

## PACKET ANALYSIS

### (A) List of applications generating background traffic:

The best-guessed applications that are running in the background are

Norton Antivirus

Virtual box

Java Update Manager

### Application Data Protocol-Transport Layer Security

115	29.768551667	192.168.43.186	192.168.43.1	DNS	76 Standard query 0xfc3e AAAA beacons.gvt2.com
116	29.768559788	192.168.43.186	192.168.43.1	DNS	76 Standard query 0xad1 A beacons.gvt2.com
117	29.778484038	192.168.43.1	192.168.43.186	DNS	92 Standard query response 0xad1 A beacons.gvt2.com A 172.217.31.195
118	29.781211898	192.168.43.186	180.87.4.163	SSL	352 Continuation Data
119	29.798021788	192.168.43.1	192.168.43.186	DNS	127 Standard query response 0xfc3e AAAA beacons.gvt2.com CNAME beacons6.gvt2.com AAAA 2404:6800:4007:811::2003
120	29.799308156	2409:4070:2ea9:4610::	2404:6800:4007:811::	TCP	86 57230 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM=1
121	29.854305561	2404:6800:4007:811::	2409:4070:2ea9:4610::	TCP	86 443 → 57230 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1360 SACK_PERM=1 WS=256
122	29.854315516	2409:4070:2ea9:4610::	2404:6800:4007:811::	TCP	74 57230 → 443 [ACK] Seq=1 Ack=1 Win=131840 Len=0
123	29.863563413	2409:4070:2ea9:4610::	2404:6800:4007:811::	TLSv1.3	591 Client Hello
124	29.907056949	180.87.4.163	192.168.43.186	SSL	189 Continuation Data
125	29.915079668	192.168.43.186	194.58.31.81	TLSv1.2	1099 Application Data
126	29.916372040	2404:6800:4007:811::	2409:4070:2ea9:4610::	TCP	74 443 → 57230 [ACK] Seq=1 Ack=518 Win=66816 Len=0
127	29.947756598	192.168.43.186	180.87.4.163	TCP	60 57229 → 443 [ACK] Seq=597 Ack=271 Win=131072 Len=0
128	29.953198683	2404:6800:4007:811::	2409:4070:2ea9:4610::	TLSv1.3	1294 Server Hello, Change Cipher Spec
129	29.953208236	2404:6800:4007:811::	2409:4070:2ea9:4610::	TCP	1294 443 → 57230 [ACK] Seq=1221 Ack=518 Win=66816 Len=1220 [TCP segment of a reassembled PDU]
130	29.953209654	2404:6800:4007:811::	2409:4070:2ea9:4610::	TCP	1294 443 → 57230 [ACK] Seq=2441 Ack=518 Win=66816 Len=1220 [TCP segment of a reassembled PDU]
131	29.953211151	2404:6800:4007:811::	2409:4070:2ea9:4610::	TLSv1.3	193 Application Data
132	29.953212239	2409:4070:2ea9:4610::	2404:6800:4007:811::	TCP	74 57230 → 443 [ACK] Seq=518 Ack=3780 Win=131840 Len=0

> Frame 125: 1099 bytes on wire (8792 bits), 1099 bytes captured (8792 bits) on interface enp0s3, id 0

> Ethernet II, Src: LiteonTe\_16:49:be (f8:28:19:16:49:be), Dst: XiaomiCo\_69:67:05 (20:34:fb:69:67:05)

> Internet Protocol Version 4, Src: 192.168.43.186, Dst: 194.58.31.81

> Transmission Control Protocol, Src Port: 57175, Dst Port: 443, Seq: 1, Ack: 341, Len: 1045

✓ Transport Layer Security

▼ TLSv1.2 Record Layer: Application Data Protocol: http-over-tls

Content Type: Application Data (23)

Version: TLS 1.2 (0x0303)

Length: 1040

Encrypted Application Data: 8c8cd5a70c8bddf5a7039fa93fe51de20774eb654a62cc37..

