

Hackinbo 2018



ELCOMSOFT

Cloud Forensics: Google

Extracting Google Account data

Google Forensics

In This Presentation

- Cloud and Over-the-Air Acquisition
- Synchronized data
- Passwords
- Two-Factor Authentication

```
* The coordinates (0, 0, 0) represents the octocube
*/
class GeoOctocube {
    /**
```

* Gets the sector from the (x, y, z) specified

* Sector will be:

* <code>



* @param int \$x the x coordinate
* @param int \$y the y coordinate
* @param int \$z the z coordinate

* @return int the number of the sector (0 if x =

```
static function get_sector ($x, $y, $z) {
```

Cloud Forensics

Cloud Acquisition: Why?

- Helps dealing with **locked** and **encrypted** devices
 - Android 6 and up encrypted by default
- Google Account may contain more data than the phone itself
- Last resort: may succeed where all other methods fail
- Google collects information from **all** signed-in devices



Cloud Forensics

Cloud Acquisition Helps Bypass All of This:

- **Secure Lock Screen**
- **Locked Bootloader**
- **Factory Reset Protection (FRP)**
- **Full-Disk Encryption (FDE) and File-Based Encryption (FBE)**
- **Device is broken, wiped, or locked**



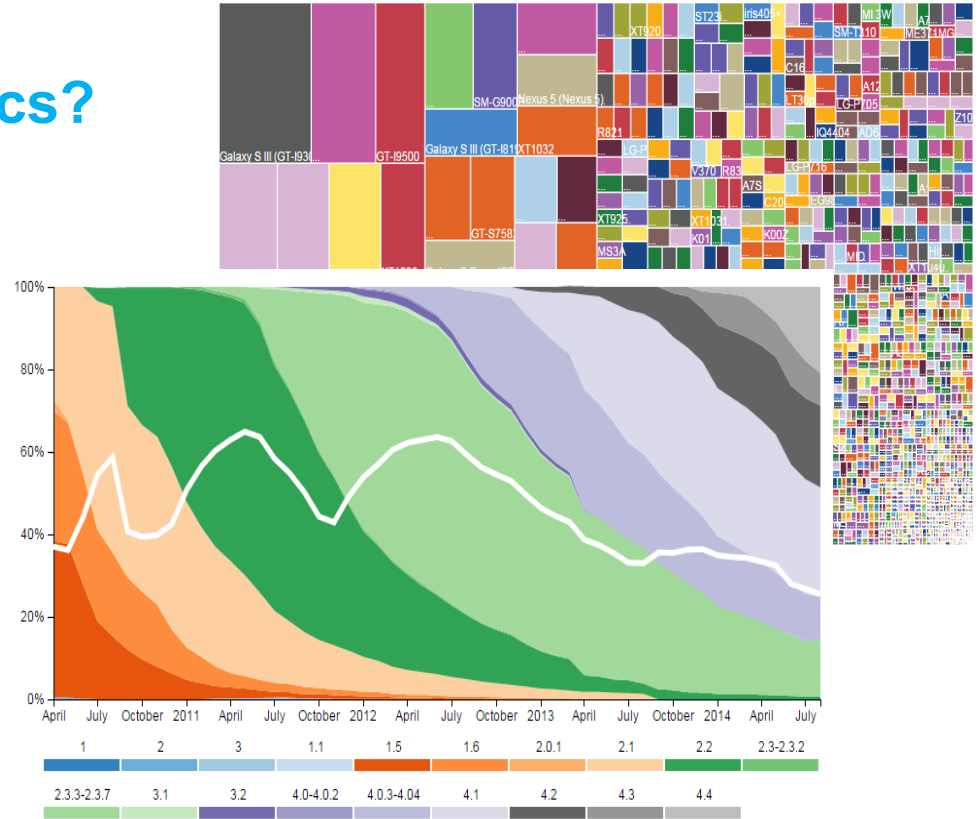
Google Forensics

Google: Why Cloud Forensics?

- Tens of thousand device models
- Several thousand manufacturers
- Extreme platform fragmentation
- Not every Android device is a Google device
- Acquisition approaches vary

Google Account acquisition

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



Google Forensics

Android Open Source vs. Google Mobile Services

- Not every Android device is a Google device
- AOSP does not mean GMS
- Google collects data from other sources if user signs in to:
 - Chrome browser
 - Google Maps
 - Gmail
 - Google Search
- **Including competing platforms**



Google Forensics

Google Collects Data from Multiple Sources

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

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](#)

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) → + 6 more

[REVIEW DEVICES](#)

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) → + 23 more

[MANAGE APPS](#)

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) → + 76 more

[MANAGE PASSWORDS](#)

Google Forensics

Google Account: What's 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



Top 10 Smartphone Apps

(source: comScore report, June 2015)

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

Google Forensics

Google Takeout

- Leaves traces
- Not everything is exported
- Limited flexibility
- Numerous awkward formats

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 Play Books	All books HTML format	<input checked="" type="checkbox"/>
Google+ Circles	vCard format	<input checked="" type="checkbox"/>
Google+ Pages	All pages HTML format	<input checked="" type="checkbox"/>

Google+ Stream	HTML format	<input checked="" type="checkbox"/>
Groups		<input checked="" type="checkbox"/>
Hangouts		<input checked="" type="checkbox"/>
Keep		<input checked="" type="checkbox"/>
Location History	JSON format	<input checked="" type="checkbox"/>
Mail	All mail	<input checked="" type="checkbox"/>
Maps (your places)		<input checked="" type="checkbox"/>
My Maps		<input checked="" type="checkbox"/>
Profile		<input checked="" type="checkbox"/>
Tasks		<input checked="" type="checkbox"/>
Voice		<input checked="" type="checkbox"/>
Wallet		<input checked="" type="checkbox"/>
YouTube	All data types OPML (RSS) format	<input checked="" type="checkbox"/>

