



## **NATIONAL UNIVERSITY OF SCIENCE AND TECHNOLOGY**

### **DEPARTMENT OF COMPUTER SCIENCE**

#### **INFORMATION SECURITY LAB**

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

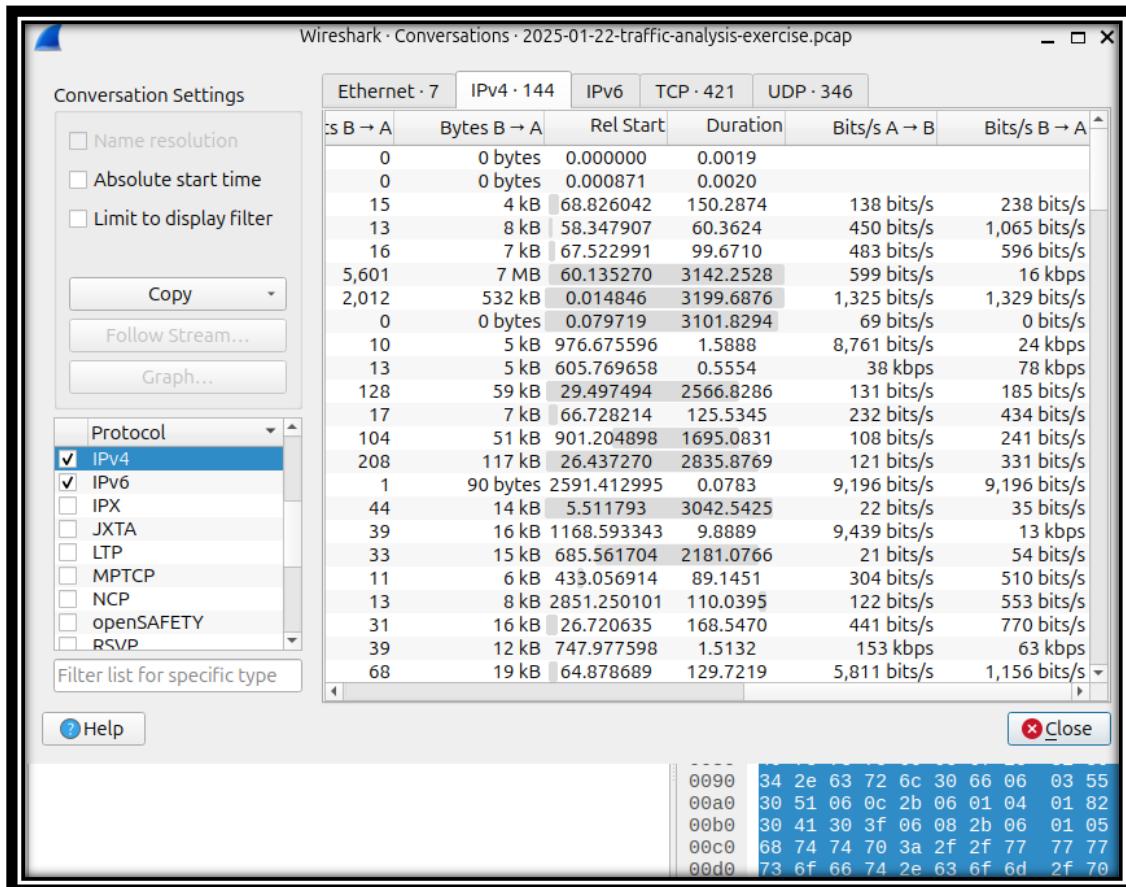
# LAB TASKS

## 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

Address A	Address B	Packets	Bytes	Packets A → B	Bytes
10.1.17.215	10.1.17.2	4,359	1 MB	2,347	
10.1.17.215	10.1.17.255	139	27 kB	139	
10.1.17.215	13.71.55.58	22	7 kB	12	
10.1.17.215	13.89.179.11	28	8 kB	15	
10.1.17.215	13.107.21.239	248	102 kB	120	
10.1.17.215	13.107.42.14	31	10 kB	14	
10.1.17.215	13.107.42.16	190	74 kB	86	
10.1.17.215	13.107.246.57	395	161 kB	187	
10.1.17.215	17.253.26.251	2	180 bytes	1	9
10.1.17.215	20.10.31.115	92	22 kB	48	
10.1.17.215	20.42.73.27	83	28 kB	44	
10.1.17.215	20.44.239.154	72	21 kB	39	
10.1.17.215	20.96.153.111	29	9 kB	18	
10.1.17.215	20.125.63.4	27	9 kB	14	
10.1.17.215	20.125.209.212	62	26 kB	31	
10.1.17.215	20.189.173.8	92	41 kB	53	
10.1.17.215	20.189.173.11	167	113 kB	99	
10.1.17.215	20.189.173.16	23	10 kB	13	
10.1.17.215	20.189.173.18	63	25 kB	34	
10.1.17.215	20.190.135.3	49	15 kB	30	
10.1.17.215	20.190.135.16	45	15 kB	27	
10.1.17.215	20.190.157.3	25	8 kB	15	
10.1.17.215	20.190.157.11	23	8 kB	14	

