Angela Ellis in collaboration with Kai Johnson

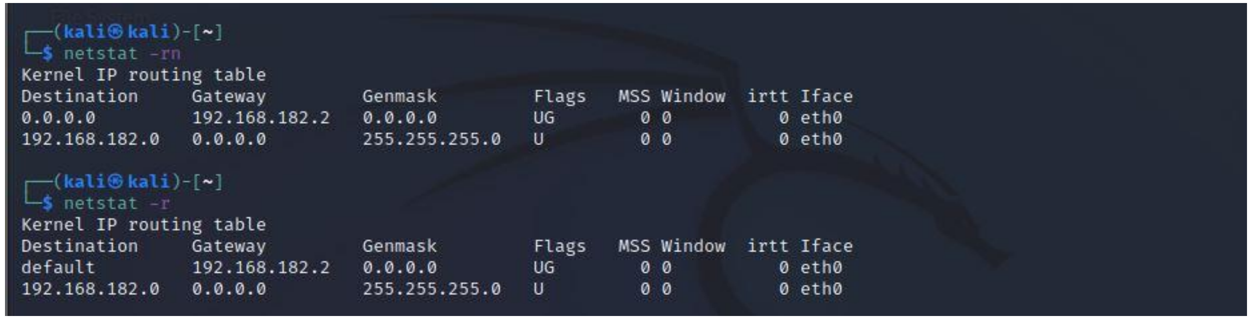
a] Kali's MAC Address: 00:0c:29:6d:09:89

b] Kali's IP Address: 192.168.182.128

c] Metasploitable MAC: 00:0c:29:10:bd:07

d] Metasploitable IP: 192.168.182.129

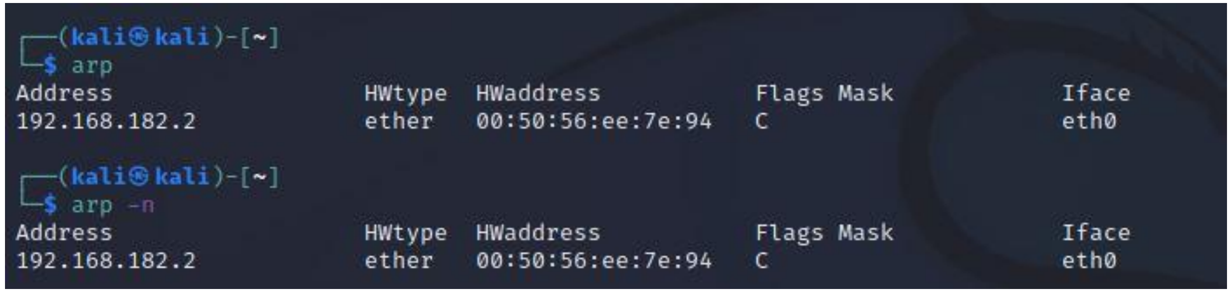
e] Kali Routing Tables



```
┌──(kali㉿kali)-[~]
└─$ netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         192.168.182.2   0.0.0.0         UG        0 0          0 eth0
192.168.182.0   0.0.0.0         255.255.255.0   U         0 0          0 eth0

┌──(kali㉿kali)-[~]
└─$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         192.168.182.2   0.0.0.0         UG        0 0          0 eth0
192.168.182.0   0.0.0.0         255.255.255.0   U         0 0          0 eth0
```

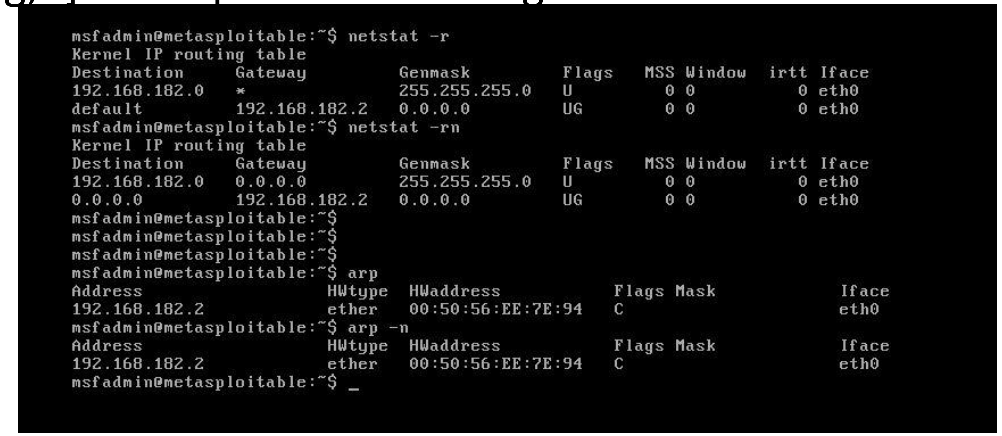
f] Kali ARP Cache



```
┌──(kali㉿kali)-[~]
└─$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.182.2            ether   00:50:56:ee:7e:94   C                     eth0

┌──(kali㉿kali)-[~]
└─$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.182.2            ether   00:50:56:ee:7e:94   C                     eth0
```

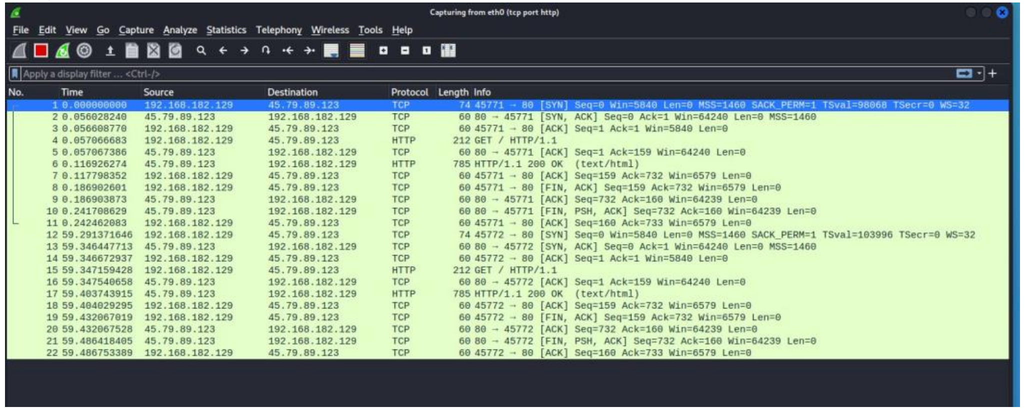
g,h] Metasploitable Routing Table & ARP Cache



```
msfadmin@metasploitable:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.182.0   *               255.255.255.0   U         0 0          0 eth0
default         192.168.182.2   0.0.0.0         UG        0 0          0 eth0
msfadmin@metasploitable:~$ netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.182.0   0.0.0.0         255.255.255.0   U         0 0          0 eth0
0.0.0.0         192.168.182.2   0.0.0.0         UG        0 0          0 eth0
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.182.2            ether   00:50:56:EE:7E:94   C                     eth0
msfadmin@metasploitable:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.182.2            ether   00:50:56:EE:7E:94   C                     eth0
msfadmin@metasploitable:~$ _
```

i] 00:50:56:ee:7e:94, MAC Address of IP 192.168.182.2
This the routing machine for Metasploitable. Because the requested HTTP do not exist locally on Metasploitable, it has to go beyond its own network to find it. The router, aka gateway, is the next step in receiving the HTTP.

j] Metasploitable terminal contains HTML. Image below of captured packets on Kali.

