



# [Ann's Deception] Write-Up

작성자	류나연
분석 일자	2024.05.17 / 06.05~07
작성 일자	2024.06.07
분석 대상	Defcon2011-Contest.tc
문서 버전	2.0
작성자 E-mail	<a href="mailto:01star01ek@gmail.com">01star01ek@gmail.com</a>

0. 목차

1. 문제 .....3

2. 분석 도구 .....3

3. 환경 .....3


4. Write-Up.....4

5. Flag..... 18

6. 별도 첨부 .....20

7. Reference .....21

### 1. 문제

URL	<a href="https://forensicscontest.com/2011/08/16/puzzle-9-anns-deception-defcon-2011">https://forensicscontest.com/2011/08/16/puzzle-9-anns-deception-defcon-2011</a>
문제 내용	(*세부 문제 별도 첨부)
문제 파일	<div>  </div> Defcon2011-Contest.tc
문제 유형	네트워크 포렌식
난이도	2 / 3

### 2. 분석 도구

도구명	다운로드 링크	Version
True Crypt	<a href="https://truecrypt.softonic.kr/">https://truecrypt.softonic.kr/</a>	V 7.2
WireShark	<a href="https://www.wireshark.org/download.html">https://www.wireshark.org/download.html</a>	4.0.10
Network Miner	<a href="https://www.netresec.com/?page=NetworkMiner">https://www.netresec.com/?page=NetworkMiner</a>	-

### 3. 환경

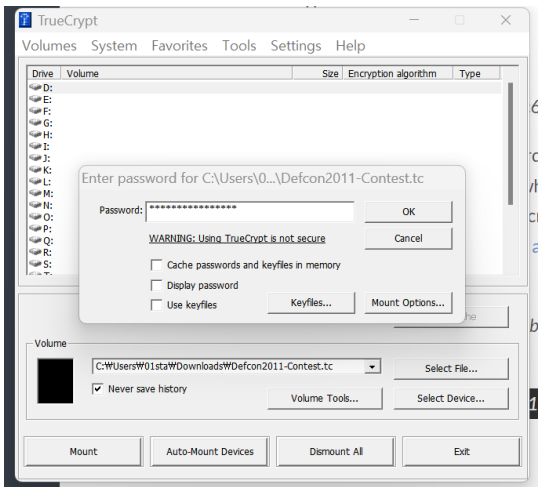
OS
Windows 11 Home, Ubuntu 2204

4. Write-Up

파일명	Defcon2011-Contest.tc
용량	50.0MB
SHA256	6906e4a08bd498c6ff78928b1c8d292a9f89f2ecfac60094528f4497e2254474
Timestamp	2024-05-17 17:38:04

Q1. What is the name of the Company being attacked?

1.tc 파일 확인 및 암호 해제



[사진 1] 암호를 해제하는 모습

해당 파일의 형식은 tc로 암호화된 가상 디스크이기에 True Cypt 도구를 사용하여 암호화를 해제 해주었다.

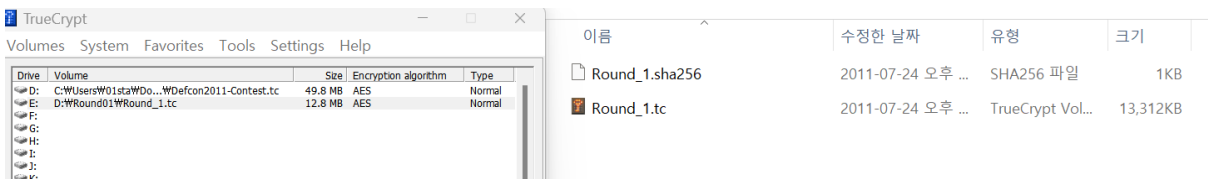
이름	수정한 날짜	유형	크기
.Trashes	2011-07-25 오전 ...	파일 폴더	
Round01	2011-07-25 오전 ...	파일 폴더	
Round02	2011-07-25 오전 ...	파일 폴더	
Round03	2011-07-25 오전 ...	파일 폴더	
Round04	2011-07-25 오전 ...	파일 폴더	
Round05	2011-07-25 오전 ...	파일 폴더	
Round06	2011-07-25 오전 ...	파일 폴더	
System Volume Information	2024-05-18 오전 ...	파일 폴더	
휴지통	2024-05-18 오전 ...	파일 폴더	
..Trashes	2011-07-25 오전 ...	TRASHES 파일	4KB

[사진 2] 해당 디스크 안에 들어있는 내용

암호가 해제된 가상 디스크에는 총 6라운드의 문제가 들어있었다. 이에 따라 각 라운드를 해결하고자 하였다.

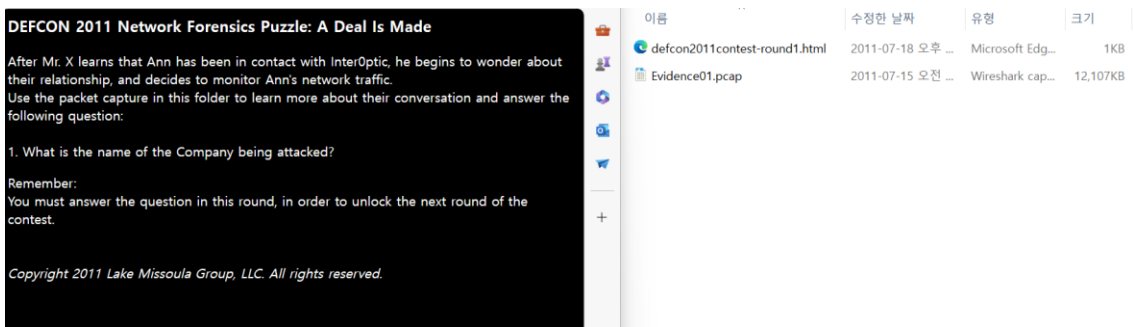
[WHS-2] .iso

1 -1. Round01 암호 파일 해제 및 문제 확인



[사진 3] Round01.tc 파일 암호 해제

첫 라운드의 폴더를 들어가보니 암호화된 가상 디스크를 발견할 수 있었다. 이에 따라 이전과 동일한 방법으로 암호를 해제해주었다.



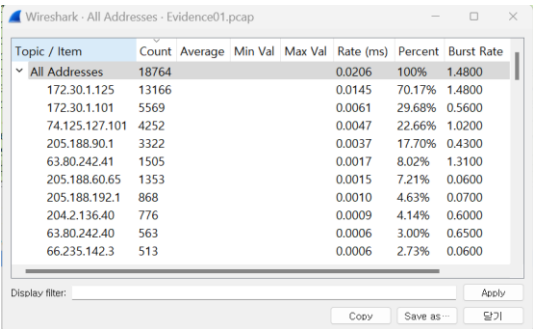
[사진 4] Round1 문제 확인

암호를 확인해보니 해당 디스크안에는 html 파일과 pcap 파일이 들어있었다.

문제는 1. What is the name of the Company being attacked? 이다.

따라서 해당 문제의 답을 찾으려고 노력하였다.

