Lab-Manual

Digital Forensics

CY-334L

Prepared By: Ms.Memoona Sadaf

Instructor: Ms.Memoona Sadaf

Lab/Teaching Assistant: Muhammad Ahmad Ali Qureshi

Semester: Spring 2025

Class: Fall 22 A, Fall 22 B

Air University Islamabad

AIR UNIVERSITY

Department of Cyber Security

Lab Schedule

Week	Lab Topics
Week 4	Network Forensics

Introduction to Network Forensics

Network forensics involves the monitoring and analysis of computer network traffic to gather information, detect intrusions, and investigate cybercrimes. It is an essential field of cybersecurity that helps identify threats, analyze attacks, and gather digital evidence. Network forensics enables security professionals to trace security breaches, analyze suspicious activities, and reconstruct cyber incidents to determine their origin and impact.

Common Network Forensics Tools

Several tools are used in network forensics to analyze and capture network traffic effectively. Each tool has unique capabilities tailored for different aspects of network security monitoring and analysis.

Wireshark

Wireshark is one of the most powerful and widely used network protocol analyzers. It allows users to capture, analyze, and inspect real-time packet flows across networks. Wireshark is commonly used for troubleshooting, performance analysis, and security investigations.

tcpdump

Tcpdump is a lightweight, command-line packet capture tool that allows users to filter and analyze network traffic. It is useful for capturing packets on Unix-based systems and can be combined with scripting for automation in forensic investigations.

NetworkMiner

NetworkMiner is a forensic analysis tool that helps in extracting metadata, credentials, files, and images from captured network traffic (PCAP files). It is particularly useful in reconstructing past network events and identifying compromised data.

Xplico

Xplico is an open-source network forensics analysis tool (NFAT) that reconstructs network sessions. It allows analysts to extract email content, HTTP sessions, VoIP calls, and other data from captured traffic, providing a detailed view of user activities on a network.

Snort

Snort is an open-source network intrusion detection and prevention system (IDS/IPS). It continuously monitors network traffic and detects potential threats based on predefined rules. Snort is widely used to analyze attack patterns and block malicious activities in real time.

Bro/Zeek

Bro/Zeek is a network analysis framework that provides deep packet inspection and behavioral analysis of network traffic. It is often used in cybersecurity monitoring and forensic investigations to detect anomalies and network attacks.

NetFlow Analyzer

NetFlow Analyzer is a traffic monitoring tool that provides visibility into network performance and bandwidth usage. It helps forensic investigators detect unusual network behavior and track down security incidents.

Wireshark: Introduction and Overview

What is Wireshark?

Wireshark is a widely used network protocol analyzer that captures and inspects packets in real time. It allows network administrators, security professionals, and forensic analysts to analyze network behavior, troubleshoot network issues, and investigate security incidents. Wireshark supports multiple protocols, making it an essential tool for identifying network anomalies and potential threats.

