



Ideas Locas

# El talento de Mr. Ripley

Identidad digital, OSINT y  
Footprinting



# Presentación

## Contenidos

¿Quién soy?

Contenidos del Taller

# Sobre Mí

Información acerca de lo que hago



Lucas Fernandez

¬\(\_ツ)\_/¬



lucferbux



lucferbux

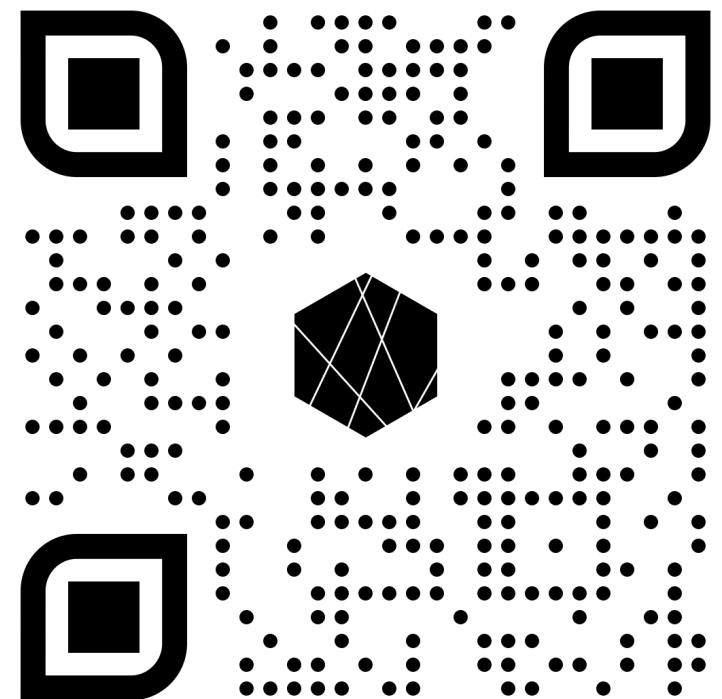


lucferbux

Investigador/Desarrollador en Ideas Locas de Telefónica

- Graduado en Ingeniería Informática
- Máster en Seguridad de la información.
- Investigación y Seguridad
- Ideas Locas
- Universidades
- Blogs

3



<https://lucferbux.dev>

# Timeline

4

## Presentación y organización

COMIENZO

¿Quién soy?  
Contenido del Taller  
Timeline

Identidad Digital  
Ataques y Causas  
OSINT  
Automatización



## OSINT



## Metadatos y Footprinting

Reconocimiento  
Footprinting  
Metadatos

# Timeline

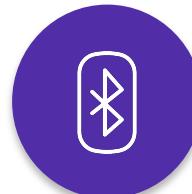


## Perfilado Red

Pila OSI  
Navegación Apps  
SSL/TSL

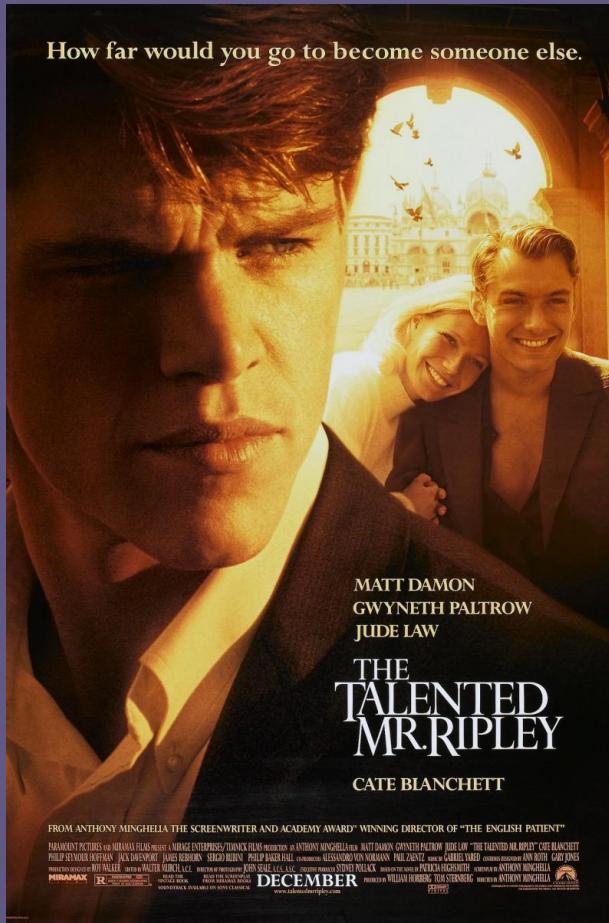


BLE Advertisements  
Sniffing Paquetes BLE  
Airdrop



## Perfilado BLE

Final





# OSINT

## Contenidos

Identidad Digital, Huella Digital,  
Open Source Intelligence, Técnicas  
de Automatización, Card Reader