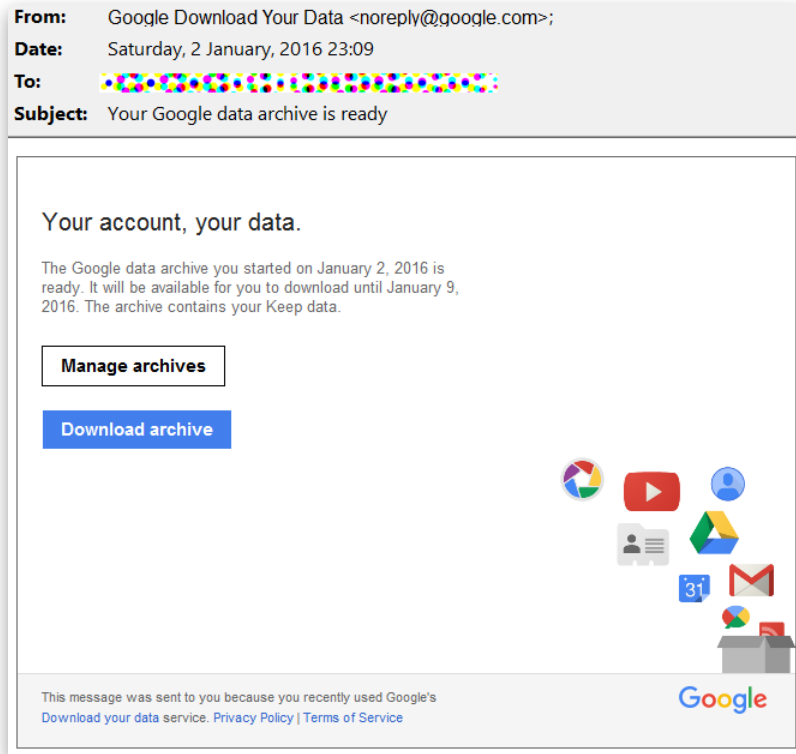
[Next](#)

Customize download format

Google Forensics

Google Takeout

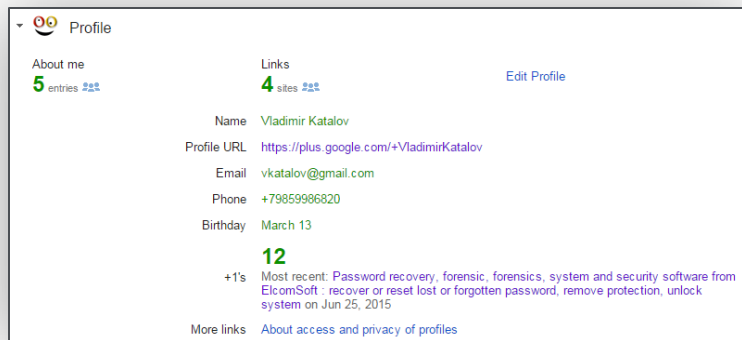
- User alerted via email
- Example of email alert >>



Google Forensics

Google Dashboard – Account Activity

- Not available via Google Takeout



Profile

About me **5** entries #2*

Links **4** sites #2*

Edit Profile

Name **Vladimir Katalov**

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

Email vkatalov@gmail.com

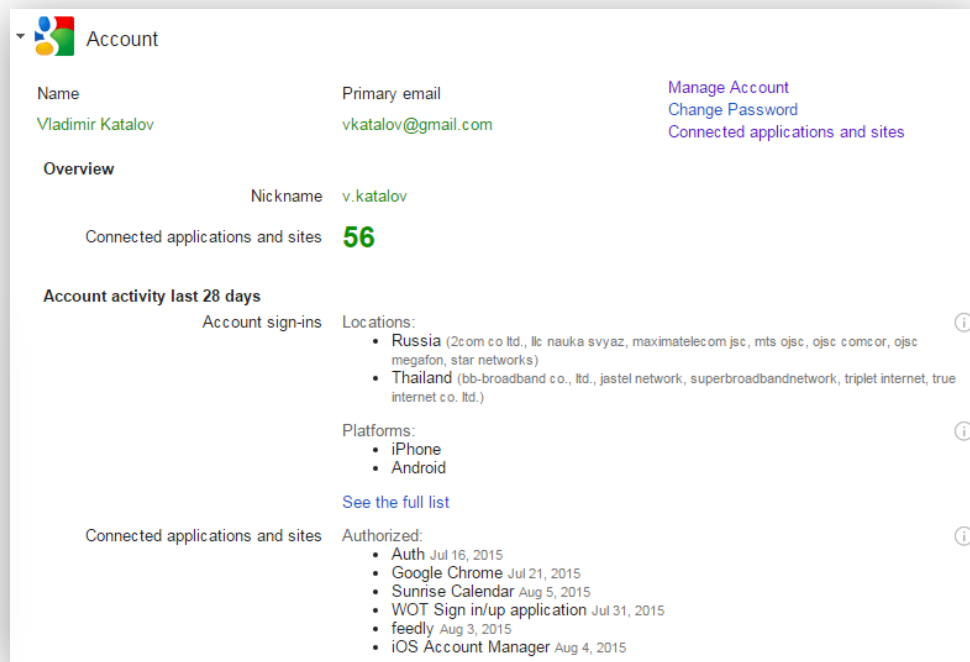
Phone **+79859986820**

Birthday **March 13**

12 +1's

Most recent: Password recovery, forensic, forensics, system and security software from ElcomSoft : recover or reset lost or forgotten password, remove protection, unlock system on Jun 25, 2015

More links [About access and privacy of profiles](#)



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 Forensics

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)

Google Forensics

Chrome Sync

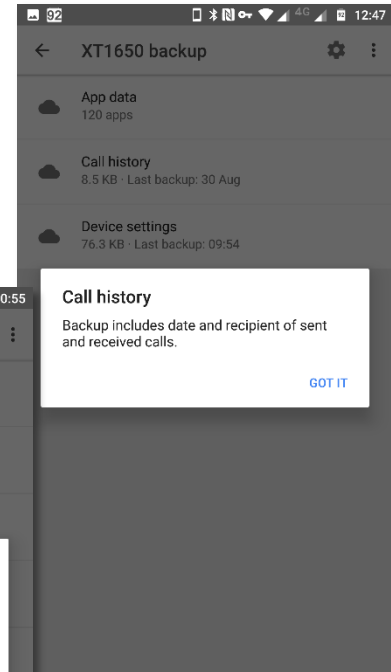
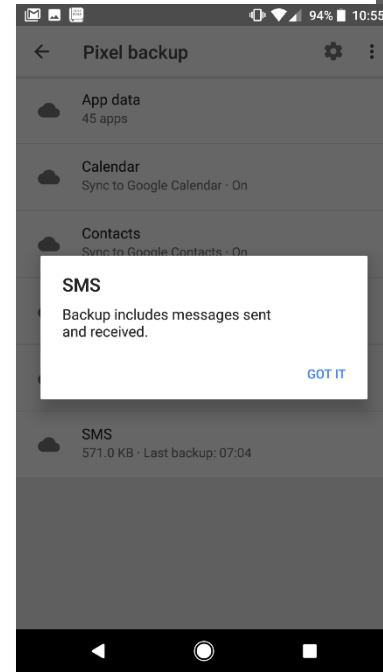
- All signed-in devices
- Bookmarks
- Browsing history
- Open tabs
- Forms
- **Passwords**
- Page transitions
- Some data not saved by Google Takeout

