

LAB SESSION 2 Packet Analysis with Wireshark

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.

Steps:

- > Start capturing packets
- > Visit <http://scratchpads.org/explore/sites-list>
- > Stop capturing packets
- > Filter by http

The image shows a Wireshark packet capture of an HTTP session. The top pane displays a list of captured packets, with the first packet (No. 202) selected. The middle pane shows the details of this packet, including the Ethernet II header, Internet Protocol Version 4 header, and the Hypertext Transfer Protocol header. The bottom pane shows the raw packet data in hexadecimal and ASCII format.

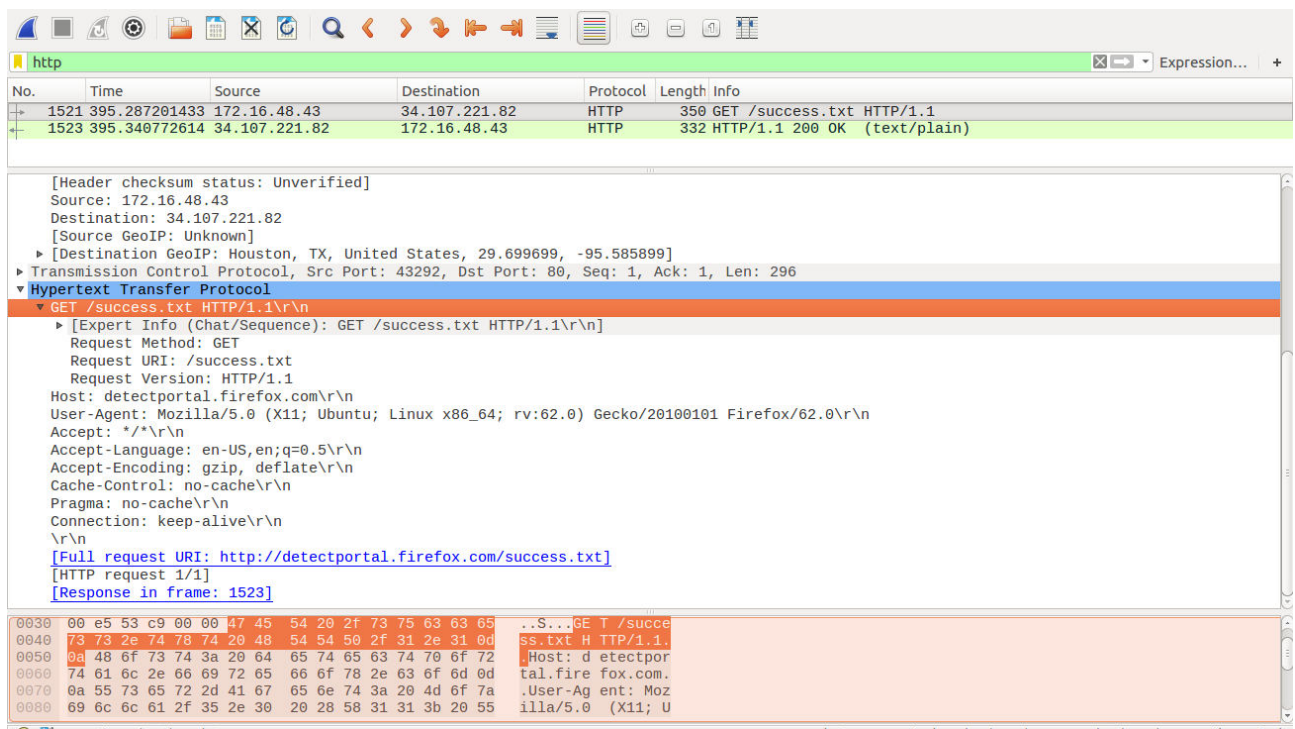
No.	Time	Source	Destination	Protocol	Length	Info
202	8.508108926	172.16.48.43	157.140.2.32	HTTP	395	GET /explore/sites-list HTTP/1.1
226	8.981162852	172.16.48.43	157.140.2.32	HTTP	366	GET /css/main.css HTTP/1.1
232	8.981594534	172.16.48.43	157.140.2.32	HTTP	366	GET /css/page.css HTTP/1.1
247	9.144693802	157.140.2.32	172.16.48.43	HTTP	1406	HTTP/1.1 200 OK (text/html)
250	9.422504326	157.140.2.32	172.16.48.43	HTTP	2714	HTTP/1.1 200 OK (text/css)
252	9.424648882	157.140.2.32	172.16.48.43	HTTP	2357	HTTP/1.1 200 OK (text/css)
254	9.425049667	172.16.48.43	157.140.2.32	HTTP	367	GET /assets/logo/logo-explore.png HTTP/1.1
255	9.425152763	172.16.48.43	157.140.2.32	HTTP	369	GET /assets/sidebar/flesh-202px.png HTTP/1.1
257	9.425253935	172.16.48.43	157.140.2.32	HTTP	367	GET /assets/sponsor-logos/ner.png HTTP/1.1
259	9.425376054	172.16.48.43	157.140.2.32	HTTP	372	GET /assets/sponsor-logos/emonocot.png HTTP/1.1
268	9.426138685	172.16.48.43	157.140.2.32	HTTP	371	GET /assets/sponsor-logos/vibrant.png HTTP/1.1
269	9.426236883	172.16.48.43	157.140.2.32	HTTP	370	GET /assets/sponsor-logos/einfra.png HTTP/1.1

