Wireshark

Analyzing 2 pcap files in wireshark

PCAP 1

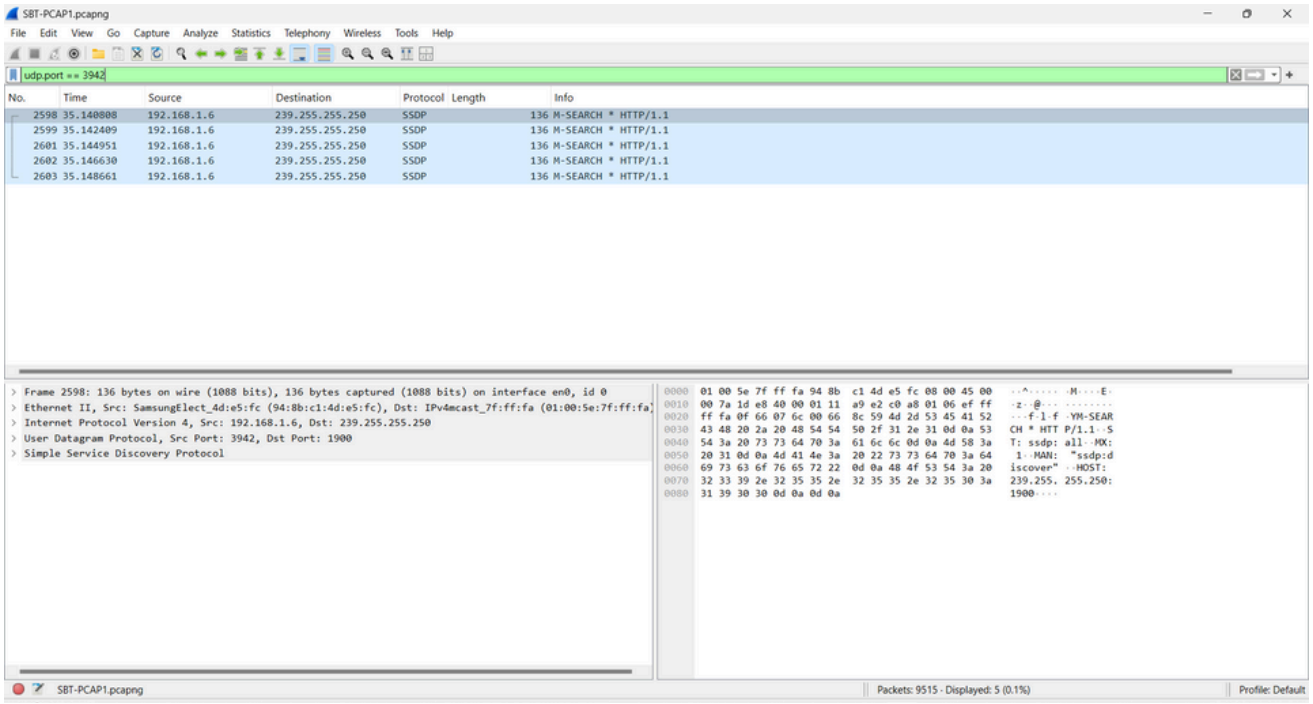
1. Which protocol was used over port 3942?
2. What is the IP address of the host that was pinged twice?
3. How many DNS query response packets were captured?
4. What is the IP address of the host which sent the most number of bytes?

PCAP 2

1. What is the WebAdmin password?
2. What is the version number of the attacker's FTP server?
3. Which port was used to gain access to the victim Windows host?
4. What is the name of a confidential file on the Windows host?
5. What is the name of the log file that was created at 4:51 AM on the Windows host?

