Evidence B – Network capture of the dormitory network.

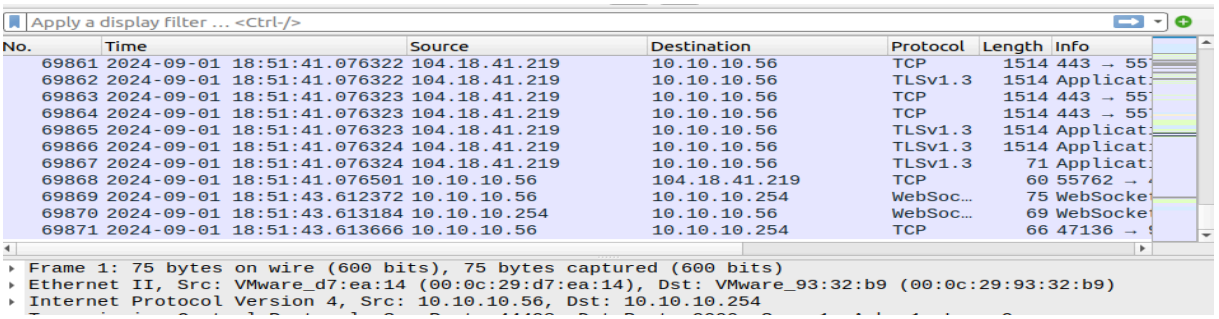
Check the MD5 checksum of the PCAP file; I used Network Miner and Wireshark for analysis.

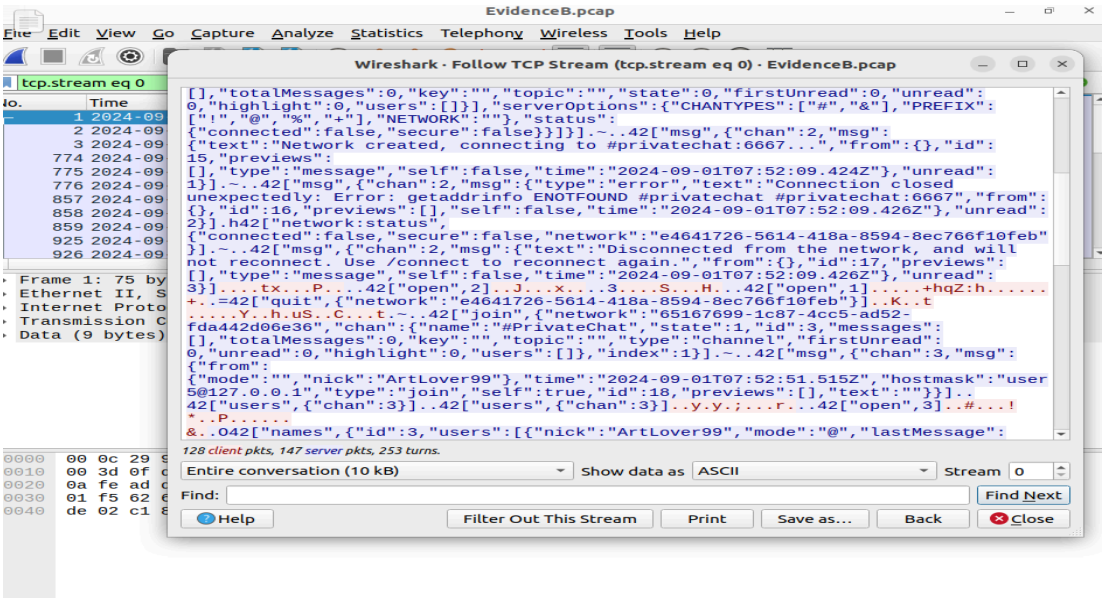
```
$ md5sum EvidenceB.pcap
b383bb9ae1dce23a4e72a0c192aafe80  EvidenceB.pcap
sansforensics@siftworkstation: ~/Desktop/cases
$
```

