Capturing a Forensic Image with FTK Imager



Phil Chapman
SENIOR INSTRUCTOR

@PhilChap777

Overview



Understanding Image Types

- Points to consider
- Physical, Logical Drives
- Types of Images

Create a Forensic Image

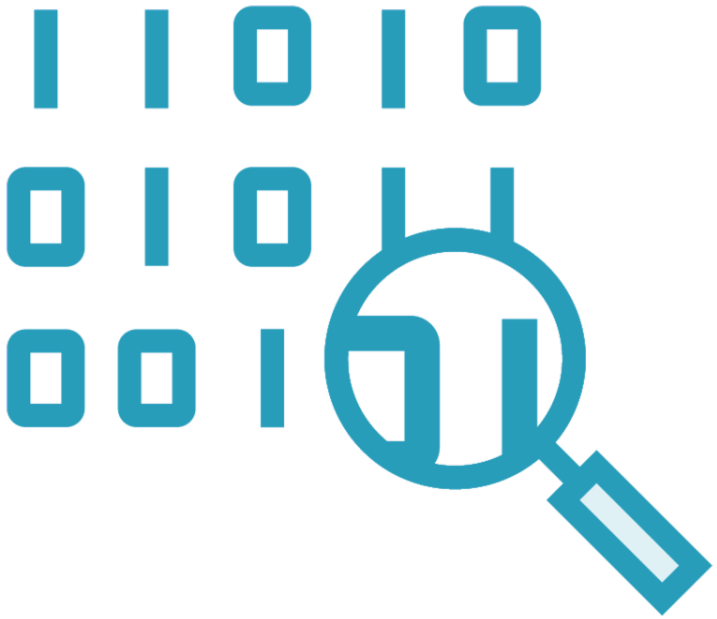
- Step by step demonstration

Using Custom Content Images

- Demonstration

Understanding Image Types

To Image or Not To Image?



Points to Consider

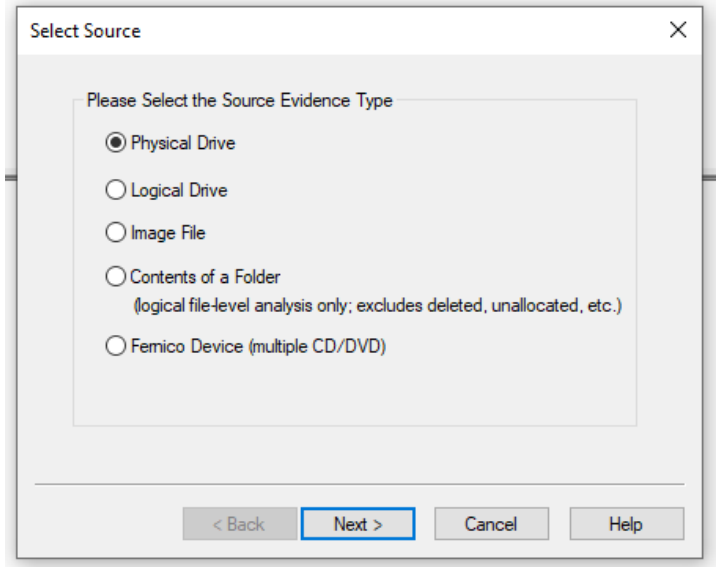
Decision to take a live image or dead box?

- Encryption
- Speed of investigation
- Level of investigation
- Law, Regulation and Standards



Points to Consider

- Time
- Cost
- Storage
- Environment
- Risk (Power, Interruption etc)
- Write-blocker



Select the Source of Evidence Type

- Physical Drive
- Logical Drive
- Image File
- Contents of a Folder
- Fernico Device

