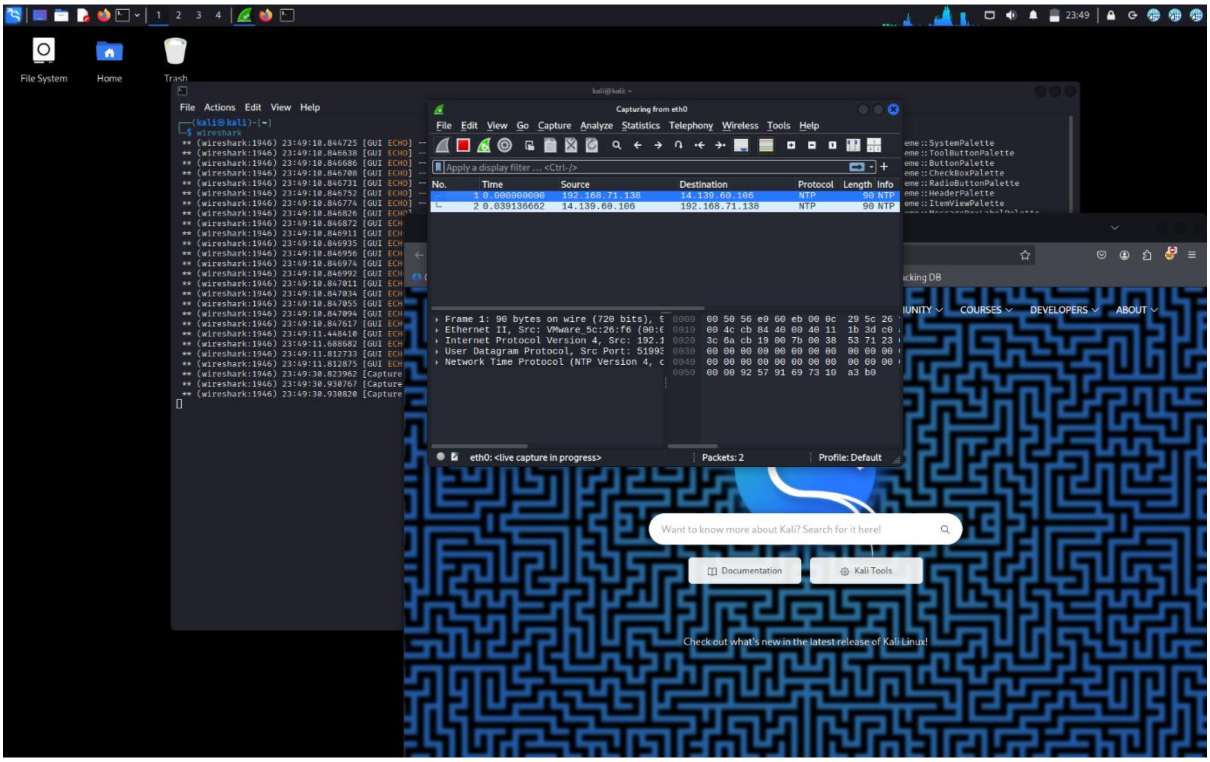
Capture and Analyze Network Traffic Using Wireshark

Introduction

This report details the process of capturing and analyzing network traffic using Wireshark on Kali Linux. The goal was to capture network packets, filter them by protocol, identify different protocols, export the capture, and summarize the findings.

Step1: Start Capturing on Active Network Interface

Opened Wireshark and selected the active network interface (eth0) to begin capturing traffic.



```
┌──(kali㉿kali)-[~]
└─$ wireshark
 ** (wireshark:1946) 23:49:10.844725 [GUI ECHO] --
 ** (wireshark:1946) 23:49:10.846638 [GUI ECHO] --
 ** (wireshark:1946) 23:49:10.846686 [GUI ECHO] --
 ** (wireshark:1946) 23:49:10.846708 [GUI ECHO] --
 ** (wireshark:1946) 23:49:10.846731 [GUI ECHO] --
 ** (wireshark:1946) 23:49:10.846752 [GUI ECHO] --
 ** (wireshark:1946) 23:49:10.846774 [GUI ECHO] --
 ** (wireshark:1946) 23:49:10.846826 [GUI ECHO]
 ** (wireshark:1946) 23:49:10.846872 [GUI ECH
 ** (wireshark:1946) 23:49:10.846911 [GUI ECH
 ** (wireshark:1946) 23:49:10.846935 [GUI ECH
 ** (wireshark:1946) 23:49:10.846956 [GUI ECH
 ** (wireshark:1946) 23:49:10.846974 [GUI ECH
 ** (wireshark:1946) 23:49:10.846992 [GUI ECH
 ** (wireshark:1946) 23:49:10.847011 [GUI ECH
 ** (wireshark:1946) 23:49:10.847034 [GUI ECH
 ** (wireshark:1946) 23:49:10.847055 [GUI ECH
 ** (wireshark:1946) 23:49:10.847094 [GUI ECH
 ** (wireshark:1946) 23:49:10.847617 [GUI ECH
 ** (wireshark:1946) 23:49:11.448410 [GUI ECH
 ** (wireshark:1946) 23:49:11.688682 [GUI ECH
 ** (wireshark:1946) 23:49:11.812733 [GUI ECH
 ** (wireshark:1946) 23:49:11.812875 [GUI ECH
 ** (wireshark:1946) 23:49:30.823962 [Capture
 ** (wireshark:1946) 23:49:30.930767 [Capture
 ** (wireshark:1946) 23:49:30.930820 [Capture
```

```
eme :: SystemPalette
eme :: ToolButtonPalette
eme :: ButtonPalette
eme :: CheckBoxPalette
eme :: RadioButtonPalette
eme :: HeaderPalette
eme :: ItemViewPalette
```

