

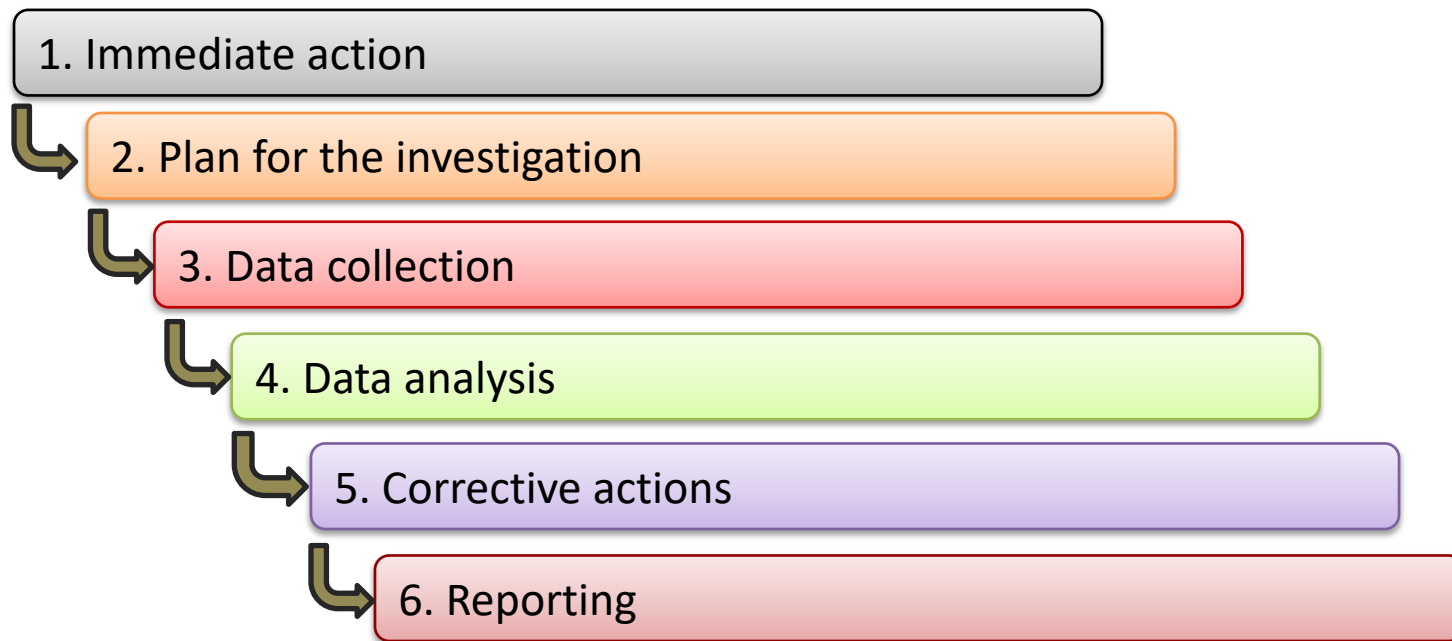
2018, Prague



Methods of accessing encrypted data for further forensics analysis

Six steps for successful incident investigation

Six steps for successful incident investigation



Six steps for successful incident investigation

Six steps for successful incident investigation

Step 1. Immediate action

In the event of an incident, immediate action to be taken may include making the area safe, preserving the scene and notifying relevant parties.

The investigation begins even at this early stage, by collecting perishable evidence, e.g. **computers, laptops, hard disks, smartphones, flash drives... etc.**

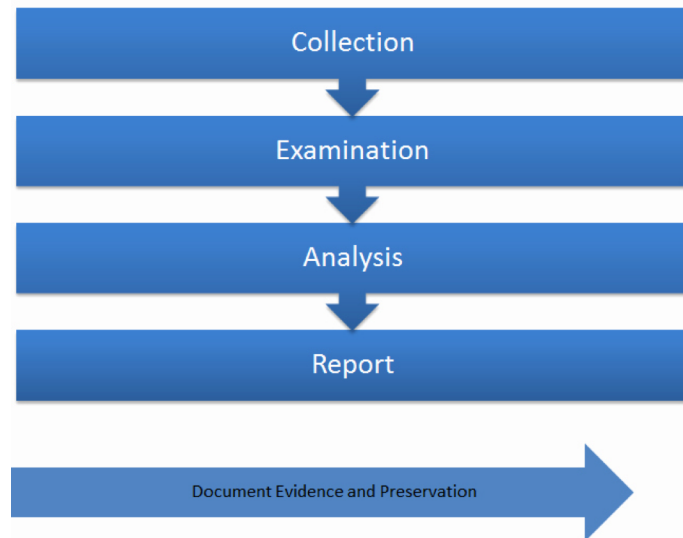


Six steps for successful incident investigation

Step 2. Plan the investigation

Planning ensures that the investigation is systematic and complete. What resources will be required? Who will be involved? How long will the investigation take?

For severe or complex incidents, an investigation team will be more effective than a single investigator.

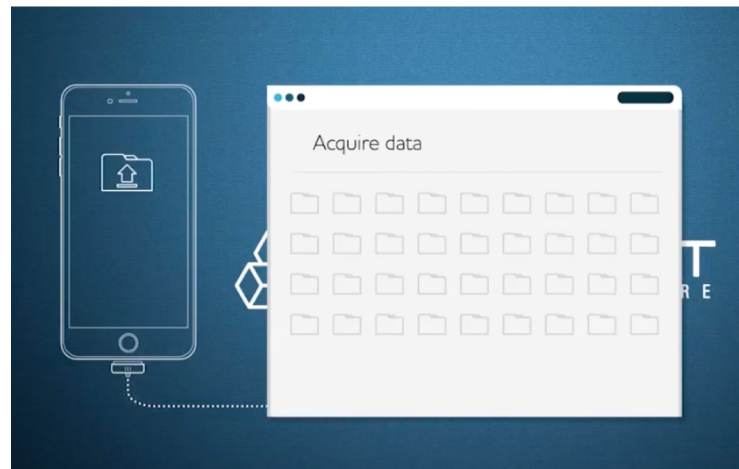


Six steps for successful incident investigation

Step 3. Data collection

Information about the incident is available from numerous sources, not only people involved or witnesses to the event, but also from equipment, documents and the scene of the incident.

Elcomsoft solutions are focused on this step.

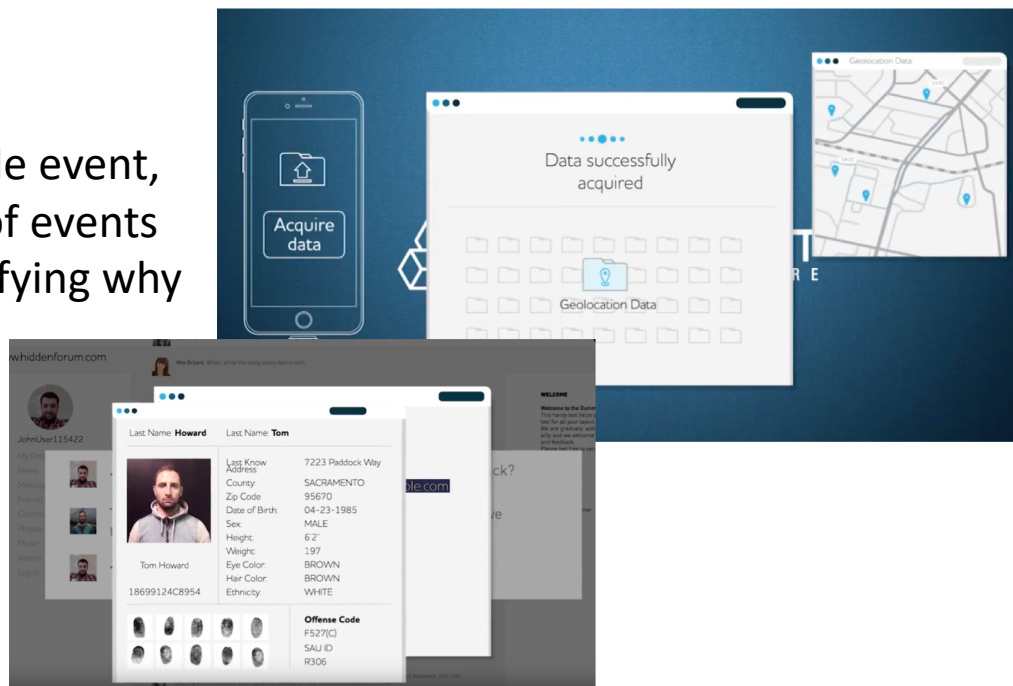


Six steps for successful incident investigation

Six steps for successful incident investigation

Step 4. Data analysis

Typically, an incident is not just a single event, but a chain of events. The sequence of events needs to be understood before identifying why and how the incident happened.



