Task 5: **Capture and Analyze Network Traffic Using Wireshark**

BY: KUSH THAKER. (kthaker442@gmail.com)

Step 0: Identifying OS:

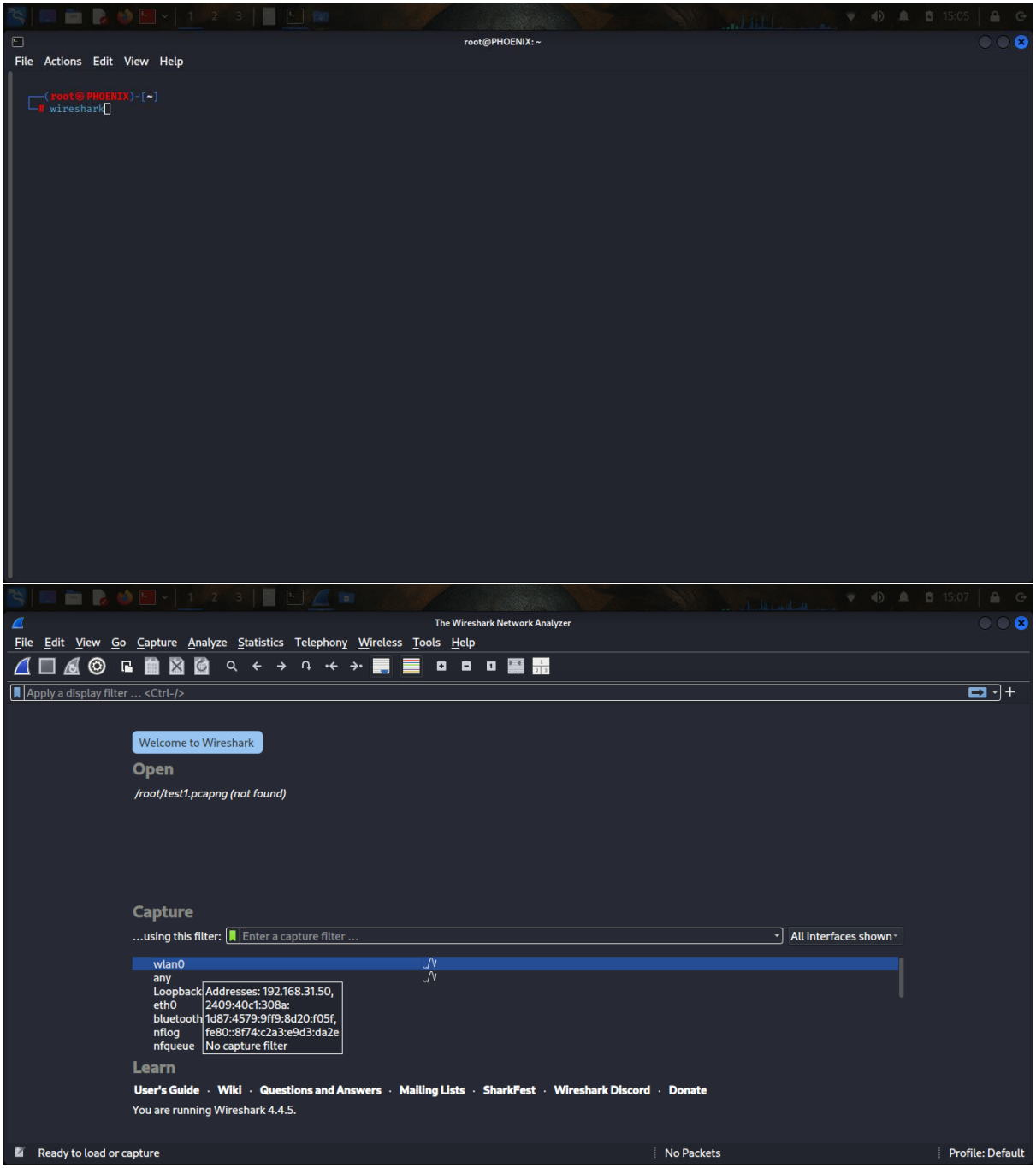
For this task I am going to use my Booted Kali Linux OS.

Step 1,2,3,4,5: Capturing on My active network interface and browsing a website or ping a server to generate traffic. Also filtering the packets (By Protocols TCP, HTTP, DNS).

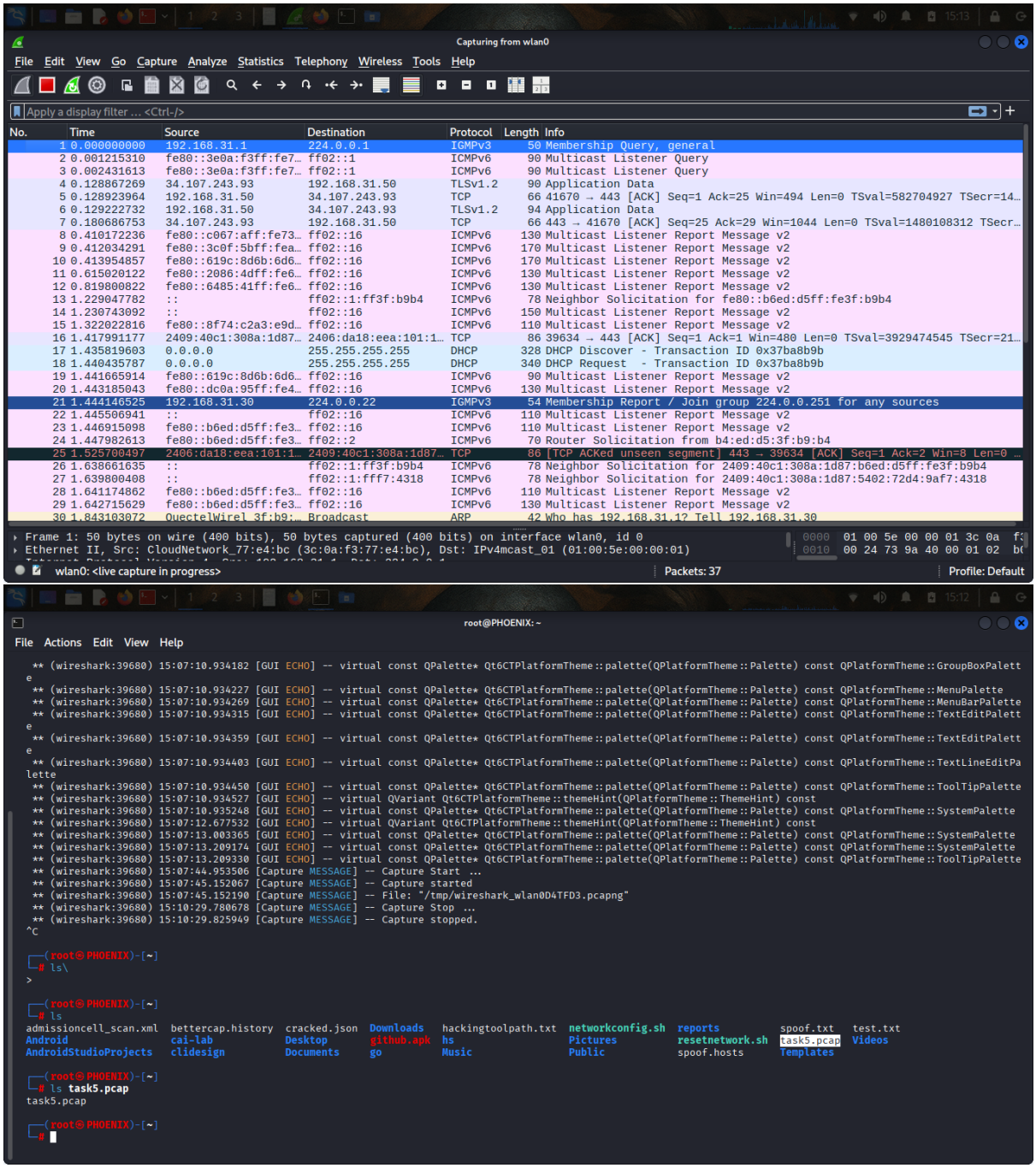
I have Preinstalled the Wireshark so I started it on my interface **wlan0**.

