4.4.2 (Kitkat)
커널 버전	Linux 3.18.24-tec
모바일 기기	
기기명	Galaxy S21
제조사	Samsung
운영체제	Android 14
커널 버전	Linux 5.4.242-27760517-abG991NKSU4FWK7



❖ 실험 대상 기기

- 차량 : Hyundai Avante, Android 4.4.2
- 스마트폰 : Samsung Galaxy S21, Android 14

실험 방법 - 이벤트 시나리오

[표 7]. 주요 이벤트 시나리오

시간	시나리오
17:13	대상 시스템 블루투스 연결
17:33	차량 시간 조작
17:33	스마트폰 시간 조작
17:34	전화 발신
17:34	전화 수신
17:34	음악 재생
17:35	차량 로그 덤프
17:59	스마트폰 로그 추출

[표 8]. 날짜 및 시간 조작 시나리오

	Hyundai Avante	Samsung Galaxy S21
현재 시간	2024.07.19.17:33	2024.07.19.17:33
변경 시간	2024.07.11.14:00	2024.07.13.12:00

- ✓ 블루투스 연결 후 시간 조작 수행
- ✓ 블루투스 연결 환경에서 사전에 정의한 이벤트 수행 후 로그 추출

실험 방법 - 스마트폰 시간 조작



✓ 스마트폰 시간 조작

=> '설정->날짜 및 시간->날짜 및 시간 자동 설정' 비활성화를 통해 가능

실험 방법 - 차량 시간 조작



- ✓ 차량 시간 조작
=> '설정->날짜/시간->시간 자동설정' 비활성화를 통해 가능

04

로그 수집 및 로그 분석

로그 수집 - 스마트폰

```
PS C:\Users\cgung> adb bugreport s21_bugreport.zip  
/data/user_de/0/com.android.shell/files/bugreports/dumpsta...le pulled, 0 skipped. 37.3 MB/s (21182152 bytes in 0.539s)  
Bug report copied to s21_bugreport.zip
```

