

2019A7PS0134G_L2

- QUESTION 1

- The different protocols include TCP, TLSv1.2, SSDP, TLSv1.3, HTTP, ICMPV6

- **QUESTION 2**

No.	Time	Source	Destination	Protocol	Length	Info
833	19:38:15.731276	192.168.29.144	128.119.245.12	HTTP	572	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
868	19:38:16.041894	128.119.245.12	192.168.29.144	HTTP	504	HTTP/1.1 200 OK (text/html)
875	19:38:16.110210	192.168.29.144	128.119.245.12	HTTP	518	GET /favicon.ico HTTP/1.1
909	19:38:16.421235	128.119.245.12	192.168.29.144	HTTP	550	HTTP/1.1 404 Not Found (text/html)

The GET response is at time = 19:38:15:731276

The OK response is at time = 19:38:16:041894

Therefore, the time difference is \approx **0.3seconds**

- **QUESTION 3**

Internet address of the gaia.cs.umass.edu : **128.119.245.12**

Internet address of the my laptop : **192.168.29.144**

- **QUESTION 4**

GET Request

/var/folders/g/_4d7_njz15hnbqp75cb_ttm40000gn/T/wireshark_Wi-Fi4LZG1.pcapng 1364 total packets, 1364 shown

No.	Time	Source	Destination	Protocol	Length	Info
833	19:38:15.731276	192.168.29.144	128.119.245.12	HTTP	572	GET /

wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 833: 572 bytes on wire (4576 bits), 572 bytes captured (4576 bits) on interface en0, id 0
Ethernet II, Src: Apple_15:98:3d (b0:be:83:15:98:3d), Dst: Serverco_14:bf:02 (a8:da:0c:14:bf:02)
Internet Protocol Version 4, Src: 192.168.29.144, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 60144, Dst Port: 80, Seq: 1, Ack: 1, Len: 506
Hypertext Transfer Protocol
GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/
1.1\r\n]
Request Method: GET
Request URI: /wireshark-labs/INTRO-wireshark-file1.html
Request Version: HTTP/1.1
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/97.0.4692.99 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
Sec-GPC: 1\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
[HTTP request 1/2]
[Response in frame: 868]
[Next request in frame: 875]

OK Request

/var/folders/g/_4d7_njz15hnfbqp75cb_ttm40000gn/T/wireshark_Wi-Fi4LZG1.pcapng 1364 total packets, 1364 shown

```
No.      Time                Source                Destination           Protocol Length Info
 868 19:38:16.041894    128.119.245.12        192.168.29.144        HTTP      504    HTTP/1.1
200 OK (text/html)
Frame 868: 504 bytes on wire (4032 bits), 504 bytes captured (4032 bits) on interface en0, id 0
Ethernet II, Src: Serverco_14:bf:02 (a8:da:0c:14:bf:02), Dst: Apple_15:98:3d (b0:be:83:15:98:3d)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.29.144
Transmission Control Protocol, Src Port: 80, Dst Port: 60144, Seq: 1, Ack: 507, Len: 438
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, 31 Jan 2022 14:08:16 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.27 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Mon, 31 Jan 2022 06:59:01 GMT\r\n
    ETag: "51-5d6db51c455ed"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 81\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
  \r\n
  [HTTP response 1/2]
  [Time since request: 0.310618000 seconds]
  [Request in frame: 833]
  [Next request in frame: 875]
  [Next response in frame: 909]
  [Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
  File Data: 81 bytes
Line-based text data: text/html (3 lines)
```

