Digital evidence requires a C.A.

Byungkil Lee a.k.a. Nullhat

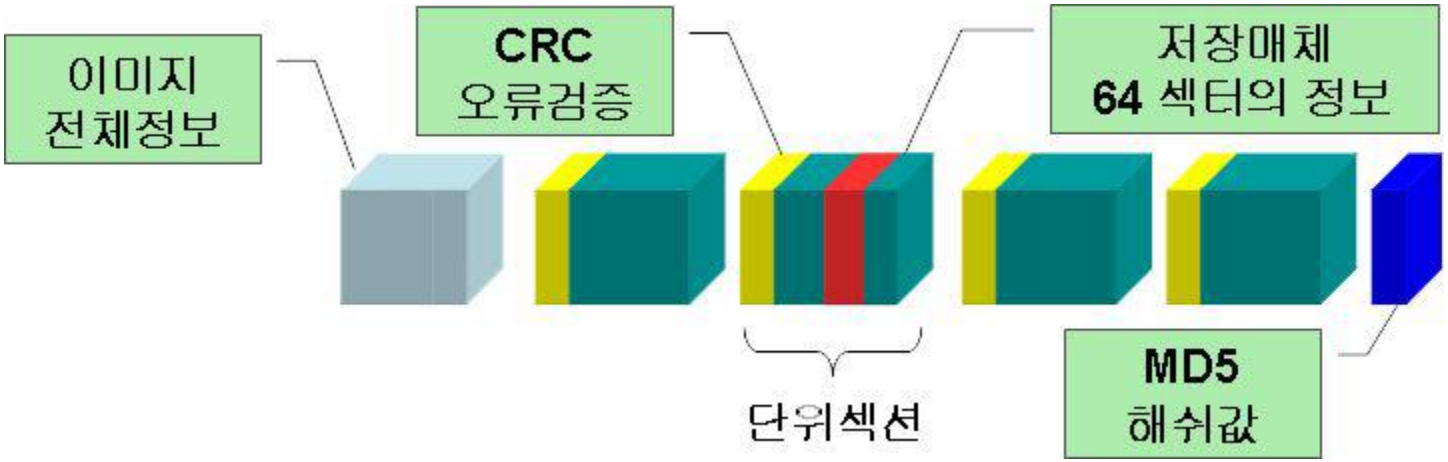
nullhat@gmail.com

목차

1. 목적

- 인증기관을 이용하여 디지털 증거에 대한 기밀성, 무결성, 진정성 확보하면서 증거능력을 부여하기 위한 방안을 제시하고 소프트웨어로 구현
- 디지털 증거수집과 인증기관과의 표준 통신 규약을 제안
- 자유롭고 안전한 디지털 증거 수집 기반 확보

1. 필요성

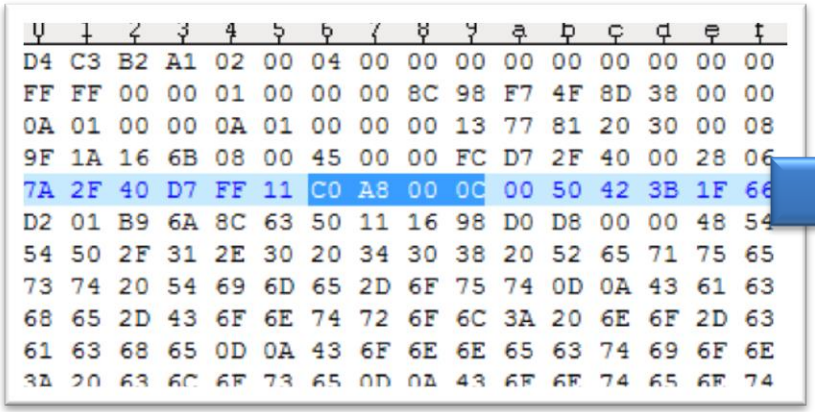


참조 : 한국형사정책연구원 연구총서 06-21
디지털 증거분석도구에 의한 증거수집절차 및 증거능력확보방안 P.145

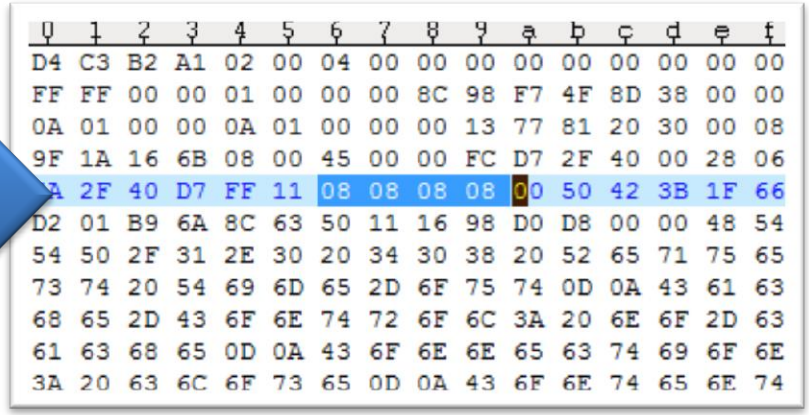
2. 필요성

가상 사례) 피해자 OO주식회사는 20XX. XX. XX. 22:20경부터 같은날 23:20경까지 서비스 거부공격을 받았으며, 이를 경찰청 사이버테러대응센터에 신고하며 피해 진술 중 공격을 받은 사실을 입증하기 위하여 MRTG 그래프와 DDoS방어장비의 기록, 당시 패킷을 pcap의 형태로 수집하여 저장한 파일을 임의 제출하였다. 이후, 수사관은 공격패킷이 저장된 pcap 파일에서 공격자의 IP주소를 확인한 뒤 가입자 정보를 파악하고 좀비컴퓨터를 확보 후 좀비를 제어하는 공격자를 찾아 검거하였다.