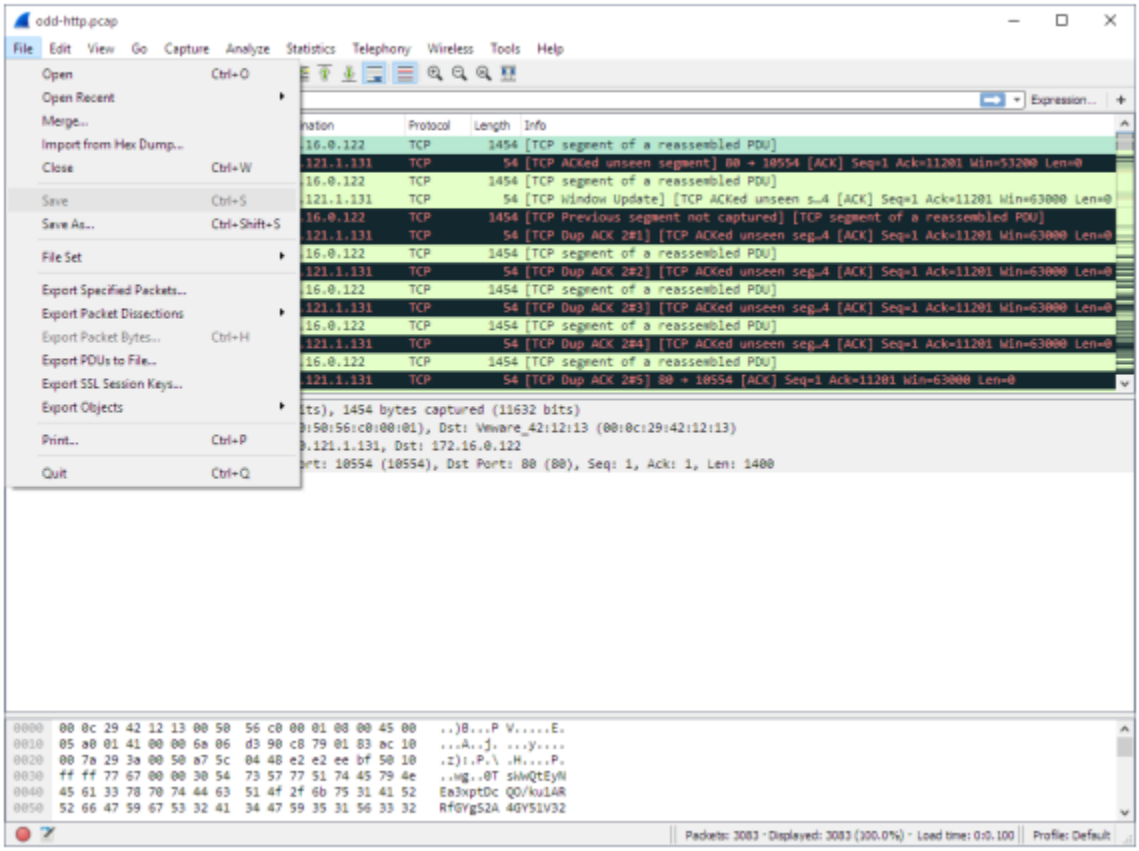
Key Features of Wireshark

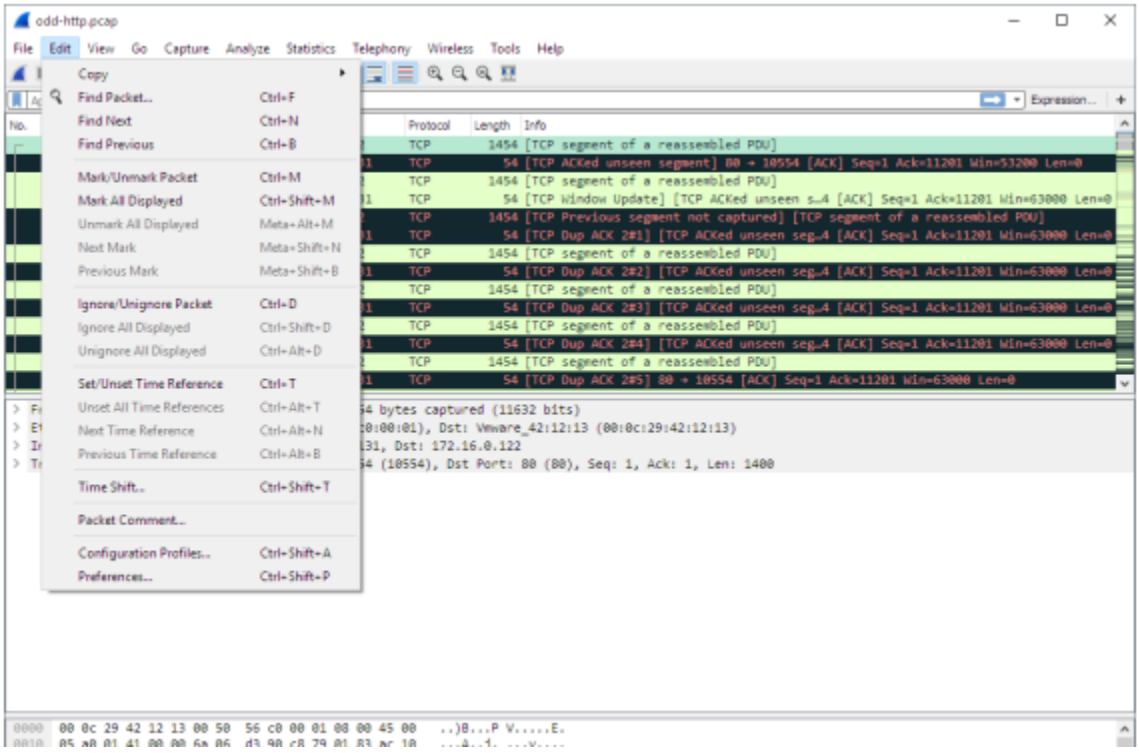
Wireshark provides several powerful features that aid in network forensics:

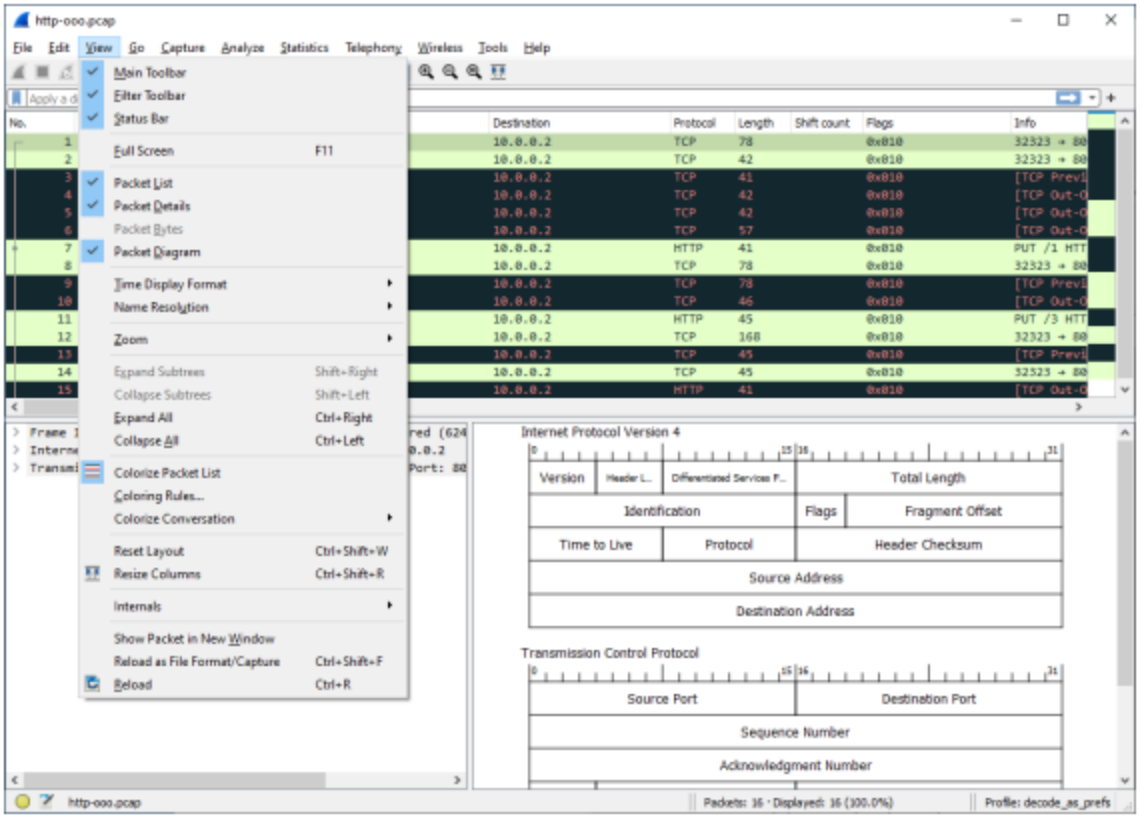
- **Packet Capture**: Captures real-time network traffic from different interfaces such as Ethernet, Wi-Fi, and VPN.
- **Protocol Analysis**: Supports hundreds of network protocols and decodes packet structures for detailed inspection.
- **Filtering Capabilities**: Allows users to apply both capture and display filters to focus on specific types of traffic.
- **Packet Inspection**: Provides deep analysis of packet headers, payloads, and protocol interactions.
- **Graphical Analysis**: Displays network traffic flow using statistical tools, enabling forensic analysts to detect unusual patterns.
- **Export and Reporting**: Saves captured data in PCAP format for further analysis and forensic reporting.

