Category: Network Traffic Analysis
Bracket: Bronze
Title: FTP Challenge **SOLUTION**

This challenge evaluates the participant's ability to understand a packet capture containing File Transfer Protocol (FTP) traffic - https://www.dropbox.com/s/ifoldfme3ip8y5p/NCL-2015-FTP.pcap?dl=0. During the game, it was suggested to use the Wireshark program to solve the challenge.

1. What was the first username/password combination attempt made to log in to the server? ex. 'user/password'	**user1/cyberskyline**
2. What software is the FTP server running (Name and version)?	**FileZilla Server 0.9.53**
3. What is the first username/password combination that allows for successful authentication?	**user1/metropolis**
4. What is the first command the user executes on the ftp server?	**list**
5. What file is deleted from the ftp server?	**bank.cap**
6. What file is uploaded to the ftp server?	**compcodes.zip**
7. What is the MD5 sum of the uploaded file?	**3303628E25D43BE4E11CC8878C5C5878**
8. What file does the anonymus user download?	**compcodes.zip**

Questions 1 and 2 can be solved by right-clicking on the first packet in the capture and using the “Follow > TCP Stream” option. Doing so will yield the following results:

```
220-FileZilla Server 0.9.53 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/
USER user1
331 Password required for user1
PASS cyberskyline
530 Login or password incorrect!
QUIT
221 Goodbye
```

Questions 4-6 can be solved by applying the filter:

ftp.response.code == 230

This filter searches for the server response that indicates that a session has been successfully authenticated. Once filtered, the “Follow > TCP Stream” option on the first packet will yield the following results:

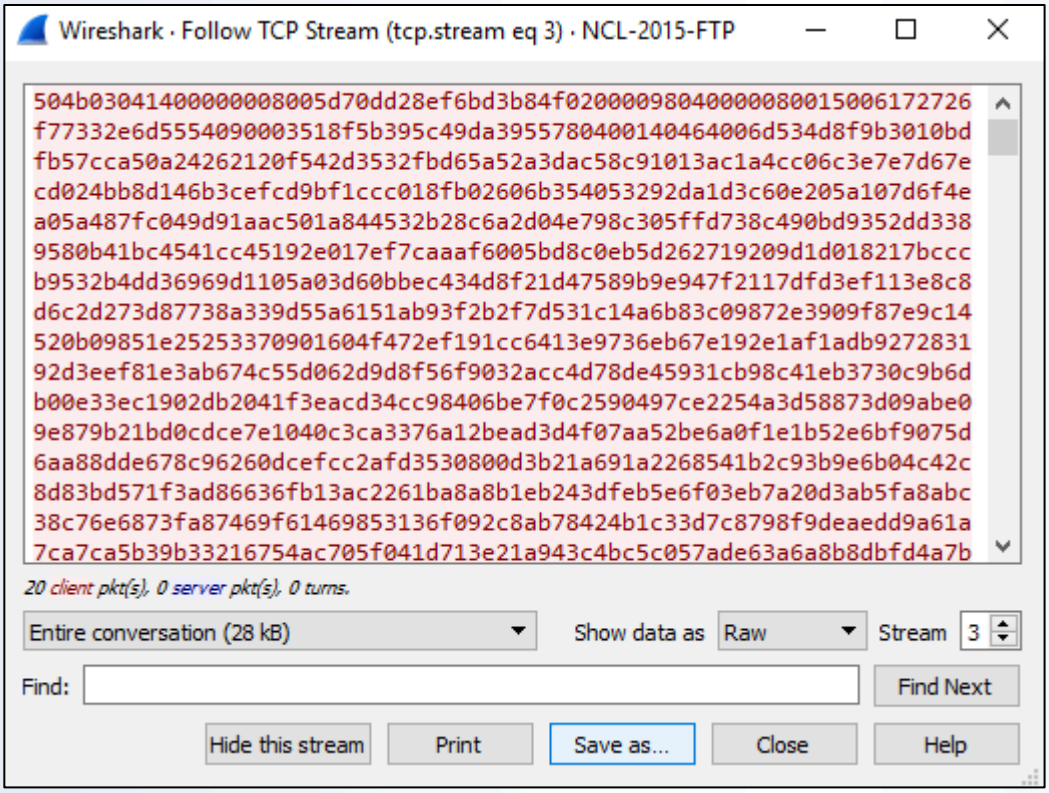
```
220-FileZilla Server 0.9.53 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/
USER user1
331 Password required for user1
PASS metropolis
230 Logged on
PORT 129,2,205,242,207,243
200 Port command successful
LIST
```


```
150 Opening data channel for directory listing of "/"
226 Successfully transferred "/"
DELE bank.cap
250 File deleted successfully
PORT 129,2,205,242,207,244
200 Port command successful
STOR compcodes.zip
150 Opening data channel for file upload to server of
"/compcodes.zip"
226 Successfully transferred "/compcodes.zip"
QUIT
221 Goodbye
```

Question 7 can be solved by applying the filter below and using knowledge of the packet numbers from the previous section:

ftp-data

The upload was started on packet number #23, thus the data should directly follow. Sure enough, there is a new stream of ftp-data starting on packet #25. The uploaded file can be saved to disk by following the TCP stream on packet #25, then selecting “Show Data as > Raw” and then saving the file by using “Save as..” The MD5 sum of the file can then be found using any hashing program/website.



Question 8 can be solved by again using the filter:

ftp.response.code == 230

However, this time, the 2nd TCP stream should be followed to yield the following:


```
220-FileZilla Server 0.9.53 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/
USER anonymous
331 Password required for anonymous
PASS
230 Logged on
PORT 129,2,205,242,207,246
200 Port command successful
RETR security
550 File not found
PORT 129,2,205,242,207,247
200 Port command successful
RETR bank.cap
550 File not found
PORT 129,2,205,242,207,248
200 Port command successful
LIST
150 Opening data channel for directory listing of "/"
226 Successfully transferred "/"
PORT 129,2,205,242,207,249
200 Port command successful
RETR compcodes.zip
150 Opening data channel for file download from server of
"/compcodes.zip"
226 Successfully transferred "/compcodes.zip"
PORT 129,2,205,242,207,250
200 Port command successful
STOR worm.txt
550 Permission denied
QUIT
221 Goodbye
```