



DEEP|SEC
IN-DEPTH SECURITY

DEEP|SEC

**STILL SECURE. WE EMPOWER WHAT WE
HARDEN BECAUSE WE CAN CONCEAL**



YURY CHERMERKIN

MULTI-SKILLED SECURITY EXPERT

CJSC ADVANCED MONITORING

YURY CHERMERKIN

I have 10+ years of experience in information security. I'm a multi-skilled security expert on security & compliance and mainly focused on privacy and leakage showdown. Key activity fields are EMM and Mobile & Cloud Computing, IAM, Forensics & Compliance.

I published many papers on mobile and cloud security, regularly appears at conferences such as CyberCrimeForum, HackerHalted, DefCamp, DeepSec & DeepSec Intelligence, NullCon, OWASP, CONFidence, Hacktivity, Hackfest, HackMiami, NotaCon, BalcCon, Intelligence-Sec, InfoSec NetSysAdmins, etc.

LINKEDIN:

[HTTPS://WWW.LINKEDIN.COM/IN/YURYCHERMERKIN](https://www.linkedin.com/in/yurychermerkin)

TWITTER: @YURYCHERMERKIN

EMAIL: YURY.S@CHERMERKIN.COM



SECURITY ISSUES



FORENSICS
CAPABILITIES 'N'
LIMITS



SOFTWARE
SECURITY
IMPLEMENTATIONS



DEVICE 'N' OS
SPECIFICS



























































LEAKS

1.1.1.1	1Password	2GIS	AccuWeather	ACDSee Pro
Acrobat	Acronis Mobile	adidas	Admin	Adobe Scan
Ads	Aeroexpress	Aeroflot	Afisha	AIDA64
Airbnb	Airport Experiences	Allo	Altimeter	Alto
Amazon Alexa	Amediateka	American	Android TV	ANT Shared Channel
Anytime	Anywayanyday	App in the Air	Apple Store	Apple Support
Asana	Asana Rebel	ASN	Authenticator	Authenticator
Authenticator	Authy	AutoSleep	AutoWake	Avalanche
Aviakassa	Aviasales	BBM	BelkaCar	Beru
Biglion	Bike Tracks	Bitwarden	Bodyweight	Booking.com
Boomerang	Bring!	Bringly	British Airways	Burger King
Business	BuzzFeed	Camera Pro	CAR5	Card Beeline
Carsharing map	Centr	Chrome	Cinemagia	CITY
ClassPass	Clever	Clips	Cloud Mail.ru	CloudPlayer
Coinbase	Color Band A1	Companion	Connect	Continue on PC
Converse	Cortana	Coursera	Creator	Cristaxi
Crono	Cryptomator	Curb Guide	CyberGhost	Cyclemeter
Dashlane	Delivery Club	Diners Club	Discord	Docs
DocsToGo	Domino's	Drive	Dropbox	Duolingo
Edge	eFax	EMIAS.INFO	Emirates	Enpass
ePayService	Evernote	Excel	Facebook	Facebook Page
FATMAP	FatSecret	Fin.do	Firefox	Firefox Focus
Fitmeter Bike	Fitness Buddy	FixTaxi	Flexi	Flights
Flipboard	Flo	Flow	Flow Mail	Fly Delta
Foodmap	Foursquare	Freeletics	GarageBand	Gateway
Gboard	Gett	Gettable	Gettworkout	Ghoshen
GigSky	Glo	Gmail	Gmoji	Google
Google Calendar	Google Duo	Google Fit	Google Home	Google Keep
Google Maps	Google News	Google News	Google Photos	Google Trips
Google+	Grammarly	GreenAddress	Groups	Gym
Gymaholic	Gymatic	Gymnotize	Hangouts	HeartWatch
Henri AppPort	Hold'em	HomeRun	Huawei Wear	Hushed
Hussle	Hyperlapse	ICQ	IEEE	IFTTT
iG-store	iHerb	IHG	iMovie	Infoclinica
Instagram	Instamart	iot.ru	iSkate	iTunes U
ivi	Jet Airways	Jollyturns	Joom	Keynote
KFC	KFC Клы6	Kik	KillFish	Kitchen Stories
KliChat	KLM	Lamoda	LastPass	Layout
Liftopia	LINE	LinkedIn	linzi.ru	Lookout
Lufthansa	Lyft	Madbarz	Magic One	Mail.ru
MaiTime Pro	Market	Marriott	Mattermost	maxim
Medium	MEGA	MegaFon.Bank	MEGOGO	Memrise
Meridian Taxi	Messenger	Messenger	Mobile Sync	MOEX
Moments	Money	Mosgorpass	MosMetro	MountainBike
MT_FREE	MTC Cashback	Muscle Booster	My Truphone	MyACUVUE
MyFitnessPal	myMail	MyUS	MyXplore	Navi
NEM	Netflix	News	Newton	Nextcloud
Nextcloud Talk	Nike Run Club	Nike Training	NowSecure	NowSecure
nRF Beacons	nRF Blinky	nRF Connect	nRF Mesh	nRF Toolbox
NS Wallet	Numbers	Número	OfficeSuite	OK
Okko Фильмы	OneDrive	OneNote	OneTwoTrip	Opera Mini
Outlook	Outlook Messages	OTON	Pass	Pass

Outlook	Output Messenger	OZON	Pacer	Pages
Pandao	Paper	Payoneer	PayPal	PEP
PhoneDetective	PICOOC	Pillow	Pilot	Ping
Pinterest	Play Books	Plazius	Plex	PnS Pro
Pobeda	Polaris Office	PowerPoint	Priority Pass	PrivacyMeterIntelligence
ProtonMail	PureVPN 2.0	Qardio	QIWI	QR Scanner
QuickSupport	R4S Home	Radio	Rate&Goods	Ready for Sky
Red Bull TV	Remote Desktop	RIDERS	Road Bike	Rocket.Chat
Rosetta Stone	RSB Mobile	RunGap	Runkeeper	Running
Rutaxi	Rutube	Safe Browser	SaveTime	Seven
Shazam	Sheets	ShowJet	SIMless	Ski AR
Ski Tracks	Ski Tracks	Ski&Snowboard Video	Skitude	SkyGuru
Skype	Slack	SleepWatch	Slides	Slopes
Smart Lock	SmartGym	SNOCRU	Snowboard Addiction	Snow-Forecast
Soap	Spaces	Speedtest	SpeedTracker	SPG
Squaw Alpine	Starbucks	Steam	Sticky Password	Strava
Stream	Strong	Summit	SUNLIGHT	Swarm
Sway	SwiftKey	Swim.com	TamTam	TapeACall Pro
Taxi Angel	Teams	TeamViewer	Telegram	Telegram X
TestFlight	The Red Bulletin	Thingy	Tinkoff	T-Mobile eSIM
Todoist	Toloka	TorVPN	Training	TransferWise
Transport	Trello	TruBe	Twitter	Type & Translate
Uber	Uber Eats	Uber Russia	Ullr	Ullr Maps
United	universe	Urban	Utair	VeloBike
Viber	Villa Gusto	Vingle	Visio Viewer	VK
VLC	VLCStrFree	VPN	Waterbalance	WeChat
Viber	Villa Gusto	Vingle	Visio Viewer	VK
VLC	VLCStrFree	VPN	Waterbalance	WeChat
WeDo	WeFi	Welltory	WhatsApp	Wheely
WiFi Finder	WiFi Map Pro	WiFi Scanner	wifimaps	Wi-Finder
WiFox	Wikitude	Winnie	Wire	Word
WordPress	Work Chat	Workouts++	Workplace	WorldMate
Y.Fines	Y.Keyboard	Y.Trains	Y.Weather	Ya.Key
Yahoo Mail	Yamb	Yandex	Yandex Music	Yandex Zen
Yandex.City	Yandex.Disk	Yandex.Eda	Yandex.Fuel	Yandex.Health
Yandex.Mail	Yandex.Maps	Yandex.Metro	Yandex.Taxi	Yogaia
YouDo	YouDrive	YouTube	YouTube Music	Zulip
Авиабилеты	Альфа-Банк	Альфа-Капитал	АльфаСтрах...	Аляска
Аптеки 2ГИС	БКИ Русский Стандарт	Бонус	Бургер Кинг	ВьетКафе
Город	Госуслуги	Делимобиль	Журнал	Инвестиции
Ипотека	Касса	КиноПоиск	Кинотеатры	Киноцентр Соловей
Кошелёк	КредитИнфо	Кукуруза	Магнит	Макдоналдс
Марк	МегаФон	МегаФон ТВ	МИД России	Мобайл
Мой Danysom	Мой Билайн	Мой Брокер	Мой МТС	Мой Спар
Моя Виктория	МТС Банк	МТС Деньги	МТС Коннект	МТС Пресса
МТС Сервис	МТС ТВ	Мясорубка	На карту	Недвижимость
НОУ-ХАУ	Обед	Очкарик	Перекресток	Поч. Гость
Почта России	Пятёрочка	Расписание	Рестораны	Рокетбанк
Сбербанк	Сбербанк УК	Связной	Суперчек	Скидка Дня
Совесть	Спасибо	Спортмастер	Юла	Такси 777
ЦИАН	Шефмаркет	Экспресс		Я.Автобусы
Яндекс	Яндекс.Шеф	米兰机场		

FORENSICS TOOLS. ADVERTISEMENT IS A MOST SCARIEST THING IN THE WORLD 😊

Applications 56

 Apple Messages 11,660	 Booking.com 85	 Discord 47	 Dropbox 1	 Event Log 218	 Evernote 30,093	 Facebook 628
 Facebook Messenger 684	 Firefox 30,907	 Flipboard 4	 Fly Delta 6	 Foursquare 10	 GetTaxi 3	 Google Chrome 6,331
 Google Duo 443	 Google Home 1	 Google Keep 4	 Google Maps 1	 Hangouts 1	 Health 1,621,781	 iBooks 1
 iCQ 1,685	 Instagram 456	 Kik Messenger 87	 LINE 16	 LinkedIn 27	 Lyft 1	 OK 53
 OneDrive 16	 Opera Mini Web Browser 20	 Outlook 9	 Passbook 1,069	 Paypal 1	 Phonebook 1,158	 Pinterest 5
 RunKeeper 1	 Safari Browser 3,900	 Sberbank online 441	 Skype 42	 Strava 111	 TamTam Messenger 2,068	 Telegram 10,006
 Telegram X 3	 Twitter 13	 Uber 8	 Viber 7,902	 VK 15	 WeChat 6	 WhatsApp Messenger 35,591
 Yandex disk 52	 Yandex.Browser 26	 Yandex.Mail 1	 Yandex.Maps 1	 Yandex.Money 41	 Yandex.Taxi 9	 YouTube 17

SECURITY NOWADAYS. FORENSICS DIRECTION



APP SERVERS



APP VENDOR
CLOUD



CDN



3RD PARTY
CLOUD



BACKUP OF
DEVICE



MOBILE &
DESKTOP
DEVICE



2FA

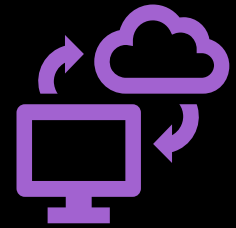


LEAKED
DATABASE

PRIVACY & RISK MANAGEMENT LOGIC

- Cornerstone accounts
- Email accounts
- “Sign-Up/In via” accounts
- Interconnected accounts
- Cloud & Storage accounts
- “Keychains” & encrypted disks
- App servers
- ...
- Finally, data

CORNERSTONE ACCOUNTS



UPD



WhatsApp Google
Backup



Google Android
Cloud Data



Google Bookmarks



Google Calendars



Google Chrome



Google Contacts



Google Drive



Google Fit



Google Home



Google Keep



Google Location
History



Google Mail



Google My Activity



Google Photos



Google Tasks

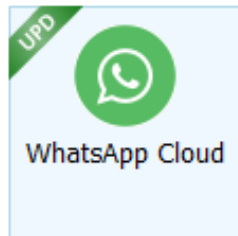


Line Google
Backup



Viber Google
Backup

EMAIL & SOCIAL



Facebook



Instagram



Line



SkyPixel



Swarm
(Foursquare)



Telegram



Twitter



VKontakte



WhatsApp QR



Wickr Me



Workplace by
Facebook



Google Mail



Mail (IMAP)



QQ Mail

EMAIL (LACK OF) SUPPORT VIA IMAP4

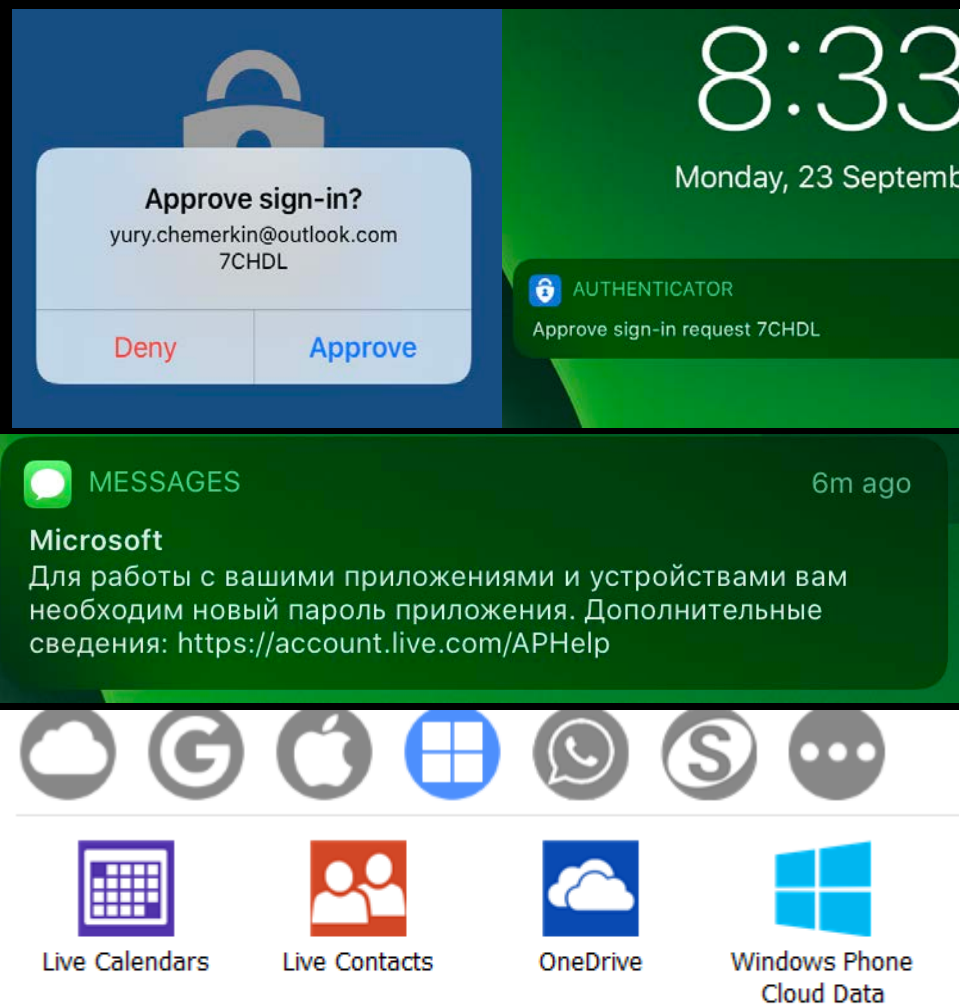


Services	Validated	Validated
<input checked="" type="checkbox"/> Mail (IMAP)	✗	✗
<input checked="" type="checkbox"/> Mail (IMAP)	✗	✗
<input checked="" type="checkbox"/> Mail (IMAP)	✗	✗
<input checked="" type="checkbox"/> Mail (IMAP)	✗	✗
<input checked="" type="checkbox"/> Google Mail	✗	✗
<input checked="" type="checkbox"/> Mail (IMAP)	✗	✗
<input checked="" type="checkbox"/> Mail (IMAP)	✗	✗
<input checked="" type="checkbox"/> Mail (IMAP)	✗	✗
<input checked="" type="checkbox"/> Mail (IMAP)	✗	✗
<input checked="" type="checkbox"/> Mail (IMAP)	✗	✗
<input checked="" type="checkbox"/> Mail (IMAP)	✗	✗

Warning

Microsoft required additional security check for this account. Please log into your Microsoft account at <https://login.live.com/> in your browser and then try downloading OneDrive data again.

