МОЛДАВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ФАКУЛЬТЕТ МАТЕМАТИКИ И ИНФОРМАТИКИ
ДЕПАРТАМЕНТ ИНФОРМАТИКИ

Отчет по дисциплине:
“Безопасность информационных систем”

Лабораторная работа №6

Обнаружение и предотвращение вторжений в компьютерные системы. Системы защиты от вредоносного ПО и журналирования.

Автор: Калинкова С. группа I2302
Проверила: Новак Л.
doctor conferentiar universitar

Кишинев, 2024

Цель работы:

1. Изучение характеристик и принципа работы систем обнаружения и предотвращения вторжений. Анализ их рабочих параметров (IDS/IPS).
2. Сравнительная характеристика систем обнаружения или предотвращения вторжений IDS/IPS.
3. Изучение функциональности некоторых систем обнаружения/предотвращения вторжений. Проверка и указание совместимости с определенными операционными системами.
4. Описание принципа работы систем обнаружения/предотвращения вторжений.
5. Установление классификации по степени популярности в использовании и эффективности эксплуатации перечисленных ниже SDI/SPI.

Ход работы:

Обнаружение и предотвращение вторжений в компьютерные системы

Компьютерные системы уязвимы к атакам: взломам, вирусам, или утечкам данных. Для защиты используют технологии обнаружения (IDS) и предотвращения (IPS) вторжений.

IDS и IPS: что это такое?

1. **IDS (Intrusion Detection System):**
    - Отслеживает подозрительные действия в сети или на устройствах.
    - Уведомляет администратора, но не останавливает атаки.
2. **IPS (Intrusion Prevention System):**
    - Не только выявляет угрозы, но и блокирует их в реальном времени.
    - Защищает, анализируя пакеты данных и действия пользователей.

Системы защиты от вредоносного ПО и журналирования

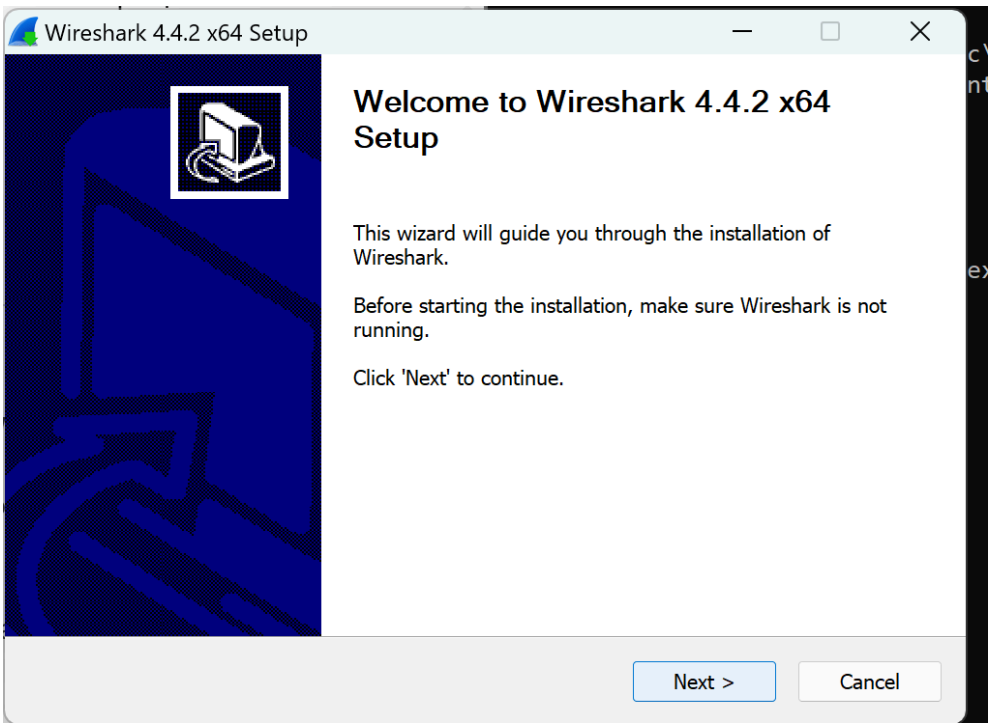
1. **Антивирусы:**
    - Находят и удаляют вирусы и трояны на операционных системах.
    - Пример: Windows Defender, ClamAV.
2. **Журналирование:**
    - Логи (журналы событий) фиксируют действия в системе.
    - Полезны для анализа атак и восстановления после инцидентов.
    - Пример: Event Viewer (Windows), Syslog (Linux).

