JBU-CTF 2020

Forensic(Network) 2문제

조재현

INDEX

1 Find_him

1. 문제 설명
2. 풀이법

2 Find_msg

1. 문제 설명
2. 풀이법

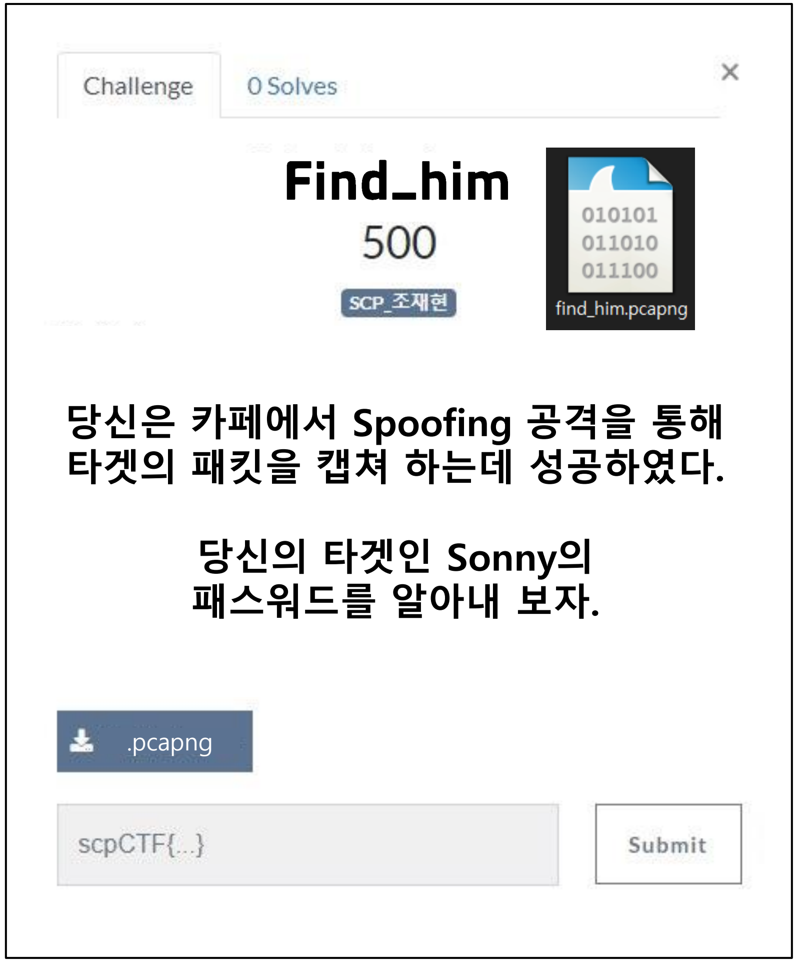
1

Find_him

1. 문제 설명
2. 풀이법

Forensic - Find_him

- 분야 : Forensic
- 세부 분야 : Network
- 난이도 : 중
- 출제 의도 :
HTTP 평문 전송 위험성을 알리고자 출제

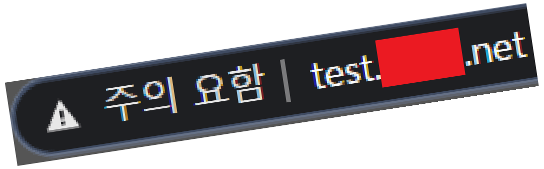


Find_him
500
SCP_조재현

당신은 카페에서 Spoofing 공격을 통해 타겟의 패킷을 캡쳐 하는데 성공하였다.

당신의 타겟인 Sonny의 패스워드를 알아내 보자.

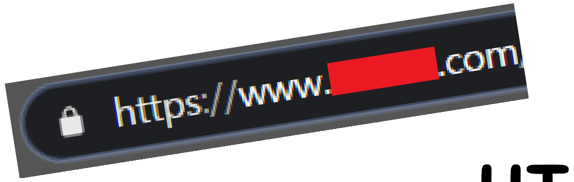
HTTP? HTTPS?



⚠ 주의 요함 | test.[redacted].net

HTTP ?

Client와 Server간의 웹페이지와 같은 자원을 주고받을 때 쓰는 통신 규약

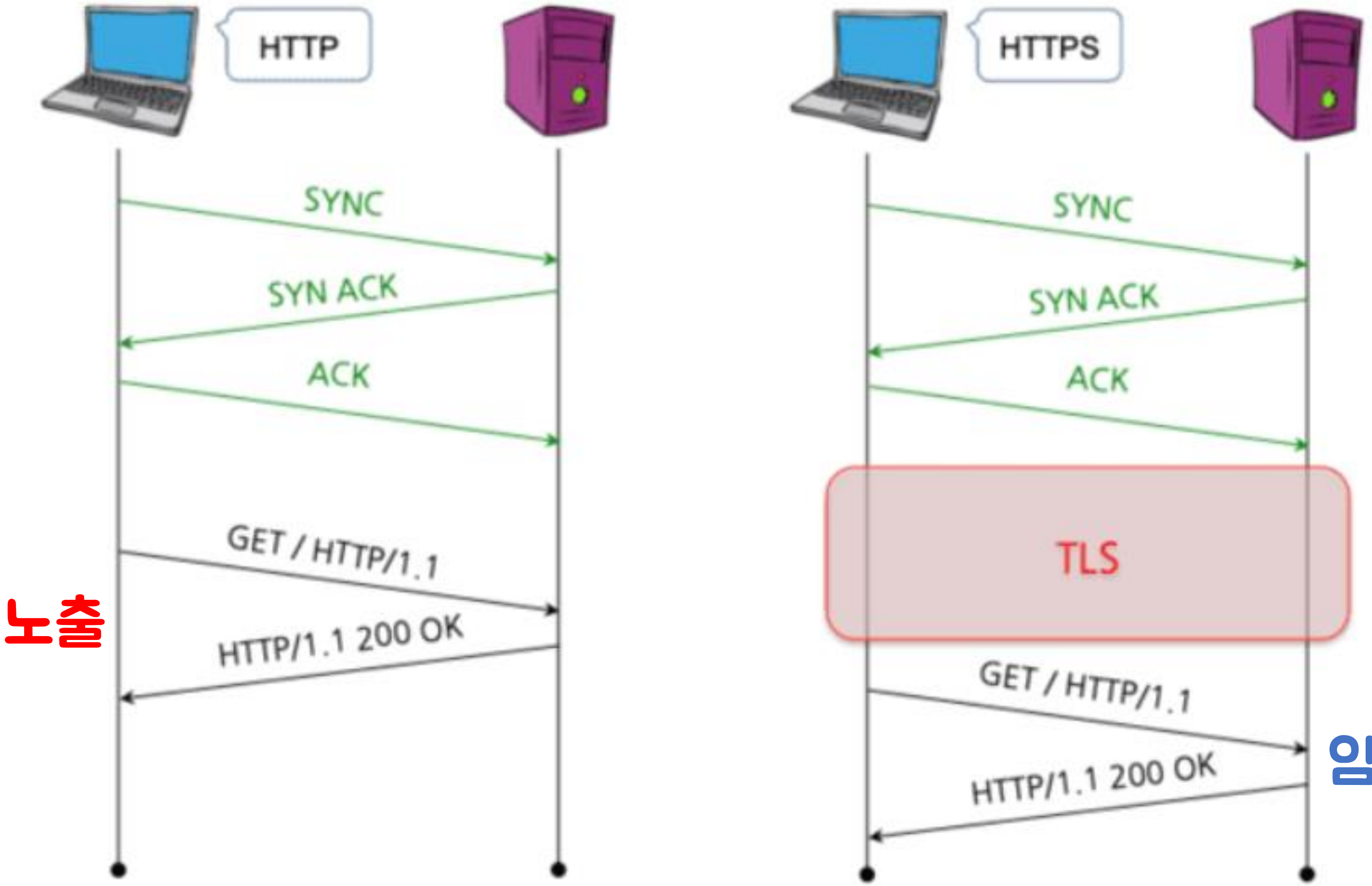


🔒 https://www.[redacted].com

HTTPS ?

