Dani Creus
Lead Researcher, GReAT

kaspersky

Día 02. RECAP:

- Kit respuesta ante incidentes.
- Veracrypt / Encrypted Disk Detector.
- FTK Imager + Alternativas.
- Sysinternals
- Nirsoft
- WSCC (Centraliza todas las utilidades)
- WinAudit
- QuickHash (funciones hash)
- Volatility (análisis memoria)
- Floss (extrae cadenas de texto)
- DnSPY (depurador .NET)

Sesión 03.

Preparación Kit IR para dispositivos móviles.

Como detectar infecciones* en pocos minutos sin conocimiento técnico y con pocos recursos ?

kaspersky

¿Qué es stalkerware?

Stalkerware es un software comercial que permite a los usuarios espiar a otras personas de forma totalmente oculta:

- Se instala en un dispositivo (principalmente Android) sin el conocimiento y consentimiento del propietario
- Se mantiene oculto, operando en segundo plano
- Tiene acceso a datos personales como localización, historial de navegación, mensajes, chats en redes sociales, fotos, etc.
- Comparte información sensible con un tercero, no solo con el acosador, también con la compañía propietaria del software
- A veces, se publicita como una solución de espionaje o de vigilancia secreta.

[Definición de Stalkerwarer según la Coalición contra el Stalkerware]

Características del stalkerware

Los programas Stalkerware pueden ser muy diferentes según sus funcionalidad y variar su precio dependiendo del número de funciones incluidas

Localización GPS

Monitorización SMS

Grabación de voz y video

Robo de los registros de las llamadas telefónicas

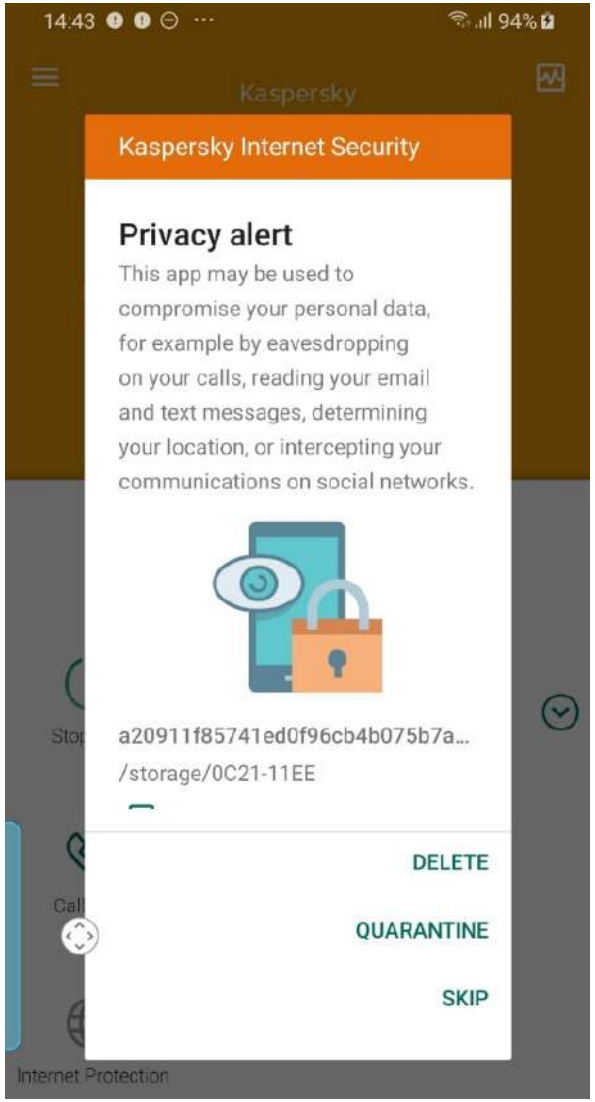
Acceso a los datos de las aplicaciones de mensajería y redes sociales

Datos del navegador

De un aviso de virus a una alerta de privacidad

Desde Abril 2019 los usuarios de Kaspersky en sus móviles están mejor protegidos contra el stalkerware :

- Clara descripción de la amenaza
- Alerta de que es posible que el usuario esté „bajo vigilancia“
- Kaspersky Internet Security for Android dispone de una versión gratuita que incluye esta alerta/protección



• Stalkerware

- En la mayoría de los casos, debe ser instalado manualmente por alguien que tenga acceso físico al dispositivo.
- El estatus legal sigue siendo vago en la mayoría de los países
- Se puede encontrar fácilmente en Internet.
- Se proporciona como un servicio y los instaladores de estas aplicaciones no tienen que preocuparse por alquilar un servidor o almacenar datos.

Spyware

- Suelen instalarse mediante exploits o ingeniería social (MDM).
- Son ilegales en la gran mayoría de países.
- No se encuentra fácilmente en Internet, a menudo desarrollado por atacantes.
- Son utilizados por atacantes que tienen sus propias herramientas e infraestructura.

- **Spyware**

Por lo general, APK (Android) o IPA (iOS) se instalan en la mayoría de los casos físicamente, a través de tiendas o mediante ingeniería social (MDM).

Una vez instalados, se comunican a intervalos regulares con los servidores de ataque para recibir pedidos. Por lo general, cada solicitud tiene un espacio de unos pocos segundos / minutos.

Tinycheck: Detección pasiva.

- Para ayudar a protegerse del stalkerware, Félix Aimé, investigador de seguridad del equipo de Análisis e Investigación de Kaspersky (GReAT) ha desarrollado 'TinyCheck' – una herramienta muy sencilla para detector el stalkerware y spyware instalado en dispositivos móviles y tablets.
- La idea surgió en una reunión con un miembro de la Coalición donde se discutía este problema. Concretamente, una organización de derechos de la mujer en Francia planteó la posibilidad de ayudar a aquellas personas que sospechaban ser víctimas de stalkerware a detectarlo sin necesidad de instalar aplicaciones adicionales para realizar n análisis forense del dispositivo.
- TinyCheck es una herramienta abierta basada en Raspberry Pi, una plataforma ampliamente accesible. Con una conexión wi-fi, TinyCheck analiza el tráfico saliente del dispositivo móvil e identifica las interacciones con fuentes maliciosa conocidas, como servidores relacionados con el spyware. El objetivo de TinyCheck es ayudar a las organizaciones sin ánimo de lucro, como proveedores de servicios, organizaciones de ayuda a las víctimas de violencia de género a proteger a estas personas y su privacidad
- ıb/tinycheck

TinyCheck crea una red wifi temporal
y analiza las comunicaciones de un dispositivo para
notificar si ha detectado rastros de actividad maliciosa.

Under the hood
(Hardware)

- **1 Raspberry Pi**
- **1 Antena Wifi** (opcional)
- **1 Pantalla táctil** (opcional)

Under the hood
(Hardware)

- **1 Raspberry Pi**
- **1 Antena Wifi** (opcional)
- **1 Pantalla táctil** (opcional)

Under the hood
(Software)

- **Raspberry Pi Os**
- **Suricata**
- **Zeek**

Motor de detección

Diseñado principalmente para detectar **stalkerware**, TinyCheck también permite la detección de otros programas espía, conocidos y desconocidos en los teléfonos inteligentes, pero también en ordenadores cuando se comunican.

Dominios

IPv4 & IPv6

Rangos de red

Certificados SSL

Servidores de nombres

Reglas Suricata

Anomalías

Detección de anomalías?

Aún son pocos los programas espía que buscan la seguridad de sus comunicaciones. Por lo tanto, a menudo encontramos muchas anomalías en ellos.

- Peticiones UDP / ICMP
- Puertos no genéricos
- DNS (uso/no-uso)
- Comms HTTP
- Certificados auto-firmados
- Certificados gratuitos
- Dominios recientes etc.

