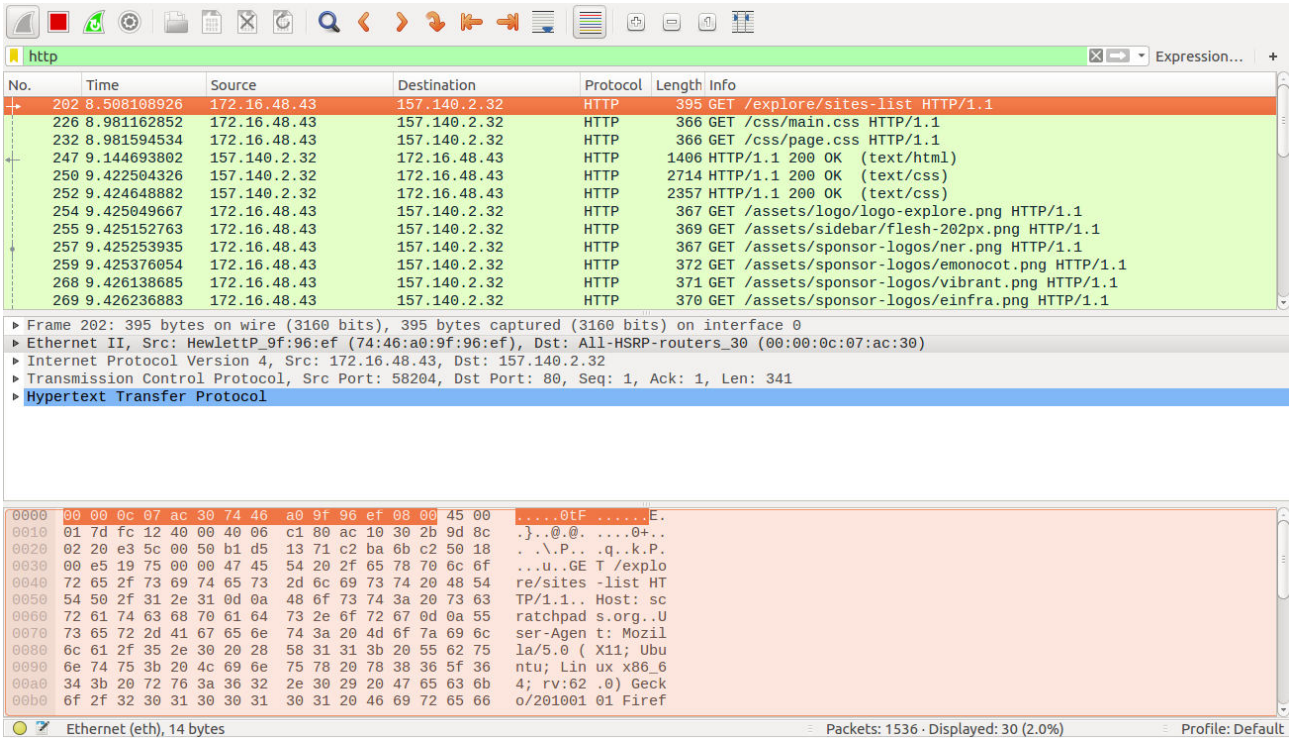
LAB SESSION 2 Packet Analysis with Wireshark

