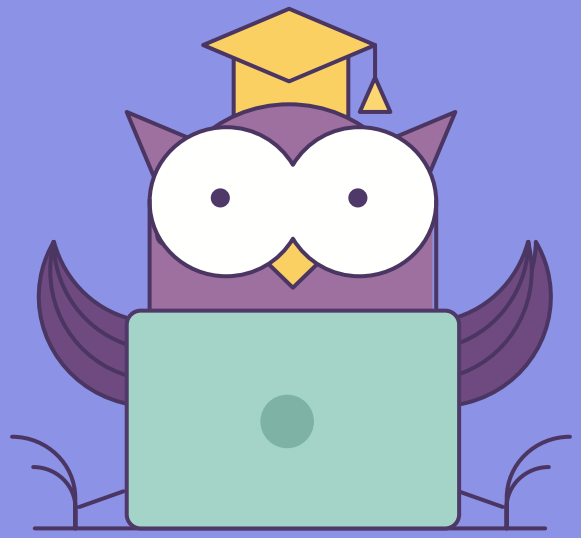
ОНЛАЙН-ОБРАЗОВАНИЕ

OTUS

Основные сетевые протоколы

Колесников Александр Александрович

Меня хорошо слышно && видно?



Напишите в чат, если есть проблемы!

Ставьте + если все хорошо

Содержание

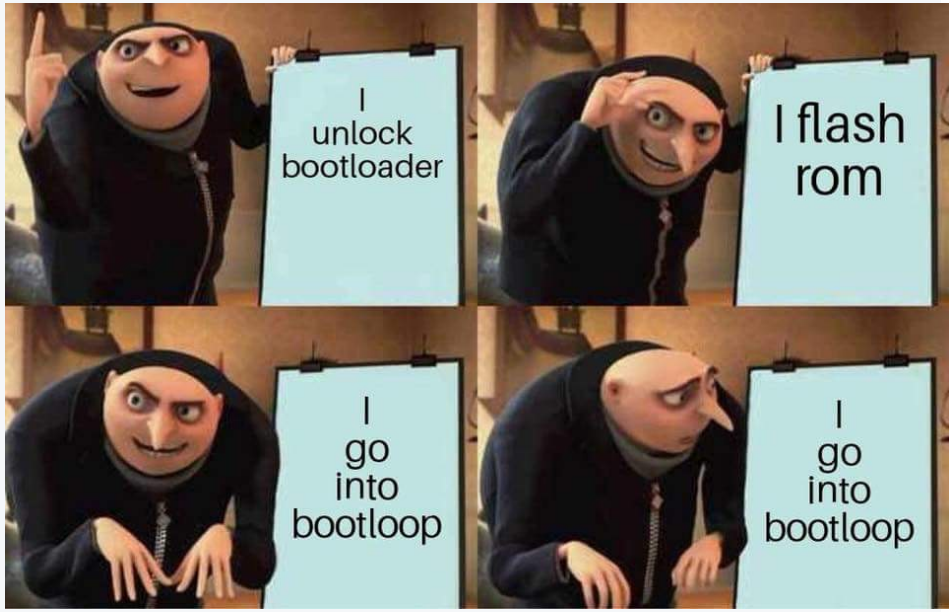
- **Сетевое взаимодействие**
  - Сетевые модели
  - Основные протоколы
  - Что такое трафик и зачем его разбирать
- **Утилиты для анализа трафика**
  - WireShark
  - Некоторые полезные утилиты для анализа
- **Практика**
  - Сканирование сети
  - Разбор трафика

Цель занятия

1. Разобраться со стеком протоколов сетевого взаимодействия

2. Получить представление о том как нестандартно можно использовать информацию из протоколов для идентификации хостов в сети

3. Получить навыки работы с утилитами для обработки сетевого трафика



Сетевые модели

1. Что такое модель

В теории:

- Набор правил
- Схема работы правил
- Куча абстракций

2. Зачем нужна

В теории:

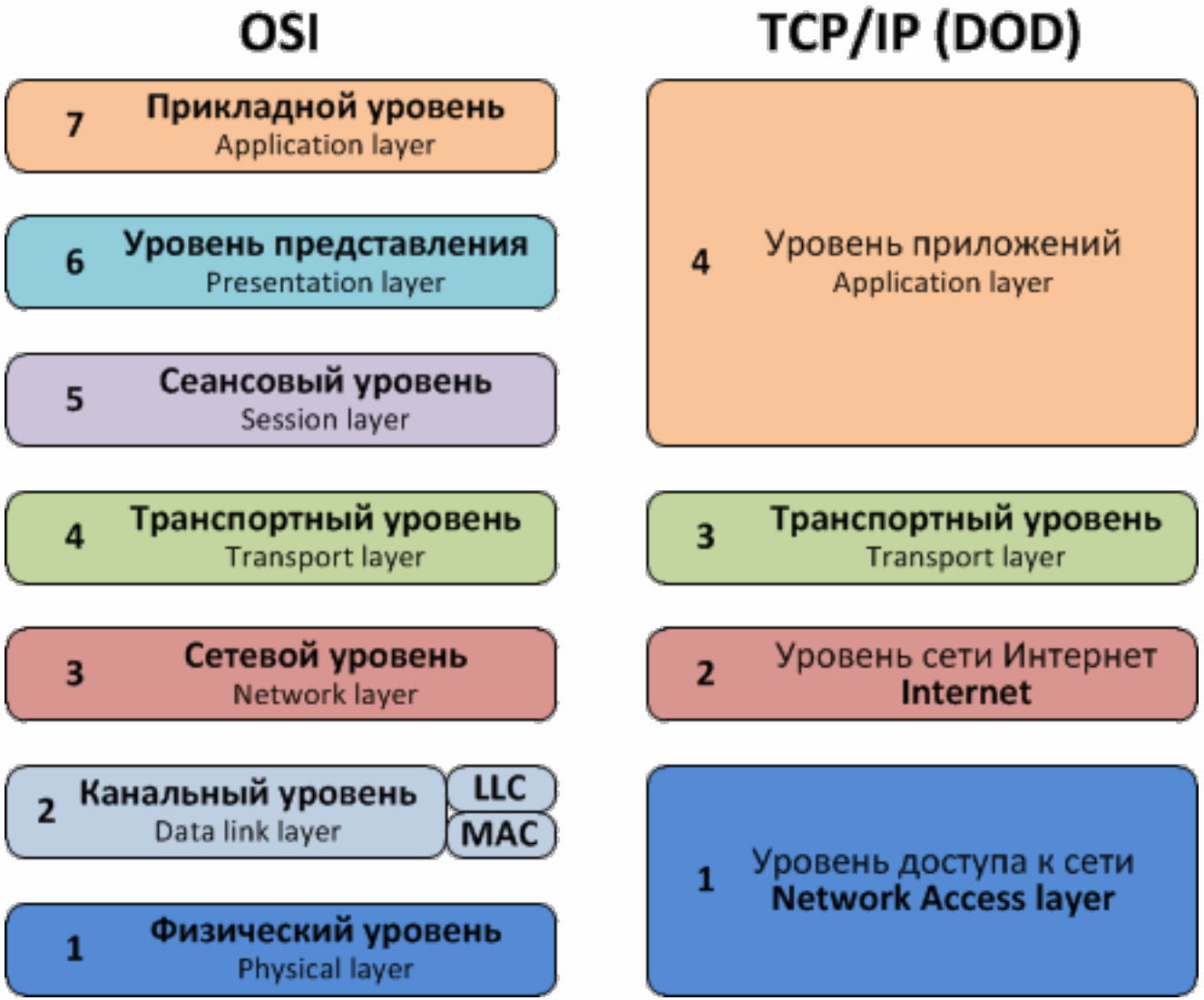
- Для того чтобы можно было делить действия на составные части
- Для создания алгоритма изучения взаимодействия систем

