FORENSIC

Legal Informatics and Multimedia

Forensic Analysis for Computer Systems

Plan of the Labs:

1. Electronic data acquisition
2. Computer Forensics technics and tools
3. Volatility Framework
4. Autopsy (Sleuthkit)
5. FTK (Forensic ToolKit)
6. Guidance software EnCase & ProDiscover Forensic

Course Lab5: FTK (Forensic ToolKit) Imager

5.1 FTK Imager for data preview and imaging

5.2 From FTK Imager to FTK ToolKit

5.3 FTK ToolKit Features

exterro®

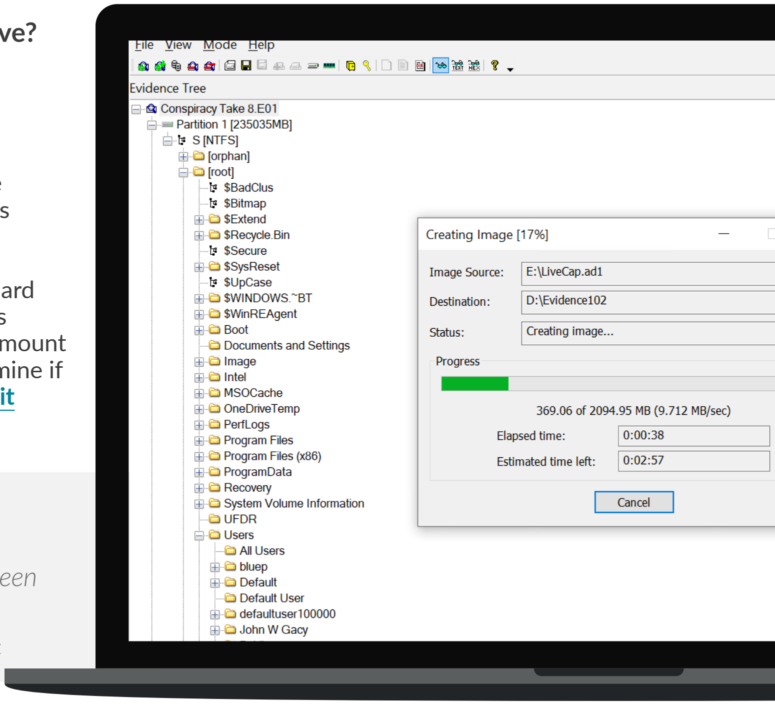
FTK® IMAGER FOR DATA PREVIEW & IMAGING

Quickly assess electronic evidence, create forensic images, and generate hash reports

Need a quick way to see what data is on a computer hard drive? Join the thousands of forensic professionals worldwide who trust FTK Imager as their go-to solution for the first step in investigating an electronic device.

FTK Imager is a FREE data preview and imaging tool used to acquire electronic evidence in a forensically sound manner by creating copies of computer data without making changes to the original evidence.

With **FTK Imager** you can create forensic images of local (physical) hard drives, CDs and DVDs, thumb drives or other USB devices, as well as preview entire folders or individual files, generate hash reports, and mount images. FTK Imager helps you evaluate computer evidence to determine if further analysis with a forensic tool such as the FTK® Forensic Toolkit is warranted.



```
Conspiracy Take 8.E01
  Partition 1 [235035MB]
    S [NTFS]
      [orphan]
      [root]
        $BadClus
        $Bitmap
        $Extend
        $Recycle.Bin
        $Secure
        $SysReset
        $UpCase
        $WINDOWS.~BT
        $WinREAgent
        Boot
        Documents and Settings
        Image
        Intel
        MSOCache
        OneDriveTemp
        PerfLogs
        Program Files
        Program Files (x86)
        ProgramData
        Recovery
        System Volume Information
        UFDR
        Users
          All Users
          bluep
          Default
          Default User
          defaultuser100000
          John W Gacy
```

Creating Image [17%]

Image Source: E:\LiveCap.ad1

Destination: D:\Evidence102

Status: Creating image...

