



Облачные хранилища Apple, Google, Microsoft. Что может быть извлечено

Частная компания, основанная в 1990 году

Полностью внутренние разработки

Microsoft Gold Certified Partner, Intel Software Partner

Зарегистрированный разработчик NVIDIA и AMD



Более 300 партнеров на всех континентах

6 зарегистрированных патентов США

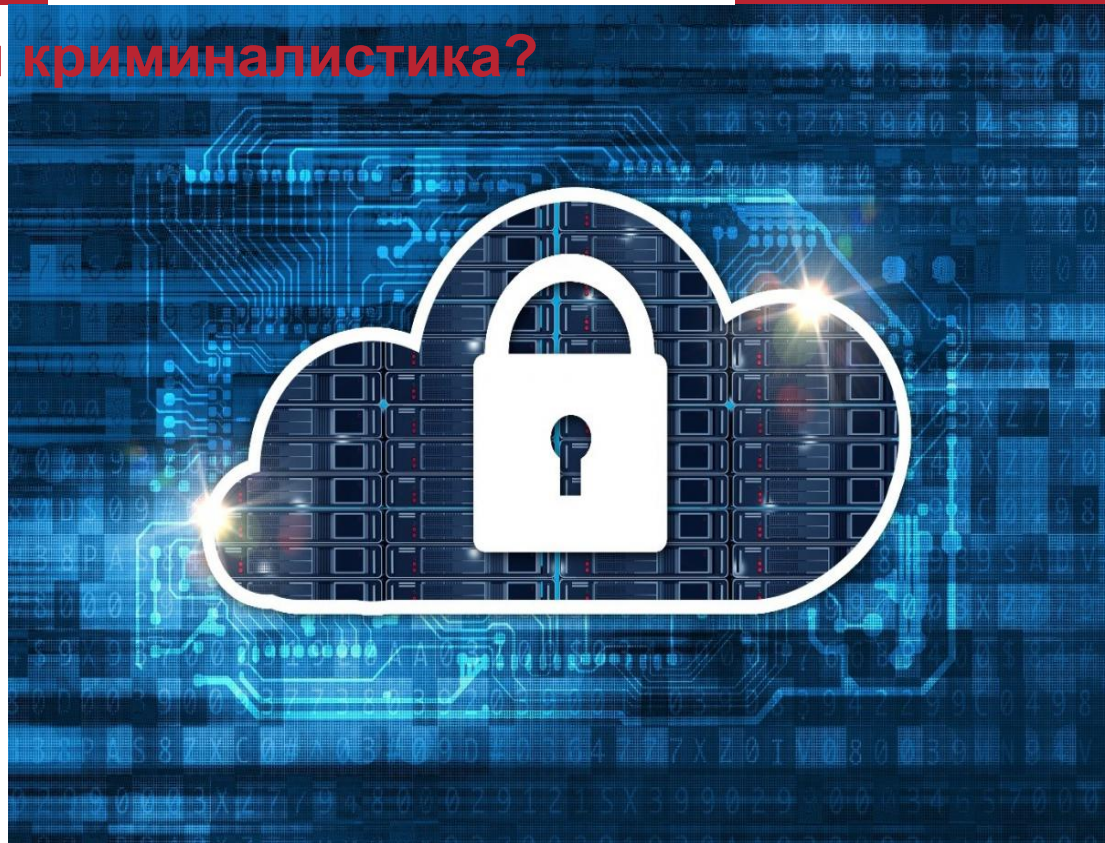
*Корпоративные, государственные, военные
и правоохранительные организации по всему миру*

Более 200 000 установок по всему миру



Почему облачная криминалистика?

- Помогает в случаях, когда **устройства защищены паролем и зашифрованы**
- «Последнее спасение»: может извлечь данные, которые недоступны другими способами
- Apple настойчиво рекомендует использование iCloud
- Google собирает данные **со всех** подписанных устройств
- Облако может содержать намного больше данных, чем само устройство



Облачные экосистемы

- **Apple iOS**
 - В облаке хранится полная резервная копия устройства
 - Резервная копия содержит наибольшее количество информации
 - Синхронизированные данные (звонки, контакты, пароли iCloud Keychain)
- **Google Android**
 - Резервные копии Android ограниченно полезны
 - Google Account хранит массу информации включая пользовательские синхронизированные данные и данные о пользователе, которые собирает Google
- **Windows Phone, Windows 10 Mobile**
 - Резервные копии
 - Собранные и синхронизированные данные (в меньшем количестве в сравнении с Google, но в большем по сравнению с iOS)

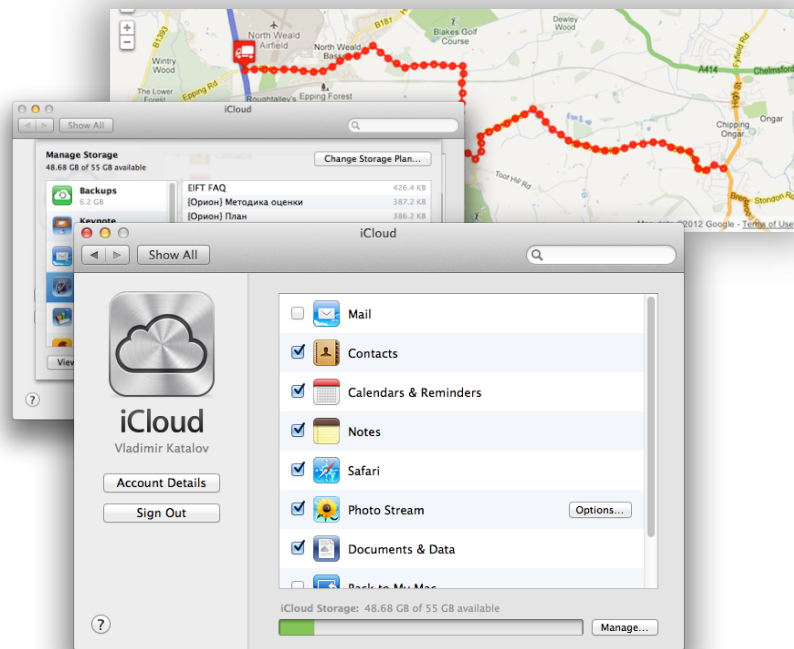


iCloud: резервные копии



То же, что и в локальных резервных копиях:

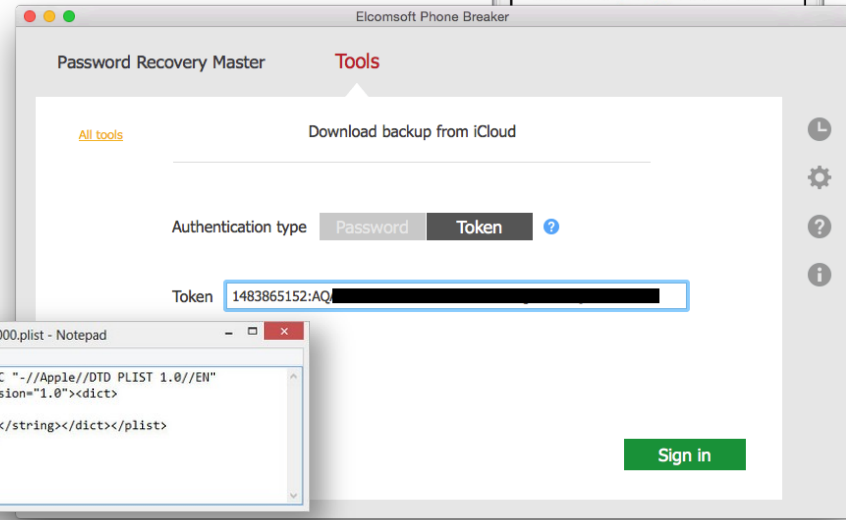
- Контакты
- Сообщения (вкл. iMessages)
- Звонки
- **Пароли iCloud Keychain**
- Данные приложений
- Настройки телефона
- Фотоальбом (фото и видео)
- Покупки (музыка, фильмы, TV, Apps, книги)
- Учётные записи E-Mail аккаунты
- Настройки интернета (сохраненные Wi-Fi, точки доступа, VPN и т.д..)
- Устройства, подсоединенные через Bluetooth
- Данные приложений и базы данных SQLite (возможен доступ к удалённым записям)
- Закладки Safari, Cookies, история просмотра, Offline-данные
- История местоположения пользователя
- ... И многое другое
- **За исключением IMEI**



Маркер аутентификации



- 2FA защищает доступ к резервным копиям
- Код подтверждения высылается на доверенное устройство
- Альтернативы:
 - Apple ID пароль + верификационный код
 - Apple ID пароль + Recovery Key
 - **Маркер аутентификации** – бинарный маркер аутентификации, сохраненный на компьютере пользователя





Почему Google Cloud?

