**Учреждение образования**

**«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**

**ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ»**

**Кафедра интеллектуальных информационных технологий**

**Лабораторная работа №8 по курсу «СиМЗИИС» на тему:**

**«Наблюдение за стеком TCP/IP»**

Выполнил студент: Исамиддинов Ботир

Группы: ***121731***

Проверил: Сальников Д.А

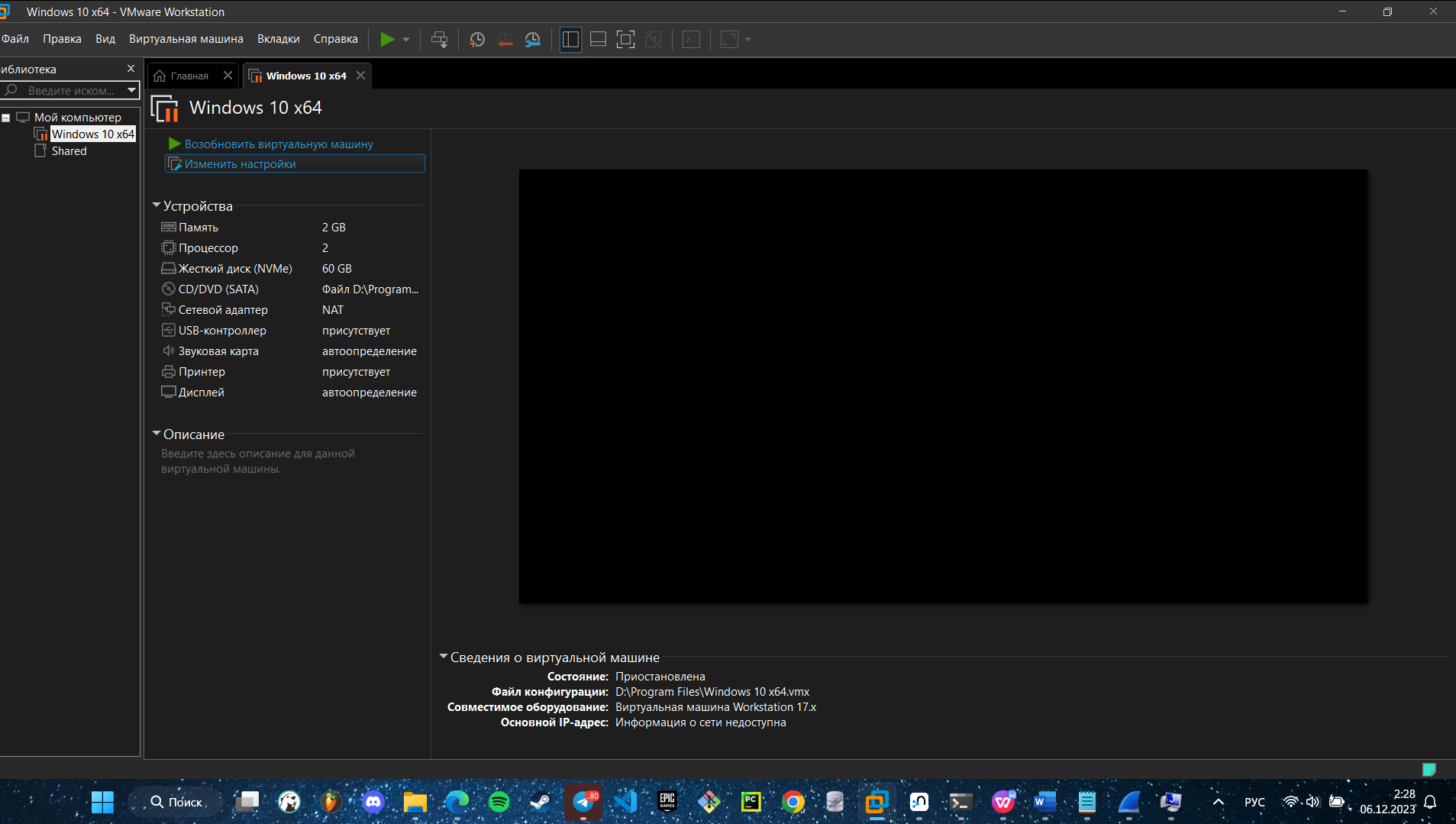
**МИНСК**

2023

**Задание**

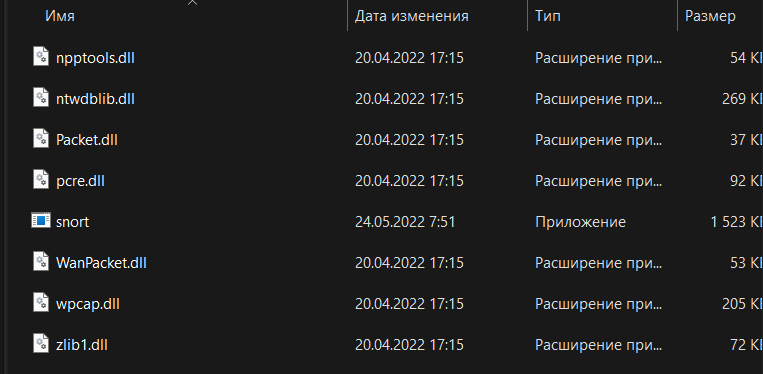
1. На основном компьютере запустить Виртуальную машину. Измените имя компьютера на уникальное.
2. Установить Snort.
3. Запустите Snort в режиме Sniffer пакетов или протоколирования с различными параметрами детализации.
4. Обратитесь к локальной сети. Выполните команду ping, запустите броузер или проводник. Сохраните какой либо файл (не большой) на материнской машине.
5. Остановите Snort. Определите к каким IP-портам и адресам были выполнены обращения.
6. Пользуясь \windows\system32\etc\service, определите какие системные службы использовались.
7. Просмотрите содержимое перехваченных пакетов.
8. **Используя дополнительную литературу расшифруйте содержание вывода заголовка.** Оформите отчет. В отчет обязательно поместите примеры пакетов и список обнаруженных протоколов и служб.

