

Mobile Verification Toolkit

github.com/mvt-project/mvt

mvt-project

mvt-project/mvt



MVT (Mobile Verification Toolkit) helps with conducting forensics of mobile devices in order to find signs of a potential compromise.

32
Contributors

15
Issues

5
Discussions

8k
Stars

683
Forks



pypi v1.5.4 docs passing CI passing downloads 133k

Mobile Verification Toolkit (MVT) is a collection of utilities to simplify and automate the process of gathering forensic traces helpful to identify a potential compromise of Android and iOS devices.

It has been developed and released by the [Amnesty International Security Lab](#) in July 2021 in the context of the [Pegasus project](#) along with [a technical forensic methodology and forensic evidence](#).

Warning: MVT is a forensic research tool intended for technologists and investigators. Using it requires understanding the basics of forensic analysis and using command-line tools. This is not intended for end-user self-assessment. If you are concerned with the security of your device please seek expert assistance.

Installation

MVT can be installed from sources or from [PyPi](#) (you will need some dependencies, check the [documentation](#)):

```
pip3 install mvt
```

For alternative installation options and known issues, please refer to the [documentation](#) as well as [GitHub Issues](#).

Usage

MVT provides two commands `mvt-ios` and `mvt-android` . [Check out the documentation to learn how to use them!](#)

License

The purpose of MVT is to facilitate the ***consensual forensic analysis*** of devices of those who might be targets of sophisticated mobile spyware attacks, especially members of civil society and marginalized communities. We do not want MVT to enable privacy violations of non-consenting individuals. In order to achieve this, MVT is released under its own license. [Read more here.](#)