



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 transferring very long bytes so it seems as Infected host.

Wireshark · Conversations · 2025-01-22-traffic-analysis-exercise.pcap

Conversation Settings

- ☐ Name resolution
- ☐ Absolute start time
- ☐ Limit to display filter
- Copy
- Follow Stream...
- Graph...

Protocol

- ☒ IPv4
- ☒ IPv6
- ☐ IPX
- ☐ JXTA
- ☐ LTP
- ☐ MPTCP
- ☐ NCP
- ☐ openSAFETY
- ☐ RSVP

Filter list for specific type

Help

| Bytes B → A | Bytes B → A | Rel Start | Duration | Bits/s A → B | Bits/s B → A |
|-------------|-------------|-------------|-----------|--------------|--------------|
| 0 | 0 bytes | 0.000000 | 0.0019 | | |
| 0 | 0 bytes | 0.000871 | 0.0020 | | |
| 15 | 4 kB | 68.826042 | 150.2874 | 138 bits/s | 238 bits/s |
| 13 | 8 kB | 58.347907 | 60.3624 | 450 bits/s | 1,065 bits/s |
| 16 | 7 kB | 67.522991 | 99.6710 | 483 bits/s | 596 bits/s |
| 5,601 | 7 MB | 60.135270 | 3142.2528 | 599 bits/s | 16 kbps |
| 2,012 | 532 kB | 0.014846 | 3199.6876 | 1,325 bits/s | 1,329 bits/s |
| 0 | 0 bytes | 0.079719 | 3101.8294 | 69 bits/s | 0 bits/s |
| 10 | 5 kB | 976.675596 | 1.5888 | 8,761 bits/s | 24 kbps |
| 13 | 5 kB | 605.769658 | 0.5554 | 38 kbps | 78 kbps |
| 128 | 59 kB | 29.497494 | 2566.8286 | 131 bits/s | 185 bits/s |
| 17 | 7 kB | 66.728214 | 125.5345 | 232 bits/s | 434 bits/s |
| 104 | 51 kB | 901.204898 | 1695.0831 | 108 bits/s | 241 bits/s |
| 208 | 117 kB | 26.437270 | 2835.8769 | 121 bits/s | 331 bits/s |
| 1 | 90 bytes | 2591.412995 | 0.0783 | 9,196 bits/s | 9,196 bits/s |
| 44 | 14 kB | 5.511793 | 3042.5425 | 22 bits/s | 35 bits/s |
| 39 | 16 kB | 1168.593343 | 9.8889 | 9,439 bits/s | 13 kbps |
| 33 | 15 kB | 685.561704 | 2181.0766 | 21 bits/s | 54 bits/s |
| 11 | 6 kB | 433.056914 | 89.1451 | 304 bits/s | 510 bits/s |
| 13 | 8 kB | 2851.250101 | 110.0395 | 122 bits/s | 553 bits/s |
| 31 | 16 kB | 26.720635 | 168.5470 | 441 bits/s | 770 bits/s |
| 39 | 12 kB | 747.977598 | 1.5132 | 153 kbps | 63 kbps |
| 68 | 19 kB | 64.878689 | 129.7219 | 5,811 bits/s | 1,156 bits/s |