### Simple Service Discovery Protocol

No.	Time	Source	Destination	Protocol	Length	Info
55	18.585163007	2404:6800:4007:809:... 2409:4070:2ea9:4610...	2409:4070:2ea9:4610...	TCP	74	[TCP Out-Of-Order] 443 → 57170 [FIN, ACK] Seq=57 Ack=2 Win=270 Len=0
56	18.585163851	2409:4070:2ea9:4610... 2404:6800:4007:809:...	2404:6800:4007:809:...	TCP	74	[TCP Dup ACK 53#1] 57170 → 443 [ACK] Seq=3 Ack=57 Win=510 Len=0
57	18.585284517	2409:4070:2ea9:4610... 2404:6800:4007:809:...	2404:6800:4007:809:...	TCP	74	57170 → 443 [ACK] Seq=3 Ack=58 Win=510 Len=0
58	18.676767612	2409:4070:2ea9:4610... 2404:6800:4007:809:...	2404:6800:4007:809:...	TCP	74	[TCP Retransmission] 57170 → 443 [FIN, ACK] Seq=2 Ack=58 Win=510 Len=0
59	18.715315105	2404:6800:4007:809:...	2409:4070:2ea9:4610...	TCP	74	443 → 57170 [ACK] Seq=58 Ack=3 Win=270 Len=0
60	18.715330873	194.58.31.81	192.168.43.186	TLSv1.2	394	Application Data
61	18.738608173	2404:6800:4007:809:...	2409:4070:2ea9:4610...	TCP	74	[TCP Dup ACK 59#1] 443 → 57170 [ACK] Seq=58 Ack=3 Win=270 Len=0
62	18.756060043	192.168.43.186	194.58.31.81	TCP	60	57182 → 443 [ACK] Seq=1 Ack=341 Win=511 Len=0
63	19.116484178	192.168.43.186	194.58.31.81	TLSv1.2	1099	Application Data
64	19.411528256	194.58.31.81	192.168.43.186	TCP	60	443 → 57182 [ACK] Seq=341 Ack=1046 Win=635 Len=0
65	19.968268305	192.168.43.186	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
66	20.969261595	192.168.43.186	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
67	21.970728855	192.168.43.186	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
68	22.665020358	194.58.31.81	192.168.43.186	TLSv1.2	93	Application Data
69	22.705222966	192.168.43.186	194.58.31.81	TCP	60	57181 → 443 [ACK] Seq=1 Ack=118 Win=513 Len=0
70	22.971816706	192.168.43.186	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
71	22.994211349	194.58.31.81	192.168.43.186	TLSv1.2	93	Application Data
72	23.036651833	192.168.43.186	194.58.31.81	TCP	60	57184 → 443 [ACK] Seq=1 Ack=118 Win=513 Len=0

> Frame 65: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface enp0s3, id 0  
 > Ethernet II, Src: LiteonTe\_16:49:be (f8:28:19:16:49:be), Dst: IPv4mcast\_7f:ff:fa (01:00:5e:7f:ff:fa)  
 > Internet Protocol Version 4, Src: 192.168.43.186, Dst: 239.255.255.250  
 > User Datagram Protocol, Src Port: 55477, Dst Port: 1900  
 > Simple Service Discovery Protocol  
   M-SEARCH \* HTTP/1.1\r\n  
     > [Expert Info (Chat/Sequence): M-SEARCH \* HTTP/1.1\r\n]  
       Request Method: M-SEARCH  
       Request URI: \*  
       Request Version: HTTP/1.1  
       HOST: 239.255.255.250:1900\r\n  
       MAN: "ssdp:discover"\r\n  
       MX: 1\r\n  
       ST: urn:dial-multiscreen-org:service:dial:1\r\n  
       USER-AGENT: Google Chrome/79.0.3945.130 Windows\r\n  
       \r\n  
       [Full request URI: http://239.255.255.250:1900\*]  
       [HTTP request 1/4]  
       [Next request in frame: 66]

