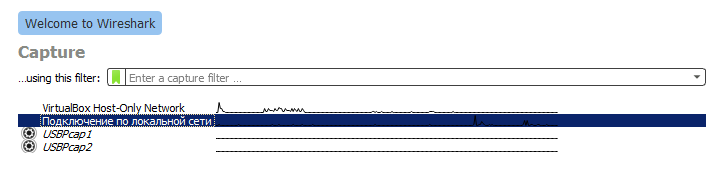
Основы работы с анализатором протоколов wireshark

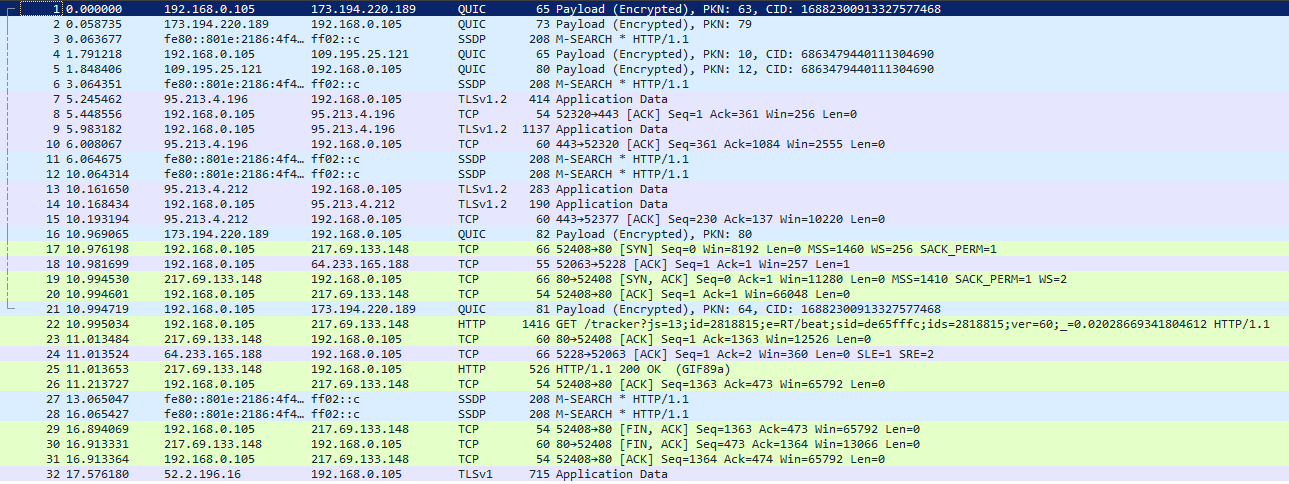
Программа wireshar предназначена для анализа пакетов, проходящих в сети Ethernet. Запустить программу можно выбрав пункт меню "Wireshark".

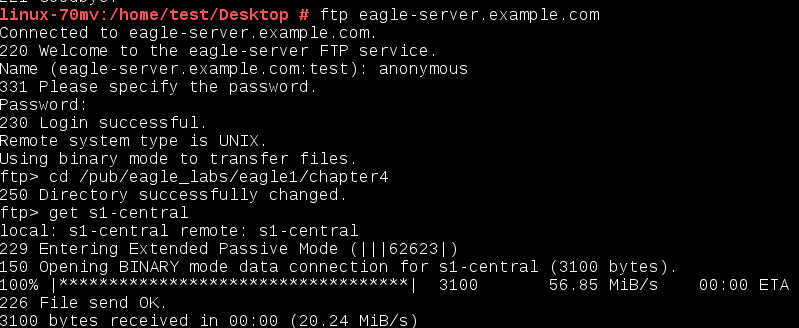
Прежде чем начинать новый сеанс захвата пакетов следует выбрать пункт "Capture", далее пункт меню "Interfaces"

Захватываем интерфейс :



