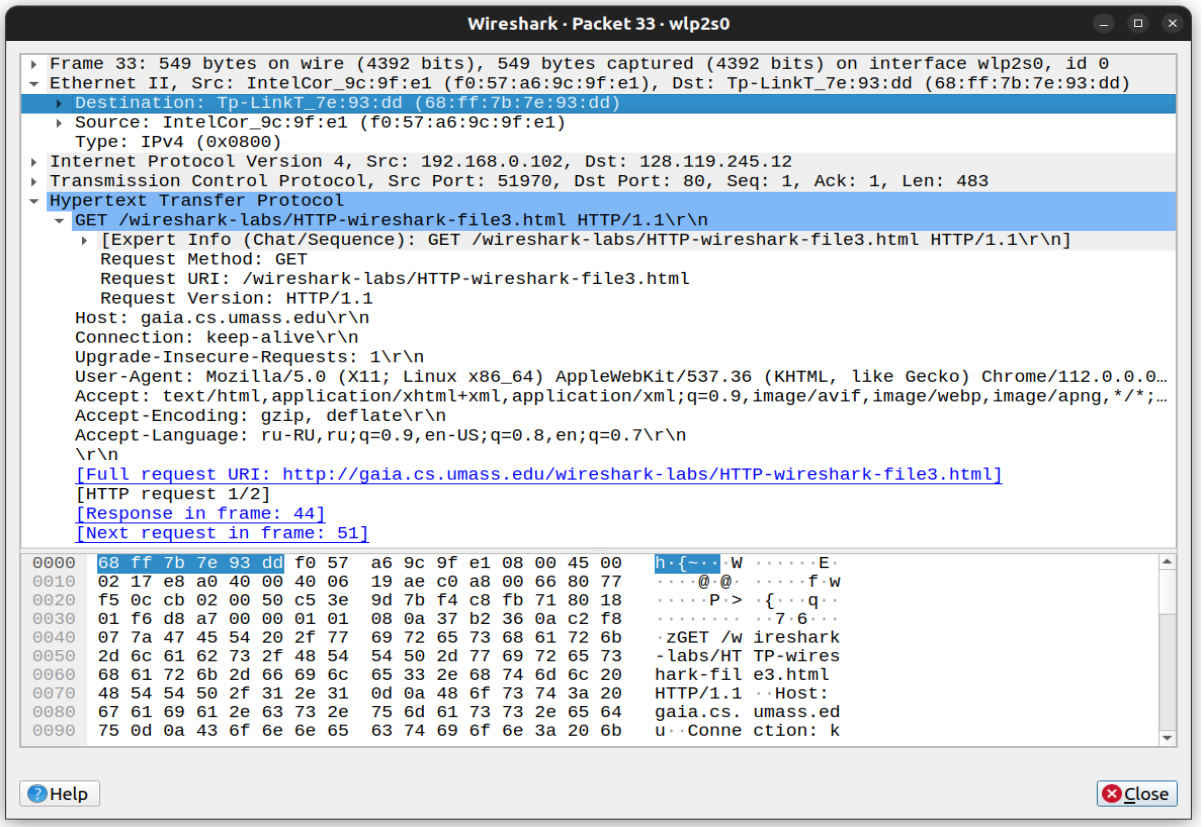
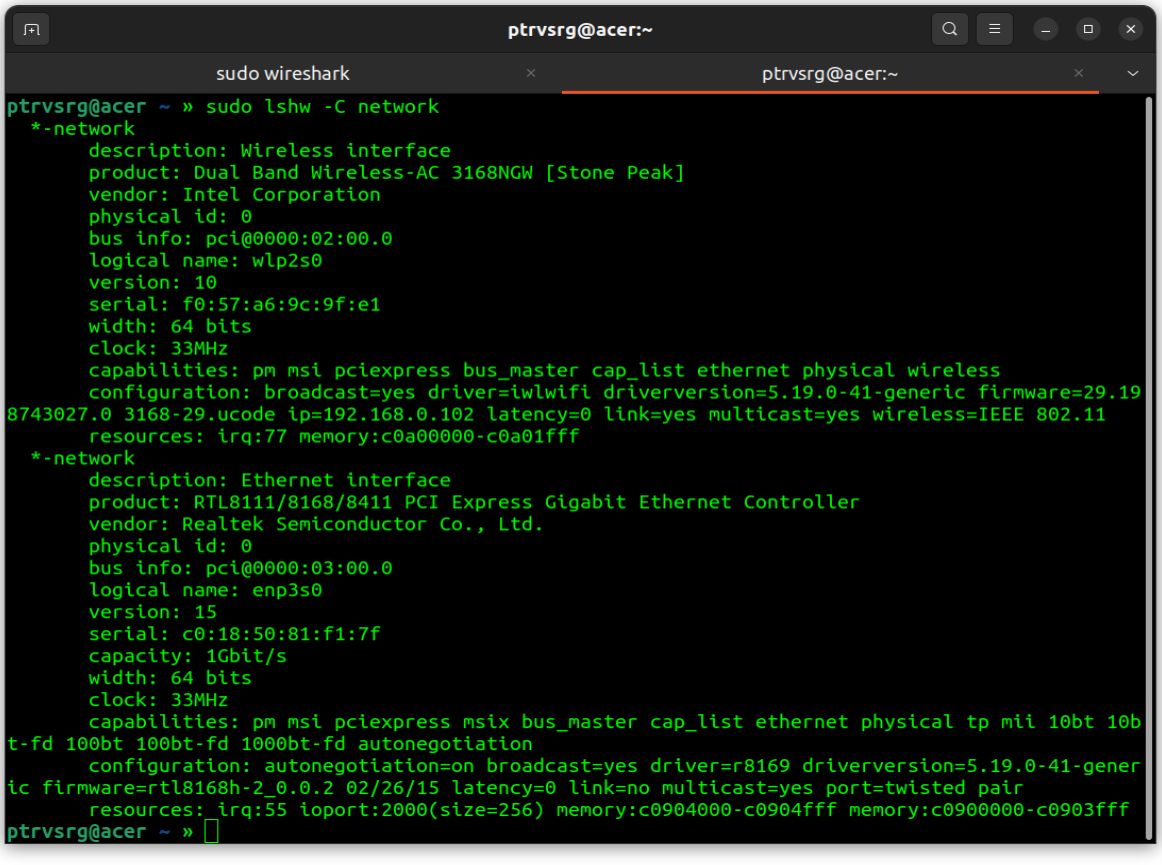
Захват и анализ кадров Ethernet

