Capstone Project: Wireshark Traffic Analysis-Malicious Download from a Fake Software Site

Incident Report of my Capstone Project

Capstone Title: *Wireshark Traffic Analysis — Malicious Download from a Fake Software Site*

📌1️⃣Executive Summary

On **22nd January 2025**, the BluemoonTuesday SOC team detected unusual network activity from a workstation within its internal LAN `10.1.17.0/24` following the download of a suspicious `.zip` file from a fake *Google Authenticator for Windows* site. The compromised host **(10.1.17.215)** communicated with external IPs, downloaded PowerShell scripts, and demonstrated signs of post-infection Command and Control (C2) beaconing.

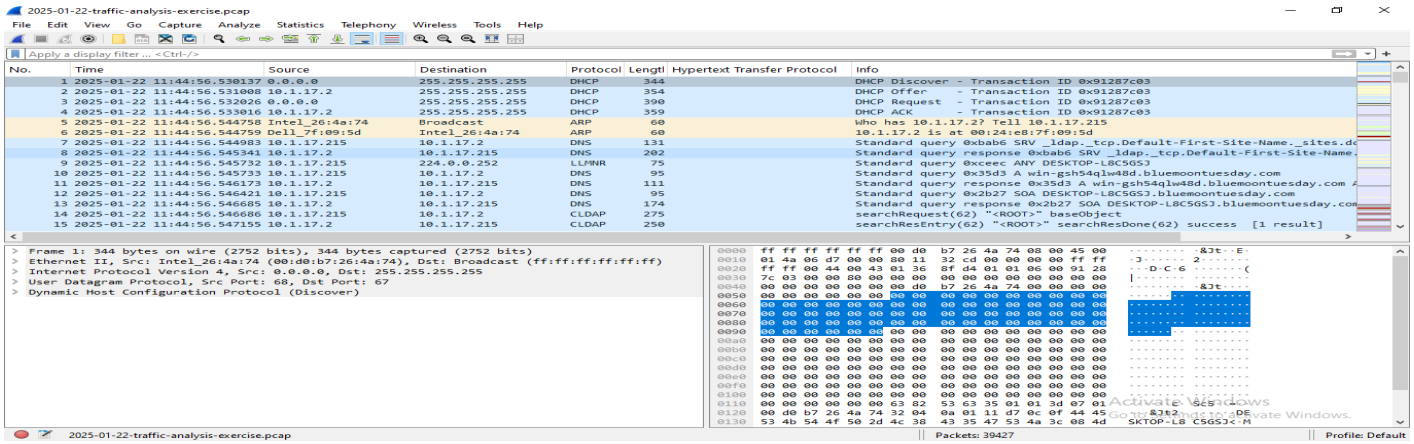
A detailed Wireshark traffic analysis confirmed the infection chain, identified Indicators of Compromise (IOCs), and recommended immediate containment actions.

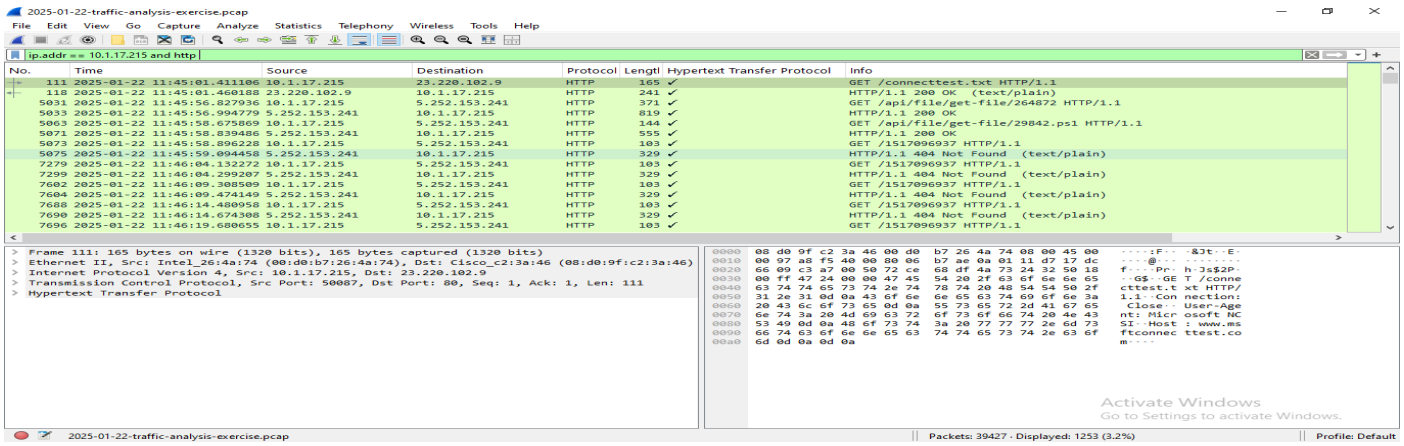
📌2️⃣Timeline of Events

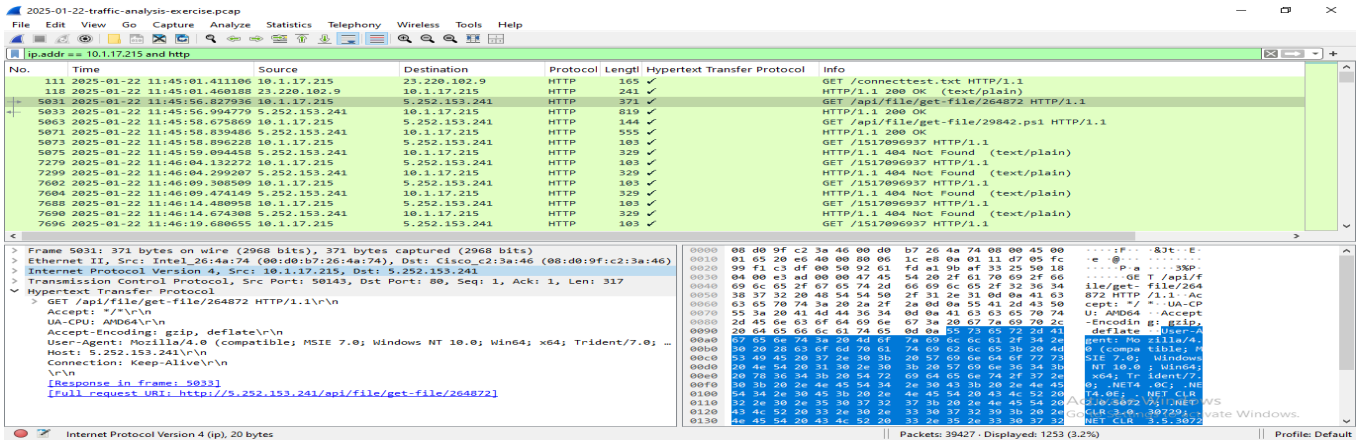
Time (UTC)	Event
11:45:56	Host **10.1.17.215** sent an HTTP GET request to `5.252.153.241` for a file download.
11:45:58	Download of multiple suspicious `.ps1` files and other payloads.
11:46:04	Beaconing requests observed to `/1517096937` on the same external IP (C2 traffic).
11:46:23	Secondary payload downloaded from `199.232.214.172` via `/filestreamingservice/files/`.
11:46:23–onward	Continued DNS queries, indicating persistence attempts and connectivity checks.

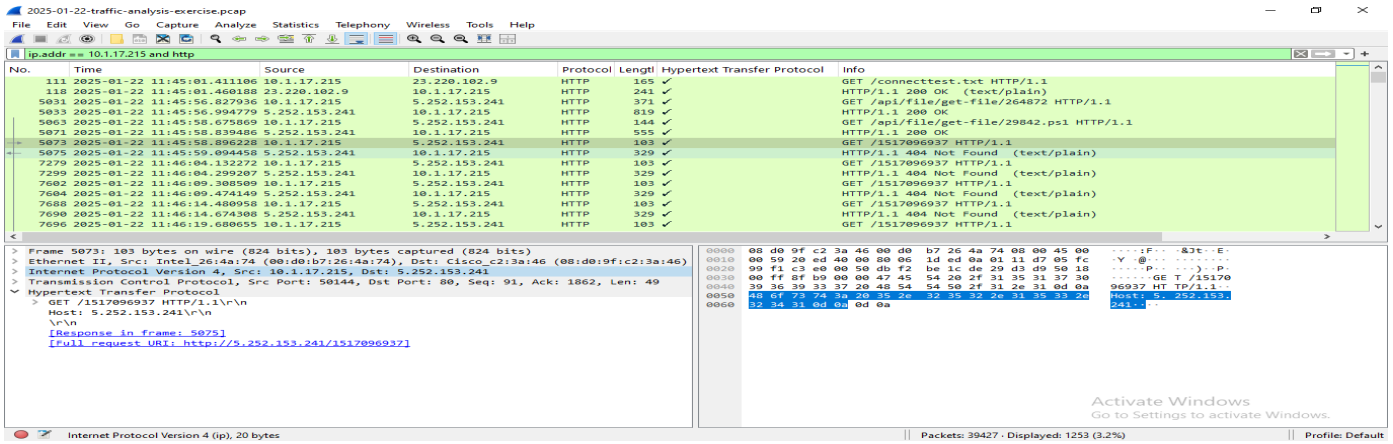
📌3️⃣Analysis Walkthrough

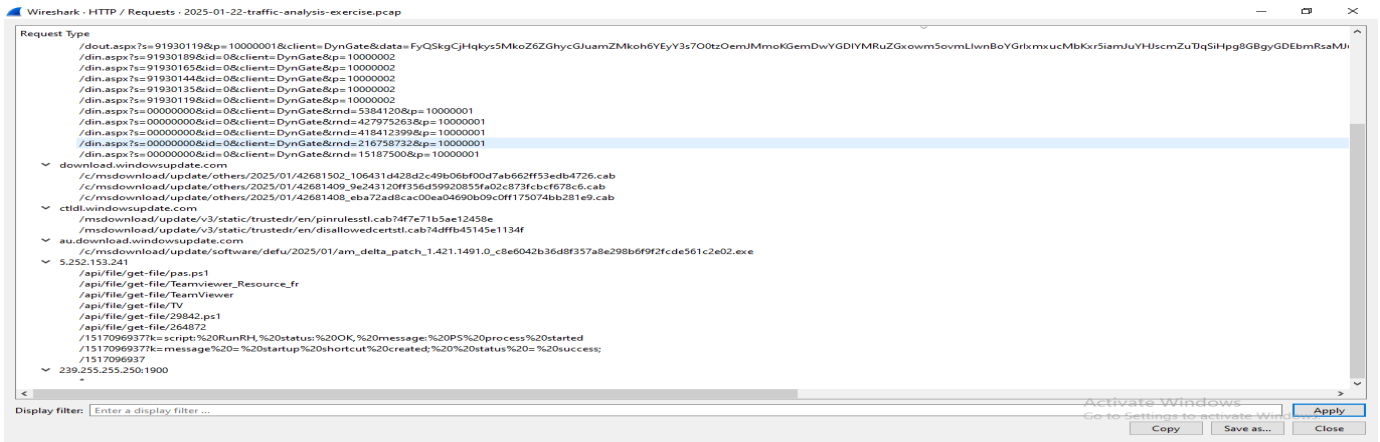
- Loaded the `2025-01-22-traffic-analysis-exercise.pcap` file into **Wireshark**.
- Filtered for suspected internal host: `ip.addr == 10.1.17.215`
- Focused on HTTP traffic: `ip.addr == 10.1.17.215 and http`
- Inspected suspicious file downloads via: `/api/file/get-file/`
- and multiple GET requests to `/1517096937`
- Used `Statistics → HTTP → Requests` for overview of request patterns.
- Checked DNS queries and resolved suspicious lookups via: `ip.addr == 10.1.17.215 and dns`

