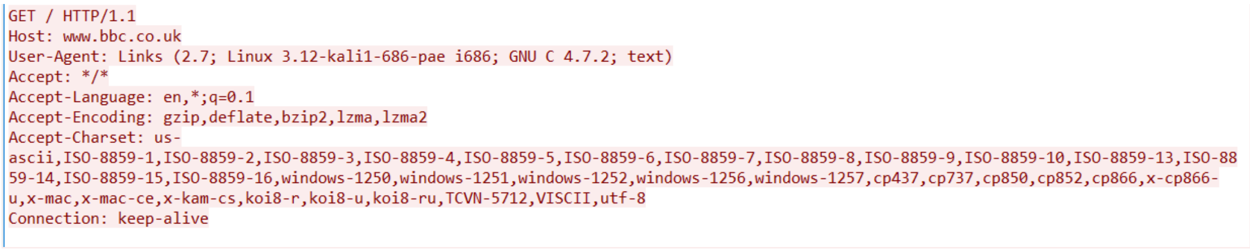
Digital Forensics Lab Task (Week 7)

- What was the browser used to visit www.bbc.co.uk for the first time in the session?
- What operating system might the user be utilizing in order to run the browser in the previous question?
- What other browser was used to visit websites according to TCP stream 26?
- Looking at TCP Stream 0, and highlighting packet identifiers 31-33 – what kind of interaction is taking place here?
- What is the title of the homepage associated with 152.19.134.41, from where did the user access this page and how can you
  tell?
- Looking at packets no. 22309 to 22323, there seems to be some anomalous behavior here – what is it and what is its purpose?
- What MAC address is associated with the IP address 192.168.142.2 and what protocol might you want to peruse more closely on the packet capture in order to determine this?

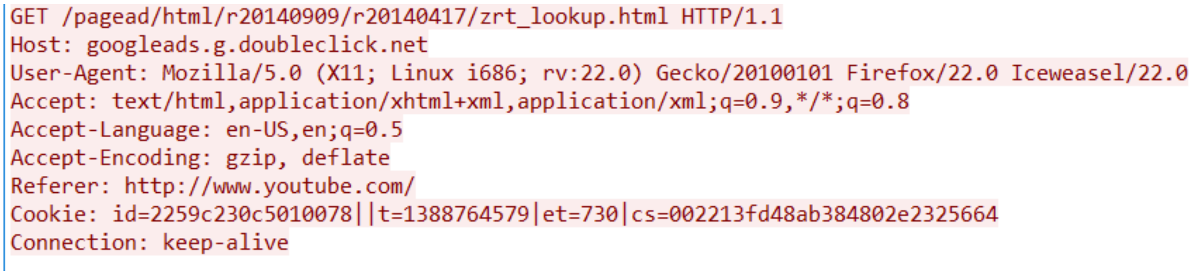
Answers:

The browser used during this session was Links browser and the OS used during this session was 2.7; Linux 3.12-kali1-686-pae i686; GNU C 4.7.2. The filter used to find this was http.



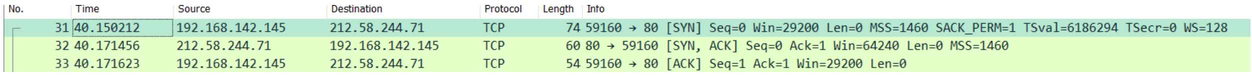
```
GET / HTTP/1.1
Host: www.bbc.co.uk
User-Agent: Links (2.7; Linux 3.12-kali1-686-pae i686; GNU C 4.7.2; text)
Accept: */*
Accept-Language: en,*;q=0.1
Accept-Encoding: gzip,deflate,bzip2,lzma,lzma2
Accept-Charset: us-
ascii,ISO-8859-1,ISO-8859-2,ISO-8859-3,ISO-8859-4,ISO-8859-5,ISO-8859-6,ISO-8859-7,ISO-8859-8,ISO-8859-9,ISO-8859-10,ISO-8859-13,ISO-88
59-14,ISO-8859-15,ISO-8859-16,windows-1250,windows-1251,windows-1252,windows-1256,windows-1257,cp437,cp737,cp850,cp852,cp866,x-cp866-
u,x-mac,x-mac-ce,x-kam-cs,koi8-r,koi8-u,koi8-ru,TCVN-5712,VISCII,utf-8
Connection: keep-alive
```

According to TCP stream 26 the other browser used was Mozilla/5.0. This result was found using filter tcp.stream eq 26 in wireshark.