**Задание 1.**

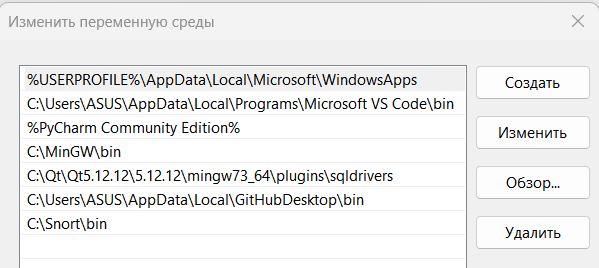
Запуск виртуальной машины 

**Задание 2.**

Установка Snort

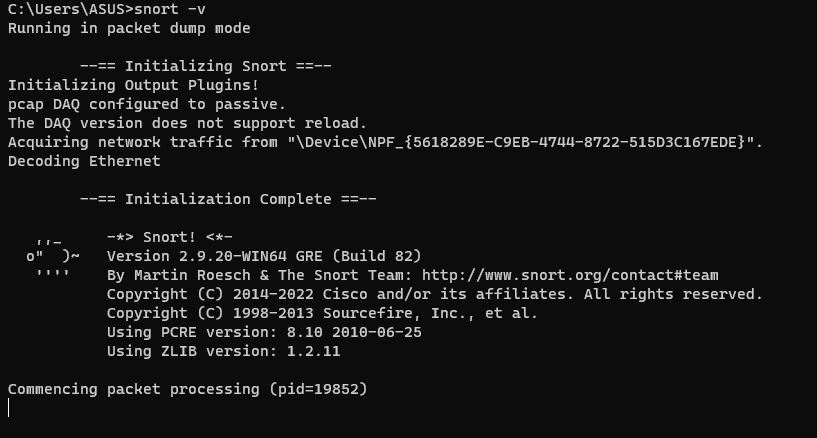


Были установлены программы для работы со snort и сам snort и NpCap



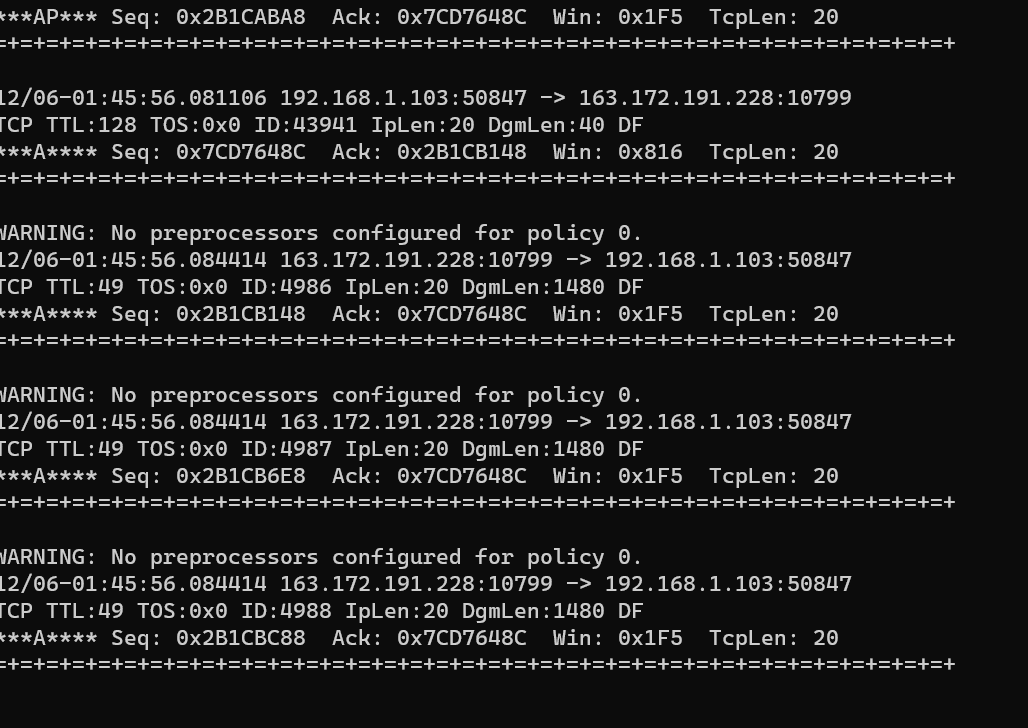
Добавили директорию Snort-а и NpCap в переменные среды Windows чтобы можно было работать с ним на прямую через Командную строку.

**Задание 3**



Запуск snort в режиме sniffer.

