ELCOMSOFT
DESKTOP, MOBILE & CLOUD FORENSICS

TRAINING

Password Recovery, Data Decryption, Mobile & Cloud Forensics

Fast links

Course Description
Program
Certification
The Trainers
Computer Requirements
Course Plan in Detail
Contact us

Feature List

- Duration: 5 days
- Group size: up to 12 students
- Instructors: experts in password recovery & 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 course

In this comprehensive course on password recovery, data decryption, mobile and cloud forensics students are led through the fundamentals of data protection, encryption and password, as well as data extraction from mobile and cloud services. The course teaches students to deal with the many types of encrypted information, explains the differences between the different types of protection, encryption and passwords. Attendees will get hands-on experience in breaking passwords to the many common types of data including encrypted volumes, protected documents, archives and backups. Attendees who successfully pass the class assignments will be given a certificate of completion.

The skills you get

The students will gain in-depth understanding of data protection methods, encryption and passwords. The attendees will learn using the most efficient workflow to access the many types of protected information. They'll learn about the specifics of recovering access to encrypted volumes and crypto containers, gaining access to password-protected documents and archives. The students will master the skills of extracting passwords from the user's computer, building targeted dictionaries and applying meaningful mutations. The attendees will gain understanding of the different types of attacks, the hardware resources required to perform those attacks, and their relation to the recovery timeframe and success probability.

Program

Day 1	• Introduction to encryption and hashing • Choosing the target: keys, passwords and instant recovery • Exploiting the human factor • Understanding distributed computing and GPU acceleration • Gathering the low-hanging fruit: extracting existing passwords from Mac and PC
Day 2	• Targeted dictionary with user's existing passwords • Building a custom dictionary based on online password leaks • Understanding mutations, setting up attack pipeline • Attacking crypto containers • Discovering encrypted content
Day 3	• A brief overview of global mobile platforms • The mobile forensics workflow (steps and techniques) • Physical, logical and cloud acquisition methods compared
Day 4	• Jailbreak-based physical acquisition (iOS devices) • Authentication tokens and pairing records • Multi-platform data extraction
Day 5	• Cloud-based over-the-air data acquisition • Handling two-factor authenticatio • Extracting IM communications (WhatsApp, Signal) and other app data

Certification

All attendees are invited to do a practical exercise on digital forensics. Using a proper workflow for gathering essential information and using all known attack techniques against encryption. Attendees will be using the skills and knowledge acquired during the training to perform data decryption. 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: About Elcomsoft. Training program.

Section 1: Encryption & hashing basics, data/password protection

Part 1.1: Encryption, hashing and password protection

- Cryptography: general information
  - Symmetric and asymmetric encryption
  - Block and stream ciphers
  - Commonly used algorithms
  - Hashing (one-way functions)
  - Salting
- Passwords: general information
  - Review of authentication methods
  - Password protection pros and cons
  - One-time passwords
  - Two-step verification
  - Two-factor authentication
- Common password protection schemes
  - Stored passwords (in plain text or with reversible encryption)
  - Sassword is hashed, but data is not encrypted
  - Data is encrypted with fixed/known key
  - Data is strongly encrypted
- Finding the weakest link (brief review)
  - Extracting/decrypting existing passwords
  - Strong password, known key
  - Strong password, weak (short) key
  - Implementation flaws (e.g. weak rng)
  - Good/strong encryption
  - Salting; many iterations

Part 1.2: Methods of decryption

- When password can be recovered instantly
- Collisions: making the password that works (though not the same as the original one)
- Password reset/replacement (when file is not encrypted)
- Cracking encryption keys instead of passwords (file decryption)
- Strong encryption- main password methods: brute-force, dictionary
- Improvements: brute-force with mask, dictionary mutations
- Other/advanced methods
  - Custom dictionary (password re-use)
  - Rainbow/thunder tables
  - Known-plaintext attack
  - Winzip: guaranteed decryption
  - Quicken: ‘escrow’ key (backdoor)
- Password recovery speeds (examples, time, gpu acceleration etc)
- Password policies, audit, laws/regulations etc.

Section 2: Desktop forensics

Part 2.1: Easy cracking

- Web browsers
- Instant messengers
- Mail clients
- WordPerfect Office
- Lotus SmartSuite
- Microsoft SQL Server
- ACT/Sage/PeachTree
- Microsoft Office (legacy versions; other passwords)
- Adobe PDF protection

Part 2.2: System protection and disk encryption

- Windows logon passwords
  - Creating bootable CD or USB flash drive
  - Auto and manual modes, system detection
  - Local and Active Directory accounts
  - Extracting stored passwords
  - Built-in attacks on passwords
  - Password reset
  - Enabling locked and disabled accounts
  - Escalating user privileges
  - Export password hashes
  - SAM database editing
- Microsoft Encrypting File System
  - Encrypting the files in Windows
  - User certificates backup and recovery
  - EFS internals (master and user keys)
  - Searching for encryption keys
  - Low-level by-sector disk scan
  - Making use of recovery agents
  - Making use of saved certificates
  - Searching for encrypted files
  - Decrypting the files
  - Case studies
    - System is unbootable
    - Accessing the file from other user's account
    - Working with disk images
    - Corrupted user profile
    - Deleted user profile
    - Re-formatted system partition
- Encrypted disks
  - Full disk encryption overview
    - Microsoft BitLocker
    - Symantec PGP
    - TrueCrypt
    - Apple FileVault2

