Automating the Computer Forensic Triage Process With MantaRay

Senior Computer Forensic Analysts– Doug Koster & Kevin Murphy

Worlds best Summer Intern – Chapin Bryce

Open Source Forensics Conference– November 5, 2013

www.mantarayforensics.com

MantaRay Team

* Doug Koster
  * 13 years of experience in computer forensics
  * MS in Computer Science, MBA
  * EnCE, GCFA, GCFE, A+, PMP
  * Programming experience in Perl & Python
* Kevin Murphy
  * 11 years of experience in computer forensics
  * BS in Computer Forensics (Champlain College)
  * EnCE, A+
  * Shell scripting & Python
* Chapin Bryce
  * Pursuing BS Degree in Computer Forensics (Champlain College)
  * Web Master / System Tester / Researcher

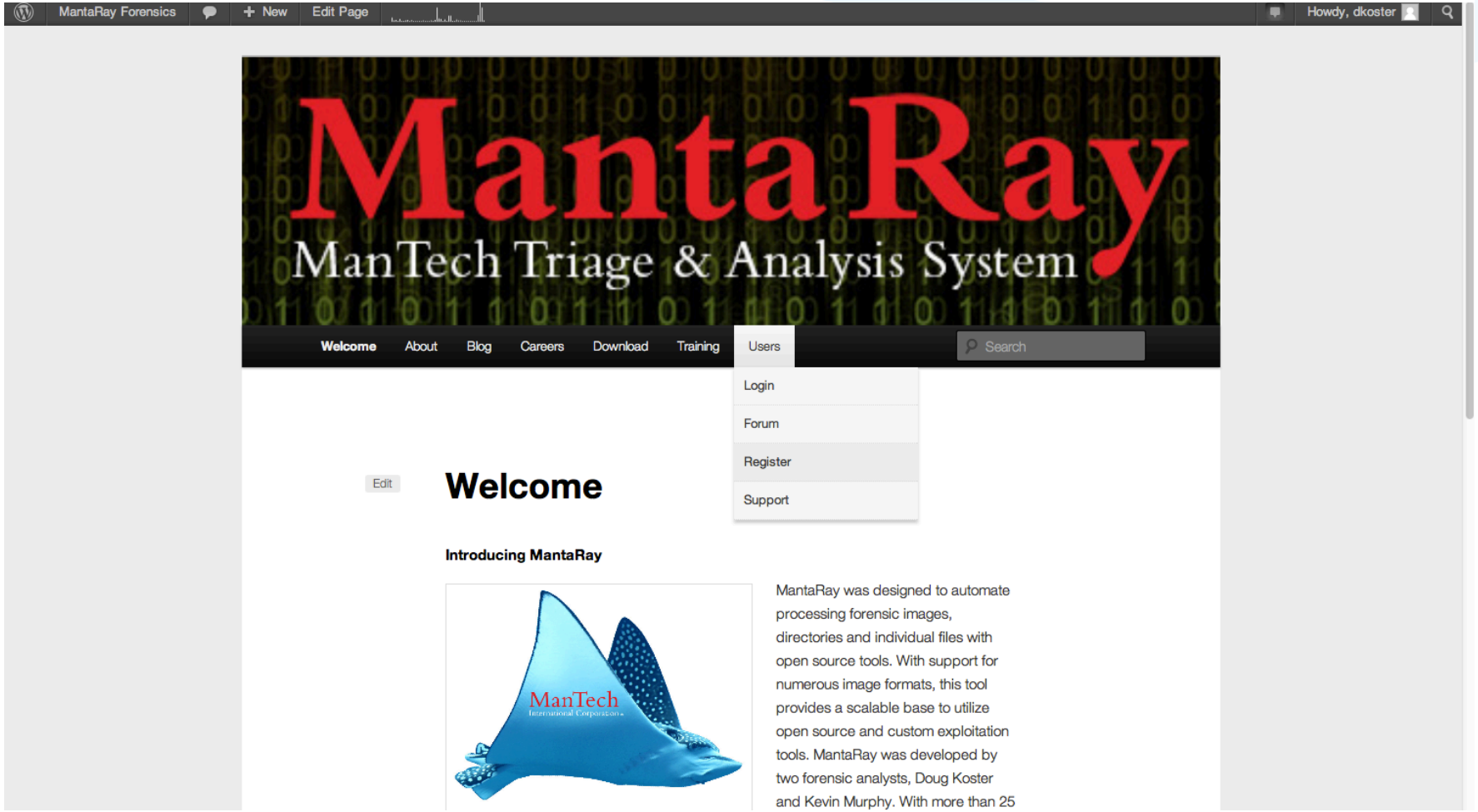
Background

* We are forensic examiners
  * We happen to know some scripting languages
  * Not professional programmers
* Spent entire careers as government contractor employees
* High volume of media
* Bulk processing to identify interesting forensic artifacts
  * "See if there is anything bad on this media"

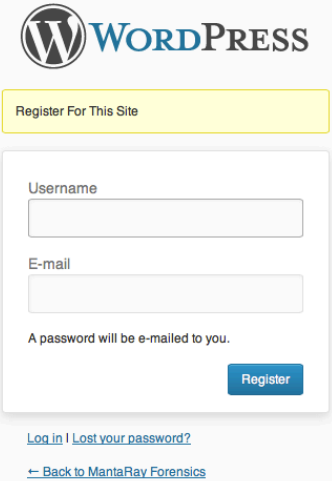
What is MantaRay?

* MantaRay – ManTech Automated Triage System
  * Set of Python modules that automate a number of open source forensic tools
  * Will be bundled into the upcoming SIFT 3.0 (release date November 2013 – fingers crossed)
    * http://computer-forensics.sans.org/community/downloads
  * Designed to allow examiner to select multiple tools, set options for each, click go and walk away
  * Website for updates, blog posts, user forum
    * www.mantarayforensics.com

Creating User Account: Click Register on Website under Users



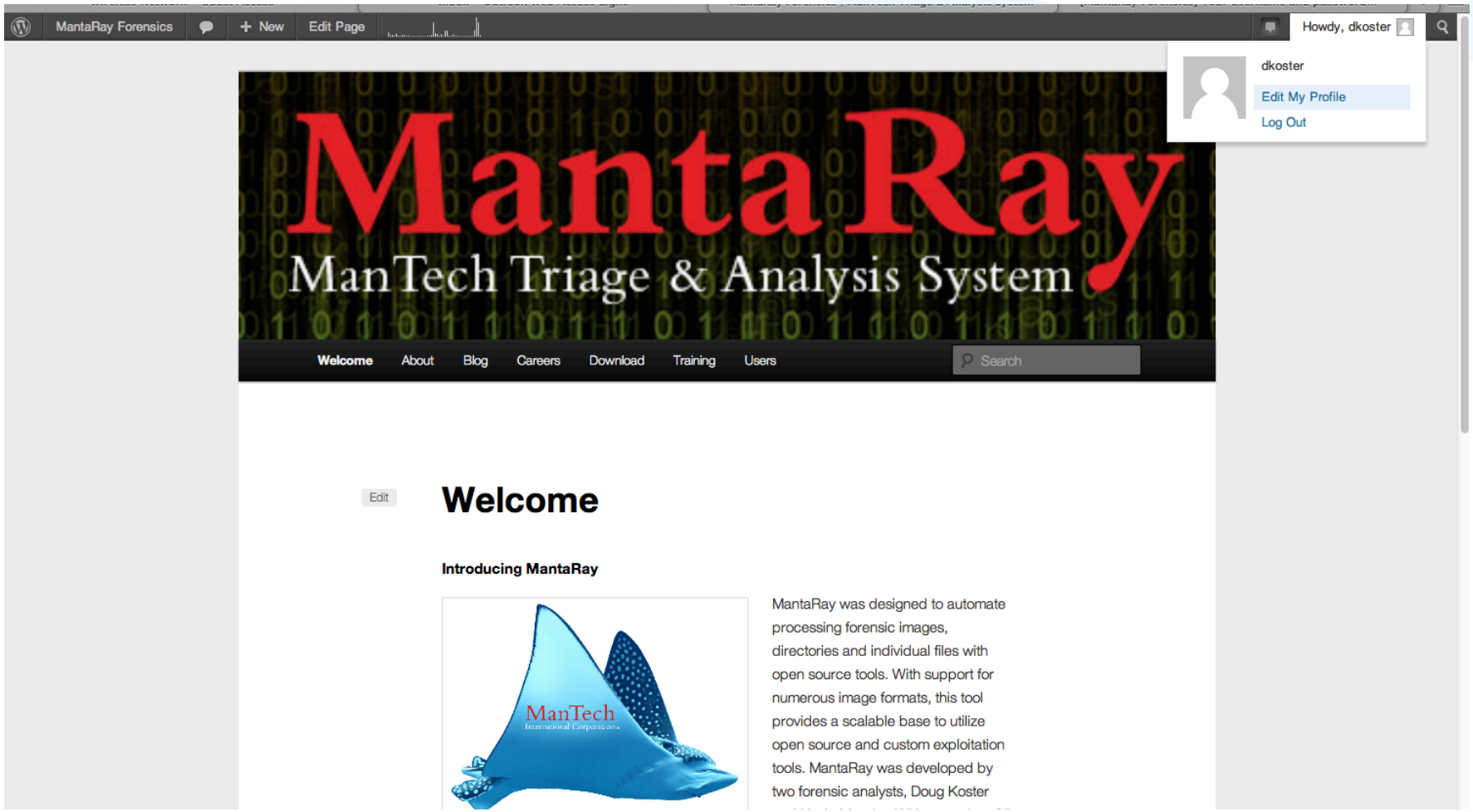
Set up Username & Email



Login with temporary password

* Your password will be sent to the email you registered with
* Logon with your password
* To change password, left click on your username in upper right hand corner and select “Edit Profile”

Edit Profile to change password



Triage Steps Automated by MantaRay

1. Creating a Super Timeline
2. Running Bulk_Extractor
3. Extracting Registry Hives & running RegRipper
4. Extracting EXIF Data
5. Carving Unallocated space
6. Scanning for high entropy files
7. Review RAM using Volatility
8. Extract GPS data from JPEGs and create .KML file
9. Extract Jumplist data
10. Extract NTFS system files
11. Process user selected .plist files

Registry Processing

* MantaRay is a triage tool
  * We want to get a quick look at all the data on the drive of interest
  * What is “Of Interest”????? -> User interaction with the system
    * One gold mine for this type of information is the Windows Registry
  * MantaRay extracts ALL registry hives from a system
    * OVERT
    * DELETED
    * UNALLOCATED
    * RESTORE POINTS
    * SHADOW VOLUMES

Extracted Registry Hives

* How many Overt Registry Hives do we typically run regripper against:
  * NTUSER.dat for each profile
  * SYSTEM hive
  * SOFTWARE hive
  * SECURITY hive
  * SAM hive
  * USRCLASS for each profile
* What are we not seeing:
  * Deleted registry hives
  * Hives in Unallocated
  * Hives in Shadow Volumes (Vista/Win7)
  * Hives in Restore Points (XP Systems)

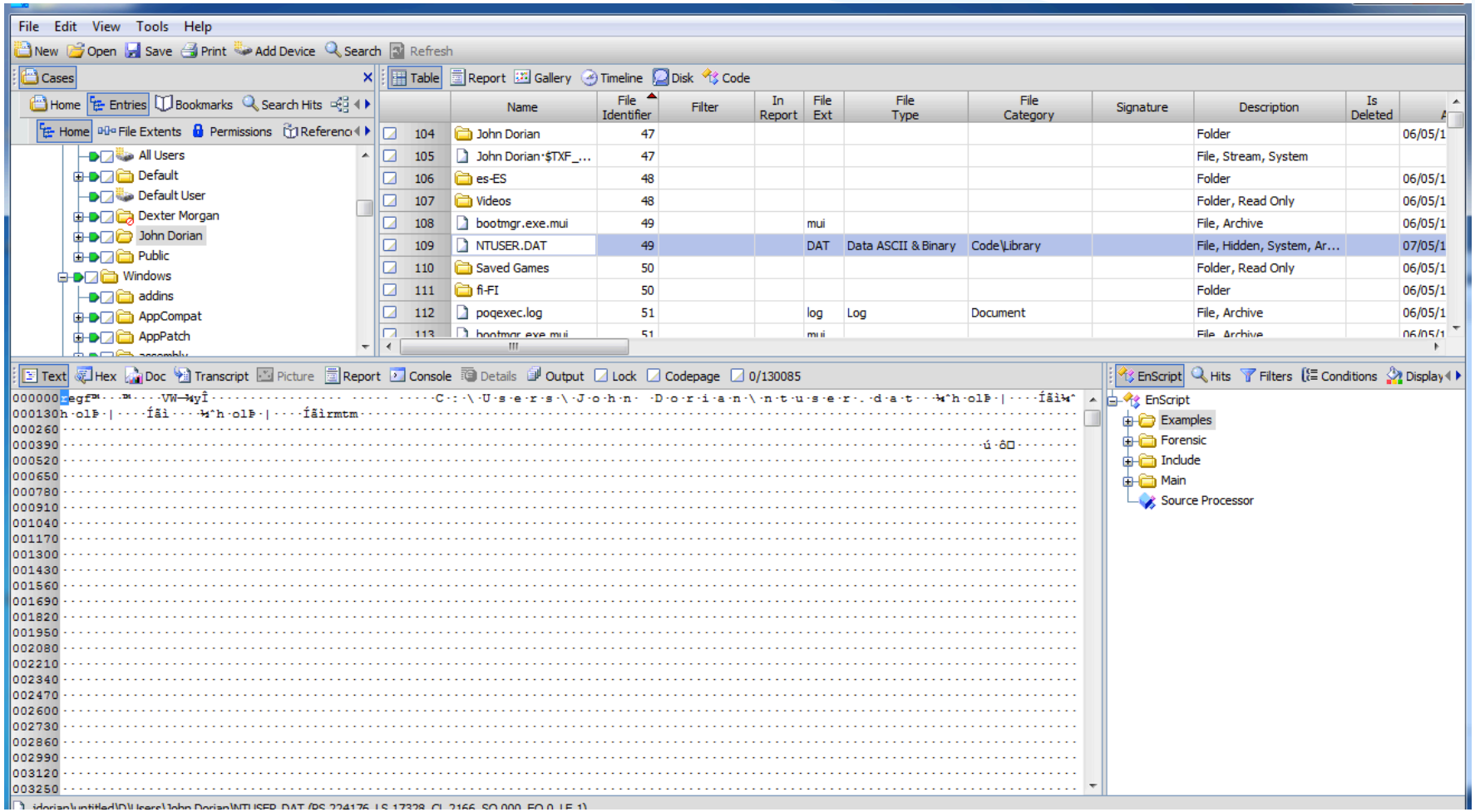
Extracted Registry Hives

* NTUSER & USRCLASS hives are named with their Windows profile names in the filename
  * For Overt, Deleted, Shadow Volumes & Unallocated
  * Allows for quick triage of users that had accounts on the system
* Time/date stamps for the hives are set to the last modified time, so that the regripper output can be organized by time
  * The last access time of a registry hive is contained in the hives header

