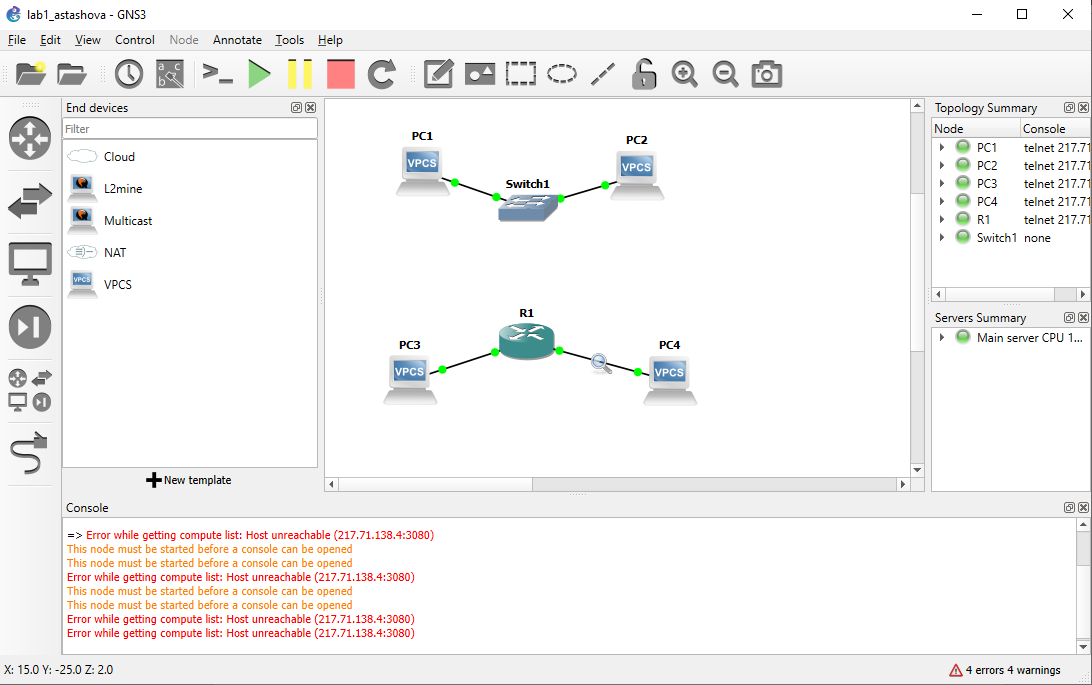
Элтекс, 1 лаба, сети, отчет.   
Асташова Полина Дмитриевна.

1) Установить и настроить эмулятор GNS3

2) Создать простейшую сеть, состоящую из 1 коммутатора и 2 компьютеров, назначить им произвольные ip адреса из одной сети



ip 198.168.1.10/24 192.168.1.1 //для 1-го пк «/24»-маска подсети, 192…-адрес шлюза

ip 198.168.2.10/24 192.168.2.1 //для 2-го пк

3) Запустить симуляцию, выполнить команду ping с одного из компьютеров, используя ip адрес второго компьютера

ping 198.168.2.10 //пингуем с 1-го пк

ping 198.168.1.10 //пингуем со 2-го пк

4) Перехватить трафик протокола arp на всех линках(nb!), задокументировать и проанализировать заголовки пакетов в программе Wireshark, для фильтрации трафика, относящегося к указанному протоколу использовать фильтры Wireshark

№ — Номер пакета в захваченной сессии.

Time — Время с начала захвата.

Source — IP-адрес источника (192.168.1.2).

