

### 1. Installation of Wireshark

- **Action:** Installed Wireshark on the system.
- **Details:** Downloaded the software from the official website: <https://www.wireshark.org/download.html>. Selected the version compatible with the operating system (e.g., Windows 11, macOS, or Linux) and followed the installation wizard. Launched Wireshark to confirm successful installation.

### 2. Initiation of Packet Capture

- **Action:** Began capturing packets on the active network interface.
- **Details:** Opened Wireshark and selected the active interface (e.g., Wi-Fi or Ethernet) from the list of available options. Clicked "Start" with administrative privileges to initiate real-time packet capture.

### 3. Generation of Network Traffic

- **Action:** Generated network traffic by browsing a website or pinging a server.
- **Details:** Opened a web browser and visited <https://www.example.com>, or used the command line to execute ping google.com. Performed these actions for approximately 30-60 seconds to create sample traffic for analysis.

### 4. Termination of Capture

- **Action:** Stopped the packet capture after one minute.
- **Details:** Returned to Wireshark and clicked the "Stop" button (red square) after capturing traffic for about one minute. Verified that a sufficient number of packets were recorded in the interface.

### 5. Application of Protocol Filters

- **Action:** Applied filters to isolate packets by protocol.
- **Details:** Utilized the Wireshark filter bar to apply specific protocol filters: typed http to view HTTP traffic, dns for DNS queries, and tcp for TCP packets. Pressed Enter after each filter to display relevant packets.

### 6. Identification of Protocols

- **Action:** Identified at least three different protocols in the captured traffic.
- **Details:** Analyzed the filtered packets and used the "Protocol Hierarchy" option (right-click a packet > Statistics > Protocol Hierarchy) to confirm protocols. Identified examples include:
  - **HTTP:** Traffic on port 80 related to web browsing.
  - **DNS:** Queries on port 53 for domain name resolution.
  - **TCP:** Handshake packets on various ports for reliable data transfer.

# Packet Analysis with Wireshark on a Personal Network

## HTTP Packets:

The screenshot shows a Wireshark packet capture of an HTTP transaction. The packet list on the left shows two packets: a GET request (No. 7356) and its corresponding 200 OK response (No. 7365). The selected packet (No. 7365) is expanded in the packet details pane, showing the Ethernet II, Internet Protocol Version 6, and Hypertext Transfer Protocol layers. The packet bytes pane on the right displays the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
7356	348.896085	2402:8100:2968:17e3::64	2402:8100:2968:17e3::64	HTTP	287	GET /en-GB/livetitle/preinstall?region=IN&appid=C98EAS0842088940588F07E1DA76512021FE3&FORN=Threshold HTTP/1.1
7365	349.830750	64:ff9b::1726:32ca	2402:8100:2968:17e3::64	HTTP/X	1289	HTTP/1.1 200 OK

Packet details for No. 7365:

- Frame 7365: 287 bytes on wire (2296 bits), 287 bytes captured (2296 bits) on interface \Device\NPF...
- Ethernet II, Src: GemtekTechno...fe59:28 (20:10:7a:fe59:28), Dst: f2:99:b6:f4:bc:64 (f2:99:b6:f4:bc:64)
- Internet Protocol Version 6, Src: 2402:8100:2968:17e3:40fc:4986:3925:f561, Dst: 64:ff9b::1726:32ca
- Transmission Control Protocol, Src Port: 51278, Dst Port: 80, Seq: 1, Ack: 1, Len: 213
- Hypertext Transfer Protocol

