exterro®
Legal GRC Software

FTK SUITE 7.6 SP5 - RELEASE NOTES

DECEMBER 2023

Table of Contents

Overview

Exterro was founded with the simple vision that applying the concepts of process optimization and data science to how companies manage digital information and respond to litigation would drive more successful outcomes at a lower cost. We remain committed to this vision today. We deliver a fully integrated Legal GRC platform that enables our clients to address their privacy, regulatory, compliance, digital forensics, and litigation risks more effectively and at lower costs. We provide software solutions that help some of the world's largest organizations, law enforcement and government agencies work smarter, more efficiently, and support the Rule of Law.

1 What's New

Enhancements

FTK Portable Cases

1. Upon applying any filters to the item list in the FTK Portable Case, the count of the associated filters will be updated dynamically in the 'Filters' panel. *(FCR-16353)*
2. FTK Portable Case is enhanced to display the File icons in the 'File Type' column. *(FCR-17726)*
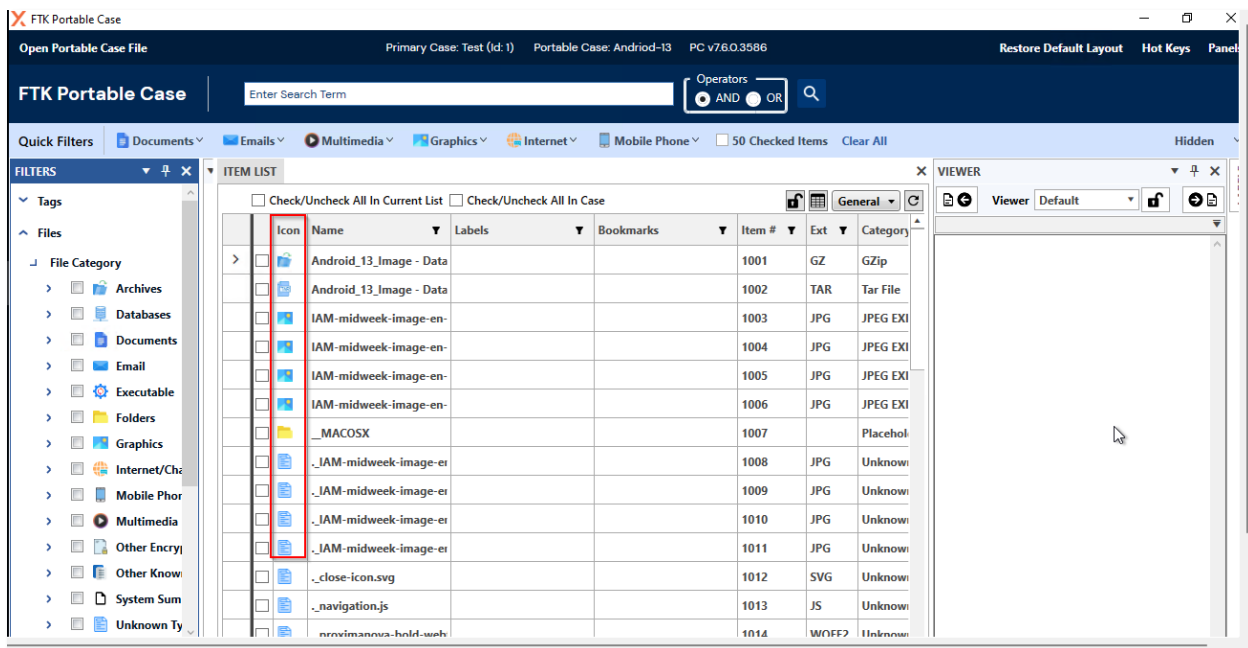
3. FTK Portable Case is enhanced to check and install the required prerequisites automatically. *(FCR-16833)*

Reporting

1. You are provisioned with the option to export the files present in the Portable Cases into XLS format. To perform the operation, select the required files from the Item List, right-click on it, and select the newly introduced 'Create Hyperlink Report' option. *(FCR-23419)*

