КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ
ИТОГИ

КОД ИБ ИТОГИ | 08 ДЕКАБРЯ 2022

КАК ЗАЩИТИТЬСЯ ОТ ИНСАЙДЕРА, КОГДА НА ЭТО СОВСЕМ НЕТ ДЕНЕГ

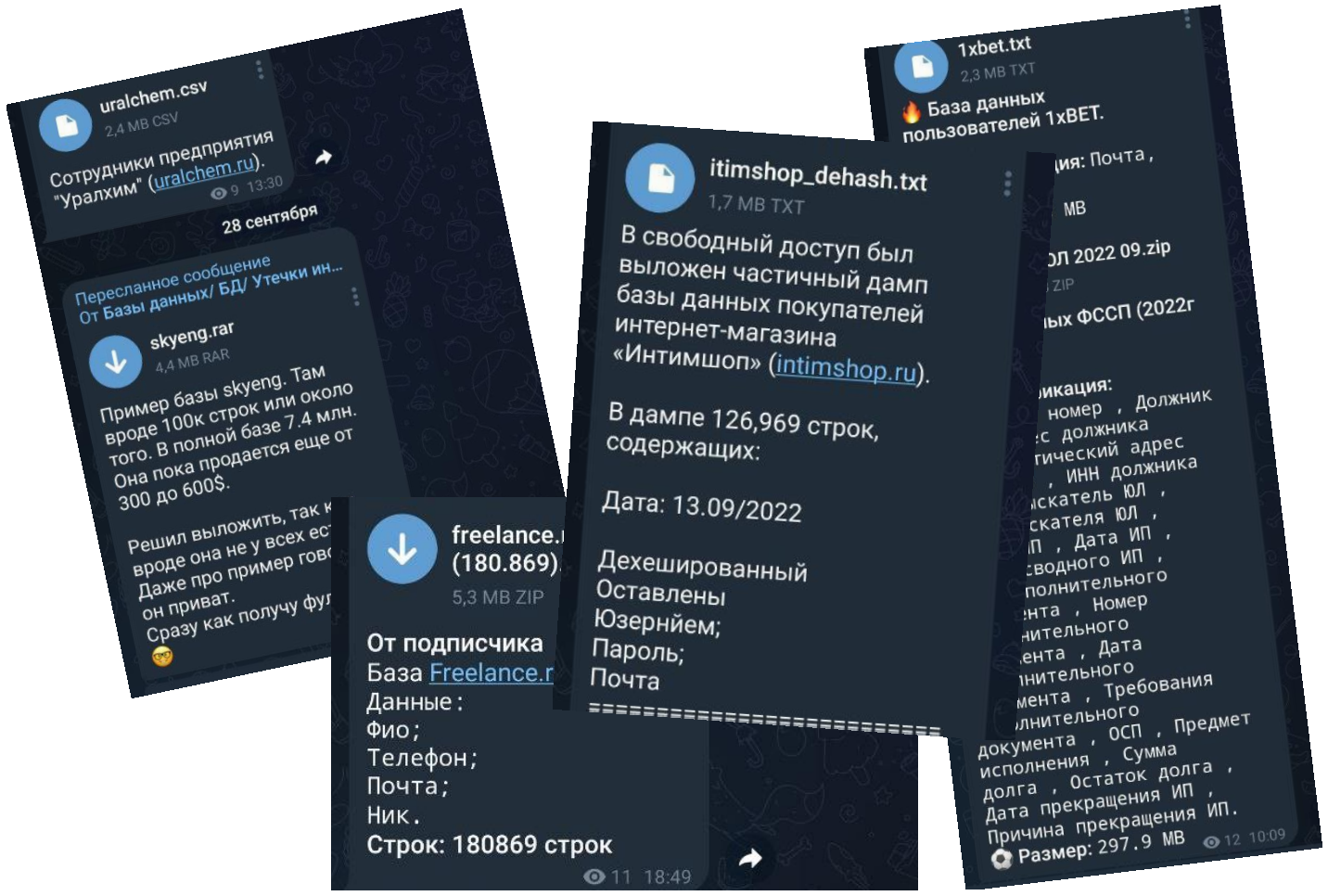
ДМИТРИЙ БОРОЩУК

МОСКВА

ОСНОВНЫЕ УГРОЗЫ

ЦЕЛЕВЫЕ АТАКИ

Телефон: 79258584075
Имя: Борощук Дмитрий
Яндекс Еда: потрачено за 6 мес 12210 руб
Устройство: Android
Модель устройства: Mozilla/5.0 (Linux; Android 11; SM-N770F
Build [redacted]
Chro[redacted]1
(samsung; SM-N770F[redacted]
Заказы: посёл[redacted]
1. 2021-07-03T23:23:45.000Z - 1212 руб
Заказы: Моск[redacted]1,
этаж 7, домофон[redacted]
1. 2021-09-29T22:28:49.000Z - 611 руб
2. 2021-09-30T18:55:23.000Z - 840 руб
3. 2021-10-04T19:04:27.000Z - 464 руб
4. 2021-10-09T15:28:34.000Z - 762 руб
5. 2021-10-27T12:57:30.000Z - 2797 руб (Хинкальная №1)
6. 2021-11-14T14:40:24.000Z - 723 руб
7. 2021-12-20T16:52:06.000Z - 701 руб
