WIRESHARK

Wireshark is a popular open-source network protocol analyzer used to capture and analyze network traffic in real time. It allows users to inspect the data flowing through their networks, troubleshoot network issues, and understand protocol behavior in-depth. Here's a breakdown of some key features and uses of Wireshark:

Key Features of Wireshark:

1. **Packet Capture**: Wireshark can capture live network traffic from various network interfaces (Wi-Fi, Ethernet, etc.), allowing users to monitor network activity.
2. **Deep Protocol Inspection**: It supports analysis of hundreds of protocols like TCP, UDP, HTTP, DNS, FTP, and more, displaying the structure of each packet down to the byte level.
3. **Filter Capabilities**: Wireshark provides powerful filtering options (e.g., display filters, capture filters) to narrow down captured traffic and focus on specific data of interest.
4. **Reassembly of Protocols**: Wireshark can reassemble higher-level protocols (e.g., HTTP or FTP) from the packets and display them as a whole stream, making it easier to understand complex network interactions.
5. **Live Capture and Offline Analysis**: You can capture network traffic in real-time or analyze previously saved capture files (PCAP files).
6. **Exporting Data**: Wireshark allows exporting captured data to various formats like CSV, JSON, or plain text for further analysis or reporting.
7. **Color Coding**: Users can apply color rules to distinguish packet types and status, which helps in quick identification of issues or anomalies.
8. **Statistics and Graphs**: Wireshark provides statistical tools to analyze traffic patterns, flow graphs, and protocol distribution over time.

Common Uses of Wireshark:

1. **Network Troubleshooting**: Network administrators and security professionals use Wireshark to troubleshoot network issues such as latency, packet loss, and protocol malfunctions.
2. **Security Auditing and Penetration Testing**: Wireshark can be used to inspect traffic for malicious activity, unauthorized access, or data breaches by analyzing packets for unusual behavior.
3. **Protocol Analysis and Development**: Developers use Wireshark to analyze network protocols for application development, debugging, or ensuring proper protocol implementation.
4. **Learning and Research**: Students and network professionals use Wireshark to understand how protocols work and to conduct network research.

How Wireshark Works:

1. **Capture Mode**: In this mode, Wireshark listens to a network interface and records all the packets traveling over the network.

2. **Display Mode**: After capturing packets, Wireshark displays them in a human-readable form, showing each packet's details such as source/destination IP, protocol, and contents.
3. **Filtering**: Users can apply filters (e.g., `ip.addr == 192.168.0.1` to view all traffic from a specific IP) to focus on relevant data.
4. **Decoding**: Wireshark decodes various protocol headers and data formats, providing detailed information about each layer in the communication stack.

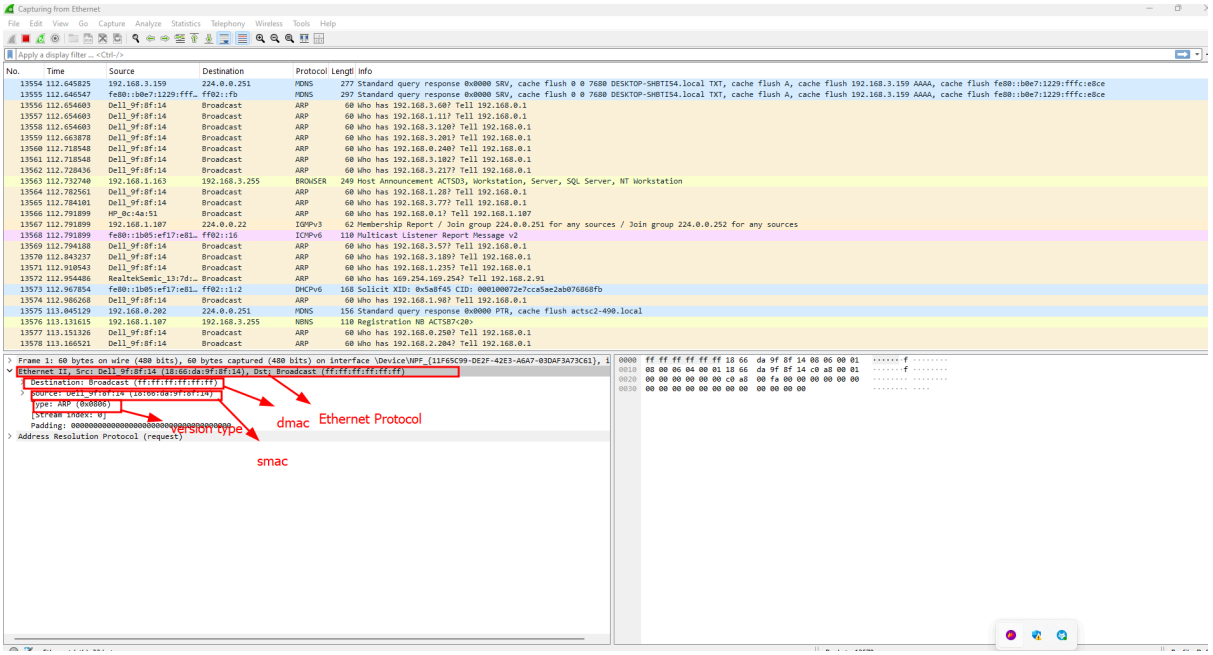
Example Workflow:

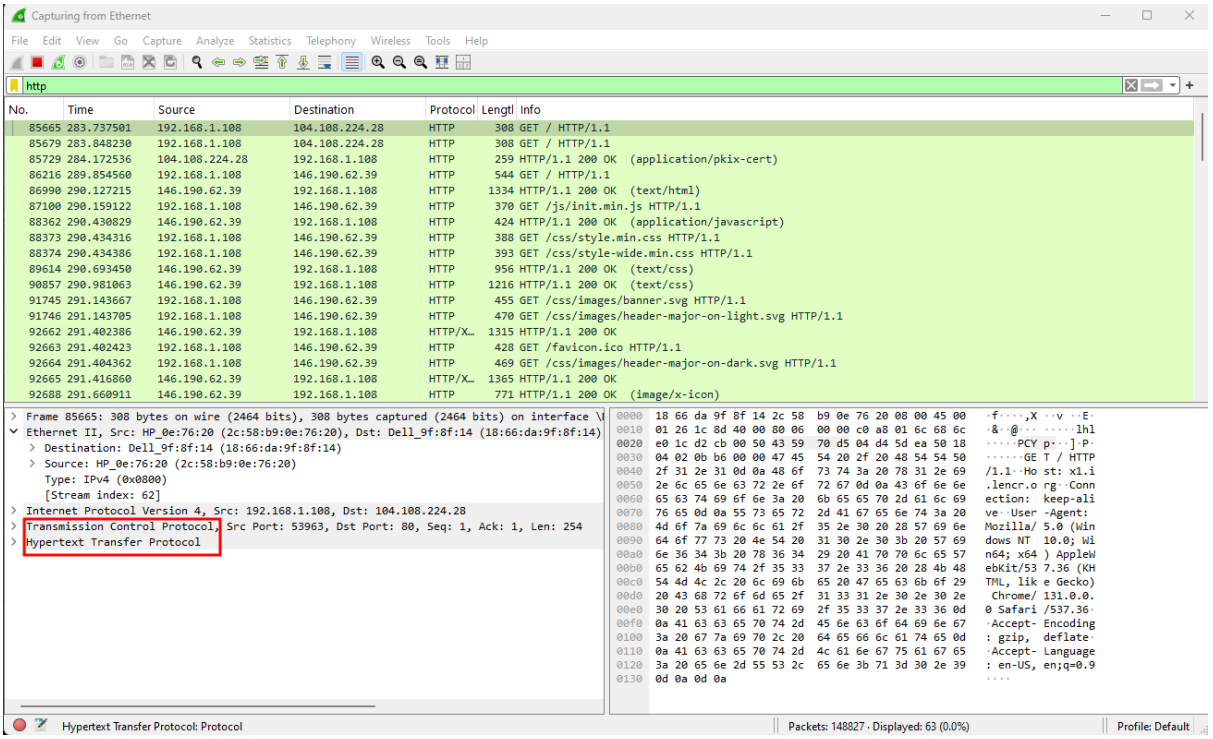
1. Open Wireshark and start a capture session on a specific network interface (e.g., Wi-Fi or Ethernet).
2. Analyze packets in real-time as they are captured, applying filters to focus on specific traffic (e.g., HTTP or DNS packets).
3. Use Wireshark's statistical tools to analyze network performance or detect unusual patterns.
4. Save the captured traffic as a `.pcap` file for later analysis or sharing.

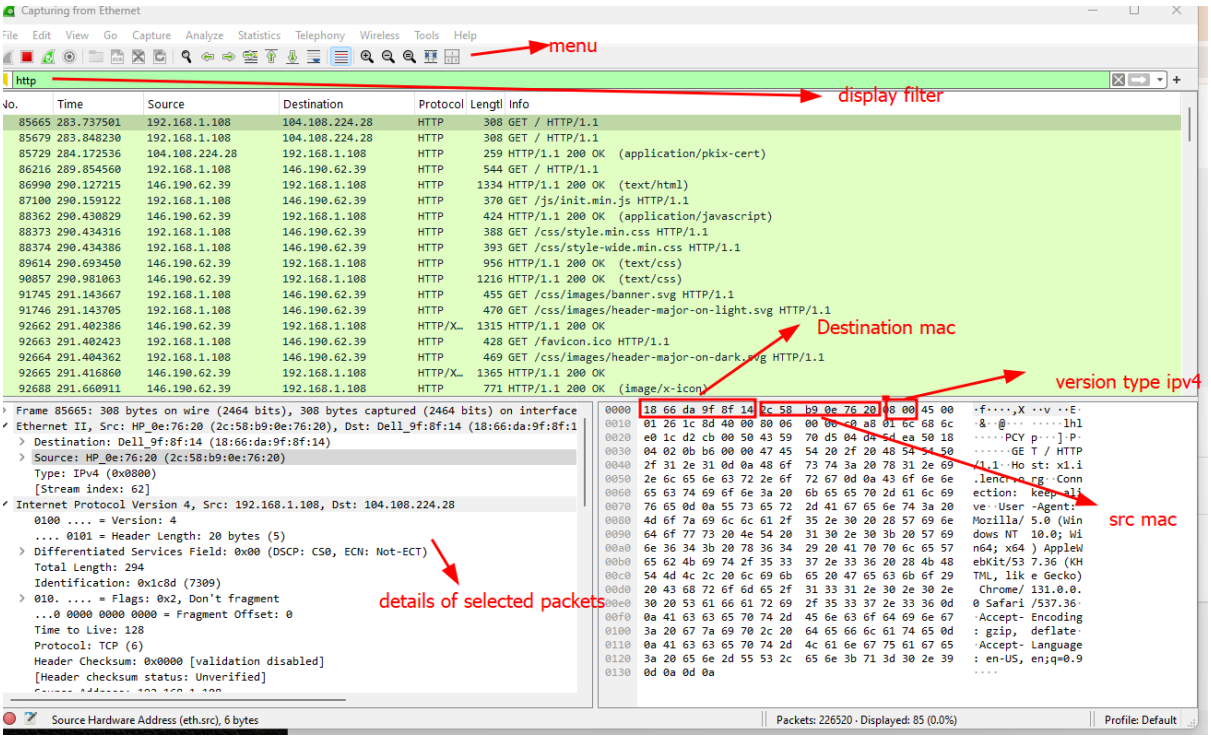
Considerations:

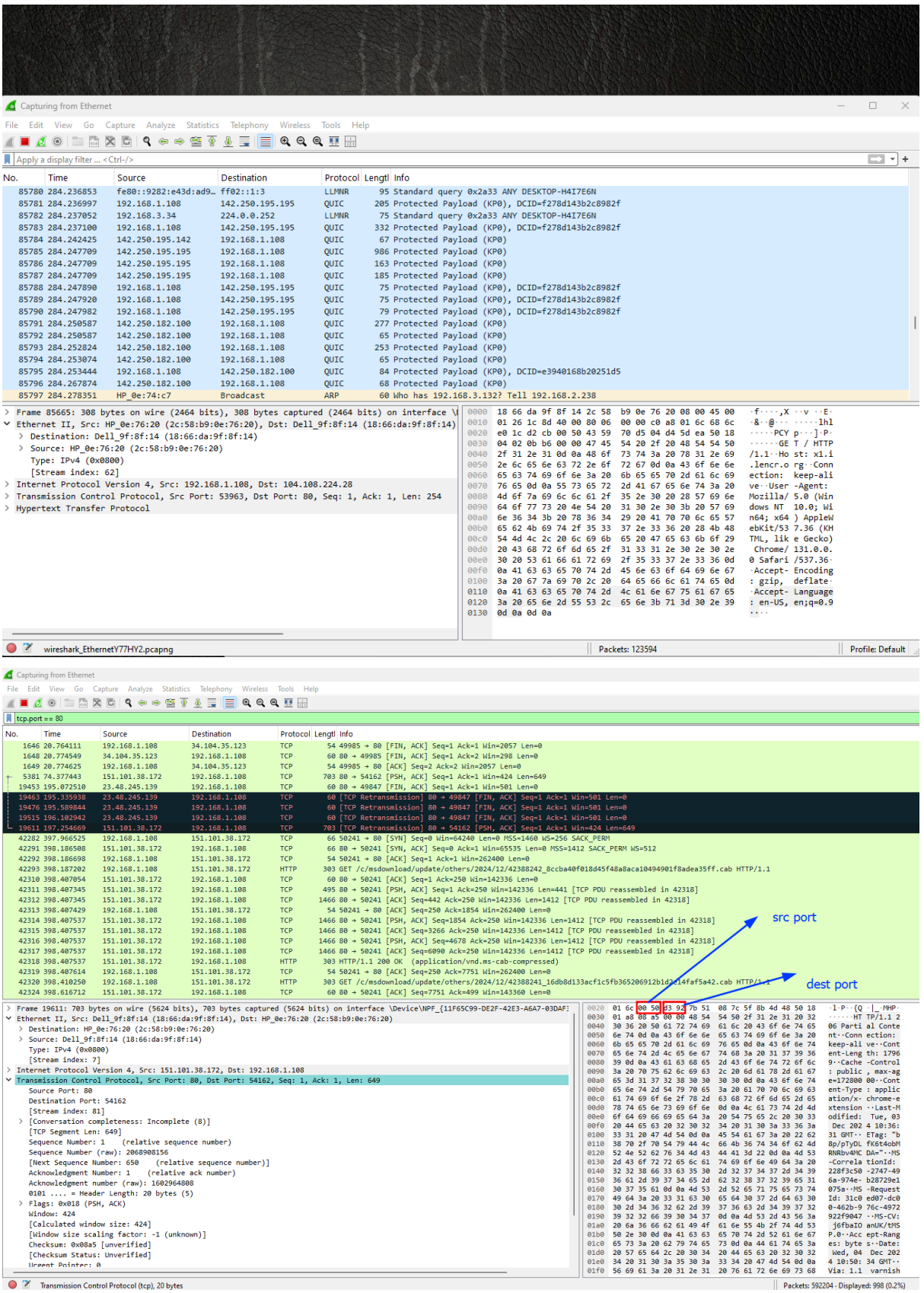
- **Legal and Ethical Issues**: Capturing network traffic can violate privacy or legal boundaries. Always obtain permission before using Wireshark on networks that you don't own or administer.
- **Overhead**: Capturing a large volume of traffic, especially on high-speed networks, can introduce overhead on system performance.

