Project Report

Project Title

Network Traffic Analysis Using Wireshark And Zeek

Submitted By: Harsh Vishwakarma

BACHELOR OF TECHNOLOGY

in

(COMPUTER SCIENCE & ENGINEERING)

ASHOKA INSTITUTE OF TECHNOLOGY & MANAGEMENT VARANASI

Submission Date: 17/07/2025

Supervisor's Name: Hrushikesh Dinkar Sir

Table of Contents

Introduction

This project is based on network traffic analysis, which is an essential part of cybersecurity and involves examining data packets traveling over a network. As cyber threats become more advanced, the ability to analyze real-time data for anomalies is becoming critical to the security of systems.

This part explains what the project aims to achieve: Monitoring, capturing, and analyzing network traffic using Wireshark and Zeek in a controlled laboratory. Traffic such as **DNS queries**, **HTTP GET** and **POST requests**, as well as **TLS** handshakes were created and analyzed for signs of malware infection, encrypted command and control communications, or **DNS tunneling**.

I chose this project because of my interest in intrusion detection and traffic monitoring, which are important skills for a cybersecurity analyst. The objective is to simulate real-world traffic, capture it using Wireshark, and analyze it using Zeek to identify anomalies or threats.

The tools used include Wireshark, a GUI-based packet analyzer, and Zeek, a powerful traffic analysis tool that logs detailed network behavior. This dual-tool approach provides deep visibility into both packet-level and session-level traffic.

Methodology

Tools and Technologies Used

- **Wireshark:** GUI-based network protocol analyzer used for packet capture and live traffic analysis.
- **Zeek (Bro):** Command-line-based network security monitor that inspects traffic and generates logs like conn.log, dns.log, http.log.
- **Kali Linux:** Host OS for running Wireshark and Zeek.
- **PCAP Files:** Used for replaying traffic during offline analysis.

Step-by-Step Approach

1. **Lab Setup**
    - Created a controlled network using Kali Linux and another VM or device to generate traffic (ping, DNS lookup, HTTP request).

2. **Packet Capture with Wireshark**
    - Applied filters: http, dns, tcp.port==80, tcp.flags.syn==1
    - Captured live traffic like HTTP browsing and DNS queries.

3. **Zeek Log Analysis**
    - Installed and ran Zeek on the same captured PCAP files.
    - Generated logs like:
        - conn.log – details of all connections.
        - dns.log – all DNS queries and responses.
        - http.log – HTTP request and response logs.

4. **Anomalies Detection**
    - **Wireshark-based Detection:**

➢ Identified TCP retransmissions and possible SYN flood patterns.
➢ Detected repeated HTTP POSTs and suspicious executable downloads.

- **Zeek-based Detection:**

➢ Logged failed DNS queries and use of DDNS services.
➢ Flagged unusual ports, malformed TLS handshakes, and encrypted traffic inconsistencies.

5. **Graphical Visualization**
    - Wireshark's Protocol Hierarchy and IO Graphs used to visualize packet flow.

Results and Discussion

Results

- **Wireshark Observations:**
  - High number of TCP SYN packets without ACK (potential scan).
  - Repeated DNS queries indicating possible misconfiguration or tunneling.
  - Multiple HTTP requests with suspicious user agents.
- **Zeek Observations:**
  - **dns.log:** Identified multiple unresolved domain names.
  - **conn.log:** Detected irregular connection attempts on port 445 and 3389.
  - **http.log:** Abnormal URLs with encoded payloads.

Statistics

- **Protocol Hierarchy:** Showed DNS, HTTP, TCP, and others.
- **IO Graph:** Spikes observed during DNS flood attempt.

Challenges Faced

- Huge amount of traffic made it difficult to filter manually.
- Interpreting Zeek logs required learning log formats and scripting.
- Network noise sometimes masked real issues.

Network Traffic Analysis Across Multiple PCAP Files (1 to 7.pcap)

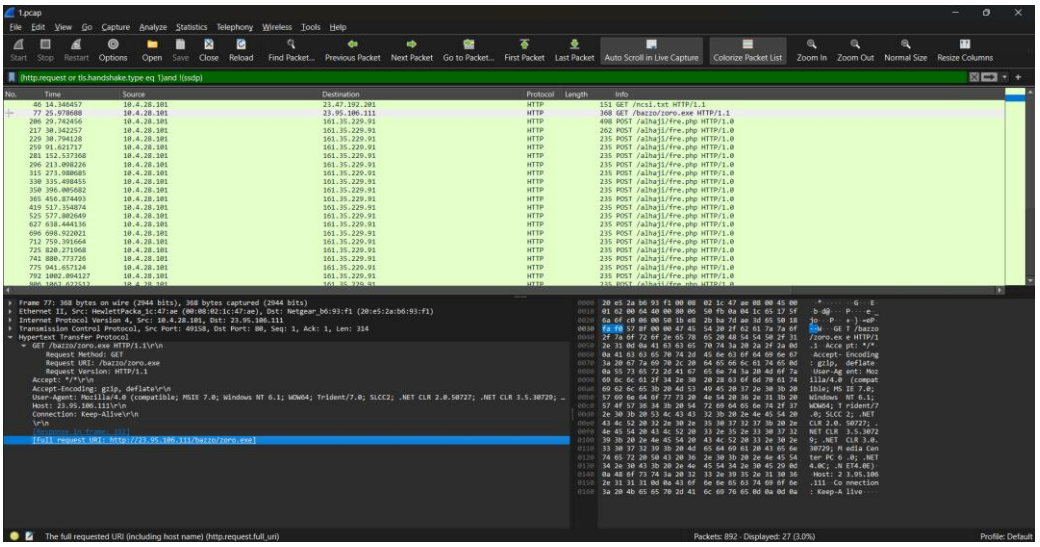
1. Analysis of 1.pcap – Suspicious HTTP POST and Executable Downloads

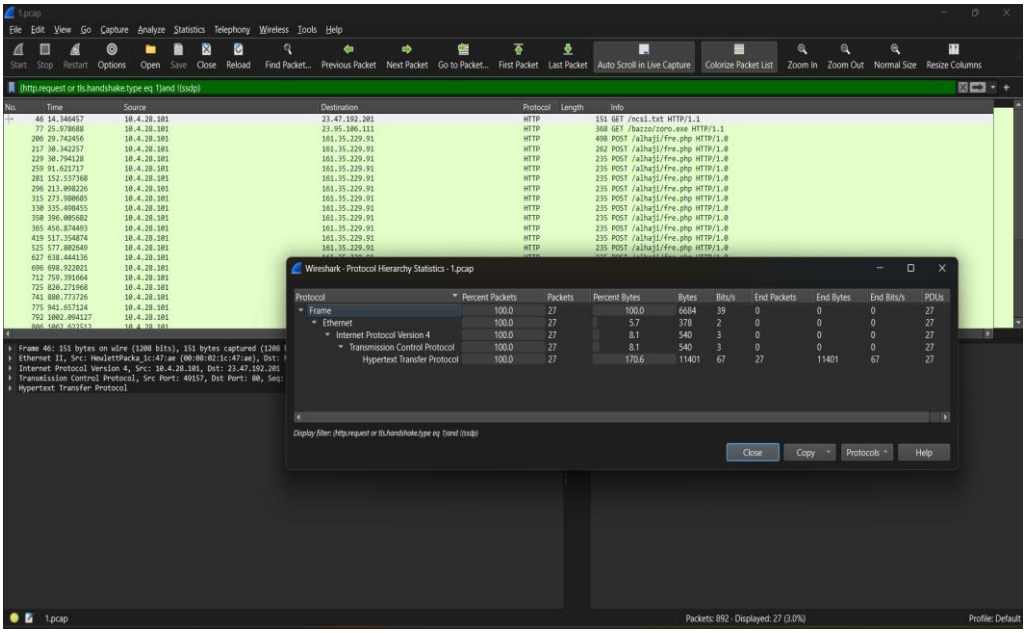
Filter uses: (http.request or tls.handshake.type eq 1)and !(ssdp)
Frame No. 206–887
Source IP: 10.4.28.101
Destination IP: 161.35.229.91
Method: POST
URL/Path: /alhaji/fre.php
Suspicious? Very Suspicious
Reason: Consistent HTTP POST to the same PHP file indicates possible data exfiltration or beaconing

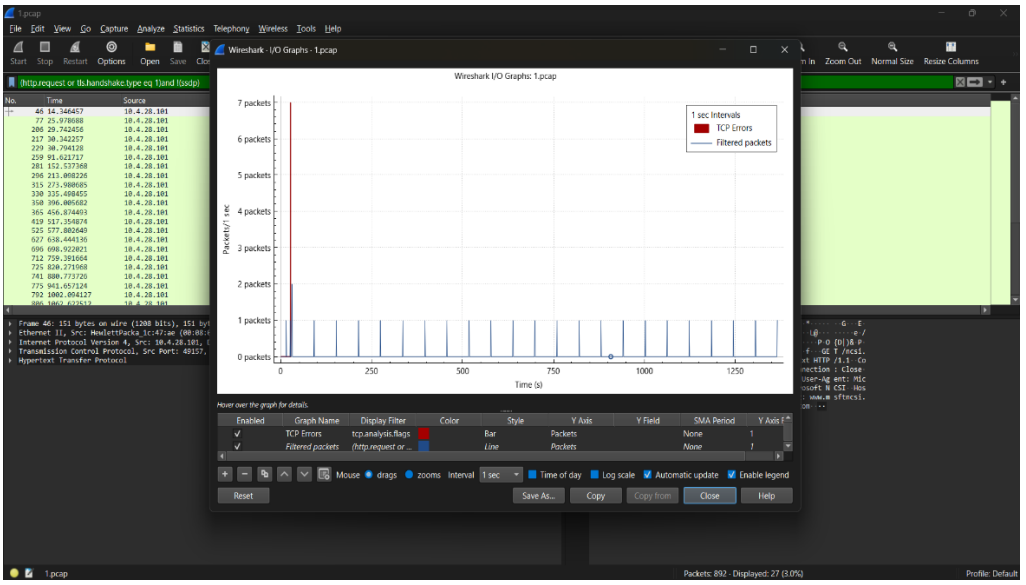
Filter uses: http.request or http contains "zoro.exe"
Frame No: 77
Source IP: 10.4.28.101
Destination IP: 23.95.106.111
Method: GET
URL/Path: /bazzo/zoro.exe
Suspicious?: Yes
Reason: Requesting a .exe file from an unknown domain is highly suspicious, especially in a context where the same host (10.4.28.101) is involved in multiple other suspicious POST requests. It may indicate: Malware download, Payload delivery phase of an attack, Initial infection vector

Filter uses: http.request and http contains "fre.php"
Frame No: 217, 229
Source IP: 10.4.28.101
Destination IP: 161.35.229.91
Method: POST
URL/Path: /alhaji/fre.php
Suspicious?: Yes
Reason: There are dozens of repeated HTTP POST requests to the same PHP script fre.php, all returning 404 Not Found. This pattern suggests:

- Possible data exfiltration or C2 communication
- Use of a backdoor script that might have been removed
- Automation via script or malware (due to exact repetition)







2. Analysis of 2.pcap – DNS Anomalies and WPAD Activity

Filter uses: dns.qry.name == "gomuzigak.com"
Frame No: 4176
Source IP: 10.5.31.139
Destination IP: 10.5.31.5
Method: DNS A query
URL/Path: gomuzigak.com
Suspicious?: Yes
Reason:

- Domain gomuzigak.com does not appear to be associated with any legitimate service.
- Name is non-standard/random, possibly used in C2 or phishing.
- Needs further threat intelligence or WHOIS lookup.

