Atividade sobre Ethernet e ARP

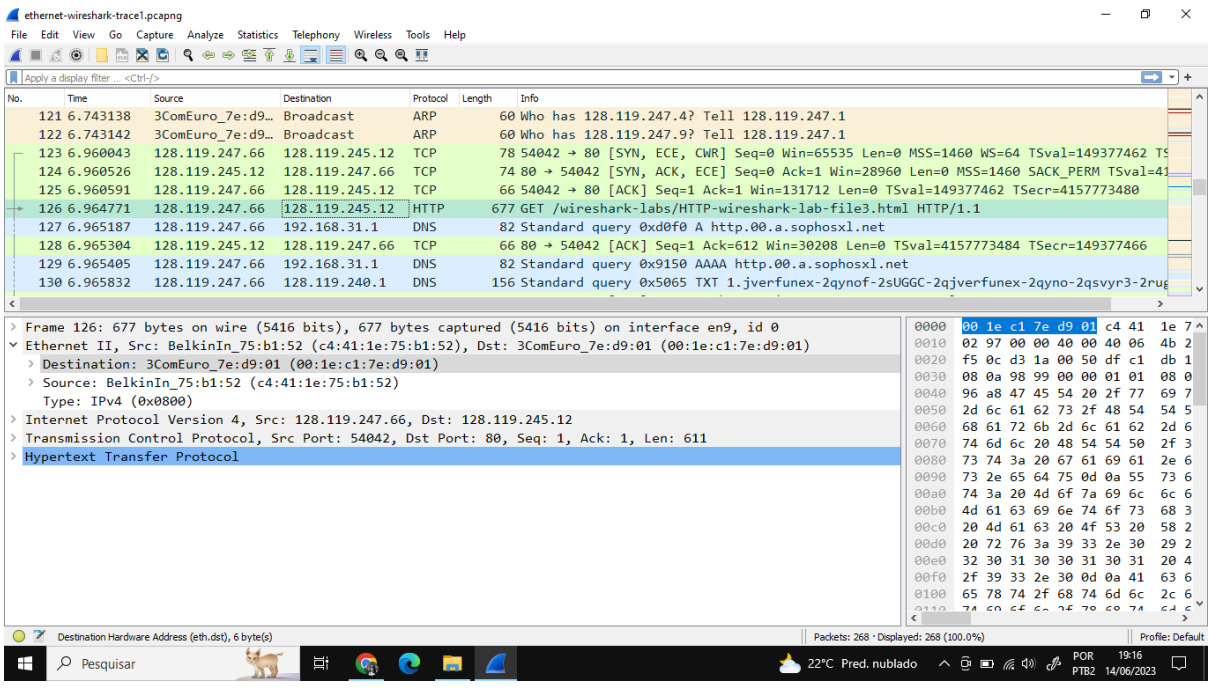
Redes de Computadores

Sabrina Araújo Cardoso - 118210114

Wireshark Lab: Ethernet and ARP

A atividade foi feita utilizando o pacote capturado pelo autor.

- **Questão 1:** Qual é o endereço Ethernet de 48 bits do seu computador?



