

블루투스로 연결된 스마트폰과 자동차 인포테인먼트 시스템에서의 시간 조작 탐지

조민혁⁰¹ 이산² 정지현³ 김선재⁴ 조성제¹

단국대학교 모바일시스템공학과⁰¹ 단국대학교 산업보안학과²,

단국대학교 컴퓨터학과^{3,4}, 단국대학교 소프트웨어학과¹

{cgumgek8, dltsdhd915, wlgjsjames7224, rlatjswo0824, sjcho}@dankook.ac.kr

Detecting Timestamp Manipulation in Bluetooth-Connected Smartphone and Automotive Infotainment System

Min Hyuk Cho⁰¹, San Lee², Jiheun Jung³, Sun Jae Kim⁴, Seong-Je Cho¹

Department of Mobile System Engineering, Dankook University⁰¹

Department of Industrial Security, Dankook University²

Department of Computer Science and Engineering, Dankook University^{3,4}

Department of Software Science, Dankook University¹

요 약

디지털 포렌식은 컴퓨터나 스마트폰 등의 IT 기기에 저장된 디지털 데이터를 과학적으로 수집·분석하여 사건을 해결하는 것이다. 이때 IT 기기에서 추출한 타임스탬프는 이벤트들을 시간대별로 분석할 수 있는 근거이므로 디지털 포렌식 조사에서 매우 기본적이면서도 중요한 정보이다. 본 논문에서는 범죄자가 자신의 행위를 숨기기 위해, 자신 IT 기기의 시간을 조작했을 경우에, 시간 조작 여부를 탐지하는 기법을 제안한다. 구체적으로는 자동차의 인포테인먼트 시스템이 운전자의 스마트폰과 블루투스로 연결된 상황에서 발생한 이벤트들의 타임스탬프를 운전자가 조작했을 때, 이를 탐지하는 방법을 제안한다. 시간 조작 여부를 탐지하기 위해서, 우리는 스마트폰과 자동차 인포테인먼트 시스템으로부터, 블루투스 HCI 스눕 로그(HCI Snoop log), 블루투스 로그, 시스템 로그 등을 추출하고 분석한다. 시나리오 기반 실험을 통해, 제안 기법이 시간 조작 여부를 탐지할 수 있음을 보인다.

1. 서 론

디지털 포렌식(Digital Forensics)이란 디지털 데이터를 통해 디지털 증거의 보존, 수집, 검증, 식별, 분석, 해석, 문서화 및 제시를 위해 과학적으로 도출되고 입증된 방법을 사용하여 사건의 재구성을 촉진하거나 사건의 행위를 예측하는 데 도움을 주는 수사기법이다[1].

안티 포렌식(Anti-Forensics)이란 데이터를 위조, 변조, 은닉, 암호 사용, 파괴, 타임스탬프 조작 등을 통해 디지털 증거의 존재, 양 및 품질을 저하시켜 포렌식 수사를 어렵게 하거나 불가능하게 만드는 행위를 말한다[2].

타임스탬프는 이벤트들을 시간대별로 분석할 수 있는 근거가 되기 때문에 디지털 포렌식 분석에 있어서 가장 기본적이면서도 중요한 정보다. 범죄자는 타임스탬프를 조작하여 포렌식 수사를 어렵게 할 수 있다[3].

본 논문에서는 차량과 스마트폰 간에 블루투스로 연결된 환경에서 각 기기의 시간이 조작된 후 이벤트가 발생되었을 때 각 기기의 로그 데이터는 타임스탬프가 상이하게 기록되어 발생한다. 이와 같은 상황에서 본 논문은 블루투스 HCI 스눕 및 블루투스 로그 분석과 시스템 로그 분석을 통하여, 안티 포렌식 행위인 시스템 시간 조작 여부를 탐지하는 기법을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 리눅스 PC와 안드로이드 시스템의 타임스탬프 변경 및 차량에서의 포렌식 관련 연구에 대해 설명하고, 3장에서는 딜러 모드 및 추출하고자 하는 로그 데이터 종류에 대해 설명한