Capturing from eth0

Apply a display filter … <Ctrl-/>

```
No.   Time          Source           Destination      Protocol  Length Info
    1 0.000000000   192.168.71.138   14.139.60.106    NTP           90 NTP
    2 0.039136662   14.139.60.106    192.168.71.138   NTP           90 NTP
```

```
▸ Frame 1: 90 bytes on wire (720 bits), 9
▸ Ethernet II, Src: VMware_5c:26:f6 (00:0
▸ Internet Protocol Version 4, Src: 192.1
▸ User Datagram Protocol, Src Port: 51993
▸ Network Time Protocol (NTP Version 4, c
```

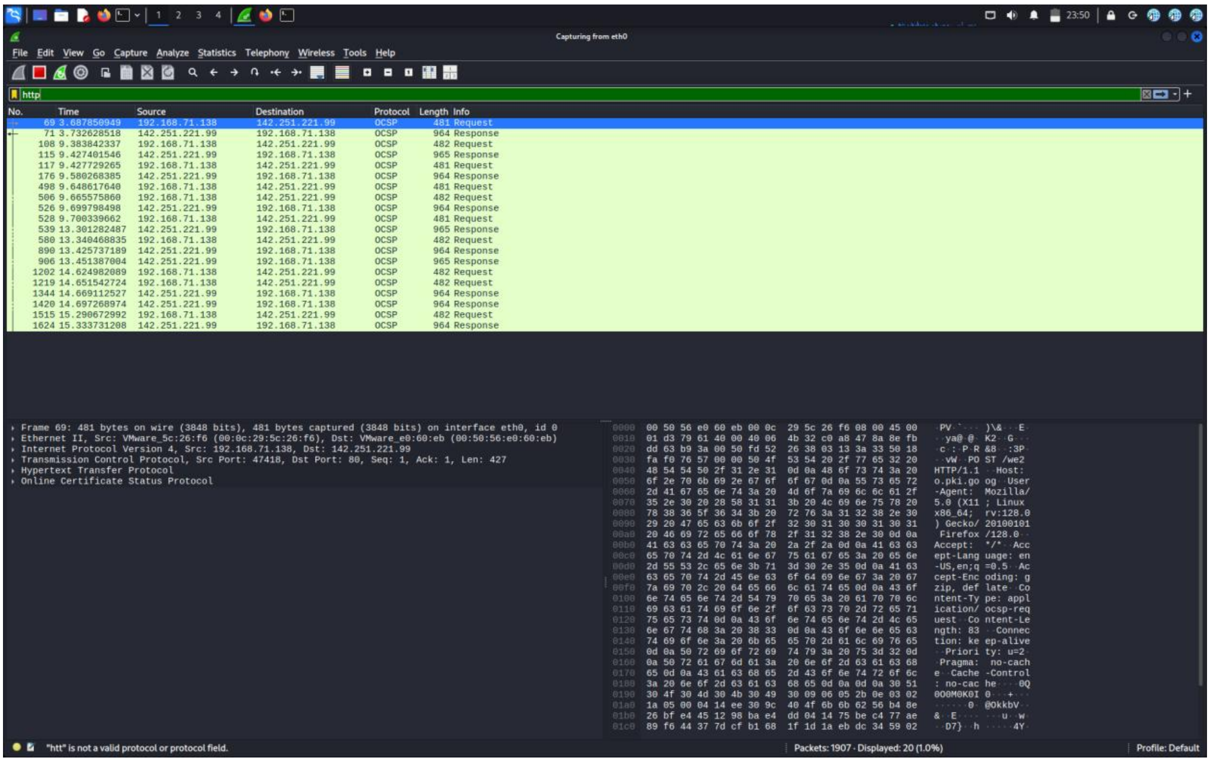
```
0000  00 50 56 e0 60 eb 00 0c  29 5c 26
0010  00 4c cb 84 40 00 40 11  1b 3d c0
0020  3c 6a cb 19 00 7b 00 38  53 71 23
0030  00 00 00 00 00 00 00 00  00 00 00
0040  00 00 00 00 00 00 00 00  00 00 00
0050  00 00 92 57 91 69 73 10  a3 b0
```

eth0: <live capture in progress> | Packets: 2 | Profile: Default

File System
Home
Trash
1 2 3 4
23:49
kali@kali: ~
File Actions Edit View Help
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
cking DB
UNITY
COURSES
DEVELOPERS
ABOUT
Want to know more about Kali? Search for it here!
Documentation
Kali Tools
Check out what's new in the latest release of Kali Linux!