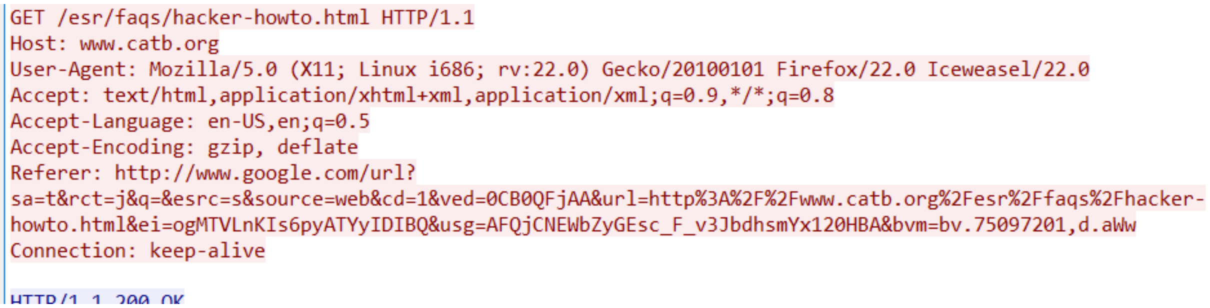
```
GET /pagead/html/r20140909/r20140417/zrt_lookup.html HTTP/1.1
Host: googleads.g.doubleclick.net
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:22.0) Gecko/20100101 Firefox/22.0 Iceweasel/22.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.youtube.com/
Cookie: id=2259c230c5010078||t=1388764579|et=730|cs=002213fd48ab384802e2325664
Connection: keep-alive
```

TCP 3-way handshake was performed in TCP stream 0 when observing packet identifiers from 31 to 33 using filter tcp.stream eq 0 in wireshark. In packet ID 31 sync is performed where and acknowledgement is sent to the website from host device, in packet ID 32 the server receives the sync and acknowledgement and in packet ID 33 the host receives information that the server has acknowledged the connection request.

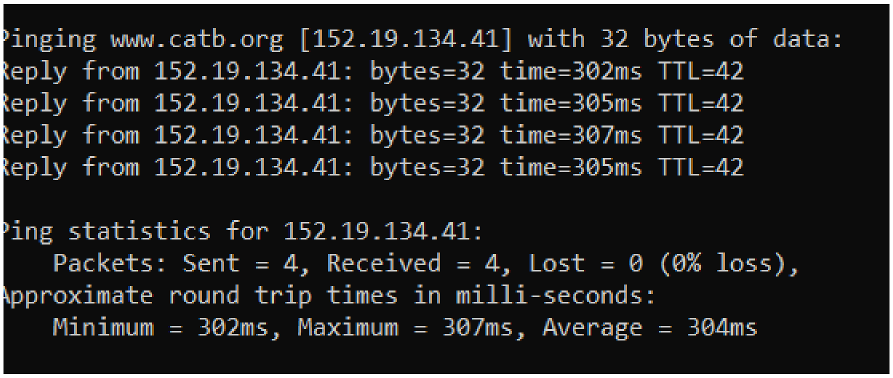


No.	Time	Source	Destination	Protocol	Length	Info
31	40.150212	192.168.142.145	212.58.244.71	TCP	74	59160 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=6186294 TSecr=0 WS=128
32	40.171456	212.58.244.71	192.168.142.145	TCP	60	80 → 59160 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
33	40.171623	192.168.142.145	212.58.244.71	TCP	54	59160 → 80 [ACK] Seq=1 Ack=1 Win=29200 Len=0

The title of the homepage associated with the ip address 152.19.134.41 is Eric S. Raymond's Home Page. This home page was accessed from www.catb.org by using the filter ip.addr == 152.19.134.41 in wireshark and following the http or tcp stream.

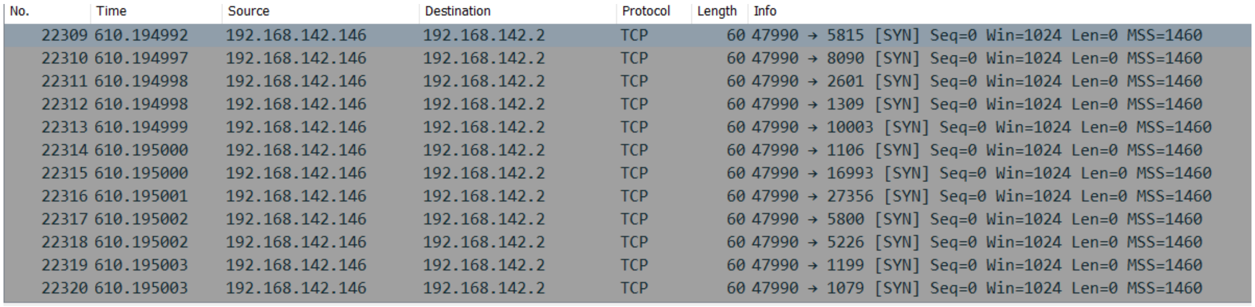


```
GET /esr/faqs/hacker-howto.html HTTP/1.1
Host: www.catb.org
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:22.0) Gecko/20100101 Firefox/22.0 Iceweasel/22.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.google.com/url?
sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CB0QFjAA&url=http%3A%2F%2Fwww.catb.org%2Fesr%2Ffaqs%2Fhacker-
howto.html&ei=ogMTVLnKIs6pyATYyIDIBQ&usg=AFQjCNEWbZyGEsc_F_v3JbdhsmYx120HBA&bvm=bv.75097201,d.aWw
Connection: keep-alive

HTTP/1.1 200 OK
```