Extract Registry Hive Output

* Making sense of scripts output:
  * **49-128-1_Partition_105906176_OVERT_John Dorian_NTUSER.DAT**
    * **49-128-1** -> Inode number of the file in the filesystem
      * **49** is the File Identifier in Encase. This number can be duplicated between partitions, so make sure you only green homeplate the partition beginning at the offset specified
    * **Partition_105906176** -> offset of the partition this file was located in
    * **OVERT** -> this hive was an OVERT file
    * **John Dorian** -> Windows Profile Name
    * **NTUSER.DAT** -> type of hive

Finding Inode number in Encase



Extract Registry Hive Output

* Making sense of script output
  * **49-128-1_Partition_0_SHADOW_VOLUME_vss1_OVERT_John Dorian_NTUSER.DAT**
    * **49-128-1** -> Inode number of the file in the filesystem
    * **Partition_0** -> offset of partition file was located in (since this file was extracted from a shadow volume, the Partition offset is showing that the shadow volume was mounted with an offset of 0 bytes)
    * **SHADOW_VOLUME** -> this file was located in a Shadow Volume
    * **Vss1** -> shadow volume number the file was found in
    * **OVERT** -> this hive was an OVERT file within Shadow Volume
    * **John Dorian** -> Windows Profile Name
    * **NTUSER.DAT** -> type of hive

Extract Registry Hive Output

* Making sense of scripts output:
  * **Partition_105906176_Unallocated_28119360.dat_systemprofile_NTUSER.DAT**
    * **Partition_105906176** -> offset of the partition this file was located in
    * **Unallocated** -> this hive was carved from unallocated using foremost
    * **28119360.dat** -> this is the filename from foremost (cluster offset)
    * **systemprofile**-> Windows Profile Name
    * **NTUSER.DAT** -> type of hive

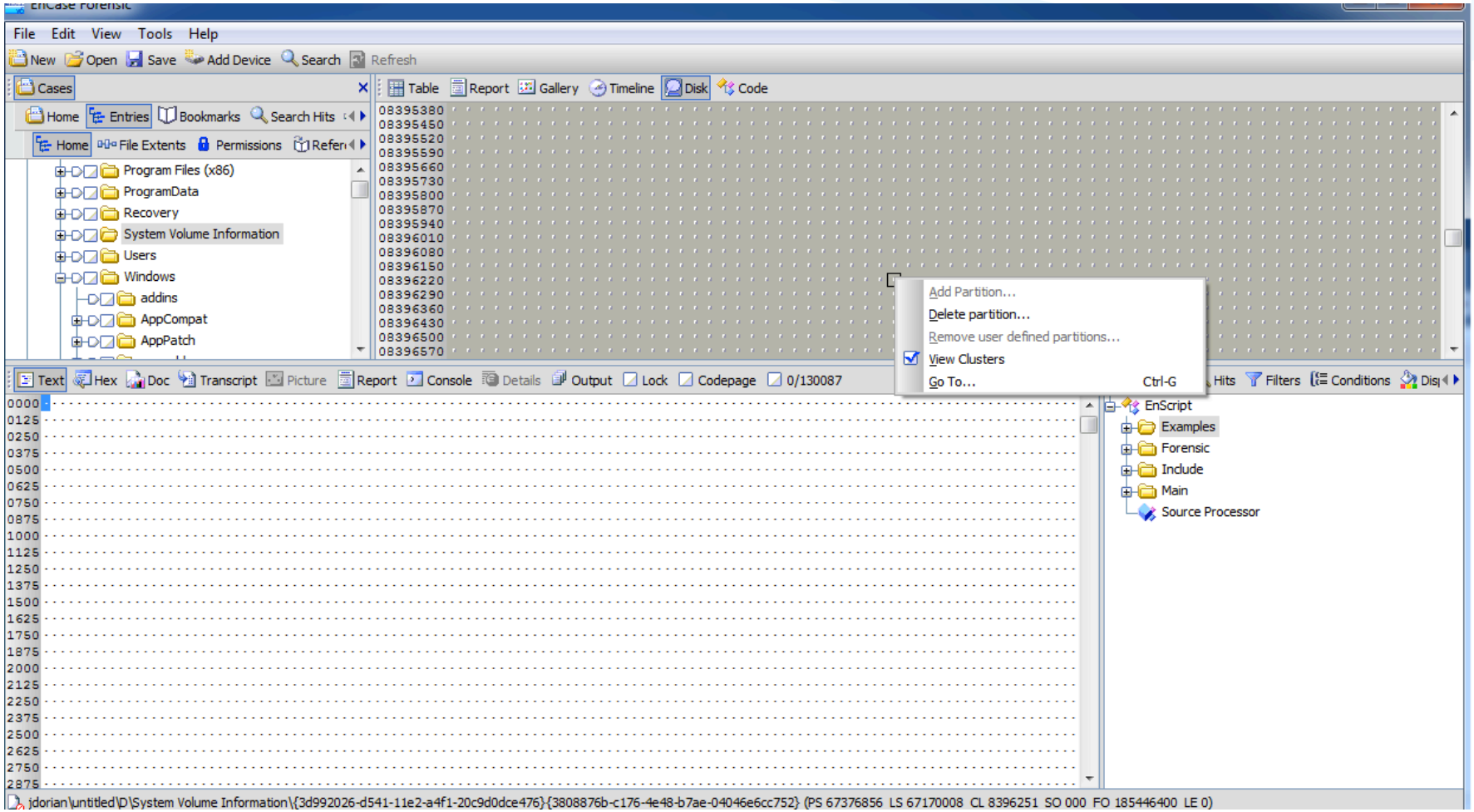
Finding files carved by Foremost

* If you need to find a file carved with Foremost using another forensic tool, follow these steps:
  * Use fsstat to calculate the cluster size for your disk image (items in red are variables that will vary depending on the specifics of each disk image)
    * Fsstat –f <partition filesystem> -i <image type> -b <block size> -o <partition offset> <disk image> | grep 'Cluster Size:' | awk '{print $3}' | sed s/-bytes//
    * Fsstat –f ntfs –i raw –b 512 –o 206848 /mnt/test/ewf1 | grep 'Cluster Size:' | awk '{print $3}' | sed s/-bytes//
    * Results in cluster size of 4096

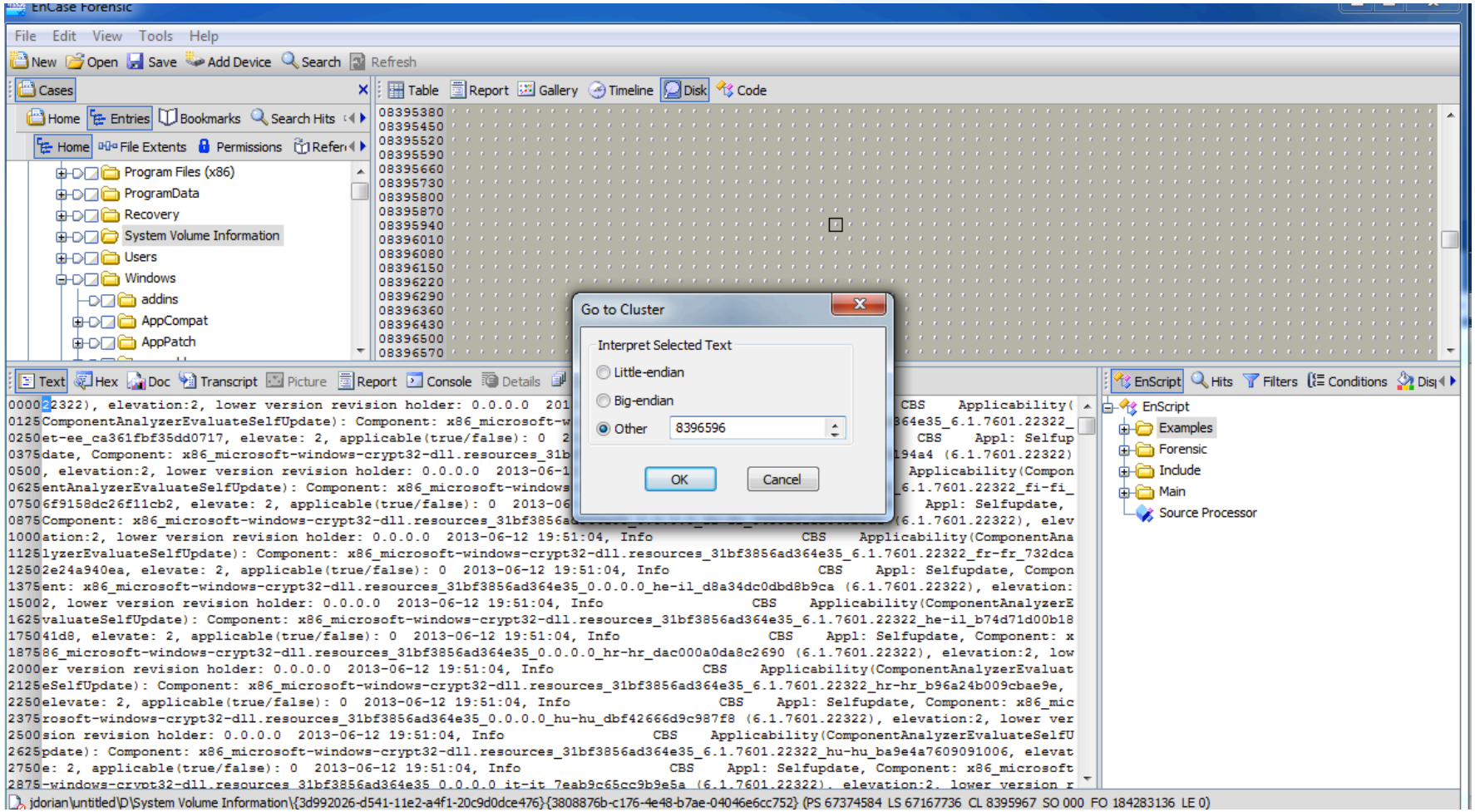
Finding files carved by Foremost

* Run blkcalc:
  * The cluster offset of your file is calculated as follows: foremost_file_offset/block_size (14399160320/4096=351420)
    * The foremost file offset is located in the audit.dat text file in the Extracted Registry Hives folder
    * Blkcalk –u <cluster offset of file> -f <file system> -I <type of image> -b <block size> -o <offset of partition> <path to image file>
    * Blkcalc –u 3515420 –f ntfs –I raw –b 512 –o 206848 /mnt/test/ewf1
    * Results in Cluster offset of **8396596**

