paraben® corporation

Electronic Evidence Examiner

paraben corporation

RELEASE VERSION

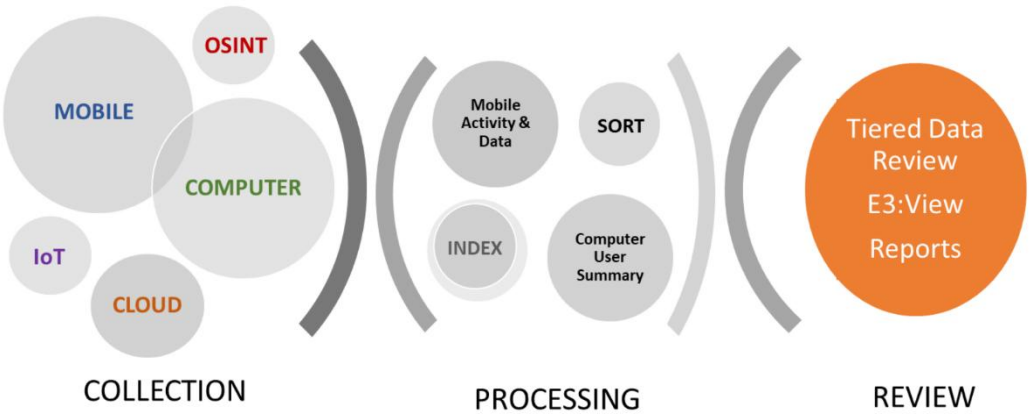
VER 4.3

WHAT IS E3 (Electronic Evidence Examiner)?

Paraben's Electronic Evidence Examiner (**E3**) represents a comprehensive digital forensic solution tailored for more efficient data handling. The E3 Platform offers a range of licensing options to suit your specific needs.

E3:UNIVERSAL, our premium license, covers a wide spectrum of data types, encompassing hard drive, smartphone, and IoT data. We also provide specialized licenses focusing on mobile data processing, computer analysis, cloud data capture and analysis, OSINT, and email examination. Paraben offers licensing options that are flexible and allow for upgrade paths between licenses.

The E3 Platform leverages Paraben's advanced plug-in architecture to create specialized engines for scrutinizing various data elements, such as email, network communications, chat logs, mobile data, file systems, Internet files, and smartphones. Moreover, it enhances data processing capacity, harnessing resources through multi-threading and task scheduling.



E3 Platform License Options

E3 Subscriptions

If you're an existing subscriber looking to renew your subscription, don't hesitate to contact us at sales@paraben.com. Subscribing provides you with valuable benefits such as receiving updates with each new release, access to our dedicated technical support team, and special discounts.

E3 Trial Licenses

If you're interested in trying out the E3 Platform with a trial version, all you must do is request it. We're more than willing to provide you with a fully functional trial, allowing you to explore and test all its features. Just send an email to trial@paraben.com, and we'll initiate your trial period.

E3 Computer Functionality

- The **Logs & Artifacts Import Wizard** has been extended with new importing options. Now you can import:
  - An archive with CSV files containing results of data analysis performed by the **KAPE (Kroll Artifact Parser and Extractor)** tool modules.
  - An output folder with results of disk image processing by the **IPED Digital Forensic Tool**. You can opt to import either the whole folder or just the parsed CSV files.
- Export of data to the **Relativity format (Load file)** has been added for the following types of file system evidence:
  - Folder
  - Logical drive
  - Disk image of NTFS, FAT32, exFAT, EXT4, and APFS logical drive
  - Archives

E3 Mobile Functionality

- A list of applications installed in the **Android Private Space** can be viewed in the **Installed Application List** grid.
- Information on whether an application **was removed** from Android device is available now in the **Installed Application List** grid.
- **Acquisition of multiple user accounts** with Android devices.
- Export of E3 data cases to the **Relativity format (Load file)** has been added. You can export the following data types:
  - Grids
  - Binary files
  - Grids' binary attachments
- Export of message grids to the **Relativity Short Message Format** has been added for:
  - iOS messages including iMessages and attachments
  - Android SMS, RCS, MMS and their attachments

E3 Supported Device Profiles

40,777+ SUPPORTED

Electronic Evidence Examiner Key Features

GENERAL FEATURES

- Full Windows 11 & 10 compatibility, including UAC and digital signature by Microsoft.
- x64 version
- Back-end Firebird database for support of massive amounts of data
- Multi-threading and task scheduling capabilities to process more data in less time.
- Simultaneous acquisition of multiple devices
- Convenient plug-in architecture
- An easy-to-use registration scheme includes a web-based licensing method that allows the use of the application on any computer without the dongle!
- Ability to save a case along with its Keyword Indexing database and attach evidence files to a single archive from the program interface.
- Single interface for all types of digital evidence.