8. 2021-12-26T17:04:03.000Z - 1964 руб
9. 2021-12-31T13:03:27.000Z - 977 руб
Заказы: М[redacted],
этаж 22, дом[redacted]
1. 2021-10-04T14:30:33.000Z - 1159 руб (Нори Мио)
VK Имя: Din
Фамилия: Moriarti
Email: [redacted]
Пароль: FallenART
Имя в СДЭК: Дмитрий
Email: Beholderishere@gmail.com
Никнейм на Пикабу: BeholderIsHere



IPlogger

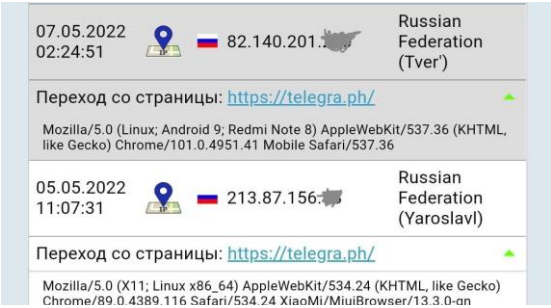
Сервис для создания треккеров с различными способами доставки до субъекта наблюдения с удобным интерфейсом управления и сбора данных.

Возможности:

- Запрос GPS
- IP треккер
- “Невидимый пиксель”
- Fingerprint устройства

WEB	WIN	MAC	LINUX	ANDROID	iOS

[iplogger.org]



CANARYTOKENS

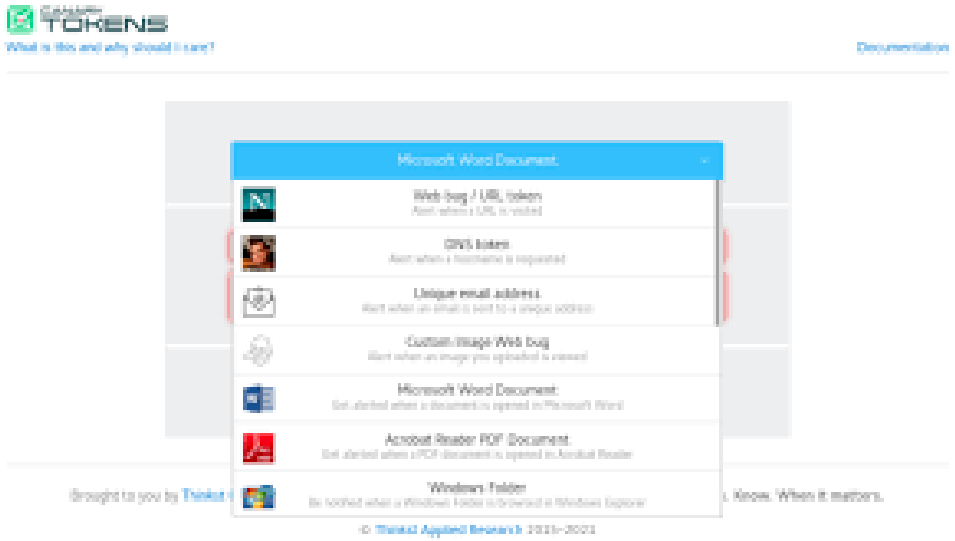
Сервис для создания трекеров срабатывающих на различные пользовательские действия и отправляющий ip адрес и отпечаток системы совершившего действия вам на почту.