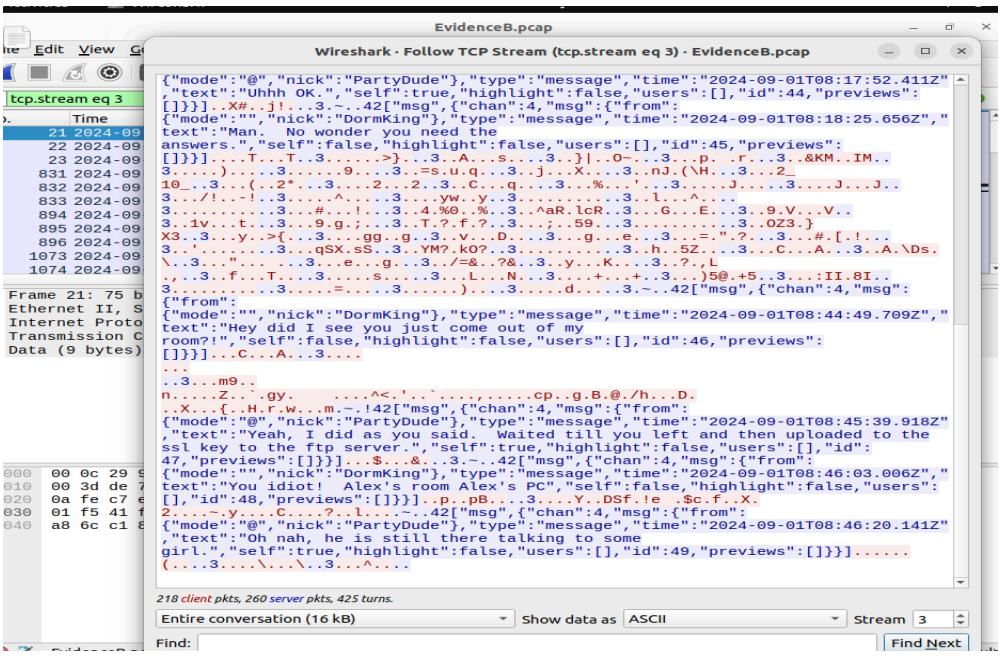
Who are the people communicating in the transmission? When does the first transmission begin and the last transmission finish?

I checked the timestamps for the first and last packets by going to the View tab in Wireshark, selecting the Time Display Format, and choosing Date and Time of Day. To examine the entire conversation for the TCP stream, I navigated to Analyze, selected Follow, and then chose TCP Stream.

The active participants between 17:28:33 and 18:51:43 were AlexM21 (Alex), DormKing, PartyDude, BookWorm, and ArtLover99 (Sophia). These timestamps are presented in local time (AES). However, the actual message timestamps in the TCP stream are recorded in UTC. For consistency with the other time events, I have used AES time in this context.







What browsers, operating systems, and IP addresses are used by the communication endpoints?

