МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Омский государственный технический университет».
Радиотехнический факультет
Кафедра «Комплексная защита информации»

# Лабораторная работа №4
по дисциплине «Безопасность вычислительных сетей»

Выполнил студент гр. КЗИ-191:
Забелина А.А.

Проверил:
доцент, к. т. н.
Щерба Е.В.

Омск 2022

**4.1.2.10 Лабораторная работа. Общие сведения о программе Wireshark.**

Виртуальная машина CyberOps располагает сценарий Python, который, будучи запущен, устанавливает и настраивает устройства, показанные на приведенном выше рисунке. Затем вы получите доступ к 4 узлам, коммутатору и маршрутизатору внутри одной ВМ. Это позволит моделировать различные сетевые протоколы и службы без необходимости настраивать физическую сеть устройств.

Wireshark — это программа для анализа протоколов (анализатор пакетов), которая используется для поиска и устранения неполадок в сети, анализа, разработки программного обеспечения и протоколов, а также обучения.

**Часть 1: Установка и проверка топологии Mininet**

В этой части лабораторной работы вы будете использовать сценарий Python для настройки топологии Mininet внутри виртуальной машины CyberOps. Затем вы запишете IP- и MAC-адреса для H1 и H2.

Запустите и выполните вход в свою рабочую станцию CyberOps, установленную в предыдущей лабораторной работе, используя следующие учетные данные.

Имя пользователя: analyst.

Откройте эмулятор терминала для запуска mininet и введите следующую команду в командной строке. В ответ на запрос введите cyberops в качестве пароля.

Пароль: cyberops.

```
[analyst@secOps ~]$ sudo ~/lab.support.files/scripts/cyberops_topo
[sudo] password for analyst:


CyberOPS Topology:

          ------       ------
          | R1 |-------| H4 |
          ------       ------
            |
            |
          ------
  |-------| S1 |-------|
  |       ------       |
  |         |          |
  |         |          |
------    ------     ------
| H1 |    | H2 |     | H3 |
------    ------     ------

*** Add links
*** Creating network
*** Adding hosts:
H1 H2 H3 H4 R1
*** Adding switches:
s1
*** Adding links:
(H1, s1) (H2, s1) (H3, s1) (H4, R1) (s1, R1)
*** Configuring hosts
H1 H2 H3 H4 R1
*** Starting controller

*** Starting 1 switches
s1 ...
*** Routing Table on Router:
```

Рисунок 1 – Запуск сценария Python для установки топологии

В командной строке mininet запустите окна терминала на узлах H1 и H2. Будут открыты отдельные окна для этих узлов. Каждый узел будет иметь собственную отдельную конфигурацию для сети, в частности уникальные IP- и MAC-адреса.

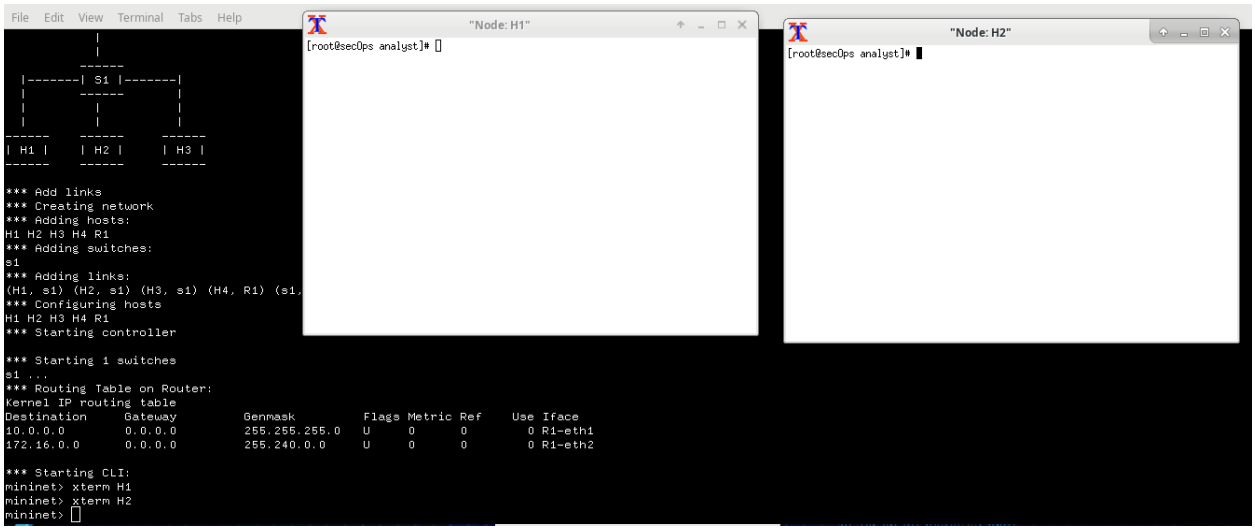

Рисунок 2 – Узлы H1 и H2

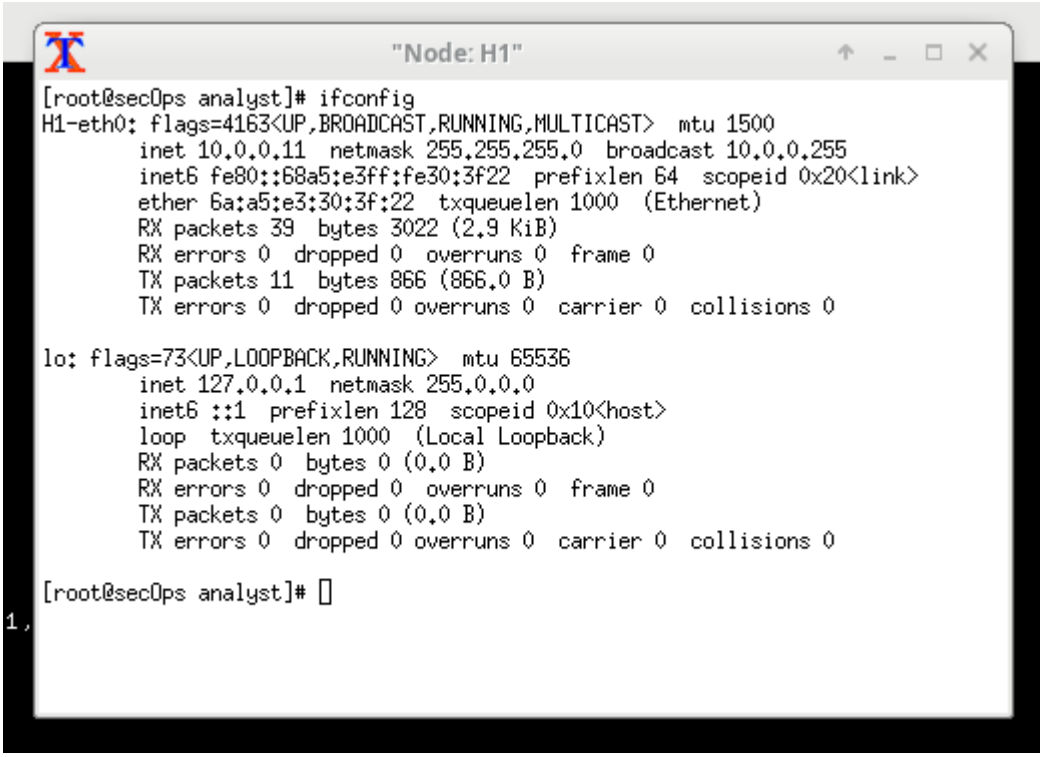

Рисунок 3 – Конфигурация узла H1

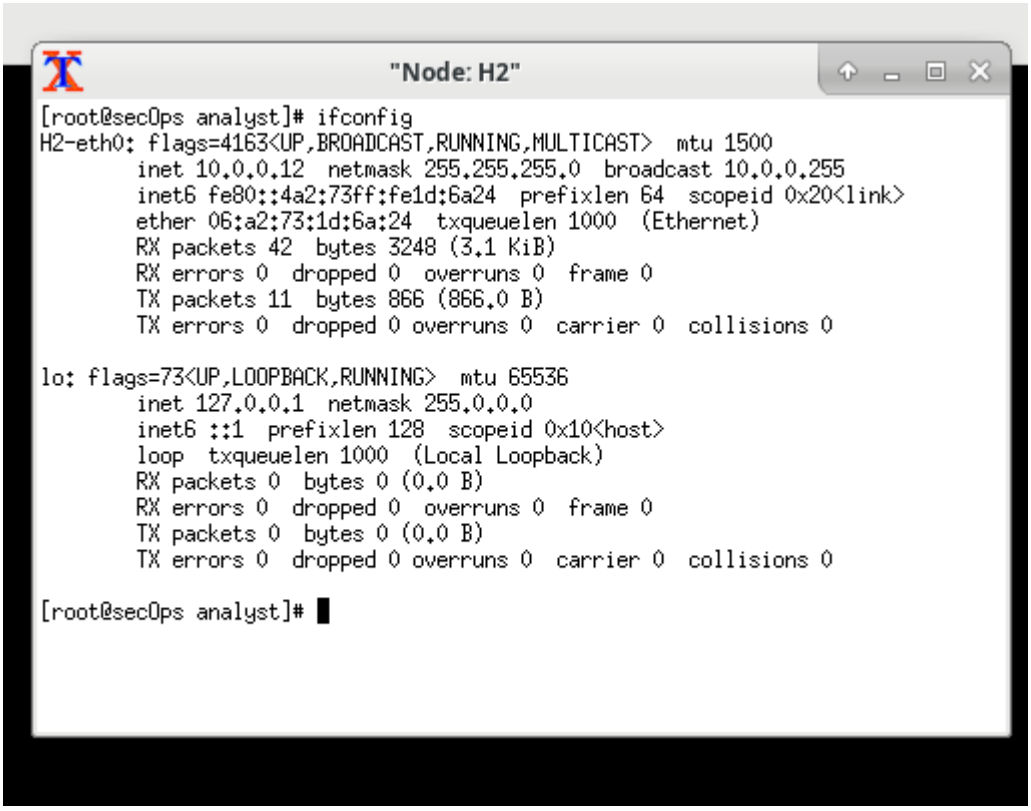

Рисунок 4 – Конфигурация узла H2

| Интерфейс узла | IP-адрес | MAC-адрес |
|---|---|---|
| H1-eth0 | 10.0.0.11 | 6a:a5:e3:30:3f:22 |
| H2-eth0 | 10.0.0.12 | 06:a2:73:1d:6a:24 |

**Часть 2: Сбор и анализ данных протокола ICMP в программе Wireshark.**

В этой части лабораторной работы вы будете посылать эхозапросы между двумя узлами в Mininet и перехватывать ICMP-запросы и отклики в программе Wireshark. Кроме того, вам нужно будет найти необходимую информацию в собранных PDU. Этот анализ поможет понять, как используются заголовки пакетов для передачи данных в место назначения.

Программа Wireshark отображает данные в трех разделах: 1) в верхнем разделе отображается список полученных кадров PDU со сводной информацией об IP-пакетах; 2) в среднем разделе приводится информация о PDU для кадра, выбранного в верхней части экрана, а также разделение перехваченного кадра PDU по уровням протоколов; 3) в нижнем разделе показываются необработанные данные каждого уровня. Необработанные данные отображаются как в шестнадцатеричном, так и в десятичном форматах.

На узле H1 введите wireshark gtk &, чтобы запустить программу Wireshark (всплывающее предупреждение не имеет значения в рамках этой лабораторной работы). Для продолжения нажмите ОК.

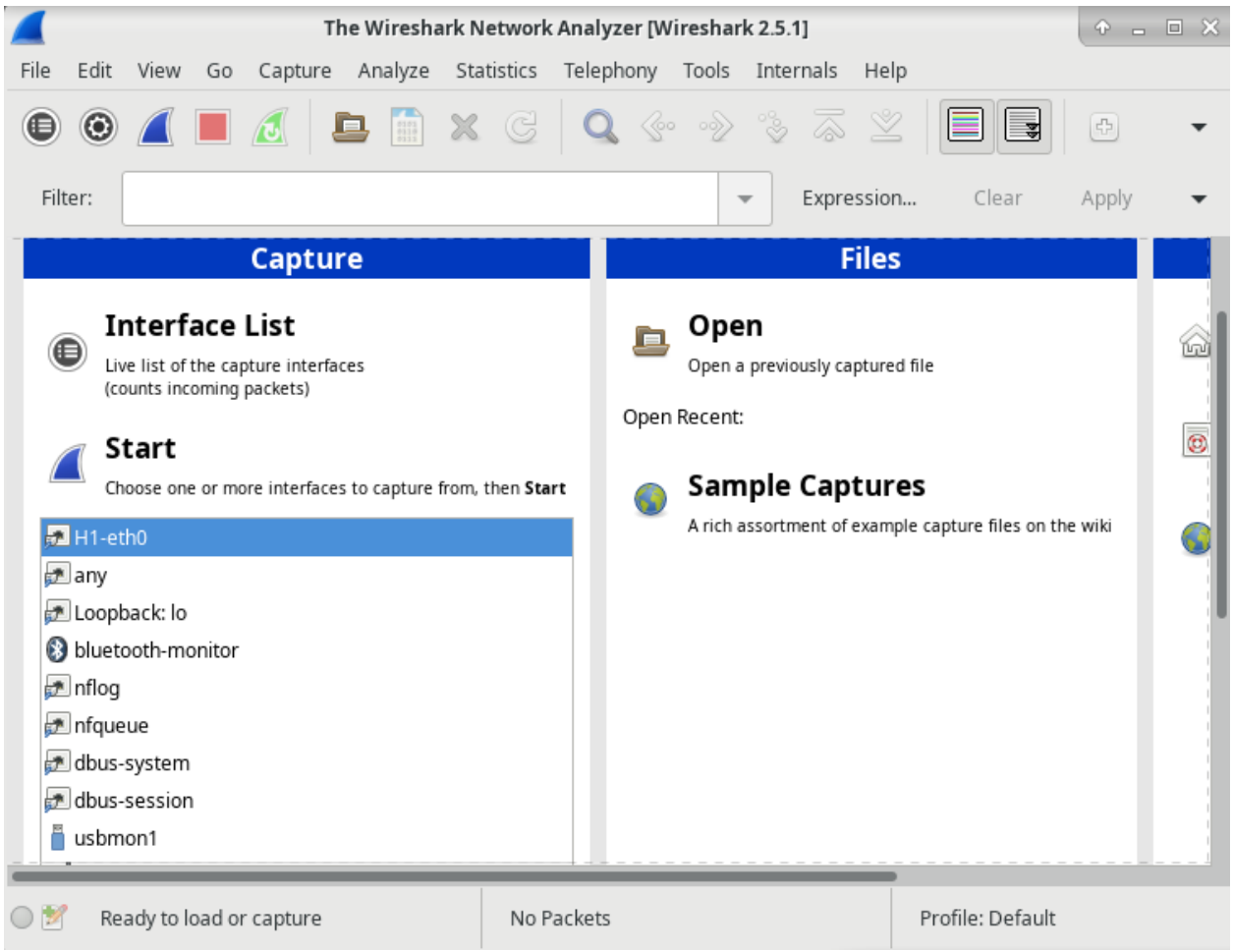


Рисунок 5 – Окно программы Wireshark

В окне Wireshark под заголовком Capture (Получить) выберите интерфейс H1 eth0. Нажмите кнопку Start (Начать) для перехвата трафика.

