<https://ch-umirann.gitbook.io/ch.umirann/soc/itmo/mang-may-tinh>

Лабораторная работа № 1

# Сканирование и анализ сетевого трафика

### Цель работы

### Изучить инструменты сканирования сетевого трафика, такие как tcpdump и Wireshark.

### Задачи

* ознакомится с назначением и возможностями следующих инструментов: tcpdump, Wireshark;
* установить на физическую или виртуальную машину указанные инструменты;
* выполнить сканирование трафика в соответствии с вариантом и сохранить дамп трафика;
* изучить использование фильтров Wireshark;
* результаты выполнения работы оформить в виде отчета.

1. З/ПК с ОС Kali Linux или другой версией Debian-based Linux, допускается использование виртуальной машины.

### Варианты

1. просмотр видео на сайте YouTube
2. отправка сообщения в мессенджере ВКонтакте
3. загрузка файла на Google.Диск
4. звонок в Zoom/Skype/WhatsApp/Telegram/Discord

### Содержание работы

1. **Установка инструментов**

В первую очередь необходимо установить tcpdump и Wireshark. Многие дистрибутивы Linux поставляются уже с tcpdump. Дистрибутив Kali Linux также поставляется с Wireshark.

Для установки tcpdump на Debian-based операционной системе, необходимо открыть терминал и выполнить команду: **sudo apt install tcpdump**.

Установка Wireshark выполняется аналогичным образом при помощи команды: **sudo apt install wireshark**.

1. **Сканирование трафика**

Для сканирования трафика откройте терминал и введите команду: **sudo tcpdump [*имя\_файла*].pcap**, где имя\_файла - имя файла, содержащего дамп трафика после остановки сканирования.

**Важно!** Необходимо выполнять действия в соответствии с вариантом только после начала сканирования.

1. **Действия по вариантам**

После запуска сканирования выполните действия в соответствии с вариантом работы.

***Примечание***: уточните задание по Вашему варианту у преподавателя.

***Примечание***: если Ваш вариант предполагает авторизацию, не выполняйте ее заранее.

***Примечание***: если Ваш вариант предполагает установку какого-либо стороннего ПО, выполните это заранее.

**Важно!** Остановите работу tcpdump только после выполнения всех действий по Вашему варианту.

Остановите работу tcpdump при помощи комбинации клавиш **ctrl+c**.

1. **Дополнительное задание**

Выполните сканирование трафика в соответствии с Вашим вариантом при помощи Wireshark и сравните полученные дампы трафика.

### Требования к отчету

### Отчет должен содержать скриншоты по использованию каждого инструмента и описывать всю последовательность действий, указанную в разделе “Содержание работы” текущего документа.

Также к отчету необходимо приложить файл, содержащий дамп сетевого трафика.

Оформление отчета выполняется в соответствии с требованиями преподавателя.

### Материалы для подготовки

<https://hackware.ru/?p=10246#8>

<https://blog.sedicomm.com/2017/05/30/tcpdump-poleznoe-rukovodstvo-s-primerami/>

<https://omgubuntu.ru/ustanovitie-i-ispolzuitie-wireshark-v-ubuntu-linux/>

<https://hackware.ru/?p=7008>

<https://networkguru.ru/wireshark-filtr-po-ip-portu-protokolu-mac/>