Avikant Saini, 140905508, CSE-B (43), CP-12

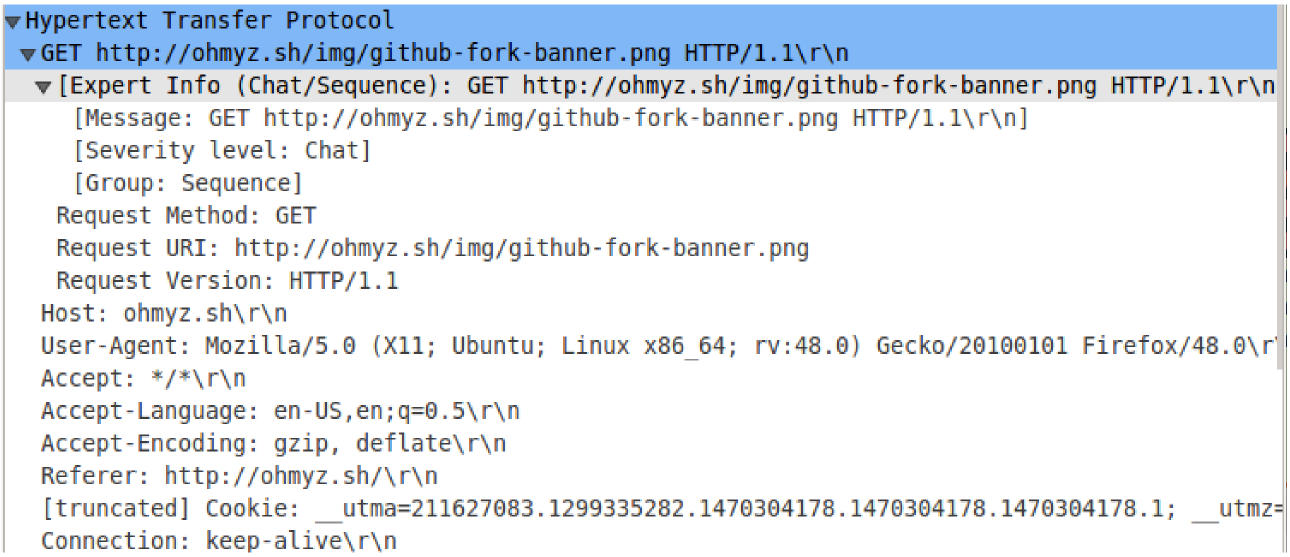
Study of application layer protocols

Lab 7.0

```
inet addr:172.16.59.52
```

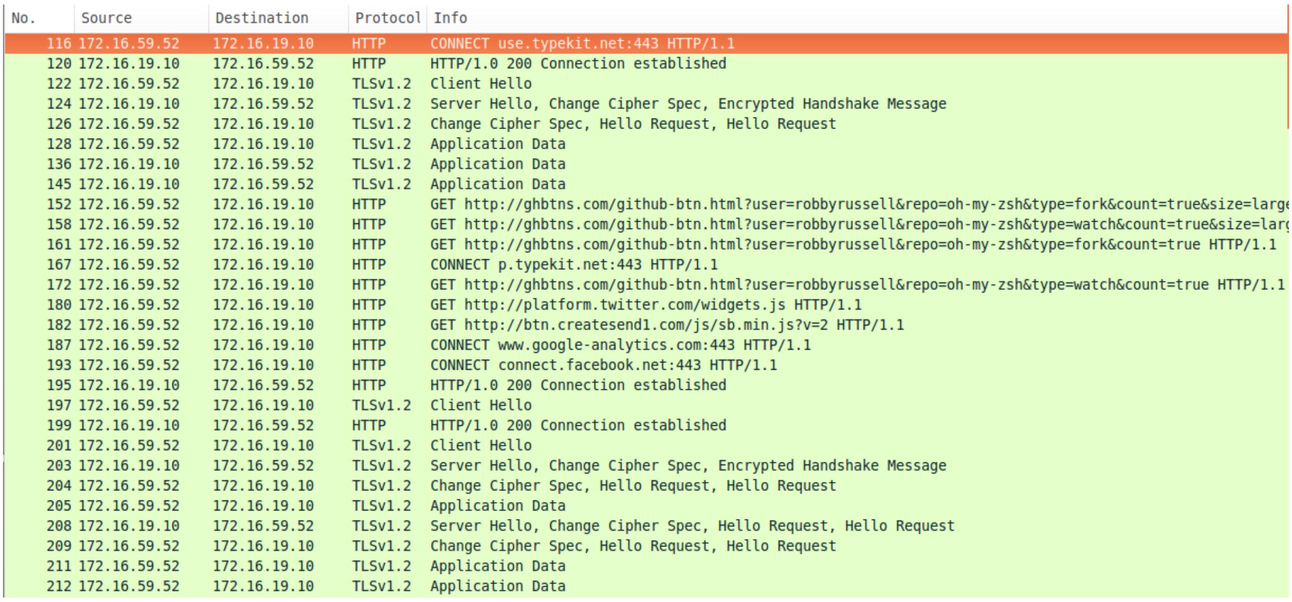
7.1 Retrieving web pages with HTTP

-- Accessing "http://ohmyz.sh/"

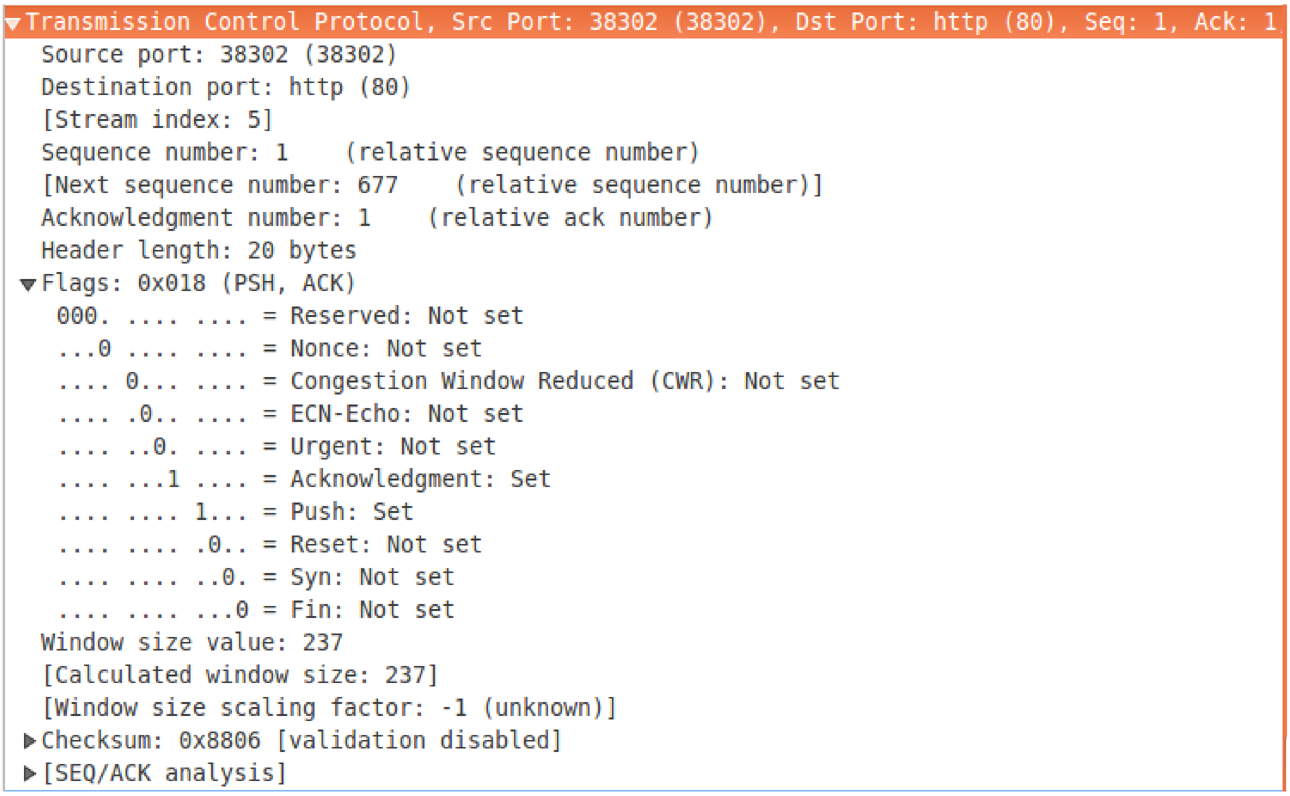


```
▼Hypertext Transfer Protocol
 ▼GET http://ohmyz.sh/img/github-fork-banner.png HTTP/1.1\r\n
  ▼[Expert Info (Chat/Sequence): GET http://ohmyz.sh/img/github-fork-banner.png HTTP/1.1\r\n
     [Message: GET http://ohmyz.sh/img/github-fork-banner.png HTTP/1.1\r\n]
     [Severity level: Chat]
     [Group: Sequence]
    Request Method: GET
    Request URI: http://ohmyz.sh/img/github-fork-banner.png
    Request Version: HTTP/1.1
  Host: ohmyz.sh\r\n
  User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:48.0) Gecko/20100101 Firefox/48.0\r
  Accept: */*\r\n
  Accept-Language: en-US,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate\r\n
  Referer: http://ohmyz.sh/\r\n
  [truncated] Cookie: __utma=211627083.1299335282.1470304178.1470304178.1470304178.1; __utmz=
  Connection: keep-alive\r\n
```

Avikant Saini, 140905508, CSE-B (43), CP-12



```
No.   Source         Destination    Protocol Info
  116 172.16.59.52   172.16.19.10   HTTP     CONNECT use.typekit.net:443 HTTP/1.1
  120 172.16.19.10   172.16.59.52   HTTP     HTTP/1.0 200 Connection established
  122 172.16.59.52   172.16.19.10   TLSv1.2  Client Hello
  124 172.16.19.10   172.16.59.52   TLSv1.2  Server Hello, Change Cipher Spec, Encrypted Handshake Message
  126 172.16.59.52   172.16.19.10   TLSv1.2  Change Cipher Spec, Hello Request, Hello Request
  128 172.16.59.52   172.16.19.10   TLSv1.2  Application Data
  136 172.16.19.10   172.16.59.52   TLSv1.2  Application Data
  145 172.16.19.10   172.16.59.52   TLSv1.2  Application Data
  152 172.16.59.52   172.16.19.10   HTTP     GET http://ghbtns.com/github-btn.html?user=robbyrussell&repo=oh-my-zsh&type=fork&count=true&size=large
  158 172.16.59.52   172.16.19.10   HTTP     GET http://ghbtns.com/github-btn.html?user=robbyrussell&repo=oh-my-zsh&type=watch&count=true&size=larg
  161 172.16.59.52   172.16.19.10   HTTP     GET http://ghbtns.com/github-btn.html?user=robbyrussell&repo=oh-my-zsh&type=fork&count=true HTTP/1.1
  167 172.16.59.52   172.16.19.10   HTTP     CONNECT p.typekit.net:443 HTTP/1.1
  172 172.16.59.52   172.16.19.10   HTTP     GET http://ghbtns.com/github-btn.html?user=robbyrussell&repo=oh-my-zsh&type=watch&count=true HTTP/1.1
  180 172.16.59.52   172.16.19.10   HTTP     GET http://platform.twitter.com/widgets.js HTTP/1.1
  182 172.16.59.52   172.16.19.10   HTTP     GET http://btn.createsend1.com/js/sb.min.js?v=2 HTTP/1.1
  187 172.16.59.52   172.16.19.10   HTTP     CONNECT www.google-analytics.com:443 HTTP/1.1
  193 172.16.59.52   172.16.19.10   HTTP     CONNECT connect.facebook.net:443 HTTP/1.1
  195 172.16.19.10   172.16.59.52   HTTP     HTTP/1.0 200 Connection established
  197 172.16.59.52   172.16.19.10   TLSv1.2  Client Hello
  199 172.16.19.10   172.16.59.52   HTTP     HTTP/1.0 200 Connection established
  201 172.16.59.52   172.16.19.10   TLSv1.2  Client Hello
  203 172.16.19.10   172.16.59.52   TLSv1.2  Server Hello, Change Cipher Spec, Encrypted Handshake Message
  204 172.16.59.52   172.16.19.10   TLSv1.2  Change Cipher Spec, Hello Request, Hello Request
  205 172.16.59.52   172.16.19.10   TLSv1.2  Application Data
  208 172.16.19.10   172.16.59.52   TLSv1.2  Server Hello, Change Cipher Spec, Hello Request, Hello Request
  209 172.16.59.52   172.16.19.10   TLSv1.2  Change Cipher Spec, Hello Request, Hello Request
  211 172.16.59.52   172.16.19.10   TLSv1.2  Application Data
  212 172.16.59.52   172.16.19.10   TLSv1.2  Application Data
```



```
▼Transmission Control Protocol, Src Port: 38302 (38302), Dst Port: http (80), Seq: 1, Ack: 1
   Source port: 38302 (38302)
   Destination port: http (80)
   [Stream index: 5]
   Sequence number: 1    (relative sequence number)
   [Next sequence number: 677    (relative sequence number)]
   Acknowledgment number: 1    (relative ack number)
   Header length: 20 bytes
 ▼Flags: 0x018 (PSH, ACK)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Nonce: Not set
    .... 0... .... = Congestion Window Reduced (CWR): Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...1 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
   Window size value: 237
   [Calculated window size: 237]
   [Window size scaling factor: -1 (unknown)]
 ▶Checksum: 0x8806 [validation disabled]
 ▶[SEQ/ACK analysis]
```

HTTP makes a lot of calls while accessing a webpage. It starts with a three way handshake – client hello, server hello, and a hello acknowledgement.

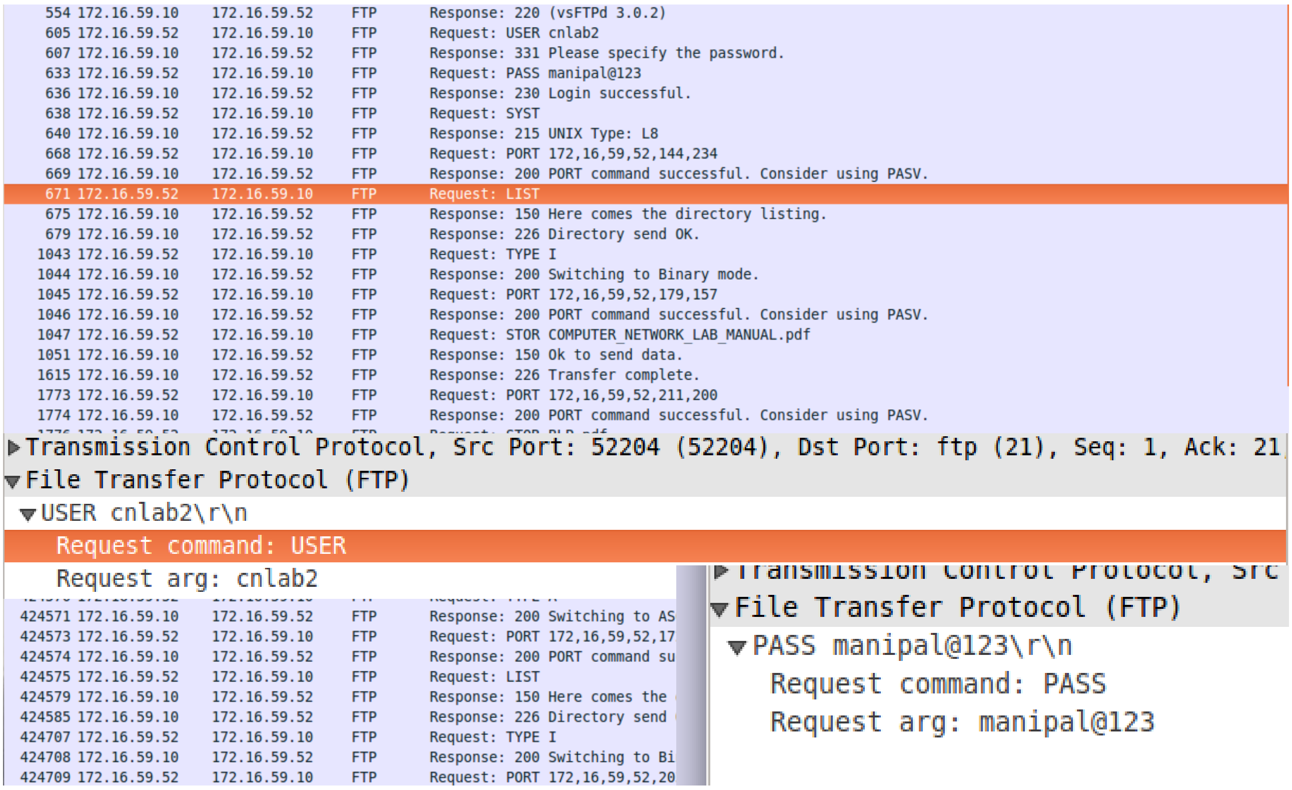
Some common HTTP status codes include 200 for OK, 204 for no content, 301 for moved, 304 for not modified, 400 for bad request, 401 if unauthorized, 404 if not found, 418 for “I'm a teapot”.

HTTP transmission works on top of Transmission Control Protocol layer.

7.2 FTP transfer

FTP is **insecure**, as we can see all the packets dump while the connection is on including the user credentials: username, and password, details of the files transferred, and even the files' data. With this information, anyone can **snoop** in to your credentials.

FTP transfer also works on top on TCP.

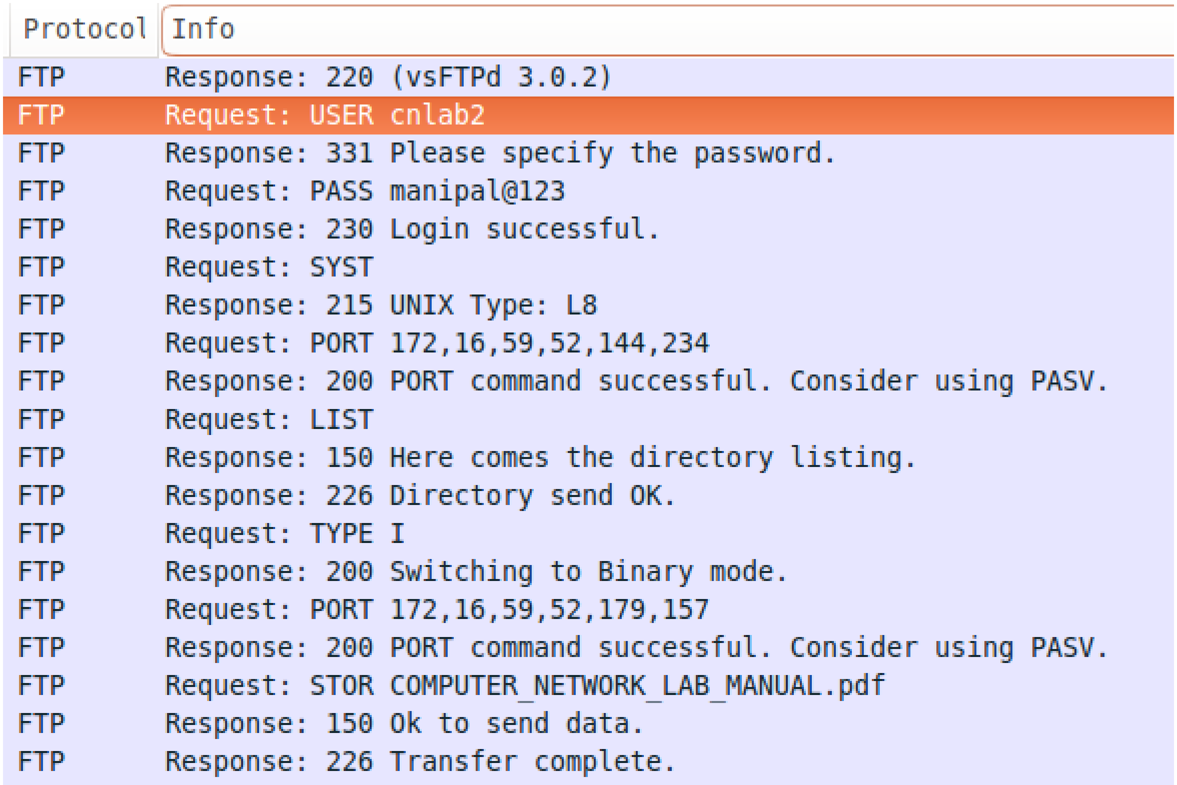


```
 554 172.16.59.10   172.16.59.52   FTP   Response: 220 (vsFTPd 3.0.2)
 605 172.16.59.52   172.16.59.10   FTP   Request: USER cnlab2
 607 172.16.59.10   172.16.59.52   FTP   Response: 331 Please specify the password.
 633 172.16.59.52   172.16.59.10   FTP   Request: PASS manipal@123
 636 172.16.59.10   172.16.59.52   FTP   Response: 230 Login successful.
 638 172.16.59.52   172.16.59.10   FTP   Request: SYST
 640 172.16.59.10   172.16.59.52   FTP   Response: 215 UNIX Type: L8
 668 172.16.59.52   172.16.59.10   FTP   Request: PORT 172,16,59,52,144,234
 669 172.16.59.10   172.16.59.52   FTP   Response: 200 PORT command successful. Consider using PASV.
 671 172.16.59.52   172.16.59.10   FTP   Request: LIST
 675 172.16.59.10   172.16.59.52   FTP   Response: 150 Here comes the directory listing.
 679 172.16.59.10   172.16.59.52   FTP   Response: 226 Directory send OK.
1043 172.16.59.52   172.16.59.10   FTP   Request: TYPE I
1044 172.16.59.10   172.16.59.52   FTP   Response: 200 Switching to Binary mode.
1045 172.16.59.52   172.16.59.10   FTP   Request: PORT 172,16,59,52,179,157
1046 172.16.59.10   172.16.59.52   FTP   Response: 200 PORT command successful. Consider using PASV.
1047 172.16.59.52   172.16.59.10   FTP   Request: STOR COMPUTER_NETWORK_LAB_MANUAL.pdf
1051 172.16.59.10   172.16.59.52   FTP   Response: 150 Ok to send data.
1615 172.16.59.10   172.16.59.52   FTP   Response: 226 Transfer complete.
1773 172.16.59.52   172.16.59.10   FTP   Request: PORT 172,16,59,52,211,200
1774 172.16.59.10   172.16.59.52   FTP   Response: 200 PORT command successful. Consider using PASV.
```

```
▶Transmission Control Protocol, Src Port: 52204 (52204), Dst Port: ftp (21), Seq: 1, Ack: 21
▼File Transfer Protocol (FTP)
 ▼USER cnlab2\r\n
    Request command: USER
    Request arg: cnlab2
```

```
424571 172.16.59.10   172.16.59.52   FTP   Response: 200 Switching to AS
424573 172.16.59.52   172.16.59.10   FTP   Request: PORT 172,16,59,52,17
424574 172.16.59.10   172.16.59.52   FTP   Response: 200 PORT command su
424575 172.16.59.52   172.16.59.10   FTP   Request: LIST
424579 172.16.59.10   172.16.59.52   FTP   Response: 150 Here comes the
424585 172.16.59.10   172.16.59.52   FTP   Response: 226 Directory send
424707 172.16.59.52   172.16.59.10   FTP   Request: TYPE I
424708 172.16.59.10   172.16.59.52   FTP   Response: 200 Switching to Bi
424709 172.16.59.52   172.16.59.10   FTP   Request: PORT 172,16,59,52,20
```

