



Quick Start Guide

Dedication and Credits

This manual is dedicated to all of those who have worked tireless hours, sacrificed time away from their families and have put their lives on the line to protect the communities in which we live and to help make the world safe.

CREDITS

PALADIN and its features could not have reached its full potential without the assistance of those who contribute to the Open Source and Digital Forensic communities. It is through their efforts that we are able to provide PALADIN.

However, it is through the tireless work of Manoj Kumar and the rest of the ForensoDigital team that we have to thank for bringing all of the elements together symbiotically to create PALADIN. For his efforts and the efforts of his team, I can not thank them enough. Their work has helped the rest of us fight terrorism, bring criminals to justice and protect children from sexual exploitation all over the world on countless occasions.

My sincerest thank you to Manoj and the forensic community who continue to make PALADIN possible.

Steve Whalen
SUMURI LLC - Co-Founder and Chief Product Officer

© 2010-2021 SUMURI LLC

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to the publisher, addressed "Attention: Permissions Coordinator," at the address below.

SUMURI LLC
P.O. Box 252
Wyoming, Delaware 19934
USA
www.sumuri.com

Quick Start Guide



What is PALADIN?



PALADIN is a bootable forensic Linux distribution based on Ubuntu and is developed and provided as a courtesy by SUMURI. The boot process has been modified to assure that the internal or external media of computers and devices are not modified or mounted.

PALADIN is available as an ISO which can be used to make a bootable DVD or USB.

Once booted, the user will find a host of precompiled open-source forensic tools that can be used to perform various tasks.

The centerpiece of these tools is the PALADIN Toolbox. The PALADIN Toolbox has combined and simplified multiple forensic tasks into an easy to use GUI (graphical user interface) that requires minimal training and does not require users to utilize the command line.

The “engine” that runs the PALADIN Toolbox is a combination of applications that have been used by forensic examiners and investigators for years and have withstood scrutiny in many courts of law.

New Features of PALADIN

PALADIN has been described as a forensic examiner's "Swiss Army Knife". It contains basic features required by any examiner and advanced features that are still not found in other expensive commercial forensic tools.

With the introduction of **PALADIN Toolbox Version 6**, we added **Autopsy** (courtesy of BASIS Technology and Brian Carrier) which is a powerful GUI-based full forensic suite that has features that rival many of the top commercial forensic suites found on the market today.



Additionally, we have added Bitlocker support and the ability to make logical images.

In addition to updating to a newer version of Ubuntu, PALADIN has also been ported to **64-bit architecture** which allows for faster processing and support for newer hardware.

Finally, we have also added and updated our collection of open source forensic applications found within our **Forensic Tools** directory.

Features at a Glance



Boots most PCs and Intel Macs into a forensically sound environment.
Supports the most popular forensic image formats - .E01, Ex01, RAW (.dd), SMART, AFF, VHD and VMDK.
Ability to clone devices.
Ability to convert from one forensic image to another including the VMDK format.
Ability to create a master and an archive image or two different image formats at the same time.
Ability to mount and image across a network.
Disk Manager allows you to easily visualize and identify attached drives and their partitions.
Ability to format as ExFAT, HFS+, EXT4, FAT32, and NTFS.
Control mounting, wiping (sterilizing) and hashing with one click.
Ability to capture and image the Unallocated Space and Free Space to a file for carving.
Automatic logging which can be saved to any device.
Built-in Triage which can search by file name, keywords or MIME types (file signatures).
Over 100+ pre-compiled open-source forensic tools and applications in our Forensic Tool Chest.
Now with Bitlocker support for Windows Vista, 7, 8, 8.1 and 10 encrypted partitions
Autopsy Digital Forensics Platform from Basis Technology and Brian Carrier!
Ability to make logical images!



About SUMURI

SUMURI is a leading provider of software, hardware, training and services relating to digital evidence, computer forensics and eDiscovery worldwide.

SUMURI LLC was founded in 2010 by Steve and Ailyn Whalen and our company is based and located in the State of Delaware in the United States of America.

Steve's experience in computer forensics dates back to 1997. Steve has developed and delivered forensic training to thousands of investigators and examiners around the world individually and through organizations such as the International Association of Computer Investigative Specialists (IACIS), the High Technology Crimes International Association (HTCIA) and the US Department of State Anti-Terrorism Assistance Program. Steve is also the developer of the successful Macintosh Forensic Survival Course (MFSC), PALADIN (previously Raptor), RECON and CARBON forensic software and co-developer of TALINO Forensic Workstations. Steve has provided training throughout North America, Central America, Asia, Europe, the Middle East, the Caribbean, Africa, and Oceania.

Previously, Steve served over 15 years as a Delaware State Trooper. During that time, he worked as a detective with the Criminal Investigations Unit and served as their first full-time forensic examiner for digital evidence. Building off that experience, Steve helped the Delaware State Police develop its first High Technology Crimes Unit in 2001, where he processed thousands of electronic items and devices containing digital evidence from hundreds of cases relating to intrusion, financial crimes, child sexual exploitation, narcotics, stalking and homicides.

SUMURI was founded on the same principals which were instilled in our founder while a State Trooper - Honor, Integrity, Courage, Loyalty, Attitude, Discipline and Service.

All of the SUMURI teams are held to these standards in every aspect of our work. We treat our clients as we would treat our family. We listen to your needs and offer innovative customized solutions.



Our team consists of some of the leading experts in the fields of digital evidence, computer forensics, and eDiscovery. Our team is made up of active practitioners who come from law enforcement, military, and corporate communities.

Our team has taught thousands of forensic examiners and investigators from Fortune 500 companies, local and federal law enforcement agencies and world governments.

SUMURI provides unparalleled services worldwide.

We look forward to assisting you and hope that you enjoy PALADIN!



Differences Between Versions (PALADIN LTS vs. EDGE)

There are three versions of PALADIN:

- PALADIN LTS (64-Bit Architecture)
- PALADIN EDGE 64 (64-Bit Architecture)
- PALADIN EDGE 32 (32-Bit Architecture)

PALADIN LTS is 64-Bit Architecture and is based on the most current LTS (Long Term Support) version of Ubuntu. LTS allows for a more stable distribution. In addition to the PALADIN Toolbox, **this version of PALADIN includes pre-compiled Open Source forensic tools and applications.**

PALADIN EDGE includes the PALADIN Toolbox but does not include any additional pre-compiled Open Source forensic tools and applications. Many PALADIN users only use the PALADIN Toolbox. By removing the extra pre-compiled tools this distribution is smaller in size and boots faster. Additionally, PALADIN EDGE editions are compiled with newer Linux kernels that tend to support newer hardware. PALADIN EDGE is available in 32 and 64-Bit architecture.

Both PALADIN and PALADIN EDGE have three modes which can be selected from the splash screen:

- Live Session - Forensic Mode
- Live Session - SUMURI Remote Services
- Live Session - Non-Forensic Mode

Forensic Mode - forensically sound with **networking disabled**. Booting to **PALADIN Forensic Mode** does not mount internal drives, attached media and/or swap files. Once booted, the mounting of devices is controlled by the PALADIN Toolbox. The user can utilize the PALADIN Toolbox and any pre-compiled forensic tool to complete tasks.

Non-Forensic Mode - **not forensically sound with networking enabled**. Booting to **Non-Forensic Mode** does mount internal drives, attached media and/or swap files.

How Can I Get PALADIN?

The PALADIN ISO (used to create the PALADIN USB) is provided as a courtesy to the forensic community by SUMURI.

For commercial use, a minimum donation of \$25.00 USD per user per year is required.

Branded and pre-compiled PALADIN USBs with all three versions of PALADIN can be purchased from SUMURI at <https://sumuri.com/product/paladin-pro/>

If you need PALADIN immediately you may download it from the SUMURI website (<https://sumuri.com/product-category/brands/paladin/>).

PALADIN is available as donationware for non-commercial use.

If you find value using PALADIN we ask that you donate in order to keep the PALADIN project alive and well. We truly appreciate any donation! Commercial use requires a minimum donation of \$25.00 USD per user per year.

How Can I Download the PALADIN ISO?

1. Navigate to www.sumuri.com.
2. Sign in to your account via the “My Account” menu. If you do not currently have an account, you will need to register for a free account.
3. Navigate to the PALADIN page via the “Products” menu.
4. Select the version of PALADIN that you would like to download.
5. Name your price then select “Add to Cart”.
6. Review your “Cart” then select “Proceed to Checkout”.
7. Provide the requested information and select “Place Order”.

Please Read Carefully:

Even if the amount entered is zero you must use this process to obtain any of the PALADIN ISOs.

Anonymous or false information may be discarded and could prevent you from downloading PALADIN.

For commercial use, a minimum donation of \$25.00 USD per user per year is required.



Please Read Carefully: In order to download PALADIN, you must create an account and agree to the **Terms and Conditions** of using our services and this site. These terms include giving us permission to contact you about SUMURI news, products, updates and events.

You may opt-out gracefully at any time.

You must create an account first and sign in before adding PALADIN to the shopping cart in order to get valid download links.



CREATE ACCOUNT & DOWNLOAD

PALADIN PRO USB

The PALADIN PRO USB is a triple-boot USB containing the most current versions of PALADIN.

The advantage of using PALADIN PRO is:

- Have all current versions of PALADIN on one USB
- Contains an extra partition to store your SEARCH criteria or LOGs
- Support for both 32-bit and 64-bit computers
- No need to create or carry multiple DVDs or USBs
- Faster boot times
- Cool branded USB
- **You are supporting the PALADIN project**

PALADIN PRO USBs can be ordered from the SUMURI website (<https://sumuri.com/product/paladin-pro/>) for \$74.99 USD.



MAKING YOUR OWN PALADIN USB

Once you have downloaded the PALADIN ISO from the SUMURI website you can use the ISO to make your own PALADIN USBs.

Step-by-step instructions for making a PALADIN USB can be found in SUMURI's blogs at: <https://sumuri.com/wp-content/uploads/2019/12/how-to-make-your-own-paladin-usb-min.pdf>

Troubleshooting PALADIN

There are three options for obtaining support with PALADIN:

- PALADIN Community Support Forums
- Ubuntu Forums and Community Support
- SUMURI Single Support Session

PALADIN Community Support Forums (Free)

The PALADIN Community Support Forum is a venue to allow PALADIN users to post questions and receive help from other PALADIN users. Additionally, we encourage the posting of tips and tricks to assist other users. This forum is supported by PALADIN users and is available for free. The forum is located at <https://sumuri.com/support/forum/>

UBUNTU Forums and Community Support (Free)

PALADIN is based on Ubuntu Linux and it supports anything that Ubuntu supports. Please refer to the Ubuntu Support pages if you encounter any issues with hardware. Answers to most hardware issues can be found within the Ubuntu Support site. The Ubuntu support sites can be found at <http://www.ubuntu.com/support/>

SUMURI Support Sessions (Paid)

We understand that there are times where users need immediate assistance with PALADIN and do not have time to wait for an answer from the Community Support Forums. SUMURI offers Single Support Sessions starting at \$60 USD. These sessions can be used for advanced troubleshooting, mini-lessons or even remote assistance from a SUMURI Team Member. A Support Session certificate can be purchased from the SUMURI website at <https://sumuri.com/product/support-session/>

Booting PALADIN USB on a PC

In order to safely boot PALADIN on standard PCs (non-Macs) please make sure that you are comfortable with the following:

- Disabling Secure Boot
- Setting Boot Options within the BIOS/UEFI (Option-1)
- Accessing the Boot Manager (Option-2)

Disabling Secure Boot

Secure Boot is a security standard found in modern computers that only allows software trusted by the PC manufacturer to boot the computer. If Secure Boot is enabled on a PC it will most likely need to be disabled to boot PALADIN which is based on Linux.

To disable Secure Boot you will need to enter the BIOS/UEFI Setup Utility. This is done by powering on the PC and pressing a “catch” key. This “catch” key can be different for every PC. The “catch” key is usually displayed for a couple of seconds after pressing the power key to turn on the PC. Common examples of BIOS/UEFI Setup Utility “catch” keys are: ESC, F1 or F2 keys.

Once you have safely entered the BIOS/UEFI Setup Utility you will need to find the “Security” menu where you can disable the Secure Boot option and save the changes.

Once the Secure Boot option is disabled and the changes are saved you can then power off the computer, restart and boot with PALADIN.

Setting Boot Options within the BIOS/UEFI (Option-1)

Follow the instructions above to enter the BIOS/UEFI Setup Utility. This time look for the “Boot” menu. Change the order in the Boot Menu to make sure that the PALADIN DVD or USB is first before any other boot source.

Accessing the Boot Manager (Option-2)

Many PCs have a “catch” key to display a Boot Manager where the boot device can be selected without entering the BIOS/UEFI Setup Utility. Common examples of Boot Manager “catch” keys for some PCs are: F10 or F12. Once the Boot Manager is displayed choose the device where the PALADIN USB is inserted.

Quick Summary to Boot PALADIN on a PC

1. Insert PALADIN USB.
2. Disable Secure Boot.
3. Set the boot order in the BIOS/UEFI Setup Menu to boot to PALADIN or choose to boot to PALADIN from the Boot Manager.

Booting PALADIN USB on a Macintosh

In order to safely boot PALADIN on Intel Macs (non-Power PCs) please make sure that you are comfortable with the following:

- Checking for a Firmware Password
- Accessing Boot Options
- Identifying if the Mac contains a T2 Security Chipset.

Checking for a Firmware Password

Similar to the Secure Boot option on PCs, Macs can have a Firmware Password (boot level password) set. If the Firmware Password has been set by the user none of the Startup Commands (key combinations held down on boot) will work other than the Option/ALT key. Instead, the computer will boot to the Login Window if a Firmware Password is set. Prior to attempting to boot PALADIN from a USB, the examiner should first hold down the Option/ALT key to check for an image of a lock.

If the Firmware Password is not set then any bootable options will be displayed including PALADIN.

Accessing Boot Options

Once you have determined that no Firmware Password has been set, the examiner can start the Mac holding down the Option/ALT key. Any boot options will be displayed. The PALADIN USB may be identified by the Mac as a “Windows” or “EFI” USB icon. Selecting this icon will boot the Mac to PALADIN.

Macs with T2 Security Chipset

Macs that have a T2 Security Chipset have Secure Boot enabled by default and most likely can not be booted by PALADIN.

SUMURI recommends our **RECON ITR** forensic software for imaging Macs. More information about **RECON ITR** can be found here <https://sumuri.com/software/recon-itr/>

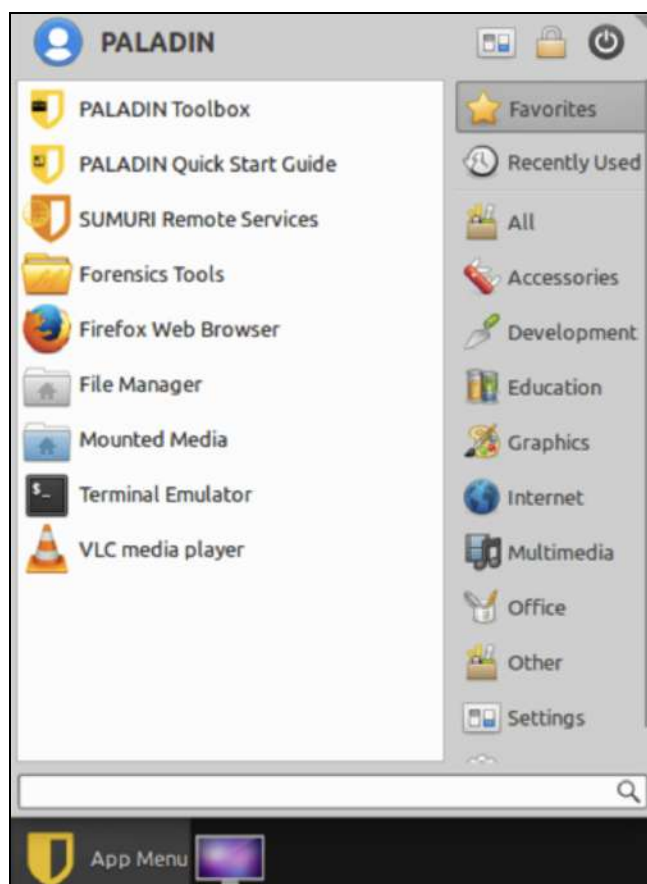
Quick Summary to Boot PALADIN on a supported Mac

1. Insert PALADIN USB.
2. Check to see if a Firmware Password is enabled by holding down the Option/ALT key upon boot.
3. If there is no Firmware Password, select the PALADIN USB which may be identified as “Windows” or “EFI”.

PALADIN Desktop - Overview

PALADIN is based on Ubuntu Linux. Many of the applications and features included with Ubuntu still remain. PALADIN is a complete operating system and the desktop and navigation are similar to other operating systems. In this section we will be highlighting the following:

- Start Menu
- PALADIN Toolbox
- SUMURI Remote Services
- Forensic Tools Directory
- Terminal



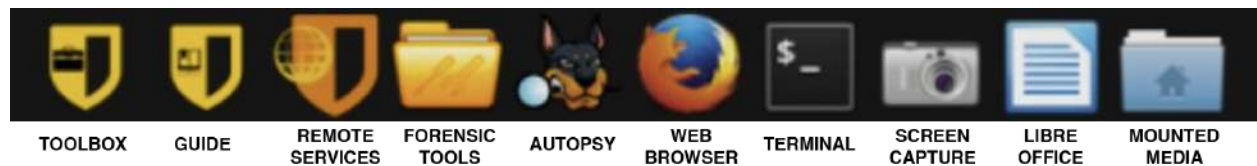
Start Menu

The PALADIN Start Menu can be accessed by clicking the PALADIN shield at the bottom left corner of the desktop (App Menu). From here you can search for installed applications or select categories on the right.

Shutting Down PALADIN

To shut down PALADIN press the power button found at the top right of the Start Menu.