HTTP + S(Secure Socket)
인터넷 상에서 정보를 암호화 하는 SSL 프로토콜 이용
(공개키 암호화 방식)

HTTP? HTTPS?



평문 노출

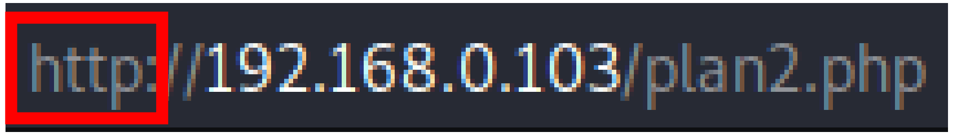
TLS Handshaking!

암호화

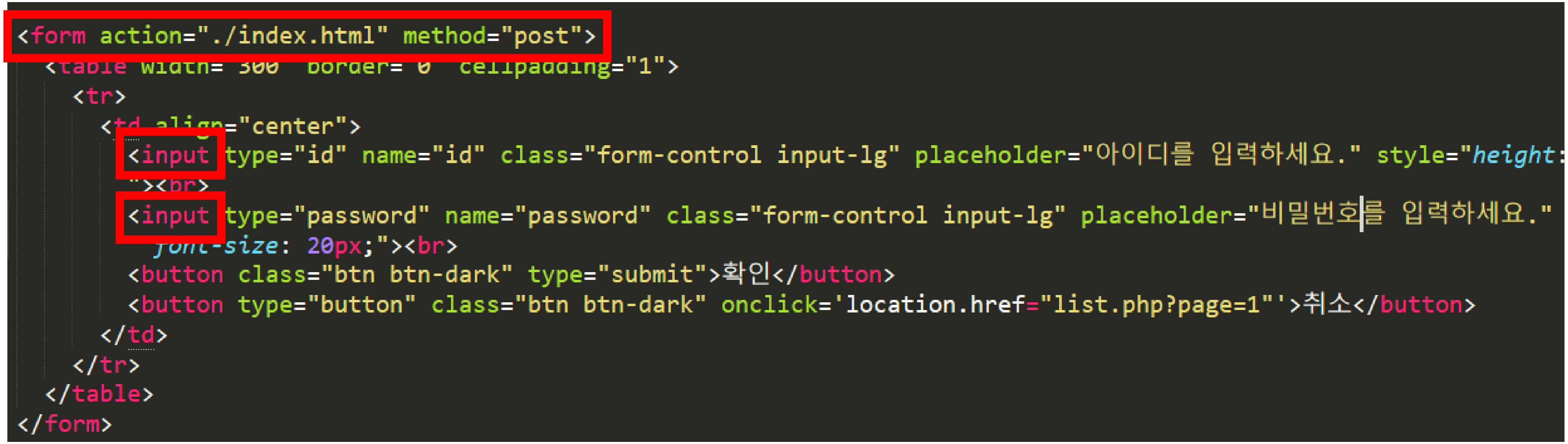
출저 : https://www.mimul.com/blog/about-https/

1 Find_him

2. 풀이법



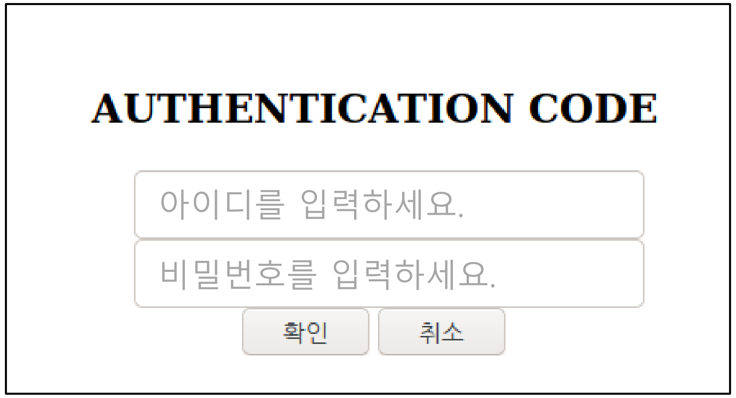
```
http://192.168.0.103/plan2.php
```



```
<form action="./index.html" method="post">
  <table width="300" border="0" cellpadding="1">
    <tr>
      <td align="center">
        <input type="id" name="id" class="form-control input-lg" placeholder="아이디를 입력하세요." style="height:
        "><br>
        <input type="password" name="password" class="form-control input-lg" placeholder="비밀번호를 입력하세요."
        font-size: 20px;"><br>
        <button class="btn btn-dark" type="submit">확인</button>
        <button type="button" class="btn btn-dark" onclick='location.href="list.php?page=1"'>취소</button>
      </td>
    </tr>
  </table>
</form>
```

1 Find_him

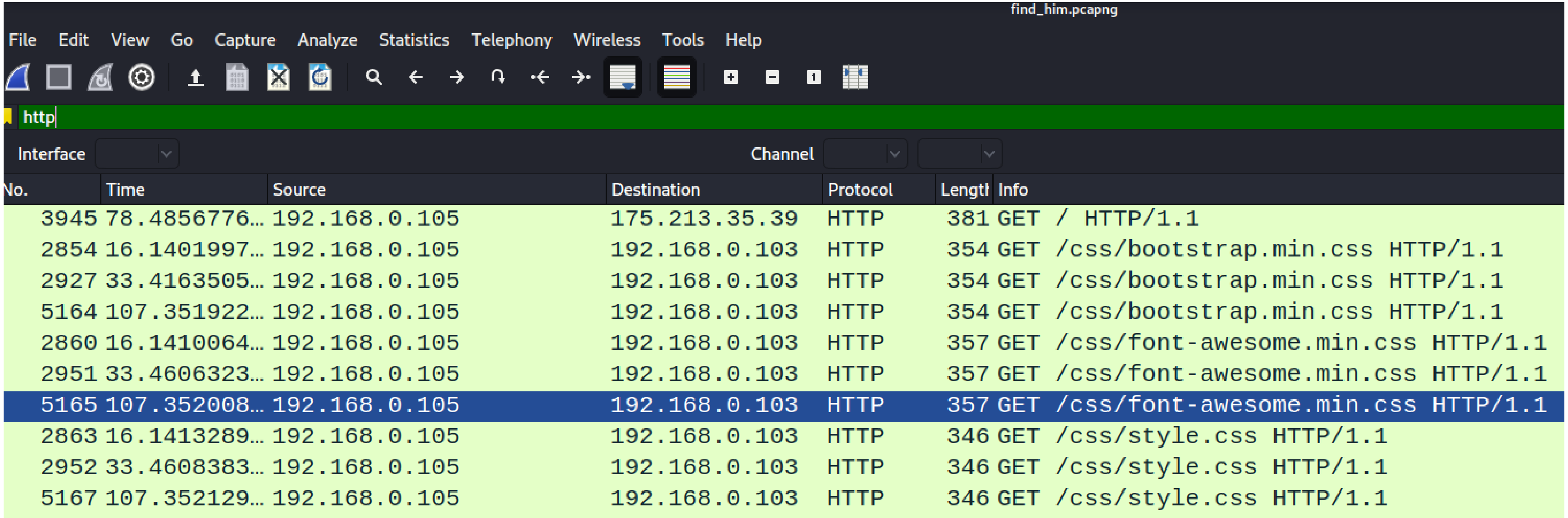
2. 풀이법



AUTHENTICATION CODE

아이디를 입력하세요.

