



K-Shield Jr.

ANGEL

침해사고대응_3팀

K-Sheild Jr 11기 최종 프로젝트
이원희, 김정완, 윤민철, 최서연, 최시온, 하주현

Contents

01 개요

- 프로젝트 의의
- 주제 요약

03 악성 앱 활동 및 덤프 분석

- 악성 앱 선정 기준
- AhMyth RAT 소개
- 악성 앱 활동 모니터링
- 덤프 데이터 분석

02 셸 스크립트 소개

- 안드로이드 셸 스크립트 설명
- 안드로이드 셸 스크립트 시연

04 결과

- 실제 환경에서 스크립트 활용 가능성
- 시사점

프로젝트 의의

1. 프로젝트 배경

: Window와 Linux에서의 데이터 수집용 자동화 스크립트는 이미 개발되어 있지만, 안드로이드용 데이터 수집 자동화 스크립트는 아직 잘 개발되어 있지 않습니다. 또한 안드로이드는 애플 플랫폼에 비해 실습하기에 더 적합한 환경을 제공하므로 안드로이드를 주제로 선정하게 되었습니다.

2. 프로젝트 목적

: 안드로이드 쉘 스크립트를 작성하여 악성 앱이 설치된 실제 스마트폰에서 데이터 덤프를 얻고, 악성 소프트웨어의 탐지 및 행위를 분석합니다.

프로젝트 의의

기대 효과

1. 안드로이드 시스템의 데이터 수집과 분석에 대한 기초지식 제공
2. 사용자의 안드로이드 데이터 수집의 업무효율성 증진
3. 향후 라이브 포렌식 도구 개발에 활용 가능

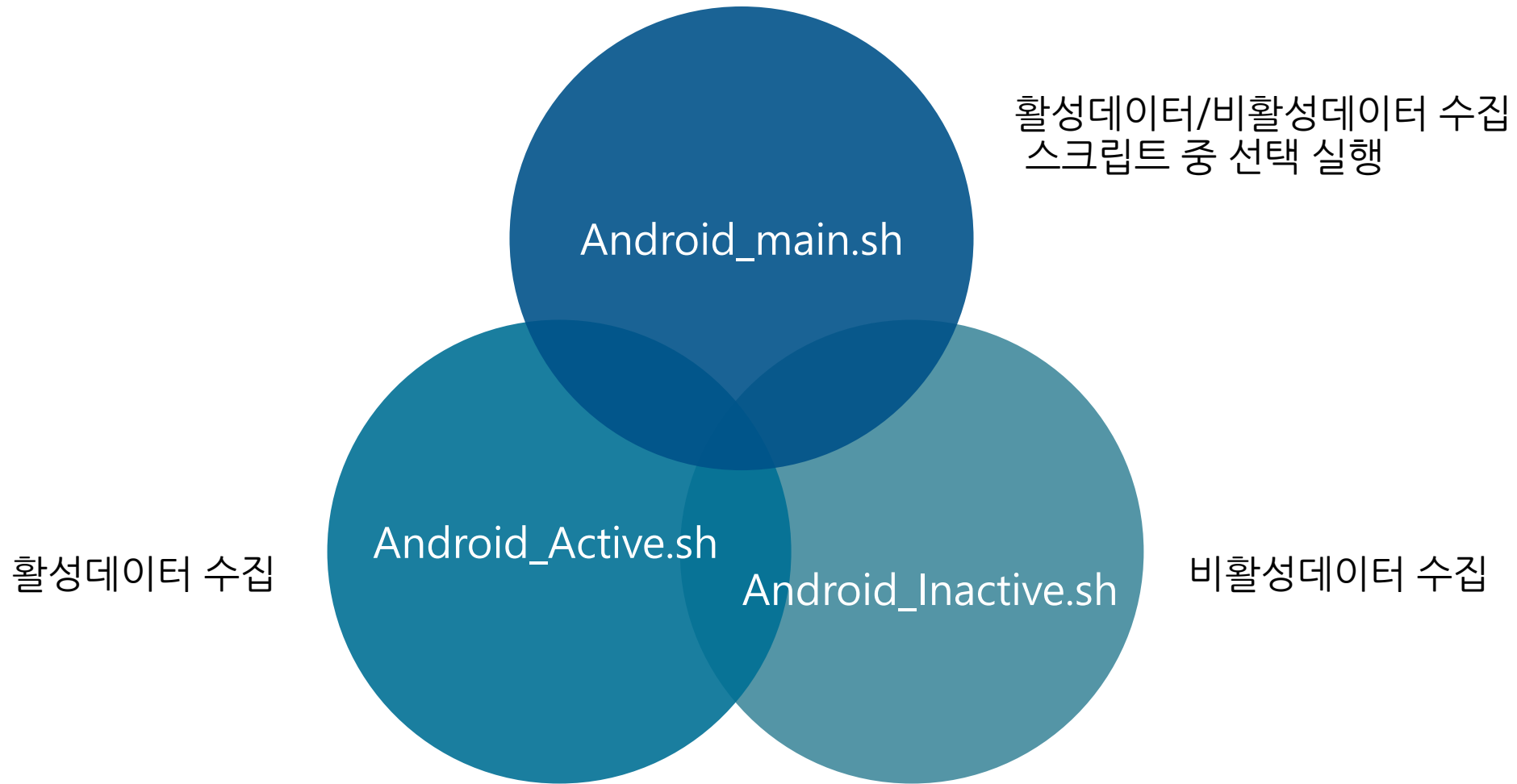
주제 요약

android 

안드로이드 쉘 스크립트를 통한
악성 앱 덤프 및 분석

안드로이드 쉘 스크립트 설명

쉘 스크립트 구성 요소



안드로이드 셸 스크립트 설명

```
beyondx:/data/local/tmp # ./Android_main.sh
```



```
ANGEL MAIN
```

```
Choose an option:
1) Run ./Android_Active.sh
2) Run ./Android_Inactive.sh
3) Run ./Android_Active.sh followed by ./Android_Inactive.sh
4) Exit
3
```

1) Android_main.sh

➤ ./Android_main.sh

활성데이터/비활성데이터 수집 스크립트 중
어느 스크립트를 실행할 지 선택

<- Android_main 스크립트 실행화면



활성 데이터 수집



비활성 데이터 수집

웹 스크립트 시연



악성 앱 선정 기준

- 다양한 악성 행위 확인

악성 앱은 여러 종류의 악성 행위를 수행할 수 있어야 하며,
이는 다양한 정보 수집 셸 스크립트를 통해 해당 앱 관련 악성 행위를 여러 형태로 수집할 수 있어야 합니다.

