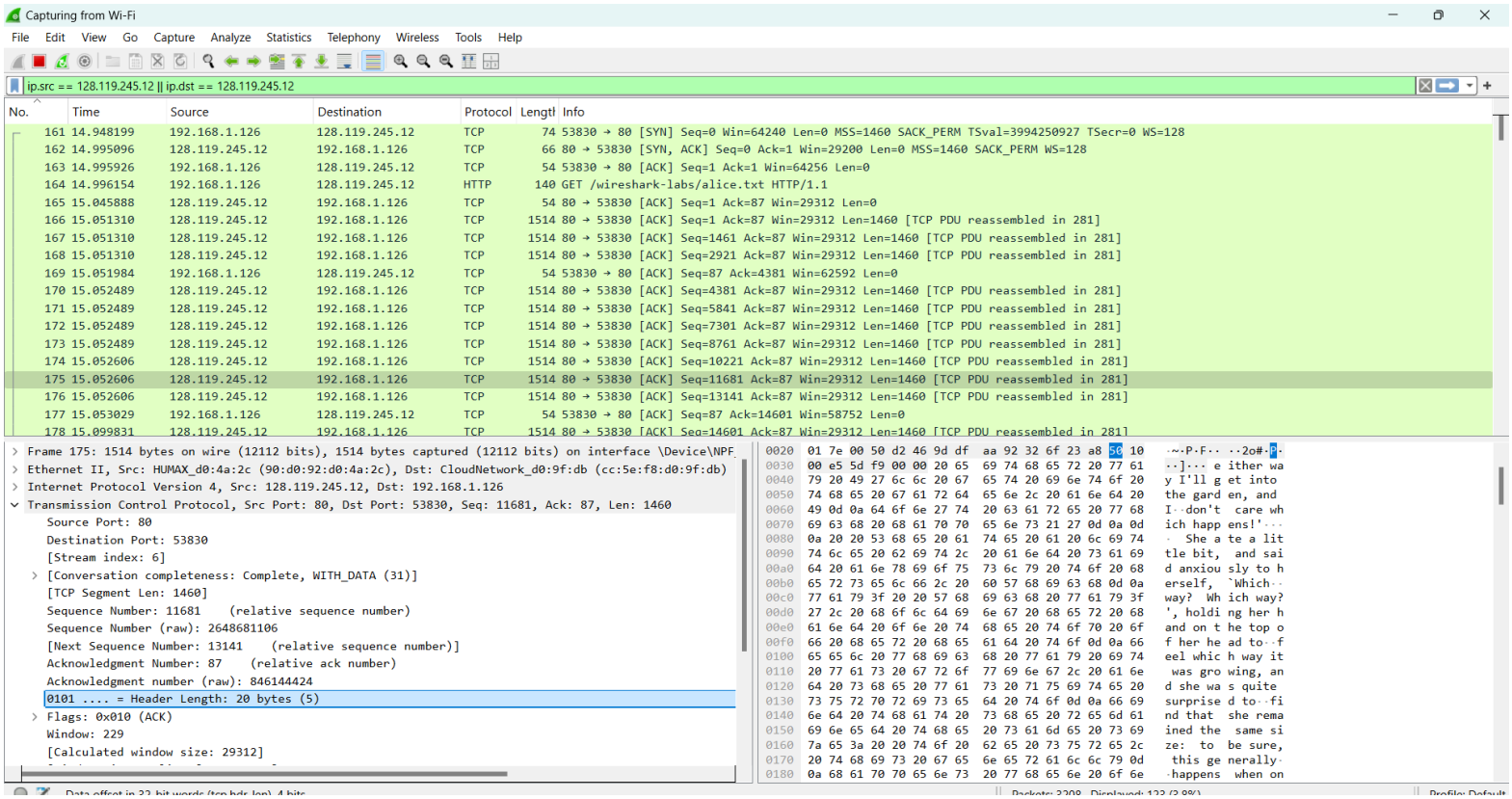
P4 Report

Part A

1. Port 80 is used for the HTTP connections.
2. The server is running an Apache version 2.4.6 web server.
3. The data is 152138 bytes.
4. HTTP/1.1 200 OK indicates that the server successfully received and processed the GET request.