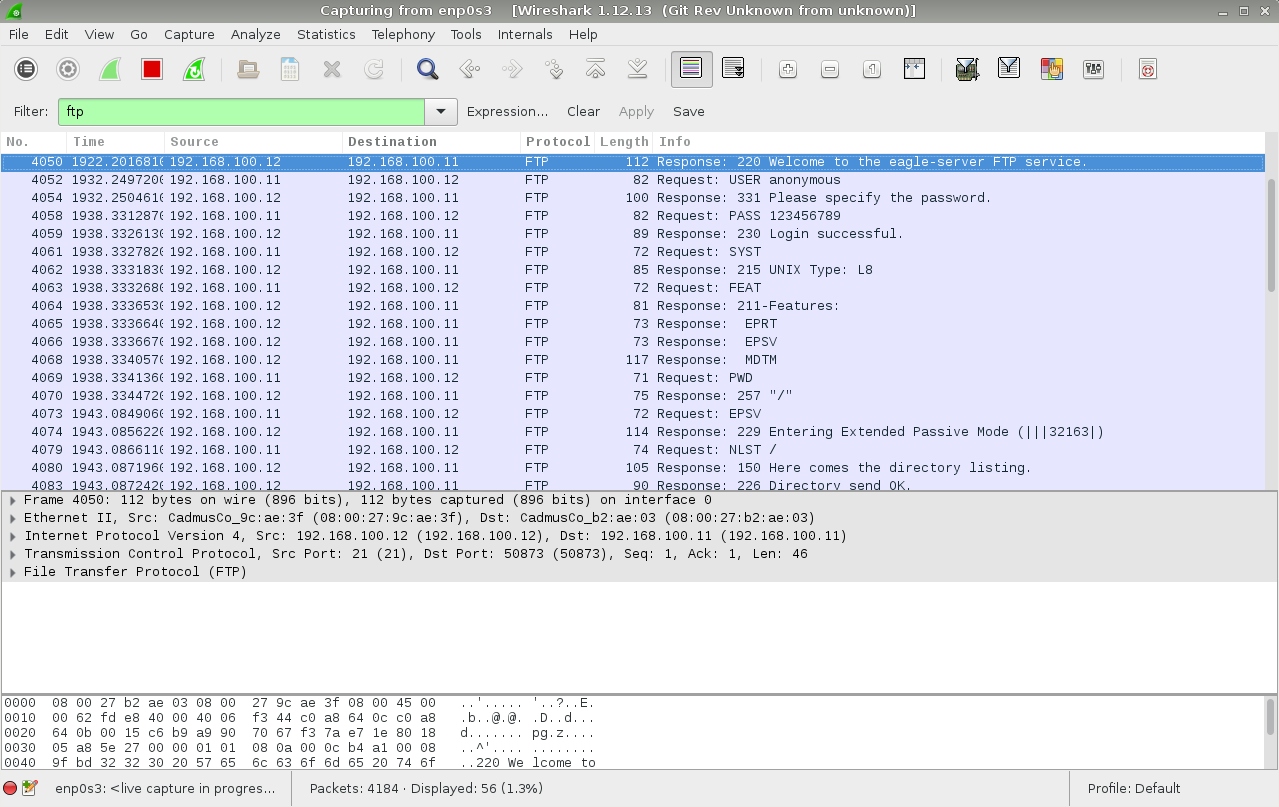
В результате этого в главном окне программы появится список захваченных пакетов, который постоянно пополняется сетевыми пакетами, проходящими по сети. Для прекращения захвата пакетов нужно выбрать пункты меню "Capture" и "Stop".



