Государственное учреждение образования

“БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ”

Кафедра: Интеллектуальных информационных технологий

Дисциплина: Средства и методы защиты информации в интеллектуальных системах

**Отчет по лабораторной работе №8**

**“Наблюдение за стеком TCP/IP”**

Выполнил:

студент гр.121702

Витковская С. И.

Проверил:

Сальников Д.А.

Минск 2023

**Содержание**

[**Задача: 3**](#_gl8o1xw3chrw)

[**Ход работы: 3**](#)

#### **Задача:**

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.

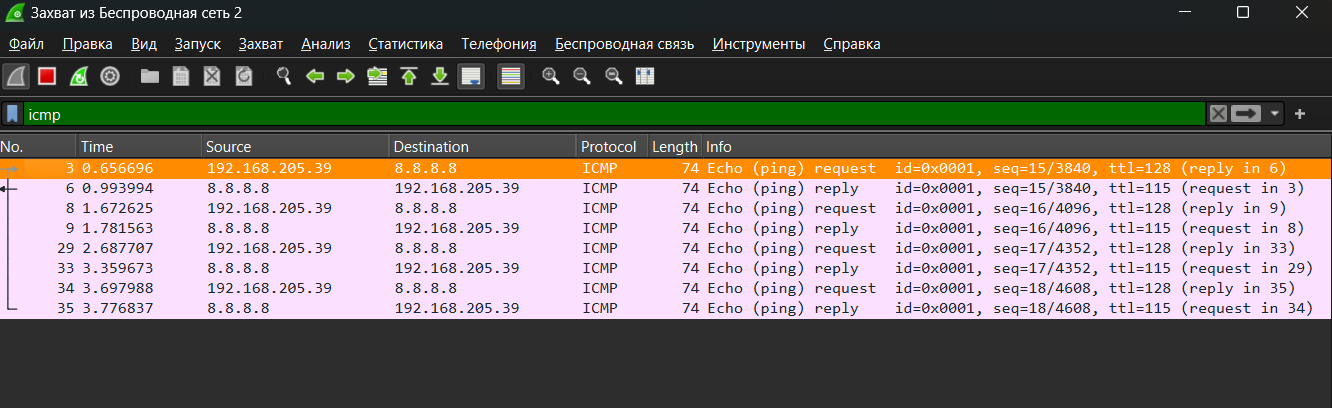
5. Остановите Snort. Определите к каким IP-портам и адресам были выполнены обращения.

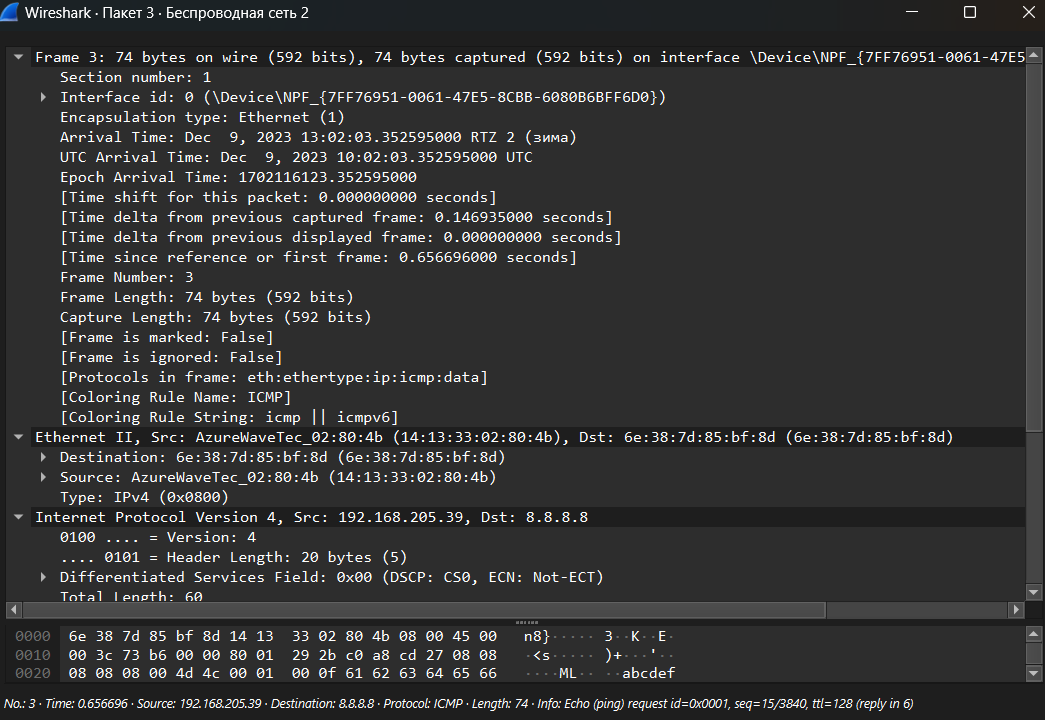
6. Пользуясь \windows\system32\etc\service, определите какие системные службы использовались.