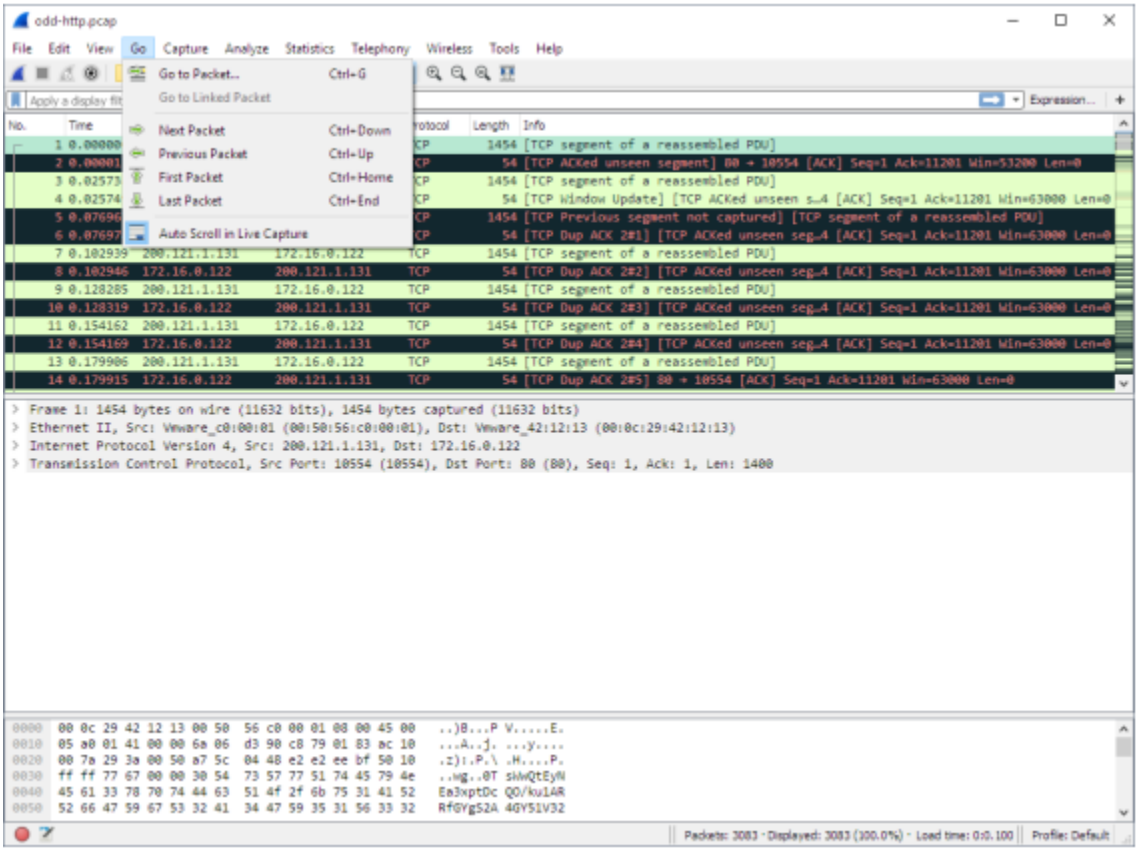
File Menu of Wireshark

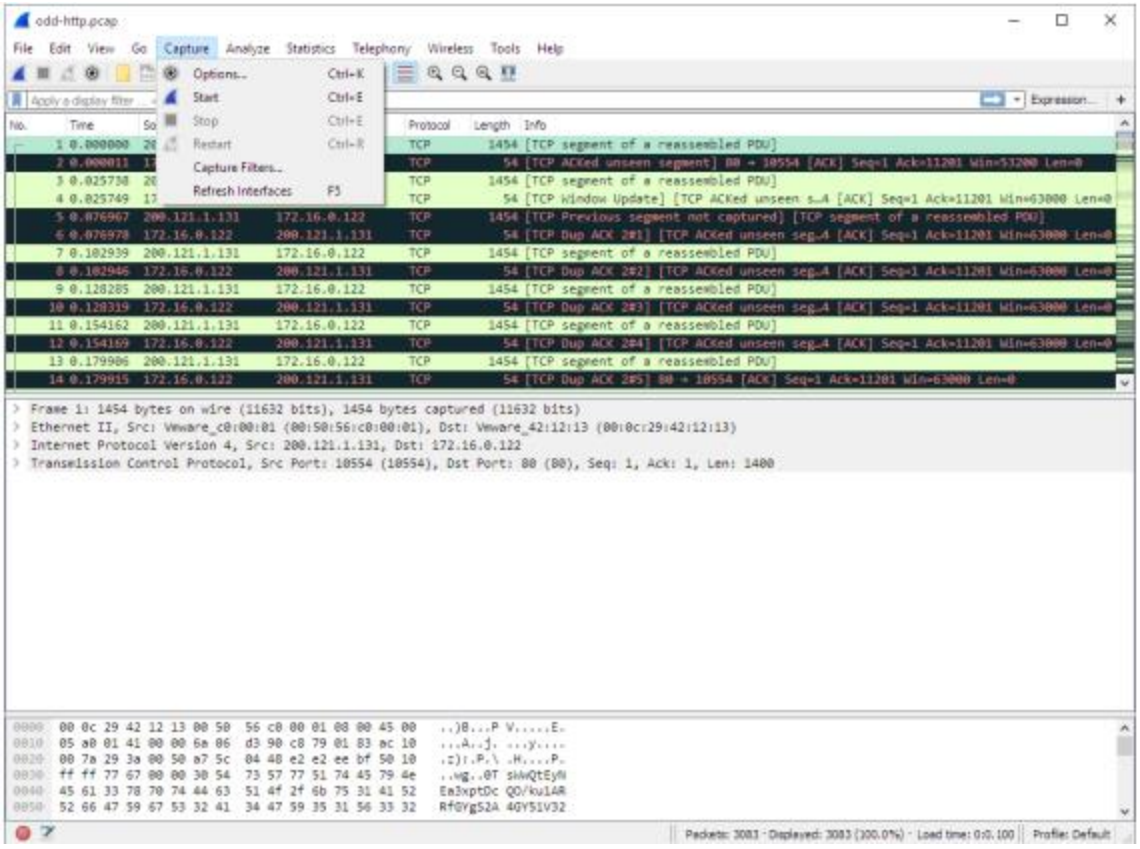
The Wireshark file menu contains the fields shown in File menu items.

