
네트워크 패킷 포렌식 및 문제풀이

201812745 김종원


A Table of Contents.

- 1** 네트워크 포렌식
- 2** 네트워크 패킷 포렌식
- 3** DEFCON#21 문제풀이



네트워크 포렌식이란?

컴퓨터 네트워크 트래픽에서 목적 정보를
수집하고, 분석하는 일련의 과정 또는 기술



네트워크 포렌식 – 수집 정보

- IDS/IPS와 방화벽 로그
- HTTP, FTP, 이메일, 그 밖에 서버 로그
- 네트워크 애플리케이션 로그
- HDD 상의 네트워크 트래픽 아티팩트
- **패킷 스니퍼나 네트워크 포렌식 도구에 의해 수집된 라이브 트래픽**
- 라우팅 및 ARP 테이블 정보, 포트 스캔 정보, SNMP 메시지

네트워크 포렌식의 문제점

- 스푸핑과 같은 공격으로 인한 **공격자 신원 특정 불가**
- 여러 대의 서버를 경유로 인한 **공격자 신원 특정 불가**
- 로그 기능 비활성화로 인한 **로그 없음**
- 시간 지체 시 유지 및 삭제 정책에 의해 **로그 삭제**
- 공격자의 의도적인 **로그 삭제**
- 국경을 넘나드는 흔적으로 인한 **관할권 확보 힘들**

네트워크 증거수집 방법(1) – 시스템

- 사라지기 쉬운 시스템 정보

- 사라지기 쉬운 시스템상의 **네트워크 정보**

기본 정보

- OS
- Version
- Resource
- Install Package 등

시간 정보

- 로컬시간 확인
- 채증 시간 저장
- 실행 중인 프로세스 Up/Down 타임
- 파일 MAC 타임

사용자 정보

- 계정정보
- Remote user account
- Remote IP
- 실제 사용자 식별 정보

분석 및 조사

- MAC 주소
- IP주소
- 라우팅 테이블
- 알려진 서비스의 내용
- 공유 정보
- 세션 정보

네트워크 증거수집 방법(2) – 네트워크 시스템

- 전체적인 네트워크 구성을 파악하고 어떤 위치에서 어떤 정보를 수집할 것인지 확인

Router

- 로그 발생 시간
- 라우터에서 발생한 로그
- Address & Host Mapping
- System 버전
- 보안 제어

Switch

- 로그 발생 시간
- 스위치에서 발생한 로그
- VLAN 통신파악
- User IP 주소와 MAC 확인
- 포트 사용 여부 확인

네트워크 증거수집 방법(3) – 네트워크 보안 시스템

- 설정이 올바르게 될 경우 손쉽게 통신 기록 확보 가능

	정보	정보내용	용도
방화벽	통신기록	방화벽을 거쳐간 통신기록	통신 시간 및 접속 정보 확인
IDS / IPS	보안정책	시스템 접근 통제	침입상태의 시스템 동작상태 파악
	로그파일	IDS에서 발생한 로그정보	침입탐지 로그정보 파악
	필터정책	정책 필터확인	허용 및 비 허용 필터링 내용파악
VPN	로그파일	VPN 접속로그	IP 정보 등 내용파악
	접속자 확인	접속 시간확인	사용자 및 접속시간 확인

네트워크 증거수집 방법(4) – 패킷 캡처 도구(스니퍼)

- Windump

```
C:\Users\Wkaspyx>windump -h
windump version 3.9.5, based on tcpdump version 3.9.5
WinPcap version 4.1.3 (packet.dll version 4.1.0.2980), based on libpcap version
1.0 branch 1_0_rel0b (20091008)
Usage: windump [-aAdDeflLnNOPqRStuUvxX] [-B size] [-c count] [-C file_size]
               [-E algo:secret] [-F file] [-i interface] [-M secret]
               [-r file] [-s snaplen] [-T type] [-w file]
               [-W filecount] [-y datalinktype] [-Z user]
               [expression]
```

- Tcpdump

```
[root@cms02 /]# tcpdump -vv -i bond1 | egrep 10.62.5.113
tcpdump: listening on bond1, link-type EN10MB (Ethernet), capture size 262144 bytes
10.62.5.113 > cms02: ICMP echo reply, id 20478, seq 215, length 64
192.168.112.26 > 10.62.5.113: ICMP echo request, id 28230, seq 5318, length 64
192.168.112.15 > 10.62.5.113: ICMP echo request, id 20217, seq 5279, length 64
192.168.110.11 > 10.62.5.113: ICMP echo request, id 42040, seq 5704, length 64
192.168.110.18 > 10.62.5.113: ICMP echo request, id 16827, seq 5616, length 64
cms02 > 10.62.5.113: ICMP echo request, id 20478, seq 216, length 64
10.62.5.113 > cms02: ICMP echo reply, id 20478, seq 216, length 64
192.168.112.26 > 10.62.5.113: ICMP echo request, id 28230, seq 5319, length 64
192.168.112.15 > 10.62.5.113: ICMP echo request, id 20217, seq 5280, length 64
192.168.110.11 > 10.62.5.113: ICMP echo request, id 42040, seq 5705, length 64
192.168.110.18 > 10.62.5.113: ICMP echo request, id 16827, seq 5617, length 64
cms02 > 10.62.5.113: ICMP echo request, id 20478, seq 217, length 64
10.62.5.113 > cms02: ICMP echo reply, id 20478, seq 217, length 64
```

「 네트워크 패킷 포렌식이란?

네트워크 패킷 포렌식은 종단간 수집된 패킷에 대해 분석 하는 기술

」

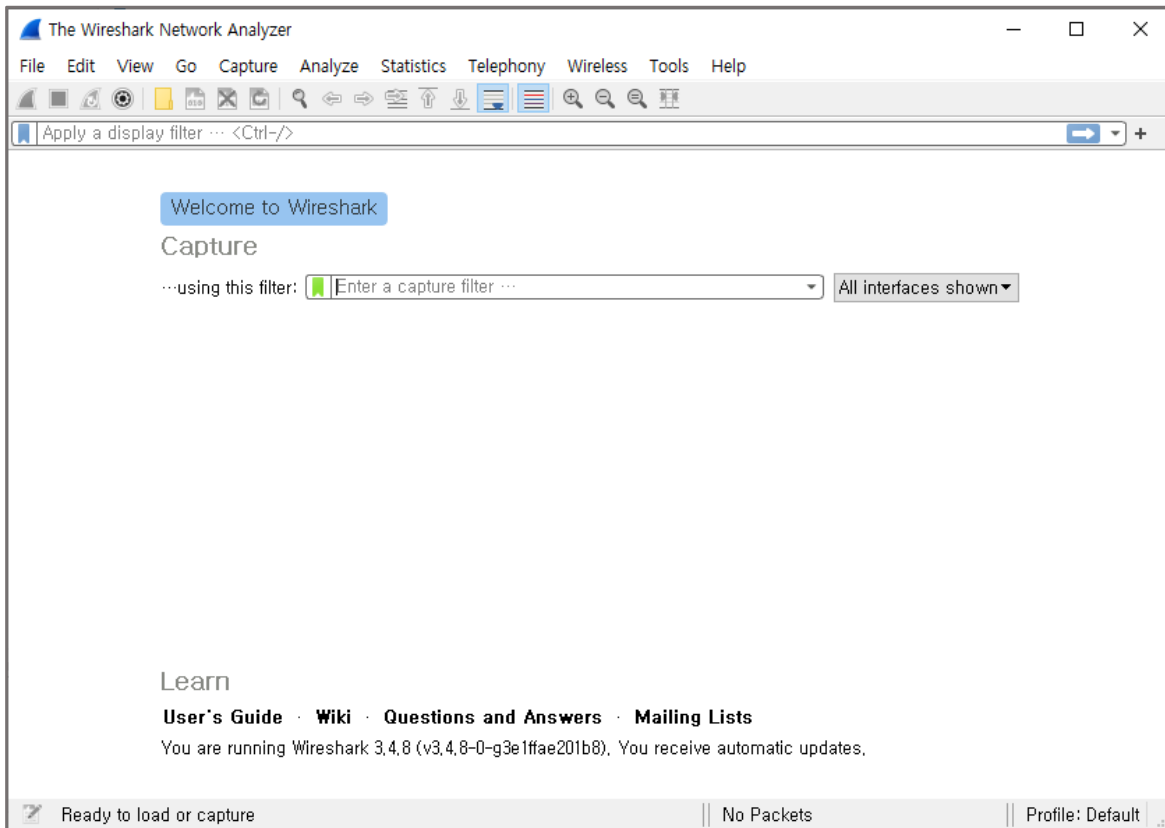
네트워크 패킷 포렌식



네트워크 포렌식 – 수집 정보

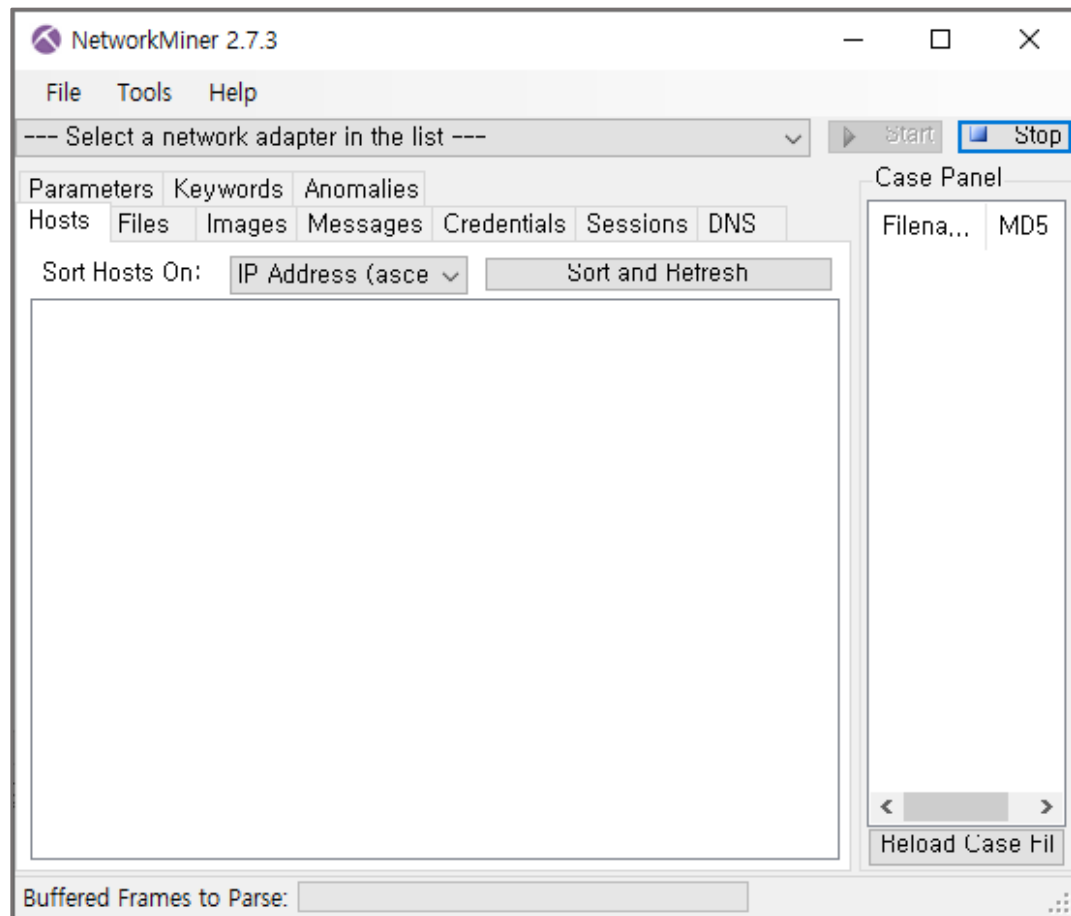
- IDS/IPS와 방화벽 로그
- HTTP, FTP, 이메일, 그 밖에 서버 로그
- 네트워크 애플리케이션 로그
- HDD 상의 네트워크 트래픽 아티팩트
- 패킷 스니퍼나 네트워크 포렌식 도구에 의해 수집된 라이브 트래픽
- 라우팅 및 ARP 테이블 정보, 포트 스캔 정보, SNMP 메시지