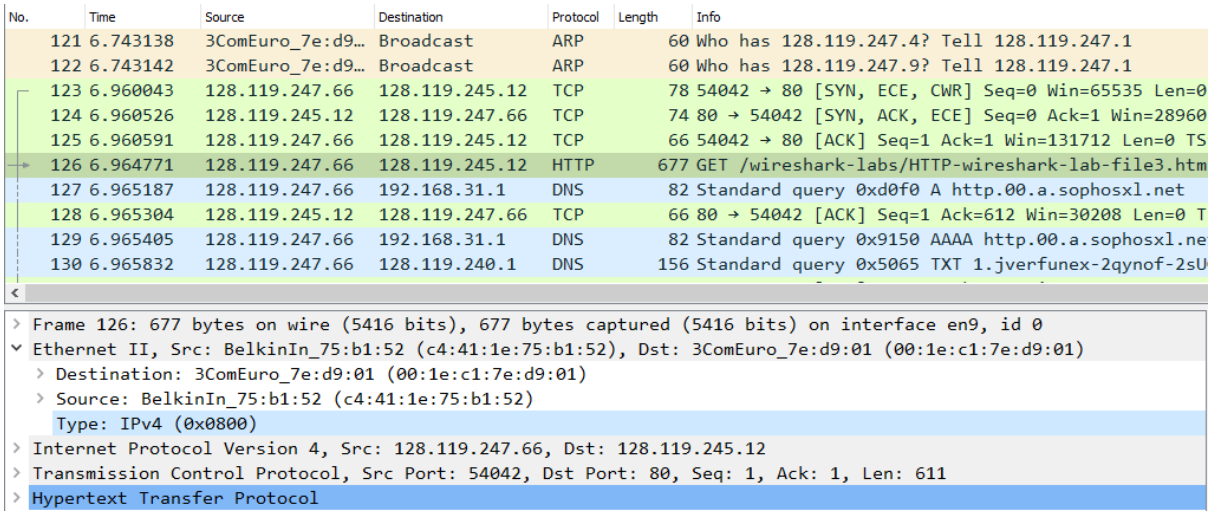
> Destination: **00:1e:c1:7e:d9:01**

- **Questão 2:** Qual é o endereço de destino de 48 bits no quadro Ethernet? Esse é o endereço Ethernet de gaia.cs.umass.edu? (Dica: a resposta é não). Que dispositivo possui este como seu endereço Ethernet?

> **O endereço de destino c4:41:1e:75:b1:52 não é o endereço Ethernet de gaia.cs.umass.edu. É o endereço do roteador**

> **que é o link usado para sair da sub-rede.**

- **Questão 3:** Qual é o valor hexadecimal para o campo de dois bytes do tipo de quadro no quadro Ethernet que transporta a solicitação HTTP GET? A qual protocolo de camada superior isso corresponde?