Начнем с рассмотрения кадра Ethernet, содержащего сообщение HTTP GET.





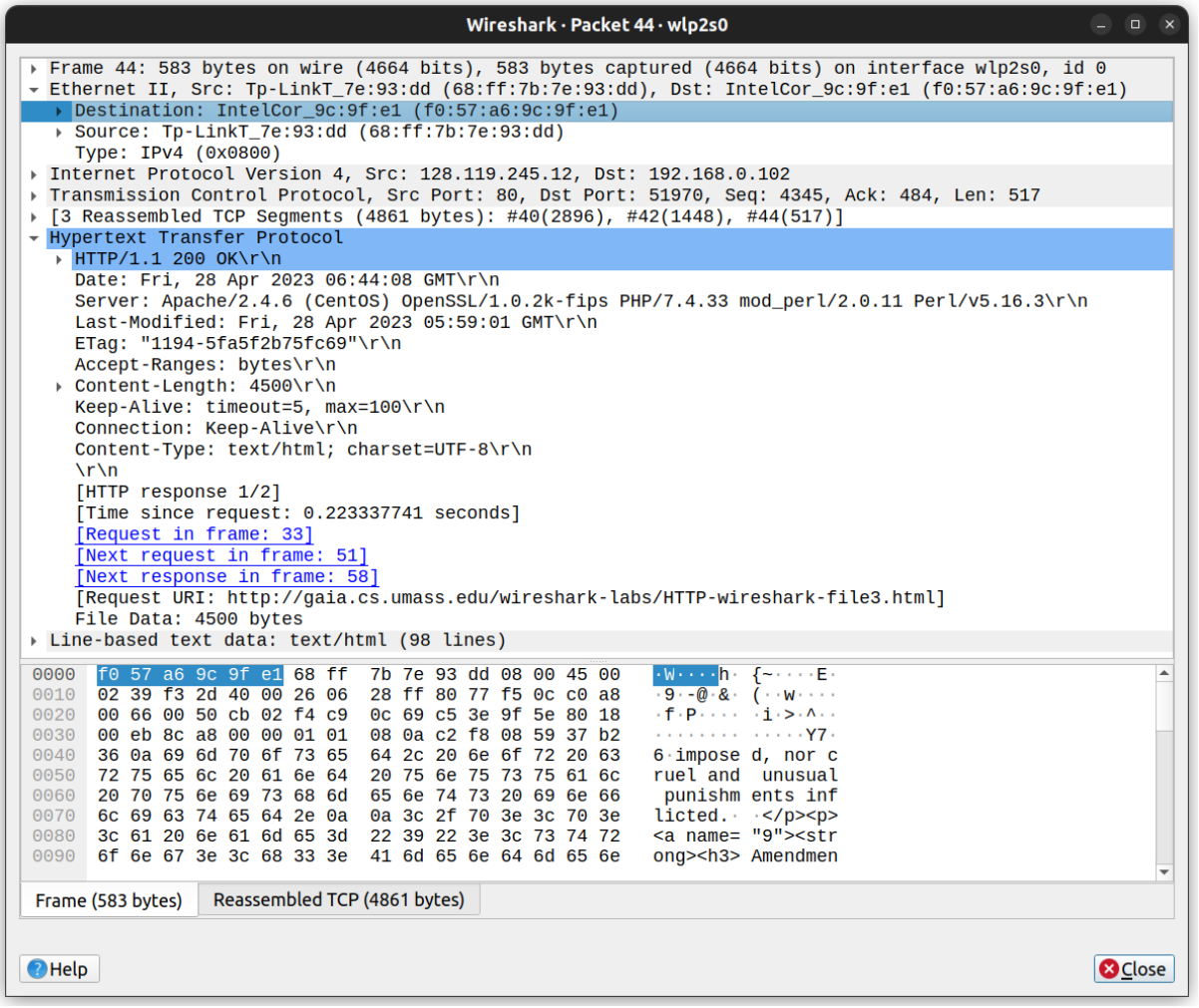
1. Какой 48-битный Ethernet-адрес вашего компьютера?
   - MAC-адрес источника - f0:57:a6:9c:9f:e1
   - Это MAC-адрес беспроводного интерфейса

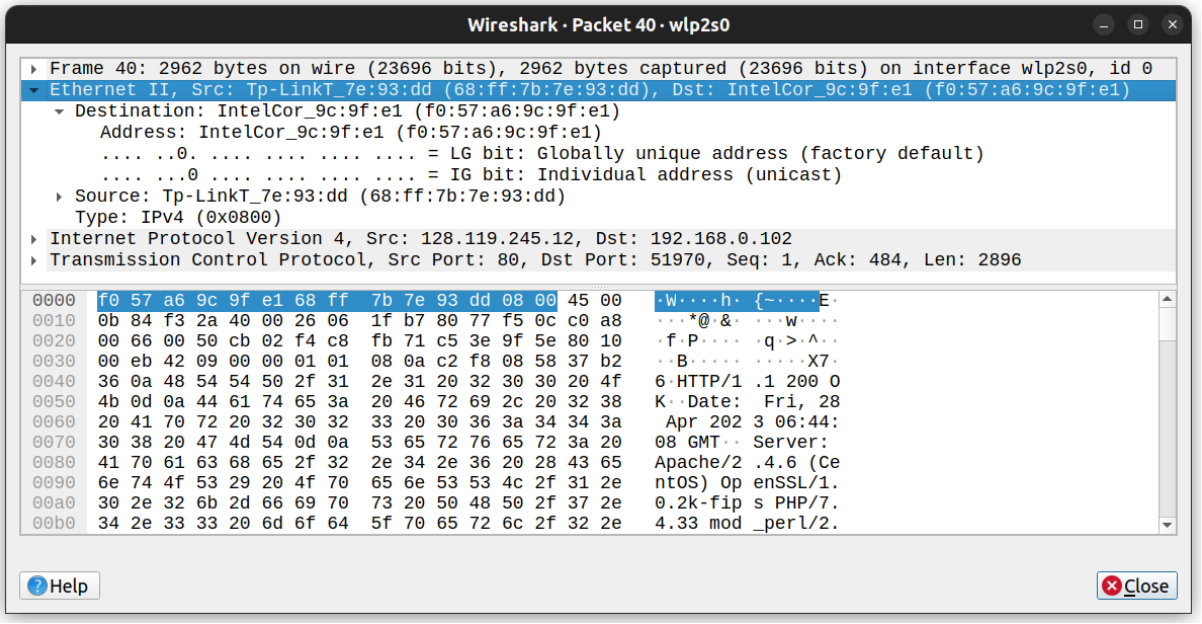
2. Что такое 48-битный адрес назначения в кадре Ethernet? Это Ethernet-адрес gaia.cs.umass.edu? Какое устройство имеет этот адрес Ethernet?
   - MAC-адрес получателя - 68:ff:7b:7e:93:dd
   - Это MAC-адрес роутера (проверено)

