|  |  |
| --- | --- |
|  | **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» К3-МФ

**Лабораторная работа №1**

*ПО ДИСЦИПЛИНЕ:*

***Сети ЭВМ и телекоммуникации***

***НА ТЕМУ:***

***\_\_\_\_\_\_\_\_Изучение программ перехвата трафика\_\_\_\_\_\_\_***

***\_\_\_\_\_\_\_\_\_\_\_компьютерной сети на примере\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Wireshark\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***

Студент \_\_К3-63Б\_\_  **\_\_\_\_\_\_\_\_\_\_** Цветков Юрий Алексеевич

(Группа) (Подпись, дата) (И.О.Фамилия)

Студент \_\_К3-63Б\_\_  **\_\_\_\_\_\_\_\_\_\_** Тимофеев Юрий Алексеевич

(Группа) (Подпись, дата) (И.О.Фамилия)

Преподаватель  **\_\_\_\_\_\_\_\_\_\_\_\_** Гизбрехт Иван Иванович

(Подпись, дата) (И.О.Фамилия)

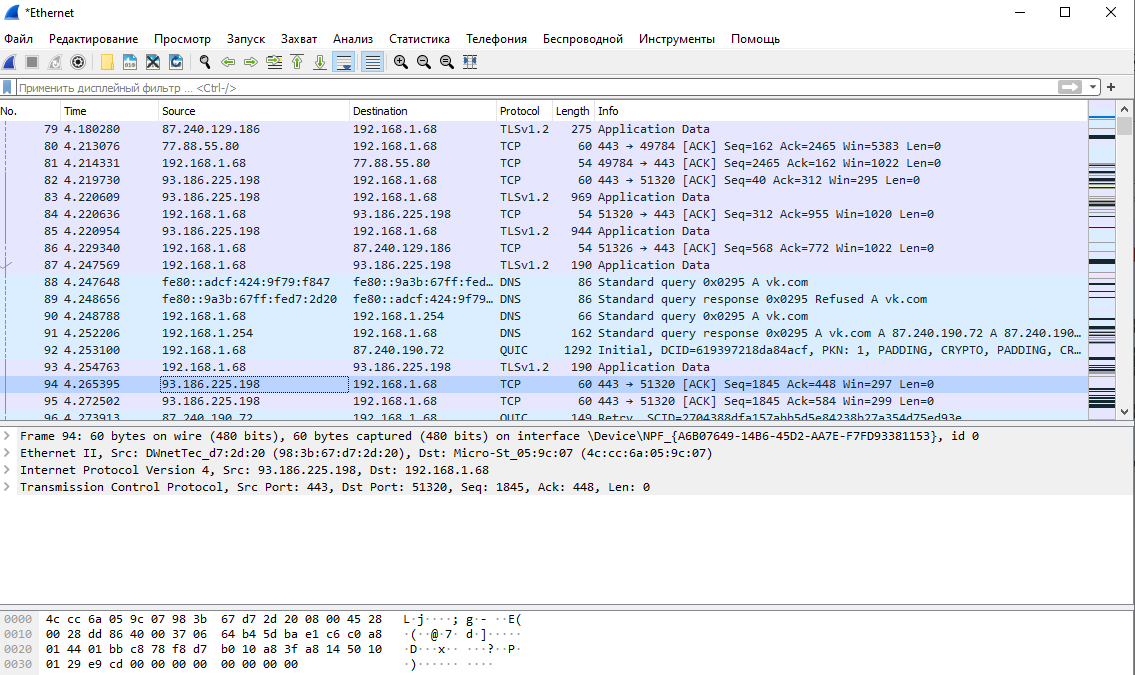
*2022 г.*

***Задание на лабораторную работу***

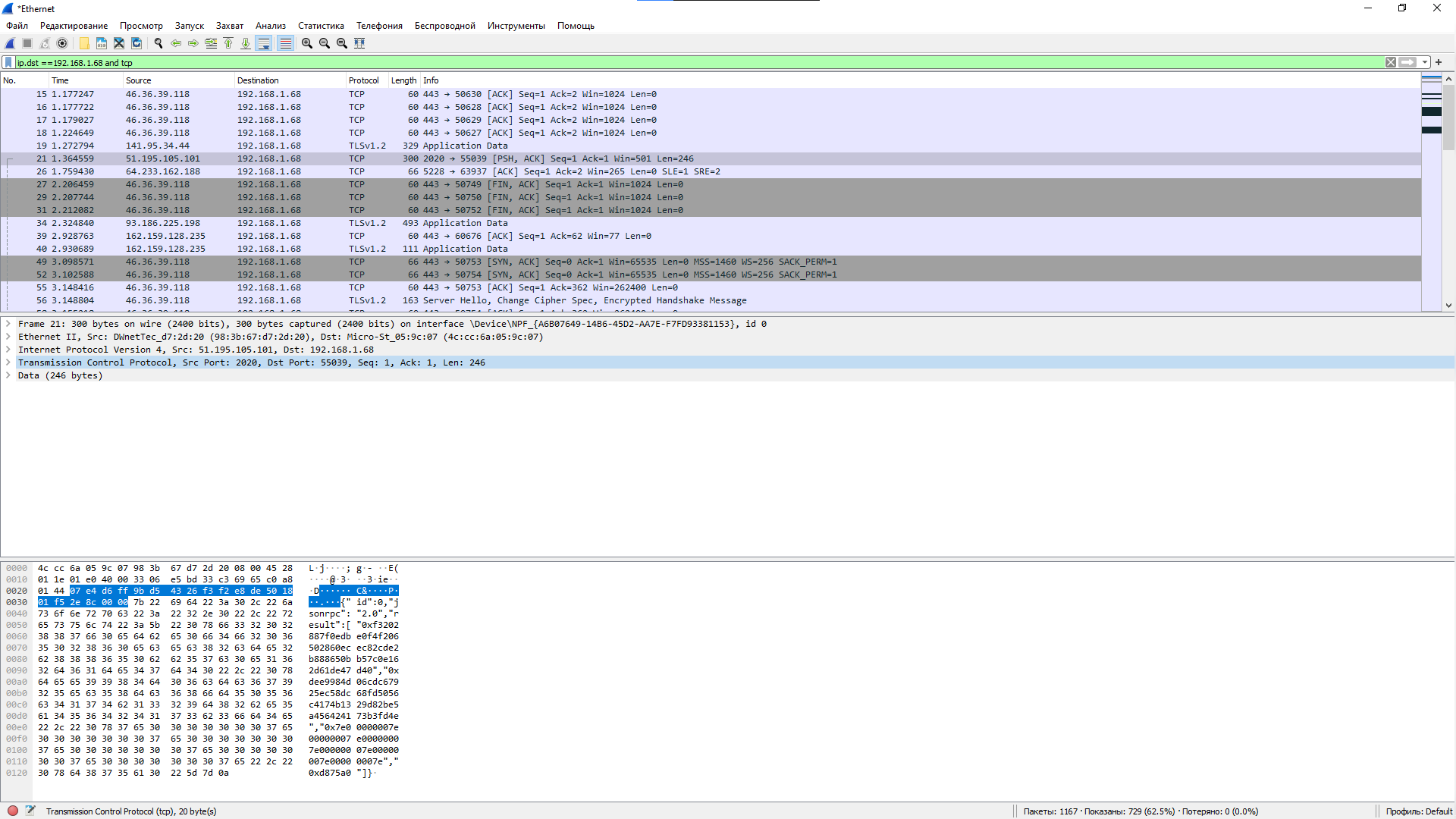
1. Запустить перехват кадров Ethernet по сети и остановите перехват, когда список перехваченных пакетов станет достаточно большой.
2. Применить фильтр к списку пакетов, введя в строку описания фильтра, например, IP-адрес шлюза или Вашего ПК, или название сетевого протокола (ARP, ICMP, TCP и др.)
3. Усложнить фильтрацию перехваченных пакетов, применяя операторы языка описания фильтров Wireshark.