Help Close

## 2. MAC address of the infected host

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

Wireshark - Packet 127 · 2025-01-22-traffic-analysis-exercise.pcap

Frame 127: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)  
Ethernet II, Src: Intel\_26:4a:74 (00:d0:b7:26:4a:74), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
Address Resolution Protocol (ARP Announcement)

0000	ff ff ff ff ff ff 00 d0 b7 26 4a 74 08 06 00 01	.....&Jt.....
0010	08 00 06 04 00 01 00 d0 b7 26 4a 74 0a 01 11 d7	.....&Jt.....
0020	00 00 00 00 00 00 0a 01 11 d7 00 00 00 00 00 00	.....
0030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....

No.: 127 · Time: 5.051279 · Source: Intel\_26:4a:74 · Destination: Br... · Protocol: ARP · Length: 60 · Info: ARP Announcement for 10.1.17.215

Show packet bytes  
Help Close

### 3. Hostname of the infected host

Host name : Dell\_7f

```
> Frame 4: 359 bytes on wire (2872 bits), 359 bytes captured (2872 bits)
> Ethernet II, Src: Dell_7f:09:5d (00:24:e8:7f:09:5d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 10.1.17.2, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 67, Dst Port: 68
> Dynamic Host Configuration Protocol (ACK)



|      |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |                  |     |
|------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|------------------|-----|
| 0000 | ff | ff | ff | ff | ff | ff | 00 | 24 | e8 | 7f | 09 | 5d | 08 | 00 | 45 | 00 | .....\$...]      | E.. |
| 0010 | 01 | 59 | 33 | ec | 00 | 00 | 80 | 11 | ea | a5 | 0a | 01 | 11 | 02 | ff | ff | Y3.....          |     |
| 0020 | ff | ff | 00 | 43 | 00 | 44 | 01 | 45 | 6e | 5e | 02 | 01 | 06 | 00 | 91 | 28 | ..C-D-E n^.....( |     |
| 0030 | 7c | 03 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 0a | 01 | 11 | d7 | 00 | 00 | .....            |     |
| 0040 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | d0 | b7 | 26 | 4a | 74 | 00 | 00 | 00 | 00 | .....&Jt.....    |     |
| 0050 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....            |     |
| 0060 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....            |     |
| 0070 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....            |     |
| 0080 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....            |     |
| 0090 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....            |     |
| 00a0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....            |     |
| 00b0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....            |     |
| 00c0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....            |     |
| 00d0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .....            |     |



No.: 4 · Time: 0.002879 · Source: 10.1.17.2 · Destination: 255.255.255.255 · DHCP · Length: 359 · Info: DHCP ACK - Transaction ID 0x91287c03



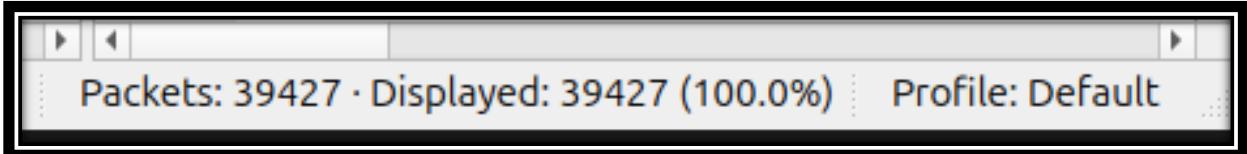
Show packet bytes



 Help  Close


```

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			
<b>Capture</b>				
Hardware:	Unknown			
OS:	Unknown			
Application:	Unknown			
<b>Interfaces</b>				
Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
Unknown	Unknown	Unknown	Ethernet	65535 bytes
<b>Statistics</b>				
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.

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

2 Endpoint Settings

Ethernet · 7 IPv4 · 145 IPv6 TCP · 545 UDP · 356								
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City
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?

