Android Forensics

*Cheat sheet

¿Necesitas realizar un diagnóstico (triaje) forense en móviles?

En **forensics.socialtic.org** encontrarás explainers, tutoriales, how-tos y referencias que te ayudarán a aprender **cómo realizar un proceso de diagnóstico forense con perspectiva de derechos humanos** utilizando procesos, protocolos y herramientas desarrolladas por la comunidad de seguridad digital de todo el mundo.

En este cheat sheet encontrarás recomendaciones útiles que te permitirán recorrer de manera rápida y sencilla el proceso de diagnóstico forense en dispositivos Android.

El proceso de forense se compone de las siguientes etapas:

1. Identificación

El primer paso es conocer a la persona, su contexto y la naturaleza del incidente.

Esto ayuda a evaluar riesgos y definir si procede un análisis forense.

✳ **Verificar identidad**

- Si no hay relación previa, realiza una videollamada inicial.
- Solicita datos verificables (nombre, afiliación, trabajo, referencias con organizaciones aliadas).
- Recuerda: en la sociedad civil, el trabajo forense puede implicar riesgos.

Guía de riesgos → forensics.socialtic.org/explainers/02-explainer-risks-threats/

✳ **Identificar la necesidad de un diagnóstico.**

Evalúa si los indicios corresponden a fallas técnicas o a una posible intrusión:

- ¿El dispositivo presenta daños físicos o configuraciones alteradas?
- ¿Existen rastros sospechosos? (phishing, apps desconocidas, mensajes extraños, filtración de información).
- ¿El ataque parece genérico o dirigido? ¿Es conocido o nuevo?
- ¿Qué fechas están asociadas a los incidentes?

✳ **Consentimiento informado**

Si confirmas la necesidad de diagnóstico, explica claramente:

- Qué información se recolectará.
- Cómo se procesará y el alcance del análisis.
- Qué ocurrirá después del análisis.
- Puedes descargar una plantilla de consentimiento

Descargar aquí → forensics.socialtic.org/how-tos/01-how-to-obtain-informed-consent/index.html

2. Recolección y adquisición

Desde la sociedad civil se ha buscado realizar diagnósticos forenses no invasivos y respetuosos a la privacidad. Es por esto que la aproximación forense basada en logs es la más adecuada.

¿Por qué usar logs? → forensics.socialtic.org/en/explainers/03-explainer-log-forensics-android/

✳ Para realizar extracciones forenses en Android te recomendamos extraer un bugreport o utilizar la herramienta androidqf.

- **Cómo extraer bugreport**

→ forensics.socialtic.org/how-tos/05-how-to-extract-bugreport/index.html

- **Cómo extraer mediante androidqf**

→ forensics.socialtic.org/how-tos/04-how-to-extract-with-androidqf/index.html

✳ Considera que una extracción mediante androidqf en este momento contiene mayor información que un bugreport.

3. Verificación y preservación

Una vez extraída la información a analizar se debe almacenar siguiendo una cadena de custodia adecuada.

✳ Almacenar la información en **un medio seguro**, por ejemplo un medio externo cifrado.

✳ Almacenar la información en **un espacio físico seguro**, por ejemplo, una caja fuerte o un mueble con llave dedicado a almacenar información forense.

✳ Almacenar la información **en modo lectura o con firma digital**, por ejemplo, se pueden generar los hashes de los archivos extraídos o firmarlos digitalmente mediante openssl.

Nota: Dependiendo de la versión de androidqf la herramienta generará un archivo hashes.csv o generará los archivos en modo de solo lectura.

4. Análisis

Para un análisis inicial puedes utilizar Mobile Verification Toolkit (MVT).
Esta es una herramienta de línea de comandos que te permite analizar bugreports o extracciones realizadas con androidqf.

* Puedes instalar la herramienta mediante pip.

```
Shell
pip install mvt
```

* Puedes descargar una serie de indicadores de compromiso (IoC) para que la herramienta los utilice durante el análisis.

```
Shell
mvt-android download-iocs
```

* Para analizar un bugreport.

```
Shell
mvt-android check-bugreport /path/to/bugreport.zip
-o /path/to/save/output
```

* Para analizar una extracción de androidqf.

```
Shell
mvt-android check-androidqf /path/to/androidqf/adquisition/
-o /path/to/save/output
```

* **Para revisar los resultados del análisis puedes hacer lo siguiente:**

  - Revisar la línea de tiempo de acciones detectadas en el dispositivo mediante el archivo timeline.csv y contrastar con las fechas relevantes identificadas en la entrevista inicial.
  - Revisar las alertas o errores registrados en el archivo command.log
  - Si una alerta es altamente sospechosa puedes revisar el archivo de salida del módulo correspondiente que haya generado la alerta.
  - Si una alerta corresponde a una coincidencia con un IoC se generará un archivo con la terminación _detected en su nombre.

* **Si requieres revisar un archivo o información en específico puedes encontrar explicaciones detalladas en:**

→ forensics.socialtic.org/references/01-reference-androidqf-dictionary/index.html

5. Presentación

Dependiendo de los resultados puedes elaborar un informe con tus hallazgos. Te recomendamos incluir:

- Información de los elementos identificados en la entrevista inicial que derivaron en el análisis forense.
- Detalles de la información extraída, por ejemplo si fue un bugreport o mediante androidqf, y el cómo y cuándo se extrajo la información.
- Resultados e interpretación del análisis realizado con MVT.

  Para esto no es necesario incluir la salida de MVT o el contenido de los archivos como tal, sino más bien precisar los hallazgos por ejemplo si había rastros de actividad sospechosa, que tipo de rastros, si había aplicaciones maliciosas, cuales eran estas aplicaciones, etc.

- Recomendaciones o siguientes pasos para atender el incidente o

* **Recuerda que la información debe ser clara y concisa, y se recomienda utilizar un lenguaje sencillo para que cualquier persona no técnica pueda entender el resultado.**

Para entender más del proceso forense te recomendamos leer:

¿Necesitas hacer un triaje forense en Android?

Entra a **forensics.socialtic.org** y aprende a realizarlo paso a paso.

Si necesitas apoyo adicional o un peer-review, no dudes en escribirnos a:

→ seguridad@socialtic.org

Sé parte de la comunidad.

Hay mucho más por desarrollar.
¡Únete a nosotros y comparte tus conocimientos!

→ forensics.socialtic.org/community/index.html

@socialTIC | forensics.socialtic.org

SOCIALTIC