❖ ADB 환경에서 bugreport 명령어로 로그 추출

✓ 추출 시 다음과 같은 로그 파일 추출 가능

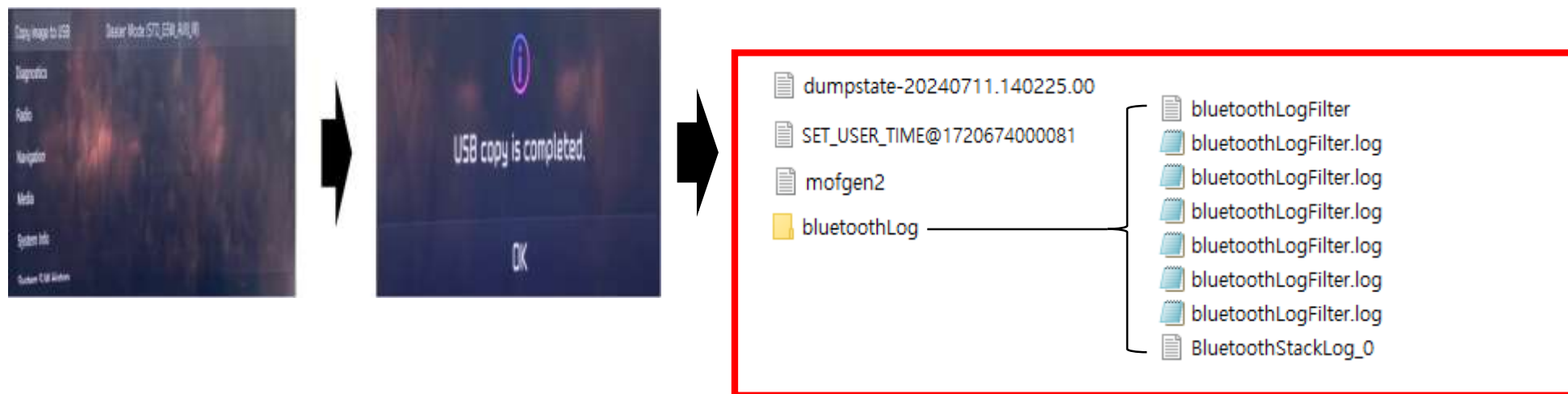
✓ 이 중 분석 대상 파일 정리

* 블루투스 로그의 경우 'FS\data\log\bt' 경로에 존재

FS	2024-07-16 오후 2:23	파일 폴더	
lshal-debug	2024-07-16 오후 2:23	파일 폴더	
proto	2024-07-16 오후 2:23	파일 폴더	
dumpstate_board	2024-07-23 오전 11:30	텍스트 문서	2,049KB
dumpstate_log	2024-07-23 오전 11:30	텍스트 문서	18KB
dumpstate-2024-07-23-11-29-42	2024-07-23 오전 11:30	텍스트 문서	110,295KB
main_entry	2024-07-23 오전 11:29	텍스트 문서	1KB
version	2024-07-23 오전 11:29	텍스트 문서	1KB
visible_windows	2024-07-23 오전 11:30	압축(ZIP) 파일	40KB

FS	bcm_bt_exp	2024-07-13 오후 12:01	텍스트 문서	2KB
dumpstate-2024-07-19-17-59-48	bcm_bt_exp.log	2024-07-19 오후 5:11	LAST 파일	1KB
	btsnoop_hci	2024-07-19 오후 6:00	텍스트 문서	2,239KB

