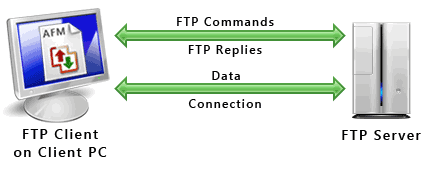
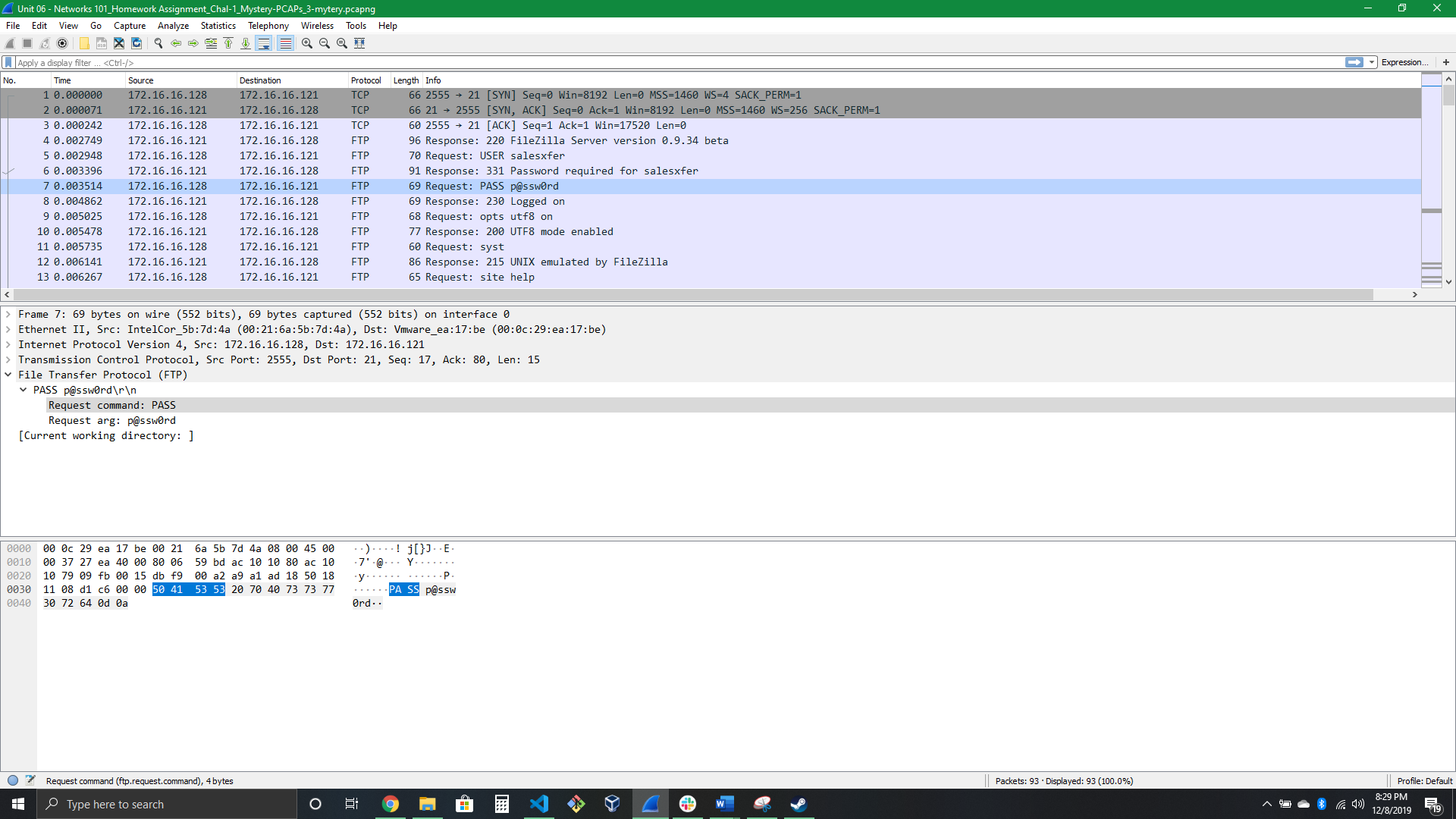
FTP Application Layer

