Cloud Forensics 2018

Vladimir Katalov
ElcomSoft Co.Ltd.
Moscow, Russia

Who we are

- Privately held company, established in 1990
- 100% in-house developments
- Microsoft Gold Certified Partner, Intel Software Partner
- NVIDIA and AMD registered developer
- Over 300 partners and resellers on all continents
- Six US patens
- Corporate, government, military and forensic customers
- Over 300,000 installations worldwide

About us: our customers

What's inside the smartphone?

- Contacts & calendars
- Call logs and text messages
- Emails and chats
- **Account and application passwords**
- **Web and Wi-Fi passwords**
- Documents, settings and databases
- Web history & searches
- Pictures and videos
- Geolocation history, routes and places
- 3rd party app data
- Cached internet data
- System and application logs
- Social network activities

Data acqusition methods

- **JTAG/chip-off**
  - there is no test access port on many devices
  - full-disk encryption makes offline attacks completely useless
- **Physical**
  - Limited compatibility
  - May alternate data
  - Data may be encrypted
- **Logical**
  - Limited compatibility
  - Bypassing screen lock is needed
- **Cloud**
  - Limited set of data
  - Need credentials
  - Legal problems

The Cloud vs. The Rest

- **Issues**
  - *Different platforms (Apple, Google, Microsoft)*
  - *Vendor-specific clouds (especially in China: 360, QQ etc.)*
  - *Third-party cloud services (Dropbox, Box.com, Amazon, Azure etc.)*
  - *Online credentials required (password or token)*

- **Benefits**
  - *No physical access required*
  - *May be performed silently*
  - *Real-time evidence*
  - *Get data from several devices at once*
  - *No pinned to the device model*
  - *Universal approach*
  - *Access to deleted data (sometimes)*

Cloud services: backups, synced data, file storage and more

- **Backups**
  - No standard way to access
  - May not be available
  - Almost all data from the device
- **Sync**
  - Limited set of data
  - **Most critical real-time data**
  - Synced across all devices
- **Storage**
  - Only files/documents
  - Easy to access

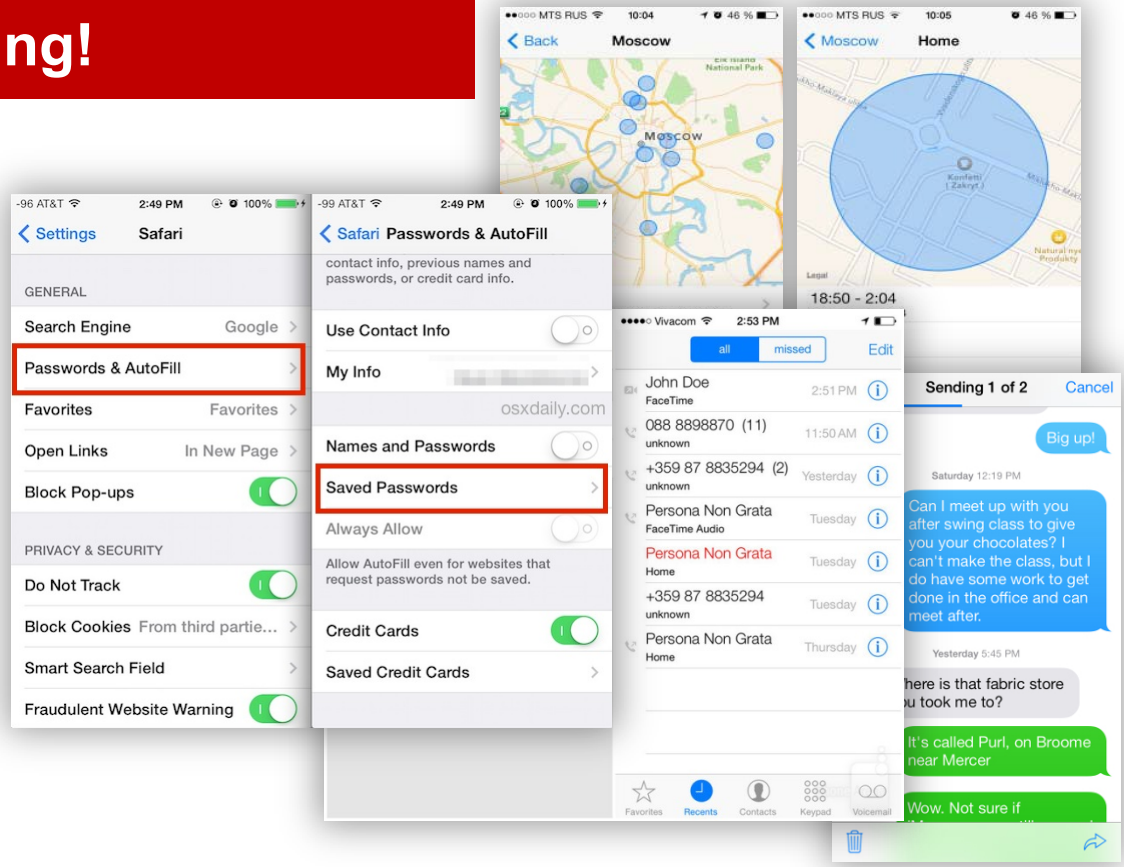
Mobile Cloud Ecosystems

- **Apple iOS**
  - Full backups stored in the cloud
  - Many types of data synced with iCloud in real-time
  - Cloud backups are very comprehensive
- **Google Android**
  - Android backups nearly useless, but…
  - Google Account contains massive amounts of data
- **Windows Phone, Windows 10 Mobile**
  - Creates partial backups
  - A lot of synced data is available

Cloud services combined: what to expect

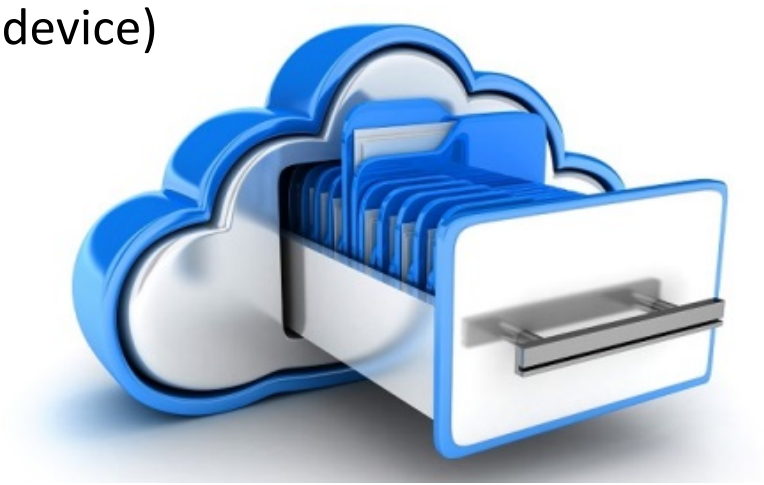
What's Inside? Everything!

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



Cloud services: backups

- Full device backups are sometimes available
- Third-party application data may be limited
- Passwords are not saved in backups, or additionally encrypted
- Daily backups (at best, unless forced from the device)
- Cannot initiate cloud backups remotely
- Third-party software is required
- Almost no way to manage
- Slow access, long download times



Synced Data

- Some information is synced in real time
- Browser history, bookmarks, forms, passwords and login credentials
- Search history (depends on search engine)
- Call logs and text messages (some systems)
- Mail, contacts, calendars and notes
- Android, iOS and Windows 10 handle synced data differently

Synced Data

Apple iOS: iCloud

- Calendars, mail, contacts
- Call logs, Notes
- Health data, Home, News, Maps, Wi-Fi, iBooks
- Safari history, bookmarks
- iOS 11.3: iMessage/SMS
- iCloud Photo Library
- **iCloud Keychain**
- **FileVault2 recovery token**
- ***Some deleted data***

Android: Google Account

- Location and POI-based mapping data
- Google search history
- Mail, calendars, notes
- Calls & messages
- Chrome history, bookmarks, **passwords**

Microsoft Account

- Bing search history
- Edge **passwords**, browsing history
- Limited location data
- **BitLocker Recovery Key**

Advantages of cloud extraction

Cloud Acquisition Helps Bypass All of This:

- **Device passcode**

  Cloud acquisition works even for locked devices

- **Obligatory hardware-backed whole disk encryption**

  Data is encrypted differently in the cloud

- **Keychain encryption**

  System-wide storage for sensitive data (keys, passwords etc.)

- **Device is broken, wiped, or locked**

  No need to access physical device

Cloud data by platform

	Apple	Google	Microsoft
Backups	+ (three)	Sort of (single)	Soft of (several)
Contacts/calendars/tasks	+	+	+
Call log	+	It depends	In backups only
Notes	+	+	+
Messages	iOS 11.3 + 2FA	8.0+	+
Mail	iCloud mail	Gmail	Outlook
Internet	Safari	Chrome	Edge
Media	iCloud Photo Library	Google Photos	OneDrive
Documents	iCloud Drive	Google Docs	OneDrive
Location	Current/last	Current, history	Current, history
3rd party apps data	iCloud Drive	Google Drive	OneDrive
Other	Health, Wallet, Maps etc	Dashboard and more	HealthVault, Skype, Cortana

Cloud passwords, keys etc

	Apple	Google	Microsoft
Wi-Fi	+	+	In backups
Web sites	+	+	+
Credit cards	+	*CVV is needed*	?
Credit cards (2)	*Apple Pay (Wallet): last 4 digits only*	*Google Pay (?)*	Wallet (?)
App-specific	*It depends*	*Sometimes*	*Sometimes*
Authentication tokens	+	+	-
Encryption keys	+	-	-
Certificates	+	-	-
Autocomplete	+	+	+

Amazon: devices and Alexa

- Amazon has device and software infrastructure
- **FireOS tablets** with Alexa: Kindle Fire, Fire HD, Fire HDX
- **FireTV** with Alexa
- **Echo** smart speakers: Amazon Echo, Echo Plus, Echo Dot, Echo Show, Echo Spot and more
- **Amazon Fire Phone**
- **Alexa** on third-party devices (Sonos One, Moto Mods etc.)
- **Alexa** app (Android, iOS)

Amazon: device backups

- Amazon tablets and Fire Phone feature cloud backups
- **Even if Android version (FireOS) lower than 6.0**
- Separate from Google infrastructure
- List of installed apps
- Photos and documents
- Wi-Fi passwords
- Silk browser data

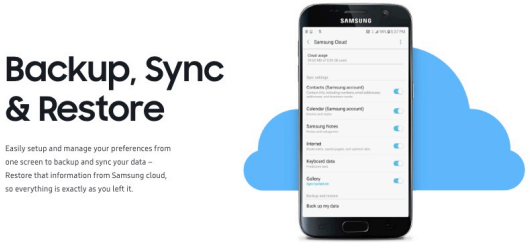
Amazon: devices and Alexa

- Account & device settings
- Amazon order history, timeline, wish list
- Billing & shipping addresses, payment methods
- Installed applications, subscriptions, services
- Games, video library
- Voice snippets (mp3 + recognized commands)
- Voice calls (some countries), messages

Other cloud services

- **Samsung**: cloud backups, photos, settings; Samsung Account required
- **Xiaomi MiCloud**: cloud backups (no app data), photos, contacts, text messages, Find My Phone, 2FA; Mi Account required
- **WeChat/QQ**: hard to say, controlled by Chinese government
- **Huawei**: device backups, synced data

小米云服务
i.xiaomi.com



App-specific cloud services

- Various apps, social networks, password managers and Web browsers maintain some of their data in the cloud
- WhatsApp: backups in iCloud Drive and Google Drive
- Telegram: chats stored in its own cloud
- Swarm/Foursquare, Facebook, Twitter, Instagram
- Password managers: LastPass, Roboform etc.
- Mozilla Firefox, Opera: browsing history and passwords
- Dropbox, Box.com etc
- DJI: drone routes, serial numbers, speed, coordinates
- File sharing and file upload services

Apple iCloud

- Introduced in Oct 2011 with iOS 5
- Optional upgrade to iCloud Drive since iOS 8
- All backups stored in iCloud Drive since iOS 9
- 5 GB free storage, up to 2 TB paid storage
- System backups and synced data
- Passwords (iCloud Keychain)
- Photos (iCloud Photo Library)
- Documents, notes, calendar, Find My Phone and more

Acquisition is Non-Trivial

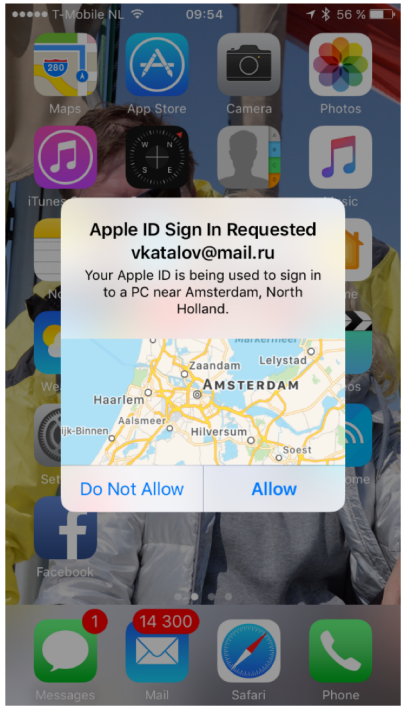
- Data stored at third-party storage providers (now mostly Google)
- Data of Chinese users are stored at GCBD
- Data of Russian users are stored at… Google (still), despite regulations
- All data is encrypted (by chunks)
- Encryption keys are always stored at Apple datacenters (except China?)
- In backups, some files (including keychain and health data) are further encrypted with device-specific key
- iCloud Keychain items are encrypted even stronger (access by trusted devices only)

Moving Target

- Apple actively resists attempts to access iCloud backups with third-party tools
- Since May 2017, Apple locks access to Apple ID accessed with many third-party tools; requires password reset
- Constant changes in authentication mechanisms break third-party tools
- Third-party tools must be promptly updated to reflect changes
- When choosing a cloud acquisition tool, consider product update policies

Two-Factor Authentication

- Protects access to backup data, keychain
- Verification code sent to trusted device
- Alternatives:
  - Recovery key
  - Authentication token



Synced data

Many types of data sync with iCloud

- Nearly real-time sync (usually up to 10 mins even on mobile network; faster on Wi-Fi)
- No need to wait for backups to be created

- Limited amount of data
- 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 11.3, if synced)

Advantages of obtaining synced data

- Usually enabled by default
- Little known, rarely disabled
  - **Challenge**: try making your iPhone to NOT sync call logs via cloud
- Real-time data and real-time availability
- Deleted data is available for many categories (documents, call logs, pictures: up to 30 days)
- Weaker protection compared to cloud backups
- Current location

Extracting iOS synced data

- iCloud Photo Library: pictures (EXIF may contain location)
- **iCloud Keychain: passwords!**
- Call logs
- Wallet (tickets, passes, cards)
- Wi-Fi access points
- Maps: My Maps, routes, saved places, searches
- Safari history, open tabs on all synced devices, bookmarks
- Calendars, notes
- Books and documents (iBooks)

OS synced data: what's next?

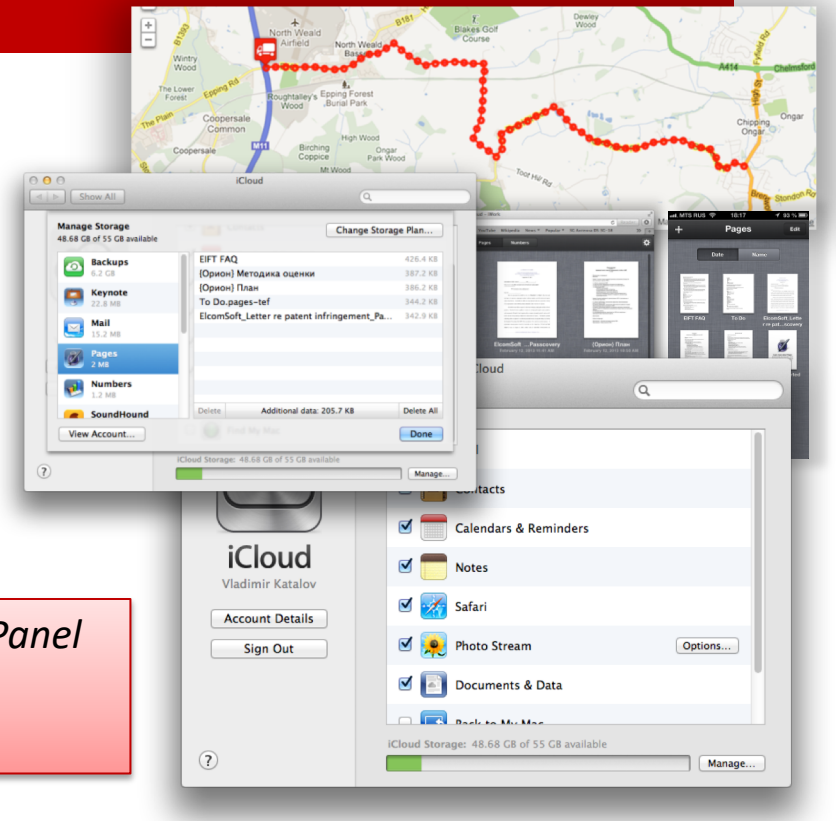
Coming soon

- Apple Health
- Apple Home
- Mail
- iMessage/SMS
- Siri data? // sorry, no ☹

What's Inside an iCloud Backup?

- Contacts and Contact Favorites
- Messages (including iMessages)
- Call history
- Application data
- Device settings
- Camera roll (photos and videos) – only if no iCloud Photo Library
- Purchases (music, movies, TV, apps, books)
- Mail accounts
- Network settings (saved Wi-Fi hotspots, VPN settings etc)
- Paired Bluetooth devices
- Offline web application cache/database
- Safari bookmarks, cookies, history, offline data
- Geolocation history and places
- **... and much more**

- **However, no IMEI**



- ***> 50%*** *cannot be downloaded using iCloud Control Panel (and not synced to PC/Mac)*
- *Still can be obtained using proper tools*

iCloud and iCloud Drive

We have:

- Apple ID and password, or
- PC synced with iCloud (binary authentication token)

Acquisition steps:

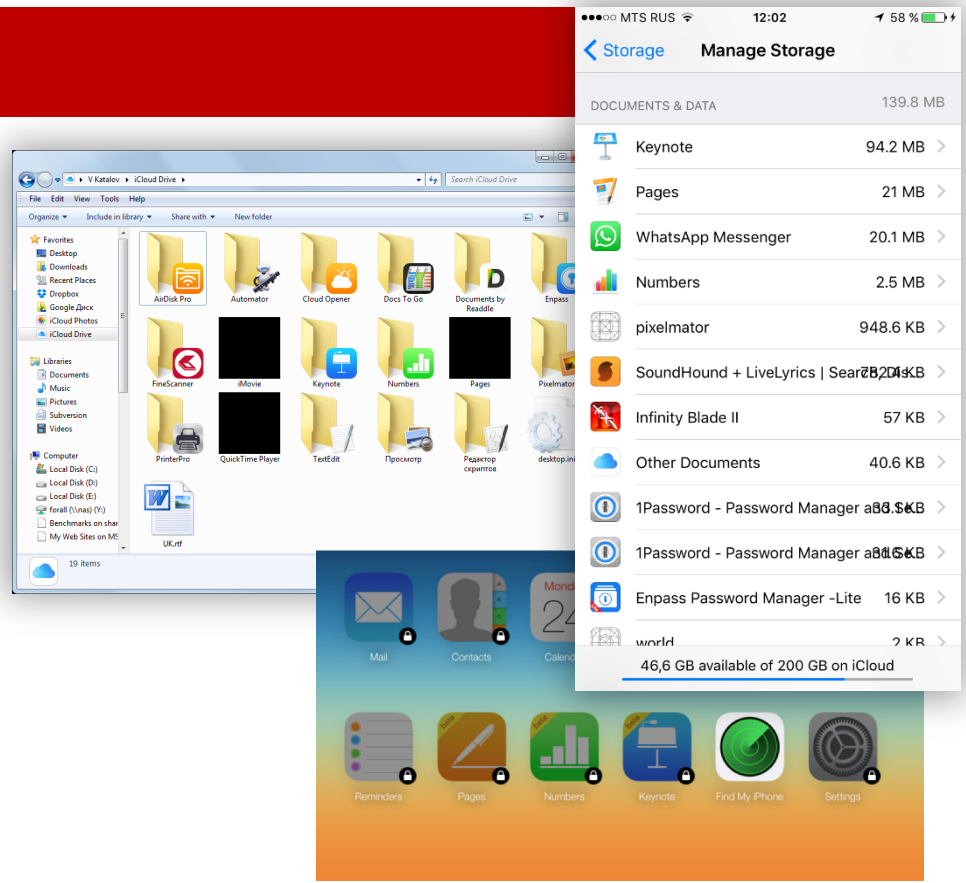
- Use Apple ID and password to download the backup
- Extract binary authentication tokens, use to download backup

Notes:

- Two-factor authentication may be an issue
  - Using binary authentication token bypasses 2FA
- Backup keychain encrypted with hardware key
  - Can be decrypted if ‘securityd’ key is extracted from the device
- Full data set acquisition speed very slow
  - Can quickly download & analyze select information, full data set later

What's different?

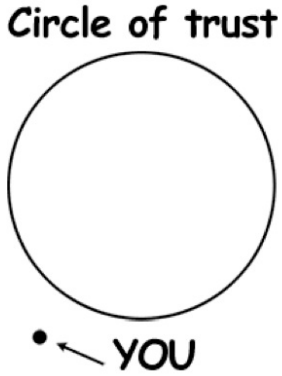
- iCloud Drive may contain arbitrary files uploaded by apps or the user
- Clients available for Mac, PC, and iOS
- iCloud Drive is used by many apps:
  - 1Password (password keeper)
  - *Pages, Numbers, Keynote*
  - EnPass, other password managers
  - Pixelmator, Printer Pro, TextEdit
  - WhatsApp, other IMs
  - and many others



iCloud Keychain

- **iCloud keychain**

  View: Only when/if synced with local device
  Protection: strong
  Decrypt/export: no way (but we did it anyway)

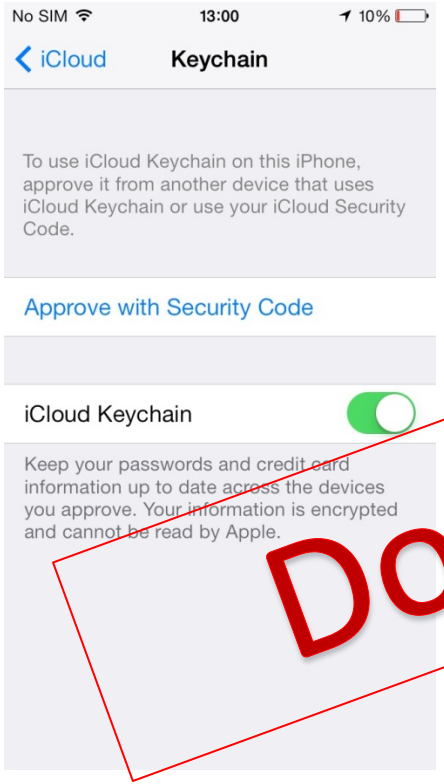


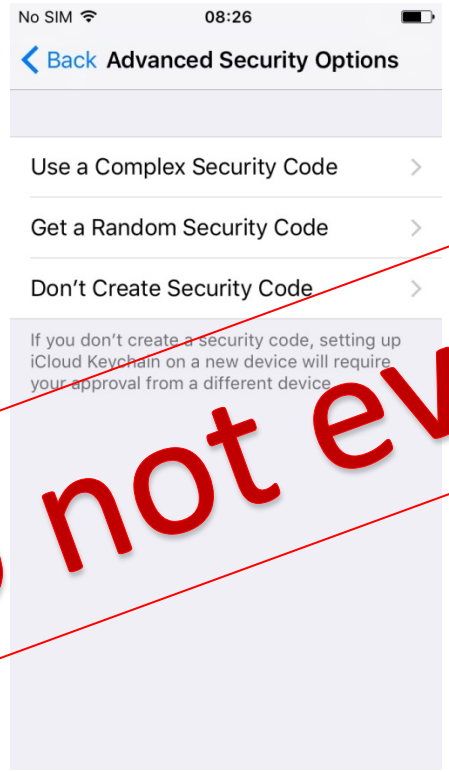
Backup vs iCloud keychains

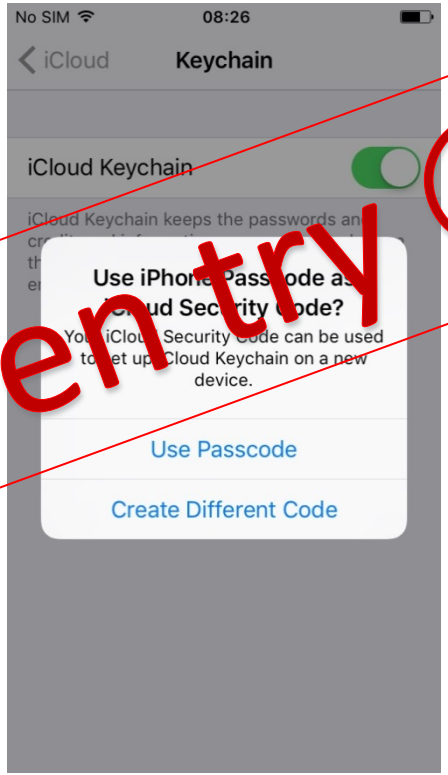
	Backup	iCloud
Wi-Fi	+	+
Web sites	+	+
Credit cards	+	+
App-specific	+	*It depends*
AirPlay/AirPort	+	+
Encryption keys & tokens	+	*It depends*
Autocomplete	+	-

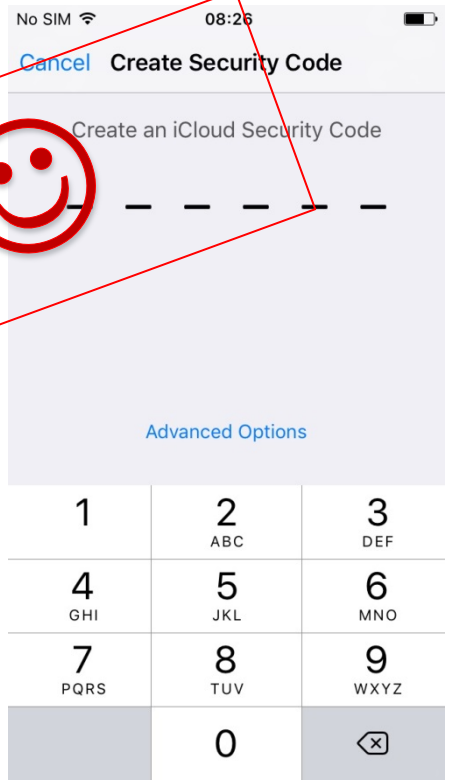
Keychain in iCloud backups have most data encrypted with device-specific key

Set up iCloud keychain – no 2FA

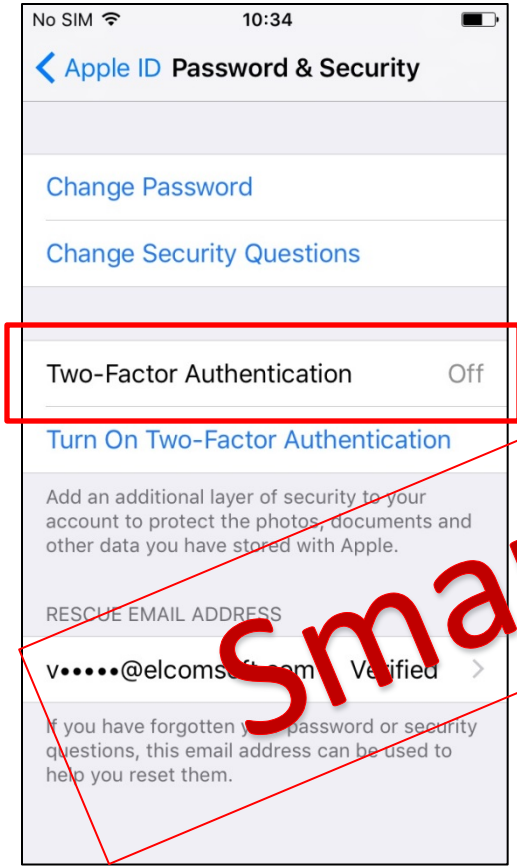


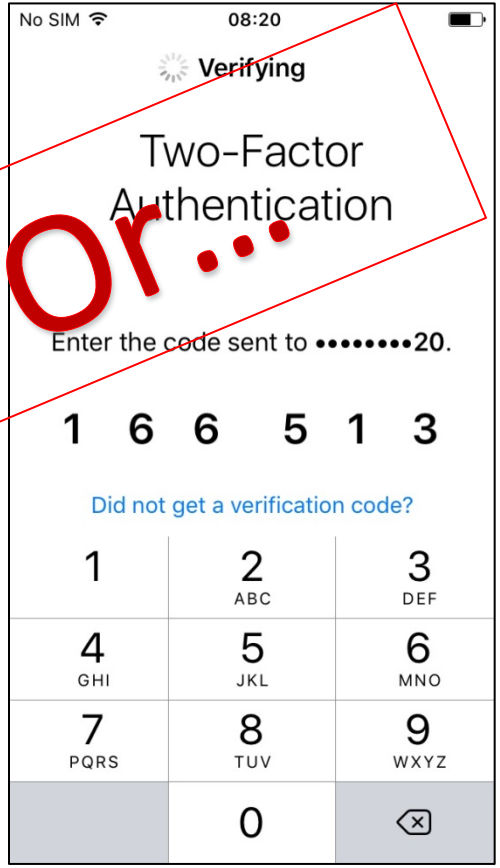






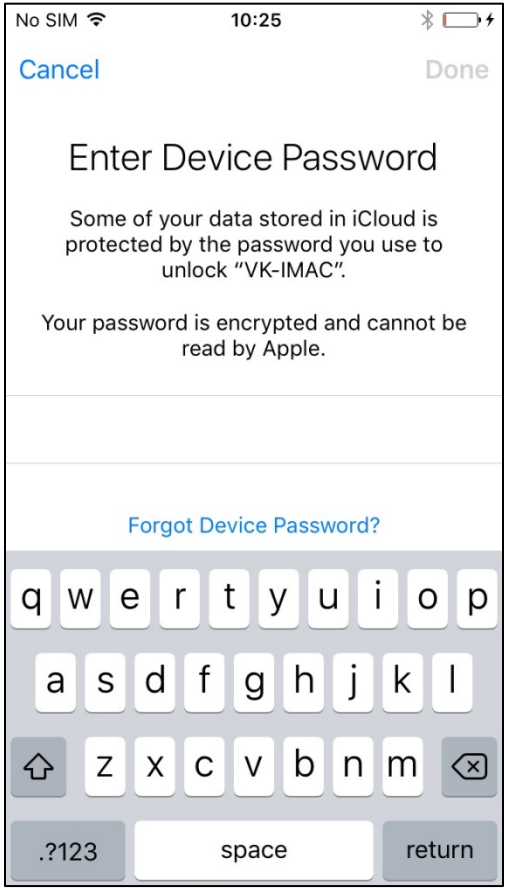
Set up 2FA

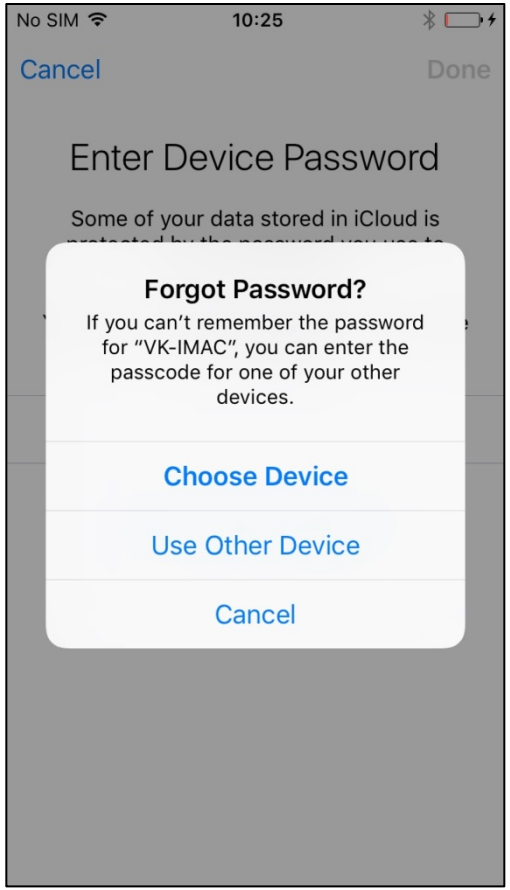


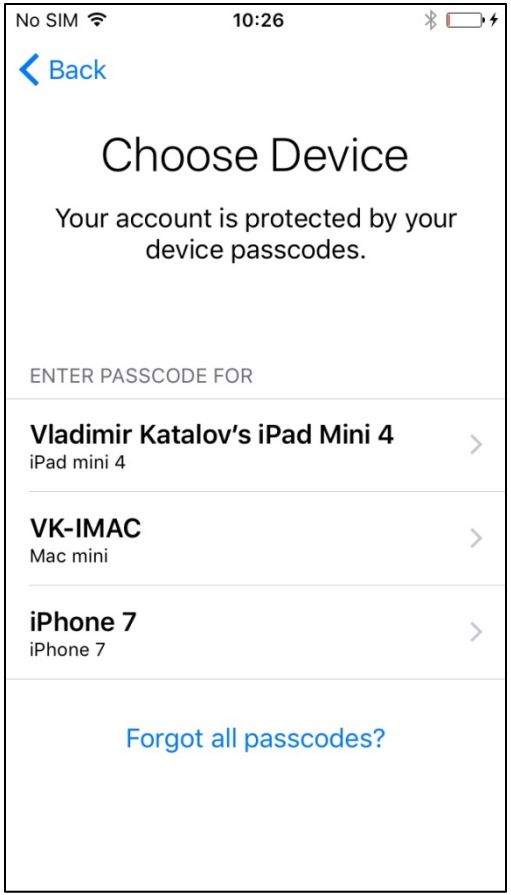


Smart choice! Or...

Set up iCloud keychain –2FA







iCloud Authentication Tokens

- Authentication tokens are used for convenience
- Saved on a Mac or PC used to access iCloud
- Allow users to avoid entering for Apple ID and password every time
- Technically, an authentication token is **stored in a file** on the user's computer
- Locating the file and extracting the token allows bypassing login/password authentication and 2FA

- Authentication tokens do not contain a password to the user's Apple account
- They don't contain a hash of the password either
- They cannot be used to brute-force the original plain-text password

Authentication Tokens: Limitations

- **iOS 8**: Authentication tokens are short-lived
  - iCloud backups can only be downloaded within a limited timeframe
  - Exact expiry timeframe not known

- **iOS 9, 10**: Backups stored in iCloud Drive, authentication tokens do not expire

- **iOS 11**: authentication tokens expire again; after expiration, allow to get everything but iCloud backups (so only files at iCloud Drive, synced data, iCloud Photo Library)

- *iCloud keychain: the other token (+anisette data); heavily obfuscated private APIs in macOS X*

iOS Cloud Acquisition: Conclusion

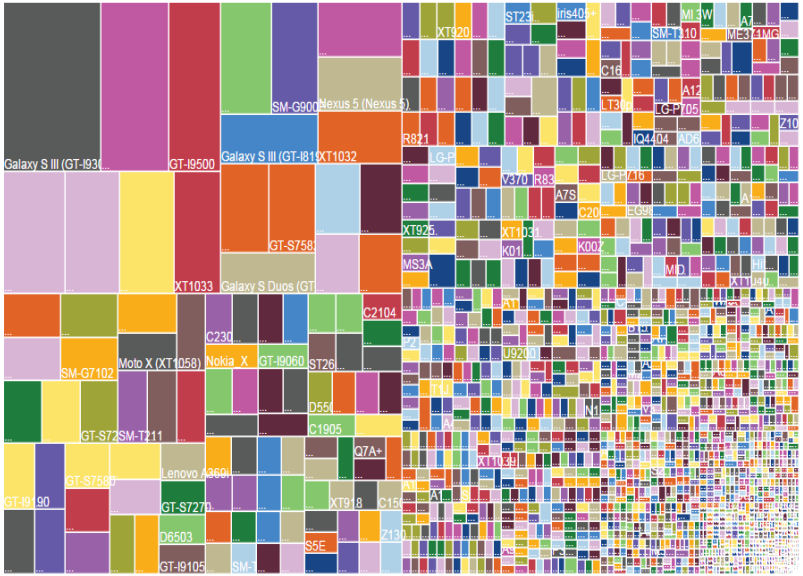
- Exemplary backup system
- Automatically created with no user interaction
- Backups contain massive amounts of data
- Some types of data synced in real time
- For synced data, it is possible to get only changes
- Acquisition IS possible with proper tools
- Keychain is harder to get
- Data from all devices (pinned to the account) can be acquired, incl. macOS X desktops

Android Open Source vs. Google Mobile Services

- Not every Android device is a Google device
- Google collects data from other sources i user signs in
  - Chrome browser
  - Google Maps
  - Gmail
  - Google search
- **Including competing platforms**

Google: Why Cloud Forensics?

