E.D.R. TOOLS SRL
for Digital Forensics & Data Recovery
Head office: Viale Giacomo Leopardi, 24/2 - 33100 UDINE (ITALY)
Headquarters: via Roveredo, 20/B – 33170 PORDENONE (ITALY)
www.edrtools.eu info@edrtools.eu

EDR TOOLS EAGLE PLATINUM 2024

EAGLE PLATINUM kit is a toolset designed to maximize the forensic investigation results on tablets, smartphones, drones, car infotainment and gps systems (based on emmc chips). The system provides different levels of acquisition allowing to work both working and non-functioning devices via download cable or chip-off. Can be used for diagnostics purpose and acquisition via data cable and, when needed, disassembly of the device to force access, extraction of decrypt keys or to read the memory chip directly. This method ensures that no chance of accessing the data is left untaken. The result of reading the memory chips is a standard file in ISO binary format that can be imported into the analysis software included in the toolset.

For chip-off a multi socket reader is provided together with its own usb cable.
Main advantages of our reader:

- Low power needed to be safely used on laptops pcs also.
- Power control and overcurrent protection
- The adapter socket doesn't need reballing, avoiding chip heat stress.
- Write blocked.
- Extractor software creates validated and complete image files (including unallocated areas)
- Advanced settings for 1,4,8, bit read, BUS Width, block size, read forward/backward, and timeout.
- Use of vendor specific commands to change the way the tool accesses the chip (decrease block size, deal with ECC, override minor controller failures or firmware issues and so on)

- Real time monitor to check hex content while reading.
- Real time skipped sectors map to refine the copy or include it in the list for partial copy hashing (SHA and MD5)
- BGA supported chips: BGA153, BGA169, BGA162, BGA186, BGA221, BGA529
- 6 frames to adapt different physical size of chips
- ISP port for ISP operations.

E.D.R. TOOLS SRL
for Digital Forensics & Data Recovery
Head office: Viale Giacomo Leopardi, 24/2 - 33100 UDINE (ITALY)
Headquarters: via Roveredo, 20/B – 33170 PORDENONE (ITALY)
www.edrtools.eu info@edrtools.eu

USB acquisition and analysis software:
Get more from the cloud with over 100 supported services
and extract data from over 40,000 app versions.

Cloud
Extract more cloud services than any other digital forensic tool on the market. Gain access to popular cloud services like WhatsApp, Telegram, iCloud, Google, Samsung, Microsoft, Facebook, Instagram, and Twitter.
The built-in extractor allows investigators to gain access to a tremendous amount of cloud services that include iCloud, Google, Microsoft, Samsung,
Huawei, E-mail server, Facebook, Twitter, Instagram, Dropbox, WhatsApp, Telegram, Viber, WickrMe, etc. Our Cloud Extractor also offers the exclusive ability to decrypt WhatsApp backups via phone number.
Investigators may utilize either account credentials or tokens to access any supported cloud storage. Using our software, investigators can extract credentials and tokens directly from
a mobile device as well as collect them on Windows, Mac, and Linux OS computers. Credentials can then be used to extract evidence from the associated cloud service.

Mobile PHYSICAL/LOGICAL da acquisition and analysis
Extract data from over 31,000 devices, a wide range of Apple iOS and Android devices are supported. Data extraction from **Apple iOS, Android devices, feature phones, media, and SIM cards**. Because time is always of importance, simultaneous acquisition of several devices is available. Import numerous backups and images, including iTunes, Android backups, GrayKey, JTAG, Chip-off, UFED, XRY images, .dar archives, Warrant Returns, and more.
Security bypassing
Encryption of user data is enabled on Android devices by default and cannot be disabled. Starting with Android 10, file-based encryption (FBE) is used for data encryption, on earlier Android versions, full disk encryption (FDE) was used. Encryption process uses the hardware key, if the chipset supports that, using proprietary methods we can extract encryption keys and bypass screen locks on mobile devices, including Samsung, LG, Motorola, as well as devices based on Mediatek, Spreadtrum, Kirin, Exynos or Qualcomm chipsets, **automatically find passwords to encrypted iTunes backups and Android image files**

