Belkasoft
forensics made easier

702 San Conrado Terrace,
Unit 1 Sunnyvale CA, Estados
Unidos 94085
+1 (650) 272-0384 (EE.UU. y
Canadá)correo electrónico:
sales@belkasoft.com

Belkasoft Evidence Center X
Especificaciones técnicas

Belkasoft Evidence Center X (Belkasoft X) es una solución forense digital todo en uno y de respuesta a incidentes para adquirir, localizar, extraer y analizar pruebas digitales almacenadas dentro de ordenadores y dispositivos móviles, RAM y nube, drones y coches.

El producto se ofrece en varias ediciones. La versión actual del documento cubre Belkasoft X Forensic v.2.4.

Índice

Belkasoft
forensics made easier

702 San Conrado Terrace,
Unit 1 Sunnyvale CA, Estados
Unidos 94085
+1 (650) 272-0384 (EE.UU. y
Canadá)correo electrónico:
sales@belkasoft.com

Belkasoft X Forense

Tipos de adquisición admitidos

Belkasoft X Forensic soporta varios métodos de adquisición de dispositivos:

- Adquisición de la memoria RAM (memoria volátil) de la máquina Windows en ejecución - realizada mediante la herramienta Live RAM Capturer incluida en el paquete de instalación.

- Adquisición de discos duros y extraíbles en formato RAW o E01.

- Adquisición de imágenes con Tableau TX1. La adquisición se ejecuta desde la interfaz X de Belkasoft, no se requiere comunicación con Tableux.

- Adquisición de la tarjeta SIM
  - Al adquirir un dispositivo móvil Android. Tiene que ser la primera ranura en caso de dispositivos con varias ranuras.
  - Con el uso de un lector hardware de tarjetas SIM

    Se admiten tarjetas SIM con código PIN, se muestra el número de intentos restantes.

Adquisición de dispositivos iOS:

- Adquisición lógica mediante copias de seguridad de iTunes (para iPhones y iPADs)
  - La copia de seguridad de iTunes puede crearse con cifrado forzado

- Adquisición de iOS basada en agentes
  - Modelos de dispositivos iOS: iPhone 5S a iPhone X, así como los más recientes iPhone XS/XS Max, iPhone XR, iPhone 11/Pro/Pro Max, iPhone 12, iPhone SE (2.ª generación), iPad Air (3.ª generación) y iPad Pro (3.ª generación), entre otros.
  - Versiones de iOS compatibles:
    - 10.3.3 a 15.1.1 (sistema de archivos completo y llavero)
    - 15.2 a 15.7.1 (sistema de archivos parcial que no incluye algunas bases de datos del sistema como SMS, calendario y similares)
    - 16.0 a 16.5 (sistema de archivos completo y llavero)
  - Podría funcionar sin ID de desarrollador de Apple de pago.

- Adquisición de iPhone 5S-iPhone X y para iPads con tipos de procesadores similares sin jailbreak.

- Adquisición mediante el protocolo Apple File Conduit (AFC).
  - Requiere que iTunes esté instalado en la máquina donde se ejecuta Belkasoft X.

- Adquisición de iOS con autenticación de archivos de bloqueo. *Nota: los archivos de bloqueo deben ser válidos (no caducados).*[1]

1

702 San Conrado Terrace, Unit 1 Sunnyvale CA, Estados Unidos 94085
+1 (650) 272-0384 (EE.UU. y Canadá)correo electrónico: sales@belkasoft.com

- Extracción del registro de fallos de iOS sin jailbreak. Tener un código de acceso o un archivo de bloqueo del dispositivo es suficiente.

- Copia de seguridad lógica completa de dispositivos iOS con jailbreak, incluida la adquisición de dispositivos iOS con jailbreak checkra1n.

- Capturador de pantalla iOS (adquisición de datos mediante captura de pantalla automatizada), hasta iOS 16.6.1.

Adquisición de dispositivos Android:

- Adquisición lógica a través de ADB.
  - Se admiten copias de seguridad ADB cifradas.
  - Adquisición de la tarjeta SD de Android es compatible a través del método de copia de seguridad ADB.
  - Soporte para el inicio automático de una copia de seguridad ADB.

- Adquisición basada en agentes
  - También se admite la adquisición basada en agentes mediante tarjeta SD.

- Adquisición física de Android o EDL (para dispositivos Android rooteados).

- Adquisición lógica de Android (para dispositivos Android rooteados).

- Android Advanced ADB backup (combinación de todos los métodos disponibles con ADB).

- Adquisición de dispositivos basados en MTK, autodetección del tipo de procesador MTK. *Nota: La descarga de la memoria flash se aplica a un dispositivo apagado, por lo que no se requiere ni desbloqueo ni acceso root.*

- Adquisición de datos mediante captura de pantalla automatizada.

- Adquisición de dispositivos Qualcomm utilizando el modo EDL (para dispositivos Android). La lista de más de 250 dispositivos compatibles:
  - Asus Zenfone 4 Pro (Z01GD)
  - Asus ZenFone 4 ZE554KL
  - Asus Zenfone 5 ZE620KL
  - Asus Zenfone Max Pro M1
  - Asus Zenfone Max Pro M2
  - Asus ZenFone 4 ZE554KL
  - Asus ZenFone 5Z
  - Asus ROG Phone (2,96 GHz)
  - Asus ZenFone 3 Deluxe (5.7" 64GB) (ZS570KL)
  - Asus ZenFone 3 Deluxe (5.7" 256GB) (ZS570KL)
  - Asus Zenfone AR
  - Asus Zenfone Ares (2018)
  - Asus ZenFone 3 (5,2") (ZE520KL)
  - Asus ZenFone 3 (5,5") (ZE552KL)
  - Asus ZenFone 3 Deluxe (5,5") (ZS550KL)
  - Asus ZenFone 3 Zoom/ZenFone Zoom S (ZE553KL)
  - Asus Zenfone 4 Selfie Pro (ZD552KL)
  - Asus ZenFone 3 Láser
  - Asus ZenFone 3 Max ZC553KL
  - Asus Zenfone 2 Laser ZE500KL
  - Asus Zenfone Max ZC550KL

702 San Conrado Terrace,
Unit 1 Sunnyvale CA, Estados Unidos 94085
+1 (650) 272-0384 (EE.UU. y Canadá)correo electrónico:
sales@belkasoft.com

- Asus ZenFone 5 Lite
- Lenovo K9 Note
- Lenovo K5 Pro
- Lenovo S5 Pro
- Lenovo Z5
- Lenovo S5 Pro GT
- Lenovo Z5s
- Lenovo Z5 Pro
- Lenovo Z6 SE/Z6 Lite/Joven
- Lenovo Phab 2 Pro
- Lenovo K9 Plus
- Lenovo P2
- Lenovo S5
- Lenovo K6
- Lenovo K6 Note
- Lenovo K6 Power
- Lenovo A805e
- Lenovo Sisley S90
- Lenovo Vibe Z2
- Lenovo A6000
- Lenovo Vibe X3
- LG G4
- LG V10
- LG X mach/X rápido
- Meizu E3
- Meizu 15
- Meizu 16X
- Meizu X8
- Meizu 16
- Meizu 16 Plus
- Meizu Zero
- Meizu 15 Lite/Meizu M15
- Meizu M6 Note
- Meizu Note 8
- Motorola Moto Z3
- Motorola Moto X4
- Motorola Moto G6 Plus
- Motorola Moto G7 Plus
- Motorola Moto Z3 Play
- Motorola One Power/P30 Note
- Motorola P30
- Motorola Moto Z
- Motorola Moto Z Force
- Motorola Moto G5 Plus
- Motorola Moto G5S Plus
- Motorola Moto Z Play
- Motorola Moto Z2 Play
- Motorola One
- Motorola Moto G4
- Motorola Moto G4 Plus
- Motorola Moto G5
- Motorola Moto G6 Play
- Motorola Moto E5 Plus (India y China)
- Motorola Moto E5 Plus
- Motorola Moto E4 (EE.UU.)
- Motorola Moto E5 Play
- Motorola Moto G6 Play
- Motorola Moto Z2 Force
- Nokia 8
- Nokia 8 Sirocco
- Nokia 6.1
- Nokia 7
- Nokia 6.1 Plus/X6
- Nokia 7.1
- Nokia 6.2
- Nokia X71
- Nokia 7 Plus
- Nokia 7.2
- Nokia 9 PureView
- Nokia 5
- Nokia 6
- Nokia 2.1
- Nokia 8110 4G
- Nokia 2720 Flip
- Nokia 800 resistente
- Nokia 2
- Nokia X2
- Nokia X7/8.1/7.1 Plus
- OnePlus 5
- OnePlus 5T
- OnePlus 6
- OnePlus 6T
- OnePlus 6T Edición McLaren
- OPPO R11
- OPPO R11 Plus
- OPPO R11s
- OPPO R11s Plus
- OPPO R15 Pro
- OPPO R15 Sueño Espejo
- OPPO K1 (sólo 64 GB, 128 GB modelo es el R15x)
- OPPO R17 Neo/RX17 Neo
- OPPO F3 Plus
- OPPO R9 Plus
- OPPO R9s Plus
- OPPO R9s
- OPPO A57