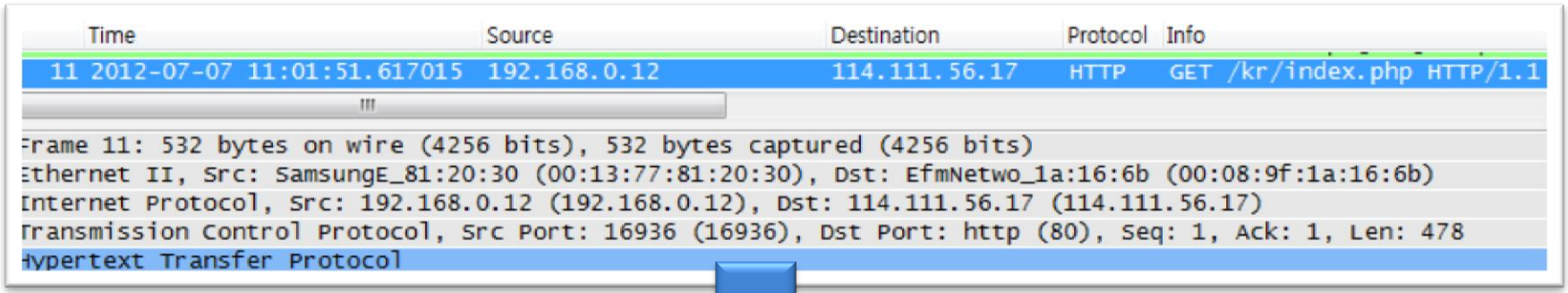
목적과 필요성



0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
D4	C3	B2	A1	02	00	04	00	00	00	00	00	00	00	00	00
FF	FF	00	00	01	00	00	00	8C	98	F7	4F	8D	38	00	00
0A	01	00	00	0A	01	00	00	00	13	77	81	20	30	00	08
9F	1A	16	6B	08	00	45	00	00	FC	D7	2F	40	00	28	06
7A	2F	40	D7	FF	11	C0	A8	00	0C	00	50	42	3B	1F	66
D2	01	B9	6A	8C	63	50	11	16	98	D0	D8	00	00	48	54
54	50	2F	31	2E	30	20	34	30	38	20	52	65	71	75	65
73	74	20	54	69	6D	65	2D	6F	75	74	0D	0A	43	61	63
68	65	2D	43	6F	6E	74	72	6F	6C	3A	20	6E	6F	2D	63
61	63	68	65	0D	0A	43	6F	6E	6E	65	63	74	69	6F	6E
3A	20	63	6C	6F	73	65	0D	0A	43	6F	6E	74	65	6E	74

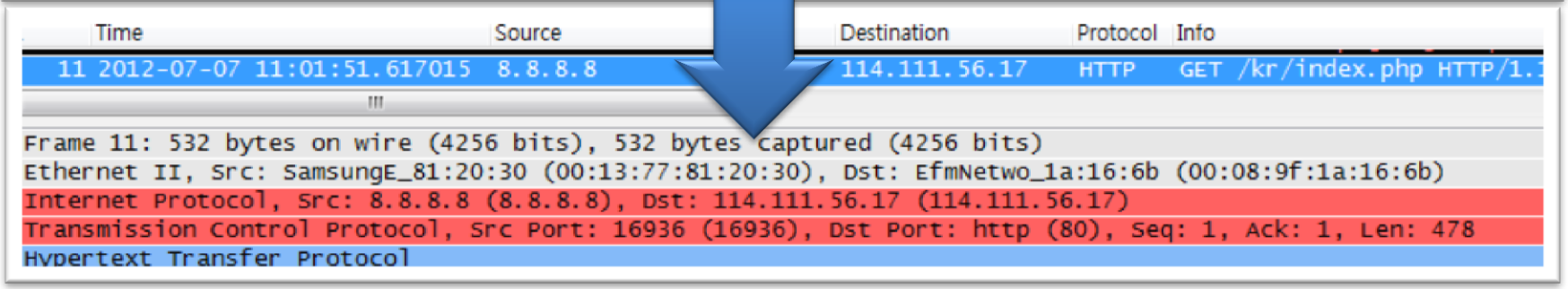


0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
D4	C3	B2	A1	02	00	04	00	00	00	00	00	00	00	00	00
FF	FF	00	00	01	00	00	00	8C	98	F7	4F	8D	38	00	00
0A	01	00	00	0A	01	00	00	00	13	77	81	20	30	00	08
9F	1A	16	6B	08	00	45	00	00	FC	D7	2F	40	00	28	06
A	2F	40	D7	FF	11	08	08	08	08	00	50	42	3B	1F	66
D2	01	B9	6A	8C	63	50	11	16	98	D0	D8	00	00	48	54
54	50	2F	31	2E	30	20	34	30	38	20	52	65	71	75	65
73	74	20	54	69	6D	65	2D	6F	75	74	0D	0A	43	61	63
68	65	2D	43	6F	6E	74	72	6F	6C	3A	20	6E	6F	2D	63
61	63	68	65	0D	0A	43	6F	6E	6E	65	63	74	69	6F	6E
3A	20	63	6C	6F	73	65	0D	0A	43	6F	6E	74	65	6E	74