Six steps for successful incident investigation

Step 5. Corrective actions

An investigator or team who believe that incidents are caused by unsafe conditions will likely try to uncover conditions as causes. On the other hand, one who believes they are caused by unsafe acts will attempt to find the human errors that are causes. Therefore, it is necessary to examine all underlying factors in a chain of events that ends in an incident.



Six steps for successful incident investigation

Step 6. Reporting

In addition to fully documenting information related to hardware and software specs, computer forensic investigators must keep an accurate record of all activity related to the investigation, including all methods used for testing system functionality and retrieving, copying, and storing data, as well as all actions taken to acquire, examine and assess evidence.

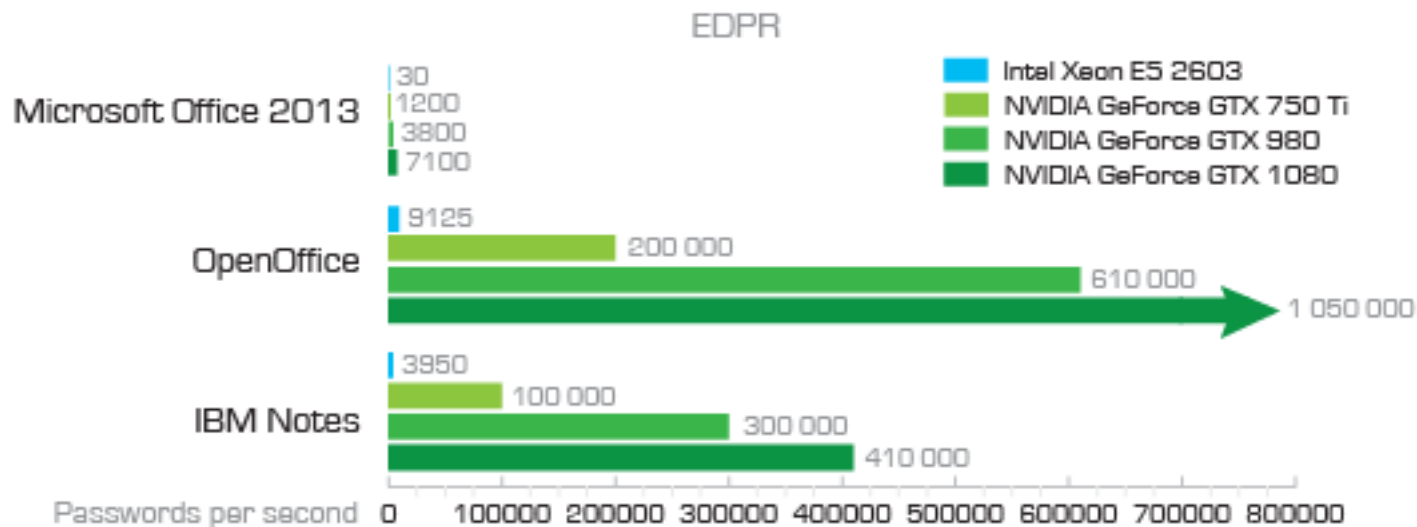


Data collection

Types of encrypted data sources

- Documents (MS Office, Open Office, IBM Notes, Adobe PDF...)
- File archives (7zip, ZIP, PKZip, WinZip, RAR, ARJ, ACE...)
- Crypto containers (TrueCrypt, VeraCrypt, MS Bitlocker, PGP...)
- Smart devices backups
- Smartphones, tablets hardware (Apple, Google, Microsoft, Blackberry)
- Cloud storages (iCloud, Google Cloud, Microsoft...)

CPU is not powerful enough to break modern encryption



Breaking documents password

MS Office 2007 / 2010 / 2013

CPU: Intel Xeon E5-2603

GPU: AMD Radeon R9 290

One instance

	Per second	Per hour
MS Office 2007	46.200	166.320.000
MS Office 2010	24.500	88.200.000
MS Office 2016	2.900	1.044.000

Breaking documents password

MS Office 2007 / 2010 / 2013

CPU: Intel Xeon E5-2603

GPU: AMD Radeon R9 290

10 instances

	Per second	Per hour
MS Office 2007	462.000	1.663.200.000
MS Office 2010	245.000	882.000.000
MS Office 2016	29.000	10.440.000

MS Office 2007 / 2010 / 2013

10 instances

Is it enough to recovery password using brute-force method
in reasonable time?

	Per second	Per hour
MS Office 2007	462.000	1.663.200.000
MS Office 2010	245.000	882.000.000
MS Office 2016	29.000	10.440.000

MS Office 2016

Very simple: 5 characters (lower case letters and numbers only)

$36^5 = 60,466,176$ possible passwords

Max. time: **4.7 hours**

MS Office 2016

Simple: 6 characters (lower and upper case letters and numbers only)

$62^6 = 56,800,235,584$ possible passwords

Max. time: **4500 hours (6 months)**

MS Office 2016

Average: 7 characters (upper and lower case letters and numbers)

$62^7 = 3,521,614,606,208$ possible passwords

Max. time:

MS Office 2016

Average: 7 characters (upper and lower case letters and numbers)

$62^7 = 3,521,614,606,208$ possible passwords

Max. time: **277.292 hours (31.5 years)**

MS Office 2016

Slightly stronger than average: 8 characters (upper and lower case letters, special characters and numbers combined)

$94^8 = 6,095,689,385,410,816$ possible passwords

Max. time: **55.000 years**

There is a catch!

About **60%** of passwords chosen by **AVERAGE** users
can be usually broken **within first two hours*!**

**) 10 instances, using GPU accelerator*

And more!!!

About **30%** of passwords chosen by **AVERAGE** users
can be usually broken **In minutes!!!*)**

**) 10 instances, using GPU accelerator*

MS Office 2016

Average: 7 characters (upper and lower case letters and numbers)

$62^7 = 3,521,614,606,208$ possible passwords

~~277.292 hours (31.5 years)~~ up 2 hours!

Mutations and dictionary attack. Best strategy.

After extensive research and nearly half year of testing, we settled on the following attacks:

- **Top-100 passwords.** This dictionary attack uses the original Top-100 Passwords list including variations (appending up to 2 numbers and trying single-word and two-word combinations).
- **Top-10,000 passwords.** This attack with the dictionary containing top-10,000 passwords including simple variations (one number appended to the end of the password).

Mutations and dictionary attack. Best strategy.

During the test run, we discovered that up to 60% of passwords chosen by average users can be usually broken within the first two hours. We're working on 10.000.000 passwords list also.

Of course, this doesn't mean you will break 6 of every 10 documents. You could break all ten, or none at all.

The 60% success rate only works on a larger scale, and is not a guarantee of any kind.

Elcomsoft Distributed Password Recovery

High-performance distributed password recovery with GPU acceleration and **scalability to over 10,000 workstations** with zero overhead.

Recover the most complex passwords and strong encryption keys in realistic timeframes!