7. Просмотрите содержимое перехваченных пакетов.

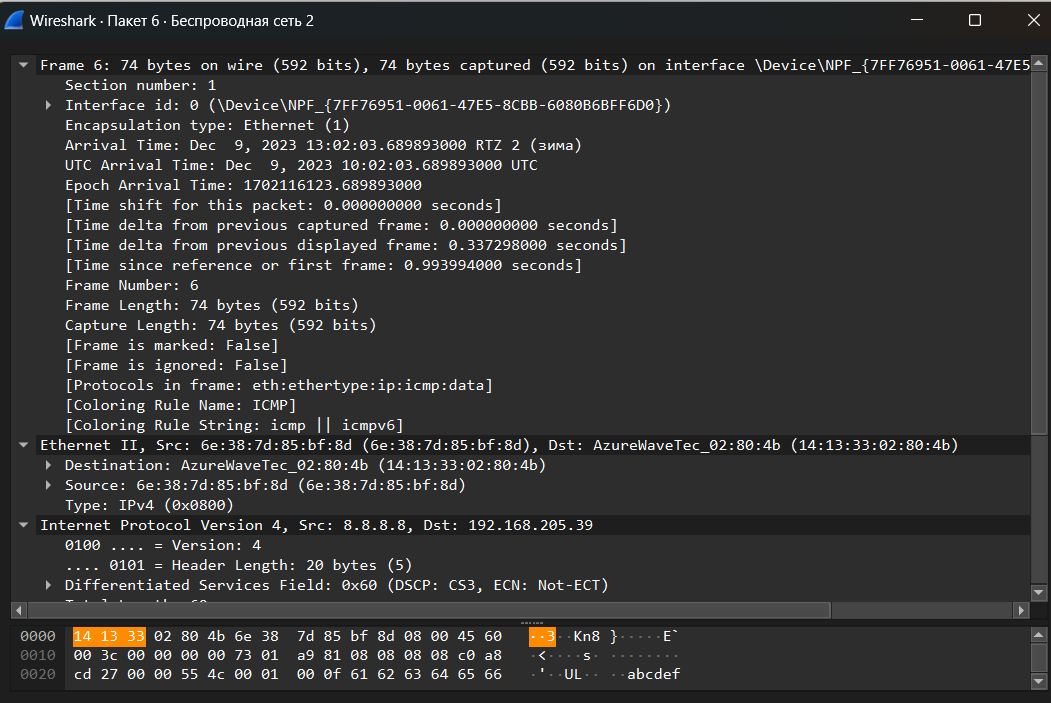
8. Используя дополнительную литературу расшифруйте содержание вывода заголовка. Оформите отчет. В отчет обязательно поместите примеры пакетов и список обнаруженных протоколов и служб.

## **Ход работы:**

1. 
2. Отправленный пакет



1. Полученный пакет



**Вывод**:

Изучили Wireshark – перехватчик и анализатор сетевого трафика. Были изучены пакеты протокола IPv4, полученные и отправленные через эхо-запрос ICMP, входящий в стек протоколов TCP.