GUI FEATURES

- Document viewer for more than 100 most popular file formats**.**
- File viewer for viewing images and documents.
- EXIF data viewer for graphic files including search in EXIF data and adding EXIF data to reports.
- Special E-mail data viewer for viewing e-mail messages in different formats including viewing attachments.
- Special Chat RTF viewer for viewing chat history in a convenient format.
- Parsed data viewer for smartphone Application data.
- Extracted text viewer with a possibility of language selection for viewing results of optical character recognition.
- Content analysis results viewer for viewing whether a file has signs of malware and malware scan report.
- Advanced Analysis grid for filesystem evidence provides a wide range of filtering and searching options for quick data analysis.
- Data Triage.
- Timelines for a wide range of parsed registry keys.
- Mobile Data Triage.
- Adjustable font color and size.
- Bookmarking for easy navigation and review of data with a tree-view bookmarks structure.
- Organizing the bookmarked data by tags.
- Possibility to change time zone representation of date/time in evidence for easier comprehension.
- Opening data with external viewers.

HARD DRIVE FORENSICS

- **File System** plug-ins allow you to examine logical and physical disks as well as individual files and folders (local, network, and stored on CD/DVD) with:
  - FAT12, FAT16, FAT 32, FATX, exFAT
  - ExtX
  - HFS+
  - NTFS (including partition free space and file slack)
  - STFS

- **Disk images** from the most popular forensic imaging software are supported:
  - Paraben's Forensic Replicator (PFR)
  - Safeback 2-3
  - EnCase 4-5-6-7-8
  - RAW disk images (created in P2 Enterprise, Smart, FTK Imager, etc.)
  - FTK Imager by AccessData (E01 and AD1 formats)
  - Virtual PC Virtual HD image
  - VMware disk image
  - APFS disk images

- Creating RAW disk images of the remote and cloud machine data storages using E3 Remote Imager tool.

- **Memory dump files** are supported.

- The **Chat Database** plug-in supports many popular chat clients for viewing chat database contents in a convenient, color-coded format for easy analysis:
  - Viber
  - Yahoo!
  - Skype
  - ICQ
  - Miranda
  - Hello (Including Thumbnails)
  - Trillian
  - MSN and Windows Live messenger

- The **OLE Storages** plug-in supports the parsing and analysis of any OLE storage.

- The **Archive** plug-in supports many popular archive types including zip, jar, xpi, iso, chm, cab, msi, ppt, doc, xls, arj, bzip2, cpio, deb, gzip, lzh, msis, rpm, split, tar, z, wim, 7z, gz, and xz.

- The **E-mail** plug-in supports viewing multiple e-mail and network e-mail formats in a special e-mail data viewer (including support for exporting data to E-mail Examiner, EML [rfc822 compliant], Attachments only, MSG [OLE message], and PST [Outlook] e-mail formats).
  - Microsoft Exchange 5.0, 5.5, 2000, 2003 SP1, 2007, 2010, 2013, 2016, and 2019 (EDB)
  - Lotus Notes 4.0, 5.0, 6.0, 7.0, 8.0, 8.5 (ODS 43 and 51), 9.0.
  - Novell GroupWise up to 2012
  - Microsoft Outlook (PST) up to 2019
  - Microsoft Outlook (OST) 2013–2019
  - Microsoft Outlook (NST): Group Storage File automatically created in Microsoft Outlook 2016, 2013 and all versions below after configuration of Office 365 account in Outlook. The file stores the Groups conversations and other local Groups data.
  - Microsoft Outlook Express (EML)
  - E-mail Examiner (EMX)
  - AOL
  - The Bat! (3.x and higher)
  - Thunderbird
  - SeaMonkey
  - Windows Mail 11, 10, 8, 7, and XP
  - Google Takeout storage
  - Eudora
  - Maildir
  - Extracted Zimbra archives
  - MBOX

- The **Internet Data** plug-in supports the parsing and analysis of:
  - Basilisk history
  - Brave history, cookies, autofill items, keywords, logins, bookmarks, and backup bookmarks
  - Google Chrome history, cookies, autofill items, keywords, logins, bookmarks, and backup bookmarks
  - Microsoft Edge history, cookies, autofill items, keywords, logins, bookmarks, and backup bookmarks
  - Iceweasel history
  - Internet Explorer cache, cookies, and history
  - K-Meleon history
  - LibreWolf history
  - Mozilla Firefox cache and history
  - Opera history, cookies, autofill items, keywords, logins, bookmarks, and backup bookmarks
  - Pale Moon history
  - SeaMonkey history
  - Tor Browser history

  - Waterfox history
  - Yandex Browser history, cookies, autofill items, keywords, logins, bookmarks, and backup bookmarks

- The **SQLite** plug-in supports the parsing and analysis of SQLite databases including: *.db, *.Sqlite, *.Sqlite3, *.sqlitedb, *.db3, and others.

