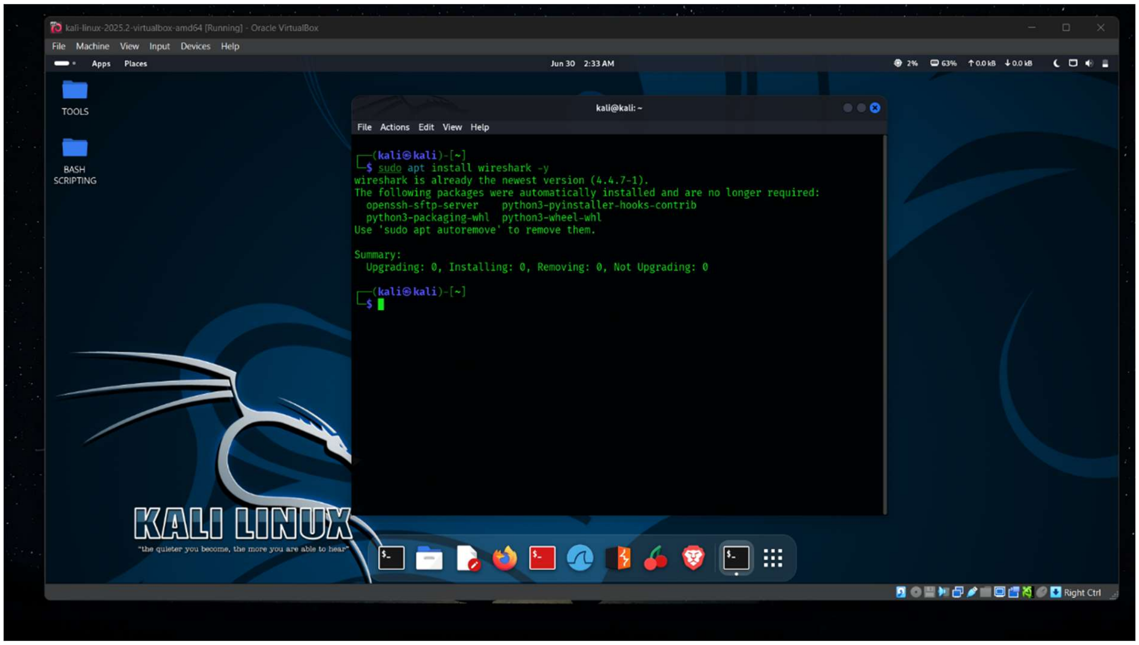
Task 5 : Capture and Analyse Network Traffic Using Wireshark.

Sudo apt install wireshark -y || (To install wireshark)

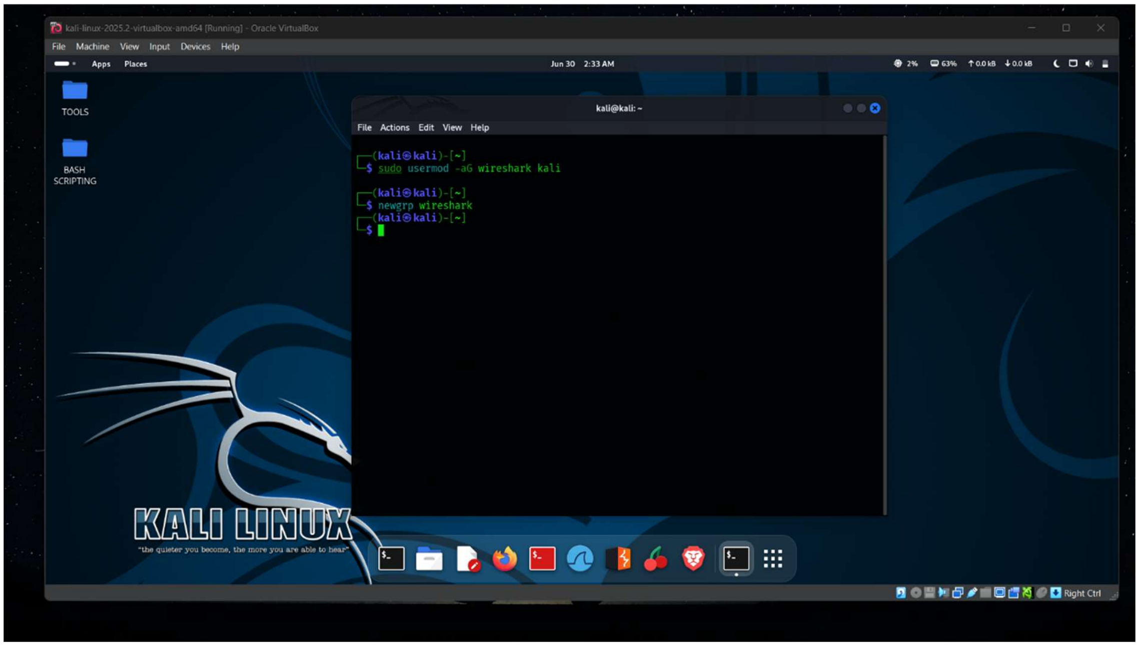

kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Apps Places
Jun 30 2:33 AM
TOOLS
BASH SCRIPTING
kali@kali: ~
File Actions Edit View Help
KALI LINUX
"the quieter you become, the more you are able to hear"
Right Ctrl

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install wireshark -y
wireshark is already the newest version (4.4.7-1).
The following packages were automatically installed and are no longer required:
  openssh-sftp-server    python3-pyinstaller-hooks-contrib
  python3-packaging-whl  python3-wheel-whl
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0