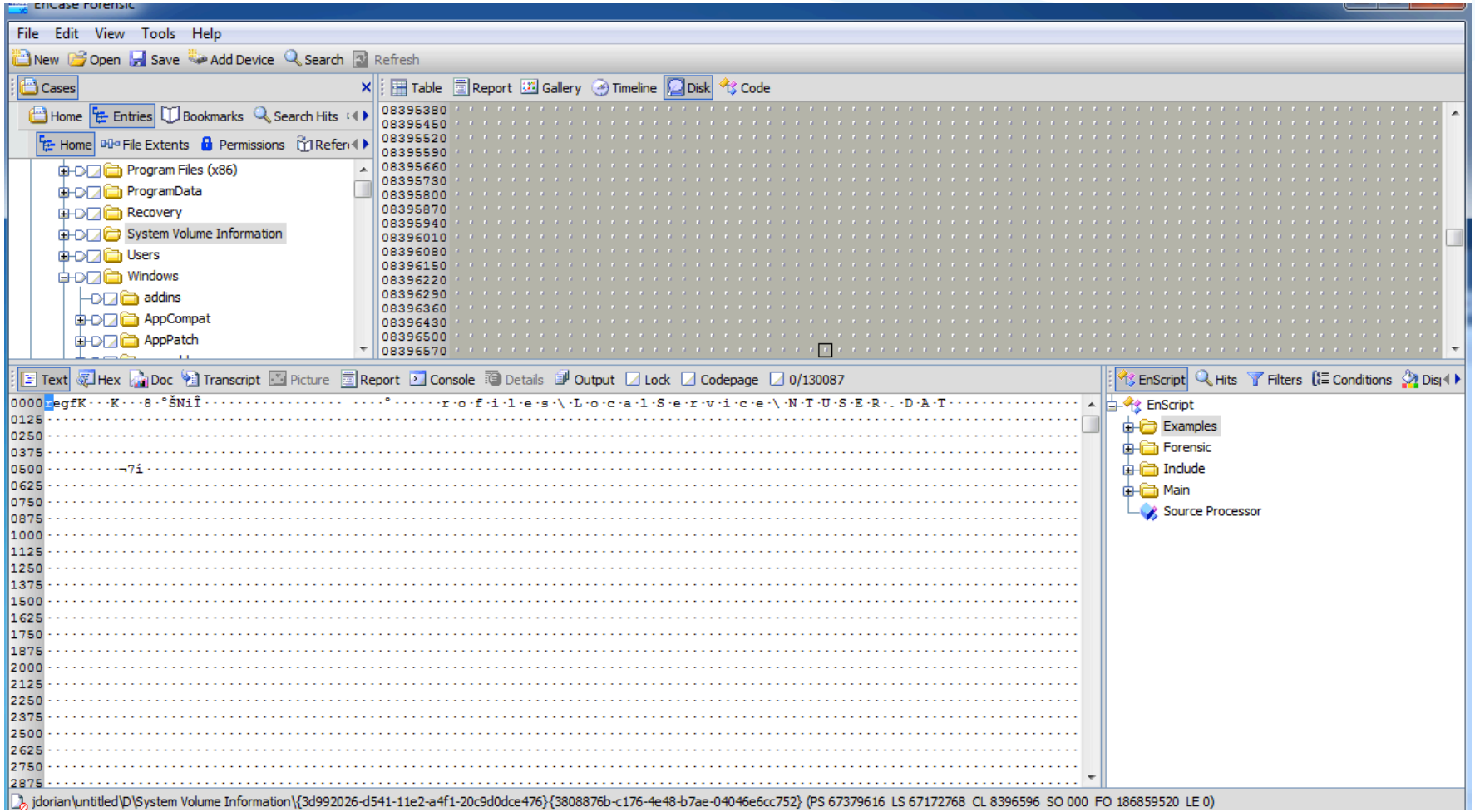
Finding files carved by Foremost



Finding files carved by Foremost



Finding files carved by Foremost



Processing Memory images w/ Volatility

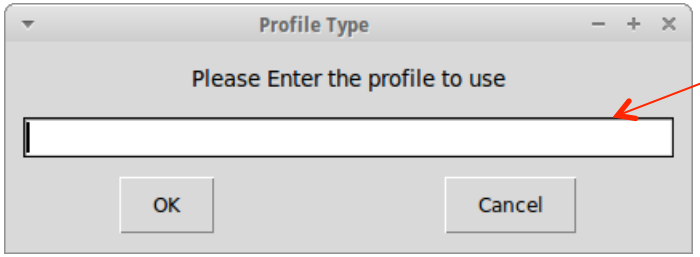
Volatility – v2.3

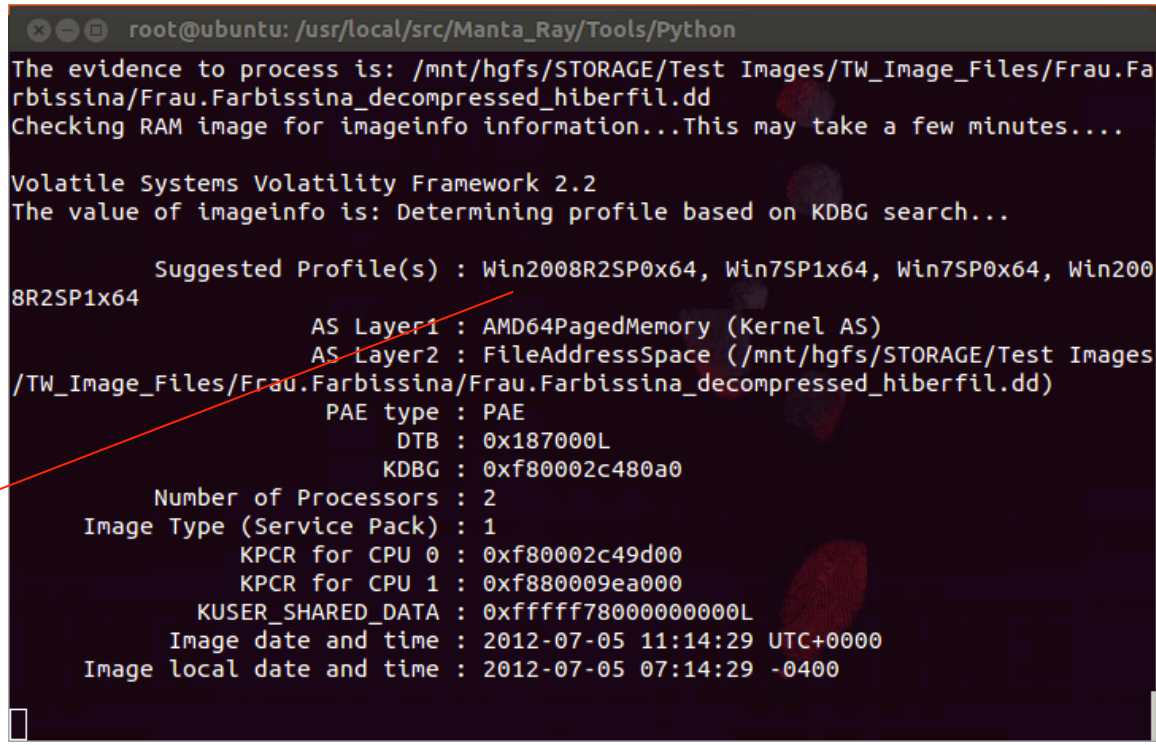
* Open source tool for artifact extraction from memory images
* https://www.volatilesystems.com/default/volatility/
* Can be run against RAM images or decompressed hiberfil.sys
* Methods of decompressing hiberfil.sys
  * Blade v1.9
  * X-Ways Forensics
  * Moonsols
  * Volatility
    * Use *imagecopy* command to convert hiberfil.sys into DD image
    * https://code.google.com/p/volatility/wiki/CommandReference#hibinfo

Volatility

MantaRay volatility script

* Wait for script to provide “Suggested Profiles”choices
* Paste choice into text box
* Review output





Extract NTFS Artifacts

* Mantaray will automatically extract the following files for each partition:
  * $MFT
  * $LOGFILE
  * $USRJRNL
* These scripts are required if you want to run David Cowen's Advanced NTFS Journal Parser
  * http://hackingexposedcomputerforensicsblog.blogspot.com/2012/11/pfic-2012-slides-bsides-dfw.html
  * http://www.youtube.com/watch?v=0b05Qeb9rHA

Plist Processor

* Plist Processor -> prints data from selected plist files into single output file
* What is a plist??? -> .plists are the Mac equivalent of the Windows Registry
  * Processes all types of plist files:
    * Binary
    * XML
    * Text
  * Base64 data is decoded
  * Plist files listed in /usr/local/src/Manta_Ray/docs/plists_to_process.txt
    * Add the filename for any additional plists you want to process

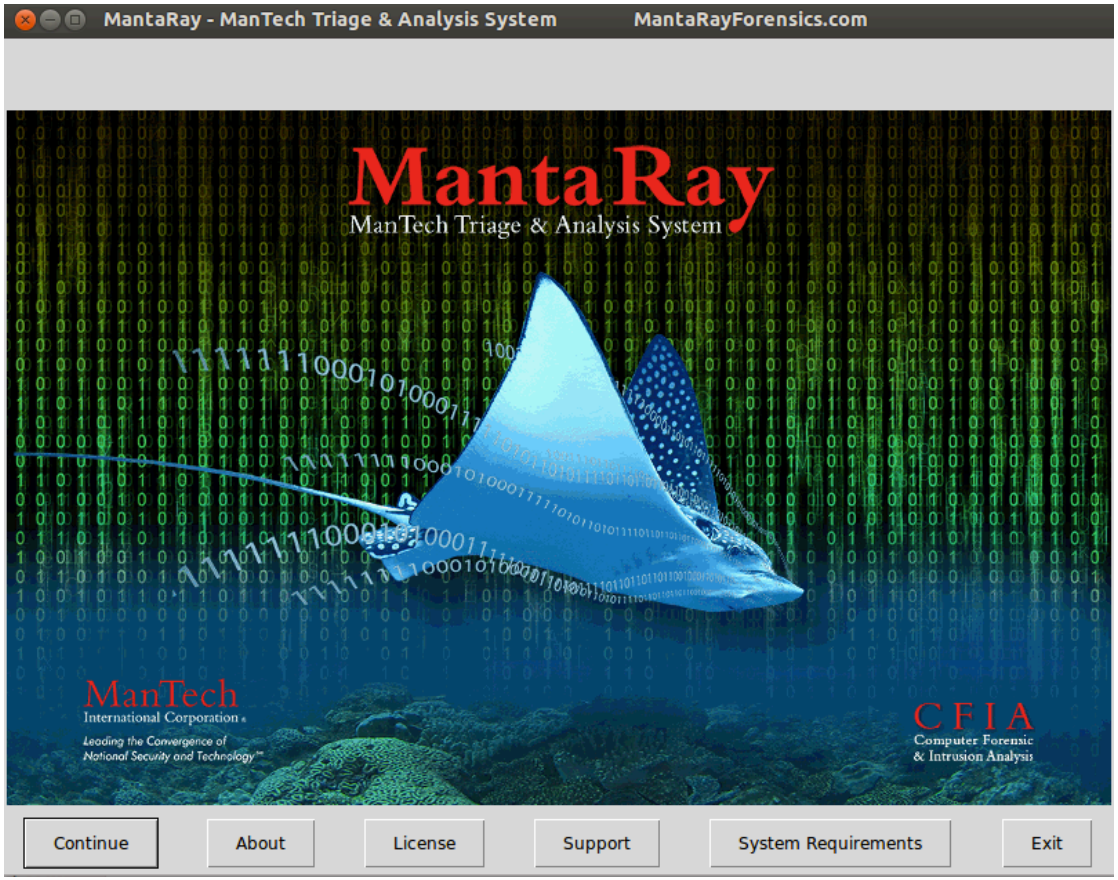
MantaRay Workflow

* Workflow is cyclical
* Run MantaRay against target media
* Then you can re-run various tools via MantaRay against the MantaRay output:
  * Ex -> run MantaRay against disk image and Extract Registry Hives
    * Then if there is a specific user you are interested in you can copy those hives into a folder and run bulk_extractor (via MantaRay) against the folder to get a good idea of what that particular user was doing
    * You can also create a supertimeline from the extracted registry hives and then merge that timeline into the supertimeline for your entire drive
* Pull MantaRay output into Encase as single files and then run your keywords against all the output

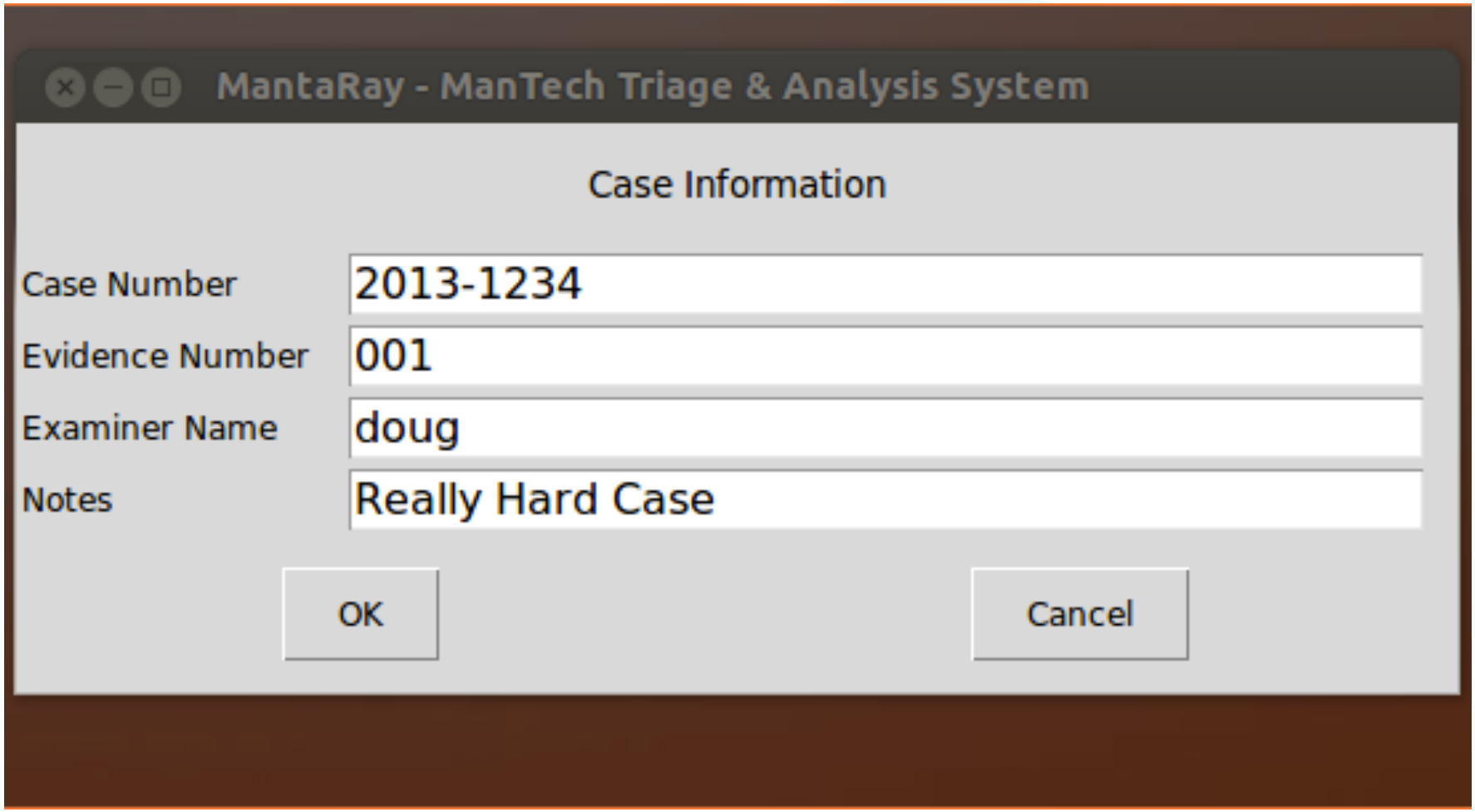
SIFT 3

* Will be available for download (hopefully soon) from sans.org
  * http://computer-forensics.sans.org/community/downloads
* MantaRay will be bundled into SIFT 3.0
* Updates to MantaRay will be available at www.mantarayforensics.com