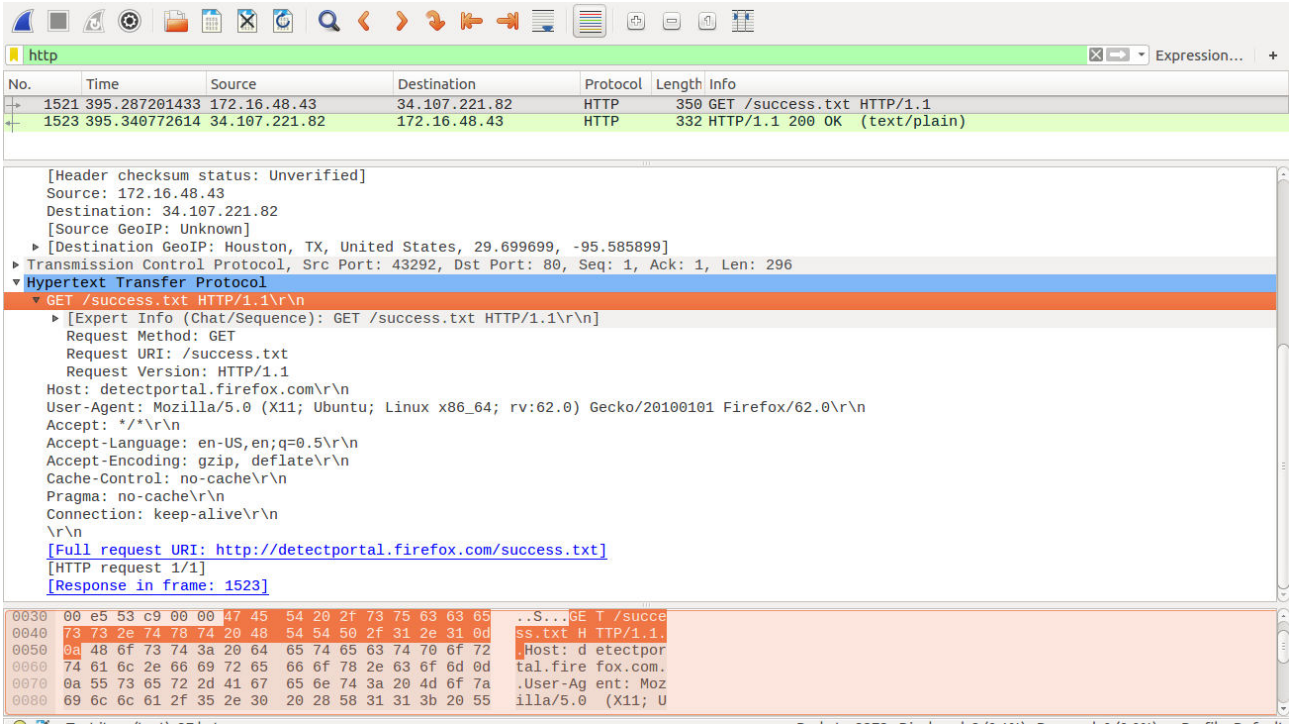
1. Retrieve web pages using HTTP. Use Wireshark to capture packets for analysis. Learn about most common HTTP messages . Also capture response messages and analyze them. During the lab session, also examine and analyze some HTTP headers.

Steps:

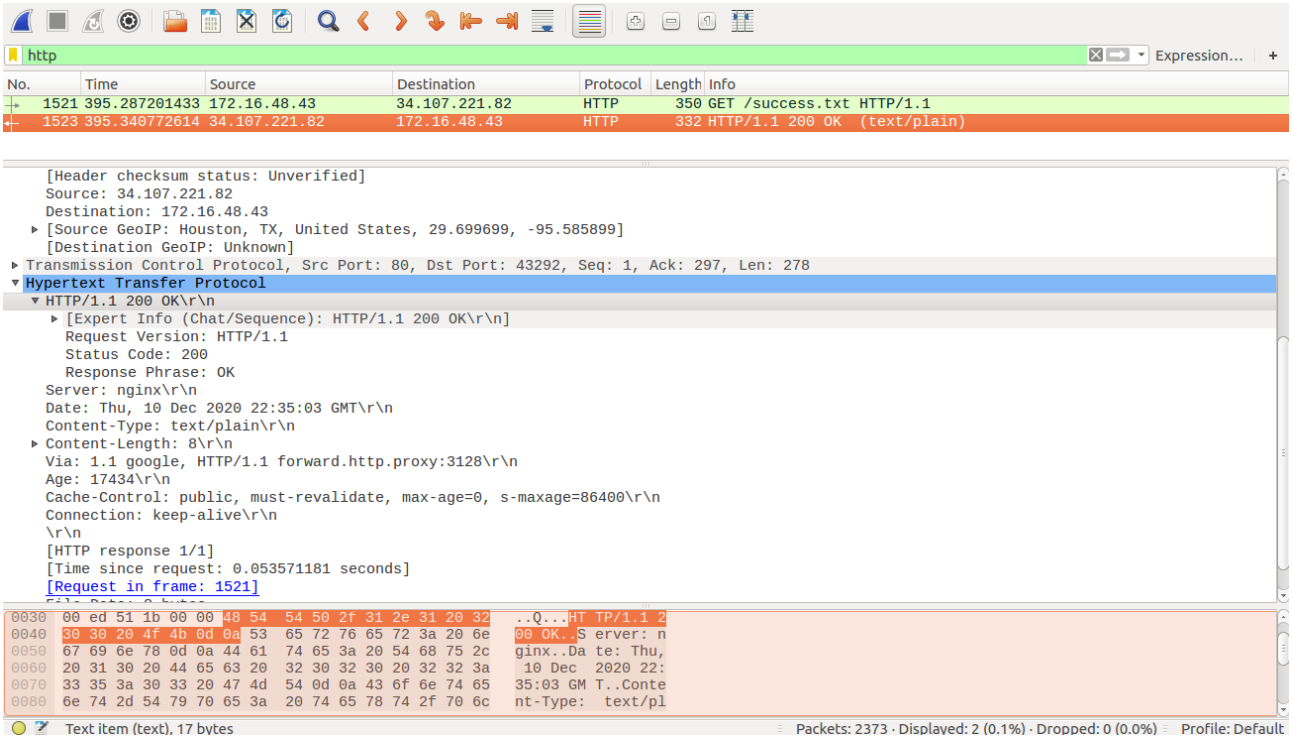
-> Start capturing packets
-> Visit http://scratchpads.org/explore/sites-list
-> Stop capturing packets
-> Filter by http