- 사용자 조작 가능성

악성 앱은 사용자가 직접 해당 앱이 수행할 악성 행위를 다룰 수 있어야 합니다

- 행위 정보의 공개성

해당 악성 앱은 온라인 상에 공개되어 있어야 하며,
이를 통해 사용자가 앱이 어떤 행위를 수행할지 전반적으로 알 수 있어야 합니다.

AhMyth RAT 소개

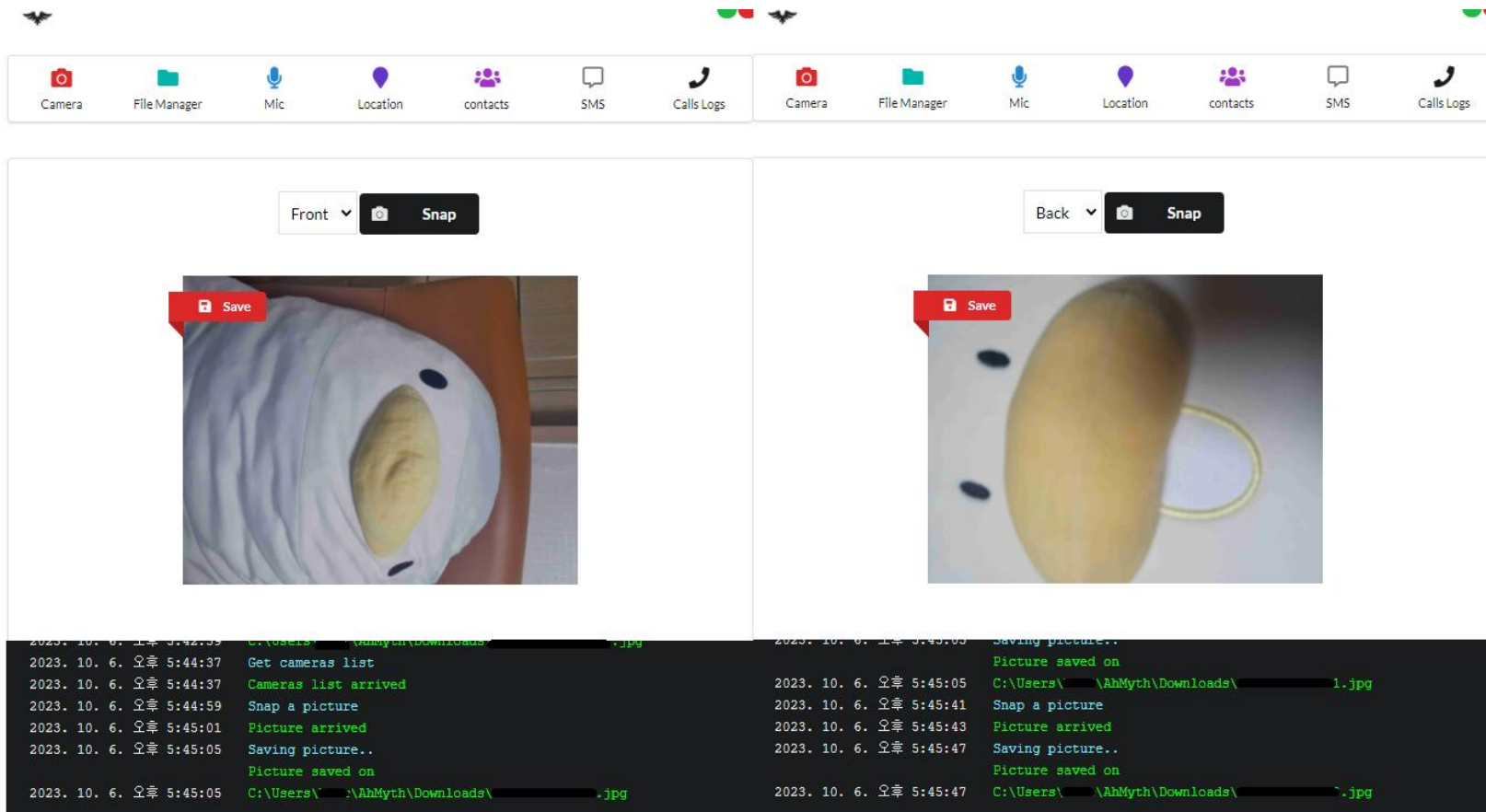
- AhMyth RAT란?

Ahmyth RAT은 Android 사용자를 대상으로 하는 원격 액세스 트로이 목마(RAT)입니다. 이는 트로이 목마에 감염된(가짜) 애플리케이션을 통해 배포됩니다.

- AhMyth RAT은 TCP와 HTTP를 통해 휴대폰과 처음 연결한 후, WebSocket 프로토콜로 전환하여 C&C 서버와의 통신을 유지합니다.
- AhMyth RAT은 카메라 사진 캡처, 디렉토리 리스팅 및 다운로드, 녹음, GPS 위치 추적, 메시지 보내기 및 메시지 리스팅, 전화로그 리스팅, 연락처 리스팅 기능을 포함합니다.