**Задание 4**

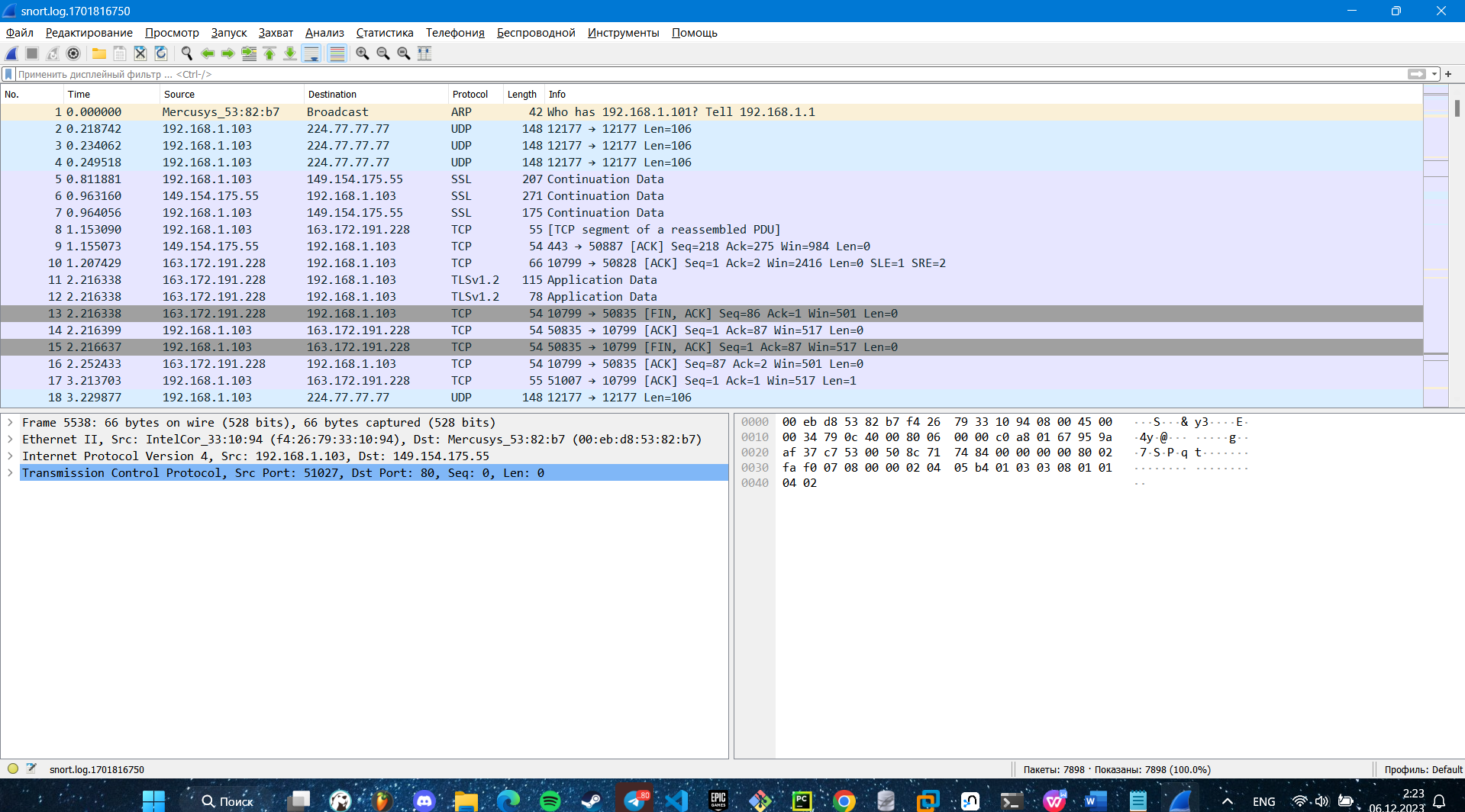


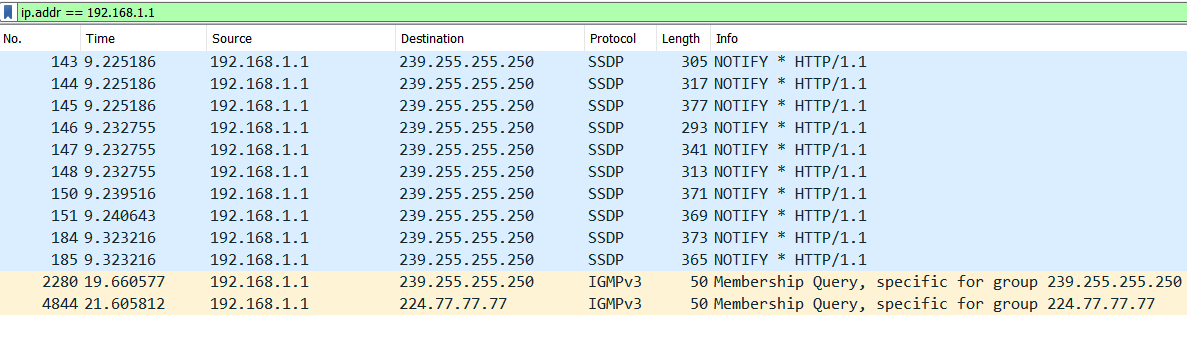
Запуск snort на режиме sniffer через команду snort -v -i 4 -l C:\Snort\log что означает что мы запустили snort на режиме sniffer -v, выбрали интерфейс в нашем случае 4 и записали результат в log – файл