다. 4장에서는 ‘시간 조작 탐지 기법’이라는 방법을 간략하게 제시하며, 5장에서는 시나리오 기반 실험을 통해 생성된 로그 데이터를 수집하는 방법을 제시한다. 6장에서는 수집된 로그에 대해 분석하는 과정을 진행한다. 7장에서는 분석된 로그를 통해 결과를 도출하고, 본 논문에서 발생하는 한계점을 기술한다. 마지막으로 8장에서는 결론과 향후 연구를 기술한다.

2. 관련 연구

이산 등[4]은 리눅스 PC와 안드로이드 기기에서 각각 시간 조작을 하였을 때, 리눅스의 syslog 파일을 분석하여 시간 조작의 흔적을 찾았다. 그 다음, 루팅된 안드로이드 기기에서 logcat 명령어로 로그를 수집하여 분석해 안드로이드 기기의 시간 조작 흔적을 찾아 시간 변경의 시점을 파악하였다.

윤지수 등[5]은 안티 포렌식 기법들과 형사 처벌 방안을 제시하였다. 또한 타임스탬프를 손상시키는 행위는 파일 및 시스템 관리에 문제를 야기하며 포렌식 수사 지연시킬 수 있다고 하였다.

Whelan 등[6]과 Le-Khac 등[7]은 Volkswagen, Dodge Dart 및 Toyota Highlander Limited의 인포테인먼트 시스템을 대상으로 포렌식 분석을 수행했다. 이 연구를 통해 내비게이션 사용 기록, Wi-Fi 및 블루투스 연결 정보, 최근 차량 위치, 트랙 로그(track log), 운전자의 개인 데이터(예: 통화 기록, 연락처 목록, SMS 메시지, 사진, 비

디오)와 같은 다양한 디지털 정보를 추출할 수 있음을 확인했다.

기존 연구에서는 안드로이드 모바일 기기와 리눅스 PC의 타임스탬프를 조작하여 실험을 진행해 로그를 수집한 후 분석하여 시간 조작 증거를 찾았다. 또한 차량 포렌식을 통하여 사용자의 데이터를 추출하였다. 그러나 블루투스 연결 환경에서 시간 조작을 통해 양 기기의 시간 정보가 다를 때 시스템 및 로그에 어떤 영향을 미치는 지에 대한 연구, 그리고 포렌식 수사에서 어떤 시간 대로 결정하여 수사를 진행해야 하는지에 대한 연구가 수행된 적이 없다. 따라서 본 논문에서는 블루투스 HCI 스냅 로그 및 블루투스 로그, 시스템 로그 분석 과정을 통해 시간 조작 탐지 기법을 제시한다.

3. 배경 지식

3.1 딜러 모드

딜러 모드는 차량의 AVN 시스템의 히든 메뉴로 특정 방법을 통해 접근 가능하다. 딜러 모드에 접근하여 소프트웨어 업데이트, 차량의 시스템 진단 정보, 그리고 'Copy to USB'를 통해 로그 수집이 가능하다.

3.2 블루투스 로그

블루투스 기능은 서로 다른 종류의 기기여도 통신이 가능하게 해준다. 만약 서로 다른 종류의 기기가 양 기기 간 통신이 필요한 상황이라면 블루투스 기능을 이용해볼 수 있다. 각 기기가 블루투스 기능을 지원한다면 블루투스 기능을 활성화함으로써 서로 다른 기기 간에 통신이 가능해진다[8]. '블루투스 로그'란 블루투스 통신을 한 기기 간에 블루투스 통신과 관련된 다양한 이벤트와 상태 변화를 기록한 로그 파일이다.