## Address resolution protocol

No.	Time	Source	Destination	Protocol	Length	Info
6	1.006541006	194.58.31.81	192.168.43.186	TCP	60	443 → 57176 [ACK] Seq=1 Ack=968 Win=635 Len=0
7	2.655661929	194.58.31.81	192.168.43.186	TLSv1.2	93	Application Data
8	2.695857067	192.168.43.186	194.58.31.81	TCP	60	57181 → 443 [ACK] Seq=1 Ack=40 Win=513 Len=0
9	2.982444430	194.58.31.81	192.168.43.186	TLSv1.2	93	Application Data
10	3.022932910	192.168.43.186	194.58.31.81	TCP	60	57184 → 443 [ACK] Seq=1 Ack=40 Win=508 Len=0
11	3.716361223	2409:4070:2ea9:4610... 2404:6800:4007:810:...	2404:6800:4007:810:...	TCP	75	57225 → 443 [ACK] Seq=1 Ack=1 Win=515 Len=1 [TCP segment of a reassembled PDU]
12	3.771284385	2404:6800:4007:810:...	2409:4070:2ea9:4610...	TCP	86	443 → 57225 [ACK] Seq=1 Ack=2 Win=286 Len=0 SLE=1 SRE=2
13	5.628958153	2409:4070:2ea9:4610... 2404:6800:4007:809:...	2404:6800:4007:809:...	TCP	75	57170 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1 [TCP segment of a reassembled PDU]
14	5.692534539	2404:6800:4007:809:...	2409:4070:2ea9:4610...	TCP	86	443 → 57170 [ACK] Seq=1 Ack=2 Win=270 Len=0 SLE=1 SRE=2
15	7.221081040	2409:4070:2ea9:4610... 2404:6800:4003:c03:...	2404:6800:4003:c03:...	TCP	75	57180 → 5228 [ACK] Seq=1 Ack=1 Win=510 Len=1
16	7.337530035	2404:6800:4003:c03:...	2409:4070:2ea9:4610...	TCP	86	5228 → 57180 [ACK] Seq=1 Ack=2 Win=251 Len=0 SLE=1 SRE=2
17	7.580956255	XiaomiCo_69:67:05	Broadcast	ARP	60	Who has 192.168.43.186? Tell 192.168.43.1
18	7.580984376	LiteonTe_16:49:be	XiaomiCo_69:67:05	ARP	60	192.168.43.186 is at f8:28:19:16:49:be
19	8.804186756	192.168.43.186	192.168.43.1	DNS	76	Standard query 0x3d84 AAAA api.protonvpn.ch
20	8.808288584	192.168.43.1	192.168.43.186	DNS	76	Standard query response 0x3d84 AAAA api.protonvpn.ch
21	8.841579719	192.168.43.186	185.159.159.170	TCP	66	57227 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
22	9.369869267	185.159.159.170	192.168.43.186	TCP	66	443 → 57227 [SYN, ACK] Seq=0 Ack=1 Win=43520 Len=0 MSS=1360 SACK_PERM=1 WS=512
23	9.369882135	192.168.43.186	185.159.159.170	TCP	60	57227 → 443 [ACK] Seq=1 Ack=1 Win=131840 Len=0

> Frame 17: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface enp0s3, id 0  
 > Ethernet II, Src: XiaomiCo\_69:67:05 (20:34:fb:69:67:05), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
 > Address Resolution Protocol (request)  
   Hardware type: Ethernet (1)  
   Protocol type: IPv4 (0x0800)  
   Hardware size: 6  
   Protocol size: 4  
   Opcode: request (1)  
   Sender MAC address: XiaomiCo\_69:67:05 (20:34:fb:69:67:05)  
   Sender IP address: 192.168.43.1  
   Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)  
   Target IP address: 192.168.43.186

## (B) Analysis of web page Download

### Website Visited:

<http://10.2.102.21:9000/psp/hcsprod/EMPLOYEE/HRMS/h/?tab=DEFAULT>

Servers for which DNS query was launched are

8.8.8.8.in-addr.arpa → dns.google

35.116.16.172.in-addr.arpa → vaibhav-VirtualBox

The image shows a Wireshark packet capture of a DNS query and a terminal window showing the command used to generate it.

**Wireshark Packet Capture:**

No.	Time	Source	Destination	Protocol	Length	Info
468	5.841178166	172.16.116.35	8.8.8.8	DNS	92	Standard query 0x90bd A erp.bits-pilani.ac.in OPT
469	5.841441591	172.16.116.35	8.8.8.8	DNS	92	Standard query 0x7f3d AAAA erp.bits-pilani.ac.in OPT
475	5.880838716	8.8.8.8	172.16.116.35	DNS	108	Standard query response 0x90bd A erp.bits-pilani.ac.in A 103.68.199.23 OPT
477	5.887099281	8.8.8.8	172.16.116.35	DNS	137	Standard query response 0x7f3d AAAA erp.bits-pilani.ac.in SOA ns3.bits-pilani.ac.in OPT

**Terminal Output:**

```
vaibhav@vaibhav-VirtualBox: ~  
File Edit View Search Terminal Help  
vaibhav@vaibhav-VirtualBox:~$ nslookup 8.8.8.8  
8.8.8.8.in-addr.arpa    name = dns.google.  
  
Authoritative answers can be found from:  
  
vaibhav@vaibhav-VirtualBox:~$
```

The image shows a Wireshark packet capture of a DNS query and a terminal window showing the commands used to generate it.

**Wireshark Packet Capture:**

No.	Time	Source	Destination	Protocol	Length	Info
468	5.841178166	172.16.116.35	8.8.8.8	DNS	92	Standard query 0x90bd A erp.bits-pilani.ac.in OPT
469	5.841441591	172.16.116.35	8.8.8.8	DNS	92	Standard query 0x7f3d AAAA erp.bits-pilani.ac.in OPT
475	5.880838716	8.8.8.8	172.16.116.35	DNS	108	Standard query response 0x90bd A erp.bits-pilani.ac.in A 103.68.199.23 OPT
477	5.887099281	8.8.8.8	172.16.116.35	DNS	137	Standard query response 0x7f3d AAAA erp.bits-pilani.ac.in SOA ns3.bits-pilani.ac.in OPT

