Министерство науки и высшего образования Российской Федерации
Мытищинский филиал
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Московский государственный технический университет
имени Н.Э. Баумана
(национальный исследовательский университет)»
(МГТУ им. Н.Э. Баумана)

ФАКУЛЬТЕТ Космический
КАФЕДРА «Прикладная математика, информатика и вычислительная техника» КЗ-МФ

Лабораторная работа №1

ПО ДИСЦИПЛИНЕ:

Сети ЭВМ и телекоммуникации

НА ТЕМУ:

Изучение программ перехвата трафика компьютерной сети на примере Wireshark

Студент КЗ-66Б _____ Чернов Владислав Дмитриевич
(Группа) (Подпись, дата) (И.О.Фамилия)

Студент КЗ-66Б _____ Братов Аким Романович
(Группа) (Подпись, дата) (И.О.Фамилия)

Преподаватель _____ Гизбрехт Иван Иванович
(Подпись, дата) (И.О.Фамилия)

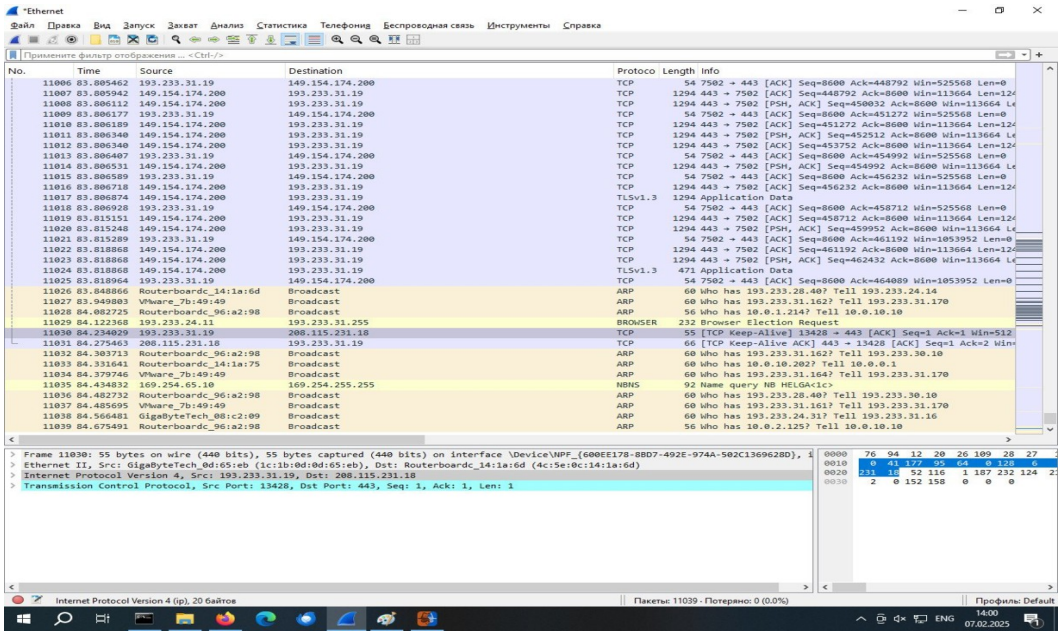
2025 г.