3.3 시스템 로그

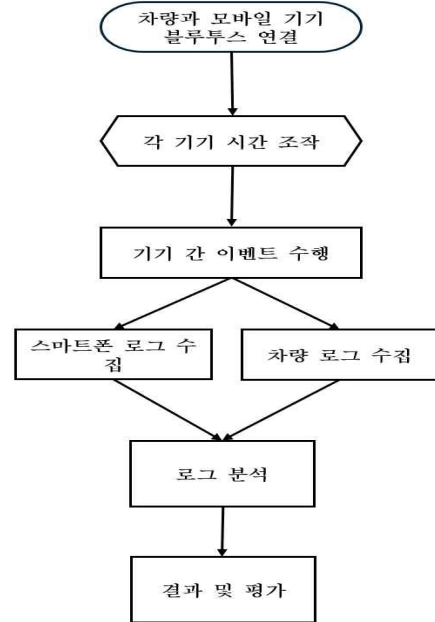
시스템 로그는 운영체제와 어플리케이션의 동작을 기록한 파일로써, 시스템의 상태를 모니터링하고 문제를 디버깅하는데 중요한 정보를 제공한다. 시스템 로그는 다양한 이벤트, 오류, 경고, 정보 메시지를 포함해 기기의 전반적인 활동을 기록한다[9].

3.4 블루투스 HCI 스냅 로그

블루투스 HCI 스냅 로그는 블루투스 통신을 모니터링하고 디버깅하기 위해 생성되는 로그다. 해당 로그는 블루투스 프로필을 통하여 로그의 특성을 보여준다[10]. 또한 HCI 이벤트 메시지를 통하여 현재 블루투스 연결된 기기들의 상태를 분석 가능하게 해준다[11]. 블루투스 HCI 스냅 로그를 사용하기 위해서는 Android 4.4(KitKat) 이상의 기기에서 수동으로 개발자 옵션을 통한 활성화를 해야 한다. 이를 통해 블루투스 호스트와 컨트롤러 간의 모든 HCI 로그를 캡처하여 블루투스 연결 상태 및 데이터 전송 상태를 분석할 수 있다.

4. 시간 조작 탐지 기법

본 논문에서 제안하는 시간 조작 탐지 기법에 대한 프로세스가 그림 1에 나타나 있다.



[그림 1]. 시간 조작 탐지 기법의 프로세스

먼저 기기 간 블루투스 연결을 진행을 한다. 이후, 각 기기의 시간을 조작한다. 시간 조작 같은 경우 표 1과 같이 여러 가지 경우의 수가 존재한다.

[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

시간 조작 이후, 각 기기 간 이벤트를 수행한다. 블루투스 연결 환경에서 가능한 이벤트의 종류는 표 2와 같다.

[표 2]. 블루투스 연결 환경 이벤트 목록

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

이벤트 수행 이후, 각 기기의 로그를 수집한다. 스마트폰의 경우, ADB(Android Debug Bridge) 환경에서 로그를 수집한다. 로그를 추출하는 명령어는 표 3과 같다.

[표 3]. ADB 로그 추출 명령어

명령어
logcat
bugreport

logcat의 명령어는 휘발성 로그에 대해 로그 추출이 가능하다. 만약 모바일 기기의 전원이 꺼진다면 로그가 모두 사라진다. bugreport 명령어의 경우 logcat의 로그 데이터를 포함하여 시스템의 전체적인 로그 데이터를 추출 가능하므로 bugreport를 통하여 모바일 기기의 로그 데이터를 추출한다[12]. 차량의 경우 로그를 추출할 수 있는 방식은 표 4와 같다.

[표 4]. 차량 로그 추출 방법

로그 추출 방법
Chip-off
Copy image to USB

Chip-off 방식의 경우 디지털 장치에서 메모리칩을 물리적으로 제거하여 로그 데이터를 추출하는 방식이다. 이 경우 메모리칩 손상 가능성이 있기에 Chip-off 방식은 본 논문에서는 사용하지 않는다. 따라서 차량 AVN의 딜러 모드에 접근하여 Copy image to USB를 통하여 로그 데이터를 추출한다.