- **QUESTION 5**

This can be done on a Linux machine using the command
netstat -stu

On a unix machine, we can use **netstat -sp tcp** for TCP and
netstat -sp udp for UDP

```

Last login: Mon Jan 31 20:35:26 on ttys000
kunalkariwala@kunals-MacBook-Air ~ % netstat -sp tcp

tcp:
  0 packet sent
    0 data packet (0 byte)
    0 data packet (0 byte) retransmitted
    0 resend initiated by MTU discovery
    0 ack-only packet (0 delayed)
    0 URG only packet
    0 window probe packet
    0 window update packet
    0 control packet
    0 data packet sent after flow control
    0 challenge ACK sent due to unexpected SYN
    0 challenge ACK sent due to unexpected RST
    0 checksummed in software
      0 segment (0 byte) over IPv4
      0 segment (0 byte) over IPv6
  0 packet received
    0 ack (for 0 byte)
    0 duplicate ack
    0 ack for unsent data
    0 packet (0 byte) received in-sequence
    0 completely duplicate packet (0 byte)
    0 old duplicate packet
    0 received packet dropped due to low memory
    0 packet with some dup. data (0 byte duped)
    0 out-of-order packet (0 byte)
    0 packet (0 byte) of data after window
    0 window probe
    0 window update packet
    0 packet recovered after loss
    0 packet received after close
    0 bad reset
    0 discarded for bad checksum
    0 checksummed in software
      0 segment (0 byte) over IPv4
      0 segment (0 byte) over IPv6
    0 discarded for bad header offset field
    0 discarded because packet too short
  0 connection request
  0 connection accept
  0 bad connection attempt
  0 listen queue overflow
  0 connection established (including accepts)
  0 connection closed (including 0 drop)
    0 connection updated cached RTT on close
    0 connection updated cached RTT variance on close
    0 connection updated cached ssthresh on close
    0 connection initialized RTT from route cache
    0 connection initialized RTT variance from route cache
    0 connection initialized ssthresh from route cache
  0 embryonic connection dropped
  0 segment updated rtt (or 0 attempt)
  0 retransmit timeout
    0 connection dropped by rexmit timeout
    0 connection dropped after retransmitting FIN
    0 unnecessary packet retransmissions
  0 persist timeout
    0 connection dropped by persist timeout
  0 keepalive timeout
    0 keepalive probe sent
    0 connection dropped by keepalive

```

```

kunalkariwala@kunals-MacBook-Air ~ % netstat -sp udp
udp:
  12645231 datagrams received
    0 with incomplete header
    0 with bad data length field
    0 with bad checksum
    4 with no checksum
  5963 checksummed in software
    226 datagrams (57632 bytes) over IPv4
    5737 datagrams (1147769 bytes) over IPv6
  3669 dropped due to no socket
  569 broadcast/multicast datagrams undelivered
    0 time multicast source filter matched
    0 dropped due to full socket buffers
    0 not for hashed pcb
  12640993 delivered
  2560809 datagrams output
    75139 checksummed in software
    135 datagrams (40822 bytes) over IPv4
    75004 datagrams (28759760 bytes) over IPv6
kunalkariwala@kunals-MacBook-Air ~ %

```

• QUESTION 6

This can be done using **netstat -l**

```
kunalkariwala — zsh — 168x45
Last login: Mon Jan 31 20:21:30 on ttys000
kunalkariwala@kunals-MacBook-Air ~ % netstat -l
Active Internet connections
Proto Recv-Q Send-Q Local Address           Foreign Address          (state)
tcp4      0      0 192.168.29.144.60537    20.205.220.48.https     ESTABLISHED
tcp6      0      0 2405:201:4:d852:f1fe:917e:5fa2:3b6d.60536 bom12s06-in-x02.1e100.net.https ESTABLISHED
tcp6      0      0 2405:201:4:d852:f1fe:917e:5fa2:3b6d.60535 2405:200:1602:1817:face:b00c:3333:7020.https ESTABLISHED
tcp6      0      0 2405:201:4:d852:f1fe:917e:5fa2:3b6d.60534 sa-in-f108.1e100.net.imaps ESTABLISHED
tcp6      0      0 2405:201:4:d852:f1fe:917e:5fa2:3b6d.60529 2606:4700::6812:176e.https ESTABLISHED
tcp6      0      0 2405:201:4:d852:f1fe:917e:5fa2:3b6d.60482 2606:4700::6812:166e.https ESTABLISHED
tcp6      0      0 2405:201:4:d852:f1fe:917e:5fa2:3b6d.60186 2606:4700::6812:166e.https ESTABLISHED
tcp6      0      0 2405:201:4:d852:f1fe:917e:5fa2:3b6d.60182 whatsapp-cdn6-shv-01-pnq1.fbcddn.net.https ESTABLISHED
tcp4      0      0 192.168.29.144.60172   ec2-34-237-73-95.https  ESTABLISHED
tcp4      0      0 192.168.29.144.59967   192.168.29.212.49743    ESTABLISHED
tcp6      0      0 2405:201:4:d852:f1fe:917e:5fa2:3b6d.59965 si-in-f188.1e100.net.5228 ESTABLISHED
tcp6      0      0 2405:201:4:d852:f1fe:917e:5fa2:3b6d.59728 sm-in-f108.1e100.net.imaps ESTABLISHED
tcp6      0      0 2405:201:4:d852:280d:f7fb:bccd:cb93:54663 sa-in-f109.1e100.net.imaps ESTABLISHED
tcp6      0      0 kunals-macbook-air.exosee fe80::a3c5:687c:56c7:e191%utun3.1025 ESTABLISHED
tcp6      0      0 kunals-macbook-air.1024 fe80::a3c5:687c:56c7:e191%utun3.1024 ESTABLISHED
tcp6      0      0 kunals-macbook-air.exosee fe80::b99b:a05c:2f8e:d2aa%utun5.1025 ESTABLISHED
tcp6      0      0 kunals-macbook-air.1024 fe80::b99b:a05c:2f8e:d2aa%utun5.1024 ESTABLISHED
tcp4      0      0 192.168.29.144.55677  17.57.145.117.5223     ESTABLISHED
```