# Identidad Digital - Introducción

OSINT

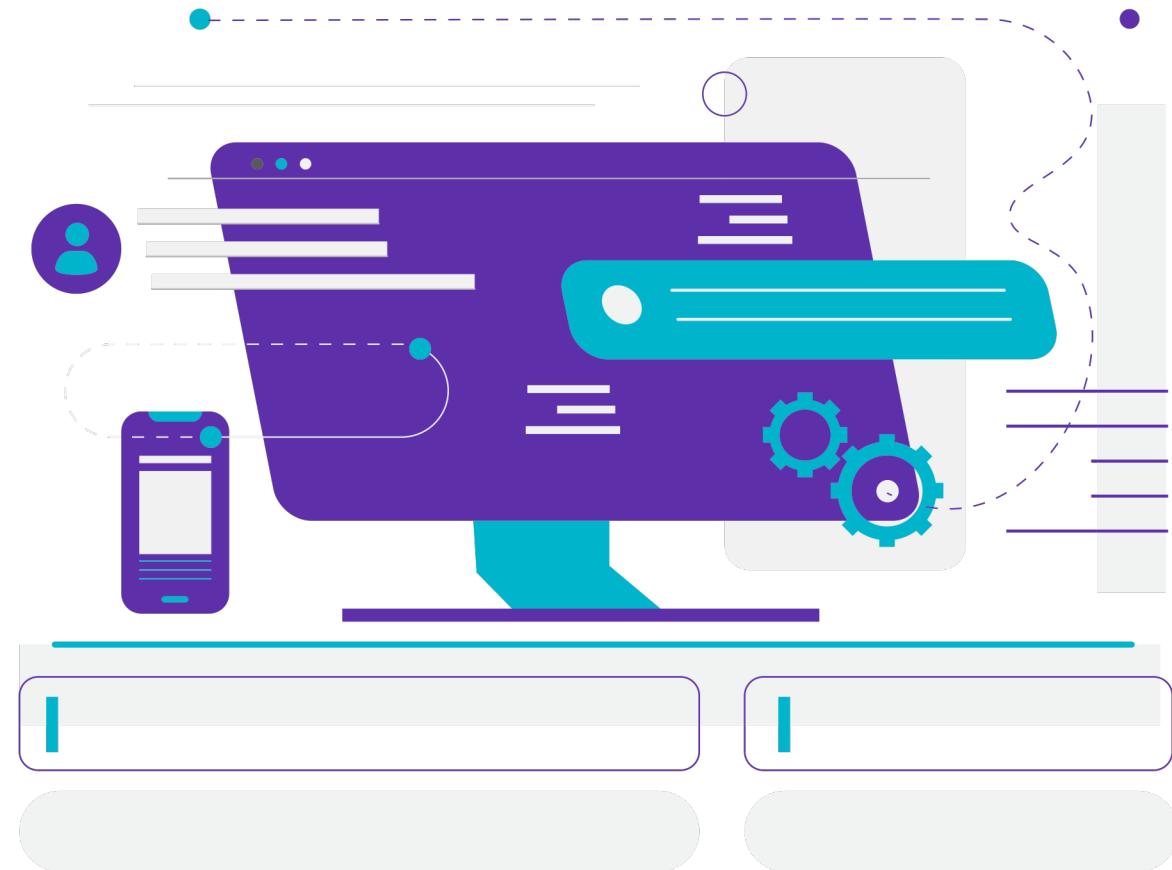
METADATOS

PERFILADO RED

PERFILADO BLE

8

- Todo lo que nos identifica en entorno **online**
- Fotos, gustos, descripciones, videos, correos
- Vamos generando continuamente información
- Al navegar, aumentamos nuestra **huella digital**



# Identidad Digital - Ataques

OSINT

METADATOS

PERFILADO RED

PERFILADO BLE

9



**7 de cada 100** usuarios victimas de robo o abuso de datos

Phising | Pharming | Identidad Sintética

Falta de concienciación, amplia huella digital,

"leaks" de datos, páginas inseguras...

# Open Source Intelligence

OSINT

METADATOS

PERFILADO RED

PERFILADO BLE

10



## PROCESAMIENTO

La información es recolectada, analizada y diseminada para el propósito designado. Muchas veces este suele ser el trabajo más complejo



## MASIFICACIÓN

Hace años, el problema en OSINT era la falta de información, actualmente el problema es la gran cantidad de ruido que produce el exceso de información



## METODOLOGÍA

Se obtiene información que está disponible al público, de lo que se denominaría "Surface Web"



## PELIGRO

OSINT es una arma de doble filo: Todo lo que encontramos que puede ayudarnos en mejorar nuestra seguridad puede ser usado por atacantes en nuestra contra



## ACTIVIDAD ESTRATÉGICA

Es una actividad estratégica de cualquier organización (e individuo) para tener control sobre sus datos



# Dirty Business Card

## Descripción

Dirty Business Card es un servicio modular de OSINT que, a través de unos pocos datos que podemos encontrar en cualquier tarjeta de visita, recopila información de la víctima a través de múltiples leaks, servicios o herramientas

The screenshot shows a web application titled "Card Reader" from "Eleven Paths". The main card information is as follows:

Field	Value
Name	Lucas Fernández Aragón
Organization	Ideas Locas
Address	Distrito Telefónica Edificio Noreste 0, planta 0 Ronda de la Comunicación s/n 28050 Madrid
Phone	+34689623546
Email	fakemail@gmail.com
Username	@lucferbux

Below the card, there is a form with the same fields for input, each with a character limit indicator (e.g., 22/30, 12/30, 18/30, 10/30) and a "Reset" button.



Recopilación de información  
A través técnicas OSINT



Extracción de datos  
Extracción de datos de una tarjeta con OCR

# Arquitectura

OSINT

METADATOS

PERFILADO RED

PERFILADO BLE

12

1. Interfaz web con capacidades **PWA**,  
disponible para móvil y ordenador.
2. Docker que contiene la página web y el  
servidor.
3. Dos contenedores, uno para la página en  
**Angular** y otro para el servidor en **Flask**



# PoC - ¿Cómo funciona?

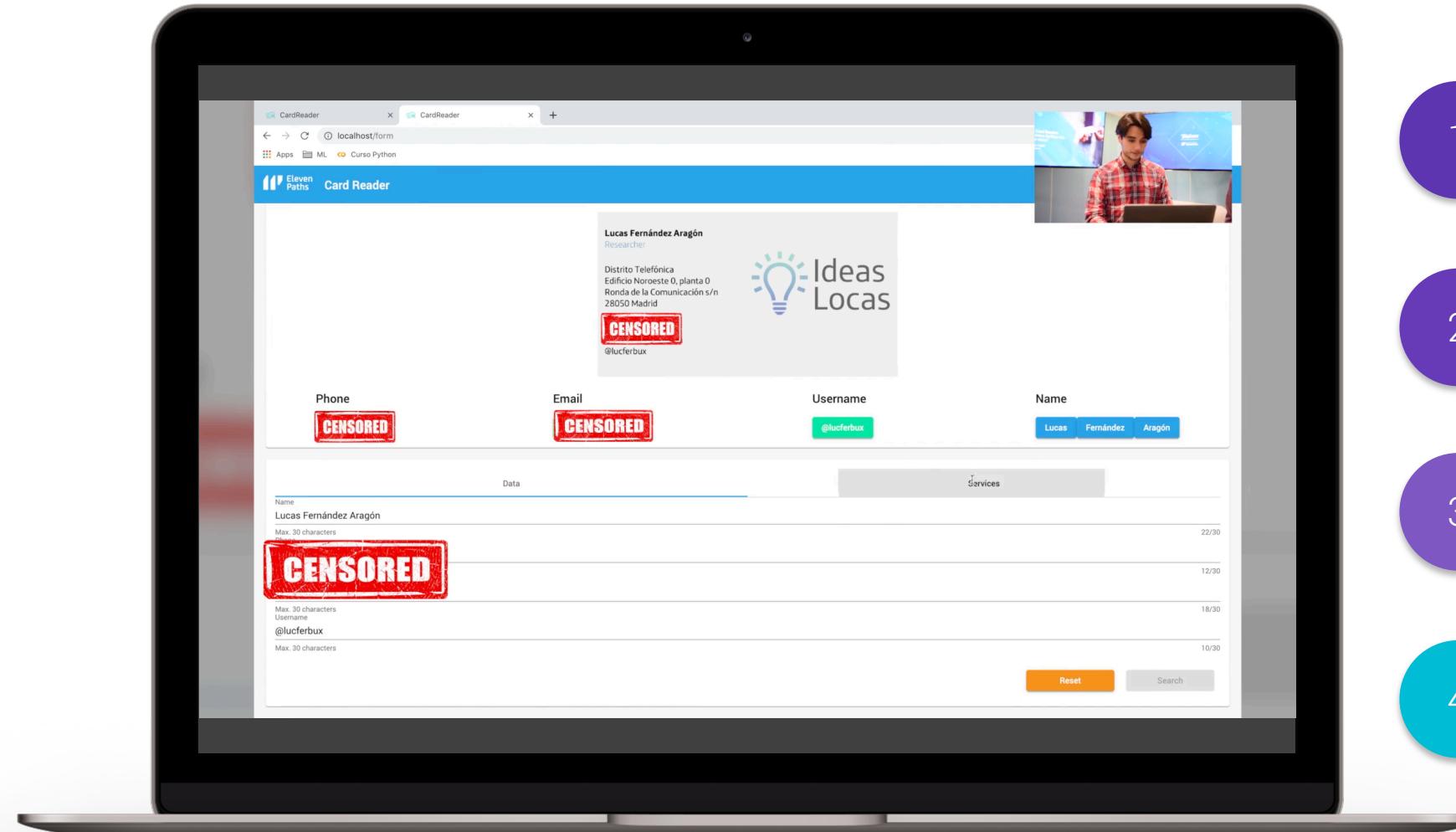
OSINT

METADATOS

PERFILADO RED

PERFILADO BLE

13



1

Se procesa la tarjeta de contacto mediante Visión Artificial

2

La información se envía a un backend

3

Los módulos son ejecutados en paralelo

4

Los resultados se devuelven y se visualizan en cartas

# Ejercicios

OSINT

METADATOS

PERFILADO RED

PERFILADO BLE

14

1

## Leak Dispositivo

1. Poner modo incognito en navegador
2. Entrar en inicio de sesión google
3. Pulsar en "he perdido contraseña"
4. Probar diferentes métodos
5. Puede aparecer el terminal de recuperación