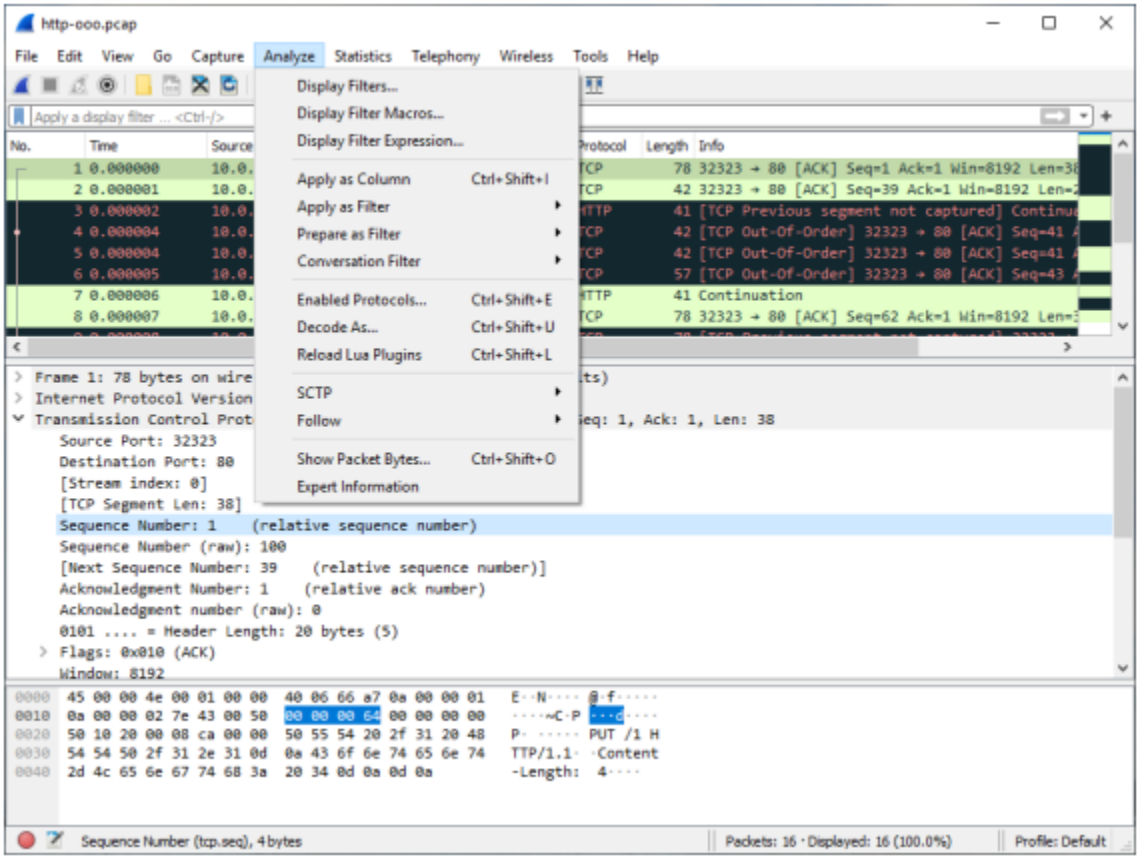


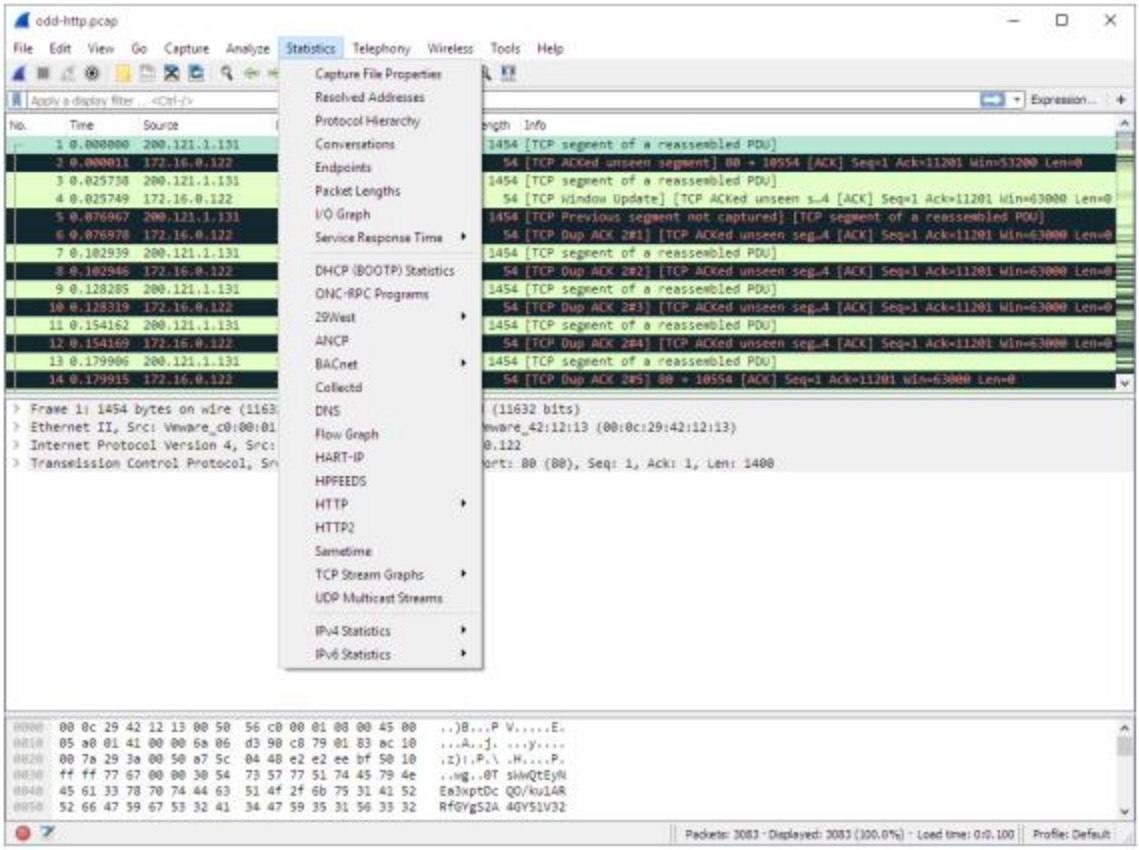


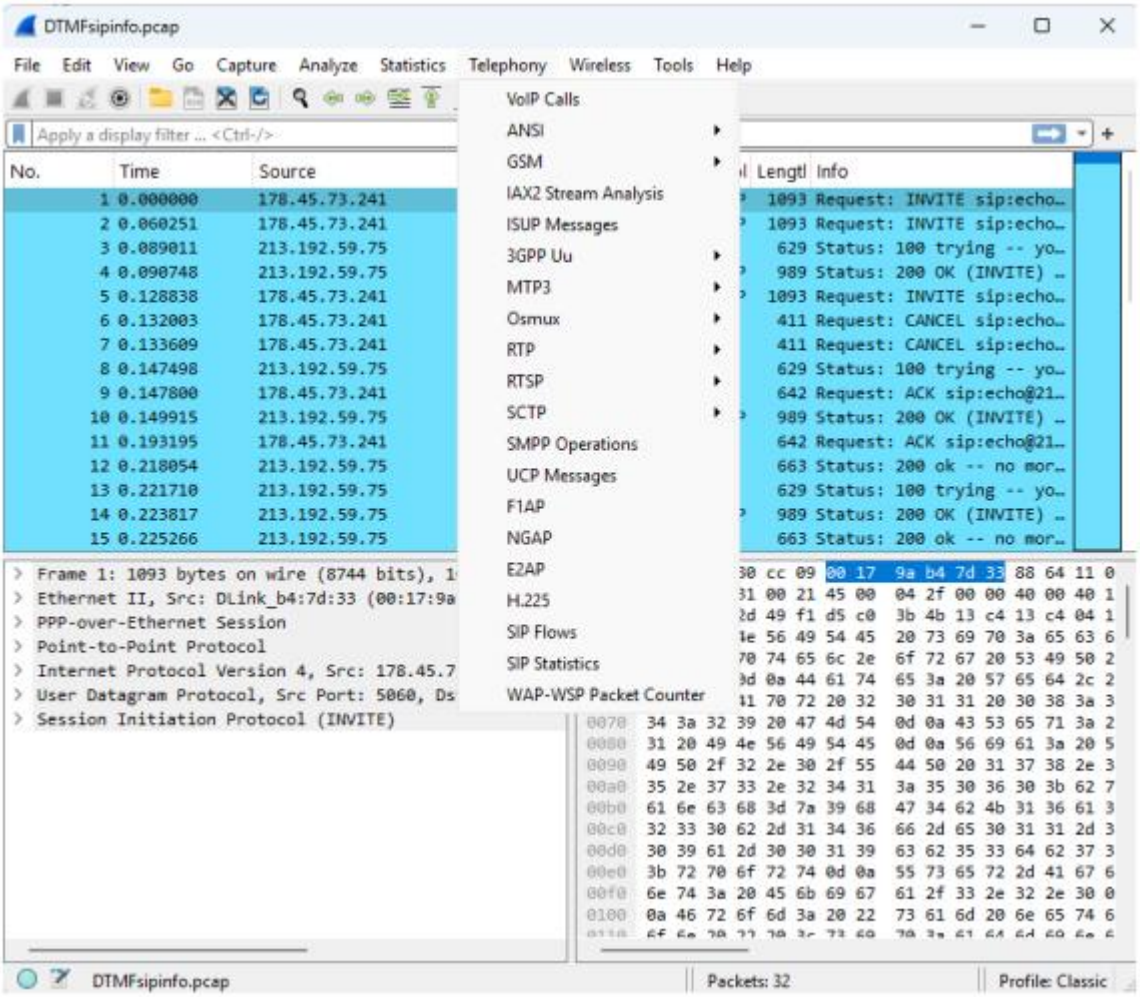

http-ooo.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Main Toolbar
Filter Toolbar
Status Bar
Full Screen F11
Packet List
Packet Details
Packet Bytes
Packet Diagram
Time Display Format
Name Resolution
Zoom
Expand Subtrees Shift+Right
Collapse Subtrees Shift+Left
Expand All Ctrl+Right
Collapse All Ctrl+Left
Colorize Packet List
Coloring Rules...
Colorize Conversation
Reset Layout Ctrl+Shift+W
Resize Columns Ctrl+Shift+R
Internals
Show Packet in New Window
Reload as File Format/Capture Ctrl+Shift+F
Reload Ctrl+R
No. Destination Protocol Length Shift count Flags Info
Internet Protocol Version 4
Version
Total Length
Identification
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
Source Address
Destination Address
Transmission Control Protocol
Source Port
Destination Port
Sequence Number
Acknowledgment Number
http-ooo.pcap
Packets: 16 · Displayed: 16 (100.0%)
Profile: decode_as_prefs

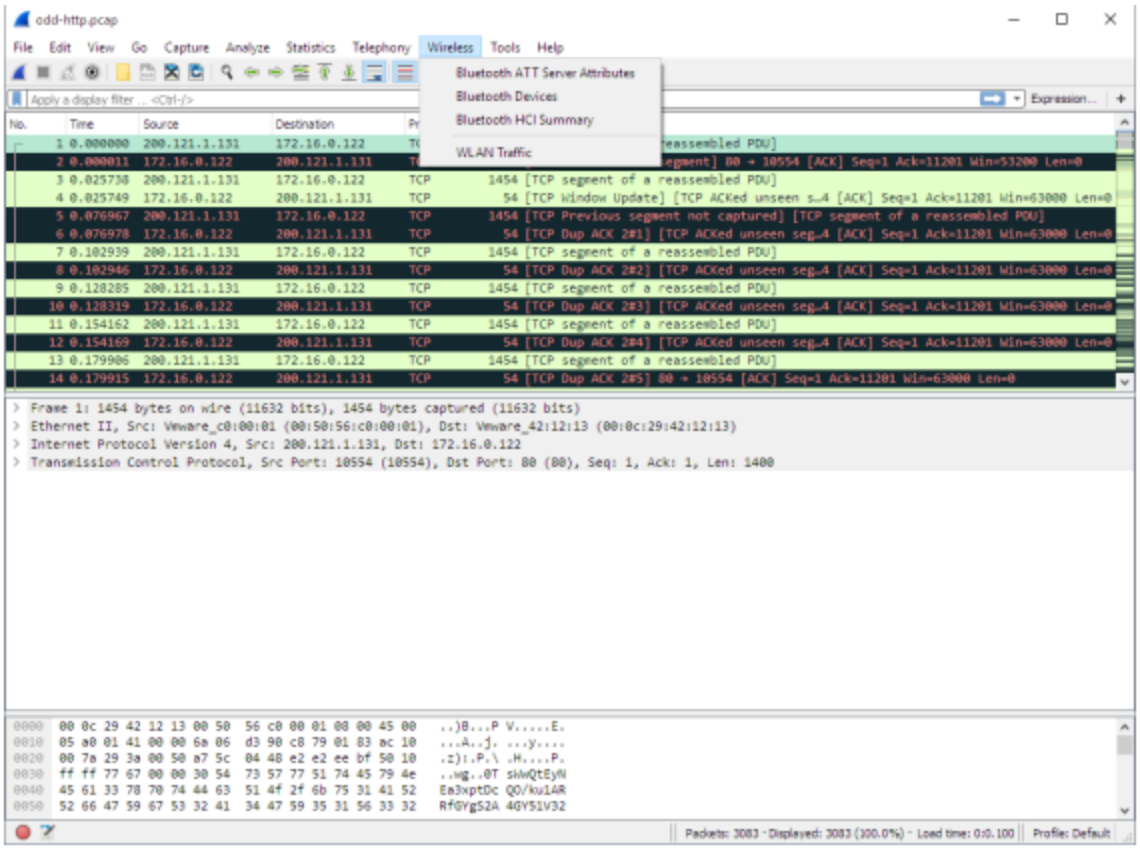

odd-http.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Go to Packet... Ctrl+G
Go to Linked Packet
Next Packet Ctrl+Down
Previous Packet Ctrl+Up
First Packet Ctrl+Home
Last Packet Ctrl+End
Auto Scroll in Live Capture
No. Time Source Destination Protocol Length Info
1 0.000000 200.121.1.131 172.16.0.122 TCP 1454 [TCP segment of a reassembled PDU]
2 0.000001 200.121.1.131 172.16.0.122 TCP 54 [TCP ACKed unseen segment] 80 → 10554 [ACK] Seq=1 Ack=11201 Win=53200 Len=0
3 0.025737 200.121.1.131 172.16.0.122 TCP 1454 [TCP segment of a reassembled PDU]