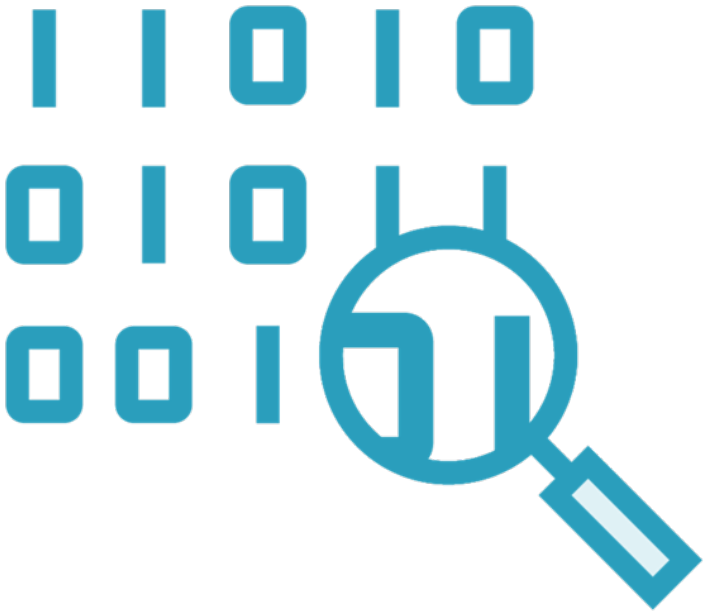
Creating a Forensic Image

Demo



Using FTK to acquire a forensic image

- Step by step
- Verification of image



Seize Suspect Machine/Drive?

Keep the Original Image

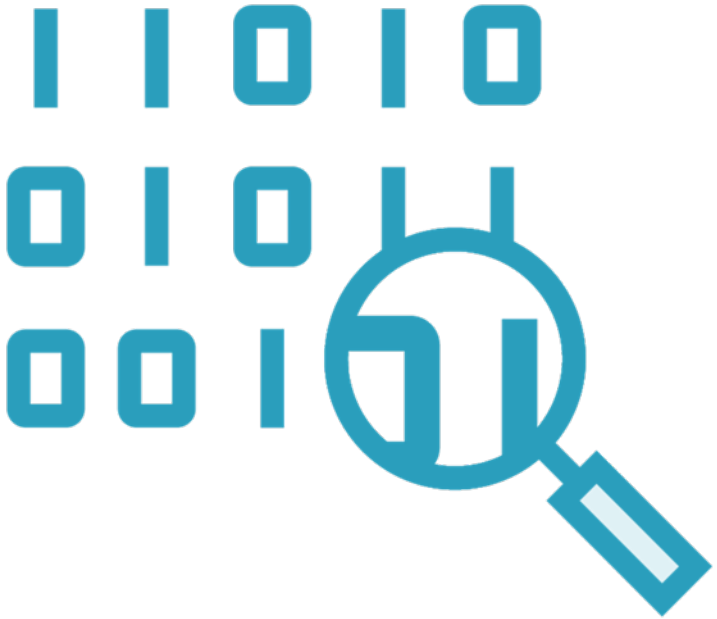
Never work on the original

Maintain Chain of Custody

Create Custom Image

Using Custom Content Images

FTK Imager Custom Content Images



May be taken from a live image/drive

- Target specific areas of interest
- Useful for triage
- Speeds up acquisition time
- Smaller image file (cost/time)

May be used to filter captured images

Search on * wild-card filters or exact matches to files

Filter on specific user accounts (SID)

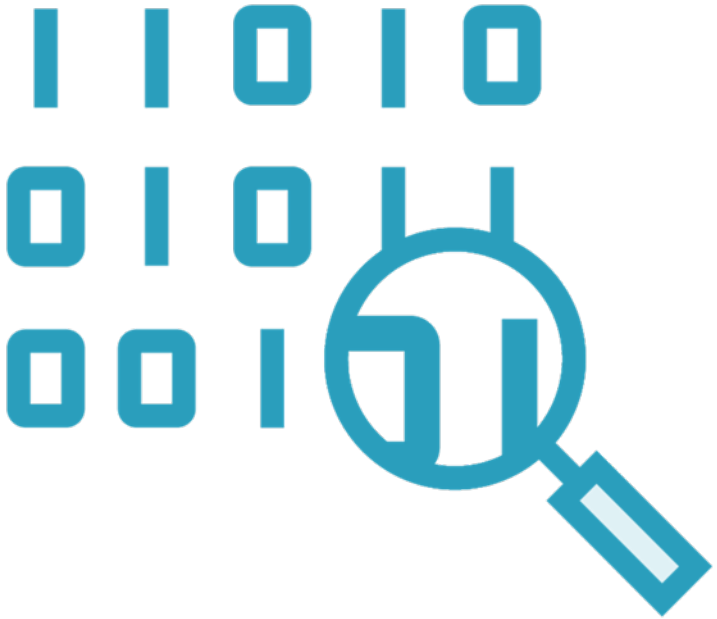
Demo



Using FTK to acquire a Custom Content Image from a live device

- Step by step
- Filters
- Verification of image

Imaging Summary



- Live acquisition may be necessary
- Apply the Law, Regulations and Ethics at all times
- Avoid uncertainty and doubt
- Plan and Preparation
- Risk
- Integrity Check
- Use Custom Content Images to save time and cost