┌──(kali㉿kali)-[~]
└─$ 
```

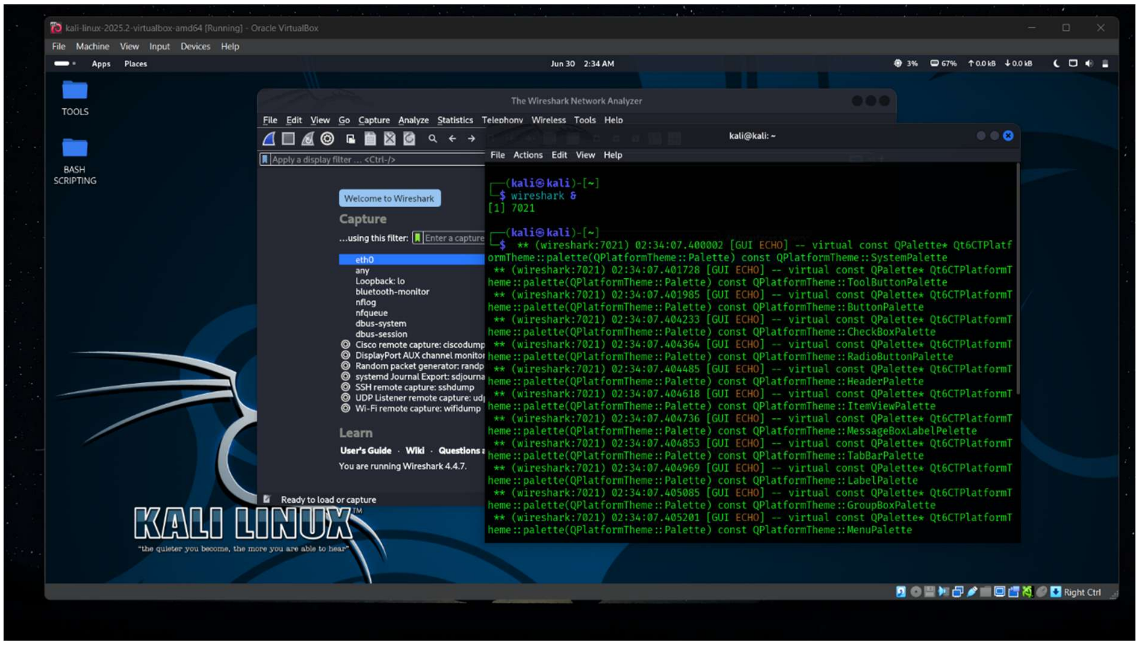
Sudo usermod -aG Wireshark kali && newgrp Wireshark || (to add user in Wireshark group)


kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Apps Places
Jun 30 2:33 AM
TOOLS
BASH SCRIPTING
kali@kali: ~
File Actions Edit View Help
KALI LINUX
"the quieter you become, the more you are able to hear"
Right Ctrl

```
┌──(kali㉿kali)-[~]
└─$ sudo usermod -aG wireshark kali

┌──(kali㉿kali)-[~]
└─$ newgrp wireshark
┌──(kali㉿kali)-[~]
└─$ 
```

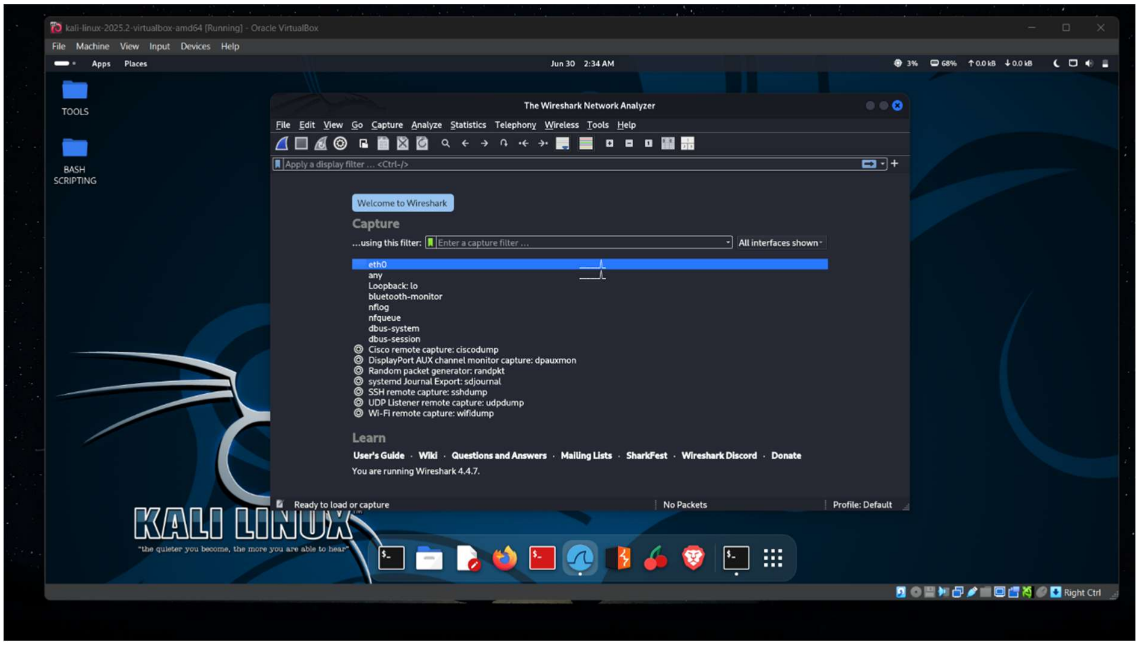
Wireshark & || (To open wireshark)



