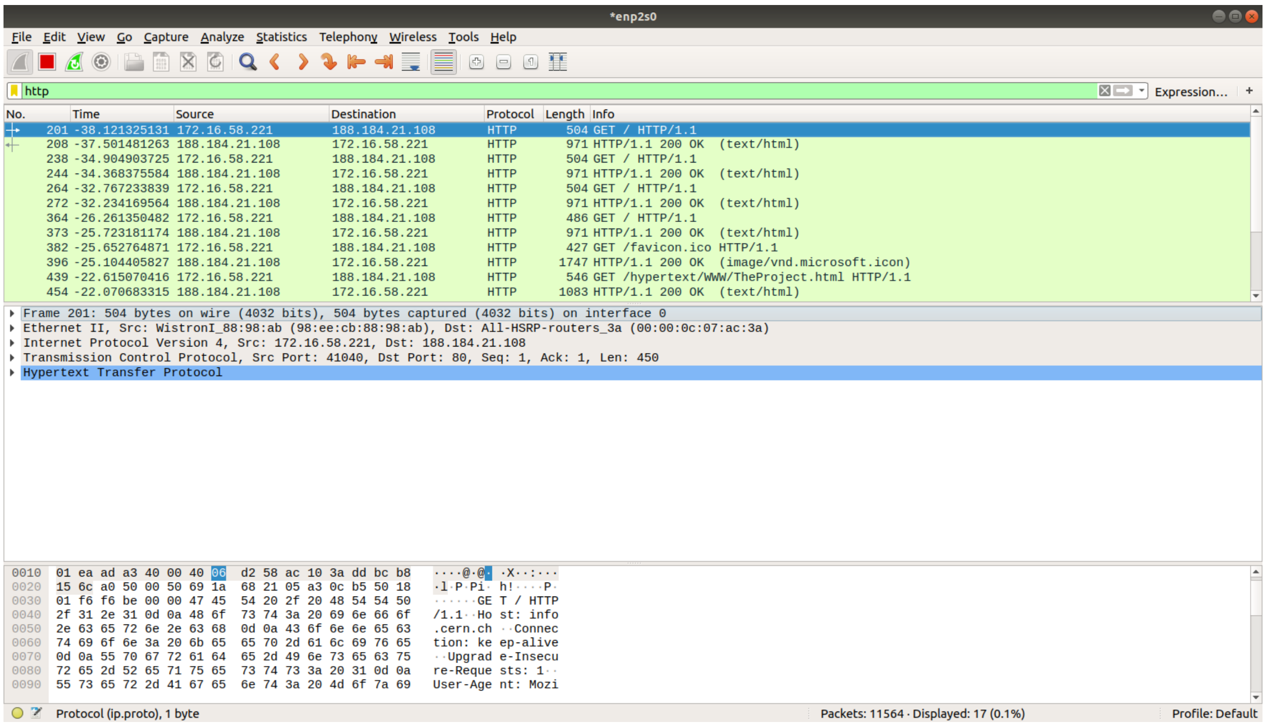
Ayush Goyal
190905522 CSE D Roll 62

Computer Networks Lab 3: Wireshark & GNS3

<u>Part 1: Study of Application Layer Protocols using Wireshark</u>

Q 3.1. Retrieve web pages using HTTP. Use Wireshark to capture packets for analysis. Learn about most common HTTP messages. Also capture response messages and analyze them. During the lab session, also examine and analyze some HTTP headers.

Http request and response packets are as shown below:
First 2 GET and responses give us the home page and the favicon and then the next 2 sets of GET and response are the 2 pages acessed in the website: http://info.cern.ch/


*enp2s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+

```
http
```

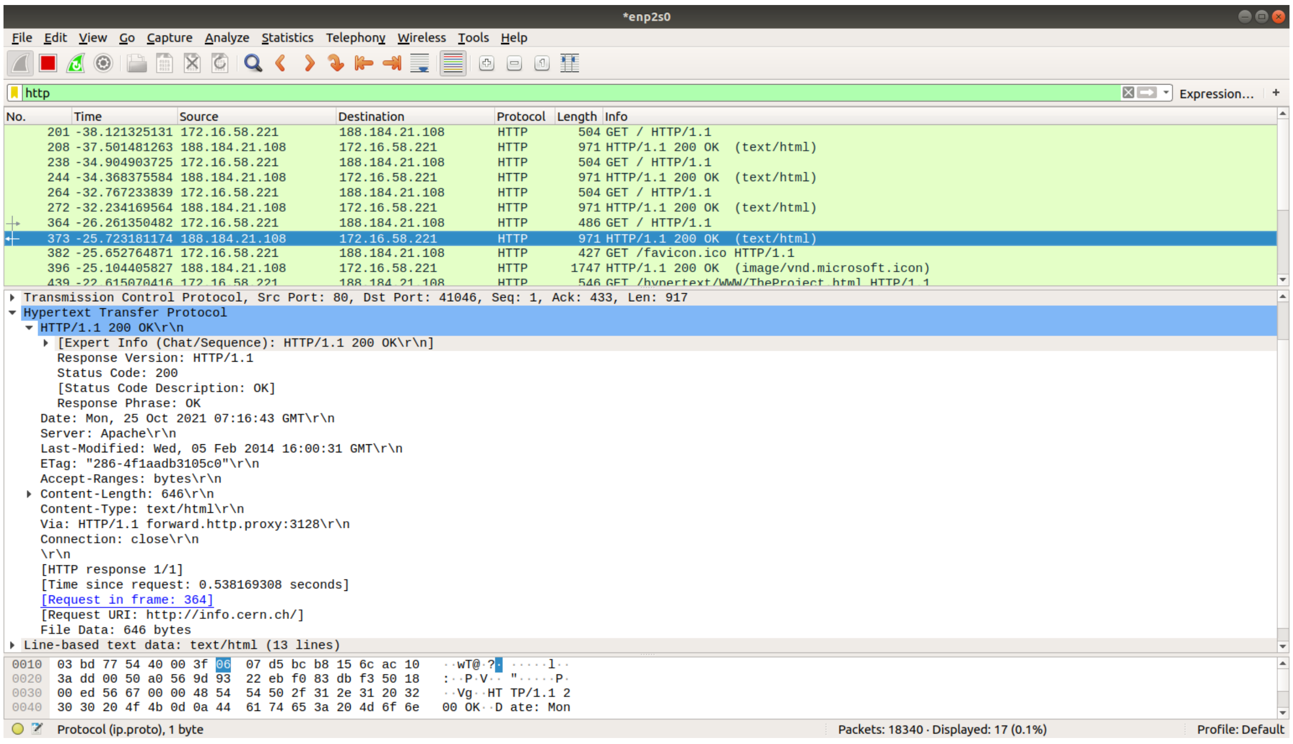
```
No.   Time          Source          Destination     Protocol Length Info
  201 -38.121325131 172.16.58.221   188.184.21.108  HTTP       504 GET / HTTP/1.1
  208 -37.501481263 188.184.21.108  172.16.58.221   HTTP       971 HTTP/1.1 200 OK  (text/html)
  238 -34.904903725 172.16.58.221   188.184.21.108  HTTP       504 GET / HTTP/1.1
  244 -34.368375584 188.184.21.108  172.16.58.221   HTTP       971 HTTP/1.1 200 OK  (text/html)
  264 -32.767233839 172.16.58.221   188.184.21.108  HTTP       504 GET / HTTP/1.1
  272 -32.234169564 188.184.21.108  172.16.58.221   HTTP       971 HTTP/1.1 200 OK  (text/html)
  364 -26.261350482 172.16.58.221   188.184.21.108  HTTP       486 GET / HTTP/1.1
  373 -25.723181174 188.184.21.108  172.16.58.221   HTTP       971 HTTP/1.1 200 OK  (text/html)
  382 -25.652764871 172.16.58.221   188.184.21.108  HTTP       427 GET /favicon.ico HTTP/1.1
  396 -25.104405827 188.184.21.108  172.16.58.221   HTTP      1747 HTTP/1.1 200 OK  (image/vnd.microsoft.icon)
  439 -22.615070416 172.16.58.221   188.184.21.108  HTTP       546 GET /hypertext/WWW/TheProject.html HTTP/1.1
  454 -22.070683315 188.184.21.108  172.16.58.221   HTTP      1083 HTTP/1.1 200 OK  (text/html)
```

```
▸ Frame 201: 504 bytes on wire (4032 bits), 504 bytes captured (4032 bits) on interface 0
▸ Ethernet II, Src: WistronI_88:98:ab (98:ee:cb:88:98:ab), Dst: All-HSRP-routers_3a (00:00:0c:07:ac:3a)
▸ Internet Protocol Version 4, Src: 172.16.58.221, Dst: 188.184.21.108
▸ Transmission Control Protocol, Src Port: 41040, Dst Port: 80, Seq: 1, Ack: 1, Len: 450
▸ Hypertext Transfer Protocol
```

```
0010  01 ea ad a3 40 00 40 06  d2 58 ac 10 3a dd bc b8   ····@·@· ·X··:···
0020  15 6c a0 50 00 50 69 1a  68 21 05 a3 0c b5 50 18   ·l·P·Pi· h!····P·
0030  01 f6 f6 be 00 00 47 45  54 20 2f 20 48 54 54 50   ······GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 69 6e 66 6f   /1.1··Ho st: info
0050  2e 63 65 72 6e 2e 63 68  0d 0a 43 6f 6e 6e 65 63   .cern.ch ··Connec
0060  74 69 6f 6e 3a 20 6b 65  65 70 2d 61 6c 69 76 65   tion: ke ep-alive
0070  0d 0a 55 70 67 72 61 64  65 2d 49 6e 73 65 63 75   ··Upgrad e-Insecu
0080  72 65 2d 52 65 71 75 65  73 74 73 3a 20 31 0d 0a   re-Reque sts: 1··
0090  55 73 65 72 2d 41 67 65  6e 74 3a 20 4d 6f 7a 69   User-Age nt: Mozi
```

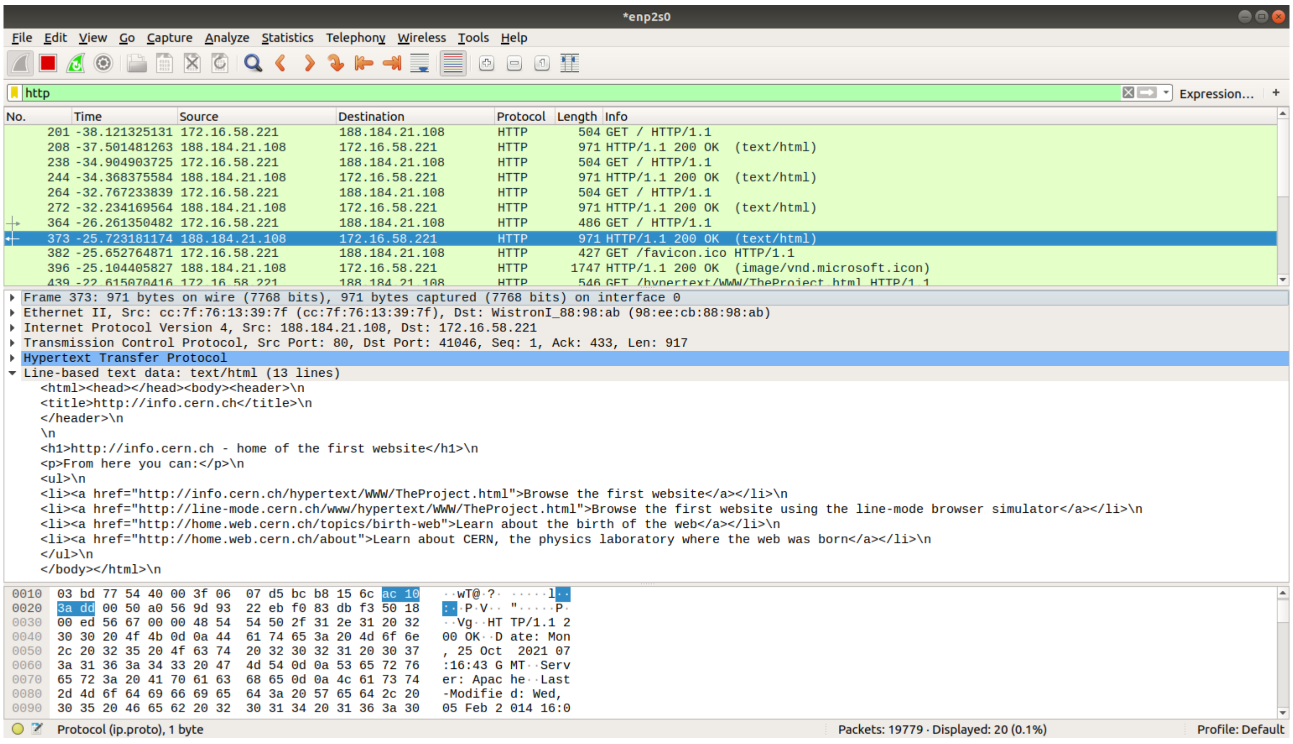
```
Protocol (ip.proto), 1 byte          Packets: 11564 · Displayed: 17 (0.1%)          Profile: Default
```

For the “Project” page the http headers are as shown below:



```
No.  Time           Source          Destination     Protocol Length Info
 201 -38.121325131 172.16.58.221   188.184.21.108   HTTP      504 GET / HTTP/1.1
 208 -37.501481263 188.184.21.108  172.16.58.221    HTTP      971 HTTP/1.1 200 OK  (text/html)
 238 -34.904903725 172.16.58.221   188.184.21.108   HTTP      504 GET / HTTP/1.1
 244 -34.368375584 188.184.21.108  172.16.58.221    HTTP      971 HTTP/1.1 200 OK  (text/html)
 264 -32.767233839 172.16.58.221   188.184.21.108   HTTP      504 GET / HTTP/1.1
 272 -32.234169564 188.184.21.108  172.16.58.221    HTTP      971 HTTP/1.1 200 OK  (text/html)
 364 -26.261350482 172.16.58.221   188.184.21.108   HTTP      486 GET / HTTP/1.1
 373 -25.723181174 188.184.21.108  172.16.58.221    HTTP      971 HTTP/1.1 200 OK  (text/html)
 382 -25.652764871 172.16.58.221   188.184.21.108   HTTP      427 GET /favicon.ico HTTP/1.1
 396 -25.104405827 188.184.21.108  172.16.58.221    HTTP     1747 HTTP/1.1 200 OK  (image/vnd.microsoft.icon)
 439 -22.615070416 172.16.58.221   188.184.21.108   HTTP      546 GET /hypertext/WWW/TheProject.html HTTP/1.1

▸ Transmission Control Protocol, Src Port: 80, Dst Port: 41046, Seq: 1, Ack: 433, Len: 917
▾ Hypertext Transfer Protocol
  ▾ HTTP/1.1 200 OK\r\n
    ▸ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Mon, 25 Oct 2021 07:16:43 GMT\r\n
    Server: Apache\r\n
    Last-Modified: Wed, 05 Feb 2014 16:00:31 GMT\r\n
    ETag: "286-4f1aadb3105c0"\r\n
    Accept-Ranges: bytes\r\n
  ▸ Content-Length: 646\r\n
    Content-Type: text/html\r\n
    Via: HTTP/1.1 forward.http.proxy:3128\r\n
    Connection: close\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.538169308 seconds]
    [Request in frame: 364]
    [Request URI: http://info.cern.ch/]
    File Data: 646 bytes
▸ Line-based text data: text/html (13 lines)

0010  03 bd 77 54 40 00 3f 06  07 d5 bc b8 15 6c ac 10   ··wT@·?· ·····l··
0020  3a dd 00 50 a0 56 9d 93  22 eb f0 83 db f3 50 18   :··P·V·· "·····P·
0030  00 ed 56 67 00 00 48 54  54 50 2f 31 2e 31 20 32   ··Vg··HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 4d 6f 6e   00 OK··D ate: Mon

Protocol (ip.proto), 1 byte          Packets: 18340 · Displayed: 17 (0.1%)          Profile: Default
```

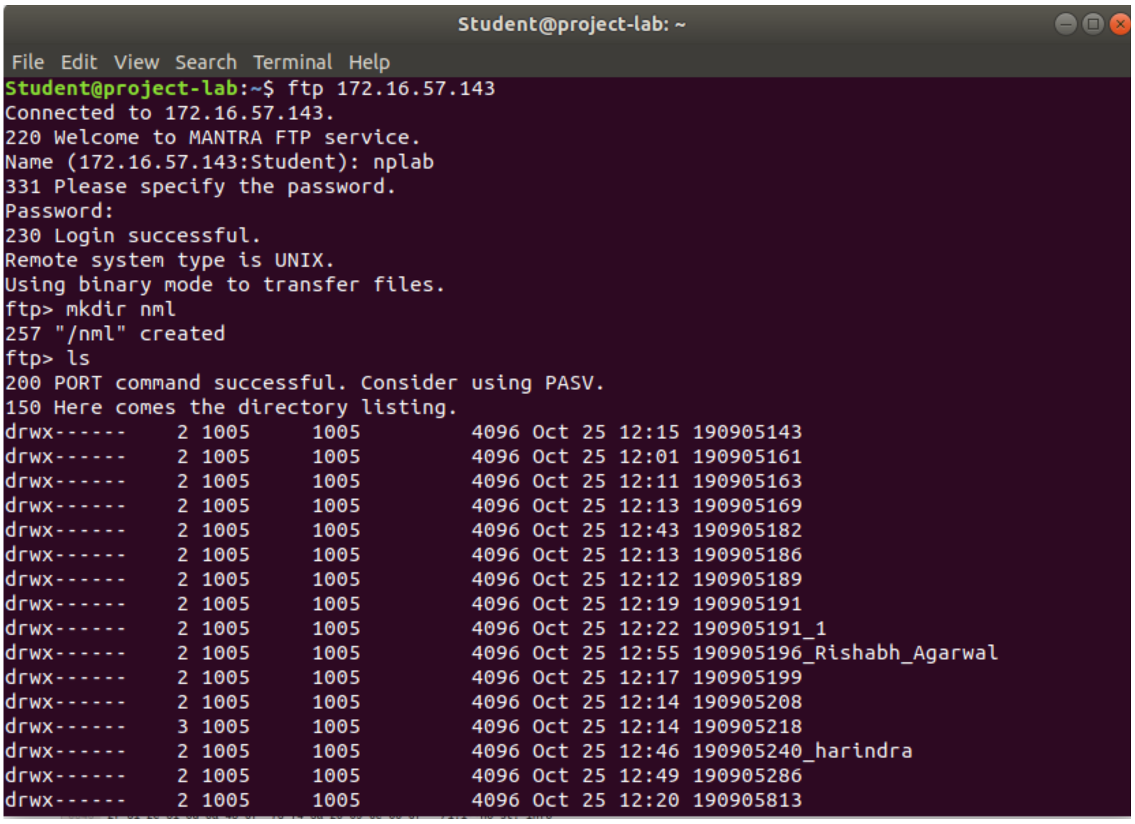
Http response for the "Project" i.e., the HTML document snippet is shown as below in the screenshot:



```
No.  Time           Source          Destination     Protocol Length Info
 201 -38.121325131 172.16.58.221   188.184.21.108   HTTP      504 GET / HTTP/1.1
 208 -37.501481263 188.184.21.108  172.16.58.221    HTTP      971 HTTP/1.1 200 OK  (text/html)
 238 -34.904903725 172.16.58.221   188.184.21.108   HTTP      504 GET / HTTP/1.1
 244 -34.368375584 188.184.21.108  172.16.58.221    HTTP      971 HTTP/1.1 200 OK  (text/html)
 264 -32.767233839 172.16.58.221   188.184.21.108   HTTP      504 GET / HTTP/1.1
 272 -32.234169564 188.184.21.108  172.16.58.221    HTTP      971 HTTP/1.1 200 OK  (text/html)
 364 -26.261350482 172.16.58.221   188.184.21.108   HTTP      486 GET / HTTP/1.1
 373 -25.723181174 188.184.21.108  172.16.58.221    HTTP      971 HTTP/1.1 200 OK  (text/html)
 382 -25.652764871 172.16.58.221   188.184.21.108   HTTP      427 GET /favicon.ico HTTP/1.1
 396 -25.104405827 188.184.21.108  172.16.58.221    HTTP     1747 HTTP/1.1 200 OK  (image/vnd.microsoft.icon)
 439 -22.615070416 172.16.58.221   188.184.21.108   HTTP      546 GET /hypertext/WWW/TheProject.html HTTP/1.1

▸ Frame 373: 971 bytes on wire (7768 bits), 971 bytes captured (7768 bits) on interface 0
▸ Ethernet II, Src: cc:7f:76:13:39:7f (cc:7f:76:13:39:7f), Dst: WistronI_88:98:ab (98:ee:cb:88:98:ab)
▸ Internet Protocol Version 4, Src: 188.184.21.108, Dst: 172.16.58.221
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 41046, Seq: 1, Ack: 433, Len: 917
▸ Hypertext Transfer Protocol
▾ Line-based text data: text/html (13 lines)
    <html><head></head><body><header>\n
    <title>http://info.cern.ch</title>\n
    </header>\n
    \n
    <h1>http://info.cern.ch - home of the first website</h1>\n
    <p>From here you can:</p>\n
    <ul>\n
    <li><a href="http://info.cern.ch/hypertext/WWW/TheProject.html">Browse the first website</a></li>\n
    <li><a href="http://line-mode.cern.ch/www/hypertext/WWW/TheProject.html">Browse the first website using the line-mode browser simulator</a></li>\n
    <li><a href="http://home.web.cern.ch/topics/birth-web">Learn about the birth of the web</a></li>\n
    <li><a href="http://home.web.cern.ch/about">Learn about CERN, the physics laboratory where the web was born</a></li>\n
    </ul>\n
    </body></html>\n

0010  03 bd 77 54 40 00 3f 06  07 d5 bc b8 15 6c ac 10   ··wT@·?· ·····l··
0020  3a dd 00 50 a0 56 9d 93  22 eb f0 83 db f3 50 18   :··P·V·· "·····P·
0030  00 ed 56 67 00 00 48 54  54 50 2f 31 2e 31 20 32   ··Vg··HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 4d 6f 6e   00 OK··D ate: Mon
0050  2c 20 32 35 20 4f 63 74  20 32 30 32 31 20 30 37   , 25 Oct  2021 07
0060  3a 31 36 3a 34 33 20 47  4d 54 0d 0a 53 65 72 76   :16:43 G MT··Serv
0070  65 72 3a 20 41 70 61 63  68 65 0d 0a 4c 61 73 74   er: Apac he··Last
0080  2d 4d 6f 64 69 66 69 65  64 3a 20 57 65 64 2c 20   -Modifie d: Wed,
0090  30 35 20 46 65 62 20 32  30 31 34 20 31 36 3a 30   05 Feb 2 014 16:0

Protocol (ip.proto), 1 byte          Packets: 19779 · Displayed: 20 (0.1%)          Profile: Default
```

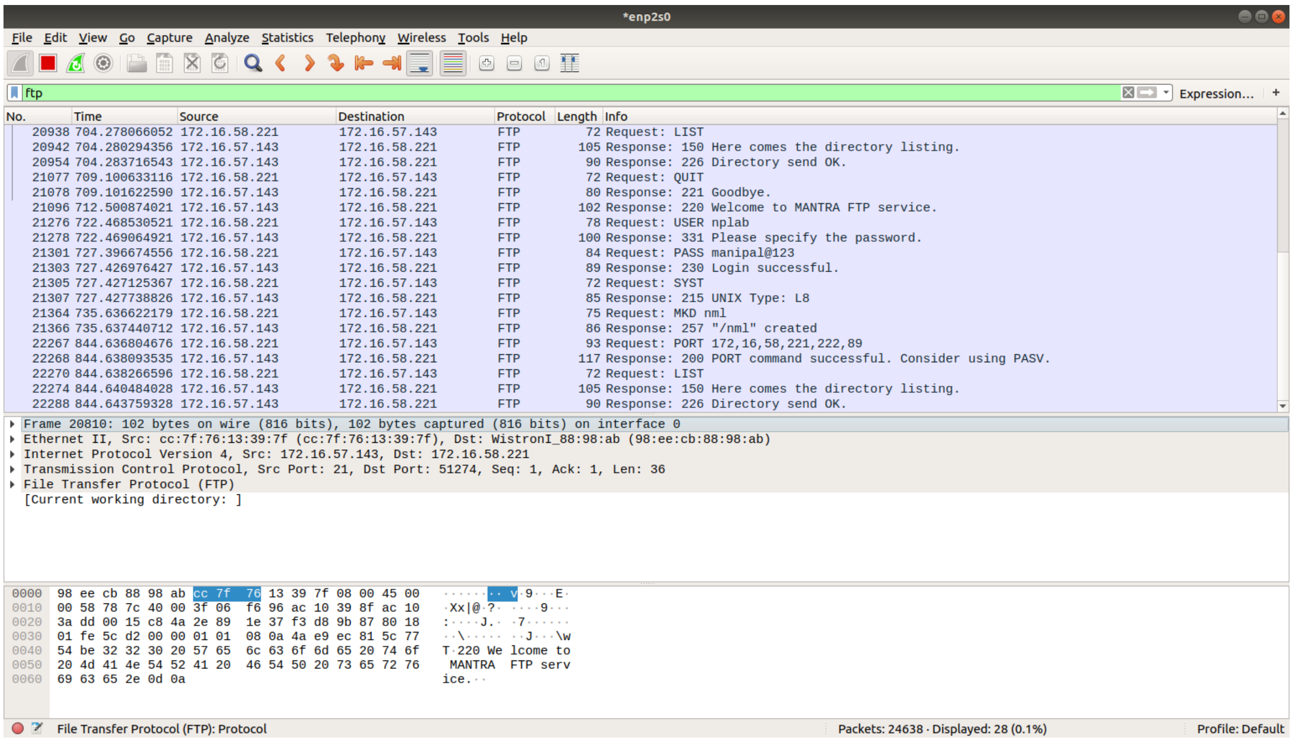
Q 3.2. Use FTP to transfer some files, Use Wireshark to capture some packets. Show that FTP uses two separate connections: a control connection and a data-transfer connection. The data connection is opened and closed for each file transfer activity. Also show that FTP is an insecure file transfer protocol because the transaction is done in plaintext.

We access FTP via terminal and execute commands as shown below:



```
Student@project-lab:~$ ftp 172.16.57.143
Connected to 172.16.57.143.
220 Welcome to MANTRA FTP service.
Name (172.16.57.143:Student): nplab
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> mkdir nml
257 "/nml" created
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwx------    2 1005     1005         4096 Oct 25 12:15 190905143
drwx------    2 1005     1005         4096 Oct 25 12:01 190905161
drwx------    2 1005     1005         4096 Oct 25 12:11 190905163
drwx------    2 1005     1005         4096 Oct 25 12:13 190905169
drwx------    2 1005     1005         4096 Oct 25 12:43 190905182
drwx------    2 1005     1005         4096 Oct 25 12:13 190905186
drwx------    2 1005     1005         4096 Oct 25 12:12 190905189
drwx------    2 1005     1005         4096 Oct 25 12:19 190905191
drwx------    2 1005     1005         4096 Oct 25 12:22 190905191_1
drwx------    2 1005     1005         4096 Oct 25 12:55 190905196_Rishabh_Agarwal
drwx------    2 1005     1005         4096 Oct 25 12:17 190905199
drwx------    2 1005     1005         4096 Oct 25 12:14 190905208
drwx------    3 1005     1005         4096 Oct 25 12:14 190905218
drwx------    2 1005     1005         4096 Oct 25 12:46 190905240_harindra
drwx------    2 1005     1005         4096 Oct 25 12:49 190905286
drwx------    2 1005     1005         4096 Oct 25 12:20 190905813
```

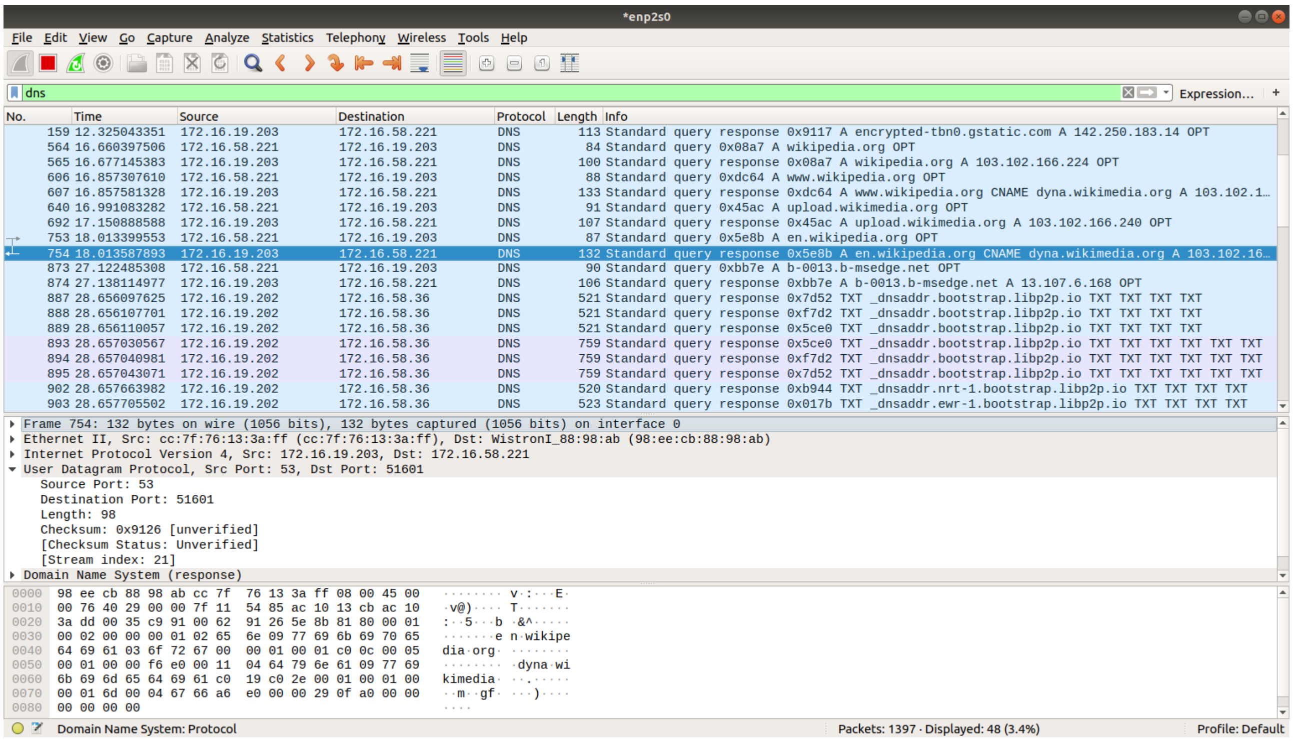
In FTP protocol we see the initial welcome message as ResponseWe see the username and password being askedNote that the password manipal@123is sent as plaintext and hence FTP is not a secure transfer protocol.A SYST request is sent when ls command is executed.


*enp2s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ftp
Expression…

```
No.   Time         Source         Destination    Protocol Length Info
20938 704.278066052 172.16.58.221 172.16.57.143  FTP      72 Request: LIST
20942 704.280294356 172.16.57.143 172.16.58.221  FTP     105 Response: 150 Here comes the directory listing.
20954 704.283716543 172.16.57.143 172.16.58.221  FTP      90 Response: 226 Directory send OK.
21077 709.100633116 172.16.58.221 172.16.57.143  FTP      72 Request: QUIT
21078 709.101622590 172.16.57.143 172.16.58.221  FTP      80 Response: 221 Goodbye.
21096 712.500874021 172.16.57.143 172.16.58.221  FTP     102 Response: 220 Welcome to MANTRA FTP service.
21276 722.468530521 172.16.58.221 172.16.57.143  FTP      78 Request: USER nplab
21278 722.469064921 172.16.57.143 172.16.58.221  FTP     100 Response: 331 Please specify the password.
21301 727.396674556 172.16.58.221 172.16.57.143  FTP      84 Request: PASS manipal@123
21303 727.426976427 172.16.57.143 172.16.58.221  FTP      89 Response: 230 Login successful.
21305 727.427125367 172.16.58.221 172.16.57.143  FTP      72 Request: SYST
21307 727.427738826 172.16.57.143 172.16.58.221  FTP      85 Response: 215 UNIX Type: L8
21364 735.636622179 172.16.58.221 172.16.57.143  FTP      75 Request: MKD nml
21366 735.637440712 172.16.57.143 172.16.58.221  FTP      86 Response: 257 "/nml" created
22267 844.636804676 172.16.58.221 172.16.57.143  FTP      93 Request: PORT 172,16,58,221,222,89
22268 844.638093535 172.16.57.143 172.16.58.221  FTP     117 Response: 200 PORT command successful. Consider using PASV.
22270 844.638266596 172.16.58.221 172.16.57.143  FTP      72 Request: LIST
22274 844.640484028 172.16.57.143 172.16.58.221  FTP     105 Response: 150 Here comes the directory listing.
22288 844.643759328 172.16.57.143 172.16.58.221  FTP      90 Response: 226 Directory send OK.

▸ Frame 20810: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0
▸ Ethernet II, Src: cc:7f:76:13:39:7f (cc:7f:76:13:39:7f), Dst: WistronI_88:98:ab (98:ee:cb:88:98:ab)
▸ Internet Protocol Version 4, Src: 172.16.57.143, Dst: 172.16.58.221
▸ Transmission Control Protocol, Src Port: 21, Dst Port: 51274, Seq: 1, Ack: 1, Len: 36
▸ File Transfer Protocol (FTP)
  [Current working directory: ]

0000  98 ee cb 88 98 ab cc 7f  76 13 39 7f 08 00 45 00   ······· v·9···E·
0010  00 58 78 7c 40 00 3f 06  f6 96 ac 10 39 8f ac 10   ·Xx|@·?· ····9···
0020  3a dd 00 15 c8 4a 2e 89  1e 37 f3 d8 9b 87 80 18   :····J.· ·7······
0030  01 fe 5c d2 00 00 01 01  08 0a 4a e9 ec 81 5c 77   ··\····· ··J···\w
0040  54 be 32 32 30 20 57 65  6c 63 6f 6d 65 20 74 6f   T·220 We lcome to
0050  20 4d 41 4e 54 52 41 20  46 54 50 20 73 65 72 76    MANTRA  FTP serv
0060  69 63 65 2e 0d 0a                                  ice.··

File Transfer Protocol (FTP): Protocol        Packets: 24638 · Displayed: 28 (0.1%)        Profile: Default
```

Q 3.3. Analyze the behavior of the DNS protocol. In addition to Wireshark [Several network utilities are available for finding some information stored in the DNS servers. Eg.dig utilities (which has replaced nslookup). Set Wireshark to capture the packets sent by this utility.]

Analyzing the DNS protocol when a request for www.wikipedia.orgis made. As seen in the image below, DNS uses the UDP protocol in the transport layer. The source port for the UDP protocol is 53 and the destination port is 51601. The request is sent from source address 172.16.19.203 to destination address 172.16.58.221.



```
*enp2s0
dns

No.  Time          Source         Destination    Protocol Length Info
 159 12.325043351  172.16.19.203  172.16.58.221  DNS      113 Standard query response 0x9117 A encrypted-tbn0.gstatic.com A 142.250.183.14 OPT
 564 16.660397506  172.16.58.221  172.16.19.203  DNS       84 Standard query 0x08a7 A wikipedia.org OPT
 565 16.677145383  172.16.19.203  172.16.58.221  DNS      100 Standard query response 0x08a7 A wikipedia.org A 103.102.166.224 OPT
 606 16.857307610  172.16.58.221  172.16.19.203  DNS       88 Standard query 0xdc64 A www.wikipedia.org OPT
 607 16.857581328  172.16.19.203  172.16.58.221  DNS      133 Standard query response 0xdc64 A www.wikipedia.org CNAME dyna.wikimedia.org A 103.102.1…
 640 16.991083282  172.16.58.221  172.16.19.203  DNS       91 Standard query 0x45ac A upload.wikimedia.org OPT
 692 17.150888588  172.16.19.203  172.16.58.221  DNS      107 Standard query response 0x45ac A upload.wikimedia.org A 103.102.166.240 OPT
 753 18.013399553  172.16.58.221  172.16.19.203  DNS       87 Standard query 0x5e8b A en.wikipedia.org OPT
 754 18.013587893  172.16.19.203  172.16.58.221  DNS      132 Standard query response 0x5e8b A en.wikipedia.org CNAME dyna.wikimedia.org A 103.102.16…
 873 27.122485308  172.16.58.221  172.16.19.203  DNS       90 Standard query 0xbb7e A b-0013.b-msedge.net OPT
 874 27.138114977  172.16.19.203  172.16.58.221  DNS      106 Standard query response 0xbb7e A b-0013.b-msedge.net A 13.107.6.168 OPT
 887 28.656097625  172.16.19.202  172.16.58.36   DNS      521 Standard query response 0x7d52 TXT _dnsaddr.bootstrap.libp2p.io TXT TXT TXT TXT
 888 28.656107701  172.16.19.202  172.16.58.36   DNS      521 Standard query response 0xf7d2 TXT _dnsaddr.bootstrap.libp2p.io TXT TXT TXT TXT
 889 28.656110057  172.16.19.202  172.16.58.36   DNS      521 Standard query response 0x5ce0 TXT _dnsaddr.bootstrap.libp2p.io TXT TXT TXT TXT
 893 28.657030567  172.16.19.202  172.16.58.36   DNS      759 Standard query response 0x5ce0 TXT _dnsaddr.bootstrap.libp2p.io TXT TXT TXT TXT TXT TXT
 894 28.657040981  172.16.19.202  172.16.58.36   DNS      759 Standard query response 0xf7d2 TXT _dnsaddr.bootstrap.libp2p.io TXT TXT TXT TXT TXT TXT
 895 28.657043071  172.16.19.202  172.16.58.36   DNS      759 Standard query response 0x7d52 TXT _dnsaddr.bootstrap.libp2p.io TXT TXT TXT TXT TXT TXT
 902 28.657663982  172.16.19.202  172.16.58.36   DNS      520 Standard query response 0xb944 TXT _dnsaddr.nrt-1.bootstrap.libp2p.io TXT TXT TXT TXT
 903 28.657705502  172.16.19.202  172.16.58.36   DNS      523 Standard query response 0x017b TXT _dnsaddr.ewr-1.bootstrap.libp2p.io TXT TXT TXT TXT

▸ Frame 754: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits) on interface 0
▸ Ethernet II, Src: cc:7f:76:13:3a:ff (cc:7f:76:13:3a:ff), Dst: WistronI_88:98:ab (98:ee:cb:88:98:ab)
▸ Internet Protocol Version 4, Src: 172.16.19.203, Dst: 172.16.58.221
▾ User Datagram Protocol, Src Port: 53, Dst Port: 51601
    Source Port: 53
    Destination Port: 51601
    Length: 98
    Checksum: 0x9126 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 21]
▸ Domain Name System (response)

0000  98 ee cb 88 98 ab cc 7f  76 13 3a ff 08 00 45 00   ········ v·:···E·
0010  00 76 40 29 00 00 7f 11  54 85 ac 10 13 cb ac 10   ·v@)···· T·······
0020  3a dd 00 35 c9 91 00 62  91 26 5e 8b 81 80 00 01   :··5···b ·&^·····
0030  00 02 00 00 00 01 02 65  6e 09 77 69 6b 69 70 65   ·······e n·wikipe
0040  64 69 61 03 6f 72 67 00  00 01 00 01 c0 0c 00 05   dia·org· ········
0050  00 01 00 00 f6 e0 00 11  04 64 79 6e 61 09 77 69   ········ ·dyna·wi
0060  6b 69 6d 65 64 69 61 c0  19 c0 2e 00 01 00 01 00   kimedia· ·.······
0070  00 01 6d 00 04 67 66 a6  e0 00 00 29 0f a0 00 00   ··m··gf· ···)····
0080  00 00 00 00                                        ····

Domain Name System: Protocol          Packets: 1397 · Displayed: 48 (3.4%)          Profile: Default
```

We see the DNS request being made to resolve the Url to actual address. Note that we use UDP and not TCP for DNS. We note that in the response the A entry i.e., the address is shown.

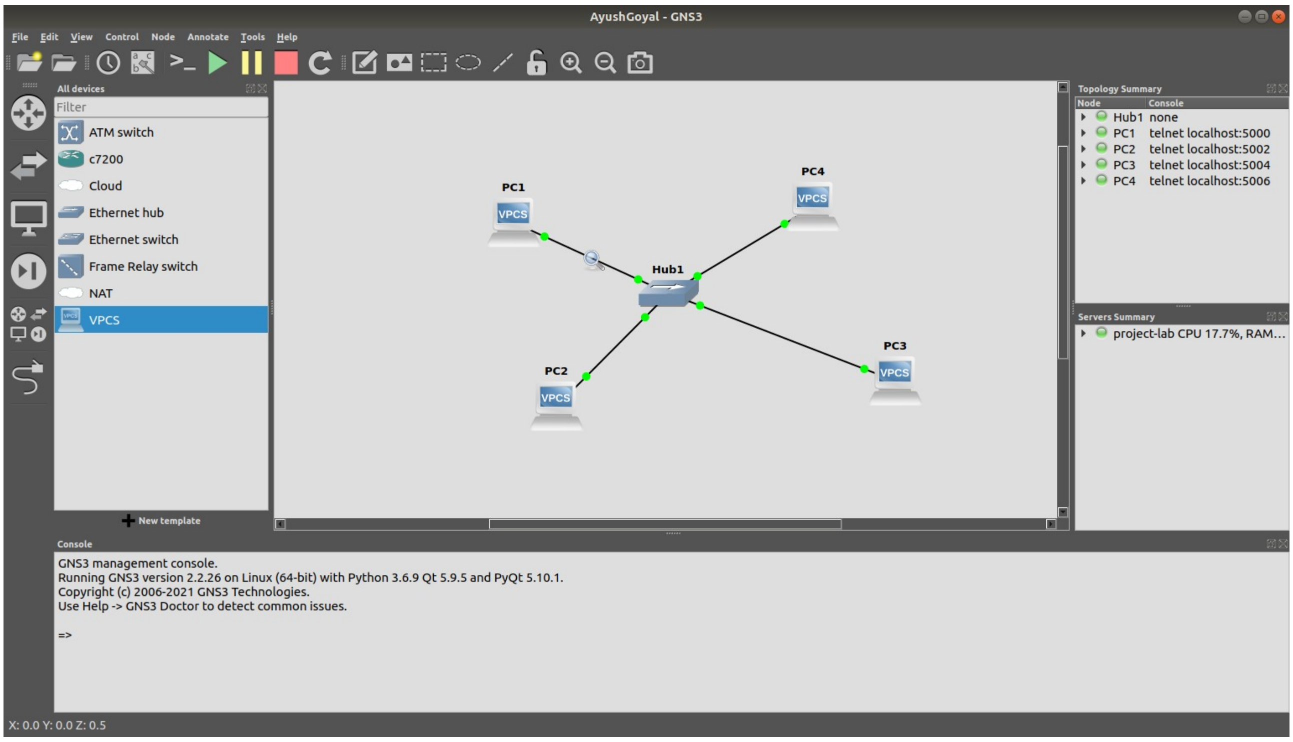
Part 2: Study of Network Devices in GNS3

Q 4.1 (a,b,c,d,e) and Q 4.3

Design network configuration shown in Figure 4.1 for all parts. Connect all four VMs to a single Ethernet segment via a single hub as shown in Figure 4.1. Configure the IP addresses for the PCs as shown in Table 4.1.
a. On PC1, view the ARP cache with showarp

b. Start Wireshark on PC1-Hub1 link with a capture filter set to the IP address ofPC2.
c. Issue a ping command from PC1toPC2:
PC1% ping 10.0.1.13 –c3
Observe the ARP packets in the Wireshark window. Explore the MAC addresses in the Ethernet headers of the captured packets.
Direct our attention to the following fields:
• The destination MAC address of the ARP Request packets.
• The Type Field in the Ethernet headers of ARP packets.

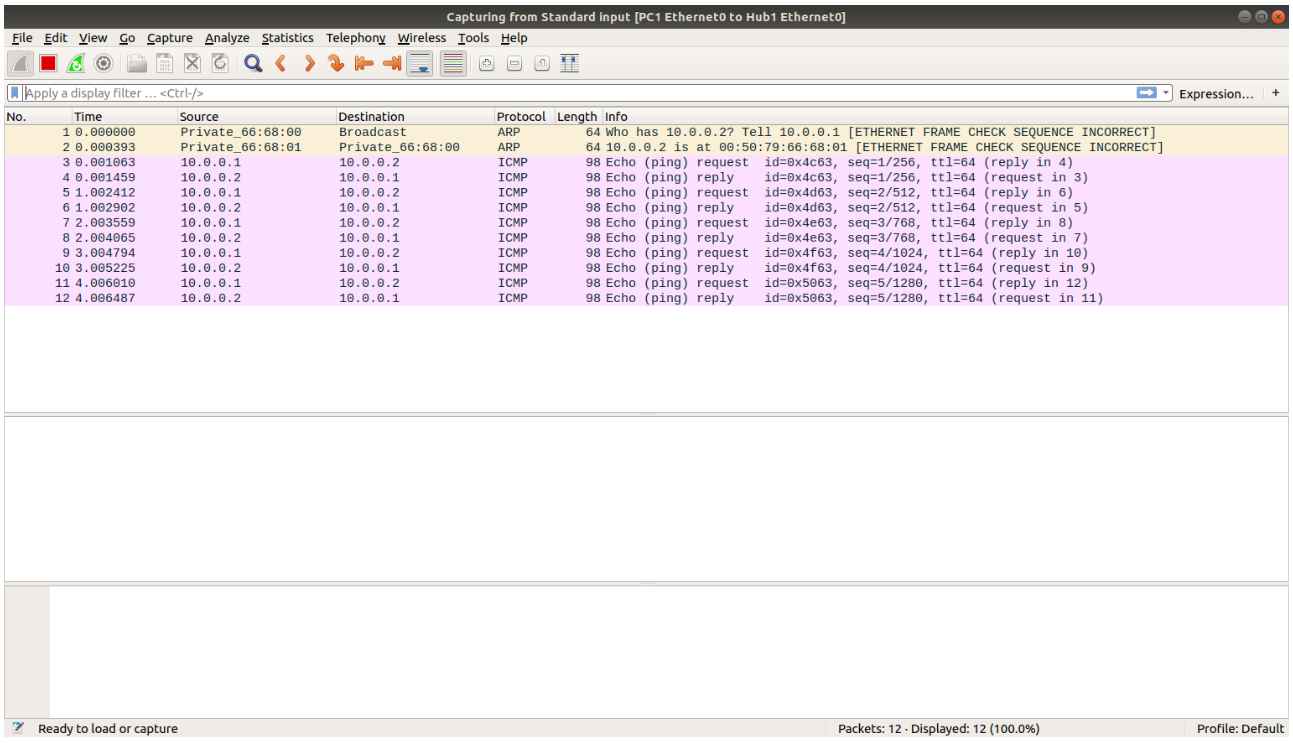
d. View the ARP cache again with the command arp -a. Note that ARP cache entries can get refreshed/deleted fairly quickly (~2minutes).
show arp
e. Save the results of Wireshark.



Node	Console
Hub1	none
PC1	telnet localhost:5000
PC2	telnet localhost:5002
PC3	telnet localhost:5004
PC4	telnet localhost:5006

```
GNS3 management console.
Running GNS3 version 2.2.26 on Linux (64-bit) with Python 3.6.9 Qt 5.9.5 and PyQt 5.10.1.
Copyright (c) 2006-2021 GNS3 Technologies.
Use Help -> GNS3 Doctor to detect common issues.

=>
```

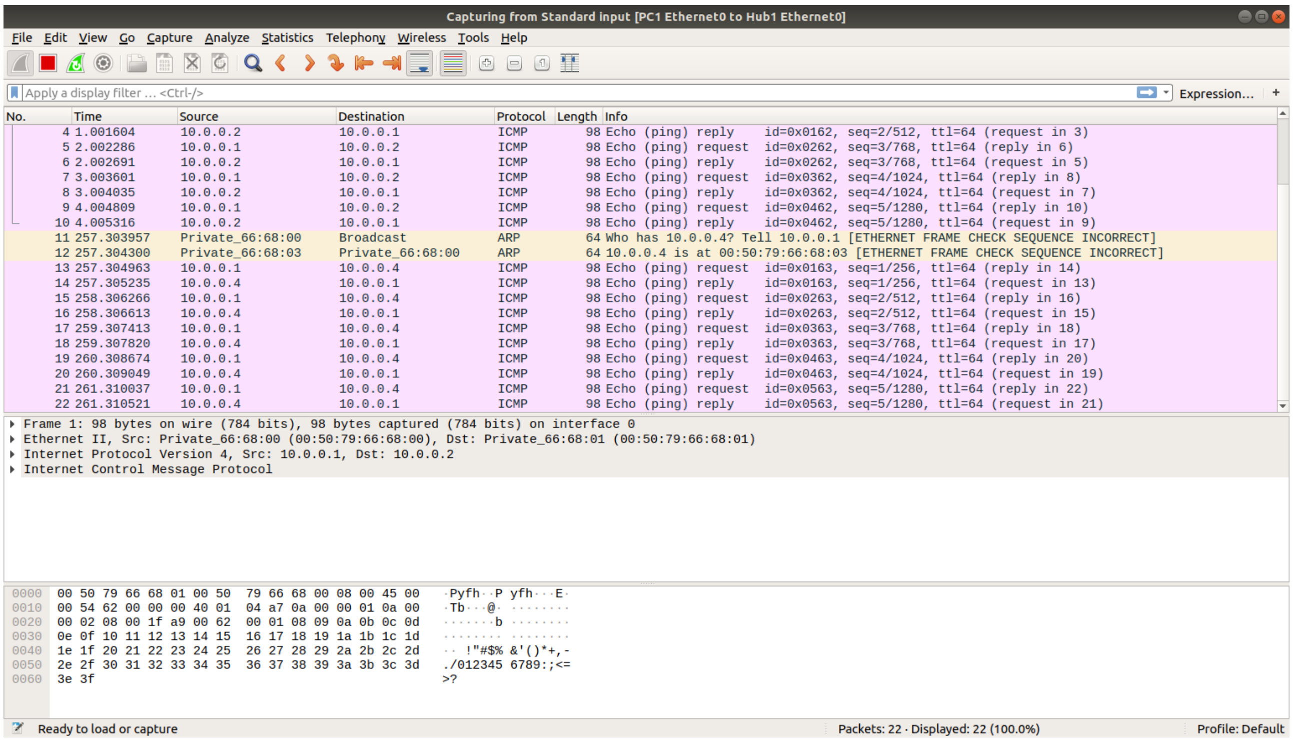
We make a ping to PC2 from PC1 while capturing packets from PC2 to Hub.We notice the request and reply pairs. We also notice the initial broadcast asking where the destination PC is and the corresponding response.


Capturing from Standard input [PC1 Ethernet0 to Hub1 Ethernet0]
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

```
No.   Time       Source            Destination       Protocol Length Info
    1 0.000000   Private_66:68:00  Broadcast         ARP        64 Who has 10.0.0.2? Tell 10.0.0.1 [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
    2 0.000393   Private_66:68:01  Private_66:68:00  ARP        64 10.0.0.2 is at 00:50:79:66:68:01 [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
    3 0.001063   10.0.0.1          10.0.0.2          ICMP       98 Echo (ping) request  id=0x4c63, seq=1/256, ttl=64 (reply in 4)
    4 0.001459   10.0.0.2          10.0.0.1          ICMP       98 Echo (ping) reply    id=0x4c63, seq=1/256, ttl=64 (request in 3)
    5 1.002412   10.0.0.1          10.0.0.2          ICMP       98 Echo (ping) request  id=0x4d63, seq=2/512, ttl=64 (reply in 6)
    6 1.002902   10.0.0.2          10.0.0.1          ICMP       98 Echo (ping) reply    id=0x4d63, seq=2/512, ttl=64 (request in 5)
    7 2.003559   10.0.0.1          10.0.0.2          ICMP       98 Echo (ping) request  id=0x4e63, seq=3/768, ttl=64 (reply in 8)
    8 2.004065   10.0.0.2          10.0.0.1          ICMP       98 Echo (ping) reply    id=0x4e63, seq=3/768, ttl=64 (request in 7)
    9 3.004794   10.0.0.1          10.0.0.2          ICMP       98 Echo (ping) request  id=0x4f63, seq=4/1024, ttl=64 (reply in 10)
   10 3.005225   10.0.0.2          10.0.0.1          ICMP       98 Echo (ping) reply    id=0x4f63, seq=4/1024, ttl=64 (request in 9)
   11 4.006010   10.0.0.1          10.0.0.2          ICMP       98 Echo (ping) request  id=0x5063, seq=5/1280, ttl=64 (reply in 12)
   12 4.006487   10.0.0.2          10.0.0.1          ICMP       98 Echo (ping) reply    id=0x5063, seq=5/1280, ttl=64 (request in 11)
```

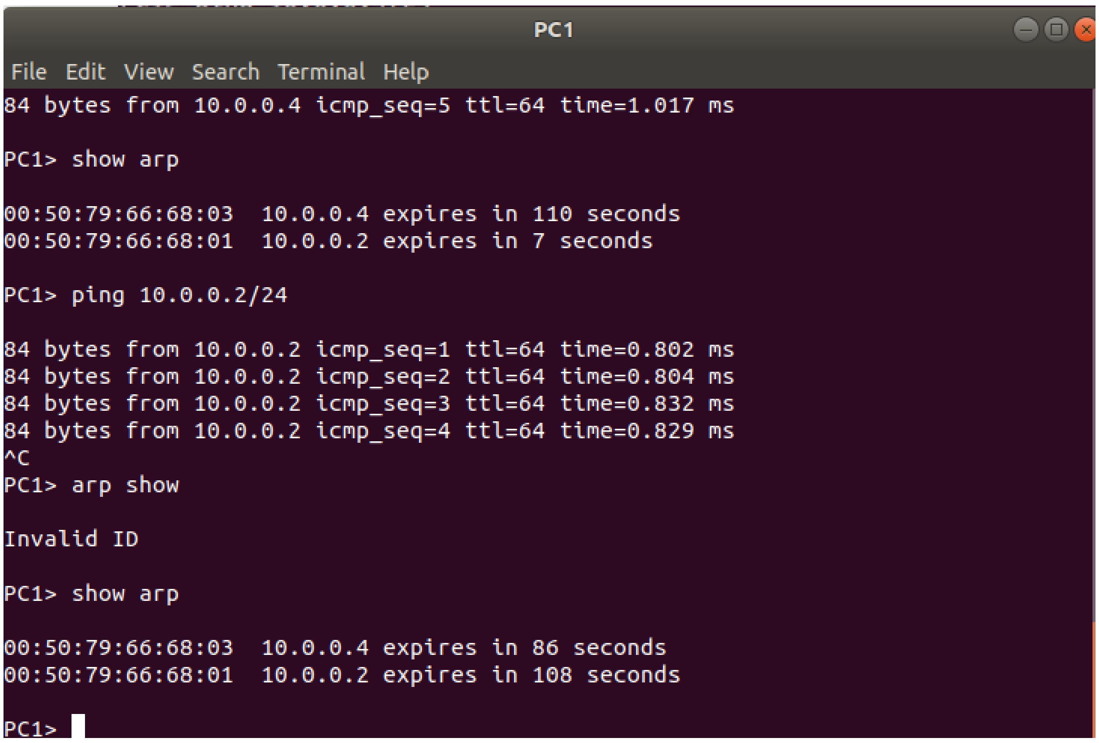
```
Ready to load or capture          Packets: 12 · Displayed: 12 (100.0%)          Profile: Default
```

Now when we ping from PC1 to PC4, we see a similar broadcast asking for the location, but we notice that even the request and reply are tracked even though PC2 is not involved. This is characteristic of the Hub as it works on the principle of broadcasting packets and not routing them exactly like a switch.