<http://www.elcomsoft.com/edpr.html>



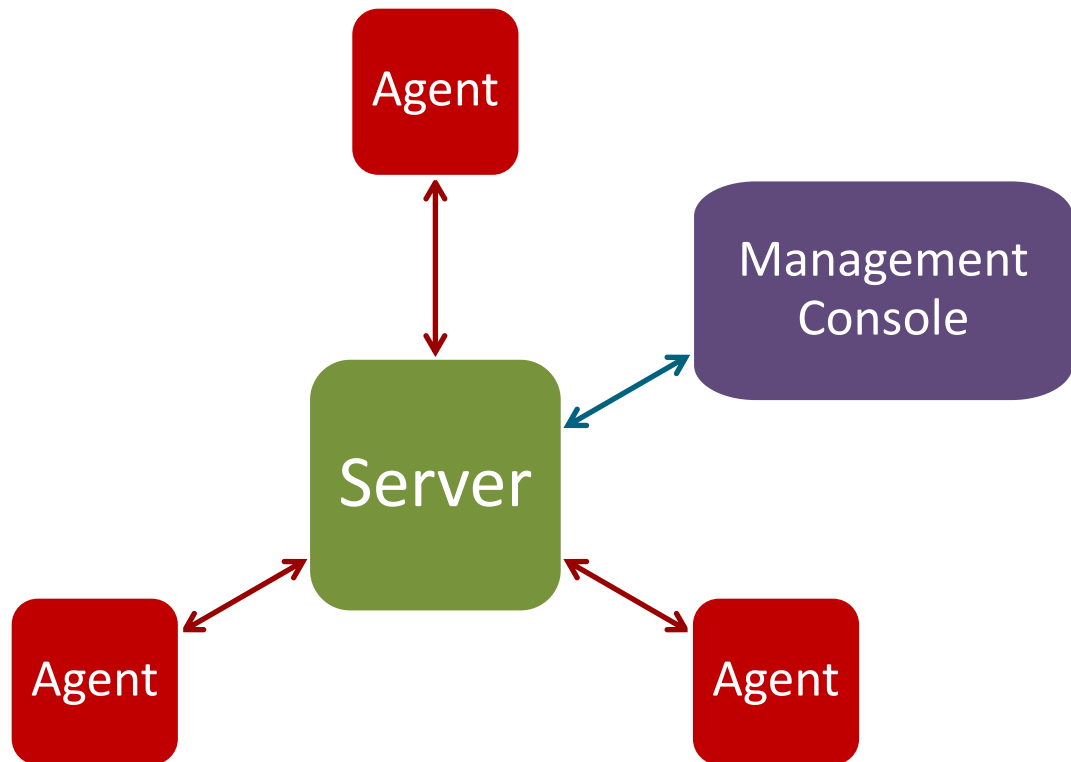
Benefits and features list

- Hardware acceleration (patented) reduces password recovery time by a factor of 50
- Support for NVIDIA CUDA and AMD Radeon cards
- Linear scalability with no overhead allows using up to 10,000 workstations without performance drop-off
- Allows up to 32 CPUs or CPU cores and up to 8 GPUs per processing node
- Distributed password recovery over LAN, Internet or both
- Console management for flexible control from any networked PC
- Schedule support for flexible load balancing



How it works?

ElcomSoft Distributed Password Recovery is a program complex that consists of 3 main modules: **the agent, the server and the management console**, that can operate independently on different computers in the local or global Internet networks



The Most Common Crypto-Containers

TrueCrypt (and its successors)

Symantec Encryption/PGP Desktop

Symantec PGP Whole Disk Encryption

Microsoft BitLocker

Apple FileVault



Encrypted containers. Transparent encryption.

Transparent encryption (real-time encryption or **on-the-fly encryption**) is used by some disk encryption software. "Transparent" refers to the fact that data is automatically encrypted or decrypted as it is loaded or saved.

With transparent encryption, the files are accessible immediately after the key is provided, and the entire volume is typically mounted as if it were a physical drive, making the files just as accessible as any unencrypted ones.

The entire file system within the volume is encrypted (including file names, folder names, file contents, and other meta-data).

Unbreakable encryption

Crypto-containers employ the strongest encryption with **no known vulnerabilities**.

- AES 128/256
- Blowfish
- Serpent
- TwoFish
- RSA
- IDEA...

OTFE keys vulnerability by design

Once the **encrypted volume is mounted**, OTFE keys must be presents in PC memory to provide On-The-Fly decryption/encryption functionality



The Cold-Boot Attack

To execute the attack, a running computer is cold-booted. A removable disk is then immediately used to boot a lightweight operating system, which is then used to **dump the contents of pre-boot physical memory to a file.**

Alternatively, the memory modules are removed from the original system and quickly placed in a compatible machine under the attacker's control, which is then booted to access the memory. Further analysis can then be performed against information that was dumped from memory to find various sensitive data, such as the keys contained in it.

Three Ways to Acquire Encryption Keys

- By analyzing the **hibernation file** (if the PC being analyzed is turned off)
- By analyzing a **memory dump** file (if the PC turned on and you have administrative access)
- By performing a **FireWire attack** (if the PC turned on, and it's locked by password)

One more thing... Clouds & Networks!

- **Apple FileVault 2** keys can be found in iCloud Apple keychain
- **Microsoft BitLocker** recovery keys can be found in Microsoft Account online
- **Microsoft BitLocker** recovery keys can be found in ActiveDirectory file

The Weakness of Crypto Containers

The main and only weakness of crypto containers is human factor. Weak passwords aside, encrypted volumes must be mounted for the user to have on-the-fly access to encrypted data.

No one likes typing their long, complex passwords every time they need to read or write a file. As a result, keys used to encrypt and decrypt data that's being written or read from protected volumes are kept readily accessible in the computer's operating memory. Obviously, what's kept readily accessible can be retrieved near instantly by a third-party tool. Such as **Elcomsoft Forensic Disk Decryptor**.

Elcomsoft Forensic Disk Decryptor

Perform the complete forensic analysis of encrypted disks and volumes protected with desktop and portable versions of BitLocker, PGP, TrueCrypt and its successors.

Elcomsoft Forensic Disk Decryptor allows instant access to encrypted data by mounting or decrypting encrypted volumes using decryption keys found in the computer's RAM, memory dumps or hibernation files.

<https://www.elcomsoft.com/efdd.html>



EnCase (.E01) Images

Elcomsoft Forensic Disk Decryptor (2.0 and up) supports **.DMG** and **EnCase** images.

This way you can work with imaged hard drives without the need to access the original physical media.



Smartphones and tablets, what data hiding within?

Actual data!

- Call logs and text messages
- Emails and chats
- Account passwords
- Web and application passwords
- Wi-Fi passwords
- Documents, settings and databases
- Web browsing history
- Pictures and videos
- Geolocation history, routes and places



Seizing and Preserving Evidence

- Use Faraday bag; Connect to a charger
- Isolates from wireless networks
- **Otherwise, remote wipe easily possible**

Cambridgeshire, Derbyshire, Nottingham, and Durham police: *"don't know how people wiped them."* (9.Oct.14)

Darvel Walker, Morristown wiped his iPhone remotely, charged with tampering with evidence (7.Apr.15)



Data Acquisition

Logical Acquisition (Backups)

- Apple Backup can be encrypted with unknown password. Slow (100 p/s w/GPU); recovery timeframe unpredictable, result not guaranteed

Over-the-Air (Cloud) Extraction

- User ID/password or binary authentication token.
- Can be obtained from Apple/Google with court order

Physical Acquisition

- On recent devices, must unlock/know the passcode
- Jailbreak required, multiple issues arise
- USB restricted mode (begin from iOS 11.4.1) may be a problem

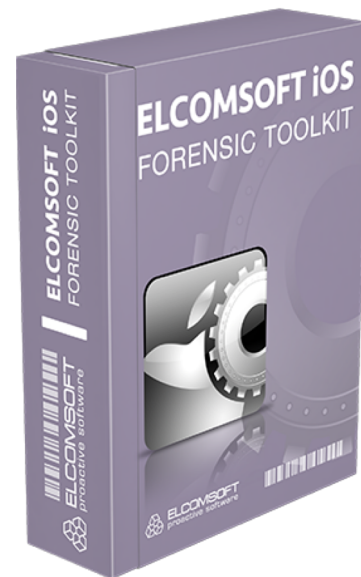
Physical Acquisition: benefits

- **Acquires complete, bit-precise device images**
- **Unallocated space is extracted** (*but cannot be decrypted on recent versions of iOS*)
- **32-bit:** Decrypts keychain items, extracts device keys
- **Guaranteed timeframe:** 20 to 50 minutes for 32 GB models
- **Passcode bypassed** for older devices or if jailbreak is installed
- **32-bit:** Simple 4-digit passcodes recovered in 10-40 minutes (for jailbroken devices)



Physical Acquisition: Elcomsoft iOS Forensic Toolkit

- Physical acquisition for 64-bit iOS devices via jailbreak
- Logical acquisition extracts backups, crash logs, media and shared files
- Extracts and decrypts protected keychain items
- Real-time file system acquisition
- Automatically disables screen lock for smooth, uninterrupted acquisition
- **Unlocks iOS devices with pairing records**



Physical Acquisition: limitations

- Difficult, not guaranteed, not forensically sound
- Permanently modifies system and user partitions
- Limited on 64-bit devices
- Must remove (and know) the passcode
- No keychain on 64-bit devices
 - Use local backup w/password



Logical acquisition: backups (iOS)

Acquisition steps:

- Make the device produce a backup or
- Access information stored in existing backup

Limitations:

- Device must be unlocked (with passcode, Touch ID, iTunes or lockdown file)
- iOS 11 or greater requires a passcode to pair
- May produce encrypted backup
- Limited amount of information



What If backup encrypted by password?