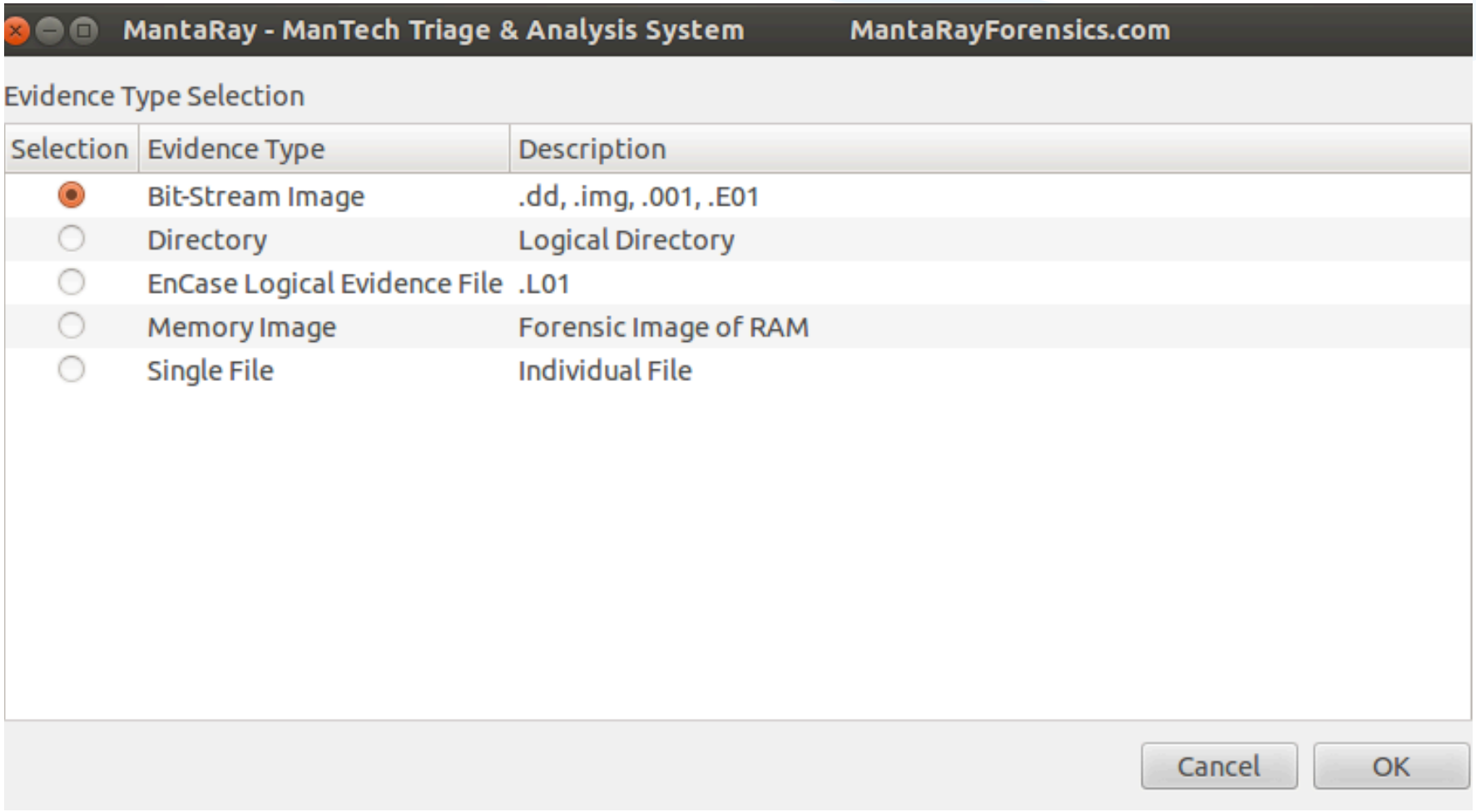
Demo


MantaRay - ManTech Triage & Analysis System
MantaRayForensics.com
MantaRay
ManTech Triage & Analysis System
ManTech
International Corporation
Leading the Convergence of
National Security and Technology
CFIA
Computer Forensic
& Intrusion Analysis
Continue
About
License
Support
System Requirements
Exit