Smart watch
Extract from the most popular brands: Apple, Samsung, Huawei, Fitbit, and more.
Through logical acquisition of smartwatches based on MTK chipsets allowing forensic experts to extract device model, contacts, calls, messages, multimedia files, and other data. Moreover, the software acquires complete data from various fitness apps, like Apple Health (including data synched with Apple Watch), Samsung Health, Google Fit, FitBit, Endomondo, and more, often containing a tremendous amount of geo locations with time stamps, health data, steps, and stair count with additional user statistics.

E.D.R. TOOLS SRL
for Digital Forensics & Data Recovery
Head office: Viale Giacomo Leopardi, 24/2 - 33100 UDINE (ITALY)
Headquarters: via Roveredo, 20/B – 33170 PORDENONE (ITALY)
www.edrtools.eu info@edrtools.eu

Drones

Extract and analyze drone data from physical dumps, drone logs, and mobile applications.

Enable the verbose data parsing and analysis from drone collections, flight logs, mobile apps, and cloud services, create or import drone physical extractions and parse GPS locations showing valuable route data as well as device telemetry to include: speed, direction, altitude, temperature, and more. Currently, various models of DJI and Parrot drones are supported.

Data parsing from drone applications is also available from iOS and Android devices. Investigators can decode drone images and videos, locations with time stamps and other data. Additionally, drone data extraction from cloud services can be accomplished via login/password or token from DJI, SkyPixel or My Parrot clouds.

IoT Devices

Extract and analyze data from the most popular IoT devices: Amazon, Alexa, and Google Home.

Oxygen Forensic® Detective currently offers data extraction from two popular IoT devices – Amazon Alexa and Google Home. Since it is difficult to extract data directly from devices, we provide investigators with the ability to access alternative sources – cloud and mobile apps. Investigators can gain access to cloud information via login/password or token that can often be extracted from the user's PC or mobile devices.

We also extract IoT app data from Apple iOS and Android devices.

Computers

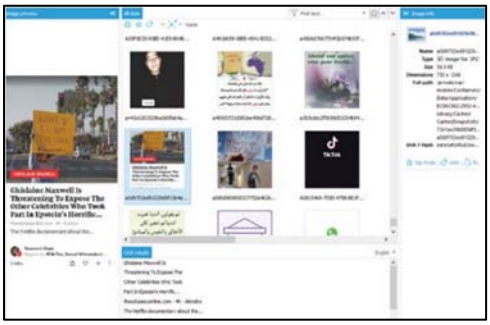
Extract and analyze data from Windows, Linux, and macOS, find passwords and tokens of web browsers and desktop apps.

Key built-in utility focuses on extracting and decrypting credentials, system files, and user data from web browsers and desktop apps on computers running Windows, macOS, or Linux.

Currently, there are numerous desktop apps supported, including WhatsApp, Viber, WickrMe, Telegram, Skype, Signal, Microsoft Mail, Microsoft Outlook, Thunderbird, all the popular Web browsers, pre-installed Apple apps, etc. Collected tokens and passwords can be immediately used for cloud data extraction while extracted web browser, messenger, and email data can be imported for further analysis and analytics with mobile data artifacts in one case.

E.D.R. TOOLS SRL
for Digital Forensics & Data Recovery
Head office: Viale Giacomo Leopardi, 24/2 - 33100 UDINE (ITALY)
Headquarters: via Roveredo, 20/B – 33170 PORDENONE (ITALY)
www.edrtools.eu info@edrtools.eu

Optical Character Recognition – OCR Investigators no longer have to spend time manually transcribing text within a picture. The included OCR section allows investigators to easily convert any words contained in a screenshot or photo to machine-encoded text. To enable and configure this feature, go to Options/Advanced Analytics in the software. Then, in the OCR section, run image OCR by pressing the relevant button on the toolbar. Once OCR has been run, investigators can use the quick filter to search for text across the processed images.