Part B

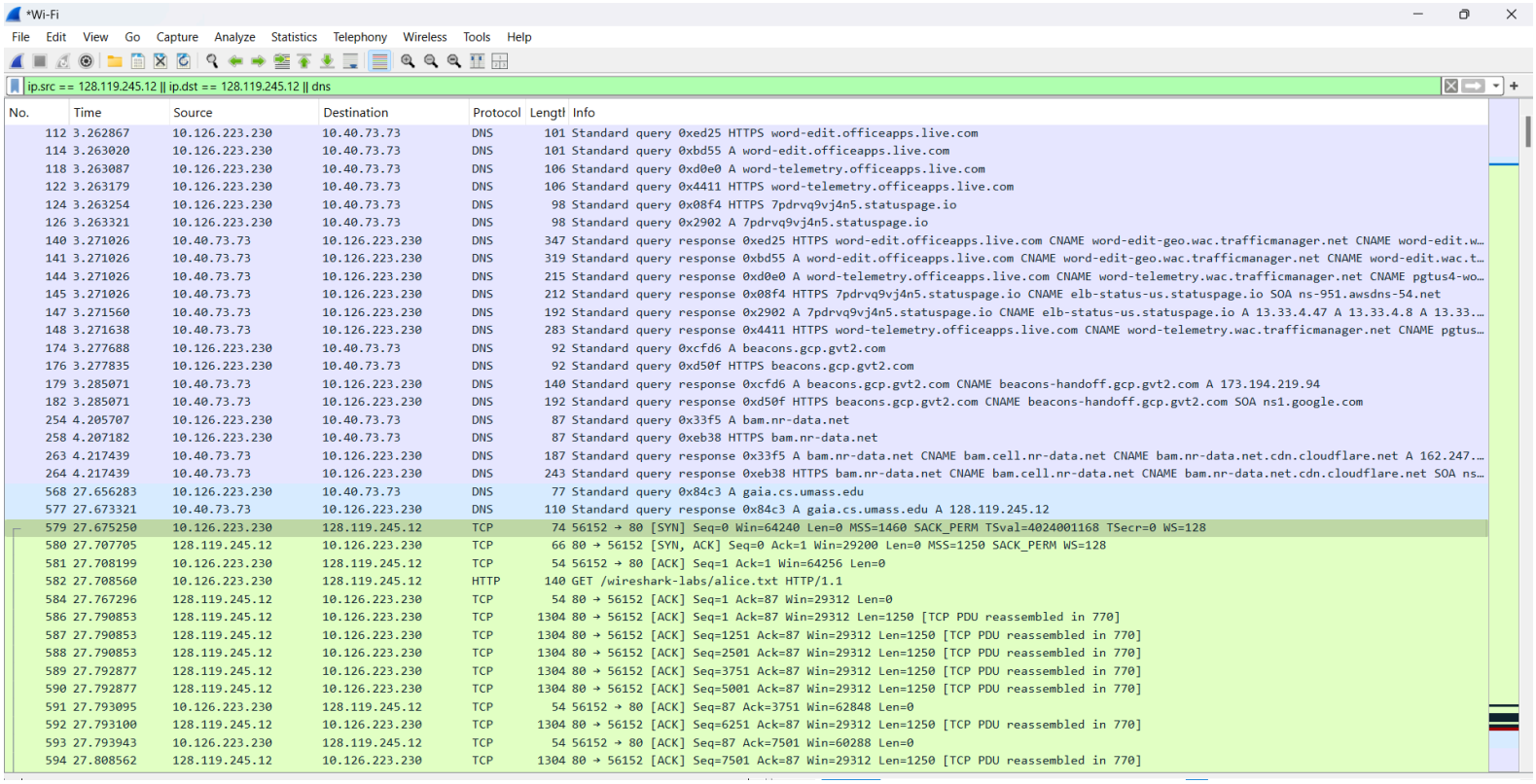
1.



