Computer Forensics:
Software and Technologies: Password Cracking and Encrypted Data Access, Mobile Forensics, Cloud Forensics
ElcomSoft

Who we are

- Privately held company, established in 1990
- 100% in-house research and development
- Offices in Moscow and Prague
- Over 300 partners and resellers on all continents
- Events and trainings in multiple countries
- Six US patents (including GPU acceleration)
- Corporate, government, military and forensic customers
- Over 400,000 installations worldwide
Endorsements and Certifications

**IT Industry**

- Microsoft Partner: Gold Application Development
- Intel Premier Elite Partner
- Member of NVIDIA's CUDA/GPU Computing Registered Developer Program
- Member of several forensic organizations worldwide
- Quotes and references: Microsoft Encyclopedia of Security, The art of deception (Kevin Mitnick), IT Auditing (Chris Davis), Hacking exposed (Stuart McClure), Hacking For Dummies (Kevin Beaver), Computer Network Security: Theory and Practice (We Wang), Investigating Digital Crime (Robin P Bryant), Security Engineering (Ross J. Anderson), Network Know-How: An Essential Guide for the Accidental Admin (John Ross)
Our Customers

Government and Law Enforcement
Our Customers

IT and Commercial

SONY  KPMG  orange  Adobe  Intel
IBM  Bank of America  AT&T
CISCO  Deutsche Bank  RBC  Royal Bank
BOEING  Microsoft  Volkswagen
pwc  citibank  AIRBUS  Deloitte
Achievements

Timeline

- **2007**: Found a government backdoor in Quicken (http://www.theregister.co.uk/2007/06/23/quicken_password_backdoor/)
- **2008**: Guaranteed near-instant cracking PDF & Word (http://www.prweb.com/releases/thunder/tables/prweb1324054.htm)
- **2010**: iOS encryption cracked, first on the market (http://www.pcworld.com/article/202629/article.html)
- **2011**: BlackBerry password recovery, first and only (https://blog.elcomsoft.com/2011/09/recovering-blackberry-device-passwords/)
Achievements

Timeline

- **2014**: Decrypt BlackBerry 10 backups, again first (https://blog.elcomsoft.com/2014/05/phone-password-breaker-3/#bb10)
- **2016**: Recover deleted iCloud photos (https://blog.elcomsoft.com/2016/08/icloud-photo-library-all-your-photos-are-belong-to-us/)
- **2016**: Instant access to call logs and real-time iCloud data (https://blog.elcomsoft.com/2016/11/iphone-user-your-calls-go-to-icloud/)
- **2017**: Extract passwords and CC data from iCloud
- **2018**: Extract & decrypt Apple Health data from iCloud
- **2019**: Extract full file system & keychain from iOS 12 devices
ElcomSoft Forensic Solutions

**DESKTOP FORENSICS**
- GPU Acceleration
- Distributed Computing
- Rainbow Tables
- Breaking Passwords

**MOBILE FORENSICS**
- Physical Acquisition
- Logical Acquisition
- Cloud Extraction
- Real-Time Tracking
GPU Acceleration

Hardware-Accelerated Distributed Desktop Forensics

- Break passwords to hundreds formats faster
  - GPU acceleration (~50-200 times faster than CPU), patented
  - Thunder tables (instantly breaks legacy 40-bit encryption: Word, Excel, PDF)
  - Distributed recovery in LAN, WAN, on Amazon EC2 and Microsoft Azure

- Several ways to break into encrypted volumes (including instant unlock)
  - BitLocker, FileVault 2, PGP, TrueCrypt, VeraCrypt

- Advanced attacks
  - Instant decryption or recovery for many formats
  - Smart attacks using dictionaries, wordlists, mutations and masks
GPU Acceleration

**Benchmarks**

![Benchmarks Graph](NVIDIA GeForce GTX 1080)

- iOS 10.2+ iTunes Backup
- Bitlocker
- Microsoft Office 2013/2019
- TrueCrypt
- Apple FileVault
- 7Zip
- RAR 3-4
- RAR 5
- MS Office 2010

