A.

00:0c:29:2f:90:c6

B.

192.168.221.129

C.

00:0c:29:35:f7:36

D.

192.168.221.128

E.

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Ifac
e
default         192.168.221.2   0.0.0.0         UG        0 0          0 eth0
192.168.221.0   0.0.0.0         255.255.255.0   U         0 0          0 eth0
```

F.

```
┌──(kali㉿kali)-[~]
└─$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.221.2            ether   00:50:56:e8:1d:31   C                     eth0
192.168.221.254          ether   00:50:56:f7:3e:03   C                     eth0
```

G and H.

```
msfadmin@metasploitable:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.221.0   *               255.255.255.0   U         0 0          0 eth0
default         192.168.221.2   0.0.0.0         UG        0 0          0 eth0
msfadmin@metasploitable:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.221.254          ether   00:50:56:F7:3E:03   C                     eth0
192.168.221.2            ether   00:50:56:E8:1D:31   C                     eth0
```

I.

It should probably send the packet using 00:50:56:f7:3E:03, since I believe the other MAC address is only for local communication.

J.

I saw an HTTP response from metasploitable on wireshark, but no packets were captured.

L.

Strangely enough, while it was poisoning Metasploitable it changed the MAC address of it to be the same as Kali's MAC address. Then after a while it just added the Kali MAC address within the ARP cache of metasploitable.

M.

My best guess would be that it would either still send from Kali's MAC address 00:0c:29:2f:90:c6, since before it was only using the vm of metasploitable to communicate, but now that they've merged it'll use the one from Kali.

O.

I now see both the HTTP response and the captured packets. I now can also see the messages between Metasploitable and your site.

P.

From what I could tell on Ettercap, it made the server on Metasploitable communicate with Kali, and then from looking at the packets contrary to what I thought before where it just added Kali's MAC address to the ARP cache, according to wireshark it actually created a duplicate of both Kali's MAC address and IP addresses and gave them to Metasploitable.

Then I'm guessing that the reason wireshark was able to pick up on the packets with 'tcp port http' this time was because by Ettercap's interference Metasploitable posed as Kali when communicating with cs338.jeffondich, and then when it communicated back it started doing what we've seen in class with other MITM scenarios where is would transfer data to Kali and then Kali would answer back and allow the illusion that Metasploitable is Kali to continue on.

Q.

I’d probably need the detector to be able to detect when its MAC address has been duplicated (if possible) and then have it detect if any unwanted MAC address has been added to its ARP.