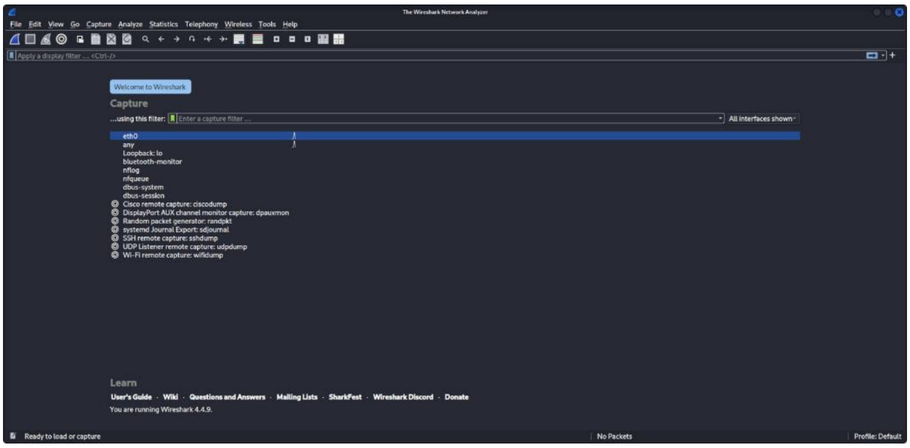
Task 5 : Capture and Analyze Network Traffic Using Wireshark

1. **Install Wireshark**
   - In linux wireshark will be pre-installed so just type command "wireshark" and press enter.
   - You will see the following interface:


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
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

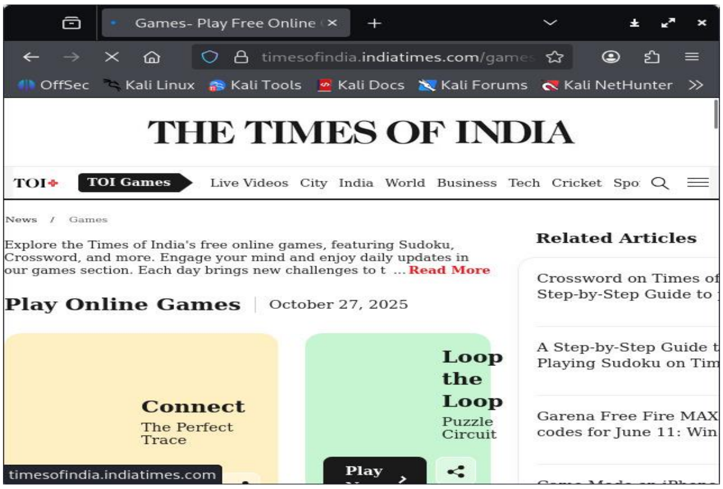
You are running Wireshark 4.4.9.

Ready to load or capture

No Packets

Profile: Default

2. **Start capturing on your active network interface:**
3. **Browse a website or ping a server to generate traffic:**
4. **Stop capture after a minute:**
   - Click on eth0 to start capturing the packets.
   - Open the browser and search any website.
   - Wireshark will capture that too.
   - Then after one minute stop the packet capturing.
   - At the top there will be an filtering search box type any 3 protocols that you wish and if those protocol packets were involved, then it will display all the packets for that particular protocol.



THE TIMES OF INDIA

News / Games

Explore the Times of India's free online games, featuring Sudoku, Crossword, and more. Engage your mind and enjoy daily updates in our games section. Each day brings new challenges to t ...Read More

Play Online Games | October 27, 2025

Related Articles

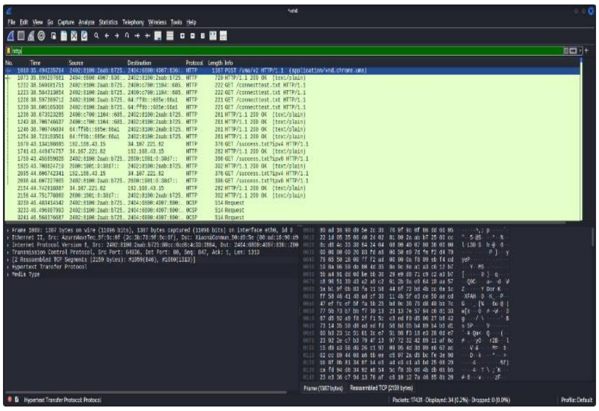
Crossword on Times of Step-by-Step Guide to

A Step-by-Step Guide t Playing Sudoku on Tim

Garena Free Fire MAX codes for June 11: Win

5. Filter captured packets by protocol (e.g., HTTP, DNS, TCP):

- I have searched "Times New India" and captured the packets.
- I had filtered HTTP, TCP and DNS protocol packets.