Frame 202: 395 bytes on wire (3160 bits), 395 bytes captured (3160 bits) on interface 0
Ethernet II, Src: HewlettP_9f:96:ef (74:46:a0:9f:96:ef), Dst: All-HSRP-routers_30 (00:00:0c:07:ac:30)
Internet Protocol Version 4, Src: 172.16.48.43, Dst: 157.140.2.32
Transmission Control Protocol, Src Port: 58204, Dst Port: 80, Seq: 1, Ack: 1, Len: 341
Hypertext Transfer Protocol

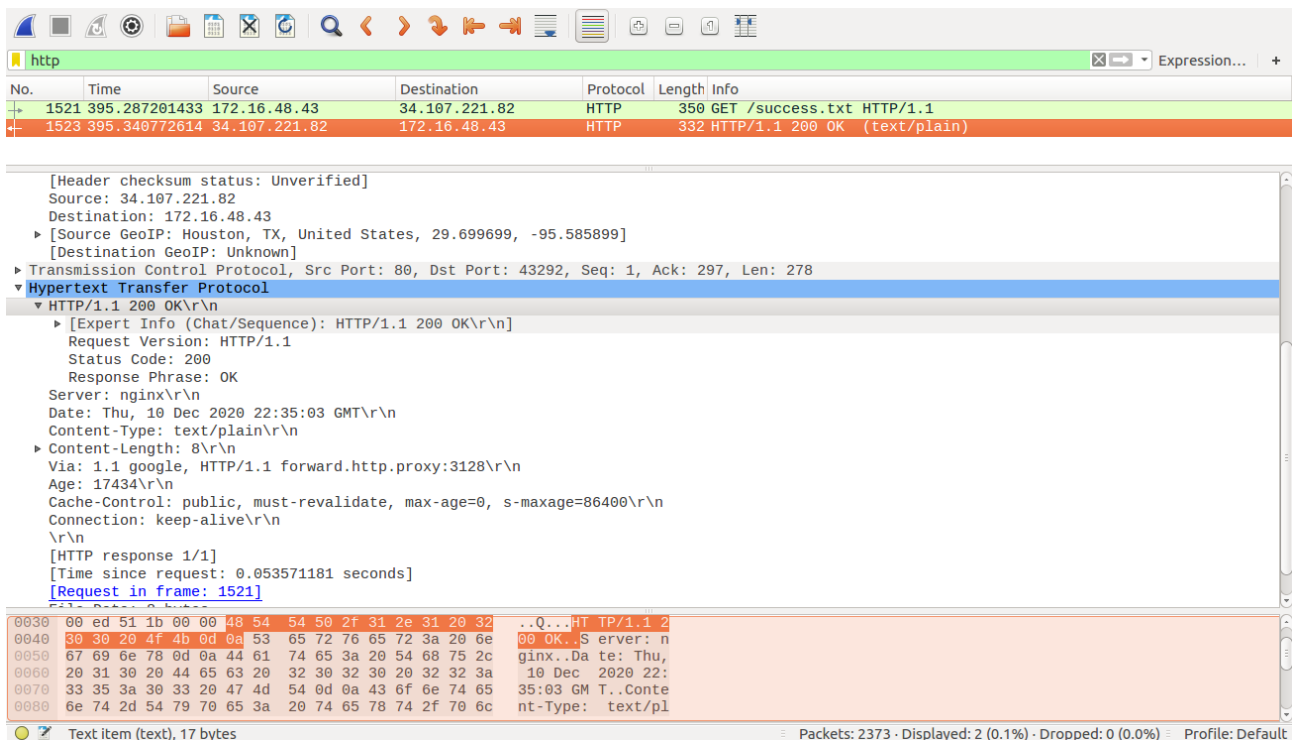
0000 00 00 0c 07 ac 30 74 46 a0 9f 96 ef 08 00 45 000tFE.
0010 01 7d fc 12 40 00 00 06 c1 80 ac 10 30 2b 9d 8c ..}..@.0+..
0020 02 20 e3 5c 00 50 b1 d5 13 71 c2 ba 6b c2 50 18 . .\..P.. .q..k.P..
0030 00 e5 19 75 00 00 47 45 54 20 2f 65 78 70 6c 6f ...u..GE T/explo
0040 72 65 2f 73 69 74 65 73 2d 6c 69 73 74 20 48 54 re/sites -list HT
0050 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 73 63 TP/1.1.. Host: sc
0060 72 61 74 63 68 70 61 64 73 2e 6f 72 67 0d 0a 55 ratchpad s.org..U
0070 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c ser-Agen t: Mozil
0080 6c 61 2f 35 2e 30 20 28 58 31 31 3b 20 55 62 75 la/5.0 (X11; Ubu
0090 6e 74 75 3b 20 4c 69 6e 75 78 20 78 38 36 5f 36 ntu; Lin ux x86_6
00a0 34 3b 20 72 76 3a 36 32 2e 30 29 20 47 65 63 6b 4; rv:62 .0) Geck
00b0 6f 2f 32 30 31 30 30 31 30 31 20 46 69 72 65 66 o/201001 01 Firef