1-2. PCAP 구조 파악

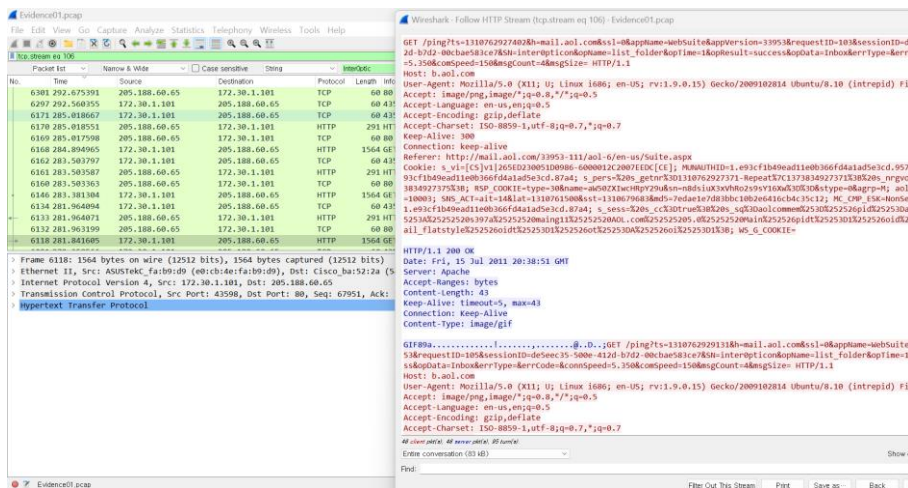


[사진 5] 와이어샤크를 통해 도출한 통신한 ip4 주소 통계

## [WHS-2] .iso

와이어샤크를 통해 기본적으로 한 번 훑으며 특이사항을 파악하였다. mail관련 키워드가 많아 이에 주목했으며 와이어샤크의 통계 기능을 활용하여 어떠한 ip들과 가장 많이 통신했는지 확인하였다.

### 1-3. 분석



The image shows a Wireshark packet capture analysis. The top pane displays a list of packets, with packet 6118 selected. The middle pane shows the details of the selected packet, including Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol. The bottom pane shows the raw data of the packet in hexadecimal and ASCII.

[사진 6] 와이어샤크를 통한 패킷 분석

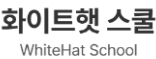
이에 따라 다양한 방법으로 분석을 시도하였다. 해본 방법은

1. InterOptic 키워드 검색을 통한 관련 stream 확인
2. 가장 많은 통신이 있던 ip 172.30.1.125 추적 (ip.addr == 172.30.1.125)
3. Company, Firm 등의 회사 관련 키워드 검색
4. Mail 관련 http stream 확인 -> webmail 중 aol.com 추적
5. Tcp dup ack 가 다량으로 발생한 지점 조사
6. http 통신 조사

해당 과정에서 배운 새로운 사실은 gzip 으로 압축된 데이터를 볼 때에는 HTTP 스트림을 보는 것이 가장 일반적인 방법이라는 것이다.

결국 정답을 찾은 방법은

**strings [파일명] | grep company** 명령어를 사용한 것으로

[illegible]

해당 명령어의 결과로 나온 무수한 글자들 사이에서 답을 발견할 수 있었다.

### 2-1. Round02 암호 파일 해제 및 문제 확인



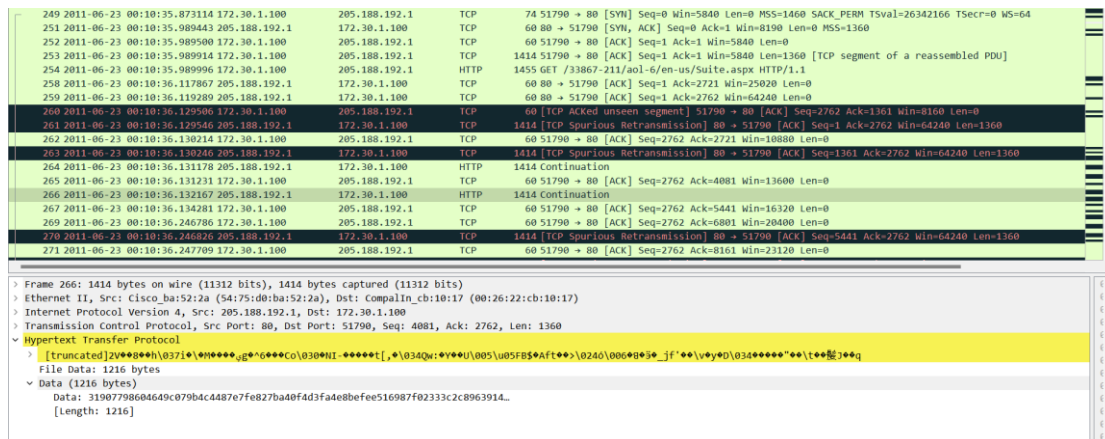
## 2-2. PCAP 구조 파악

[사진 9] 와이어샹크를 통해 도출한 통신한 ip4 주소 통계

## [WHS-2] .iso

와이어샤크를 통해 기본적으로 한 번 훑으며 특이사항을 파악하였다. 모든 통신이 172.30.1.100을 바탕으로 진행됨을 알 수 있었다. 즉 자기 자신의 가장 많이 통신한 205.188.192.1에 관심을 가지게 되었다.

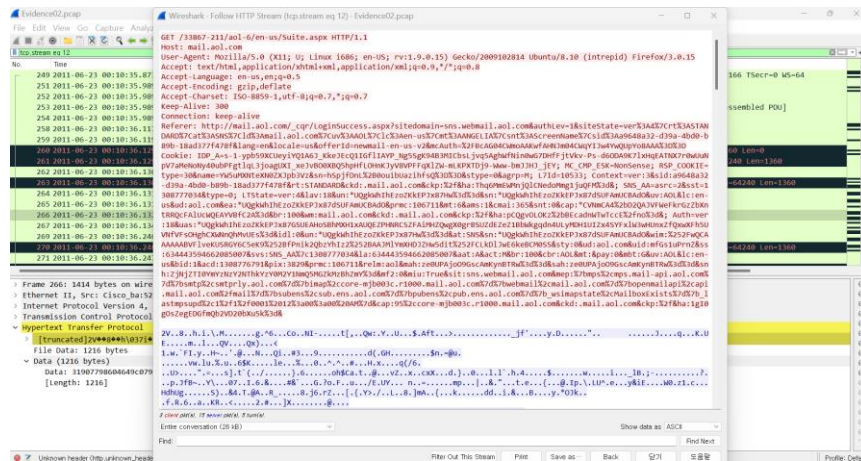
### 2-3. 분석



The image shows a Wireshark packet capture analysis. The top pane displays a list of packets, with packet 266 highlighted. The middle pane shows the details of packet 266, which is an HTTP GET request. The bottom pane shows the raw data of the packet, which is a gzip-compressed file named 'data'.

[사진 10] ip.addr == 205.188.192.1 && http 필터 내용 탐색 중 발견한 눈에 띄는 내용

따라서 ip.addr == 205.188.192.1 && http를로 필터를 준 뒤 특이점이 있는지 탐색하였다. 이 중 한 http 통신에서 내용이 깨져있음을 발견하였다.



The image shows a Wireshark packet capture analysis. The top pane displays a list of packets, with packet 266 highlighted. The middle pane shows the details of packet 266, which is an HTTP GET request. The bottom pane shows the raw data of the packet, which is a gzip-compressed file named 'data'.

[사진 11] gzip으로 암호화 되어 있는 내용 확인

해당 내용을 잘 분석해보니 gzip으로 암호화되어 있으며 찾아보니 압축 전송을 통해 사이트 최적화를 위해 사용되기도 한다고 한다. 따라서 이를 복호화 하고자 했다.



sZegEDGfmQb2VD20bXu5k%3d&

이건 g-zip으로 압축되어 있나요?