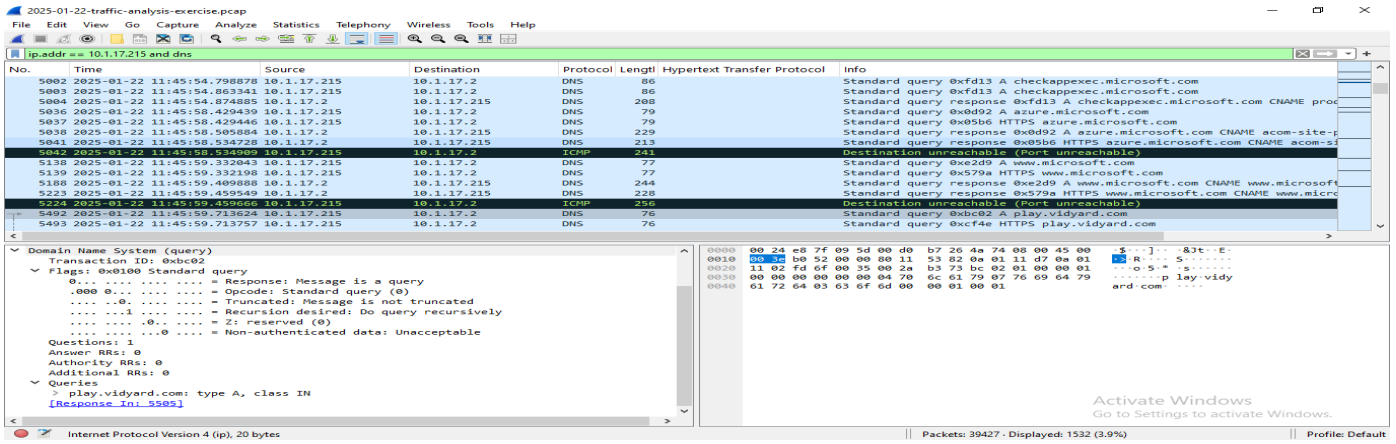




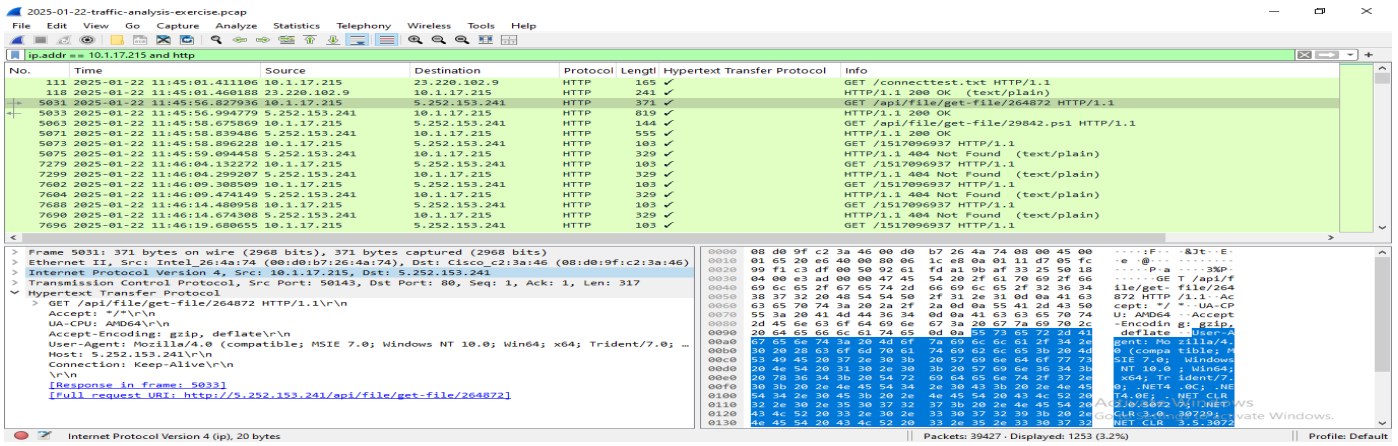

2025-01-22-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 10.1.17.215 and http
No. Time Source Destination Protocol Lengtl Hypertext Transfer Protocol Info
111 2025-01-22 11:45:01.411106 10.1.17.215 23.220.102.9 HTTP 165 ✓ GET /connecttest.txt HTTP/1.1
118 2025-01-22 11:45:01.460188 23.220.102.9 10.1.17.215 HTTP 241 ✓ HTTP/1.1 200 OK (text/plain)
5031 2025-01-22 11:45:56.827936 10.1.17.215 5.252.153.241 HTTP 371 ✓ GET /api/file/get-file/264872 HTTP/1.1
5033 2025-01-22 11:45:56.994779 5.252.153.241 10.1.17.215 HTTP 819 ✓ HTTP/1.1 200 OK
5063 2025-01-22 11:45:58.675869 10.1.17.215 5.252.153.241 HTTP 144 ✓ GET /api/file/get-file/29842.ps1 HTTP/1.1
5071 2025-01-22 11:45:58.839486 5.252.153.241 10.1.17.215 HTTP 555 ✓ HTTP/1.1 200 OK
5073 2025-01-22 11:45:58.896228 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
5075 2025-01-22 11:45:59.094458 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7279 2025-01-22 11:46:04.132272 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
7299 2025-01-22 11:46:04.299207 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7602 2025-01-22 11:46:09.308509 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
7604 2025-01-22 11:46:09.474149 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7688 2025-01-22 11:46:14.480958 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
7690 2025-01-22 11:46:14.674308 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7696 2025-01-22 11:46:19.680655 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
Frame 5031: 371 bytes on wire (2968 bits), 371 bytes captured (2968 bits)
Ethernet II, Src: Intel_26:4a:74 (00:d0:b7:26:4a:74), Dst: Cisco_c2:3a:46 (08:d0:9f:c2:3a:46)
Internet Protocol Version 4, Src: 10.1.17.215, Dst: 5.252.153.241
Transmission Control Protocol, Src Port: 50143, Dst Port: 80, Seq: 1, Ack: 1, Len: 317
Hypertext Transfer Protocol
GET /api/file/get-file/264872 HTTP/1.1\r\n
Accept: */*\r\n
UA-CPU: AMD64\r\n
Accept-Encoding: gzip, deflate\r\n
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; …
Host: 5.252.153.241\r\n
Connection: Keep-Alive\r\n
\r\n
[Response in frame: 5033]
[Full request URI: http://5.252.153.241/api/file/get-file/264872]
Internet Protocol Version 4 (ip), 20 bytes
Packets: 39427 · Displayed: 1253 (3.2%)
Profile: Default

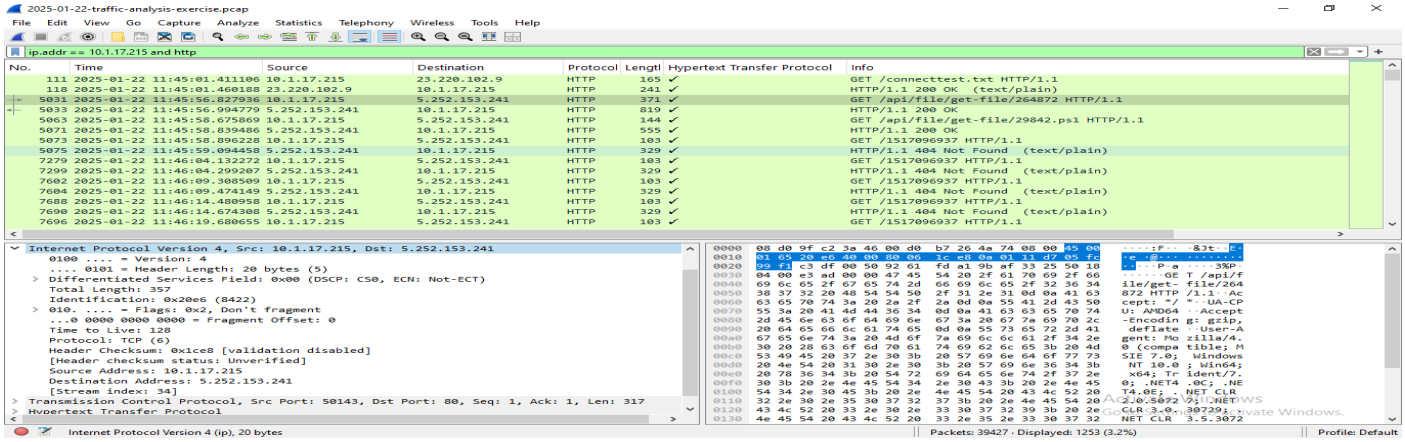

2025-01-22-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 10.1.17.215 and http
No. Time Source Destination Protocol Lengtl Hypertext Transfer Protocol Info
111 2025-01-22 11:45:01.411106 10.1.17.215 23.220.102.9 HTTP 165 ✓ GET /connecttest.txt HTTP/1.1
118 2025-01-22 11:45:01.460188 23.220.102.9 10.1.17.215 HTTP 241 ✓ HTTP/1.1 200 OK (text/plain)
5031 2025-01-22 11:45:56.827936 10.1.17.215 5.252.153.241 HTTP 371 ✓ GET /api/file/get-file/264872 HTTP/1.1
5033 2025-01-22 11:45:56.994779 5.252.153.241 10.1.17.215 HTTP 819 ✓ HTTP/1.1 200 OK
5063 2025-01-22 11:45:58.675869 10.1.17.215 5.252.153.241 HTTP 144 ✓ GET /api/file/get-file/29842.ps1 HTTP/1.1
5071 2025-01-22 11:45:58.839486 5.252.153.241 10.1.17.215 HTTP 555 ✓ HTTP/1.1 200 OK
5073 2025-01-22 11:45:58.896228 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
5075 2025-01-22 11:45:59.094458 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7279 2025-01-22 11:46:04.132272 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
7299 2025-01-22 11:46:04.299207 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7602 2025-01-22 11:46:09.308509 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
7604 2025-01-22 11:46:09.474149 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7688 2025-01-22 11:46:14.480958 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
7690 2025-01-22 11:46:14.674308 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7696 2025-01-22 11:46:19.680655 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
Frame 5073: 103 bytes on wire (824 bits), 103 bytes captured (824 bits)
Ethernet II, Src: Intel_26:4a:74 (00:d0:b7:26:4a:74), Dst: Cisco_c2:3a:46 (08:d0:9f:c2:3a:46)
Internet Protocol Version 4, Src: 10.1.17.215, Dst: 5.252.153.241
Transmission Control Protocol, Src Port: 50144, Dst Port: 80, Seq: 91, Ack: 1862, Len: 49
Hypertext Transfer Protocol
GET /1517096937 HTTP/1.1\r\n
Host: 5.252.153.241\r\n
\r\n
[Response in frame: 5075]
[Full request URI: http://5.252.153.241/1517096937]
Internet Protocol Version 4 (ip), 20 bytes
Packets: 39427 · Displayed: 1253 (3.2%)
Profile: Default