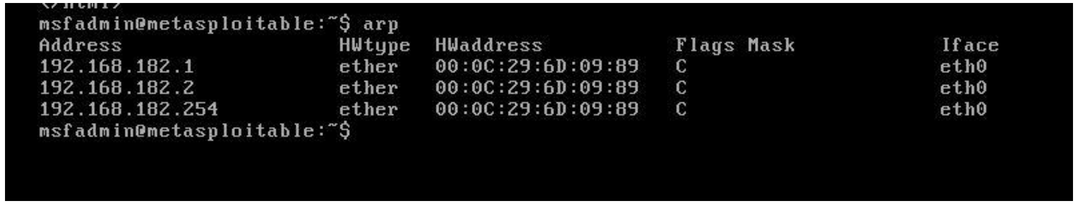


Capturing from eth0 (tcp port http)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Time          Source           Destination      Protocol Length Info
   1 0.000000000   192.168.182.129  45.79.89.123     TCP        74 45771 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=98068 TSecr=0 WS=32
   2 0.056028240   45.79.89.123     192.168.182.129  TCP        60 80 → 45771 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
   3 0.056608770   192.168.182.129  45.79.89.123     TCP        60 45771 → 80 [ACK] Seq=1 Ack=1 Win=5840 Len=0
   4 0.057066683   192.168.182.129  45.79.89.123     HTTP      212 GET / HTTP/1.1
   5 0.057067386   45.79.89.123     192.168.182.129  TCP        60 80 → 45771 [ACK] Seq=1 Ack=159 Win=64240 Len=0
   6 0.116926274   45.79.89.123     192.168.182.129  HTTP      785 HTTP/1.1 200 OK  (text/html)
   7 0.117798352   192.168.182.129  45.79.89.123     TCP        60 45771 → 80 [ACK] Seq=159 Ack=732 Win=6579 Len=0
   8 0.186902601   192.168.182.129  45.79.89.123     TCP        60 45771 → 80 [FIN, ACK] Seq=159 Ack=732 Win=6579 Len=0
   9 0.186903873   45.79.89.123     192.168.182.129  TCP        60 80 → 45771 [ACK] Seq=732 Ack=160 Win=64239 Len=0
  10 0.241708629   45.79.89.123     192.168.182.129  TCP        60 80 → 45771 [FIN, PSH, ACK] Seq=732 Ack=160 Win=64239 Len=0
  11 0.242462083   192.168.182.129  45.79.89.123     TCP        60 45771 → 80 [ACK] Seq=160 Ack=733 Win=6579 Len=0
  12 59.291371646  192.168.182.129  45.79.89.123     TCP        74 45772 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=103996 TSecr=0 WS=32
  13 59.346447713  45.79.89.123     192.168.182.129  TCP        60 80 → 45772 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
  14 59.346672937  192.168.182.129  45.79.89.123     TCP        60 45772 → 80 [ACK] Seq=1 Ack=1 Win=5840 Len=0
  15 59.347159428  192.168.182.129  45.79.89.123     HTTP      212 GET / HTTP/1.1
  16 59.347540658  45.79.89.123     192.168.182.129  TCP        60 80 → 45772 [ACK] Seq=1 Ack=159 Win=64240 Len=0
  17 59.403743915  45.79.89.123     192.168.182.129  HTTP      785 HTTP/1.1 200 OK  (text/html)
  18 59.404029295  192.168.182.129  45.79.89.123     TCP        60 45772 → 80 [ACK] Seq=159 Ack=732 Win=6579 Len=0
  19 59.432067019  192.168.182.129  45.79.89.123     TCP        60 45772 → 80 [FIN, ACK] Seq=159 Ack=732 Win=6579 Len=0
  20 59.432067528  45.79.89.123     192.168.182.129  TCP        60 80 → 45772 [ACK] Seq=732 Ack=160 Win=64239 Len=0
  21 59.486418405  45.79.89.123     192.168.182.129  TCP        60 80 → 45772 [FIN, PSH, ACK] Seq=732 Ack=160 Win=64239 Len=0
  22 59.486753389  192.168.182.129  45.79.89.123     TCP        60 45772 → 80 [ACK] Seq=160 Ack=733 Win=6579 Len=0
```

k] ...

