NATIONAL UNIVERSITY OF SCIENCE AND TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE

INFORMATION SECURITY LAB

NAME	Ayesha Imran
Class	CS-A
Lab	OEL
Course	Information Security
Date	22-December-25
Submitted To	Lec. Attiya Ashraf

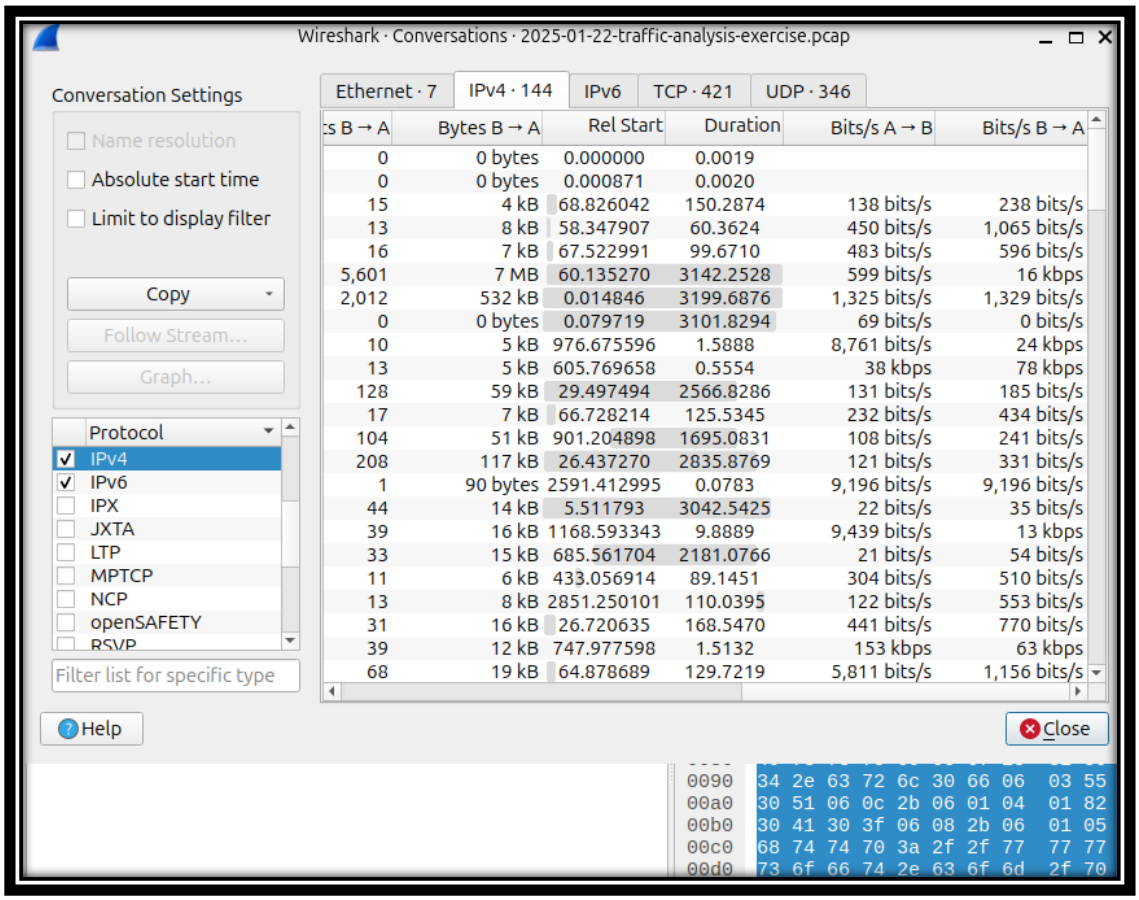
LAB TASKS

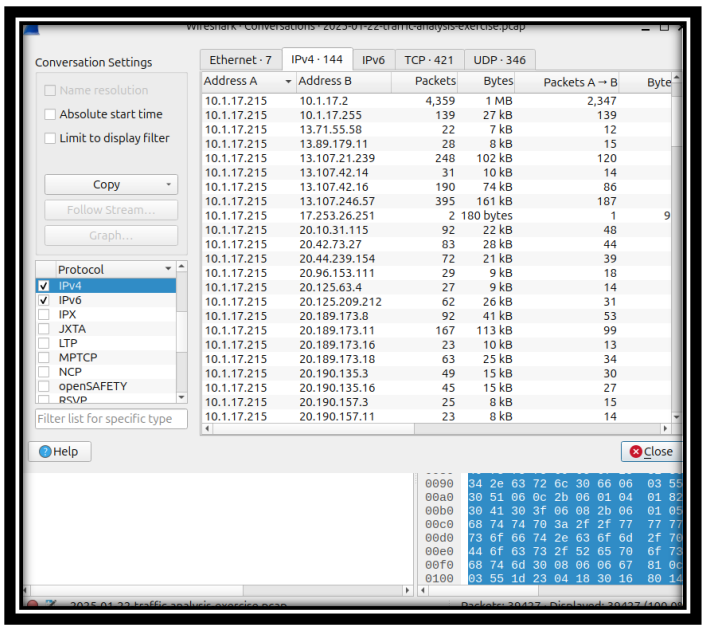
Tasks

Use Wireshark to answer the following questions about infected Windows client details:

1. IP address of the infected host

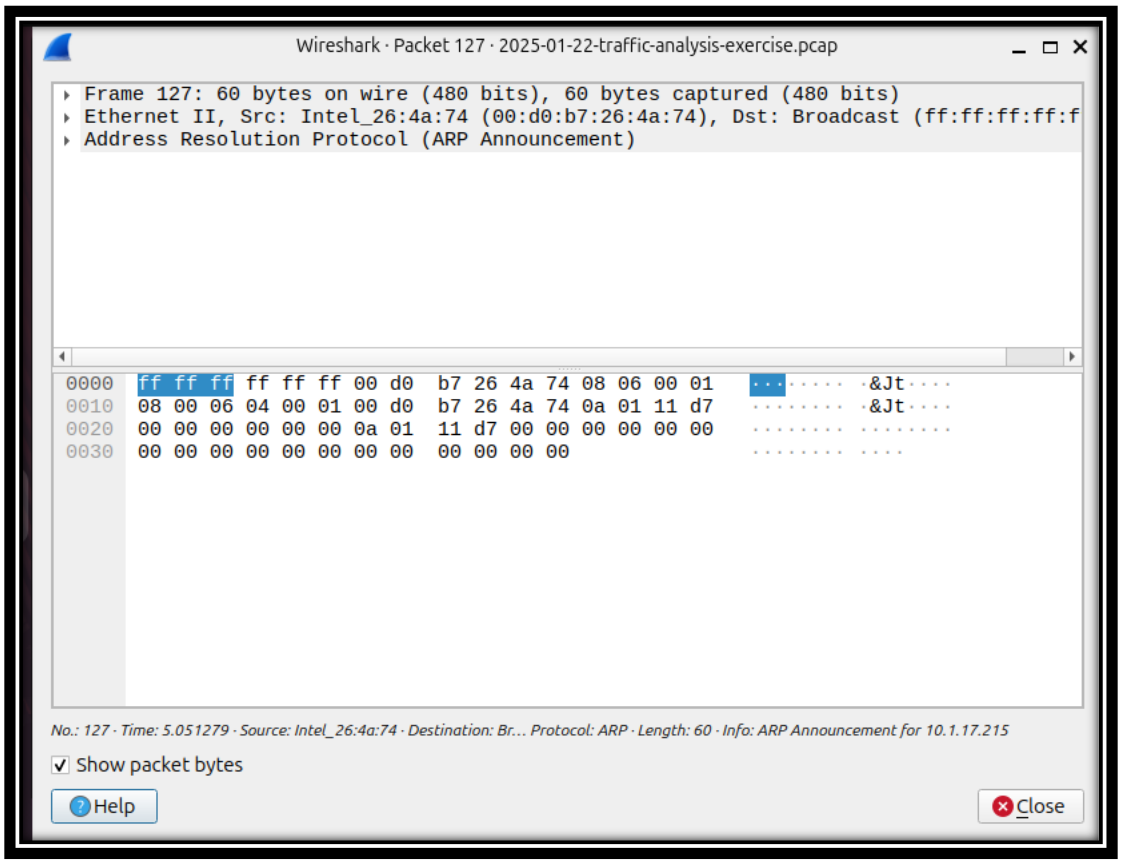
As the 10.1.17.215 has a very long session and transfering very long bytes so it seems as Infected host.