Flujo de análisis (usuario)

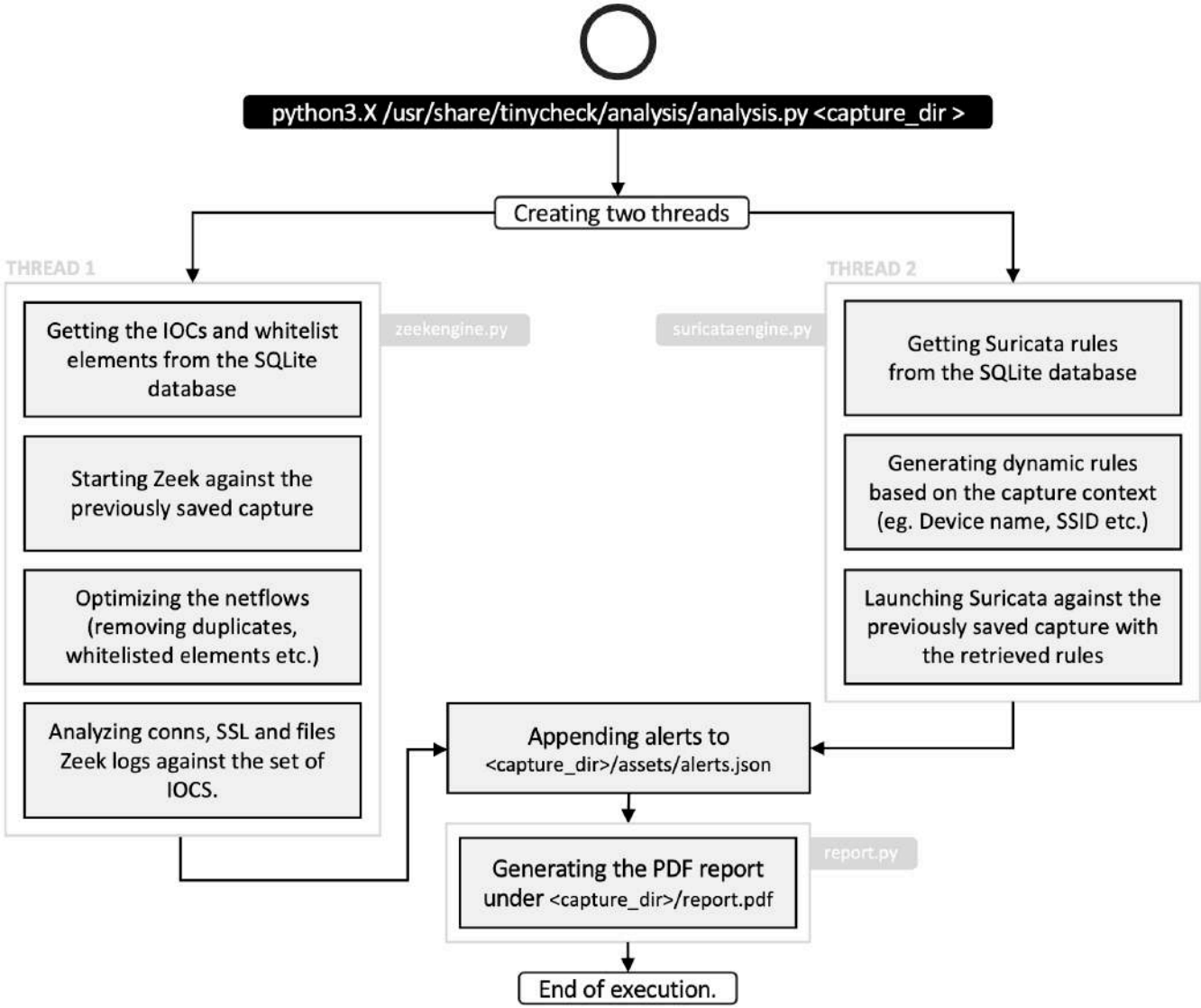
Conecta el dispositivo a la WiFi de Tinycheck.

Espera unos minutos (10-15)

Analizar las alertas que ha emitido Tinycheck.

Guarda toda la sesión y el informe final en un USB.

Flujo de análisis (motor)

