



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
(Группа)

(Подпись, дата)

Чернов Владислав Дмитриевич
(И.О.Фамилия)

Студент КЗ-66Б
(Группа)

(Подпись, дата)

Братов Аким Романович
(И.О.Фамилия)

Преподаватель

(Подпись, дата)

Гизбрехт Иван Иванович
(И.О.Фамилия)

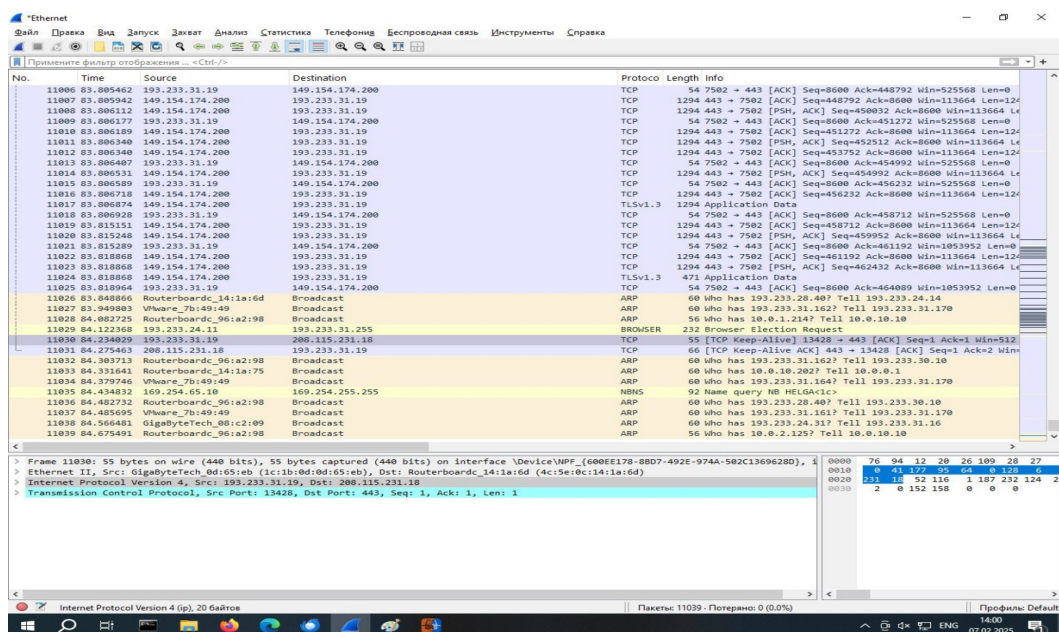
2025 г.

Задание на лабораторную работу

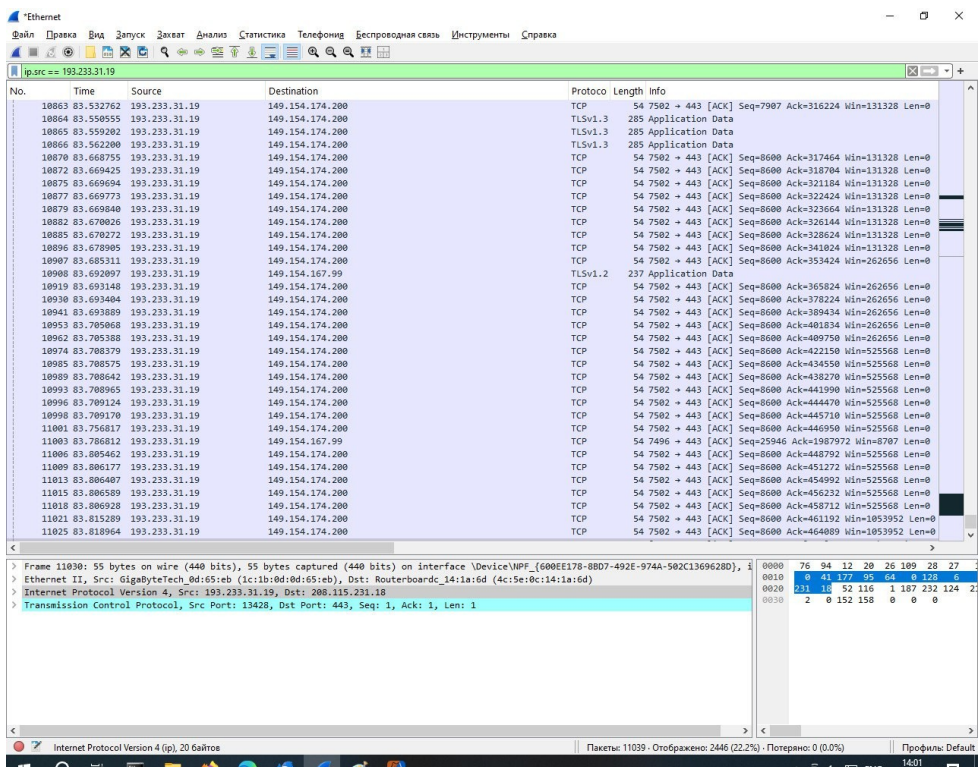
1. Запустить перехват кадров Ethernet по сети и остановить перехват, когда список перехваченных пакетов станет достаточно большой.
2. Попробовать применить фильтр к списку пакетов, введя в строку описания фильтра, например, IP-адрес шлюза или Вашего ПК, или название сетевого протокола (ARP, ICMP, TCP 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

