Simple Imaging. Tactical Triage. Zero Clicks.

CIPHER TECH SOLUTIONS

AGENDA

- **IO Overview**
  - Why IO?
  - Imaging Overview
  - Logging Overview
  - What makes IO unique?
- **Triage**
- **Open Source Engagement**

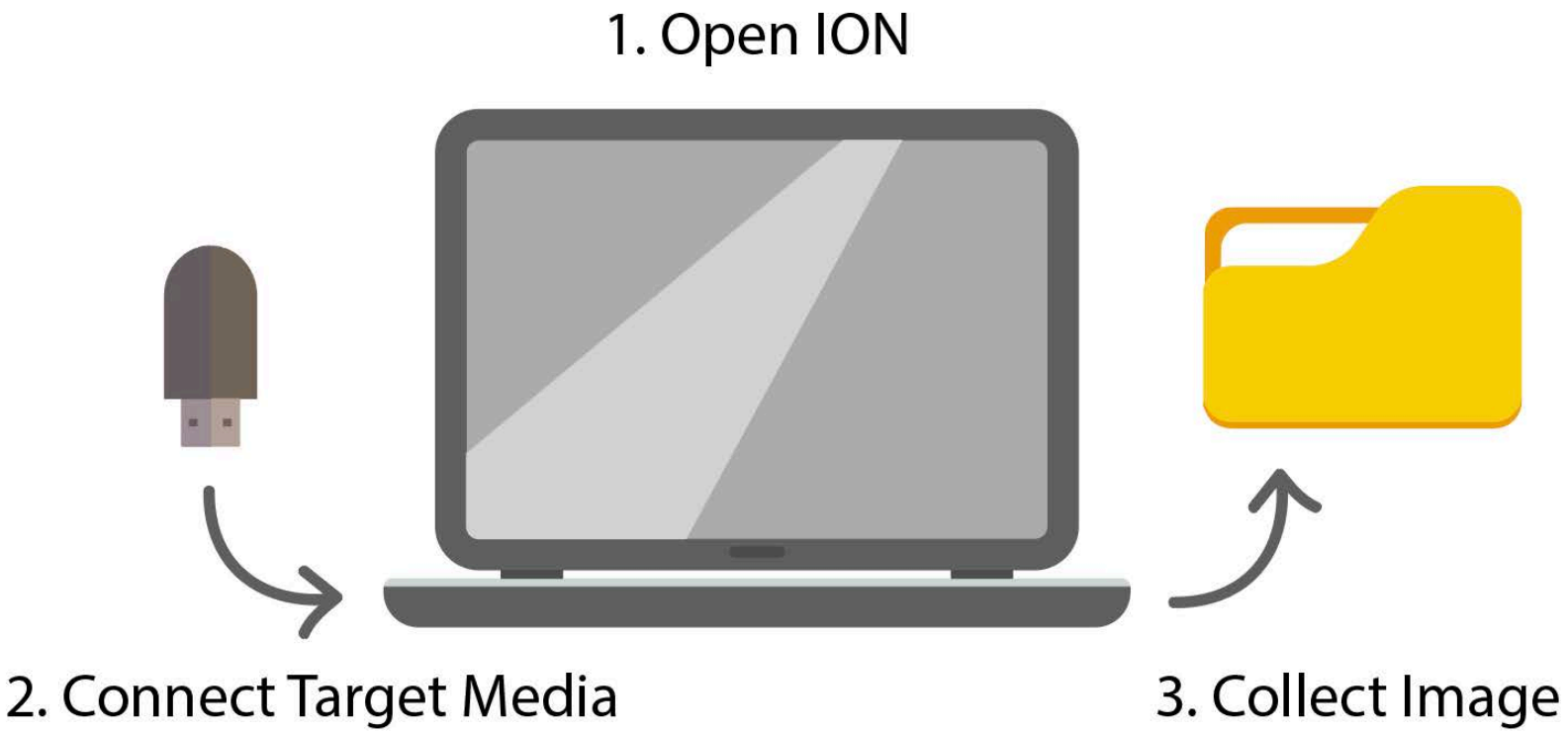
CIPHER TECH SOLUTIONS

WHY IO?