비밀번호를 입력하세요.



find_him.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Interface
Channel

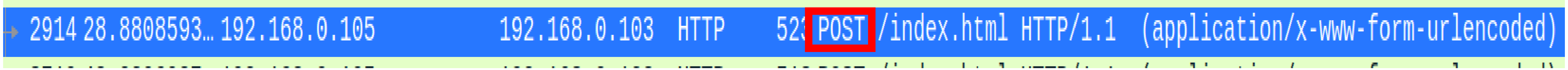
http

No.	Time	Source	Destination	Protocol	Lengtl	Info
3945	78.4856776...	192.168.0.105	175.213.35.39	HTTP	381	GET / HTTP/1.1
2854	16.1401997...	192.168.0.105	192.168.0.103	HTTP	354	GET /css/bootstrap.min.css HTTP/1.1
2927	33.4163505...	192.168.0.105	192.168.0.103	HTTP	354	GET /css/bootstrap.min.css HTTP/1.1
5164	107.351922...	192.168.0.105	192.168.0.103	HTTP	354	GET /css/bootstrap.min.css HTTP/1.1
2860	16.1410064...	192.168.0.105	192.168.0.103	HTTP	357	GET /css/font-awesome.min.css HTTP/1.1
2951	33.4606323...	192.168.0.105	192.168.0.103	HTTP	357	GET /css/font-awesome.min.css HTTP/1.1
5165	107.352008...	192.168.0.105	192.168.0.103	HTTP	357	GET /css/font-awesome.min.css HTTP/1.1
2863	16.1413289...	192.168.0.105	192.168.0.103	HTTP	346	GET /css/style.css HTTP/1.1
2952	33.4608383...	192.168.0.105	192.168.0.103	HTTP	346	GET /css/style.css HTTP/1.1
5167	107.352129...	192.168.0.105	192.168.0.103	HTTP	346	GET /css/style.css HTTP/1.1

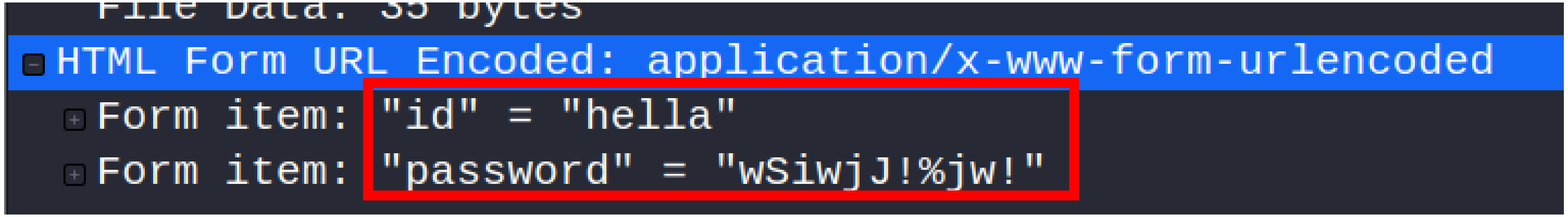
1

Find_him

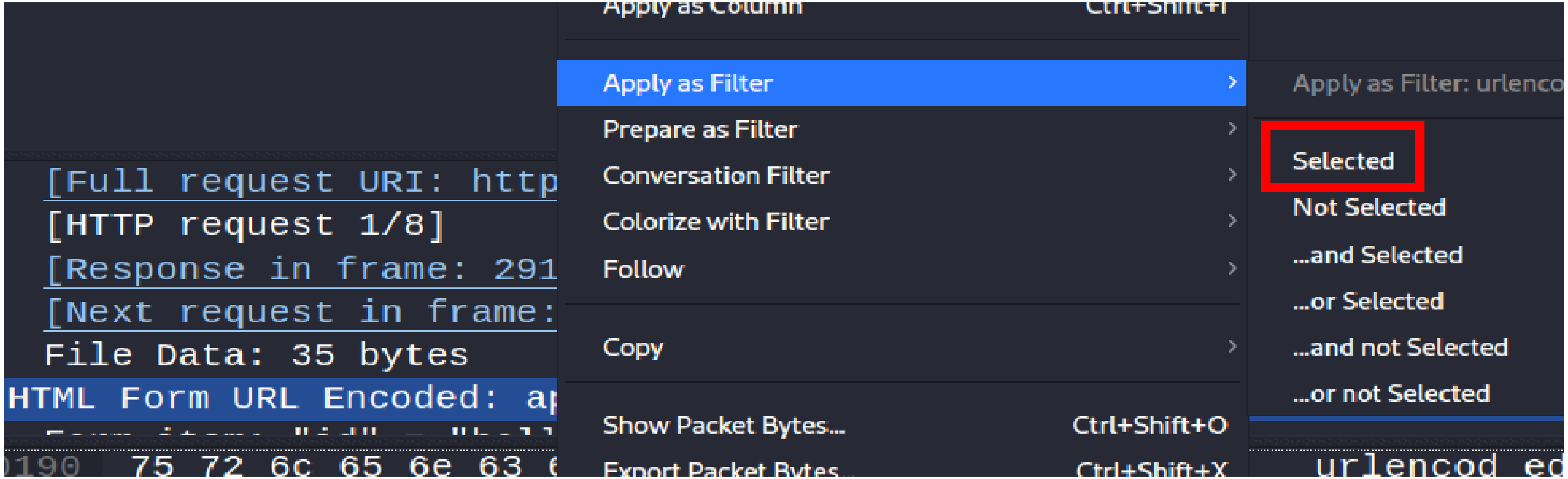
2. 풀이법



```
2914 28.8808593… 192.168.0.105          192.168.0.103   HTTP      523 POST /index.html HTTP/1.1  (application/x-www-form-urlencoded)
```



```
  File Data: 35 bytes
⊟ HTML Form URL Encoded: application/x-www-form-urlencoded
   ⊞ Form item: "id" = "hella"
   ⊞ Form item: "password" = "wSiwjJ!%jw!"
```

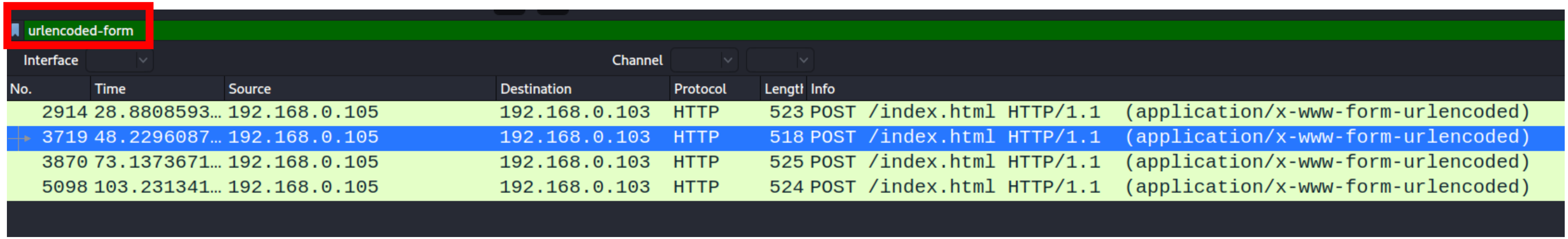


```
[Full request URI: http
[HTTP request 1/8]
[Response in frame: 291
[Next request in frame:
File Data: 35 bytes
HTML Form URL Encoded: ap
0190  75 72 6c 65 6e 63 6
```