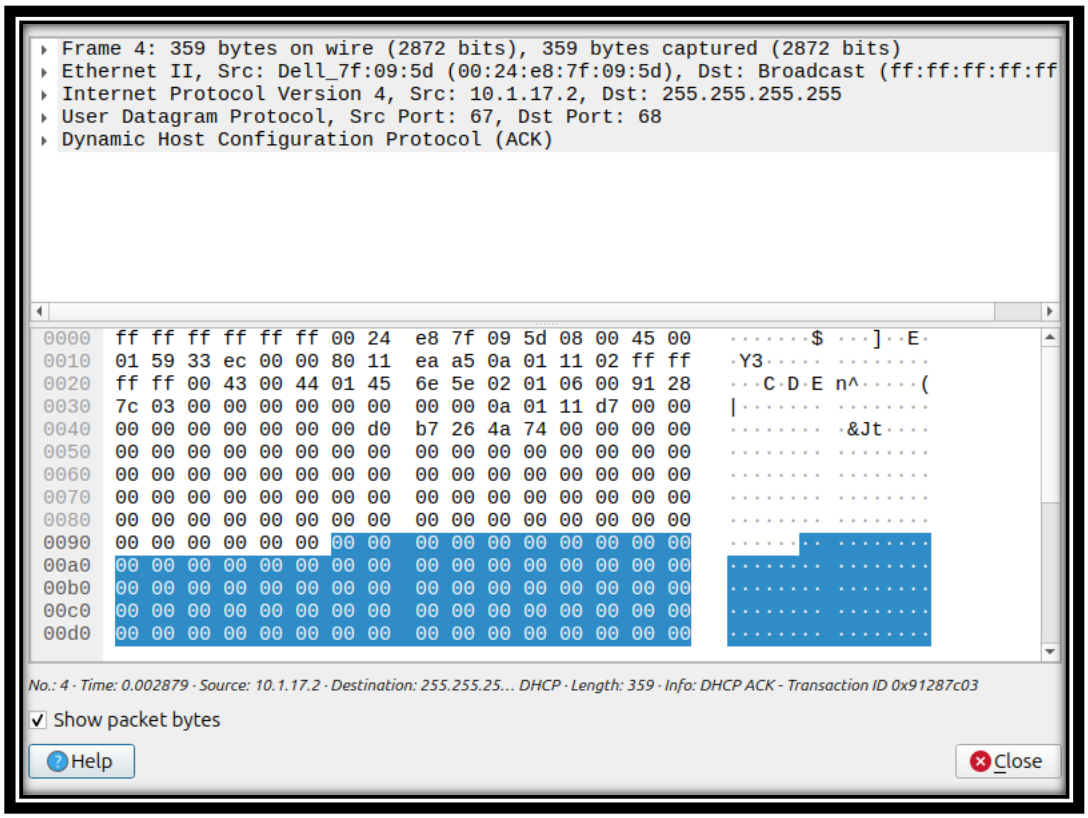
2. MAC address of the infected host

MAC Address = 00:d0:b7:26:4a:74 infected host

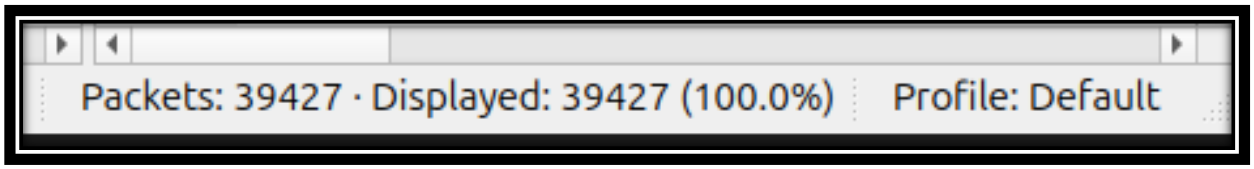


3. Hostname of the infected host

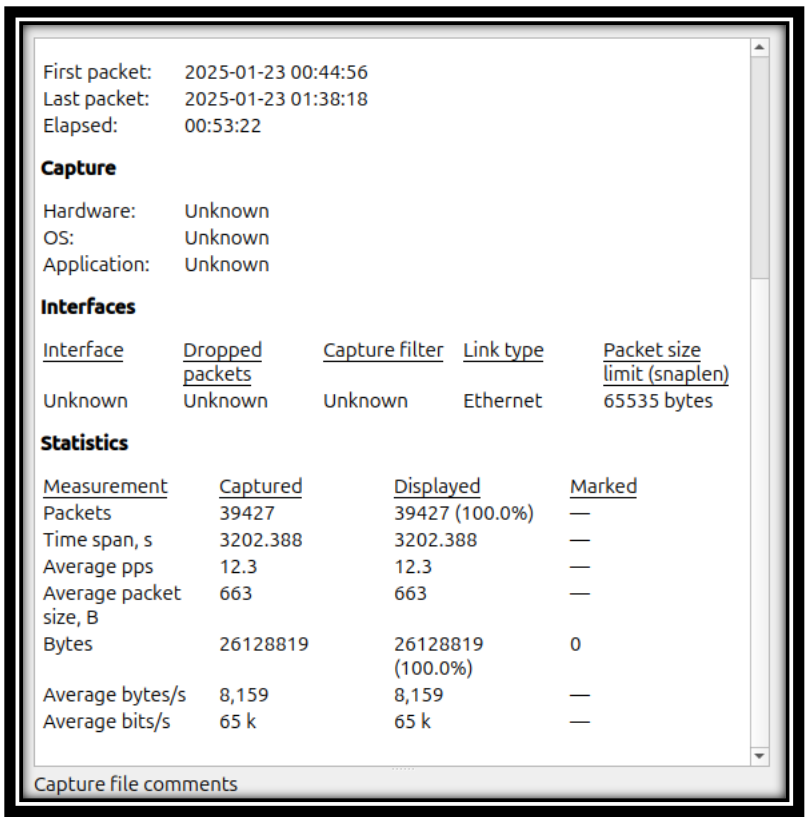
Host name : Dell_7f



Q1. How many packets are in the PCAP?