PALADIN Desktop - Dock



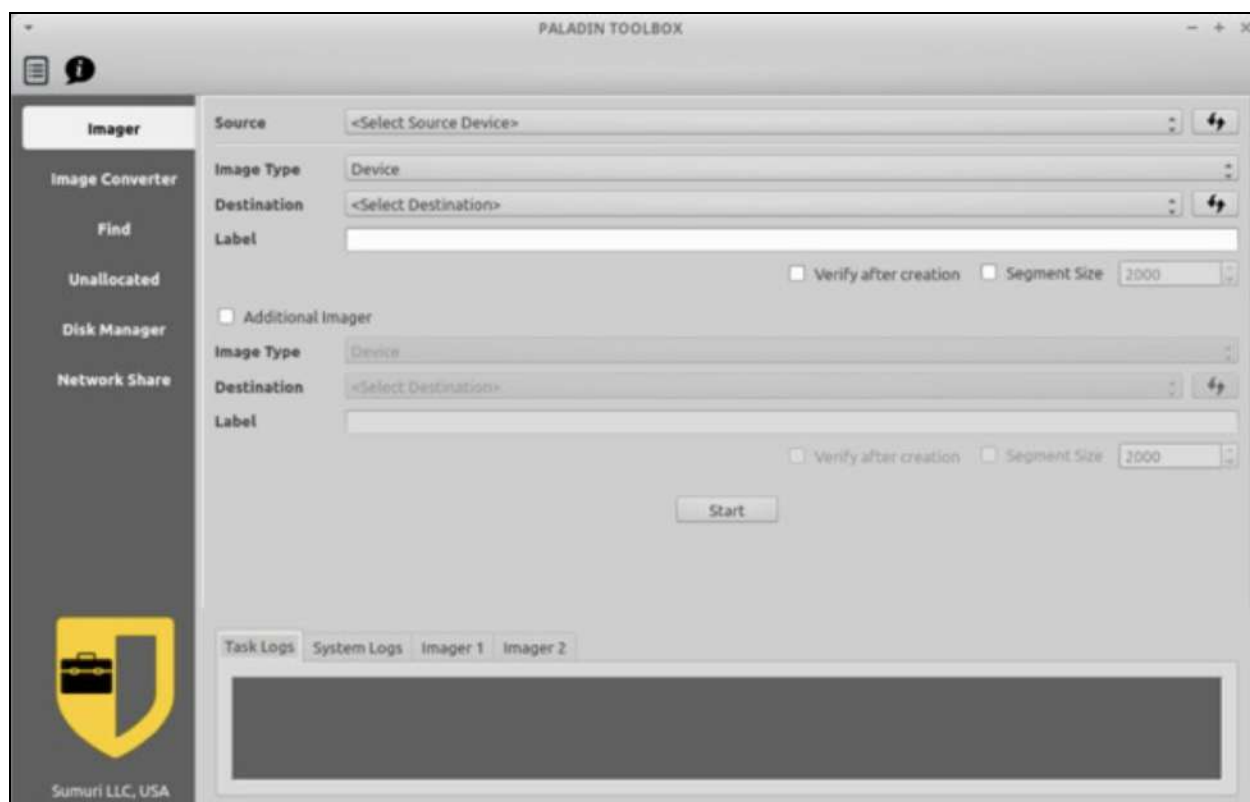
PALADIN Toolbox

The PALADIN Toolbox is the heart of PALADIN. We have worked hard to create a tool and interface to handle a majority of basic and advanced forensic tasks and organized them into a simple to use GUI. The PALADIN Toolbox can be accessed by double-clicking its icon found on the Dock.

Forensic Tools Directory

The Forensic Tools Directory contains pre-compiled applications which have been found useful in forensic examinations and investigations. These tools have been organized by categories that cover a wide range of forensic topics for Windows, Mac, Mobile forensics and more.

PALADIN Toolbox



The PALADIN project was conceived by Steve Whalen in 2006 out of the need to have an easy-to-use low or no-cost solution for imaging and previewing computers. This was released as “Raptor” in 2007. “Raptor” was abandoned in 2010 by Whalen when SUMURI was founded and PALADIN was released. Since 2010, the PALADIN Toolbox has been completely re-written to account for changes to technology and continues to be updated.

The PALADIN Toolbox has combined and simplified multiple forensic tasks into one easy to use GUI (graphical user interface) that requires minimal training and does not require users to utilize the command line.

We are frequently questioned about the validity of the PALADIN Toolbox. As with any tool that you choose to use the validation and testing is your responsibility. Every tool, whether it is ours or someone else’s, should be tested by the examiner prior to using it. We can say that the “engine” that runs the PALADIN Toolbox is a combination of applications that have been used by forensic examiners and investigators for years and have withstood scrutiny within many courts of law. Versions of PALADIN have also been tested by the National Institute of Standards and Technology (NIST).

PALADIN Toolbox - Toolbox

- In this section we will be covering the following:
- Date and Time Settings
- Logging
- Preparing Media (Drives) - Sterilize, Format
- Imaging and Cloning
- Imaging Across a Network
- Converting an Image
- Imaging Unallocated and Free Space Only
- Hashing and Verification
- Mounting a Logical Forensic Image
- Mounting Media (Drives)
- Bitlocker Encryption



The advertisement features a black background with a subtle grid pattern. On the left, a computer monitor displays a software interface with a bar chart. In front of the monitor is a box for the 'RECON LAB FORENSIC SUITE'. To the right, the 'RECON LAB' logo is displayed, consisting of a yellow microscope icon and the text 'RECON LAB'. Below the logo, the text '14X FASTER' is written in large, bold, yellow letters, followed by 'PROCESSING THAN THE LEADING WINDOWS FORENSIC TOOL' in white. A yellow button with the text 'LEARN MORE' is positioned below the text.

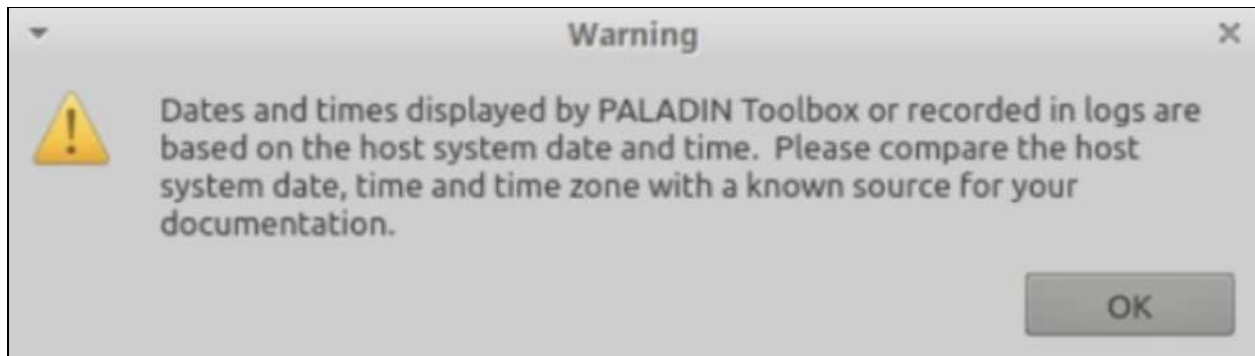
RECON LAB

14X FASTER
PROCESSING THAN THE LEADING
WINDOWS FORENSIC TOOL

[LEARN MORE](#)

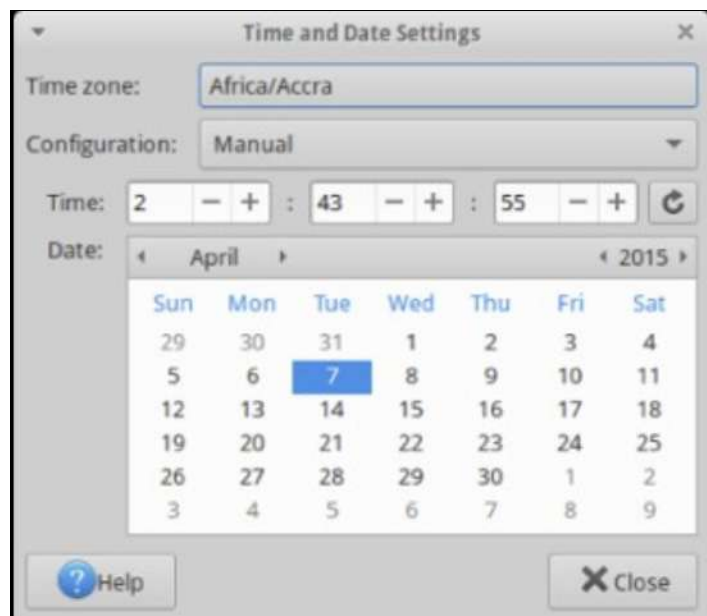
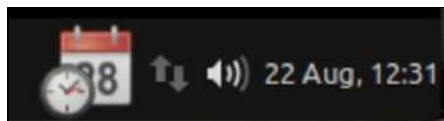
PALADIN Toolbox - Date and Time Settings

When the PALADIN Toolbox is first started a warning message appears.



This message is to remind the examiner that any times recorded in PALADIN logs will be based on the system (computer) date, time and time zone. If the system date, time and time zones are wrong on the computer then the log dates and times will also be incorrect. It is important to always check the system time with a known time (e.g. atomic wristwatch) and document both the system time and the actual time in your notes.

The default Time Zone in PALADIN is GMT. To change the time zone click on the Time and Date icon found at the bottom of the desktop to access its settings.



Note: It may take a minute or two for the displayed system clock to update.

PALADIN Toolbox - Logging

There are two main types of logs in PALADIN:

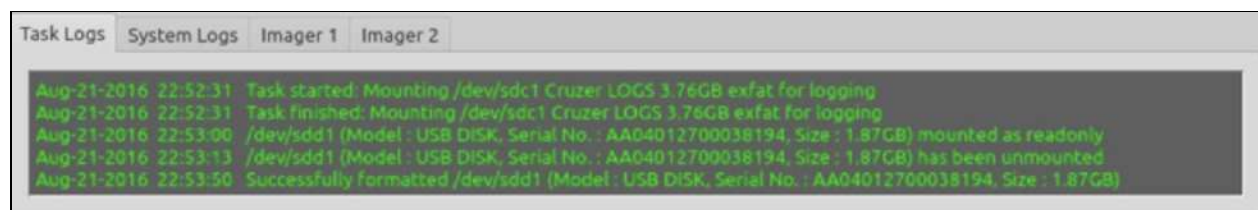
- Task Logs
- System Logs
- Module Specific Logs

All the logs are found in tabs at the bottom of the PALADIN Toolbox window.

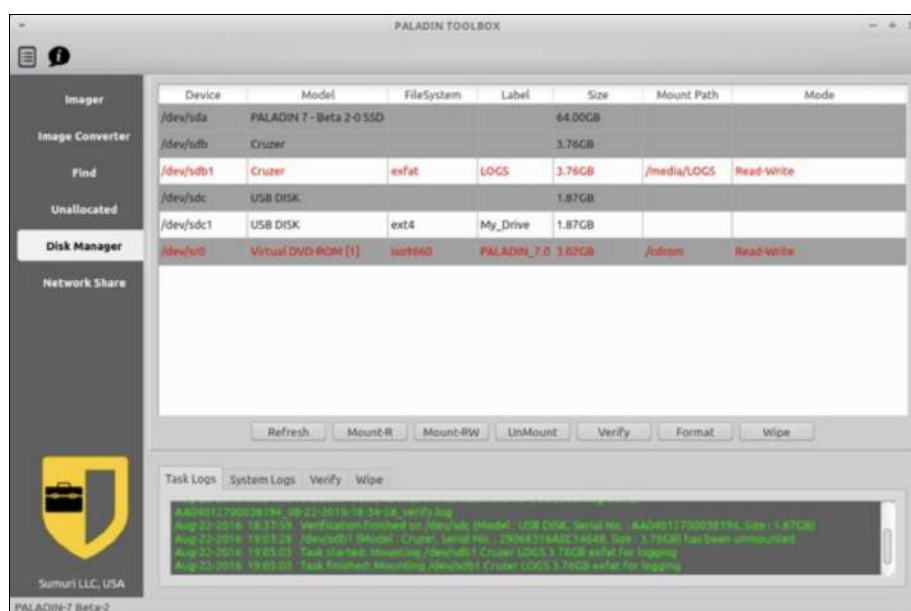
Task Logs keep a historical record of the “tasks” that have been executed within a single PALADIN Toolbox session.

System Logs display information to assist with troubleshooting.

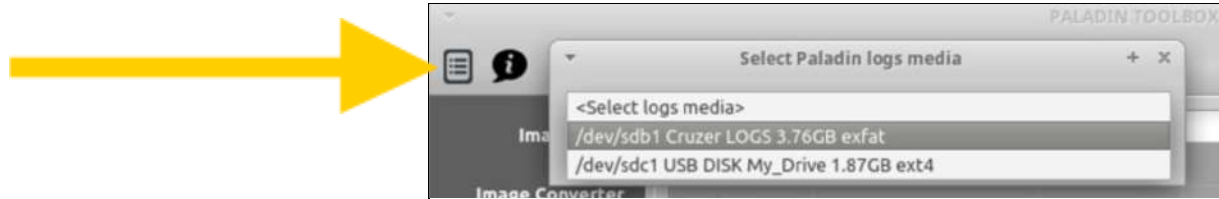
Module Specific Logs show information relating to the current module being used and typically shows live information. For example, in the image below you are seeing Module Specific Logs for the Imager Module (“Imager 1” and “Imager 2”).



Logs in PALADIN Toolbox can be saved automatically to a destination drive of your choice. Insert and drive where you would like your logs to be stored. If necessary, you can prepare the drive using the Disk Manager in the PALADIN Toolbox.

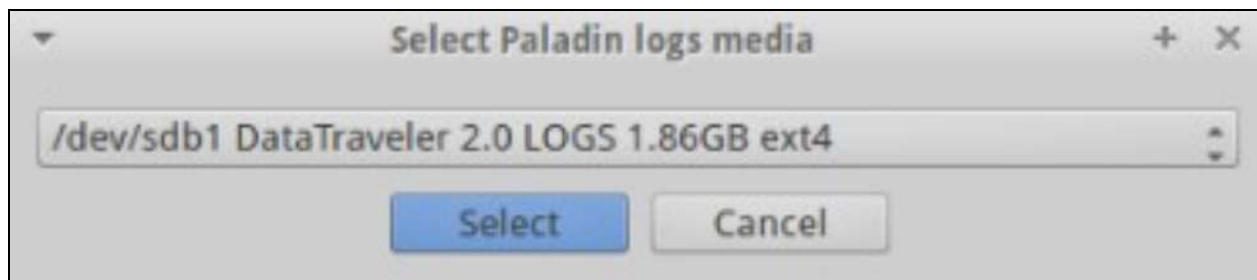


Click the “Logs” icon in the upper right-hand corner of the PALADIN Toolbox Window.

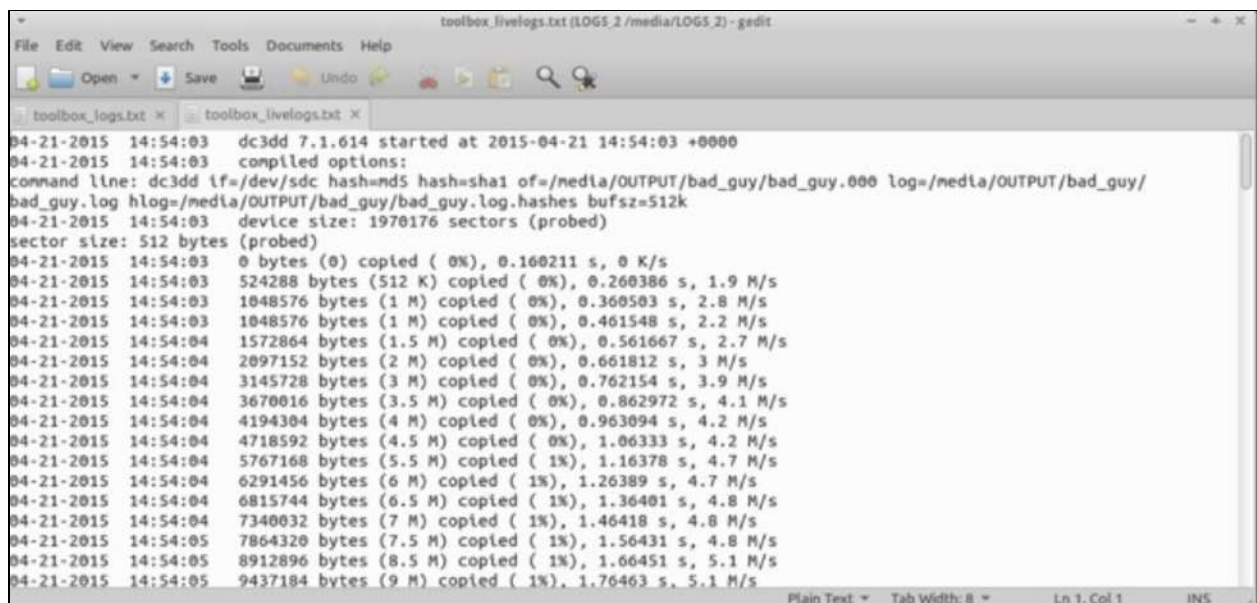


PALADIN Toolbox - Automatic Logging

A dropdown box will appear giving you the option of selecting a connected drive to store your PALADIN Toolbox Logs.



Logs from the Imager and Unallocated tabs will now be saved automatically to the drive you selected in text format.