- All encryption is **performed inside the device** (iPhone, iPad)
- Encryption keys are stored in device
- iTunes pulls encrypted data stream
- **No way to intercept plain data since there is none**
- If you don't know the password, there is no way to reset or remove it
 - But can still access device info including Serial Number



What If backup encrypted by password?

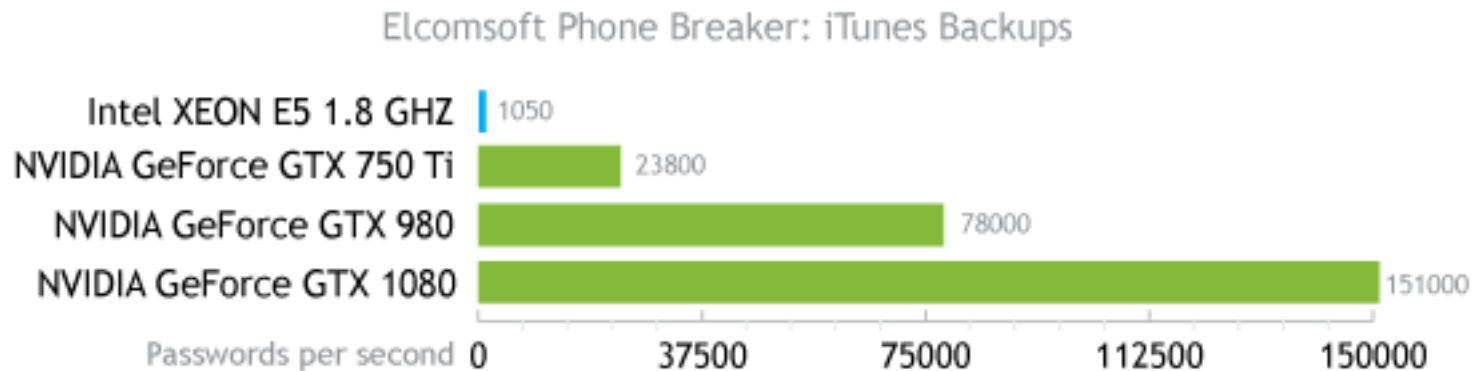
Elcomsoft Phone Breaker

Elcomsoft Phone Breaker **enables forensic access to password-protected backups** for smartphones and portable devices based on RIM BlackBerry and Apple iOS platforms.

The password recovery tool supports all Blackberry smartphones as well as Apple devices running iOS including iPhone, iPad and iPod Touch devices of all generations released to date, including the iPhone 8/Plus, iPhone X and iOS 11

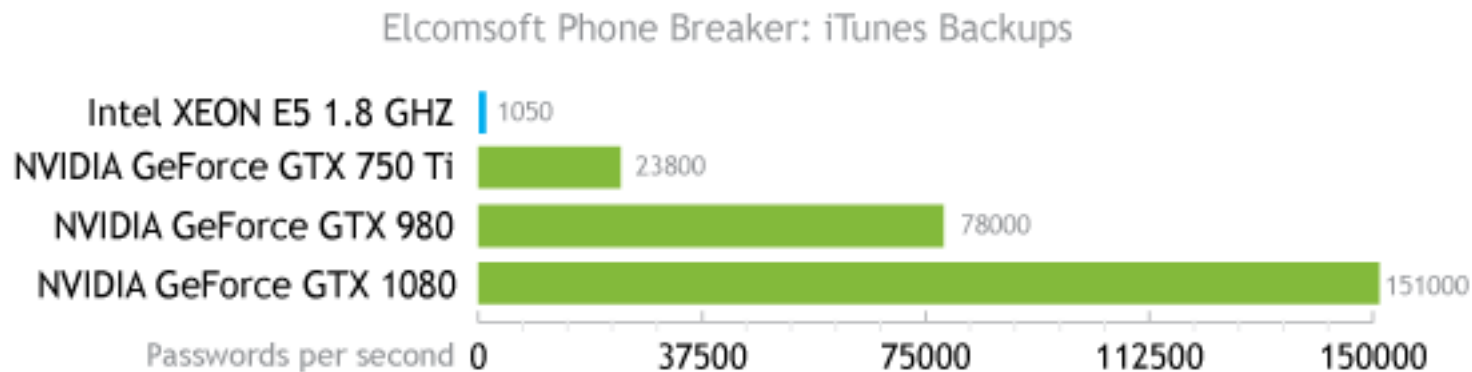


Logical acquisition: GPU is required!



iOS 9: 1050 combinations per second with CPU; 151,000 with GTX 1080

Logical acquisition: GPU is required!



iOS 9: 1050 combinations per second with CPU; 151,000 with GTX 1080

* *iOS 10, iOS 11: extremely slow at 100 p/s with GTX 1080 GPU*

Over-the-Air Acquisition

Cloud Acquisition: Why?

- Helps dealing with locked and encrypted devices
 - Android 6 and up encrypted by default
 - iOS device can be inaccessible for forensics analysis
- Cloud data can contain more data than the phone itself
- Last resort: may succeed where all other methods fail
- Google and Apple collect information from all signed-in devices



Over-the-Air Acquisition: iCloud (Apple)

You have to know before begin:

- May be sporadic
- Fresh backup may not be available
- *San-Bernardino case*: last backup several months old



Over-the-Air Acquisition: iCloud (Apple)

OTA requirements:

- Apple ID/password or ...
- Binary authentication token or ...
- Can be obtained directly from Apple with court order



Over-the-Air Acquisition: iCloud (Apple)

Apple ID/Password facts:

- If you know the password to user's Apple ID, perform cloud acquisition first
- If you don't, **DO NOT RESET APPLE ID PASSWORD EVEN IF YOU CAN**
- Otherwise, you won't be able to make the phone produce a fresh cloud backup without unlocking it first

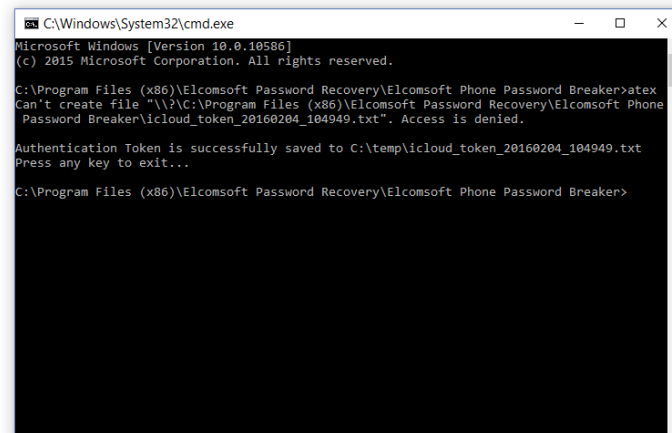
- What can happen:

San-Bernardino case: *password reset, iCloud backup impossible even with Apple cooperation*

Over-the-Air Acquisition: iCloud (Apple)

Binary authentication token:

- If you are able to extract binary token, Apple ID/Password does not need to get access into iCloud data
- Bypass two-factor authentication
- iOS 8.x: iCloud; tokens have limited lifespan
- iOS 9.x: iCloud Drive; tokens do not expire



```
CA\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\Elcomsoft Password Recovery\Elcomsoft Phone Password Breaker>atex
Can't create file "\\?\C:\Program Files (x86)\Elcomsoft Password Recovery\Elcomsoft Phone Password Breaker\icloud_token_20160204_104949.txt". Access is denied.

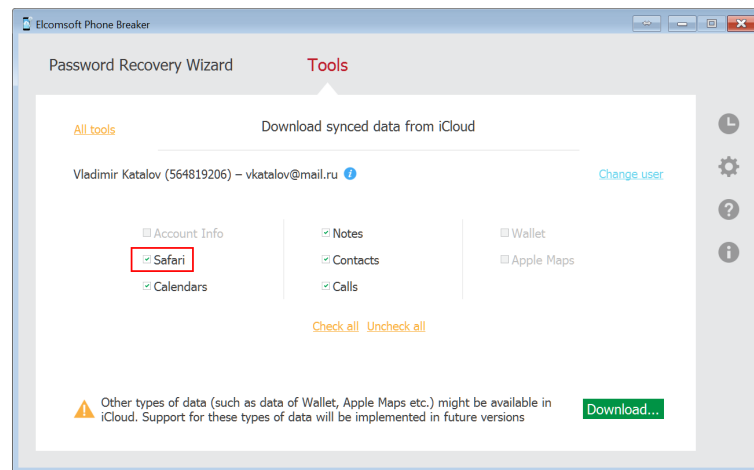
Authentication Token is successfully saved to C:\temp\icloud_token_20160204_104949.txt
Press any key to exit...

C:\Program Files (x86)\Elcomsoft Password Recovery\Elcomsoft Phone Password Breaker>
```