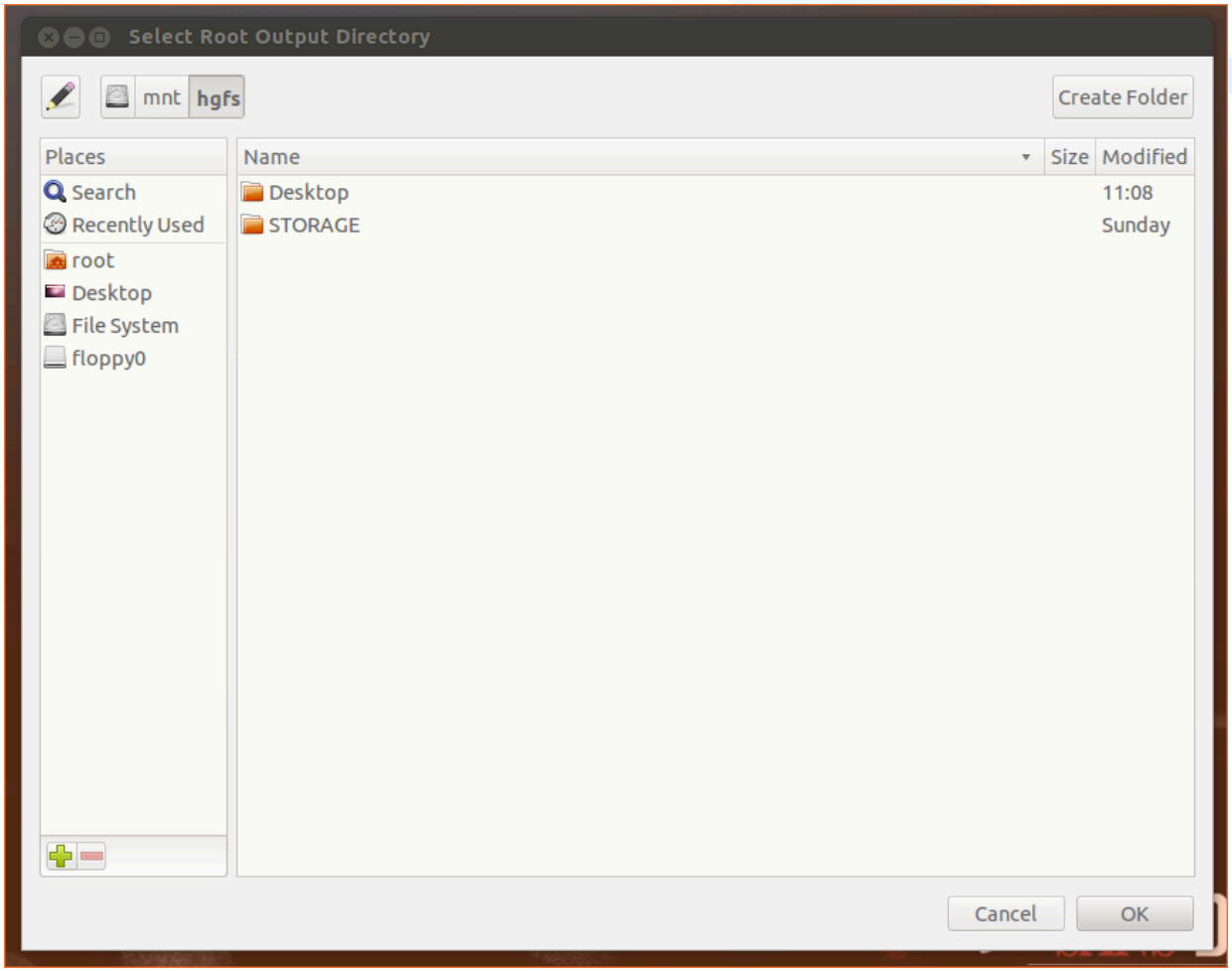
Enter Case Information



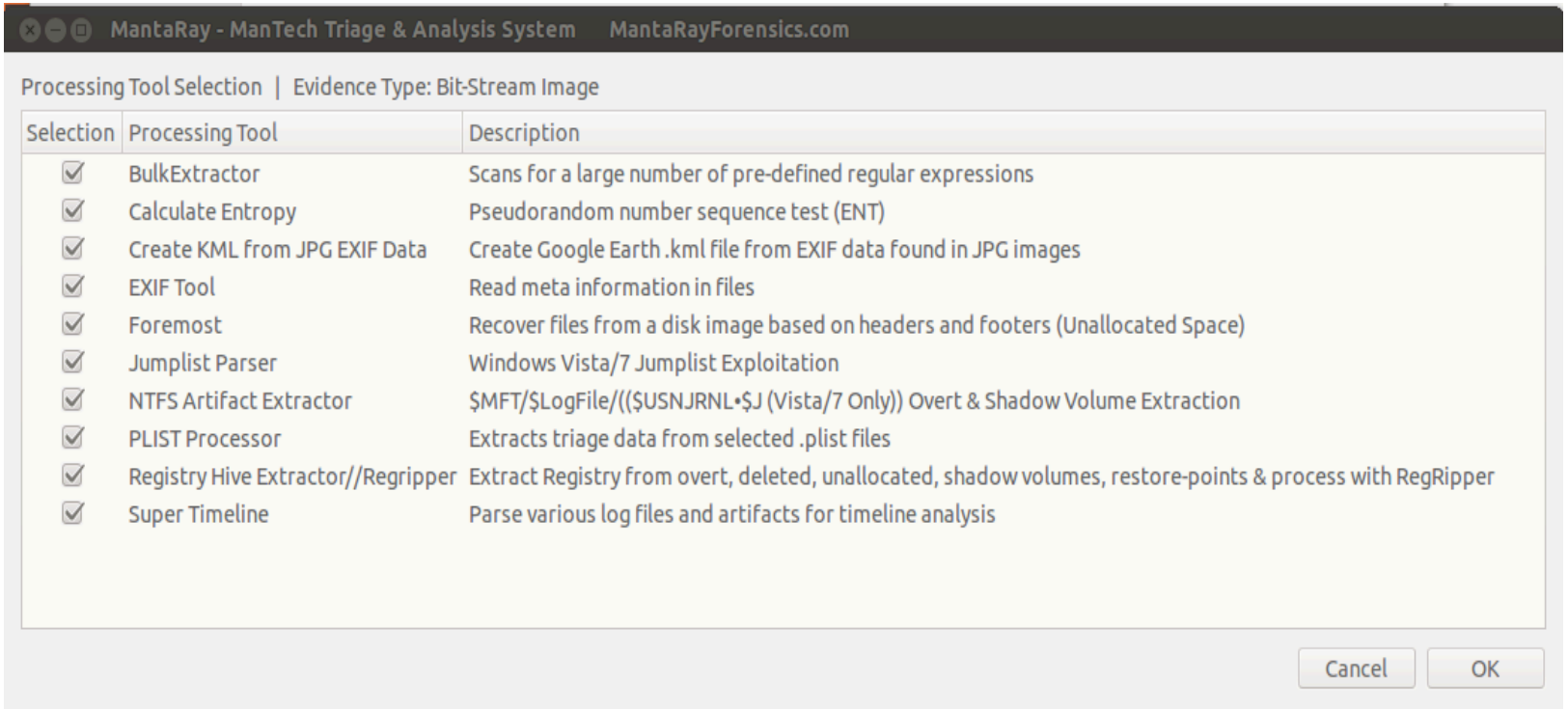
Select Evidence Type



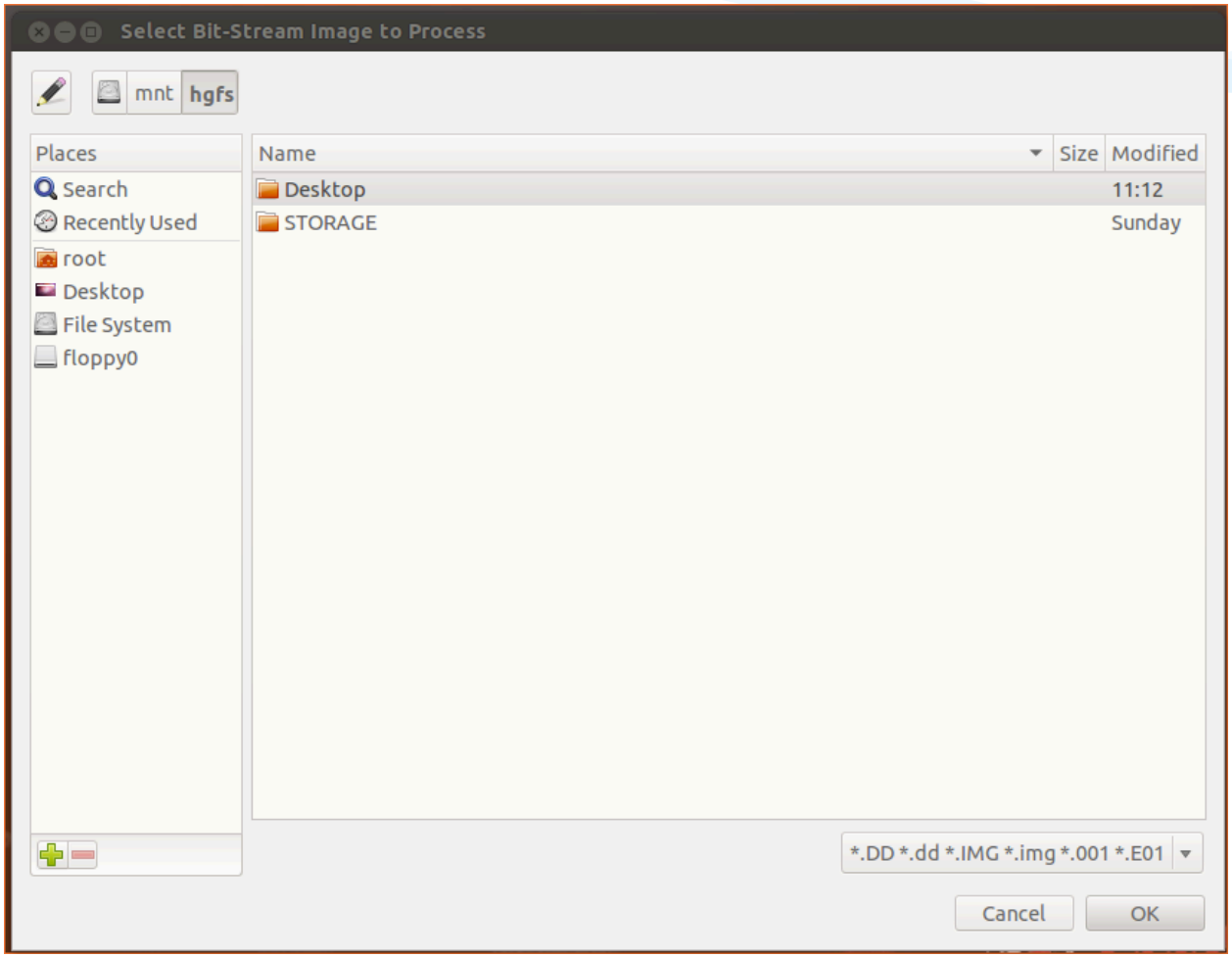
Select Output Directory



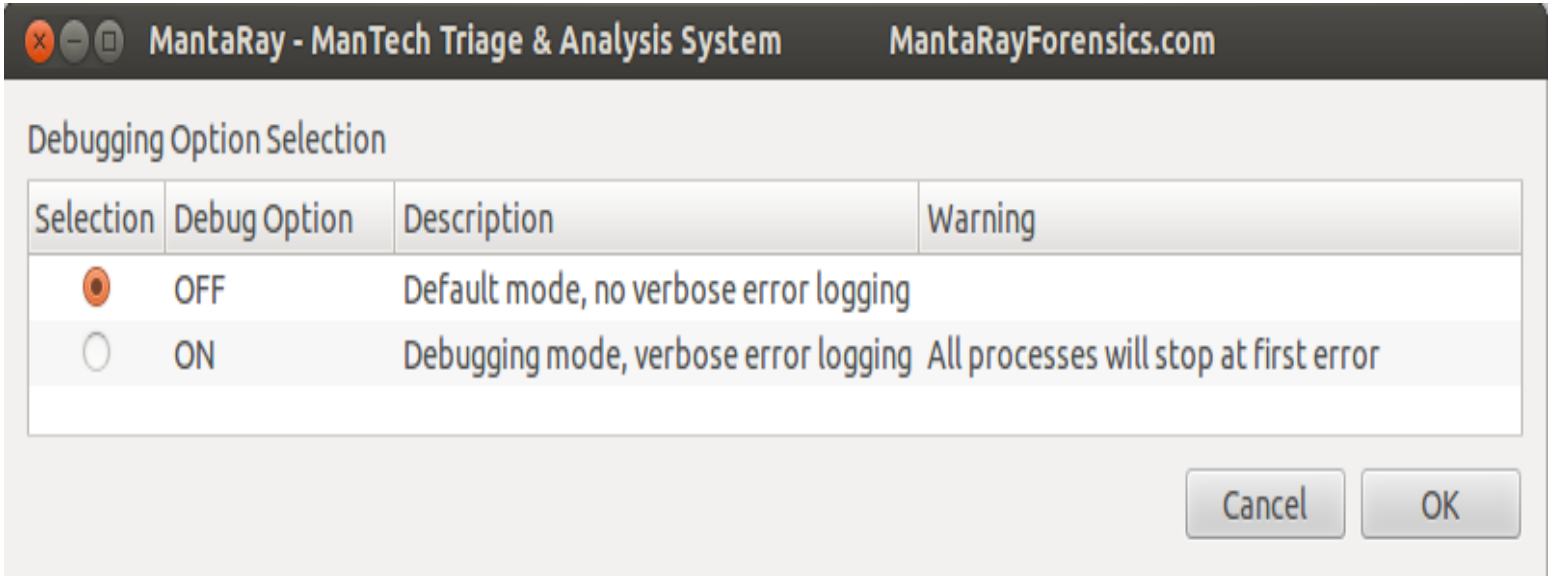
Select tools to run



Select Evidence to Process

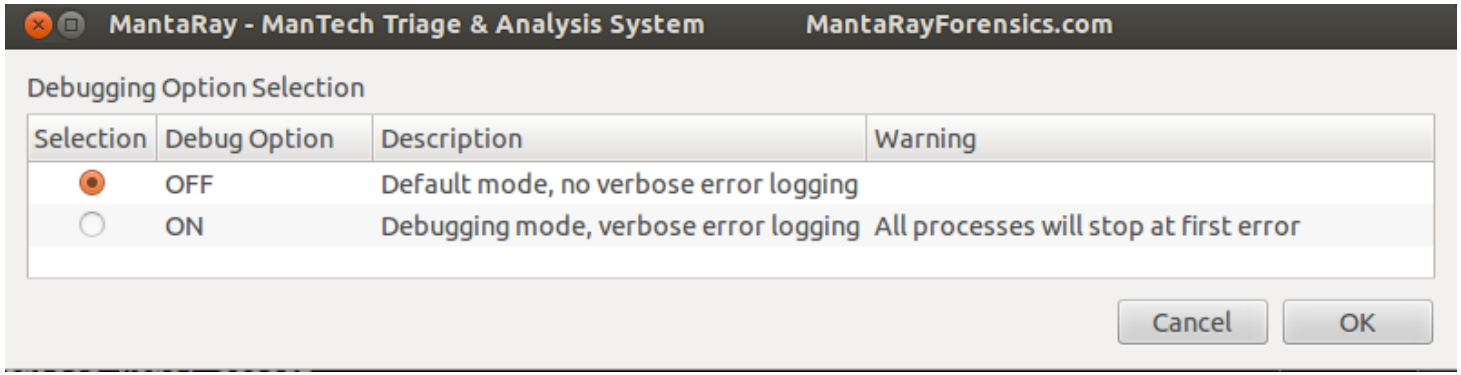


Select Debug Mode Setting

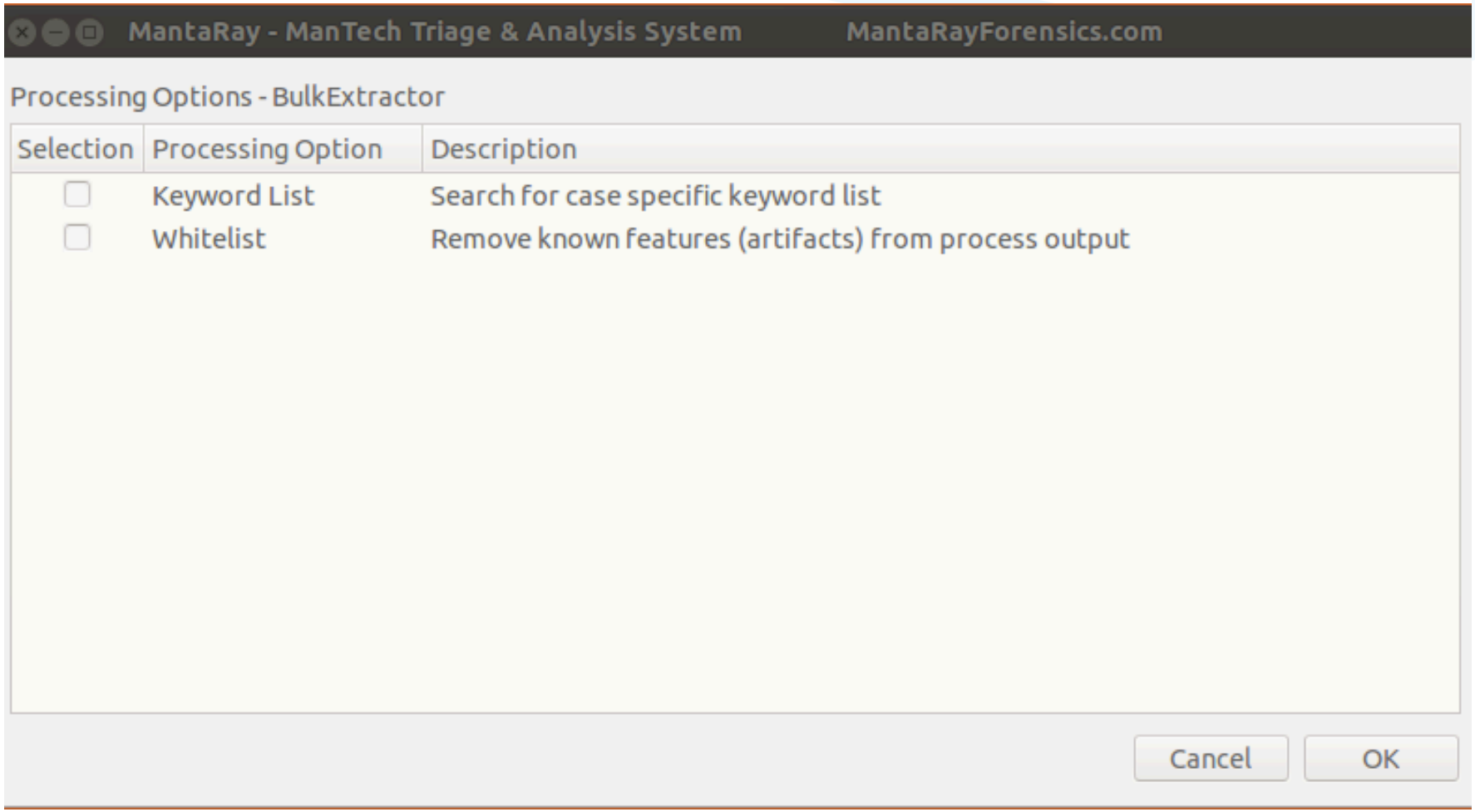


Debug Mode

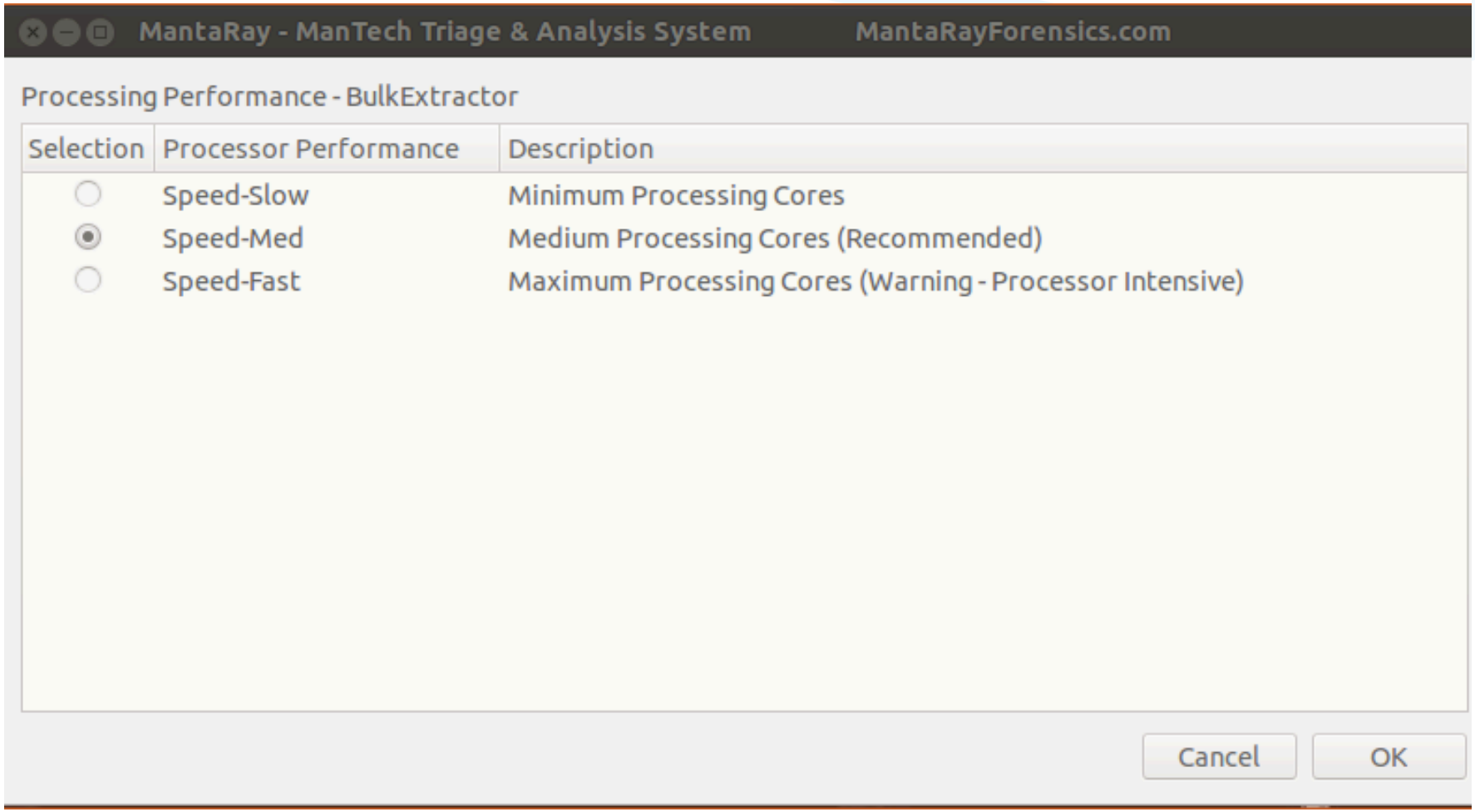
* GUI Option (Default OFF)
* When set to ON the program will exit when it hits an error and print error to screen.
  * If you need to run with Debug Mode ON then run from command line (otherwise terminal will close after error)
* sudo python3 /usr/local/src/Manta_Ray/Tools/Python/Manta_Ray_Master_GUI.py



