Лабораторная работа

1. Мониторинг с помощью сниффера Wireshark

Wireshark – программа-анализатор трафика для компьютерных сетей Ethernet и некоторых других.

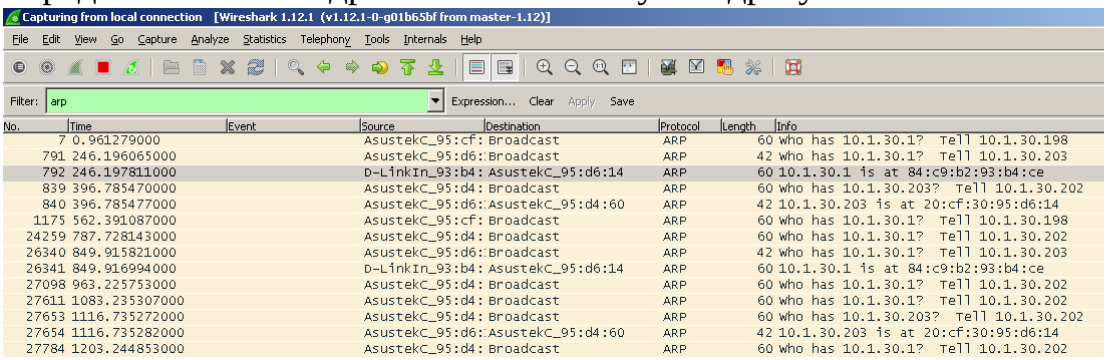
Это приложение, которое «знает» структуру самых различных сетевых протоколов, и поэтому позволяет разобрать сетевой пакет, отображая значение каждого поля протокола любого уровня.

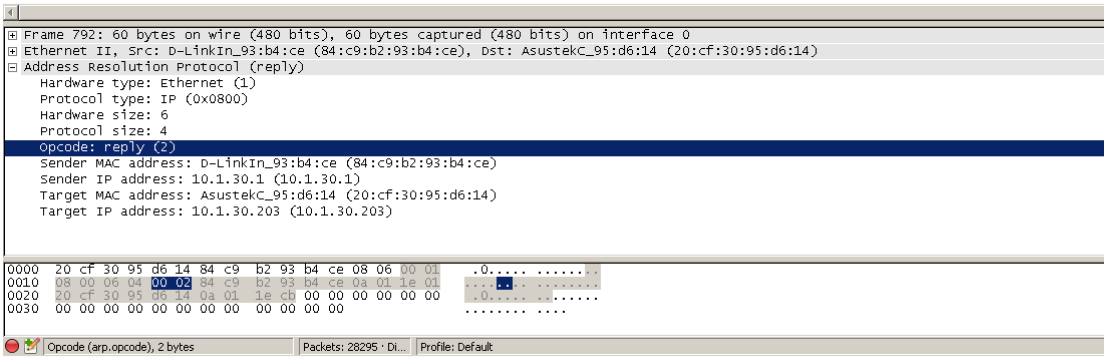
Цель: ознакомиться с работой программы Wireshark, найти и проанализировать посылаемые запросы. Научиться составлять фильтры.

Найти следующие протоколы:

1.1 ARP;

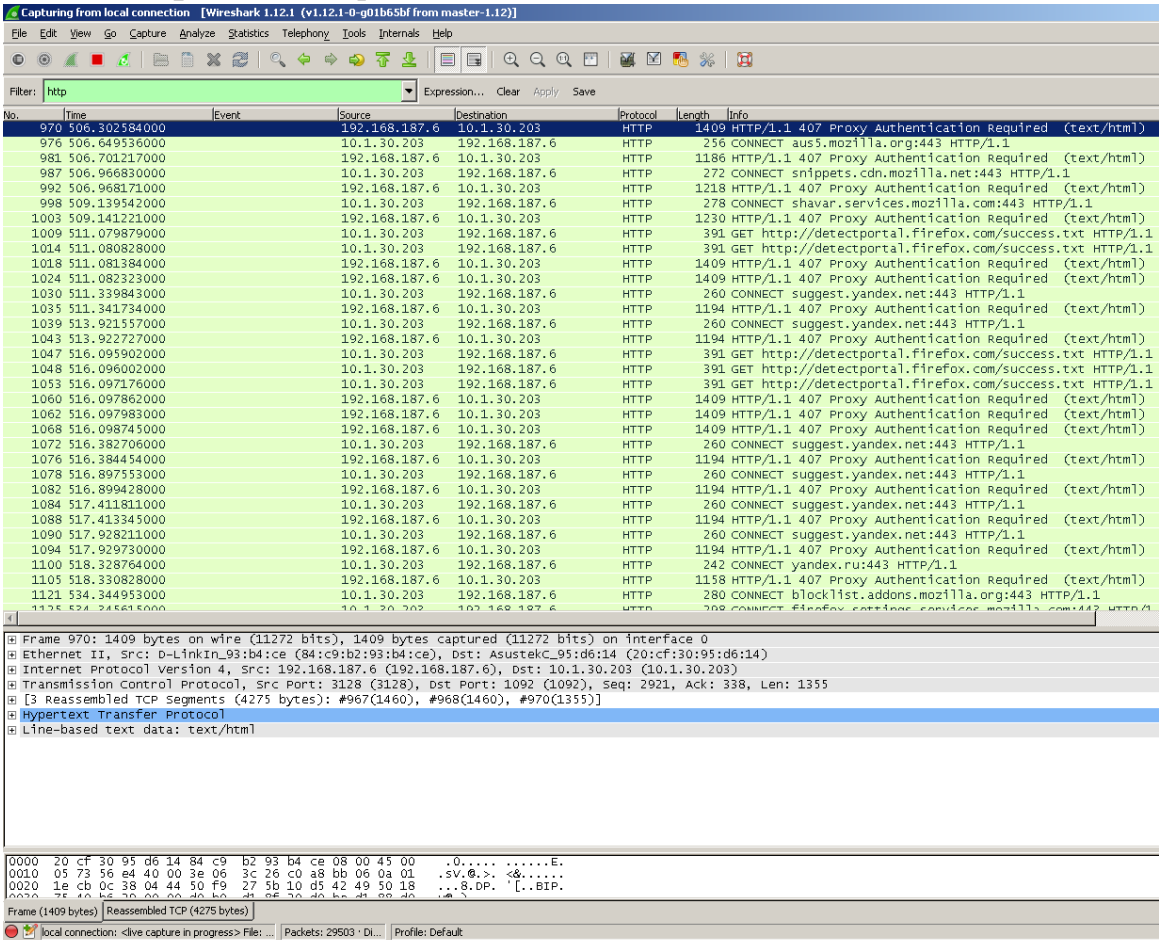
ARP — **протокол** в компьютерных сетях, предназначенный для определения MAC-адреса по известному IP-адресу