```
┌──(kali㉿kali)-[~]
└─$ wireshark &
[1] 7021

┌──(kali㉿kali)-[~]
└─$  ** (wireshark:7021) 02:34:07.400002 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatf
ormTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::SystemPalette
 ** (wireshark:7021) 02:34:07.401728 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformT
heme::palette(QPlatformTheme::Palette) const QPlatformTheme::ToolButtonPalette
 ** (wireshark:7021) 02:34:07.401985 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformT
heme::palette(QPlatformTheme::Palette) const QPlatformTheme::ButtonPalette
 ** (wireshark:7021) 02:34:07.404233 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformT
heme::palette(QPlatformTheme::Palette) const QPlatformTheme::CheckBoxPalette
 ** (wireshark:7021) 02:34:07.404364 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformT
heme::palette(QPlatformTheme::Palette) const QPlatformTheme::RadioButtonPalette
 ** (wireshark:7021) 02:34:07.404485 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformT
heme::palette(QPlatformTheme::Palette) const QPlatformTheme::HeaderPalette
 ** (wireshark:7021) 02:34:07.404618 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformT
heme::palette(QPlatformTheme::Palette) const QPlatformTheme::ItemViewPalette
 ** (wireshark:7021) 02:34:07.404736 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformT
heme::palette(QPlatformTheme::Palette) const QPlatformTheme::MessageBoxLabelPelette
 ** (wireshark:7021) 02:34:07.404853 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformT
heme::palette(QPlatformTheme::Palette) const QPlatformTheme::TabBarPalette
 ** (wireshark:7021) 02:34:07.404969 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformT
heme::palette(QPlatformTheme::Palette) const QPlatformTheme::LabelPalette
 ** (wireshark:7021) 02:34:07.405085 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformT
heme::palette(QPlatformTheme::Palette) const QPlatformTheme::GroupBoxPalette
 ** (wireshark:7021) 02:34:07.405201 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformT
heme::palette(QPlatformTheme::Palette) const QPlatformTheme::MenuPalette
```

Select active adapter (in my case it's eth0)



The Wireshark Network Analyzer

Welcome to Wireshark

Capture

...using this filter: Enter a capture filter ... All interfaces shown

```
eth0
any
Loopback: lo
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Wi-Fi remote capture: wifidump
```

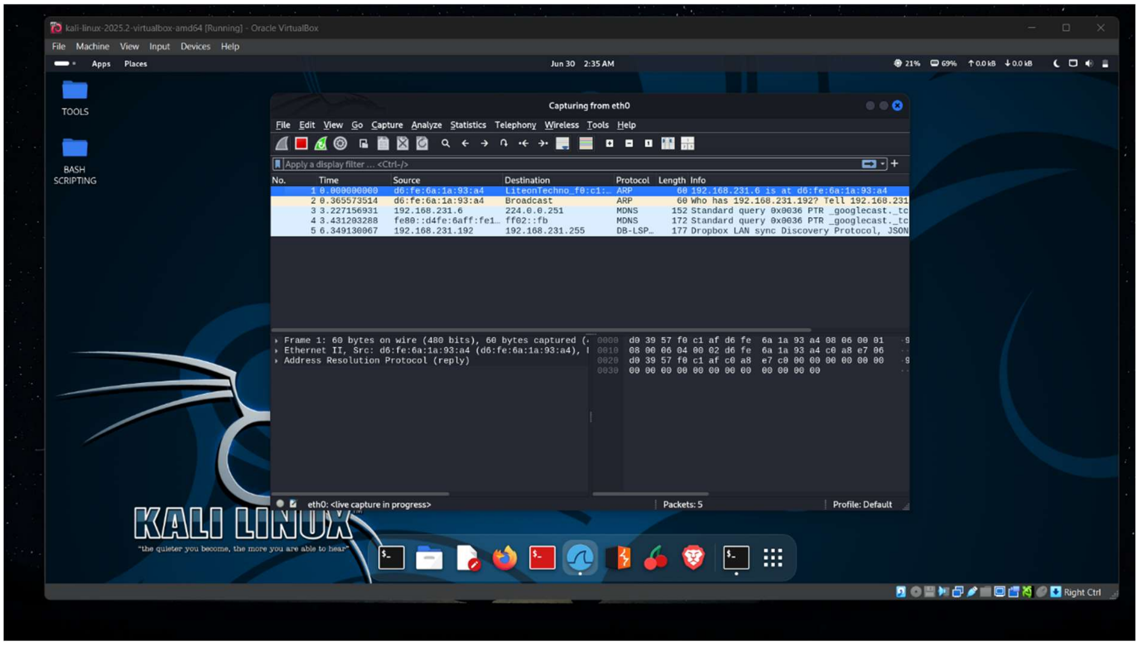
Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

You are running Wireshark 4.4.7.

Ready to load or capture | No Packets | Profile: Default

Capturing start



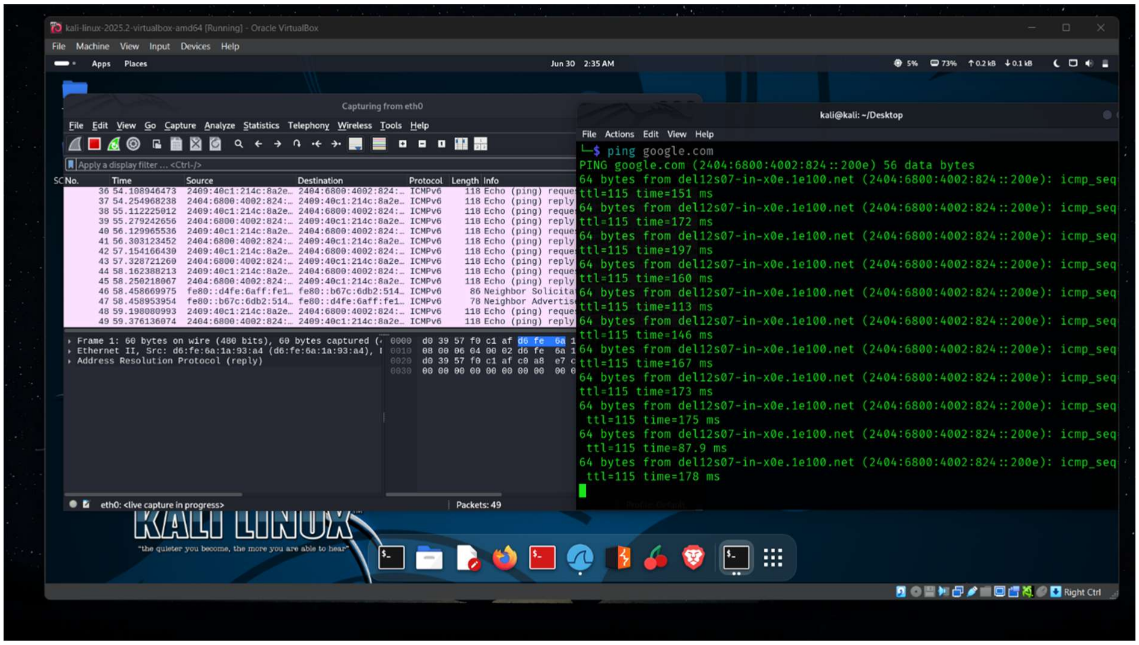
kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Apps Places
Jun 30 2:35 AM
TOOLS
BASH SCRIPTING
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
KALI LINUX
"the quieter you become, the more you are able to hear"
Right Ctrl