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

2 Endpoint Settings

Ethernet · 7 IPv4 · 145 IPv6 TCP · 545 UDP · 356							
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	
0.0.0	2	734 bytes	2	734 bytes	0	0	
3.82.67.153	26	7 kB	15	4 kB	11		
4.150.155.223	26	11 kB	13	8 kB	13		
4.153.72.49	33	13 kB	16	7 kB	17		
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		
13.71.55.58	22	7 kB	10	5 kB	12		
13.89.179.11	28	8 kB	13	5 kB	15		
13.107.21.239	248	102 kB	128	59 kB	120		
13.107.42.14	31	10 kB	17	7 kB	14		
13.107.42.16	190	74 kB	104	51 kB	86		
13.107.246.57	395	161 kB	208	117 kB	187		
17.253.26.251	2	180 bytes	1	90 bytes	1	90 bytes	
20.10.31.115	92	22 kB	44	14 kB	48		
20.42.73.27	83	28 kB	39	16 kB	44		
20.44.239.154	72	21 kB	33	15 kB	39		
20.96.153.111	29	9 kB	11	6 kB	18		
20.125.63.4	27	9 kB	13	8 kB	14		
20.125.209.212	62	26 kB	31	16 kB	31		
20.189.173.8	92	41 kB	39	12 kB	53		
20.189.173.11	167	113 kB	68	19 kB	99		
20.189.173.16	23	10 kB	10	8 kB	13		

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

bluemontuesday.com page was accessed firstly.

```

    ▾ Queries
      ▾ _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.bluemoontuesday.com: type
        Name: _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.bluemoontuesday.c
        [Name Length: 71]
        [Label Count: 8]
        Type: SRV (33) (Server Selection)

```

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

77 Queries were made by the host.

**dns && ip.src == 10.1.17.2**

No.	Time	Source	Destination
70	4.270783	10.1.17.215	10.1.17.2
107	4.833364	10.1.17.2	10.1.17.215
138	5.510522	10.1.17.2	10.1.17.215
166	7.736252	10.1.17.2	10.1.17.215
176	11.855312	10.1.17.2	10.1.17.215
206	12.745313	10.1.17.2	10.1.17.215
353	16.640494	10.1.17.2	10.1.17.215
377	16.870214	10.1.17.2	10.1.17.215
385	16.914250	10.1.17.2	10.1.17.215
422	17.085866	10.1.17.2	10.1.17.215
465	17.190332	10.1.17.2	10.1.17.215
536	17.506793	10.1.17.2	10.1.17.215
644	19.314922	10.1.17.2	10.1.17.215
684	19.665254	10.1.17.2	10.1.17.215
692	19.726636	10.1.17.2	10.1.17.215
693	19.726637	10.1.17.2	10.1.17.215
723	26.150113	10.1.17.2	10.1.17.215
724	26.150113	10.1.17.2	10.1.17.215
743	26.356266	10.1.17.2	10.1.17.215
750	26.412366	10.1.17.2	10.1.17.215

Frame 8: 202 bytes on wire (1616 bits), 202 bytes captured (1616 bits)  
 Ethernet II, Src: Dell\_7f:09:5d (00:24:e8:7f:09:5d), Dst: Intel\_26:4  
 Internet Protocol Version 4, Src: 10.1.17.2, Dst: 10.1.17.215  
 User Datagram Protocol, Src Port: 53, Dst Port: 57386  
 Domain Name System (response)  
 Transaction ID: 0xbab6  
 Flags: 0x8580 Standard query response, No error  
 Questions: 1  
 Answer RRs: 1  
 Authority RRs: 0  
 Additional RRs: 1  
 Queries  
 ▾ \_ldap.\_tcp.Default-First-Site-Name.\_sites.dc.\_msdcs.bluemoontuesday.com: type  
 Name: \_ldap.\_tcp.Default-First-Site-Name.\_sites.dc.\_msdcs.bluemoontuesday.com  
 [Name Length: 71]  
 [Label Count: 8]  
 Type: SRV (33) (Server Selection)  
 Class: IN (0x0001)  
 Answers  
 Additional records  
 [Request In: 7]  
 [Time: 0.000358000 seconds]

Ethernet (eth), 14 bytes

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	381	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	62.029529	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
31206	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 → 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 bytes	
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 bytes	
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
<b>Infected Host IP</b>	10.1.17.215	DHCP ACK / High outbound traffic
<b>Infected Host MAC Address</b>	Dell_7f:09:5d	ARP Reply
<b>Infected Host Hostname</b>	SFC./wyffyfl	DHCP Option: Hostname
<b>External Communication Count</b>	20+ external IPs	Endpoint/IP stats
<b>Largest Data Exchange</b>	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./wyff1 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
-