Over-the-Air Acquisition: iCloud (Apple)

iCloud Synchronized Data

- Some types of data are synced across iOS devices
- Sync is real-time or near real-time
- Independent of iOS cloud backups
- Independent of Continuity



Over-the-Air Acquisition: iCloud (Apple)

iCloud Synchronized Data:

- If Settings | iCloud | Safari is enabled, it syncs:
 - Call logs, Bookmarks, Open tabs, Reading list, Browsing history
- Contacts, Notes, Calendars, Wallet (including boarding passes), Maps (searches and bookmarks)
- **Text messages, Health data**
- **iCloud Keychain**
 - With luck, **password to Google Account**

Over-the-Air Acquisition: iCloud (Apple)

iCloud KeyChain:

- Passwords, credit card data, authentication tokens are synced across trusted iOS devices
- Acquisition non-trivial
- Different mechanisms with and without 2FA
 - iCloud Security Code (if no 2FA)
 - Device passcode (if 2FA enabled)
 - SMS verification code (if 2FA enabled)

Over-the-Air Acquisition: iCloud (Apple)

Roadblock: Two-Factor Authentication

- Protects access to backup data, keychain
- Verification code sent to trusted device
- If enabled, 2FA is enforced for iCloud backups - *but not files sideloaded to iCloud Drive*
- Overcoming 2FA is easy - *if the second authentication factor is available*

Alternatives:

- Recovery key or Authentication binary token



Two-step verification has been enabled for your Apple ID.

Over-the-Air Acquisition: iCloud (Apple)

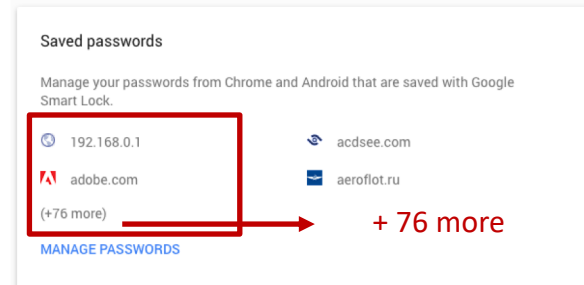
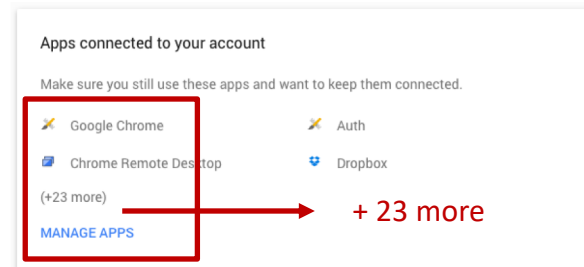
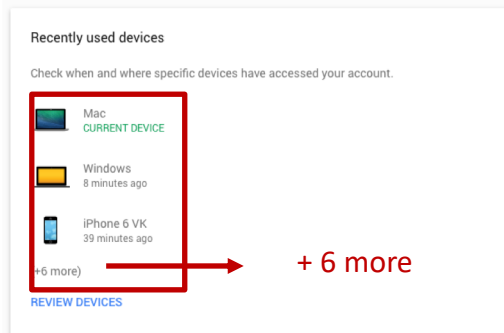
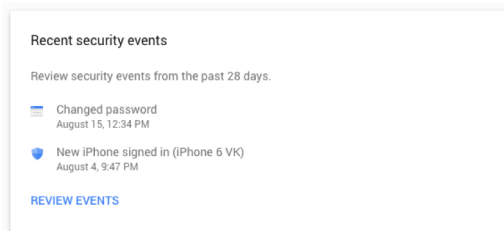
Elcomsoft Phone Breaker

- Download iCloud backups and synced data with or without Apple ID password
- Decrypt iCloud Keychain and iMessages from iCloud
- Download files stored in the user's iCloud account such as documents or third-party application data (such as WhatsApp own backups, 1Password database, Passbook/Wallet data etc.), and more
- Supports Two-Step Verification and Two-Factor Authentication



Google Collects Data from Multiple Sources

- **Multiple devices**
 - Mac
 - Windows
 - iPhone
 - iPad
 - ...and Android
- **Apps**
 - Dropbox
 - Chrome
 - Remote desktop
 - Many more



Google: What inside?

- User data
- All connected devices
- Devices/browsers that requested access
- Applications that requested access
- Google ads settings (age, interests etc.)
- Contacts
- Calendars
- Notes
- Mails
- Albums (photos/pictures/videos)
- Hangouts conversations
- Chrome
 - History
 - Synced passwords and autofill data
 - Bookmarks
 - Search history
 - YouTube [search] history
- A lot of statistical information



Google: What inside?

Account

- email
- number of Google API clients (sites and apps)
- account time: personal, work, both
- Activities in last 28 days
 - browsers and OSs that had access
 - locations
 - new apps and sites

YouTube

- number of videos and playlists loaded
- user name
- sex
- last video rating (+video name and date)
- activities for last 28 days
 - number of views, by day
 - total views
 - searches
 - likes and dislikes

Search history (query + date)

- last Web search
- last image search
- last news search
- last video search
- last maps search
- last books search
- activities for last 28 days
 - top 10 searches
 - percentage of searches by category (web, image etc.)
 - activity (by day)

Google Sync. (non-Android devices)

- number of bookmarks
- last sync date
- number of passwords
- number of Chrome extensions

Profile info

- Google+ name
- profile URL
- number of phone numbers
- number of "+1"

Gmail

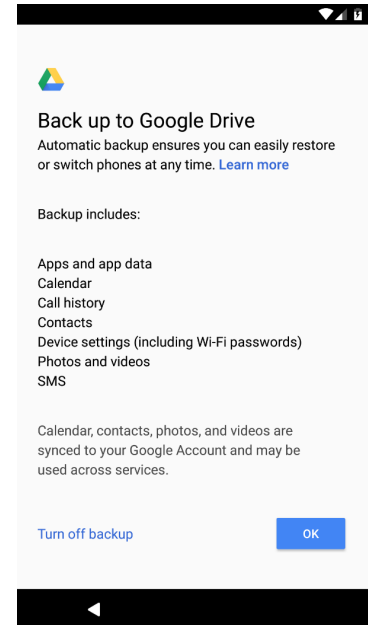
- number of mail threads
- last thread subject
- number of messages in inbox
- last incoming message subject
- number of sent mails
- last sent mail subject

Android

- make, model
- first auth date/time
- last activity date/time
- apps that backup their data (name, date, size)

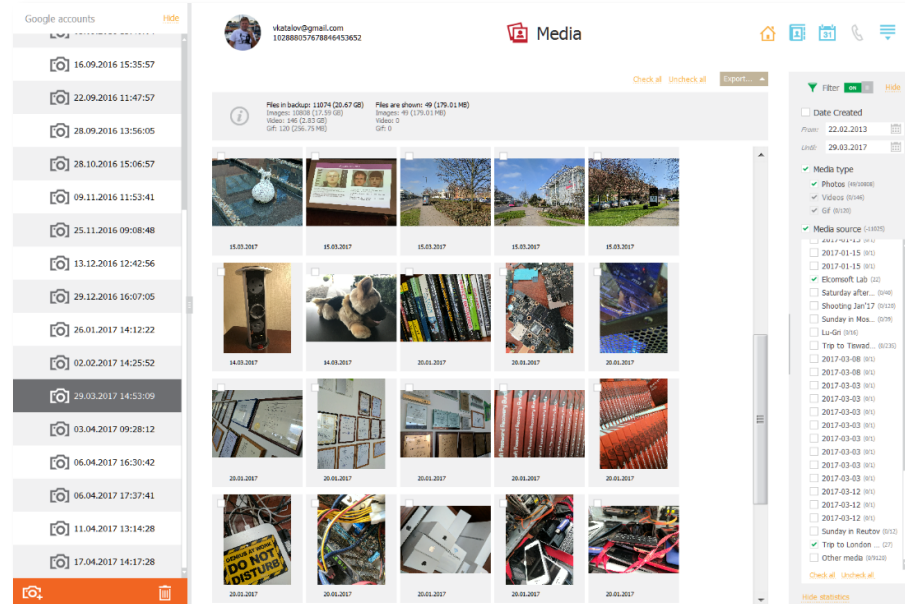
Android Backups

- Google Calendar settings
- Wi-Fi networks & password
- Home screen wallpapers
- Gmail settings
- Apps installed through Google Play
- Display settings
- Language & Input settings
- Date & Time
- 3rd party app settings & data