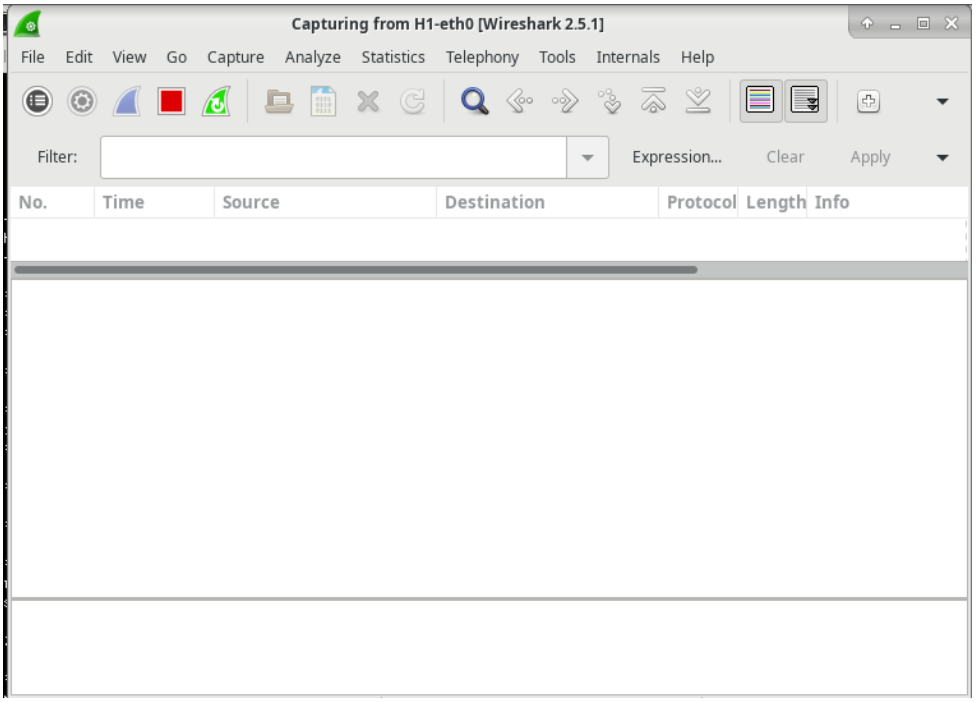


Рисунок 6 – Перехват трафика

На узле H1 нажмите клавишу Enter, если необходимо получить запрос. Введите ping -c 5 10.0.0.12, чтобы послать эхозапрос H2 пять раз. Параметр команды -c указывает число проверок связи. 5 указывает, что должно быть отправлено пять эхозапросов. Эта проверка связи будет успешной.

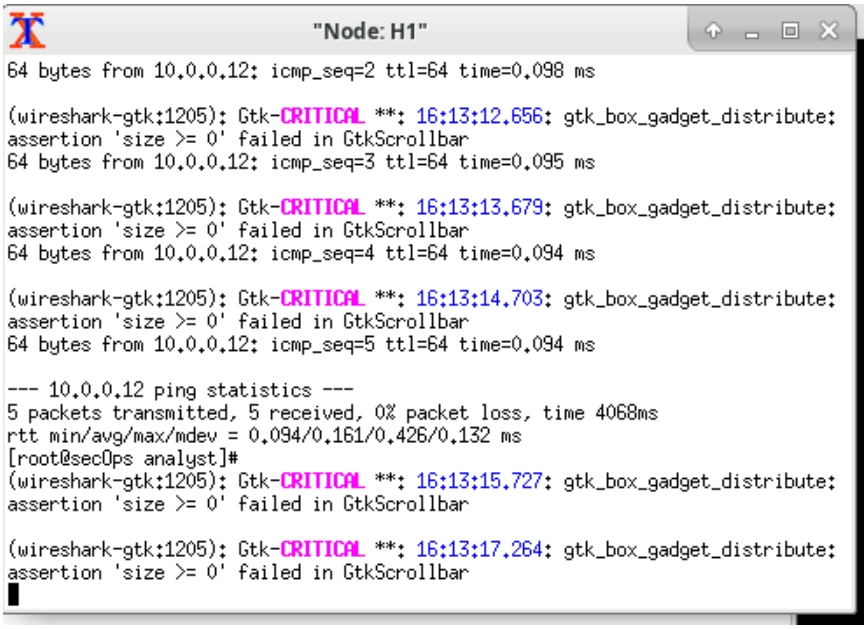


Рисунок 7 – Проверка связи

Перейдите в окно Wireshark, щелкните Stop (Остановить), чтобы остановить перехват пакетов.

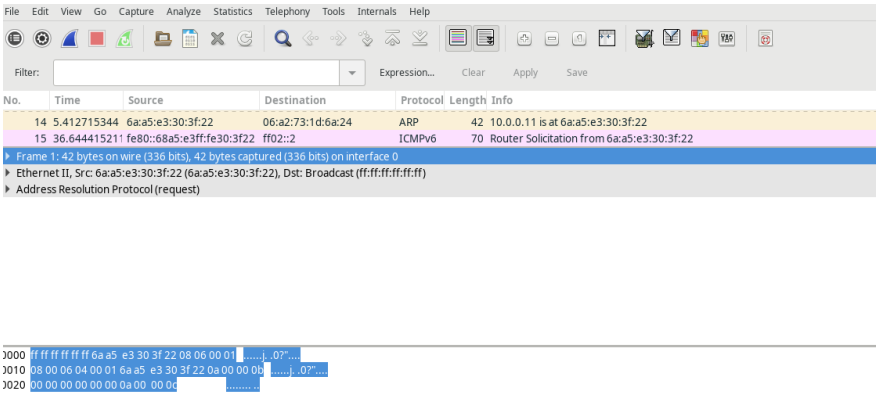


Рисунок 8 – Остановка перехвата пакетов

Фильтр может применяться для показа только интересующего вас трафика. Введите icmp в поле Filter (Фильтр) и щелкните Apply (Применить).

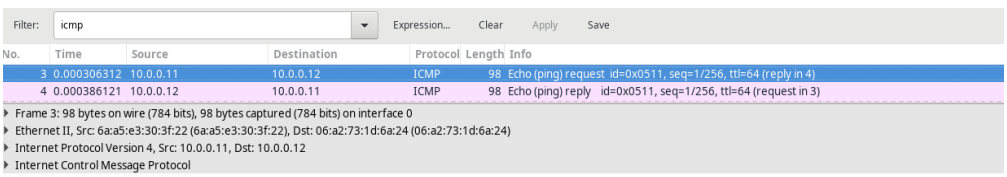


Рисунок 9 – Фильтр трафика

При необходимости выберите кадры PDU первого ICMP-запроса в верхней части окна программы Wireshark. Обратите внимание, что в столбце Source имеется IP-адрес H1, а в столбце назначения содержится IP-адрес H2.

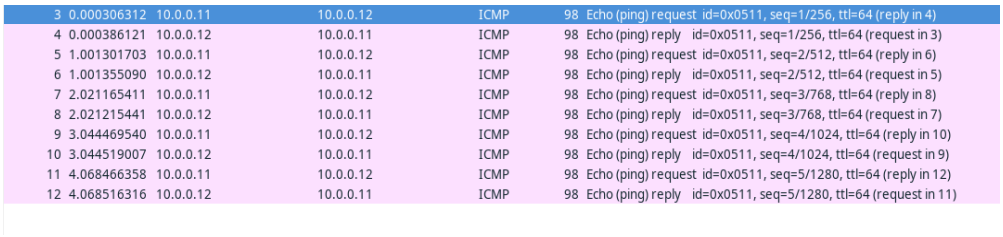


Рисунок 10 – Кадры PDU ICMP-запроса

Не меняя выбор кадра PDU в верхнем разделе окна, перейдите в средний раздел. Щелкните стрелку слева от строки Ethernet II, чтобы просмотреть MAC-адреса источника и назначения.

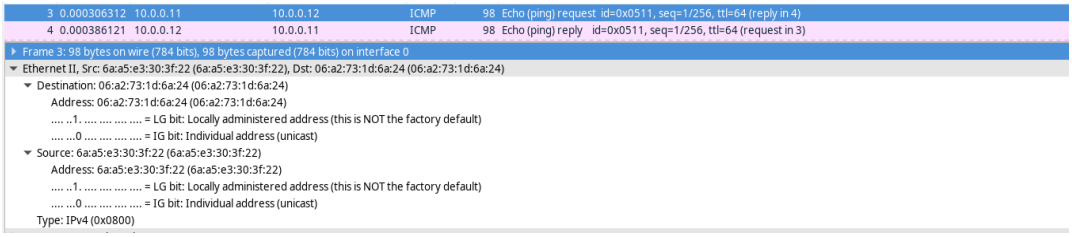


Рисунок 11 – Просмотр MAC-адреса источника и назначения

Вы должны будете отправить эхо запросы с помощью команды ping на удаленные узлы (расположенные за пределами локальной сети) и изучить данные, сформированные этими запросами. Затем вам нужно будет определить различия между этими данными и данными, которые вы изучали в части 1.

В командной строке mininet запустите окна терминала на узлах H4 и R1.

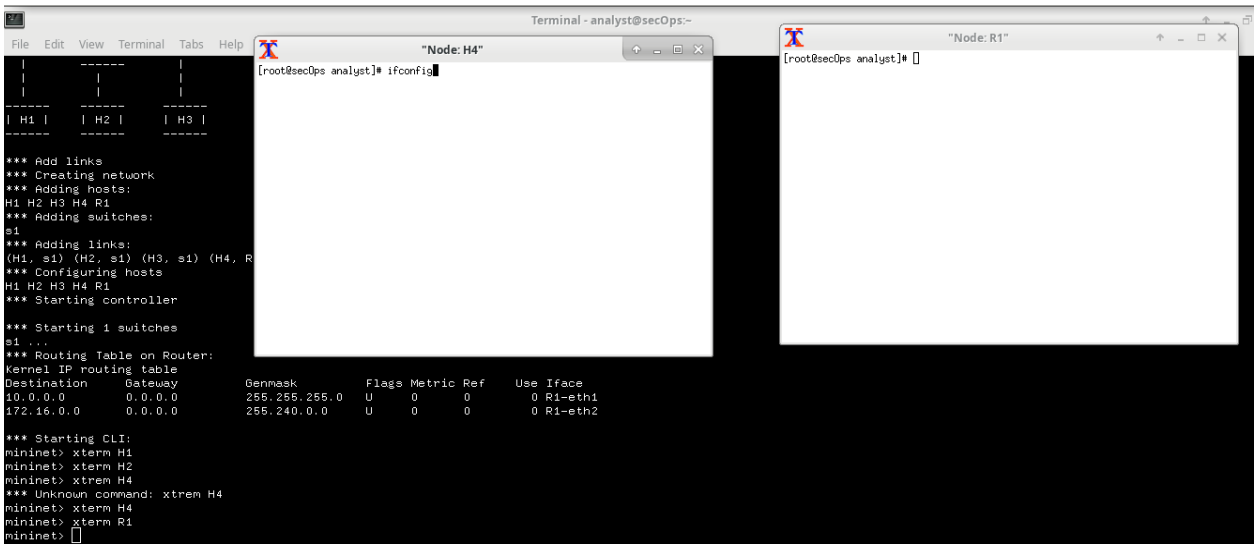


Рисунок 12 – Окна терминала на узлах H4 и R1

В командной строке на узле H4 введите ifconfig для проверки IPv4-

адреса и запишите MAC-адрес. Повторите операцию для узла R1.

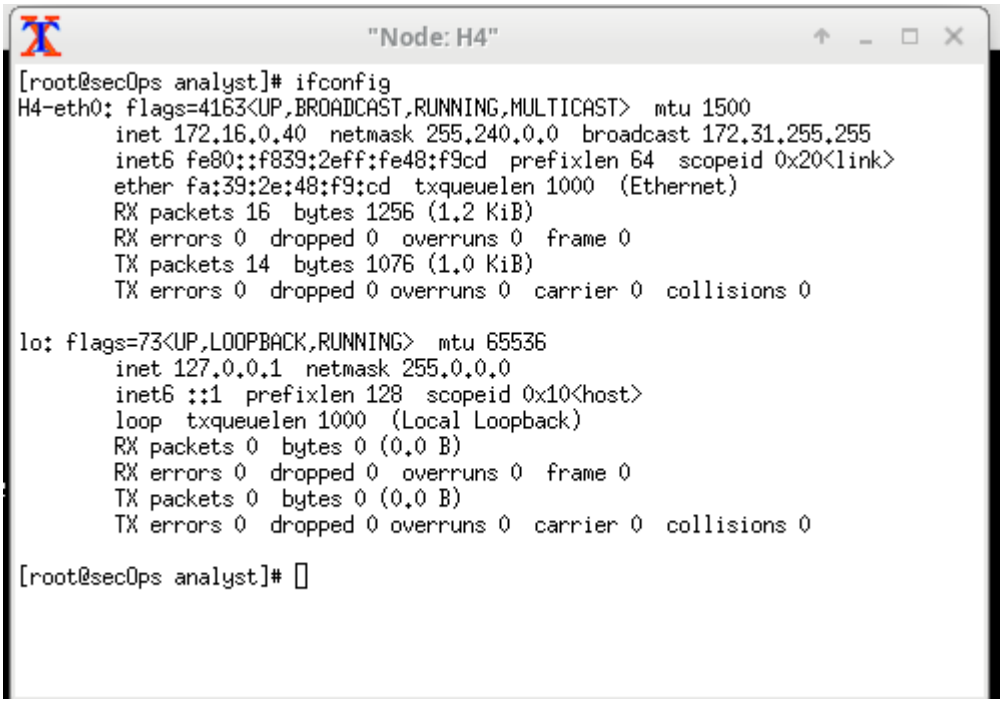


Рисунок 13 – Проверка IPv4-адреса на узле H4

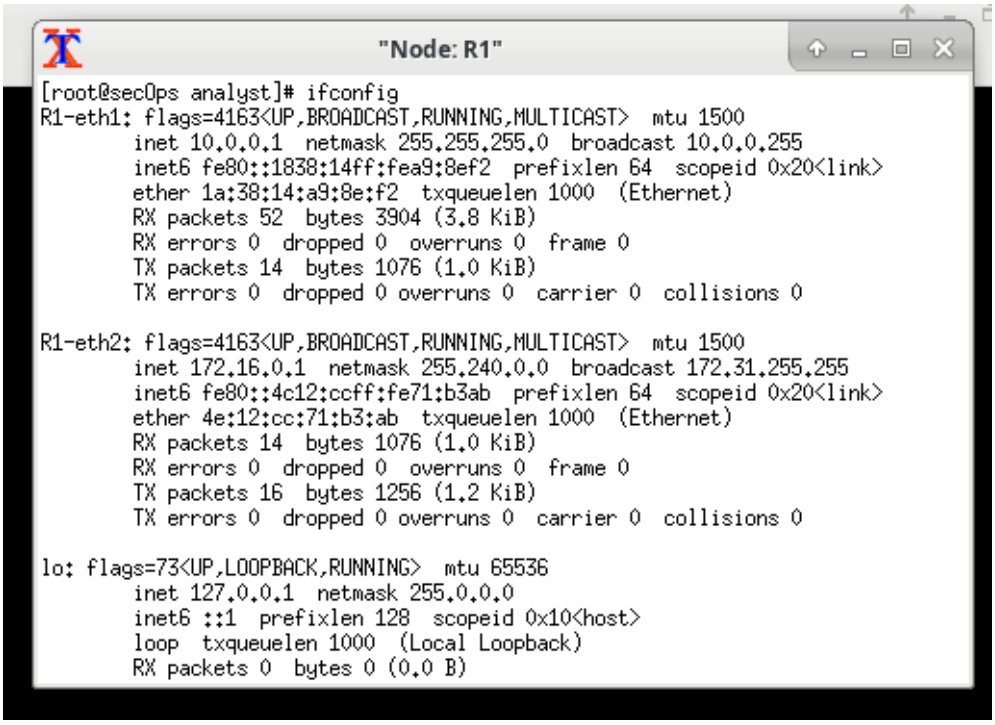


Рисунок 14 – Проверка IPv4-адреса на узле H4

| **Интерфейс узла** | **IP-адрес** | **MAC-адрес** |
|---|---|---|
| H4-eth0 | 172.16.0.40 | fa:392e:48:f9:cd |
| R1-eth1 | 10.0.0.1 | 1a:38:14:a9:8e:f2 |
| R1-eth2 | 172.16.0.1 | 4e:12:cc:71:b3:ab |

Начните новый перехват данных программой Wireshark на H1, выбрав Capture > Start (Получение > Начать). Можно нажать кнопку Start (Начать) или ввести Ctrl-E. Щелкните Continue without Saving (Продолжить без сохранения), чтобы начать новый перехват.

H4 является смоделированным удаленным сервером. Эхозапрос для H4 от H1. На эти ping запросы должны приходить ответы.