AhMyth RAT 기능 소개 스크립트 실행

1) 카메라 제어



(정면/후면 카메라를 통해 사진을 촬영하고 촬영한 이미지 파일을 저장)

AhMyth RAT 기능 소개 스크립트 실행

1) 카메라 제어

01_cam_front_back.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 5

No.	Time	Source	Destination	Protocol	Length	Info
45	3.705522	52.217.71.92	192.168.0.103	TCP	54	443 → 48388 [ACK] Seq=1 Ack=2 Win=251 Len=0
180	14.115659	192.168.0.103	20.198.118.190	TCP	55	56855 → 443 [ACK] Seq=1 Ack=1 Win=516 Len=1 [TCP segment of a reassembled PDU]
181	14.115674	192.168.0.103	20.198.118.190	TCP	55	[TCP Keep-Alive] 56855 → 443 [ACK] Seq=1 Ack=1 Win=516 Len=1
185	14.229720	20.198.118.190	192.168.0.103	TCP	66	443 → 56855 [ACK] Seq=1 Ack=2 Win=7002 Len=0 SLE=1 SRE=2
218	16.936377	192.168.0.103	192.168.0.118	TCP	97	4444 → 35324 [PSH, ACK] Seq=4 Ack=8 Win=508 Len=43
219	16.936382	192.168.0.103	192.168.0.118	TCP	97	[TCP Retransmission] 4444 → 35324 [PSH, ACK] Seq=4 Ack=8 Win=508 Len=43
223	16.993564	192.168.0.118	192.168.0.103	TCP	54	35324 → 4444 [ACK] Seq=8 Ack=47 Win=87 Len=0
240	18.601758	192.168.0.118	192.168.0.103	TCP	129	35324 → 4444 [PSH, ACK] Seq=8 Ack=47 Win=87 Len=75
241	18.601758	192.168.0.118	192.168.0.103	TCP	1514	35324 → 4444 [ACK] Seq=83 Ack=47 Win=87 Len=1460
242	18.601758	192.168.0.118	192.168.0.103	TCP	1514	35324 → 4444 [ACK] Seq=1543 Ack=47 Win=87 Len=1460

> Frame 218: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface \Device\NPF{...}

> Ethernet II, Src: IntelCor_... (e4:70:b8:5c:3a:00), Dst: 92:64:26:00:00:00 (92:64:26:00:00:00)

> Internet Protocol Version 4, Src: 192.168.0.103, Dst: 192.168.0.118

> Transmission Control Protocol, Src Port: 4444, Dst Port: 35324, Seq: 4, Ack: 8, Len: 43

> Data (43 bytes)

Data: 812934325b226f72646572222c7b226f72646572223a22783030306361222c22657874... [Length: 43]

```

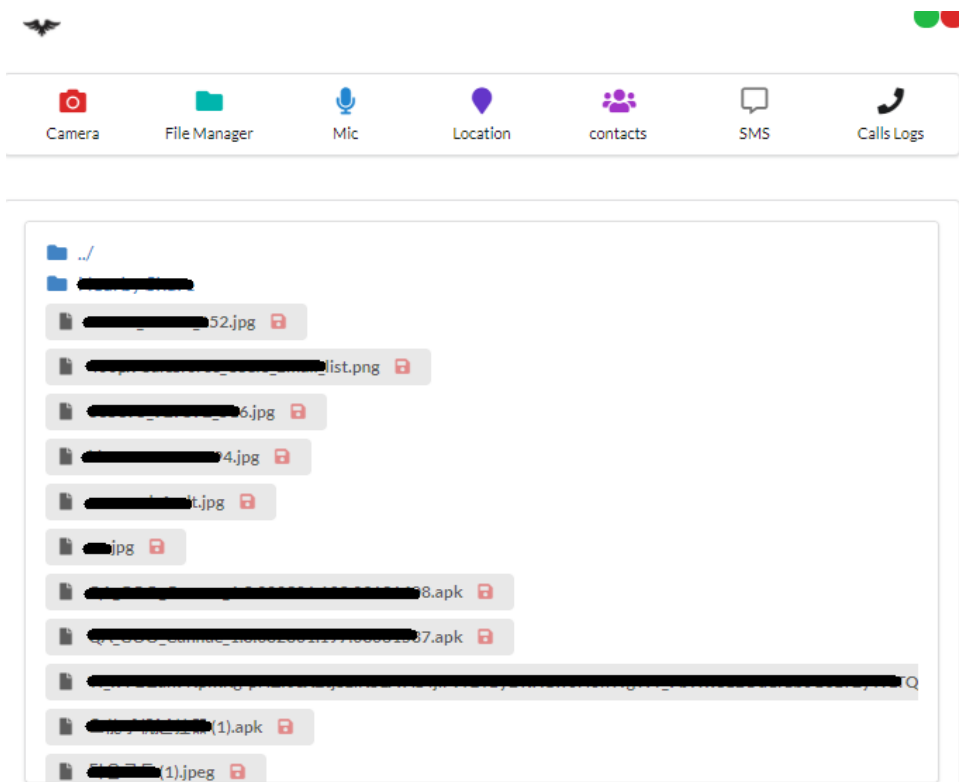
0000  92 64 26 ac 7a c7 e4 70 b8 9e 5a b6 08 00 45 00  ·d&·z·p ··Z···E·
0010  00 53 84 cd 40 00 80 06 f3 a9 c0 a8 00 67 c0 a8  ·S·@··· ····g·
0020  00 76 11 5c 89 fc d9 ec 41 4e 8a 2e e8 a1 50 18  ·v·\··· AN···P·
0030  01 fc 9c 47 00 00 81 29 34 32 5b 22 6f 72 64 65  ··G···) 42["orde
0040  72 22 2c 7b 22 6f 72 64 65 72 22 3a 22 78 30 30  r",{"ord er":"x00
0050  30 30 63 61 22 2c 22 65 78 74 72 61 22 3a 31 7d  00ca","e xtra":1}
0060  5d
  
```

Length (data.len) | Packets: 1445 · Displayed: 296 (20.5%) | Profile: Default

(C&C 서버에서 카메라 리스팅 명령 전달)

AhMyth RAT 기능 소개 스크립트 실행

2) 디렉토리 리스팅 및 다운로드



```
2023. 10. 6. 오후 5:42:33 Saving file..  
2023. 10. 6. 오후 5:42:33 File saved on C:\Users\...\AhMyth\Downloads\..._52.jpeg  
Downloading  
2023. 10. 6. 오후 5:42:39 //storage/emulated/0/Download/..._52.jpg  
2023. 10. 6. 오후 5:42:39 Saving file..  
2023. 10. 6. 오후 5:42:39 File saved on  
2023. 10. 6. 오후 5:42:39 C:\Users\...\AhMyth\Downloads\..._52.jpg
```