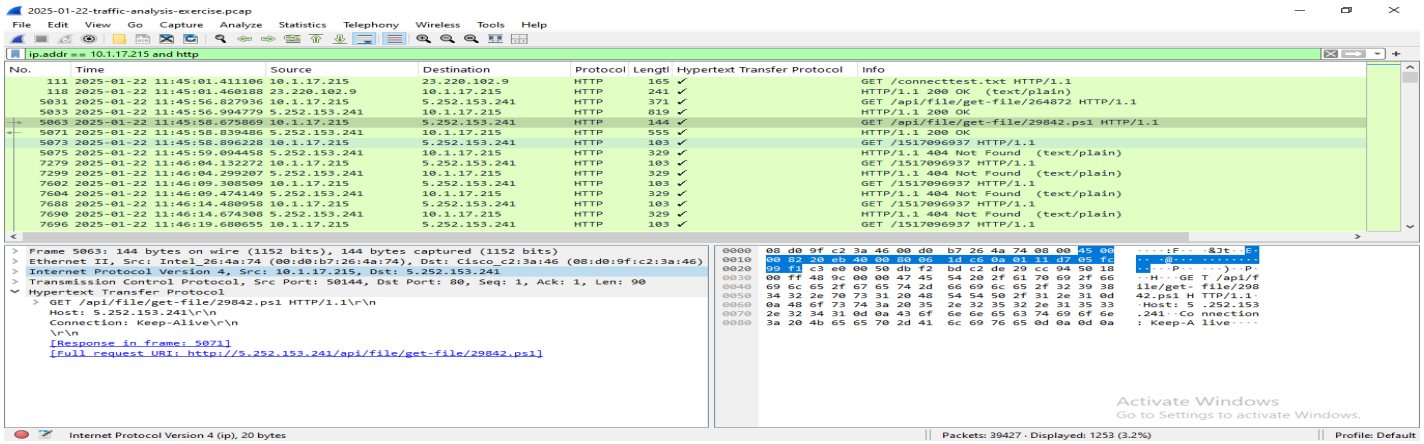

Wireshark · HTTP / Requests · 2025-01-22-traffic-analysis-exercise.pcap
Request Type
/dout.aspx?s=919301198&p=10000001&client=DynGate&data=FyQSkgCjHqkys5MkoZ6ZGhycGJuamZMkoh6YEyV3s7O0tzOemJMmoKGemDwYGDIYMRuZGxowm5ovmLlwnBoYGrlxmxucMbKxr5iamJuYHJscmZuTqSiHpg8GBgyGDEbmRsaMJ
/din.aspx?s=919301089&id=0&client=DynGate&p=10000002
/din.aspx?s=919301065&id=0&client=DynGate&p=10000002
/din.aspx?s=919301448&id=0&client=DynGate&p=10000002
/din.aspx?s=919301358&id=0&client=DynGate&p=10000002
/din.aspx?s=919301198&id=0&client=DynGate&p=10000002
/din.aspx?s=000000008&id=0&client=DynGate&rnd=5384120&p=10000001
/din.aspx?s=000000008&id=0&client=DynGate&rnd=427975263&p=10000001
/din.aspx?s=000000008&id=0&client=DynGate&rnd=418412399&p=10000001
/din.aspx?s=000000008&id=0&client=DynGate&rnd=216758732&p=10000001
/din.aspx?s=000000008&id=0&client=DynGate&rnd=15187500&p=10000001
download.windowsupdate.com
/c/msdownload/update/others/2025/01/42681502_106431d428d2c49b06bf00d7ab662ff53edb4726.cab
/c/msdownload/update/others/2025/01/42681409_9e243120ff356d59920855fa02c873fcbcf678c6.cab
/c/msdownload/update/others/2025/01/42681408_eba72ad8cac00ea04690b09c0ff175074bb281e9.cab
ctldl.windowsupdate.com
/msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?4f7e71b5ae12458e
/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?4dffb45145e1134f
au.download.windowsupdate.com
/c/msdownload/update/software/defu/2025/01/am_delta_patch_1.421.1491.0_c8e6042b36d8f357a8e298b6f9f2fcde561c2e02.exe
5.252.153.241
/api/file/get-file/pas.ps1
/api/file/get-file/Teamviewer_Resource_fr
/api/file/get-file/TeamViewer
/api/file/get-file/TV
/api/file/get-file/29842.ps1
/api/file/get-file/264872
/15170969377k=script:%20RunRH,%20status:%20OK,%20message:%20PS%20process%20started
/15170969377k=message%20=%20startup%20shortcut%20created;%20%20status%20=%20success;
/1517096937
239.255.255.250:1900
Display filter: Enter a display filter …
Apply
Copy
Save as…
Close

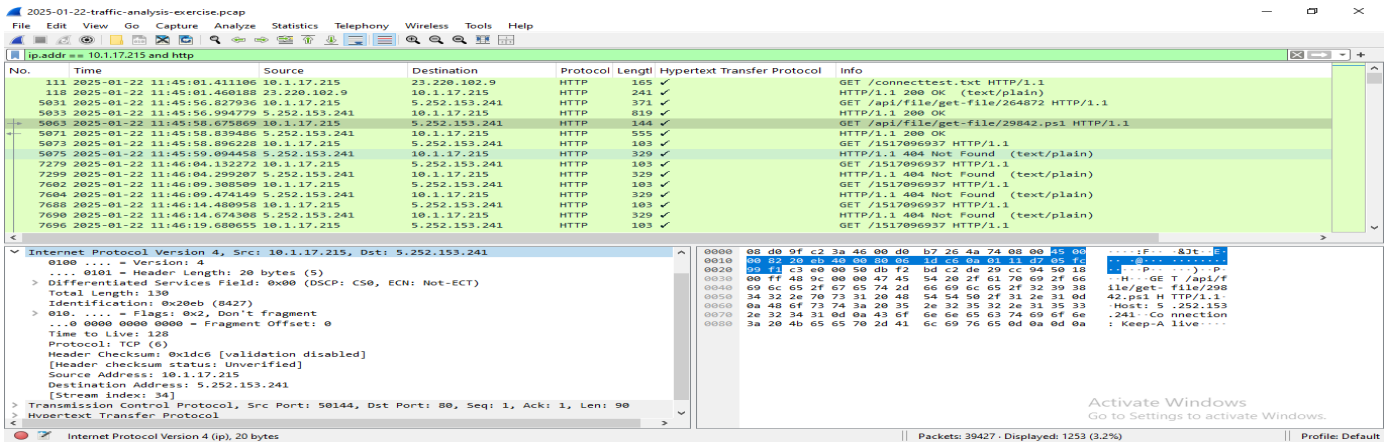


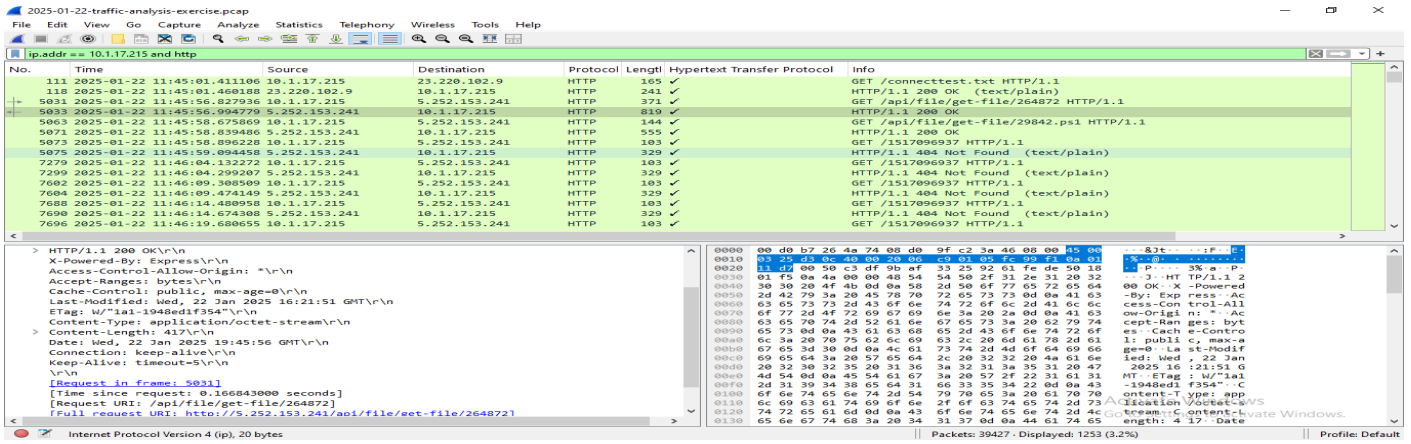
- Captured screenshots of:
  - HTTP request URIs
  - C2 communication GET requests
  - DNS requests to `play.vidyard.com`, `msftconnecttest.com`, etc.