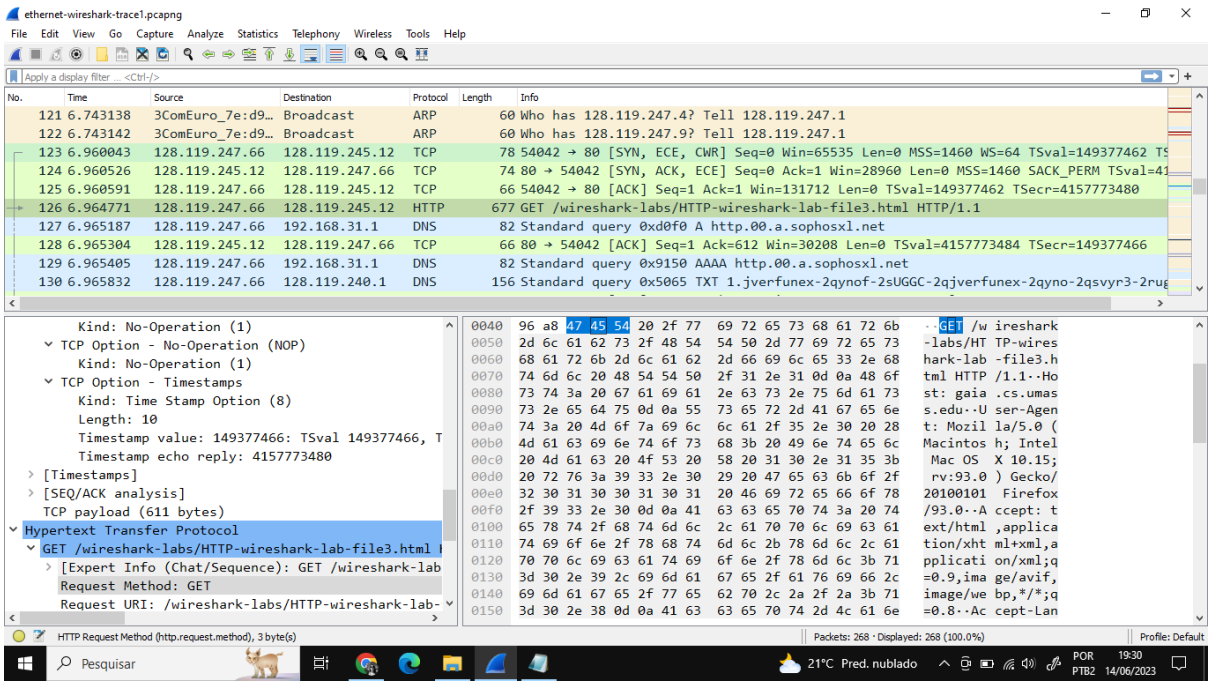


No.	Time	Source	Destination	Protocol	Length	Info
121	6.743138	3ComEuro_7e:d9…	Broadcast	ARP	60	Who has 128.119.247.4? Tell 128.119.247.1
122	6.743142	3ComEuro_7e:d9…	Broadcast	ARP	60	Who has 128.119.247.9? Tell 128.119.247.1
123	6.960043	128.119.247.66	128.119.245.12	TCP	78	54042 → 80 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0
124	6.960526	128.119.245.12	128.119.247.66	TCP	74	80 → 54042 [SYN, ACK, ECE] Seq=0 Ack=1 Win=28960
125	6.960591	128.119.247.66	128.119.245.12	TCP	66	54042 → 80 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TS
126	6.964771	128.119.247.66	128.119.245.12	HTTP	677	GET /wireshark-labs/HTTP-wireshark-lab-file3.htm
127	6.965187	128.119.247.66	192.168.31.1	DNS	82	Standard query 0xd0f0 A http.00.a.sophosxl.net
128	6.965304	128.119.245.12	128.119.247.66	TCP	66	80 → 54042 [ACK] Seq=1 Ack=612 Win=30208 Len=0 T
129	6.965405	128.119.247.66	192.168.31.1	DNS	82	Standard query 0x9150 AAAA http.00.a.sophosxl.ne
130	6.965832	128.119.247.66	128.119.240.1	DNS	156	Standard query 0x5065 TXT 1.jverfunex-2qynof-2sU

```
> Frame 126: 677 bytes on wire (5416 bits), 677 bytes captured (5416 bits) on interface en9, id 0
v Ethernet II, Src: BelkinIn_75:b1:52 (c4:41:1e:75:b1:52), Dst: 3ComEuro_7e:d9:01 (00:1e:c1:7e:d9:01)
  > Destination: 3ComEuro_7e:d9:01 (00:1e:c1:7e:d9:01)
  > Source: BelkinIn_75:b1:52 (c4:41:1e:75:b1:52)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 128.119.247.66, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 54042, Dst Port: 80, Seq: 1, Ack: 1, Len: 611
> Hypertext Transfer Protocol
```

> Value: **0x0800**
> Typo: **Ipv4**
>
> **Isso corresponde ao protocolo IP (o campo do tipo de quadro indica que a camada acima do IP - a camada para a qual o payload deste quadro Ethernet será passado - é o IP).**

Questão 4: Quantos bytes a partir do início do quadro Ethernet a letra "G" em "GET" aparece? Não inclua nenhum bit de preâmbulo em sua contagem, ou seja, assuma que o quadro Ethernet começa com o endereço de destino do quadro Ethernet.



> **A letra "G" em ASCII aparece 52 bytes a partir do início do quadro Ethernet. Existem 14 bytes no quadro Ethernet e em seguida, 20 bytes de cabeçalho IP, seguidos por 20 bytes de cabeçalho TCP antes que os dados HTTP sejam encontrados.**

- **Questão 5:** Qual é o valor do endereço de origem Ethernet? Este é o endereço do seu computador ou do gaia.cs.umass.edu (Dica: a resposta é não). Que dispositivo possui este endereço Ethernet?

