

Q1.

Measurement	Captured	Displayed	Marked
Packets	434	—	—
Time span, s	1654.784	—	—
Average pps	0.3	—	—
Average packet size, B	72	—	—
Bytes	31060	0	0
Average bytes/s	18	—	—
Average bits/s	150	—	—

Capture file comments

Q2.

The image shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. The main display area is divided into three panes:

- Packet List:** A table showing a list of captured packets. The selected packet is number 401, which is a DNS packet from 192.168.217.3 to 192.168.217.2.
- Packet Bytes:** A hex dump of the selected packet's raw data, showing the structure of an Ethernet II frame, an IPv4 header, and an ICMP header.
- Packet Details:** A tree view showing the hierarchical structure of the selected packet, including Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol.

No.	Time	Source	Destination	Protocol	Length	Info
401	75.249590400	192.168.217.3	192.168.217.2	DNS	87	Standard
402	75.249609300	192.168.217.3	192.168.217.2	DNS	87	Standard
403	75.251760600	192.168.217.2	192.168.217.3	DNS	54	Standard
404	75.251764800	192.168.217.2	192.168.217.3	DNS	54	Standard
405	75.289995800	192.168.217.3	192.168.217.2	DNS	89	Standard
406	75.290014400	192.168.217.3	192.168.217.2	DNS	89	Standard
407	75.298618300	192.168.217.2	192.168.217.3	DNS	54	Standard
408	75.298622400	192.168.217.2	192.168.217.3	DNS	54	Standard
409	75.910312200	192.168.217.3	192.168.217.2	DNS	79	Standard
410	75.910334100	192.168.217.3	192.168.217.2	DNS	79	Standard
411	75.915198300	192.168.217.2	192.168.217.3	DNS	54	Standard

Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface eth0  
Ethernet II, Src: Microsoft\_40:57:27 (00:15:00:00:00:00), Dst: 192.168.217.2 (08:00:2b:01:02:02)  
Internet Protocol Version 4, Src: 192.168.217.3, Dst: 192.168.217.2  
Internet Control Message Protocol

I didn't see any icmp traffic captured the first time

Q.3

```
Source Address: 192.168.10.18
Destination Address: 192.168.217.3
```

```
Internet Control Message Protocol
Type: 0 (Echo (ping) reply)
Code: 0
Checksum: 0xa050 [correct]
[Checksum Status: Good]
Identifier (BE): 28387 (0x6ee3)
Identifier (LE): 58222 (0xe36e)
Sequence Number (BE): 1 (0x0001)
Sequence Number (LE): 256 (0x0100)
[Request frame: 1]
[Response time: 10.042 ms]
```

Q4.

The screenshot shows the Wireshark interface with a filter on 'dns'. The packet list pane shows 300 packets from source 192.168.217.3. The packet details pane shows a Domain Name System (query) frame. The statistics pane shows 420 packets captured, 260 displayed (61.9%), and 3,501 average bits/s.

Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
eth0	0 (0.0%)	none	Ethernet	262144 bytes

Measurement	Captured	Displayed	Marked
Packets	420	260 (61.9%)	—
Time span, s	77.129	65.990	—
Average pps	5.4	3.9	—
Average packet size, B	80	70	—
Bytes	33754	18298 (54.2%)	0
Average bytes/s	437	277	—
Average bits/s	3,501	2,218	—

70 DNS packets

Q5.

[push.services.mozilla.com](https://push.services.mozilla.com)

Source IP: 192.168.217.3 port: 36893

Destination IP: 192.168.217.2 port: 53

The screenshot shows the Wireshark interface with a filter on 'dns'. The packet list pane shows a list of 19 DNS standard queries from source 192.168.217.3 to destination 192.168.217.2. The packet details pane shows a Domain Name System (query) frame for 'push.services.mozilla.com'.