Q2. What is the capture duration?



First packet: 2025-01-23 00:44:56
Last packet: 2025-01-23 01:38:18
Elapsed: 00:53:22

Capture

Hardware: Unknown
OS: Unknown
Application: Unknown

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
Unknown	Unknown	Unknown	Ethernet	65535 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	39427	39427 (100.0%)	—
Time span, s	3202.388	3202.388	—
Average pps	12.3	12.3	—
Average packet size, B	663	663	—
Bytes	26128819	26128819 (100.0%)	0
Average bytes/s	8,159	8,159	—
Average bits/s	65 k	65 k	—

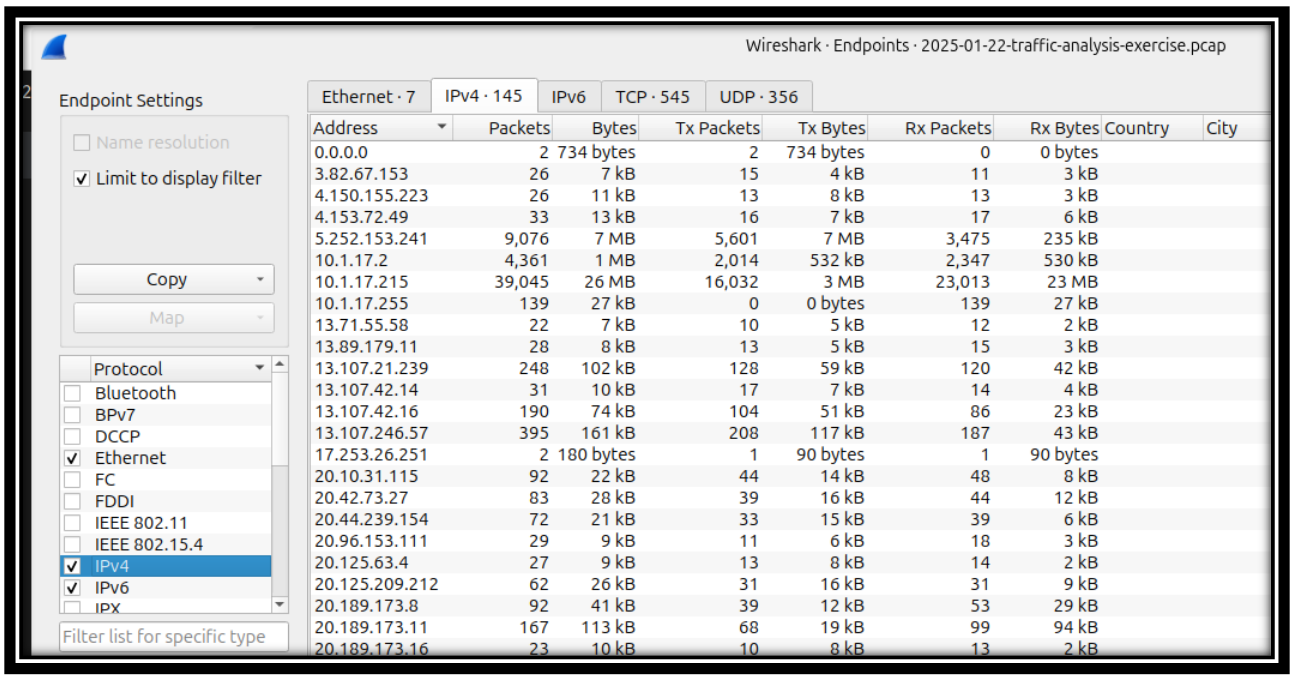
Capture file comments

Q3. What are the top 3 protocols seen in the capture?

