Android Forensics

*Cheat sheet ✱

Do you need to perform a forensic triage on Android phones?

At **forensics.socialtic.org**, you'll find **explainers, tutorials, how-to guides, and references** to guide you step-by-step through the forensic triage process with a human rights perspective, using protocols and tools created by the global digital security community.

This cheat sheet provides quick and clear recommendations for performing **forensic triage on Android**, from initial preparation to evidence collection.

Forensic process consists of the following stages:

1. Identification

The first step is to understand the person, their context, and the nature of the incident. This helps assess risks and determine whether a forensic analysis is appropriate

✱ **Verify identity**

- If there is no prior relationship, conduct an initial video call.
- **Request verifiable information** (name, affiliation, job, references from partner organizations).
- **Remember: in civil society, forensic work can involve risks.**

Risk guide → forensics.socialtic.org/en/explainers/02-explainer-risks-threats/

✱ **Identify the need for a diagnosis**

Evaluate whether the signs indicate a technical failure or a possible intrusion:

- **Does the device have physical damage or modified settings?**
- **Are there any suspicious traces?** (phishing, unknown apps, strange messages, information leaks)
- **Does the attack seem generic or targeted? Is it a known attack or a new one?**
- **What dates are associated with the incidents?**

✱ **Informed consent**

If you confirm the need for diagnosis, clearly explain:

- **What information will be collected.**
- **How it will be processed and the scope of the analysis.**
- **What will happen after the analysis.**
- **You can download a consent template:**

Download here → forensics.socialtic.org/en/how-tos/01-how-to-obtain-informed-consent/

2. Collection and acquisition

Civil society has sought to perform non-invasive and privacy-friendly forensic diagnoses. This is why a log-based forensic approach is the most appropriate.

Why use logs? → forensics.socialtic.org/en/explainers/03-explainer-log-forensics-android/

✱ To perform forensic extractions on Android, we recommend extracting a bugreport or using the androidqf tool.

- **How to extract a bugreport** →forensics.socialtic.org/en/how-tos/05-how-to-extract-bugreport/
- **How to extract using androidqf** → forensics.socialtic.org/en/how-tos/04-how-to-extract-with-androidqf/

✱ Both methods support a rapid and responsible triage approach, without unnecessarily compromising the privacy of those tested.

✱ Consider that an extraction using androidqf currently contains more information than a bugreport.

3. Verification and preservation

Once the information to be analyzed has been extracted, it must be stored following an appropriate chain of custody. For this purpose, we recommend:

✱ Store the information in **a secure medium**, such as an encrypted external device.

✱ Store the information in **a secure physical space**, such as a safe or a locked cabinet dedicated to storing forensic information.

✱ Store the information **in read-only mode or with a digital signature.** For example, you can generate hashes of the extracted files or digitally sign them using OpenSSL.

Note: Depending on the androidqf version, the tool will generate a hashes.csv file or generate the files in read-only mode.

↘

4. Analysis

For an initial analysis, you can use the Mobile Verification Toolkit (MVT). This is a command-line tool that allows you to analyze bugreports or acquisitions made with androidqf.

✻ You can install the tool using pip.

Shell
```
pip install mvt
```

✻ You can download a set of indicators of compromise (IoCs) for the tool to use during the scan.

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

✻ To analyze a bugreport.

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

✻ To analyze an androidqf acquisition.

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

✻ **To review the analysis results you can do the following:**

- Review the timeline of actions detected on the device using the timeline.csv file and compare it with the relevant dates identified in the initial interview.
- Review alerts or errors recorded in the command.log file
- If an alert is highly suspicious, you can review the output file of the corresponding module that generated the alert.
- If an alert corresponds to a match with an IoC, a file with the _detected append in its name will be generated.

✻ **If you need to review a specific file or information, you can find detailed explanations in the References section.**

→ forensics.socialtic.org/en/references/index.html

5. Presentations

Depending on the results, you can prepare a report with your findings. We recommend including:

- Information on the elements identified in the initial interview that led to the forensic analysis.
- Details of the information extracted, for example, whether it was a bugreport or through androidqf, and how and when the information was extracted.
- Results and interpretation of the analysis performed with MVT.

  For this, it is not necessary to include the MVT output or the contents of the files themselves, but rather to specify the findings, such as whether there were traces of suspicious activity, what type of traces, if there were malicious applications, which applications they were, etc.

✻ **Remember that the information should be clear and concise, and it is recommended to use simple language so that any non-technical person can understand the result.**

To understand more about the forensic process, we recommend reading:

Do you need to perform forensic triage on Android?

Visit forensics.socialtic.org/en/how-tos/index.html and learn how to do it step by step.

If you need additional support or peer review, please feel free to contact us at:

→ seguridad@socialtic.org

Join the effort.

There is plenty more to develop.
Come join us and share your knowledge!

→ forensics.socialtic.org/en/community

@socialTIC | forensics.socialtic.org

SOCIALTIC