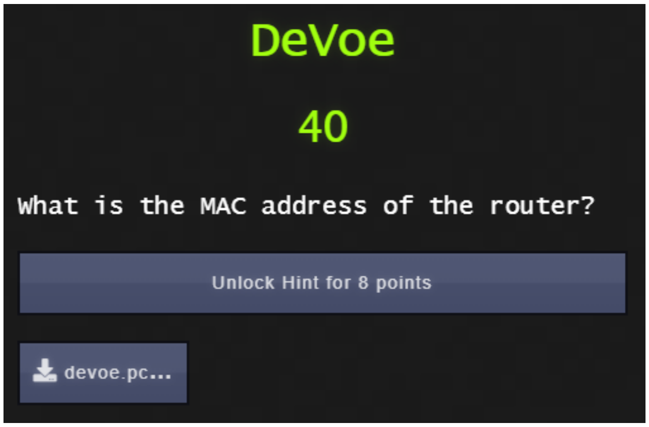
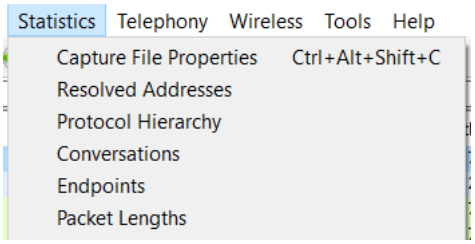


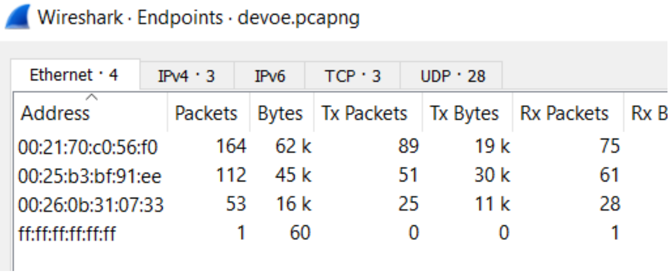
DeVoe

40

What is the MAC address of the router?

Start off with looking at the end points statistics.

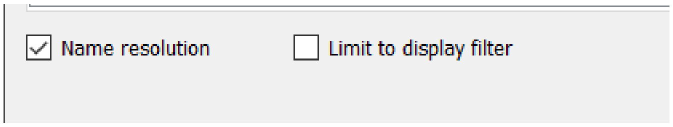




Wireshark · Endpoints · devoe.pcapng

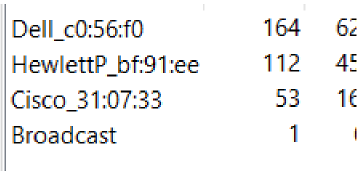
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx B
00:21:70:c0:56:f0	164	62 k	89	19 k	75	
00:25:b3:bf:91:ee	112	45 k	51	30 k	61	
00:26:0b:31:07:33	53	16 k	25	11 k	28	
ff:ff:ff:ff:ff:ff	1	60	0	0	1	

Click on Name Resolution check box at the bottom.



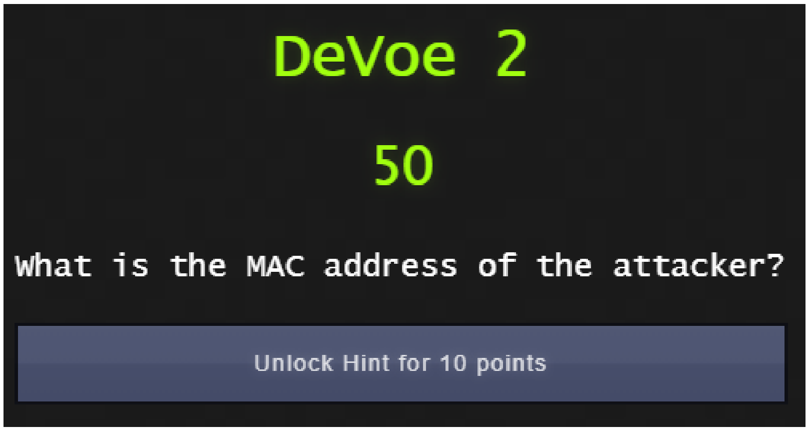
☑ Name resolution ☐ Limit to display filter

