**File Transfer**

***Log Analysis***

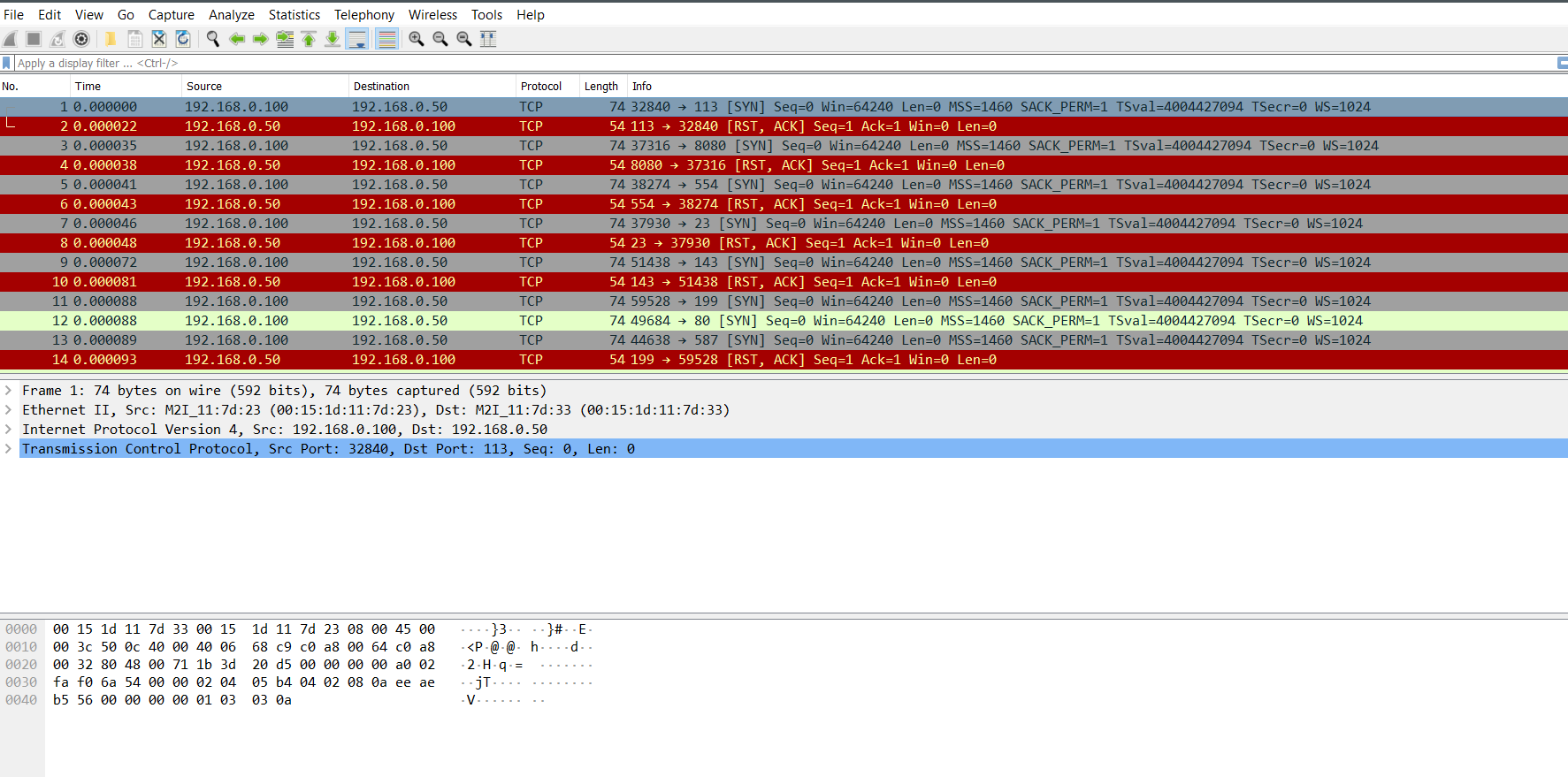
**Challenge:**

Can you find the name of the file exfiltrated from the target host?

