ELCOMSOFT
DESKTOP, MOBILE & CLOUD FORENSICS

TRAINING
Advanced Password Recovery

Fast links

Feature List

- Duration: 3 days
- Group size: up to 12 students
- Instructors: experts in password recovery
- 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 Password Recovery course

In this comprehensive course on password recovery, students are led through the fundamentals of data protection, encryption and passwords. 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 • Custom dictionary based on online password leaks • Understanding mutations • Setting up attack pipeline
Day 3	• Attacking BitLocker • Extracting user's existing passwords and building a custom dictionary • Discovering encrypted content • Setting up attack pipeline and recovering password

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.

Data protection. Methods and solutions.

Methods and algorithms used for protecting secrets (keys, tokens, passwords etc.) We'll discuss each method and detail its weaknesses and how to exploit them to break protection.

Cryptography. Encryption algorithms and hash functions.

It's impossible to talk about breaking passwords without knowing the basics of data encryption. We'll introduce students to cryptography and talk about the most widely used encryption algorithms and encryption keys. We'll also discuss hashes from the very basics to advanced concepts including multiple hash iterations, salt and pepper.

Encryption in Microsoft Office. Working with Elcomsoft products to decrypt documents

Before we start breaking Microsoft Office documents, we'll discuss how the data is protected in the many different generations of Microsoft Office products. We'll talk about passwords to open and restrictions passwords, learn breaking weak encryption using Thunder Tables, and more.

Lab: Using Elcomsoft products to break MS Office document

Password protection. Weak and strong algorithms. History and evolution.

A brief introduction to the history and evolution of password protection.

Passwords stored in internet browsers.

Today's Web browsers include fully featured password management. These passwords can be easily extracted from the user's computer or downloaded from their cloud account (Apple, Google or Microsoft). We'll tell how to access those passwords.

Lab: Acquiring passwords with Elcomsoft Internet Password Breaker. Making and using dictionaries.

The easiest method of extracting passwords from the user's computer is using Elcomsoft Internet Password Breaker. A single click exports user's account credentials, while another click creates a filtered dictionary that can be readily used with Elcomsoft Distributed Password Recovery for breaking encrypted files and documents.

Password protection in Adobe PDF. Advanced PDF Password Recovery.

We'll talk about PDF protection and learn how to break it.

Lab: PDF files. Remove restrictions and break passwords.

Human factor in password protection. Facts and statistics.

The human factor is very important for successful decryption. We'll talk about password reuse and the common methods users employ to make their passwords pass the requirements imposed by today's Web services and corporate security policies. We'll also teach how to use security leaks to attack passwords.

Encryption in crypto-containers. Forensic analysis with Elcomsoft Forensic Disk Decryptor.

Lab: Using Elcomsoft Forensic Disk Decryptor to get access to crypto-containers

Hardware acceleration for password recovery. Using Cloud services.

Computer from crime scene. Common approaches and forensic data acquisition.

Lab: Computer from the crime scene. Forensic analysis and data extraction.
EFDD, MS Office, EINPB, APDFPR

Apple iTunes backups. Decryption and forensic analysis.

Elcomsoft Distributed Password Recovery: Program architecture, setting up server and agents.

Elcomsoft Distributed Password Recovery: supported file formats, speed of password recovery, using GPU acceleration.

Lab: Working with with Elcomsoft Distributed Password Recovery. Configuring server and agents. Using Elcomsoft Hash Extractor. Breaking simple passwords.

Elcomsoft Distributed Password Recovery: Attacks based on human factor. Using mutations and masks.

Elcomsoft Distributed Password Recovery: Hybrid attack

Lab: Using advanced attacks to break passwords.

Using Elcomsoft Phone Breaker and Elcomsoft Distributed Password Recovery to break iTunes password

Demonstration and hands-on experience with two forensic tools.

Elcomsoft Phone Viewer. Exploring iTunes backup data.

Lab: Exploring iTunes Backup.

Windows secrets and passwords. Using Elcomsoft System Recovery and Proactive System Password Recovery.