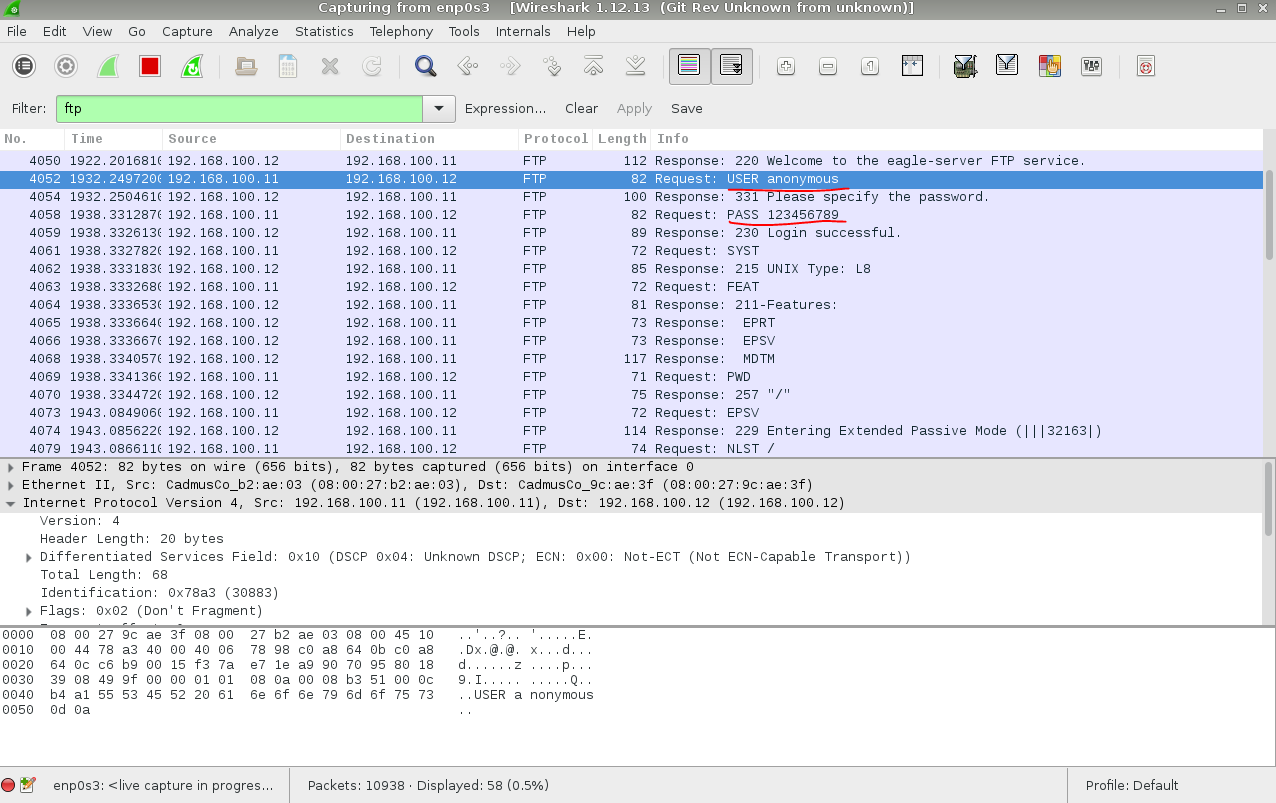


Подключимся по ftp клиенту и скачаем файл .

Отследим наши пакеты . Для это в левом верхнем углу перейдём в display filter и введём туда ftp.

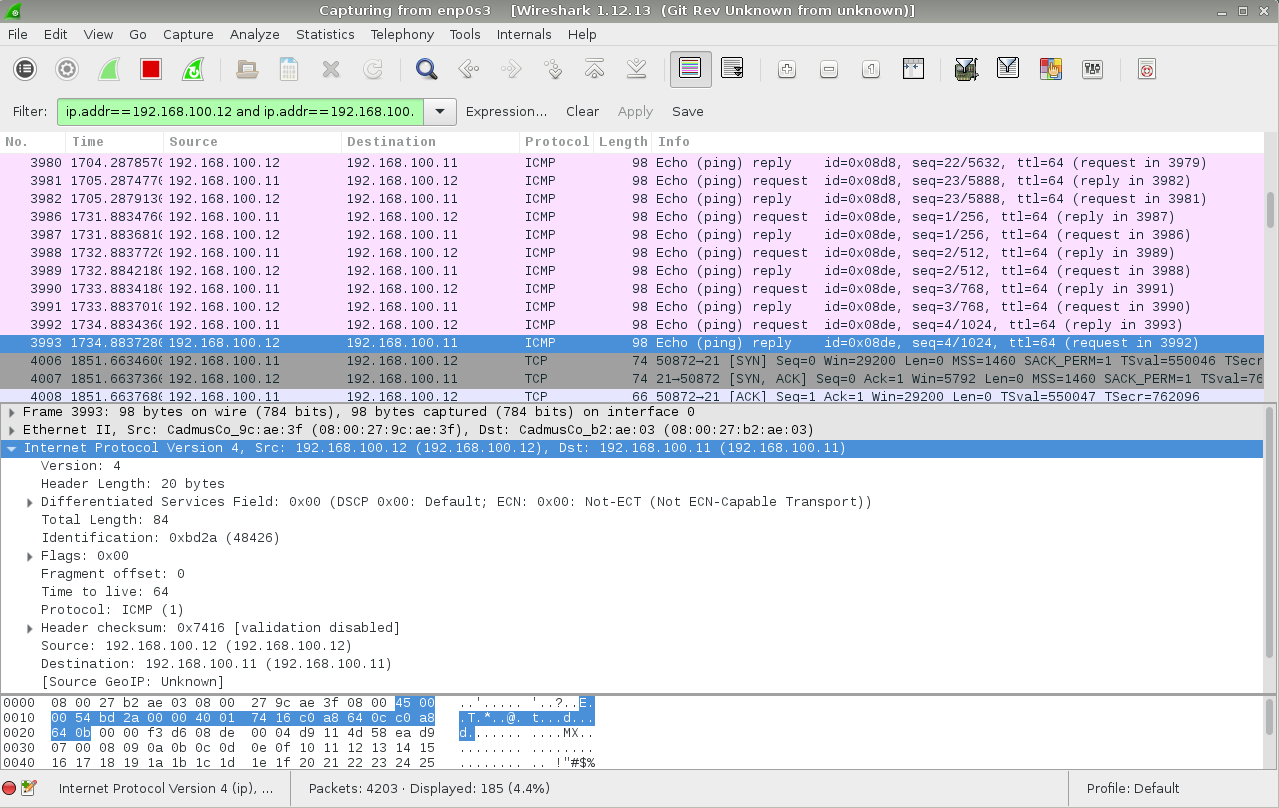


Как мы видим , у нас довольно много пакетов ftp. Особенностью этого протокола в том , что он не шифрует данные , то есть они передаются в открытом виде. В связи с этим , мы легко можем узнать логин и пароль.