- Simple
- Prevents imaging incorrect device
- Triage concurrently while imaging
- Extensible
- Developed in Java

CIPHER TECH SOLUTIONS

IMAGING OVERVIEW



CIPHER TECH SOLUTIONS

IMAGING OVERVIEW

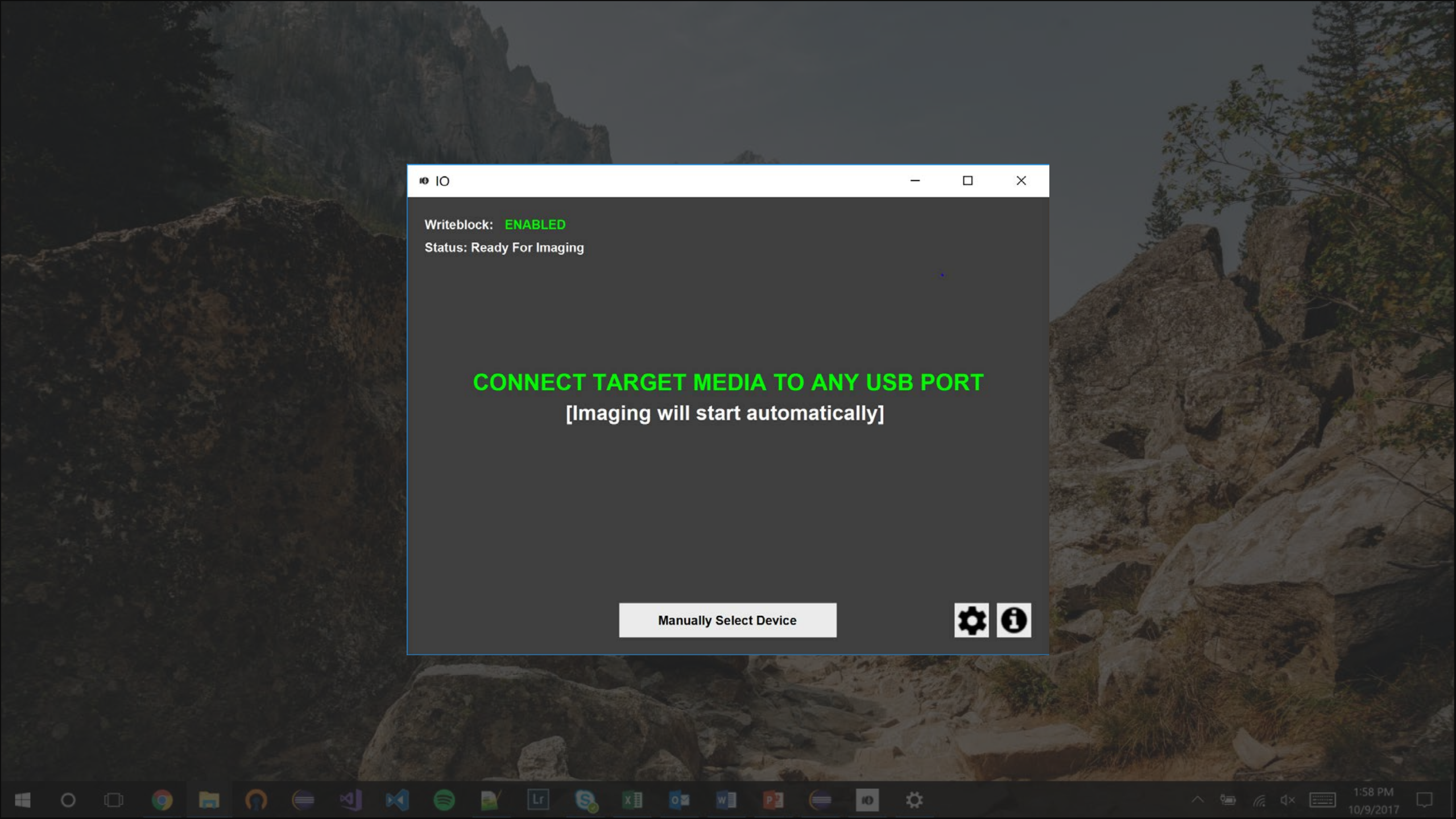
- **Automated initialization of software write-blocks prevent changes to target media**

