Paraben's
ELECTRONIC EVIDENCE EXAMINER

RELEASE NOTES

Bronze Edition 2.4

Welcome to Paraben's Electronic Evidence Examiner

Bronze Edition 2.4

Paraben's Electronic Evidence Examiner—E3 is a comprehensive digital forensic platform designed to handle more data, more efficiently while adhering to Paraben's paradigm of specialized focus of the entire forensic exam process. The E3 Platform is broken into a variety of different licensing options. From the E3:UNIVERSAL version that is designed to do all data types from hard drive data, smartphones, and IoT data. **All boundaries that used to exist for digital evidence have been broken with this one universal tool.**

The E3 Platform utilizes Paraben's advanced plug-in architecture to create specialized engines that examine elements like e-mail, network e-mail, chat logs, mobile data, file systems, Internet file analysis, smartphones, and more – all while increasing the amount of data that can be processed and utilizing resources through multi-threading and task scheduling.

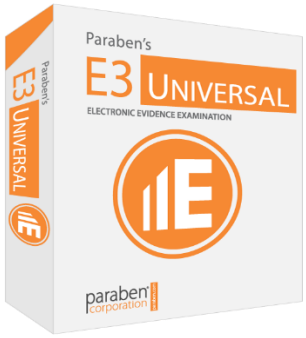
Depending on the licensing option selected the E3 Platform comes with coordinating items. P2X Pro and DP2C are included with E3:Universal and E3:P2C. The E3 Mobile Toolbox which is a hardware kit that includes all the common cables required for processing devices as well as other accessories used in forensics analysis that is included with E3:Universal and E3:DS. No matter which option is selected we have you covered with comprehensive support.

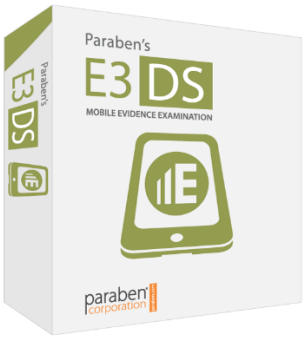
Trials and Subscriptions

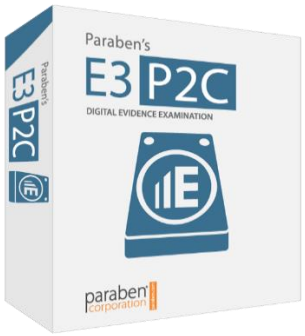
If you are interested in a trial version of the E3 Platform you simply need to ask. We are happy to set you up with a fully functional trial to be able to utilize and test all of the features simply email us at trial@paraben.com and we will start you in the trial process.

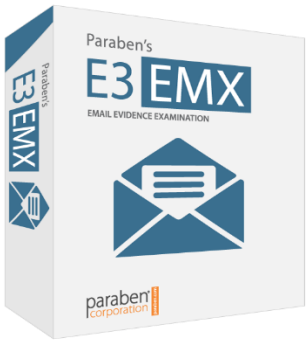
For subscriptions, you can contact sales@paraben.com to make sure your subscription is current and receive a quote to continue support. Paraben maintains the most cost friendly subscription costs for its customers with the most features.

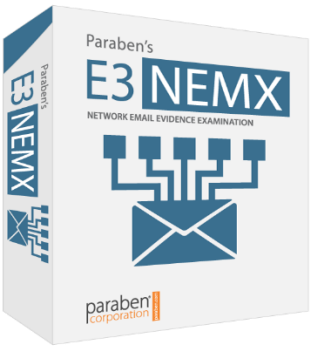
E3 Platform License Options











What's New in E3 Platform Bronze Edition 2.4

Hard Drive Forensics Features:

- **Social media backup evidence** is available for adding to E3 now. A social media backup is an archive with the user account data generated and downloaded directly from the social media accounts, for example, from Facebook, Twitter, Snapchat, etc. Watch for new mini-book about how to capture this data.
- New **Windows 10 registry keys** and values have been added to the existing and new categories of the Data Triage.
- Microsoft **Outlook Group Storage Files (.nst)** associated with Office365 are supported now.
- Potential issue with the disk images parsing has been fixed.
- Potential issue with E3 crash during the content analysis of OST mailstorage evidence has been fixed.
- Possible issue with out of memory crash during the generation of report containing the Data Triage data has been fixed.