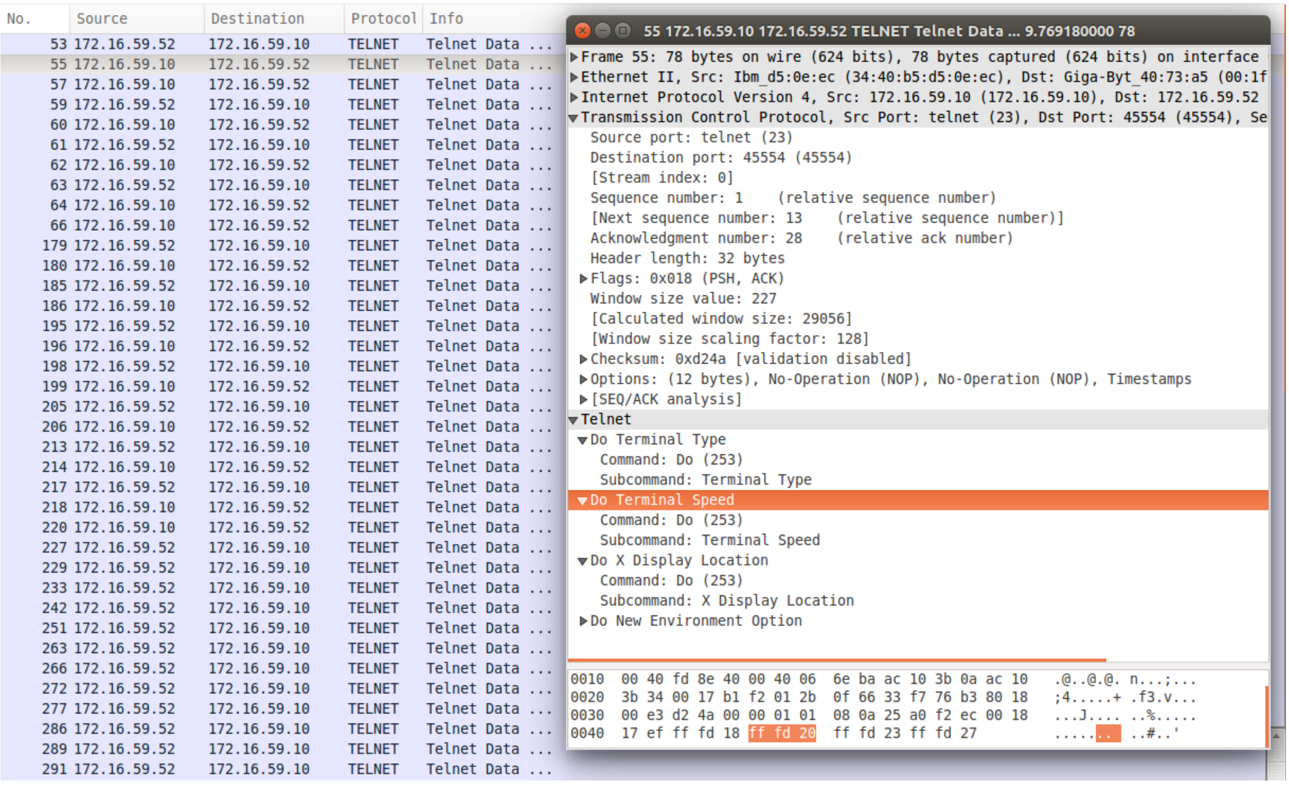
```
▶Transmission Control Protocol, Src
▼File Transfer Protocol (FTP)
 ▼PASS manipal@123\r\n
    Request command: PASS
    Request arg: manipal@123
```



```
Protocol  Info
FTP       Response: 220 (vsFTPd 3.0.2)
FTP       Request: USER cnlab2
FTP       Response: 331 Please specify the password.
FTP       Request: PASS manipal@123
FTP       Response: 230 Login successful.
FTP       Request: SYST
FTP       Response: 215 UNIX Type: L8
FTP       Request: PORT 172,16,59,52,144,234
FTP       Response: 200 PORT command successful. Consider using PASV.
FTP       Request: LIST
FTP       Response: 150 Here comes the directory listing.
FTP       Response: 226 Directory send OK.
FTP       Request: TYPE I
FTP       Response: 200 Switching to Binary mode.
FTP       Request: PORT 172,16,59,52,179,157
FTP       Response: 200 PORT command successful. Consider using PASV.
FTP       Request: STOR COMPUTER_NETWORK_LAB_MANUAL.pdf
FTP       Response: 150 Ok to send data.
FTP       Response: 226 Transfer complete.
```