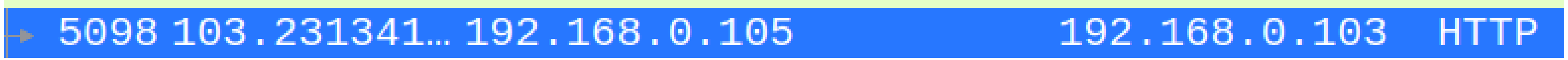
1

Find_him

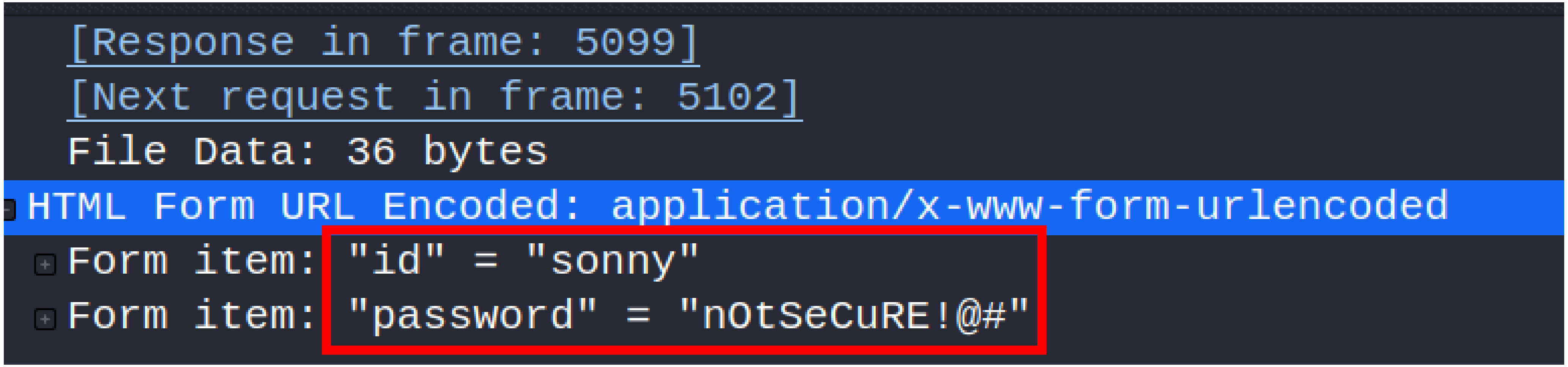
2. 풀이법



```
No.   Time          Source          Destination     Protocol  Length Info
 2914 28.8808593…   192.168.0.105   192.168.0.103   HTTP      523 POST /index.html HTTP/1.1  (application/x-www-form-urlencoded)
 3719 48.2296087…   192.168.0.105   192.168.0.103   HTTP      518 POST /index.html HTTP/1.1  (application/x-www-form-urlencoded)
 3870 73.1373671…   192.168.0.105   192.168.0.103   HTTP      525 POST /index.html HTTP/1.1  (application/x-www-form-urlencoded)
 5098 103.231341…   192.168.0.105   192.168.0.103   HTTP      524 POST /index.html HTTP/1.1  (application/x-www-form-urlencoded)
```



```
5098 103.231341… 192.168.0.105          192.168.0.103   HTTP
```



```
  [Response in frame: 5099]
  [Next request in frame: 5102]
  File Data: 36 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "id" = "sonny"
  Form item: "password" = "nOtSeCuRE!@#"
```

2

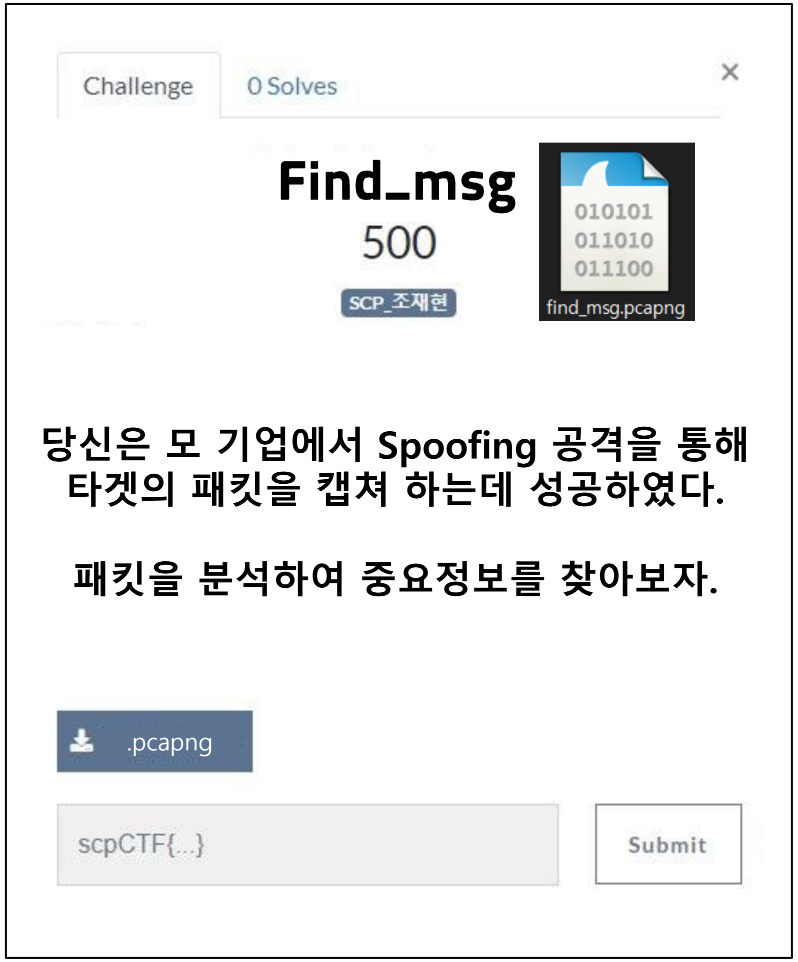
Find_msg

1. 문제 설명
2. 풀이법

Forensic - Find_msg

- 분야 : Forensic
- 세부 분야 : Network
- 난이도 : 중
- 출제 의도 :

FTP의 보안 위험성을 알려주기 위해 출제



당신은 모 기업에서 Spoofing 공격을 통해
타겟의 패킷을 캡쳐 하는데 성공하였다.

패킷을 분석하여 중요정보를 찾아보자.

FTP? SFTP?

FTP ?

