APPLIED NETWORK FORENSICS - PROCESOS AUTOMATIZADOS DE ANÁLISIS

GUILLERMO ROMÁN FERRERO

MORTERUELOCON 2019

WHOAMI

- Guillermo Román Ferrero
  - Telegram/Twitter: @guille_hartek
  - Cofundador y coautor de Follow the White Rabbit
    - https://www.fwhibbit.es/
  - Ingeniero Informático (TI), Máster en Seguridad de las TIC
  - Experto en Respuesta a Incidentes en el CSIRT Global de Telefónica

CAPTURA DE MUESTRAS DE TRÁFICO DE RED

- Existe una gran cantidad de métodos de captura de tráfico.
- ¿Con qué razones podría yo querer capturar esto?
  - Buenas intenciones: Monitorización de redes, redireccionamiento a IDS/IPS, mirroring, análisis de protocolos, ingeniería reversa.
  - Malas intenciones: Espionaje de redes inalámbricas, espionaje industrial, perfilado no autorizado de usuarios, obtención de credenciales, servicio VPN maligno.

PROBLEMÁTICA

- Falta de consciencia de la importancia de la privacidad digital.
  - “No tengo nada que ocultar”.
- Falta de concienciación a la hora de utilizar redes inalámbricas abiertas.
  - No existe conciencia de sus riesgos y paliativos.
- Falta de cifrado en aplicaciones de dispositivos móviles.
  - Desconocimiento del desarrollador.
  - Eficiencia vs seguridad.
- Facilidad de obtención de los datos en MiTM.
  - Espionaje de redes inalámbricas.
- Interceptación de comunicaciones.
  - Relación entre la actividad del dispositivo y el perfil del usuario.

CAPTURAS EN DISPOSITIVOS MÓVILES ¿QUÉ PASA POR MI TELÉFONO?

- Por nuestros dispositivos móviles circula una cantidad enorme de información cifrada y no cifrada.
  - Las aplicaciones que utilizo, ¿cifran mis comunicaciones?
  - Las que sí, ¿cómo lo hacen? ¿Lo hacen bien? ¿Cifran todo?
  - Mis datos no cifrados, ¿son fácilmente recuperables? (Sí).
  - Mis datos cifrados, ¿pueden aun así revelar información? (Pues también sí)

CAPTURAS EN DISPOSITIVOS MÓVILES ¿QUÉ PASA POR MI TELÉFONO?

- Protocolos interesantes a analizar:
  - HTTP/HTTPS: Utilizado en la mayoría de las aplicaciones. Peticiones con un destino o estructura conocidos.
    - Muy relevantes datos como el agente de usuario y peticiones en plano de aplicaciones.
  - XMPP: Aplicaciones de mensajería.
    - Aún muy utilizado con una capa de cifrado.
  - STUN: Establecimiento de llamadas VoIP.
    - Negociación de punto a punto con NAT intermedias.
  - DNS: Consulta de nombres de dominio reconocibles.
    - Casi cualquier comunicación a un servidor comenzará por una petición DNS.

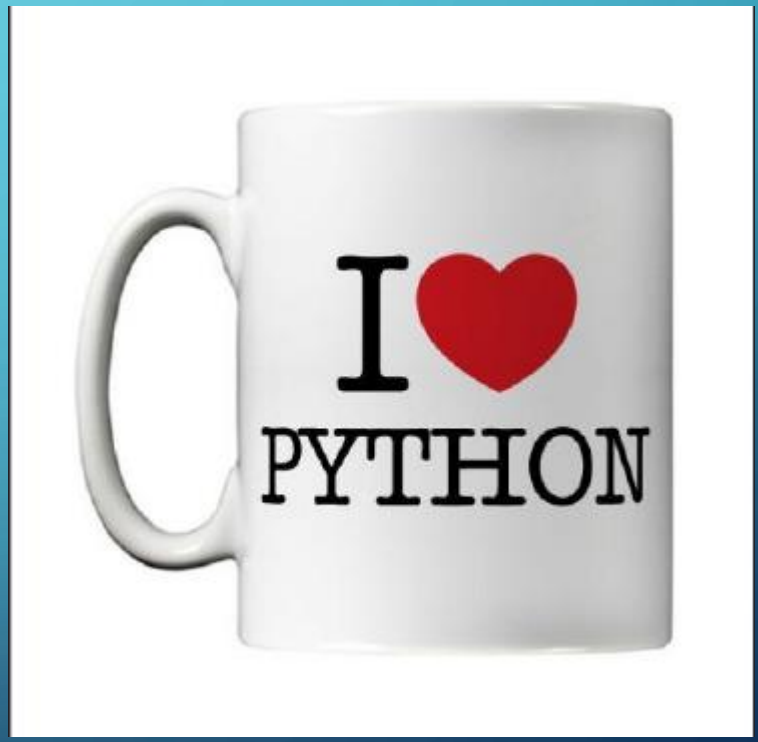
ANÁLISIS CON WIRESHARK Y TSHARK

- Filtros y elementos interesantes:
  - Agentes de usuario: http.user_agent
  - URLs completas: http.request.full_uri
  - Respuestas DNS: dns.flags == 0x8180
  - Estadísticas por protocolo: Statistics – Protocol Hierarchy
  - Conexiones realizadas por servidor: Statistics – Endpoints
  - Podemos también inspeccionar el origen el tráfico (Importante tener instalado en Wireshark las bases de datos GeoIP2)