(Victim 기기의 디렉토리를 리스팅 및 다운로드)

AhMyth RAT 기능 소개 스크립트 실행

2) 디렉토리 리스팅 및 다운로드

No.	Time	Source	Destination	Protocol	Length	Info
10	0.163104	192.168.0.103	51.104.162.168	TCP	54	48383 → 443 [FIN, ACK] Seq=1 Ack=1 Win=514 Len=0
11	0.163113	192.168.0.103	51.104.162.168	TCP	54	[TCP Retransmission] 48383 → 443 [FIN, ACK] Seq=1 Ack=1 Win=514 Len=0
18	0.454705	51.104.162.168	192.168.0.103	TCP	54	443 → 48383 [FIN, ACK] Seq=1 Ack=2 Win=2048 Len=0
19	0.454749	192.168.0.103	51.104.162.168	TCP	54	48383 → 443 [ACK] Seq=2 Ack=2 Win=514 Len=0
20	0.454753	192.168.0.103	51.104.162.168	TCP	54	[TCP Dup ACK 19#1] 48383 → 443 [ACK] Seq=2 Ack=2 Win=514 Len=0
63	2.657147	192.168.0.103	192.168.0.118	TCP	130	4444 → 35324 [PSH, ACK] Seq=1 Ack=1 Win=511 Len=76
64	2.657153	192.168.0.103	192.168.0.118	TCP	130	[TCP Retransmission] 4444 → 35324 [PSH, ACK] Seq=1 Ack=1 Win=511 Len=76
67	2.702339	192.168.0.118	192.168.0.103	TCP	54	35324 → 4444 [ACK] Seq=1 Ack=77 Win=87 Len=0
69	2.719914	192.168.0.118	192.168.0.103	TCP	1514	35324 → 4444 [ACK] Seq=1 Ack=77 Win=87 Len=1460
70	2.719914	192.168.0.118	192.168.0.103	TCP	386	35324 → 4444 [PSH, ACK] Seq=1461 Ack=77 Win=87 Len=332

> Frame 63: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits) on interface \Dev

> Ethernet II, Src: IntelCor_ (e4:70:b8:), Dst: 92:64:26: (92:64:26:)

> Internet Protocol Version 4, Src: 192.168.0.103, Dst: 192.168.0.118

> Transmission Control Protocol, Src Port: 4444, Dst Port: 35324, Seq: 1, Ack: 1, Len: 76

> Data (76 bytes)

```

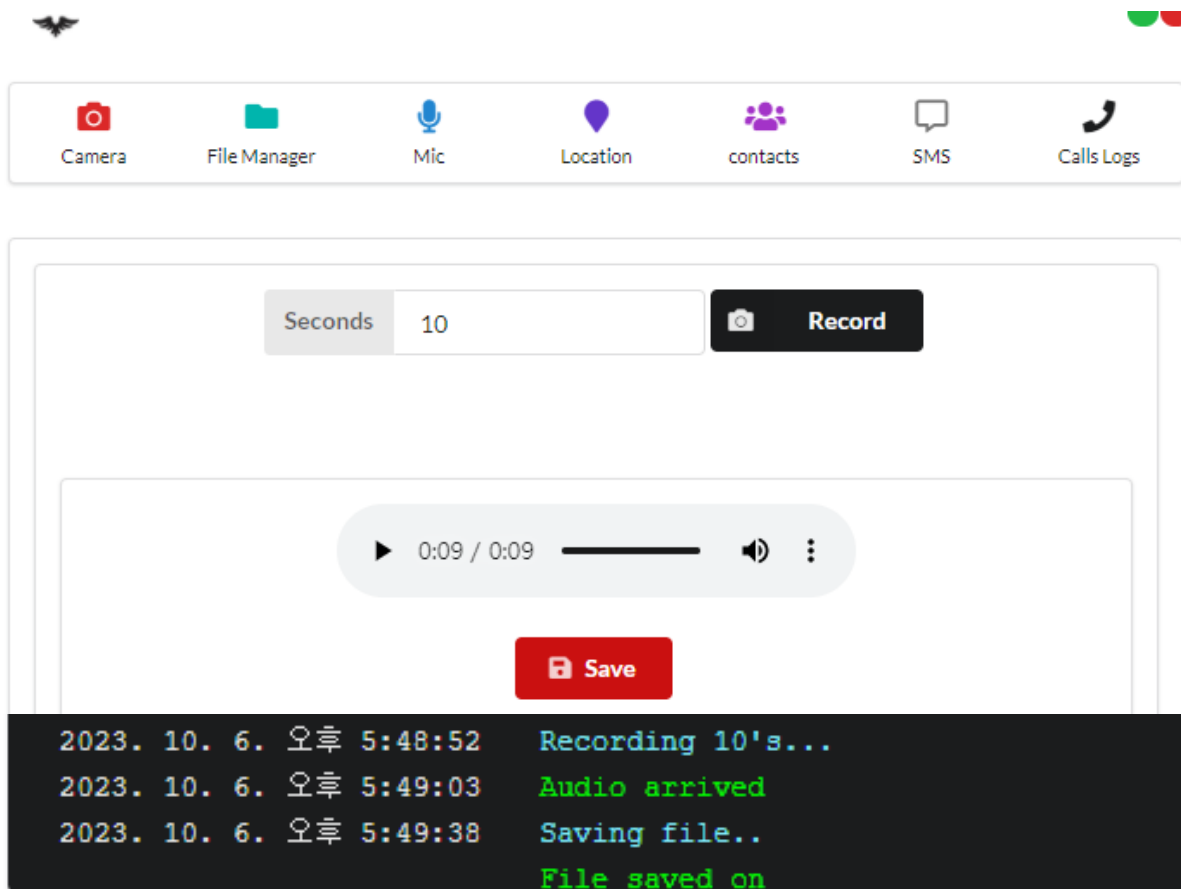
0000  92 64 26 ac 7a c7 e4 70 b8 9e 5a b6 08 00 45 00  .d&·z··p ··Z··E·
0010  00 74 84 12 40 00 80 06 f4 43 c0 a8 00 67 c0 a8  ·t··@··· ·C··g·
0020  00 76 11 5c 89 fc d9 ec 3f 98 8a 2c 0e 9f 50 18  ·v·\···· ?···P·
0030  01 ff f1 6a 00 00 81 4a 34 32 5b 22 6f 72 64 65  ···j···J 42["orde
0040  72 22 2c 7b 22 6f 72 64 65 72 22 3a 22 78 30 30  r",{"ord er":"x00
0050  30 30 66 6d 22 2c 22 65 78 74 72 61 22 3a 22 6c  00fm","e xtra":"l
0060  73 22 2c 22 70 61 74 68 22 3a 22 2f 73 74 6f 72  s","path ":"/stor
0070  61 67 65 2f 65 6d 75 6c 61 74 65 64 2f 30 2f 22  age/emul ated/0/"
0080  7d 5d  }]
  
