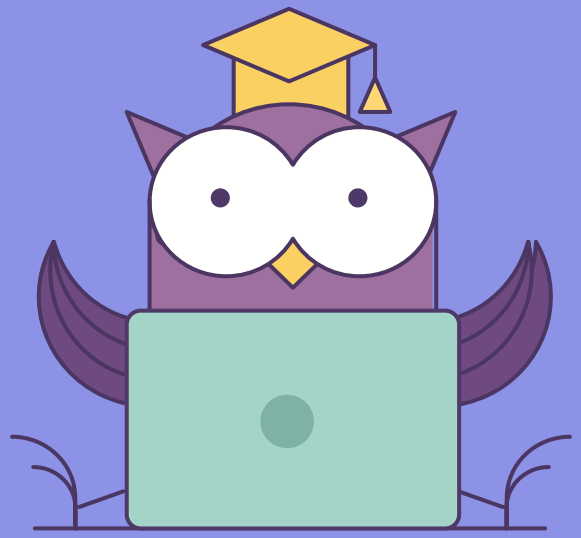
ОНЛАЙН-ОБРАЗОВАНИЕ

OTUS

Основные сетевые протоколы. Разбор трафика.

Колесников Александр Александрович

Меня хорошо слышно && видно?



Напишите в чат, если есть проблемы!

Ставьте + если все хорошо

Содержание

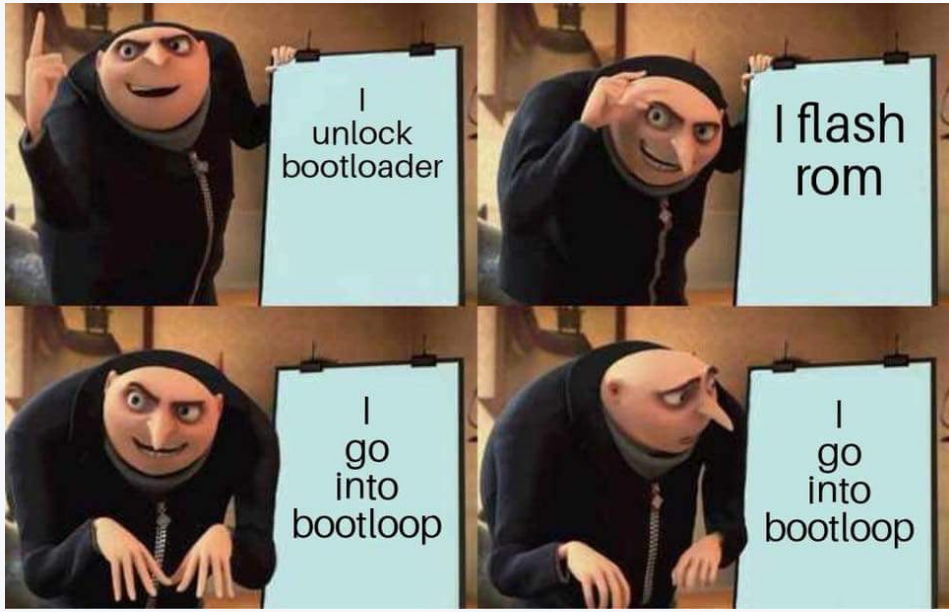
- **Утилиты для анализа трафика**
  - WireShark
  - Некоторые полезные утилиты для анализа
- **Практика**
  - Разбор тестового трафика
    - Фильтры
    - Форматы
    - Вспомогательные утилиты