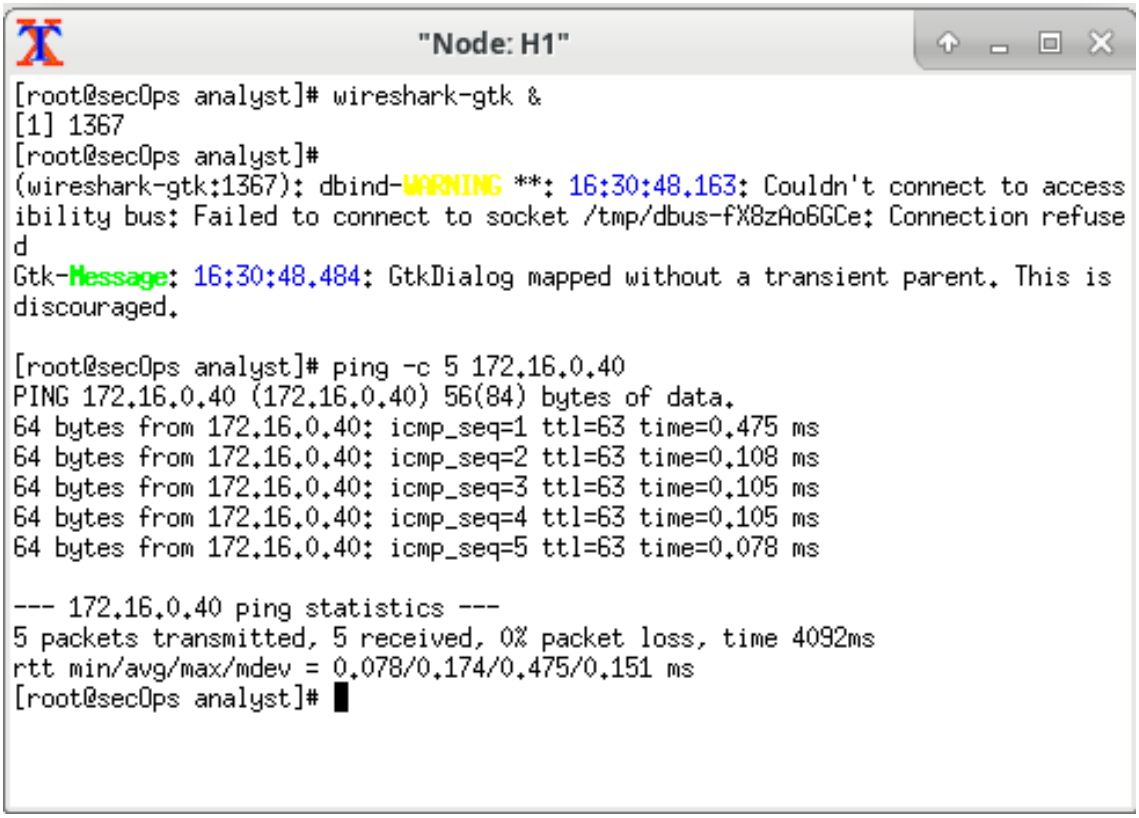


Рисунок 15 – Эхозапрос для H4 от H1

Просмотрите собранные данные в программе Wireshark. Изучите IP- и MAC-адреса, на которые вы отправили эхозапрос. Обратите внимание, что MAC-адрес — для интерфейса R1-eth1. Укажите IP- и MAC-адрес места назначения.

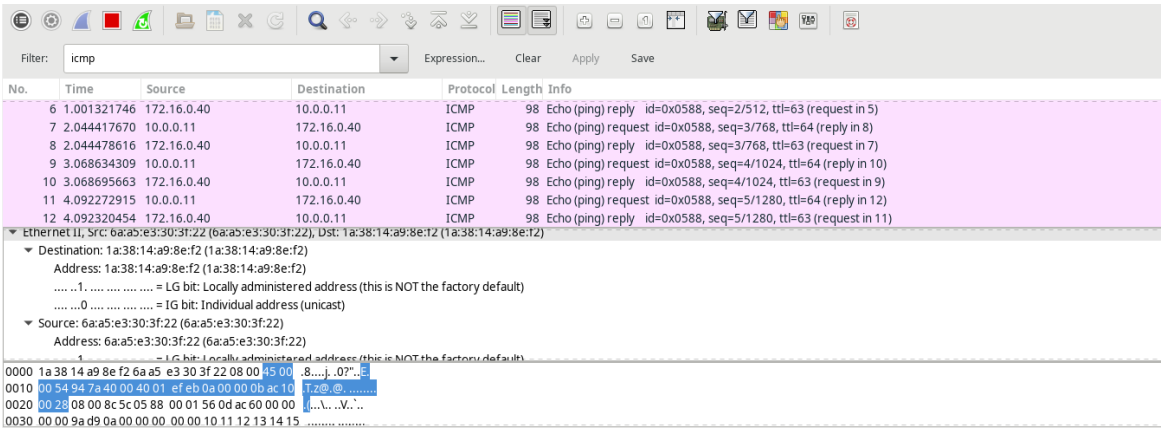


Рисунок 16 – IP- и MAC-адрес места назначения

В главном окне ВМ CyberOps введите quit, чтобы остановить Mininet.

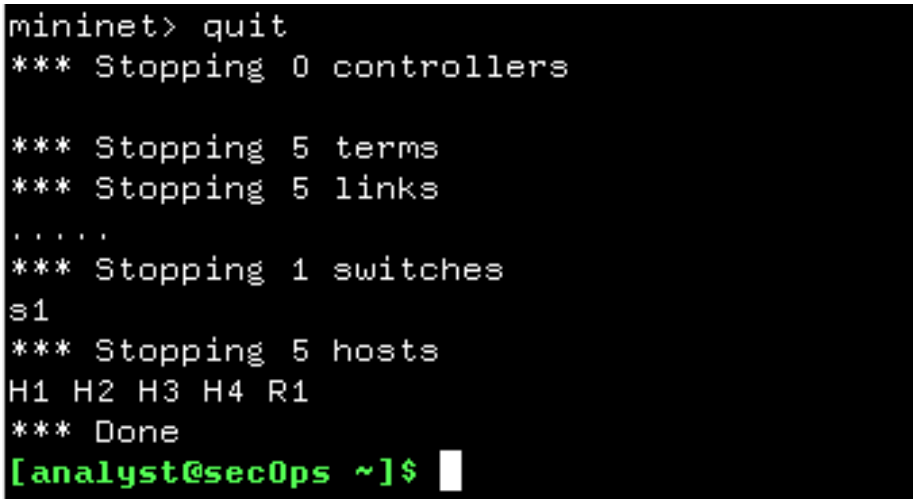


Рисунок 17 – Остановка Mininet

Для того чтобы очистить все процессы, которые использовались Mininet, введите команду sudo mn - c в командной строке.

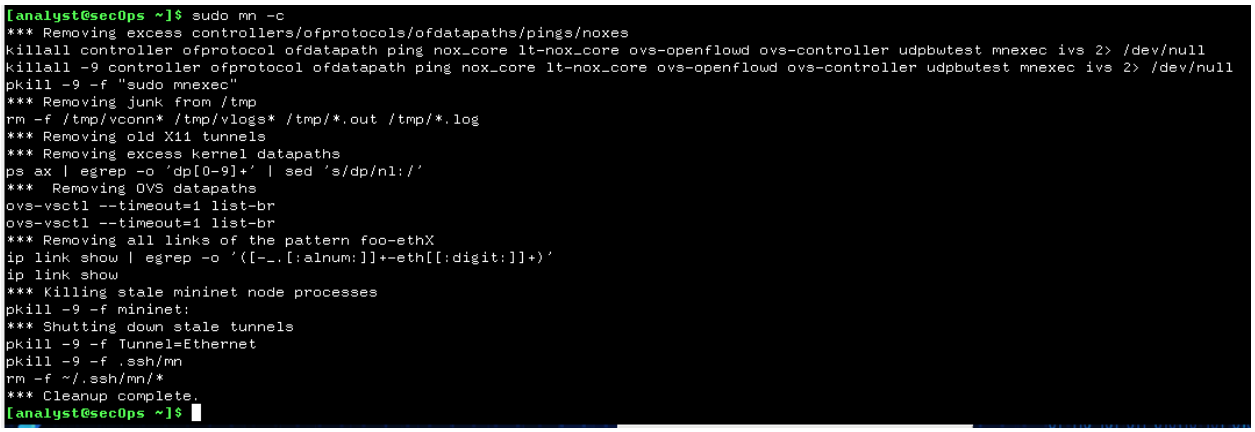


Рисунок 18 – Очищение процессов Mininet

**4.4.2.8 Лабораторная работа. Анализ кадров Ethernet с помощью программы Wireshark.**

**Часть 1: Изучение полей заголовков в кадре Ethernet II**

В части 1 вы изучите поля и содержание заголовков в предоставленном вам кадре Ethernet II. Для этого будет использован перехват данных программой Wireshark.

Шаг 1: Просмотрите длины и описания полей заголовков Ethernet II.

Шаг 2: Изучите кадры Ethernet в данных, перехваченных программой Wireshark.

Показанный ниже результат захвата данных в программе Wireshark отображает пакеты, которые были сгенерированы с помощью команды ping, отправленной с узла ПК на шлюз по умолчанию. В программе Wireshark включен фильтр для просмотра только ARP- и ICMP-протоколов. Сеанс начинается с ARP-запроса MAC-адреса маршрутизатора шлюза, за которым следуют четыре эхозапроса и ответа.

Шаг 3: Изучите содержание заголовков Ethernet II в ARP-запросе.

Адреса уровня 2 для кадра. Длина каждого адреса составляет 48 бит или 6 октетов, выраженных 12 шестнадцатеричными цифрами: 0-9, A-F. Общий формат — 12:34:56:78:9A:BC. Первые шесть шестнадцатеричных чисел обозначают производителя сетевой платы, а последние — ее серийный номер. Адрес назначения может быть адресом широковещательной рассылки (состоящим только из единиц) или одноадресной рассылки. Адрес источника всегда является адресом одноадресной рассылки.

**Часть 2: Перехват и анализ кадров Ethernet с помощью программы Wireshark**

Запустите и выполните вход в свою рабочую станцию CyberOps с использованием следующих учетных данных.

Откройте эмулятор терминала для запуска mininet и введите следующую команду в командной строке. В ответ на запрос введите cyberops в качестве пароля.

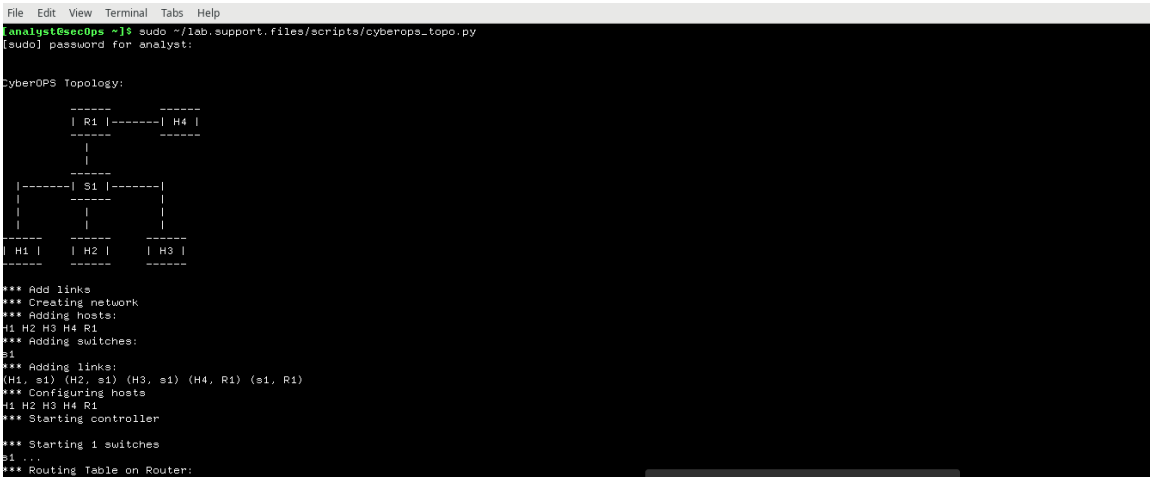


Рисунок 19 – Топология узлов

В командной строке mininet запустите окна терминала на узле H3.

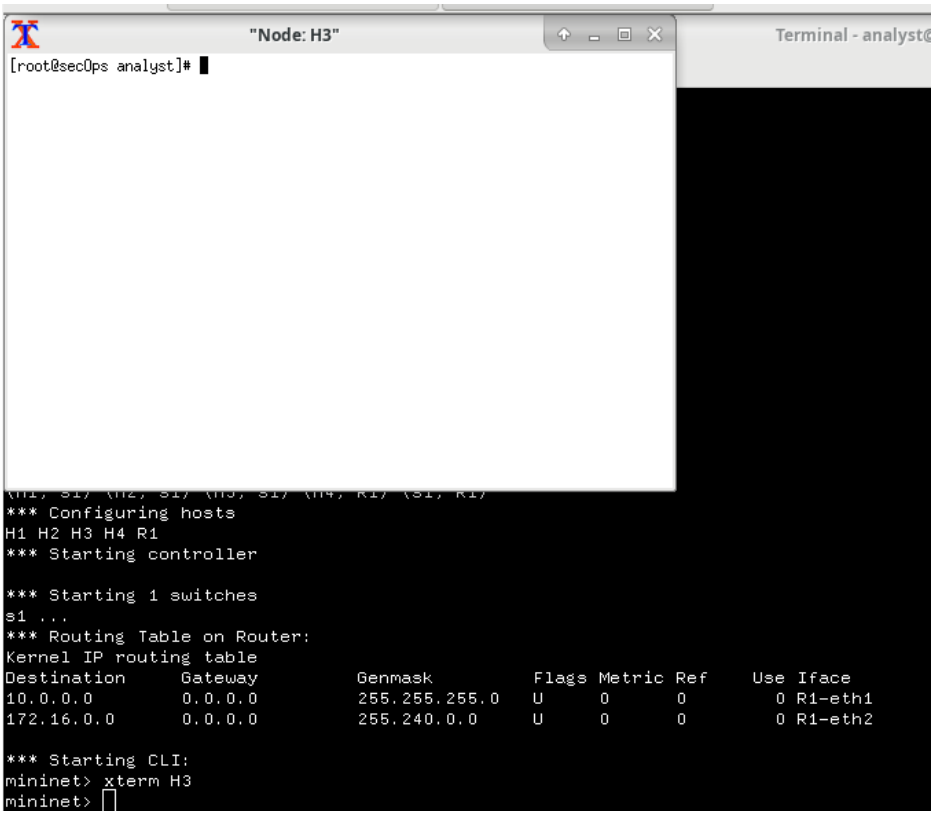


Рисунок 20 – Окно узла H3

В командной строке на узле H3 введите ifconfig для проверки IPv4-адреса и запишите MAC-адрес.

