2022-04-14

네트워크 패킷 포렌식 및 문제풀이

201812745 김종원

ⓒSaebyeol Yu. Saebyeol's PowerPoint

A Table of Contents.

1 네트워크 포렌식

2 네트워크 패킷 포렌식

3 DEFCON#21 문제풀이

ⓒSaebyeol Yu. Saebyeol's PowerPoint

네트워크 포렌식이란?

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

ⓒSaebyeol Yu. Saebyeol's PowerPoint

네트워크 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

ⓒSaebyeol Yu. Saebyeol's PowerPoint

네트워크 포렌식

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 힘듦**

ⓒSaebyeol Yu. Saebyeol's PowerPoint

네트워크 증거수집 방법(1) – 시스템

- 사라지기 쉬운 시스템 정보

기본 정보	시간 정보	사용자 정보
• OS • Version • Resource • Install Package 등	• 로컬시간 확인 • 채증 시간 저장 • 실행 중인 프로세스 Up/Down 타임 • 파일 MAC 타임	• 계정정보 • Remote user account • Remote IP • 실제 사용자 식별 정보

- 사라지기 쉬운 시스템상의 **네트워크 정보**

분석 및 조사
• MAC 주소 • IP주소 • 라우팅 테이블 • 알려진 서비스의 내용 • 공유 정보 • 세션 정보

ⓒSaebyeol Yu. Saebyeol's PowerPoint

네트워크 포렌식

네트워크 증거수집 방법(2) – 네트워크 시스템

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

Router	Switch
• 로그 발생 시간 • 라우터에서 발생된 로그 • Address & Host Mapping • System 버전 • 보안 제어	• 로그 발생 시간 • 스위치에서 발생된 로그 • VLAN 통신파악 • User IP 주소와 MAC 확인 • 포트 사용 여부 확인

ⓒSaebyeol Yu. Saebyeol's PowerPoint

네트워크 포렌식

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 발생된 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

ⓒSaebyeol Yu. Saebyeol's PowerPoint

네트워크 포렌식

네트워크 증거수집 방법(4) – 패킷 캡쳐 도구(스니퍼)

- Windump

```
C:₩Users₩kaspyx>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 ]

C:₩Users₩kaspyx>
```