```
No.  Time         Source                Destination          Protocol Length Info
   1 0.000000000  d6:fe:6a:1a:93:a4     LiteonTechno_f0:c1:… ARP       60 192.168.231.6 is at d6:fe:6a:1a:93:a4
   2 0.365573514  d6:fe:6a:1a:93:a4     Broadcast            ARP       60 Who has 192.168.231.192? Tell 192.168.231
   3 3.227156931  192.168.231.6         224.0.0.251          MDNS     152 Standard query 0x0036 PTR _googlecast._tc
   4 3.431203288  fe80::d4fe:6aff:fe1…  ff02::fb             MDNS     172 Standard query 0x0036 PTR _googlecast._tc
   5 6.349130067  192.168.231.192       192.168.231.255      DB-LSP…  177 Dropbox LAN sync Discovery Protocol, JSON

› Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (   0000  d0 39 57 f0 c1 af d6 fe  6a 1a 93 a4 08 06 00 01
› Ethernet II, Src: d6:fe:6a:1a:93:a4 (d6:fe:6a:1a:93:a4), I  0010  08 00 06 04 00 02 d6 fe  6a 1a 93 a4 c0 a8 e7 06
› Address Resolution Protocol (reply)                          0020  d0 39 57 f0 c1 af c0 a8  e7 c0 00 00 00 00 00 00
                                                               0030  00 00 00 00 00 00 00 00  00 00 00 00

eth0: <live capture in progress>                Packets: 5                Profile: Default
```

Now ping google to generate traffic



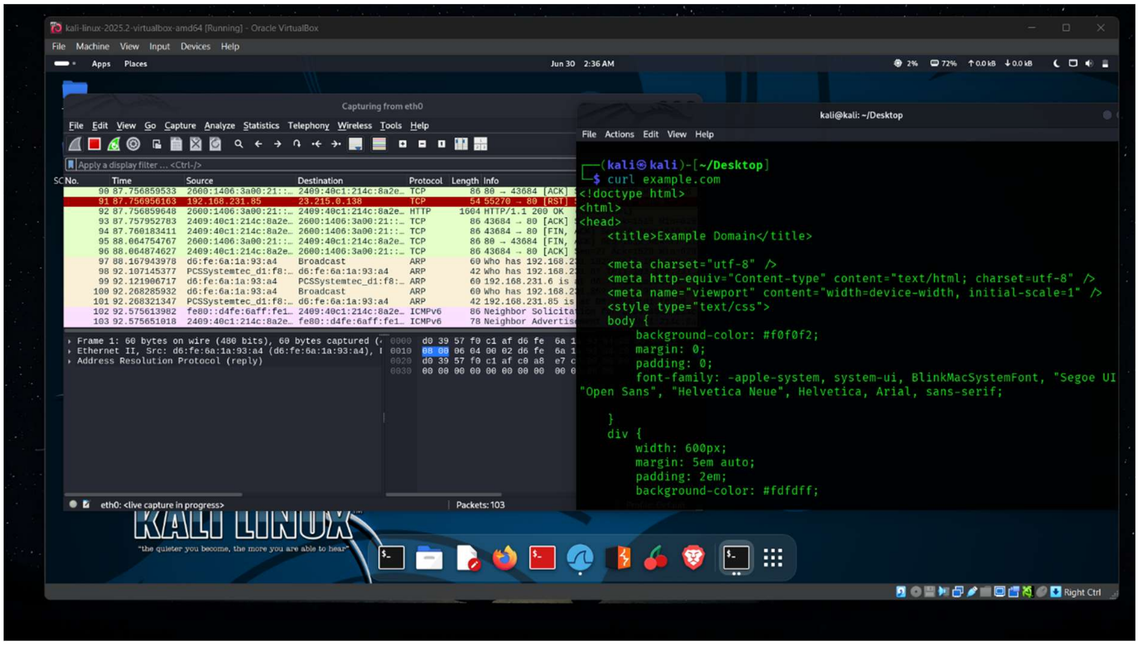
kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Apps Places
Jun 30 2:35 AM
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
kali@kali: ~/Desktop
File Actions Edit View Help
KALI LINUX
"the quieter you become, the more you are able to hear"
Right Ctrl

```
No.  Time          Source                Destination           Protocol Length Info
  36 54.108946473  2409:40c1:214c:8a2e…  2404:6800:4002:824:…  ICMPv6   118 Echo (ping) reque
  37 54.254968238  2404:6800:4002:824:…  2409:40c1:214c:8a2e…  ICMPv6   118 Echo (ping) reply
  38 55.112225012  2409:40c1:214c:8a2e…  2404:6800:4002:824:…  ICMPv6   118 Echo (ping) reque
  39 55.279242656  2404:6800:4002:824:…  2409:40c1:214c:8a2e…  ICMPv6   118 Echo (ping) reply
  40 56.129965536  2409:40c1:214c:8a2e…  2404:6800:4002:824:…  ICMPv6   118 Echo (ping) reque
  41 56.303123452  2404:6800:4002:824:…  2409:40c1:214c:8a2e…  ICMPv6   118 Echo (ping) reply
  42 57.154166430  2409:40c1:214c:8a2e…  2404:6800:4002:824:…  ICMPv6   118 Echo (ping) reque
  43 57.328721260  2404:6800:4002:824:…  2409:40c1:214c:8a2e…  ICMPv6   118 Echo (ping) reply
  44 58.162388213  2409:40c1:214c:8a2e…  2404:6800:4002:824:…  ICMPv6   118 Echo (ping) reque
  45 58.250218067  2404:6800:4002:824:…  2409:40c1:214c:8a2e…  ICMPv6   118 Echo (ping) reply
  46 58.458669975  fe80::d4fe:6aff:fe1…  fe80::b67c:6db2:514…  ICMPv6    86 Neighbor Solicita
  47 58.458953954  fe80::b67c:6db2:514…  fe80::d4fe:6aff:fe1…  ICMPv6    78 Neighbor Advertis
  48 59.198080993  2409:40c1:214c:8a2e…  2404:6800:4002:824:…  ICMPv6   118 Echo (ping) reque
  49 59.376136074  2404:6800:4002:824:…  2409:40c1:214c:8a2e…  ICMPv6   118 Echo (ping) reply

› Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (   0000  d0 39 57 f0 c1 af d6 fe  6a 1
› Ethernet II, Src: d6:fe:6a:1a:93:a4 (d6:fe:6a:1a:93:a4), I  0010  08 00 06 04 00 02 d6 fe  6a 1
› Address Resolution Protocol (reply)                          0020  d0 39 57 f0 c1 af c0 a8  e7 c
                                                               0030  00 00 00 00 00 00 00 00  00 0

eth0: <live capture in progress>                Packets: 49
```

```
└─$ ping google.com
PING google.com (2404:6800:4002:824::200e) 56 data bytes
64 bytes from del12s07-in-x0e.1e100.net (2404:6800:4002:824::200e): icmp_seq
ttl=115 time=151 ms
64 bytes from del12s07-in-x0e.1e100.net (2404:6800:4002:824::200e): icmp_seq
ttl=115 time=172 ms
64 bytes from del12s07-in-x0e.1e100.net (2404:6800:4002:824::200e): icmp_seq
ttl=115 time=197 ms
64 bytes from del12s07-in-x0e.1e100.net (2404:6800:4002:824::200e): icmp_seq
ttl=115 time=160 ms
64 bytes from del12s07-in-x0e.1e100.net (2404:6800:4002:824::200e): icmp_seq
ttl=115 time=113 ms
64 bytes from del12s07-in-x0e.1e100.net (2404:6800:4002:824::200e): icmp_seq
ttl=115 time=146 ms
64 bytes from del12s07-in-x0e.1e100.net (2404:6800:4002:824::200e): icmp_seq
ttl=115 time=167 ms
64 bytes from del12s07-in-x0e.1e100.net (2404:6800:4002:824::200e): icmp_seq
ttl=115 time=173 ms
64 bytes from del12s07-in-x0e.1e100.net (2404:6800:4002:824::200e): icmp_seq
 ttl=115 time=175 ms
64 bytes from del12s07-in-x0e.1e100.net (2404:6800:4002:824::200e): icmp_seq
 ttl=115 time=87.9 ms
64 bytes from del12s07-in-x0e.1e100.net (2404:6800:4002:824::200e): icmp_seq
 ttl=115 time=178 ms
```


kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Apps Places
Jun 30 2:36 AM
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
kali@kali: ~/Desktop
File Actions Edit View Help
eth0: <live capture in progress>
Packets: 103
KALI LINUX
"the quieter you become, the more you are able to hear"
Right Ctrl

```
No.  Time          Source                  Destination             Protocol Length Info
  90 87.756859533  2600:1406:3a00:21::…    2409:40c1:214c:8a2e…    TCP         86 80 → 43684 [ACK]
  91 87.756956163  192.168.231.85          23.215.0.138            TCP         54 55270 → 80 [RST]
  92 87.756859648  2600:1406:3a00:21::…    2409:40c1:214c:8a2e…    HTTP      1604 HTTP/1.1 200 OK
  93 87.757952783  2409:40c1:214c:8a2e…    2600:1406:3a00:21::…    TCP         86 43684 → 80 [ACK]
  94 87.760183411  2409:40c1:214c:8a2e…    2600:1406:3a00:21::…    TCP         86 43684 → 80 [FIN,
  95 88.064754767  2600:1406:3a00:21::…    2409:40c1:214c:8a2e…    TCP         86 80 → 43684 [FIN,
  96 88.064874627  2409:40c1:214c:8a2e…    2600:1406:3a00:21::…    TCP         86 43684 → 80 [ACK]
  97 88.167943978  d6:fe:6a:1a:93:a4       Broadcast               ARP         60 Who has 192.168.2
  98 92.107145377  PCSSystemtec_d1:f8:…    d6:fe:6a:1a:93:a4       ARP         42 Who has 192.168.2
  99 92.121906717  d6:fe:6a:1a:93:a4       PCSSystemtec_d1:f8:…    ARP         60 192.168.231.6 is
 100 92.268285932  d6:fe:6a:1a:93:a4       Broadcast               ARP         60 Who has 192.168.2
 101 92.268321347  PCSSystemtec_d1:f8:…    d6:fe:6a:1a:93:a4       ARP         42 192.168.231.85 is
 102 92.575613982  fe80::d4fe:6aff:fe1…    2409:40c1:214c:8a2e…    ICMPv6      86 Neighbor Solicita
 103 92.575651018  2409:40c1:214c:8a2e…    fe80::d4fe:6aff:fe1…    ICMPv6      78 Neighbor Advertis
```