예, 이것은 gzip으로 압축된 것입니다. Content-Encoding 헤더가 "gzip"로 설정되어 있으며, 이는 서버가 해당 본문을 gzip으로 압축하여 클라이언트에게 전송했음을 나타냅니다.

해제해줘

좋습니다. 압축을 해제하고 내용을 풀어드리겠습니다.

HTML

```
<!DOCTYPE html>
<html lang="ko">
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">
<title>Untitled Document</title>
</head>
<body>
<p>이건 뭘니까?</p>
</body>
</html>
```

위의 코드는 gzip으로 압축 해제된 내용입니다.

### [사진 12] chat gpt를 사용하여 복호화

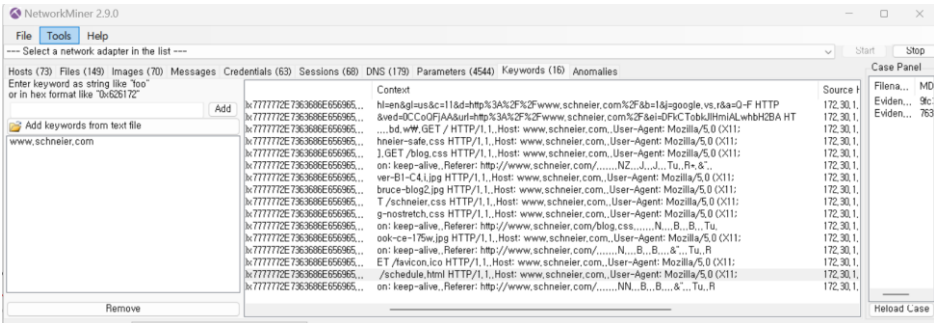
이것은 HTTP 요청 헤더와 본문으로 구성된 HTTP 요청 메시지입니다. 이 요청은 "mail.aol.com" 호스트로 전송되며, gzip 및 deflate와 같은 압축 방법을 수락하고 있습니다. 또한, "www.schneier.com"이라는 다른 호스트에 대한 참조를 나타내는 것으로 보이는데, 이는 아마도 웹 페이지에서 자바스크립트 파일을 가져오기 위한 것으로 추정됩니다.

해당 요청의 세부 내용은 다음과 같습니다:

1. HTTP 메서드: GET
2. 요청 URI: /33867-211/aol-6/en-us/common/bundle.js.aspx?version=33867-2&iu=False
3. 호스트: mail.aol.com
4. 사용자 에이전트(User-Agent): Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.0.15) Gecko/2009102814 Ubuntu/8.10 (intrepid) Firefox/3.0.15
5. 수용하다 : /
6. Accept-Language : en-us,en;q=0.5

### [사진 13] chat gpt를 사용하여 세부 내용 파악

이를 복호화해보니 위와 같은 텍스트 내용이 있어 이가 중요하다고 생각되었다. 추가적으로 chat gpt 는 해당 통신들이 [www.schneier.com](http://www.schneier.com) 를 참고함을 알려주었다. 이에 따라



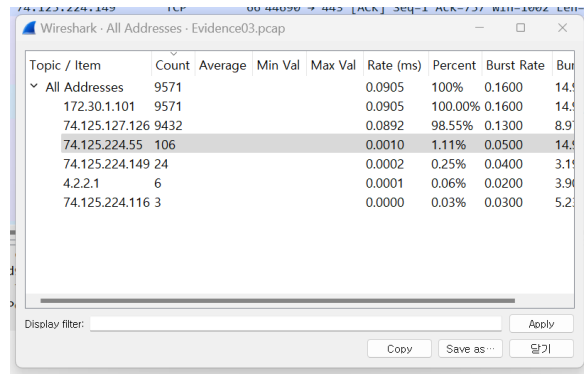
### [사진 14] network miner를 통한 검색

## [WHS-2] .iso

[www.schneier.com](http://www.schneier.com)와 관련된 키워드들을 network miner로 검색하여 찾아냈다. 이에 따라 [www.schneier.com/schedule.html](http://www.schneier.com/schedule.html) 을 방문하였음을 알게 되었고 해당 사이트를 접속했으나 시간이 오래 흐름에 따라 해당 사이트가 존재하지 않아 답을 찾지 못하였다.

### Q3. What is Romulus' password?

#### 3-1. Round03 암호 파일 해제 및 문제 확인 및 PCAP 구조 파악

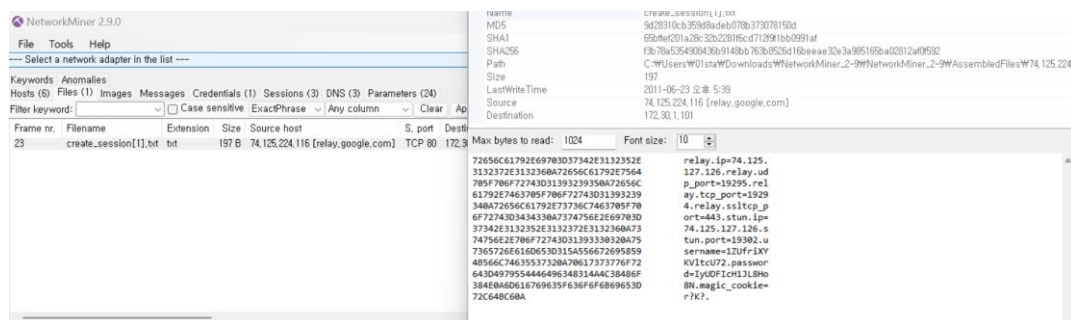


Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Bur
All Addresses	9571				0.0905	100%	0.1600	14.1
172.30.1.101	9571				0.0905	100.00%	0.1600	14.1
74.125.127.126	9432				0.0892	98.55%	0.1300	8.9
74.125.224.55	106				0.0010	1.11%	0.0500	14.1
74.125.224.149	24				0.0002	0.25%	0.0400	3.1
4.2.2.1	6				0.0001	0.06%	0.0200	3.9
74.125.224.116	3				0.0000	0.03%	0.0300	5.2

[사진 15] 와이어샤크를 통해 도출한 통신한 ip4 주소 통계

앞전에 했던 내용과 동일한 과정을 통해 문제파일을 확인하고 문제를 파악하였다. 이에 이번에도 PCAP 파일이 있었기에 구조를 파악했다. 해당 통신 중 가장 많이 통신한 74.125.127.126 에 집중하였다.