Цель занятия

1. Вспомнить основы протоколы сетевого взаимодействия

2. Собрать информацию о сеть посредством анализа трафика

3. Получить навыки работы с утилитами для обработки сетевого трафика



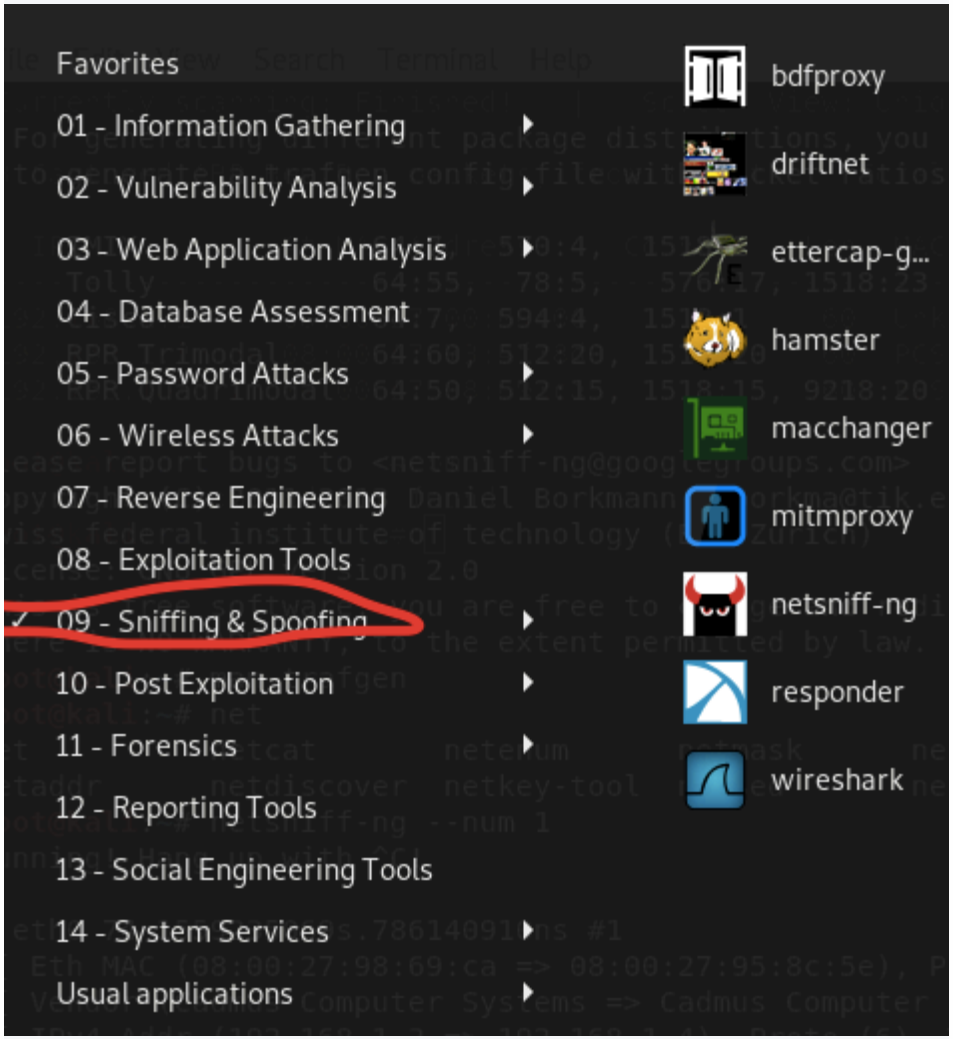
01

Утилиты для анализа трафика

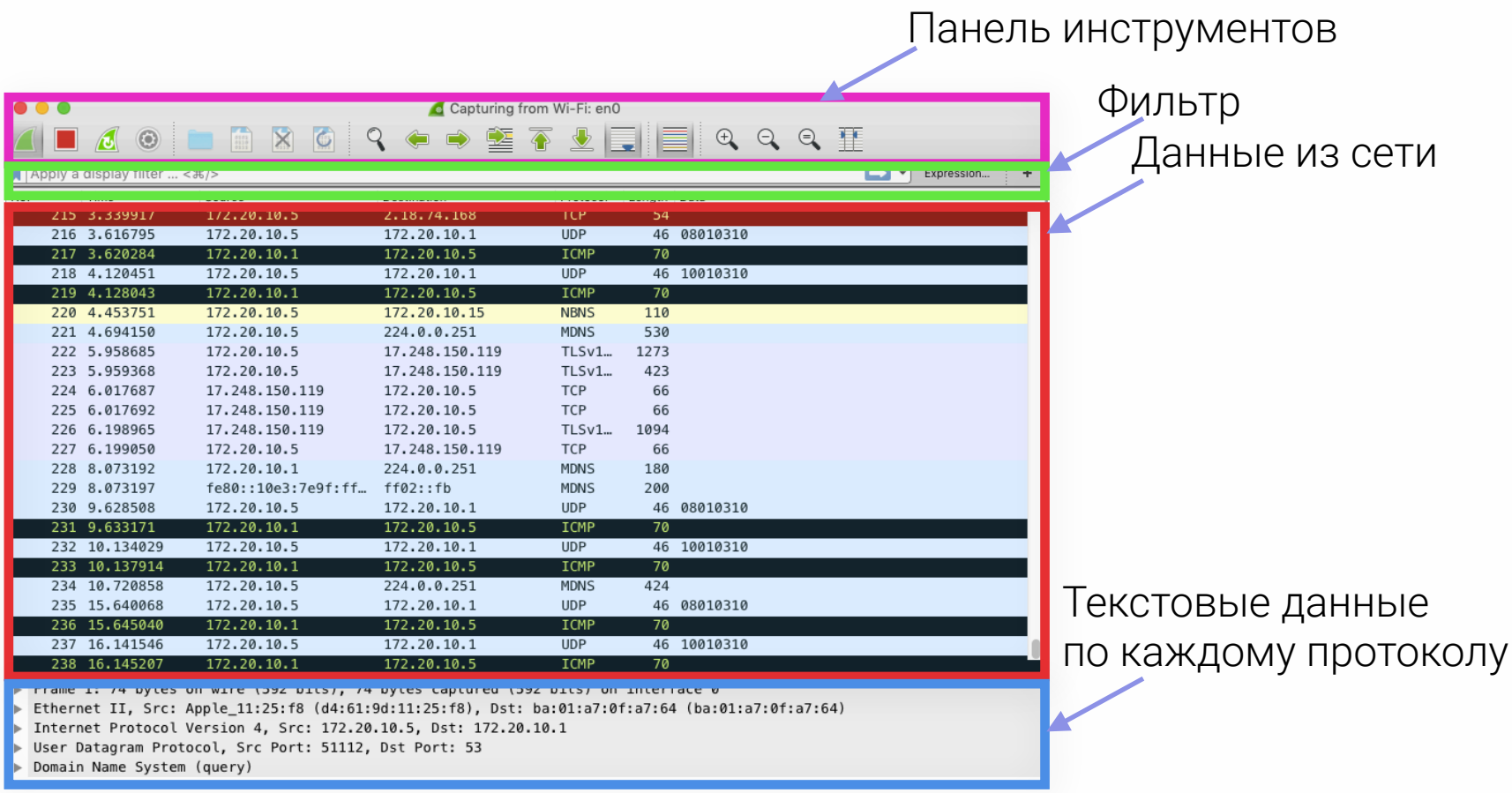
Основные утилиты

Типы утилит:

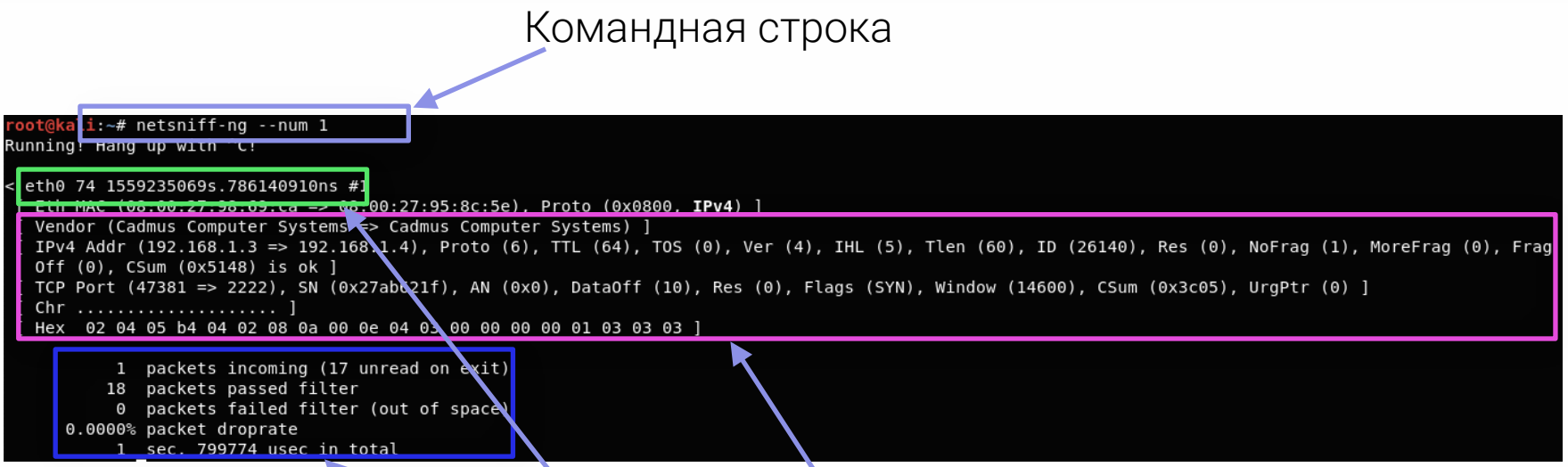
1. Снифферы
    - WireShark
    - Net-Miner
    - tcpdump
    - netsniff-ng
2. Респондеры
    - Responder
    - Ettercap
3. Прокси
    - Burp Suite
    - Owasp ZAP
    - mitmproxy
4. Библиотеки
    - libpcap
    - NpCap



WireShark (tshark)



netsniffer-ng



00

Анализ трафика

01

Разбор трафика

Вопросы для исследования

- Какие операционные системы есть в сети?
- Какие протоколы используются для общения?
- Можно ли установить название машин?
- Можно ли получить имена пользователей и другую пользовательскую информацию?
- Перечислить название общих ресурсов (шар)

Александр Колесников

Спасибо
за внимание!