네트워크 패킷 포렌식 도구 - Wireshark



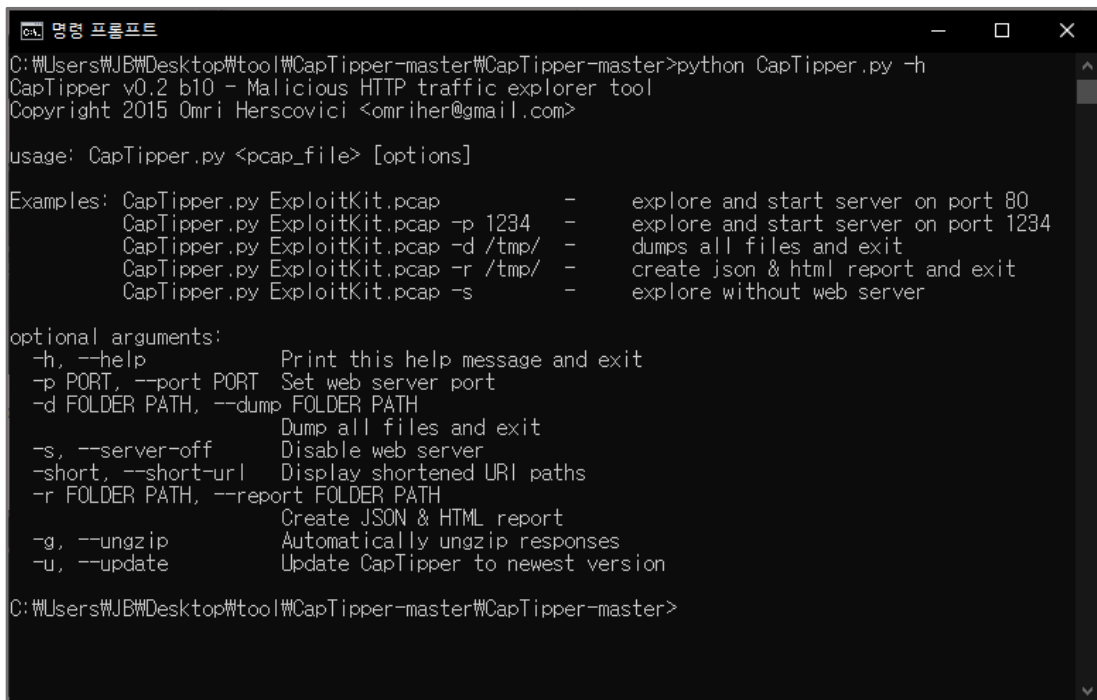
- 무료로 사용 할 수 있는 패킷 캡처 도구
- 많은 기능과 플러그인 지원.
- 강력한 필터 기능 지원
- CLI 패킷 분석 도구 지원
- AND(&&), OR(||), NOT(!) 같은 논리 연산 사용 가능
ex) dst host 192.168.0.1 && tcp port 1024

네트워크 패킷 포렌식 도구 – NetworkMinor



- 다양한 파싱 기능을 지원
- 네트워크 패킷 캡처 기능 지원
- 무료/유로 버전으로 나뉘어 제공

네트워크 패킷 포렌식 도구 – CapTipper(캡티퍼)



```
명령 프롬프트
C:\Users\JB\Desktop\tool\CapTipper-master\CapTipper-master>python CapTipper.py -h
CapTipper v0.2 b10 - Malicious HTTP traffic explorer tool
Copyright 2015 Omri Herscovici <omriher@gmail.com>

usage: CapTipper.py <pcap_file> [options]

Examples: CapTipper.py ExploitKit.pcap - explore and start server on port 80
          CapTipper.py ExploitKit.pcap -p 1234 - explore and start server on port 1234
          CapTipper.py ExploitKit.pcap -d /tmp/ - dumps all files and exit
          CapTipper.py ExploitKit.pcap -r /tmp/ - create json & html report and exit
          CapTipper.py ExploitKit.pcap -s - explore without web server

optional arguments:
  -h, --help            Print this help message and exit
  -p PORT, --port PORT  Set web server port
  -d FOLDER PATH, --dump FOLDER PATH
                        Dump all files and exit
  -s, --server-off      Disable web server
  -short, --short-url   Display shortened URI paths
  -r FOLDER PATH, --report FOLDER PATH
                        Create JSON & HTML report
  -g, --ungzip          Automatically ungzip responses
  -u, --update          Update CapTipper to newest version

C:\Users\JB\Desktop\tool\CapTipper-master\CapTipper-master>
```

- Python으로 제작된 악성 트래픽 분석 도구
- 트래픽 내에서 파일 추출
- 트래픽 흐름 분석
- 패킷 헤더, 내용 분석
- hexa 뷰어
- 분석 보고서 생성 기능 제공

Round1

Jensen 사건을 알게 된 Jack과 그의 팀은 Jensen의 회사와 가정에 네트워크 탭과 무선 캡처 장비를 설치했다. 모니터링을 하는 동안 Jack과 그의 팀은 흥미로운 용의자인 Betty를 발견했다. 이 사람은 Jensen 부인이 남편과 바람을 피고 있다고 걱정하는 사람일 수도 있다. Jack은 포렌식 전문가인 당신에게 캡처 정보를 자세히 보여준다. 그리고 **회의가 진행된다**. Round 1 패킷을 사용해서 사건에 대해 자세히 알아보고 다음의 질문에 답 하시오.

회의가 예정된 요일은 언제인가?

Jack
(수사관)



Jensen
(엔센씨)



Mrs.Jensen
(엔센부인)



Betty
(내연녀?)

Round1

2

1

No.	Time	Source	Destination	Protocol	Length	Info
20861	321.915406	172.29.1.55	173.245.61.168	TCP	60	1425 → 80 [ACK] Seq=837 Ack=1863 Win=65535 Len=0
20862	321.918132	172.29.1.55	173.245.61.168	TCP	60	1425 → 80 [FIN, ACK] Seq=837 Ack=1863 Win=65535 Len=0
20863	321.918859	172.29.1.55	74.125.28.104	HTTP	1294	GET /gen_204?atyp=i&ct=ircnl&cad=&tbnid=eNj18pWjUNGhcM&imgur1=http%3A%2F%2Fmemeboss.co...
20864	321.930641	173.245.61.168	172.29.1.55	TCP	60	80 → 1425 [FIN, ACK] Seq=1863 Ack=838 Win=16616 Len=0
20865	321.930677	172.29.1.55	173.245.61.168	TCP	60	1425 → 80 [ACK] Seq=838 Ack=1864 Win=65535 Len=0
20866	321.941350	74.125.28.104	172.29.1.55	HTTP	252	HTTP/1.1 204 No Content
20867	322.064783	172.29.1.55	74.125.28.104	TCP	60	1388 → 80 [FIN, ACK] Seq=2609 Ack=765 Win=64771 Len=0
20868	322.084012	74.125.28.104	172.29.1.55	TCP	60	80 → 1388 [FIN, ACK] Seq=765 Ack=2610 Win=63760 Len=0
20869	322.084025	172.29.1.55	74.125.28.104	TCP	60	1388 → 80 [ACK] Seq=2610 Ack=766 Win=64771 Len=0
20870	322.121006	172.29.1.55	74.125.28.104	TCP	60	1145 → 80 [ACK] Seq=42449 Ack=775247 Win=64925 Len=0
20871	322.542013	172.29.1.50	255.255.255.255	UDP	82	65281 → 1947 Len=40
20872	323.064701	172.29.1.55	173.194.127.17	TCP	60	1380 → 80 [FIN, ACK] Seq=1635 Ack=12459 Win=65535 Len=0
20873	323.064736	172.29.1.55	173.194.127.17	TCP	60	1379 → 80 [FIN, ACK] Seq=2174 Ack=28841 Win=65535 Len=0
20874	323.064741	172.29.1.55	173.194.127.17	TCP	60	1381 → 80 [FIN, ACK] Seq=2713 Ack=38938 Win=65535 Len=0
20875	323.215877	173.194.127.17	172.29.1.55	TCP	60	80 → 1381 [FIN, ACK] Seq=38938 Ack=2714 Win=63882 Len=0
20876	323.215908	173.194.127.17	172.29.1.55	TCP	60	80 → 1379 [FIN, ACK] Seq=28841 Ack=2175 Win=63765 Len=0
20877	323.215913	173.194.127.17	172.29.1.55	TCP	60	80 → 1380 [FIN, ACK] Seq=12459 Ack=1636 Win=63882 Len=0
20878	323.215917	172.29.1.55	173.194.127.17	TCP	60	1381 → 80 [ACK] Seq=2714 Ack=38939 Win=65535 Len=0
20879	323.215922	172.29.1.55	173.194.127.17	TCP	60	1379 → 80 [ACK] Seq=2175 Ack=28842 Win=65535 Len=0
20880	323.216096	172.29.1.55	173.194.127.17	TCP	60	1380 → 80 [ACK] Seq=1636 Ack=12460 Win=65535 Len=0
20881	324.539338	172.29.1.50	10.0.1.3	SNMP	119	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.1 1.3.6.1.2.1.25.3.5.1.2.1
20882	324.539377	172.29.1.50	10.0.1.3	SNMP	119	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.1 1.3.6.1.2.1.25.3.5.1.2.1
20883	324.539377	172.29.1.50	10.0.1.3	SNMP	119	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.1 1.3.6.1.2.1.25.3.5.1.2.1
20884	324.540048	66.109.149.121	172.29.1.50	ICMP	70	Destination unreachable (Host unreachable)

> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
 Ethernet II, Src: Netgear (08:00:27:00:00:00), Dst: LLDP_Multicast (01:80:c2:00:00:0e)
 > Link Layer Discovery Protocol
 > VSS Monitoring Ethernet trailer, Source Port: 27904

0000 01 80 c2 00 00 0e 4c 60 de ce 16 2c 88 cc 02 07L.....
 0010 04 4c 60 de ce 16 2a 04 04 05 67 32 35 06 02 00 ..L.....g25...
 0020 78 10 14 05 01 c0 a8 01 04 02 00 00 00 21 08 62 x.....!..b
 0030 72 6f 61 64 63 6f 6d 00 00 00 00 00roadcom....