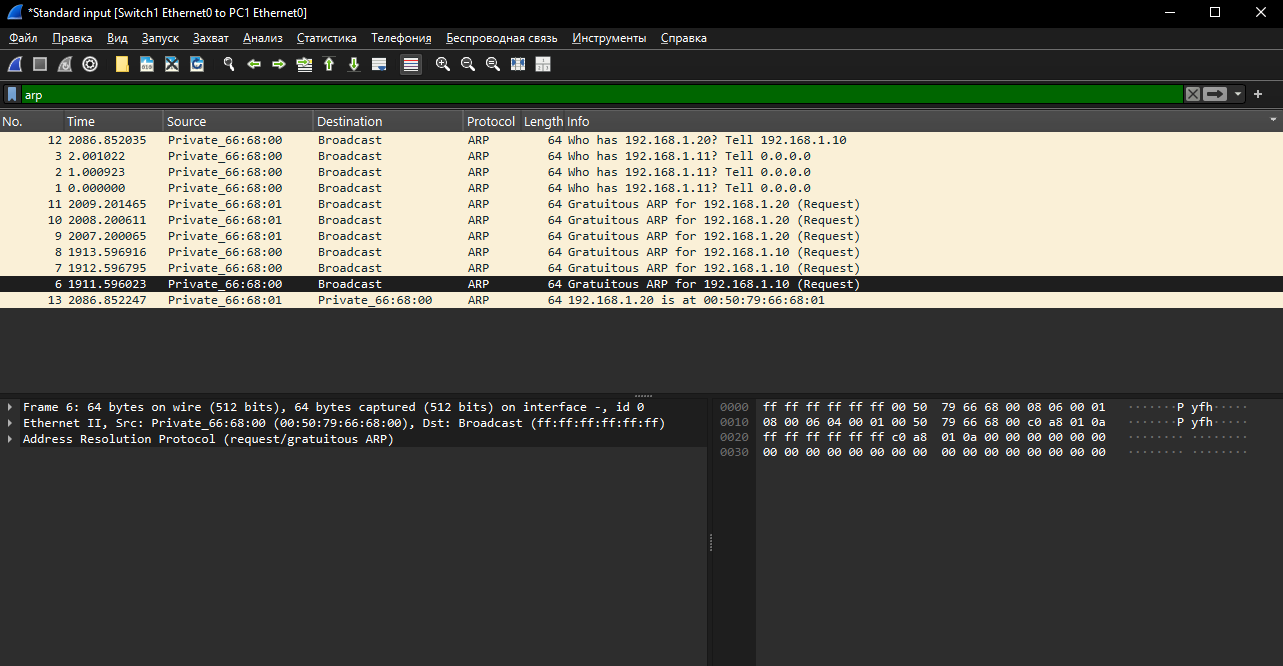
Destination — IP-адрес назначения (192.168.1.1).

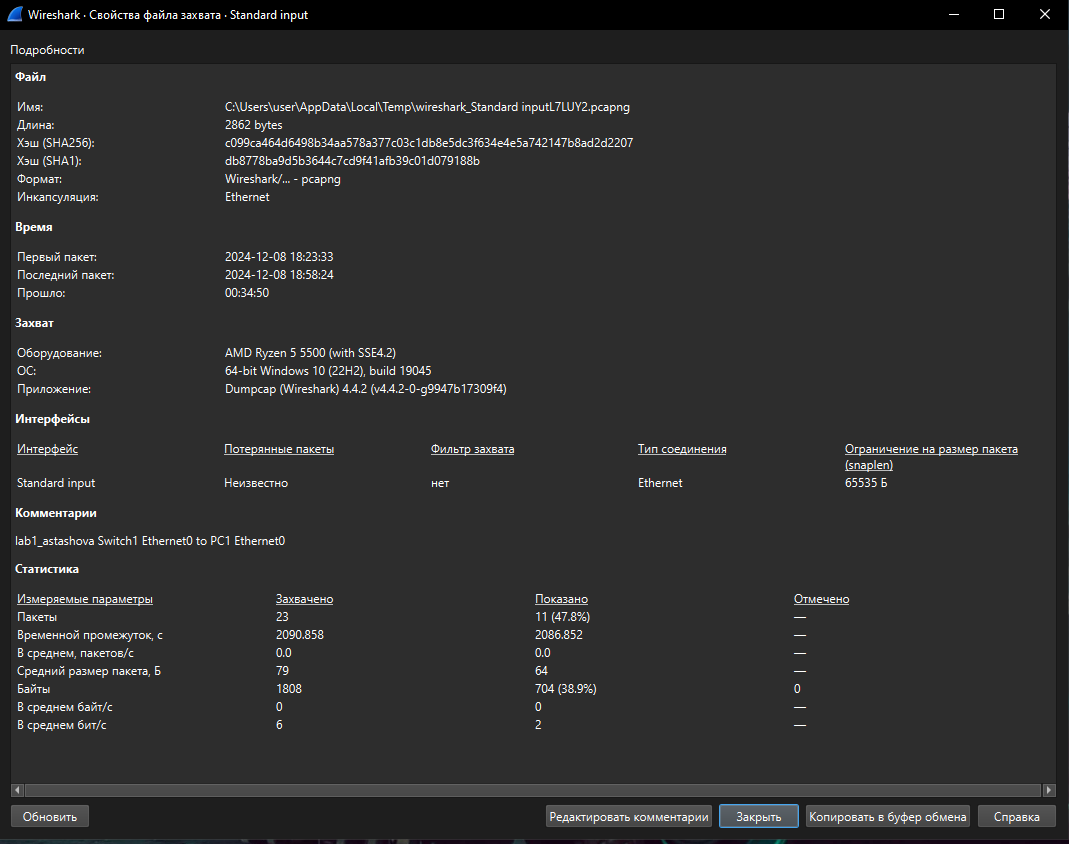
Protocol — Протокол, использованный в пакете (ARP).