0090 34 2e 63 72 6c 30 66 06 03 55

00a0 30 51 06 0c 2b 06 01 04 01 82

00b0 30 41 30 3f 06 08 2b 06 01 05

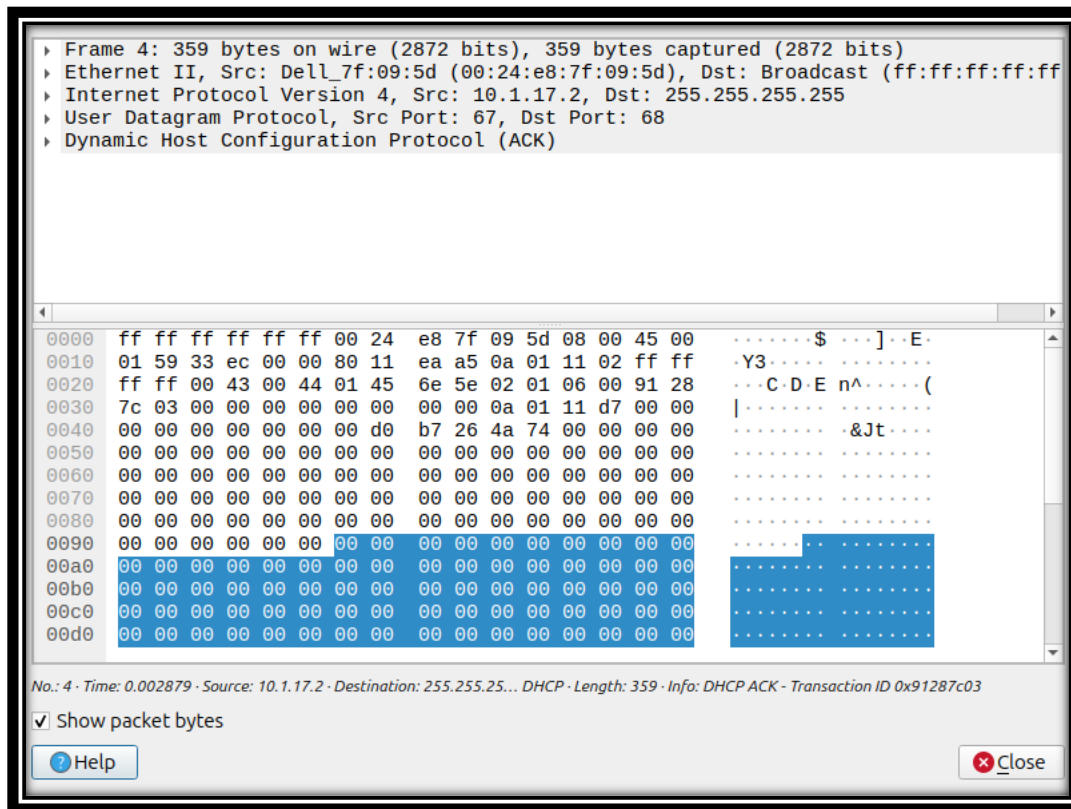
00c0 68 74 74 70 3a 2f 2f 77 77 77

00d0 73 6f 66 74 2e 63 6f 6d 2f 70

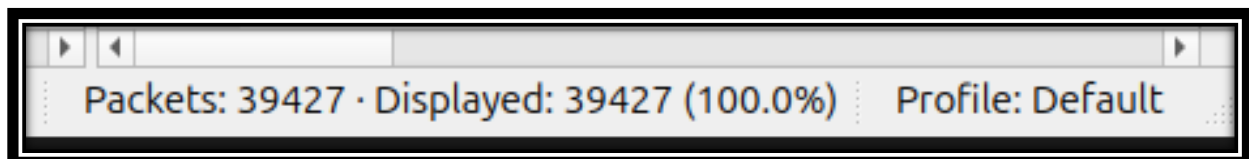
Close

3. Hostname of the infected host

Host name : Dell_7f



Q1. How many packets are in the PCAP?



Q2. What is the capture duration?