- 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
```

ⓒSaebyeol Yu. Saebyeol's PowerPoint

네트워크 패킷 포렌식이란?

네트워크 패킷 포렌식은 종단간 수집된 패킷에 대해 분석 하는 기술

ⓒSaebyeol Yu. Saebyeol's PowerPoint

네트워크 패킷 포렌식

네트워크 패킷 포렌식

ⓒSaebyeol Yu. Saebyeol's PowerPoint

네트워크 포렌식

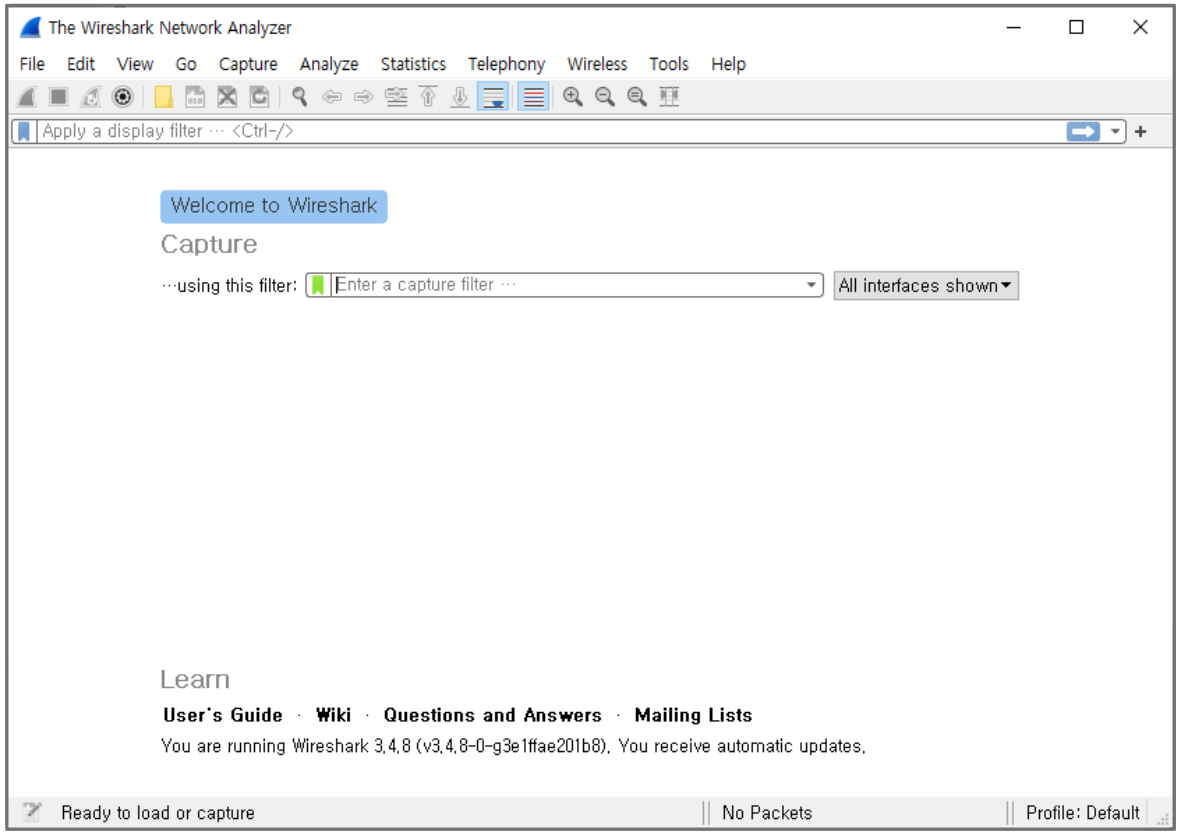
네트워크 포렌식 – 수집 정보

- 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

ⓒSaebyeol Yu. Saebyeol's PowerPoint

네트워크 패킷 포렌식

네트워크 패킷 포렌식 도구 – Wireshark

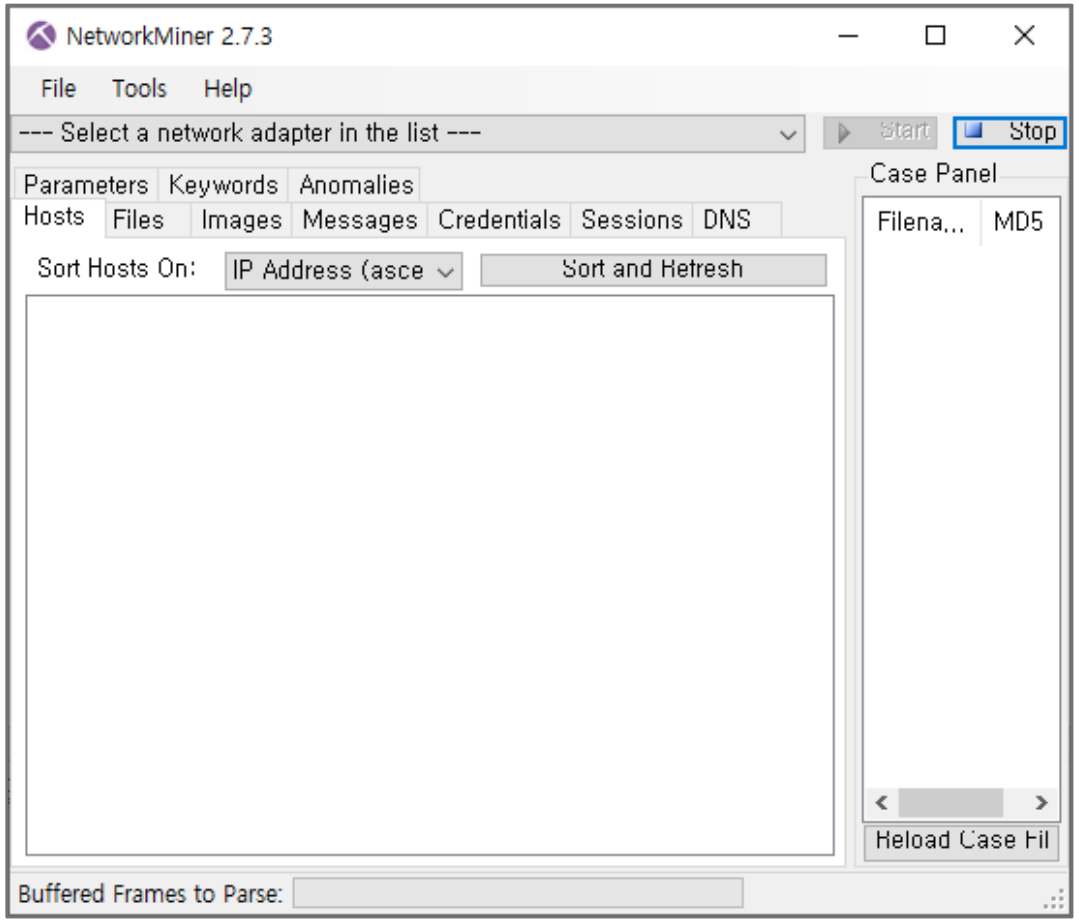


- 무료로 사용 할 수 있는 패킷 캡처 도구
- 많은 기능과 플러그인 지원.
- 강력한 필터 기능 지원
- CLI 패킷 분석 도구 지원
- AND(&&), OR(||), NOT(!) 같은 논리 연산 사용 가능
  ex) dst host 192.168.0.1 && tcp port 1024

ⓒSaebyeol Yu. Saebyeol's PowerPoint

네트워크 패킷 포렌식

네트워크 패킷 포렌식 도구 – NetworkMinor

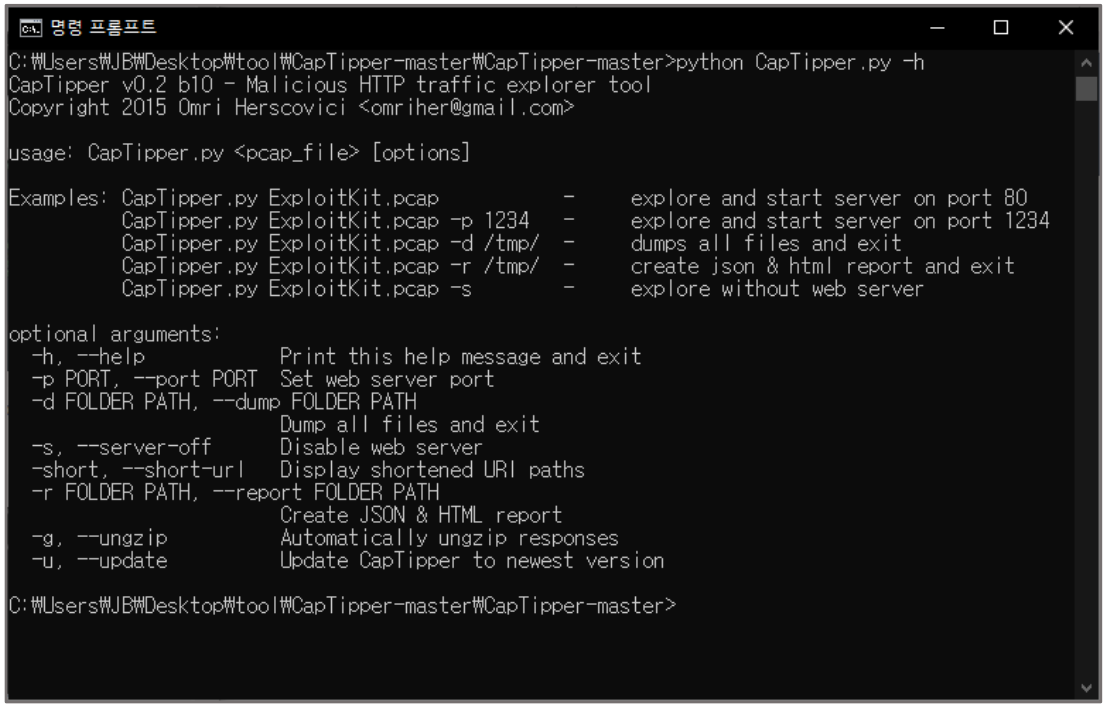


- 다양한 파싱 기능을 지원
- 네트워크 패킷 캡쳐 기능 지원
- 무료/유로 버전으로 나뉘어 제공

ⓒSaebyeol Yu. Saebyeol's PowerPoint

네트워크 패킷 포렌식

