

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

```

$ md5sum EvidenceB.pcap
b383bb9ae1dce23a4e72a0c192aafe80 EvidenceB.pcap
samsforensics@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.

No.	Time	Source	Destination	Protocol	Length	Info
69861	2024-09-01 18:51:41.076322	104.18.41.219	10.10.10.56	TCP	1514	443 → 55...
69862	2024-09-01 18:51:41.076322	104.18.41.219	10.10.10.56	TLsv1.3	1514	Applicat...
69863	2024-09-01 18:51:41.076323	104.18.41.219	10.10.10.56	TCP	1514	443 → 55...
69864	2024-09-01 18:51:41.076323	104.18.41.219	10.10.10.56	TCP	1514	443 → 55...
69865	2024-09-01 18:51:41.076323	104.18.41.219	10.10.10.56	TLsv1.3	1514	Applicat...
69866	2024-09-01 18:51:41.076324	104.18.41.219	10.10.10.56	TLsv1.3	1514	Applicat...
69867	2024-09-01 18:51:41.076324	104.18.41.219	10.10.10.56	TLsv1.3	71	Applicat...
69868	2024-09-01 18:51:41.076501	10.10.10.56	104.18.41.219	TCP	60	55762 → 4...
69869	2024-09-01 18:51:43.612372	10.10.10.56	10.10.10.254	WebSoc...	75	WebSoc...
69870	2024-09-01 18:51:43.613184	10.10.10.254	10.10.10.56	WebSoc...	69	WebSoc...
69871	2024-09-01 18:51:43.613666	10.10.10.56	10.10.10.254	TCP	66	47136 → 5...

Frame 1: 75 bytes on wire (600 bits), 75 bytes captured (600 bits)

Ethernet II, Src: VMware\_d7:ea:14 (00:0c:29:d7:ea:14), Dst: VMware\_93:32:b9 (00:0c:29:93:32:b9)

Internet Protocol Version 4, Src: 10.10.10.56, Dst: 10.10.10.254

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The main window is titled "Wireshark - Follow TCP Stream (tcp.stream eq 0) - Evidence-B.pcap".

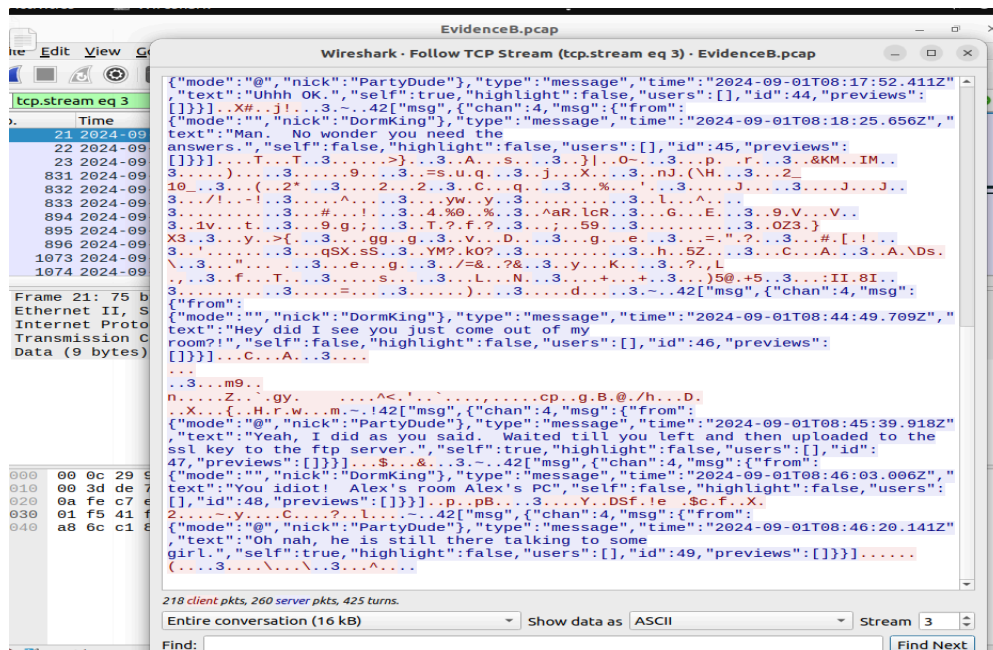
On the left, the "Packet List" pane shows a list of captured packets. The first packet (Frame 1) is selected, showing it is an Ethernet II, Internet Protocol, and Transmission Control Protocol (TCP) packet, with a length of 9 bytes.

The "Packet Details" pane for the selected packet shows the following structure:

- Ethernet II, Src: Intel (08:00:00:00:00:00), Dst: Intel (08:00:00:00:00:00), Length: 9 bytes
- Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.2, Length: 28 bytes
- Transmission Control Protocol, Src Port: 80, Dst Port: 80, Seq: 344016000, Win: 0, Len: 0

The "Packet Bytes" pane shows the raw data of the packet, which is a TCP reset (RST) packet. The data is displayed in hexadecimal and ASCII format.