> **O endereço de destino c4:41:1e:75:b1:52 não é o endereço Ethernet de gaia.cs.umass.edu. É o endereço do roteador que é o link usado para sair da sub-rede.**

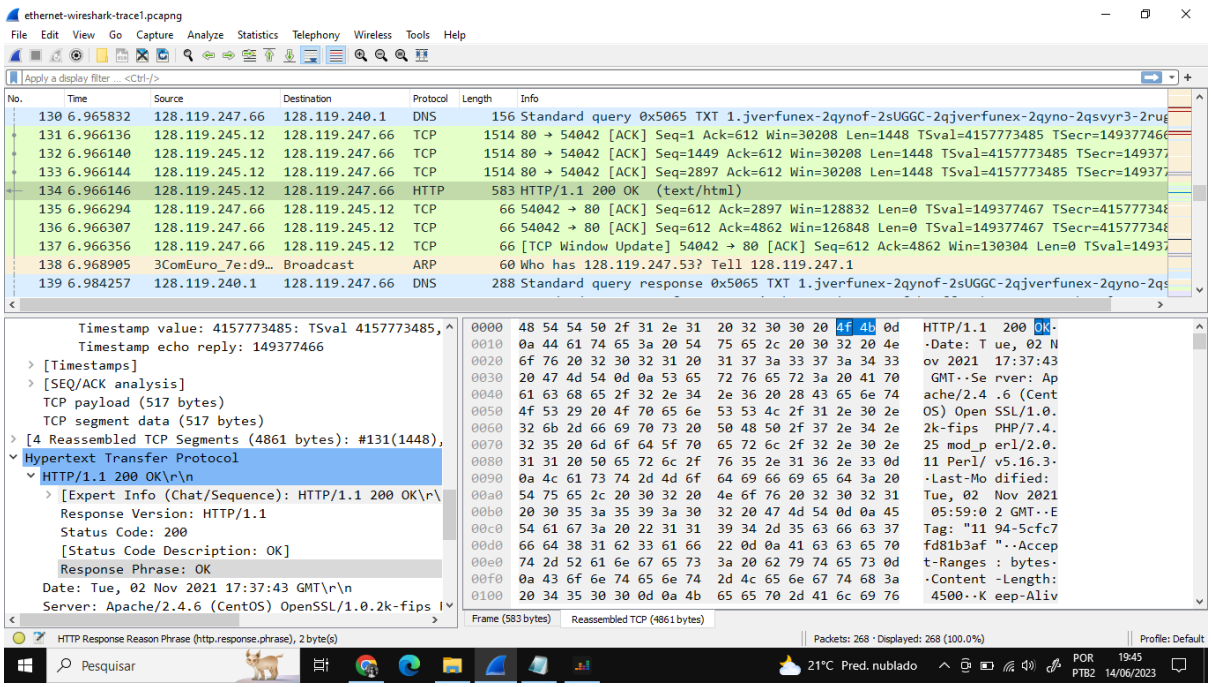
- **Questão 6:** Qual é o endereço de destino no quadro Ethernet? Este é o endereço Ethernet do seu computador?

> Destination: **00:1e:c1:7e:d9:01.**
> **É o endereço do meu computador**

- **Questão 7:** Forneça o valor hexadecimal para o campo de dois bytes do tipo de quadro. A que protocolo de camada superior isso corresponde?