로그를 수집한 후 로그 분석을 진행한다. 생성된 로그 파일에서 '수정한 날짜' 태그를 확인하여 해당 실험 날짜 타임스탬프로 생성된 로그 파일 위주로 분석한다. 또한 기기 간에 블루투스 연결을 통한 통신을 하였기에 블루투스 로그 역시 분석한다. 이후, 시간 조작 관련 키워드를 이용해 분석을 한다. 시간 관련 키워드는 표 5와 같다. 만약 시간 조작 관련 로그 메시지가 존재하지 않는다면 변경된 타임스탬프 전후로 로그 데이터를 분석하도록 한다. 마지막으로 분석 결과를 평가한다.

[표 5]. 시간 관련 키워드

시간 관련 키워드	
TimeChange	DateSet
TimeSet	UsetTime
DateChange	UsetDate

5. 실험 환경 및 실험 방법

5.1 실험 대상 시스템

본 논문의 실험 대상 시스템은 국내 차량에 탑재되는 Android 4.4.2(KitKat) 버전의 AVN과 Android 14버전을 탑재한 Galaxy S21이다. 본 논문에서 사용한 AVN 시스템과 모바일 기기의 사양은 표 6과 같다.

[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-tcc
모바일 기기	
기기명	Galaxy S21
제조사	Samsung
운영체제	Android 14
커널 버전	Linux 5.4.242-27760517-abG991NKSU4FWK7

AVN 내부에서 운전자 행위와 관련된 로그 데이터를 생성하기 위해서 시나리오 기반의 실험을 했다. 주행 중 운전자가 수행할 수 있는 이벤트를 선별하고 표 7과 같은 시나리오를 작성했다.

[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

차량 시간 조작 당시 시스템 시간은 2024.07.19.17:33이었으며, 스마트폰 시간 조작 당시 시스템 시간은 2024.07.19.17:33이었다.

만약 안티 포렌식 행위를 수행하는 범죄자가 날짜 및 시간을 조작한다면 미래 시간보다는 과거로 조작하여 포렌식 행위에 혼란을 줄 수 있다. 예를 들어, 사건 발생 시간대에 본인은 그 시간대에 다른 행위를 하고 있었다고 주장할 수 있다. 따라서 표 8과 같이 두 기기 모두 과거로 조작하되 서로 다른 과거로 조작하여 혼란을 증가시켰다.

[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

5.2 로그 수집

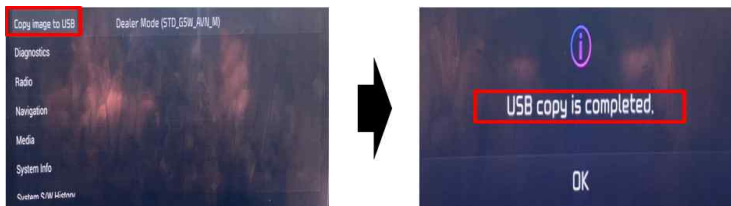
시나리오 기반으로 실험을 진행한 후 로그 데이터를 수집하였다. 먼저, 스마트폰의 경우 4장에서 언급한 방식으로 bugreport 명령어를 이용하여 로그 데이터를 수집

한다. 로그 데이터를 추출한 후 분석 대상 로그 파일은 그림 2와 같다.

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

[그림 2]. 추출된 스마트폰의 로그 중 분석 대상 파일

차량의 로그는 그림 3과 같이 '딜러 모드'에 접근 후 'Copy image to USB' 버튼을 클릭하여 로그 덤프를 하였다. 로그 데이터를 추출한 후 분석 대상 로그 파일은 그림 4와 같다.