4 0.025741 172.16.0.122 200.121.1.131 TCP 54 [TCP Window Update] [TCP ACKed unseen s…4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
5 0.076961 200.121.1.131 172.16.0.122 TCP 1454 [TCP Previous segment not captured] [TCP segment of a reassembled PDU]
6 0.076971 172.16.0.122 200.121.1.131 TCP 54 [TCP Dup ACK 2#1] [TCP ACKed unseen seg…4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
7 0.102939 200.121.1.131 172.16.0.122 TCP 1454 [TCP segment of a reassembled PDU]
8 0.102946 172.16.0.122 200.121.1.131 TCP 54 [TCP Dup ACK 2#2] [TCP ACKed unseen seg…4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
9 0.128285 200.121.1.131 172.16.0.122 TCP 1454 [TCP segment of a reassembled PDU]
10 0.128319 172.16.0.122 200.121.1.131 TCP 54 [TCP Dup ACK 2#3] [TCP ACKed unseen seg…4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
11 0.154162 200.121.1.131 172.16.0.122 TCP 1454 [TCP segment of a reassembled PDU]
12 0.154169 172.16.0.122 200.121.1.131 TCP 54 [TCP Dup ACK 2#4] [TCP ACKed unseen seg…4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
13 0.179906 200.121.1.131 172.16.0.122 TCP 1454 [TCP segment of a reassembled PDU]
14 0.179915 172.16.0.122 200.121.1.131 TCP 54 [TCP Dup ACK 2#5] 80 → 10554 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
Frame 1: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits)
Ethernet II, Src: Vmware_c0:00:01 (00:50:56:c0:00:01), Dst: Vmware_42:12:13 (00:0c:29:42:12:13)
Internet Protocol Version 4, Src: 200.121.1.131, Dst: 172.16.0.122
Transmission Control Protocol, Src Port: 10554 (10554), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 1400
Packets: 3083 · Displayed: 3083 (100.0%) · Load time: 0:0.100
Profile: Default