Задание на лабораторную работу

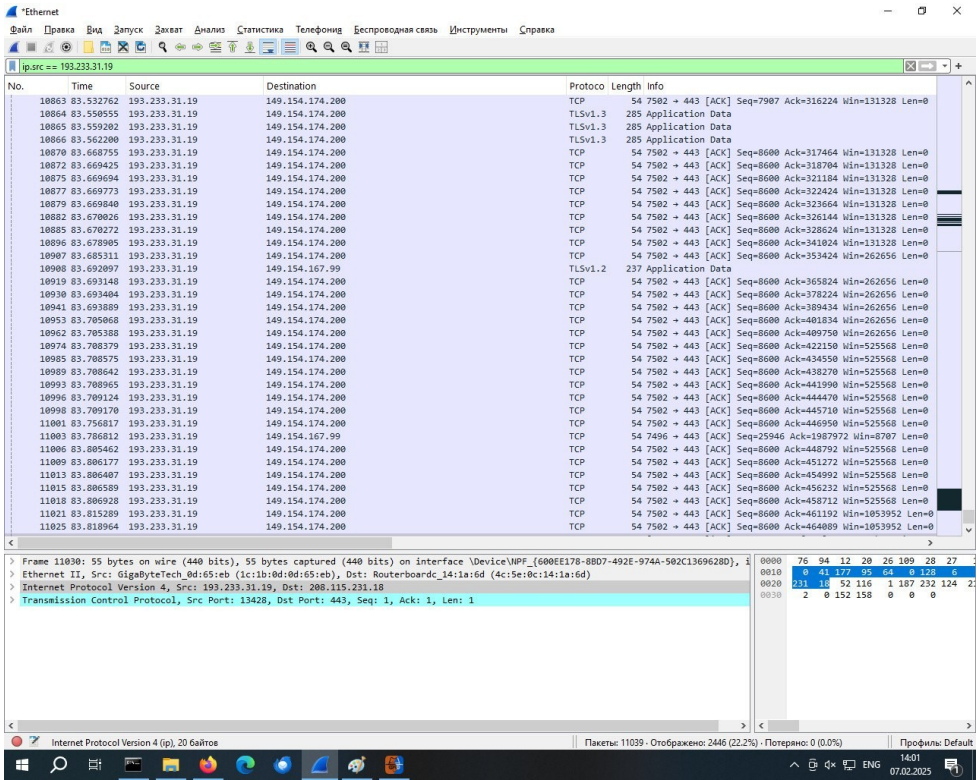
1. Запустить перехват кадров Ethernet по сети и остановите перехват, когда список перехваченных пакетов станет достаточно большой.
2. Попробовать применить фильтр к списку пакетов, введя в строку описания фильтра, например, IP-адрес шлюза или Вашего ПК, или название сетевого протокола (ARP, ICMP, TCP и др.)
3. Попробовать усложнить фильтрацию перехваченных пакетов, применяя операторы языка описания фильтров Wireshark.
4. Ознакомиться с функцией Wireshark Информация эксперта (Expert Info).
5. Попробовать перехват трафика при помощи программы Tshark.

Выполнение

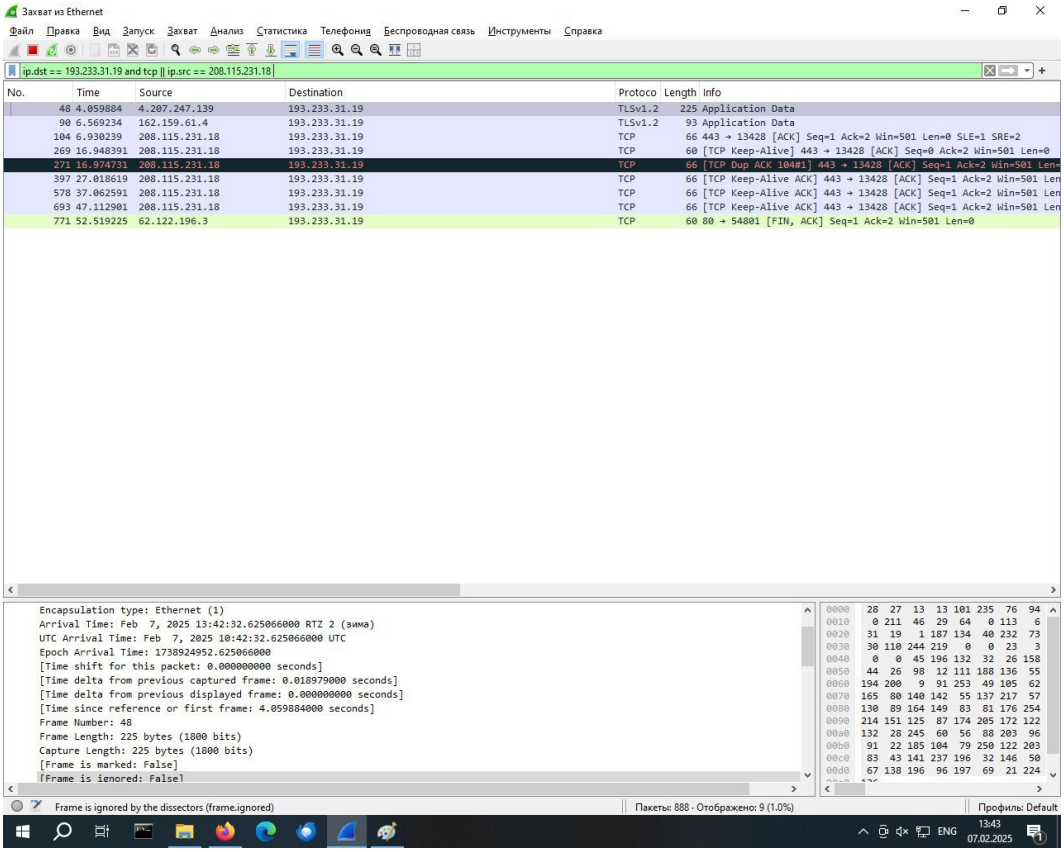
1) Выполняем перехват и останавливаем его, нажатием на красный квадрат, когда список стал достаточно большим



