# Antiphishing / Antimalware на трафике с применением Network Extension

Кудинов
Денис


@kudinovdw


@kudinovdenis

kaspersky

# Кому будет полезен этот доклад?



Разработчикам VPN / VPN-based технологий

Интересующимся сетевым взаимодействием на платформе iOS, или подробностями работы сети

Тем, кто хочет иметь возможность контролировать весь трафик на устройстве

# Агенда



Для чего анализировать трафик?

Доступный инструментарий

Решение от Kaspersky

Развитие технологии

# Агенда



Для чего анализировать трафик?

Доступный инструментарий

Решение от Kaspersky

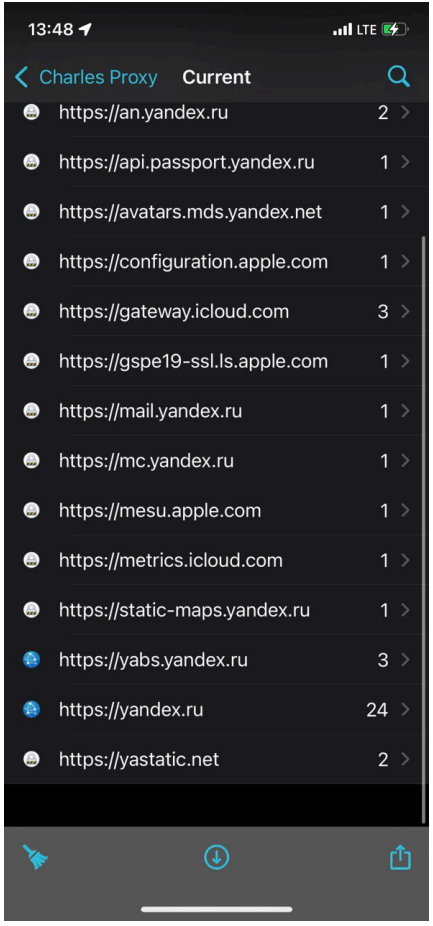
Развитие технологии

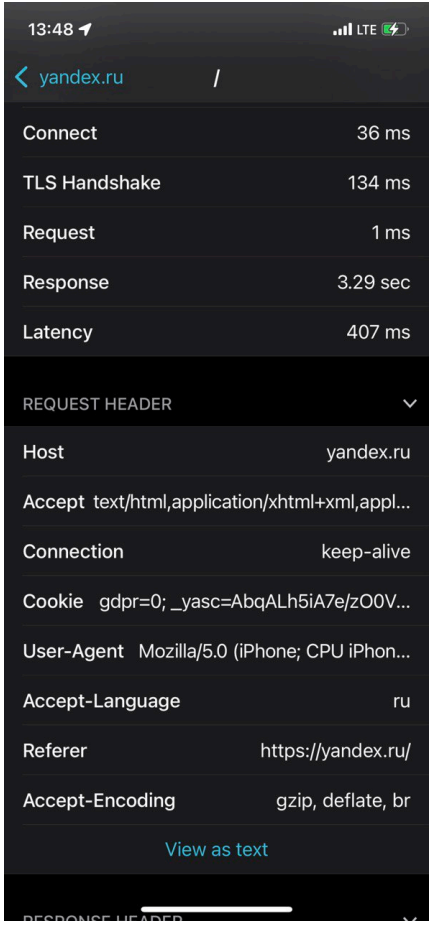
# Для чего анализировать трафик?

# Применимость технологии

Слышали про Charles Proxy?

# Для чего анализировать трафик?
# Charles Proxy



# Применимость технологии

Do not track технологии
Трекеры, сбор аналитики, etc

Слышали про Charles Proxy?

Антивирусные и антифишинговые технологии

Контроль использования устройства

Блокировка нежелательного контента

# Агенда



Для чего анализировать трафик?