I captured the Traffic for 2-2.5 minutes and saved it in a file named **tasks.pcap**.

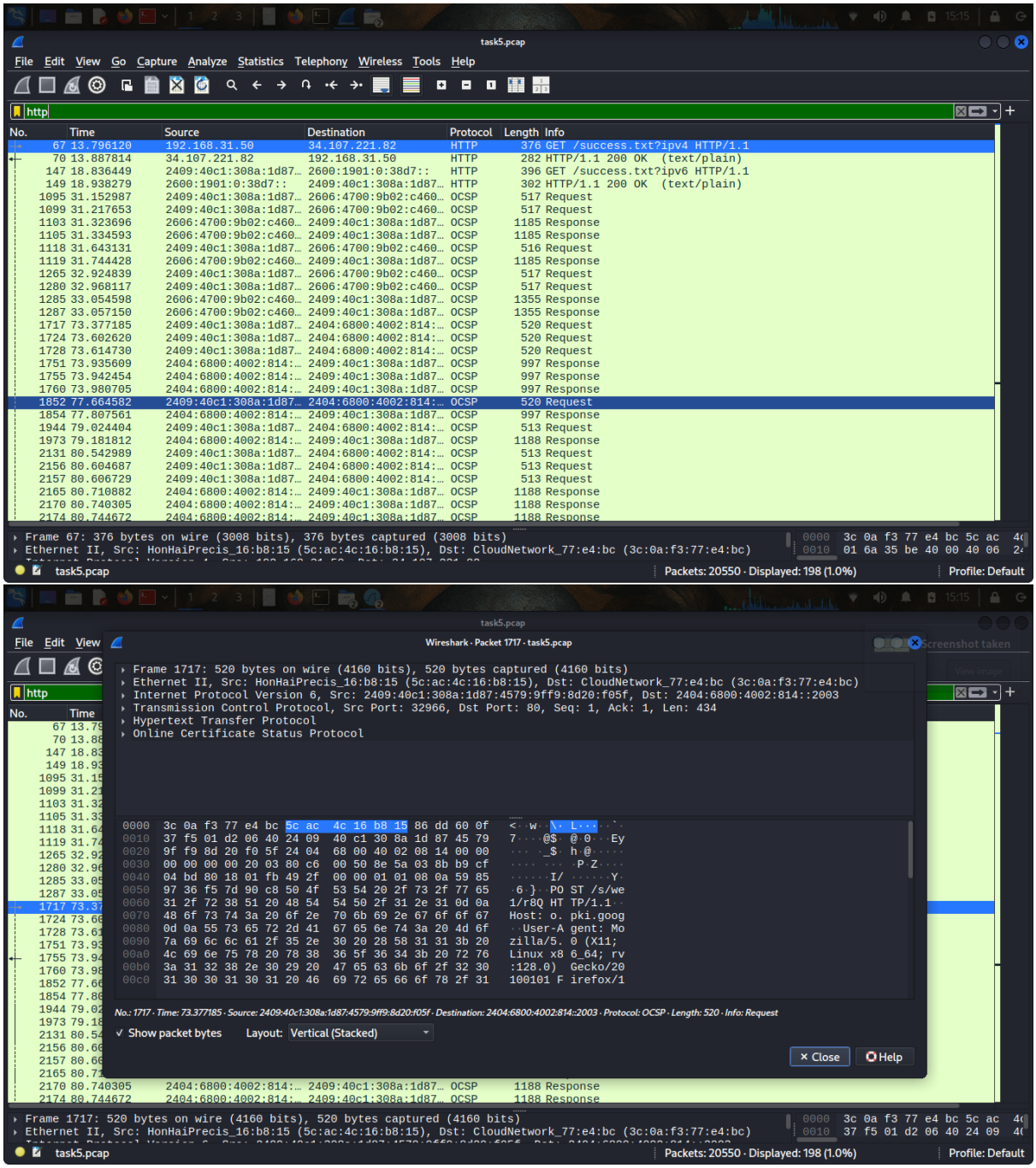
The screenshots are pasted below.