We see a popular router device manufacturer



Dell_c0:56:f0	164	62
HewlettP_bf:91:ee	112	45
Cisco_31:07:33	53	16
Broadcast	1	

Flag: 00:26:0b:31:07:33



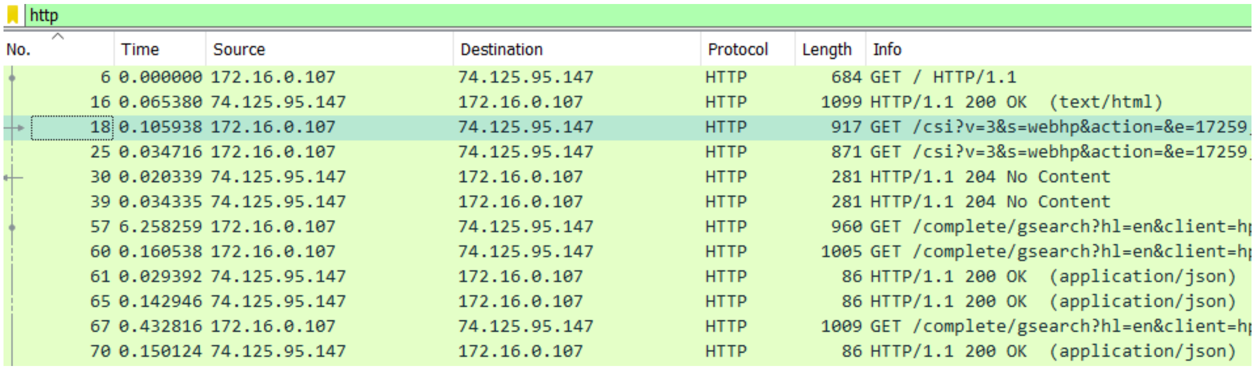
DeVoe 2

50

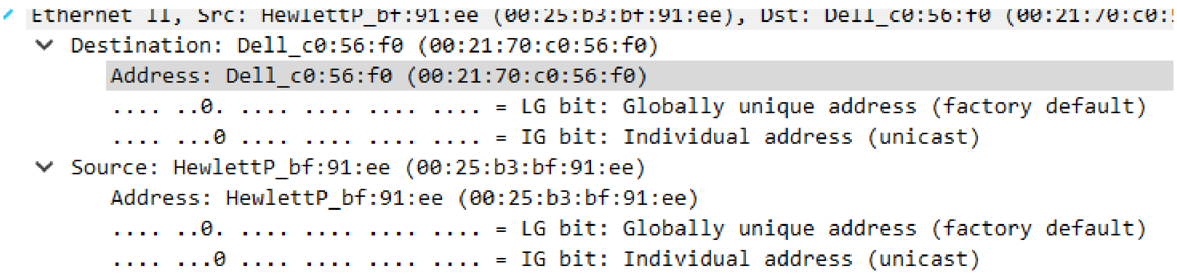
What is the MAC address of the attacker?

Filter: http

We see one device requesting a bunch of GET requests and the Attacker pc answering them with a bunch of JSON files.