l] Two new entries in the cache: 192.168.182.1, 192.168.182.254 whose MAC addresses are both 00:0c:29:6d:09:89.

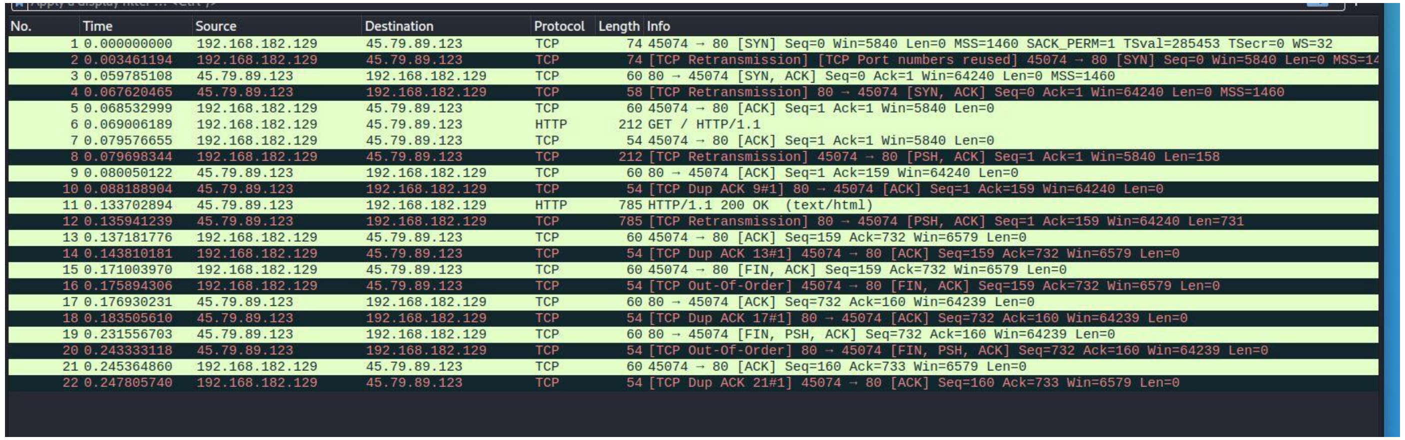


```
msfadmin@metasploitable:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.182.1            ether   00:0C:29:6D:09:89   C                     eth0
192.168.182.2            ether   00:0C:29:6D:09:89   C                     eth0
192.168.182.254          ether   00:0C:29:6D:09:89   C                     eth0
msfadmin@metasploitable:~$
```

m] I think Metasploitable will try to send the TCP SYN packet to 192.168.182.2 because I think this is the Gateway machine. Since there only needs to be one gateway machine per local network, it doesn't make sense that Metasploitable would reach out to another nongateway machine to connect to the remote network.

