

# 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



# 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](http://www.mantarayforensics.com)

# Creating User Account: Click Register on Website under Users

A screenshot of the MantaRay website. The top navigation bar includes links for 'Welcome', 'About', 'Blog', 'Careers', 'Download', 'Training', and 'Users'. The 'Users' menu is open, showing options for 'Login', 'Forum', 'Register', and 'Support'. The 'Register' option is highlighted. Below the navigation bar, the main content area features a 'Welcome' heading and an 'Introducing MantaRay' section. This section includes an image of the MantaRay logo and a paragraph of text describing the system's capabilities and development.

ManTech Forensics + New Edit Page Howdy, dkoster

# MantaRay


ManTech Triage & Analysis System

Welcome About Blog Careers Download Training Users Search

Login Forum Register Support

Edit **Welcome**

**Introducing MantaRay**



MantaRay was designed to automate processing forensic images, directories and individual files with open source tools. With support for numerous image formats, this tool provides a scalable base to utilize open source and custom exploitation tools. MantaRay was developed by two forensic analysts, Doug Koster and Kevin Murphy. With more than 25

# Set up Username & Email



Register For This Site

Username

E-mail

A password will be e-mailed to you.

Register

[Log in](#) | [Lost your password?](#)

[← Back to MantaRay Forensics](#)

# 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



A screenshot of the MantaRay website interface. At the top, there is a navigation bar with "MantaRay Forensics", "+ New", and "Edit Page". On the right, a user profile for "Howdy, dkoster" is shown with a dropdown menu containing "dkoster", "Edit My Profile", and "Log Out". The main content area features a large banner with "MantaRay" in red and "ManTech Triage &amp; Analysis System" in white on a black background with binary code. Below the banner is a navigation menu with "Welcome", "About", "Blog", "Careers", "Download", "Training", and "Users", along with a search bar. The "Welcome" section has an "Edit" button and a heading "Welcome". Underneath is "Introducing MantaRay" with a smaller version of the MantaRay logo and a paragraph of text describing the tool's capabilities and development.



# 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



The screenshot displays the Encase software interface. The top menu bar includes File, Edit, View, Tools, and Help. Below the menu is a toolbar with icons for New, Open, Save, Print, Add Device, Search, and Refresh. The main window is divided into several panes:

- Left Pane:** A tree view showing the file system structure, including folders like Home, File Extents, Permissions, Referenc..., All Users, Default, Default User, Dexter Morgan, John Dorian, Public, Windows, addins, AppCompat, and AppPatch.
- Table Pane:** A table listing files and folders with columns for Name, File Identifier, Filter, In Report, File Ext, File Type, File Category, Signature, Description, and Is Deleted. The file "NTUSER.DAT" is highlighted.
- Bottom Pane:** A hex view showing the raw data of the selected file, with columns for address (e.g., 000000, 000130, 000260) and hex values.
- Right Pane:** A pane for EnScript, showing a tree view with folders like Examples, Forensic, Include, Main, and Source Processor.

Name	File Identifier	Filter	In Report	File Ext	File Type	File Category	Signature	Description	Is Deleted
John Dorian	47							Folder	06/05/1
John Dorian-STXF_...	47							File, Stream, System	
es-ES	48							Folder	06/05/1
Videos	48							Folder, Read Only	06/05/1
bootmgr.exe.mui	49			mui				File, Archive	06/05/1
NTUSER.DAT	49			DAT	Data ASCII & Binary	CodeLibrary		File, Hidden, System, Ar...	07/05/1
Saved Games	50							Folder, Read Only	06/05/1
fi-FI	50							Folder	06/05/1
poqexec.log	51			log	Log	Document		File, Archive	06/05/1
bootmgr.exe.mui	51			mui				File, Archive	06/05/1

# 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



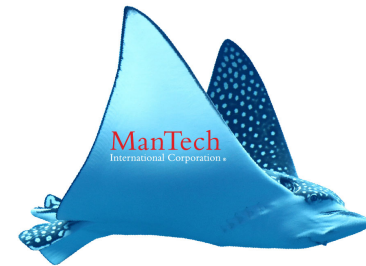
- \* Run blkcalc:
  - \* The cluster offset of your file is calculated as follows:  
foremost\_file\_offset/block\_size (14399160320/4096=351420)
    - \* The foremost file offset is located in the audit.dat text file in the Extracted Registry Hives folder
    - \* Blkcalc -u <cluster offset of file>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

# Finding files carved by Foremost



The screenshot shows the Encase forensic software interface. The top menu bar includes File, Edit, View, Tools, and Help. Below the menu is a toolbar with icons for New, Open, Save, Add Device, Search, and Refresh. The main window is divided into several panes. On the left, there is a 'Cases' pane with a tree view showing folders like Program Files (x86), ProgramData, Recovery, System Volume Information, Users, Windows, addins, AppCompat, and AppPatch. The central pane displays a list of file entries with hexadecimal addresses ranging from 08395380 to 08396570. A context menu is open over this list, showing options: Add Partition..., Delete partition..., Remove user defined partitions..., View Clusters (checked), and Go To... On the right, there is a 'Hits' pane with a tree view showing folders like EnScript, Examples, Forensic, Include, Main, and Source Processor. At the bottom, there is a console window with a grid of addresses from 0000 to 2875. The status bar at the very bottom displays the path: D:\idorian\untitled\D\System Volume Information\{3d992026-d541-11e2-a4f1-20c9d0dce476}\{3808876b-c176-4e48-b7ae-04046e6cc752} (PS 67376856 LS 67170008 CL 8396251 SO 000 FO 185446400 LE 0).

# Finding files carved by Foremost

A screenshot of the EnCase Forensic software interface. The main window displays a file tree on the left and a list of files in the center. A console window at the bottom shows hex data and file details. A "Go to Cluster" dialog box is open, showing "Interpret Selected Text" with radio buttons for "Little-endian", "Big-endian", and "Other" (selected), and a dropdown menu showing "8396596".