Mobile Data Acquisition/Parsing Changes:

- The ability to **acquire multiple devices simultaneously** has been added. Now you can drastically reduce your time spent for successive acquisition of devices as this feature allows you to acquire different devices in different combinations at one time, regardless of their type and number. The number of devices is only limited by the connections available by the direct ports of the machine.
- New **Android Qualcomm EDL (physical)** plug-in is available now. It can be used for physical acquisition of devices with Qualcomm processors being put into the EDL mode. Full bypass of encryption of the device is available with this option.
- Support of **iOS 13** has been added.
- Support of **Android 10** has been added.
- Potential issue with SMS acquisition from Android devices has been fixed.
- Potential issue with SMS parsing in imported BlackBerry 10 backups has been fixed.
- Potential issue with obtaining the authentication data during physical acquisition of Android devices has been fixed.

General Changes:

- Possibility to change the image size in the Thumbnails viewer has been added.
- Link to the Paraben's YouTube channel is available now in E3. Watch our step-by-step video instructions aimed at facilitating your work with E3. Note that collection of video records is constantly growing.

Supported device profiles is constantly growing and expanding. Please email us at forensics@paraben.com for the latest available list at any time.

Supported Device Profiles Total:	35,725+

Electronic Evidence Examiner Key Features

GENERAL FEATURES

- Full Windows 10 compatibility, including UAC and digital signature by Microsoft
- x86 and x64 versions
- Back-end Firebird database for support of massive amounts of data
- Multi-threading and task scheduling capabilities to process more data in less time
- [NEW!] Acquisition of multiple devices simultaneously
- Convenient plug-in architecture
- Easy-to-use registration scheme including a web-based licensing method that allows using the application on any computer without the dongle!
- Ability to save a case along with its Keyword Indexing database and attached evidence file to single archive from the program interface.
- Single interface for all types of digital evidence.

GUI FEATURES

- File viewers for popular file formats.
- 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.
- Data Triage.
- Mobile Data Triage.
- Adjustable font color and size.
- Bookmarking for easy navigation and review of data with a tree-view bookmarks structure.
- 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
  - 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
  - RAW disk images (created in P2 Enterprise, Smart, etc.)
  - Virtual PC Virtual HD image
  - VMware disk image
- Memory dump files are supported.

- 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
  - [NEW!] 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
  - Windows Mail 10, 8, 7, and XP
  - Google Takeout storage
  - Eudora
  - Maildir
  - Extracted Zimbra archives

- The **Chat Database** plug-in supports many popular chat clients for viewing chat database contents in a convenient, color-coded format for easy analysis:
  - 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, and 7z.

- The **Internet Data** plug-in supports the parsing and analysis of:
  - Mozilla Firefox cache and history
  - Internet Explorer cache, cookies, and history
  - Google Chrome history, cookies, auto fill items, keywords, logins, and 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.

- Import of data from **Microsoft Office 365** allows getting the emails from the Outlook accounts using the admin credentials.

- [NEW!] Adding **social media backup** as evidence allows viewing and analyzing the user account data downloaded from the social media accounts.

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, BlackBerry, and Tizens)
        - Smartwatches (Androids and Tizens)
        - 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
    - 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.
- 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 (XML only)
    - GrayKey cases
- Support of data acquisition from cloud-based services:
    - Facebook
    - Gmail
    - Google Drive
    - Google Locations
    - iCloud Backup
    - Twitter
    - Amazon Alexa
- 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 & Tizen
- Authentication Data capture for **Amazon Echo** devices
- Data analysis for **Fitbit** systems associated with Android & 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.

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 keywords database for keywords searches:
    - Perform keywords indexing of any text data
    - Quick keywords 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 (Drugs, Gore, Porn, Swim underwear, Extremism, 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 most popular formats.
- Robust advanced searching and filtering options including multi-encoding support:

- Search within e-mail attachments including search by attachments type
- Search in 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)
- 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 providing data in the most comprehensive format for forensic investigators
  - E-mail messages 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 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 & multimedia
  - Export graphics & 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 GPS data to MapLink
  - Export from search results and bookmarked data including multi-selection
  - Batch export for e-mail databases
- An encrypted dynamic Forensic Container creation for storing exported data.