root@PHOENIX: ~
File Actions Edit View Help
(root㉿PHOENIX)-[~]
wireshark

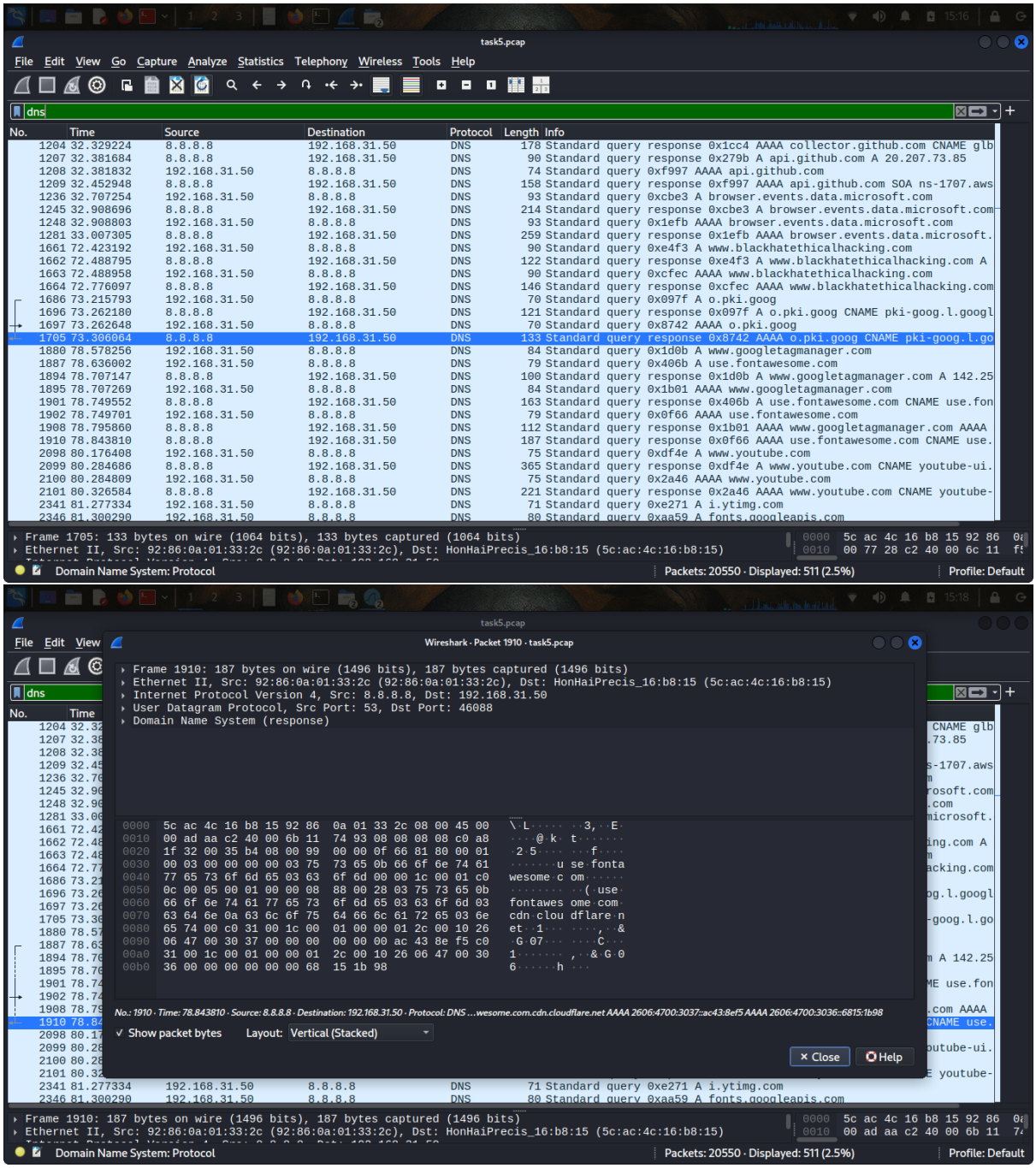
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Open
/root/test1.pcapng (not found)
Capture
...using this filter: Enter a capture filter ...
All interfaces shown
wlan0
any
Loopback
eth0
bluetooth
nflog
nfqueue
Addresses: 192.168.31.50, 2409:40c1:308a:1d87:4579:9ff9:8d20:f05f, fe80::8f74:c2a3:e9d3:da2e
No capture filter
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
You are running Wireshark 4.4.5.
Ready to load or capture
No Packets
Profile: Default


Capturing from wlan0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000000 192.168.31.1 224.0.0.1 IGMPv3 50 Membership Query, general
2 0.001215310 fe80::3e0a:f3ff:fe7… ff02::1 ICMPv6 90 Multicast Listener Query
3 0.002431613 fe80::3e0a:f3ff:fe7… ff02::1 ICMPv6 90 Multicast Listener Query
4 0.128867269 34.107.243.93 192.168.31.50 TLSv1.2 90 Application Data
5 0.128923964 192.168.31.50 34.107.243.93 TCP 66 41670 → 443 [ACK] Seq=1 Ack=25 Win=494 Len=0 TSval=582704927 TSecr=14…
6 0.129222732 192.168.31.50 34.107.243.93 TLSv1.2 94 Application Data
7 0.180686753 34.107.243.93 192.168.31.50 TCP 66 443 → 41670 [ACK] Seq=25 Ack=29 Win=1044 Len=0 TSval=1480108312 TSecr…
8 0.410172236 fe80::c067:aff:fe73… ff02::16 ICMPv6 130 Multicast Listener Report Message v2
9 0.412034291 fe80::3c0f:5bff:fea… ff02::16 ICMPv6 170 Multicast Listener Report Message v2
10 0.413954857 fe80::619c:8d6b:6d6… ff02::16 ICMPv6 170 Multicast Listener Report Message v2
11 0.615020122 fe80::2086:4dff:fe6… ff02::16 ICMPv6 130 Multicast Listener Report Message v2
12 0.819800822 fe80::6485:41ff:fe6… ff02::16 ICMPv6 130 Multicast Listener Report Message v2
13 1.229047782 :: ff02::1:ff3f:b9b4 ICMPv6 78 Neighbor Solicitation for fe80::b6ed:d5ff:fe3f:b9b4
14 1.230743092 :: ff02::16 ICMPv6 150 Multicast Listener Report Message v2
15 1.322022816 fe80::8f74:c2a3:e9d… ff02::16 ICMPv6 110 Multicast Listener Report Message v2
16 1.417991177 2409:40c1:308a:1d87… 2406:da18:eea:101:1… TCP 86 39634 → 443 [ACK] Seq=1 Ack=1 Win=480 Len=0 TSval=3929474545 TSecr=21…
17 1.435819603 0.0.0.0 255.255.255.255 DHCP 328 DHCP Discover - Transaction ID 0x37ba8b9b
18 1.440435787 0.0.0.0 255.255.255.255 DHCP 340 DHCP Request - Transaction ID 0x37ba8b9b
19 1.441665914 fe80::619c:8d6b:6d6… ff02::16 ICMPv6 90 Multicast Listener Report Message v2
20 1.443185043 fe80::dc0a:95ff:fe4… ff02::16 ICMPv6 130 Multicast Listener Report Message v2
21 1.444146525 192.168.31.30 224.0.0.22 IGMPv3 54 Membership Report / Join group 224.0.0.251 for any sources
22 1.445506941 :: ff02::16 ICMPv6 110 Multicast Listener Report Message v2
23 1.446915098 fe80::b6ed:d5ff:fe3… ff02::16 ICMPv6 110 Multicast Listener Report Message v2
24 1.447982613 fe80::b6ed:d5ff:fe3… ff02::2 ICMPv6 70 Router Solicitation from b4:ed:d5:3f:b9:b4
25 1.525700497 2406:da18:eea:101:1… 2409:40c1:308a:1d87… TCP 86 [TCP ACKed unseen segment] 443 → 39634 [ACK] Seq=1 Ack=2 Win=8 Len=0 …
26 1.638661635 :: ff02::1:ff3f:b9b4 ICMPv6 78 Neighbor Solicitation for 2409:40c1:308a:1d87:b6ed:d5ff:fe3f:b9b4
27 1.639800408 :: ff02::1:fff7:4318 ICMPv6 78 Neighbor Solicitation for 2409:40c1:308a:1d87:5402:72d4:9af7:4318
28 1.641174862 fe80::b6ed:d5ff:fe3… ff02::16 ICMPv6 110 Multicast Listener Report Message v2
29 1.642715629 fe80::b6ed:d5ff:fe3… ff02::16 ICMPv6 130 Multicast Listener Report Message v2
30 1.843103072 QuectelWirel_3f:b9:… Broadcast ARP 42 Who has 192.168.31.1? Tell 192.168.31.30
Frame 1: 50 bytes on wire (400 bits), 50 bytes captured (400 bits) on interface wlan0, id 0
Ethernet II, Src: CloudNetwork_77:e4:bc (3c:0a:f3:77:e4:bc), Dst: IPv4mcast_01 (01:00:5e:00:00:01)
0000 01 00 5e 00 00 01 3c 0a
0010 00 24 73 9a 40 00 01 02
wlan0: <live capture in progress>
Packets: 37
Profile: Default