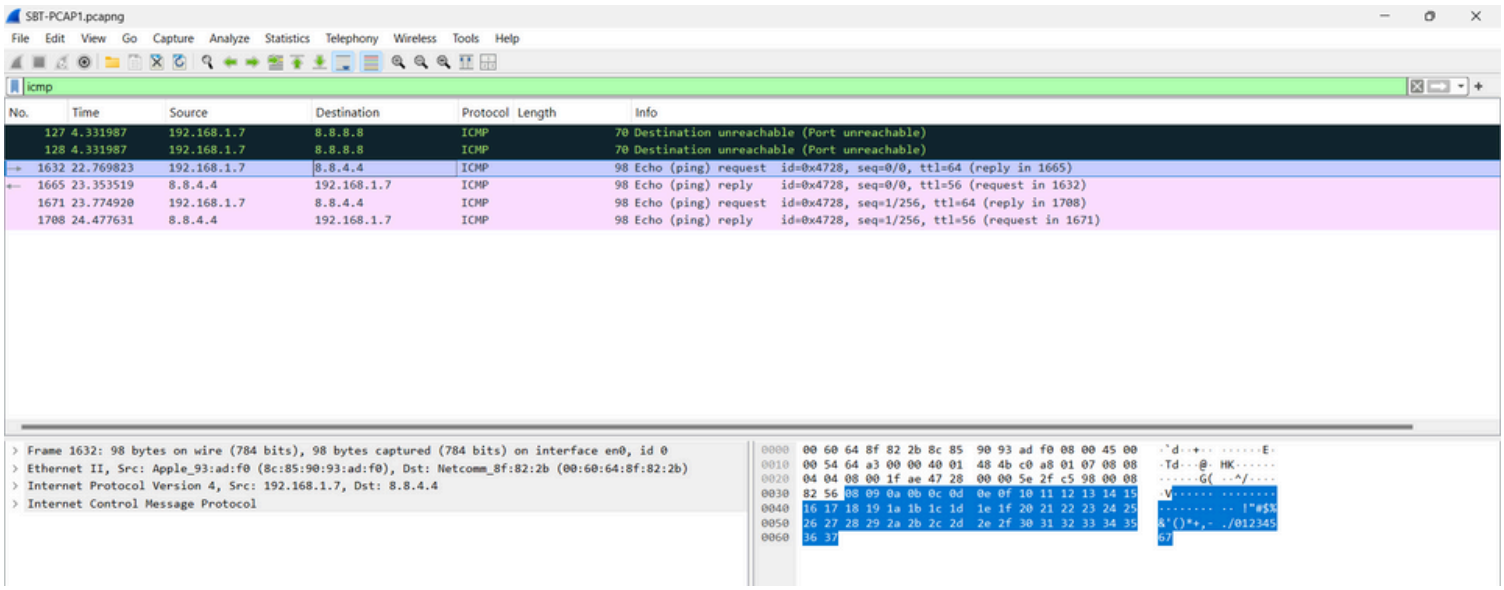
1. Protocol Used Over Port 3942

To identify the protocol, I applied the Wireshark filter udp.port == 3942. By doing this, I observed that the protocol being used over port 3942 was **SSDP (Simple Service Discovery Protocol).**