round1.pcap Packets: 20890 · Displayed: 20890 (100,0%) Profile: Default

1

2

Round1

2

1

round1.pcap

File Edit Capture Filter Statistics Telephony Wireless Tools Help

irc

No.	Time	Source	Destination	Protocol	Length	Info
2	1.182799	172.29.1.50	255.255.255.255	LLDP_Multicast	60	MA/4c:60:de:ce:16:2a IN/g25 120
3	4.762447	46.165.193.136	172.29.1.50	TCP	86	6669 → 1036 [PSH, ACK] Seq=1 Ack=1 Win=5840 Len=32
4	4.765167	172.29.1.55	46.165.193.136	TCP	86	1036 → 6669 [PSH, ACK] Seq=1 Ack=33 Win=64679 Len=31
5	4.933344	46.165.193.136	172.29.1.50	TCP	60	6669 → 1036 [ACK] Seq=33 Ack=32 Win=5840 Len=0
6	5.195671	172.29.1.50	172.29.1.55	UDP	82	65281 → 1947 Len=40
7	10.675195	172.29.1.50	46.165.193.136	IRC	86	Request (PRIVMSG)
8	10.840830	46.165.193.136	172.29.1.50	TCP	60	6667 → 49164 [ACK] Seq=1 Ack=33 Win=46 Len=0
9	10.858558	46.165.193.136	172.29.1.55	TCP	130	6669 → 1036 [PSH, ACK] Seq=33 Ack=32 Win=5840 Len=76
10	11.043204	172.29.1.55	46.165.193.136	TCP	60	1036 → 6669 [ACK] Seq=32 Ack=109 Win=64603 Len=0
11	15.539315	Dell_fa:a6:cc	Cisco_ba:52:2a	ARP	60	Who has 172.29.1.254? Tell 172.29.1.50
12	15.539350	Cisco_ba:52:2a	Dell_fa:a6:cc	ARP	60	172.29.1.254 is at 54:75:d0:ba:52:2a
13	15.977044	172.29.1.50	192.168.30.30	Syslog	468	LOCAL2.NOTICE: Jun 25 16:13:44 fox-ws MSWinEventLog\t0\tSecurity\t346\tTue Jun 25 16:1...
14	15.978032	66.109.149.121	172.29.1.50	ICMP	70	Destination unreachable (Host unreachable)
15	20.198831	172.29.1.55	46.165.193.136	TCP	84	1036 → 6669 [PSH, ACK] Seq=32 Ack=109 Win=64603 Len=30
16	20.366946	46.165.193.136	172.29.1.55	TCP	60	6669 → 1036 [ACK] Seq=109 Ack=62 Win=5840 Len=0
17	20.375932	46.165.193.136	172.29.1.50	IRC	137	Response (PRIVMSG)
18	20.586069	172.29.1.50	46.165.193.136	TCP	60	49164 → 6667 [ACK] Seq=33 Ack=84 Win=255 Len=0
19	24.305387	172.29.1.50	10.0.1.3	SNMP	119	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.1 1.3.6.1.2.1.25.3.5.1.2.1
20	24.305420	172.29.1.50	10.0.1.3	SNMP	119	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.1 1.3.6.1.2.1.25.3.5.1.2.1
21	24.305426	172.29.1.50	10.0.1.3	SNMP	119	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.1 1.3.6.1.2.1.25.3.5.1.2.1
22	24.412821	66.109.149.121	172.29.1.50	ICMP	70	Destination unreachable (Host unreachable)
23	30.021000	Netgear_ce:16:2c	LLDP_Multicast	LLDP	60	MA/4c:60:de:ce:16:2a IN/g25 120
24	34.976823	172.29.1.50	10.0.1.3	SNMP	119	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.1 1.3.6.1.2.1.25.3.5.1.2.1

Frame 7: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)

Ethernet II, Src: Dell_fa:a6:cc (00:08:74:fa:a6:cc), Dst: Cisco_ba:52:2a (54:75:d0:ba:52:2a)

Internet Protocol Version 4, Src: 172.29.1.50, Dst: 46.165.193.136

Transmission Control Protocol, Src Port: 49164, Dst Port: 6667, Seq: 1, Ack: 1, Len: 32

0000 54 75 d0 ba 52 2a 00 08 74 fa a6 cc 08 00 45 00 Tu...R... t....E..

0010 00 48 10 79 40 00 00 06 4c ba ac 1d 01 32 2e a5 ..H.y@... L....2..

0020 c1 88 c0 0c 1a 0b fb de 2b d1 bc 7b 37 1d 50 18+...{7.P...

0030 01 00 32 9e 00 00 50 52 49 56 4d 53 47 20 23 53 ...2...PR IVMSG #S

0040 33 63 72 33 74 53 70 30 74 20 3a 48 69 20 47 72 3cr3tSp0 t :Hi Gr

0050 65 67 20 3a 29 0a eg :).

Internet Relay Chat: Protocol

Packets: 20890 · Displayed: 20890 (100.0%)

Profile: Default

1

No.	Time	Source	Destination	Protocol	Length	Info
2	1.182799	172.29.1.50	255.255.255.255	TCP	60	6669 → 1036 [PSH, ACK] Seq=1 Ack=1 Win=5840 Len=32
3	4.762447	46.165.193.136	172.29.1.50	UDP	82	65281 → 1947 Len=40
4	4.765167	172.29.1.55	46.165.193.136	IRC	86	Request (PRIVMSG)
5	4.933344	46.165.193.136	172.29.1.50	TCP	60	6669 → 1036 [ACK] Seq=33 Ack=32 Win=5840 Len=0
6	5.195671	172.29.1.50	172.29.1.55	TCP	82	65281 → 1947 Len=40
7	10.675195	172.29.1.50	46.165.193.136	TCP	60	6667 → 49164 [ACK] Seq=1 Ack=33 Win=46 Len=0
8	10.840830	46.165.193.136	172.29.1.55	TCP	130	6669 → 1036 [PSH, ACK] Seq=33 Ack=32 Win=5840 Len=76
9	10.858558	46.165.193.136	172.29.1.50	TCP	60	1036 → 6669 [ACK] Seq=32 Ack=109 Win=64603 Len=0
10	11.043204	172.29.1.55	46.165.193.136	TCP	60	1036 → 6669 [ACK] Seq=32 Ack=109 Win=64603 Len=0
11	15.539315	Dell_fa:a6:cc	Cisco_ba:52:2a	ARP	60	Who has 172.29.1.254? Tell 172.29.1.50
12	15.539350	Cisco_ba:52:2a	Dell_fa:a6:cc	ARP	60	172.29.1.254 is at 54:75:d0:ba:52:2a
13	15.977044	172.29.1.50	192.168.30.30	Syslog	468	LOCAL2.NOTICE: Jun 25 16:13:44 fox-ws MSWinEventLog\t0\tSecurity\t346\tTue Jun 25 16:1...
14	15.978032	66.109.149.121	172.29.1.50	ICMP	70	Destination unreachable (Host unreachable)
15	20.198831	172.29.1.55	46.165.193.136	TCP	84	1036 → 6669 [PSH, ACK] Seq=32 Ack=109 Win=64603 Len=30
16	20.366946	46.165.193.136	172.29.1.55	TCP	60	6669 → 1036 [ACK] Seq=109 Ack=62 Win=5840 Len=0
17	20.375932	46.165.193.136	172.29.1.50	IRC	137	Response (PRIVMSG)
18	20.586069	172.29.1.50	46.165.193.136	TCP	60	49164 → 6667 [ACK] Seq=33 Ack=84 Win=255 Len=0
19	24.305387	172.29.1.50	10.0.1.3	SNMP	119	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.1 1.3.6.1.2.1.25.3.5.1.2.1
20	24.305420	172.29.1.50	10.0.1.3	SNMP	119	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.1 1.3.6.1.2.1.25.3.5.1.2.1
21	24.305426	172.29.1.50	10.0.1.3	SNMP	119	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.1 1.3.6.1.2.1.25.3.5.1.2.1
22	24.412821	66.109.149.121	172.29.1.50	ICMP	70	Destination unreachable (Host unreachable)
23	30.021000	Netgear_ce:16:2c	LLDP_Multicast	LLDP	60	MA/4c:60:de:ce:16:2a IN/g25 120
24	34.976823	172.29.1.50	10.0.1.3	SNMP	119	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.1 1.3.6.1.2.1.25.3.5.1.2.1

인터넷 릴레이 챗(Internet Relay Chat, 약칭: IRC)은 실시간 채팅 프로토콜이다. 채널이라 불리는 토론 포럼에서 그룹 대화를 하기 위해 설계되었으나^[1] 개인 메시지를 통한 1:1 소통^[2], 그리고 파일 공유를 포함한 채팅 및 대화 전송^[3]도 가능하다.^[4]

그리고 IRC는 전통적인 채팅 프로토콜로, 이를 지원하는 수많은 서버 네트워크와 클라이언트가 존재한다.

2

irc

No.	Time	Source	Destination	Protocol	Length	Info
2	1.182799	172.29.1.50	255.255.255.255	TCP	60	6669 → 1036 [PSH, ACK] Seq=1 Ack=1 Win=5840 Len=32
3	4.762447	46.165.193.136	172.29.1.50	UDP	82	65281 → 1947 Len=40
4	4.765167	172.29.1.55	46.165.193.136	IRC	86	Request (PRIVMSG)
5	4.933344	46.165.193.136	172.29.1.50	TCP	60	6669 → 1036 [ACK] Seq=33 Ack=32 Win=5840 Len=0
6	5.195671	172.29.1.50	172.29.1.55	TCP	82	65281 → 1947 Len=40
7	10.675195	172.29.1.50	46.165.193.136	TCP	60	6667 → 49164 [ACK] Seq=1 Ack=33 Win=46 Len=0
8	10.840830	46.165.193.136	172.29.1.55	TCP	130	6669 → 1036 [PSH, ACK] Seq=33 Ack=32 Win=5840 Len=76
9	10.858558	46.165.193.136	172.29.1.50	TCP	60	1036 → 6669 [ACK] Seq=32 Ack=109 Win=64603 Len=0
10	11.043204	172.29.1.55	46.165.193.136	TCP	60	1036 → 6669 [ACK] Seq=32 Ack=109 Win=64603 Len=0
11	15.539315	Dell_fa:a6:cc	Cisco_ba:52:2a	ARP	60	Who has 172.29.1.254? Tell 172.29.1.50
12	15.539350	Cisco_ba:52:2a	Dell_fa:a6:cc	ARP	60	172.29.1.254 is at 54:75:d0:ba:52:2a
13	15.977044	172.29.1.50	192.168.30.30	Syslog	468	LOCAL2.NOTICE: Jun 25 16:13:44 fox-ws MSWinEventLog\t0\tSecurity\t346\tTue Jun 25 16:1...
14	15.978032	66.109.149.121	172.29.1.50	ICMP	70	Destination unreachable (Host unreachable)
15	20.198831	172.29.1.55	46.165.193.136	TCP	84	1036 → 6669 [PSH, ACK] Seq=32 Ack=109 Win=64603 Len=30
16	20.366946	46.165.193.136	172.29.1.55	TCP	60	6669 → 1036 [ACK] Seq=109 Ack=62 Win=5840 Len=0
17	20.375932	46.165.193.136	172.29.1.50	IRC	137	Response (PRIVMSG)
18	20.586069	172.29.1.50	46.165.193.136	TCP	60	49164 → 6667 [ACK] Seq=33 Ack=84 Win=255 Len=0
19	24.305387	172.29.1.50	10.0.1.3	SNMP	119	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.1 1.3.6.1.2.1.25.3.5.1.2.1
20	24.305420	172.29.1.50	10.0.1.3	SNMP	119	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.1 1.3.6.1.2.1.25.3.5.1.2.1
21	24.305426	172.29.1.50	10.0.1.3	SNMP	119	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.1 1.3.6.1.2.1.25.3.5.1.2.1
22	24.412821	66.109.149.121	172.29.1.50	ICMP	70	Destination unreachable (Host unreachable)
23	30.021000	Netgear_ce:16:2c	LLDP_Multicast	LLDP	60	MA/4c:60:de:ce:16:2a IN/g25 120
24	34.976823	172.29.1.50	10.0.1.3	SNMP	119	get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.1 1.3.6.1.2.1.25.3.5.1.2.1

Frame 7: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)

Ethernet II, Src: Dell_fa:a6:cc (00:08:74:fa:a6:cc), Dst: Cisco_ba:52:2a (54:75:d0:ba:52:2a)

Internet Protocol Version 4, Src: 172.29.1.50, Dst: 46.165.193.136

Transmission Control Protocol, Src Port: 49164, Dst Port: 6667, Seq: 1, Ack: 1, Len: 32

0000 54 75 d0 ba 52 2a 00 08 74 fa a6 cc 08 00 45 00 Tu...R... t....E..

0010 00 48 10 79 40 00 00 06 4c ba ac 1d 01 32 2e a5 ..H.y@... L....2..

0020 c1 88 c0 0c 1a 0b fb de 2b d1 bc 7b 37 1d 50 18+...{7.P...