```

02_directory_listing.pcapng | Packets: 524 · Displayed: 216 (41,2%) | Profile: Default

(디렉토리 리스팅 확인)

AhMyth RAT 기능 소개 스크립트 실행

3) 녹화



(10초를 지정하여 그 시간만 녹화를 수행)



(녹화 활성화시 화면 변화)

AhMyth RAT 기능 소개 스크립트 실행

3) 녹화

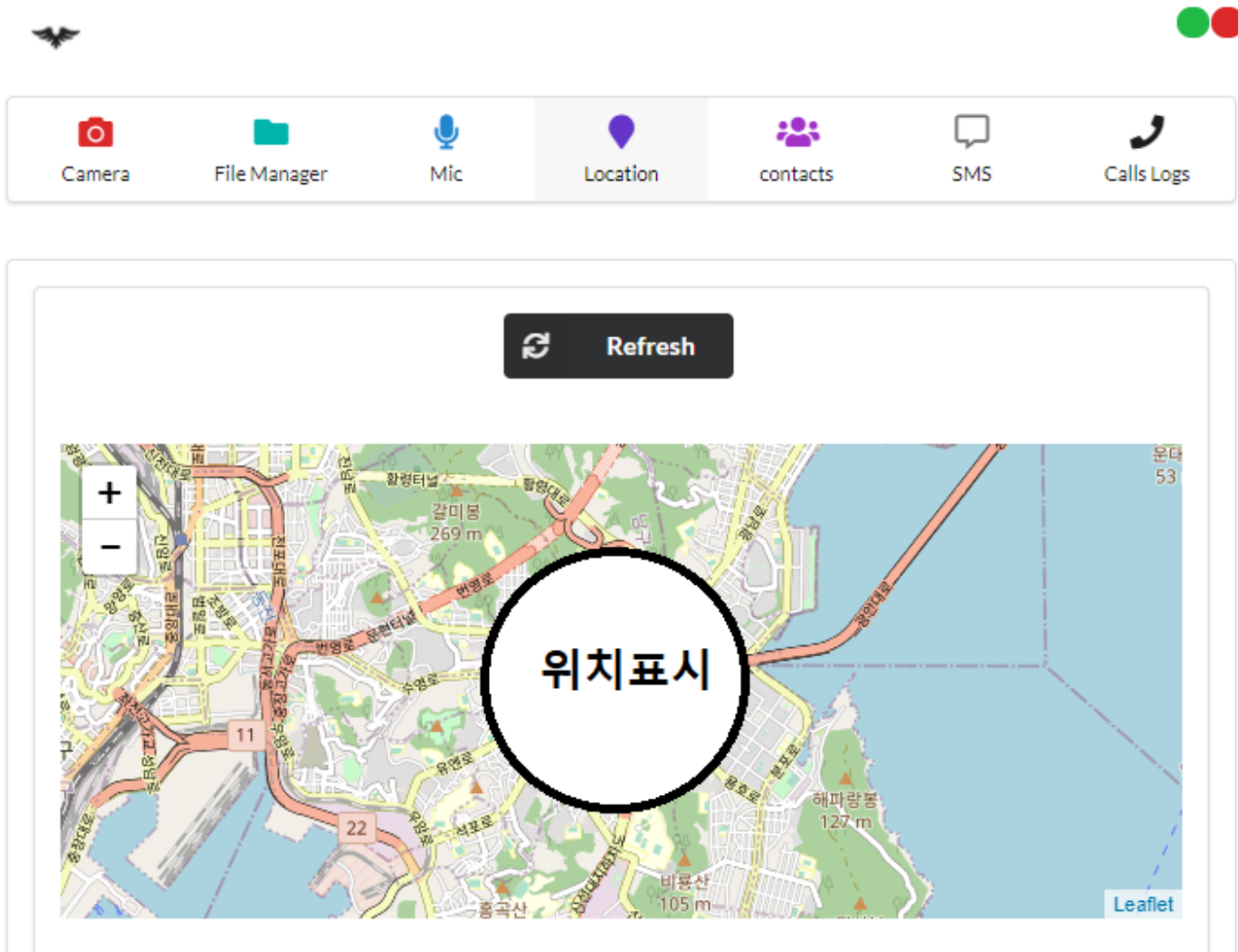
No.	Time	Source	Destination	Protocol	Length	Info
180	12.752446	192.168.0.103	192.168.0.118	TCP	98	4444 → 35324 [PSH, ACK] Seq=1 Ack=1 Win=1026 Len=44
181	12.752452	192.168.0.103	192.168.0.118	TCP	98	[TCP Retransmission] 4444 → 35324 [PSH, ACK] Seq=1 Ack=1 Win=1026 Len=44
182	12.761205	192.168.0.118	192.168.0.103	TCP	61	35324 → 4444 [PSH, ACK] Seq=1 Ack=1 Win=87 Len=7
183	12.761727	192.168.0.103	192.168.0.118	TCP	57	4444 → 35324 [PSH, ACK] Seq=45 Ack=8 Win=1026 Len=3
184	12.761734	192.168.0.103	192.168.0.118	TCP	57	[TCP Retransmission] 4444 → 35324 [PSH, ACK] Seq=45 Ack=8 Win=1026 Len=3
185	12.763599	192.168.0.118	192.168.0.103	TCP	54	35324 → 4444 [ACK] Seq=8 Ack=45 Win=87 Len=0
186	12.764574	192.168.0.118	192.168.0.103	TCP	54	35324 → 4444 [ACK] Seq=8 Ack=48 Win=87 Len=0
315	23.058657	192.168.0.118	192.168.0.103	TCP	166	35324 → 4444 [PSH, ACK] Seq=8 Ack=48 Win=87 Len=112
316	23.058657	192.168.0.118	192.168.0.103	TCP	1514	35324 → 4444 [ACK] Seq=120 Ack=48 Win=87 Len=1460
317	23.058657	192.168.0.118	192.168.0.103	TCP	1514	35324 → 4444 [ACK] Seq=1580 Ack=48 Win=87 Len=1460