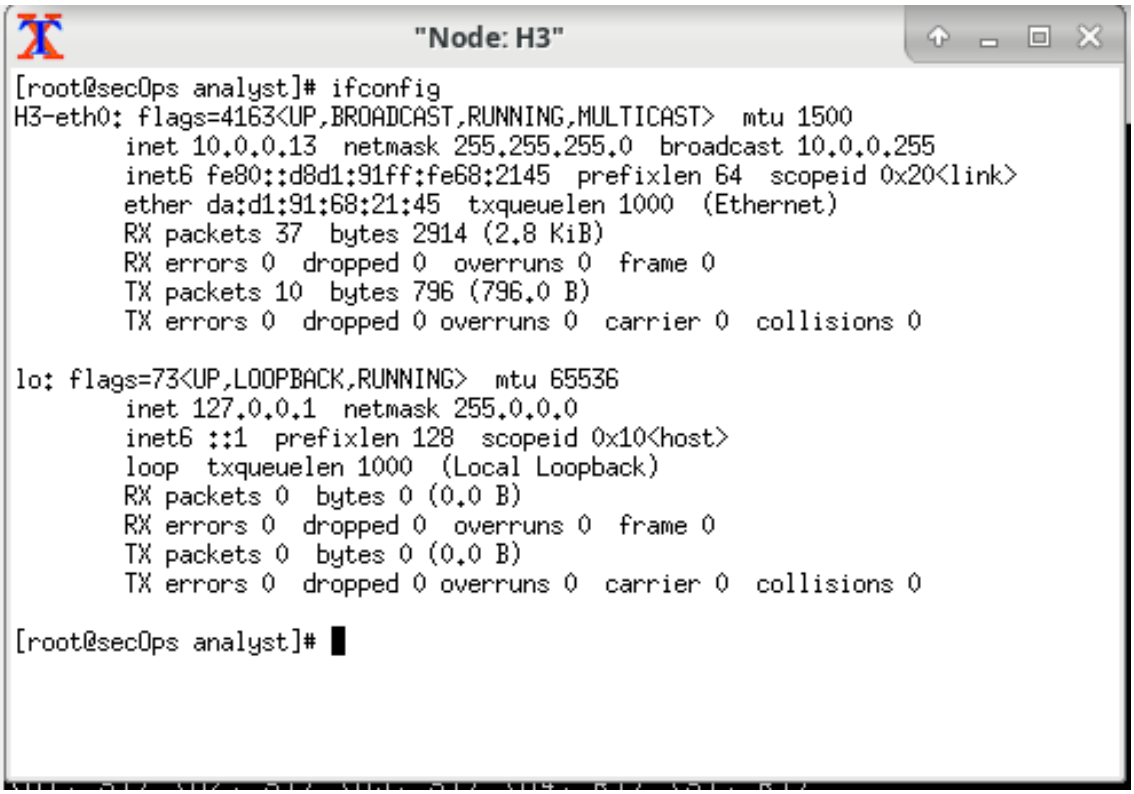


Рисунок 21 – Вывод сетевых интерфейсов узла H3

| Интерфейс узла | IP-адрес | MAC-адрес |
|---|---|---|
| H3-eth0 | 10.0.0.13 | da:d1:91:68:21:45 |

В командной строке на узле H3 введите netstat -r, чтобы показать информацию о шлюзе по умолчанию.

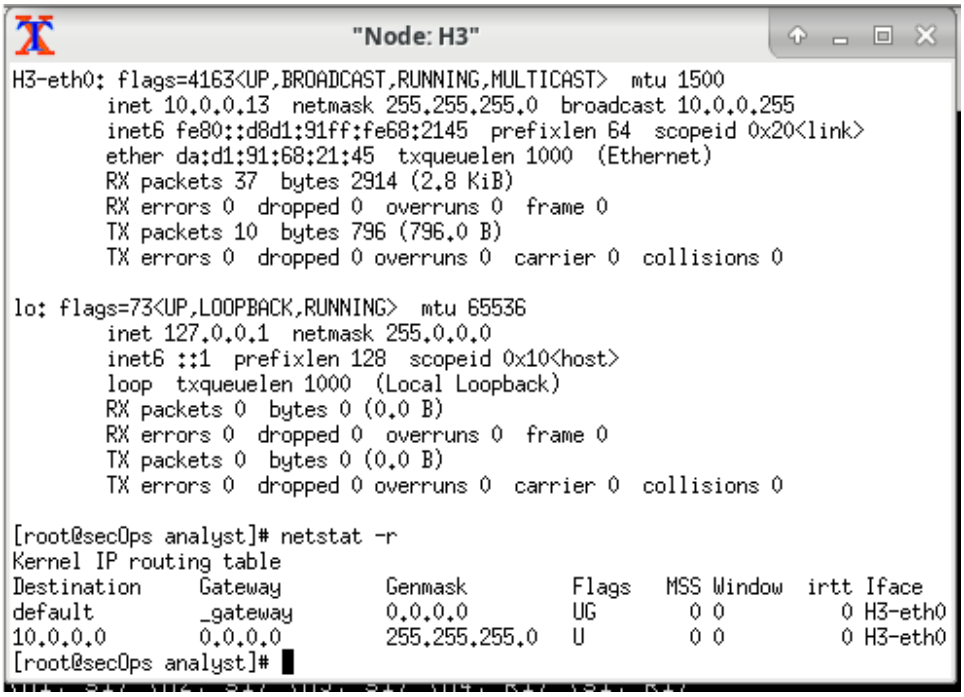

Рисунок 22 – Информация о шлюзе по умолчанию

В окне терминала для узла H3 введите arp -n, чтобы показать содержимое кэша ARP.

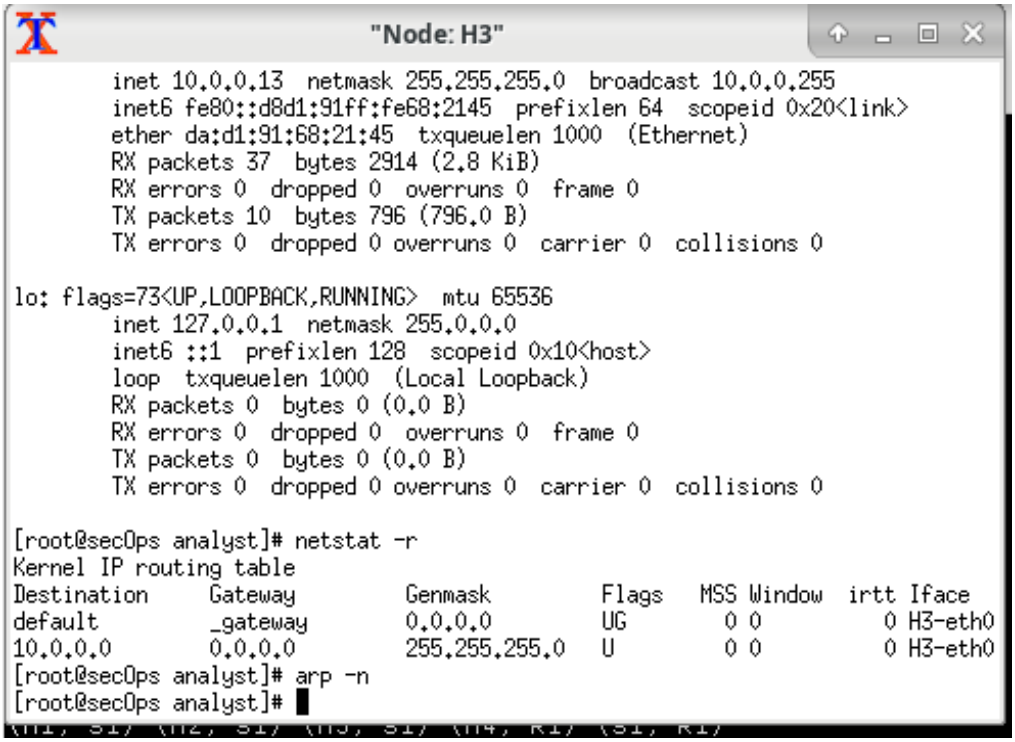

Рисунок 23 – Содержимое кэша ARP

Если в кэше есть какие-либо сведения ARP, очистите их, введя следующую команду: arp -d IPадрес. Повторите, пока все кэшированные сведения не будут удалены

В окне терминала для узла H3 откройте Wireshark и начните перехват пакетов для интерфейса H3-eth0.

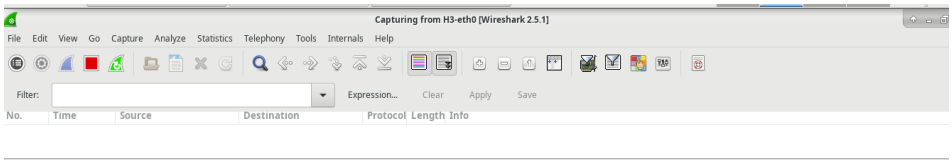


Рисунок 24 – Перехват пакетов для H3-eth0

В терминале на H3 отправьте эхозапрос на шлюз по умолчанию и остановитесь после отправки 5 пакетов эхозапроса.

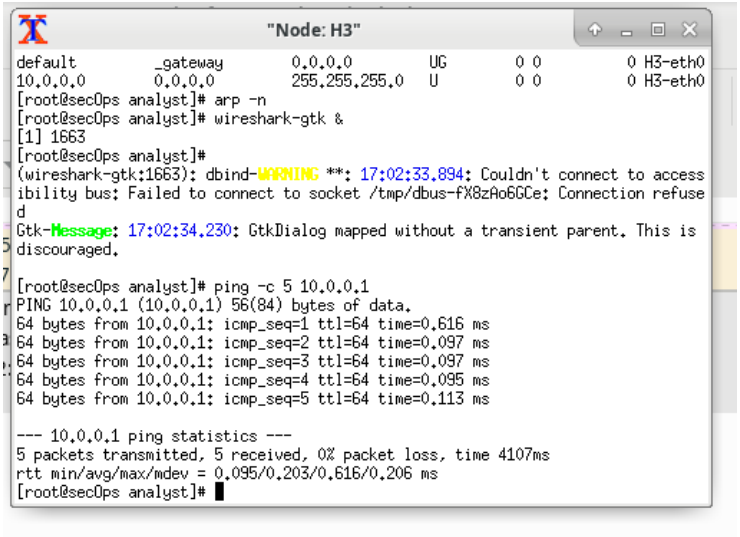


Рисунок 25 – Отправление эхозапросов на шлюз по умолчанию

После завершения команды ping остановите перехват данных программой Wireshark.

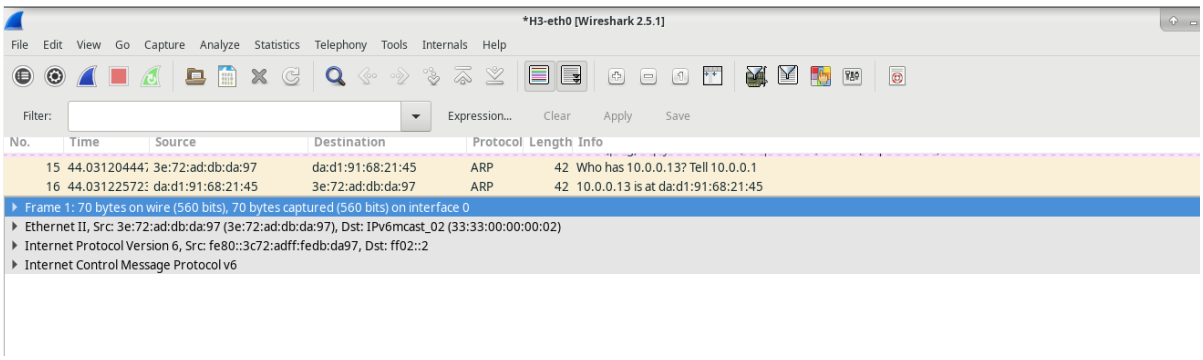


Рисунок 26 – Остановка перехвата пакетов

Примените фильтр icmp для перехваченного трафика, чтобы в результатах отображался только трафик ICMP.

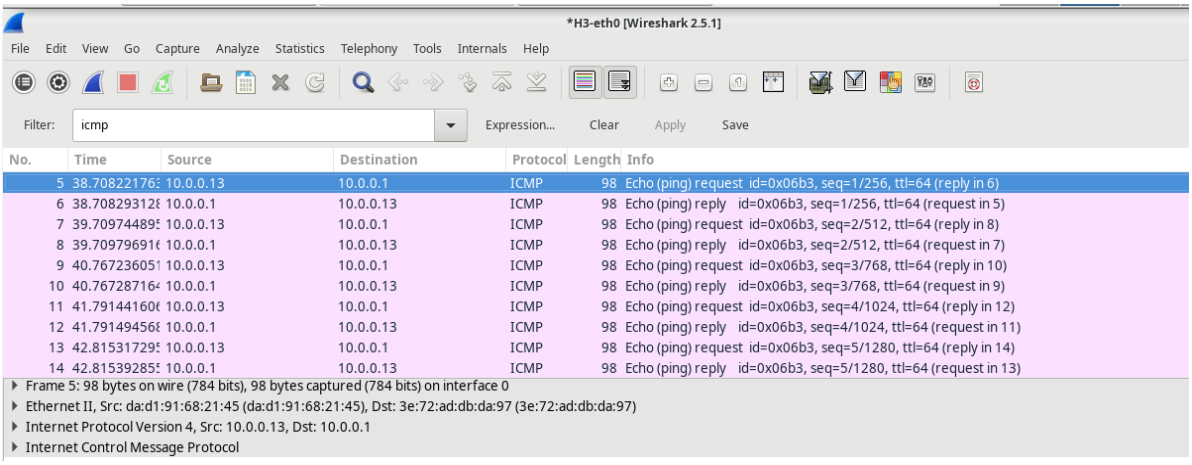


Рисунок 27 – Применение фильтра ICMP

На панели списка пакетов (верхний раздел) выберите первый указанный кадр. В столбце Info (Информация) появится значение Echo (ping) request (Эхозапрос с помощью команды ping). Строка станет синей.

Изучите первую строку на панели сведений о пакете в средней части экрана. В этой строке показана длина кадра (в данном примере 98 байт)

Вторая строка на панели Packet Details (Сведения о пакете) показывает, что это кадр Ethernet II. Также отображаются MAC-адреса источника и назначения.

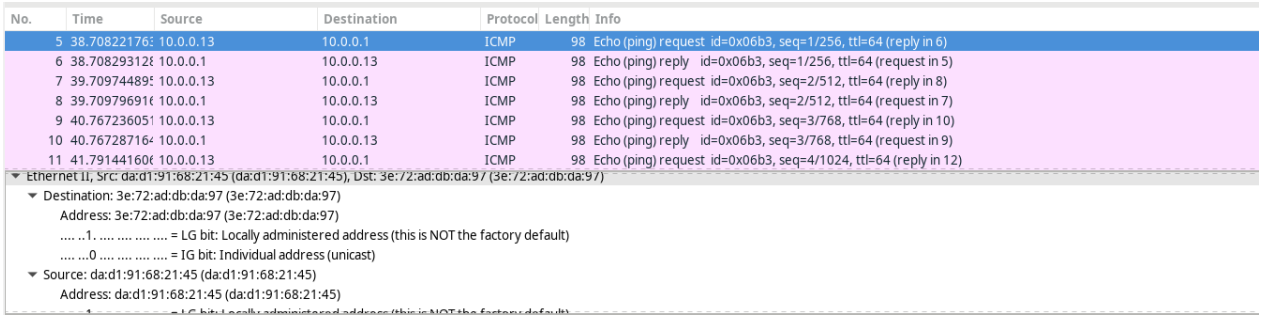


Рисунок 28 – Список пакетов

Для того чтобы получить больше информации о кадре Ethernet II, нажмите стрелку в начале второй строки.

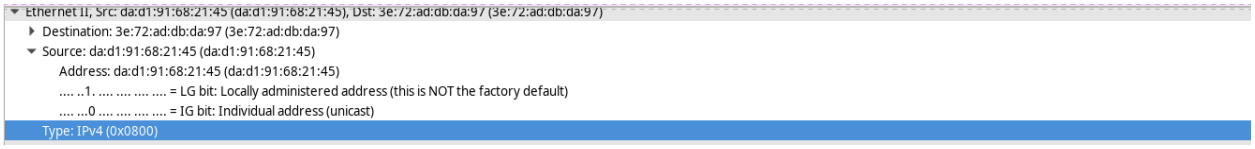


Рисунок 29 – Информация о кадре Ethernet II

Последние две строки среднего раздела содержат информацию о поле данных кадра. Обратите внимание на то, что данные содержат IPv4-адреса источника и назначения.


Рисунок 30 – IPv4-адреса источника и назначения

Для того чтобы выделить эту часть кадра (в шестнадцатеричной системе и ASCII) на панели отображения пакета в виде последовательности байтов (нижний раздел), щелкните любую строку в среднем разделе. Нажмите строку Internet Control Message Protocol в среднем разделе и посмотрите, что будет выделено на панели отображения пакета в виде последовательности байтов.