Filtering

1. A new panel, 'Filters' is introduced in the Portable Cases to filter the files using the predefined set of filter options available in the panel. *(FCR-13887)*
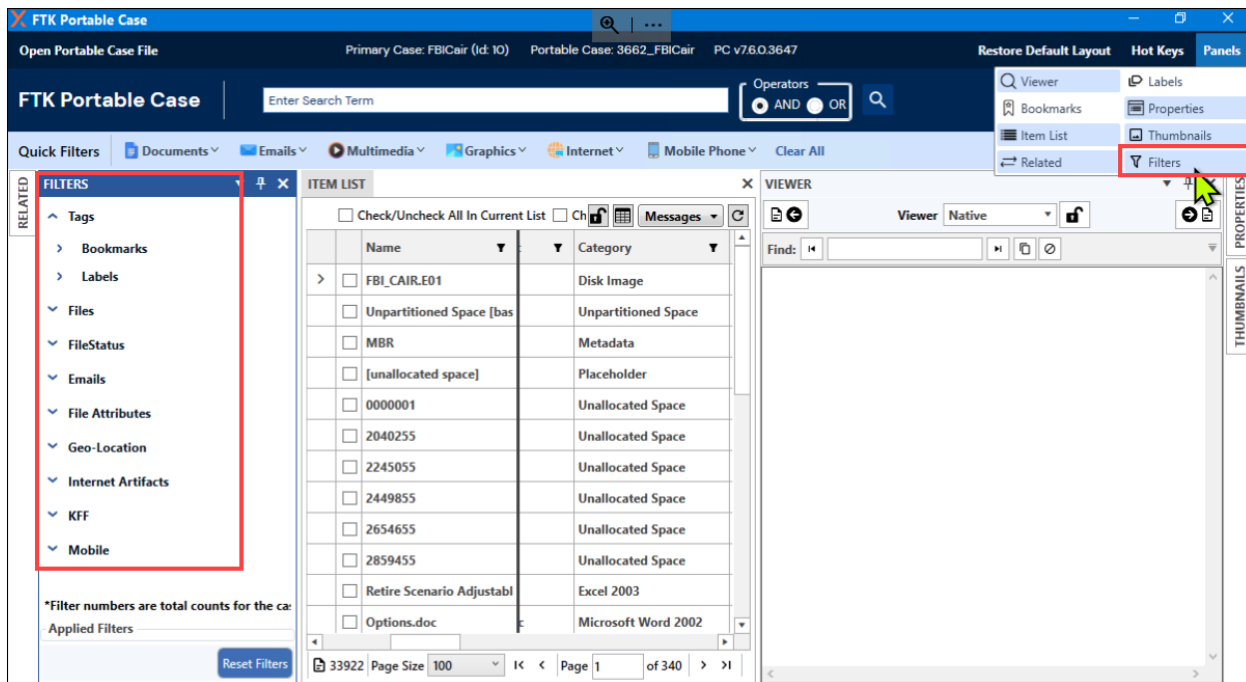
2. The following column options are newly introduced in the Item List of Portable Case: *(FCR-13655)*

- Auto Column - To automatically add/remove the columns displayed in the Item List to match the file types selected.

- Custom Column – To create customized column templates.

Search Functionalities

1. 'Create Searchable Index' and 'Index Binary' options are newly introduced on the 'Portable Case' and 'Sub Portable Case' pop-up windows for you to specifically search the information in portable and sub portable case items. *(FCR-17303) (FCR-14783)*

   Note: The corresponding subportablecasecreation.log will also have these details.

