THM_Wireshark 101 [Task 7 ARP]

I learned about Ipcodes, how to find the MAC address of a sent packet, how to find reply packets, and to find an ipaddress from a given MAC address

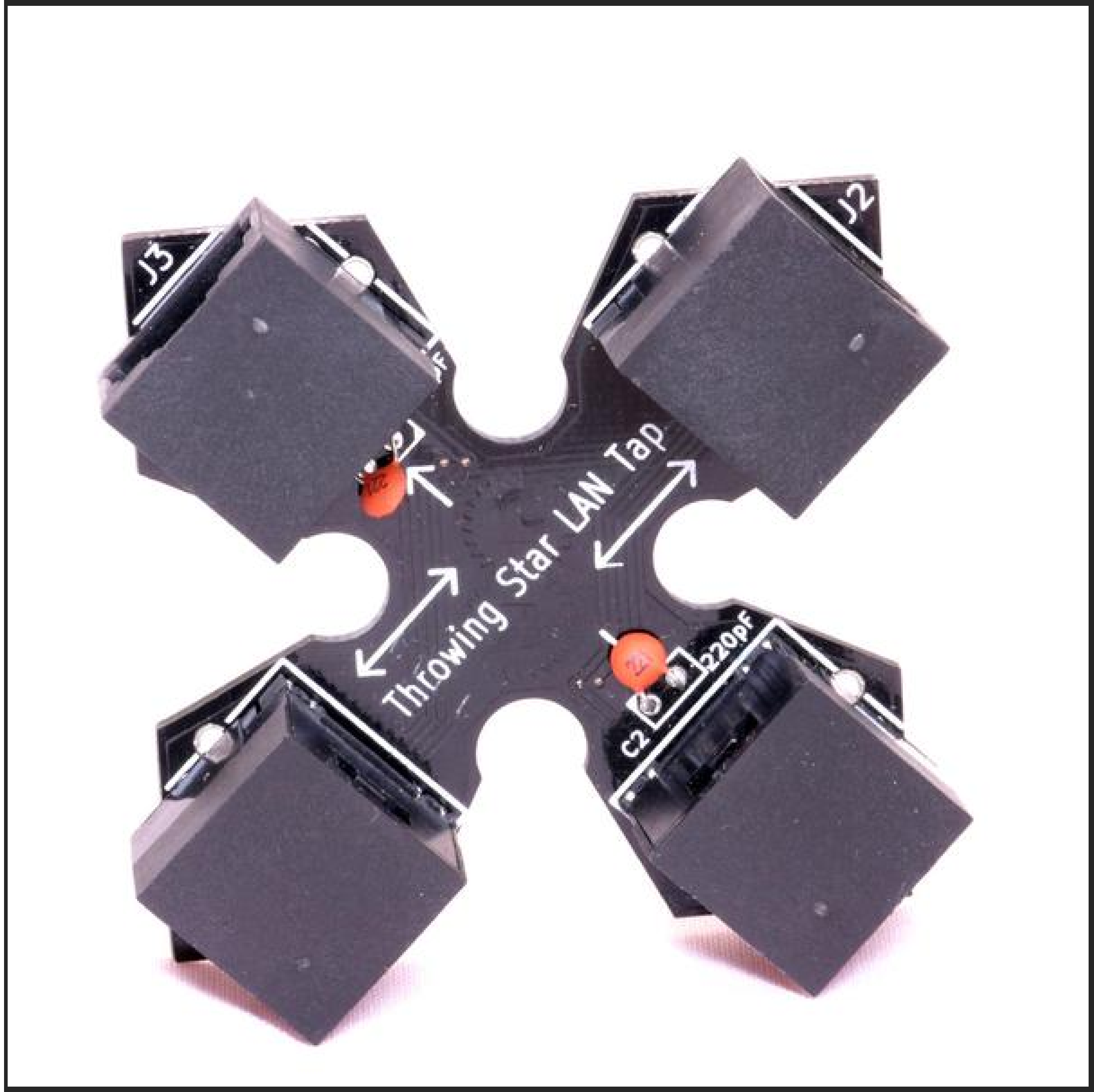
https://tryhackme.com/room/wireshark

Network Taps

Network taps are a physical implant in which you physically tap between a cable, these techniques are commonly used by Threat Hunting/DFIR teams and red teams in an engagement to sniff and capture packets.