Имеет возможность привязать к отправке информации о пользователи различные триггеры:

- Открытие документа
- Открытие папки
- Переход по определенному адресу
- Пересылка по электронной почте

WEB	WIN	MAC	LINUX	ANDROID	iOS

[canarytokens.org]



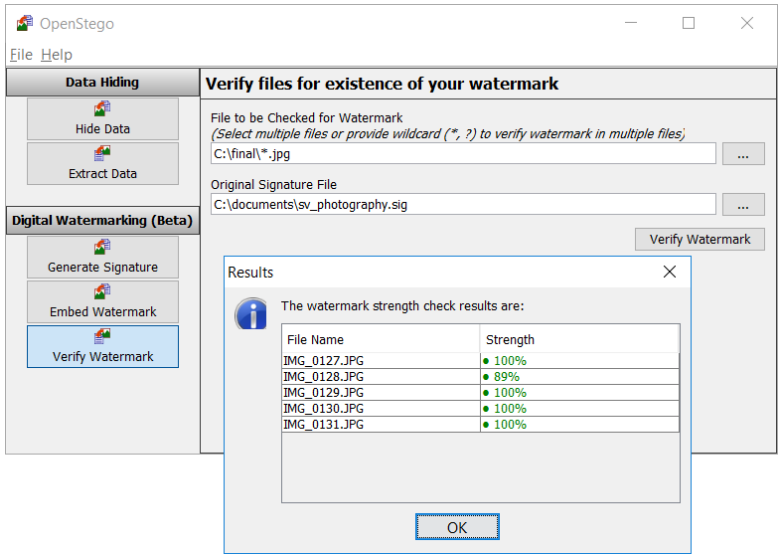
«ВОДЯНЫЕ ЗНАКИ»

OpenStego

- Скрытие любых данных в «файле- обложке»
- Встраивание «водяных знаков»

WEB	WIN	MAC	LINUX	ANDROID	iOS

[www.openstego.com]



«ВОДЯНЫЕ ЗНАКИ»

