AGENDA

• IO Overview
  • Why IO?
  • Imaging Overview
  • Logging Overview
  • What makes IO unique?

• Triage

• Open Source Engagement
WHY IO?

• Simple
• Prevents imaging incorrect device
• Triage concurrently while imaging
• Extensible
• Developed in Java
1. Open ION

2. Connect Target Media

3. Collect Image
IMAGING OVERVIEW

- Automated initialization of software write-blocks prevent changes to target media

- Outputs EWF, Expert Witness Format, images
  - Compressed and searchable
  - Allows for error detection using checksums
  - Segmented, using the ascending naming scheme E01
• Automated detection of connected media - eliminates user error

• Resulting images conform to standard naming conventions, sizes, and E01 output specifications
CONNECT TARGET MEDIA TO ANY USB PORT
[Imaging will start automatically]
Manually Select Device
Model: SanDisk Cruzer Slide USB Device
Size: 20550109008
PNPDeviceID: USBSTOR\DISK&VEN_SANDISK&PLOD_CODE\PROD_CRUZER_SLIDE\&REV_4.05.000018865749008
Physical Serial: 0000188E56749008
Vendor ID: 0x0761
Vendor: SanDisk Corporation
Product ID: 0x5191
Geometry:
Heads: 255
Cylinders: 249
Tracks: 63495
Sectors: 4013709
Volumes:
Volume: E:
Root: E:
Volume Serial: 0000-0000
Volume UUID: 13537882869762104169
Volume Filesystem: VFAT

87% remaining: 01:07
Abort Imaging
Complete

Return To Main

Imaging Completed Successfully.
One Folder Per Device

Default Image Path
• Automatically extracts and logs critical information for down-stream examiners.
  • Standard Imaging Details
    • Device Type
    • Model
    • Size
    • Geometry
    • MD5 & SHA1 Hash
  • Hardware Serial Number
  • Volume Serial Number(s)
  • Device VID/PID (if applicable)
  • Volume UUID (if applicable)
• **To image a drive, we have to read all the data.** If we are reading all the data anyway, why not process it?

• Triage processing does not impact imaging time because the process is limited by disk read speed

• IO’s API allows developers to create additional processing modules and customize output
TRIAGE

• **Base Triage Functionality**
  • File Snapshot: An estimate of how many files (by type) exist on the target device
  • Exif Geo Extraction: A list of all geo-location information extracted from JPEGs

• **Countless possibilities for additional in-line parsers**
  • File Extracts
  • Flash Review of Media Content
  • Incorporation of Text Selectors
TIMELINES

Traditional Media Processing Track

Acquire Media
Configure Tool
Imaging
Transfer Image
Triage
Further Examination
Additional Intel Report
TIMELINES

Traditional Media Processing Track

Acquire Media  Configure Tool  Imaging  Transfer Image  Triage  Further Examination  Additional Intel Report
• IO is open-source, fully tested, and is completely free to use and modify

• Cipher Tech will release updates as core functionality is improved
• We plan to continue to extend IO’s functionality, and invite the community to download IO, use it, and add triage methods

• IO’s framework handles basic parallelization for new triage methods

IO is available on GitHub at:
https://github.com/ciphertechsolutions/IO
IO is available at:
https://www.ciphertechsolutions.com/open-source

Reach the IO team:
io@ciphertechsolutions.com

Keith D. Bertolino, CEO
Cipher Tech Solutions, Inc.
kbertolino@ciphertechsolutions.com

Matthew B. Kowalski, CTO
Cipher Tech Solutions, Inc.
mkowalski@ciphertechsolutions.com