



What Google knows about you and your devices (and how to get it)

Vladimir Katalov
ElcomSoft Ltd.
www.elcomsoft.com

Research motivations

- Curiosity
- Privacy
- The right to know
- Government surveillance
- Forensics
- Backup and recovery



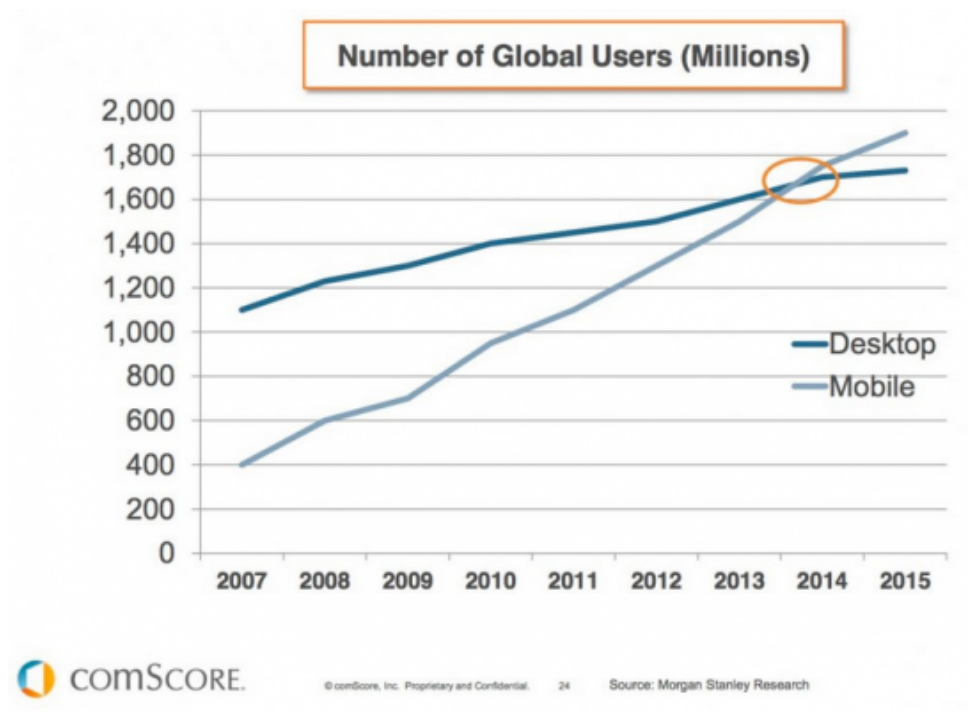
What this presentation is NOT about

- Hacking
- Accessing someone else' account
- Compromising Google
- Criminal activities
- Profit



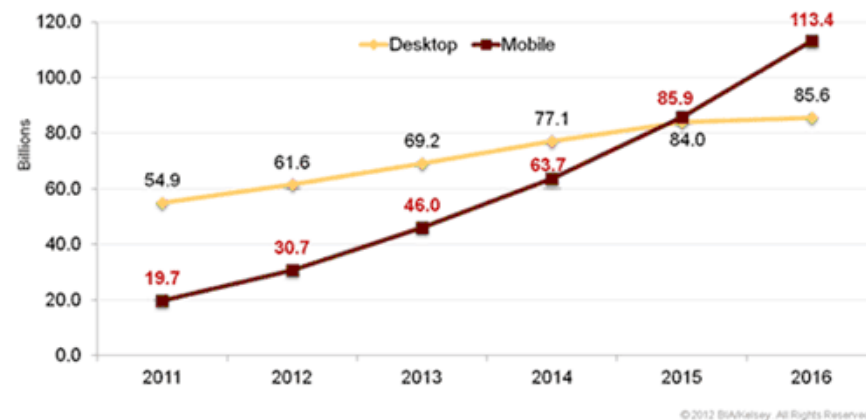
Most information used for this research is public

Desktop vs Mobile forensics



U.S. Local Search Market: Mobile vs. Desktop

In 2015 mobile local search volume will surpass desktop local search for the first time. By 2016 we expect mobile to exceed desktop by 27.8 billion queries.



Smartphone sales

Worldwide Smartphone Sales to End Users by Vendor in 2Q15 (Thousands of Units)

Company	2Q15 Units	2Q15 Market Share (%)	2Q14 Units	2Q14 Market Share (%)
Samsung	72,072.5	21.9	76,129.2	26.2
Apple	48,085.5	14.6	35,345.3	12.2
Huawei	25,825.8	7.8	17,657.7	6.1
Lenovo*	16,405.9	5.0	19,081.2	6.6
Xiaomi	16,064.9	4.9	12,540.8	4.3
Others	151,221.7	45.9	129,630.2	44.6
Total	329,676.4	100.0	290,384.4	100.0

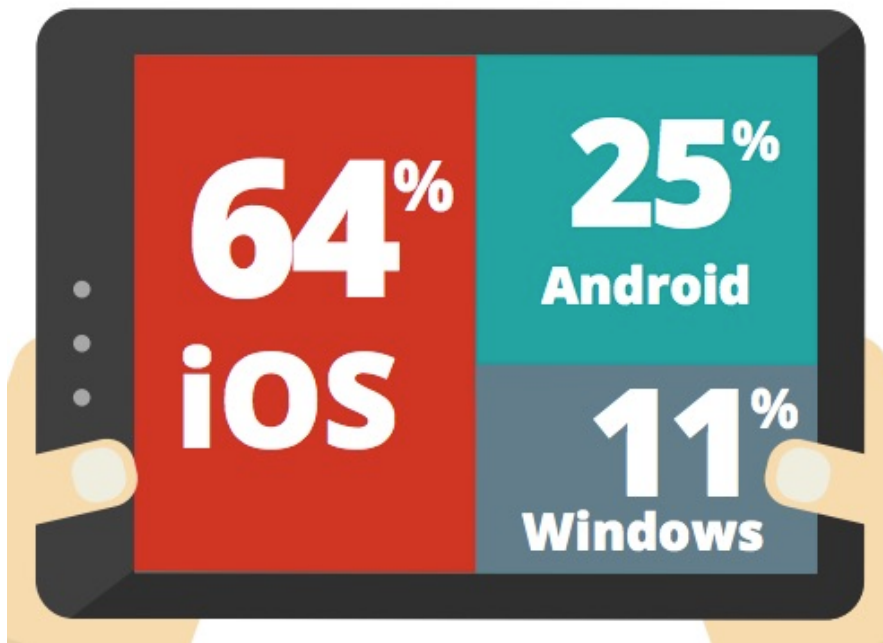


Worldwide Smartphone Sales to End Users by Operating System in 2Q15 (Thousands of Units)

Operating System	2Q15 Units	2Q15 Market Share (%)	2Q14 Units	2Q14 Market Share (%)
Android	271,010	82.2	243,484	83.8
iOS	48,086	14.6	35,345	12.2
Windows	8,198	2.5	8,095	2.8
BlackBerry	1,153	0.3	2,044	0.7
Others	1,229.0	0.4	1,416.8	0.5
Total	329,676.4	100.0	290,384.4	100.0

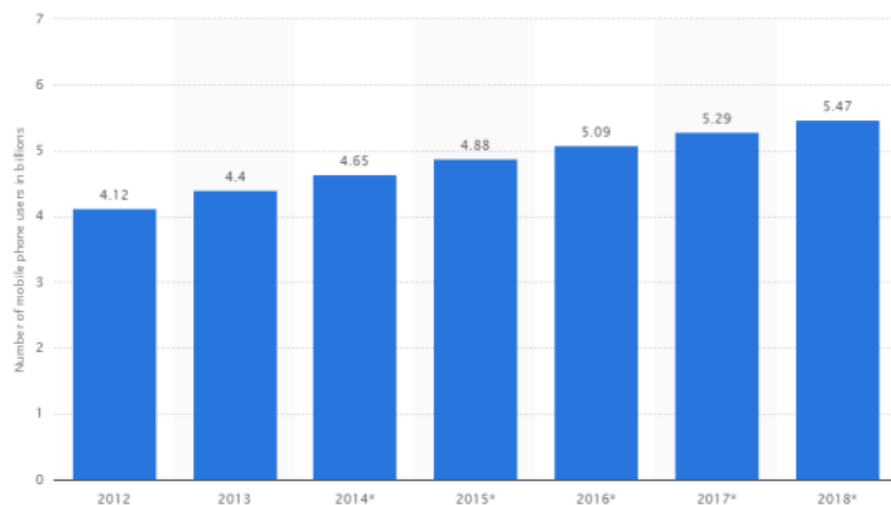
Source: Gartner, August 2015

Enterprise tablet market



Source: Q2'2015 Mobility Index Report

Mobile vs Cloud forensics



Apple iCloud

- Introduced in Oct 2011 with iOS 5
- Optional upgrade to iCloud Drive since iOS 8
- 5 GB free storage, up to 1 TB paid storage
- Extremely convenient: over 500 million users