There are two primary means of tapping a wire. The first is by using hardware to tap the wire and intercept the traffic as it comes across, an example of this would be a vampire tap as pictured below.

Another option for planting a network tap would be an inline network tap, which you would plant between or 'inline' two network devices. The tap will replicate packets as they pass the tap. An example of this tap would be the very common Throwing Star LAN Tap



MAC Floods

MAC Floods are a tactic commonly used by red teams as a way of actively sniffing packets. MAC Flooding is intended to stress the switch and fill the CAM table. Once the CAM table is filled the switch will no longer accept new MAC addresses and so in order to keep the network alive, the switch will send out packets to all ports of the switch.

Note: This technique should be used with extreme caution and with explicit prior consent.

ARP Poisoning

ARP Poisoning is another technique used by red teams to actively sniff packets. By ARP Poisoning you can redirect the traffic from the host(s) to the machine you're monitoring from. This technique will not stress network equipment like MAC Flooding however should still be used with caution and only if other techniques like network taps are unavailable.

Combining these methods with your previous knowledge of capturing traffic from the previous task will allow you to proactively monitor and collect live packet captures from scratch.

Wireshark only has a few that you will need to be familiar with:

- and - operator: and / &&
- or - operator: or / ||I learned about Ipcodes, how to find the MAC address of a sent packet, how to find reply packets, and to find an ipaddress from a given MAC address
- equals - operator: eq / ==
- not equal - operator: ne / !=
- greater than - operator: gt / >
- less than - operator: lt / <

https://www.wireshark.org/docs/wsug_html_chunked/ChWorkBuildDisplayFilterSection.html

https://wiki.wireshark.org/DisplayFilters

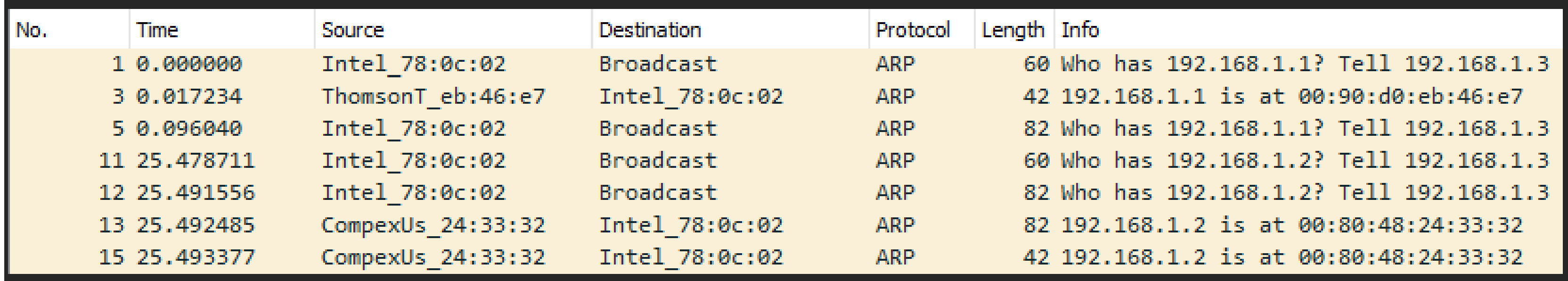
TASK 7 [ARP Traffic]y

nb6-startup.pcap 87 kB

ARP or Address Resolution Protocol is a Layer 2 protocol that is used to connect IP Addresses with MAC Addresses. They will contain REQUEST messages and RESPONSE messages. To identify packets the message header will contain one of two operation codes:

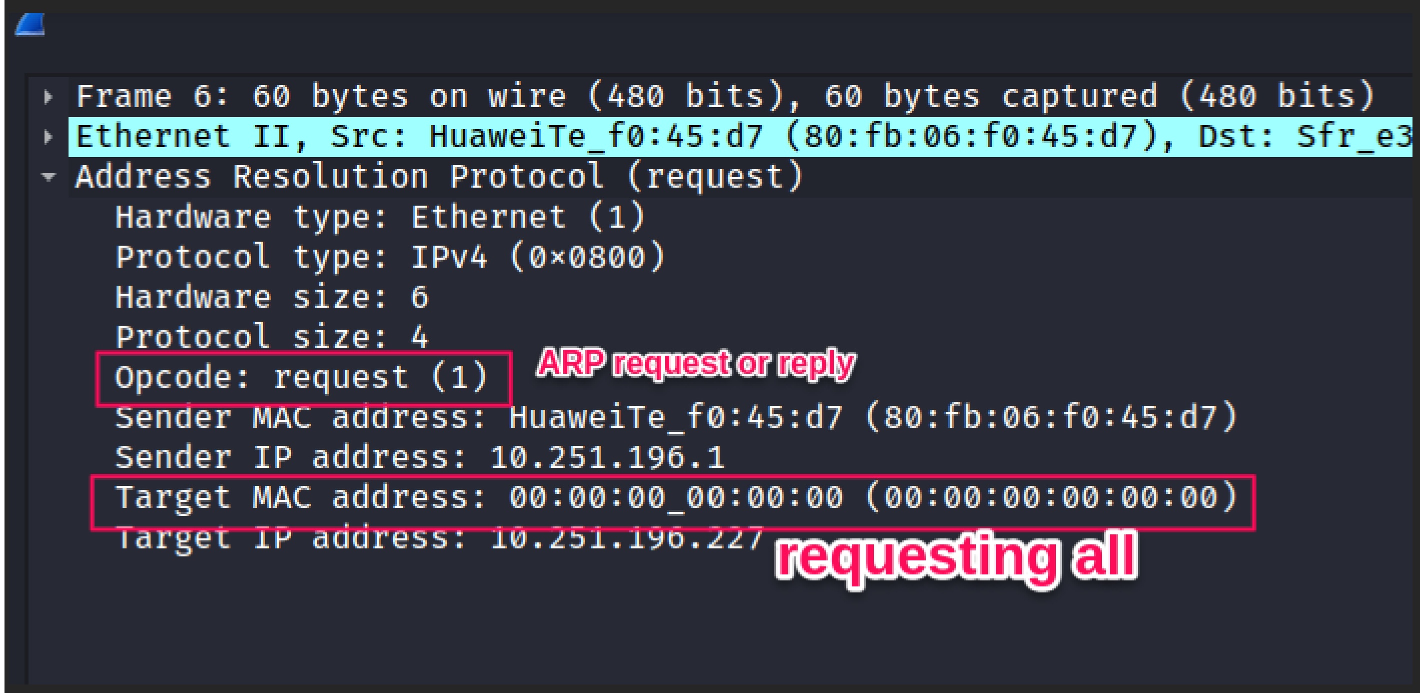
- Request (1)
- Reply (2)

Below you can see a packet capture of multiple ARP requests and replies.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Intel_78:0c:02	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.3
3	0.017234	ThomsonT_eb:46:e7	Intel_78:0c:02	ARP	42	192.168.1.1 is at 00:90:d0:eb:46:e7
5	0.096040	Intel_78:0c:02	Broadcast	ARP	82	Who has 192.168.1.1? Tell 192.168.1.3
11	25.478711	Intel_78:0c:02	Broadcast	ARP	60	Who has 192.168.1.2? Tell 192.168.1.3
12	25.491556	Intel_78:0c:02	Broadcast	ARP	82	Who has 192.168.1.2? Tell 192.168.1.3
13	25.492485	CompexUs_24:33:32	Intel_78:0c:02	ARP	82	192.168.1.2 is at 00:80:48:24:33:32
15	25.493377	CompexUs_24:33:32	Intel_78:0c:02	ARP	42	192.168.1.2 is at 00:80:48:24:33:32