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 MAC-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 MAC-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 «O» в «OK» (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.

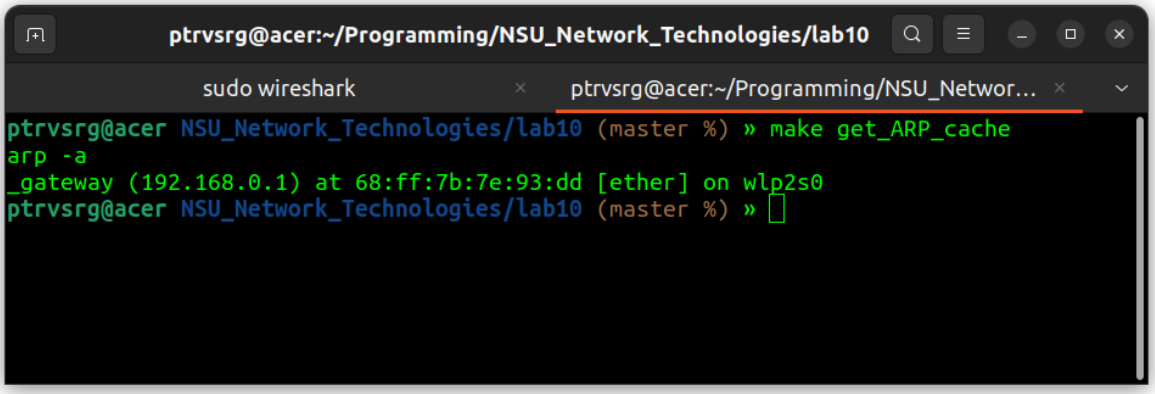
- Во вкладке байтов пакета видно, что адрес начала MAC-адреса получателя - 0x0000, а адрес ASCII-буквы «O» - 0x004f. Значит ASCII-буква «O» появляется через 79 байтов

9. Сколько кадров Ethernet (каждый из которых содержит дейтаграмму IP, каждый из которых содержит сегмент TCP) несут данные, являющиеся частью полного ответного сообщения HTTP «OK 200…»?

- 3 кадра Ethernet

Кэширование ARP

Давайте посмотрим на содержимое кэша ARP на вашем компьютере.