네트워크 패킷 포렌식 도구 – CapTipper(캡티퍼)



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

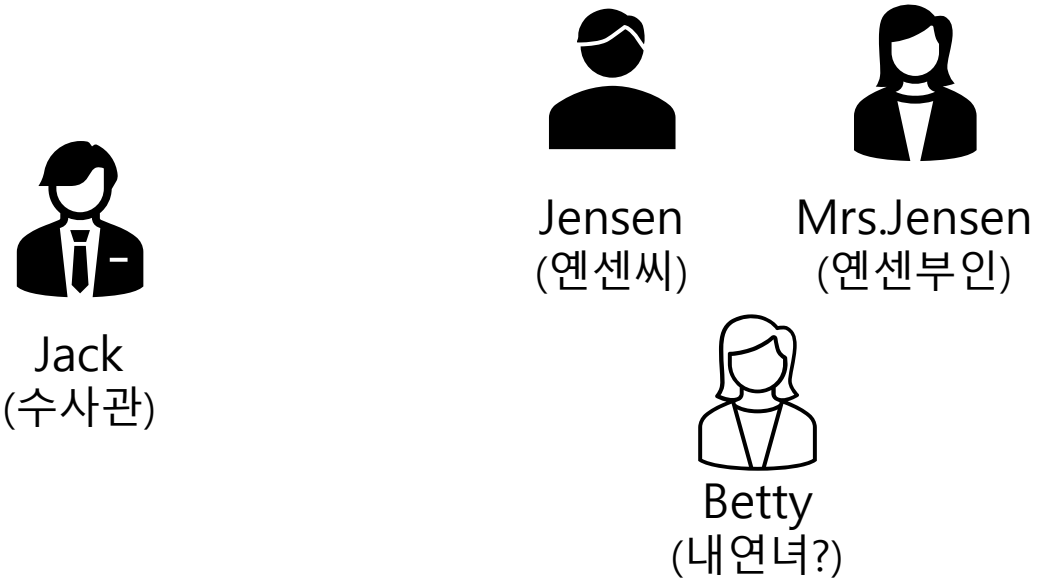
ⓒSaebyeol Yu. Saebyeol's PowerPoint

DeFCoN #21 문제풀이

Round1

Jensen 사건을 맡게 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 캡쳐 정보를 자세히 보여준다.
그리고 **회의가 진행된다**. Round 1 패킷을 사용해서 사건에 대해 자세히 알아보고 다음의 질문에 답 하시오.

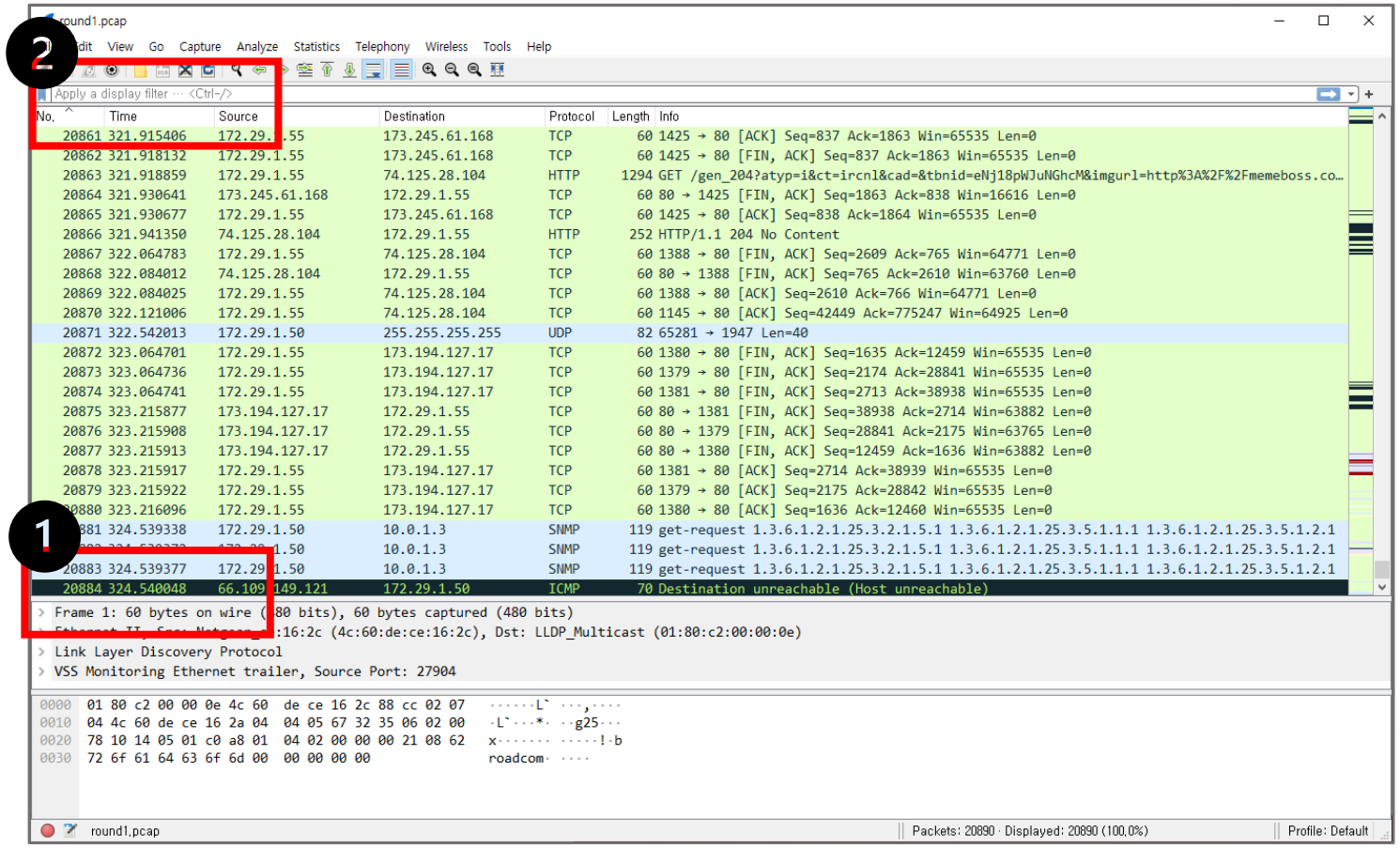
회의가 예정된 요일은 언제인가?

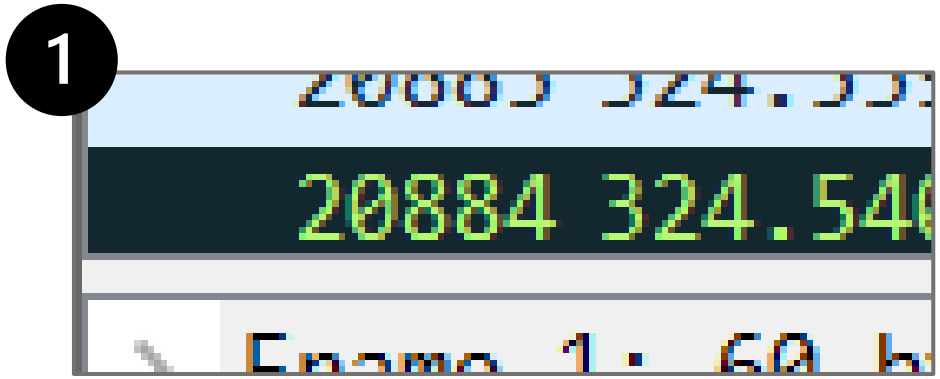


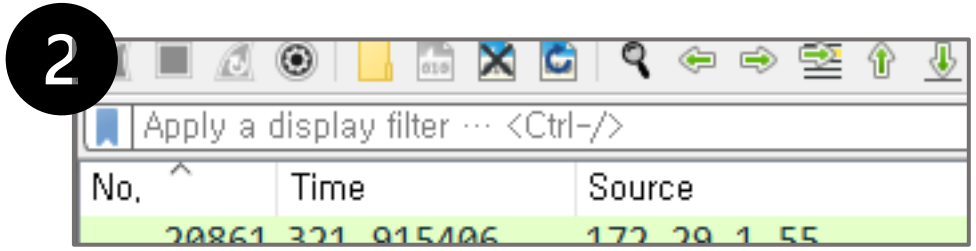
ⓒSaebyeol Yu. Saebyeol's PowerPoint

DeFCoN#21 문제풀이

Round1



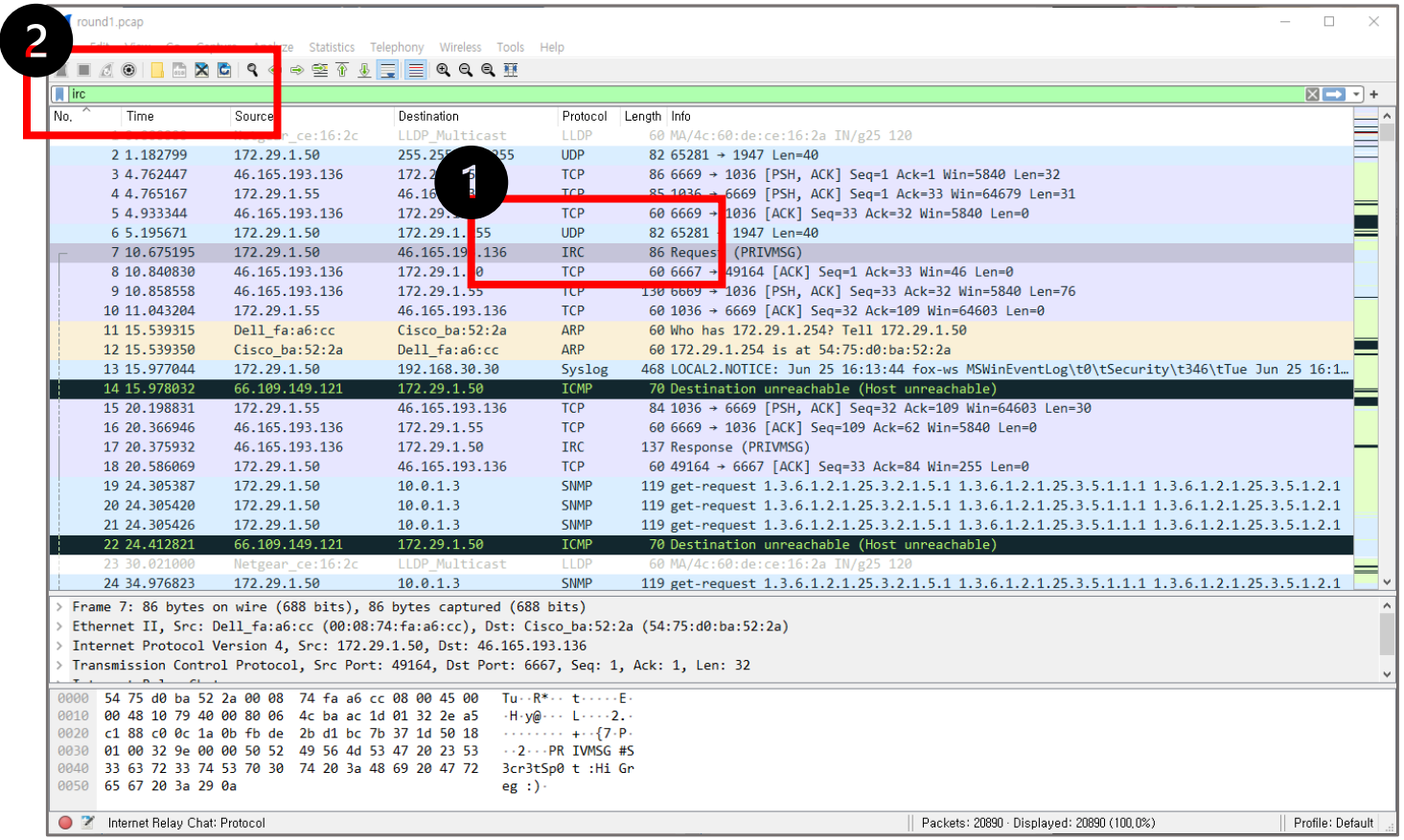


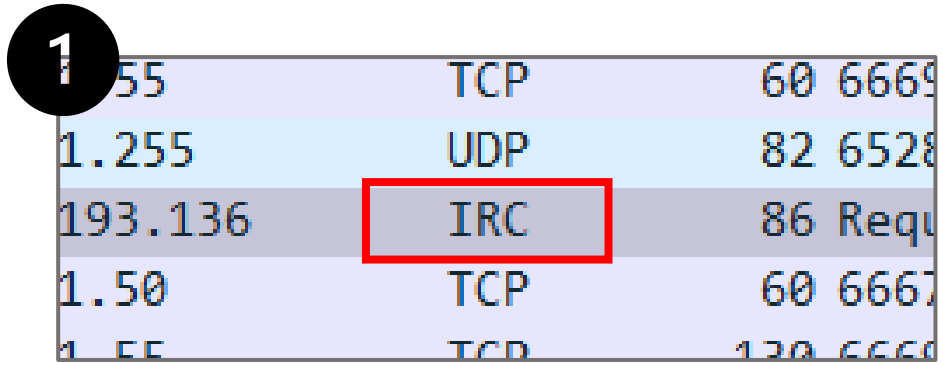


ⓒSaebyeol Yu. Saebyeol's PowerPoint

DeFCoN#21 문제풀이

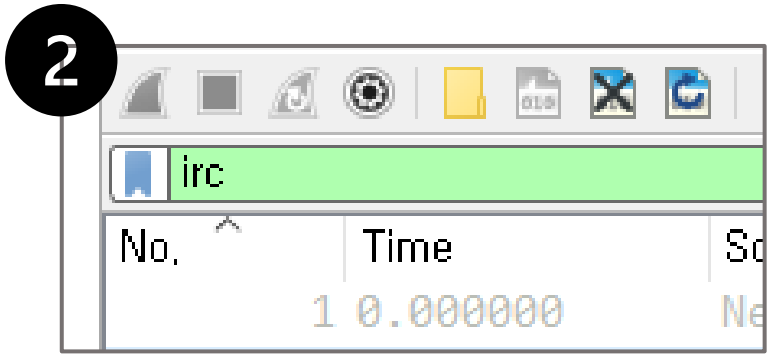
Round1





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]

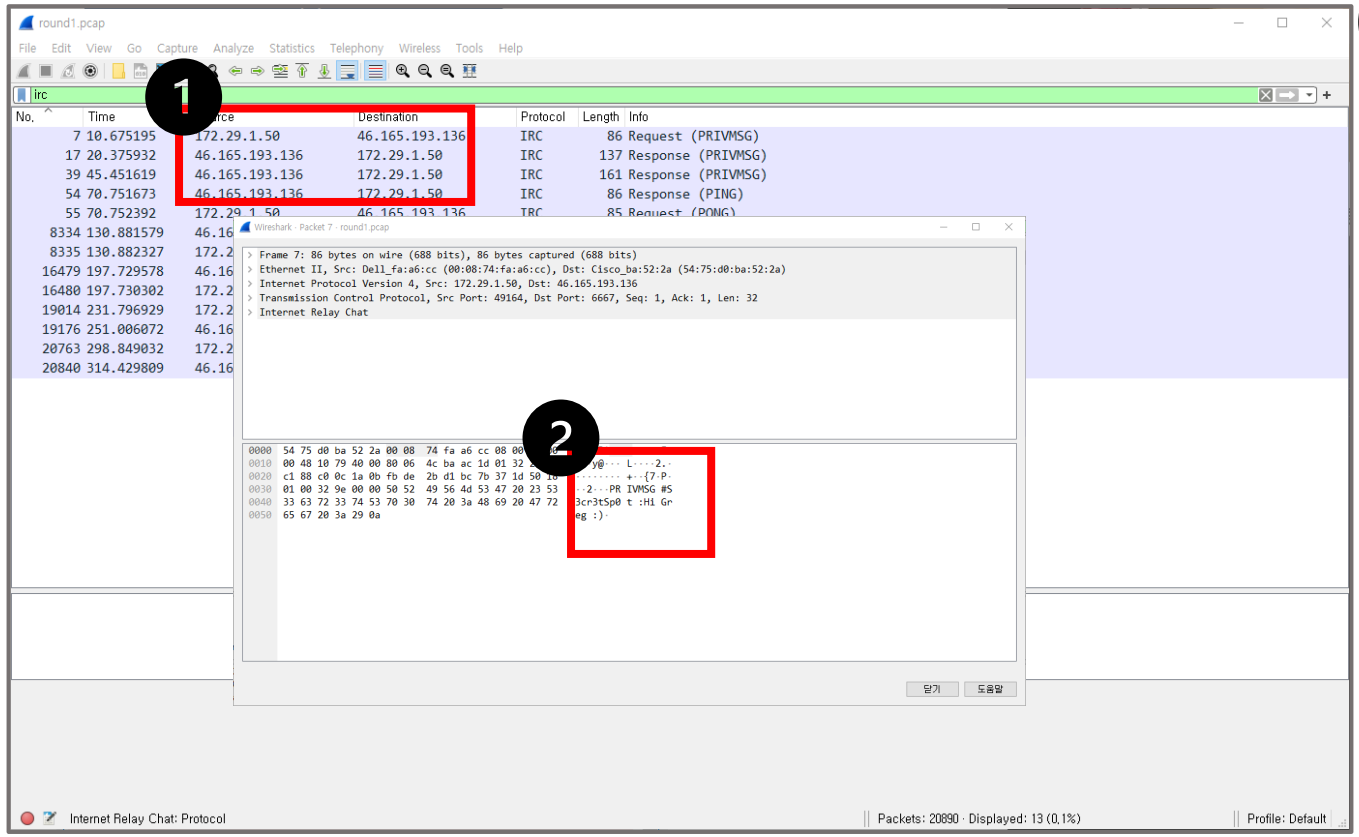
그리고 IRC는 전통적인 채팅 프로토콜로, 이를 지원하는 수많은 서버 네트워크와 클라이언트가 존재한다.