- Десятки тысяч моделей устройств
- Несколько тысяч производителей
- Не каждое Android-устройство является Google-устройством
- Разные способы извлечения данных

Извлечение данных Google Аккаунта

- **Общий вход в базу данных**
- **Унифицированный подход к хранению данных**
- **Огромный массив данных**



Google Takeout

- Оставляет следы
- Не все данные экспортируются (например Dashboard)
- Неудобная выборка данных
- Много неудобных форматов
- Оповещение пользователя через email

Что хранится

- Подробные, максимально детализированные данные о местоположении пользователя начиная с 2010 года
- Информация об использовании устройств
- Поисковые запросы
- Подробная история посещаемых веб-сайтов и просмотренных страниц
- Закладки, контакты
- История телефонных звонков
- Для Android 8.0 Oreo: SMS сообщения
- Запросы к голосовому помощнику (включая запись голоса)

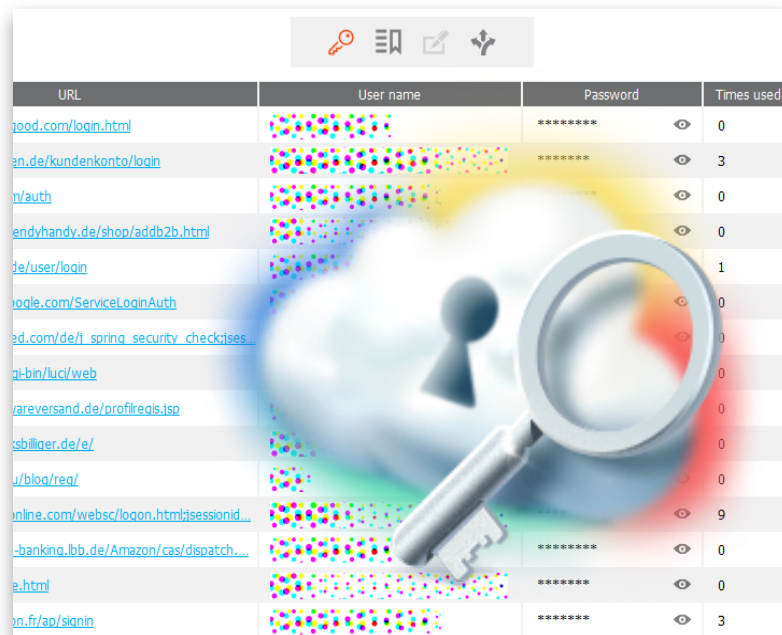


- Почта Gmail
- Календари, события, напоминания
- **Ключи и пароли от веб-сайтов, соц. сетей, Wi-Fi**



Elcomsoft Cloud Explorer - удобный инструмент для скачивания, просмотра и анализа данных

- Google ID + пароль
- Поддержка двухфакторной аутентификации
- Просмотр, поиск, настраиваемые фильтры, экспорт данных
- Пароли из Google Chrome
- Переходы между страницами
- NEW: экспорт всех данных в Excel



URL	User name	Password	Times used
ood.com/login.html	[REDACTED]	*****	0
en.de/kundenkonto/login	[REDACTED]	*****	3
n/auth	[REDACTED]	*****	0
endvhandv.de/shop/addb2b.html	[REDACTED]	*****	0
de/user/login	[REDACTED]	*****	1
oogle.com/ServiceLoginAuth	[REDACTED]	*****	0
ed.com/de/i_spring_security_check.jses	[REDACTED]	*****	0
g-bin/luc/web	[REDACTED]	*****	0
areversand.de/profilregis.jsp	[REDACTED]	*****	0
sbilliger.de/e/	[REDACTED]	*****	0
u/blog/req/	[REDACTED]	*****	0
nline.com/websec/login.html?isessionid...	[REDACTED]	*****	9
-banking.lbb.de/Amazon/cas/dispatch...	[REDACTED]	*****	0
e.html	[REDACTED]	*****	0
on.fr/ap/signin	[REDACTED]	*****	3

