1. Wireshark: Ethernet и ARP

- 1.Захват и анализ Ethernet-кадров
- 1. Каков 48-разрядный Ethernet-адрес вашего компьютера?

f0:03:8c:0a:67:59

```
54 60711 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
                                                                                            54 60712 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
584 GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
        91 3 183872
                          192 168 0 101
                                                      128.119.245.12
                                                                                  TCP
       92 3.184095 192.168.0.101
                                                  128.119.245.12
                                                                              HTTP
        93 3.220526
                         23.2.215.95
                                                                                              1514 443 → 60709 [ACK] Seq=3724 Ack=3831 Win=64128 Len=1460 [TCP segment of a re
       94 3.220718 23.2.215.95
                                                                                             1514 443 → 60709 [PSH, ACK] Seq=5184 Ack=3831 Win=64128 Len=1460 [TCP segment of
                                                     192,168,0,101
> Frame 92: 584 bytes on wire (4672 bits), 584 bytes captured (4672 bits) on interface \Device\NPF_{E4A60854-AB14-4EB8-BC8C-E5C0ACCE9AA5}, id 0 
V Ethernet II, Src: AzureWav_0a:67:59 (f0:03:8c:0a:67:59), Dst: Tp-LinkT_7e:a8:d7 (68:ff:7b:7e:a8:d7)
    > Destination: Tp-LinkT_7e:a8:d7 (68:ff:7b:7e:a8:d7)
> Source: AzureWav_0a:67:59 (f0:03:8c:0a:67:59)
       Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.0.101, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 60712, Dst Port: 80, Seq: 1, Ack: 1, Len: 530
  Hypertext Transfer Protocol
```

2. Какому устройству соответствует значение Ethernet-адреса?

Судя по скриншоту: AzureWav 0a:67:59

3. Каково значение исходного Ethernet-адреса? Какое устройство имеет такой Ethernet-адрес?

Ethernet-адрес: (68:ff:7b:7e:a8:d7) Устройство: Tp-LinkT_7e:a8:d7

```
> Frame 102: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{E4A60854-AB14-4EB8-BC8C-E5C0ACCE9AA5}, id 0

> Ethernet II, Src: Tp-LinkT_7e:a8:d7 (68:ff:7b:7e:a8:d7), Dst: AzureWav_0a:67:59 (f0:03:8c:0a:67:59)

> Destination: AzureWav_0a:67:59 (f0:03:8c:0a:67:59)

> Source: Tp-LinkT_7e:a8:d7 (68:ff:7b:7e:a8:d7)

    Type: IPv4 (0x0800)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.101

> Transmission Control Protocol, Src Port: 80, Dst Port: 60712, Seq: 4381, Ack: 531, Len: 481

> [4 Reassembled TCP Segments (4861 bytes): #99(1460), #100(1460), #101(1460), #102(481)]

> Hypertext Transfer Protocol

> Line-based text data: text/html (98 lines)
```

4. Каков адрес назначения в этом Ethernet-кадре? Это Ethernet-адрес вашего компьютера?

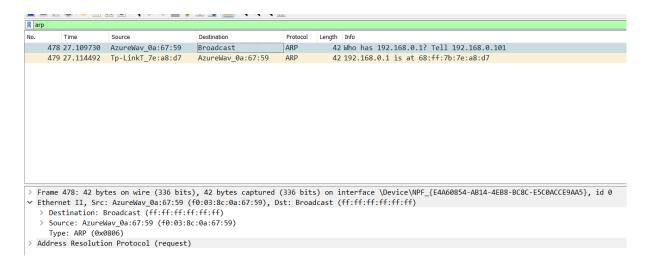
f0:03:8c:0a:67:59 – что соответствует Ethernet-адресу моего компьютера.

2. ARP-протокол

1. Каковы шестнадцатеричные значения исходного и конечного адресов в Ethernet-кадре, содержащем сообщение с broadcast ARP-запросом?

Source: AzureWav_0a:67:59 (f0:03:8c:0a:67:59)

Destination: Broadcast (ff:ff:ff:ff:ff)



2. Содержится ли в ARP-сообщении IP-адрес отправителя?

Да, содержится: Sender IP address: 192.168.0.101

```
Type: ARP (0x0806)

Address Resolution Protocol (request)

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: request (1)

Sender MAC address: AzureWav_0a:67:59 (f0:03:8c:0a:67:59)

Sender IP address: 192.168.0.101

Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00)

Target IP address: 192.168.0.1
```

3. Где в ARP-запросе находится сама «вопросная часть» – Ethernet-адрес той машины, чей соответствующий IP-адрес мы запрашиваем?

Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00)

Оно установлено в нули, так как адрес машины неизвестен на текущий момент.

4. Где в сообщении с ARP-откликом хранится Ethernet-адрес, который мы запрашивали на основе соответствующего IP-адреса?

Его можно увидеть в поле: Sender MAC address: Tp-LinkT 7e:a8:d7 (68:ff:7b:7e:a8:d7)

```
> Source: Tp-LinkT_7e:a8:d7 (68:ff:7b:7e:a8:d7)
    Type: ARP (0x0806)

Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Tp-LinkT_7e:a8:d7 (68:ff:7b:7e:a8:d7)
    Sender IP address: 192.168.0.1
    Target MAC address: AzureWav_0a:67:59 (f0:03:8c:0a:67:59)
    Target IP address: 192.168.0.101
```