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 Forensics

Calls 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



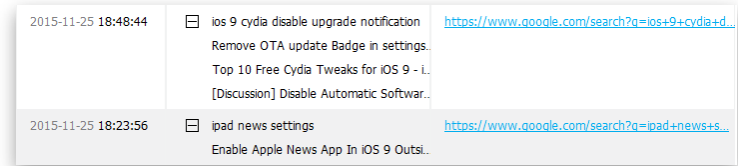
Google Forensics

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



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:

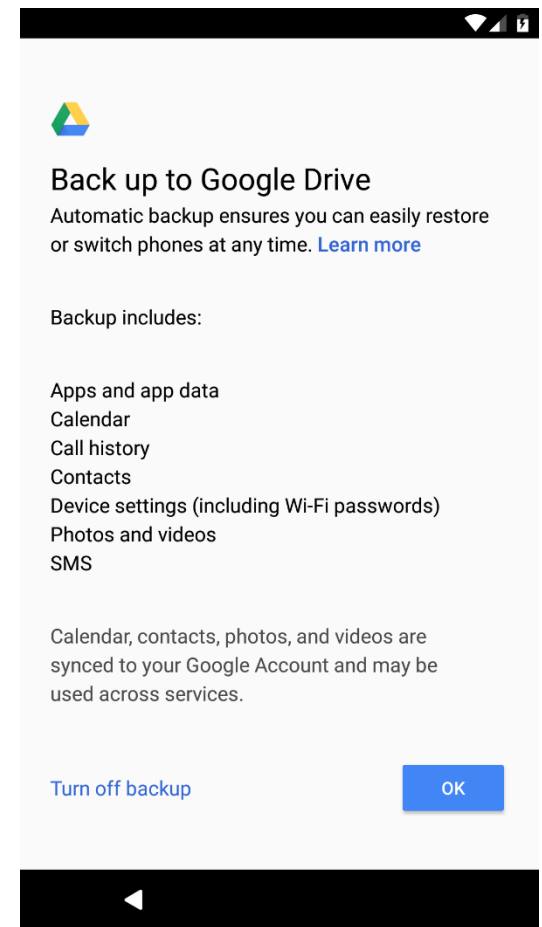
- Searches in all Google services
- Browser or mobile application
- Actions for search results (opened or not)
- Actions on Ads (clicks/purchases)
- IP address
- Browser information

Google Takeout does NOT work with history

Google Forensics

Android Device Backups

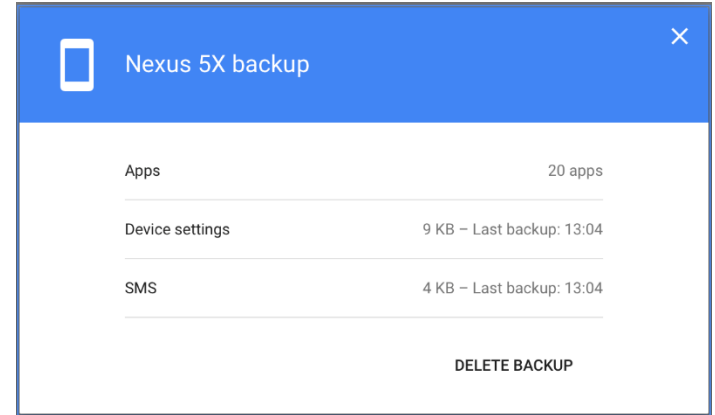
- Google Calendar settings
- Wi-Fi networks & password
- Home screen wallpapers
- Gmail settings
- Apps installed through Google Play
- Display settings
- Language & Input settings
- Date & Time
- 3rd party app settings & data (extremely limited)



Google Forensics

Android Device Backups: Limitations

- 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 not using backups for its own apps
- Facebook disables backups as well
- Yes, even in Android 8.0



Google Forensics

Google Photos

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

The screenshot displays the Google Photos web interface for a user named vkatslov@gmail.com. The interface is divided into several sections:

- Google accounts:** A sidebar on the left lists various photos with their timestamps, such as "16.09.2016 15:35:57" and "29.03.2017 14:53:09".
- Media Overview:** The main area shows a grid of photo thumbnails. At the top, it displays summary statistics: "Files in backup: 11074 (20.67 GB)", "Files are shown: 49 (179.01 MB)", "Images: 10916 (17.59 GB)", "Videos: 146 (2.53 GB)", "Gf: 120 (236.75 MB)", "Images: 49 (179.01 MB)", and "Videos: 0".
- Filters and Controls:** On the right, there are filters for "Date Created" (From: 22.02.2013, To: 29.03.2017), "Media type" (Photos, Videos, Gf), and "Media source" (Ekomssoft Lab, Saturday after..., Shooting Jan'17, Sunday in Mos..., Lu-Gri, Trip to Tiewad..., 2017-03-06, 2017-03-08, 2017-03-09, 2017-03-03, 2017-03-03, 2017-03-03, 2017-03-03, 2017-03-03, 2017-03-03, 2017-03-12, 2017-03-12, 2017-03-12, Sunday in Reutov, Trip to London, Other media).
- Navigation:** The bottom of the interface features a navigation bar with a camera icon and a trash icon.

