Основы построения защищенных компьютерных сетей

Лекция 4
Анализ сетевого трафика

Семён Новосёлов

2021

Wireshark

Самый популярный инструмент для анализа сетевого трафика.

- Поддерживает сотни протоколов
- Есть поддержка расшифровки IPsec, SSL/TLS, WEP, WPA/WPA2
- https://www.wireshark.org/
- Консольная версия: tshark

Сбор трафика для анализа

На удалённом сервере без графического интерфейса (при работе по ssh):

1. Сбор:
   [sudo] `tcpdump -w` имя_файла
2. Загрузка:
   `scp` пользователь@адрес_сервера:путь_к_файлу/имя_файла имя_файла_для_сохранения
3. Анализ: открыть в Wireshark

Пример. VDS (virtual dedicated server)

- Виртуальный выделенный сервер, арендуется у провайдера (например, firstvds).
- Сразу после запуска на сервере начинается:
  - сканирование различными ботам и компаниями из ИБ
  - перебор паролей для SSH
  - попытки примененеия эксплойтов к запущенным сервисам

В дальнейших примерах используются дампы трафика на VDS с адресом novsem1.fvds.ru

Сбор трафика для анализа II

Трафик Wi-Fi:

1. перевести карту в неразборчивый режим (через aircrack-ng)
2. запустить wireshark/tcpdump

- Трафик не шифруется для подключенных к сети устройств
- известен пароль сети ⇒ можно сделать дамп шифрованного трафика сети и расшифровать потом в wireshark без подключения к сети

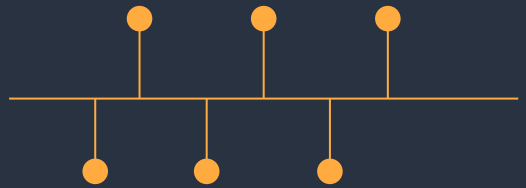
Сбор трафика для анализа III

Сеть Ethernet:

- Многие роутеры поддерживают сбор трафика в сети
- В топологии “звезда” сбор трафика возможен через атаки типа MiTM: ARP-poisoning

Топология “звезда”

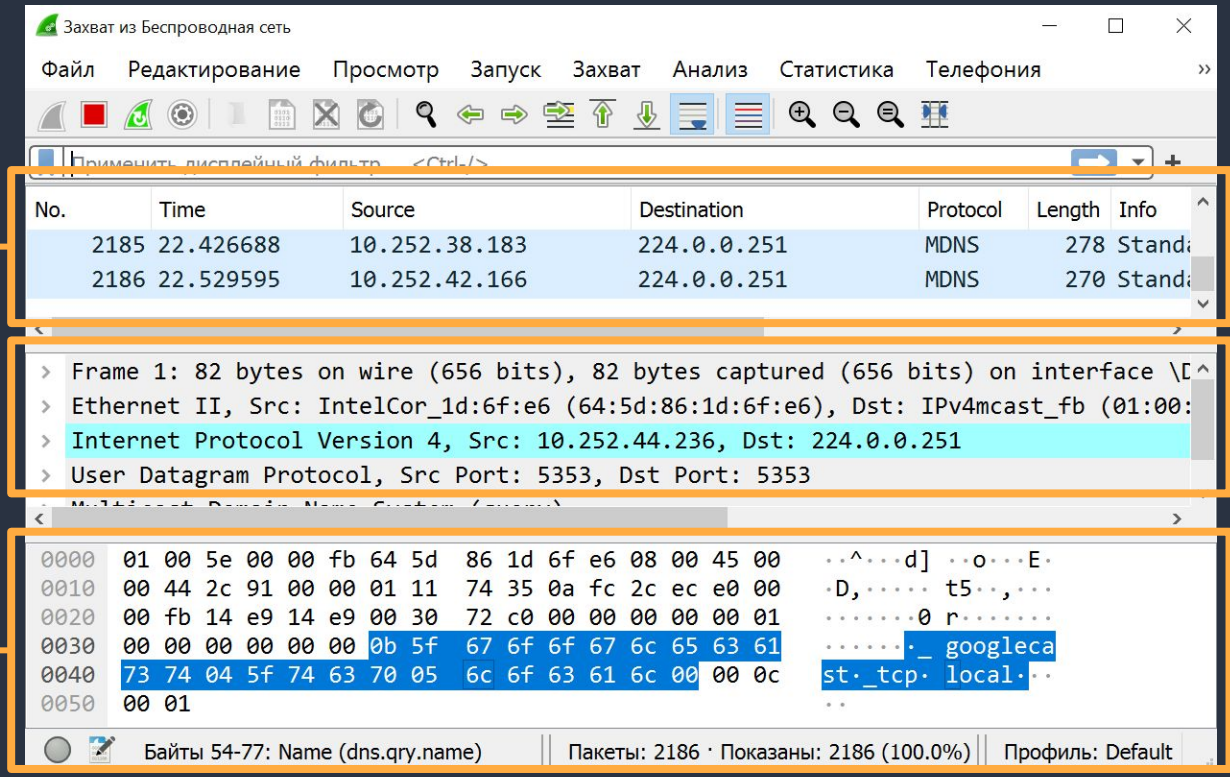
- от других хостов видны только широковещательные запросы



Топология “шина”

- видны все пакеты всем хостам

Wireshark. Интерфейс



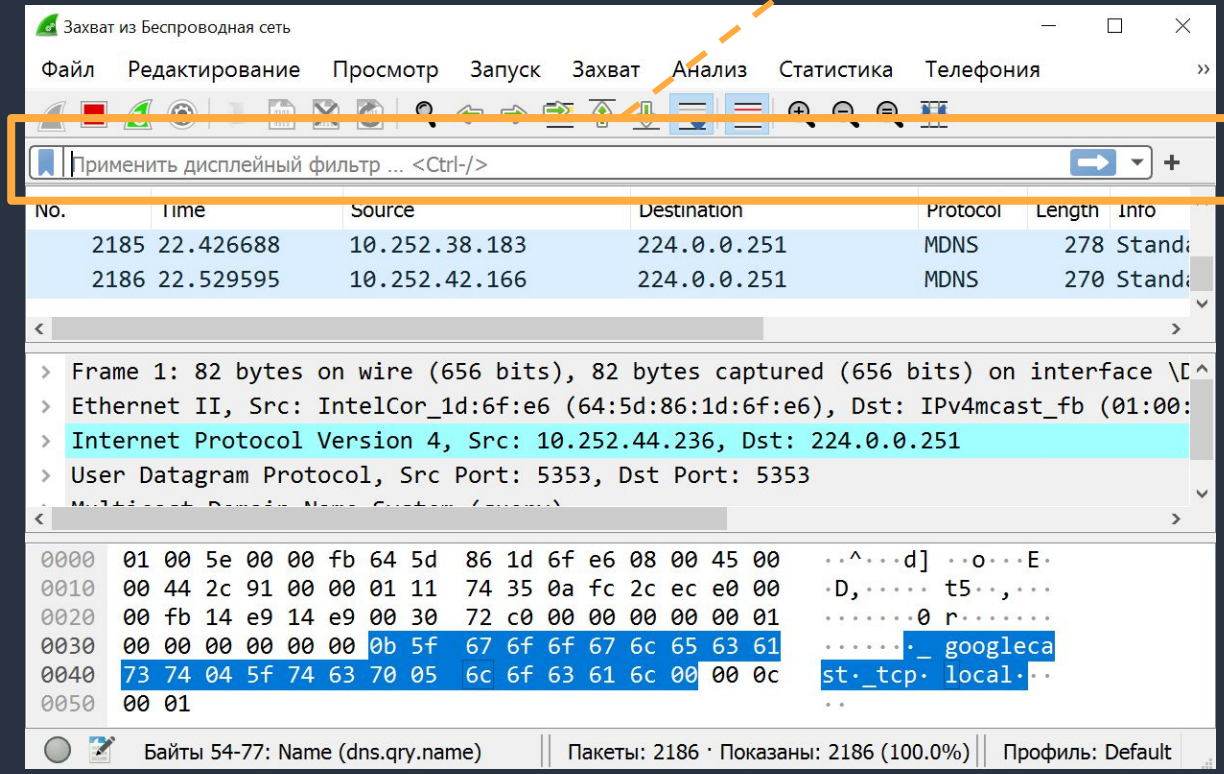
Список пакетов

Разбор пакета

Сырые данные пакета

Wireshark. Фильтры

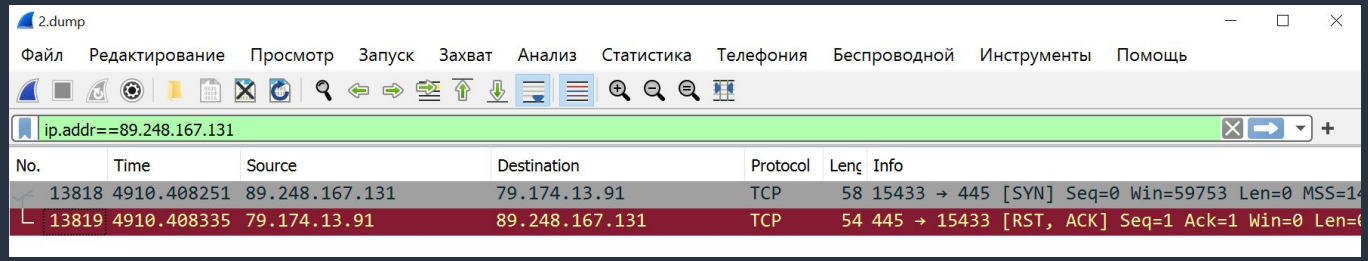
- интересные пакеты находятся среди кучи других пакетов
- необходимо отфильтровать лишние



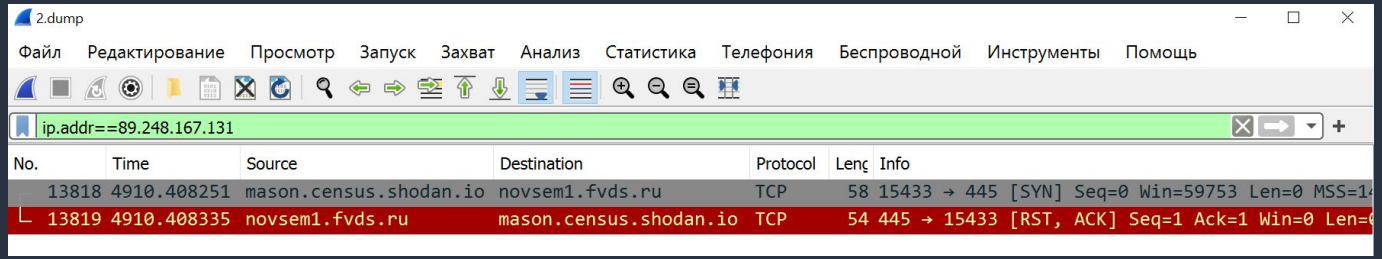
Основные фильтры

- Показ трафика (исходящего/входящего) определенного хоста:
  `ip.addr == 192.168.0.1`
- Фильтрация по протоколу:
  `http`
  `tcp`
  `smb`
- Логические операторы (И, ИЛИ, НЕ):
  `ip.src==192.168.0.0/16 and ip.dst==192.168.0.0/16`
- Поиск по содержимому пакетов:
  `data contains “string”`
  `http contains “string”`

Отображение доменных имён хостов



По-умолчанию отключено.



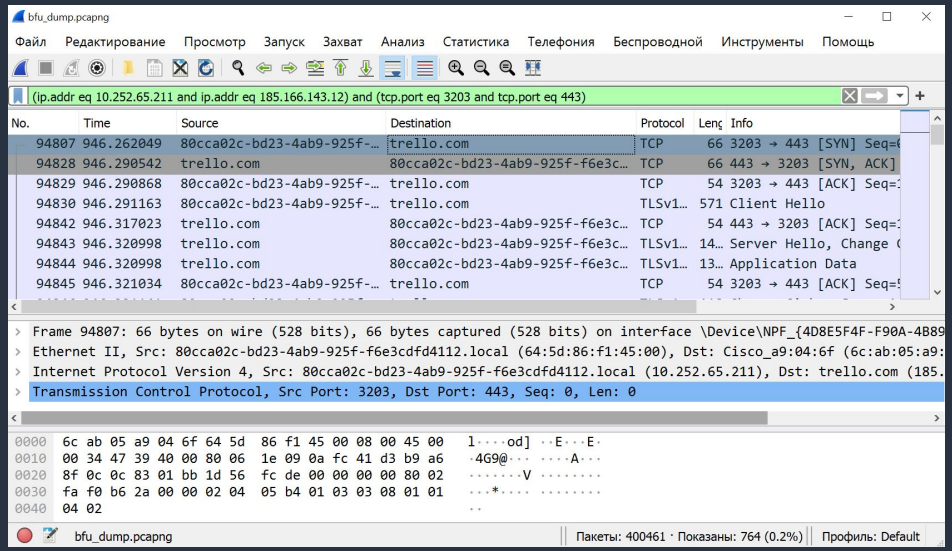
Включение:

Edit ⇒ Preferences ⇒ Name Resolution ⇒ Resolve Network (IP) addresses

Выделение соединений

Wireshark поддерживает выборку пакетов соединений (потоков)

- Выделить Пакет ⇒ Follow ⇒ TCP Stream
- Выделить Пакет ⇒ Conversation Filter ⇒ TCP

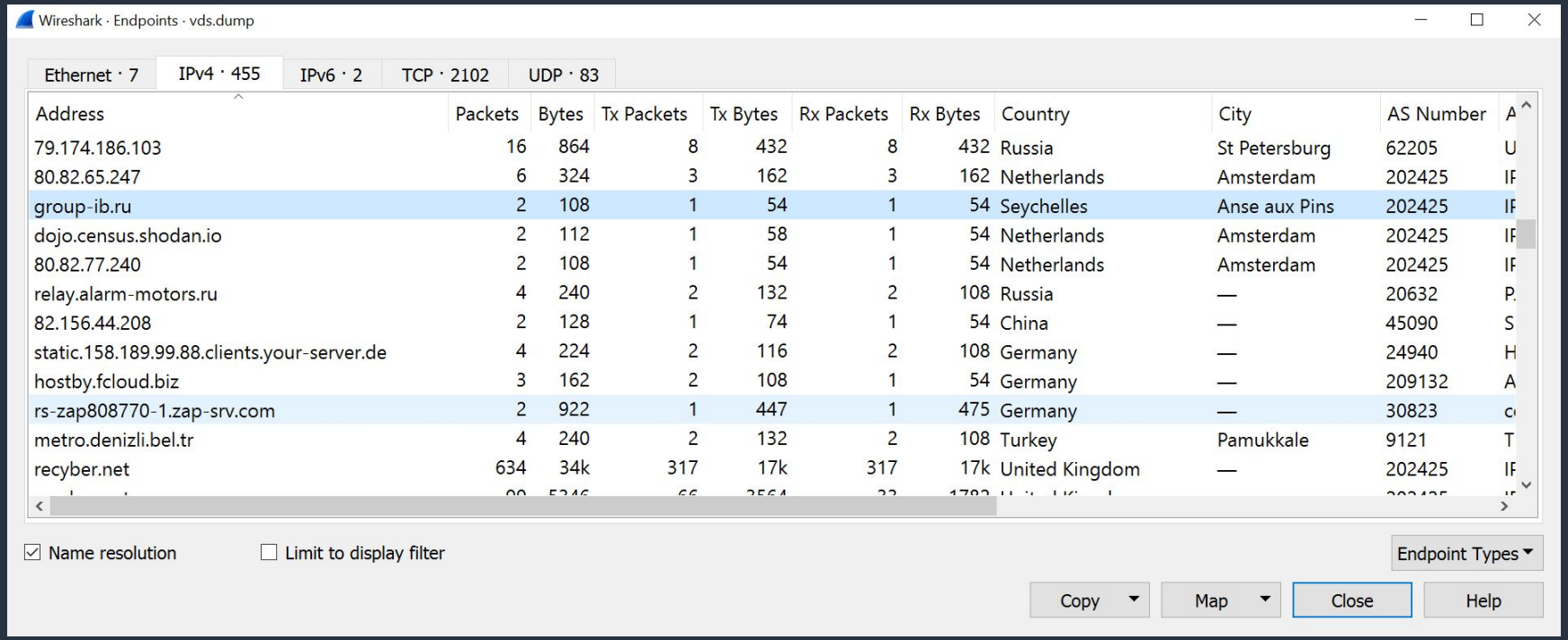


Пример. Подключение к trello.com по TLS

База GeoIP

Для отображения информации о местоположениях IP-адресов:

1. Скачать базы MaxMind (достаточно GeoLite2 Free)
2. Указать их в Edit ⇒ Preferences ⇒ Name Resolution ⇒ MaxMind Database Directory
3. Информация о локациях доступна через: Statistics ⇒ Endpoints

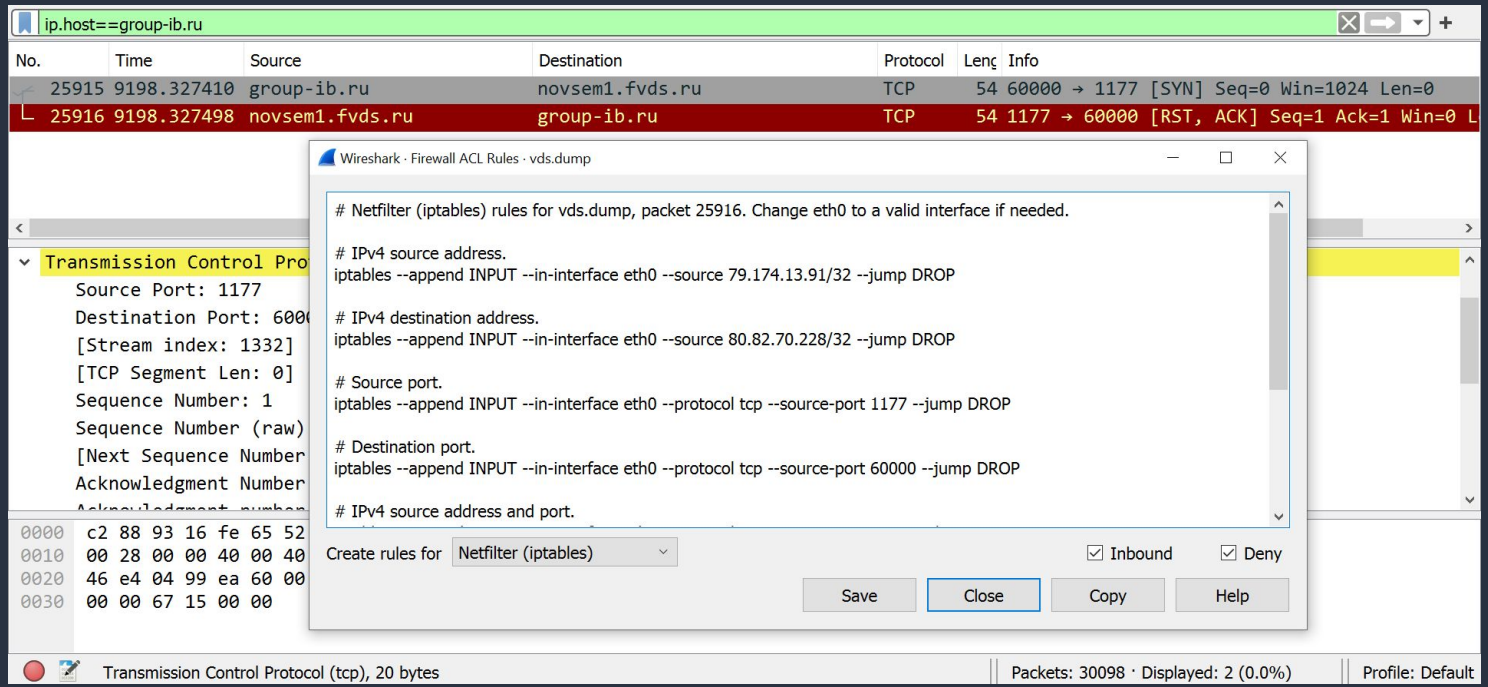


Пример: Анализ дампа трафика с VDS, видно адреса компаний из ИБ, сканирующих сеть.

Генерация правил для файервола

Wireshark поддерживает автоматическую генерацию правил доступа для различных файерволов.

- Tools ⇒ Firewall ACL Rules

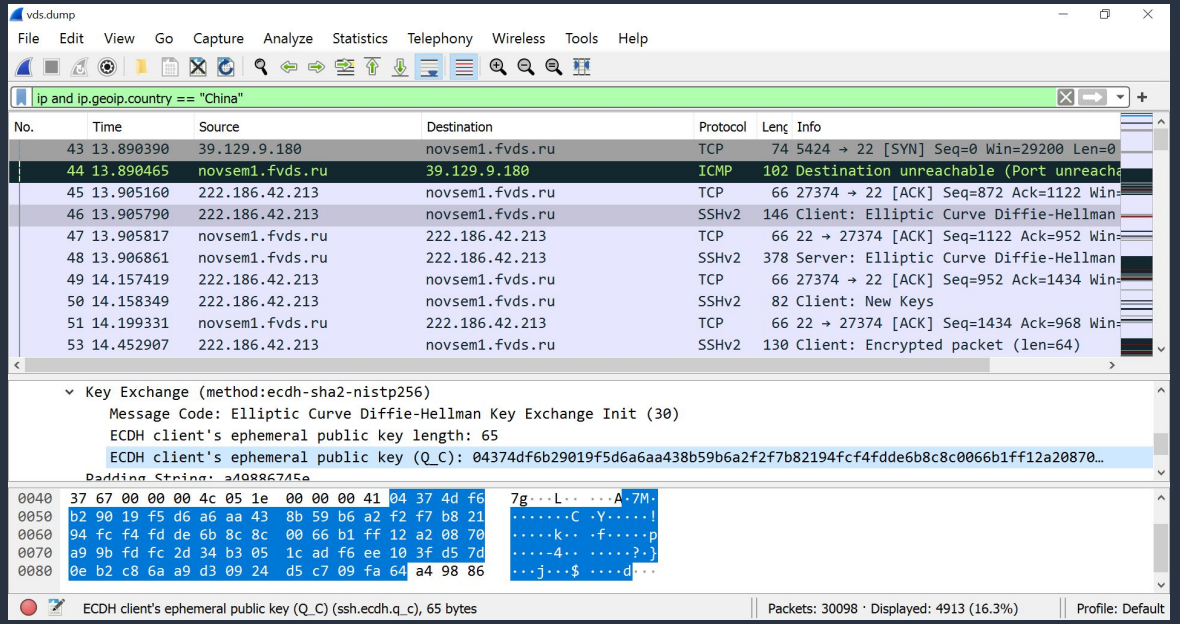


Пример: правило для блокировки group-ib.ru

База GeoIP. Фильтрация по стране

После установки баз GeoIP можно фильтровать пакеты по стране:

```
ip and ip.geoip.country == “China”
```



Пример: Анализ дампа трафика с VDS, видно китайские хосты, перебирающие ключи SSH.

Анализ TLS-трафика

В перехваченном TLS-трафике доступен только анализ заголовков IP/TCP.

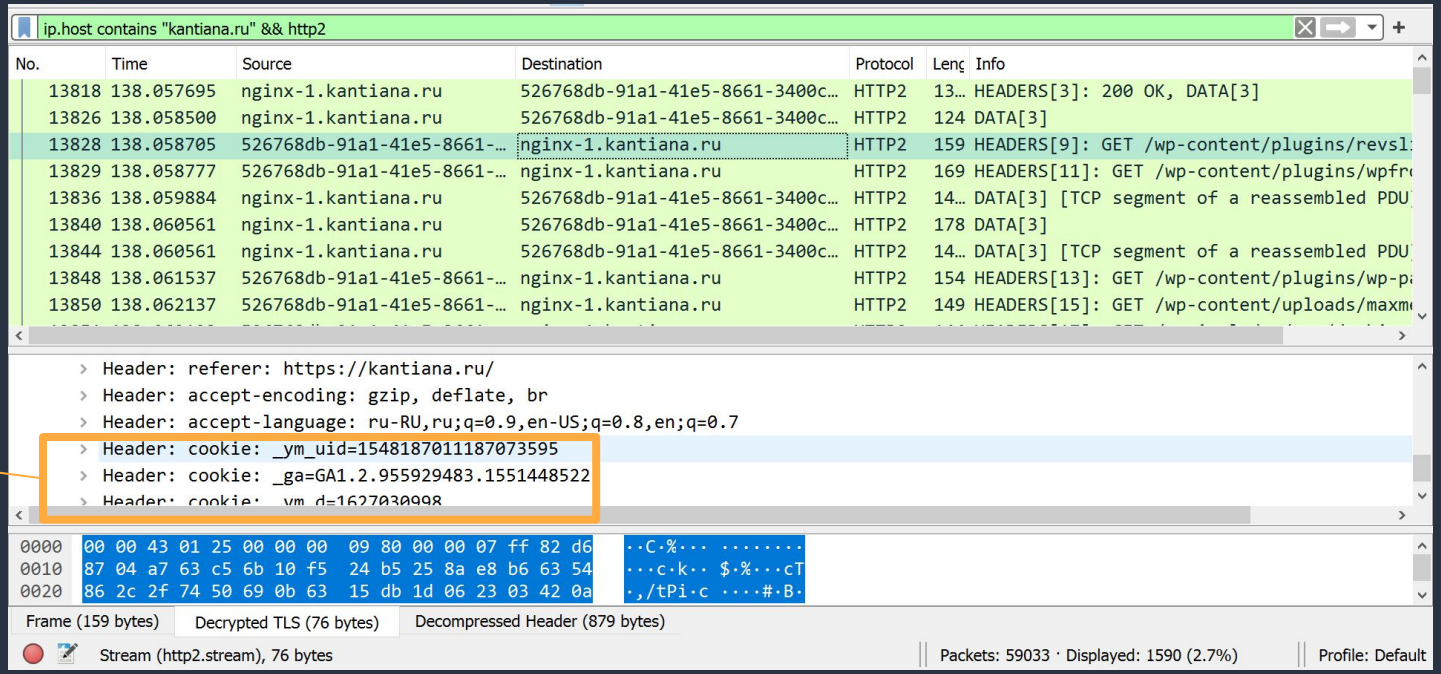
Расшифровка трафика на своём компьютере:

Linux/Windows:

1. установить переменную окружения SSLKEYLOGFILE=путь_к_файлу/sslkey.log
2. В Wireshark указать путь к файлу sslkey.log в настройках TLS

Linux:
переменная LD_PRELOAD для переопределения функций read/send/write

Можно перехватить cookie



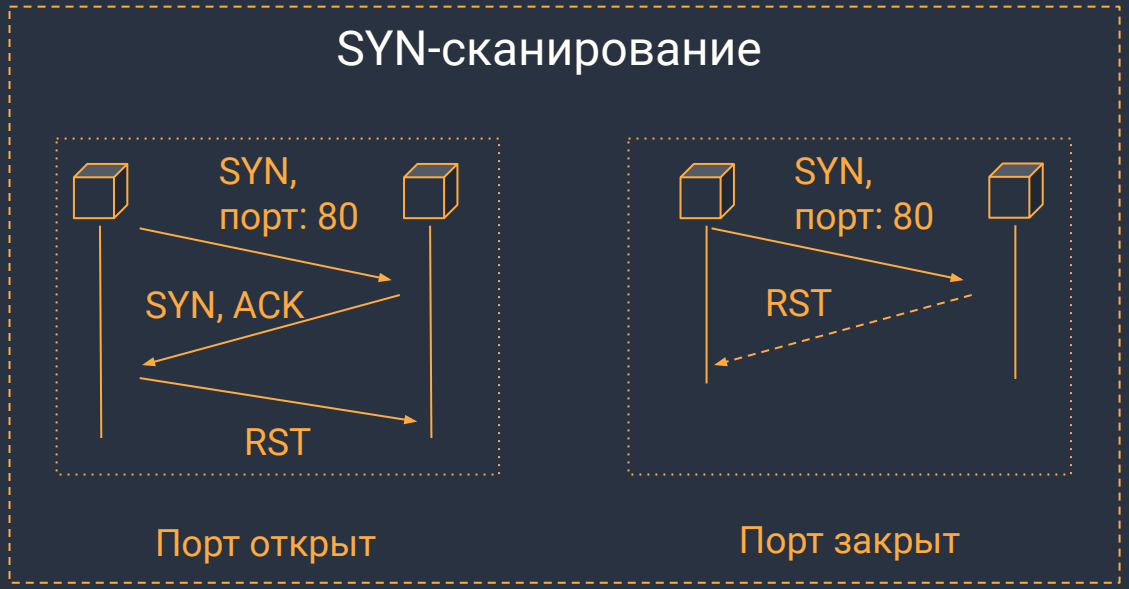
Пример: подключение по https к kantiana.ru

Важно: установка переменных среды SSLKEYLOGFILE отрывает дыру в безопасности, так как позволяет следить за трафиком пользователя системы

Определение источника сканирования портов

ищем последовательности пакетов вида:

1. SYN (⇒), SYN+ACK (⇐), RST (⇒)
2. SYN (⇒), RST+ACK (⇐)



No.	Time	Source	Destination	Protocol	Leng	Info
80578	29310.3652…	recyber.net	novsem1.fvds.ru	TCP	54	43891 → 19350 [SYN] Seq=0
80579	29310.3653…	novsem1.fvds.ru	recyber.net	TCP	54	19350 → 43891 [RST, ACK]
80581	29310.4396…	recyber.net	novsem1.fvds.ru	TCP	54	43891 → 19350 [RST] Seq=1

Литература и ссылки

- Дуглас Э. Камер - Сети TCP IP. Принципы, протоколы и структура (2003)
- Дампы трафика Wireshark: https://gitlab.com/wireshark/wireshark/-/wikis/SampleCaptures