[그림 3]. 차량의 로그 덤프 과정

dumpstate-20240711.140225.00	bluetoothLogFilter
SET_USER_TIME@1720674000081	bluetoothLogFilter.log
moften2	bluetoothLogFilter.log
bluetoothLog	bluetoothLogFilter.log
	bluetoothLogFilter.log
	bluetoothLogFilter.log
	bluetoothLogFilter.log
	BluetoothStackLog_0

[그림 4]. 추출된 차량의 로그

6. 로그 분석

본 장에서는 5장에서 획득한 로그 데이터를 분석한다. 수집한 로그 데이터는 작성한 시나리오를 기반으로 시간 조작 후 수행한 이벤트 위주로 분석하였다. 블루투스 패킷의 경우 와이어샤크로 분석을 하였고, 그 외 로그 데이터는 메모장, VSCode를 이용하여 분석하였다.

2024-07-19 17:33:32.703606	controller	host	HCI_EVT	8 Rcvd Number of Completed Packets
2024-07-13 17:33:32.722573	SamsungElect_85:e7:b7 (SOS*** S21)	LGIInnotek_8c:11:84 (Avante)	RTP	63 PT=MPEG Audio, SSRC=0x2, Seq=4018, Time=250880, Mark
↓ 날짜 변경				
2024-07-13 17:33:41.846439	controller	host	HCI_EVT	14 Rcvd Sniff Subrating
2024-07-13 12:00:00.307375	controller	host	HCI_EVT	60 Rcvd LE Meta (LE Extended Advertising Report)
↓ 시간 변경				

[그림 5]. 스마트폰의 변경된 타임스탬프

2024-07-13 12:00:22.415200	SamsungElect_85:e7:b7 (SOS*** S21)	LGIInnotek_8c:11:84 (Avante)	HFP	52 Sent +CLCC: 1,0,2,,0,"01049232198",129
2024-07-13 12:01:16.998617	SamsungElect_85:e7:b7 (SOS*** S21)	LGIInnotek_8c:11:84 (Avante)	AVRCP	123 Sent Vendor dependent: Stable - GetElementAttributes - Title: "Over the Horizon"

[그림 6]. 스마트폰의 변경된 시간 정보에서의 이벤트

6.1 스마트폰 블루투스 HCI 스냅 로그 분석

스마트폰 블루투스 HCI 스냅 로그를 분석한 결과, 시스템 시간을 기준으로 로그가 생성되다가 스마트폰 시간을 조작한 시점에서 그림 5와 같이 타임스탬프가 변경되어 로그가 발생했다.

이후, 그림 6과 같이 시나리오에서 작성한 이벤트들이 발생한 로그들을 발견할 수 있었다. 따라서 시간 조작된 상태에서 타임스탬프는 변경된 시간을 기준으로 로그가 생성되고, 변경된 타임스탬프에서 이벤트가 수행되었음을 알 수 있었다.

6.2 차량 블루투스 로그 분석

차량의 블루투스 로그를 분석한 결과 스마트폰 블루투스 HCI 스냅 로그 분석 결과와 유사하게 차량의 시스템 시간을 따르는 로그들이 생성되다가 그림 7과 같이 시간 조작이 수행된 시점에 타임스탬프가 변경되어 로그가 생성되었다. 이후 그림 8과 같이 변경된 타임스탬프에서 통화 이벤트, 음악 이벤트가 수행된 로그를 확인할 수 있었다.

6.1절에서와 같이 스마트폰 블루투스 HCI 스냅 로그 분석한 결과와 차량 블루투스 로그 분석한 결과를 정리해보았을 때, 타임스탬프가 변경되었음을 통해 시간 조작에 대한 안티 포렌식 행위를 의심해볼 수 있었다.

또한 변경된 타임스탬프에서 이벤트에 대한 로그들이 발생하는 것을 알 수 있었다. 그러나 타임스탬프가 변경되었음을 알 수 있음을 제외하고는 시간 조작에 대한 증거를 블루투스 로그에서 발견할 수 없었다.

