Miguel Alvarez, Fabricio Rua-Sanchez, Martin Bernard

A. fe80::a00:27ff:fed7:b608

B. 10.0.2.15

C. fe80::a00:27ff:fe07:87af/64

D. 10.0.2.4

E.

```
┌──(martin㉿kali)-[~]
└─$ netstat -rn                                                    130 ×
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Ifac
e
0.0.0.0         10.0.2.2        0.0.0.0         UG        0 0          0 eth0
10.0.2.0        0.0.0.0         255.255.255.0   U         0 0          0 eth0
```

F.

```
┌──(martin㉿kali)-[~]
└─$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.2                 ether   52:54:00:12:35:02   C                     eth0
```

G.

```
msfadmin@metasploitable:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
10.0.2.0        *               255.255.255.0   U         0 0          0 eth0
default         10.0.2.1        0.0.0.0         UG        0 0          0 eth0
msfadmin@metasploitable:~$
```

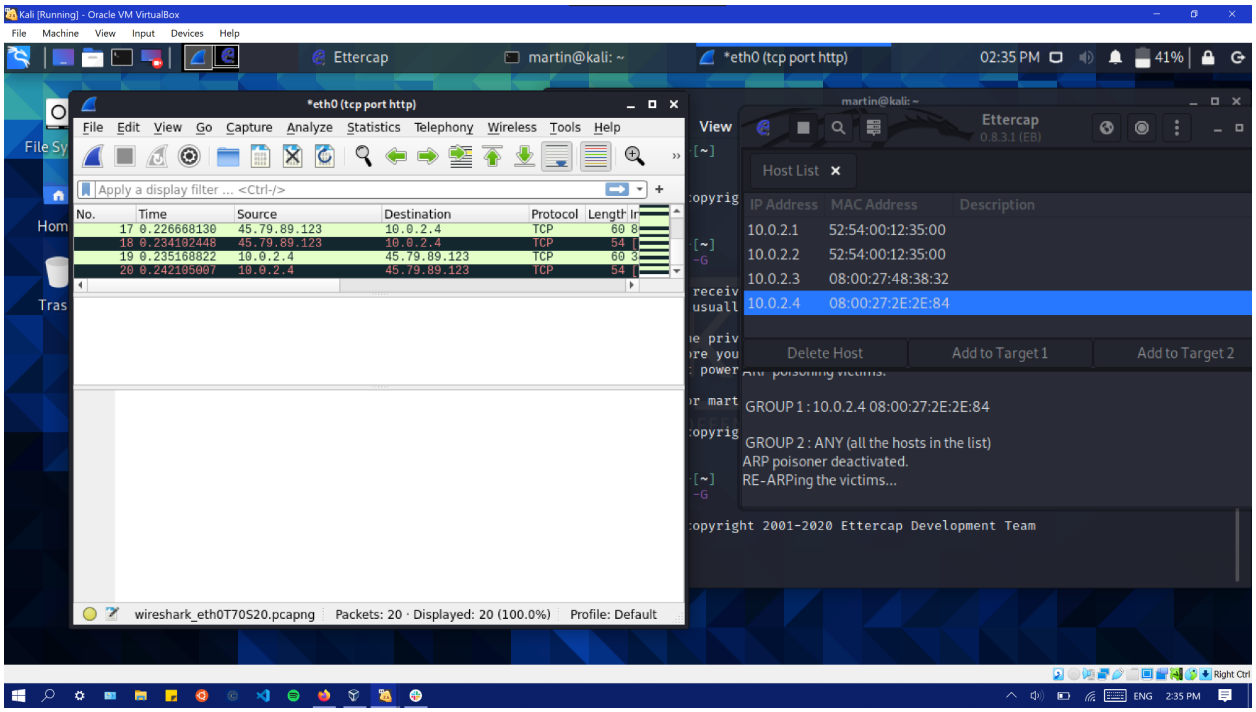
H.

```
msfadmin@metasploitable:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.1                 ether   52:54:00:12:35:00   C                     eth0
msfadmin@metasploitable:~$
```

I. The MAC address of the server that's hosting Jeff's website because that's the piece of software that we're requesting it from.

J. Yes, we see an HTTP response on Metasploitable but we do not see any captured packets in Wireshark.

K.



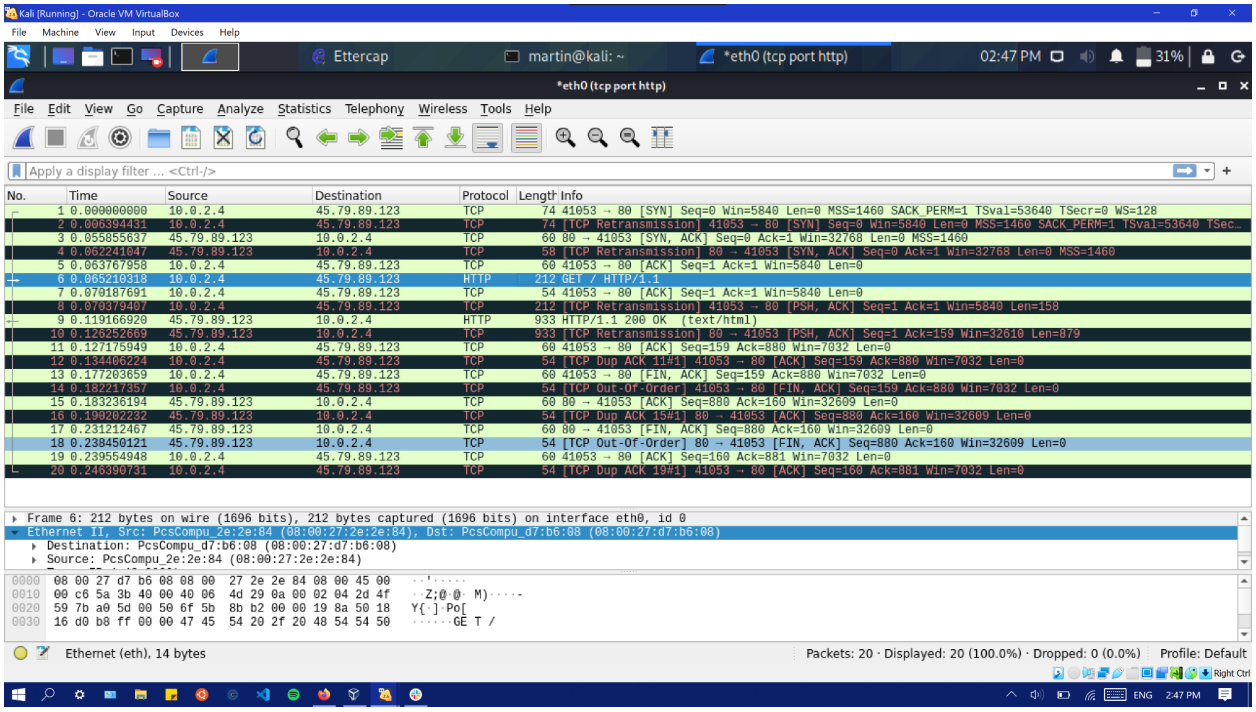
L.

```
msfadmin@metasploitable:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.3                 ether   08:00:27:48:38:32   C                     eth0
10.0.2.2                 ether   52:54:00:12:35:00   C                     eth0
10.0.2.1                 ether   52:54:00:12:35:00   C                     eth0
msfadmin@metasploitable:~$ _
```

There are two more addresses/connections in the arp cache. This is because this shows the connection with the person in the middle (aka Kali).

M. Metasploitable sends the [SYN] packet to 08:00:27:d7:b6:08, which is the MAC address of my Kali. It sends it to Kali because Kali is the man in the middle listening to network activities.

N.



O. We see a response on Metasploitable, we are able to get Jeff's website. We can also see the capture packets between metasploitable and the server. We're able to see the TCP handshake as well the status codes (200 OK) and GET responses.

P. Kali used ettercap to send ARP packets to Metasploitable, this added a new IP and MAC address to the ARP cache causing Metasploitable to send all traffic to Kali where we use Wireshark to view the incoming traffic.

Q. Our ARP detector would compare the initial ARP cache to the one after an HTTP request. This would show the changes in the ARP cache and see what addresses/connections have been added. This might detect false positives if you have other devices connected to the computer like a printer or other similar devices.