702 San Conrado Terrace,
Unit 1 Sunnyvale CA, Estados Unidos 94085
+1 (650) 272-0384 (EE.UU. y Canadá)correo electrónico:
sales@belkasoft.com

- Samsung Galaxy S8 (EE.UU./Canadá/China/Hong Kong/Japón)
- Samsung Galaxy S8+ (EE.UU./Canadá/China/Hong Kong/Japón)
- Samsung Galaxy S8 Active (AT&T EE.UU.)
- Samsung Galaxy Note 8 (EE.UU./Canadá/China/Hong Kong/Japón)
- Samsung Galaxy Tab S4
- Samsung W2018
- Samsung Galaxy S7 (SM-G9300/A/P/T/U/V)
- Samsung Galaxy S7 Edge (SM-G9350/A/P/T/U/V)
- Samsung Galaxy S7 Active (SM-G891A)
- Samsung Galaxy Note 7 (SM-N9300)
- Samsung Galaxy Tab S3
- Samsung W2017
- Samsung Galaxy Note FE (SM-N9350)
- Sharp Aquos C10
- Sharp Aquos D10
- Sharp Aquos S2 64GB
- Sharp Aquos S3
- Sharp Aquos S3 Mini
- Sharp Aquos Sense Plus
- Sharp Aquos S2 128GB
- Sharp Aquos S3 128GB
- Sharp Aquos R Compact
- Vivo Z1i
- Vivo V9 6GB (España)
- Vivo V11 Pro
- Vivo X20
- Vivo X20 Plus
- Vivo X20 Plus UD
- Vivo X21
- Vivo X21 UD
- Vivo X21s
- Vivo Z1
- Vivo X23 Symphony
- Vivo Nex A
- Vivo Nex A UD
- Vivo X27 (256 GB)
- Vivo X27 Pro
- Vivo Z3 (6 GB RAM)
- Vivo Z5x
- Vivo Nex S
- Vivo iQOO Neo
- Vivo Xplay 5
- Vivo Xplay 5 Elite
- Vivo Xplay 6
- Vivo V3 Max
- Vivo X6s
- Vivo X6s Plus
- Vivo X7
- Vivo X7 Plus
- Vivo X9 Plus
- Vivo X9s
- Vivo X9s Plus
- Vivo V5 Plus
- Vivo V9
- Vivo X9
- Vivo Y79
- Vivo Y53
- Vivo Y66
- Vivo Y93
- Vivo Y95
- Vivo U1
- Vivo Y3
- Xiaomi Mi 6
- Xiaomi Mi MIX 2
- Xiaomi Redmi Note 5/Redmi Note 5 Pro
- Xiaomi Redmi Note 5 AI Doble Cámara
- Xiaomi Redmi Note 6 Pro
- Xiaomi Mi Max 3
- Xiaomi Mi Note 3
- Xiaomi Mi 8 Lite/Mi 8 Youth
- Xiaomi Mi A2/Mi 6X
- Xiaomi Mi Pad 4
- Xiaomi Mi Pad 4 Plus
- Xiaomi Redmi Note 7 España
- Xiaomi Redmi Note 7 Internacional/7S
- Xiaomi Mi CC9 (Mi 9 Lite)
- Xiaomi Mi CC9 Meitu Edition
- Xiaomi Mi 8 SE
- Xiaomi Mi MIX 2S
- Xiaomi Mi MIX 3
- Xiaomi Pocophone F1
- Xiaomi Mi 8
- Xiaomi Mi 8 Explorer Edition
- Xiaomi Mi 8 Pro/Mi 8 Pantalla Fingerprint Edition

702 San Conrado Terrace, Unit 1 Sunnyvale CA, Estados Unidos 94085
+1 (650) 272-0384 (EE.UU. y Canadá)correo electrónico: sales@belkasoft.com

- Xiaomi Black Shark
- Xiaomi Black Shark Helo
- Xiaomi Mi 5 32GB
- Xiaomi Mi 5s Plus
- Xiaomi Mi Note 2
- Xiaomi Mi MIX
- Xiaomi Mi 5 64GB/128GB
- Xiaomi Mi 5s
- Xiaomi Mi Note Pro
- Xiaomi Mi 4c
- Xiaomi Mi 4s
- Xiaomi Mi Max (16GB/32GB)
- Xiaomi Mi Max (64GB/128GB)
- Xiaomi Mi 5X/Mi A1
- Xiaomi Mi A2 Lite/Redmi 6 Pro
- Xiaomi Mi Max 2
- Xiaomi Redmi 4 Prime
- Xiaomi Redmi 5 Plus/Redmi Note 5
- Xiaomi Redmi Note 4
- Xiaomi Redmi Note 4X (32GB)
- Xiaomi Redmi S2/Redmi Y2
- Xiaomi Redmi 4 (India)
- Xiaomi Redmi Y1 (India)
- Xiaomi Redmi 4X
- Xiaomi Redmi Note 5A Pro
- Xiaomi Redmi 3S
- Xiaomi Redmi 4 (China)
- Xiaomi Redmi 4A
- Xiaomi Redmi 5A
- Xiaomi Redmi Note 5A
- Xiaomi Redmi Y1 Lite
- Xiaomi Redmi Go
- ZTE Nubia Z17
- ZTE Nubia Z17S
- ZTE Nubia Red Magi
- ZTE Axon 7s
- ZTE Axon M
- ZTE Axon 7
- ZTE Nubia Z11
- ZTE Axon & Axon Pro & Axon Lux & Axon Elite
- ZTE Nubia Z9 Max y Max Elite
- ZTE Nubia Z9
- ZTE Nubia Z9 Elite
- ZTE Nubia Z9 Exclusivo
- ZTE Nubia Z11 Max
- ZTE Nubia Z17 mini
- ZTE Axon 7 MAX
- ZTE Axon Max 2
- ZTE Blade Max 3
- ZTE Blade V8 Pro
- ZTE Nubia M2
- ZTE Nubia N3
- ZTE Nubia V18
- ZTE Nubia Z11s mini
- ZTE Zmax Pro

- Adquisición de APK downgrade. Lista de aplicaciones compatibles:
  - Badoo
  - Delfín
  - Evernote
  - Facebook
  - Facebook Messenger
  - Navegador Firefox
  - Hangouts
  - Instagram
  - ICQ
  - Kakao Talk
  - Kate Móvil
  - Kate Móvil Lite
  - Likee
  - Línea
  - Odnoklassniki
  - Onedrive
  - Ópera
  - Opera beta
  - Pinterest
  - Navegador Puffin
  - QQ
  - SHAREit
  - Señal
  - Sina Weibo
  - Skype
  - TamTam
  - Telegrama
  - Tik Tok
  - Tumblr
  - Twitter
  - A través del navegador
  - Viber
  - VKontakte
  - Voxer

702 San Conrado Terrace, Unit 1 Sunnyvale CA, Estados Unidos 94085
+1 (650) 272-0384 (EE.UU. y Canadá)correo electrónico: sales@belkasoft.com

  - WeChat
  - WhatsApp
  - Wickr Me
  - Navegador Yandex
  - Correo Yandex
  - Zello
  - Zoom
- Sólo se muestran las aplicaciones instaladas en un dispositivo concreto. Solo se adquieren las aplicaciones seleccionadas.
- Las copias de seguridad de los archivos .apk se guardan en la carpeta case.
- La adquisición de la tarjeta SD de Android es compatible con el método de downgrade APK.
- El APK downgrade está disponible para las aplicaciones que utilizan la función Dual Messenger en los dispositivos Samsung

- **Adquisición de MTK basada en agentes**
  - Acer Iconia One 10 serie B3-A30/B3- A40/B3-A50
  - Acer Iconia One 8 serie B1-860
  - Acer Iconia Talk S
  - Serie de tabletas Alba
  - Alcatel serie 1 5033
  - Alcatel 1C
  - Alcatel 3L (2018) serie 5034
  - Alcatel 3T 8
  - Alcatel A5 LED serie 5085
  - Alcatel serie A30 5049
  - Alcatel Idol 5
  - Alcatel/TCL A1 A501DL
  - Alcatel/TCL LX A502DL
  - Alcatel Tetra 5041C
  - Alcatel U5 / Orange Rise 52
  - Alldocube iPlay10 Pro
  - Alldocube iPlay8
  - Amazon Fire 7 2019 hasta Fire OS 6.3.1.2 build 0002517050244 sólo
  - Amazon Fire HD 8 2016 hasta Fire OS 5.3.6.4 build 626533320
  - Amazon Fire HD 8 2017 hasta Fire OS 5.6.4.0 build 636558520 sólo
  - Amazon Fire HD 8 2018-sólo hasta Fire OS 6.3.0.1
  - Amazon Fire HD 10 2017 hasta Fire OS 5.6.4.0 build 636558520 sólo
  - Amazon Fire HD 10 2019 solo hasta Fire OS 7.3.1.0
  - Amazon Fire TV 2-sólo hasta Fire OS 5.2.6.9
  - ANRY S20
  - ASUS ZenFone 3 Max ZC520TL
  - ASUS ZenFone Max Plus X018D
  - ASUS ZenPad 3s 10 Z500M
  - ASUS ZenPad Z3xxM(F) Serie basada en MT8163
  - Barnes & Noble NOOK Tablet 7" BNTV450 & BNTV460
  - Barnes & Noble NOOK Tablet 10.1" BNTV650
  - Blackview A8 Max
  - Blackview BV9600 Pro (Helio P60)
  - BLU Life Max
  - BLU Life One X
  - Serie BLU R1
  - BLU R2 LTE
  - BLU S1
  - BLU Tank Xtreme Pro
  - BLU Vivo 8L
  - BLU Vivo XI
  - BLU Vivo XL4
  - Bluboo S8
  - BQ Aquaris M4.5
  - BQ Aquaris M8
  - CAT S41
  - Coolpad Cool Play 8 Lite
  - Coolpad Legacy S(R)
  - Cubot Power
  - Dragon Touch K10
  - Sensación de eco