<u>Практическая часть:</u>

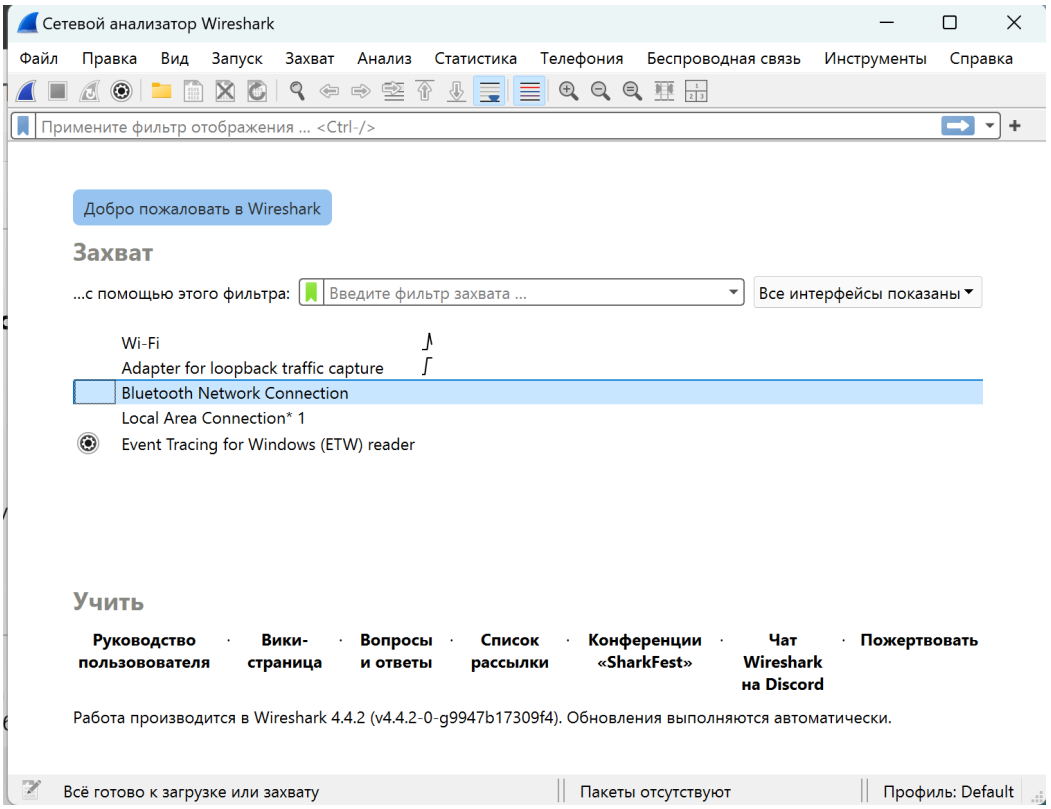
1. **Wireshark**

Wireshark — это инструмент для анализа сетевого трафика, который позволяет перехватывать и исследовать пакеты в реальном времени. Подходит для диагностики сети, тестирования безопасности и изучения протоколов.