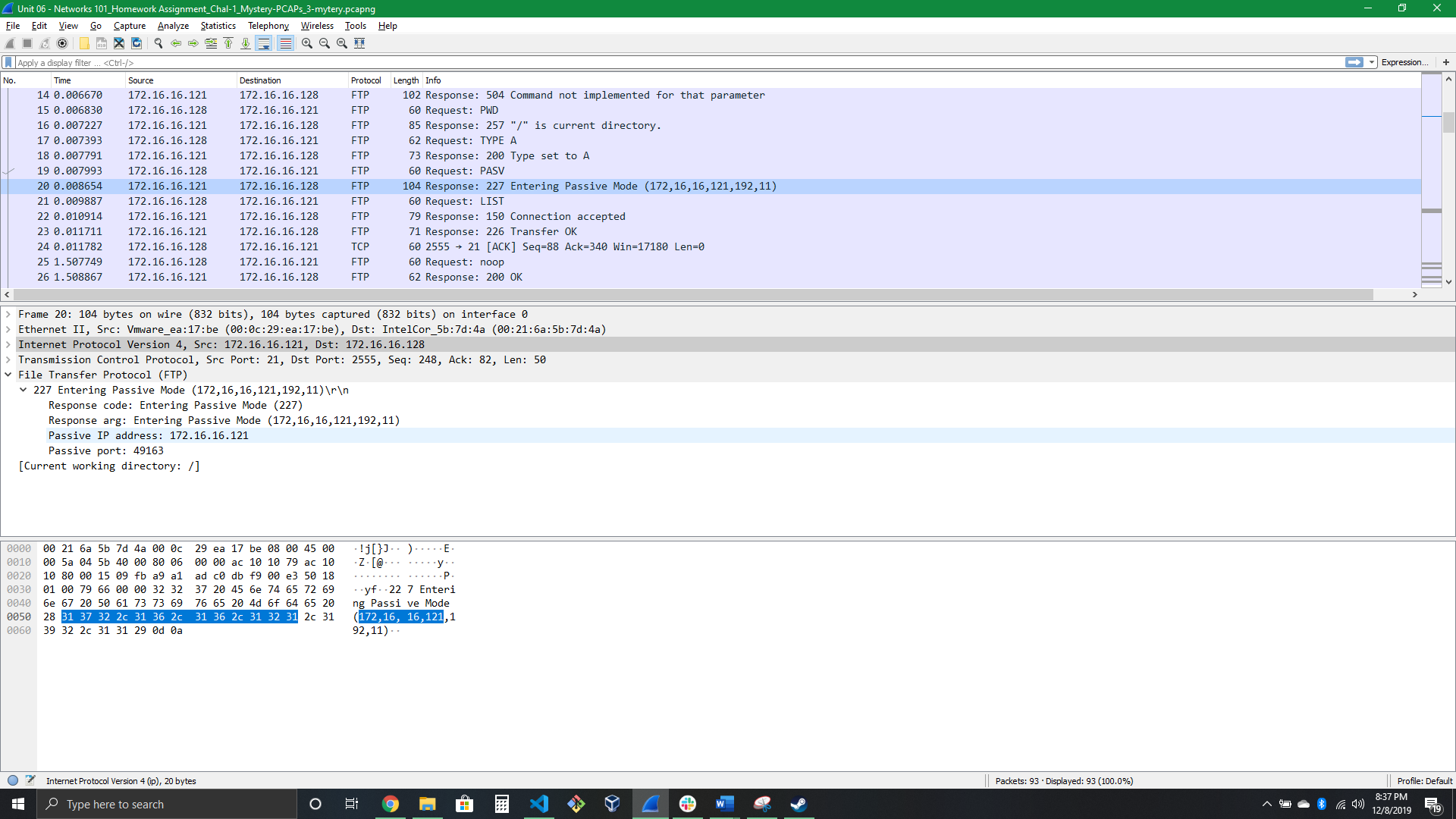
You may have heard of [FTP, or File Transfer Protocol](https://www.ftptoday.com/blog/sftp-vs-ftp-understanding-the-difference), but you might be unsure what it is exactly. At its core, the file transfer protocol is a way to connect two computers to one another in the safest possible way to help transfer files between two or more points. To put it simply, it’s the means by which files are securely shared between parties. (ftptoday)

 (Deskshare)