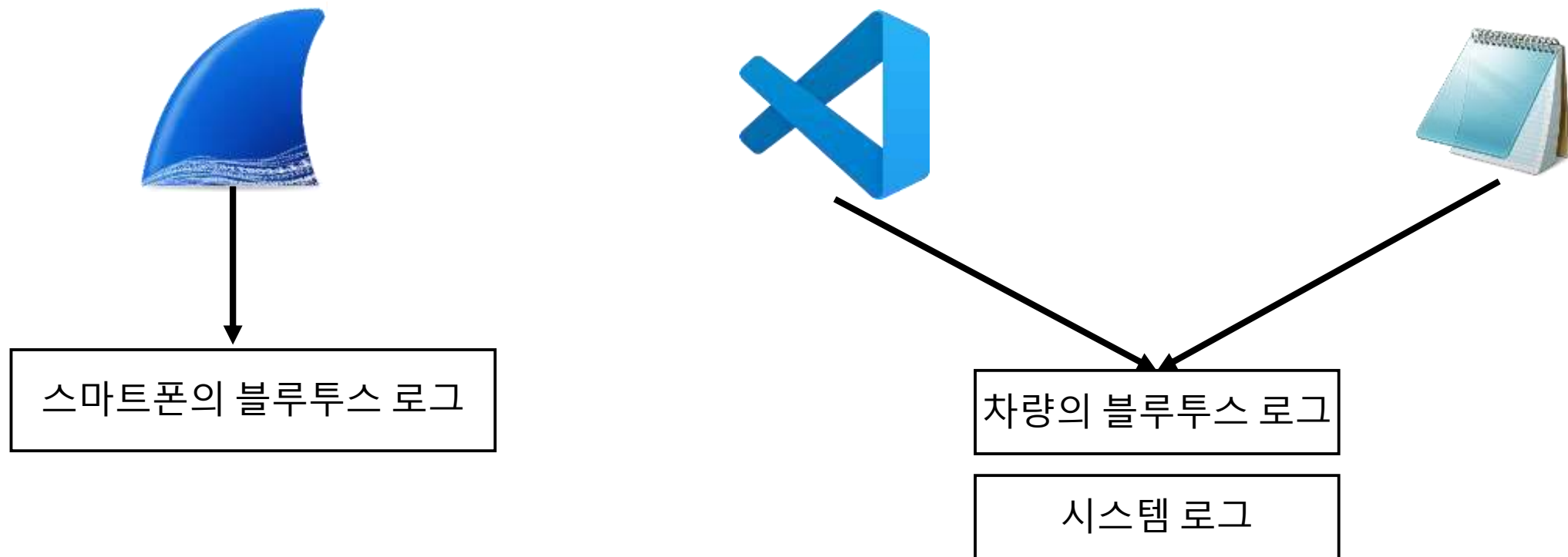
로그 수집 - 차량



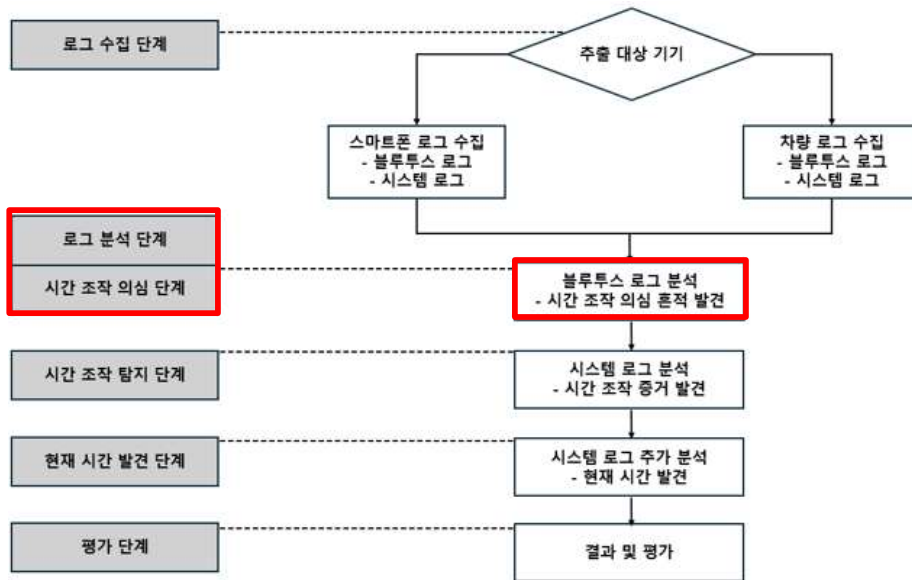
❖ 차량의 'Copy image to USB'를 통한 로그 데이터 추출

✓ 이 중 분석 대상 파일 정리

* 'bluetoothLog/' 경로에 블루투스 로그 데이터 존재



로그 분석 - 스마트폰 블루투스 로그 분석



❖ 스마트폰 블루투스 로그 분석 결과

- ✓ 날짜 변경이 먼저 이루어지고, 시간 변경이 이루어짐
- ✓ 이후 변경된 시간에서 수행된 이벤트에 대한 로그 확인 가능
- ✓ 시간 조작에 대한 로그 메시지는 확인 불가

2024-07-19 17:33:32.703606 controller
2024-07-13 17:33:32.722573 SamsungElect_85:e7:b7 (SOS*** S21)

→ 날짜 변경

host
LGInnotek_8c:11:b4 (Avante)

HCI_EVT
RTP

8 Rcvd Number of Completed Packets
63 PT=HPEG Audio, SSRC=0x2, Seq=4018, Time=250880, Mark

2024-07-13 17:33:41.046439 controller
2024-07-13 12:00:00.307375 controller

→ 시간 변경

host
host

HCI_EVT
HCI_EVT

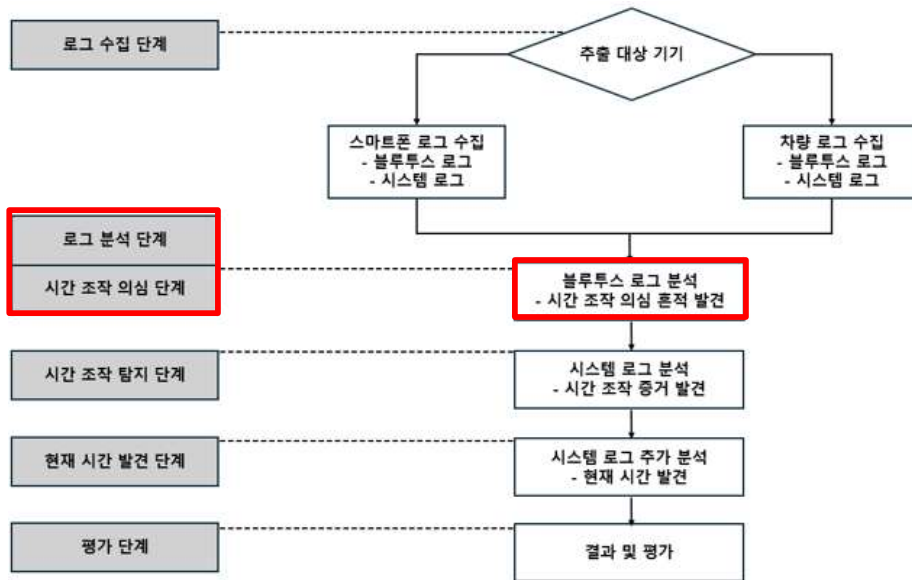
14 Rcvd Sniff Subrating
60 Rcvd LE Meta (LE Extended Advertising Report)