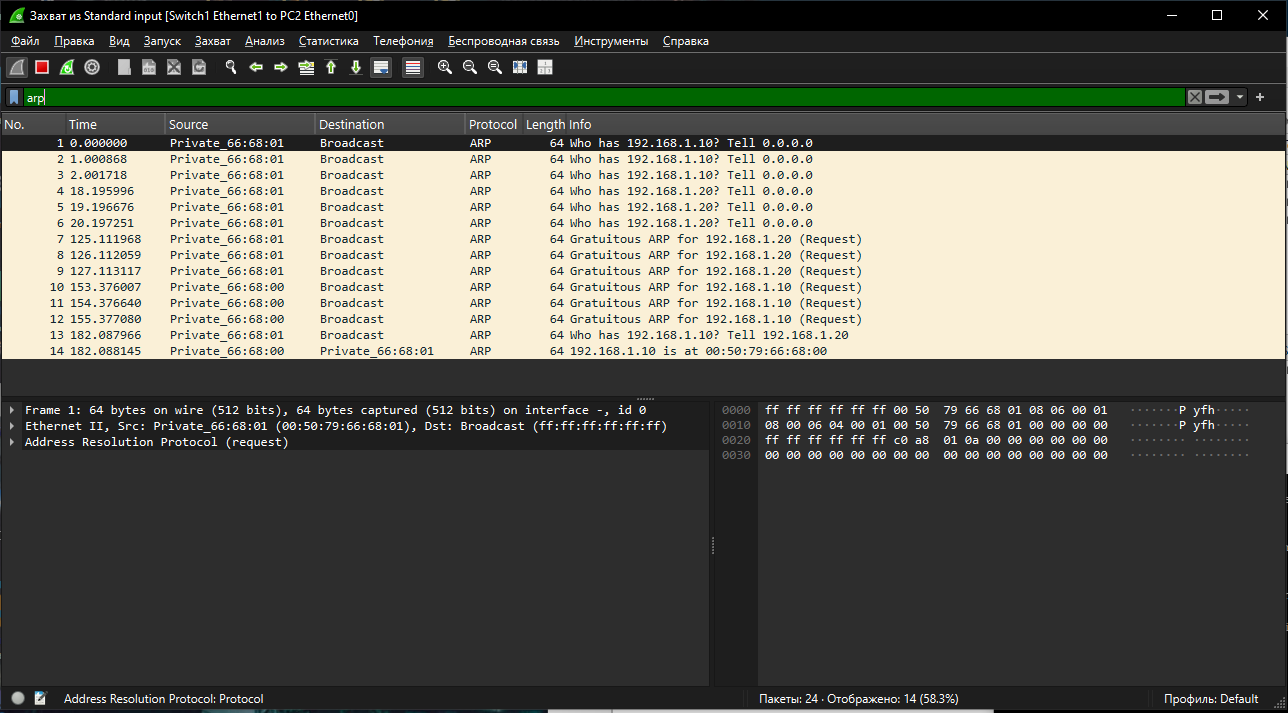
Length — Длина пакета в байтах (42 байта).