0030 01 00 32 9e 00 00 50 52 49 56 4d 53 47 20 23 53 ...2...PR IVMSG #S

0040 33 63 72 33 74 53 70 30 74 20 3a 48 69 20 47 72 3cr3tSp0 t :Hi Gr

0050 65 67 20 3a 29 0a eg :).

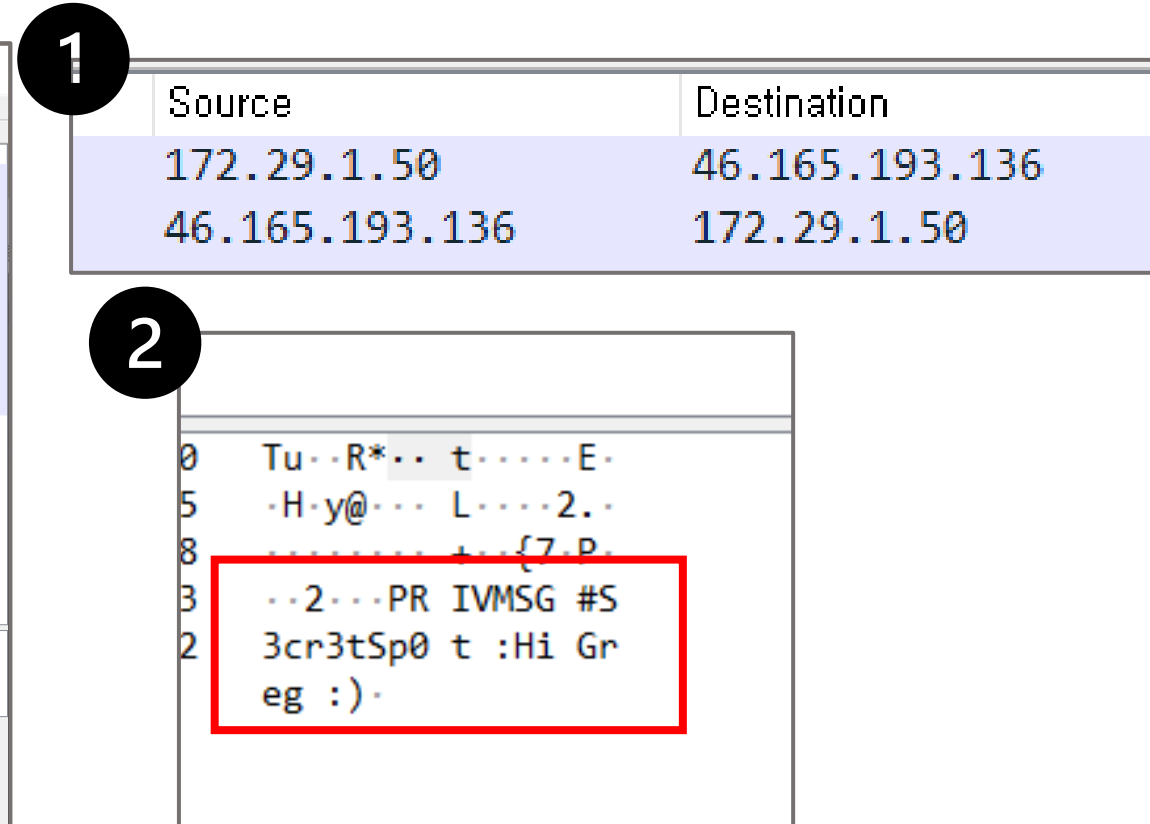
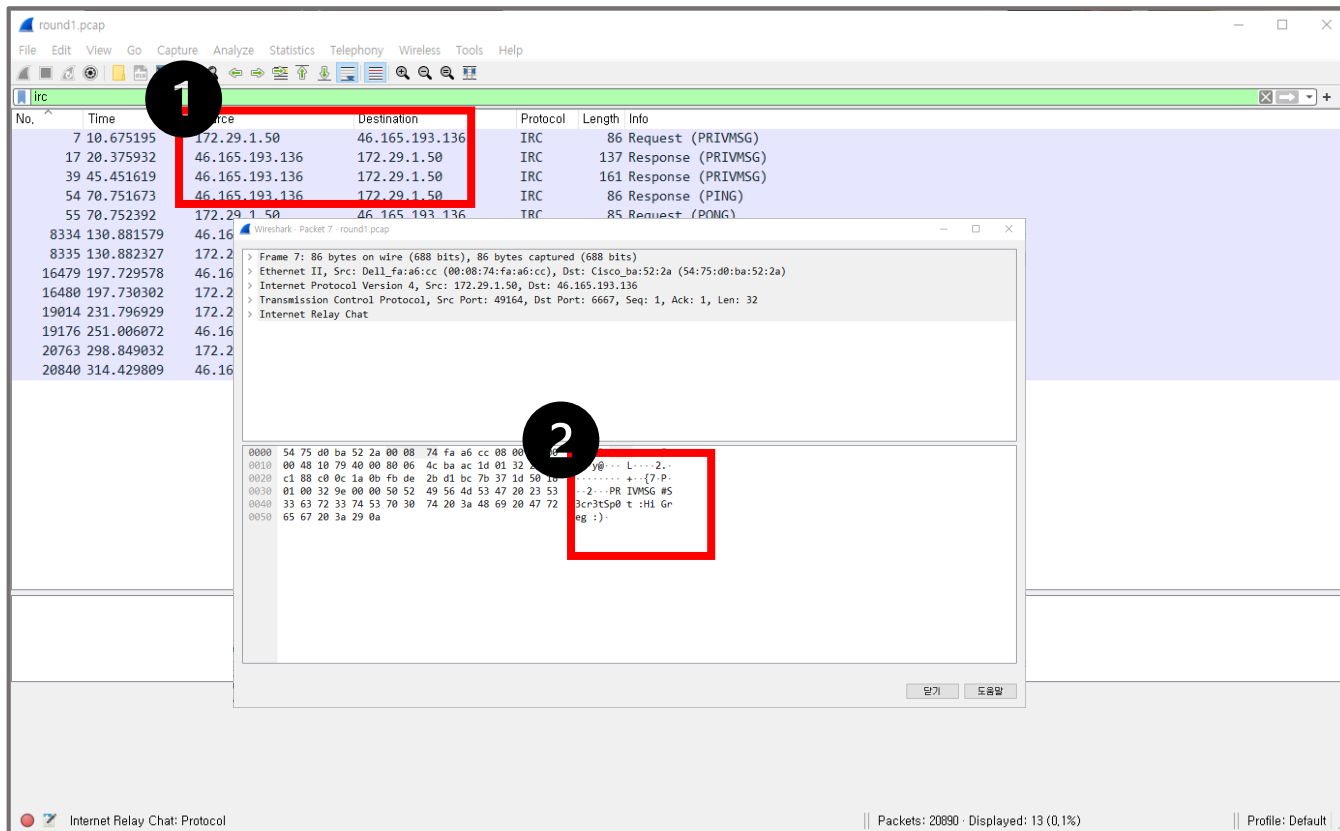
Internet Relay Chat: Protocol

Packets: 20890 · Displayed: 20890 (100.0%)

Profile: Default

Part 3, DeFCoN#21 문제풀이

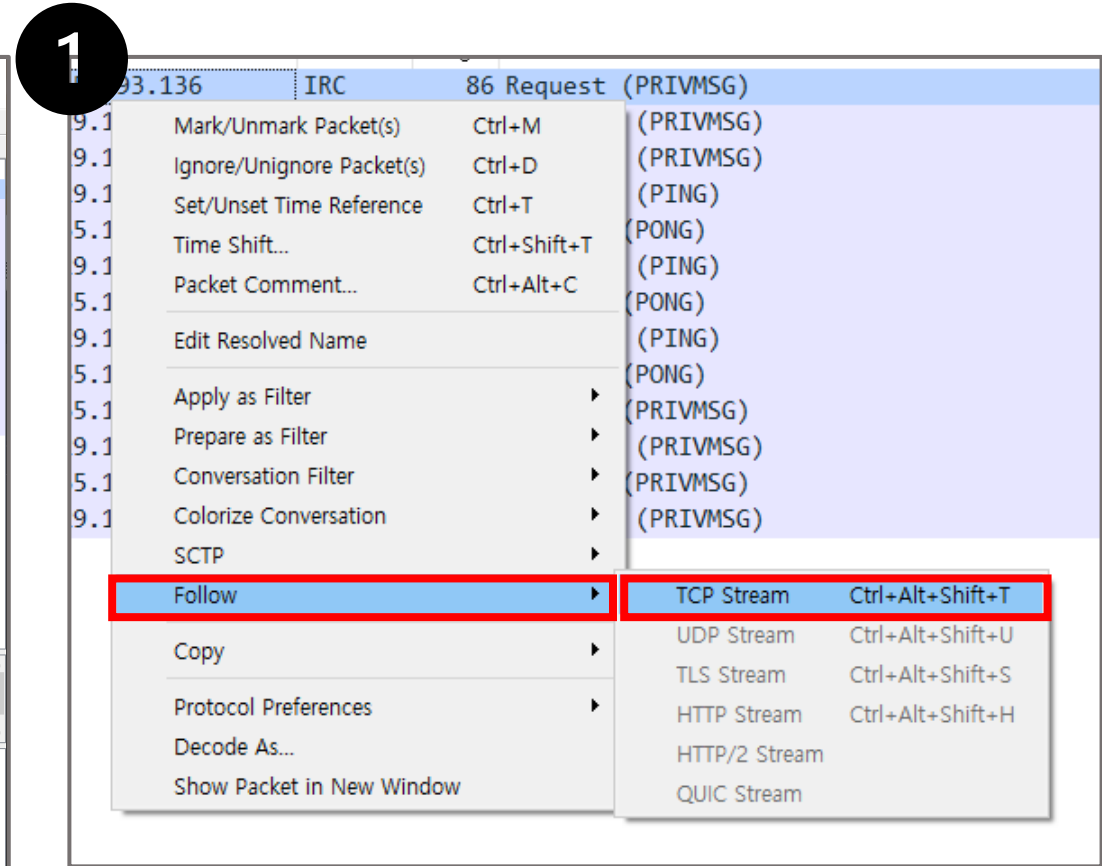
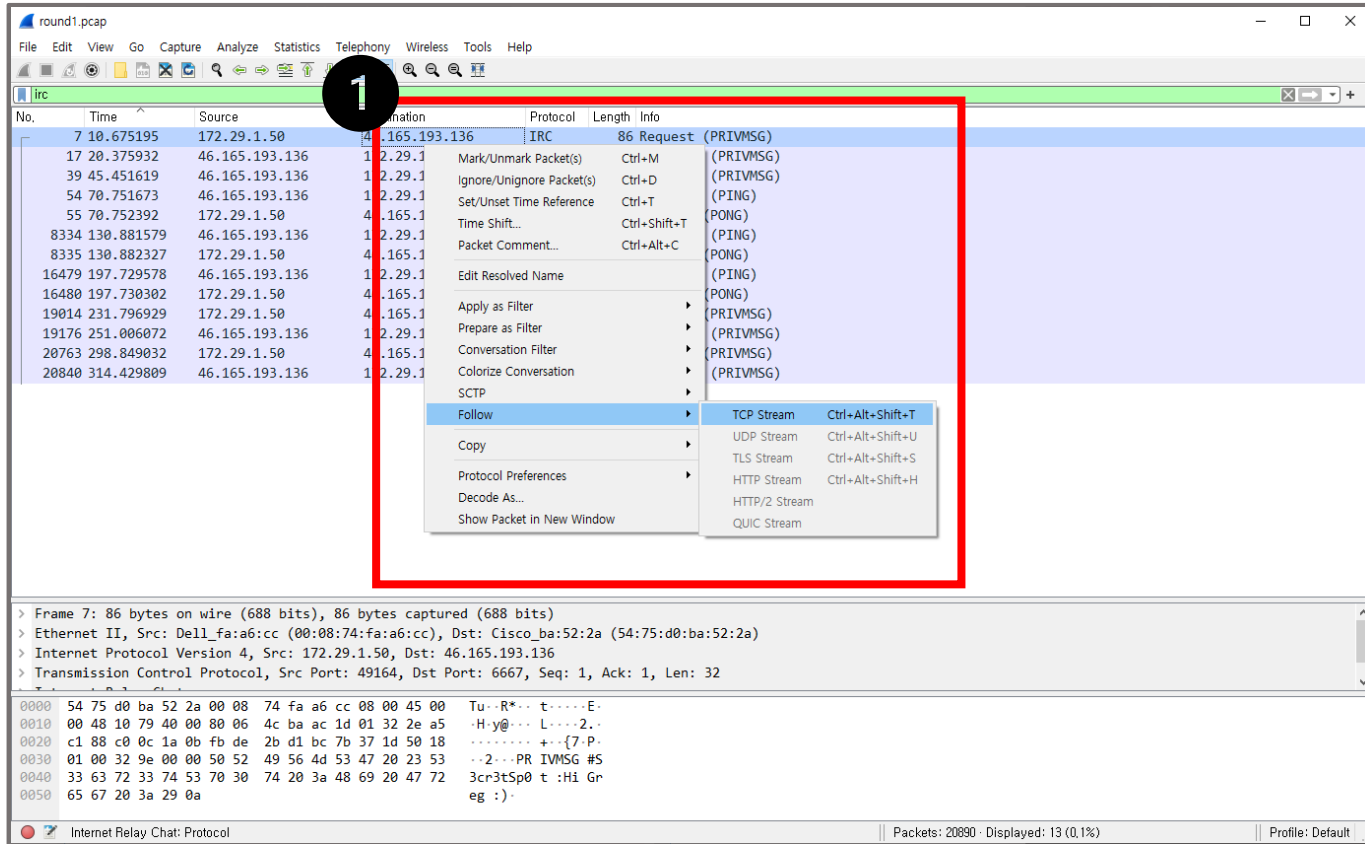
Round1