Google Forensics


Google Account
Acquisition:

Elcomsoft Cloud
Explorer

- Google ID + password

Download snapshot

Google ID (example@example.com)

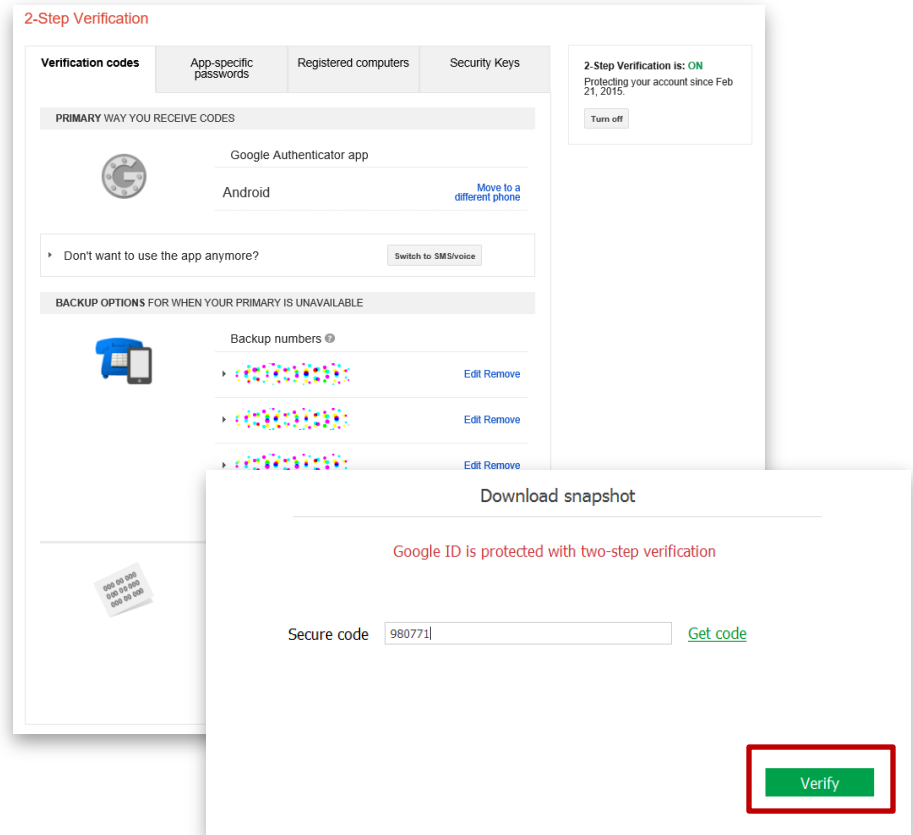
Password 

Save credentials for future use [?](#)

Google Forensics

Two-factor authentication

- Google relies on OATH tokens via Google Authenticator app
- Generic authenticator apps are compatible
- Single-use backup codes
- Must have access to the secondary authentication factor



Google Forensics

What's Available via Elcomsoft Cloud Explorer

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

Download snapshot ?

Select data categories to download

<input checked="" type="checkbox"/> User Info	<input checked="" type="checkbox"/> Chrome	<input checked="" type="checkbox"/> Calls
<input checked="" type="checkbox"/> Dashboard	<input checked="" type="checkbox"/> Calendars	<input checked="" type="checkbox"/> Wi-Fi
<input checked="" type="checkbox"/> Chats	<input checked="" type="checkbox"/> Locations	<input checked="" type="checkbox"/> Mail (35654 mails)
<input checked="" type="checkbox"/> Contacts	<input checked="" type="checkbox"/> Media (17221 files)	Add date filter
<input checked="" type="checkbox"/> Google Keep	<input checked="" type="checkbox"/> History	<input checked="" type="checkbox"/> Messages

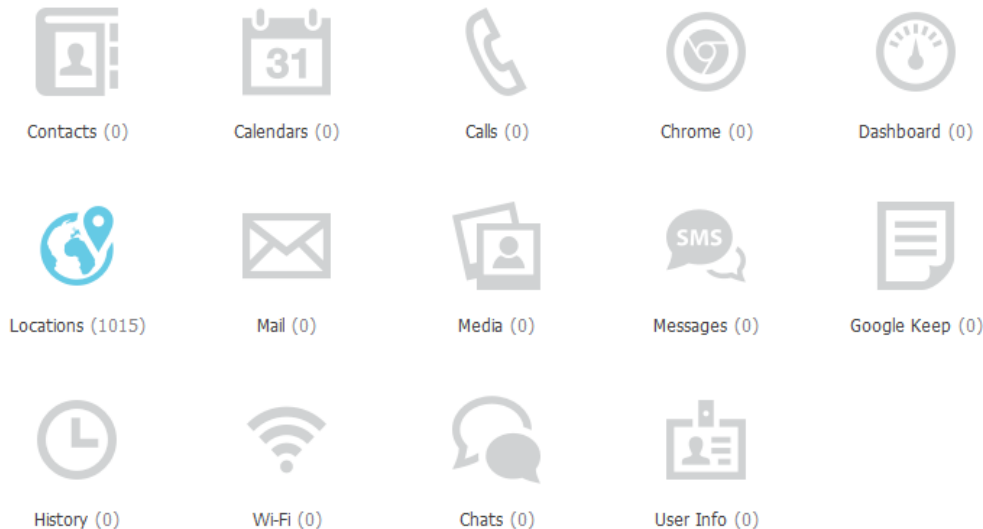
[Check All](#) [Uncheck All](#)

Download

Google Forensics

Built-in Viewer

- Explore user's Google Account
- Navigate by category
- Search messages, view pictures, access calendar events etc.



Google Forensics

Passwords

- Data from Google Chrome
- Synced between all signed-in devices
- Not just Android
- **Screenshot:** sorry, we masked the actual usernames and passwords :)
- Also available: bookmarks, page transitions