• QUESTION 7

This can be done using **dig www.gmail.com MX**

```
kunalkariwala@kunals-MacBook-Air ~ % dig www.gmail.com MX

; <<>> DiG 9.10.6 <<>> www.gmail.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15627
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;www.gmail.com.                IN      MX

;; ANSWER SECTION:
www.gmail.com.                22000   IN      CNAME   mail.google.com.
mail.google.com.             116428  IN      CNAME   googlemail.l.google.com.

;; AUTHORITY SECTION:
l.google.com.                 60      IN      SOA      ns1.google.com. dns-admin.google.com. 425175900 900 900 1800 60

;; Query time: 72 msec
;; SERVER: 2405:201:4:d852::c0a8:1d01#53(2405:201:4:d852::c0a8:1d01)
;; WHEN: Mon Jan 31 20:39:56 IST 2022
;; MSG SIZE rcvd: 145
```

• QUESTION 8

This can be done using **netstat -i**

```
kunalkariwala@kunals-MacBook-Air ~ % netstat -i
```

Name	Mtu	Network	Address	Ipkts	Ierrs	Opkts	Oerrs	Coll
lo0	16384	<Link#1>		78709	0	78709	0	0
lo0	16384	127	localhost	78709	-	78709	-	-
lo0	16384	localhost	::1	78709	-	78709	-	-
lo0	16384	kunals-macb	fe80::1:1	78709	-	78709	-	-
gif0*	1280	<Link#2>		0	0	0	0	0
stf0*	1280	<Link#3>		0	0	0	0	0
anp11	1500	<Link#4>	9e:fa:b4:73:84:ce	0	0	0	0	0
anp11	1500	kunals-macb	fe80:4:19cfa:b4ff	0	-	0	-	-
anp10	1500	<Link#5>	9e:fa:b4:73:84:cd	0	0	0	0	0
anp10	1500	kunals-macb	fe80:15:19cfa:b4ff	0	-	0	-	-
en3	1500	<Link#6>	9e:fa:b4:73:84:ad	0	0	0	0	0
en4	1500	<Link#7>	9e:fa:b4:73:84:ae	0	0	0	0	0
en1	1500	<Link#8>	36:f4:9d:f8:1c:00	0	0	0	0	0
en2	1500	<Link#9>	36:f4:9d:f8:1c:04	0	0	0	0	0
ap1	1500	<Link#10>	b2:be:83:15:98:3d	0	0	0	0	0
en0	1500	<Link#11>	b0:be:83:15:98:3d	22077279	0	4438181	0	0
en0	1500	kunals-macb	fe80:b:14b9:db9b	22077279	-	4438181	-	-
en0	1500	192.168.29	192.168.29.144	22077279	-	4438181	-	-
en0	1500	2405:201:4	2405:201:4:d852:1	22077279	-	4438181	-	-
en0	1500	2405:201:4	2405:201:4:d852:f	22077279	-	4438181	-	-
awd10	1500	<Link#12>	4e:f2:6c:9e:45:6b	9672	0	7037	0	0
awd10	1500	fe80::4cf2	fe80:c:14cf2:6cff	9672	-	7037	-	-
llw0	1500	<Link#13>	4e:f2:6c:9e:45:6b	0	0	0	0	0
llw0	1500	fe80::4cf2	fe80:d:14cf2:6cff	0	-	0	-	-
bridge0	1500	<Link#14>	36:f4:9d:f8:1c:00	0	0	0	0	0
utun0	1380	<Link#15>		0	0	60	0	0
utun0	1380	kunals-macb	fe80:f:16e4:18c31	0	-	60	-	-
utun1	2000	<Link#16>		0	0	60	0	0
utun1	2000	kunals-macb	fe80:10:15b35:174	0	-	60	-	-
utun2	1000	<Link#17>		0	0	60	0	0
utun2	1000	kunals-macb	fe80:11:1ce81:b1c	0	-	60	-	-
utun3	1380	<Link#18>		174	0	208	0	0
utun3	1380	kunals-macb	fe80:12:134d7:3e8	174	-	208	-	-
utun4	1380	<Link#19>		0	0	60	0	0
utun4	1380	kunals-macb	fe80:13:17d85:14d	0	-	60	-	-
utun5	1380	<Link#21>		68	0	67	0	0
utun5	1380	kunals-macb	fe80:15:16e23:3fc	68	-	67	-	-
utun6	1380	<Link#22>		0	0	2	0	0
utun6	1380	kunals-macb	fe80:16:19e61:d15	0	-	2	-	-

```
kunalkariwala@kunals-MacBook-Air ~ %
```