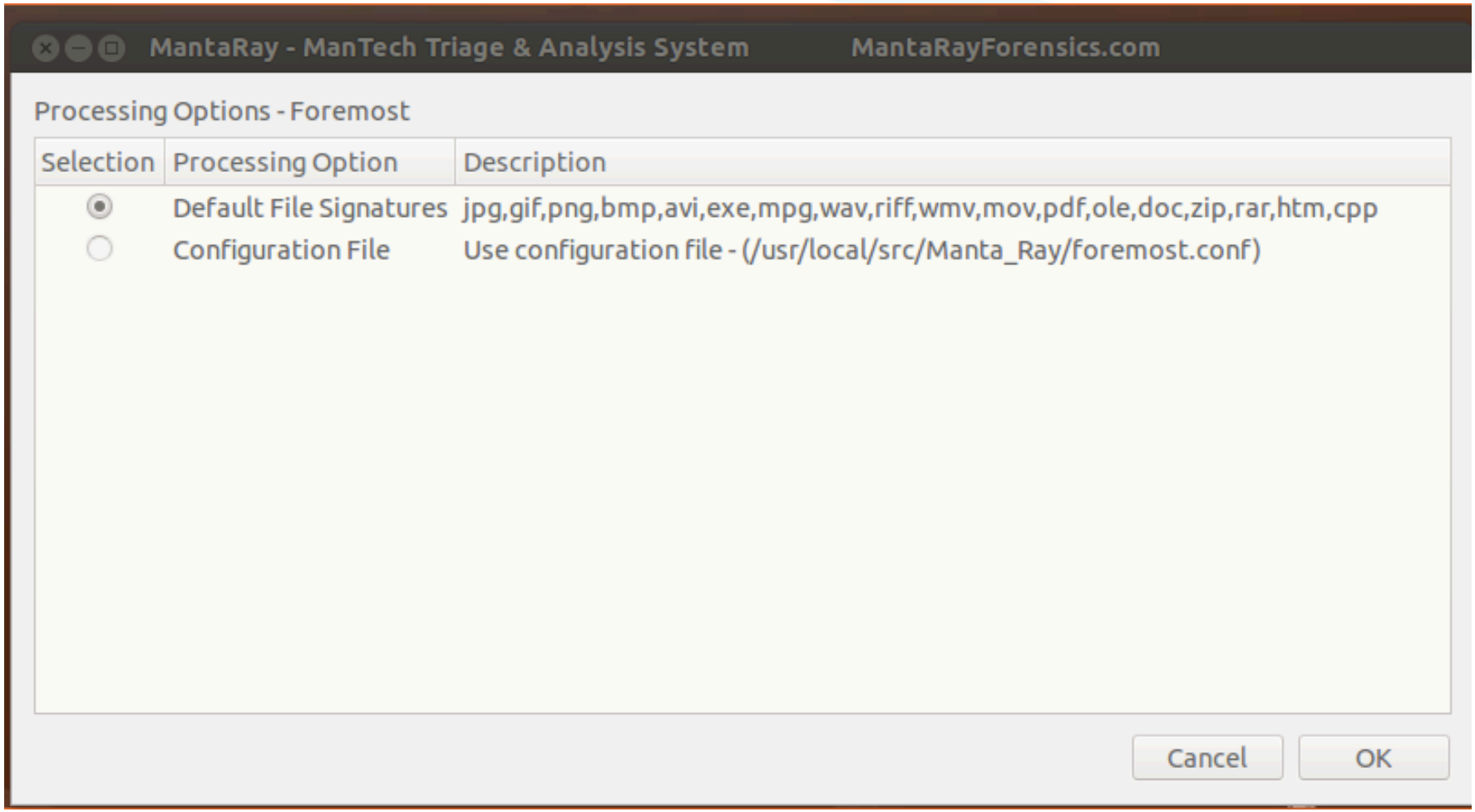
Select Bulk Extractor Options



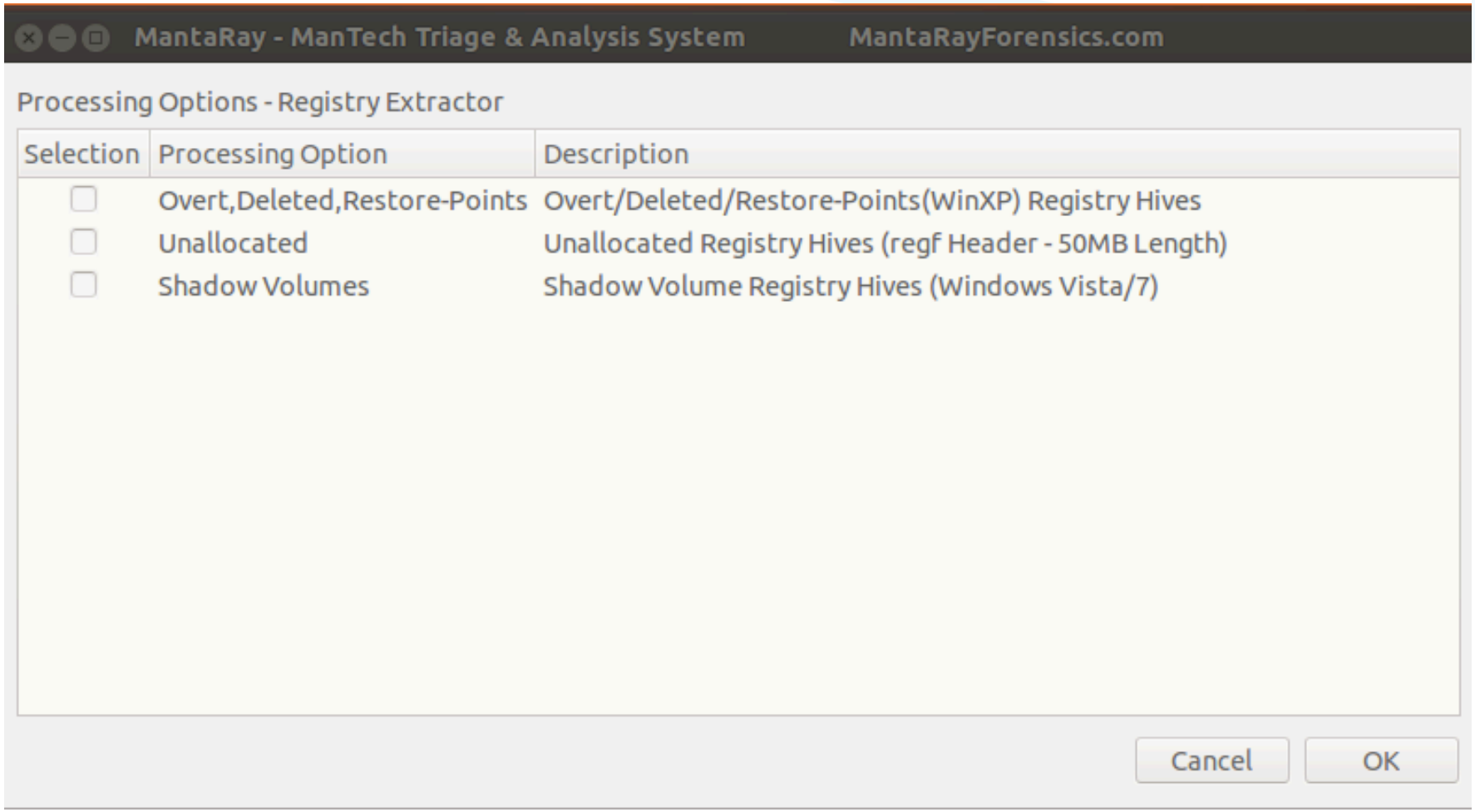
Select Bulk Extractor Speed



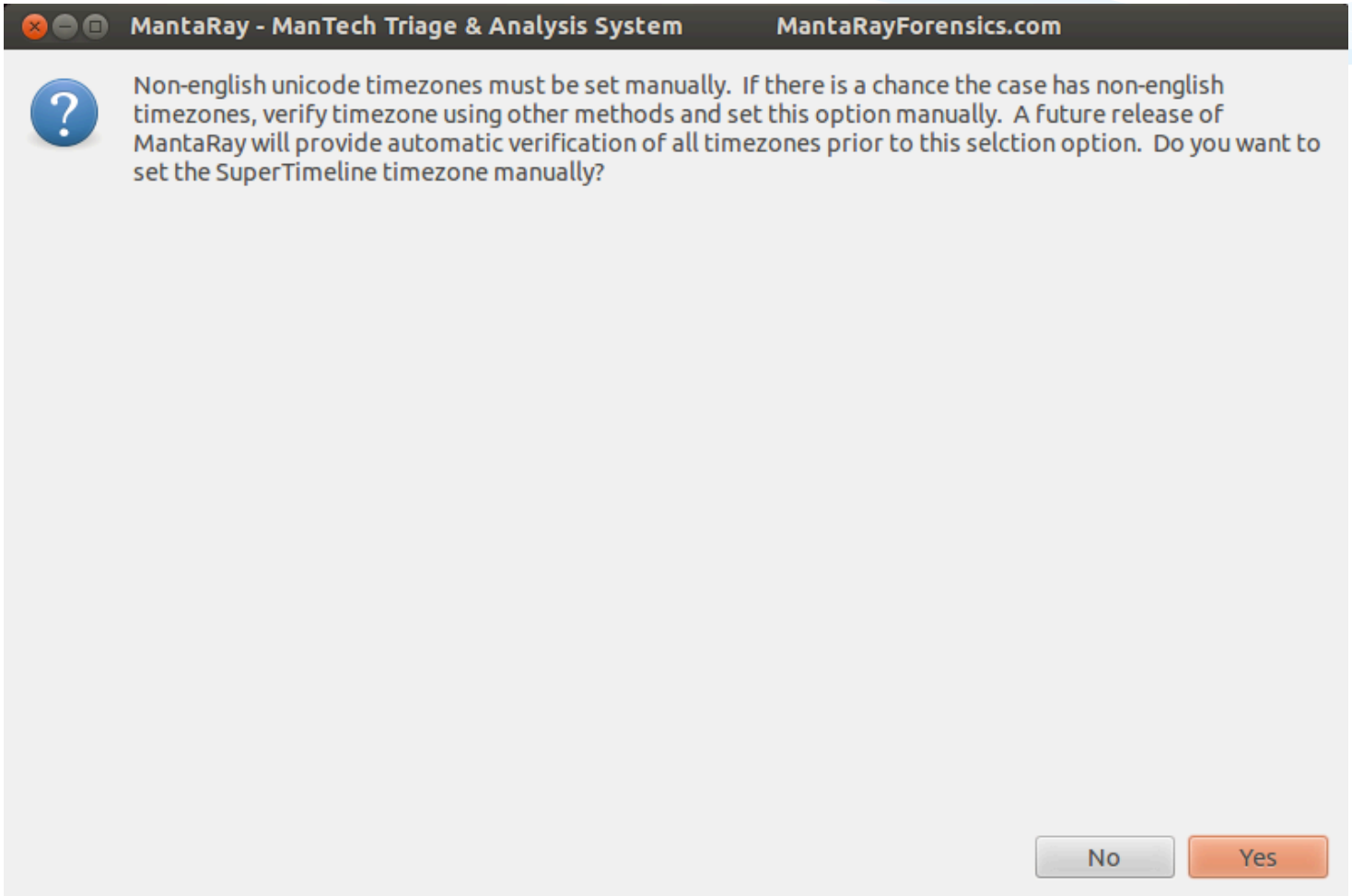
Select Foremost signatures



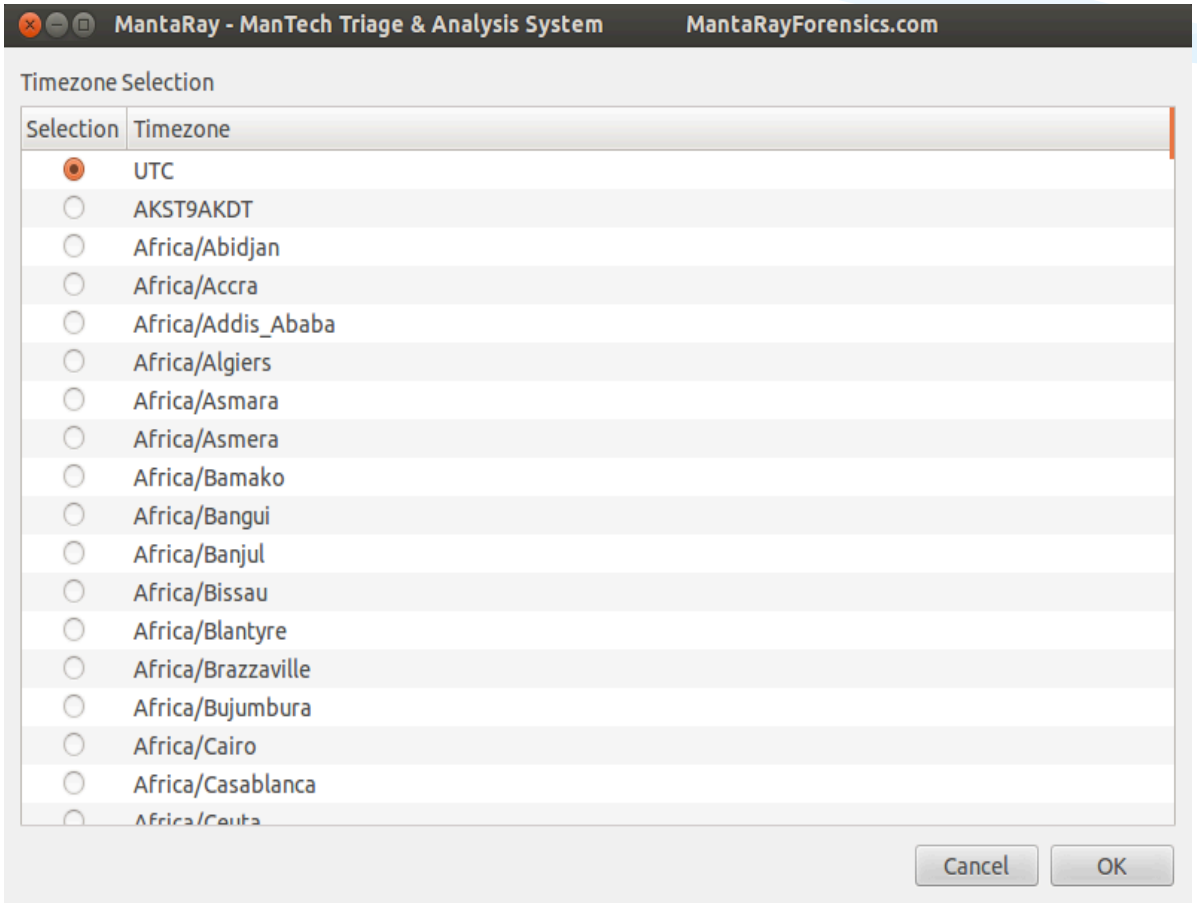
Select Registry Hives to Extract



Set time zone manually?