> Frame 180: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface \Device\NPF{...}	0000	92 64 26 ac 7a c7 e4 70 b8 9e 5a b6 08 00 45 00	.d&·z·p ··Z···E·
> Ethernet II, Src: IntelCor_9e:5a:b6 (e4:70:b8:9e:5a:b6), Dst: 92:64:26:ac:7a:c7 (92:64:26:ac:7a:c7)	0010	00 54 85 f1 40 00 80 06 f2 84 c0 a8 00 67 c0 a8	·T··@·... ·····g··
> Internet Protocol Version 4, Src: 192.168.0.103, Dst: 192.168.0.118	0020	00 76 11 5c 89 fc d9 ec 42 17 8a 32 66 c7 50 18	·v·\·... B··2f·P·
> Transmission Control Protocol, Src Port: 4444, Dst Port: 35324, Seq: 1, Ack: 1, Len: 44	0030	04 02 55 7c 00 00 81 2a 34 32 5b 22 6f 72 64 65	··U ·...* 42["orde
> Data (44 bytes)	0040	72 22 2c 7b 22 6f 72 64 65 72 22 3a 22 78 30 30	r",{"ord er":"x00
	0050	30 30 6d 63 22 2c 22 73 65 63 22 3a 22 31 30 22	00mc","s ec":"10"
	0060	7d 5d	}]

(녹화 확인)

AhMyth RAT 기능 소개 스크립트 실행

4) GPS 위치 추적



The image displays the AhMyth RAT interface. At the top, there is a navigation bar with icons for Camera, File Manager, Mic, Location (highlighted), contacts, SMS, and Calls Logs. Below this, a map is shown with a large white circle in the center containing the text "위치표시" (Location Mark). A "Refresh" button is located above the map. The map shows a street view with various landmarks and elevation markers.

```
2023. 10. 7. 오후 9:51:05 Get Location..  
2023. 10. 7. 오후 9:51:05 Location arrived => 05-10-101, 123-0000-101  
2023. 10. 7. 오후 9:51:06 Get Location..  
2023. 10. 7. 오후 9:51:06 Location arrived => 05-10-101, 123-0000-101  
2023. 10. 7. 오후 9:51:06 Get Location..  
2023. 10. 7. 오후 9:51:06 Location arrived => 05-10-101, 123-0000-101
```

AhMyth RAT 기능 소개 스크립트 실행

4) GPS 위치 추적

No.	Time	Source	Destination	Protocol	Length	Info
12	1.152114	172.65.229.194	192.168.0.103	TCP	60	443 → 48403 [ACK] Seq=1 Ack=1 Win=8 Len=0
13	1.152170	192.168.0.103	172.65.229.194	TCP	54	[TCP ACKed unseen segment] 48403 → 443 [ACK] Seq=1 Ack=2 Win=510 Len=0
14	1.152176	192.168.0.103	172.65.229.194	TCP	54	[TCP Dup ACK 13#1] 48403 → 443 [ACK] Seq=1 Ack=2 Win=510 Len=0
25	2.343641	192.168.0.103	192.168.0.118	TCP	87	4444 → 35324 [PSH, ACK] Seq=1 Ack=1 Win=1026 Len=33
26	2.343647	192.168.0.103	192.168.0.118	TCP	87	[TCP Retransmission] 4444 → 35324 [PSH, ACK] Seq=1 Ack=1 Win=1026 Len=33
27	2.361285	192.168.0.103	146.75.49.91	HTTP	456	GET /13/4094/2723.png HTTP/1.1
28	2.361292	192.168.0.103	146.75.49.91	TCP	456	[TCP Retransmission] 48406 → 80 [PSH, ACK] Seq=1 Ack=1 Win=515 Len=402
29	2.361891	192.168.0.103	146.75.49.91	HTTP	456	GET /13/4093/2724.png HTTP/1.1
30	2.361895	192.168.0.103	146.75.49.91	TCP	456	[TCP Retransmission] 48407 → 80 [PSH, ACK] Seq=1 Ack=1 Win=515 Len=402
31	2.362070	192.168.0.103	146.75.49.91	HTTP	456	GET /13/4094/2724.png HTTP/1.1