Progress

369.06 of 2094.95 MB (9.712 MB/sec)

Elapsed time: 0:00:38

Estimated time left: 0:02:57

> *"I've used FTK Imager for nearly 20 years. Imager has always been a dependable imaging tool but the recent improvements in speed are really outstanding. We've seen the time to image a device cut in half! Great work!"*
>
> —**Tom Angle**, forensic consultant for federal law enforcement

Selected Features

Data Imaging

FTK Imager can create perfect copies, also known as forensic images, of computer data without making changes to the original evidence. The forensic image is identical in every way to the original, including file slack and unallocated space or drive free space. This allows you to store the original media safe from harm or tampering while the investigation proceeds using the image.

The newest version of **FTK Imager** also includes significant speed improvements in image creation—the time to image a device has been cut in half! To achieve this speed increase, we optimized the method we use to preserve the forensic image. The faster you preserve the data, the quicker analysis can begin.

Custom Content Images

Create a custom content image of your dataset where you select only the data you want to image, in order to reduce the size of your dataset, thereby making your investigation more efficient yet still forensically sound. You can manually add files or directories to your custom image, or use wildcard search criteria to select files.

Data Preview

Preview the contents of forensic images stored on the local machine or on a network drive. You can preview files and folders on local hard drives, network drives, CDs and DVDs, thumb drives or other USB devices.

Hash Reports

Generate hash reports for regular files and disk images (including files inside disk images) that you can later use as a benchmark to prove the integrity of your case evidence. When a full drive is imaged, a hash generated by **FTK Imager** can be used to verify that the image and the original drive are identical and that the image has remained unchanged since acquisition. You can use either of the two leading hash functions available in **FTK Imager:** Message Digest 5 (MD5) and Secure Hash Algorithm (SHA-1).

Image Mounting

Mount an image for a read-only view that leverages Windows® File Explorer to see the content of the image exactly as the user saw it on the original drive. See and recover files that have been deleted from the Recycle Bin, but have not yet been overwritten on the drive. You can also run a virus scan on a mounted image, or run a Python script against mounted image files to easily show a jury how a user would have seen their own files and folder structure.

RAM Capture

FTK Imager allows you to perform memory capture or registry capture on a live device, allowing you to recover passwords or other data stored in memory on the active device.

Exporting

FTK Imager can write and read all of the most common forensic image formats, making it easy to continue your forensic analysis and review in whatever tool you use in your workflow, including the full-featured FTK Forensic Toolkit. You can also export individual files and folders from forensic images, including recovered deleted files in their native formats, or export into another forensic image as an AD1 file.

Whether you're imaging a drive, viewing an image, or triaging a live machine, FTK Imager has you covered!

10 REASONS WHY YOU SHOULD UPGRADE FROM IMAGER *to* FTK®

While FTK Imager excels at electronic device imaging, its analysis and review capabilities are limited. Count on the full-featured FTK Forensic Toolkit to complete your workflow.

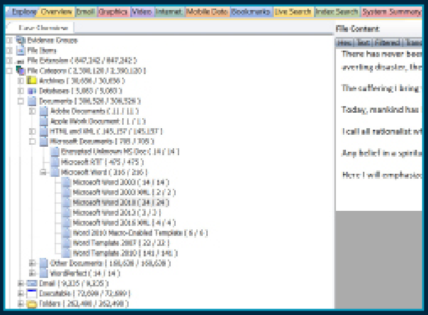
*What can **FTK** do that **FTK Imager** can't do? Read on for 10 core forensic analysis and review tasks you're going to want to perform in FTK:*

Manual Navigation

FTK's File Categorization & Overview Tab

SEE IT IN ACTION

In **FTK Imager** you can load an image and search for files, but it's a manual process to navigate through files individually or by directory. By contrast, **FTK's** Overview Tab categorizes all the files on the disk automatically. The File Category section breaks up files into categories like documents, emails, spreadsheets, executables, registry files, deleted files, or files with bad extensions–they're all automatically categorized, ready for you to analyze, bookmark, save, label, or export.



```
Evidence Groups
File Items
File Extension ( 847,242 / 847,242 )
File Category ( 2,390,120 / 2,390,120 )
  Archives ( 30,656 / 30,656 )
  Databases ( 5,083 / 5,083 )
  Documents ( 506,526 / 506,526 )
    Adobe Documents ( 11 / 11 )
    Apple iWork Document ( 1 / 1 )
    HTML and XML ( 145,157 / 145,157 )
    Microsoft Documents ( 785 / 785 )
      Encrypted Unknown MS Doc ( 14 / 14 )
      Microsoft RTF ( 475 / 475 )
      Microsoft Word ( 216 / 216 )
        Microsoft Word 2000 ( 14 / 14 )
        Microsoft Word 2003 XML ( 2 / 2 )
        Microsoft Word 2010 ( 24 / 24 )
        Microsoft Word 2013 ( 3 / 3 )
        Microsoft Word 2016 XML ( 4 / 4 )
        Word 2010 Macro-Enabled Template ( 6 / 6 )
        Word Template 2007 ( 22 / 22 )
        Word Template 2010 ( 141 / 141 )
    Other Documents ( 168,628 / 168,628 )
    WordPerfect ( 14 / 14 )
  Email ( 9,235 / 9,235 )
  Executable ( 72,699 / 72,699 )
  Folders ( 262,498 / 262,498 )
```

```
There has never bee
averting disaster, the
The suffering I bring
Today, mankind has
I call all rationalist wi
Any belief in a spiritu
Here I will emphasize
```