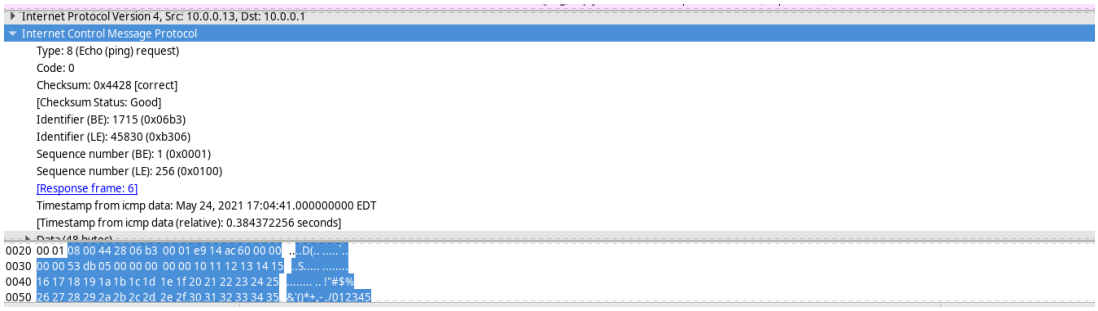


Рисунок 31 – Панель отображения пакетов

Нажмите пиктограмму Start Capture (Начать перехват), чтобы начать новый перехват данных в программе Wireshark. Откроется всплывающее окно с предложением сохранить предыдущие перехваченные пакеты в файл перед началом нового перехвата. Нажмите Continue without Saving (Продолжить без сохранения).

В окне терминала узла H3 отправьте 5 пакетов эхозапроса на 172.16.0.40.

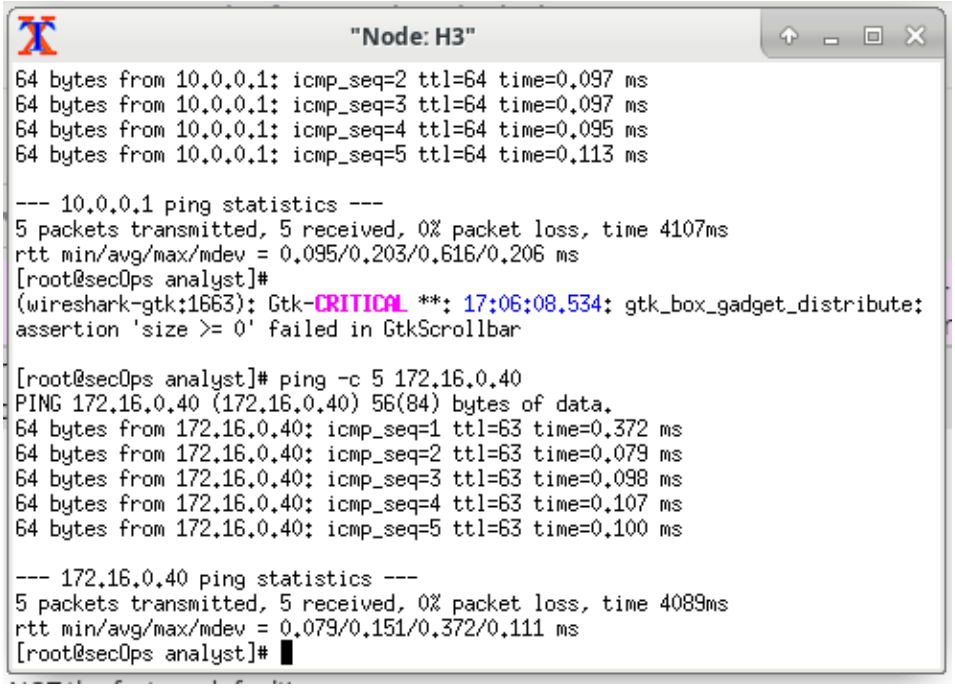


Рисунок 32 – Отправка пакетов эхозапроса

Остановите захват пакетов по завершении команд ping.

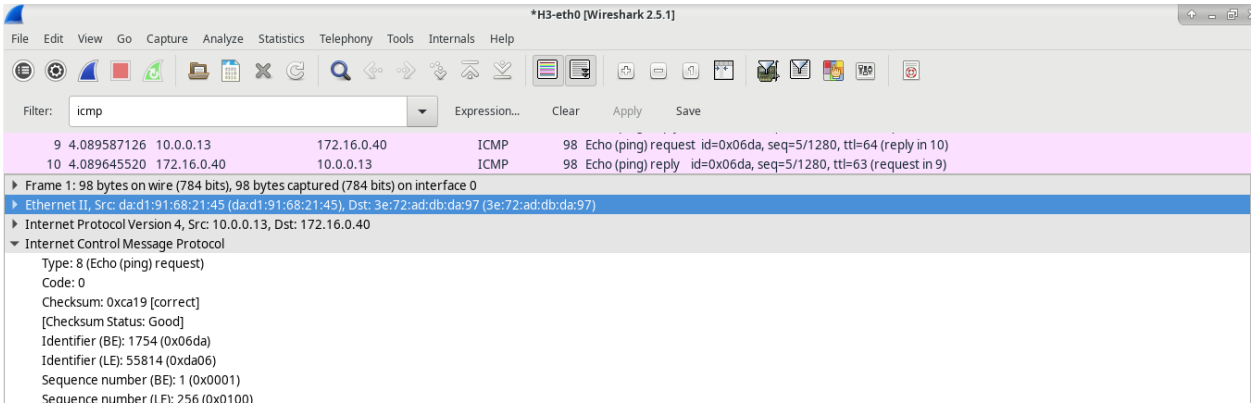


Рисунок 33 – Остановка захвата пакетов

### 4.5.2.4 Лабораторная работа. Наблюдение за процессом трехстороннего квитирования протокола TCP с помощью программы Wireshark

В данной лабораторной работе вам предстоит воспользоваться программой Wireshark для перехвата и изучения пакетов, которыми обмениваются браузер ПК, использующий HTTP-протокол, и веб-сервер, например www.google.com.

При первом запуске на узле приложения, например, HTTP или FTP, протокол TCP устанавливает между двумя узлами надежный TCP-сеанс с помощью трехстороннего квитирования.

**Часть 1: Подготовьте хосты для перехвата трафика**

Запустите виртуальную машину CyberOps. Войдите в систему под именем пользователя analyst с паролем cyberops.

Запустите Mininet.

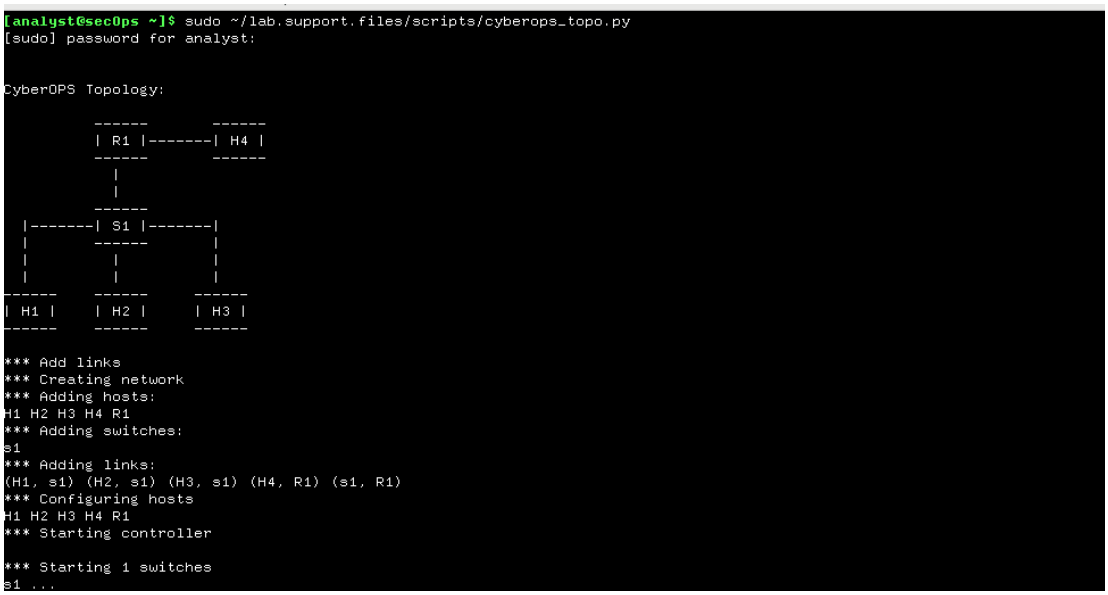


Рисунок 34 – Запуск Mininet

Запустите хост H1 и H4 в Mininet.

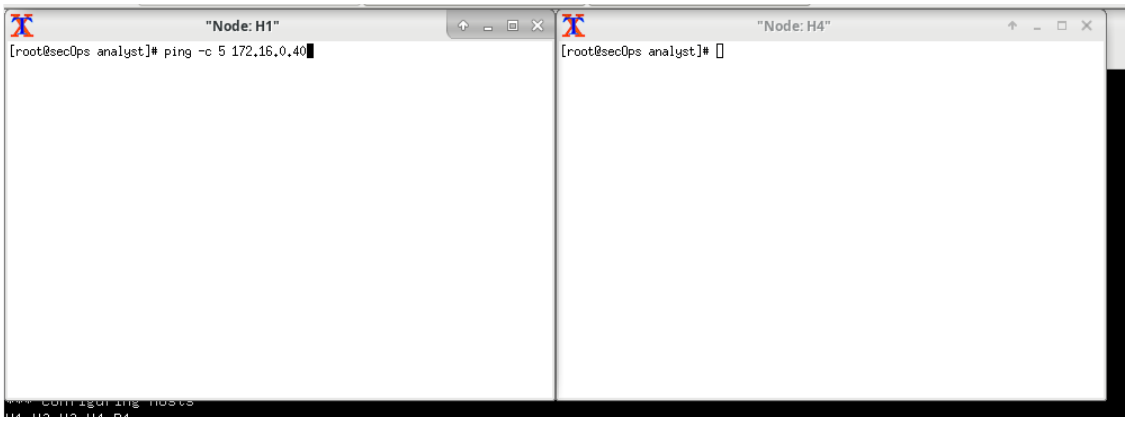


Рисунок 35 – Запуск хостов H1 и H4 в Mininet

Запустите веб-сервер на H4.

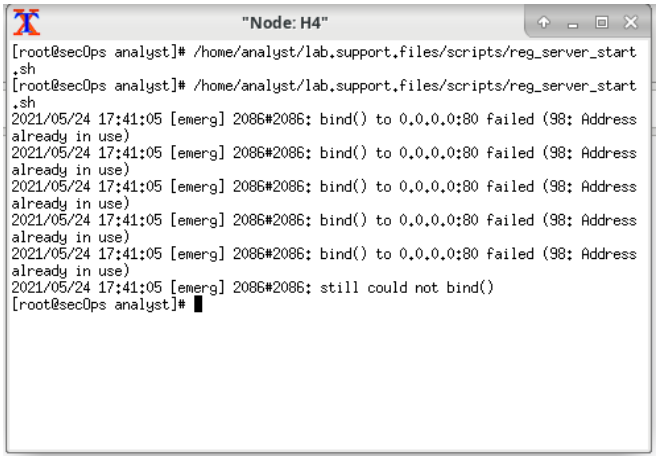


Рисунок 36 – Запуск веб-сервера на H4

Запустите веб-обозреватель на H1. Это займет несколько минут.

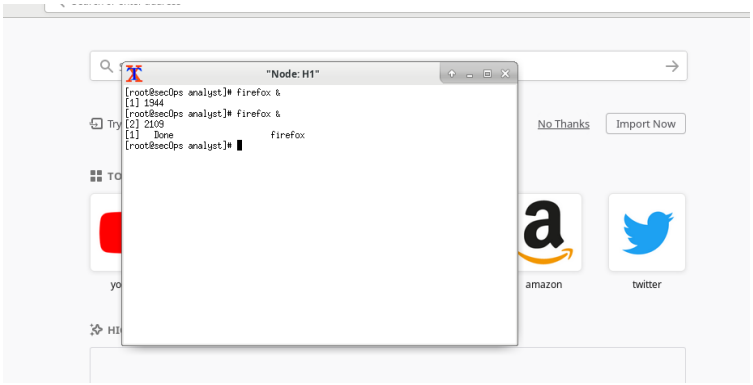


Рисунок 37 – Запуск веб-обозревателя на H1

Когда откроется окно Firefox, запустите сеанс tcpdump в терминале Узел H1 и отправьте выходные данные в файл с именем capture.pcap. С помощью параметра -v можно отслеживать ход выполнения. Этот перехват будет остановлен после 50 пакетов, так как указан параметр -c 50.

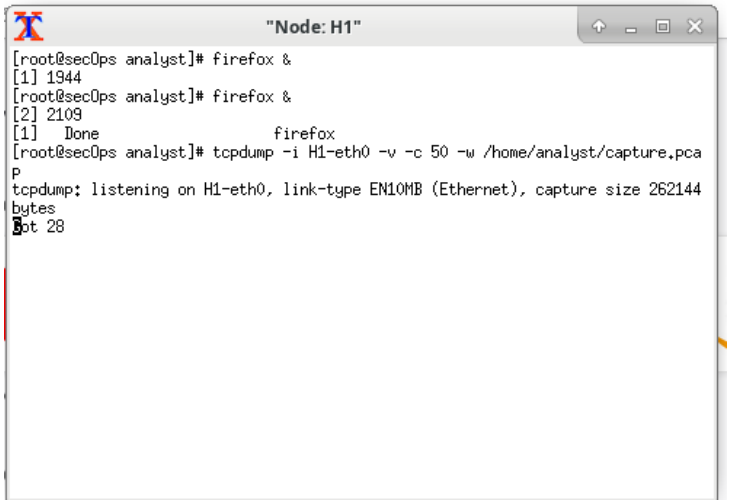


Рисунок 38 – Работа сеанса TCPDump

После запуска служебной программы tcpdump быстро перейдите по адресу 172.16.0.40 в веб-обозревателе Firefox.


Рисунок 39 – Веб-обозреватель программы tcpdump

**Часть 2: Анализ пакетов с помощью программы Wireshark**

Нажмите ENTER (ВВОД), чтобы вывести на экран приглашение. Запустите программу Wireshark на узле H1. Нажмите кнопку OK в ответ на предупреждение относительно запуска Wireshark в качестве суперпользователя.

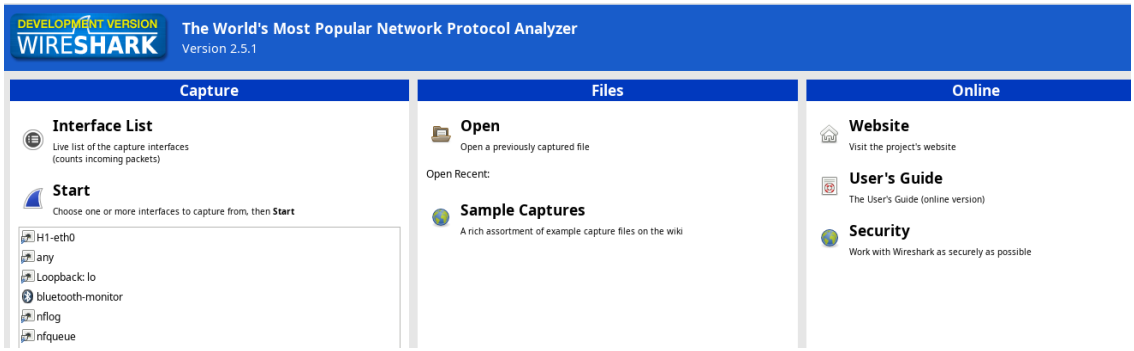


Рисунок 40 – Запуск программы Wireshark на узле H1

В программе Wireshark щелкните File (Файл) > Open (Открыть). Выберите сохраненной файл pcap, расположенный по адресу /home/analyst/capture.pcap.