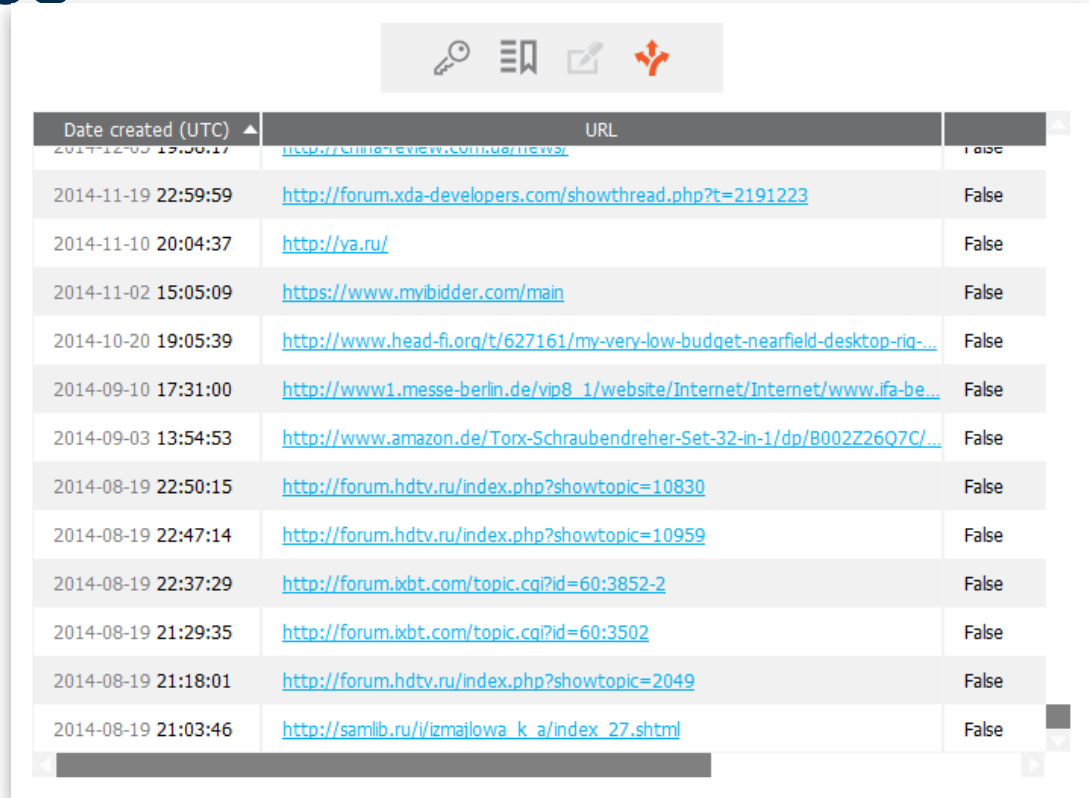


URL	User name	Password	Times used
ood.com/login.html	[Masked]	*****	0
en.de/kundenkonto/login	[Masked]	*****	3
n/auth	[Masked]	*****	0
endyhandy.de/shop/addb2b.html	[Masked]	*****	0
de/user/login	[Masked]	*****	1
oogle.com/ServiceLoginAuth	[Masked]	*****	0
ed.com/de/j_spring_security_check;jses...	[Masked]	*****	0
qi-bin/luci/web	[Masked]	*****	0
areversand.de/profilreqis.jsp	[Masked]	*****	0
sbilliger.de/e/	[Masked]	*****	0
j/blog/reg/	[Masked]	*****	0
nline.com/websec/loqon.html;jsessionid...	[Masked]	****	9
-banking.lbb.de/Amazon/cas/dispatch...	[Masked]	*****	0
e.html	[Masked]	*****	0
on.fr/ap/signin	[Masked]	*****	3

Google Forensics

Page Transitions

- Where did the user go after firing a search?
- Data comes from:
 - Google Chrome
 - Google searches on other browsers (if signed-in)



The screenshot shows the Google Chrome Page Transitions tool interface. At the top, there are four icons: a magnifying glass, a bookmark icon, a pencil, and a red double-headed arrow. Below the icons is a table with two columns: 'Date created (UTC)' and 'URL'. The table contains 13 rows of data, each representing a page transition. The 'Date created (UTC)' column shows dates and times in UTC, and the 'URL' column shows the corresponding web addresses. The 'False' column indicates that the page was not visited directly from a search engine.

Date created (UTC)	URL	
2014-12-09 19:30:17	https://chrome-review.com/user/news/	False
2014-11-19 22:59:59	http://forum.xda-developers.com/showthread.php?t=2191223	False
2014-11-10 20:04:37	http://ya.ru/	False
2014-11-02 15:05:09	https://www.mvbidder.com/main	False
2014-10-20 19:05:39	http://www.head-fi.org/t/627161/my-very-low-budget-nearfield-desktop-rig-...	False
2014-09-10 17:31:00	http://www1.messe-berlin.de/vip8_1/website/Internet/Internet/www.ifa-be...	False
2014-09-03 13:54:53	http://www.amazon.de/Torx-Schraubendreher-Set-32-in-1/dp/B002Z26Q7C/...	False
2014-08-19 22:50:15	http://forum.hdtv.ru/index.php?showtopic=10830	False
2014-08-19 22:47:14	http://forum.hdtv.ru/index.php?showtopic=10959	False
2014-08-19 22:37:29	http://forum.ixbt.com/topic.cgi?id=60:3852-2	False
2014-08-19 21:29:35	http://forum.ixbt.com/topic.cgi?id=60:3502	False
2014-08-19 21:18:01	http://forum.hdtv.ru/index.php?showtopic=2049	False
2014-08-19 21:03:46	http://samlib.ru/i/izmajlova_k_a/index_27.shtml	False

Google Forensics

Search History

- Combined data
- Google Chrome
- Google searches in other browsers (signed-in)
- All platforms (desktops, laptops, tablets, phones)