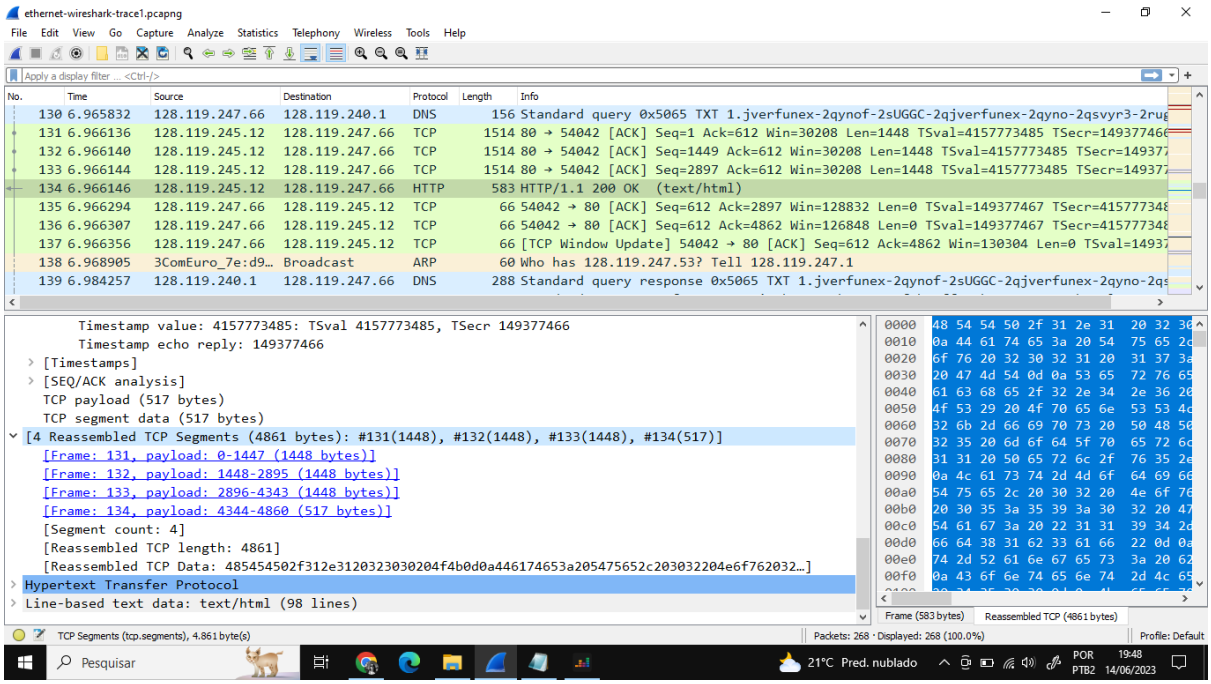
> **O valor hexadecimal para o campo "Frame type" é 0x0800. Esse valor corresponde ao protocolo IP.**

- **Questão 8:** Quantos bytes a partir do início do quadro Ethernet o caractere "O" em "OK" (ou seja, o código de resposta HTTP) aparece no quadro Ethernet? Não conte quaisquer bits de preâmbulo em sua contagem, ou seja, assuma que o quadro Ethernet começa com o endereço de destino do quadro Ethernet.



