ELCOMSOFT
DESKTOP, MOBILE & CLOUD FORENSICS

TRAINING

Mobile & Cloud Forensics

Fast links

Feature List

- Duration: 3 days
- Group size: up to 12 students
- Instructors: experts in mobile forensics
- Certification: provided
- Included: 90-day access to full versions of all software tools used during the training
- Extra benefits: the book “Mobile Forensics — Advanced Investigative Strategies” by **Vladimir Katalov** and **Oleg Afonin**

Course Description

Reasons to take the Advanced iOS Forensics course

In this 3-day course on iOS forensics, students are led through the fundamentals of mobile forensics including an overview of common mobile platforms and operating systems. They will learn about the most effective workflow including evidence preservation, logical, physical and cloud based acquisition. Students will learn how to cope with encryption and password protection and develop skills necessary to successfully obtain evidence from locked devices and password-protected backups. Attendees who successfully pass the class assignments will be given a certificate of completion.

The skills you get

The students will develop an in-depth knowledge of password protection and data encryption techniques used in mobile forensics. The attendees will further master modern technologies for mobile forensics, evidence preservation, data extraction and decryption. The students will master the data extraction workflow using logical, physical and cloud acquisition methods; develop jailbreaking skills and learn how to use a jailbreak for data extraction on different generations of iOS devices. The attendees will master cloud extraction, including the extraction of static backups and dynamic (synced) evidence.

Program

Day 1	• A brief overview of global mobile platforms • The mobile forensics workflow (steps and techniques) • Physical, logical and cloud acquisition methods compared
Day 2	• Jailbreak-based physical acquisition (iOS devices) • Authentication tokens and pairing records • Multi-platform data extraction
Day 3	• Cloud-based over-the-air data acquisition • Handling two-factor authentication • Extracting IM communications (WhatsApp, Signal) and other app data

Certification

All attendees are invited to do a practical exercise on mobile forensics. Using a proper workflow for seizing and storing mobile devices to preserve evidence and using all available acquisition steps in the right order are essential parts of the training. Attendees will be using the skills and knowledge acquired during the training to perform acquisition of a given device. Attendees who successfully pass the assignments will be awarded a certificate of ElcomSoft standard.

The Trainers

Vladimir Katalov is CEO, co-founder and co-owner of ElcomSoft Co.Ltd. Vladimir manages all technical research and product development in the company. He regularly presents on various events and runs security and computer forensics training both for foreign and inner (Russian) computer investigative committees and other law enforcement organizations.

Oleg Afonin is a researcher and an expert in digital forensics. He is a frequent speaker at industry-known conferences such as CEIC, HTCIA, FT-Day, Techno Forensics and others. Oleg co-authored multiple publications on IT security and mobile forensics. With years of experience in digital forensics and security domain, Oleg led forensic training courses for law enforcement departments in multiple countries.

Andrey Malyshev is Director of ElcomSoft in Czech Republic. In 1997 Andrey started working as Head of R&D department and in 2000 became CTO. Now, he is co-responsible for business progress and heads the development of new products. He has been developing some of the most popular programs in the company. He regularly talks at LE & security conferences and runs computer forensic trainings.

Computer Requirements

Computers are generally provided in the class. If students prefer to bring their own laptops, we kindly ask to indicate so on the registration page. For students bringing a laptop to class, please ensure they meet the following **minimum requirements**:

- Windows 7 or
- Windows 8.x and 10.x using these instructions (turn off driver signature enforcement)
- macOS with Bootcamp Windows 7 or
- macOS with Bootcamp Windows 8.x and Win 10.x using these instructions
- macOS alone will not work (No Virtual Machines)
- 8GB RAM (minimum)
- 100GB storage (minimum)
- You must have Admin rights or have the admin password for software installation.

Course Plan in Detail

Introduction: what's inside and how to access it

We'll discuss the types of evidence available in an iOS device, and list some of the methods we can use to extract that evidence.

iPhone acquisition as a chain process

We'll talk about the importance of every procedural step from seizing, handling and storing the device to using acquisition methods in the right order.

