리눅스와 안드로이드에서 시간 정보 조작이 로깅에 미치는 영향 분석

이산, 조성제, 정지헌, 안석현

1. 서론

o 디지털 포렌식: 디지털 데이터를 수집.복구.분석.보고하는 과정을 수행하여, 법적 증거를 확보하는 것
o 안티-포렌식 : 디지털 포렌식 수사를 방해하는 기법. (예: 타임스탬프 조작)
o 본 연구의 목표:
- 리눅스 PC와 안드로이드 폰에서, 시스템 시간정보 조작이 로깅 시스템에 미치는 영향 분석
- 로그 파일을 분석하여 타임스탬프가 조작된 시점 파악

2. 실험 방법

- **실험 대상**

  리눅스 PC(Ubuntu 22.04)
  안드로이드 스마트폰(Samsung Galaxy S8, PIE)

- **환경 설정**

  리눅스 PC: 설정 - Automatic Date & Time(비활성화) - Date & Time 조작
  안드로이드: 설정 - 날짜 및 시간(비활성화) - USB 디버깅 활성화

- **실험 방법**

1. 리눅스에서 시간 조작 및 로그 분석

1-1. 과거 시간대로 타임스탬프 변경

-> 현재 일시 : 2024.03.10. 15:00
-> 변경 일시 : 2019.03.03. 08:30

```
Mar  3 08:30:07 san-virtual-machine apt.systemd.daily[5464]: WARNING: file /var/lib/apt/periodic/upgrade-stamp has a timestamp in the future: 1710082800
```

'cat /var/log/syslog' 내용 중 일부 로그메시지

- 대부분의 로그들이 기록된 syslog를 logcat 명령어로 읽다가 'WARNING' 경고메시지가 기록된 로그를 발견
- 해당 로그 메시지의 내용은 1710082800 utc 시간대에 타임스탬프가 변경되었다는 경고메시지
- 해당 utc 시간대를 현재 시간으로 바꾼 결과, 시간 변경을 시도했던 '2024.03.10 15:00' 시간을 확인

```
root@san-virtual-machine:/home/san# date -u -d @1710082800
2024. 03. 10. (일) 15:00:00 UTC
```

- 이 결과로 해당 utc 시간에 시스템 시간 변경을 시도한 것을 찾을 수 있음

1-2. 미래 시간대로 타임스탬프 변경

-> 현재 일시 : 2024.03.11. 14:20
-> 변경 일시 : 2025.02.01. 05:30

```
san@san-virtual-machine:~$ cat /var/log/syslog
Mar 11 14:20:40 san-virtual-machine systemd[1]: rsyslog.service: Sent signal SIGHUP to main process 831 (rsyslogd) on client request.
Mar 11 14:20:40 san-virtual-machine systemd[1]: logrotate.service: Deactivated successfully.
Mar 11 14:20:40 san-virtual-machine systemd[1]: Finished Rotate log files.
Feb 11 14:20:40 san-virtual-machine systemd-resolved[618]: Clock change detected. Flushing caches.
Feb 11 14:20:40 san-virtual-machine systemd-timedated[3980]: Changed local time to Tue 2025-02-11 14:20:40 KST
Feb 11 14:20:41 san-virtual-machine systemd[1]: apt-daily-upgrade.service: Deactivated successfully.
Feb 11 14:20:41 san-virtual-machine systemd[1]: Finished Daily apt upgrade and clean activities.
Feb 11 14:20:41 san-virtual-machine systemd[1]: apt-daily-upgrade.service: Consumed 2.288s CPU time.
Feb  1 14:20:40 san-virtual-machine systemd-timedated[3980]: Changed local time to Sat 2025-02-01 14:20:40 KST
Feb  1 14:20:40 san-virtual-machine systemd-resolved[618]: Clock change detected. Flushing caches.
Feb  1 04:20:40 san-virtual-machine systemd-timedated[3980]: Changed local time to Sat 2025-02-01 04:20:40 KST
```

'cat /var/log/syslog' 내용 중 일부 로그메시지

- 정상로그들이 생성되다가 특정 시점에 시간이 상이하게 찍힌 로그가 생성되며, 그 이후부터 해당 시간으로 로그들이 생성됨
- 'Changed local time to' 라는 메시지가 Mar 11 에서 Feb 11로 넘어갈 때 최초로 생성되었으며, 연도-월-날짜-시간 순으로 순차적으로 변경되는 것을 관측
- 시간이 상이하게 찍히며 시간 변경 메시지들 담은 시점이 변경 시점

2. 안드로이드에서 시간 조작 및 로그 분석

2-1. 과거 시간대로 타임스탬프 변경

-> 현재 일시 : 2024.03.11 18:17
-> 변경 일시 : 2025.03.03 08:30

- adb로 접근하여 logcat명령어로 생성되는 로그들을 분석한 결과

```
03-11 18:17:00.555  3799  4377 D AlarmManagerService: Setting time of day to sec=1710148621
03-11 18:17:11.139  3799  8422 D AlarmManagerService: Setting time of day to sec=1551604631
03-03 18:17:17.988  3799  5560 D AlarmManagerService: Setting time of day to sec=1551569400
```

- 리눅스와 마찬가지로 utc시간대에 시간변경이 시도된 흔적이 있는 로그 메시지를 발견('Setting time of day to sec = utc')
- '2024.03.11 18:17' 에 시간 조작을 시도하였다는 것을 확인

2-2 미래 시간대로 타임스탬프 변경

-> 현재 일시: 2024.03.11 16:38
-> 변경 일시: 2025.02.01 05:30

```
03-11 16:38:18.959 16213 16213 D ViewRootImpl@c38c6c2[SubSettings]: ViewPostIme pointer 1
03-11 16:38:19.503 16213 16213 D ViewRootImpl@c38c6c2[SubSettings]: ViewPostIme pointer 0
03-11 16:38:19.572  3799  8142 D AlarmManagerService: Setting time of day to sec=1738395499
02-01 16:38:19.577 16213 16213 D DateTimeSettings: Cannot find preference with key auto_24hour in Controller AutoTimeFormatPreferenceController
02-01 16:38:19.618  3349  5101 E BufferQueueProducer: [com.android.settings/com.android.settings.SubSettings[16213]#1] disconnect: not connected (req=1)
02-01 16:38:19.619 16213 16213 D ViewRootImpl@c38c6c2[SubSettings]: dispatchDetachedFromWindow
```

- 과거시간대와 마찬가지로 logcat 명령어로 변경된 시점을 찾음

3. 실험 결과

o 리눅스 : 'WARNING' ,'Change local time'등의 문구로 시간 조작 확인
o 안드로이드 : 'Setting time to'문구로 시간 조작 확인 가능

**용의자(범죄자)가 언제 시간을 조작하였는지 확인 가능*

	과거시간대	미래시간대
리눅스 PC (Ubuntu 22.04)	'WARING' 타임스탬프 경고 문구로 변경된 시점 확인	'Change local time' 문구가 생성된 로그로 변경된 시점 확인
안드로이드 스마트폰 (삼성 갤럭시 S8, PIE)	'Setting time to day' 해당 UTC time으로 변경된 시점 확인 가능	'Setting time to day' 해당 UTC time으로 변경된 시점 확인 가능

4. 결론

- 리눅스 기반 PC와 안드로이드 기반 스마트폰을 대상으로 연구 수행
- 시간 정보 변경이 로그 정보에 미치는 영향 분석
- 사용자(용의자, 범죄자)의 의도적인 시간 변경 가능성
- 수사관이 기기 로그 분석을 통해 시간 변경 시점 파악

- **한계점**

  - 시간 변경 시 생성된 로그 메시지가 시스템 용량 초과 시 사라질 가능성
  - 다양한 운영체제에서 시스템 시간 조작 상황의 로깅 기법 영향 연구 필요

5. Acknowledgement

이 연구는 2021년도 정부(과학기술정보통신부)의재원으로 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 구축을통한 자동차 내·외부아티팩트 수집 및 통합 분석기술 개발)

Dankook univ.
Computer Security & OS LAB