Filter uses: dns.qry.name contains "wpad"
Frame No: Multiple (e.g., 1476, 3783, 9798, 11221, 11801)
Source IP: 10.5.31.139
Destination IP: 10.5.31.5
Method: DNS A query
URL/Path: wpad.roadtoruin.digital, wpad.mshome.net
Suspicious?: Possibly
Reason:

- Repeated WPAD queries can indicate proxy auto-discovery activity.
- If misconfigured or maliciously intercepted, WPAD can be exploited to redirect traffic (Man-in-the-Middle attacks).
- Verify if this is normal behavior in your AD/domain setup or something unusual.

Filter uses: dns.qry.name contains ".roadtoruin.digital"
Frame No: Multiple (e.g., 11122, 11209, 11355)
Source IP: 10.5.31.139
Destination IP: 10.5.31.5
Method: DNS A query
URL/Path: njnpafxoj.roadtoruin.digital, dcknqlwwqj.roadtoruin.digital**, etc.**
Suspicious?: Yes
Reason:

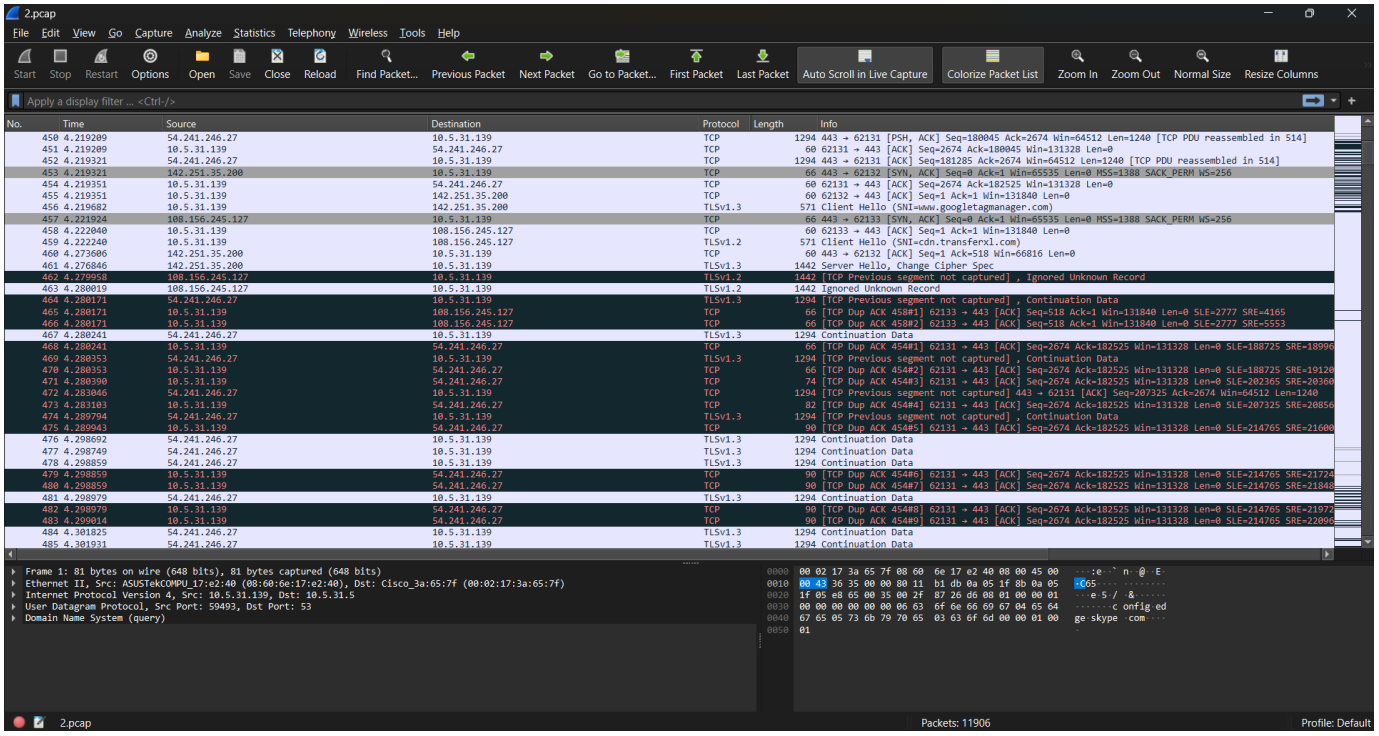
- These hostnames (njnpafxoj, dcknqlwwqj) appear randomly generated, indicating:
  - Malware with Domain Generation Algorithm (DGA)
  - Beaconing to unavailable hosts
- Should check endpoint behavior, look for malware traces.

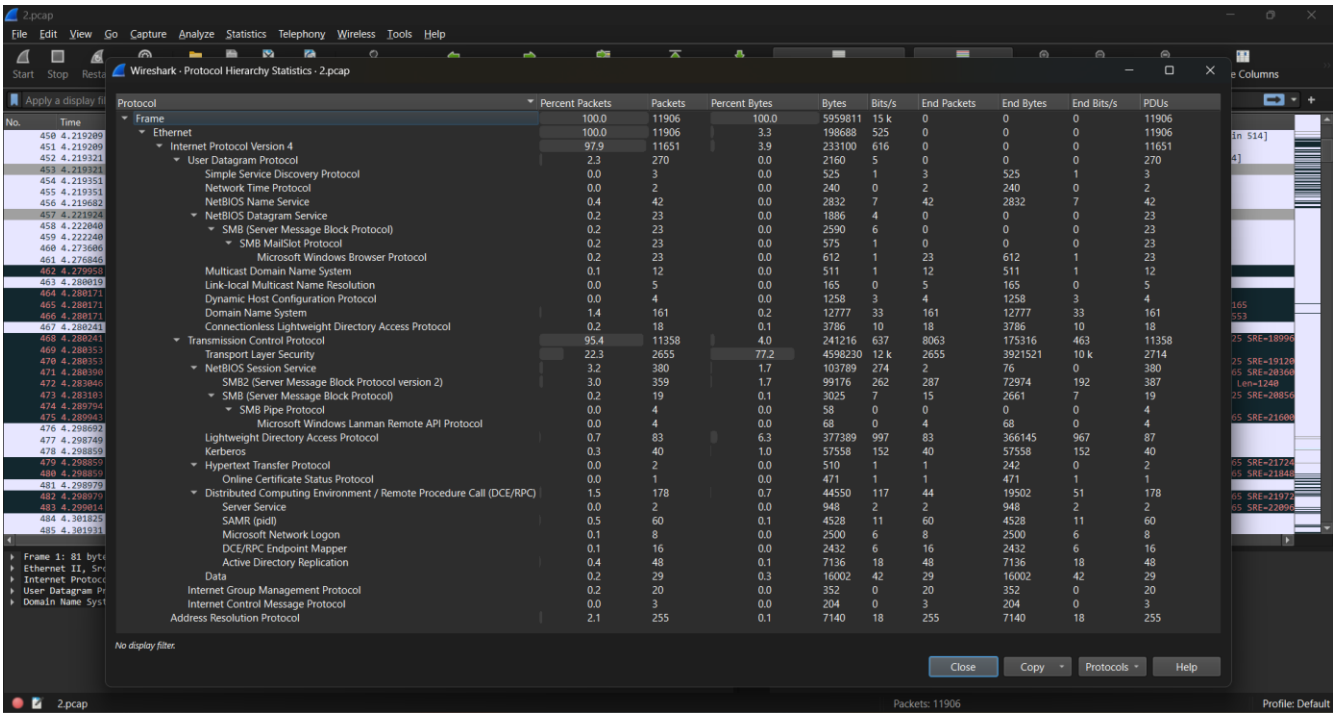
Filter uses: icmp.type == 5
Frame No: 11106
Source IP: 10.5.31.1
Destination IP: 10.5.31.139
Method: ICMP Redirect (Network)
URL/Path: *N/A*
Suspicious?: Yes
Reason:

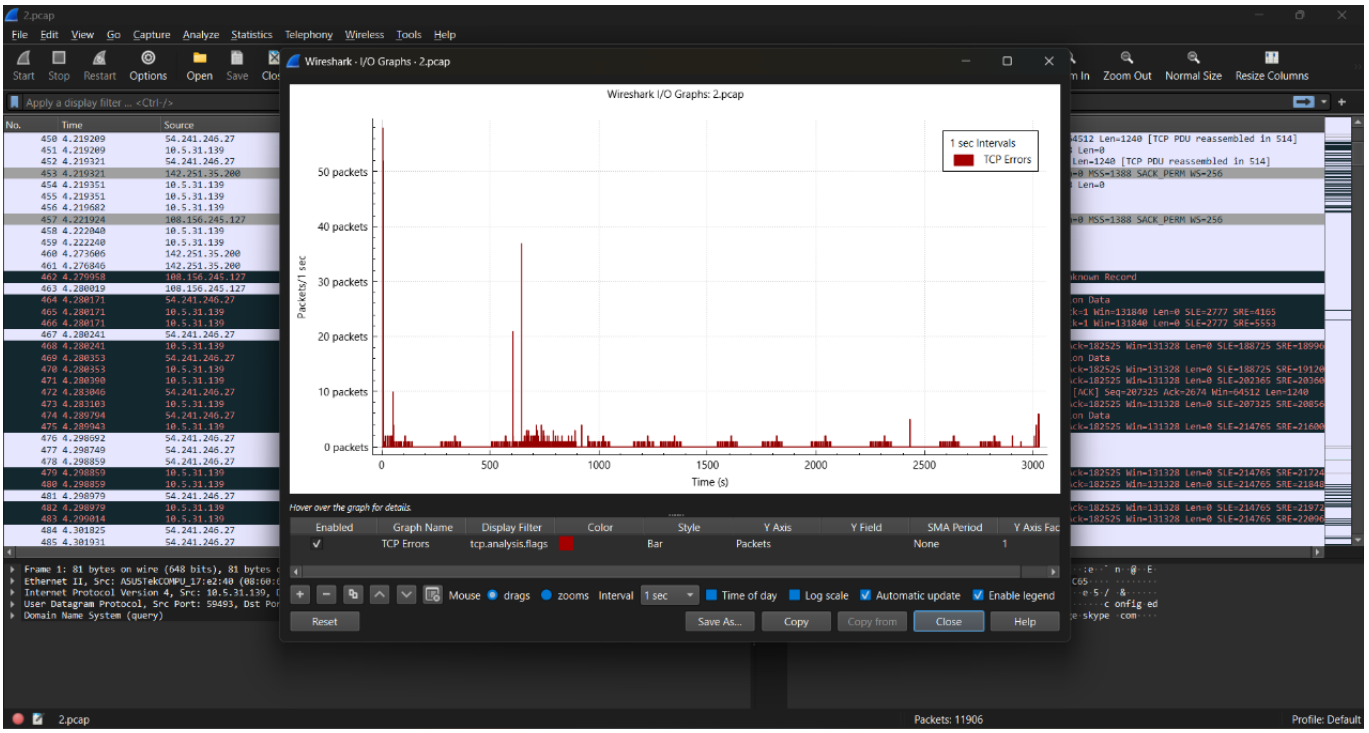
- This message tells host 10.5.31.139 to use a different route for some destination.
- Can be a sign of misconfiguration or Man-in-the-Middle (MitM) attempt.
- Must check routing policies or gateway logs to validate.

