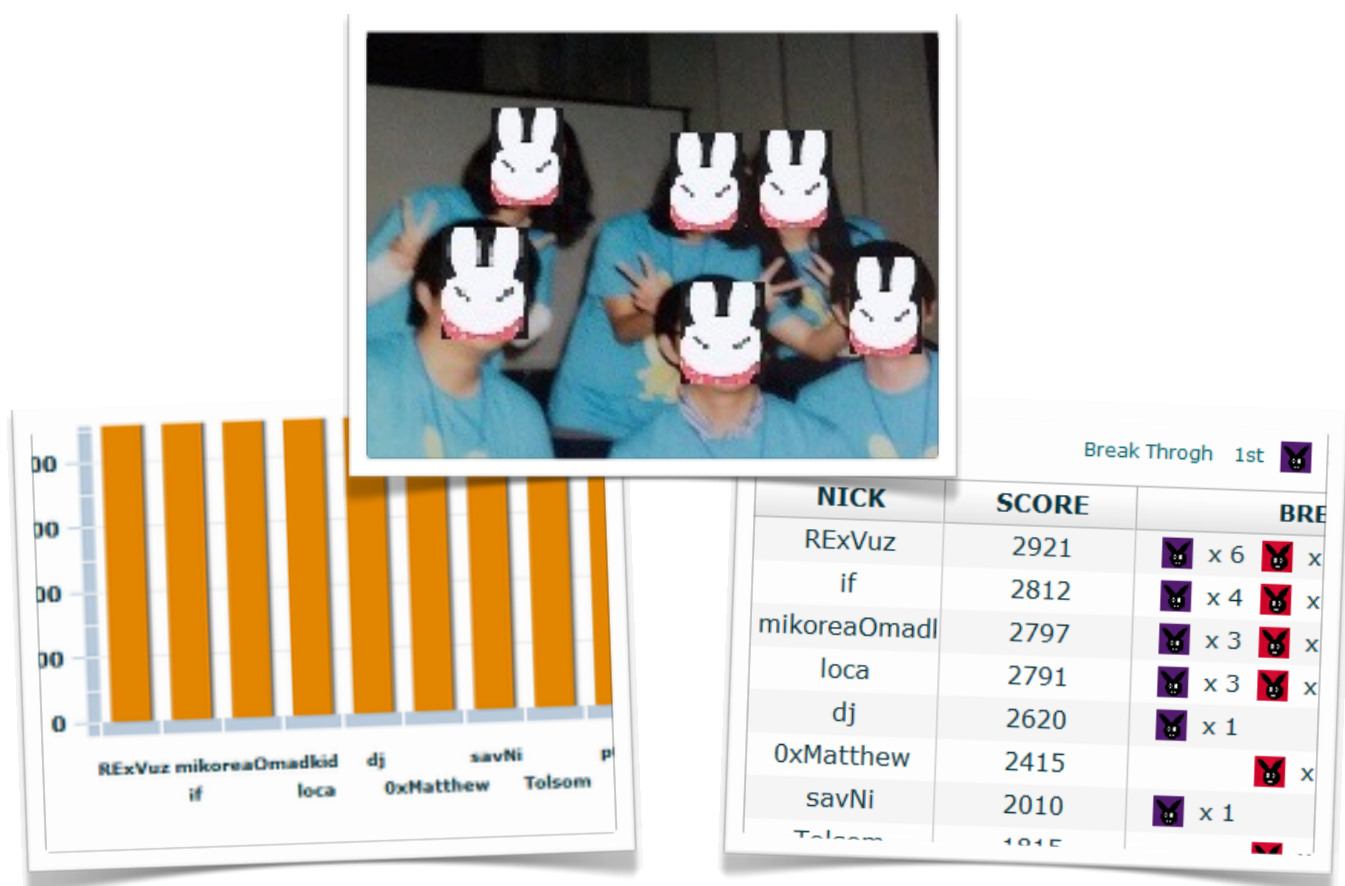


# Hack the Packet

## 2012 Prequals Write-up



김 창 엽 (0xMatthew@HighFive)

Security Researcher & Forensic Analyst @ A-FIRST Team AhnLab,Inc.

2012년 11월 3일

## 들어가기 전에...

먼저 예선을 6위로 마감하였는 데, 허접한 저에게 본선으로 갈 수 있게 양보 해주신 **mikoreaOmadkid** 님께 감사의 말씀을 드립니다....^^

대회가 주말이었다면 더 좋았을 텐데(프리하니까...ㅜㅜ) 갑자기 일이 생겨 9시반 부터 참여가 가능했습니다..다행히(?ㅋ) 서버 문제로 대회 시작 시간이 한 시간 연기되어 운 좋게 참여할 수 있었습니다. 남은 시간 동안 화장실도 안가고 풀었지만 결국 6위로 끝났네요..ㅋ

제가 풀었던 문제 외에 풀지 못했던 문제들 일부 포함해서 작성하였습니다.  
(붉은 색으로 표시 해 두었습니다.)

날씨가 많이 추워졌습니다..

다들 감기 조심하시고... 제발 이번 크리스마스는 이쁜 여자 친구와 보내시길 바랍니다...ㅋㅋㅋ



급하게 작성하느라 그냥 편한 채팅 말투로 작성하였습니다.  
많은 이해 부탁드립니다.. =)

L01

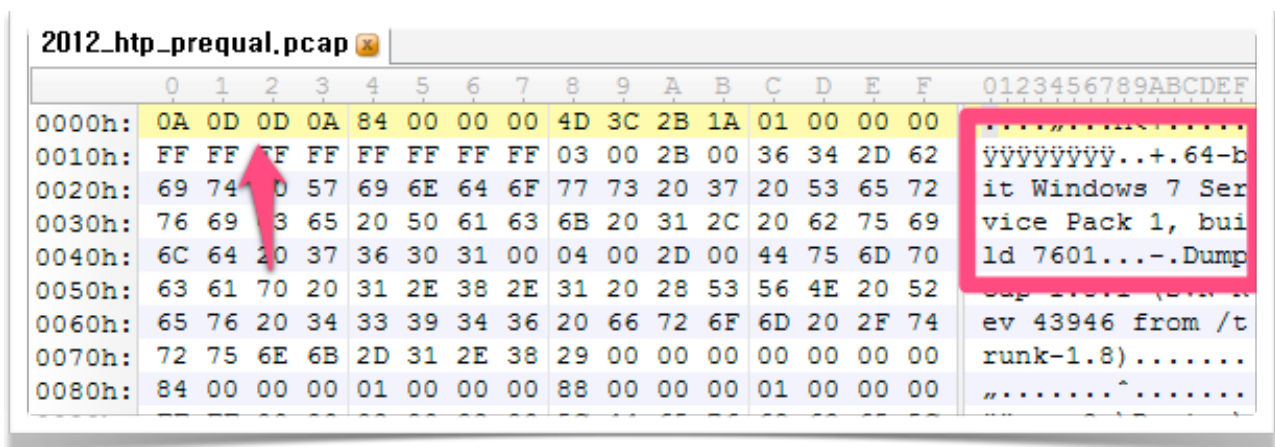
Q 2012\_http\_prequal.pcap 파일은 어떤 환경(System Information)에서 캡처한 것일까?  
EQ Which System be used when this 2012\_http\_prequal.pcap file captured?

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

파일의 수집 환경에 대해 묻는 질문이었습니다.

libpcap 형태에는 없지만 전에 pcap-ng 형태에서는 시스템 정보가 포함된 걸 본 적이 있어 헥스 에디터로 열어 보았습니다.

libpcap 형태에서는 ABCD1234를 뒤집어 놓은 D4 C3 B2 A1 으로 시작하는 데 pcap-ng 포맷 (0A 0D 0D 0A )인 것을 확인했고 오른쪽에 박스친 부분에서 시스템 정보를 확인할 수 있었습니다.



	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	0A	0D	0D	0A	84	00	00	00	4D	3C	2B	1A	01	00	00	00	.....
0010h:	FF	FF	FF	FF	FF	FF	FF	FF	03	00	2B	00	36	34	2D	62	ÿÿÿÿÿÿÿÿ..+.64-b
0020h:	69	74	00	57	69	6E	64	6F	77	73	20	37	20	53	65	72	it Windows 7 Ser
0030h:	76	69	03	65	20	50	61	63	6B	20	31	2C	20	62	75	69	vice Pack 1, bui
0040h:	6C	64	20	37	36	30	31	00	04	00	2D	00	44	75	6D	70	ld 7601...-.Dump
0050h:	63	61	70	20	31	2E	38	2E	31	20	28	53	56	4E	20	52	cap 2012 (S&T)
0060h:	65	76	20	34	33	39	34	36	20	66	72	6F	6D	20	2F	74	ev 43946 from /t
0070h:	72	75	6E	6B	2D	31	2E	38	29	00	00	00	00	00	00	00	runk-1.8).....
0080h:	84	00	00	00	01	00	00	00	88	00	00	00	01	00	00	00	.....^.....

L02

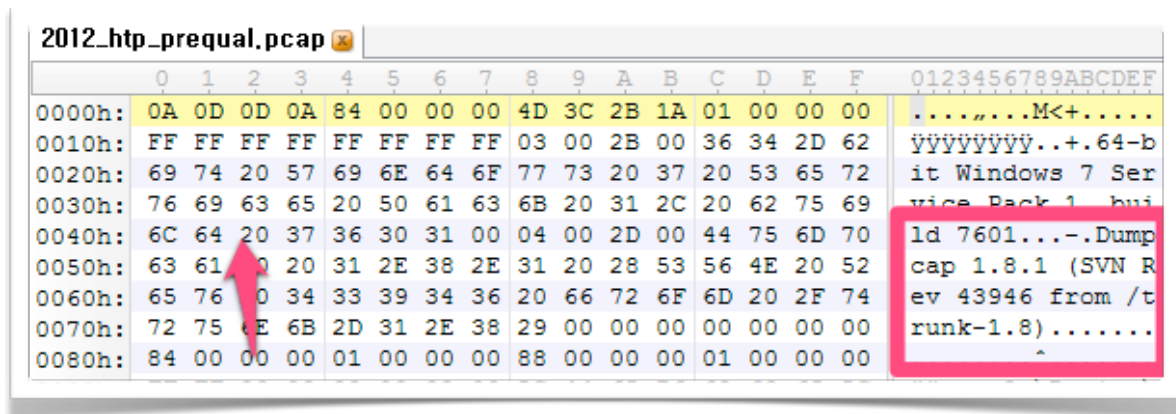
Q 2012\_http\_prequal.pcap 파일은 어떤 도구로 캡처한 것일까? (대문자로 입력)

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

답 : WIRESHARK

대회 초반에는 인증을 못하다가, 운 좋게 맞힌 문제입니다.

위 문제와 마찬가지로 pcap-ng 포맷의 특징으로 수집한 툴 정보가 보이는 데, 답은 Dumpcap 으로 생각했습니다... Dumpcap 뒤로 포함된 괄호 안까지 문자를 전부다 대문자로 바꿔보고 띄어쓰기 만큼 잘라보고, 여러번 인증하였지만 계속 실패하였습니다.



그러다가 설마... 하고 Wireshark를 입력하였더니 인증이 되었습니다.

물론, 지금도 답은 Dumpcap 이라고 우기고 싶네요.. ㄹ ㄹ

Wireshark는 분석 도구고.... 저장할 때 여러 포맷으로 변경하려면 CLI의 editcap, 수집하려면 dumpcap, 여러 패킷을 합치려면 mergecap 등을 사용하지요..

암튼 인증되었으니까 넘어가겠습니다.. =P

## 넘어가기 전에...

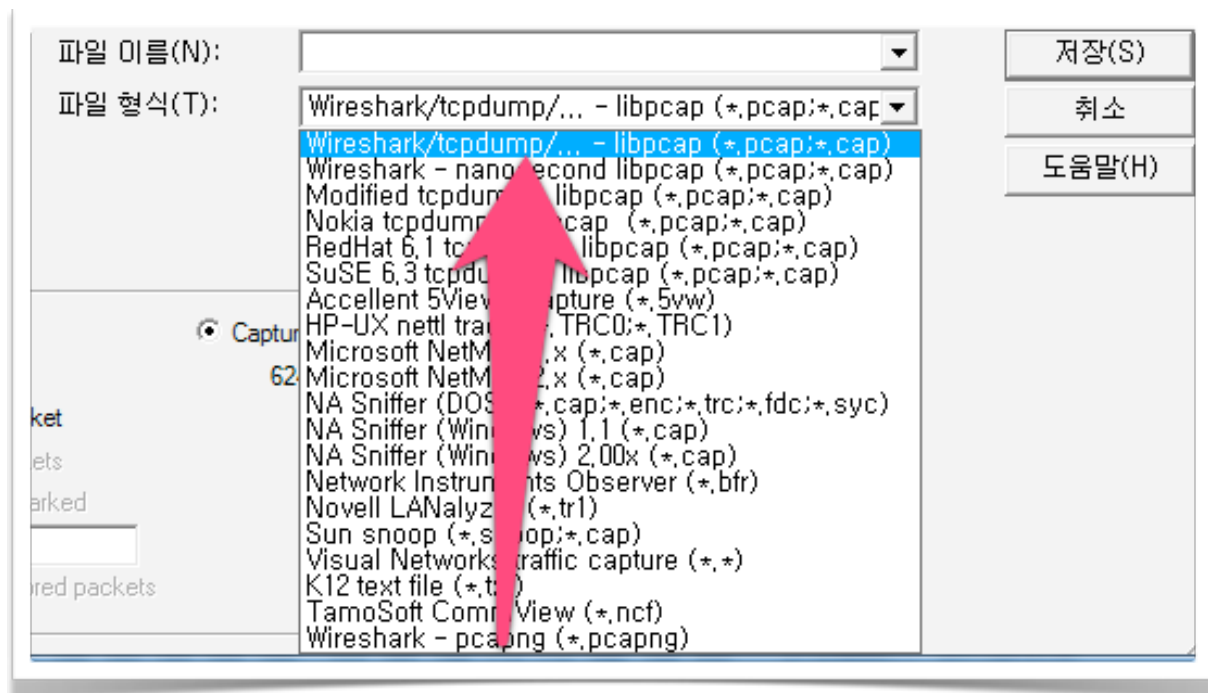
이번 예선에서는 와이어샤크와 Network Miner와 Netwitness Investigator라는 네트워크 포렌식 툴(Network Forensic Analysis Tool,NFAT)을 사용하였습니다.