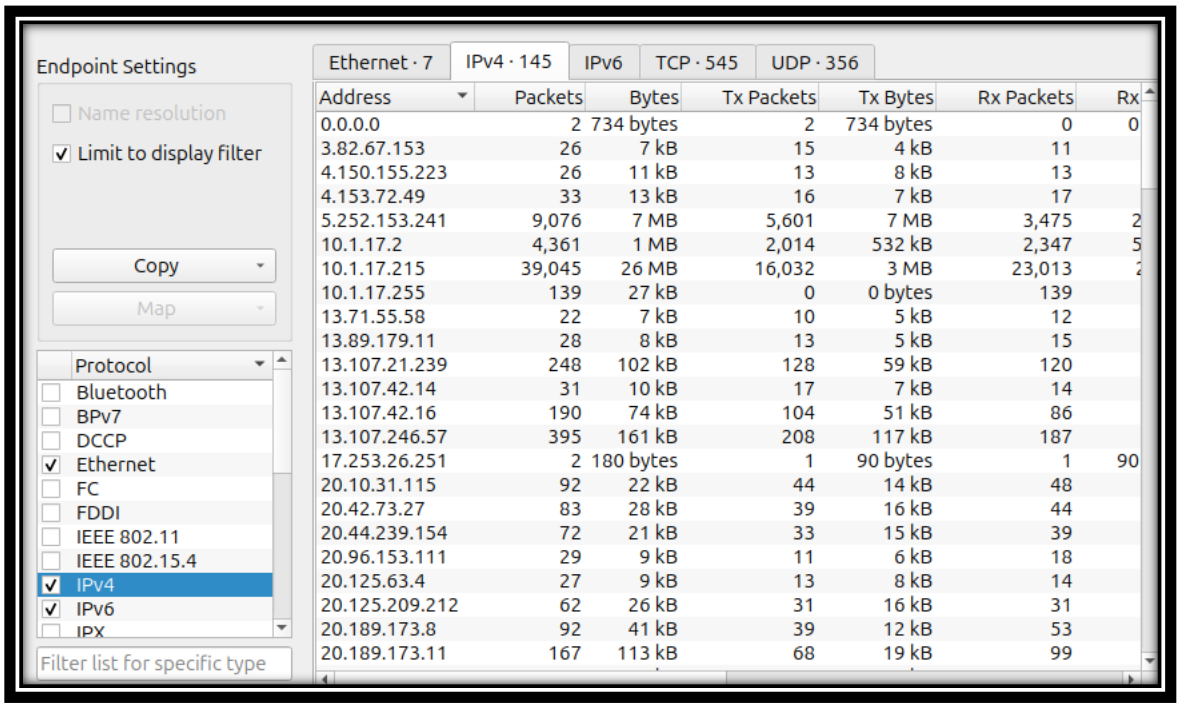
Protocol	Percent Packets	Packets
Frame	100.0	39427
Ethernet	100.0	39427
Internet Protocol Version 4	99.1	39087

Q4. How many unique IP addresses are present?

As we counted so these are approximately between 136-139 our counted value was 138.

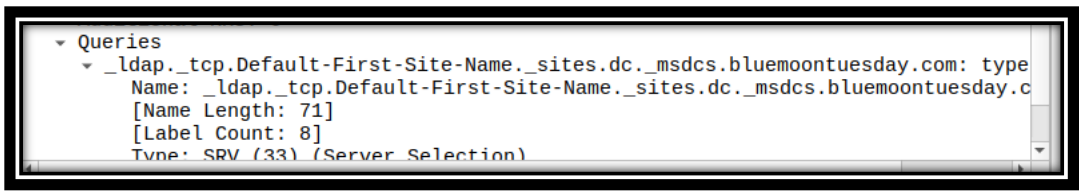


5. How many devices are active on the LAN?



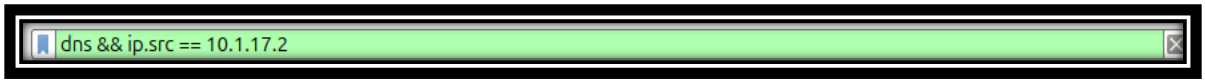
6. What was the first DNS query in the capture?

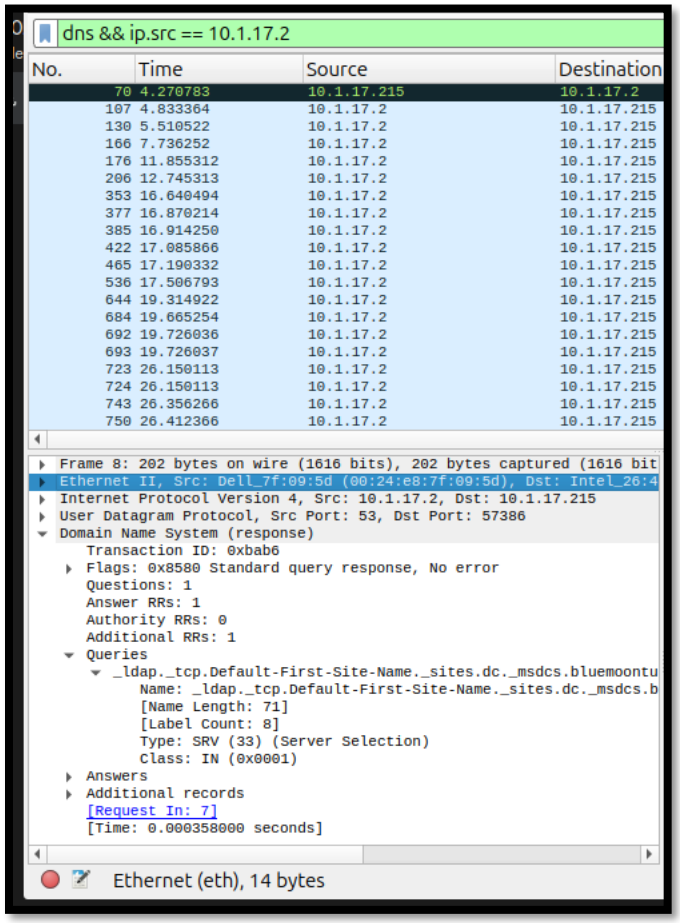
bluemoontuesday.com page was accessed firstly.