2

## Implementación Login

1. Entrar en wallapop.com
2. Pulsar registro o inicio de sesión
3. Pulsar "he perdido contraseña"
4. Si el usuario no está registrado la web nos lo dirá

3

## Búsqueda Inversa

1. Entrar en yandex.com
2. Ir a la sección de imágenes
3. Seleccionar la imagen que queramos hacer búsqueda inversa

4

## Averiguar Operador

1. Navegar a ardilla.ai
2. Seleccionar el número deseado
3. Realizar consulta
4. Comprobar la fiabilidad de la respuesta



# Metadata y Footprinting

## Contenidos

Reconocimienots  
Footprinting  
Metadatos  
Foca

# Reconocimiento

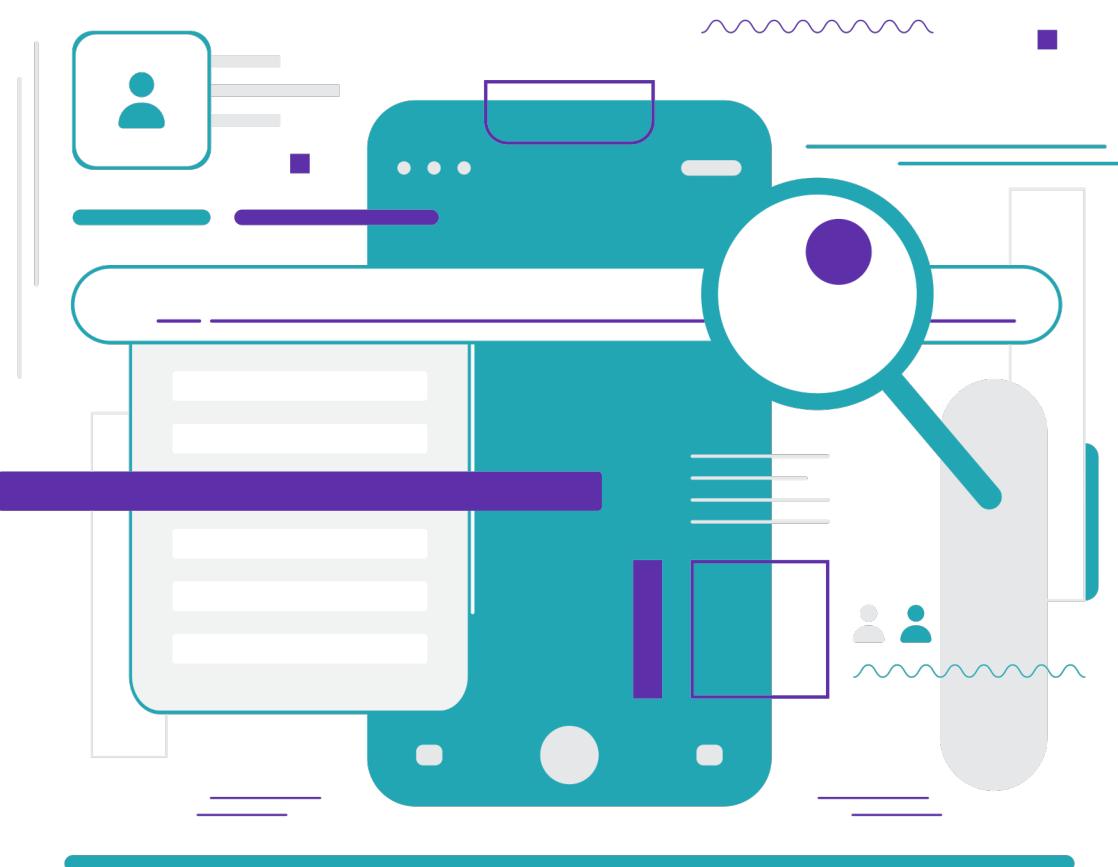
OSINT

METADATOS

PERFILADO RED

PERFILADO BLE

16



**Reconocimiento** -> Recolección de información  
de un entorno o víctima

**Footprinting** -> Recoge información de un  
ordenador, red o archivo.

**Fingerprinting** -> Proceso de encontrar  
características de un equipo

# Metadatos

OSINT

METADATOS

PERFILADO RED

PERFILADO BLE

17

1. **Metadato** -> “Datos sobre datos”, viene del griego μετά que significa más allá.
2. Datos estructurados que describen características de los datos.
3. Presentan diferencias dependiendo de las reglas.
4. Pueden clasificarse según diferentes criterios.
5. Ejemplos: Localización de fotos y resolución, fechas de modificaciones de archivos, autores...