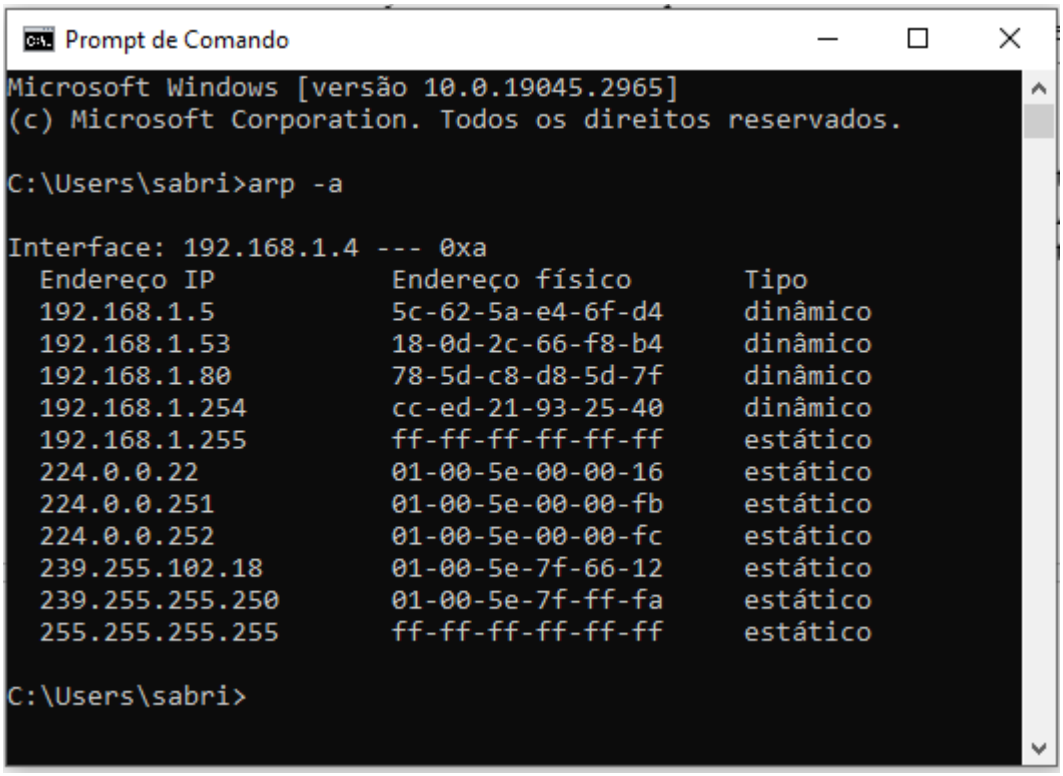
> **O caractere ASCII "O" aparece 52 bytes a partir do início do quadro Ethernet. Novamente, há 14 bytes de quadro Ethernet, seguidos por 20 bytes de cabeçalho IP e mais 20 bytes de cabeçalho TCP antes dos dados HTTP serem encontrados.**

- **Questão 9:** 1. Quantos quadros Ethernet (cada um contendo um datagrama IP, cada um contendo um segmento TCP) transportam dados que fazem parte da mensagem completa de resposta HTTP "OK 200 ..."?



4 quadros

- **Questão 10:** Quantas entradas estão armazenadas em seu cache ARP?