2. The search operation speed in the Portable Case is improved. *(FCR-12605)*
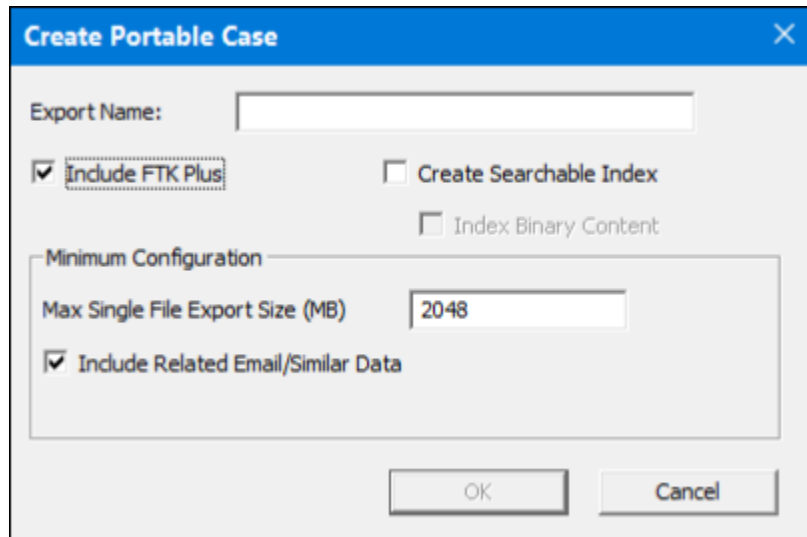
Smart View

1. You are now provisioned with an option to perform bulk delete files. To do so, you can select multiple files on the Review page > right-click> click on Delete. *(FTKC-26453)*

Reporting

1. The fields with empty or null values will no longer be displayed in the 'Detail Report' of Smart View. *(FTKC-32548)*

   Note: The system will not exclude the empty chat messages and the document files.

Other Enhancement

1. FTK is enhanced to parse the Volume Serial Number (VSN) of USB devices from event logs. *(FCR-15390)*

Site Server and Agents

1. FTK is enhanced to automatically restart the Agents when it fails to connect to a Public Site Server. *(FCR-15665)* *(ER-13483)*

   - If a Public Site Server and the 'retry_failed_attempt' parameter is passed, an agent will restart automatically once it fails to connect to a Public Site Server after a configured amount of attempts.

   Note: Refer to the Manually Installing the Windows Enterprise Agent article for more information.

2. Exterro FTK is enhanced to record the logs (with detailed information) for every successful or failed check-in made to a Public Site Servers. *(FCR-15420)*

3. FTK Enterprise includes support for DoD STIG Compliance, allowing seamless installation and configuration of our Linux agent in alignment with DoD security standards. *(FCR-15989)*
   Note: DISA is part of the Department of Defense (DoD) which includes the Security Technical Implementation Guide (STIG) guidelines and outlines how an organization should handle and manage the security software and systems (for organizing, delivering, and managing the defense-related information).

Connectors

1. Exterro FTK application now uses the 'Connect-ExchangeOnline' PowerShell cmdlet instead of Microsoft's now-deprecated 'New-PSSession' cmdlet for O365 Export-based collection. This is applicable to Microsoft Exchange Online, Microsoft SharePoint Online, Microsoft OneDrive, and Microsoft Teams data sources. *(ER-14213)*
   Note: The 'ExchangeOnlineManagement' module should be installed in the Exterro Server to avail this upgrade.

2 Resolved Issues

FTK Plus

1. Resolved an issue where users were not able to generate a PDF report consisting of more than 5,000 records. *(QR-5193) (QR-4920)*

2. Resolved an issue where all users in the application were displayed while selecting users for the Event Audit Log Report instead of displaying only the users associated with the case. *(QR-4957)*

3. Resolved an issue where the Chat conversation attachments in MP4 file format were not embedded into the corresponding Details Report generated as PDF or DOCX/DOC (Microsoft Word) format. *(QR-4921) (QR-4915)*

4. Resolved an issue where a non-admin user was able to view the 'Evidence Item' details of a case from the 'Job Status' section. *(QR-4791)*