**Terminal Output:**

```
vaibhav@vaibhav-VirtualBox: ~  
File Edit View Search Terminal Help  
vaibhav@vaibhav-VirtualBox:~$ nslookup 8.8.8.8  
8.8.8.8.in-addr.arpa    name = dns.google.  
  
Authoritative answers can be found from:  
  
vaibhav@vaibhav-VirtualBox:~$ nslookup 172.16.116.35  
35.116.16.172.in-addr.arpa    name = vaibhav-VirtualBox.  
35.116.16.172.in-addr.arpa    name = vaibhav-VirtualBox.local.  
  
Authoritative answers can be found from:  
  
vaibhav@vaibhav-VirtualBox:~$
```



## Number of HTTP requests generated:

Total 5 requests are generated, these are the ones with GET/ HEADER

The image shows a Wireshark packet capture of an HTTP session. The top pane displays a list of captured packets, with the first five being GET requests. The bottom pane shows the details of the selected packet (No. 463), which is an HTTP GET request for /favicon.ico.

No.	Time	Source	Destination	Protocol	Length	Info
282	4.199837291	172.16.116.35	10.2.102.21	HTTP	671	GET /psprod/EMPLOYEE/HRMS/h/?tab=DEFAULT&cmd=Login&errorCode=106&languageCo=ENG HTTP/1.1
307	4.168500152	10.2.102.21	172.16.116.35	HTTP	611	HTTP/1.1 200 OK (text/html)
375	5.112934715	172.16.116.35	10.2.102.21	HTTP	612	GET /hcsprod/styles.css HTTP/1.1
384	5.146781561	10.2.102.21	172.16.116.35	HTTP	78	HTTP/1.1 200 OK (text/css)
426	5.679332910	172.16.116.35	10.2.102.21	HTTP	618	GET /hcsprod/images/OPSE_logo.gif HTTP/1.1
434	5.702835988	172.16.116.35	10.2.102.21	HTTP	623	GET /hcsprod/images/PT_LOGIN_ERROR.gif HTTP/1.1
451	5.717679871	10.2.102.21	172.16.116.35	HTTP	1780	HTTP/1.1 200 OK (GIF89a)
458	5.735720825	10.2.102.21	172.16.116.35	HTTP	276	HTTP/1.1 200 OK (GIF89a)
463	5.818328657	172.16.116.35	10.2.102.21	HTTP	487	GET /favicon.ico HTTP/1.1
473	5.847661224	10.2.102.21	172.16.116.35	HTTP	1230	HTTP/1.1 404 Not Found (text/html)

Frame 463: 487 bytes on wire (3896 bits), 487 bytes captured (3896 bits) on interface 0  
Ethernet II, Src: PcsCompu\_8e:56:73 (08:00:27:0e:56:73), Dst: Cisco\_07:b0:07 (b0:0b:cf:d7:b0:07)  
Internet Protocol Version 4, Src: 172.16.116.35, Dst: 10.2.102.21  
Transmission Control Protocol, Src Port: 53722, Dst Port: 9000, Seq: 1704, Ack: 28043, Len: 421  
Source Port: 53722  
Destination Port: 9000  
[Stream index: 0]  
[TCP Segment Len: 421]  
Sequence number: 1704 (relative sequence number)  
[Next sequence number: 2125 (relative sequence number)]  
Acknowledgment number: 28043 (relative ack number)  
1000 .... = Header Length: 32 bytes (8)  
... = Flags: 0x018 /DSU, ACK