Доступный инструментарий

Решение от Kaspersky

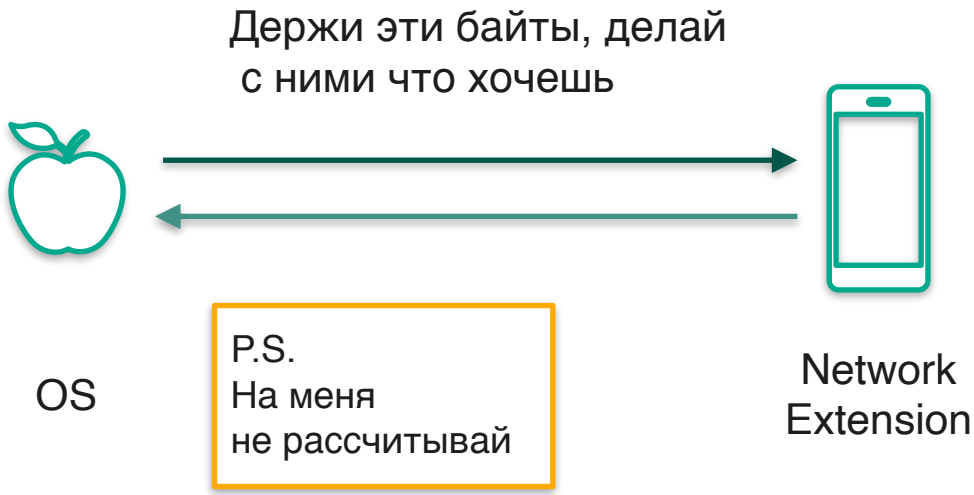
Развитие технологии

# Доступный инструментарий

# Как хотелось бы, чтобы оно работало

# Как работает на самом деле





# Доступный инструментарий:

NetworkExtension.framework

# NetworkExtension.framework



Самый низкоуровневый API на платформе для взаимодействия с сетевым интерфейсом

Позволяет получать доступ ко всему трафику, или выборочно

Слабо документирована, и редко используема

# NetworkExtension.framework: Виды



PacketTunnel

AppProxy

Supervise

ContentFilter

Supervise

DNS

Supervise

# NetworkExtension.framework: PacketTunnel



Предоставляет возможность использовать Туннелирование

Применяется для VPN-технологий

Возможно изменение пакетов на самом низком уровне

# Как поможет PacketTunnel?



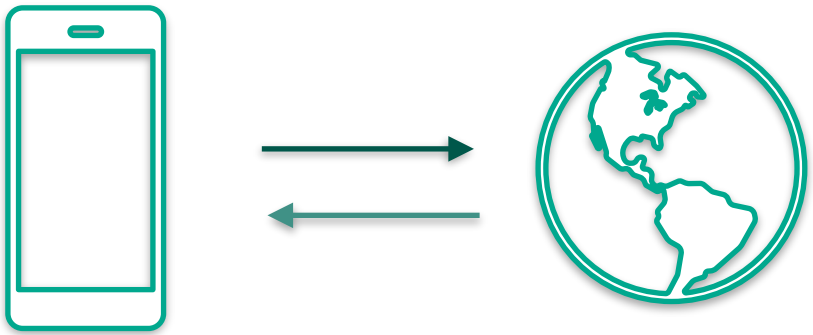
Никто не обязывает действительно создавать туннель до удалённого сервера

Доступ ко всему трафику на устройстве

Система (читай приложения) не получат ответ от сети, пока мы его не обработаем

Always-On (пока не крашнется 🙂)

# PacketTunnel: Structure



iOS Application

Extension

```
func startTunnel(options: [String : NSObject]? = nil,
                 completionHandler: @escaping (Error?) -> Void)
```

```
func stopTunnel(with reason: NEProviderStopReason,
                completionHandler: @escaping () -> Void)
```

```
func readPacketObjects(
    completionHandler: @escaping ([NEPacket]) -> Void
)
```

```
func writePacketObjects(_ packets: [NEPacket]) -> Bool
```

```
open class NEPacket : NSObject, NSCopying, NSSecureCoding {

    public init(data: Data, protocolFamily: sa_family_t)

    open var data: Data { get }
    open var protocolFamily: sa_family_t { get }
    open var metadata: NEFlowMetaData? { get }

}
```

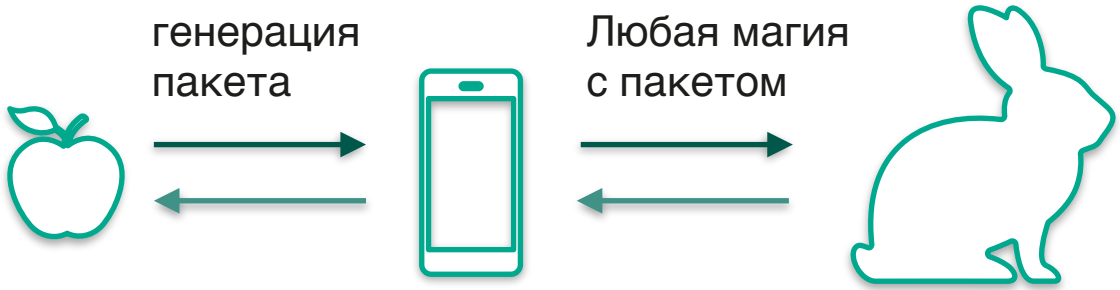
# Почему NEPacket такой, какой он есть?

Сделали максимально простую API

Парсинг пакетов — сложная и дорогостоящая операция

При необходимости разработчик сам будет парсить пакет

Те


генерация
пакета
Любая магия
с пакетом
OS
Network
Extension

# Агенда



Для чего анализировать трафик?