따라서 시스템 로그 분석을 통해 시간 정보 조작에 대한 안티 포렌식 행위를 찾는 과정이 필요하다.


```
07-19 17:33:17.733 - D BTA_BT_PLAYER_MANAGER sendMetaDataToHomeWidget , title:Over the Horizon ,artist:Samsung ,device:S05의 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
```

[그림 7]. 차량의 변경된 타임스탬프

```
07-11 14:00:48.212 - D ===BTHFPManger=== onMobisBTCallInfo :: getContactPhoto callNum = 01049232198, callerName = 조민혁
07-11 14:01:02.806 - D BTA_BT_PLAYER_MANAGER sendMetaDataToHomeWidget , title:Over the Horizon ,artist:Samsung ,device:S05의 S21 ,Tune:null ,Browsing:false ,Cur:-1 ,Tot:-1 ,Play:0 ,Key:9466
```

[그림 8]. 차량의 변경된 타임스탬프에서의 이벤트

6.3 스마트폰 시스템 로그 분석

스마트폰 시스템 로그 분석은 'dumpstate-2024-07-19-17-59-48.txt' 파일을 통해 분석 가능하다. 해당 파일의 로그를 분석해본 결과 'data/misc/wifi_hostapd/dataUsage_log.txt' 경로에 그림 9와 같은 로그들이 존재하였다.


먼저 '7-19 17:32:30'에서 '7-13 17:33:32'로 날짜 변경이 먼저 이루어졌고, 이후 '07-13 12:00:00'로 시간 변경이 이루어졌다. 또한 'date changed', 'User Change Time to yyyy-MM-dd HH:mm:ss' 메시지가 존재하였다. 따라서 해당 로그를 통해 안티 포렌식 행위가 수행되었음을 알 수 있었다.

```
07-19 17:32:30.917 SemWifiApDataUsage date changed: current date = 2024-07-19 17:32:30, new date = 2024-07-13 17:33:32
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 = 2024-07-13 17:33:32, new date = 2024-07-13 12:00:00
07-13 12:00:00.110 SemWifiApDataUsage User Changed Time to yyyy-MM-dd HH:mm:ss = 2024-07-13 12:00:00
```

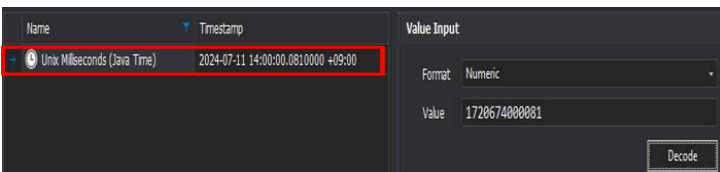
[그림 9]. 시간 조작 시스템 로그

6.4 차량 시스템 로그 분석

차량의 시간을 조작한다면 그림 10과 같이 'SET_USER_TIME@Unix Epoch Time.txt' 파일이 생성된다. @뒤에 있는 숫자는 변경된 시간을 Unix Epoch Time으로 표현된 것이다. 따라서 이에 대해 해당 Unix Epoch Time을 'DCode v5.6' 프로그램을 이용하여 시간 변환하면 그림 11과 같이 표현됨을 통해 조작된 시간임을 알 수 있다. 해당 텍스트 파일을 메모장을 통해 열어보면 그림 12와 같은 화면을 볼 수 있다.