- The **Forensic Container** plug-in allows:

  - Creating a new Forensic Container
  - Adding an existing Forensic Container as evidence
  - Parsing the content of a Forensic Container as embedded data in the added file system evidence.

- The **Registry** plug-in allows analyzing exported registry hives and Windows Registry data on the images of system disks.

- Adding **social media backup** as evidence allows viewing and analyzing the user account data downloaded from the social media accounts such as:

  - Facebook Data Backup
  - Instagram Data Backup
  - Linkedin Data Backup
  - TikTok Data Backup
  - X (Twitter) Data Backup
  - Other Social media Backup

- Adding **Google Takeout evidence** allows viewing and analyzing the archive with Google services data generated and downloaded from a Google account.

- Import of **Google Takeout Archive** data allows viewing data from the archive in the parsed format.

- The **Compliance Archive** plug-in allows for analyzing archives obtained from legal sources during the investigation such as:

  - Facebook Compliance Archive
  - Instagram Compliance Archive
  - Linkedin Compliance Archive
  - Telegram Compliance Archive
  - TikTok Compliance Archive
  - X (Twitter) Compliance Archive
  - Other Compliance Archive

- The **separate file evidence** allows adding separate files as evidence and analyzing them or including them in the reports. This includes:
  - Documents
  - Graphics
  - Spreadsheets
  - Uncategorized files
- Import of **Lyft**, **LinkedIn**, **Ring Camera,** and **Uber Compliance Archives** allows viewing data in the parsed format.
- Import of Microsoft Exchange message tracking logs through **Logs & Artifacts Import Wizard** allows viewing and analyzing the obtained data.
- Import of **Volatility Framework textual outputs** allows analyzing Windows, macOS, and Linux memory dumps.
- [NEW] Import of **KAPE (Kroll Artifact Parser and Extractor)** archives with CSV files allows viewing and analyzing the obtained data.
- [NEW] Import of **IPED Digital Forensic Tool** output folder with results of disk image processing allows viewing and analyzing both the whole folder data or just the parsed CSV files.

MOBILE DATA FEATURES

- Logical imaging and physical imaging of a variety of mobile devices. More than 50 plug-ins for working with more than 25 types of devices including:
  - Cell/feature phones
  - Smartphones (iPhones, Androids, GrapheneOS, BlackBerry, Tizen)
  - Smartwatches (Androids and Tizen)
  - Windows Phones & Portable devices
  - PDAs
  - Tablets (iPads/iPod Touches and Android tablets)
  - Media Devices (iPods and eReaders)
  - GPS devices
  - Media cards
  - Acquisition of complete GSM and CDMA SIM card information including deleted data.
  - Device autodetection during acquisition.
  - Ability to create templates of feature sets and use them during Android device acquisition.
  - USB, serial, and Bluetooth (Limited) support
  - Deleted data recovery on all types of devices.
  - Full flash download for certain models of cell phones, PDAs, and smartphones

  - Encrypted image files to guarantee image integrity.
- A specialized Root Utility for advanced rooting of Android devices.
- Android ADB Downgrade feature.
- JTAG plugin for analyzing JTAG dumps and Chip Off dumps.
- Import of device-related desktop data:
  - RIM BlackBerry Backup (IPD & BBB) including BlackBerry 10
  - Apple iPhone Backup (including encrypted back-ups) with parsing of iOS keychain files.
  - KML and GPS maps
- Import of data from other tools
  - Cellebrite cases (Android filesystem dumps, iOS filesystem dumps, iPhone backups, and XML Reports)
  - GrayKey images and cases
  - Android Artifacts Analyzer (ALEAPP) and iOS Artifacts Analyzer (iLEAPP)
- Ability to view recorded GPS locations on Open Street maps.
- Data validation and protection:
  - Database-driven case format for secure data storage and large-volume storage
  - Verification of acquired case data integrity via acquired data hash code validation.
  - Case Comparer for comparing two databases to verify differences in their structure with bookmarks creation and quick reporting.
- SIM Cards cloner
- Cell Tower Import for viewing call locations.

INTERNET of THINGS-IoT

- Data acquisition of **smartwatches** from Android and Tizen
- Authentication Data capture for **Amazon Echo** devices
- Data acquisition of **Oculus/VR** devices
- Support of **smart home devices** from a variety of manufacturers
- Data analysis for **Fitbit** systems associated with Android and iOS devices.
- Support of **DJI Drone** data from both 3 and 4 versions
- Support of **trail cameras** through media acquisition
- Support of **smart toys** through App review
- The **Game Console** plug-in allows you to examine images of logical and physical disks with evidence from Xbox 360 including:
  - FATX filesystem used by Xbox.
  - STFS filesystem data intended to store packages created and downloaded by the Xbox.
  - XDBF databases containing gamer profile data.