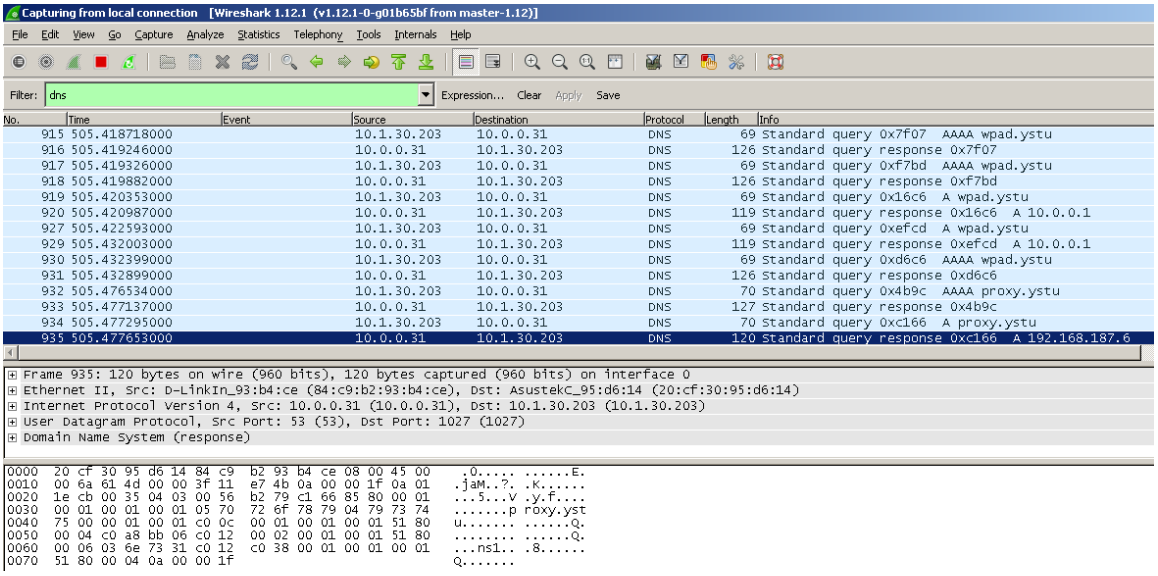


1.2 HTTP (запрос и ответ);

HTTP —протокол передачи данных.

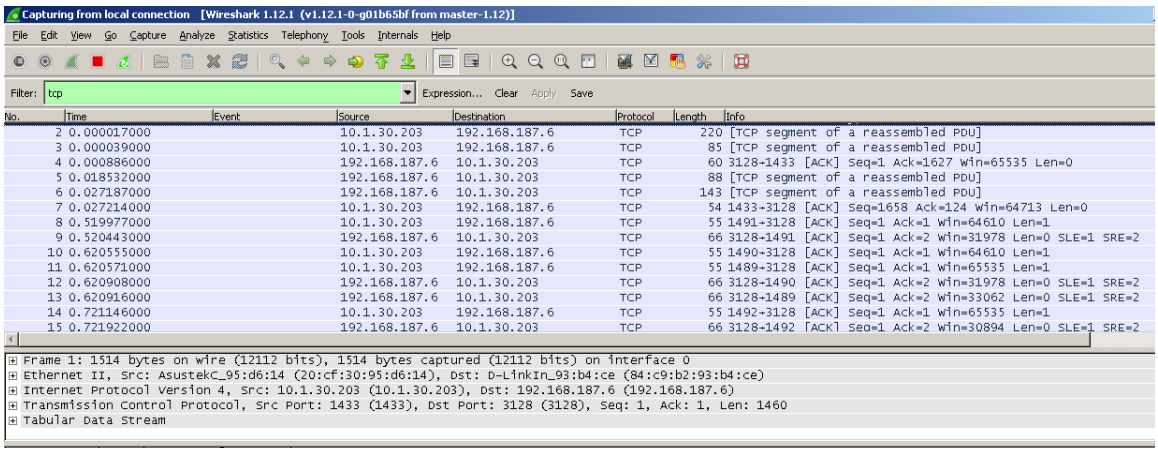


1.3 DNS;



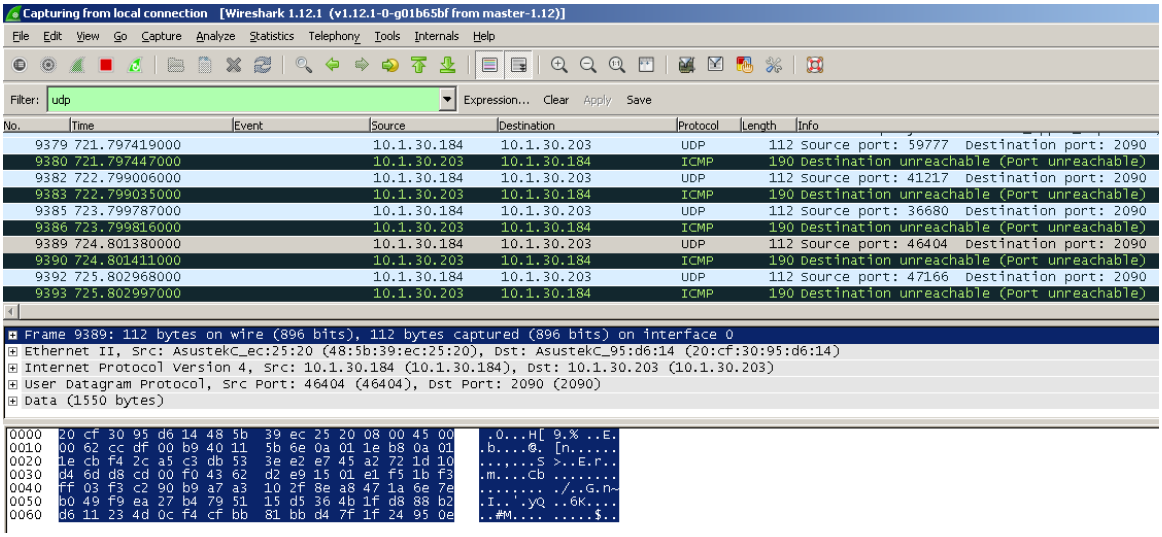
1.4 TCP;