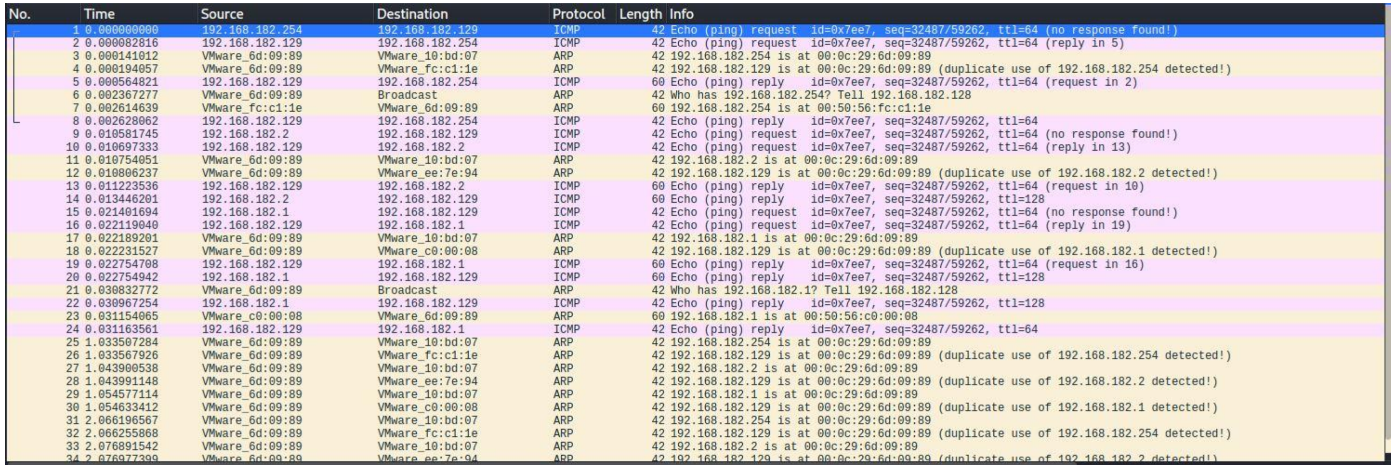
n] ...

o] Yes, there is an HTTP response on Metasploitable, the HTML is present in the terminal. There are a series of SYN, SYN/ACK, and many retransmissions.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.182.129	45.79.89.123	TCP	74	45074 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=285453 TSecr=0 WS=32
2	0.003461194	192.168.182.129	45.79.89.123	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 45074 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=14
3	0.059785108	45.79.89.123	192.168.182.129	TCP	60	80 → 45074 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
4	0.067620465	45.79.89.123	192.168.182.129	TCP	58	[TCP Retransmission] 80 → 45074 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
5	0.068532999	192.168.182.129	45.79.89.123	TCP	60	45074 → 80 [ACK] Seq=1 Ack=1 Win=5840 Len=0
6	0.069006189	192.168.182.129	45.79.89.123	HTTP	212	GET / HTTP/1.1
7	0.079576655	192.168.182.129	45.79.89.123	TCP	54	45074 → 80 [ACK] Seq=1 Ack=1 Win=5840 Len=0
8	0.079698344	192.168.182.129	45.79.89.123	TCP	212	[TCP Retransmission] 45074 → 80 [PSH, ACK] Seq=1 Ack=1 Win=5840 Len=158
9	0.080050122	45.79.89.123	192.168.182.129	TCP	60	80 → 45074 [ACK] Seq=1 Ack=159 Win=64240 Len=0
10	0.088188904	45.79.89.123	192.168.182.129	TCP	54	[TCP Dup ACK 9#1] 80 → 45074 [ACK] Seq=1 Ack=159 Win=64240 Len=0
11	0.133702894	45.79.89.123	192.168.182.129	HTTP	785	HTTP/1.1 200 OK (text/html)
12	0.135941239	45.79.89.123	192.168.182.129	TCP	785	[TCP Retransmission] 80 → 45074 [PSH, ACK] Seq=1 Ack=159 Win=64240 Len=731
13	0.137181776	192.168.182.129	45.79.89.123	TCP	60	45074 → 80 [ACK] Seq=159 Ack=732 Win=6579 Len=0
14	0.143810181	192.168.182.129	45.79.89.123	TCP	54	[TCP Dup ACK 13#1] 45074 → 80 [ACK] Seq=159 Ack=732 Win=6579 Len=0
15	0.171003970	192.168.182.129	45.79.89.123	TCP	60	45074 → 80 [FIN, ACK] Seq=159 Ack=732 Win=6579 Len=0
16	0.175894306	192.168.182.129	45.79.89.123	TCP	54	[TCP Out-Of-Order] 45074 → 80 [FIN, ACK] Seq=159 Ack=732 Win=6579 Len=0
17	0.176930231	45.79.89.123	192.168.182.129	TCP	60	80 → 45074 [ACK] Seq=732 Ack=160 Win=64239 Len=0
18	0.183505610	45.79.89.123	192.168.182.129	TCP	54	[TCP Dup ACK 17#1] 80 → 45074 [ACK] Seq=732 Ack=160 Win=64239 Len=0
19	0.231556703	45.79.89.123	192.168.182.129	TCP	60	80 → 45074 [FIN, PSH, ACK] Seq=732 Ack=160 Win=64239 Len=0
20	0.243333118	45.79.89.123	192.168.182.129	TCP	54	[TCP Out-Of-Order] 80 → 45074 [FIN, PSH, ACK] Seq=732 Ack=160 Win=64239 Len=0