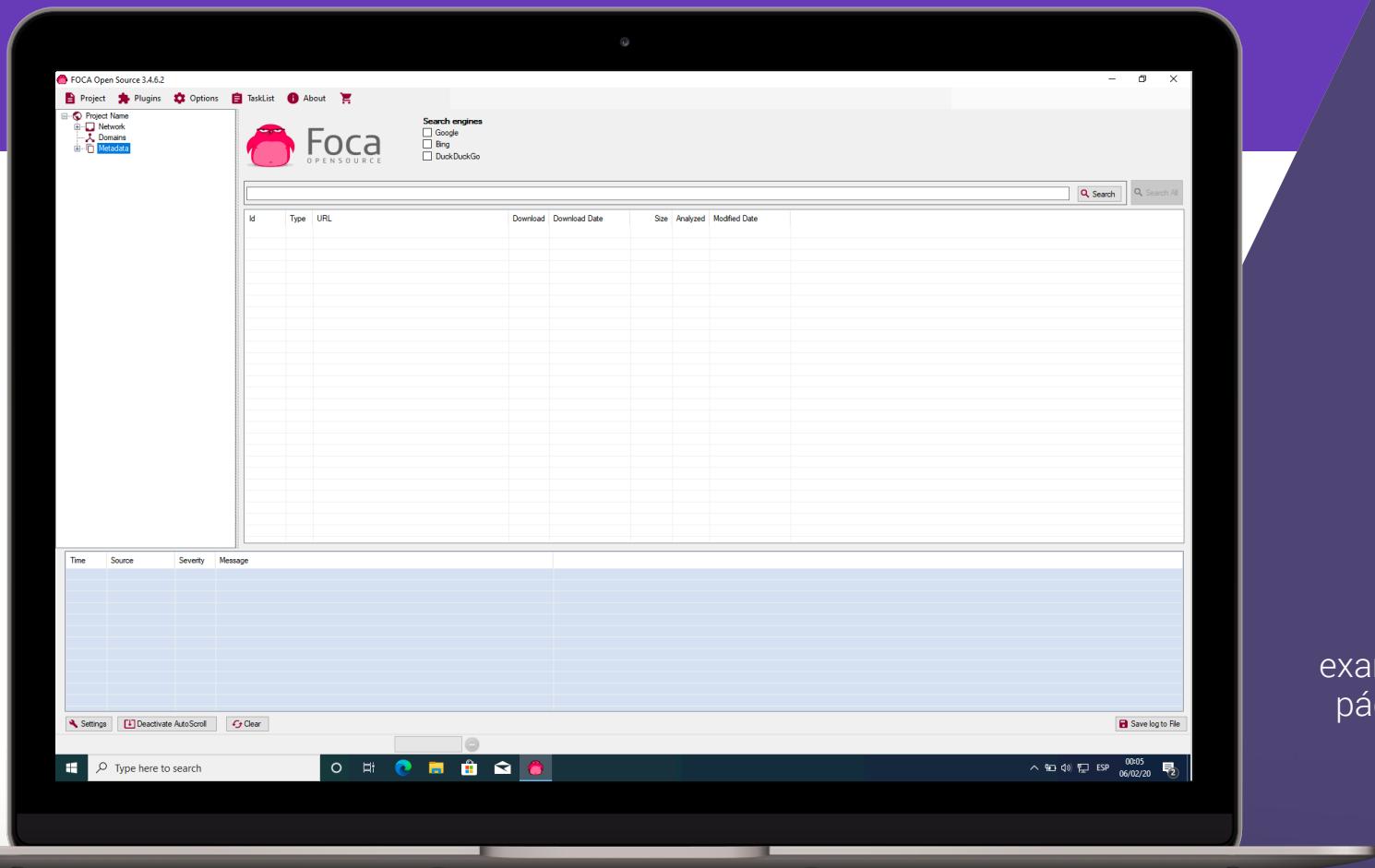




# Foca

PoC

Fingerprinting Organizations with Collected Archives es una herramienta utilizada principalmente para encontrar metadatos e información oculta en los documentos que examinamos. Estos documentos pueden estar en páginas web, y con FOCA se pueden descargar y analizar



Recopilación de información  
A través técnicas de Fingerprinting



Extracción de datos  
Y clasificación de organizaciones, archivos, roles...



Descarga

## Paso 1

Descargar la herramienta desde  
<https://github.com/El evenPaths/FOCA/releases>



.NET Framework 4.7.1

## Paso 2

Descargar e instalar .NET desde  
<https://www.microsoft.com/es-es/download/details.aspx?id=56116>



Visual C++ 2010

## Paso 3

Descargar e instalar Visual C++ desde  
<https://www.microsoft.com/es-es/download/details.aspx?id=14632>



SQL Server Express



Ejecución

## Paso 4

Descargar e instalar SQL Sserver desde  
<https://www.microsoft.com/es-es/sql-server/sql-server-downloads>

## Paso 5

Ejecutar la herramienta desde el fichero .exe

# PoC - ¿Cómo funciona?

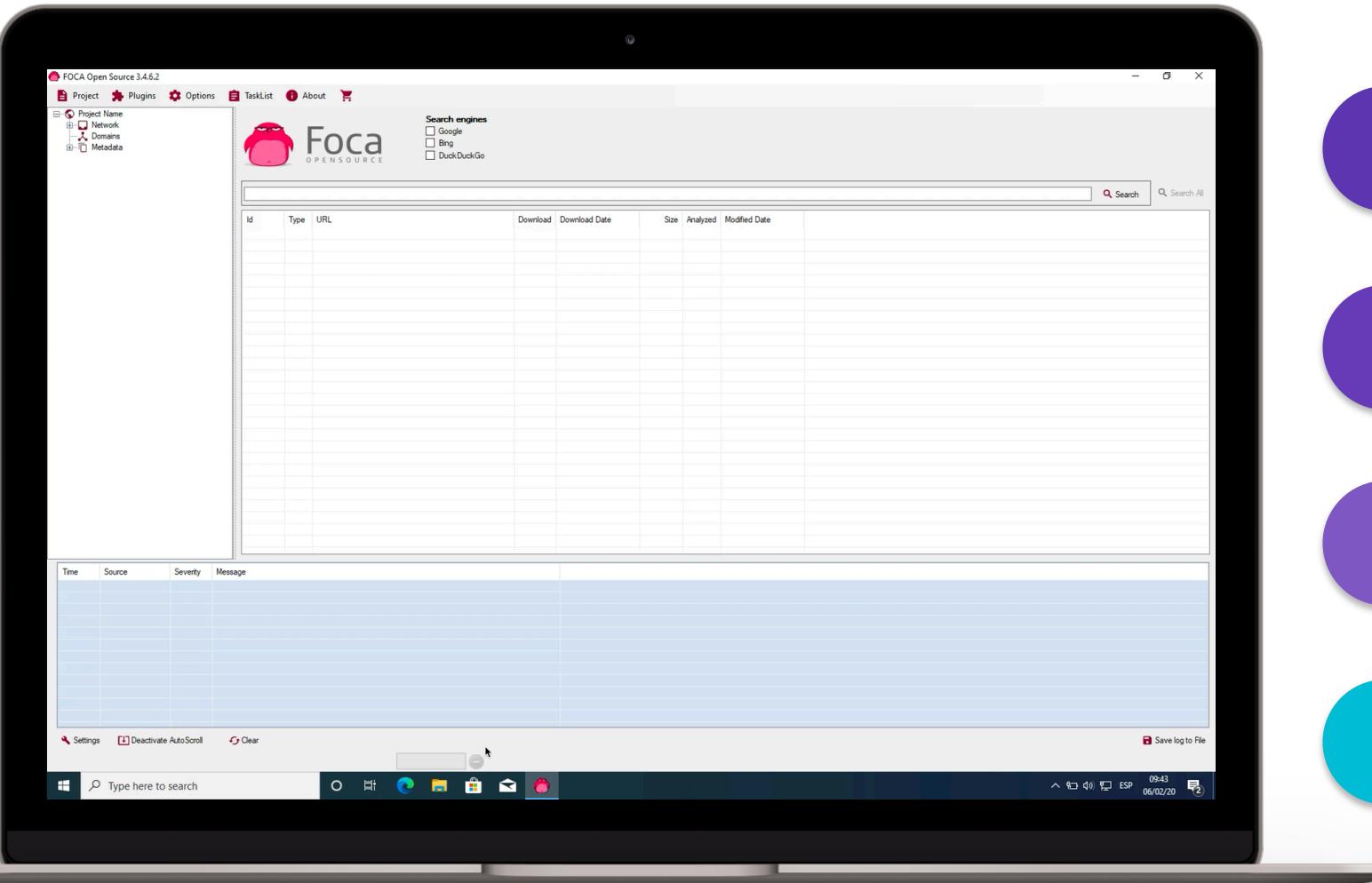
OSINT

METADATOS

PERFILADO RED

PERFILADO BLE

20



1

Se crea un nuevo proyecto dentro de una instancia de SQL

2

Se levanta la aplicación en .NET que contiene los plugins

3

Todos los progresos de la investigación se guardan en la instancia del proyecto

4

Desde la interfaz gráfica se van mostrando todos los resultados jerarquizados

# Ejercicios

OSINT

METADATOS

PERFILADO RED

PERFILADO BLE

21

1

2

3

4

## Fingerprinting

1. Instalar nmap
2. Abrir una terminal
3. Escribir el comando “sudo nmap -O -v [url]”
4. Visualizar la información

## Whois y Traceroute

1. Entrar en terminal
2. Ejecutar whois, ver la resolución del dominio
3. Ejecutar traceroute
4. Visualizar los saltos hasta el CDN

## Dnsmap

1. Instalar dnsmap
2. Ejecutar la herramienta en el dominio seleccionado
3. Argumentar los resultados

## Visualizar metadatos

1. Ejecutar el comando mdls en un archivo
2. Ejecutar el comando xattr en un archivo
3. Instalar exiftool
4. Ejecutar exiftool en un archivo



# Perfilado Red

## Contenidos

Pila OSI  
Navegación Apps  
SSL/TLS

# Pila OSI/TCP

OSINT

METADATOS

PERFILADO RED

PERFILADO BLE

23

1. Comunicación entre aplicación y programas
2. Se encarga del formato de datos y el cifrado
3. Establece, mantiene y maneja sesiones
4. Establece las conexiones punto a punto
5. Provee el direccionado y enrutamiento
6. Responsable de transferencia fiable a través de circuito
7. Transmisión bit a bit por el medio



# TCP, HTTP y TLS

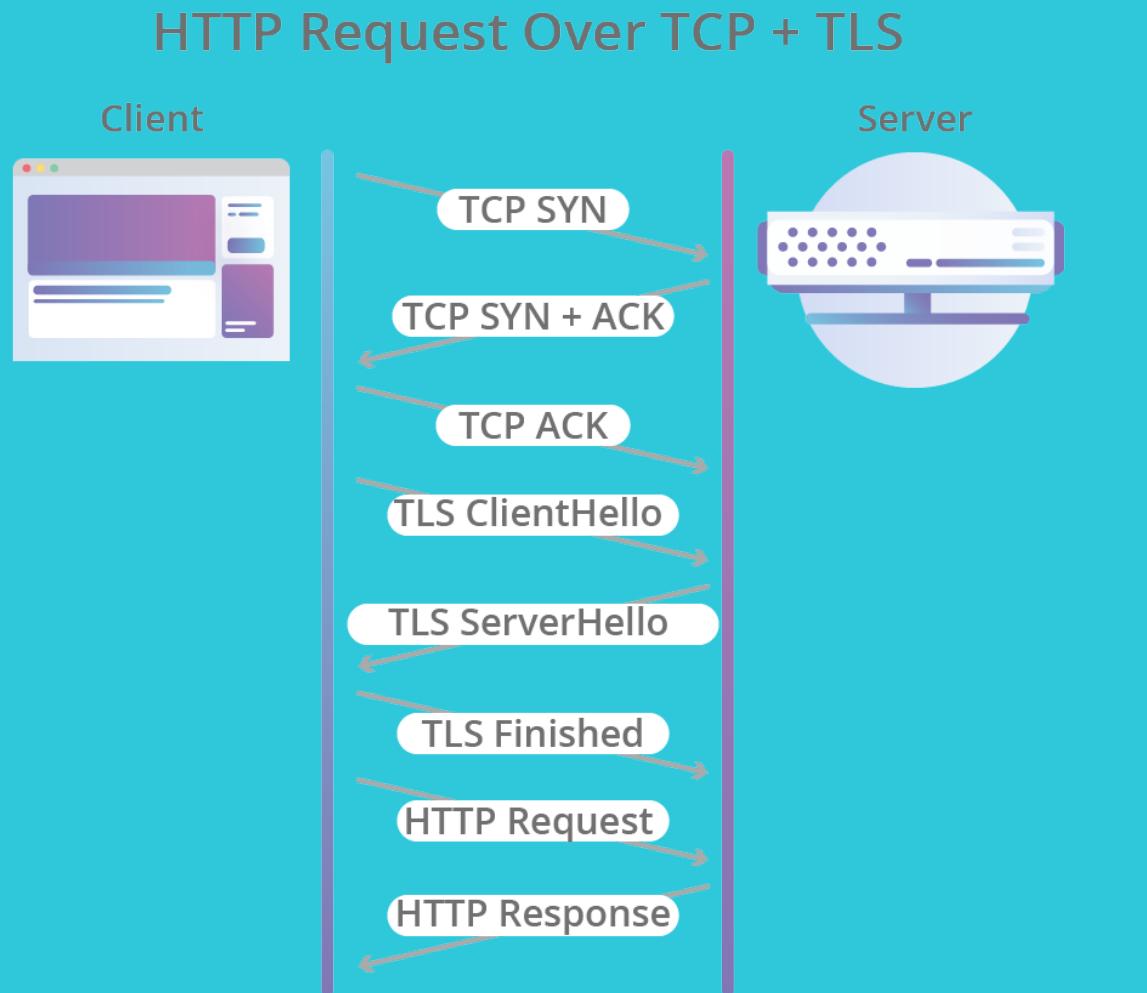
OSINT

METADATOS

PERFILADO RED

PERFILADO BLE

24



1. **TCP** -> Transmission Control Protocol. Capa de Transporte. Establece las conexiones punto a punto. Orientado a la conexión.
2. **HTTP** -> HyperText Transfer Protocol. Capa de aplicación. Permite las transferencias de información en la WWW. Actualmente HTTP/2.
3. **TLS** -> Transport Layer Security. Sustituyó a **SSL** como protocolo criptográfico que proporciona comunicaciones seguras por una red.

# Perfilado Red

OSINT

METADATOS

PERFILADO RED

PERFILADO BLE

25

**Sniffing** -> Técnica por la que un atacante “escucha” el tráfico entre dos puntos.

**Tcpdump/wireshark** -> Herramientas para capturar tráfico de sesión.

**TLS** -> Hace unos años, la mayoría de conexión estaba sin cifrar, pudiendo leer el contenido, alterar la información...

