Computer Networks Lab Report- Assignment 5

TITLE:

Name: Debarghya Maitra
Class: BCSE 3 rd Year
Group: A3
Submission Date: 14/10/2022

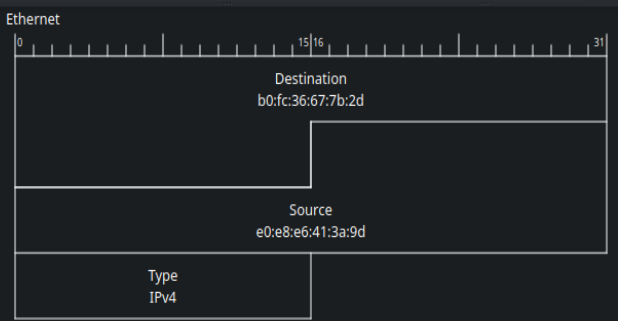
Q1) Generate some ICMP traffic by using the Ping command line tool to check the connectivity of a neighbouring machine (or router). Note the results in Wireshark. The initial ARP request broadcast from your PC determines the physical MAC address of the network IP Address, and the ARP reply from the neighboring system. After the ARP request, the pings (ICMP echo request and replies) can be seen.

RESULTS:

```
→ ping 192.168.101.1
PING 192.168.101.1 (192.168.101.1) 56(84) bytes of data.
64 bytes from 192.168.101.1: icmp_seq=1 ttl=64 time=1.44 ms
64 bytes from 192.168.101.1: icmp_seq=2 ttl=64 time=1.70 ms
64 bytes from 192.168.101.1: icmp_seq=3 ttl=64 time=1.53 ms
64 bytes from 192.168.101.1: icmp_seq=4 ttl=64 time=1.70 ms
64 bytes from 192.168.101.1: icmp_seq=5 ttl=64 time=1.51 ms
64 bytes from 192.168.101.1: icmp_seq=6 ttl=64 time=1.44 ms
```

1	0.000000000	0.000000000	60.6.224.90	192.168.101.6	ICMP	70	Destination unreachable (Port unreachable)
2	1.073195349	1.073195349	192.168.101.6	192.168.101.1	ICMP	98	Echo (ping) request id=0x000c, seq=1/256, ttl=64 (reply in 3)
3	1.074579853	0.001384504	192.168.101.1	192.168.101.6	ICMP	98	Echo (ping) reply id=0x000c, seq=1/256, ttl=64 (request in 2)
4	2.074425989	0.999846136	192.168.101.6	192.168.101.1	ICMP	98	Echo (ping) request id=0x000c, seq=2/512, ttl=64 (reply in 5)
5	2.076054983	0.001628994	192.168.101.1	192.168.101.6	ICMP	98	Echo (ping) reply id=0x000c, seq=2/512, ttl=64 (request in 4)
6	3.076956999	1.000902016	192.168.101.6	192.168.101.1	ICMP	98	Echo (ping) request id=0x000c, seq=3/768, ttl=64 (reply in 7)
7	3.078411427	0.001454428	192.168.101.1	192.168.101.6	ICMP	98	Echo (ping) reply id=0x000c, seq=3/768, ttl=64 (request in 6)
8	4.078402227	0.999990800	192.168.101.6	192.168.101.1	ICMP	98	Echo (ping) request id=0x000c, seq=4/1024, ttl=64 (reply in 9)
9	4.080029702	0.001627475	192.168.101.1	192.168.101.6	ICMP	98	Echo (ping) reply id=0x000c, seq=4/1024, ttl=64 (request in 8)
10	4.478067929	0.398038227	181.10.78.241	192.168.101.6	ICMP	161	Destination unreachable (Host unreachable)
11	5.080531835	0.602463906	192.168.101.6	192.168.101.1	ICMP	98	Echo (ping) request id=0x000c, seq=5/1280, ttl=64 (reply in 12)

```
Frame 5: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlp2
Ethernet II, Src: Shenzhen_41:3a:9d (e0:e8:e6:41:3a:9d), Dst: CyberTAN_67:7b:2d (b0:
Internet Protocol Version 4, Src: 192.168.101.1, Dst: 192.168.101.6
Internet Control Message Protocol
```



Q2) Generate some web traffic and

a. find the list the different protocols that appear in the protocol column in the unfiltered packet-listing window of Wireshark.

b. 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 Display Format, then select Time-of-day.)
c. What is the Internet address of the website? What is the Internet address of your computer?
d. Search back through your capture, and find an HTTP packet containing a GET command. Click on the packet in the Packet List Panel. Then expand the HTTP layer in the Packet Details Panel, from the packet.
e. Find out the value of the Host from the Packet Details Panel, within the GET command.