2024-07-13 12:00:22.415200 SamsungElect_85:e7:b7 (SOS*** S21) LGInnotek_8c:11:b4 (Avante)
2024-07-13 12:01:16.998617 SamsungElect_85:e7:b7 (SOS*** S21) LGInnotek_8c:11:b4 (Avante)

HFP
AURCP

52 Sent +CLCC: 1,0,2,0,0,"01049232190",129
123 Sent Vendor dependent: Stable - GetElementAttributes - title: "Over the Horizon"

로그 분석 - 차량 블루투스 로그



❖ 차량 블루투스 로그 분석 결과

- ✓ 날짜 변경과 시간 변경이 동시에 이루어짐
- ✓ 이후 변경된 시간에서 수행된 이벤트에 대한 로그 확인 가능
- ✓ 차량 또한 시간 조작에 대한 로그 메시지 확인 불가능

```
07-10 17:33:17.733 - D BTA_BT_PLAYER_MANAGER sendMetaDataToHomeWidget , title:Over the Horizon ,artist:Samsung ,device:SOS S21 ,Tune:null ,Browsing:false ,Cur:-1 ,Tot:-1 ,Play:0 ,Key:9466
07-11 14:00:00.104 - D AvrcpControllerService [BTAD] BroadcastPlayPosition pos:-1 ,len:-1
```

```
07-11 14:00:48.212 - D ===BTHFPManager=== onMobisBTCallInfo :: getContactPhoto callNum = 01049232198, callerName = 조민혁
07-11 14:01:02.006 - D BTA_BT_PLAYER_MANAGER sendMetaDataToHomeWidget , title:Over the Horizon ,artist:Samsung ,device:SOS S21 ,Tune:null ,Browsing:false ,Cur:-1 ,Tot:-1 ,Play:0 ,Key:9466
```

❖ 블루투스 로그 분석 결과 평가

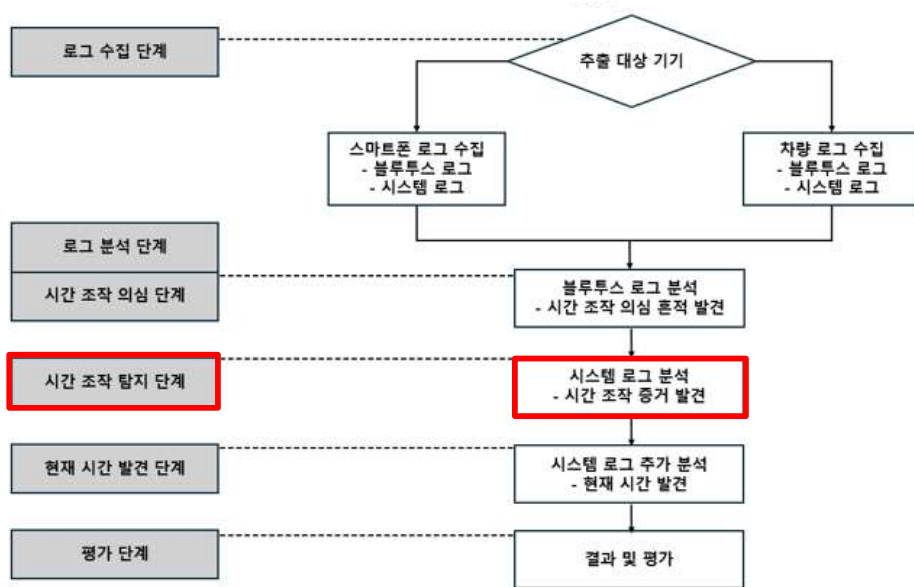
✓ '시간 조작 의심 단계'