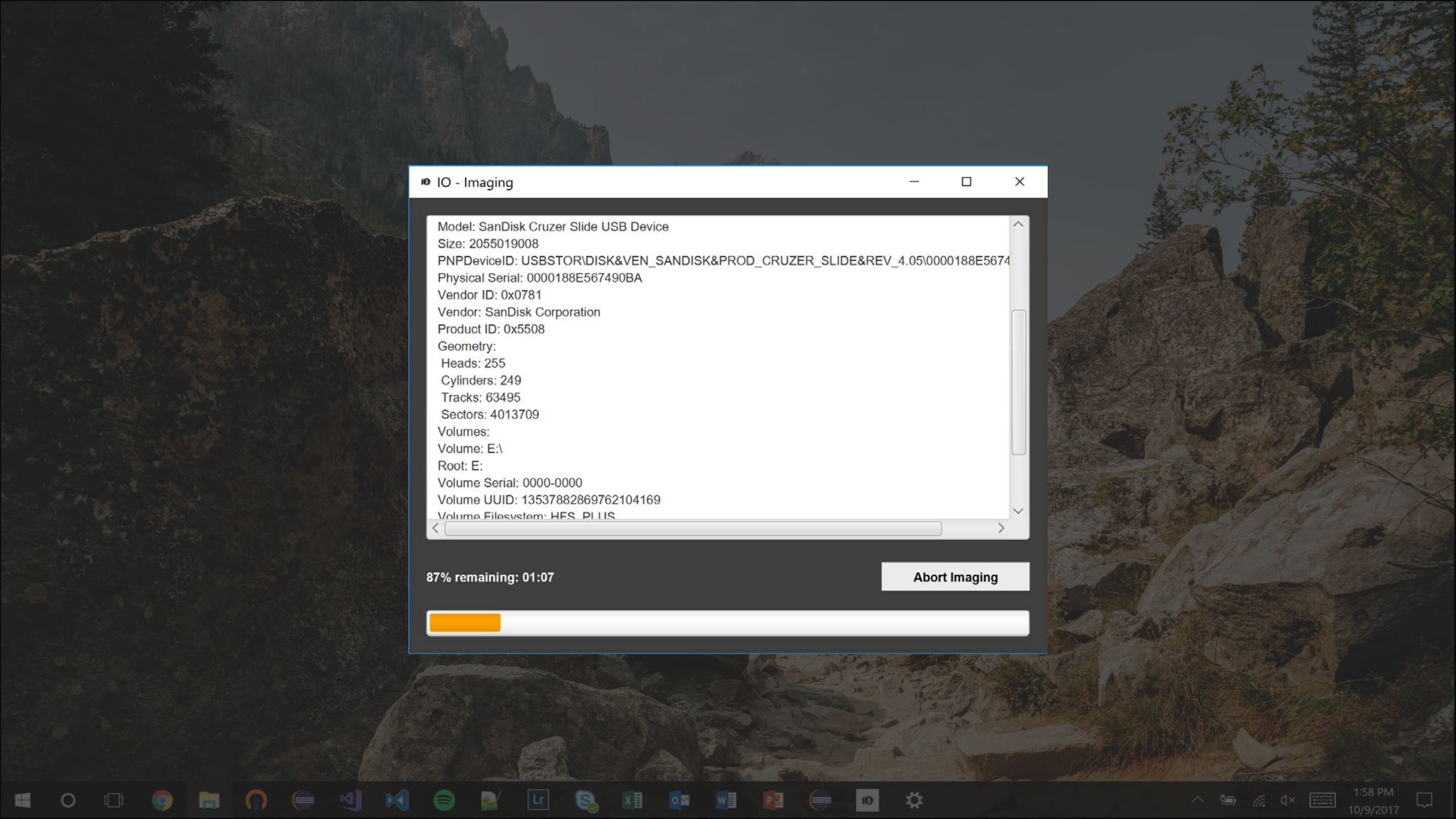
- **Outputs EWF, Expert Witness Format, images**
  - Compressed and searchable
  - Allows for error detection using checksums
  - Segmented, using the ascending naming scheme E01

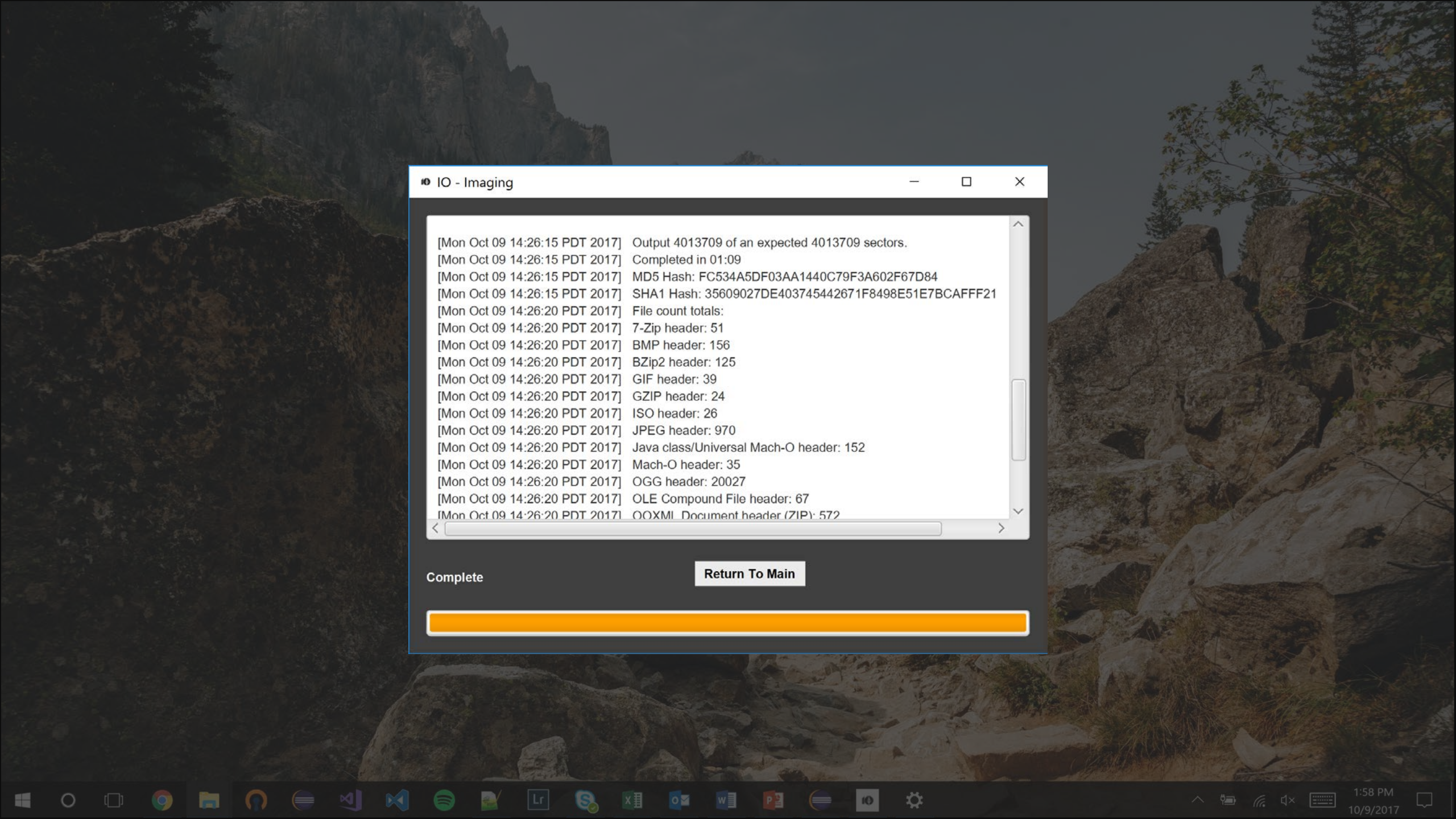
IMAGING OVERVIEW

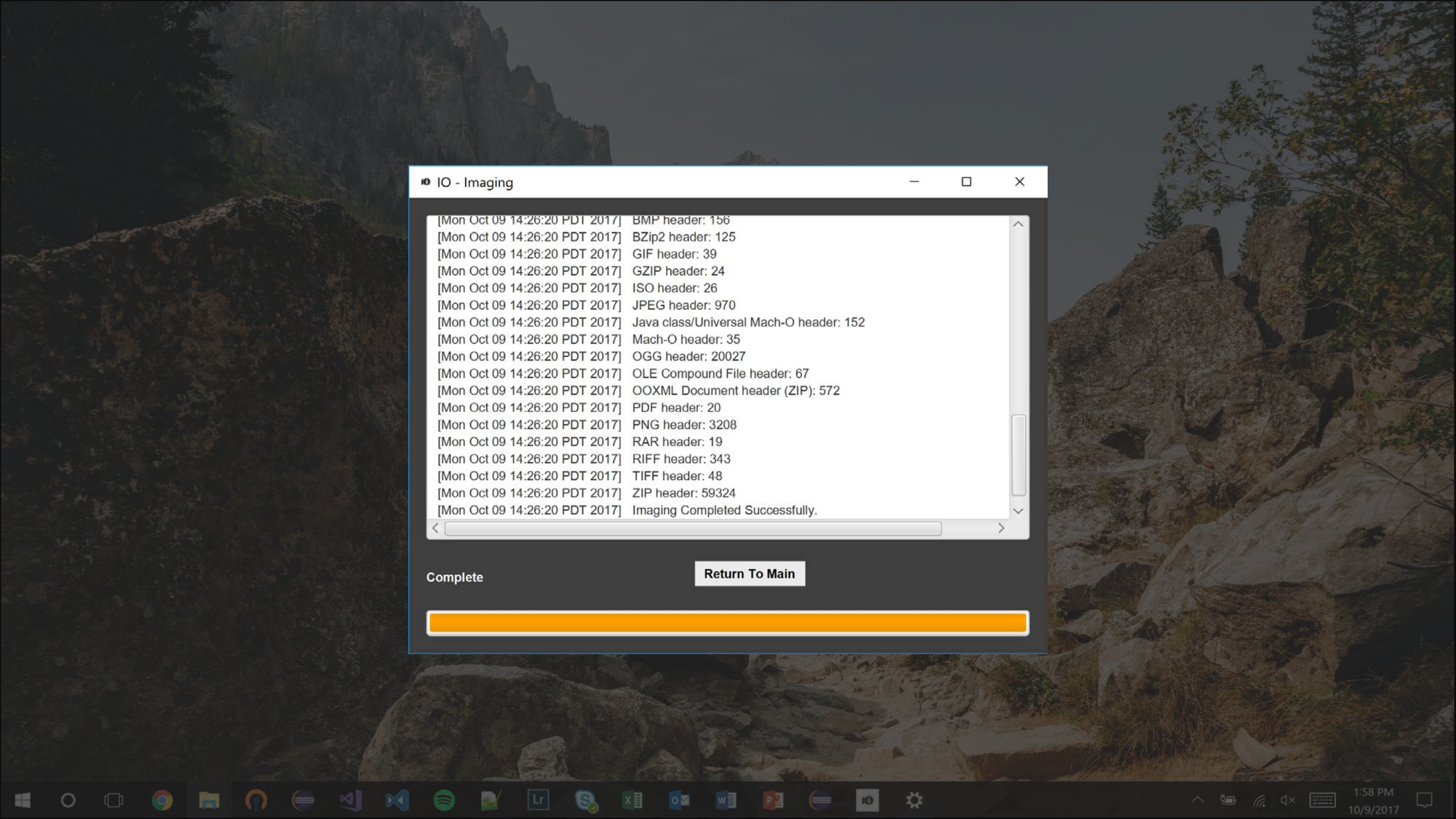
- Automated detection of connected media - eliminates user error
- Resulting images conform to standard naming conventions, sizes, and E01 output specifications