0000 00 80 c7 d7 00 07 08 00 27 8e 56 73 08 99 45 09 ..... 'Vs:E-  
0010 01 d9 40 5d 40 09 40 06 08 77 ac 19 74 23 0a 02 -[0]0 0 hw-ta..  
0020 06 15 d1 da 23 28 ab f9 a6 e9 fd 63 aa 36 80 18 f...H[...-c-6..  
0030 01 75 02 15 00 09 01 01 08 0a 2c 85 4b 09 20 50 ..... -,K, A  
0040 a3 06 47 45 54 29 2f 66 61 76 69 63 6f 6e 2e 60 --GET /f avicon.i  
0050 63 6f 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 co HTTP/ 1.1-Hos  
0060 74 3a 20 31 30 2e 32 2e 31 39 32 2e 32 31 3a 39 t: 10.2. 102.21:9  
0070 30 39 30 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 009: Use r-Agent:  
0080 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 39 20 28 58 31 Mozilla /5.0 (X1  
0090 31 20 20 55 62 75 6e 74 75 30 20 4c 69 8e 75 78 1; Ubuntu; Linux  
00a0 20 78 38 36 5f 36 34 3b 20 72 76 3a 37 32 2e 30 x86\_64; rv:72.0  
00b0 29 20 47 65 63 6b 6f 2f 32 30 31 39 30 31 30 31 ) Gecko/ 20100101  
00c0 20 46 69 72 65 65 6f 78 2f 37 32 2e 30 9d 0a 41 Firefox /72.0-A  
00d0 63 63 65 70 74 3a 20 69 6d 61 67 65 2f 77 65 62 ccept: i mage/web  
00e0 70 2c 2a 2f 2a 0d 0a 41 63 63 65 70 74 2d 4c 61 p,/\*-A ccept-La  
00f0 6e 67 75 61 67 65 3a 29 65 6e 2d 55 53 2c 65 60 nguage: en-US,en  
0100 3b 71 3d 30 2e 35 0d 0a 41 63 63 65 70 74 2d 45 ;q=0.5-Accept-E  
0110 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 ncoding: gzip, d  
0120 65 66 6c 61 74 65 0d 0a 43 6f 6e 6e 65 63 74 69 eflate- Connecti  
0130 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a on: keep-alive-  
0140 43 6f 6f 6b 69 65 3a 29 48 43 53 50 52 4f 44 2d Cookie: HCSPROD-  
0150 50 4f 52 54 41 4c 2d 59 53 4a 53 45 53 53 49 4f PORTAL-P SJS3S3IO  
0160 4c 49 44 3d 51 34 6b 07 58 61 76 75 4f 76 43 37 NTD-Q4kg NavoVC7  
0170 6b 6b 69 59 34 61 4a 63 6c 6a 6a 45 62 37 6a 76 kkiV4aJc 1jF07jv  
0180 71 39 32 77 21 32 34 32 34 39 38 36 30 36 3b 29 a02w1242 496895:

## The number of TCP connections opened:

The number of TCP connections opened are 4 ( ones with SYN including acknowledgment )