RESULTS:

Wireshark · Protocol Hierarchy Statistics · rest.pcapng

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	1984	100.0	1377790	152 k	0	0	0
Ethernet	100.0	1984	2.0	27776	3,078	0	0	0
Internet Protocol Version 4	99.8	1980	2.9	39604	4,389	0	0	0
User Datagram Protocol	81.4	1615	0.9	12920	1,432	0	0	0
Simple Service Discovery Protocol	0.9	17	0.2	2890	320	17	2890	320
QUIC IETF	79.6	1579	77.1	1062229	117 k	1542	1029898	114 k
Malformed Packet	0.1	2	0.0	0	0	2	0	0
Domain Name System	1.6	32	0.2	2699	299	32	2699	299
Data	1.1	22	0.2	3359	372	22	3359	372
Transmission Control Protocol	18.3	364	16.9	232159	25 k	207	47748	5,292
Transport Layer Security	7.7	153	15.5	213154	23 k	149	180256	19 k
Hypertext Transfer Protocol	0.4	8	0.8	10977	1,216	2	997	110
Line-based text data	0.2	4	1.2	17032	1,887	4	8422	933
HTML Form URL Encoded	0.1	2	0.0	42	4	2	42	4
Internet Group Management Protocol	0.1	1	0.0	8	0	1	8	0
Address Resolution Protocol	0.2	4	0.0	112	12	4	112	12

No display filter.

Close Copy Help

a) All the protocols that were captured are listed above.

b)

127	14.594135412	0.001185216	142.250.195.42	192.168.101.6	QUIC	67	Pro
128	14.618763635	0.024628223	192.168.101.6	142.250.76.78	QUIC	75	Pro
129	14.658368995	0.039605360	142.250.76.78	192.168.101.6	QUIC	67	Pro
130	14.658369554	0.000000559	44.228.249.3	192.168.101.6	HTTP	342	HT
131	14.658485563	0.000116009	192.168.101.6	44.228.249.3	TCP	66	472
132	14.666256710	0.007771147	192.168.101.6	44.228.249.3	HTTP	584	GE
133	14.672450181	0.006193471	44.228.249.3	192.168.101.6	TCP	66	80
134	14.954965554	0.282515373	44.228.249.3	192.168.101.6	TCP	1514	80
135	14.955051747	0.000086193	44.228.249.3	192.168.101.6	HTTP	1366	HT
136	14.955235751	0.000184004	192.168.101.6	44.228.249.3	TCP	66	472
137	15.325703858	0.370468107	192.168.101.6	239.255.255.250	SSDP	215	M-S
138	15.332108620	0.006404762	192.168.101.2	192.168.101.6	SSDP	380	HT
139	16.326381890	0.994273270	192.168.101.6	239.255.255.250	SSDP	215	M-S

```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Server: nginx/1.19.0\r\n
  Date: Wed, 12 Oct 2022 12:20:14 GMT\r\n
  Content-Type: text/html; charset=UTF-8\r\n
  Transfer-Encoding: chunked\r\n
  Connection: keep-alive\r\n
  X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1\r\n
  Content-Encoding: gzip\r\n
  \r\n
  [HTTP response 3/4]
  [Time since request: 0.288795037 seconds]
  [Prev request in frame: 88]
  [Prev response in frame: 130]
  [Request in frame: 132]
```

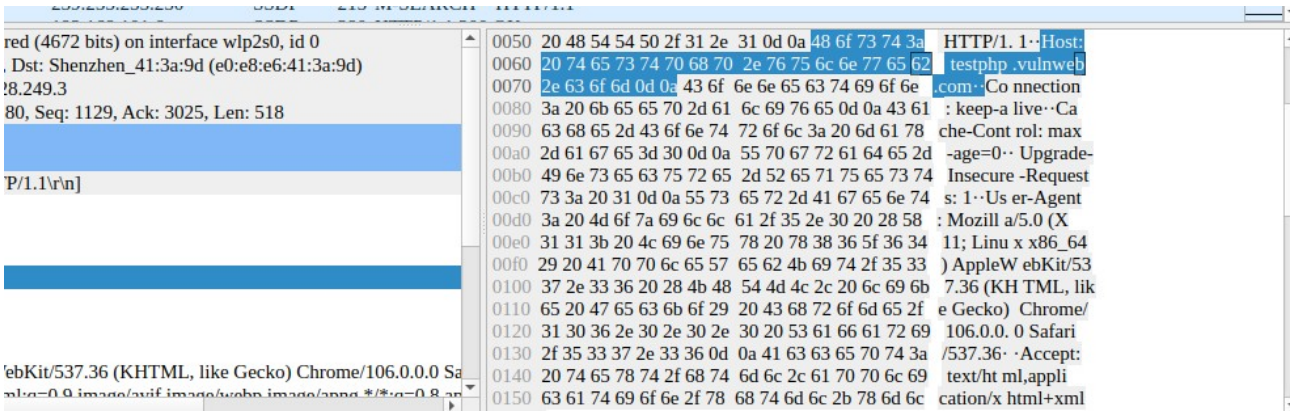
According to the delta time taken, it took 0.2888 seconds approx. To get the HTTP response.