702 San Conrado Terrace,
Unit 1 Sunnyvale CA, Estados Unidos 94085
+1 (650) 272-0384 (EE.UU. y Canadá)correo electrónico:
sales@belkasoft.com

- Evercoss Genpro X Pro S50
- Gionee F103 Pro
- Gionee M7
- Gionee S9
- HiSense Infinity H12 Lite
- HTC Desire 12
- HomTom HT20
- Serie GR3 de Huawei
- Huawei Y5II
- Huawei Y6II MT6735 serie
- ION Gravedad
- Lava Iris 88S
- Lenovo A5
- Lenovo serie C2
- Lenovo Tab E7
- Lenovo Tab E8
- Lenovo Tab2 A10-70F
- Lenovo Tab3 10
- Lenovo Vibe K5 Note
- LG K8+ (2018) X210ULMA (MTK)
- LG Serie K10-K430
- LG K10 (2017)
- LG K50
- LG Q7 (MTK)
- LG Stylo 4 (MTK)-hasta Q710AL11k
- LG Tribute Dynasty
- LG X power serie 2/M320 (MTK)
- LG Xpression Plus 2/Harmony 3/K40 Serie LMX420
- Lumigon T3
- Meizu M5c
- Meizu M6
- Meizu Pro 7 Plus
- Motorola Moto serie C
- Motorola Moto E3 series (MTK)
- Motorola Moto serie E4 (MTK)
- Nokia 1
- Nokia 1 Plus
- Nokia 3
- Nokia 3.1
- Nokia 3.1 Plus
- Nokia 5.1
- Nokia 5.1 Plus/X5
- Odys PACE 10 (MT8163)
- Onn 7" Android tablet
- Serie de tabletas Onn de 8" y 10" (MT8163)-hasta 10/2019 FW
  sólo
- Oppo serie A59
- Oppo A5s-sólo hasta A.30
- Oppo A7x-hasta Android 8.x
- Oppo serie F5/A73-hasta A.39
- Oppo serie F7-Sólo Android 8.x
- Oppo serie F9-Sólo Android 8.x
- Oppo serie R9xm
- Oukitel K6
- Oukitel K9
- Oukitel K12
- Oukitel U18
- Philips E518
- Protruly D7
- RCA Voyager III-RCT6973W43MDN
- Realme 1
- Realme 3
- Snopow serie M10
- Sony Xperia C4
- Sony Xperia serie C5
- Sony Xperia L1
- Sony Xperia L3
- Sony Xperia serie M5
- Sony Xperia serie XA
- Serie Sony Xperia XA1
- Southern Telecom Smartab ST1009X (MT8167)
- Teclast M30
- TECNO Spark serie 3
- UFmidigi serie F1
- Umidigi Power
- Verizon Ellipsis 10 HD QTAXIA1
- Vernee Mix 2
- Wiko Ride
- Wiko Sunny
- Wiko View3
- Xiaomi Redmi serie 6/6A
- ZTE Blade 10 Prime
- ZTE Blade A530

702 San Conrado Terrace,
Unit 1 Sunnyvale CA, Estados Unidos 94085
+1 (650) 272-0384 (EE.UU. y Canadá)correo electrónico:
sales@belkasoft.com

- ZTE Blade A7 Prime
- ZTE Blade D6/V6
- ZTE Blade V8 Lite
- ZTE Quest 5 Z3351S
- ZTE Voyage 4S/Blade A611

Adquisición de Spreadtrum. La lista de los 88 dispositivos Android compatibles:

- Alcatel 1C 5003D
- Alcatel 1S 5024D
- Archos 40D Titanio
- Archos 55 Platino
- Prestación ARK Nota 1
- ARK Beneficio S402
- ARK Beneficio S453
- Asistente AS-5411
- BLU G5
- BLU G60
- BQ 5528L Strike Adelante
- BQ 5731L Magic S
- BQ 6040L Magia
- BQ 6042L Magia E
- Coolpad Mega 5A
- DEXP Ixion E140 Huelga
- DEXP Ixion E150 Alma
- DEXP Ixion E250 Alma
- DEXP Ixion E345 Jet
- DEXP Ixion E350 Alma 3
- DEXP Ursus TS370
- Digma Citi Z520
- Digma Hit Q400
- Digma Linx A400
- Digma Linx A401
- Digma Linx A420
- Digma Linx A450
- Digma LINX Rage 4G
- Digma LINX Trix 4G
- Plano Digma 7574s
- Digma Vox A10
- Digma VOX E502 4G
- Digma Vox G450
- Digma Vox S507
- FinePower C2
- FinePower C5
- Fly FS528 Memoria Plus
- Fly FS551 Nimbus4
- Fly IQ436i Era Nano 9
- Fly IQ4490i Era Nano 10
- Gigaset GS80
- Ginzzu S4020
- Gionee Max
- GoClever Max
- HTC Desire 326G DualSim
- INOI 7
- Intex 7
- Intex Elyt Dual
- Intex Indie 6
- Intex Staari 11
- Irbis SP05
- Irbis SP06
- Itel P36 Pro
- Itel Visión 1
- Itel Vision 1 Plus
- Jinga A400
- Leagoo Z5c
- Lenovo A1000
- Lenovo A2800D
- Lenovo A398T+
- Micromax Q301
- Micromax Q326
- Micromax Q346
- Micromax Q346 Lite
- Micromax Q379
- Micromax Q385
- Micromax Q465
- Nobby X800
- Philips S260
- Philips S307
- Prestigio Muze V3 LTE
- Prestigio Wize NV3 3537Duo
- TeXet TM-4003
- TeXet TM-5073
- TeXet TM-5075
- TeXet TM-5076
- TeXet TM-5077
- TeXet X-line TM-5006

702 San Conrado Terrace,
Unit 1 Sunnyvale CA, Estados Unidos 94085
+1 (650) 272-0384 (EE.UU. y Canadá)correo electrónico:
sales@belkasoft.com

- TeXet X-quad TM-4503
- Vértice Impress Lobo
- Wiko Sunny 2
- Wiko Sunny 3
- Wiko Sunny 4
- ZTE Blade A3 2019
- ZTE Blade A3 2020
- ZTE Blade A5
- ZTE Blade AF3
- ZTE Blade GF3

- **Adquisición de varios servicios de correo web y en la nube.**

  La lista de nubes soportadas cambia constantemente debido a la naturaleza de este tipo de datos, en el momento de escribir esta referencia las soportadas son:

  - Huawei
  - Google Drive
  - Cronología de Google
  - Google Keep
  - Sincronización de Google
  - Google MiActividad
  - Gmail
  - iCloud
  - Copias de seguridad de iCloud
  - Llavero de iCloud
  - Instagram
  - Mega nube
  - Microsoft Office 365
  - Telegrama
  - VK
  - WhatsApp
  - WhatsApp con código QR

  - Se admiten los siguientes servicios de Historial de Google:

    - Android
    - Cromo
    - Búsqueda en la nube
    - Soñar despierto
    - Espacio de ocio
    - Gmail
    - Google Analytics
    - Google Apps
    - Google Arte y Cultura
    - Nube de Google
    - Desarrolladores de Google
    - Google Home
    - Consola de Google Play
    - Juegos de Google Play
    - Google Play Libros
    - Google Play Market
    - Google Play Música
    - Google Play Películas
    - Tienda Google
    - Asistente de Google
    - Google Drive
    - Calendario de Google
    - Google My Business
    - Noticias de Google
    - Google Lens
    - Traductor de Google
    - Google+
    - Guías
    - Bandeja de entrada
    - Socrático
    - Mercado Wing
    - YouTube
    - Búsqueda de audio
    - Control por voz
    - Mapas
    - Libros
    - Noticias
    - Buscar
    - Búsqueda de vídeos
    - Búsqueda de imágenes
    - Compras
    - Viajes
    - Publicidad
    - Recomendaciones
    - Ayuda
    - Finanzas

702 San Conrado Terrace,
Unit 1 Sunnyvale CA, Estados Unidos 94085
+1 (650) 272-0384 (EE.UU. y Canadá)correo electrónico:
sales@belkasoft.com

Se puede recuperar la siguiente información sobre la actividad de los usuarios:

- Página visitada
- Búsqueda realizada
- Imagen vista
- Vídeo visto
- Video gustado

Se admiten los siguientes servicios de webmail en la nube:

- 21cn
- Alibaba
- aol.com
- Comcast
- email.ua
- Correo rápido
- Gratis.fr
- Gmx
- GNU
- Hotmail
- Hushmail.com
- Bandeja de entrada.com
- KolabNow
- Mac.com
- Mail.ru
- online.ua
- Ópera
- Pochta.ru
- Qip
- QQ
- Rambler
- Runbox
- Sohu.com
- Vip Sohu
- Yahoo
- Yandex
- Ziggo.es

La autorización de dos factores es compatible con la adquisición de Google Cloud, iCloud, Instagram y Microsoft Office 365.

