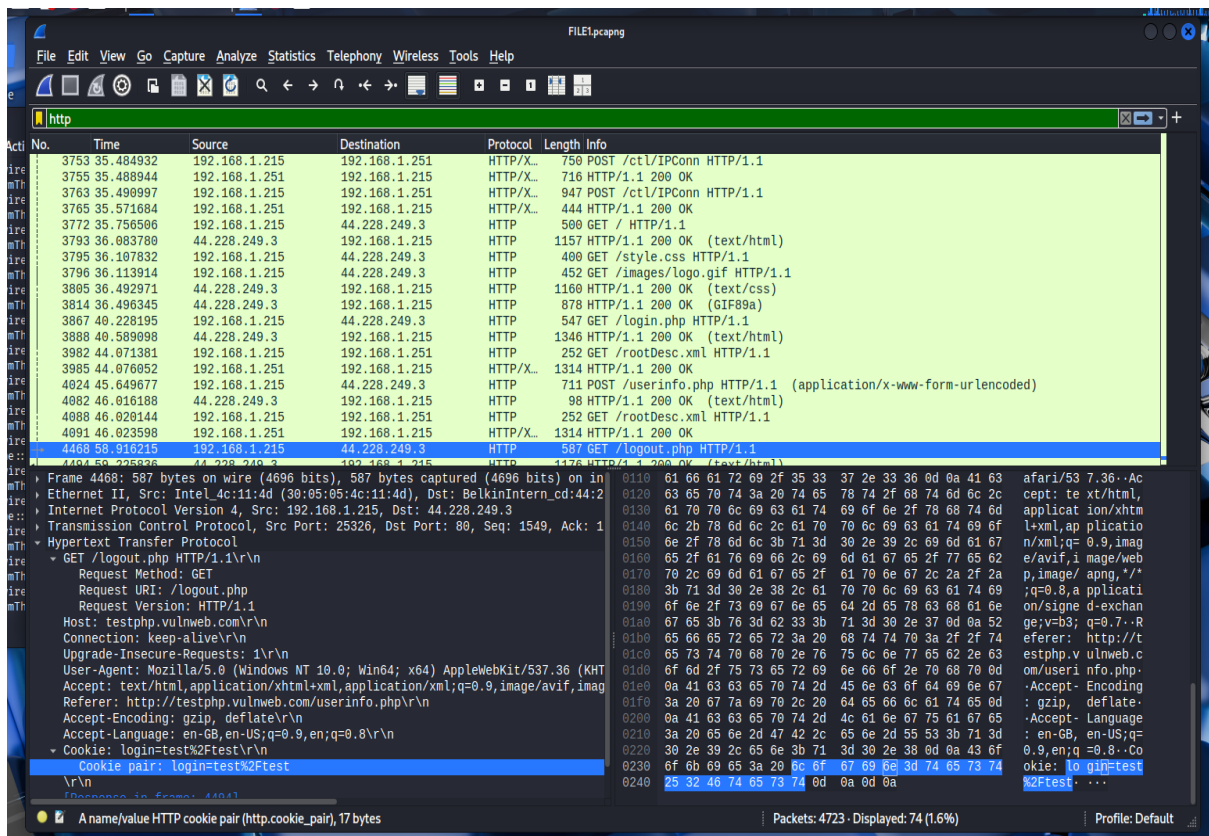
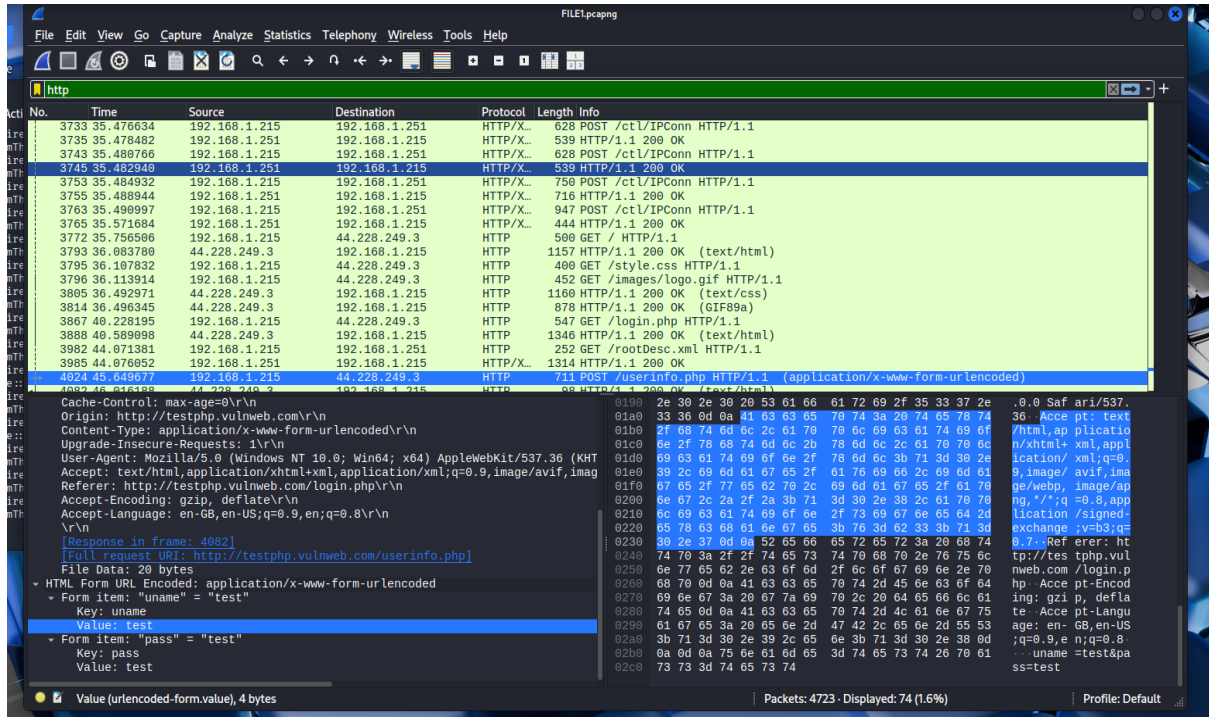