패킷 더블 클릭 : 해당 패킷의 헤더와 바디 정보 파악 가능

Part 3, DeFCoN#21 문제풀이

Round1



Follow -> TCP Stream : 해당 패킷의 흐름을 보여줌

Part 3, DeFCoN#21 문제풀이

Round1

1

```
Wireshark - Follow TCP Stream (tcp.stream eq 1) - round1.pcap
PRIVMSG #S3cr3tSp0t :Hi Greg :)
:D34thM3rch4nt!~blah2@7FF07A37.29E7D414.B9027CEB.IP PRIVMSG #S3cr3tSp0t :Hi Betty
:D34thM3rch4nt!~blah2@7FF07A37.29E7D414.B9027CEB.IP PRIVMSG #S3cr3tSp0t :what day do you want to meet up?
PING :hades.de.eu.SwiftIRC.net
PONG :hades.de.eu.SwiftIRC.net
PING :hades.de.eu.SwiftIRC.net
PONG :hades.de.eu.SwiftIRC.net
PING :hades.de.eu.SwiftIRC.net
PONG :hades.de.eu.SwiftIRC.net
PRIVMSG #S3cr3tSp0t
:&#x48;&#x6F;&#x77;&#x20;&#x64;&#x6F;&#x57;&#x20;&#x65;&#x64;&#x6E;&#x5;&#x73;&#x64;&#x61;&#x79;&#x20;&#x73;&#x6F;&#x75;&#x6E;&#x64;&#x3F;
:D34thM3rch4nt!~blah2@7FF07A37.29E7D414.B9027CEB.IP PRIVMSG #S3cr3tSp0t
:&#x47;&#x72;&#x65;&#x61;&#x74;&#x20;&#x3A;&#x29;&#x20;&#x77;&#x68;&#x61;&#x74;&#x20;&#x69;&#x6D;&#x65;&#x3F;
PRIVMSG #S3cr3tSp0t :&#x61;&#x68;&#x20;&#x32;&#x70;&#x6D;
:D34thM3rch4nt!~blah2@7FF07A37.29E7D414.B9027CEB.IP PRIVMSG #S3cr3tSp0t
:&#x4F;&#x6B;&#x2C;&#x20;&#x49;&#x20;&#x63;&#x61;&#x6E;&#x27;&#x74;&#x20;&#x77;&#x61;&#x69;&#x74;&#x21;
```

1

```
Wireshark - Follow TCP Stream (tcp.stream eq 1) - round1.pcap
PRIVMSG #S3cr3tSp0t :Hi Greg :)
:D34thM3rch4nt!~blah2@7FF07A37.29E7D414.B9027CEB.IP PRIVMSG #S3cr3tSp0t :Hi Betty
:D34thM3rch4nt!~blah2@7FF07A37.29E7D414.B9027CEB.IP PRIVMSG #S3cr3tSp0t :what day do you want to meet up?
PING :hades.de.eu.SwiftIRC.net
PONG :hades.de.eu.SwiftIRC.net
PING :hades.de.eu.SwiftIRC.net
PONG :hades.de.eu.SwiftIRC.net
PING :hades.de.eu.SwiftIRC.net
PONG :hades.de.eu.SwiftIRC.net
PRIVMSG #S3cr3tSp0t
:&#x48;&#x6F;&#x77;&#x20;&#x64;&#x6F;&#x57;&#x20;&#x65;&#x64;&#x6E;&#x5;&#x73;&#x64;&#x61;&#x79;&#x20;&#x73;&#x6F;&#x75;&#x6E;&#x64;&#x3F;
:D34thM3rch4nt!~blah2@7FF07A37.29E7D414.B9027CEB.IP PRIVMSG #S3cr3tSp0t
:&#x47;&#x72;&#x65;&#x61;&#x74;&#x20;&#x3A;&#x29;&#x20;&#x77;&#x68;&#x61;&#x74;&#x20;&#x69;&#x6D;&#x65;&#x3F;
PRIVMSG #S3cr3tSp0t :&#x61;&#x68;&#x20;&#x32;&#x70;&#x6D;
:D34thM3rch4nt!~blah2@7FF07A37.29E7D414.B9027CEB.IP PRIVMSG #S3cr3tSp0t
:&#x4F;&#x6B;&#x2C;&#x20;&#x49;&#x20;&#x63;&#x61;&#x6E;&#x27;&#x74;&#x20;&#x77;&#x61;&#x69;&#x74;&#x21;
```

Part 3, DeFCoN#21 문제풀이

Round1

Wireshark - Follow TCP Stream (tcp.stream eq 1) - round1.pcap

```
PRIVMSG #S3cr3tSp0t :Hi Greg :)
:D34thM3rch4nt!~b1ah2@7FF07A37.29E7D414.B9027CEB.IP PRIVMSG #S3cr3tSp0t :Hi Betty
:D34thM3rch4nt!~b1ah2@7FF07A37.29E7D414.B9027CEB.IP PRIVMSG #S3cr3tSp0t :what day do you want to meet up?
PING :hades.de.eu.SwiftIRC.net
PONG :hades.de.eu.SwiftIRC.net
PING :hades.de.eu.SwiftIRC.net
PONG :hades.de.eu.SwiftIRC.net
PING :hades.de.eu.SwiftIRC.net
PONG :hades.de.eu.SwiftIRC.net
PRIVMSG #S3cr3tSp0t :
:&#x48;&#x6F;&#x77;&#x20;&#x64;&#x6F;&#x65;&#x73;&#x20;&#x57;&#x65;&#x64;&#x6E;&#x65;&#x73;&#x64;&#x61;&#x79;&#x20;&#x73;&#x6F;&#x75;&#x6E;&#x64;&#x3F;
:D34thM3rch4nt!~b1ah2@7FF07A37.29E7D414.B9027CEB.IP PRIVMSG #S3cr3tSp0t :
:&#x47;&#x72;&#x65;&#x61;&#x74;&#x20;&#x3A;&#x29;&#x20;&#x77;&#x68;&#x61;&#x74;&#x20;&#x74;&#x69;&#x6D;&#x65;&#x3F;
PRIVMSG #S3cr3tSp0t :&#x61;&#x68;&#x20;&#x32;&#x70;&#x6D;
:D34thM3rch4nt!~b1ah2@7FF07A37.29E7D414.B9027CEB.IP PRIVMSG #S3cr3tSp0t :
:&#x4F;&#x6B;&#x2C;&#x20;&#x49;&#x20;&#x63;&#x61;&#x6E;&#x27;&#x74;&#x20;&#x77;&#x61;&#x69;&#x74;&#x21;
```

1

```
:&#x48;&#x6F;&#x77;&#x20;&#x64;&#x6F;&#x65;&#x73;&#x20;&#x57;&#x65;&#x64;&#x6E;&#x65;&#x73;&#x64;&#x61;&#x79;&#x20;&#x73;&#x6F;&#x75;&#x6E;&#x64;&#x3F;
:D34thM3rch4nt!~b1ah2@7FF07A37.29E7D414.B9027CEB.IP PRIVMSG #S3cr3tSp0t :
:&#x47;&#x72;&#x65;&#x61;&#x74;&#x20;&#x3A;&#x29;&#x20;&#x77;&#x68;&#x61;&#x74;&#x20;&#x74;&#x69;&#x6D;&#x65;&#x3F;
PRIVMSG #S3cr3tSp0t :&#x61;&#x68;&#x20;&#x32;&#x70;&#x6D;
:D34thM3rch4nt!~b1ah2@7FF07A37.29E7D414.B9027CEB.IP PRIVMSG #S3cr3tSp0t :
:&#x4F;&#x6B;&#x2C;&#x20;&#x49;&#x20;&#x63;&#x61;&#x6E;&#x27;&#x74;&#x20;&#x77;&#x61;&#x69;&#x74;&#x21;
```

Google How does Wednesday sound? X

List of ASCII and HTML codes

Symbol	ASCII; Decimal; Code	ASCII; Hexadecimal; Code	HTML; Decimal; Code	HTML; ...
^@	0	0	�	�
^A	1	1		
^B	2	2		

1019행 더보기

Round1

여기에 HTML 디코딩하고자하는 텍스트를 붙여 넣습니다

```
PRIVMSG #S3cr3tSp0t :&#x48;&#x6F;&#x77;&#x20;&#x64;&#x6F;&#x65;&#x73;&#x20;&#x57;&#x65;&#x64;&#x6E;&#x65;&#x73;&#x64;&#x61;&#x79;&#x20;&#x73;&#x6F;&#x75;&#x6E;&#x64;&#x3F;
:D34thM3rch4nt!~blah2@7FF07A37.29E7D414.B9027CEB.IP PRIVMSG #S3cr3tSp0t :&#x47;&#x72;&#x65;&#x61;&#x74;&#x20;&#x3A;&#x29;&#x20;&#x77;&#x68;&#x61;&#x74;&#x20;&#x74;&#x69;&#x6D;&#x65;&#x3F;
PRIVMSG #S3cr3tSp0t :&#x61;&#x68;&#x20;&#x32;&#x70;&#x6D;
:D34thM3rch4nt!~blah2@7FF07A37.29E7D414.B9027CEB.IP PRIVMSG #S3cr3tSp0t :&#x4F;&#x6B;&#x2C;&#x20;&#x49;&#x20;&#x63;&#x61;&#x6E;&#x27;&#x74;&#x20;&#x77;&#x61;&#x69;&#x74;&#x21;
```