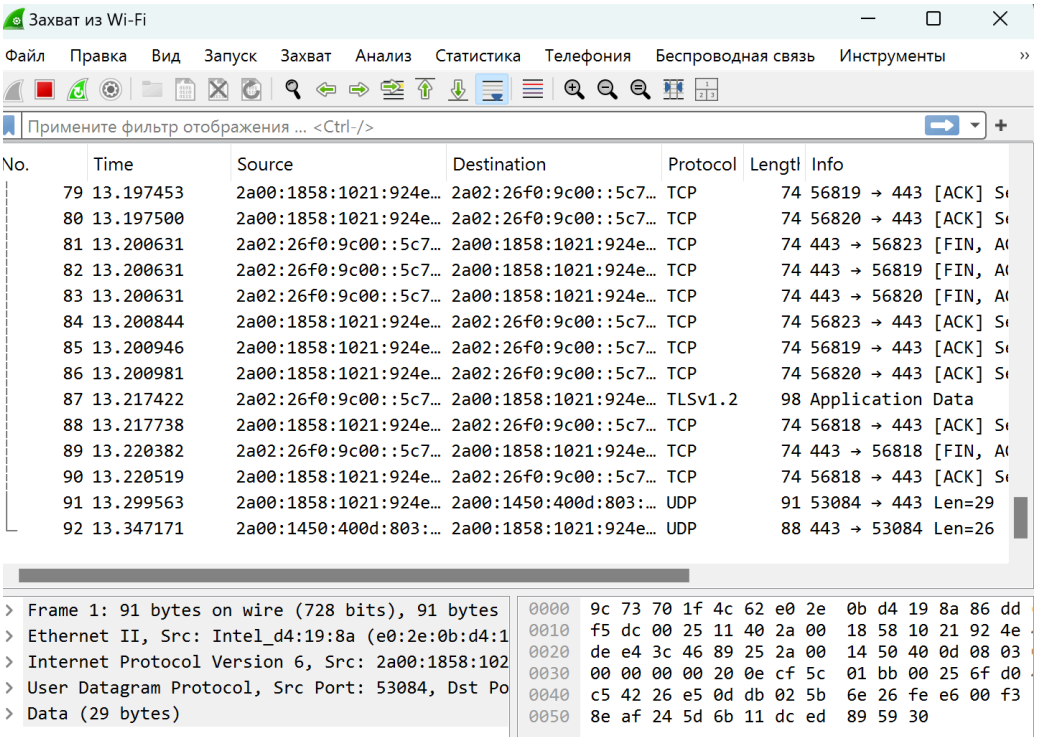
1. Загружаю версию Wireshark для Windows с официального сайта https://www.wireshark.org/.



1. Устанавливаю программу, оставив стандартные настройки. Wireshark имеет простой и удобный графический интерфейс