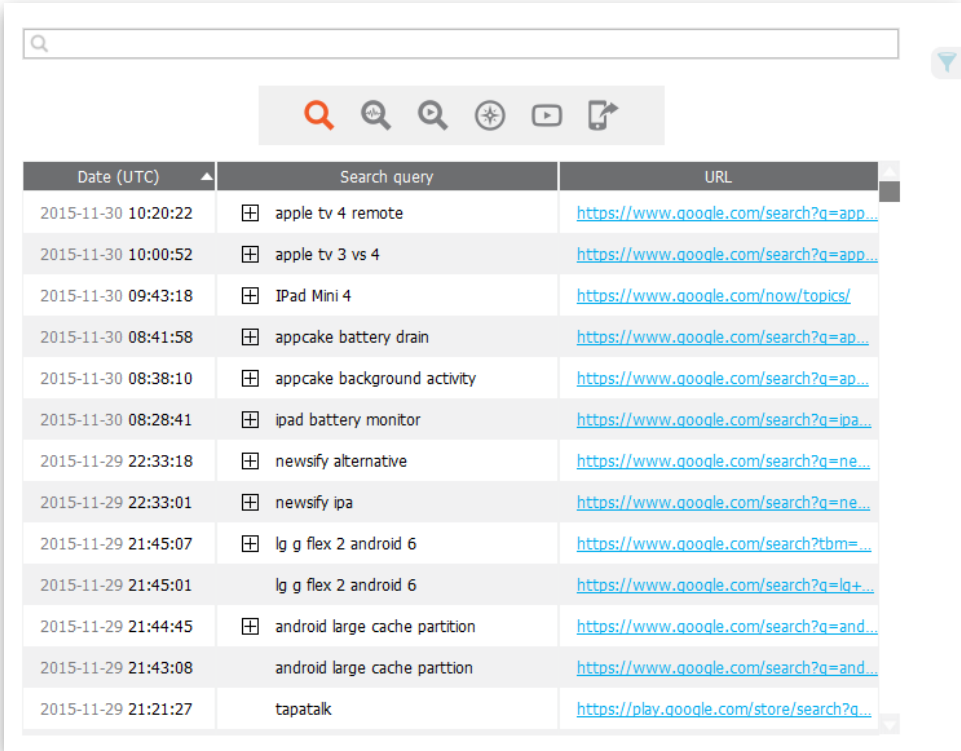
The screenshot displays a mobile interface for viewing search history. At the top, there is a horizontal toolbar containing icons for Android, a calendar, a list, a search magnifying glass, a video player, an email, a location pin, and a Google logo. Below the toolbar, the title "Search history" is centered. A blue header bar labeled "Activities" is followed by a white box containing the text "Delta: 27" and "Searches 976". Another blue header bar labeled "Top Queries" is positioned above a table. The table has two columns: "Query" and "Url".

Query	Url
kaeppel new school	https://www.google.com/search?q=kaeppel+new+school
lumia 640 blue gray background	https://www.google.com/search?tbm=isch&q=lumia+640+blue+gray...
lumia 640 stock wallpaper	https://www.google.com/search?q=lumia+640+stock+wallpaper
BLUBOO XTOUCH	https://www.google.com/search?q=BLUBOO+XTOUCH
KAEPPEL MAKO SATIN BETTWÄSCHE	https://www.google.com/search?q=KAEPPEL+MAKO+SATIN+BETT...

Google Forensics

Browsing History

- Before Android 6.0
 - Browsing history easily available to “monitoring” apps
- Android 6.0 and up
 - Access to browsing history is limited
 - No “monitoring” app can access browsing history without root
 - This data can still be extracted from the cloud
- Android 6 market share: 32.2% (Sep 2017), Android 7: 15.8%
<https://developer.android.com/about/dashboards/index.html>

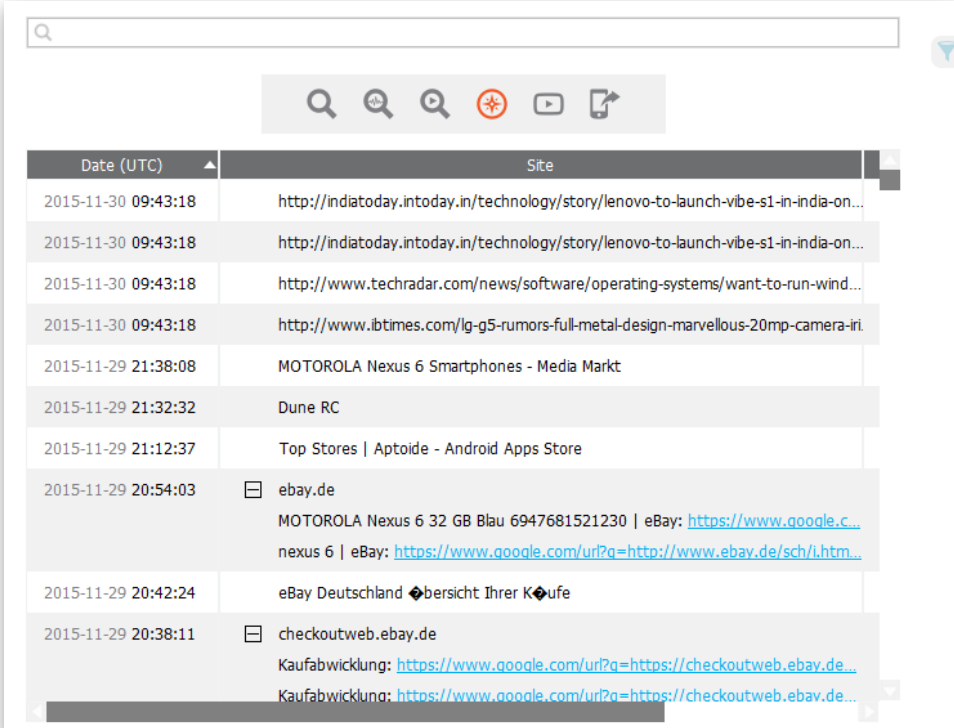


Date (UTC)	Search query	URL
2015-11-30 10:20:22	apple tv 4 remote	https://www.google.com/search?q=app...
2015-11-30 10:00:52	apple tv 3 vs 4	https://www.google.com/search?q=app...
2015-11-30 09:43:18	iPad Mini 4	https://www.google.com/now/topics/
2015-11-30 08:41:58	appcake battery drain	https://www.google.com/search?q=ap...
2015-11-30 08:38:10	appcake background activity	https://www.google.com/search?q=ap...
2015-11-30 08:28:41	ipad battery monitor	https://www.google.com/search?q=ipa...
2015-11-29 22:33:18	newsify alternative	https://www.google.com/search?q=ne...
2015-11-29 22:33:01	newsify ipa	https://www.google.com/search?q=ne...
2015-11-29 21:45:07	lg g flex 2 android 6	https://www.google.com/search?tbm=...
2015-11-29 21:45:01	lg g flex 2 android 6	https://www.google.com/search?q=lg+...
2015-11-29 21:44:45	android large cache partition	https://www.google.com/search?q=and...
2015-11-29 21:43:08	android large cache parttion	https://www.google.com/search?q=and...
2015-11-29 21:21:27	tapataik	https://play.google.com/store/search?q...