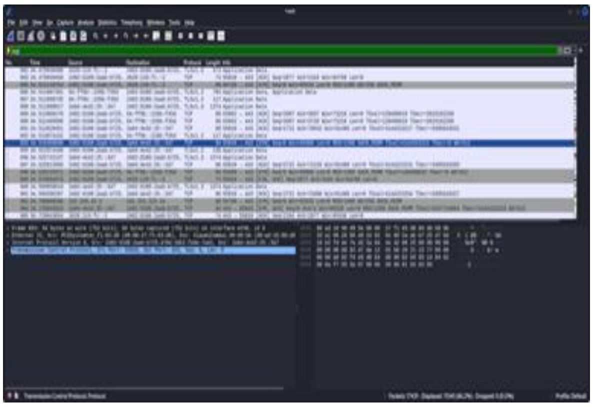


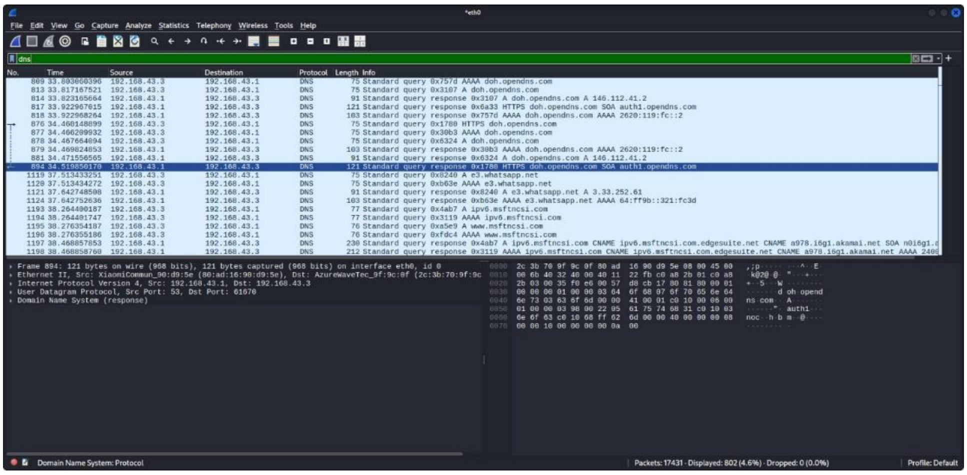
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.  Time          Source               Destination          Protocol Length Info
1080 35.494235764  2402:8100:2aab:b725… 2404:6800:4007:836:… HTTP     1387 POST /sma/v2 HTTP/1.1  (application/vnd.chrome.ums)
1073 35.899257681  2404:6800:4007:836:… 2402:8100:2aab:b725… HTTP      720 HTTP/1.1 200 OK  (text/plain)
1222 38.569081751  2402:8100:2aab:b725… 2400:c700:1104::685… HTTP      222 GET /connecttest.txt HTTP/1.1
1223 38.584313854  2402:8100:2aab:b725… 2400:c700:1104::685… HTTP      222 GET /connecttest.txt HTTP/1.1
1226 38.597269712  2402:8100:2aab:b725… 64:ff9b::685e:66a1   HTTP      221 GET /connecttest.txt HTTP/1.1
1230 38.605165308  2402:8100:2aab:b725… 64:ff9b::685e:66a1   HTTP      221 GET /connecttest.txt HTTP/1.1
1236 38.673023285  2400:c700:1104::685… 2402:8100:2aab:b725… HTTP      261 HTTP/1.1 200 OK  (text/plain)
1243 38.708746637  2400:c700:1104::685… 2402:8100:2aab:b725… HTTP      261 HTTP/1.1 200 OK  (text/plain)
1246 38.708746834  64:ff9b::685e:66a1   2402:8100:2aab:b725… HTTP      261 HTTP/1.1 200 OK  (text/plain)
1254 38.723193501  64:ff9b::685e:66a1   2402:8100:2aab:b725… HTTP      261 HTTP/1.1 200 OK  (text/plain)
1670 43.134190095  192.168.43.15        34.107.221.82        HTTP      376 GET /success.txt?ipv4 HTTP/1.1
1741 43.449474757  34.107.221.82        192.168.43.15        HTTP      282 HTTP/1.1 200 OK  (text/plain)
1750 43.455559028  2402:8100:2aab:b725… 2600:1901:0:38d7::   HTTP      396 GET /success.txt?ipv6 HTTP/1.1
1825 43.708824710  2600:1901:0:38d7::   2402:8100:2aab:b725… HTTP      302 HTTP/1.1 200 OK  (text/plain)
2085 44.606742341  192.168.43.15        34.107.221.82        HTTP      376 GET /success.txt?ipv4 HTTP/1.1
2086 44.607227005  2402:8100:2aab:b725… 2600:1901:0:38d7::   HTTP      396 GET /success.txt?ipv6 HTTP/1.1
2154 44.742918087  34.107.221.82        192.168.43.15        HTTP      282 HTTP/1.1 200 OK  (text/plain)
2156 44.751778088  2600:1901:0:38d7::   2402:8100:2aab:b725… HTTP      302 HTTP/1.1 200 OK  (text/plain)
3230 46.483414542  2402:8100:2aab:b725… 2404:6800:4007:800:… OCSP      514 Request
3233 46.496867903  2402:8100:2aab:b725… 2404:6800:4007:800:… OCSP      514 Request
3241 46.568376687  2402:8100:2aab:b725… 2404:6800:4007:800:… OCSP      514 Request