개발자에게 딱 맞춘 이력서 양식

개발자 이력서 어떻게 쓰는지 고민되었다면, 이력서 양식 및 샘플/가이드까지 무료로 확인하세요 점핏

① X

HTML을 디코딩

열기

1

html로 여기에 텍스트를 디코딩 복사

```
PRIVMSG #S3cr3tSp0t :How does Wednesday sound?
:D34thM3rch4nt!~blah2@7FF07A37.29E7D414.B9027CEB.IP PRIVMSG #S3cr3tSp0t :Great :) what
time?
PRIVMSG #S3cr3tSp0t :ah 2pm
:D34thM3rch4nt!~blah2@7FF07A37.29E7D414.B9027CEB.IP PRIVMSG #S3cr3tSp0t :Ok, I can't
wait!
```

1

html로 여기에 텍스트를 디코딩 복사

```
PRIVMSG #S3cr3tSp0t :How does Wednesday sound?
:D34thM3rch4nt!~blah2@7FF07A37.29E7D414.B9027CEB.IP PRIVMSG #S3cr3tSp0t :Great :) what
time?
PRIVMSG #S3cr3tSp0t :ah 2pm
:D34thM3rch4nt!~blah2@7FF07A37.29E7D414.B9027CEB.IP PRIVMSG #S3cr3tSp0t :Ok, I can't
wait!
```


Round1

여기에 HTML 디코딩하고자하는 텍스트를 붙여 넣습니다

```
PRIVMSG #S3cr3tSp0t :&#x48;&#x6F;&#x77;&#x20;&#x64;&#x6F;&#x65;&#x73;&#x20;&#x57;&#x65;&#x64;&#x6E;&#x65;&#x73;&#x64;&#x61;&#x79;&#x20;&#x73;&#x6F;&#x75;&#x6E;&#x64;&#x3F;&#x47;&#x72;&#x65;&#x61;&#x74;&#x20;&#x3A;&#x29;&#x20;&#x77;&#x68;&#x61;&#x74;&#x20;&#x74;&#x69;&#x6D;&#x65;&#x3F;&#x4F;&#x6B;&#x2C;&#x20;&#x49;&#x20;&#x63;&#x61;&#x6E;&#x27;&#x74;&#x20;&#x77;&#x61;&#x69;&#x74;&#x21;
```

개발자에게 딱 맞춘 이력서 양식

개발자 이력서 어떻게 쓰는지 고민되었다면, 이력서 양식 및 샘플/가이드까지 무료로 확인하세요 점핏



HTML을 디코딩

열기

1

html로 여기에 텍스트를 디코딩 복사

```
PRIVMSG #S3cr3tSp0t :How does Wednesday sound?&#x20;&#x2D;&#x34;&#x44;&#x4D;&#x2D;&#x20;&#x77;&#x68;&#x61;&#x74;&#x20;&#x74;&#x69;&#x6D;&#x65;&#x3F;&#x4F;&#x6B;&#x2C;&#x20;&#x49;&#x20;&#x63;&#x61;&#x6E;&#x27;&#x74;&#x20;&#x77;&#x61;&#x69;&#x74;&#x21;Great :) what time?ah 2pmOk, I can't wait!
```

1

html로 여기에 텍스트를 디코딩 복사

```
PRIVMSG #S3cr3tSp0t :How does Wednesday sound?&#x20;&#x2D;&#x34;&#x44;&#x4D;&#x2D;&#x20;&#x77;&#x68;&#x61;&#x74;&#x20;&#x74;&#x69;&#x6D;&#x65;&#x3F;&#x4F;&#x6B;&#x2C;&#x20;&#x49;&#x20;&#x63;&#x61;&#x6E;&#x27;&#x74;&#x20;&#x77;&#x61;&#x69;&#x74;&#x21;Great :) what time?ah 2pmOk, I can't wait!
```


Round2

벤티는 그레고리와 만날 장소를 정할 때 자신의 행적을 감추려 한다.
이 폴더의 Round 2 패킷 캡처를 사용하여 다음 질문에 답하십시오.

그들은 어떤 도시에서 만납니까?



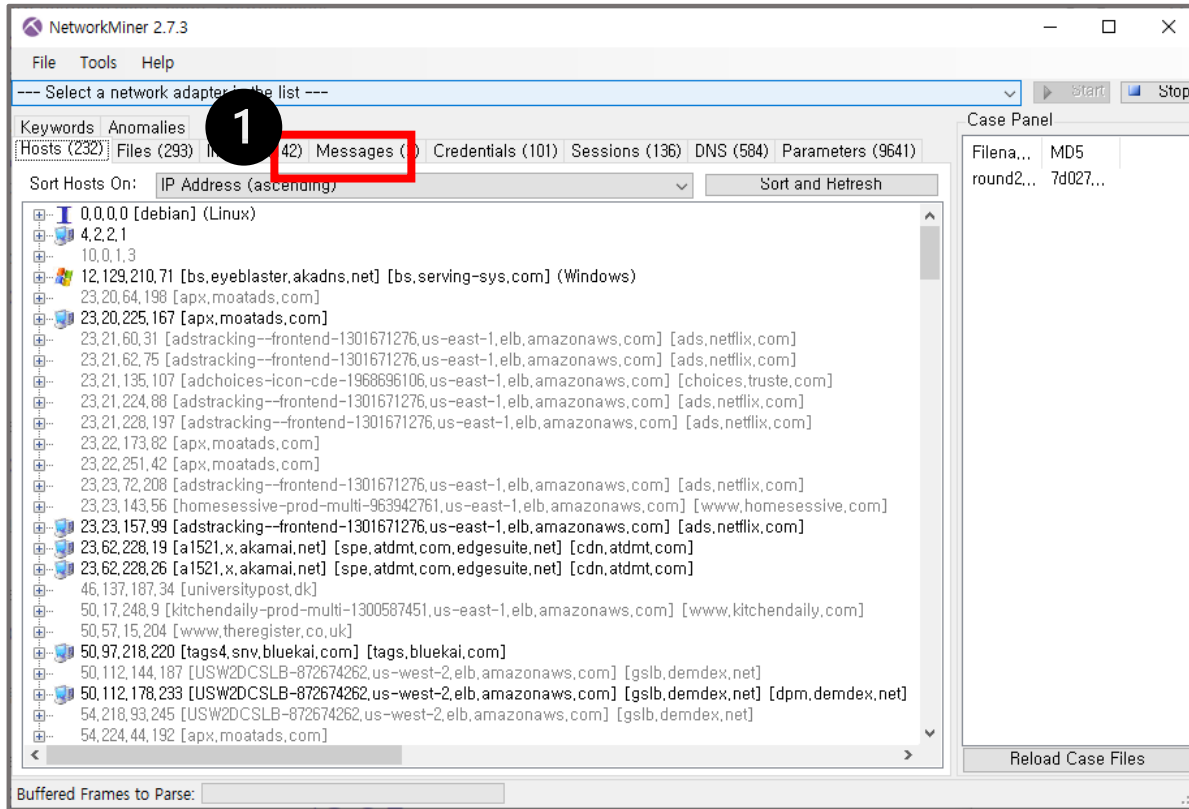
Jensen
(엔센씨)



Gregory
(그레고리씨)

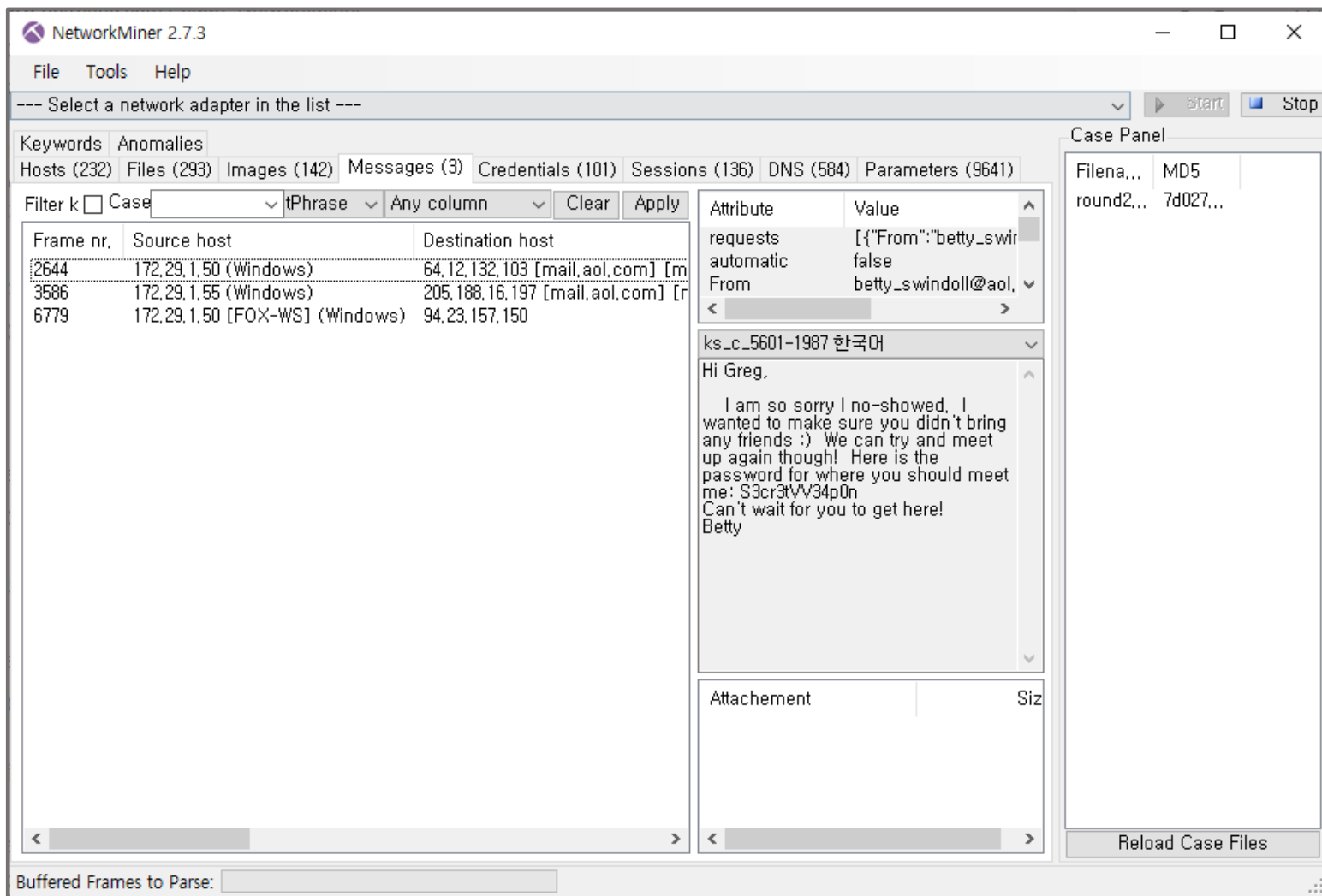
Part 3, DeFCoN#21 문제풀이

Round2



Messages : 패킷 패키지 안의 메시지를 복호화하여 보여줌

Round2



Round2

ks_c_5601-1987 한국어

Hi Greg.

I am so sorry I no-showed, I wanted to make sure you didn't bring any friends :) We can try and meet up again though! Here is the password for where you should meet me: S3cr3tVV34p0n
Can't wait for you to get here!
Betty

ks_c_5601-1987 한국어

Hi Betty,
I've got the password, I'll be there
Greg

-----Original Message-----
From: Betty Swindoll
<betty_swindoll@aol.com>
To: d34thm3rch4nt
<d34thm3rch4nt@aol.com>
Sent: Wed, Jul 3, 2013 10:01 am
Subject: Sorry

ks_c_5601-1987 한국어

DCC SEND r3nd3zv0us 2887582002
1024 819200_r

Round2

DCC

DCC allows you to connect **directly** to another IRC client, instead of going through the IRC Network, to **Send** and **Get** files, and to **Chat** privately over a more secure connection.

IRC 관련 프로토콜로, 파일을 교환할 때 사용. 단말기 대 단말기 통신을 위해 사용하는 프로토콜.

