

## Evidence B – Network capture of the dormitory network.

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

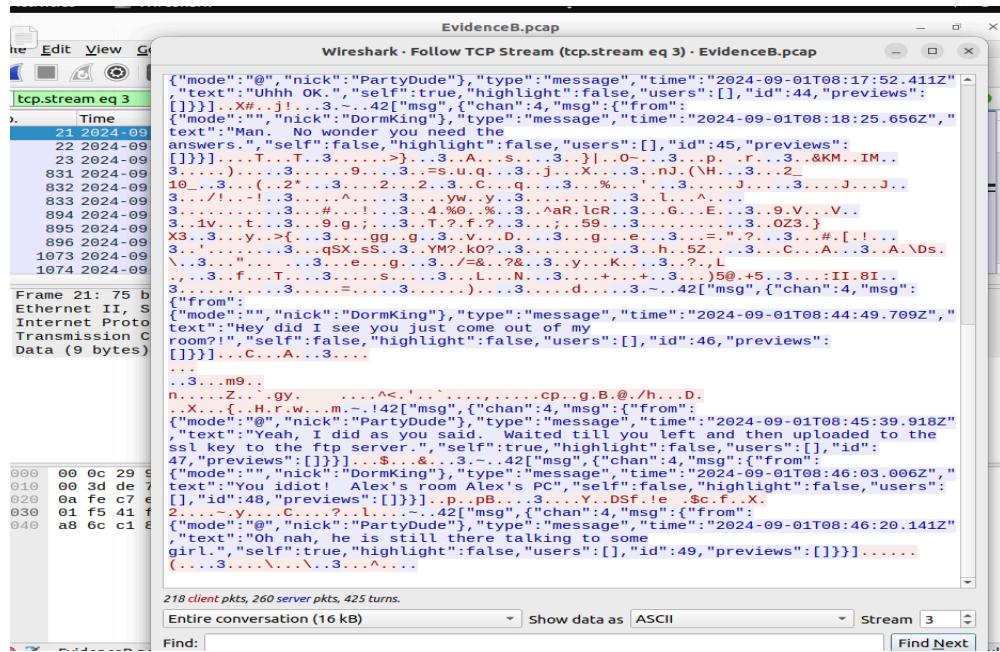
```
$ md5sum EvidenceB.pcap
b383bb9ae1dce23a4e72a0c192aafe80  EvidenceB.pcap
sansforensics@siftworkstation: ~/Desktop/cases
$
```

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.

The screenshot shows two windows of Wireshark. The top window displays a list of network packets (No., Time, Source, Destination, Protocol, Length, Info) from a capture named 'EvidenceB.pcap'. The bottom window shows a detailed view of a specific TCP stream (tcp.stream eq 0) for the same capture. The stream details the communication between multiple users, with the most recent activity shown in UTC time (e.g., 2024-09-01 18:51:43). The packet list shows the final frame (Frame 1) was captured at 18:51:43, consisting of 75 bytes over wire and 75 bytes captured.



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

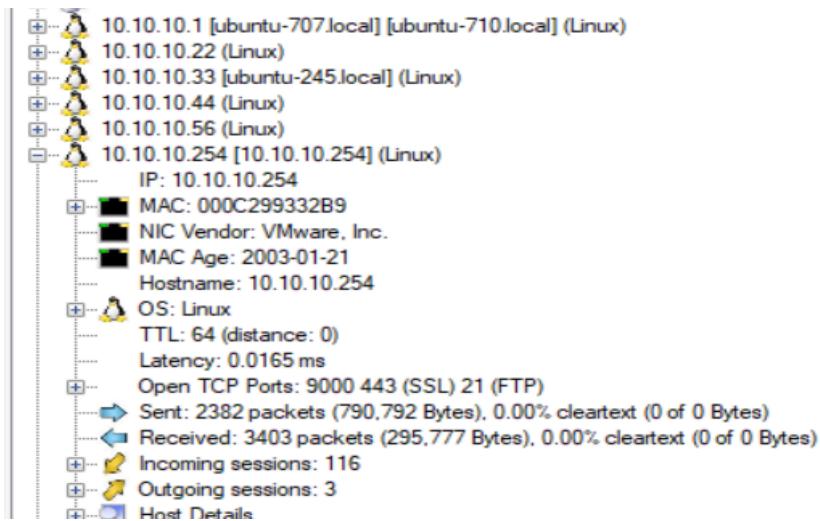
To identify the browser, I used Wireshark, searching for HTTP and expanding the Hypertext Transfer Protocol section to check the user-agent. For the operating system and IP addresses, I utilized Network Miner and clicked on the Host tab to locate this information.

Browser:

lo.	Time	Source	Destination	Protocol	Length	Info
6876	2024-09-01 07:42:32.600561	10.10.10.44	10.10.10.254	HTTP	414	GET /img
6881	2024-09-01 07:42:32.601083	10.10.10.44	10.10.10.254	HTTP	423	GET /img
6883	2024-09-01 07:42:32.602263	10.10.10.254	10.10.10.44	HTTP/X...	1589	HTTP/1.1
6885	2024-09-01 07:42:32.602711	10.10.10.254	10.10.10.44	HTTP/X...	1586	HTTP/1.1
7021	2024-09-01 07:42:35.261257	10.10.10.44	10.10.10.254	HTTP	347	GET /soc
7023	2024-09-01 07:42:35.261767	10.10.10.254	10.10.10.44	HTTP	343	HTTP/1.1
7093	2024-09-01 07:42:37.482594	10.10.10.44	10.10.10.254	HTTP	347	GET /soc
7095	2024-09-01 07:42:37.483091	10.10.10.254	10.10.10.44	HTTP	343	HTTP/1.1
7112	2024-09-01 07:42:38.298583	10.10.10.22	10.10.10.254	HTTP	347	GET /soc
7114	2024-09-01 07:42:38.299082	10.10.10.254	10.10.10.22	HTTP	343	HTTP/1.1
7116	2024-09-01 07:42:38.346247	10.10.10.22	10.10.10.254	HTTP	372	GET /soc

Frame 7093: 347 bytes on wire (2776 bits), 347 bytes captured (2776 bits)  
 Ethernet II, Src: VMware\_ef:df:ec (00:0c:29:ef:df:ec), Dst: VMware\_93:32:b9 (00:0c:29:93:32:b9)  
 Internet Protocol Version 4, Src: 10.10.10.44, Dst: 10.10.10.254  
 Transmission Control Protocol, Src Port: 42738, Dst Port: 9000, Seq: 630, Ack: 1801, Len: 281  
 Hypertext Transfer Protocol  
 > GET /socket.io/?EIO=3&transport=polling&t=P6iYIVF HTTP/1.1\r\n
 Host: 10.10.10.254:9000\r\n
 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:129.0) Gecko/20100101 Firefox/129.0\r\n
 Accept: \*/\*\r\n
 Accept-Language: en-US,en;q=0.5\r\n
 Accept-Encoding: gzip, deflate\r\n
 Connection: keep-alive\r\n
 \r\n

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."

Frame nr.	Filename	Extension	Size	Source host	S.port	Destination host	D.port	Protocol
52954	sslkeyfile[1]		26 983 B	10.10.10.22	TCP 52483	10.10.10.254 [10.10.10.254]	TCP 20	FTP

Case Panel  
 Filename: MD5  
 Evidence: b383b...

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.