

## Wireshark lab1 :

Source id : 172.20.0.54

Destination id : 34.104.35.123

The image displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for packet capture and analysis. The main display area is divided into three panes:

- Packets Pane:** Shows a list of captured packets. The selected packet is 586, which is an HTTP GET request to /edgedl/chromewebstore/L2Nocm9tZV9leHRlbnNpb24vYm9vYnVjZDctOTExOjU0LTgyLWJtN2FLY2ZjNDg0NmNj/1.0. The packet length is 427 bytes.
- Packet Details Pane:** Provides a hierarchical view of the selected packet's structure. It shows the Ethernet II header, Internet Protocol Version 4 header, and Hypertext Transfer Protocol header.
- Packet Bytes Pane:** Displays the raw data of the selected packet in hexadecimal and ASCII. The data starts with 0000 00 50 56 92 93 9d 00 50 56 92 1d 18 08 00 45 00.

The status bar at the bottom indicates that 1885 packets are displayed, with 8 (0.4%) selected. The profile is set to Default.

### Overview of Wireshark

Wireshark is a widely-used network protocol analyzer that captures and interactively browses the traffic running on a computer network. It provides deep inspection of hundreds of protocols and is valuable for troubleshooting network problems, examining security issues, and developing software and protocols.

**Start Wireshark :** Open Wireshark and select the network interface you want to capture packets from (e.g., Ethernet, Wi-Fi).

- **Start Capture :** Click on the interface name and then click the green "Start" button to begin capturing packets.

- **Apply Capture Filters :** Optionally, apply capture filters to limit the captured packets to specific criteria (e.g., IP addresses, protocols) to focus on relevant traffic.

## Analyzing Packets

Once you've captured packets, you can analyze them in various ways:

- Packet List Pane : Displays a list of captured packets with summary information (e.g., source and destination addresses, protocols, packet length).
- Packet Details Pane : Provides a detailed view of a selected packet, showing the packet header, its raw data (hex dump), and protocol-specific information.
- Packet Bytes Pane : Shows the raw bytes of the selected packet in hexadecimal and ASCII format.

The image shows the Wireshark network protocol analyzer interface. The top pane displays a list of captured packets. The middle pane shows the details of the selected packet (Frame 586), including the Ethernet II header, Internet Protocol Version 4 header, and Hypertext Transfer Protocol header. The bottom pane shows the raw bytes of the packet in hexadecimal and ASCII format.

No.	Time	Source	Destination	Protocol	Length	Info
592	925.107723	34.104.35.123	172.20.0.54	HTTP	874	HTTP/1.1 200 OK (application/x-chrome-extension)
761	1084.002946	95.140.236.0	172.20.0.54	HTTP	309	HTTP/1.1 304 Not Modified
764	1084.202694	95.140.236.0	172.20.0.54	HTTP	306	HTTP/1.1 304 Not Modified
767	1084.392674	95.140.236.0	172.20.0.54	HTTP	309	HTTP/1.1 304 Not Modified
586	925.068577	172.20.0.54	34.104.35.123	HTTP	427	GET /edgedl/chromewebstore/L2Nocm9tZV9leHRlbnNpb24vYmVxYnVjYjYwZDctOTExOjU0MjY2ZjY0Dg0mNj/1.0.0.1
759	1083.837179	172.20.0.54	95.140.236.0	HTTP	340	GET /msdownload/update/v3/static/trusted/en/disallowedcertstl.cab?e0001f50e08ae05f HTTP/1.1
762	1084.036489	172.20.0.54	95.140.236.0	HTTP	335	GET /msdownload/update/v3/static/trusted/en/authrootstl.cab?ef1838a3f036bfad HTTP/1.1
765	1084.226728	172.20.0.54	95.140.236.0	HTTP	336	GET /msdownload/update/v3/static/trusted/en/pinrulesstl.cab?256af5aebd65fc99 HTTP/1.1

Frame 586: 427 bytes on wire (3416 bits), 427 bytes captured (3416 bits) on interface 0

Ethernet II, Src: VMware\_92:1d:18 (00:50:56:92:1d:18), Dst: VMware\_92:93:9d (00:50:56:92:93:9d)

Source: VMware\_92:1d:18 (00:50:56:92:1d:18)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 172.20.0.54, Dst: 34.104.35.123