ⓒSaebyeol Yu. Saebyeol's PowerPoint

DeFCoN#21 문제풀이

Round1



1

Source	Destination
172.29.1.50	46.165.193.136
46.165.193.136	172.29.1.50

2

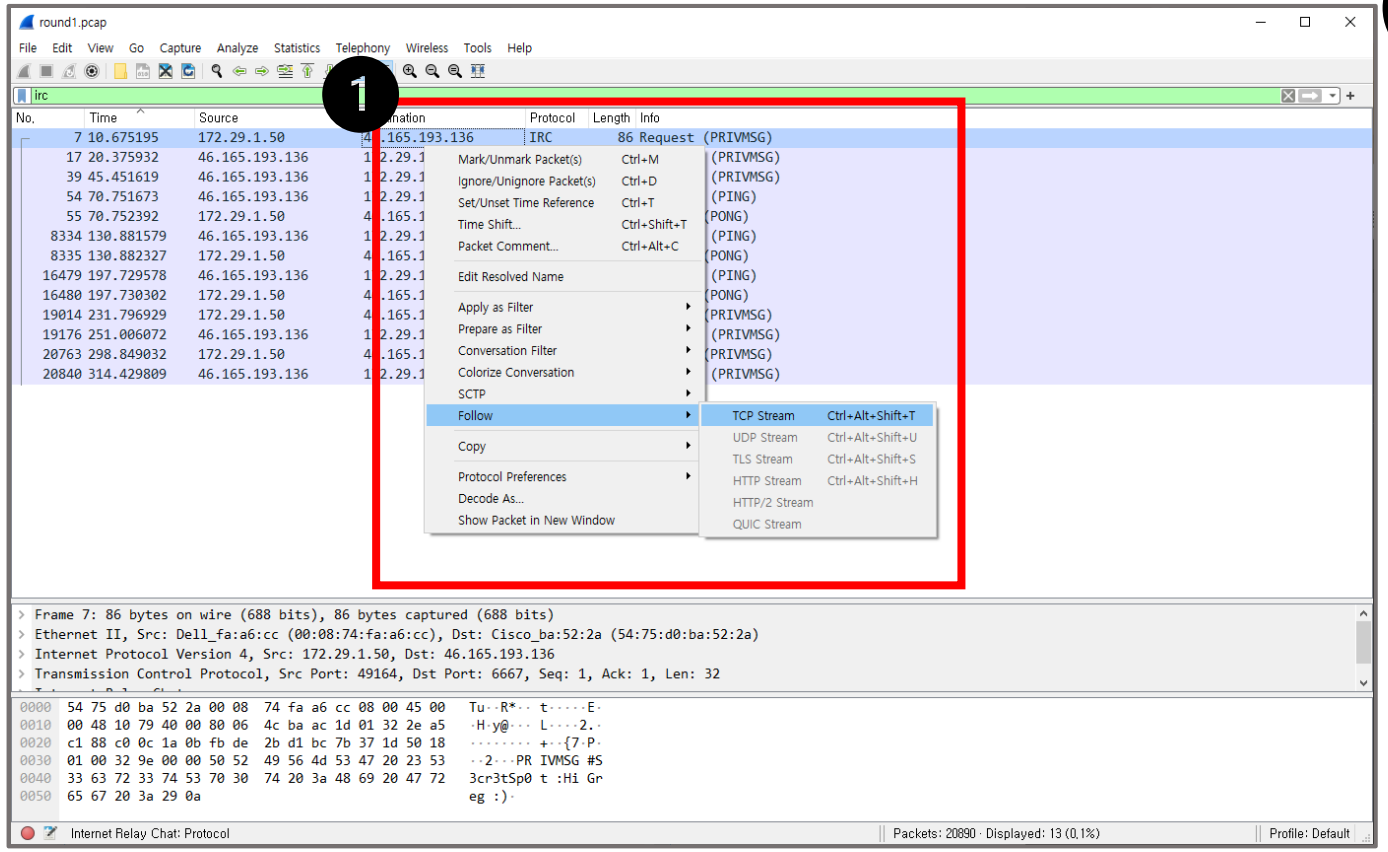
```
0   Tu··R*·· t·····E·
5   ·H·y@··· L····2.·
8   ····· t··{7·P·
3   ··2···PR IVMSG #S
2   3cr3tSp0 t :Hi Gr
    eg :)·
```

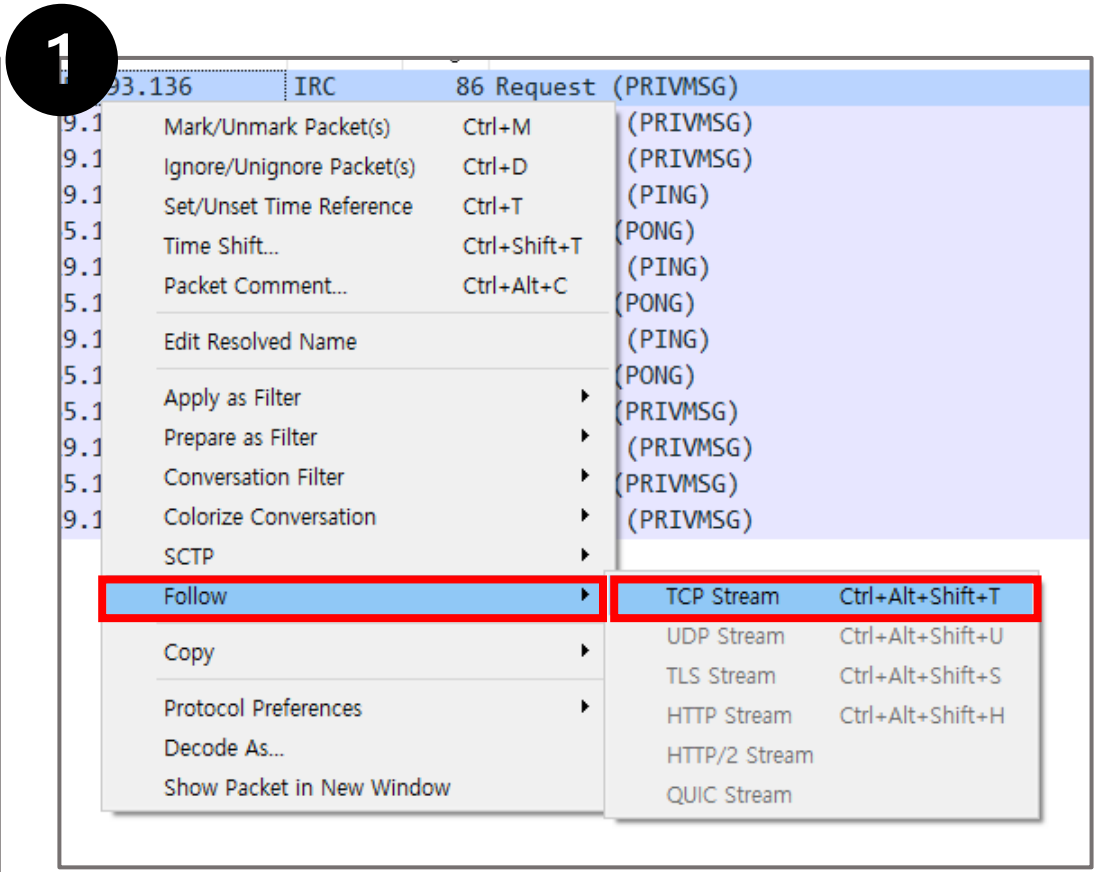
패킷 더블 클릭 : 해딩 패킷의 헤더와 바디 정보 파악 가능

ⓒSaebyeol Yu. Saebyeol's PowerPoint

DeFCoN#21 문제풀이

Round1





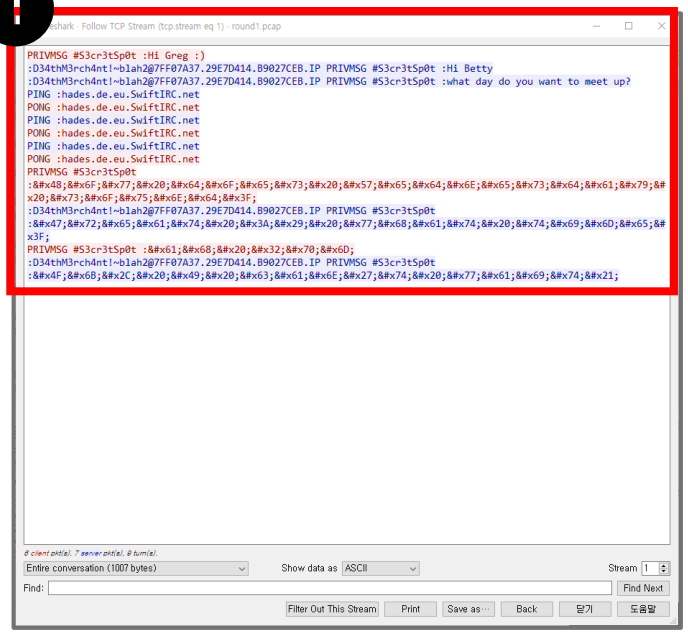
Follow -> TCP Stream : 해딩 패킷의 흐름을 보여줌

ⓒSaebyeol Yu. Saebyeol's PowerPoint

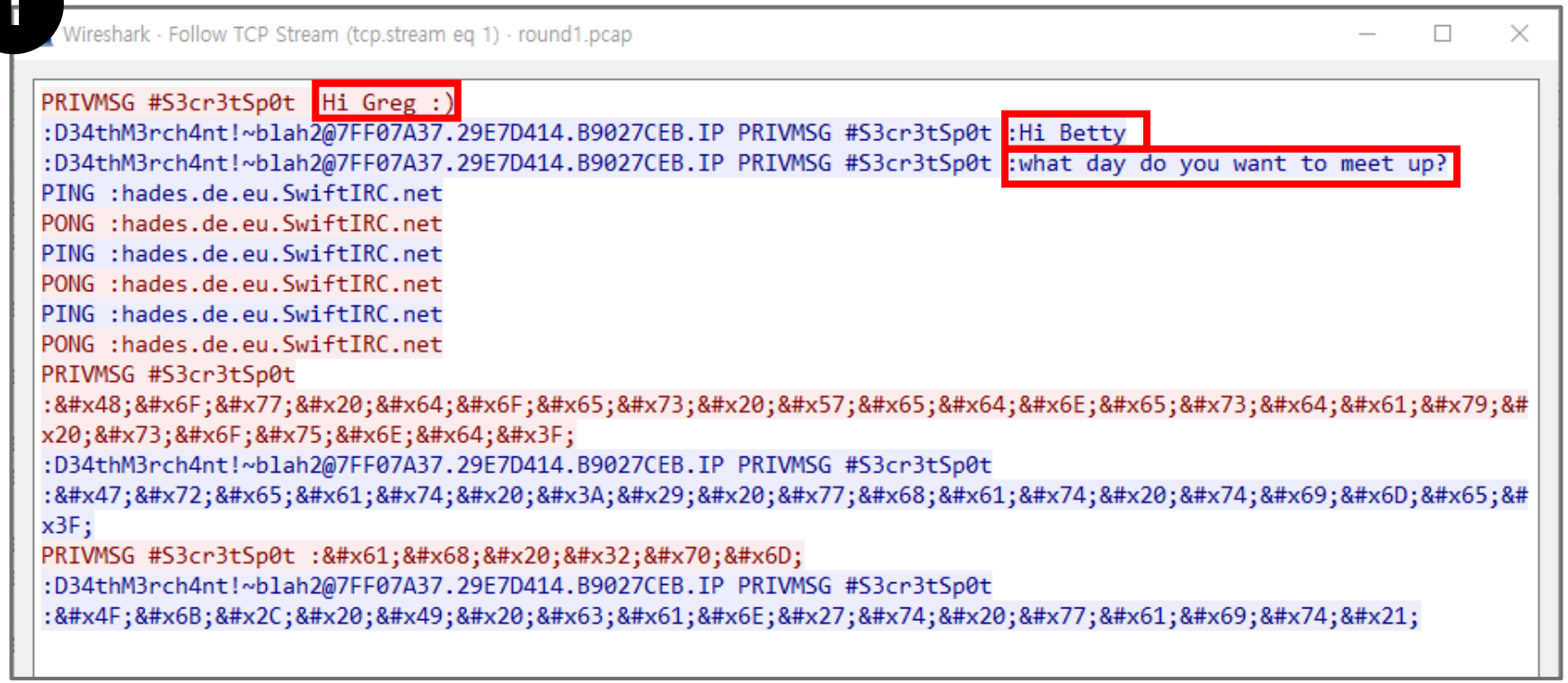
DeFCoN#21 문제풀이

Round1

1



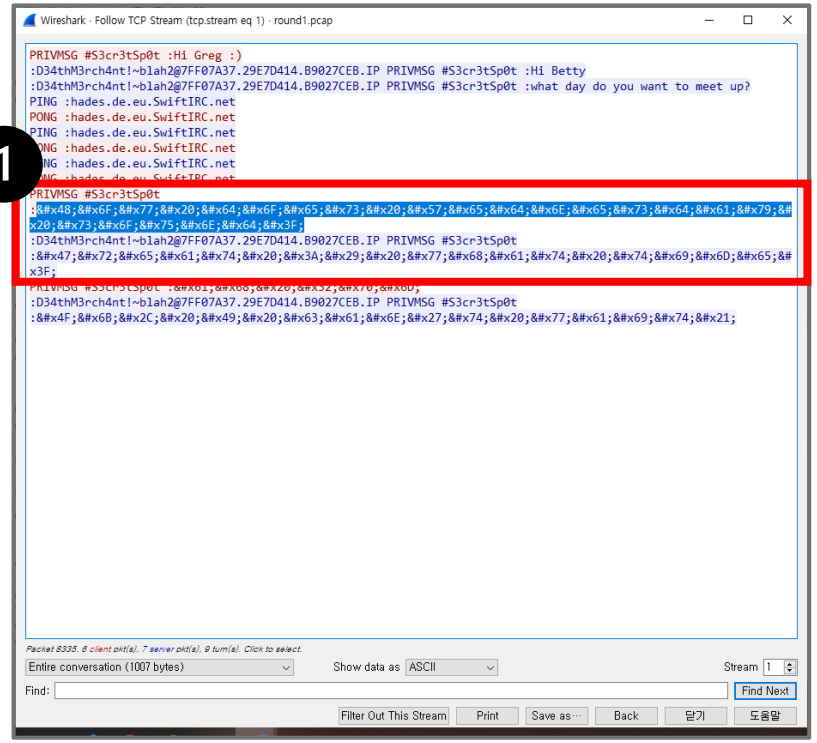
1



ⓒSaebyeol Yu. Saebyeol's PowerPoint

DeFCoN#21 문제풀이

Round1



1

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!~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;
```