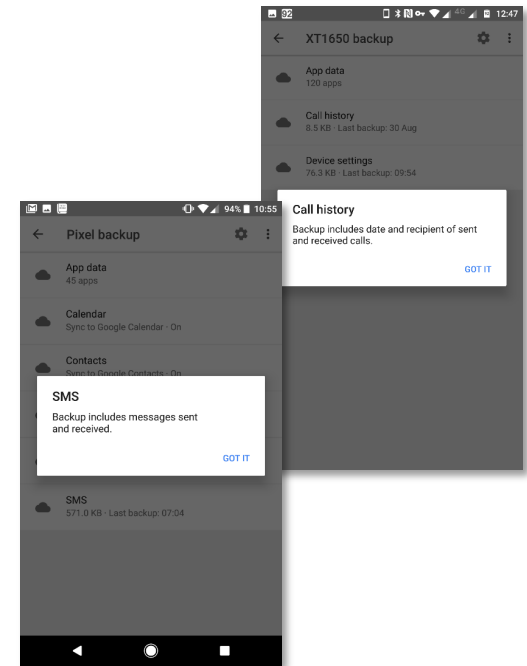
Google Photos

- Albums/events
- Comments
- EXIF
- Geo tags
- Subscriptions
- View counters
- People



Call Logs and Text Messages

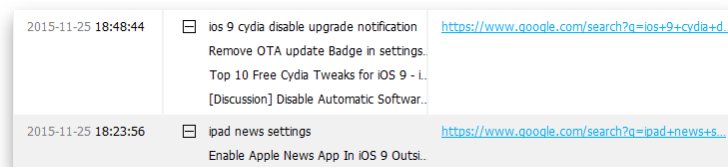
- **Call logs**
 - Android 6 and newer, recent Google Play Services
- **Text messages**
 - All devices: Android 8.0 Oreo
 - Google Pixel and Pixel XL: Android 7.1.1 and newer
- User's Google Account contains call logs and text messages backed up by all compatible devices



Google Chrome: Search & Browsing History

- Collected on all signed-in devices
- **Not just Android**

- Total searches
- Searches by day
- Top search clicks
- Map search history
- Voice search history
- Info on devices
- **Location history**



2015-11-25 18:48:44	<input type="checkbox"/> ios 9 cydia disable upgrade notification Remove OTA update Badge in settings. Top 10 Free Cydia Tweaks for iOS 9 - L [Discussion] Disable Automatic Softwar...	https://www.google.com/search?q=ios+9+cydia+d...
2015-11-25 18:23:56	<input type="checkbox"/> ipad news settings Enable Apple News App In iOS 9 Outsi...	https://www.google.com/search?q=ipad+news+s...

What is saved:

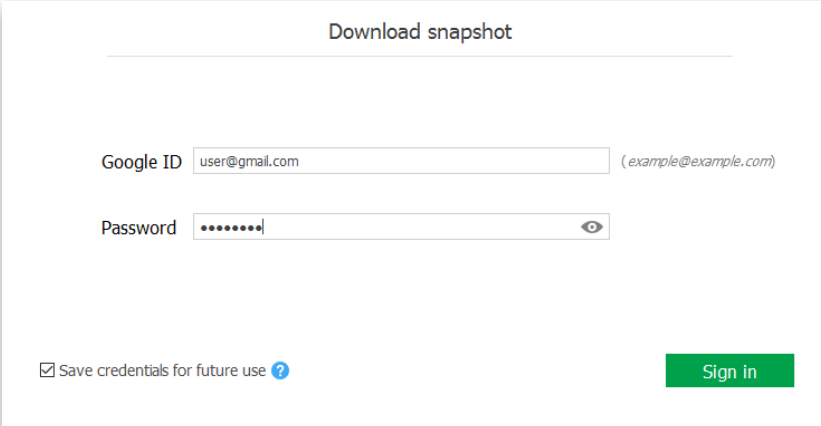
- Searches in all Google services
- Browser or mobile application
- Actions for search results (opened or not)
- Actions on Ads (clicks/purchases)
- IP address
- Browser information

Locations...



Google OTA Acquisition: Requirements

- **User ID / Password or ...**
- **Binary Token**
Is available if Google Chrome is installed on the user's computer, and the user signed in to at least one Google service via the browser.



The screenshot shows a sign-in form with the following elements:

- Title: Download snapshot
- Google ID field: Contains the text "user@gmail.com" and a placeholder "(example@example.com)".
- Password field: Contains a series of dots and a toggle icon (an eye).
- Checkbox: "Save credentials for future use" with a question mark icon.
- Sign in button: A green button with the text "Sign in".

Google OTA Acquisition

Elcomsoft Cloud eXplorer

- Download the complete set of data from Google Account
- Extract significantly more information than available via Google Takeout
- **Authenticate without a password and bypass Two-Factor Authentication**
- Access user passwords, browsing history, contacts, location history, email and much more
- Obtain files and documents from Google Drive



A \$1.000.000 Question:

How to find the Password?

Main rule: most of all passwords are re-usable

The 50 Most Used Passwords

- | | | | | |
|--------------|--------------|----------------|--------------|-------------|
| 1. 123456 | 11. 123123 | 21. mustang | 31. 7777777 | 41. harley |
| 2. password | 12. baseball | 22. 666666 | 32. f*cky*u | 42. zxcvbnm |
| 3. 12345678 | 13. abc123 | 23. qwertyuiop | 33. qazwsx | 43. asdfgh |
| 4. qwerty | 14. football | 24. 123321 | 34. jordan | 44. buster |
| 5. 123456789 | 15. monkey | 25. 1234...890 | 35. jennifer | 45. andrew |
| 6. 12345 | 16. letmein | 26. p*s*y | 36. 123qwe | 46. batman |
| 7. 1234 | 17. shadow | 27. superman | 37. 121212 | 47. soccer |
| 8. 111111 | 18. master | 28. 270 | 38. killer | 48. tigger |
| 9. 1234567 | 19. 696969 | 29. 654321 | 39. trustno1 | 49. charlie |
| 10. dragon | 20. michael | 30. 1qaz2wsx | 40. hunter | 50. robert |

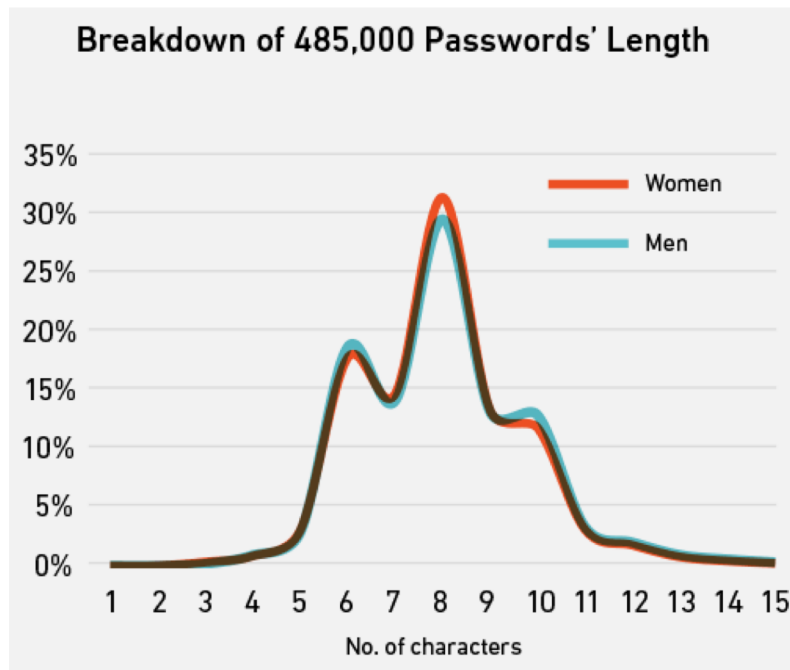
Evaluating Password Entropy

How much symbols is enough to make password secure?

Five, six, seven, maybe ten???

Evaluating Password Entropy

How much symbols is enough to make password secure?



MS Office 2016

8 is enough (>65% of users thinks so).