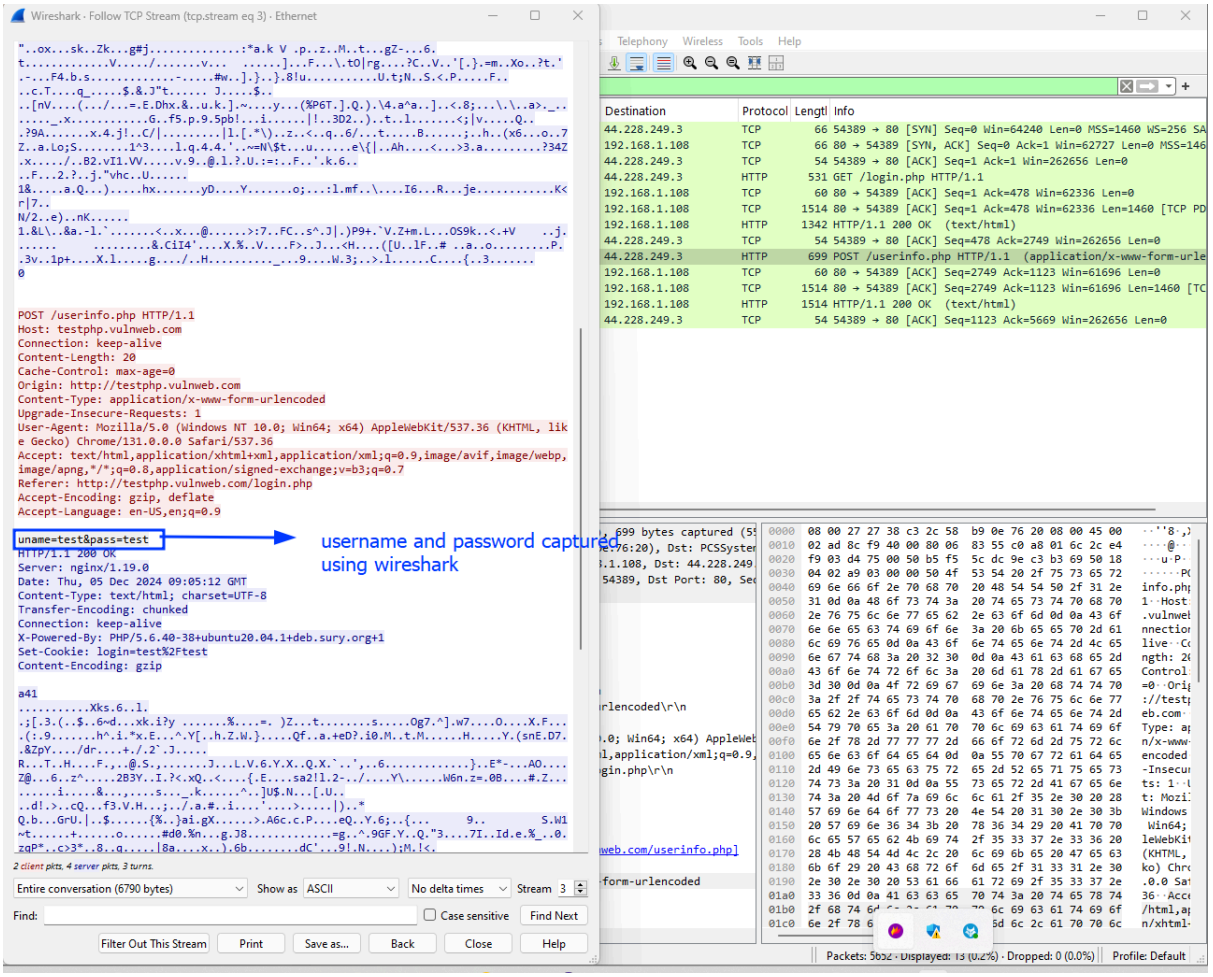
Wireshark is widely considered a go-to tool for network engineers, administrators, and security experts for its powerful features and user-friendly interface.


