БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Кафедра интеллектуальных информационных технологий

ОТЧЁТ  
по лабораторной работе №8  
по дисциплине

«Наблюдение за стеком TCP/IP»

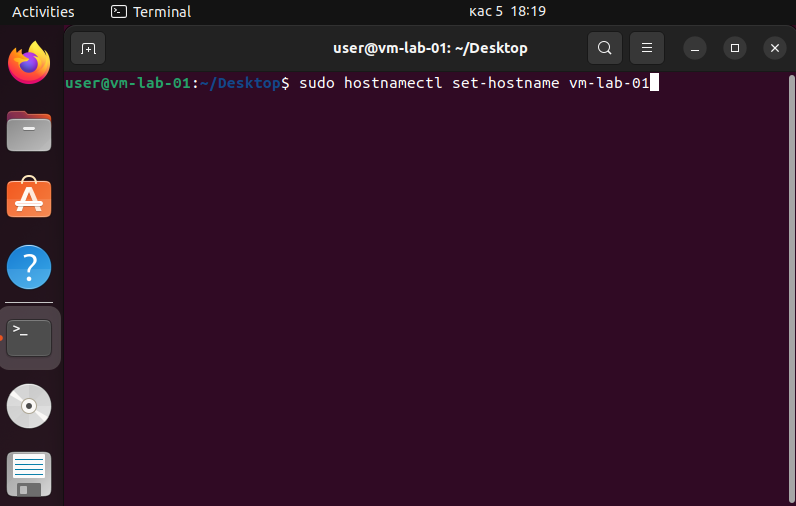
Выполнил студент гр. 321701  
Романов К.В.  
Проверил  
Сальников Д. А.

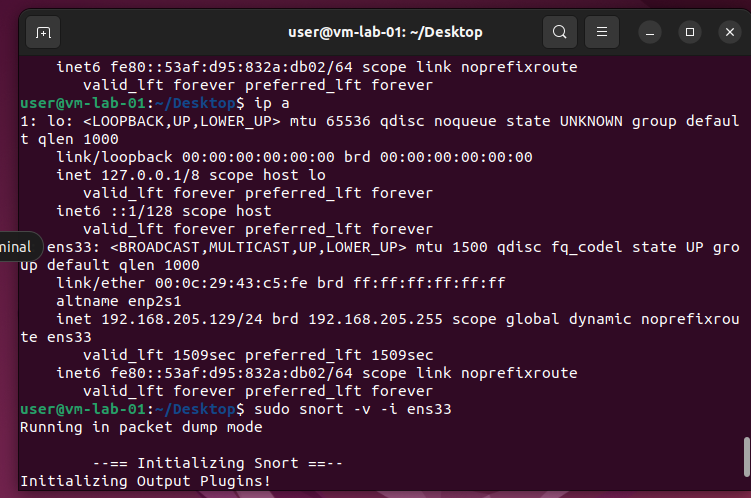
**Минск 2025**

**Задание**

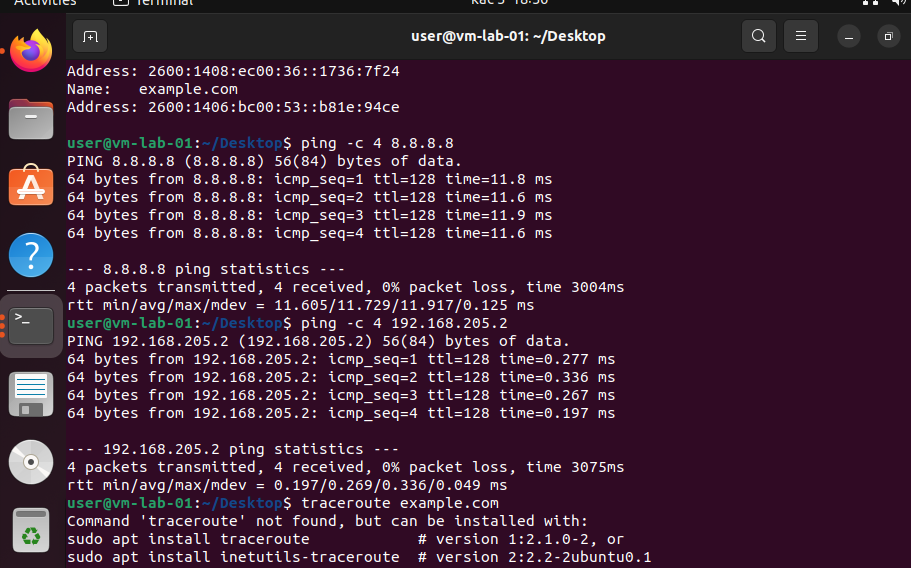
1. На основном компьютере запустить Виртуальную машину. Измените имя компьютера на уникальное.
2. Установить Snort.
3. Запустите Snort в режиме Sniffer пакетов или протоколирования с различными параметрами детализации.
4. Обратитесь к локальной сети. Выполните команду ping, запустите броузер или проводник. 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.