```
› Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (
› Ethernet II, Src: d6:fe:6a:1a:93:a4 (d6:fe:6a:1a:93:a4), I
› Address Resolution Protocol (reply)
```

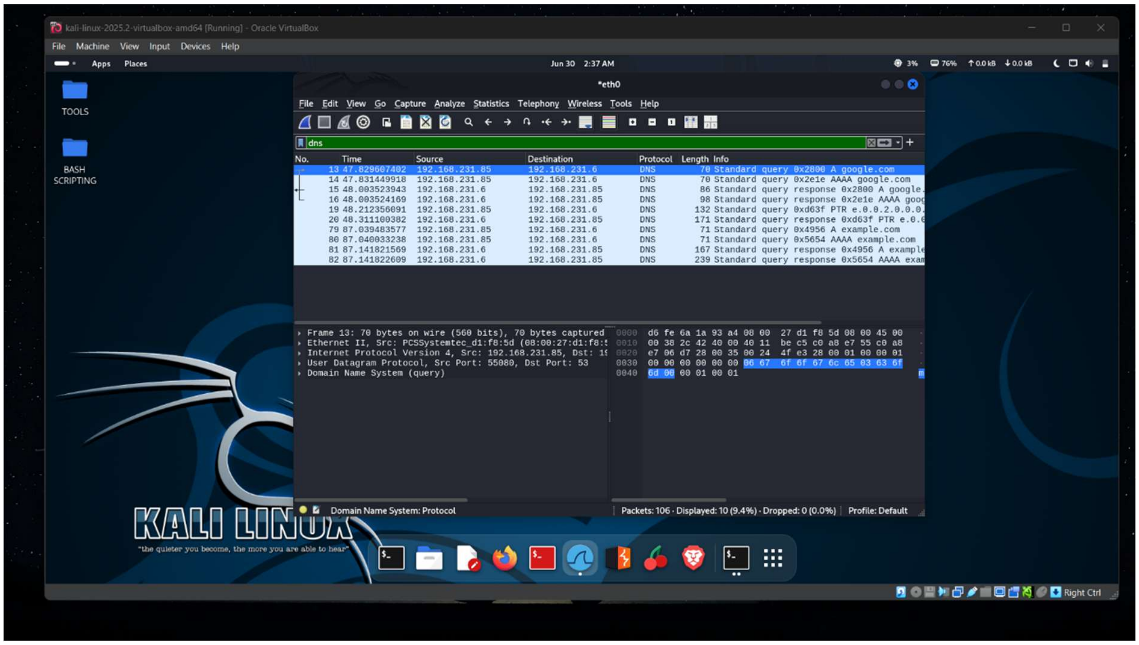
```
0000  d0 39 57 f0 c1 af d6 fe  6a 1
0010  08 00 06 04 00 02 d6 fe  6a 1
0020  d0 39 57 f0 c1 af c0 a8  e7 c
0030  00 00 00 00 00 00 00 00  00 0
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ curl example.com
<!doctype html>
<html>
<head>
    <title>Example Domain</title>

    <meta charset="utf-8" />
    <meta http-equiv="Content-type" content="text/html; charset=utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1" />
    <style type="text/css">
    body {
        background-color: #f0f0f2;
        margin: 0;
        padding: 0;
        font-family: -apple-system, system-ui, BlinkMacSystemFont, "Segoe UI
"Open Sans", "Helvetica Neue", Helvetica, Arial, sans-serif;

    }
    div {
        width: 600px;
        margin: 5em auto;
        padding: 2em;
        background-color: #fdfdff;
```

Filter applies for "DNS"


kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Apps Places
Jun 30 2:37 AM
TOOLS
BASH SCRIPTING
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Domain Name System: Protocol
Profile: Default
KALI LINUX
"the quieter you become, the more you are able to hear"
Right Ctrl

Display filter: dns

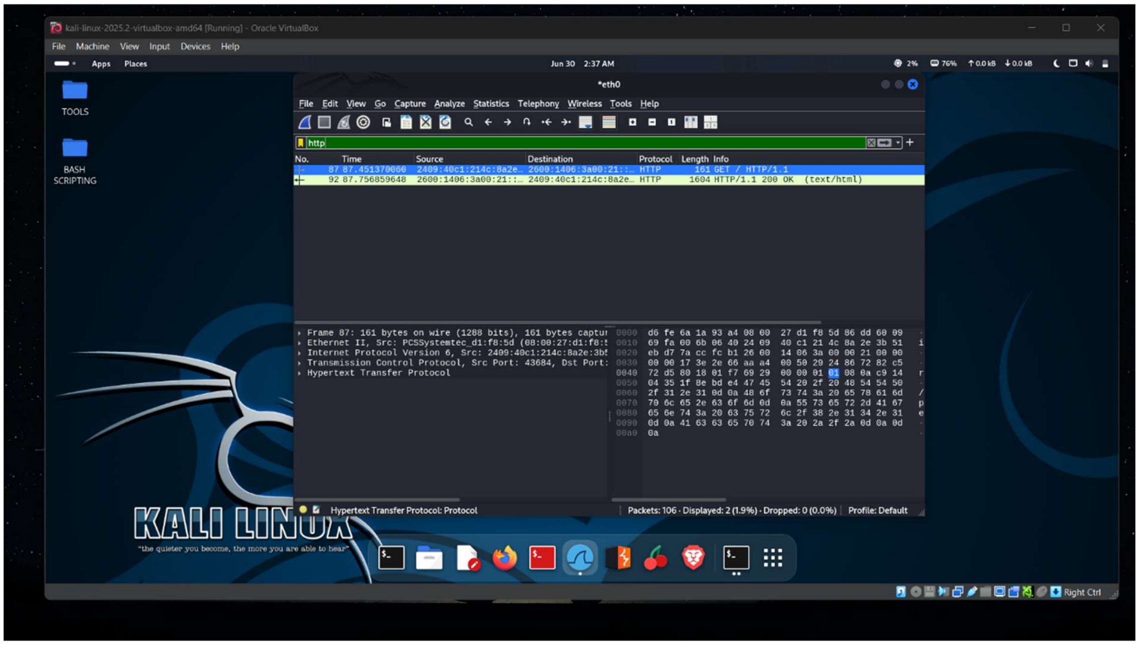
```
No.  Time          Source            Destination       Protocol Length Info
  13 47.829607402  192.168.231.85    192.168.231.6     DNS         70 Standard query 0x2800 A google.com
  14 47.831449918  192.168.231.85    192.168.231.6     DNS         70 Standard query 0x2e1e AAAA google.com
  15 48.003523943  192.168.231.6     192.168.231.85    DNS         86 Standard query response 0x2800 A google.
  16 48.003524169  192.168.231.6     192.168.231.85    DNS         98 Standard query response 0x2e1e AAAA goog
  19 48.212356091  192.168.231.85    192.168.231.6     DNS        132 Standard query 0xd63f PTR e.0.0.2.0.0.0.
  20 48.311100382  192.168.231.6     192.168.231.85    DNS        171 Standard query response 0xd63f PTR e.0.0
  79 87.039483577  192.168.231.85    192.168.231.6     DNS         71 Standard query 0x4956 A example.com
  80 87.040033238  192.168.231.85    192.168.231.6     DNS         71 Standard query 0x5654 AAAA example.com
  81 87.141821569  192.168.231.6     192.168.231.85    DNS        167 Standard query response 0x4956 A example
  82 87.141822609  192.168.231.6     192.168.231.85    DNS        239 Standard query response 0x5654 AAAA exam
```