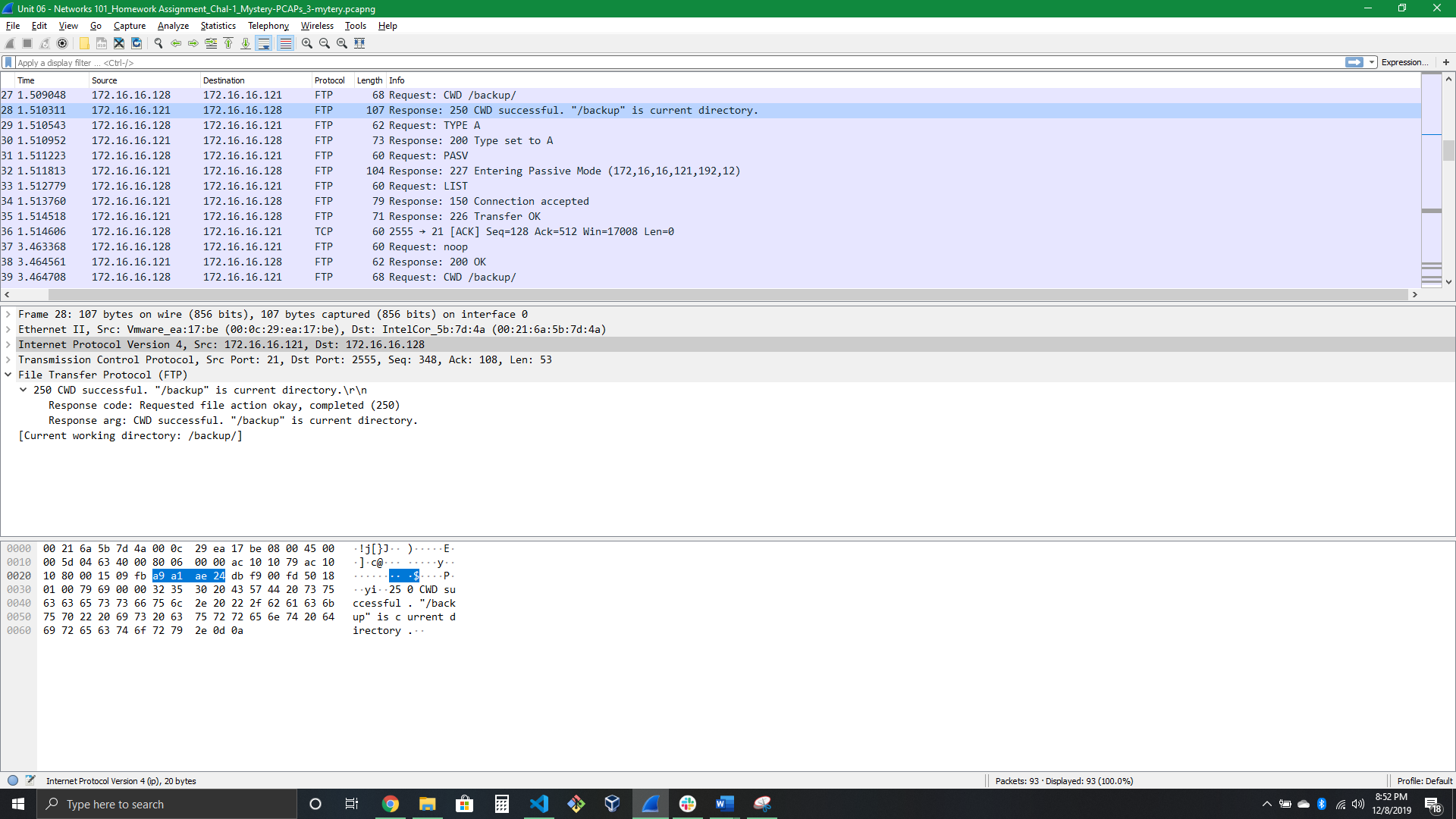
IP Address 172.16.16.128 on port 2555 is transferring files to Ip Address 172.16.16.121 on port 21. The Ip address ending in .128 is salesxfer and the Ip address ending in .121 is FileZilla. You can see where once the user tries to login as salesxfer, filezilla askes for a password. Next you can see how salesxfer sets UTF8 to on then they do a system command, and ask for help