08395380  
08395450  
08395520  
08395590  
08395660  
08395730  
08395800  
08395870  
08395940  
08396010  
08396080  
08396150  
08396220  
08396290  
08396360  
08396430  
08396500  
08396570

File Edit View Tools Help  
New Open Save Add Device Search Refresh  
Cases Table Report Gallery Timeline Disk Code  
Home Entries Bookmarks Search Hits  
Home File Exts Permissions Refer  
Program Files (x86)  
ProgramData  
Recovery  
System Volume Information  
Users  
Windows  
adds  
AppComp  
AppPatch

Text Hex Doc Transcript Picture Report Console Details  
00002322, elevation:2, lower version revision holder: 0.0.0.0 201  
0125ComponentAnalyzerEvaluateSelfUpdate): Component: x86\_microsoft-w  
0250et-ee\_ca361fbf35dd0717, elevate: 2, applicable(true/false): 0 2  
0375date, Component: x86\_microsoft-windows-crypt32-dll.resources\_31b  
0500, elevation:2, lower version revision holder: 0.0.0.0 2013-06-1  
0625entAnalyzerEvaluateSelfUpdate): Component: x86\_microsoft-windows  
07506f9158dc26f11cb2, elevate: 2, applicable(true/false): 0 2013-06  
0875Component: x86\_microsoft-windows-crypt32-dll.resources\_31bf3856a  
1000ation:2, lower version revision holder: 0.0.0.0 2013-06-12 19:51:04, Info CBS Applicability(ComponentAna  
1125lyzerEvaluateSelFUpdate): Component: x86\_microsoft-windows-crypt32-dll.resources\_31bf3856ad364e35\_6.1.7601.22322\_fr-fr\_732dca  
12502e24a940ea, elevate: 2, applicable(true/false): 0 2013-06-12 19:51:04, Info CBS Appl: Selfupdate, Compon  
1375ent: x86\_microsoft-windows-crypt32-dll.resources\_31bf3856ad364e35\_0.0.0.0\_he-il\_d8a34dc0dbd8b9ca (6.1.7601.22322), elevation:  
15002, lower version revision holder: 0.0.0.0 2013-06-12 19:51:04, Info CBS Applicability(ComponentAnalyzerE  
1625valuateSelfUpdate): Component: x86\_microsoft-windows-crypt32-dll.resources\_31bf3856ad364e35\_6.1.7601.22322\_he-il\_b74d71d00b18  
175041d8, elevate: 2, applicable(true/false): 0 2013-06-12 19:51:04, Info CBS Appl: Selfupdate, Component: x  
187586\_microsoft-windows-crypt32-dll.resources\_31bf3856ad364e35\_0.0.0.0\_hr-hr\_dac000a0da8c2690 (6.1.7601.22322), elevation:2, low  
2000er version revision holder: 0.0.0.0 2013-06-12 19:51:04, Info CBS Applicability(ComponentAnalyzerEvaluat  
2125eSelfUpdate): Component: x86\_microsoft-windows-crypt32-dll.resources\_31bf3856ad364e35\_6.1.7601.22322\_hr-hr\_b96a24b009cb9e9e,  
2250elevate: 2, applicable(true/false): 0 2013-06-12 19:51:04, Info CBS Appl: Selfupdate, Component: x86\_mic  
2375rosoft-windows-crypt32-dll.resources\_31bf3856ad364e35\_0.0.0.0\_hu-hu\_dbf42666d9c987f8 (6.1.7601.22322), elevation:2, lower ver  
2500sion revision holder: 0.0.0.0 2013-06-12 19:51:04, Info CBS Applicability(ComponentAnalyzerEvaluateSelfU  
2625pdate): Component: x86\_microsoft-windows-crypt32-dll.resources\_31bf3856ad364e35\_6.1.7601.22322\_hu-hu\_ba9e4a7609091006, elevat  
2750e: 2, applicable(true/false): 0 2013-06-12 19:51:04, Info CBS Appl: Selfupdate, Component: x86\_microsoft  
2875-windows-crvt32-dll.resources\_31bf3856ad364e35\_0.0.0.0\_it-it\_7eab9c65cc9b9e5a (6.1.7601.22322), elevation:2, lower version r  
idorian\untitled\D:\System Volume Information\{3d992026-d541-11e2-a4f1-20c9d0dce476}\{3808876b-c176-4e48-b7ae-04046c6cc752} (PS 67374584 LS 67167736 CL 8395967 SO 000 FO 184283136 LE 0)

Go to Cluster  
Interpret Selected Text  
 Little-endian  
 Big-endian  
 Other 8396596  
OK Cancel

EnScript Hits Filters Conditions Disj  
EnScript  
Examples  
Forensic  
Include  
Main  
Source Processor

# Finding files carved by Foremost



The screenshot displays the EnCase Forensic software interface. The top menu bar includes File, Edit, View, Tools, and Help. Below the menu is a toolbar with icons for New, Open, Save, Add Device, Search, and Refresh. The main window is divided into several panes:

- Left Pane:** A tree view showing the file system structure. The "Program Files (x86)" folder is expanded, showing subfolders like "ProgramData", "Recovery", "System Volume Information", "Users", and "Windows".
- Center Pane:** A list of files with columns for file name, size, and date. The files listed are:

File Name	Size	Date
08395380		
08395450		
08395520		
08395590		
08395660		
08395730		
08395800		
08395870		
08395940		
08396010		
08396080		
08396150		
08396220		
08396290		
08396360		
08396430		
08396500		
08396570		

- Bottom Left Pane:** A hex view of a file. The address bar shows "0/130087". The hex data is displayed in a grid format, with the first few lines showing:

```
0000 egfK . . K . . 8 ° S N i . . . . . r o f i l e s \ L o c a l S e r v i c e \ N T U S E R . . D A T . . . . .
0125 . . . . .
0250 . . . . .
0375 . . . . .
0500 . . . . . - 7 i . . . . .
0625 . . . . .
0750 . . . . .
0875 . . . . .
1000 . . . . .
1125 . . . . .
1250 . . . . .
1375 . . . . .
1500 . . . . .
1625 . . . . .
1750 . . . . .
1875 . . . . .
2000 . . . . .
2125 . . . . .
2250 . . . . .
2375 . . . . .
2500 . . . . .
2625 . . . . .
2750 . . . . .
2875 . . . . .
```

- Bottom Right Pane:** A pane for EnScript, showing a tree view of the script structure. The tree includes folders for "Examples", "Forensic", "Include", "Main", and "Source Processor".