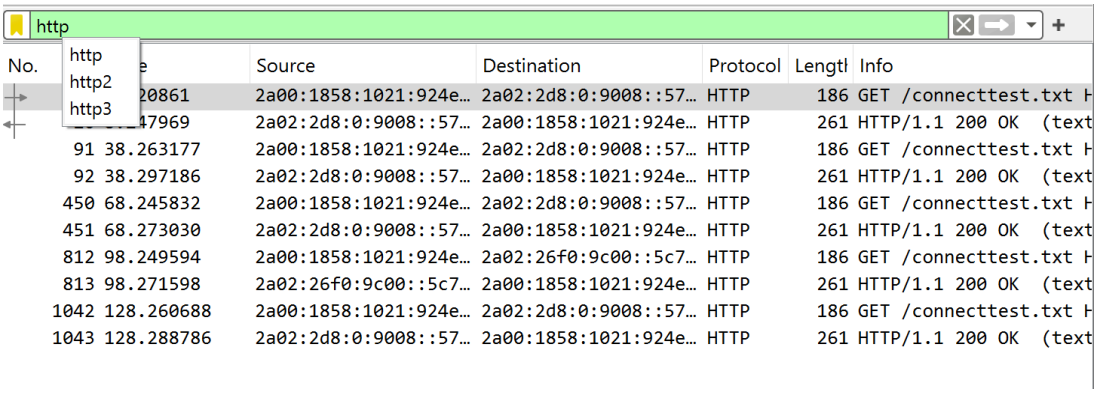


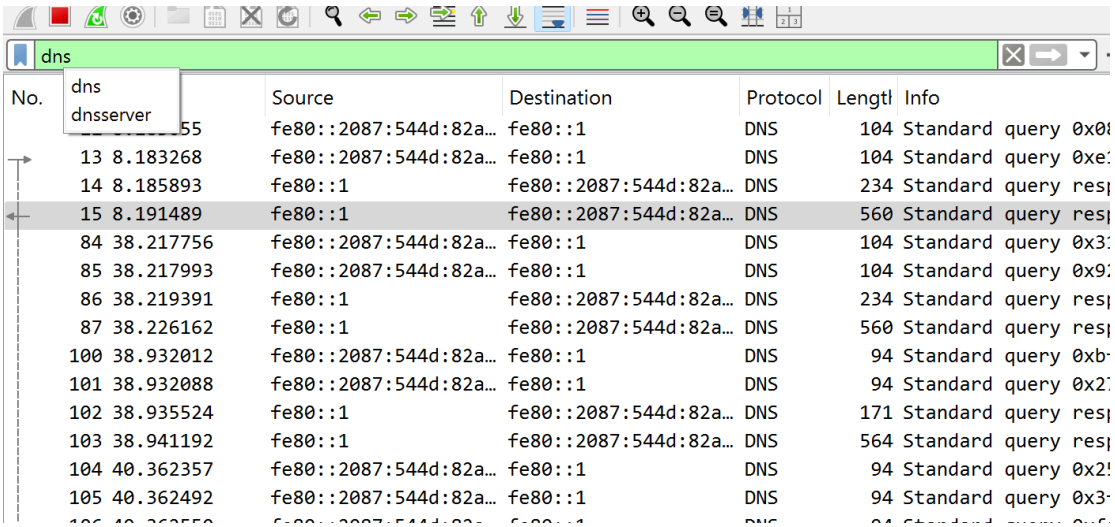
2. Запускаю Wireshark выбрав сетевой интерфейс (Wi-Fi) для мониторинга.



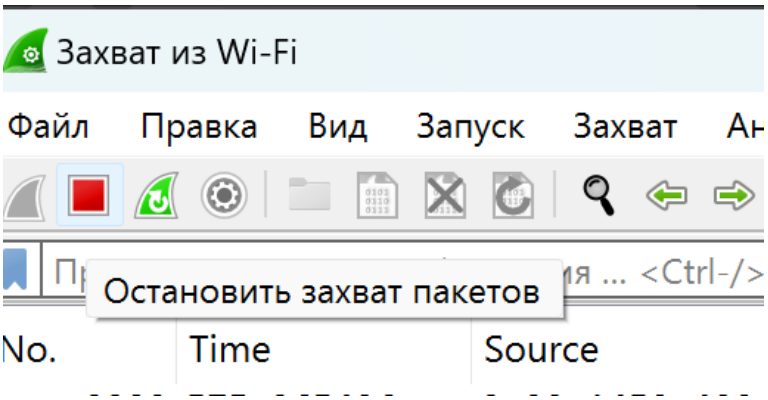
На скриншоте виден список пакетов с информацией о времени, адресах, протоколах и размере данных. Выбранный пакет детально отображается внизу, показывая его содержимое и параметры.