Activities Wireshark Fri 22:31 Q4 (b).pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
277	4.076372082	172.16.116.35	10.2.192.21	TCP	74	53722 → 9000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=746931250 TSecr=0 WS=128
278	4.099452876	10.2.192.21	172.16.116.35	TCP	74	9000 → 53722 [SYN, ACK] Seq=0 Ack=1 Win=14360 Len=0 MSS=1436 WS=1 SACK_PERM=1 TSval=543071421 TSecr=746931250
279	4.099545418	172.16.116.35	10.2.192.21	TCP	66	53722 → 9000 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=746931274 TSecr=543071421
282	4.109837291	172.16.116.35	10.2.192.21	HTTP	671	GET /psp/hcsprod/EMPLOYEE/HRMS/h/?tab=DEFAULT&cmd=login&errorCode=106&languageCd=ENG HTTP/1.1
284	4.138527110	10.2.192.21	172.16.116.35	TCP	66	9000 → 53722 [ACK] Seq=1 Ack=606 Win=14965 Len=0 TSval=543071461 TSecr=746931284
285	4.144527166	10.2.192.21	172.16.116.35	TCP	488	9000 → 53722 [PSH, ACK] Seq=1 Ack=606 Win=14965 Len=422 TSval=543071466 TSecr=746931284 [TCP segment of a reassembled PDU]
286	4.144718765	172.16.116.35	10.2.192.21	TCP	66	53722 → 9000 [ACK] Seq=606 Ack=423 Win=64128 Len=0 TSval=746931319 TSecr=543071466
287	4.146574796	10.2.192.21	172.16.116.35	TCP	1490	9000 → 53722 [PSH, ACK] Seq=423 Ack=606 Win=14965 Len=1424 TSval=543071466 TSecr=746931284 [TCP segment of a reassembled PDU]
288	4.146592768	172.16.116.35	10.2.192.21	TCP	66	53722 → 9000 [ACK] Seq=606 Ack=1847 Win=64128 Len=0 TSval=746931321 TSecr=543071466
289	4.146940779	10.2.192.21	172.16.116.35	TCP	1490	9000 → 53722 [PSH, ACK] Seq=1847 Ack=606 Win=14965 Len=1424 TSval=543071466 TSecr=746931284 [TCP segment of a reassembled PDU]
290	4.146951681	172.16.116.35	10.2.192.21	TCP	66	53722 → 9000 [ACK] Seq=606 Ack=3271 Win=64128 Len=0 TSval=746931321 TSecr=543071466
291	4.148128566	10.2.192.21	172.16.116.35	TCP	1490	9000 → 53722 [PSH, ACK] Seq=3271 Ack=606 Win=14965 Len=1424 TSval=543071466 TSecr=746931284 [TCP segment of a reassembled PDU]
292	4.148147184	172.16.116.35	10.2.192.21	TCP	66	53722 → 9000 [ACK] Seq=606 Ack=4695 Win=64128 Len=0 TSval=746931322 TSecr=543071466
293	4.149357882	10.2.192.21	172.16.116.35	TCP	1490	9000 → 53722 [PSH, ACK] Seq=4695 Ack=606 Win=14965 Len=1424 TSval=543071466 TSecr=746931284 [TCP segment of a reassembled PDU]
294	4.149393254	172.16.116.35	10.2.192.21	TCP	66	53722 → 9000 [ACK] Seq=606 Ack=6119 Win=64128 Len=0 TSval=746931323 TSecr=543071466
295	4.150398982	10.2.192.21	172.16.116.35	TCP	1490	9000 → 53722 [PSH, ACK] Seq=6119 Ack=606 Win=14965 Len=1424 TSval=543071466 TSecr=746931284 [TCP segment of a reassembled PDU]
296	4.150418704	172.16.116.35	10.2.192.21	TCP	66	53722 → 9000 [ACK] Seq=606 Ack=7543 Win=64128 Len=0 TSval=746931324 TSecr=543071466
297	4.151384911	10.2.192.21	172.16.116.35	TCP	1490	9000 → 53722 [PSH, ACK] Seq=7543 Ack=606 Win=14965 Len=1424 TSval=543071466 TSecr=746931284 [TCP segment of a reassembled PDU]
298	4.151401305	172.16.116.35	10.2.192.21	TCP	66	53722 → 9000 [ACK] Seq=606 Ack=8967 Win=64128 Len=0 TSval=746931325 TSecr=543071466
299	4.152680699	10.2.192.21	172.16.116.35	TCP	1490	9000 → 53722 [ACK] Seq=8967 Ack=606 Win=14965 Len=1424 TSval=543071466 TSecr=746931284 [TCP segment of a reassembled PDU]
300	4.152709561	172.16.116.35	10.2.192.21	TCP	66	53722 → 9000 [ACK] Seq=606 Ack=10391 Win=64128 Len=0 TSval=746931327 TSecr=543071466
301	4.153708592	10.2.192.21	172.16.116.35	TCP	1490	9000 → 53722 [ACK] Seq=10391 Ack=606 Win=14965 Len=1424 TSval=543071466 TSecr=746931284 [TCP segment of a reassembled PDU]
302	4.153719494	172.16.116.35	10.2.192.21	TCP	66	53722 → 9000 [ACK] Seq=606 Ack=11815 Win=64128 Len=0 TSval=746931328 TSecr=543071466
303	4.154787717	10.2.192.21	172.16.116.35	TCP	1490	9000 → 53722 [PSH, ACK] Seq=11815 Ack=606 Win=14965 Len=1424 TSval=543071466 TSecr=746931284 [TCP segment of a reassembled PDU]
304	4.154804586	172.16.116.35	10.2.192.21	TCP	66	53722 → 9000 [ACK] Seq=606 Ack=13239 Win=64128 Len=0 TSval=746931329 TSecr=543071466
305	4.168134374	10.2.192.21	172.16.116.35	TCP	1490	9000 → 53722 [PSH, ACK] Seq=13239 Ack=606 Win=14965 Len=1424 TSval=543071488 TSecr=746931319 [TCP segment of a reassembled PDU]
306	4.168185336	172.16.116.35	10.2.192.21	TCP	66	53722 → 9000 [ACK] Seq=606 Ack=14663 Win=64128 Len=0 TSval=746931342 TSecr=543071488
307	4.168500152	10.2.192.21	172.16.116.35	HTTP	611	HTTP/1.1 200 OK (text/html)