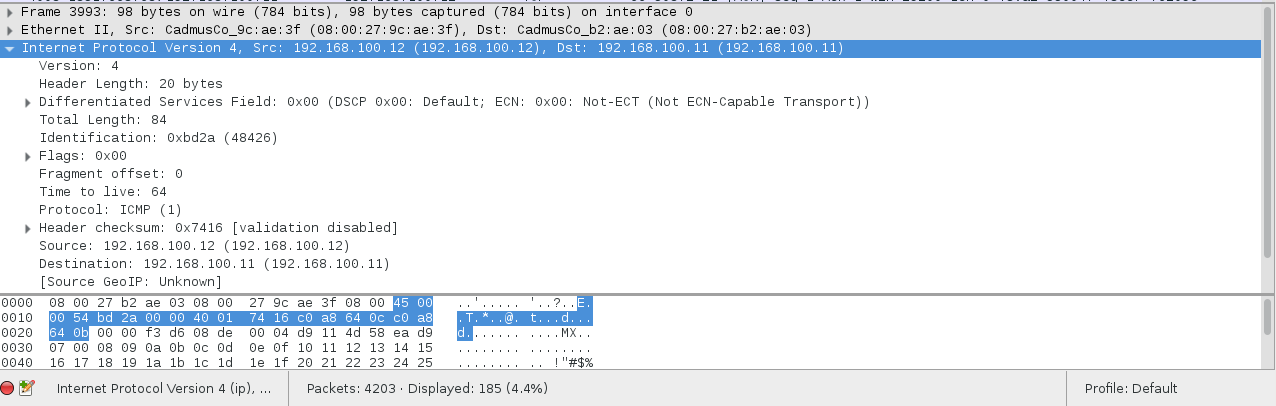
Давайте еще «поиграемся» . Установим фильтр для отслеживания трафика между двумя хостами.