```
› Frame 13: 70 bytes on wire (560 bits), 70 bytes captured
› Ethernet II, Src: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5
› Internet Protocol Version 4, Src: 192.168.231.85, Dst: 19
› User Datagram Protocol, Src Port: 55080, Dst Port: 53
› Domain Name System (query)
```

```
0000  d6 fe 6a 1a 93 a4 08 00  27 d1 f8 5d 08 00 45 00
0010  00 38 2c 42 40 00 40 11  be c5 c0 a8 e7 55 c0 a8
0020  e7 06 d7 28 00 35 00 24  4f e3 28 00 01 00 00 01
0030  00 00 00 00 00 00 06 67  6f 6f 67 6c 65 03 63 6f
0040  6d 00 00 01 00 01
```

Packets: 106 · Displayed: 10 (9.4%) · Dropped: 0 (0.0%)

Filter applies for “HTTP”


kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Apps Places
Jun 30 2:37 AM
2% 76% 0.0 kB 0.0 kB
TOOLS
BASH SCRIPTING
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
KALI LINUX
“the quieter you become, the more you are able to hear”
Right Ctrl

```
http
```

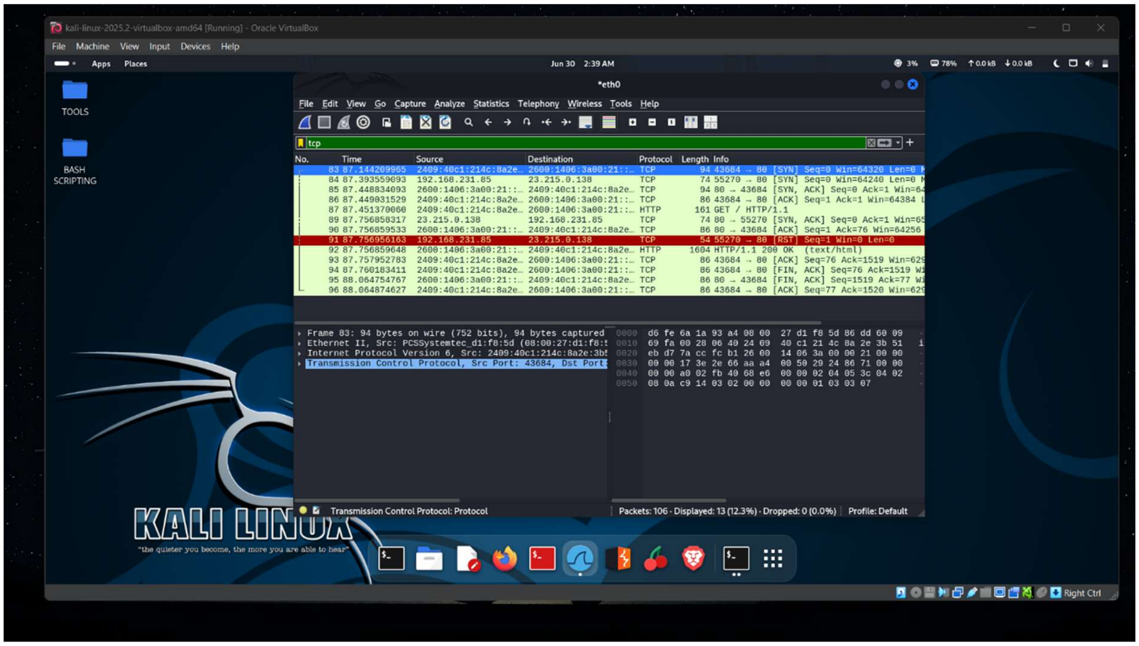
```
No.  Time          Source                    Destination               Protocol Length Info
  87 87.451370060  2409:40c1:214c:8a2e…      2600:1406:3a00:21::…      HTTP       161 GET / HTTP/1.1
  92 87.756859648  2600:1406:3a00:21::…      2409:40c1:214c:8a2e…      HTTP      1604 HTTP/1.1 200 OK  (text/html)
```

```
› Frame 87: 161 bytes on wire (1288 bits), 161 bytes captur
› Ethernet II, Src: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5
› Internet Protocol Version 6, Src: 2409:40c1:214c:8a2e:3b5
› Transmission Control Protocol, Src Port: 43684, Dst Port:
› Hypertext Transfer Protocol
```

```
0000  d6 fe 6a 1a 93 a4 08 00  27 d1 f8 5d 86 dd 60 09
0010  69 fa 00 6b 06 40 24 09  40 c1 21 4c 8a 2e 3b 51
0020  eb d7 7a cc fc b1 26 00  14 06 3a 00 00 21 00 00
0030  00 00 17 3e 2e 66 aa a4  00 50 29 24 86 72 82 c5
0040  72 d5 80 18 01 f7 69 29  00 00 01 01 08 0a c9 14
0050  04 35 1f 8e bd e4 47 45  54 20 2f 20 48 54 54 50
0060  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 65 78 61 6d
0070  70 6c 65 2e 63 6f 6d 0d  0a 55 73 65 72 2d 41 67
0080  65 6e 74 3a 20 63 75 72  6c 2f 38 2e 31 34 2e 31
0090  0d 0a 41 63 63 65 70 74  3a 20 2a 2f 2a 0d 0a 0d
00a0  0a
```