	To	Subject	Protocol	Timestamp	Size
l@aol.com	d34thm3rch4nt@aol.com,	Sorry	Http	2004-11-12 19:28:52 UTC	292
t@aol.com	betty_swindoll@aol.com,	Re: Sorry	Http	2004-11-12 19:30:07 UTC	541
	D34thM3rch4nt	rDCC SEND r3nd3zv0us 2887582002 1024 819200,	Irc	2004-11-12 19:31:54 UTC	68

DCC SEND <filename> <ip> <port> <file size>

Round2

round2.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

Resolved Addresses

1

Conversations

Endpoints

Packet Lengths

I/O Graphs

Service Response Time

DHCP (BOOTP) Statistics

ONC-RPC Programs

29West

ANCP

BACnet

Collectd

DNS

Flow Graph

HART-IP

HPFEEDS

HTTP

HTTP2

Sametime

TCP Stream Graphs

UDP Multicast Streams

F5

IPv4 Statistics

IPv6 Statistics

ts)

fa:a6:cc (00:08:74:fa:a6:cc)

IPV6 Statistics

Transmission Control Protocol, Src Port: 1024, Dst Port: 1024, Seq: 269, Ack: 211817, Len: 4

Data (4 bytes)

0000 00 08 74 fa a6 cc 00 0b cd c2 e4 91 08 00 45 00 ..t.....E..

0010 00 2c ba b8 40 00 00 06 e5 6f ac 1d 01 37 ac 1d ..,....o....7..

0020 01 32 04 00 04 00 2d ab 0f 1b 07 81 97 02 50 18 -2.....P...

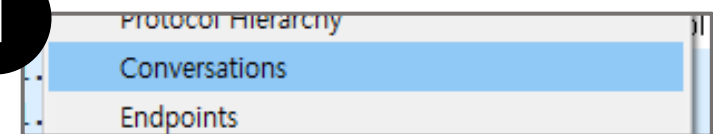
0030 ff ff 3c 24 00 00 03 35 b4 00 00 ...<\$.....5...

round2.pcap

Packets: 7618 · Displayed: 7618 (100.0%)

Profile: Default

1



호스트와 호스트 사이에 통신했던 연결을 보여줌.

Wireshark · Conversations · round2.pcap

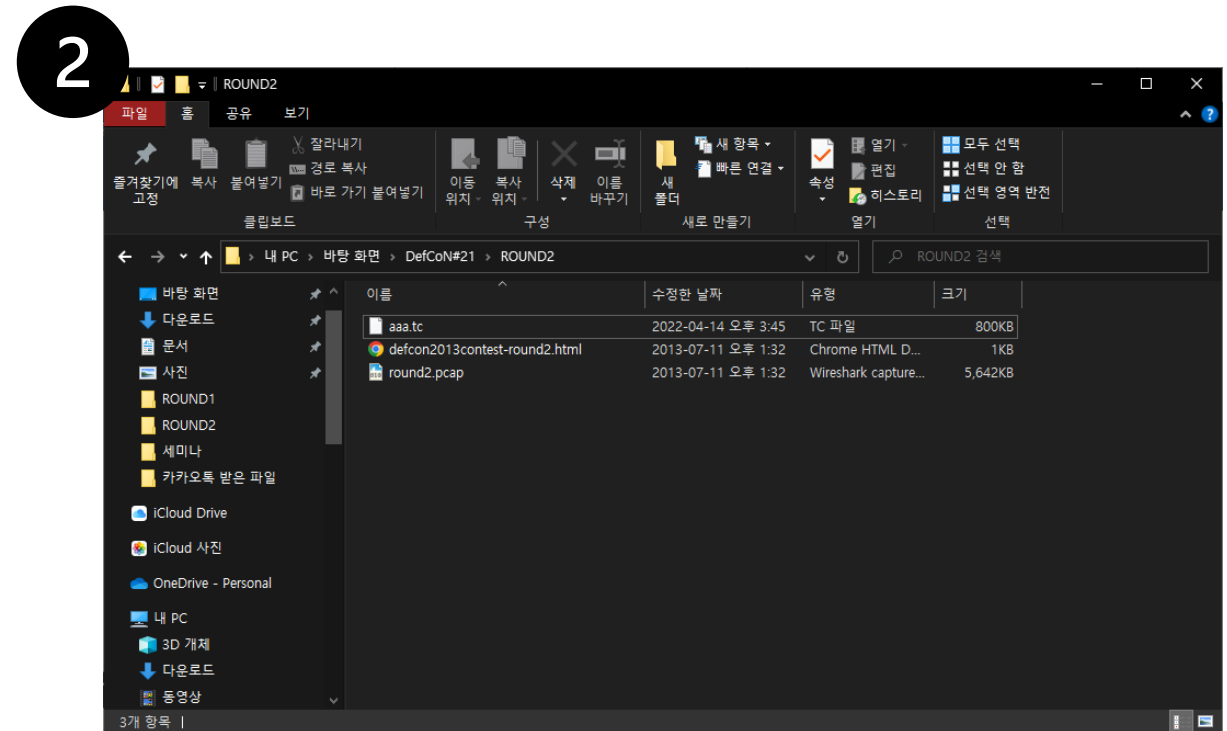
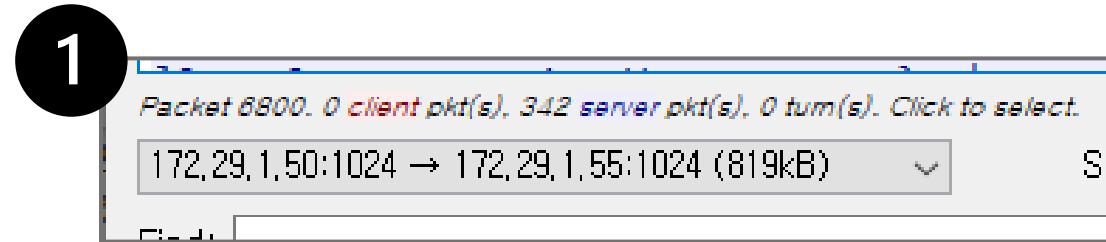
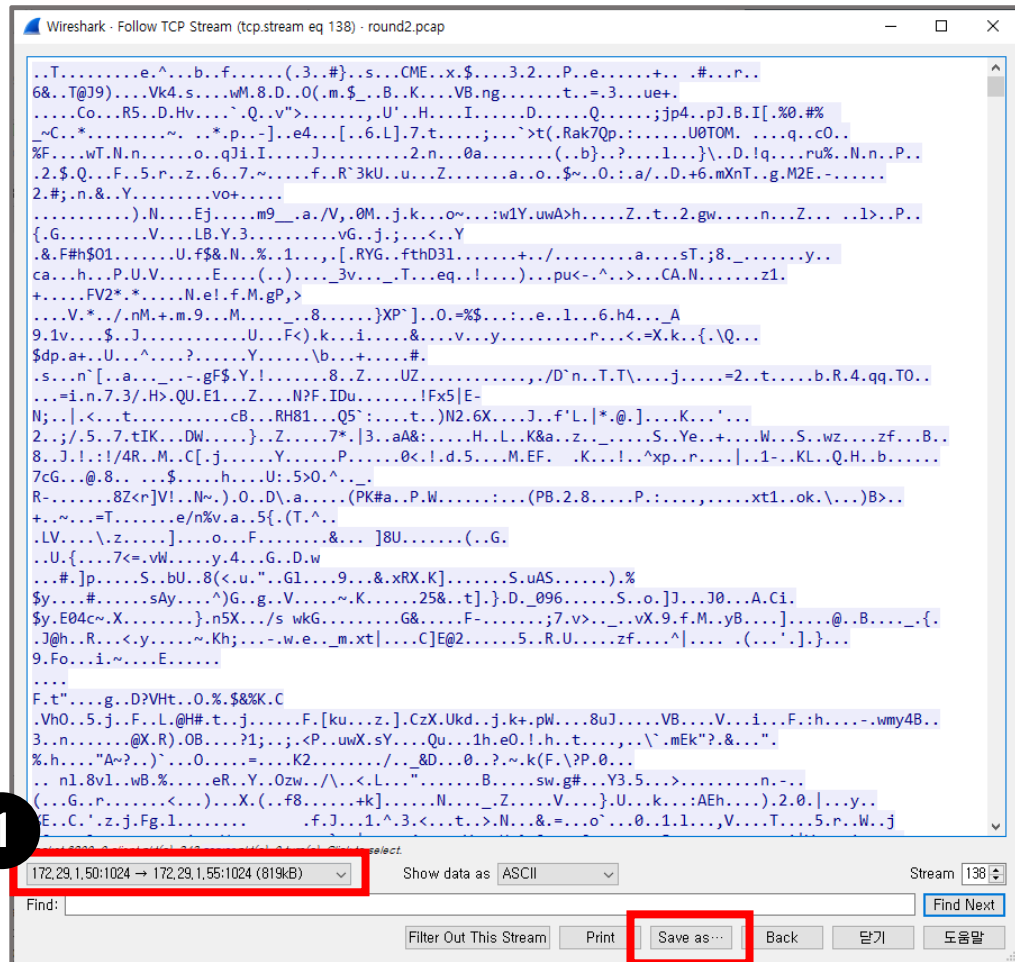
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
172.29.1.50	50564	23.23.157.99	443	14	5816	8	1974	6	3842	113.183145	1.2328	12k	24k
172.29.1.50	50565	12.129.210.71	80	8	2090	5	1345	3	745	113.528196	0.6241	17k	9549
172.29.1.50	50566	54.230.140.148	80	25	20k	14	3412	11	16k	114.32375c	3.8267	7133	34k
172.29.1.50	50567	64.12.79.64	80	9	1605	6	807	3	798	114.719487	5.3734	1201	1188
172.29.1.50	50568	54.225.189.169	80	9	1833	5	971	4	862	115.630224	0.3935	19k	17k
172.29.1.50	50569	96.17.148.130	80	46	39k	26	2563	20	36k	115.748404	0.2021	101k	1456k
172.29.1.50	50570	96.17.148.105	80	12	5147	7	1642	5	3505	117.66825c	0.8885	14k	31k
172.29.1.50	50571	216.120.27.21	80	9	1150	5	649	4	501	117.872651	0.1349	38k	29k
172.29.1.50	50572	54.230.140.148	80	6	372	4	246	2	126	117.976621	5.1387	352	196
172.29.1.50	50573	68.142.253.31	80	7	1716	4	847	3	869	118.66240c	0.2694	25k	25k
172.29.1.50	1024	172.29.1.55	1024	810	865k	381	840k	429	25k	140.39936c	1.8551	3622k	111k
172.29.1.55	3700	74.125.129.99	80	50	38k	21	2980	29	35k	14.844368	117.9632	202	2426
172.29.1.55	3701	74.125.129.99	80	254	205k	109	14k	145	191k	5.076980	135.3710	830	11k
172.29.1.55	3702	74.125.129.99	80	1,072	906k	428	59k	644	846k	5.148193	142.3618	3352	47k
172.29.1.55	3703	74.125.129.99	80	10	1340	6	969	4	371	6.018414	115.7920	66	25
172.29.1.55	3704	74.125.224.175	80	34	22k	15	1550	19	20k	7.524769	117.3027	105	1402
172.29.1.55	3705	74.125.224.180	80	70	49k	30	4597	40	44k	11.705583	134.8305	272	2663
172.29.1.55	3706	74.125.224.196	80	10	1529	6	1153	4	376	24.520496	115.9477	79	25
172.29.1.55	3707	74.125.224.177	80	24	13k	12	1348	12	12k	24.548973	117.9198	91	854
172.29.1.55	3708	74.125.224.178	80	45	28k	21	2496	24	26k	24.550972	121.9851	163	1736
172.29.1.55	3709	74.125.224.178	80	32	20k	15	2102	17	18k	24.551741	121.9846	137	1206
172.29.1.55	3710	74.125.224.177	80	22	12k	11	1266	11	11k	24.552206	115.9155	87	799
172.29.1.55	3711	74.125.224.178	80	44	27k	22	2658	22	25k	24.600452	122.9298	172	1630
172.29.1.55	3712	74.125.224.177	80	24	15k	11	1252	13	14k	24.600951	115.8667	86	967
172.29.1.55	3713	74.125.224.180	80	40	24k	20	2490	20	21k	24.608455	122.9218	162	1427
172.29.1.55	3714	74.125.224.177	80	24	14k	12	1344	12	12k	24.610674	116.8719	91	882
172.29.1.55	3715	74.125.224.177	80	48	32k	21	3086	27	29k	24.611166	121.9252	202	1938
172.29.1.55	3716	74.125.224.180	80	49	30k	24	2684	25	28k	24.611665	122.9186	174	1840
172.29.1.55	3717	74.125.224.180	80	104	83k	49	8147	55	76k	24.612206	122.9186	512	6001