<table>
<thead>
<tr>
<th>Software</th>
<th>Passwords/sec</th>
</tr>
</thead>
<tbody>
<tr>
<td>iOS 10.2+ iTunes Backup</td>
<td>Low</td>
</tr>
<tr>
<td>Bitlocker</td>
<td>Very Low</td>
</tr>
<tr>
<td>Microsoft Office 2013/2019</td>
<td>Low</td>
</tr>
<tr>
<td>TrueCrypt</td>
<td>Low</td>
</tr>
<tr>
<td>Apple FileVault</td>
<td>Low</td>
</tr>
<tr>
<td>7Zip</td>
<td>Medium</td>
</tr>
<tr>
<td>RAR 3-4</td>
<td>High</td>
</tr>
<tr>
<td>RAR 5</td>
<td>Very High</td>
</tr>
<tr>
<td>MS Office 2010</td>
<td>Highest</td>
</tr>
</tbody>
</table>
Crypto Containers

Instant Unlock of Encrypted Volumes

- Break into all major crypto containers without brute forcing the password
- Encrypted volumes and full-disk encryption
- BitLocker, PGP, TrueCrypt, VeraCrypt, FileVault2
- Get encryption/recovery keys from memory, hibernation file, Active Directory, cloud
- Mounts encrypted volumes as drive letters
- Decrypts encrypted content
Some passwords can be recovered instantly or very quickly

- Extract passwords and autocomplete forms from all popular browsers
- Microsoft IE & Edge, Google Chrome, Mozilla Firefox, Opera
- POP3/IMAP/SMTP/NNTP passwords in MS Outlook, Outlook Express, Windows Mail and Live Mail, Thunderbird
- Passwords saved for over 80 instant messengers
- View individual passwords or export everything into text file
- Dozens applications use weak encryption so allowing instant recovery
- Build a custom dictionary and attack strong passwords to other files and documents
Smartphone usage over the world

- Apple: 1.4 billion active (January 2019)
  - theverge.com/2019/1/29/18202736/apple-devices-ios-earnings-q1-2019
- Google: 2.5 billion active Android devices (May 2019)
- 33% of the world population have a smartphone (stats include small children)

**DEVICES**

- Apple: 61%
- Google: 39%

**USERS**

- Have smartphone: 67%
- Don't have: 33%
Mobile Forensics

Apple iOS, Google and Microsoft

- Logical, physical and cloud extraction
- File system acquisition of Apple iOS devices
- Advanced logical extraction
- Access locked iOS devices
- Extraction from Google accounts
- Microsoft accounts: web browsing data, Skype
- Complete support for two-factor authentication
- Tools for viewing and analyzing extracted evidence
Mobile Forensics

iOS file system acquisition

- Captures iOS devices file system image
  - Downloaded mail and messages
  - Chats, including protected and private
  - Temporary files and cache
  - Private app data, system databases, logs, temp files
- Full access to private application data, system databases, logs, temp files etc
- Comprehensive location data from multiple sources
- Now possible without jailbreaking - for all phones up to iPhone X
- For newer devices, directly through known exploits
- Device secrets (iOS keychain)
  - User passwords
  - Encryption keys, authentication tokens
Advanced logical extraction for iOS

- Logical acquisition is more than an iTunes backup
- Extract backups, media files, crash logs and shared files
- Decrypt user passwords (iOS keychain)
- Break unknown passwords to iTunes backups
- Shared files accessible via a yet another dedicated mechanism; may contain valuable information, e.g. password databases (for third-party password managers)
- Crash logs may give insight into what was installed on the device (in the past) and build a timeline
- Cannot be password-protected; always accessible if the device can be paired
- Media files (photos and videos) available through a separate mechanism; may include info on deleted media files
- Unlike backups, media cannot be password-protected
- Sometimes possible even for locked devices (using lockdown/pairing records)
Advanced logical: backups

- A comprehensive solution to extract everything available without a jailbreak

- iTunes backups
  - Data for apps allowed to back up, including photos
  - User passwords, but no other secrets
  - Password-protected backups have advantages
  - Unknown passwords are a huge disadvantage
  - Backup password can be reset with passcode
  - We have tools to attack unknown backup passwords
  - Extract and decrypt the keychain: passwords, tokens and much more
Cloud data: not just smartphones

Apple iCloud
- Apple smartphones and tablets
- Mac computers

Google cloud
- Android devices
- Computers with Google Chrome or Google Drive
- Any smartphone with Google Chrome or Google Maps

Desktops with iCloud for Windows
Cloud forensics

Apple iCloud contains a lot of valuable evidence

- iOS device backups: 2 snapshots of each device
- Synchronized data
- **Passwords and tokens**
- File/document storage
- Data from all devices connected to the account (iPhones, iPads, Apple TV, Apple Watch, Apple Home accessories, desktops running Windows or macOS)
- Most data updated in real time (over W-Fi or mobile data)
- May contain data already deleted from devices
- Protected with password, second factor and additional security measures
Synced data vs backups