  - La autorización de cuentas a través de un emulador de navegador también es compatible con Google Clouds.
  - 2FA a través de Authenticator también es compatible con Instagram.

- **Adquisición basada en Checkm8**

Este tipo de adquisición le permite a uno realizar la extracción sin jailbreak de dispositivos iOS seleccionados a través de exploit unpachable. Los dispositivos compatibles incluyen la gama de dispositivos iPhone y iPad equipados con SoC A7 a A11 de Apple (iPhone 5s a iPhone X). Las versiones de iOS compatibles son de la 12.0 a la 15.5.
Esta extracción está disponible para todos los dispositivos de la gama soportada independientemente de su estado de bloqueo. En caso de dispositivos bloqueados se extraen los datos disponibles en modo BFU.

La extracción de llaveros está soportada, los llaveros pueden ser extraídos vía adquisición basada en checkm8 y desde cualquier iPhone con jailbreak. Basándose en la información extraída, varias tareas de descifrado son posibles (por ejemplo, iOS Signal messenger descifrado).

La funcionalidad está disponible en Windows 10.

Tipos de extracción admitidos

702 San Conrado Terrace,
Unit 1 Sunnyvale CA, Estados Unidos 94085
+1 (650) 272-0384 (EE.UU. y Canadá)correo electrónico:
sales@belkasoft.com

Belkasoft X extrae y recupera artefactos utilizando varios métodos:

- Análisis de los expedientes existentes
- Carving (análisis basado en firmas) de datos eliminados u ocultos, incluido el espacio no asignado o libre de un disco duro o una imagen.
- Extracción de volcados de memoria RAM. El análisis de memoria viva (RAM volátil) permite extraer restos de redes sociales (por ejemplo, Facebook, Twitter), correos electrónicos basados en la web (por ejemplo, Gmail, Hotmail), datos de aplicaciones en la nube (por ejemplo, Dropbox, Flickr), etc.
    - Se admite la integración de la volatilidad.
- Análisis de la papelera de reciclaje
- Tallado de archivos de hibernación y de páginas
- Análisis de instantáneas de Volume Shadow Copy (VSC)
    - Se admite la deduplicación NTFS VSC
- Análisis de archivos de máquinas virtuales sin encenderlas
- Triaje (extracción de perfiles sin análisis de su contenido)
- Compatible con descifrado WDE y FVE integrado:
    - APFS
    - Bitlocker
    - DriveCrypt
    - Bóveda de archivos
    - Seguridad para puntos finales de McAfee
    - PGP y Symantec PGP
    - TrueCrypt
    - VeraCrypt
- Descifrado LUKS con una contraseña conocida

Fuentes de datos compatibles

- **Imágenes de disco (incluidas imágenes de varias partes e imágenes comprimidas):**
    - AccessData Archivo de imagen (*.AD1)
    - Formato de archivo forense avanzado (*.AFF4)
    - Formatos forenses avanzados (*.Afd, *.Aff, *.Afm)
    - Volúmenes APFS T2 adquiridos por MacQuisition
    - Archivos comprimidos (*.7z, *.Cpio, *.Cpio.gz, *.Jz001, *.Tar, *.Tar.gz, *.Tgz, *.Zip, *.Zip001)
    - Archivo de imagen Atola (*.Img)
    - Archivo de información de arranque (*.Bif)
    - Archivo de imagen DD (*.000, *.0000, *.0001, *.001, *.DD)
    - Formato de archivo de disco (*.DAR)
    - Archivo de imagen DMG (*.DMG)
    - Encase Archivo de imagen (*.E01, *.Ex01)
    - Archivo de imagen de disquete (*.Flp, *.Ima, *.Vfd)
    - Archivo de pruebas lógicas (*.L01, *.Lx01)
    - Archivo de imagen sin procesar (*.Raw)
    - Archivo de imagen inteligente (*.S01)
    - Archivo de imagen X-Ways (*.Ctr)
    - Archivo de imagen Belkasoft

- **Imágenes móviles**
    - Copias de seguridad iTunes de iPhones/iPADs
    - Copias de seguridad ADB de Android
    - Volcados físicos de Android

702 San Conrado Terrace,
Unit 1 Sunnyvale CA, Estados Unidos 94085
+1 (650) 272-0384 (EE.UU. y Canadá)correo electrónico:
sales@belkasoft.com

- Xiaomi MIUI copias de seguridad
- Copias de seguridad de Huawei HiSuite
- Imágenes OFB
- Imágenes UFED y UFDR de Androids y iPhones/iPADs
- Imágenes de GrayKey iOS
- Elcomsoft iOS imágenes
- Copias de seguridad de Blackberry IPD y BBB
- Imágenes TWRP
- Copia de seguridad cifrada del iPhone adquirida con UFED Physical Analyzer

- **Imágenes de drones**
  - ArduPilot DIY Drone
  - DJI Agras MF-1S
  - DJI Matrice
  - DJI Mavic
  - DJI Phantom 3
  - DJI Phantom 4
  - DJI Spark
  - Loro Anafi
  - Qysea Fifish P3
  - Ryze Tello
  - Sense Fly
  - Víbora del cielo
  - Yuneec H520
  - Yuneec Typhoon Q500
  - Y modelos de drones compatibles

- **Máquinas virtuales**
  - VMWare
  - Virtual PC/Hyper-V
  - VirtualBox
  - XenServer

- **Discos duros y extraíbles**
  - Físico o lógico conectado a una máquina con Belkasoft X en ejecución
  - Unidades de red
  - Unidades dentro de dispositivos bloqueadores de escritura

- **Volcados de RAM en directo de dispositivos con Windows, Linux y Android**
  - Archivos de hibernación (hiberfil.sys)
  - Imágenes Mdd RAM (.mddramimage)
  - Imágenes de RAM (.mem), creadas con Belkasoft Live RAM Capturer o cualquier otra herramienta de terceros.
  - Archivos de intercambio (pagefile.sys)
  - Archivos de intercambio de la máquina virtual (.vmem)

- **Carpeta**

702 San Conrado Terrace,
Unit 1 Sunnyvale CA, Estados
Unidos 94085
+1 (650) 272-0384 (EE.UU. y
Canadá)correo electrónico:
sales@belkasoft.com

Puede especificar cualquier carpeta para analizar. Las subcarpetas se analizarán automáticamente.

- **Nube**
  Puede adquirir y analizar una nube compatible con Belkasoft X

- **Fuentes de datos en la nube Amazon S3**
  Varios investigadores pueden analizar la misma fuente de datos al mismo tiempo con las mismas o diferentes opciones de análisis. Se admiten imágenes de una o varias partes.

  - **Imágenes de coches Berla**

Se admite el análisis automático de fuentes de datos anidadas (como archivos de máquinas virtuales, archivos comprimidos, copias de seguridad móviles, etc.).