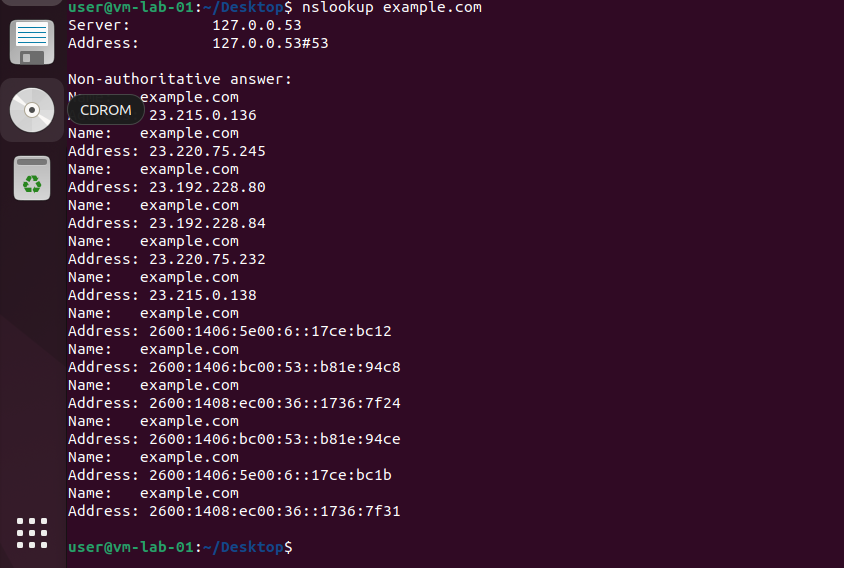
**Изменяем имя на уникальное.**



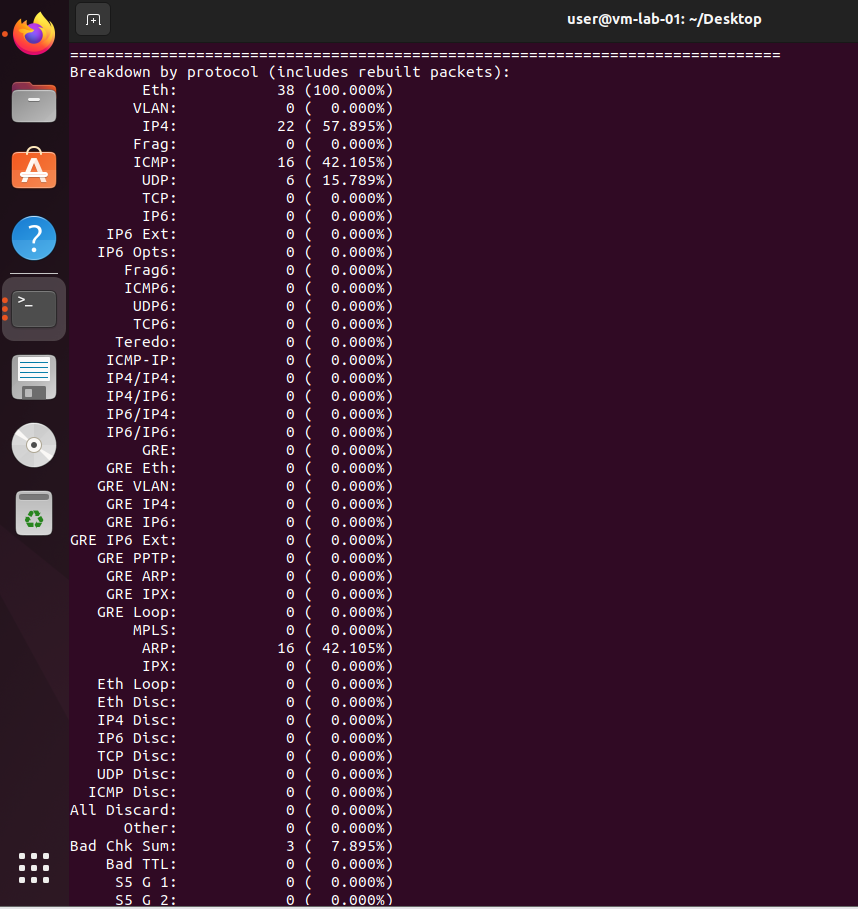
**Определяем сетевой интерфейс:**  


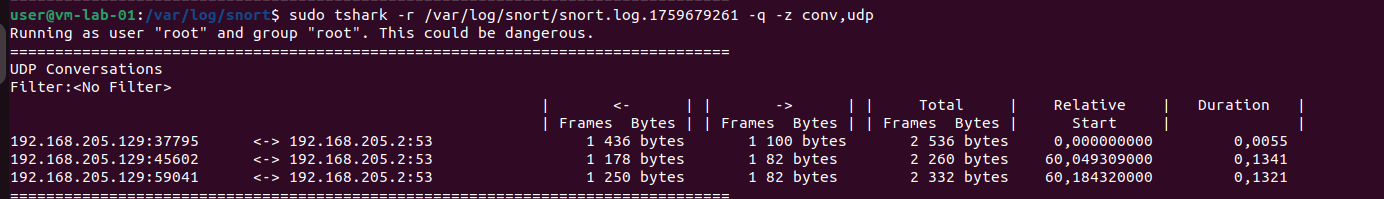
**Взаимодействие с локальной сетью:**

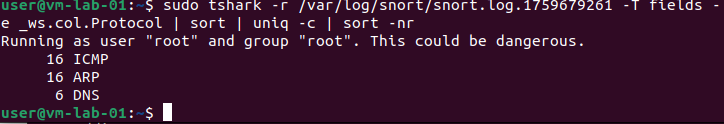