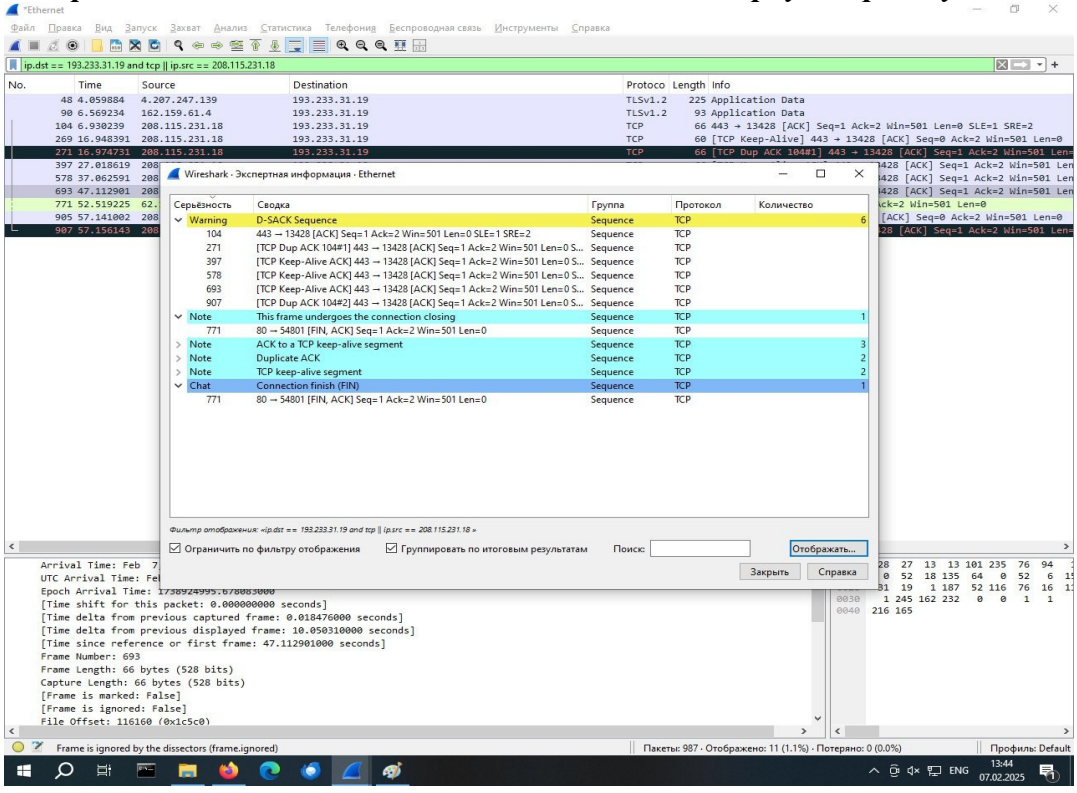
2) Фильтрируем. Указываем, что нужно отобразить всё, что связано с определённым ip-адресом источника и всё, что связано с протоколом tcp, который предназначен для обеспечения надёжной передачи данных между процессами, выполняемыми на компьютере.