**Задание 5**

Дальше мы переходим в директорию где сохранился log-файл в нашем случае это C:\Snort\log

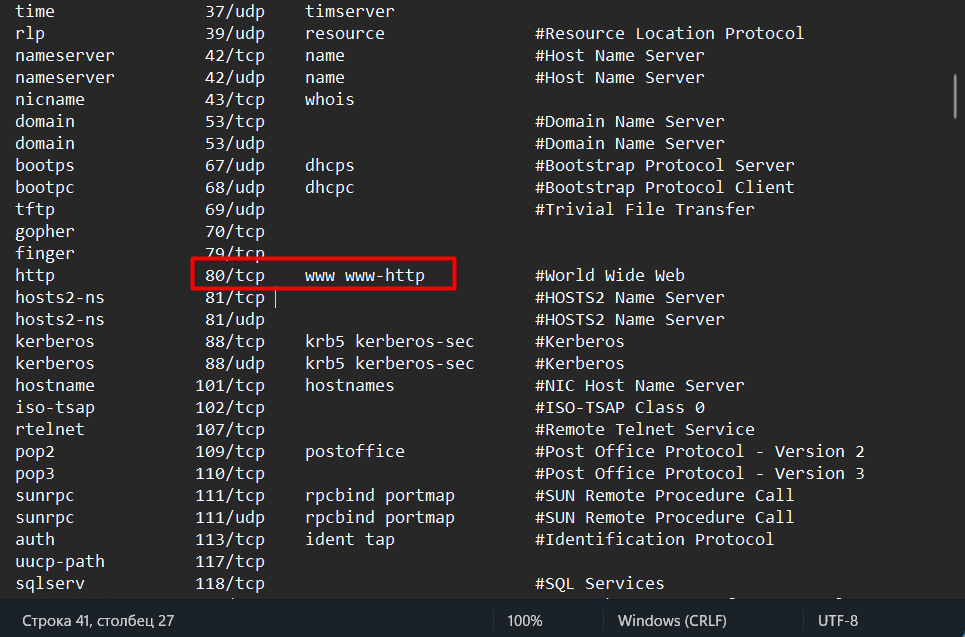
И открываем ее программой Wireshark

При открытии у нас появляется список перехваченных пакетов с запросами, портами и адресами.