No.	Time	Delta	Source	Destination	Protocol	Length	Info
125	14.592219778	0.000000595	142.250.76.78	192.168.101.6	QUIC	67	Protected Payload (KP0)
126	14.592950196	0.000730418	192.168.101.6	142.250.76.78	QUIC	77	Protected Payload (KP0), DCID=f
127	14.594135412	0.001185216	142.250.195.42	192.168.101.6	QUIC	67	Protected Payload (KP0)
128	14.618763635	0.024628223	192.168.101.6	142.250.76.78	QUIC	75	Protected Payload (KP0), DCID=f
129	14.658368995	0.039605360	142.250.76.78	192.168.101.6	QUIC	67	Protected Payload (KP0)
130	14.658369554	0.000000559	44.228.249.3	192.168.101.6	HTTP	342	HTTP/1.1 302 Found (text/html)
131	14.658485563	0.000116009	192.168.101.6	44.228.249.3	TCP	66	47210 → 80 [ACK] Seq=1129 Ack
132	14.666256710	0.007771147	192.168.101.6	44.228.249.3	HTTP	584	GET /login.php HTTP/1.1
133	14.672450181	0.006193471	44.228.249.3	192.168.101.6	TCP	66	80 → 47210 [ACK] Seq=3025 Ack
134	14.954965554	0.282515373	44.228.249.3	192.168.101.6	TCP	1514	80 → 47210 [ACK] Seq=3025 Ack
135	14.955051747	0.000086193	44.228.249.3	192.168.101.6	HTTP	1366	HTTP/1.1 200 OK (text/html)
136	14.955235751	0.000184004	192.168.101.6	44.228.249.3	TCP	66	47210 → 80 [ACK] Seq=1647 Ack
137	15.325703858	0.370468107	192.168.101.6	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
138	15.332108620	0.006404762	192.168.101.2	192.168.101.6	SSDP	380	HTTP/1.1 200 OK
139	16.326381890	0.994273270	192.168.101.6	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1

c) The local IP is 192.168.101.6 and the server IP is 44.228.249.3

```
Hypertext Transfer Protocol
  GET /login.php HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /login.php HTTP/1.1\r\n]
    Request Method: GET
    Request URI: /login.php
    Request Version: HTTP/1.1
  Host: testphp.vulnweb.com\r\n
  Connection: keep-alive\r\n
  Cache-Control: max-age=0\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
  Referer: http://testphp.vulnweb.com/login.php\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n
  \r\n
```

d) The above is the details of a HTTP packet

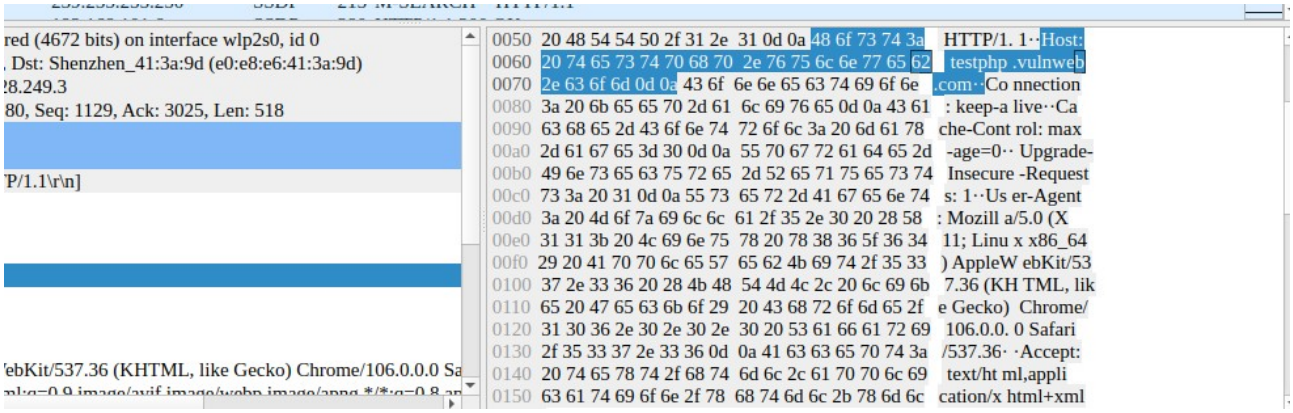


e) The value of Host as shown above is: testphp.vulnweb.com

Q3)Highlight the Hex and ASCII representations of the packet in the Packet Bytes Panel.
RESULTS: The above picture clearly shows the hex and ASCII representation of the packet in Packet Bytes panel.

Q4) Find out the first 4 bytes of the Hex value of the Host parameter from the Packet Bytes Panel.

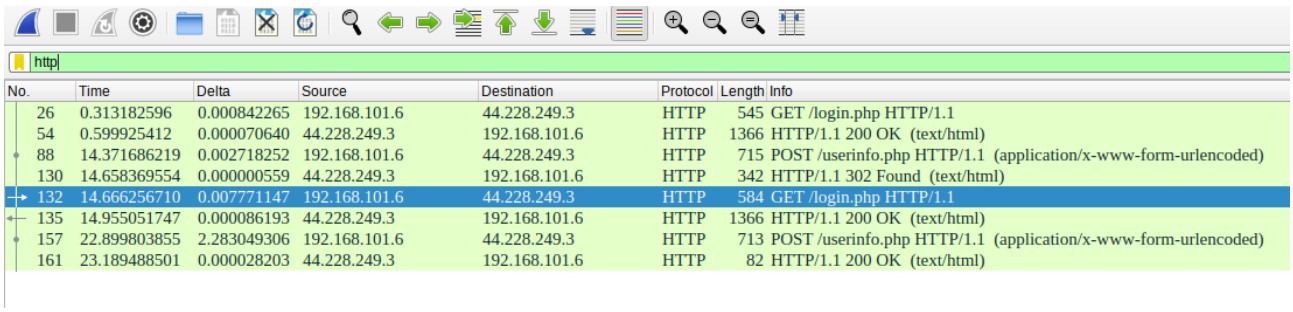
RESULTS:



Ans: The first 4 bytes of the Hex value of the Host parameter from the Packet Bytes Panel are: 48 6f 73 74

Q5) Filter packets with http, TCP, DNS and other protocols.