CLOUD DATA FEATURES

- Support of data importing from cloud-based services:
  - Amazon Alexa
  - Discord
  - Dropbox
  - Facebook
  - Gmail
  - Google Drive
  - Google Locations
  - iCloud Backup
  - iCloud Contacts
  - iCloud Photos
  - Instagram
  - Skype
  - Slack
  - Steam
  - Teams Business
  - Twitch
  - Twitter

- **Live Cloud Collection** allows collecting data remotely using a provided link and then starting the cloud data import.
- Import of data from **Microsoft Office 365** allows getting the emails from the Outlook accounts using the admin credentials.

OSINT FEATURES

- Support of data importing from cloud-based services:
  - Facebook
  - Google Maps
  - Instagram
  - Twitter

ADVANCED DATA ANALYSIS

- The **Auto-Exam** option guides you through the process of evidence examination and does most things automatically without your interaction.
- The **Keyword Search** plug-in creates a keyword database for keyword searches:
  - Perform keyword indexing of any text data.
  - Quick keyword search in indexed data including multiple parameters for email evidence.
- The **Malware Scan** plug-in allows you to check if an executable file has the signs of malware.
- File sorting:
  - Sort binary files by their file type
  - Sort e-mail attachments
  - Sort recovered deleted data.
  - Analyze file type/file extension mismatch.
  - Analyze the sorted graphic files using the Thumbnails viewer.
- **Image Analyzer** for sorting images by potentially illicit categories (Alcohol, Chat, Currency, Documents, Drugs, Extremism, Gambling, Gore, ID_Credit Card, Map, Porn, QR_Barcode, Swim underwear, Tattoo, Vehicle, and Weapons). (Additional Licensing Required.)
- Deleted data recovery.
- Hash database features can manage and filter out common hashes (FOCH) including import of hash values from text files to Electronic Evidence Examiner hash databases for filtering out required files.
- SHA-256 calculation.
- Optical character recognition for images of the most popular formats.
- The skip list feature for e-mail databases and E3 data cases.
- Robust advanced searching and filtering options including multi-encoding support:
  - Search within e-mail attachments including search by attachment type.
  - Search for deleted data, unallocated disk space, file slack, etc.
  - Multi-parameter search for each type of data
  - Regular Expressions search
  - Ability to search for data without searching for its contents (file name/directory names)
  - Emoji and emoticons search
  - Multi-selection of search results for adding to a Search Results report.
  - Displaying matches for the quick review in the Search Results pane.

EXPORTING & REPORTING

- Multiple reporting options:
  - Mobile Data Review report provides mobile data in the most comprehensive format for forensic investigators.
  - Email Data Review report providing email data of certain email database in the most comprehensive format for forensic investigators.
  - HTML e-mail message report for mail archives analysis
  - Mobile data timeline report for analysis of mobile data evidence
  - HTML, PDF, CSV, TXT, RTF, and Excel reports for presenting data in the most usable format
  - Special malware report
  - Reports are compatible with **Paraben Zandra AI**
- Full customization of reports:
  - Possibility to add a custom logo, header, and footer.
  - Possibility to add Examination Summary and Examination Conclusion sections directly from the Electronic Evidence Examiner Interface
  - Investigator and case details sections in reports
  - Full customization of data to be added to the reports (select columns you want to see in the report)
  - Mobile Data Review report can be localized into Chinese, Spanish, Polish, and French
- Exporting:
  - Export any file in its native format.
  - Export multiple files from different folders/disks/evidence types
  - Export graphics and multimedia
  - Export graphics and multimedia while sorting data.
  - Export files/folders to forensic containers
  - Export mail storage contents to EML, EMX, PST, MHTML, and MSG formats
  - Export e-mail attachments in their native format
  - Export from search results and bookmarked data including multi-selection.
  - Batch export for e-mail databases
  - Export authentication data to the AuthData file, which can be used during cloud data import.
  - Logs & Artifacts Export allows exporting data detected in the Data Triage for future analysis in Microsoft excel. This includes exporting event log, jump lists, etc.
  - Cross Use export of E3 case data to E3-XML format for its further import to the third-party tools
  - [NEW] Export of E3 case data and filesystem data to the Relativity format (load file)
  - [NEW] Export of iOS and Android message grids to the Relativity Short Message Format (RSMF)
- An encrypted dynamic Forensic Container creation for storing exported data.