Examining Evidence with FTK Imager



Phil Chapman
SENIOR INSTRUCTOR

@PhilChap777

Overview



Viewing Evidence Items

- Add Evidence Item
- Mount Image

Triaging Evidence

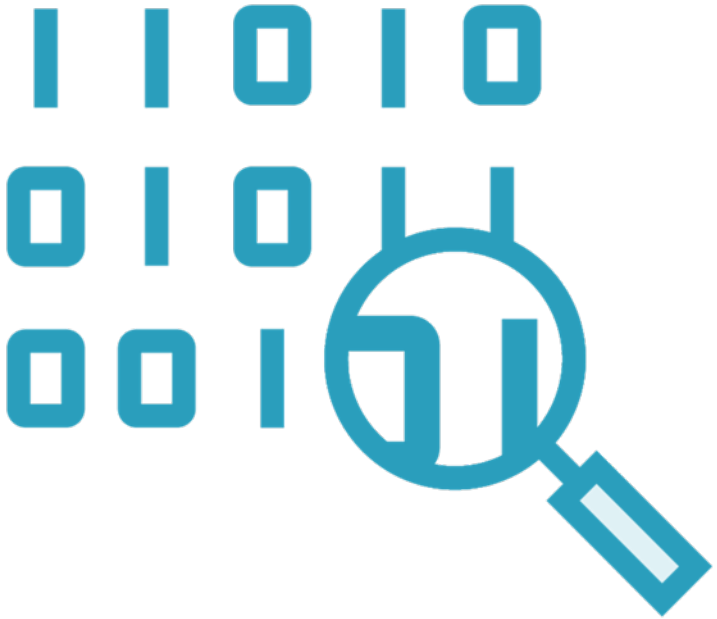
- Searching
- Saving/Exporting

Course Summary

- Key points

Viewing Evidence Items

Working with Evidence



Previewing Evidence using FTK Imager

Add Evidence Item

- Full preview of image

Mount Image

- Physical/Logical
- Natively view contents
- Share and view logically mounted image
- Easily copy files
- Read only

Demo



Viewing Evidence Items

- Add Evidence Item
- Mount an Image

Demo



Triaging Evidence

Summary



FTK Imager

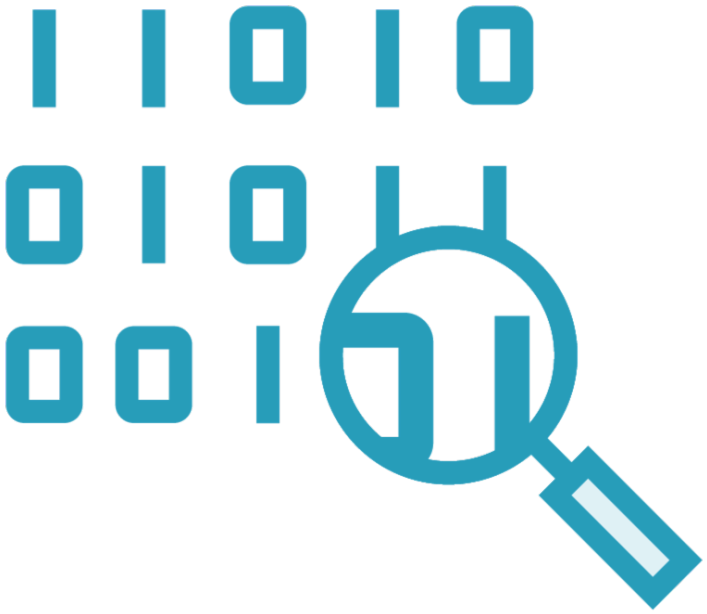
- Evidence Items
- Mounted Images

Triage

Forensic Analysis

- MFT File Properties
- Recovery of deleted items
- Slack space/Unallocated space

Triaging Evidence



What can FTK Imager provide us with?

The ability to quickly and effectively triage evidence

- Evidence Items
- Mounted Images

The ability to view system file properties for forensic analysis

Forensic Toolkit (FTK) for the full toolset/capability

Demo



Triaging Evidence

- Viewing and Searching
- Converting data
- Saving
- Exporting

Course Summary

Summary



Installation and Configuration of FTK Imager

- Windows
- Linux
- USB

Capturing Volatile and Protected Data

- Order of volatility

Capturing a Forensic Image

- Considerations of Live v Dead-box

Examining Evidence

Summary



Prepare and practice

Course discussion

Other Forensic courses in the series