RESULTS:



http

No.	Time	Delta	Source	Destination	Protocol	Length	Info
26	0.313182596	0.000842265	192.168.101.6	44.228.249.3	HTTP	545	GET /login.php HTTP/1.1
54	0.599925412	0.000070640	44.228.249.3	192.168.101.6	HTTP	1366	HTTP/1.1 200 OK (text/html)
88	14.371686219	0.002718252	192.168.101.6	44.228.249.3	HTTP	715	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
130	14.658369554	0.000000559	44.228.249.3	192.168.101.6	HTTP	342	HTTP/1.1 302 Found (text/html)
132	14.666256710	0.007771147	192.168.101.6	44.228.249.3	HTTP	584	GET /login.php HTTP/1.1
135	14.955051747	0.000086193	44.228.249.3	192.168.101.6	HTTP	1366	HTTP/1.1 200 OK (text/html)
157	22.899803855	2.283049306	192.168.101.6	44.228.249.3	HTTP	713	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
161	23.189488501	0.000028203	44.228.249.3	192.168.101.6	HTTP	82	HTTP/1.1 200 OK (text/html)

Filtered for HTTP packets

tcp.

No.	Time	Delta	Source	Destination	Protocol	Length	Info
460	54.028508917	0.000532977	192.168.101.6	35.197.145.196	TCP	74	37786 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=10
463	54.059918897	0.005583956	216.58.196.163	192.168.101.6	TCP	66	[TCP ACKed unseen segment] 443 → 59092 [FIN, ACK] Seq=1 Ack=3 Win=261 Len=
464	54.059965143	0.000046246	192.168.101.6	216.58.196.163	TCP	66	59092 → 443 [ACK] Seq=3 Ack=2 Win=501 Len=0 TSval=2338172582 TSecr=587916
474	54.099342132	0.003444556	35.197.145.196	192.168.101.6	TCP	74	443 → 37786 [SYN, ACK] Seq=0 Ack=1 Win=64768 Len=0 MSS=1420 SACK_PERM
475	54.099397144	0.000055012	192.168.101.6	35.197.145.196	TCP	66	37786 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1058527480 TSecr=1540
476	54.099707495	0.000310351	192.168.101.6	35.197.145.196	TLS…	583	Client Hello
486	54.170751471	0.002372822	35.197.145.196	192.168.101.6	TCP	66	443 → 37786 [ACK] Seq=1 Ack=518 Win=64256 Len=0 TSval=1540384396 TSecr=10
487	54.176215130	0.005463659	35.197.145.196	192.168.101.6	TLS…	1474	Server Hello
488	54.176262872	0.000047742	192.168.101.6	35.197.145.196	TCP	66	37786 → 443 [ACK] Seq=518 Ack=1409 Win=64128 Len=0 TSval=1058527557 TSecr
490	54.176631506	0.000319487	35.197.145.196	192.168.101.6	TCP	1474	443 → 37786 [PSH, ACK] Seq=1409 Ack=518 Win=64256 Len=1408 TSval=15403844
491	54.176652211	0.000020705	192.168.101.6	35.197.145.196	TCP	66	37786 → 443 [ACK] Seq=518 Ack=2817 Win=64128 Len=0 TSval=1058527557 TSecr
492	54.176724025	0.000071814	35.197.145.196	192.168.101.6	TCP	1474	443 → 37786 [ACK] Seq=2817 Ack=518 Win=64256 Len=1408 TSval=1540384402 TS
493	54.176735277	0.000011252	192.168.101.6	35.197.145.196	TCP	66	37786 → 443 [ACK] Seq=518 Ack=4225 Win=64128 Len=0 TSval=1058527557 TSecr
494	54.176752623	0.000017346	35.197.145.196	192.168.101.6	TLS…	452	Certificate, Server Key Exchange, Server Hello Done
495	54.176807038	0.000054415	192.168.101.6	35.197.145.196	TCP	66	37786 → 443 [ACK] Seq=518 Ack=4611 Win=64128 Len=0 TSval=1058527557 TSecr
496	54.177016858	0.000209820	192.168.101.6	35.197.145.196	TLS…	73	Alert (Level: Fatal, Description: Certificate Unknown)
497	54.177297793	0.000280935	192.168.101.6	35.197.145.196	TCP	74	37794 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=10
498	54.177370294	0.000072501	192.168.101.6	35.197.145.196	TCP	66	37786 → 443 [FIN, ACK] Seq=525 Ack=4611 Win=64128 Len=0 TSval=1058527558 T
511	54.245500881	0.001493810	35.197.145.196	192.168.101.6	TCP	74	443 → 37794 [SYN, ACK] Seq=0 Ack=1 Win=64768 Len=0 MSS=1420 SACK_PERM
512	54.245539732	0.000038851	192.168.101.6	35.197.145.196	TCP	66	37794 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1058527626 TSecr=1540
513	54.245501045	-0.000038687	35.197.145.196	192.168.101.6	TCP	66	443 → 37786 [FIN, ACK] Seq=4611 Ack=525 Win=64256 Len=0 TSval=1540384472 T