Filter uses: cldap
Frame No: 3546
Source IP: 10.5.31.139
Destination IP: 10.5.31.5
Method: searchRequest "<ROOT>"
URL/Path: baseObject
Suspicious?: Potentially suspicious
Reason: CLDAP queries may be abused for reflection attacks
Port Number: 389 (UDP)

Filter uses: llmnr
Frame No: 11041
Source IP: 169.254.114.24
Destination IP: 224.0.0.252
Method: Standard query
URL/Path: DESKTOP-JGTCUDZ
Suspicious?: Potentially suspicious
Reason: LLMNR can be exploited for spoofing attacks
Port Number: 5355 (UDP)




Wireshark · Protocol Hierarchy Statistics · 2.pcap
Protocol
Percent Packets
Packets
Percent Bytes
Bytes
Bits/s
End Packets
End Bits/s
PDUs
Frame 100.0 11906 100.0 5959811 15 k 0 0 11906
Ethernet 100.0 11906 3.3 198688 525 0 0 11906
Internet Protocol Version 4 97.9 11651 3.9 233100 616 0 0 11651
User Datagram Protocol 2.3 270 0.0 2160 5 0 0 270
Simple Service Discovery Protocol 0.0 3 0.0 525 1 3 525 1 3
Network Time Protocol 0.0 2 0.0 240 0 2 240 0 2
NetBIOS Name Service 0.4 42 0.0 2832 7 42 2832 7 42
NetBIOS Datagram Service 0.2 23 0.0 1886 4 0 0 0 23
SMB (Server Message Block Protocol) 0.2 23 0.0 2590 6 0 0 0 23
SMB MailSlot Protocol 0.2 23 0.0 575 1 0 0 0 23
Microsoft Windows Browser Protocol 0.2 23 0.0 612 1 23 612 1 23
Multicast Domain Name System 0.1 12 0.0 511 1 12 511 1 12
Link-local Multicast Name Resolution 0.0 5 0.0 165 0 5 165 0 5
Dynamic Host Configuration Protocol 0.0 4 0.0 1258 3 4 1258 3 4
Domain Name System 1.4 161 0.2 12777 33 161 12777 33 161
Connectionless Lightweight Directory Access Protocol 0.2 18 0.1 3786 10 18 3786 10 18
Transmission Control Protocol 95.4 11358 4.0 241216 637 8063 175316 463 11358
Transport Layer Security 22.3 2655 77.2 4598230 12 k 2655 3921521 10 k 2714
NetBIOS Session Service 3.2 380 1.7 103789 274 2 76 0 380
SMB2 (Server Message Block Protocol version 2) 3.0 359 1.7 99176 262 287 72974 192 387
SMB (Server Message Block Protocol) 0.2 19 0.1 3025 7 15 2661 7 19
SMB Pipe Protocol 0.0 4 0.0 58 0 0 0 0 4
Microsoft Windows Lanman Remote API Protocol 0.0 4 0.0 68 0 4 68 0 4
Lightweight Directory Access Protocol 0.7 83 6.3 377389 997 83 366145 967 87
Kerberos 0.3 40 1.0 57558 152 40 57558 152 40
Hypertext Transfer Protocol 0.0 2 0.0 510 1 1 242 0 2
Online Certificate Status Protocol 0.0 1 0.0 471 1 1 471 1 1
Distributed Computing Environment / Remote Procedure Call (DCE/RPC) 1.5 178 0.7 44550 117 44 19502 51 178
Server Service 0.0 2 0.0 948 2 2 948 2 2
SAMR (pidl) 0.5 60 0.1 4528 11 60 4528 11 60
Microsoft Network Logon 0.1 8 0.0 2500 6 8 2500 6 8
DCE/RPC Endpoint Mapper 0.1 16 0.0 2432 6 16 2432 6 16
Active Directory Replication 0.4 48 0.1 7136 18 48 7136 18 48
Data 0.2 29 0.3 16002 42 29 16002 42 29
Internet Group Management Protocol 0.2 20 0.0 352 0 20 352 0 20
Internet Control Message Protocol 0.0 3 0.0 204 0 3 204 0 3
Address Resolution Protocol 2.1 255 0.1 7140 18 255 7140 18 255
No display filter.
Close
Copy
Protocols
Help
2.pcap
Packets: 11906
Profile: Default


Wireshark · I/O Graphs · 2.pcap
Wireshark I/O Graphs: 2.pcap
1 sec Intervals
TCP Errors
50 packets
40 packets
30 packets
20 packets
10 packets
0 packets
Packets/1 sec
0
500
1000
1500
2000
2500
3000
Time (s)
Hover over the graph for details.
Enabled
Graph Name
Display Filter
Color
Style
Y Axis
Y Field
SMA Period
TCP Errors
tcp.analysis.flags
Bar
Packets
None
Mouse drags zooms
Interval 1 sec
Time of day
Log scale
Automatic update
Enable legend
Reset
Save As...
Copy
Copy from
Close
Help
2.pcap
Packets: 11906
Profile: Default

3. Analysis of 3.pcap – Obfuscated HTTP Traffic and TLS to Unknown Domains

Filter uses: http.request && ip.dst == 208.84.119.179
Frame No: 226
Source IP: 10.5.31.125
Destination IP: 208.84.119.179
Method: GET
URL/Path: /media/18TKQU36V/
Suspicious?: Potentially
Reason: Attempt to access unknown media content; could be linked to suspicious user activity or malware beaconing
Port Number: 80 (HTTP)

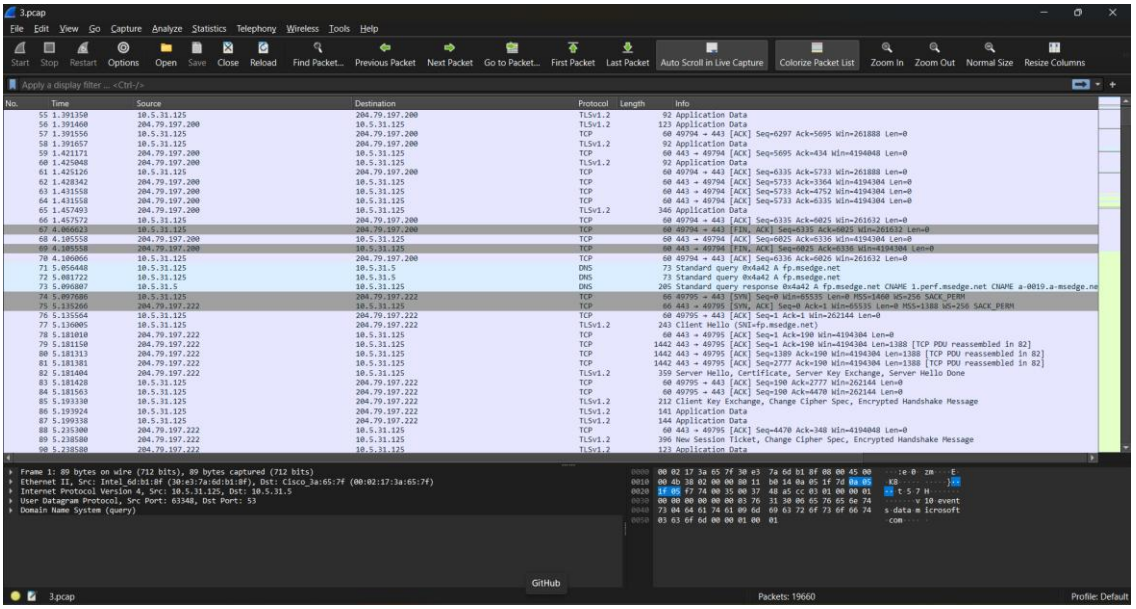
Filter uses: http
Frame No: 236
Source IP: 10.5.31.125
Destination IP: 162.246.59.177
Method: GET
URL/Path: /__MACOSX/7XV9svnWeDq/
Suspicious?: Yes
Reason: Accessing __MACOSX directory is unusual outside of a macOS environment and may indicate file extraction from a malicious ZIP
Port Number: 80

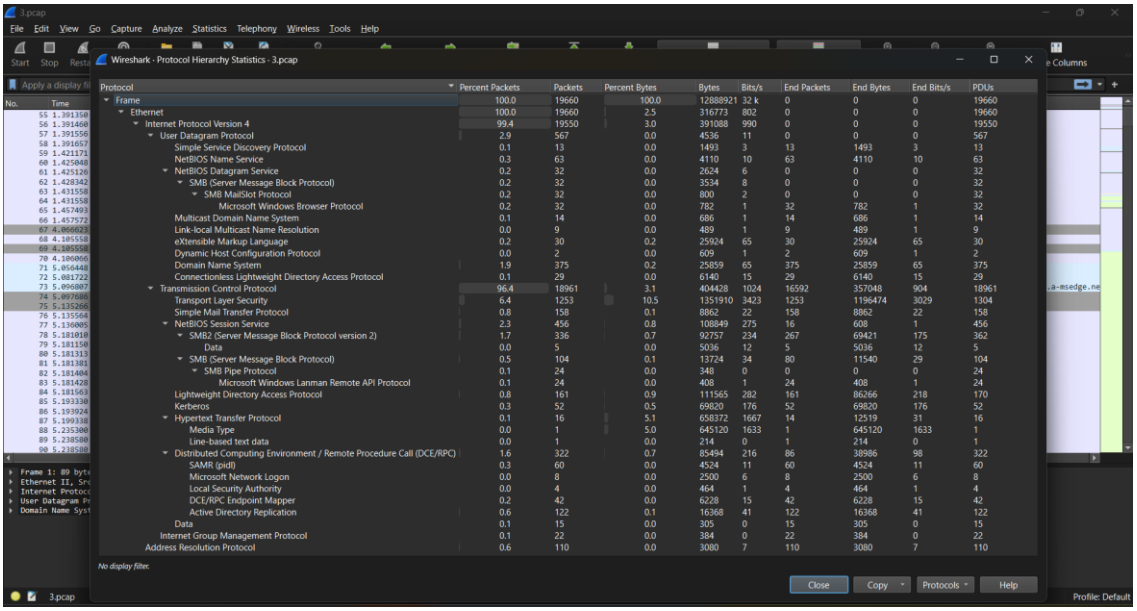
Filter uses: http
Frame No: 320
Source IP: 10.5.31.125
Destination IP: 64.41.86.36
Method: GET
URL/Path: /gJRWFBGvKVVxjE/
Suspicious?: Yes
Reason: Random-looking path on GET request; often associated with malware command and control (C2) or obfuscated traffic
Port Number: 80

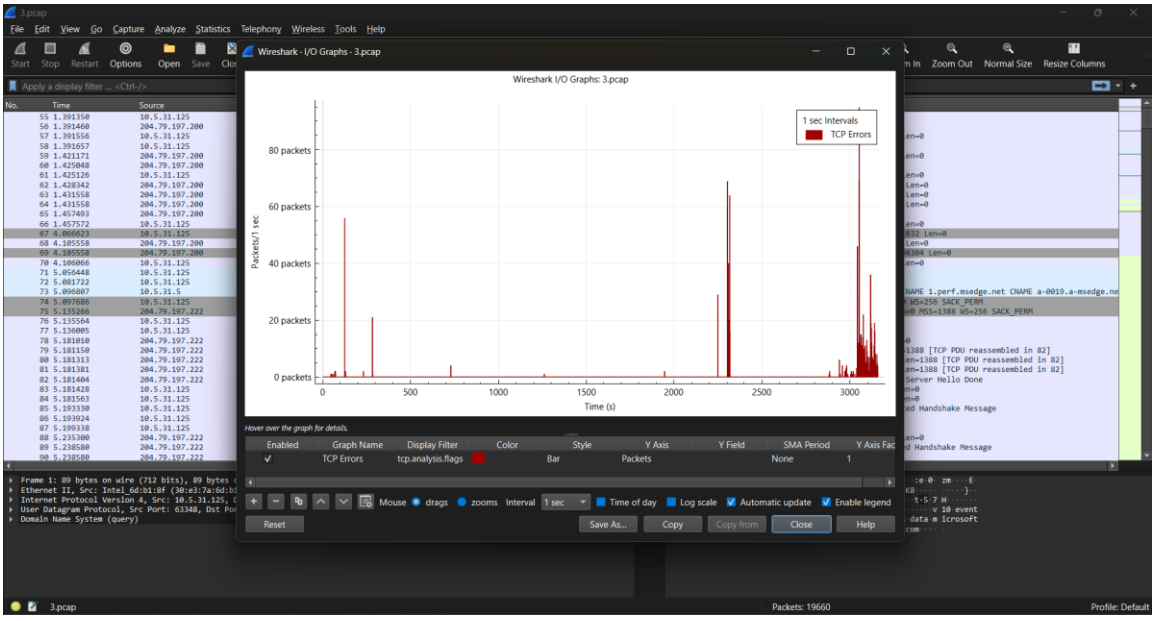
Filter uses: http
Frame No: 985
Source IP: 64.41.86.36
Destination IP: 10.5.31.125
Method: Response
URL/Path: /gJRWFBGvKVVxjE/
Suspicious?: Yes
Reason: Server responded with downloadable content (application/x-msdownload); this could indicate malware being delivered
Port Number: 80