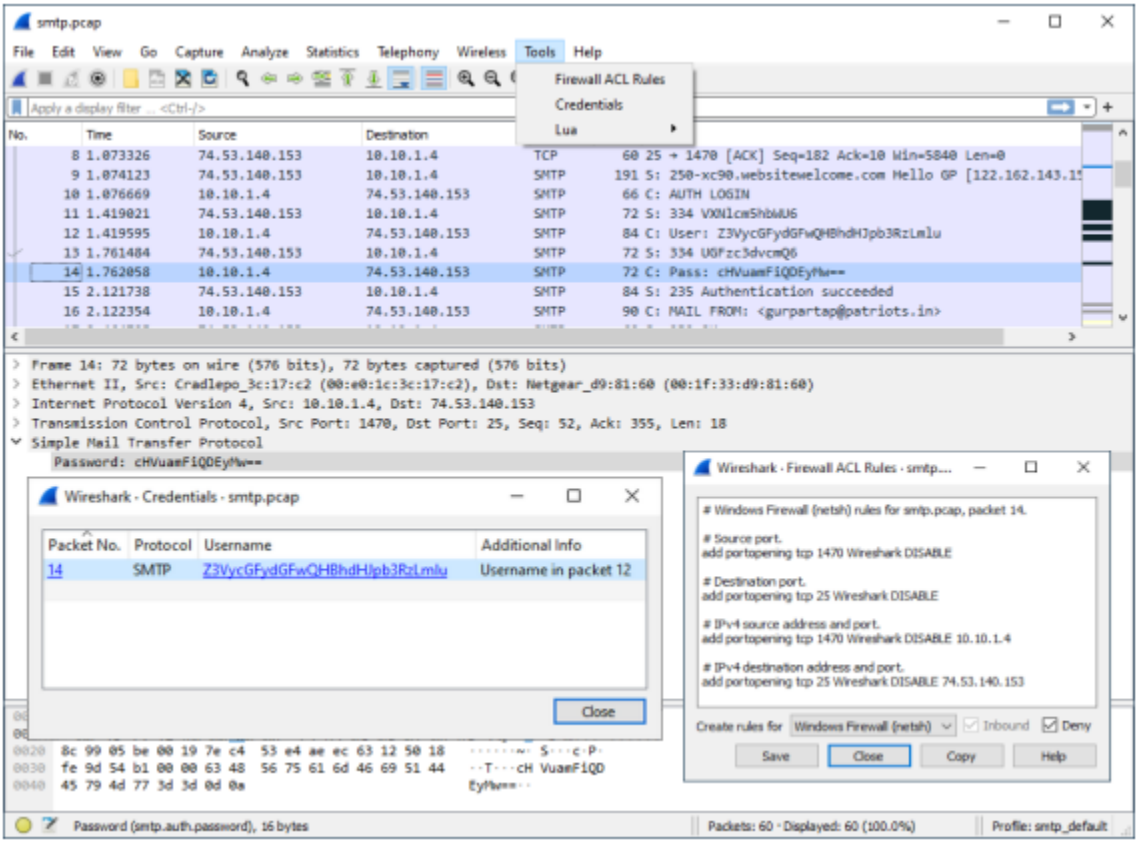

odd-http.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Options... Ctrl+K
Start Ctrl+E
Stop Ctrl+E
Restart Ctrl+R
Capture Filters...
Refresh Interfaces F5
No. Time Protocol Length Info
1 0.000000 TCP 1454 [TCP segment of a reassembled PDU]
2 0.000011 TCP 54 [TCP ACKed unseen segment] 80 → 10554 [ACK] Seq=1 Ack=11201 Win=53200 Len=0
3 0.025730 TCP 1454 [TCP segment of a reassembled PDU]
4 0.025749 TCP 54 [TCP Window Update] [TCP ACKed unseen s…A [ACK] Seq=1 Ack=11201 Win=63000 Len=0
5 0.076967 200.121.1.131 172.16.0.122 TCP 1454 [TCP Previous segment not captured] [TCP segment of a reassembled PDU]
6 0.076978 172.16.0.122 200.121.1.131 TCP 54 [TCP Dup ACK 2#1] [TCP ACKed unseen seg…A [ACK] Seq=1 Ack=11201 Win=63000 Len=0
7 0.102939 200.121.1.131 172.16.0.122 TCP 1454 [TCP segment of a reassembled PDU]
8 0.102946 172.16.0.122 200.121.1.131 TCP 54 [TCP Dup ACK 2#2] [TCP ACKed unseen seg…A [ACK] Seq=1 Ack=11201 Win=63000 Len=0
9 0.128285 200.121.1.131 172.16.0.122 TCP 1454 [TCP segment of a reassembled PDU]
10 0.128319 172.16.0.122 200.121.1.131 TCP 54 [TCP Dup ACK 2#3] [TCP ACKed unseen seg…A [ACK] Seq=1 Ack=11201 Win=63000 Len=0
11 0.154162 200.121.1.131 172.16.0.122 TCP 1454 [TCP segment of a reassembled PDU]
12 0.154189 172.16.0.122 200.121.1.131 TCP 54 [TCP Dup ACK 2#4] [TCP ACKed unseen seg…A [ACK] Seq=1 Ack=11201 Win=63000 Len=0
13 0.179906 200.121.1.131 172.16.0.122 TCP 1454 [TCP segment of a reassembled PDU]
14 0.179915 172.16.0.122 200.121.1.131 TCP 54 [TCP Dup ACK 2#5] 80 → 10554 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
Frame 1: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits)
Ethernet II, Src: Vmware_c0:00:01 (00:50:56:c0:00:01), Dst: Vmware_42:12:13 (00:0c:29:42:12:13)
Internet Protocol Version 4, Src: 200.121.1.131, Dst: 172.16.0.122
Transmission Control Protocol, Src Port: 10554 (10554), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 1400
0000 00 0c 29 42 12 13 00 50 56 c0 00 01 08 00 45 00
0010 05 a8 01 41 00 00 6a 06 d3 90 c8 79 01 83 ac 10
0020 00 7a 29 3a 00 50 a7 5c 04 48 e2 e2 ee bf 50 10
0030 ff ff 77 67 00 00 30 54 73 57 77 51 74 45 79 4e
0040 45 61 33 78 70 74 44 63 51 4f 2f 6b 75 31 41 52
0050 52 66 47 59 67 53 32 41 34 47 59 35 31 56 33 32
Packets: 3083 · Displayed: 3083 (100.0%) · Load time: 0:0.100
Profile: Default