Filtered for TCP packets

dns

No.	Time	Delta	Source	Destination	Protocol	Length	Info
19	0.218157895	0.080304747	192.168.101.6	192.168.101.1	DNS	79	Standard query 0x783c A clients4.google.com
20	0.263122006	0.044964111	192.168.101.1	192.168.101.6	DNS	129	Standard query response 0x783c A clients4.google.com CNAME clients.l.google.com A
58	0.686341993	0.012015504	192.168.101.6	192.168.101.1	DNS	76	Standard query 0xacd6 A www.acunetix.com
64	0.745510970	0.004712297	192.168.101.1	192.168.101.6	DNS	174	Standard query response 0xacd6 A www.acunetix.com CNAME acunetix-websites-4911
86	14.363911553	2.469781251	192.168.101.6	192.168.101.1	DNS	95	Standard query 0x8a07 A optimizationguide-pa.googleapis.com
87	14.368967967	0.005056414	192.168.101.1	192.168.101.6	DNS	351	Standard query response 0x8a07 A optimizationguide-pa.googleapis.com A 142.250.195
149	20.103834654	0.098447771	192.168.101.6	192.168.101.1	DNS	74	Standard query 0xbfd6 A www.google.com
150	20.109092767	0.005258113	192.168.101.1	192.168.101.6	DNS	90	Standard query response 0xbfd6 A www.google.com A 142.250.77.132
163	23.301971665	0.112328978	192.168.101.6	192.168.101.1	DNS	91	Standard query 0x7a61 A content-autofill.googleapis.com
164	23.304049737	0.002078072	192.168.101.6	192.168.101.1	DNS	78	Standard query 0xbf64 A www.googleapis.com
165	23.306830106	0.002780369	192.168.101.1	192.168.101.6	DNS	347	Standard query response 0x7a61 A content-autofill.googleapis.com A 142.250.77.106 A
169	23.309858543	0.000568823	192.168.101.1	192.168.101.6	DNS	334	Standard query response 0xbf64 A www.googleapis.com A 142.250.195.74 A 172.217.1
186	23.424149956	0.000941799	192.168.101.6	192.168.101.1	DNS	96	Standard query 0xa257 A passwordsleakcheck-pa.googleapis.com
187	23.429622825	0.005472869	192.168.101.1	192.168.101.6	DNS	352	Standard query response 0xa257 A passwordsleakcheck-pa.googleapis.com A 142.250.1
399	33.975381867	0.022821232	192.168.101.6	192.168.101.1	DNS	79	Standard query 0xe7ee A clients2.google.com
400	33.980267712	0.004885845	192.168.101.1	192.168.101.6	DNS	129	Standard query response 0xe7ee A clients2.google.com CNAME clients.l.google.com A
456	54.023002142	0.000849503	192.168.101.6	192.168.101.1	DNS	80	Standard query 0x6f42 A beacons.gcp.gvt2.com
459	54.027975940	0.003368110	192.168.101.1	192.168.101.6	DNS	152	Standard query response 0x6f42 A beacons.gcp.gvt2.com CNAME beacons-handoff.gcp
505	54.218921774	0.001158074	192.168.101.6	192.168.101.1	DNS	76	Standard query 0xe3ae A beacons.gvt2.com
506	54.222804595	0.003882821	192.168.101.1	192.168.101.6	DNS	115	Standard query response 0xe3ae A beacons.gvt2.com CNAME beacons6.gvt2.com A 21
611	56.048945938	0.021103791	192.168.101.6	192.168.101.1	DNS	70	Standard query 0xfc75 A github.com

Filtered for DNS packets

File Edit View Go Capture Analyze Statistics Telephony Wireless Too

tcp.stream eq 1

No.	Time	Delta	Source	Destination
4	0.027177712	0.000888614	192.168.101.6	44.228.249
24	0.312170488	0.031157929	44.228.249.3	192.168.10
25	0.312340331	0.000169843	192.168.101.6	44.228.249
26	0.313182596	0.000842265	192.168.101.6	44.228.249
27	0.320316794	0.007134198	44.228.249.3	192.168.10
52	0.599824123	0.030781294	44.228.249.3	192.168.10
53	0.599854772	0.000030649	192.168.101.6	44.228.249
54	0.599925412	0.000070640	44.228.249.3	192.168.10
55	0.599934580	0.000009168	192.168.101.6	44.228.249
88	14.371686219	0.002718252	192.168.101.6	44.228.249
90	14.375601791	0.001897921	44.228.249.3	192.168.10
130	14.658369554	0.000000559	44.228.249.3	192.168.10
131	14.658485563	0.000116009	192.168.101.6	44.228.249
132	14.666256710	0.007771147	192.168.101.6	44.228.249
133	14.672450181	0.006193471	44.228.249.3	192.168.10
134	14.954965554	0.282515373	44.228.249.3	192.168.10
135	14.955051747	0.000086193	44.228.249.3	192.168.10
136	14.955235751	0.000184004	192.168.101.6	44.228.249
157	22.899803855	2.283049306	192.168.101.6	44.228.249
158	22.903859262	0.004055407	44.228.249.3	192.168.10
159	23.189248515	0.285389253	44.228.249.3	192.168.10