Acquisition methods that don't work

Some familiar acquisition methods (JTAG, chip-off etc.) are not available for iOS devices. We'll talk about why that is.

Seizing and preserving evidence

The use of procedures. Do's and don'ts. Trade-offs and compromises. Faraday bags.

Touch ID

We'll discuss the important forensic aspects of Touch ID and its effects on subsequent acquisition.
Additional details in supplement: Touch ID Unlock.pdf

Existing acquisition methods

We'll discuss the available acquisition methods and learn to decide which methods can be used, when and in what order.

Passcode lock and passcode recovery

Bypassing passcode lock is essential. We'll learn why. We'll also talk about passcode recovery boxes and their use in modern iOS forensics.

Practical steps to iOS forensics

Here is where we start discussing the practical steps. First things first; available acquisition methods; what you have and what you know.

What do you have and what do you know?

We'll learn how to make the most from what you have at your disposal and know about the device.

Procedures for unlocked devices

We'll learn what we can do with devices for which you know the passcode or that can be unlocked with Touch ID.

Logical acquisition: local backups

Hands-on: How to approach logical acquisition. Using temporary backup password to decrypt keychain.

Unlocking with pairing records (lockdown files)

Hands-on: How to use and where to obtain lockdown files.

Additional details in supplement: Logical Acquisition.pdf

What if: the backup is encrypted with a password you don't know

Hands-on: Steps to break backup passwords with Elcomsoft Phone Breaker.

Decrypting and exploring backups

Hands-on: How to decrypt iOS backups with a known password. Using Elcomsoft Phone Viewer to explore their content.

Physical acquisition

What you need to know about physical acquisition. Three generations of physical acquisition:

- Gen 1: iPhone 3G, 3GS, 4
- Gen 2: iPhone 4s, 5, 5c
- Gen 3: iPhone 5s, 6/Plus, 6s/Plus, 7/Plus

Additional details in supplements: Physical Acquisition Legacy Devices.pdf, Physical Acquisition iOS 10.pdf and Physical Acquisition with iOS Forensic Toolkit Manual.pdf

Jailbreak

Hands-on: Why jailbreak is required for physical acquisition. How to install jailbreak on different versions of iOS.

Additional details in supplement: How to Install Jailbreak iOS 5 through 10.pdf

Jailbreak tools: all jailbreak tools mentioned in the guide stored in the \jailbreak folder.

Practical guide: physical acquisition of iPhone 5s and newer models (6s through iPhone 11)

Hands-on.

Additional details in supplement: Physical Acquisition iOS 10.pdf

What next? Analyzing iOS Tarball.pdf

What if...

Discussion of potential issues arising during jailbreaking and physical acquisition.

Cloud backups

We'll discuss the benefits and dangers of cloud acquisition.

Locked device: when and how to produce a fresh cloud backup

How to make a device you cannot unlock to produce a fresh cloud backup.

Unlocked device: when and how to produce a fresh cloud backup

Should we try and make an unlocked iPhone produce a cloud backup? Local backups contain just as much data; a fresh cloud backup may be needed if local backup is encrypted with a password you don't know and can't break.

The risks and issues of cloud backups

We'll discuss the risks associated with allowing the device connect to the network.

Downloading cloud backups

Hands-on: Practical steps for downloading backups from iCloud. Using Apple ID and password, the issue of two-factor authentication, extracting and using authentication tokens.

Viewing cloud backups

Hands-on: Using Elcomsoft Phone Viewer to examine iCloud backups.

Authentication tokens

Hands-on: Extracting and using authentication tokens to bypass login, password and two-factor authentication.