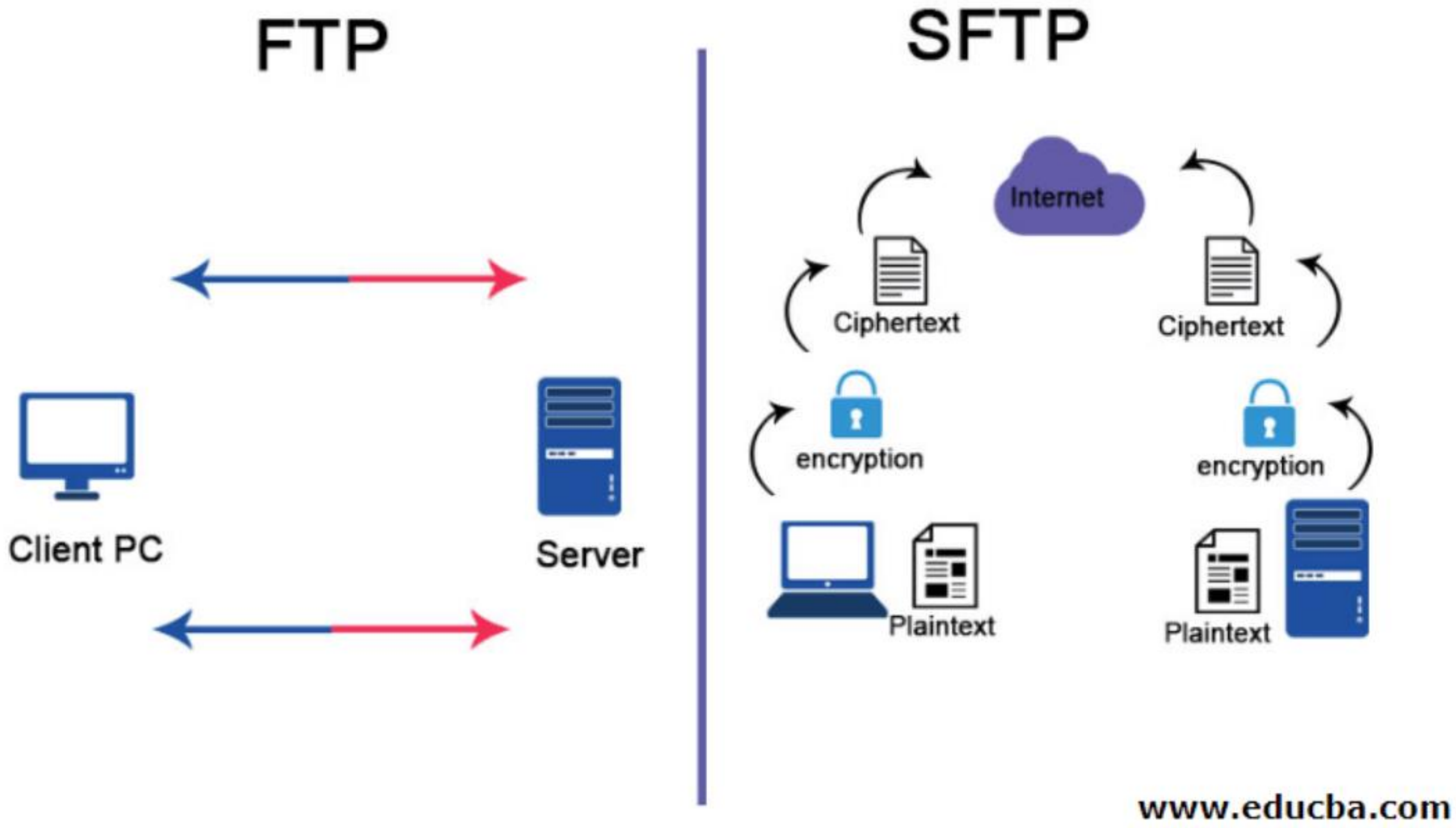
원격에 있는 서버에 파일을 주고 받을 때
사용하는 인터넷 통신 규약

SFTP ? (+FTPS/SecureFTP)

S(Secure) + FTP
인터넷 상에서 정보를 암호화 하는 SSL 프로토콜 이용
(공개키 암호화 방식)

1. 문제 설명

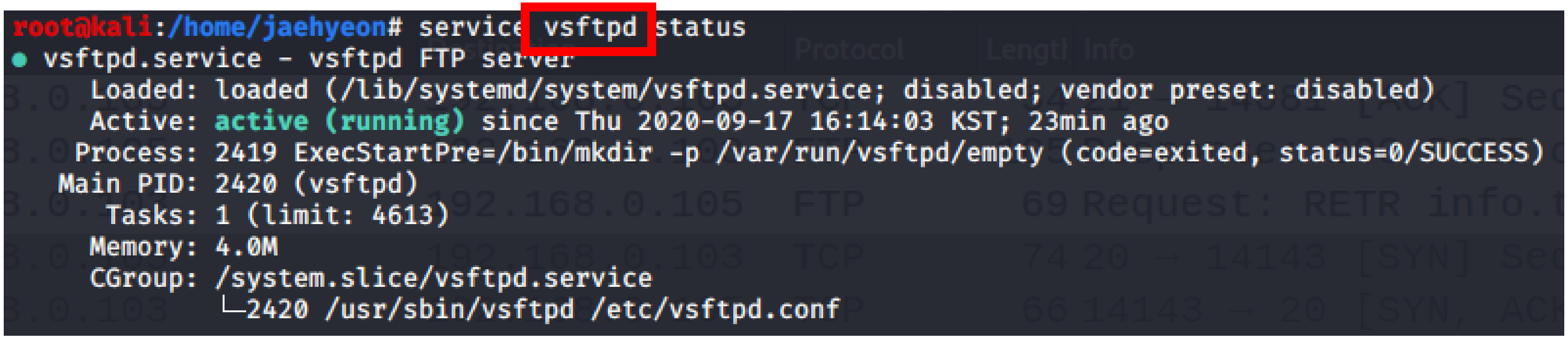
FTP? SFTP?



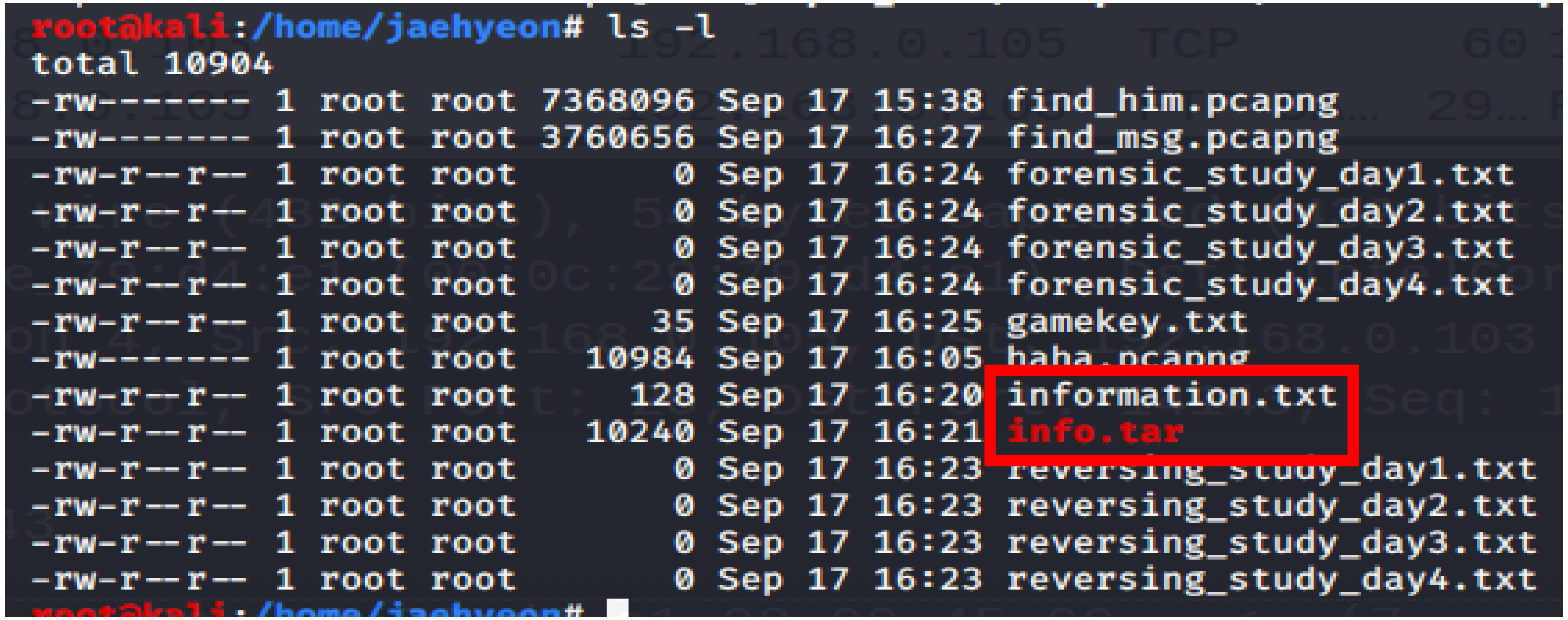
출처 : https://www.educba.com/ftp-vs-sftp/