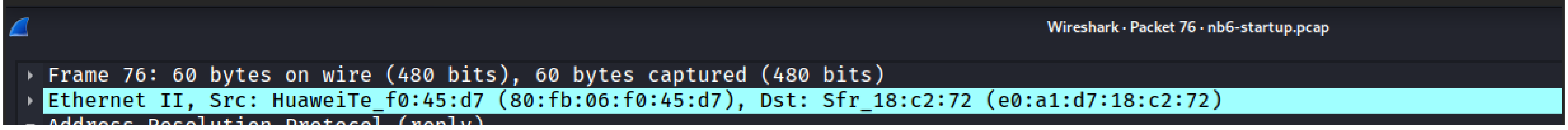
It is useful to note that most devices will identify themselves or Wireshark will identify it such as Intel_78, an example of suspicious traffic would be many requests from an unrecognized source. You need to enable a setting within Wireshark however to resolve physical addresses. **To enable this feature, navigate to View > Name Resolution > Ensure that Resolve Physical Addresses is checked.**



```
▸ Frame 6: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
▸ Ethernet II, Src: HuaweiTe_f0:45:d7 (80:fb:06:f0:45:d7), Dst: Sfr_e3
▾ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: HuaweiTe_f0:45:d7 (80:fb:06:f0:45:d7)
    Sender IP address: 10.251.196.1
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 10.251.196.227
```

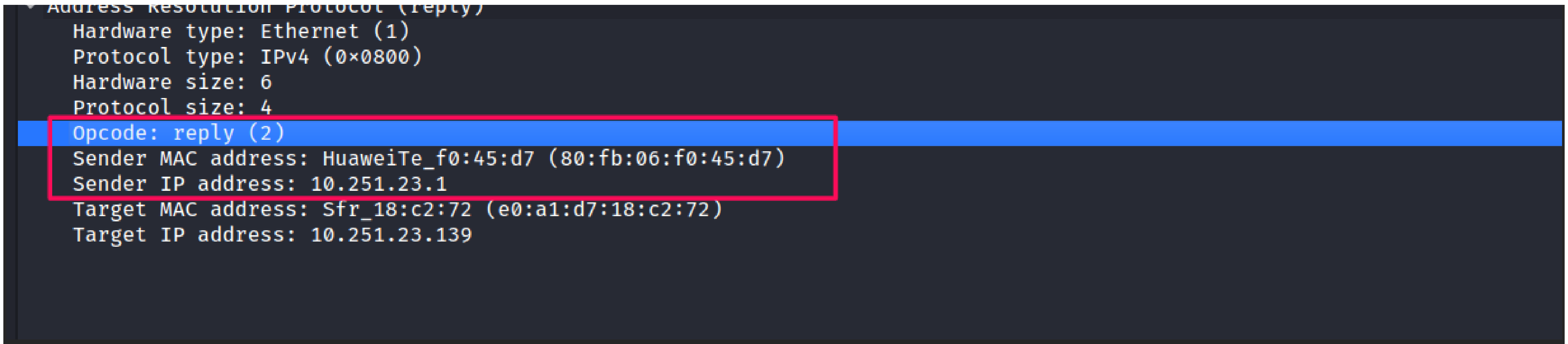
ARP request or reply

requesting all



Wireshark · Packet 76 · nb6-startup.pcap

```
▸ Frame 76: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
▸ Ethernet II, Src: HuaweiTe_f0:45:d7 (80:fb:06:f0:45:d7), Dst: Sfr_18:c2:72 (e0:a1:d7:18:c2:72)
  Address Resolution Protocol (reply)
```



```
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: HuaweiTe_f0:45:d7 (80:fb:06:f0:45:d7)
    Sender IP address: 10.251.23.1
    Target MAC address: Sfr_18:c2:72 (e0:a1:d7:18:c2:72)
    Target IP address: 10.251.23.139
```

Answer the questions below

What is the Opcode for Packet 6?

request (1)

What is the source MACAddress of Packet 19?