ip.addr== *ip* and ap.addr=  *ip*

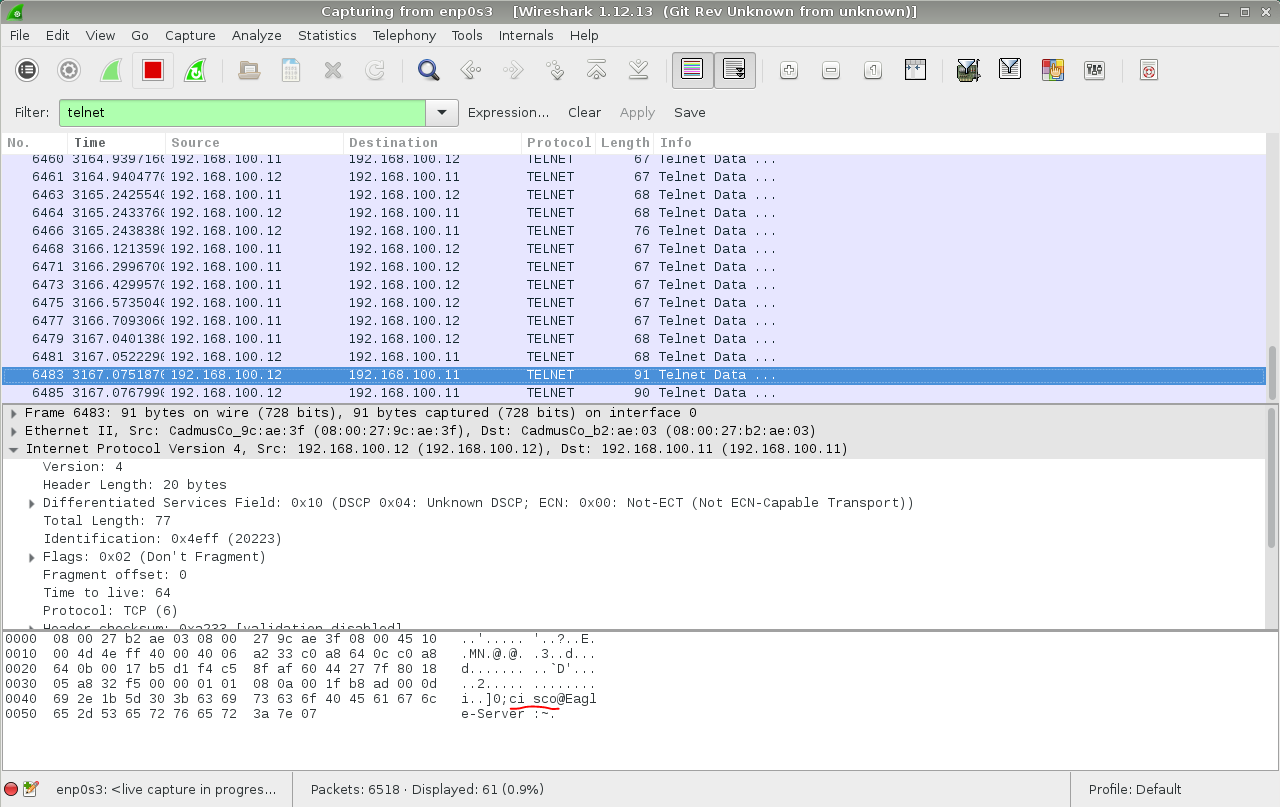


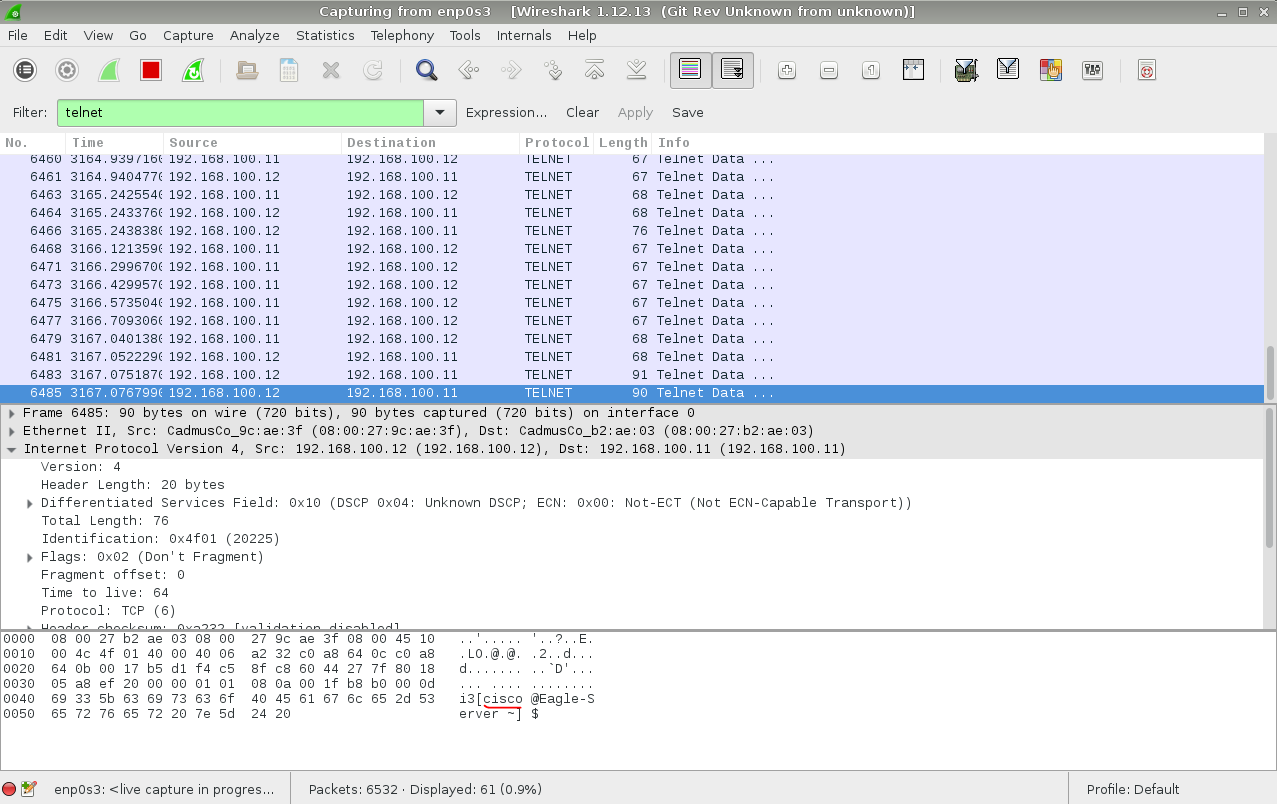
Мы видим , что между нашими адресами передавался протокол ICMP . В данном случае , я проверял связь между двумя компьютерами командой ping.

Более подробную информацию о каждом из пакетов можно получить, выделяя интересущий пакет в полученном списке пакетов и анализируя его содержимое с помощью инфрмации, представленной в среднем окне анализатора.