Time	Source	Destination	Protocol	Info
11 2012-07-07 11:01:51.617015	192.168.0.12	114.111.56.17	HTTP	GET /kr/index.php HTTP/1.1

```
Frame 11: 532 bytes on wire (4256 bits), 532 bytes captured (4256 bits)
Ethernet II, Src: SamsungE_81:20:30 (00:13:77:81:20:30), Dst: EfmNetwo_1a:16:6b (00:08:9f:1a:16:6b)
Internet Protocol, Src: 192.168.0.12 (192.168.0.12), Dst: 114.111.56.17 (114.111.56.17)
Transmission Control Protocol, Src Port: 16936 (16936), Dst Port: http (80), Seq: 1, Ack: 1, Len: 478
Hypertext Transfer Protocol
```



Time	Source	Destination	Protocol	Info
11 2012-07-07 11:01:51.617015	8.8.8.8	114.111.56.17	HTTP	GET /kr/index.php HTTP/1.1

```
Frame 11: 532 bytes on wire (4256 bits), 532 bytes captured (4256 bits)
Ethernet II, Src: SamsungE_81:20:30 (00:13:77:81:20:30), Dst: EfmNetwo_1a:16:6b (00:08:9f:1a:16:6b)
Internet Protocol, Src: 8.8.8.8 (8.8.8.8), Dst: 114.111.56.17 (114.111.56.17)
Transmission Control Protocol, Src Port: 16936 (16936), Dst Port: http (80), Seq: 1, Ack: 1, Len: 478
Hypertext Transfer Protocol
```

1. **기밀성**

   디지털 증거를 수집하는 **수행자**가 지정한 비밀번호로 채증 파일 암호화

2. **무결성**

   디지털 증거 수집 중 모든 디지털 정보는 암호학적 해쉬값을 계속하여 갱신하고, 완료시 **참관자**가 전자서명

3. **진정성**

   전자서명과 인증기관으로 해쉬값의 유효성 검증

※ 수행자와 참관자란?
수행자는 디지털증거의 수집자이며, 참관자는 수집 과정을 현장 또는 원격에서 참관한다.
따라서, 참관자 없이 수행자 단독으로 수집하는 행위를 방지하기 위해 인증기관이 필요!

디지털 증거의 정의
증거로서의 가치가 있는 디지털 형태로 저장되어 있거나, 전송 중인 정보

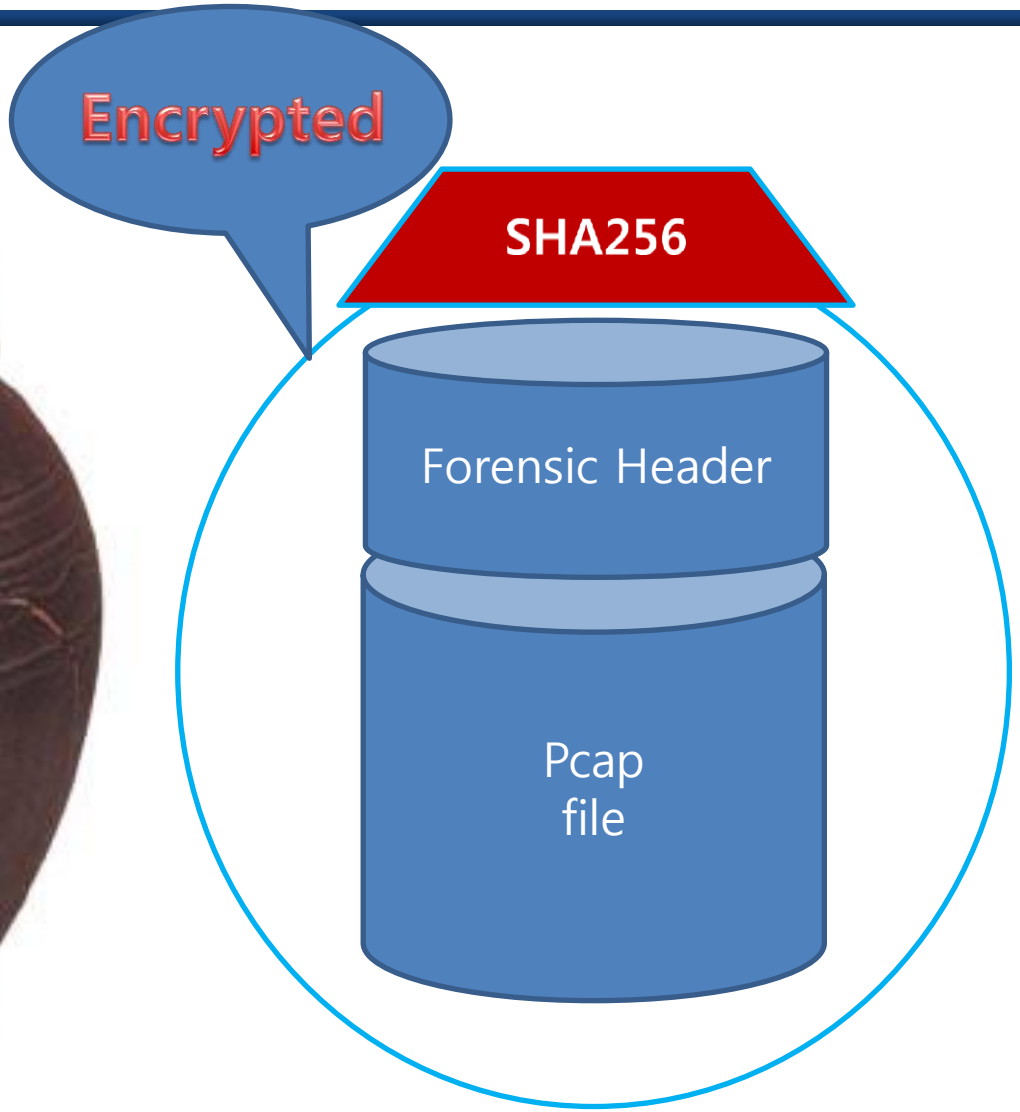
- 하드디스크등 물리적 저장매체는 디지털 증거로서의 채증 절차, 분석, 이동, 무결성 유지등에 대한 연구가 활발한 반면,