OUTLOOK/EXCHANGE SUPPORT



Требуется действие для двухшаговой проверки



Служба технической поддержки учетных записей Майкрософт <ассоциация>
To yury.chemerkin@gmail.com

Учетная запись Майкрософт

Вам необходим пароль прило

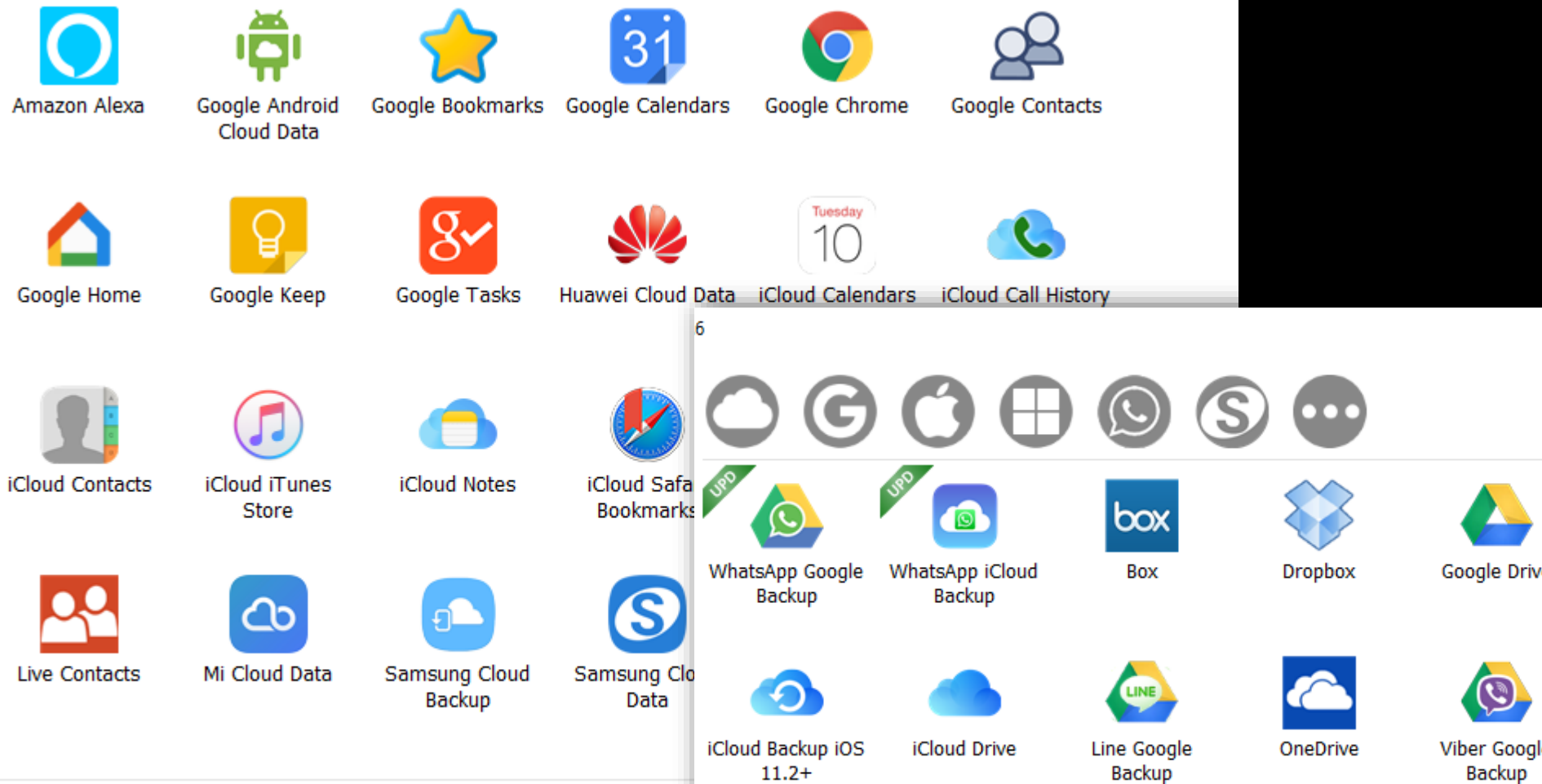
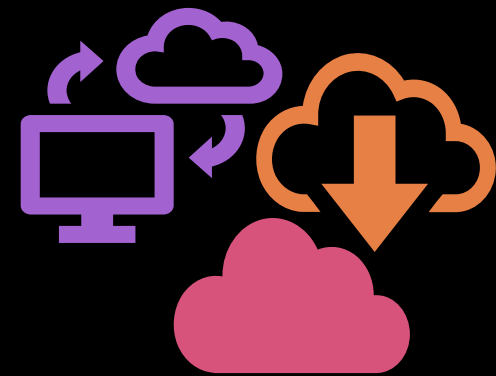
Мы заметили попытку входа с паролем для вашей учетной записи Майкрософт при м...
yu*****@outlook.com двухшаговую проверку, для работы следующих приложений и...
напоминание всеми способами, указанными в сведениях для защиты вашей учетной...
паролей приложений, мы поможем вам сделать это.

- Классическое приложение Outlook для ПК или Mac
- Почтовые приложения на устройстве iOS, Android или BlackBerry
- Office 2010, Office для Mac 2011 или более ранних версий
- Основные компоненты Windows (Фотоальбом, Киностудия, Почта)
- Классическое приложение Zune
- Xbox 360
- Windows Phone 8 или более ранней версии

[Настроить мои приложения и устройства](#)

С уважением,
Служба технической поддержки учетных записей Майкрософт

CLOUD



CLOUDY DATA. EXTRACTION

The screenshot displays a data extraction tool interface. The top navigation bar includes icons for 'Extraction info', 'Export', 'Reset filters', 'View', and 'Maps'. Below this, a sidebar on the left shows 'Dropbox' as the source and a 'Categories' list with 'Account' selected. The main area shows a list of files and folders, with a red circle highlighting a section. The right sidebar shows a 'Categories' list with 'Images', 'Video', 'Audio', 'Documents', 'Archives', 'Other files', 'Contacts', 'Comments', 'Other', and 'Revisions' checked. At the bottom, there are filters for 'Date range' and 'Apply for all services'.

Extraction info **Export** **Reset filters** **View** **Maps**

Dropbox **<<** **:**

Categories 1

Account 1

All data **Files** **Contacts** **Chats** **Timeline** **Social Graph**

Last updated (UTC)

10/08/2019 07:00:22 AM (UTC+0)

BlackBerry SMS Backup 1/3/2014 5:14 PM

IOS 12/31/2018 5:51 PM

EnpassBackupsManual 4/11/2019 6:35 PM

HTC Backup 10/17/2019 4:23 PM

RunGap 10/17/2019 4:34 PM

HD_DEV 10/17/2019 4:49 PM

SMSBackupRestore 10/17/2019 5:04 PM

Enpass 10/17/2019 5:17 PM

MAMP PRO 10/17/2019 5:20 PM

AttidoMobile PassWallet 10/17/2019 5:31 PM

ABBY FineScanner 10/17/2019 9:49 PM

ClockworkMod Carbon 10/18/2019 6:48 AM

sms.xml 11/15/2013 3:54 PM

SMS Backup BlackBerry.xml 11/15/2013 3:54 PM

SMS Backup BlackBerry-fixed.xml 11/15/2013 3:54 PM

BlackBerry SMS Backup.xml 12/12/2013 9:51 PM

BlackBerry SMS Backup-fixed.xml 12/12/2013 9:51 PM

Categories

Images

Video

Audio

Documents

Archives

Other files

Contacts

Comments

Other

Revisions

Date range

1/ 1/2000 **9/23/2019**

Apply for all services

Mac-style

partial

RUNGAP APP.

AN INTERFACE FOR DATA EXCHANGE



DROPBOX
SUPPORTS



SPORT
ACTIVITIES



HEALTH DATA



BODY
MEASURES



ZIPPED FILES



ROUTES



MAPS

RUNGAP – DETAILS

- Analytics, 3rd party sdk – Google, Facebook,
- Network
- Dropbox support to exchange & store data – highly detailed files with a source info
- Some general activities data is available but mainly transfer as zipped files
- Examples are on next slides

Name
2019-03-10_1-29-42 PM_hk_1552213782.zip
2019-03-11_3-36-22 PM_hk_1552307782.zip
2019-03-11_6-12-20 AM_hk_1552273940.zip
2019-03-11_6-42-33 PM_hk_1552318953.zip
2019-03-12_3-03-59 PM_hk_1552392239.zip
2019-03-12_5-46-34 AM_hk_1552358794.zip
2019-03-13_2-34-09 PM_hk_1552476849.zip
2019-03-13_5-59-59 AM_hk_1552445999.zip
2019-03-14_3-05-22 PM_hk_1552565122.zip
2019-03-14_5-14-13 PM_hk_1552572853.zip

https://api.dropboxapi.com

2
files
create_folder
create_folder
list_folder
search
search
search
search
search
search
search
search
search
create_folder
create_folder
list_folder
create_folder
create_folder
list_folder

```

{id": 39567539,
"username": null,
"resource_state": 3,
"firstname": "Yury",
"lastname": "Chemerkina",
"city": null,
"state": null,
"country": null,
"sex": "M",
"premium": true,
"summit": true,
"created_at": "2019-02-24T16:28:44Z",
"updated_at": "2019-06-18T11:05:43Z",
"badge_type_id": 1,
"profile_medium": "https://graph.facebook.com/2467474379990116/p",
"profile": "https://graph.facebook.com/2467474379990116/picture?",
"friend": null,
"follower": null,
"follower_count": 1,
"friend_count": 0

```

Name
2019-03-10_1-29-42 PM_hk_15522
2019-03-10_1-29-42 PM_hk_15522
2019-03-10_1-29-42 PM_hk_15522

v3
athlete
activities
activities
activities
uploads
2967806745
2967806793
2967806767
2967806805
2967806830
2967806855
2967806877
2967806903
2967806930
2967806943
2967806966
athlete
uploads
uploads
uploads
uploads
uploads
uploads
uploads
uploads
uploads
uploads
athlete
athlete

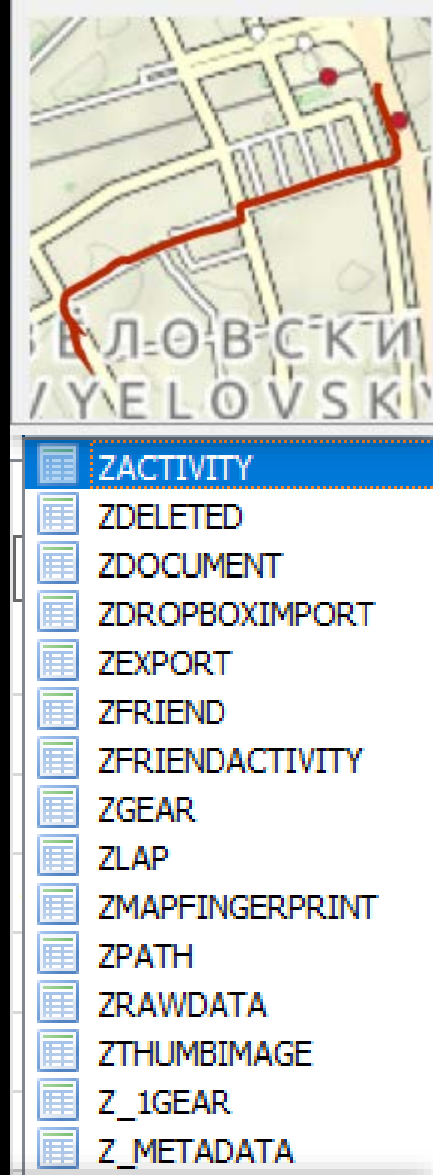
```

{"title": "High Intensity Interval Training", "description": "HIIT for 1:34:39 hr", "source": "HealthKit", "startTime": {"time": "2019-03-10T10:29:42Z", "distance": 0, "duration": 5678.938822984695, "elapsedTime": 5678.938822746277, "avgSpeed": 0, "maxSpeed": 0, "calories": 748, "avgHeartRate": 100, "maxHeartRate": 157, "avgCadence": 5, "maxCadence": 51, "steps": 977, "elevationGain": 0, "elevationLoss": 0, "minElevation": 0, "maxElevation": 0, "lapLength": 0, "activityType": {"internalId": 1414, "internalName": "HIIT", "sourceName": "High Intensity Interval Training"}, "sourceId": "hk_1552213782", "laps": [{"startTime": "2019-03-10T10:29:42Z", "distance": 0, "duration": 5678.760028839111, "elapsedTime": 5678.760028839111, "avgSpeed": 0, "avgCadence": 22, "maxCadence": 51, "avgHeartRate": 100, "maxHeartRate": 157}], "services": [{"autoshare": {"days": 30, "noprompt": true}, "services": [{"autoshare": {"target": false, "targettypes": [], "source": true, "import": true, "name": "strava", "friendfeed": true}, {"autoshare": {"target": false, "targettypes": [], "source": true, "import": true, "name": "health", "friendfeed": true}, {"autoshare": {"target": false, "targettypes": [], "source": false, "import": true, "name": "nike+", "friendfeed": true}, {"autoshare": {"target": true, "targettypes": [], "source": false, "import": true, "name": "dropbox", "friendfeed": true}}], "appversion": "2.22. (383)", "swag": "Purchased: 2019-04-05 6:25:35 AM +0000 Expires: 2020-04-07 6:25:35 AM +0000"}

```

RUNGAP – DETAILS

- Analytics, 3rd party sdk – Google, Facebook,
- No useful backup data
- Activity – Raw data with geo and activity type
- LAP – similar data items like above
- Thumbimage – route with a map background
- Also Mapfingerprint, path, raw data tables contains raw data



ZAVGSPEED	ZDISTANCE	ZDURATION	ZELAPSEDTIME	ZLAPLENGTH	ZMAXLATITUDE	ZMAXLONGITUDE	ZMAXSPEED	ZMINLATITUDE	ZMINLONGITUDE	ZSOURCEID	ZSPORT	ZTIMEZONE	ZTITLE
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
.0000063087...	3158.1183485...	3158.0984250...	3580.6639151...	0.0	0.0	0.0	4.3338007353...	0.0	0.0	hk_1554432415	Walking	Europe/Moscow	Petrovsko-Raz...
.2734796898...	5293.6048535...	4156.8035169...	4156.8035171...	0.0	0.0	0.0	4.6557071571...	0.0	0.0	hk_1551017018	Walking	NULL	Walking
0.0	0.0	5249.1124509...	5249.1124510...	0.0	0.0	0.0	0.0	0.0	0.0	hk_1552572853	High Intensity ...	NULL	High Intensity ...

