Захват и анализ кадров Ethernet

Начнем с рассмотрения кадра Ethernet, содержащего сообщение HTTP GET.

```
Wireshark · Packet 33 · wlp2s0
                                                                                                                                                                                       □ ×
 Frame 33: 549 bytes on wire (4392 bits), 549 bytes captured (4392 bits) on interface wlp2s0, id 0
Fighernet II, Src: IntelCor_9c:9f:e1 (f0:57:a6:9c:9f:e1), Dst: Tp-LinkT_7e:93:dd (68:ff:7b:7e:93:dd)
                                     _9c:9f:e1 (f0:57:a6:9c:9f:e1)
Type: IPv4 (0x0800)

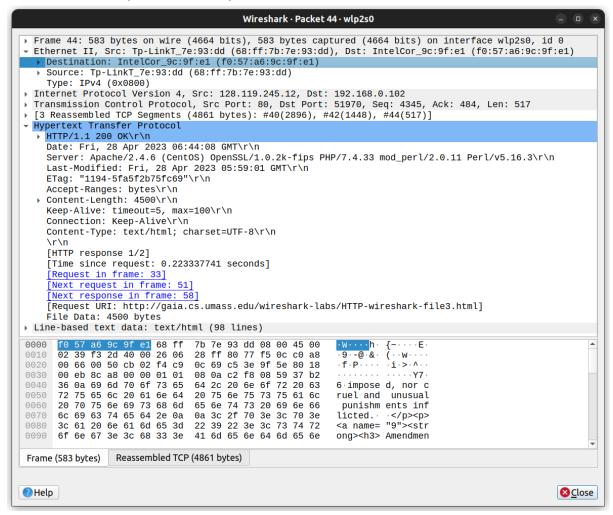
Internet Protocol Version 4, Src: 192.168.0.102, Dst: 128.119.245.12

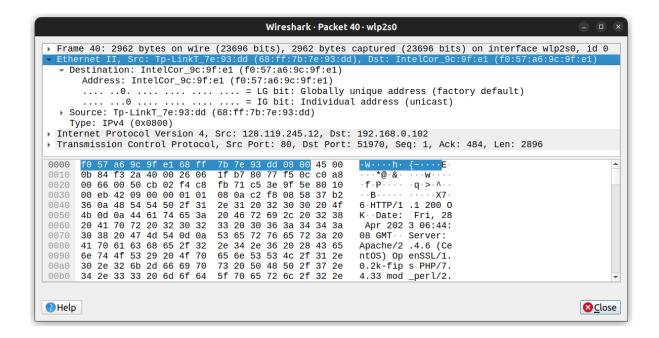
Transmission Control Protocol, Src Port: 51970, Dst Port: 80, Seq: 1, Ack: 1, Len: 483
  Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n]
            Request Method: GET
           Request Version: HTTP/1.1
        Host: gaia.cs.umass.edu\r\n
       Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
       User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.0.0... Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;... Accept-Encoding: gzip, deflate\r\n Accept-Language: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7\r\n
        r\n
        [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
        [HTTP request 1/2]
[Response in frame:
        [Next request in frame: 51]
                                                        a6 9c 9f e1 08 00 45 00
19 ae c0 a8 00 66 80 77
9d 7b f4 c8 fb 71 80 18
08 0a 37 b2 36 0a c2 f8
           68 ff 7b 7e 93 dd f0 57
02 17 e8 a0 40 00 40 06
                                                                                                        h · {~·· · W
· · · · · @ · @ ·
                                                                                                                            . . . f . w
           {···q·
·7·6··
                                                                                                                · P · >
                                                        69 72 65 73 68 61 72 6b 54 50 2d 77 69 72 65 73
                                                                                                        zGET /w ireshark
-labs/HT TP-wires
           68 61 72 6b 2d 66 69 6c
48 54 54 50 2f 31 2e 31
67 61 69 61 2e 63 73 2e
75 0d 0a 43 6f 6e 6e 65
                                                        65 33 2e 68 74 6d 6c 20 0d 0a 48 6f 73 74 3a 20
                                                                                                        hark-fil e3.html
HTTP/1.1 · Host:
                                                                                                        gaia.cs. umass.ed
u Conne ction: k
                                                        75 6d 61 73 73 2e 65 64
63 74 69 6f 6e 3a 20 6b
? Help
```

```
ptrvsrg@acer:~
                                  sudo wireshark
                                                                                                                            ptrvsrg@acer:~
ptrvsrg@acer ~ » sudo lshw -C network
             description: Wireless interface
product: Dual Band Wireless-AC 3168NGW [Stone Peak]
             vendor: Intel Corporation physical id: 0 bus info: pci@0000:02:00.0
             logical name: wlp2s0
             version: 10
serial: f0:57:a6:9c:9f:e1
             width: 64 bits clock: 33MHz
 capabilities: pm msi pciexpress bus_master cap_list ethernet physical wireless configuration: broadcast=yes driver=iwlwifi driverversion=5.19.0-41-generic firmware=29.19 3743027.0 3168-29.ucode ip=192.168.0.102 latency=0 link=yes multicast=yes wireless=IEEE 802.11 resources: irq:77 memory:c0a00000-c0a01fff
             description: Ethernet interface
             product: RTL8111/8168/8411 PCI Express Gigabit Ethernet Controller vendor: Realtek Semiconductor Co., Ltd.
             physical id: 0
bus info: pci@0000:03:00.0
             logical name: enp3s0
version: 15
             version: 13
serial: c0:18:50:81:f1:7f
capacity: 1Gbit/s
width: 64 bits
clock: 33MHz
capabilities: pm msi pciexpress msix bus_master cap_list ethernet physical tp mii 10bt 10b
   fd 100bt 100bt-fd 1000bt-fd autonegotiation
     configuration: autonegotiation=on broadcast=yes driver=r8169 driverversion=5.19.0-41-gener firmware=rtl8168h-2_0.0.2 02/26/15 latency=0 link=no multicast=yes port=twisted pair resources: _irq:55 ioport:2000(size=256) memory:c0904000-c0904fff memory:c0900000-c0903fff
 trvsrg@acer ~ »
```