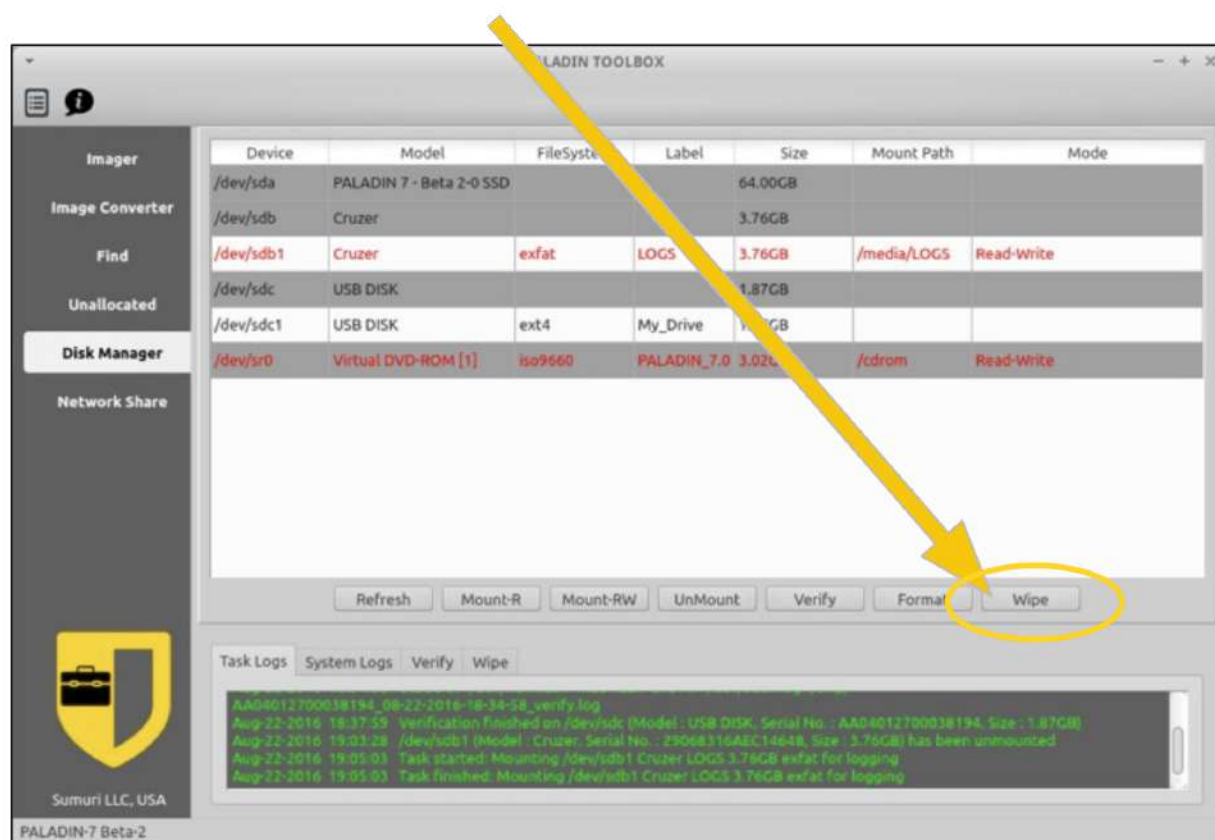
PALADIN Toolbox - Preparing Media - Sterilize (Wiping)

Many agencies require that media to be used for the storage of evidence must be “wiped” or “sterilized” to ensure that it is free from pre-existing data.

PALADIN Toolbox sterilizes media by writing “zeros” to the entire device with a single pass. Toolbox gives you the option to perform a verification to ensure that the drive only consists of zeros. Most tools tend to hash the drive with a CRC-64 algorithm which will return a result of zero if properly wiped. Any algorithm takes time to calculate.

PALADIN Toolbox speeds up the process of verification by simply scanning the device for anything that is not a zero which is much more efficient and faster. The results of this scan are either pass or fail.

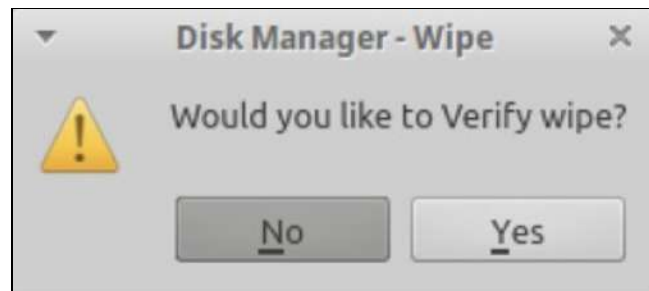
To sterilize a drive navigate to the Disk Manager tab, highlight the physical drive that you want to sterilize and click “Wipe”.



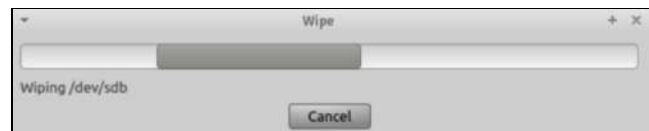
Once you have clicked “Wipe” Toolbox will ask you if you are sure ... ONCE!



PALADIN Toolbox will then ask if you would like to “Verify” the Wipe.



Wiping of the device that you selected now begins.



“Device Wiped successfully” message appears after successful verification. The device is now ready for formatting if desired.

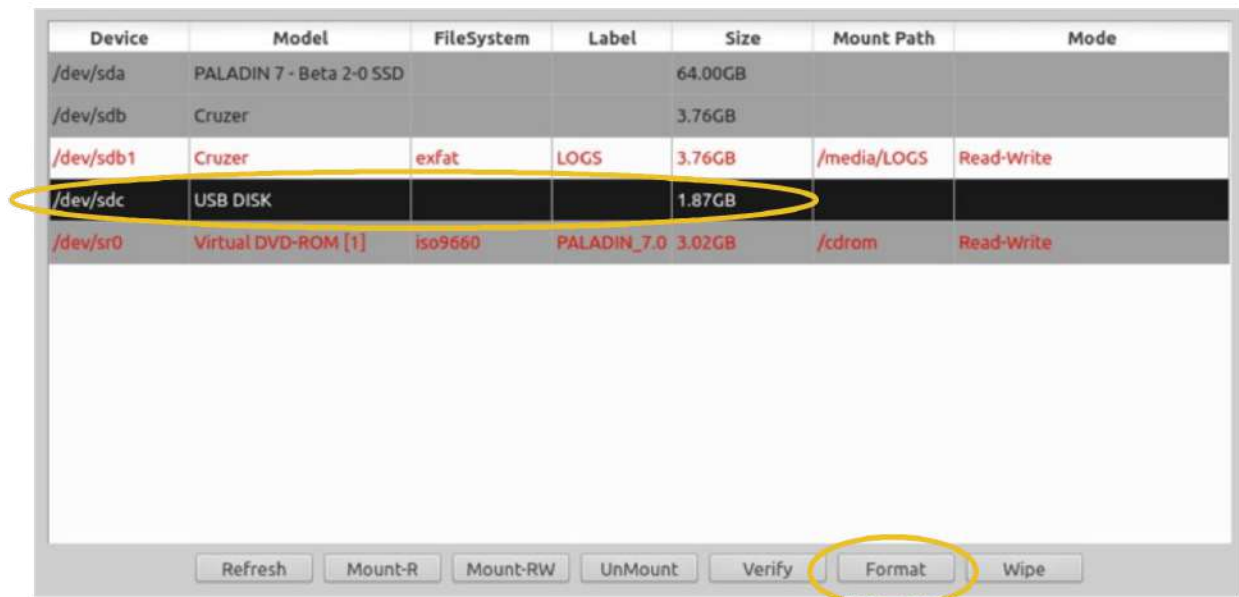


PALADIN Toolbox - Preparing Media - Formatting

PALADIN Toolbox supports makes it easy to format a device with anyone of five File Systems:

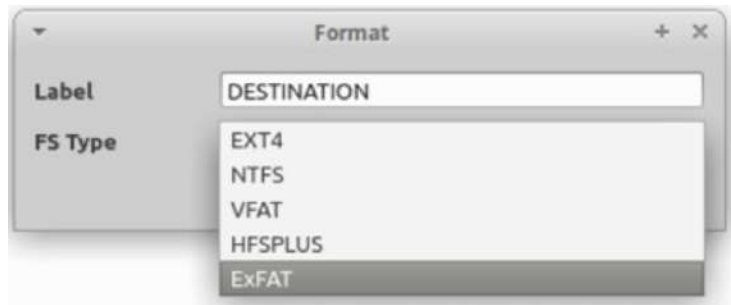
- Linux EXT4
- NTFS
- VFAT (FAT32)
- HFSPLUS (Mac OS X Extended - no journaling)
- ExFAT

From the Disk Manager select the drive or volume to format and then select the “Format” button.

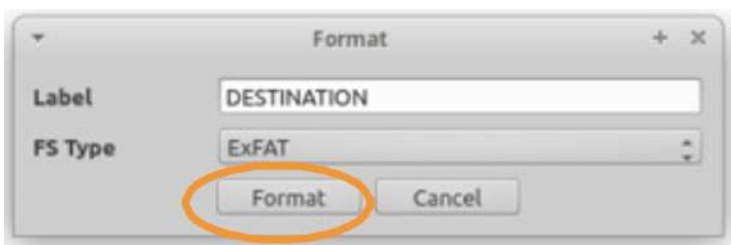


PALADIN Toolbox - Formatting

In the “Format” window provide a name for the Volume and choose your File System type.



When ready select the format button to begin.



Verification of the formatting can be found in the Task Logs. Once the format is completed click the “Refresh” button in the Disk Manager to re-poll the devices to show the newly formatted volume.

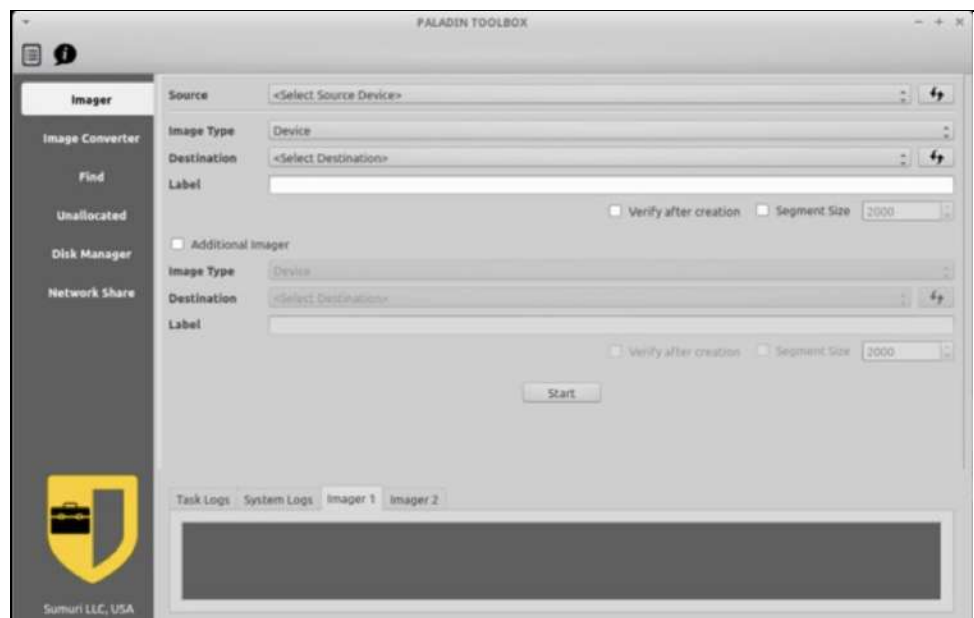
PALADIN Toolbox is the easiest way to image a device in a forensically sound manner. Since PALADIN is based on Ubuntu a majority of modern and legacy hardware is supported. This includes PCs, Macs, internal hard drives, external hard drives, RAIDs, and servers. All without the need for hardware write-blockers. Several versions of the PALADIN Toolbox have already been tested by the NIST (National Institute of Standards and Technology).

PALADIN Toolbox supports the following forensic image formats (types):

- **DD** (raw uncompressed output)
- **EWf** (Expert Witness Format or .E01)
- **EWf2** (Expert Witness Format - Version 2 or .Ex01)
- **SMART** (ASR Data Image format - www.asrdata.com)
- **DMG** (Apple Disk Image format - same as DD, raw uncompressed output)
- **VMDK** (VMWare Virtual Disk Format which can be used for virtualization in a tool such as SUMURI's **CARBON**)
- **Device** (for device cloning, to be discussed later)

PALADIN Toolbox - Imaging a Drive

Imaging functions can be found in the PALADIN Toolbox Imager Module.



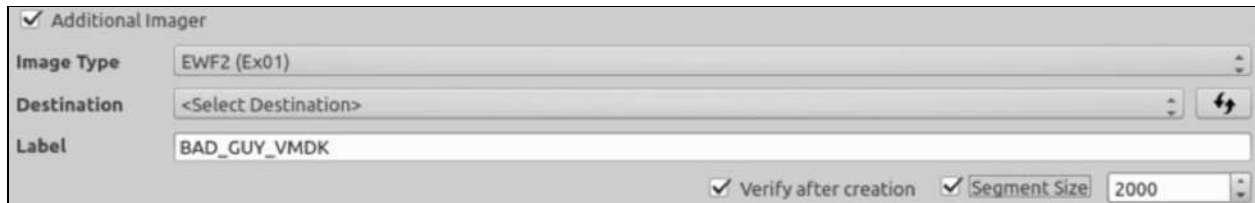
- **Source** = Select the physical or logical drive that you want to image.
- **Image Type** = This is where you select the type of forensic image for the output or select "Device" to make a clone.
- **Destination** = This is the volume where you want your forensic image to go.
- **Label** = Name for your image (no spaces).
- **Verify after creation** = Select this if you want to hash the forensic image files after they have been created (SHA-1 and MD5).
- **Segment Size** = Select this if you would like to divide your forensic image file into smaller segments or "chunks". Due to Linux FAT32 limitations (VFAT), 2000 Mb is the largest size allowed.
- **Start** - Starts imaging once your parameters are set.

Any drives connected while PALADIN boots or drives that are plugged in afterward are write-protected automatically.

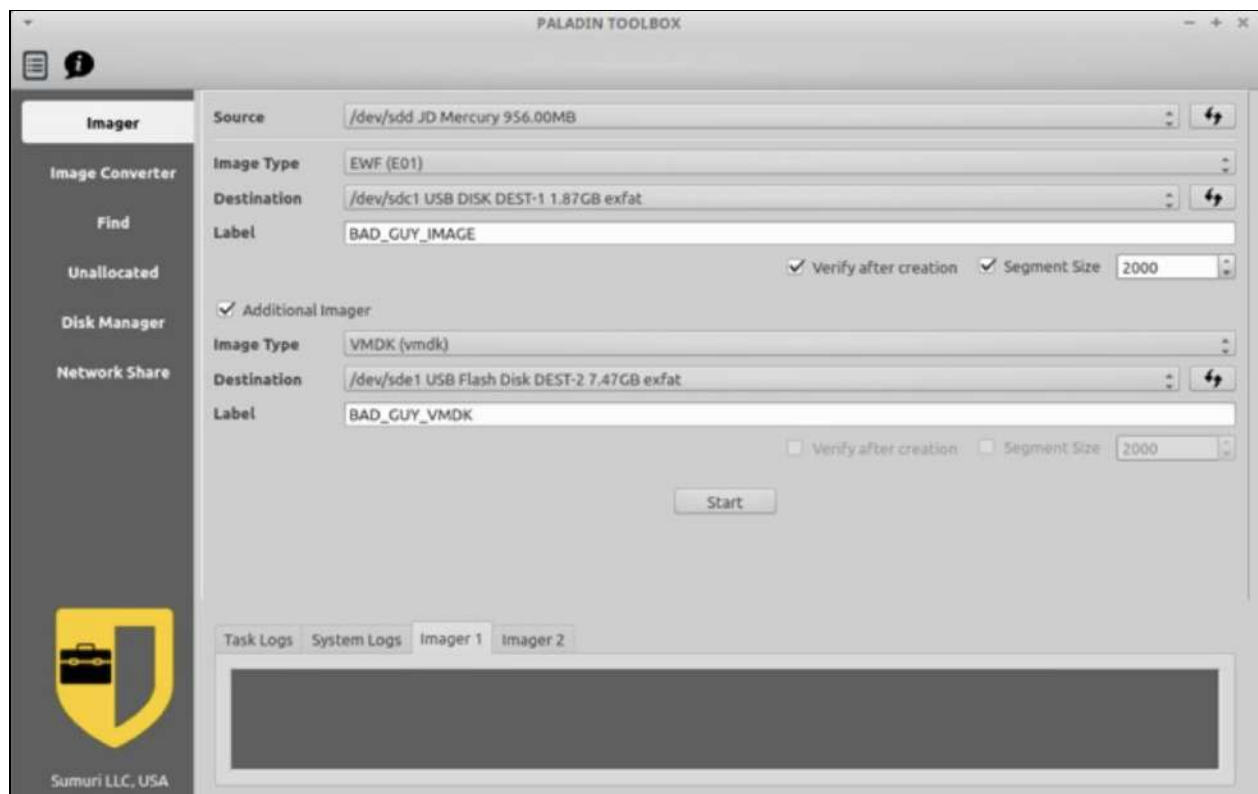
There is no need to pre-mount any devices or drives for imaging. PALADIN automatically mounts the destination drive that you have selected.

Imaging to an Additional Drive or Creating Two Different Images

PALADIN Toolbox supports imaging to two separate destinations or as a different format on a single destination drive in a different format by selecting the “Additional” box. It is important to remember if you are using the “Additional” image option you must use a different “Label” for each image to avoid overwriting.



PALADIN Toolbox - Imaging a Drive



The example of the above shows the following configuration:

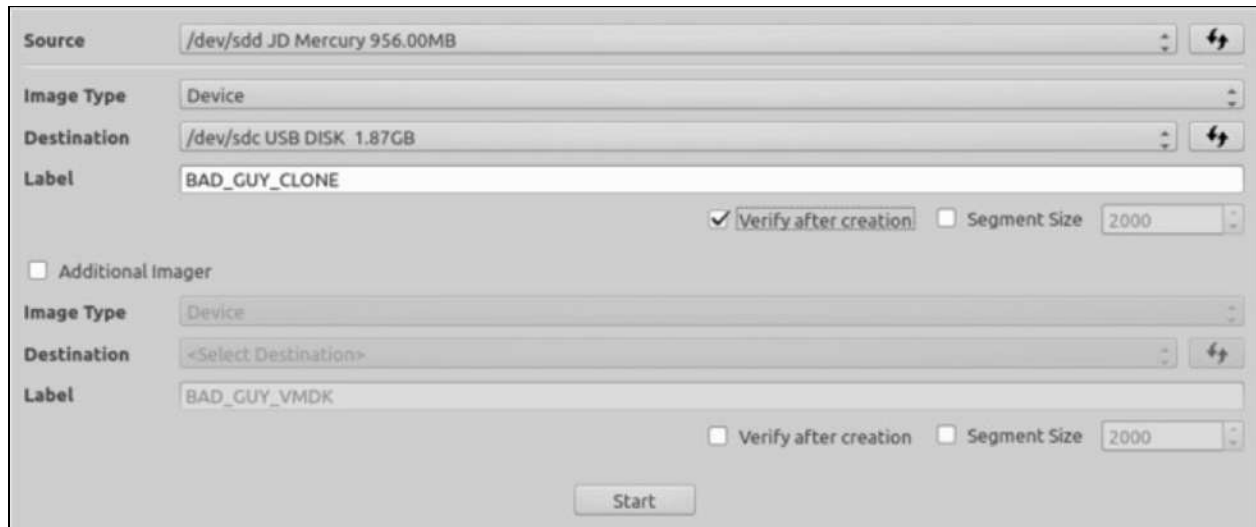
A single physical drive (/dev/sdd JD Mercury) being imaged to a collection drive (/dev/ sdc1 “DEST-1” volume) and then as a Virtual Machine image to a second drive “DEST-2”.

The first is an .E01 format with the name “BAD_GUY_IMAGE”. The second (“Additional”) image is a .vmdk format with the name “BAD_GUY_VMDK”.