DATA ACQUISITION



- Ability to stop extraction process
- Mosaic data types
- Network retrieving data issue

FORENSICS. UNSTOPPABLE ACCESS



Your account recently was logged in and active on a new device.

Swarm for Android

September 23, 2019

8:42:15 PM MSK

If you did not take this action, we recommend you reset your password by following the

We Noticed a New Login,
yurychemerkin

We noticed a login from a device you don't
usually use.



Apple iPhone · Instagram app · Moscow,
Russia

September 23 at 10:43 AM (PDT)

If this was you, you can safely disregard this

Uber

New device sign in

Your Uber account was used to sign in on the following device. Please review the details below to confirm it was you.

Date & time of login: Sep 23, 2019, 10:04:02 PM GMT+4
Login country: Russia
Login city: Moscow
Type of device: iPhone
IP address: 95.24.122.247

Swarm (Foursquare)

Instagram - yurychemerkin

199 173 0 0 0 0 200 ? 0

```
8:57:18 PM Requesting user 2481699 information
8:57:19 PM Requesting friendship status information
8:57:20 PM Adding file 2481699.jpg to .OCB archive
8:57:20 PM Writing information about user 2481699 to database
8:57:20 PM Requesting user 5599817502 information
8:57:21 PM Requesting friendship status information
8:57:22 PM Adding file 5599817502.jpg to .OCB archive
8:57:22 PM Writing information about user 5599817502 to database
8:57:22 PM Requesting user 43190719 information
8:57:23 PM Requesting friendship status information
8:57:24 PM Adding file 43190719.jpg to .OCB archive
8:57:24 PM Writing information about user 43190719 to database
8:57:24 PM Requesting user 1576047868 information
```

```
8:57:29 PM Error code: 429({"message": "Please wait a few minutes before you try again.", "status": "fail
8:57:29 PM Error code: 429(Please wait a 300 seconds, after which the extraction will continue.)
```

100%



Completed

25%



Downloading

MAIN OWNER DATA

Phone number +7 (985) 171-91-22

Full name Yury Chemerkin

Full name Chemerkin Yury

Email yury.chemerkin@yandex.ru

Email yury.chemerkin@gmail.com

Phone number +79261230008

Phone number 229215300015357952

OK profile <https://ok.ru/profile/573311526812>

OK profile <https://www.ok.ru/profile/573311526812>

Website <http://re.vu/yury.chemerkin>

Hide full profile

Full name ТанТан - чаты и каналы

First name Yury

Last name Chemerkin

Nickname yurychemerkin

Nickname Yury Chemerkin

Nickname WYRN

Nickname yury.chemerkin

Nickname 410011424745305

Email yury.s@chemerkin.com

Email yury.chemerkin@icloud.com

TamTam link <https://tt.me/j/AAAAhXwHp5w>

Twitter profile <http://twitter.com/PrivacyMeter>

Twitter profile <http://twitter.com/YuryChemerkin>

Website <https://plus.google.com/j/0/108216608239392698703>

Website <https://www.pinterest.com/yurychemerkin>

Common information

Retail name Apple iPhone XR

Manufacturer Apple

AirDrop ID BD45A3298793

Advertising ID 1CD2E2CE-DD78-47D1-8079-1BA013927DE6

Advertising ID 97D5524B-D78B-48E2-89AE-D7E9D9AFFEDD

Advertising ID B98455CB-F3EE-4B06-A4DE-A2A41924BFBF

Advertising ID D1F2DCAC-877E-465E-8630-FD181A854203

Unique ID (UDID) 00008020-001A61382641002E

Apple ID wanderer.star@gmail.com

Apple ID yury.chemerkin@icloud.com

Alias yury.chemerkin@icloud.com

Cached iCloud username yury.chemerkin@icloud.com

ICCID 89701010061184254081

Last known ICCID 89701010061184254081

Last known serving MCC Russian Federation (250)

Phone number +7 (985) 171-91-22

iTunes display name iPhone XR

iTunes version 12.9.0

Evernote ID 63459050

Instagram ID yurychemerkin

Line ID u12bc61d5b2ebd594989d6440303e2769

LinkedIn ID ACoAAAYdYQkBaPqNTO_k7loWJTXqdhWxsSRyy-I

Account name yury_s177

Facebook ID <https://www.facebook.com/yury.chemerkin>

Facebook ID 100001827345335

Instagram ID yurychemerkin

Skype ID yury.chemerkin

Twitter ID PrivacyMeter

Address Kotovsk

Address Moscow

Address Russia, Moscow

Address 28a Poskonkina, 124

City Москва

Country Russia

Birthday 06/05/1988

Blood type O-

Country RU

Gender Male

Height 184 cm

Medical card Titanium plate on the humerus, from elbow to almost end of biceps (right hand)

Note I'm experienced in Reverse Engineering, Programming, Cyber & Mobile Security Researching, Documentation, Cloud Security, Secu...

Status Собери всех друзей в одном мессенджере

Status Available

Wallet number 410011424745305

Weight 87.4000015258789 kg

Sync data

Host №1

Sync host name DESKTOP-KCF8MJ5\YurySChemerkin

Host №2

Sync host name HOME\Yury

Host №3

Sync host name HOME

Last sync 3/15/2017 6:51:12 PM

OS platform Windows 10

Disk usage №1

ENVIRONMENT DISCOVERING

Extraction info

Export

Reset filters

View

Maps

Wireless Connections

<< :

738

Categories

738

WiFi connections

53

Bluetooth connections

601

Locations

84

Reminder

84

All data

Timeline

MAC address

MAC address type

Device name

Default name

BC:B8:63:59:F2:D1

Yury's AirPods

Headphones

50:13:95:7A:04:35

MITV-MSSPO

PDA

A4:B8:05:E7:E9:6C

Yury's iPad

PDA

FF:53:0B:9A:4A:9E

Random

MI Band 2

FF:38:5B:DF:89:93

Random

Mi Band 3

FF:0A:6F:69:35:94

Random

MI Band 2

FE:E7:52:B6:81:26

Random

FE:B1:53:68:4A:30

Random

FE:28:51:A0:46:59

Random

FE:13:36:00:4F:D6

Random

MI Band 2

FD:F4:44:DB:43:C5

Random

Mi Band 3

FD:D4:69:B2:B9:2B

Random

MI Band 2

FD:B7:DA:F1:E2:9E

Random

My IQOS 2.4+

FD:8B:8D:BF:D2:0B

Random

FC:F1:36:35:61:1A

Public

FC:F1:36:32:D1:38

Public

FC:F1:36:32:80:91

Public

FC:F1:36:32:5B:AD

Public

FC:F1:36:31:EE:C8

Public

FC:F1:36:31:1E:F3

Public

[TV] Samsung

FC:EC:DA:D2:71:64

Public

UCK

FC:A8:9A:ED:12:30

Public

JBL Flip 3

FC:A8:9A:E8:9E:DE

Public

JBL Charge

FC:A8:9A:BE:C2:4F

Public

JBL Flip 3

FC:8F:90:96:FA:E7

Public

FC:8F:90:1A:46:DF

Public

FC:4B:17:A1:64:D2

Random

FC:4A:D9:55:2D:FC

Random

FT-5 2DFC

Group by: Month | Day | Hour

All data

Timeline

SSID

BSSID

ASUS

48:5b:39:13:c9:4d

ASUS_Home_plus

34:ce:00:7e:e5:1d

RZD

00:19:92:40:8e:c1

ASUS_Home

bc:ae:c5:eb:9d:75

Otopeni Airport

0c:85:25:68:d1:73

Free WiFi Bestvalue

c8:67:5e:74:db:24

AFI_FREE

28:c7:ce:54:57:b0

FreeWiFi@SweetSide

6c:3b:6b:eb:bb:3d

ViaMilano.WiFi

84:78:ac:99:51:7f

Biblioteca FREE

a0:f3:c1:eb:75:d0

Minerva-Guest

92:2a:a8:95:35:93

NanJing-Guest

80:2a:a8:11:1d:0a

.Dominium_FreeWiFi

6c:3b:6b:27:12:64

DefCamp Public_

00:c0:ca:90:86:fb

DefCamp Public

70:7d:b9:b4:08:ef

Meridian314

4a:a2:2d:62:01:22

Bjorn

e4:8d:8c:6f:5d:27

BG-Free

3c:d9:2b:7f:6f:22

B.H.DINER

46:d9:e7:b5:1e:52

#DXB Free WiFi

dc:eb:94:97:74:f8

@NAIA_FreeGoWiFi

70:3a:0e:04:ea:33

Taal Vista Hotel

6c:3b:6b:73:f1:64

Starbucks_Beeline_Free

00:19:e1:02:d6:20

Yakitoriya

e4:8d:8c:de:3d:36

OBIT - Tokyo City Free Internet

82:2a:a8:51:a4:8d

AA Inflight

74:46:a0:33:f5:c1

Google Starbucks

18:64:72:6d:ec:08

PM

From Chemerkin Yuri
<18998743>

To Cardrona Hotel
<1337440>

Photo [2838598143.jpg](#)

Booker name Chemerkin Yuri

Booker email yuri.chemerkin@gmail.com

Last four digits 5497

Price 1890

Booking site 3438

confirmation number

Source type web

Booking total 1890

cost

ID 2838598143

Checkout 8/8/2019 10:18:28

period AM-Cardrona Hotel



Cardrona Hotel

(Contact)

[Booking.com](#)

Messages 1

0 1

 Key Evidence

 Add tag

 Note

Email 2838598143-ufff.cdcy.u7v...

Phone number +643.4438153

Website <https://www.booking.com/hotel/nz/cardrona-cardrona.html>

Address 2312 Cardrona Valley Road, 9382 Cardrona

Company Cardrona Hotel

Hotel checkin 14:00-21:00

Hotel checkout 07:30-10:00

Language code en

Room count 16



You have 4 new notifications

Accounts


☒  Chemerkin Yuri

Contacts

☒  None
 ☒  Cardrona Hotel
 ☒  Gutenberg Hotel
 ☒  Hotel Des Roses
 ☒  Hotel Elite
 ☒  Hotel Europa
 ☒  Hotel Razvan
 ☒  Hotel Signal
 ☒  Kino Hostel on Vyborgskaya
 ☒  Ladoga Hotel
 ☒  Oceanside Hotel and Suites
 ☒  Residence Bellevue
 ☒  Station Hotel Premier S10
 ☒  Vertical Aparthotel
 ☒  Waiorau Homestead

Sources

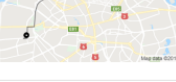
☒  Booking.com



4de2f425-2f33-40c2-a041-dd23992b...

0-d6e4-466a-901f-aa5a6e4...

098b0f4126fcc8827e83b34a749911b...



☆ Key Evidence

🏷 Add tag

📝 Note

Name

4de2f425-2f33-40c2-a041-dd239...

Type

🖼 Image file "PNG"

Category

Images

Size

53.9 KB

Dimensions

540 x 200

Full path

/cloud.uber.data/+79851719122/Maps/4de2f425-2f33-40c2-a041-dd239...

SHA-1 Hash

bf62d5557f663e04689ab379fbfbc...

🏷 Add tag

📝 Note

0-d6e4-466a-901f-aa5a6e4...

es

KB

479

d.uber.data/+79851719122/its/450-d6e4-466a-901f-aa5a6a...

37ed59fed0b80386c7c8d9a...

098b0f4126fcc8827e83b34a749911b...

098b0f4126fcc8827e83b34a7499...

Type

🖼 Image file "JPG"

Category

Images

Size

53.9 KB

Dimensions


599 x 337

Full path

/cloud.social.twitter/NEW/yurichemerkin/Files/098b0f4126fcc8827e83b34a7499...

A-1 Hash

12ca26dfb068c382e6458d32a8f...



Key Evidence

Add tag

Note

Name

098b0f4126fcc8827e83b34a7499...

Type

🖼 Image file "JPG"

Category

Images

Size

53.9 KB

Dimensions

599 x 337

Full path

/cloud.social.twitter/NEW/yurichemerkin/Files/098b0f4126fcc8827e83b34a7499...

A-1 Hash

12ca26dfb068c382e6458d32a8f...