그 외에도 Xplico 등이 있는 데, 이 툴들은 PCAP파일을 읽어 들일 때 pcap-ng 형태를 불러 들이면 NetworkMiner는 오류 메시지를... Netwitness Investigator, Xplico 는 멍~ 때립니다.

그래서, pcap-ng 포맷을 libpcap 포맷으로 변환해야 합니다.

변환은 여러 방법이 있겠지만 와이어샤크에서 다른 이름으로 저장을 해서 포맷을 변경하거나, CLI에서 editcap을 사용하는 방법이 있습니다.

저는 CLI말고 GUI로 변경하였습니다.



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 Spoofing을 이용하여 공격하는 친구를 먼저 찾아야겠다는 생각으로, 와이어샤크로 열어 보았습니다.

Protocol	Length	Info
SSDP	208	M-SEARCH * HTTP/1.1
ARP	42	who has 192.168.232.1? Tell 192.168.232.131
ARP	42	192.168.232.1 is at 00:50:56:c0:00:08
ARP	42	who has 192.168.232.159? Tell 192.168.232.131
ARP	42	who has 192.168.232.238? Tell 192.168.232.131
ARP	42	who has 192.168.232.80? Tell 192.168.232.131
ARP	42	who has 192.168.232.132? Tell 192.168.232.131
ARP	42	who has 192.168.232.214? Tell 192.168.232.131
ARP	42	who has 192.168.232.196? Tell 192.168.232.131
ARP	42	who has 192.168.232.58? Tell 192.168.232.131
ARP	42	who has 192.168.232.252? Tell 192.168.232.131
ARP	42	who has 192.168.232.114? Tell 192.168.232.131
ARP	42	who has 192.168.232.172? Tell 192.168.232.131
ARP	42	who has 192.168.232.23? Tell 192.168.232.131
ARP	42	who has 192.168.232.195? Tell 192.168.232.131
ARP	42	who has 192.168.232.253? Tell 192.168.232.131
ARP	42	who has 192.168.232.237? Tell 192.168.232.131
ARP	42	who has 192.168.232.177? Tell 192.168.232.131
ARP	42	who has 192.168.232.244? Tell 192.168.232.131
ARP	42	who has 192.168.232.199? Tell 192.168.232.131
ARP	42	who has 192.168.232.249? Tell 192.168.232.131
ARP	42	who has 192.168.232.233? Tell 192.168.232.131

맨 윗 부분에 같은 대역에 여러 IP들에게 대량의 ARP Request 메시지를 뿌리는 192.168.232.131을 확인할 수 있었습니다.

여기서, 공격자는 192.168.232.131인 것을 알 수 있었구요...

그럼.. 시간도 없으니까 간단하게 ip.addr == 192.168.232.131 로 필터를 적용하였습니다.

그럼 HTTP로 통신하는 내역들이 나옵니다..



Filter:	ip.addr == 192.168.232.131		▼ Expression...	Clear	Apply	
	Time	Source	Destination	Protocol	Length	Info
	296	29.4698340	192.168.232.140	192.168.232.13:TCP	62	lonworks > http [SYN] Seq=0 win=65535 Len=0 MSS=1460
	297	29.4702130	192.168.232.131	192.168.232.14:TCP	62	http > lonworks [SYN, ACK] Seq=0 Ack=1 win=14600 Len=0
	298	29.4717910	192.168.232.140	192.168.232.13:TCP	54	lonworks > http [ACK] Seq=1 Ack=1 win=65535 Len=0
	299	29.4721830	192.168.232.140	192.168.232.13:TCP	54	lonworks > http [FIN, ACK] Seq=1 Ack=1 win=65535 Len=0
	300	29.4725050	192.168.232.131	192.168.232.14:TCP	54	http > lonworks [FIN, ACK] Seq=1 Ack=2 win=14600 Len=0
	301	29.4738510	192.168.232.140	192.168.232.13:TCP	54	lonworks > http [ACK] Seq=2 Ack=2 win=65535 Len=0
	304	33.3380940	192.168.232.140	192.168.232.13:TCP	62	lonworks2 > http [SYN] Seq=0 win=65535 Len=0 MSS=1460
	305	33.3384900	192.168.232.131	192.168.232.14:TCP	62	http > lonworks2 [SYN, ACK] Seq=0 Ack=1 win=14600 Len=0
	306	33.3399020	192.168.232.140	192.168.232.13:TCP	54	lonworks2 > http [ACK] Seq=1 Ack=1 win=65535 Len=0
	307	33.3402940	192.168.232.140	192.168.232.13:HTTP	422	GET / HTTP/1.1
	308	33.3406120	192.168.232.131	192.168.232.14:TCP	54	http > lonworks2 [ACK] Seq=1 Ack=369 win=15544 Len=0

그럼 131번과 140번의 통신 내역이 나와있고... HTTP 통신에서 내가 전송하려면 POST 니까 POST Method를 찾아봅니다.

460	82.4259870	192.168.232.140	192.168.232.13:HTTP	893	POST /login.php?login_attempt=1 HTTP/1.1 (appl
461	82.4263130	192.168.232.131	192.168.232.14:TCP	54	http > vmware_f3:21:ad [ACK] Seq=1 Ack=840 win=1
462	82.4296360	192.168.232.131	192.168.232.14:HTTP	363	HTTP/1.1 200 OK (text/html)
Captured (7144 bits)					
, Dst: Vmware_f3:21:ad (00:0c:29:f3:21:ad)					
192.168.232.140), Dst: 192.168.232.131 (192.168.232.131)					
TCP (2546), Dst Port: http (80), Seq: 1, Ack: 1, Len: 839					
Method					
POST /login.php?login_attempt=1 HTTP/1.1 (application/x-www-form-urlencoded)					
Host: 192.168.232.131					
User-Agent: Mozilla/5.0 (Windows NT 6.0; rv:3.0) Gecko/20100603 Firefox/3.0					
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8					
Accept-Language: ko-KR,en-US;q=0.7,en;q=0.3					
Accept-Encoding: gzip, deflate					
Content-Type: application/x-www-form-urlencoded					
Content-Length: 839					
Cache-Control: no-cache					
Connection: close					
Cookie: PHPSESSID=...					
&pass=YONG_GAL&default=1					

그럼 login.php로 전송한 부분이 처음으로 나오고 내용을 보면, pass=YONG\_GAL로 전송한 것을 볼 수 있습니다.

다음으로 공격자의 맥 주소를 찾아야 하고... 위에서 192.168.232.131이 공격자 인 것을 알았으니깐 그 친구의 MAC주소를 확인하면 됩니다. 00:0c:29:f3:21:ad

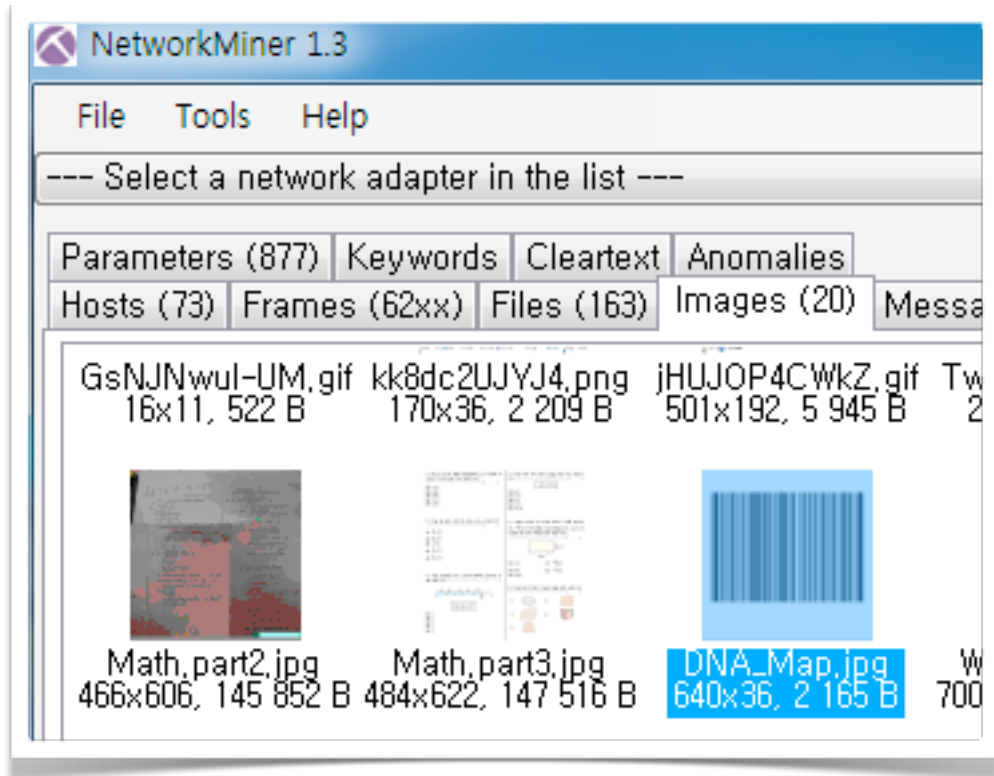
Frame 460: 893 bytes on wire (7144 bits), 893 bytes captured (7144 bits)	
Ethernet II, Src: Vmware_e5:e4:da (00:0c:29:e5:e4:da), Dst: Vmware_f3:21:ad (00:0c:29:f3:21:ad)	
Destination: vmware_f3:21:ad (00:0c:29:f3:21:ad)	
Source: Vmware_e5:e4:da (00:0c:29:e5:e4:da)	
Type: IP (0x0800)	
Internet Protocol Version 4, Src: 192.168.232.140 (192.168.232.140), Dst: 192.168.232.131 (192.168.232.131)	

답 : 00:0c:29:f3:21:ad\_YONG\_GAL

용갈아 밥은 잘 먹고 다니니??

L2

Q. 남자들이 뺏속까지 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!



“넘어가기 전에” 에서 변환한 파일을 Network Miner에서 열어보면 Images 폴더에 DNA\_Map.jpg 파일을 확인할 수 있습니다.

이 파일을 해석하기 위해 구글신께 “online xxxxxxxx decoder” 라는 형태로 online barcode decoder를 물어보았습니다.

그럼, <http://online-barcode-reader.inliteresearch.com/> 사이트를 알려 주고 여기에 DNA\_MAP.jpg를 올려보면 결과를 알려 줍니다.



online-barcode-reader.inliteresearch.com

**Inlite** COMPANY PRODUCTS DOWNLOAD

## ClearImage Free Online Barcode Reader / Decoder

Select barcode types to decode. Learn more about [barcode types](#).

☒ 1D Barcodes
 ☐ PDF417
 ☐ Postal Barcodes

☐ DataMatrix
 ☐ QR
 ☐ Driver License/ID Card

Select Image File Use single- or multi-page PDF or TIFF, JPEG, BMP, GIF, PNG. Maximum file size: 10MB.

파일 선택 DNA\_Map.jpg

**READ BARCODES**

## ClearImage Free Online Barcode Reader / Decoder

[Download barcode and image data](#) in XML format or request help from barcode expert.