  - Making use of hibernation files
  - Software memory dumping
  - Hardware memory dumping (FireWire)
  - Making use of recovery keys
  - Recovery keys in the cloud (on account)
  - Last resort: brute-force
- **macOS passwords**
  - macOS users' password
  - macOS keychain
    - Keychain password cracking
    - Passwords stored in the keychain
    - Other keychain data: tokens, certificates, keys
  - FileVault2 encryption, password and recovery key
  - DMG file passwords

Part 2.3: Advanced technologies

- **Thunder Tables®**
  - Pre-computed hash tables explained
  - Thunder Tables® vs. Rainbow Tables
  - Performing MS Office Word/Excel and Adobe PDF decryption using pre-computed hash tables
- **Hardware acceleration**
  - NVIDIA GPUs
  - AMD GPUs
  - FPGA-based solutions
- **Distributed computing**
  - General information (architecture)
  - Software and hardware requirements

Part 2.4: Distributed Password Recovery

- **Available attacks (brute force, dictionary, mask, key recovery)**
- **Installation (console, server, agent)**
- **User interface; settings**
- **Hardware preferences (GPU Manager)**
- **Password cache**
- **Logs, alerts, statistics, priority, limitations**
- **Benchmarks**
- **Using Amazon cloud**
- **Future development**
  - Deployment
  - Support for additional file formats
  - Adding multiple files/tasks at once
  - More hardware acceleration (ati, tableau); simultaneous use
  - Different jobs on different agents [groups]
  - More flexible masks

Part 2.5: Wireless password cracking

- Wireless networks and WPA/WPA2-PSK password protection
- Network sniffing using AirPCap adapters
- Network sniffing using 3rd party software
- Performing advanced dictionary attacks with highly customizable permutations
- Packet injection
- Creating fake access points

Section 3: Mobile forensics

Part 3.1: Introduction

- Mobile devices overview
- Mobile devices market
- Mobile operating systems
  - iOS (legacy and 4-9)
  - BlackBerry OS (legacy and 10)
  - Windows Phone and Windows 10 Mobile
  - Android
  - Other systems
- Data stored on mobile devices
- Encryption and protection
- Mobile forensics methods and approaches
  - Data preservation
  - Logical extraction
  - Physical extraction
  - Chip-off and JTAG
  - Acquisition and analysis of local backups
  - Acquisition and analysis of cloud backups
  - Acquisition and analysis of cloud-synced data

Part 3.2: Working with iOS devices – physical acquisition

- Introduction
  - What is physical acquisition
  - Advantages of physical acquisition
    - » Cached mail
    - » Location data
    - » iOS and third-party application data
    - » System & network logs
    - » Photo library (if iCloud Photos is enabled)
    - » Caches, temp files, log
    - » WAL data
- Compatible devices (new, with jailbreak)
  - 64-bit devices: file system acquisition, keychain extraction
- Working with the disk images (DMG) on Windows and OS X

Part 3.3: Working with iOS devices – iCloud acquisition

- Introduction
  - iTunes backups
  - iTunes backup protection
  - Making use of lockdown records
  - Extracting backup passwords from Windows and OS X
  - Backup password cracking
- iCloud backups
  - iCloud backups creation
  - iCloud backups storage and encryption
  - Downloading using apple id and password
  - Downloading using authentication tokens
  - Extracting authentication token from windows
  - Extracting authentication token from OS X
  - Extracting dsid and authentication token from other device
  - Handling two-step verification
  - Differences between itunes and iCloud backups
    - » IMEI and some other data
    - » Keychain encryption
- Handling two-factor authentication
- Data on iCloud Drive
  - Documents
  - 3rd party application data
  - System data

Part 3.4: Working with iOS devices – other facilities

- Backup password cracking
- Backup decryption
- Cracking 1Password databases
- Decrypting and analysing keychain data
  - Wi-Fi passwords
  - Mail passwords
  - RDP & VPN passwords
  - Application passwords
  - Apple ID and password
  - Dsid and authentication token
  - Social network tokens
  - Other tokens and keys
  - Saved credit card data
  - Browser auto-complete data

Part 3.5: iOS data analysis

- Data categories
  - Contacts
  - Calendars
  - Notes
  - Messages
    - » SMS & iMessage