✓ 두 기기 모두 시간 변경에 대한 타임스탬프는 확인 가능하였다

✓ 그러나, 두 기기 모두 시간 조작 로그 메시지는 확인할 수 없어서 안티 포렌식 행위인지는 판단 불가

✓ 즉, **시스템 로그 분석을 통한 시간 조작 로그 메시지 확인 필요**

로그 분석 - 스마트폰 시스템 로그



❖ 스마트폰 시스템 로그 분석 결과

- ✓ 'dumpstate.txt' 파일에서 다음과 같은 로그 메시지 확인 가능
- ✓ 'data/misc/wifi hostapd/dataUsage_log.txt' 경로에서 시간 조작 로그 메시지 발견 가능
- ✓ 'date changed', 'User Change Time to yyyy-MM-dd HH:mm:ss' 메시지를 통하여 안티 포렌식 행위가 수행되었음을 확인 가능

07-19 17:32:30.917 SemWifiApDataUsage date changed: current date = 2024-07-12 17:32:30, new date = 2024-07-19 17:32:30

07-13 17:33:32.831 SemWifiApDataUsage User Changed Time to yyyy-MM-dd HH:mm:ss = 2024-07-13 17:33:32

07-13 17:33:32.833 SemWifiApDataUsage date changed: current date = 2024-07-19 17:33:32, new date = 2024-07-13 17:33:32

07-13 12:00:00.110 SemWifiApDataUsage User Changed Time to yyyy-MM-dd HH:mm:ss = 2024-07-13 12:00:00

로그 분석 - 차량 시스템 로그

❖ 차량 시스템 로그 분석 결과

- ✓ 'SET_USER_TIME@UNIX Epoch Time' 파일이 생성됨
- ✓ @뒤 UNIX Epoch Time을 변환 시 조작된 시간임을 확인 가능
- ✓ 해당 파일 내 'isUsetTimeSet'이 true로 설정된 것을 확인 가능
- ✓ Offset을 반영하여 변환해본 결과 이전 시간을 확인할 수 있음

SET_USER_TIME@1720674000081

USER TIME SETTING

millis: 1720674000000

offset: [new] -703998606, [old] 0

timezone: [tz] Mobis/UTC+09:00, [dst] false

gps: Location[gps 37.584927,126.884593 acc=8 accH=0 accV=0 accP=0 odoS=1

gyroS=1 back=0 modocount=0 gpsstatus=1 drstatus=1 accelstatus=0 angle=0 t=2012113564000

tv=0 et=+26m24s520ms alt=0.0 vel=0.0 bear=299.42688 gnssSpeed=0.0 gnssHeading=0.0

(Bundle[[satellites=0, DREHPE=12.263329]])

nitz: [time]1721377998606, [lastTime] 1721376436008, [LastReceived] 22095, [systemElapsed] 1584693

user: [user] 0, [isSet] true

status: [isTimeSet] true, [isRealTimeArrived] true, [isGpsTimeArrived] false, [isNitzArrived] true, [isUsetTimeSet] true

Name	Timestamp	Value Input
Unix Milliseconds (Java Time)	2024-07-11 14:00:00.0810000 +09:00	Format: Numeric Value: 1720674000081 Decode

Name	Timestamp	Value Input
Unix Milliseconds (Java Time)	2024-07-19 17:33:18.6060000 +09:00	Format: Numeric Value: 1721377998606 Decode