**Отчет работы Snort:**

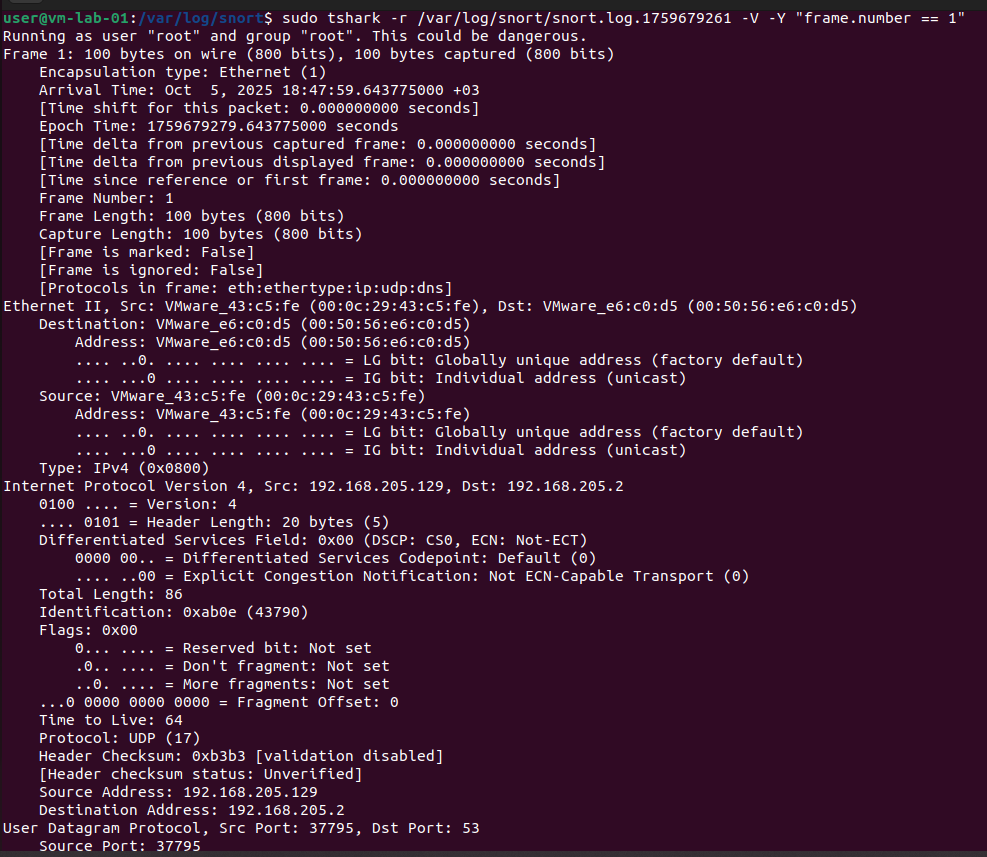


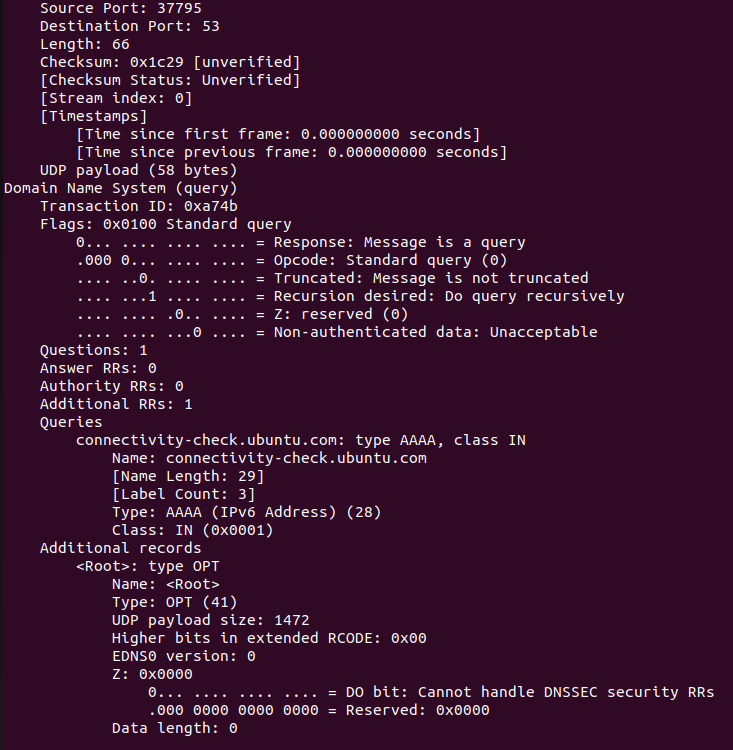




| **Протокол** | **Порт** | **Служба** |
| --- | --- | --- |
| UDP | 53 | DNS (domain) |
| ICMP | — | ping / echo request/reply |
| ARP | — | локальная адресация MAC |