- 전기통신의 감청은 법률에서 그 이유가 분명하고 집행 조건에 부합할 경우 허가를 하며 집행절차에 있어서도 엄격함에도 불구하고,

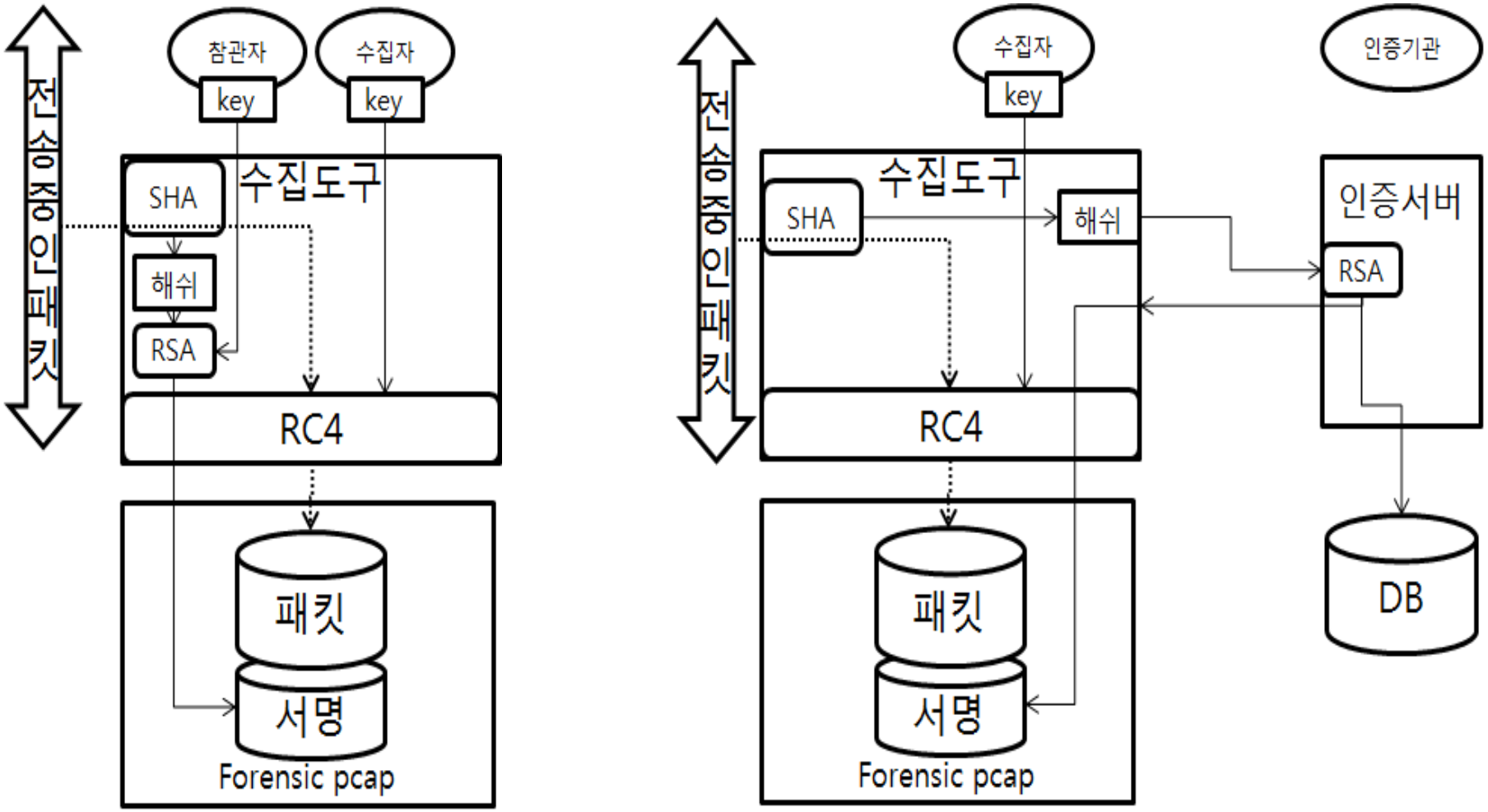
- 디지털 통신의 감청 절차의 부재로 디지털 증거능력이 공격받을 수 있다.