The screenshot shows a web browser interface. The main content area displays a list of contacts, each with a row of icons (checkmark, star, cloud, Twitter) and text identifying the contact. The contacts are:

- Twitter YuryChemerkin
- Twitter YuryChemerkin
- Uber yury.chemerkin@gmail.com
- Uber yury.chemerkin@gmail.com

Below this list, a sidebar menu is visible on the left, showing categories and their counts:

- Categories: 67
 - Accounts: 1
 - yury.chemerkin@gmail.com: 66
 - Payment methods: 3
 - Search history: 10
 - Reviews: 5

On the right side of the sidebar, there is a table with columns for 'All data', 'Files', 'Contacts', 'Chats', and 'Timeline'. The 'Contacts' column is expanded, showing a list of payment methods:

	Type	Status
<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	MasterCard	active
<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	MasterCard	active
<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	American Express	active

10 Time (21 May 2012 - 8 August 2018)

21 May 2012 21 Feb 2013 22 Nov 2013 19 Aug 2014 18 Apr 2015

Uber - yury.chernenko@gmail.com - 11/10/2016 6.5.1
 Uber - yury.chernenko@gmail.com - 11/10/2016 5.0.1
 Uber - yury.chernenko@gmail.com - 11/9/2016 3.34.
 Uber - yury.chernenko@gmail.com - 11/9/2016 3.09.1
 Uber - yury.chernenko@gmail.com - 11/9/2016 3.07.1
 Uber - yury.chernenko@gmail.com - 11/9/2016 3.07.2
 Uber - yury.chernenko@gmail.com - 11/9/2016 3.34.
 Uber - yury.chernenko@gmail.com - 11/9/2016 3.05.1
 Uber - yury.chernenko@gmail.com - 11/7/2016 1.07.1
 Uber - yury.chernenko@gmail.com - 11/7/2016 5.37.
 Uber - yury.chernenko@gmail.com - 11/7/2016 4.03.
 Uber - yury.chernenko@gmail.com - 11/7/2016 1.25.1
 Uber - yury.chernenko@gmail.com - 11/7/2016 1.25.2
 Uber - yury.chernenko@gmail.com - 11/11/2017 5.5.1
 Uber - yury.chernenko@gmail.com - 11/10/2017 3.05.1
 Uber - yury.chernenko@gmail.com - 11/9/2017 3.46.
 Uber - yury.chernenko@gmail.com - 11/9/2017 5.03.
 Uber - yury.chernenko@gmail.com - 11/9/2017 12.1.
 Uber - yury.chernenko@gmail.com - 11/9/2017 5.37.
 Uber - yury.chernenko@gmail.com - 5/22/2017 2.59.2
 Uber - yury.chernenko@gmail.com - 4/17/2017 3.12.1
 Twitter - Yury Chernenko

9 Nov 2018 21:34:51 UTC+3
 B 44.643132, E 26.096543

Details
 Map: lat:23.08-70.0-4.90-89645616747642
 Start point: 44.4402122754862; 26.09663006455457
 Start address: Strada D. I. Meșterilor 1, București 030167, Romania

The image is a collage of five screenshots from the Oxygen Forensic JetEngine application.

- Top Left:** A screenshot of the 'Accounts and Pass...' window. It shows a list of credentials under the heading 'Credentials (2)'. The list includes:

Type	Service	Account
Password	Booking.com	yury.chemerkin@gmail.com
Token	Booking.com	yury.chemerkin@gmail.com
- Top Right:** A screenshot of the 'Social Graph' window. It displays a table with the following data:

Status	Cardholder name	Last four digits	Expiration	Is business	ID
Active	Yury Chemerkin	7193	09/2022	No	1829322952
Active	Yury Chemerkin	5497	10/2022	Yes	1849645642
Active	Yury Chemerkin	6699	10/2022	Yes	1849646573
- Middle:** A screenshot of a map showing a location in Bucharest, Romania. A red pin is placed on the map near 'Piața Română' and 'Spitalul Clinic de Urgență Oftalmologie'.
- Bottom Left:** A screenshot of a network diagram. A central node labeled 'Chemerkin Yury' is connected to several other nodes, including 'Hotel Signal', 'Hotel Razvan', 'Vertical Aparthotel', 'Hotel Elite', 'Kino Hostel on Vy...', 'Hotel Europa', 'Residence Bellevue', 'Station Hotel Prem...', 'Oceanside Hotel a...', 'Les Roses', 'Henningsberg Hotel', and 'Waiaurua Homestead'.
- Bottom Right:** A screenshot of a mobile application interface showing a list of hotels. The list includes 'Hotel Signal', 'Hotel Razvan', 'Vertical Aparthotel', 'Hotel Elite', 'Kino Hostel on Vy...', 'Hotel Europa', 'Residence Bellevue', 'Station Hotel Prem...', 'Oceanside Hotel a...', 'Les Roses', 'Henningsberg Hotel', and 'Waiaurua Homestead'.

DATA ACQUISITION VIA 'NETWORK'

The screenshot displays a data acquisition tool interface with multiple app categories and their associated data counts. A red circle highlights the 'WhatsApp Messenger' category, which includes sub-categories like Account, Media statuses, Contacts, Chats, Calls, Shared data, Locations, Photos, Others, and Cookies. Another red circle highlights the 'Google Keep' category, which includes sub-categories like Accounts, Notes, and Attachments. A third red circle highlights the 'Fly Delta' category, which includes sub-categories like Accounts, Info, Addresses, and Payment info. A fourth red circle highlights the 'Firefox' category, which includes sub-categories like Logins, Web history, Bookmarks, Tabs, General, Reading list, Top sites, Activity history, Cache, Files, and Cookies. The interface also shows a table of data for 'GetTaxi' with columns for Title, Full address, State, City, ZIP, Street, House, Building, Housing, and Coordinates.

App	Category	Count		
WhatsApp Messenger	Account	1		
	Media statuses	6		
	Contacts	6		
	WhatsApp	6		
	Contacts	922		
	WhatsApp	380		
	Phonebook	542		
	Group chats info	5		
	Chats	32,720		
	Private	30,520		
Google Keep	Accounts	1		
	Notes	3		
Fly Delta	Info	1		
	Addresses	1		
	Payment info	4		
	Google Duo	443		
Firefox	Logins	486		
	Web history	29,838		
	Bookmarks	9		
Safari Browser	Passwords	129		
	Folders	405		
	Bookmarks	2,471		
	Search history	20		
	GetTaxi	Locations	3	
		Petrovsko-Razumovskiy pr-d, 23c1, Moscow, Russia, 127287	1	
		Abramsevsckaya ulitsa, 14, Housing 1	1	
		Staroy Petrovsko-Razumovskiy pr-d, 1/23c1, Moscow, Russia, 127287	1	
		State	Moscow	1
		City	Moskva	1
ZIP		127287	1	
Street		Petrovsko-Razumovskiy pr-d	1	
House		23	1	
Coordinates		N 55.8010600	1	

STRAVA

Extraction info	Export	Reset filters
Strava	<<	:
Categories	111	
Account	1	
Cache	103	
Images	103	
Cookies	7	



GOOGLE,
CRASHLYTICS,
FACEBOOK,
ZENDESK,
IO.BRANCH



NETWORK
DATA IS
PROTECTED
FROM MITM



GEO DATA IN
BACKUPS



CREDENTIALS,
PROFILE AND
MEASURES



ZENDESK
USERID &
TOKEN
+ BASIC
PROFILE



SPORT GEAR
MEASURES IF IT
EXISTS



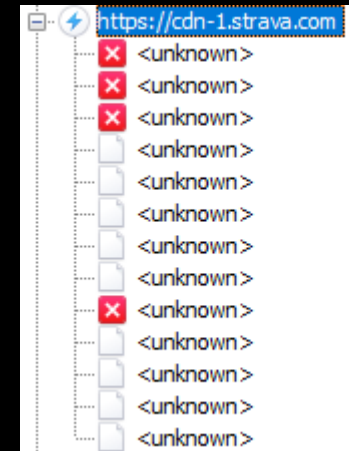
PHOTOS
TAKEN BY
USERS ON
CLOUDFRONT



MAINLY KEEP
ON STRAVA
SERVERS

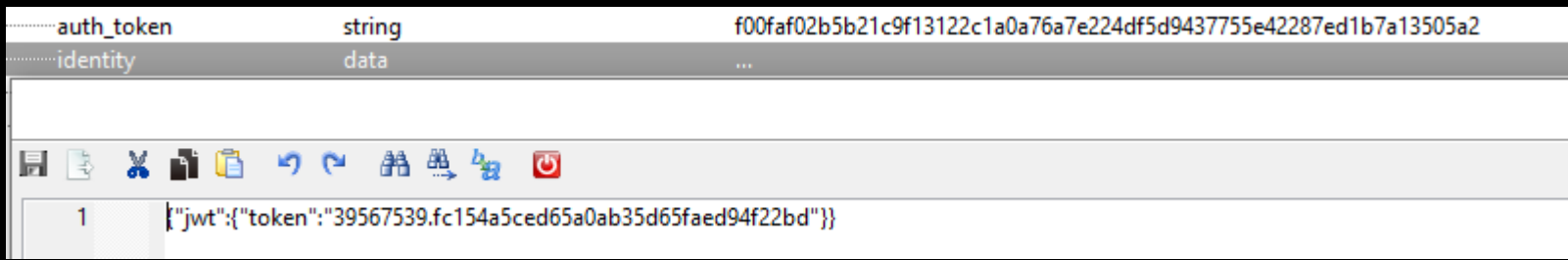
STRAVA – DETAILS

- Analytics, 3rd party sdk – Google, Crashlytics, Facebook, Zendesk, io.branch
- Network:
 - Traffic is generally protected by certificate (Pinning), however developer API doesn't have it as a built-in feature
 - Protected credentials, profile and measures related to runs, walking stats sync but aren't correctly incorporated to overall stats (not supported over years)
 - Gear measures if it exists
- Mainly keep on strava servers



STRAVA – DETAILS

- Geo Route details Documents*.stravactivity
- wp: lat:55.899412; long:37.575460; hacc:64.000000; vacc:63.175690; alt:187.060074; speed:4.348559; course:124.105452; t:1554864639.673529; dt:1554864639.612675
- Zendesk UserID & Token
- \Library\Preferences\com.zendesk.core.identity.plist



STRAVA – DETAILS

- Photos taken by users
- \Library\Preferences\ com.strava.stravaride.plist
- + basic bio
- Full Name + email

user.photo.cache.fullsize		
1:120d208e-f3c6-4e13-80bf-a33ef5e94356	dict	
1:804dde89-9b6b-4806-ad6e-43ab04dcc938	string	https://dgtzuqphqg23d.cloudfront.net/ePF5Fm3b2i2pb9FIXHPLTOH1PN_QCpPWMng9X6G3158-1536x2048.jpg
1:9966f961-12b6-48a5-b8a2-22259f2ce1ba	string	https://dgtzuqphqg23d.cloudfront.net/Hbl9Xoah0m-KtuFQKelxsN8DaSyMmE-0EotK0EbNjV4-1536x2048.jpg
1:0f78b316-4250-4f22-98ce-8712af926ba7	string	https://dgtzuqphqg23d.cloudfront.net/GyppTX2yYiDH712G1pNt3MYAJsTVuA5KDjeVCK6QyLI-2048x1536.jpg
1:fa15f45d-8907-408e-91d8-0ba7ead776a1	string	https://dgtzuqphqg23d.cloudfront.net/R-X376WgX-VzvyoJ9u3MLj4tGYhpLMb_Op3T1RQbHek-2048x1536.jpg
1:8916bf6d-77f1-49d2-8b59-e76debaa6c56	string	https://dgtzuqphqg23d.cloudfront.net/kDxcKZrJ9eaaWedDn-6jBoPnDZBLU9KyzzzNA9DdM1I-1536x2048.jpg

DISK ENCRYPTION & PROTECTION

TPM module ✓	Removable volumes	Mounted volumes
RAM	Profile, MDM ✓	Encrypted boot-volume ✓
Recovery keys ✗	Slow Bruteforce	Administration Privileges ✓

DISK PROTECTION – LAST MILES IN PROTECTION

computers

✓ Connecting to the remote host DESKTOP-KCF8MJ5...
✓ Copying service to the remote computer...
✗ Establishing the service on the remote computer...
✗ Failed to open SCM: 5, Access is denied...

Volume Password

Password:

Confirm:

☐ Use keyfiles

☐ Display password

☒ Use PIM

It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = \$ * + etc. We recommend choosing a password consisting of 20 or more characters (the longer, the better). The maximum possible length is 64 characters.

Volume PIM

Volume PIM: Remember Number to Mount Volume

☐ Display PIM

PIM (Personal Iterations Multiplier) is a value that controls the number of iterations used by the header key derivation as follows:
$$\text{Iterations} = 15000 + (\text{PIM} \times 1000).$$

When left empty or set to 0, VeraCrypt will use a default value that ensures a high security.

When the password is less than 20 characters, PIM can't be smaller than 485 in order to maintain a minimal security level. When the password is 20 characters or more, PIM can be set to any value.

A PIM value larger than 485 will lead to slower mount. A small PIM value (less than 485) will lead to a quicker mount but it can reduce security if the password is not strong enough.


[Information on PIM](#)

ADMINISTRATION PRIVILEGES ISSUES

ppData > Roaming > Oxygen Software

Name	Date modified	Type	Size
3778430512982	9/23/2019 8:01 PM	File folder	
<input checked="" type="checkbox"/> 3778430771087	9/23/2019 8:06 PM	File folder	
Dew	9/27/2019 8:06 PM	File folder	
InternalTest.dat	9/21/2019 8:47 AM	DAT File	
OxyKeywordLists.dat	9/23/2019 9:11 PM	DAT File	

3778430771087

 You don't currently have permission to access this folder.

Click Continue to permanently get access to this folder.

[Continue](#) [Cancel](#)

Error occurred

The application has encountered a problem. We are sorry for the inconvenience.

Cannot open file "C:\Users\YuryS\AppData\Roaming\OxygenEngine\{158BF4EF-2C36-4CF6-99A0-3D3E1E6F3AA6}.taskend". Access is denied.

Please tell us about this problem.

We have created an error report that you can send to help us improve application. We will treat this report as confidential and anonymous.

To see what data this error report contains, [click here](#).

Error occurred

The application has encountered a problem. We are sorry for the inconvenience.

Cannot open file "C:\Users\YuryS\AppData\Roaming\OxygenEngine\Desktop.settings". Access is denied.


Please tell us about this problem.

We have created an error report that you can send to help us improve application. We will treat this report as confidential and anonymous.

To see what data this error report contains, [click here](#).

What were you doing when the problem happened (optional)?

What were you doing when the problem happened (optional)?

 boost::filesystem::status: Access is denied: "C:\Users\YuryS\AppData\Roaming\Elcomsoft\Elcomsoft Phone Password Breaker\PasswordCache.xml"

MEMORY PROTECTION AGAINST DMA ATTACKS

Windows Security

<

☰

Home

Virus & threat protection

Account protection

Firewall & network protection

App & browser control

Device security

Device performance & health

Family options

Core isolation

Security features available on your device that use virtualization-based security.

Memory integrity

Prevents attacks from inserting malicious code into high-security processes.

Off

[Learn more](#)

Memory access protection

Protects your device's memory from attacks by malicious external devices.