Wireshark · Endpoints · 2025-01-22-traffic-analysis-exercise.pcap

Endpoint Settings

☐ Name resolution

☒ Limit to display filter

Copy

Map

Protocol

☐ Bluetooth

☐ BPv7

☐ DCCP

☒ Ethernet

☐ FC

☐ FDDI

☐ IEEE 802.11

☐ IEEE 802.15.4

☒ IPv4

☒ IPv6

☐ IPX

Filter list for specific type

| Address | Packets | Bytes | Tx Packets | Tx Bytes | Rx Packets | Rx Bytes | Country | City |
|----------------|---------|-----------|------------|-----------|------------|----------|---------|------|
| 0.0.0.0 | 2 | 734 bytes | 2 | 734 bytes | 0 | 0 bytes | | |
| 3.82.67.153 | 26 | 7 kB | 15 | 4 kB | 11 | 3 kB | | |
| 4.150.155.223 | 26 | 11 kB | 13 | 8 kB | 13 | 3 kB | | |
| 4.153.72.49 | 33 | 13 kB | 16 | 7 kB | 17 | 6 kB | | |
| 5.252.153.241 | 9,076 | 7 MB | 5,601 | 7 MB | 3,475 | 235 kB | | |
| 10.1.17.2 | 4,361 | 1 MB | 2,014 | 532 kB | 2,347 | 530 kB | | |
| 10.1.17.215 | 39,045 | 26 MB | 16,032 | 3 MB | 23,013 | 23 MB | | |
| 10.1.17.255 | 139 | 27 kB | 0 | 0 bytes | 139 | 27 kB | | |
| 13.71.55.58 | 22 | 7 kB | 10 | 5 kB | 12 | 2 kB | | |
| 13.89.179.11 | 28 | 8 kB | 13 | 5 kB | 15 | 3 kB | | |
| 13.107.21.239 | 248 | 102 kB | 128 | 59 kB | 120 | 42 kB | | |
| 13.107.42.14 | 31 | 10 kB | 17 | 7 kB | 14 | 4 kB | | |
| 13.107.42.16 | 190 | 74 kB | 104 | 51 kB | 86 | 23 kB | | |
| 13.107.246.57 | 395 | 161 kB | 208 | 117 kB | 187 | 43 kB | | |
| 17.253.26.251 | 2 | 180 bytes | 1 | 90 bytes | 1 | 90 bytes | | |
| 20.10.31.115 | 92 | 22 kB | 44 | 14 kB | 48 | 8 kB | | |
| 20.42.73.27 | 83 | 28 kB | 39 | 16 kB | 44 | 12 kB | | |
| 20.44.239.154 | 72 | 21 kB | 33 | 15 kB | 39 | 6 kB | | |
| 20.96.153.111 | 29 | 9 kB | 11 | 6 kB | 18 | 3 kB | | |
| 20.125.63.4 | 27 | 9 kB | 13 | 8 kB | 14 | 2 kB | | |
| 20.125.209.212 | 62 | 26 kB | 31 | 16 kB | 31 | 9 kB | | |
| 20.189.173.8 | 92 | 41 kB | 39 | 12 kB | 53 | 29 kB | | |
| 20.189.173.11 | 167 | 113 kB | 68 | 19 kB | 99 | 94 kB | | |
| 20.189.173.16 | 23 | 10 kB | 10 | 8 kB | 13 | 2 kB | | |