• QUESTION 9

This can be done using **traceroute 8.8.8.8**

```
kunalkariwala@kunals-MacBook-Air ~ % traceroute 8.8.8.8
```

```
traceroute to 8.8.8.8 (8.8.8.8), 64 hops max, 52 byte packets
```

```
1  reliance.reliance (192.168.29.1)  5.687 ms  4.390 ms  3.717 ms
```

```
2  10.25.248.1 (10.25.248.1)  5.697 ms  5.733 ms  4.880 ms
```

```
3  * * 172.31.2.22 (172.31.2.22)  36.779 ms
```

```
4  192.168.70.12 (192.168.70.12)  29.150 ms
```

```
   192.168.70.16 (192.168.70.16)  28.429 ms
```

```
   192.168.70.12 (192.168.70.12)  28.949 ms
```

```
5  * 172.26.76.164 (172.26.76.164)  27.346 ms  27.463 ms
```

```
6  172.26.76.130 (172.26.76.130)  28.605 ms  28.972 ms  27.531 ms
```

```
7  192.168.7.248 (192.168.7.248)  27.732 ms  27.582 ms
```

```
   192.168.7.246 (192.168.7.246)  29.834 ms
```

```
8  192.168.7.247 (192.168.7.247)  29.045 ms
```

```
   192.168.7.249 (192.168.7.249)  30.604 ms
```

```
   192.168.7.251 (192.168.7.251)  31.158 ms
```

```
9  172.31.2.99 (172.31.2.99)  32.631 ms *
```

```
   172.31.3.23 (172.31.3.23)  40.026 ms
```

```
10 72.14.211.138 (72.14.211.138)  33.039 ms
```

```
    72.14.217.206 (72.14.217.206)  29.898 ms
```

```
    72.14.211.138 (72.14.211.138)  29.844 ms
```

```
11 * * *
```

```
12 dns.google (8.8.8.8)  26.761 ms  26.545 ms  25.455 ms
```

```
kunalkariwala@kunals-MacBook-Air ~ %
```

To read the latency:-

The times to the right hand side of every index can be used to get latency. It corresponds to the time required to send the packet to the address + time to return.

- QUESTION 10

This can be done using **ping 8.8.8.8 -c 10**

```
kunalkariwala@kunals-MacBook-Air ~ % ping 8.8.8.8 -c 10
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=112 time=13.981 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=112 time=9.664 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=112 time=8.012 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=112 time=7.681 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=112 time=8.495 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=112 time=8.851 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=112 time=13.877 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=112 time=15.207 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=112 time=22.737 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=112 time=14.814 ms

--- 8.8.8.8 ping statistics ---
10 packets transmitted, 10 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 7.681/12.332/22.737/4.495 ms
kunalkariwala@kunals-MacBook-Air ~ %
```

- QUESTION 11

This can be done using
nslookup www.bits-pilani.ac.in or **dig www.bits-pilani.ac.in**

```
kunalkariwala@kunals-MacBook-Air ~ % dig www.bits-pilani.ac.in

; <<>> DiG 9.10.6 <<>> www.bits-pilani.ac.in
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3836
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.bits-pilani.ac.in.      IN      A

;; ANSWER SECTION:
www.bits-pilani.ac.in. 63321 IN      CNAME  universe.bits-pilani.ac.in.
universe.bits-pilani.ac.in. 63221 IN      A      14.139.243.20
universe.bits-pilani.ac.in. 63221 IN      A      103.144.92.33

;; Query time: 9 msec
;; SERVER: 2405:201:4:d852::c0a8:1d01#53(2405:201:4:d852::c0a8:1d01)
;; WHEN: Mon Jan 31 20:51:46 IST 2022
;; MSG SIZE rcvd: 111

kunalkariwala@kunals-MacBook-Air ~ % nslookup www.bits-pilani.ac.in
Server:      2405:201:4:d852::c0a8:1d01
Address:     2405:201:4:d852::c0a8:1d01#53

Non-authoritative answer:
www.bits-pilani.ac.in canonical name = universe.bits-pilani.ac.in.
Name:   universe.bits-pilani.ac.in
Address: 103.144.92.33
Name:   universe.bits-pilani.ac.in
Address: 14.139.243.20
```