Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники»

Факультет информационных технологий и управления
Кафедра интеллектуальных информационных технологий
Дисциплина «Средства и методы защиты информации в интеллектуальных системах»

ОТЧЁТ
к лабораторной работе №8
на тему
«НАБЛЮДЕНИЕ ЗА СТЕКОМ TCP/IP»

БГУИР 6-05-0611-03 130

Выполнил студент группы 321701
СЕМЕНЯКО Владимир Дмитриевич

_____
(дата, подпись студента)

Проверил
САЛЬНИКОВ Даниил Андреевич

_____
(дата, подпись преподавателя)

Минск 2025

1 ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ

а) Запустите Snort в режиме Sniffer пакетов или протоколирования с различными параметрами детализации.

б) Обратитесь к локальной сети. Выполните команду ping, запустите броузер или проводник. Сохраните какой либо файл (не большой) на материнской машине.

в) Остановите Snort. Определите к каким IP-портам и адресам были выполнены обращения.

г) Просмотрите содержимое перехваченных пакетов.

2 ВЫПОЛНЕНИЕ РАБОТЫ

Первым делом, стоит определить доступные интерфейсы. Для определения воспользуемся командой:

```
snort -W
```

Для запуска утилиты Snort в режиме Sniffer, выполним следующую команду:

```
snort -v -i 1
```

Также для более подробного вывода с полезными данными (вывод содержимого уровня приложений):

```
snort -v -d -i 1
```

Для последующего анализа в ходе лабораторной работы, применим логирование всего перехваченного трафика с помощью команды:

```
snort -l C:\Snort\log -b -i 1
```

После запуска Snort, выполнения команды ping, выполнения запроса в адресной строке на веб-сайт google.com, приостановим работу Snort

Далее перейдем в программу Wireshark и откроем log файл

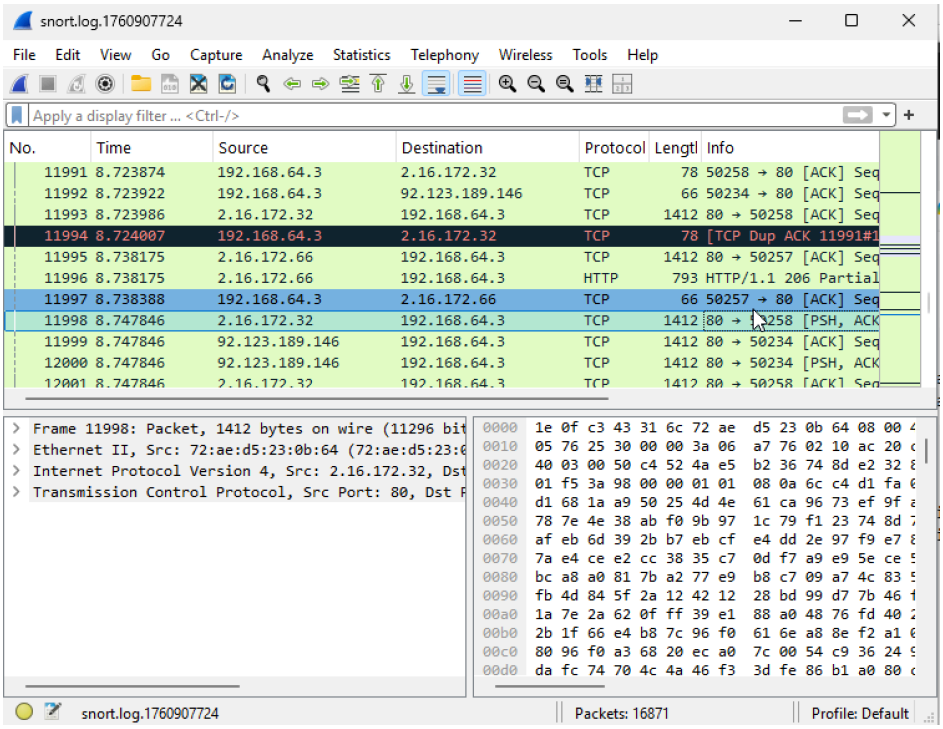

Рисунок 1 – Содержание log файла внутри Wireshark

В данной программе мы можем выполнить фильтрацию с помощью неких условий. Например:

```
http && ip.addr == 192.168.64.3
```

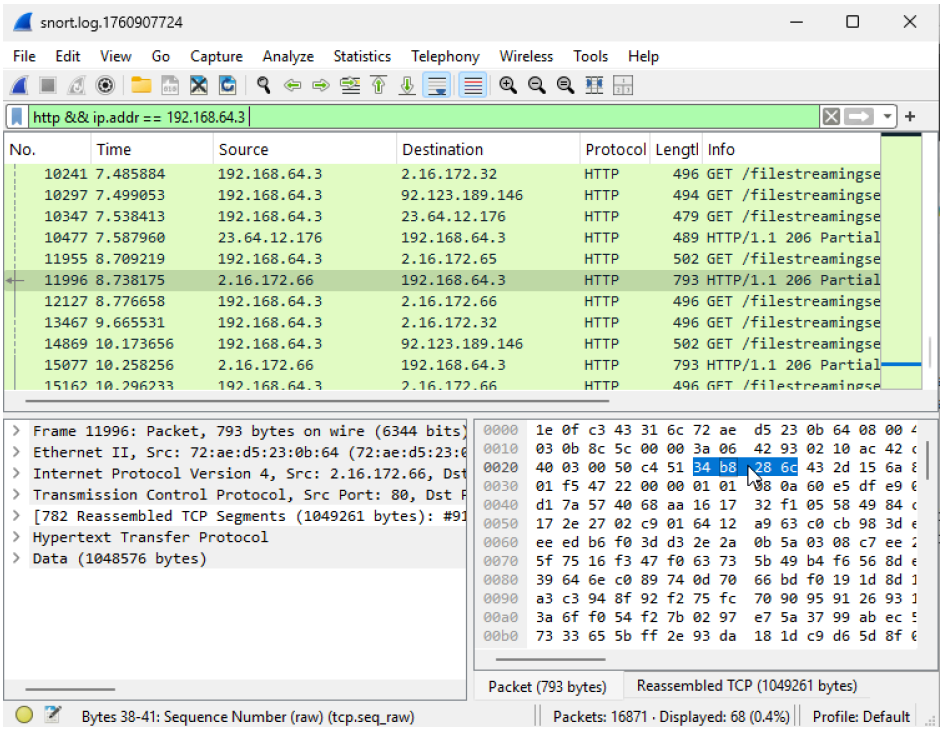

Рисунок 2 – Пример фильтрации внутри Wireshark

ВЫВОД

В ходе лабораторной работы были изучены принципы работы системы перехвата и анализа сетевых пакетов с использованием утилиты Snort. В процессе выполнения задания был произведён запуск Snort в различных режимах детализации, сгенерирован сетевой трафик с помощью команды ping, браузера и передачи файла на материнскую машину. Были собраны и проанализированы перехваченные пакеты, определены IP-адреса и используемые порты, сопоставленные с соответствующими сетевыми службами. Полученные результаты позволили закрепить практические навыки работы с системами мониторинга сети, изучить структуру сетевых пакетов и понять механизмы взаимодействия протоколов на разных уровнях.