The status bar at the bottom of the window displays the following information: jdorlan\untitled\D\System Volume Information\{3d992026-d541-11e2-a4f1-20c9d0dce476}\{3808876b-c176-4e48-b7ae-04046e6cc752} (PS 67379616 LS 67172768 CL 8396596 SO 000 FO 186859520 LE 0)

# 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



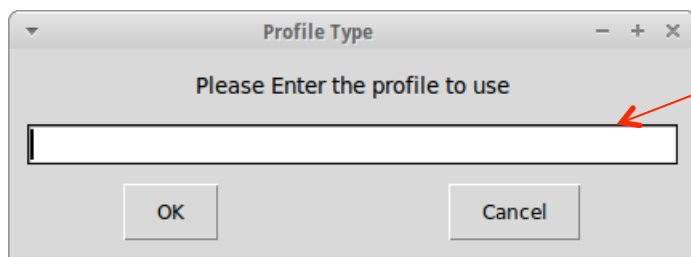
## MantaRay volatility script

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

```
root@ubuntu: /usr/local/src/Manta_Ray/Tools/Python
The evidence to process is: /mnt/hgfs/STORAGE/Test Images/TW_Image_Files/Frau.Far
rbissina/Frau.Farbissina_decompressed_hiberfil.dd
Checking RAM image for imageinfo information...This may take a few minutes...

Volatile Systems Volatility Framework 2.2
The value of imageinfo is: Determining profile based on KDBG search...

Suggested Profile(s) : Win2008R2SP0x64, Win7SP1x64, Win7SP0x64, Win200
8R2SP1x64
AS_Layer1 : AMD64PagedMemory (Kernel AS)
AS_Layer2 : FileAddressSpace (/mnt/hgfs/STORAGE/Test Images
/TW_Image_Files/Frau.Farbissina/Frau.Farbissina_decompressed_hiberfil.dd)
PAE type : PAE
DTB : 0x187000L
KDBG : 0xf80002c480a0
Number of Processors : 2
Image Type (Service Pack) : 1
KPCR for CPU 0 : 0xf80002c49d00
KPCR for CPU 1 : 0xf880009ea000
KUSER_SHARED_DATA : 0xfffff78000000000L
Image date and time : 2012-07-05 11:14:29 UTC+0000
Image local date and time : 2012-07-05 07:14:29 -0400
```





# 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=obo5Qeb9rHA>



# 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://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](http://www.mantarayforensics.com)

# Demo



# Enter Case Information



MantaRay - ManTech Triage & Analysis System

### Case Information

Case Number	2013-1234
Evidence Number	001
Examiner Name	doug
Notes	Really Hard Case

OK Cancel

# Select Evidence Type



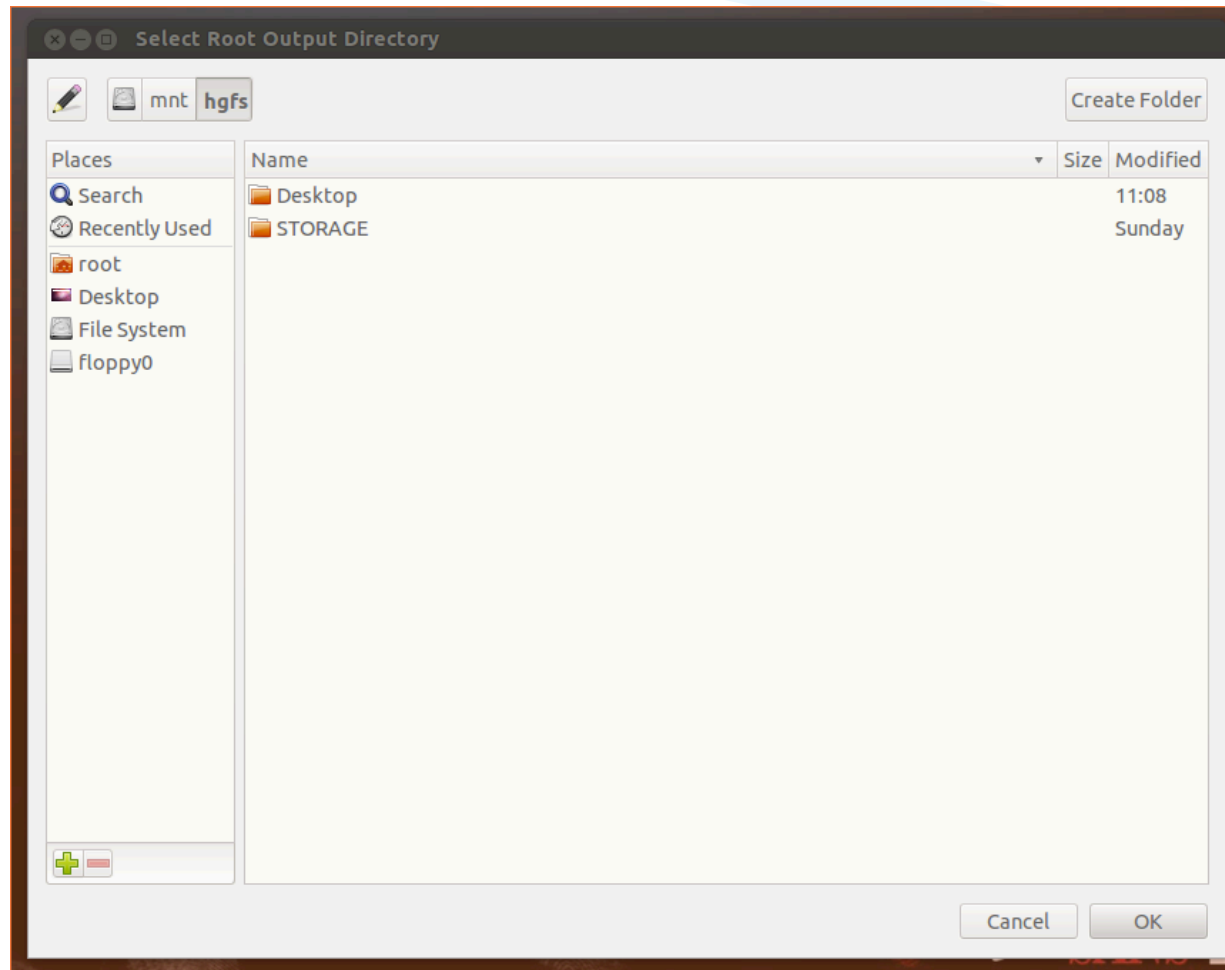
MantaRay - ManTech Triage & Analysis System MantaRayForensics.com