File: DNA\_Map.jpg Pages: 1 Barcodes: 1 [New File](#)

Barcode: 1 of 1 Type: Code93 Page 1 of 1

Length: 11 Rotation: none

Module: 3.0pix Rectangle: {X=34,Y=5,Width=570,Height=22}

**Key: IU Good**

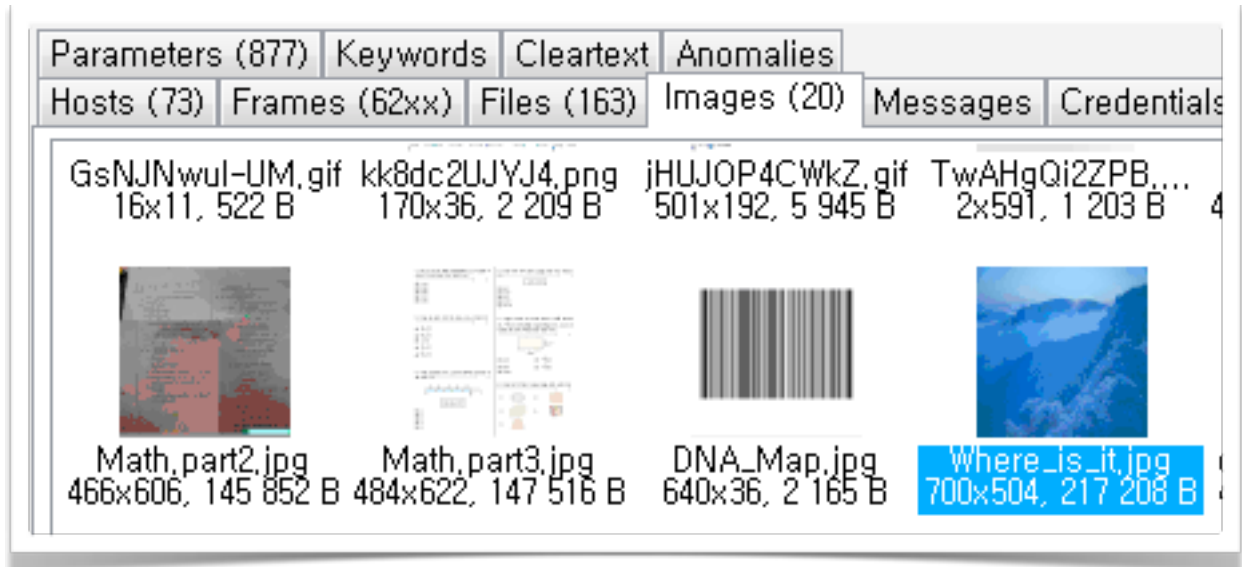
답 : IU Good

But, Suzy is the best.

L4 Q. 우탱아, 가을인데 단풍놀이 가야지~ 어디로 갈까?

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

where is it 으로 물어 보셨고... Network Miner Image 탭에서 where\_is\_it.jpg를 확인할 수 있었습니다.



JPG에 EXIF로 GPS 정보가 담겨 있을 까 하고 살펴 보았지만 없었습니다.

그래서 이번에도 구글신께 물었습니다.

다 아시겠지만 내 이미지를 올려서 찾을 수 있는 기능이 있고 구글 이미지에서 아래 사진을 누르면 됩니다~



파일을 업로드 해보면, 해당 이미지와 일치하는 것을 찾을 수 있습니다.

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 ...

김봉선 작가 님이 “Hallasan” 에서 찍은 사진인 것 같습니다.

답 : hallasan

흑돼지 먹으러 같이 가자 우탱아..

L5

Q 악성 다운로드

EQ Malware Downloader

HttpGetNormal	-eXzfKGI5Cz.js,x-javascript	x-javascript	44 608 B	2012-1...	b,static.ak.fbcdn.net/rsrc....
HttpGetNormal	noexe.exe,x-msdownload	x-msdownload	30 720 B	2012-1...	192.168.100.200/noexe.exe
...	neohelp.exe.zip	zip	245 B	2012-1...	neohelp.exe.zip

Network Miner에서 HTTP 형태로 noexe.exe를 받아오는 것을 볼 수 있었습니다.

캡처 부분에는 없지만 Network Miner에서는 제일 왼쪽에 Frame 번호가 있습니다. (2800)

The screenshot shows a list of network frames in Network Miner. Frame 2800 is highlighted in blue. A right-click context menu is open over frame 2800, with the option 'Follow TCP Stream' selected and highlighted in blue. The menu also includes options like 'Mark Packet (toggle)', 'Ignore Packet (toggle)', 'Set Time Reference (toggle)', 'Manually Resolve Address', 'Apply as Filter', 'Prepare a Filter', 'Conversation Filter', 'Colorize Conversation', 'SCTP', and 'Follow TCP Stream'.

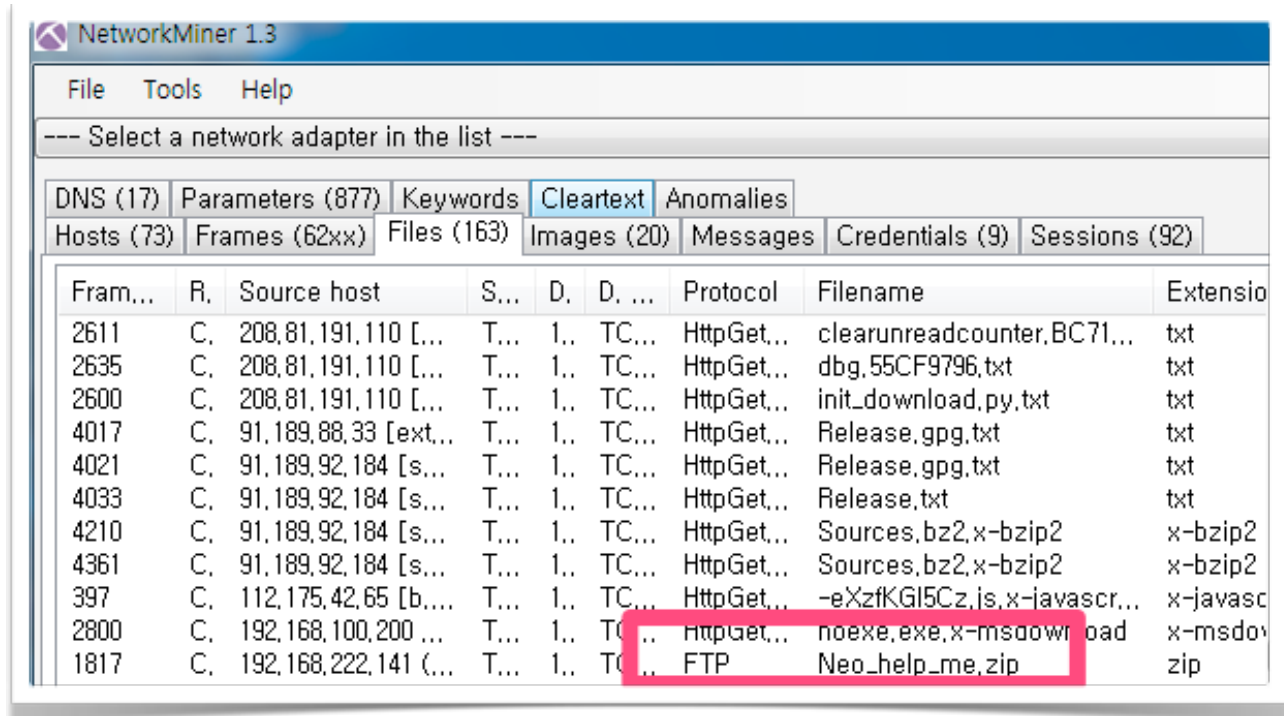
2800 번 Frame으로 이동하여 Follow TCP Stream 을 해보았습니다.

The screenshot shows the 'Follow TCP Stream' window. The 'Stream Content' tab is active, displaying the raw data of the selected frame. The text 'An\$w3r is HTP\_Forever@^^@~' is highlighted in a red box. Below this, there are several lines of error messages, including 'Stack memory around \_alloca was corrupted', 'A local variable was used before it was initialized', and 'Stack memory was corrupted'. The window title is 'Follow TCP Stream'.

마우스 휠을 돌리다 보면 꼬부랑글씨들이 막 보이기 시작하는 데, 제일 위에 보면 답처럼 생긴 문자열을 확인할 수 있습니다.

답 : An\$w3r is 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...



NetworkMiner 1.3

File Tools Help

--- Select a network adapter in the list ---

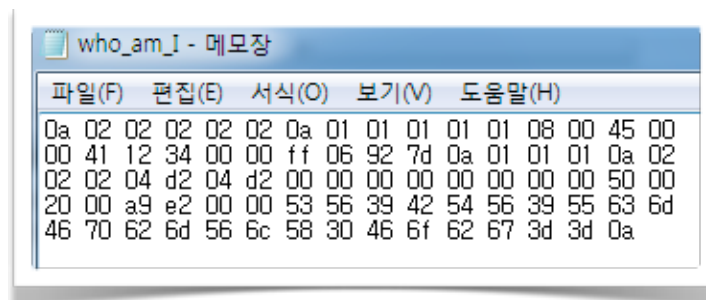
DNS (17) Parameters (877) Keywords Cleartext Anomalies

Hosts (73) Frames (62xx) Files (163) Images (20) Messages Credentials (9) Sessions (92)

Fram...	R.	Source host	S...	D.	D. ...	Protocol	Filename	Extensio
2611	C.	208,81,191,110 [...]	T...	1..	TC...	HttpGet...	clearunreadcounter,BC71...	txt
2635	C.	208,81,191,110 [...]	T...	1..	TC...	HttpGet...	dbg,55CF9796.txt	txt
2600	C.	208,81,191,110 [...]	T...	1..	TC...	HttpGet...	init_download.py.txt	txt
4017	C.	91,189,88,33 [ext...	T...	1..	TC...	HttpGet...	Release.gpg.txt	txt
4021	C.	91,189,92,184 [s...	T...	1..	TC...	HttpGet...	Release.gpg.txt	txt
4033	C.	91,189,92,184 [s...	T...	1..	TC...	HttpGet...	Release.txt	txt
4210	C.	91,189,92,184 [s...	T...	1..	TC...	HttpGet...	Sources,bz2,x-bzip2	x-bzip2
4361	C.	91,189,92,184 [s...	T...	1..	TC...	HttpGet...	Sources,bz2,x-bzip2	x-bzip2
397	C.	112,175,42,65 [b...	T...	1..	TC...	HttpGet...	-eXzfKG15Cz,is,x-javascr...	x-javascr
2800	C.	192,168,100,200 ...	T...	1..	TC...	HttpGet...	noexe.exe,x-msdown load	x-msdov
1817	C.	192,168,222,141 (...]	T...	1..	TC...	FTP	Neo_help_me.zip	zip

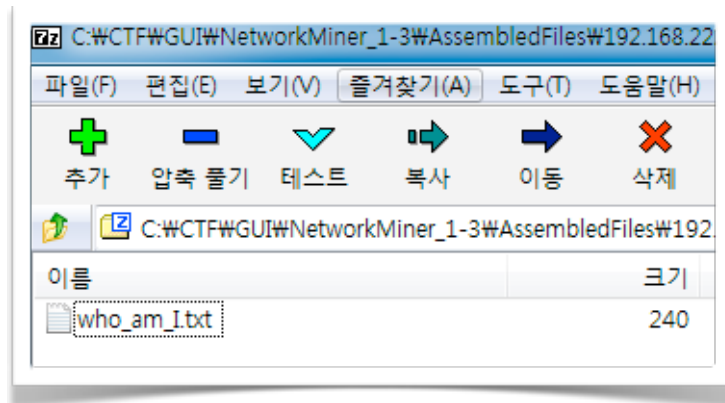
마찬가지로 Network Miner에서 Extension으로 정렬(zip을 찾기 위해...)하면 Neo\_help\_me.zip 을 확인할 수 있었습니다.

압축 암호 없이 who\_am\_i.txt가 있었습니다.



who\_am\_i - 메모장

파일(F)	편집(E)	서식(O)	보기(V)	도움말(H)
0a 02 02 02 02 02 0a 01 01 01 01 01 08 00 45 00				
00 41 12 34 00 00 ff 06 92 7d 0a 01 01 01 0a 02				
02 02 04 d2 04 d2 00 00 00 00 00 00 00 00 50 00				
20 00 a9 e2 00 00 53 56 39 42 54 56 39 55 63 6d				
46 70 62 6d 56 6c 58 30 46 6f 62 67 3d 3d 0a				



who\_am\_I.txt 내용을 Hex Editor에 옮겨 보니 뒷 부분에 Base64로 인코딩 되어 있는 문자열들이 보였습니다.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0000h:	0A	02	02	02	02	02	0A	01	01	01	01	01	08	00	45	00	.....E.															
0010h:	00	41	12	34	00	00	FF	06	92	7D	0A	01	01	01	0A	02	.A.4..ÿ.'}.....															
0020h:	02	02	04	D2	04	D2	00	00	00	00	00	00	00	00	50	00	...Ò.Ò.....P.															
0030h:	20	00	A9	E2	00	00	53	56	39	42	54	56	39	55	63	6D	.@â..SV9BT	V9Ucm														
0040h:	46	70	62	6D	56	6C	58	30	46	6F	62	67	3D	3D	pA		FpbmVlX0F	obg==.														

이 문자들을 발파이션(import base64... print base64.standard\_b64decode("blabla~"))으로 풀어 인증키를 얻을 수 있었습니다.

답 : I\_AM\_Trainee\_Ahn

안랩연수생이 인증키가 될 줄이야.....