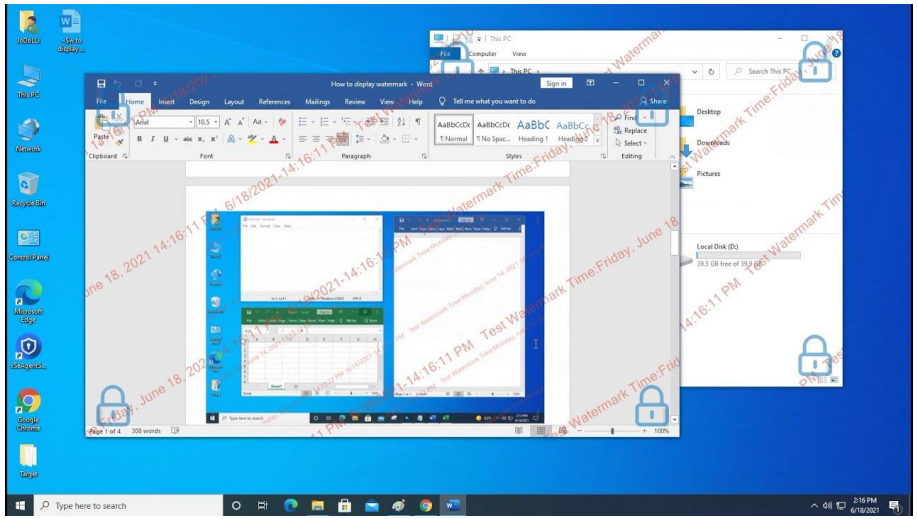
Screen Watermark

Вы можете вывести нужный водяной знак непосредственно на экран. Такой водяной знак не влияет на работу других программ. Кроме того, в качестве водяного знака можно использовать до четырех видов текстовой информации и изображений.

- Автоматически перезапускается после перезагрузки компьютера (даже в безопасном режиме).
- Поддерживает мультисеансовые среды: водяной знак отображается при смене пользователя.
- Водяные знаки веб-камеры могут отображаться на видеоэкране организатора и участника во время видеоконференции.
- Водяной знак не отображается на экране, и водяной знак может быть включен в снятое изображение при захвате экрана.

WEB	WIN	MAC	LINUX	ANDROID	iOS

dn.xsecuritas.com/person_download/Setup-screen-watermark.exe



«ВОДЯНЫЕ ЗНАКИ»

Output Watermark

Вы можете распечатать водяной знак. Водяные знаки можно выводить даже в файлах формата PDF или XPS. Вы также можете решить, следует ли печатать водяные знаки для каждого отдельного приложения.

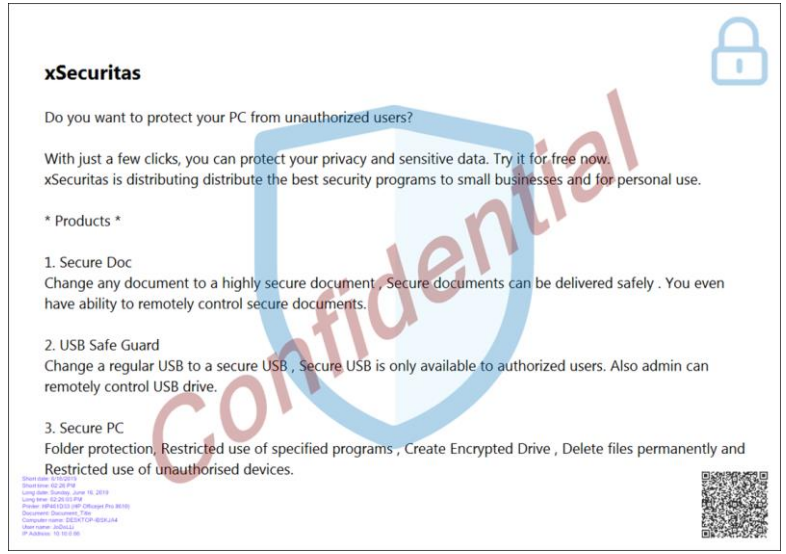
Водяной знак печатается даже при выводе в форматы PDF, XPS и других

Метаданные водяных знаков поддерживают различные виды информации. Например, дата и время вывода, имя принтера, имя документа, имя пользователя и т. д. могут быть выведены в виде водяного знака.

Водяные знаки поддерживают:
- до четырех типов текстовых водяных знаков.
- до четырех типов изображений.
- один QR-код.

WEB	WIN	MAC	LINUX	ANDROID	iOS

https://dn.xsecuritas.com/person_download/Setup-output-watermark.exe



VIRUS TOTAL

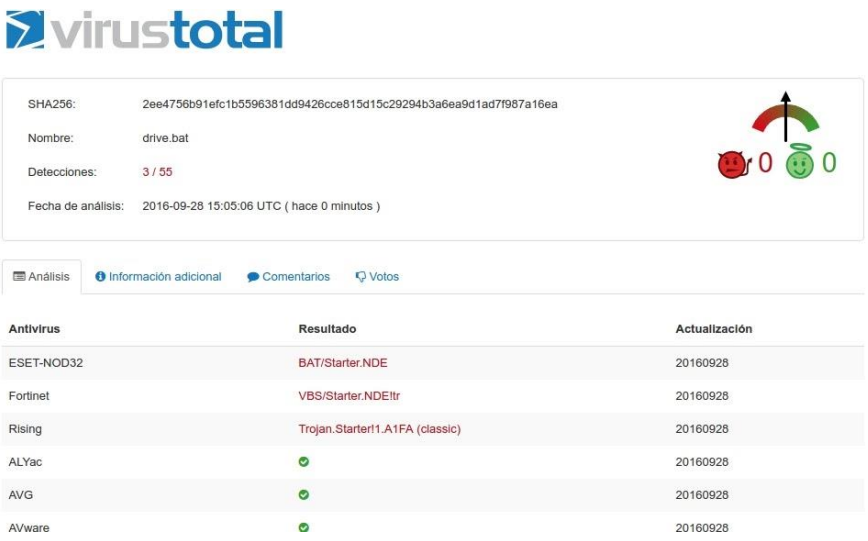
Облачные антивирусные сканеры для:

- файлов
- ссылок
- доменов
- хешей
- ip адресов

Кроме сканирования на угрозы может вытаскивать метаданные и перечень запрашиваемых разрешений.

WEB	WIN	MAC	LINUX	ANDROID	iOS

[www.virustotal.com/gui/home/search]



ОСНОВНЫЕ УГРОЗЫ

VeraCrypt

Шифрование данных для Windows/MacOs/Linux

- Создание зашифрованных контейнеров
- Создание зашифрованных разделов
- Работа с ключами
- Мультифакторная авторизация

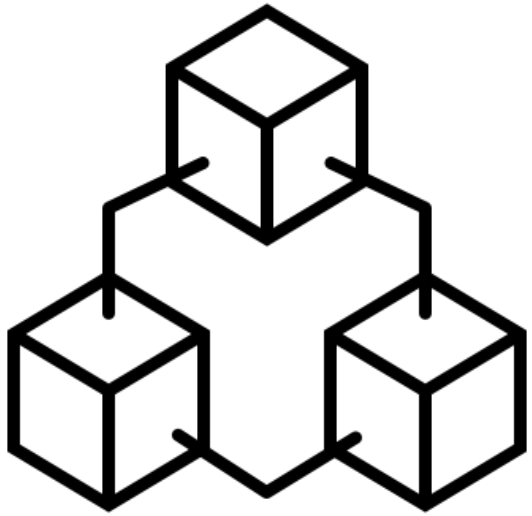
WEB	WIN	MAC	LINUX	ANDROID	iOS

[veracrypt.fr]

TinyCheck

github.com/KasperskyLab/TinyCheck

АНТИ ФОРЕНЗИКА



ФАКТИЧЕСКИЙ ДОСТУП К УСТРОЙСТВУ.

- Прямое извлечение информации с встроенных носителей.
- Восстановление удаленных данных носителей.
- Извлечение информации из log- файлов системы
- Извлечение кэша приложений
- Извлечение сведений об учетных записях в различных сервисах.
- Извлечение сведений о подключение WiFi/BT
- Восстановление истории сетевой активности
- Восстановление данных из оперативной памяти (Cold boot atak-и)
- Возможная расшифровка крипто-контейнеров

ФАКТИЧЕСКИЙ ДОСТУП К УСТРОЙСТВУ.