TASK 2

FILE 1

I was browsing unsecured website while my wireshark was active. Analyse the PCAP file and find out a credential present in the network logs.



FILE 2

Analyse the file and tell me what's wrong with the network data

The image shows a Wireshark packet capture analysis of a file named 'File2.pcap'. The packet list on the left shows a series of TCP SYN packets from various sources to 10.10.10.10. Packet 513, at time 0.109903, is highlighted and labeled as a 'Malformed Packet'. The packet details pane on the right shows the following information:

- Destination Port: 25565
- [Stream index: 494]
- [Conversation completeness: Incomplete, SYN_SENT (1)]
- [TCP Segment Len: 0]
- Sequence Number: 0 (relative sequence number)
- Sequence Number (raw): 4139384832
- [Next Sequence Number: 1 (relative sequence number)]
- Acknowledgment Number: 0
- Acknowledgment number (raw): 0
- 0101 = Header Length: 20 bytes (5)
- Flags: 0x002 (SYN)
- Window: 0
- [Calculated window size: 0]
- Checksum: 0xd373 [unverified]
- [Checksum Status: Unverified]
- Urgent Pointer: 0
- [Timestamps]
- Malformed Packet: PRP
- [Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]

The packet bytes pane on the right shows the raw data of the packet, which is mostly zeros, indicating a corrupted or malformed packet.

The image shows a Wireshark packet capture analysis of a file named 'File.pcap'. The packet list on the left shows a series of packets from 44:77:0f:ea:49 to 4c:72:b9:7c:b5:b7. The packet details pane on the right shows the following information:

- 0101 = Header Length: 20 bytes (5)
- Flags: 0x002 (SYN)
- Window: 0
- [Calculated window size: 0]
- Checksum: 0xb02f [unverified]

The packet bytes pane on the right shows the raw data of the packet, which is mostly zeros, indicating a corrupted or malformed packet.