Google mail

- 900 million users (May'2015)
- Monthly unique users: 90 million (2014)
- Percentage of Americans using Gmail: 24% (2013)
- Gmail app downloads from Google Play: 1 billion (2014)
- Percentage of Gmail users working on mobile device: 75% (2015)

Google Chrome

- Google Chrome users: 1 billion (2015)
- Percentage of web browser usage: 35% (2013)

Android

- Number of Android devices: 1 billion (2013)
- Android share: over 80%
- Average daily Android activations: 1.5 million
- About 25,000 **unique** devices

What Apple Knows About You?

<https://www.apple.com/privacy/government-information-requests/>

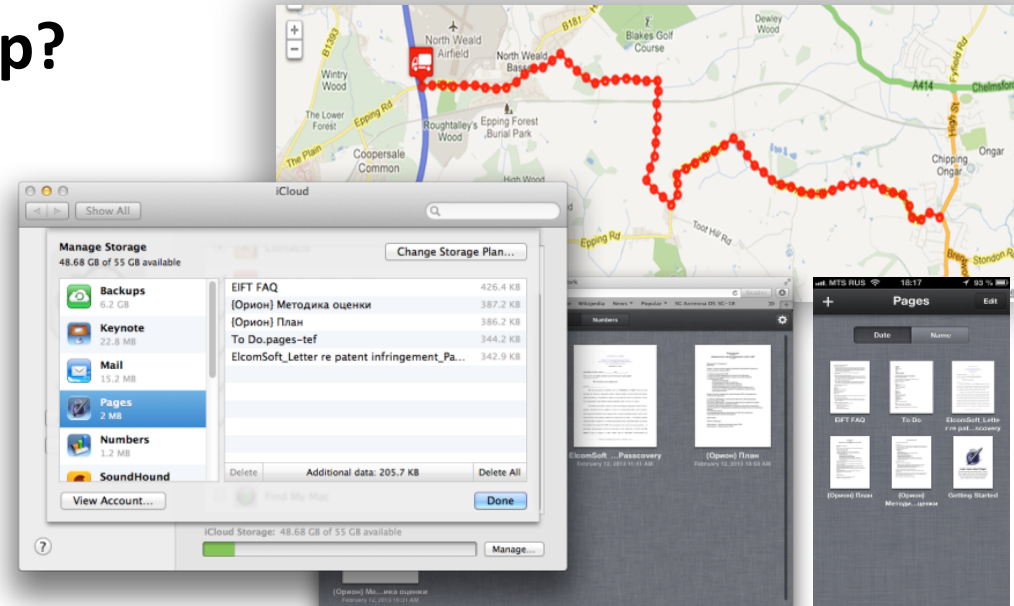
- Device registration
- Customer service records
- iTunes
- Apple retail store transactions
- Apple online store purchases
- Find My iPhone
- Other device information
 - MAC address
 - UDID



- iCloud
 - Subscriber information
 - Mail logs
 - Email contents
 - Photo streams
 - Documents
 - Contacts
 - Calendars
 - Bookmarks
 - App-specific data
 - All files stored on iCloud Drive
 - Device backups

What's Inside an iCloud Backup?

- Contacts and Contact Favorites
- Messages (including iMessages)
- Call history
- Application data
- Device settings
- Camera roll (photos and videos)
- 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
- *Passwords (encrypted with device key)*
- **... and much more**



+ iCloud Drive

- More application data
- Passbook data
- User's dictionaries
- Documents
- 1Password database
- WhatsApp own backup

Over-the-Air Acquisition: iCloud and iCloud Drive

We have:

- Apple ID and password, or
- PC or Mac 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 or data

Notes:

- Two-factor authentication may be an issue
 - Using binary authentication token bypasses 2FA
- Keychain is encrypted with hardware key
 - Can be decrypted if *securityd* key is extracted from the device
- Full data set acquisition speed is slow
 - Can quickly download & analyze selected information, full data set later
- Account owner *may* receive a notification email in 10 minutes after download is started (iCloud backup only)



Most Known iCloud Hacks

- Dmitry Medvedev (Russian Prime Minister) Twitter account hacked (August 2014)

<http://www.theguardian.com/world/2014/aug/14/dmitry-medvedev-russian-pm-twitter-account-hacked>

- Celebrity photo hack (August 2015)

http://en.wikipedia.org/wiki/2014_celebrity_photo_hack

- Leaked Emails Reveal What Vladimir Putin Tells World Leaders at Private Meals (May 2015)

<http://globalvoicesonline.org/2015/05/08/russia-leaked-emails-reveal-what-vladimir-putin-tells-world-leaders-at-private-meals/>

Sorry guys, see our disclaimer ☺



Solution: Two-Step Verification?

- If enabled, 2FA is enforced for iCloud backups
 - but not files sideloaded to iCloud Drive
 - ...and not for iCloud-compatible app data
- Overcoming 2FA is easy
 - if the second authentication factor is available
- **Bypassing 2FA is possible**
 - if binary authentication token is extracted from user's PC/Mac



iCloud Authentication Tokens

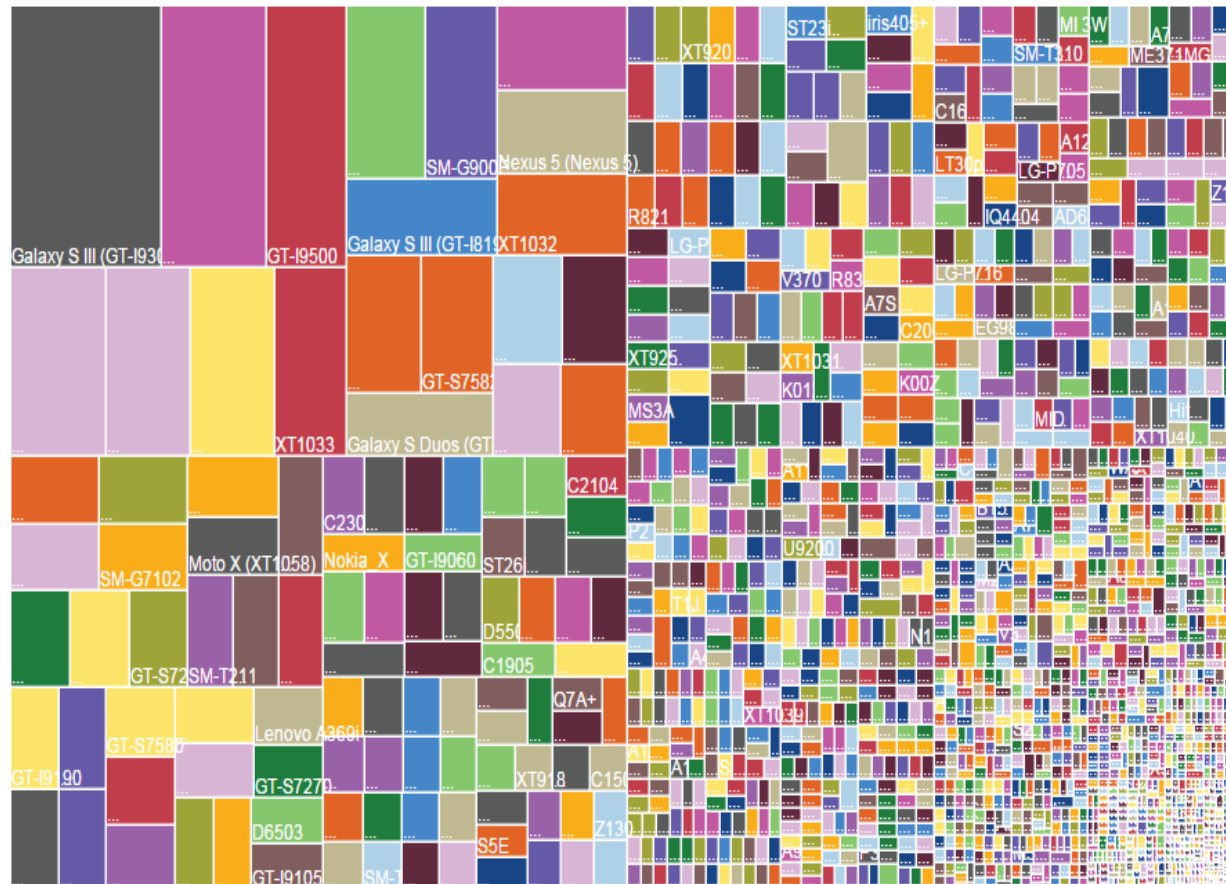
- Authentication tokens are used for convenience
- Saved on a Mac or PC used to access iCloud
- Allow users to avoid entering for Apple ID and password every time
- Technically, an authentication token is **stored in a file** on the user's computer (see figure)
- Locating the file and extracting the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