No.	Time	Source	Destination	Protocol	Length	Info
415	77.012037200	192.168.217.3	192.168.217.2	DNS	85	Standard query 0x00a3 A push.services.mozilla.com
379	70.286585400	192.168.217.3	192.168.217.2	DNS	89	Standard query 0x0263 A location.services.mozilla.com
405	75.289995800	192.168.217.3	192.168.217.2	DNS	89	Standard query 0x0263 A location.services.mozilla.com
316	62.581953000	192.168.217.3	192.168.217.2	DNS	97	Standard query 0x06b5 AAAA firefox.settings.services.mozilla.com
358	67.586310800	192.168.217.3	192.168.217.2	DNS	97	Standard query 0x06b5 AAAA firefox.settings.services.mozilla.com
149	40.890694700	192.168.217.3	192.168.217.2	DNS	95	Standard query 0x0714 A content-signature-2.cdn.mozilla.net
185	45.895478200	192.168.217.3	192.168.217.2	DNS	95	Standard query 0x0714 A content-signature-2.cdn.mozilla.net
278	57.967349500	192.168.217.3	192.168.217.2	DNS	84	Standard query 0x0f57 AAAA normandy.cdn.mozilla.net
320	62.969988900	192.168.217.3	192.168.217.2	DNS	84	Standard query 0x0f57 AAAA normandy.cdn.mozilla.net
150	40.890717000	192.168.217.3	192.168.217.2	DNS	95	Standard query 0x11f5 AAAA content-signature-2.cdn.mozilla.net
186	45.895503200	192.168.217.3	192.168.217.2	DNS	95	Standard query 0x11f5 AAAA content-signature-2.cdn.mozilla.net
215	50.272203800	192.168.217.3	192.168.217.2	DNS	79	Standard query 0x1ad6 A spocs.getpocket.com

Q6 src port: 53 IP 192.168.217.2  
, dst port: 36893 IP 192.168.217.3

The image shows a Wireshark network traffic capture window titled "eth0". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar with various icons. A filter bar at the top shows "dns". The main pane displays a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. Packet 417 is selected and highlighted in blue. Below the list, the packet details pane shows the structure of the selected packet: Frame 417 (54 bytes on wire, 54 bytes captured on interface eth0), Ethernet II, Internet Protocol Version 4, User Datagram Protocol (Src Port: 53, Dst Port: 36893), and Domain Name System (response). The DNS details show Transaction ID: 0x00a3, Flags: 0x8105 (Standard query response, Refused), and 0 questions and authority records.

No.	Time	Source	Destination	Protocol	Length	Info
216	50.272221600	192.168.217.3	192.168.217.2	DNS	79	Standard query 0xfc38 AAAA spocs.getpocket.com
254	55.276837100	192.168.217.3	192.168.217.2	DNS	79	Standard query 0xfc38 AAAA spocs.getpocket.com
417	77.027271000	192.168.217.2	192.168.217.3	DNS	54	Standard query response 0x00a3 Refused
381	70.287870200	192.168.217.2	192.168.217.3	DNS	54	Standard query response 0x0263 Refused
407	75.298618300	192.168.217.2	192.168.217.3	DNS	54	Standard query response 0x0263 Refused
318	62.589541700	192.168.217.2	192.168.217.3	DNS	54	Standard query response 0x06b5 Refused
360	67.594912800	192.168.217.2	192.168.217.3	DNS	54	Standard query response 0x06b5 Refused
151	40.898147300	192.168.217.2	192.168.217.3	DNS	54	Standard query response 0x0714 Refused
187	45.902547200	192.168.217.2	192.168.217.3	DNS	54	Standard query response 0x0714 Refused
280	57.968710000	192.168.217.2	192.168.217.3	DNS	54	Standard query response 0x0f57 Refused
322	62.978763500	192.168.217.2	192.168.217.3	DNS	54	Standard query response 0x0f57 Refused
152	40.898151300	192.168.217.2	192.168.217.3	DNS	54	Standard query response 0x11f5 Refused

Frame 417: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0  
Ethernet II, Src: Microsoft\_40:57:38 (00:15:5d:40:57:38), Dst: Microsoft\_40:57:27 (00:15:5d:40:57:27)  
Internet Protocol Version 4, Src: 192.168.217.2, Dst: 192.168.217.3  
User Datagram Protocol, Src Port: 53, Dst Port: 36893  
Domain Name System (response)  
Transaction ID: 0x00a3  
Flags: 0x8105 Standard query response, Refused  
Questions: 0  
Answer RRs: 0  
Authority RRs: 0