2. First, to establish a connection, the TCP handshake takes place. The client (192.168.1.126) sends a SYN packet to the web server (128.119.245.12) to initiate a connection. The server then responds with a SYN-ACK packet to the client to

acknowledge the request. Then, the client sends an ACK packet back to complete the connection. After the TCP handshake takes place, the client sends an HTTP GET request to get the alice.txt information. Once this request is sent, the server responds with file data. Following the full data transmission, the server sends an HTTP OK response to indicate a successful data transfer. Finally, the client sends the server an ACK to acknowledge the success followed by a FIN-ACK packet to end the connection. The server responds with an ACK.

Part C

1. Compared to Part B, there is more network traffic because of the DNS packets. DNS packets must be transmitted before the TCP and HTTP packets.
2. 

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src == 128.119.245.12 || ip.dst == 128.119.245.12 || dns

No.	Time	Source	Destination	Protocol	Length	Info
112	3.262867	10.126.223.230	10.40.73.73	DNS	101	Standard query 0xed25 HTTPS word-edit.officeapps.live.com
114	3.263020	10.126.223.230	10.40.73.73	DNS	101	Standard query 0xbd55 A word-edit.officeapps.live.com
118	3.263087	10.126.223.230	10.40.73.73	DNS	106	Standard query 0xd0e0 A word-telemetry.officeapps.live.com
122	3.263179	10.126.223.230	10.40.73.73	DNS	106	Standard query 0x4411 HTTPS word-telemetry.officeapps.live.com
124	3.263254	10.126.223.230	10.40.73.73	DNS	98	Standard query 0x08f4 HTTPS 7pdrvq9vj4n5.statuspage.io
126	3.263321	10.126.223.230	10.40.73.73	DNS	98	Standard query 0x2902 A 7pdrvq9vj4n5.statuspage.io
140	3.271026	10.40.73.73	10.126.223.230	DNS	347	Standard query response 0xed25 HTTPS word-edit.officeapps.live.com CNAME word-edit-geo.wac.trafficmanager.net CNAME word-edit.w…
141	3.271026	10.40.73.73	10.126.223.230	DNS	319	Standard query response 0xbd55 A word-edit.officeapps.live.com CNAME word-edit-geo.wac.trafficmanager.net CNAME word-edit.wac.t…
144	3.271026	10.40.73.73	10.126.223.230	DNS	215	Standard query response 0xd0e0 A word-telemetry.officeapps.live.com CNAME word-telemetry.wac.trafficmanager.net CNAME pgtus4-wo…
145	3.271026	10.40.73.73	10.126.223.230	DNS	212	Standard query response 0x08f4 HTTPS 7pdrvq9vj4n5.statuspage.io CNAME elb-status-us.statuspage.io SOA ns-951.awsdns-54.net
147	3.271560	10.40.73.73	10.126.223.230	DNS	192	Standard query response 0x2902 A 7pdrvq9vj4n5.statuspage.io CNAME elb-status-us.statuspage.io A 13.33.4.47 A 13.33.4.8 A 13.33.…
148	3.271638	10.40.73.73	10.126.223.230	DNS	283	Standard query response 0x4411 HTTPS word-telemetry.officeapps.live.com CNAME word-telemetry.wac.trafficmanager.net CNAME pgtus…
174	3.277688	10.126.223.230	10.40.73.73	DNS	92	Standard query 0xcfd6 A beacons.gcp.gvt2.com
176	3.277835	10.126.223.230	10.40.73.73	DNS	92	Standard query 0xd50f HTTPS beacons.gcp.gvt2.com
179	3.285071	10.40.73.73	10.126.223.230	DNS	140	Standard query response 0xcfd6 A beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com A 173.194.219.94