Step2: **Generate Traffic**

Browsed a website and pinged a server to generate network traffic. The capture included HTTP requests and DNS queries.

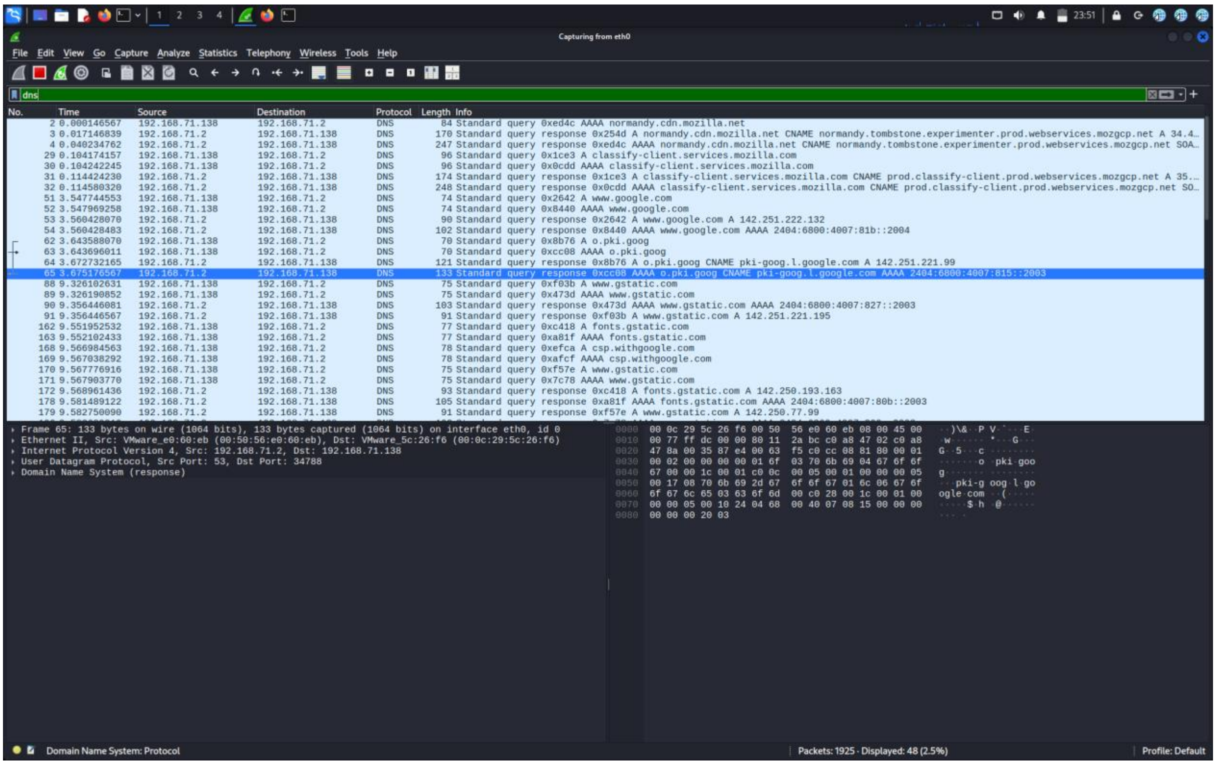

Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
23:50

```
http
No.    Time          Source           Destination      Protocol Length Info
   69 3.687850949   192.168.71.138   142.251.221.99   OCSP     481 Request
   71 3.732628518   142.251.221.99   192.168.71.138   OCSP     964 Response
  108 9.383842337   192.168.71.138   142.251.221.99   OCSP     482 Request
  115 9.427401546   142.251.221.99   192.168.71.138   OCSP     965 Response
  117 9.427729265   192.168.71.138   142.251.221.99   OCSP     481 Request
  176 9.580268385   142.251.221.99   192.168.71.138   OCSP     964 Response
  498 9.648617640   192.168.71.138   142.251.221.99   OCSP     481 Request
  506 9.665575860   192.168.71.138   142.251.221.99   OCSP     482 Request
  526 9.699798498   142.251.221.99   192.168.71.138   OCSP     964 Response
  528 9.700339662   192.168.71.138   142.251.221.99   OCSP     481 Request
  539 13.301282487  142.251.221.99   192.168.71.138   OCSP     965 Response
  580 13.340468835  192.168.71.138   142.251.221.99   OCSP     482 Request
  890 13.425737189  142.251.221.99   192.168.71.138   OCSP     964 Response
  906 13.451387004  142.251.221.99   192.168.71.138   OCSP     965 Response
 1202 14.624982089  192.168.71.138   142.251.221.99   OCSP     482 Request
 1219 14.651542724  192.168.71.138   142.251.221.99   OCSP     482 Request
 1344 14.669112527  142.251.221.99   192.168.71.138   OCSP     964 Response
 1420 14.697268974  142.251.221.99   192.168.71.138   OCSP     964 Response
 1515 15.290672992  192.168.71.138   142.251.221.99   OCSP     482 Request
 1624 15.333731208  142.251.221.99   192.168.71.138   OCSP     964 Response
```

```
› Frame 69: 481 bytes on wire (3848 bits), 481 bytes captured (3848 bits) on interface eth0, id 0
› Ethernet II, Src: VMware_5c:26:f6 (00:0c:29:5c:26:f6), Dst: VMware_e0:60:eb (00:50:56:e0:60:eb)
› Internet Protocol Version 4, Src: 192.168.71.138, Dst: 142.251.221.99
› Transmission Control Protocol, Src Port: 47418, Dst Port: 80, Seq: 1, Ack: 1, Len: 427
› Hypertext Transfer Protocol
› Online Certificate Status Protocol
```

```