Limited File Viewing

FTK's All File Types Viewer

SEE IT IN ACTION

FTK Imager lists all the device's files and directories, but it only displays four rudimentary file types: graphics, text documents, html documents, and basic video files. You cannot view databases or complex files like Microsoft Word or Excel. Imager can help you SEE and FIND a file, but you can't open it unless it's one of those four types.

With **FTK**, you can open and view all file types, including system files, user activity, and system activity from Microsoft Windows and Apple's MacOS operating system. FTK makes forensic review easier by automatically finding and parsing all the necessary data, including:

- **Application data**, such as install, prefetch, and user assist files
- **Network information** like the interfaces and networks the user was connected to
- **Operating system information** such as configured time zone, device owner, various user accounts, and windows timeline activity
- **Recent files** like jump lists, linked files, shell bags, and windows event logs

Manually Locate Files

FTK's Powerful, Fast Searching

SEE IT IN ACTION

Exterro's **FTK** Index search engine allows users to quickly search hundreds of gigabytes of data in seconds. No need to manually hunt for files in **FTK Imager** when you can search accurately and quickly in FTK. Plus, if you want to search byte-for-byte through every object in your case, use FTK's Live Search. It supports text, pattern and hex searching, so you can use regular search expressions and search for any type of file you want.

Limited Browser Data

FTK's Web History & Artifacts

SEE IT IN ACTION

You cannot view things like web browser search history in **FTK Imager**, since that URL data is stored in a database that Imager can't display. **FTK** offers URL detection and parsing capabilities across devices, without regard to browser, neatly organized in one section so you can quickly get to the web activity that matters most with pre-filtered web artifact categories like social media, mapping, adult, and much more.

No Video Viewer

FTK's Video Analysis Workflow

SEE IT IN ACTION

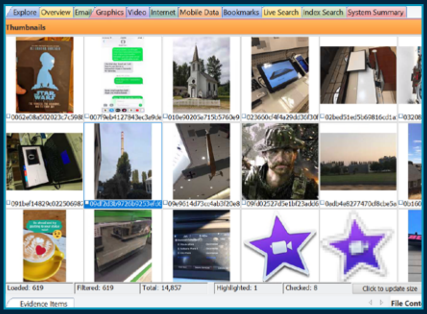
While you can find video files in **FTK Imager**, you cannot render and view them. You must export the video and use another third-party tool to watch it. **FTK** will not only find and categorize different video file types automatically, it will also generate thumbnails to give you an idea of the content of each video before you watch it. When you do watch the video, it will render and play directly within the FTK interface, making video analysis convenient and easy.

Inefficient Image Review

FTK's Graphics Analysis

SEE IT IN ACTION

In **FTK Imager**, you can manually navigate through the file structure to select an image from the list, but you have no idea what the image is until you select it. You are only able to view images one at a time, and you can't resize the image once it's selected either. In **FTK**, you have a robust, customizable image thumbnail pane, where you're able to see multiple images at once. Once selected, images contain all associated metadata and can be displayed at full size, resized and rotated.



Laborious File Recovery

FTK's Extensive Data Carvers

SEE IT IN ACTION

In **FTK Imager**, you can recover a deleted file, but you have to manually find the header and the footer of the file in order to recover it. With **FTK**, you can see and recover files that have been deleted from the Recycle Bin, but have not yet been overwritten on the drive. FTK's data carvers offer you the ability to automatically carve a diverse amount of file types easily–and you can even create your own data carvers!