Filter uses: tls.handshake.extensions_server_name == "talbiz.com"
Frame No: 245
Source IP: 10.5.31.125
Destination IP: 162.246.59.177
Method: Client Hello
URL/Path: talbiz.com
Suspicious?: Yes
Reason: Unknown domain, not part of known Microsoft services – investigate reputation
Port Number: 443

Filter uses: ip.addr == 162.215.249.100
Frame No: 17511
Source IP: 10.5.31.125
Destination IP: 162.215.249.100
Method: TLSv1.2
URL/Path: Encrypted (Application Data)
Suspicious?: Yes
Reason: Start of heavy TLS session with repeated large data bursts
Port Number: 49823







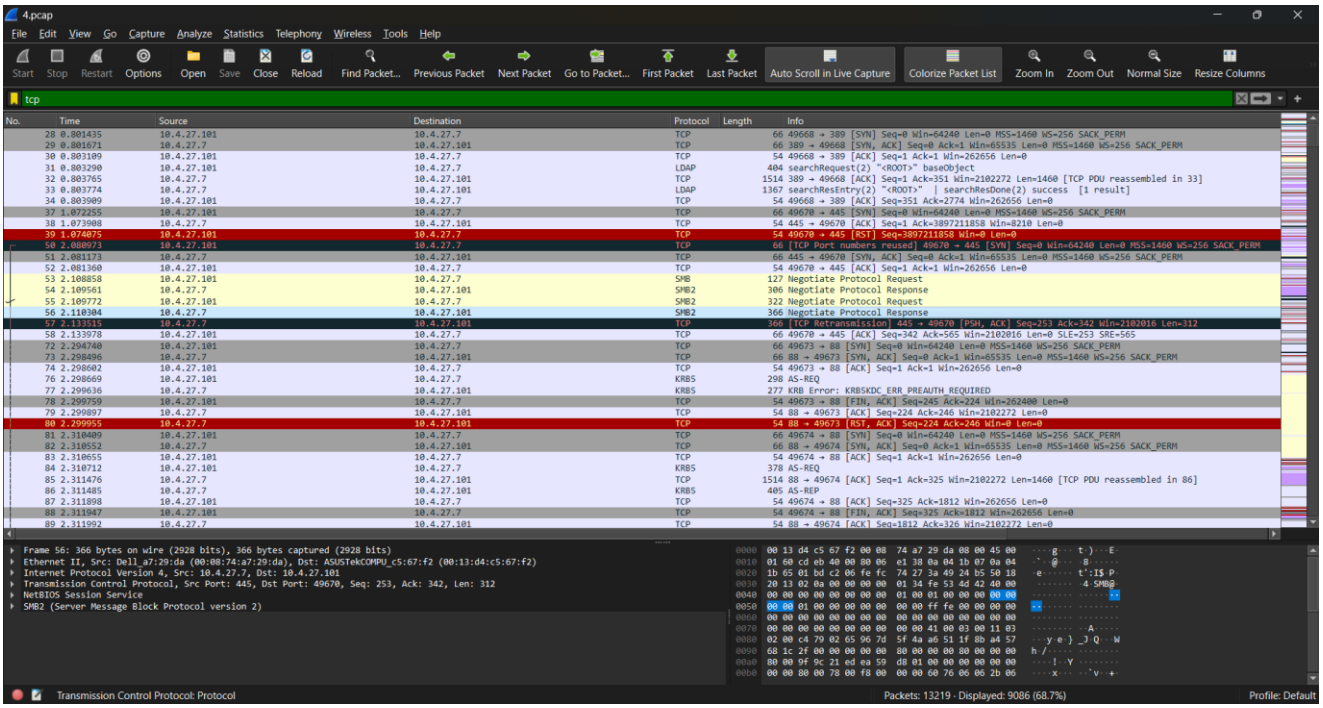
4. Analysis of 4.pcap – SMB and Kerberos Session Resets

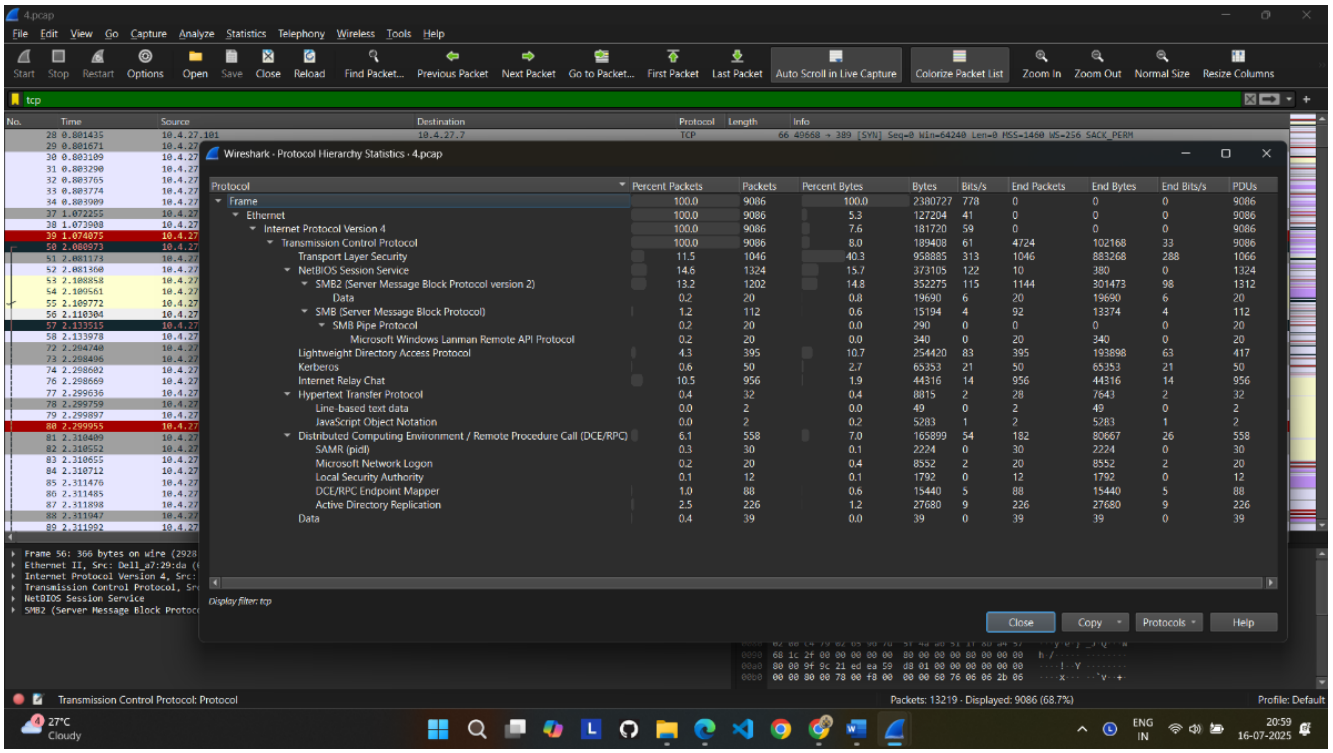
Filter uses: tcp.flags.reset==1
Frame No: 39
Source IP: 10.4.27.101
Destination IP: 10.4.27.7
Method: TCP [RST]
URL/Path: N/A
Suspicious?: Yes
Reason: TCP connection to SMB port was reset immediately after ACK, may indicate error or forced closure
Port Number: 445

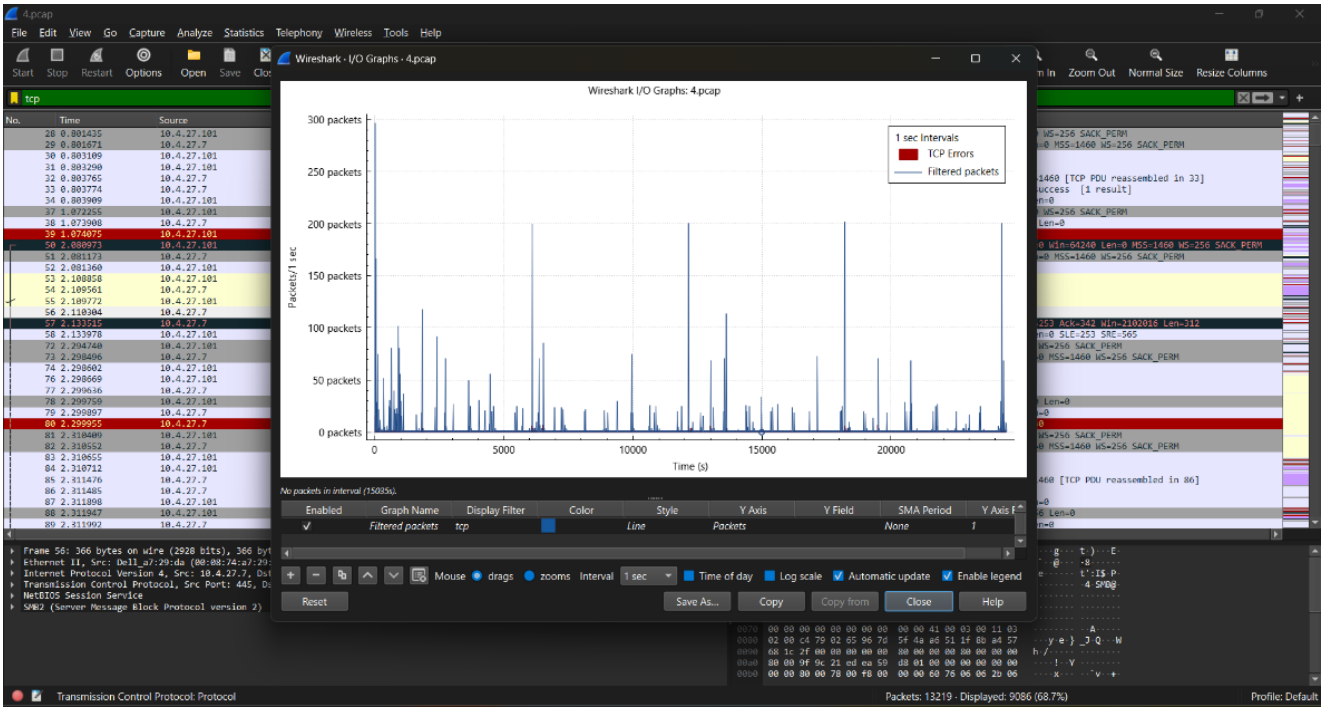
Filter uses: tcp.flags.reset==1
Frame No: 80
Source IP: 10.4.27.7
Destination IP: 10.4.27.101
Method: TCP [RST, ACK]
URL/Path: Kerberos (KRB5)
Suspicious?: Yes
Reason: Server abruptly terminated Kerberos session after AS-REQ failure
Port Number: 88

Filter uses: tcp.flags.reset==1
Frame No: 96
Source IP: 10.4.27.7
Destination IP: 10.4.27.101
Method: TCP [RST, ACK]
URL/Path: Kerberos
Suspicious?: Yes
Reason: Repeated reset indicates session rejection or security policy enforcement
Port Number: 88