5. Resolved an issue where the filters applied from the 'Filter' panel were reflected in the 'Item List' only after manually refreshing the 'Item List' panel. *(QR-4650)*

6. Resolved an issue where the audit log report generated from FTK Plus consisted of all the information regardless of all the filter configurations made in the 'Event Audit Log' pop-up. *(QR-4827)*

7. Resolved an issue where no files or folders were displayed upon clicking on the 'Browse' button against the 'Report Path' field during Report creation. *(QR-4919)*

8. Resolved an issue where users were not able to download the reports generated in DOCX/DOC (Microsoft Word) format when the value for 'PDFTRONDOCX' configuration key was set as 'true' in the ADG config file. *(QR-4822)*

9. Resolved an issue where some folders of a report intended to be generated in a custom location were stored in the below path: *(QR-4655)*

    <casepath>\FTK_Reports\<reportname>\<jobid_reportname>

10. Resolved an issue where the 'Word' option was not displayed in the 'Report Format' drop-down field while creating a report. *(QR-4475)*

FTK Central

1. Resolved an issue where the machines with Agents were woken from Sleep automatically after 2 minutes. This issue occurred even when the machine was manually forced into sleep mode. *(FTKC-23090)*
2. Resolved an issue where the automatically created temporary folder was not automatically deleted upon successful completion of Agent Collection jobs. This issue occurred only for the collections enabled with the 'Create AD1 on agent' Advance option. *(ER-13631)*
3. Resolved an issue where the MAMA (periodic connection check) was not working appropriately for Linux OS agents. *(ER-13434)*
4. Resolved an issue where the FTK Enterprise application crashed when a non-administrator tried to open a case created in FTK Central. *(FTKC-30120)*
5. Resolved an issue where the users were not able to use the Gmail 'Service account API Key' for GDrive 'Service account API Key' and vice versa. *(ER-12618)*
6. Resolved an issue where the users were not able to edit the custom case properties. *(FTKC-25304)*
7. Resolved an issue where the viewer opened in the 'Pop Out' mode was not updated when a file was selected from the 'Email Conversation' pane. *(FTKC-30081)*
8. Resolved an issue where the users were not able to view the details of a Collection created via Enterprise API for 'Full Disk' acquisition. *(FTKC-32128)*
9. Resolved an issue where the users were not able to execute the Additional Analysis (AA) job when all the default 'Quick Filters' were disabled. *(FTKC-32647)*
10. Resolved a sporadic issue where incorrect search results were displayed. *(FTKC-29594)*
11. Resolved a sporadic issue where the Exchange EWS Collection failed due to an error. *(ER-13541)*
12. PDF Conversions and Migrations from Summation Pro to FTK Central have been improved. *(FTKC-20583)*
13. Resolved an issue where the collection of data from Network Share failed when the provided path exceeded 250 characters. *(ER-13360)*
14. Resolved an issue where the creation of a DAT type load file for an export was being processed indefinitely. *(FTKC-24450)*
15. Resolved an issue where users with the 'View Tags' and 'Assign Tags' roles were not able to view or access the coding panel. *(FTKC-23085)*

FTK Portable Case

1. Resolved an issue where the scroll bar of the 'Applied Filters' section was disabled in the FTK Portable Case upon applying multiple filters. **(FCR-17557)**

2. Resolved an issue where the cancellation of FTK Portable Case job took a longer time than expected. **(FCR-17172)**

3. Resolved an issue where the 'Reports Options' pop-up was not closed automatically upon generating a report either in Portable Case or HTML format. *(FCR-16826)*

4. Resolved an issue where the users were not able to index the graphic files via Exterro FTK Portable Cases. *(FCR-12796)*

5. Resolved an issue where users were not able to perform 'Exclusion' for the 'Web Page Category' filters (under 'Internet Artifacts') in the FTK Portable Case. *(FCR-19684)*

6. Resolved an issue where the 'Select All' and 'Clear All' buttons were not displayed in the 'Evidence Refinement (Advanced)' section in the 'Detailed Options' pop-up of Exterro FTK Portable Case. *(FCR-11033)*