Ethernet II, Src: Dell_9f:8f:14 (18:66:da:9f:8f:14), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Destination: Broadcast (ff:ff:ff:ff:ff:ff)
Type: ARP (0x0806)
Address Resolution Protocol (request)
version type
dmac
Ethernet Protocol
smac


Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Lengtl Info
85665 283.737501 192.168.1.108 104.108.224.28 HTTP 308 GET / HTTP/1.1
85679 283.848230 192.168.1.108 104.108.224.28 HTTP 308 GET / HTTP/1.1
85729 284.172536 104.108.224.28 192.168.1.108 HTTP 259 HTTP/1.1 200 OK (application/pkix-cert)
86216 289.854560 192.168.1.108 146.190.62.39 HTTP 544 GET / HTTP/1.1
86990 290.127215 146.190.62.39 192.168.1.108 HTTP 1334 HTTP/1.1 200 OK (text/html)
87100 290.159122 192.168.1.108 146.190.62.39 HTTP 370 GET /js/init.min.js HTTP/1.1
88362 290.430829 146.190.62.39 192.168.1.108 HTTP 424 HTTP/1.1 200 OK (application/javascript)
88373 290.434316 192.168.1.108 146.190.62.39 HTTP 388 GET /css/style.min.css HTTP/1.1
88374 290.434386 192.168.1.108 146.190.62.39 HTTP 393 GET /css/style-wide.min.css HTTP/1.1
89614 290.693450 146.190.62.39 192.168.1.108 HTTP 956 HTTP/1.1 200 OK (text/css)
90857 290.981063 146.190.62.39 192.168.1.108 HTTP 1216 HTTP/1.1 200 OK (text/css)
91745 291.143667 192.168.1.108 146.190.62.39 HTTP 455 GET /css/images/banner.svg HTTP/1.1
91746 291.143705 192.168.1.108 146.190.62.39 HTTP 470 GET /css/images/header-major-on-light.svg HTTP/1.1
92662 291.402386 146.190.62.39 192.168.1.108 HTTP/X… 1315 HTTP/1.1 200 OK
92663 291.402423 192.168.1.108 146.190.62.39 HTTP 428 GET /favicon.ico HTTP/1.1
92664 291.404362 192.168.1.108 146.190.62.39 HTTP 469 GET /css/images/header-major-on-dark.svg HTTP/1.1
92665 291.416860 146.190.62.39 192.168.1.108 HTTP/X… 1365 HTTP/1.1 200 OK
92688 291.660911 146.190.62.39 192.168.1.108 HTTP 771 HTTP/1.1 200 OK (image/x-icon)
Frame 85665: 308 bytes on wire (2464 bits), 308 bytes captured (2464 bits) on interface \
Ethernet II, Src: HP_0e:76:20 (2c:58:b9:0e:76:20), Dst: Dell_9f:8f:14 (18:66:da:9f:8f:14)
Destination: Dell_9f:8f:14 (18:66:da:9f:8f:14)
Source: HP_0e:76:20 (2c:58:b9:0e:76:20)
Type: IPv4 (0x0800)
[Stream index: 62]
Internet Protocol Version 4, Src: 192.168.1.108, Dst: 104.108.224.28
Transmission Control Protocol, Src Port: 53963, Dst Port: 80, Seq: 1, Ack: 1, Len: 254
Hypertext Transfer Protocol
Hypertext Transfer Protocol: Protocol
Packets: 148827 · Displayed: 63 (0.0%)
Profile: Default


Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
menu
http
display filter
No. Time Source Destination Protocol Length Info
85665 283.737501 192.168.1.108 104.108.224.28 HTTP 308 GET / HTTP/1.1
85679 283.848230 192.168.1.108 104.108.224.28 HTTP 308 GET / HTTP/1.1
85729 284.172536 104.108.224.28 192.168.1.108 HTTP 259 HTTP/1.1 200 OK (application/pkix-cert)
86216 289.854560 192.168.1.108 146.190.62.39 HTTP 544 GET / HTTP/1.1
86990 290.127215 146.190.62.39 192.168.1.108 HTTP 1334 HTTP/1.1 200 OK (text/html)