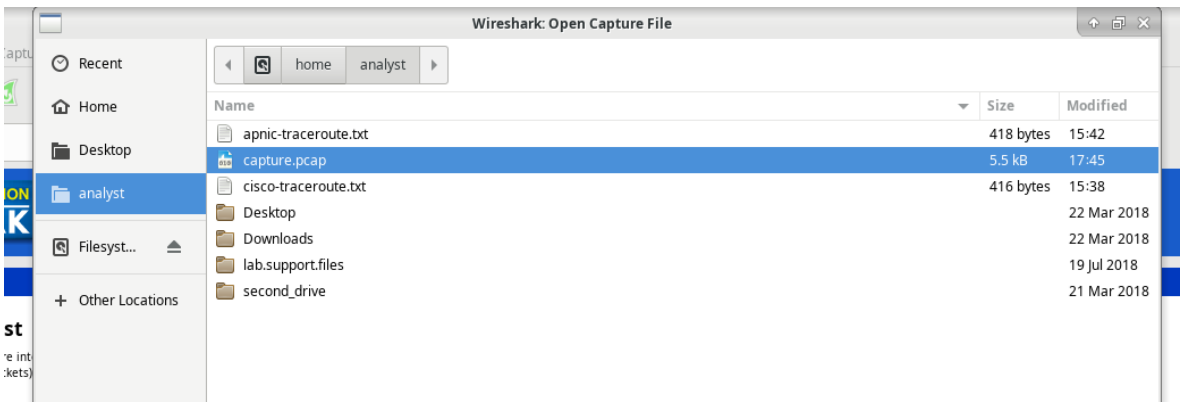


Рисунок 41 – Файл pcap

Примените фильтр tcp к собранным данным. В этом примере первые три кадра представляют собой интересующий нас трафик.

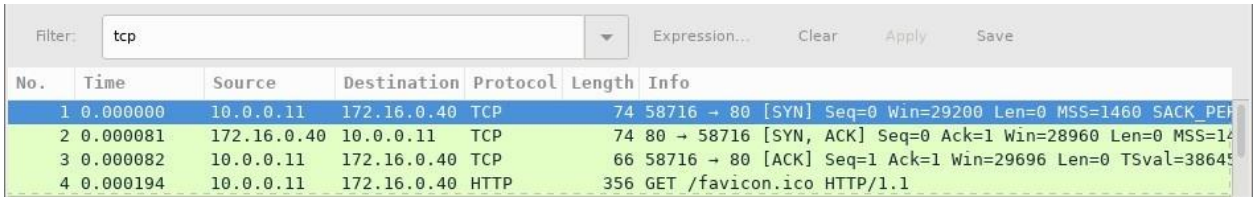


Рисунок 42 – Применение фильтра tcp

В этом примере кадр 1 представляет собой начало трехстороннего квитирования между ПК и сервером на H4. При необходимости на панели списка пакетов (верхний раздел основного окна) выберите первый пакет.

На панели сведений о пакетах нажмите стрелку слева от строки Transmission Control Protocol (Протокол управления передачей данных) в области подробной информации о пакете, чтобы увидеть подробную информацию о TCP. Найдите информацию о портах источника и назначения.

Нажмите стрелку слева от строки Flags (Флаги). Значение 1 означает, что флаг установлен. Найдите флаг, который устанавливается в этом пакете.

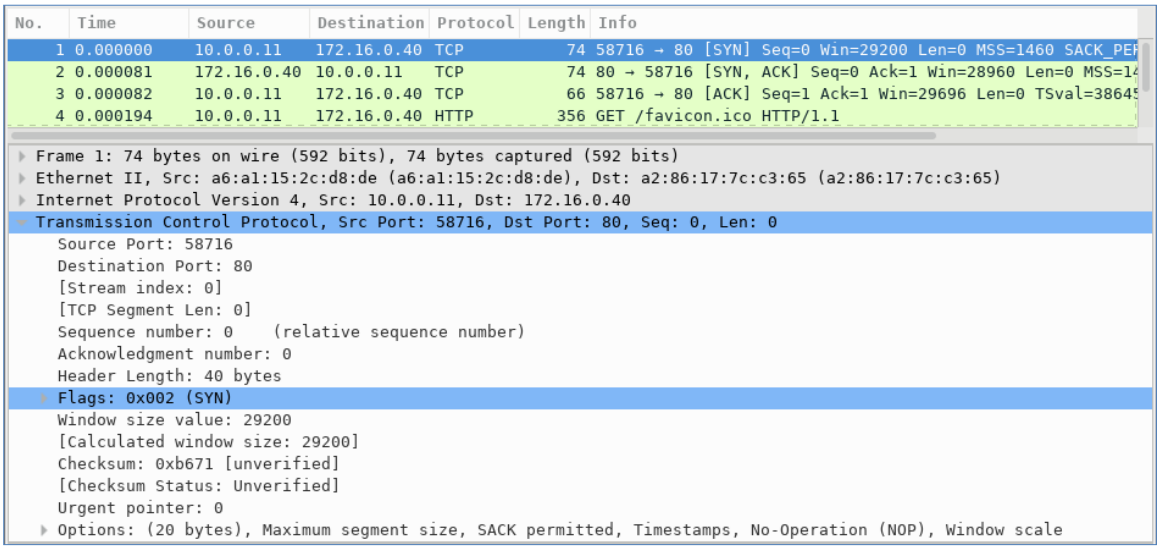


Рисунок 43 – Информация о портах источника и назначения

Выберите следующий пакет трехстороннего квитирования. В данном примере это кадр 2. Это веб-сервер, отвечающий на исходный запрос для начала сеанса.

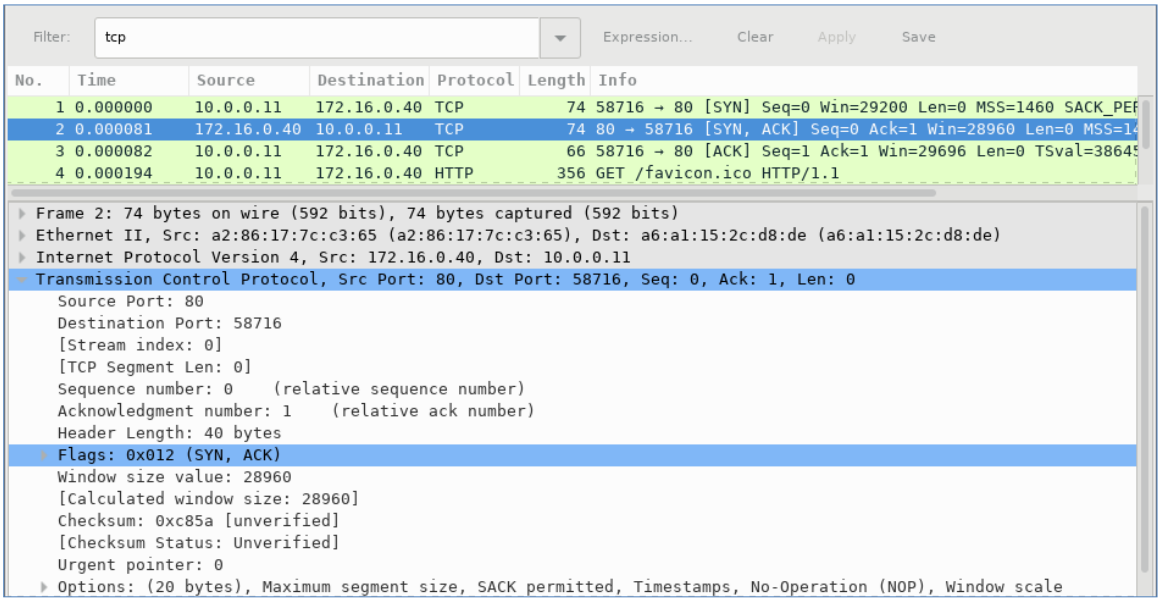


Рисунок 44 – Веб-сервер

Наконец, выберите третий пакет трехстороннего квитирования.

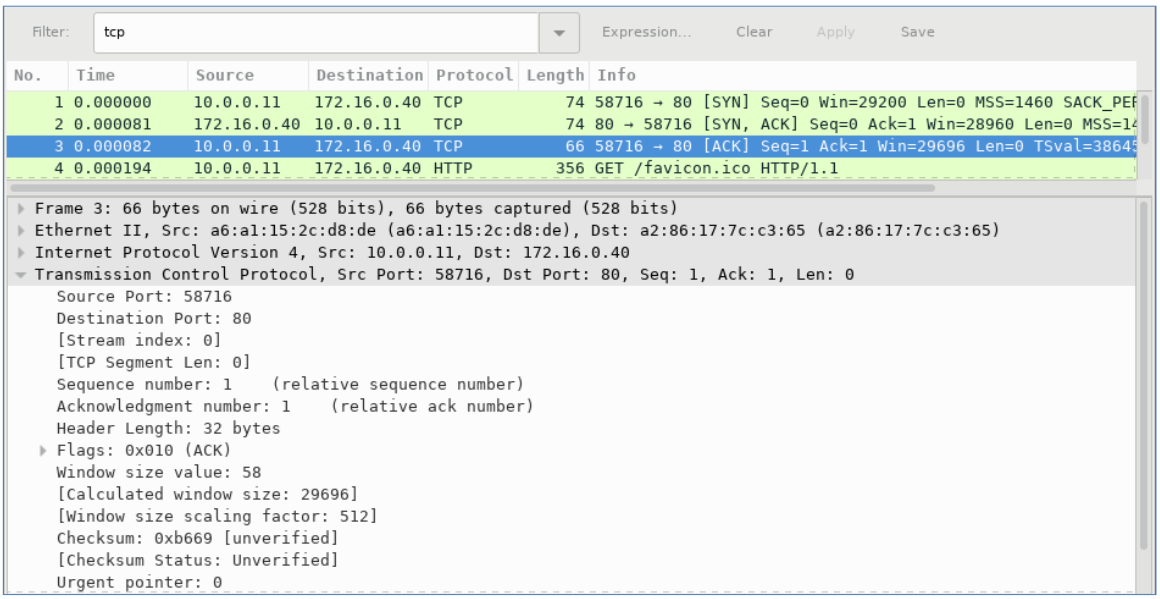


Рисунок 45 – Выбор третьего пакета

**Часть 3: Просмотр пакетов с помощью программы tcpdump**

Откройте новое окно терминала, введите man tcpdump. Возможно, потребуется нажать клавишу ENTER (ВВОД), чтобы увидеть командную строку. На страницах справки, доступных в операционной системе Linux, найдите и прочитайте сведения о вариантах выбора нужной информации из файла pcap.


Рисунок 46 – Сведения о вариантах выбора

Перейдите к терминалу, используемому для запуска Mininet. Завершите работу Mininet, введя команду quit в главном окне терминала виртуальной машины CyberOps.

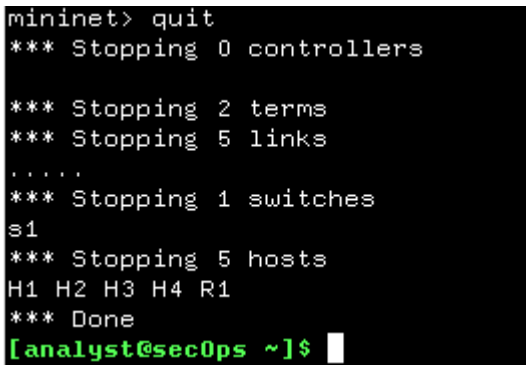


Рисунок 47 – Завершение работы Mininet

После выхода из Mininet введите sudo mn -c для очистки процессов, запущенных Mininet. При появлении соответствующего запроса введите пароль cyberops.


Рисунок 48 – Очистка процессов Mininet

### 4.5.2.10 Лабораторная работа. Изучение Nmap

Сканирование портов обычно является частью разведывательной атаки. Существует множество методов сканирования портов, которые могут использоваться злоумышленниками. Мы будем изучать использование утилиты Nmap. Nmap - утилита с большим набором возможностей, предназначенная для обнаружения сетевых ресурсов и аудита средств безопасности.

**Часть 1: Изучение Nmap**

Запустите виртуальную машину рабочей станции CyberOps.

Откройте терминал.

В командной строке терминала введите man nmap.

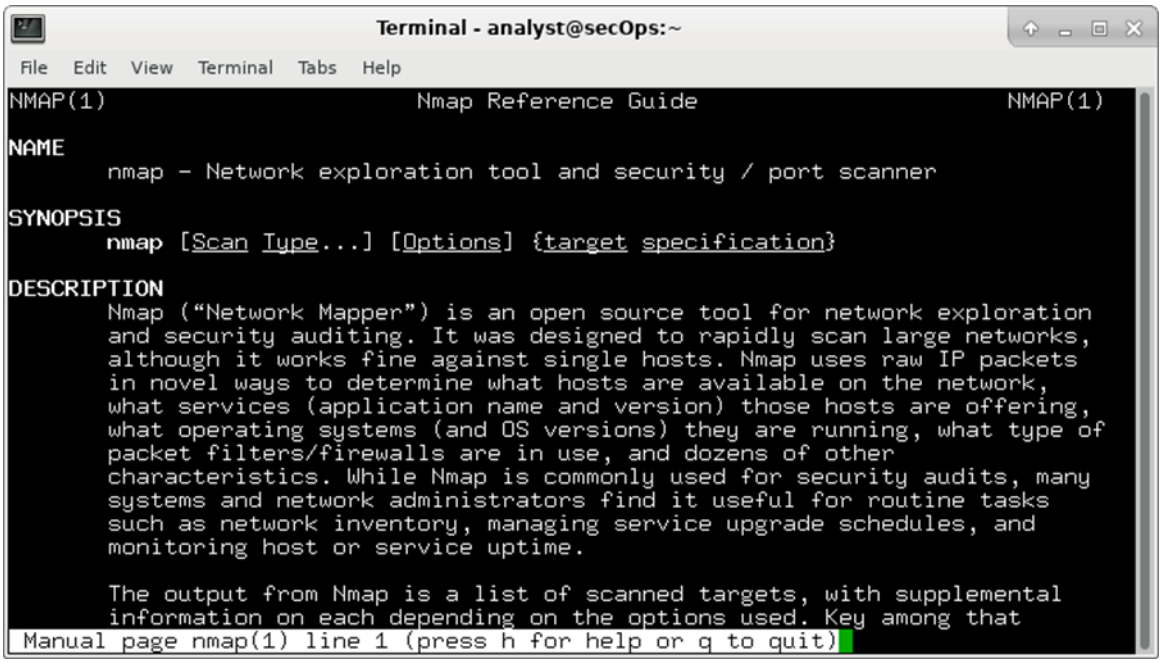


Рисунок 49 – Команда man nmap

На странице справки можно использовать клавиши со стрелками вверх и вниз для прокрутки страниц. Можно также нажать клавишу пробела, чтобы перейти вперед на одну страницу. Для поиска случаев использования определенного слова или фразы введите косую черту (/) или вопросительный знак (?), а следом слово или фразу. При использовании косой черты выполняется поиск вперед по документу, а вопросительного знака — поиск назад по документу. Ключ n переводит к следующему совпадению.

Введите /example и нажмите клавишу ввода. Будет выполнен поиск слова пример вперед по странице справки.