Google Forensics

Browsing History

- Can be viewed as a tree
- Convenient per-domain grouping
- Page title and URL (where available)



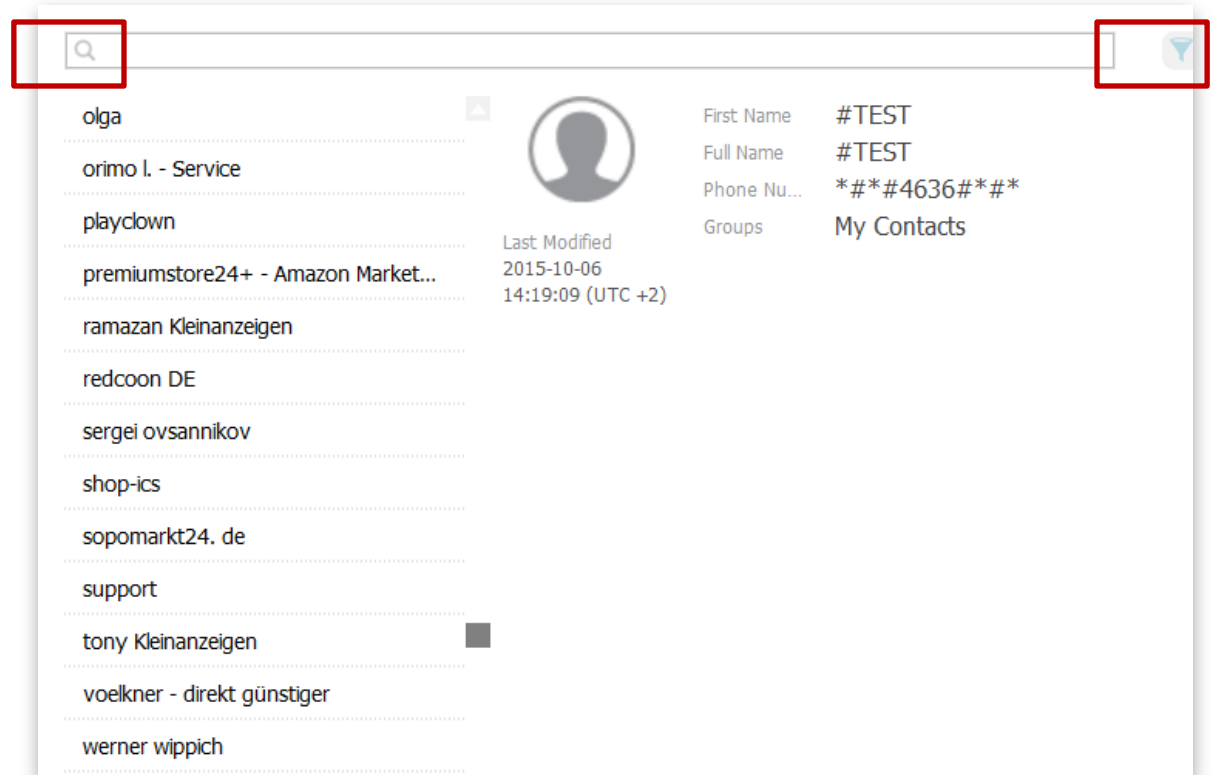
The screenshot shows the Google Chrome Browsing History interface. At the top, there is a search bar and a toolbar with icons for search, zoom, back, refresh, forward, and share. Below the toolbar is a table of browsing history entries. The table has two columns: 'Date (UTC)' and 'Site'. The entries are as follows:

Date (UTC)	Site
2015-11-30 09:43:18	http://indiatoday.intoday.in/technology/story/lenovo-to-launch-vibe-s1-in-india-on...
2015-11-30 09:43:18	http://indiatoday.intoday.in/technology/story/lenovo-to-launch-vibe-s1-in-india-on...
2015-11-30 09:43:18	http://www.techradar.com/news/software/operating-systems/want-to-run-wind...
2015-11-30 09:43:18	http://www.ibtimes.com/lg-g5-rumors-full-metal-design-marvellous-20mp-camera-iri...
2015-11-29 21:38:08	MOTOROLA Nexus 6 Smartphones - Media Markt
2015-11-29 21:32:32	Dune RC
2015-11-29 21:12:37	Top Stores Aptoide - Android Apps Store
2015-11-29 20:54:03	ebay.de MOTOROLA Nexus 6 32 GB Blau 6947681521230 eBay: https://www.google.c... nexus 6 eBay: https://www.google.com/ur?q=http://www.ebay.de/sch/i.htm...
2015-11-29 20:42:24	eBay Deutschland bersicht Ihrer Kufe
2015-11-29 20:38:11	checkoutweb.ebay.de Kaufabwicklung: https://www.google.com/ur?q=https://checkoutweb.ebay.de... Kaufabwicklung: https://www.google.com/ur?q=https://checkoutweb.ebay.de...

Google Forensics

Contacts

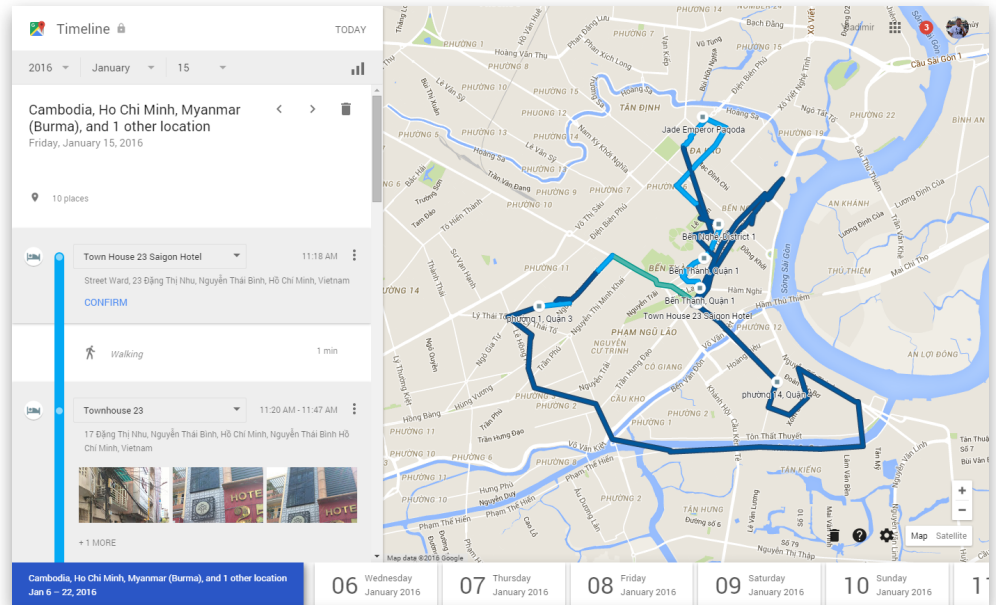
- Conveniently synchronized
- Available for extraction
- Filtering helps find specific contacts (e.g. all contacts with phone numbers, names etc.)