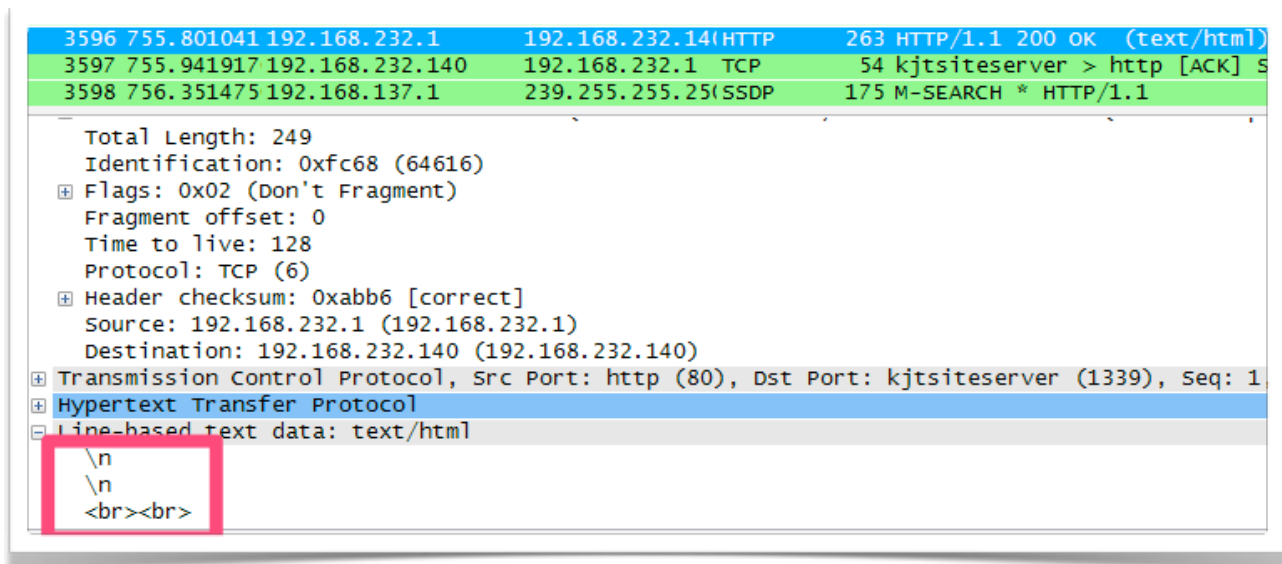
## M2 Q. DB이름을 찾아라! EQ. Fine the name of DataBase

네트워크 패킷 분석 대회에서 데이터베이스라....  
어딘가에 SQL Injection 이 있을 수도 있겠구나 하고 일단 넘어 갔습니다.

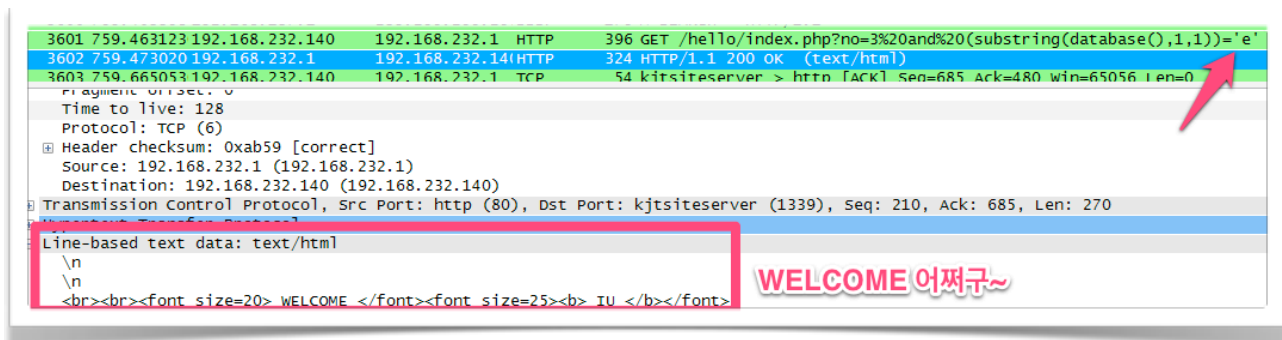
시간이 없어, Network Miner로 훑을 수 있는 문제부터 풀어야 했기에...  
나중에 다시 살펴 보니 substring 을 이용해서 한 문자씩 찾는 걸 찾을 수 있었습니다.  
(Frame 3595 부터~~)

참, 거짓을 확인하기 위해 응답패킷을 확인하였습니다..

거짓인 경우: 첫번째 글자에 'd'로 했을 때



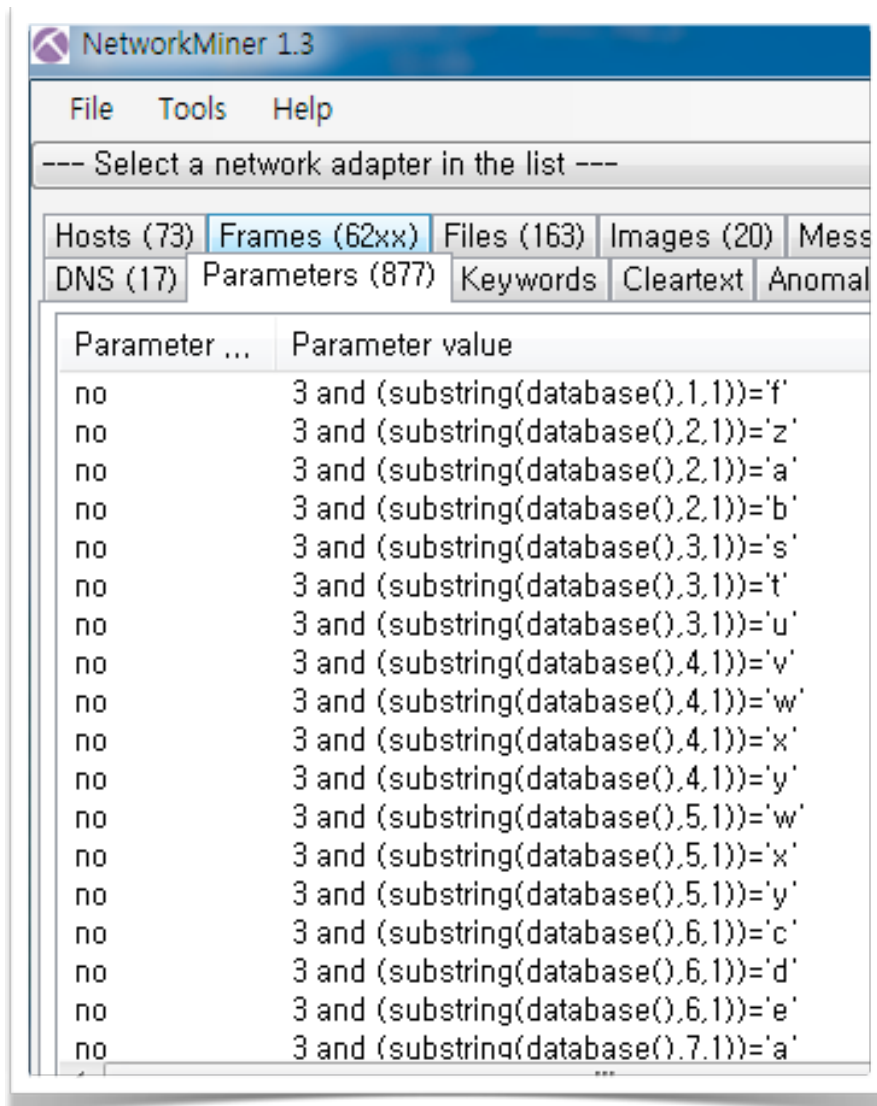
참인 경우: 첫번째 글자는 'e' !!!



위 그림에서는 첫번째 글자가 'e' 임을 알 수 있습니다.

마찬가지로 WELCOME ~~ 로 응답 받을 때 입력한 값을 확인하면 됩니다.

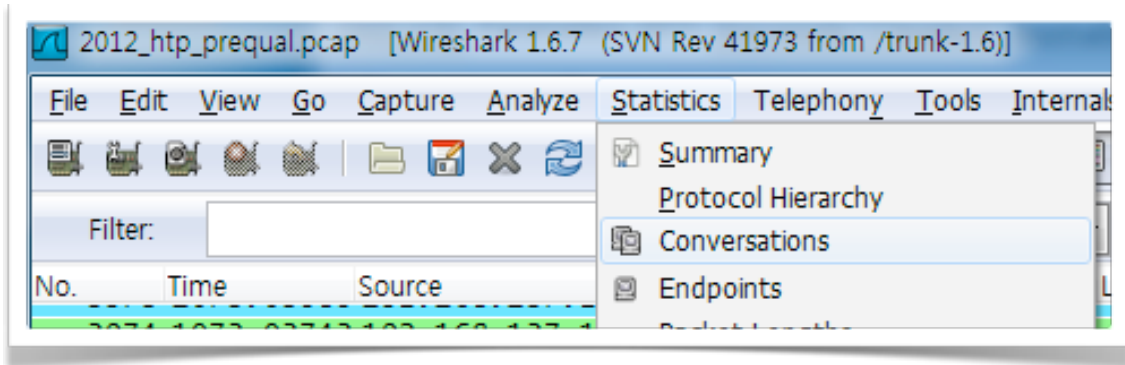
substring(database(),1,1))= 부터 substring(database(),17,1))= 까지 17글자를 확인하면 “easywebsiteattack” 을 찾을 수 있습니다.



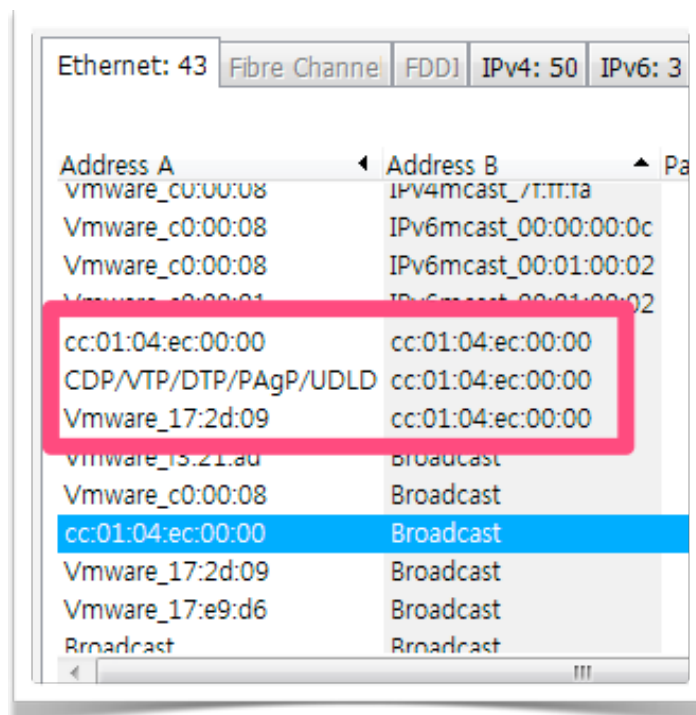
답 : easywebsiteattack

M3 Q. 라우터에 백도어가 삽입되어 있다. 마지막으로 실행된 명령어는?  
EQ. Backdoor injected in Router, what's the last command?

우선 라우터가 통신한 내역을 찾기 위해 Statistics의 Conversations로 가봅니다.

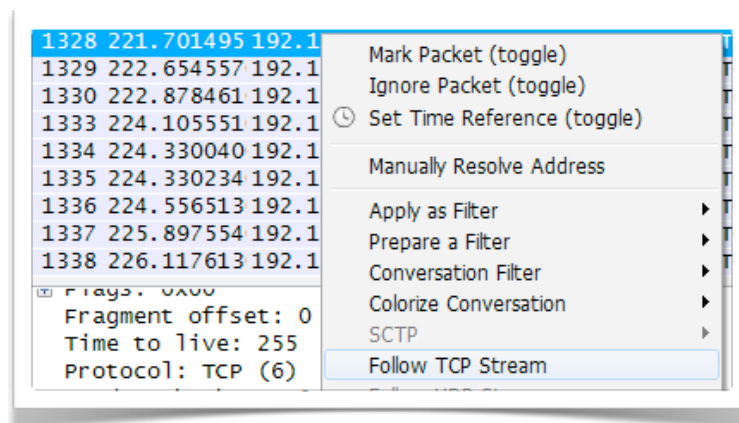
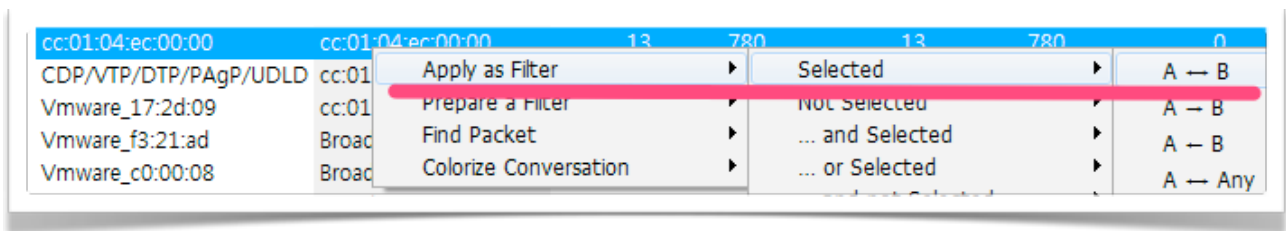


그럼 Ethernet 레이어에서의 주소를 보면, 대부분 Vmware 호스트 간의 통신이거나 멀티캐스트거나 브로드캐스트 인 것을 볼 수 있습니다.