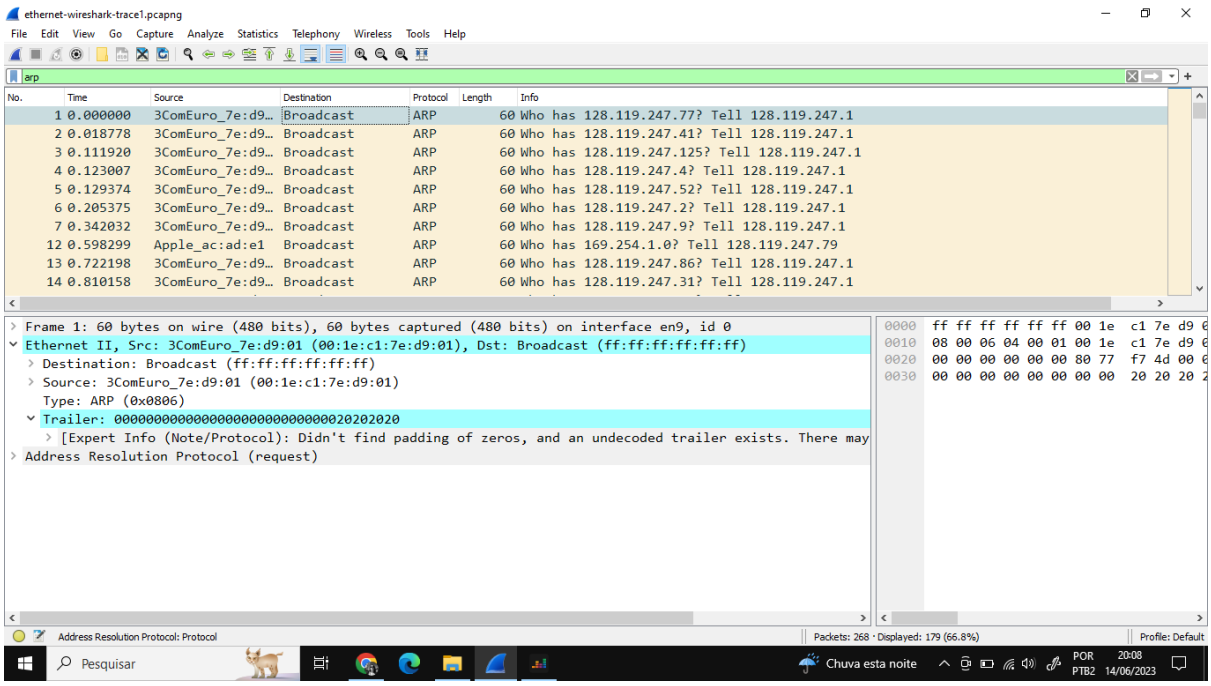


11 Entradas

- **Questão 11:** O que cada entrada exibida no cache ARP contém?

O endereço IP, o Endereço Físico e o Tipo

- **Questão 12:** Qual é o valor hexadecimal do endereço de origem no quadro Ethernet contendo a mensagem de solicitação ARP enviada pelo seu computador?



> **O valor hexadecimal do endereço de origem é 00:1e:c1:7e:d9:01. O valor hexadecimal do endereço de destino é ff:ff:ff:ff:ff:ff, o endereço de broadcast.**

- **Questão 13:** Qual é o valor hexadecimal dos endereços de destino no quadro Ethernet contendo a mensagem de solicitação ARP enviada pelo seu computador? E qual dispositivo (se houver) corresponde a esse endereço (por exemplo, cliente, servidor, roteador, switch ou outro...)?

> **O valor hexadecimal do endereço de destino é ff:ff:ff:ff:ff:ff. Não há dispositivo, este endereço é de broadcast.**

- **Questão 14:** Qual é o valor hexadecimal para o campo de dois bytes do tipo de quadro Ethernet? A que protocolo de camada superior isso corresponde?

> **O valor hexadecimal do campo "Ethernet Frame type" é 0x0806, correspondente ao protocolo ARP.**

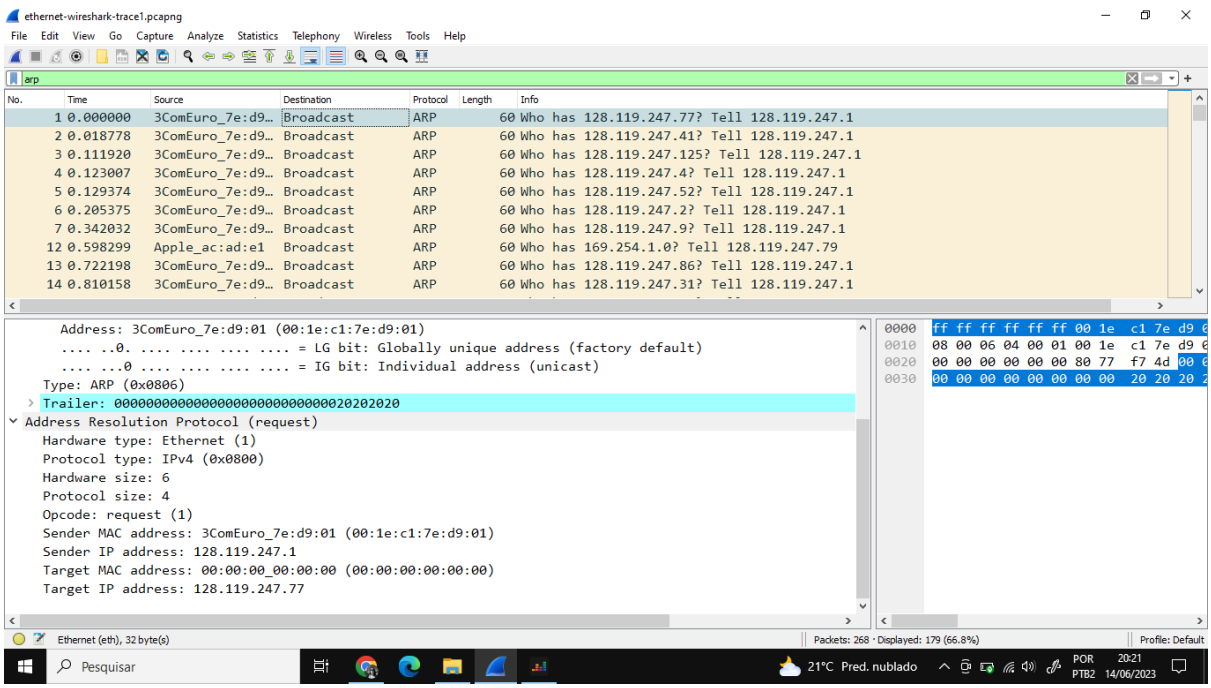
- **Questão 15:** Quantos bytes a partir do início do quadro Ethernet o campo "opcode" do ARP começa?