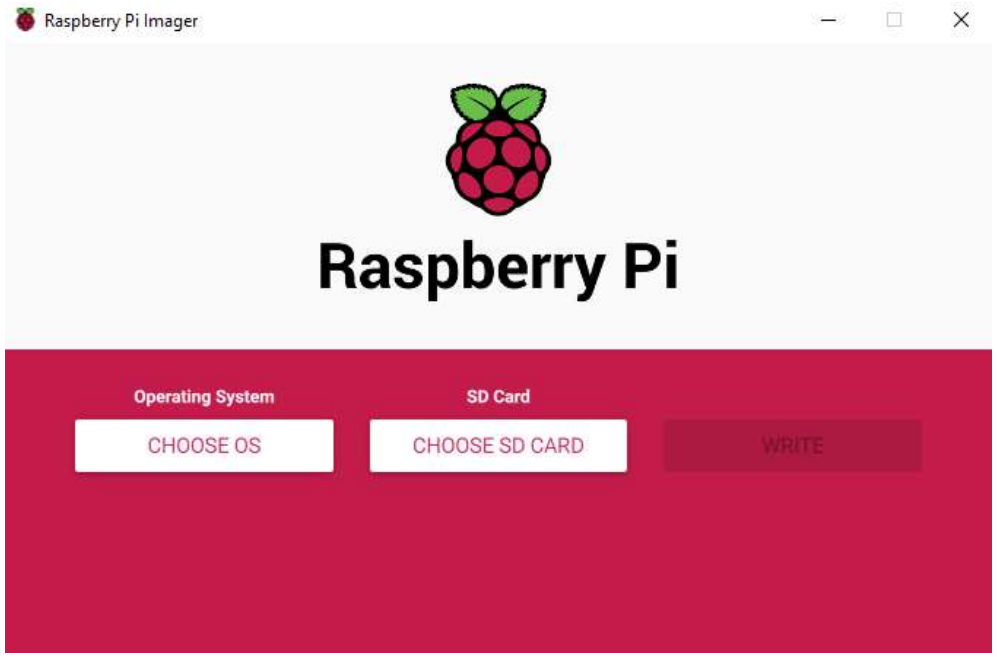


TALLER DE CONSTRUCCIÓN

TINYCHECK

PREPARACIÓN

https://www.raspberrypi.com/software/

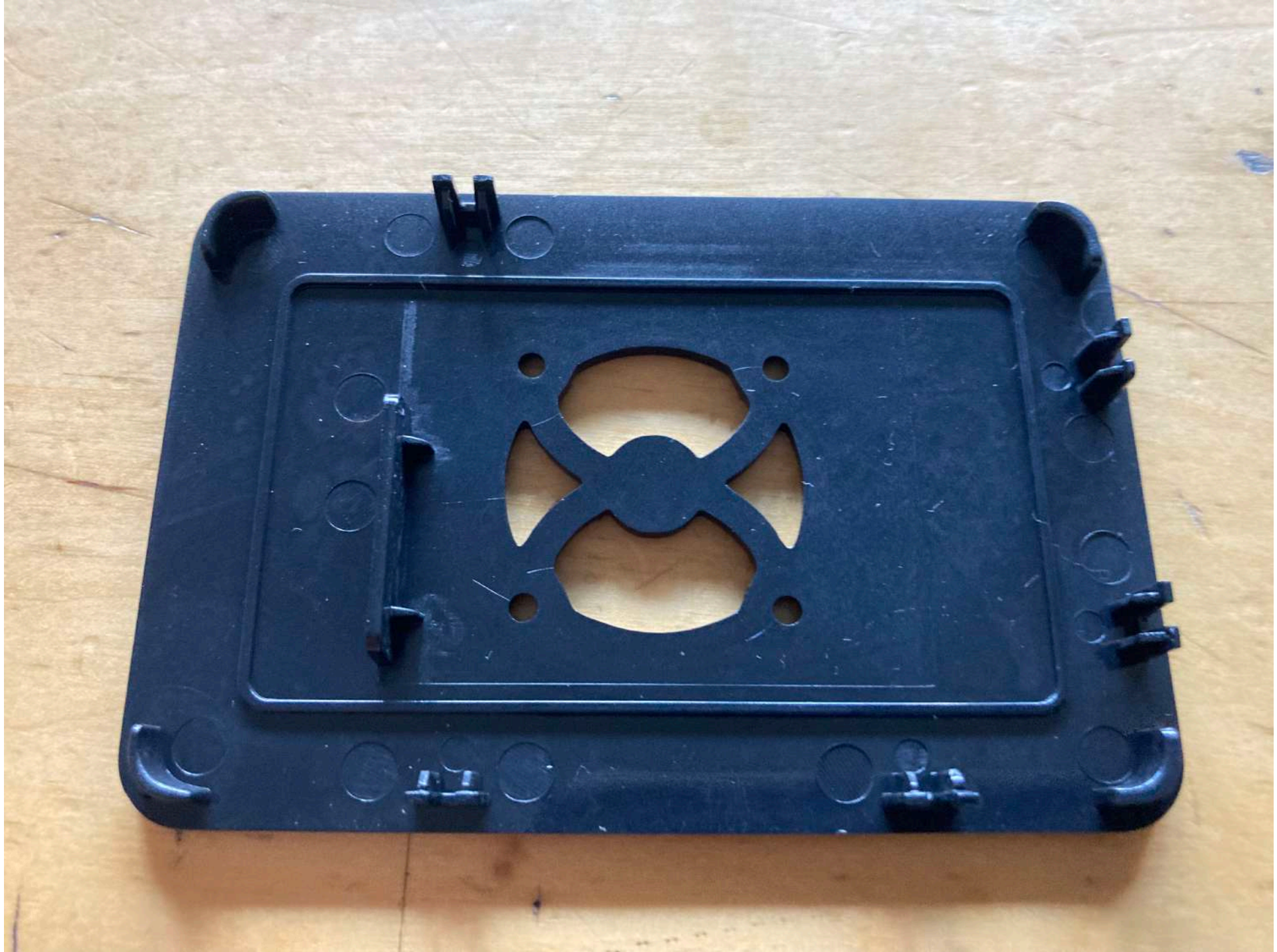


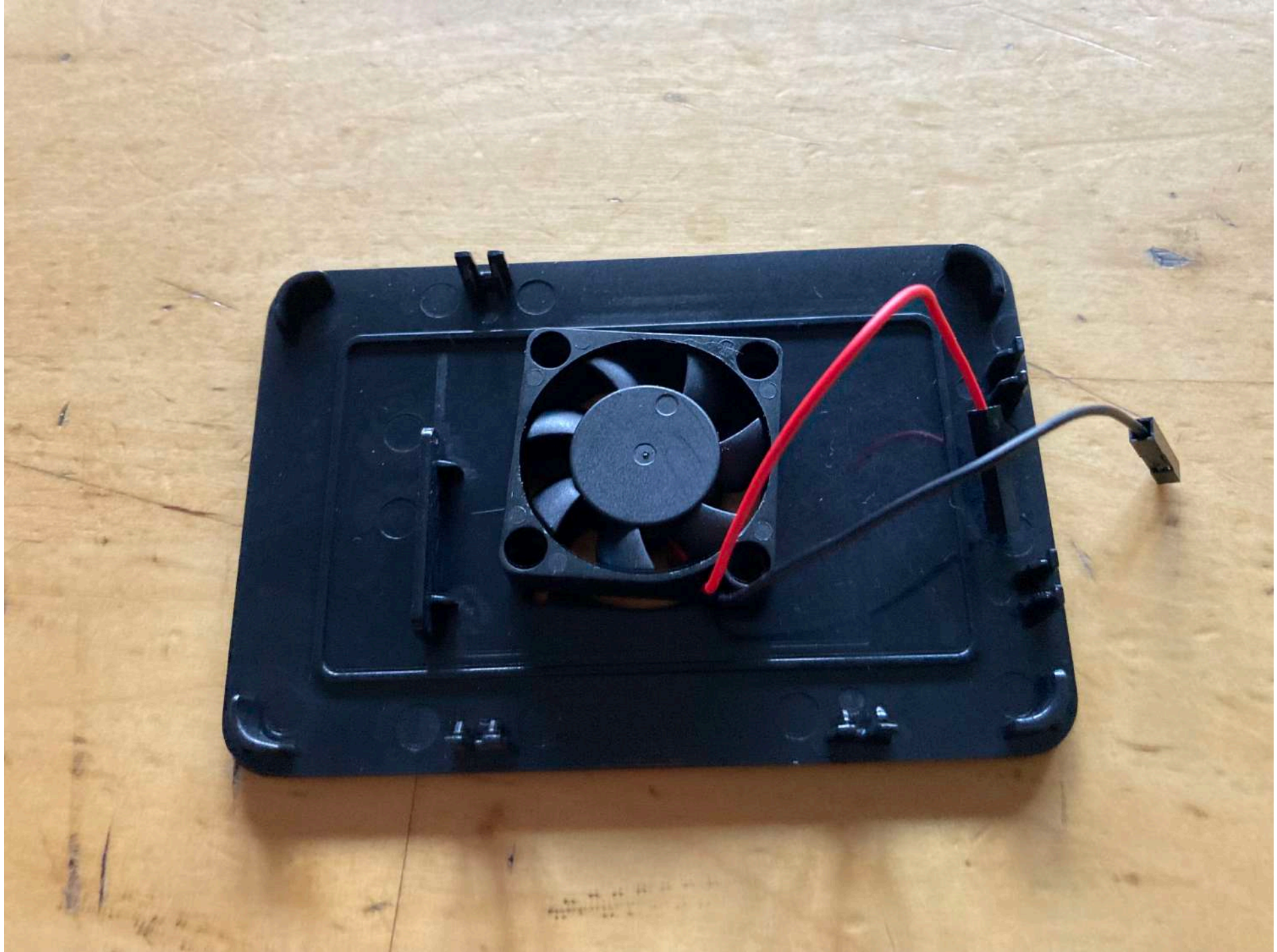
https://www.raspberrypi.com/documentation/computers/getting-started.html

