

International Conference on
FORENSIC RESEARCH & TECHNOLOGY
&
ANNUAL BIOMARKERS CONGRESS

September 17-18, 2018 | Osaka, Japan



Oleg Afonin

ElcomSoft Co. Ltd, Germany

The complete iOS forensic workflow: From physical extraction to iCloud

Accessing evidence stored in iOS devices (iPhones and iPads) is a challenge. Full-disk encryption stands in the way of low-level acquisition, while the many hardware and system level restrictions make physical extraction extremely difficult. At the same time, the iPhone must remain usable and accessible to the owner, which means a forensic specialist may still be able to get around iOS security measures.

iOS devices feature several layers of protection, which makes seizing, storing and transporting iOS devices a challenge requiring expertise. Latest version of Apple's mobile operating system actively resist forensic efforts by disabling the less secure biometric identification (Touch ID or Face ID) and blocking USB connectivity after a short

period of time. Many of these restrictions can be effectively bypassed with proper timing and the right technique.

In this talk, we'll cover the entire iOS forensic workflow. We'll start from seizing, transporting and storing the device, and discuss approaches, methods and tools to access information and extract evidence. We'll address USB restricted mode, talk about using existing pairing records to extract locked devices, and discuss physical acquisition via jailbreaking. We'll look at the types of data Apple devices store and sync via iCloud, and learn how to extract that data. Finally, we will talk about extracting stored passwords from local and iCloud keychain. Logical, physical and cloud acquisition methods will be covered.

Biography

Oleg Afonin is an IT security researcher and a mobile forensic specialist at ElcomSoft Co. Ltd., the company developing digital forensics tools. Oleg has trained forensic specialists and police forces in Canada, Germany, Austria and the UK. He speaks regularly at forensic events and conferences all over the world. Oleg co-authored a book on Mobile Forensics - Advanced Investigative Strategies¹.

aoleg78@gmail.com

Notes: