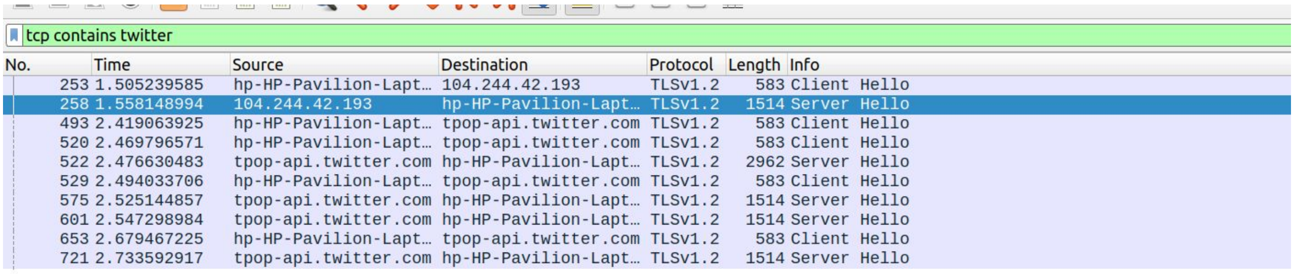
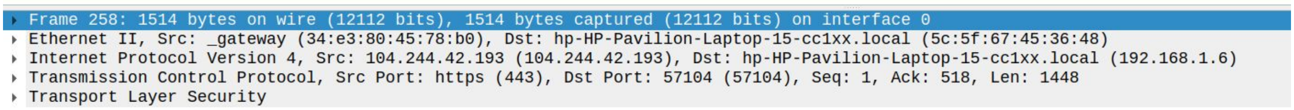
Wireshark Exercises

Keerti Chaudhary (181CO226)

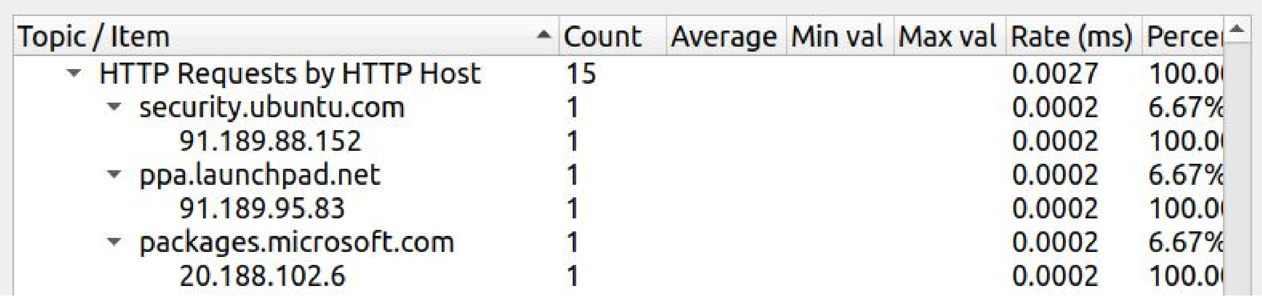
Start a Wireshark capture and browse to twitter.com. Use display filtering to reduce displayed packets to only those sent and received by your computer. How many sites are you interacting with when you interact with Twitter? What are they?



```
tcp contains twitter
No.   Time          Source                    Destination               Protocol Length Info
  253 1.505239585   hp-HP-Pavilion-Lapt…      104.244.42.193            TLSv1.2    583 Client Hello
  258 1.558148994   104.244.42.193            hp-HP-Pavilion-Lapt…      TLSv1.2   1514 Server Hello
  493 2.419063925   hp-HP-Pavilion-Lapt…      tpop-api.twitter.com      TLSv1.2    583 Client Hello
  520 2.469796571   hp-HP-Pavilion-Lapt…      tpop-api.twitter.com      TLSv1.2    583 Client Hello
  522 2.476630483   tpop-api.twitter.com      hp-HP-Pavilion-Lapt…      TLSv1.2   2962 Server Hello
  529 2.494033706   hp-HP-Pavilion-Lapt…      tpop-api.twitter.com      TLSv1.2    583 Client Hello
  575 2.525144857   tpop-api.twitter.com      hp-HP-Pavilion-Lapt…      TLSv1.2   1514 Server Hello
  601 2.547298984   tpop-api.twitter.com      hp-HP-Pavilion-Lapt…      TLSv1.2   1514 Server Hello
  653 2.679467225   hp-HP-Pavilion-Lapt…      tpop-api.twitter.com      TLSv1.2    583 Client Hello
  721 2.733592917   tpop-api.twitter.com      hp-HP-Pavilion-Lapt…      TLSv1.2   1514 Server Hello
```