#### 3-2. 분석



Frame no.	Filename	Extension	Size	Source host	S. port	Dest
23	create_session[1].txt	txt	197 B	74.125.224.116 [relay.google.com]	TCP 80	172.30.1.101

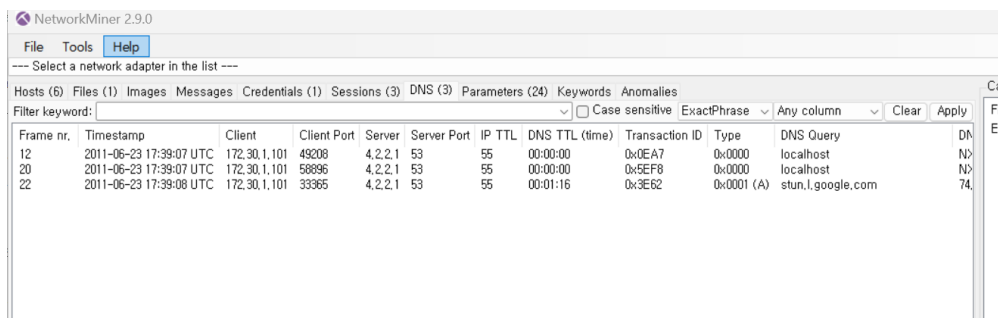
Field	Value
Frame time	2011-06-23 오후 5:39
Source	74.125.224.116 [relay.google.com]
Destination	172.30.1.101
Max bytes to read:	1024
Font size:	10

```

72656C61792E69783D37342E3132352E
3132372E3132366A72656C61792E7564
705F706F72743D31393239350A72656C
61792E7463706F706F72743D31393239
340A72656C61792E73736C7463706F70
6F72743D343430A7374756E2E69783D
37342E3132352E3132372E3132366A73
74756E2E706F72743D31393239350A73
7365726E610D653D315A556672695859
48566C74635537320A70617373776F72
643D6977554464696348314A4C38A66F
384E0A6D616769635F636F6F6869653D
72C648C60A
relay.ip=74.125.
127.126.relay.ud
p_port=19295,rel
ay.tcp.port=1929
4.relay.ssltcp.p
ort=443.stun.ip=
74.125.127.126.s
tun.port=19362,u
sername=12uffr-IXY
kV1tcU72.passwor
d=1ydpfCn1JL8n6
8N.magic_cookie=
r7K7.
  
```

[사진 16] network miner를 통한 파일 확인

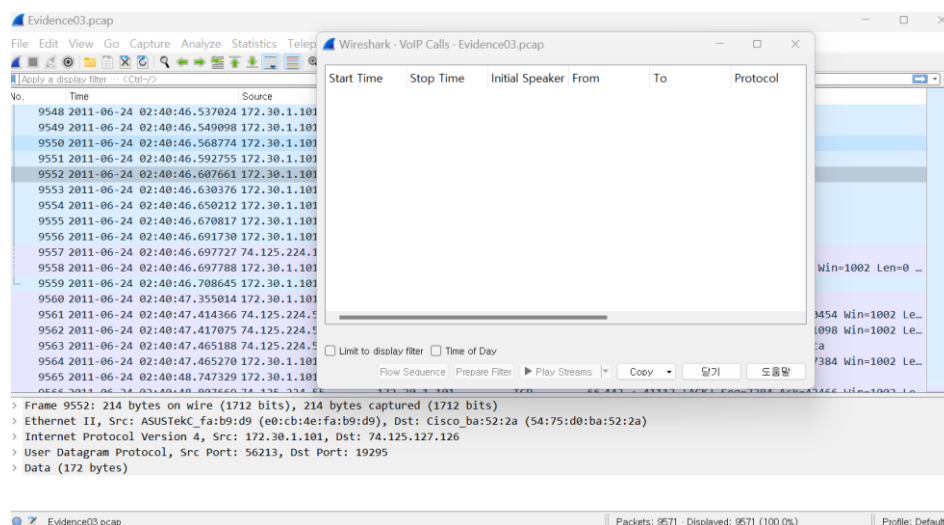
이전 문제에서 network miner에 도움을 많이 받았던 터라 일단 network miner를 돌려보았다. 이를 통해 단 하나의 파일을 발견하였다. 딱 봐도 의심스러운 파일명이었기에 이를 확인해보았다. 세션으로 통신을 했음을 알게 되었으며 이에 대한 ip와 port, password를 확인할 수 있었다. 해당 통신을 통해 패스워드가 전달되었을 것 같아 이에 집중하여 탐색하였다.



Frame nr.	Timestamp	Client	Client Port	Server	Server Port	IP TTL	DNS TTL (time)	Transaction ID	Type	DNS Query	DN
12	2011-06-23 17:39:07 UTC	172.30.1.101	49208	4.2.2.1	53	55	00:00:00	0x0EA7	0x0000	localhost	N>
20	2011-06-23 17:39:07 UTC	172.30.1.101	58896	4.2.2.1	53	55	00:00:00	0x0EF8	0x0000	localhost	N>
22	2011-06-23 17:39:08 UTC	172.30.1.101	33365	4.2.2.1	53	55	00:01:16	0x0E62	0x0001 (A)	stun.l.google.com	74.

[사진 17] network miner – DNS

DNS정보에서 이전 파일의 응답에 reply였던 google이 나오는 것을 보고 stun.l.google.com에 대해 찾아보았다. 이에 대해 알아보니 STUN 서버는 NAT(Network Address Translation) 환경에서 VoIP(Voice over Internet Protocol), 영상 통화 및 기타 멀티미디어 통신에 사용되는 프로토콜이라고 한다. 이를 통해 통화를 통해 정보를 주고 받았음을 의심하게 되었다.



Vo.	Time	Source
9548	2011-06-24 02:40:46.537024	172.30.1.101
9549	2011-06-24 02:40:46.549098	172.30.1.101
9550	2011-06-24 02:40:46.568774	172.30.1.101
9551	2011-06-24 02:40:46.592755	172.30.1.101
9552	2011-06-24 02:40:46.607661	172.30.1.101
9553	2011-06-24 02:40:46.630376	172.30.1.101
9554	2011-06-24 02:40:46.650212	172.30.1.101
9555	2011-06-24 02:40:46.670817	172.30.1.101
9556	2011-06-24 02:40:46.691730	172.30.1.101
9557	2011-06-24 02:40:46.697727	74.125.224.1
9558	2011-06-24 02:40:46.697788	172.30.1.101
9559	2011-06-24 02:40:46.708645	172.30.1.101
9560	2011-06-24 02:40:47.355014	172.30.1.101
9561	2011-06-24 02:40:47.414366	74.125.224.1
9562	2011-06-24 02:40:47.417075	74.125.224.1
9563	2011-06-24 02:40:47.465188	74.125.224.1
9564	2011-06-24 02:40:47.465270	172.30.1.101
9565	2011-06-24 02:40:48.747329	172.30.1.101

Start Time	Stop Time	Initial Speaker	From	To	Protocol

Frame 9552: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits) on interface 0  
 Ethernet II, Src: ASUSTekC\_fa:b9:d9 (e0:cb:de:fa:b9:d9), Dst: Cisco\_ba:52:2a (54:75:d0:ba:52:2a)  
 Internet Protocol Version 4, Src: 172.30.1.101, Dst: 74.125.127.126  
 User Datagram Protocol, Src Port: 56213, Dst Port: 19295  
 Data (172 bytes)

[사진 18] wireshark VOIP 기록 확인




그러나 해당 PCAP를 아무리 확인해봐도 해당 통신내 VOIP에 대한 기록을 와이어샤크가 따로 인식하여 보여주지 못하였다. (이전에도 분명히 gzip으로 압축되어 내용을 확인하지 못하였으므로 이번에도 해당 기록 또는 파일을 다른 형식으로 압축했을 것이라고 생각했다. 따라서 툴을 통해 추출해보기로 하였다. 따라서 관련된 정보를 찾아보던 중 mp4의 압축 형식인 h264에 대해 알게 되었다. 따라서 이가 있는지 검색해보고자 했고 videosnarf - pcap 파일에서 h264 패킷을 추출하여서 264 파일로 저장하는 프로그램이라는 명의 블로그에서 videosnarf를 알게 되어 이를 시도해보았다.)