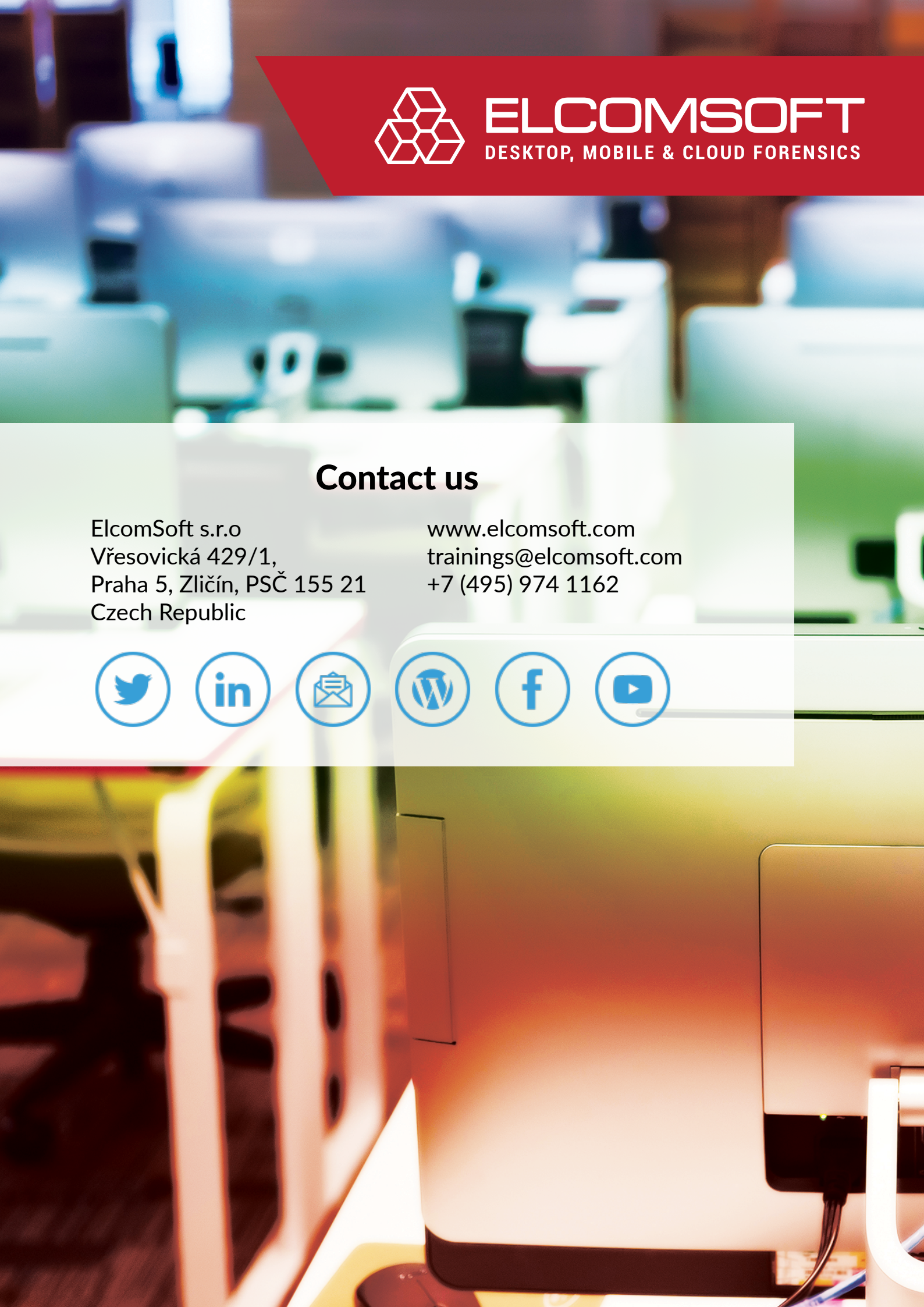
    - » Encrypted messages (iOS 9.3)
    - » Message attachments
    - » Recovery of deleted messages
  - Call log
  - Web (Safari) data
    - » Bookmarks
    - » History
    - » Search history
    - » Auto-complete data
  - Media library
    - » Albums
    - » Location data
    - » iCloud Photos
- Filtering and searching
  - By date/time
  - By data type
- Export and reporting

Part 3.6: Acquisition and analysis of WhatsApp data

- iOS: local iTunes backups
- iOS: iCloud backups
- iOS: data on iCloud Drive
- Android: data in internal memory
- Android: backups on SD card
- Android: backups on Google Drive
- Android: backups encryption

Part 3.7: Google account acquisition and analysis

- Information stored in Google account
- Android and iOS data syncing with Google accounts
- Extracting and browsing information from Google
  - User info
  - Contacts
  - Calendars
  - Notes
  - Messages
  - Dashboard
  - Backup data
  - Web data (Chrome) & History
    - » Browsing history
    - » Search history
    - » YouTube data
  - Location data
  - Media files
    - » Albums
    - » EXIF data
    - » Contacts & cycles
- Handling two-factor authentication
- How to get password to Google account



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