

Ariana Borlak

===== EXECUTION =====

a. 00:0c:29:c5:f8:ff

b. 172.16.32.128

c. 00:0c:29:d6:11:c7

d. 172.16.34.129

e.

```
(kali㉿kali)-[~]  
$ netstat -rn  
Kernel IP routing table  
Destination      Gateway          Genmask          Flags   MSS Window  irtt Iface  
0.0.0.0           172.16.34.2      0.0.0.0          UG      0 0        0 eth0  
172.16.34.0       0.0.0.0          255.255.255.0    U      0 0        0 eth0
```

f.

```
(kali㉿kali)-[~]  
$ arp -n  
Address           HWtype  HWaddress         Flags Mask          Iface  
172.16.34.2       ether    00:50:56:f8:24:ca C                  eth0  
172.16.34.254     ether    00:50:56:fe:82:ea C                  eth0
```

g.

```
msfadmin@metasploitable:~$ netstat -rn  
Kernel IP routing table  
Destination      Gateway          Genmask          Flags   MSS Window  irtt Iface  
172.16.34.0       0.0.0.0          255.255.255.0    U      0 0        0 eth0  
0.0.0.0           172.16.34.2      0.0.0.0          UG      0 0        0 eth0
```

h.

```
msfadmin@metasploitable:~$ arp -n  
Address           HWtype  HWaddress         Flags Mask          Iface  
172.16.34.254     ether    00:50:56:FE:82:EA C                  eth0
```

i. The website has an ip address of 172.16.34.2

===== SYNTHESIS =====

q. Yes, Wireshark can detect it but you have to save old information