The "Follow TCP Stream" pane shows the raw data of the selected packet, which is a TCP reset (RST) packet. The data is displayed in hexadecimal and ASCII format.



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

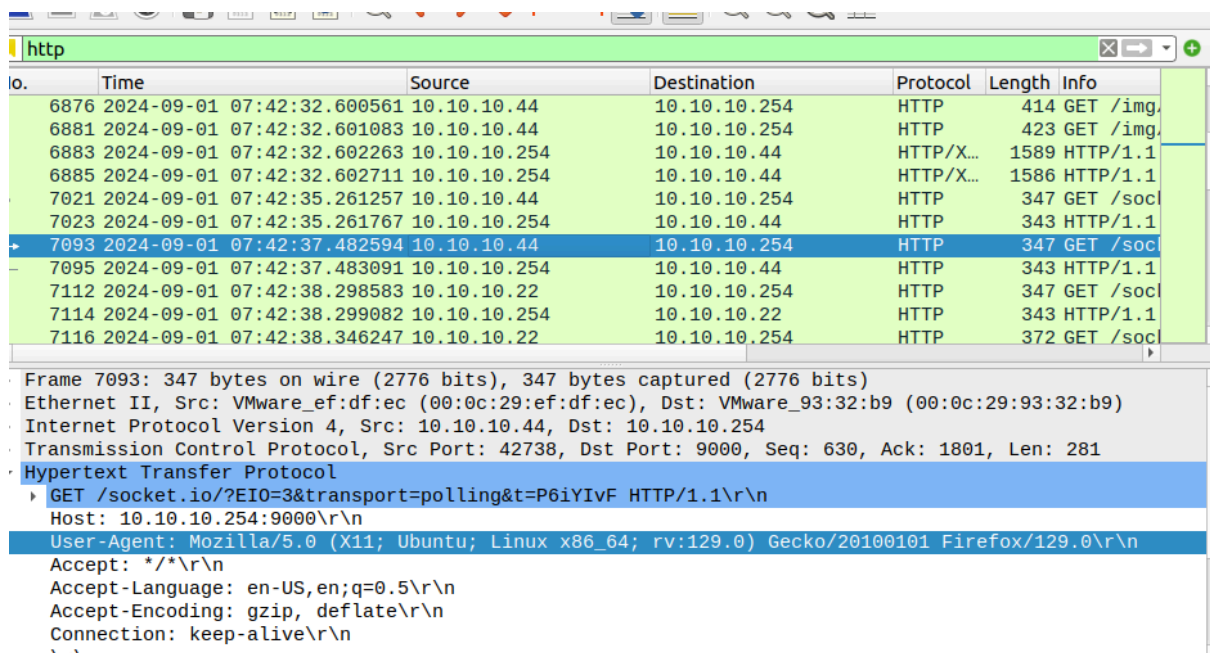
Browser: Firefox 129

Operating systems: Linux

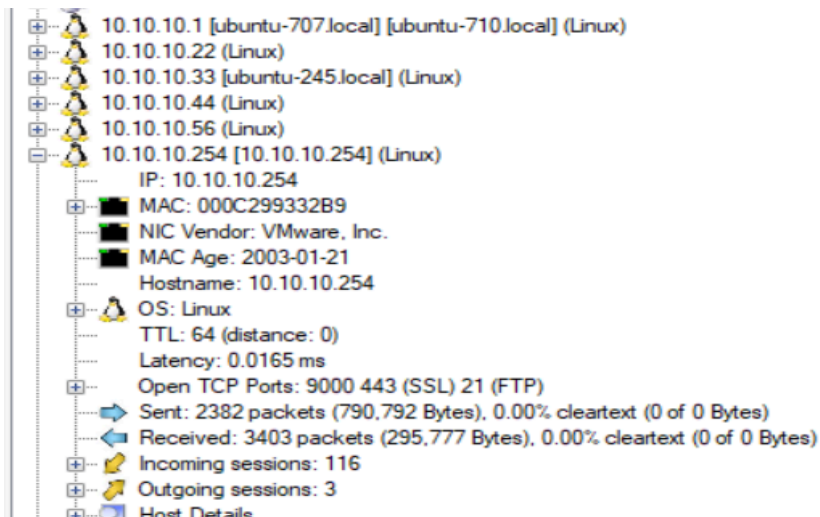
IP addresses: 10.10.10.22, 10.10.10.33, 10.10.10.44, 10.10.10.56 and 10.10.10.254

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."

Hosts (345) Files (323) Images Messages Credentials (12) Sessions (907) DNS (3159) Parameters (11827) Keywords Anomalies									
Filter keyword: <input type="text" value="ftp"/> <input type="checkbox"/> Case sensitive ExactPhrase <input type="text" value="Any column"/> <input type="button" value="Clear"/> <input type="button" value="Apply"/>									
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

Evidenc... b383bb...

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.