2 Find_him

2. 풀이법



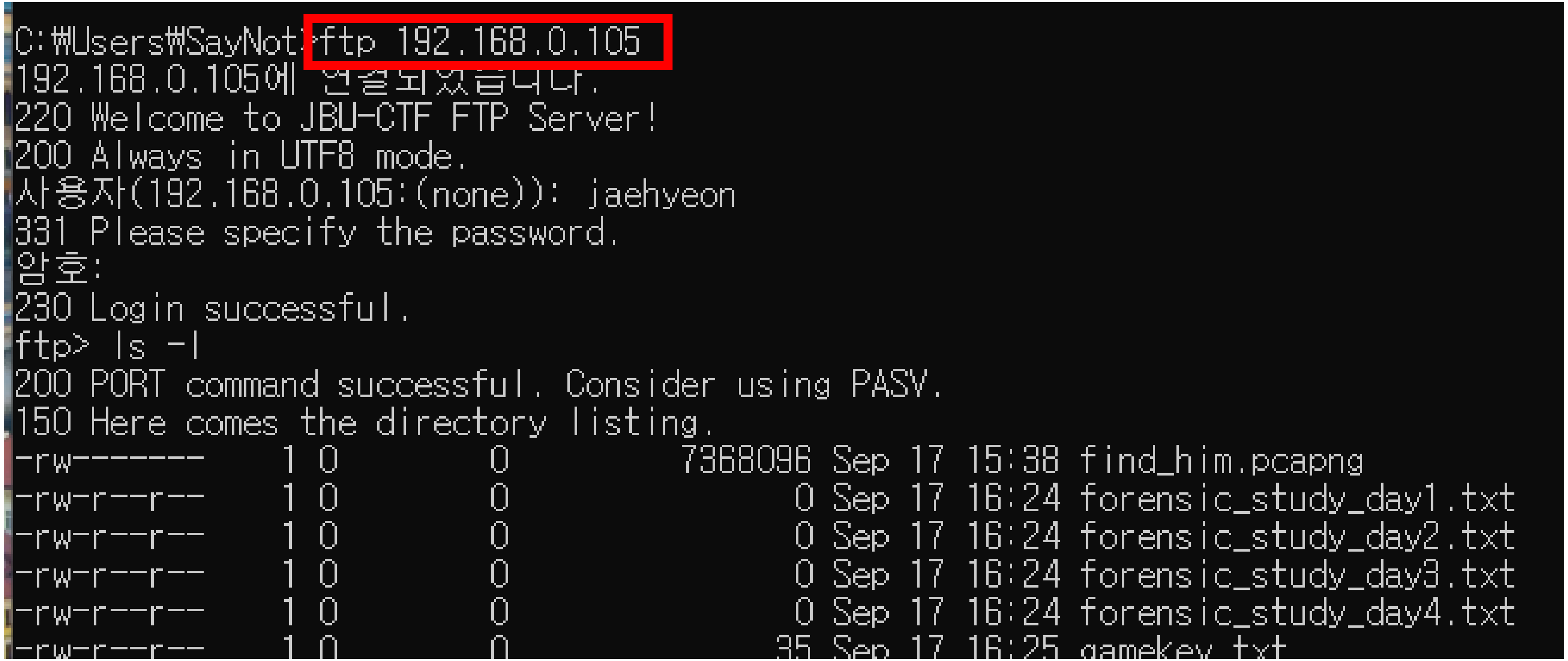
```
root@kali:/home/jaehyeon# service vsftpd status
● vsftpd.service - vsftpd FTP server
     Loaded: loaded (/lib/systemd/system/vsftpd.service; disabled; vendor preset: disabled)
     Active: active (running) since Thu 2020-09-17 16:14:03 KST; 23min ago
    Process: 2419 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)
   Main PID: 2420 (vsftpd)
      Tasks: 1 (limit: 4613)
     Memory: 4.0M
     CGroup: /system.slice/vsftpd.service
             └─2420 /usr/sbin/vsftpd /etc/vsftpd.conf
```



```
root@kali:/home/jaehyeon# ls -l
total 10904
-rw------- 1 root root 7368096 Sep 17 15:38 find_him.pcapng
-rw------- 1 root root 3760656 Sep 17 16:27 find_msg.pcapng
-rw-r--r-- 1 root root       0 Sep 17 16:24 forensic_study_day1.txt
-rw-r--r-- 1 root root       0 Sep 17 16:24 forensic_study_day2.txt
-rw-r--r-- 1 root root       0 Sep 17 16:24 forensic_study_day3.txt
-rw-r--r-- 1 root root       0 Sep 17 16:24 forensic_study_day4.txt
-rw-r--r-- 1 root root      35 Sep 17 16:25 gamekey.txt
-rw------- 1 root root   10984 Sep 17 16:05 haha.pcapng
-rw-r--r-- 1 root root     128 Sep 17 16:20 information.txt
-rw-r--r-- 1 root root   10240 Sep 17 16:21 info.tar
-rw-r--r-- 1 root root       0 Sep 17 16:23 reversing_study_day1.txt
-rw-r--r-- 1 root root       0 Sep 17 16:23 reversing_study_day2.txt
-rw-r--r-- 1 root root       0 Sep 17 16:23 reversing_study_day3.txt
-rw-r--r-- 1 root root       0 Sep 17 16:23 reversing_study_day4.txt
root@kali:/home/jaehyeon#
```

2 Find_him

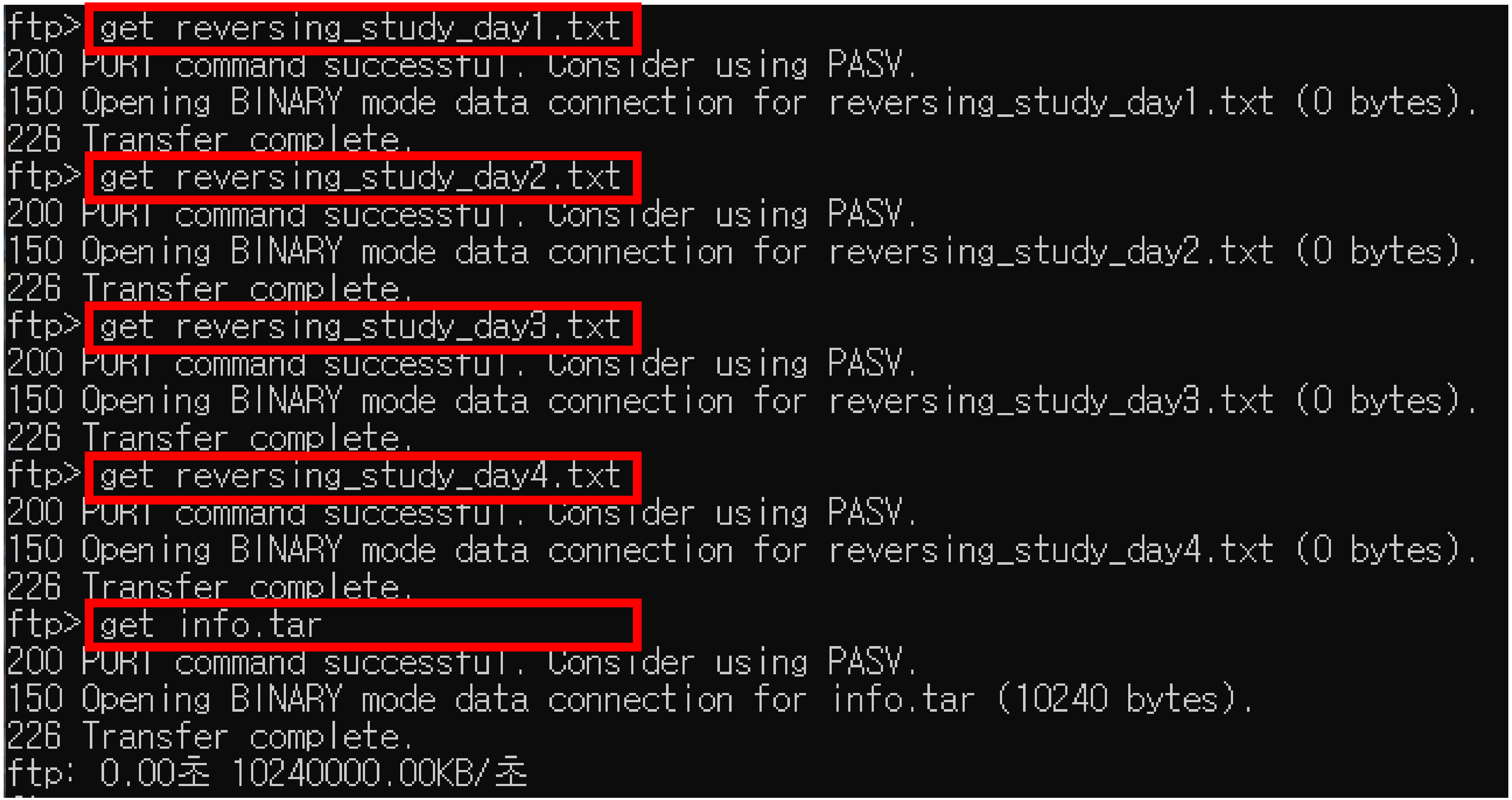
2. 풀이법



```
C:₩Users₩SayNot>ftp 192.168.0.105
192.168.0.105에 연결되었습니다.
220 Welcome to JBU-CTF FTP Server!
200 Always in UTF8 mode.
사용자(192.168.0.105:(none)): jaehyeon
331 Please specify the password.
암호:
230 Login successful.
ftp> ls -l
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-------    1 0        0         7368096 Sep 17 15:38 find_him.pcapng
-rw-r--r--    1 0        0               0 Sep 17 16:24 forensic_study_day1.txt
-rw-r--r--    1 0        0               0 Sep 17 16:24 forensic_study_day2.txt
-rw-r--r--    1 0        0               0 Sep 17 16:24 forensic_study_day3.txt
-rw-r--r--    1 0        0               0 Sep 17 16:24 forensic_study_day4.txt
-rw-r--r--    1 0        0              35 Sep 17 16:25 gamekey.txt
```