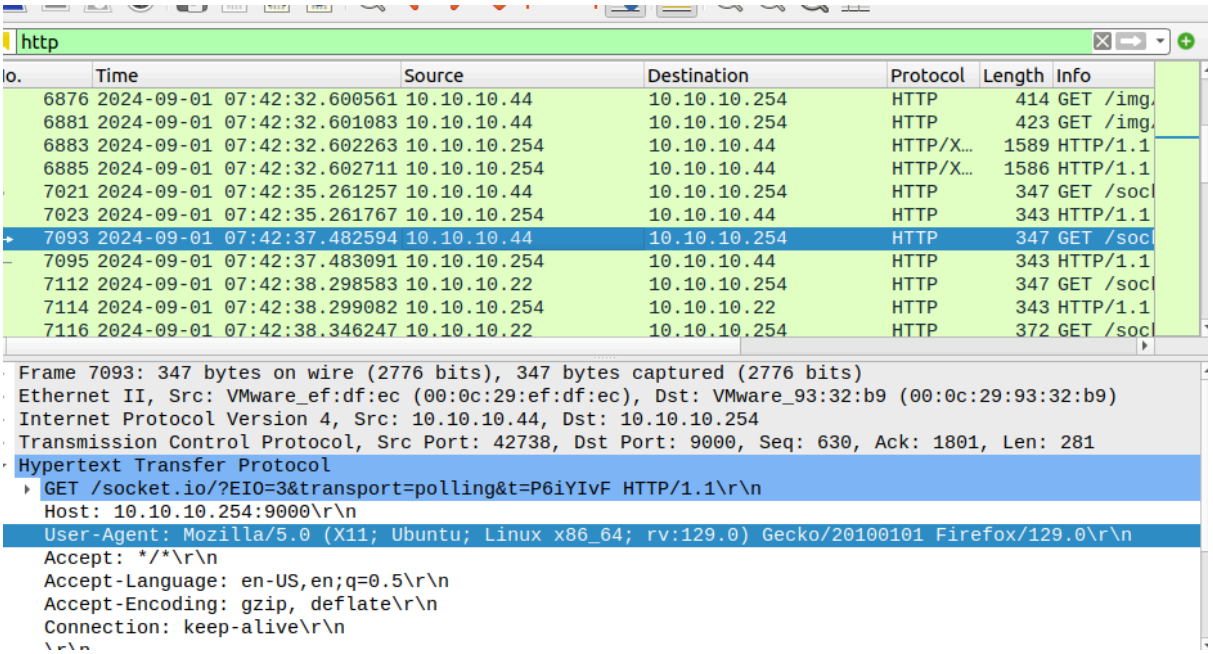
Browser: Firefox 129

Operating systems: Linux

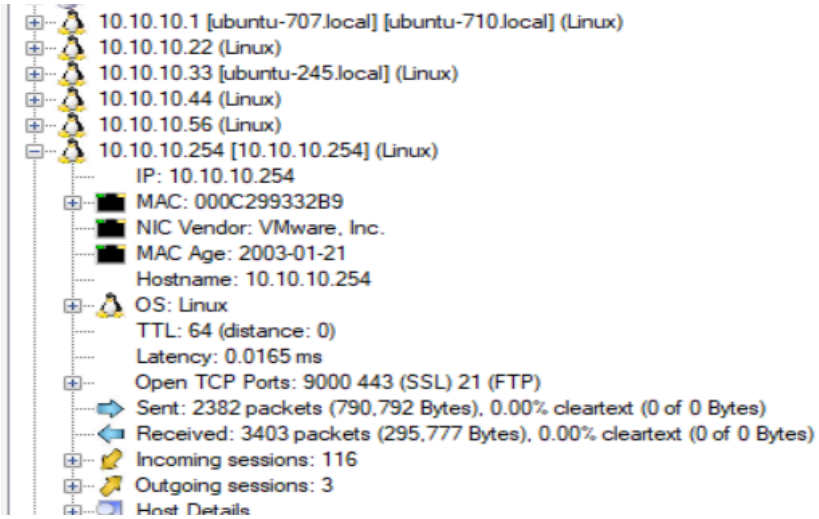
IP addresses: 10.10.10.22, 10.10.10.33, 10.10.10.44, 10.10.10.56 and 10.10.10.254

To identify the browser, I used Wireshark, searching for HTTP and expanding the Hypertext Transfer Protocol section to check the user-agent. For the operating system and IP addresses, I utilized Network Miner and clicked on the Host tab to locate this information.

Browser:

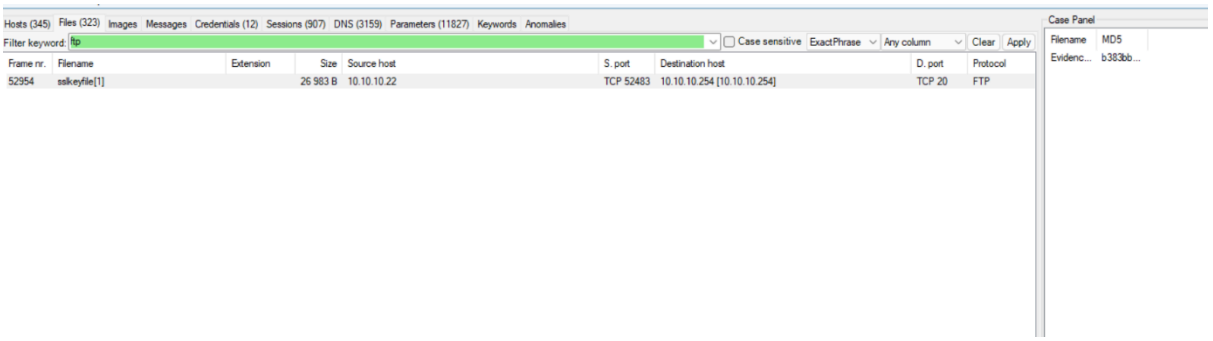


OS and IP addresses:



What files were transmitted on the local network?

From the group chat conversation, the participants discussed sending a file using FTP. I searched for "ftp" in the file keyword search on Network Miner and found the transmitted file named "sslkeyfile."



What is the relationship of the people communicating in the network capture? How are they related to the victim?

The individuals communicating in the network capture are university friends and girlfriend (Sophia) of the victim.