Total Forensic Solutions

FORENSIC MEDIA EXPLOITATION TOOLKIT

NLP-DMX-103

Excellence through Research and Relevancy

Key Points of Tactical Exploitation

- Time
- Equipment
  - On Target
  - Off Target
- Scope of the Mission

METL

- Mission Essential Task List
  - Should power procurement
  - What will you use
  - Solutions that bridge gaps or the add-ons to tools`

- What is the Forensic Media Exploitation Toolkit?
- A set of tools that have been put together allowing the SOF Exploitation Team the ability to gather Media and Cellular data
- The toolkit can be run from USB
- The toolkit requires Windows 7x or higher and a read write USB interface
- The tool uses Community Edition Tools
  - No license
  - No Renewals
- Tool can be used as an 80% extraction toolkit

FMETK Hardware Kit 2019

Tool	Media	Cellular	SIM	Target	
Cool Gear Write Blocker	X	X		X	Hardware write blocker that will allow for unpowered collection at target. Drive size will matter due to power consumption
FMETK USB Thumb drive	X	X	X	X	USB that maintains all the applications for use on target and at the objective
USB Kill Device Blocker	X	X		X	USB current and voltage surge protector. Device will not allow the USB bus to be over powered
OmniKey USB SIM Card Reader			X	X	Imaging and file collection tool for media, will extract a memory image.
Kindle Reader Android Tablet	X	X	X	X	Device to manage all video tutorials and manuals

FMETK Toolkit

FMETK USB Drive with pre-installed programs

USB SIM Card Reader

USB Killer detector

3 Way Universal Data/Power Cable for Cellular Devices

USB C Connector for Hardware Write Blocker

Credit Card Magnifier

FMETK Toolkit

Power Brick for the Hardware Write Blocker

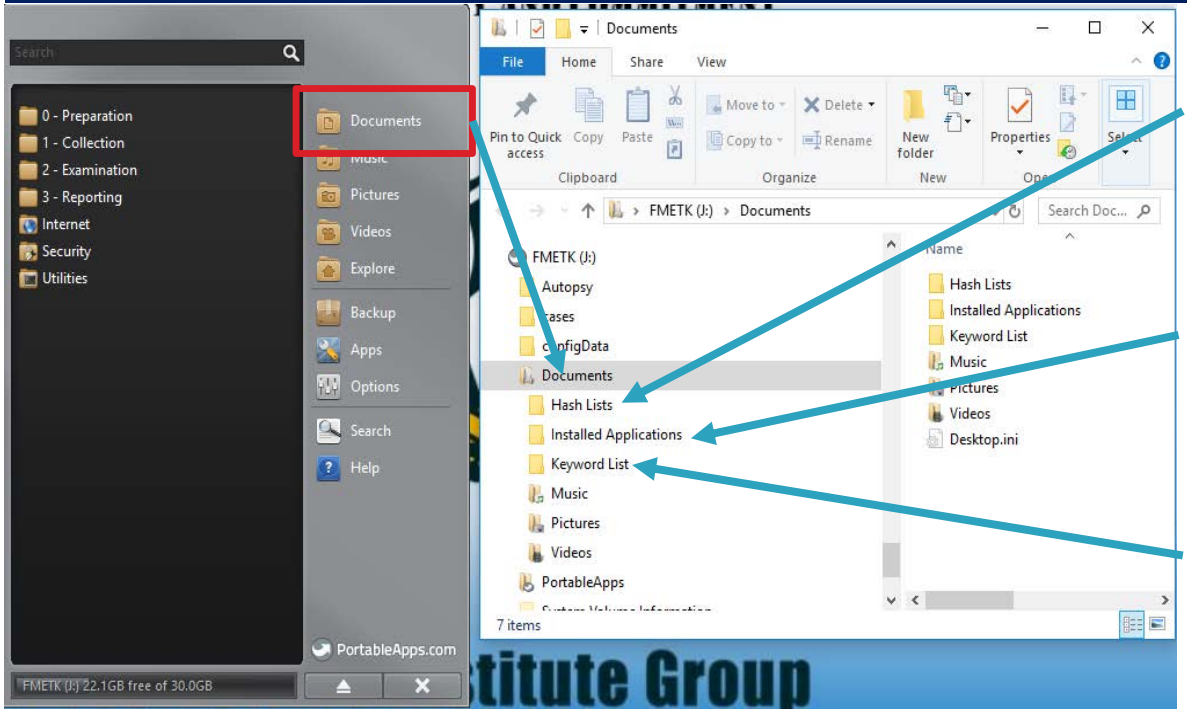
Hardware Write Blocker W/IDE and SATA Cables

Kindle E- Reader

Forensic Media Exploitation Toolkit 2019

Tool	Media	Cellular	SIM	Target	
Autopsy The Sleuthkit	X	X	X	X	Core application for reviewing collected data. Can also be used as an imaging tool creating a VHD image
Autopsy Plugins	X	X	X	X	Plugins add functionality to autopsy allowing the collection of additional artifacts
Magnet Acquire CE	X	X		X	Community Edition Cellphone extraction tool. Creates backups of IOS and Android devices
FTK Imager Lite	X			X	Imaging and file collection tool for media, will extract a memory image.
HTCI SIM			X	X	SIM Card Reader and extraction tool
HTCI USB Toggle	X			X	Software Write Blocking Tool
Android Ripping Tool		X		X	Tool to extract the contents from and Android device
HTCI Extractor		X			Tool to convert the backup images created in Magnet Acquire to ingestible Autopsy data
DiskWipe	X				Tool to prepare media collection drives

DOCUMENTS



Hash lists such as the current NSRL and other known Hash Lists.

Installable applications. Applications that will not run from the USB.

Like Hash lists, these are known dictionaries that can be used in Autopsy.

Challenges of Open Source

- Documentation that relates to a workflow
- Update notification
- Verification of the updated tools

Summary

The FMETK toolkit is a complete Open Source or Community based application set allowing operators to investigate media on target and at FOB based locations


Computer
Select Manage
Select Disk Management
Verify that a new Physical Drive has been added
Click on the Disk and
Initialize

Questions