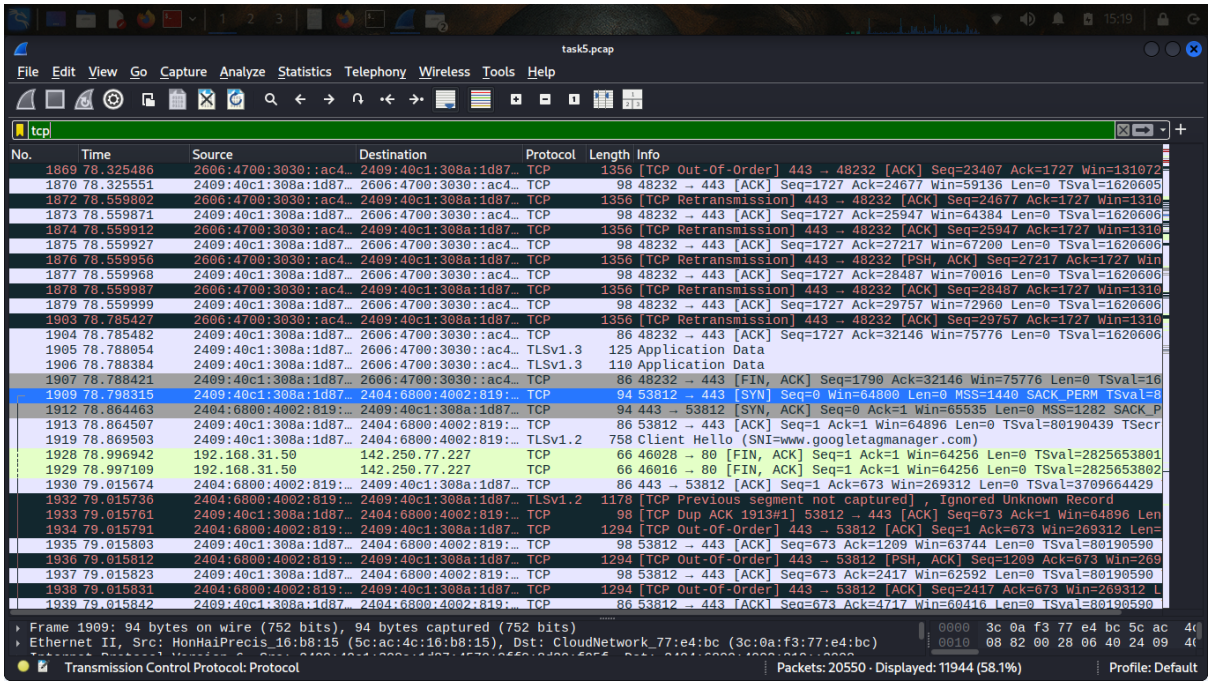
root@PHOENIX: ~
File Actions Edit View Help
** (wireshark:39680) 15:07:10.934182 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::GroupBoxPalette
** (wireshark:39680) 15:07:10.934227 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::MenuPalette
** (wireshark:39680) 15:07:10.934269 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::MenuBarPalette
** (wireshark:39680) 15:07:10.934315 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::TextEditPalette
** (wireshark:39680) 15:07:10.934359 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::TextEditPalette
** (wireshark:39680) 15:07:10.934403 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::TextLineEditPalette
** (wireshark:39680) 15:07:10.934450 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::ToolTipPalette
** (wireshark:39680) 15:07:10.934527 [GUI ECHO] -- virtual QVariant Qt6CTPlatformTheme::themeHint(QPlatformTheme::ThemeHint) const
** (wireshark:39680) 15:07:10.935248 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::SystemPalette
** (wireshark:39680) 15:07:12.677532 [GUI ECHO] -- virtual QVariant Qt6CTPlatformTheme::themeHint(QPlatformTheme::ThemeHint) const
** (wireshark:39680) 15:07:13.003365 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::SystemPalette
** (wireshark:39680) 15:07:13.209174 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::SystemPalette
** (wireshark:39680) 15:07:13.209330 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::ToolTipPalette
** (wireshark:39680) 15:07:44.953506 [Capture MESSAGE] -- Capture Start ...
** (wireshark:39680) 15:07:45.152067 [Capture MESSAGE] -- Capture started
** (wireshark:39680) 15:07:45.152190 [Capture MESSAGE] -- File: "/tmp/wireshark_wlan0D4TFD3.pcapng"
** (wireshark:39680) 15:10:29.780678 [Capture MESSAGE] -- Capture Stop ...
** (wireshark:39680) 15:10:29.825949 [Capture MESSAGE] -- Capture stopped.
^C
(root㉿PHOENIX)-[~]
ls\
>
(root㉿PHOENIX)-[~]
ls
admissioncell_scan.xml bettercap.history cracked.json Downloads hackingtoolpath.txt networkconfig.sh reports spoof.txt test.txt
Android cai-lab Desktop github.apk hs Pictures resetnetwork.sh task5.pcap Videos
AndroidStudioProjects clidesign Documents go Music Public spoof.hosts Templates
(root㉿PHOENIX)-[~]
ls task5.pcap
task5.pcap
(root㉿PHOENIX)-[~]
#