Limited PST Access

FTK's PST Email File Viewer

SEE IT IN ACTION

If you're looking for a user's Outlook PST file, **FTK Imager** can show you that a user directory exists for that person, and you can see that there is a PST file, but you can't see any emails in the PST file. Imager's capabilities at least let you know that you need to image that hard drive, but you'll need **FTK** to open and view that PST file to see its contents.

Lost Progress

FTK's AutoSave:

SEE IT IN ACTION

FTK Imager doesn't save any of your progress when you close the program. You have to reload the image and start over again from scratch. **FTK** not only automatically saves your position within the evidence that you've loaded and processed, but also saves your file analysis work!

Read-only Reports

FTK's Portable Case:

SEE IT IN ACTION

This feature is an 'FTK Fan Favorite'! With **FTK Imager**, you have to spend time generating reports that can only be viewed in limited formats. Using **FTK**, you can export your data into a portable case for offline review by a detective, analyst, attorney or outside reviewer, and any labels and bookmarks created by the reviewers are synced back to the original case.

BONUS FEATURE

FTK's Full Volume BitLocker decryption

SEE IT IN ACTION

Need to investigate a BitLocker-encrypted Windows device? No problem! **FTK** can decrypt a device in a locked, unlocked, or disabled BitLocker state. And it can decrypt on the fly, without having to create a fully decrypted image first.

Learn more about the **FTK® Forensic Toolkit** visit

www.exterro.com/forensic-toolkit

TOP 10 MOST UNDERRATED FTK® FEATURES

exterro®

1

Full Volume BitLocker decryption—

Need to investigate a BitLocker-encrypted Windows device? No problem! FTK can decrypt a device in a locked, unlocked, or disabled BitLocker state. And it can decrypt *on-the-fly*, without having to create a fully decrypted *image* first. Even with computers in a "Disabled–Protectors Suspended" BitLocker state (often shipped this way by default from hardware vendors), FTK can detect the suspended encryption, and automatically attempt to recover a clear key from the master boot record and decrypt the drive, all without the computer user's input.

2

Use the KFF to identify and ignore irrelevant files—

You can reduce the number of files in your case by 40-70% when you use the Known File Filter (KFF) utility to ignore irrelevant or "known" files. The KFF is a collection of MD5 and SHA1 hash values used to locate files residing within *your* case evidence that have been previously encountered by other investigators or archivists. Identifying previously catalogued (i.e., known) files within a case allows you to skip over them, thus expediting your investigation. The KFF also identifies files you *want* to be alerted to, like malware or other contraband files.

3

Parse all major browsers with URL categorization—

Get a head start on your investigation with URL detection and parsing capabilities across devices, without regard to browser, now neatly organized under one section so that you can easily review the data and connect the dots in your investigation. Quickly get to the web activity that matters most with pre-filtered web page categories. Web artifacts will be grouped into categories such as social media, mapping, adult, and much more!

4

Recover deleted data with data carvers—

Use FTK's extensive set of data carvers to view and recover files that have been deleted from the Recycle Bin but have not yet been overwritten on the drive. You can also use FTK data carvers to recover data from unallocated or slack disk space, which is especially relevant in CSAM cases when looking for deleted pictures and videos, specifically.

Investigate mobile phone data—

FTK supports native, unprocessed extractions from mobile devices provided by tools like Cellebrite and Oxygen. Processing and parsing mobile data *directly* in FTK means you can speed through review and analysis, and even find common connections across data sources since FTK has the fastest processing engine on the market for ALL data types.

BONUS: *As a certified Grayshift Technology Alliances Partner, FTK can fully and accurately import and parse mobile iOS and Android extractions created by GrayKey.*

Investigate Mac devices—

Use FTK to analyze key Mac data types and applications such as iMessage, iWork, and Safari data, as well as Mac artifacts like Spotlight Search data, KnowledgeC, and Power Log data. FTK can clearly reconstruct and display native Apple Mail and Outlook for Mac email formats and associate all of the email attachments, making forensic review a cinch. And with FTK, you can process a Mac AFF4 image faster than any other tools on the market. (26 mins vs. 3.5 hours!)