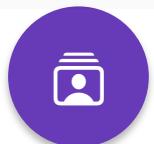
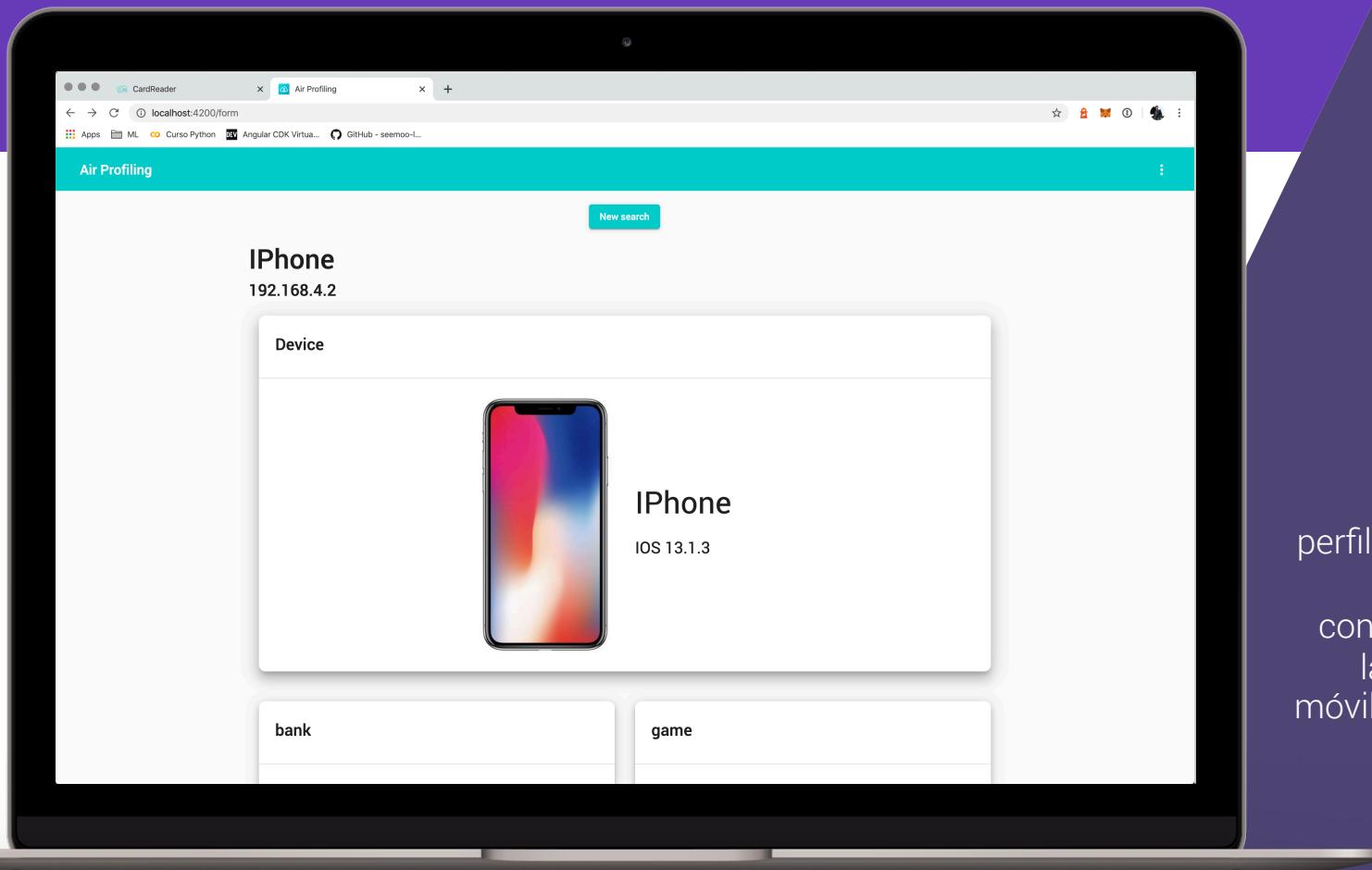




# Air Profiling

PoC

Air Profiling es una herramienta que hace un perfilado del tráfico generado por un móvil, clasifica las cabeceras TCP para sacar la url a la que consultan las distintas aplicaciones, las clasifica y las mapea para visualización. Recoge el tipo de móvil del User Agent y saca un perfilado a través de reglas heurísticas.



Recopilación de información  
A través técnicas de Sniffing



Extracción de datos  
Clasifica el tráfico consultando los paquetes TCP y datos de navegación

# PoC - ¿Cómo funciona?

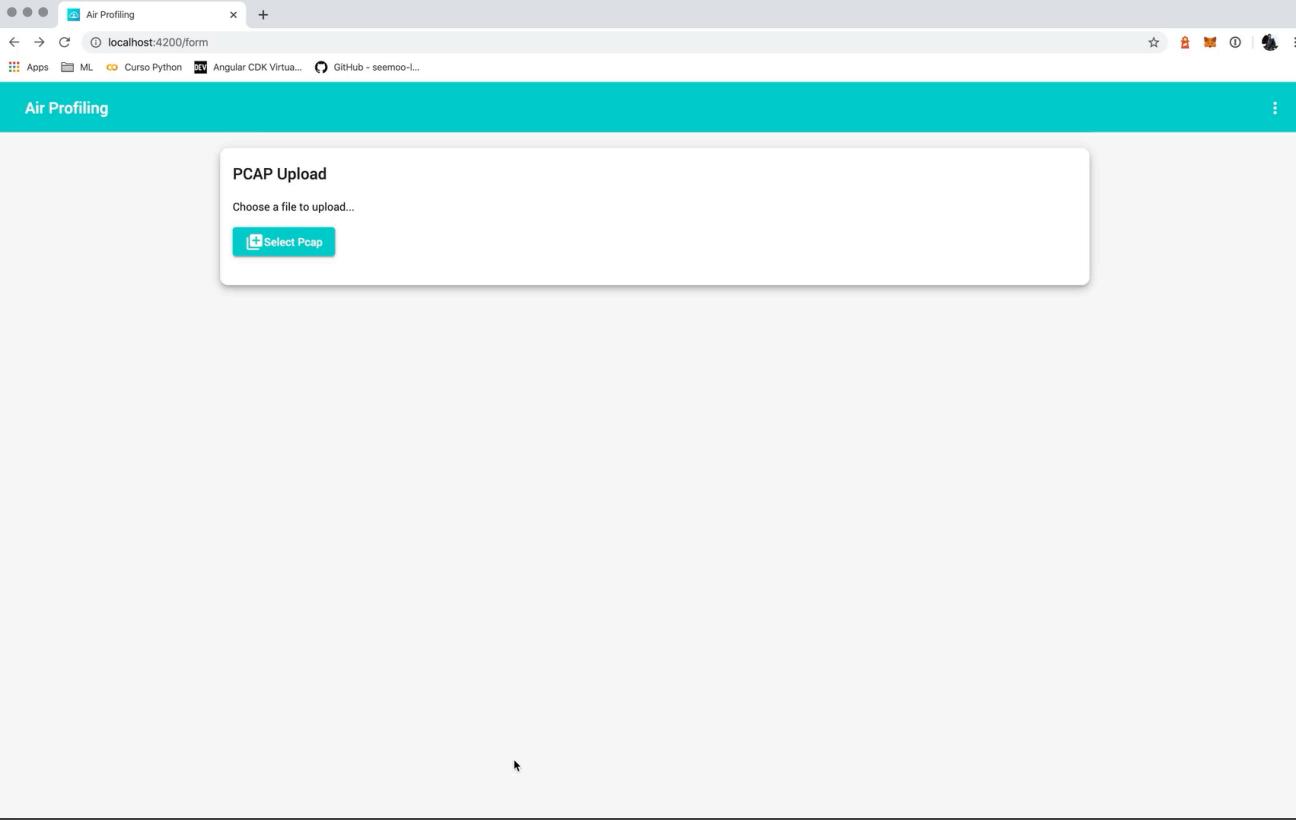
OSINT

METADATOS

PERFILADO RED

PERFILADO BLE

27



1

Desde la interfaz web se carga un fichero .pcap

2

El fichero es enviado al backend donde se procesa

3

Con un diccionario se clasifica la navegación por IP y se aplican las reglas heurísticas