21	0.245364860	192.168.182.129	45.79.89.123	TCP	60	45074 → 80 [ACK] Seq=160 Ack=733 Win=6579 Len=0
22	0.247805740	192.168.182.129	45.79.89.123	TCP	54	[TCP Dup ACK 21#1] 45074 → 80 [ACK] Seq=160 Ack=733 Win=6579 Len=0

p] When Kali did the ARP broadcast, it added two address to the cache. Kali changed Metasploitable's ARP cache by changing the MAC addresses of all the machines to be the same as Kali's MAC address, 00:0c:29:6d:09:89.
In Wireshark, we see that nearly every packet sent between Metasploitable and jeffondich.com is retransmitted. This is because the PITM, Kali, is picking up each of these packets. After Kali receives the packets, because everything is being routed through 00:0c:29:6d:09:89, Kali must send them on again.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.182.254	192.168.182.129	ICMP	42	Echo (ping) request id=0x7ee7, seq=32487/59262, ttl=64 (no response found!)
2	0.000082816	192.168.182.129	192.168.182.254	ICMP	42	Echo (ping) request id=0x7ee7, seq=32487/59262, ttl=64 (reply in 5)
3	0.000141012	VMware_6d:09:89	VMware_10:bd:07	ARP	42	192.168.182.254 is at 00:0c:29:6d:09:89
4	0.000194057	VMware_6d:09:89	VMware_fc:c1:1e	ARP	42	192.168.182.129 is at 00:0c:29:6d:09:89 (duplicate use of 192.168.182.254 detected!)
5	0.000564821	192.168.182.129	192.168.182.254	ICMP	60	Echo (ping) reply id=0x7ee7, seq=32487/59262, ttl=64 (request in 2)
6	0.002367277	VMware_6d:09:89	Broadcast	ARP	42	Who has 192.168.182.254? Tell 192.168.182.128
7	0.002614639	VMware_fc:c1:1e	VMware_6d:09:89	ARP	60	192.168.182.254 is at 00:50:56:fc:c1:1e
8	0.002628062	192.168.182.129	192.168.182.254	ICMP	42	Echo (ping) reply id=0x7ee7, seq=32487/59262, ttl=64
9	0.010581745	192.168.182.2	192.168.182.129	ICMP	42	Echo (ping) request id=0x7ee7, seq=32487/59262, ttl=64 (no response found!)
10	0.010697333	192.168.182.129	192.168.182.2	ICMP	42	Echo (ping) request id=0x7ee7, seq=32487/59262, ttl=64 (reply in 13)
11	0.010754051	VMware_6d:09:89	VMware_10:bd:07	ARP	42	192.168.182.2 is at 00:0c:29:6d:09:89
12	0.010806237	VMware_6d:09:89	VMware_ee:7e:94	ARP	42	192.168.182.129 is at 00:0c:29:6d:09:89 (duplicate use of 192.168.182.2 detected!)
13	0.011223536	192.168.182.129	192.168.182.2	ICMP	60	Echo (ping) reply id=0x7ee7, seq=32487/59262, ttl=64 (request in 10)
14	0.013446201	192.168.182.2	192.168.182.129	ICMP	60	Echo (ping) reply id=0x7ee7, seq=32487/59262, ttl=128
15	0.021401694	192.168.182.1	192.168.182.129	ICMP	42	Echo (ping) request id=0x7ee7, seq=32487/59262, ttl=64 (no response found!)