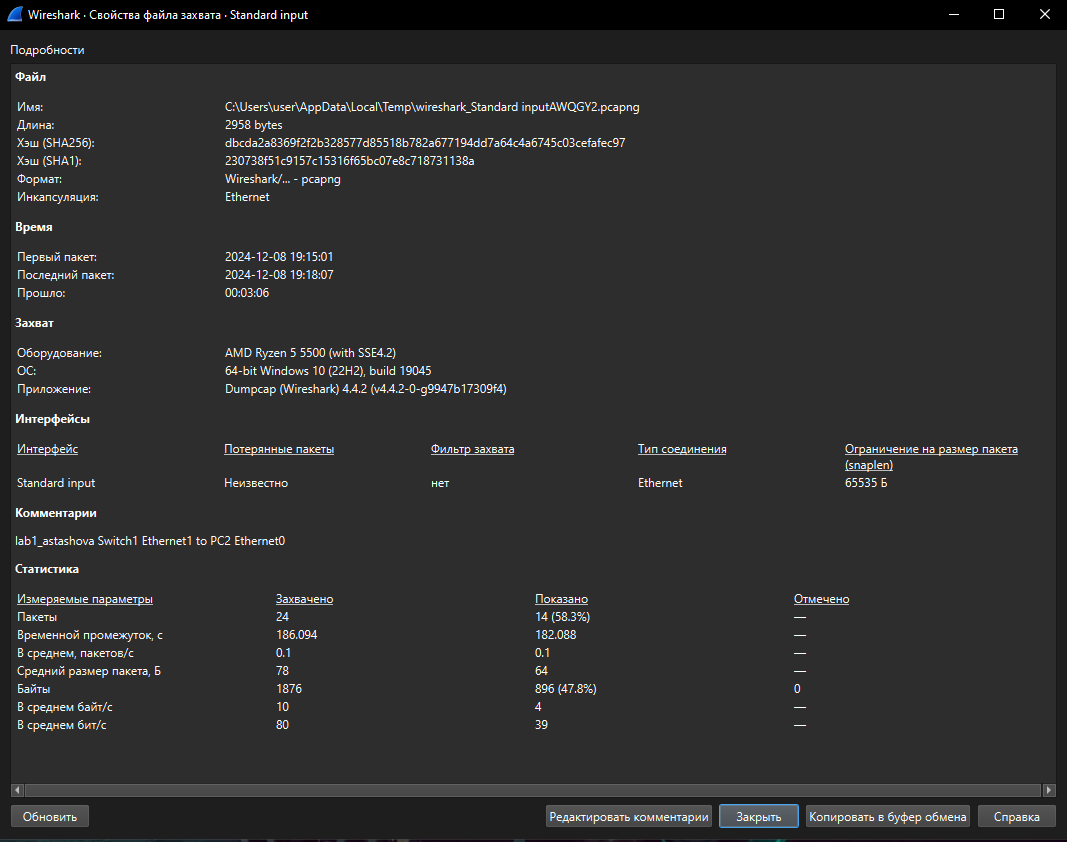
Info — Дополнительная информация о пакете (ARP запрос).