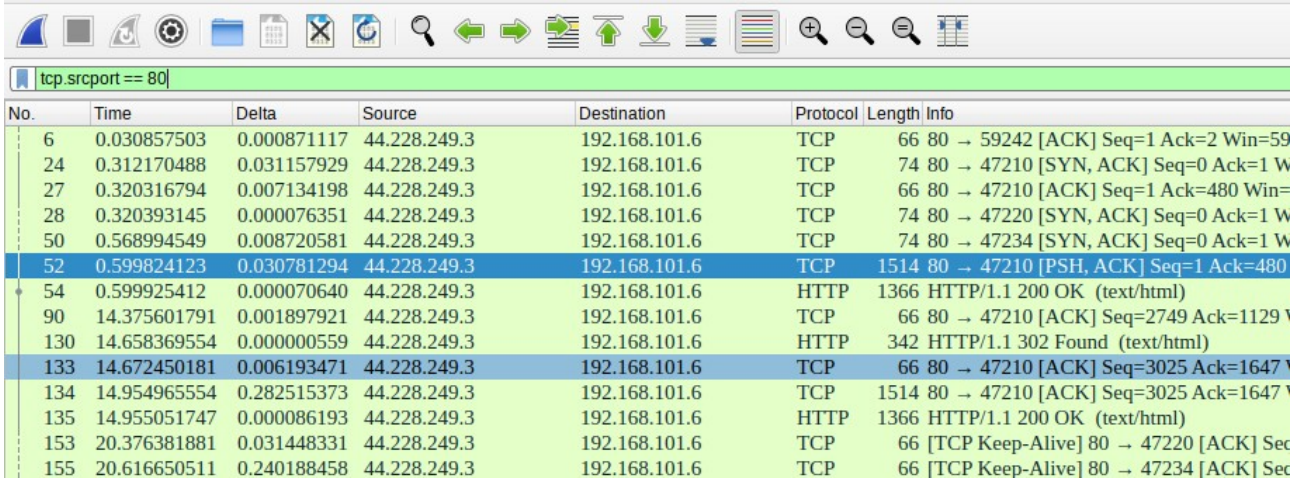
Frame 52: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits
Ethernet II, Src: Shenzhen_41:3a:9d (e0:e8:e6:41:3a:9d), Dst: CyberTAN_(
Internet Protocol Version 4, Src: 44.228.249.3, Dst: 192.168.101.6
Transmission Control Protocol, Src Port: 80, Dst Port: 47210, Seq: 1, Ack:

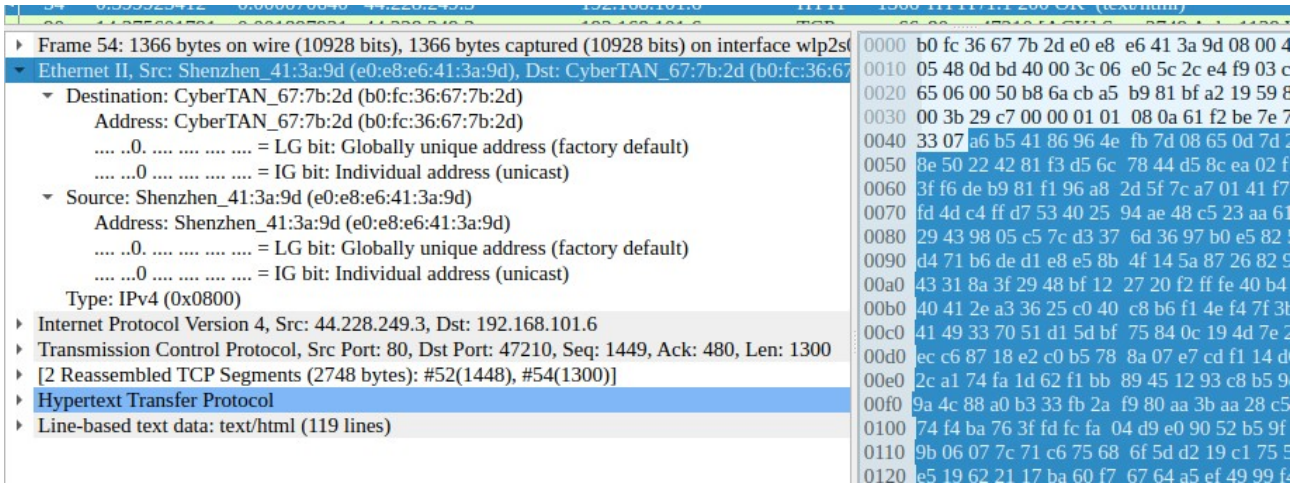
```
GET /login.php HTTP/1.1
Host: testphp.vulnweb.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Referer: https://www.google.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8

HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Wed, 12 Oct 2022 12:20:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip

9b4
............Xms.6....
.7M..P...IdQm...;n.......IH.."....^...Y..(..3.iG..X..>..7.?...qs....t.n~=..:gQ.$...'....?8........V..WIr.>..Jk.Q,......@.Yr.KR.yu.TJ.1(l.M...
5......6...8.3Y3+.M..H....i.9..}...\.....X.AS6..U!~n... ......D.FS^...8.../.3..3.2..[.H.sU[Q..n..4..4...:.OY^rm.M.Q..W/^.GP`.S./.iyV
9!...v...VJ..Y.$q.I.H....8.;,/.b..)P...iQ....J.R...R.i....D.B. >...'F^....e.6=                    .F).`3%..r.._'M..'..\.......
...|.o.....m/....s.'..O..U.....e-.../cI.w
..`KY.j......c...?E..h..IS.[q.B[.../..[...(.y..'_..{aM....O..7......o...9H...\.o.:.. d3.......,ly.s.....rV.S.j/b...)..o.... x...t.)..._...9...;`..9.p....p.....s..$.{I...
G2U.&lo\...H#J.k..:b....Q>.G<3.j.8.......a.x......8.R.m..8.#.....C....9!......)=M("<oka.. W..4r>cF.i$.....2S...F^.4z~x..p...U.2...it.1^.4z.
8....qfD.jiW..p._.'p...d-.U=U.....`.b.P...5sl.J..Va.V...d..c.....[K.Ad..>...DA..        I..tV..W.~oT..'c_.zz....^...9;..4<...wi4<<..F.z..&..%gu.U
9...;)....O._....b.....l...\[il ..zh.a!M^q9..3..w)s0.4+.jF.@....
c3..<.z...7?..=..Kk.}.........T..
g                    .
```