Avikant Saini, 140905508, CSE-B (43), CP-12

7.3 TELNET packets exchange

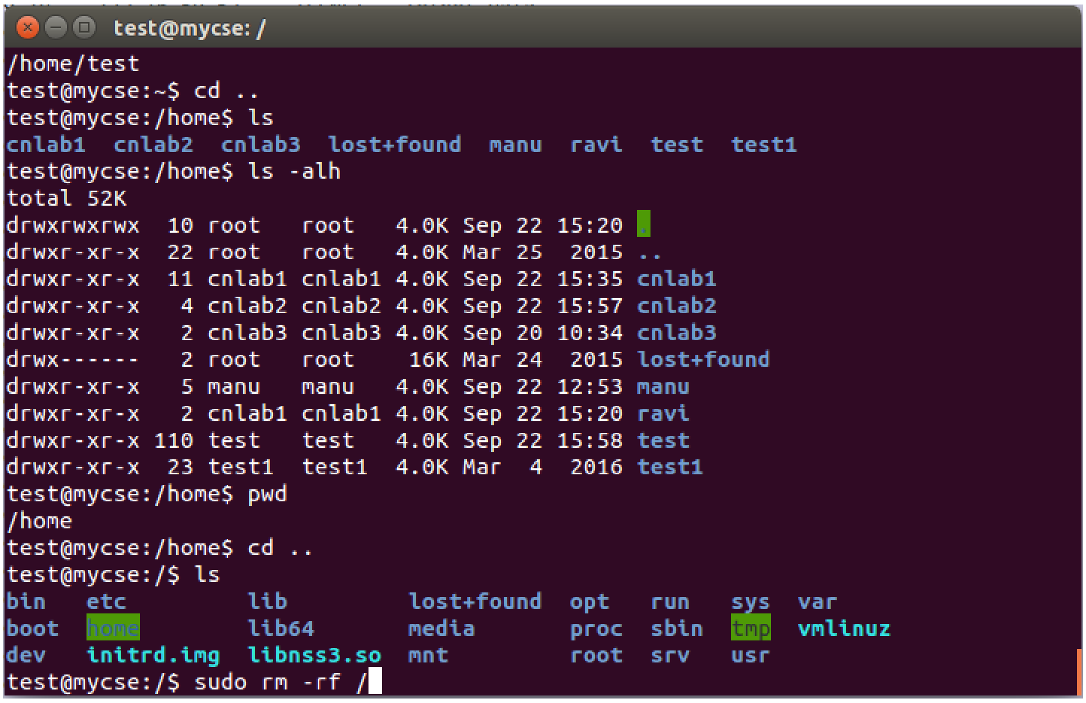


No.	Source	Destination	Protocol	Info
53	172.16.59.52	172.16.59.10	TELNET	Telnet Data ...
55	172.16.59.10	172.16.59.52	TELNET	Telnet Data ...
57	172.16.59.10	172.16.59.52	TELNET	Telnet Data ...
59	172.16.59.52	172.16.59.10	TELNET	Telnet Data ...
60	172.16.59.10	172.16.59.52	TELNET	Telnet Data ...
61	172.16.59.52	172.16.59.10	TELNET	Telnet Data ...
62	172.16.59.10	172.16.59.52	TELNET	Telnet Data ...
63	172.16.59.52	172.16.59.10	TELNET	Telnet Data ...
64	172.16.59.10	172.16.59.52	TELNET	Telnet Data ...
66	172.16.59.10	172.16.59.52	TELNET	Telnet Data ...
179	172.16.59.52	172.16.59.10	TELNET	Telnet Data ...
180	172.16.59.10	172.16.59.52	TELNET	Telnet Data ...
185	172.16.59.52	172.16.59.10	TELNET	Telnet Data ...
186	172.16.59.10	172.16.59.52	TELNET	Telnet Data ...
195	172.16.59.52	172.16.59.10	TELNET	Telnet Data ...
196	172.16.59.10	172.16.59.52	TELNET	Telnet Data ...
198	172.16.59.52	172.16.59.10	TELNET	Telnet Data ...
199	172.16.59.10	172.16.59.52	TELNET	Telnet Data ...
205	172.16.59.52	172.16.59.10	TELNET	Telnet Data ...
206	172.16.59.10	172.16.59.52	TELNET	Telnet Data ...
213	172.16.59.52	172.16.59.10	TELNET	Telnet Data ...
214	172.16.59.10	172.16.59.52	TELNET	Telnet Data ...
217	172.16.59.52	172.16.59.10	TELNET	Telnet Data ...
218	172.16.59.10	172.16.59.52	TELNET	Telnet Data ...
220	172.16.59.10	172.16.59.52	TELNET	Telnet Data ...
227	172.16.59.52	172.16.59.10	TELNET	Telnet Data ...
229	172.16.59.52	172.16.59.10	TELNET	Telnet Data ...
233	172.16.59.52	172.16.59.10	TELNET	Telnet Data ...
242	172.16.59.52	172.16.59.10	TELNET	Telnet Data ...
251	172.16.59.52	172.16.59.10	TELNET	Telnet Data ...
263	172.16.59.52	172.16.59.10	TELNET	Telnet Data ...
266	172.16.59.52	172.16.59.10	TELNET	Telnet Data ...
272	172.16.59.52	172.16.59.10	TELNET	Telnet Data ...
277	172.16.59.52	172.16.59.10	TELNET	Telnet Data ...
286	172.16.59.52	172.16.59.10	TELNET	Telnet Data ...
289	172.16.59.52	172.16.59.10	TELNET	Telnet Data ...
291	172.16.59.52	172.16.59.10	TELNET	Telnet Data ...

55 172.16.59.10 172.16.59.52 TELNET Telnet Data ... 9.769180000 78

```
▶Frame 55: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface
▶Ethernet II, Src: Ibm_d5:0e:ec (34:40:b5:d5:0e:ec), Dst: Giga-Byt_40:73:a5 (00:1f
▶Internet Protocol Version 4, Src: 172.16.59.10 (172.16.59.10), Dst: 172.16.59.52
▼Transmission Control Protocol, Src Port: telnet (23), Dst Port: 45554 (45554), Se
   Source port: telnet (23)
   Destination port: 45554 (45554)
   [Stream index: 0]
   Sequence number: 1    (relative sequence number)
   [Next sequence number: 13    (relative sequence number)]
   Acknowledgment number: 28    (relative ack number)
   Header length: 32 bytes
  ▶Flags: 0x018 (PSH, ACK)
   Window size value: 227
   [Calculated window size: 29056]
   [Window size scaling factor: 128]
  ▶Checksum: 0xd24a [validation disabled]
  ▶Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▶[SEQ/ACK analysis]
▼Telnet
  ▼Do Terminal Type
     Command: Do (253)
     Subcommand: Terminal Type
  ▼Do Terminal Speed
     Command: Do (253)
     Subcommand: Terminal Speed
  ▼Do X Display Location
     Command: Do (253)
     Subcommand: X Display Location
  ▶Do New Environment Option

0010  00 40 fd 8e 40 00 40 06  6e ba ac 10 3b 0a ac 10   .@..@.@. n...;...
0020  3b 34 00 17 b1 f2 01 2b  0f 66 33 f7 76 b3 80 18   ;4.....+ .f3.v...
0030  00 e3 d2 4a 00 00 01 01  08 0a 25 a0 f2 ec 00 18   ...J.... ..%.....
0040  17 ef ff fd 18 ff fd 20  ff fd 23 ff fd 27         ........ ..#..'
```



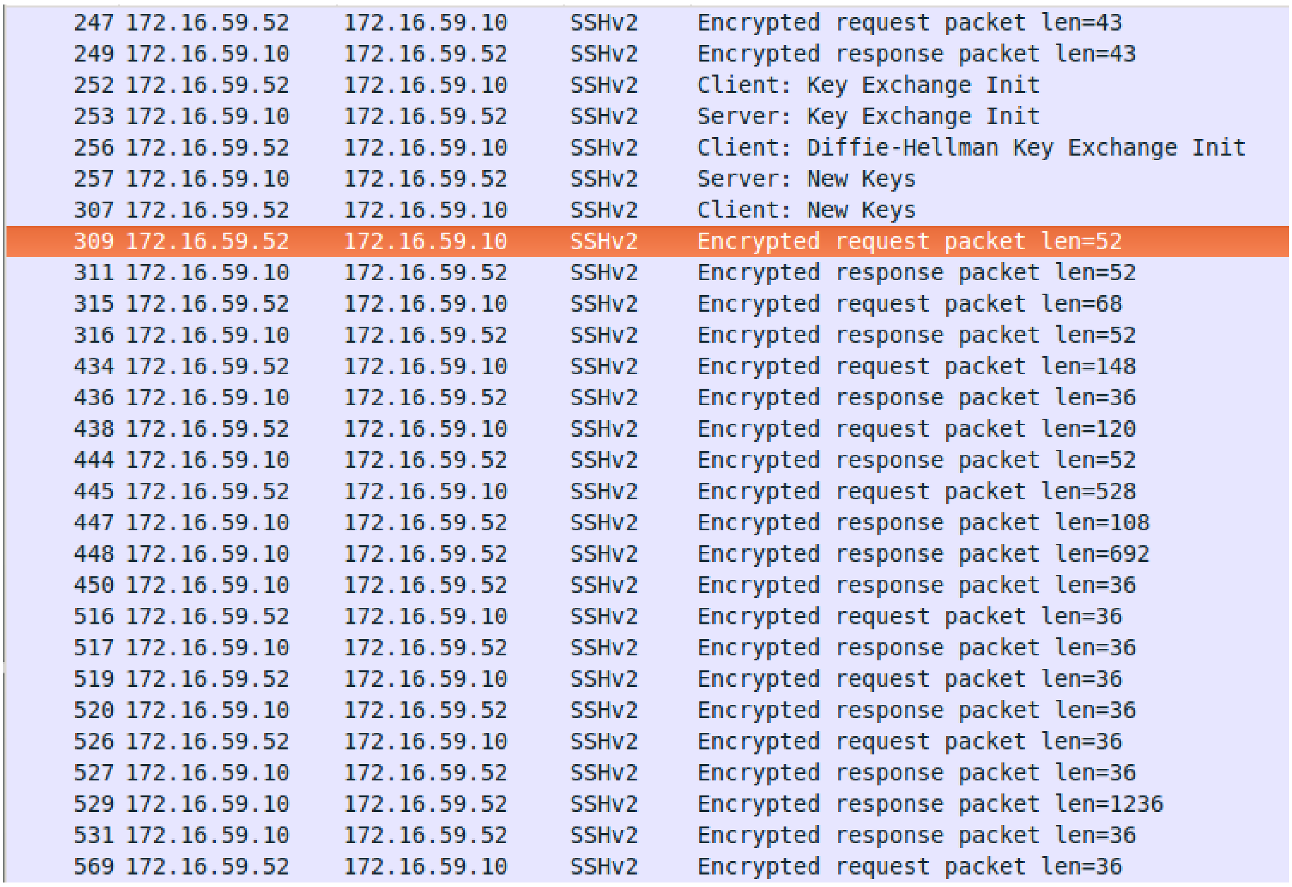
test@mycse: /

```
/home/test
test@mycse:~$ cd ..
test@mycse:/home$ ls
cnlab1  cnlab2  cnlab3  lost+found  manu  ravi  test  test1
test@mycse:/home$ ls -alh
total 52K
drwxrwxrwx  10 root    root    4.0K Sep 22 15:20 .
drwxr-xr-x  22 root    root    4.0K Mar 25  2015 ..
drwxr-xr-x  11 cnlab1 cnlab1 4.0K Sep 22 15:35 cnlab1
drwxr-xr-x   4 cnlab2 cnlab2 4.0K Sep 22 15:57 cnlab2
drwxr-xr-x   2 cnlab3 cnlab3 4.0K Sep 20 10:34 cnlab3
drwx------   2 root    root     16K Mar 24  2015 lost+found
drwxr-xr-x   5 manu    manu    4.0K Sep 22 12:53 manu
drwxr-xr-x   2 cnlab1 cnlab1 4.0K Sep 22 15:20 ravi
drwxr-xr-x 110 test    test    4.0K Sep 22 15:58 test
drwxr-xr-x  23 test1   test1   4.0K Mar  4  2016 test1
test@mycse:/home$ pwd
/home
test@mycse:/home$ cd ..
test@mycse:/$ ls
bin   etc         lib         lost+found  opt   run   sys  var
boot  home        lib64       media       proc  sbin  tmp  vmlinuz
dev   initrd.img  libnss3.so  mnt         root  srv   usr
test@mycse:/$ sudo rm -rf /
```

