AccessData Forensic Toolkit (FTK) Imager

INSTALLATION AND FAMILIARIZATION OF THE FTK IMAGER INTERFACE



Phil Chapman
SENIOR INSTRUCTOR

@PhilC777

Overview



Overview of FTK Imager

Install and Configure FTK Imager on Windows

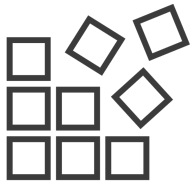
Install and running FTK Imager from a USB drive

Install and running FTK Imager on Linux

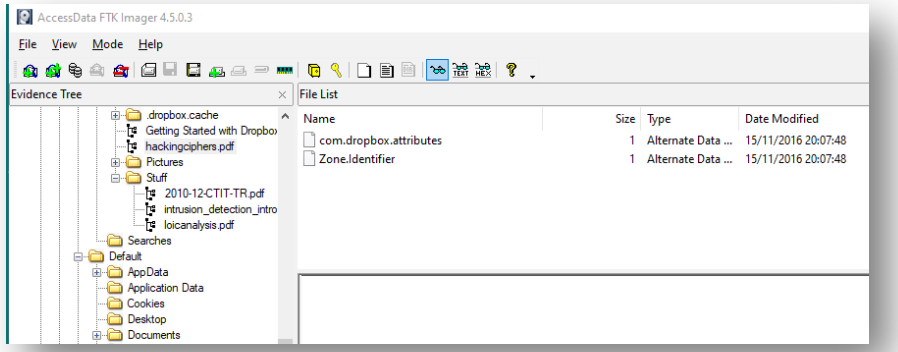
FTK Imager Overview



Capture Volatile and Protected data



Capture a forensic image





View and analyse captured images

Installing on a Windows Desktop



Download from AccessData (Release Notes and User Guide)

https://accessdata.com

Email Link

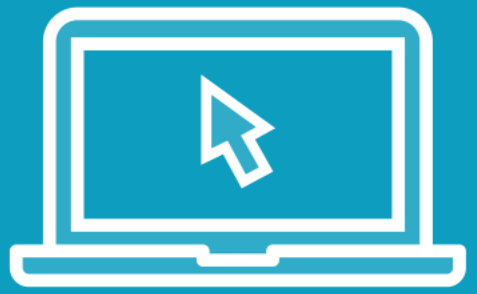


Extract and Install onto local drive



Configure Interface

Demo



Installing FTK Imager on Windows Workstation

Explore & Configure Interface

Running from Command Line

Installing FTK Imager on a USB Drive

Running FTK Imager from USB



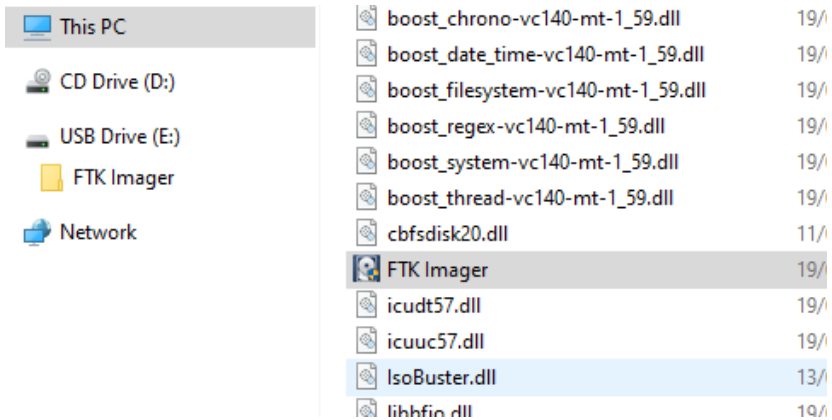
Removes the risk of locally installing on suspect computer



Application is portable to multiple devices



Minimal overhead



Install FTK Imager on forensic workstation

Insert formatted flash drive (FAT32 or NTFS)

Copy FTK Imager installation folder to flash drive

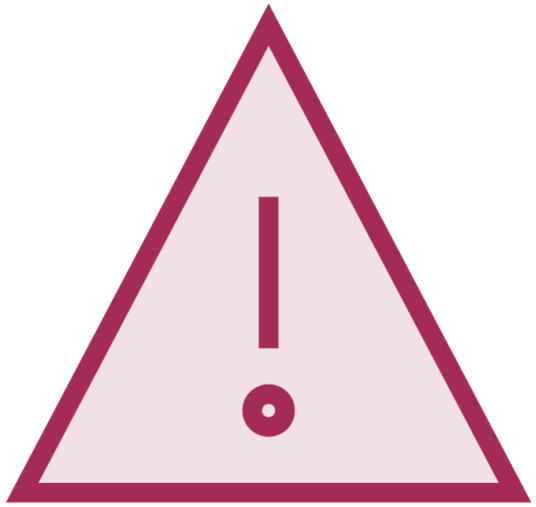
Separate Partitions / Tools Folder

Or Download directly to USB Device, extract and install locally

USB Considerations



USB Access may be restricted



Running application will impact on target machine



Storage requirements



Ensure that all actions are recorded and audited

Ensure Harvest Drive is clean and formatted

Consider using a powered USB hub

Always conduct risk assessment

Have an tested Incident Response Plan

Cater for contingency

Installing FTK Imager For Linux

Demo



Installing FTK Imager on a Linux Workstation

Running FTK Imager on Linux