Packet bytes (hex):

```
0000  f2 99 b6 f4 bc 64 20 10 7a fe 59 28 86 dd 60 0c  ....d zY(....
0010  2e 26 00 e9 06 ff 24 02 81 00 29 b8 17 e3 40 fc  .&...$-...@
0020  49 86 39 25 f5 61 00 64 ff 9b 00 00 00 00 00 00  I-%a:d .....
0030  00 00 17 26 32 ca c8 4e 00 58 82 3c 17 56 91 ae  ...82~M-P<V-
0040  ac 2a 50 18 02 01 35 1c 00 00 47 45 54 20 2f 65  +p-5-GET /e
0050  6e 2d 47 42 2f 6c 69 76 65 74 69 6c 65 2f 70 72  n-GB/liv etitle/pr
0060  65 69 6e 73 74 61 6c 6c 3f 72 65 67 69 6f 6e 3d  einstall?region=
0070  49 4e 26 61 70 70 69 64 3d 43 39 38 45 41 35 42  IN&appid=C98EAS0
0080  30 38 34 32 44 42 42 39 34 30 35 42 42 46 30 37  08420889 40588F07
0090  31 45 31 44 41 37 36 35 31 32 44 32 31 46 45 33  1E1DA765 12021FE3
00a0  36 26 46 4f 52 4d 3d 54 68 72 65 73 68 6f 6c 64  &FORN=Threshol
00b0  20 48 54 50 2f 31 2e 31 00 0a 43 6f 6e 6e 65  HTTP/1.1: conne
00c0  63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76  ction: Keep-Aliv
00d0  65 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d  e-User-Agent: M
00e0  69 63 72 6f 73 6f 66 74 2d 57 4e 53 2f 31 30 2e  icrosoft-MS/10.
00f0  30 00 0a 48 6f 73 74 3a 20 74 69 6c 65 2d 73 65  0-Host: title-se
0100  72 76 69 63 65 2e 77 65 61 74 68 65 72 2e 6d 69  rvice.weather.m
0110  63 72 6f 73 6f 66 74 2e 63 6f 6d 0d 0a 0d 0a  crosoft.com....
```

## ICMP Packets:

The screenshot shows a Wireshark packet capture of ICMP Echo (ping) traffic. The packet list on the left shows eight packets: four requests (No. 200, 203, 205, 207) and four replies (No. 208, 209, 213, 217). The selected packet (No. 200) is expanded in the packet details pane, showing the Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol layers. The packet bytes pane on the right displays the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
200	30.036929	172.20.10.2	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=64 (reply in 203)
203	30.127591	8.8.8.8	172.20.10.2	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=115 (request in 200)
205	31.050809	172.20.10.2	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=64 (reply in 207)
207	31.140578	8.8.8.8	172.20.10.2	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=115 (request in 205)
208	32.061518	172.20.10.2	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=64 (reply in 209)
209	32.151774	8.8.8.8	172.20.10.2	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=115 (request in 208)
213	33.076922	172.20.10.2	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=64 (reply in 217)
217	33.167224	8.8.8.8	172.20.10.2	ICMP	74	Echo (ping) reply id=0x0001, seq=6/1536, ttl=115 (request in 213)

Packet details for No. 200:

- Frame 200: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF...
- Ethernet II, Src: GemtekTechno...fe59:28 (20:10:7a:fe59:28), Dst: f2:99:b6:f4:bc:64 (f2:99:b6:f4:bc:64)
- Internet Protocol Version 4, Src: 172.20.10.2, Dst: 8.8.8.8
- Internet Control Message Protocol

Packet bytes (hex):

```
0000  f2 99 b6 f4 bc 64 20 10 7a fe 59 28 08 00 45 00  ....d zY(E-
0010  00 3c 49 5c 00 00 40 01 6b 3f ac 14 0a 02 08 08  <I~g.k2.....
0020  08 08 08 00 4d 58 00 01 00 03 61 62 63 64 65 66  ...JK...abcdeg
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklm opqrstuv
0040  77 61 62 63 64 65 66 67 68 69  wabcdegf hi
```