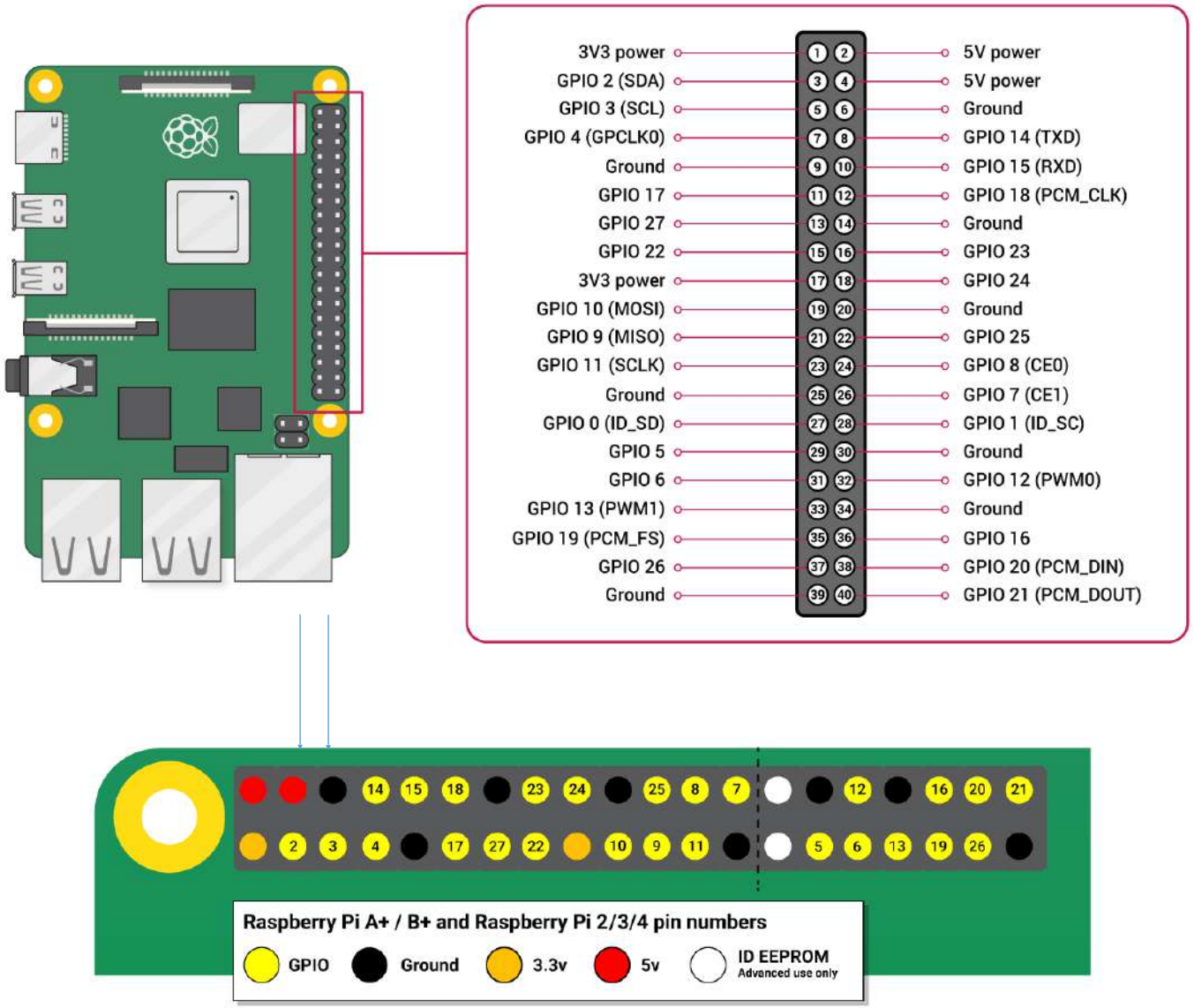

ETEPON
BrosTrend

Raspberry Pi 4 Model B
© Raspberry Pi 2018
Made in the UK
FCC ID: 2ABCB-RPI4B
IC: 20953-RPI4B
VLI
IEA77
D97CL
VQ3Z
HDMI
CAMERA
DISPLAY
POWER IN
GLOBAL_EN
RUN
GPIO

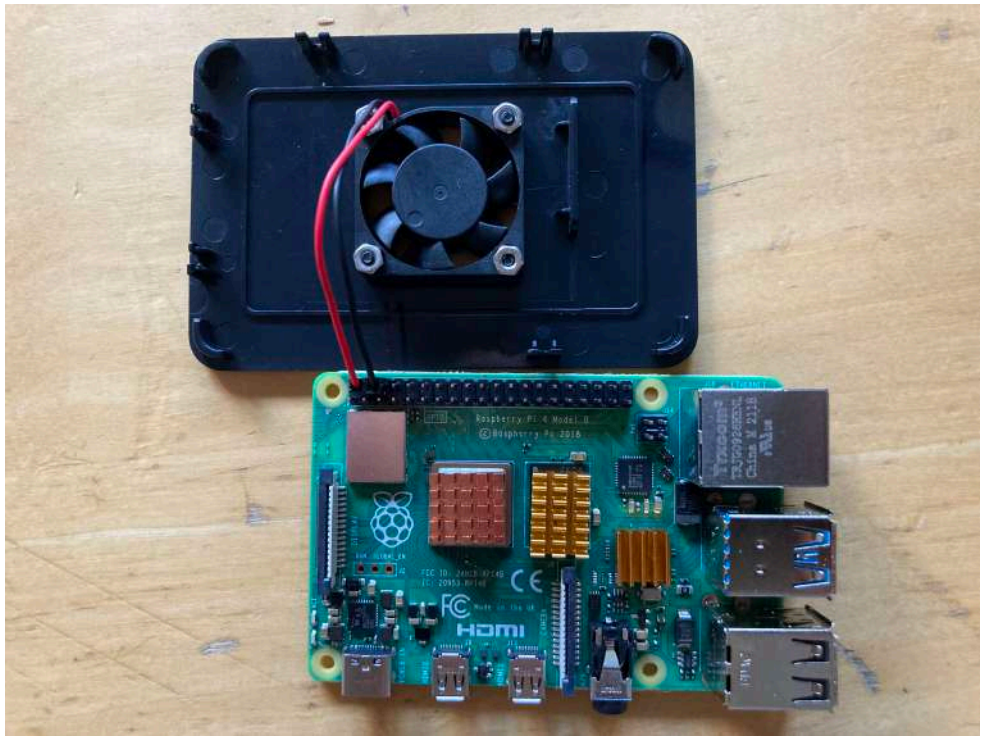
Raspberry Pi 4 Model B
©Raspberry Pi 2018
Made in the UK
FCC ID: 2ABCB-RPI4B
IC: 20953-RPI4B
HDMI
POWER IN
DISPLAY
CAMERA
A/V
GPIO
RUN
GLOBAL_EN
PoE