Tipos de datos admitidos

Belkasoft X está diseñado para recopilar tantos tipos de pruebas como sea posible de una forma sólida desde el punto de vista forense. Los tipos de pruebas compatibles incluyen documentos de oficina, buzones de clientes de correo electrónico, aplicaciones de dispositivos móviles e historial de uso, archivos de sistema y de registro, archivos de imagen y vídeo, bases de datos SQLite, comunicaciones de redes sociales, historiales de mensajería instantánea, sesiones de navegación por Internet, correo web, datos de aplicaciones P2P, aplicaciones en la nube, chats de MMORPG, archivos cifrados, etc.
Se incluyen los siguientes tipos de datos:

- **Archivos de audio**
  - Formatos compatibles: TTA, VOX, WAV, WEBM, WMA, 3GP, 8SVX, AA, AAC, AAX, ACT, AIFC, AIFF, AMR, APE, AU, AWB, CDA, DCT, DSS, DVF, FLAC, GSM, IKLAX, IVS, M4A, M4B, M4P, MID, MIDI, MMF, MOGG, MP3, MPC, MSV, OGA, OGG, OPUS, QCP, RA, RAW, RM, RMI

- **Navegadores**
  (las aplicaciones de la siguiente lista sin SO especificado son aplicaciones de Windows)
  - Adobe Flash
  - Avant
  - Navegador Baidu
  - Chrome (Windows, macOS)
  - Borde
  - Firefox (Windows, macOS)
  - Internet Explorer
  - Maxthon 5
  - Ópera
  - Puffin
  - Qihoo 360
  - Navegador QQ (Windows, macOS)
  - Safari (Windows, macOS)
  - Explorador de Sogou
  - Tor
  - Yandex

702 San Conrado Terrace,
Unit 1 Sunnyvale CA, Estados Unidos 94085
+1 (650) 272-0384 (EE.UU. y Canadá)correo electrónico:
sales@belkasoft.com

- **Aplicaciones en la nube**
  Varias nubes populares
  se admiten aplicaciones como:
  - Dropbox (con descifrado)
  - Google Drive
  - Una unidad
  - Yandex.Disk
  - Flickr

  Las aplicaciones que no tienen un cliente instalable se analizan en busca de artefactos de RAM.

- **Correo electrónico**
  Análisis de archivos de bases de datos de programas clientes de correo electrónico:
  - Correo de Apple (EML/EMLX)
  - GMail fuera de línea
  - Letras sueltas en formato MIME, Mbox, MSG
  - Correo 163
  - Mozilla Thunderbird
  - Outlook (a partir de la versión 2003)
  - Outlook Express
  - ¡El murciélago!
  - Windows Live Mail

  Detección de mensajes de correo electrónico en volcados de memoria RAM:
  - GMail
  - Hotmail
  - MIME
  - Correo Yahoo

- **Mensajería instantánea** ("chats")
  (las aplicaciones de la siguiente lista sin SO especificado son aplicaciones de Windows)
  - &RQ
  - Adium (macOS)
  - AIM (Win, macOS)
  - AIM Express
  - aMSN (Linux, macOS)
  - Brosix (Win, macOS)
  - ChatZilla
  - Contactos (macOS)
  - Digbsy
  - E-buddy
  - Cliente eM
  - Emesene (Win, Linux)
  - Empatía (Linux)
  - Facebook Desktop (Win, macOS)
  - Aplicación Facebook Messenger (Win, macOS)
  - Fuego (macOS)
  - Gadu-Gadu (antiguo)
  - Gadu-Gadu 10
  - Gajim
  - Gigatriba
  - Google Hola
  - Google Talk
  - GTalk
  - Hotmail
  - iChat (macOS)
  - ICQ 99b
  - ICQ 2000a
  - ICQ 2000b
  - ICQ 2003b
  - ICQ 4 - ICQ 5
  - ICQ 6 Lite
  - ICQ 6.5
  - ICQ 7
  - ICQ 7.5+

702 San Conrado Terrace, Unit 1 Sunnyvale CA, Estados Unidos 94085
+1 (650) 272-0384 (EE.UU. y Canadá)correo electrónico: sales@belkasoft.com

- ICQ 8.2
- ICQ (Linux)
- ICQ (macOS)
- Icq2Go
- Imo
- InstantBird (Win, macOS)
- Ircle (macOS)
- JClaim (macOS)
- Jitsi (Win, macOS)
- Kadu (macOS)
- KMess (Linux)
- Kopete (Linux)
- Línea
- Agente de Mail.Ru
- Agente de Mail.Ru para Win8
- Agente de Mail.Ru (macOS)
- Meebo
- Mercury (Linux, macOS)
- Mensajes (macOS)
- Messenger Plus
- Miranda IM
- miRC
- MSN / Live Messenger
- MI de MySpace
- Nate ON
- Nimbuzz (Win, macOS)
- Notas (macOS)
- ooVoo
- Paltalk
- Pidgin
- Pidgin (Linux)
- Psi (Win, Linux)
- Qip 2005
- Qip Infium / 2010
- qutIM
- SIM
- Skype (Win, Linux, macOS)
- Skype para Win 10
- Slack
- Snak (macOS)
- Visor de equipos
- Chat de visor de equipo
- Telegram (Win, macOS)
- Trillian (Win, macOS)
- Viber
- Viber para Windows 8
- Vipole
- Virtus
- Wickr Me (Win, Linux)
- X-Chat Acqua (macOS)
- Ya-Online
- Yahoo! Messenger (Win, macOS)
- Zello

- **Criptomonedas**
  - Cartera Bitcoin Armory
  - Billetera Bitcoin Core
  - Jaxx

- **Archivos y volúmenes cifrados** (detección)
  Se pueden detectar más de 300 tipos de cifrado, como Bitlocker, documentos cifrados de Microsoft Office, archivos (RAR, 7z, gz, etc.), copias de seguridad cifradas de iTunes, etc.

- **Formatos de archivo especiales**
  - Contenedores OLE
  - yEnc

- **Datos de geolocalización**
  Belkasoft X extraerá la geolocalización de imágenes geohabilitadas (que tengan etiquetas GPS en los metadatos EXIF), archivos de vídeo geoetiquetados, búsquedas en el navegador de Google Maps, mapas de Windows 10, aplicaciones de taxi y apps de fitness.
  También admite la extracción de geolocalización de iPhone GeoFences, iOS Frequent locations y Facebook check-ins.

702 San Conrado Terrace,
Unit 1 Sunnyvale CA, Estados
Unidos 94085
+1 (650) 272-0384 (EE.UU. y
Canadá)correo electrónico:
sales@belkasoft.com

- **MMORPG (juegos en línea)**
  Se pueden extraer datos de los volcados de memoria RAM.
  - Karos
  - Linaje
  - World of Warcraft

- Documentos de oficina
  - **Microsoft Office**: DOC, DOCX, XLS, XLSX, PPT, PPTX
  - **OpenOffice**: ODT, ODS, ODP
  - **Oficina Hangul**: HWP
  - **macOS:** Keynote, Numbers, Pages
  - PDF
  - RTF
  - Y otros formatos de documentos

  Para todos estos archivos se extrae e indexa tanto el texto plano como los metadatos. Los archivos incrustados se pueden extraer y mostrar. La vista previa de documentos se muestra para archivos PDF, Microsoft Word, Microsoft Excel y Microsoft PowerPoint.

- **P2P (aplicaciones entre iguales)**
  - Galaxia Ares
  - eMule
  - Frostwire
  - Gigatriba
  - Limewire
  - Shareaza
  - Torrente
  - ShareIT

- **Fotos**
  - Se admiten más de 170 formatos de imagen, incluidos muchos formatos de cámara RAW:

    32, 3FR, AI, AIF, AIFC, AIFF, ANI, ANIM, APNG, ART, ARW, ASF, AU, BAY, BEF, BMF, BMP, BMQ, BSAVE, BW, CAL, CAP, CDR, CGM, CH3, CIFF, CIN, CINE, CLP, CMX, CNV, CPC, CR2, CRW, CS1, CUR, CUT, CVX, DC2, DCR, DDS, DIB, DNG, DPX, DRF, DSC, DSF, DWG, DXF, ECW, EMF, ERF, EVA, EXIF, EXR, FAX, FFF, FITS, FLIC, FMV, FPX, G3, GEM, GIF, HDR, HEIC, IA, ICL, ICN, ICNS, ICO, ICS, IFF, IGES, IGS, IIQ, IIBM, IMG, INT, INTA, J2C, J2K, JBIG, JBIG2, JFIF, JIF, JNG, JP2, JPC, JPE, JPEG, JPG, JPK, JPX, K25, KC2, KDC, KOA, LBM, M1V, MAC, MDC, MEF, MET, MID, MIFF, MNG, MOS, MRV, MSP, NEF, NRW, ORF, PBM, PCD, PCT, PCX, PDD, PEF, PFM, PGF, PGL, PGM, PGML, PIC, PICT, PIF, PIX, PLE, PNG, PNM, PPM, PRS, PSD, PSP, PTX, PXN, QTK, RAD, RAF, RAS, RAW, RDC, RGB, RGBE, RLE, RMI, RND, RPBM, RPGM, RPPM, RSB, RW2, RWZ, SDW, SGI, SND, SR2, SRF, STI, SVG, TGA, THM, TIF, TIFF, VML, WBM, WBMP, WEBP, WMF, WPG, X3F, XAR, XBM, XCF, XIF, XMP, XPM, XWD

702 San Conrado Terrace,
Unit 1 Sunnyvale CA, Estados Unidos 94085
+1 (650) 272-0384 (EE.UU. y Canadá)correo electrónico:
sales@belkasoft.com

- Extracción de propiedades adicionales de archivos gráficos (metadatos EXIF, para formatos que admitan dichas propiedades), filtrado por propiedades EXIF, visualización de fotos con coordenadas GPS en Open Street Maps y Google Earth;
- Recupera archivos de los siguientes formatos gráficos mediante la búsqueda de firmas ("tallado") GIF, JPEG / JPG, PNG, BMP, WMF
- Las imágenes podían analizarse para detectar el tono de la piel, los rostros y el texto escaneado (OCR). Detección de pornografía, armas y estupefacientes mediante redes neuronales artificiales (RNA).
  - Se admite la agrupación de caras (agrupación de caras similares en imágenes fijas y fotogramas clave de vídeo)