***Выполнение***

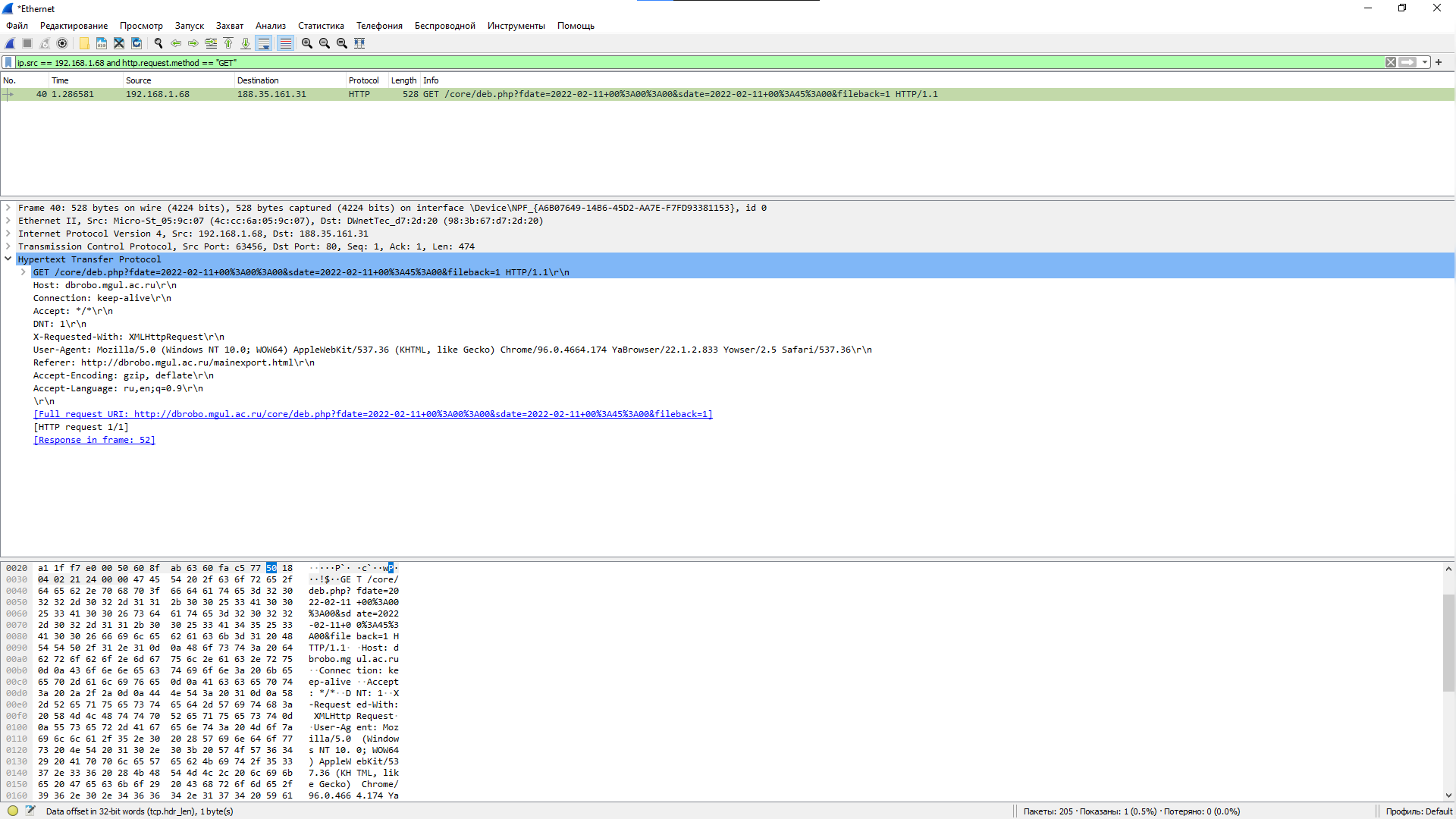
* 1. Выполняем перехват и останавливаем его, нажатием на красный квадрат, когда список стал достаточно большим



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



* 1. ***В данном примере применяется фильтр, который показывает get-запросы сделанные с определённого ip.***

******

***Ответы на вопросы***

* **Что представляет собой программа Wireshark?**

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

* **К какому классу программ относится Wireshark?**

Программа принадлежит к классу программ — снифферы (Sniffer).

* **Для чего предназначены программы типа Wireshark?**

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?**

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)*