**Lab 8: Decoding an FTP Protocol Session for Forensic Evidence**

**By**

**Natnael Kebede**



**University of Dallas**

**2020**

This Paper Submitted in Partial Fulfillment of the Requirements for

CYBS 7359 – Digital Forensics

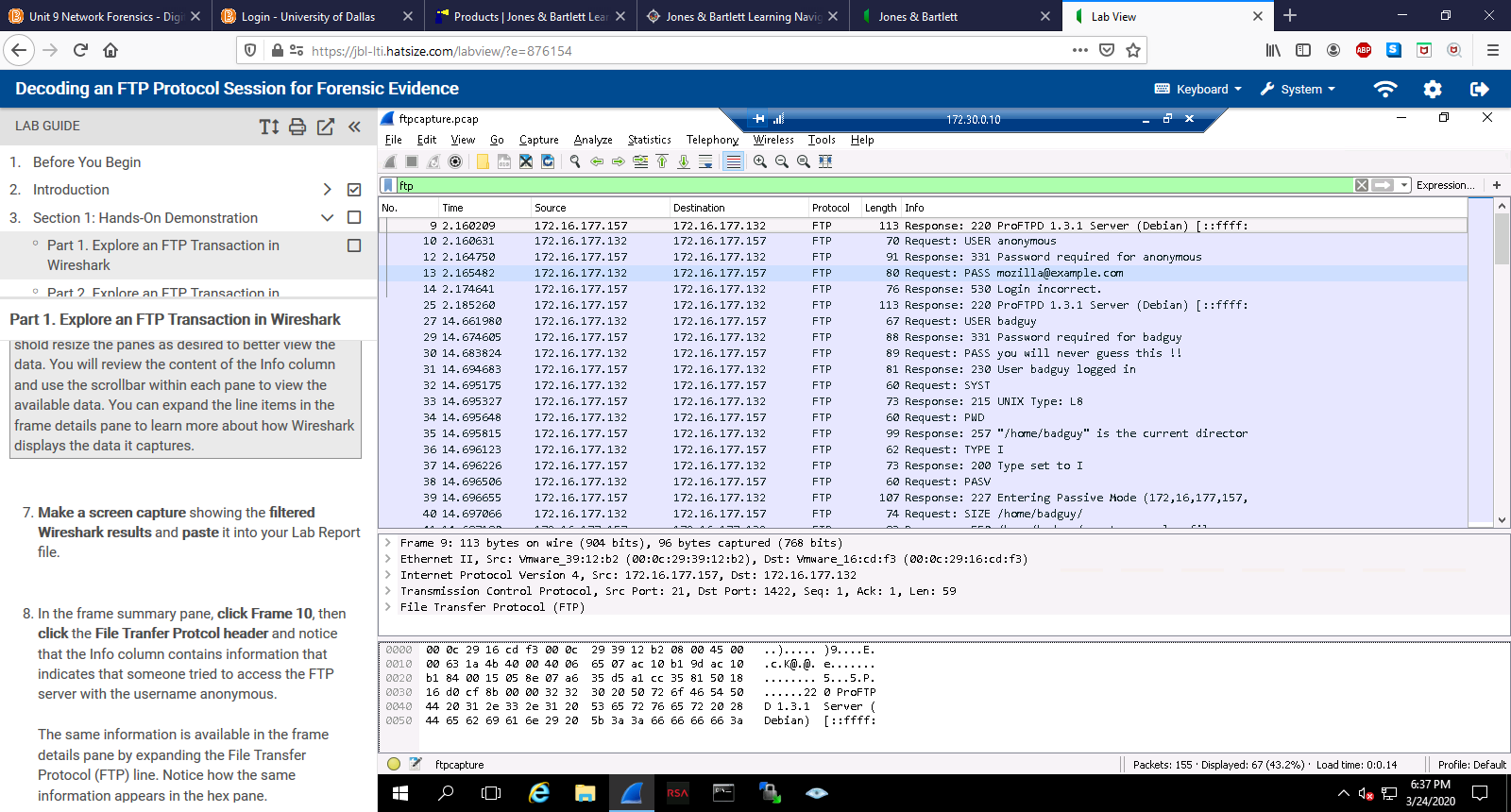
Spring 2020

Presented to Dr. Renita Murimi

**Section 1**

**Part 1**

1. Make a screen capture showing the filtered Wireshark results and paste it into your Lab Report file.

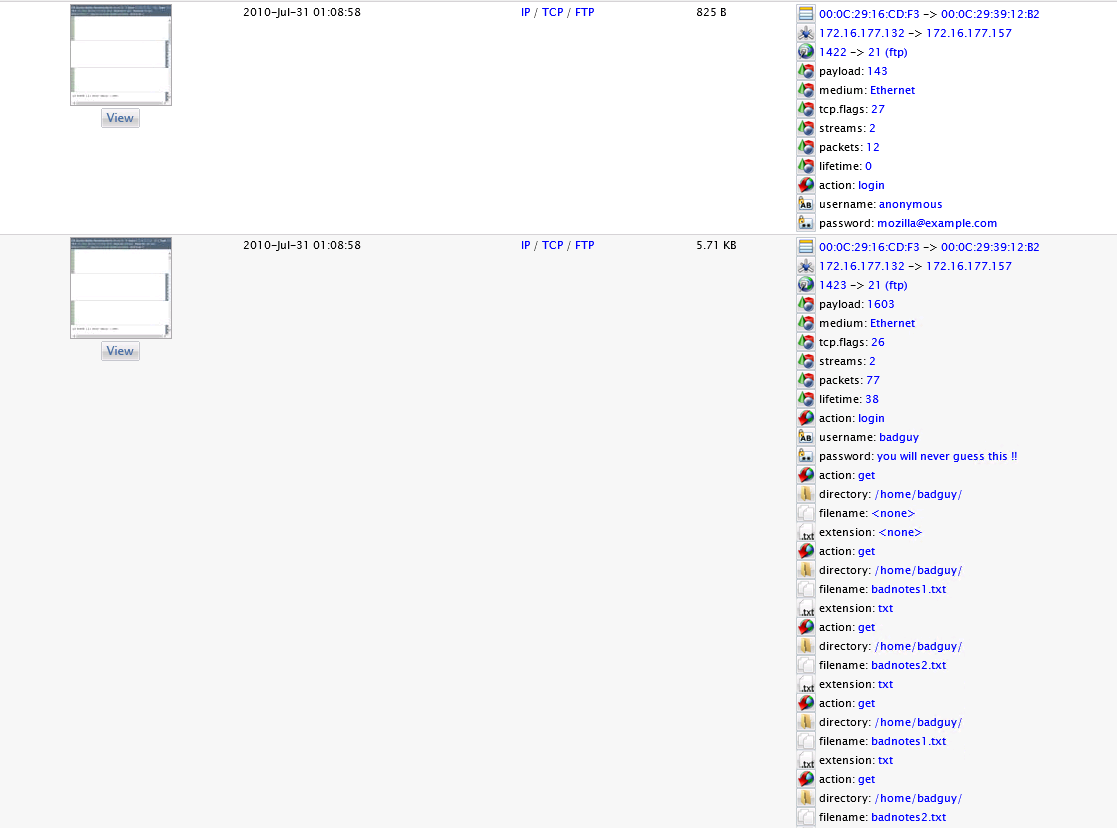


1. In the Lab Report file, document each item in the following list:

* IP address for the FTP client (the computer requesting login access)
  + 172.16.177.132
* IP address for the FTP sever (the computer granting login access)
  + 172.16.177.157
* MAC layer address of the FTP client
  + 00:0c:29:16:cd:f3
* MAC layer address of the FTP server
  + 00:0c:29:39:12:b2
* Source FTP port number and the destination FTP port number
  + Source (server): 21, destination (client):1422,1423

**Part 2**

Required list of NetWitness FTP details:



1. In the Lab Report file, document each item in the following list:

* The user accounts and passwords used to connect to the FTP server

|  |  |
| --- | --- |
| User Accounts | Passwords |
| anonymous | mozilla@example.com |
| badguy | you will never guess this !! |

* The names of the text files that were transferred via FTP

badnotes1.txt, badnotes2.txt

* The total file size of the FTP file transfer

5.71 KB

* The directory on the FTP server where the two text files are located

/home/badguy/