Ethernet (eth), 14 bytes Packets: 1536 · Displayed: 30 (2.0%) Profile: Default

Http Request:



Http Response:



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.

Steps:

- > Set up ftp client and server
- > Start capturing packets
- > Connect with a ftp server
- > Stop capturing packets
- > Filter ftp
- > Filter tcp.port==20 (for data connection)
- > Filter tcp.port==21 (for control connection)

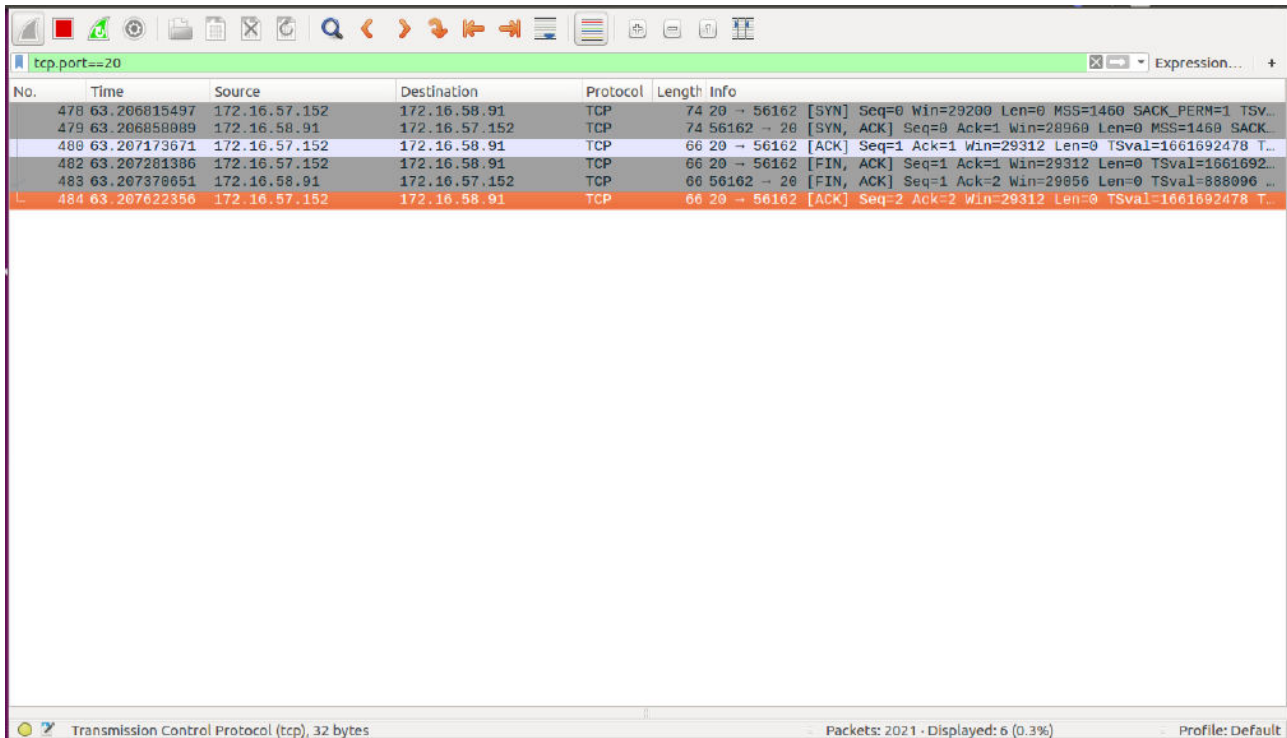
FTP:

Wireshark packet capture showing an FTP session. The filter is 'ftp'. The packet list shows several packets, including a '220 Welcome to DEPARTMENT OF CSE, MIT MANIPAL FTP service.\r\n' packet. The packet details pane shows the 'File Transfer Protocol (FTP)' section expanded, displaying the '220 Welcome to DEPARTMENT OF CSE, MIT MANIPAL FTP service.\r\n' message. The packet bytes pane shows the raw data of the packet.

tcp.port==21 (control connection):

Wireshark packet capture showing an FTP session. The filter is 'tcp.port==21'. The packet list shows several packets, including a '215 UNIX Type: L8\r\n' packet. The packet details pane shows the 'File Transfer Protocol (FTP)' section expanded, displaying the '215 UNIX Type: L8\r\n' message. The packet bytes pane shows the raw data of the packet.

tcp.port==20 (data connection):



The image shows a Wireshark packet capture for the TCP port 20 filter. The packet list shows several packets, with the selected packet (No. 484) being a TCP ACK from 172.16.57.152 to 172.16.58.91. The packet details pane shows the TCP header information.

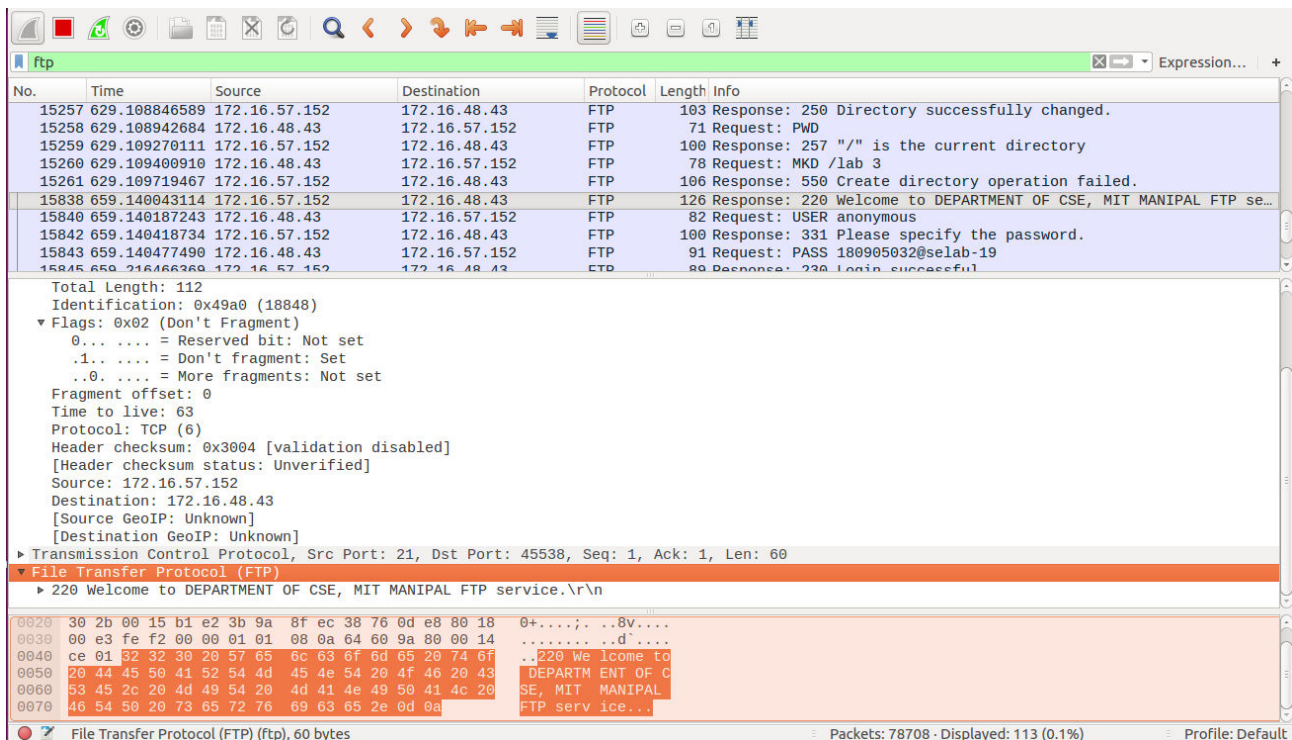
No.	Time	Source	Destination	Protocol	Length	Info
478	63.206815497	172.16.57.152	172.16.58.91	TCP	74	20 → 56162 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSv...
479	63.206858089	172.16.58.91	172.16.57.152	TCP	74	56162 → 20 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK...
480	63.207173671	172.16.57.152	172.16.58.91	TCP	66	20 → 56162 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1661692478 T...
482	63.207281386	172.16.57.152	172.16.58.91	TCP	66	20 → 56162 [FIN, ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1661692...