The EWF format will be hashed after the completion of the imaging (“Verify after creation”) and will be segmented into 2GB “chunks” if the source is larger than 2 GBs (“Segment Size”).

PALADIN Toolbox - Cloning a Drive

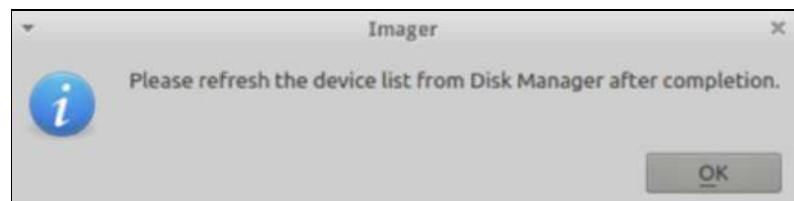
PALADIN Toolbox provides the ability to clone devices through the Device Imager Tab. When cloning a drive make sure that your destination drive is larger than the source. Keep in mind that even though devices are advertised as being the same size this is not always true.



The screenshot shows the 'Device Imager' window in PALADIN Toolbox. It has two main sections for cloning. The top section has 'Source' set to '/dev/sdd JD Mercury 956.00MB', 'Image Type' set to 'Device', 'Destination' set to '/dev/sdc USB DISK 1.87GB', and 'Label' set to 'BAD_GUY_CLONE'. It also has a checked 'Verify after creation' checkbox and a 'Segment Size' of 2000. The bottom section is disabled, with 'Additional Imager' unchecked, 'Image Type' set to 'Device', 'Destination' set to '<Select Destination>', and 'Label' set to 'BAD_GUY_VMDK'. A 'Start' button is at the bottom.

To clone a device simply select the physical drive from the “Source” field. In “Image Type” select “Device”. In the “Destination” field select the drive that will become the clone. Finally, provide any name in the Label field and press start.

Once the cloning is complete you may need to re-poll the devices by selecting “Refresh” within the Disk Manager.



PALADIN Toolbox - Imaging Across a Network

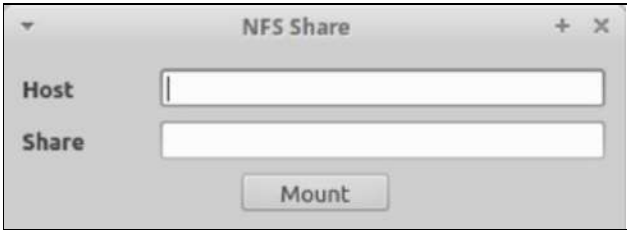
One of the coolest features of the PALADIN Toolbox is its ability to image across a network. This could be from your workstation to an Image Server or it could be out in the field imaging a large RAID or server to a NAS (Network Attached Storage) that you brought along. As long as you have set up a Samba (SMB) or Network File Share (NFS) share for a folder or drive you are good to go!

The following information is needed to create a successful **SMB connection** in the PALADIN Toolbox (SMB is the default Windows network protocol):

- **Host** - Typically, the IP Address of the server.
- **Username** - Your user logon.
- **Password** - the password for your username.
- **Domain** - optional.
- **Share** - this is the drive or directory that you are sharing.
- **Read Only** - "No" is used to mount your remote directory read-write. "Yes" is to mount your remote directory read-only.



The following information is needed to create a successful **NFS connection** in the PALADIN Toolbox:

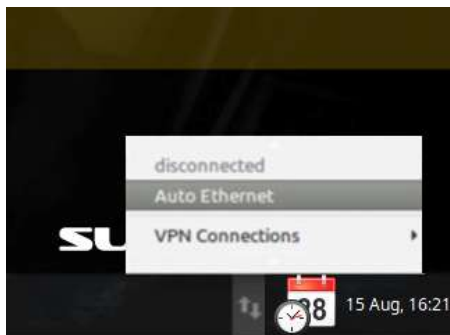
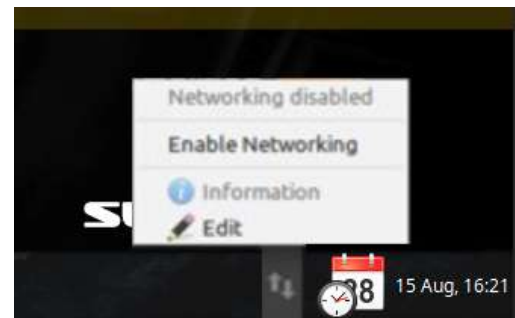


- **Host** - Typically, the IP Address of the server.
- **Share** - this is the drive or directory that you are sharing.

PALADIN Toolbox - Imaging Across a Network

By default, networking is disabled and remains silent if a computer is on a network. To begin, you must enable networking in PALADIN.

To enable networking in PALADIN locate the double arrows next to the date in the bottom right-hand corner and click them to bring up the menu. Select “Enable Networking” from the menu.



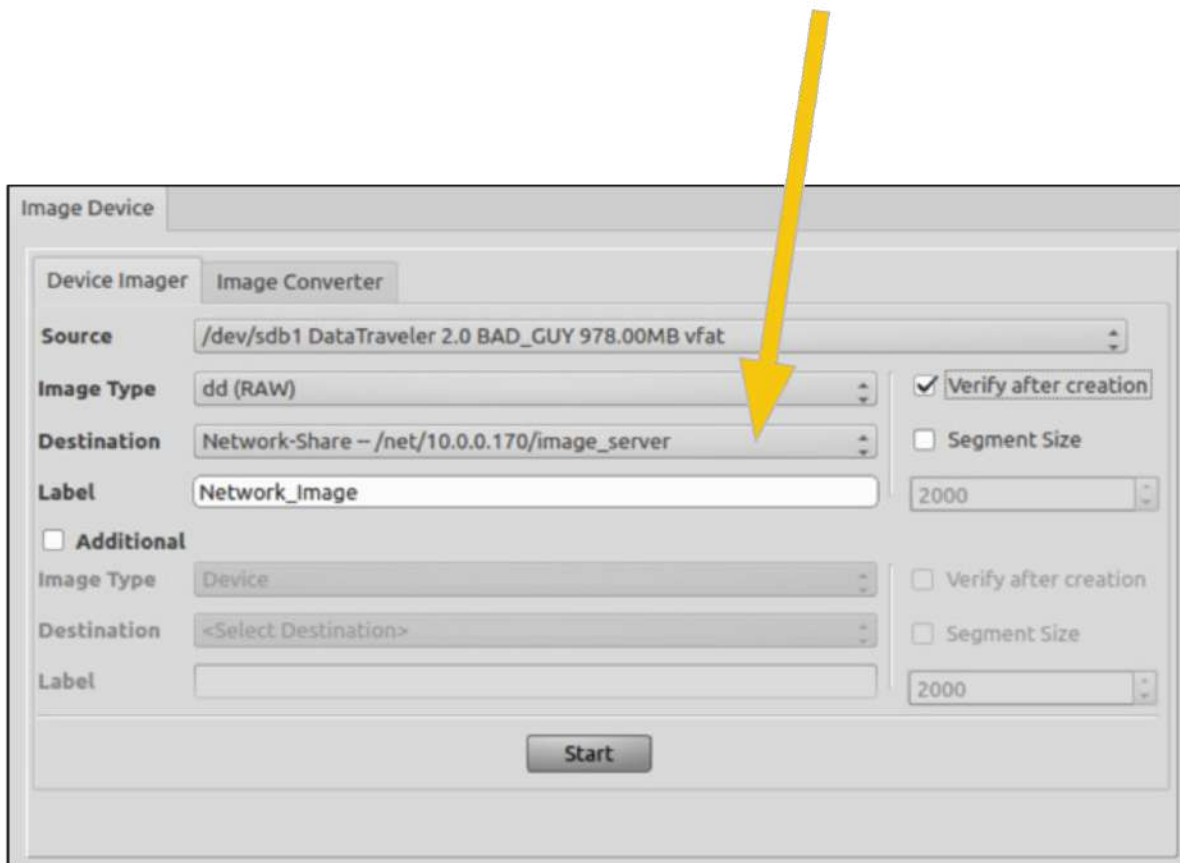
Once the network is enabled select “Auto Ethernet” if you have DHCP active. For wired connections, you will be ready to connect at this point. If you are using a wireless connection, return to the networking menu and select the correct SSID (wireless network).

Now that the network is up and running you can now connect the PALADIN Toolbox to your server by using the “Network Share” module and entering your SMB or NFS connection settings and click “Mount”.



PALADIN Toolbox - Imaging Across a Network

Upon successful connection, your SMB or NFS share will be available in the “Destination” dropdown in the Imaging module.



PALADIN Toolbox - Converting a Forensic Image

PALADIN has the ability to convert forensic images from one type to another using the “**Image Converter**” Module. Make sure that you have a drive mounted read-write with the images that you would like to convert.

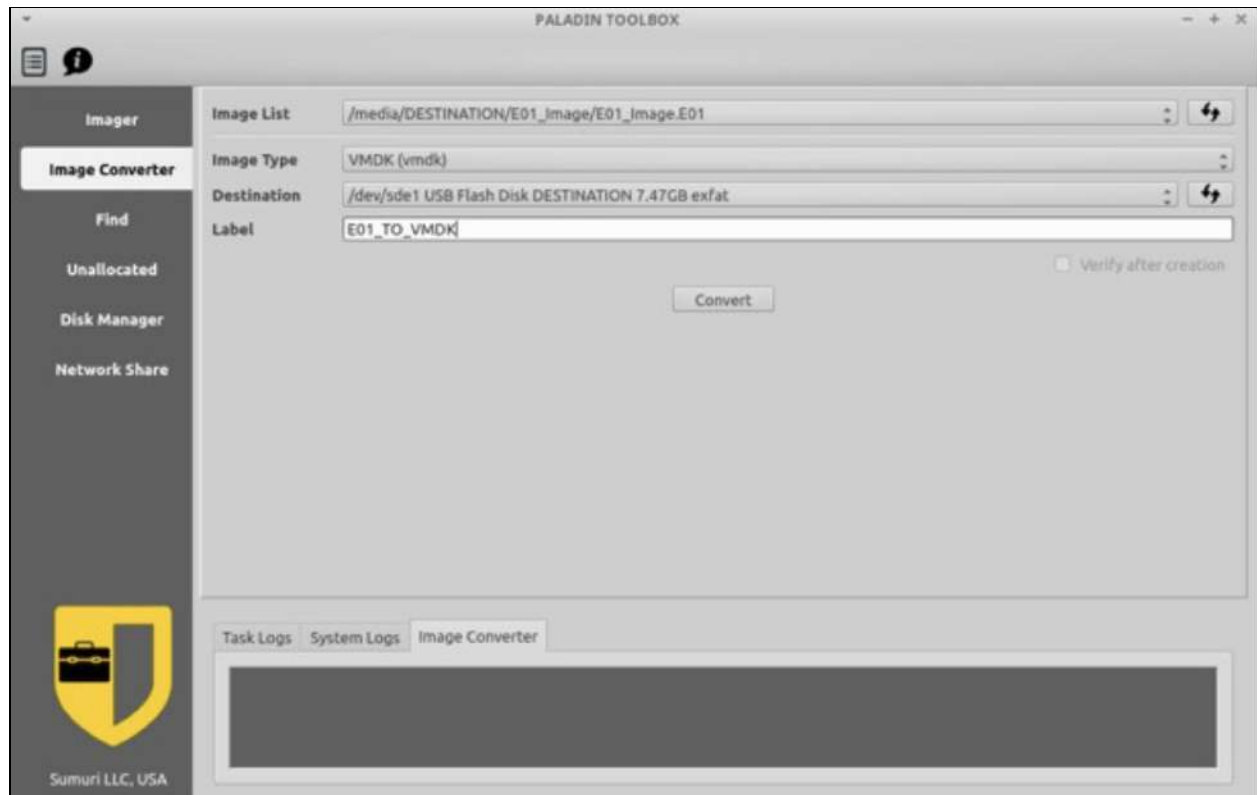


Image List - your forensic images to convert. If you do not see your images hit the refresh button next to the dropdown box.

Image Type - select the new format for the forensic image.

Destination - where to send the new image format.

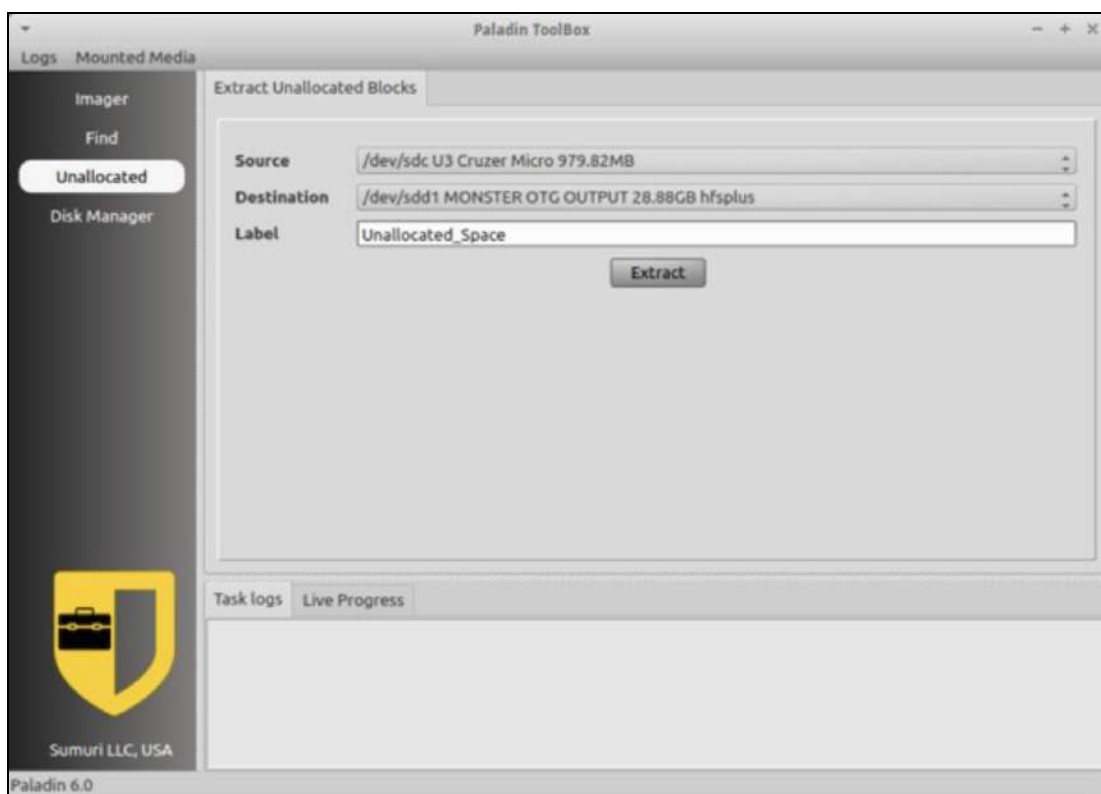
Label - enter a name for the conversion.

Click “**Convert**” to begin.

PALADIN Toolbox - Imaging Unallocated Space

Another useful feature of PALADIN is its ability to image only the Unallocated Space and Free Space (unpartitioned space) to as raw image files that can be later carved for data. Unallocated Space and Free Space are areas where deleted files are typically found.

To begin extracting the Unallocated space and Free Space select “**Unallocated**” from the Toolbox sidebar.



Source - select the device for unallocated and free space extraction.

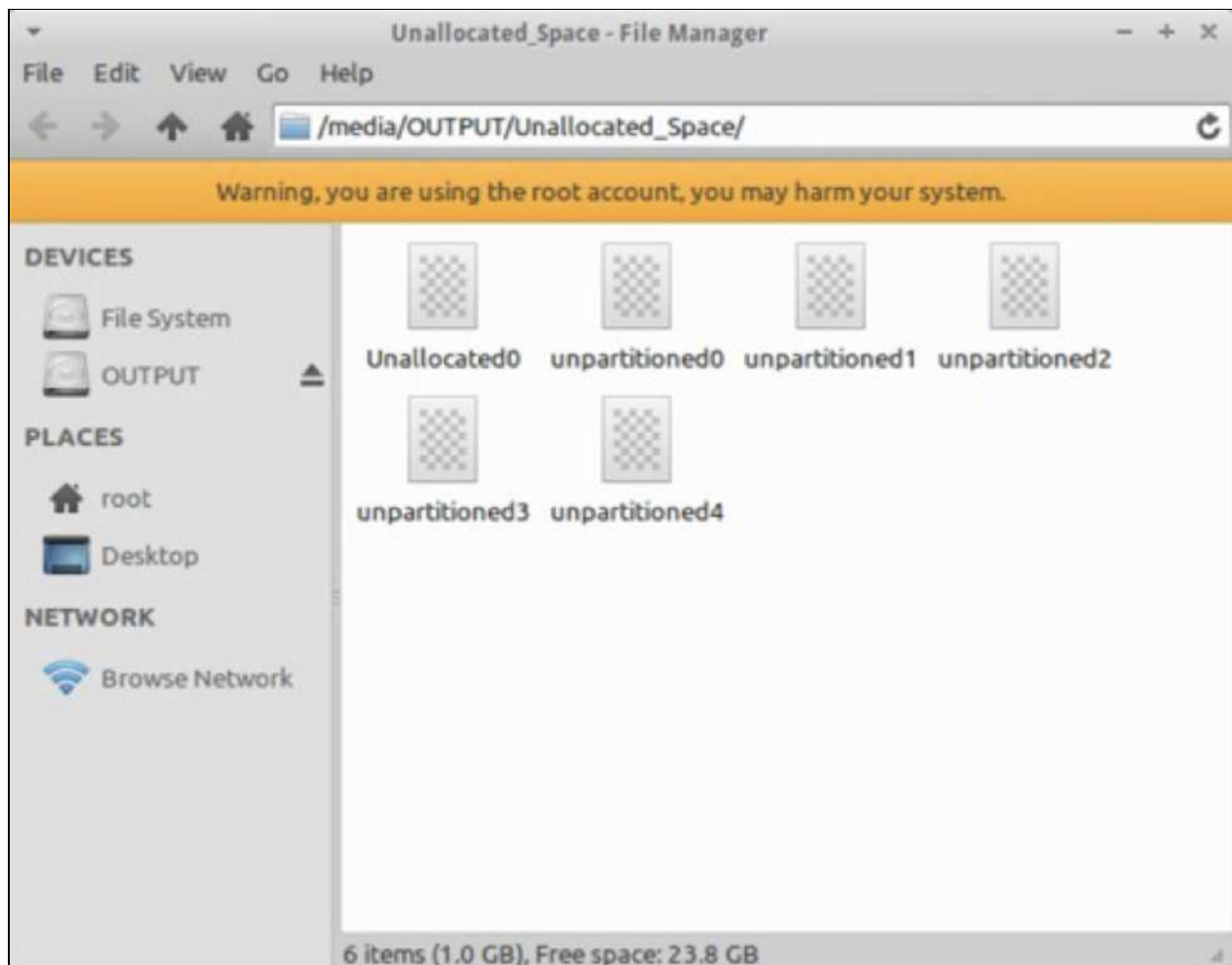
Destination - select the drive that will store the extracted data.