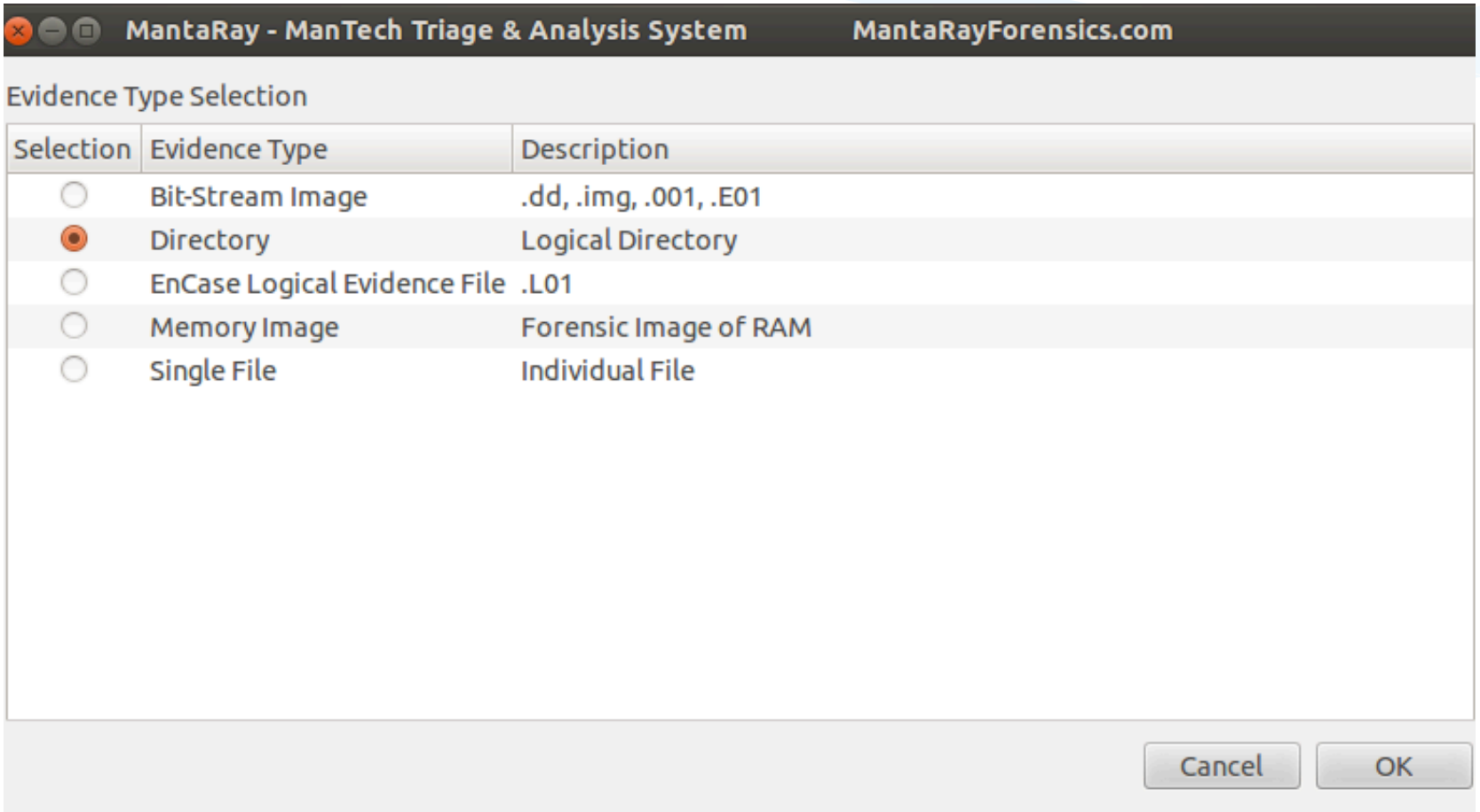
Manual time zone selection



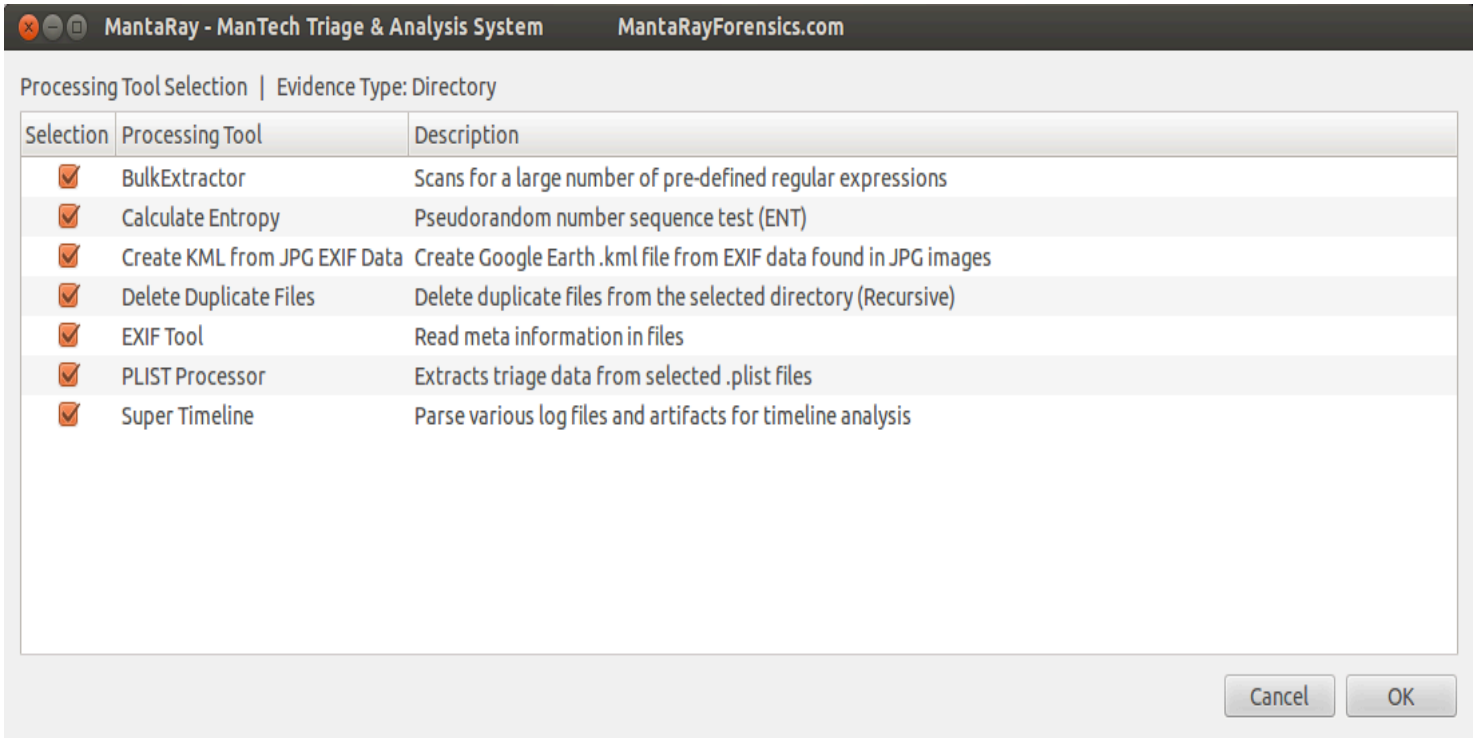
Processing Begins

```
Terminal
Timezone Option: UTC
BulkExtractor
This VM has 4 cores
Item to process is: Bit-Stream Image
Case number is: 2013-1234-001-MantaRay_2013-08-06_11_06_13_586314
Output folder is: /mnt/hgfs/STORAGE/MantaRay/2013-1234-001-MantaRay_2013-08-06_1
1_06_13_586314
Evidence type is: "/mnt/hgfs/STORAGE/Test Images/xp dblake.dd"
Whitelist location is: NONE
Processing speed is: Speed-Med
Keyword list is: NONE
The be command is: bulk_extractor -o "/mnt/hgfs/STORAGE/MantaRay/2013-1234-001-M
antaRay_2013-08-06_11_06_13_586314/Bulk_Extractor_Results" -j 2 "/mnt/hgfs/STORA
GE/Test Images/xp dblake.dd"
bulk_extractor version: 1.4.0-beta4
Hostname: ubuntu
Input file: /mnt/hgfs/STORAGE/Test Images/xp dblake.dd
Output directory: /mnt/hgfs/STORAGE/MantaRay/2013-1234-001-MantaRay_2013-08-06_1
1_06_13_586314/Bulk_Extractor_Results
Disk Size: 1261822464
Threads: 2
11:20:22 Offset 67MB (5.32%) Done in  0:02:51 at 11:23:13
11:20:32 Offset 150MB (11.97%) Done in  0:02:25 at 11:22:57
```