http-ooo.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Display Filters...
Display Filter Macros...
Display Filter Expression...
Apply as Column Ctrl+Shift+I
Apply as Filter
Prepare as Filter
Conversation Filter
Enabled Protocols... Ctrl+Shift+E
Decode As... Ctrl+Shift+U
Reload Lua Plugins Ctrl+Shift+L
SCTP
Follow
Show Packet Bytes... Ctrl+Shift+O
Expert Information
No. Time Source Protocol Length Info
1 0.000000 10.0. TCP 78 32323 → 80 [ACK] Seq=1 Ack=1 Win=8192 Len=38
2 0.000001 10.0. TCP 42 32323 → 80 [ACK] Seq=39 Ack=1 Win=8192 Len=0
3 0.000002 10.0. HTTP 41 [TCP Previous segment not captured] Continuation
4 0.000004 10.0. TCP 42 [TCP Out-Of-Order] 32323 → 80 [ACK] Seq=41 Ack=1
5 0.000004 10.0. TCP 42 [TCP Out-Of-Order] 32323 → 80 [ACK] Seq=41 Ack=1
6 0.000005 10.0. TCP 57 [TCP Out-Of-Order] 32323 → 80 [ACK] Seq=43 Ack=1
7 0.000006 10.0. HTTP 41 Continuation
8 0.000007 10.0. TCP 78 32323 → 80 [ACK] Seq=62 Ack=1 Win=8192 Len=38
Frame 1: 78 bytes on wire
Internet Protocol Version
Transmission Control Prot
Source Port: 32323
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 38]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 100
[Next Sequence Number: 39 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 0
0101 .... = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
Window: 8192
0000 45 00 00 4e 00 01 00 00 40 06 66 a7 0a 00 00 01
0010 0a 00 00 02 7e 43 00 50 00 00 00 64 00 00 00 00
0020 50 10 20 00 08 ca 00 00 50 55 54 20 2f 31 20 48
0030 54 54 50 2f 31 2e 31 0d 0a 43 6f 6e 74 65 6e 74
0040 2d 4c 65 6e 67 74 68 3a 20 34 0d 0a 0d 0a
Sequence Number (tcp.seq), 4 bytes
Packets: 16 · Displayed: 16 (100.0%)
Profile: Default


odd-http.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Capture File Properties
Resolved Addresses
Protocol Hierarchy
Conversations
Endpoints
Packet Lengths
I/O Graph
Service Response Time
DHCP (BOOTP) Statistics
ONC-RPC Programs
29West
ANCP
BACnet
Collectd
DNS
Flow Graph
HART-IP
HPFEEDS
HTTP
HTTP2
Sametime
TCP Stream Graphs
UDP Multicast Streams
IPv4 Statistics
IPv6 Statistics
Packets: 3083 · Displayed: 3083 (100.0%) · Load time: 0:0.100
Profile: Default


DTMFsipinfo.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source
1 0.000000 178.45.73.241
2 0.060251 178.45.73.241
3 0.089011 213.192.59.75
4 0.090748 213.192.59.75
5 0.128838 178.45.73.241
6 0.132003 178.45.73.241
7 0.133609 178.45.73.241
8 0.147498 213.192.59.75
9 0.147800 178.45.73.241
10 0.149915 213.192.59.75
11 0.193195 178.45.73.241
12 0.218054 213.192.59.75
13 0.221710 213.192.59.75
14 0.223817 213.192.59.75
15 0.225266 213.192.59.75
Lengtl Info
1093 Request: INVITE sip:echo…
1093 Request: INVITE sip:echo…
629 Status: 100 trying -- yo…
989 Status: 200 OK (INVITE) …
1093 Request: INVITE sip:echo…
411 Request: CANCEL sip:echo…
411 Request: CANCEL sip:echo…
629 Status: 100 trying -- yo…
642 Request: ACK sip:echo@21…
989 Status: 200 OK (INVITE) …
642 Request: ACK sip:echo@21…
663 Status: 200 ok -- no mor…
629 Status: 100 trying -- yo…
989 Status: 200 OK (INVITE) …
663 Status: 200 ok -- no mor…
VoIP Calls
ANSI
GSM
IAX2 Stream Analysis
ISUP Messages
3GPP Uu
MTP3
Osmux
RTP
RTSP
SCTP
SMPP Operations
UCP Messages
F1AP
NGAP
E2AP
H.225
SIP Flows
SIP Statistics
WAP-WSP Packet Counter
Frame 1: 1093 bytes on wire (8744 bits), 1
Ethernet II, Src: DLink_b4:7d:33 (00:17:9a
PPP-over-Ethernet Session
Point-to-Point Protocol
Internet Protocol Version 4, Src: 178.45.7
User Datagram Protocol, Src Port: 5060, Ds
Session Initiation Protocol (INVITE)
30 cc 09 00 17 9a b4 7d 33 88 64 11 0
31 00 21 45 00 04 2f 00 00 40 00 40 1
2d 49 f1 d5 c0 3b 4b 13 c4 13 c4 04 1
1e 56 49 54 45 20 73 69 70 3a 65 63 6
70 74 65 6c 2e 6f 72 67 20 53 49 50 2
0d 0a 44 61 74 65 3a 20 57 65 64 2c 2
11 70 72 20 32 30 31 31 20 30 38 3a 3
0070 34 3a 32 39 20 47 4d 54 0d 0a 43 53 65 71 3a 2
0080 31 20 49 4e 56 49 54 45 0d 0a 56 69 61 3a 20 5
0090 49 50 2f 32 2e 30 2f 55 44 50 20 31 37 38 2e 3
00a0 35 2e 37 33 2e 32 34 31 3a 35 30 36 30 3b 62 7
00b0 61 6e 63 68 3d 7a 39 68 47 34 62 4b 31 36 61 3
00c0 32 33 30 62 2d 31 34 36 66 2d 65 30 31 31 2d 3
00d0 30 39 61 2d 30 30 31 39 63 62 35 33 64 62 37 3
00e0 3b 72 70 6f 72 74 0d 0a 55 73 65 72 2d 41 67 6
00f0 6e 74 3a 20 45 6b 69 67 61 2f 33 2e 32 2e 30 0
0100 0a 46 72 6f 6d 3a 20 22 73 61 6d 20 6e 65 74 6
DTMFsipinfo.pcap
Packets: 32
Profile: Classic