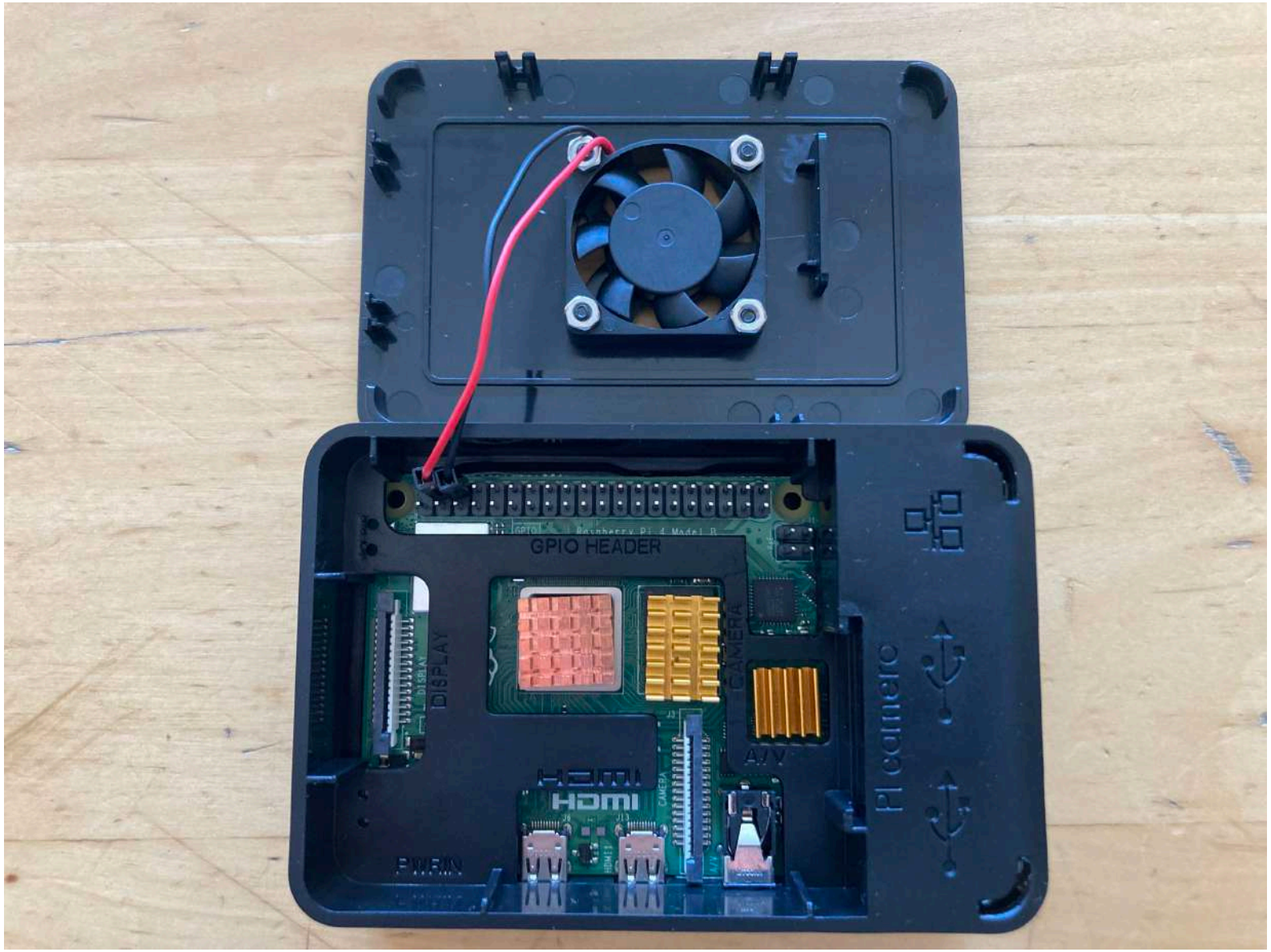


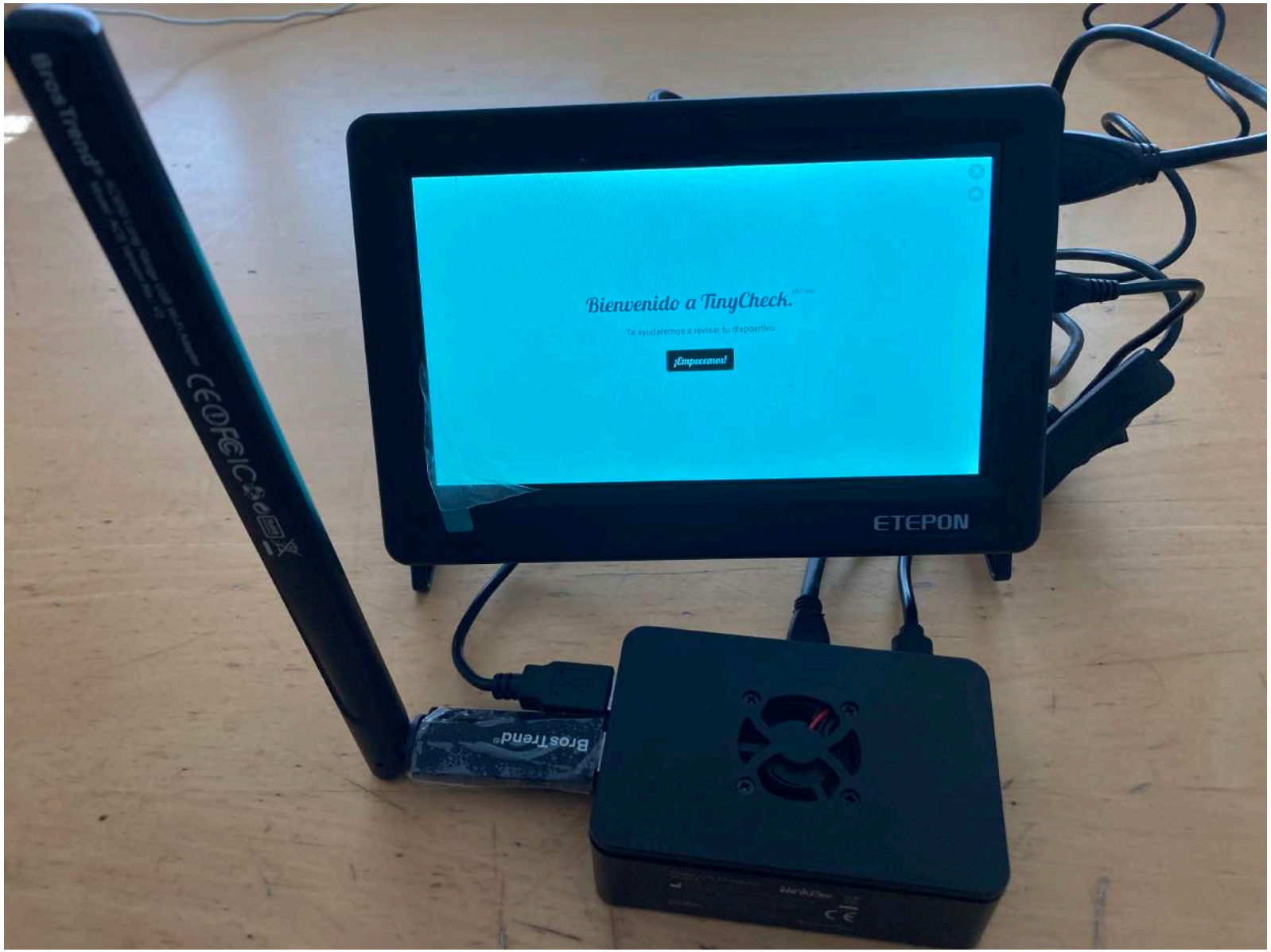



3V3 power 1 2 5V power
GPIO 2 (SDA) 3 4 5V power
GPIO 3 (SCL) 5 6 Ground
GPIO 4 (GPCLK0) 7 8 GPIO 14 (TXD)
Ground 9 10 GPIO 15 (RXD)
GPIO 17 11 12 GPIO 18 (PCM_CLK)
GPIO 27 13 14 Ground
GPIO 22 15 16 GPIO 23
3V3 power 17 18 GPIO 24
GPIO 10 (MOSI) 19 20 Ground
GPIO 9 (MISO) 21 22 GPIO 25
GPIO 11 (SCLK) 23 24 GPIO 8 (CE0)
Ground 25 26 GPIO 7 (CE1)
GPIO 0 (ID_SD) 27 28 GPIO 1 (ID_SC)
GPIO 5 29 30 Ground
GPIO 6 31 32 GPIO 12 (PWM0)
GPIO 13 (PWM1) 33 34 Ground
GPIO 19 (PCM_FS) 35 36 GPIO 16
GPIO 26 37 38 GPIO 20 (PCM_DIN)
Ground 39 40 GPIO 21 (PCM_DOUT)

14 15 18 23 24 25 8 7 12 16 20 21
2 3 4 17 27 22 10 9 11 5 6 13 19 26
Raspberry Pi A+ / B+ and Raspberry Pi 2/3/4 pin numbers
GPIO
Ground
3.3v
5v
ID EEPROM
Advanced use only


HDMI


GPIO HEADER
DISPLAY
CAMERA
A/V
HDMI
HDMI
CAMERA
Pi camera


Bienvenido a TinyCheck.
Te ayudaremos a revisar tu dispositivo
¡Empecemos!
ETEPON
BrosTrend

Software Necesario.

Drivers:

https://deb.trendtechcn.com/

Tinycheck:

https://github.com/KasperskyLab/TinyCheck

Limitaciones.

Red / geo-cercado para comunicaciones de red;

Domain Fronting;

Canales encubiertos a través de API de redes sociales;

Stalkerware ya no funciona (finaliza la suscripción paga, etc.)

Fuentes adicionales.

Integración con OpenCTI & MISP
para actualización de IOCs.

Reproducir capturas de red (PCAP) desde USB.

Mobile Verification Toolkit

Mobile Verification Toolkit (MVT) is a tool to facilitate the consensual forensic analysis of Android and iOS devices, for the purpose of identifying traces of compromise.

https://github.com/mvt-project/mvt
https://docs.mvt.re/en/latest/ios/filesystem/check/

Mobile Verification Toolkit (Evidence from Backup)

Instalación.
git clone https://github.com/mvt-project/mvt.git
cd mvt
pip3 install

Dependencias.
sudo apt install python3 python3-pip libusb-1.0-0
sudo apt install usbmuxd libimobiledevice6 libimobiledevice-utils ideviceinstaller

Backup (phone is already connected via USB cable).
idevicepair pair
idevicebackup2 backup encryption on (encrypted backups == more data)
idevicebackup2 backup --full ~/evidence_mobile/

Análisis.
mvt-ios decrypt-backup -p password -d ~/evidence_mobile_decrypted ~/ evidence_mobile /
mvt-ios check-backup --output ~/evidence_output ~/evidence_mobile_decrypte/udid/
mvt-ios check-backup -o logs --iocs ~/IOCs/malware_iocs.stix2 ~/evidence_mobile_decrypted

Mobile Verification Toolkit (Evidence from full acquisition)

Instalación (a parte de MVT).
sudo apt install libusbmuxd-tools (we´ll need iProxy tool from this package).