FTK Enterprise

1. Resolved an issue where the evidence locations were not marked on the Maps in the 'Geo Location' window of the FTK application. *(FCR-8551)*

2. Resolved an issue where the following categories were not displayed in the 'System Summary' tab for the evidence processed using the 'Field mode' processing profile: *(FCR-23418)*
   - Desktop Item
   - MUICache Information

3. Resolved an issue where some of the categories were not displayed in the 'System Summary' tab for the Mac evidence processed using the 'Field mode' processing profile. *(FCR-23405)*

4. Resolved an issue where the Shellbags information was not parsed from the AD1 file collected via FTK Imager with the 'Obtain Protected Registry Files' option enabled. *(FCR-21282)*

5. Resolved an issue where Email Archive files that were marked as indexed were not producing search results. *(FCR-17896)*

6. Resolved an issue where the iMessages from Apple File System (APFS) were not displayed as expected. *(FCR-16888)*

7. Resolved an issue where the 'Evidence' filter was displayed only after reopening a case. *(FCR-12381)*

8. Resolved an issue where some of the HTML tables were duplicated in the viewer upon setting the Scaling and Layout percentage (%) more than 125. *(FCR-2049)*

9. Resolved a sporadic issue where the importing of memory dump failed in FTK Enterprise. *(FCR-15463)*

10. Resolved an issue where the CPU utilization was higher than expected while using the KFF functionality with more than a million Hash sets. *(FCR-15712)*

11. Resolved an issue where the users were not able to decrypt the Apple File System (APFS) drive. *(FCR-16964)*

12. Resolved an issue where the FTK Lab application's response was slow in anthe Active Directory environment. *(FCR-16017)*

13. Resolved an issue where the FTK application was not able to collect the files consisting of International characters from macOS Ventura. *(FCR-14728)*

14. Resolved an issue where the Memory Analysis failed on the below mentioned versions of Windows: *(FCR-15453)*
    - Microsoft Windows 10 (20H2, 21H2, 22H2)
    - Microsoft Server 2019
    - Microsoft Server 2016
    - Microsoft Windows 11 (22H2)

15. Resolved an issue where the FTK application was not able to recognize multiple partitions of Bitlocker produced images. *(FCR-20716)*

16. Resolved an issue where the system was not able to recognize the Bitlocker's primary partition upon loading an .E01 image that was captured using FTK Imager. *(FCR-19709)*

17. Resolved an issue where the Temp Drive was running out of disk space and the RAM utilization was more than 90% upon running an AA job on a case. *(FCR-18879)*

3 Open Issues

General

1. Exterro Mobile Parsers options are not selected by default for the profiles created with the below obsolete categories of Android, Blackberry, and iOS: *(FTKC-13436)*

   - Android Application
   - Android calendar
   - Android Hangouts
   - Android Gmail
   - Blackberry IPD backup file
   - iOS WeChat
   - iOS WhatsApp

Portable Case

1. Total file counts within Portable Case sporadically become out of sync with files within the file list. *(FCR-20917)*

FTK Central

1. The values for the 'File Count' and the 'Hits' columns are updated as '0' for the collections enabled with the 'Collect Specific Sectors' option. This issue is applicable only to the collection initiated for 'Computers' data sources. *(ER-13273)*

Contact Exterro

If you have any questions, please refer to this document, or any other related materials provided to you by Exterro. For usage questions, please check with your organization's internal application administrator. Alternatively, you may contact your Exterro Training Manager or other Exterro account contact directly.

For technical difficulties, support is available through support@exterro.com.

Contact:

Exterro, Inc.

2175 NW Raleigh St., Suite 400

Portland, OR 97210.

Telephone: 503-501-5100

Toll Free: 1-877-EXTERRO (1-877-398-3776)

Fax: 1-866-408-7310

General E-mail:info@exterro.com

Website: www.exterro.com