No.	Time	Source	Destination	Protocol	Length	Info
370.0.091045	35.82.237.82	10.10.10.10	TCP	60	46182 → 25565 [SYN] Seq=0 Win=0 Len=0	
371.0.091121	209.237.195.197	10.10.10.10	TCP	60	29199 → 25565 [SYN] Seq=0 Win=0 Len=0	
372.0.091247	89.42.84.15	10.10.10.10	TCP	60	68031 → 25565 [SYN] Seq=0 Win=0 Len=0	
373.0.091248	47.45.192.16	10.10.10.10	TCP	60	61044 → 25565 [SYN] Seq=0 Win=0 Len=0	
374.0.091389	153.2.158.95	10.10.10.10	TCP	60	54946 → 25565 [SYN] Seq=0 Win=0 Len=0	
375.0.091619	218.121.78.61	10.10.10.10	TCP	60	25099 → 25565 [SYN] Seq=0 Win=0 Len=0	
376.0.091891	8.66.239.79	10.10.10.10	TCP	60	7722 → 25565 [SYN] Seq=0 Win=0 Len=0	
377.0.091977	29.209.159.86	10.10.10.10	TCP	60	10846 → 25565 [SYN] Seq=0 Win=0 Len=0	
378.0.092054	2.189.97.187	10.10.10.10	TCP	60	1501 → 25565 [SYN] Seq=0 Win=0 Len=0	
379.0.092493	14.99.45.29	10.10.10.10	TCP	60	12421 → 25565 [SYN] Seq=0 Win=0 Len=0	
380.0.092494	46.182.118.170	10.10.10.10	TCP	60	[TCP Retransmission] 18445 → 25565 [SYN] Seq=0 Win=0 Len=0	
381.0.092555	26.72.235.96	10.10.10.10	TCP	60	37312 → 25565 [SYN] Seq=0 Win=0 Len=0	
382.0.092556	176.44.171.200	10.10.10.10	TCP	60	82294 → 25565 [SYN] Seq=0 Win=0 Len=0	
383.0.093061	4.27.3.25	10.10.10.10	TCP	60	44358 → 25565 [SYN] Seq=0 Win=0 Len=0	
384.0.093132	186.18.13.152	10.10.10.10	TCP	60	906 → 25565 [SYN] Seq=0 Win=0 Len=0	
385.0.093197	122.194.215.62	10.10.10.10	TCP	60	93 → 25565 [SYN] Seq=0 Win=0 Len=0	
386.0.093335	78.194.212.88	10.10.10.10	TCP	60	[TCP Retransmission] 33069 → 25565 [SYN] Seq=0 Win=0 Len=0	
387.0.093363	150.209.145.229	10.10.10.10	TCP	60	58227 → 25565 [SYN] Seq=0 Win=0 Len=0	
388.0.093962	211.118.89.146	10.10.10.10	TCP	60	8696 → 25565 [SYN] Seq=0 Win=0 Len=0	
389.0.094332	141.246.245.40	10.10.10.10	TCP	60	43894 → 25565 [SYN] Seq=0 Win=0 Len=0	
390.0.094882	12.133.188.106	10.10.10.10	TCP	60	89268 → 25565 [SYN] Seq=0 Win=0 Len=0	

Frame 14: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
 Ethernet II, Src: JuniperNetwo_0f:ea:49 (44:f4:77:0f:ea:49), Dst: Pegatron_7c:b5:b7 (4c:72:b9:7c:b5:b7)
 Internet Protocol Version 4, Src: 62.150.70.105, Dst: 10.10.10.10
 Transmission Control Protocol, Src Port: 11043, Dst Port: 25565, Seq: 0, Len: 0