Capturing from Standard input [PC1 Ethernet0 to Hub1 Ethernet0]
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

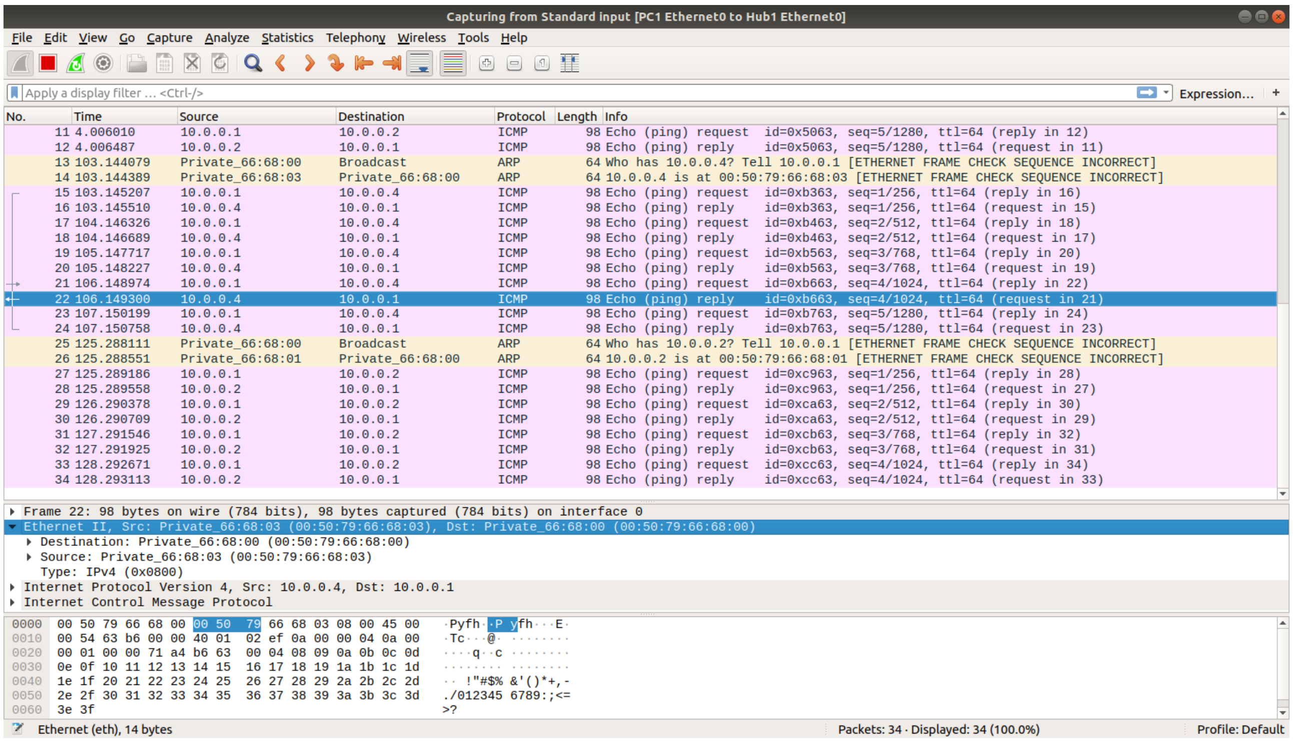
```
No.  Time        Source            Destination       Protocol Length Info
   4 1.001604    10.0.0.2          10.0.0.1          ICMP       98 Echo (ping) reply    id=0x0162, seq=2/512, ttl=64 (request in 3)
   5 2.002286    10.0.0.1          10.0.0.2          ICMP       98 Echo (ping) request  id=0x0262, seq=3/768, ttl=64 (reply in 6)
   6 2.002691    10.0.0.2          10.0.0.1          ICMP       98 Echo (ping) reply    id=0x0262, seq=3/768, ttl=64 (request in 5)
   7 3.003601    10.0.0.1          10.0.0.2          ICMP       98 Echo (ping) request  id=0x0362, seq=4/1024, ttl=64 (reply in 8)
   8 3.004035    10.0.0.2          10.0.0.1          ICMP       98 Echo (ping) reply    id=0x0362, seq=4/1024, ttl=64 (request in 7)
   9 4.004809    10.0.0.1          10.0.0.2          ICMP       98 Echo (ping) request  id=0x0462, seq=5/1280, ttl=64 (reply in 10)
  10 4.005316    10.0.0.2          10.0.0.1          ICMP       98 Echo (ping) reply    id=0x0462, seq=5/1280, ttl=64 (request in 9)
  11 257.303957  Private_66:68:00  Broadcast         ARP        64 Who has 10.0.0.4? Tell 10.0.0.1 [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
  12 257.304300  Private_66:68:03  Private_66:68:00  ARP        64 10.0.0.4 is at 00:50:79:66:68:03 [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
  13 257.304963  10.0.0.1          10.0.0.4          ICMP       98 Echo (ping) request  id=0x0163, seq=1/256, ttl=64 (reply in 14)
  14 257.305235  10.0.0.4          10.0.0.1          ICMP       98 Echo (ping) reply    id=0x0163, seq=1/256, ttl=64 (request in 13)
  15 258.306266  10.0.0.1          10.0.0.4          ICMP       98 Echo (ping) request  id=0x0263, seq=2/512, ttl=64 (reply in 16)
  16 258.306613  10.0.0.4          10.0.0.1          ICMP       98 Echo (ping) reply    id=0x0263, seq=2/512, ttl=64 (request in 15)
  17 259.307413  10.0.0.1          10.0.0.4          ICMP       98 Echo (ping) request  id=0x0363, seq=3/768, ttl=64 (reply in 18)
  18 259.307820  10.0.0.4          10.0.0.1          ICMP       98 Echo (ping) reply    id=0x0363, seq=3/768, ttl=64 (request in 17)
  19 260.308674  10.0.0.1          10.0.0.4          ICMP       98 Echo (ping) request  id=0x0463, seq=4/1024, ttl=64 (reply in 20)
  20 260.309049  10.0.0.4          10.0.0.1          ICMP       98 Echo (ping) reply    id=0x0463, seq=4/1024, ttl=64 (request in 19)
  21 261.310037  10.0.0.1          10.0.0.4          ICMP       98 Echo (ping) request  id=0x0563, seq=5/1280, ttl=64 (reply in 22)
  22 261.310521  10.0.0.4          10.0.0.1          ICMP       98 Echo (ping) reply    id=0x0563, seq=5/1280, ttl=64 (request in 21)

▸ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▸ Ethernet II, Src: Private_66:68:00 (00:50:79:66:68:00), Dst: Private_66:68:01 (00:50:79:66:68:01)
▸ Internet Protocol Version 4, Src: 10.0.0.1, Dst: 10.0.0.2
▸ Internet Control Message Protocol

0000  00 50 79 66 68 01 00 50  79 66 68 00 08 00 45 00   ·Pyfh··P yfh···E·
0010  00 54 62 00 00 00 40 01  04 a7 0a 00 00 01 0a 00   ·Tb···@· ········
0020  00 02 08 00 1f a9 00 62  00 01 08 09 0a 0b 0c 0d   ·······b ········
0030  0e 0f 10 11 12 13 14 15  16 17 18 19 1a 1b 1c 1d   ········ ········
0040  1e 1f 20 21 22 23 24 25  26 27 28 29 2a 2b 2c 2d   ·· !"#$% &'()*+,-
0050  2e 2f 30 31 32 33 34 35  36 37 38 39 3a 3b 3c 3d   ./012345 6789:;<=
0060  3e 3f                                              >?

Ready to load or capture          Packets: 22 · Displayed: 22 (100.0%)          Profile: Default
```

2. We notice the cache entry when we run show arp on PC1



```
84 bytes from 10.0.0.4 icmp_seq=5 ttl=64 time=1.017 ms

PC1> show arp

00:50:79:66:68:03  10.0.0.4 expires in 110 seconds
00:50:79:66:68:01  10.0.0.2 expires in 7 seconds

PC1> ping 10.0.0.2/24

84 bytes from 10.0.0.2 icmp_seq=1 ttl=64 time=0.802 ms
84 bytes from 10.0.0.2 icmp_seq=2 ttl=64 time=0.804 ms
84 bytes from 10.0.0.2 icmp_seq=3 ttl=64 time=0.832 ms
84 bytes from 10.0.0.2 icmp_seq=4 ttl=64 time=0.829 ms
^C
PC1> arp show

Invalid ID

PC1> show arp

00:50:79:66:68:03  10.0.0.4 expires in 86 seconds
00:50:79:66:68:01  10.0.0.2 expires in 108 seconds

PC1>
```

We notice that when we send the same ping request before the arp table entry expires, the initial broadcast asking for the location is not sent, as the location is already known from the cache.


Capturing from Standard input [PC1 Ethernet0 to Hub1 Ethernet0]
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…

```
No.    Time         Source              Destination         Protocol Length Info
    11 4.006010     10.0.0.1            10.0.0.2            ICMP       98 Echo (ping) request  id=0x5063, seq=5/1280, ttl=64 (reply in 12)
    12 4.006487     10.0.0.2            10.0.0.1            ICMP       98 Echo (ping) reply    id=0x5063, seq=5/1280, ttl=64 (request in 11)
    13 103.144079   Private_66:68:00    Broadcast           ARP        64 Who has 10.0.0.4? Tell 10.0.0.1 [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
    14 103.144389   Private_66:68:03    Private_66:68:00    ARP        64 10.0.0.4 is at 00:50:79:66:68:03 [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
    15 103.145207   10.0.0.1            10.0.0.4            ICMP       98 Echo (ping) request  id=0xb363, seq=1/256, ttl=64 (reply in 16)
    16 103.145510   10.0.0.4            10.0.0.1            ICMP       98 Echo (ping) reply    id=0xb363, seq=1/256, ttl=64 (request in 15)
    17 104.146326   10.0.0.1            10.0.0.4            ICMP       98 Echo (ping) request  id=0xb463, seq=2/512, ttl=64 (reply in 18)
    18 104.146689   10.0.0.4            10.0.0.1            ICMP       98 Echo (ping) reply    id=0xb463, seq=2/512, ttl=64 (request in 17)
    19 105.147717   10.0.0.1            10.0.0.4            ICMP       98 Echo (ping) request  id=0xb563, seq=3/768, ttl=64 (reply in 20)
    20 105.148227   10.0.0.4            10.0.0.1            ICMP       98 Echo (ping) reply    id=0xb563, seq=3/768, ttl=64 (request in 19)
    21 106.148974   10.0.0.1            10.0.0.4            ICMP       98 Echo (ping) request  id=0xb663, seq=4/1024, ttl=64 (reply in 22)
    22 106.149300   10.0.0.4            10.0.0.1            ICMP       98 Echo (ping) reply    id=0xb663, seq=4/1024, ttl=64 (request in 21)
    23 107.150199   10.0.0.1            10.0.0.4            ICMP       98 Echo (ping) request  id=0xb763, seq=5/1280, ttl=64 (reply in 24)
    24 107.150758   10.0.0.4            10.0.0.1            ICMP       98 Echo (ping) reply    id=0xb763, seq=5/1280, ttl=64 (request in 23)
    25 125.288111   Private_66:68:00    Broadcast           ARP        64 Who has 10.0.0.2? Tell 10.0.0.1 [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
    26 125.288551   Private_66:68:01    Private_66:68:00    ARP        64 10.0.0.2 is at 00:50:79:66:68:01 [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
    27 125.289186   10.0.0.1            10.0.0.2            ICMP       98 Echo (ping) request  id=0xc963, seq=1/256, ttl=64 (reply in 28)
    28 125.289558   10.0.0.2            10.0.0.1            ICMP       98 Echo (ping) reply    id=0xc963, seq=1/256, ttl=64 (request in 27)
    29 126.290378   10.0.0.1            10.0.0.2            ICMP       98 Echo (ping) request  id=0xca63, seq=2/512, ttl=64 (reply in 30)
    30 126.290709   10.0.0.2            10.0.0.1            ICMP       98 Echo (ping) reply    id=0xca63, seq=2/512, ttl=64 (request in 29)
    31 127.291546   10.0.0.1            10.0.0.2            ICMP       98 Echo (ping) request  id=0xcb63, seq=3/768, ttl=64 (reply in 32)
    32 127.291925   10.0.0.2            10.0.0.1            ICMP       98 Echo (ping) reply    id=0xcb63, seq=3/768, ttl=64 (request in 31)
    33 128.292671   10.0.0.1            10.0.0.2            ICMP       98 Echo (ping) request  id=0xcc63, seq=4/1024, ttl=64 (reply in 34)
    34 128.293113   10.0.0.2            10.0.0.1            ICMP       98 Echo (ping) reply    id=0xcc63, seq=4/1024, ttl=64 (request in 33)
```

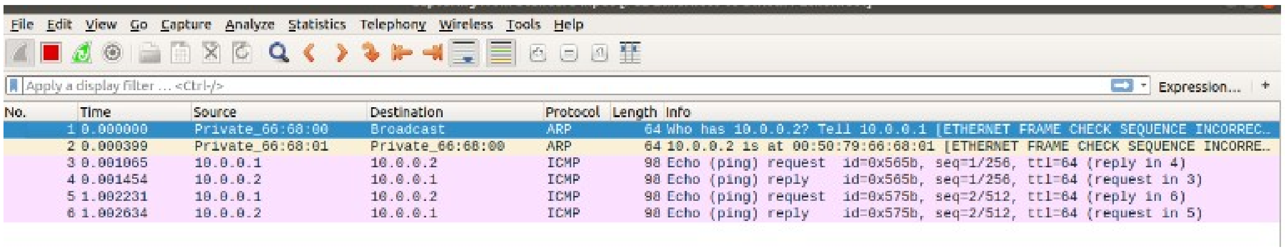
```
▸ Frame 22: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▾ Ethernet II, Src: Private_66:68:03 (00:50:79:66:68:03), Dst: Private_66:68:00 (00:50:79:66:68:00)
   ▸ Destination: Private_66:68:00 (00:50:79:66:68:00)
   ▸ Source: Private_66:68:03 (00:50:79:66:68:03)
     Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 10.0.0.4, Dst: 10.0.0.1
▸ Internet Control Message Protocol
```

```
0000  00 50 79 66 68 00 00 50  79 66 68 03 08 00 45 00   ·Pyfh··P yfh···E·
0010  00 54 63 b6 00 00 40 01  02 ef 0a 00 00 04 0a 00   ·Tc···@· ········
0020  00 01 00 00 71 a4 b6 63  00 04 08 09 0a 0b 0c 0d   ····q··c ········
0030  0e 0f 10 11 12 13 14 15  16 17 18 19 1a 1b 1c 1d   ········ ········
0040  1e 1f 20 21 22 23 24 25  26 27 28 29 2a 2b 2c 2d   ·· !"#$% &'()*+,-
0050  2e 2f 30 31 32 33 34 35  36 37 38 39 3a 3b 3c 3d   ./012345 6789:;<=
0060  3e 3f                                              >?
```

```
Ethernet (eth), 14 bytes          Packets: 34 · Displayed: 34 (100.0%)          Profile: Default
```

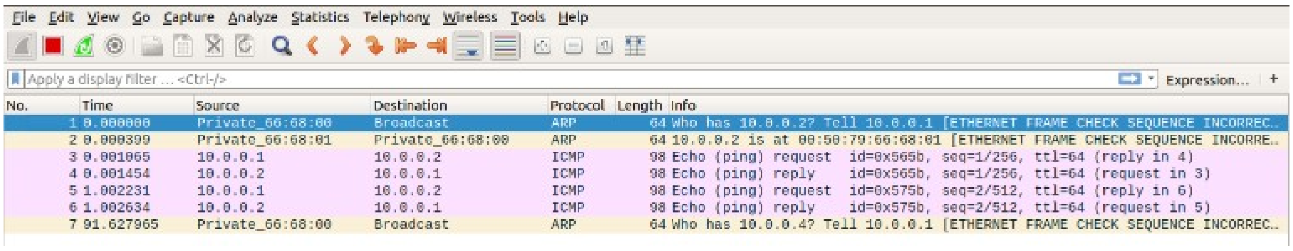
Destination MAC address of the ARP Request packets: 00:50:79:66:68:00
Type field in the ethernet headers is Ipv4 (0x0800)

3. When using a Switch and tracking PC2 to Switch, and ping from PC1 to PC2 we observer no change as compared to Hub.


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

```
No.    Time        Source              Destination         Protocol Length Info
     1 0.000000    Private_66:68:00    Broadcast           ARP        64 Who has 10.0.0.2? Tell 10.0.0.1 [ETHERNET FRAME CHECK SEQUENCE INCORREC…
     2 0.000399    Private_66:68:01    Private_66:68:00    ARP        64 10.0.0.2 is at 00:50:79:66:68:01 [ETHERNET FRAME CHECK SEQUENCE INCORRE…
     3 0.001065    10.0.0.1            10.0.0.2            ICMP       98 Echo (ping) request  id=0x565b, seq=1/256, ttl=64 (reply in 4)
     4 0.001454    10.0.0.2            10.0.0.1            ICMP       98 Echo (ping) reply    id=0x565b, seq=1/256, ttl=64 (request in 3)
     5 1.002231    10.0.0.1            10.0.0.2            ICMP       98 Echo (ping) request  id=0x575b, seq=2/512, ttl=64 (reply in 6)
     6 1.002634    10.0.0.2            10.0.0.1            ICMP       98 Echo (ping) reply    id=0x575b, seq=2/512, ttl=64 (request in 5)
```

But, when we ping PC4 from PC1We notice that the initial broadcast asking for the location of PC4 is the same but the subsequent request and responses are not seen as Switch routes the packets only to the involved Pcs and does not broadcast like Hub.


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

```
No.    Time        Source              Destination         Protocol Length Info
     1 0.000000    Private_66:68:00    Broadcast           ARP        64 Who has 10.0.0.2? Tell 10.0.0.1 [ETHERNET FRAME CHECK SEQUENCE INCORREC…
     2 0.000399    Private_66:68:01    Private_66:68:00    ARP        64 10.0.0.2 is at 00:50:79:66:68:01 [ETHERNET FRAME CHECK SEQUENCE INCORRE…
     3 0.001065    10.0.0.1            10.0.0.2            ICMP       98 Echo (ping) request  id=0x565b, seq=1/256, ttl=64 (reply in 4)
     4 0.001454    10.0.0.2            10.0.0.1            ICMP       98 Echo (ping) reply    id=0x565b, seq=1/256, ttl=64 (request in 3)
     5 1.002231    10.0.0.1            10.0.0.2            ICMP       98 Echo (ping) request  id=0x575b, seq=2/512, ttl=64 (reply in 6)
     6 1.002634    10.0.0.2            10.0.0.1            ICMP       98 Echo (ping) reply    id=0x575b, seq=2/512, ttl=64 (request in 5)
     7 91.627965   Private_66:68:00    Broadcast           ARP        64 Who has 10.0.0.4? Tell 10.0.0.1 [ETHERNET FRAME CHECK SEQUENCE INCORREC…
```

THE END