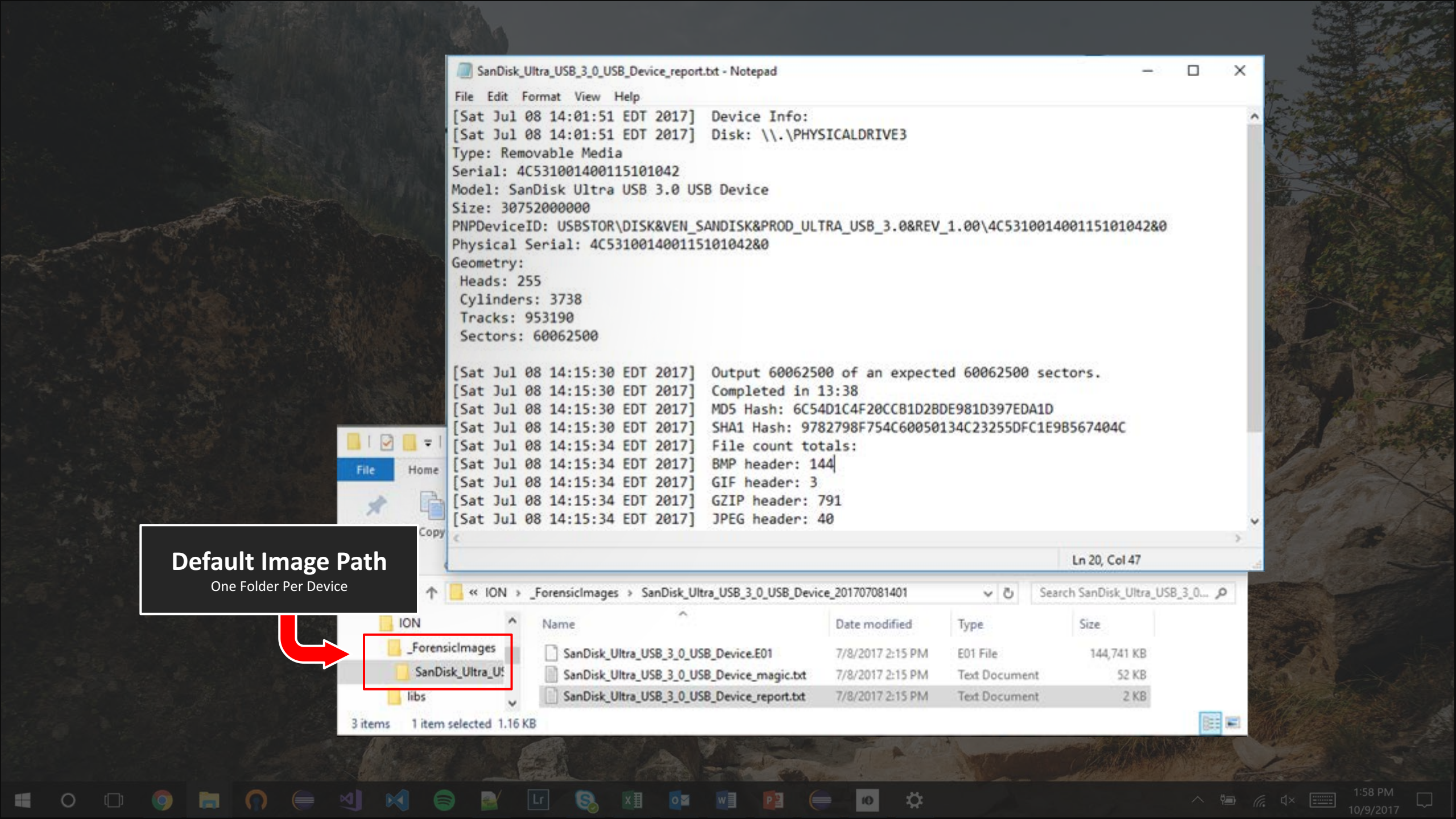
CIPHER TECH SOLUTIONS


IO
Writeblock: ENABLED
Status: Ready For Imaging
CONNECT TARGET MEDIA TO ANY USB PORT
[Imaging will start automatically]
Manually Select Device
1:58 PM
10/9/2017


IO - Imaging
Model: SanDisk Cruzer Slide USB Device
Size: 2055019008
PNPDeviceID: USBSTOR\DISK&VEN_SANDISK&PROD_CRUZER_SLIDE&REV_4.05\0000188E5674
Physical Serial: 0000188E567490BA
Vendor ID: 0x0781
Vendor: SanDisk Corporation
Product ID: 0x5508
Geometry:
Heads: 255
Cylinders: 249
Tracks: 63495
Sectors: 4013709
Volumes:
Volume: E:\
Root: E:
Volume Serial: 0000-0000
Volume UUID: 13537882869762104169
87% remaining: 01:07
Abort Imaging
1:58 PM
10/9/2017


IO - Imaging
[Mon Oct 09 14:26:15 PDT 2017] Output 4013709 of an expected 4013709 sectors.
[Mon Oct 09 14:26:15 PDT 2017] Completed in 01:09