task5.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
67 13.796120 192.168.31.50 34.107.221.82 HTTP 376 GET /success.txt?ipv4 HTTP/1.1
70 13.887814 34.107.221.82 192.168.31.50 HTTP 282 HTTP/1.1 200 OK (text/plain)
147 18.836449 2409:40c1:308a:1d87… 2600:1901:0:38d7:: HTTP 396 GET /success.txt?ipv6 HTTP/1.1
149 18.938279 2600:1901:0:38d7:: 2409:40c1:308a:1d87… HTTP 302 HTTP/1.1 200 OK (text/plain)
1095 31.152987 2409:40c1:308a:1d87… 2606:4700:9b02:c460… OCSP 517 Request
1099 31.217653 2409:40c1:308a:1d87… 2606:4700:9b02:c460… OCSP 517 Request
1103 31.323696 2606:4700:9b02:c460… 2409:40c1:308a:1d87… OCSP 1185 Response
1105 31.334593 2606:4700:9b02:c460… 2409:40c1:308a:1d87… OCSP 1185 Response
1118 31.643131 2409:40c1:308a:1d87… 2606:4700:9b02:c460… OCSP 516 Request
1119 31.744428 2606:4700:9b02:c460… 2409:40c1:308a:1d87… OCSP 1185 Response
1265 32.924839 2409:40c1:308a:1d87… 2606:4700:9b02:c460… OCSP 517 Request
1280 32.968117 2409:40c1:308a:1d87… 2606:4700:9b02:c460… OCSP 517 Request
1285 33.054598 2606:4700:9b02:c460… 2409:40c1:308a:1d87… OCSP 1355 Response
1287 33.057150 2606:4700:9b02:c460… 2409:40c1:308a:1d87… OCSP 1355 Response
1717 73.377185 2409:40c1:308a:1d87… 2404:6800:4002:814:… OCSP 520 Request
1724 73.602620 2409:40c1:308a:1d87… 2404:6800:4002:814:… OCSP 520 Request
1728 73.614730 2409:40c1:308a:1d87… 2404:6800:4002:814:… OCSP 520 Request
1751 73.935609 2404:6800:4002:814:… 2409:40c1:308a:1d87… OCSP 997 Response
1755 73.942454 2404:6800:4002:814:… 2409:40c1:308a:1d87… OCSP 997 Response
1760 73.980705 2404:6800:4002:814:… 2409:40c1:308a:1d87… OCSP 997 Response
1852 77.664582 2409:40c1:308a:1d87… 2404:6800:4002:814:… OCSP 520 Request
1854 77.807561 2404:6800:4002:814:… 2409:40c1:308a:1d87… OCSP 997 Response
1944 79.024404 2409:40c1:308a:1d87… 2404:6800:4002:814:… OCSP 513 Request
1973 79.181812 2404:6800:4002:814:… 2409:40c1:308a:1d87… OCSP 1188 Response
2131 80.542989 2409:40c1:308a:1d87… 2404:6800:4002:814:… OCSP 513 Request
2156 80.604687 2409:40c1:308a:1d87… 2404:6800:4002:814:… OCSP 513 Request
2157 80.606729 2409:40c1:308a:1d87… 2404:6800:4002:814:… OCSP 513 Request
2165 80.710882 2404:6800:4002:814:… 2409:40c1:308a:1d87… OCSP 1188 Response
2170 80.740305 2404:6800:4002:814:… 2409:40c1:308a:1d87… OCSP 1188 Response
2174 80.744672 2404:6800:4002:814:… 2409:40c1:308a:1d87… OCSP 1188 Response
Frame 67: 376 bytes on wire (3008 bits), 376 bytes captured (3008 bits)
Ethernet II, Src: HonHaiPrecis_16:b8:15 (5c:ac:4c:16:b8:15), Dst: CloudNetwork_77:e4:bc (3c:0a:f3:77:e4:bc)
0000 3c 0a f3 77 e4 bc 5c ac
0010 01 6a 35 be 40 00 40 06
task5.pcap
Packets: 20550 · Displayed: 198 (1.0%)
Profile: Default