**Пример DNS пакета:**

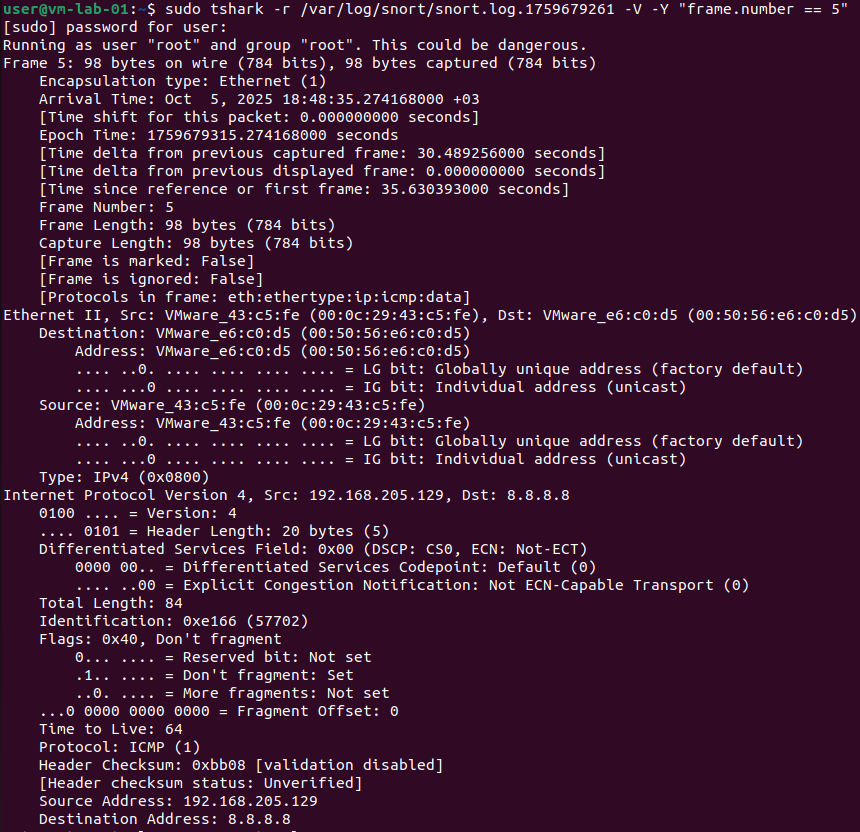
****

****

**Расшифровка:**

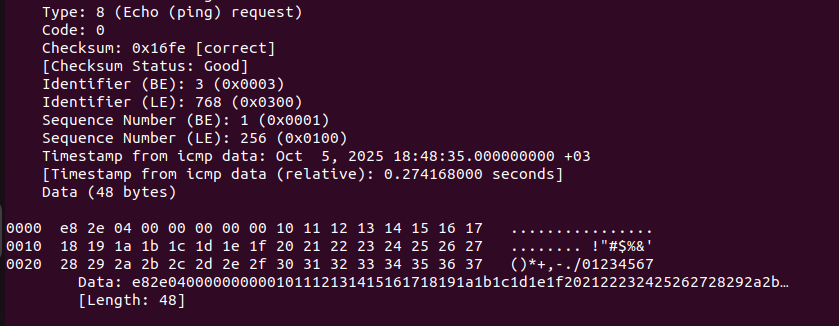
* **IP**: VM → локальный DNS-сервер.
* **UDP**: Src порт — динамический, Dst порт 53 — стандартный для DNS.
* **DNS**: запрос AAAA (IPv6 адрес) для connectivity-check.ubuntu.com.

**Пример ICMP пакета:**

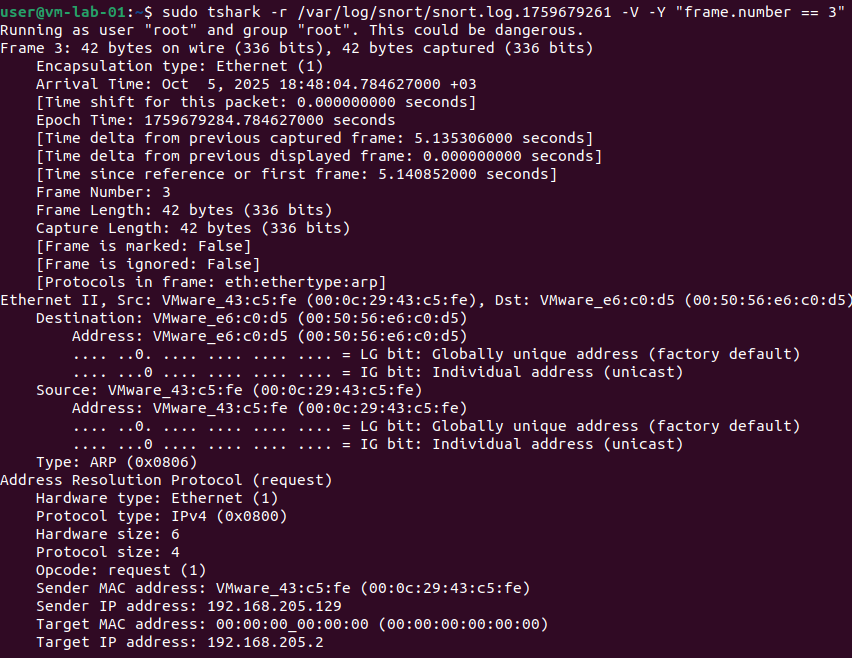
****

**Расшифровка:**

* **IP**: Src —VM, Dst — 8.8.8.8 (Google DNS).
* **ICMP Type 8**: Echo Request (ping). Тип 0 — Echo Reply.
* **Data**: полезная нагрузка пинга (48 байт).

****

**Пример ARP пакета:**

****

**Расшифровка:**

* **Ethernet II**: Src — MAC VM, Dst — MAC шлюза; ARP пакет передаётся внутри локальной сети.
* **ARP Opcode 1 (request)**: пакет запрашивает MAC-адрес для IP 192.168.205.2.

**Вывод:**

В ходе работы с сетевым анализатором Snort мы изучили процесс перехвата и анализа сетевого трафика. Мы провели захват пакетов в локальной сети и проанализировали их содержимое. Были выявлены использованные протоколы (ARP, ICMP, DNS) и сопоставлены их порты с системными службами. Также мы просмотрели структуру пакетов, расшифровали заголовки Ethernet, IP, ICMP, UDP и DNS, изучили поля и назначение каждого из них. В результате мы получили практические навыки мониторинга сетевого трафика, анализа протоколов и выявления активности в локальной сети, а также научились оформлять результаты анализа в виде отчета с примерами пакетов и таблицей используемых служб.