∴ **전송중인 디지털 정보에 대한 인증기관 연동한 채증 절차를 구현**

설계



설계 (개요도)

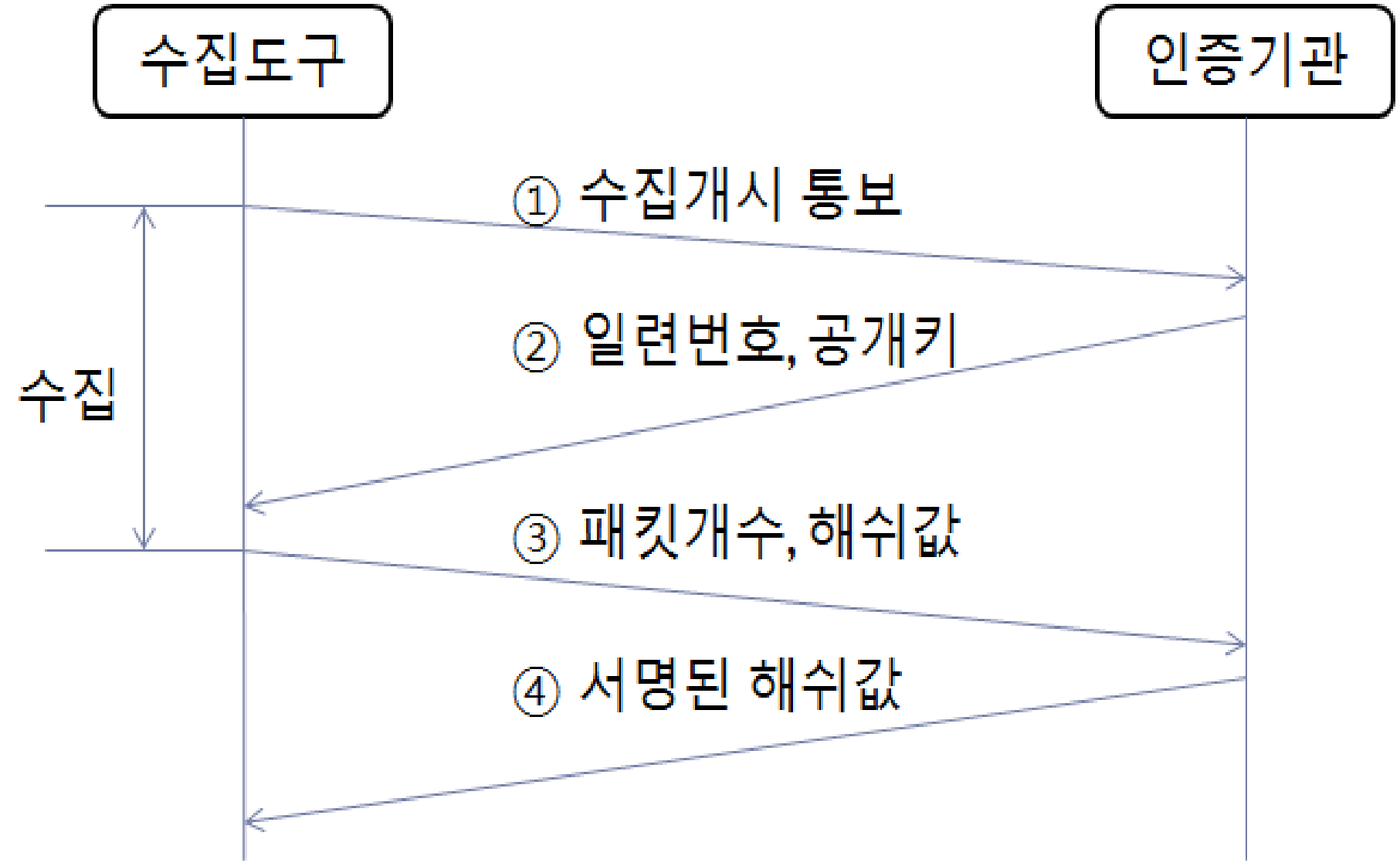


$$\text{forensic pcap} = E(\ \text{packets} \mid S(\ H(\text{packets})\ ,\ \text{Private-Key}_{\text{observer}}\ )\ ,\ K_{\text{executer}}\ )$$

설계 (FPCAP STRUCTURE)

연번	내용	설명	사이즈	데이터형
1	version	forensic pcap의 버전	2	short
2	hdr_len	forensic pcap의 헤더길이	2	short
3	mode	현장참관(1),원격참관(2)	4	int
4	row_id	인증기관 발급 일련번호	4	u int
5	executer_hash	수집자가 입력한 비밀번호의 SHA256 해쉬	32	Char
6	observer_hash	참관자가 입력한 비밀번호의 SHA256 해쉬	32	Char
7	size_n	Modulus의 문자열 길이	4	Int
8	n	Modulus의 hex 문자열	가변	Char
9	size_e	공개키의 길이	4	Int
10	e	공개키의 hex 문자열	가변	Char
11	size_d	비밀키의 문자열 길이	4	Int
12	d	현장참관자의 비밀번호로 암호화된 비밀키의 문자열	가변	Bin
13	pcap_file_header	Pcap 파일의 전역 header		
14	pcap_sf_pkthdr	Packet별 pcap header		
15	packet	Packet 본문	가변	
16	crc	Packet header와 packet의 CRC값	4	Int
		…		
n	forensic hash	1~n-1까지의 자료에 대한 SHA256 해쉬를 RSA 암호화값	RSA Block size	Bin

설계 (Communication protocol)



설계 (Communication protocol)