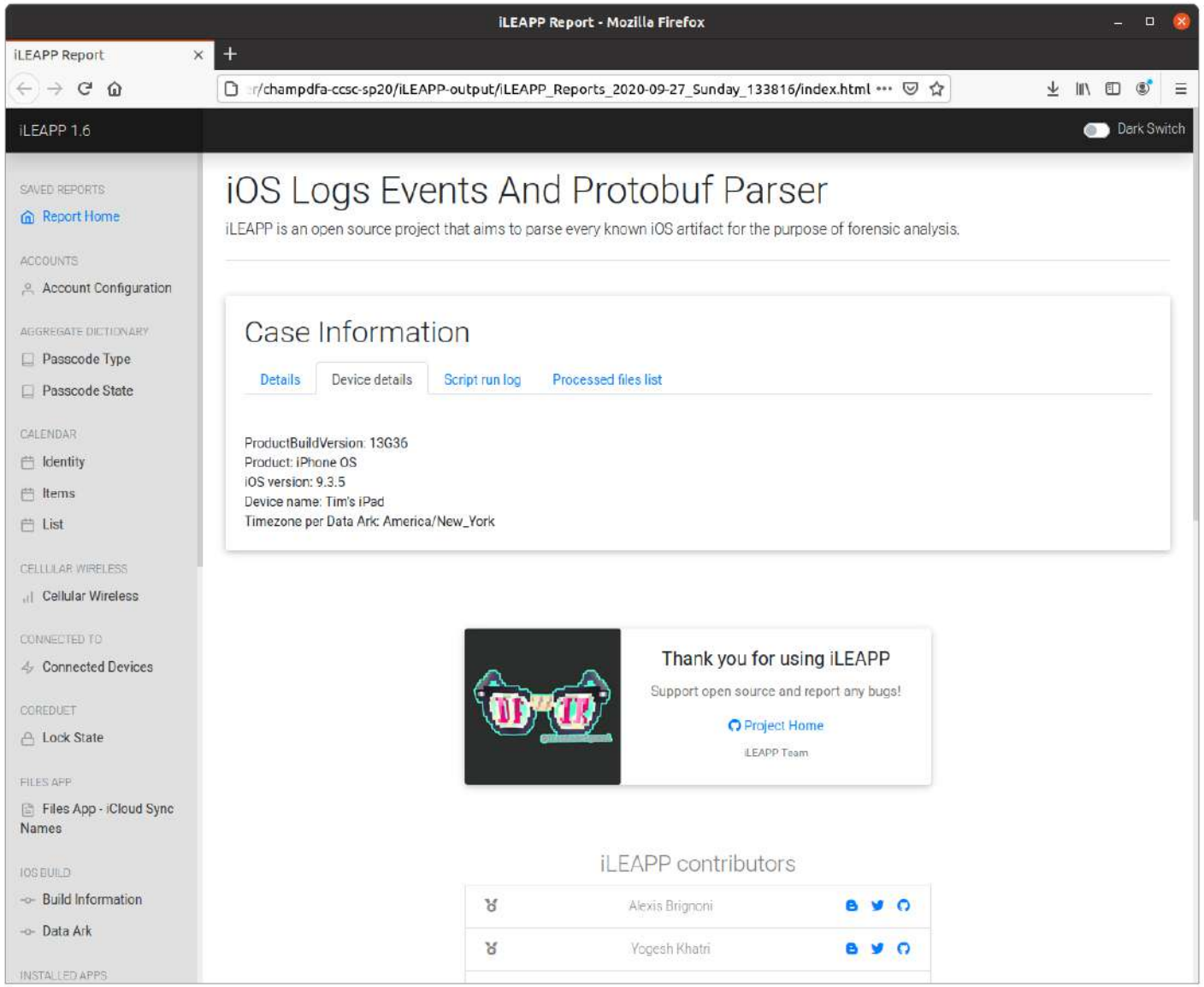
Jailbreak.
https://checkra.in/ (o unc0ver.dev)
sudo checkra1n

Acceso.
iproxy 4242 22 (allow ssh to device via USB)
ssh root@127.0.0.1 -p 4242

Adquisición.
ssh root@127.0.0.1 -p 4242 dd if=/dev/rdisk0s1s1 bs=4k | dd of=ios_evidence.dd
ssh root@127.0.0.1 -p 4242 'tar -cf - /private/var/' > private-var.tar (user data)

Análisis.
Montar y Volcar datos de la imagen **(**ios_evidence.dd).
mvt-ios check-fs /evidence_dumped/ --output /evidence_dumped_checked/
* https://docs.mvt.re/en/latest/ios/records/