TCP - это протокол транспортного уровня, предоставляющий транспортировку (передачу) потока данных, с необходимостью предварительного установления соединения, благодаря чему гарантирует уверенность в целостности получаемых данных, также выполняет повторный запрос данных в случае потери данных или искажения.



1.5 UDP

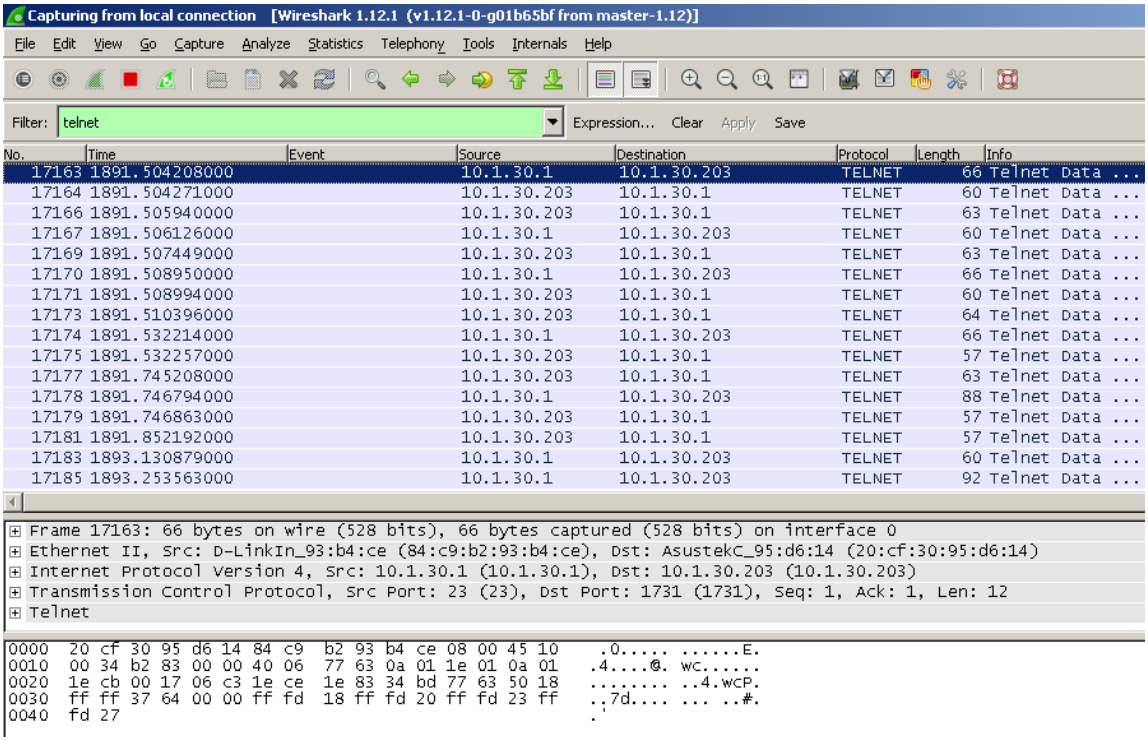
UDP это протокол транспортного уровня стека протоколов TCP/IP. В отличие от TCP протокол UDP надежные доставки данных не обеспечивает.



1.6 Telnet;

Telnet — это текстовый сетевой протокол, который позволяет клиенту общаться с удаленным компьютером.

Для отправления сообщений по протоколу Telnet используйте утилиту Telnet



Найти и разобрать протоколы утилит:

2.1 ping; (изучить протокол ICMP)