// Packet Details зафиксировала только в конце…

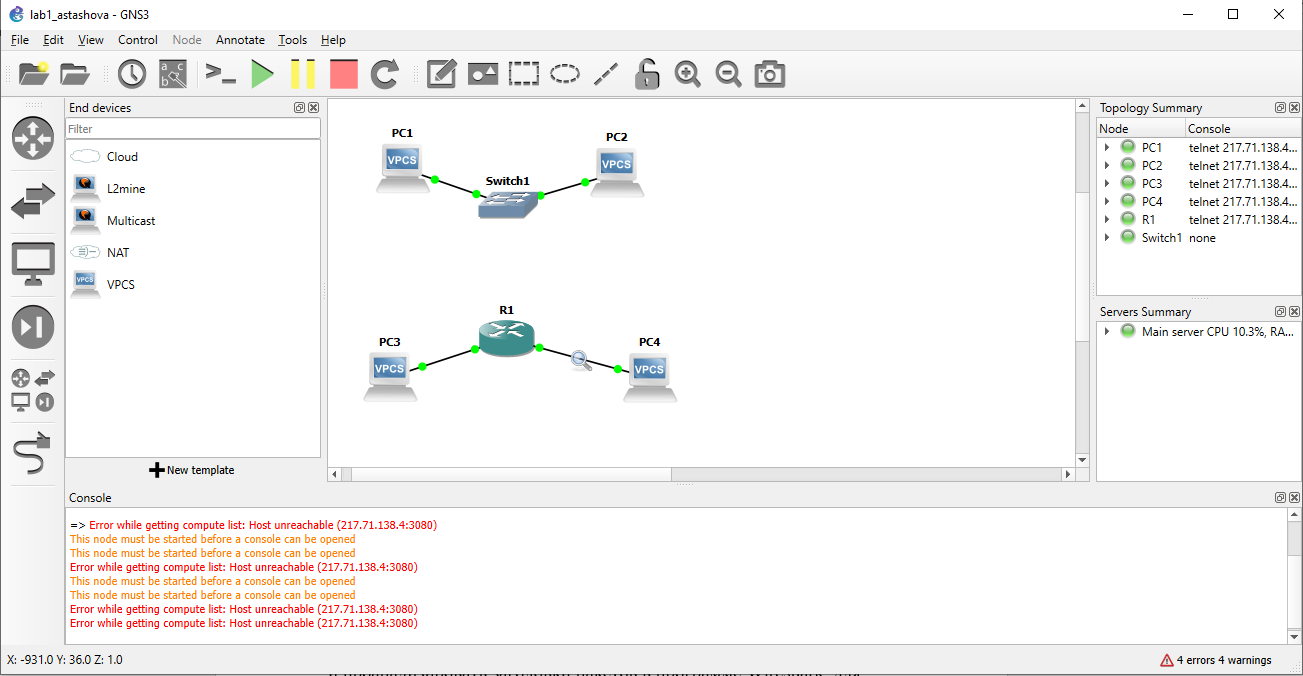
Первый линк:   




Второй линк   




5) Создать простейшую сеть, состоящую из 1 маршрутизатора и 2 компьютеров, назначить им произвольные ip адреса из разных сетей



ip 198.168.1.10/24 192.168.1.1 //для 3-го пк «/24»-маска подсети, 192…-адрес шлюза

ip 198.168.2.10/24 192.168.2.1 //для 4-го пк

Настройка маршрутизатора:

enable

configure terminal

interface FastEthernet0/0

ip address 192.168.1.1 255.255.255.0

no shutdown

exit

interface FastEthernet1/0

ip address 192.168.2.1 255.255.255.0

no shutdown

exit

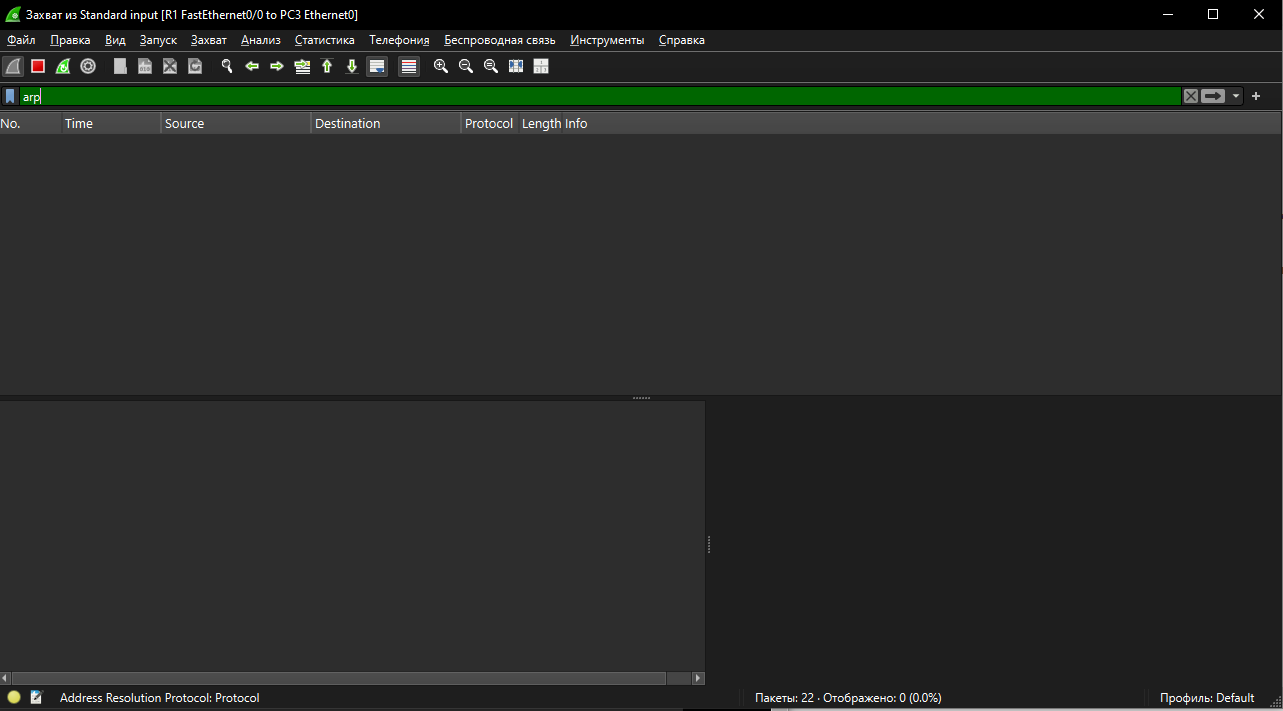
6) Запустить симуляцию, выполнить команду ping с одного из компьютеров, используя ip адрес второго компьютера