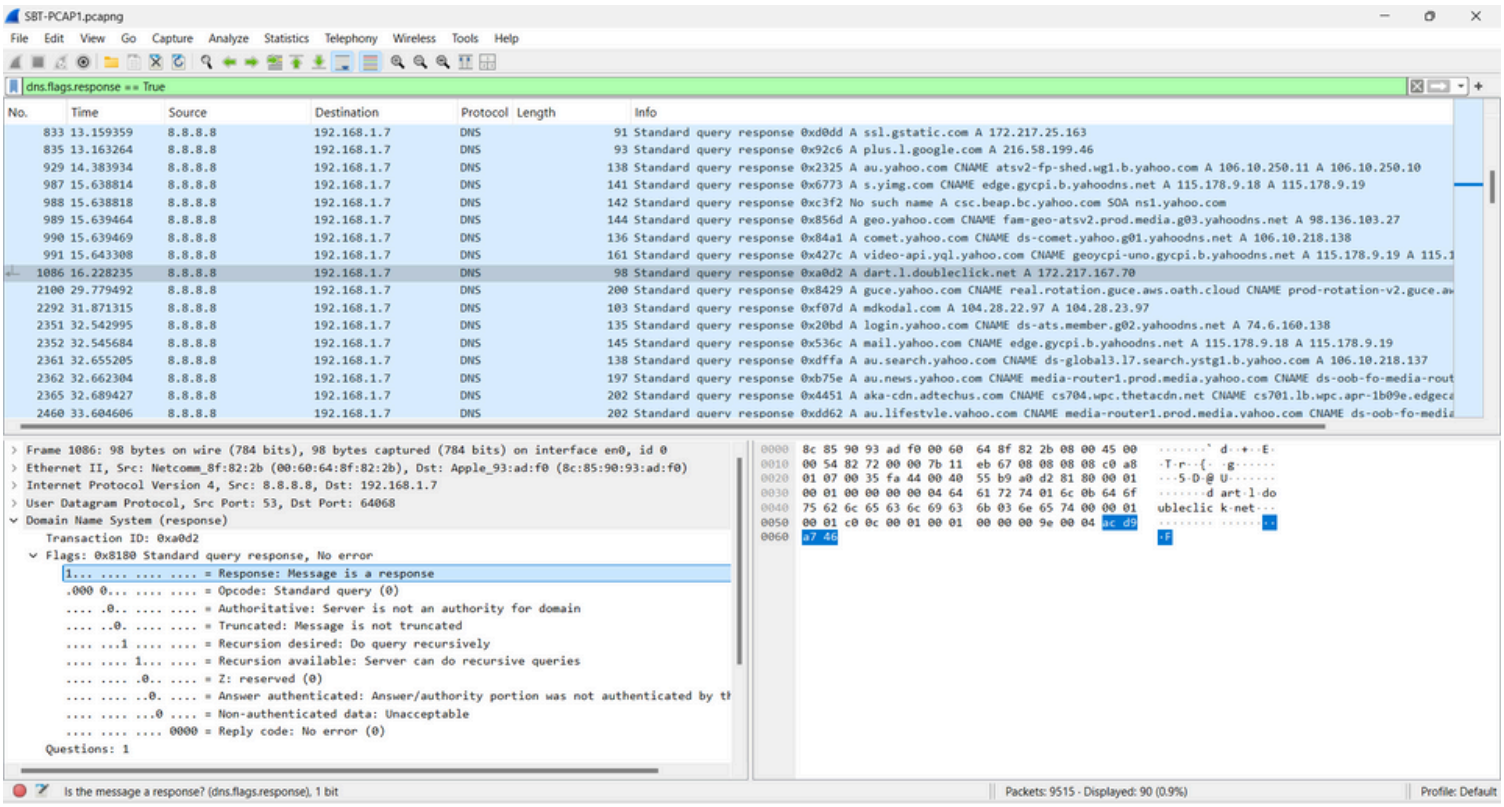
2. IP Address of Host Pinged Twice

I used the icmp filter and looked specifically for "echo request" packets. Through this analysis, I identified that the IP address **8.8.4.4** was the host that was pinged twice.

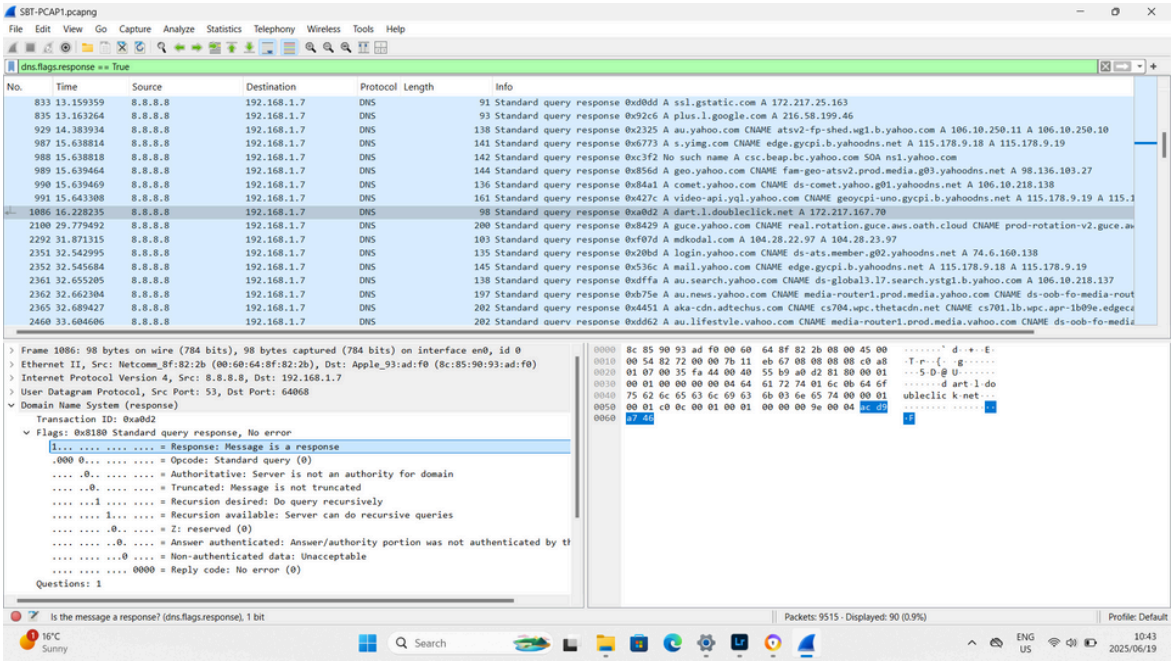


3. Number of DNS Query Response Packets Captured

To count the DNS query response packets, I applied the Wireshark display filter dns.flags.response == True. This filter specifically shows packets that are DNS responses. The analysis revealed that there were **90** such packets captured in the PCAP file.