87100 290.159122 192.168.1.108 146.190.62.39 HTTP 370 GET /js/init.min.js HTTP/1.1
88362 290.430829 146.190.62.39 192.168.1.108 HTTP 424 HTTP/1.1 200 OK (application/javascript)
88373 290.434316 192.168.1.108 146.190.62.39 HTTP 388 GET /css/style.min.css HTTP/1.1
88374 290.434386 192.168.1.108 146.190.62.39 HTTP 393 GET /css/style-wide.min.css HTTP/1.1
89614 290.693450 146.190.62.39 192.168.1.108 HTTP 956 HTTP/1.1 200 OK (text/css)
90857 290.981063 146.190.62.39 192.168.1.108 HTTP 1216 HTTP/1.1 200 OK (text/css)
91745 291.143667 192.168.1.108 146.190.62.39 HTTP 455 GET /css/images/banner.svg HTTP/1.1
91746 291.143705 192.168.1.108 146.190.62.39 HTTP 470 GET /css/images/header-major-on-light.svg HTTP/1.1
92662 291.402386 146.190.62.39 192.168.1.108 HTTP/X... 1315 HTTP/1.1 200 OK
92663 291.402423 192.168.1.108 146.190.62.39 HTTP 428 GET /favicon.ico HTTP/1.1
92664 291.404362 192.168.1.108 146.190.62.39 HTTP 469 GET /css/images/header-major-on-dark.svg HTTP/1.1
92665 291.416860 146.190.62.39 192.168.1.108 HTTP/X... 1365 HTTP/1.1 200 OK
92688 291.660911 146.190.62.39 192.168.1.108 HTTP 771 HTTP/1.1 200 OK (image/x-icon)
Destination mac
version type ipv4
src mac
Frame 85665: 308 bytes on wire (2464 bits), 308 bytes captured (2464 bits) on interface
Ethernet II, Src: HP_0e:76:20 (2c:58:b9:0e:76:20), Dst: Dell_9f:8f:14 (18:66:da:9f:8f:1
Destination: Dell_9f:8f:14 (18:66:da:9f:8f:14)
Source: HP_0e:76:20 (2c:58:b9:0e:76:20)
Type: IPv4 (0x0800)
[Stream index: 62]
Internet Protocol Version 4, Src: 192.168.1.108, Dst: 104.108.224.28
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 294
Identification: 0x1c8d (7309)
010. .... = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: TCP (6)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
details of selected packets
0000 18 66 da 9f 8f 14 2c 58 b9 0e 76 20 08 00 45 00
0010 01 26 1c 8d 40 00 80 06 00 00 c0 a8 01 6c 68 6c
0020 e0 1c d2 cb 00 50 43 59 70 d5 04 d4 5d ea 50 18
0030 04 02 0b b6 00 00 47 45 54 20 2f 20 48 54 54 50
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 78 31 2e 69
0050 2e 6c 65 6e 63 72 2e 6f 72 67 0d 0a 43 6f 6e 6e
0060 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69
0070 76 65 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20
0080 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e
0090 64 6f 77 73 20 4e 54 20 31 30 2e 30 3b 20 57 69
00a0 6e 36 34 3b 20 78 36 34 29 20 41 70 70 6c 65 57
00b0 65 62 4b 69 74 2f 35 33 37 2e 33 36 20 28 4b 48
00c0 54 4d 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29
00d0 20 43 68 72 6f 6d 65 2f 31 33 31 2e 30 2e 30 2e
00e0 30 20 53 61 66 61 72 69 2f 35 33 37 2e 33 36 0d
00f0 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67
0100 3a 20 67 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d
0110 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 65
0120 3a 20 65 6e 2d 55 53 2c 65 6e 3b 71 3d 30 2e 39
0130 0d 0a 0d 0a
Source Hardware Address (eth.src), 6 bytes
Packets: 226520 · Displayed: 85 (0.0%)
Profile: Default


Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Lengt Info
85780 284.236853 fe80::9282:e43d:ad9… ff02::1:3 LLMNR 95 Standard query 0x2a33 ANY DESKTOP-H4I7E6N
85781 284.236997 192.168.1.108 142.250.195.195 QUIC 205 Protected Payload (KP0), DCID=f278d143b2c8982f
85782 284.237052 192.168.3.34 224.0.0.252 LLMNR 75 Standard query 0x2a33 ANY DESKTOP-H4I7E6N
85783 284.237100 192.168.1.108 142.250.195.195 QUIC 332 Protected Payload (KP0), DCID=f278d143b2c8982f
85784 284.242425 142.250.195.142 192.168.1.108 QUIC 67 Protected Payload (KP0)
85785 284.247709 142.250.195.195 192.168.1.108 QUIC 986 Protected Payload (KP0)
85786 284.247709 142.250.195.195 192.168.1.108 QUIC 163 Protected Payload (KP0)
85787 284.247709 142.250.195.195 192.168.1.108 QUIC 185 Protected Payload (KP0)
85788 284.247890 192.168.1.108 142.250.195.195 QUIC 75 Protected Payload (KP0), DCID=f278d143b2c8982f
85789 284.247920 192.168.1.108 142.250.195.195 QUIC 75 Protected Payload (KP0), DCID=f278d143b2c8982f
85790 284.247982 192.168.1.108 142.250.195.195 QUIC 79 Protected Payload (KP0), DCID=f278d143b2c8982f
85791 284.250587 142.250.182.100 192.168.1.108 QUIC 277 Protected Payload (KP0)
85792 284.250587 142.250.182.100 192.168.1.108 QUIC 65 Protected Payload (KP0)
85793 284.252824 142.250.182.100 192.168.1.108 QUIC 253 Protected Payload (KP0)
85794 284.253074 142.250.182.100 192.168.1.108 QUIC 65 Protected Payload (KP0)
85795 284.253444 192.168.1.108 142.250.182.100 QUIC 84 Protected Payload (KP0), DCID=e3940168b20251d5
85796 284.267874 142.250.182.100 192.168.1.108 QUIC 68 Protected Payload (KP0)
85797 284.278351 HP_0e:74:c7 Broadcast ARP 60 Who has 192.168.3.132? Tell 192.168.2.238
Frame 85665: 308 bytes on wire (2464 bits), 308 bytes captured (2464 bits) on interface \
Ethernet II, Src: HP_0e:76:20 (2c:58:b9:0e:76:20), Dst: Dell_9f:8f:14 (18:66:da:9f:8f:14)
Destination: Dell_9f:8f:14 (18:66:da:9f:8f:14)
Source: HP_0e:76:20 (2c:58:b9:0e:76:20)
Type: IPv4 (0x0800)
[Stream index: 62]
Internet Protocol Version 4, Src: 192.168.1.108, Dst: 104.108.224.28
Transmission Control Protocol, Src Port: 53963, Dst Port: 80, Seq: 1, Ack: 1, Len: 254
Hypertext Transfer Protocol
0000 18 66 da 9f 8f 14 2c 58 b9 0e 76 20 08 00 45 00
0010 01 26 1c 8d 40 00 80 06 00 00 c0 a8 01 6c 68 6c
0020 e0 1c d2 cb 00 50 43 59 70 d5 04 d4 5d ea 50 18
0030 04 02 0b b6 00 00 47 45 54 20 2f 20 48 54 54 50
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 78 31 2e 69
0050 2e 6c 65 6e 63 72 2e 6f 72 67 0d 0a 43 6f 6e 6e
0060 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69
0070 76 65 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20
0080 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e
0090 64 6f 77 73 20 4e 54 20 31 30 2e 30 3b 20 57 69
00a0 6e 36 34 3b 20 78 36 34 29 20 41 70 70 6c 65 57
00b0 65 62 4b 69 74 2f 35 33 37 2e 33 36 20 28 4b 48
00c0 54 4d 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29
00d0 20 43 68 72 6f 6d 65 2f 31 33 31 2e 30 2e 30 2e
00e0 30 20 53 61 66 61 72 69 2f 35 33 37 2e 33 36 0d
00f0 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67
0100 3a 20 67 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d
0110 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 65
0120 3a 20 65 6e 2d 55 53 2c 65 6e 3b 71 3d 30 2e 39
0130 0d 0a 0d 0a
wireshark_EthernetY77HY2.pcapng
Packets: 123594
Profile: Default
Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 80
No. Time Source Destination Protocol Lengt Info
1646 20.764111 192.168.1.108 34.104.35.123 TCP 54 49985 → 80 [FIN, ACK] Seq=1 Ack=1 Win=2057 Len=0
1648 20.774549 34.104.35.123 192.168.1.108 TCP 60 80 → 49985 [FIN, ACK] Seq=1 Ack=2 Win=298 Len=0
1649 20.774625 192.168.1.108 34.104.35.123 TCP 54 49985 → 80 [ACK] Seq=2 Ack=2 Win=2057 Len=0
5381 74.377443 151.101.38.172 192.168.1.108 TCP 703 80 → 54162 [PSH, ACK] Seq=1 Ack=1 Win=424 Len=649
19453 195.072510 23.48.245.139 192.168.1.108 TCP 60 80 → 49847 [FIN, ACK] Seq=1 Ack=1 Win=501 Len=0
19463 195.335938 23.48.245.139 192.168.1.108 TCP 60 [TCP Retransmission] 80 → 49847 [FIN, ACK] Seq=1 Ack=1 Win=501 Len=0
19476 195.589844 23.48.245.139 192.168.1.108 TCP 60 [TCP Retransmission] 80 → 49847 [FIN, ACK] Seq=1 Ack=1 Win=501 Len=0
19515 196.102942 23.48.245.139 192.168.1.108 TCP 60 [TCP Retransmission] 80 → 49847 [FIN, ACK] Seq=1 Ack=1 Win=501 Len=0
19611 197.254669 151.101.38.172 192.168.1.108 TCP 703 [TCP Retransmission] 80 → 54162 [PSH, ACK] Seq=1 Ack=1 Win=424 Len=649
42282 397.966525 192.168.1.108 151.101.38.172 TCP 66 50241 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
42291 398.186508 151.101.38.172 192.168.1.108 TCP 66 80 → 50241 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=512