## [WHS-2] .iso

```
Segmentation fault
(base) dorothy08ek@localhost:~/videosnarf-0.63$ explorer.exe .
(base) dorothy08ek@localhost:~/videosnarf-0.63$ videosnarf -i ./pcap/Evidence03.pcap
Starting videosnarf 0.63
[+]Starting to snarf the media packets
[+] Please wait while decoding pcap file...
added new stream. :172.30.1.101(56213) to 74.125.127.126(19295). codec is 00
added new stream. :74.125.127.126(19295) to 172.30.1.101(56213). codec is 00
added new stream. :172.30.1.101(56213) to 74.125.127.126(19295). codec is 65
[+]Stream saved to file G711ULAW-media-1.wav
[+]Stream saved to file G711ULAW-media-2.wav
[+]Stream saved to file H264-media-3.264
[+]Number of streams found are 3
[+]Snarfing Completed
(base) dorothy08ek@localhost:~/videosnarf-0.63$ explorer.exe .
(base) dorothy08ek@localhost:~/videosnarf-0.63$
```

[사진 19] videosnarf를 통해 추출해본 파일들

따라서 이를 실행해 보았다.

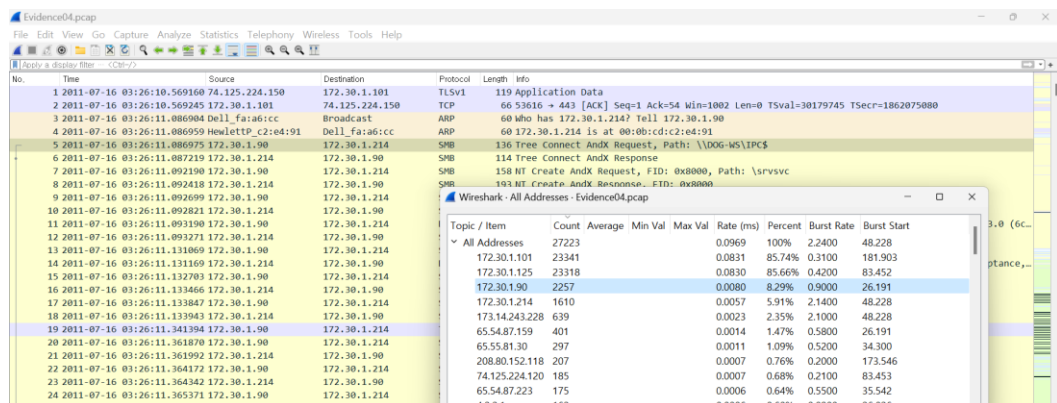
 G711ULAW-media-1.wav	2024-06-08 오전 5:51	WAV 파일	744KB
 G711ULAW-media-2.wav	2024-06-08 오전 5:51	WAV 파일	729KB
 H264-media-3.264	2024-06-08 오전 5:51	264 파일	1KB

[사진 20] 추출한 .wav 파일

이를 통해 3개의 파일이 생겼으며 해당 음성파일에서 화자는 비밀번호를 영어로 말하였다. 이를 통해 **비밀번호인 rom127#**를 찾아내었다.

## Q4. What is the 16th name inside the mysterious file transferred?

### 4-1. Round04 암호 파일 해제 및 문제 확인 및 PCAP 구조 파악



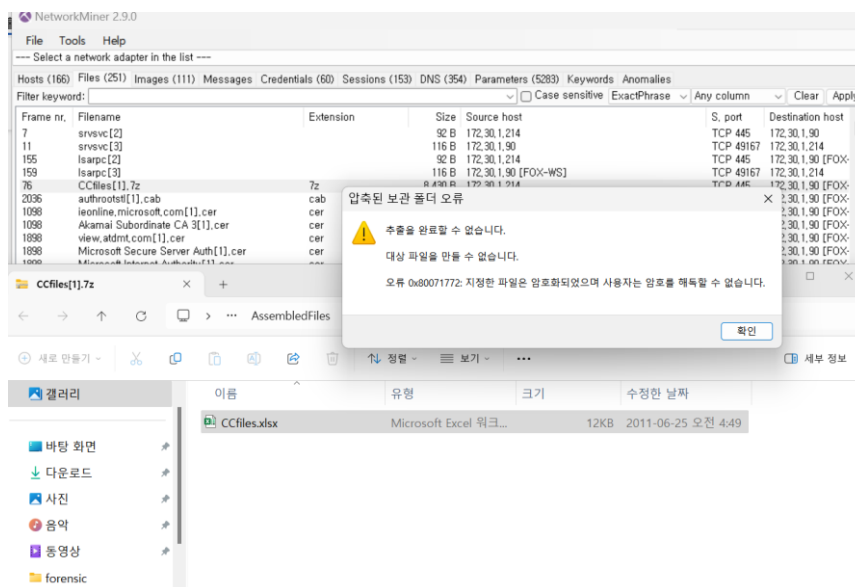
No.	Time	Source	Destination	Protocol	Length	Info
1	2011-07-16 03:26:10.569160	74.125.224.150	172.30.1.101	TLSv1	119	Application Data
2	2011-07-16 03:26:10.569245	172.30.1.101	74.125.224.150	TCP	66	53616 → 443 [ACK] Seq=1 Ack=54 Win=1002 Len=0 TSval=30179745 TSecr=1862075080
3	2011-07-16 03:26:11.086904	Dell fa:a6:cc	Broadcast	ARP	60	who has 172.30.1.214? Tell 172.30.1.90
4	2011-07-16 03:26:11.086959	HewlettP c2:e4:91	Dell fa:a6:cc	ARP	60	172.30.1.214 is at 00:0b:cd:c2:e4:91
5	2011-07-16 03:26:11.086975	172.30.1.90	172.30.1.214	SMB	136	Tree Connect AndX Request, Path: \\DOG-WS\IPC\$
6	2011-07-16 03:26:11.087219	172.30.1.214	172.30.1.90	SMB	114	Tree Connect AndX Response
7	2011-07-16 03:26:11.092190	172.30.1.90	172.30.1.214	SMB	158	NT Create AndX Request, FID: 0x8000, Path: \srvsvc
8	2011-07-16 03:26:11.092418	172.30.1.214	172.30.1.90	SMB	103	NT Create AndX Response, FID: 0x8000
9	2011-07-16 03:26:11.092699	172.30.1.90	172.30.1.214	SMB	103	NT Create AndX Request, FID: 0x8000
10	2011-07-16 03:26:11.092821	172.30.1.214	172.30.1.90	SMB	103	NT Create AndX Response, FID: 0x8000
11	2011-07-16 03:26:11.093190	172.30.1.90	172.30.1.214	SMB	103	NT Create AndX Request, FID: 0x8000
12	2011-07-16 03:26:11.093271	172.30.1.214	172.30.1.90	SMB	103	NT Create AndX Response, FID: 0x8000
13	2011-07-16 03:26:11.131069	172.30.1.90	172.30.1.214	SMB	103	NT Create AndX Request, FID: 0x8000
14	2011-07-16 03:26:11.131169	172.30.1.214	172.30.1.90	SMB	103	NT Create AndX Response, FID: 0x8000
15	2011-07-16 03:26:11.132703	172.30.1.90	172.30.1.214	SMB	103	NT Create AndX Request, FID: 0x8000
16	2011-07-16 03:26:11.133466	172.30.1.214	172.30.1.90	SMB	103	NT Create AndX Response, FID: 0x8000
17	2011-07-16 03:26:11.133847	172.30.1.90	172.30.1.214	SMB	103	NT Create AndX Request, FID: 0x8000
18	2011-07-16 03:26:11.133943	172.30.1.214	172.30.1.90	SMB	103	NT Create AndX Response, FID: 0x8000
19	2011-07-16 03:26:11.341394	172.30.1.90	172.30.1.214	SMB	103	NT Create AndX Request, FID: 0x8000
20	2011-07-16 03:26:11.361870	172.30.1.90	172.30.1.214	SMB	103	NT Create AndX Request, FID: 0x8000
21	2011-07-16 03:26:11.361992	172.30.1.214	172.30.1.90	SMB	103	NT Create AndX Response, FID: 0x8000
22	2011-07-16 03:26:11.364172	172.30.1.90	172.30.1.214	SMB	103	NT Create AndX Request, FID: 0x8000
23	2011-07-16 03:26:11.364342	172.30.1.214	172.30.1.90	SMB	103	NT Create AndX Response, FID: 0x8000
24	2011-07-16 03:26:11.365371	172.30.1.90	172.30.1.214	SMB	103	NT Create AndX Request, FID: 0x8000
25	2011-07-16 03:26:11.365477	172.30.1.214	172.30.1.90	SMB	103	NT Create AndX Response, FID: 0x8000