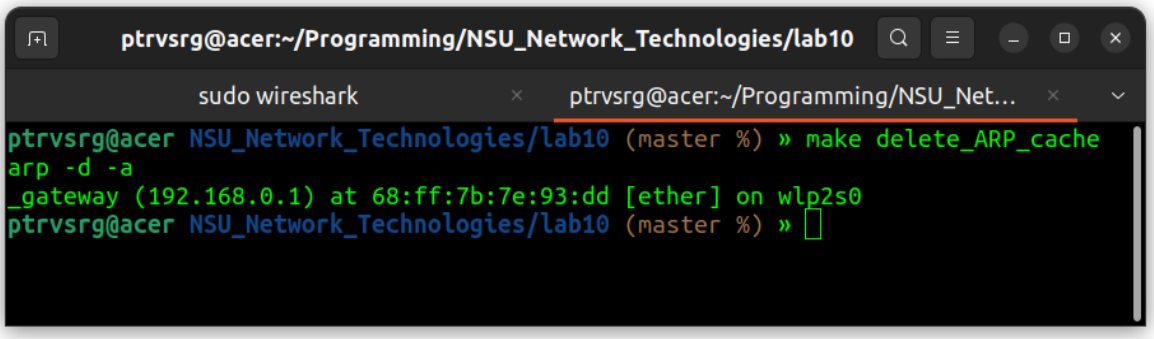


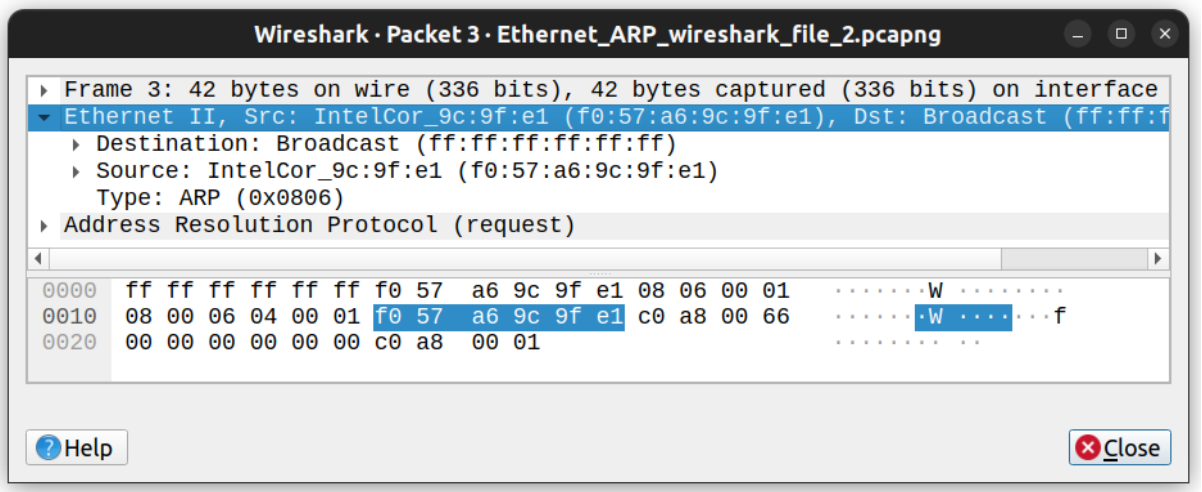
10. Сколько записей хранится в вашем кэше ARP?
    - Хранится 1 запись

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.





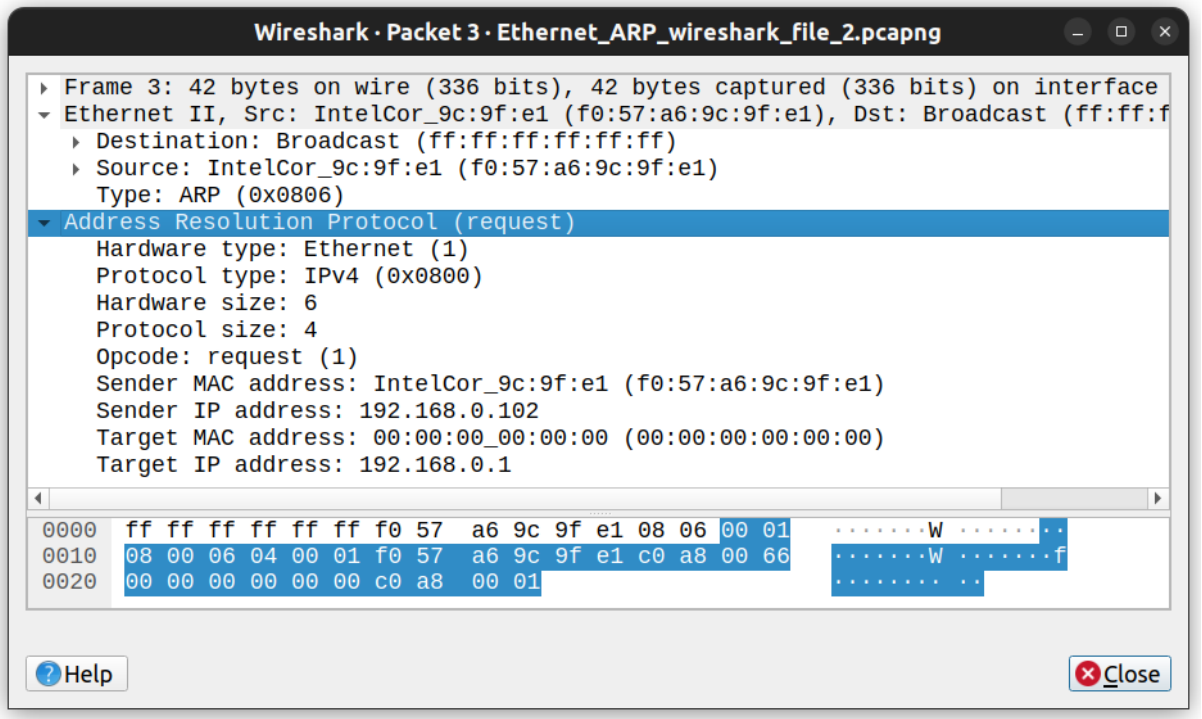
12. Каково шестнадцатеричное значение адреса источника в кадре Ethernet, содержащем сообщение запроса ARP, отправленное вашим компьютером?