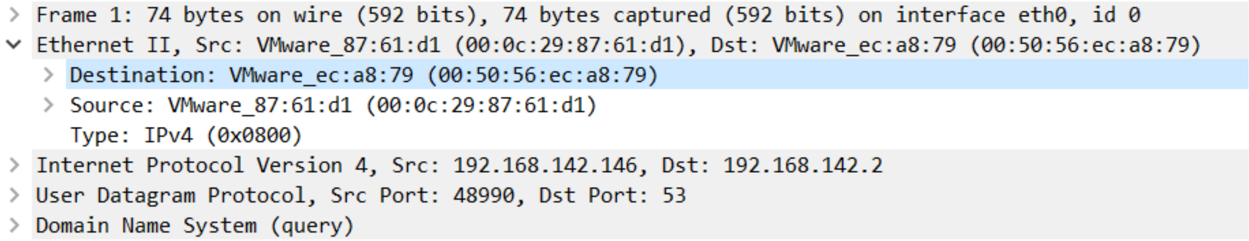
```
Pinging www.catb.org [152.19.134.41] with 32 bytes of data:
Reply from 152.19.134.41: bytes=32 time=302ms TTL=42
Reply from 152.19.134.41: bytes=32 time=305ms TTL=42
Reply from 152.19.134.41: bytes=32 time=307ms TTL=42
Reply from 152.19.134.41: bytes=32 time=305ms TTL=42

Ping statistics for 152.19.134.41:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 302ms, Maximum = 307ms, Average = 304ms
```

In ID 22309 to 22323 there seems to be an attempt to attack the server using TCP SYN Flood (a type of DDoS attack) where multiple SYN requests are sent to the server to keep the server busy. This was found by observing the ID from 22309 to 22323 where we can see multiple SYN requests being sent to the server and from 22324 onward, we can see the server is denying these requests as there was detection of some anomalous activities.



```
No.    Time          Source            Destination      Protocol  Length  Info
22309 610.194992    192.168.142.146   192.168.142.2    TCP       60 47990 → 5815 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
22310 610.194997    192.168.142.146   192.168.142.2    TCP       60 47990 → 8090 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
22311 610.194998    192.168.142.146   192.168.142.2    TCP       60 47990 → 2601 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
22312 610.194998    192.168.142.146   192.168.142.2    TCP       60 47990 → 1309 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
22313 610.194999    192.168.142.146   192.168.142.2    TCP       60 47990 → 10003 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
22314 610.195000    192.168.142.146   192.168.142.2    TCP       60 47990 → 1106 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
22315 610.195000    192.168.142.146   192.168.142.2    TCP       60 47990 → 16993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
22316 610.195001    192.168.142.146   192.168.142.2    TCP       60 47990 → 27356 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
22317 610.195002    192.168.142.146   192.168.142.2    TCP       60 47990 → 5800 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
22318 610.195002    192.168.142.146   192.168.142.2    TCP       60 47990 → 5226 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
22319 610.195003    192.168.142.146   192.168.142.2    TCP       60 47990 → 1199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
22320 610.195003    192.168.142.146   192.168.142.2    TCP       60 47990 → 1079 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
```

The mac address associated with the ip address 192.168.142.2 is 00:50:56:ec:a8:79.



```
> Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
v Ethernet II, Src: VMware_87:61:d1 (00:0c:29:87:61:d1), Dst: VMware_ec:a8:79 (00:50:56:ec:a8:79)
  > Destination: VMware_ec:a8:79 (00:50:56:ec:a8:79)
  > Source: VMware_87:61:d1 (00:0c:29:87:61:d1)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.142.146, Dst: 192.168.142.2
> User Datagram Protocol, Src Port: 48990, Dst Port: 53
> Domain Name System (query)
```

The protocol used to determine the mac address were ARP and DNS protocols.