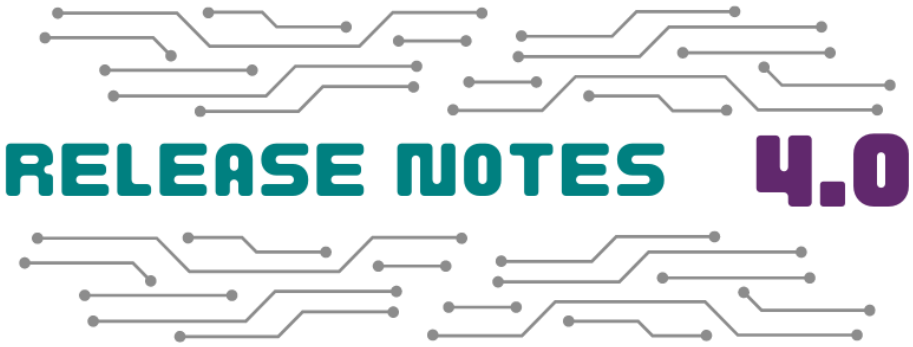
paraben® corporation

Electronic Evidence Examiner



Welcome to

paraben® corporation

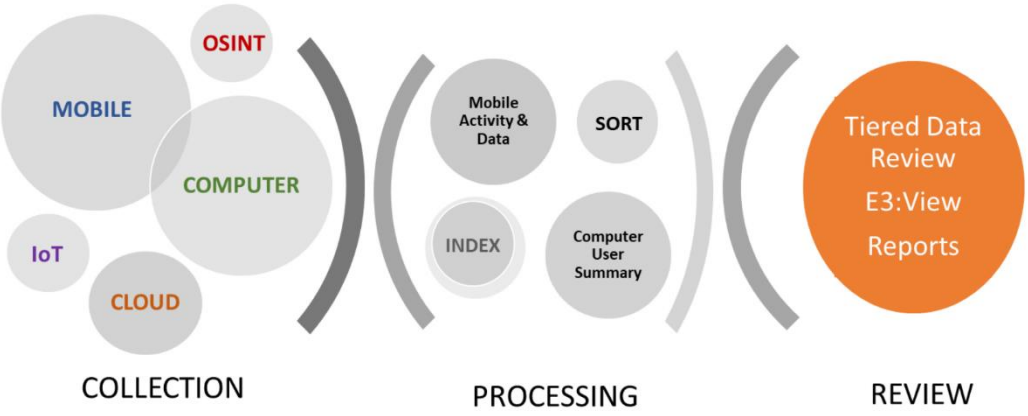
DILITHIUM EDITION 4.0

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 keen on 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 Trial Licenses

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 Computer Functionality

- An **Apple evidence category** has been added for easier access to all features for analyzing Apple data.
- New ability to analyze **APFS disk images** (.dmg) has been added.
- New types of evidence have been added to the **Compliance category** for easier access:
  - Facebook Compliance Archive
  - Instagram Compliance Archive
  - Linkedin Compliance Archive
  - Telegram Compliance Archive
  - TikTok Compliance Archive
  - X (Twitter) Compliance Archive
- New types of evidence have been added to the S**ocial Media category** for easier access:
  - Facebook Data Backup
  - Instagram Data Backup
  - Linkedin Data Backup
  - TikTok Data Backup
  - X (Twitter) Data Backup
- Parsing of **new categories during Google Takeout Archive data import** has been added. This includes**:**
  - Google Chrome History
  - Google Chrome Types URLs
  - Google Chrome Autofill
  - Google Chrome Autofill Profile
- Parsing of the **Location History (Timeline) during Google Takeout Archive data import** has been improved to match the latest Google changes.
- The **Messaging Apps Installation** timeline has been added to Data Triage. Now you can see installation dates for Discord, Facebook Messenger, Signal, Slack, Teams, Telegram, and Viber.

- New registry keys have been added to Data Triage:
  - **Recently Used File category:**
    - HKU\Software\Microsoft\Office\16.0\Access\Security\Trusted Documents\TrustRecords
    - HKU\Software\Microsoft\Office\16.0\Access\Security\Trusted Locations
    - HKU\Software\Microsoft\Office\16.0\Excel\Security\Trusted Documents\TrustRecords
    - HKU\Software\Microsoft\Office\16.0\Excel\Security\Trusted Locations
    - HKU\Software\Microsoft\Office\16.0\PowerPoint\Security\Trusted Documents\TrustRecords
    - HKU\Software\Microsoft\Office\16.0\PowerPoint\Security\Trusted Location
    - HKU\Software\Microsoft\Office\16.0\Word\Security\Trusted Documents\TrustRecords
    - HKU\Software\Microsoft\Office\16.0\Word\Security\Trusted Locations
    - HKU\Software\Microsoft\Office\16.0\OneNote\OpenNotebooks
    - HKU\Software\Microsoft\Office\16.0\Publisher\User MRU
    - HKU\Software\Microsoft\Windows\CurrentVersion\Applets\Paint\Recent File ListHKU\Software\Microsoft\Office\16.0\Publisher\File MRU
    - HKU\Software\Microsoft\Windows\CurrentVersion\Applets\WordPad\Recent File List
  - **Users account**
    - HKU\Software\Microsoft\Office\Common\UserInfo
    - HKU\Software\Microsoft\OneDrive\Accounts
    - HKU\Software\SyncEngines\Providers\OneDrive\

E3 Mobile Functionality

- **Voicemail transcription obtaining** is implemented for iOS device acquisition and iOS backup import.
- **State of Mind** parsing for the native iOS Health application has been added.
- Import of **Cellebrite UFED Android** data has been added.
- **Wal files obtaining** is improved for iOS device acquisition and iOS backup import.
- **Deleted messages recovery** during for iOS device acquisition and iOS backup import has been improved.
- Work with **large message grids (more than 10,000 messages)** acquired/imported from iOS-based devices and backups has been improved.