Google How do&#x65

List of ASCII and HTML codes

Symbol	ASCII; Decimal; Code	ASCII; Hexadecimal; Code	HTML; Decimal; Code	HTML; …
^@	0	0	&#0	&#x0
^A	1	1	&#1	&#x1
^B	2	2	&#2	&#x2

1019행 더보기

ⓒSaebyeol Yu. Saebyeol's PowerPoint

DeFCoN#21 문제풀이

Round1

여기에 HTML 디코딩하고자하는 텍스트를 붙여 넣습니다

PRIVMSG #S3cr3tSp0t
:How does Wedne
sday sound?
:D34thM3rch4nt!~blah2@7FF07A37.29E7D414.B9027CEB.IP PRIVMSG #S3cr3tSp0t
:Great :) what &
#x74;ime?
PRIVMSG #S3cr3tSp0t :ah 2pm
:D34thM3rch4nt!~blah2@7FF07A37.29E7D414.B9027CEB.IP PRIVMSG #S3cr3tSp0t
:Ok, I can't wa
it!

개발자에게 딱 맞춘 이력서 양식
개발자 이력서 어떻게 쓰는지 고민되었다면, 이력서 양식 및 샘플/가이드까지 무료로 확인하세요 점핏
열기

HTML을 디코드!

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!

ⓒSaebyeol Yu. Saebyeol's PowerPoint

DeFCoN#21 문제풀이

Round1

여기에 HTML 디코딩하고자하는 텍스트를 붙여 넣습니다

PRIVMSG #S3cr3tSp0t
:How does Wedne
sday sound?
:D34thM3rch4nt!~blah2@7FF07A37.29E7D414.B9027CEB.IP PRIVMSG #S3cr3tSp0t
:Great :) what &
#x74;ime?
PRIVMSG #S3cr3tSp0t :ah 2pm
:D34thM3rch4nt!~blah2@7FF07A37.29E7D414.B9027CEB.IP PRIVMSG #S3cr3tSp0t
:Ok, I can't wa
it!

개발자에게 딱 맞춘 이력서 양식
개발자 이력서 어떻게 쓰는지 고민되었다면, 이력서 양식 및 샘플/가이드까지 무료로 확인하세요 점핏
열기

HTML을 디코드!

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!

ⓒSaebyeol Yu. Saebyeol's PowerPoint

DeFCoN #21 문제풀이

Round2

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

<u>그들은 어떤 도시에서 만납니까?</u>

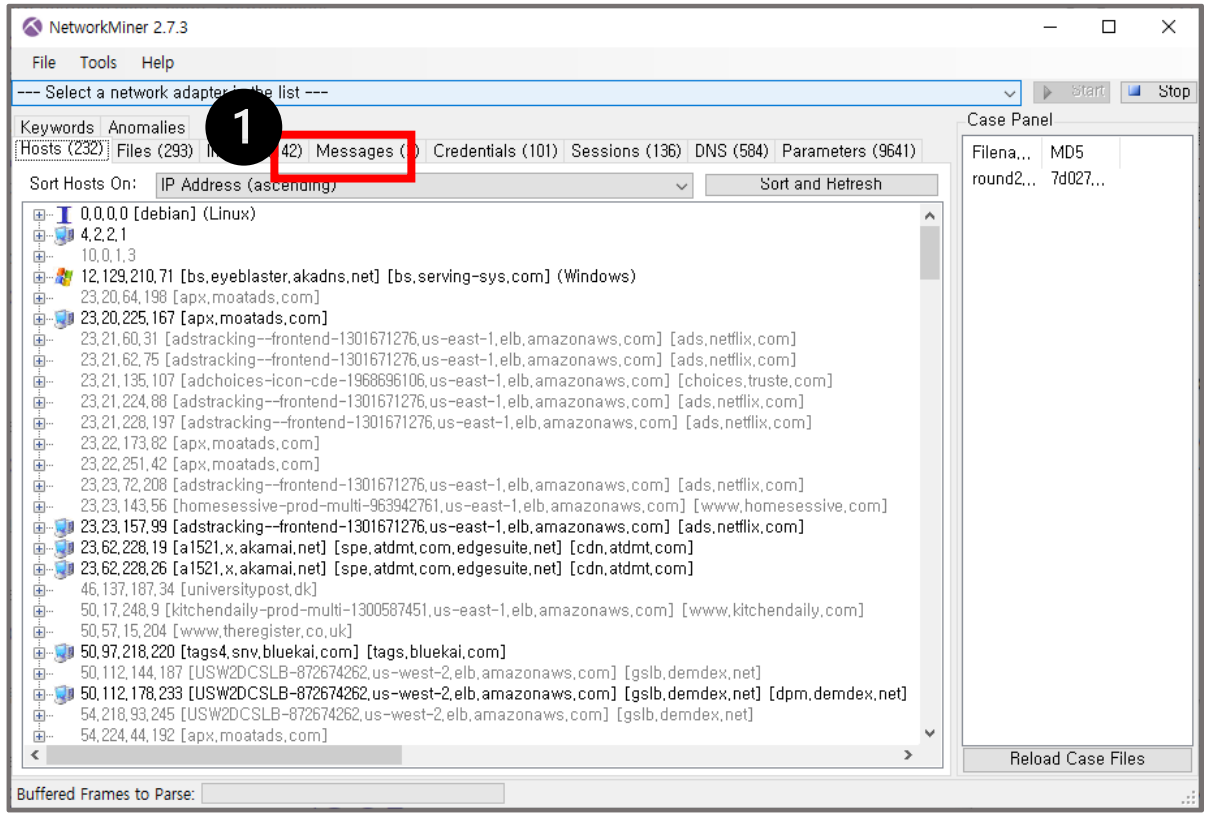
Jensen
(옌센씨)

Gregory
(그레고리씨)

ⓒSaebyeol Yu. Saebyeol's PowerPoint

DeFCoN#21 문제풀이

Round2

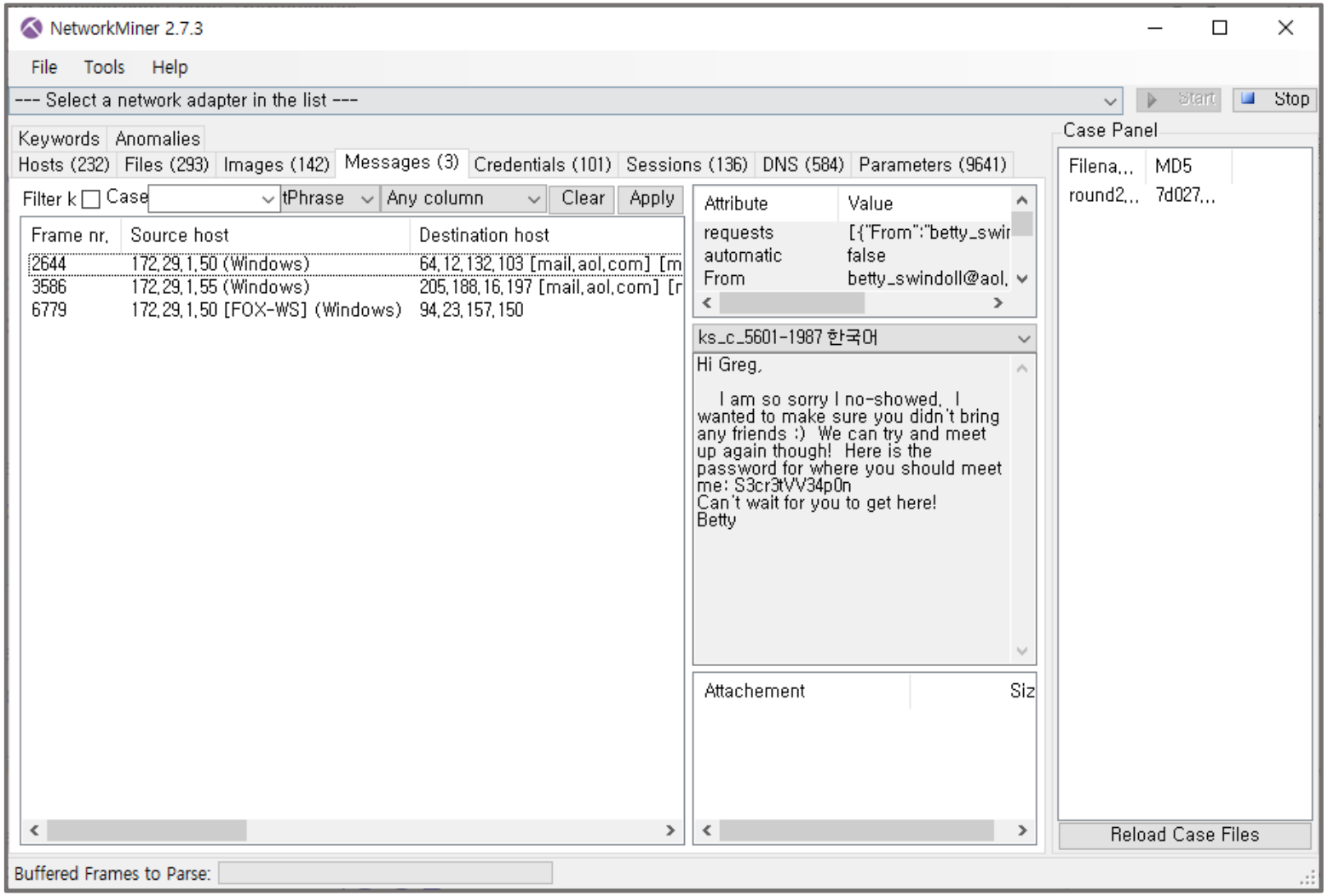


Messages : 패킷 패키지 안의 메시지를 복호화하여 보여줌

ⓒSaebyeol Yu. Saebyeol's PowerPoint

DeFCoN#21 문제풀이

Round2



ⓒSaebyeol Yu. Saebyeol's PowerPoint

DeFCoN#21 문제풀이

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

ⓒSaebyeol Yu. Saebyeol's PowerPoint

DeFCoN#21 문제풀이

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.