Wireshark - Endpoints - file.pcap

Endpoint Settings	Ethernet - 2	IPv4 - 37624	IPv6	TCP - 37670	UDP						
Name resolution	Address	Port	Packets	Bytes	Total Packets	Percent Filtered	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	
✓ Limit to display filter	8.244.162.10	46990	1	60 bytes	1	100.00%	1	60 bytes	0	0 bytes	
	8.246.114.181	49096	1	60 bytes	1	100.00%	1	60 bytes	0	0 bytes	
	8.246.156.229	8452	1	60 bytes	1	100.00%	1	60 bytes	0	0 bytes	
	8.247.13.196	53191	1	60 bytes	1	100.00%	1	60 bytes	0	0 bytes	
	8.251.128.21	48549	1	60 bytes	1	100.00%	1	60 bytes	0	0 bytes	
	8.252.130.22	57079	1	60 bytes	1	100.00%	1	60 bytes	0	0 bytes	
	8.253.168.183	49713	1	60 bytes	1	100.00%	1	60 bytes	0	0 bytes	
	8.254.214.26	17634	1	60 bytes	1	100.00%	1	60 bytes	0	0 bytes	
Copy	10.10.10.10	25565	37,841	2 MB	37,841	100.00%	0	0 bytes	37,841	2 MB	
Map	11.3.164.77	56987	1	60 bytes	1	100.00%	1	60 bytes	0	0 bytes	
	11.7.12.128	37788	1	60 bytes	1	100.00%	1	60 bytes	0	0 bytes	
	11.7.99.166	49405	1	60 bytes	1	100.00%	1	60 bytes	0	0 bytes	
	11.7.146.31	15121	1	60 bytes	1	100.00%	1	60 bytes	0	0 bytes	
Protocol	11.8.62.166	54953	1	60 bytes	1	100.00%	1	60 bytes	0	0 bytes	
Bluetooth	11.10.44.251	37596	1	60 bytes	1	100.00%	1	60 bytes	0	0 bytes	
IPV7	11.10.98.29	13814	1	60 bytes	1	100.00%	1	60 bytes	0	0 bytes	
DCCP	11.14.240.156	13018	1	60 bytes	1	100.00%	1	60 bytes	0	0 bytes	
✓ Ethernet	11.17.117.197	18856	1	60 bytes	1	100.00%	1	60 bytes	0	0 bytes	
FC	11.18.228.49	41346	1	60 bytes	1	100.00%	1	60 bytes	0	0 bytes	
FDDI	11.20.187.50	54814	1	60 bytes	1	100.00%	1	60 bytes	0	0 bytes	
IEEE 802.11	11.23.102.142	26432	1	60 bytes	1	100.00%	1	60 bytes	0	0 bytes	
✓ IEEE 802.15.4	11.24.185.20	25809	1	60 bytes	1	100.00%	1	60 bytes	0	0 bytes	
✓ IPv4	11.26.74.115	1446	1	60 bytes	1	100.00%	1	60 bytes	0	0 bytes	
✓ IPv6	11.27.184.32	2598	1	60 bytes	1	100.00%	1	60 bytes	0	0 bytes	
LEMP	11.72.226.252	48089	1	60 bytes	1	100.00%	1	60 bytes	0	0 bytes	
JXTA	11.29.235.4	42302	1	60 bytes	1	100.00%	1	60 bytes	0	0 bytes	
LTP	11.29.242.135	45190	1	60 bytes	1	100.00%	1	60 bytes	0	0 bytes	
Modem	11.30.72.96	64081	1	60 bytes	1	100.00%	1	60 bytes	0	0 bytes	
File filters for specific host	11.30.205.106	14144	1	60 bytes	1	100.00%	1	60 bytes	0	0 bytes	