- **Comunicaciones en redes sociales**
  Utilizando el análisis de volcado de RAM, Belkasoft X analiza:
  - Bebo
  - Facebook
  - Facebook Messenger
  - Google Plus
  - MySpace
  - OK (Odnoklassniki)
  - Orkut
  - Twitter
  - VK (Vkontakte)

- **Archivos de sistema**
  Búsqueda de archivos del sistema, y también restauración de dichos archivos mediante búsqueda de firmas ("carving") como:
  - Para Windows:
    - Registro de Windows
    - Archivos de salto (Jumplist)
    - Archivos LNK
    - Precargar archivos
    - Conexiones TeamViewer
    - Registros de eventos del sistema
    - Notificaciones de Windows
    - Cronología de Windows 10
    - Suscripción a eventos WMI
    - Conexiones Wi-Fi
  - Para macOS
    - Configuración Bluetooth
    - Información del dispositivo
    - Aplicaciones instaladas
    - ejecución automática de macOS
    - notificaciones de macOS
    - macOS Time Machine
    - Configuraciones del sistema
    - Registros de eventos del sistema
    - Usuarios

702 San Conrado Terrace,
Unit 1 Sunnyvale CA, Estados
Unidos 94085
+1 (650) 272-0384 (EE.UU. y
Canadá)correo electrónico:
sales@belkasoft.com

- Conexiones Wi-Fi

- Para Linux
  - Historia de Bash
  - Información del dispositivo
  - Paquetes instalados
  - Tareas programadas
  - Configuraciones del sistema
  - Usuarios

La compatibilidad nativa con archivos de registro de Windows permite recuperar registros muy dañados y parcialmente sobrescritos.
El visor de registros integrado ayuda a visualizar los registros de Windows sin necesidad de aplicaciones de terceros.

Extracción de datos importantes de los archivos de registro, como:
- Usuarios del SO (nombre, último inicio de sesión, último inicio de sesión fallido, hora de cambio de contraseña, RID de usuario, LM-hash, NT-hash)
- AutoRun (USB, CD, DVD)
- Nombre del ordenador
- Ubicación del registro del sistema
- Lista de dispositivos USB que se han conectado alguna vez al sistema
- Lista de dispositivos conectados
- Los últimos archivos abiertos por diferentes aplicaciones de Microsoft Office y Adobe Acrobat
- Tarjetas de red
- Fechas de instalación del SO
- Versión del sistema operativo
- Precargar archivos
- Programas que se ejecutan al iniciar sesión (Inicio del programa)
- Hora en que se apagó el ordenador por última vez
- Huso horario
- Datos de UserAssists
- Perfiles de redes inalámbricas

- **Vídeos**
  - Se pueden encontrar más de 30 tipos de vídeos:
    3GP, 3G2, ASF, AVC, AVI, DIVX, DRC, F4A, F4B, F4P, F4V, FLV, IFO, M2V, M4P, M4V, MK3D, MKA, MKS, MP2, MP4, MKV, MOV, MPE, MPEG, MPG, MPV, NSV, OGG, OGV, QT, RM, RMV8, SVI, TS, VOB, WEBM, WMV, MOD, MTS
  - La extracción de fotogramas clave es compatible con vídeos en los siguientes formatos: 3GP, 3G2, AVI, AVC, MP4, MPEG, MPG, WMV, MOV, MKV. Es necesario instalar un códec adecuado en la misma máquina.
  - Detección del número de secuencias de vídeo, extracción de fotogramas clave de secuencias de vídeo secundarias. Posibilidad de seleccionar el flujo de vídeo que se reproducirá en el reproductor multimedia.

Belkasoft
forensics made easier

702 San Conrado Terrace,
Unit 1 Sunnyvale CA, Estados
Unidos 94085
+1 (650) 272-0384 (EE.UU. y
Canadá)correo electrónico:
sales@belkasoft.com

Android

- **Aplicaciones estándar**
  - Calendario
  - Llamadas
  - Contactos
  - Aplicaciones instaladas
  - SMS, MMS

- **Correos**
  - Aplicación de correo predeterminada
  - Gmail
  - buzón.lv
  - bandeja de entrada.lt
  - bandeja de entrada.ee
  - CorreoRu Mail
  - Correo Yahoo
  - Correo Yandex
  - Correo de voz

- **Servicios en la nube**
  - Dropbox
  - Google Drive
  - OneDrive

- **Navegadores**
  - Explorador 360 Extreme
  - Aplicación Android web-data
  - Baidu
  - Cromo
  - Navegador por defecto
  - Delfín
  - Descargas
  - Borde
  - Firefox
  - Maxthon
  - Mercurio
  - Ópera
  - Puffin
  - Navegador Samsung
  - Navegador UC

- **Mensajeros**
  - AIM
  - Badoo
  - BBM
  - Brosix
  - Chaatz
  - ChatON
  - CommFort
  - Draugiem.lv
  - eBuddy XMS
  - Facebook Messenger
  - FireChat
  - Fring
  - Espacio de trabajo de Google
  - Google+
  - Grindr
  - Growlr
  - Hangouts
  - HeyTell
  - Caliente o no
  - ICQ
  - Agente ICQ \ Mail.Ru
  - Im+
  - OMI
  - Instagram Directo
  - KakaoTalk
  - KateMóvil
  - Kik
  - Línea
  - Agente de Mail.ru
  - MeetMe
  - MEGAChat
  - Chat Miau
  - SiguientePlus
  - Odnoklassniki
  - ooVoo
  - Paltalk
  - Señal
  - Skout
  - Skype
  - Slack
  - Snapchat
  - StarChat
  - TamTam
  - Tango
  - Telegrama
  - Telegrama X

702 San Conrado Terrace,
Unit 1 Sunnyvale CA, Estados Unidos 94085
+1 (650) 272-0384 (EE.UU. y Canadá)correo electrónico:
sales@belkasoft.com

- Texto Plus
- Textie
- TextMe
- TikTok
- Toque
- Tox
- Tumblr
- Twitter
- Viber
- Vipole
- Café VK
- Vkontakte
- Voxer
- Wamba
- WeChat
- WhatsApp
- WhatsApp Negocios
- Wickr Me
- Xabber
- Yahoo Messenger
- Yalla
- YapChat
- YouMagic
- Zangi

- **Otras aplicaciones**
  - AllTrails
  - Cualquiera
  - Ctrip
  - Evernote
  - Facebook
  - Foursquare
  - Gettaxi
  - Calendario de Google
  - Google Docs
  - Google Duo
  - Google Keep
  - Google Maps
  - Búsqueda en Google Maps
  - Google Translate
  - Imgur
  - Instagram
  - Likee
  - LinkedIn
  - Memo
  - Pinterest
  - Pokemon GO
  - Richnote
  - Notas de Samsung
  - Sango
  - Sgallery (calculadora secreta)
  - SharePoint
  - Sina Weibo
  - Enjambre
  - Threema
  - Tinder
  - Uber
  - Susurro
  - YandexTaxi
  - Zalo
  - Zello
  - Zoom

- **P2P**
  - Transferencia de datos por Bluetooth
  - ShareIT

- **Sistemas de pago**
  - Monedero Bitcoin para Android
  - Cartera Bitcoin Armory
  - Billetera Bitcoin Core
  - Jaxx
  - Billetera Qiwi

- **Pulseras de fitness**
  - Fitbit
  - Mi Fit

- **Archivos de sistema**
  - Cuentas
  - ADB acoge
  - Actualizaciones de la aplicación
  - Uso de la batería
  - Dispositivos Bluetooth
  - Información del dispositivo
  - Bienestar digital
  - Búsquedas en Google Play
  - Paquetes instalados
  - Actividad reciente
  - Permisos
  - Estadísticas de uso
  - Conexiones Wi-Fi

Belkasoft
forensics made easier

702 San Conrado Terrace, Unit 1 Sunnyvale CA, Estados Unidos 94085
+1 (650) 272-0384 (EE.UU. y Canadá)correo electrónico: sales@belkasoft.com

iOS

- **Aplicaciones estándar**
  - Alarma
  - Calendario
  - Llamadas
  - Contactos
  - Aplicaciones instaladas
  - Notas
  - SMS
  - Correo de voz
  - Tiempo

- **Navegadores**
  - Cromo
  - Delfín
  - Borde
  - Firefox
  - Maxthon
  - Mercurio
  - Cebolla
  - Ópera
  - Puffin
  - Safari
  - Navegador UC