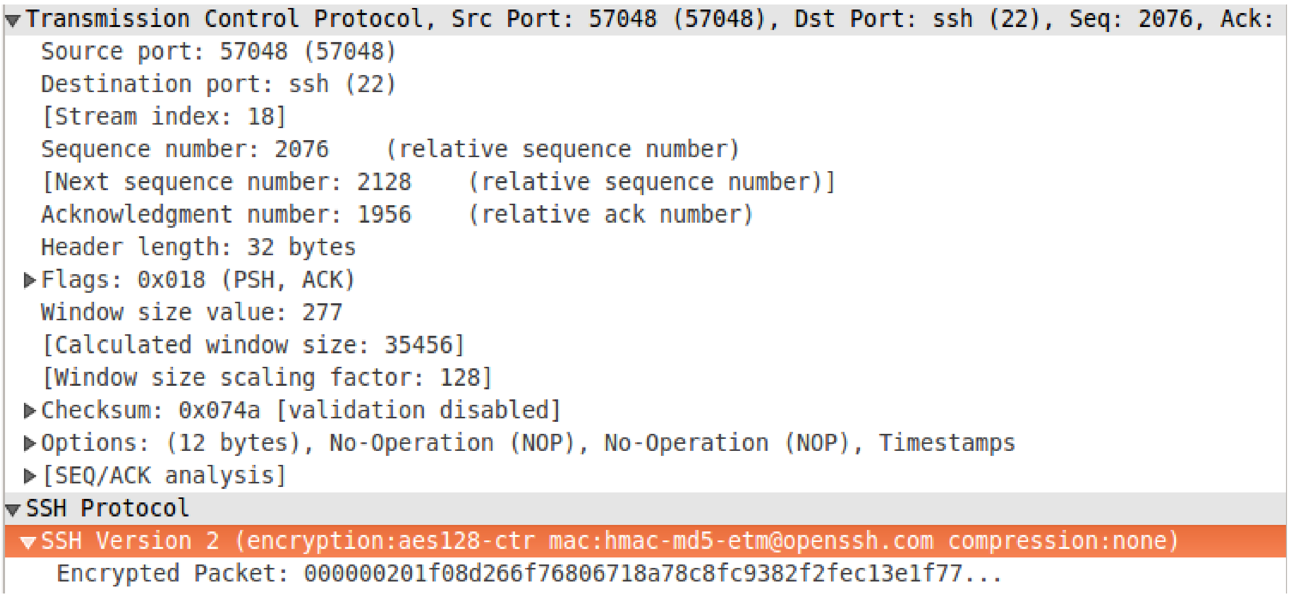
Telnet is insecure, as you can access a remote shell, and execute any command.

TELNET packets are of fixed length, and contain every key and response logged. One can easily snoop in using these, and that's why it's not recommended.

7.4 SSH packets exchange



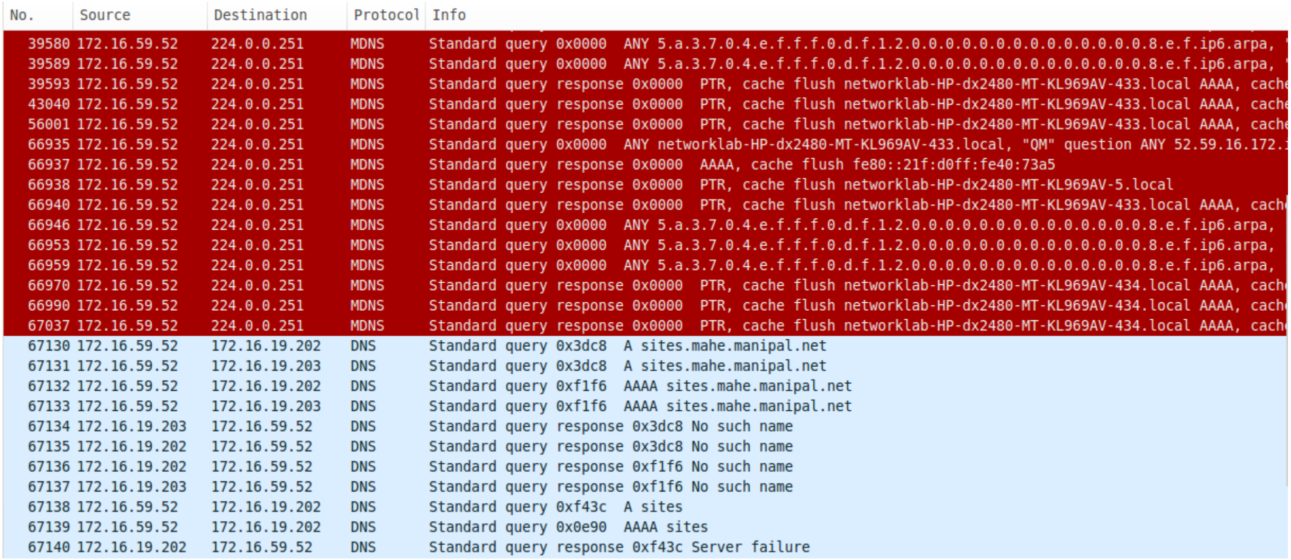
```
247 172.16.59.52   172.16.59.10   SSHv2   Encrypted request packet len=43
249 172.16.59.10   172.16.59.52   SSHv2   Encrypted response packet len=43
252 172.16.59.52   172.16.59.10   SSHv2   Client: Key Exchange Init
253 172.16.59.10   172.16.59.52   SSHv2   Server: Key Exchange Init
256 172.16.59.52   172.16.59.10   SSHv2   Client: Diffie-Hellman Key Exchange Init
257 172.16.59.10   172.16.59.52   SSHv2   Server: New Keys
307 172.16.59.52   172.16.59.10   SSHv2   Client: New Keys
309 172.16.59.52   172.16.59.10   SSHv2   Encrypted request packet len=52
311 172.16.59.10   172.16.59.52   SSHv2   Encrypted response packet len=52
315 172.16.59.52   172.16.59.10   SSHv2   Encrypted request packet len=68
316 172.16.59.10   172.16.59.52   SSHv2   Encrypted response packet len=52
434 172.16.59.52   172.16.59.10   SSHv2   Encrypted request packet len=148
436 172.16.59.10   172.16.59.52   SSHv2   Encrypted response packet len=36
438 172.16.59.52   172.16.59.10   SSHv2   Encrypted request packet len=120
444 172.16.59.10   172.16.59.52   SSHv2   Encrypted response packet len=52
445 172.16.59.52   172.16.59.10   SSHv2   Encrypted request packet len=528
447 172.16.59.10   172.16.59.52   SSHv2   Encrypted response packet len=108
448 172.16.59.10   172.16.59.52   SSHv2   Encrypted response packet len=692
450 172.16.59.10   172.16.59.52   SSHv2   Encrypted response packet len=36
516 172.16.59.52   172.16.59.10   SSHv2   Encrypted request packet len=36
517 172.16.59.10   172.16.59.52   SSHv2   Encrypted response packet len=36
519 172.16.59.52   172.16.59.10   SSHv2   Encrypted request packet len=36
520 172.16.59.10   172.16.59.52   SSHv2   Encrypted response packet len=36
526 172.16.59.52   172.16.59.10   SSHv2   Encrypted request packet len=36
527 172.16.59.10   172.16.59.52   SSHv2   Encrypted response packet len=36
529 172.16.59.10   172.16.59.52   SSHv2   Encrypted response packet len=1236
531 172.16.59.10   172.16.59.52   SSHv2   Encrypted response packet len=36
569 172.16.59.52   172.16.59.10   SSHv2   Encrypted request packet len=36
```