Evidence Type Selection

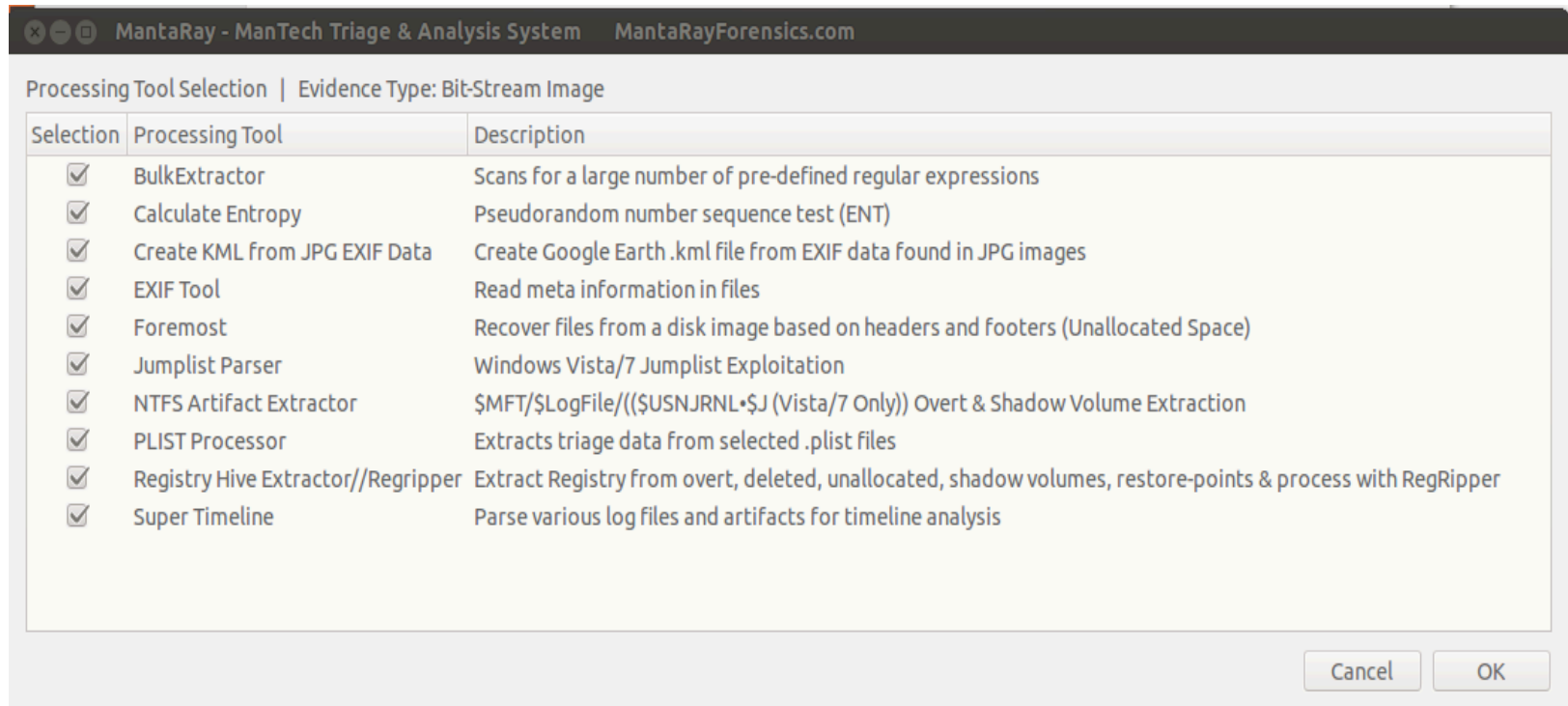
Selection	Evidence Type	Description
<input checked="" type="radio"/>	Bit-Stream Image	.dd, .img, .001, .E01
<input type="radio"/>	Directory	Logical Directory
<input type="radio"/>	EnCase Logical Evidence File	.L01
<input type="radio"/>	Memory Image	Forensic Image of RAM
<input type="radio"/>	Single File	Individual File