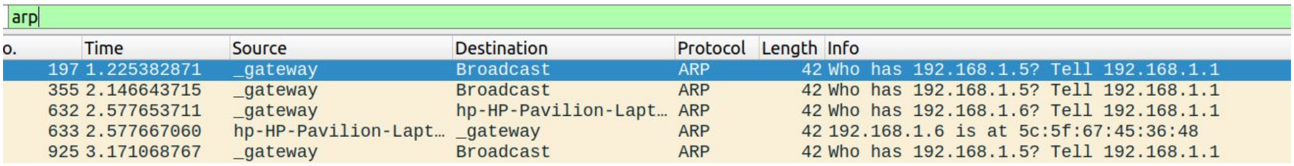
```
▸ Frame 258: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
▸ Ethernet II, Src: _gateway (34:e3:80:45:78:b0), Dst: hp-HP-Pavilion-Laptop-15-cc1xx.local (5c:5f:67:45:36:48)
▸ Internet Protocol Version 4, Src: 104.244.42.193 (104.244.42.193), Dst: hp-HP-Pavilion-Laptop-15-cc1xx.local (192.168.1.6)
▸ Transmission Control Protocol, Src Port: https (443), Dst Port: 57104 (57104), Seq: 1, Ack: 518, Len: 1448
▸ Transport Layer Security
```



Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percei
▾ HTTP Requests by HTTP Host	15				0.0027	100.0
▾ security.ubuntu.com	1				0.0002	6.67%
91.189.88.152	1				0.0002	100.0
▾ ppa.launchpad.net	1				0.0002	6.67%
91.189.95.83	1				0.0002	100.0
▾ packages.microsoft.com	1				0.0002	6.67%
20.188.102.6	1				0.0002	100.0

The 2 sites that are interacting with during interaction with twitter.com is security.ubuntu.com and ppa.launchpad.net.

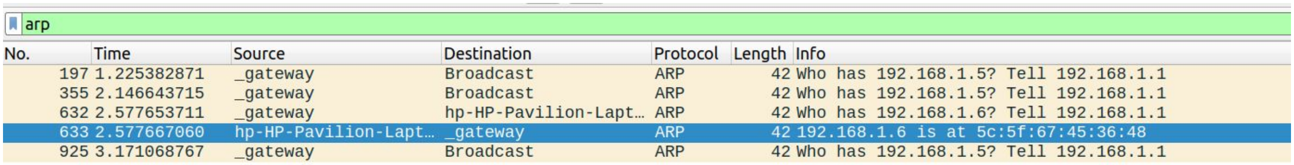
a) Write and test capture filters that capture only your machine's ARP requests. How often are
they sent (i.e., how many ARP packets your machine sends per minute, on average?) This, of
course, depends on your OS and network usage pattern.



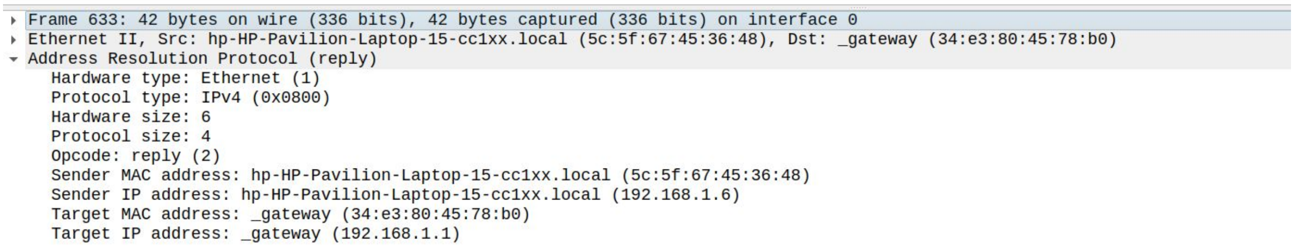
```
arp
o.   Time          Source                 Destination            Protocol Length Info
 197 1.225382871   _gateway               Broadcast              ARP         42 Who has 192.168.1.5? Tell 192.168.1.1
 355 2.146643715   _gateway               Broadcast              ARP         42 Who has 192.168.1.5? Tell 192.168.1.1
 632 2.577653711   _gateway               hp-HP-Pavilion-Lapt…   ARP         42 Who has 192.168.1.6? Tell 192.168.1.1
 633 2.577667060   hp-HP-Pavilion-Lapt…   _gateway               ARP         42 192.168.1.6 is at 5c:5f:67:45:36:48
 925 3.171068767   _gateway               Broadcast              ARP         42 Who has 192.168.1.5? Tell 192.168.1.1
```