[Learn more](#)

Available Physical Memory

4.14 GB

Total Virtual Memory

21.0 GB

Available Virtual Memory

3.40 GB

Page File Space

5.08 GB

Page File

C:\pagefile.sys

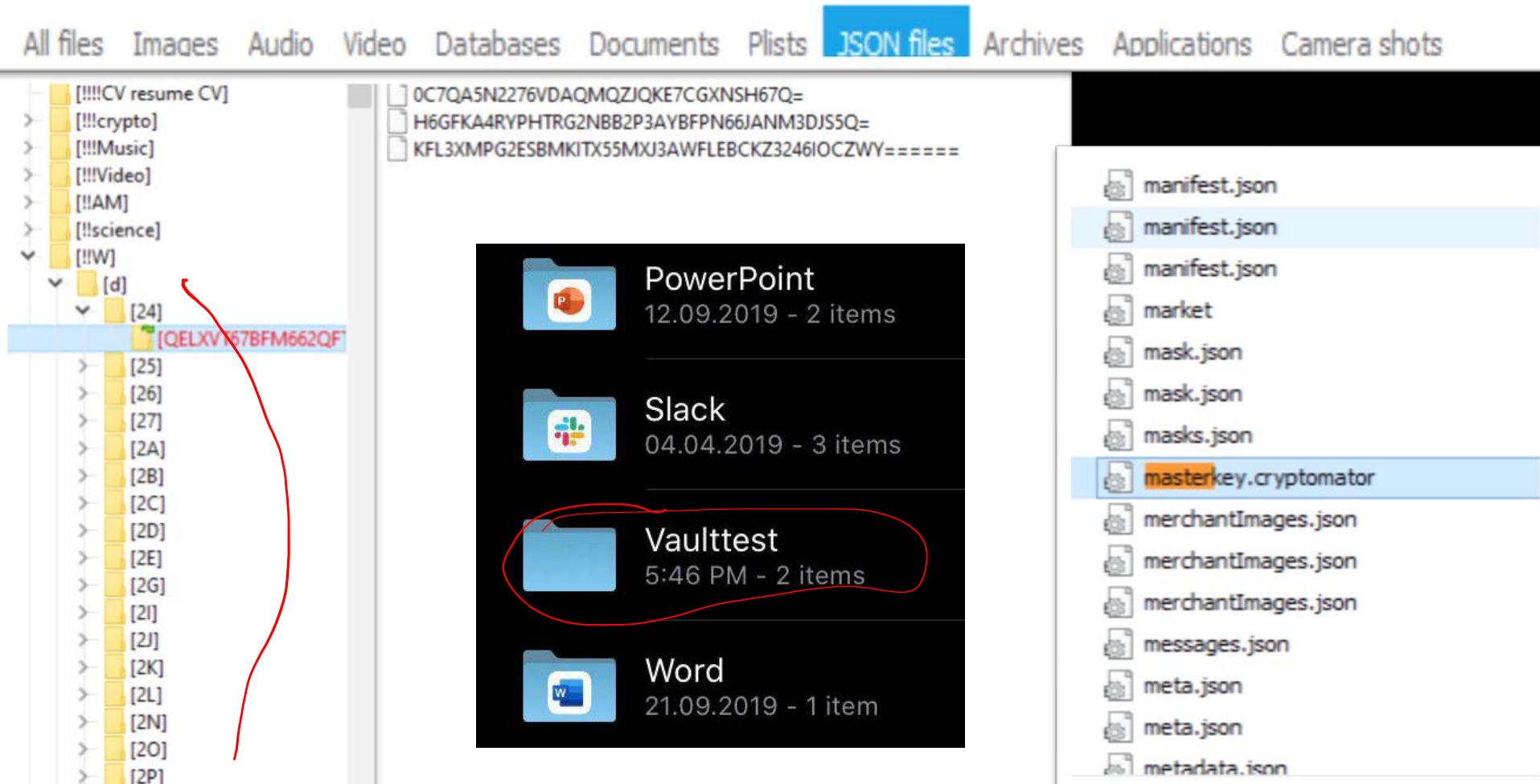
Kernel DMA Protection

On

Virtualization-based security

Running

FORENSICS. DEVELOPED IN A MAC STYLE 😊



UNSUPPORTED OF PROTECTED FF

The image displays the Firefox application settings and a Windows File Explorer window. Red circles highlight specific paths and folders.

Firefox Settings:

- Profile 1:** ☒ C:/Users/Admin/AppData/Roaming/Mozilla/Firefox/Profiles/g5xkgs0e.Default User on Disk C
Data: ☒ History ☒ Web forms ☒ Bookmarks ☒ Cookies ☒ Local storage
- Profile 2:** ☒ C:/Users/Admin/AppData/Roaming/Mozilla/Firefox/Profiles/zs4diabn.default-release
Data: ☒ Passwords ☒ History ☒ Web forms ☒ Bookmarks ☒ Cookies ☒ Local storage
- Profile 3:** ☒ E:/portable test/FirefoxPortable/Data/profile
Data: ☒ Passwords ☒ History ☒ Web forms ☒ Bookmarks ☒ Cookies ☒ Local storage

Windows File Explorer:

- Left pane: Shows drive letters [I:] through [U:]. The folder [U:] ef577c7e54c03aaecc2dfbffd1db7a83c is expanded, showing a subfolder [bn].
- Right pane: Shows the contents of the [bn] folder, including [Profiles].
- Far right pane: Shows the contents of the [Profiles] folder, listing various files and folders such as [bookmarkbackups], [browser-extension-data], [cache2], [crashes], [datareporting], [extensions], [features], [gmp-gmpopenh264], [gmp-widevinecdm], [jumpListCache], [minidumps], [OfflineCache], [safebrowsing], [sessionstore-backups], [startupCache], [storage], [thumbnails], [weave], [et], [fll], and [sc].

BROWSERS OPPORTUNITIES

Features / Browser	Firefox	Chrome	IE & EDGE	Safari	Opera + Game FX
Self-hosted Sync storage	+	-	-	-	-
Self-hosted Accounts	+	-	-	-	-
EMM / MDM Policies	Windows Side only	Windows Side only	+	MacOS Server Side only	-
Mobile support	No encryption	Encryption by user-password without recovering this key	No encryption	No encryption	-

ARTEFACTS ON DESKTOPS AND LAPTOPS

- iTunes backups, except
 - *Content from the iTunes and App Stores, Apple Books, Media Content synced from iTunes*
 - *Data already stored in iCloud, like iCloud Photos, iMessages, and text (SMS) and multimedia (MMS) messages*
 - *Face ID or Touch ID, Apple Pay information and settings, plus Apple Mail data*
 - *Activity, Health, and Keychain data (without iTunes password)*
- Saved passwords
- Email account
- Authentication tokens

CREDENTIALS COLLECTION



- Keychains: Credentials Manager for Windows, Keychain for MacOS
- Browsers Credentials: Chrome, Firefox, IE & Edge, Safari, Opera, Yandex
- Email accounts: resetting accounts, sent password via email
- Tokens & Paired records: bypassing credentials & authorization needs
- Cornerstone accounts' credentials: various limitations to manage account & credentials

PASSWORD MANAGEMENT ISSUE. Y2017 REPORT



- The average business employee must keep track of 191 passwords, according to a report from LastPass.
- According to the report, 81% of confirmed data breaches are due to passwords.
- And the average 250-employee company has 47,750 passwords in use, the report found
- Only 27% of businesses have enabled multi-factor authentication to protect their password vaults, LastPass found.
- <https://www.securitymagazine.com/articles/88475-average-business-user-has-191-passwords>

PASSWORD MANAGEMENT ISSUE. MAPPING TO USER CREDENTIALS' USE CASES.



Screen lock
password



iCloud
password



iTunes backup
password



Screen Time
password



One-time
codes



Lockdown
records

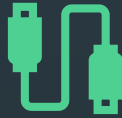
PASSWORD MANAGEMENT ISSUE. MAPPING TO USER CREDENTIALS' USE CASES.

- Screen lock password (= iPhone passcode)
- iCloud password (= Apple Account password)
- iTunes backup password (= local backup password)
- Screen Time password (secures device, account, and changes)
- One-time codes (2FA passwords shared across account-linked devices)
- Lockdown records: In iOS 9, if a pairing record hasn't been used for more than six months, it expires. This timeframe is shortened to 30 days in iOS 11 or later.

PASSWORD MANAGEMENT ISSUE. SCREEN LOCK PASSCODE.



Unlock the device



USB accessories



Device pairing &
local backup



Change account
password & trusted
phone number



Reset local backup
password



View passwords
saved in the keychain



Access certain types
of data from iCloud



Physical analysis

PASSWORD MANAGEMENT ISSUE.

SCREEN LOCK PASSCODE.

- Unlock the device & Connect to USB accessories (unlocking the device disables USB restrictions)
- Pair the device with the new computer and make a new local backup
- Change the iCloud password and trusted phone number (only on 2FA accounts; one-time 2FA password not required)
- Reset (remove) the iTunes backup password (if Screen Time password is not set)
- iOS 13: Change or set new iTunes backup password, Update iOS & Reset the device to factory settings
- View passwords saved in the keychain
- Access certain types of data from iCloud (iCloud password and one-time 2FA password required). This includes iCloud keychain, Health data, synced messages, Screen Time data
- Perform physical analysis. If the device screen lock passcode is known and there are no Screen Time restrictions on installing apps, then jailbreak, extract the file system and decrypt the keychain are possible. The keychain contains the **Screen Lock password** and the **iCloud password** among other things.

PASSWORD MANAGEMENT ISSUE. ICLOUD PASSWORD.



Reset device via
Recovery mode



Sign in, Authorize
App Store
purchases, app
updates



Some data from
iCloud without
2FA, more data
with 2FA, much
more – 2FA +
screen lock
password



Account, Device
Lock, Find Device,
Factory reset



Remote location,
lock & erase,
Change Account &
cloud password

PASSWORD MANAGEMENT ISSUE.

ICLOUD PASSWORD.

- Reset device via Recovery mode, then enter iCloud password when prompted during setup
- Sign in, Authorize App Store purchases, app updates
- Extract some data from iCloud without 2FA, more data with 2FA, much more – 2FA, screen lock password
- Sign into Apple Account, Disable iCloud lock, turn off Find my iPhone, perform factory reset
- Remotely locate, lock or erase devices via Find My (even for 2FA accounts, one-time 2FA codes are NOT required)
- Change your Apple ID/iCloud password, Sign in on Apple devices to make them trusted

PASSWORD MANAGEMENT ISSUE. ITUNES PASSWORD.



Restore the original or
new iOS device including
keychain passwords



Backup to get Screen
Time or Restriction
password



Backup to get password
from backup

appleid.apple.com
www.icloud.com
idmsa.apple.com
id.apple.com
secure1.store.apple.com
secure2.store.apple.com
mapsconnect.apple.com
daw2.apple.com

PASSWORD MANAGEMENT ISSUE.

ITUNES PASSWORD.

- Restore the original or new iOS device including keychain passwords
- Analyze the backup and obtain the Screen Time password (iOS 12 only) or the Restrictions password (older versions of iOS).
- Analyze the backup and obtain passwords from the keychain (may or may not contain the user's Apple ID/iCloud password)
 - appleid.apple.com
 - www.icloud.com
 - idmsa.apple.com
 - id.apple.com
 - secure1.store.apple.com
 - secure2.store.apple.com
 - mapsconnect.apple.com
 - daw2.apple.com

PASSWORD MANAGEMENT ISSUE. SCREEN TIME PASSWORD.



Remove individual Screen Time
restrictions & password



Device screen lock password →
reset local backup password

PASSWORD MANAGEMENT ISSUE. SCREEN TIME PASSWORD.

- You can remove individual Screen Time restrictions, turn off Screen Time or just disable the Screen Time password
- If you know the device screen lock password, you can reset the iTunes backup password

PASSWORD MANAGEMENT ISSUE. 2FA.



Reset Account
password
(2FA, trusted
devices)