Cancel OK

# Select Output Directory

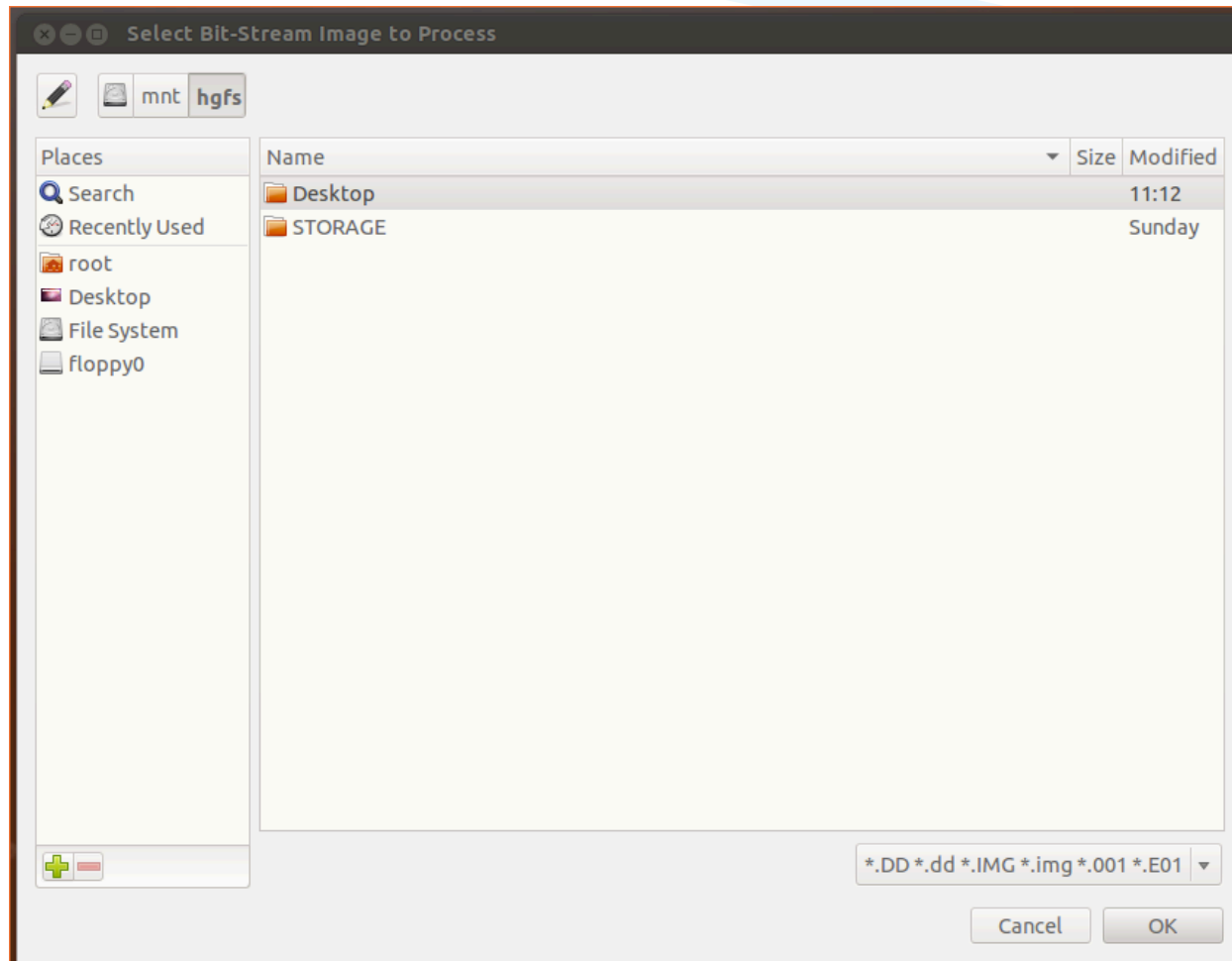


# Select tools to run





# Select Evidence to Process



# Select Debug Mode Setting



MantaRay - ManTech Triage & Analysis System MantaRayForensics.com

Debugging Option Selection

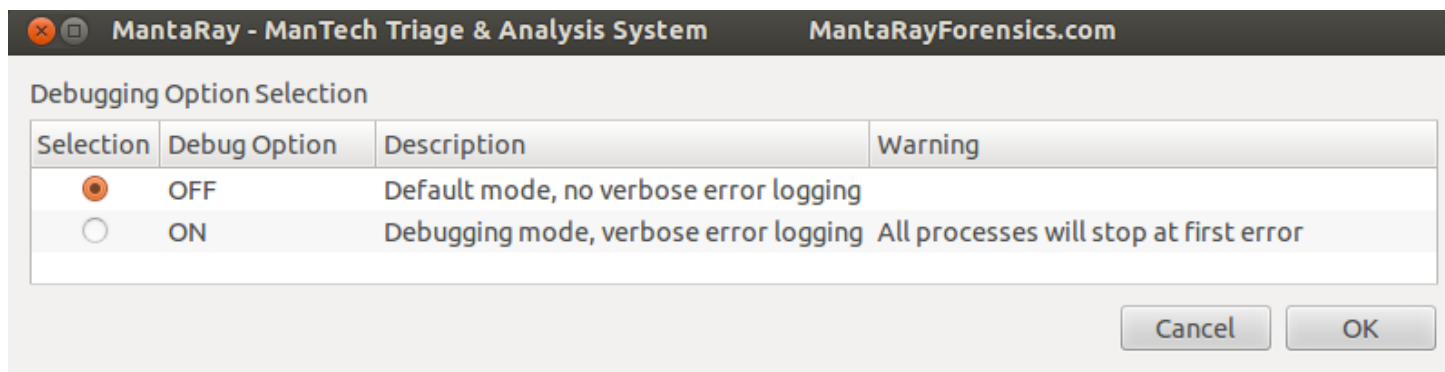
Selection	Debug Option	Description	Warning
<input checked="" type="radio"/>	OFF	Default mode, no verbose error logging	
<input type="radio"/>	ON	Debugging mode, verbose error logging	All processes will stop at first error

Cancel OK

# 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



MantaRay - ManTech Triage & Analysis System MantaRayForensics.com

Processing Options - BulkExtractor

Selection	Processing Option	Description
<input type="checkbox"/>	Keyword List	Search for case specific keyword list
<input type="checkbox"/>	Whitelist	Remove known features (artifacts) from process output