Slightly stronger than average: 8 characters (upper and lower case letters, special characters and numbers combined)

$94^8 = 6,095,689,385,410,816$ possible passwords

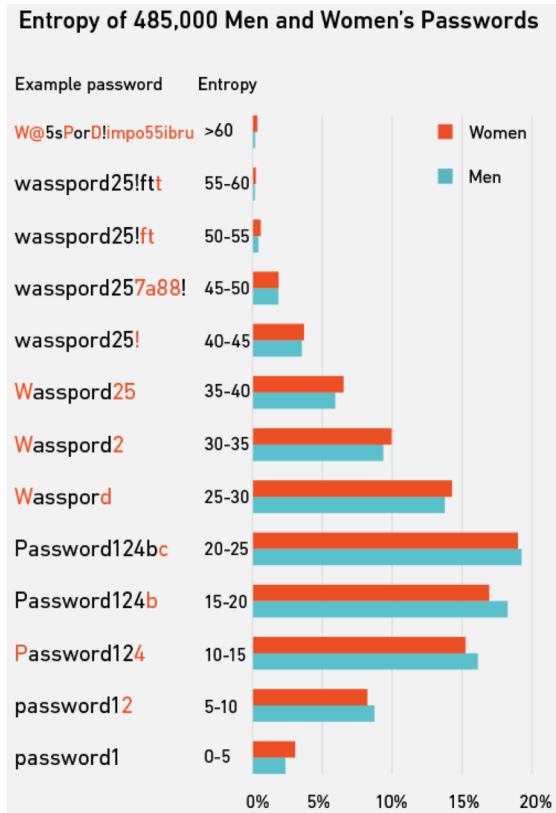
Max. time: **55.000 years**

What users thinks?

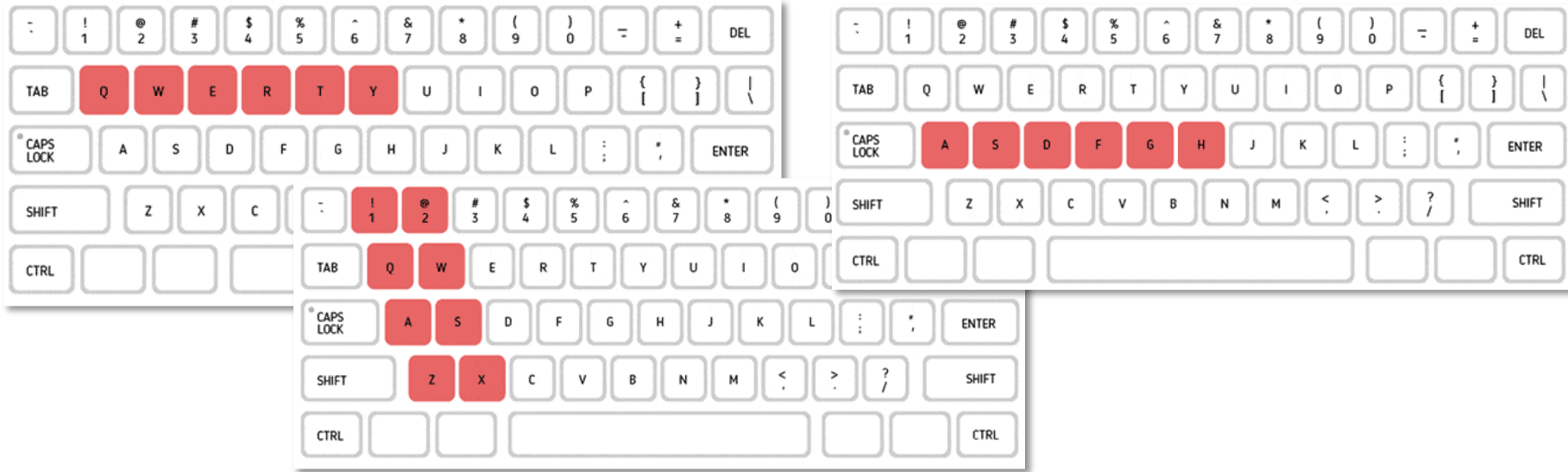
“I’ll Add a Number to Make it More Secure.”

Most Used Numbers (0-99) at the End of Passwords		Least Used Numbers (0-99) at the End of Passwords	
1.	examplepassword1 23.84%	100.	examplepassword39 0.15%
2.	examplepassword2 6.72%	99.	examplepassword49 0.16%
3.	examplepassword3 3.86%	98.	examplepassword60 0.17%
4.	examplepassword12 3.55%	97.	examplepassword38 0.18%
5.	examplepassword7 3.54%	96.	examplepassword37 0.18%
6.	examplepassword5 3.35%	95.	examplepassword41 0.18%
7.	examplepassword4 3.19%	94.	examplepassword61 0.18%
8.	examplepassword6 3.06%	93.	examplepassword46 0.19%
9.	examplepassword9 2.91%	92.	examplepassword53 0.19%
10.	examplepassword8 2.89%	91.	examplepassword48 0.19%

Social engineering

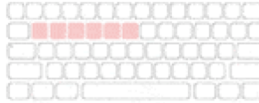


Keyboard patterns

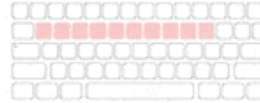


Keyboard patterns

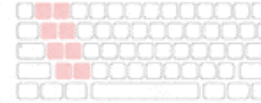
① qwerty



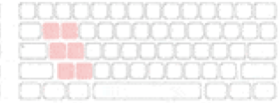
② qwertyuiop



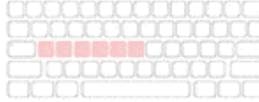
③ 1qaz2wsx



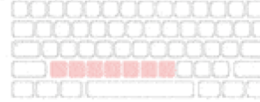
④ qazwsx



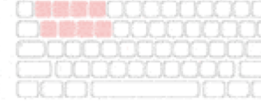
⑤ asdfgh



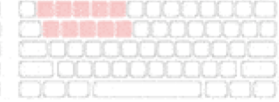
⑥ zxcvbnm



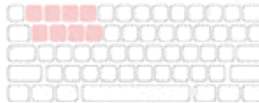
⑦ 1234qwer



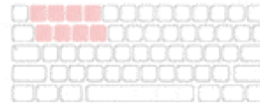
⑧ q1w2e3r4t5



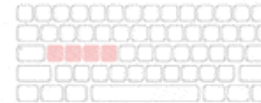
⑨ qwer1234



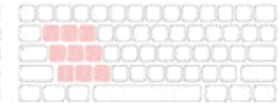
⑩ q1w2e3r4



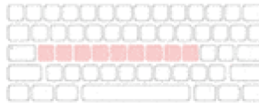
⑪ asdfasdf



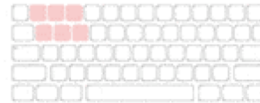
⑫ qazwsxedc



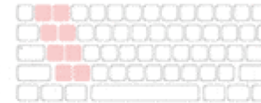
⑬ asdfghjkl



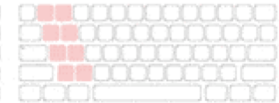
⑭ q1w2e3



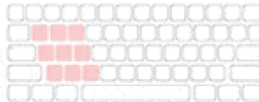
⑮ 1qazxsw2



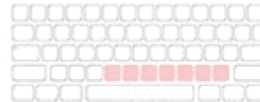
⑯ 12QWaszx



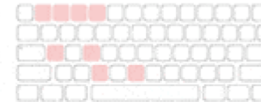
⑰ qweasdzxc



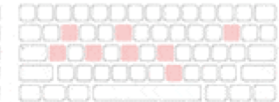
⑱ mnbcvxz



⑲ a1b2c3d4



⑳ adgjpmptw



Common passwords

Most Used Base Phrase (4+ characters)	Most Used Noun (1,000 most common)	Most Used Verb (1,000 most common)	Most Used Colors (Used with numbers)
<ol style="list-style-type: none">1. password2. qwerty3. qwer4. dragon5. qazwsx6. alex7. love8. monkey9. master10. shadow	<ol style="list-style-type: none">1. master2. football3. killer4. angel5. summer6. money7. freedom8. access9. green10. silver	<ol style="list-style-type: none">1. welcome2. enter3. please4. flash5. chase6. catch7. express8. enjoy9. remember10. rescue	<ol style="list-style-type: none">1. red2. blue3. black4. green5. white6. pink7. orange8. brown9. purple10. yellow

Common passwords

Animals

1. fish
2. bear
3. monkey
4. tiger
5. wolf
6. bird
7. eagle
8. lion
9. fox
10. chicken

Fruits

1. apple
2. orange
3. banana
4. peach
5. lemon
6. cherry
7. mango
8. kiwi
9. grape
10. melon

I love...

1. iloveyou
2. lloveU
3. lloves*x
4. iloveme
5. ilovegod
6. ilovehim
7. iloveit
8. iloveher
9. ilovep*rn
10. ilovemyself

My...