Reinstate
account if 2FA
received



Sign into
services
without iCloud
password



Restoring
backups on
new devices



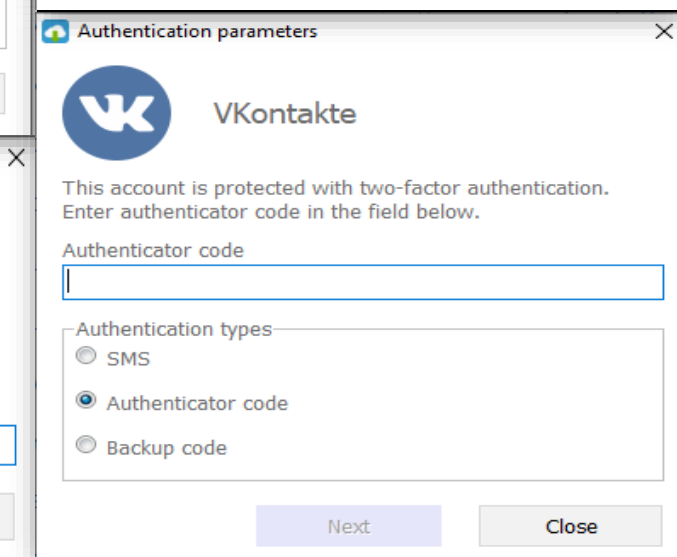
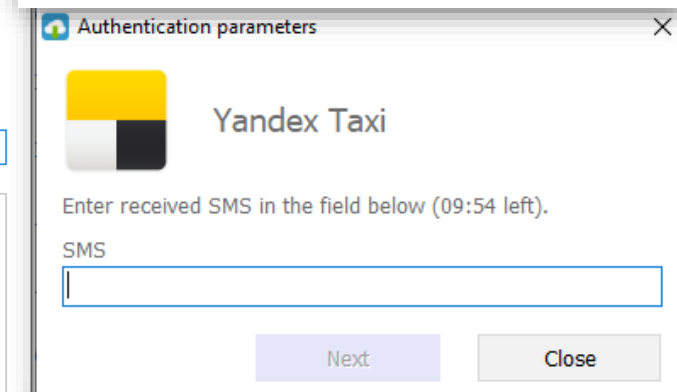
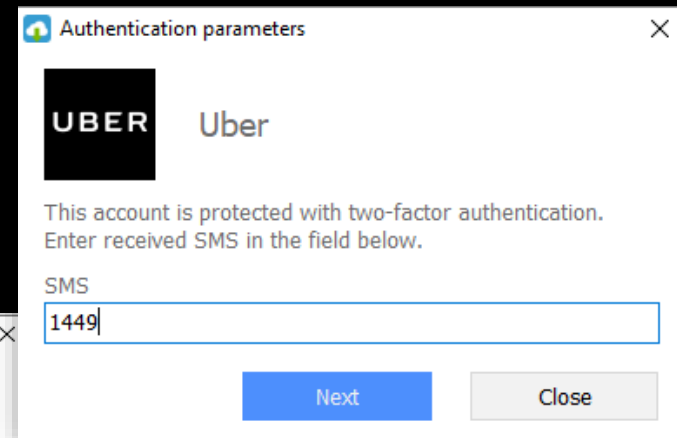
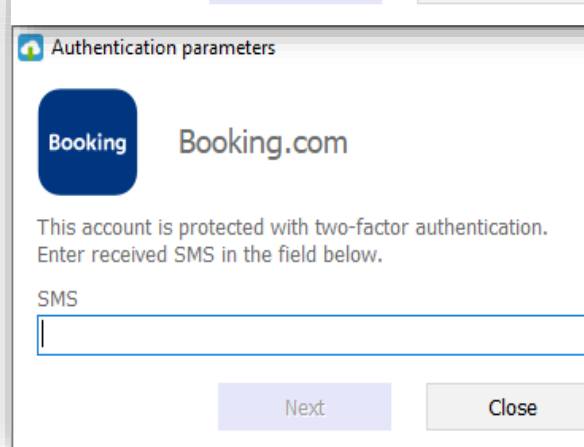
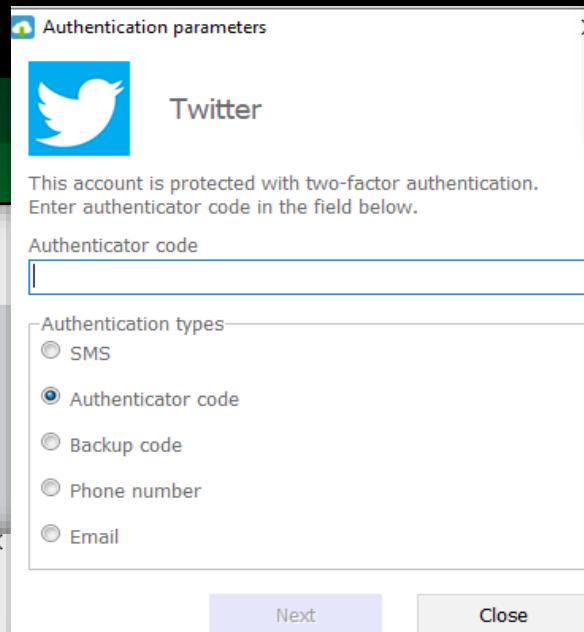
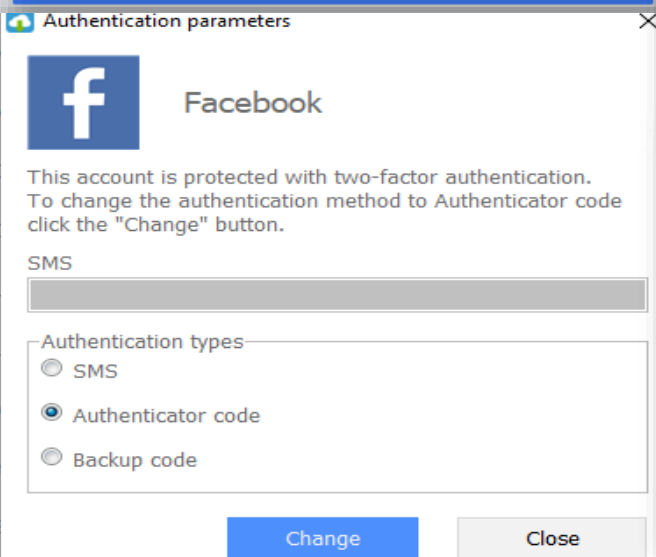
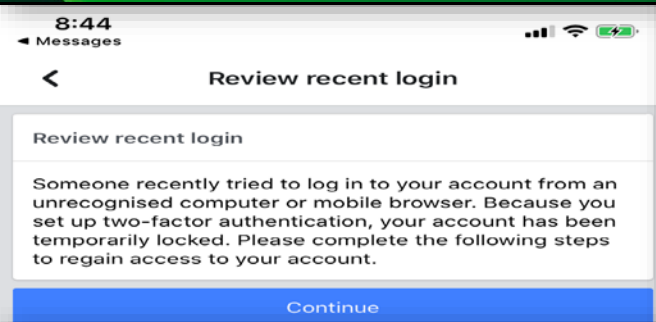
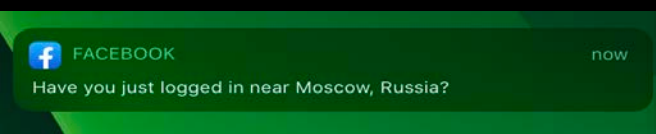
Restoring all
device data
on the same
device

PASSWORD MANAGEMENT ISSUE.

2FA.

- Easily reset your Apple ID/iCloud password if you have access to a trusted device (that device is considered your second authentication factor)
- Reinstate your Apple account (and reset your Apple ID/iCloud password) if you can receive the 2FA code (trusted phone number/SIM card)
- Sign in to your Apple ID/iCloud services even if you forget your iCloud password (by resetting the password)
- Restore existing or new devices from iCloud backups
- If restoring existing device (the same physical device an iCloud backup was made from), saved passwords (keychain items) will be restored as well even if you don't know the screen lock passcode
- You can download many types of data (such as calendars, mail, notes, reminders, Voice Memos etc.)

2FA SUPPORT



PASSWORD MANAGEMENT ISSUE. PASSWORD POLICIES.



Screen lock
passcode: no
definite policy



iCloud password:
strong policy



iTunes backup
password: no
policy



Screen time
password:
exactly 4 digits

PASSWORD MANAGEMENT ISSUE.

PASSWORD POLICIES.

- Screen lock passcode: no definite policy.
- iCloud password: must be at least 8 characters; must include at least one small letter, one capital letter, and one digit.
- iTunes backup password: no policy.
- Screen time password: exactly 4 digits

The figure displays three screenshots of the Apple Health app interface, illustrating different data views and their corresponding data sources. Red circles highlight specific sections in each view.

Left Screenshot (Categories View): The 'Categories' view shows a list of health metrics on the left and a table of data sources on the right. The 'Data sources' section is highlighted with a red circle. The table lists various data sources and their associated health metrics.

ID	Name
com.apple.health.14D1CBA9-9477-41D9-9DE9-07AF3E62F7DE	iPhone XR
se.perigee.7minute-workout	Seven
se.perigee.7minute-workout	Seven
com.crossforward.WorkoutPlusPlus	Workouts++
com.crossforward.WorkoutPlusPlus	Workouts++
io.bodymatter.SleepWatch	SleepWatch
io.bodymatter.SleepWatch	SleepWatch
com.skiplan.squawvalley	Squaw Alpine
com.yogaglo.main	Glo
com.nike.nikeplus-gps	Nike Run Club
com.nike.nikeplus-gps	Nike Run Club
com.nike.nikeplus-gps	Nike Run Club
com.tantissa.Haptick	AutoWake
com.tantissa.AutoSleep	AutoSleep
com.tantissa.AutoSleep	AutoSleep
com.getqardio.Qardio	Qardio
com.cameronchow.Strong	Strong
co.vimo.vimotrack	Gymatic
com.tantissa.Heartbeat	HeartWatch
com.google.fit	Google Fit
co.vimo.vimotrack	Gymatic
com.tantissa.Heartbeat	HeartWatch
com.nike.nikettrainingclub	Nike Training
com.musdeboost	Muscle Booster
com.picoc.international	PICOOC
com.fatsecret.caloriecounter	FatSecret
com.neybox.Pillow	Pillow
com.strava.stravaride	Strava

Middle Screenshot (Workouts View): The 'Workouts' view shows a list of workout types on the left and a table of data sources on the right. The 'Body measurements' section is highlighted with a red circle. The table lists various data sources and their associated health metrics.

ID	Name
com.consumedbycode.slopes	Slopes
com.rungap.RunGap	RunGap
com.strava.stravaride	Strava
com.consumedbycode.slopes	Slopes
com.apple.mobiletimer	Clock
com.apple.health.BEF3A0CD-D568-482A-B390-1F1831AA9B72	Yury's Apple Watch
com.apple.health.08D11776-EFD3-4966-A5E7-D1C24A62B135	Yury's Apple Watch
com.apple.Health	Health
com.tantissa.Heartbeat	HeartWatch
com.fatsecret.caloriecounter	FatSecret
com.apple.mobiletimer	Clock
com.Scraft.pep	PEP
com.tantissa.Haptick	AutoWake
com.tantissa.Heartbeat	HeartWatch
com.corecoders.BikeTracks	Bike Tracks
iSkate	iSkate
com.consumedbycode.slopes	Slopes
com.corecoders.SkiTracks	Ski Tracks
com.strava.stravaride	Strava
com.consumedbycode.slopes	Slopes
com.tantissa.AutoSleep	AutoSleep
com.neybox.Pillow	Pillow
com.tantissa.AutoSleep	AutoSleep
com.mosgorpass.socialsys	Mosgorpass
com.apple.health.27729498-FF72-4E02-AF9A-25AA0C48C3F6	Yury's Apple Watch
com.apple.health.27729498-FF72-4E02-AF9A-25AA0C48C3F6	Yury's Apple Watch
com.apple.health.27729498-FF72-4E02-AF9A-25AA0C48C3F6	Yury's Apple Watch
com.getqardio.Qardio	Qardio

Right Screenshot (Body measurements View): The 'Body measurements' view shows a list of body measurement types on the left and a table of data sources on the right. The 'Data sources' section is highlighted with a red circle. The table lists various data sources and their associated health metrics.

ID	Name
com.consumedbycode.slopes	Slopes
com.rungap.RunGap	RunGap
com.strava.stravaride	Strava
com.consumedbycode.slopes	Slopes
com.apple.mobiletimer	Clock
com.apple.health.BEF3A0CD-D568-482A-B390-1F1831AA9B72	Yury's Apple Watch
com.apple.health.08D11776-EFD3-4966-A5E7-D1C24A62B135	Yury's Apple Watch
com.apple.Health	Health
com.tantissa.Heartbeat	HeartWatch
com.fatsecret.caloriecounter	FatSecret
com.apple.mobiletimer	Clock
com.Scraft.pep	PEP
com.tantissa.Haptick	AutoWake
com.tantissa.Heartbeat	HeartWatch
com.corecoders.BikeTracks	Bike Tracks
iSkate	iSkate
com.consumedbycode.slopes	Slopes
com.corecoders.SkiTracks	Ski Tracks
com.strava.stravaride	Strava
com.consumedbycode.slopes	Slopes
com.tantissa.AutoSleep	AutoSleep
com.neybox.Pillow	Pillow
com.tantissa.AutoSleep	AutoSleep
com.mosgorpass.socialsys	Mosgorpass
com.apple.health.27729498-FF72-4E02-AF9A-25AA0C48C3F6	Yury's Apple Watch
com.apple.health.27729498-FF72-4E02-AF9A-25AA0C48C3F6	Yury's Apple Watch
com.apple.health.27729498-FF72-4E02-AF9A-25AA0C48C3F6	Yury's Apple Watch
com.getqardio.Qardio	Qardio

ALTERNATIVE SOURCES ARE NOT SUPPORTED. ~50 APPS W/O 2FA

- **General Sport:** Strava, RunGap, Pacer, Nike RUN Club & Training, MyFitnesspal
- **Gym:** Smartgym, Gymaholic, GYM & Freelitics, Flexi, Hussle, Strong
- **Health & Sleep:** Pillow, HeartWatch, SleepWatch, Welltory
- **Summer Sports:** RunKeeper, Road & Mountain Bike, iSkate, Bike Tracks, SpeedTracker, CycleMeter, FitMeter Bike, Crono, Altimeter
- **Winter Sports:** Ullr & Ullr Maps, Squaw alpine, Snow forecast, SnocRu, Slopes, Skitude, SkiTracks, Ski AR, Jolly Turns, Riders, Fatmap, Avalanche
- **Workouts:** Workouts++, Running, Gymatic, Gymnotize, Muscle Booster, Fitness buddy, Centr, Body weight, Asan Rebel, Training (Adidas, Runtastic)

DOWNLOADS W/O RESTRICTIONS. PUBLIC DATA, BACKUP ACROSS CLOUDS



SLEEPWATCH:
SLEEP & HEART
DATA



**ROADBIKE,
MOUNTAIN BIKE:**
IMAGES ON CDN



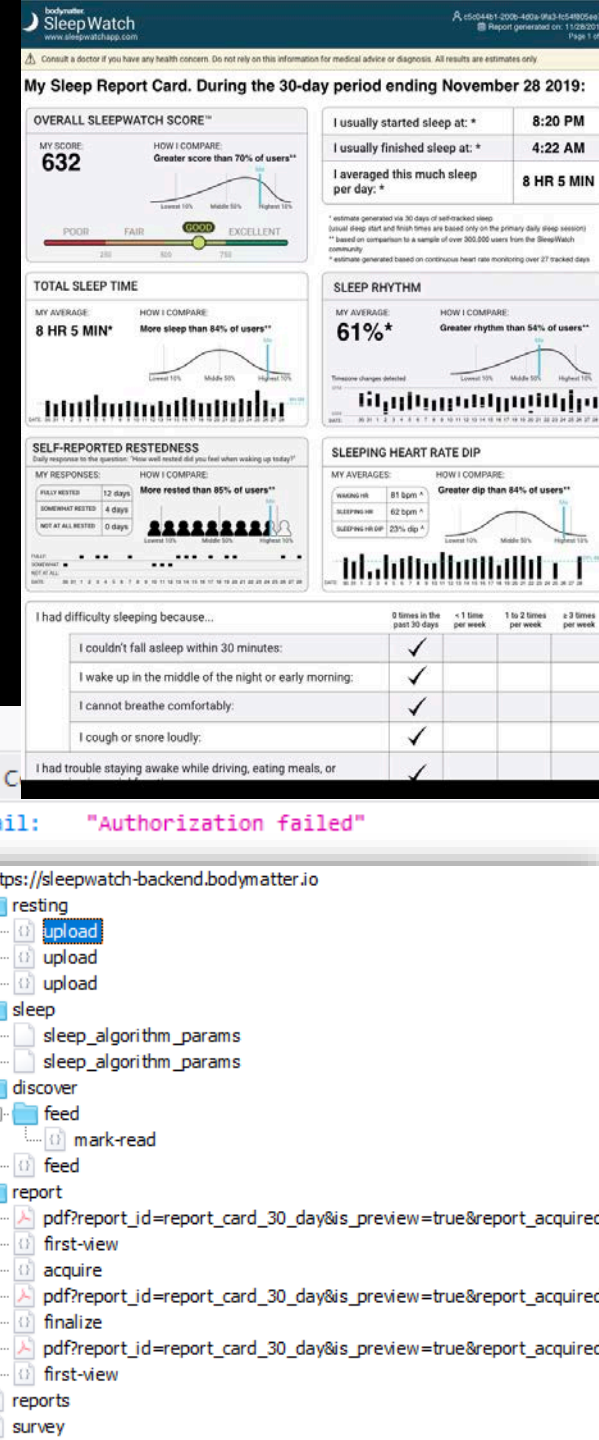
PACER:
WORKOUTS,
HEATH & GPS



SKITUDE: RIDER LIST
AND THEIR TRACKS

SLEEPWATCH – DETAILS

- Analytics, 3rd party sdk – Google, Facebook,
- Network
- Surveys, pdf report with strong auth without publicly available data unless developer credentials from AWS S3 leaks
- https://sleepwatch-backend.bodymatter.io/report/pdf?report_id=xxxx
- Daily tracked sleep data