Доступный инструментарий

Решение от Kaspersky

Развитие технологии

# Решение от Kaspersky

# Что реализовали мы



Решение однонаправленное

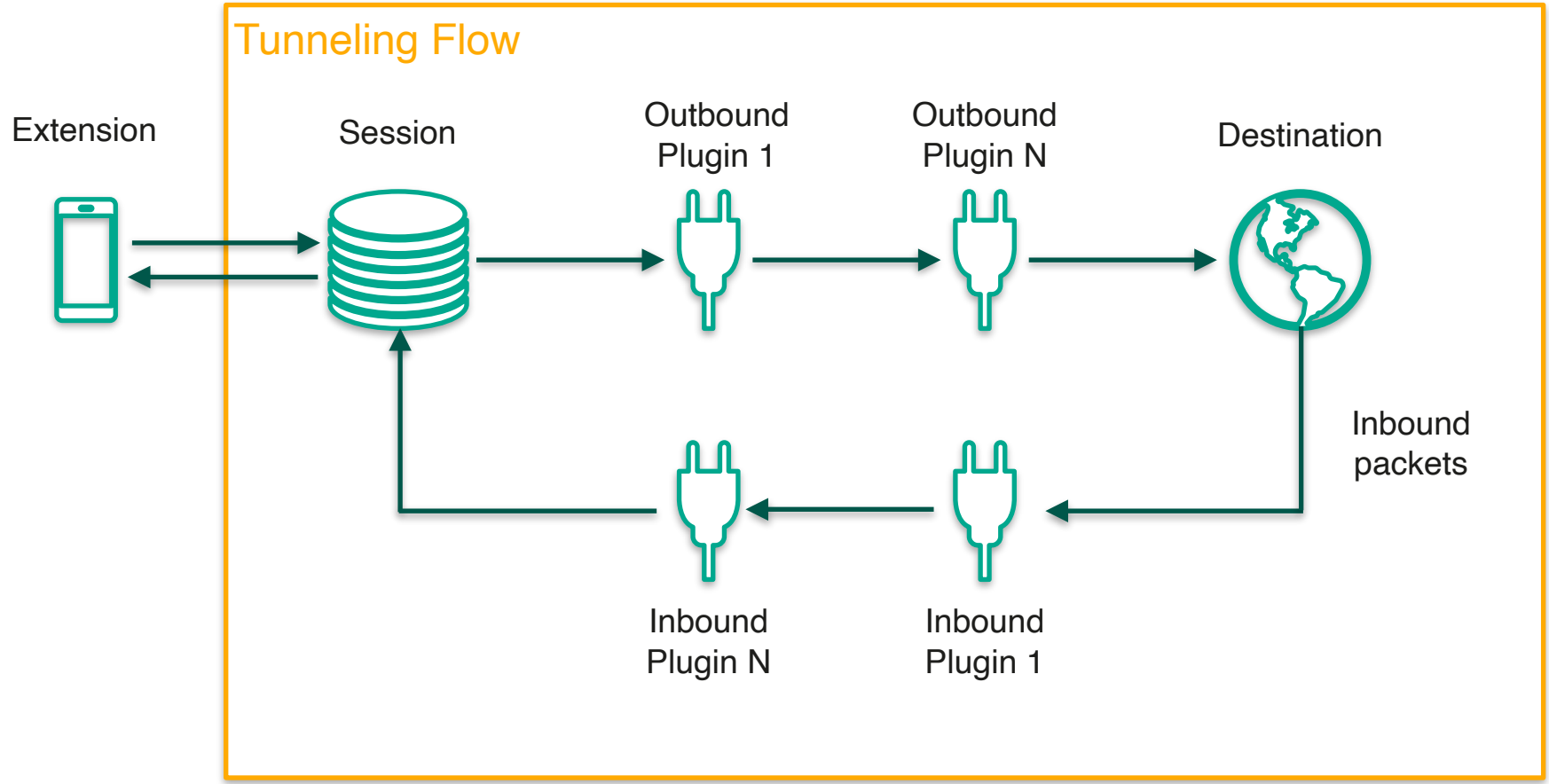
Построили систему,
основанную на плагинах

Ввели собственные абстракции
взамен никаких от Apple

Учли свой предыдущий опыт

Держали в уме
производительность

# Поверхностная схема нашего решения



TunnelingFlow

Outbound Plugins

Inbound Plugins

Destination

# TunnelingFlow: OutboundPlugins



Работают параллельно

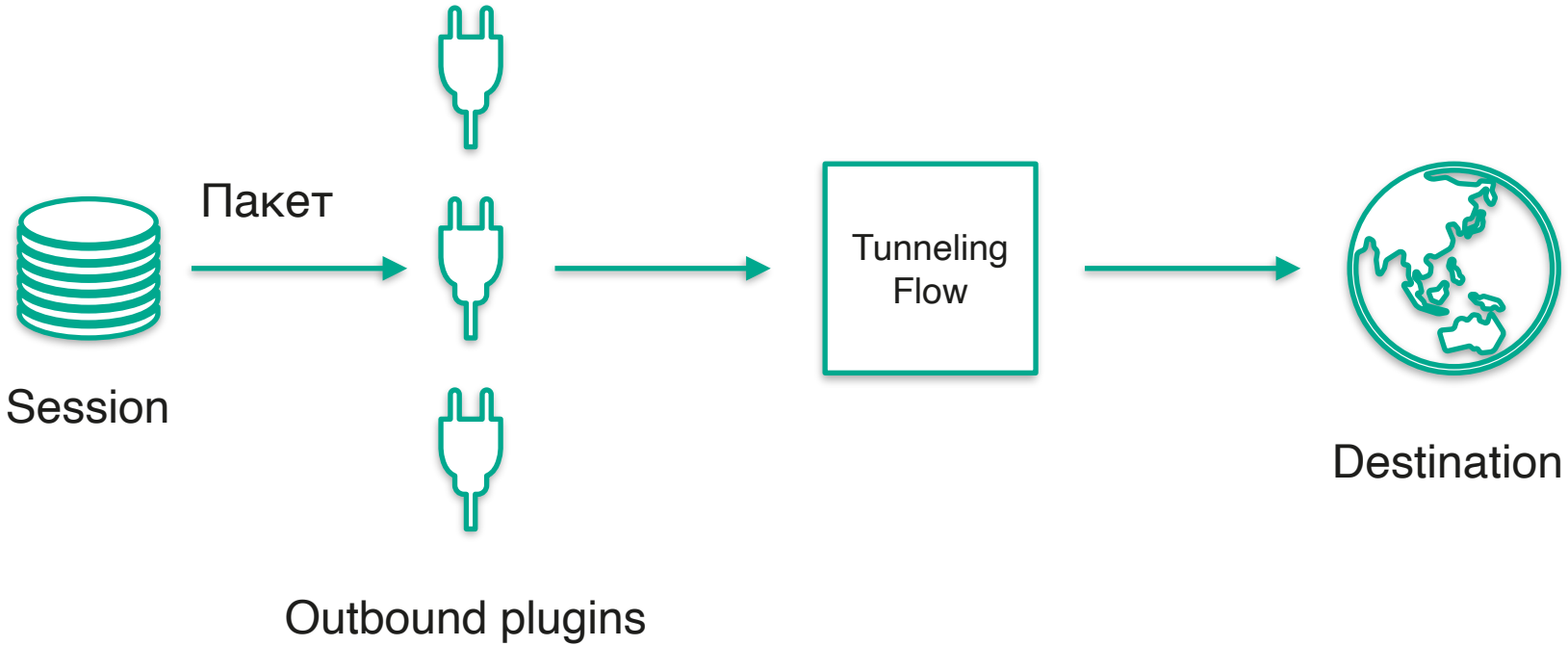
Предназначены для обработки исходящих пакетов