483	63.207370651	172.16.58.91	172.16.57.152	TCP	66	56162 → 20 [FIN, ACK] Seq=1 Ack=2 Win=20856 Len=0 TSval=888096 ...
484	63.207622356	172.16.57.152	172.16.58.91	TCP	66	20 → 56162 [ACK] Seq=2 Ack=2 Win=29312 Len=0 TSval=1661692478 T...

Transmission Control Protocol (tcp), 32 bytes

Packets: 2021 - Displayed: 6 (0.3%)

Profile: Default

Not safe – transaction is plain text:



The image shows a Wireshark packet capture for the FTP filter. The packet list shows several packets, with the selected packet (No. 15845) being an FTP response. The packet details pane shows the FTP header information.

No.	Time	Source	Destination	Protocol	Length	Info
15257	629.108846589	172.16.57.152	172.16.48.43	FTP	103	Response: 250 Directory successfully changed.
15258	629.108942684	172.16.48.43	172.16.57.152	FTP	71	Request: PWD
15259	629.109270111	172.16.57.152	172.16.48.43	FTP	100	Response: 257 "/" is the current directory
15260	629.109400910	172.16.48.43	172.16.57.152	FTP	78	Request: MKD /lab 3
15261	629.109719467	172.16.57.152	172.16.48.43	FTP	106	Response: 550 Create directory operation failed.
15838	659.140043114	172.16.57.152	172.16.48.43	FTP	126	Response: 220 Welcome to DEPARTMENT OF CSE, MIT MANIPAL FTP se...
15840	659.140187243	172.16.48.43	172.16.57.152	FTP	82	Request: USER anonymous
15842	659.140418734	172.16.57.152	172.16.48.43	FTP	100	Response: 331 Please specify the password.
15843	659.140477490	172.16.48.43	172.16.57.152	FTP	91	Request: PASS 180905032@selab-19
15845	659.216466369	172.16.57.152	172.16.48.43	FTP	88	Response: 230 Login successful