Cancel OK

# Select Bulk Extractor Speed



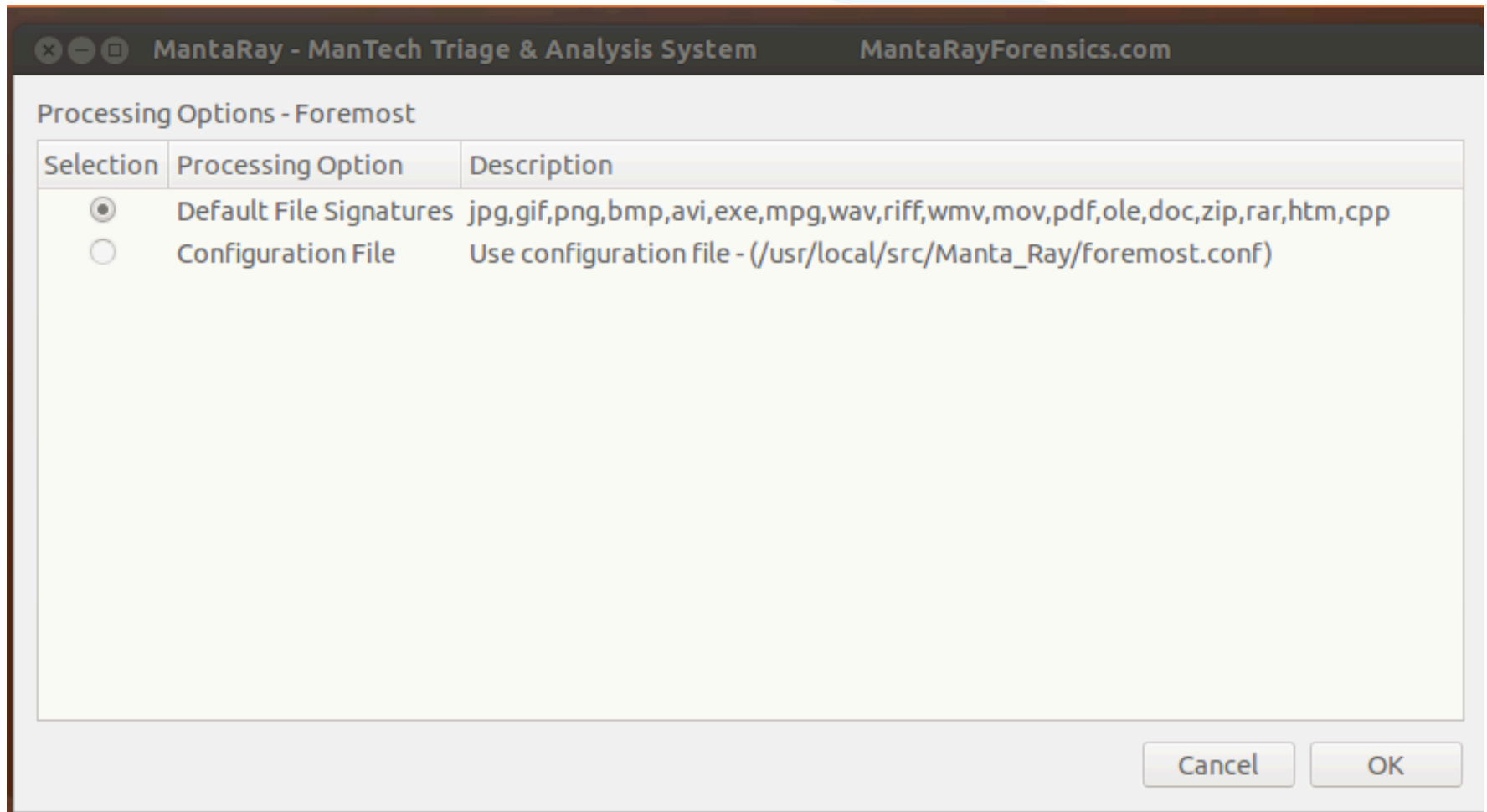
MantaRay - ManTech Triage & Analysis System MantaRayForensics.com

Processing Performance - BulkExtractor

Selection	Processor Performance	Description
<input type="radio"/>	Speed-Slow	Minimum Processing Cores
<input checked="" type="radio"/>	Speed-Med	Medium Processing Cores (Recommended)
<input type="radio"/>	Speed-Fast	Maximum Processing Cores (Warning - Processor Intensive)

Cancel OK

# Select Foremost signatures



# Select Registry Hives to Extract



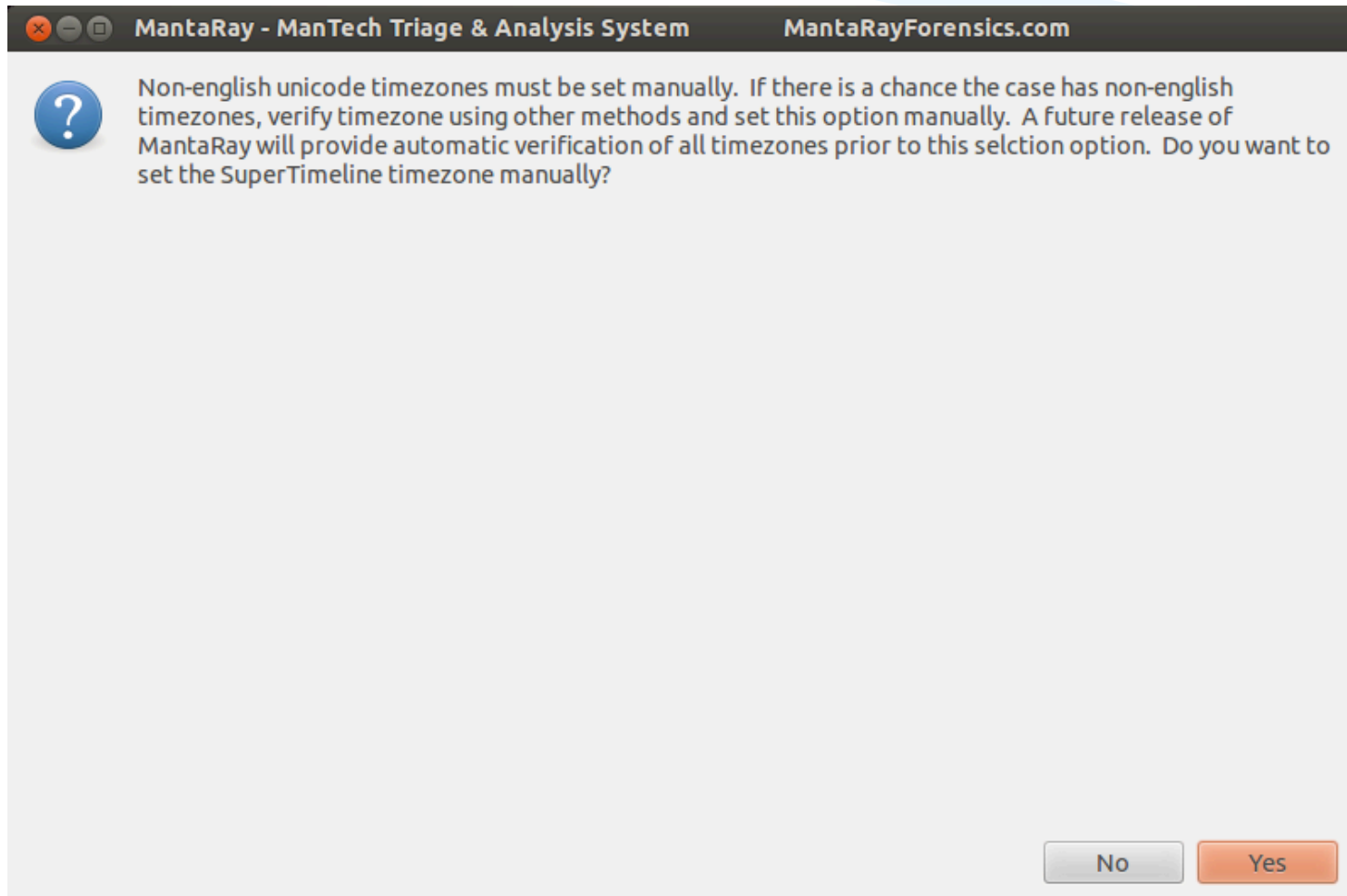
MantaRay - ManTech Triage & Analysis System MantaRayForensics.com

Processing Options - Registry Extractor

Selection	Processing Option	Description
<input type="checkbox"/>	Overt, Deleted, Restore-Points	Overt/Deleted/Restore-Points(WinXP) Registry Hives
<input type="checkbox"/>	Unallocated	Unallocated Registry Hives (regf Header - 50MB Length)
<input type="checkbox"/>	Shadow Volumes	Shadow Volume Registry Hives (Windows Vista/7)

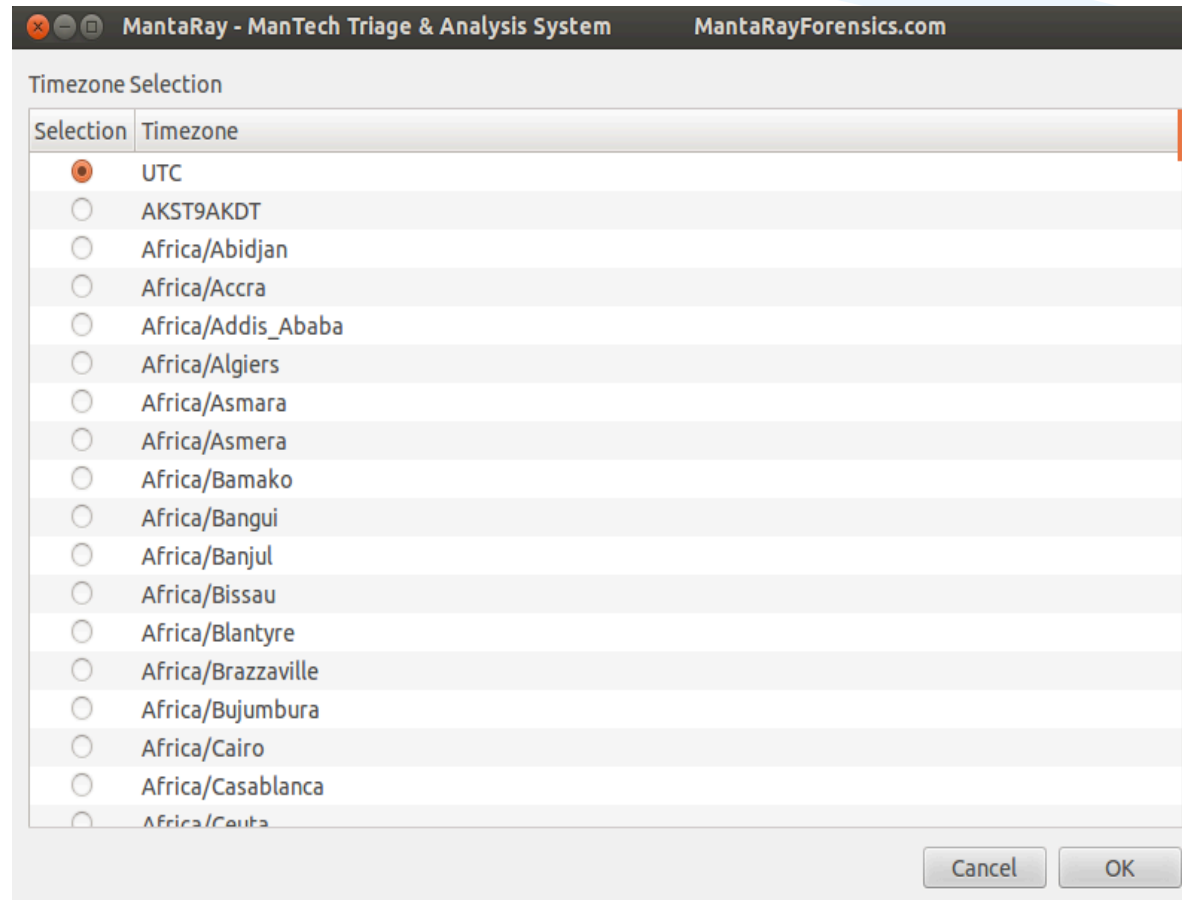
Cancel OK

# 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_11_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-MantaRay_2013-08-06_11_06_13_586314/Bulk_Extractor_Results" -j 2 "/mnt/hgfs/STORAGE/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_11_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



MantaRay - ManTech Triage & Analysis System MantaRayForensics.com

Evidence Type Selection

Selection	Evidence Type	Description
<input type="radio"/>	Bit-Stream Image	.dd, .img, .001, .E01
<input checked="" type="radio"/>	Directory	Logical Directory
<input type="radio"/>	EnCase Logical Evidence File	.L01
<input type="radio"/>	Memory Image	Forensic Image of RAM
<input type="radio"/>	Single File	Individual File

Cancel OK

# Tool Options: Directory



MantaRay - ManTech Triage & Analysis System MantaRayForensics.com

Processing Tool Selection | Evidence Type: Directory

Selection	Processing Tool	Description
<input checked="" type="checkbox"/>	BulkExtractor	Scans for a large number of pre-defined regular expressions
<input checked="" type="checkbox"/>	Calculate Entropy	Pseudorandom number sequence test (ENT)
<input checked="" type="checkbox"/>	Create KML from JPG EXIF Data	Create Google Earth .kml file from EXIF data found in JPG images
<input checked="" type="checkbox"/>	Delete Duplicate Files	Delete duplicate files from the selected directory (Recursive)
<input checked="" type="checkbox"/>	EXIF Tool	Read meta information in files
<input checked="" type="checkbox"/>	PLIST Processor	Extracts triage data from selected .plist files
<input checked="" type="checkbox"/>	Super Timeline	Parse various log files and artifacts for timeline analysis

Cancel OK

# Evidence Type: Logical Evidence File



MantaRay - ManTech Triage & Analysis System MantaRayForensics.com

Evidence Type Selection

Selection	Evidence Type	Description
<input type="radio"/>	Bit-Stream Image	.dd, .img, .001, .E01
<input type="radio"/>	Directory	Logical Directory
<input checked="" type="radio"/>	EnCase Logical Evidence File	.L01
<input type="radio"/>	Memory Image	Forensic Image of RAM
<input type="radio"/>	Single File	Individual File