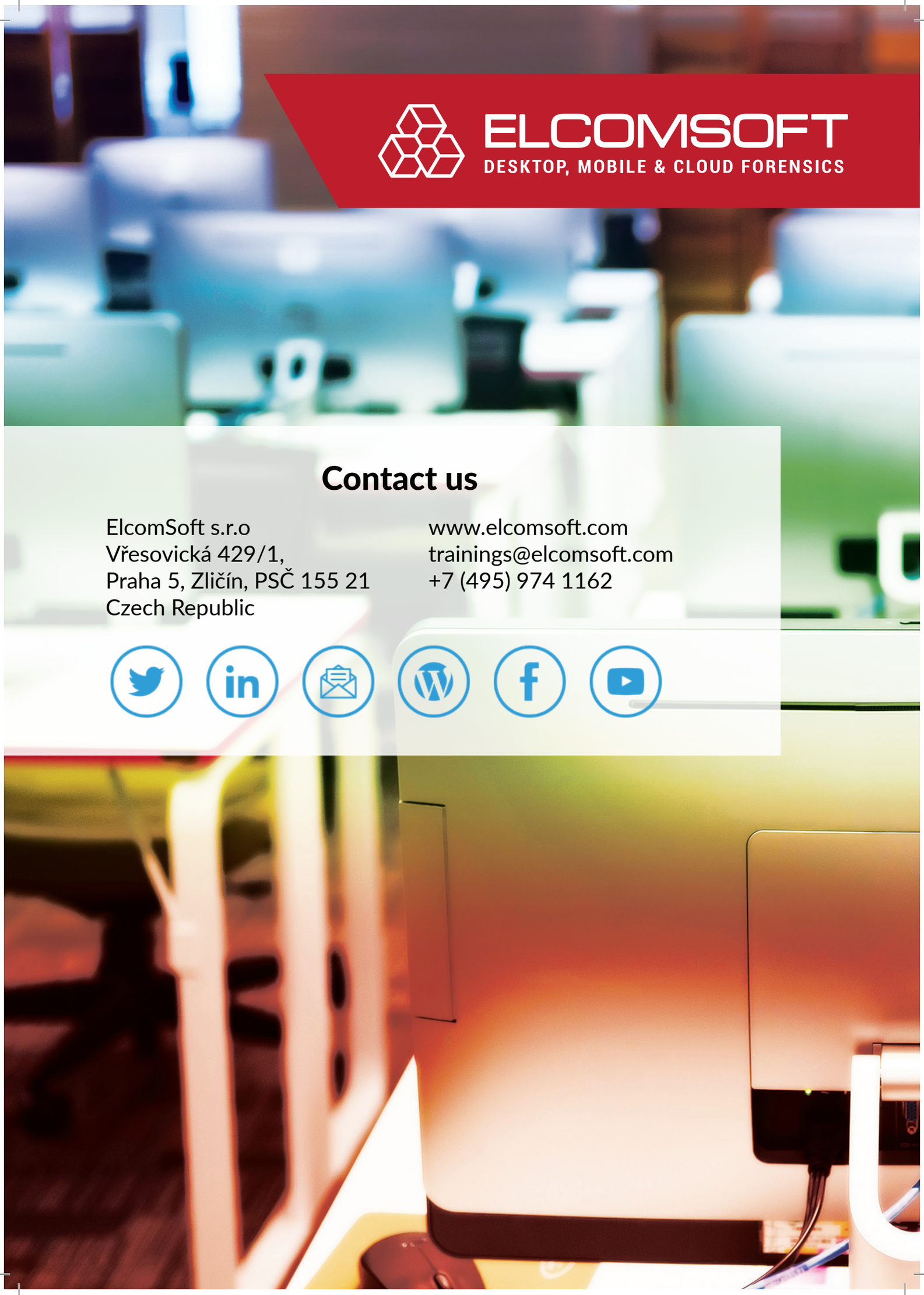
Lab: Breaking into suspect's computer. Using ESR, EFDD and EDPR. Data extraction and analysis.

Microsoft Encrypted File System (EFS). Advanced EFS Data Recovery.

Lab: Breaking into EFS, decrypting files.

Elcomsoft Distributed Password Recovery: Advanced Technics

Lab: Elcomsoft Distributed Password Recovery. Breaking passwords in reasonable timeframe.



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