5. How many devices are active on the LAN?

Endpoint Settings

☐ Name resolution

☒ Limit to display filter

Copy

Map

Protocol

☐ Bluetooth

☐ BPv7

☐ DCCP

☒ Ethernet

☐ FC

☐ FDDI

☐ IEEE 802.11

☐ IEEE 802.15.4

☒ IPv4

☒ IPv6

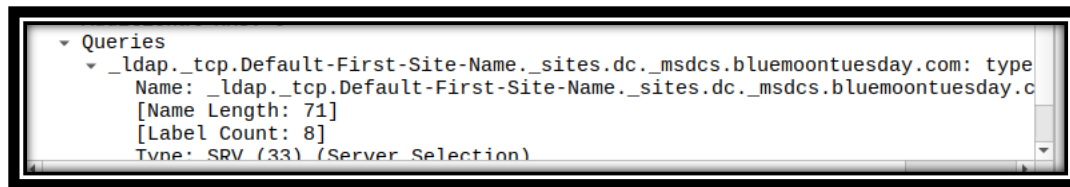
☐ IPX

Filter list for specific type

| Address | Packets | Bytes | Tx Packets | Tx Bytes | Rx Packets | Rx Bytes |
|----------------|---------|-----------|------------|-----------|------------|----------|
| 0.0.0.0 | 2 | 734 bytes | 2 | 734 bytes | 0 | 0 |
| 3.82.67.153 | 26 | 7 kB | 15 | 4 kB | 11 | 3 kB |
| 4.150.155.223 | 26 | 11 kB | 13 | 8 kB | 13 | 3 kB |
| 4.153.72.49 | 33 | 13 kB | 16 | 7 kB | 17 | 6 kB |
| 5.252.153.241 | 9,076 | 7 MB | 5,601 | 7 MB | 3,475 | 235 kB |
| 10.1.17.2 | 4,361 | 1 MB | 2,014 | 532 kB | 2,347 | 530 kB |
| 10.1.17.215 | 39,045 | 26 MB | 16,032 | 3 MB | 23,013 | 23 MB |
| 10.1.17.255 | 139 | 27 kB | 0 | 0 bytes | 139 | 27 kB |
| 13.71.55.58 | 22 | 7 kB | 10 | 5 kB | 12 | 2 kB |
| 13.89.179.11 | 28 | 8 kB | 13 | 5 kB | 15 | 3 kB |
| 13.107.21.239 | 248 | 102 kB | 128 | 59 kB | 120 | 42 kB |
| 13.107.42.14 | 31 | 10 kB | 17 | 7 kB | 14 | 4 kB |
| 13.107.42.16 | 190 | 74 kB | 104 | 51 kB | 86 | 23 kB |
| 13.107.246.57 | 395 | 161 kB | 208 | 117 kB | 187 | 43 kB |
| 17.253.26.251 | 2 | 180 bytes | 1 | 90 bytes | 1 | 90 bytes |
| 20.10.31.115 | 92 | 22 kB | 44 | 14 kB | 48 | 8 kB |
| 20.42.73.27 | 83 | 28 kB | 39 | 16 kB | 44 | 12 kB |
| 20.44.239.154 | 72 | 21 kB | 33 | 15 kB | 39 | 6 kB |
| 20.96.153.111 | 29 | 9 kB | 11 | 6 kB | 18 | 3 kB |
| 20.125.63.4 | 27 | 9 kB | 13 | 8 kB | 14 | 2 kB |
| 20.125.209.212 | 62 | 26 kB | 31 | 16 kB | 31 | 9 kB |
| 20.189.173.8 | 92 | 41 kB | 39 | 12 kB | 53 | 29 kB |
| 20.189.173.11 | 167 | 113 kB | 68 | 19 kB | 99 | 94 kB |

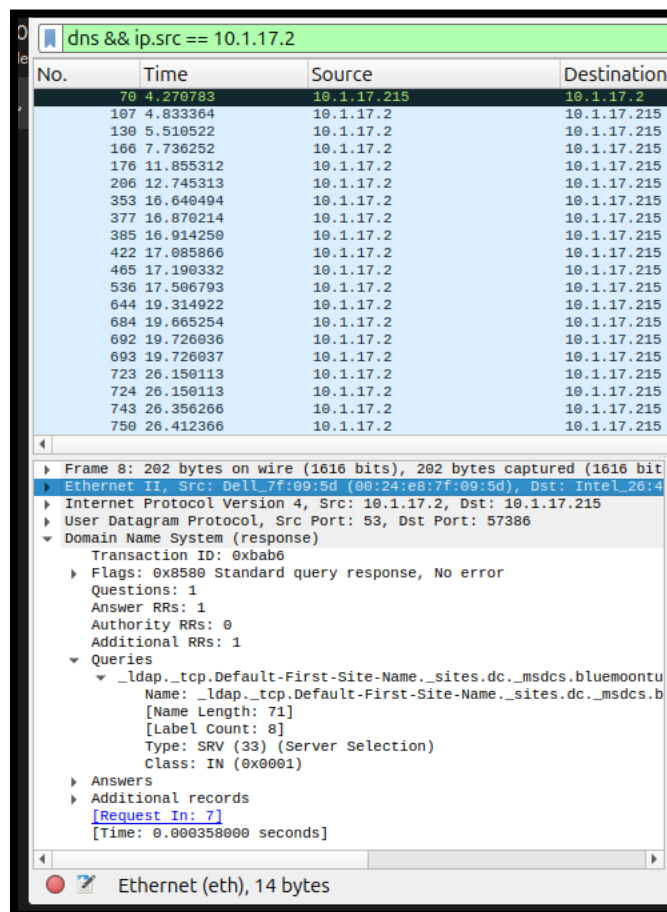
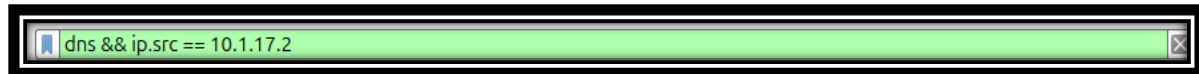
6. What was the first DNS query in the capture?

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

| http tls | | | | | | |
|-------------|----------|---------------|---------------|----------|--------|------------------------------|
| 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 | 4.880909 | 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 | 391 | 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.

| icmp | | | | | | |
|-------|-------------|-------------|-------------|----------|--------|------------------------------|
| 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 |
| 4044 | 52.424900 | 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 | 179 | 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 | 2596.156601 | 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 → B |
| 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
-