80:fb:06:f0:45:d7

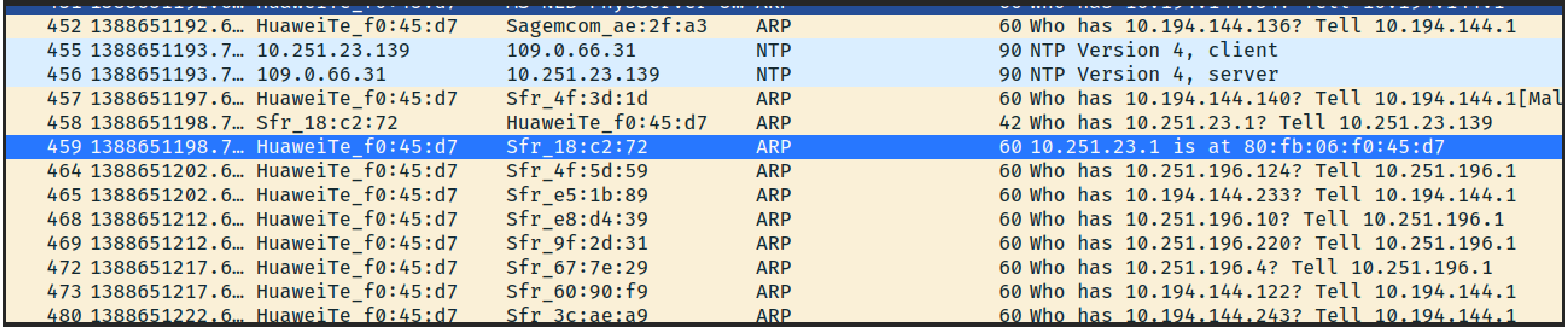
What 4 packets are Reply packets?

76,400,459,520

What IP Address is at 80:fb:06:f0:45:d7?

Using this filter

eth.addr == 80:fb:06:f0:45:d7



```
452 1388651192.6… HuaweiTe_f0:45:d7   Sagemcom_ae:2f:a3   ARP   60 Who has 10.194.144.136? Tell 10.194.144.1
455 1388651193.7… 10.251.23.139       109.0.66.31         NTP   90 NTP Version 4, client
456 1388651193.7… 109.0.66.31         10.251.23.139       NTP   90 NTP Version 4, server
457 1388651197.6… HuaweiTe_f0:45:d7   Sfr_4f:3d:1d        ARP   60 Who has 10.194.144.140? Tell 10.194.144.1[Mal
458 1388651198.7… Sfr_18:c2:72        HuaweiTe_f0:45:d7   ARP   42 Who has 10.251.23.1? Tell 10.251.23.139
459 1388651198.7… HuaweiTe_f0:45:d7   Sfr_18:c2:72        ARP   60 10.251.23.1 is at 80:fb:06:f0:45:d7
464 1388651202.6… HuaweiTe_f0:45:d7   Sfr_4f:5d:59        ARP   60 Who has 10.251.196.124? Tell 10.251.196.1
465 1388651202.6… HuaweiTe_f0:45:d7   Sfr_e5:1b:89        ARP   60 Who has 10.194.144.233? Tell 10.194.144.1
468 1388651212.6… HuaweiTe_f0:45:d7   Sfr_e8:d4:39        ARP   60 Who has 10.251.196.10? Tell 10.251.196.1
469 1388651212.6… HuaweiTe_f0:45:d7   Sfr_9f:2d:31        ARP   60 Who has 10.251.196.220? Tell 10.251.196.1
472 1388651217.6… HuaweiTe_f0:45:d7   Sfr_67:7e:29        ARP   60 Who has 10.251.196.4? Tell 10.251.196.1
473 1388651217.6… HuaweiTe_f0:45:d7   Sfr_60:90:f9        ARP   60 Who has 10.194.144.122? Tell 10.194.144.1
480 1388651222.6… HuaweiTe_f0:45:d7   Sfr_3c:ae:a9        ARP   60 Who has 10.194.144.243? Tell 10.194.144.1
```

10.251.23.1