Name: Atish Kumar
Roll No: 120CS0173
Date: 12 Jan,2023

Q1: Answer the following questions for captured file http.pcap (HTTP Protocol)

1. **List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.**

Soln:

-TCP(Transmission Control)
-DNS (Domain Name System)

-ARP(Address Resolution Protocol)

2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time DisplayFormat, then select Time-of-day.

Soln:

HTTP GET request time-12:47:55.414218
HTTP OK time-12:47:56.18899

time duration-0.774772 s

3. What is the Internet address of iitd.ac.in? What is the Internet address of your computer?

Soln: 192.168.43.1 (iitd.ac.in)

192.168.43.153 (My Computer Internet Address)

4. Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select Printfrom the Wireshark

Filecommand menu, and select the "SelectedPacketOnly" and "Printasdisplayed" radial buttons, and then click OK.

Soln:

GET

/home/nit/Downloads/http.pcap 773 total packets, 194 shownNo.
Time
Source
Destinatio
n

Protocol Length Info
9 12:47:55.414218

192.168.43.153

103.27.9.20
HTTP
491
GET / HTTP/1.1

Frame 9: 491 bytes on wire (3928 bits), 491 bytes captured (3928 bits)
Encapsulation type: Ethernet (1)
Arrival Time: Jul 29, 2017 12:47:55.414218000 IST

[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1501312675.414218000 seconds
[Time delta from previous captured frame: 0.000104000 seconds][Time delta from previous displayed frame: 0.000000000 seconds][Time since reference or first frame: 4.076601000 seconds]
Frame Number: 9

Frame Length: 491 bytes (3928 bits)
Capture Length: 491 bytes (3928 bits)
[Frame is marked: False]
[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:tcp:http]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]

Ethernet II, Src: HonHaiPr_8c:90:55 (e0:06:e6:8c:90:55), Dst: XiaomiCo_9e:9c:c3 (ac:c1:ee:9e:9c:c3)
Internet Protocol Version 4, Src: 192.168.43.153, Dst: 103.27.9.20

Transmission Control Protocol, Src Port: 34574, Dst Port: 80, Seq: 1, Ack: 1, Len: 425
Source Port: 34574
Destination Port: 80
[Stream index: 1]
[Conversation completeness: Complete, WITH_DATA (31)][TCP Segment Len: 425]
Sequence Number: 1
(relative sequence number)

Sequence Number (raw): 3262819859
[Next Sequence Number: 426
(relative sequence number)]

Acknowledgment Number: 1
(relative ack number)

Acknowledgment number (raw): 898238161
1000 ..... = Header Length: 32 bytes (8)

Flags: 0x018 (PSH, ACK)

Window: 115

[Calculated window size: 14720]
[Window size scaling factor: 128]
Checksum: 0x0c62 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps[Timestamps]

[SEQ/ACK analysis]
TCP payload (425
bytes)

Hypertext Transfer Protocol
GET / HTTP/1.1\r\n

Host: www.iitd.ac.in\r\n

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:18.0) Gecko/20100101 Firefox/18.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n

Accept-Encoding: gzip, deflate\r\n

Cookie: SESS1f002926bf876664ed5383994cb4c1de=tunjfm6na70hvls5sh989n7cl2; has_js=1\r\n
Connection: keep-alive\r\n

If-Modified-Since: Sat, 29 Jul 2017 07:16:24 GMT\r\n
\r\n
[Full request URI: http://www.iitd.ac.in/]
[HTTP request 1/9]
[Response in frame: 32] [Next request in frame: 34]OK

/home/nit/Downloads/http.pcap 773 total packets, 194 shownNo.
Time
Source
Destinatio
n

Protocol Length Info
32 12:47:56.188990

103.27.9.20

192.168.43.153
HTTP
945
HTTP/1.1 200

OK (text/html)
Frame 32: 945 bytes on wire (7560 bits), 945 bytes captured (7560 bits)
Encapsulation type: Ethernet (1)
Arrival Time: Jul 29, 2017 12:47:56.188990000 IST

[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1501312676.188990000 seconds
[Time delta from previous captured frame: 0.003258000 seconds] [Time delta from previous displayed frame: 0.017152000 seconds][Time since reference or first frame: 4.851373000 seconds]
Frame Number: 32

Frame Length: 945 bytes (7560 bits)
Capture Length: 945 bytes (7560 bits)
[Frame is marked: False]
[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]

Ethernet II, Src: XiaomiCo_9e:9c:c3 (ac:c1:ee:9e:9c:c3), Dst: HonHaiPr_8c:90:55 (e0:06:e6:8c:90:55)
Internet Protocol Version 4, Src: 103.27.9.20, Dst: 192.168.43.153

Transmission Control Protocol, Src Port: 80, Dst Port: 34574, Seq: 8737, Ack: 426, Len:879
Source Port: 80

Destination Port: 34574
[Stream index: 1]
[Conversation completeness: Complete, WITH_DATA (31)][TCP Segment Len: 879]
Sequence Number: 8737
(relative sequence number)

Sequence Number (raw): 898246897
[Next Sequence Number: 9616
(relative sequence number)]
Acknowledgment Number: 426
(relative ack number)