7. How many DNS queries were made by the infected host?

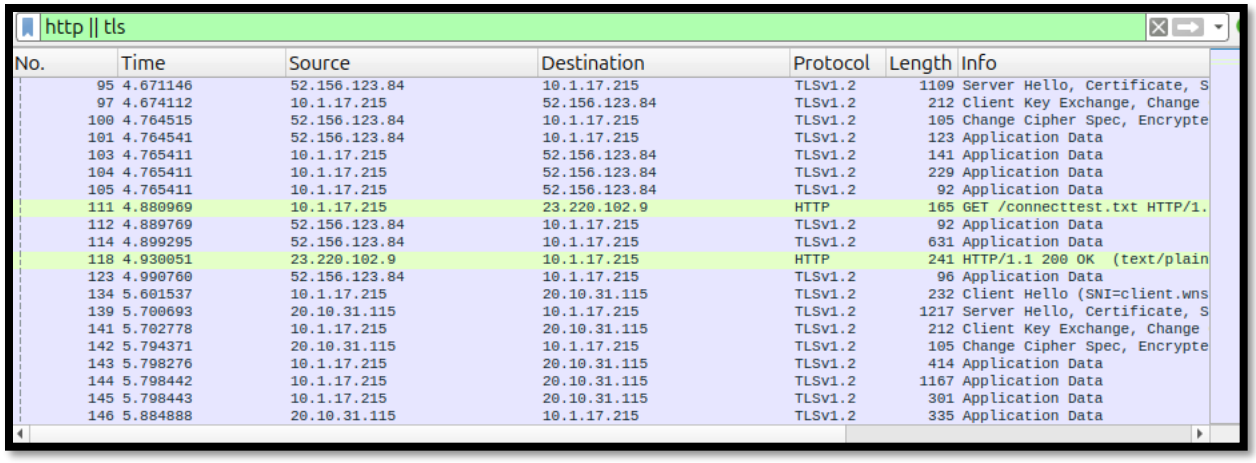
77 Queries were made by the host.





8. Was the suspicious website accessed over HTTP or HTTPS?

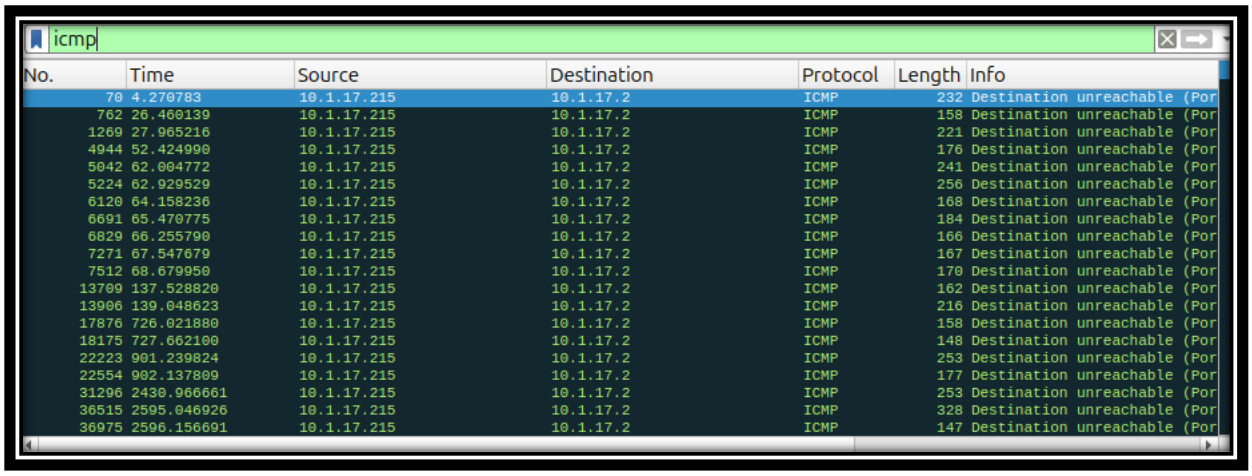
As the GET query shows that the website is accessed over http protocol