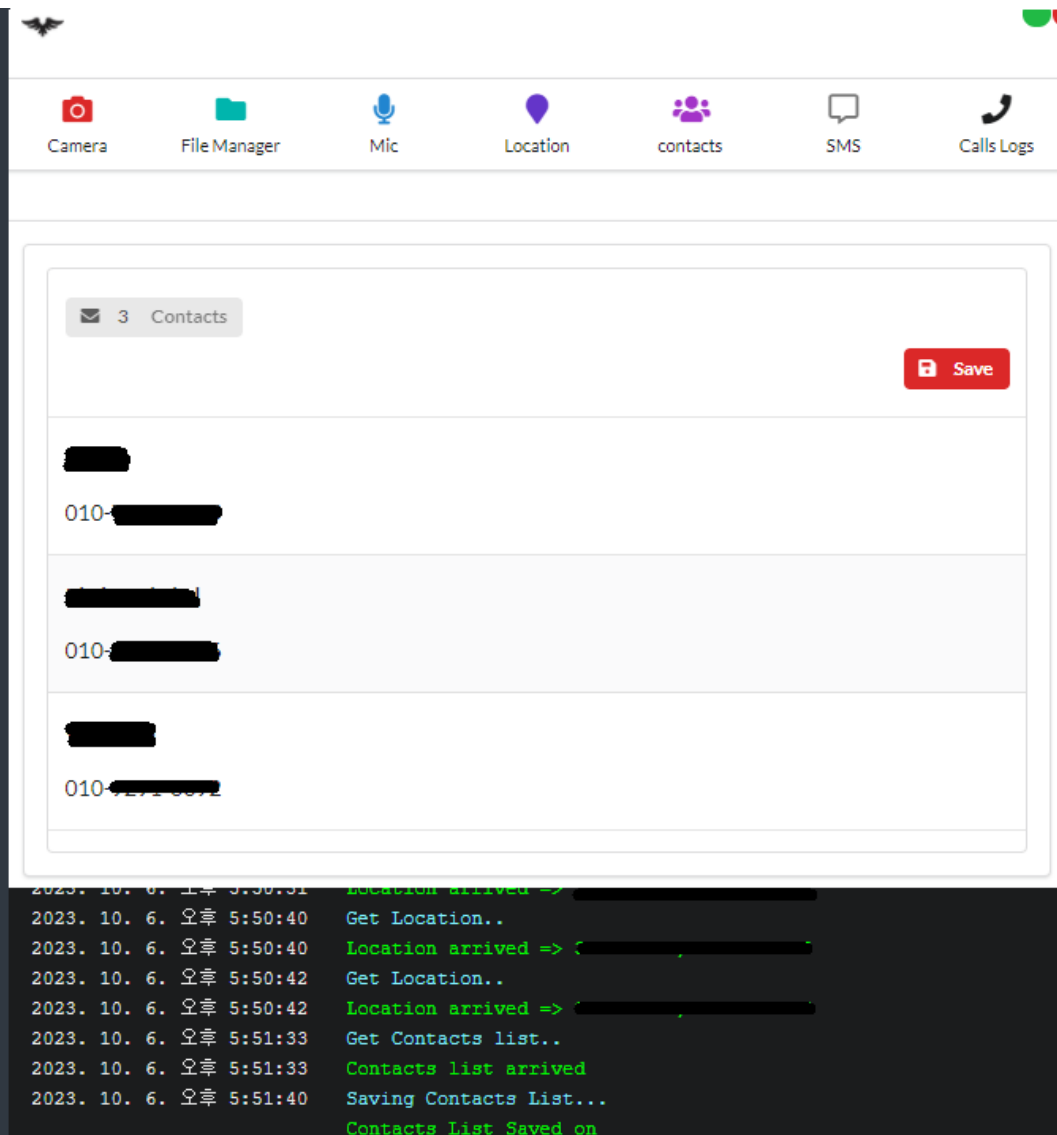
> Frame 25: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface \Device\NPF{...}	0000	92 64 26 ac 7a c7 e4 70 b8 9e 5a b6 08 00 45 00	·d&·z··p ··Z···E·
> Ethernet II, Src: IntelCor_9e:5a:b6 (e4:70:b8:████████), Dst: 92:64:26:████████ (92:64:26:████████)	0010	00 49 86 61 40 00 80 06 f2 1f c0 a8 00 67 c0 a8	·I·a@··· ····g··
> Internet Protocol Version 4, Src: 192.168.0.103, Dst: 192.168.0.118	0020	00 76 11 5c 89 fc d9 ec 42 73 8a 32 a6 bb 50 18	·v·\···· Bs·2··P·
> Transmission Control Protocol, Src Port: 4444, Dst Port: 35324, Seq: 1, Ack: 1, Len: 33	0030	04 02 32 a8 00 00 81 1f 34 32 5b 22 6f 72 64 65	··2····· 42["orde
✓ Data (33 bytes)	0040	72 22 2c 7b 22 6f 72 64 65 72 22 3a 22 78 30 30	n",{"ord er":"x00
Data: 811f34325b226f72646572222c7b226f72646572223a22783030306c6d227d5d	0050	30 30 6c 6d 22 7d 5d	001m"}]
[Length: 33]			

(GPS 위치 추적 확인)

AhMyth RAT 기능 소개 스크립트 실행

5) 연락처

```
243 -Contacts-
244
245 12987813 ->
246
247 display_name
248 data1
249 ContactsCursor
250 010-██████████
251 phoneNo
252 010-██████████
253 010-██████████
254 #3McontactsList
255 writing packet
256 2896687
257 ██████████
258 2896687
259 writing packet ██████████
260 2896687
261 encoding packet
262 2896687
263 b.a.h.b
264 2896687
265 encoding packet b.a.h.b
266 2896687
267 encoded
268 2896687
269 b.a.h.b
270 2896687
271 flushing
272 packets in socket
273 flushing 1 packets in socket
274 x0000cn
275 contactsList
276 phoneNo
277 010-██████████
278 phoneNo
279 010-██████████
280 phoneNo
281 010-██████████
```