# Packet Analysis with Wireshark on a Personal Network

## DNS Packets:

Network\_packet\_analysis.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
3004	223.139284	fe80::62ab:a6e9:b5c...	fe80::f099:b6ff:fe...	DNS	108	Standard query 0x877a HTTPS r.msftstatic.com
3020	223.153828	fe80::f099:b6ff:fe...	fe80::62ab:a6e9:b5c...	DNS	213	Standard query response 0x86e1 HTTPS edge.microsoft.com CNAME edge-microsoft-com-ax-0002-ax-msedge.net SOA n
3024	223.155699	fe80::f099:b6ff:fe...	fe80::62ab:a6e9:b5c...	DNS	236	Standard query response 0x86d2 AAAA edge.microsoft.com CNAME edge-microsoft-com-ax-0002-ax-msedge.net CNAME
3039	223.168049	fe80::f099:b6ff:fe...	fe80::62ab:a6e9:b5c...	DNS	212	Standard query response 0x86d3 A edge.microsoft.com CNAME edge-microsoft-com-ax-0002-ax-msedge.net CNAME ax-
3046	223.216217	fe80::f099:b6ff:fe...	fe80::62ab:a6e9:b5c...	DNS	332	Standard query response 0x7255 AAAA assets.msn.com CNAME assets-msn-com-world-atm-default-trafficmanager.net
3049	223.216839	fe80::f099:b6ff:fe...	fe80::62ab:a6e9:b5c...	DNS	309	Standard query response 0x8696 HTTPS assets.msn.com CNAME assets-msn-com-world-atm-default-trafficmanager.net
3053	223.217563	fe80::f099:b6ff:fe...	fe80::62ab:a6e9:b5c...	DNS	280	Standard query response 0x861a A assets.msn.com CNAME assets-msn-com-world-atm-default-trafficmanager.net CN
3072	223.220805	fe80::f099:b6ff:fe...	fe80::62ab:a6e9:b5c...	DNS	281	Standard query response 0x80b7 HTTPS r.bing.com CNAME p-static.bing-trafficmanager.net CNAME r.bing.com edge
3077	223.234036	fe80::f099:b6ff:fe...	fe80::62ab:a6e9:b5c...	DNS	252	Standard query response 0x7371 A r.bing.com CNAME p-static.bing-trafficmanager.net CNAME r.bing.com edgekey
3080	223.234288	fe80::f099:b6ff:fe...	fe80::62ab:a6e9:b5c...	DNS	202	Standard query response 0x9990 AAAA r.msftstatic.com CNAME r-msftstatic-com-a-0016-a-msedge.net CNAME a-0016-a-
3084	223.234433	fe80::f099:b6ff:fe...	fe80::62ab:a6e9:b5c...	DNS	190	Standard query response 0x5abc A r.msftstatic.com CNAME r-msftstatic-com-a-0016-a-msedge.net CNAME a-0016-a-
3087	223.234624	fe80::f099:b6ff:fe...	fe80::62ab:a6e9:b5c...	DNS	231	Standard query response 0x877a HTTPS r.msftstatic.com CNAME r-msftstatic-com-a-0016-a-msedge.net CNAME a-001

> Frame 7830: 254 bytes on wire (2032 bits), 254 bytes captured (2032 bits) on interface \Device\NPF...  
> Ethernet II, Src: f2:99:b6:f4:bc:64 (f2:99:b6:f4:bc:64), Dst: GantekTechno\_fe59:28 (20:10:7a:f2:99:b6:f4:bc:64)  
> Internet Protocol Version 4, Src: 172.20.10.1, Dst: 172.20.10.2  
> Transmission Control Protocol, Src Port: 53, Dst Port: 51298, Seq: 1, Ack: 57, Len: 200  
Source Port: 53  
Destination Port: 51298  
[Stream Index: 243]  
[Stream Packet Number: 9]  
> [Conversation completeness: Complete, WITH\_DATA (31)]  
[TCP Segment Len: 200]  
Sequence Number: 1 (relative sequence number)  
Sequence Number (raw): 64273534  
[Next Sequence Number: 201 (relative sequence number)]  
Acknowledgment Number: 57 (relative ack number)  
Acknowledgment Number (raw): 523872299  
0101 .... + Header Length: 20 bytes (5)  
Flags: 0x018 (PSH, ACK)  
Window: 4096  
[Calculated window size: 262144]  
[Window size scaling factor: 64]  
Checksum: 0x00000000 (0) (unverified)  
Test item (text), 144 bytes

