Forensic Imaging and Analysis of Apple iOS Devices

Background:

- 700M iOS devices sold so far, ~300M in the last year.
- Smartphones and tablets hold huge amounts of personal data.
- Relatively new OS and apps - ideal for forensic research.

Objectives:

- Acquire a forensic image of the data stored in the device.
- Analyse the information, extract traces of user activity.

Methods:

- iOS runs only signed apps – and even those run with limited privileges.

→ Jailbreak: exploit software bugs to gain root access and run custom code.

Results:

- Forensic imaging: The iPad supports USB! Using a cheap accessory, data can be dumped to an external hard drive. 30x faster than existing Wi-Fi methods.
- Forensic analysis: We observed that printing documents leaves certain traces in the device, and developed a method to recover such traces, gaining access to the contents and metadata of printed documents.

Future work:

- iCloud Forensics: How file syncing affects certain metadata such as file creation and modification timestamps.
- Analysis of the AirDrop feature to share files across nearby devices.

Luis Gómez-Miralles, Joan Arnedo-Moreno

First UOC International Research Symposium

December 2013, Barcelona (Spain)

UOC
Universitat Oberta de Catalunya