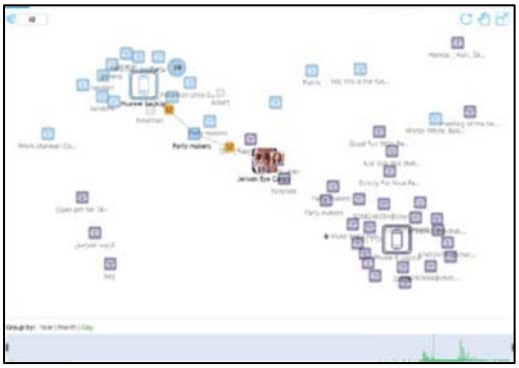


Statistics

The Statistics section consists of several widgets that are divided into two categories–data on the device and investigator interaction. Data on the device is displayed in the first group of widgets and shows the data present within the extraction in charts or tables (Activity Chart, Activity Matrix, Last Contacted, Data Types, Top 10 Applications, Contacts, or Groups). The second group of widgets, or investigator interactions widgets, display the investigator's interactions with the evidence: assigning tags, marking data as Key Evidence, adding and editing notes, running hash set searches.

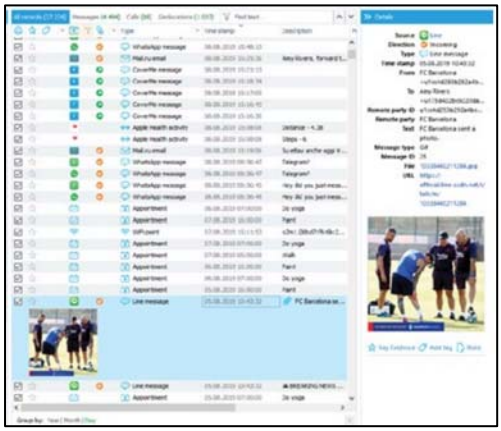
Social Links

The built-in Social Graph provides a convenient platform to explore social connections between a device owner and contacts or between several devices. Using the Social Graph, investigators can identify the device owner's closest contacts in one click. Click on any contact to open a card containing detailed information about the selected contact and all communications across device sources. The Social Graph interface is dynamic and nimble, and investigators can drag and drop to move, hide, or merge contacts while producing a crystal clear view of device and case connections.



E.D.R. TOOLS SRL
for Digital Forensics & Data Recovery
Head office: Viale Giacomo Leopardi, 24/2 - 33100 UDINE (ITALY)
Headquarters: via Roveredo, 20/B – 33170 PORDENONE (ITALY)
www.edrtools.eu info@edrtools.eu

Timeline The Timeline section provides a view of all device events in one list – chats within apps, calls, web activity, web connections, photos and videos, calendar events, and more. Events can be viewed for one device or a group of devices, allowing easy identification of common group activities. Sort and filter by date, time, activity frequency, contact, remote party, or other data points to focus only on the most relevant data. The geo Timeline tab contains the full list of geo coordinates from all the sources that include photos, videos, apps, drone flight logs, and more.

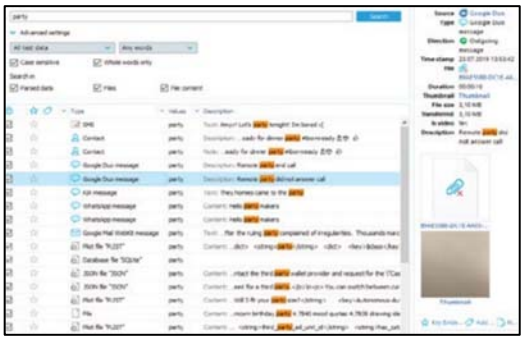


Maps, acquires geo coordinates from all possible sources including mobile devices, drones, cloud storages, media cards, and imported images. Once analyzed, the data can be viewed within our Maps application either online or offline.

The Maps module includes the ability to:

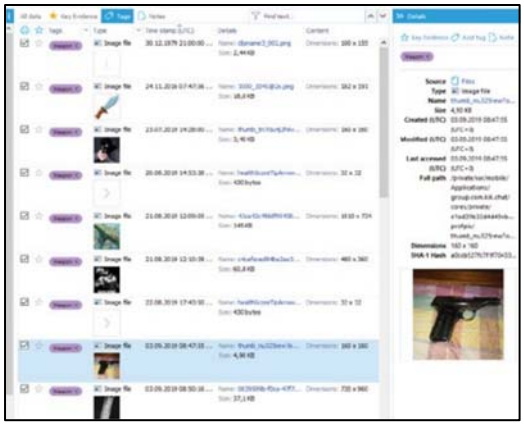
- Identify a device's frequently visited places
- Visualization of a device's movements within specified period of time
- Pinpointing common locations of several devices
- Playing an animated route showing the direction of Travel

Data Search, allows investigators to search across a single device, all devices in a case, or all devices in a database for text, phone numbers, email addresses, geo coordinates, IP addresses, MAC addresses, credit card numbers, and file hashes including Project VIC. A Regular Expression library is available for custom search functions, and the Keyword List Manager and Watchlists allow investigators to create a set of keywords and perform searches during or after an extraction.



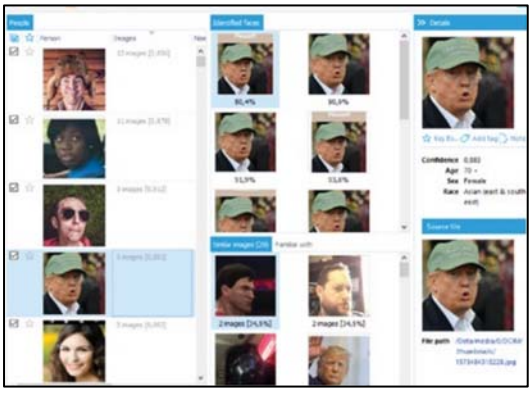
E.D.R. TOOLS SRL
for Digital Forensics & Data Recovery
Head office: Viale Giacomo Leopardi, 24/2 - 33100 UDINE (ITALY)
Headquarters: via Roveredo, 20/B – 33170 PORDENONE (ITALY)
www.edrtools.eu info@edrtools.eu

Image Categorization, provides the ability to classify images into eighteen different categories that include pornography, extremism, drugs, alcohol, and weapons.

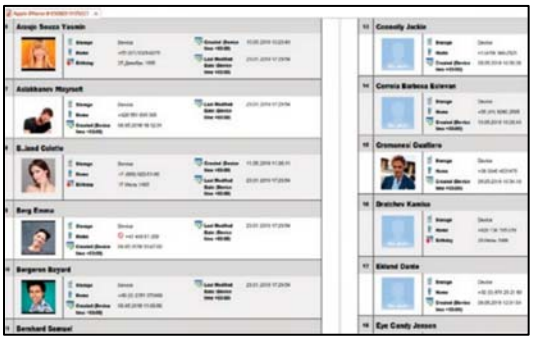


Our image categorization is available when importing device data and also on already-imported extractions. Investigators can select all or selected categories while also having the ability to fine-tune the positive "hit" settings. After running the image analysis, the number of matching images for each supported category is tagged and shown in Key Evidence and the Files sections. Investigators can review the tagged data and manually exclude any false positives.

Facial Categorization, offers the ability for investigators to categorize human faces. Facial categorization is available in the Faces section at no additional charge. The unique features include detailed face analytics (gender, race, age), immediate categorization and matching, and support for massive volumes of data. Using built-in facial categorization investigators will spend less time looking through thousands of photos or videos in mobile, cloud, or drone extractions.