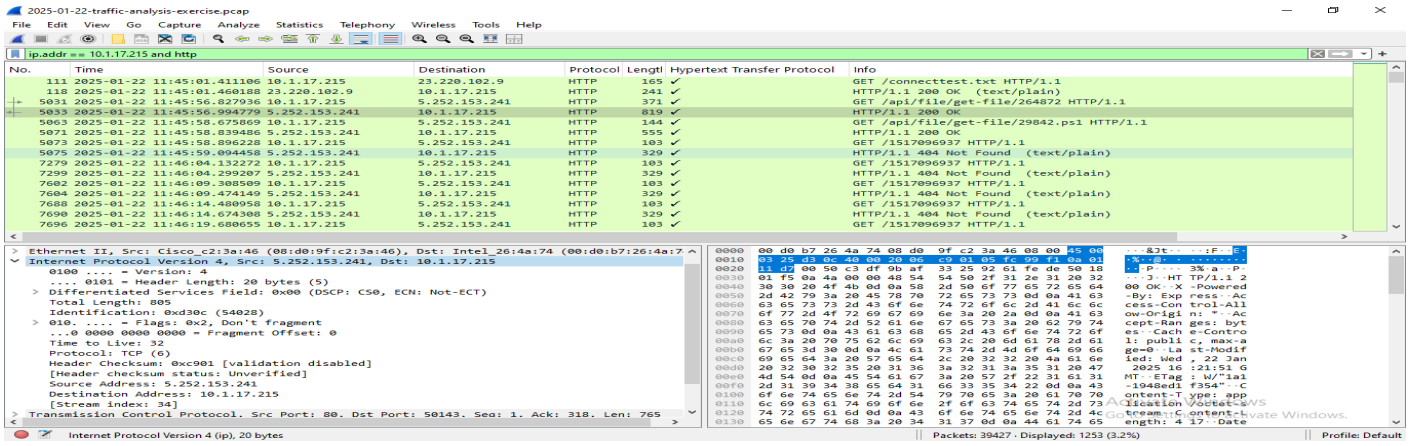


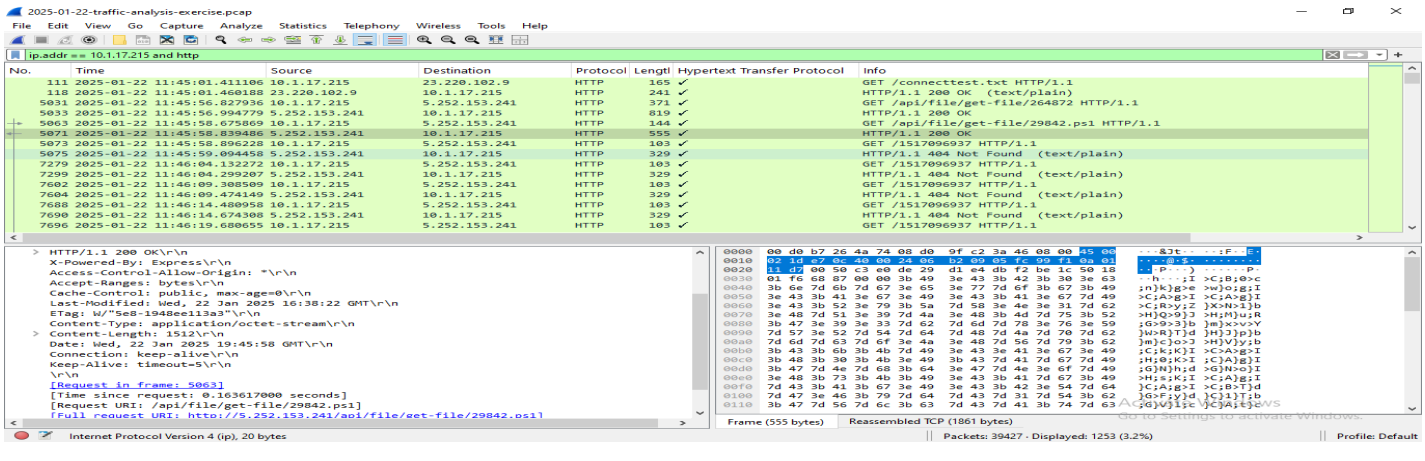

2025-01-22-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 10.1.17.215 and http
No. Time Source Destination Protocol Lengtl Hypertext Transfer Protocol Info
111 2025-01-22 11:45:01.411106 10.1.17.215 23.220.102.9 HTTP 165 ✓ GET /connecttest.txt HTTP/1.1
118 2025-01-22 11:45:01.460188 23.220.102.9 10.1.17.215 HTTP 241 ✓ HTTP/1.1 200 OK (text/plain)
5031 2025-01-22 11:45:56.827936 10.1.17.215 5.252.153.241 HTTP 371 ✓ GET /api/file/get-file/264872 HTTP/1.1
5033 2025-01-22 11:45:56.994779 5.252.153.241 10.1.17.215 HTTP 819 ✓ HTTP/1.1 200 OK
5063 2025-01-22 11:45:58.675869 10.1.17.215 5.252.153.241 HTTP 144 ✓ GET /api/file/get-file/29842.ps1 HTTP/1.1
5071 2025-01-22 11:45:58.839486 5.252.153.241 10.1.17.215 HTTP 555 ✓ HTTP/1.1 200 OK
5073 2025-01-22 11:45:58.896228 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
5075 2025-01-22 11:45:59.094458 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7279 2025-01-22 11:46:04.132272 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
7299 2025-01-22 11:46:04.299207 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7602 2025-01-22 11:46:09.308509 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
7604 2025-01-22 11:46:09.474149 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7688 2025-01-22 11:46:14.480958 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
7690 2025-01-22 11:46:14.674308 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7696 2025-01-22 11:46:19.680655 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
Internet Protocol Version 4, Src: 10.1.17.215, Dst: 5.252.153.241
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 357
Identification: 0x20e6 (8422)
010. .... = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: TCP (6)
Header Checksum: 0x1ce8 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.1.17.215
Destination Address: 5.252.153.241
[Stream index: 34]
Transmission Control Protocol, Src Port: 50143, Dst Port: 80, Seq: 1, Ack: 1, Len: 317
Hypertext Transfer Protocol
0000 08 d0 9f c2 3a 46 00 d0 b7 26 4a 74 08 00 45 00 ····:F··· ·&Jt··E·
0010 01 65 20 e6 40 00 80 06 1c e8 0a 01 11 d7 05 fc ·e ·@··· ········
0020 99 f1 c3 df 00 50 92 01 fd a1 9b af 33 25 50 18 ·····P·· ····3%P·
0030 04 00 e3 ad 00 00 47 45 54 20 2f 61 70 69 2f 66 ····GE T /api/f
0040 69 6c 65 2f 67 65 74 2d 66 69 6c 65 2f 32 36 34 ile/get- file/264
0050 38 37 32 20 48 54 54 50 2f 31 2e 31 0d 0a 41 63 872 HTTP /1.1 ··Ac
0060 63 65 70 74 3a 20 2a 2f 2a 0d 0a 55 41 2d 43 50 cept: */ *··UA-CP
0070 55 3a 20 41 4d 44 36 34 0d 0a 41 63 63 65 70 74 U: AMD64 ··Accept
0080 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c -Encodin g: gzip,
0090 20 64 65 66 6c 61 74 65 0d 0a 55 73 65 72 2d 41 deflate ··User-A
00a0 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 34 2e gent: Mo zilla/4.
00b0 30 20 28 63 6f 6d 70 61 74 69 62 6c 65 3b 20 4d 0 (compa tible; M
00c0 53 49 45 20 37 2e 30 3b 20 57 69 6e 64 6f 77 73 SIE 7.0; Windows
00d0 20 4e 54 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b NT 10.0 ; Win64;
00e0 20 78 36 34 3b 20 54 72 69 64 65 6e 74 2f 37 2e x64; Tr ident/7.
00f0 30 3b 20 2e 4e 45 54 34 2e 30 43 3b 20 2e 4e 45 0; .NET4 .0C; .NE
0100 54 34 2e 30 45 3b 20 2e 4e 45 54 20 43 4c 52 20 T4.0E; . NET CLR
0110 32 2e 30 2e 35 30 37 32 37 3b 20 2e 4e 45 54 20 2.0.5072 7; .NET
0120 43 4c 52 20 33 2e 30 2e 33 30 37 32 39 3b 20 2e CLR 3.0. 30729; .
0130 4e 45 54 20 43 4c 52 20 33 2e 35 2e 33 30 37 32 NET CLR 3.5.3072
Internet Protocol Version 4 (ip), 20 bytes
Packets: 39427 · Displayed: 1253 (3.2%)
Profile: Default

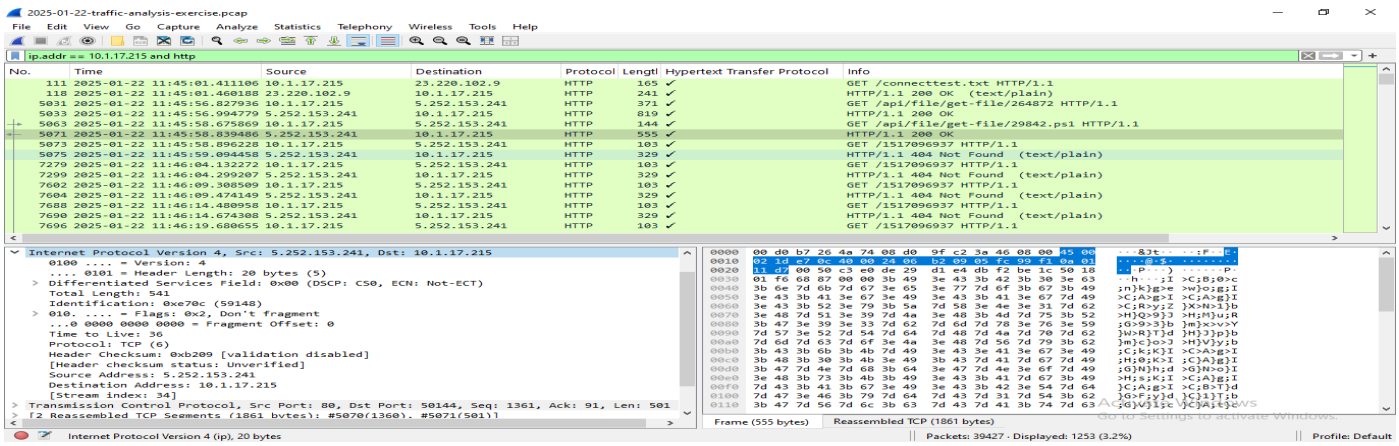

2025-01-22-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 10.1.17.215 and http
No. Time Source Destination Protocol Lengtl Hypertext Transfer Protocol Info
111 2025-01-22 11:45:01.411106 10.1.17.215 23.220.102.9 HTTP 165 ✓ GET /connecttest.txt HTTP/1.1
118 2025-01-22 11:45:01.460188 23.220.102.9 10.1.17.215 HTTP 241 ✓ HTTP/1.1 200 OK (text/plain)
5031 2025-01-22 11:45:56.827936 10.1.17.215 5.252.153.241 HTTP 371 ✓ GET /api/file/get-file/264872 HTTP/1.1
5033 2025-01-22 11:45:56.994779 5.252.153.241 10.1.17.215 HTTP 819 ✓ HTTP/1.1 200 OK
5063 2025-01-22 11:45:58.675869 10.1.17.215 5.252.153.241 HTTP 144 ✓ GET /api/file/get-file/29842.ps1 HTTP/1.1
5071 2025-01-22 11:45:58.839486 5.252.153.241 10.1.17.215 HTTP 555 ✓ HTTP/1.1 200 OK
5073 2025-01-22 11:45:58.896228 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
5075 2025-01-22 11:45:59.094458 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7279 2025-01-22 11:46:04.132272 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
7299 2025-01-22 11:46:04.299207 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7602 2025-01-22 11:46:09.308509 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
7604 2025-01-22 11:46:09.474149 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7688 2025-01-22 11:46:14.480958 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
7690 2025-01-22 11:46:14.674308 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7696 2025-01-22 11:46:19.680655 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
Frame 5063: 144 bytes on wire (1152 bits), 144 bytes captured (1152 bits)
Ethernet II, Src: Intel_26:4a:74 (00:d0:b7:26:4a:74), Dst: Cisco_c2:3a:46 (08:d0:9f:c2:3a:46)
Internet Protocol Version 4, Src: 10.1.17.215, Dst: 5.252.153.241
Transmission Control Protocol, Src Port: 50144, Dst Port: 80, Seq: 1, Ack: 1, Len: 90
Hypertext Transfer Protocol
GET /api/file/get-file/29842.ps1 HTTP/1.1\r\n
Host: 5.252.153.241\r\n
Connection: Keep-Alive\r\n
\r\n
[Response in frame: 5071]
[Full request URI: http://5.252.153.241/api/file/get-file/29842.ps1]
0000 08 d0 9f c2 3a 46 00 d0 b7 26 4a 74 08 00 45 00 ····:F··· ·&Jt··E·
0010 00 82 20 eb 40 00 80 06 1d c6 0a 01 11 d7 05 fc ·· ·@··· ········
0020 99 f1 c3 e0 00 50 db f2 bd c2 de 29 cc 94 50 18 ·····P·· ···)··P·
0030 00 ff 48 9c 00 00 47 45 54 20 2f 61 70 69 2f 66 ··H···GE T /api/f
0040 69 6c 65 2f 67 65 74 2d 66 69 6c 65 2f 32 39 38 ile/get- file/298
0050 34 32 2e 70 73 31 20 48 54 54 50 2f 31 2e 31 0d 42.ps1 H TTP/1.1·
0060 0a 48 6f 73 74 3a 20 35 2e 32 35 32 2e 31 35 33 ·Host: 5 .252.153
0070 2e 32 34 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e .241··Co nnection
0080 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 0d 0a : Keep-A live····
Internet Protocol Version 4 (ip), 20 bytes
Packets: 39427 · Displayed: 1253 (3.2%)
Profile: Default