Total Length: 112
Identification: 0x49a0 (18848)
▼ Flags: 0x02 (Don't Fragment)
0... .. = Reserved bit: Not set
.1... .. = Don't fragment: Set
..0... .. = More fragments: Not set
Fragment offset: 0
Time to live: 63
Protocol: TCP (6)
Header checksum: 0x3004 [validation disabled]
[Header checksum status: Unverified]
Source: 172.16.57.152
Destination: 172.16.48.43
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
► Transmission Control Protocol, Src Port: 21, Dst Port: 45538, Seq: 1, Ack: 1, Len: 60
▼ File Transfer Protocol (FTP)
► 220 Welcome to DEPARTMENT OF CSE, MIT MANIPAL FTP service.\r\n

0020 30 2b 00 15 b1 e2 3b 9a 8f ec 38 76 0d e8 80 18 0+...;. ..8v...
0030 00 e3 fe f2 00 00 01 01 08 0a 64 60 9a 80 00 14d'...
0040 ce 01 32 32 30 20 57 65 6c 63 6f 6d 65 20 74 6f ..220 We lcome to
0050 20 44 45 50 41 52 54 4d 45 4e 54 20 4f 46 20 43 DEPARTM ENT OF C
0060 53 45 2c 20 4d 49 54 20 4d 41 4e 49 50 41 4c 20 SE, MIT MANIPAL
0070 46 54 50 20 73 65 72 76 69 63 65 2e 0d 0a FTP serv ice...

File Transfer Protocol (FTP) (ftp), 60 bytes

Packets: 78708 - Displayed: 113 (0.1%)

Profile: Default

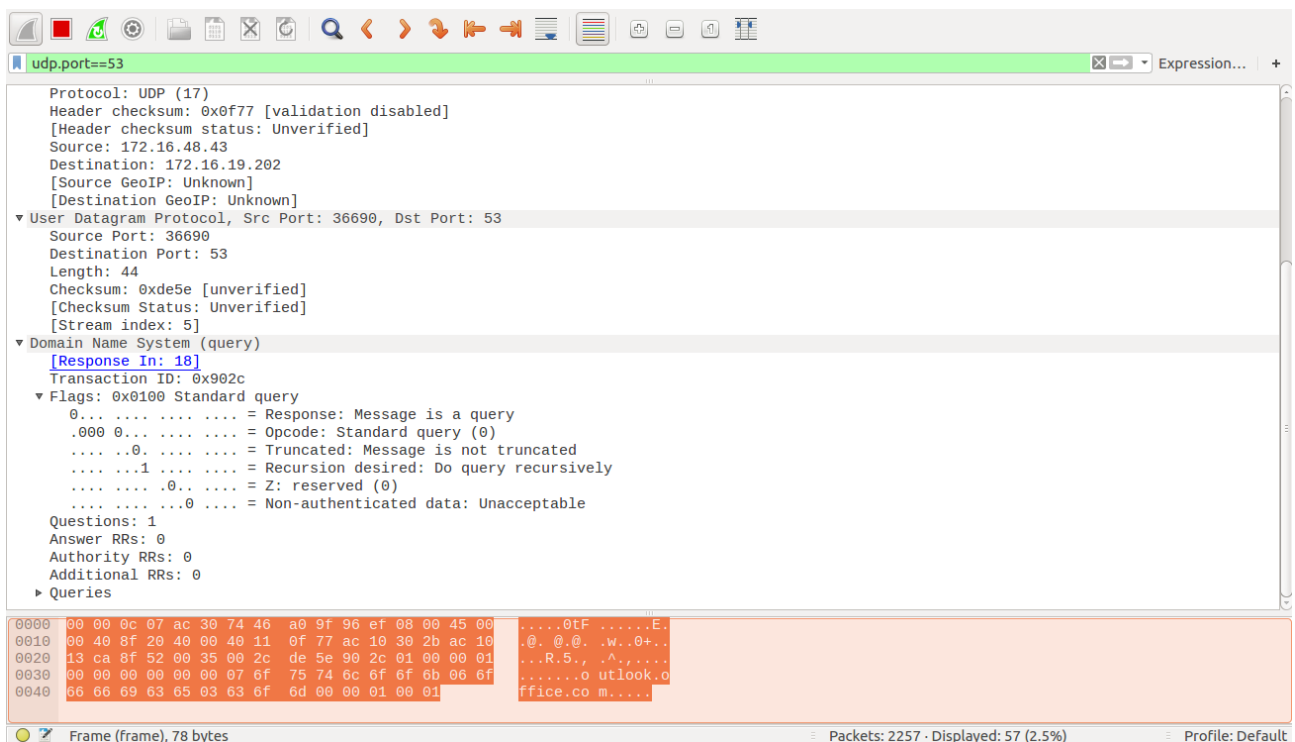
3. Analyze the behavior of the DNS protocol. In addition to Wireshark, several network utilities are available for finding some information stored in the DNS