Также можно применить фильтр для захвата написав его в строке в верхней части экрана (например я ввела http и dns)





для того чтобы остановить захват пакетов нажимаю на кнопку стоп в верхнем левом углу



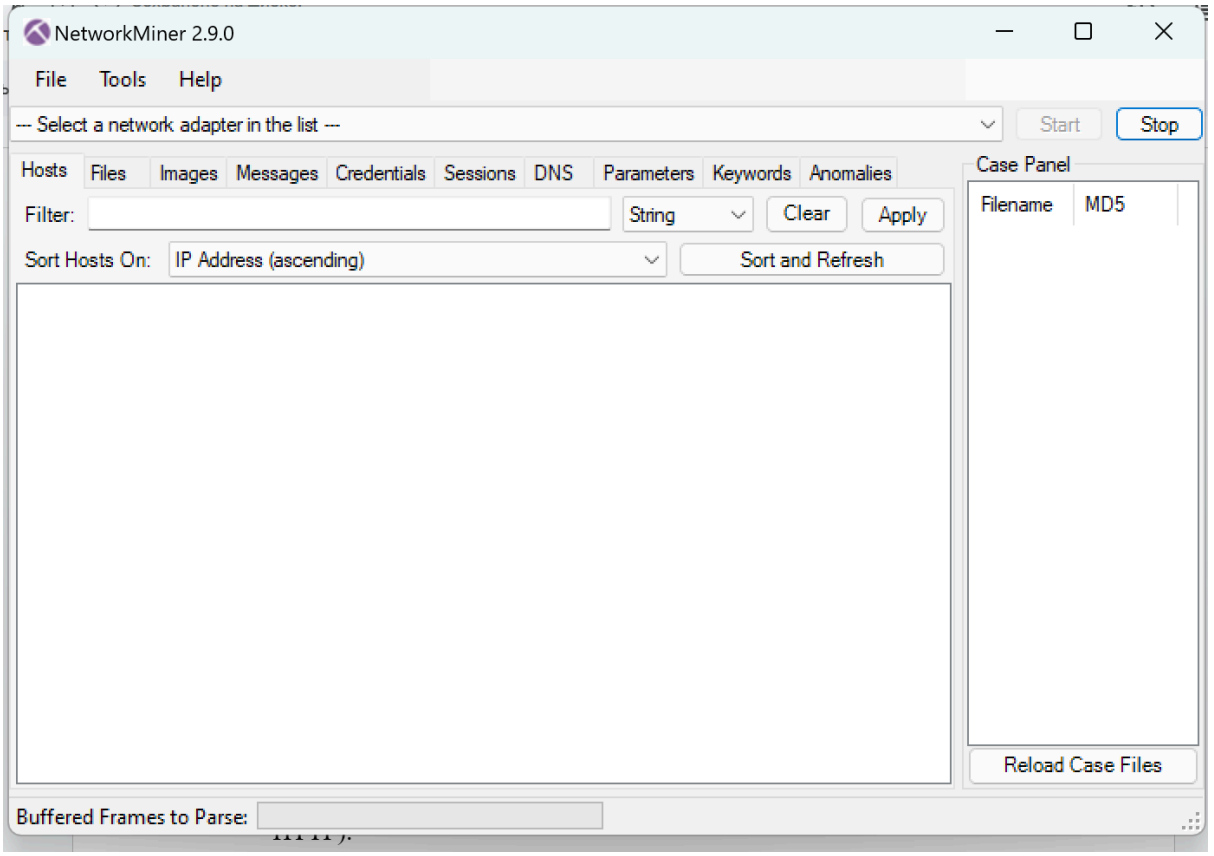
2. **NetworkMiner**

NetworkMiner — это пассивный анализатор сети для извлечения данных из сетевых захватов. Используется для анализа трафика, восстановления файлов и изучения сетевых артефактов.