Filter uses: tcp.flags.reset==1
Frame No: 214
Source IP: 10.4.27.7
Destination IP: 10.4.27.101
Method: TCP [RST, ACK]
URL/Path: Kerberos
Suspicious?: Yes
Reason: Session reset directly after TGS-REP message – unexpected behavior
Port Number: 88




4.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Protocol Hierarchy Statistics · 4.pcap
Protocol
Percent Packets
Packets
Percent Bytes
Bytes
Bits/s
End Packets
End Bytes
End Bits/s
PDUs
Frame
Ethernet
Internet Protocol Version 4
Transmission Control Protocol
Transport Layer Security
NetBIOS Session Service
SMB2 (Server Message Block Protocol version 2)
Data
SMB (Server Message Block Protocol)
SMB Pipe Protocol
Microsoft Windows Lanman Remote API Protocol
Lightweight Directory Access Protocol
Kerberos
Internet Relay Chat
Hypertext Transfer Protocol
Line-based text data
JavaScript Object Notation
Distributed Computing Environment / Remote Procedure Call (DCE/RPC)
SAMR (pidl)
Microsoft Network Logon
Local Security Authority
DCE/RPC Endpoint Mapper
Active Directory Replication
Data
Display filter: tcp
Close
Copy
Protocols
Help
Transmission Control Protocol: Protocol
Packets: 13219 · Displayed: 9086 (68.7%)
Profile: Default
27°C
Cloudy
ENG
IN
20:59
16-07-2025


4.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · I/O Graphs · 4.pcap
Wireshark I/O Graphs: 4.pcap
300 packets
250 packets
200 packets
150 packets
100 packets
50 packets
0 packets
Packets/1 sec
0
5000
10000
15000
20000
Time (s)
1 sec Intervals
TCP Errors
Filtered packets
No packets in interval (15035s).
Enabled
Graph Name
Display Filter
Color
Style
Y Axis
Y Field
SMA Period
Y Axis F
Filtered packets
tcp
Line
Packets
None
Mouse drags zooms
Interval
1 sec
Time of day
Log scale
Automatic update
Enable legend
Reset
Save As...
Copy
Copy from
Close
Help
Transmission Control Protocol: Protocol
Packets: 13219 · Displayed: 9086 (68.7%)
Profile: Default

5. Analysis of 5.pcap – Malware Download via HTTP and DDNS Usage

Filter uses: http.request.uri contains "ffmpeg.exe"
Frame No: 642
Source IP: 10.4.27.101
Destination IP: 77.231.103.213
Method: HTTP GET
URL/Path: /downloader/ffmpeg.exe
Suspicious?: Yes
Reason: Direct download of executable (.exe) from an external IP; could be part of malware dropper or lateral movement
Port Number: 80

Filter uses: http.response.code == 200
Frame No: 38674
Source IP: 77.231.103.213
Destination IP: 10.4.27.101
Method: HTTP 200 OK
URL/Path: /downloader/ffmpeg.exe
Suspicious?: Yes
Reason: .exe file successfully downloaded over unencrypted HTTP; extremely risky, potential malware
Port Number: 80

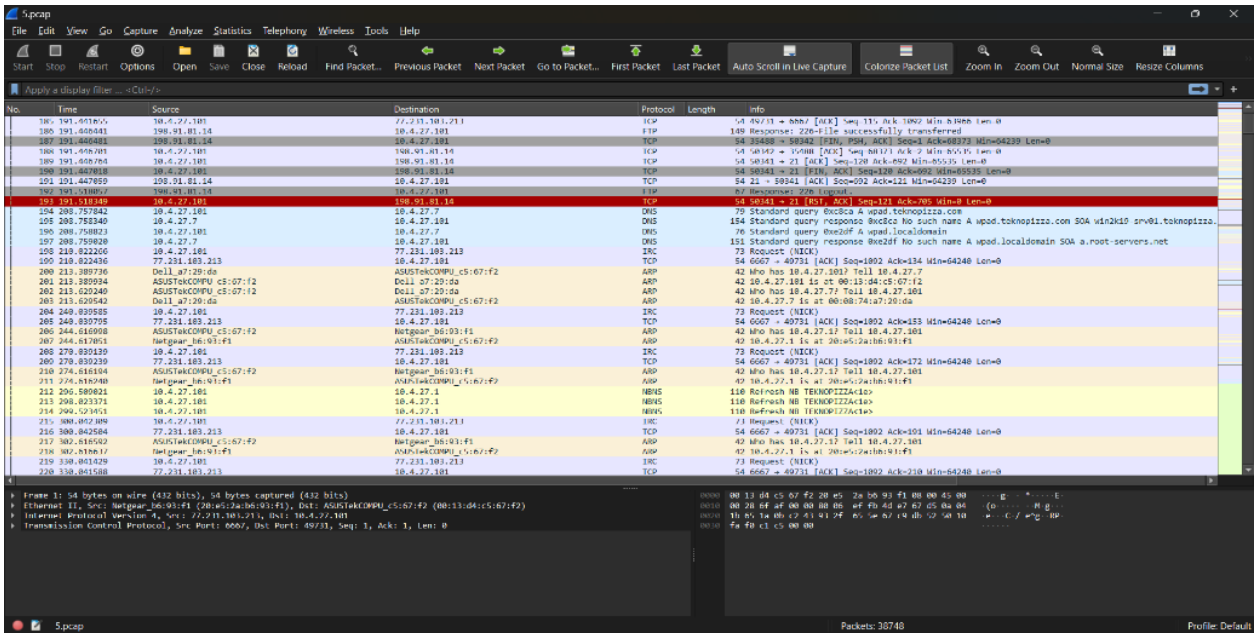
Filter uses: dns.qry.name contains "oreokitkat.ddns.net"
Frame No: 636
Source IP: 10.4.27.101
Destination IP: 10.4.27.7
Method: DNS A Query
URL/Path: oreokitkat.ddns.net
Suspicious?: Yes
Reason: Query to Dynamic DNS (DDNS) domain — often used for C2 (Command and Control) infrastructure in malware
Port Number: 53

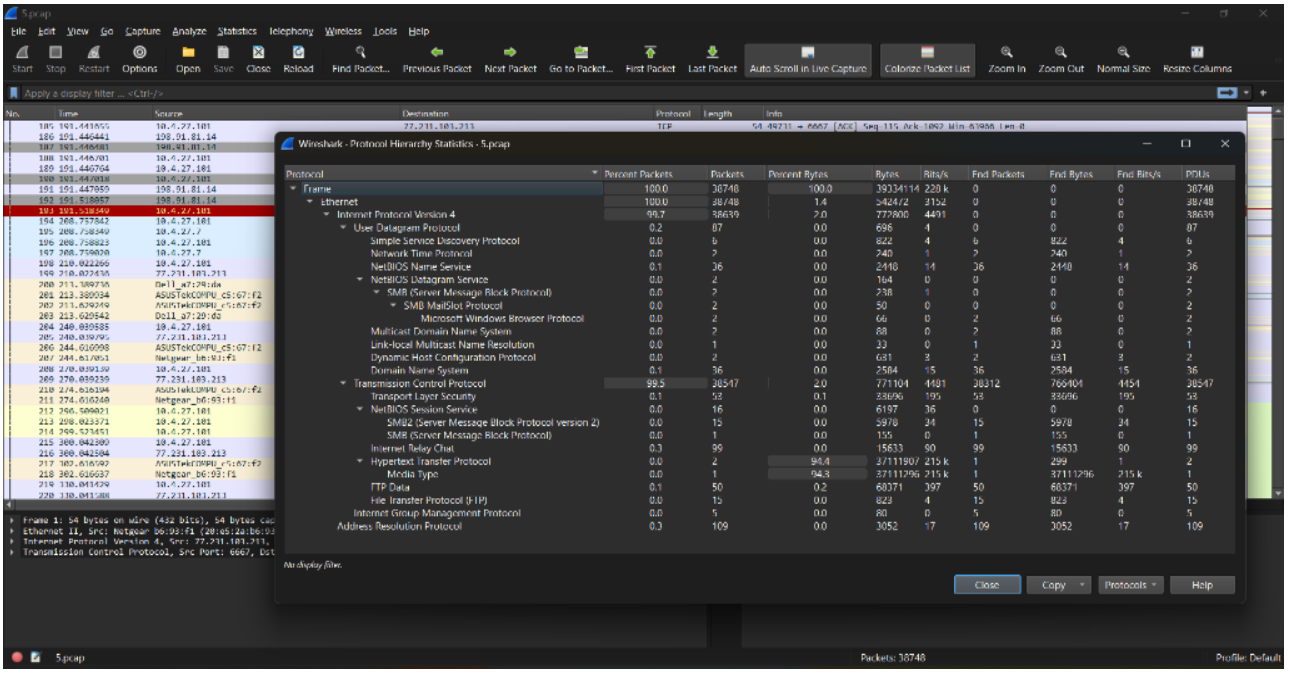
Filter uses: dns.a == 77.231.103.213
Frame No: 638
Source IP: 10.4.27.7
Destination IP: 10.4.27.101
Method: DNS A Response
URL/Path: oreokitkat.ddns.net resolved to 77.231.103.213
Suspicious?: Yes
Reason: DDNS resolution with known match to malicious download server (see HTTP GET /ffmpeg.exe)
Port Number: 53

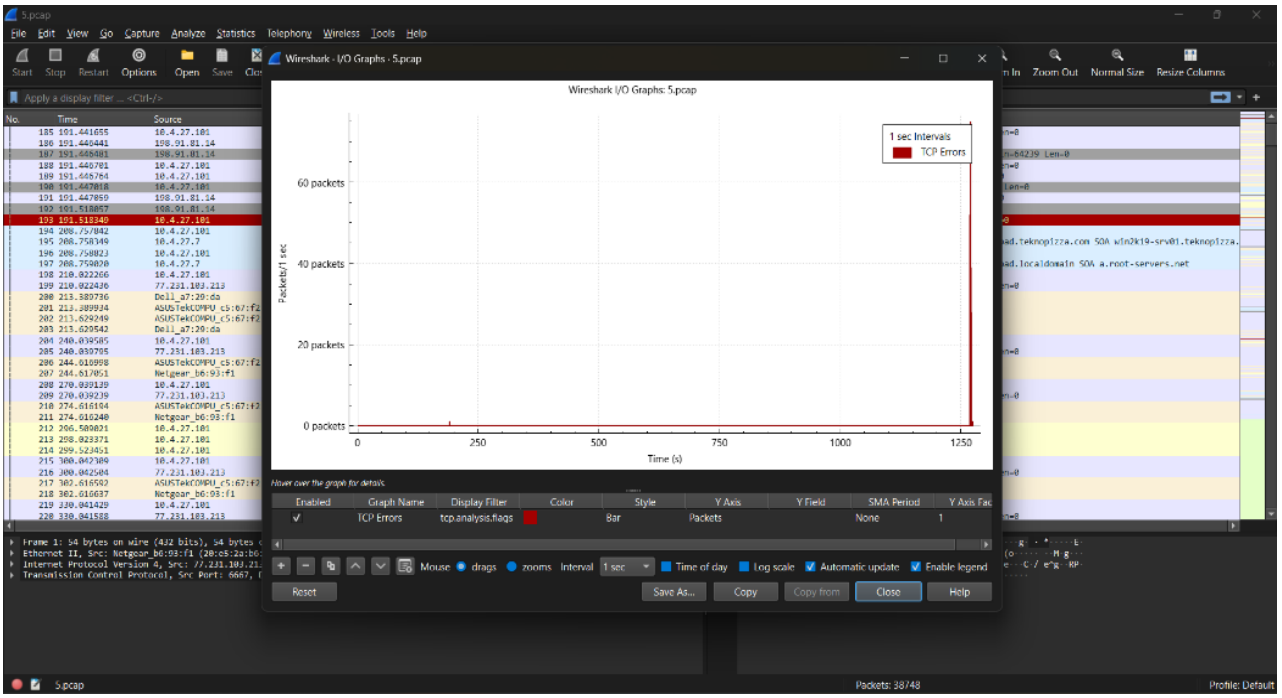
Filter uses: tls.handshake.extensions_server_name contains "settings-win.data.microsoft.com"
Frame No: 38686, 38711 (and many others like 360, 38691, 38715)
Source IP: 10.4.27.101
Destination IP: 52.185.211.133
Method: TLSv1.2 Client Hello
URL/Path: settings-win.data.microsoft.com
Suspicious?: Possibly suspicious
Reason: 3 back-to-back TLS handshakes to the **same endpoint** (52.185.211.133) within ~1 second can indicate:

- Misconfigured client
- Attempt to bypass detection via short-lived sessions
- Malware mimicking Microsoft SNI

Port Number: 443




Wireshark - Protocol Hierarchy Statistics - 5.pcap
Close
Copy
Protocols
Help


Wireshark - I/O Graphs - 5.pcap
Wireshark I/O Graphs: 5.pcap
1 sec Intervals
TCP Errors
60 packets
40 packets
20 packets
0 packets
Packets/1 sec
0
250
500
750
1000
1250
Time (s)
Enabled
Graph Name
Display Filter
Color
Style
Y Axis
Y Field
SMA Period
Y Axis Fac
TCP Errors
tcp.analysis.flags
Bar
Packets
None
1
Mouse
drags
zooms
Interval
1 sec
Time of day
Log scale
Automatic update
Enable legend
Reset
Save As...
Copy
Copy from
Close
Help

6. Analysis of 6.pcap – FTP-Based Data Exfiltration and Insecure Authentication

Filter uses: dns.qry.name contains "ftp"
Frame No: 1
Source IP: 172.16.9.132
Destination IP: 172.16.9.35
Method: DNS Query
URL/Path: ftp.alonsorojasmudanzasnacionales.com
Suspicious?: Yes
Reason: Suspicious FTP domain queried (unusual, not typical for user/system activity)
Port Number: 53

Filter uses: dns.qry.name contains "ftp"
Frame No: 776
Source IP: 172.16.9.132
Destination IP: 172.16.9.35
Method: DNS Query
URL/Path: ftp.alonsorojasmudanzasnacionales.com
Suspicious?: Yes
Reason: Repeated query to the same FTP domain — indicates potential persistence/beaconing
Port Number: 53

Filter uses: dns.qry.name contains "ftp"
Frame No: 1631
Source IP: 172.16.9.132
Destination IP: 172.16.9.35
Method: DNS Query
URL/Path: ftp.alonsorojasmudanzasnacionales.com
Suspicious?: Yes
Reason: Third query to same FTP domain over time — strong sign of automated communication
Port Number: 53

Filter uses: dns.qry.name contains "ftp"

Frame No: 2265
Source IP: 172.16.9.132
Destination IP: 172.16.9.35
Method: DNS Query
URL/Path: ftp.alonsorojasmudanzasnacionales.com
Suspicious?: Yes
Reason: Fourth time querying same FTP domain — likely beaconing or data exfiltration behavior
Port Number: 53

Filter uses: ip.addr == 162.213.251.217 && ftp
Frame No: 29
Source IP: 172.16.9.132
Destination IP: 162.213.251.217
Method: STOR
URL/Path: PW_tsalvaggi-DESKTOP-NHAN2PX_2022_05_17_20_51_08.html
Suspicious?: Yes
Reason: HTML file being uploaded to an external FTP server — indicative of potential data exfiltration
Port Number: 21

Filter uses: ip.addr == 162.213.251.217 && ftp
Frame No: 804
Source IP: 172.16.9.132
Destination IP: 162.213.251.217
Method: STOR
URL/Path: SC_tsalvaggi-DESKTOP-NHAN2PX_2022_05_17_21_11_10.jpeg
Suspicious?: Yes
Reason: JPEG file upload to FTP server — suspicious as it may conceal hidden payload or data
Port Number: 21

Filter uses: ip.addr == 162.213.251.217 && ftp

Frame No: 1659
Source IP: 172.16.9.132
Destination IP: 162.213.251.217
Method: STOR
URL/Path: SC_tsalvaggi-DESKTOP-NHAN2PX_2022_05_17_21_31_10.jpeg
Suspicious?: Yes
Reason: Repeated upload of JPEGs — could indicate use of steganography or repeated data leaks
Port Number: 21

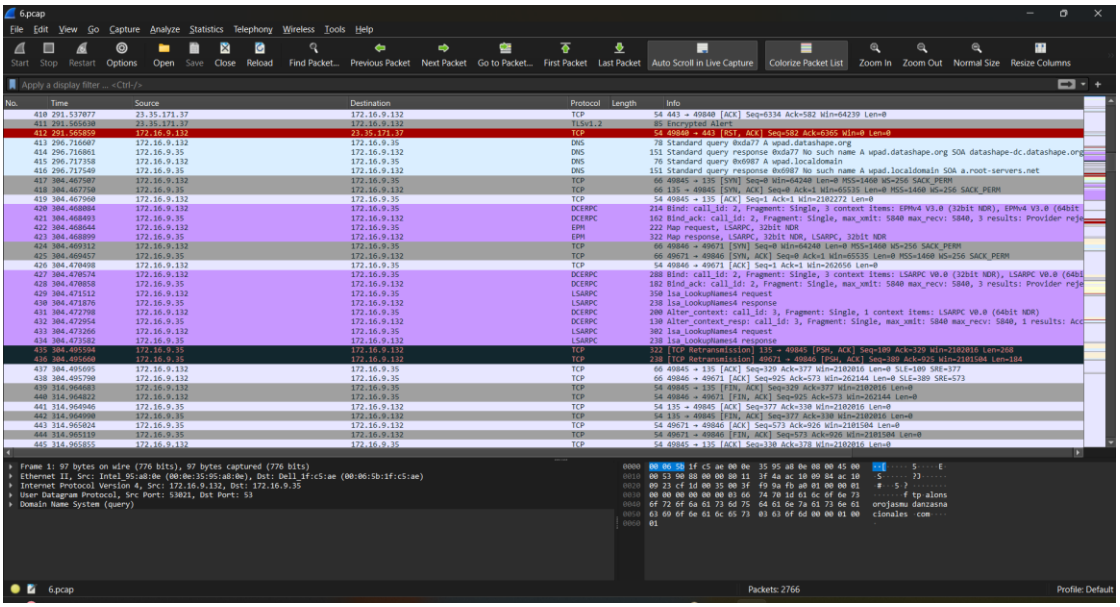
Filter uses: ip.addr == 162.213.251.217 && ftp
Frame No: 2292
Source IP: 172.16.9.132
Destination IP: 162.213.251.217
Method: STOR
URL/Path: SC_tsalvaggi-DESKTOP-NHAN2PX_2022_05_17_21_51_10.jpeg
Suspicious?: Yes
Reason: Continuous file uploads using a pattern — possible automated data exfiltration
Port Number: 21

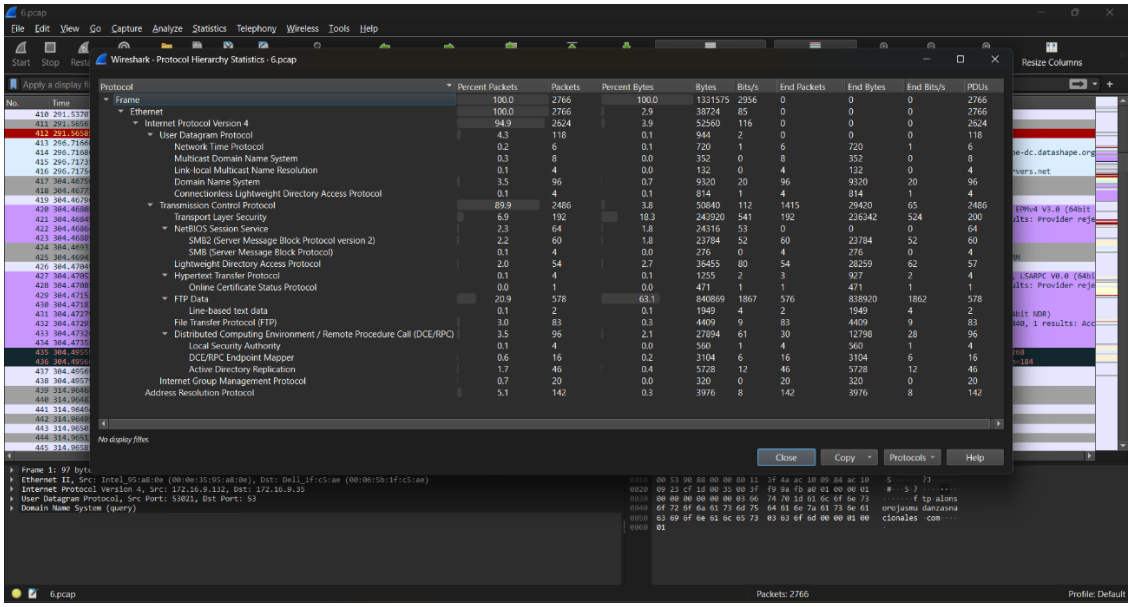
Filter uses: ftp.request.command == "USER" || ftp.request.command == "PASS"
Frame No: 7
Source IP: 172.16.9.132
Destination IP: 162.213.251.217
Method: USER
URL/Path: ama@alonsorojasmudanzasnacionales.com
Suspicious?: Yes
Reason: FTP username observed in plaintext — insecure authentication
Port Number: 21

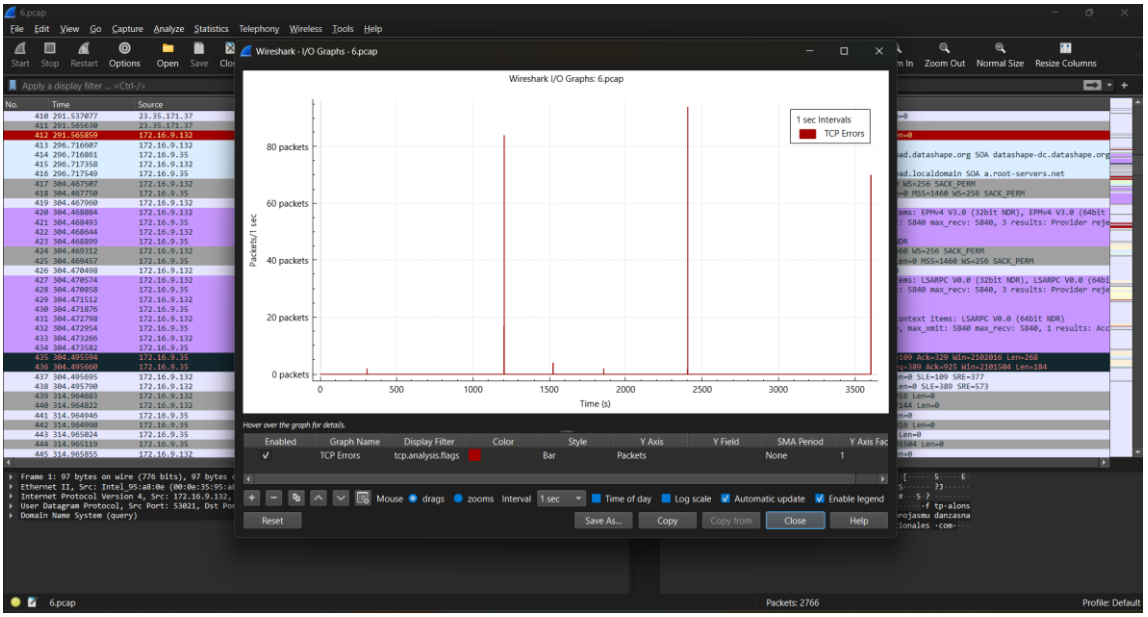
Filter uses: ip.addr == 72.21.91.29 && http