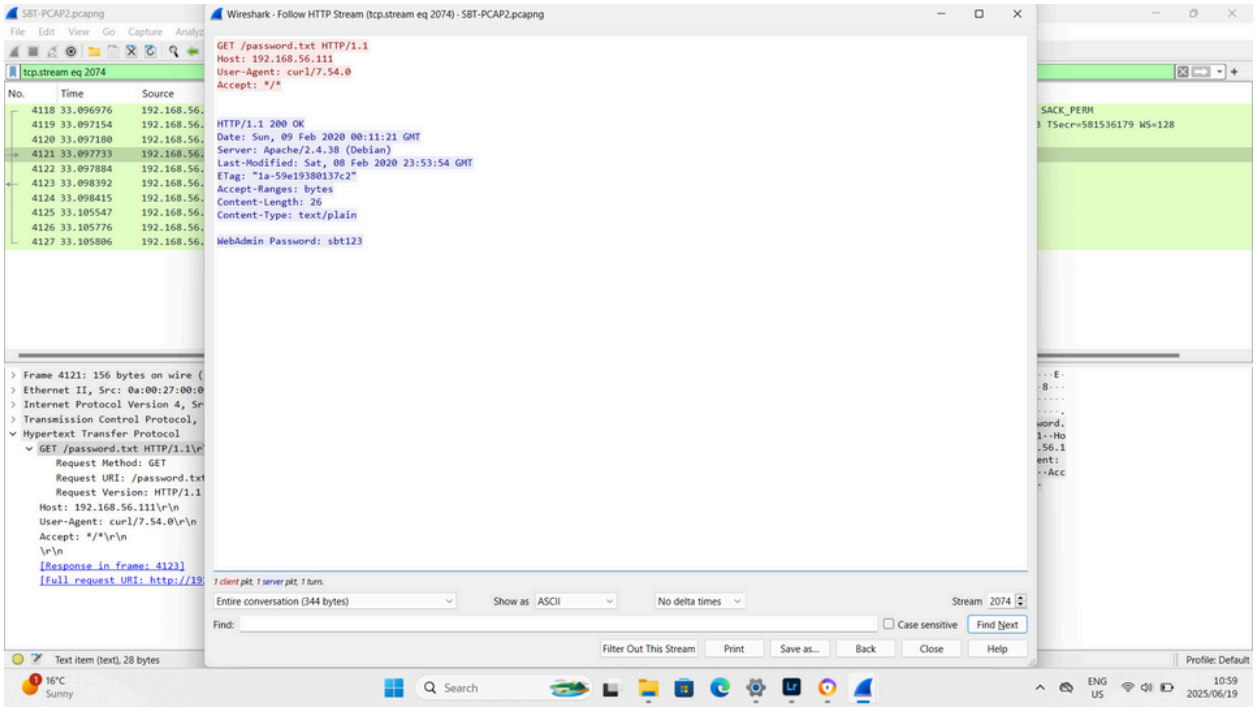


4. To find the IP address of the host that sent the most bytes, I navigated to the Statistics menu, then selected Endpoints, and specifically the IPv4 tab. From there, I clicked on Tx Bytes (transmit bytes) to arrange the results in descending order. The IP address that sent the most data was **115.178.9.18**.