- **Real-time synchronization**, data appears in the cloud in minutes
- Backups are huge, difficult to access, contain a lot of useless information
- Backups are often disabled; sync is enabled by default
- Deleted data is often available from both sources
- **Apple detects backup downloads by third-party apps and may lock accounts**
- Some types of synced data not included in iCloud backups if sync is enabled:
  - Photos (if iCloud Photo Library is enabled)
  - Text messages and iMessages (iOS 11.4 and newer, if synced)
  - Health & Home: not in iCloud backups (regardless the settings)
iCloud Keychain

- Synchronized over all connected devices
- Requires Two-Factor Authentication and device passcode
- Contains:
  - Apple IDs with passwords
  - Wi-Fi passwords
  - E-Mail account passwords
  - Passwords stored in Safari
  - Credit cards (no CVC/CVV)
  - Authentication tokens (e.g. for social networks)
  - FileVault2 recovery token (may help to unlock desktop)
Apple Health and Cloud

- Apple Health stores a plethora of evidence
- Health data such as heart rate measurements, walking and running activities helped solve hundreds of crimes
  - Including several murders
- Apple Watch is NOT required for Apple Health to work; steps, floors climbed are counted using iPhone hardware (dedicated low-power co-processor)
  - Native Apple Health data is synced with iCloud to all registered devices
  - Third-party app data contribute even more data but sometimes do not share some with Apple Health, but use proprietary cloud sync (Strava, Endomondo)
- Apple Health data can be obtained from iCloud
- May contain significantly more information compared to what is available on device
- Technically, Apple Health belongs to “synced data” as opposed to “cloud backups”
  - Since iOS 12, Health is additionally encrypted
  - Apple won’t provide Health data to LE through government requests
  - Our software can download and decrypt it
Apple Screen Time

- Comprehensive usage statistics (incl. Safari history)
- Usage restrictions remotely enforceable
- Collected from all devices sharing the same Apple ID
  + from child accounts
- iCloud sync requires Two-Factor Authentication
- Screen Time data is additionally protected
- Passcode or system password required to access Screen Time data
- Screen Time password is stored in the iCloud, and we can extract it
Google account forensics

- Google is not equal to Android
- Data is collected and synced across multiple devices and sources: smartphones (Android and iOS), tablets, desktops (Windows and macOS)
- Devices backups do not contain valuable information; most data is synced
- Full Google Chrome data is being saved
- Location is almost always tracked and saved forever
- All passwords used in Google Chrome are saved and so accessible
- Complete statistics on device and app usage is collected
Cloud Forensics: Conclusion

- Apple and Google collects as much data as possible (and increasing)
- Most data synchronized in real-time, sometimes once a day
- 2FA is used to secure cloud access
- Apple has additional protection (device passcode required to access passwords, Health, Screen Time, Messages)
- Always collect passwords and token from desktops even if you are investigating the smartphone only
- Cloud data provided by Apple to LE is limited; our software can extract more information
- Cloud acquisition can help access data from multiple devices (including locked or damaged)
- Cloud credentials can be collected from desktop computer, another smartphone or tablet
Download snapshot

Select data categories to download

- User Info
- Dashboard
- Chats
- Contacts
- Google Keep
- Chrome
- Calendars
- Locations
- Media (0 files)
- History
- Calls
- Wi-Fi
- Mail (73965 mails)

Selected token allows extracting only a limited set of data categories. To get the ones disabled here, use the password authentication.

[Check All] [Uncheck All]

[Cancel] [Download]
Cloud Forensics: Credentials

- Passwords saved in desktop and mobile browsers
- Passwords re-use (human factor issue)
- An ability to reset password and replace second factor right from passcode-protected device
- An ability to reset password through email
- Authentication tokens saved on device or desktop (Windows & macOS X)
- Social engineering attacks
- Keyloggers and malware (used by GCHQ and similar agencies)
- Access via IoT devices
- Legal access (for serious crime cases)
Computer, Mobile & Cloud Forensics

(c) Vladimir Katalov
ElcomSoft Co. Ltd

http://www.elcomsoft.com
http://blog.crackpassword.com

Facebook: ElcomSoft
Twitter: @elcomsoft

© ElcomSoft Co. Ltd.