- **Mensajeros**
  - Brosix
  - Quemador
  - ChatOn
  - ChatSecure
  - Confíe en
  - CoverMe
  - eBuddy XMS
  - Facebook Messenger
  - FireChat
  - Fring
  - Google Meet
  - Google Voz
  - Grindr
  - GroupMe
  - Growlr
  - HeyTell
  - ICQ
  - Im+
  - iMessage
  - OMI
  - Instagram Directo
  - Hangouts para iOS
  - KakaoTalk
  - Kik
  - Likee
  - Línea
  - MeetMe
  - Chat Miau
  - MSTeams
  - SiguientePlus
  - Odnoklassniki
  - ooVoo
  - Paltalk
  - Recientes
  - Señal
  - Skout
  - Skype
  - Slack
  - TamTam
  - Tango
  - Telegrama
  - Texto Plus
  - Textie
  - TextMe
  - TikTok
  - Toque
  - Tumblr
  - Twitter
  - Viber
  - Vipole
  - Aplicación VK
  - WeChat
  - WhatsApp
  - Wickr Me
  - Yahoo! Messenger
  - YapApp
  - Yubo
  - Zangi

- **Correos**
  - Correo de Apple
  - CorreoRu Mail
  - Correo Yahoo
  - Yandex Mail.ru

- **Otras aplicaciones**
  - Cualquiera
  - CarPlay
  - Evernote
  - FaceTime
  - Garmin
  - Gettaxi

702 San Conrado Terrace,
Unit 1 Sunnyvale CA, Estados Unidos 94085
+1 (650) 272-0384 (EE.UU. y Canadá)correo electrónico:
sales@belkasoft.com

- Salud
- Instagram
- Hilos de Instagram
- LiveMe
- Pinterest
- Pokemon GO
- Richnote
- ShareIT
- Snapchat
- Tinder
- Twitter
- Uber
- Susurro
- Zello

- **Archivos de sistema**
  - Cuentas
  - Información de la cuenta de Apple
  - Dispositivos Bluetooth
  - Configuraciones celulares
  - Información del dispositivo
  - Información sobre hardware
  - Bioma iOS
  - Conexiones IP
  - Notificaciones
  - Software e información de la tarjeta SIM
  - Zona horaria y fecha/hora de la última copia de seguridad
  - Estadísticas de uso: ADDataStore, DataUsage, knowledgeC
  - Notificaciones a los usuarios
  - Conexiones Wi-Fi

- **Servicios en la nube**
  - Dropbox

Blackberry

- **Aplicaciones estándar**
  - Calendario
  - Llamadas
  - Contactos

Las listas anteriores pueden variar de una versión a otra, ya que con cada nueva versión se admiten artefactos adicionales.

Tipos de análisis admitidos

Belkasoft X cuenta con las siguientes funciones analíticas:

- Búsqueda de texto completo en todos los tipos de pruebas recopiladas
  - Búsqueda por palabra o frase, búsqueda por archivo de palabras clave, búsqueda por expresión regular.
  - Indexación automática de varias plantillas de texto importantes, como correos electrónicos, números de teléfono y SSN, direcciones MAC e IP, etc.
  - Los resultados de la búsqueda se visualizan en una ventana aparte. Se almacena el historial de búsqueda.
  - Los resultados de la búsqueda pueden filtrarse por datos, fuente de datos y tipo de datos.
  - Los resultados de la búsqueda pueden añadirse a un marcador o a un informe.
- La línea de tiempo gráfica se encuentra en la pestaña Línea de tiempo, donde se puede cambiar entre Vista de cuadrícula y Vista de gráfico.
- Generación de archivos de palabras clave específicos para ataques de fuerza bruta a contraseñas
- Las imágenes pueden analizarse en busca de textos escaneados, rostros, armas y pornografía
  - Las imágenes detectadas como pornografía pueden difuminarse.

702 San Conrado Terrace,
Unit 1 Sunnyvale CA, Estados Unidos 94085
+1 (650) 272-0384 (EE.UU. y Canadá)correo electrónico:
sales@belkasoft.com

- Los datos de geolocalización pueden mostrarse en la ventana de **Open Street Maps** o en una aplicación de terceros de Google Earth. También se puede crear un informe a partir de este visor.
    - La ventana Mapas muestra rutas para vuelos de drones y otras aplicaciones con geodatos.
- Los vínculos entre personas pueden encontrarse utilizando funciones **de Connection Graph** como la visualización de comunicaciones y la detección de comunidades.

- **Compatibilidad con SQLite**
    - La compatibilidad nativa con bases de datos SQLite permite recuperar bases de datos gravemente dañadas y parcialmente sobrescritas.
    - El visor de SQLite incorporado ayuda a visualizar la base de datos SQLite sin necesidad de aplicaciones de terceros. Puede inspeccionar el esquema de la base de datos, ver los datos existentes y eliminados, hacer conversiones de fecha y hora y columnas de cadena.
    - A diferencia de los visores SQLite estándar, Belkasoft X **SQLite Viewer** abrirá perfectamente archivos SQLite dañados y mostrará la parte correcta del archivo.
    - El análisis de SQLite freelist, WAL y journal file, así como SQLite Unallocated, extrae pruebas destruidas y muestra información eliminada, como mensajes SMS de iPhone borrados y chats de Skype limpiados.

- El visor de bases de datos SQLite incorporado admite los siguientes tipos de análisis:
    - Visualización de todas las tablas de la base de datos
    - Visualización del esquema de la base de datos
    - Visualización de todos los datos de la tabla seleccionada
    - Posibilidad de ocultar o mostrar una columna
    - Posibilidad de crear un informe para todos los registros de la tabla o para los seleccionados
    - Visualización del espacio no asignado dentro del archivo de base de datos
    - Posibilidad de ver el registro seleccionado del espacio no asignado en el Visor hexadecimal
    - Capacidad para analizar automáticamente el archivo de registro de base de datos adjunto (en formatos .journal y .wal).
    - Posibilidad de encontrar y visualizar los datos eliminados (registros de la lista freelist), marcándolos con un color diferente.
    - Posibilidad de ver tanto la base de datos añadida al caso, como una base de datos arbitraria del almacén.
    - Posibilidad de visualizar la base de datos SQLite, obtenida mediante búsqueda de firmas ("carving") en discos, imágenes de disco e imágenes RAM.
    - Visualización de metadatos de bases de datos SQLite
    - Posibilidad de ver una vista previa de los datos BLOB

Otras funciones incluidas

Entre otras funciones incluidas en Belkasoft X se encuentran:

- Informes en numerosos formatos como texto, HTML, XML, CSV, PDF, RTF, Excel, Word, EML, KML, S21 (Semantics21). También es posible crear un informe para la vista de burbujas.
- La herramienta gratuita Evidence Reader (también conocida como "maletín portátil") permite compartir tus hallazgos con tus colegas con o sin Belkasoft X instalado. Permite guardar archivos multimedia en la base de datos
- Capacidad para ejecutar el software Belkasoft X en una nube
- Visor Plist integrado

702 San Conrado Terrace,
Unit 1 Sunnyvale CA, Estados Unidos 94085
+1 (650) 272-0384 (EE.UU. y Canadá)correo electrónico:
sales@belkasoft.com

- Gestión de casos: posibilidad de almacenar varios casos al mismo tiempo, abrir y editar casos en orden aleatorio, añadir nuevas fuentes de datos (discos, imágenes de disco, dispositivos móviles, volcados de memoria, etc.) a un caso, posibilidad de eliminar casos, cambiar la ubicación de los casos, etc.
- Posibilidad de analizar varias fuentes de datos en un mismo caso (por ejemplo, varios discos duros, imágenes de disco y teléfonos móviles) sin necesidad de crear un nuevo caso para cada fuente de datos.
- Talla personalizada, incluida la compatibilidad con los conjuntos Scalpel y FTK.
- El motor ElasticSearch agiliza y refuerza el proceso de indexación, permitiendo el acceso multihilo al índice y a herramientas de terceros para examinarlo.
- La opción Motor de base de datos permite seleccionar una base de datos al crear un nuevo caso: SQLite o PostgreSQL, dependiendo de la complejidad del caso.
- Reproductores de audio y vídeo
- Visores de correo electrónico e imágenes
- Tutoriales de productos integrados

Entre las funciones de eDiscovery incluidas en Belkasoft X se encuentran:

- Filtrado de datos en FileSystem por cualquier columna disponible
- Tipos de condiciones en los filtros, como filtros basados en texto ("contiene", "empieza por", "termina por"), filtros de rango de fechas.
- Filtro "IN" basado en listas (construcción de criterios complejos, basados en listas largas)
- Conjunciones AND u OR, cláusulas NOT
- Filtros con nombre
- Los filtros globales del visor del sistema de archivos son ahora globales (se aplican a todos los datos)
- Filtrado de archivos por conjuntos de hash de listas blancas y negras.
- Filtrado de datos en el visor del sistema de archivos mediante la minilínea de tiempo
- Los resultados del trabajo pueden exportarse a los formatos RSMF y Concordance.
- El archivo de carga de concordancia puede importarse a un caso Belkasoft X

Se admite API para la automatización de análisis. Los usuarios de Belkasoft X pueden realizar múltiples tareas en el modo CLI (interfaz de línea de comandos):

- Crear un caso o abrir uno existente
- Añadir una nueva fuente de datos al caso
- Adquirir una fuente de datos desde un disco duro o a través de un dispositivo Tableau TX1
- Analizar la fuente de datos utilizando un perfil de análisis predefinido
- Realizar análisis de disco en directo
- Cree un informe en uno o varios formatos a la vez, como PDF, HTML, CSV, Excel, Word y otros.
- Exportación de datos a numerosos formatos, como Semantics 21, RSMF (Relativity Short Message Format) y Project VIC.
- Y realizar tipos adicionales de procesamiento, que Belkasoft X también permite realizar dentro de su Interfaz de Usuario

El configurador de línea de comandos es compatible y permite editar el archivo JSON de configuración en una interfaz de usuario.