servers. Use dig utilities (which has replaced nslookup). Set Wireshark to capture the packets sent by this utility.

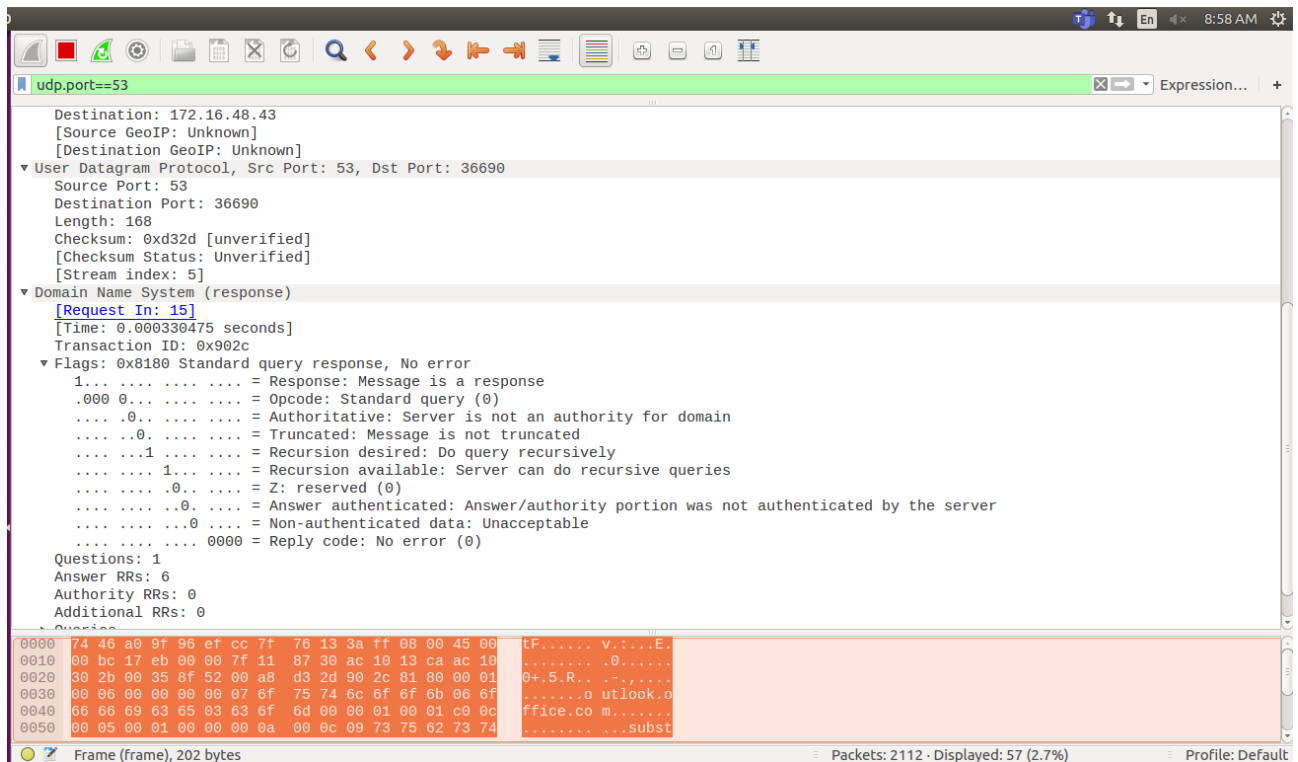
Steps:

- > Start capturing packets
- > Type nslookup en.wikiversity.org
- > Stop capturing
- > Filter udp.port == 53

DNS query:



DNS response:



DNS packets:

