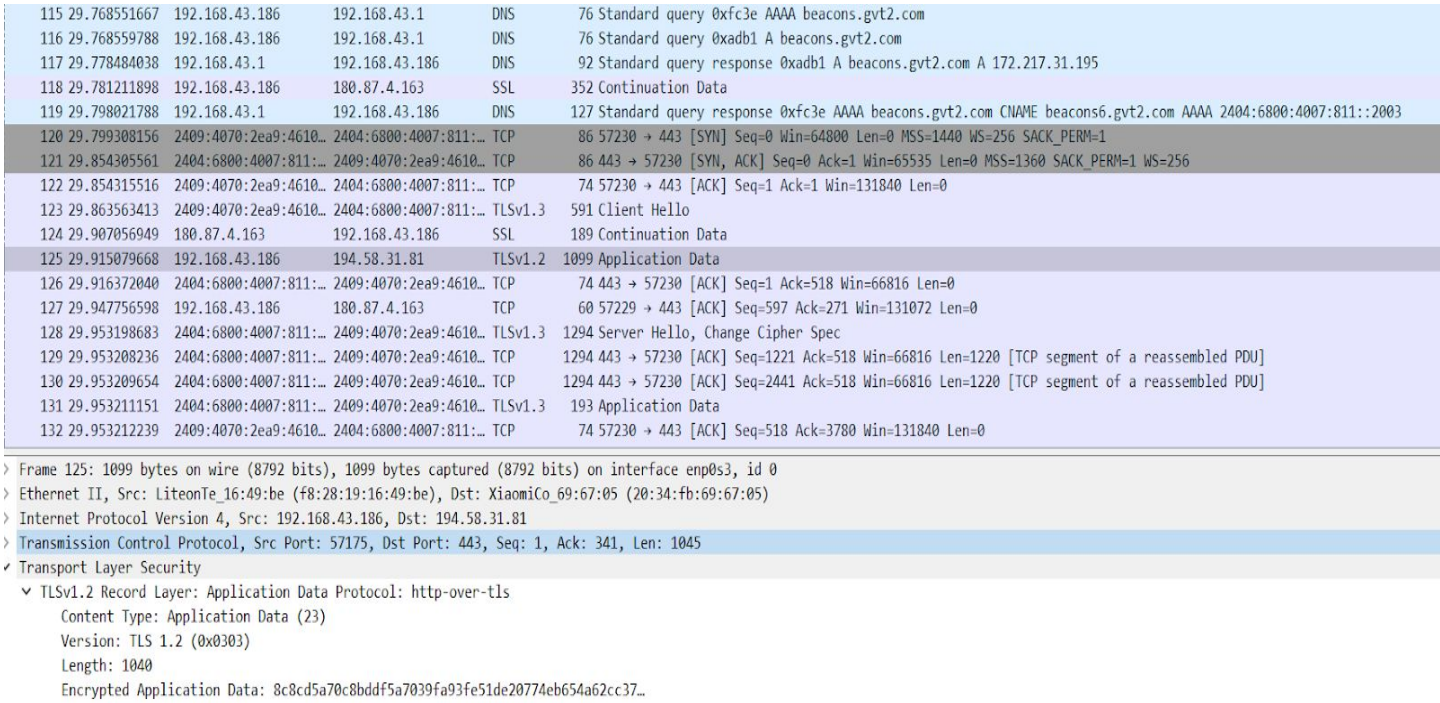
PACKET ANALYSIS

(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



Simple Service Discovery Protocol

No.	Time	Source	Destination	Protocol	Length	Info
55	18.585163007	2404:6800:4007:809:…	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:…	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:…	TCP	74	57170 → 443 [ACK] Seq=3 Ack=58 Win=510 Len=0
58	18.676767612	2409:4070:2ea9:4610…	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
v Simple Service Discovery Protocol
  v 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:…	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:…	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:…	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)
v 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