No.	Time	Source	Destination	Protocol	Length	Info
95	4.671146	52.156.123.84	10.1.17.215	TLSv1.2	1109	Server Hello, Certificate, S
97	4.674112	10.1.17.215	52.156.123.84	TLSv1.2	212	Client Key Exchange, Change
100	4.764515	52.156.123.84	10.1.17.215	TLSv1.2	105	Change Cipher Spec, Encrypte
101	4.764541	52.156.123.84	10.1.17.215	TLSv1.2	123	Application Data
103	4.765411	10.1.17.215	52.156.123.84	TLSv1.2	141	Application Data
104	4.765411	10.1.17.215	52.156.123.84	TLSv1.2	229	Application Data
105	4.765411	10.1.17.215	52.156.123.84	TLSv1.2	92	Application Data
111	4.880969	10.1.17.215	23.220.102.9	HTTP	165	GET /connecttest.txt HTTP/1.
112	4.889769	52.156.123.84	10.1.17.215	TLSv1.2	92	Application Data
114	4.899295	52.156.123.84	10.1.17.215	TLSv1.2	631	Application Data
118	4.930051	23.220.102.9	10.1.17.215	HTTP	241	HTTP/1.1 200 OK (text/plain
123	4.990760	52.156.123.84	10.1.17.215	TLSv1.2	96	Application Data
134	5.601537	10.1.17.215	20.10.31.115	TLSv1.2	232	Client Hello (SNI=client.wns
139	5.700693	20.10.31.115	10.1.17.215	TLSv1.2	1217	Server Hello, Certificate, S
141	5.702778	10.1.17.215	20.10.31.115	TLSv1.2	212	Client Key Exchange, Change
142	5.794371	20.10.31.115	10.1.17.215	TLSv1.2	105	Change Cipher Spec, Encrypte
143	5.798276	10.1.17.215	20.10.31.115	TLSv1.2	414	Application Data
144	5.798442	10.1.17.215	20.10.31.115	TLSv1.2	1167	Application Data
145	5.798443	10.1.17.215	20.10.31.115	TLSv1.2	301	Application Data
146	5.884888	20.10.31.115	10.1.17.215	TLSv1.2	335	Application Data

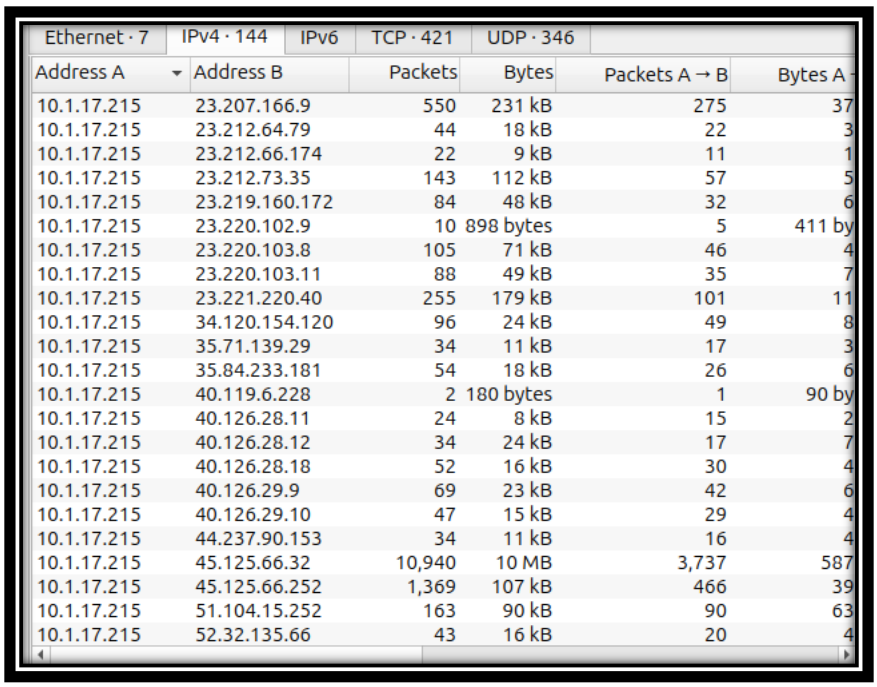
9. Are there any ICMP packets present?

Yes they are present.