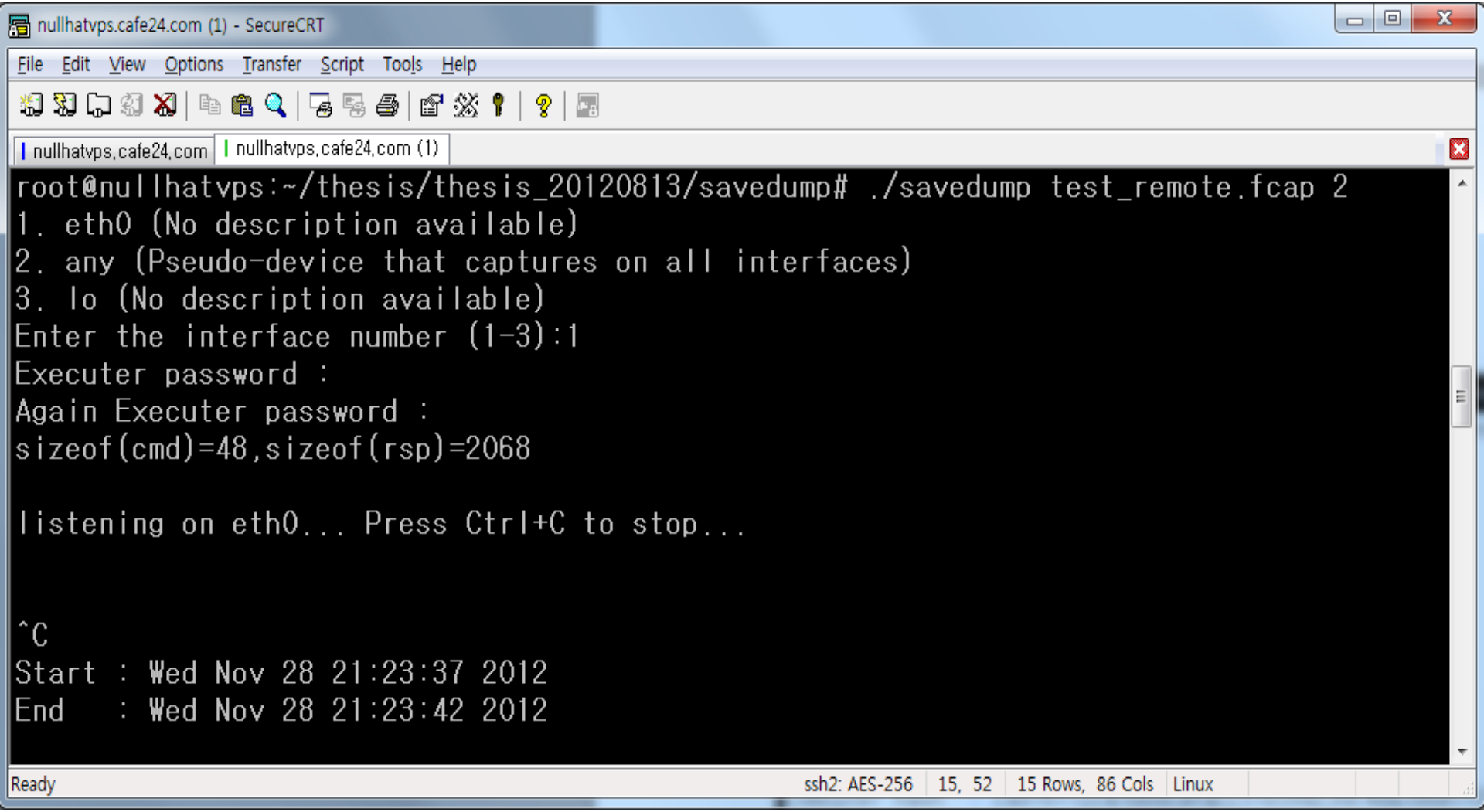
수집도구 -> 인증기관		
연번	내용	데이터형
1	mode	int
2	row_id	u int
3	count	u int
4	hash_len	int
5	hash	char[]

인증기관 -> 수집도구		
연번	내용	데이터형
1	status	int
2	row_id	u int
3	signed_hash_len	int
4	signed_hash	가변
5	e_size	int
6	e	char
7	n_size	int
8	n	int