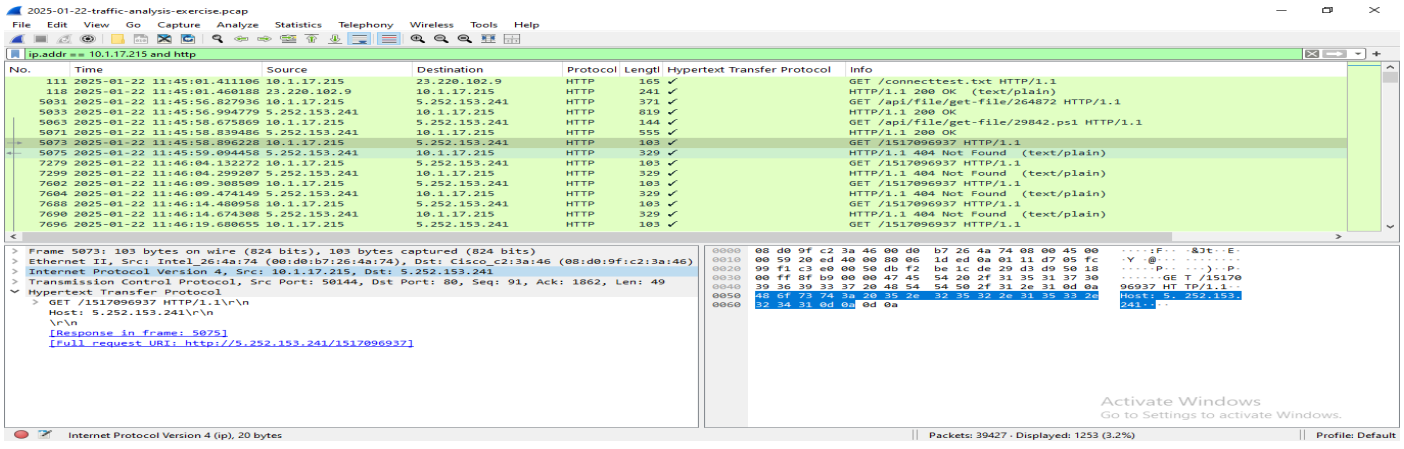

2025-01-22-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 10.1.17.215 and http
No. Time Source Destination Protocol Lengtl Hypertext Transfer Protocol Info
111 2025-01-22 11:45:01.411106 10.1.17.215 23.220.102.9 HTTP 165 ✓ GET /connecttest.txt HTTP/1.1
118 2025-01-22 11:45:01.460188 23.220.102.9 10.1.17.215 HTTP 241 ✓ HTTP/1.1 200 OK (text/plain)
5031 2025-01-22 11:45:56.827936 10.1.17.215 5.252.153.241 HTTP 371 ✓ GET /api/file/get-file/264872 HTTP/1.1
5033 2025-01-22 11:45:56.994779 5.252.153.241 10.1.17.215 HTTP 819 ✓ HTTP/1.1 200 OK
5063 2025-01-22 11:45:58.675869 10.1.17.215 5.252.153.241 HTTP 144 ✓ GET /api/file/get-file/29842.ps1 HTTP/1.1
5071 2025-01-22 11:45:58.839486 5.252.153.241 10.1.17.215 HTTP 555 ✓ HTTP/1.1 200 OK
5073 2025-01-22 11:45:58.896228 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
5075 2025-01-22 11:45:59.094458 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7279 2025-01-22 11:46:04.132272 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
7299 2025-01-22 11:46:04.299207 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7602 2025-01-22 11:46:09.308509 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
7604 2025-01-22 11:46:09.474149 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7688 2025-01-22 11:46:14.480958 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
7690 2025-01-22 11:46:14.674308 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7696 2025-01-22 11:46:19.680655 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
Internet Protocol Version 4, Src: 10.1.17.215, Dst: 5.252.153.241
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 130
Identification: 0x20eb (8427)
010. .... = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: TCP (6)
Header Checksum: 0x1dc6 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.1.17.215
Destination Address: 5.252.153.241
[Stream index: 34]
Transmission Control Protocol, Src Port: 50144, Dst Port: 80, Seq: 1, Ack: 1, Len: 90
Hypertext Transfer Protocol
0000 08 d0 9f c2 3a 46 00 d0 b7 26 4a 74 08 00 45 00 ····:F··· ·&Jt··E·
0010 00 82 20 eb 40 00 80 06 1d c6 0a 01 11 d7 05 fc ·· ·@··· ········
0020 99 f1 c3 e0 00 50 db f2 bd c2 de 29 cc 94 50 18 ·····P·· ···)··P·
0030 00 ff 48 9c 00 00 47 45 54 20 2f 61 70 69 2f 66 ··H···GE T /api/f
0040 69 6c 65 2f 67 65 74 2d 66 69 6c 65 2f 32 39 38 ile/get- file/298
0050 34 32 2e 70 73 31 20 48 54 54 50 2f 31 2e 31 0d 42.ps1 H TTP/1.1·
0060 0a 48 6f 73 74 3a 20 35 2e 32 35 32 2e 31 35 33 ·Host: 5 .252.153
0070 2e 32 34 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e .241··Co nnection
0080 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 0d 0a : Keep-A live····
Internet Protocol Version 4 (ip), 20 bytes
Packets: 39427 · Displayed: 1253 (3.2%)
Profile: Default

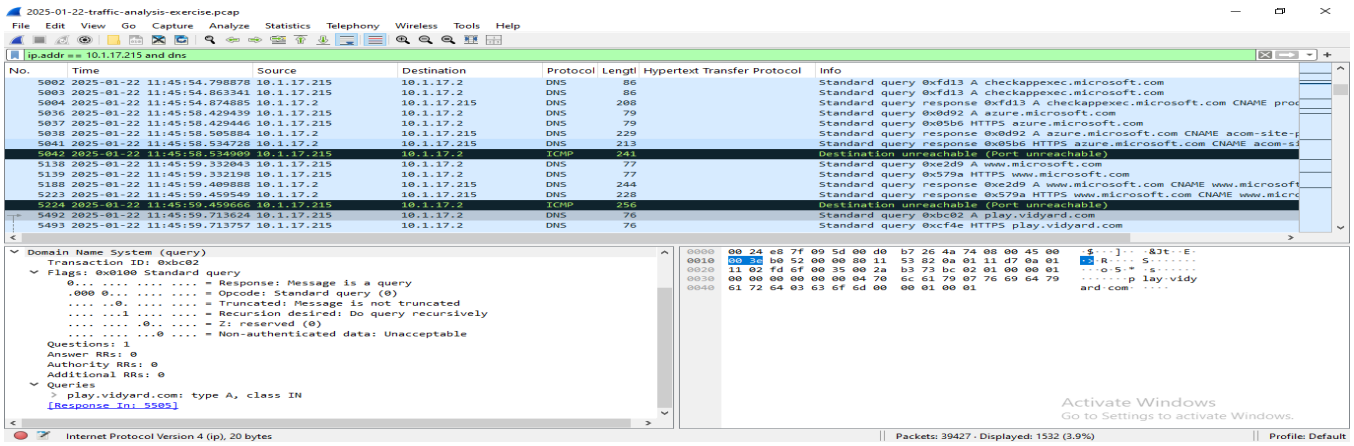

2025-01-22-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 10.1.17.215 and http
No. Time Source Destination Protocol Lengtl Hypertext Transfer Protocol Info
111 2025-01-22 11:45:01.411106 10.1.17.215 23.220.102.9 HTTP 165 ✓ GET /connecttest.txt HTTP/1.1
118 2025-01-22 11:45:01.460188 23.220.102.9 10.1.17.215 HTTP 241 ✓ HTTP/1.1 200 OK (text/plain)
5031 2025-01-22 11:45:56.827936 10.1.17.215 5.252.153.241 HTTP 371 ✓ GET /api/file/get-file/264872 HTTP/1.1
5033 2025-01-22 11:45:56.994779 5.252.153.241 10.1.17.215 HTTP 819 ✓ HTTP/1.1 200 OK
5063 2025-01-22 11:45:58.675869 10.1.17.215 5.252.153.241 HTTP 144 ✓ GET /api/file/get-file/29842.ps1 HTTP/1.1
5071 2025-01-22 11:45:58.839486 5.252.153.241 10.1.17.215 HTTP 555 ✓ HTTP/1.1 200 OK
5073 2025-01-22 11:45:58.896228 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
5075 2025-01-22 11:45:59.094458 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7279 2025-01-22 11:46:04.132272 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
7299 2025-01-22 11:46:04.299207 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7602 2025-01-22 11:46:09.308509 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
7604 2025-01-22 11:46:09.474149 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7688 2025-01-22 11:46:14.480958 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
7690 2025-01-22 11:46:14.674308 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7696 2025-01-22 11:46:19.680655 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
HTTP/1.1 200 OK\r\n
X-Powered-By: Express\r\n
Access-Control-Allow-Origin: *\r\n
Accept-Ranges: bytes\r\n
Cache-Control: public, max-age=0\r\n
Last-Modified: Wed, 22 Jan 2025 16:21:51 GMT\r\n
ETag: W/"1a1-1948ed1f354"\r\n
Content-Type: application/octet-stream\r\n
Content-Length: 417\r\n
Date: Wed, 22 Jan 2025 19:45:56 GMT\r\n
Connection: keep-alive\r\n
Keep-Alive: timeout=5\r\n
\r\n
[Request in frame: 5031]
[Time since request: 0.166843000 seconds]
[Request URI: /api/file/get-file/264872]
[Full request URI: http://5.252.153.241/api/file/get-file/264872]
Internet Protocol Version 4 (ip), 20 bytes
Packets: 39427 · Displayed: 1253 (3.2%)
Profile: Default


2025-01-22-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 10.1.17.215 and http
No. Time Source Destination Protocol Lengtl Hypertext Transfer Protocol Info
111 2025-01-22 11:45:01.411106 10.1.17.215 23.220.102.9 HTTP 165 ✓ GET /connecttest.txt HTTP/1.1
118 2025-01-22 11:45:01.460188 23.220.102.9 10.1.17.215 HTTP 241 ✓ HTTP/1.1 200 OK (text/plain)
5031 2025-01-22 11:45:56.827936 10.1.17.215 5.252.153.241 HTTP 371 ✓ GET /api/file/get-file/264872 HTTP/1.1
5033 2025-01-22 11:45:56.994779 5.252.153.241 10.1.17.215 HTTP 819 ✓ HTTP/1.1 200 OK
5063 2025-01-22 11:45:58.675869 10.1.17.215 5.252.153.241 HTTP 144 ✓ GET /api/file/get-file/29842.ps1 HTTP/1.1
5071 2025-01-22 11:45:58.839486 5.252.153.241 10.1.17.215 HTTP 555 ✓ HTTP/1.1 200 OK
5073 2025-01-22 11:45:58.896228 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
5075 2025-01-22 11:45:59.094458 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7279 2025-01-22 11:46:04.132272 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
7299 2025-01-22 11:46:04.299207 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7602 2025-01-22 11:46:09.308509 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
7604 2025-01-22 11:46:09.474149 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7688 2025-01-22 11:46:14.480958 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
7690 2025-01-22 11:46:14.674308 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7696 2025-01-22 11:46:19.680655 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
Ethernet II, Src: Cisco_c2:3a:46 (08:d0:9f:c2:3a:46), Dst: Intel_26:4a:74 (00:d0:b7:26:4a:74)
Internet Protocol Version 4, Src: 5.252.153.241, Dst: 10.1.17.215
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 805
Identification: 0xd30c (54028)
010. .... = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 32
Protocol: TCP (6)
Header Checksum: 0xc901 [validation disabled]
[Header checksum status: Unverified]
Source Address: 5.252.153.241
Destination Address: 10.1.17.215
[Stream index: 34]
Transmission Control Protocol, Src Port: 80, Dst Port: 50143, Seq: 1, Ack: 318, Len: 765
Internet Protocol Version 4 (ip), 20 bytes
Packets: 39427 · Displayed: 1253 (3.2%)
Profile: Default


2025-01-22-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 10.1.17.215 and http
No. Time Source Destination Protocol Lengtl Hypertext Transfer Protocol Info
111 2025-01-22 11:45:01.411106 10.1.17.215 23.220.102.9 HTTP 165 ✓ GET /connecttest.txt HTTP/1.1
118 2025-01-22 11:45:01.460188 23.220.102.9 10.1.17.215 HTTP 241 ✓ HTTP/1.1 200 OK (text/plain)
5031 2025-01-22 11:45:56.827936 10.1.17.215 5.252.153.241 HTTP 371 ✓ GET /api/file/get-file/264872 HTTP/1.1
5033 2025-01-22 11:45:56.994779 5.252.153.241 10.1.17.215 HTTP 819 ✓ HTTP/1.1 200 OK
5063 2025-01-22 11:45:58.675869 10.1.17.215 5.252.153.241 HTTP 144 ✓ GET /api/file/get-file/29842.ps1 HTTP/1.1
5071 2025-01-22 11:45:58.839486 5.252.153.241 10.1.17.215 HTTP 555 ✓ HTTP/1.1 200 OK
5073 2025-01-22 11:45:58.896228 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
5075 2025-01-22 11:45:59.094458 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7279 2025-01-22 11:46:04.132272 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
7299 2025-01-22 11:46:04.299207 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7602 2025-01-22 11:46:09.308509 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
7604 2025-01-22 11:46:09.474149 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7688 2025-01-22 11:46:14.480958 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
7690 2025-01-22 11:46:14.674308 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7696 2025-01-22 11:46:19.680655 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
HTTP/1.1 200 OK\r\n
X-Powered-By: Express\r\n
Access-Control-Allow-Origin: *\r\n
Accept-Ranges: bytes\r\n
Cache-Control: public, max-age=0\r\n
Last-Modified: Wed, 22 Jan 2025 16:38:22 GMT\r\n
ETag: W/"5e8-1948ee113a3"\r\n
Content-Type: application/octet-stream\r\n
Content-Length: 1512\r\n
Date: Wed, 22 Jan 2025 19:45:58 GMT\r\n
Connection: keep-alive\r\n
Keep-Alive: timeout=5\r\n
\r\n
[Request in frame: 5063]
[Time since request: 0.163617000 seconds]
[Request URI: /api/file/get-file/29842.ps1]
[Full request URI: http://5.252.153.241/api/file/get-file/29842.ps1]
Frame (555 bytes)
Reassembled TCP (1861 bytes)
Internet Protocol Version 4 (ip), 20 bytes
Packets: 39427 · Displayed: 1253 (3.2%)
Profile: Default