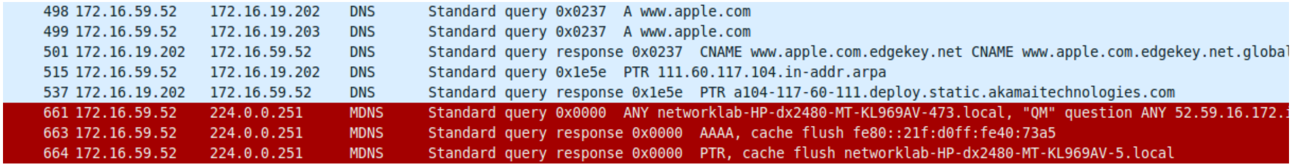
```
▼Transmission Control Protocol, Src Port: 57048 (57048), Dst Port: ssh (22), Seq: 2076, Ack:
   Source port: 57048 (57048)
   Destination port: ssh (22)
   [Stream index: 18]
   Sequence number: 2076    (relative sequence number)
   [Next sequence number: 2128    (relative sequence number)]
   Acknowledgment number: 1956    (relative ack number)
   Header length: 32 bytes
  ▶Flags: 0x018 (PSH, ACK)
   Window size value: 277
   [Calculated window size: 35456]
   [Window size scaling factor: 128]
  ▶Checksum: 0x074a [validation disabled]
  ▶Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▶[SEQ/ACK analysis]
▼SSH Protocol
  ▼SSH Version 2 (encryption:aes128-ctr mac:hmac-md5-etm@openssh.com compression:none)
     Encrypted Packet: 000000201f08d266f76806718a78c8fc9382f2fec13e1f77...
```

SSH is secure, as every bit of data sent through it is encrypted. There's no way for someone to decode that data even after sniffing it.

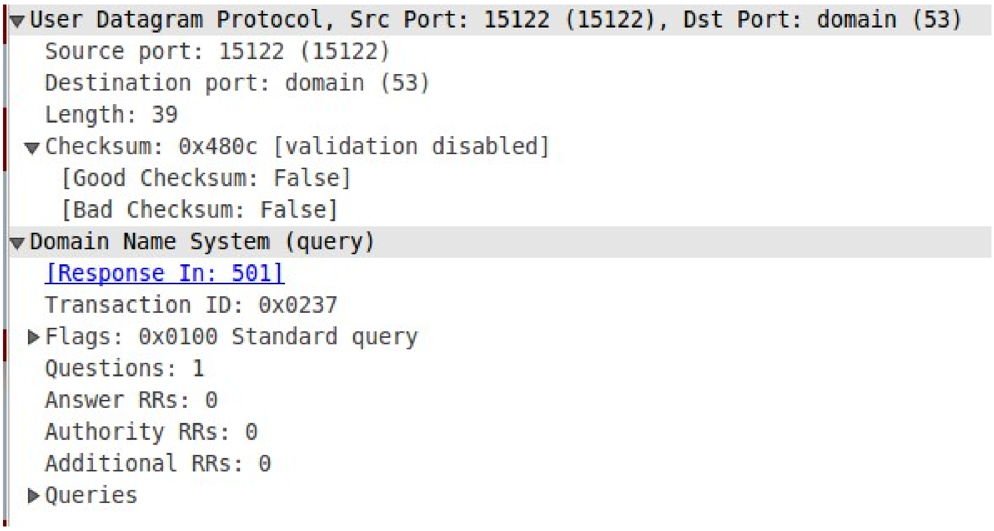
7.7 DNS Lookup



```
No.    Source         Destination    Protocol Info
 39580 172.16.59.52   224.0.0.251    MDNS     Standard query 0x0000  ANY 5.a.3.7.0.4.e.f.f.f.0.d.f.1.2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa, "
 39589 172.16.59.52   224.0.0.251    MDNS     Standard query 0x0000  ANY 5.a.3.7.0.4.e.f.f.f.0.d.f.1.2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa, "
 39593 172.16.59.52   224.0.0.251    MDNS     Standard query response 0x0000  PTR, cache flush networklab-HP-dx2480-MT-KL969AV-433.local AAAA, cache
 43040 172.16.59.52   224.0.0.251    MDNS     Standard query response 0x0000  PTR, cache flush networklab-HP-dx2480-MT-KL969AV-433.local AAAA, cache
 56001 172.16.59.52   224.0.0.251    MDNS     Standard query response 0x0000  PTR, cache flush networklab-HP-dx2480-MT-KL969AV-433.local AAAA, cache
 66935 172.16.59.52   224.0.0.251    MDNS     Standard query 0x0000  ANY networklab-HP-dx2480-MT-KL969AV-433.local, "QM" question ANY 52.59.16.172.i
 66937 172.16.59.52   224.0.0.251    MDNS     Standard query response 0x0000  AAAA, cache flush fe80::21f:d0ff:fe40:73a5
 66938 172.16.59.52   224.0.0.251    MDNS     Standard query response 0x0000  PTR, cache flush networklab-HP-dx2480-MT-KL969AV-5.local
 66940 172.16.59.52   224.0.0.251    MDNS     Standard query response 0x0000  PTR, cache flush networklab-HP-dx2480-MT-KL969AV-433.local AAAA, cach
 66946 172.16.59.52   224.0.0.251    MDNS     Standard query 0x0000  ANY 5.a.3.7.0.4.e.f.f.f.0.d.f.1.2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa,
 66953 172.16.59.52   224.0.0.251    MDNS     Standard query 0x0000  ANY 5.a.3.7.0.4.e.f.f.f.0.d.f.1.2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa,
 66959 172.16.59.52   224.0.0.251    MDNS     Standard query 0x0000  ANY 5.a.3.7.0.4.e.f.f.f.0.d.f.1.2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa,
 66970 172.16.59.52   224.0.0.251    MDNS     Standard query response 0x0000  PTR, cache flush networklab-HP-dx2480-MT-KL969AV-434.local AAAA, cach
 66990 172.16.59.52   224.0.0.251    MDNS     Standard query response 0x0000  PTR, cache flush networklab-HP-dx2480-MT-KL969AV-434.local AAAA, cach
 67037 172.16.59.52   224.0.0.251    MDNS     Standard query response 0x0000  PTR, cache flush networklab-HP-dx2480-MT-KL969AV-434.local AAAA, cach
 67130 172.16.59.52   172.16.19.202  DNS      Standard query 0x3dc8  A sites.mahe.manipal.net
 67131 172.16.59.52   172.16.19.203  DNS      Standard query 0x3dc8  A sites.mahe.manipal.net
 67132 172.16.59.52   172.16.19.202  DNS      Standard query 0xf1f6  AAAA sites.mahe.manipal.net
 67133 172.16.59.52   172.16.19.203  DNS      Standard query 0xf1f6  AAAA sites.mahe.manipal.net
 67134 172.16.19.203  172.16.59.52   DNS      Standard query response 0x3dc8 No such name
 67135 172.16.19.202  172.16.59.52   DNS      Standard query response 0x3dc8 No such name
 67136 172.16.19.202  172.16.59.52   DNS      Standard query response 0xf1f6 No such name
 67137 172.16.19.203  172.16.59.52   DNS      Standard query response 0xf1f6 No such name
 67138 172.16.59.52   172.16.19.202  DNS      Standard query 0xf43c  A sites
 67139 172.16.59.52   172.16.19.202  DNS      Standard query 0x0e90  AAAA sites
 67140 172.16.19.202  172.16.59.52   DNS      Standard query response 0xf43c Server failure
```



```
   498 172.16.59.52   172.16.19.202  DNS      Standard query 0x0237  A www.apple.com
   499 172.16.59.52   172.16.19.203  DNS      Standard query 0x0237  A www.apple.com
   501 172.16.19.202  172.16.59.52   DNS      Standard query response 0x0237  CNAME www.apple.com.edgekey.net CNAME www.apple.com.edgekey.net.global
   515 172.16.59.52   172.16.19.202  DNS      Standard query 0x1e5e  PTR 111.60.117.104.in-addr.arpa
   537 172.16.19.202  172.16.59.52   DNS      Standard query response 0x1e5e  PTR a104-117-60-111.deploy.static.akamaitechnologies.com
   661 172.16.59.52   224.0.0.251    MDNS     Standard query 0x0000  ANY networklab-HP-dx2480-MT-KL969AV-473.local, "QM" question ANY 52.59.16.172.i
   663 172.16.59.52   224.0.0.251    MDNS     Standard query response 0x0000  AAAA, cache flush fe80::21f:d0ff:fe40:73a5
   664 172.16.59.52   224.0.0.251    MDNS     Standard query response 0x0000  PTR, cache flush networklab-HP-dx2480-MT-KL969AV-5.local
```