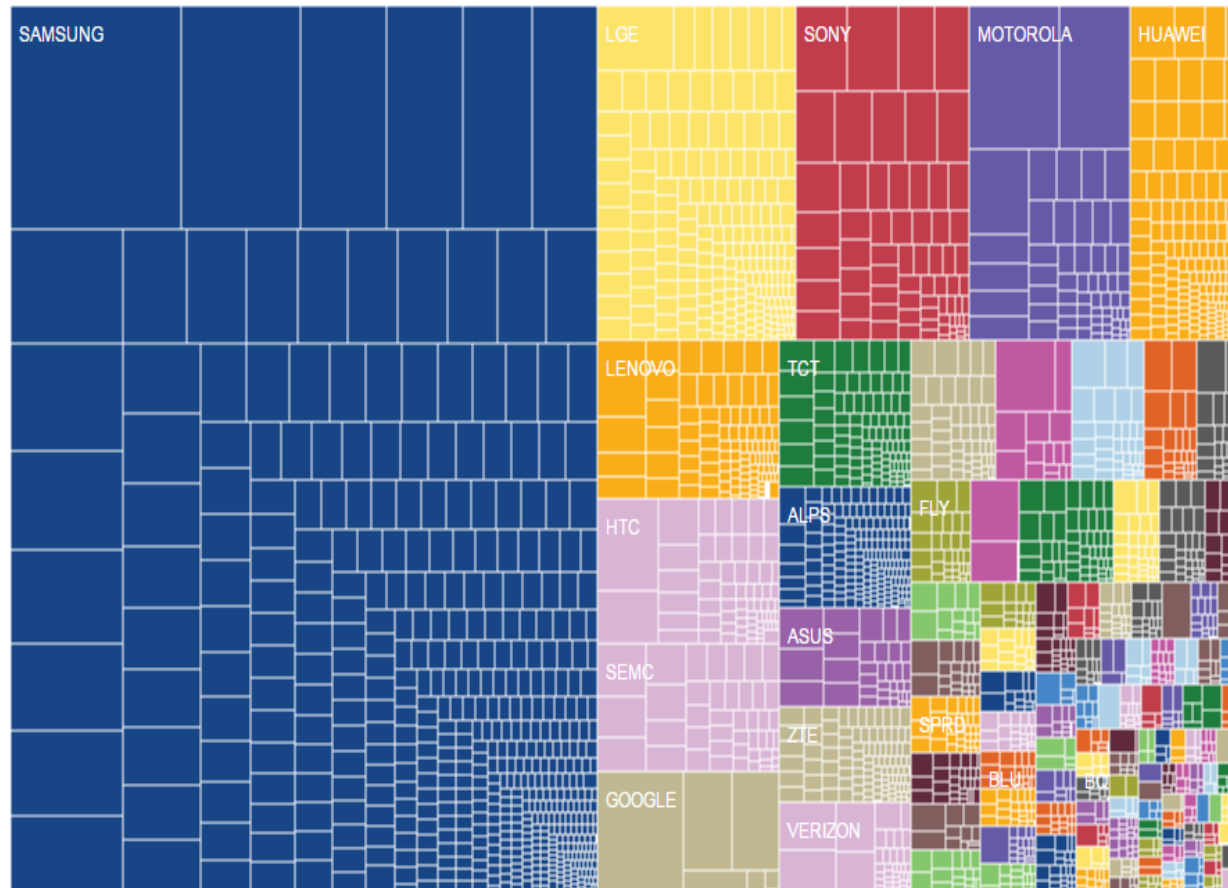
What Authentication Tokens Are Not

- 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

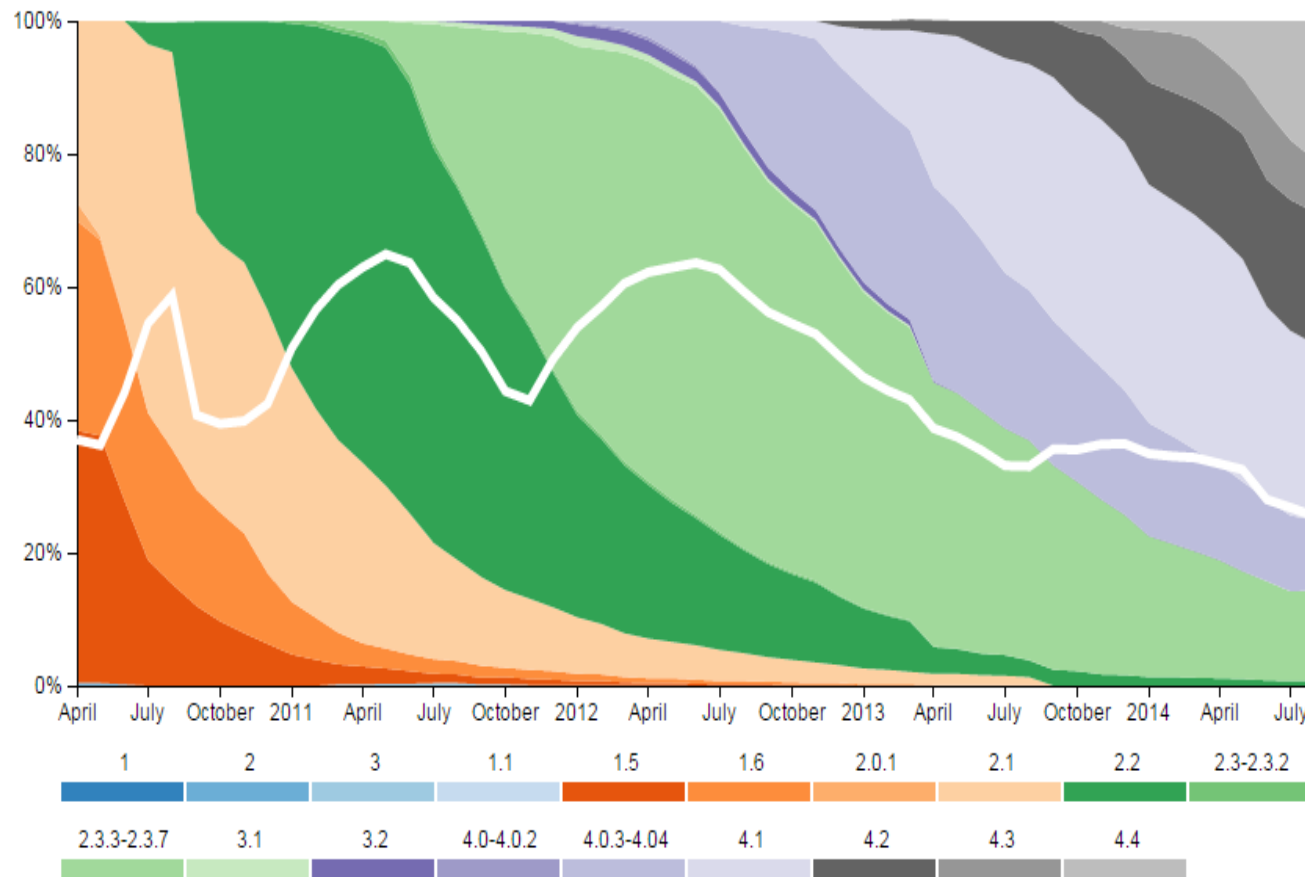
Android device fragmentation



Android brand fragmentation



Android operating system fragmentation



Android to the Rescue? Not So Sure

- user's 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

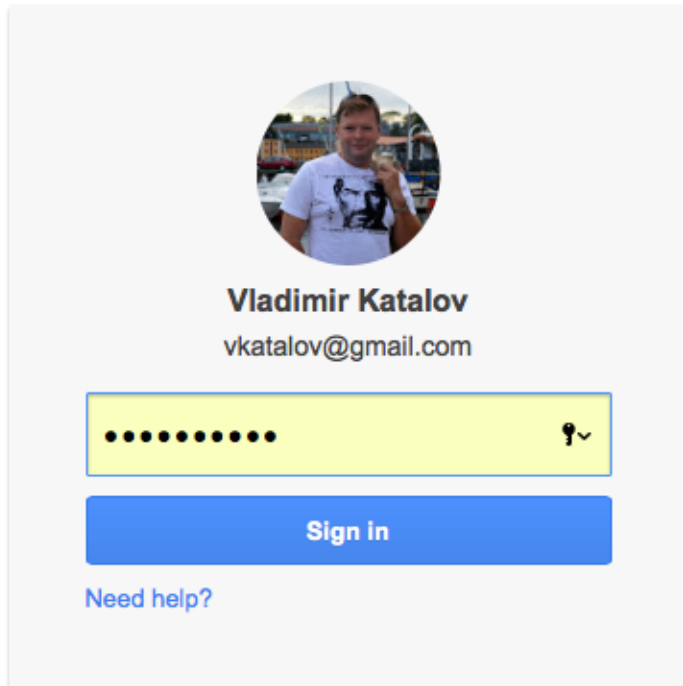


Top 10 Smartphone Apps

(source: comScore report, June 2015)

- | | |
|------------------------|----------------------|
| • Facebook | • Google Maps |
| • YouTube | • Pandora Radio |
| • Facebook Messenger | • Gmail |
| • Google Search | • Instagram |
| • Google Play | • Yahoo Stocks |

Google Sign-On



Google Sign-On interface showing a user profile for Vladimir Katalov (vkatalov@gmail.com) and a password field with a 'Sign in' button. A 'Need help?' link is also visible.

Vladimir Katalov
vkatalov@gmail.com

.....

Sign in

[Need help?](#)



New sign-in from iPhone

Hi Vladimir,
Your Google Account vkatalov@gmail.com was just used to sign in on iPhone.



Vladimir Katalov
vkatalov@gmail.com



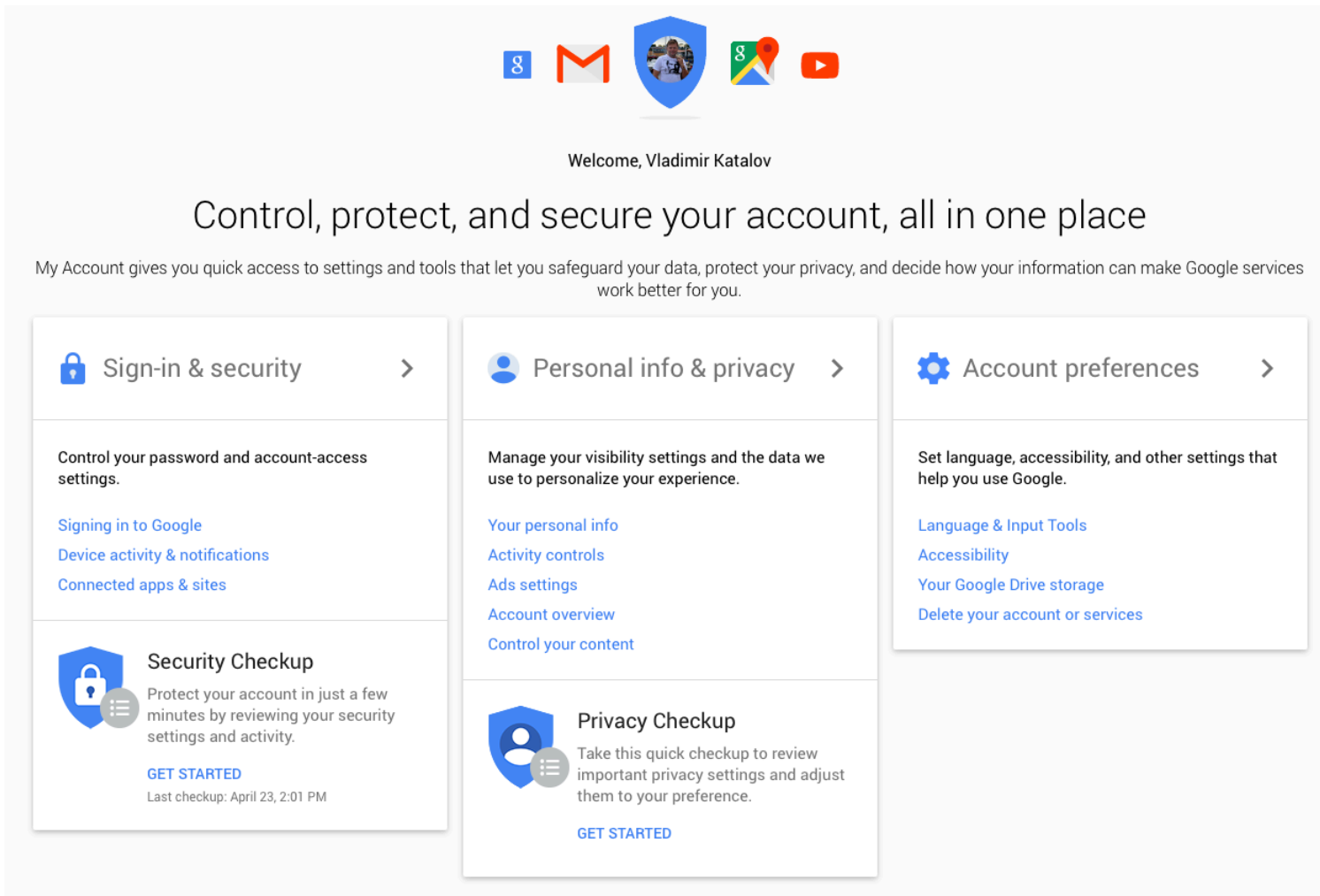
iPhone

Tuesday, August 4, 2015 9:47 PM (Moscow Standard Time)
Yasenevo District, Moscow, Russia*

Don't recognize this activity?

Review your [recently used devices](#) now.

Google Security Settings



The screenshot shows the Google Security Settings interface. At the top, there are icons for Google, Gmail, a profile picture, Google Maps, and YouTube. Below these is the text "Welcome, Vladimir Katalov". The main heading is "Control, protect, and secure your account, all in one place". A subtext explains: "My Account gives you quick access to settings and tools that let you safeguard your data, protect your privacy, and decide how your information can make Google services work better for you." The interface is divided into three main sections: "Sign-in & security", "Personal info & privacy", and "Account preferences". Each section has a list of settings and links. The "Sign-in & security" section includes "Control your password and account-access settings" and a "Security Checkup" button. The "Personal info & privacy" section includes "Manage your visibility settings and the data we use to personalize your experience" and a "Privacy Checkup" button. The "Account preferences" section includes "Set language, accessibility, and other settings that help you use Google".