[사진 21] 와이어샤크를 통해 도출한 통신한 ip4 주소 통계 및 특이한 프로토콜 확인

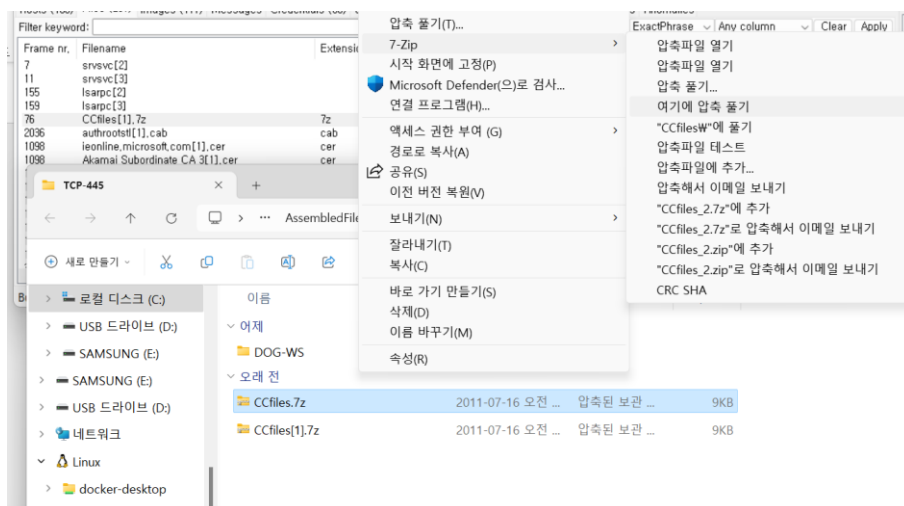
## [WHS-2] .iso

앞전에 했던 내용과 동일한 과정을 통해 문제파일을 확인하고 문제를 파악하였다. 이에 이번에도 PCAP 파일이 있었기에 구조를 파악했다. 해당 통신 중 가장 많이 통신한 74.125.127.126 에 집중하였다.

### 4-2. 분석



[사진 22] 네트워크 마이너를 통해 도출한 .7z 파일



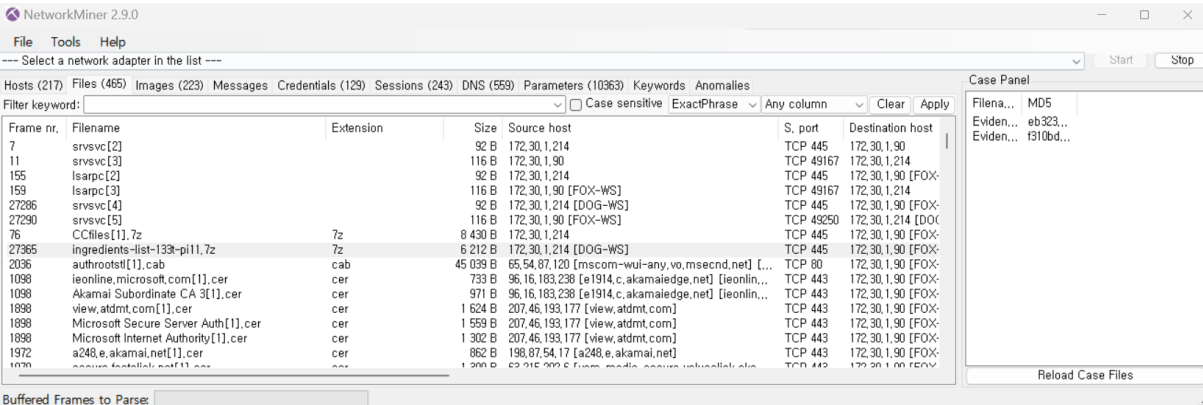
[사진 23]

[WHS-2] .iso

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	Steve Jerry	4040-2074-8970-8090	777 Amex														
2	Frank Azar	5080-2587-6420-8899	999 Visa														
3	Ben Dover	9865-2565-4514-7852	258 Visa														
4	Sally Slinger	6541-9872-9347-9363	804 Mastercard														
5	Hank Man	9874-5698-5287-2536	672 Mastercard														
6	Lane Car	7852-6982-2463-7824	987 Visa														
7	John Silver	6521-5426-1872-8765	123 Visa														
8	Larry Underman	3416-6517-8452-7820	947 Visa														
9	James Misco	4587-2587-9632-4752	652 Amex														
10	Mike Hawk	2596-6421-8998-1266	285 Discover														
11	Dixie Normis	8795-3215-9875-9654	852 Amex														
12	Nancy Landen	8742-8947-2873-4845	176 Mastercard														
13	Jenny Calpoly	5478-6548-6545-4558	984 Amex														
14	Ashley Vandervand	6541-8725-9521-5436	587 Visa														
15	Jessica Reverone	8965-1524-4567-8621	214 Visa														
16	Jason Wilson	8247-9524-9825-1265	654 Discover														
17	Phil Jacksle	4387-8694-9624-7825	247 Amex														
18	Jack MeHoff	8524-4625-7861-8641	367 Mastercard														
19	Janice freedum	7824-9624-4852-9621	347 Visa														
20	Nat Sass	6524-5842-9534-4824	725 Visa														
21	Jenny Tull	5831-4236-8964-1785	345 Mastercard														

[사진 24]

Q5. What is the 3rd ingredient on the list from the mysterious file that was transfered?