1. mylove
2. mypass
3. myself
4. mybaby
5. mylife
6. myname
7. mypassword
8. mygirl
9. mykids
10. mynameis

Common passwords

Superheroes

1. batman
2. superman
3. ironman
4. hawkeye
5. spiderman
6. gambit
7. wolverine
8. thor
9. punisher
10. cyclops

Names in Usernames

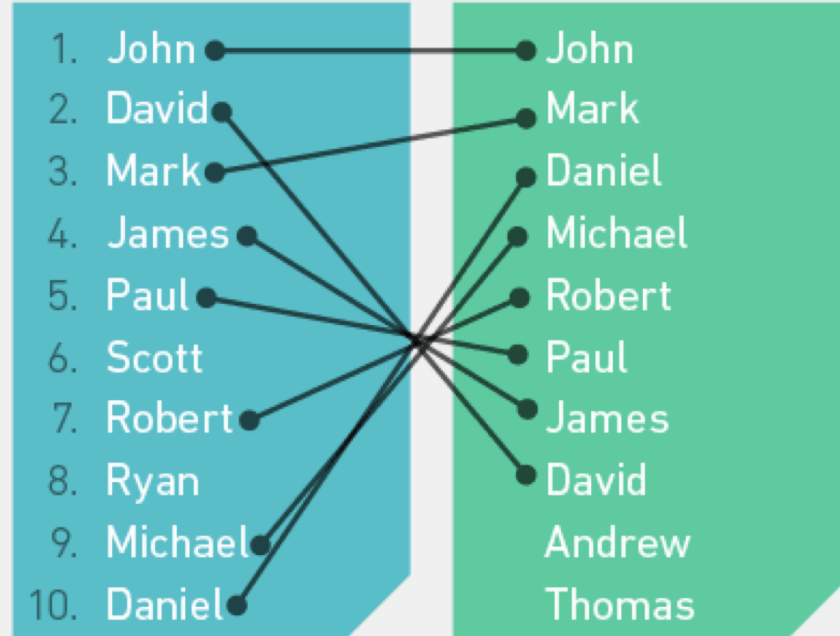
1. John
2. David
3. Mark
4. James
5. Paul
6. Scott
7. Robert
8. Ryan
9. Michael
10. Daniel

Names in Passwords

1. John
2. Mark
3. Daniel
4. Michael
5. Robert
6. Paul
7. James
8. David
9. Andrew
10. Thomas

Days of the Week

1. Friday
2. Monday
3. Sunday
4. Tuesday
5. Thursday
6. Saturday
7. Wednesday



Common passwords rules

Rule #1

Users uses one password for most of all documents

- * Store all found passwords and trying to use them at first
- * Password from some type of documents can be acquired instantly or in reasonable time
- * You can build your own passwords list to use it later

Common passwords rules

Rule #2

About 55% of users use digits only password

- * EDPR can limit characters and password length range in brute-force operation
- * 10 digits password will be recovered in just a seconds

Common passwords rules

Rule #3

Top 10,000 passwords can be used by up to **98.8%** of all users (at year 2014)

False...

Top 10,000 passwords dictionary can open about 98.8% of all passwords

A 98.8% recovery rate during the first minute?

Unfortunately today simple dictionary attack using the Top-10,000 passwords list brings modest results (about 30% success rate at best)

In order to achieve a higher success rate, we analyzed our extensive experience with desktop-based password recovery tools (we sold several hundred thousand of those during the past few years).

Top 10.000.000 real passwords

What we analyzed? 10.000.000 passwords collected by Mark Burnett

<https://archive.org/details/10MillionPasswords>

All passwords are collected from 2011 to present days



*IT security analyst
Utah, USA*

What about huge dictionaries?

Not so great as you can imagine yourself 😞

10,000 passwords are used by 30% of all users

What about huge dictionaries?

Not so great as you can imagine yourself 😞

10,000 passwords are used by **30%** of all users

10,000,000 passwords are used by **34%** of all users

What about huge dictionaries?

Not so great as you can imagine yourself 😞

10,000 passwords are used by **30%** of all users

10,000,000 passwords are used by **34%** of all users

20,000,000 passwords are used by **34.4%** of all users

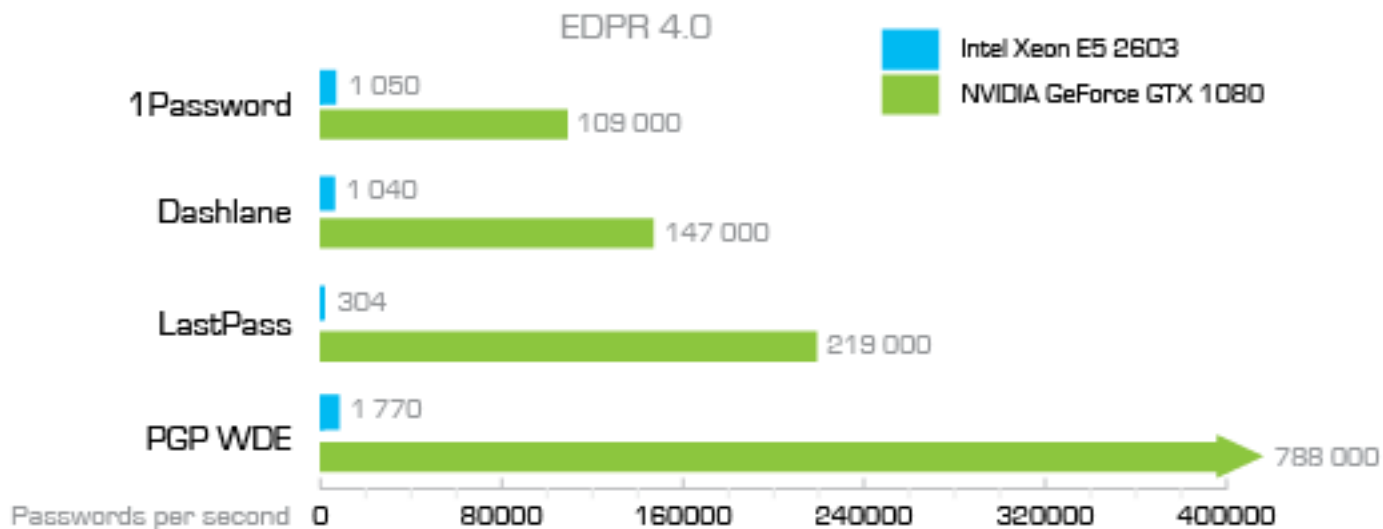
Step 1

Acquire passwords, **that can be recovered instantly or in reasonable time at first.**

Try this passwords list on time-consuming documents (MS Office 2010-2013, for example)

If you have access to mobile devices, try to get access using that passwords to the Passwords Managers, like 1Password or Wallet

Strategy. Conclusion.



Step 2

Use digits only brute-force. It will take split seconds.

Step 3

Analyze known user passwords and use simple mutations or mask method, if known passwords are build on some rules, of course

Example:

AEx1234
aLeX4321
1Alex1
E1com\$oft
eLCoMSoFT

Step 4

Use Top-100/10.000 passwords dictionary without mutations (at first)

Step 5

Use language specific passwords dictionary **without mutations**

** We separated common passwords list into language specific dictionaries. For example – english, german, russian, etc.*

** Basic dictionaries are included in the program distribution. Additional dictionaries are available for purchase and immediate download.*

Step 6

Use brute-force with reasonable time settings (dictionary with mutations)

Step 7

Use brute-force ☹

Elcomsoft Password Recovery Bundle: Forensic Edition

Elcomsoft Password Recovery Bundle is capable of instantly recovering passwords for a wide range of business and office applications, text processors, spreadsheets, database management programs, office suites, email clients, instant messengers, etc.

Over a hundred different file formats and types of password encryption methods can be recovered instantly.

<https://www.elcomsoft.com/eprb.html>



Elcomsoft Mobile Forensic Bundle

The complete mobile forensic kit enables law enforcement, corporate and government customers to acquire and analyze the content of a wide range of mobile devices.

The kit allows experts to **perform physical, logical and over-the-air acquisition of smartphones and tablets, break mobile backup passwords and decrypt encrypted backups**, view and analyze information stored in mobile devices.

<https://www.elcomsoft.com/emfb.html>



Demo versions and copy of this presentation 😊



Methods of accessing encrypted data for further forensics analysis

(c) 2018

Alexey Shtol, ElcomSoft Co. Ltd.

<https://www.elcomsoft.com>