0000  00 50 56 e0 60 eb 00 0c  29 5c 26 f6 08 00 45 00   ·PV·`··· )\&··E·
0010  01 d3 79 61 40 00 40 06  4b 32 c0 a8 47 8a 8e fb   ··ya@·@· K2··G···
0020  dd 63 b9 3a 00 50 fd 52  26 38 03 13 3a 33 50 18   ·c·:·P·R &8··:3P·
0030  fa f0 76 57 00 00 50 4f  53 54 20 2f 77 65 32 20   ··vW··PO ST /we2 
0040  48 54 54 50 2f 31 2e 31  0d 0a 48 6f 73 74 3a 20   HTTP/1.1 ··Host: 
0050  6f 2e 70 6b 69 2e 67 6f  6f 67 0d 0a 55 73 65 72   o.pki.go og··User
0060  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61 2f   -Agent:  Mozilla/
0070  35 2e 30 20 28 58 31 31  3b 20 4c 69 6e 75 78 20   5.0 (X11 ; Linux 
0080  78 38 36 5f 36 34 3b 20  72 76 3a 31 32 38 2e 30   x86_64;  rv:128.0
0090  29 20 47 65 63 6b 6f 2f  32 30 31 30 30 31 30 31   ) Gecko/ 20100101
00a0  20 46 69 72 65 66 6f 78  2f 31 32 38 2e 30 0d 0a    Firefox /128.0··
00b0  41 63 63 65 70 74 3a 20  2a 2f 2a 0d 0a 41 63 63   Accept:  */*··Acc
00c0  65 70 74 2d 4c 61 6e 67  75 61 67 65 3a 20 65 6e   ept-Lang uage: en
00d0  2d 55 53 2c 65 6e 3b 71  3d 30 2e 35 0d 0a 41 63   -US,en;q =0.5··Ac
00e0  63 65 70 74 2d 45 6e 63  6f 64 69 6e 67 3a 20 67   cept-Enc oding: g
00f0  7a 69 70 2c 20 64 65 66  6c 61 74 65 0d 0a 43 6f   zip, def late··Co
0100  6e 74 65 6e 74 2d 54 79  70 65 3a 20 61 70 70 6c   ntent-Ty pe: appl
0110  69 63 61 74 69 6f 6e 2f  6f 63 73 70 2d 72 65 71   ication/ ocsp-req
0120  75 65 73 74 0d 0a 43 6f  6e 74 65 6e 74 2d 4c 65   uest··Co ntent-Le
0130  6e 67 74 68 3a 20 38 33  0d 0a 43 6f 6e 6e 65 63   ngth: 83 ··Connec
0140  74 69 6f 6e 3a 20 6b 65  65 70 2d 61 6c 69 76 65   tion: ke ep-alive
0150  0d 0a 50 72 69 6f 72 69  74 79 3a 20 75 3d 32 0d   ··Priori ty: u=2·
0160  0a 50 72 61 67 6d 61 3a  20 6e 6f 2d 63 61 63 68   ·Pragma:  no-cach
0170  65 0d 0a 43 61 63 68 65  2d 43 6f 6e 74 72 6f 6c   e··Cache -Control
0180  3a 20 6e 6f 2d 63 61 63  68 65 0d 0a 0d 0a 30 51   : no-cac he····0Q
0190  30 4f 30 4d 30 4b 30 49  30 09 06 05 2b 0e 03 02   0O0M0K0I 0···+···
01a0  1a 05 00 04 14 ee 30 9c  40 4f 6b 6b 62 56 b4 8e   ······0· @OkkbV··
01b0  26 bf e4 45 12 98 ba e4  dd 04 14 75 be c4 77 ae   &··E···· ···u··w·
01c0  89 f6 44 37 7d cf b1 68  1f 1d 1a eb dc 34 59 02   ··D7}··h ·····4Y·
```

"htt" is not a valid protocol or protocol field. | Packets: 1907 · Displayed: 20 (1.0%) | Profile: Default


Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
23:51

```
dns
No.    Time          Source           Destination      Protocol Length Info
    2 0.000146567   192.168.71.138   192.168.71.2     DNS      84 Standard query 0xed4c AAAA normandy.cdn.mozilla.net
    3 0.017146839   192.168.71.2     192.168.71.138   DNS     170 Standard query response 0x254d A normandy.cdn.mozilla.net CNAME normandy.tombstone.experimenter.prod.webservices.mozgcp.net A 34.4…
    4 0.040234762   192.168.71.2     192.168.71.138   DNS     247 Standard query response 0xed4c AAAA normandy.cdn.mozilla.net CNAME normandy.tombstone.experimenter.prod.webservices.mozgcp.net SOA…
   29 0.104174157   192.168.71.138   192.168.71.2     DNS      96 Standard query 0x1ce3 A classify-client.services.mozilla.com
   30 0.104242245   192.168.71.138   192.168.71.2     DNS      96 Standard query 0x0cdd AAAA classify-client.services.mozilla.com
   31 0.114424230   192.168.71.2     192.168.71.138   DNS     174 Standard query response 0x1ce3 A classify-client.services.mozilla.com CNAME prod.classify-client.prod.webservices.mozgcp.net A 35.…
   32 0.114580320   192.168.71.2     192.168.71.138   DNS     248 Standard query response 0x0cdd AAAA classify-client.services.mozilla.com CNAME prod.classify-client.prod.webservices.mozgcp.net SO…
   51 3.547744553   192.168.71.138   192.168.71.2     DNS      74 Standard query 0x2642 A www.google.com
   52 3.547969258   192.168.71.138   192.168.71.2     DNS      74 Standard query 0x8440 AAAA www.google.com
   53 3.560428070   192.168.71.2     192.168.71.138   DNS      90 Standard query response 0x2642 A www.google.com A 142.251.222.132
   54 3.560428483   192.168.71.2     192.168.71.138   DNS     102 Standard query response 0x8440 AAAA www.google.com AAAA 2404:6800:4007:81b::2004
   62 3.643588070   192.168.71.138   192.168.71.2     DNS      70 Standard query 0x8b76 A o.pki.goog
   63 3.643696011   192.168.71.138   192.168.71.2     DNS      70 Standard query 0xcc08 AAAA o.pki.goog
   64 3.672732165   192.168.71.2     192.168.71.138   DNS     121 Standard query response 0x8b76 A o.pki.goog CNAME pki-goog.l.google.com A 142.251.221.99
   65 3.675176567   192.168.71.2     192.168.71.138   DNS     133 Standard query response 0xcc08 AAAA o.pki.goog CNAME pki-goog.l.google.com AAAA 2404:6800:4007:815::2003
   88 9.326102631   192.168.71.138   192.168.71.2     DNS      75 Standard query 0xf03b A www.gstatic.com
   89 9.326190852   192.168.71.138   192.168.71.2     DNS      75 Standard query 0x473d AAAA www.gstatic.com
   90 9.356446081   192.168.71.2     192.168.71.138   DNS     103 Standard query response 0x473d AAAA www.gstatic.com AAAA 2404:6800:4007:827::2003
   91 9.356446567   192.168.71.2     192.168.71.138   DNS      91 Standard query response 0xf03b A www.gstatic.com A 142.251.221.195
  162 9.551952532   192.168.71.138   192.168.71.2     DNS      77 Standard query 0xc418 A fonts.gstatic.com
  163 9.552102433   192.168.71.138   192.168.71.2     DNS      77 Standard query 0xa81f AAAA fonts.gstatic.com
  168 9.566984563   192.168.71.138   192.168.71.2     DNS      78 Standard query 0xefca A csp.withgoogle.com
  169 9.567038292   192.168.71.138   192.168.71.2     DNS      78 Standard query 0xafcf AAAA csp.withgoogle.com
  170 9.567776916   192.168.71.138   192.168.71.2     DNS      75 Standard query 0xf57e A www.gstatic.com
  171 9.567903770   192.168.71.138   192.168.71.2     DNS      75 Standard query 0x7c78 AAAA www.gstatic.com
  172 9.568961436   192.168.71.2     192.168.71.138   DNS      93 Standard query response 0xc418 A fonts.gstatic.com A 142.250.193.163
  178 9.581489122   192.168.71.2     192.168.71.138   DNS     105 Standard query response 0xa81f AAAA fonts.gstatic.com AAAA 2404:6800:4007:80b::2003
  179 9.582750090   192.168.71.2     192.168.71.138   DNS      91 Standard query response 0xf57e A www.gstatic.com A 142.250.77.99
```