182	3.285071	10.40.73.73	10.126.223.230	DNS	192	Standard query response 0xd50f HTTPS beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com SOA ns1.google.com
254	4.205707	10.126.223.230	10.40.73.73	DNS	87	Standard query 0x33f5 A bam.nr-data.net
258	4.207182	10.126.223.230	10.40.73.73	DNS	87	Standard query 0xeb38 HTTPS bam.nr-data.net
263	4.217439	10.40.73.73	10.126.223.230	DNS	187	Standard query response 0x33f5 A bam.nr-data.net CNAME bam.cell.nr-data.net CNAME bam.nr-data.net.cdn.cloudflare.net A 162.247.…
264	4.217439	10.40.73.73	10.126.223.230	DNS	243	Standard query response 0xeb38 HTTPS bam.nr-data.net CNAME bam.cell.nr-data.net CNAME bam.nr-data.net.cdn.cloudflare.net SOA ns…
568	27.656283	10.126.223.230	10.40.73.73	DNS	77	Standard query 0x84c3 A gaia.cs.umass.edu
577	27.673321	10.40.73.73	10.126.223.230	DNS	110	Standard query response 0x84c3 A gaia.cs.umass.edu A 128.119.245.12
579	27.675250	10.126.223.230	128.119.245.12	TCP	74	56152 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=4024001168 TSecr=0 WS=128
580	27.707705	128.119.245.12	10.126.223.230	TCP	66	80 → 56152 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1250 SACK_PERM WS=128
581	27.708199	10.126.223.230	128.119.245.12	TCP	54	56152 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0
582	27.708560	10.126.223.230	128.119.245.12	HTTP	140	GET /wireshark-labs/alice.txt HTTP/1.1
584	27.767296	128.119.245.12	10.126.223.230	TCP	54	80 → 56152 [ACK] Seq=1 Ack=87 Win=29312 Len=0
586	27.790853	128.119.245.12	10.126.223.230	TCP	1304	80 → 56152 [ACK] Seq=1 Ack=87 Win=29312 Len=1250 [TCP PDU reassembled in 770]
587	27.790853	128.119.245.12	10.126.223.230	TCP	1304	80 → 56152 [ACK] Seq=1251 Ack=87 Win=29312 Len=1250 [TCP PDU reassembled in 770]
588	27.790853	128.119.245.12	10.126.223.230	TCP	1304	80 → 56152 [ACK] Seq=2501 Ack=87 Win=29312 Len=1250 [TCP PDU reassembled in 770]
589	27.792877	128.119.245.12	10.126.223.230	TCP	1304	80 → 56152 [ACK] Seq=3751 Ack=87 Win=29312 Len=1250 [TCP PDU reassembled in 770]
590	27.792877	128.119.245.12	10.126.223.230	TCP	1304	80 → 56152 [ACK] Seq=5001 Ack=87 Win=29312 Len=1250 [TCP PDU reassembled in 770]
591	27.793095	10.126.223.230	128.119.245.12	TCP	54	56152 → 80 [ACK] Seq=87 Ack=3751 Win=62848 Len=0
592	27.793100	128.119.245.12	10.126.223.230	TCP	1304	80 → 56152 [ACK] Seq=6251 Ack=87 Win=29312 Len=1250 [TCP PDU reassembled in 770]
593	27.793943	10.126.223.230	128.119.245.12	TCP	54	56152 → 80 [ACK] Seq=87 Ack=7501 Win=60288 Len=0
594	27.808562	128.119.245.12	10.126.223.230	TCP	1304	80 → 56152 [ACK] Seq=7501 Ack=87 Win=29312 Len=1250 [TCP PDU reassembled in 770]

Since the DNS cache had been flushed, the web server's IP address was no longer in the cache for easy retrieval. Before requests and acknowledgements can be sent back and forth between the client and the server, the server's IP address needs to be known. Because that information was no longer in the DNS cache, the client had to get that information, which was requested in DNS

packet 568 and received in packet 577. These DNS packets are just resolving unknown web IP addresses before connection and data transfer.