Могут реджектить пакеты

Могут вносить изменения в пакеты

Таких плагинов может быть N

# TunnelingFlow: OutboundPlugins



# TunnelingFlow: Destination



Выполняет роль полезной нагрузки

Как результат своей работы — генерирует InboundPacket

Отправляет пакеты в VPN / другие удалённые машины

# TunnelingFlow: InboundPlugins



Работают с “входящим” трафиком

Могут изменять пакеты

Могу реджектить пакеты

Работают последовательно

# TunnelingFlow: Какие бенефиты получаем



Получаем удобные механизмы для похода в сеть при необходимости

Чётко разграничиваем работу с входящим и исходящим трафиком

Можем включать и отключать функциональность (плагины) на лету

Получаем возможность “из коробки” блокировать запросы

Абстрагируемся от работы с изменениями в сети (Wi-Fi - LTE)

# Реализация защитных технологий

# Какие технологии можно реализовать



Анализ DNS запросов пользователя

Анализ HTTPS трафика

Анализ HTTP трафика

# Необходимые операции

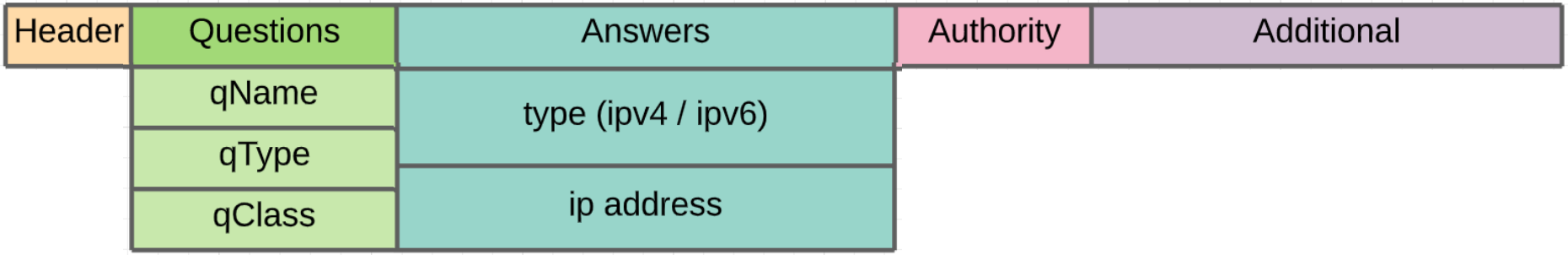
Распознать исходящий DNS-запрос

Резолв доменного имени

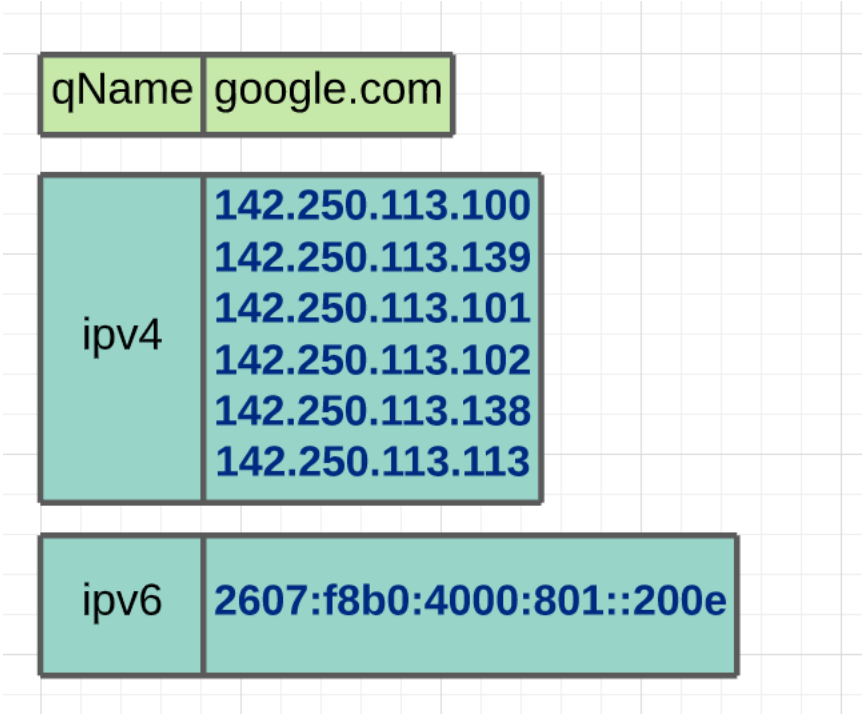
Выделить доменное имя

Модификация ответа от DNS-сервера при необходимости

# Как выглядит DNS пакет



# google.com


qName
google.com
ipv4
142.250.113.100
142.250.113.139
142.250.113.101
142.250.113.102
142.250.113.138
142.250.113.113
ipv6
2607:f8b0:4000:801::200e