task5.pcap
File Edit View
Wireshark · Packet 1717 · task5.pcap
Frame 1717: 520 bytes on wire (4160 bits), 520 bytes captured (4160 bits)
Ethernet II, Src: HonHaiPrecis_16:b8:15 (5c:ac:4c:16:b8:15), Dst: CloudNetwork_77:e4:bc (3c:0a:f3:77:e4:bc)
Internet Protocol Version 6, Src: 2409:40c1:308a:1d87:4579:9ff9:8d20:f05f, Dst: 2404:6800:4002:814::2003
Transmission Control Protocol, Src Port: 32966, Dst Port: 80, Seq: 1, Ack: 1, Len: 434
Hypertext Transfer Protocol
Online Certificate Status Protocol
0000 3c 0a f3 77 e4 bc 5c ac 4c 16 b8 15 86 dd 60 0f
0010 37 f5 01 d2 06 40 24 09 40 c1 30 8a 1d 87 45 79
0020 9f f9 8d 20 f0 5f 24 04 68 00 40 02 08 14 00 00
0030 00 00 00 00 20 03 80 c6 00 50 8e 5a 03 8b b9 cf
0040 04 bd 80 18 01 fb 49 2f 00 00 01 01 08 0a 59 85
0050 97 36 f5 7d 90 c8 50 4f 53 54 20 2f 73 2f 77 65
0060 31 2f 72 38 51 20 48 54 54 50 2f 31 2e 31 0d 0a
0070 48 6f 73 74 3a 20 6f 2e 70 6b 69 2e 67 6f 67
0080 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f
0090 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 31 31 3b 20
00a0 4c 69 6e 75 78 20 78 38 36 5f 36 34 3b 20 72 76
00b0 3a 31 32 38 2e 30 29 20 47 65 63 6b 6f 2f 32 30
00c0 31 30 30 31 30 31 20 46 69 72 65 66 6f 78 2f 31
No.: 1717 · Time: 73.377185 · Source: 2409:40c1:308a:1d87:4579:9ff9:8d20:f05f · Destination: 2404:6800:4002:814::2003 · Protocol: OCSP · Length: 520 · Info: Request
Show packet bytes
Layout: Vertical (Stacked)
Close
Help
Frame 1717: 520 bytes on wire (4160 bits), 520 bytes captured (4160 bits)
Ethernet II, Src: HonHaiPrecis_16:b8:15 (5c:ac:4c:16:b8:15), Dst: CloudNetwork_77:e4:bc (3c:0a:f3:77:e4:bc)
0000 3c 0a f3 77 e4 bc 5c ac
0010 37 f5 01 d2 06 40 24 09
task5.pcap
Packets: 20550 · Displayed: 198 (1.0%)
Profile: Default


task5.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Length Info
1204 32.329224 8.8.8.8 192.168.31.50 DNS 178 Standard query response 0x1cc4 AAAA collector.github.com CNAME glb
1207 32.381684 8.8.8.8 192.168.31.50 DNS 90 Standard query response 0x279b A api.github.com A 20.207.73.85
1208 32.381832 192.168.31.50 8.8.8.8 DNS 74 Standard query 0xf997 AAAA api.github.com
1209 32.452948 8.8.8.8 192.168.31.50 DNS 158 Standard query response 0xf997 AAAA api.github.com SOA ns-1707.aws
1236 32.707254 192.168.31.50 8.8.8.8 DNS 93 Standard query 0xcbe3 A browser.events.data.microsoft.com
1245 32.908696 8.8.8.8 192.168.31.50 DNS 214 Standard query response 0xcbe3 A browser.events.data.microsoft.com
1248 32.908803 192.168.31.50 8.8.8.8 DNS 93 Standard query 0x1efb AAAA browser.events.data.microsoft.com
1281 33.007305 8.8.8.8 192.168.31.50 DNS 259 Standard query response 0x1efb AAAA browser.events.data.microsoft.
1661 72.423192 192.168.31.50 8.8.8.8 DNS 90 Standard query 0xe4f3 A www.blackhatethicalhacking.com
1662 72.488795 8.8.8.8 192.168.31.50 DNS 122 Standard query response 0xe4f3 A www.blackhatethicalhacking.com A
1663 72.488958 192.168.31.50 8.8.8.8 DNS 90 Standard query 0xcfec AAAA www.blackhatethicalhacking.com
1664 72.776097 8.8.8.8 192.168.31.50 DNS 146 Standard query response 0xcfec AAAA www.blackhatethicalhacking.com
1686 73.215793 192.168.31.50 8.8.8.8 DNS 70 Standard query 0x097f A o.pki.goog
1696 73.262180 8.8.8.8 192.168.31.50 DNS 121 Standard query response 0x097f A o.pki.goog CNAME pki-goog.l.googl
1697 73.262648 192.168.31.50 8.8.8.8 DNS 70 Standard query 0x8742 AAAA o.pki.goog
1705 73.306064 8.8.8.8 192.168.31.50 DNS 133 Standard query response 0x8742 AAAA o.pki.goog CNAME pki-goog.l.go
1880 78.578256 192.168.31.50 8.8.8.8 DNS 84 Standard query 0x1d0b A www.googletagmanager.com
1887 78.636002 192.168.31.50 8.8.8.8 DNS 79 Standard query 0x406b A use.fontawesome.com
1894 78.707147 8.8.8.8 192.168.31.50 DNS 100 Standard query response 0x1d0b A www.googletagmanager.com A 142.25
1895 78.707269 192.168.31.50 8.8.8.8 DNS 84 Standard query 0x1b01 AAAA www.googletagmanager.com
1901 78.749552 8.8.8.8 192.168.31.50 DNS 163 Standard query response 0x406b A use.fontawesome.com CNAME use.fon
1902 78.749701 192.168.31.50 8.8.8.8 DNS 79 Standard query 0x0f66 AAAA use.fontawesome.com
1908 78.795860 8.8.8.8 192.168.31.50 DNS 112 Standard query response 0x1b01 AAAA www.googletagmanager.com AAAA
1910 78.843810 8.8.8.8 192.168.31.50 DNS 187 Standard query response 0x0f66 AAAA use.fontawesome.com CNAME use.
2098 80.176408 192.168.31.50 8.8.8.8 DNS 75 Standard query 0xdf4e A www.youtube.com
2099 80.284686 8.8.8.8 192.168.31.50 DNS 365 Standard query response 0xdf4e A www.youtube.com CNAME youtube-ui.
2100 80.284809 192.168.31.50 8.8.8.8 DNS 75 Standard query 0x2a46 AAAA www.youtube.com
2101 80.326584 8.8.8.8 192.168.31.50 DNS 221 Standard query response 0x2a46 AAAA www.youtube.com CNAME youtube-
2341 81.277334 192.168.31.50 8.8.8.8 DNS 71 Standard query 0xe271 A i.ytimg.com
2346 81.300290 192.168.31.50 8.8.8.8 DNS 80 Standard query 0xaa59 A fonts.googleapis.com
Frame 1705: 133 bytes on wire (1064 bits), 133 bytes captured (1064 bits)
Ethernet II, Src: 92:86:0a:01:33:2c (92:86:0a:01:33:2c), Dst: HonHaiPrecis_16:b8:15 (5c:ac:4c:16:b8:15)
0000 5c ac 4c 16 b8 15 92 86
0010 00 77 28 c2 40 00 6c 11
Domain Name System: Protocol
Packets: 20550 · Displayed: 511 (2.5%)
Profile: Default