Frame No: 314
Source IP: 172.16.9.132
Destination IP: 72.21.91.29
Method: GET
URL/Path:
/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D
Suspicious?: Yes
Reason: OCSP GET request with encoded certificate string — may indicate verification of a forged certificate or unexpected validation flow
Port Number: 80

Filter uses: ip.addr == 72.21.81.240 && http
Frame No: 2220
Source IP: 172.16.9.132
Destination IP: 72.21.81.240
Method: GET
URL/Path:
/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?ef780060a5173fdb
Suspicious?: Potentially
Reason: Accessing disallowed certificate list (STL) — can be normal, but may indicate security checking after a suspicious certificate chain
Port Number: 80


6.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Start Stop Restart Options Open Save Close Reload Find Packet... Previous Packet Next Packet Go to Packet... First Packet Last Packet Auto Scroll in Live Capture Colorize Packet List Zoom In Zoom Out Normal Size Resize Columns
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
Frame 1: 97 bytes on wire (776 bits), 97 bytes captured (776 bits)
Ethernet II, Src: Intel_95:a8:0e (00:0e:35:95:a8:0e), Dst: Dell_1f:c5:ae (00:06:5b:1f:c5:ae)
Internet Protocol Version 4, Src: 172.16.9.132, Dst: 172.16.9.35
User Datagram Protocol, Src Port: 53021, Dst Port: 53
Domain Name System (query)
6.pcap
Packets: 2766
Profile: Default


6.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Protocol Hierarchy Statistics · 6.pcap
Protocol Percent Packets Packets Percent Bytes Bytes Bits/s End Packets End Bytes End Bits/s PDUs
Frame 100.0 2766 100.0 1331575 2956 0 0 0 2766
Ethernet 100.0 2766 2.9 38724 85 0 0 0 2766
Internet Protocol Version 4 94.9 2624 3.9 52560 116 0 0 0 2624
User Datagram Protocol 4.3 118 0.1 944 2 0 0 0 118
Network Time Protocol 0.2 6 0.1 720 1 6 720 1 6
Multicast Domain Name System 0.3 8 0.0 352 0 8 352 0 8
Link-local Multicast Name Resolution 0.1 4 0.0 132 0 4 132 0 4
Domain Name System 3.5 96 0.7 9320 20 96 9320 20 96
Connectionless Lightweight Directory Access Protocol 0.1 4 0.1 814 1 4 814 1 4
Transmission Control Protocol 89.9 2486 3.8 50840 112 1415 29420 65 2486
Transport Layer Security 6.9 192 18.3 243920 541 192 236342 524 200
NetBIOS Session Service 2.3 64 1.8 24316 53 0 0 0 64
SMB2 (Server Message Block Protocol version 2) 2.2 60 1.8 23784 52 60 23784 52 60
SMB (Server Message Block Protocol) 0.1 4 0.0 276 0 4 276 0 4
Lightweight Directory Access Protocol 2.0 54 2.7 36455 80 54 28259 62 57
Hypertext Transfer Protocol 0.1 4 0.1 1255 2 3 927 2 4
Online Certificate Status Protocol 0.0 1 0.0 471 1 1 471 1 1
FTP Data 20.9 578 63.1 840869 1867 576 838920 1862 578
Line-based text data 0.1 2 0.1 1949 4 2 1949 4 2
File Transfer Protocol (FTP) 3.0 83 0.3 4409 9 83 4409 9 83
Distributed Computing Environment / Remote Procedure Call (DCE/RPC) 3.5 96 2.1 27894 61 30 12798 28 96
Local Security Authority 0.1 4 0.0 560 1 4 560 1 4
DCE/RPC Endpoint Mapper 0.6 16 0.2 3104 6 16 3104 6 16
Active Directory Replication 1.7 46 0.4 5728 12 46 5728 12 46
Internet Group Management Protocol 0.7 20 0.0 320 0 20 320 0 20
Address Resolution Protocol 5.1 142 0.3 3976 8 142 3976 8 142
No display filter.
Close Copy Protocols Help
6.pcap
Packets: 2766
Profile: Default


6.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · I/O Graphs · 6.pcap
Wireshark I/O Graphs: 6.pcap
1 sec Intervals
TCP Errors
80 packets
60 packets
40 packets
20 packets
0 packets
Packets/1 sec
0 500 1000 1500 2000 2500 3000 3500
Time (s)
Hover over the graph for details.
Enabled Graph Name Display Filter Color Style Y Axis Y Field SMA Period Y Axis Fac
TCP Errors tcp.analysis.flags Bar Packets None 1
Mouse drags zooms Interval 1 sec Time of day Log scale Automatic update Enable legend
Reset Save As... Copy Copy from Close Help
6.pcap
Packets: 2766
Profile: Default

7. Analysis of 7.pcap – TLS Obfuscation and C2 Behavior

Filter uses: ip.addr == 8.212.147.0 && tls
Frame No: 192
Source IP: 10.5.12.101
Destination IP: 8.212.147.0
Method: Client Hello
URL/Path: SNI=barkunode.com
Suspicious?: Yes
Reason: TLSv1.2 handshake with unknown, potentially shady domain. Followed by a very high volume of "Ignored Unknown Record" messages and missing TCP segments — indicative of obfuscation, evasion, or possible malware C2 (Command & Control).
Port Number: 443

Filter uses: ip.addr == 8.212.147.0 && tls && tcp.analysis.flags
Frame No: 194–805
Source IP: 8.212.147.0
Destination IP: 10.5.12.101
Method: Application Data / Unknown TLS Records
URL/Path: —
Suspicious?: Yes
Reason: High frequency of "Ignored Unknown Record" and "[TCP Previous segment not captured]" alerts — strongly suggests unusual or malicious encrypted communication patterns or evasion tactics.
Port Number: 443

Filter uses: ip.addr == 8.212.147.0 && tls
Frame No: 604
Source IP: 8.212.147.0
Destination IP: 10.5.12.101
Method: TCP ACK
URL/Path: —
Suspicious?: Yes
Reason: TCP segment not captured; begins a suspicious stream of malformed TLS packets
Port Number: 443

Filter uses: ip.addr == 8.212.147.0 && tls.record.content_type == 23
Frame No: 607
Source IP: 8.212.147.0
Destination IP: 10.5.12.101
Method: TLSv1.2
URL/Path: Ignored Unknown Record
Suspicious?: Yes
Reason: TLS application data flagged as ignored/unknown record type, indicating non-compliant TLS usage
Port Number: 443

Filter uses: ip.addr == 8.212.147.0 && tls.record.content_type == 23
Frame No: 619
Source IP: 8.212.147.0
Destination IP: 10.5.12.101
Method: TLSv1.2
URL/Path: 94 bytes Application Data
Suspicious?: Maybe
Reason: Unusually small encrypted data during continuous transfer — may indicate beaconing or control signal
Port Number: 443

Filter uses: frame.number == 743
Frame No: 743
Source IP: 8.212.147.0
Destination IP: 10.5.12.101
Method: TLSv1.2
URL/Path: 1382 bytes Application Data
Suspicious?: Yes
Reason: Encrypted data injected after multiple gaps, TCP segment not captured prior to this — possible obfuscation
Port Number: 443

Filter uses: frame.number == 1126
Frame No: 1126
Source IP: 8.212.147.0
Destination IP: 10.5.12.101
Method: TLSv1.2
URL/Path: Application Data + Ignored Unknown Record
Suspicious?: Yes
Reason: Mixed encrypted data with unknown TLS record types — strongly suggests non-standard or malicious TLS usage
Port Number: 443

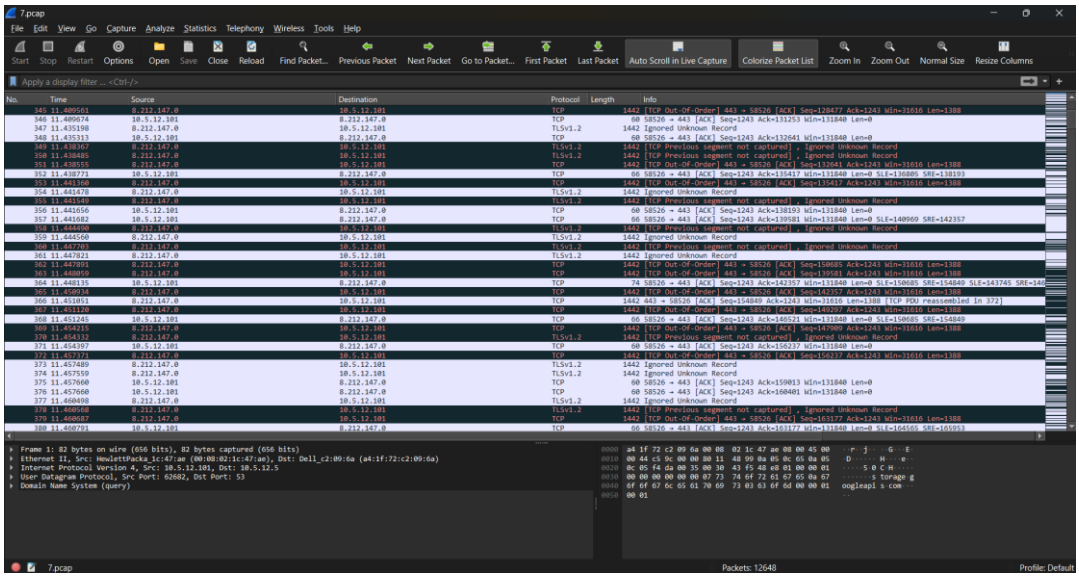
Filter uses: dns.qry.name == "barkunode.com"
Frame No: 187
Source IP: 10.5.12.101
Destination IP: 10.5.12.5
Method: DNS Standard Query
URL/Path: barkunode.com
Suspicious?: Yes
Reason: The domain resolves to **8.212.147.0**, which matches the source IP of suspicious TLSv1.2 activity in previous analysis. Potential link to malicious C2 (Command & Control) server.
Port Number: 53

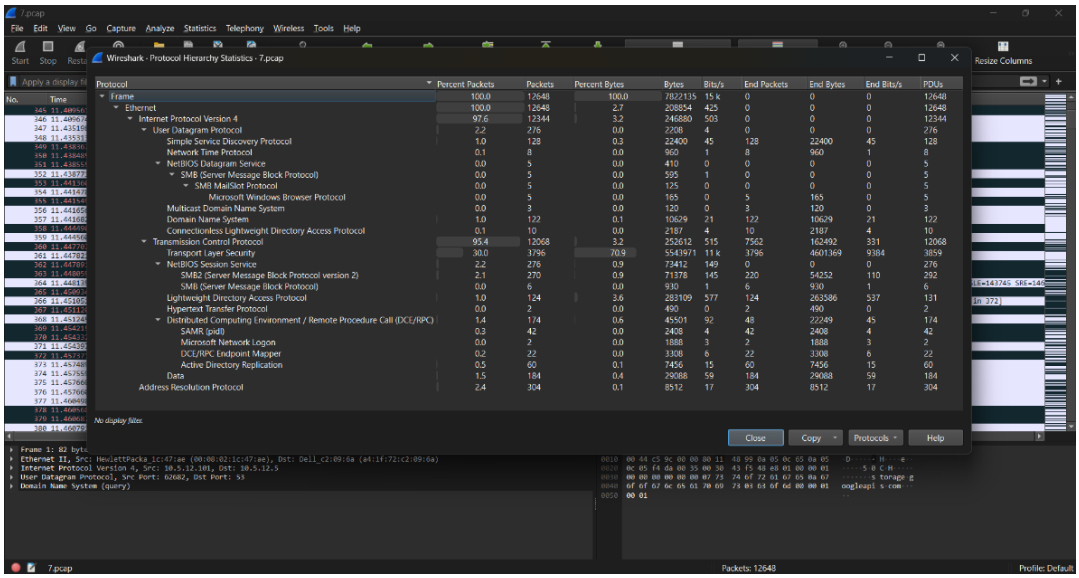
Filter uses:
dns.qry.name == "a572d5d90792d5db11a13813dba68569.clo.footprintdns.com"
Frame No: 4619
Source IP: 10.5.12.101
Destination IP: 10.5.12.5
Method: DNS Standard Query
URL/Path: a572d5d90792d5db11a13813dba68569.clo.footprintdns.com
Suspicious?: Yes
Reason: Extremely long, obfuscated subdomain pattern — typically seen in malware for **payload staging**, **fingerprinting**, or **data exfiltration** via DNS tunneling.
Port Number: 53