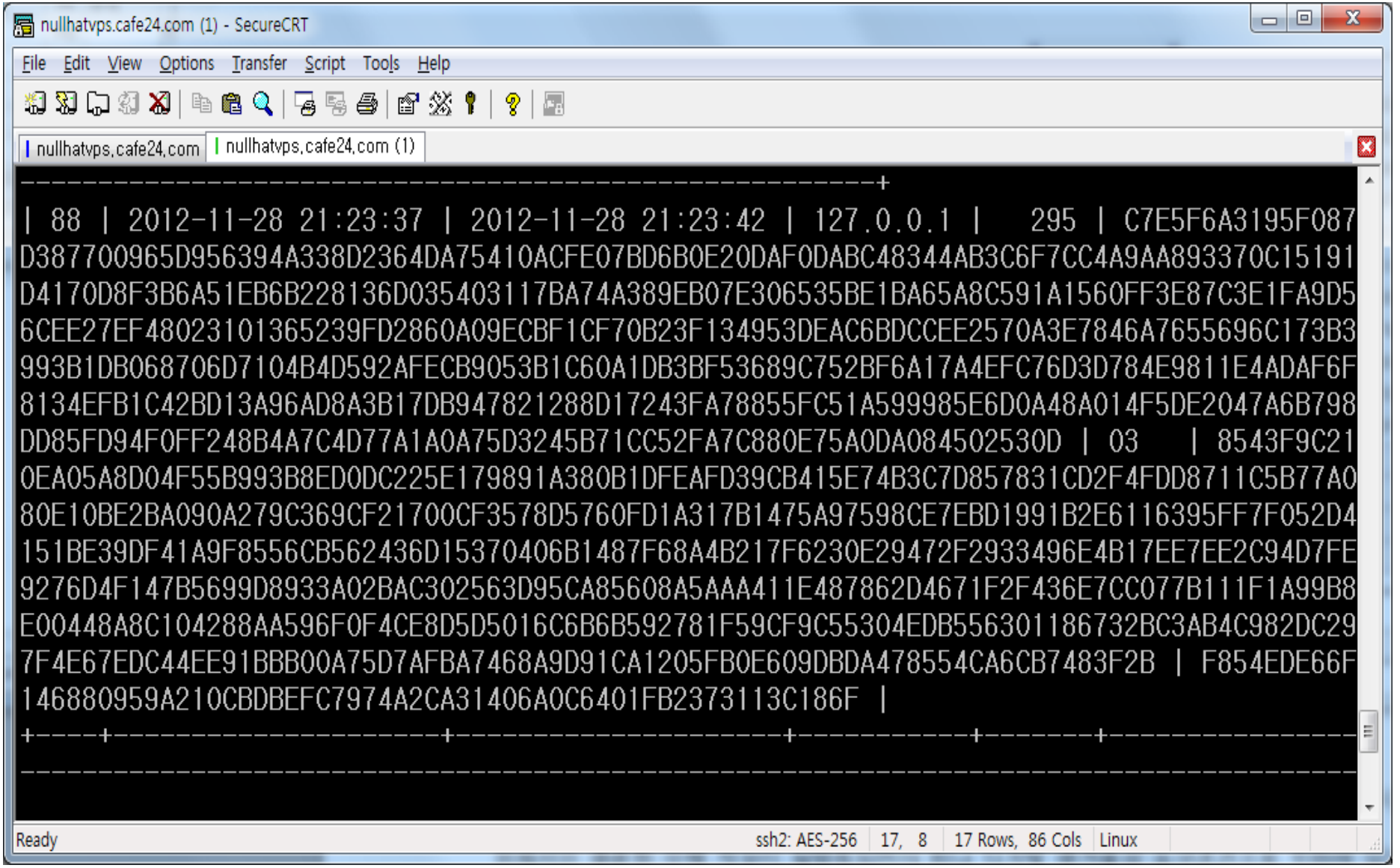
설계 (Database schema)

연번	내용	데이터형	연번	내용	데이터형
1	row_id	u int	6	n	char
2	start_date	datetime	7	e	char
3	end_date	datetime	8	d	char
4	src_ip	char	9	hash	char
5	count	u int			

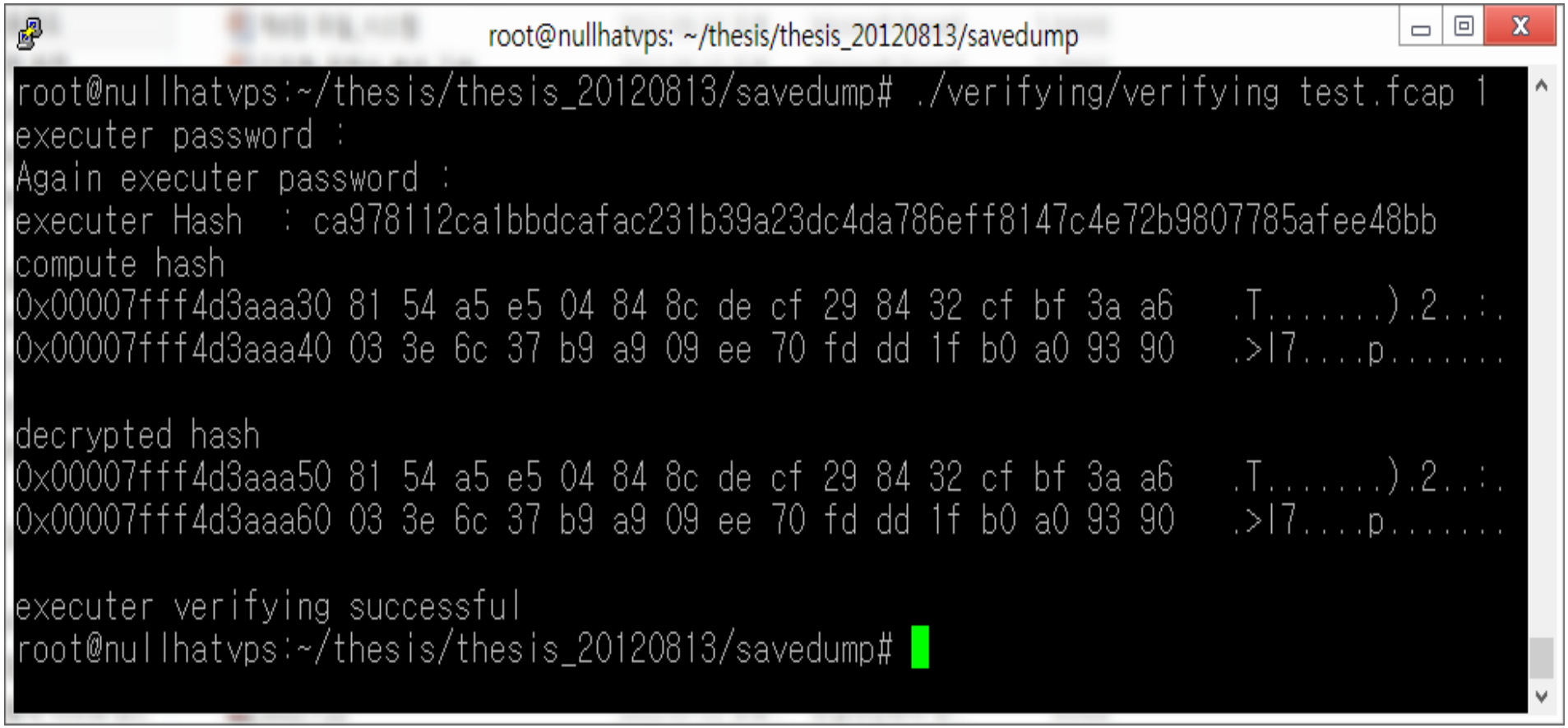
시연 (수집)