📌4 Host and User Details

Question	Answer

IP address of infected client	`10.1.17.215`
MAC address	Can be extracted via `eth.addr` filter if needed
Hostname	Seen in DNS traffic: `DESKTOP-L8C5GSJ`
User account name	Not captured in this PCAP (no SMB/LDAP)
Domain of fake site	Connected to `5.252.153.241` directly
C2 server IP addresses	`5.252.153.241`, `199.232.214.172`

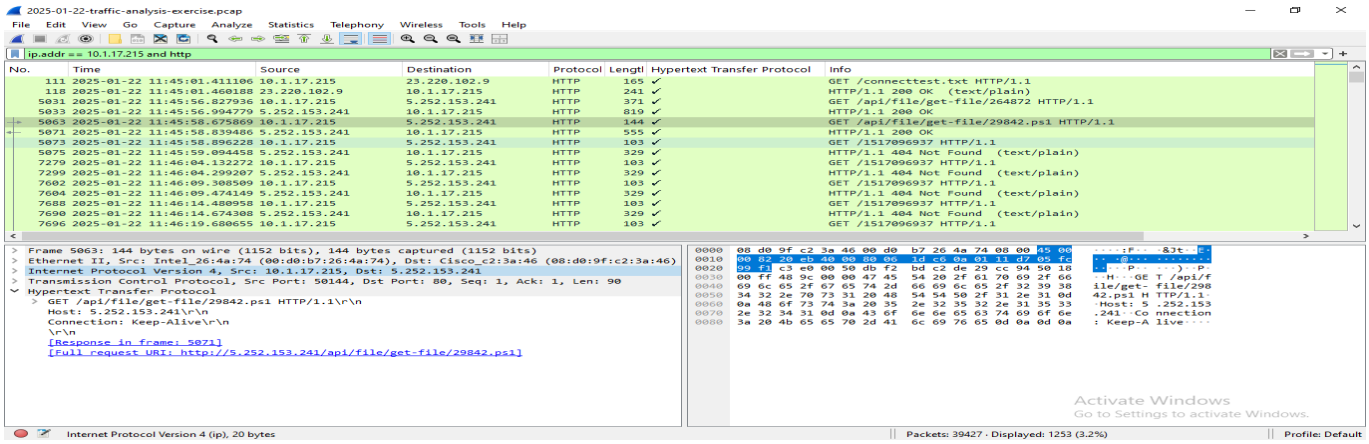
📌5️⃣ IOC Table

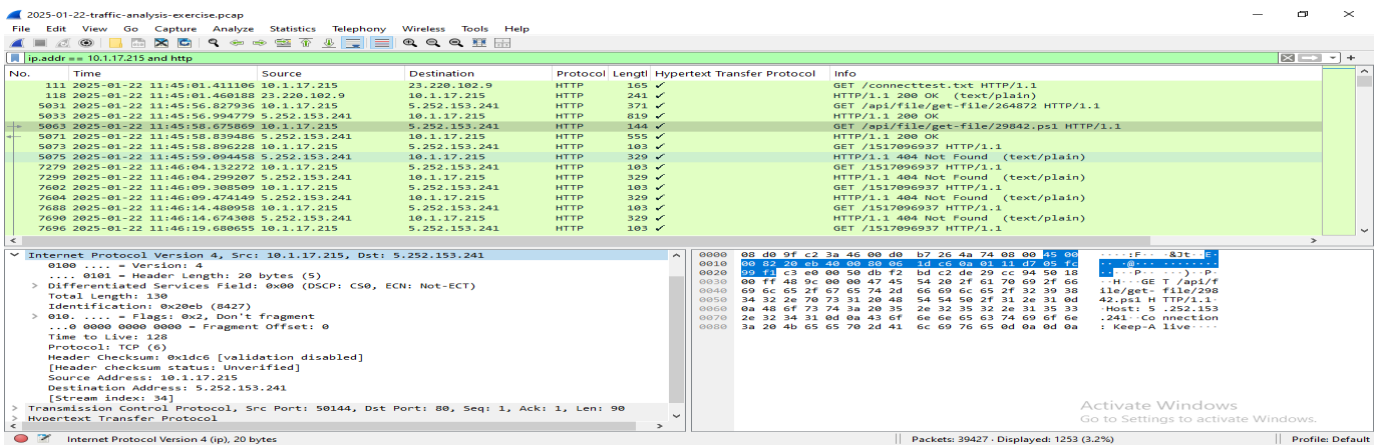
Indicator Type	Value
Malicious IPs	`5.252.153.241`, `199.232.214.172`
Suspicious URLs	`/api/file/get-file/`, `/1517096937`, `/filestreamingservice/files/`
Domains	`play.vidyard.com`, `msftconnecttest.com`
Payload Types	PowerShell scripts, executable payloads

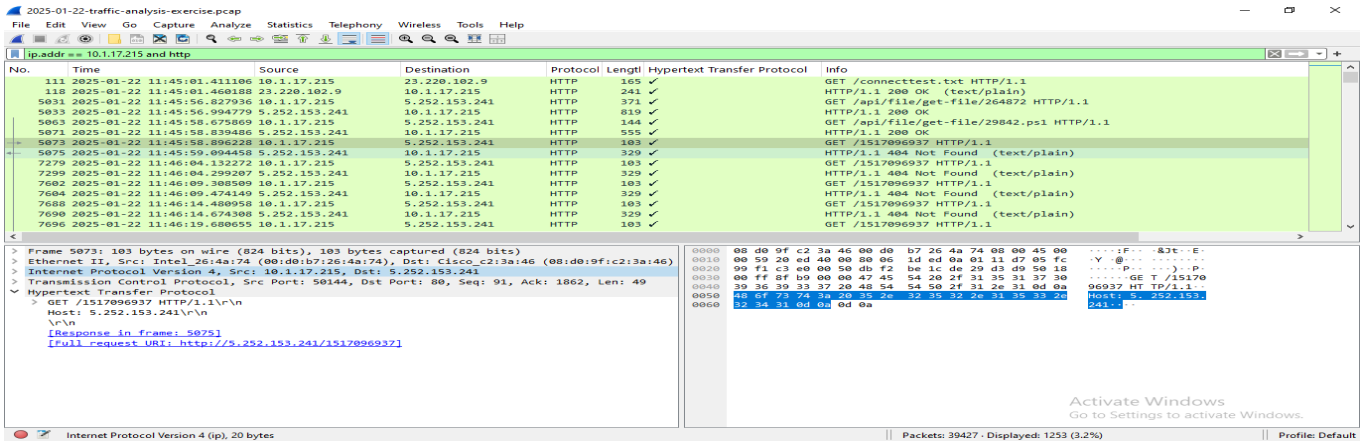
📌6️⃣ Screenshots from Wireshark

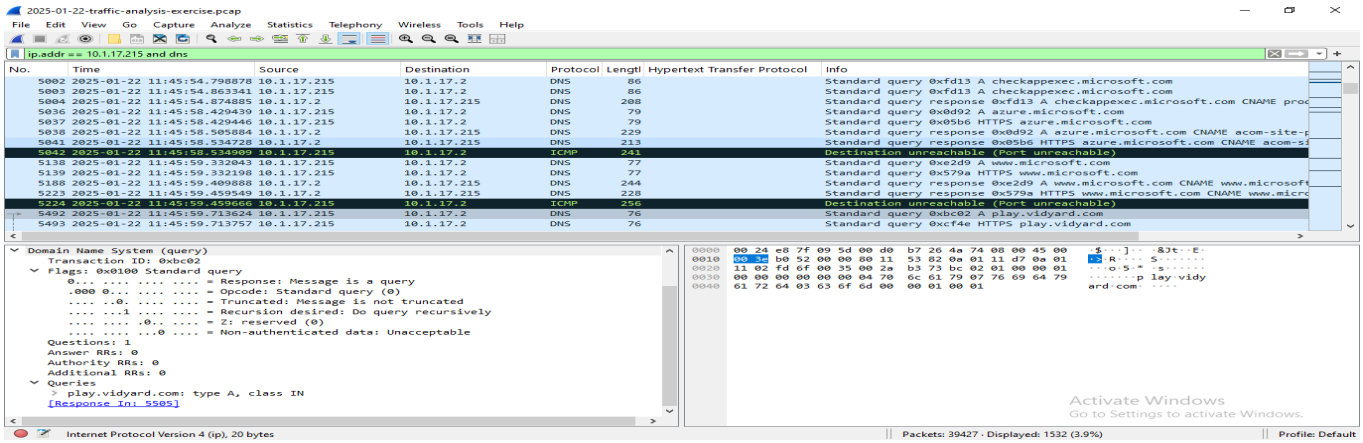
📌 Screenshots to capture:

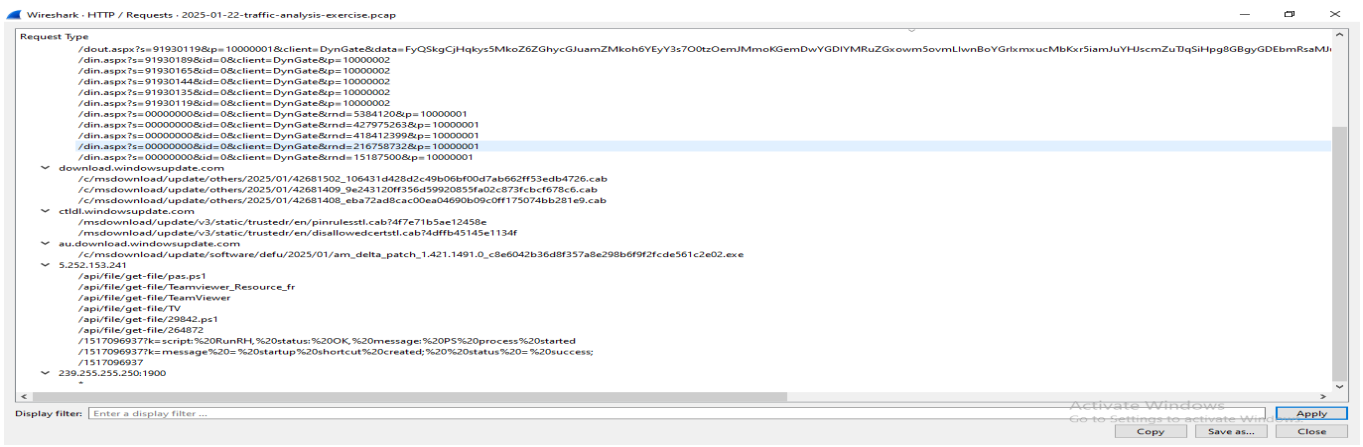
- Filtered HTTP GET requests to `/api/file/get-file/`
- Repeated C2 beaconing GET requests to `/1517096937`
- DNS queries to `play.vidyard.com` and other unusual domains
- HTTP Statistics window from `Statistics → HTTP → Requests`