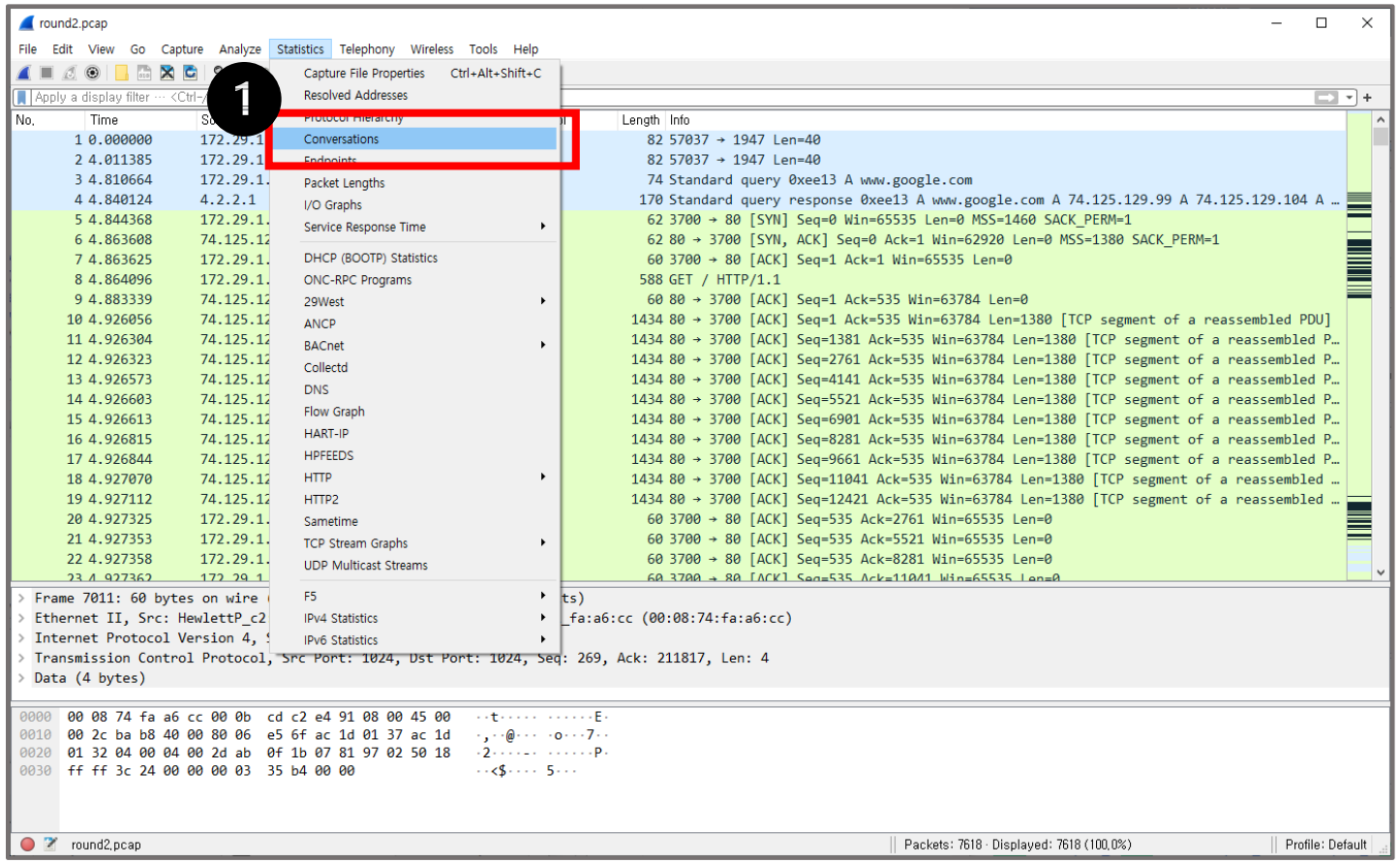
	To	Subject	Protocol	Timestamp	Size
l@aol.com	d34thm3rch4nt@aol.com,	Sorry	Http	2004-11-12 19:28:52 UTC	292
t@aol.com	betty_swindoll@aol.com,	Re: Sorry	Http	2004-11-12 19:30:07 UTC	541
	D34thM3rch4nt	┌DCC SEND r3nd3zv0us 2887582002 1024 819200┌	Irc	2004-11-12 19:31:54 UTC	68

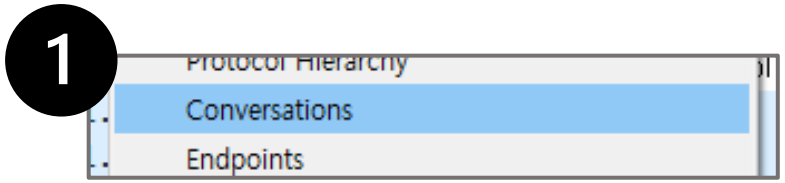
DCC SEND <filename> <ip> <port> <file size>

ⓒSaebyeol Yu. Saebyeol's PowerPoint

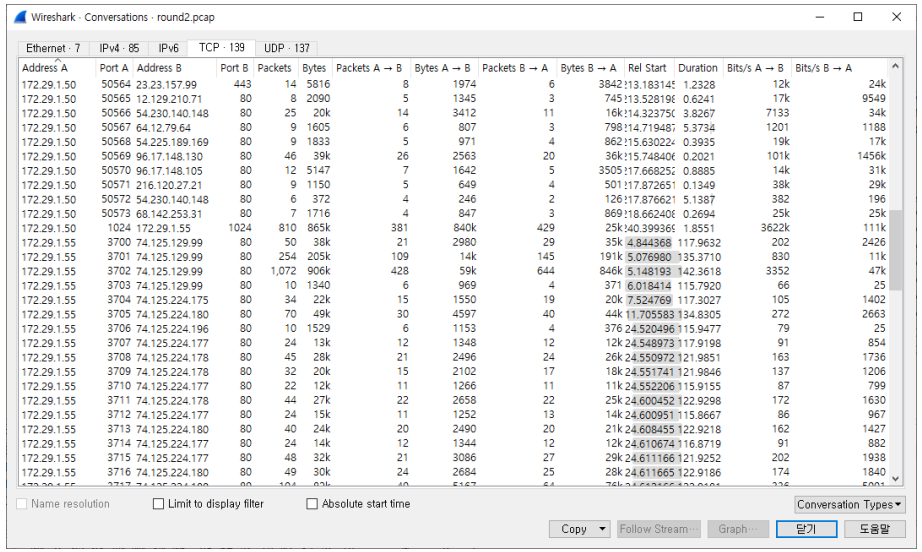
DeFCoN#21 문제풀이

Round2





호스트와 호스트 사이에 통신했던 연결을 보여줌.



ⓒSaebyeol Yu. Saebyeol's PowerPoint

DeFCoN#21 문제풀이

Round2

Wireshark · Conversations · round2.pcap

Ethernet · 7 | IPv4 · 85 | IPv6 | TCP · 139 | UDP · 137

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	13.183145	1.2328	12k	24k
172.29.1.50	50565	12.129.210.71	80	8	2090	5	1345	3	745	13.528198	0.6241	17k	9549
172.29.1.50	50566	54.230.140.148	80	25	20k	14	3412	11	16k	14.323750	3.8267	7133	34k
172.29.1.50	50567	64.12.79.64	80	9	1605	6	807	3	798	14.719487	5.3734	1201	1188
172.29.1.50	50568	54.225.189.169	80	9	1833	5	971	4	862	15.630224	0.3935	19k	17k
172.29.1.50	50569	96.17.148.130	80	46	39k	26	2563	20	36k	15.748406	0.2021	101k	1456k
172.29.1.50	50570	96.17.148.105	80	12	5147	7	1642	5	3505	17.668252	0.8885	14k	31k
172.29.1.50	50571	216.120.27.21	80	9	1150	5	649	4	501	17.872651	0.1349	38k	29k
172.29.1.50	50572	54.230.140.148	80	6	372	4	246	2	126	17.876621	5.1387	382	196
172.29.1.50	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	4	847	3	869	18.662408	0.2694	25k	25k
172.29.1.50	1024	172.29.1.55	1024	810	865k	381	840k	429	25k	40.399369	1.8551	3622k	111k
172.29.1.55	[illegible]	74.125.129.99	80	50	38k	21	2980	29	35k	4.844368	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
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Name resolution | Limit to display filter | Absolute start time | Conversation Types

Copy | Follow Stream··· | Graph··· | 닫기 | 도움말

1

1024 172.29.1.55 1024 810 865k

2

Wireshark · Follow TCP Stream (tcp.stream eq 138) · round2.pcap

```
.T........e.^...b..f......(.3..#}..s...CME..x.$....3.2...P..e.....+.. .#...r..
&..T@J9)....Vk4.s....wM.8.D..O(.m.$_..B..K....VB.ng.......t..=.3...ue+.
.....Co...R5..D.Hv....`.Q..v">.......,.U'..H....I......D.....Q......;jp4..pJ.B.I[.%0.#%
_~C..*.........~. ..*.p..-]..e4...[..6.L].7.t.....;...`>t(.Rak7Qp.:......U0TOM. ....q..cO..
%F....wT.N.n......o..qJi.I.....J.........2.n...0a........(..b}..?....1...}\..D.!q....ru%..N.n..P..
.2.$.Q...F..5.r..z..6..7.~.....f..R`3kU..u...Z.......a..o..$~..O.:.a/..D.+6.mXnT..g.M2E.-......
2.#;.n.&..Y.........vo+.....
...........).N....Ej.....m9__.a./V,.0M..j.k...o~...:w1Y.uwA>h.....Z..t..2.gw.....n...Z... ..1>..P..
{.G.........V....LB.Y.3.........vG..j.;...<..Y
.&.F#h$O1......U.f$&.N..%..1...,.[.RYG..fthD31......+../.........a....sT.;8._.......y..
ca...h...P.U.V......E....(..)....3v..._.T...eq..!....)...pu<-.^..>...CA.N.......z1.
+.....FV2*.*.....N.e!.f.M.gP,>
....V.*../.nM.+.m.9...M...._..8......}XP`]..O.=%$...:..e..1...6.h4..._A
9.1v....$..J...........U...F<).k...i.....&....v...y.........r...<.=X.k..{.\Q...
$dp.a+..U...^....?......Y......\b...+.....#.
.s...n`[..a..._..-.gF$.Y.!......8..Z....UZ...........,./D^n..T.T\....j.....=2..t.....b.R.4.qq.TO..
...=i.n.7.3/.H>.QU.E1...Z....N?F.IDu.......!Fx5|E-
N;..|.<...t..........cB...RH81...Q5`:....t..)N2.6X....J..f'L.|*.@.]....K...'...
2..;/.5..7.tIK...DW.....}..Z.....7*.|3..aA&:.....H..L..K&a..z.._.....S..Ye..+....W...S..wz....zf...B..
8..J.!.:!/4R..M..C[.j......Y.....P......0<.!.d.5....M.EF.  .K...!..^xp..r....|..1-..KL..Q.H..b......
7cG...@.8.. ...$.....h....U:.5>O.^.._.
R-.......8Z<r]V!..N~.).O..D\.a.....(PK#a..P.W.....:...(PB.2.8.....P.:....,.....xt1..ok.\...)B>..
+..~...=T.......e/n%v.a..5{.(T.^..
.LV....\.z.....]....o...F.......&... ]8U.......(..G.
..U.{....7<=.vW.....y.4...G..D.w
...#.]p.....S..bU..8(<.u."..Gl....9...&.xRX.K].......S.uAS.....).%
$y....#.....sAy....^)G..g..V.....~.K.....25&..t].}.D._096.....S..o.]J...J0...A.Ci.
$y.E04c~.X........}.n5X...//s wkG.........G&.....F-........;7.v>.._..vX.9.f.M..yB....]....@..B...._.{.
.J@h..R...<.y.....~.Kh;...-.w.e..._m.xt|....C]E@2......5..R.U.....zf....^|.... .(...'.].}...
9.Fo...i.~....E......
....
F.t"....g..D?VHt..O.%.$&%K.C
.VhO..5.j..F..L.@H#.t..j.....F.[ku...z.].CzX.Ukd..j.k+.pW....8uJ.....VB....V...i...F.:h....-.wmy4B..
3..n.......@X.R).OB....?1;..;.<P..uwX.sY....Qu...1h.eO.!.h..t....,..\`.mEk"?.&...".
%.h....^A~?..)`...O.....=....K2......../..&D...0..?.~.k(F.\?P.0...
.. n1.8v1..wB.%.....eR..Y..Ozw../\..<.L..."......B.....sw.g#...Y3.5...>.........n.-..
(...G..r.......<...)...X.(..f8......+k].......N....._Z.....V....}.U...k...:AEh....).2.0.|...y..
%E..C.'.z.j.Fg.1........      .f.J...1.^.3.<...t..>.N...&.=...o`...0..1.l...,V....T....5.r..W..j
```