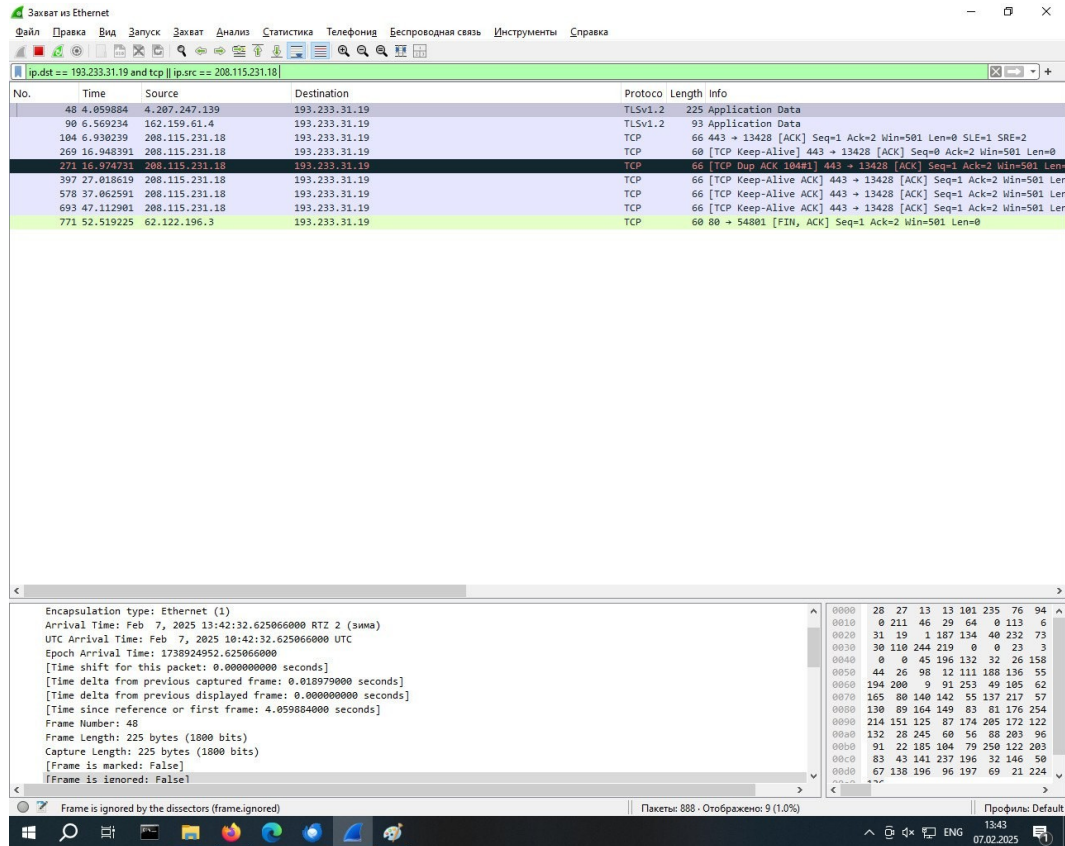
- 1) Выполняем перехват и останавливаем его, нажатием на красный квадрат, когда список стал достаточно большим



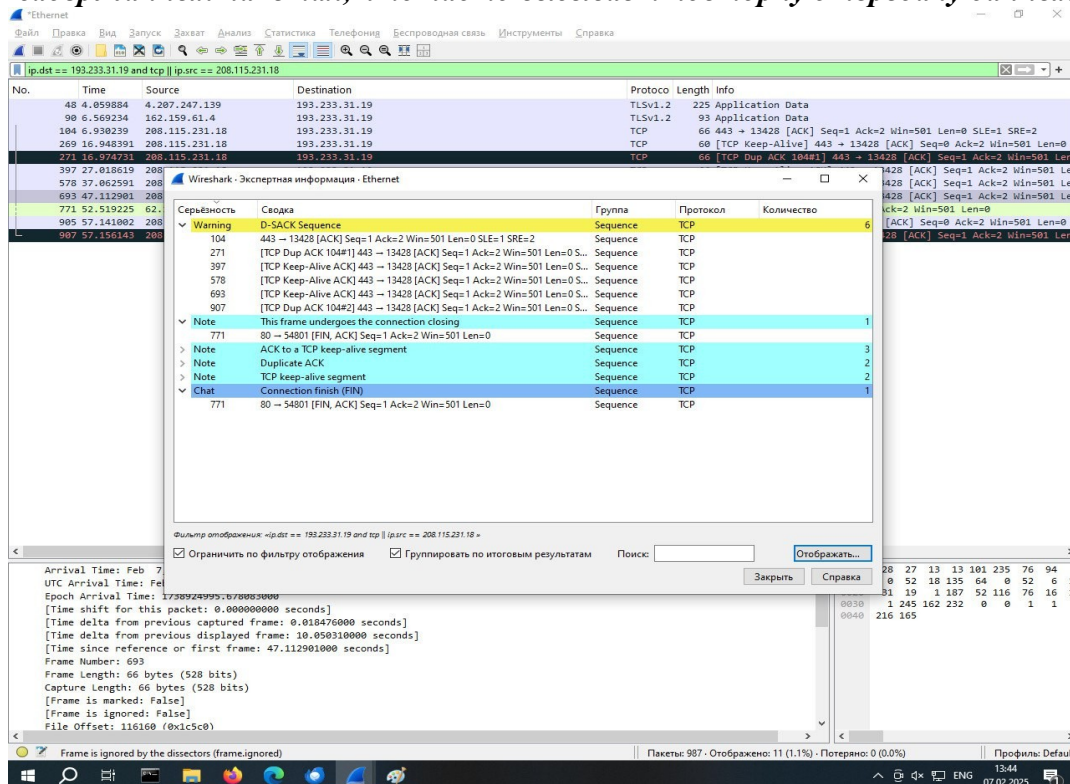
- 2) Фильтруем. Указываем, что нужно отобразить всё, что связано с определённым ip-адресом источника и всё, что связано с протоколом tcp, который предназначен для обеспечения надёжной передачи данных между процессами, выполняемыми на компьютере.