❖ 시스템 로그 분석 결과 평가

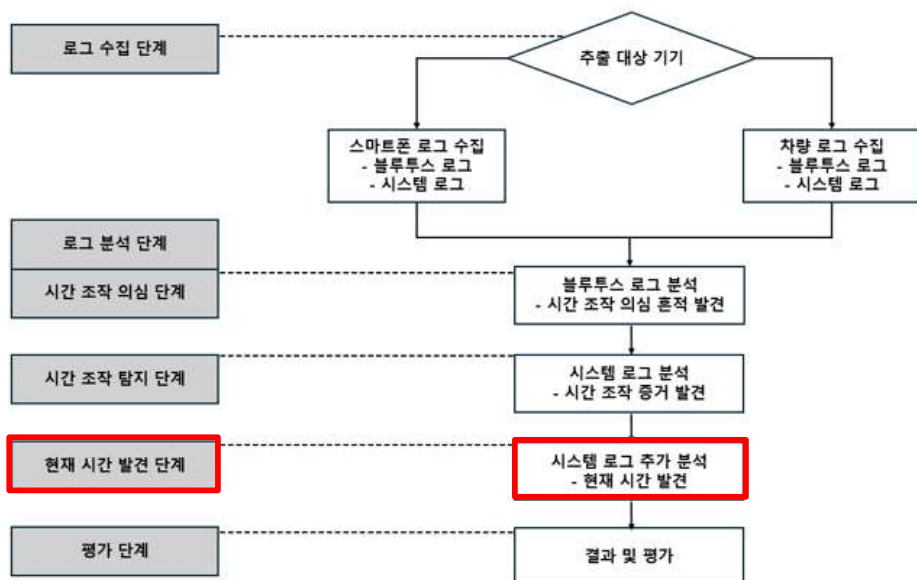
- ✓ '시간 조작 탐지 단계'

- ✓ 각 기기에서 시간 조작 로그 메시지 확인 가능

- ✓ 그러나, 조작 전 시간도 조작된 시간일 수 있기에 현재 시간을 찾는 과정 필요

- ✓ 즉, 시스템 로그 추가 분석 필요

로그 분석 - 시스템 로그 추가 분석



❖ 시스템 로그 추가 분석 결과

- ✓ 'mofgen2.txt' 파일에서 다음과 같은 로그 메시지 확인 가능
- ✓ 'GMT'로 표현된 것을 통해 그리니치 시간대인 것을 확인 가능
- ✓ 그리니치 시간대를 기준으로 한국은 9시간 빠르기에 +9 해준 결과 'Date Fri, 19 Jul 2024 17:33:31 GMT' 로 정확한 시간임을 알 수 있다

[MOF] 2024-07-11 14:00:13,130 INFO [HTTPHeader] root

(a.handleMessage:64)

- Date: Fri, 19 Jul 2024 08:33:31 GMT

❖ 시스템 로그 추가 분석 결과 평가

✓ '현재 시간 발견 단계'