No.	Time	Source	Destination	Protocol	Length	Info
70	4.270783	10.1.17.215	10.1.17.2	ICMP	232	Destination unreachable (Por
762	26.460139	10.1.17.215	10.1.17.2	ICMP	158	Destination unreachable (Por
1269	27.965216	10.1.17.215	10.1.17.2	ICMP	221	Destination unreachable (Por
4944	52.424990	10.1.17.215	10.1.17.2	ICMP	176	Destination unreachable (Por
5042	62.004772	10.1.17.215	10.1.17.2	ICMP	241	Destination unreachable (Por
5224	62.929529	10.1.17.215	10.1.17.2	ICMP	256	Destination unreachable (Por
6120	64.158236	10.1.17.215	10.1.17.2	ICMP	168	Destination unreachable (Por
6691	65.470775	10.1.17.215	10.1.17.2	ICMP	184	Destination unreachable (Por
6829	66.255790	10.1.17.215	10.1.17.2	ICMP	166	Destination unreachable (Por
7271	67.547679	10.1.17.215	10.1.17.2	ICMP	167	Destination unreachable (Por
7512	68.679950	10.1.17.215	10.1.17.2	ICMP	170	Destination unreachable (Por
13709	137.528820	10.1.17.215	10.1.17.2	ICMP	162	Destination unreachable (Por
13906	139.048623	10.1.17.215	10.1.17.2	ICMP	216	Destination unreachable (Por
17876	726.021880	10.1.17.215	10.1.17.2	ICMP	158	Destination unreachable (Por
18175	727.662100	10.1.17.215	10.1.17.2	ICMP	148	Destination unreachable (Por
22223	901.239824	10.1.17.215	10.1.17.2	ICMP	253	Destination unreachable (Por
22554	902.137809	10.1.17.215	10.1.17.2	ICMP	177	Destination unreachable (Por
31296	2430.966661	10.1.17.215	10.1.17.2	ICMP	253	Destination unreachable (Por
36515	2595.046926	10.1.17.215	10.1.17.2	ICMP	328	Destination unreachable (Por
36975	2596.156691	10.1.17.215	10.1.17.2	ICMP	147	Destination unreachable (Por

10. Does the infected host communicate with more internal or external IPs?



Ethernet · 7	IPv4 · 144	IPv6	TCP · 421	UDP · 346		
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A	
10.1.17.215	23.207.166.9	550	231 kB	275	37	
10.1.17.215	23.212.64.79	44	18 kB	22	3	
10.1.17.215	23.212.66.174	22	9 kB	11	1	
10.1.17.215	23.212.73.35	143	112 kB	57	5	
10.1.17.215	23.219.160.172	84	48 kB	32	6	
10.1.17.215	23.220.102.9	10	898 bytes	5	411 by	
10.1.17.215	23.220.103.8	105	71 kB	46	4	
10.1.17.215	23.220.103.11	88	49 kB	35	7	
10.1.17.215	23.221.220.40	255	179 kB	101	11	
10.1.17.215	34.120.154.120	96	24 kB	49	8	
10.1.17.215	35.71.139.29	34	11 kB	17	3	
10.1.17.215	35.84.233.181	54	18 kB	26	6	
10.1.17.215	40.119.6.228	2	180 bytes	1	90 by	
10.1.17.215	40.126.28.11	24	8 kB	15	2	
10.1.17.215	40.126.28.12	34	24 kB	17	7	
10.1.17.215	40.126.28.18	52	16 kB	30	4	
10.1.17.215	40.126.29.9	69	23 kB	42	6	
10.1.17.215	40.126.29.10	47	15 kB	29	4	
10.1.17.215	44.237.90.153	34	11 kB	16	4	
10.1.17.215	45.125.66.32	10,940	10 MB	3,737	587	
10.1.17.215	45.125.66.252	1,369	107 kB	466	39	
10.1.17.215	51.104.15.252	163	90 kB	90	63	
10.1.17.215	52.32.135.66	43	16 kB	20	4	

External IPs.

The infected host 10.1.17.215 communicates with many public IPs such as 23.212.66.174, 23.207.166.9, 45.125.66.252, 52.32.135.66, and others with high packet counts and large data volumes (e.g., 7 MB, 514 kB, 261 kB). Internal IPs are fewer and mostly local

1. Table of Findings

Item	Value	Source Packet/Method
Infected Host IP	`10.1.17.215`	DHCP ACK / High outbound traffic
Infected Host MAC Address	`Dell_7f:09:5d`	ARP Reply
Infected Host Hostname	`SFC./wyyfl`	DHCP Option: Hostname
External Communication Count	20+ external IPs	Endpoint/IP stats
Largest Data Exchange	`5.252.153.241`	7 MB outbound, 235 kB inbound

3. Description of the Infection (Your Words)

The infected Windows client (`10.1.17.215`) shows signs of compromise due to excessive outbound traffic to multiple external IPs, especially `5.252.153.241`. The volume and persistence of these connections suggest possible data exfiltration or command-and-control activity. The hostname `SFC./wyyfl` appears suspicious and may be spoofed or malware-generated.

---

4. Incident Summary

Timeline:

- **0.000s**: DHCP Discover initiated
- **0.002s**: IP assigned via DHCP ACK
- **0.014s onward**: ARP and DNS activity begins
- **~60s onward**: High-volume external communication starts
- **Duration**: Over 3100 seconds of sustained traffic

Recommended Next Steps:

- Isolate host `10.1.17.215` from the network
- Perform full malware scan and forensic disk analysis
- Review firewall and proxy logs for external IPs
- Block known malicious IPs (e.g., `5.252.153.241`)
- Reset credentials and monitor for lateral movement