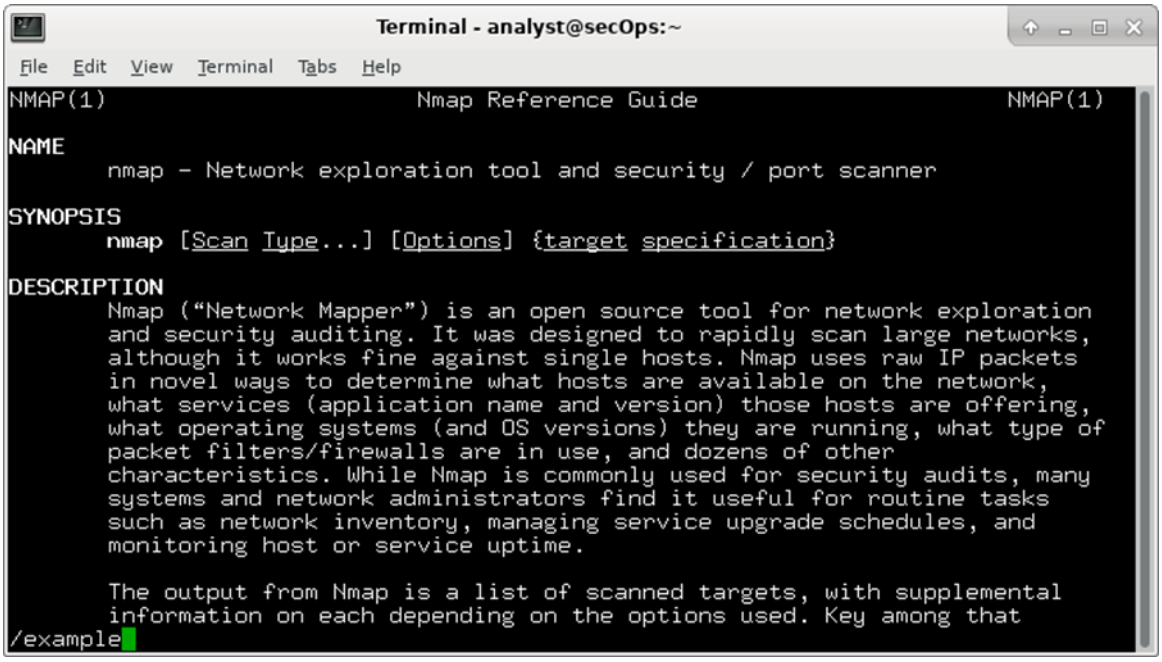


Рисунок 50 – Ввод команды для поиска

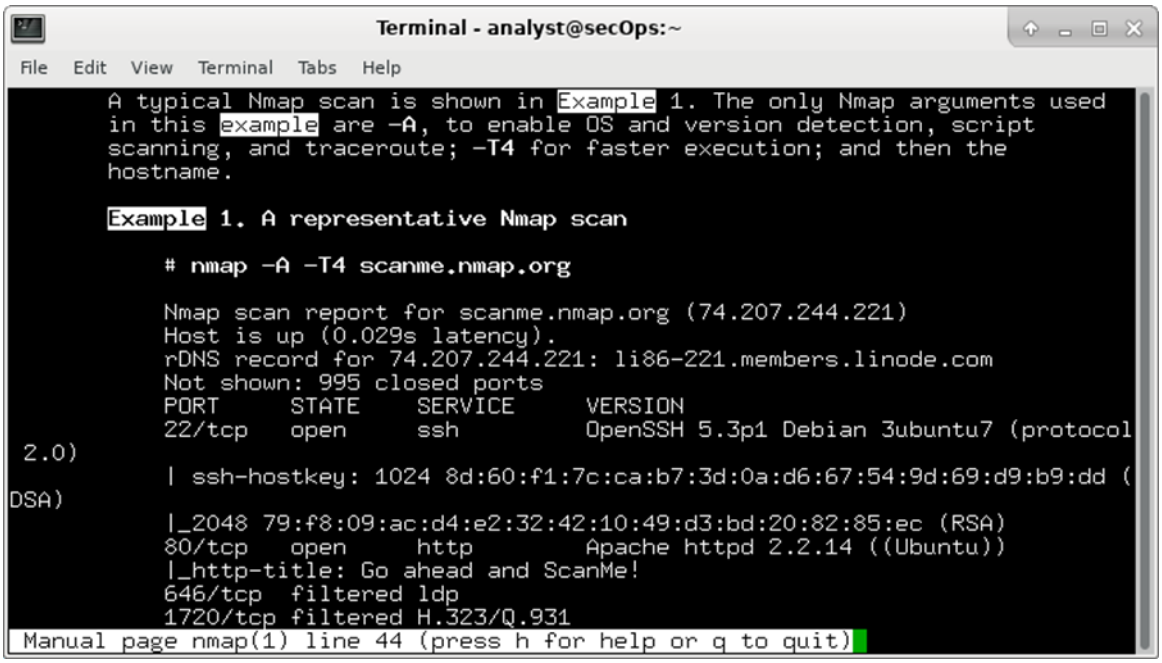


Рисунок 51 – Результат поиска слова example

**Часть 2: Проверка на наличие открытых портов**

При необходимости откройте терминал на виртуальной машине. В командной строке введите nmap -A -T4 localhost. В зависимости от локальной сети и устройств сканирование может занять от нескольких секунд до нескольких минут.

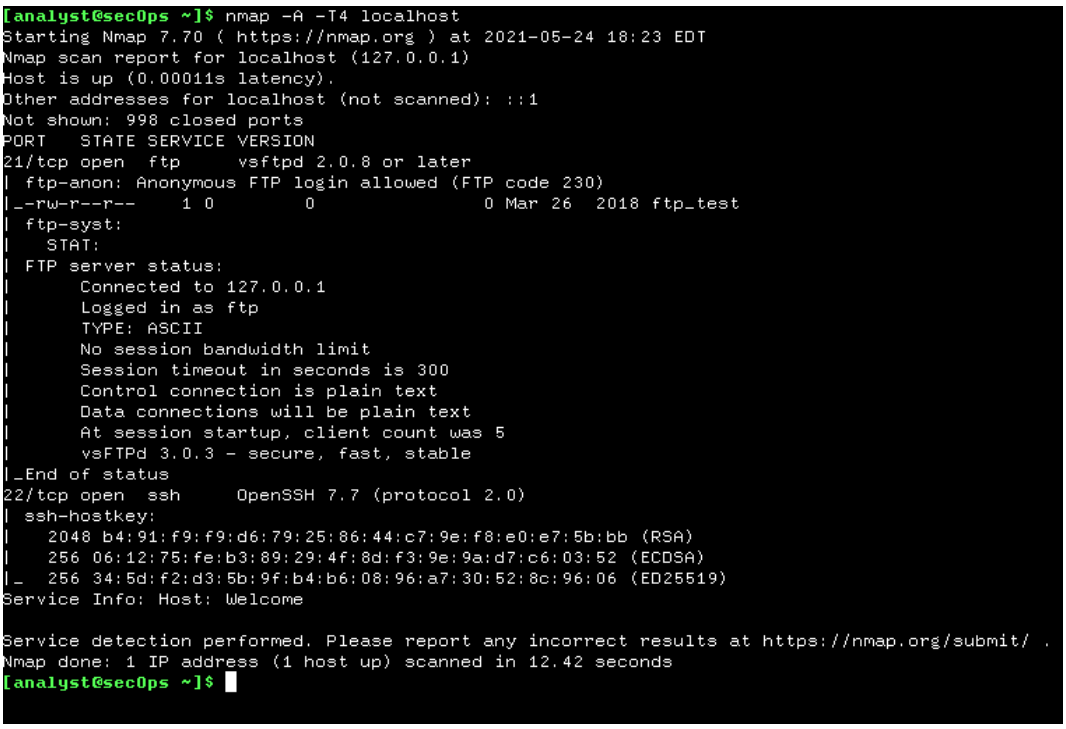


Рисунок 52 – Вывод команды nmap -A -T4 localhost

В командную строку терминала введите ifconfig, чтобы определить IP-адрес и маску подсети для этого хоста.

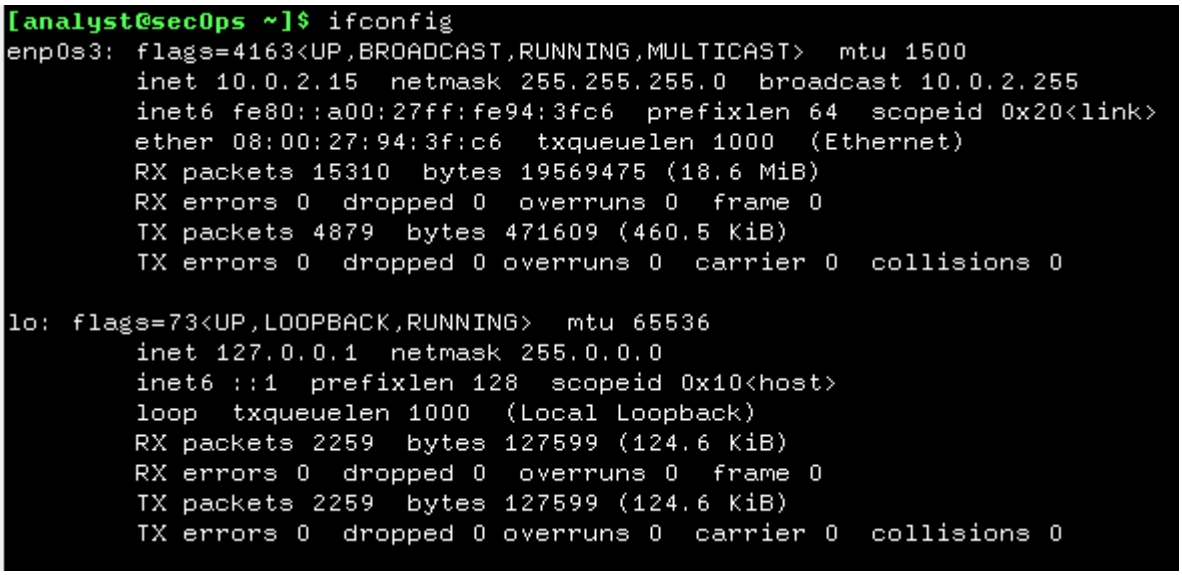


Рисунок 53 – Определение IP-адреса и маски хоста

Для того чтобы найти другие хосты в этой локальной сети, введите nmap --T4 сетевой адрес / префикс.

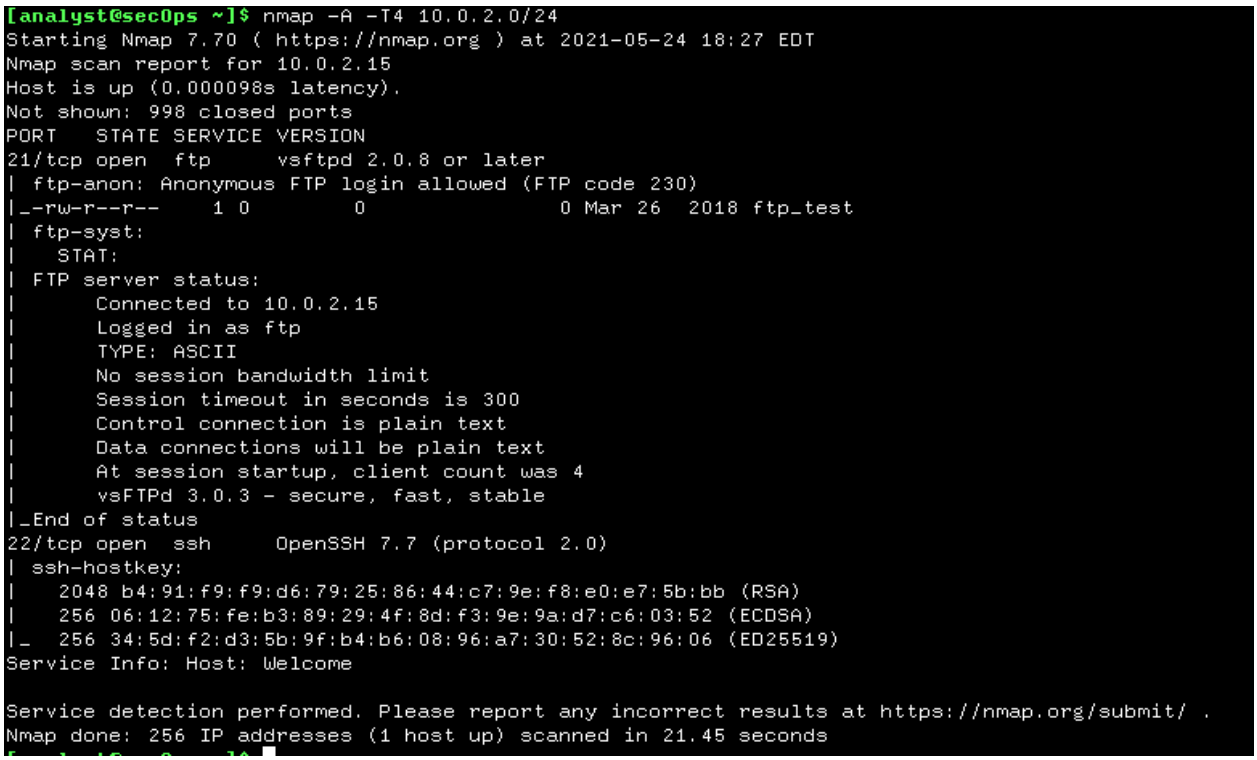


Рисунок 54 – Вывод команды nmap -A -T4 10.0.2.0/24

Введите в командной строке терминала nmap -A -T4 scanme.nmap.org.

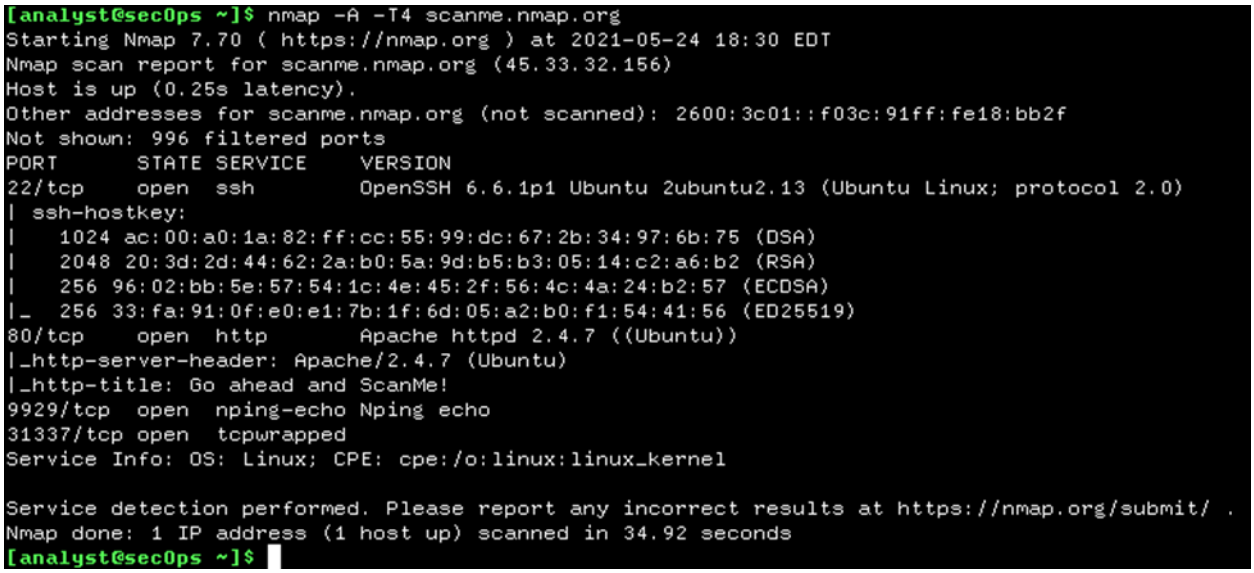


Рисунок 55 – Вывод команды nmap -A -T4 scanme.nmap.org

**4.6.2.7 Лабораторная работа. Изучение перехваченных пакетов DNS и UDP с помощью программы Wireshark.**

**Часть 1: Запись данных IP-конфигурации ВМ**

В части 1 вы воспользуетесь командами на ВМ рабочей станции CyberOps, чтобы найти и записать MAC-адрес и IP-адрес сетевой интерфейсной платы своей ВМ, IP-адрес указанного шлюза по умолчанию и IP-адрес DNS-сервера, указанного для ПК. Запишите эти данные в приведенную ниже таблицу. Они потребуются вам для анализа пакетов в следующих частях лабораторной работы. IP-адрес MAC-адрес IP-адрес шлюза по умолчанию IP-адрес DNS-сервера.

| | |
|---|---|
| IP-адрес | 10.0.2.15 |
| MAC-адрес | 08:00:27:91:a4:d8 |
| IP-адрес шлюза по умолчанию | 8.8.4.4 |
| IP-адрес DNS-сервера | _gateway |

Откройте терминал на ВМ. Введите ifconfig в командную строку, чтобы отобразить сведения об интерфейсе.

```
[analyst@secOps ~]$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe91:a4d8  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:91:a4:d8  txqueuelen 1000  (Ethernet)
        RX packets 34478  bytes 29740305 (28.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 21618  bytes 2337283 (2.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8498  bytes 560366 (547.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8498  bytes 560366 (547.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[analyst@secOps ~]$
```

Рисунок 56 – Выполнение команды ifconfig

В командной строке терминала введите cat /etc/resolv.conf для определения DNS-сервера.

```
[analyst@secOps ~]$  cat /etc/resolv.conf
# Resolver configuration file.
# See resolv.conf(5) for details.
nameserver 8.8.4.4
nameserver 209.165.200.235
[analyst@secOps ~]$
```

Рисунок 57 – Выполнение команды cat /etc/resolv.conf

В командной строке терминала введите netstat -r для отображения таблицы IP-маршрутизации на IP-адрес шлюза по умолчанию.

```
[analyst@secOps ~]$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         _gateway        0.0.0.0         UG        0 0          0 enp0s3
10.0.2.0        0.0.0.0         255.255.255.0   U         0 0          0 enp0s3
_gateway        0.0.0.0         255.255.255.255 UH        0 0          0 enp0s3
[analyst@secOps ~]$
```

Рисунок 58 – Выполнение команды netstat -r

**Часть 2: Перехват запросов и ответов DNS с помощью программы Wireshark**

В окне терминала запустите программу Wireshark и нажмите кнопку ОК в ответ на приглашение.