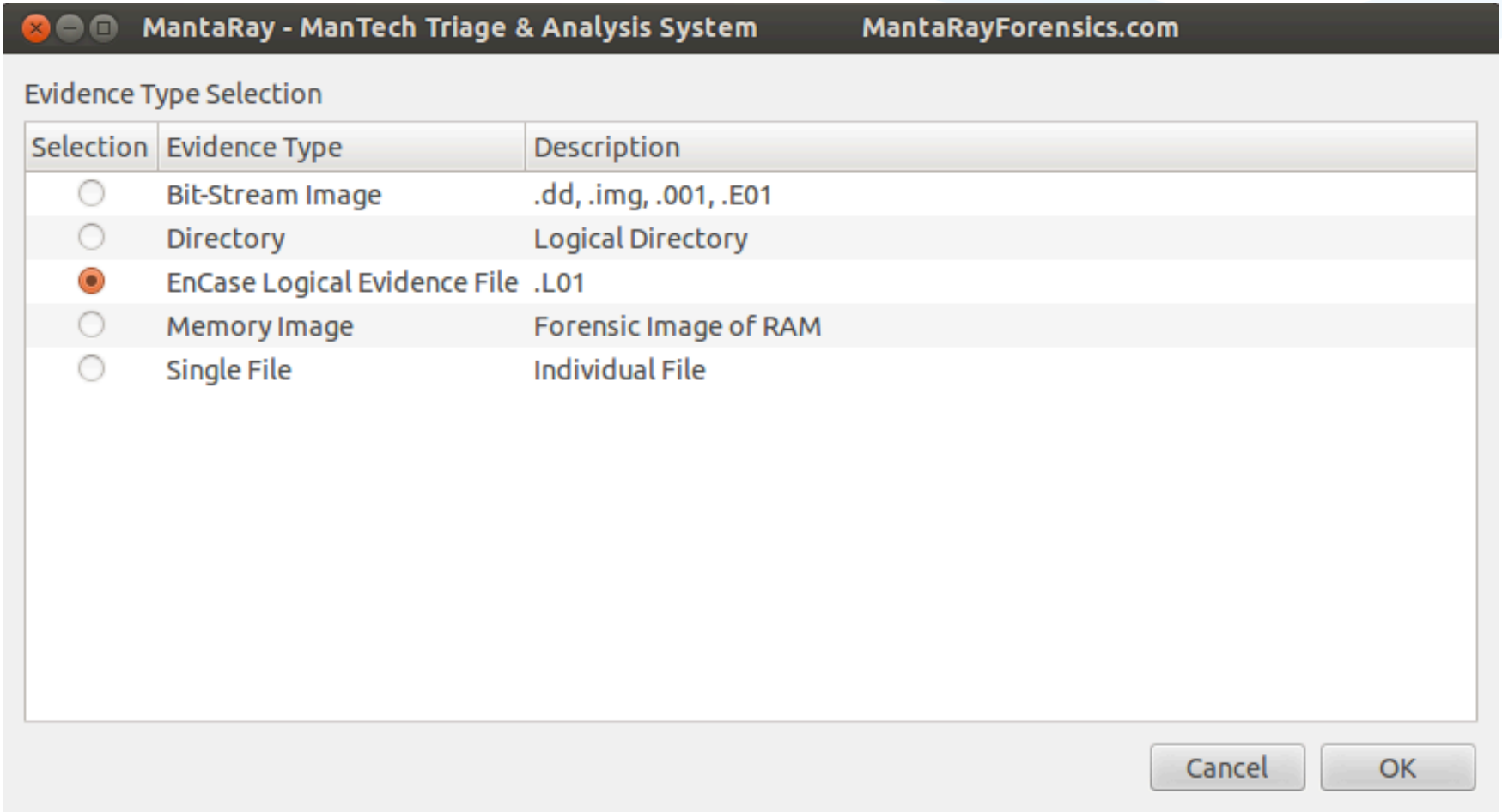
Evidence Type: Directory



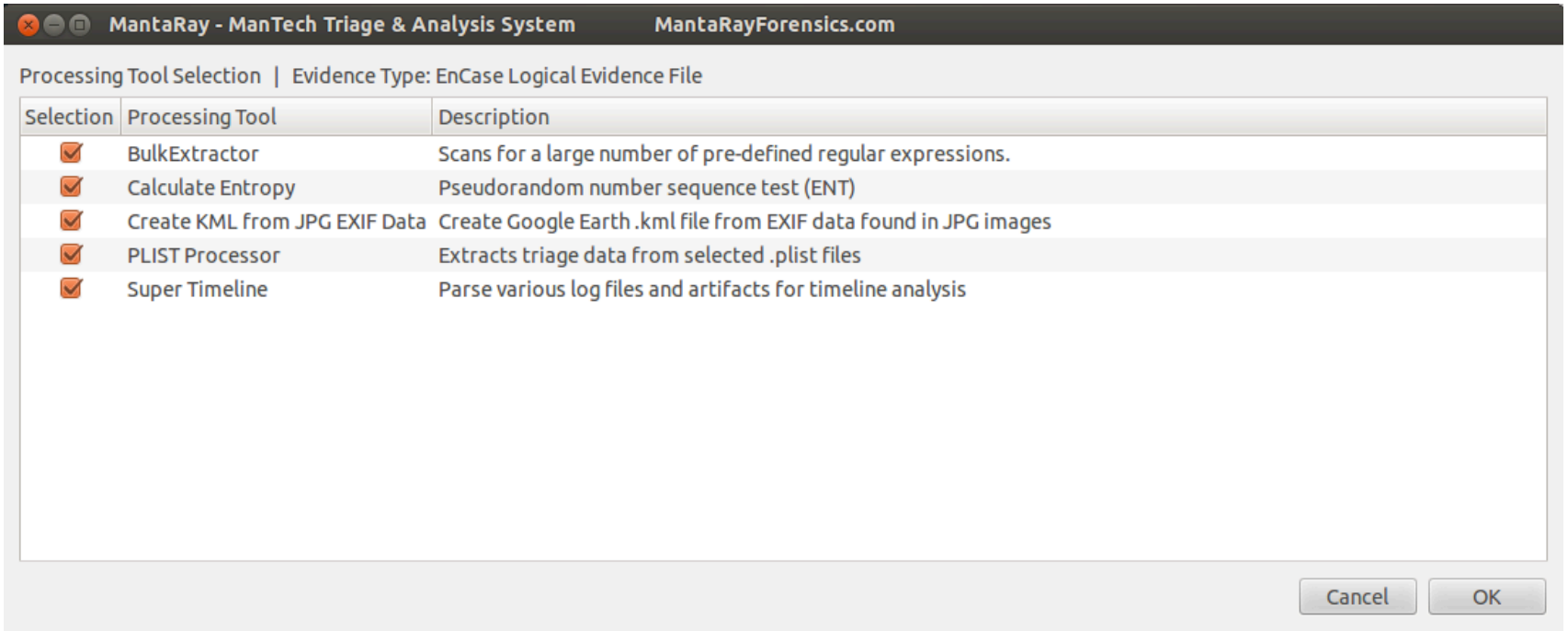
Tool Options: Directory



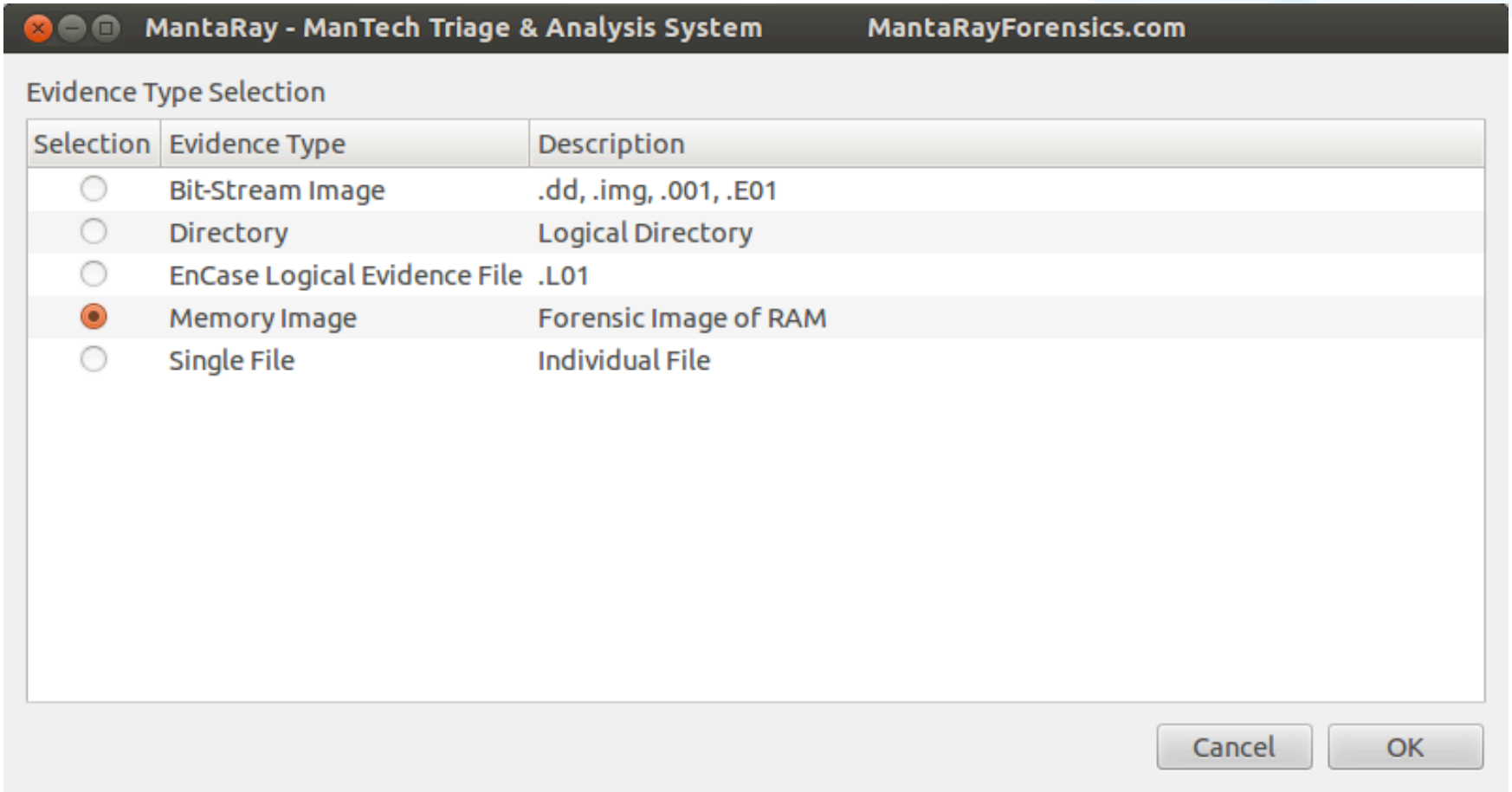
Evidence Type: Logical Evidence File



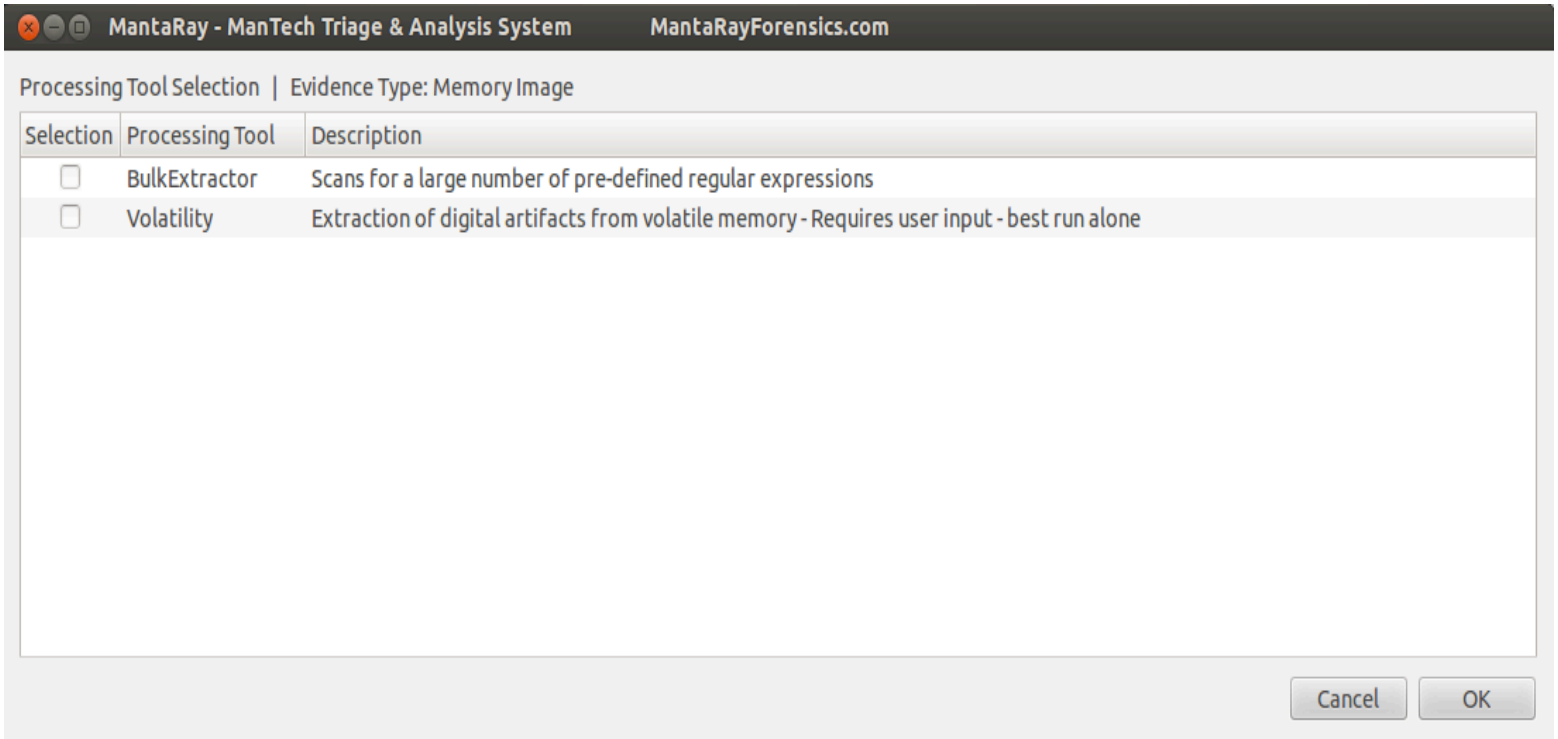
Tool Options: Logical Evidence File



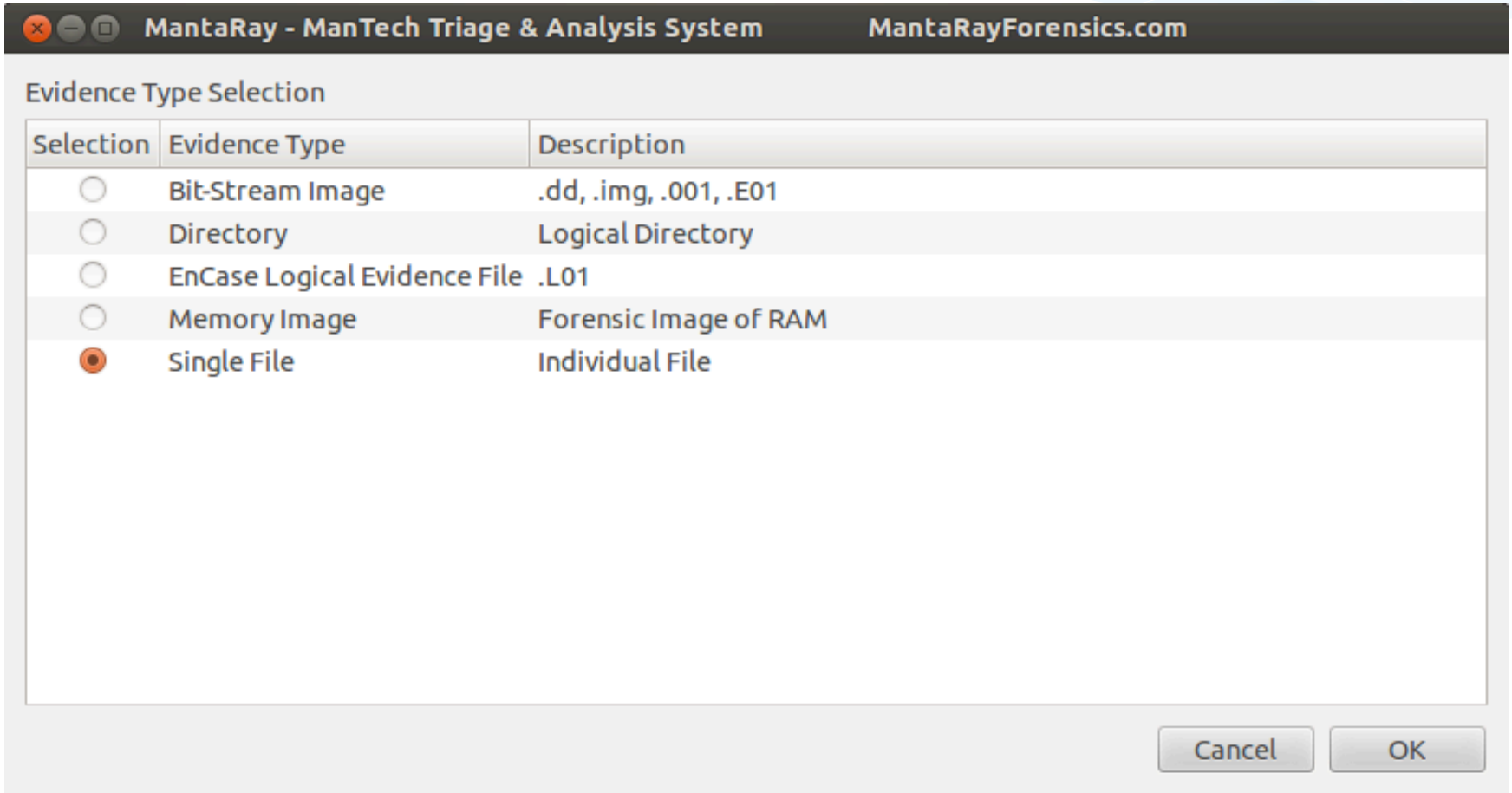
Evidence Type: Memory Image



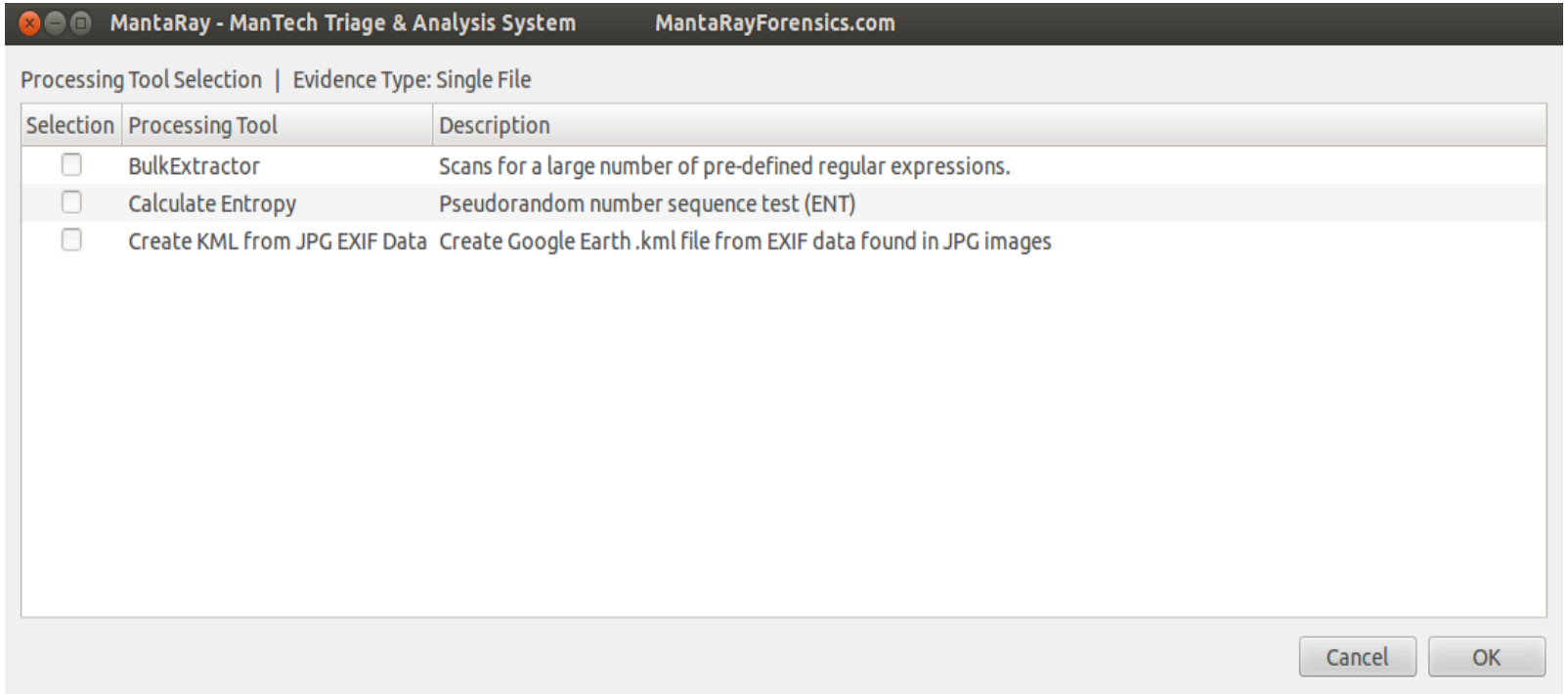
Tool Options: Memory Image



Evidence Type: Single File



Tool Options: Single File



Download

* To download SIFT3_beta
  * Go to www.MantaRayForensics.com
  * Create a user account
  * Click on downloads tab
* To download this presentation
  * Go to www.MantaRayForensics.com
  * Create a user account
  * Click on downloads tab

Questions

* If you have questions on MantaRay please submit them via the forum at www.MantaRayForensics.com
  * To submit to the forum you will need to create a user account