2 Find_him

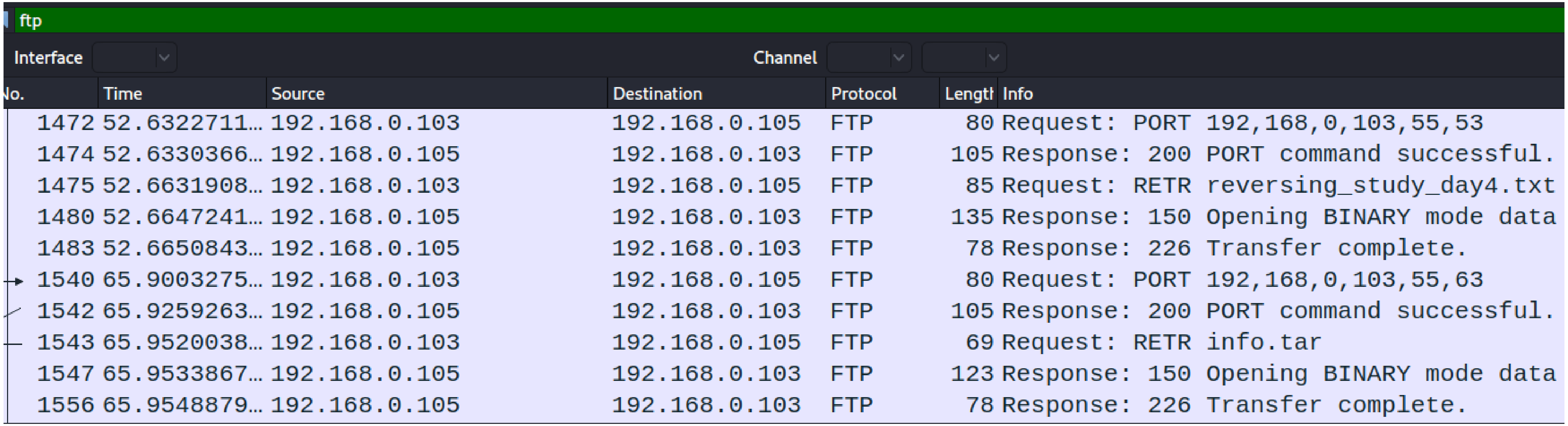
2. 풀이법



```
ftp> get reversing_study_day1.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for reversing_study_day1.txt (0 bytes).
226 Transfer complete.
ftp> get reversing_study_day2.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for reversing_study_day2.txt (0 bytes).
226 Transfer complete.
ftp> get reversing_study_day3.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for reversing_study_day3.txt (0 bytes).
226 Transfer complete.
ftp> get reversing_study_day4.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for reversing_study_day4.txt (0 bytes).
226 Transfer complete.
ftp> get info.tar
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for info.tar (10240 bytes).
226 Transfer complete.
ftp: 0.00초 10240000.00KB/초
```

2 Find_him

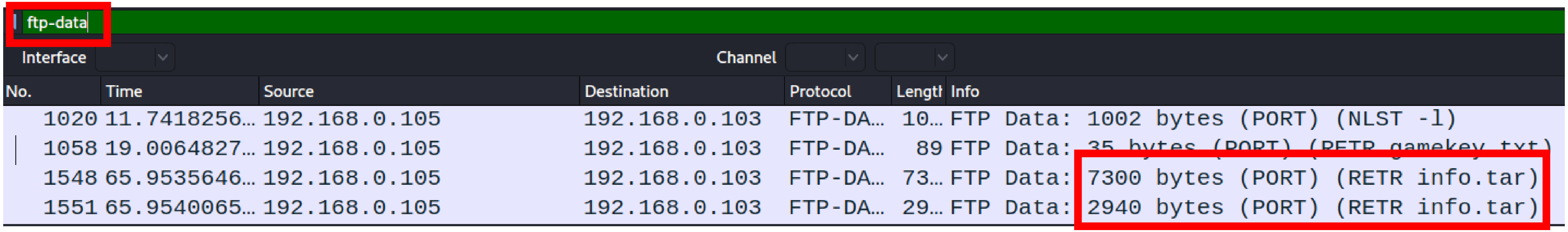
2. 풀이법



ftp

Interface Channel

No.	Time	Source	Destination	Protocol	Lengtl	Info
1472	52.6322711…	192.168.0.103	192.168.0.105	FTP	80	Request: PORT 192,168,0,103,55,53
1474	52.6330366…	192.168.0.105	192.168.0.103	FTP	105	Response: 200 PORT command successful.
1475	52.6631908…	192.168.0.103	192.168.0.105	FTP	85	Request: RETR reversing_study_day4.txt
1480	52.6647241…	192.168.0.105	192.168.0.103	FTP	135	Response: 150 Opening BINARY mode data
1483	52.6650843…	192.168.0.105	192.168.0.103	FTP	78	Response: 226 Transfer complete.
1540	65.9003275…	192.168.0.103	192.168.0.105	FTP	80	Request: PORT 192,168,0,103,55,63
1542	65.9259263…	192.168.0.105	192.168.0.103	FTP	105	Response: 200 PORT command successful.
1543	65.9520038…	192.168.0.103	192.168.0.105	FTP	69	Request: RETR info.tar
1547	65.9533867…	192.168.0.105	192.168.0.103	FTP	123	Response: 150 Opening BINARY mode data
1556	65.9548879…	192.168.0.105	192.168.0.103	FTP	78	Response: 226 Transfer complete.