Label - enter a name for the session.

Click “**Extract**” to begin.

PALADIN Toolbox - Imaging Unallocated Space

Upon completion, an explorer will open showing the files containing the extracted unallocated and free space.

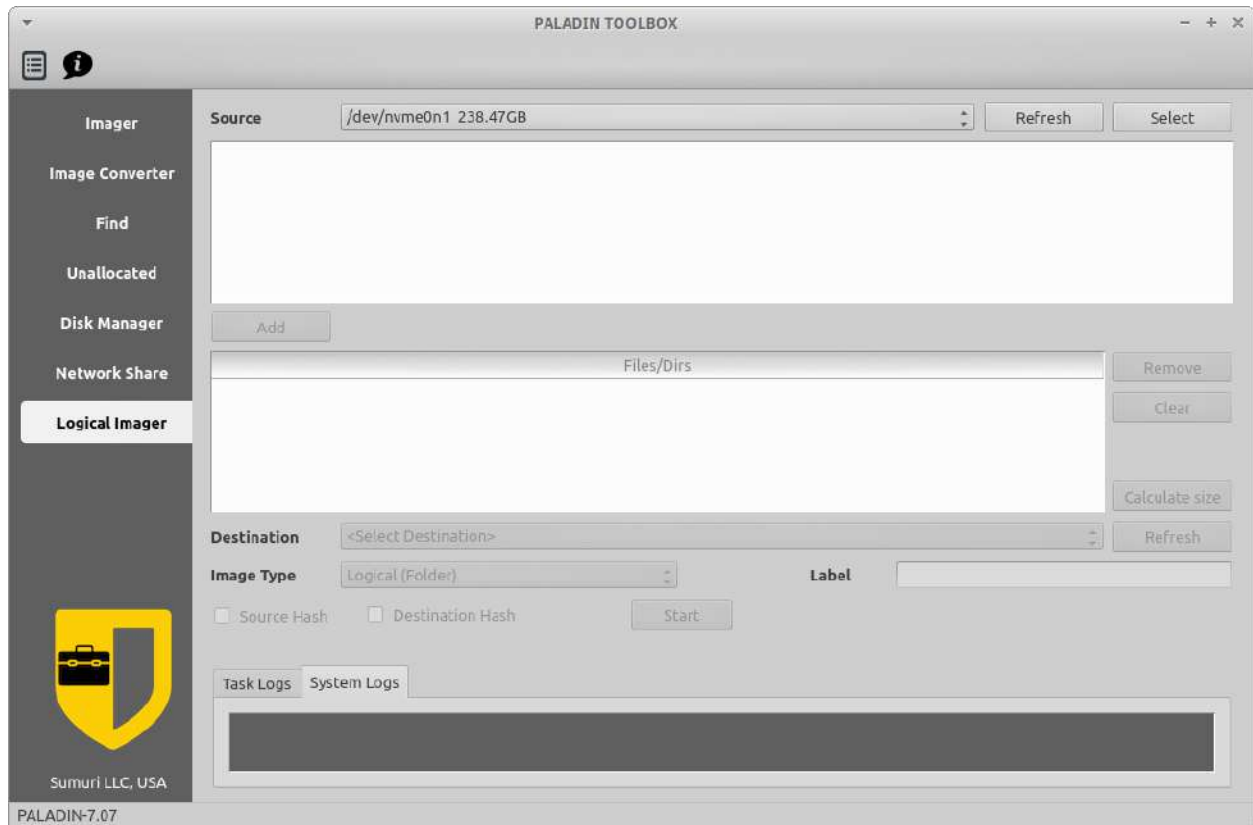


These files can be carved with a variety of tools. The following data carving tools can be found in the PALADIN Forensic Apps directory under "Carving Tools":

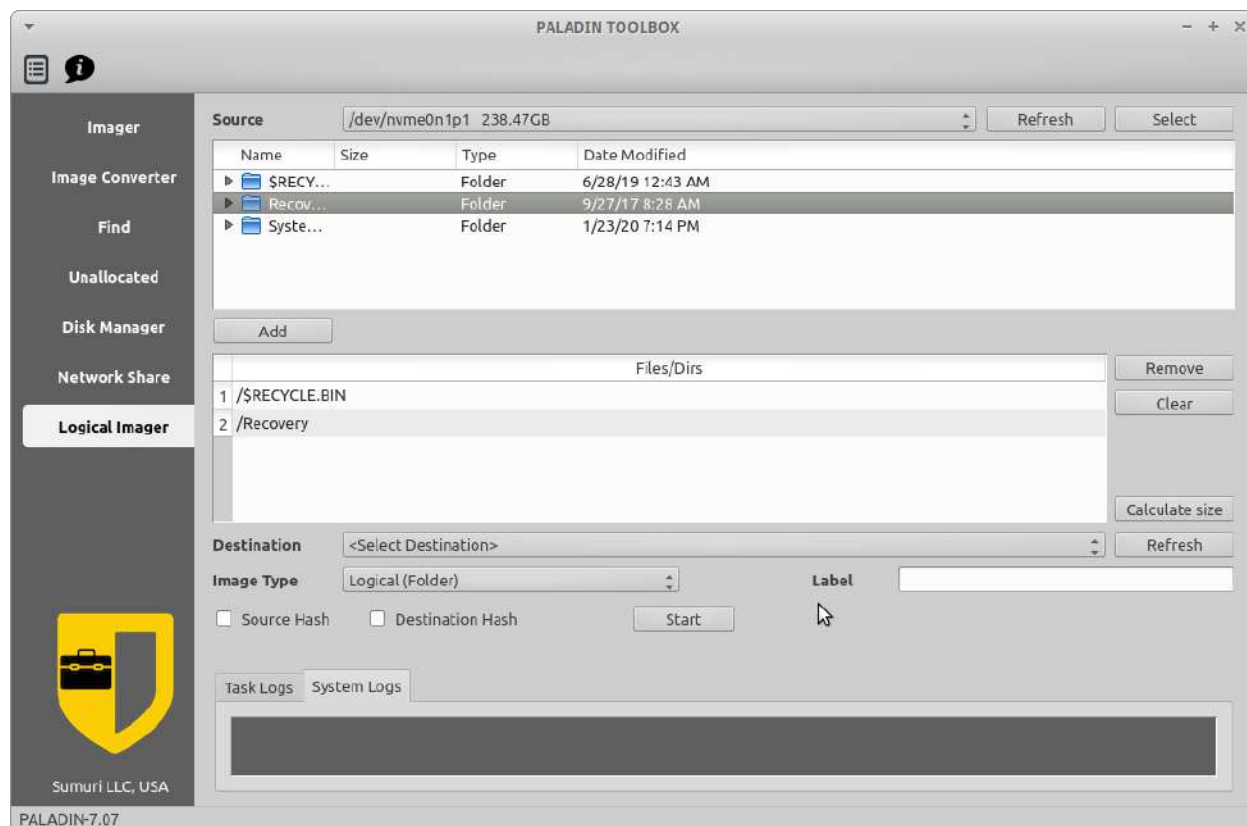
- Foremost
- Photorec
- Scalpel
- TestDisk
- and more!

PALADIN Toolbox - Logical Imaging

The Logical Imager option allows the examiner to image folders and files and can be accessed through the Logical Imager module.



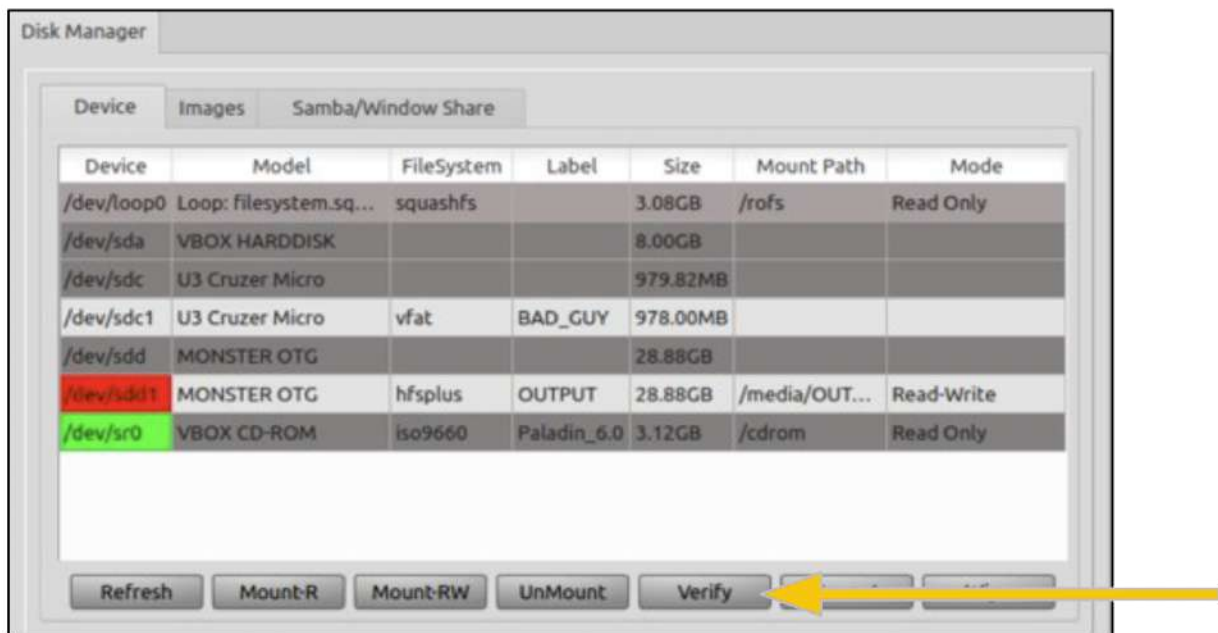
Once the source is selected individual folders and/or files can be selected and sent to a destination. The image can also be hashed at both the source and destination.



PALADIN Toolbox - Hashing

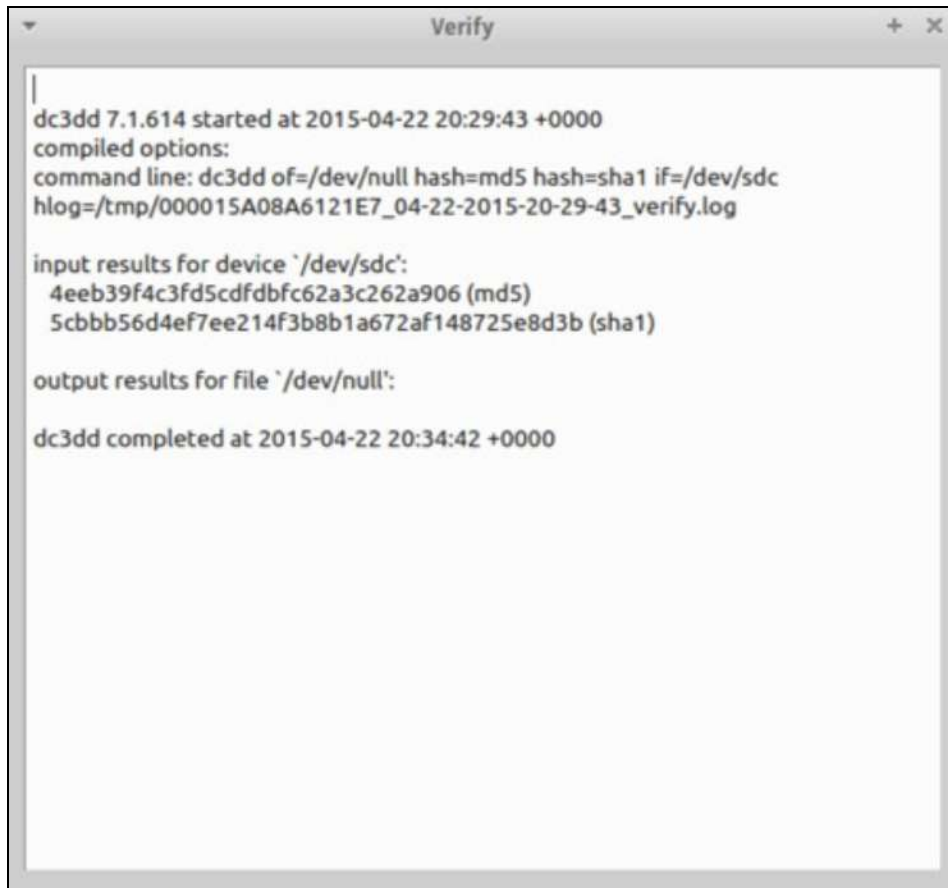
Physical disks and volumes verified or hashed within PALADIN Toolbox under Disk Manager. Both an MD5 and a SHA-1 value will be calculated.

For physical devices or logical volumes select the device or volume to be hashed and click “Verify” to begin.



PALADIN Toolbox - Hashing

Upon completion of the verification/hashing, the results window will appear with an MD5 and SHA-1 hash values.



```
Verify
|
dc3dd 7.1.614 started at 2015-04-22 20:29:43 +0000
compiled options:
command line: dc3dd of=/dev/null hash=md5 hash=sha1 if=/dev/sdc
hlog=/tmp/000015A08A6121E7_04-22-2015-20-29-43_verify.log

input results for device `/dev/sdc':
  4eeb39f4c3fd5cdfdbfc62a3c262a906 (md5)
  5cbbb56d4ef7ee214f3b8b1a672af148725e8d3b (sha1)

output results for file `/dev/null':

dc3dd completed at 2015-04-22 20:34:42 +0000
```


PALADIN Toolbox - Mounting and Unmounting

Whenever using PALADIN the mounting and unmounting of drives should be done through the PALADIN Toolbox. This will ensure that the Toolbox works correctly and attached devices are not accidentally altered. Mounting and unmounting occurs in the Disk Manager module. Simply highlight a device or volume and click the appropriate button.



GREEN - mounted read-only

RED - mounted read-write

- **Refresh** - re-polls attached devices for changes.
- **Mount-R** - mounts volumes read-only.
- **Mount-RW** - mounts volumes read-write.
- **UnMount** - Unmounts a mounted volume.

PALADIN Toolbox - Mounting and Unmounting

For convenience, we have added the Mounted Media Folder Icon in the dock to find currently mounted Devices, Images, and Network Shares.



Once the mount type is selected an explorer window will open showing currently mounted items.



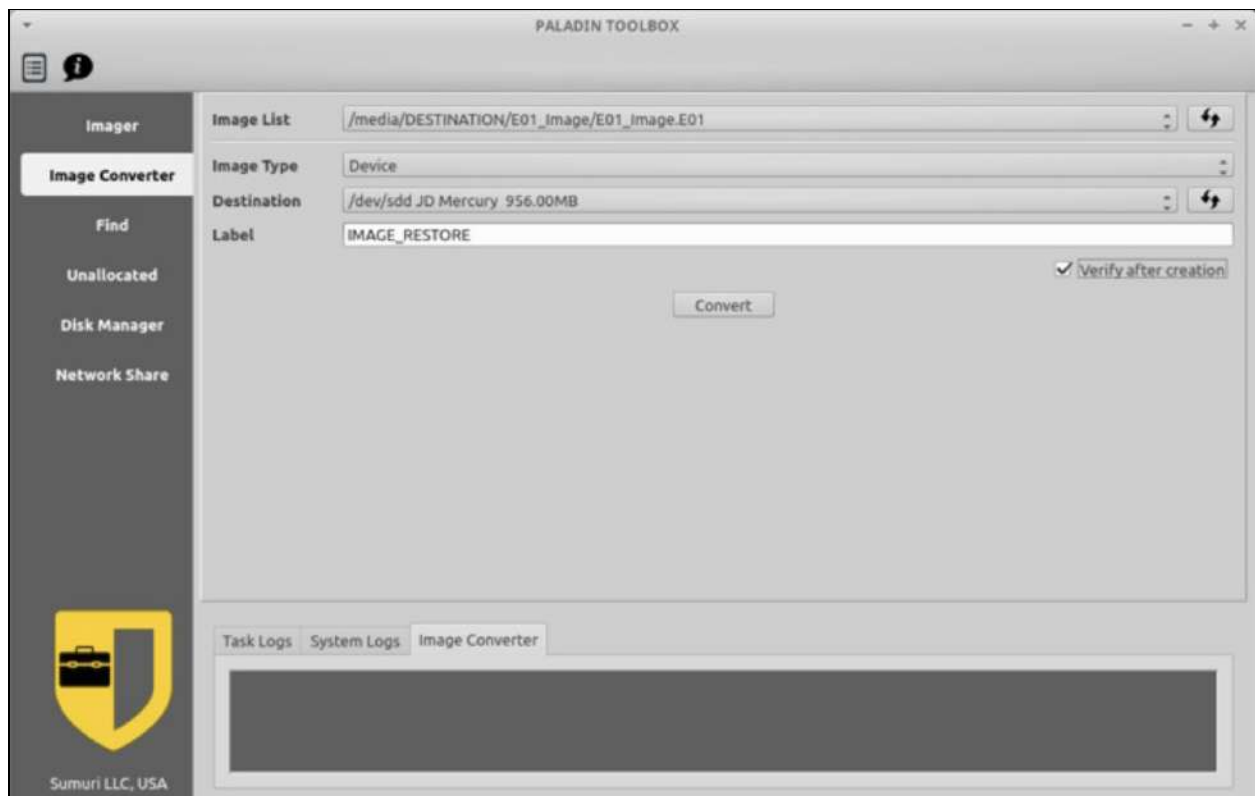
PALADIN Toolbox - Restoring a Forensic Image

To restore a forensic image back to a physical disk use the Image Converter module.

Make sure that the device containing the forensic image to be restored is mounted read-write. If you do not see your image in the drop down please select the refresh tab. Select the forensic image to be restored from the “Image List”.

Set the “Image Type” to “Device”.