iLEAPP



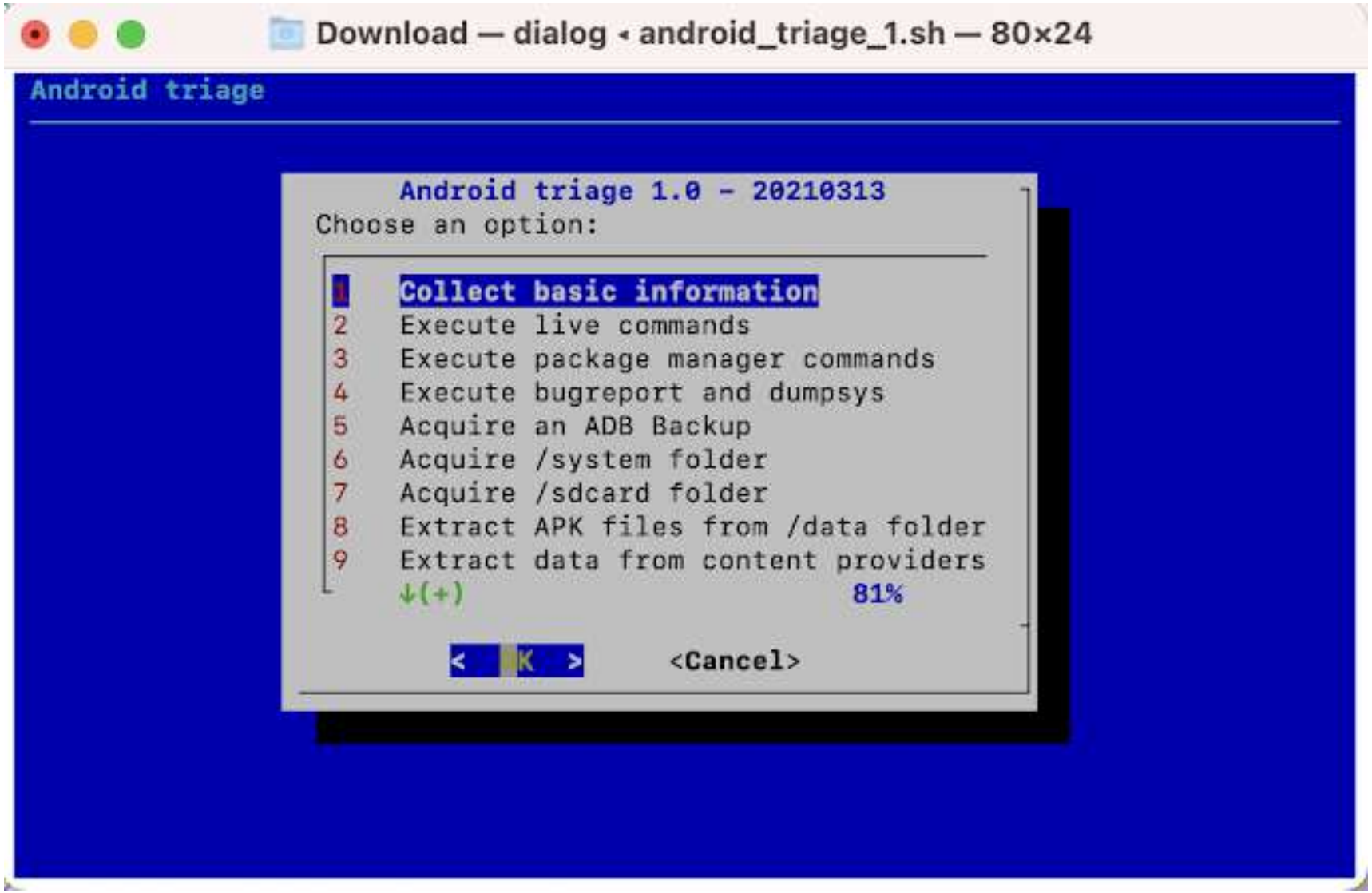
https://github.com/abrignoni/iLEAPP

Apple Pattern of Life Lazy Output'er (APOLLO)

```
Sarahs-Air:APoLLO oompa$ python apollo.py --help
usage: apollo.py [-h] -o {sql,csv} -p {ios,mac,yolo} -v {8,9,10,11,12,yolo}
                 modules_directory data_dir_to_analyze

        Apple Pattern of Life Lazy Outputter (APoLLO)

Very lazy parser to extract pattern-of-life data from SQLite databases on iOS/macOS datasets (though really any SQLite
 database if you make a configuration file and provide it the proper metadata details.

Outputs include SQLite Database or CSV.

Yolo! Meant to run on anything and everything, like a honey badger - it don't care. Can be used with multiple dumps of
 devices. It will run all queries in all modules with no regard for versioning. May lead to redundant data since it ca
n run more than one similar query. Be careful with this option.

        Version: BETA 01172019 - TESTING PURPOSES ONLY, SERIOUSLY.
        Updated: 01/17/2019
        Author: Sarah Edwards | @iamevltwin | mac4n6.com
        Added Efficiency: Sam Alptekin of @sjc_CyberCrimes

positional arguments:
  modules_directory     Path to Module Directory
  data_dir_to_analyze   Path to Data Directory. It can be full file system dump or directory of extracted databases, i
t is recursive.

optional arguments:
  -h, --help            show this help message and exit
  -o {sql,csv}          Output: sql=SQLite or csv=CSV (required)
  -p {ios,mac,yolo}     Platform: ios=iOS [supported] or mac=macOS [not yet supported] (required).
  -v {8,9,10,11,12,yolo}
                        Version of OS (required).
```

https://github.com/mac4n6/APOLLO

Android Triage

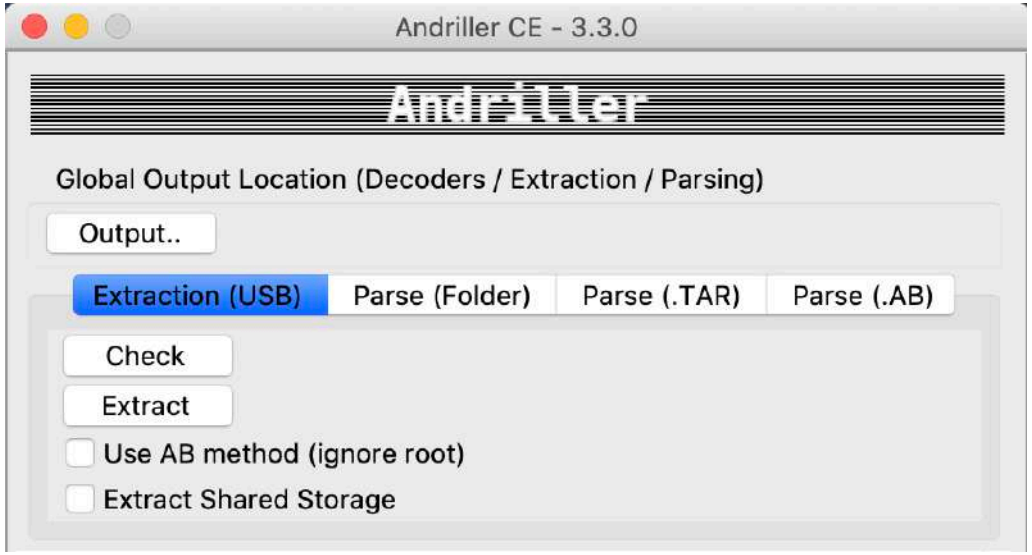


https://github.com/RealityNet/android_triage

Andriller

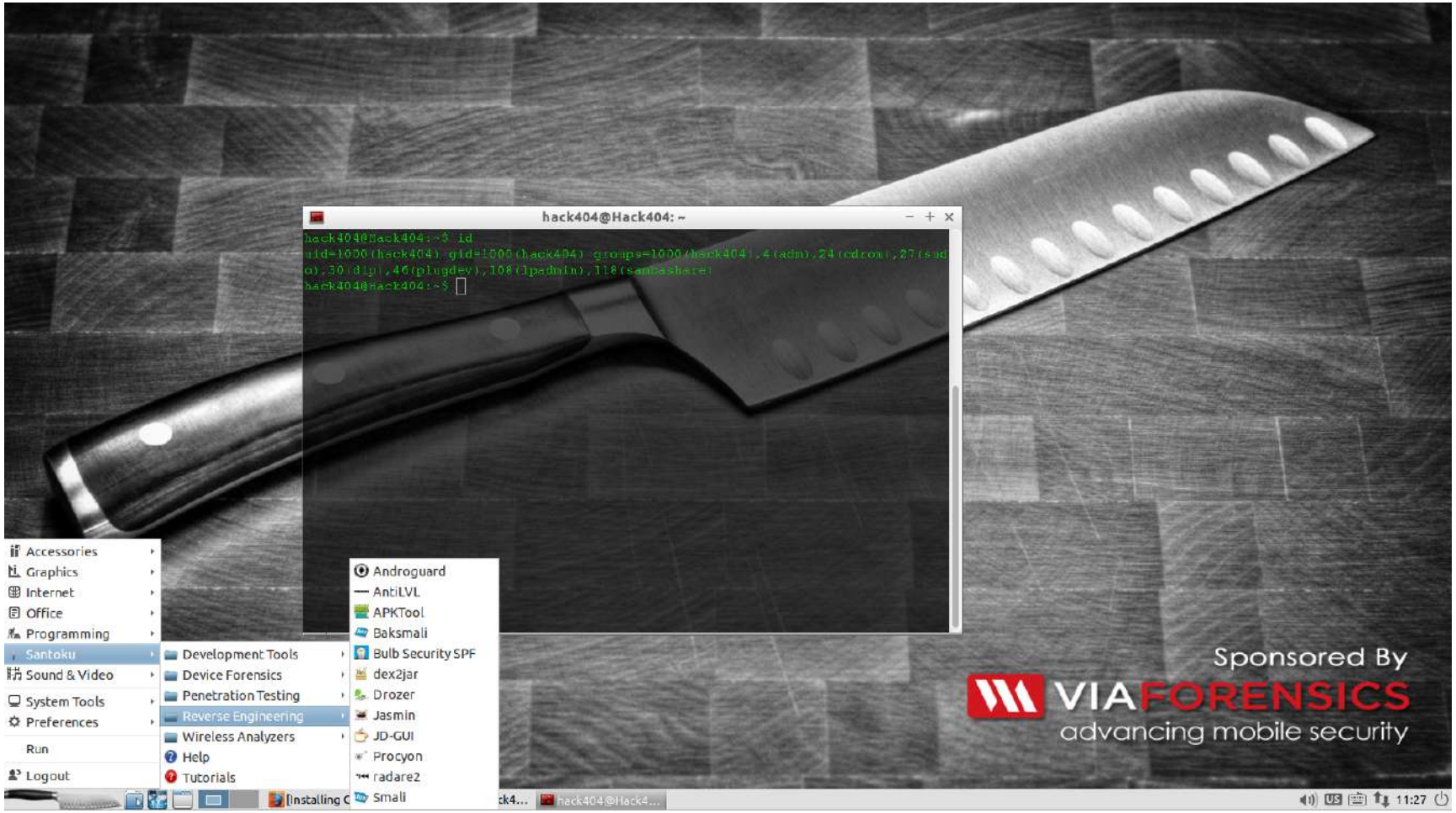
Utility with a collection of forensic tools for smartphones. It performs read-only, forensically sound, non-destructive acquisition from Android devices.