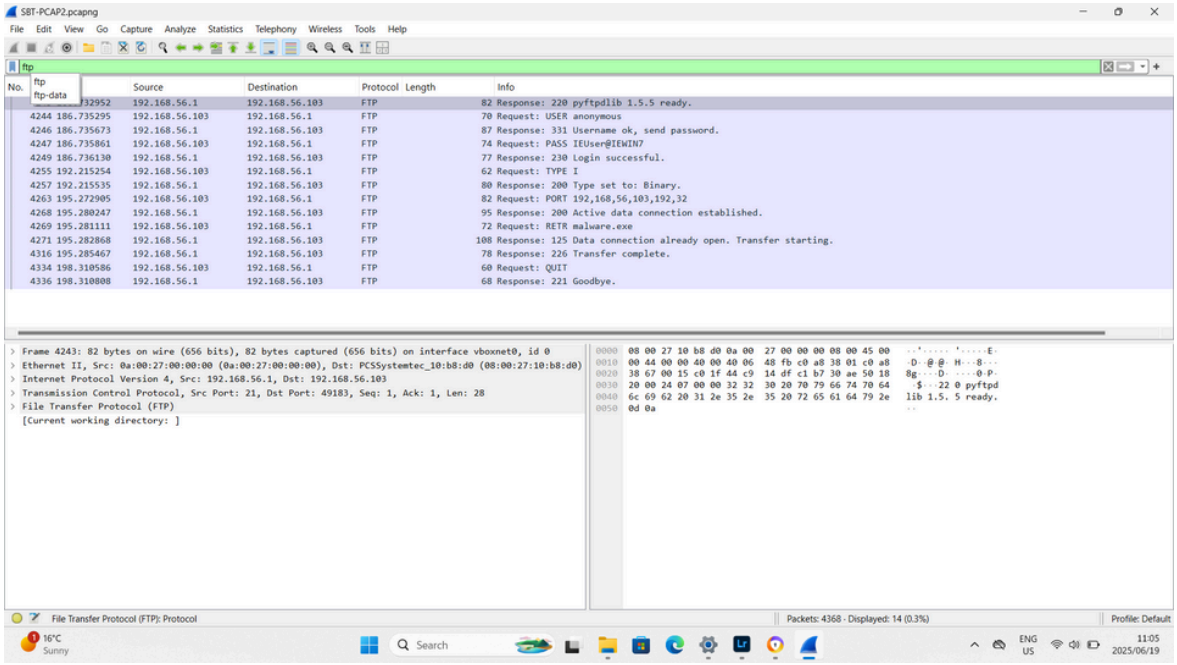
1. WebAdmin Password

To find the WebAdmin password in PCAP 2, I started by applying an http filter in Wireshark. I then looked for packets that used the GET method. After selecting the relevant packet, I clicked on the "Hypertext Transfer Protocol" details and chose to "Follow HTTP Stream." This allowed me to see the full conversation. Through this stream, I successfully found the WebAdmin password, which was **sbt123**.



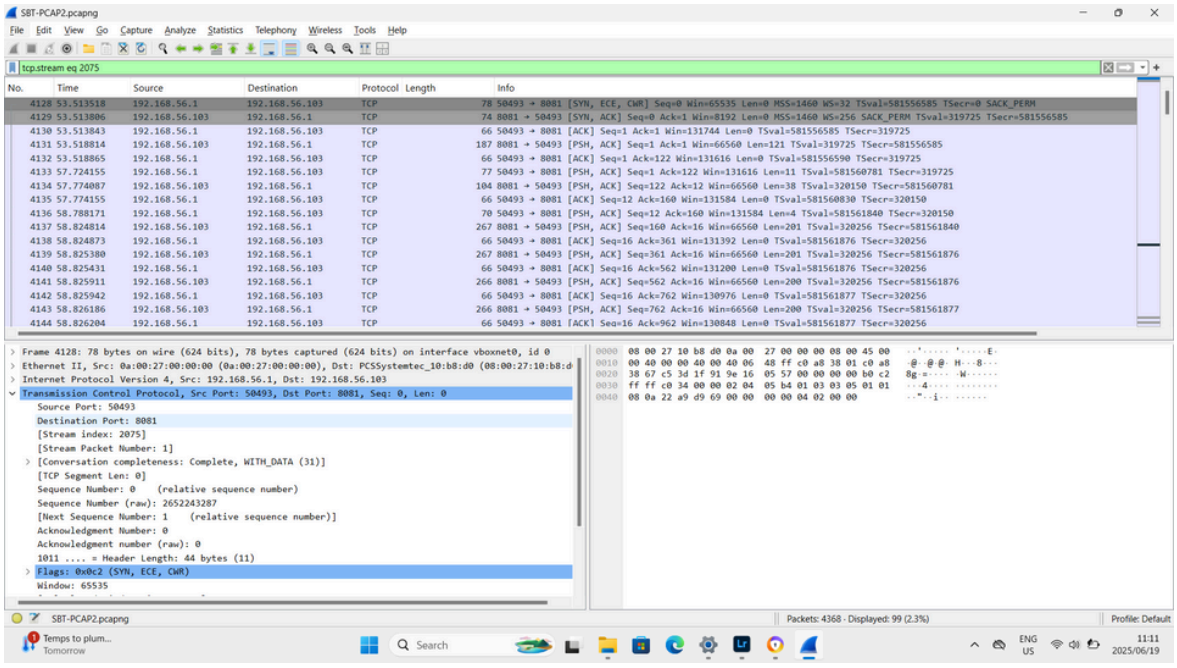
2. Attacker's FTP Server Version

To determine the version number of the attacker's FTP server, I applied an ftp filter in Wireshark. I then examined the information contained within the first FTP packet. This packet revealed that the FTP server version was pyftpdlib **1.5.5.**