ping 198.168.2.10 //пингуем с 3-го пк

ping 198.168.1.10 //пингуем со 4-го пк

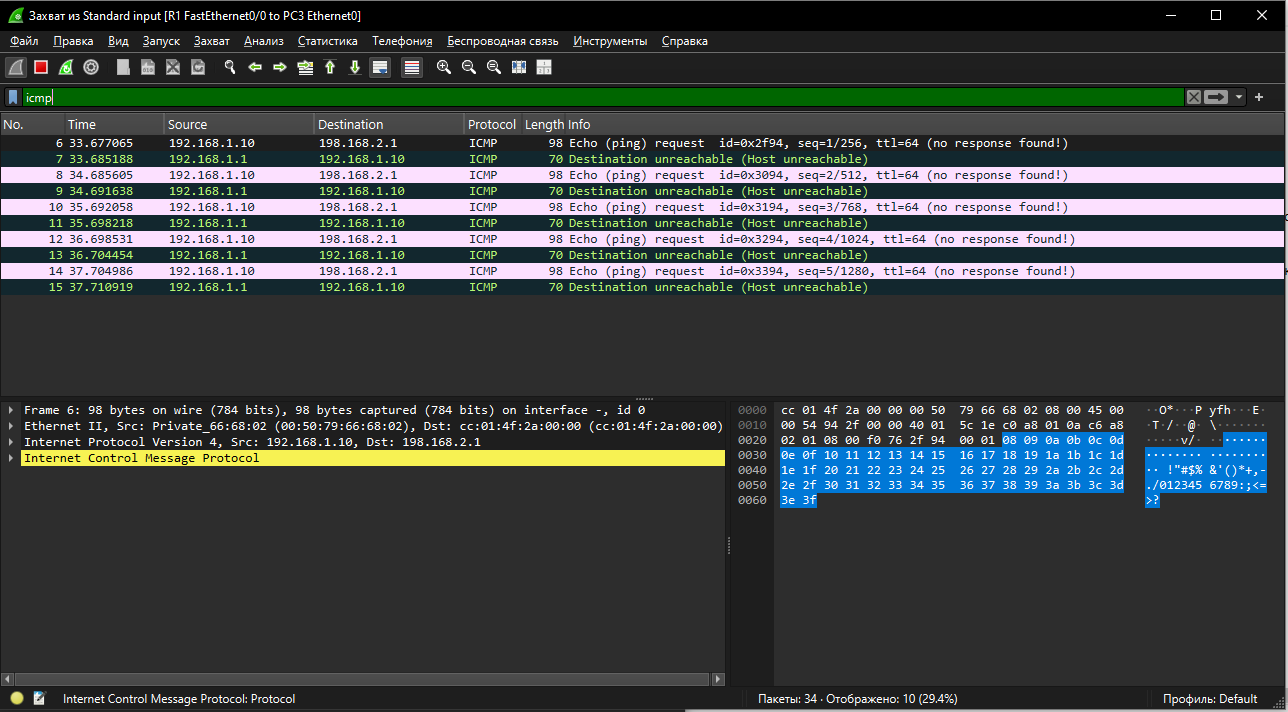
7) Перехватить трафик протокола arp и icmp на всех линках(nb!), задокументировать и проанализировать заголовки пакетов в программе Wireshark, для фильтрации трафика, относящегося к указанному протоколу использовать фильтры Wireshark