- Hundreds manufacturers
- Tens of thousands device models
- Extreme platform fragmentation
- Acquisition approaches vary (logical, physical, JTAG)



Google Account acquisition

- Single point of entry
- Unified approach
- Impressive amount of information

Google Account: What's Inside

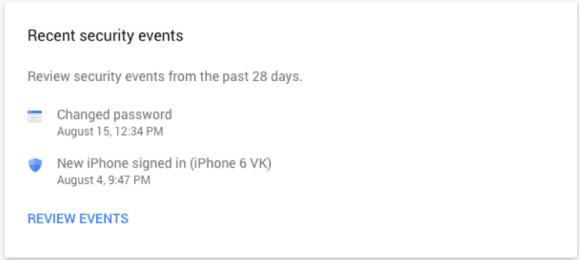
- User data
- All connected devices
- Devices/browsers and apps requested access
- Google ads settings (incl. interests: good for profiling)
- Contacts, calendars
- Notes, mail
- Call logs and SMS (depending on Android version)
- Albums (photos/pictures/videos)
- Hangouts conversations
- Chrome
  - Browsing & search history
  - Synced passwords and autofill data
  - Bookmarks
- A lot of statistical information

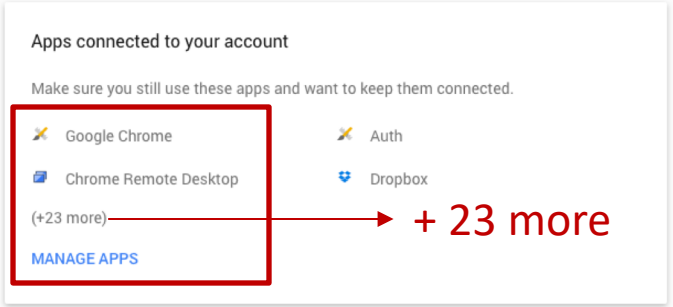
Top Smartphone Apps

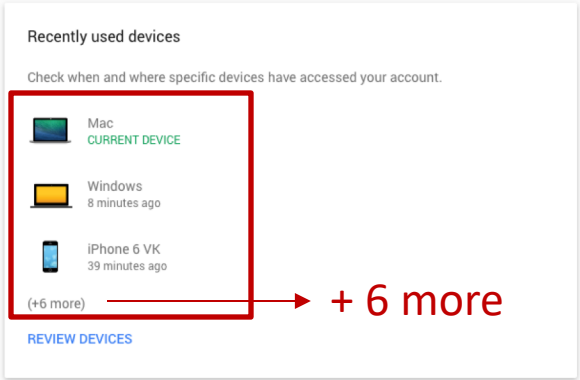
- Facebook
- **YouTube**
- Facebook Messenger
- **Google Search**
- **Google Play**

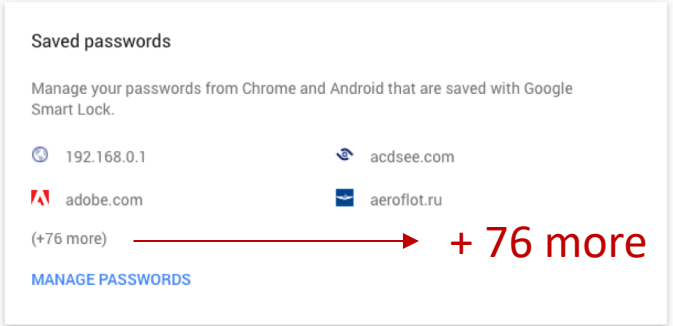
Google Collects Data from Multiple Sources

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



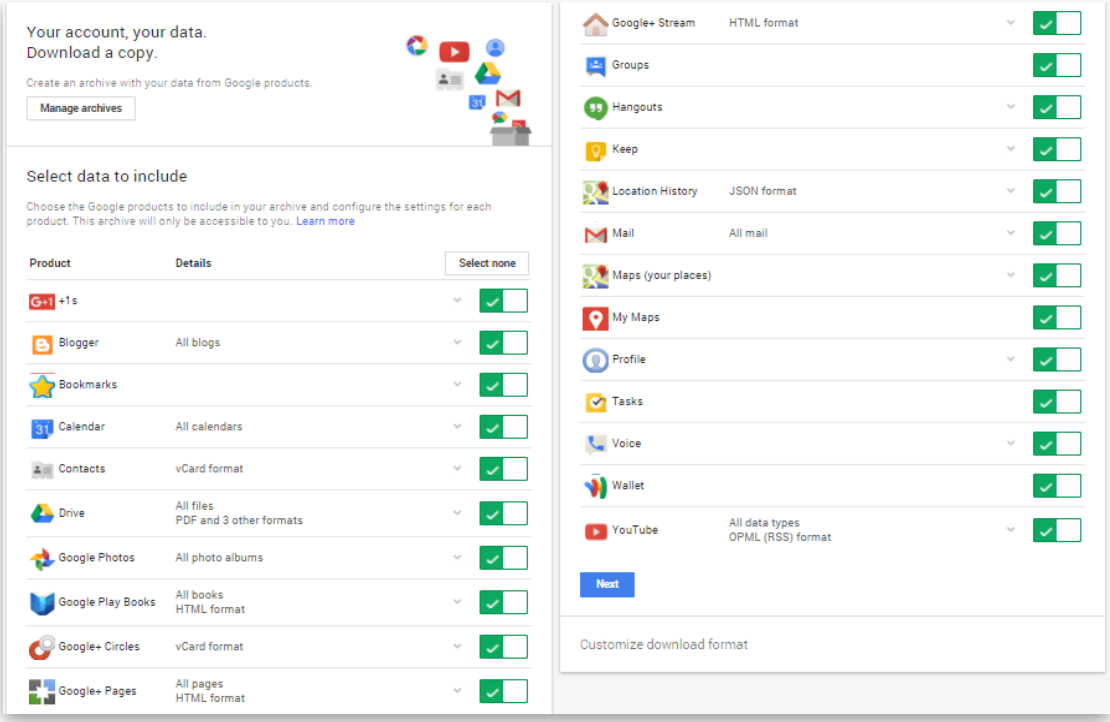






Google Takeout

- Leaves many traces
- Not everything is exported
- Limited flexibility
- Numerous awkward formats
- User alerted via email



Google Dashboard – Not Available via Google Takeout

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

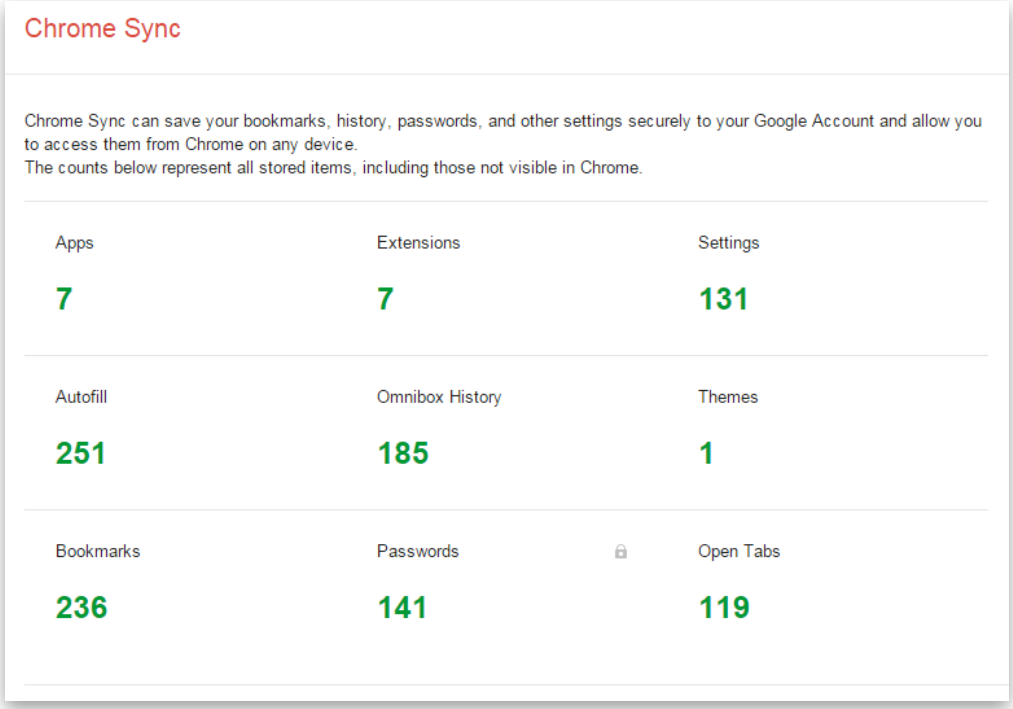
Profile info
- Google+ name
- profile URL
- number of phone numbers
- number of "+1"