task5.pcap
File Edit View
Wireshark · Packet 1910 · task5.pcap
Frame 1910: 187 bytes on wire (1496 bits), 187 bytes captured (1496 bits)
Ethernet II, Src: 92:86:0a:01:33:2c (92:86:0a:01:33:2c), Dst: HonHaiPrecis_16:b8:15 (5c:ac:4c:16:b8:15)
Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.31.50
User Datagram Protocol, Src Port: 53, Dst Port: 46088
Domain Name System (response)
0000 5c ac 4c 16 b8 15 92 86 0a 01 33 2c 08 00 45 00
0010 00 ad aa c2 40 00 6b 11 74 93 08 08 08 08 c0 a8
0020 1f 32 00 35 b4 08 00 99 00 00 0f 66 81 80 00 01
0030 00 03 00 00 00 00 03 75 73 65 0b 66 6f 6e 74 61
0040 77 65 73 6f 6d 65 03 63 6f 6d 00 00 1c 00 01 c0
0050 0c 00 05 00 01 00 00 08 88 00 28 03 75 73 65 0b
0060 66 6f 6e 74 61 77 65 73 6f 6d 65 03 63 6f 6d 03
0070 63 64 6e 0a 63 6c 6f 75 64 66 6c 61 72 65 03 6e
0080 65 74 00 c0 31 00 1c 00 01 00 00 01 2c 00 10 26
0090 06 47 00 30 37 00 00 00 00 00 00 ac 43 8e f5 c0
00a0 31 00 1c 00 01 00 00 01 2c 00 10 26 06 47 00 30
00b0 36 00 00 00 00 00 00 68 15 1b 98
No.: 1910 · Time: 78.843810 · Source: 8.8.8.8 · Destination: 192.168.31.50 · Protocol: DNS ...wesome.com.cdn.cloudflare.net AAAA 2606:4700:3037::ac43:8ef5 AAAA 2606:4700:3036::6815:1b98
Show packet bytes
Layout: Vertical (Stacked)
Close
Help
1910 78.84
2341 81.277334 192.168.31.50 8.8.8.8 DNS 71 Standard query 0xe271 A i.ytimg.com
2346 81.300290 192.168.31.50 8.8.8.8 DNS 80 Standard query 0xaa59 A fonts.googleapis.com
Frame 1910: 187 bytes on wire (1496 bits), 187 bytes captured (1496 bits)
Ethernet II, Src: 92:86:0a:01:33:2c (92:86:0a:01:33:2c), Dst: HonHaiPrecis_16:b8:15 (5c:ac:4c:16:b8:15)
0000 5c ac 4c 16 b8 15 92 86
0010 00 ad aa c2 40 00 6b 11
Domain Name System: Protocol
Packets: 20550 · Displayed: 511 (2.5%)
Profile: Default


task5.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
1869 78.325486 2606:4700:3030::ac4… 2409:40c1:308a:1d87… TCP 1356 [TCP Out-Of-Order] 443 → 48232 [ACK] Seq=23407 Ack=1727 Win=131072
1870 78.325551 2409:40c1:308a:1d87… 2606:4700:3030::ac4… TCP 98 48232 → 443 [ACK] Seq=1727 Ack=24677 Win=59136 Len=0 TSval=1620605
1872 78.559802 2606:4700:3030::ac4… 2409:40c1:308a:1d87… TCP 1356 [TCP Retransmission] 443 → 48232 [ACK] Seq=24677 Ack=1727 Win=1310
1873 78.559871 2409:40c1:308a:1d87… 2606:4700:3030::ac4… TCP 98 48232 → 443 [ACK] Seq=1727 Ack=25947 Win=64384 Len=0 TSval=1620606
1874 78.559912 2606:4700:3030::ac4… 2409:40c1:308a:1d87… TCP 1356 [TCP Retransmission] 443 → 48232 [ACK] Seq=25947 Ack=1727 Win=1310
1875 78.559927 2409:40c1:308a:1d87… 2606:4700:3030::ac4… TCP 98 48232 → 443 [ACK] Seq=1727 Ack=27217 Win=67200 Len=0 TSval=1620606
1876 78.559956 2606:4700:3030::ac4… 2409:40c1:308a:1d87… TCP 1356 [TCP Retransmission] 443 → 48232 [PSH, ACK] Seq=27217 Ack=1727 Win
1877 78.559968 2409:40c1:308a:1d87… 2606:4700:3030::ac4… TCP 98 48232 → 443 [ACK] Seq=1727 Ack=28487 Win=70016 Len=0 TSval=1620606
1878 78.559987 2606:4700:3030::ac4… 2409:40c1:308a:1d87… TCP 1356 [TCP Retransmission] 443 → 48232 [ACK] Seq=28487 Ack=1727 Win=1310
1879 78.559999 2409:40c1:308a:1d87… 2606:4700:3030::ac4… TCP 98 48232 → 443 [ACK] Seq=1727 Ack=29757 Win=72960 Len=0 TSval=1620606
1903 78.785427 2606:4700:3030::ac4… 2409:40c1:308a:1d87… TCP 1356 [TCP Retransmission] 443 → 48232 [ACK] Seq=29757 Ack=1727 Win=1310
1904 78.785482 2409:40c1:308a:1d87… 2606:4700:3030::ac4… TCP 86 48232 → 443 [ACK] Seq=1727 Ack=32146 Win=75776 Len=0 TSval=1620606
1905 78.788054 2409:40c1:308a:1d87… 2606:4700:3030::ac4… TLSv1.3 125 Application Data
1906 78.788384 2409:40c1:308a:1d87… 2606:4700:3030::ac4… TLSv1.3 110 Application Data
1907 78.788421 2409:40c1:308a:1d87… 2606:4700:3030::ac4… TCP 86 48232 → 443 [FIN, ACK] Seq=1790 Ack=32146 Win=75776 Len=0 TSval=16
1909 78.798315 2409:40c1:308a:1d87… 2404:6800:4002:819:… TCP 94 53812 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 SACK_PERM TSval=8
1912 78.864463 2404:6800:4002:819:… 2409:40c1:308a:1d87… TCP 94 443 → 53812 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1282 SACK_P
1913 78.864507 2409:40c1:308a:1d87… 2404:6800:4002:819:… TCP 86 53812 → 443 [ACK] Seq=1 Ack=1 Win=64896 Len=0 TSval=80190439 TSecr
1919 78.869503 2409:40c1:308a:1d87… 2404:6800:4002:819:… TLSv1.2 758 Client Hello (SNI=www.googletagmanager.com)
1928 78.996942 192.168.31.50 142.250.77.227 TCP 66 46028 → 80 [FIN, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2825653801
1929 78.997109 192.168.31.50 142.250.77.227 TCP 66 46016 → 80 [FIN, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2825653802
1930 79.015674 2404:6800:4002:819:… 2409:40c1:308a:1d87… TCP 86 443 → 53812 [ACK] Seq=1 Ack=673 Win=269312 Len=0 TSval=3709664429
1932 79.015736 2404:6800:4002:819:… 2409:40c1:308a:1d87… TLSv1.2 1178 [TCP Previous segment not captured] , Ignored Unknown Record
1933 79.015761 2409:40c1:308a:1d87… 2404:6800:4002:819:… TCP 98 [TCP Dup ACK 1913#1] 53812 → 443 [ACK] Seq=673 Ack=1 Win=64896 Len
1934 79.015791 2404:6800:4002:819:… 2409:40c1:308a:1d87… TCP 1294 [TCP Out-Of-Order] 443 → 53812 [ACK] Seq=1 Ack=673 Win=269312 Len=
1935 79.015803 2409:40c1:308a:1d87… 2404:6800:4002:819:… TCP 98 53812 → 443 [ACK] Seq=673 Ack=1209 Win=63744 Len=0 TSval=80190590
1936 79.015812 2404:6800:4002:819:… 2409:40c1:308a:1d87… TCP 1294 [TCP Out-Of-Order] 443 → 53812 [PSH, ACK] Seq=1209 Ack=673 Win=269
1937 79.015823 2409:40c1:308a:1d87… 2404:6800:4002:819:… TCP 98 53812 → 443 [ACK] Seq=673 Ack=2417 Win=62592 Len=0 TSval=80190590
1938 79.015831 2404:6800:4002:819:… 2409:40c1:308a:1d87… TCP 1294 [TCP Out-Of-Order] 443 → 53812 [ACK] Seq=2417 Ack=673 Win=269312 L
1939 79.015842 2409:40c1:308a:1d87… 2404:6800:4002:819:… TCP 86 53812 → 443 [ACK] Seq=673 Ack=4717 Win=60416 Len=0 TSval=80190590
Frame 1909: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)
Ethernet II, Src: HonHaiPrecis_16:b8:15 (5c:ac:4c:16:b8:15), Dst: CloudNetwork_77:e4:bc (3c:0a:f3:77:e4:bc)
0000 3c 0a f3 77 e4 bc 5c ac
0010 08 82 00 28 06 40 24 09
Transmission Control Protocol: Protocol
Packets: 20550 · Displayed: 11944 (58.1%)
Profile: Default

Step 6: Identifying the 3 different protocols.

1. TCP (Transmission Control Protocol)

- **Observation from Capture:**
    - Packets show the **3-way handshake**: SYN, SYN/ACK, ACK.
    - Data transfer packets include [PSH, ACK] and retransmissions.
    - Connection terminations observed with FIN, ACK.
- **Example Packet (from screenshot):**
    - Source: 2409:40c1:308a:1d87...
    - Destination: 2404:6800:4002:819... (Google server IPv6)
    - Info: TCP 94 53812 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440
- **Key Point:** TCP is the backbone for reliable data transfer. It ensures packets are ordered and retransmitted if lost.

2. HTTP (Hypertext Transfer Protocol)

- **Observation from Capture:**
    - Requests like GET /success.txt?ipv4 HTTP/1.1 were made.
    - Server responded with HTTP/1.1 200 OK (text/plain) messages.
    - Communication occurred over port 80 (plain HTTP).
- **Example Packet (from screenshot):**
    - Source: 192.168.31.50
    - Destination: 34.107.221.82
    - Info: GET /success.txt?ipv4 HTTP/1.1
- **Key Point:** HTTP is an application-layer protocol used for fetching web resources. Each request contains methods (GET/POST) and responses include status codes (200 OK, etc.).

PTO.

3. DNS (Domain Name System)

- **Observation from Capture:**
    - Queries and responses were exchanged with Google's public DNS (8.8.8.8).
    - Queries included domains like: www.google.com, www.youtube.com, fonts.googleapis.com, etc.
    - Both IPv4 (A records) and IPv6 (AAAA records) queries were seen.
- **Example Packet (from screenshot).**
    - Source: 192.168.31.50
    - Destination: 8.8.8.8
    - Info: Standard query 0x8742 AAAA o.pki.goog CNAME pki-goog.l.google.com
- **Key Point:** DNS is critical for translating domain names into IP addresses before TCP/HTTP can establish communication.

Step 7: Export the capture as a .pcap file.

This file is saved as **task5.pcap**. which is available in this repository's main branch.

Step 8: Summary

Summary of Findings

During the Wireshark capture on **Raavan@PHOENIX (Kali Linux)**, I identified multiple network protocols actively in use. The traffic was generated by browsing websites and performing network queries. The following protocols were captured and analysed:

1. **TCP (Transmission Control Protocol):**
    - Observed the complete 3-way handshake (SYN, SYN/ACK, ACK), data transfer, and connection termination (FIN, ACK).
    - TCP provided reliable, ordered delivery for higher-level protocols like HTTP and TLS.
    - Example: 53812 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440.

2. **HTTP (Hypertext Transfer Protocol):**
    - Captured plain HTTP requests and responses.
    - Requests included GET /success.txt?ipv4 HTTP/1.1.
    - Responses showed HTTP/1.1 200 OK (text/plain), confirming successful retrieval of resources.
    - Example: 192.168.31.50 → 34.107.221.82, GET /success.txt?ipv4 HTTP/1.1.
3. **DNS (Domain Name System):**
    - DNS queries were sent to Google's public resolver (8.8.8.8).
    - Queries included domains such as www.google.com, www.youtube.com, and fonts.googleapis.com.
    - Both A (IPv4) and AAAA (IPv6) records were observed.
    - Example: 192.168.31.50 → 8.8.8.8, Standard query response A www.google.com 142.250.77.227.
4. **TLS (Transport Layer Security):** *(optional, but visible in capture)*
    - TLSv1.2 and TLSv1.3 traffic was present, showing encrypted HTTPS connections.
    - Packets included Client Hello and Application Data.
    - This confirmed secure communication for websites using HTTPS.

Thank You.
Regards,

Kush Thaker