3. Какие бывают

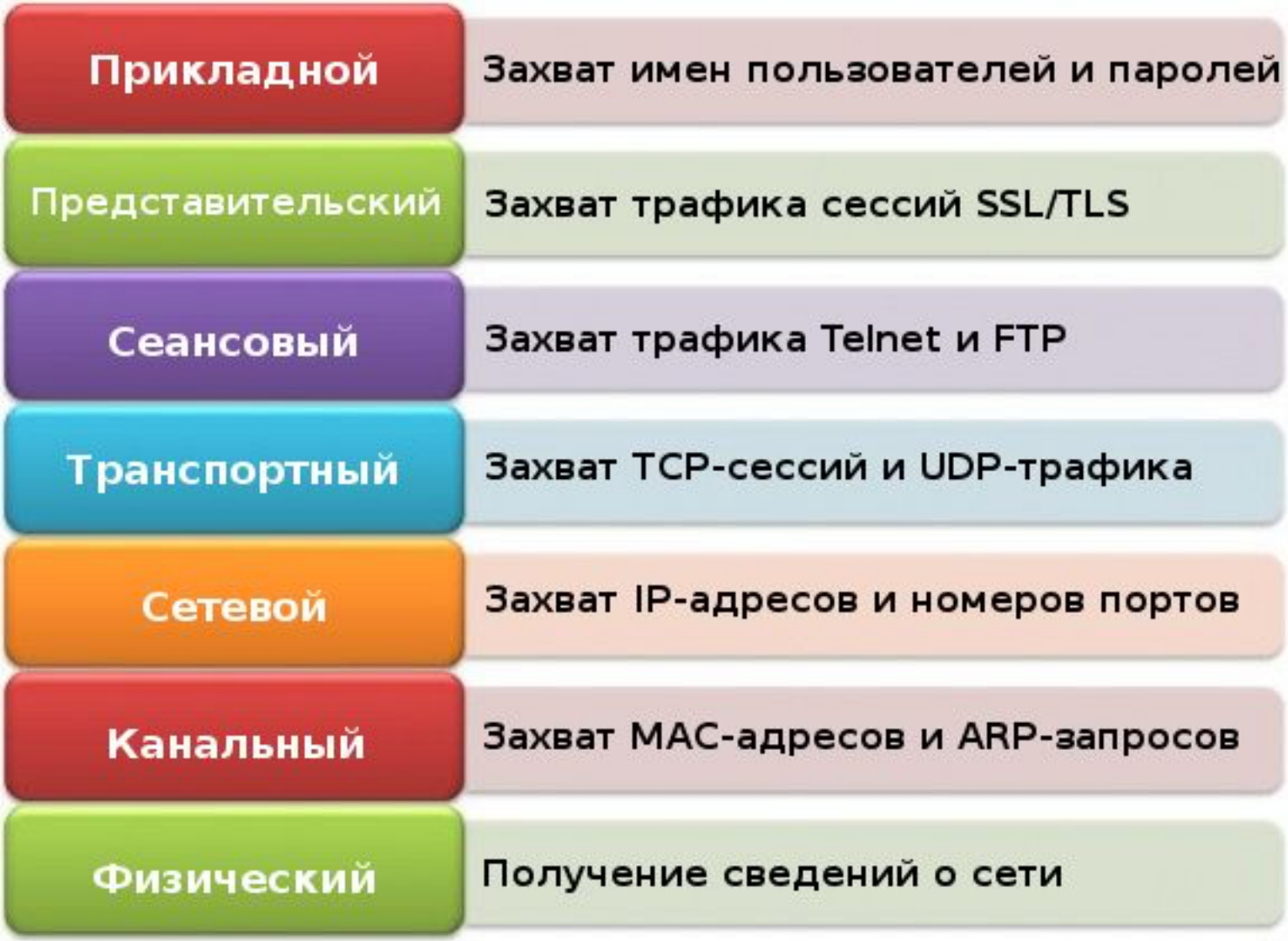
На практике:

- TCP/IP
- IPX/SPX
- DOD

Соотношение между теоритическими и практическими моделями



Атаки на уровни с помощью сниффинга



01

Сетевое взаимодействие

Протокол IP

Основные данные:

1. Протокол сетевого уровня модели TCP/IP

2. Основная задача протокола - адресация в сети

3. Популярные версии: v4, v6, безопасная версия - IPSec

4. Основные понятия протокола:

   - ip адрес

   - маска подсети

   - класс сети (v4)

   - маршрут

IPv4

1. Адресация в протоколе возможна в пределах: 2^32-1.
2. Чтобы расширить диапазон адресов можно использовать механизм NAT (Network Address Translation)
3. Для выдачи нового адреса нуждается в DHCP сервере
4. Создает адрес для каждого хоста с помощью адреса и маски подсети.
5. Хоть и задумывался как протокол с классификацией сетей, на данный момент используется с бесклассовой адресацией.

```
Возможные записи адреса: 192.168.1.1 255.255.255.0 или 192.168.1.1/24
```

Октет	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	Версия				IHL				Differentiated Services Code Point						ECN		Длина пакета															
4	Идентификатор																Флаги			Смещение фрагмента											
8	Время жизни (TTL)								Протокол								Контрольная сумма заголовка															
12	IP-адрес отправителя																															
16	IP-адрес получателя																															
20	Параметры (от 0 до 10 32-битных слов)																															
	Данные																															

IPv6

1. Адресация в протоколе возможна в пределах: 2^128-1.
2. Не нуждается в NAT
3. Самостоятельно конфигурирует сеть и выдает адреса
4. Имеет отдельные адреса для передачи данных выбранным нодам
5. Адрес состоит только из адреса, маски подсети не используются

Возможные записи адреса: 2001:0DB8:AA10:0001:0000:0000:0000:00FB или 2001:0DB8:AA10:0001::::00FB

Позиция в октетах		0								1								2								3							
	Позиция в битах	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Версия				Класс трафика								Метка потока																			
4	32	Длина полезной нагрузки																След. заголовок								Число переходов							
8	64	IP-адрес отправителя																															
12	96																																
16	128																																
20	160																																
24	192	IP-адрес получателя																															
28	224																																
32	256																																
36	288																																

Общая табличка различий протоколов

IPv4	IPv6
32 битный адрес	128 битный адрес
Статические адреса и динамические от DHCP	Автоконфигурация
Не гарантирует целостности	Предоставляет механизм целостности
Безопасность реализуется приложением	IPSec встроена в протокол
Десятичное представление адреса	Шестнадцатеричное представление адреса
Фрагментация на совести передающего	Фрагментация задается отправителем
Нет механизмов идентификации конкретного пользователя	Есть система тегирования в заголовке
Контрольная сумма пакета возможна	Контрольная сумма недоступна
Есть бродкастовая схема	Есть мультикастовая и эникастовая схема
Шифрование и аутентификация недоступны	Встроенная аутентификация и шифрование

ARP

1. Address Resolution Protocol
2. Протокол используется для обнаружения хостов в сети
3. Основные понятия:
    - ARP таблица
    - ip адрес
    - Mac адрес

+	Bits 0 — 7	8 — 15	16 — 31
0	Hardware type (HTYPE)		Protocol type (PTYPE)
32	Hardware length (HLEN)	Protocol length (PLEN)	Operation (OPER)
64	Sender hardware address (SHA)		
?	Sender protocol address (SPA)		
?	Target hardware address (THA)		
?	Target protocol address (TPA)		

ICMP

1. Internet Control Message Protocol
2. Протокол помогает идентифицировать ошибки в сети
3. Основные понятия:
    - код ошибки

Октет (байт)	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
[0—3]	Тип								Код								Контрольная сумма																
…	Данные (формат зависит от значений полей «Код» и «Тип»)																															

TCP

1. Transmission Control Protocol
2. Позволяет контролировать соединение
3. Основное понятие протокола: порт

Примечание: Первая 1000 портов используется популярными сервисами и благодаря этому их можно с высокой точностью определять.

Бит	0 — 3	4 — 9	10 — 15	16 — 31
0	Порт источника, **Source Port**			Порт назначения, **Destination Port**
32	Порядковый номер, **Sequence Number (SN)**			
64	Номер подтверждения, **Acknowledgment Number (ACK SN)**			
96	Длина заголовка	Зарезервировано	Флаги	Размер Окна
128	Контрольная сумма			Указатель важности
160	Опции (необязательное, но используется практически всегда)			
160/192+	Данные			

UDP

1. User Datagram Protocol
2. Часто используется для передачи потоковых данных (звук, видео)
3. Основные понятия протокола: порт

Примечание: Протокол не требует ответа от целевого хоста. Так же таймаут отправки таких пакетов регулируется параметрами ядра операционных систем.

Биты	0 - 15	16 - 31
0-31	Порт отправителя (Source port)	Порт получателя (Destination port)
32-63	Длина датаграммы (Length)	Контрольная сумма (Checksum)
64-...	Данные (Data)	

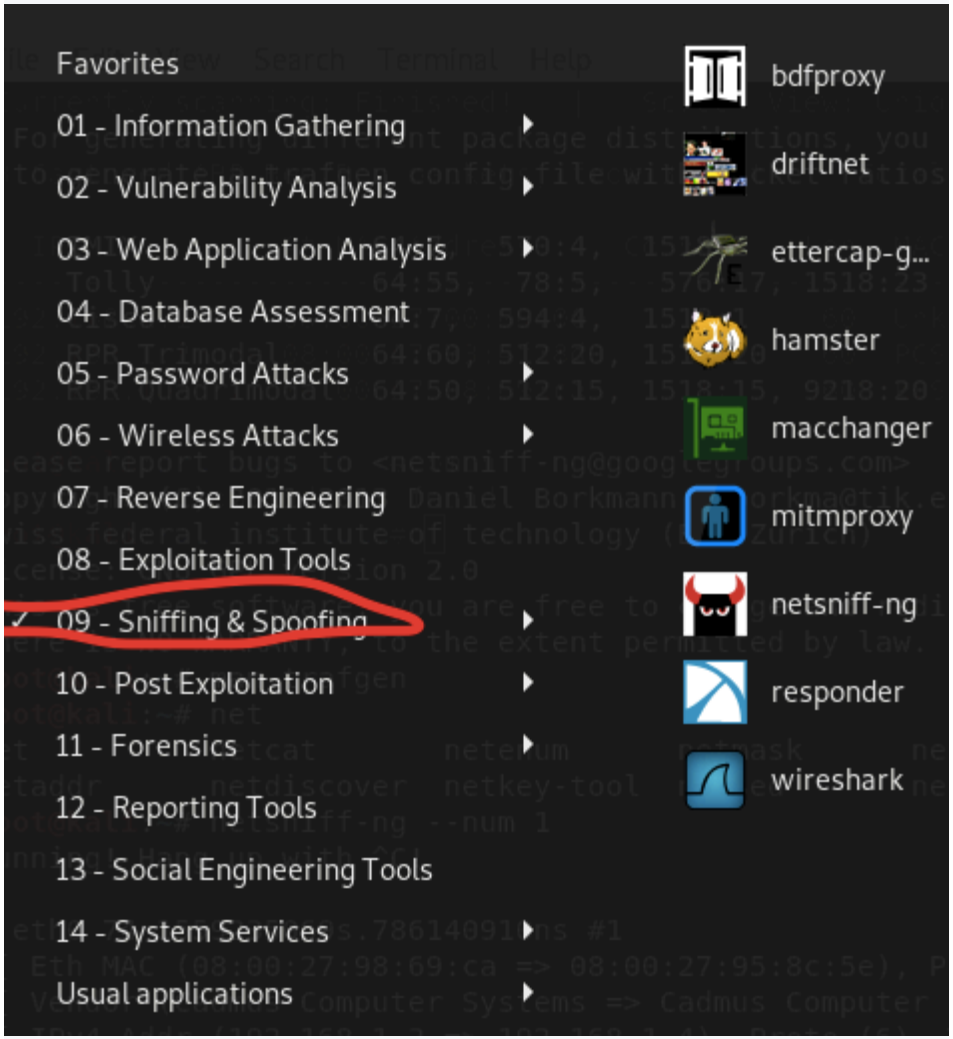
02

Утилиты для анализа трафика

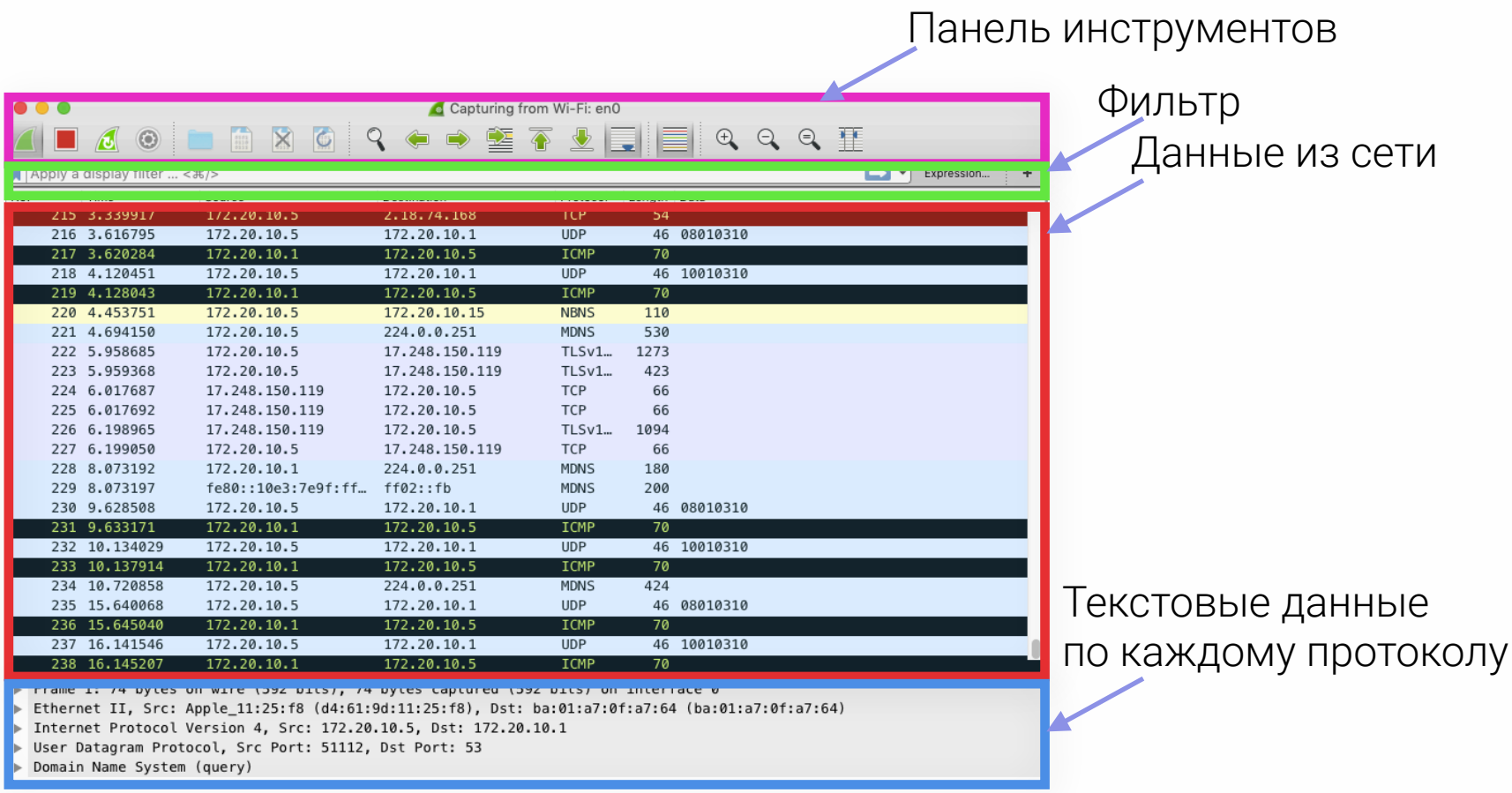
Основные утилиты

Типы утилит:

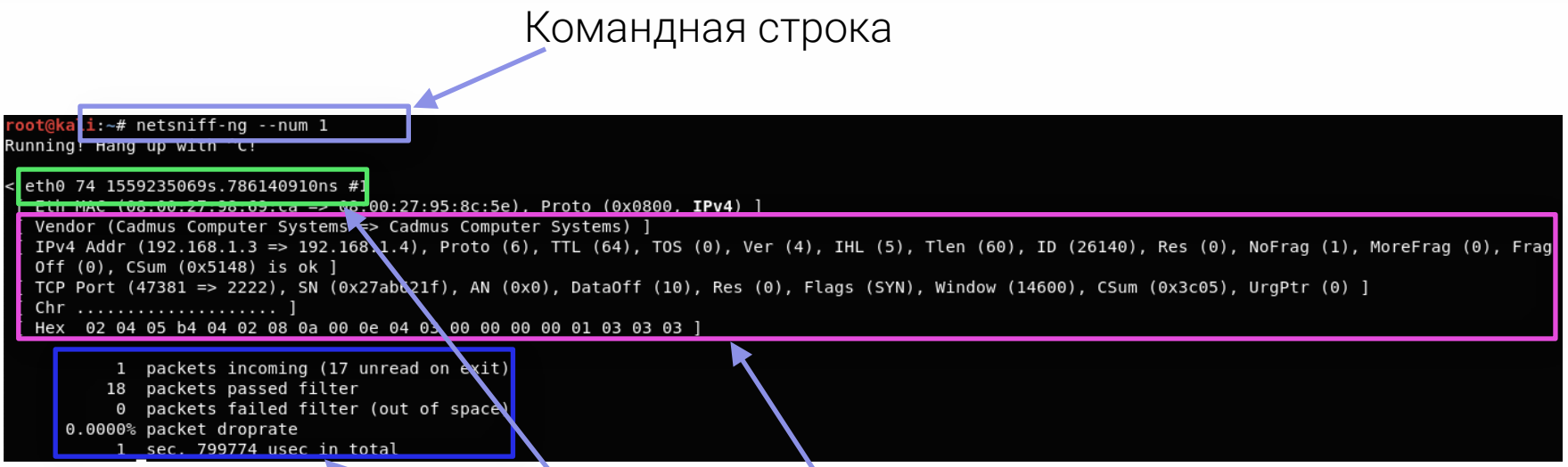
1. Снифферы
    - WireShark
    - Net-Miner
    - tcpdump
    - netsniff-ng
2. Респондеры
    - Responder
    - Ettercap
3. Прокси
    - Burp Suite
    - Owasp ZAP
    - mitmproxy
4. Библиотеки
    - libpcap
    - NpCap



WireShark (tshark)



netsniffer-ng



03

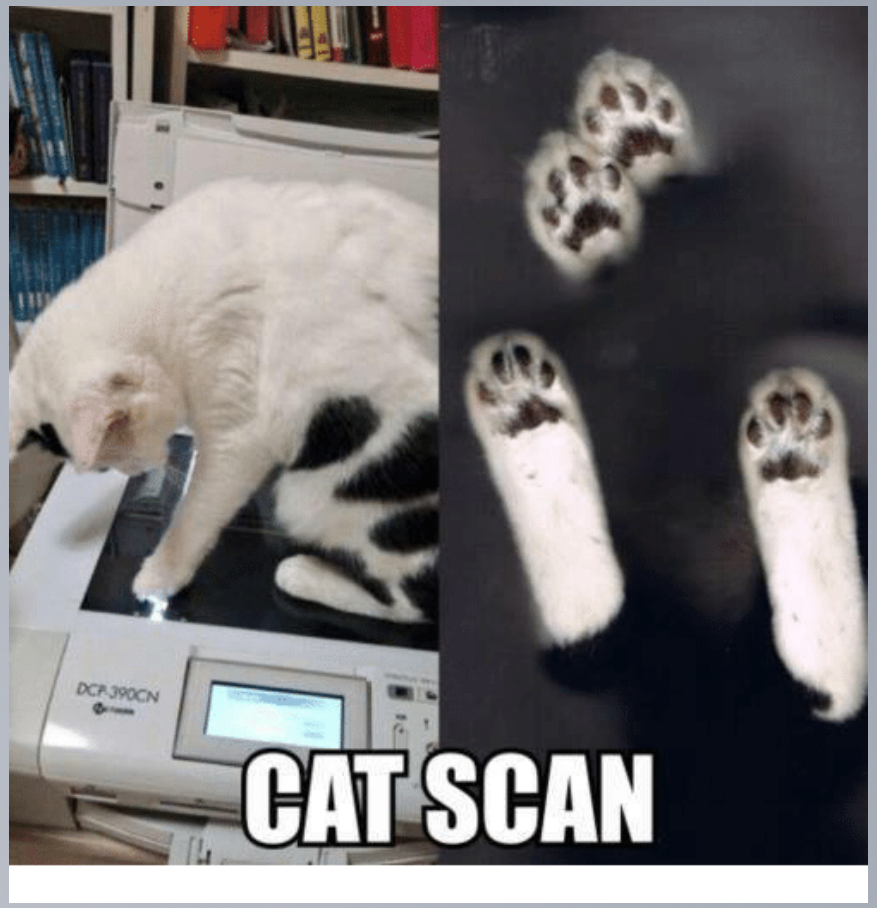
Сканирование сети

nmap

Сканирование:

Типы сканирования:

1. Syn, Fin, Ack, Xmas, Mainmon
2. Ping scan
3. Zombie Scan



01

Сканирование

Александр Колесников

Спасибо
за внимание!