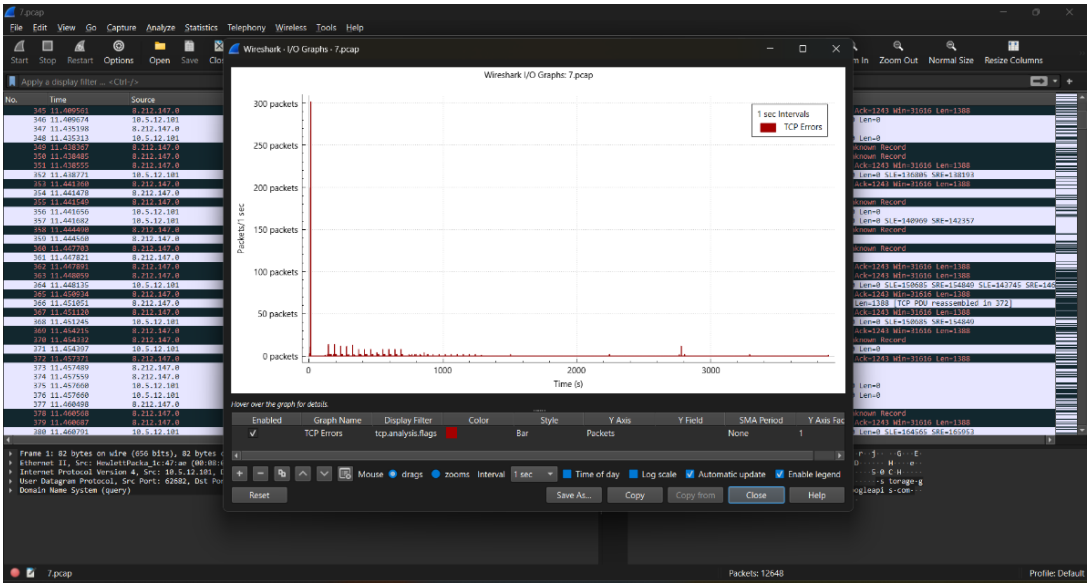
Filter uses: dns && dns.qry.name contains "wpad.mockingbirds.com"
Frame No: 2915
Source IP: 10.5.12.101
Destination IP: 10.5.12.5
Method: DNS Query
URL/Path: wpad.mockingbirds.com
Suspicious?: Yes
Reason: Repeated WPAD queries can indicate misconfigured proxy discovery or WPAD spoofing risks.
Port Number: 53

Filter uses: dns && dns.qry.name == "barkunode.com"
Frame No: 187
Source IP: 10.5.12.101
Destination IP: 10.5.12.5
Method: DNS Query
URL/Path: barkunode.com
Suspicious?: Yes
Reason: Non-standard, low-reputation domain (potential malware C2 or tracking).
Port Number: 53

Filter uses: dns && dns.qry.name contains "footprintdns.com"
Frame No: 4619
Source IP: 10.5.12.101
Destination IP: 10.5.12.5
Method: DNS Query
URL/Path: a572d5d90792d5db11a13813dba68569.clo.footprintdns.com
Suspicious?: Yes
Reason: Contains long hash-like subdomain typical of beaconing or tracking.
Port Number: 53


7.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Start Stop Restart Options Open Save Close Reload Find Packet... Previous Packet Next Packet Go to Packet... First Packet Last Packet Auto Scroll in Live Capture Colorize Packet List Zoom In Zoom Out Normal Size Resize Columns
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
Frame 1: 82 bytes on wire (656 bits), 82 bytes captured (656 bits)
Ethernet II, Src: HewlettPacka_1c:47:ae (00:08:02:1c:47:ae), Dst: Dell_c2:09:6a (a4:1f:72:c2:09:6a)
Internet Protocol Version 4, Src: 10.5.12.101, Dst: 10.5.12.5
User Datagram Protocol, Src Port: 62682, Dst Port: 53
Domain Name System (query)
7.pcap
Packets: 12648
Profile: Default


Wireshark · Protocol Hierarchy Statistics · 7.pcap
Protocol Percent Packets Packets Percent Bytes Bytes Bits/s End Packets End Bytes End Bits/s PDUs
Frame 100.0 12648 100.0 7822135 15 k 0 0 0 12648
Ethernet 100.0 12648 2.7 208854 425 0 0 0 12648
Internet Protocol Version 4 97.6 12344 3.2 246880 503 0 0 0 12344
User Datagram Protocol 2.2 276 0.0 2208 4 0 0 0 276
Simple Service Discovery Protocol 1.0 128 0.3 22400 45 128 22400 45 128
Network Time Protocol 0.1 8 0.0 960 1 8 960 1 8
NetBIOS Datagram Service 0.0 5 0.0 410 0 0 0 0 5
SMB (Server Message Block Protocol) 0.0 5 0.0 595 1 0 0 0 5
SMB MailSlot Protocol 0.0 5 0.0 125 0 0 0 0 5
Microsoft Windows Browser Protocol 0.0 5 0.0 165 0 5 165 0 5
Multicast Domain Name System 0.0 3 0.0 120 0 3 120 0 3
Domain Name System 1.0 122 0.1 10629 21 122 10629 21 122
Connectionless Lightweight Directory Access Protocol 0.1 10 0.0 2187 4 10 2187 4 10
Transmission Control Protocol 95.4 12068 3.2 252612 515 7562 162492 331 12068
Transport Layer Security 30.0 3796 70.9 5543971 11 k 3796 4601369 9384 3859
NetBIOS Session Service 2.2 276 0.9 73412 149 0 0 0 276
SMB2 (Server Message Block Protocol version 2) 2.1 270 0.9 71278 145 220 54252 110 292
SMB (Server Message Block Protocol) 0.0 6 0.0 930 1 6 930 1 6
Lightweight Directory Access Protocol 1.0 124 3.6 283109 577 124 263586 537 131
Hypertext Transfer Protocol 0.0 2 0.0 490 0 2 490 0 2
Distributed Computing Environment / Remote Procedure Call (DCE/RPC) 1.4 174 0.6 45501 92 48 22249 45 174
SAMR (pidl) 0.3 42 0.0 2408 4 42 2408 4 42
Microsoft Network Logon 0.0 2 0.0 1888 3 2 1888 3 2
DCE/RPC Endpoint Mapper 0.2 22 0.0 3308 6 22 3308 6 22
Active Directory Replication 0.5 60 0.1 7456 15 60 7456 15 60
Data 1.5 184 0.4 29088 59 184 29088 59 184
Address Resolution Protocol 2.4 304 0.1 8512 17 304 8512 17 304
No display filter.
Close Copy Protocols Help
7.pcap
Packets: 12648
Profile: Default


Wireshark · I/O Graphs · 7.pcap
Wireshark I/O Graphs: 7.pcap
300 packets
250 packets
200 packets
150 packets
100 packets
50 packets
0 packets
Packets / sec
0
1000
2000
3000
Time (s)
1 sec Intervals
TCP Errors
Hover over the graph for details.
Enabled Graph Name Display Filter Color Style Y Axis Y Field SMA Period Y Axis Fac
TCP Errors tcp.analysis.flags Bar Packets None 1
Mouse drags zooms Interval 1 sec Time of day Log scale Automatic update Enable legend
Reset Save As... Copy Copy from Close Help
7.pcap
Packets: 12648
Profile: Default

Conclusion

This project effectively demonstrated the practical use of Wireshark and Zeek in identifying suspicious network activity within a controlled lab environment. Using Wireshark, we captured DNS, HTTP, and TCP packets and applied filters to detect anomalies such as repeated POST requests, executable file downloads, and TCP SYN floods. Zeek logs further revealed failed DNS resolutions, abnormal port access (445, 3389), and unusual TLS behavior linked to suspicious domains.

The analysis helped uncover potential malware indicators like beaconing, data exfiltration, and domain generation algorithms (DGAs). By combining packet-level inspection and behavioral logging, the project strengthened key skills in network security monitoring and threat detection, which are crucial for any cybersecurity analyst.

Key Learnings:

- Effective use of filters and logs is essential in traffic analysis.
- Zeek complements Wireshark by offering behavior-level insights.
- Hands-on exposure to real traffic patterns builds real-world skills.
-

Future Work:

- Integrate log outputs into a SIEM (e.g., Splunk or ELK).
- Automate detection using Zeek scripting and alerting systems.
- Expand scope to include encrypted traffic analysis.

Recommendations

- **Use Zeek** as a continuous monitoring tool for behavioral anomaly detection.
- **Monitor DNS traffic** for signs of tunnelling or C2 activity, DGA domains, and DDNS usage.
- **Avoid unencrypted protocols** like FTP; prefer secure alternatives.
- **Inspect TLS sessions** for handshake anomalies or suspicious SNI domains.
- **Correlate Wireshark and Zeek with threat intelligence** using tools like VirusTotal and AbuseIPDB.
- **Automate alerts** using Zeek scripting for failed DNS, unusual ports, or POST patterns.
- **Train analysts** to read logs and packets effectively.

References

- **Wireshark Documentation** – https://www.wireshark.org/docs/
- **Zeek Documentation** – https://docs.zeek.org/en/current/
- **Practical Packet Analysis** – Chris Sanders
- **SANS Network Traffic Analysis Tutorials** – https://www.sans.org/
- **VirusTotal & AbuseIPDB** – For domain/IP reputation lookup
- **RFCs** – TCP/IP, DNS, TLS protocol references

Appendices

Appendix A: Wireshark Filter Examples Used

- http.request
- dns.qry.name contains "wpad"
- tcp.flags.syn == 1
- tls.handshake.type == 1
- http contains ".exe"
- icmp.type == 5
- cldap
- llmnr
- ftp.request.command == "USER" || ftp.request.command == "PASS"

Appendix B: Zeek Log Files Generated

- **conn.log –** All connection metadata (IP, port, protocol, duration)
- **dns.log –** DNS queries and responses
- **http.log –** HTTP method, host, URI

Appendix C: List of PCAP Files Analyzed

PCAP File	Description
1.pcap	HTTP POST and EXE file detection
2.pcap	DNS tunneling, WPAD activity
3.pcap	TLS handshake with unknown domain
4.pcap	SMB and Kerberos TCP resets
5.pcap	DDNS and malware file download
6.pcap	FTP-based data exfiltration
7.pcap	TLS obfuscation and C2 activity

Appendix D: Tools and Versions

Tool	Version Used
Wireshark	4.x.x
Zeek	5.x.x
Kali Linux	2023.4 Rolling
VM Software	VirtualBox 7 / VMware

Appendix E: Suspicious Domains Identified

- barkunode.com
- oreokitkat.ddns.net
- footprintdns.com
- gomuzigak.com
- wpad.mockingbirds.com

Appendix F: Sample Screenshot

- Wireshark IO Graph
- Protocol Hierarchy window
- Zeek log snippet (e.g., dns.log showing failed queries)