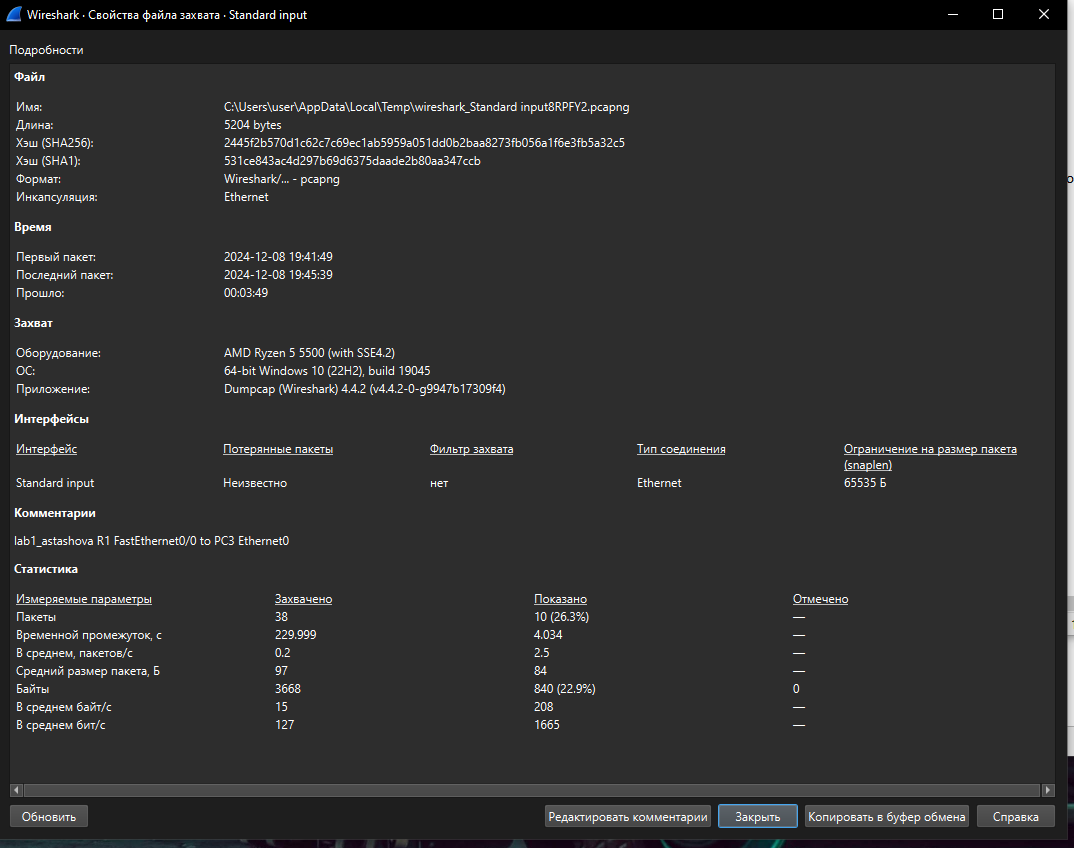
Первый линк с фильтром arp



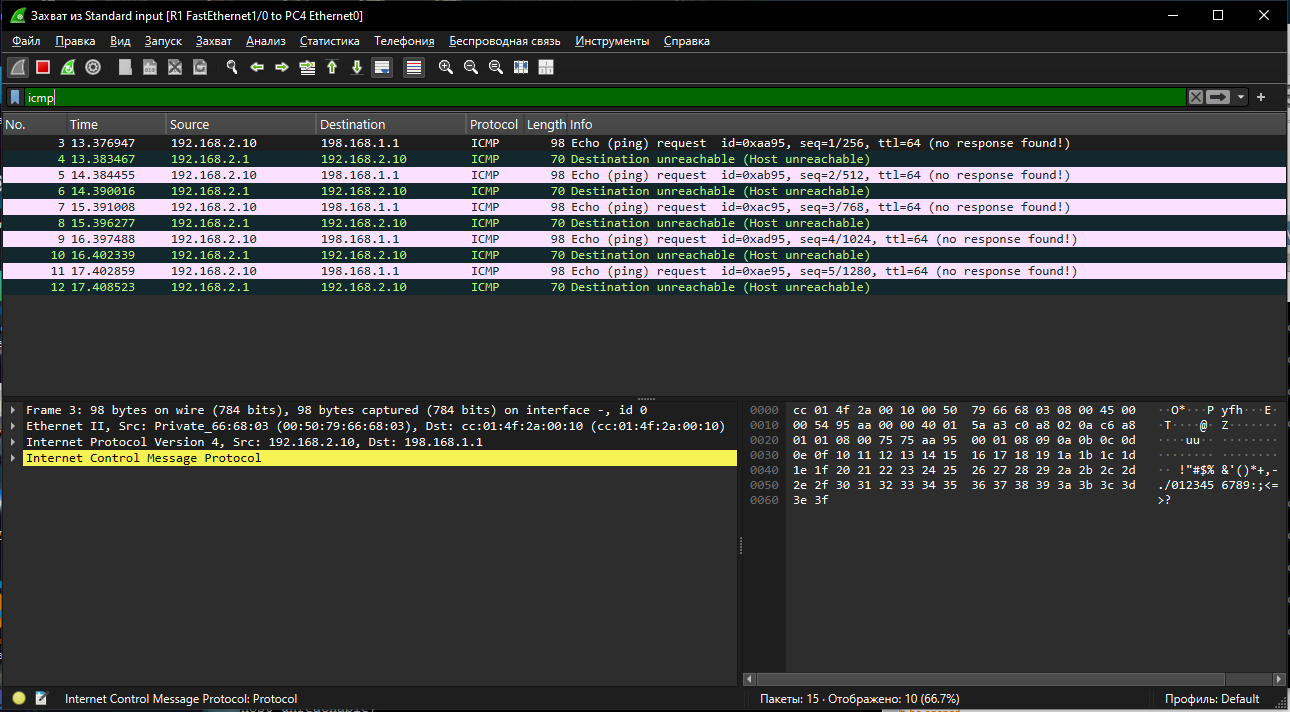
//мы видим что данный фильтр не отображается, потому что маршрутизатор не участвует в arp-процессах

Первый линк с фильтром icmp





Второй линк с фильтром icmp



Packet Details, не знаю что тут добавить, все указано на скриншоте.