Frame nr.	Filename	Extension	Size	Source host	S. port	Destination host
7	srsvvc[2]		92 B	172.30.1.214	TCP 445	172.30.1.90
11	srsvvc[3]		116 B	172.30.1.90	TCP 49167	172.30.1.214
155	lsarpc[2]		92 B	172.30.1.214	TCP 445	172.30.1.90 [FOX-...]
159	lsarpc[3]		116 B	172.30.1.90 [FOX-WS]	TCP 49167	172.30.1.214
27286	srsvvc[4]		92 B	172.30.1.214 [DOG-WS]	TCP 445	172.30.1.90 [FOX-...]
27290	srsvvc[5]		116 B	172.30.1.90 [FOX-WS]	TCP 49250	172.30.1.214 [DOC-...]
76	CFiles[1].7z	7z	8 430 B	172.30.1.214	TCP 445	172.30.1.90 [FOX-...]
27365	Ingredients-list-139-pi11,7z	7z	6 212 B	172.30.1.214 [DOG-WS]	TCP 445	172.30.1.90 [FOX-...]
2036	authroots[1].cab	cab	45 039 B	65.54.87.120 [mscom-wui-any.vo.msecnd.net] [...]	TCP 80	172.30.1.90 [FOX-...]
1098	ieonline.microsoft.com[1].cer	cer	733 B	96.16.183.238 [e1914.c.akamaiedge.net] [ieonlin...]	TCP 443	172.30.1.90 [FOX-...]
1098	Akamai Subordinate CA 3[1].cer	cer	971 B	96.16.183.238 [e1914.c.akamaiedge.net] [ieonlin...]	TCP 443	172.30.1.90 [FOX-...]
1898	view.atdmt.com[1].cer	cer	1 624 B	207.46.193.177 [view.atdmt.com]	TCP 443	172.30.1.90 [FOX-...]
1898	Microsoft Secure Server Auth[1].cer	cer	1 559 B	207.46.193.177 [view.atdmt.com]	TCP 443	172.30.1.90 [FOX-...]
1898	Microsoft Internet Authority[1].cer	cer	1 302 B	207.46.193.177 [view.atdmt.com]	TCP 443	172.30.1.90 [FOX-...]
1972	a248.e.akamai.net[1].cer	cer	862 B	198.87.54.17 [a248.e.akamai.net]	TCP 443	172.30.1.90 [FOX-...]
1979	www.fastclick.net[1].cer	cer	1 209 B	62.915.209.6 [www.fastclick.net]	TCP 443	172.30.1.90 [FOX-...]

[사진 25]

**DEFCON 2011 네트워크 포렌식 퍼즐: 강도**

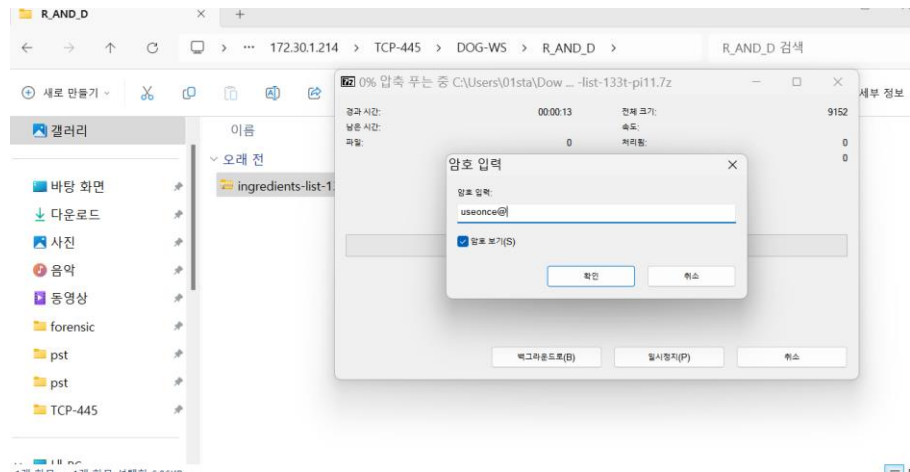
InterOptic은 Factory-Made-Winning에 도착하여 아무렇지도 않게 프런트 보안 데스크를 지나갔습니다. 그런 다음 그는 직원 뒤를 따라 보안 접근 구역으로 미끄러졌습니다. 가는 길에 그는 "useonce@"라는 비밀번호가 적힌 스티커 메모를 발견했습니다. 비밀번호는 나중에 유용할 수도 있습니다! InterOptic은 싱긋 웃으며 빈 입방체를 발견하고 노트북을 연결했습니다. 이 폴더에 있는 패킷 캡처를 사용하여 제약회사에서 InterOptic의 모험에 대해 자세히 알아보고 아래 질문에 답하십시오. 1. 전송된 신비한 파일 내의 16번째 이름은 무엇입니까?

기억하세요:  
콘테스트의 다음 라운드를 잠금 해제하려면 이번 라운드의 질문에 답해야 합니다.

저작권 2011 Lake Missoula Group, LLC. 판권 소유.

[사진 26]

일전의 4 번 문제의 상세설명을 참고하면 비밀번호를 알 수 있다.



[사진 27]

클립보드					
글꼴					
A5	A	B	C	D	E
1	<b>Ingredients List for 133T pi11</b>				
2	1 fingernail clipping from Linus Torvalds				
3	2 hairs from Richard Stallman's beard				
4	8.4 oz- Red Bull				
5					
6					
7					

[사진 28]



6. What is the final ingredient?

**DEFCON 2011 네트워크 포렌식 퍼즐: 마지막 조각**

마지막 성분은 Dr. Creedence Clearwater의 개인 Truecrypt 볼륨에 저장됩니다. 그의 하드 드라이브에는 "cipher"라는 파일이 있었습니다. 아마도 여기에는 볼륨을 잠금 해제하고 InterOptic이 마지막 성분을 찾는 데 사용할 수 있는 단서가 포함되어 있을 수 있습니다.

1) 최종 성분은 무엇입니까?

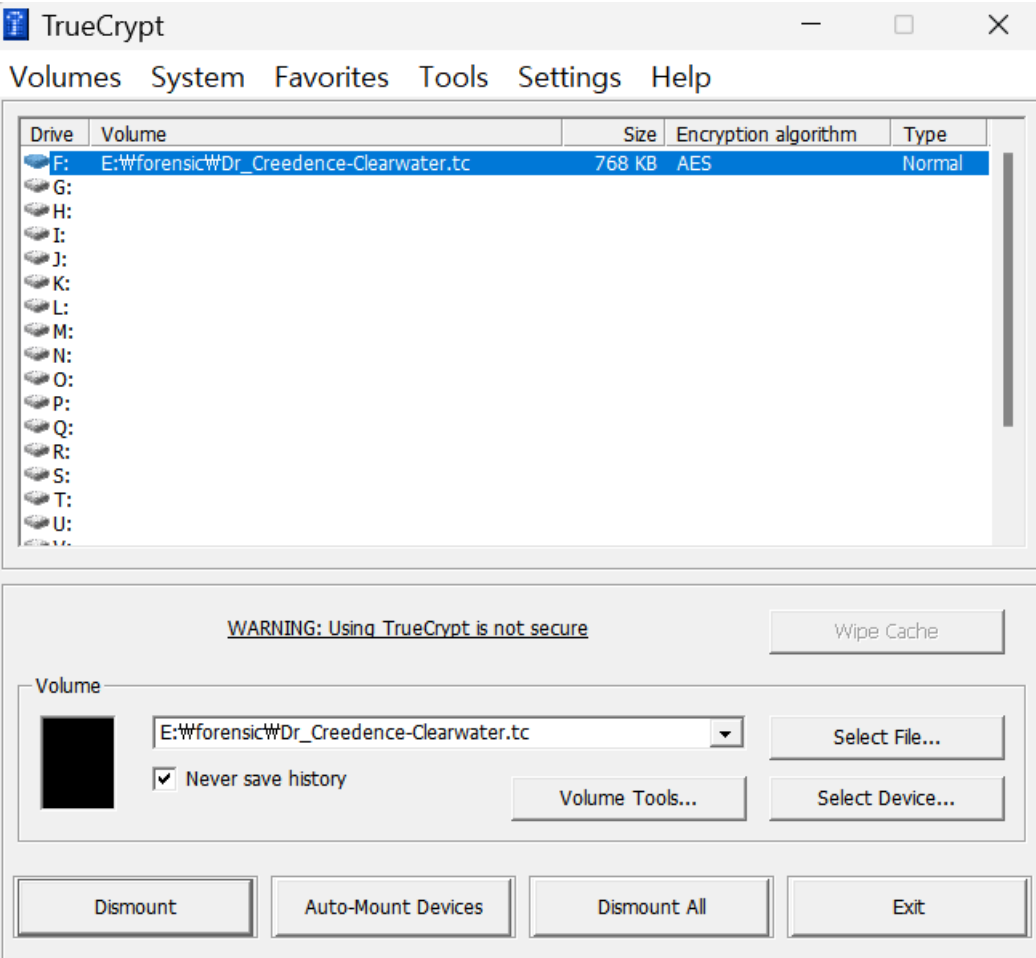
*저작권 2011 Lake Missoula Group, LLC. 판권 소유.*