Synced data

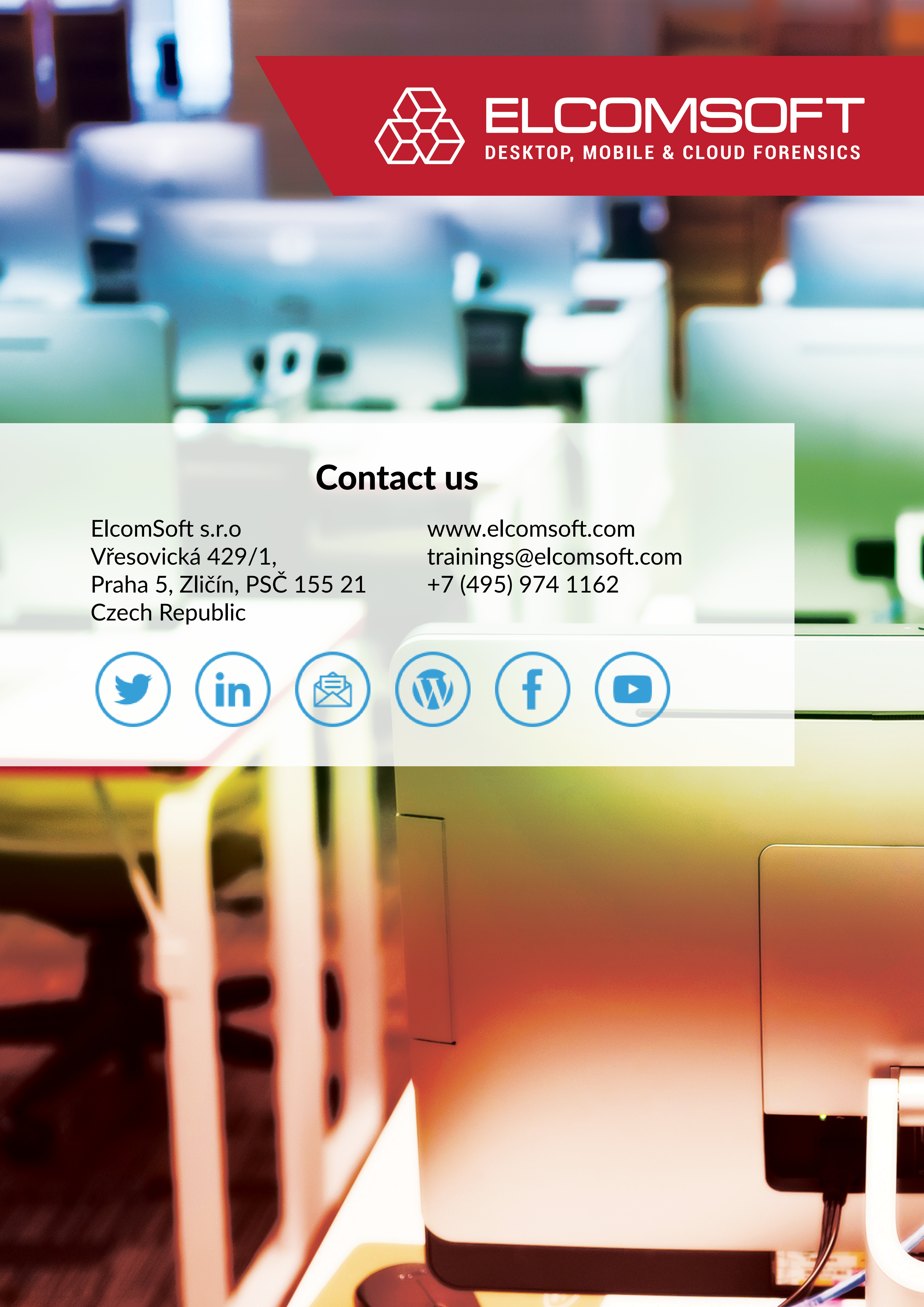
iOS provides real-time synchronization of many types of data. Call logs, Safari browsing history, notes, bookmarks and some other types of data can be extracted in real time.

Extracting, decrypting and exploring the keychain

The keychain stores a lot of valuable information such as Safari passwords, account authentication tokens, and even the Apple ID password. We'll learn how to extract, decrypt and explore keychain items.

Tools used for this guide

Finally, we'll talk about the tools we used through the course of this training.



ELCOMSOFT

DESKTOP, MOBILE & CLOUD FORENSICS

Contact us

ElcomSoft s.r.o
Vřesovická 429/1,
Praha 5, Zličín, PSČ 155 21
Czech Republic

www.elcomsoft.com
trainings@elcomsoft.com
+7 (495) 974 1162