4

Se muestra la información clasificada en la web

# Ejercicios

OSINT

METADATOS

PERFILADO RED

PERFILADO BLE

28

1

2

## Escaneo

1. Descargar wireshark
2. Ejecutar el programa
3. Elegir la interfaz de conexión deseada
4. Empezar captura

## Clasificación

1. Con la captura anterior, diferenciar tipos de protocolo.
2. Intentar averiguar algunas aplicaciones que realizan conexión
3. Utilizar el filtro con "tcp contains xxxx"



# Perfilado BLE

## Contenidos

Sniffing de paquetes BLE  
BLE Advertising  
Airdrop Crazy

# BLE – Bluetooth Low Energy

OSINT

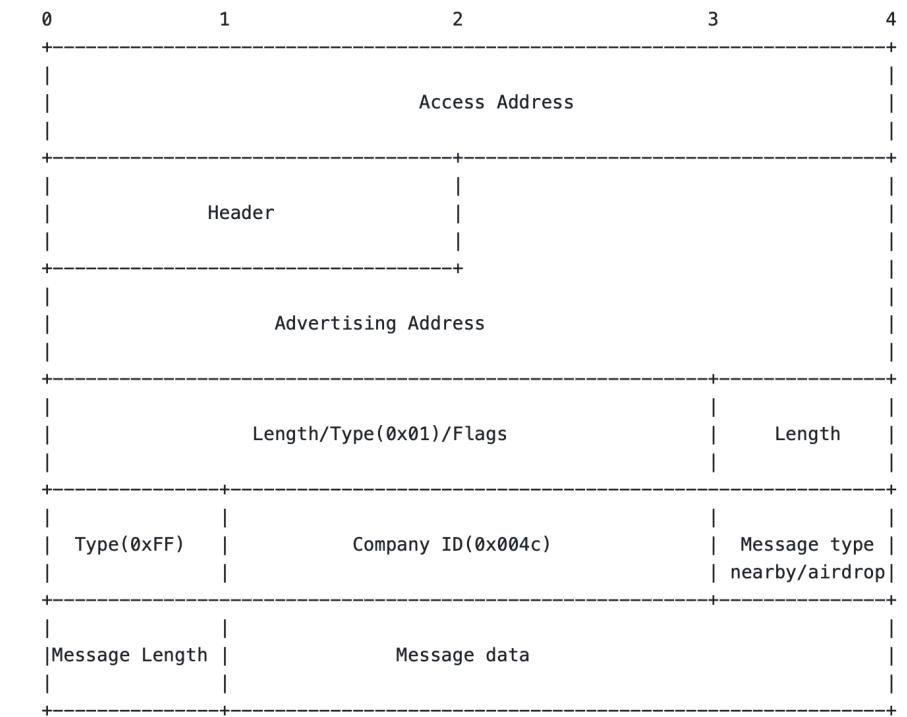
METADATOS

PERFILADO RED

PERFILADO BLE

30

1. Subconjunto del estándar Bluetooth v4.0
2. Pila de protocolos nueva y orientadas a baja potencia
3. Capa Física | Capa de Enlace | HCI | Capa L2CAP
4. ATT y SMP
5. GATT y GAP
6. Roles: Advertiser, Scanner, Master & Slave



# AWDL y Airdrop

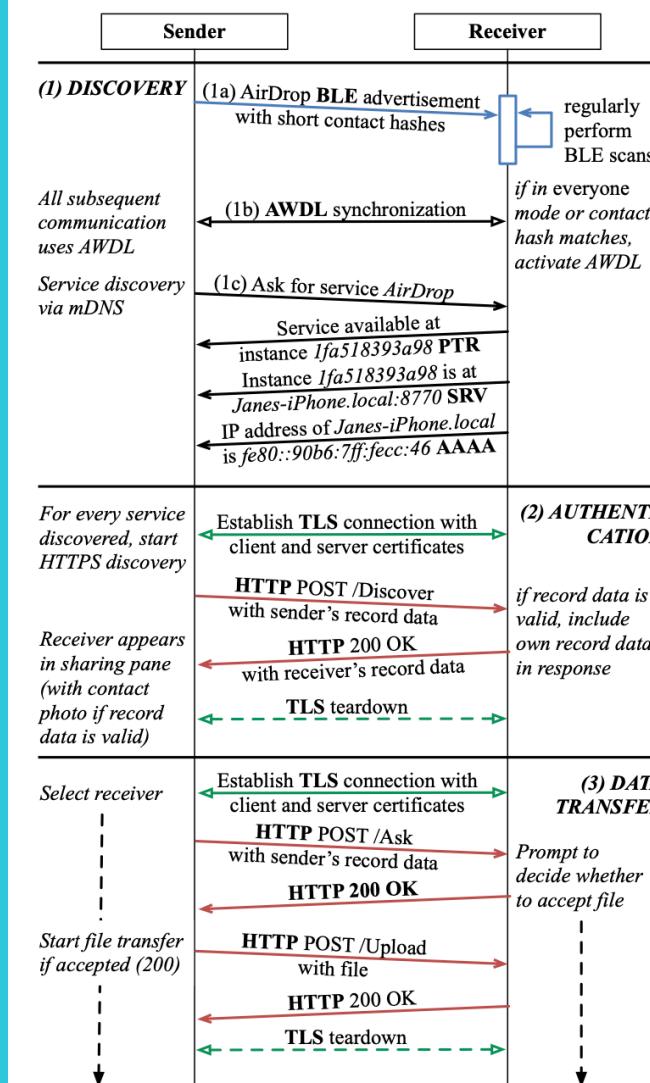
OSINT

METADATOS

PERFILADO RED

PERFILADO BLE

31



1. Protocolo propietario de baja latencia
2. Orientado a la transferencia de información entre dispositivos adyacentes sin servidor central
3. Usa su propia interfaz de red, normalmente "awdl0"
4. Usado en Airdrop, Gamekit, Airplay, Wifi transfer, Apple Continuity
5. Airdrop utiliza BLE y AWDL en Discovery
6. Autenticación y transferencia de datos por HTTPS

# Arquitectura

OSINT

METADATOS

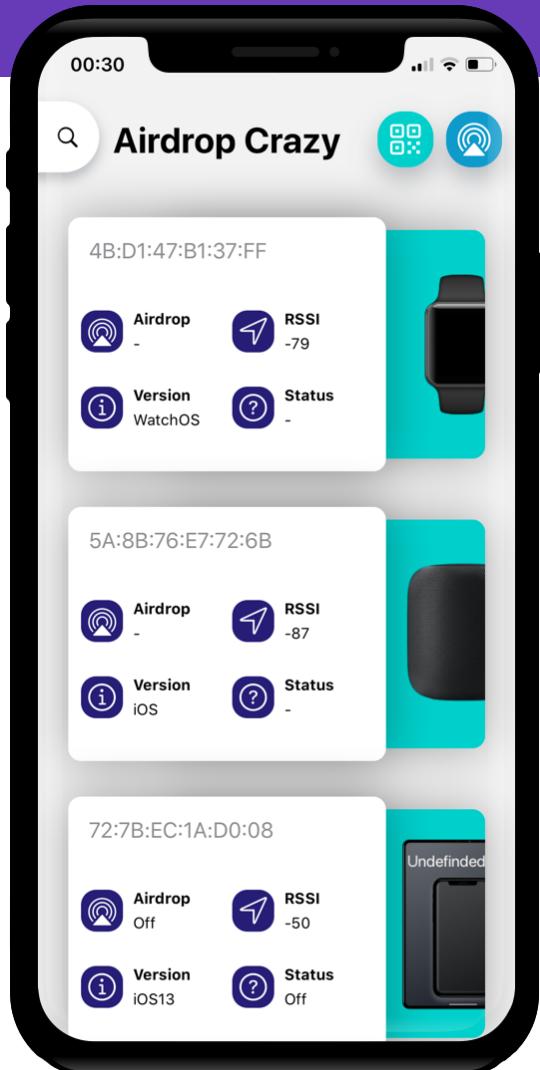
PERFILADO RED

PERFILADO BLE

32

1. Script BLE Read State y Airdrop
2. Servidor flask levanta las herramientas anteriores
3. Comunicación con app a través de sockets
4. Automatización de la herramienta y desarrollo del servicio Airdrop Crazy