- 1. Какой 48-битный Ethernet-адрес вашего компьютера?
 - MAC-адрес источника f0:57:a6:9c:9f:e1
 - Это МАС-адрес беспроводного интерфейса
- 2. Что такое 48-битный адрес назначения в кадре Ethernet? Это Ethernet-адрес gaia.cs.umass.edu? Какое устройство имеет этот адрес Ethernet?
 - MAC-адрес получателя 68:ff:7b:7e:93:dd
 - Это МАС-адрес роутера (проверено)
- 3. Каково шестнадцатеричное значение двухбайтового поля типа кадра в кадре Ethernet, несущем HTTP-запрос GET? Какому протоколу верхнего уровня это соответствует?
 - Type 0x0800 (IPv4)
- 4. Через сколько байтов с самого начала кадра Ethernet появляется ASCII-буква «G» в «GET» в кадре Ethernet? Не учитывайте биты преамбулы при подсчете, т. е. предположите, что кадр Ethernet начинается с адреса назначения кадра Ethernet.
 - Во вкладке байтов пакета видно, что адрес начала MAC-адреса получателя 0x0000, а адрес ASCII-буквы «G» 0x0042. Значит ASCII-буква «G» появляется через 66 байтов

Затем ответьте на вопросы, основываясь на содержимом кадра Ethernet, содержащего первый байт сообщения HTTP OK.





- 5. Каково значение адреса источника Ethernet? Это адрес вашего компьютера или gaia.cs.umass.edu (Подсказка: ответнет). Какое устройство имеет этот адрес Ethernet?
 - MAC-адрес источника 68:ff:7b:7e:93:dd
 - Это МАС-адрес роутера (проверено)
- 6. Что такое адрес назначения в кадре Ethernet? Это Ethernet-адрес вашего компьютера?
 - MAC-адрес получателя f0:57:a6:9c:9f:e1
 - Это МАС-адрес беспроводного интерфейса
- 7. Введите шестнадцатеричное значение для двухбайтового поля типа кадра. Какому протоколу верхнего уровня это соответствует?
 - Type 0x0800 (IPv4)
- 8. Через сколько байтов с самого начала кадра Ethernet появляется буква ASCII «О» в «ОК» (т. е. код ответа HTTP) в кадре Ethernet? Не учитывайте биты преамбулы при подсчете, т. е. предположите, что кадр Ethernet начинается с адреса назначения кадра Ethernet.
 - Во вкладке байтов пакета видно, что адрес начала MAC-адреса получателя 0x0000, а адрес ASCII-буквы «О» 0x004f. Значит ASCII-буква «О» появляется через 79 байтов
- 9. Сколько кадров Ethernet (каждый из которых содержит дейтаграмму IP, каждый из которых содержит сегмент TCP) несут данные, являющиеся частью полного ответного сообщения HTTP «ОК 200…»?
 - 3 кадра Ethernet

Кэширование ARP

Давайте посмотрим на содержимое кэша ARP на вашем компьютере.