> **O campo "opcode" do ARP começa 20 bytes a partir do início do quadro Ethernet.**

- **Questão 16:** Qual é o valor do campo "opcode" na mensagem de solicitação ARP enviada pelo seu computador?

> **O valor hexadecimal do campo "opcode" dentro da carga útil do ARP no pedido é 0x0001, correspondente a uma solicitação.**

- **Questão 17:** A mensagem de solicitação ARP contém o endereço IP do remetente? Se a resposta for sim, qual é o valor desse endereço?



> **Sim, a mensagem ARP contém o endereço IP 128.119.247.77 como endereço do remetente.**

- **Questão 18:** Qual é o endereço IP do dispositivo para o qual está sendo solicitado o endereço Ethernet correspondente na mensagem de solicitação ARP enviada pelo seu computador?

> **O campo "Target MAC address" é definido como 00:00:00:00:00:00 para questionar a máquina cujo endereço IP correspondente (128.119.247.1) está sendo consultado.**

- **Questão 19:** Qual é o valor do campo opcode dentro da mensagem de resposta ARP recebida pelo seu computador?

> **O valor hexadecimal do campo "opcode" dentro da mensagem de resposta ARP recebida é 0x0001.**

- **Questão 20:** Por fim (!), vamos analisar a resposta à mensagem de solicitação ARP! Qual é o endereço Ethernet correspondente ao endereço IP especificado na mensagem de solicitação ARP enviada pelo seu computador (veja a pergunta 18)?

> **O campo "Target MAC address" é definido como 00:00:00:00:00:00 para questionar a máquina cujo endereço IP correspondente (128.119.247.1) está sendo consultado.**

- **Questão 21:** Analisamos a mensagem de solicitação ARP enviada pelo seu computador usando o Wireshark e a mensagem de resposta ARP enviada em resposta. Mas existem outros dispositivos nesta rede que também estão enviando mensagens de solicitação ARP que você pode encontrar no rastreamento. Por que não há respostas ARP no seu rastreamento que são enviadas em resposta a essas outras mensagens de solicitação ARP?

> **Existem várias razões pelas quais não há respostas ARP em seu rastreamento em resposta a outras mensagens de solicitação ARP. Isso pode ocorrer devido ao momento em que a captura foi feita, configurações de rede específicas ou ao comportamento dos dispositivos envolvidos. A ausência de respostas ARP no rastreamento não é necessariamente um problema, pois diferentes dispositivos e configurações de rede podem ter comportamentos distintos em relação às solicitações ARP.**