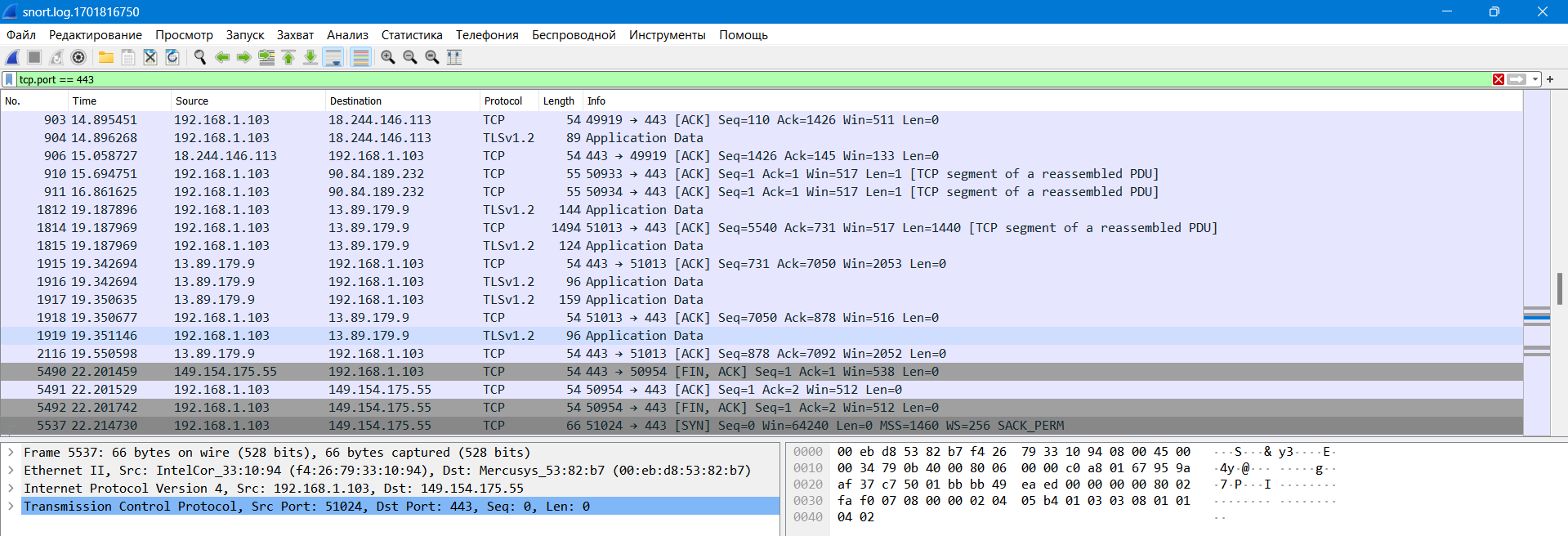
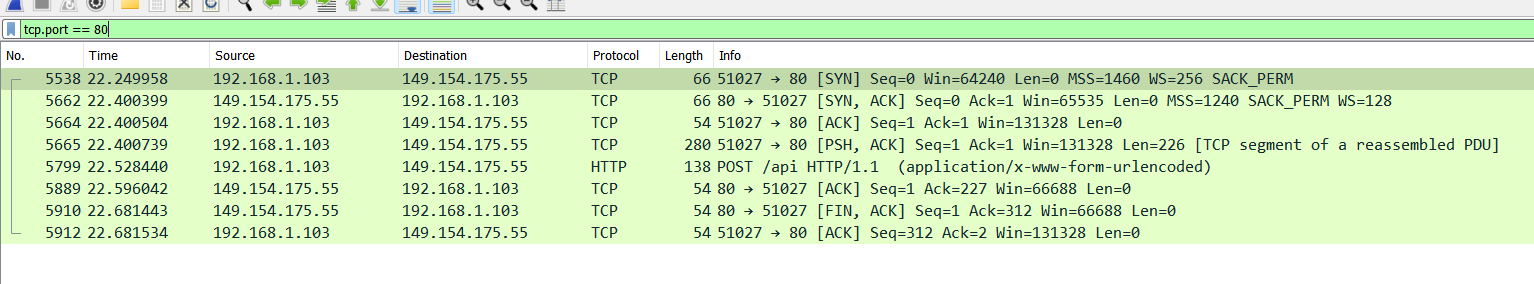
Можно посмотреть какие адреса были задействованы в запуске sniffer