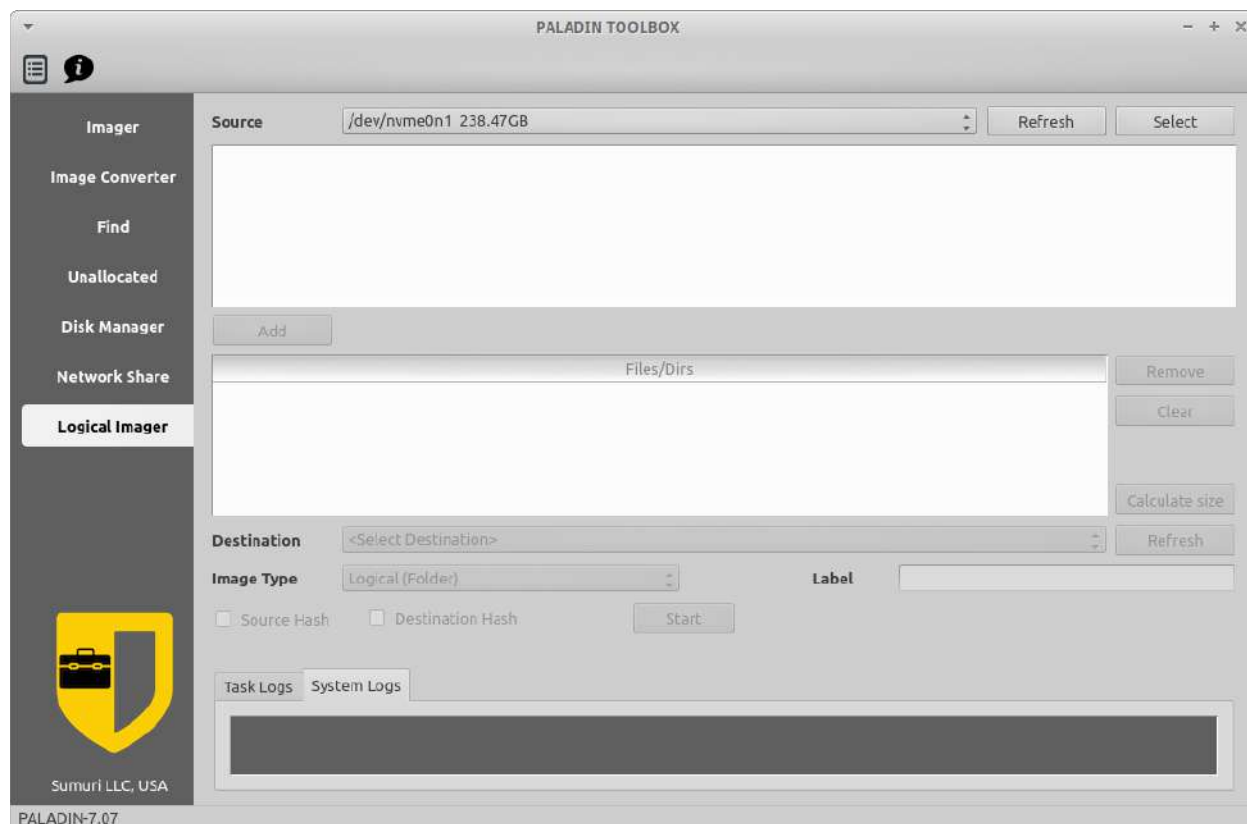
In “Destination” select the drive to be restored. Provide a name in “Label” and select “Convert”.



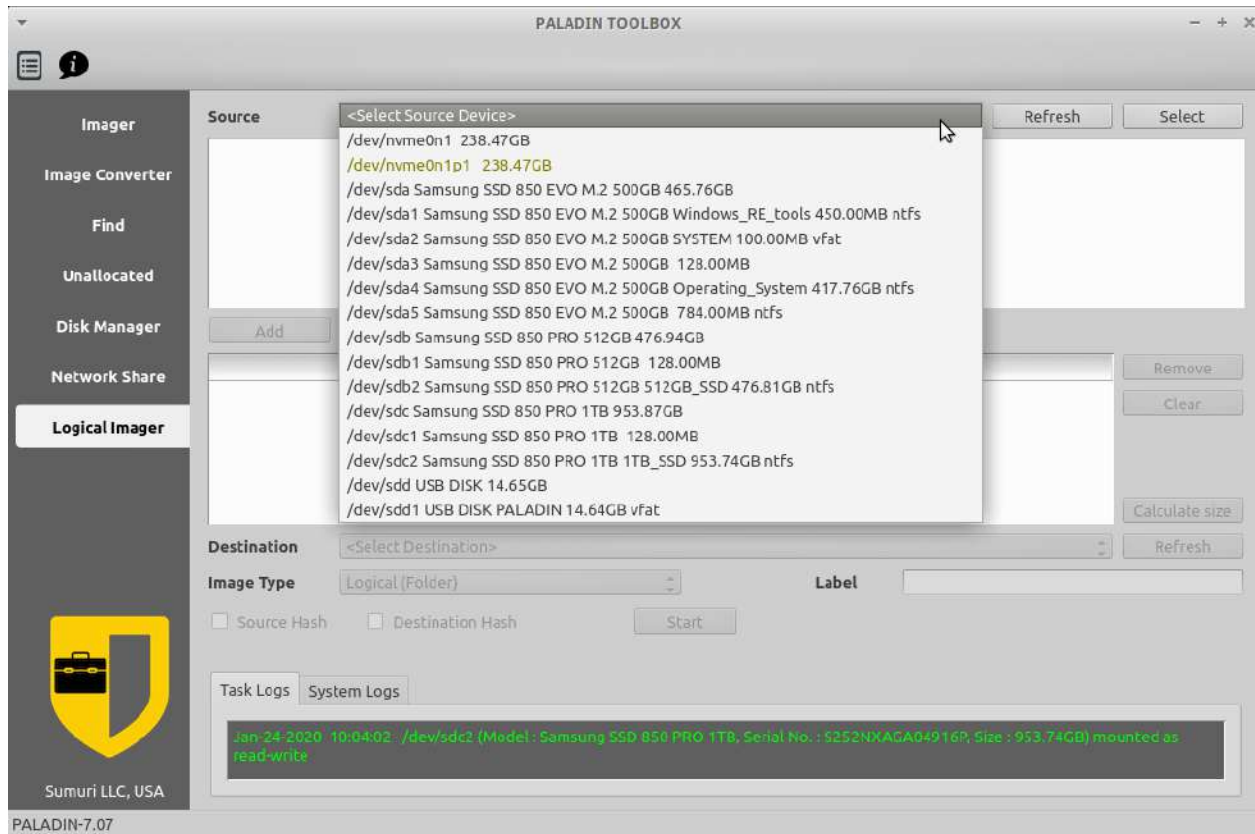
PALADIN Toolbox - Bitlocker Decryption

BitLocker is a full volume encryption feature included with Microsoft Windows (Pro and Enterprise only) versions starting with Windows Vista.

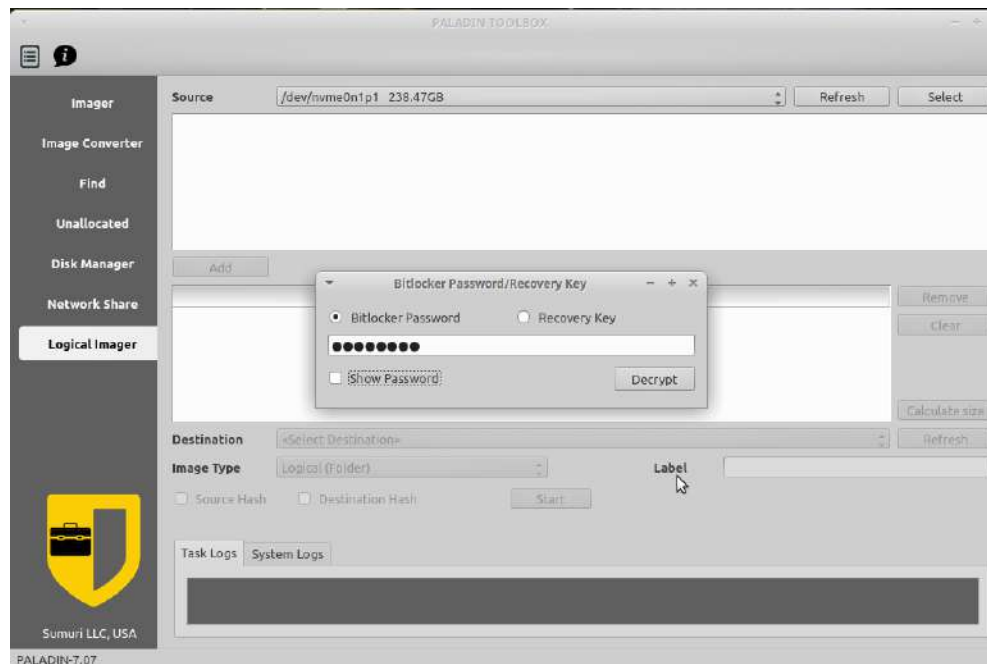
To decrypt a BitLocker partition in PALADIN Toolbox select the Logical Imager module.



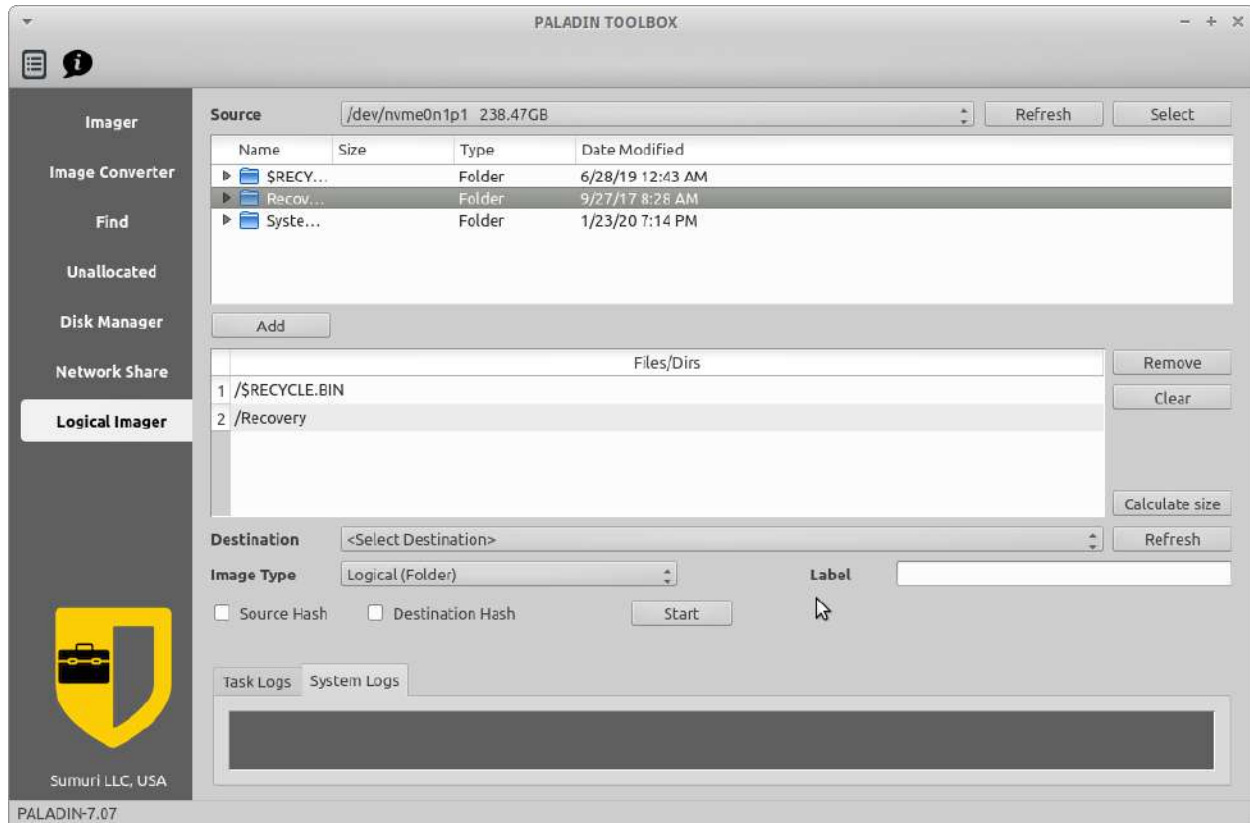
The source dropdown will display all the available partitions and BitLocker encrypted partitions will have olive text.



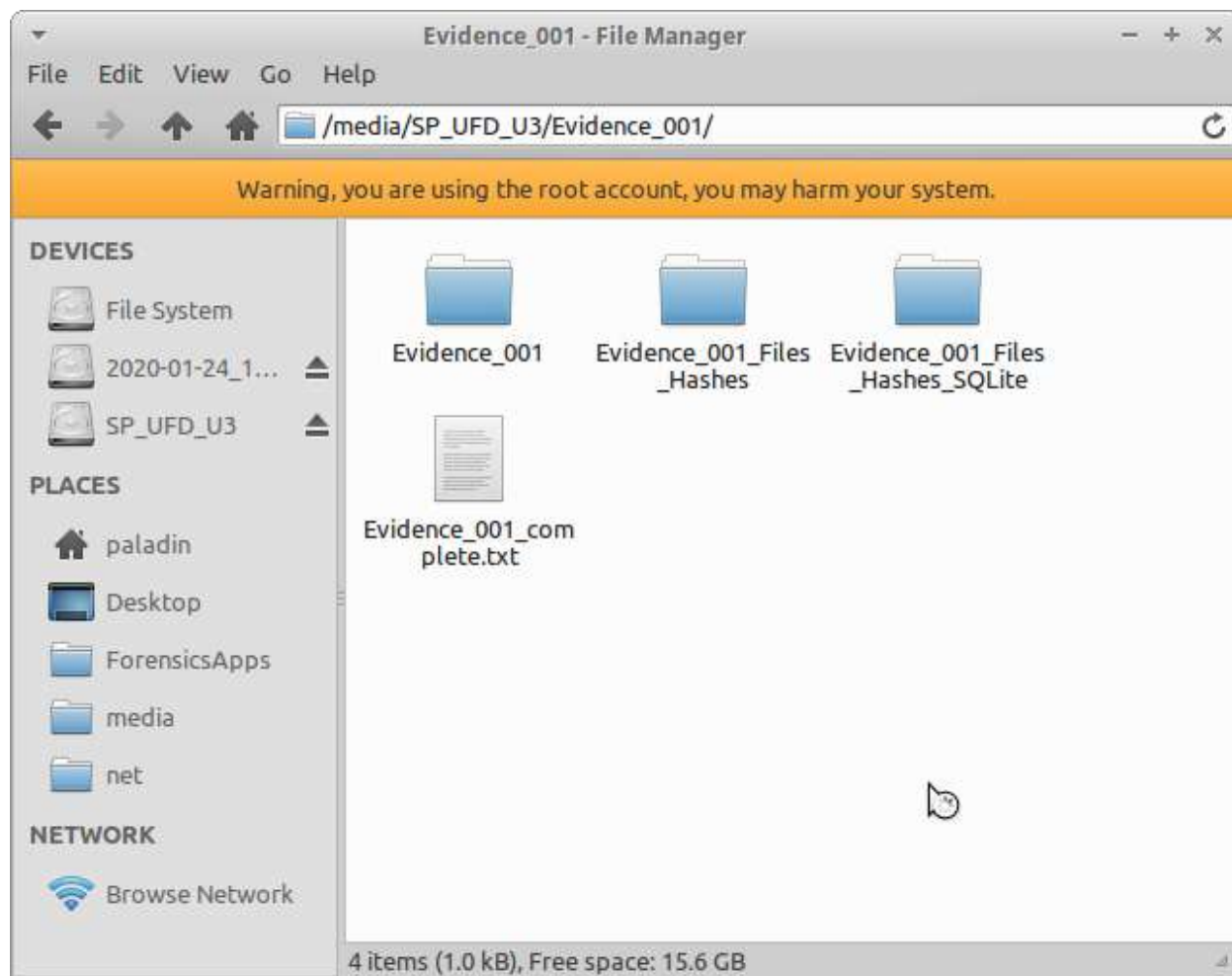
After selecting the BitLocker partition enter the password and click decrypt.



After decryption finishes, select the folders or files to be recovered, the destination drive, label the partition and select whether to hash the source and/or destination.



Navigate to the destination for the decrypted data, hashes and log reports.

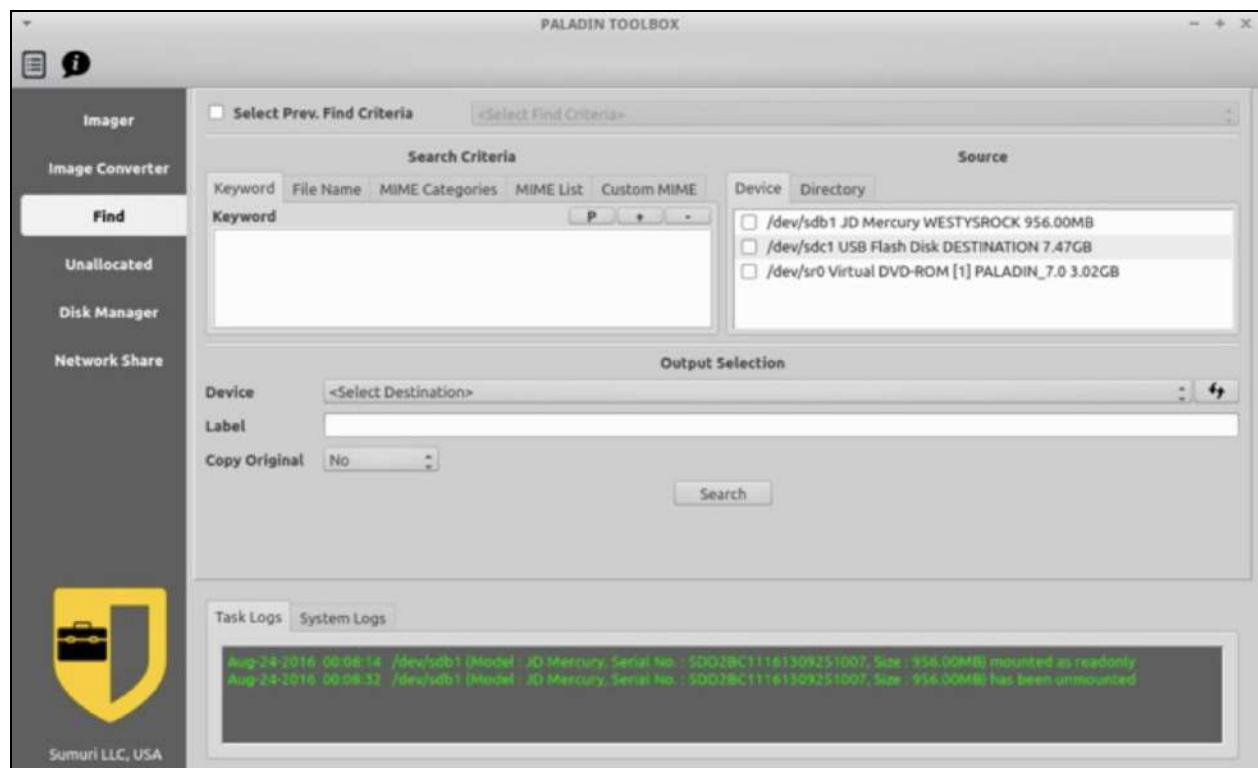


TRIAGE with PALADIN

One of the most important features of PALADIN is its ability to search (or triage) a computer or device for data without making any changes whatsoever. This feature was initially designed to assist law enforcement in their efforts to combat the sexual exploitation of children by providing a tool which can quickly locate files to determine if they are illicit.