Http Request:



Http Response:

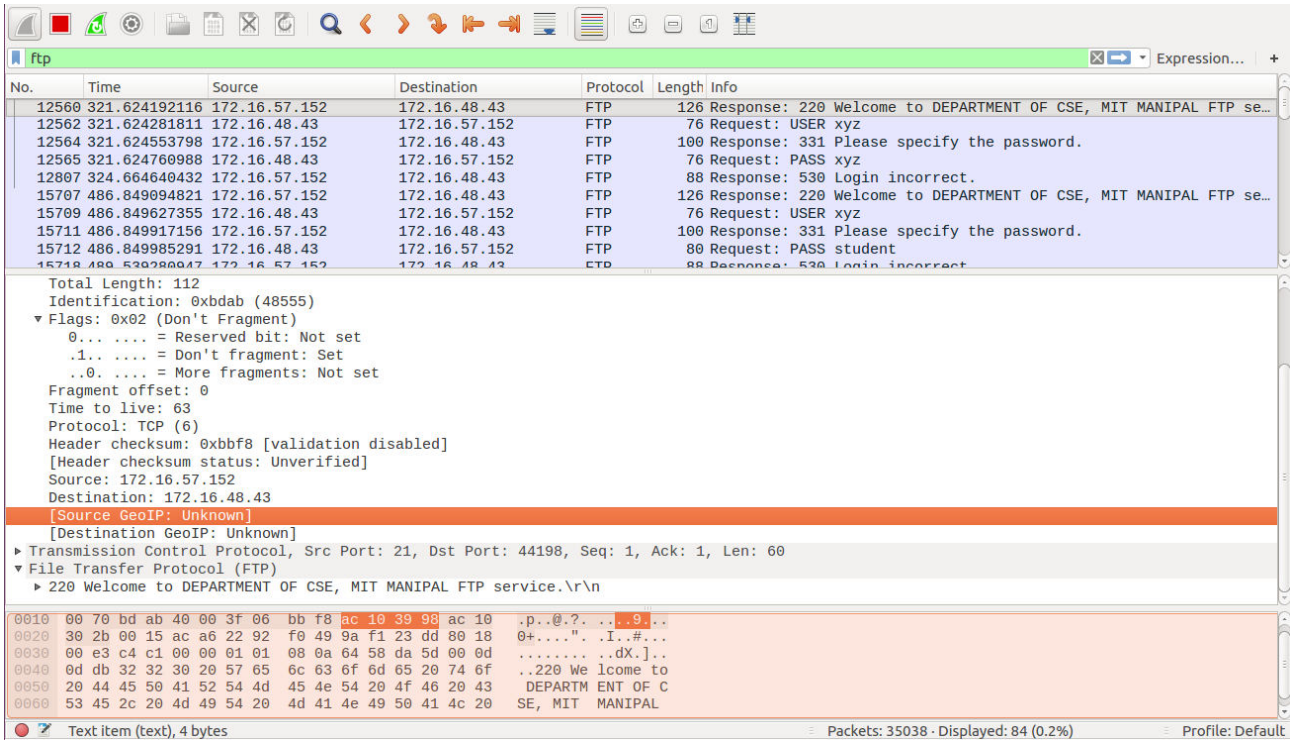


2. Use FTP to transfer some files, Use Wireshark to capture some packets. Show that FTP uses two separate connections: a control connection and a data-transfer connection. The data connection is opened and closed for each file transfer activity. Also show that FTP is an insecure file transfer protocol because the transaction is done in plaintext.