ANÁLISIS CON WIRESHARK Y TSHARK

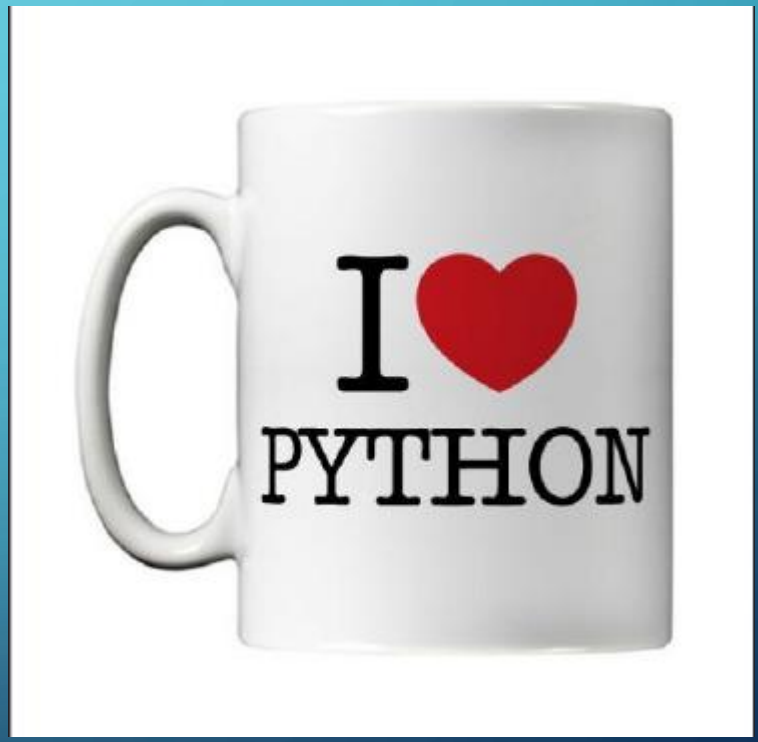
ANÁLISIS AUTOMATIZADO CON PYTHON Y DPKT

- Pueden programarse de forma fácil scripts en diversos lenguajes para proporcionar un análisis personalizado de una captura de red.
- Utilizaremos dpkt, una librería para Python escriba por Dug Sony y otros contribuidores, para realizar inspección a nivel de paquete.
  - pip install dpkt