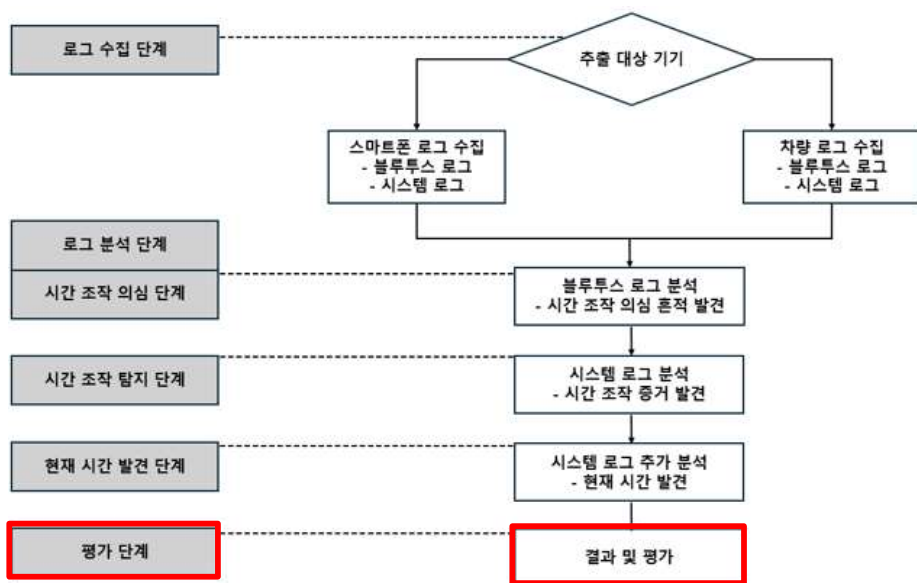
✓ 'mofgen2.txt' 파일에서 'GMT' 메시지 확인 가능

✓ 'GMT' 시간에 +9를 통하여 정확한 시간 발견 가능

05

결론 및 향후 연구

결과 및 평가



[표 9]. 각 로그 별 아티팩트 확인 가능 여부

	블루투스 로그	시스템 로그
타임스탬프 변경	O	O
시간 정보 조작	X	O
기존의 시스템 시간	X	O

❖ 결론

- ✓ 시간 정보가 조작된 상황에서 이를 탐지할 수 있는 기법 제시
- ✓ 블루투스 로그를 통해 시간 조작을 의심
- ✓ 시스템 로그를 통해 시간 조작을 탐지
- ✓ 시스템 로그를 추가 분석하여 정확한 시간을 찾을
- ✓ 이와 같은 시간 조작 프로세스를 통하여 효율적인 수사 가능할 것이라 기대
- ✓ 단, '블루투스 HCI 스냅 로그' 기능은 기본적으로 활성화 되어있는 기능이 아니다.
- ✓ 따라서 해당 기능이 활성화 되어있지 않다면 스마트폰의 블루투스 로그를 수집할 수 없다는 한계점 존재

❖ 향후 연구

- ✓ '블루투스 HCI 스냅 로그' 가 비활성화 되어있는 상태에서도 적용 방안 연구
- ✓ 여러 가지 시나리오를 추가 검증함으로써 해당 기법에 대한 일반화 예정

References

1. John Wiley & Sons Inc, Hoboken, NJ. "Digital Forensics: An Academic Introduction." 2018.
2. Gary C. Kessler. "Anti-Forensics and the Digital Investigator." 5th Australian Digital Forensics Conference, 3, 12, 2007.
3. Cho, Gyu-Sang. "Digital Forensic Analysis of Timestamp Change Tools: An Anti-Forensics Perspective." Korean Society of Computer Information Conference, 07a, Pages.391-392, 2019.
4. 이산, 정지현, 안석현, 조성제. "리눅스와 안드로이드에서 시간 정보 조작이 로깅에 미치는 영향 분석." 한국차세대컴퓨팅학회, 2024.
5. 윤지수, 이경렬. "안티 포렌식 신증기법에 대한 형사법적 대응방안." 한국형사정책학회 논문지, 32(4), 65-99. 2021.
6. Whelan, C. J., Sammons, J., McManus, B., and Fenger, T. W., "Retrieval of infotainment system artifacts from vehicles using iVe," Journal of Applied Digital Evidence, 1(1), 30, 2018.
7. Le-Khac, N.-A., Jacobs, D., Nijhoff, J., Bertens, K., and Choo, K.-K. R.. "Smart vehicle forensics: Challenges and case study." Future Generation Computer Systems, 109: 500-510, 2020.
8. R. Nusser and R. M. Pelz, "Bluetooth-based wireless connectivity in an automotive environment," Vehicular Technology Conference Fall 2000. IEEE VTS Fall VTC2000. 52nd Vehicular Technology Conference (Cat. No. 00CH37152), Vol. 4, pp.1935-1942, 2000.
9. 강해인, 박민수, 조성제, 정지현. "차량 디지털 포렌식에서 타임라인 분석을 위한 안드로이드 기반 오디오 비디오 내비게이션 시스템의 로그 활용." 한국정보과학회 2023 한국컴퓨터종합학술대회 논문집, 1,259-1,261. 2023
10. https://source.android.com/docs/core/connect/bluetooth/verifying_debugging?hl=ko
11. https://source.android.com/docs/core/connect/bluetooth/hci_requirements?hl=ko
12. <https://source.android.com/docs/core/tests/debug/read-bug-reports?hl=ko#event-log>

Acknowledgement

이 연구는 2021년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(no. 2021R1A2C2012574),

또한

2022년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(No.2022-0-01022, 이벤트 기반 실험시스템 구축을 통한 자동차 내·외부 아티팩트 수집 및 통합 분석 기술 개발).

감사합니다 !

Q&A