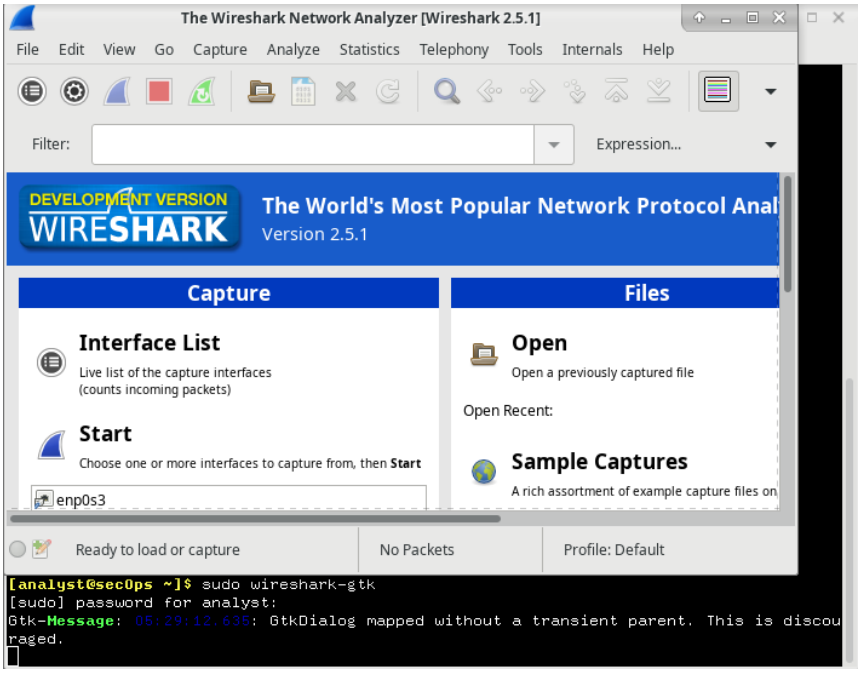


Рисунок 59 – Запуск Wireshark

В окне Wireshark выберите enp0s3 из списка интерфейсов и нажмите кнопку Start (Пуск).

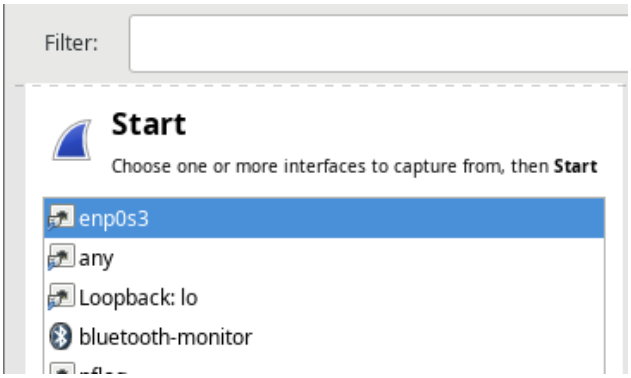


Рисунок 60 – Выбор enp0s3

Выбрав нужный интерфейс, нажмите Start (Пуск), чтобы начать захват пакетов.

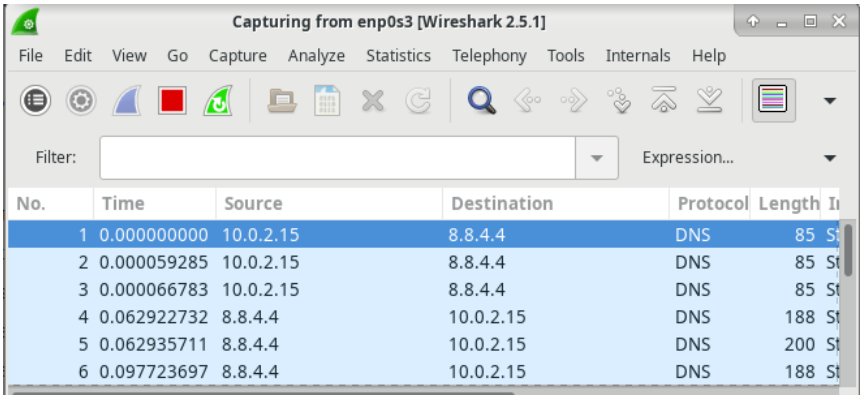


Рисунок 61 – Захват пакетов

Откройте веб-обозреватель и введите адрес www.google.com. Нажмите клавишу Enter (Ввод), чтобы продолжить.

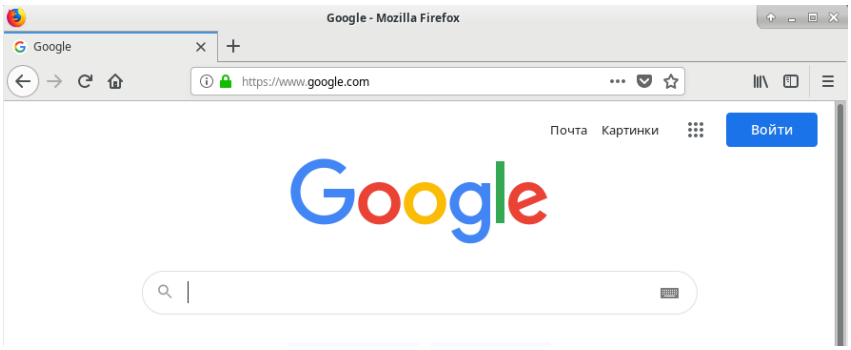


Рисунок 62 – Адрес www.google.com в веб-браузере

Как только откроется главная страница Google, нажмите кнопку Stop (Остановить), чтобы остановить перехват данных программой Wireshark.

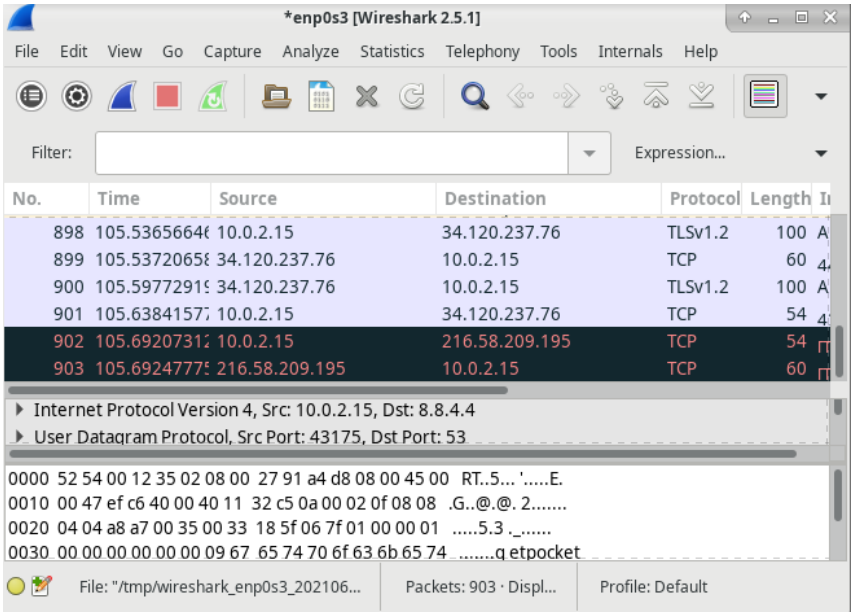


Рисунок 63 – Остановка перехвата данных

**Часть 3: Анализ перехваченных пакетов DNS или UDP**

В главном окне программы Wireshark введите dns в поле Filter (Фильтр). Нажмите Apply (Применить).

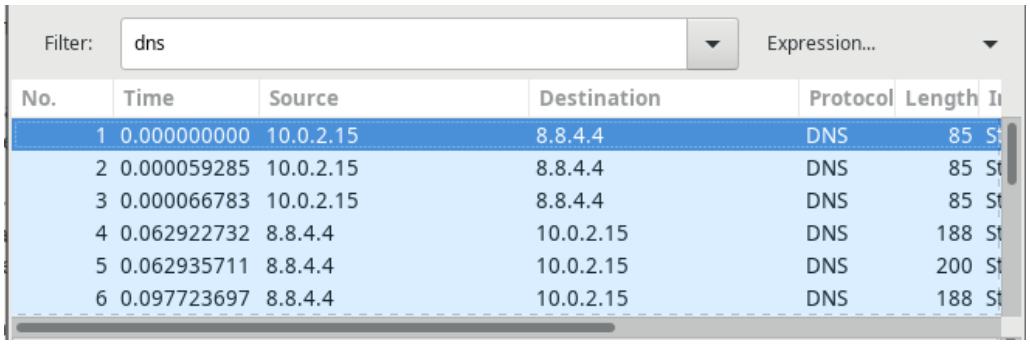


Рисунок 64 – Применение фильтра dns

Примечание. Если после применения фильтра DNS вы не видите никаких результатов, закройте веб-обозреватель. В окне терминала введите ping www.google.com в качестве альтернативы браузеру.

На панели списка захваченных пакетов (верхний раздел) в главном окне программы найдите пакет с информацией Standard query (Стандартный запрос) и A www.google.com.

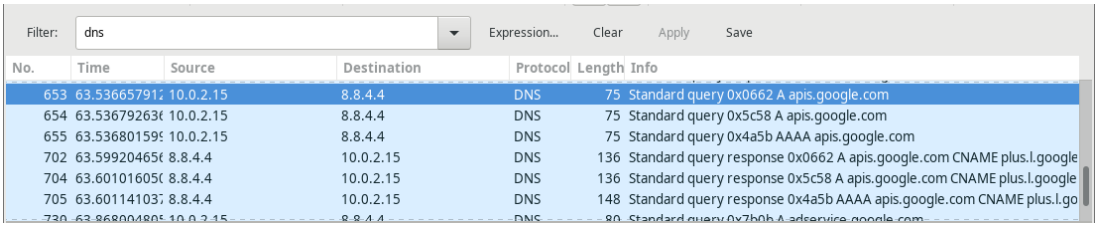


Рисунок 65 – Пакет с информацией Standard query

Поля протокола, выделенные серым, отображаются на панели сведений о пакетах (средний раздел) главного окна.

Как показано в первой строке на панели сведений о пакетах, кадр 22 содержал 74 байта данных во время передачи. Это число байтов, потребовавшееся для отправки DNS-запроса на именованный сервер, запросивший IP-адреса сайта www.google.com. Если используется другой веб-адрес, например, www.cisco.com, количество байтов может быть иным.

Строка Ethernet II содержит MAC-адреса источника и места назначения. MAC-адрес источника принадлежит вашей ВМ как источнику DNS-запроса. MAC-адрес назначения — это шлюз по умолчанию, поскольку это последняя остановка перед выходом запроса из локальной сети.

В строке Internet Protocol Version 4 перехваченные программой Wireshark данные IP-пакета показывают, что IP-адрес источника данного DNS-запроса — 192.168.1.19, а IP-адрес назначения — 192.168.1.1. В данном примере адрес назначения — это шлюз по умолчанию. В данной сети шлюзом по умолчанию является маршрутизатор.

Щелкните стрелку рядом с протоколом пользовательских датаграмм,

чтобы просмотреть сведения. Заголовок UDP имеет только четыре поля: порт источника, порт назначения, длина и контрольная сумма. Как показано ниже, длина каждого поля в заголовке UDP составляет всего 16 бит.

Щелкните стрелку рядом с протоколом пользовательских датаграмм, чтобы просмотреть сведения. Обратите внимание на то, что отображаются всего четыре поля. Номер порта источника в данном примере — 39964. Порт источника был случайным образом сформирован ВМ с использованием незарезервированных номеров портов. Порт назначения — 53. Порт 53 — это хорошо известный порт, зарезервированный для использования с DNS. DNS-серверы прослушивают порт 53 для получения DNS-запросов от клиентов.

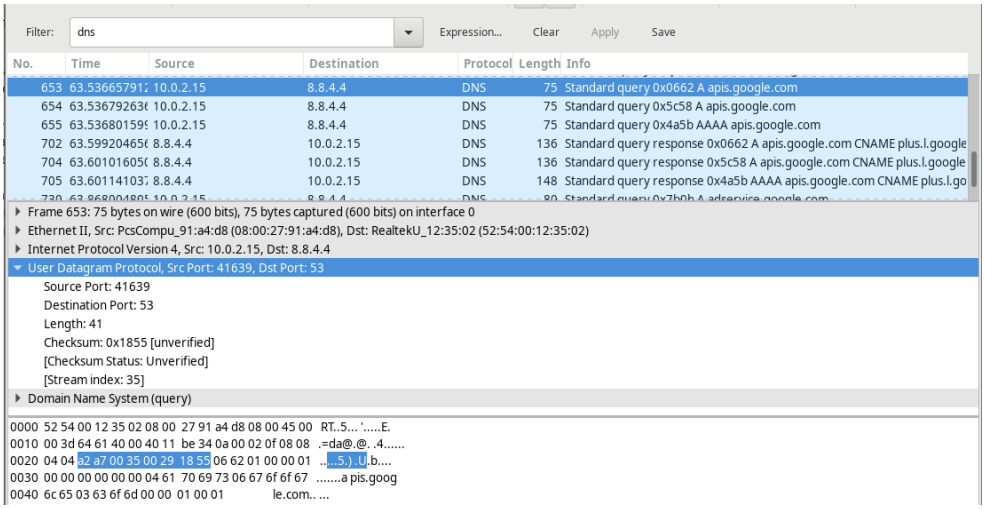


Рисунок 66 – Порт назначения 53

В данном примере длина сегмента UDP составляет 40 байт. Длина сегмента UDP в данном примере может быть иной. 8 из 40 байт используются в качестве заголовка. Остальные 32 байта используются данными DNS-запроса. На следующем рисунке показаны 32 байта данных DNS запроса на панели отображения байтов пакета (нижний раздел) главного окна Wireshark.

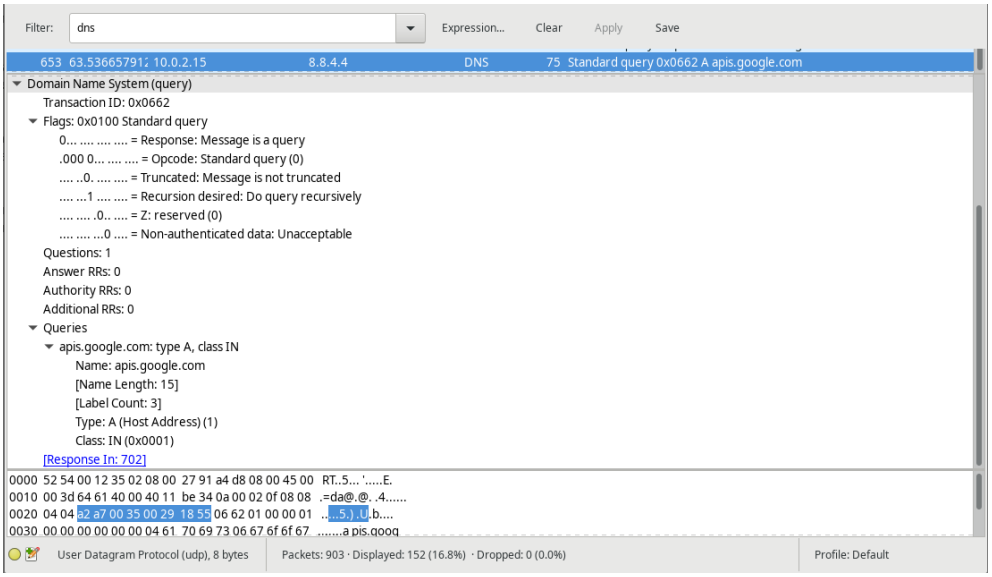


Рисунок 67 – Данные DNS запроса