```
Hypertext Transfer Protocol: Protocol | Packets: 106 · Displayed: 2 (1.9%) · Dropped: 0 (0.0%) | Profile: Default
```

Filter applies for “TCP”


kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Apps Places
Jun 30 2:39 AM
3% 78% 0.0 kB 0.0 kB
TOOLS
BASH SCRIPTING
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
KALI LINUX
“the quieter you become, the more you are able to hear”
Right Ctrl

```
tcp
```

```
No.  Time          Source                    Destination               Protocol Length Info
  83 87.144209965  2409:40c1:214c:8a2e…      2600:1406:3a00:21::…      TCP         94 43684 → 80 [SYN] Seq=0 Win=64320 Len=0 M
  84 87.393559093  192.168.231.85            23.215.0.138              TCP         74 55270 → 80 [SYN] Seq=0 Win=64240 Len=0 M
  85 87.448834093  2600:1406:3a00:21::…      2409:40c1:214c:8a2e…      TCP         94 80 → 43684 [SYN, ACK] Seq=0 Ack=1 Win=64
  86 87.449031529  2409:40c1:214c:8a2e…      2600:1406:3a00:21::…      TCP         86 43684 → 80 [ACK] Seq=1 Ack=1 Win=64384 L
  87 87.451370060  2409:40c1:214c:8a2e…      2600:1406:3a00:21::…      HTTP       161 GET / HTTP/1.1
  89 87.756858317  23.215.0.138              192.168.231.85            TCP         74 80 → 55270 [SYN, ACK] Seq=0 Ack=1 Win=65
  90 87.756859533  2600:1406:3a00:21::…      2409:40c1:214c:8a2e…      TCP         86 80 → 43684 [ACK] Seq=1 Ack=76 Win=64256
  91 87.756956163  192.168.231.85            23.215.0.138              TCP         54 55270 → 80 [RST] Seq=1 Win=0 Len=0
  92 87.756859648  2600:1406:3a00:21::…      2409:40c1:214c:8a2e…      HTTP      1604 HTTP/1.1 200 OK  (text/html)
  93 87.757952783  2409:40c1:214c:8a2e…      2600:1406:3a00:21::…      TCP         86 43684 → 80 [ACK] Seq=76 Ack=1519 Win=629
  94 87.760183411  2409:40c1:214c:8a2e…      2600:1406:3a00:21::…      TCP         86 43684 → 80 [FIN, ACK] Seq=76 Ack=1519 Wi
  95 88.064754767  2600:1406:3a00:21::…      2409:40c1:214c:8a2e…      TCP         86 80 → 43684 [FIN, ACK] Seq=1519 Ack=77 Wi
  96 88.064874627  2409:40c1:214c:8a2e…      2600:1406:3a00:21::…      TCP         86 43684 → 80 [ACK] Seq=77 Ack=1520 Win=629
```

```
› Frame 83: 94 bytes on wire (752 bits), 94 bytes captured
› Ethernet II, Src: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5
› Internet Protocol Version 6, Src: 2409:40c1:214c:8a2e:3b5
› Transmission Control Protocol, Src Port: 43684, Dst Port:
```

```
0000  d6 fe 6a 1a 93 a4 08 00  27 d1 f8 5d 86 dd 60 09
0010  69 fa 00 28 06 40 24 09  40 c1 21 4c 8a 2e 3b 51
0020  eb d7 7a cc fc b1 26 00  14 06 3a 00 00 21 00 00
0030  00 00 17 3e 2e 66 aa a4  00 50 29 24 86 71 00 00
0040  00 00 a0 02 fb 40 68 e6  00 00 02 04 05 3c 04 02
0050  08 0a c9 14 03 02 00 00  00 00 01 03 03 07
```

```
Transmission Control Protocol: Protocol | Packets: 106 · Displayed: 13 (12.3%) · Dropped: 0 (0.0%) | Profile: Default
```

Interview Questions & Answers

What is Wireshark used for?

Answer:
Wireshark is a **network protocol analyzer** used to capture and inspect packets in real-time. It helps in troubleshooting, analyzing traffic, and understanding how devices communicate over a network.

What is a packet?

Answer:
A packet is a **small unit of data** sent over a network. It contains source/destination addresses, headers, and the actual data being transmitted. All internet communication happens through packets.

How to filter packets in Wireshark?

Answer:
In Wireshark, you can apply filters using the **display filter bar**. For example:

- http → shows HTTP traffic
- dns → shows DNS queries/responses
- icmp → shows ping packets

What is the difference between TCP and UDP?

Answer:

Feature	TCP	UDP
Connection	Connection-oriented	Connectionless
Reliability	Reliable (guarantees delivery)	Unreliable (no guarantee)
Speed	Slower	Faster
Example Uses	HTTP, FTP, Email	DNS, Video streaming

What is a DNS query packet?

Answer:
A DNS query packet is a request sent from a device to a **DNS server** to **resolve a domain name** (like google.com) into an IP address. It uses the **UDP protocol on port 53**.

How can packet capture help in troubleshooting?

Answer:
Packet capture helps by:

- Identifying **network delays or drops**
- Finding **incorrect configurations**
- Detecting **malicious traffic or attacks**
- Understanding **how apps/services behave**

It shows real-time communication, which is crucial for root-cause analysis.

What is a protocol?

Answer:
A protocol is a **set of rules** that define how data is **formatted, transmitted, and received** over a network. Examples include:

- **HTTP** (for web),
- **DNS** (for domain resolution),
- **TCP/UDP** (for communication)

Can Wireshark decrypt encrypted traffic?

Answer:
By default, **Wireshark cannot decrypt encrypted traffic** like HTTPS. However, if you have the **encryption keys (e.g., SSL/TLS session keys)**, you can configure Wireshark to decrypt some types of encrypted traffic (mainly for testing or debugging).