# Как правильно парсить DNS пакет

Open Source решения:
wireshark, Pcap++, …

Писать своё

# Как можно использовать резолв DNS для защиты?

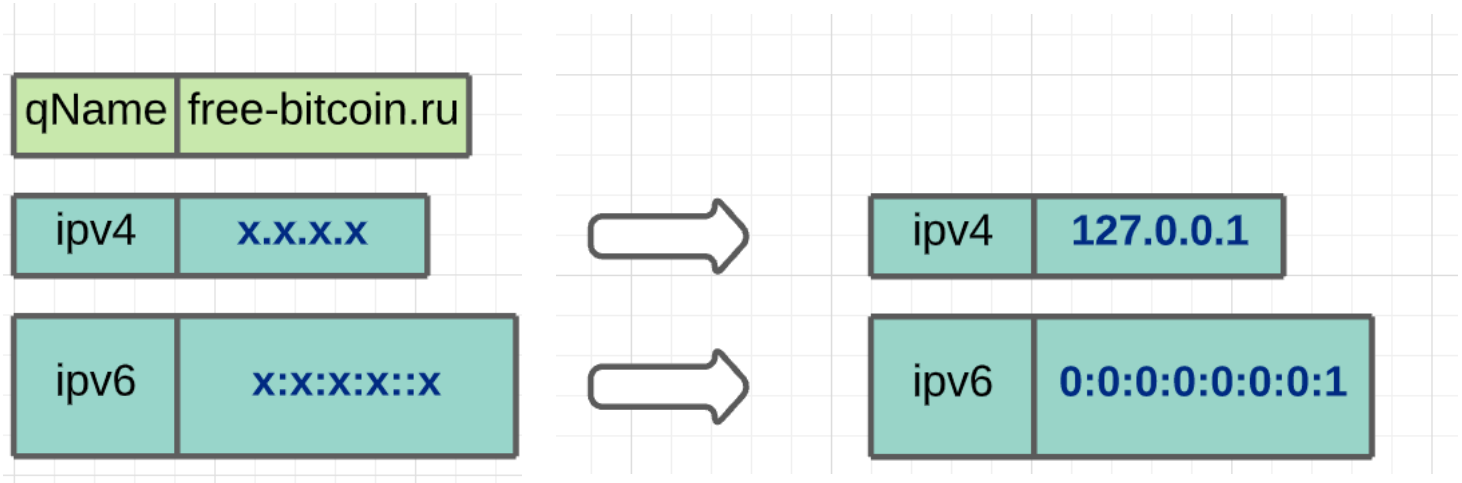
Можем подменить адрес в ответе от DNS-сервера

Не отвечать на запрос совсем. Тогда запрос отвалится по таймауту

Если заведомо знаем о блокировке, можем крафтить dns-ответ локально

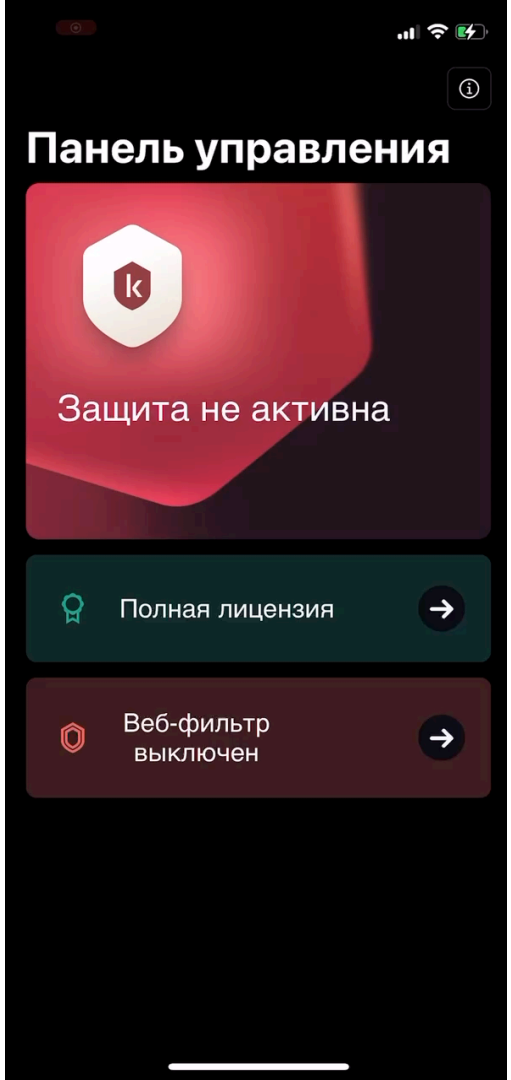
Поменять на какой-то свой ip сайта не получится. Браузеры для такого слишком умные

