FORMOBILE

From Mobile Phones to Court

19 Partners

15 Countries

€7 Milion

Work Package 6.2

Malware analysis

Primary Objectives

To develop an automated analysis platform for Android malware. This system should classify according to respective behaviours and have the ability to overcome anti-forensic techniques in malware. This system should generate reports to summarise its findings.

FACTS & FIGURES

DID YOU KNOW?

6 **Parallelised analysis routes** for effective processing of analysis orders

8-11 **Minutes to analyse an application**, depending on its size and range of functions

14.27 **Million Android applications** of various ages and functionality evaluated to increase the knowledge about the properties

2717 **Applications examined more closely to train** the decision-making function of the analysis platform

Main Tasks

- **Automated examination** of Android applications for malicious functions and strategies
- **Detection and classification of malware** and inclusion of a wide range of information about suspicious applications in the investigative work
- **Use of data** from the code-based analysis combined with the behaviour from the dynamic execution on real hardware components
- **Benefits from realistic results** and basic protection against antiforensic mechanisms through the integrated simulation of manufacturers and Android versions
- **Generation of a report valid** for legal purposes, including detailed forensic information

Key Output

Functional prototype for automated and hardware-based Android malware analysis

This project has received funding from the European Union's Horizon 2020 – Research and Innovation Framework Programme H2020-SU-SEC-2018, under grant agreement no. 832800.