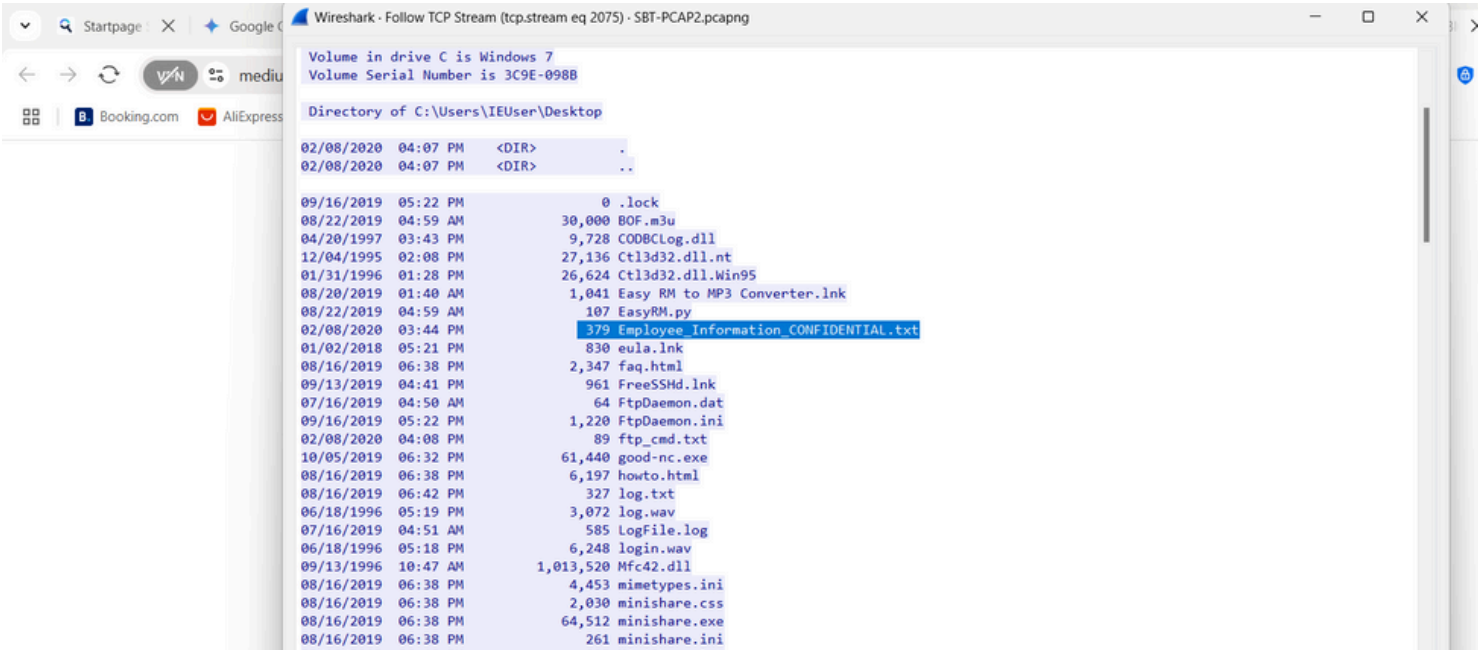
3. Port Used to Gain Access to Victim Windows Host

To identify the port used to gain access to the victim's Windows host, I applied a filter for ip.src == 192.168.56.1. After identifying relevant packets, I clicked packet 4128 then examined the "Transmission Control Protocol" panel. There, I found that the destination port used for access was **8081.** This port is often used for alternate HTTP services or web management interfaces.



4. Name of Confidential File on Windows Host

Continuing my analysis on packet 4128, I followed its TCP stream. Within this stream, I discovered a highly sensitive file named **Employee_Information_CONFIDENTIAL.txt**. This file likely contains private employee data and should not have been accessible or transferred in this manner



5. Name of Log File Created at 4:51 AM on Windows Host

Still within the same TCP stream from packet 4128, I looked for evidence of log file creation. I successfully found a log file named **LogFile.log**. This file was created on July 16, 2019, at 4:51 AM,