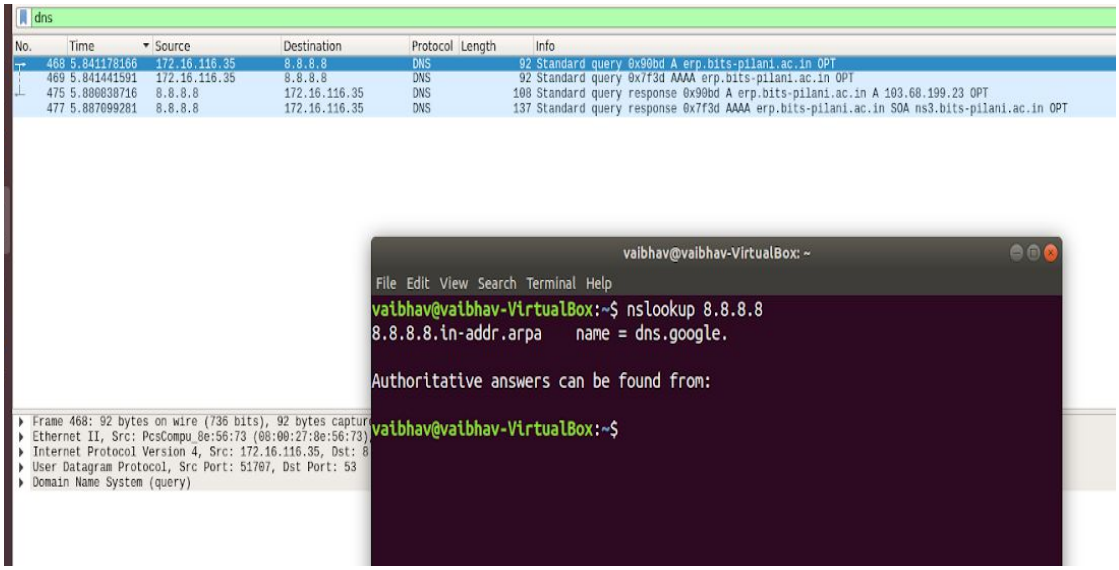
Website Visited:

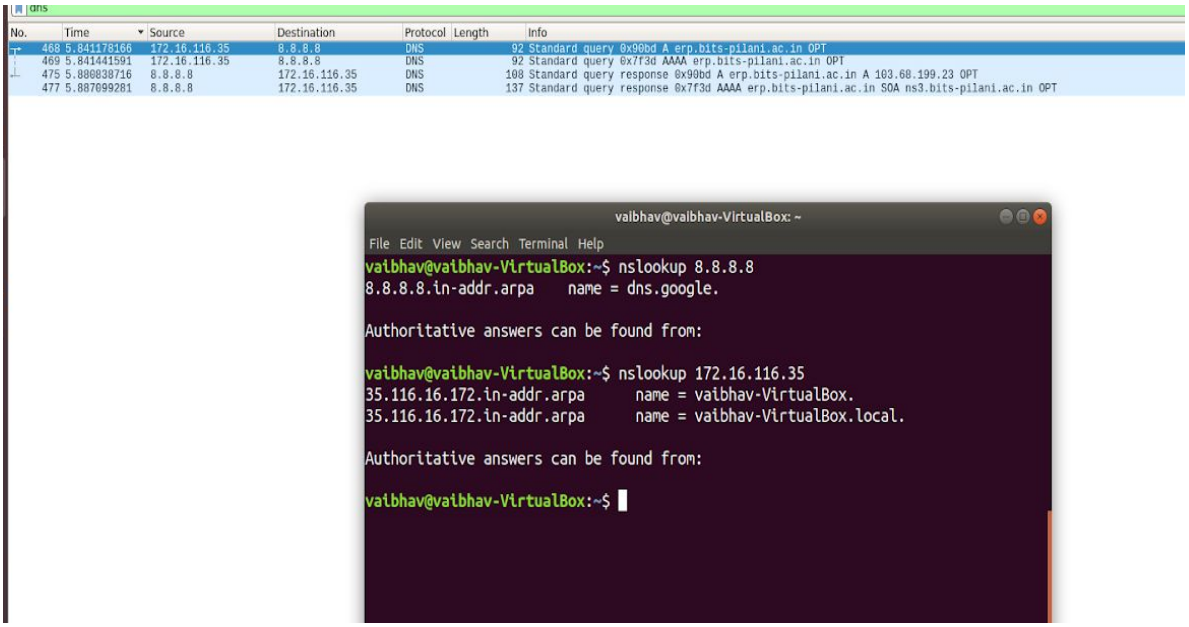
http://10.2.102.21:9000/psp/hcsprod/EMPLOYEE/HRMS/h/?tab=DEFAULT