16	0.022119040	192.168.182.129	192.168.182.1	ICMP	42	Echo (ping) request id=0x7ee7, seq=32487/59262, ttl=64 (reply in 19)
17	0.022189201	VMware_6d:09:89	VMware_10:bd:07	ARP	42	192.168.182.1 is at 00:0c:29:6d:09:89
18	0.022231527	VMware_6d:09:89	VMware_c0:00:08	ARP	42	192.168.182.129 is at 00:0c:29:6d:09:89 (duplicate use of 192.168.182.1 detected!)
19	0.022754708	192.168.182.129	192.168.182.1	ICMP	60	Echo (ping) reply id=0x7ee7, seq=32487/59262, ttl=64 (request in 16)
20	0.022754942	192.168.182.1	192.168.182.129	ICMP	60	Echo (ping) reply id=0x7ee7, seq=32487/59262, ttl=128
21	0.030832772	VMware_6d:09:89	Broadcast	ARP	42	Who has 192.168.182.1? Tell 192.168.182.128
22	0.030967254	192.168.182.1	192.168.182.129	ICMP	42	Echo (ping) reply id=0x7ee7, seq=32487/59262, ttl=128
23	0.031154065	VMware_c0:00:08	VMware_6d:09:89	ARP	60	192.168.182.1 is at 00:50:56:c0:00:08
24	0.031163561	192.168.182.129	192.168.182.1	ICMP	42	Echo (ping) reply id=0x7ee7, seq=32487/59262, ttl=64
25	1.033507284	VMware_6d:09:89	VMware_10:bd:07	ARP	42	192.168.182.254 is at 00:0c:29:6d:09:89
26	1.033567926	VMware_6d:09:89	VMware_fc:c1:1e	ARP	42	192.168.182.129 is at 00:0c:29:6d:09:89 (duplicate use of 192.168.182.254 detected!)
27	1.043900538	VMware_6d:09:89	VMware_10:bd:07	ARP	42	192.168.182.2 is at 00:0c:29:6d:09:89
28	1.043991148	VMware_6d:09:89	VMware_ee:7e:94	ARP	42	192.168.182.129 is at 00:0c:29:6d:09:89 (duplicate use of 192.168.182.2 detected!)
29	1.054577114	VMware_6d:09:89	VMware_10:bd:07	ARP	42	192.168.182.1 is at 00:0c:29:6d:09:89
30	1.054633412	VMware_6d:09:89	VMware_c0:00:08	ARP	42	192.168.182.129 is at 00:0c:29:6d:09:89 (duplicate use of 192.168.182.1 detected!)
31	2.066196567	VMware_6d:09:89	VMware_10:bd:07	ARP	42	192.168.182.254 is at 00:0c:29:6d:09:89
32	2.066255868	VMware_6d:09:89	VMware_fc:c1:1e	ARP	42	192.168.182.129 is at 00:0c:29:6d:09:89 (duplicate use of 192.168.182.254 detected!)
33	2.076891542	VMware_6d:09:89	VMware_10:bd:07	ARP	42	192.168.182.2 is at 00:0c:29:6d:09:89
34	2.076977399	VMware_6d:09:89	VMware_ee:7e:94	ARP	42	192.168.182.129 is at 00:0c:29:6d:09:89 (duplicate use of 192.168.182.2 detected!)

q] The detector could note how many times a retransmission timeout (RTO) occurs. Once it reaches past a certain threshold, the detector should assume there is a PITM and cut the connection. This would cause an issue if there was no PITM and the client/server were just having a tough time sending/receiving packets, like if there was a problem with the network (i.e., a busy network).

helpful websites:
https://wiki.amahi.org/index.php/Find_Your_Gateway_IP
https://ieeexplore.ieee.org/document/8515845