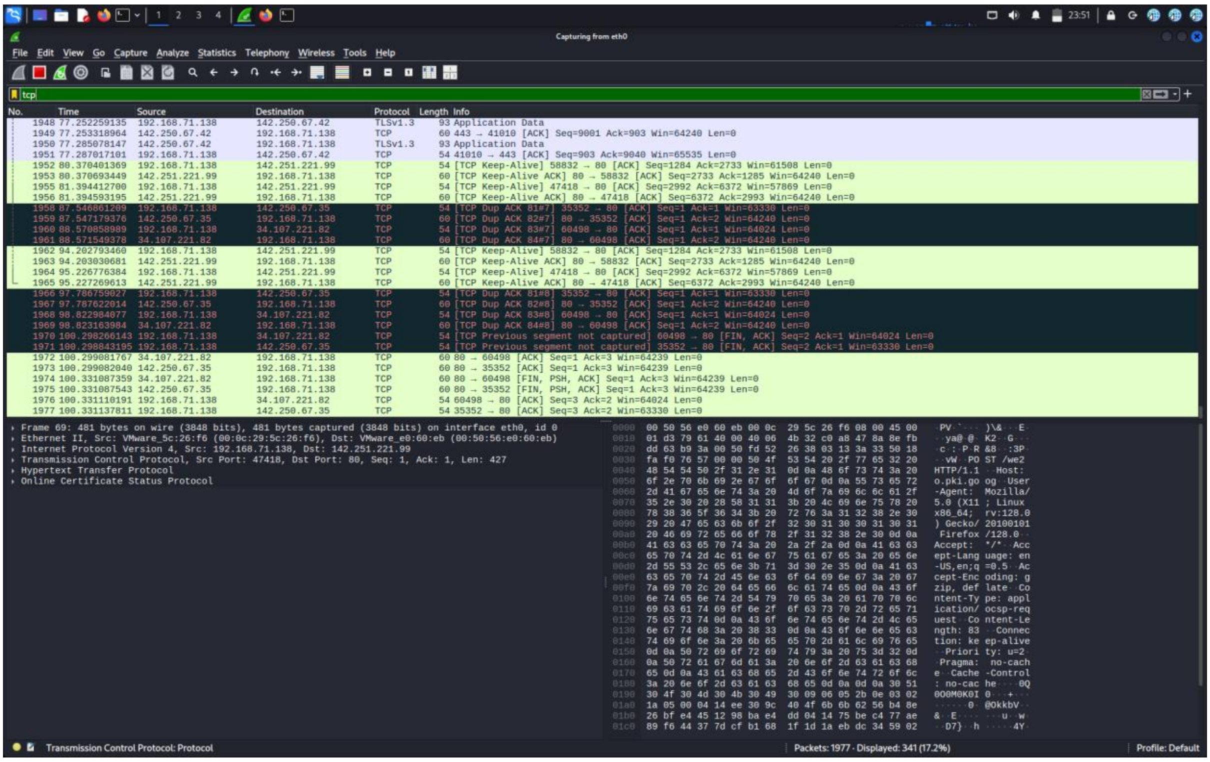
```
› Frame 65: 133 bytes on wire (1064 bits), 133 bytes captured (1064 bits) on interface eth0, id 0
› Ethernet II, Src: VMware_e0:60:eb (00:50:56:e0:60:eb), Dst: VMware_5c:26:f6 (00:0c:29:5c:26:f6)
› Internet Protocol Version 4, Src: 192.168.71.2, Dst: 192.168.71.138
› User Datagram Protocol, Src Port: 53, Dst Port: 34788
› Domain Name System (response)
```

```
0000  00 0c 29 5c 26 f6 00 50  56 e0 60 eb 08 00 45 00   ··)\&··P V·`···E·
0010  00 77 ff dc 00 00 80 11  2a bc c0 a8 47 02 c0 a8   ·w······ *···G···
0020  47 8a 00 35 87 e4 00 63  f5 c0 cc 08 81 80 00 01   G··5···c ········
0030  00 02 00 00 00 00 01 6f  03 70 6b 69 04 67 6f 6f   ·······o ·pki·goo
0040  67 00 00 1c 00 01 c0 0c  00 05 00 01 00 00 00 05   g······· ········
0050  00 17 08 70 6b 69 2d 67  6f 6f 67 01 6c 06 67 6f   ···pki-g oog·l·go
0060  6f 67 6c 65 03 63 6f 6d  00 c0 28 00 1c 00 01 00   ogle·com ··(·····
0070  00 00 05 00 10 24 04 68  00 40 07 08 15 00 00 00   ·····$·h ·@······
0080  00 00 00 20 03                                     ··· ·
```

Domain Name System: Protocol | Packets: 1925 · Displayed: 48 (2.5%) | Profile: Default

Step 3 : **Filter Captured Packets by Protocol**

Applied filters in Wireshark to isolate packets by protocols such as HTTP, DNS, and TCP for detailed analysis.



1 2 3 4
23:51
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

```
No.    Time           Source           Destination      Protocol  Length Info
  1948 77.252259135   192.168.71.138   142.250.67.42    TLSv1.3   93 Application Data
  1949 77.253318964   142.250.67.42    192.168.71.138   TCP       60 443 → 41010 [ACK] Seq=9001 Ack=903 Win=64240 Len=0
  1950 77.285078147   142.250.67.42    192.168.71.138   TLSv1.3   93 Application Data
  1951 77.287017101   192.168.71.138   142.250.67.42    TCP       54 41010 → 443 [ACK] Seq=903 Ack=9040 Win=65535 Len=0
  1952 80.370401369   192.168.71.138   142.251.221.99   TCP       54 [TCP Keep-Alive] 58832 → 80 [ACK] Seq=1284 Ack=2733 Win=61508 Len=0
  1953 80.370693449   142.251.221.99   192.168.71.138   TCP       60 [TCP Keep-Alive ACK] 80 → 58832 [ACK] Seq=2733 Ack=1285 Win=64240 Len=0
  1955 81.394412700   192.168.71.138   142.251.221.99   TCP       54 [TCP Keep-Alive] 47418 → 80 [ACK] Seq=2992 Ack=6372 Win=57869 Len=0
  1956 81.394593195   142.251.221.99   192.168.71.138   TCP       60 [TCP Keep-Alive ACK] 80 → 47418 [ACK] Seq=6372 Ack=2993 Win=64240 Len=0
  1958 87.546861209   192.168.71.138   142.250.67.35    TCP       54 [TCP Dup ACK 81#7] 35352 → 80 [ACK] Seq=1 Ack=1 Win=63330 Len=0
  1959 87.547179376   142.250.67.35    192.168.71.138   TCP       60 [TCP Dup ACK 82#7] 80 → 35352 [ACK] Seq=1 Ack=2 Win=64240 Len=0
  1960 88.570858989   192.168.71.138   34.107.221.82    TCP       54 [TCP Dup ACK 83#7] 60498 → 80 [ACK] Seq=1 Ack=1 Win=64024 Len=0
  1961 88.571549378   34.107.221.82    192.168.71.138   TCP       60 [TCP Dup ACK 84#7] 80 → 60498 [ACK] Seq=1 Ack=2 Win=64240 Len=0
  1962 94.202793460   192.168.71.138   142.251.221.99   TCP       54 [TCP Keep-Alive] 58832 → 80 [ACK] Seq=1284 Ack=2733 Win=61508 Len=0
  1963 94.203030681   142.251.221.99   192.168.71.138   TCP       60 [TCP Keep-Alive ACK] 80 → 58832 [ACK] Seq=2733 Ack=1285 Win=64240 Len=0
  1964 95.226776384   192.168.71.138   142.251.221.99   TCP       54 [TCP Keep-Alive] 47418 → 80 [ACK] Seq=2992 Ack=6372 Win=57869 Len=0
  1965 95.227269613   142.251.221.99   192.168.71.138   TCP       60 [TCP Keep-Alive ACK] 80 → 47418 [ACK] Seq=6372 Ack=2993 Win=64240 Len=0
  1966 97.786759027   192.168.71.138   142.250.67.35    TCP       54 [TCP Dup ACK 81#8] 35352 → 80 [ACK] Seq=1 Ack=1 Win=63330 Len=0
  1967 97.787622014   142.250.67.35    192.168.71.138   TCP       60 [TCP Dup ACK 82#8] 80 → 35352 [ACK] Seq=1 Ack=2 Win=64240 Len=0
  1968 98.822984077   192.168.71.138   34.107.221.82    TCP       54 [TCP Dup ACK 83#8] 60498 → 80 [ACK] Seq=1 Ack=1 Win=64024 Len=0
  1969 98.823163984   34.107.221.82    192.168.71.138   TCP       60 [TCP Dup ACK 84#8] 80 → 60498 [ACK] Seq=1 Ack=2 Win=64240 Len=0
  1970 100.298266143  192.168.71.138   34.107.221.82    TCP       54 [TCP Previous segment not captured] 60498 → 80 [FIN, ACK] Seq=2 Ack=1 Win=64024 Len=0
  1971 100.298843195  192.168.71.138   142.250.67.35    TCP       54 [TCP Previous segment not captured] 35352 → 80 [FIN, ACK] Seq=2 Ack=1 Win=63330 Len=0
  1972 100.299081767  34.107.221.82    192.168.71.138   TCP       60 80 → 60498 [ACK] Seq=1 Ack=3 Win=64239 Len=0
  1973 100.299082040  142.250.67.35    192.168.71.138   TCP       60 80 → 35352 [ACK] Seq=1 Ack=3 Win=64239 Len=0
  1974 100.331087359  34.107.221.82    192.168.71.138   TCP       60 80 → 60498 [FIN, PSH, ACK] Seq=1 Ack=3 Win=64239 Len=0
  1975 100.331087543  142.250.67.35    192.168.71.138   TCP       60 80 → 35352 [FIN, PSH, ACK] Seq=1 Ack=3 Win=64239 Len=0