# free-bitcoin.ru



# Demo




Панель управления
Защита не активна
Полная лицензия
Веб-фильтр
выключен

# Как правильно парсить DNS пакет

Open Source решения:
wireshark, Pcap++, …

Писать своё

# Как правильно парсить DNS пакет

Open Source решения:
wireshark, Pcap++, …

Писать своё

# Плагины для работы с DNS

## Outbound Plugin

Разбирает DNS пакет, достаёт из него имя
Инициирует получение вердикта

## Destination

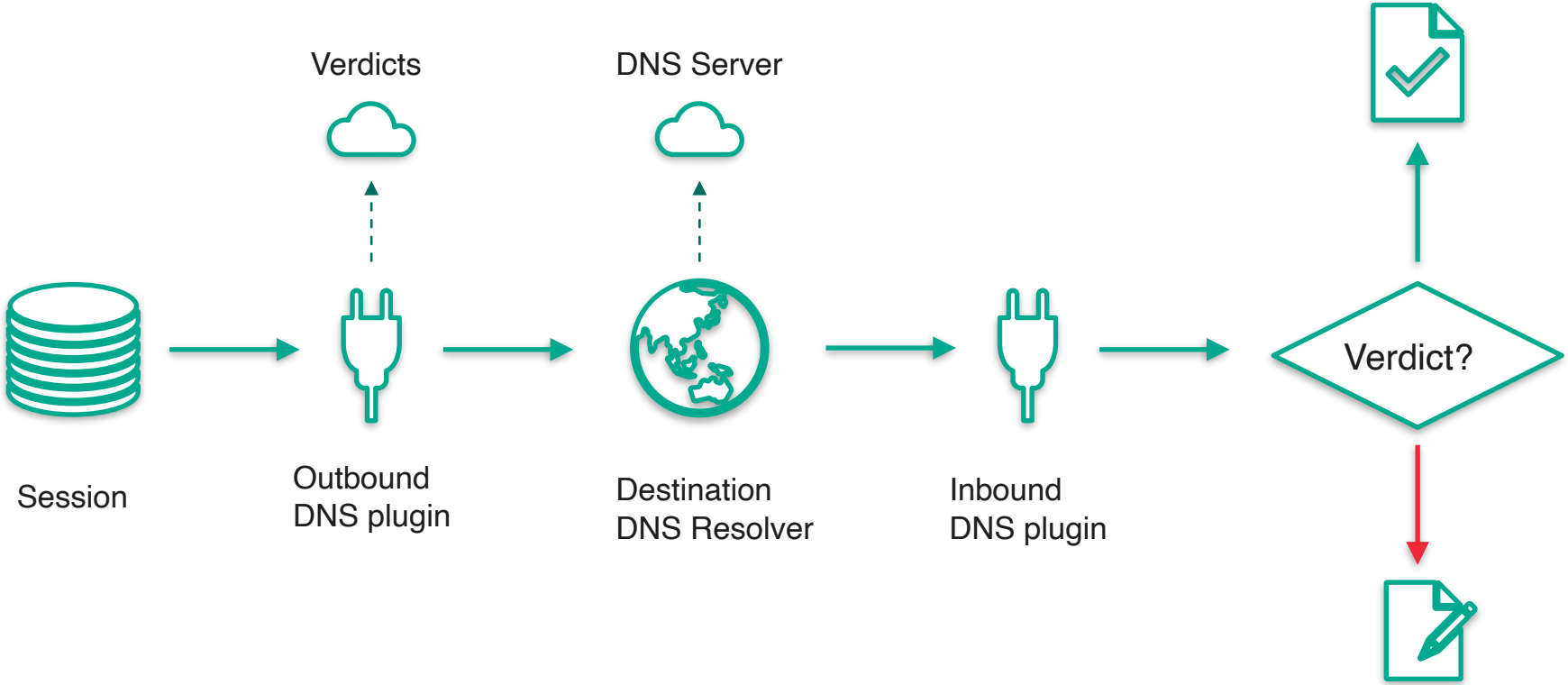
Резолвит доменное имя в ip-адрес

## Inbound Plugin

Модифицирует пакет
Проводит фильтрацию

# Реализация защиты. TunnelingFlow





# VPN

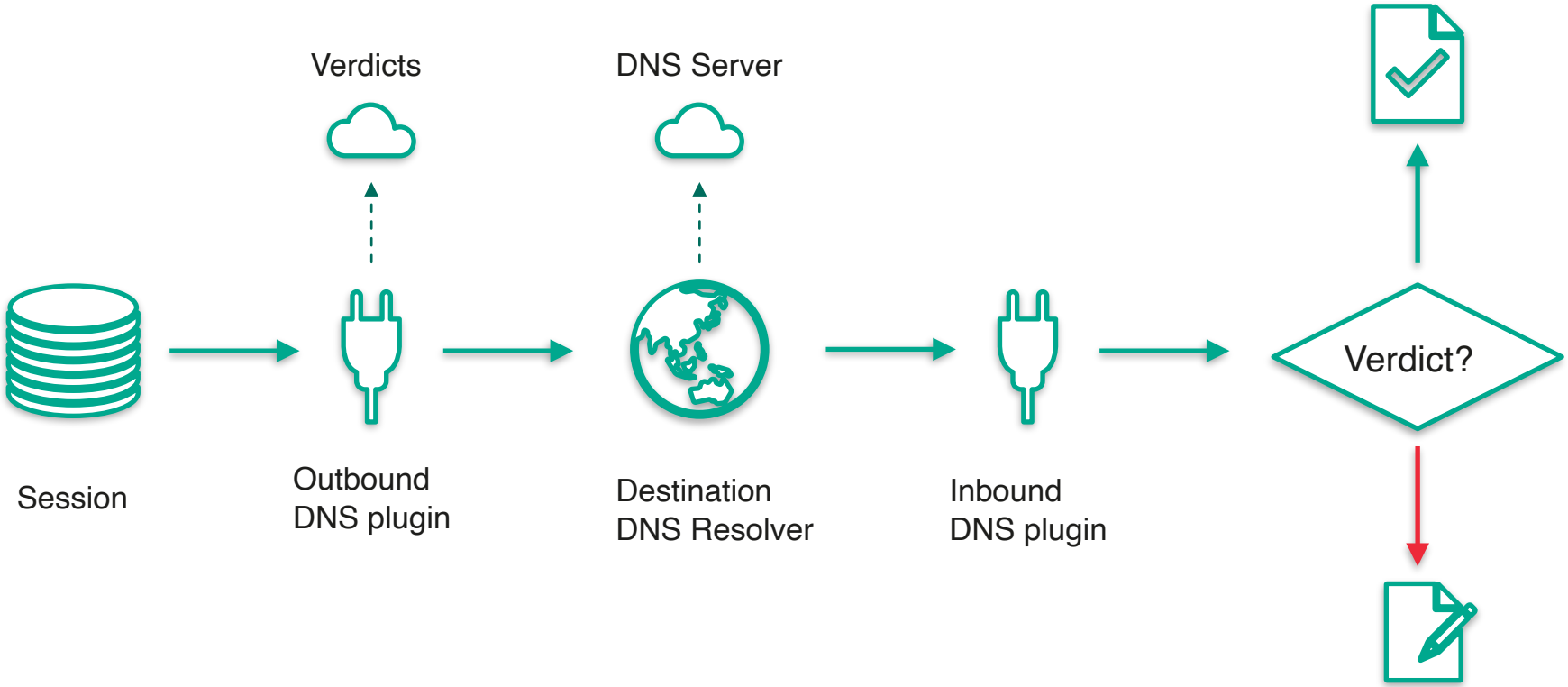