Servers for which DNS query was launched are

8.8.8.8.in-addr.arpa → dns.google

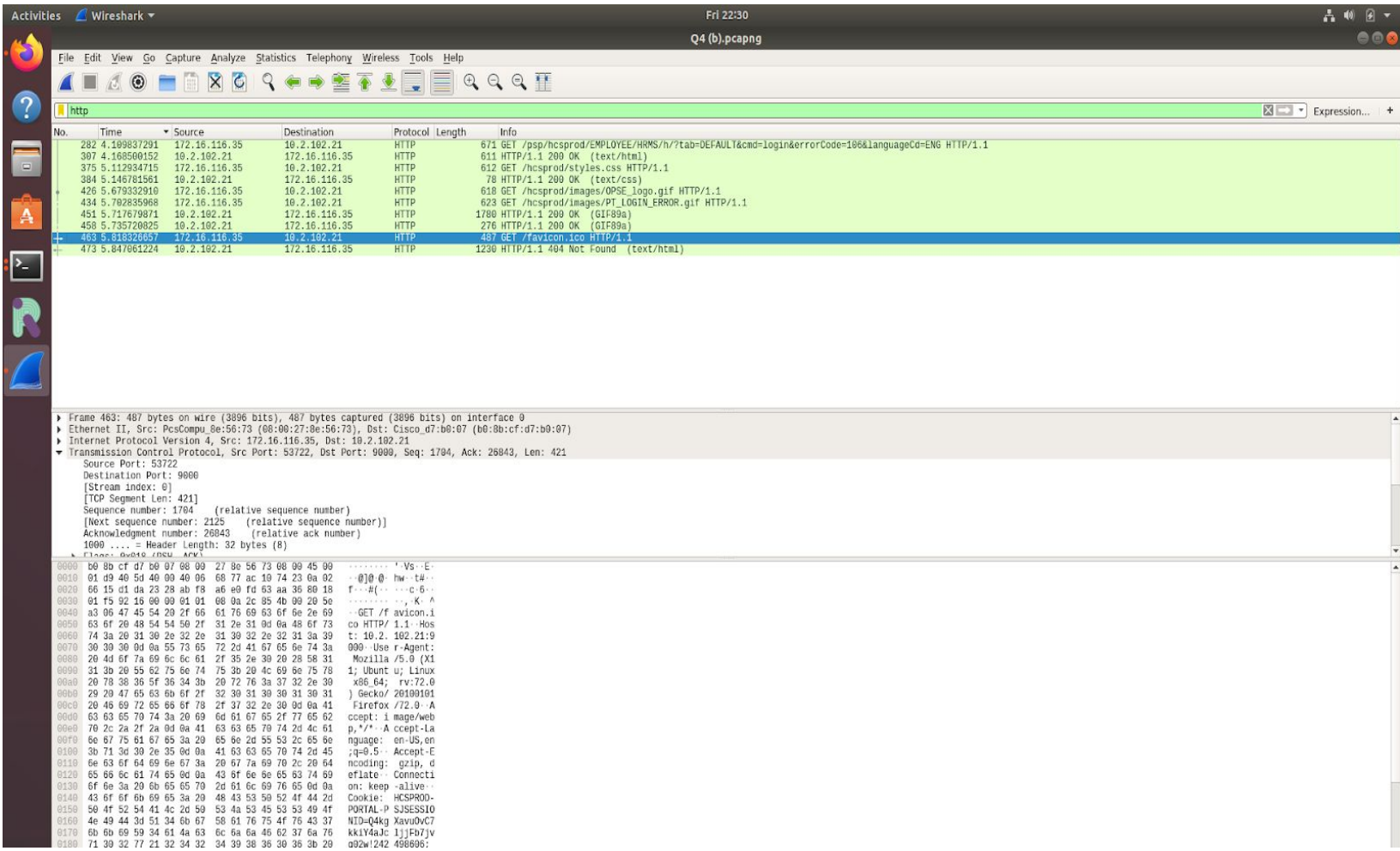
35.116.16.172.in-addr.arpa → vaibhav-VirtualBox