Acknowledgment number (raw): 3262820284
1000 ..... = Header Length: 32 bytes (8)

Flags: 0x018 (PSH, ACK)

Window: 122
[Calculated window size: 15616]
[Window size scaling factor: 128]Checksum: 0x595d [unverified]

[Checksum Status: Unverified] Urgent
Pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[Timestamps]

[Srver: Apache/2.2.22
(Ubuntu)
mod_fcgid/2.3.6
proxy_html/3.0.1
mod_ssl/2.2.22
OpenSSL/1.0.1\r\n

X-Powered-By: PHP/5.3.10-1ubuntu3.19\r\n
Expires: Sun, 19 Nov 1978 05:00:00 GMT\r\n

Cache-Control: store, no-cache, must-revalidate, post-check=0, pre-check=0\r\n
Last-Modified: Sat, 29 Jul 2017 07:17:55 GMT\r\n

Vary: Accept-Encoding\r\n
Content-Encoding: gzip\r\n
Content-Length: 9099\r\n

Keep-Alive: timeout=15, max=100\r\n
Connection: Keep-Alive\r\n

Content-Type: text/html; charset=utf-8\r\n

\r\n
[HTTP response 1/9]
[Time since request: 0.774772000 seconds]
[Request in frame: 9]
[Next request in frame: 34]
[Next response in frame:
52]

[Request URI: http://www.iitd.ac.in/]

Content-encoded entity body (gzip): 9099 bytes -> 50795 bytesFile
Data: 50795 bytes
Line-based text data:
text/html (709
lines)EQ/ACK
analysis] TCP payload
(879 bytes)

TCP segment data (879 bytes)

[8 Reassembled TCP Segments (9615 bytes): #13(1248), #15(1248), #17(1248), #19(1248),
#23(1248),
#28(1248), #30(1248), #32(879)]
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Sat, 29 Jul 2017 07:17:55 GMT\r\n

Server: Apache/2.2.22 (Ubuntu) mod_fcgid/2.3.6 proxy_html/3.0.1 mod_ssl/2.2.22
OpenSSL/1.0.1\r\n

X-Powered-By: PHP/5.3.10-1ubuntu3.19\r\n
Expires: Sun, 19 Nov 1978 05:00:00 GMT\r\n

Cache-Control: store, no-cache, must-revalidate, post-check=0, pre-check=0\r\n
Last-Modified: Sat, 29 Jul 2017 07:17:55 GMT\r\n

Vary: Accept-Encoding\r\n
Content-Encoding: gzip\r\n
Content-Length: 9099\r\n

Keep-Alive: timeout=15, max=100\r\n
Connection: Keep-Alive\r\n

Content-Type: text/html; charset=utf-8\r\n

\r\n
[HTTP response 1/9]
[Time since request: 0.774772000 seconds]
[Request in frame: 9]
[Next request in frame: 34]
[Next response in frame:
52]

[Request URI: http://www.iitd.ac.in/]

Content-encoded entity body (gzip): 9099 bytes -> 50795 bytesFile
Data: 50795 bytes
Line-based text data:
text/html (709 lines)

5. Find the packet number that includes HTTP GET message for a file IITD-IRD-122-2017.pdf. Also find the length of the file in bytes and time when file is downloaded successfully.

Soln: Packet numbber-478

File length-602 Bytes

HTTP GET request time-12:49:13.440096

HTTP OK time-12:49:13.700007

time duration-0.259911 s

Q2: Open the http.pcap file given in study material in Wireshark. Use File->Export Packet Dissections to save the data in csv file format. Write a C/C++/Java/Python code to read the data in csv file and print a. source IP addresses and destination IP addresses

b. source port numbers and destination port numbers
c. http request and response messages.

Soln:

Python code-

```
import pandas as pd

df = pd.read_csv("http.csv", usecols
    ['Source','Destination','Info'])

print(df)
```

Output:

```
                Source         Destination                                                 Info
0    XiaomiCo_9e:9c:c3           Broadcast          Who has 192.168.43.153? Tell 192.168.43.1
1    HonHaiPr_8c:90:55   XiaomiCo_9e:9c:c3             192.168.43.153 is at e0:06:e6:8c:90:55
2       192.168.43.153        103.27.9.20  34573  >  80 [SYN] Seq=0 Win=14600 Len=0 MSS=1...
3       192.168.43.153       192.168.43.1             Standard query 0x9f1d A www.iitd.ac.in
4         192.168.43.1     192.168.43.153  Standard query response 0x9f1d A www.iitd.ac.i...
..                  ...                ...                                                 ...
768      54.149.16.101     192.168.43.153  443  >  45136 [ACK] Seq=154 Ack=321 Win=28160 ...
769      54.149.16.101     192.168.43.153                                    Encrypted Alert
770     192.168.43.153      54.149.16.101           45136  >  443 [RST] Seq=321 Win=0 Len=0
771      54.149.16.101     192.168.43.153  443  >  45136 [FIN, ACK] Seq=191 Ack=321 Win=2...
772     192.168.43.153      54.149.16.101           45136  >  443 [RST] Seq=321 Win=0 Len=0

[773 rows x 3 columns]
```