odd-http.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Bluetooth ATT Server Attributes
Bluetooth Devices
Bluetooth HCI Summary
WLAN Traffic
No. Time Source Destination
1 0.000000 200.121.1.131 172.16.0.122
2 0.000011 172.16.0.122 200.121.1.131
3 0.025738 200.121.1.131 172.16.0.122 TCP 1454 [TCP segment of a reassembled PDU]
4 0.025749 172.16.0.122 200.121.1.131 TCP 54 [TCP Window Update] [TCP ACKed unseen s…4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
5 0.076967 200.121.1.131 172.16.0.122 TCP 1454 [TCP Previous segment not captured] [TCP segment of a reassembled PDU]
6 0.076978 172.16.0.122 200.121.1.131 TCP 54 [TCP Dup ACK 2#1] [TCP ACKed unseen seg…4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
7 0.102939 200.121.1.131 172.16.0.122 TCP 1454 [TCP segment of a reassembled PDU]
8 0.102946 172.16.0.122 200.121.1.131 TCP 54 [TCP Dup ACK 2#2] [TCP ACKed unseen seg…4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
9 0.128285 200.121.1.131 172.16.0.122 TCP 1454 [TCP segment of a reassembled PDU]
10 0.128319 172.16.0.122 200.121.1.131 TCP 54 [TCP Dup ACK 2#3] [TCP ACKed unseen seg…4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
11 0.154162 200.121.1.131 172.16.0.122 TCP 1454 [TCP segment of a reassembled PDU]
12 0.154169 172.16.0.122 200.121.1.131 TCP 54 [TCP Dup ACK 2#4] [TCP ACKed unseen seg…4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
13 0.179906 200.121.1.131 172.16.0.122 TCP 1454 [TCP segment of a reassembled PDU]
14 0.179915 172.16.0.122 200.121.1.131 TCP 54 [TCP Dup ACK 2#5] 80 → 10554 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
Frame 1: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits)
Ethernet II, Src: Vmware_c0:00:01 (00:50:56:c0:00:01), Dst: Vmware_42:12:13 (00:0c:29:42:12:13)
Internet Protocol Version 4, Src: 200.121.1.131, Dst: 172.16.0.122
Transmission Control Protocol, Src Port: 10554 (10554), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 1400
Packets: 3083 · Displayed: 3083 (100.0%) · Load time: 0:0.100
Profile: Default


smtp.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Firewall ACL Rules
Credentials
Lua
No. Time Source Destination
8 1.073326 74.53.140.153 10.10.1.4 TCP 60 25 → 1470 [ACK] Seq=182 Ack=10 Win=5840 Len=0
9 1.074123 74.53.140.153 10.10.1.4 SMTP 191 S: 250-xc90.websitewelcome.com Hello GP [122.162.143.15
10 1.076669 10.10.1.4 74.53.140.153 SMTP 66 C: AUTH LOGIN
11 1.419021 74.53.140.153 10.10.1.4 SMTP 72 S: 334 VXNlcm5hbWU6
12 1.419595 10.10.1.4 74.53.140.153 SMTP 84 C: User: Z3VycGFydGFwQHBhdHJpb3RzLmlu
13 1.761484 74.53.140.153 10.10.1.4 SMTP 72 S: 334 UGFzc3dvcmQ6
14 1.762058 10.10.1.4 74.53.140.153 SMTP 72 C: Pass: cHVuamFiQDEyMw==
15 2.121738 74.53.140.153 10.10.1.4 SMTP 84 S: 235 Authentication succeeded
16 2.122354 10.10.1.4 74.53.140.153 SMTP 90 C: MAIL FROM: <gurpartap@patriots.in>
Frame 14: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)
Ethernet II, Src: Cradlepo_3c:17:c2 (00:e0:1c:3c:17:c2), Dst: Netgear_d9:81:60 (00:1f:33:d9:81:60)
Internet Protocol Version 4, Src: 10.10.1.4, Dst: 74.53.140.153
Transmission Control Protocol, Src Port: 1470, Dst Port: 25, Seq: 52, Ack: 355, Len: 18
Simple Mail Transfer Protocol
Password: cHVuamFiQDEyMw==
Wireshark · Credentials · smtp.pcap
Packet No. Protocol Username Additional Info
14 SMTP Z3VycGFydGFwQHBhdHJpb3RzLmlu Username in packet 12
Close
Wireshark · Firewall ACL Rules · smtp....
Windows Firewall (netsh) rules for smtp.pcap, packet 14.
Source port.
add portopening tcp 1470 Wireshark DISABLE
Destination port.
add portopening tcp 25 Wireshark DISABLE
IPv4 source address and port.
add portopening tcp 1470 Wireshark DISABLE 10.10.1.4
IPv4 destination address and port.
add portopening tcp 25 Wireshark DISABLE 74.53.140.153
Create rules for Windows Firewall (netsh) Inbound Deny
Save Close Copy Help
Password (smtp.auth.password), 16 bytes
Packets: 60 · Displayed: 60 (100.0%)
Profile: smtp_default

Understanding Network Protocols in Wireshark

Wireshark supports various network protocols, each playing a crucial role in communication between devices. Understanding these protocols is essential for analyzing network activity effectively.

Ethernet

Ethernet is the fundamental protocol for wired networks. It defines how data packets are structured and transmitted over a local area network (LAN). Ethernet packets contain source and destination MAC addresses, making it possible to trace the origin of network traffic.

IP (Internet Protocol)

The Internet Protocol (IP) is responsible for addressing and routing packets across networks. There are two versions:

- **IPv4**: Uses 32-bit addresses (e.g., 192.168.1.1) and is widely used in networks today.
- **IPv6**: Uses 128-bit addresses (e.g., 2001:db8::ff00:42:8329) and provides an extended address space for future networking needs.

IP helps identify devices on a network and ensures that packets are correctly routed between source and destination.

TCP (Transmission Control Protocol)

TCP is a connection-oriented protocol that ensures reliable communication between devices. It follows a three-way handshake process (SYN, SYN-ACK, ACK) to establish a connection before transmitting data. TCP is commonly used for web browsing, email, and file transfers where data integrity is critical.

UDP (User Datagram Protocol)

UDP is a connectionless protocol used for fast, low-latency communication. Unlike TCP, UDP does not guarantee packet delivery, making it ideal for real-time applications like video streaming, online gaming, and VoIP.

HTTP/HTTPS

- **HTTP (Hypertext Transfer Protocol)**: Used for communication between web browsers and servers. It operates over TCP port 80 and transmits data in plaintext.
- **HTTPS (Secure HTTP)**: An encrypted version of HTTP that uses SSL/TLS to protect data from eavesdropping. It operates over TCP port 443.

Analyzing HTTP/HTTPS traffic in Wireshark helps identify web requests, responses, and potential security threats like unencrypted credentials.

DNS (Domain Name System)

DNS resolves domain names (e.g., google.com) into IP addresses. It operates over UDP port 53 and is a common target for cyber threats such as DNS spoofing and cache poisoning. Wireshark can be used to monitor DNS queries and detect suspicious domains.

ARP (Address Resolution Protocol)

ARP translates IP addresses to MAC addresses within a local network. It is essential for communication between devices on the same subnet. However, ARP spoofing attacks can manipulate MAC address resolution to redirect traffic maliciously.

ICMP (Internet Control Message Protocol)

ICMP is used for network diagnostics and error reporting. The most common ICMP command is **ping**, which tests network connectivity. Attackers often exploit ICMP for reconnaissance (e.g., ping sweeps) or denial-of-service (DoS) attacks.

Conclusion

Wireshark is a fundamental tool in network forensics, enabling professionals to capture, analyze, and interpret network traffic effectively. By understanding key network protocols and forensic techniques, analysts can detect security threats, troubleshoot network issues, and gather evidence for cyber investigations.