308	4.168531952	172.16.116.35	10.2.192.21	TCP	66	53722 → 9000 [ACK] Seq=606 Ack=15208 Win=63616 Len=0 TSval=746931343 TSecr=543071489
363	4.954061743	194.58.31.81	172.16.116.176	TLSv1.2	93	Application Data
366	4.995556050	172.16.116.176	194.58.31.81	TCP	60	57350 → 443 [ACK] Seq=1 Ack=40 Win=4104 Len=0
375	5.112934715	172.16.116.35	10.2.192.21	HTTP	612	GET /hcsprod/styles.css HTTP/1.1
379	5.137102595	10.2.192.21	172.16.116.35	TCP	66	9000 → 53722 [ACK] Seq=15208 Ack=1152 Win=15511 Len=0 TSval=543072460 TSecr=746932286
380	5.143621346	10.2.192.21	172.16.116.35	TCP	236	9000 → 53722 [PSH, ACK] Seq=15208 Ack=1152 Win=15511 Len=170 TSval=543072465 TSecr=746932286 [TCP segment of a reassembled PDU]
381	5.143639738	172.16.116.35	10.2.192.21	TCP	66	53722 → 9000 [ACK] Seq=1152 Ack=15378 Win=64128 Len=0 TSval=746932317 TSecr=543072465
382	5.146742204	10.2.192.21	172.16.116.35	TCP	1490	9000 → 53722 [PSH, ACK] Seq=15378 Ack=1152 Win=15511 Len=1424 TSval=543072465 TSecr=746932286 [TCP segment of a reassembled PDU]
383	5.146756677	172.16.116.35	10.2.192.21	TCP	66	53722 → 9000 [ACK] Seq=1152 Ack=16802 Win=64128 Len=0 TSval=746932320 TSecr=543072465
384	5.146781561	10.2.192.21	172.16.116.35	HTTP	78	HTTP/1.1 200 OK (text/css)
385	5.146786440	172.16.116.35	10.2.192.21	TCP	66	53722 → 9000 [ACK] Seq=1152 Ack=16814 Win=64128 Len=0 TSval=746932320 TSecr=543072465
388	5.203077506	194.58.31.81	172.16.116.176	TLSv1.2	93	Application Data
392	5.243526376	172.16.116.176	194.58.31.81	TCP	60	57351 → 443 [ACK] Seq=1 Ack=40 Win=4103 Len=0
405	5.453766508	40.90.189.152	172.16.116.176	TCP	60	443 → 57450 [FIN, ACK] Seq=1 Ack=1 Win=262 Len=0
406	5.453853123	172.16.116.176	40.90.189.152	TCP	60	57450 → 443 [ACK] Seq=1 Ack=2 Win=4103 Len=0
407	5.453996294	172.16.116.176	40.90.189.152	TCP	60	57450 → 443 [FIN, ACK] Seq=1 Ack=2 Win=4103 Len=0
408	5.455062079	40.90.189.152	172.16.116.176	TCP	60	443 → 57450 [ACK] Seq=2 Ack=2 Win=262 Len=0
426	5.679332910	172.16.116.35	10.2.192.21	HTTP	618	GET /hcsprod/images/OPSE_logo.gif HTTP/1.1
427	5.679836052	172.16.116.35	10.2.192.21	TCP	74	53724 → 9000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=746932853 TSecr=0 WS=128
432	5.702448015	10.2.192.21	172.16.116.35	TCP	74	9000 → 53724 [SYN, ACK] Seq=0 Ack=1 Win=14360 Len=0 MSS=1436 WS=1 SACK_PERM=1 TSval=543073025 TSecr=746932853
433	5.702519786	172.16.116.35	10.2.192.21	TCP	66	53724 → 9000 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=746932876 TSecr=543073025
434	5.702835968	172.16.116.35	10.2.192.21	HTTP	623	GET /hcsprod/images/PT_LOGIN_ERROR.gif HTTP/1.1
435	5.703638562	10.2.192.21	172.16.116.35	TCP	66	9000 → 53722 [ACK] Seq=16814 Ack=1704 Win=16063 Len=0 TSval=543073026 TSecr=746932853
436	5.708542627	10.2.192.21	172.16.116.35	TCP	237	9000 → 53722 [ACK] Seq=16814 Ack=1704 Win=16063 Len=171 TSval=543073030 TSecr=746932853 [TCP segment of a reassembled PDU]
437	5.708562875	172.16.116.35	10.2.192.21	TCP	66	53722 → 9000 [ACK] Seq=1704 Ack=16985 Win=64128 Len=0 TSval=746932882 TSecr=543073030
439	5.712034755	10.2.192.21	172.16.116.35	TCP	1490	9000 → 53722 [PSH, ACK] Seq=16985 Ack=1704 Win=16063 Len=1424 TSval=543073030 TSecr=746932853 [TCP segment of a reassembled PDU]
440	5.712087270	172.16.116.35	10.2.192.21	TCP	66	53722 → 9000 [ACK] Seq=1704 Ack=18409 Win=64128 Len=0 TSval=746932885 TSecr=543073030
441	5.712526387	10.2.192.21	172.16.116.35	TCP	1490	9000 → 53722 [ACK] Seq=18409 Ack=1704 Win=16063 Len=1424 TSval=543073030 TSecr=746932853 [TCP segment of a reassembled PDU]
442	5.712563652	172.16.116.35	10.2.192.21	TCP	66	53722 → 9000 [ACK] Seq=1704 Ack=19833 Win=64128 Len=0 TSval=746932886 TSecr=543073030
443	5.713583459	10.2.192.21	172.16.116.35	TCP	1290	9000 → 53722 [ACK] Seq=19833 Ack=1704 Win=16063 Len=1224 TSval=543073030 TSecr=746932853 [TCP segment of a reassembled PDU]
444	5.713607506	172.16.116.35	10.2.192.21	TCP	66	53722 → 9000 [ACK] Seq=1704 Ack=21957 Win=64128 Len=0 TSval=746932887 TSecr=543073030
445	5.714565021	10.2.192.21	172.16.116.35	TCP	1490	9000 → 53722 [ACK] Seq=21957 Ack=1704 Win=16063 Len=1424 TSval=543073030 TSecr=746932853 [TCP segment of a reassembled PDU]
446	5.714580751	172.16.116.35	10.2.192.21	TCP	66	53722 → 9000 [ACK] Seq=1704 Ack=22401 Win=64128 Len=0 TSval=746932888 TSecr=543073030