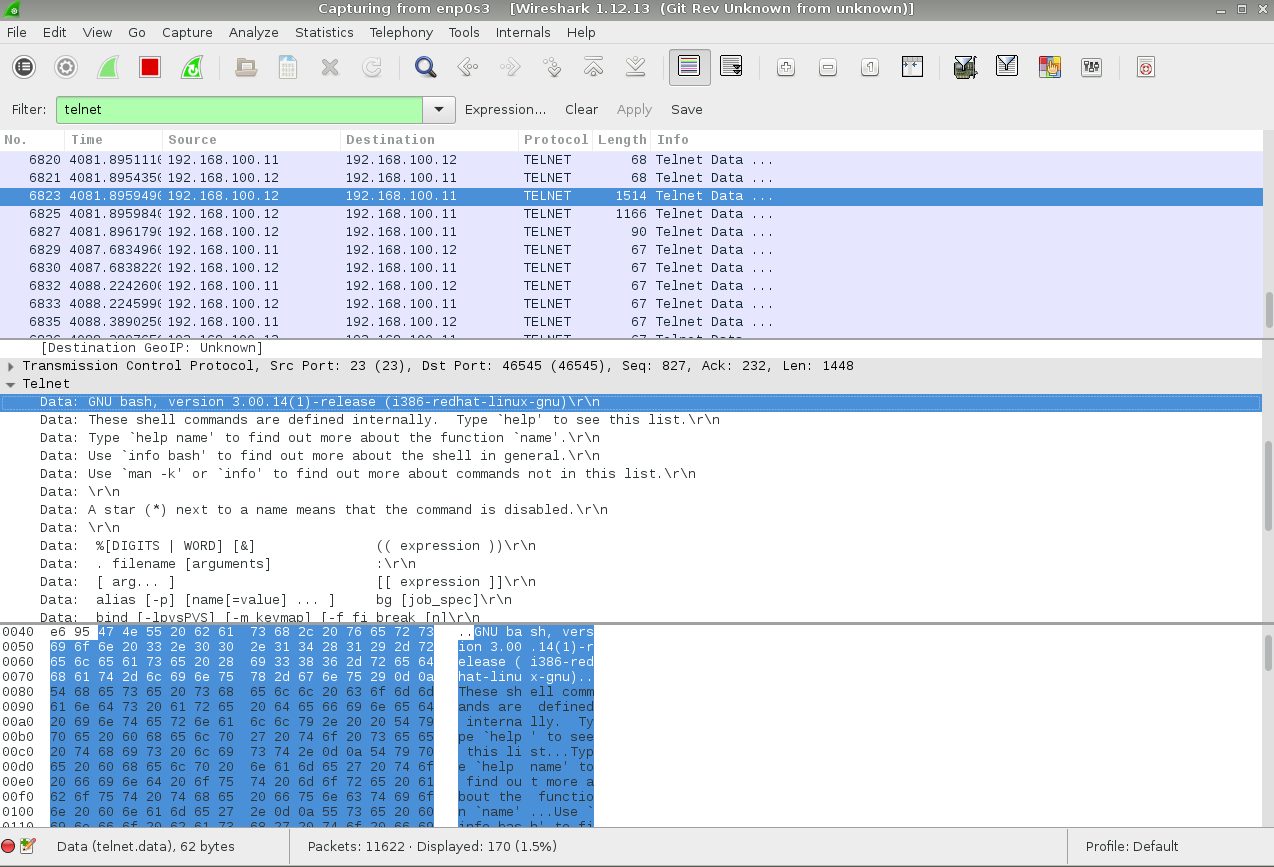


Теперь захватим трафик протокола Telnet



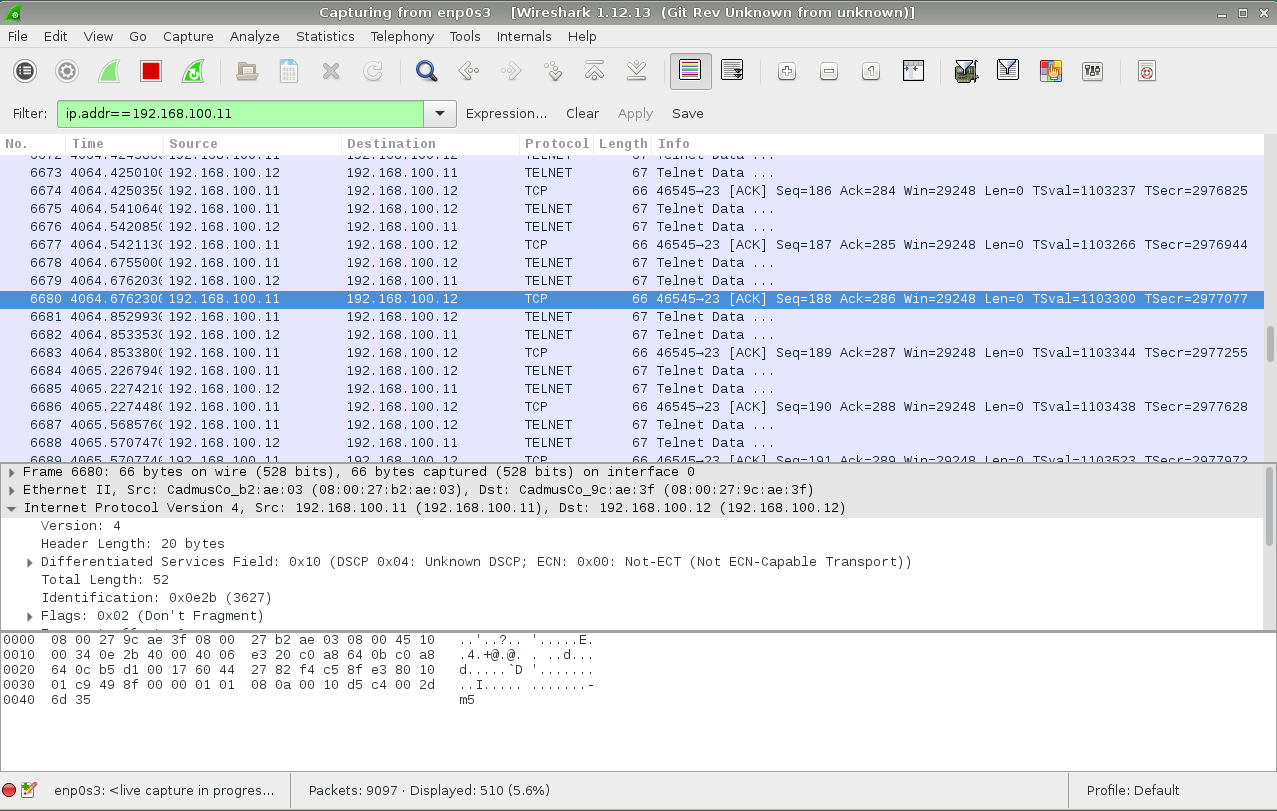


В отличии от SSH , telnet не шифрует данные , поэтому мы можем спокойно получить пароль и логин.