There are 4 ARP packets the machine sends per minute.

b) Write and test capture filters that capture only ARP requests sent to your computer. Who
sends them, and how often?



```
arp
No.     Time          Source               Destination          Protocol Length Info
    197 1.225382871   _gateway             Broadcast            ARP          42 Who has 192.168.1.5? Tell 192.168.1.1
    355 2.146643715   _gateway             Broadcast            ARP          42 Who has 192.168.1.5? Tell 192.168.1.1
    632 2.577653711   _gateway             hp-HP-Pavilion-Lapt… ARP          42 Who has 192.168.1.6? Tell 192.168.1.1
    633 2.577667060   hp-HP-Pavilion-Lapt… _gateway             ARP          42 192.168.1.6 is at 5c:5f:67:45:36:48
    925 3.171068767   _gateway             Broadcast            ARP          42 Who has 192.168.1.5? Tell 192.168.1.1
```



```
▸ Frame 633: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
▸ Ethernet II, Src: hp-HP-Pavilion-Laptop-15-cc1xx.local (5c:5f:67:45:36:48), Dst: _gateway (34:e3:80:45:78:b0)
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: hp-HP-Pavilion-Laptop-15-cc1xx.local (5c:5f:67:45:36:48)
    Sender IP address: hp-HP-Pavilion-Laptop-15-cc1xx.local (192.168.1.6)
    Target MAC address: _gateway (34:e3:80:45:78:b0)
    Target IP address: _gateway (192.168.1.1)
```

Sender IP address is 192.168.1.6 and 4 packets per minute are sent on average.

1) What is the IP address of the host?
Ans:- 145.254.160.237

2) What is the IP address of the router?
Ans;- 145.253.2.203

3)What protocol is used to resolve the website domain name?
Ans:-DNS Protocol

4)What is the IP address of the HTTP server?
Ans:- 65.208.228.223

5) Which transport layer protocol is used by DNS?
Ans:- User Datagram Protocol (UDP)

6)Which well-known port is used when contacting the DNS server?
Ans:-53

7) Which ephemeral port does the host initiating the DNS query use?
Ans:- port 3009

8) What is the Ethernet address of the host?
Ans:- 00:00:01:00:00:00

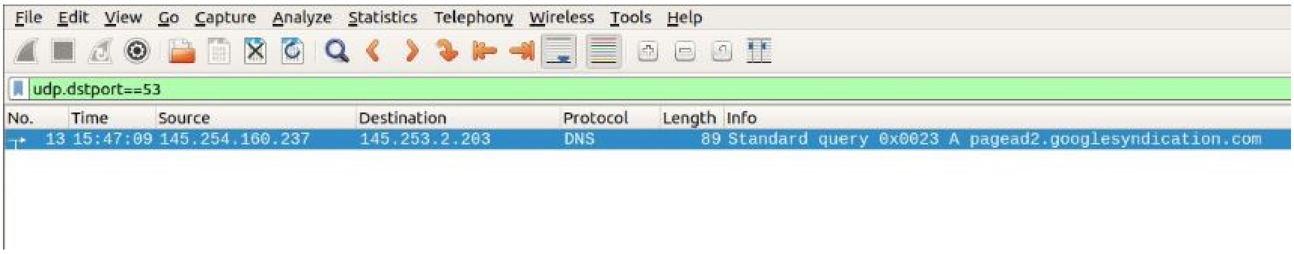
9)What is the Ethernet address of the router?
Ans:- fe:ff:20:00:01:00

10) How long does the 3-way handshake take to complete?
Ans:- 0.9 seconds

11) Which website is the host machine trying to access?
Ans:- www.ethereal.com

12) What version of HTTP is the browser running?
Ans:- HTTP /1.1

13) In the filter box enters the following query: udp.dstport==53 and click apply. What does the
query means and what are the results?
Ans:-