Belkasoft X Forensic le permite ver y navegar a través de todas las carpetas y archivos dentro de una fuente de datos añadida a su caso, incluyendo archivos y carpetas ocultos, eliminados y especiales del sistema, por ejemplo, $OrphanFiles o $Extends. Los procesos de memoria se extraen de los volcados de RAM.

702 San Conrado Terrace,
Unit 1 Sunnyvale CA, Estados
Unidos 94085
+1 (650) 272-0384 (EE.UU. y
Canadá)correo electrónico:
sales@belkasoft.com

Puede examinar cualquier sistema de archivos de móvil u ordenador, así como un volcado de memoria, adquirido con Belkasoft X o cualquier software de terceros. Conveniente ventana Visor hexadecimal le permite revisar el archivo elegido o procesar el contenido binario.
Se puede extraer todo el contenido de una fuente de datos o subcarpeta de forma recursiva desde una fuente de datos a un ordenador para su posterior investigación. Se admite la vista recursiva de la ventana Sistema de archivos.

Se incluye la función de análisis de hashset. Tipos de hashset admitidos:

- Ficheros NSRL
- Listas hash simples
- Archivos ProjectVic
- Bases de datos NIST RDSv3

Se admite el filtrado de archivos por base de datos hashset seleccionada (lista blanca/negra).
La vista de galería está disponible para los archivos encontrados.
También puedes calcular hashes de archivos utilizando los algoritmos SHA y MD5.

Además, es posible comprobar los procesos y archivos de la memoria en busca de malware utilizando varios métodos, como la detección de nombres falsos de procesos del sistema y la comprobación con VirusTotal.

Sistemas de archivos compatibles

- APFS
- BTRFS
- ext2
- ext3
- ext4
- F2FS
- FAT
- exFAT
- HFS
- HFS+
- NTFS
- XFS
- YAFFS
- YAFFS2

El **Visor Hexadecimal** incorporado tiene la siguiente funcionalidad:

- Mostrar el contenido del archivo seleccionado, mostrar los procesos de un volcado de memoria, mostrar los registros del espacio no asignado en la base de datos SQLite seleccionada, mostrar la información encontrada mediante la búsqueda de firmas
- Posibilidad de crear marcadores dentro del contenido del archivo.
- Posibilidad de establecer el color, el nombre y la descripción de un marcador.
- Posibilidad de navegar entre marcadores.
- Posibilidad de cambiar la codificación del texto visualizado, en particular, compatibilidad con codificaciones cirílicas, ANSI, Unicode, UTF 7, UTF 8 y juegos de caracteres chinos y asiáticos.
- Posibilidad de guardar el fragmento de texto seleccionado en un archivo.
- Posibilidad de navegar por el texto por desplazamiento relativo al inicio o al final del archivo, la posición actual del cursor.

702 San Conrado Terrace,
Unit 1 Sunnyvale CA, Estados
Unidos 94085
+1 (650) 272-0384 (EE.UU. y
Canadá)correo electrónico:
sales@belkasoft.com

MFT Viewer muestra información MFT de un archivo seleccionado en la lista de archivos. Se puede encontrar diversa información útil sobre los archivos, como tamaño, fecha y hora, permisos. También se muestra el contenido de los archivos residentes.

El Visor de flujos de datos alternativos (ADS) muestra los datos binarios del flujo alternativo elegido para un archivo seleccionado en el Sistema de archivos.

Integraciones de terceros

- **Volatilidad**

  Volatility es una herramienta multiplataforma de código abierto para analizar imágenes de RAM. Se admiten los siguientes módulos de Volatility:
  - Memmap
  - PsList
  - dlllist
  - escáner de archivos
  - módulos
  - malfind
- **Cisco Clam AV**

  Clam AV es un popular software antivirus de código abierto que puede detectar varios tipos de malware, incluidos virus, troyanos y gusanos. El software es compatible con la mayoría de los sistemas operativos, incluidos Windows, Linux y macOS. Clam AV puede funcionar sin conexión a Internet.
- **VirusTotal**

  Para analizar archivos sospechosos en VirusTotal, se envía la memoria de procesos (para RAM) y la suma hash (para archivos).

Belkasoft
forensics made easier

702 San Conrado Terrace,
Unit 1 Sunnyvale CA, Estados
Unidos 94085
+1 (650) 272-0384 (EE.UU. y
Canadá)correo electrónico:
sales@belkasoft.com

Complementos

Módulo de fuerza bruta para móviles

El módulo permite forzar (es decir, adivinar) códigos de acceso, también conocidos como contraseñas y códigos pin, para una amplia gama de dispositivos iOS y varios dispositivos Android. No se requiere hardware especializado; todo lo que necesitas es Belkasoft X con el nuevo módulo. El producto puede superar varias restricciones, como el Modo Restringido USB, los retrasos entre intentos de contraseña y la desactivación del teléfono tras una serie de entradas fallidas del código de acceso.

Dispositivos

compatibles

Dispositivos iOS

- iPhone 5 con iOS 9.0-10.3.4
- iPhone 5C con iOS 9.0-10.3.4
- iPhone 6s con iOS 14-iOS 15
- iPhone 6s Plus con iOS 14-iOS 15
- iPhone SE (1ª generación) con iOS 14-iOS 15
- iPhone 7 con iOS 14-iOS 15
- iPhone 7 Plus con iOS 14-iOS 15
- iPad Pro (12,9 pulgadas) (2ª generación) con iOS 14-iOS 15
- iPad (6ª generación) con iOS 14-iOS 15
- iPad (7ª generación) con iOS 14-iOS 15
- iPad Pro (10,5 pulgadas) (1ª generación) con iOS 14-iOS 15

Dispositivos Android

- Huawei Nova 4 con Android 9-10
- Huawei P20 Pro con Android 9-10
- Honor 10 con Android 9-10
- Huawei Mate 10 con Android 9-10
- Huawei P20 con Android 9-10
- Huawei Nova 3 con Android 9-10
- Honor Note 10 con Android 9-10
- Y otros basados en el chipset Kirin 970

Velocidades de fuerza bruta

- iPhone 5 y 5C: 11 contraseñas por segundo
- iPhone 6, 6 Plus, SE (1ª generación), 7, 7 Plus, iPad Pro, iPad (6ª generación), iPad (7ª generación), iPad Pro (10,5 pulgadas) (1ª generación):
    - Fuerza bruta rápida: 3 contraseñas por segundo
    - Fuerza bruta lenta: 1 contraseña cada 8-9 minutos
- Dispositivos basados en Kirin 970: 80 contraseñas por segundo

Belkasoft
forensics made easier

702 San Conrado Terrace,
Unit 1 Sunnyvale CA, Estados Unidos 94085
+1 (650) 272-0384 (EE.UU. y Canadá)correo electrónico:
sales@belkasoft.com

Módulo de descifrado

Mientras que Belkasoft X es capaz de detectar más de 300 tipos de archivos y volúmenes cifrados, el módulo de descifrado perfectamente integrado de Passware le permite descifrar con éxito los elementos protegidos y extraer su contenido, todo desde la interfaz del producto.

Equipado con el Módulo de Descifrado, Belkasoft X será capaz de descubrir y descifrar: numerosos formatos de documentos, Bitlocker y McAfee Endpoint Security, archivos RAR y ZIP, Quickbooks, copias de seguridad de iTunes, y mucho más.

Se admite el descifrado de FileVault, Bitlocker y McAfee Endpoint Security dentro de imágenes cifradas, por ejemplo, dentro de archivos DMG cifrados.

Nota: se requiere una contraseña conocida.

Gracias a la completa integración entre Belkasoft X y Passware Kit Forensic, el descifrado se puede realizar dentro de Belkasoft X simplemente haciendo clic en un botón. Esta característica facilita significativamente el proceso de investigación, ya que le permite examinar los datos descifrados inmediatamente utilizando las potentes capacidades analíticas de Belkasoft X.
En particular, la encriptación bruta de archivos se puede realizar mediante los siguientes métodos:

- Utilizar un diccionario de claves del caso
- Utilizar diccionarios de contraseñas externos
- Iterar sobre todas las contraseñas, que coinciden con un tipo específico de ataque

El módulo también incluye licencia independiente Passware Kit Forensic.