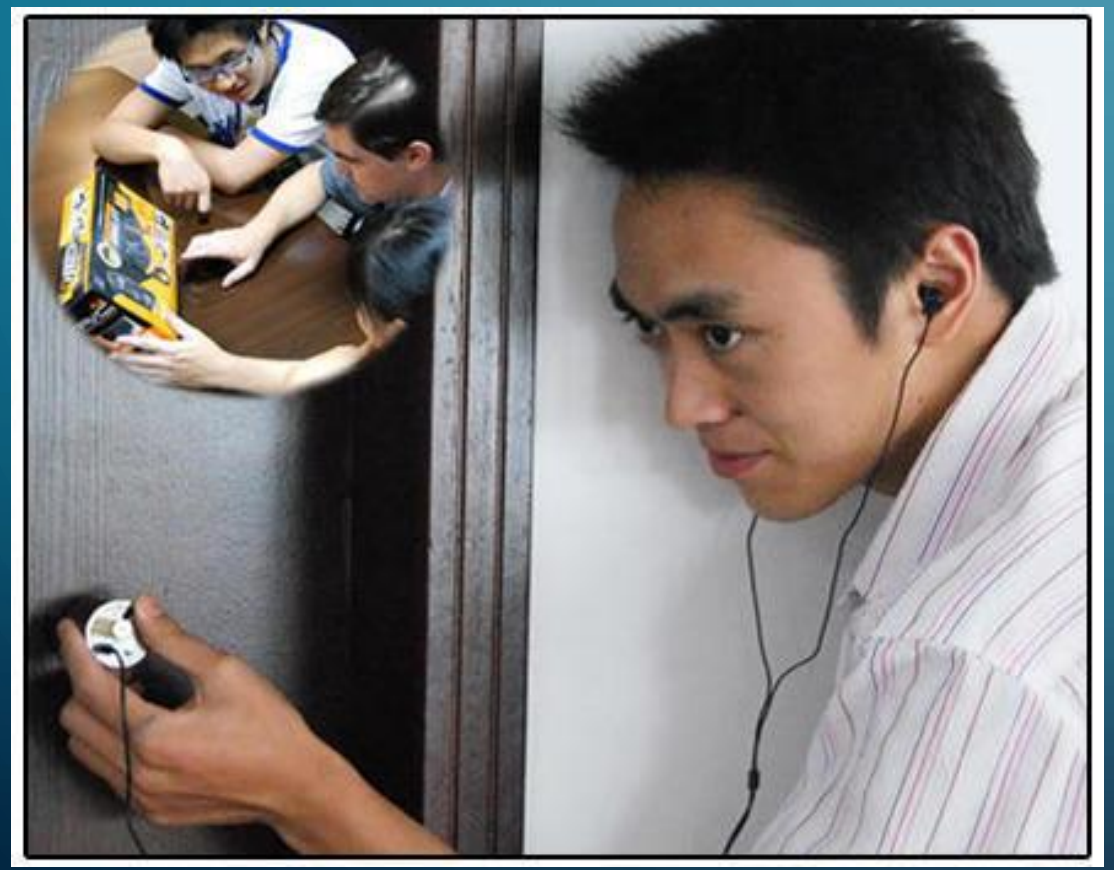


ANÁLISIS AUTOMATIZADO CON PYTHON Y DPKT

- Probaremos tres sencillos scripts en Python para realizar las siguientes acciones:
  - Extraer estadísticas de los diferentes protocolos de cada capa TCP/IP.
  - Extraer los agentes de usuario por orden de uso.
  - Extraer las resoluciones DNS de tipo A y CNAME.

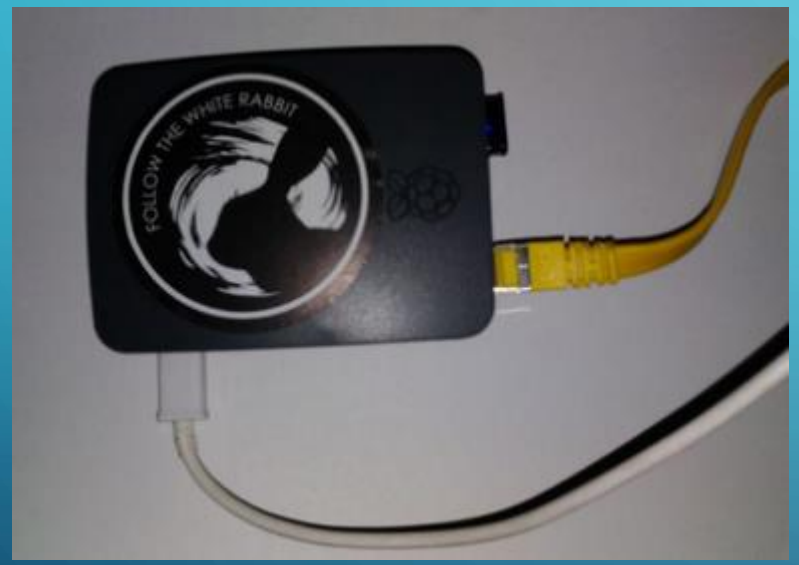


MÉTODOS DE CAPTURA



- Existe una gran cantidad de métodos de captura de tráfico: mirroring, escucha de redes inalámbricas, ARP/DNS poisoning (Man in the Middle), network tapping…
- Un caso muy conocido es el de la escucha de redes inalámbricas mediante un punto de acceso falso. Vamos a trastear un poco.

PUNTO DE ACCESO FALSO SONDA



- Basado en Raspberry Pi 3.
- Proceso de captura:
  - Crea una red inalámbrica abierta con *hostapd*.
  - Controla conexiones/desconexiones de dispositivos con *hostapd_cli*.
  - Captura el tráfico filtrando por MAC en *tcpdump*.
  - Salida a *pcap* nombrando con la MAC, fecha y hora de la captura.
- Accesible remotamente.

AIRE – PRUEBA DE CONCEPTO

- AIRE – Automated Inspection and Recognision Engine
- Desarrollado junto a Javier Gutiérrez Navío.
- Capaz de:
  - Exraer datos relevantes de una captura de tráfico
  - Analizar estos datos e inferir resultados.
  - Mostrar los datos al usuario.
- Datos extraídos de la captura:
  - Aplicaciones utilizadas
  - Páginas visibles y temática.
  - Geolocalización de servidores accedidos.
  - Timeline de navegación y uso de aplicaciones.

- Tecnologías utilizadas:
  - Raspberry Pi 3 (visto antes).
  - Python + dpkt
  - ELK Stack (Elastic Search, Logstash, Kibana).
  - Django + Django Rest Framework

GRACIAS POR VENIR!!