AhMyth RAT 기능 소개 스크립트 실행

6) SMS

The screenshot displays the AhMyth RAT interface, specifically the SMS functionality. The left pane shows a list of SMS messages, with the first message having a redacted body. The right pane shows the 'SMS List' tab, which includes a 'Send SMS' button and a 'SMS List' button. Below the buttons, there are two message entries, each with a phone number and a redacted body. The bottom pane shows a terminal window with log output for saving contacts and SMS lists.

```
5020003 86[REDACTED]
5020004 58[REDACTED]
5020005 2.38%
5020006 [REDACTED].com/s
5020007 95559
5020008 [REDACTED]
5020009 com.samsung.android.messaging
5020010 [REDACTED]
5020011 [REDACTED]
5020012 [REDACTED]
5020013 C:/[REDACTED]
5020014 [REDACTED]
5020015 [REDACTED]
5020016 com.samsung.android.messaging
5020017 [REDACTED]
5020018 a6b663b2f0a253fd
5020019 [REDACTED]
5020020 [REDACTED]
5020021 MU5042
5020022 [REDACTED]
5020023 01com.samsung.android.messaging
5020024 [REDACTED]
5020025 [REDACTED]
5020026 [REDACTED]
5020027 [REDACTED]
5020028 [REDACTED]
5020029 com.samsung.android.messaging
5020030 [REDACTED]
5020031 [REDACTED]
5020032 8610001
5020033 [REDACTED]
5020034 com.samsung.android.messaging
5020035 [REDACTED]
5020036 [REDACTED]
5020037 [REDACTED]
5020038 http://[REDACTED]
5020039 [REDACTED]
5020040 com.samsung.android.messaging
5020041 [REDACTED]
5020042 70[REDACTED]
```

Camera File Manager Mic Location contacts SMS Calls Logs

Send SMS SMS List

146 Messages

+86[REDACTED]

[REDACTED]

+86[REDACTED]

[REDACTED]

```
2023. 10. 6. 오후 5:51:40 Saving Contacts List...
2023. 10. 6. 오후 5:51:40 Contacts List Saved on
2023. 10. 6. 오후 5:53:11 C:\Users\[REDACTED]\AhMyth\Downloads\Contacts_[REDACTED].csv
2023. 10. 6. 오후 5:53:11 Get SMS list..
2023. 10. 6. 오후 5:53:11 SMS list arrived
2023. 10. 6. 오후 5:53:26 Saving SMS List...
2023. 10. 6. 오후 5:53:26 SMS List Saved on
2023. 10. 6. 오후 5:53:26 C:\Users\[REDACTED]\AhMyth\Downloads\SMS_[REDACTED].csv
```

AhMyth RAT 기능 소개 스크립트 실행

7) 통화 기록

```
6369115 callsList
6369116 phoneNo
6369117 18[REDACTED]
6369118 duration
6369119 phoneNo
6369120 02[REDACTED]
6369121 duration
6369122 phoneNo
6369123 010[REDACTED]
6369124 duration
6369125 phoneNo
6369126 006[REDACTED]
6369127 duration
6369128 phoneNo
6369129 009[REDACTED]
6369130 duration
6369131 phoneNo
6369132 009[REDACTED]
6369133 duration
6369134 encoded [REDACTED]
6369135 [REDACTED]
6369136 [REDACTED]
```

Camera File Manager Mic Location contacts SMS Calls Logs

6 Logs

Save

Phone No	Name	Duration	Status
18[REDACTED]	Unknown	0	OUTGOING
02[REDACTED]	Unknown	0	OUTGOING

```
2023. 10. 6. 오후 5:54:46 Get Calls list..
2023. 10. 6. 오후 5:54:46 Calls list arrived
2023. 10. 6. 오후 5:55:09 Saving Calls List...
Calls List Saved on
2023. 10. 6. 오후 5:55:09 C:\Users\[REDACTED]\AhMyth\Downloads\Call_[REDACTED].csv
```

실제 환경에서 스크립트 활용 가능성 > Android_Active

단계	세부항목	가상기기	실기기
1단계	가상메모리	성공	성공
2단계	arp	성공	성공
	netstat	성공	성공
	ifconfig	성공	성공
	wifi	성공	성공
	network_interface	성공	성공
	route	성공	성공
	network properties	성공	성공
	iptables	성공	성공
	sysctl	성공	성공
	tcp 소켓	성공	성공
	udp 소켓	성공	성공

실제 환경에서 스크립트 활용 가능성 > Android_Active

단계	세부항목	가상기기	실기기
3단계	top	성공	성공
	ps	성공	성공
	ls -l	성공	성공
	activity process	성공	성공
	meminfo	성공	성공
	strace	성공	실패
4단계	연락처	성공	성공
	DCIM	성공	성공
	앱 데이터	성공	성공
5단계	장치 정보	성공	성공
	cpu 정보	성공	성공
	메모리 & 배터리 정보	성공	성공
6단계	자동실행 항목 덤프	성공	성공
7단계	클립 보드 덤프	성공	성공

실제 환경에서 스크립트 활용 가능성 > Android_Inactive

단계	세부항목	가상기기	실기기
1단계	파일시스템 메타데이터	성공	성공
2단계	모든 계정 정보	성공	성공
	Activity 상태 확인	성공	성공
	최근 activity 상태 확인	성공	성공
	설치된 앱 리스트	성공	성공
	설치된 앱 상세 정보	성공	성공
	CPU 프로세서 정보	성공	성공
3단계	이벤트 로그	성공	성공
	작업 예약 관리	성공	성공
4단계	trash	성공	성공
	.Trash	성공	성공
	lost+found	성공	성공

실제 환경에서 스크립트 활용 가능성 > Android_Inactive

단계	세부항목	가상기기	실기기
5단계	chrome	성공	성공
	firefox	성공	성공
	opera	성공	성공
	whale	성공	성공
	tor	성공	성공
	vivaldi	성공	성공
6단계	cache	성공	성공
	LocalTmp	성공	성공
7단계	blkid	성공	성공
	logcat	성공	성공

“ *Total : 48/49 = 97%* ”

시사점

- 안드로이드 가상머신에서 실행한 쉘 스크립트를
실제 악성 앱에 감염된 스마트폰에 실행했을 때, 97%의 결과물을 얻음
- 안드로이드 시스템의 기본 정보를 수집하고 분석하는 이 과정을 통해,
쉘 스크립트에 대한 이해도를 높임
안드로이드 시스템의 구성 환경 이해
또한, 침해사고 발생 시 필요한 접근 방식에 대한 시야를 확장
- 향후 쉘 스크립트가 실제 안드로이드 포렌식으로 활용될 수 있도록 각 생성된 데이터에
대한 타임스탬프 및 해시값을 생성하는 기능을 추가
네트워크 상에서 원격으로 수집될 수 있도록 기능을 확장하고자 함

감사합니다