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help											
Wireshark - Endpoints - file.pcap											
Endpoint Settings		Ethernet - 2 IPv4 - 37624 IPv6 TCP - 37670 UDP									
Name resolution		Address	Port	Packets	Bytes	Total Packets	Percent Filtered	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
✓ Limit to display filter		10.10.10.10	25565	37,841	2 MB	37,841	100.00%	0	0 bytes	37,841	2 MB
		112.124.85.108	49869	2	120 bytes	2	100.00%	2	120 bytes	0	0 bytes
		38.19.55.108	49467	2	120 bytes	2	100.00%	2	120 bytes	0	0 bytes
		80.194.243.3	38722	2	120 bytes	2	100.00%	2	120 bytes	0	0 bytes
		210.128.16.155	47300	2	120 bytes	2	100.00%	2	120 bytes	0	0 bytes
		46.182.118.170	18445	2	120 bytes	2	100.00%	2	120 bytes	0	0 bytes
		78.194.212.88	33669	2	120 bytes	2	100.00%	2	120 bytes	0	0 bytes
		39.218.67.47	59551	2	120 bytes	2	100.00%	2	120 bytes	0	0 bytes
Copy		121.242.222.159	37806	2	120 bytes	2	100.00%	2	120 bytes	0	0 bytes
Map		66.87.87.33	4278	2	120 bytes	2	100.00%	2	120 bytes	0	0 bytes
		105.230.193.203	22608	2	120 bytes	2	100.00%	2	120 bytes	0	0 bytes
		45.115.187.209	56984	2	120 bytes	2	100.00%	2	120 bytes	0	0 bytes
		187.83.180.252	46336	2	120 bytes	2	100.00%	2	120 bytes	0	0 bytes
		195.208.193.206	18888	2	120 bytes	2	100.00%	2	120 bytes	0	0 bytes
Protocol		120.107.127.106	64573	2	120 bytes	2	100.00%	2	120 bytes	0	0 bytes
Bluetooth		215.47.113.141	11486	2	120 bytes	2	100.00%	2	120 bytes	0	0 bytes
IPv6		205.77.208.240	14326	2	120 bytes	2	100.00%	2	120 bytes	0	0 bytes
✓ Ethernet		47.196.214.70	898	2	120 bytes	2	100.00%	2	120 bytes	0	0 bytes
FC		91.0.0.230	42018	2	120 bytes	2	100.00%	2	120 bytes	0	0 bytes
FD-01		154.38.65.45	5339	2	120 bytes	2	100.00%	2	120 bytes	0	0 bytes
IEEE 802.11		88.157.253.221	64793	2	120 bytes	2	100.00%	2	120 bytes	0	0 bytes
IEEE 802.15.4		134.163.84.63	3448	2	120 bytes	2	100.00%	2	120 bytes	0	0 bytes
✓ IPv4		123.26.51.213	14456	2	120 bytes	2	100.00%	2	120 bytes	0	0 bytes
IPv6		213.252.36.112	20214	2	120 bytes	2	100.00%	2	120 bytes	0	0 bytes
IPX		63.44.91.76	17589	2	120 bytes	2	100.00%	2	120 bytes	0	0 bytes
JXTA		83.187.177.179	21685	2	120 bytes	2	100.00%	2	120 bytes	0	0 bytes
LTP		126.69.200.137	39114	2	120 bytes	2	100.00%	2	120 bytes	0	0 bytes
Mnmp		158.215.254.169	52093	2	120 bytes	2	100.00%	2	120 bytes	0	0 bytes
		14.99.45.29	12421	2	120 bytes	2	100.00%	2	120 bytes	0	0 bytes
Filter list for specific type		26.72.235.96	37312	2	120 bytes	2	100.00%	2	120 bytes	0	0 bytes

Wireshark - Endpoints - file.pcap

tcp.flags.syn == 1 && tcp.flags.ack == 1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Note: Per review found there is only SYN and no ACK, SYN = 1 and ACK = 0

So as a conclusion the type of attacks are SYN flood (A **SYN flood** is a form of denial-of-service attack on data communications in which an attacker rapidly initiates a connection to a server without finalizing the connection. The server has to spend resources waiting for half-opened connections, which can consume enough resources to make the system unresponsive to legitimate traffic.).

Also, as my assumption found port scanning too. port scanning itself is not inherently an attack, it is a common technique used in malicious attacks .