Google Forensics

Location: Google Timeline vs. Elcomsoft Cloud Explorer

- Comprehensive analysis
- Single day view only
- Displays suggested places and activities (e.g. time spent at a certain establishment)



Google Forensics

Location: Google Timeline vs. Elcomsoft Cloud Explorer

- Selectable date range
- Adjustable scale
- Facts only (location + date & time)
- List and map views

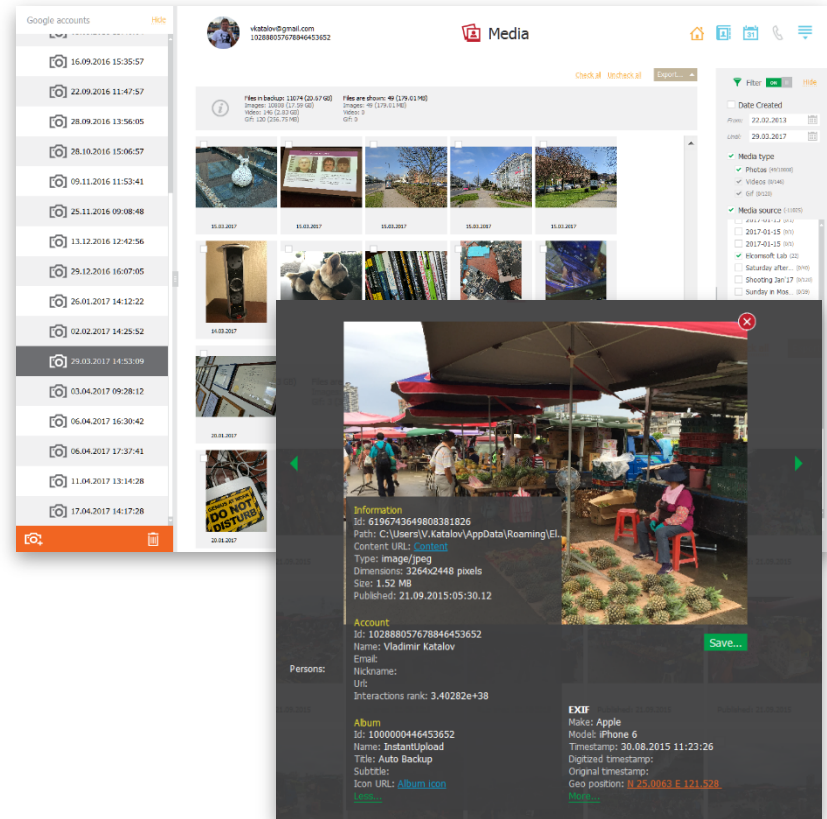
The image displays two side-by-side screenshots. The left screenshot shows the Google Timeline interface, which is a map of Europe and North Africa with red lines indicating movement paths. The right screenshot shows the Elcomsoft Cloud Explorer interface, which includes a list of location events and a detailed view of a specific event.

Start Date	Start Point	Finish Date	Finish Point	Share Link	Type
24.03.2017 11:42:44 (UTC +3)	55.725590 37.633...	24.03.2017 12:36:02 (UTC +3)	55.819236 37.626...		Dining
24.03.2017 10:38:55 (UTC +3)	55.710380 37.620...	24.03.2017 10:21:51 (UTC +3)	55.725590 37.633...		On a bus
24.03.2017 09:38:14 (UTC +3)	55.619260 37.537...	24.03.2017 10:12:49 (UTC +3)	55.710380 37.620...		Dining
23.03.2017 16:36:05 (UTC +3)	55.619260 37.537...	23.03.2017 16:36:05 (UTC +3)	55.614289 37.541...		Dining
23.03.2017 15:37:32 (UTC +3)	55.619260 37.624...	23.03.2017 16:04:55 (UTC +3)	55.637566 37.527...		Dining
23.03.2017 08:48:58 (UTC +3)	55.819260 37.637...	23.03.2017 08:01:17 (UTC +3)	55.819260 37.626...		Working
23.03.2017 07:57:46 (UTC +3)	55.642920 37.538...	23.03.2017 08:39:44 (UTC +3)	55.896566 37.627...		On the subway
23.03.2017 06:28:39 (UTC +3)	55.619260 37.537...	23.03.2017 07:52:12 (UTC +3)	55.642920 37.528...		Working
22.03.2017 12:38:18 (UTC +3)	55.619260 37.639...	22.03.2017 12:43:19 (UTC +3)	55.629566 37.537...		Dining
22.03.2017 00:00:00 (UTC +3)	55.639260 37.538...	22.03.2017 12:14:53 (UTC +3)	55.619260 37.539...		Dining
21.03.2017 09:14:32 (UTC +3)	55.619260 37.624...	22.03.2017 00:00:00 (UTC +3)	55.639260 37.538...		Dining
21.03.2017 07:57:59 (UTC +3)	55.619260 37.537...	21.03.2017 08:02:50 (UTC +3)	55.819260 37.626...		On the subway
20.03.2017 21:39:39 (UTC +3)	55.639260 37.539...	21.03.2017 03:00:00 (UTC +3)	55.629566 37.537...		Working
20.03.2017 20:05:39 (UTC +3)	55.619260 37.624...	20.03.2017 21:07:31 (UTC +3)	55.639260 37.528...		Dining

Google Forensics

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.)
- Elcomsoft Cloud Explorer uses Google Photos to access full image metadata



Google Forensics

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 Forensics

Google Cloud Backups: Conclusion

- Data in Android **backups** extremely limited
- Massive amounts of information **synced** with Google Account
- 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
- **Elcomsoft Phone Breaker**: forensically sound, complete acquisition and analysis



Google Forensics

Tools Mentioned in This Presentation

- Elcomsoft Cloud Explorer
cloud acquisition of Google Accounts
- Elcomsoft Mobile Forensic Bundle
contains all of the above tools in PC and Mac versions at
a 30% discount