Что хранится

- Ограниченные данные о местоположении пользователя
- Информация об использовании устройств
- Поискные запросы Bing
- Подробная история посещаемых веб-сайтов и просмотренных страниц Edge / IE
- Закладки, контакты
- История телефонных звонков
- SMS сообщения
- Запросы Cortana



- Почта Outlook.com, Hotmail
- Календари, события, напоминания
- **Ключи и пароли от веб-сайтов, соц. сетей**

Elcomsoft Mobile Forensic Bundle:

- Elcomsoft iOS Forensic Toolkit (PC, Mac)
- физическое извлечение данных из 32- и 64-битных iOS-устройств
- Elcomsoft Phone Breaker (PC, Mac)
- извлечение данных из локальных и облачных резервных копий iOS, Windows Phone/W10M, BB10; восстановление паролей к резервным копиям
- Elcomsoft Phone Viewer
- компактный и быстрый инструмент для просмотра и поиска информации
- Elcomsoft eXplorer for WhatsApp
- извлечение, расшифровка и просмотра истории коммуникаций WhatsApp.



- 7,599,492 - Система и метод быстрого восстановления криптографического ключа (*Fast cryptographic key recovery system and method*);
- 7,783,046 - Идентификация вероятного ключа шифрования с детерминированным результатом (*Probabilistic cryptographic key identification with deterministic result*);
- 7,787,629 - Использование графических процессоров как со-процессоров параллельного вычисления для перебора паролей (*Use of graphics processors as parallel math co-processors for password recovery*);
- 7,809,130 - Система и метод восстановления паролей (*Password recovery system and method*);
- 7,929,707 - Использование графических процессоров как со-процессоров параллельного вычисления для перебора паролей (*Use of graphics processors as parallel math co-processors for password recovery*).



ЭлкомСофт является признанным экспертом на рынке восстановления доступа к защищенным файлам и системам, а также в области компьютерной криминалистики. Технологические достижения компании и экспертные оценки часто цитируются во множестве авторитетных публикаций на разных языках, например:

'Microsoft Encyclopedia of Security', 'The art of deception' (Kevin Mitnick), 'IT Auditing: Using Controls to Protect Information Assets' (Chris Davis), 'Hacking exposed' (Stuart McClure), 'Hacking For Dummies' (Kevin Beaver), 'Practical Intrusion Analysis: Prevention and Detection for the Twenty-First Century' (Ryan Trost), 'FISMA Certification & Accreditation Handbook' (L. Taylor), 'Computer Network Security: Theory and Practice' (Jie Wang), 'A+ Certification Study Guide, Sixth Edition' (Jane Holcombe, Charles Holcombe), 'Investigating Digital Crime' (Robin PBryant), 'Security Engineering: A Guide to Building Dependable Distributed Systems' (Ross J. Anderson), 'Network Know-How: An Essential Guide for the Accidental Admin' by John Ross, 'Hacking Exposed: Network Security Secrets and Solutions, Sixth Edition' (Stuart McClure, Joel Scambray, George Kurtz), 'Windows Server 2008 PKI and Certificate Security' (Brian Komar), и другие.

Наши клиенты



Государственные



Финансовые

Bank of America

EQUIFAX

J.P.Morgan citibank



HSBC

CREDIT SUISSE

Высокие технологии

Microsoft



IBM



Ритейл

Woolworths



Walmart

Консалтинг

KPMG

ANDERSEN CONSULTING

ERNST & YOUNG



Deloitte.

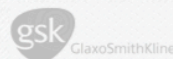
Телекоммуникации



france telecom

Фармацевтика

Johnson+Johnson



NOVARTIS



Производство

LOCKHEED MARTIN

SIEMENS



BOEING



www.elcomsoft.ru
olga@elcomsoft.com
+7 (495) 974-1162