Name resolution Limit to display filter Absolute start time

Conversation Types

Copy Follow Stream Graph 닫기 도움말

Round2



Round2

파일 확장자 홈 / 모든 확장자 / 파일 확장자 TC

TC 파일 유형

저자 [Jay Geater](#) | 편집: November 26, 2018

Silver
Microsoft
Partner

TC 파일 요약

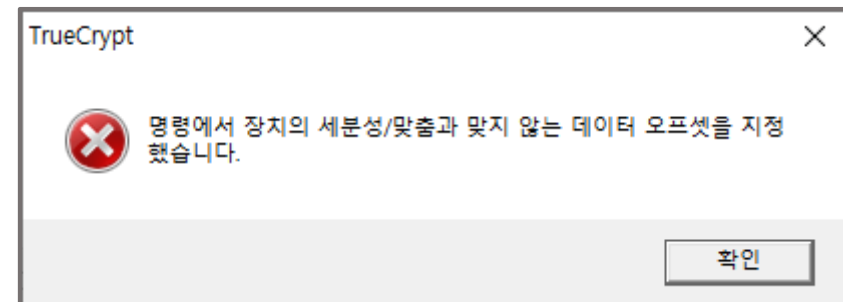
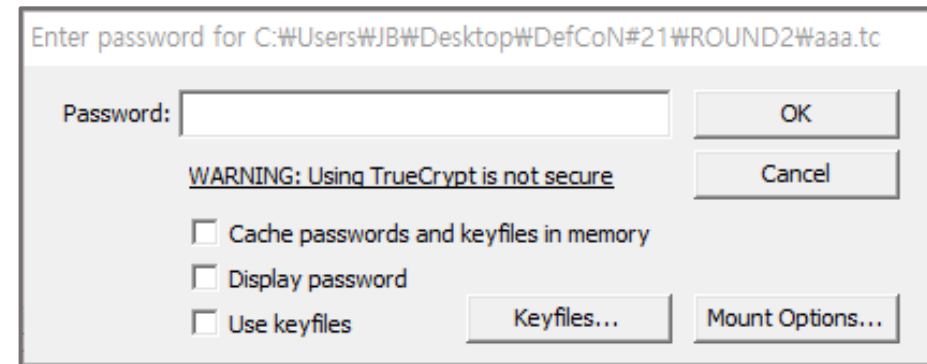
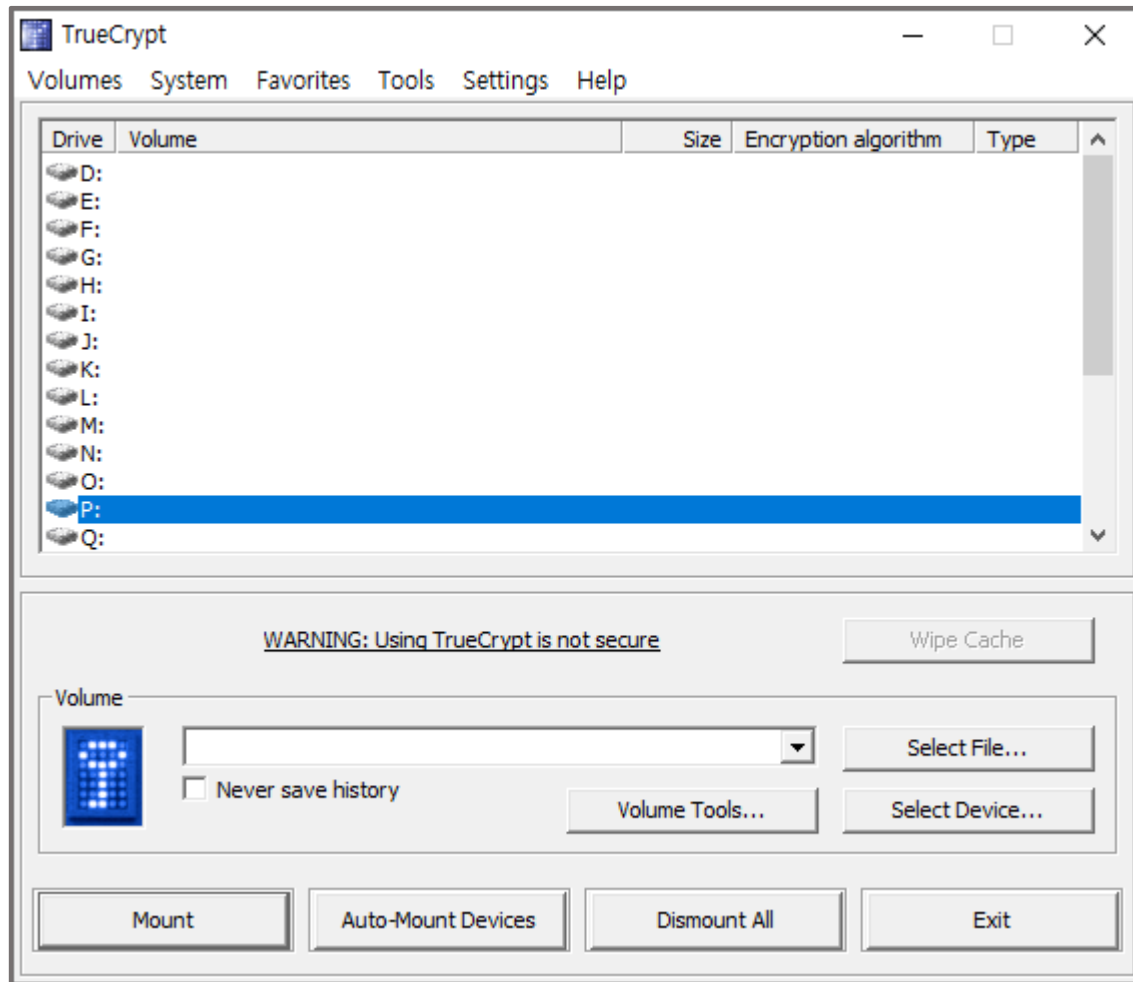
TC파일은 이개의 파일 형식과 연결되며 **TrueCrypt**의 **TrueCrypt**를 통해 볼 수 있습니다. 집합적으로 이 형식은 이개의 알려진 소프트웨어 응용 프로그램과 연결됩니다. 이 형식은 일반적으로 파일 형식 **TrueCrypt Volume**에서 찾을 수 있습니다. TC 파일은 대부분 **Disk Image Files**로 분류됩니다. 그 외의 파일 형식들은 Data Files가 될 수 있습니다.

Windows, Linux 운영 체제를 사용하여 TC 파일을 볼 수 있습니다. 이들은 데스크톱 (및 일부 모바일) 장치에서 흔히 볼 수 있으며 이러한 파일을 보거나 때때로 편집할 수 있게 해줍니다. 주요 파일 형식 TC의 인기도는 "낮음"이고 이들 파일은 종종 일반 데스크톱이나 모바일 장치에서 찾을 수 없습니다.

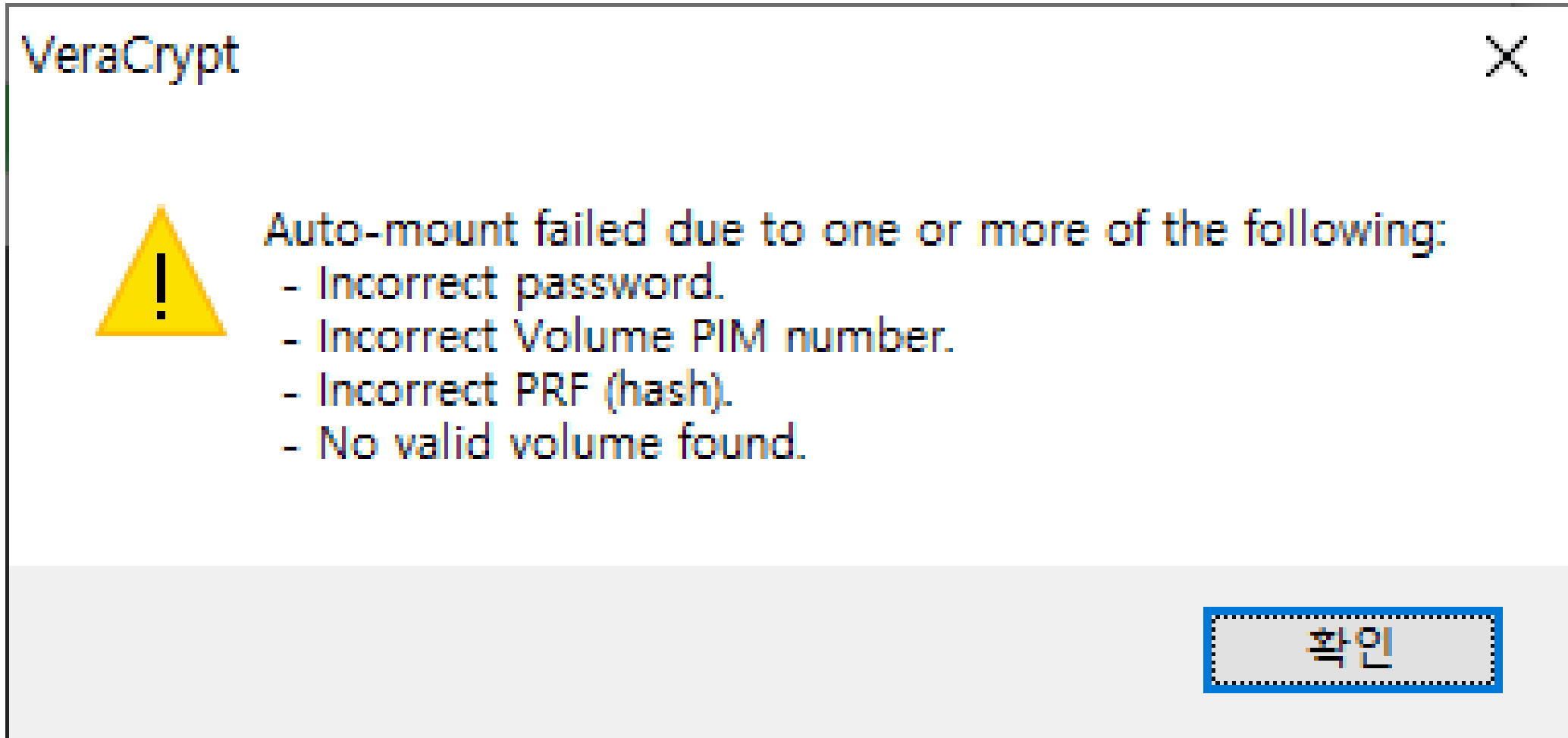
TC파일 및 파일을 여는 소프트웨어에 대한 자세한 내용은 아래의 추가 세부 정보를 참조하십시오. 또한 이러한 파일을 여는 데 문제가 있는 경우 기본 TC 파일 문제 해결 방법을 배울 수 있습니다.



Round2



Round2



Round2