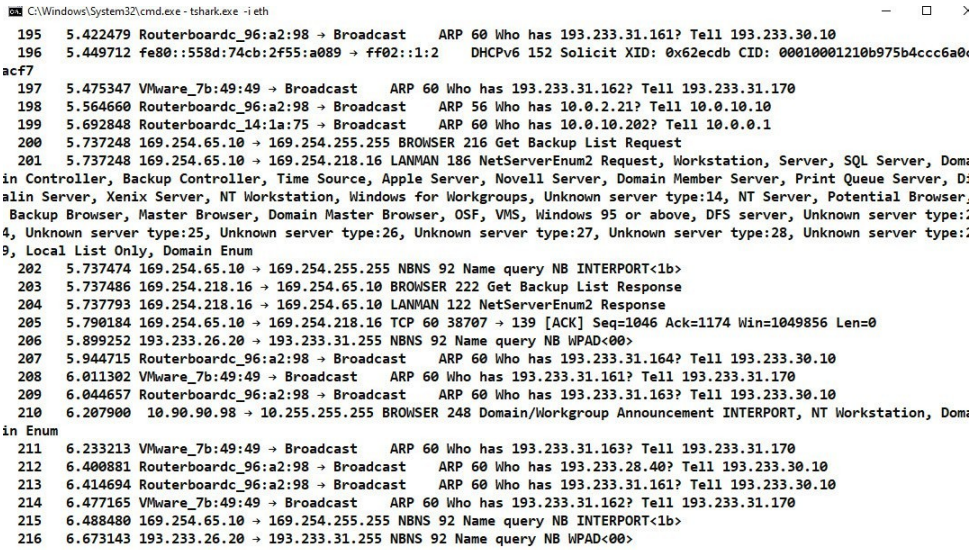
3) *В данном примере применяется фильтр, который показывает только те пакеты которые имеют ip- адрес источника 208.115.23.18 либо ip-адрес назначения 193.233.31.19.*



4)*С помощью информации эксперта(Expert Info) можно узнать подробнее о состоянии каждого пакета и выявлять сетевые проблемы. Например: если в разделе warning колонка сводки содержит [TCP Dup ACK], то это может свидетельствовать о потерянных или задержанных пакетах, что часто вызывает повторную передачу данных.*



5) Tshark позволяет просматривать и анализировать весь проходящий по сети трафик в режиме реального времени через консоль. Чтобы запустить программу необходимо перейти в директорию в которой находится исполняемый файл и написать команду tshark.exe -i .



Ответы на вопросы

- **Что представляет собой программа Wireshark ?**

  Wireshark (ранее называлась — Ethereal) — программа-анализатор трафика для компьютерных сетей

- **К какому классу программ относятся Wireshark, TShark и Sniffnet ?**

  Программа принадлежит к классу программ — снифферы (Sniffer).

- **Для чего предназначены программы типа Wireshark, Tshark и Sniffnet ?**

  Программы-снифферы позволяют пользователю просматривать и анализировать весь проходящий по сети трафик в режиме реального времени.

- **Для каких прикладных целей можно использовать программы типа Wireshark, Tshark и Sniffnet ?**

  1. *Исследование локальной сети, ее параметров, состава оборудования и т.д.*
  2. *Изучение работы сетевых протоколов разных уровней Эталонной модели взаимодействия открытых систем (ЭМВОС), структуры и заголовков пакетов данных*
  3. *Поиск неполадок в сети (неисправное или неправильно настроенное оборудование, закольцовки в сети и т.д.)*
  4. *Поиск источников хакерских атак или зараженных вирусами компьютеров*
  5. *Для хакерских целей (например, перехват паролей и др. конфиденциальных данных, передаваемых по сети. (Но тут следует заметить, что в последнее время пароли почти никогда не передаются по сети в незашифрованном виде, и больше половины сайтов работают с шифрованием по протоколам SSL/TLS)*

- ***В каких случаях вместо снифферов с графическим интерфейсом лучше использовать снифферы командной строки (например, TCPDump или TShark)?***

Использование снифферов комманндной строки лучше использовать в следующих случаях:

1. Если нужно анализировать трафик в условиях ограниченных ресурсов.
2. При подключении к удаленному серверу без графической оболочки по SSH.
3. При написании скриптов.