Cancel OK

# Tool Options: Logical Evidence File



MantaRay - ManTech Triage & Analysis System MantaRayForensics.com

Processing Tool Selection | Evidence Type: EnCase Logical Evidence File

Selection	Processing Tool	Description
<input checked="" type="checkbox"/>	BulkExtractor	Scans for a large number of pre-defined regular expressions.
<input checked="" type="checkbox"/>	Calculate Entropy	Pseudorandom number sequence test (ENT)
<input checked="" type="checkbox"/>	Create KML from JPG EXIF Data	Create Google Earth .kml file from EXIF data found in JPG images
<input checked="" type="checkbox"/>	PLIST Processor	Extracts triage data from selected .plist files
<input checked="" type="checkbox"/>	Super Timeline	Parse various log files and artifacts for timeline analysis

Cancel OK

# Evidence Type: Memory Image



MantaRay - ManTech Triage & Analysis System MantaRayForensics.com

Evidence Type Selection

Selection	Evidence Type	Description
<input type="radio"/>	Bit-Stream Image	.dd, .img, .001, .E01
<input type="radio"/>	Directory	Logical Directory
<input type="radio"/>	EnCase Logical Evidence File	.L01
<input checked="" type="radio"/>	Memory Image	Forensic Image of RAM
<input type="radio"/>	Single File	Individual File

Cancel OK

# Tool Options: Memory Image



MantaRay - ManTech Triage & Analysis System MantaRayForensics.com

Processing Tool Selection | Evidence Type: Memory Image

Selection	Processing Tool	Description
<input type="checkbox"/>	BulkExtractor	Scans for a large number of pre-defined regular expressions
<input type="checkbox"/>	Volatility	Extraction of digital artifacts from volatile memory - Requires user input - best run alone

Cancel OK



# Evidence Type: Single File



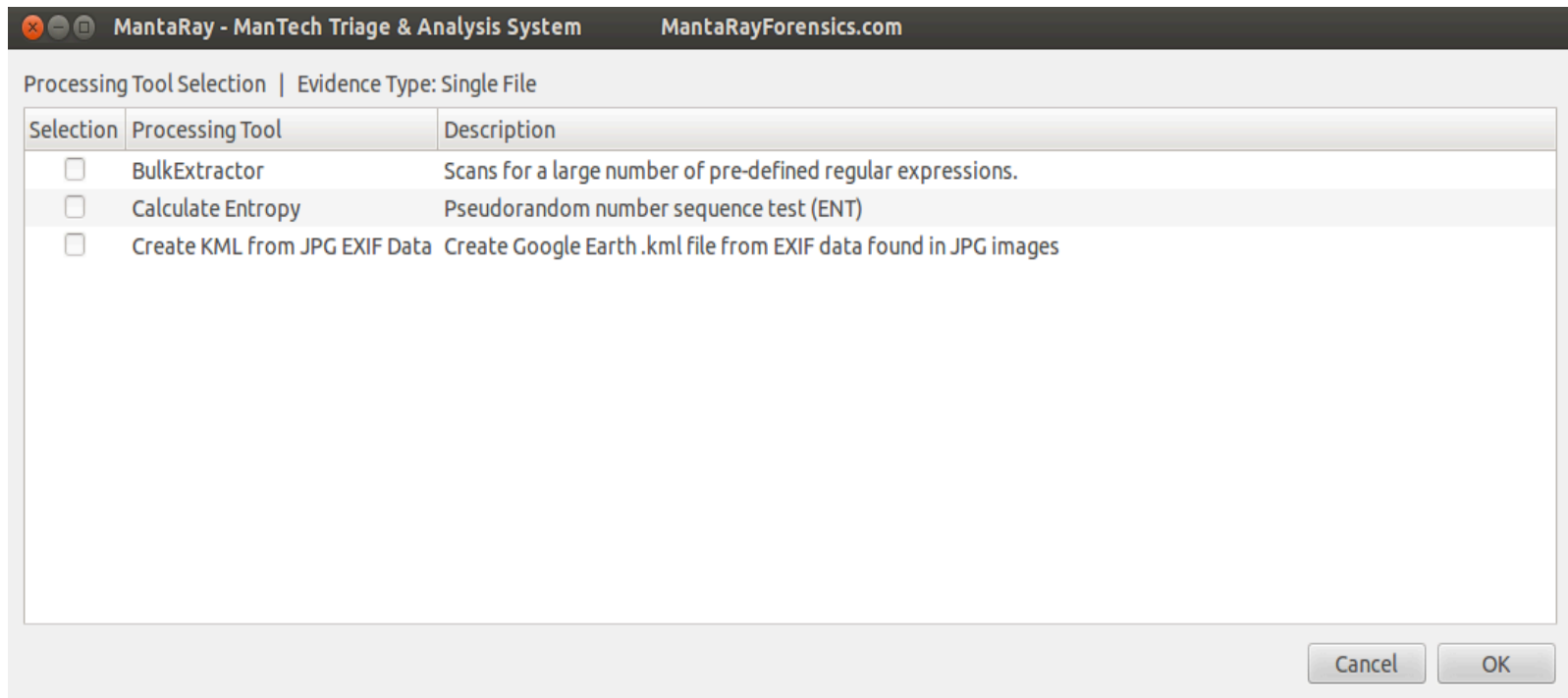
MantaRay - ManTech Triage & Analysis System MantaRayForensics.com

Evidence Type Selection

Selection	Evidence Type	Description
<input type="radio"/>	Bit-Stream Image	.dd, .img, .001, .E01
<input type="radio"/>	Directory	Logical Directory
<input type="radio"/>	EnCase Logical Evidence File	.L01
<input type="radio"/>	Memory Image	Forensic Image of RAM
<input checked="" type="radio"/>	Single File	Individual File

Cancel OK

# Tool Options: Single File



# Download



- \* To download SIFT3\_beta
  - \* Go to [www.MantaRayForensics.com](http://www.MantaRayForensics.com)
  - \* Create a user account
  - \* Click on downloads tab
- \* To download this presentation
  - \* Go to [www.MantaRayForensics.com](http://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](http://www.MantaRayForensics.com)
- \* To submit to the forum you will need to create a user account