- 10. Сколько записей хранится в вашем кэше ARP?
 - Хранится 1 запись
- 11. Что содержится в каждой отображаемой записи кэша ARP?
 - В отображаемой записи содержится IP-адрес, MAC-адрес, тип и имя сетевого интерфейса устройства

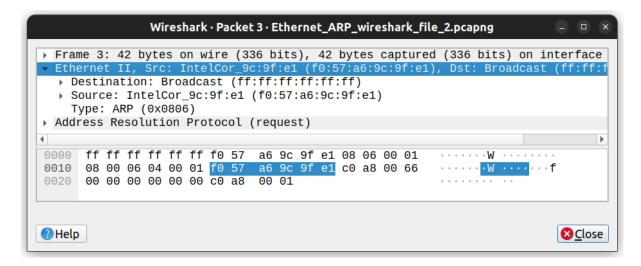
Наблюдение за ARP в действии

Начнем с рассмотрения кадров Ethernet, содержащих сообщения ARP.

```
ptrvsrg@acer:~/Programming/NSU_Network_Technologies/lab10 Q = - - ×

sudo wireshark × ptrvsrg@acer:~/Programming/NSU_Net... × ∨

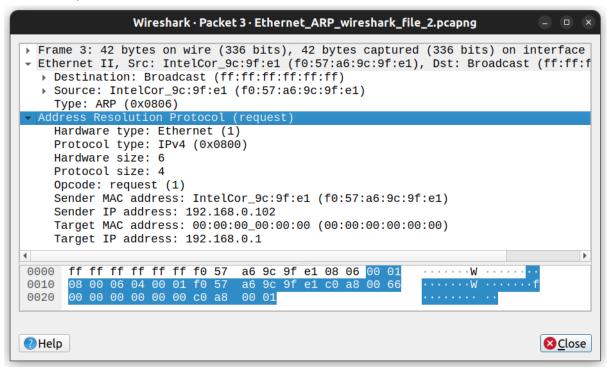
ptrvsrg@acer NSU_Network_Technologies/lab10 (master %) » make delete_ARP_cache
arp -d -a
_gateway (192.168.0.1) at 68:ff:7b:7e:93:dd [ether] on wlp2s0
ptrvsrg@acer NSU_Network_Technologies/lab10 (master %) » [
```



12. Каково шестнадцатеричное значение адреса источника в кадре Ethernet, содержащем сообщение запроса ARP, отправленное вашим компьютером?

- MAC-адрес источника f0:57:a6:9c:9f:e1
- 13. Каково шестнадцатеричное значение адресов назначения в кадре Ethernet, содержащем сообщение запроса ARP, отправленное вашим компьютером? И какое устройство соответствует этому адресу?
 - MAC-адрес получателя ff:ff:ff:ff:ff:ff
 - Это широковещательный МАС-адрес
- 14. Каково шестнадцатеричное значение двухбайтового поля *Туре* кадра Ethernet? Какому протоколу верхнего уровня это соответствует?
 - Type 0x0800 (IPv4)

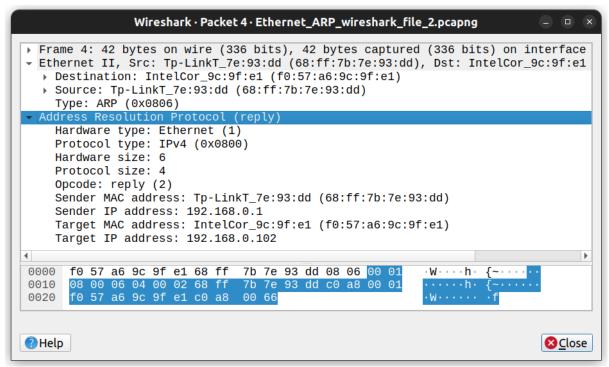
Теперь давайте углубимся в сами ARP-сообщения. Рассмотрим ARP-запрос.



- 15. Сколько байтов между началом кадра Ethernet и ARP полем opcode?
 - Во вкладке байтов пакета видно, что адрес начала MAC-адреса получателя 0x0000, а адрес ARP поля *opcode* 0x0014. Значит ARP поле *opcode* появляется через 20 байтов
- 16. Каково значение поля *opcode* в сообщении запроса ARP, отправленном вашим компьютером?
 - Значение поля opcode 1 (request)
- 17. Содержит ли сообщение запроса ARP IP-адрес отправителя? Если ответ да, то каково его значение?
 - IP-адрес отправителя 192.168.0.102
- 18. Каков IP-адрес устройства, соответствующий Ethernet-адрес которого запрашивается в сообщении запроса ARP, отправляемом вашим компьютером?

- IP-адрес устройства, соответствующий Ethernet-адрес которого запрашивается в сообщении запроса ARP - 192.168.0.1

Теперь найдите ответное сообщение ARP, отправленное в ответ на запрос ARP с вашего компьютера.



- 19. Каково значение поля *opcode* в ответном сообщении ARP, полученном вашим компьютером?
 - Значение поля *opcode* 2 (reply)
- 20. Какой адрес Ethernet соответствует IP-адресу, который был указан в сообщении ARP-запроса, отправленном вашим компьютером?
 - MAC-адрес, соответствующий IP-адресу, указанному в ARP-запросе 68:ff:7b:7e:93:dd