[Mon Oct 09 14:26:15 PDT 2017] MD5 Hash: FC534A5DF03AA1440C79F3A602F67D84
[Mon Oct 09 14:26:15 PDT 2017] SHA1 Hash: 35609027DE403745442671F8498E51E7BCAFFF21
[Mon Oct 09 14:26:20 PDT 2017] File count totals:
[Mon Oct 09 14:26:20 PDT 2017] 7-Zip header: 51
[Mon Oct 09 14:26:20 PDT 2017] BMP header: 156
[Mon Oct 09 14:26:20 PDT 2017] BZip2 header: 125
[Mon Oct 09 14:26:20 PDT 2017] GIF header: 39
[Mon Oct 09 14:26:20 PDT 2017] GZIP header: 24
[Mon Oct 09 14:26:20 PDT 2017] ISO header: 26
[Mon Oct 09 14:26:20 PDT 2017] JPEG header: 970
[Mon Oct 09 14:26:20 PDT 2017] Java class/Universal Mach-O header: 152
[Mon Oct 09 14:26:20 PDT 2017] Mach-O header: 35
[Mon Oct 09 14:26:20 PDT 2017] OGG header: 20027
[Mon Oct 09 14:26:20 PDT 2017] OLE Compound File header: 67
Complete
Return To Main
1:58 PM
10/9/2017