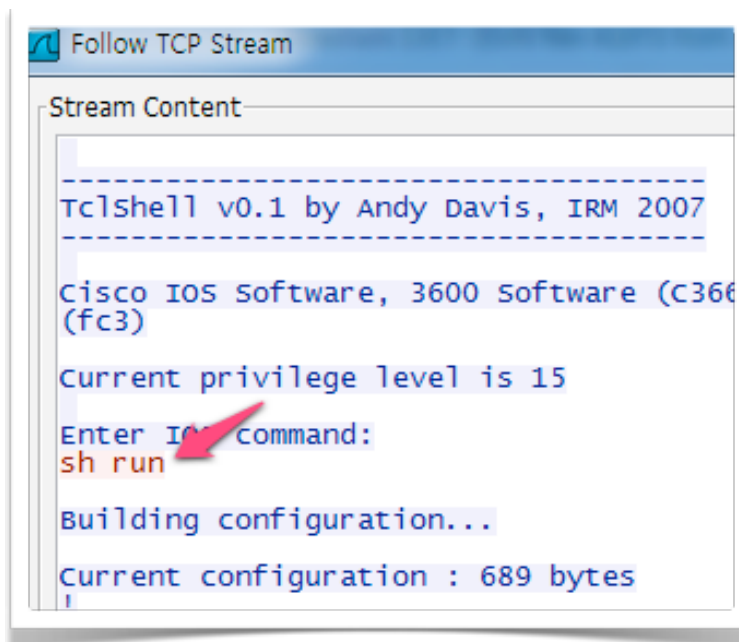


박스 친 부분이 뭔가... 네트워크 장비와 관련된 것이라고 생각해 볼 수 있구요..

제일 위에 항목에서 우클릭해서 필터를 적용하였습니다. 캡처 결과에서 “Follow TCP Stream”을 봅니다.



그럼, Cisco 3600 시리즈 라우터의 설정 내용들을 볼 수 있습니다.. 처음으로는 show running-config를 실행했네요..



마우스 휠을 열심히 내리다 보면.. 마지막에 호스트네임을 변경한 것을 확인할 수 있습니다.

```
!
line con 0
  exec-timeout 0 0
  logging synchronous
line aux 0
line vty 0 4
!
!
end
enable
conf ter
Enter configuration commands, one per line. End with CNTL/Z.
hostname An$w3r_is^tclsh
```

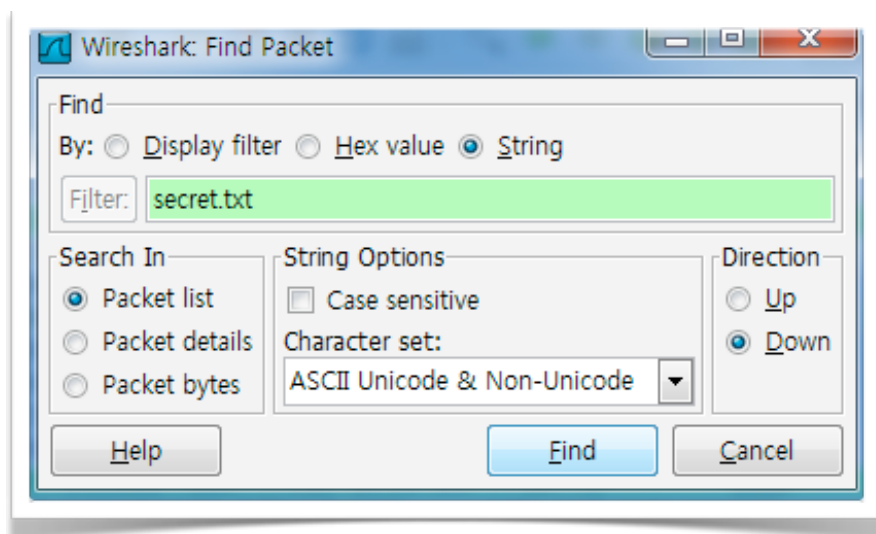
답 : hostname An\$w3r\_is^tclsh

M4 Q. 누군가가 나의 Secret폴더의 내용을 읽었다!  
EQ. Someone read a Secret folder of min!

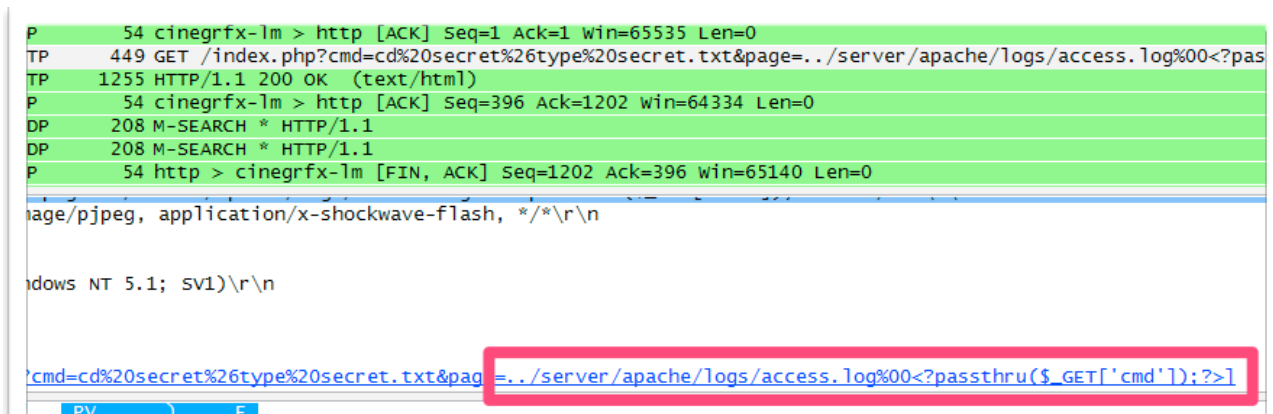
\*\* Key is Secret.txt\_hidden.txt\_pass.txt in Secret Folder  
\*\* hidden is not wrong. it's just typo

문제는 영어로 번역을 해 주는데, 힌트는 한글로 안 바뀌워서 살짝 빠지고 시작했습니다.  
(여기는 대한민국입니다..)

패킷에서 secret.txt , hidden.txt, pass.txt 만 찾으면 되꺼라고 생각을 하고 와이어샤크의 "Find Packet, 컨트롤-에프"을 이용하였습니다.



그럼, 아래 패킷 (Frame : 3452)이 출력되는 데, 아파치 액세스 로그에 로그인섹션을 시도하는 것을 확인할 수 있습니다. cmd 파라미터로 받은 것을 passthru PHP 함수로 실행하도록 했네요.





```

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<?pas
3453 641.844961 192.168.232.1 192.168.232.140 HTTP 1255 HTTP/1.1 200 OK (text/html)
3454 641.991982 192.168.232.140 192.168.232.1 TCP 54 cinegrfx-lm > http [ACK] Seq=3157878767 Win=1202 Len=0
3455 643.104275 fe80::fcd2:e499:83ff02::c ::c SSDP 208 M-SEARCH * HTTP/1.1
[07/oct/2011:18:35:22 +0900] "GET /index.php?page=board HTTP/1.1" 200 729\r\n
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\r\n
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 1968\r\n

```

```

ess.log%00NOOPEN HTTP/1.1" 200 567\r\n
ess.log%00NOOPEN HTTP/1.1" 200 2048\r\n
pache/logs/access.log%00NOOPEN HTTP/1.1" 20

```

응답 패킷을 보면 secret.txt에는 NOOPEN 이 들어 있는 것을 확인할 수 있습니다.

마찬가지로, hidden.txt, pass.txt를 Find Packet으로 찾아보면 됩니다.

```

HELOC HTTP/1.1" 200 2048\r\n
ess.log%00HIDDEN HTTP/1.1" 200 1968\r\n
pache/logs/access.log%00HIDDEN HTTP/1.1" 200 1968\r\n
ne/logs/access.log%00APACHELOG HTTP/1.1" 200 1968\r\n

```

```

%pass.txt HTTP/1.1" 200 1968\r\n
ogs/access.log%00INJECTION HTTP/1.1" 200 1968\r\n
/access.log%00INJECTION HTTP/1.1" 200 11\r\n
gs/access.log%00INJECTION HTTP/1.1" 200 11\r\n

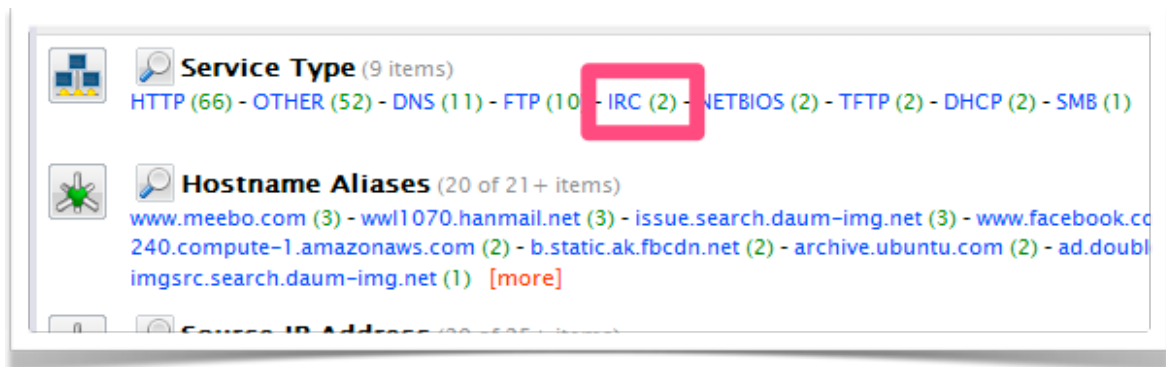
```

답 : 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

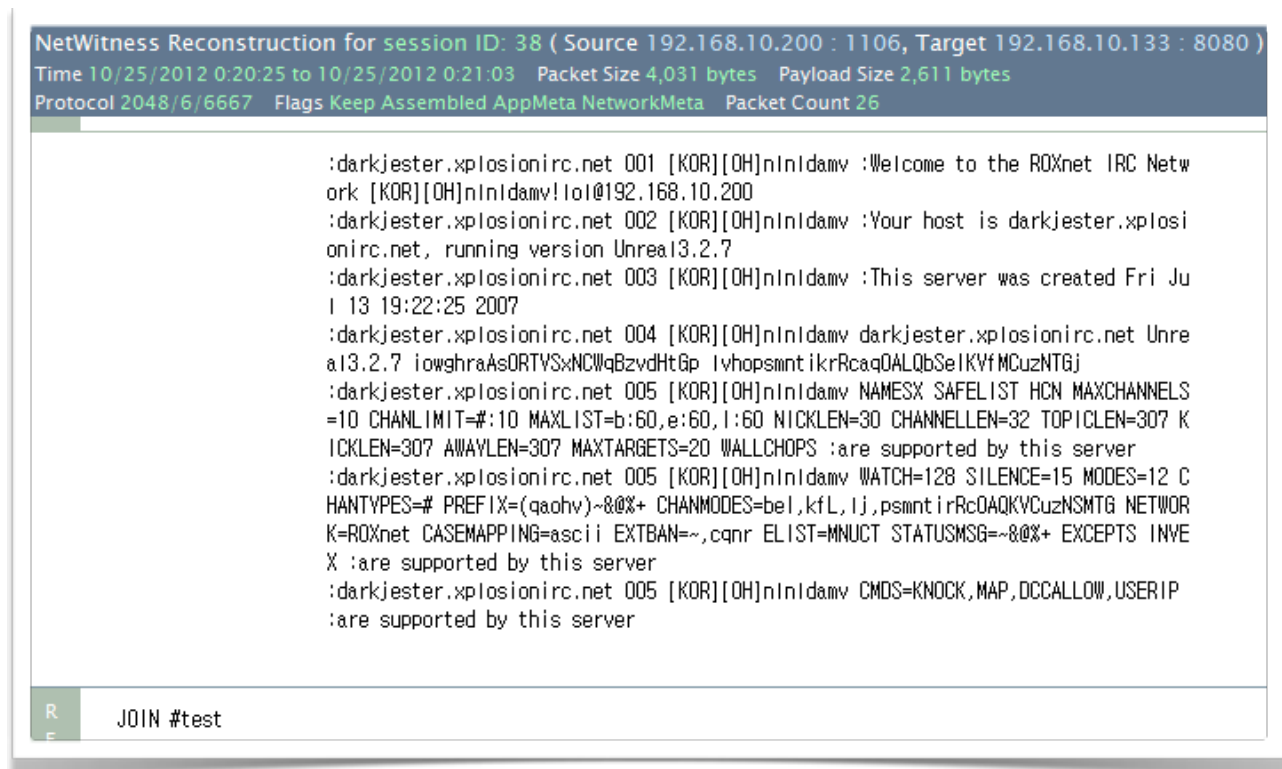
IRC Bot에 감염되었다고 하네요.  
저는 NetWitness Investigator라는 NFAT 툴로 풀어보았습니다.