0000 b0 0b cf d7 07 09 00 27 8e 56 73 08 00 45 00 ..... Vs: E  
0010 01 40 40 5f 40 00 40 06 60 77 2f 10 74 73 0a 02 ..... AIA: h...F...



## Total Time taken to download

The Total time taken for download of the entire webpage measured as the time at which the first request was sent and the time when the last packet was received.

So the answer is  $(4.168500 - 4.10983) = 0.05867s$

No.	Time	Source	Destination	Protocol	Length	Info
282	4.109837291	172.16.116.35	10.2.102.21	HTTP	671	GET /psp/hcsprod/EMPLOYEE/HRMS/h/?tab=DEFAULT&cmd=login&errorCode=106&languageCd=ENG HTTP/1.1
307	4.168500152	10.2.102.21	172.16.116.35	HTTP	611	HTTP/1.1 200 OK (text/html)
375	5.112934715	172.16.116.35	10.2.102.21	HTTP	612	GET /hcsprod/styles.css HTTP/1.1
384	5.146781561	10.2.102.21	172.16.116.35	HTTP	78	HTTP/1.1 200 OK (text/css)
426	5.679332910	172.16.116.35	10.2.102.21	HTTP	618	GET /hcsprod/images/OPSE_logo.gif HTTP/1.1
434	5.702835968	172.16.116.35	10.2.102.21	HTTP	623	GET /hcsprod/images/PT_LOGIN_ERROR.gif HTTP/1.1
451	5.717679871	10.2.102.21	172.16.116.35	HTTP	1780	HTTP/1.1 200 OK (GIF89a)
458	5.735720825	10.2.102.21	172.16.116.35	HTTP	276	HTTP/1.1 200 OK (GIF89a)
463	5.818326657	172.16.116.35	10.2.102.21	HTTP	487	GET /favicon.ico HTTP/1.1
473	5.847061224	10.2.102.21	172.16.116.35	HTTP	1230	HTTP/1.1 404 Not Found (text/html)

> Frame 307: 611 bytes on wire (4888 bits), 611 bytes captured (4888 bits) on interface enp0s3, id 0  
> Ethernet II, Src: Cisco\_d7:b0:07 (b0:8b:cf:d7:b0:07), Dst: PcsCompu\_8e:56:73 (08:00:27:8e:56:73)  
> Internet Protocol Version 4, Src: 10.2.102.21, Dst: 172.16.116.35  
> Transmission Control Protocol, Src Port: 9000, Dst Port: 53722, Seq: 14663, Ack: 606, Len: 545  
> [12 Reassembled TCP Segments (15207 bytes): #285(422), #287(1424), #289(1424), #291(1424), #293(1424), #295(1424), #297(1424), #299(1424), #301(1424), #303(1424), #305(1424)]  
v Hypertext Transfer Protocol  
  > HTTP/1.1 200 OK\r\n  
    Cache-Control: no-cache\r\n  
    Cache-Control: no-store\r\n  
    Date: Fri, 07 Feb 2020 15:56:14 GMT\r\n  
  > Content-Length: 14785\r\n  
    Content-Type: text/html; CHARSET=utf-8\r\n  
    Expires: Thu, 01 Dec 1994 16:00:00 GMT\r\n  
    Set-Cookie: HCSPROD-PORTAL-PSJSESSIONID=Q4kgXavu0vc7kkiY4aJcljjFb7jvq02w!242498606; path=/; HttpOnly\r\n  
    Set-Cookie: PS\_TOKEN=; domain=; expires=Thu, 01-Jan-1970 01:00:00 GMT; path=/\r\n  
    RespondingWithSignonPage: true\r\n  
    \r\n  
    [HTTP response 1/4]  
    [Time since request: 0.058662861 seconds]  
    [Request in frame: 282]  
    [Next request in frame: 375]  
    [Next response in frame: 384]  
    [Request URI: http://10.2.102.21:9000/psp/hcsprod/EMPLOYEE/HRMS/h/?tab=DEFAULT&cmd=login&errorCode=106&languageCd=ENG]  
    File Data: 14785 bytes  
  > Line-based text data: text/html (281 lines)

## No TCP losses/retransmits were noticed