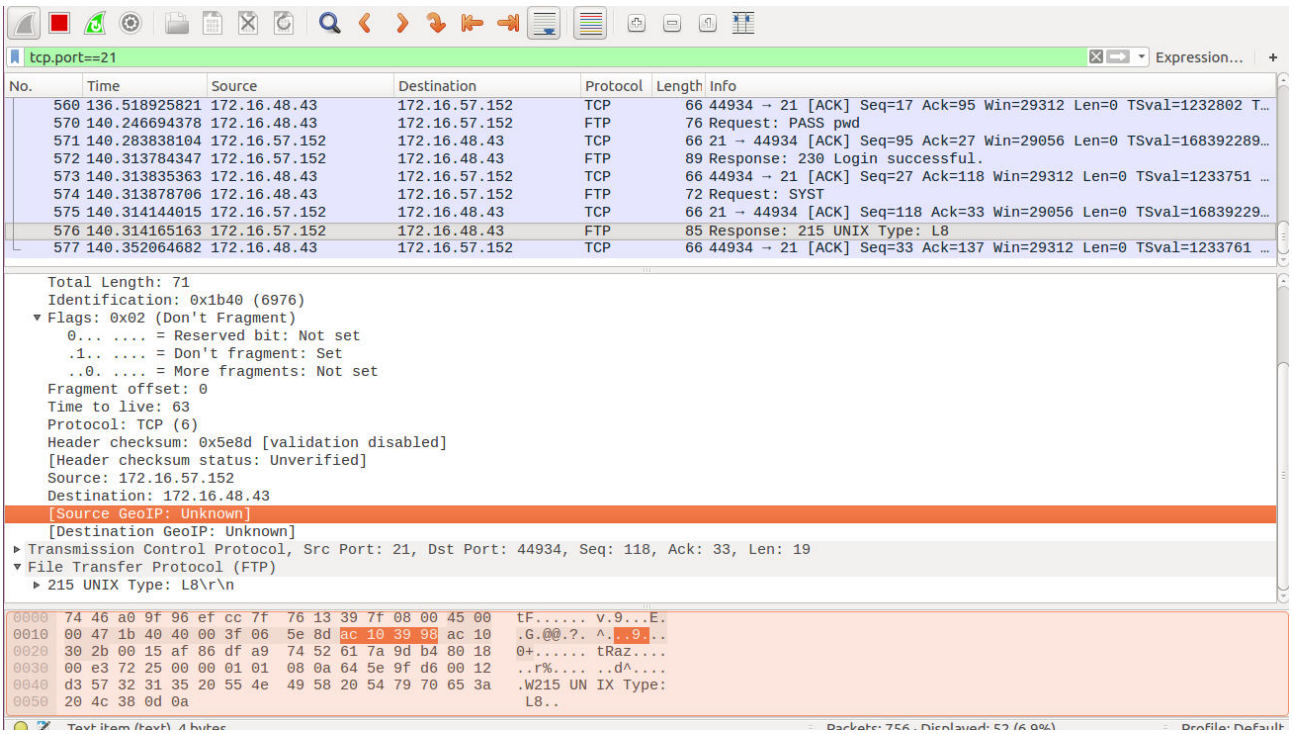
Steps:

-> 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)

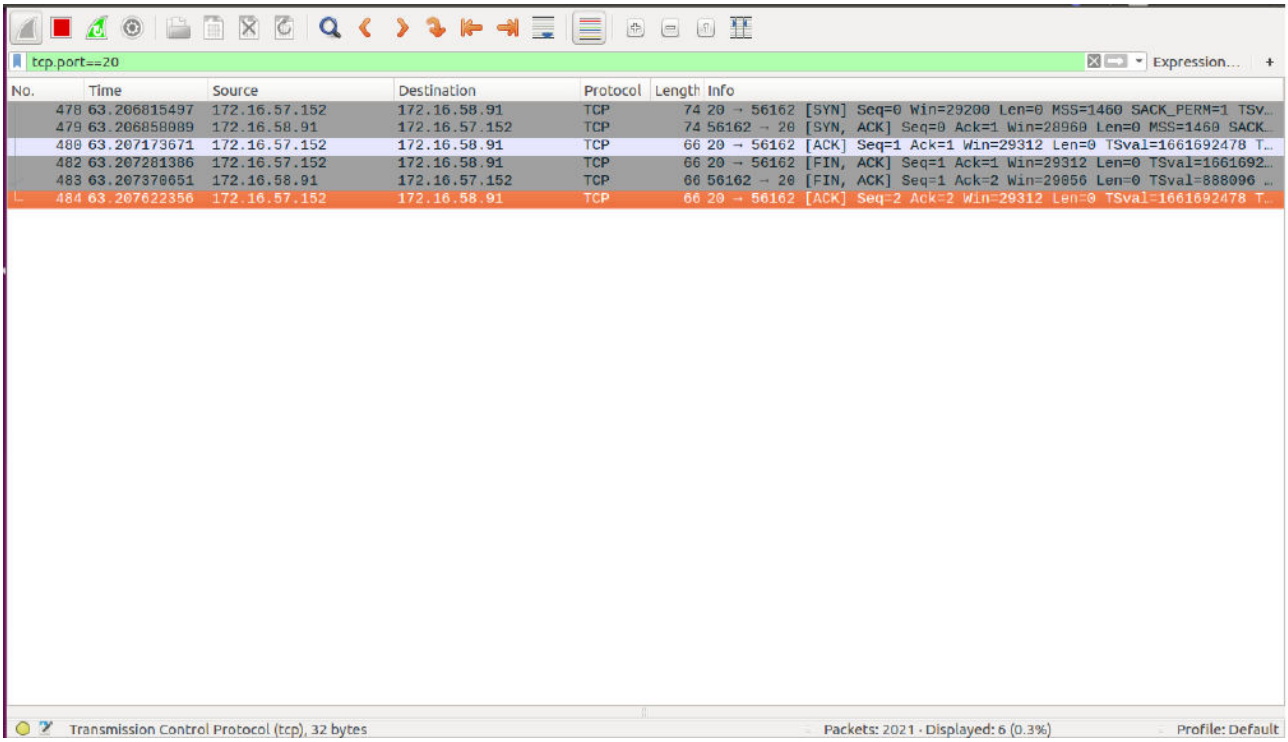
FTP:



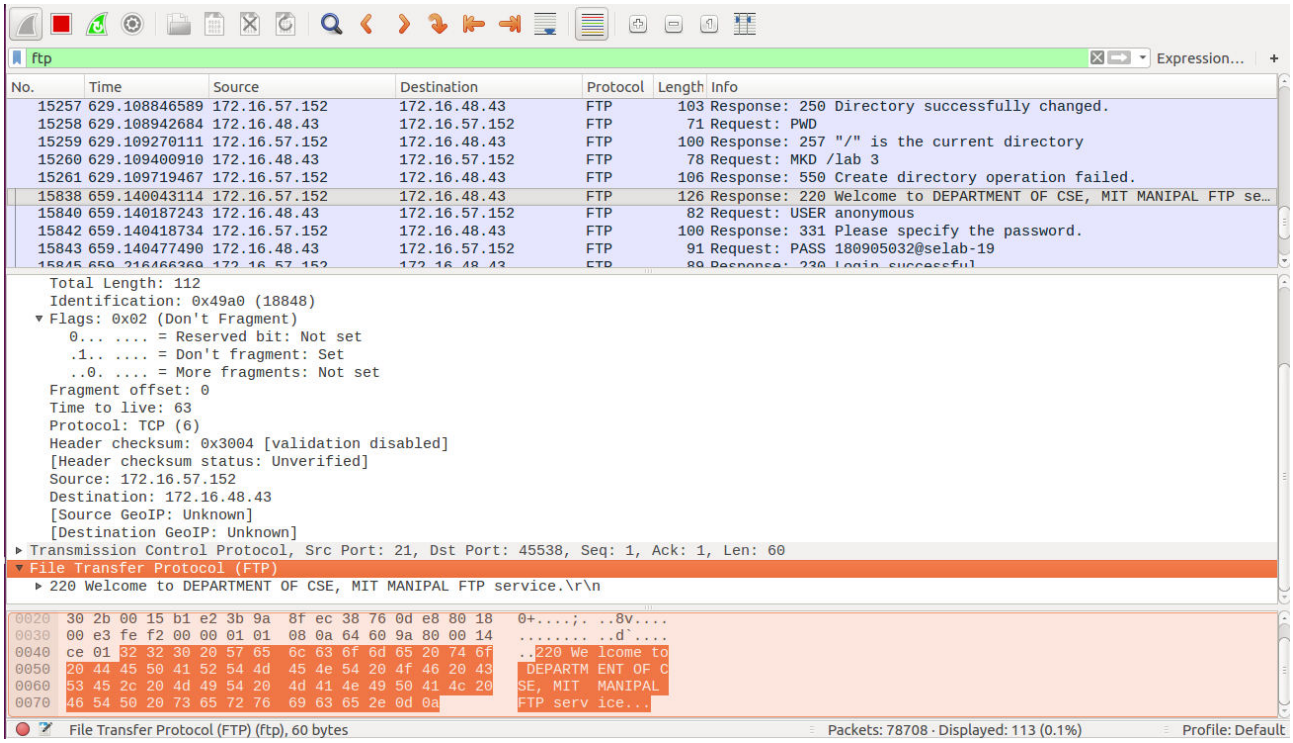
tcp.port==21 (control connection):



tcp.port==20 (data connection):



Not safe – transaction is plain text:

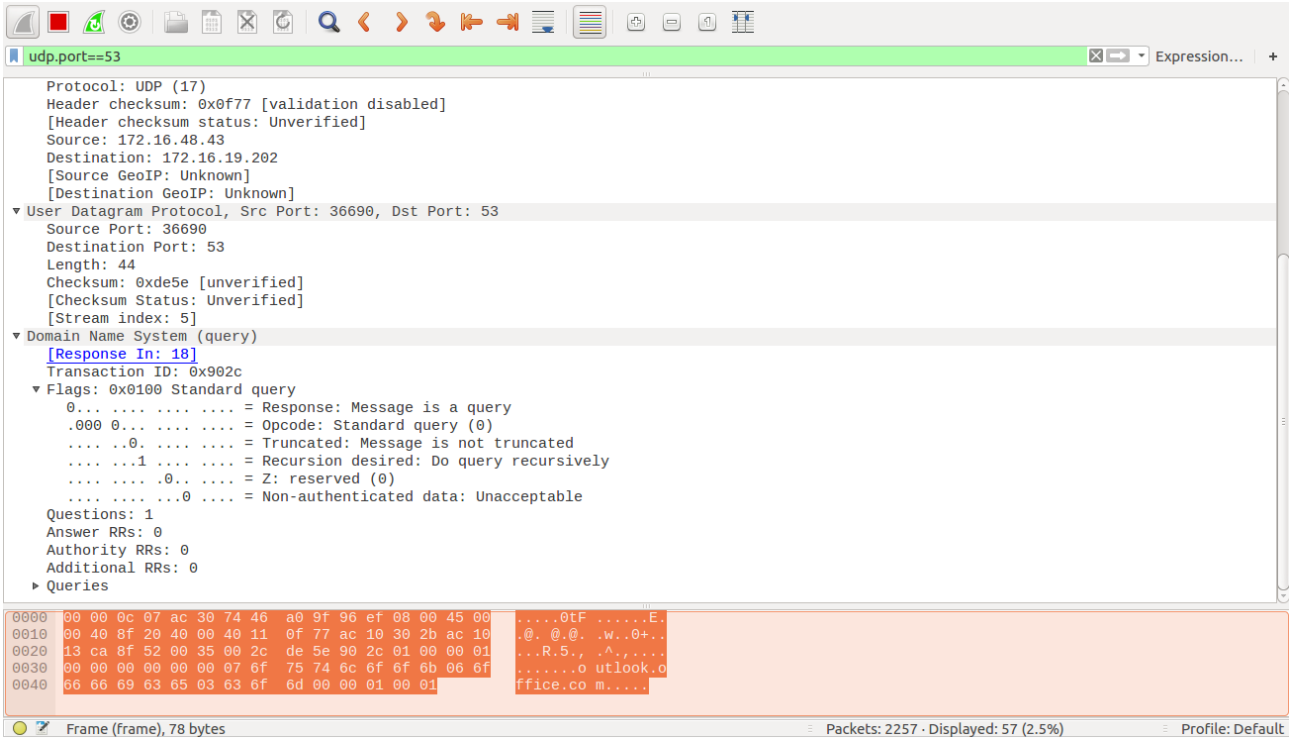


3. Analyze the behavior of the DNS protocol. In addition to Wireshark, s everal network utilities are available for finding some information stored in the DNS

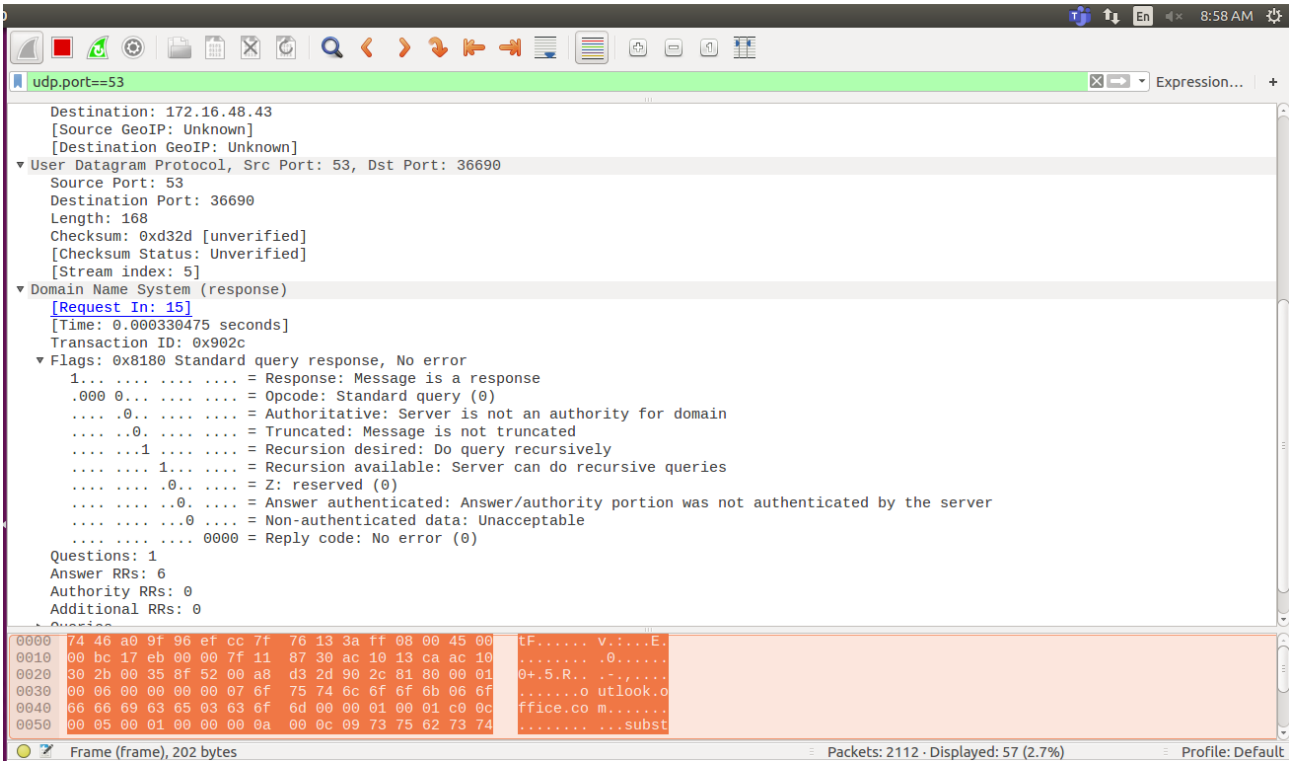
servers. Use dig utilities (which has replaced nslookup). Set Wireshark to capture the packets sent by this utility.