  1976 100.331110191  192.168.71.138   34.107.221.82    TCP       54 60498 → 80 [ACK] Seq=3 Ack=2 Win=64024 Len=0
  1977 100.331137811  192.168.71.138   142.250.67.35    TCP       54 35352 → 80 [ACK] Seq=3 Ack=2 Win=63330 Len=0
```

```
› Frame 69: 481 bytes on wire (3848 bits), 481 bytes captured (3848 bits) on interface eth0, id 0
› Ethernet II, Src: VMware_5c:26:f6 (00:0c:29:5c:26:f6), Dst: VMware_e0:60:eb (00:50:56:e0:60:eb)
› Internet Protocol Version 4, Src: 192.168.71.138, Dst: 142.251.221.99
› Transmission Control Protocol, Src Port: 47418, Dst Port: 80, Seq: 1, Ack: 1, Len: 427
› Hypertext Transfer Protocol
› Online Certificate Status Protocol
```

```
0000  00 50 56 e0 60 eb 00 0c  29 5c 26 f6 08 00 45 00   ·PV·`···)\&···E·
0010  01 d3 79 61 40 00 40 06  4b 32 c0 a8 47 8a 8e fb   ··ya@·@·K2··G···
0020  dd 63 b9 3a 00 50 fd 52  26 38 03 13 3a 33 50 18   ·c·:·P·R&8··:3P·
0030  fa f0 76 57 00 00 50 4f  53 54 20 2f 77 65 32 20   ··vW··POST /we2 
0040  48 54 54 50 2f 31 2e 31  0d 0a 48 6f 73 74 3a 20   HTTP/1.1··Host: 
0050  6f 2e 70 6b 69 2e 67 6f  6f 67 0d 0a 55 73 65 72   o.pki.goog··User
0060  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61 2f   -Agent: Mozilla/
0070  35 2e 30 20 28 58 31 31  3b 20 4c 69 6e 75 78 20   5.0 (X11; Linux 
0080  78 38 36 5f 36 34 3b 20  72 76 3a 31 32 38 2e 30   x86_64; rv:128.0
0090  29 20 47 65 63 6b 6f 2f  32 30 31 30 30 31 30 31   ) Gecko/20100101
00a0  20 46 69 72 65 66 6f 78  2f 31 32 38 2e 30 0d 0a    Firefox/128.0··
00b0  41 63 63 65 70 74 3a 20  2a 2f 2a 0d 0a 41 63 63   Accept: */*··Acc
00c0  65 70 74 2d 4c 61 6e 67  75 61 67 65 3a 20 65 6e   ept-Language: en
00d0  2d 55 53 2c 65 6e 3b 71  3d 30 2e 35 0d 0a 41 63   -US,en;q=0.5··Ac
00e0  63 65 70 74 2d 45 6e 63  6f 64 69 6e 67 3a 20 67   cept-Encoding: g
00f0  7a 69 70 2c 20 64 65 66  6c 61 74 65 0d 0a 43 6f   zip, deflate··Co
0100  6e 74 65 6e 74 2d 54 79  70 65 3a 20 61 70 70 6c   ntent-Type: appl
0110  69 63 61 74 69 6f 6e 2f  6f 63 73 70 2d 72 65 71   ication/ocsp-req
0120  75 65 73 74 0d 0a 43 6f  6e 74 65 6e 74 2d 4c 65   uest··Content-Le
0130  6e 67 74 68 3a 20 38 33  0d 0a 43 6f 6e 6e 65 63   ngth: 83··Connec
0140  74 69 6f 6e 3a 20 6b 65  65 70 2d 61 6c 69 76 65   tion: keep-alive
0150  0d 0a 50 72 69 6f 72 69  74 79 3a 20 75 3d 32 0d   ··Priority: u=2·
0160  0a 50 72 61 67 6d 61 3a  20 6e 6f 2d 63 61 63 68   ·Pragma: no-cach
0170  65 0d 0a 43 61 63 68 65  2d 43 6f 6e 74 72 6f 6c   e··Cache-Control
0180  3a 20 6e 6f 2d 63 61 63  68 65 0d 0a 0d 0a 30 51   : no-cache····0Q
0190  30 4f 30 4d 30 4b 30 49  30 09 06 05 2b 0e 03 02   0O0M0K0I0···+···
01a0  1a 05 00 04 14 ee 30 9c  40 4f 6b 6b 62 56 b4 8e   ······0·@OkkbV··
01b0  26 bf e4 45 12 98 ba e4  dd 04 14 75 be c4 77 ae   &··E·······u··w·
01c0  89 f6 44 37 7d cf b1 68  1f 1d 1a eb dc 34 59 02   ··D7}··h·····4Y·
```

Transmission Control Protocol: Protocol

Packets: 1977 · Displayed: 341 (17.2%)

Profile: Default

Step 4 : Types of Protocols

- **HTTP**: Seen in the First screenshot with requests to mozilla.net and responses (e.g., Frame 69, 481 bytes).
- **DNS**: Visible in the second screenshot with queries and responses (e.g., AAAA records for normandy.cdn.mozilla.net).
- **TCP**: Present in the third screenshot, managing data flow with sequence and acknowledgment numbers.

Conclusion :

This exercise successfully demonstrated network traffic analysis on Kali Linux using Wireshark. The presence of HTTP, DNS, and TCP protocols illustrates the layered communication process.