198 client pkt(s), 342 server pkt(s), 265 turn(s).

Entire conversation (820kB) | Show data as ASCII | Stream 138

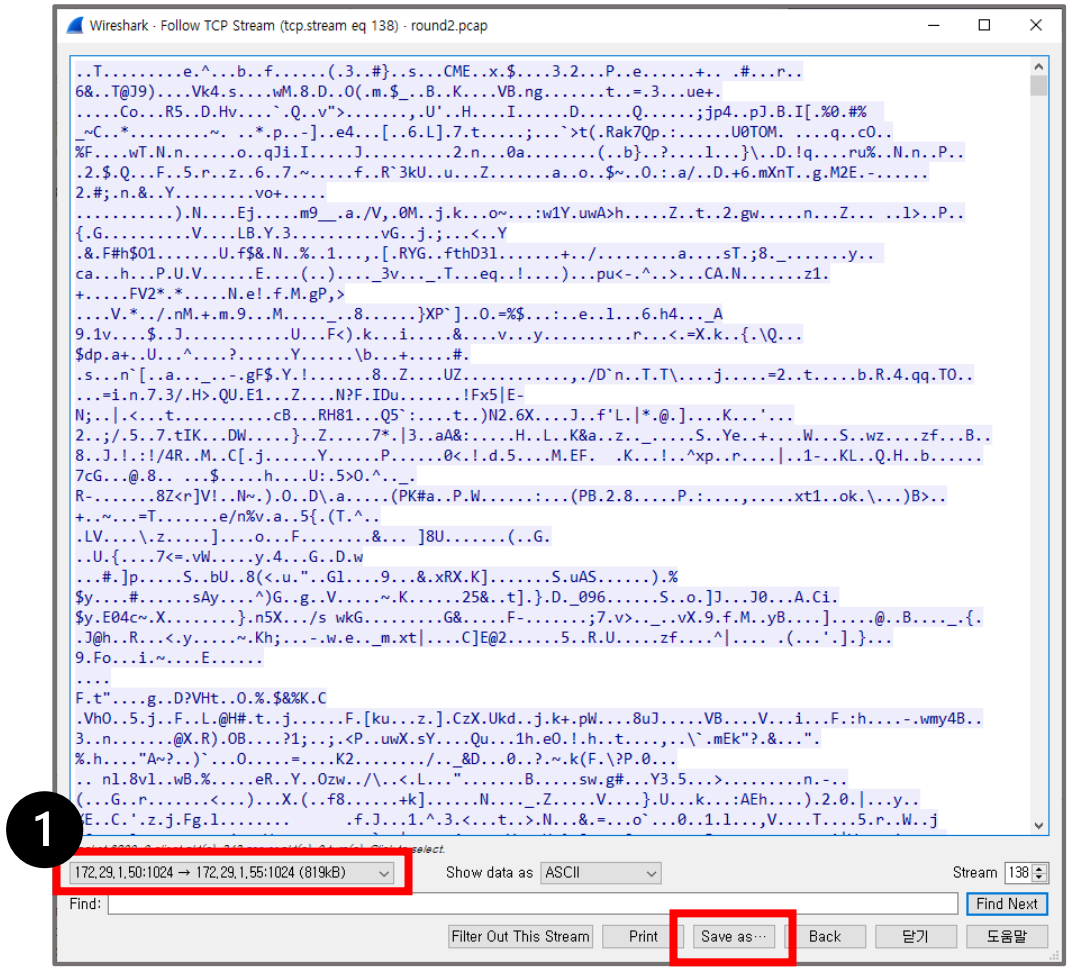
Find: | Find Next

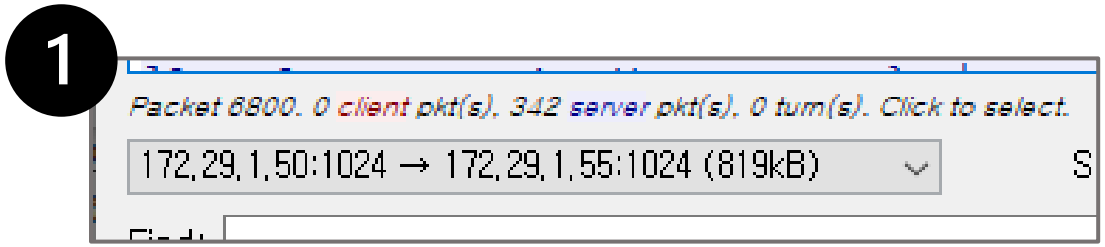
Filter Out This Stream | Print | Save as··· | Back | 닫기 | 도움말

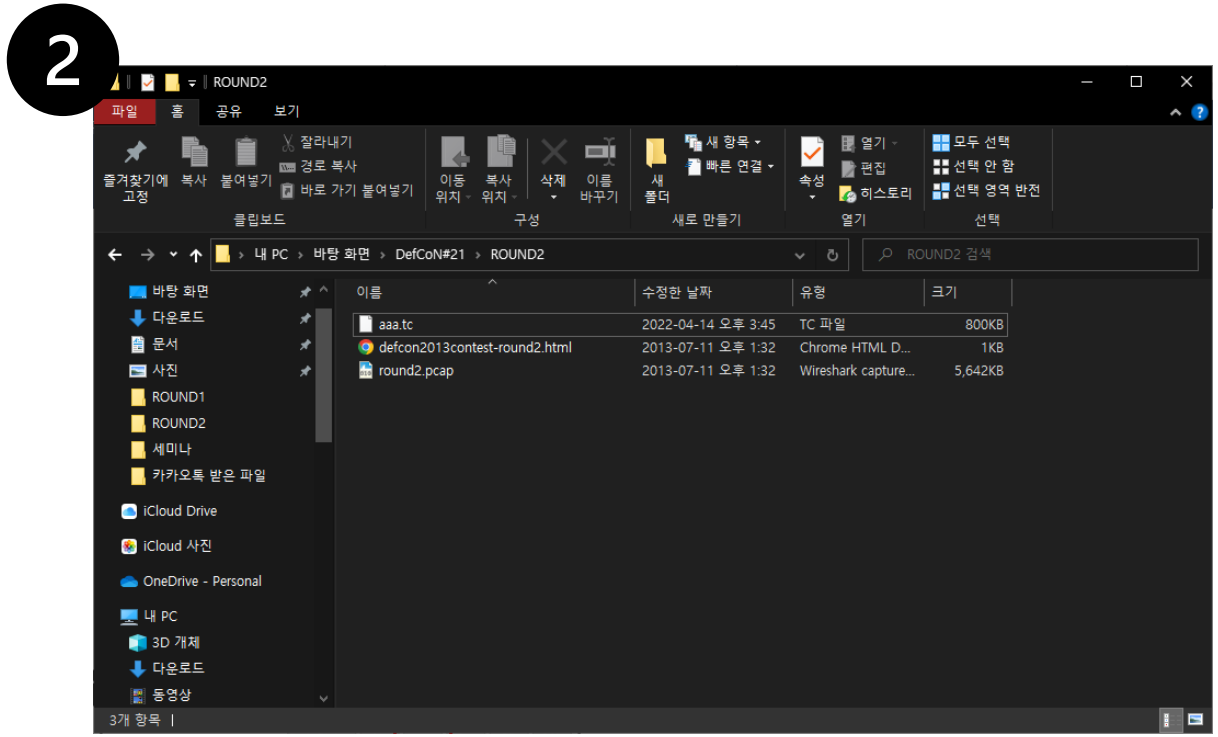
ⓒSaebyeol Yu. Saebyeol's PowerPoint

DeFCoN#21 문제풀이

Round2







ⓒSaebyeol Yu. Saebyeol's PowerPoint

DeFCoN#21 문제풀이

Round2

파일 확장자 홈 / 모든 확장자 / 파일 확장자 TC

Silver Microsoft Partner

TC 파일 유형

저자 Jay Geater | 편집: November 26, 2018

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.