› Frame 1080: 1387 bytes on wire (11096 bits), 1387 bytes captured (11096 bits) on interface eth0, id 0
› Ethernet II, Src: AzureWaveTec_9f:9c:0f (2c:3b:70:9f:9c:0f), Dst: XiaomiCommun_90:d9:5e (80:ad:16:90:d9
› Internet Protocol Version 6, Src: 2402:8100:2aab:b725:80cc:6cd6:4c33:3884, Dst: 2404:6800:4007:836::200
› Transmission Control Protocol, Src Port: 64936, Dst Port: 80, Seq: 847, Ack: 1, Len: 1313
› [2 Reassembled TCP Segments (2159 bytes): #1069(846), #1080(1313)]
› Hypertext Transfer Protocol
› Media Type
```

Frame (1387 bytes)
Reassembled TCP (2159 bytes)
Hypertext Transfer Protocol: Protocol
Packets: 17431 · Displayed: 34 (0.2%) · Dropped: 0 (0.0%)
Profile: Default





*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

```
No.  Time          Source         Destination    Protocol Length Info
 809 33.803060396  192.168.43.3   192.168.43.1   DNS        75 Standard query 0x757d AAAA doh.opendns.com
 813 33.817167521  192.168.43.3   192.168.43.1   DNS        75 Standard query 0x3107 A doh.opendns.com
 814 33.823165664  192.168.43.1   192.168.43.3   DNS        91 Standard query response 0x3107 A doh.opendns.com A 146.112.41.2
 817 33.922967015  192.168.43.1   192.168.43.3   DNS       121 Standard query response 0x6a33 HTTPS doh.opendns.com SOA auth1.opendns.com
 818 33.922968264  192.168.43.1   192.168.43.3   DNS       103 Standard query response 0x757d AAAA doh.opendns.com AAAA 2620:119:fc::2
 876 34.460148899  192.168.43.3   192.168.43.1   DNS        75 Standard query 0x1780 HTTPS doh.opendns.com
 877 34.466209932  192.168.43.3   192.168.43.1   DNS        75 Standard query 0x30b3 AAAA doh.opendns.com
 878 34.467664094  192.168.43.3   192.168.43.1   DNS        75 Standard query 0x6324 A doh.opendns.com
 879 34.469824853  192.168.43.1   192.168.43.3   DNS       103 Standard query response 0x30b3 AAAA doh.opendns.com AAAA 2620:119:fc::2
 881 34.471556565  192.168.43.1   192.168.43.3   DNS        91 Standard query response 0x6324 A doh.opendns.com A 146.112.41.2
 894 34.519850170  192.168.43.1   192.168.43.3   DNS       121 Standard query response 0x1780 HTTPS doh.opendns.com SOA auth1.opendns.com
1119 37.513433251  192.168.43.3   192.168.43.1   DNS        75 Standard query 0x8240 A e3.whatsapp.net
1120 37.513434272  192.168.43.3   192.168.43.1   DNS        75 Standard query 0xb63e AAAA e3.whatsapp.net
1121 37.642748508  192.168.43.1   192.168.43.3   DNS        91 Standard query response 0x8240 A e3.whatsapp.net A 3.33.252.61