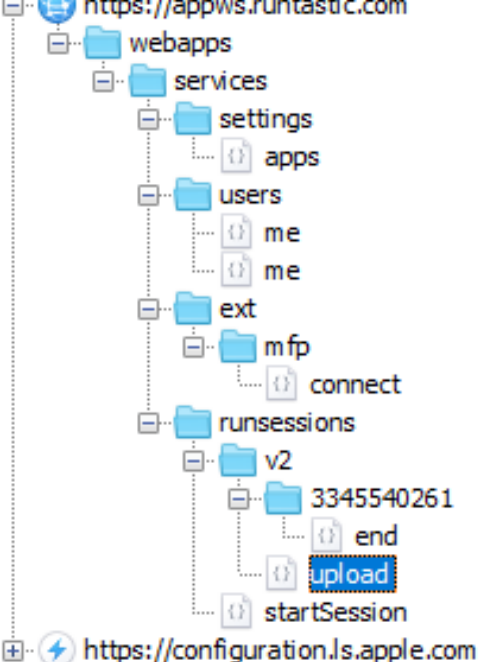
SLEEPWATCH – DETAILS

- Analytics, 3rd party sdk – Google, Facebook,
- No useful backup data
 - Documents\data*.json – Apple Watch model, last ~5 sleep records (timeframe only)
 - Body profile -
\\Library\\Preferences\\io.bodymatter.SleepWatch.plist

BodyProfile	dict	
age	integer	31
sex	string	Male
weight	real	194.006791
height	real	71.653543
birthdate	string	1988-06-05T11:00:00Z
watchOsBundleVersion	string	6.0.2.0
localNotificationReminder6We	boolean	true
AccountEmail	string	yury.chemerkin@gmail.com

ROAD BIKE, MOUNTAIN BIKE – DETAILS

- Analytics, 3rd party sdk – Google, Facebook, Flurry
- Network
- Basic info, Cloudfront'ed images
- General and details of tracks
- Video not analyzed
- Examples are on next slides



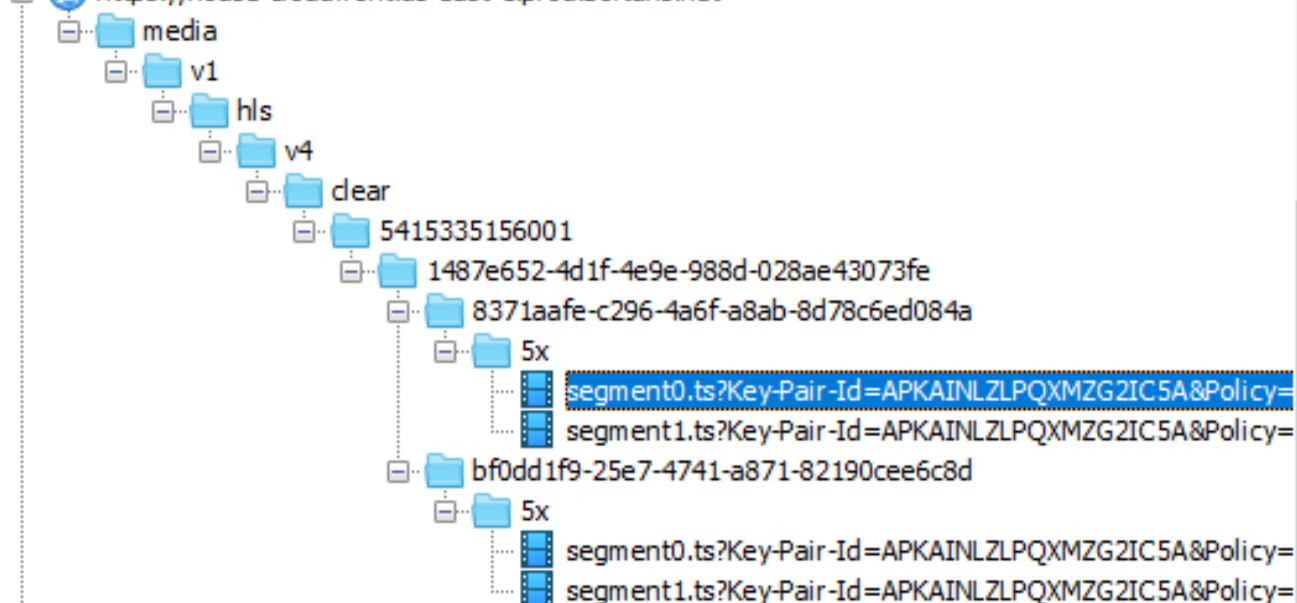
<https://configuration.ls.apple.com>

```
"distance": "0",
"time": "1571720128000",
"gpsData": {
  "trace": "AAAAAQAAW3x0b+jQhZMDk",
  "longitude": "37.5742722",
  "count": "1",
  "latitude": "55.9008064",
  "version": "1"
},
"calories": "0",
"duration": "11644",
"elevationGain": "0",
"pause": "0",
"elevationLoss": "0"
```

Readers Cookies Authentication Text Hex JS

```
"runSessionId": "3345540261",
"updatedAt": "1571720129000",
"cheeringSummary": {
  "noOfFriends": "0",
  "noOfCheerings": "0"
}
```

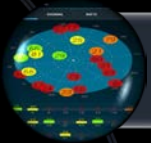
<https://house-cloudfront.us-east-1.prod.boltdns.net>



<https://house-cloudfront.us-east-1.prod.boltdns.net>

```
"userInfo": {
  "userData": {
    "firstName": "Yury",
    "lastName": "Chemerkina",
    "height": "1.84",
    "isDefaultHeight": "false",
    "weight": "79.0",
    "isDefaultWeight": "false",
    "gender": "M",
    "birthday": "581472000000",
    "birthdayEstimated": "false",
    "countryCode": "RU",
    "locale": "en",
    "unit": "0",
    "avatarUrl": "https://dvp86gw5pkelr.cloudfront.net/default__default_avatar_male.jpg?w=480&h=480",
    "avatarUrlMedium": "https://dvp86gw5pkelr.cloudfront.net/default__default_avatar_male.jpg?w=170&h=170",
    "avatarUrlSmall": "https://dvp86gw5pkelr.cloudfront.net/default__default_avatar_male.jpg?w=70&h=70",
    "roles": ["pro_app_customer"],
    "activityLevel": "2",
    "weightUnit": "0",
    "temperatureUnit": "0",
    "agbAccepted": "true",
    "id": "128341489",
```

ROAD BIKE, MOUNTAIN BIKE – DETAILS



GPS Data: longitude, latitude, altitude, accuracy, distanceInMeter, upward/downward (meters), timestamp local, timestamp gps



Session Data: timestamp (start, end), distance, duration, avg & max speed, upward/downward, heartZone values (need special device)



Speed Data: timestamp, speed, duration, distance



User Data: email, password, weight, height, gender, name, birthday

DOCUMENTS\DATABASE.SQLITE3

Where to search data (tables):

- GPS & location
 - HeartRate (requires special devices)
 - Session Data, Speed, User Data
- Location and geo snapshots - Documents\MapOpenCycleMap.sqlite
- User info - Documents\database.sqlite3

The screenshot shows a SQLite database viewer with the 'ZCACHE' table selected. The table has four columns: 'ztileHash', 'zlastUsed', 'zdata', and 'zInserte'. The 'zdata' column contains 'BLOB' values. A red arrow points from a 'BLOB' entry in the 'zdata' column to a map view below it. The map shows a street labeled 'Пичная Улица' and a red location pin. Below the map is a list of tables (17) including Abilities, CADENCE, COMPETITION, ELEVATION_DATA, GEOIMAGEDATA, GPS_DATA, HEARTRATE, RouteHasTags, Routes, SESSION DATA, SPEED, TRACK_DATA, USER_DATA, and VOICE. The 'HEARTRATE' table is highlighted with a red box and a red arrow, and a red text label 'Need special devices to track' is next to it.

ztileHash	zlastUsed	zdata	zInserte
Filter	Filter	Filter	Filter
122500074876...	1528599341.7...	BLOB	1528599342
122500074876...	1528599341.7...	BLOB	1528599342
122500074876...	1528599341.7...	BLOB	1528599342
122500074876...	1528599341.7...	BLOB	1528599342

Tables (17)

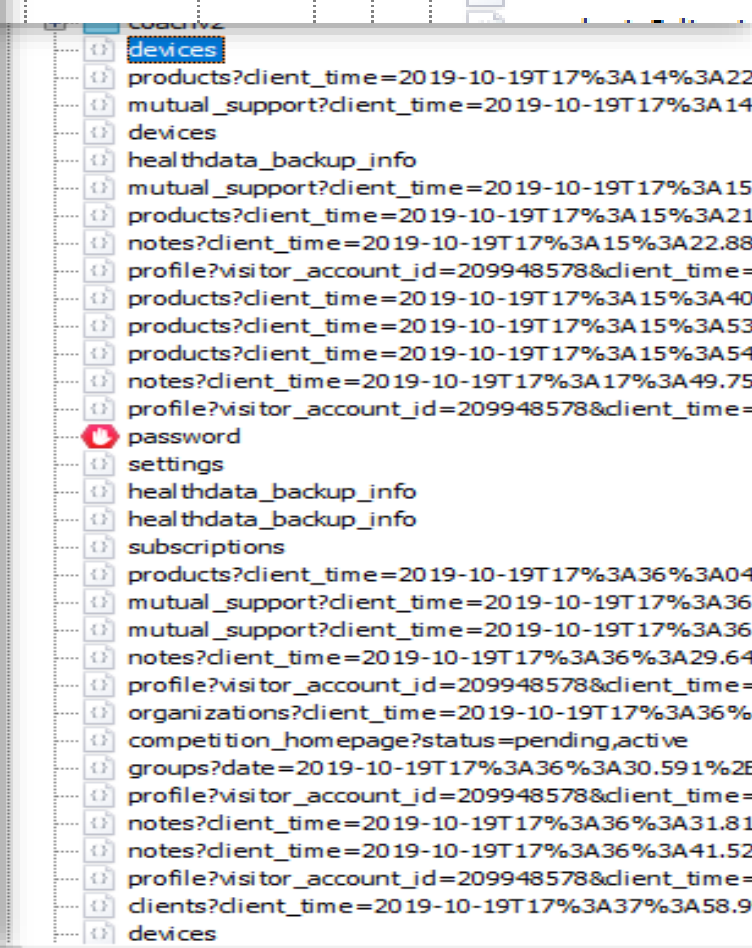
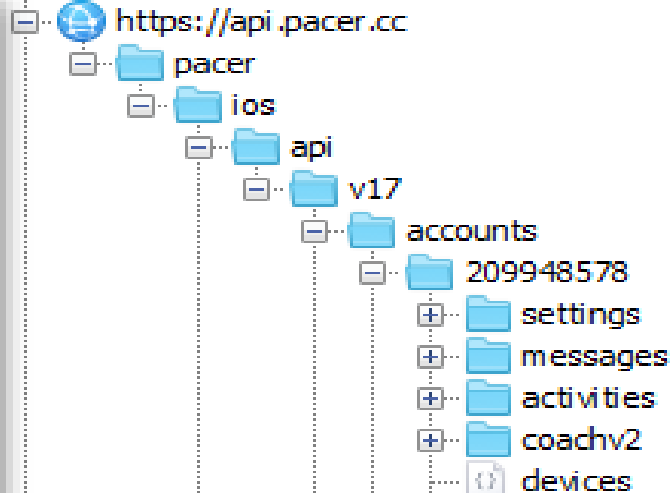
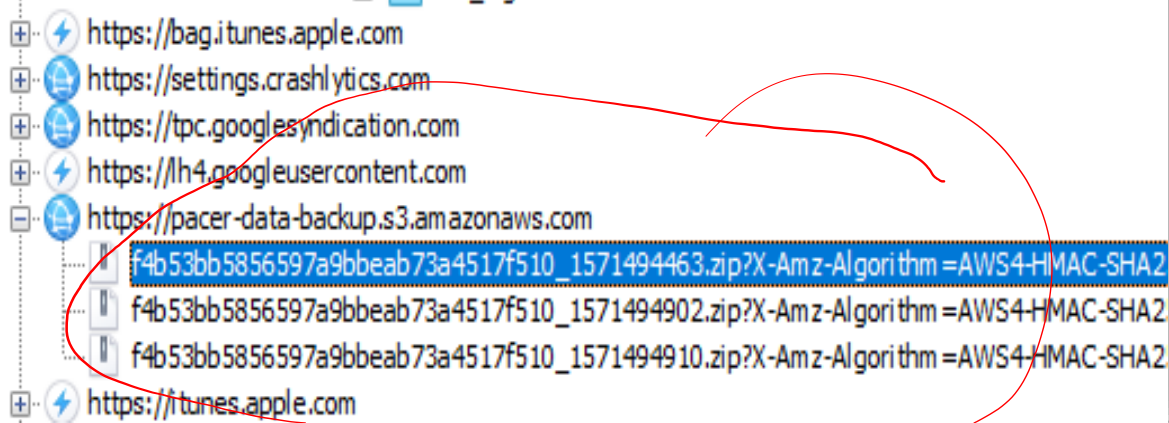
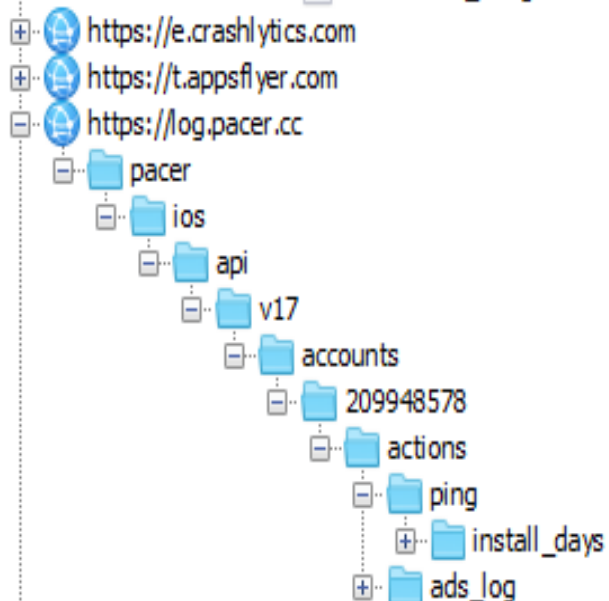
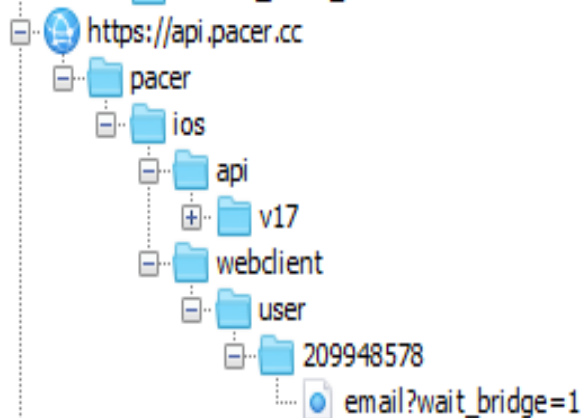
- Abilities
- CADENCE
- COMPETITION
- ELEVATION_DATA
- GEOIMAGEDATA
- GPS_DATA
- HEARTRATE
- RouteHasTags
- Routes
- SESSION DATA
- SPEED
- TRACK_DATA
- USER_DATA
- VOICE