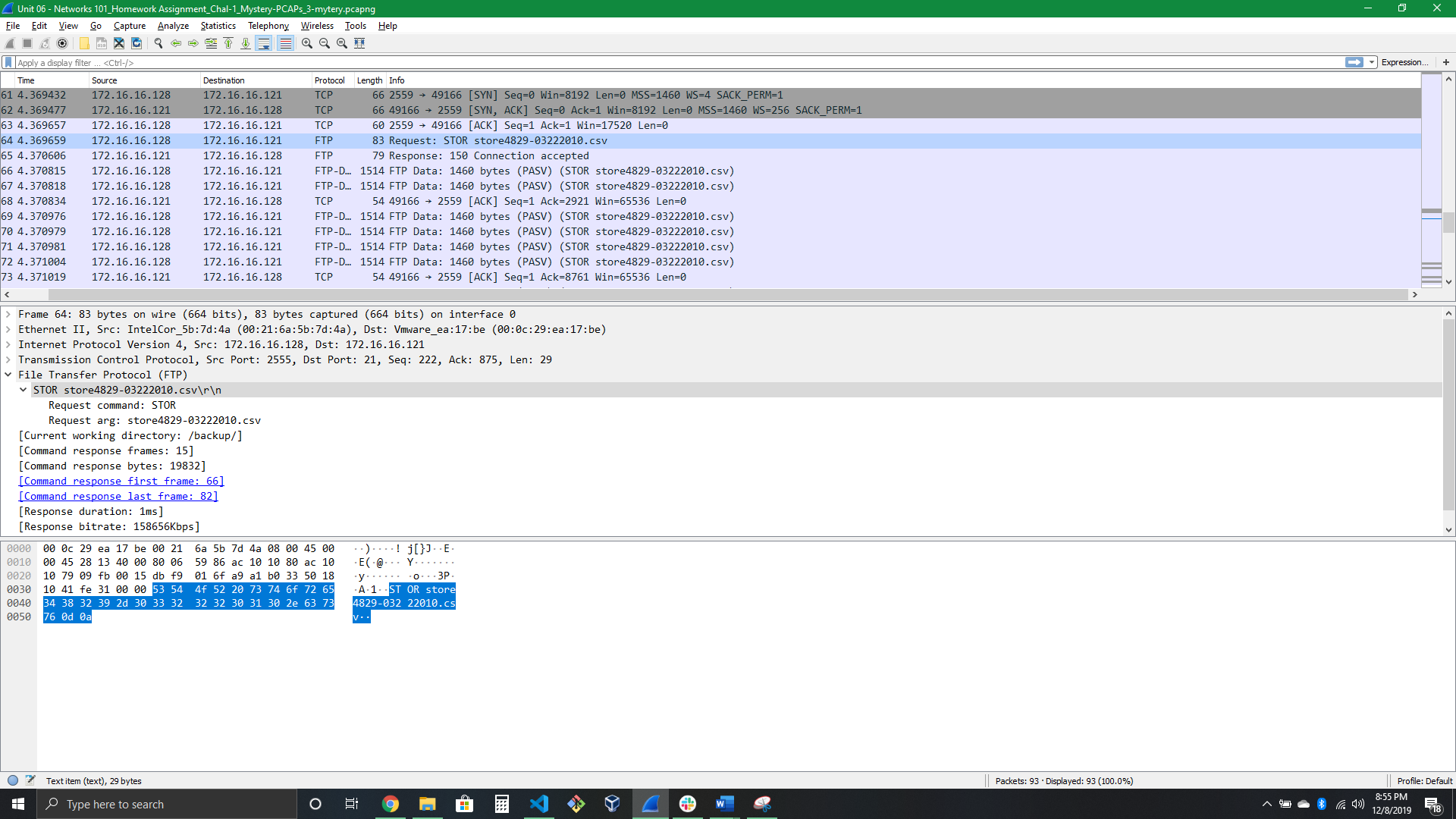
Now we get to see them try to figure out what directory they are in, then they set themselves to type A, enter passive mode on port 49163, list the contents of the directory and then transfer the info. The NOOP command does not cause the server to perform any action beyond acknowledging the receipt of the command. This command can be issued to the server to prevent the client from being automatically disconnected for being idle. It can also prevent modern routers/firewalls from closing a connection that it perceives as being idle as well. (servu)



We see salesxfer navigate to the backup directory and after going passive again, start to copy the files over to their system again.



After this we see salesxfer asking filezilla to store all the data in store4829-03222010.csv. Salesxfer just transferred 19 kilobytes worth of data for their personal use.

 The Biggest take away is that while using FTP Your data is not secure, not only that but if an attacker knows your file structure, they can nab the data like its nothing. This looks a lot like a man in the middle type of attack or at least privilege misuse.

# References

Horan, M. (2019, September 4). How Does an FTP Server Work and What are Its Benefits? Retrieved December 8, 2019, from <https://www.ftptoday.com/blog/how-does-an-ftp-server-work-the-benefits>.

Knowledge Base Resources – SolarWinds. (n.d.). Retrieved December 8, 2019, from <https://www.serv-u.com/resources/tutorial/mdtm-mkd-mode-noop-sscn-xcrc-ftp-command?Prod=su&cmd=MKD>.

List of FTP Commands for Windows: Serv-U. (n.d.). Retrieved December 8, 2019, from <https://www.serv-u.com/features/file-transfer-protocol-server-windows/commands>.

Understanding how FTP Works. (n.d.). Retrieved December 8, 2019, from <https://www.deskshare.com/resources/articles/ftp-how-to.aspx>.