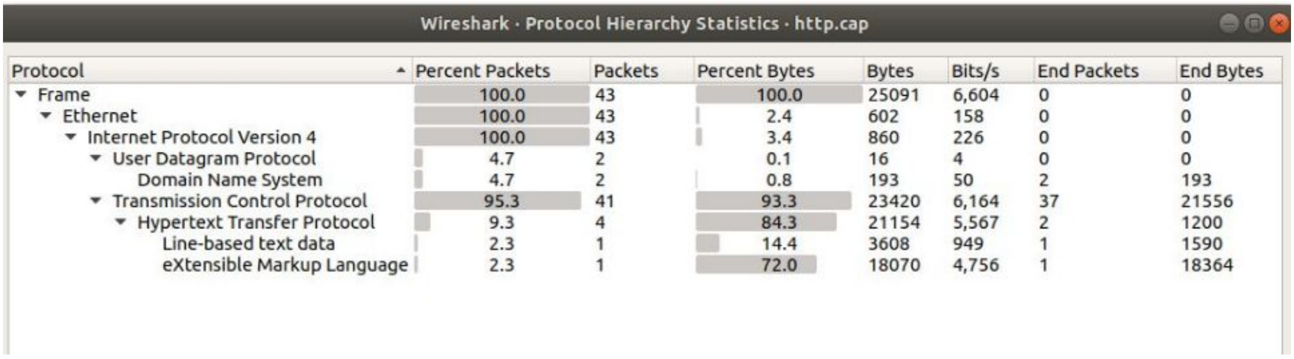

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
udp.dstport==53

No. Time        Source          Destination    Protocol Length Info
 13 15:47:09 145.254.160.237 145.253.2.203  DNS      89 Standard query 0x0023 A pagead2.googlesyndication.com
```

Capture only UDP packets with destination port 53

14) Go to Statistics -> Protocol Hierarchy and answer:

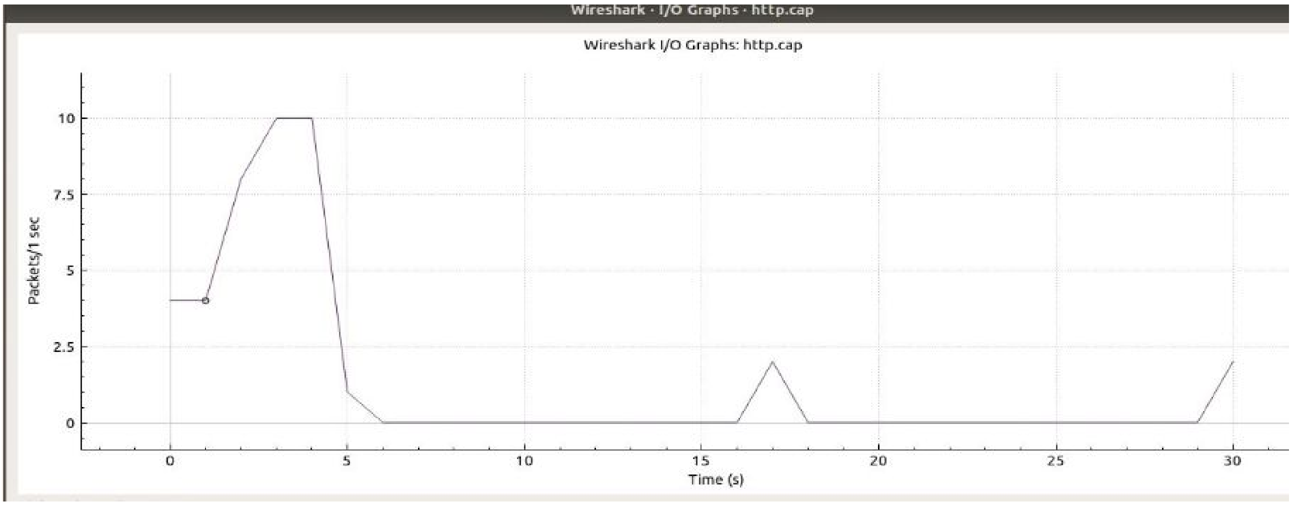

Wireshark · Protocol Hierarchy Statistics · http.cap

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes
▾ Frame	100.0	43	100.0	25091	6,604	0	0
▾ Ethernet	100.0	43	2.4	602	158	0	0
▾ Internet Protocol Version 4	100.0	43	3.4	860	226	0	0
▾ User Datagram Protocol	4.7	2	0.1	16	4	0	0
Domain Name System	4.7	2	0.8	193	50	2	193
▾ Transmission Control Protocol	95.3	41	93.3	23420	6,164	37	21556