이 툴의 장점은 프로토콜을 해석하고 여러 기준이나 헤더에 있는 데이터 들로 인덱싱을 해주는 것입니다.

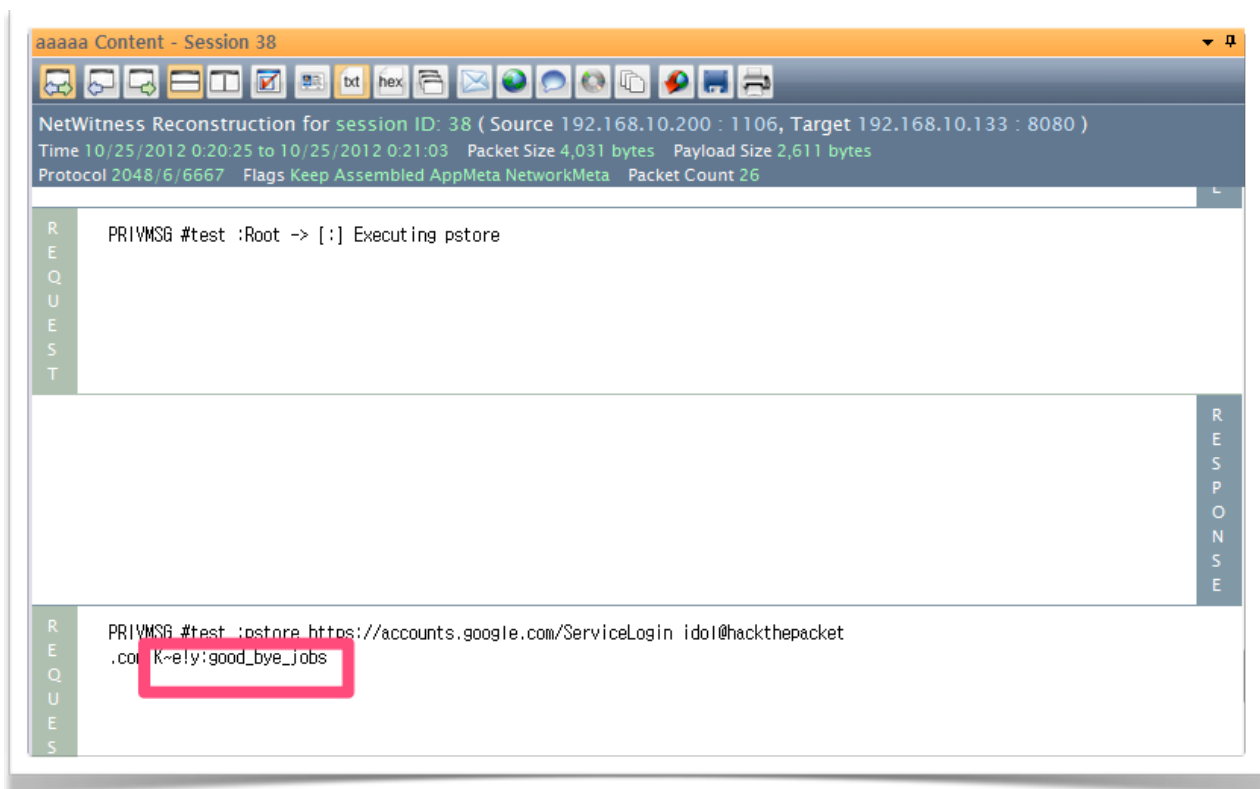


IRC로 통신한 흔적이 2건이 있습니다.

내용을 살펴 보면 IRC를 통해 뭔가 주고 받고, shadow bot과 관련되었다는 것을 알게 됩니다.



밑으로 계속 내려가보면..



pstore를 실행하는 것과 계정 정보를 보내는 것을 확인할 수 있습니다.

답 : good\_bye\_jobs

M7 Q : chakyi는 원격지 시스템에 매일 일정한 시간에 프로그램이 자동으로 실행되도록 만들었다. chakyi가 실행시키고자 하는 명령을 찾아라. (대회 때 못푼 문제)

EQ : chakyi has a program running automatically on a remote system in a daily basis. Find out the 'command'.

이 문제는 지문만 읽고도 풀 엄두가 나지 않았습니다.  
대회가 끝나고 나서 천천히 보다 보니 SMB 트래픽 중에 다음과 같은 내용 들이 있었습니다.

Source	Destination	Protocol	Length	Info
192.168.10.75	192.168.10.77	SMB	380	Session Setup AndX Request, NTLMSSP_AUTH, User: TEST-75\Administrator
192.168.10.77	192.168.10.75	SMB	175	Session Setup AndX Response
192.168.10.75	192.168.10.77	SMB	138	Tree Connect AndX Request, Path: \\TEST-77\IPC\$
192.168.10.77	192.168.10.75	SMB	114	Tree Connect AndX Response
192.168.10.75	192.168.10.77	SMB	142	Tree Connect AndX Request, Path: \\TEST-77\ADMIN\$
192.168.10.77	192.168.10.75	SMB	118	Tree Connect AndX Response
192.168.10.75	192.168.10.77	SMB	156	[TCP ACKed lost segment] [TCP Previous segment lost] NT Create AndX Request, FID: 0x4002
192.168.10.77	192.168.10.75	SMB	193	NT Create AndX Response, FID: 0x4002
192.168.10.75	192.168.10.77	DCERPC	214	Bind: call_id: 1 Fragment: Single ATSVc v1.0
192.168.10.77	192.168.10.75	DCERPC	202	BindAck: call_id: 1 Fragment: Single accept max_xmit: 4280 max_recv: 4280
192.168.10.75	192.168.10.77	ATSVC	290	JobAdd request
192.168.10.77	192.168.10.75	ATSVC	146	JobAdd response
192.168.10.75	192.168.10.77	SMB	80	Close Request, FID: 0x4002
192.168.10.77	192.168.10.75	SMB	93	Close Response, FID: 0x4002

AT (예약된 작업) 서비스로 작업을 등록하고 응답을 받는 패킷이었습니다.

1849	321.684985	192.168.10.75	192.168.10.77	ATSVC	290 JobAdd request
1850	321.735901	192.168.10.77	192.168.10.75	ATSVC	146 JobAdd response

[Response in frame: 1850]

- ☞ Pointer to Servername (uint16): \\TEST-77
- ☞ Pointer to Job Info (atsvc\_JobInfo)
  - ☞ JobInfo
    - Job Time: 64800000
    - ☞ Days Of Month: 0x00000000: (No values set)
    - ☞ Days Of week: 0x7f: DAYSOFWEEK\_MONDAY, DAYSOFWEEK\_TUESDAY, DAYSOFWEEK\_WEDNESDAY, DAYSOFWEEK\_THURSDAY
    - ☞ Flags: 0x11: JOB\_RUN\_PERIODICALLY, JOB\_NONINTERACTIVE
    - ☞ Pointer to Command (uint16): rundll32.exe redhidden,\_main\_
      - Referent ID: 0x019efc48

Request 패킷을 보니 매일매일 반복 실행되도록 하였으며, 실행하는 명령어는 rundll32.exe redhidden,\_main\_ 이었네요..

답 : rundll32.exe redhidden,\_main\_ (????)

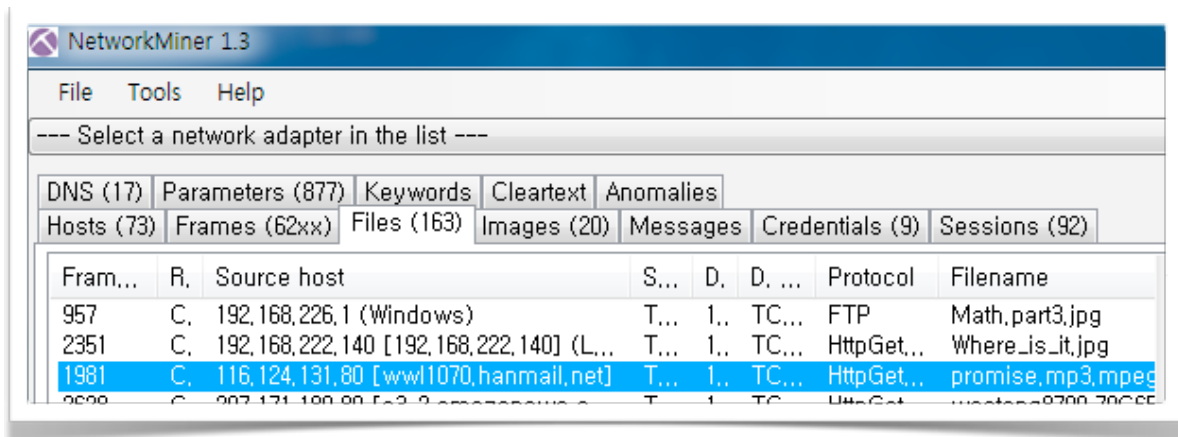
착이님.. 미움.. ㅋ

H1

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

하지만 내용없이 파일만 첨부되어 있었다. 데이트 장소는 언제 몇시에 어디인가?

EQ. SOMEONE GOT A SECRET INFORMATION OF jitae 's FIRST DATE VIA E-MAIL ...  
BUT THRER IS ONLY ONE ATTACHED FILE WITH NOTHING. WHEN AND WHERE?



Network Miner에서 promise.mp3 라는 파일을 확인할 수 있었다.

내용을 보니... “개동이네 버블~버블~”이라는 아주 친숙한 목소리가 들렸다..  
목소리가 변조되었다고 하더라도 주말만 빼고 매일 만나는 개구리님의 목소리 같았다.  
그래서 답았다.. 이 문제는 못 풀것 같았고 그냥 버리기로 했다.



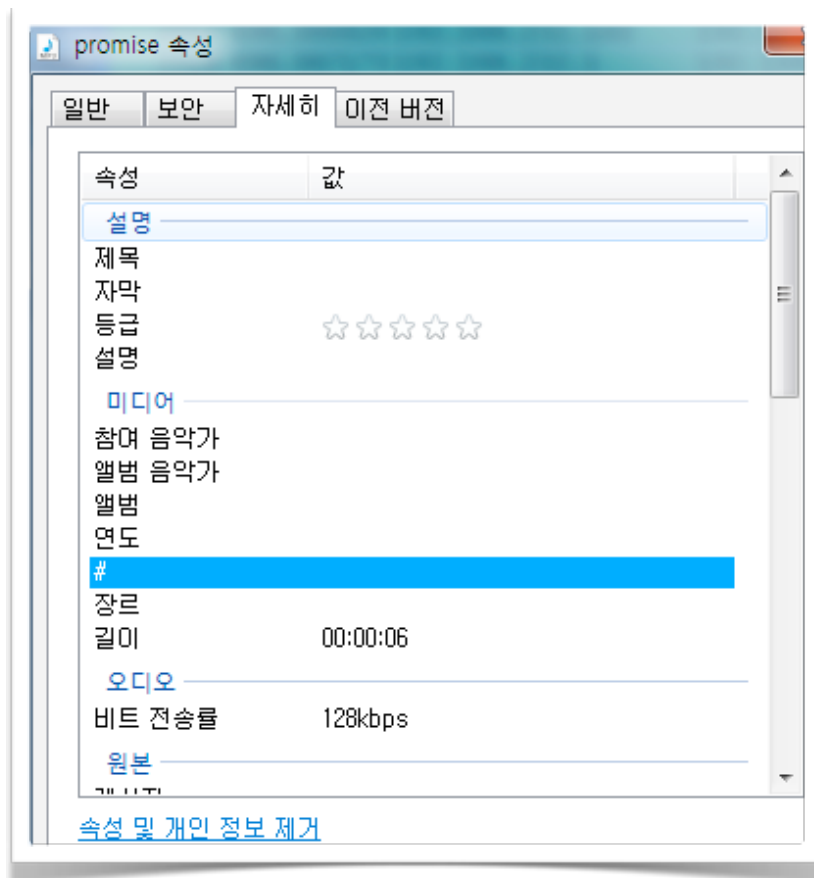
그러다가 페이스북에서 위 힌트를 확인했다...

MP3에 스테가노그래피.... 그럼 MP3Stego나 해보자 하면서 시도를 해봤다.  
(Hack-me.org에서 유사한 문제가 있어 옵션에 대해서는 알고 있었다..)

decode.exe -X -P “패스워드”

그럼 패스워드가 될만한 것들을 찾아 봤다.