[사진 29]

1-2  
5-1  
3-8  
4-1  
1-3  
2-3  
1-1  
3-5  
5-5  
4-7

[사진 30]





[사진 31]



[WHS-2] .iso

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	44	65	61	72	20	49	6E	74	65	72	30	70	74	69	63	2C	Dear InterOptic,
00000010	20	0A	0A	49	66	20	79	6F	75	20	61	72	65	20	72	65	...If you are re
00000020	61	64	69	6E	67	20	74	68	69	73	20	6D	65	73	73	61	ading this messa
00000030	67	65	2C	20	74	68	65	6E	20	79	6F	75	20	6D	75	73	ge, then you mus
00000040	74	20	68	61	76	65	20	65	73	63	61	70	65	64	2E	20	t have escaped.
00000050	43	6F	6E	67	72	61	74	73	2E	20	59	6F	75	20	64	69	Congrats. You di
00000060	64	6E	27	74	20	74	68	69	6E	6B	20	74	68	61	74	20	dn't think that
00000070	49	20	77	61	73	20	67	6F	69	6E	67	20	74	6F	20	6C	I was going to l
00000080	65	74	20	79	6F	75	20	68	61	76	65	20	74	68	65	20	et you have the
00000090	69	6E	67	72	65	64	69	65	6E	74	73	20	74	6F	20	74	ingredients to t
000000A0	68	65	20	31	33	33	74	20	70	69	6C	6C	2C	20	64	69	he l33t pill, di
000000B0	64	20	79	6F	75	3F	20	41	73	20	79	6F	75	20	68	61	d you? As you ha
000000C0	76	65	20	70	72	6F	62	61	62	6C	79	20	67	75	65	73	ve probably gues
000000D0	73	65	64	2C	20	49	20	6F	62	74	61	69	6E	65	64	20	sed, I obtained
000000E0	74	68	65	20	63	72	65	64	69	74	63	61	72	64	20	6E	the creditcard n
000000F0	75	6D	62	65	72	73	20	61	6E	64	20	74	68	65	20	69	umbers and the i
00000100	6E	67	72	65	64	69	65	6E	74	73	20	6F	66	20	74	68	ngredients of th
00000110	65	20	31	33	33	74	20	70	69	6C	6C	20	6D	79	73	65	e l33t pill myse
00000120	6C	66	2C	20	61	6E	64	20	73	6F	6C	64	20	74	68	65	lf, and sold the
00000130	6D	20	66	6F	72	20	61	20	76	65	72	79	20	6E	69	63	m for a very nic
00000140	65	20	70	72	6F	66	69	74	2E	20	0A	0A	4A	75	73	74	e profit. ...Just
00000150	20	69	6E	20	63	61	73	65	20	79	6F	75	20	61	72	65	in case you are
00000160	20	63	75	72	69	6F	75	73	2C	20	74	68	65	20	6D	69	curious, the mi
00000170	73	73	69	6E	67	20	69	6E	67	72	65	64	69	65	6E	74	ssing ingredient
00000180	20	66	6F	72	20	74	68	65	20	31	33	33	74	20	70	69	for the l33t pi
00000190	6C	6C	20	77	61	73	20	22	32	6F	7A	20	56	6F	64	6B	ll was "2oz Vodk
000001A0	61	2E	22	20	0A	0A	49	74	20	77	61	73	20	67	72	65	a." ..It was gre
000001B0	61	74	20	77	6F	72	6B	69	6E	20	77	69	74	68	20	79	at workin with y
000001C0	6F	75	2C	20	6D	79	20	70	61	77	6E	2E	20	0A	0A	58	ou, my pawn. ...X
000001D0	4F	58	4F	2C	0A	0A	41	6E	6E	0A							OXO,..Ann.

[사진 32]

5. Flag

- 1. Factory-Made-Winning-Pharmaceuticals
- 2. 현재 존재하지 않는 페이지라 확인 불가 – (원본 답 : 2011 년 10 월 6~7 일)
- 3. rom127#
- 4. Jason Wilson
- 5. 8.4 oz- Red Bull; Tim
- 6. 4

## [WHS-2] .iso

- **Decryption Key**

1. r0und1g0!!입니다.
2. !n1c3?w0rk 입니다.
3. ?g3tting!t0ugh
4. m4k1ng?pr0g
5. 0v3r#h4lf?w4y
6. ch33rs!0n3\$m0r3

## 6. 별도 첨부

### - 문제 (원본)

The lead chemist of a high-profile pharmaceutical company was involved in a serious accident, leaving him in a coma days before the release of the company's highly publicized "133t pill." The chemist was the only person in possession of the list of ingredients required to produce the wonder drug, and it is not known if he will ever recover. All chemical evidence of the drug has been destroyed, but the company believes that the missing ingredients may have been stored electronically. You have been hired as a forensic investigator, to recover the final ingredient of their 133t pill. Can you find the missing ingredient?

1. What is the name of the Company being attacked?
2. What is the date, as it appears in the capture, of the cryptographer's speaking engagement?  
(hint: It isn't at Defcon)
- 3 What is Romulus' password?
4. What is the 16th name inside the mysterious file transfered?
5. What is the 3rd ingredient on the list from the mysterious file that was transfered?
6. What is the final ingredient?

### - 문제 (번역본)

세간의 이목을 끄는 제약회사의 수석 화학자가 중대한 사고를 당해 회사의 세간의 이목을 끄는 "133t 알약"이 출시되기 며칠 전에 혼수상태에 빠졌습니다. 이 화학자는 원더 의약품을 생산하는데 필요한 성분 목록을 가지고 있는 유일한 사람이었고, 그가 언제 회복될지는 알 수 없습니다. 이 약의 화학적 증거는 모두 파괴되었지만, 회사는 사라진 성분이 전자적으로 저장되었을 수 있다고 믿고 있습니다. 당신은 그들의 133t 알약의 최종 성분을 회수하기 위해 법의학 수사관으로 고용되었습니다. 당신은 사라진 성분을 찾을 수 있나요?

1. 공격을 받고 있는 회사의 이름은 무엇입니까?
2. 캡처에 나타난 것처럼 암호학자의 대화 참여 날짜는 언제입니까? (힌트: Defcon 에는 없습니다.)
3. 로물루스의 비밀번호는?
4. 전송된 의문의 파일 안에 있는 16 번째 이름은 무엇입니까?
5. 전송된 의문의 파일에서 목록의 세 번째 성분은 무엇입니까?
6. 최종 재료는 무엇입니까?

## 7. Reference

- 블로그 : videosnarf - pcap 파일에서 h264 패킷을 추출하여서 264 파일로 저장하는 프로그램  
<https://blog.naver.com/websearch/70155889283>
- Chat GPT  
<https://chatgpt.com/>