2025-01-22-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 10.1.17.215 and http
No. Time Source Destination Protocol Length Hypertext Transfer Protocol Info
111 2025-01-22 11:45:01.411106 10.1.17.215 23.220.102.9 HTTP 165 ✓ GET /connecttest.txt HTTP/1.1
118 2025-01-22 11:45:01.460188 23.220.102.9 10.1.17.215 HTTP 241 ✓ HTTP/1.1 200 OK (text/plain)
5031 2025-01-22 11:45:56.827936 10.1.17.215 5.252.153.241 HTTP 371 ✓ GET /api/file/get-file/264872 HTTP/1.1
5033 2025-01-22 11:45:56.994779 5.252.153.241 10.1.17.215 HTTP 819 ✓ HTTP/1.1 200 OK
5063 2025-01-22 11:45:58.675869 10.1.17.215 5.252.153.241 HTTP 144 ✓ GET /api/file/get-file/29842.ps1 HTTP/1.1
5071 2025-01-22 11:45:58.839486 5.252.153.241 10.1.17.215 HTTP 555 ✓ HTTP/1.1 200 OK
5073 2025-01-22 11:45:58.896228 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
5075 2025-01-22 11:45:59.094458 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7279 2025-01-22 11:46:04.132272 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
7299 2025-01-22 11:46:04.299207 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7602 2025-01-22 11:46:09.308509 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
7604 2025-01-22 11:46:09.474149 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7688 2025-01-22 11:46:14.480958 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
7690 2025-01-22 11:46:14.674308 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7696 2025-01-22 11:46:19.680655 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
Frame 5063: 144 bytes on wire (1152 bits), 144 bytes captured (1152 bits)
Ethernet II, Src: Intel_26:4a:74 (00:d0:b7:26:4a:74), Dst: Cisco_c2:3a:46 (08:d0:9f:c2:3a:46)
Internet Protocol Version 4, Src: 10.1.17.215, Dst: 5.252.153.241
Transmission Control Protocol, Src Port: 50144, Dst Port: 80, Seq: 1, Ack: 1, Len: 90
Hypertext Transfer Protocol
GET /api/file/get-file/29842.ps1 HTTP/1.1\r\n
Host: 5.252.153.241\r\n
Connection: Keep-Alive\r\n
\r\n
[Response in frame: 5071]
[Full request URI: http://5.252.153.241/api/file/get-file/29842.ps1]
0000 08 d0 9f c2 3a 46 00 d0 b7 26 4a 74 08 00 45 00
0010 00 82 20 eb 40 00 80 06 1d c6 0a 01 11 d7 05 fc
0020 99 f1 c3 e0 00 50 db f2 bd c2 de 29 cc 94 50 18
0030 00 ff 48 9c 00 00 47 45 54 20 2f 61 70 69 2f 66
0040 69 6c 65 2f 67 65 74 2d 66 69 6c 65 2f 32 39 38
0050 34 32 2e 70 73 31 20 48 54 54 50 2f 31 2e 31 0d
0060 0a 48 6f 73 74 3a 20 35 2e 32 35 32 2e 31 35 33
0070 2e 32 34 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e
0080 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 0d 0a
Activate Windows
Go to Settings to activate Windows.
Internet Protocol Version 4 (ip), 20 bytes
Packets: 39427 · Displayed: 1253 (3.2%)
Profile: Default


2025-01-22-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 10.1.17.215 and http
No. Time Source Destination Protocol Length Hypertext Transfer Protocol Info
111 2025-01-22 11:45:01.411106 10.1.17.215 23.220.102.9 HTTP 165 ✓ GET /connecttest.txt HTTP/1.1
118 2025-01-22 11:45:01.460188 23.220.102.9 10.1.17.215 HTTP 241 ✓ HTTP/1.1 200 OK (text/plain)
5031 2025-01-22 11:45:56.827936 10.1.17.215 5.252.153.241 HTTP 371 ✓ GET /api/file/get-file/264872 HTTP/1.1
5033 2025-01-22 11:45:56.994779 5.252.153.241 10.1.17.215 HTTP 819 ✓ HTTP/1.1 200 OK
5063 2025-01-22 11:45:58.675869 10.1.17.215 5.252.153.241 HTTP 144 ✓ GET /api/file/get-file/29842.ps1 HTTP/1.1
5071 2025-01-22 11:45:58.839486 5.252.153.241 10.1.17.215 HTTP 555 ✓ HTTP/1.1 200 OK
5073 2025-01-22 11:45:58.896228 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
5075 2025-01-22 11:45:59.094458 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7279 2025-01-22 11:46:04.132272 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
7299 2025-01-22 11:46:04.299207 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7602 2025-01-22 11:46:09.308509 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
7604 2025-01-22 11:46:09.474149 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7688 2025-01-22 11:46:14.480958 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
7690 2025-01-22 11:46:14.674308 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7696 2025-01-22 11:46:19.680655 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
Internet Protocol Version 4, Src: 10.1.17.215, Dst: 5.252.153.241
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 130
Identification: 0x20eb (8427)
010. .... = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: TCP (6)
Header Checksum: 0x1dc6 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.1.17.215
Destination Address: 5.252.153.241
[Stream index: 34]
Transmission Control Protocol, Src Port: 50144, Dst Port: 80, Seq: 1, Ack: 1, Len: 90
Hypertext Transfer Protocol
0000 08 d0 9f c2 3a 46 00 d0 b7 26 4a 74 08 00 45 00
0010 00 82 20 eb 40 00 80 06 1d c6 0a 01 11 d7 05 fc
0020 99 f1 c3 e0 00 50 db f2 bd c2 de 29 cc 94 50 18
0030 00 ff 48 9c 00 00 47 45 54 20 2f 61 70 69 2f 66
0040 69 6c 65 2f 67 65 74 2d 66 69 6c 65 2f 32 39 38
0050 34 32 2e 70 73 31 20 48 54 54 50 2f 31 2e 31 0d
0060 0a 48 6f 73 74 3a 20 35 2e 32 35 32 2e 31 35 33
0070 2e 32 34 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e
0080 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 0d 0a
Activate Windows
Go to Settings to activate Windows.
Internet Protocol Version 4 (ip), 20 bytes
Packets: 39427 · Displayed: 1253 (3.2%)
Profile: Default


2025-01-22-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 10.1.17.215 and http
No. Time Source Destination Protocol Length Hypertext Transfer Protocol Info
111 2025-01-22 11:45:01.411106 10.1.17.215 23.220.102.9 HTTP 165 ✓ GET /connecttest.txt HTTP/1.1
118 2025-01-22 11:45:01.460188 23.220.102.9 10.1.17.215 HTTP 241 ✓ HTTP/1.1 200 OK (text/plain)
5031 2025-01-22 11:45:56.827936 10.1.17.215 5.252.153.241 HTTP 371 ✓ GET /api/file/get-file/264872 HTTP/1.1
5033 2025-01-22 11:45:56.994779 5.252.153.241 10.1.17.215 HTTP 819 ✓ HTTP/1.1 200 OK
5063 2025-01-22 11:45:58.675869 10.1.17.215 5.252.153.241 HTTP 144 ✓ GET /api/file/get-file/29842.ps1 HTTP/1.1
5071 2025-01-22 11:45:58.839486 5.252.153.241 10.1.17.215 HTTP 555 ✓ HTTP/1.1 200 OK
5073 2025-01-22 11:45:58.896228 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
5075 2025-01-22 11:45:59.094458 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7279 2025-01-22 11:46:04.132272 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
7299 2025-01-22 11:46:04.299207 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7602 2025-01-22 11:46:09.308509 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
7604 2025-01-22 11:46:09.474149 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7688 2025-01-22 11:46:14.480958 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
7690 2025-01-22 11:46:14.674308 5.252.153.241 10.1.17.215 HTTP 329 ✓ HTTP/1.1 404 Not Found (text/plain)
7696 2025-01-22 11:46:19.680655 10.1.17.215 5.252.153.241 HTTP 103 ✓ GET /1517096937 HTTP/1.1
Frame 5073: 103 bytes on wire (824 bits), 103 bytes captured (824 bits)
Ethernet II, Src: Intel_26:4a:74 (00:d0:b7:26:4a:74), Dst: Cisco_c2:3a:46 (08:d0:9f:c2:3a:46)
Internet Protocol Version 4, Src: 10.1.17.215, Dst: 5.252.153.241
Transmission Control Protocol, Src Port: 50144, Dst Port: 80, Seq: 91, Ack: 1862, Len: 49
Hypertext Transfer Protocol
GET /1517096937 HTTP/1.1\r\n
Host: 5.252.153.241\r\n
\r\n
[Response in frame: 5075]
[Full request URI: http://5.252.153.241/1517096937]
0000 08 d0 9f c2 3a 46 00 d0 b7 26 4a 74 08 00 45 00
0010 00 59 20 ed 40 00 80 06 1d ed 0a 01 11 d7 05 fc
0020 99 f1 c3 e0 00 50 db f2 be 1c de 29 d3 d9 50 18
0030 00 ff 8f b9 00 00 47 45 54 20 2f 31 35 31 37 30
0040 39 36 39 33 37 20 48 54 54 50 2f 31 2e 31 0d 0a
0050 48 6f 73 74 3a 20 35 2e 32 35 32 2e 31 35 33 2e
0060 32 34 31 0d 0a 0d 0a
Activate Windows
Go to Settings to activate Windows.
Internet Protocol Version 4 (ip), 20 bytes
Packets: 39427 · Displayed: 1253 (3.2%)
Profile: Default