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`.

```
C:\Windows\System32\cmd.exe - tshark.exe -i eth
195 5.422479 Routerboardc_96:a2:98 → Broadcast ARP 60 Who has 193.233.31.161? Tell 193.233.30.10
196 5.449712 fe80::558d:74cb:2f55:a089 → ff02::1:2 DHCPv6 152 Solicit XID: 0x62ecdb CID: 00010001210b975b4ccc6a0
acff7
197 5.475347 VMware_7b:49:49 → Broadcast ARP 60 Who has 193.233.31.162? Tell 193.233.31.170
198 5.564660 Routerboardc_96:a2:98 → Broadcast ARP 56 Who has 10.0.2.21? Tell 10.0.10.10
199 5.692848 Routerboardc_14:1a:75 → Broadcast ARP 60 Who has 10.0.10.202? Tell 10.0.0.1
200 5.737248 169.254.65.10 → 169.254.255.255 BROWSER 216 Get Backup List Request
201 5.737248 169.254.65.10 → 169.254.218.16 LANMAN 186 NetServerEnum2 Request, Workstation, Server, SQL Server, Dom
in Controller, Backup Controller, Time Source, Apple Server, Novell Server, Domain Member Server, Print Queue Server, D
alin Server, Xenix Server, NT Workstation, Windows for Workgroups, Unknown server type:14, NT Server, Potential Browser,
Backup Browser, Master Browser, Domain Master Browser, OSF, VMS, Windows 95 or above, DFS server, Unknown server type:
4, Unknown server type:25, Unknown server type:26, Unknown server type:27, Unknown server type:28, Unknown server type:
9, Local List Only, Domain Enum
202 5.737474 169.254.65.10 → 169.254.255.255 NBNS 92 Name query NB INTERPORT<1b>
203 5.737486 169.254.218.16 → 169.254.65.10 BROWSER 222 Get Backup List Response
204 5.737793 169.254.218.16 → 169.254.65.10 LANMAN 122 NetServerEnum2 Response
205 5.790184 169.254.65.10 → 169.254.218.16 TCP 60 38707 → 139 [ACK] Seq=1046 Ack=1174 Win=1049856 Len=0
206 5.899252 193.233.26.20 → 193.233.31.255 NBNS 92 Name query NB WIPAD<00>
207 5.944715 Routerboardc_96:a2:98 → Broadcast ARP 60 Who has 193.233.31.164? Tell 193.233.30.10
208 6.011302 VMware_7b:49:49 → Broadcast ARP 60 Who has 193.233.31.161? Tell 193.233.31.170
209 6.044657 Routerboardc_96:a2:98 → Broadcast ARP 60 Who has 193.233.31.163? Tell 193.233.30.10
210 6.207900 10.90.90.98 → 10.255.255.255 BROWSER 248 Domain/Workgroup Announcement INTERPORT, NT Workstation, Dom
in Enum
211 6.233213 VMware_7b:49:49 → Broadcast ARP 60 Who has 193.233.31.163? Tell 193.233.31.170
212 6.400881 Routerboardc_96:a2:98 → Broadcast ARP 60 Who has 193.233.28.40? Tell 193.233.30.10
213 6.414694 Routerboardc_96:a2:98 → Broadcast ARP 60 Who has 193.233.31.161? Tell 193.233.30.10
214 6.477165 VMware_7b:49:49 → Broadcast ARP 60 Who has 193.233.31.162? Tell 193.233.31.170
215 6.488480 169.254.65.10 → 169.254.255.255 NBNS 92 Name query NB INTERPORT<1b>
216 6.673143 193.233.26.20 → 193.233.31.255 NBNS 92 Name query NB WIPAD<00>
```

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 — sniffеры (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 sniffеров с графическим интерфейсом лучше использовать sniffеры командной строки (например, TCPDump или TShark)?**

Использование sniffеров командной 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.