Need special devices to track

USER_DATA											
user_id	isLocal	name	email	passwd	std_user	weight	height	gender	firstname	lastname	irthday_unixirr
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1		NULL	NULL	NULL	NULL	75	180	1	NULL	NULL	579068944674
0		NewRunner	yury.chemerki...		YES	79	184	1	Yury	Chemerkin	581472000000

PACER – DETAILS

- Analytics, 3rd party sdk – Google, Facebook, Flurry, Mopub, Appsflyer, Crashlytics, Amplitude, AWS ads
- Network
- Profile data, device data, geo data,
- Data mainly stored on AWS S3 as backup files
 - Workout plan & progression
 - MinutelyActivityLog, DailyActivity, HeartLog
 - GPS Route logs and indoor routes
- Examples are on next slides



PACER – DETAILS

- Analytics, 3rd party sdk – Google, Facebook, Flurry, Mopub, Appsflyer, Crashlytics, Amplitude, AWS ads
- No useful backup data
- \Shared\AppDomainGroup-group.cc.pacer.shareddata\Library\Preferences\group.cc.pacer.shareddata.plist

gender	integer	1
heightInCentimeter	integer	182
class	dict	
hasStride	boolean	false
age	integer	31
weightInKg	real	87.000000

SKITUDE – DETAILS

- Analytics, 3rd party sdk – Google, Facebook, Crashlytics
- Network
- Credentials + token, basic info
- Rider list with name, photo and their tracks stored on AWS per resort you're searched for
- User DB – not analyzed
- Examples are on next slides



```
"content": [{
  "username": "edu2720",
  "user_id": 104147,
  "avatar": "https://userdatacf.skitude.com/images/thumb145_145/jpg5951c182bd5c01498530178.jpg",
  "id_resort": null,
  "resort_name": null,
  "city": "R\u00edo Grande",
  "country": "Argentina",
  "timestamp": 1571738034,
  "date": "Yesterday",
  "hour": "11:53",
  "time": "01h 13m 45s",
  "type": "track",
  "track_id": 581256,
  "track_name": "2019-10-22 11:53:54",
  "track_type": "btt",
  "distance": "19,3 km",
  "kml_track": "https://s3.eu-central-1.amazonaws.com/userdata-s3/tracks/processed/kml5daee31aalc031571742490.kml",
  "url_thumbnail": "https://userdatacf.skitude.com/tracks/thumbs_timeline/kml5daee31aalc031571742490.kml.jpg?id=6",
  "duration": "4425",
  "statistics": [{
    "key": "distance",
    "value": "19,3 km"
  ]
}]
```

AppId	com.b-labsolution
lang	en
login_source	skitude
name	Yury
password	SoJ_-KgPej4PhbL
surname	Chemerkín
timestamp	1571807816
userid	yury.chemerkín@

AppId	com.b-labsolution
AppIdCorrect	com.b-labsolution
acceptinfo	true
app_version	79.1.119
email	yury.chemerkín@
email2	yury.chemerkín@
lang	en
login_source	skitude
name	Yury
password	SoJ_-KgPej4PhbL
password2	SoJ_-KgPej4PhbL

Headers	Text	Hex	Form	Raw
---------	------	-----	------	-----

```
{
  "result": "success",
  "message": "login ok",
  "username": "yuryche",
  "sessionid": "5d4fe2",
  "fullname": "Yury Ch",
  "user_token": "68b71",
  "isskitude": "1"
}
```

AppId	com.b-labsolution
AppIdCorrect	com.b-labsolution
acceptinfo	true
app_version	79.1.119
email	yury.chemerkín@
email2	yury.chemerkín@
lang	en
login_source	skitude
name	Yury
password	SoJ_-KgPej4PhbL
password2	SoJ_-KgPej4PhbL

Headers	Text	Hex	Form	Raw
---------	------	-----	------	-----

```
{
  "result": "success",
  "message": "registered",
  "isskitude": "1"
}
```

https://datacdn.skitude.com

- app_specifc_db
 - getnewappdb.php?app_id=Y29tLmItbGFic29sdXRp
 - getnewappdb.php?app_id=Y29tLmItbGFic29sdXRp
 - getnewappdb.php?app_id=Y29tLmItbGFic29sdXRp
 - getnewappdb.php?app_id=Y29tLmItbGFic29sdXRp
 - getnewappdb.php?app_id=Y29tLmItbGFic29sdXRp
- app_db
 - skitude_data.db.zip
- app_resorts_pois
 - pois_2032.sqlite.zip
 - pois_1019.sqlite.zip
 - pois_1550.sqlite.zip

```
"result": "success",
"user_name": "Yury",
"user_surname": "Chemerkín",
"user_birthday": 0,
"gender": "",
"user_weight": "0 kg",
"user_height": "0 cm",
"activity_prefer": "",
"privacy_media": 0,
"privacy_tracks": 0,
"privacy_profile": 0,
"privacy_activity": 0,
"getnewsletter": 1,
"getchallengeinfo": 1,
"getactivityinfo": 1,
"getcommunications": 1,
"country": "",
"share_position": 0,
"modified": 1571815013
```

SKITUDE – DETAILS

- Analytics, 3rd party sdk – Google, Facebook, Crashlytics
- No useful backup data
 - Tracks & Images - Documents\skitude_tracking.db & skitude_images.db
 - Friends - FFDData.db
 - Avatar – avatar.jpg
 - May also contains separate photos, videos, audio and temp data from Apple Watch
- Examples are on next slides

SKITUDE – DETAILS

Table: userdata

	distancefilter	username	personalmessage	actualstatus
	Filter	Filter	Filter	Filter
1	NULL	yurychemerkin		offline

Table: contacts

currentimage	contactusername	username	profileimage	personalmessage	lat	lon	cation_timestam	status
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter

Table: points

track	_id	lat	lng	time	speed	subtrack	accuracy	altitude	bearing	vertical_accuracy	pause
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter

Table: tracks

synchronize	in_statistics	_id	name	time	date	duration	resort_id	distance	max_speed	mean_speed	height_diff	description	annotation
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter

New Record Delete Record

distance	max_speed	mean_speed	height_diff	description	annotation	type	inserver_id	status	challenge_id	privacy	timestamp	device	uuid
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter

Table: images

_id	name	lat	lng	orientation	date	track	username	url	check_resort	resort_id	public	challenge_id	privacy
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter

New Record Delete Record

SHARING YOUR DATA. LEAKING OUT OF HEALTH APP



INTER-ACCESS:
GYMAHOLIC,
WELLTORY,
FATMAP,
CYCLEMETER



DISCOVERING IDs:
MUSCLE BOOSTER



TRANSFERRING:
WELLTORY



NOT CLEANING:
GYMNOTIZE

SECURE APPS. NO DATA, NO ISSUES

- No backup data, no network data
 - Speed tracker, Altimeter
 - Workouts++, Gymatic, Flexi, Hussle, & Smart gym, BodyWeight
 - Squaw alpine, JollyTurns, Avalance
- No network data
 - Pillow, SleepWatch
 - Cyclemeter, FitmeterBike, Crono
 - Muscle Booster
- No backup data
 - Pacer, GYM & Freelitics, Gymnotize, Centr
 - Ullr & Maps, Snow Forecast, Slopes

OVERLOADED APPS



ROAD BIKE, MOUNTAIN
BIKE, ISKATE, BIKE
TRACKS, CYCLEMETER,
FITMETER BIKE, FATMAP,
RUNNING, WELLTORY,
RUNKEEPER



ULLR & MAPS, SNOW
FORECAST, SLOPES,
SKITUDE, SKITRACKS,
RIDERS, FATMAP, FITNESS
BUDDY, CENTR,
WELLTORT



ISKATE, SKITRACKS,
FITNESS BUDDY, CENTR,
RUNKEEPER

ANALYTICS & SDK – 16

- Google, Facebook, Crashlytics, io.branch
- Flurry, Mopub, Appsflyer, Amplitude, AWS ads
- NewRelic, Localytics, Zendesk, MixPanel
- AppAnex, Twitter, OneSignal

AMOUNT OF DATA WASTED ON ANALYTICS MODULES

- Reduced from 0.5 TB per year down to 0.063 TB
- 1 hour: 0.59 → 0.06
- 1 day: 1.76 → 0.18
- 1 week: 12.30 → 1.23
- 1 month: 52.73 → 5.27
- 1 year: 632.81 → 63.28

APPS – 50

- Strava, RunGap, Pacer, Nike RUN Club & Training, MyFitnesspal
- Smartgym, Gymaholic, GYM & Freelitics, Flexi
- Hussle, Strong
- Pillow, HeartWatch, SleepWatch, Welltory
- RunKeeper, Road & Mountain Bike, iSkate, Bike Tracks, SpeedTracker, CycleMeter, FitMeter Bike, Crono, Altimeter
- Ullr & Ullr Maps, Squaw alpine, Snow forecast, SnocRu, Slopes, Skitude, SkiTracks, Ski AR, Jolly Turns, Riders, Fatmap, Avalanche
- Workouts++, Running, Gymatic, Gymnotize, Muscle Booster, Fitness buddy, Centr, Body weight, Asan Rebel, Training (Adidas, Runtastic)

Total, GB

700.00

600.00

500.00

400.00

300.00

200.00

100.00

0.00

0.06 0.29 0.59

0.18 0.88 1.76

1.23 6.15 12.30

5.27 26.37 52.73

63.28 316.41 632.81

1 hour

1 day

1 week

1 month

1 year

Low, GB

0.06

0.18

1.23

5.27

63.28

Medium, GB

0.29

0.88

6.15

26.37

316.41

High, GB

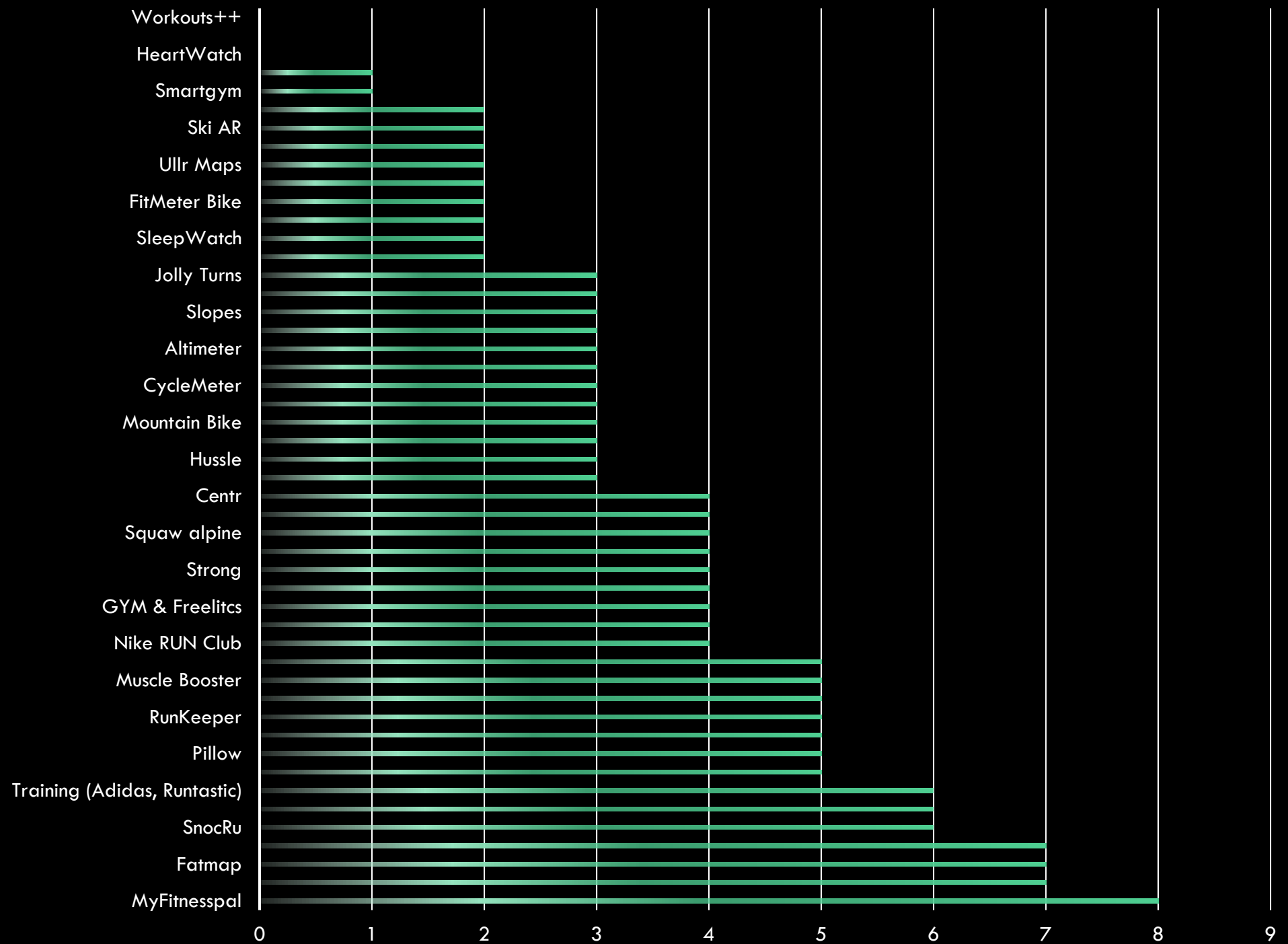
0.59

1.76

12.30

52.73

632.81



STILL SECURE. WE EMPOWER WHAT WE HARDEN BECAUSE WE CAN CONCEAL



YURY CHERMERKIN

SEND A MAIL TO: YURY.S@CHEMERKIN.COM



ADD ME IN LINKEDIN:

[HTTPS://WWW.LINKEDIN.COM/IN/YURYPHERMERKIN](https://www.linkedin.com/in/yurychermerkin)