Followed HTTP stream

Q6) Search through your capture, and find an HTTP packet coming back from the server (TCP Source Port == 80). Expand the Ethernet layer in the Packet Details Panel.

RESULTS:





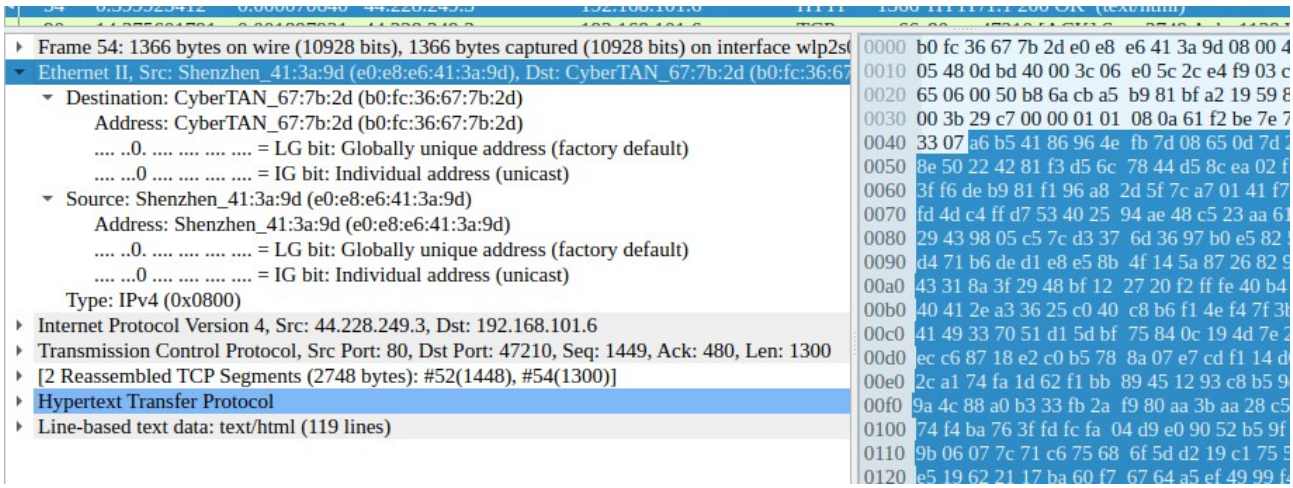
The above images shows the Ethernet layer in the Packet details.

Q7) What are the manufacturers of your PC's Network Interface Card (NIC), and the servers NIC?

Ans- So according to the details, my PC's Network Interface Card (NIC) has the manufacturer: CyberTAN.
And the server's Network Interface Card (NIC) has the manufacturer: Shenzhen.

Q8) What are the Hex values (shown the raw bytes panel) of the two NICS Manufacturers OUIs?

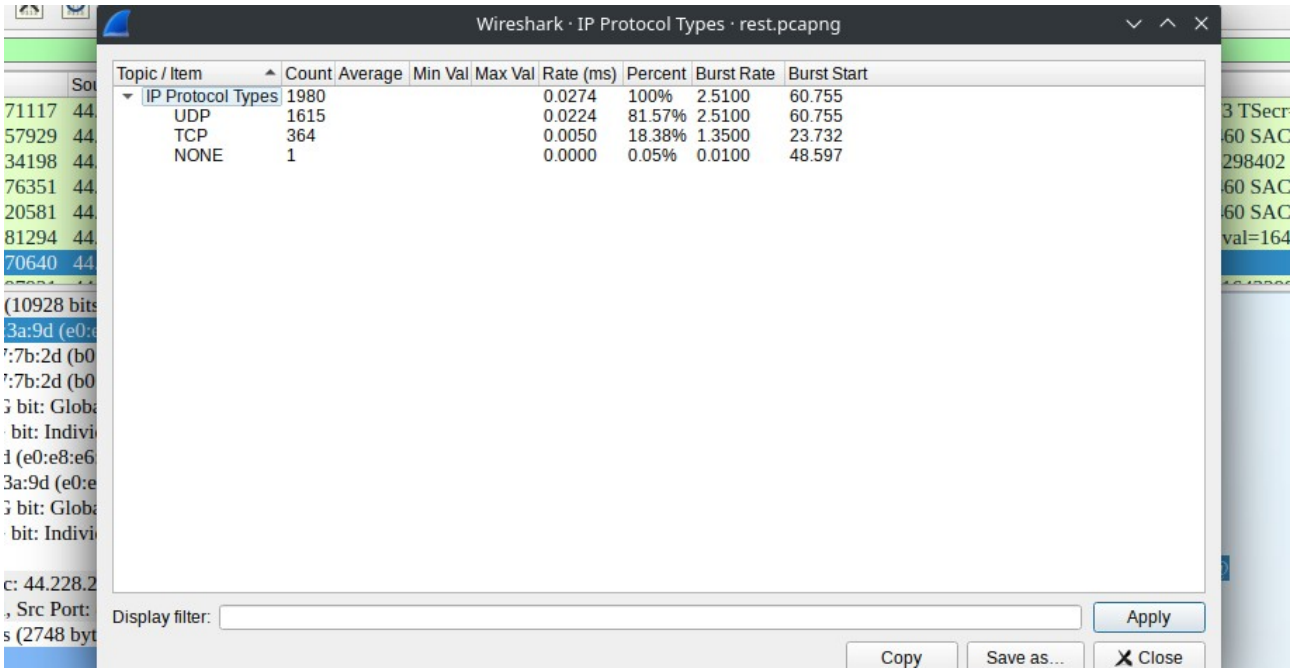
RESULTS:



Ans: The hex values (shown the raw bytes panel) of the two NICS Manufacturers OUIs are: b0 fc 36 67 7b 2d (my NIC raw bytes) and e0 e8 e6 41 3a 9d (server NIC)

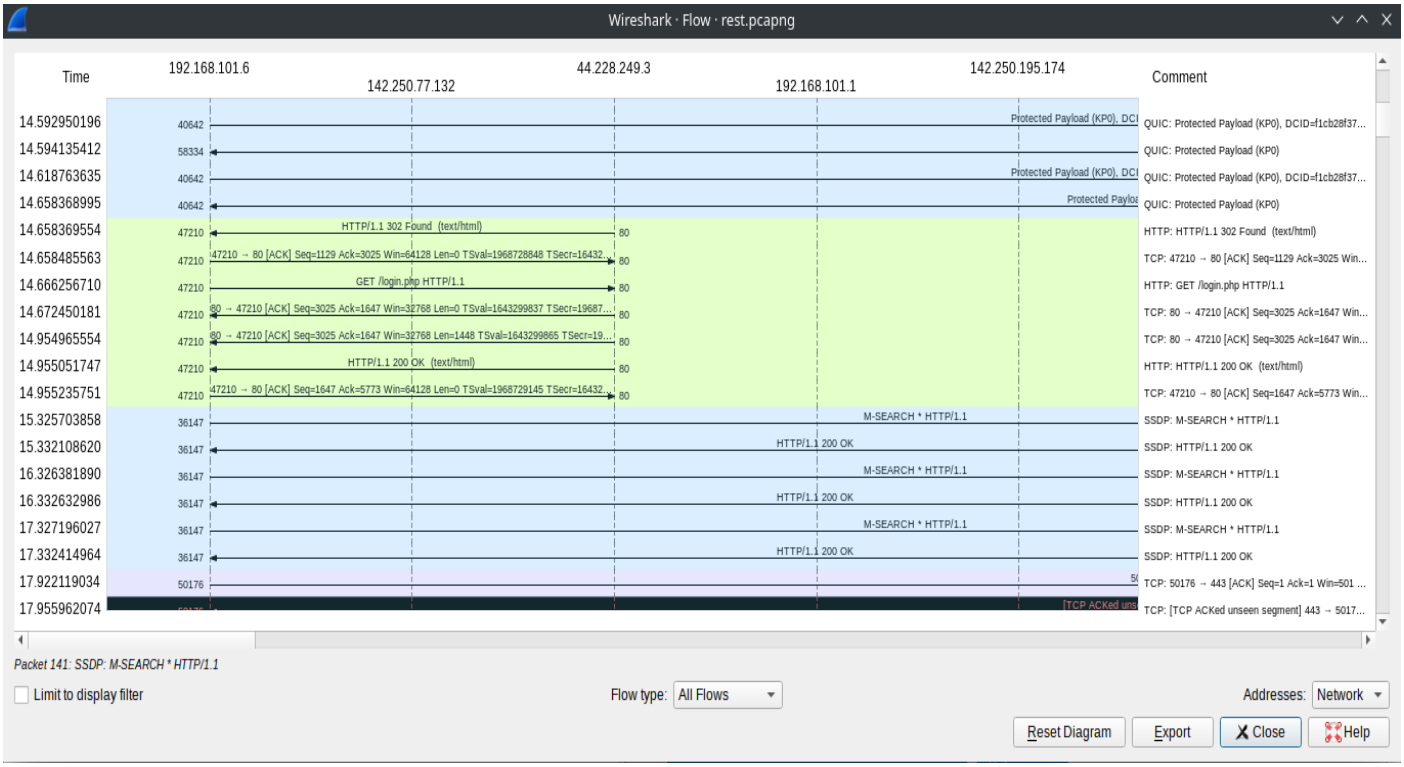
Q9) Find the following statistics:
a. What percentage of packets in your capture are TCP, and give an example of the higher level protocol which uses TCP?
b. What percentage of packets in your capture are UDP, and give an example of the higher level protocol which uses UDP?

RESULTS:



Ans: a) From the above statistics, the percentage of TCP packets is 18.38%
A protocol that uses TCP is HTTP.
b) The percentage of UDP packets is 81.57%. A protocol that uses UDP is DNS.

Q10)Find the traffic flow Select the Statistics->Flow Graph menu option. Choose General Flow and Network Source options, and click the OK button.



Shown as mentioned in question