It has features, such as powerful Lockscreen cracking for Pattern, PIN code, or Password; custom decoders for Apps data from Android (some Apple iOS & Windows) databases for decoding communications. Extraction and decoders produce reports in HTML and Excel formats.

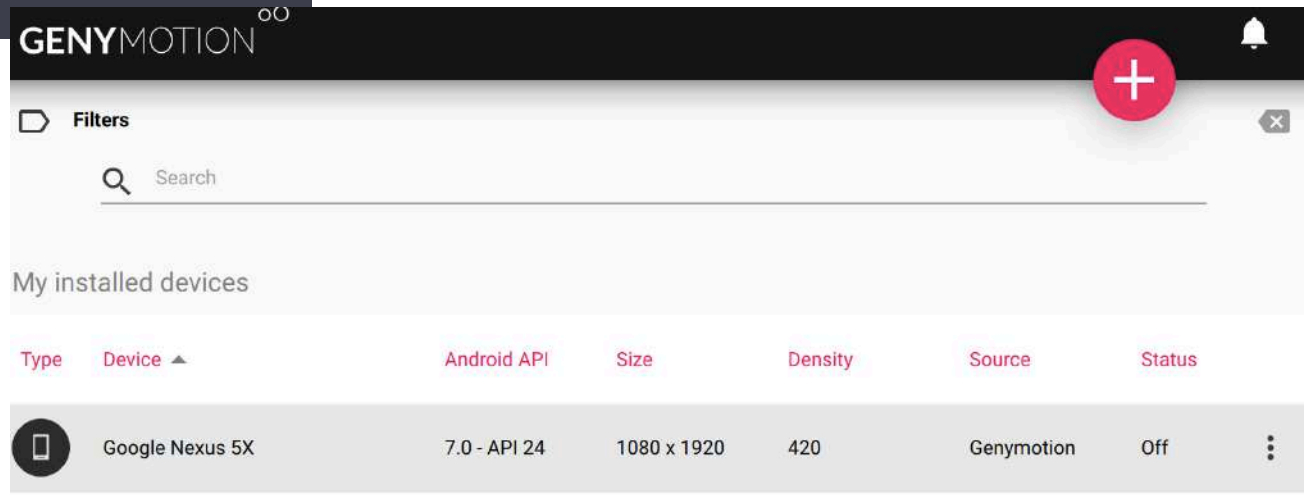


https://github.com/den4uk/andriller

Santoku Linux



https://santoku-linux.com/



Mobile Security Framework + Genymotion

https://github.com/MobSF/Mobile-Security-Framework-MobSF

Dani Creus
Lead Researcher, GReAT

kaspersky

kaspersky

Fundada en 2019

COALITION AGAINST STALKERWARE

La Coalición contra el Stalkerware se fundó en 2019 para facilitar la comunicación entre las organizaciones que trabajan para combatir la violencia de género y la comunidad TI.

Los 10 miembros fundadores se han comprometido a luchar contra la violencia doméstica, stalking y el abuso abordando el uso del stalkerware y concienciando y formando acerca de este problema.

Miembros fundadores

Organizaciones de ayuda

NNEDV NATIONAL NETWORK TO END DOMESTIC VIOLENCE

OPERATION SAFE ESCAPE

WEISSER RING Wir helfen Kriminalitätsopfern.

WWP || EUROPEAN NETWORK

ONGs

EFF

Proveedores de seguridad

kaspersky

Avira

Malwarebytes

G DATA

NortonLifeLock™

Objetivos de la Coalición

COALITION AGAINST STALKERWARE

- Definir las mejores prácticas respecto al stalkerware y otras tecnologías potencialmente no deseadas que se despliegan sin el consentimiento del usuario
- Facilitar el aprendizaje sobre el stalkerware y amenazas relacionadas entre los profesionales de seguridad y las empresas
- Mejorar la respuesta de la industria TI, compartiendo muestras de stalkerware conocido entre los fabricantes de ciberseguridad y evaluando las soluciones de seguridad TI
- Consensuar criterios para la detección del stalkerware
- Concienciar, sensibilizar y educar respecto al stalkerware a través de la formación y la creación de diverso contenido
- Incrementar la capacidad técnica de las organizaciones que asesoran y trabajan con las víctimas

Logros en 2020

COALITION AGAINST STALKERWARE

Durante 2020, los partners de la Coalición han llevado a cabo las siguientes actividades:

- Producción de **recursos online de ayuda para víctimas y supervivientes,** incluyendo un video explicativo disponible en 6 idiomas y listado de organizaciones de ayuda
- **Mayor concienciación sobre el stalkerware** entre organizaciones de ayuda, periodistas y reguladores a través de eventos públicos, investigaciones, prensa, etc.
- Creación de una **definición y criterios de detección estándar y consensuados** para el stalkerware, que no existían previamente. Es importante disponer de estándares en la industria para combatir mejor el stalkerware ya que son una guía y ayudan a mejorar la detección.
- **Incremento de los socios** (de 10 miembros a 26 in total) y regiones (Australia, África, Norte América, Europa)

Crecimiento en 2020

COALITION AGAINST STALKERWARE

En menos de 1 año, la Coalición ha duplicado sus miembros lo que es un indicador más de la relevancia social del stalkerware. En 2020, 16 nuevas organizaciones se han unido para proteger a las víctimas de la violencia digital. La Coalición contra el Stalkerware cuenta actualmente con 26 partners de diferentes países.

Miembros

Organizaciones de ayuda

NNEDV National Network to End Domestic Violence
Operation Safe Escape
bff: Frauen gegen Gewalt e.V.
centre hubertine auclert
SPARC Stalking Prevention, Awareness, and Resource Center
Weisser Ring – Wir helfen Kriminalitätsopfern.
WWP European Network
AEQUITAS
WESNET The Women's Services Network
Illinois Stalking Advocacy Center – Together we make a difference.

Org. tech. sin ánimo de lucro

EFF
Cyber Peace Foundation
CPAUG – Bringing People Together
AppEsteem
ECHO
Institut für Technik und Journalismus

Proveedores seguridad

kaspersky
G DATA
Malwarebytes
Avira
NortonLifeLock
F-Secure
Corrata – Immune System for Mobile
COPPERHEAD
Certo
traced

Video explicativo

COALITION AGAINST STALKERWARE

Con el fin de proporcionar información útil, los miembros de la Coalición contra el Stalkerware han creado un video explicativo sobre esta problemática que incluye lista de indicadores y los pasos que han de seguirse y evitarse en caso de sospecha

- Español https://www.youtube.com/watch?v=_ens5N_36yo
- Portugués https://www.youtube.com/watch?v=Vlp1RWR1HKQ
- Inglés https://www.youtube.com/watch?v=zLtfoCw16Z0&t=20s
- Francés https://www.youtube.com/watch?v=NdPaADXKUOs
- Alemán https://www.youtube.com/watch?v=L3Ww-uWXw7M
- Italiano https://www.youtube.com/watch?v=dJV1wM6zgtw

Los videos también están disponibles en la página de inicio de la Coalición www.stopstalkerware.org

Acciones llevadas a cabo por Kaspersky

En qué estamos trabajando:

- Intercambio de muestras de Stalkerware para mejorar los ratios de detección en la industria
- Formación técnica
- Mejorar la notificación de las detecciones
- Orientar y guiar las actividades junto con la Coalición
- Concienciar y compartir conocimiento

Qué nos gustaría conseguir y queremos ofrecer:

- Un dialogo abierto para combatir juntos el stalkerware
- Sensibilizar y compartir conocimiento
- Formación y cursos online para ONGs, reguladores y otras partes interesadas