42292 398.186698 192.168.1.108 151.101.38.172 TCP 54 50241 → 80 [ACK] Seq=1 Ack=1 Win=262400 Len=0
42293 398.187202 192.168.1.108 151.101.38.172 HTTP 303 GET /c/msdownload/update/others/2024/12/42388242_8ccba40f018d45f48a8aca10494901f8adea35ff.cab HTTP/1.1
42310 398.407054 151.101.38.172 192.168.1.108 TCP 60 80 → 50241 [ACK] Seq=1 Ack=250 Win=142336 Len=0
42311 398.407345 151.101.38.172 192.168.1.108 TCP 495 80 → 50241 [PSH, ACK] Seq=1 Ack=250 Win=142336 Len=441 [TCP PDU reassembled in 42318]
42312 398.407345 151.101.38.172 192.168.1.108 TCP 1466 80 → 50241 [ACK] Seq=442 Ack=250 Win=142336 Len=1412 [TCP PDU reassembled in 42318]
42313 398.407429 192.168.1.108 151.101.38.172 TCP 54 50241 → 80 [ACK] Seq=250 Ack=1854 Win=262400 Len=0
42314 398.407537 151.101.38.172 192.168.1.108 TCP 1466 80 → 50241 [PSH, ACK] Seq=1854 Ack=250 Win=142336 Len=1412 [TCP PDU reassembled in 42318]
42315 398.407537 151.101.38.172 192.168.1.108 TCP 1466 80 → 50241 [ACK] Seq=3266 Ack=250 Win=142336 Len=1412 [TCP PDU reassembled in 42318]
42316 398.407537 151.101.38.172 192.168.1.108 TCP 1466 80 → 50241 [PSH, ACK] Seq=4678 Ack=250 Win=142336 Len=1412 [TCP PDU reassembled in 42318]
42317 398.407537 151.101.38.172 192.168.1.108 TCP 1466 80 → 50241 [ACK] Seq=6090 Ack=250 Win=142336 Len=1412 [TCP PDU reassembled in 42318]
42318 398.407537 151.101.38.172 192.168.1.108 HTTP 303 HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
42319 398.407614 192.168.1.108 151.101.38.172 TCP 54 50241 → 80 [ACK] Seq=250 Ack=7751 Win=262400 Len=0
42320 398.410250 192.168.1.108 151.101.38.172 HTTP 303 GET /c/msdownload/update/others/2024/12/42388241_16db8d133acf1c5fb365206912b1d2c14faf5a42.cab HTTP/1.1
42324 398.616712 151.101.38.172 192.168.1.108 TCP 60 80 → 50241 [ACK] Seq=7751 Ack=499 Win=143360 Len=0
src port
dest port
Frame 19611: 703 bytes on wire (5624 bits), 703 bytes captured (5624 bits) on interface \Device\NPF_{11F65C99-DE2F-42E3-A6A7-03DAF:
Ethernet II, Src: Dell_9f:8f:14 (18:66:da:9f:8f:14), Dst: HP_0e:76:20 (2c:58:b9:0e:76:20)
Destination: HP_0e:76:20 (2c:58:b9:0e:76:20)
Source: Dell_9f:8f:14 (18:66:da:9f:8f:14)
Type: IPv4 (0x0800)
[Stream index: 7]
Internet Protocol Version 4, Src: 151.101.38.172, Dst: 192.168.1.108
Transmission Control Protocol, Src Port: 80, Dst Port: 54162, Seq: 1, Ack: 1, Len: 649
Source Port: 80
Destination Port: 54162
[Stream index: 81]
[Conversation completeness: Incomplete (8)]
[TCP Segment Len: 649]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 2063908156
[Next Sequence Number: 650 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 1602964808
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window: 424
[Calculated window size: 424]
[Window size scaling factor: -1 (unknown)]
Checksum: 0x08a5 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
0020 01 6c 00 50 d3 92 7b 51 08 7c 5f 8b 4d 48 50 18
0030 01 a8 08 a5 00 00 48 54 54 50 2f 31 2e 31 20 32
0040 30 36 20 50 61 72 74 69 61 6c 20 43 6f 6e 74 65
0050 6e 74 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20
0060 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 43 6f 6e 74
0070 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 31 37 39 36
0080 39 0d 0a 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c
0090 3a 20 70 75 62 6c 69 63 2c 20 6d 61 78 2d 61 67
00a0 65 3d 31 37 32 38 30 30 30 0d 0a 43 6f 6e 74
00b0 65 6e 74 2d 54 79 70 65 3a 20 61 70 70 6c 69 63
00c0 61 74 69 6f 6e 2f 78 2d 63 68 72 6f 6d 65 2d 65
00d0 78 74 65 6e 73 69 6f 6e 0d 0a 4c 61 73 74 2d 4d
00e0 6f 64 69 66 69 65 64 3a 20 54 75 65 2c 20 30 33
00f0 20 44 65 63 20 32 30 32 34 20 31 30 3a 33 36 3a
0100 33 31 20 47 4d 54 0d 0a 45 54 61 67 3a 20 22 62
0110 38 70 2f 70 54 79 44 4c 66 4b 36 74 34 6f 62 4d
0120 52 4e 52 62 76 34 4d 43 44 41 3d 22 0d 0a 4d 53
0130 2d 43 6f 72 72 65 6c 61 74 69 6f 6e 49 64 3a 20
0140 32 32 38 66 33 63 35 30 2d 32 37 34 37 2d 34 39
0150 36 61 2d 39 37 34 65 2d 62 32 38 37 32 39 65 31
0160 30 37 35 61 0d 0a 4d 53 2d 52 65 71 75 65 73 74
0170 49 64 3a 20 33 31 63 30 65 64 30 37 2d 64 63 30
0180 30 2d 34 36 32 62 2d 39 37 36 63 2d 34 39 37 32
0190 39 32 32 66 39 30 34 37 0d 0a 4d 53 2d 43 56 3a
01a0 20 6a 36 66 62 61 49 4f 61 6e 55 4b 2f 74 4d 53
01b0 50 2e 30 0d 0a 41 63 63 65 70 74 2d 52 61 6e 67
01c0 65 73 3a 20 62 79 74 65 73 0d 0a 44 61 74 65 3a
01d0 20 57 65 64 2c 20 30 34 20 44 65 63 20 32 30 32
01e0 34 20 31 30 3a 35 30 3a 33 34 20 47 4d 54 0d 0a
01f0 56 69 61 3a 20 31 2e 31 20 76 61 72 6e 69 73 68
Transmission Control Protocol (tcp), 20 bytes
Packets: 592204 · Displayed: 998 (0.2%)



Username and password of http website captured using wireshark

Anushree N
Roll no : 07