PALADIN's triage and search features are found in the “**Find**” tab of the PALADIN Toolbox. Searches from within the Find tab can be based on:

- **Content** - searches the content of files for matches to keywords provided.
- **Name** - searches file names for the keywords provided.
- **MIME Type** - identifies files based on their “signature” and does not rely on extensions or file names.



TRIAGE with PALADIN - Setup

Start PALADIN

Boot a computer to search with PALADIN or attach a device to search with a computer already running PALADIN.

Prepare Your Keyword List

PALADIN Find can load multiple keywords at one time. In order to do this you need to have a text file with one keyword per line. In PALADIN you can open your keyword list and copy the keywords into the clipboard. In the Find configuration window there is a “P” button that can be used to “paste” multiple keywords from the clipboard.

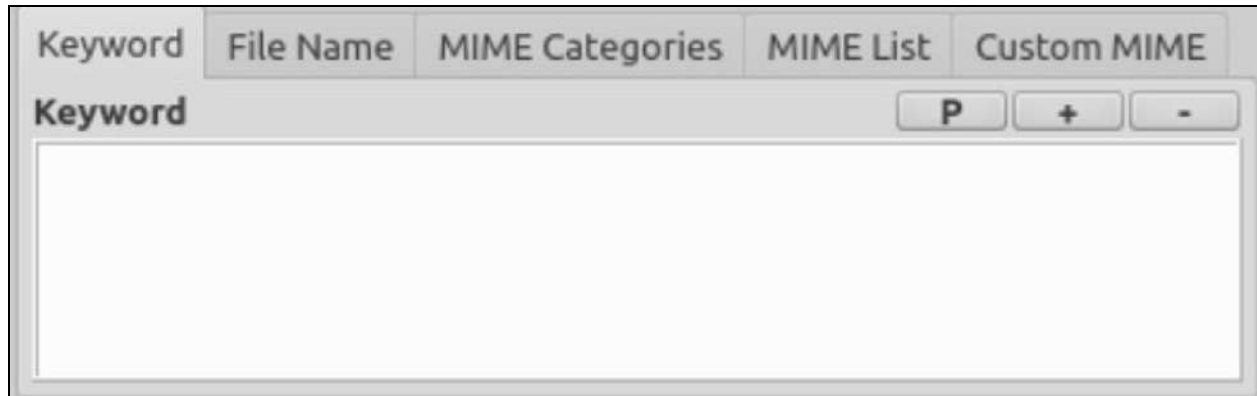
Attach Your Destination Drive

Attach a destination drive to save your search results and to optionally copy out files of interest and mount as read-write. PALADIN will remember your searches which can then be reloaded later. This saves you from having to enter a large amount of search parameters more than once.

“Find” creates symlinks (soft links) on your destination drive during the search process. FAT32 and ExFAT file systems do not support symlinks. Therefore, it is recommended that you should format your destination as HFSPLUS, NTFS or EXT4. FAT32 (VFAT) and ExFAT can be used for the destination drive, however, the files which are located will automatically be copied to your destination drive.

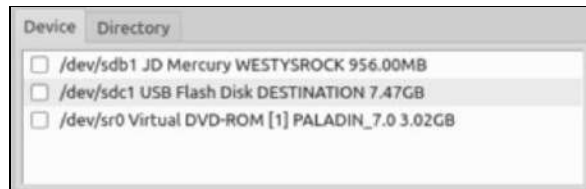
You are now ready to begin your Triage/Search.

TRIAGE with PALADIN - Find Search Window

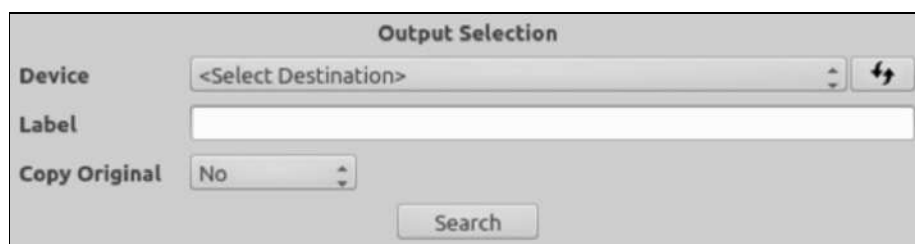


- Select Prev. Find Criteria - this is where you will find previously saved searches if you check the checkbox.
- “P” button - used to paste keywords saved to the clipboard.
- “+” (plus) button - used to add a single keyword.
- “-” (minus) button - used to remove a single keyword.

- Device Tab - Used to search full volumes.
- Directory Tab - Used to select single or multiple directories to search.

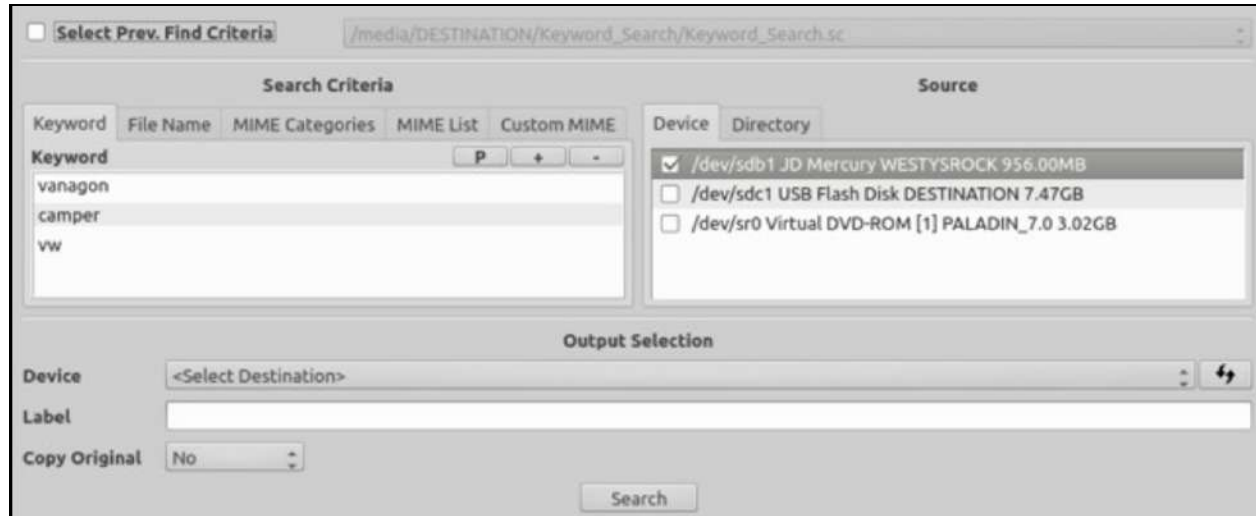


- Device - select your Destination drive to store you search results and search parameters.
- Label - provide a unique name for each search. You will be able to use this to reload the search again.
- Copy Original - files that match your keyword search can be copied to your destination drive.



TRIAGE with PALADIN - Content Search

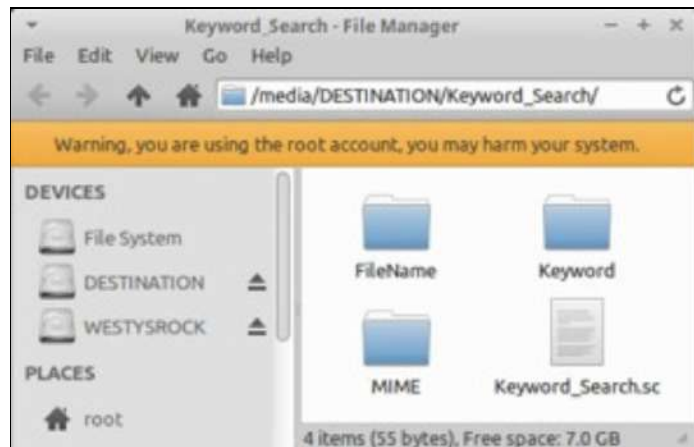
Example of a search for content (keywords found within a file).



- Use the “+” (plus) button in the **Keyword** window to add keywords. To add multiple keywords all at once use the clipboard to copy your single-spaced keyword list into the window with the “P” button. Example above is “vanagon”, “camper” and “vw”.
- **Select the Device** or add directories to search. The volume /dev/sdb1 “WESTYSROCK” is used this example.
- **Provide a “Label”** for you search. “Keyword_Search” is the label for this search.
- **Choose a destination “Device”**. The device /dev/sdc1 “DESTINATION” is used in this example.
- Decide if you want to have PALADIN copy the files that are found to your destination drive. We chose “No” in the “**Copy Original**” dropdown box.
- Click the “**Search**” button to begin your search.

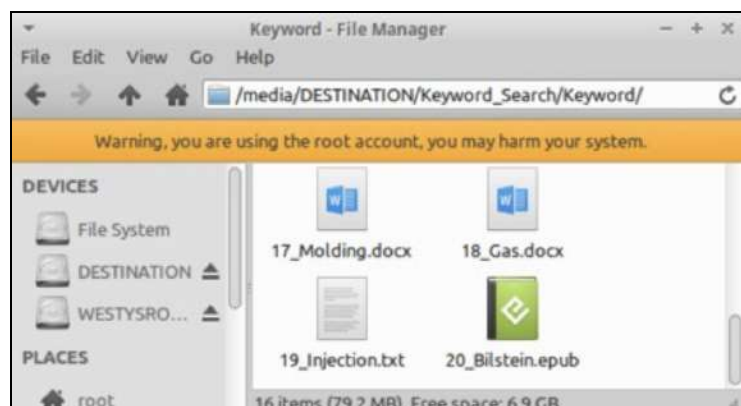
TRIAGE with PALADIN - Content Search

A progress bar will let you know that the search is ongoing and an explorer window will appear with three directories.



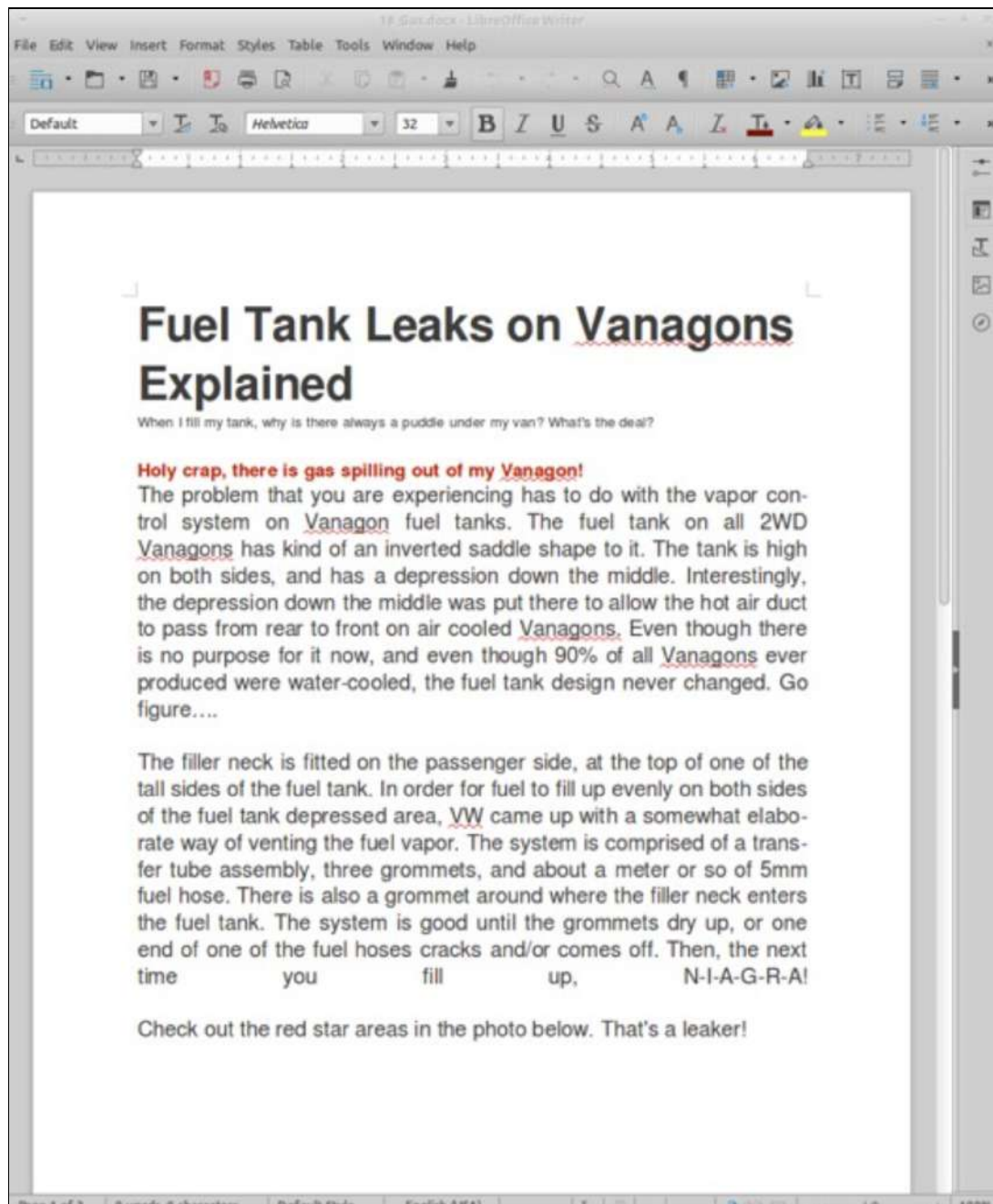
When the Find Result window appears the search will be complete. Here we see **“16 Matches by Keyword”**.

Open the **“Keywords”** directory to see the files found that matched the keywords that were provided.



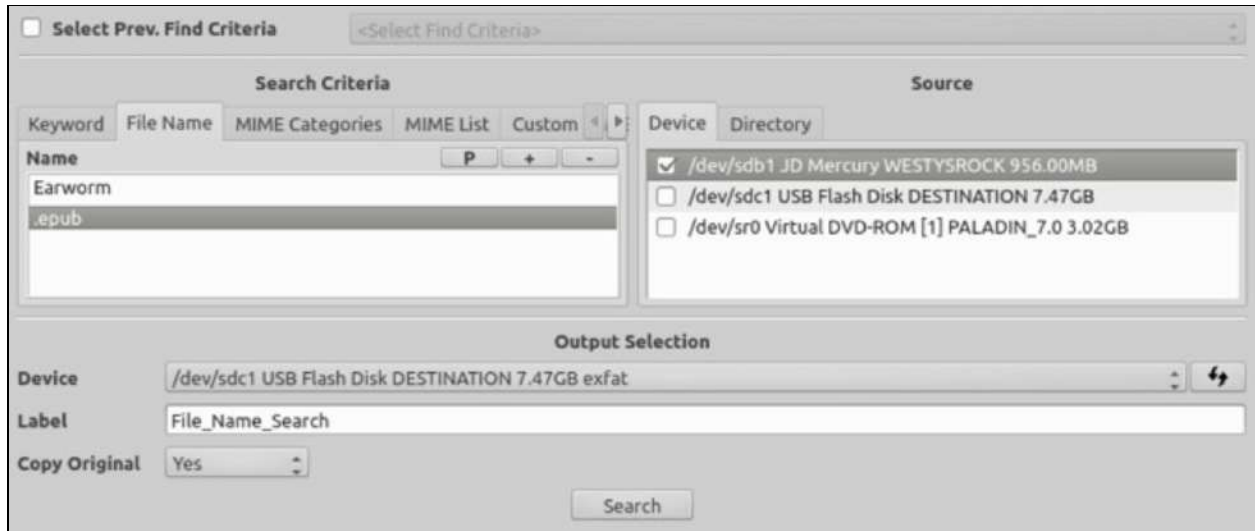
TRIAGE with PALADIN - Content Search

PALADIN includes multiple applications to open and view the files found. As seen below “vanagon” was found inside the document.



TRIAGE with PALADIN - Filename Search

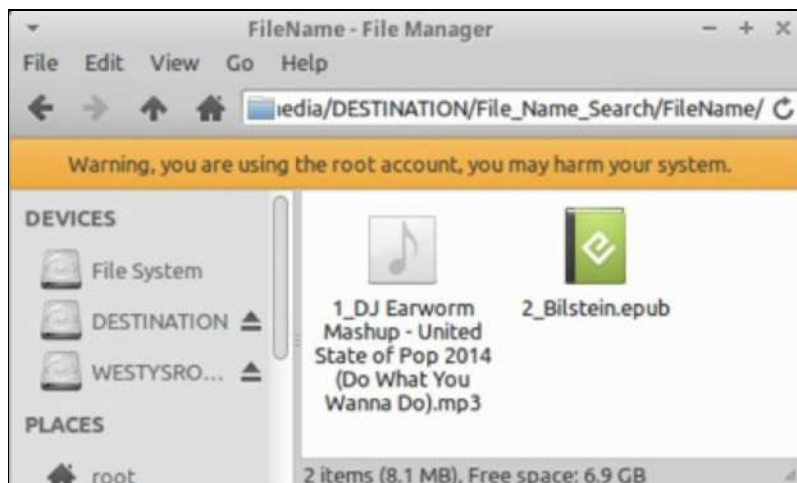
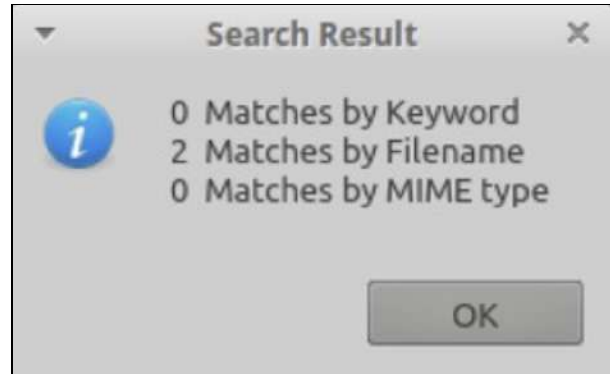
Example of a search for keywords in the name of the file which can include extensions.