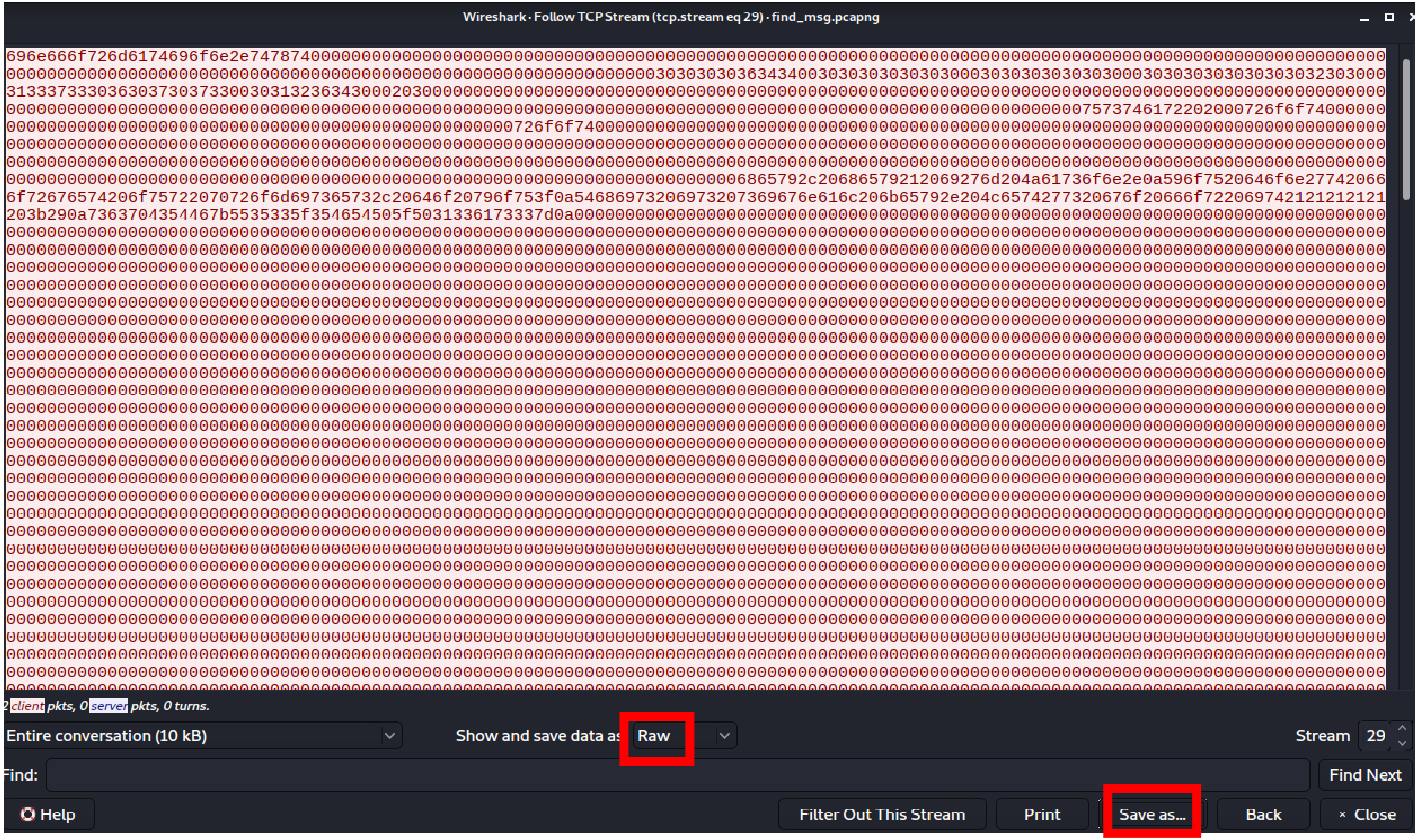
ftp-data

Interface Channel

No.	Time	Source	Destination	Protocol	Lengtl	Info
1020	11.7418256…	192.168.0.105	192.168.0.103	FTP-DA…	10…	FTP Data: 1002 bytes (PORT) (NLST -l)
1058	19.0064827…	192.168.0.105	192.168.0.103	FTP-DA…	89	FTP Data: 35 bytes (PORT) (RETR gamekey.txt)
1548	65.9535646…	192.168.0.105	192.168.0.103	FTP-DA…	73…	FTP Data: 7300 bytes (PORT) (RETR info.tar)
1551	65.9540065…	192.168.0.105	192.168.0.103	FTP-DA…	29…	FTP Data: 2940 bytes (PORT) (RETR info.tar)

2 Find_him

2. 풀이법



Wireshark · Follow TCP Stream (tcp.stream eq 29) · find_msg.pcapng

```
696e666f726d6174696f6e2e7478740000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000303030303634340030303030303030003030303030303000303030303030303032303000
3133373330363037303733003031323634300020300000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000007573746172202000726f6f74000000
00000000000000000000000000000000000000000000000000726f6f740000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000006865792c20686579212069276d204a61736f6e2e0a596f7520646f6e27742066
6f72676574206f75722070726f6d697365732c20646f20796f753f0a546869732069732073696776e616c206b65792e204c6574277320676f20666f722069742121212121
203b290a7363704354467b5535335f354654505f5031336173337d0a00000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
```

2 client pkts, 0 server pkts, 0 turns.

Entire conversation (10 kB)

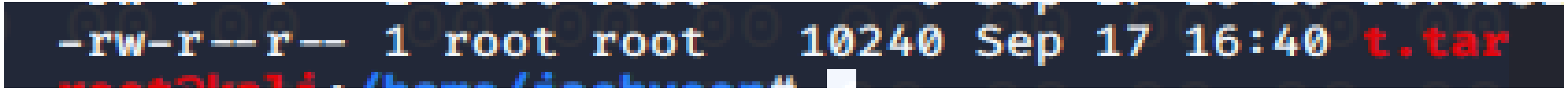
Show and save data as Raw

Stream 29

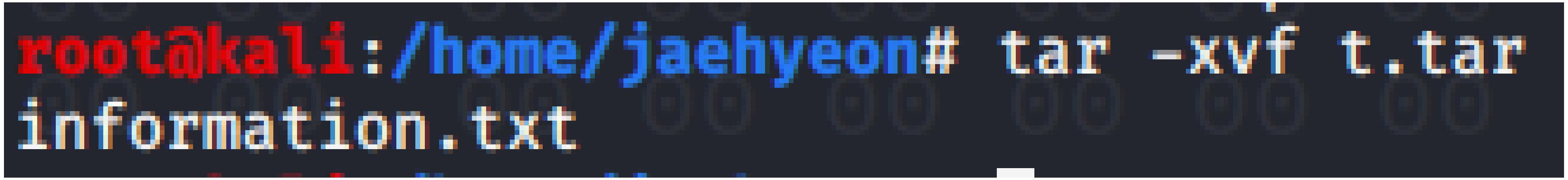
Find:

2 Find_him

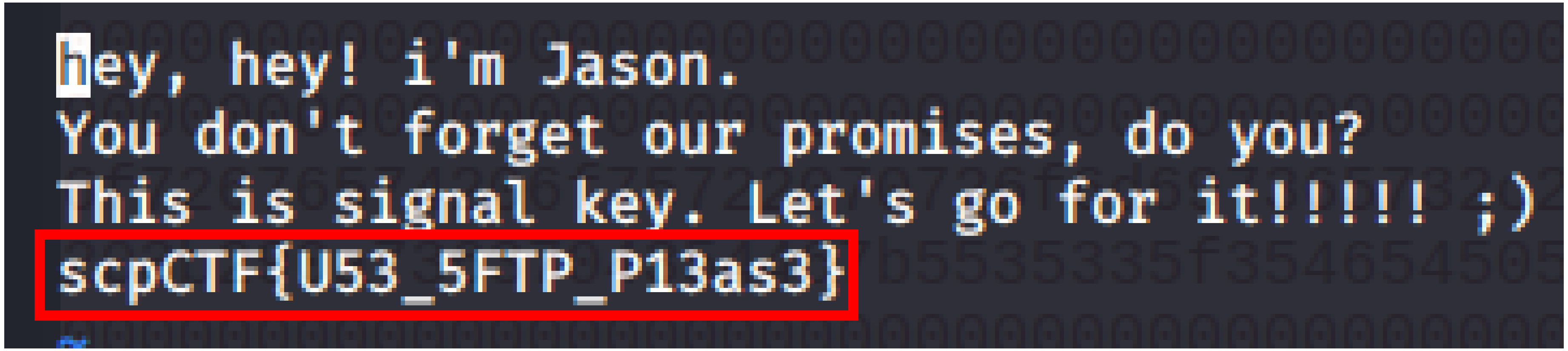
2. 풀이법



```
-rw-r--r-- 1 root root   10240 Sep 17 16:40 t.tar
```



```
root@kali:/home/jaehyeon# tar -xvf t.tar
information.txt
```



```
hey, hey! i'm Jason.
You don't forget our promises, do you?
This is signal key. Let's go for it!!!!! ;)
scpCTF{U53_5FTP_P13as3}
```

감사합니다 :)