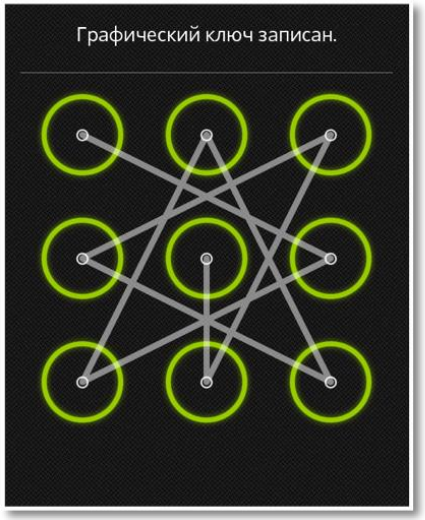
- ✓ Прямое получение от пользователя связки логин/пароль
- ✓ Обход защиты учетной записи при помощи загрузочных инструментов
- ✓ Получение данных о связке логин/пароль при помощи наблюдения
- ✓ Использование «временного окна» между отходом пользователя от АРМ и автоматической блокировкой при бездействии

АНТИ ФОРЕНЗИКА

МИНИМИЗАЦИЯ «ТОЧЕК ВХОДА»

АУТОТЕНТИФИКАЦИЯ:

- ✓ Парольная фраза от 12 символов.
- ✓ Сложный графический ключ.
- ✓ Мульти факторная авторизация.
- ✓ Отключить биометрию.
- ✓ Отключить SmartLock
- ✓ Не хранить пароли в Google Chrome

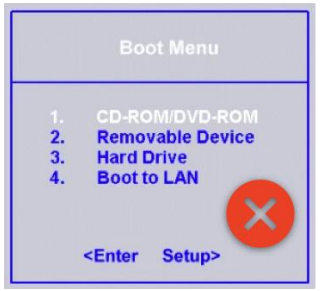


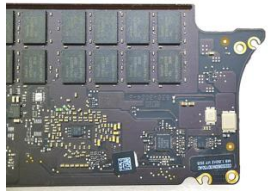
АНТИ ФОРЕНЗИКА

МИНИМИЗАЦИЯ «ТОЧЕК ВХОДА»

АППАРАТНЫЕ ИНТЕРФЕЙСЫ:

- ✓ Заблокировать BIOS / Bootloader
- ✓ Отключить отладочный режим USB Debuging
- ✓ Включить режим USB «Только зарядка»
- ✓ Запретить альтернативные варианты загрузки.
- ✓ Использовать быстро съемный/уничтожаемый носитель данных.
- ✓ Заблокировать доступ к контактным группам чипов BIOS, RAM, eMMC, SSD





АНТИ ФОРЕНЗИКА

МИНИМИЗАЦИЯ «ТОЧЕК ВХОДА»

ОБЛАЧНЫЕ СЕРВИСЫ:

- ✓ Берегите логины/пароли от облачных сервисов
- ✓ Отключайте автоматическое копирование

АНТИ ФОРЕНЗИКА

МИНИМИЗАЦИЯ «ТОЧЕК ВХОДА»

Что хранят ваши гаджеты в облаке
или когда не нужен даже телефон:

Apple

- Резервные копии
- Синхронизированные данные: контакты, заметки, календари, закладки браузера Safari и т.п.
- Фотографии (если включён iCloud Photo Library), в т.ч. недавно удалённые
- Журнал звонков и историю браузера
- Некоторые данные Карт

Если узнают код блокировки телефона или пароль от компьютера Mac, то и все «облачные» пароли (iCloud Keychain) и данные «Здоровья» (журнал повседневной активности), а также SMS и iMessage

Google

- Резервные копии и данные приложений (кстати, в Android именно в этой категории будут храниться журналы звонков, SMS, а также маркеры аутентификации отдельных приложений)
- Резервные копии в Android 9 и более свежих версиях будут зашифрованы паролем блокировки экрана; для их расшифровки потребуется этот код блокировки. А вот для более старых версий Android шифрования резервных копий не предусмотрено
- Синхронизированные данные: календари, контакты, заметки
- Пароли Chrome (какой-либо дополнительной защиты, как в iOS, для них не предусмотрено)
- Подробнейшая история местоположения за последние много лет. Пожалуй, на этот пункт будут обращать внимание в первую очередь.
- История браузера и поисковых запросов. Исследуется в обязательном порядке.
- Почта Gmail, которую можно использовать, например, для сброса пароля к другим учётным записям