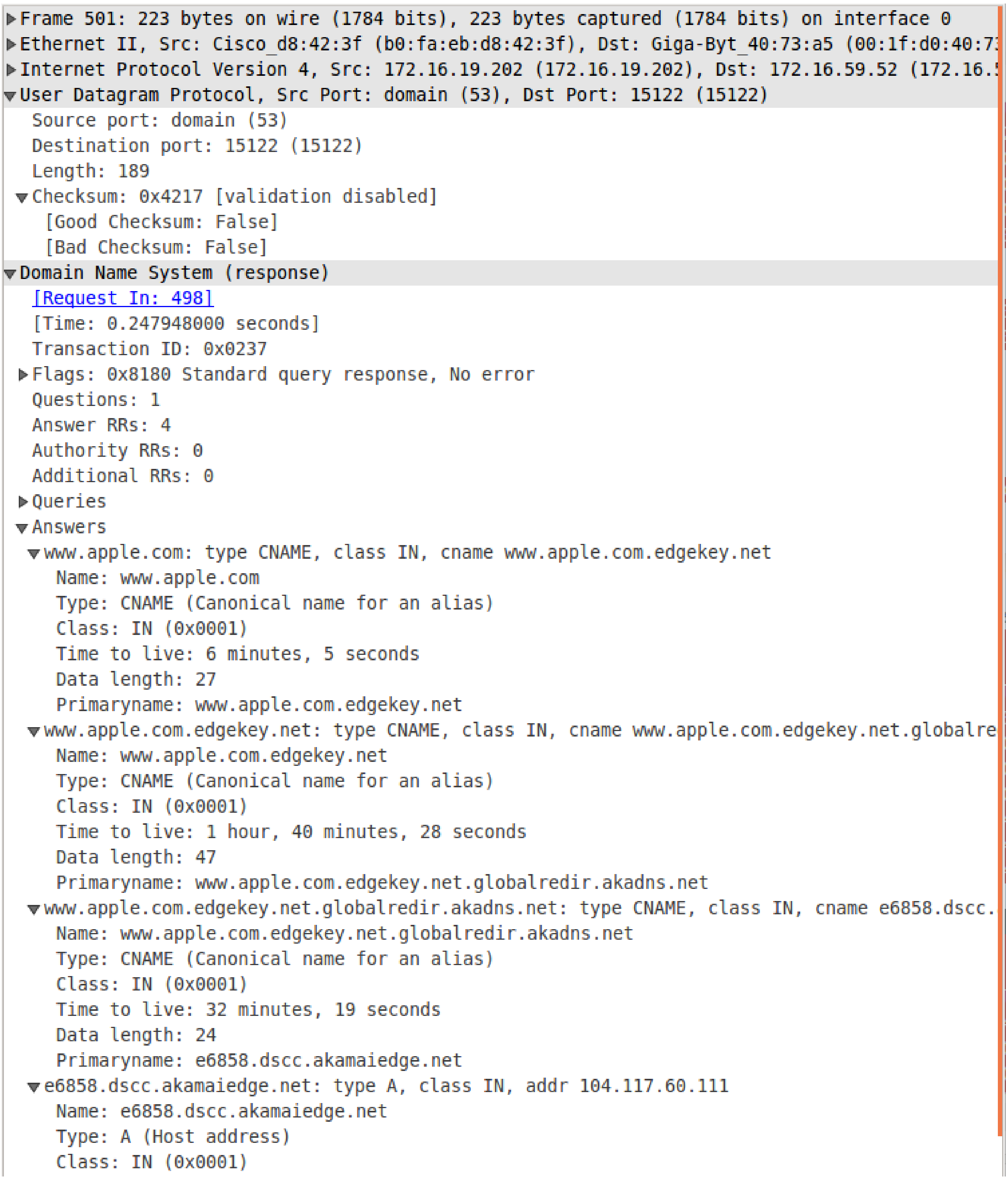


```
▼User Datagram Protocol, Src Port: 15122 (15122), Dst Port: domain (53)
   Source port: 15122 (15122)
   Destination port: domain (53)
   Length: 39
 ▼Checksum: 0x480c [validation disabled]
    [Good Checksum: False]
    [Bad Checksum: False]
▼Domain Name System (query)
   [Response In: 501]
   Transaction ID: 0x0237
 ▶Flags: 0x0100 Standard query
   Questions: 1
   Answer RRs: 0
   Authority RRs: 0
   Additional RRs: 0
 ▶Queries
```

A DNS Lookup query looks like this.

Unlike other protocols dicussed above, DNS works on top of UDP instead of TCP, as the packet sizes are less compared to TCP packets.

Avikant Saini, 140905508, CSE-B (43), CP-12



```
▶Frame 501: 223 bytes on wire (1784 bits), 223 bytes captured (1784 bits) on interface 0
▶Ethernet II, Src: Cisco_d8:42:3f (b0:fa:eb:d8:42:3f), Dst: Giga-Byt_40:73:a5 (00:1f:d0:40:7
▶Internet Protocol Version 4, Src: 172.16.19.202 (172.16.19.202), Dst: 172.16.59.52 (172.16.
▼User Datagram Protocol, Src Port: domain (53), Dst Port: 15122 (15122)
   Source port: domain (53)
   Destination port: 15122 (15122)
   Length: 189
  ▼Checksum: 0x4217 [validation disabled]
     [Good Checksum: False]
     [Bad Checksum: False]
▼Domain Name System (response)
   [Request In: 498]
   [Time: 0.247948000 seconds]
   Transaction ID: 0x0237
  ▶Flags: 0x8180 Standard query response, No error
   Questions: 1
   Answer RRs: 4
   Authority RRs: 0
   Additional RRs: 0
  ▶Queries
  ▼Answers
    ▼www.apple.com: type CNAME, class IN, cname www.apple.com.edgekey.net
       Name: www.apple.com
       Type: CNAME (Canonical name for an alias)
       Class: IN (0x0001)
       Time to live: 6 minutes, 5 seconds
       Data length: 27
       Primaryname: www.apple.com.edgekey.net
    ▼www.apple.com.edgekey.net: type CNAME, class IN, cname www.apple.com.edgekey.net.globalre
       Name: www.apple.com.edgekey.net
       Type: CNAME (Canonical name for an alias)
       Class: IN (0x0001)
       Time to live: 1 hour, 40 minutes, 28 seconds
       Data length: 47
       Primaryname: www.apple.com.edgekey.net.globalredir.akadns.net
    ▼www.apple.com.edgekey.net.globalredir.akadns.net: type CNAME, class IN, cname e6858.dscc.
       Name: www.apple.com.edgekey.net.globalredir.akadns.net
       Type: CNAME (Canonical name for an alias)
       Class: IN (0x0001)
       Time to live: 32 minutes, 19 seconds
       Data length: 24
       Primaryname: e6858.dscc.akamaiedge.net
    ▼e6858.dscc.akamaiedge.net: type A, class IN, addr 104.117.60.111
       Name: e6858.dscc.akamaiedge.net
       Type: A (Host address)
       Class: IN (0x0001)
```

A DNS response looks like this.