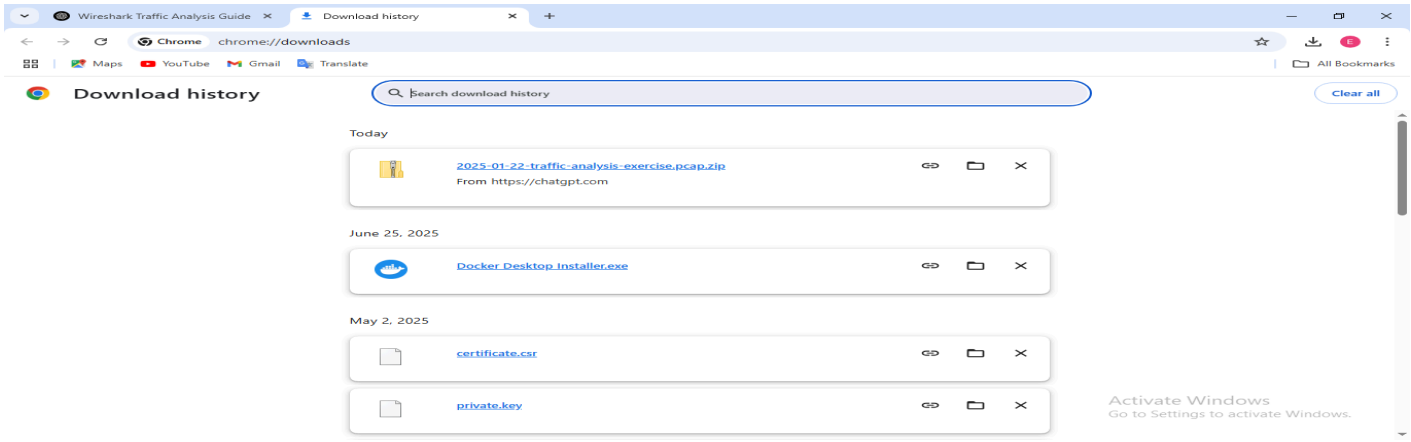


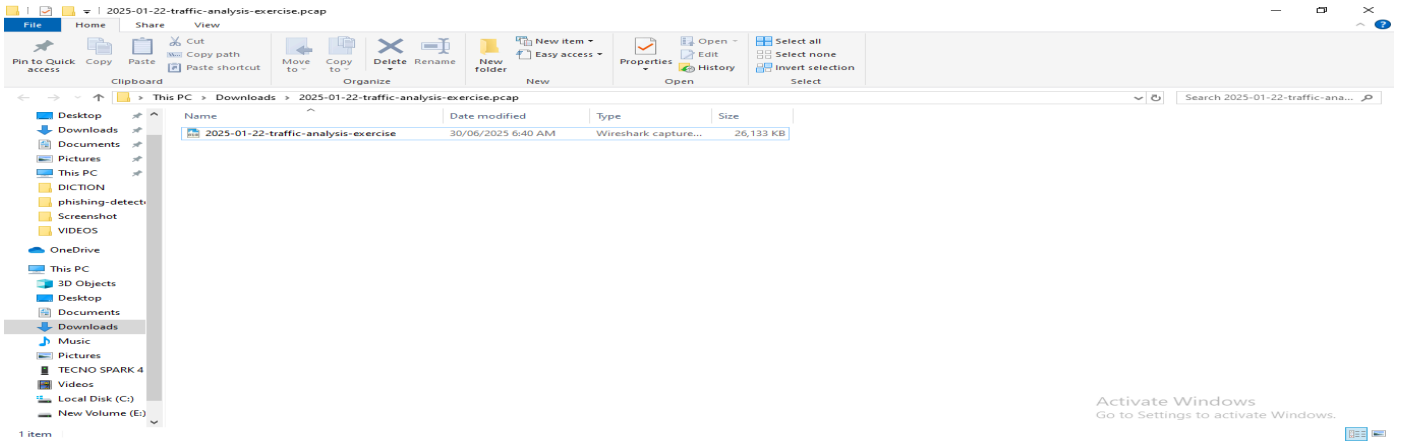
📌7️⃣ Recommendations for Mitigation

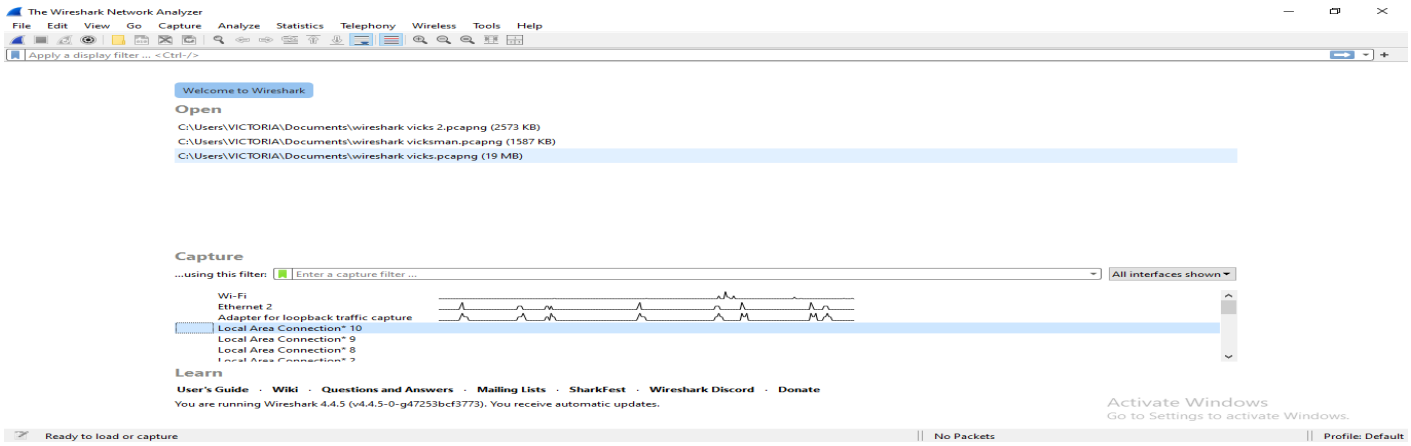
1. Isolate infected host `10.1.17.215` from the network immediately.
2. Block malicious IP addresses `5.252.153.241` and `199.232.214.172`.
3. Perform full endpoint malware scan and forensics.
4. Reset all credentials used on the affected system.
5. Update antivirus and EDR signatures.
6. Conduct a company-wide phishing awareness refresher.
7. Audit Active Directory for suspicious new accounts or privilege escalations.

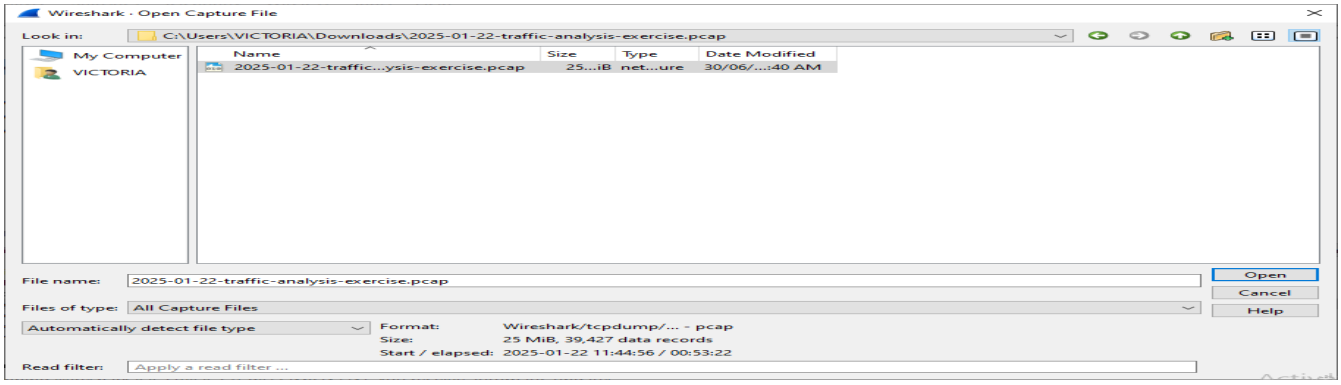
Pcap file:

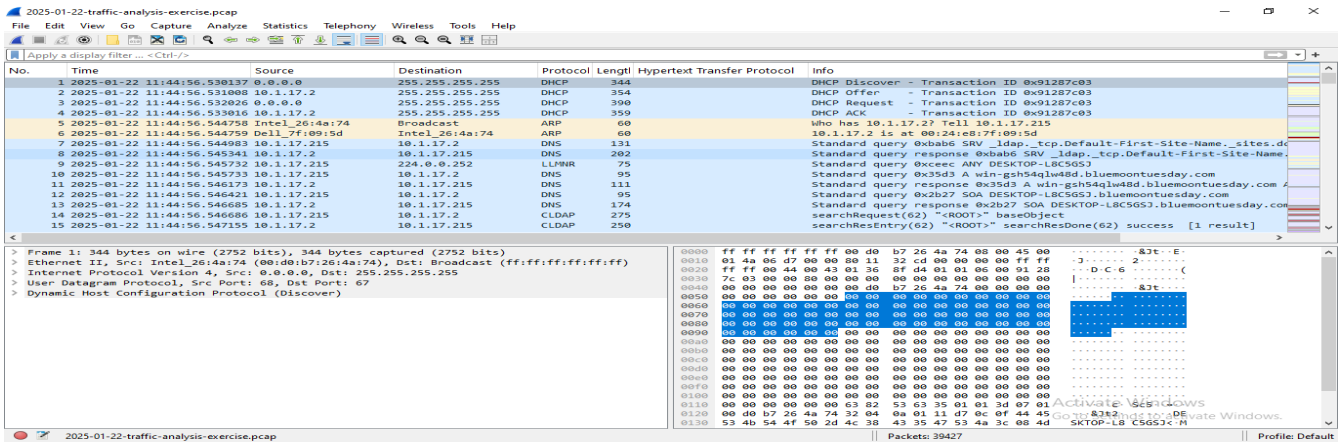
Screenshot of the processes involved in downloading and uploading pcap file on Wireshark:


Wireshark Traffic Analysis Guide
Download history
chrome://downloads
Maps
YouTube
Gmail
Translate
All Bookmarks
Download history
Search download history
Clear all
Today
2025-01-22-traffic-analysis-exercise.pcap.zip
From https://chatgpt.com
June 25, 2025
Docker Desktop Installer.exe
May 2, 2025
certificate.csr
private.key
Activate Windows
Go to Settings to activate Windows.

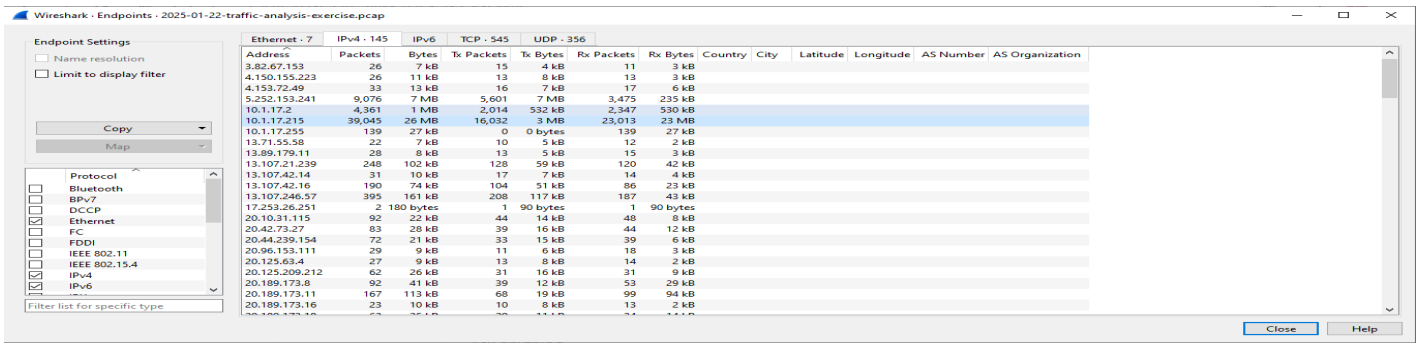

2025-01-22-traffic-analysis-exercise.pcap
File
Home
Share
View
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New folder
New item
Easy access
New
Properties
Open
Edit
History
Open
Select all
Select none
Invert selection
Select
This PC
Downloads
2025-01-22-traffic-analysis-exercise.pcap
Search 2025-01-22-traffic-ana...
Desktop
Documents
Pictures
This PC
DICTION
phishing-detect
Screenshot
VIDEOS
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
TECNO SPARK 4
Videos
Local Disk (C:)
New Volume (E:)
Name
Date modified
Type
Size
2025-01-22-traffic-analysis-exercise
30/06/2025 6:40 AM
Wireshark capture...
26,133 KB
1 item
Activate Windows
Go to Settings to activate Windows.


The Wireshark Network Analyzer
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Open
C:\Users\VICTORIA\Documents\wireshark vicks 2.pcapng (2573 KB)
C:\Users\VICTORIA\Documents\wireshark vicksman.pcapng (1587 KB)
C:\Users\VICTORIA\Documents\wireshark vicks.pcapng (19 MB)
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Wi-Fi
Ethernet 2
Adapter for loopback traffic capture
Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
You are running Wireshark 4.4.5 (v4.4.5-0-g47253bcf3773). You receive automatic updates.
Activate Windows
Go to Settings to activate Windows.
Ready to load or capture
No Packets
Profile: Default





Screenshot of the method i used to identify the Filtered suspected internal host:



Note:
Cross-referenced the identified Indicators of Compromise (IOCs) — such as `play.vidyard.com`, beaconing IP addresses, and suspicious HTTP requests — against the provided threat intelligence resources (LinkedIn and Twitter/X posts from Unit42). The analysis confirmed alignment between the captured network traffic and the reported malicious activity patterns described in those sources.

✅ Conclusion

The investigation into the suspicious network activity originating from host **10.1.17.215** successfully confirmed a malware infection incident within the BluemoonTuesday corporate network. Through detailed Wireshark traffic analysis, multiple Indicators of Compromise (IOCs) were identified — including malicious file downloads, repeated Command and Control (C2) beaconing attempts, and suspicious DNS queries.

The infection chain was reconstructed, beginning with an initial malicious HTTP download from **5.252.153.241**, followed by subsequent PowerShell script retrievals, repeated unauthorized external communications, and secondary payload downloads from **199.232.214.172**.

These findings were cross-referenced with the provided **threat intelligence resources from Unit42 on LinkedIn and Twitter/X**, validating that the observed malicious domains and network behavior matched known threat actor tactics documented in those reports.

In response, immediate containment and remediation actions were recommended, including host isolation, network blocklists, malware scans, credential resets, and staff awareness training. This case underscores the importance of proactive traffic monitoring, timely incident response, and integrating threat intelligence into SOC workflows.

The incident has been fully documented with supporting evidence, including decoded packet captures, analysis walkthroughs, IOC tables, and recommended mitigations for the organization’s security leadership team.