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

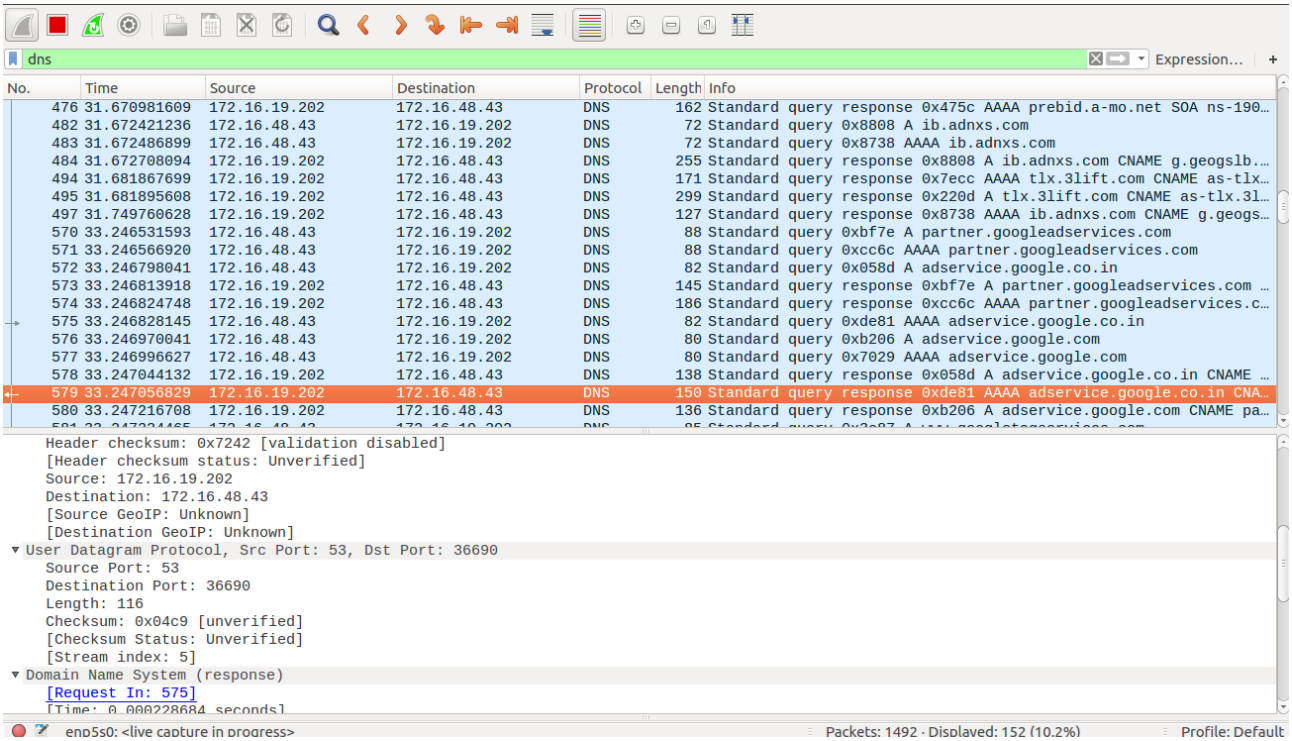
DNS query:



DNS response:


udp.port==53
Expression...
Destination: 172.16.48.43
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: 53, Dst Port: 36690
Source Port: 53
Destination Port: 36690
Length: 168
Checksum: 0xd32d [unverified]
[Checksum Status: Unverified]
[Stream index: 5]
Domain Name System (response)
[Request In: 15]
[Time: 0.000330475 seconds]
Transaction ID: 0x902c
Flags: 0x8180 Standard query response, No error
1... .... = Response: Message is a response
.000 0... .... = Opcode: Standard query (0)
.... .0.. .... = Authoritative: Server is not an authority for domain
.... ..0. .... = Truncated: Message is not truncated
....1 .... = Recursion desired: Do query recursively
.... 1... .... = Recursion available: Server can do recursive queries
.... .0.. .... = Z: reserved (0)
....0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 .... = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 6
Authority RRs: 0
Additional RRs: 0
0000 74 46 a0 9f 96 ef cc 7f 76 13 3a ff 08 00 45 00 tF..... v.:...E.
0010 00 bc 17 eb 00 00 7f 11 87 30 ac 10 13 ca ac 10 ..... .0.....
0020 30 2b 00 35 8f 52 00 a8 d3 2d 90 2c 81 80 00 01 0+.5.R.. .-.,....
0030 00 06 00 00 00 00 07 6f 75 74 6c 6f 6f 6b 06 6f .....o utlook.o
0040 66 66 69 63 65 03 63 6f 6d 00 00 01 00 01 c0 0c ffice.co m.....
0050 00 05 00 01 00 00 00 0a 00 0c 09 73 75 62 73 74 ....subst
Frame (frame), 202 bytes
Packets: 2112 · Displayed: 57 (2.7%)
Profile: Default

DNS packets:


dns
Expression...
No. Time Source Destination Protocol Length Info
476 31.670981609 172.16.19.202 172.16.48.43 DNS 162 Standard query response 0x475c AAAA prebid.a-mo.net SOA ns-190…
482 31.672421236 172.16.48.43 172.16.19.202 DNS 72 Standard query 0x8808 A ib.adnxs.com
483 31.672486899 172.16.48.43 172.16.19.202 DNS 72 Standard query 0x8738 AAAA ib.adnxs.com
484 31.672708094 172.16.19.202 172.16.48.43 DNS 255 Standard query response 0x8808 A ib.adnxs.com CNAME g.geogslb.…
494 31.681867699 172.16.19.202 172.16.48.43 DNS 171 Standard query response 0x7ecc AAAA tlx.3lift.com CNAME as-tlx…
495 31.681895608 172.16.19.202 172.16.48.43 DNS 299 Standard query response 0x220d A tlx.3lift.com CNAME as-tlx.3l…
497 31.749760628 172.16.19.202 172.16.48.43 DNS 127 Standard query response 0x8738 AAAA ib.adnxs.com CNAME g.geogs…
570 33.246531593 172.16.48.43 172.16.19.202 DNS 88 Standard query 0xbf7e A partner.googleadservices.com
571 33.246566920 172.16.48.43 172.16.19.202 DNS 88 Standard query 0xcc6c AAAA partner.googleadservices.com
572 33.246798041 172.16.48.43 172.16.19.202 DNS 82 Standard query 0x058d A adservice.google.co.in
573 33.246813918 172.16.19.202 172.16.48.43 DNS 145 Standard query response 0xbf7e A partner.googleadservices.com …
574 33.246824748 172.16.19.202 172.16.48.43 DNS 186 Standard query response 0xcc6c AAAA partner.googleadservices.c…
575 33.246828145 172.16.48.43 172.16.19.202 DNS 82 Standard query 0xde81 AAAA adservice.google.co.in
576 33.246970041 172.16.48.43 172.16.19.202 DNS 80 Standard query 0xb206 A adservice.google.com
577 33.246996627 172.16.48.43 172.16.19.202 DNS 80 Standard query 0x7029 AAAA adservice.google.com
578 33.247044132 172.16.19.202 172.16.48.43 DNS 138 Standard query response 0x058d A adservice.google.co.in CNAME …
579 33.247056829 172.16.19.202 172.16.48.43 DNS 150 Standard query response 0xde81 AAAA adservice.google.co.in CNA…
580 33.247216708 172.16.19.202 172.16.48.43 DNS 136 Standard query response 0xb206 A adservice.google.com CNAME pa…
Header checksum: 0x7242 [validation disabled]
[Header checksum status: Unverified]
Source: 172.16.19.202
Destination: 172.16.48.43
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: 53, Dst Port: 36690
Source Port: 53
Destination Port: 36690
Length: 116
Checksum: 0x04c9 [unverified]
[Checksum Status: Unverified]
[Stream index: 5]
Domain Name System (response)
[Request In: 575]
enp5s0: <live capture in progress>
Packets: 1492 · Displayed: 152 (10.2%)
Profile: Default