Это отдельный Destination

Всё общение зашифровано, в том числе DNS

Весь трафик перегоняет в удалённый сервер

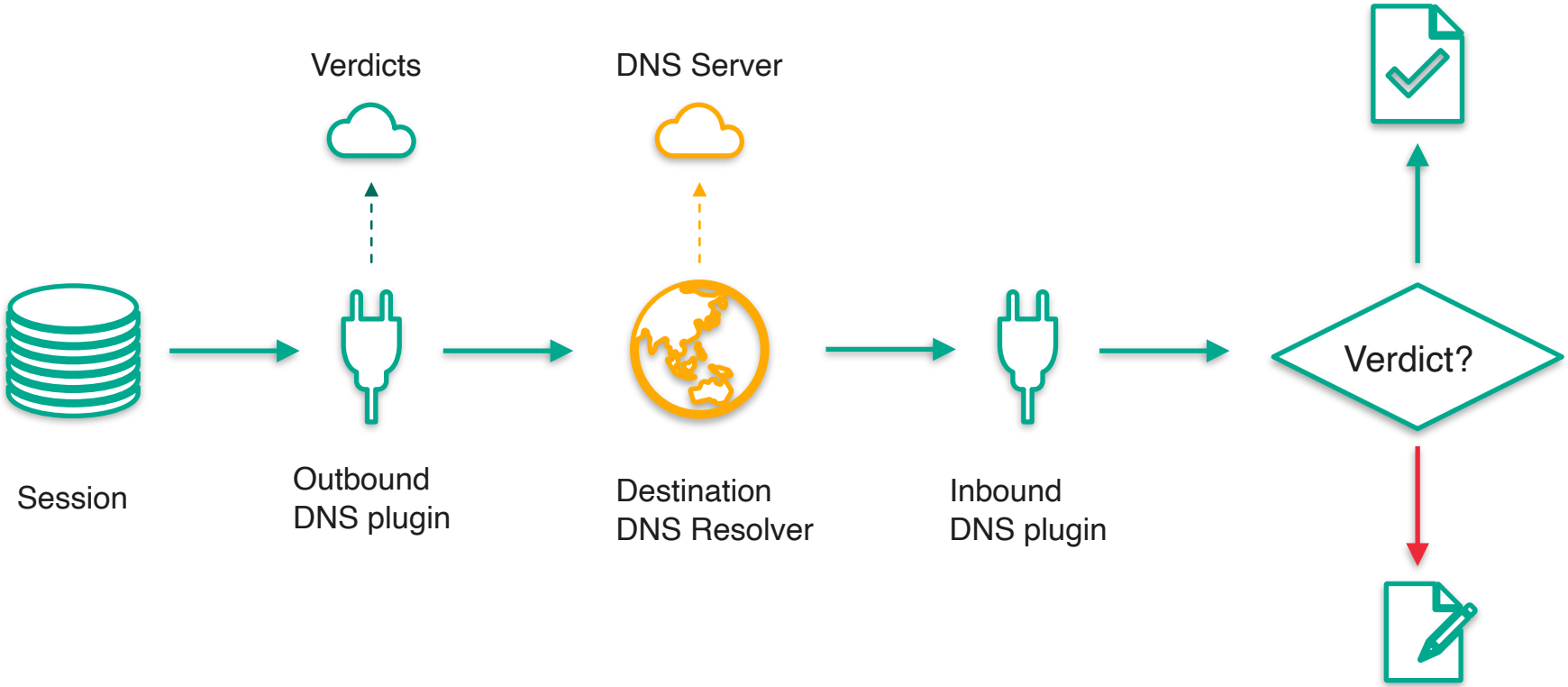
# Реализация защиты. VPN





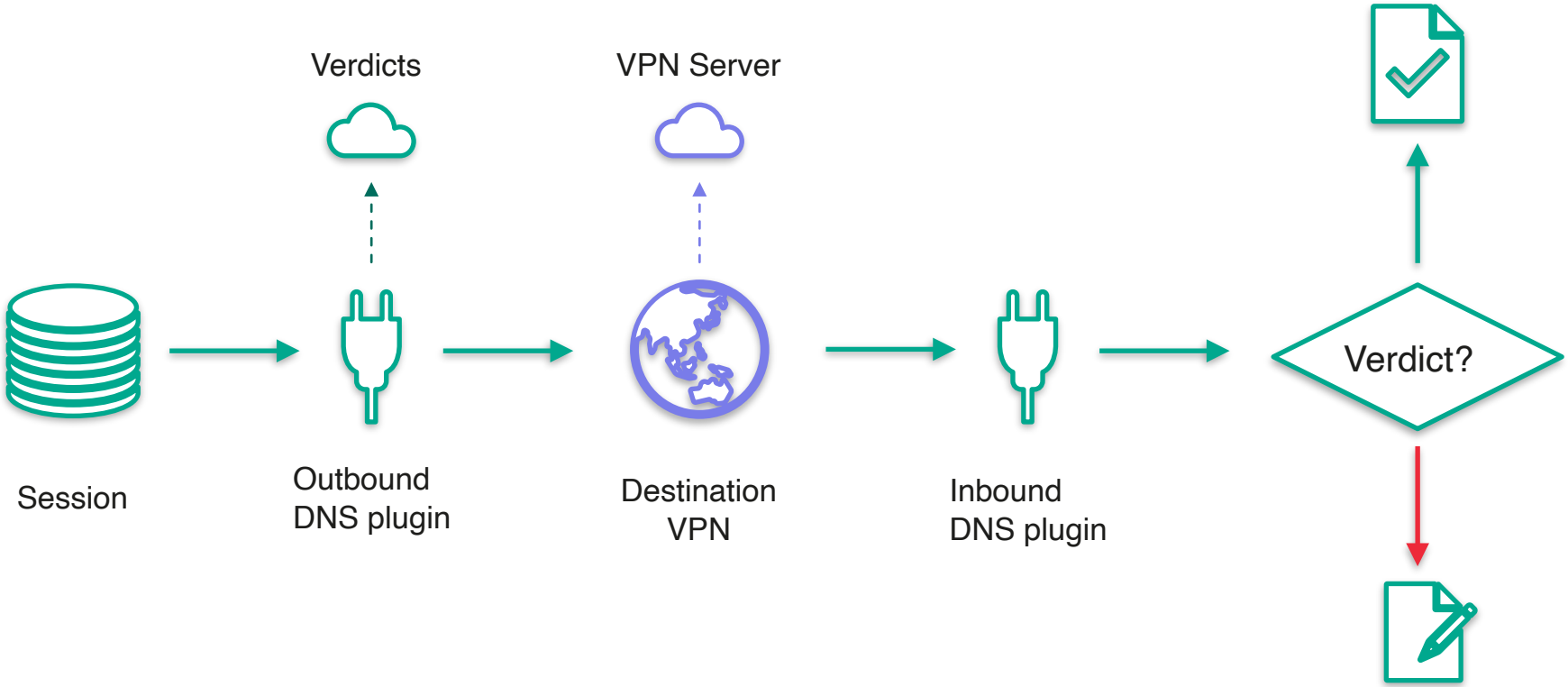
# Реализация защиты. VPN





# Реализация защиты. VPN





# Агенда



Для чего анализировать трафик?

Доступный инструментарий

Решение от Kaspersky

Развитие технологии

# “Там было что-то про HTTP”

Проводить анализ HTTP трафика можно

Есть больше возможностей для контроля. Например, видны url

Довольно сложный стандарт для парсинга

HTTP трафика осталось не так много. Но фишинг на нём встречается.

# HTTPS

С некоторыми оговорками тоже возможно

Все бенефиты от HTTP

Требуется установка рутового сертификата

Пиннинг в большинстве случаев не позволит такой трюк, и приложение просто перестанет работать

# Полезные ссылки



Исследование от  ETH (SpySpy)
https://nsg.ee.ethz.ch/fileadmin/user_upload/theses/MA-2016-47.pdf

Apple Documentation
https://developer.apple.com/documentation/networkextension

Стандарт DNS
https://datatracker.ietf.org/doc/html/rfc1035

# Спасибо за внимание. Вопросы?

P.S. Мы активно нанимаем iOS разработчиков
https://careers.kaspersky.com/vacancy/13457/

kaspersky

Кудинов
Денис

@kudinovdw

@kudinovdenis