АНТИ ФОРЕНЗИКА

ШИФРОВАНИЕ

ДЛЯ КОМПЬЮТЕРА:

VeraCrypt [veracrypt.fr] - Шифрование данных для Windows/MacOs/Linux

- Создание зашифрованных контейнеров
- Создание зашифрованных разделов
- Работа с ключами
- Мультифакторная авторизация

ДЛЯ СМАРТФОНА:

BoxCryptor [boxcryptor.com] - шифрование файлов в облаках

EDS [sovworks.com] - работа с крипто-контейнерами для Android

АНТИ ФОРЕНЗИКА

СТЕГАНОГРАФИЯ

OpenStego [www.openstego.com]

- Скрытие любых данных в «файле- обложке»
- Встраивание «водяных знаков»

OpenPuff [embeddedsw.net/OpenPuff_Steganography_Home_ru.html]

- поддерживает форматы файлов: Изображения (BMP, JPG, PCX, PNG, TGA) Аудио файлы (AIFF, MP3, NEXT/SUN, WAV) Видео (3GP, MP4, MPG, VOB) Flash-Adobe (FLV, SWF, PDF
- двойное скрытие
- разделение на цепочку файлов

DeepSound [jpinsoft.net/deepsound]

скрытие файлов в аудио файлах или cd треках

АНТИ ФОРЕНЗИКА

ОТРИЦАНИЕ ШИФРОВАНИЯ

МЕССЕНДЖЕРЫ:
- Graph Messenger [www.graphmessenger.com] - Использует API Telegram
- Briar [briarproject.org] - Децентрализованный мессенджер

OS ANDROID
- LineageOS [lineageos.org] - Альтернативная прошивка AOSP Android

КОМПЬЮТЕР
VeraCrypt [veracrypt.fr] - Создание шифрованных разделов Windows/MacOs/Linux

СКРЫТОЕ РАБОЧЕЕ ПРОСТРАНСТВО
NextCloud [nextcloud.com] удаленное рабочее пространство
HiddenVM [ithub.com/aforensics/HiddenVM] скрытая виртуальная машина на базе TAILS OS
TAILS OS [tails.boum.org] Live-дистрибутив

АНТИ ФОРЕНЗИКА

УДОБСТВО

ДЛЯ СМАРТФОНА:
Ripple [guardianproject.info/apps/info.guardianproject.ripple] - мощная и гибко настраиваемая система унииктожения информации на Android устройствах.

ДЛЯ КОМПЬЮТЕРА:
UsbKill [github.com/hephaest0s/usbkill] - запуск очистки системы при удаление usb устройства

АНТИ ФОРЕНЗИКА

- ✓ Понимание основ криминалистического анализа и его возможностей.
- ✓ Полное шифрование встроенного носителя информации.
- ✓ Использование быстро съёмный/уничтожаемых носителей информации в качестве системного устройства.
- ✓ Не восстанавливаемое удаление файлов при помощи специального ПО
- ✓ Отключение Swap-а
- ✓ Программная система очистки логов системы
- ✓ Использование системы быстрой очистки оперативной памяти

АНТИ ФОРЕНЗИКА

- ✓ Использование мульти-факторный аутентификации
- ✓ Использование системы контроля нахождения пользователя в пределах контроля за АРМ.
- ✓ Использование крипто-контейнеров.
- ✓ Использование крипто-контейнеров с двойным дном.
- ✓ Маскировка криптоконтейнеров.
- ✓ Использование нативного триггера запуска контрмер.

T.ME/BEHOLDERISHERE

T.ME/FORENSICTOOLS