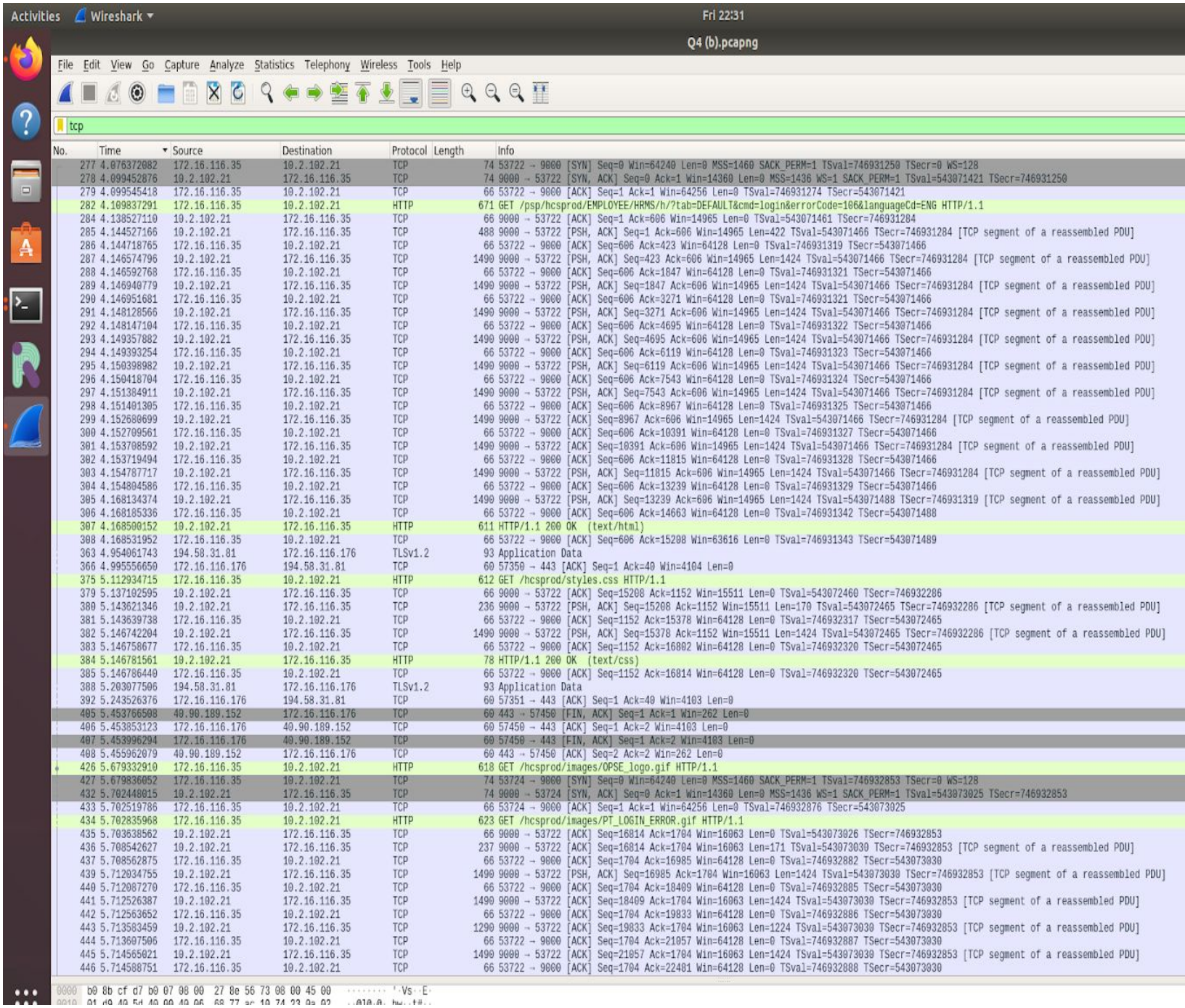
Number of HTTP requests generated:

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



The number of TCP connections opened:

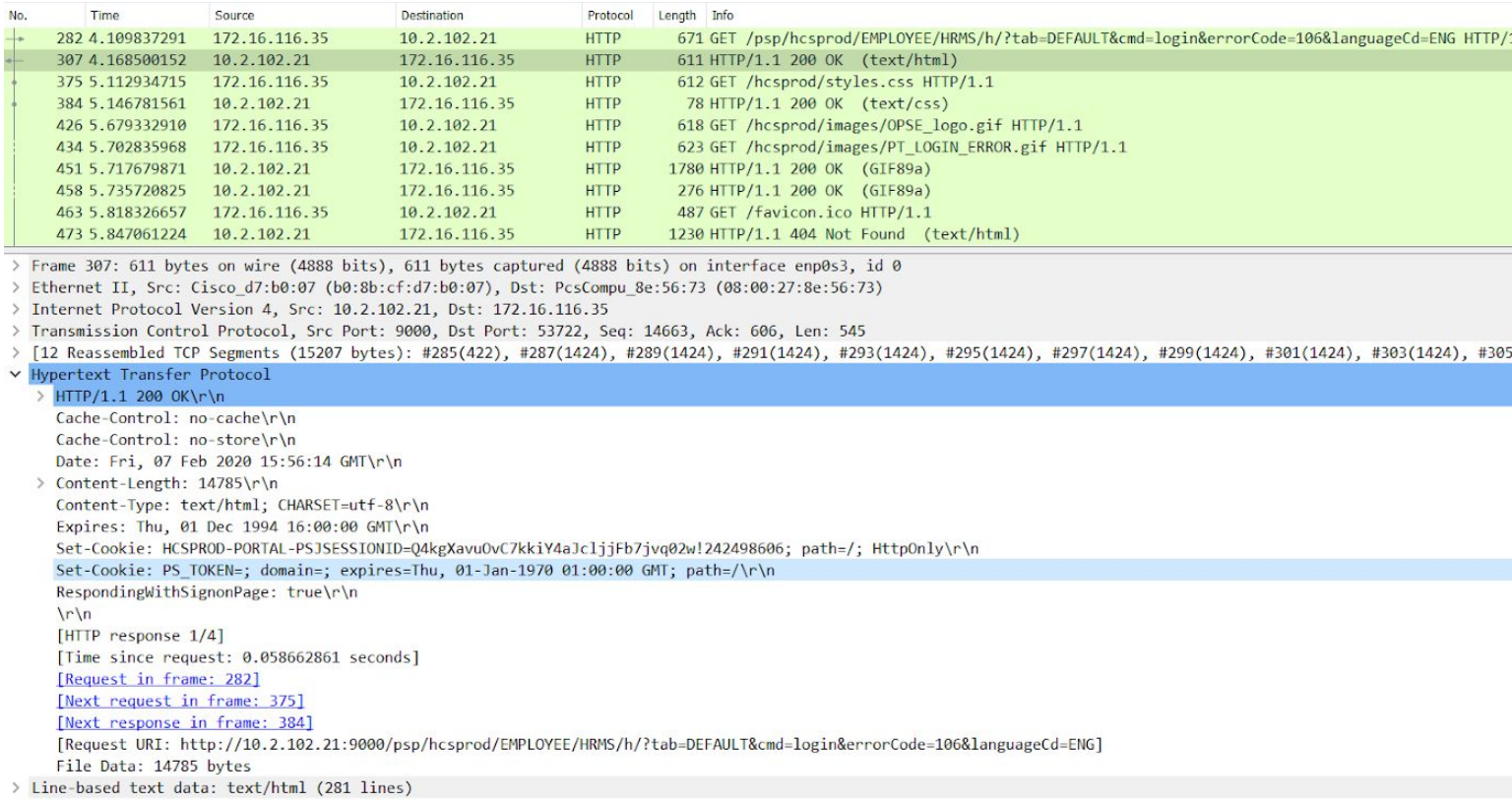
The number of TCP connections opened are 4 (ones with SYN including acknowledgment)



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
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
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=Q4kgXavuOvC7kkiY4aJc1jjFb7jvq02w!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