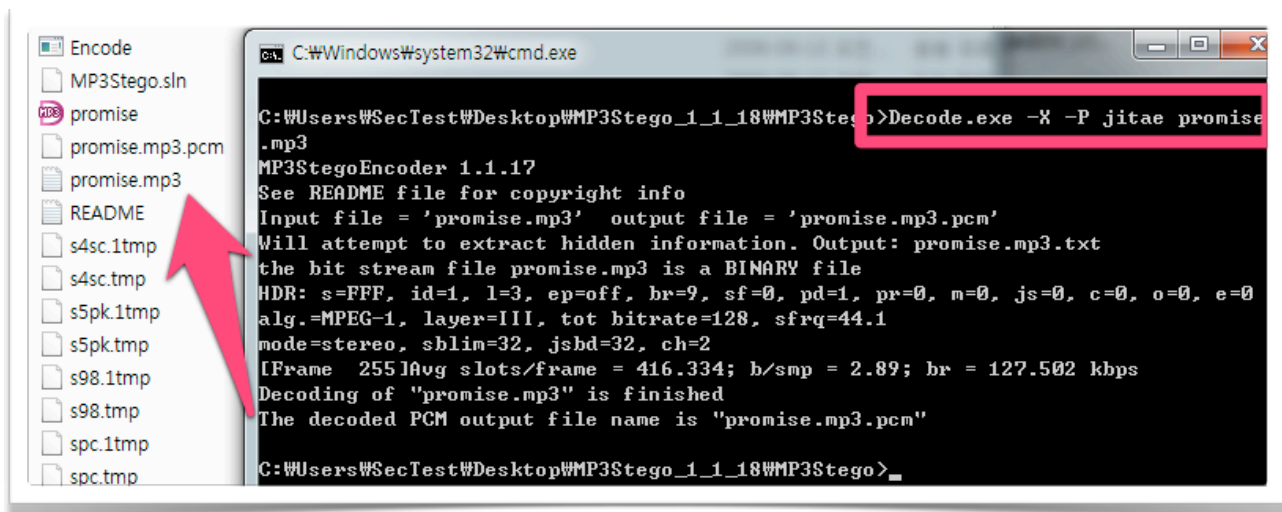
Hack-me.org처럼 ID3 태그에 숨겼는지 확인해 보았다.



역시나 깨끗했다.  
“멘붕”이었다..

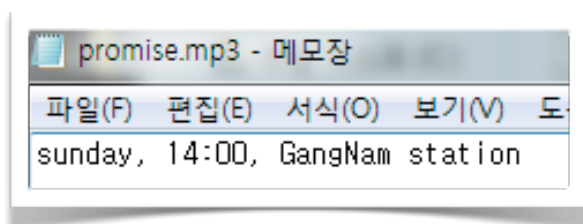
그러다 문제를 다시 읽어보니 “jitae” 라는 문자열이 보았다.. 한국 이름인데 영어로 써놓았다..  
아 이거다 싶었다..

우탱 꼬비 착이 우태혁 등 다 친숙한 이름들인데..





jitae로 해보니 역시 잘 풀렸고 결과 파일로 promise.mp3.txt가 생성되었다. 내용에는 키 값이 들어 있었다.



답 : sunday, 14:00, GangNam station

H2 Q. 수학을 공부 하던 꼬비는 잠이 들었는데, 공식이 다른 이상한 글자들로 바뀌어있는 꿈을 꾸게 되었다. (대회 때 못푼 문제)

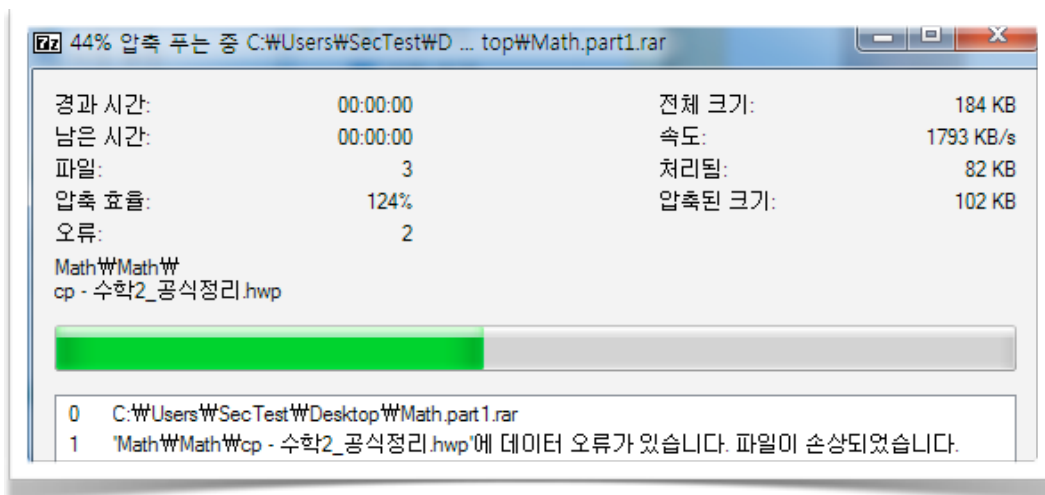
EQ. GGOBI went to sleep in studying math and had a dream that the function replaced with strange words.

대회 때는 Network Miner로 FTP로 전송되는 Math.part1 ~ Part3 파일이 있는 것만 확인하였습니다. 어렸을 때 봤던 시험지들.. 대회 때 시간이 없어 결국 못풀고 끝나고 나서 파일을 헥스에 디터로 열어 보았습니다.

Protocol	Filename	Extension
HttpG...	kk8dc2UJYJ4[1],p...	png
HttpG...	kPX0tjvFAV6[1],c...	css
HttpG...	login.php,C14C5B...	html
FTP	Math.part1[1].jpg	jpg
FTP	Math.part2[1].jpg	jpg
FTP	Math.part3[1].jpg	jpg

헉... FF D9 뒤에 RAR 파일이 붙어 있는 것을 보았습니다. ㅜㅜ

해당 파일을 하나 복구해서 풀어보니 아래와 같이 오류 메시지가 나왔습니다.

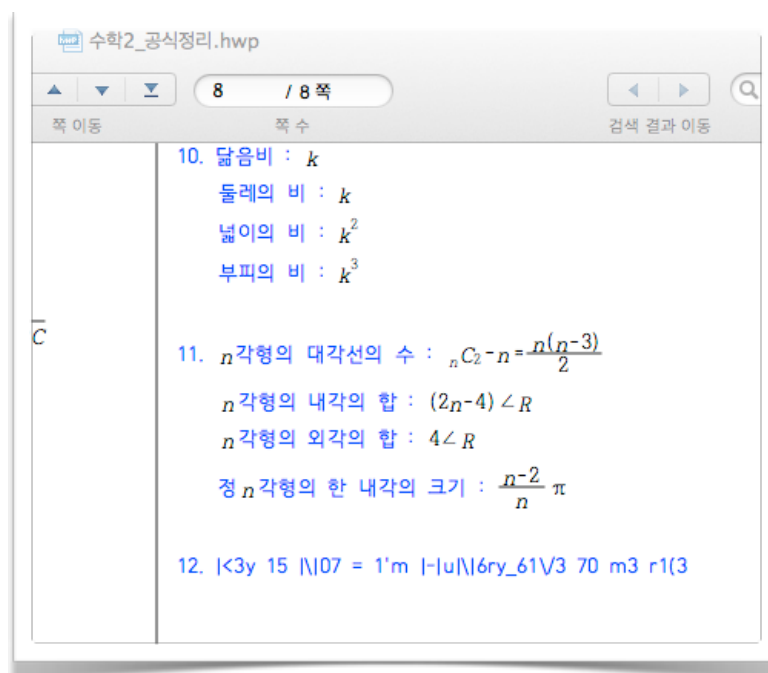


아... 그러면 part라는 게 분할 압축일 수도 있겠구나..

그래서 나머지 파일들도 전부 복구 한 후에 Math.part2.rar, Math.part3.rar라는 이름으로 저장했습니다. 그러니 압축이 정상적으로 풀리면서 다음의 내용들을 담고 있었습니다.

이름	수정한 날짜	유형	크기
cp - 공통수학정리.hwp	2011-10-07 오전...	HWP 파일	36KB
cp - 수학1_공식정리.hwp	2011-10-07 오전...	HWP 파일	47KB
cp - 수학2_공식정리.hwp	2011-10-07 오전...	HWP 파일	102KB
공통수학정리.hwp	2011-10-07 오전...	HWP 파일	36KB
수학1_공식정리.hwp	2011-10-07 오전...	HWP 파일	47KB
수학2_공식정리.hwp	2011-10-07 오전...	HWP 파일	102KB

가장 밑의 수학2\_공식정리.hwp를 열어보니 제일 밑에 줄에 다음의 내용이 있었습니다.



Key is Not 이더군요.....

더 찾아 보니.. 공통수학정리.hwp에 다음 내용이 있습니다.

#### 4. 공통수학공식집

##### ▶대칭이동

- ①  $y=x$ 대칭 :  $f(x,y)=0 \rightarrow f(y,x)=0$
- ②  $y=-x$ 대칭 :  $f(x,y)=0 \rightarrow f(-y,-x)=0$
- ③  $x=a$ 대칭 :  $f(x,y)=0 \rightarrow f(2a-x,y)=0$
- ④  $y=b$ 대칭 :  $f(x,y)=0 \rightarrow f(x,2b-y)=0$
- ⑤  $(a,b)$ 대칭 :  $f(x,y)=0 \rightarrow f(2a-x,2b-y)=0$
- ⑥ 직선  $y=ax+b$ 대칭 : i.중점조건 ii.수직조건

##### ▶부등식영역의 최대,최소

- ① 조건식의 영역을 도식한다.
- ②  $f(x,y)=k$ 로 두고, 영역내에서 이동
- ③ k의 최대값, 최소값

##### ▶절댓값그래프

- 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.

답 : 응??????????

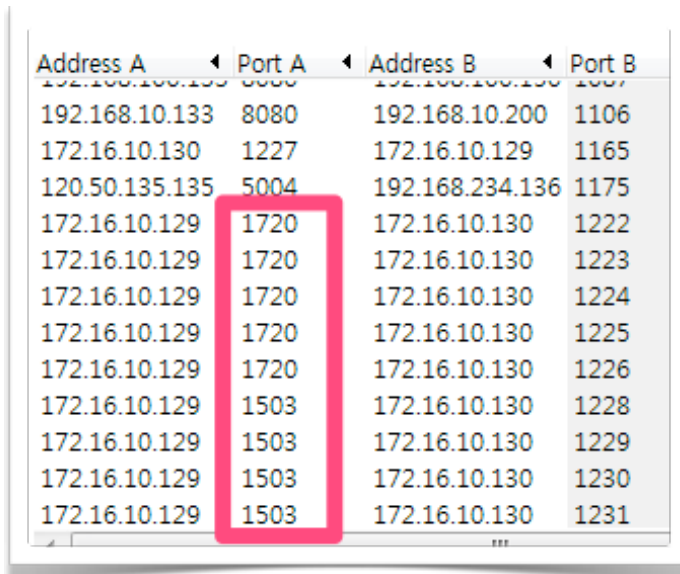
H3 Q. 우태혁의 여자친구 이름은 무엇이고, 어디에 살고 있는가?

EQ What is the name of Woo Tae Hyuck's girl firend, and where she is?  
(Key Format :: Woo Tae Hyuck\_Hanla Mountain)

태혁이가 여자친구가 있었나???

이 문제는 처음 어디 숨어있는지 찾기 힘들었다.

Network Miner가 HTTP나 FTP 등의 파일들은 떨어뜨려주니까 나머지 패킷을 보기로 했다.  
Wireshark의 Statistics - Conversation 에서 TCP 포트로 정렬을 하였다. (하단의 Name Resolution 체크 해제)



Address A	Port A	Address B	Port B
192.168.100.133	8080	192.168.100.130	1107
192.168.10.133	8080	192.168.10.200	1106
172.16.10.130	1227	172.16.10.129	1165
120.50.135.135	5004	192.168.234.136	1175
172.16.10.129	1720	172.16.10.130	1222
172.16.10.129	1720	172.16.10.130	1223
172.16.10.129	1720	172.16.10.130	1224
172.16.10.129	1720	172.16.10.130	1225
172.16.10.129	1720	172.16.10.130	1226
172.16.10.129	1503	172.16.10.130	1228
172.16.10.129	1503	172.16.10.130	1229
172.16.10.129	1503	172.16.10.130	1230
172.16.10.129	1503	172.16.10.130	1231

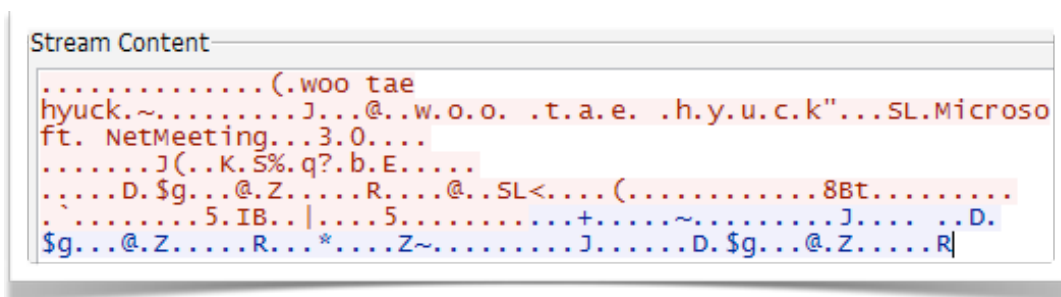
20~21(FTP), 80,8080 (HTTP)는 넘어가고 5004가 보였다.. 이는 네이트온으로 뒤에서 나온 문제와 연관되었다.

좌측에 TCP 1720 포트가 여러개 있었고 이어서 TCP 1503 포트가 이어졌다.