nullhatvps.cafe24.com (1) - SecureCRT
File Edit View Options Transfer Script Tools Help
nullhatvps.cafe24.com
nullhatvps.cafe24.com (1)
root@nullhatvps:~/thesis/thesis_20120813/savedump# ./savedump test_remote.fcap 2
1. eth0 (No description available)
2. any (Pseudo-device that captures on all interfaces)
3. lo (No description available)
Enter the interface number (1-3):1
Executer password :
Again Executer password :
sizeof(cmd)=48,sizeof(rsp)=2068
listening on eth0... Press Ctrl+C to stop...
^C
Start : Wed Nov 28 21:23:37 2012
End : Wed Nov 28 21:23:42 2012
Ready
ssh2: AES-256
15, 52
15 Rows, 86 Cols
Linux

시연 (CA)


nullhatvps.cafe24.com (1) - SecureCRT
File Edit View Options Transfer Script Tools Help
nullhatvps.cafe24.com
nullhatvps.cafe24.com (1)
| 88 | 2012-11-28 21:23:37 | 2012-11-28 21:23:42 | 127.0.0.1 | 295 | C7E5F6A3195F087
D387700965D956394A338D2364DA75410ACFE07BD6B0E20DAF0DABC48344AB3C6F7CC4A9AA893370C15191
D4170D8F3B6A51EB6B228136D035403117BA74A389EB07E306535BE1BA65A8C591A1560FF3E87C3E1FA9D5
6CEE27EF4802310136523 9FD2860A09ECBF1CF70B23F134953DEAC6BDCCEE2570A3E7846A7655696C173B3
993B1DB068706D7104B4D592AFECB9053B1C60A1DB3BF53689C752BF6A17A4EFC76D3D784E9811E4ADAF6F
8134EFB1C42BD13A96AD8A3B17DB947821288D17243FA78855FC51A599985E6D0A48A014F5DE2047A6B798
DD85FD94F0FF248B4A7C4D77A1A0A75D3245B71CC52FA7C880E75A0DA084502530D | 03 | 8543F9C21
0EA05A8D04F55B993B8ED0DC225E179891A380B1DFEAFD39CB415E74B3C7D857831CD2F4FDD8711C5B77A0
80E10BE2BA090A279C369CF21700CF3578D5760FD1A317B1475A97598CE7EBD1991B2E6116395FF7F052D4
151BE39DF41A9F8556CB562436D15370406B1487F68A4B217F6230E29472F2933496E4B17EE7EE2C94D7FE
9276D4F147B5699D8933A02BAC302563D95CA85608A5AAA411E487862D4671F2F436E7CC077B111F1A99B8
E00448A8C104288AA596F0F4CE8D5D5016C6B6B592781F59CF9C55304EDB556301186732BC3AB4C982DC29
7F4E67EDC44EE91BBB00A75D7AFBA7468A9D91CA1205FB0E609DBDA478554CA6CB7483F2B | F854EDE66F
146880959A210CBDBEFC7974A2CA31406A0C6401FB2373113C186F |
Ready
ssh2: AES-256
17, 8
17 Rows, 86 Cols
Linux

시연 (검증)


root@nullhatvps: ~/thesis/thesis_20120813/savedump
root@nullhatvps:~/thesis/thesis_20120813/savedump# ./verifying/verifying test.fcap 1
executer password :
Again executer password :
executer Hash : ca978112ca1bbdcafac231b39a23dc4da786eff8147c4e72b9807785afee48bb
compute hash
0x00007fff4d3aaa30 81 54 a5 e5 04 84 8c de cf 29 84 32 cf bf 3a a6 .T.....).2..:.
0x00007fff4d3aaa40 03 3e 6c 37 b9 a9 09 ee 70 fd dd 1f b0 a0 93 90 .>l7....p.....
decrypted hash
0x00007fff4d3aaa50 81 54 a5 e5 04 84 8c de cf 29 84 32 cf bf 3a a6 .T.....).2..:.
0x00007fff4d3aaa60 03 3e 6c 37 b9 a9 09 ee 70 fd dd 1f b0 a0 93 90 .>l7....p.....
executer verifying successful
root@nullhatvps:~/thesis/thesis_20120813/savedump#

전송 중인 디지털 증거뿐 아니라 모든 디지털 증거의 수집시 제출자 또는 참관자의 전자서명을 디지털 증거에 포함하는 한편 공정한 **인증기관의 설립**으로 누구나 진정성과 무결성을 담보 받을 수 있도록 디지털 포렌식 **도구와 절차들은 개선이 필요하다**.

Question and Answer