7

Image Identification & Categorization—

FTK can help reduce the mental burden on investigators who face repeated exposure to graphic abuse images by using artificial intelligence. Use FTK's AI to search video and photo evidence for clues like faces, guns, money, vehicles, and explicit material. Use facial and object recognition to automatically locate images containing that same content. Help identify victims faster in CSAM investigations by analyzing and grading images & videos and comparing them with collaborative hash databases like Project Vic and CAID UK.

8

Package up your data and send to a reviewer with FTK Portable Case—

Export your data into a portable case for offline review by a detective, analyst, attorney or outside reviewer. No need to spend time generating reports that can only be viewed in limited formats. Portable case creates an offline version of your FTK case file with a quick export, and any labels and bookmarks created by the reviewers are synced back to the original case.

9

Enhanced system summary—

No more manual searching through registry files to find relevant system data! As Windows captures the timeline of actions of the user, FTK will parse those registry files for you. See every application the user opened, internet activity performed, networks the user was connected to, and where and when this activity occurred. FTK has parsing support for AmCache registry files, SRUM artifacts, Windows timeline events and more. You can also label, bookmark and export individual objects to easily search, filter, and report.

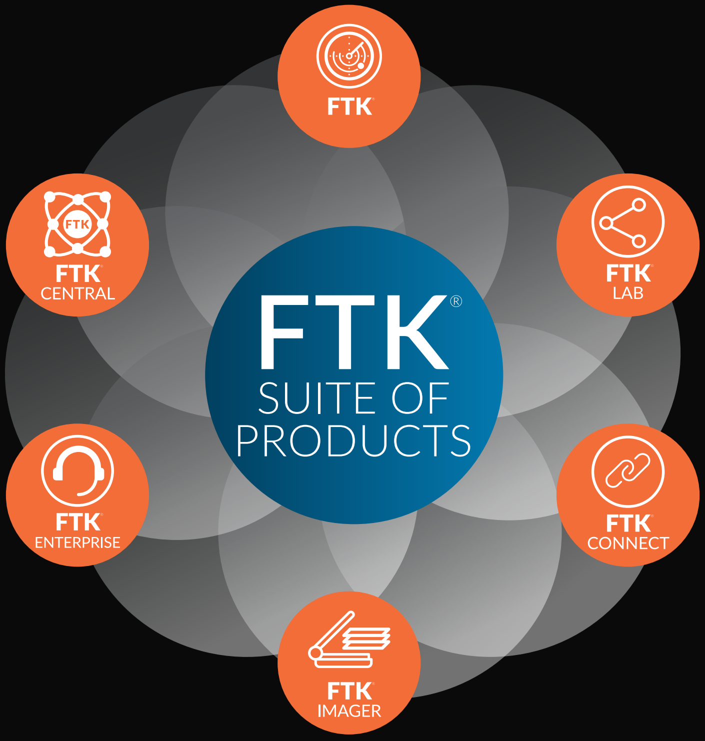
10

Automate processes with Python—

Invoke and utilize the capabilities of Python scripting directly from within the FTK interface, which keeps all the data in one location and reduces the risk of spoliation. Python scripting provides two key advantages. First, it can be used as a custom parser for non-supported data and applications, which eliminates manual processes used previously for non-supported data. Second, it can be used to create custom reports to easily present complex information and analysis to non-technical stakeholders like attorneys or prosecutors.

BONUS FEATURE: Did you know you can customize FTK's interface?
Design a personalized interface for your forensic workflow by creating your own new tabs for custom data types. You can also undock any of the UI panels and reorganize them, place them side-by-side, or move them to a second computer monitor for easier viewing.

In addition to the classic standalone version of the FTK Forensic Toolkit, there is an entire suite of FTK solutions to handle your complex collection, processing, and analysis needs. Turn to FTK Lab for scalable, distributed processing power, or use FTK Enterprise for remote endpoint collection both on and off your network. Need to involve non-technical users or outside reviewers to your forensic review workflow? Look no further than FTK Central's web-based, collaborative, and intuitive platform.



No matter the type of forensic investigation, there's an FTK Solution designed specifically for your investigative workflow – all with the industry's fastest processing engine for repeatable, defensible, forensically-sound collection and analysis.

Looking for video content on how to use all of FTK's features? Visit our YouTube channel

For more than 30 years, **FTK** has pioneered forensic investigations and we are proud to be the only American-owned and operated forensic company in the industry.

GET A DEMO