172.16.10.129 와 172.16.10.130 사이의 통신이고 172.16.10.130번의 소스 포트는 1~2씩 증가하는 것으로 보아 130번에서 129번으로 접속한 것으로 추정해 볼 수 있다.

또한 1720 포트와 1503이 잘하면 연관되었을 수도 있겠다는 추정도 해볼 수 있다.

먼저 1720 를 살펴 보니, NetMeeting과 연관된 것을 알 수 있었다.



```
Stream Content
.....(.wooo tae
hyuck.~.....J...@...w.o.o. .t.a.e. .h.y.u.c.k"...SL.Microso
ft. NetMeeting...3.0....
.....J(.K.S%.q?.b.E.....
.....D.$g...@.Z....R....@...SL<.....(.....8Bt.....
.....5.IB..|.....5.....+.....~.....J.....D.
$g...@.Z....R....*.....Z~.....J.....D.$g...@.Z....R|
```

하지만 우태혁에 관련된 내용만 보이다가 TCP 1720 마지막에서 처음으로 김하늘의 이름이 보였다.

```
Stream Content
.....(.woo tae
hyuck.~.J...@..w.o.o. .t.a.e. .h.y.u.c.k"...SL.Microsoft. NetMeeting.
.....;;8.B.O.9Z..u`..E....
.....w2.Z...E..w.....@..SL<....(.8Bt.....
.....5.IB..|.....5.....+.....~.....J....w2.Z...E..w.....w
(.Kim Ha-Neul~.Y.....J.....
..."...SL.Microsoft. NetMeeting...3.0...;;8.B.O.9Z..u`.....w2.Z...E..w.....|
```

TCP 1720에선 별다른 것을 못찾아 연결되어 있는 TCP 1503 까지 보게 되었다.

```
Stream Content
.....H...
.....{.....H.P.....{.....g....
.....h
.....v...d?gckp.g...?g. ?
b...K.i.m. .H.a.-.N.e.u.l..@..SL...p..l....._t..T.C.P.:1.7.2...1.6...1.0...1.2.9...
T...P.:1.7.2...1.6...1.0...1.2.9...V.E.R.:0.4.0.4.0.D.4.8...E.M...I.L.:.H.a.-.N.e.u.
l...A.B.C.D...C.o.m...L.O.C.A.T.I.O.N.:D.o.k.d.o._i.s.l.a.n.d...@..SL.....^
Y...
...@..SL. .8Bt.....
...{.....E.d.AS.8..... @..SL..@..?gl..
.....Kim Ha-Neul.....t...p?b..p.e.D.?b!
.w.o.o. .t.a.e. .h.y.u.c.k..@..SL.zp..l....._t..T.C.P.:1.7.2...1.6...1.0...1.3.0...
V.E.R.:0.4.0.4.0.D.4.8...E.M.A.I.L.:w.o.o.@.p.a.c.k.e.t...c.o.m.....@..SL.....^
```

TCP 1503으로 가는 패킷 중 세번째에서 위와 같은 내용을 확인할 수 있었다.

답 : Kim Ha Neul\_Dokdo island

사실 IP가 할당된 172.16.x.x 에서 바로 옆자리(129,130)에 앉아 넷미팅 화상 컨퍼런스로 통신하고 있는 우태혁과 김하늘임을 알 수 있었다.....

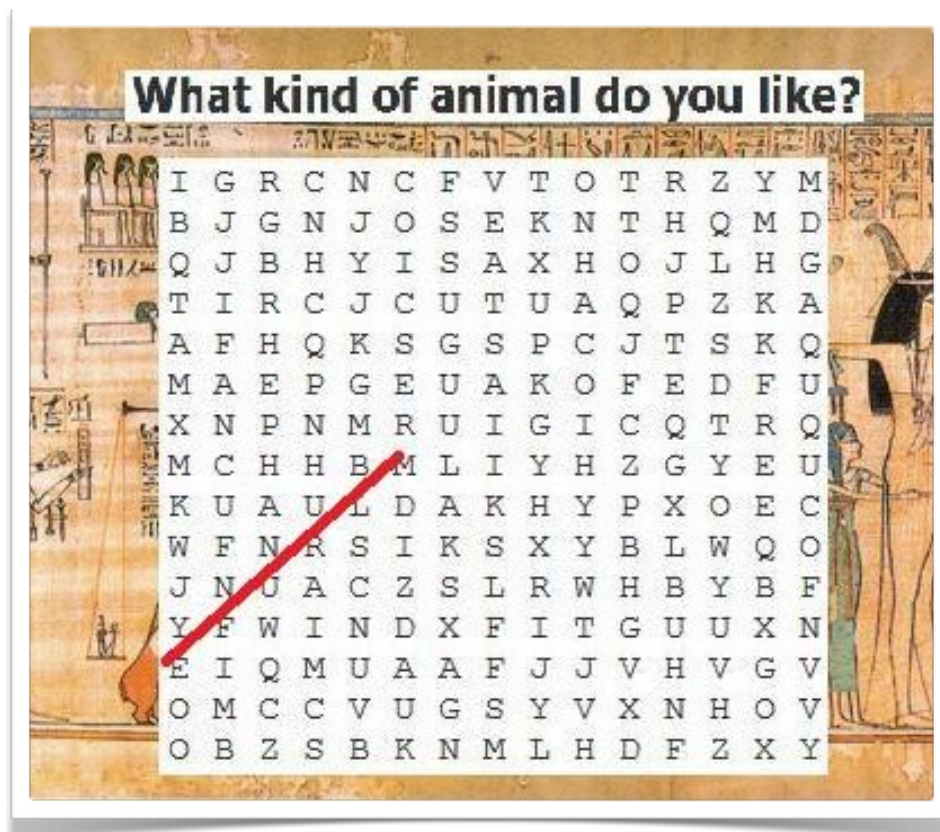


H4 Q 무슨 동물 좋아하니? - 대회 때 못푼 문제  
EQ What kind of animal do you like?

Network Miner 이미지 탭에서 바로 확인 가능했지만, 결국 못푼 문제입니다.

그림에서 보이는 문자열을 옮겨다가, 복호화 툴의 갑 Cryptool에서 ROT--13~ ROT-13, Caesar, Substitution, Vigenere 등등등 해보려고 했지만.... 바로 내려놓았습니다...

결국 대회가 끝나고 아래와 같은 그림을 올려 주셨습니다.



네.. BUNNY 였군요.... 풀라고 내신 문제는 아니죠??? ㅋ

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

정답은 수학문제를 푼 값입니다.

H3 에서 문제를 풀다가 WEB(HTTP), FTP를 뺀 나머지 프로토콜을 보았다.

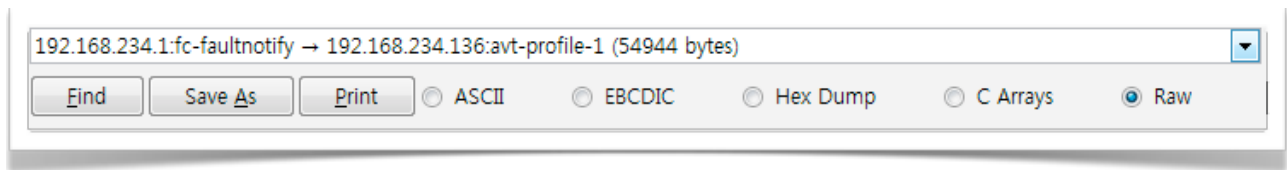
Conversations: 2012\_http\_prequal.pcap

Ethernet: 43	Fibre Channel	FDDI	IPv4: 50	IPv6: 3	IPX	JXTA	NCP	RSVP	SCTP	TCP: 113
TCP Conversations										
Address A	Port A	Address B	Port B	Packets	Bytes	Pa				
192.168.232.140	2545	112.175.42.65	80	28	22 606					
192.168.232.140	2546	192.168.232.131	80	7	1 542					
192.168.226.1	3308	192.168.226.130	21	110	7 969					
192.168.226.1	5002	192.168.226.130	20	8	1 071					
120.50.133.112	5004	192.168.234.136	1462	14	1 713					
120.50.135.135	5004	192.168.234.136	1175	5	81					
192.168.234.136	5004	192.168.234.1	2819	65	58 566					
192.168.0.2	5004	192.168.234.136	1465	3	174					

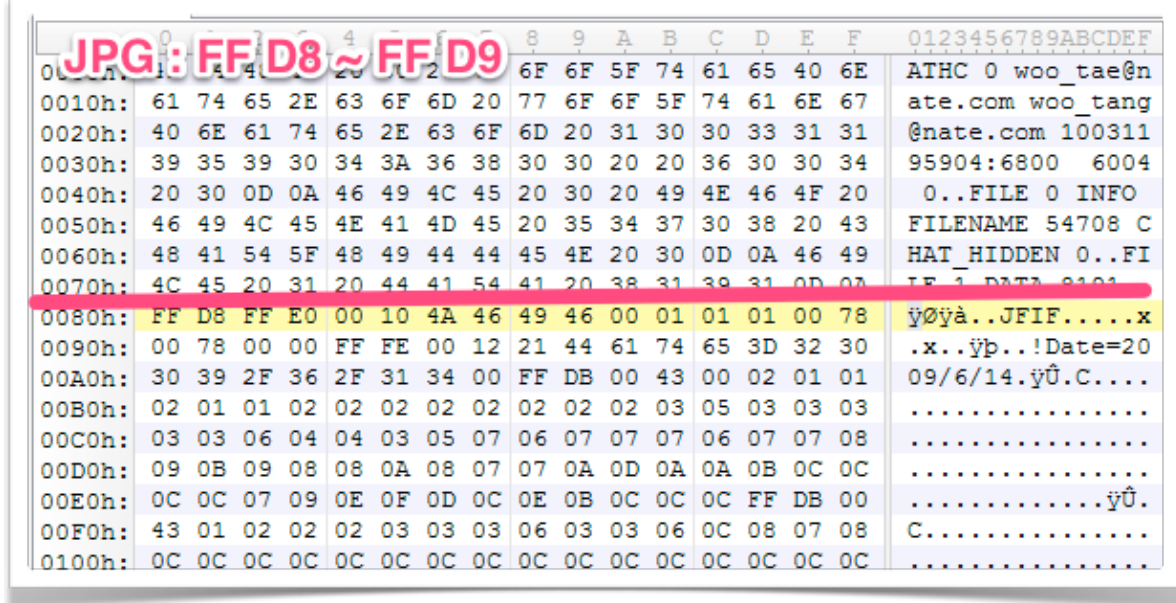
[illegible]

아~ 뭔가 사진을 전송하는 구나...

그래서 해당 통신을 저장하여 hexs 에디터로 보냈다.

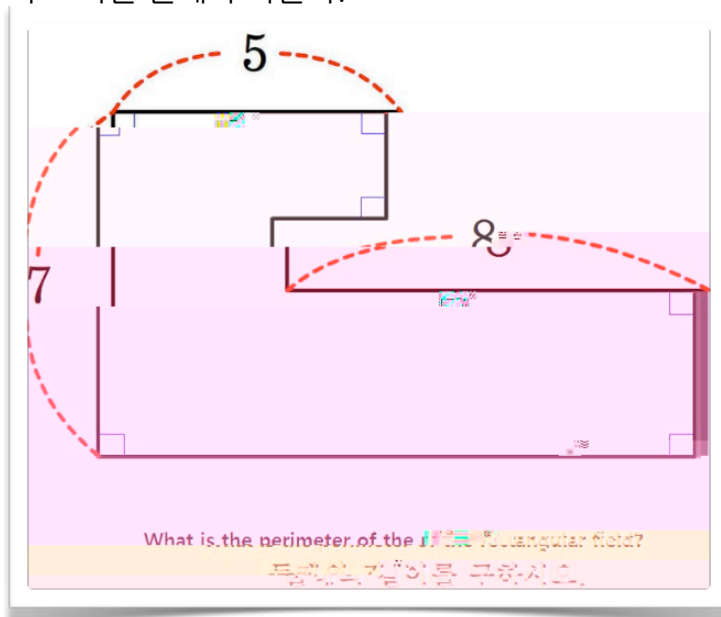


저장은 Raw로 하고, 위의 드롭다운 메뉴에서 한쪽 방향 (사이즈가 큰~)만 선택하고 Save As 로 저장한다.



hexs로 보면 가운데 줄을 친 부분에서 FF D8을 볼 수 있다. JPEG 그림 파일은 FF D8 로 시작해서 FF D9로 끝난다. 위에 부분을 지우고 다시 저장을 해보자.

그럼 아래 그림과 같이, 초등학교를 야간으로 나온 나는 도저히 풀 수 없는 “둘레의 길이를 구하시오”라는 문제가 나온다.



갈고리 모양의 둘레의 길이... 근데 가운데는 들어간 부분의 사이즈는 알 수가 없었다.  
5하고 7하고 8 그리고 직각.. 그게 전부였다.

이럴 땐 어떻게 해야할 까...

그 다음은 각자의 판단에 맡기겠습니다.

어찌 되었던 답은 40 이었습니다.

답 : 40

부족한 풀이 끝까지 읽어 주셔서 감사합니다. =)

(End of Document)