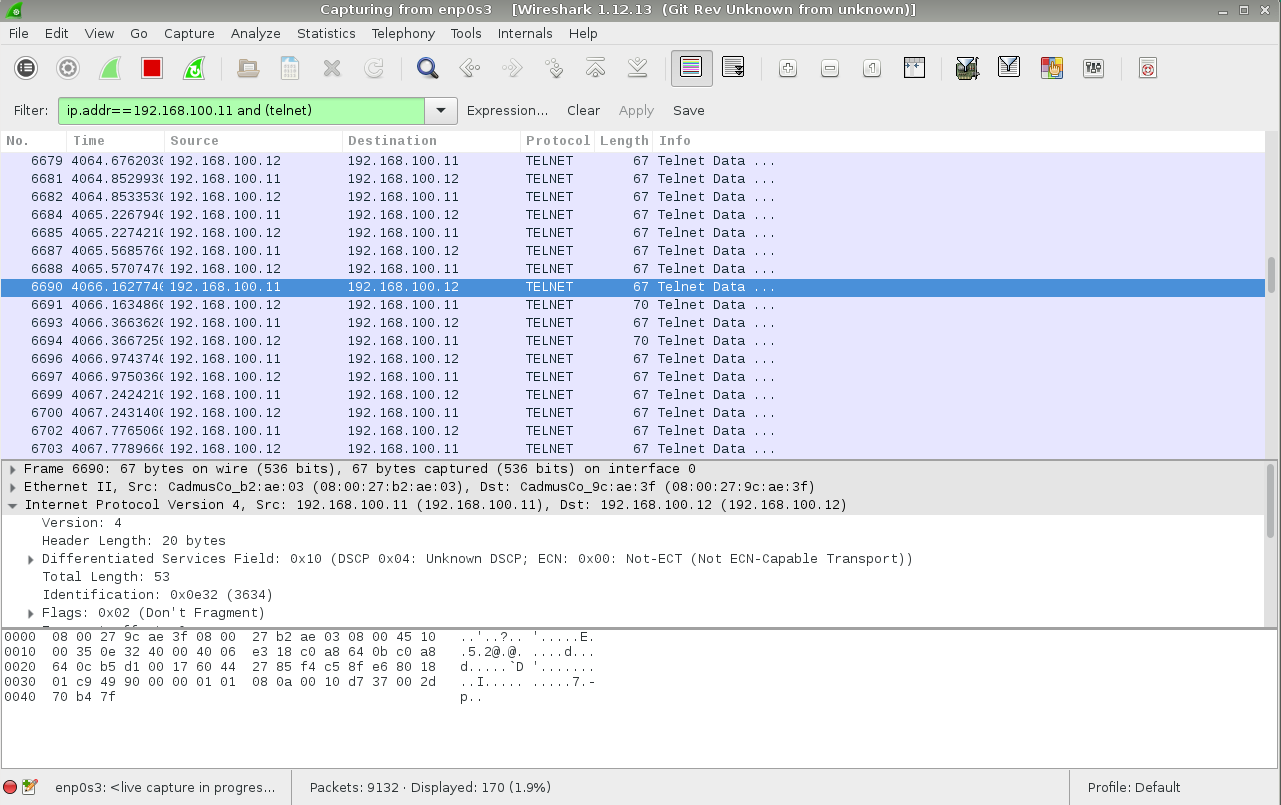


Так же мы спокойно видим всё что вводится в консоль. Например , тут мы видим что я запросил справку по команде .

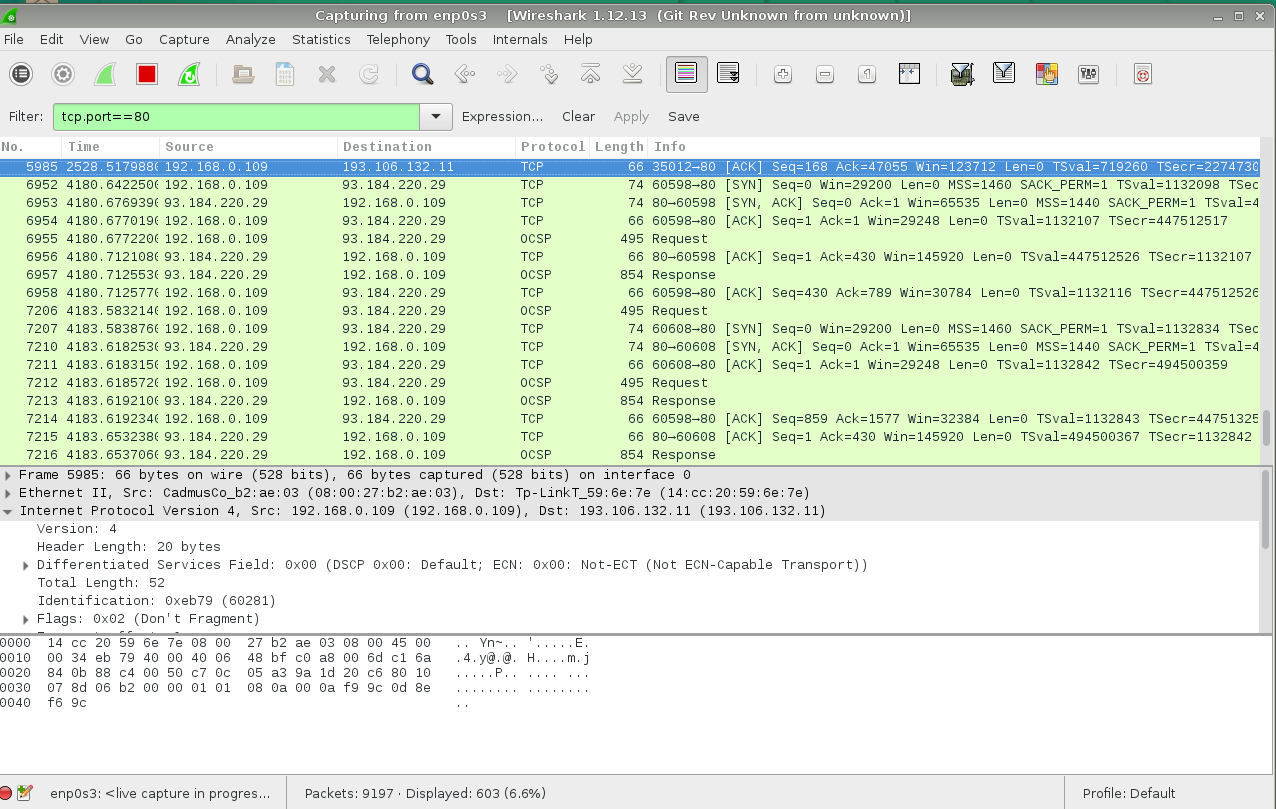
Пример различных фильтров.



Находим все пакеты содержащие нужный IP.



Теперь мы захватываем весь трафик адреса 192.168.100.11 и хотим чтобы нам отображались только пакеты относящиеся к протоколу telnet.



Отображаем весь трафик исходящий от порта 80 (HTTP).