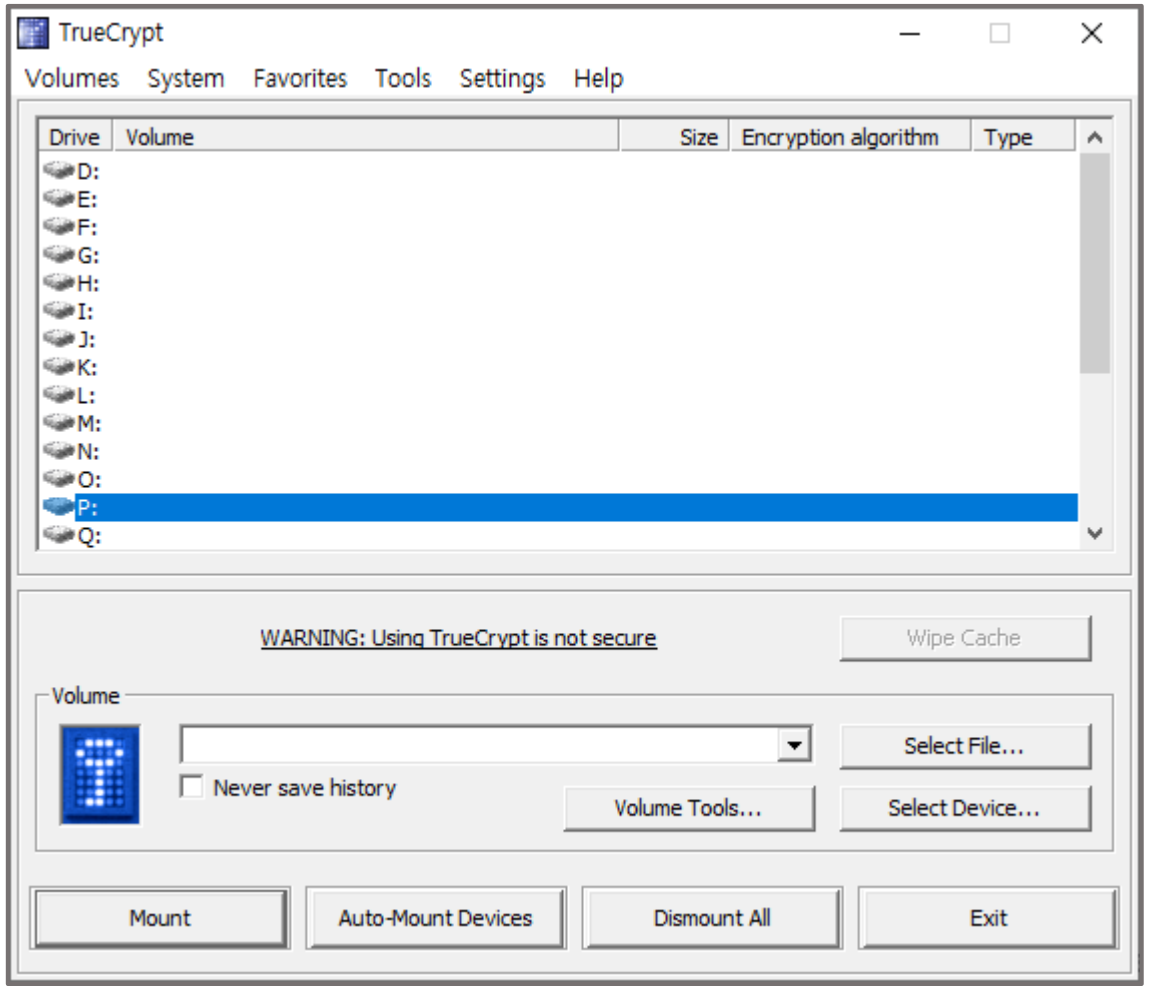
Windows, Linux 운영 체제를 사용하여 TC 파일을 볼 수 있습니다. 이들은 데스크톱 (및 일부 모바일) 장치에서 흔히 볼 수 있으며 이러한 파일을 보거나 때때로 편집할 수 있게 해줍니다. 주요 파일 형식 TC의 인기도는 "낮음"이고 이들 파일은 종종 일반 데스크톱이나 모바일 장치에서 찾을 수 없습니다.

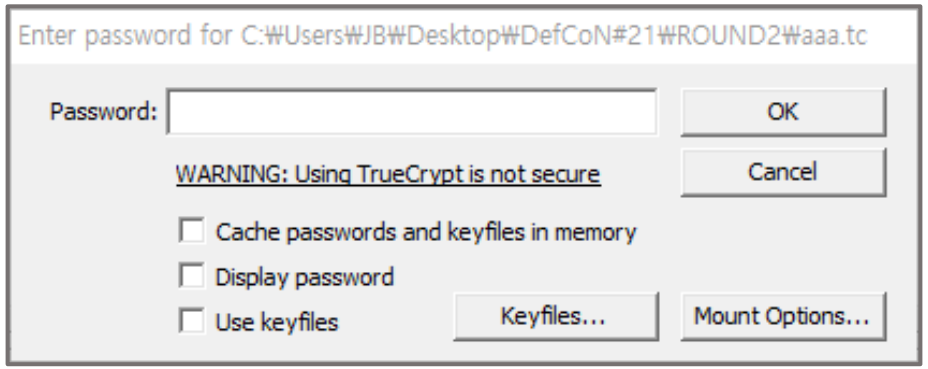
TC파일 및 파일을 여는 소프트웨어에 대한 자세한 내용은 아래의 추가 세부 정보를 참조하십시오. 또한 이러한 파일을 여는 데 문제가 있는 경우 기본 TC 파일 문제 해결 방법을 배울 수 있습니다.

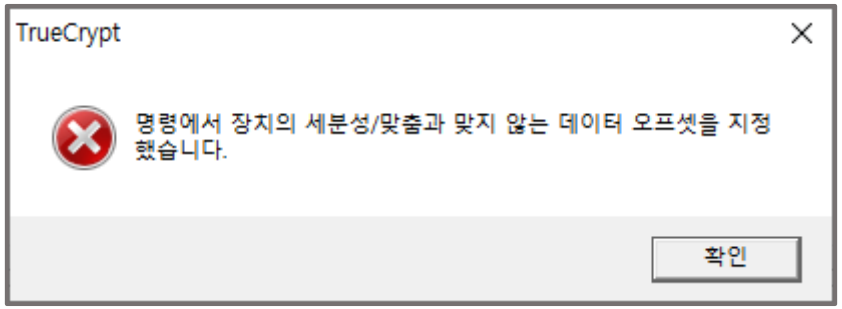
ⓒSaebyeol Yu. Saebyeol's PowerPoint

DeFCoN#21 문제풀이

Round2



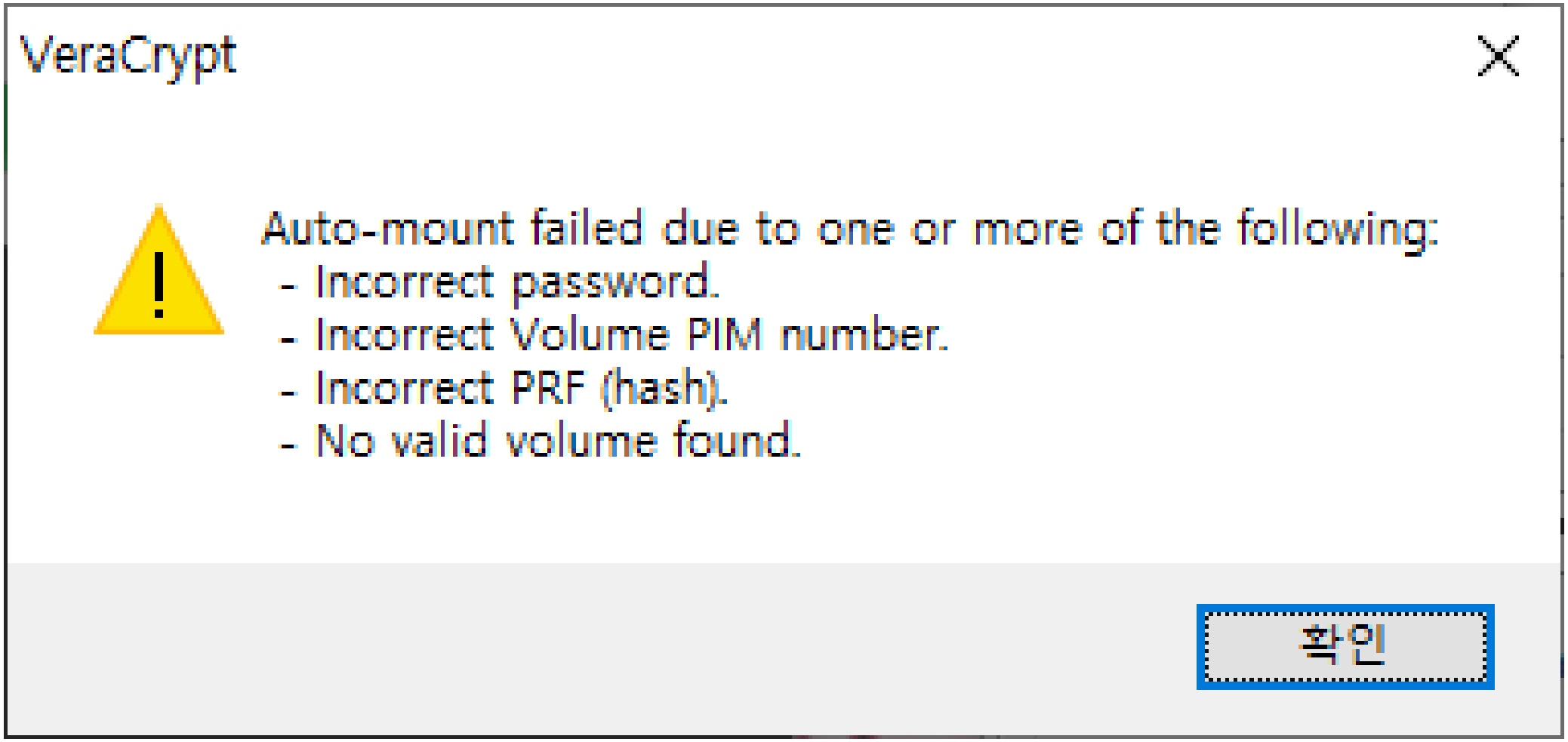




ⓒSaebyeol Yu. Saebyeol's PowerPoint

DeFCoN#21 문제풀이

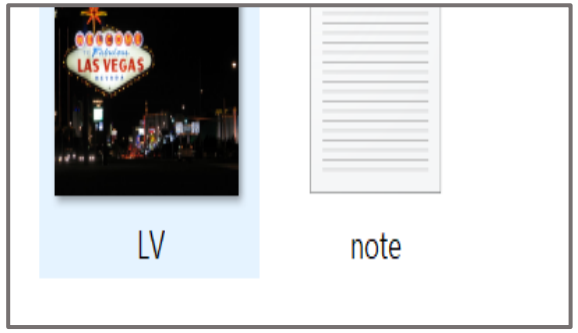
Round2

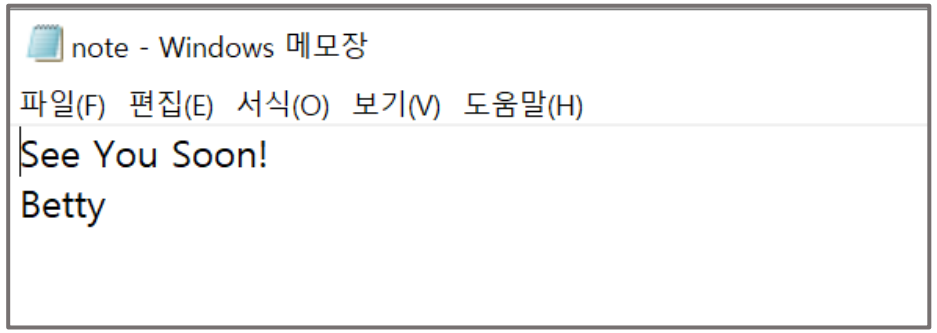


ⓒSaebyeol Yu. Saebyeol's PowerPoint

DeFCoN#21 문제풀이

Round2





ⓒSaebyeol Yu. Saebyeol's PowerPoint