E3 Supported Device Profiles

39,255+ SUPPORTED

E3 Cloud Functionality

- Import of **iCloud Contacts** has been added.
- A new **Paraben's E3 Google Authenticator utility** is now available. It allows obtaining Google authenticator tokens for investigated accounts both protected and not protected with two-factor authentication. Obtained tokens can be used for importing data from Google services.

GENERAL/UI FEATURES

- The product workflow has been updated.
- The Document viewer has been updated that includes the following changes:
  - Support of viewing new file formats:
    - Microsoft Excel 97-2003 Template (.xlt)
    - Excel 2003 XML file (SpreadsheetML) (.xml)
    - Plotter Document (.plt, .hpg)
    - OpenDocument Flat XML Graphics (.fodg)
    - OpenDocument Flat XML Presentation files (.fodp)
    - IGES Drawing File (.igs)
    - Common File Format (.cf2)
    - Wavefront 3D Object File (.obj)
    - Microsoft Project files with notes
    - Apple numbers (.numbers)
    - WinRAR Compressed Archive (.rar)
    - SVGZ (Compressed SVG)
    - Adobe Photoshop Large Document Format (.psb)
    - Compressed Windows Metafile (.wmz)
    - Windows Compressed Enhanced Metafile (.emz)
    - Corel Presentation Exchange Image (.cmx)
    - CorelDRAW Image (.cdr)
    - RAR5 archive
    - AI (Adobe Illustrator Artwork)
    - CHM (Microsoft Compiled HTML Help)
    - Truevision TGA (TARGA) (tga)
    - Animated PNG (apng)
    - TAR GZipped (TGZ)
    - TAR XZipped (TXZ)
    - XZipped (XZ)
    - Power shell script (.PS1)
    - Power shell script module (.PSM1)
    - Power shell script module manifest (.PSD1)
    - Lossless JPEG (JLS)
    - Unix CPIO Archive (.CPIO)
    - Design Web Format XPS File (.dwfx)
    - Autodesk FBX Interchange File (.FBX)
    - Amazon AZW3/KF8 ebook (.azw3)
  - Numerous improvements in displaying other file formats:
    - Support for printer configuration files (PC3 files) when rendering CAD formats
    - Support for rendering VCF files with multiple contacts

        - Support for rendering QR-codes in Word files
        - Support for rendering presentations that contain shapes and text with 3D effects
        - Support for multi-paged Dicom files
        - Getting sheet names from an Excel file
        - Rendering spreadsheets similar to Excel (by page breaks) by default
        - Support of file format detection for passed stream
        - Rendering text files into a single HTML page
        - Ability to render shapes used in a Visio diagram rather than the diagram itself
        - Syntax highlight to programming language formats
        - Rendering PSD files with custom fonts
        - Support of text gradient for DOCX files
        - Setting page size and margins when rendering Web documents
        - Autodetect of the text file encoding
        - Support for PDF file optimizations
    - Performance optimization
    - Numerous minor issues fixes and minor improvements.
- File type detection has been improved to correctly detect more data types, such as IFC CAD files.

SECURITY

- The **7-zip library** has been updated to avoid having potential vulnerabilities in the product. It is strictly recommended to update to this version of Electronic Evidence Examiner.

RESOLVED ISSUES

- An issue with **viewing folders with a single file** in different types of evidence (archive, social media backup, compliance archive, etc.) has been fixed.
- Potential problems with authentication during **iCloud Photos import** have been fixed.
- Potential problems with **Teams Business Cloud** import have been fixed.
- Potential problems with authentication during **Office 365 data import** have been fixed.

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
  - [NEW!] 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 [NEW!] 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:

  - [NEW!] Facebook Data Backup
  - [NEW!] Instagram Data Backup
  - [NEW!] Linkedin Data Backup
  - [NEW!] TikTok Data Backup
  - [NEW!] 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:

  - [NEW!] Facebook Compliance Archive
  - [NEW!] Instagram Compliance Archive
  - [NEW!] Linkedin Compliance Archive
  - [NEW!] Telegram Compliance Archive
  - [NEW!] TikTok Compliance Archive
  - [NEW!] X (Twitter) Compliance Archive
  - Other Compliance Archive

- Import of **Rng Camera Compliance Archive** allows viewing data in the parsed format.

- Import of logs using **Logs & Artifacts Import Wizard** allows getting information about Microsoft Exchange message tracking logs.

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 ([NEW!] Android filesystem dumps, iPhone backups and XML Reports only)
  - GrayKey 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
- Data analysis for **Fitbit** systems associated with Android and iOS devices.
- Support of **DJI Drone** data from both 3 and 4 versions
- 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
  - [NEW!] iCloud Contacts
  - iCloud Photos
  - Instagram
  - Skype
  - Slack
  - 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
- 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
- An encrypted dynamic Forensic Container creation for storing exported data.