Packets: 7858 - Displayed: 392 (5.0%) Profile: Default

## DNS Packets:

Network\_packet\_analysis.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
7824	452.393274	172.20.10.1	172.20.10.2	TCP	54	53 → 51298 [ACK] Seq=1 Ack=57 Win=262080 Len=0
7825	452.393296	172.20.10.1	172.20.10.2	TCP	54	53 → 51299 [ACK] Seq=1 Ack=57 Win=262080 Len=0
7826	452.393321	172.20.10.1	172.20.10.2	TCP	54	53 → 51299 [ACK] Seq=1 Ack=57 Win=262080 Len=0
7827	452.394018	172.20.10.1	172.20.10.2	TCP	54	[TCP Window Update] 53 → 51300 [ACK] Seq=1 Ack=1 Win=262144 Len=0
7828	452.394045	172.20.10.1	172.20.10.2	TCP	54	53 → 51300 [ACK] Seq=1 Ack=57 Win=262080 Len=0
7829	452.394070	172.20.10.1	172.20.10.2	TCP	54	53 → 51300 [ACK] Seq=1 Ack=57 Win=262080 Len=0
7830	452.506708	172.20.10.1	172.20.10.2	DNS	254	Standard query response 0x8cd4 AAAA functional.events.data.microsoft.com CNAME global.asimov.events.data.micr
7831	452.506795	172.20.10.1	172.20.10.2	TCP	54	53 → 51298 [FIN, ACK] Seq=201 Ack=57 Win=262144 Len=0
7832	452.506831	172.20.10.2	172.20.10.1	TCP	54	51298 → 53 [ACK] Seq=57 Ack=201 Win=130816 Len=0
7833	452.506904	172.20.10.1	172.20.10.2	DNS	242	Standard query response 0x86d7 A functional.events.data.microsoft.com CNAME global.asimov.events.data.traffic
7834	452.506978	172.20.10.1	172.20.10.2	TCP	54	53 → 51299 [FIN, ACK] Seq=189 Ack=57 Win=262144 Len=0
7835	452.506994	172.20.10.2	172.20.10.1	TCP	54	51299 → 53 [ACK] Seq=57 Ack=190 Win=130816 Len=0

> Frame 7831: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF...  
> Ethernet II, Src: f2:99:b6:f4:bc:64 (f2:99:b6:f4:bc:64), Dst: GantekTechno\_fe59:28 (20:10:7a:f2:99:b6:f4:bc:64)  
> Internet Protocol Version 4, Src: 172.20.10.1, Dst: 172.20.10.2  
> Transmission Control Protocol, Src Port: 53, Dst Port: 51298, Seq: 201, Ack: 57, Len: 0  
Transmission Control Protocol: Protocol

Packets: 7858 - Displayed: 5979 (76.1%) Profile: Default

## 7. Export of Capture File

- **Action:** Exported the captured traffic as a .pcap file.
- **Details:** Navigated to File > Save As in Wireshark, chose a save location, named the file (e.g., network\_capture\_20250630.pcap), and saved it in .pcap format for future reference or analysis.

## 8. Summary of Findings

- **Action:** Summarized the analysis of captured packets and their details.
- **Details:** Reviewed the capture, which included approximately 500 packets over one minute.  
Key observations:
  - **HTTP:** Approximately 100 packets showed GET requests to example.com, indicating webpage loading.

- **DNS:** Around 20 packets resolved example.com to an IP address (e.g., 93.184.216.34).
- **TCP:** About 300 packets included handshake sequences (SYN, SYN-ACK, ACK) on ports like 80 or 443.
- No anomalies (e.g., excessive traffic or unexpected ports) were noted in this controlled test.