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)

Chrome Sync

- **All signed-in devices**
- Bookmarks
- Browsing history
- Open tabs
- Forms
- Passwords
- Page transitions
- Some data not saved by Google Takeout



Google Chrome: Search & Browsing History

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

https://history.google.com/history/

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

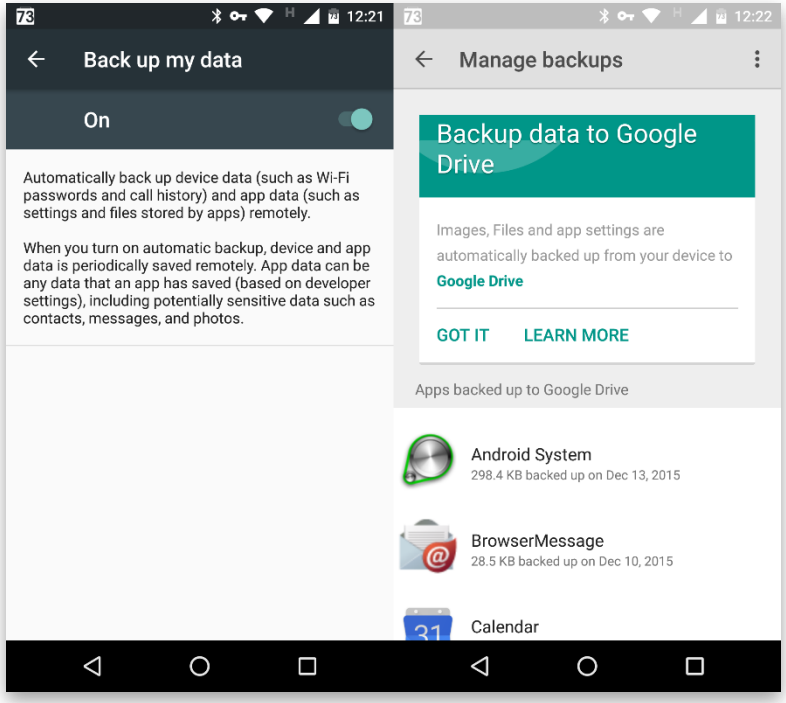
What is saved:

- 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

***Google Takeout** does NOT work with history*

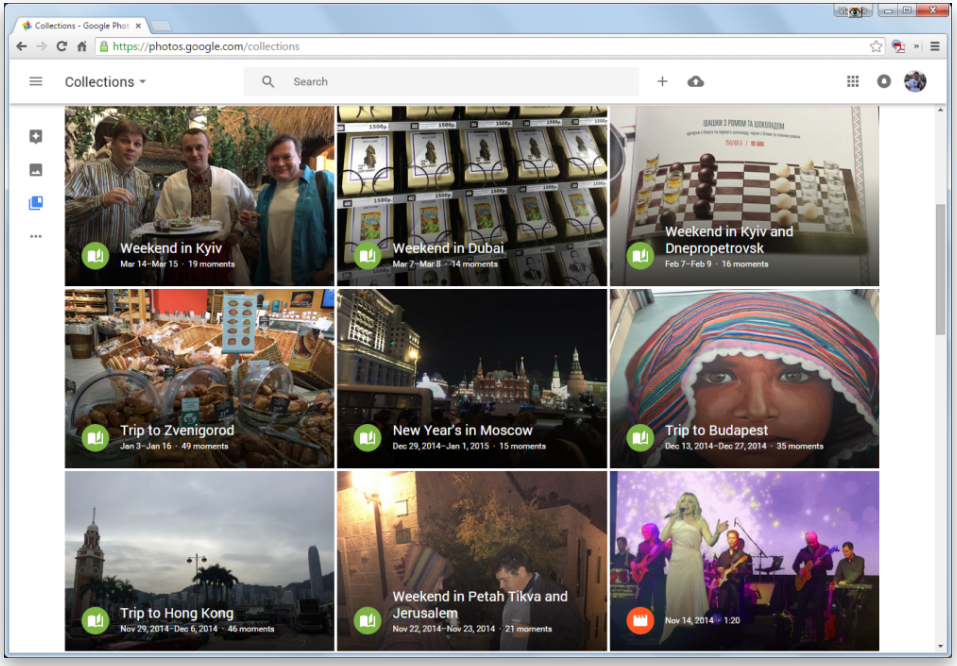
Android Device Backups

- Wi-Fi networks & passwords
- Apps installed through Google Play
- Display, language, input and other settings
- Date & Time
- 3rd party app settings & data (extremely limited)
- Limited content, nearly useless in real life
- Developers can disable backups per app
- Developers must explicitly enable backups to make use of Android 6.0 features
- Google disables backups for its own apps



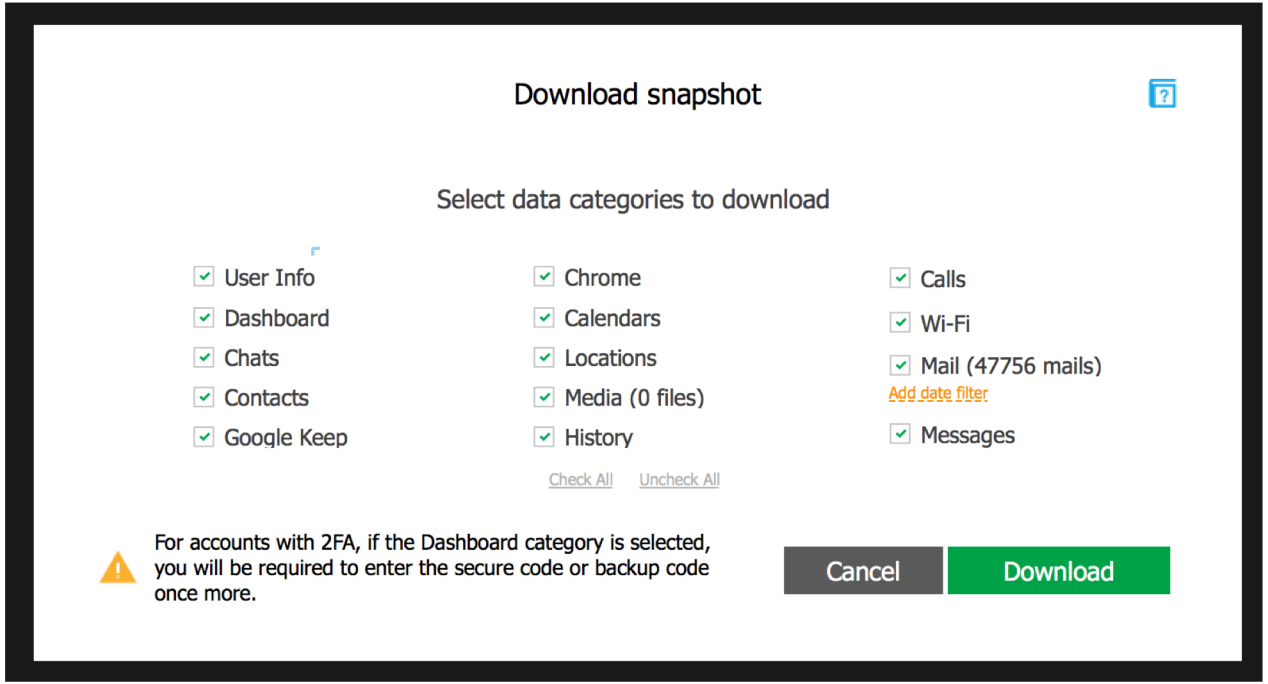
Google Photos

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



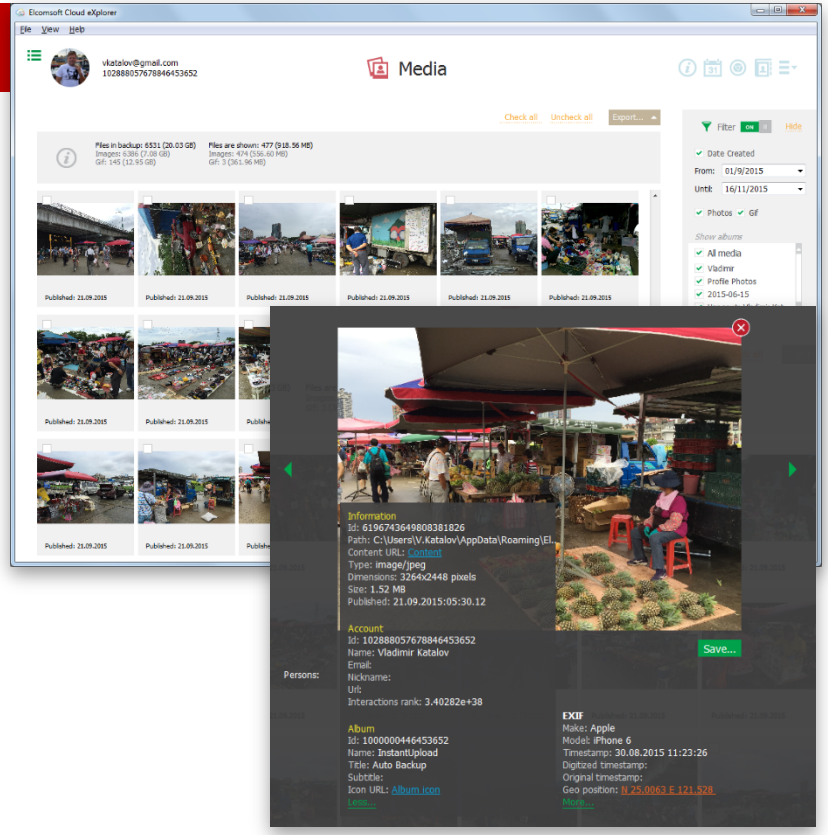
What's Available via Elcomsoft Cloud Explorer

- User profile
- Messages
- Contacts
- Notes (Google Keep)
- History
- Chrome data
- Media
- Calendars
- Dashboard
- Location
- Android data



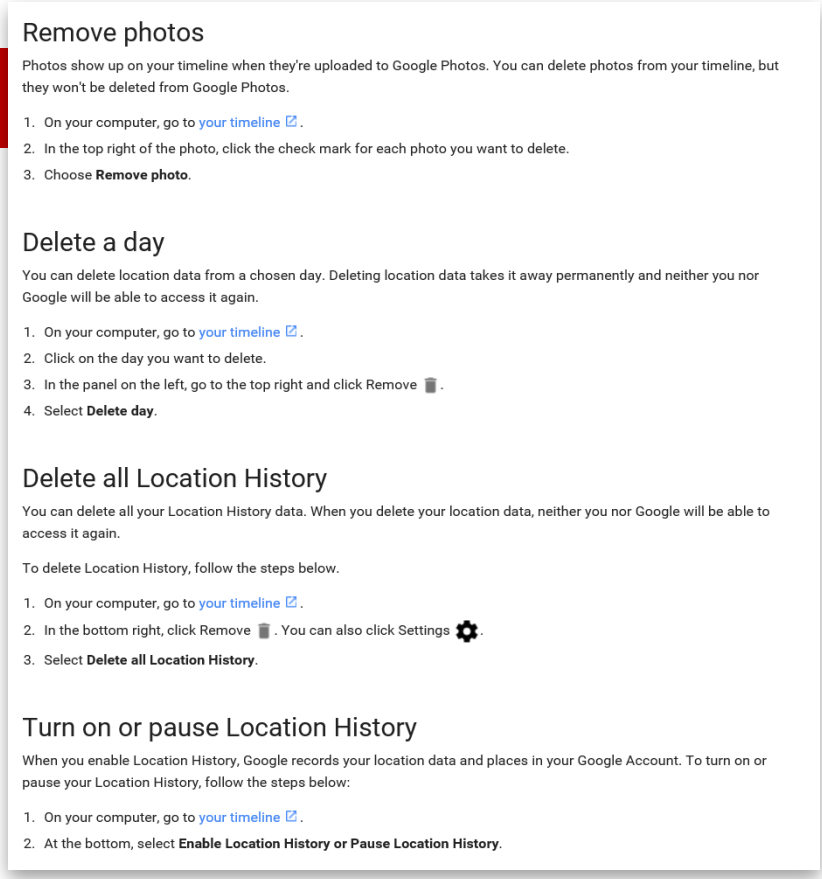
Media

- Photos from all user's devices can be uploaded to Google Photos
- Can be downloaded with Elcomsoft Cloud Explorer or manually via Google Drive
- Google Photos **not the same as** Google Drive!
- More information (e.g. tagged faces, location data, street addresses etc.)
- It is possible to use Google Photos to access full image metadata



Google and Privacy Concerns

- Users can delete data stored in their Google Account
- Google offers various options
- No all-in-one “stop tracking and delete all saved data” switch
- Various trackers must be disabled individually through various Google pages
- **Work in progress**: tool for disabling Google tracking and clearing collected data



Remove photos

Photos show up on your timeline when they're uploaded to Google Photos. You can delete photos from your timeline, but they won't be deleted from Google Photos.

1. On your computer, go to your timeline.
2. In the top right of the photo, click the check mark for each photo you want to delete.
3. Choose **Remove photo**.

Delete a day

You can delete location data from a chosen day. Deleting location data takes it away permanently and neither you nor Google will be able to access it again.

1. On your computer, go to your timeline.
2. Click on the day you want to delete.
3. In the panel on the left, go to the top right and click Remove.
4. Select **Delete day**.

Delete all Location History

You can delete all your Location History data. When you delete your location data, neither you nor Google will be able to access it again.

To delete Location History, follow the steps below.

1. On your computer, go to your timeline.
2. In the bottom right, click Remove. You can also click Settings.
3. Select **Delete all Location History**.

Turn on or pause Location History

When you enable Location History, Google records your location data and places in your Google Account. To turn on or pause your Location History, follow the steps below:

1. On your computer, go to your timeline.
2. At the bottom, select **Enable Location History or Pause Location History**.

Google Cloud data: Conclusion

- Data in Android backups extremely limited
- Massive amounts of information in Google Account, synced in real time
- Cloud backups can be enforced through ADB
- Browsing history, searches and page transitions, comprehensive location history, mail, notes, pictures and much more can be acquired
- **Google Takeout**: free, limited data, sends user alert, leaves traces, data in different cumbersome formats, analysis very difficult
- Limited use of authentication tokens from PC or Mac
- Make sure you have proper tools ☺

Microsoft Account and Cloud Backups

- Windows 8 and later have comprehensive cloud backup system
- Automated backups similar to iOS
- Contain lots of data including call history and messages (Windows mobile only)
- Synced data from desktop:
  - Edge browsing history
  - Search history (Bing)
  - Location history
  - Some Cortana data
  - Passwords saved in Edge (hard to obtain)
- Data on OneDrive
- Skype conversations (last 30 days)
- BitLocker recovery key (!)

How to get cloud password or token?

- Legally (court order)
- Social engineering
- From computer (cached browser passwords)
- From computer (saved token from system or apps)
- Extract macOS keychain
- From other account that was easier to break (Apple / Google / Microsoft)
- Extract from local iTunes backup (with password)
- From password manager (need to crack master password first)
- Password re-use often helps
- From the sticker on monitor or note under the keyboard
- Rubberhose cryptanalysis ☺

Thanks!
Questions?