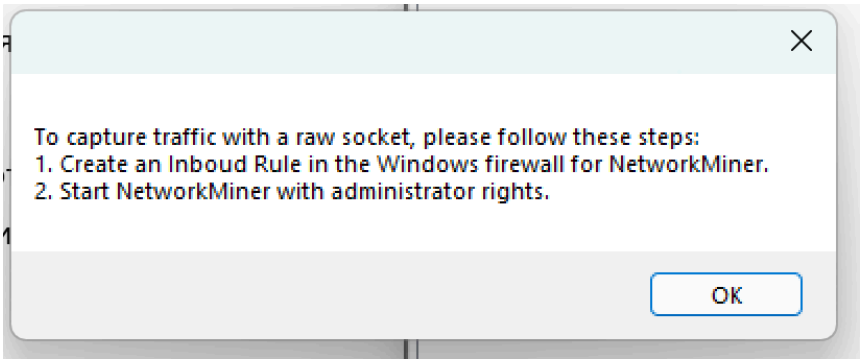
1. Скачиваю NetworkMiner с официального сайта https://www.netresec.com/.
2. Распаковываю архив и запускаю приложение просто нажав на exe файл, так как установка не требуется.

Использование NetworkMiner:

1. Интерфейс программы:
   простой и удобный, который позволяет легко начать анализ сети.



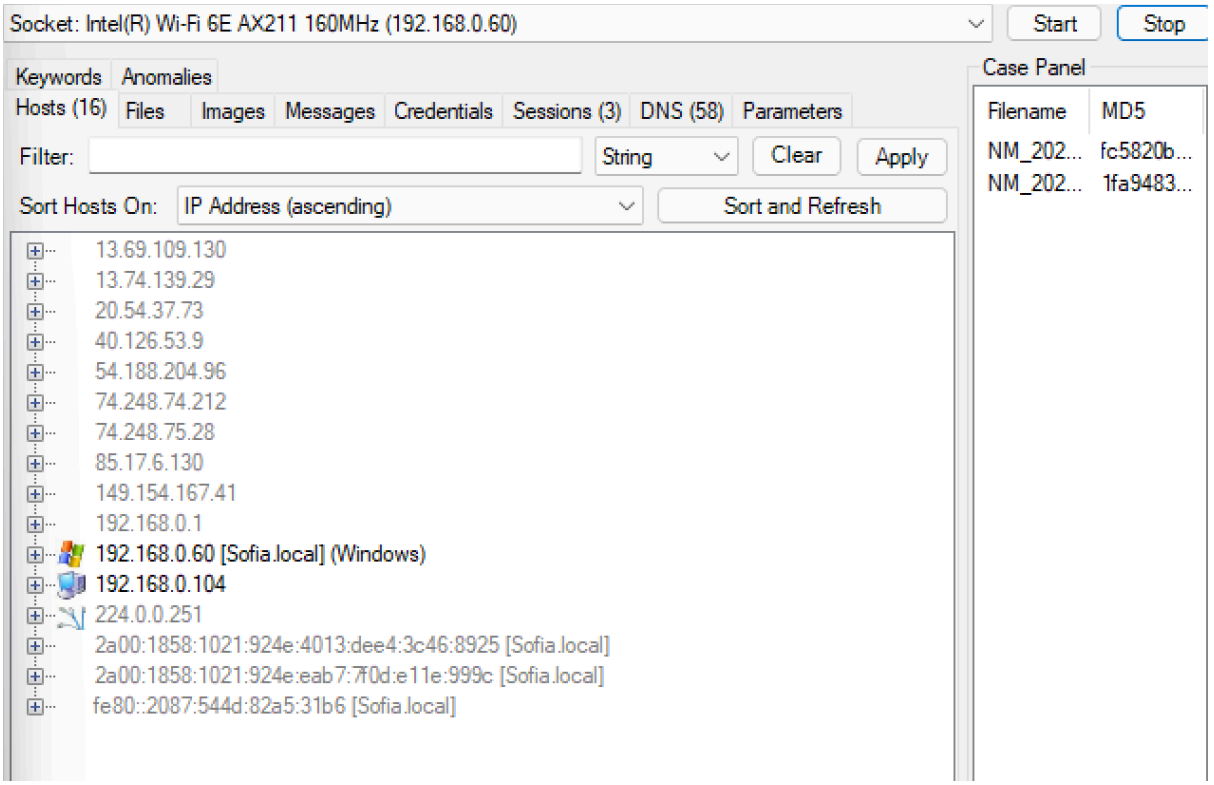
   при попытке выбрать сеть высвечивается сообщение



поэтому открываю программу заново от имени администратора

2. Захват трафика:

- В главном меню выбираю сетевой интерфейс (Wi-Fi или Ethernet).
- Нажимаю кнопку Start для начала анализа.