Welcome, Vladimir Katalov


Control, protect, and secure your account, all in one place

My Account gives you quick access to settings and tools that let you safeguard your data, protect your privacy, and decide how your information can make Google services work better for you.

Sign-in & security

Control your password and account-access settings.

- [Signing in to Google](#)
- [Device activity & notifications](#)
- [Connected apps & sites](#)



Security Checkup

Protect your account in just a few minutes by reviewing your security settings and activity.


[GET STARTED](#)

Last checkup: April 23, 2:01 PM

Personal info & privacy

Manage your visibility settings and the data we use to personalize your experience.

- [Your personal info](#)
- [Activity controls](#)
- [Ads settings](#)
- [Account overview](#)
- [Control your content](#)



Privacy Checkup

Take this quick checkup to review important privacy settings and adjust them to your preference.

[GET STARTED](#)

Account preferences



Set language, accessibility, and other settings that help you use Google.

- [Language & Input Tools](#)
- [Accessibility](#)
- [Your Google Drive storage](#)
- [Delete your account or services](#)

Recent security events and used devices, apps connected, saved passwords

Recent security events

Review security events from the past 28 days.

-  Changed password
August 15, 12:34 PM
-  New iPhone signed in (iPhone 6 VK)
August 4, 9:47 PM

[REVIEW EVENTS](#)

Apps connected to your account

Make sure you still use these apps and want to keep them connected.




-  Google Chrome
-  Auth
-  Chrome Remote Desktop
-  Dropbox

(+23 more)

[MANAGE APPS](#)

Recently used devices

Check when and where specific devices have accessed your account.

-  Mac
CURRENT DEVICE
-  Windows
8 minutes ago
-  iPhone 6 VK
39 minutes ago

(+6 more)

[REVIEW DEVICES](#)

Saved passwords

Manage your passwords from Chrome and Android that are saved with Google Smart Lock.

-  192.168.0.1
-  acdsee.com
-  adobe.com
-  aeroflot.ru

(+76 more)

[MANAGE PASSWORDS](#)

Google Takeout

- Leaves traces
- No all the data is exported
- Limited flexibility
- Not convenient format

Archive	Created on	Available until	Details
22 products 113.5 MB	August 26, 2015		OPEN IN DRIVE

[CREATE NEW ARCHIVE](#) [VIEW HISTORY](#) [DONE](#)

Note: Your content from Google Play Music isn't included when you create an archive. To download your music, use the [Google Play Music Manager](#).

Note: Your past searches aren't included when you create an archive. Learn how to [download your past searches](#).

Your account, your data.
Download a copy.

Create an archive with your data from Google products.


[Manage archives](#)

Select data to include

Choose the Google products to include in your archive and configure the settings for each product. This archive will only be accessible to you. [Learn more](#)

Product	Details	Select none
+1s		<input checked="" type="checkbox"/>
Blogger	All blogs	<input checked="" type="checkbox"/>
Bookmarks		<input checked="" type="checkbox"/>
Calendar	All calendars	<input checked="" type="checkbox"/>
Contacts	vCard format	<input checked="" type="checkbox"/>
Drive	All files PDF and 3 other formats	<input checked="" type="checkbox"/>
Google Photos	All photo albums	<input checked="" type="checkbox"/>

Google Dashboard – account activity

 Account

Name

Vladimir Katalov

Primary email

vkatalov@gmail.com

Manage Account

Change Password

Connected applications and sites

Overview

Nickname

v.katalov

Connected applications and sites

56

Account activity last 28 days

Account sign-ins

Locations:

- Russia (2com co ltd., llc nauka svyaz, maximatelecom jsc, mts ojsc, ojsc comcor, ojsc megafon, star networks)
- Thailand (bb-broadband co., ltd., jastel network, superbroadbandnetwork, triplet internet, true internet co. ltd.)

Platforms:

- iPhone
- Android


[See the full list](#)


Connected applications and sites


Authorized:

- Auth Jul 16, 2015
- Google Chrome Jul 21, 2015
- Sunrise Calendar Aug 5, 2015
- WOT Sign in/up application Jul 31, 2015
- feedly Aug 3, 2015
- iOS Account Manager Aug 4, 2015

Google Dashboard – profile, connected devices & apps

 Profile

About me
5 entries 

Links
4 sites 

Edit Profile

Name

Vladimir Katalov

Profile URL

<https://plus.google.com/+VladimirKatalov>

Email

vkatalov@gmail.com

Phone

+79859986820

Birthday

March 13

+1's










Most recent: [Password recovery, forensic, forensics ElcomSoft : recover or reset lost or forgotten password system on Jun 25, 2015](#)

More links

[About access and privacy of profiles](#)

← Apps connected to your account

You've authorized access to your Google Account for the apps, sites, and devices listed below. [Learn more](#)

	New Nexus	Grants access to apps on this Android device
	Nexus 6	Grants access to apps on this Android device
	Nexus 6	Grants access to apps on this Android device
	Android device	Grants access to apps on this Android device
	iPhone 6 VK	Grants access to apps on this iOS device
	Vladimir Katalov's iPad Air	Grants access to apps on this iOS device
	Google Chrome	Has full access to your Google Account
	Auth	Has some account access, including Google+, basic account info
	BlackBerry	Has access to Gmail, Google Calendar, Google Contacts, basic account info

Google Dashboard – mail



Conversations

14,141

Most recent

[Снижаем цены! СКИДКА 7% на букет...](#)

[Manage Chat History](#)

[Settings](#)

[Privacy and security](#)

Inbox

9,700 conversations

Most recent: [Снижаем цены! СКИДКА 7% на букеты из роз! Только в эти выходные!](#) at 3:47 PM

Sent Mail

3,218 conversations

Most recent: [iPhone](#) on Aug 4, 2015

Saved drafts

1 conversation

Most recent: [Mark Timm Photography](#) on Jun 27, 2015

Chat history

19 conversations

Trash

4 conversations


Most recent: [Самый кассовый фильм августа уже на экранах города!](#) at 1:02 PM

Google Chrome Sync

Chrome Sync

Chrome Sync can save your bookmarks, history, passwords, and other settings securely to your Google Account and allow you to access them from Chrome on any device.

The counts below represent all stored items, including those not visible in Chrome.

Apps	Extensions	Settings
7	7	131
Autofill	Omnibox History	Themes
251	185	1
Bookmarks	Passwords 	Open Tabs
236	141	119

Google Chrome: search & browsing history

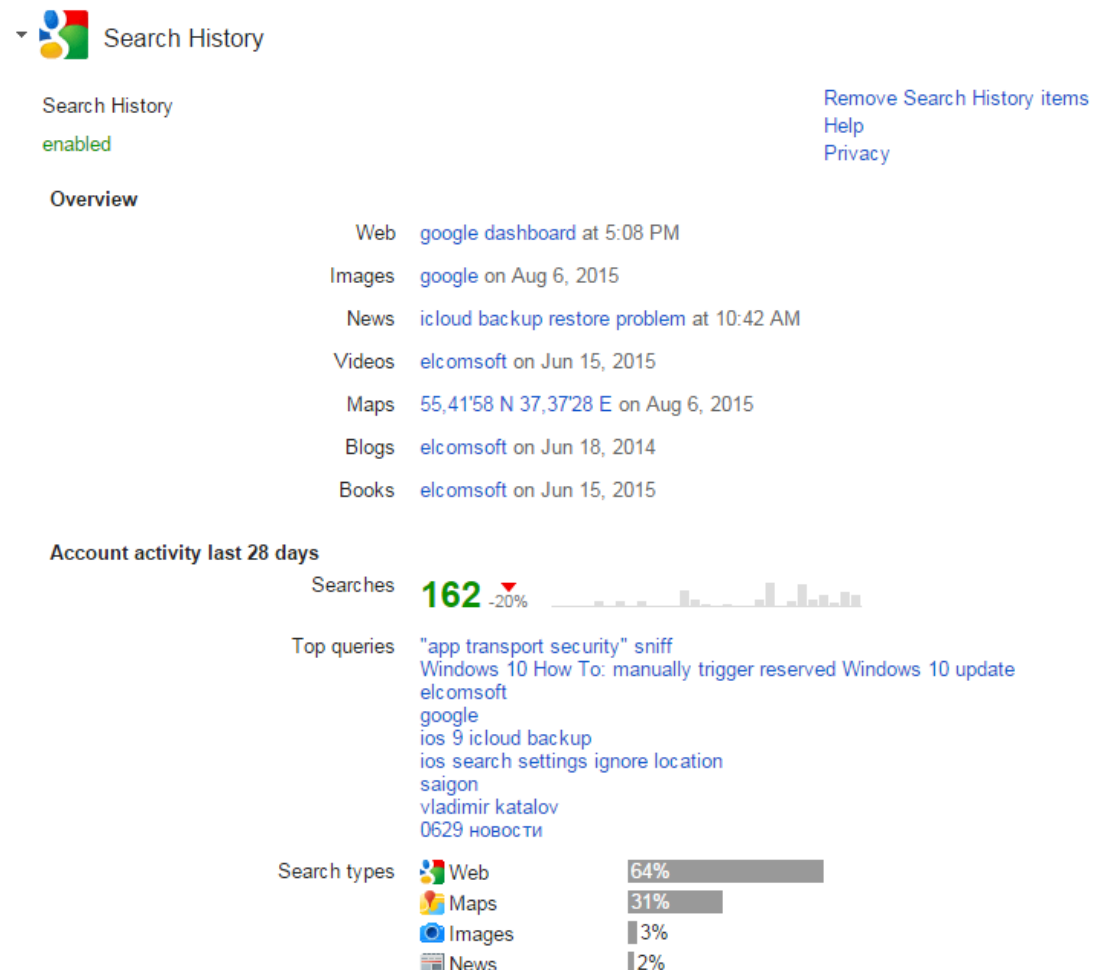
<https://history.google.com/history/>

- 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



Devices

3

- 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

motorola Nexus 6 MTS

IMEI: 355470061393944

Model Name: Nexus 6

Manufacturer: motorola

Carrier: MTS

Last activity seen on: Aug 6, 2015

Registered date: Jun 12, 2015

Applications with backup on servers

Android Wallpaper

Backup date: Aug 2, 2015 3:03 PM

Backup size: 1.31 MB

Android System Settings

Backup date: Aug 3, 2015 8:52 PM

Backup size: 2.51 KB

Android Market

Backup date: Jul 31, 2015 10:40 AM

Backup size: 17 B

Google

Backup date: Aug 5, 2015 6:16 AM

Backup size: 740.37 KB

New Nexus

IMEI: 353490069672588

Model Name: Nexus 5

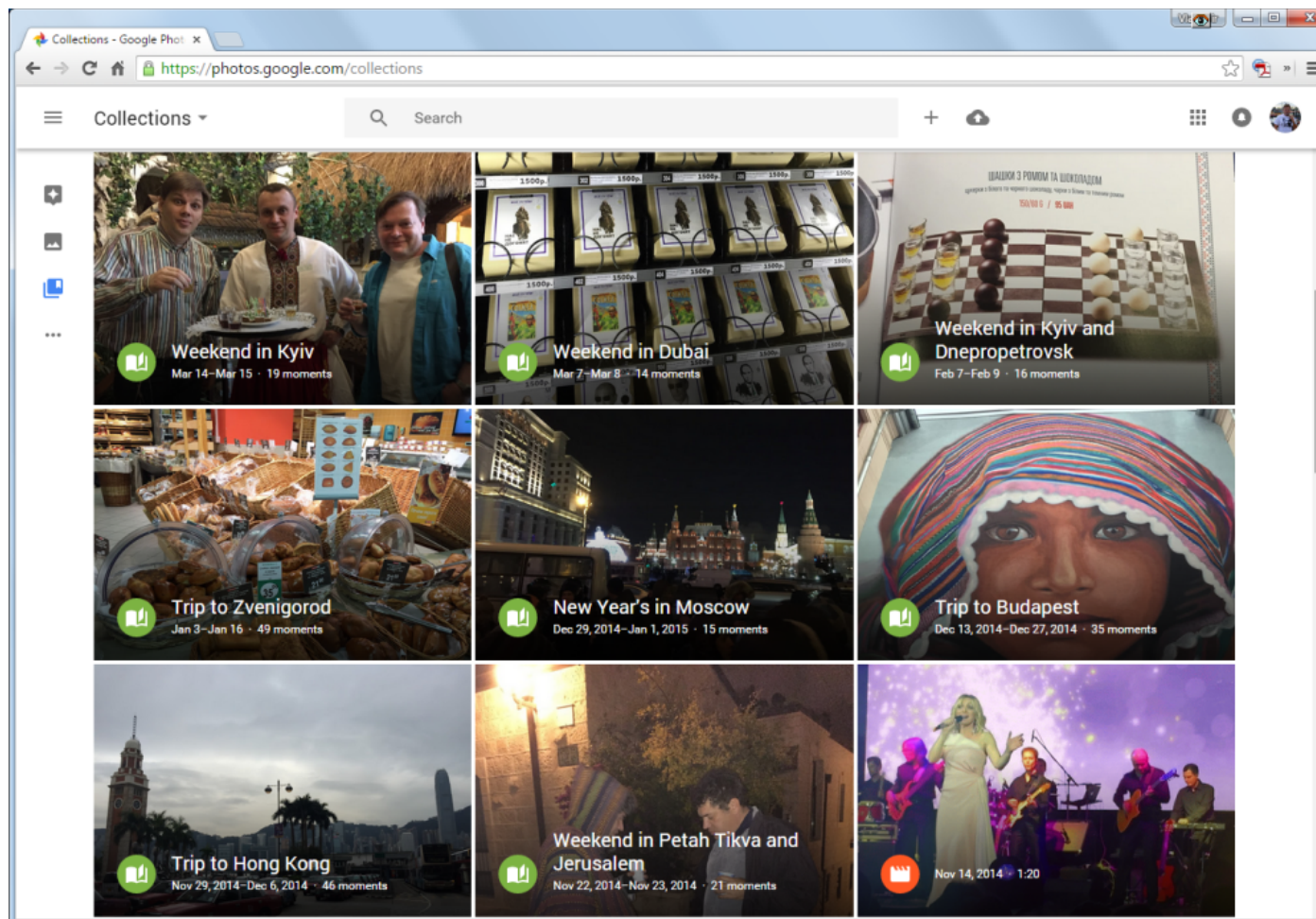
Manufacturer: LGE

Carrier: No carrier

Last activity seen on: Jul 5, 2015

Registered date: Jan 27, 2015

Google Photos (aka PicasaWeb, aka Google+ Photos)



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

Android device backups - downloading

IBackupTransport (com.android.internal.backup in GoogleBackupTransport.apk)

No source code provided; works with <https://android.googleapis.com/backup>

Authentication: <https://android.clients.google.com/auth>

- Get refresh token (input: email, password)
- Get authentication token (input: refresh token)

Get info on backups available: <https://android.googleapis.com/backup>

- Input: android_id, authentication token)
- Output (array)
 - Android_id
 - Backup creation date/time
 - Date/time of device registration on account
 - Device name or model
 - SDK version
 - Last activity date/time

Download backup: <https://android.clients.google.com/backup>

- Input: android_id, package to restore (download), Auth
- Output (array of strings):
 - pm (general info on applications)
 - android (wallpaper: xml + picture)
 - com.android.nfc
 - com.android.providers.settings (including Wi-Fi passwords!)
 - com.android.vending
 - com.google.android.talk
 - com.google.android.googlequicksearchbox
 - com.google.android.calendar
 - com.google.android.inputmethod.latin
 - com.google.android.gm

Android M

- Get system backup (@pm@): <https://android.clients.google.com/googlefood/backup>
- Get backups on particular apps: returns package name, download URL (on Google Drive)
- Authenticate on Google Drive: <https://android.clients.google.com/auth>

New auto-backups for application data; stored on Google Drive as .tar archives

Google Hangouts

https://accounts.google.com/ServiceLogin?hl=en-US&Email={email}

Set-Cookie: GAPS=1:iv-YjJtIF-coJ0RpCZhImMBj97IRA:RKppYacKUG4PUMNX

Set-Cookie: GALX=mltW3iafLoo;Path=/;Secure

https://accounts.google.com/ServiceLoginAuth HTTP/1.1

Cookie: GoogleAccountsLocale_session=en; GAPS=[...]; GALX=[...]&Email={email}&Passwd={password}

Set-Cookie: NID=[...] Set-Cookie: SID=[...] Set-Cookie: LSID=[...]

Set-Cookie: HSID=[...] Set-Cookie: SSID=[...] Set-Cookie: APISID=[...] Set-Cookie: SAPISID=[...]

GET https://talkgadget.google.com/u/0/talkgadget/_/chat?{parameters}

Cookie: NID=[...]; HSID=[...]; SSID=[...]; SID=[...]; APISID=[...]; SAPISID=[...]

Set-Cookie: S=talkgadget=VIFAZCxB-G_h53WWt_g6Q

To get conversation (dialog):

https://clients6.google.com/chat/v1/conversations/getconversation?alt=protojson&key=API_KEY

Cookie: NID=[...];

HSID=[...]; SSID=[...]; SID=[...];

APISID=[...]; [...]

Authorization:SAPISIDHASH {hash}

(SAPISIDHASH: SHA-1(timestamp+SAPISID+URL)

- Dialog data (id, inviteTime, activatedTime)
- Participants' data (id, name, avatarUrl)
- Events (Message, AddUser, RemoveUser, SentPhoto, VideoCall, Location)
- Date/time
- Info on video call: date/time (start+end)
- Text
- Locations (address, mapUrl, latitude, longitude)
- Picture (photoUrl, width, height, album_name)



Obtaining Google Chrome history

POST <https://history.google.com/history/?jspb=1&max=1435697999999999> HTTP/1.1

max=1435697999999999 (in milliseconds since 01.01.1970)

Headers:

Accept: */*

Accept-Language: ru,en-US;q=0.8,en;q=0.6

Connection: keep-alive

Host: history.google.com

Cookie: cookie (obtained after auth-n, includes auth. token)

To get results in English, add to the Cookie:

PREF=ID=1111111111111111:FF=0:LD=en;

YouTube watch history

<https://history.google.com/history/youtube/watch?jspb=1&>


Or

Use YouTube API

<https://developers.google.com/youtube/v3/docs/>

YouTube search history

<https://history.google.com/history/youtube/search?jspb=1&>

▼  YouTube

My videos


5

Overview


Playlists

1

[Manage YouTube account](#)
[Privacy settings](#)
[Connected accounts](#)


Username [vkatalov](#) 

Name [Vladimir Katalov](#) 


Gender [Male](#) 

My videos **5** private **0** public 

Most recent: [Breakthrough in Password Recovery: Thunder Tables and GPUs](#) on Nov 1, 2012

Playlists **0** private **1** public 

Most recent: [Favorites](#) on Aug 25, 2011

Most recent rating [Путин - хуйло в Питере 15.01.15](#) on Jan 19, 2015 

Account activity last 28 days

Viewed videos **27**  

Searches **2**

Votes **0**  **0** 

More links [Manage profile](#)
[Manage history](#)
[Manage search history](#)

Google Drive

Authenticate:

<https://www.googleapis.com/auth/drive>

Get file list:

GET https://www.googleapis.com/drive/v2/files?key={YOUR_API_KEY}

(pretend to be Chromium)

Returns:

- Download URL
- ID
- Parent ID
- If “Shared with me”
 - Owner
 - Access rights
- File name
- File size
- Description
- Properties

Detailed ‘list’ request:

GET [https://www.googleapis.com/drive/v2/files?](https://www.googleapis.com/drive/v2/files?maxResults={MAX_RESULT}&pageToken={PAGE_TOKEN}&fields={FIELDS}&key={YOUR_API_KEY})

[maxResults={MAX_RESULT}&pageToken={PAGE_TOKEN}&fields={FIELDS}&key={YOUR_API_KEY}](https://www.googleapis.com/drive/v2/files?maxResults={MAX_RESULT}&pageToken={PAGE_TOKEN}&fields={FIELDS}&key={YOUR_API_KEY})

{PAGE_TOKEN} – page token

{MAX_RESULT} number of files in response

{FIELDS} fields to return

To get info on particular file, set its ID in the request, provide parameters:

<https://developers.google.com/drive/v2/reference/files/get>

Get file meta data:

GET https://www.googleapis.com/drive/v2/files/fileID?key={YOUR_API_KEY}

Download file:

GET <https://www.googleapis.com/drive/v2/files/fileID?alt=media>

Search by file owner:

https://www.googleapis.com/drive/v2/files?q=not+{your_email_address}'+in+owners

https://www.googleapis.com/drive/v2/files?q='{your_email_address}'+in+owners

Google Photos

Picasa Web Albums Data API

(use OAuth2 to get token)

https://developers.google.com/picasa-web/docs/2.0/developers_guide_protocol

Get albums list:

GET <https://picasaweb.google.com/data/feed/api/user/{userId}>

(userId = default to get own photos; Authorization: token)

Get own album(s):

GET [https://picasaweb.google.com/data/feed/api/user/{USER_ID}/albumid/{ALBUM_ID}?kind=photo&\[..\]](https://picasaweb.google.com/data/feed/api/user/{USER_ID}/albumid/{ALBUM_ID}?kind=photo&[..])

(returns full properties of every album)

Get circles:

POST [https://clients6.google.com/rpc/plusi?key=\[..\]](https://clients6.google.com/rpc/plusi?key=[..])

(returns circles, friends: email, contactId, **obfuscatedGaiId**, displayName)

GET [https://picasaweb.google.com/data/feed/api/user/{USER_ID}/albumid/{ALBUM_ID}?kind=comment&\[..\]](https://picasaweb.google.com/data/feed/api/user/{USER_ID}/albumid/{ALBUM_ID}?kind=comment&[..])

Returns:

- gphoto:id (own id)
- gphoto:photoid
- authorId
- published
- updated
- title
- content

Google Chrome: passwords

```
message PasswordSpecificsData {  
  optional int32 scheme = 1;  
  optional string signon_realm = 2;  
  optional string origin = 3;  
  optional string action = 4;  
  optional string username_element = 5;  
  optional string username_value = 6;  
  optional string password_element = 7;  
  optional string password_value = 8;  
  optional bool ssl_valid = 9;  
  optional bool preferred = 10;  
  optional int64 date_created = 11;  
  optional bool blacklisted = 12;  
  optional int32 type = 13;  
  optional int32 times_used = 14;  
}
```

```
message PasswordSpecifics {  
  optional EncryptedData encrypted = 1;  
  optional PasswordSpecificsData client_only_encrypted_data = 2;  
}
```

Obtaining master encryption keys

Chrome sync

[https://clients4.google.com/chrome-sync/command/?client=Chromium&client_id=\[...\]](https://clients4.google.com/chrome-sync/command/?client=Chromium&client_id=[...])
(body:protobuf with GetUpdatesMessage(need_encryption_key=true))
response: GetUpdatesResponse with entries & encryption key

Get master encryption keys

Key=pbkdf2_sha1(base64(encryption_key)+"saltsalt",1003)
MacKey=pbkdf2_sha1(base64(encryption_key)+"saltsalt",1004)

The keys can be additionally encrypted using the *passphrase* (on the client side)

Google Dashboard: stats we can get

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

Android

- manufacturer, model
- first authorization date/time
- last activity date/time
- apps that backups their data (name, date, size)

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

Profile info

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

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)