▾ Hypertext Transfer Protocol	9.3	4	84.3	21154	5,567	2	1200
Line-based text data	2.3	1	14.4	3608	949	1	1590
eXtensible Markup Language	2.3	1	72.0	18070	4,756	1	18364

A)What percentage of frames are Ethernet frames?
Ans:- 100 %

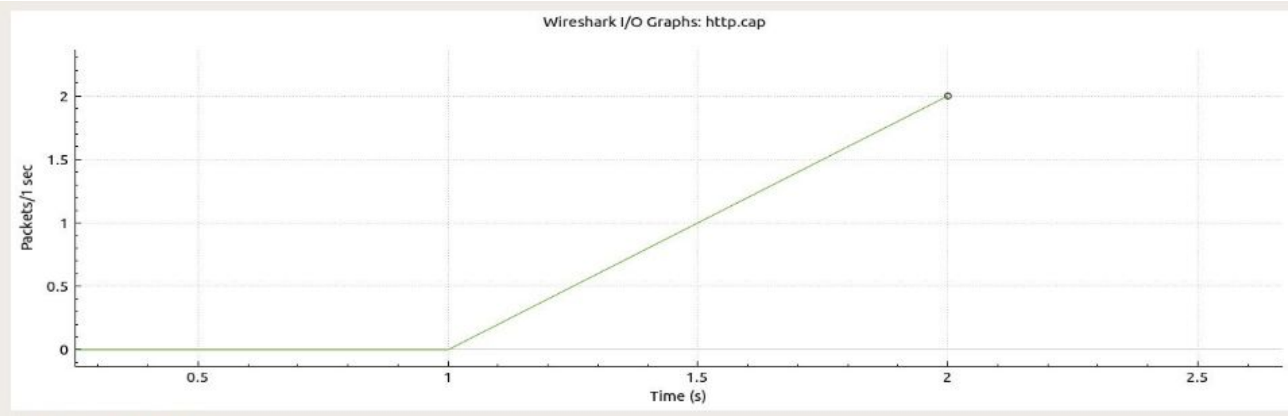
B) Which transport layer protocols were present and which one made up more of the traffic?
Ans:- UDP and TCP are present
TCP- 95.3%

15) A) What is the highest number of TCP packets/sec observed? Around what time (second)?
Ans:- 10 packets/sec at 3sec and 4sec



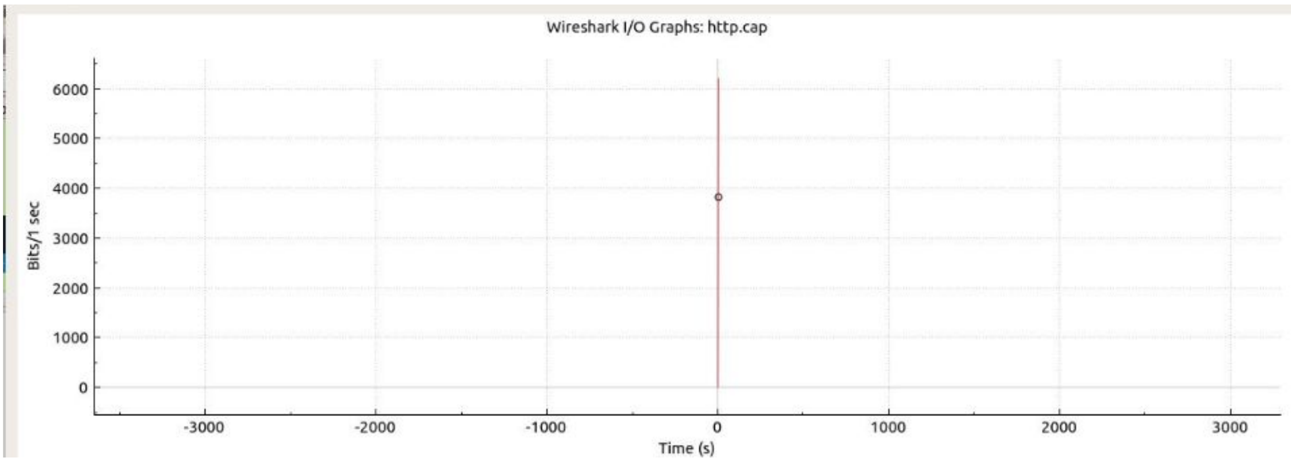
B) What is the highest number of UDP packets/sec observed? Around what time (second)?

Ans:- 2 packets/sec at 2 seconds



C) What is the highest number of HTTP bits/sec observed? Around what time (second)?

Ans:- 6200 bits/ sec at 2 seconds


Wireshark I/O Graphs: http.cap
Bits/1 sec
Time (s)