На скриншоте представлен процесс анализа сети. Выбранный сетевой интерфейс – Wi-Fi адаптер с IP-адресом **192.168.0.60**, который анализирует трафик в локальной сети.

Во вкладке **Hosts** отображены обнаруженные устройства в сети. Среди них:

- Локальный компьютер с именем **Sofia.local** и IP-адресом **192.168.0.60**, работающий на Windows.
- Узел с IP-адресом **192.168.0.104**, подключенный к той же сети.

Также присутствуют другие внешние и мультикаст-адреса. Справа, в **Case Panel**, находятся файлы с захваченным трафиком, готовые для анализа, с указанием их MD5-хешей.

Сравнительное описание NetworkMiner и Wireshark

Критерий	**NetworkMiner**	**Wireshark**
Тип лицензии	Бесплатное программное обеспечение. Также есть платная версия с расширенным функционалом.	Бесплатное программное обеспечение с открытым исходным кодом .
Совместимость с ОС	Windows (основная поддержка), может запускаться на Linux и macOS через Wine.	Windows, macOS, Linux, FreeBSD, другие Unix-подобные системы.
Описание услуг/принцип работы	Сетевой анализатор, фокусируется на пассивном анализе трафика. Извлекает файлы, изображения, учетные данные из трафика.	Захват сетевых пакетов и их подробный анализ в реальном времени. Поддерживает анализ на уровне приложений, протоколов и т. д.
Преимущества	- Удобен для начинающих благодаря простому интерфейсу. - Эффективно извлекает полезные данные, такие как файлы и логины.	- Широкий функционал для глубокого анализа. - Поддерживает множество форматов файлов и протоколов. - Бесплатен.
Недостатки	- Ограниченный функционал в бесплатной версии. - Требуется запуск от администратора .	- Может быть сложным для новичков из-за обилия функций.

Интерфейс работы	Графический интерфейс, удобный и интуитивно понятный.	Графический интерфейс, но насыщен функциями.
Простота использования	Высокая, особенно для задач базового анализа и извлечения данных.	Средняя: высокая сложность из-за широкого спектра инструментов.
Степень безопасности/ложные тревоги	Низкий риск ложных тревог, так как анализирует уже собранный трафик.	Может генерировать ложные тревоги из-за ошибок при анализе сложных протоколов.
Популярность	Чаще используется аналитиками и исследователями, фокусирующимися на извлечении данных из захваченного трафика.	Очень популярна среди сетевых администраторов, инженеров и исследователей безопасности.
Простота настройки	Простая настройка, но требует правил для брандмауэра и прав администратора.	Простая установка, но для настройки и использования требуется понимание сетевых концепций.
Другие аспекты	- Сфокусирован на пассивном анализе. - Подходит для судебной экспертизы и восстановления данных из трафика.	- Обширные возможности фильтрации. - Подходит для анализа в реальном времени и устранения неполадок сети.

Вывод:

В процессе выполнения лабораторной работы я изучила принципы работы систем обнаружения и предотвращения вторжений (IDS/IPS), а также их

роль в обеспечении информационной безопасности. Я провела анализ сетевого трафика с использованием таких инструментов, как Wireshark и NetworkMiner, которые предоставили работу с трафиком и базовое понимание анализа сетевых угроз.

Библиография

1. https://habr.com/ru/articles/204274/
2. https://selectel.ru/blog/ips-and-ids/
3. https://www.wireshark.org/download.html
4. https://www.netresec.com/?page=NetworkMiner
5. https://spy-soft.net/networkminer/