1124 37.642752636  192.168.43.1   192.168.43.3   DNS       103 Standard query response 0xb63e AAAA e3.whatsapp.net AAAA 64:ff9b::321:fc3d
1193 38.264400187  192.168.43.3   192.168.43.1   DNS        77 Standard query 0x4ab7 A ipv6.msftncsi.com
1194 38.264401747  192.168.43.3   192.168.43.1   DNS        77 Standard query 0x3119 AAAA ipv6.msftncsi.com
1195 38.276354187  192.168.43.3   192.168.43.1   DNS        76 Standard query 0xa5e9 A www.msftncsi.com
1196 38.276355186  192.168.43.3   192.168.43.1   DNS        76 Standard query 0xfdc4 AAAA www.msftncsi.com
1197 38.468857853  192.168.43.1   192.168.43.3   DNS       230 Standard query response 0x4ab7 A ipv6.msftncsi.com CNAME ipv6.msftncsi.com.edgesuite.net CNAME a978.i6g1.akamai.net SOA n0i6g1.a
1198 38.468858760  192.168.43.1   192.168.43.3   DNS       212 Standard query response 0x3119 AAAA ipv6.msftncsi.com CNAME ipv6.msftncsi.com.edgesuite.net CNAME a978.i6g1.akamai.net AAAA 240

› Frame 894: 121 bytes on wire (968 bits), 121 bytes captured (968 bits) on interface eth0, id 0
› Ethernet II, Src: XiaomiCommun_90:d9:5e (80:ad:16:90:d9:5e), Dst: AzureWaveTec_9f:9c:0f (2c:3b:70:9f:9c
› Internet Protocol Version 4, Src: 192.168.43.1, Dst: 192.168.43.3
› User Datagram Protocol, Src Port: 53, Dst Port: 61670
› Domain Name System (response)

0000  2c 3b 70 9f 9c 0f 80 ad  16 90 d9 5e 08 00 45 00   ,;p·····  ···^··E·
0010  00 6b 40 32 40 00 40 11  22 fb c0 a8 2b 01 c0 a8   ·k@2@·@·  "···+···
0020  2b 03 00 35 f0 e6 00 57  d8 cb 17 80 81 80 00 01   +··5···W  ········
0030  00 00 00 01 00 00 03 64  6f 68 07 6f 70 65 6e 64   ·······d  oh·opend
0040  6e 73 03 63 6f 6d 00 00  41 00 01 c0 10 00 06 00   ns·com··  A·······
0050  01 00 00 03 98 00 22 05  61 75 74 68 31 c0 10 03   ······"·  auth1···
0060  6e 6f 63 c0 10 68 ff 62  6d 00 00 40 00 00 00 08   noc··h·b  m··@····
0070  00 00 10 00 00 00 0a 00  00                        ········  ·
```

Domain Name System: Protocol
Packets: 17431 · Displayed: 802 (4.6%) · Dropped: 0 (0.0%)
Profile: Default

6. **Export the capture as a .pcap file:**
    - To save press “ctrl+s” give it name then press enter.

7. **Summarize your findings and packet details:**
   Identified Protocols:

1. **DNS**
    - Resolves domain names like *google.com* → IP address.
    - Example: Standard query 0x1a2b A google.com
2. **TCP**
    - Manages connections between client and server.
    - Example: TCP SYN, ACK packets between 192.168.1.5 and 142.250.183.14
3. **HTTP**
    - Transports web content.
    - Example: GET /index.html HTTP/1.1