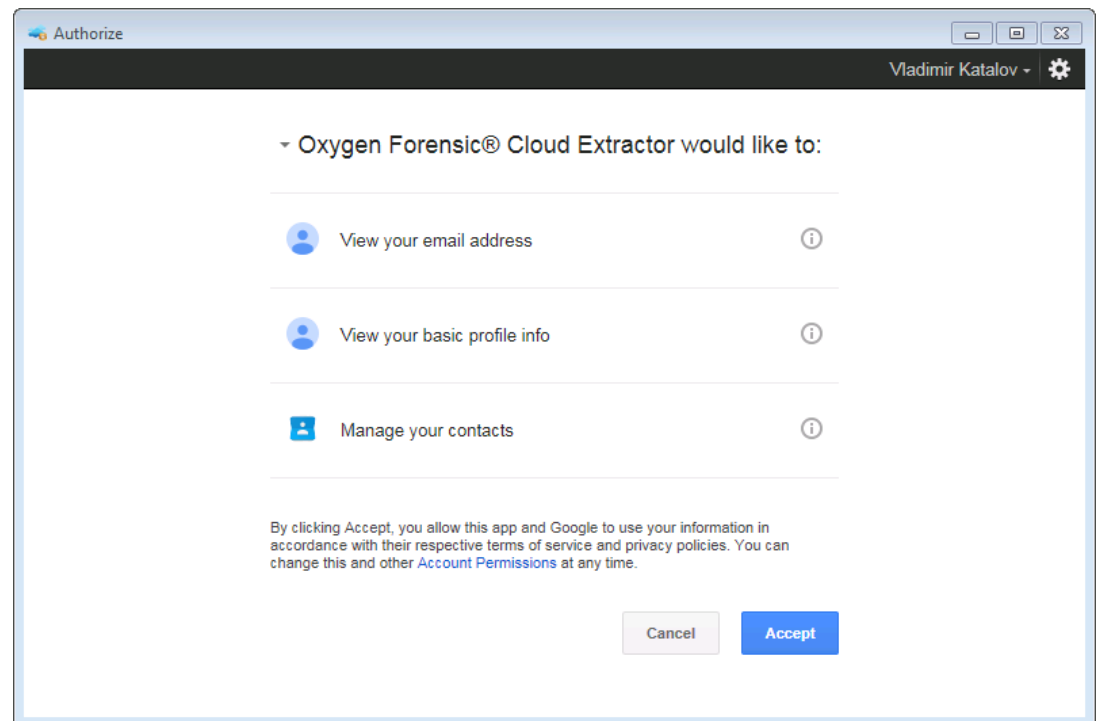
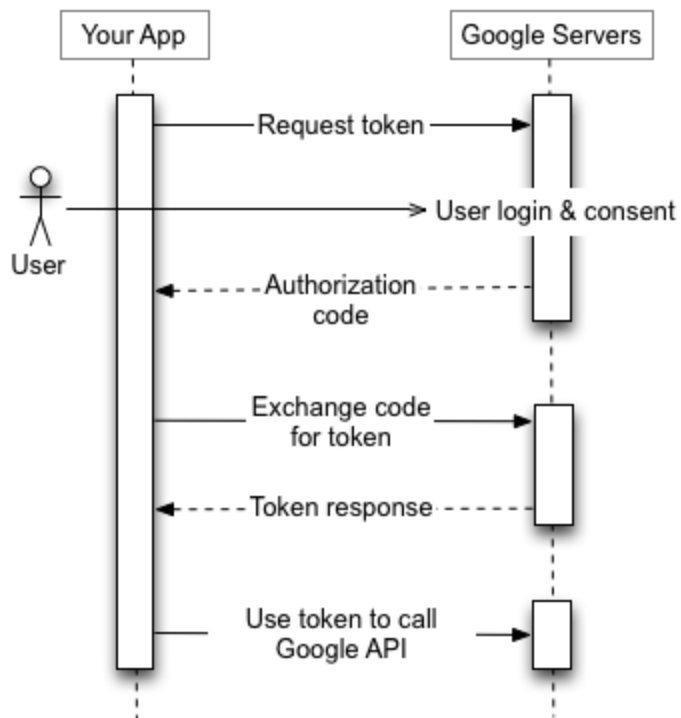
Google Sync. (non-Android devices)

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

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

Google Authentication – the easy way (Oauth 2.0)



Authentication: w/o browser

get loginCookies

<https://accounts.google.com/ServiceLogin?hl=en-US&Email=<login>>
Set-Cookie: GAPS=1:Y5AaGrj-_VQrcWkpM6f75T6H8A:B2wnWWUI2DKLUWCd
Set-Cookie: GALX=EmxneFPdphD;Path=/;Secure

get client_id

POST <https://accounts.google.com/ServiceLoginAuth>
Cookie: GALX=[...]
Set-Cookie: NID=[...]
Set-Cookie: SID=[...]

...

get refresh_token (by client_id, then by client_secret и oauth_code)

https://accounts.google.com/o/oauth2/programmatic_auth?authuser=0
Set-Cookie: oauth_code=4/5xOmK7KEXG70-3cYAJu66pp8sx1U4FyCIRWI_J1zQ
<https://accounts.google.com/o/oauth2/token>

```
{  
  "access_token": "ya29.yAHuL5IPQW63Yn90hVETqe95ueyM8SpoqhyqPmy-hTywd4chkANfQTt0VNeTBMQhrkw",  
  "refresh_token": "1/sIXyWGQPs1IVI7t-VC3_VKWSWUYJONt1Ue8tRG-pc"  
}
```

get access_token

<https://accounts.google.com/o/oauth2/token> HTTP/1.1
client_id=[...]&client_secret=[...]&grant_type=refresh_token&refresh_token=[...]&scope=[...]

Calendar

<https://www.googleapis.com/auth/calendar.readonly>

Contacts

<https://www.googleapis.com/auth/contacts.readonly>

User info

<https://www.googleapis.com/auth/userinfo.profile>

Chrome data

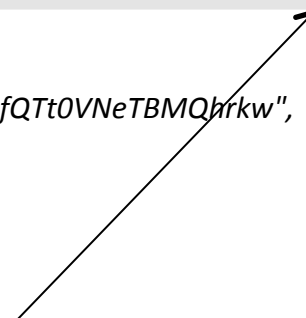
<https://www.googleapis.com/auth/chromesync>

Photos

<https://picasaweb.google.com/data/>

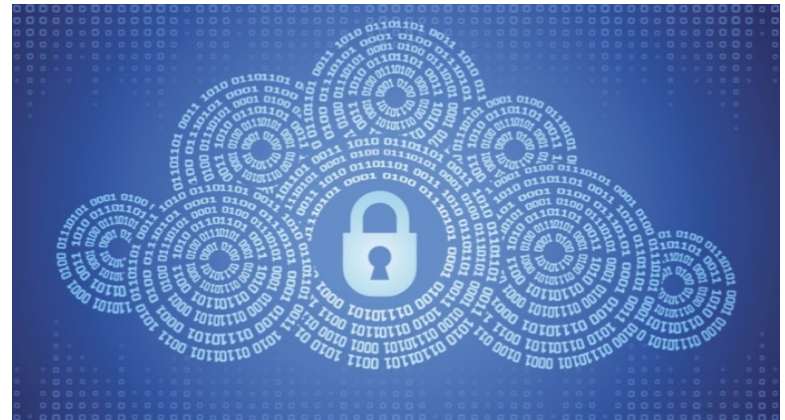
Google drive

<https://www.googleapis.com/auth/drive>



How *Hackers* Get Passwords

- Phishing
- Brute-force attacks
- “Reverse” brute-force attacks
- Password reset/recovery
- Key loggers
- Fake AP
- Network sniffing
- Social engineering
- Passwords re-use



Please confirm your apple ID.

Confirmation of your Apple ID gives you easy access to a variety of Apple services, including the iTunes Store, Apple Online Store, iChat, and more. We will not share your information with anyone else unless you authorize us to do so.

[confirm Now](#)

How *LE* Get Passwords

- Same way as hackers
- Surveillance
- From suspect's PC or Mac
- Direct access to cloud storage
- Just ask 😊



How to protect yourself?

- Do not use clouds*
- Do not keep sensitive information on smartphone*
- Use 3rd party encryption apps**
- Avoid phishing
- Think of physical security
- Use a strong password
- Change the password regularly
- Pay attention to notification emails
- Enable two-step verification

(*) Not actually possible

(**) Bad advise



What Google knows about you and your devices (and how to get it)

Vladimir Katalov, ElcomSoft Co. Ltd.

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

Facebook: ElcomSoft

Twitter: @elcomsoft