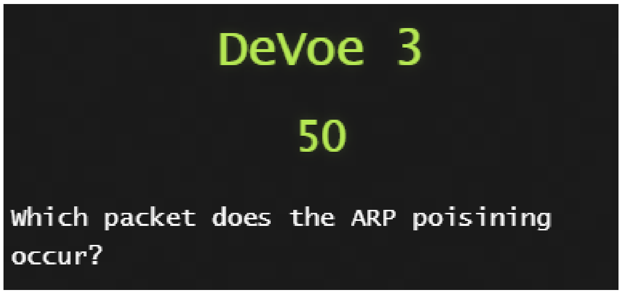


```
http
No.      Time     Source          Destination     Protocol  Length Info
      6 0.000000 172.16.0.107    74.125.95.147   HTTP       684 GET / HTTP/1.1
     16 0.065380 74.125.95.147   172.16.0.107    HTTP      1099 HTTP/1.1 200 OK  (text/html)
     18 0.105938 172.16.0.107    74.125.95.147   HTTP       917 GET /csi?v=3&s=webhp&action=&e=17259
     25 0.034716 172.16.0.107    74.125.95.147   HTTP       871 GET /csi?v=3&s=webhp&action=&e=17259
     30 0.020339 74.125.95.147   172.16.0.107    HTTP       281 HTTP/1.1 204 No Content
     39 0.034335 74.125.95.147   172.16.0.107    HTTP       281 HTTP/1.1 204 No Content
     57 6.258259 172.16.0.107    74.125.95.147   HTTP       960 GET /complete/gsearch?hl=en&client=h
     60 0.160538 172.16.0.107    74.125.95.147   HTTP      1005 GET /complete/gsearch?hl=en&client=h
     61 0.029392 74.125.95.147   172.16.0.107    HTTP        86 HTTP/1.1 200 OK  (application/json)
     65 0.142946 74.125.95.147   172.16.0.107    HTTP        86 HTTP/1.1 200 OK  (application/json)
     67 0.432816 172.16.0.107    74.125.95.147   HTTP      1009 GET /complete/gsearch?hl=en&client=h
     70 0.150124 74.125.95.147   172.16.0.107    HTTP        86 HTTP/1.1 200 OK  (application/json)
```



```
Ethernet II, Src: HewlettP_bf:91:ee (00:25:b3:bf:91:ee), Dst: Dell_c0:56:f0 (00:21:70:c0:
  Destination: Dell_c0:56:f0 (00:21:70:c0:56:f0)
      Address: Dell_c0:56:f0 (00:21:70:c0:56:f0)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: HewlettP_bf:91:ee (00:25:b3:bf:91:ee)
      Address: HewlettP_bf:91:ee (00:25:b3:bf:91:ee)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
```

Flag: 00:25:b3:bf:91:ee

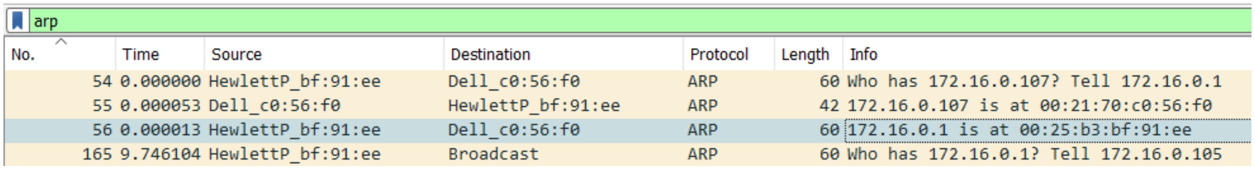


DeVoe 3

50

which packet does the ARP poisining occur?

Filter: arp



arp

No.	Time	Source	Destination	Protocol	Length	Info
54	0.000000	HewlettP_bf:91:ee	Dell_c0:56:f0	ARP	60	Who has 172.16.0.107? Tell 172.16.0.1
55	0.000053	Dell_c0:56:f0	HewlettP_bf:91:ee	ARP	42	172.16.0.107 is at 00:21:70:c0:56:f0
56	0.000013	HewlettP_bf:91:ee	Dell_c0:56:f0	ARP	60	172.16.0.1 is at 00:25:b3:bf:91:ee
165	9.746104	HewlettP_bf:91:ee	Broadcast	ARP	60	Who has 172.16.0.1? Tell 172.16.0.105

In the shot above we see out attacker MAC address answering a request from the HP box.

Flag: 56