 SET_USER_TIME@1720674000081

[그림 10]. 'SET_USER_TIME' 파일



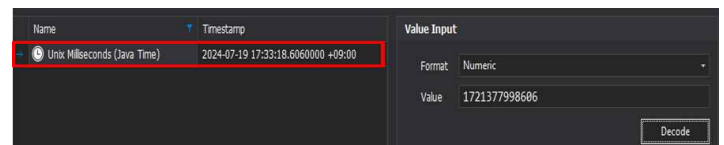
[그림 11]. Unix Epoch Time 시간 변환

```
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]]])
nits: [time]1721377998606, [lastTime] 1721376436008, [LastReceived] 22095, [systemElapsed] 1584693
user: [user] 0, [isSet] true
status: [isTimeSet] true, [isRealTimeArrived] true, [isGpsTimeArrived] false, [isNitsArrived] true, [isUserTimeSet] true
```

[그림 12]. SET_USER_TIME@Unix Epoch Time 파일

해당 파일의 내용을 분석해보면 'status' 항목의 'isUserTimeSet' 부분이 true로 설정되어있다. 이를 통해 사용자가 설정한 시간임을 알 수 있고, 'offset' 항목의 'new' 부분이 -703998606로 설정되어있다. 이를 통해 설정된 시간이 기존 시간에서 얼마만큼 차이가 났는지를 알 수 있다.

설정된 Unix Epoch Time과 -703998606를 계산하여 시간 변환을 진행하면 그림 13과 같은 결과를 통해 시간이 조작되었다고 알 수 있다.



[그림 13]. Unix Epoch Time 시간 변환

차량의 'SET_USER_TIME@Unix Epoch Time.txt' 파일 분석을 통해 시간이 조작되었음을 알 수 있었다. 또한 이전의 시간은 어떤 시간이었는지 어느 시간으로 시간 조작을 시도했는지 알 수 있었다. 그러나 이전의 시간 역시 조작된 시간일 수 있기에 진짜 시간을 찾는 과정이 필요하다. 이를 위해 'mofgen2.txt' 파일을 분석하였다.

해당 파일을 열어 분석을 해본 결과, 그림 14와 같은 로그 메시지를 확인할 수 있었다.

[MOF 2024-07-11 14:00:13.130] INFO [HTTPHeader] root (a.handleMessage:64) - Date: Fri, 19 Jul 2024 08:33:31 GMT

[그림 14]. mofgen2.txt 파일의 로그 메시지

해당 파일을 분석해보면 '2024-07-11-14:00:13' 으로 조작된 시간이 타임스탬프로 존재한다. 그리고 로그 메시지는 'Date: Fri, 19 Jul 2024 08:33:31 GMT'로 그리니치 시간대로 존재한다. 그리니치 시간대로 존재하기에 오른쪽 메시지는 시스템 시간인 것을 알 수 있다. 따라서 한

국의 시간이 그리니치 시간대를 기준으로 9시간 빠르기
에 +9를 해주면 'Date Fri, 19 Jul 2024 17:33:31'로 정확
한 시간을 알 수 있다.

7. 논의 및 한계점

본 논문에서는 Hyundai Avante AVN 시스템의 로그
데이터를 '딜러 모드'에 접속하여 'Copy image to USB'
를 통해 로그 데이터를 획득했다. 또한 Samsung Galaxy
S21, Android 14 모바일 기기를 'bugreport' 명령을 통해
서 로그 데이터 및 패킷을 획득할 수 있었다. 6절에서는
획득한 로그 데이터 및 패킷을 분석을 진행하였다.

먼저, 스마트폰 블루투스 HCI 스냅 로그 및 차량의 블
루투스 로그에서는 타임스탬프가 변경된 로그를 통해 시
간 조작이 이루어졌단 걸 의심해볼 수 있었다. 그러나
사용자가 안티 포렌식 행위를 했다는 메시지는 발견할
수 없었다.

따라서 안티 포렌식에 대한 명확한 증거를 찾기 위해
스마트폰 시스템 로그와 차량의 시스템 로그를 분석해본
결과 시간 조작이 이루어졌다는 걸 알 수 있었다. 또한
기존의 시스템 시간이 무엇인지 알 수 있었다. 분석된
결과를 정리하면 표 9와 같다.