IO - Imaging
[Mon Oct 09 14:26:20 PDT 2017] BMP header: 156
[Mon Oct 09 14:26:20 PDT 2017] BZip2 header: 125
[Mon Oct 09 14:26:20 PDT 2017] GIF header: 39
[Mon Oct 09 14:26:20 PDT 2017] GZIP header: 24
[Mon Oct 09 14:26:20 PDT 2017] ISO header: 26
[Mon Oct 09 14:26:20 PDT 2017] JPEG header: 970
[Mon Oct 09 14:26:20 PDT 2017] Java class/Universal Mach-O header: 152
[Mon Oct 09 14:26:20 PDT 2017] Mach-O header: 35
[Mon Oct 09 14:26:20 PDT 2017] OGG header: 20027
[Mon Oct 09 14:26:20 PDT 2017] OLE Compound File header: 67
[Mon Oct 09 14:26:20 PDT 2017] OOXML Document header (ZIP): 572
[Mon Oct 09 14:26:20 PDT 2017] PDF header: 20
[Mon Oct 09 14:26:20 PDT 2017] PNG header: 3208
[Mon Oct 09 14:26:20 PDT 2017] RAR header: 19
[Mon Oct 09 14:26:20 PDT 2017] RIFF header: 343
[Mon Oct 09 14:26:20 PDT 2017] TIFF header: 48
[Mon Oct 09 14:26:20 PDT 2017] ZIP header: 59324
[Mon Oct 09 14:26:20 PDT 2017] Imaging Completed Successfully.
Complete
Return To Main
1:58 PM
10/9/2017


SanDisk_Ultra_USB_3_0_USB_Device_report.txt - Notepad
File Edit Format View Help
[Sat Jul 08 14:01:51 EDT 2017] Device Info:
[Sat Jul 08 14:01:51 EDT 2017] Disk: \\.\PHYSICALDRIVE3
Type: Removable Media
Serial: 4C531001400115101042
Model: SanDisk Ultra USB 3.0 USB Device
Size: 30752000000
PNPDeviceID: USBSTOR\DISK&VEN_SANDISK&PROD_ULTRA_USB_3.0&REV_1.00\4C5310014001151010 42&0
Physical Serial: 4C531001400115101042&0
Geometry:
Heads: 255
Cylinders: 3738
Tracks: 953190
Sectors: 60062500
[Sat Jul 08 14:15:30 EDT 2017] Output 60062500 of an expected 60062500 sectors.
[Sat Jul 08 14:15:30 EDT 2017] Completed in 13:38
[Sat Jul 08 14:15:30 EDT 2017] MD5 Hash: 6C54D1C4F20CCB1D2BDE981D397EDA1D
[Sat Jul 08 14:15:30 EDT 2017] SHA1 Hash: 9782798F754C60050134C23255DFC1E9B567404C
[Sat Jul 08 14:15:34 EDT 2017] File count totals:
[Sat Jul 08 14:15:34 EDT 2017] BMP header: 144
[Sat Jul 08 14:15:34 EDT 2017] GIF header: 3
[Sat Jul 08 14:15:34 EDT 2017] GZIP header: 791
[Sat Jul 08 14:15:34 EDT 2017] JPEG header: 40
Ln 20, Col 47
Default Image Path
One Folder Per Device
ION › _ForensicImages › SanDisk_Ultra_USB_3_0_USB_Device_201707081401
Search SanDisk_Ultra_USB_3_0...
ION
_ForensicImages
SanDisk_Ultra_U
libs
Name
Date modified
Type
Size
SanDisk_Ultra_USB_3_0_USB_Device.E01 7/8/2017 2:15 PM E01 File 144,741 KB
SanDisk_Ultra_USB_3_0_USB_Device_magic.txt 7/8/2017 2:15 PM Text Document 52 KB
SanDisk_Ultra_USB_3_0_USB_Device_report.txt 7/8/2017 2:15 PM Text Document 2 KB
3 items 1 item selected 1.16 KB
1:58 PM
10/9/2017

LOGGING OVERVIEW

- 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)

CIPHER TECH SOLUTIONS

TRIAGE

- **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

Traditio[illegible]  **[illegible]sing Track**

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

CIPHER TECH SOLUTIONS

TIMELINES

Acquire Media

Imaging

Triage

Further Examination

Additional Intel Report

Traditional Media Processing Track

Acquire Media

Configure Tool

Imaging

Transfer Image

Triage

Further Examination

Additional Intel Report

ENGAGEMENT

- IO is open-source, fully tested, and is completely free to use and modify
- Cipher Tech will release updates as core functionality is improved

CIPHER TECH SOLUTIONS

ENGAGEMENT

- 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

CIPHER TECH SOLUTIONS

CONTACT INFO

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