**Задание 6**



Открыв файл services мы обратили внимание на порт 80 и 443 с протоколом tcp

**Задание 7**



Тут видно что был задействован именно этот порт 80 и 443 потому что в процессе sniffer-а мы заходили на сайт youtube.com, что прямиком ссылается на то что был задействован порт 80 и 443, потому что он нужен для обработки http запросов что дает понять что мы пользовались браузером.

**Вывод**

В рамках данного задания была проведена установка и конфигурация сетевого анализатора Snort на виртуальной машине для мониторинга сетевого трафика. Целью эксперимента являлось изучение основ работы с Snort, анализ проходящего сетевого трафика, идентификация активных портов и служб, а также применение полученных знаний для составления детального отчета.

1. Настройка виртуальной машины Виртуальная машина была успешно запущена на хост-компьютере. Имя машины было изменено на "VM-SnortTest" для обеспечения уникальности в сетевой среде.

2. Установка Snort Snort был установлен на виртуальную машину с использованием официального дистрибутива для Windows. Конфигурация была выполнена согласно рекомендациям из официальной документации Snort.

3. Запуск Snort Snort был запущен в режиме сниффера с различными уровнями детализации вывода. Для мониторинга использовался сетевой интерфейс, соответствующий локальной сети виртуальной машины.

4. Активность в локальной сети С хост-компьютера были выполнены следующие действия для генерации трафика: выполнение команды ping до виртуальной машины, использование веб-браузера для доступа к внешним ресурсам, и сохранение тестового файла в общем сетевом ресурсе.

5. Анализ трафика После остановки Snort был проанализирован лог-файл для идентификации активных IP-адресов и портов. Были обнаружены обращения к внешним веб-сайтам на стандартные порты HTTP (80) и HTTPS (443), а также внутренние обращения в сети на порт ICMP (протокол пинга).

6. Использование системных служб Сопоставление зафиксированных портов с файлом services позволило установить, что использовались следующие службы: HTTP (80), HTTPS (443) и служба удаленного доступа (ICMP).

7. Просмотр содержимого пакетов Содержимое перехваченных пакетов было просмотрено с использованием Wireshark, где были детально расшифрованы заголовки и содержание данных в пакетах.

8. Расшифровка заголовков Заголовки пакетов были проанализированы, и для каждого поля заголовка было дано объяснение его значения и роли в протоколе.

Примеры пакетов:

* Пакет TCP на порту 443 с флагами [SYN], обозначающий начало TCP-сессии.
* Пакет ICMP с типом 8, кодом 0, обозначающий запрос эхо (ping). Пакет HTTP на порту 80 с GET-запросом для загрузки веб-страницы.
* **Список обнаруженных протоколов и служб:**
* **HTTP (80)**: Протокол прикладного уровня для передачи гипертекстовых документов. Используется веб-браузерами и серверами для обмена веб-страницами и другими данными.
* **HTTPS (443)**: Расширение HTTP, поддерживающее шифрование для повышения безопасности данных. Используется для защищенных транзакций, таких как онлайн-банкинг и торговля.
* **ICMP (протокол пинга)**: Используется для отправки сообщений об ошибках и операционных запросов, например, для проверки доступности хостов с помощью команды ping.
* **Расшифровка содержания вывода заголовка:**
* **IP-адрес источника и назначения**: Указывает, откуда и куда отправляется пакет.
* **Порт источника и назначения**: Указывают на приложение или службу, которая используется для обмена данными.
* **Флаги TCP**: Например, флаг [SYN] используется для инициализации соединения TCP, а флаг [ACK] подтверждает получение пакета.
* **Тип и код ICMP**: Указывают на тип запроса или ответа ICMP; тип 8 и код 0 обозначают запрос эхо.

**Заключение**

Анализ сетевого трафика с использованием Snort и Wireshark позволил выявить активные сетевые соединения и использование стандартных сетевых служб. Расшифровка заголовков пакетов дала понимание протоколов и механизмов обмена данными в сети. Этот опыт подчеркивает важность мониторинга сетевой активности для обеспечения безопасности и эффективного управления сетевыми ресурсами.