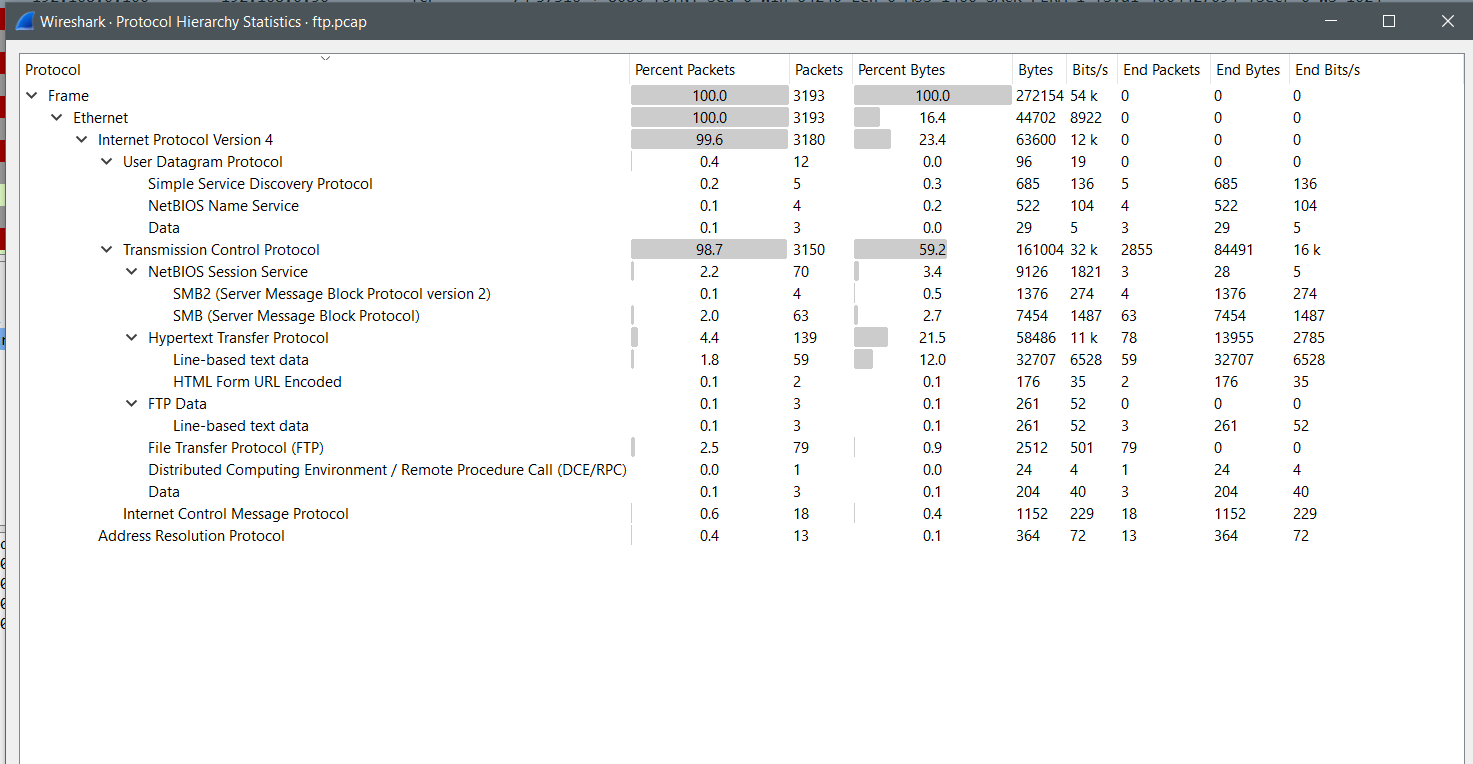
Attached - ftp.pcap

**Approach:**

That’s a wireshark capture file so we first open it up on wireshark.

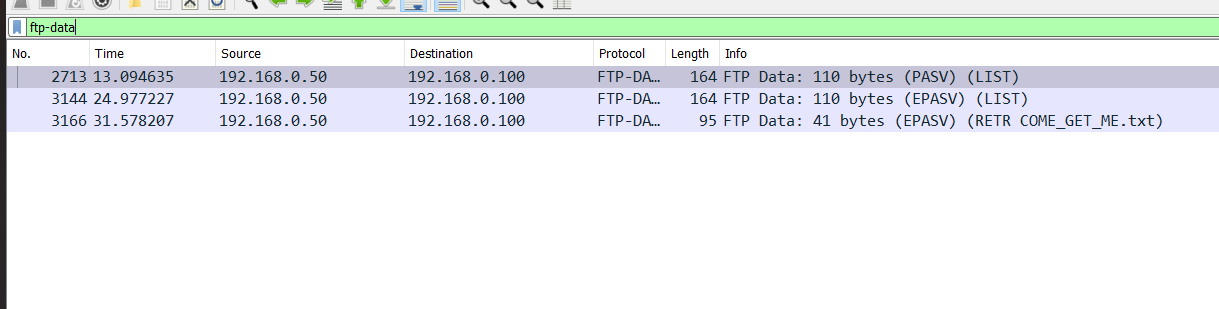


Go to ‘Statistics > Protocol Hierarchy’ and we see the type of protocols used in the capture.



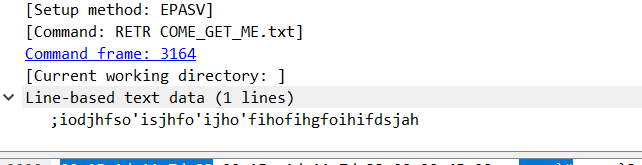
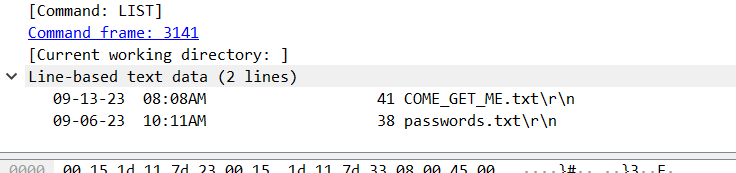
FTP Data packets? Hmm, interesting

Put up the display filter for ‘ftp-data’ and we see only 3 packets now



Upon further inspection we notice the following details:

1. There are 2 files that were listed using the LIST command, COME\_GET\_ME.txt and passwords.txt
2. Out of these two files, only the COME\_GET\_ME.txt file was retrieved using the RETR command, hence our answer!



We needed the file name only, hence the flag:

**Flag: COME\_GET\_ME**

Congrats!!

Happy Hacking!