Estado dispositivos  
Captación del estado de los dispositivos gracias a BLE



Obtención números de Teléfono  
Mediante Airdrop



# Airdrop Crazy

PoC

Airdrop Crazy es un servicio mediante el cuál colocar balizas en puntos estratégicos para monitorizar el estado de los dispositivos Apple del entorno y capturar información sensible explotando la funcionalidad interna del protocolo Airdrop



Descarga



WiFi



BLE



Instalación



Ejecución

## Paso 1

Descargar la herramienta desde  
<https://github.com/ElEvenPaths/Airdrop-Crazy>

## Paso 2

Comprobar que la tarjeta de red y el firmware es compatible

## Paso 3

Comprobar que la tarjeta BLE y el firmware es compatible

## Paso 4

Ejecutar el script de instalación con *sudo bash ./install*

## Paso 5

Ejecutar la herramienta bien en modo CLI o el servicio

# PoC - ¿Cómo funciona?

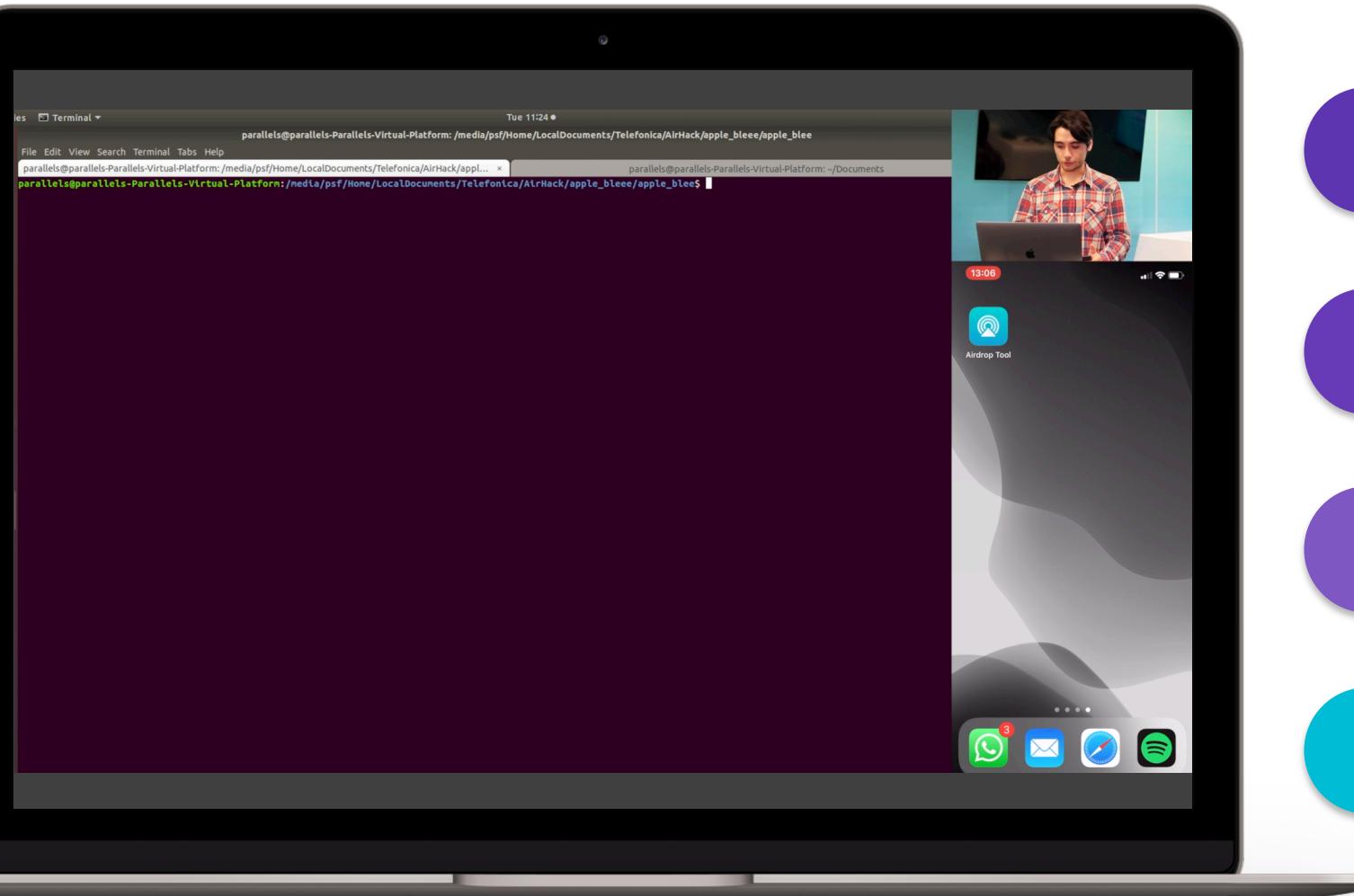
OSINT

METADATOS

PERFILADO RED

PERFILADO BLE

35



1

La app abre un socket a través de un servidor inverso

2

El servidor arranca las herramientas automatizadas y empieza el escaneo

3

Dos servicios arrancados, escaneo BLE y AWDL

4

La información se actualiza en el cliente cada vez que hay un cambio

# Ejercicios

OSINT

METADATOS

PERFILADO RED

PERFILADO BLE

36

1

## Escaneo BLE

1. Abrir *HomePWN*
2. Cargar el módulo *discovery/BLE*
3. Mirar las opciones del módulo
4. Ejecutar el módulo
5. Ver los resultados

2

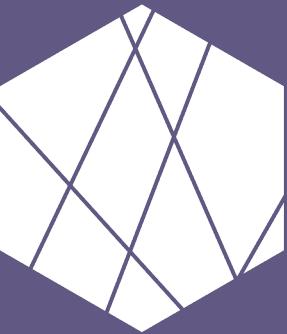
## Listado de atributos

1. Abrir *HomePWN*
2. Cargar el módulo *BLE/list-characteristics*
3. Mirar las opciones del módulo y cambiar el *bmac* y *type*
4. Ejecutar el módulo
5. Ver los resultados

3

## Lectura de atributos

1. Abrir *HomePWN*
2. Cargar el módulo *BLE/subscribe-and-write*
3. Mirar las opciones del módulo y cambiar el *bmac*, *type*, *uuid-subscribe*, *uuid-write*
4. Ejecutar el módulo
5. Ver los resultados



Gracias  
¿Preguntas?