Transmission Control Protocol, Src Port: 49894, Dst Port: 80

Hypertext Transfer Protocol

0000 00 50 56 92 93 9d 00 50 56 92 1d 18 00 00 45 00 PV...P V....E-  
0010 01 9d ac ef 40 00 00 06 00 00 ac 14 00 36 22 68 ...@... ..6"h  
0020 23 7b c2 e6 00 50 da 0e a4 89 4e 20 7d 74 50 18 #...P...N }tP  
0030 04 04 f3 bc 00 00 47 45 54 20 2f 65 64 67 65 64 ...GE T /edged  
0040 6c 2f 63 68 72 6f 6d 65 77 65 62 73 74 6f 72 65 l/chrome webstore  
0050 2f 4c 32 4e 6f 63 6d 39 74 5a 56 39 6c 65 48 52 /L2Nocm9 tZV9leHR  
0060 6c 62 6e 4e 70 62 32 34 76 59 6d 78 76 59 6e 4d lbnNpb24 vYmVxYnM  
0070 76 59 6a 68 6b 59 57 59 77 5a 44 63 74 4f 54 45 vYjYkYwY wZDctOTE  
0080 78 4f 53 30 30 4d 47 51 35 4c 54 67 79 4e 6a 41 xO500MGQ 5LTgyNjA  
0090 74 4e 32 4e 6c 59 32 5a 6a 4d 44 67 30 4e 6d 4e tN2f1Y2Z jYDg0mN  
00a0 6a 2f 31 2e 30 2e 30 2e 31 37 5f 6c 6b 67 6a j/1.0.0. 17 1lkGj  
00b0 66 66 63 64 70 66 66 6d 68 69 61 6b 6d 66 63 64 ffdpffe hIakmfcd  
00c0 63 62 6c 6f 68 63 63 70 66 6d 6f 2e 63 72 78 20 cblohcp fmo.crx  
00d0 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 HTTP/1.1 .Host:  
00e0 65 64 67 65 64 6c 2e 6d 65 2e 67 76 74 31 2e 63 edgedl.m e.gvtl.c  
00f0 6f 6d 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 om .Conn ection:  
0100 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 73 65 72 keep-all ve .User  
0110 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f -Agent: Mozilla/  
0120 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 5.0 (win dows NT  
0130 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 36 34 10.0; Wl n64; x64  
0140 29 20 41 70 70 6c 65 57 65 62 4b 69 74 2f 35 33 ) ApplkI ebKit/53  
0150 37 2e 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 69 6b 7.36 (KH TML, lik  
0160 65 20 47 65 63 6b 6f 29 20 43 68 72 6f 6d 65 2f e Gecko) Chrome/  
0170 31 30 35 2e 30 2e 30 2e 30 20 53 61 66 61 72 69 105.0.0. 0 Safari  
0180 2f 35 33 37 2e 33 36 0d 0a 41 63 63 65 70 74 2d /537.36 .Accept-

Wireshark capture of HTTP traffic on interface Ethernet0. The packet list shows several HTTP requests and responses. The selected packet (No. 586) is a GET request to /edgedl/chromewebstore/L2Nocm9tZV9leHRlbnNpb24vYmxvYnNkVjhhkVnWZdOTExOS08MGQ5LTgytjAtN2F1Y2ZjMDg0NmNj/1.0.0.1. The packet details pane shows the structure of the HTTP request, including the GET method, host, and user-agent. The packet bytes pane shows the raw data in hexadecimal and ASCII.

## Using Filters:

Display filters (e.g., http, tcp.port == 80).

Capture filters to limit the data being captured (e.g., host 192.168.1.1).

Exporting Data:

Save capture files for later analysis or sharing.

Export specific packets or summaries to various formats (e.g., CSV, XML).

Wireshark capture of HTTP traffic on interface Ethernet0. The packet list shows several HTTP requests and responses. The selected packet (No. 586) is a GET request to /edgedl/chromewebstore/L2Nocm9tZV9leHRlbnNpb24vYmxvYnNkVjhhkVnWZdOTExOS08MGQ5LTgytjAtN2F1Y2ZjMDg0NmNj/1.0.0.1. The packet details pane shows the structure of the HTTP request, including the GET method, host, and user-agent. The packet bytes pane shows the raw data in hexadecimal and ASCII.

Filtering: Use display filters to isolate specific traffic, such as `http:tcp.port == 80`, or `ip.addr == 192.168.1.1`.