Data Reports, enables data export from any section to many popular file formats including PDF, RTF, XLS, XML, HTML, etc. A report can be created to include a single device, several devices, several sections or even selected records. Reports are highly customizable to display only the data required for any type of case. Our XML reports can be integrated into other analytic software platforms.



E.D.R. TOOLS SRL
for Digital Forensics & Data Recovery
Head office: Viale Giacomo Leopardi, 24/2 - 33100 UDINE (ITALY)
Headquarters: via Roveredo, 20/B – 33170 PORDENONE (ITALY)
www.edrtools.eu info@edrtools.eu

Sim Card Reader

EDR Tools SIM card reader set include the hardware to read SIM Cards.
Using EDR Tools software is possible to dump the chip to be analyzed and create a forensic clone on another card.
Forensic clone means that the SIM card is detected with original content but will not connect to carrier to prevent any change or wipe remotely.

FEATURES:

License type: perpetual
devices: Mobile phones, smart watches, feature phones, drones, cars
Unlocking utility: Android phones
Data decoding: Both FDE and FBE
Phone operating system support: iOS, Android, KaiOS
Support damaged phones: yes.
Support chip-off method: both Emmc and Emcp chips
Memory card support: yes
Write Block: yes.
cloud services: Dropbox, Google, Instagram, Twitter (X), telegram, WhatsApp…
Phone application support: yes, more than 800 apps supported (40.000 app versions)
Recover deleted data:Yes
Image recognition: Yes
Face recognition: Yes
Timeline analysis: Yes
Generate reports: Yes, in PDF, RTF, XLS, XML, HTML, etc,

What's included in the EAGLE PLATINUM set:

Acquisition, unlock and analysis software
USB cable to acquire smartphones/tablets
EDR Tools EAGLE READER (with ISP port)
Full set of Emmc/Emcp frames
Equipment hard case

No More SwissKnife and CheckRa1n box as all the unlock options are now included in the main software without the need of any add-on, with many new features and supported models

E.D.R. TOOLS SRL
for Digital Forensics & Data Recovery
Head office: Viale Giacomo Leopardi, 24/2 - 33100 UDINE (ITALY)
Headquarters: via Roveredo, 20/B – 33170 PORDENONE (ITALY)
www.edrtools.eu info@edrtools.eu

OPTIONAL

MediaTek 6261DA Adapter

The MediaTek 6261DA SoC Adapter is a socket adapter that connects to the USB port that allows access to data stored into the internal NOR memory in MediaTEK SoC (MTK) 6261DA. These processors (SoCs) are often found in cheap smartwatch and phones, so-called Feature phones, such as Nokia 106 TA 1114, Nokia 108 RM 944, Nokia 105-2 RM 1133, Nokia 105 TA 1034 and many smartwatches. Its use is simple: immediately after ChipOFF, place the processor in the adapter and connect the adapter to the USB for data reading.

Features:

- physical reading of NOR memory directly from the MTK 6261DA based processor regardless of manufacturer
- reading deleted messages, calls list, Contacts, compatible with many analysis software
- possibility of RAW copy of the FLASH within contained for forensic verification

Spreadtrum 6531E Adapter

The Spreadtrum 6531E SOC Adapter is a socket adapter that connects to the USB port allowing to access data stored into the internal NOR memory in the SC6531E Spreadtrum (SPD) SoC. These processors (SoCs) are found in cheap smartwatches and phones, so-called feature phones, such as nokia 105 (2019) TA-1174, as well as in many smartwatches. Its use is simple: immediately after ChipOFF, place the processor in the adapter and connect the adapter to the USB to enable data reading.

Features:

- physical reading of NOR memory directly from SC 6531E based processor, regardless of manufacturer
- full communication in SVC/FTM mode and DLOAD mode by simply pressing the button
- Universal boot key for all 6531E
- reading deleted messages, calls list, Contacts, compatible with many analysis software