- 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 MAC-адрес

14. Каково шестнадцатеричное значение двухбайтового поля *Type* 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

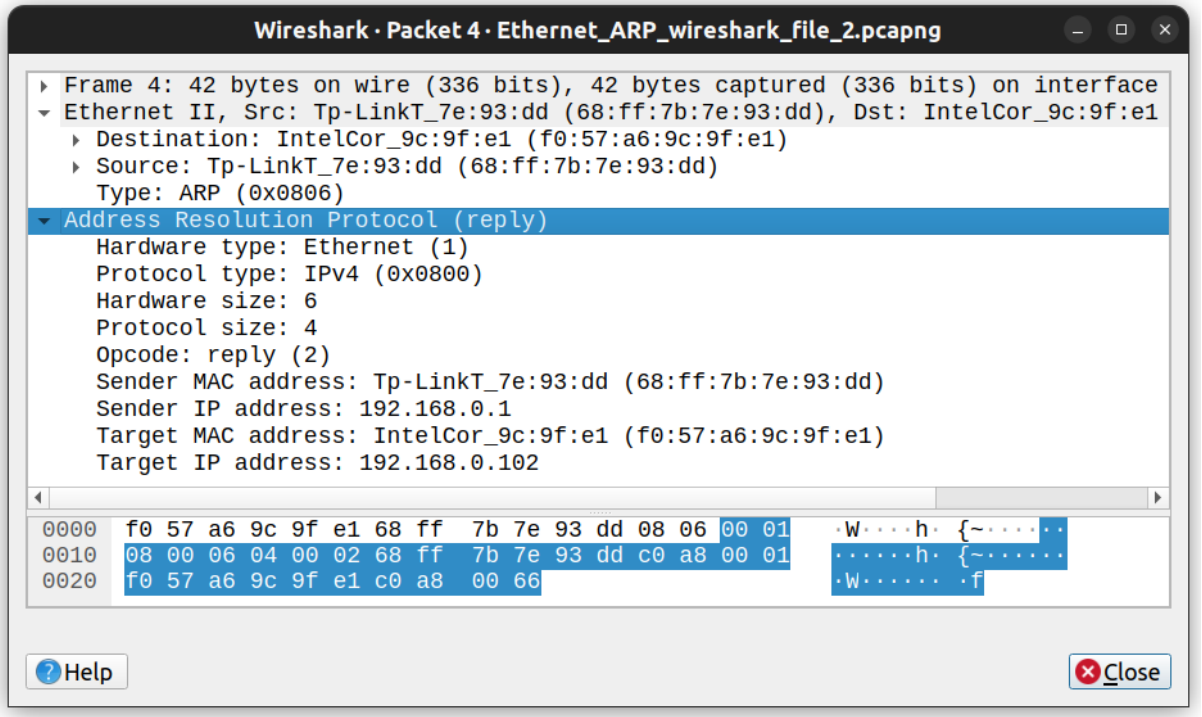
16. Каково значение поля *opcode* в сообщении запроса ARP, отправленном вашим компьютером?
- Значение поля *opcode* - 1 (request)

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