본 논문에서는 '블루투스 HCI 스냅 로그' 기능을 활성
화를 하여 블루투스 로그 수집하였다. 그러나 해당 기능
은 기본적으로 활성화 되어있는 기능이 아니기 때문에
수동으로 ON/OFF를 해줘야한다. 만약 해당 기능이 OF
F 상태라면 블루투스 로그가 생성되지 않기 때문에 블루
투스 로그 수집할 수 없다는 한계점이 존재한다.

[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

8. 결론 및 향후 연구

본 논문에서는 차량 및 모바일 기기 간 블루투스 연결
이 된 환경에서 각 기기의 시간 정보가 조작되었고, 시
간 정보가 조작된 상황에서 이벤트가 발생했을 때 시간
정보 조작을 탐지할 수 있는 기법을 제시했다. 먼저 블
루투스 로그를 수집 후 분석하여 시간 조작을 의심하고,
시스템 로그를 분석하여 시간 조작에 대한 아티팩트를
찾음으로써 시간 조작 행위가 이루어졌다는 걸 알 수 있
었다.

마지막으로 시스템 로그를 추가 분석하여 정확한 시간
을 찾을 수 있었다. 범죄자가 시간을 조작한 후 이벤트를
수행하여도 위와 같은 과정을 통해 정확한 시스템 시
간을 알아내어 사건에 대한 조사를 효율적으로 진행할
수 있을 것이다.

단, '블루투스 HCI 스냅 로그' 기능은 기본적으로 활성
화 되어 있는 기능이 아니기에 향후 해당 기능이 비활성

화 되어 있는 환경에서도 블루투스 로그를 수집할 수 있
는 방법을 연구하고, 본 논문에서는 하나의 시나리오만
으로 실험을 진행하였지만 여러 시나리오를 두어 실험을
함으로써 해당 기법에 대해 일반화를 할 계획이다.

ACKNOWLEDGEMENT

이 연구는 2021년도 정부(과학기술정보통신부)의 재원으
로 한국연구재단의 지원을 받아 수행된 기초연구사업임
(no. 2021R1A2C2012574), 또한 2022년도 정부(과학기술
정보통신부)의 재원으로 정보통신기획평가원의 지원을
받아 수행된 연구임(No.2022-0-01022, 이벤트 기반 실험
시스템 구축을 통한 자동차 내·외부 아티팩트 수집 및
통합 분석 기술 개발).

참고 문헌

- [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 Times tamp Change Tools: An Anti-Forensics Perspective." Korean Society of Computer Information Conference, 07 a, Pages.391-392, 2019.
- [4] 이산, 정지현, 안석현, 조성제. "리눅스와 안드로이드
에서 시간 정보 조작이 로깅에 미치는 영향 분석." 한국
차세대컴퓨팅학회, 2024.
- [5] 윤지수, 이경렬. "안티 포렌식 신종기법에 대한 형사
법적 대응방안." 한국형사정책학회 논문지, 32(4), 65-99.
2021.
- [6] Whelan, C. J., Sammons, J., McManus, B., and Fen
ger, T. W., "Retrieval of infotainment system artif
acts from vehicles using iVe," Journal of Applied Digit
al Evidence, 1(1), 30, 2018.
- [7] Le-Khac, N.-A., Jacobs, D., Nijhoff, J., Bertens, K.,
and Choo, K.-K. R.. "Smart vehicle forensics: Challenge
s and case study." Future Generation Computer System
s, 109: 500-510, 2020.
- [8] R. Nusser and R. M. Pelz, "Bluetooth-based wireles
s connectivity in an automotive environment," Vehicula
r Technology Conference Fall 2000. IEEE VTS Fall VT
C2000. 52nd Vehicular Technology Conference (Cat. N
o. 00CH37152), Vol. 4, pp.1935-1942, 2000.
- [9] 강해인, 박민수, 조성제, 정지현. "차량 디지털 포렌식
에서 타임라인 분석을 위한 안드로이드 기반 오디오 비
디오 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>