- Use the “+” (plus) button in the **Name** window to add keywords. To add multiple keywords all at once use the clipboard to copy your single-spaced keyword list into the window with the “P” button. Example above is “Earworm” and “.epub”.
- **Select the Device** or add directories to search. The volume /dev/sdb1 “WESTYSROCK” is used this example.
- **Provide a “Label”** for you search. “File_Name_Search” is the label for this search.
- **Choose a destination “Device”**. The device /dev/sdc1 “DESTINATION” is used in this example.
- Decide if you want to have PALADIN copy the files that are found to your destination drive. We chose “Yes” in the “**Copy Original**” dropdown box.
- Click the “**Search**” button to begin your search.

TRIAGE with PALADIN - Filename Search

When the Find Result window appears the search will be complete. Here we see “**2 Matches by Filename**”.



Open the “**FileName**” directory to see the files found that matched the keywords that were provided.

TRIAGE with PALADIN - MIME Search

MIME is an acronym for “Multipurpose Internet Mail Extensions”. Its original purpose was to assist in identifying and exchanging various file types via the Internet. The MIME libraries which identify file types have been built into PALADIN Find.

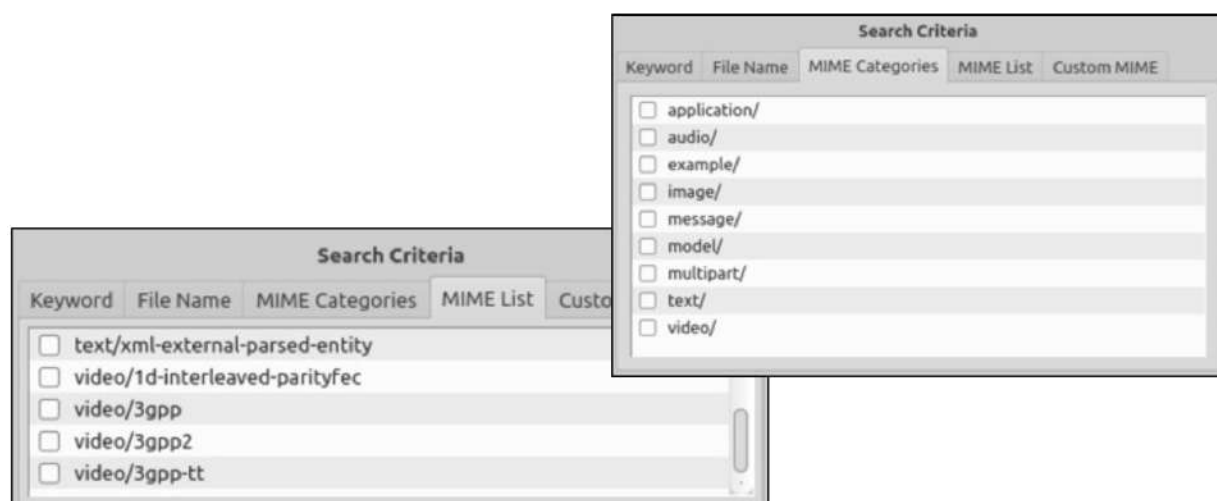
File TYPE/S	MIME Code
JPEG Image	image/jpeg
Portable Document Format	application/pdf
MPEG-4 Video	video/mp4
Find All Images	image/
Find All Videos	video/

Searching by MIME types is similar to searching by signatures in traditional forensic tools.

Several websites can be found which provide a list of MIME types.

We have included hundreds of MIME types into the PALADIN Find Module.

In PALADIN Find you can search by individual MIME signatures, MIME Categories or Custom MIME Types. Using “Categories” you can search every file type within that category. For example, selecting “image” will find every image format known such as JPEG, PNG, BMP and more.



TRIAGE with PALADIN - MIME Search

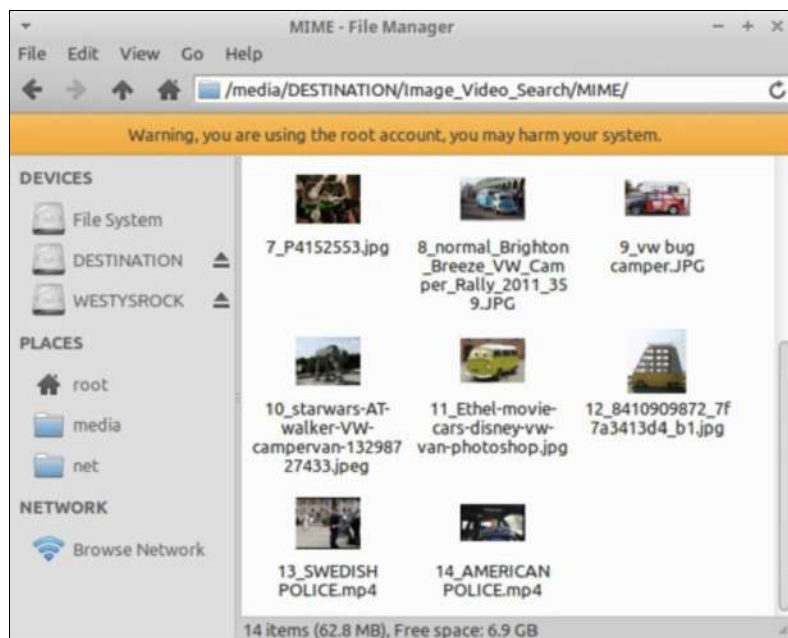
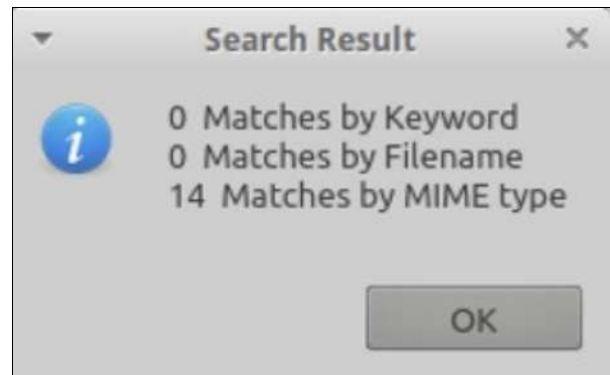
Example of a search based on MIME Categories for all Images and Videos.

The screenshot shows the PALADIN search interface. The 'Search Criteria' tab is active, with 'MIME Categories' selected. Under 'MIME Categories', the 'image/' and 'video/' checkboxes are checked. The 'Source' tab is also active, showing a list of devices: '/dev/sdb1 JD Mercury WESTYSROCK 956.00MB' (checked), '/dev/sdc1 USB Flash Disk DESTINATION 7.47GB' (unchecked), and '/dev/sr0 Virtual DVD-ROM [1] PALADIN_7.0 3.02GB' (unchecked). The 'Output Selection' section at the bottom shows the 'Device' as '/dev/sdc1 USB Flash Disk DESTINATION 7.47GB exfat', the 'Label' as 'Image_Video_Search', and the 'Copy Original' option set to 'Yes'.

- Use the **MIME Categories** tab to select file categories. To search for all videos and images select the “image” and “video” categories.
- **Select the Device** or add directories to search. The volume /dev/sdb1 “WESTYSROCK” is used this example.
- **Provide a “Label”** for you search. “Image_Video_Search” is the label for this search.
- **Choose a destination “Device”**. The device /dev/sdc1 “DESTINATION” is used in this example.
- Decide if you want to have PALADIN copy the files that are found to your destination drive. We chose “Yes” in the “**Copy Original**” dropdown box to copy out the files.
- Click the “**Search**” button to begin your search.

TRIAGE with PALADIN - MIME Search

When the Find Result window appears the search will be complete. Here we see “**14 Matches by MIME type**”.



Open the “**MIME**” directory to see the files found that matched the keywords which were provided.

These files are physical files (not symlinks) since we chose to copy out the files when found.

TRIAGE with PALADIN - Extra Features

In PALADIN Find you can add multiple search terms to any or all of the categories and run them at the same time.

--

In PALADIN Find it is possible to reload previous searches.



Make sure that your destination drive with your previous saved searches is mounted read-write.

Click the box next to "Select Prev. Find Criteria".

Once you have selected your previous search name the keywords will automatically populate.

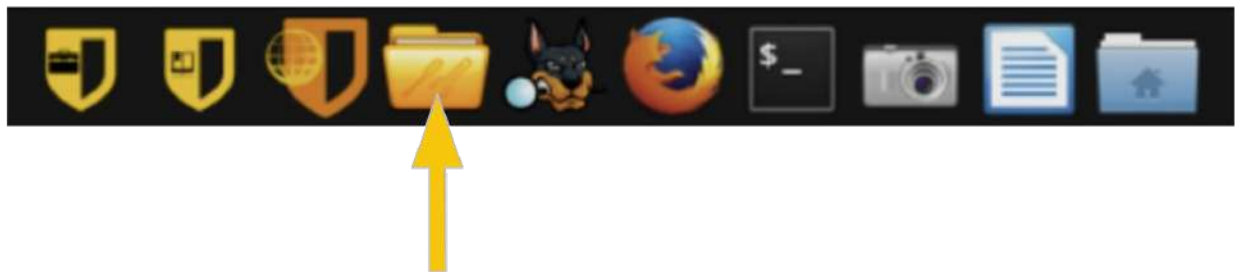
Edit the keywords or begin your search.

PALADIN - Forensic Apps

PALADIN contains over 100+ pre-compiled applications to assist with your forensic tasks divided into 33 different categories. PALADIN is truly an all-in-one forensic suite!



The Forensic Apps Directory can be accessed via the Dock at the bottom of the desktop. Simply click the folder icon.



PALADIN - Forensic Apps - Autopsy

With the introduction of PALADIN Version 6 we have added **Autopsy** courtesy of BASIS Technology and Brian Carrier. Autopsy is a powerful GUI based full forensic suite which has features that rival many of the top commercial forensic suites found on the market today without the cost or annual renewal fees.

As described on Basis Technology's website:

"Autopsy® is the premier open source digital forensics platform that has thousands of users worldwide. It has been developed by Basis Technology and an open source community."

Autopsy has the core analysis features that are needed by law enforcement and corporate investigators to conduct an investigation of a hard drive or mobile device."

Images made with PALADIN can immediately be processed with Autopsy making PALADIN a complete full forensic suite!

To start Autopsy in PALADIN click the Autopsy (dog) icon in the PALADIN dock.

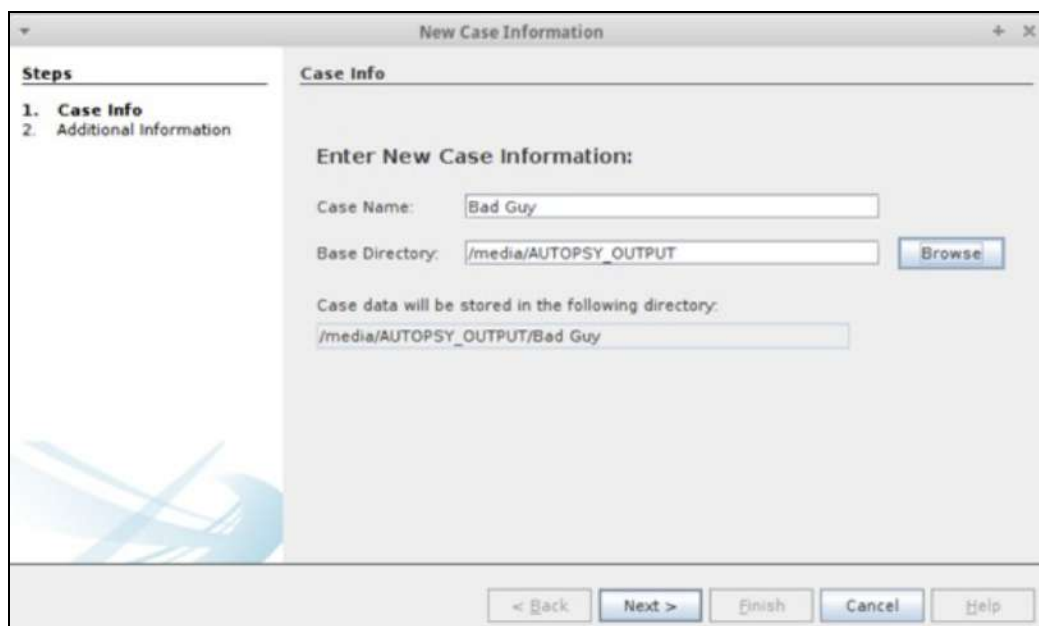


PALADIN - Forensic Apps - Autopsy

After imaging with PALADIN start Autopsy and select “**Create New Case**”.

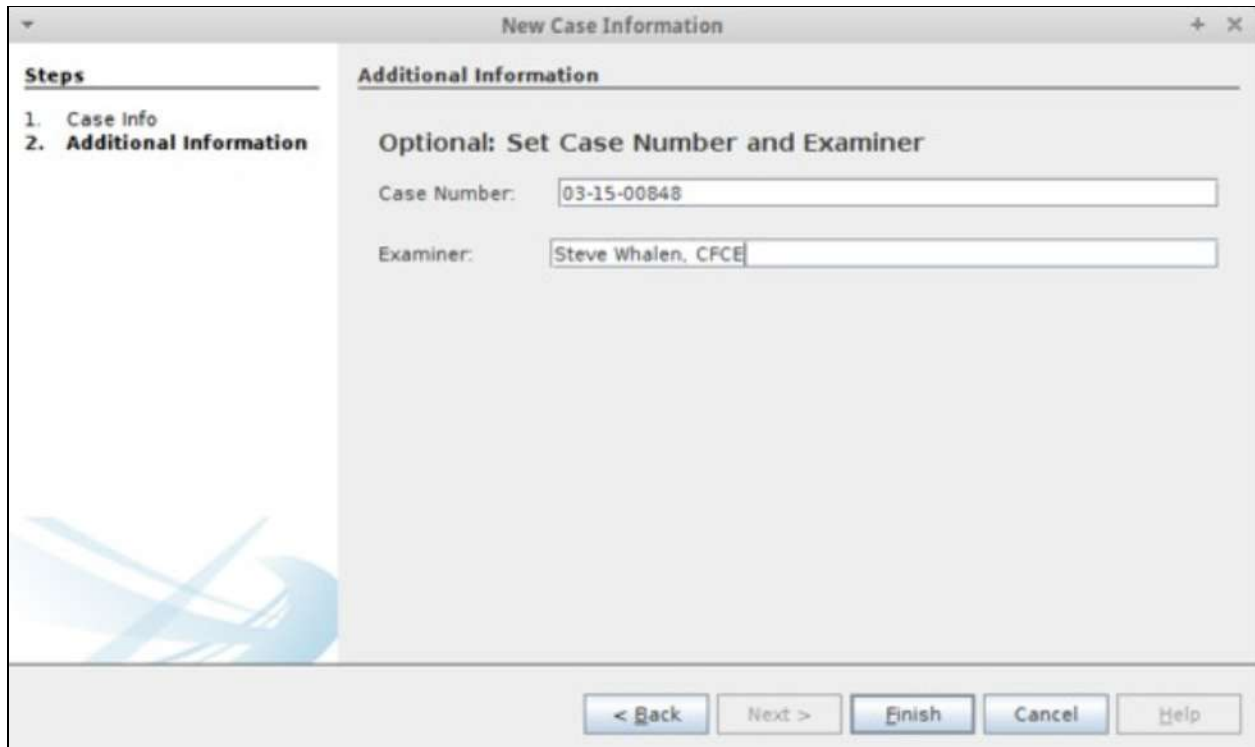


Enter a “Case Name” select your “**Base Directory**” (drive mounted read-write) for output.



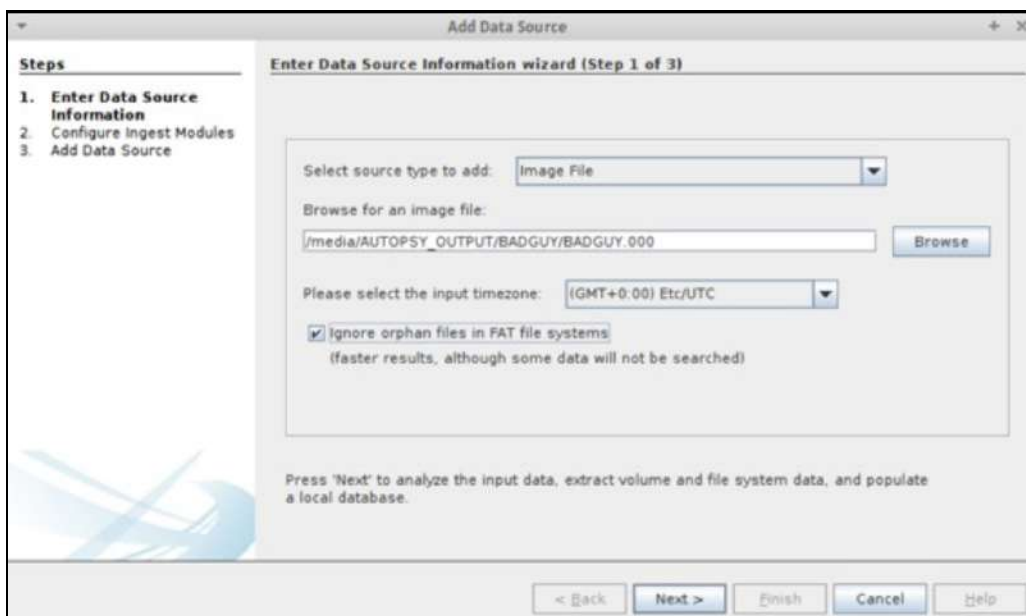
PALADIN and Autopsy - Starting a Case

Add a “Case Number” and “Examiner” name.



The screenshot shows the 'New Case Information' dialog box. On the left, a 'Steps' pane lists '1. Case Info' and '2. Additional Information'. The main area is titled 'Additional Information' and contains the heading 'Optional: Set Case Number and Examiner'. Below this, there are two text input fields: 'Case Number:' with the value '03-15-00848' and 'Examiner:' with the value 'Steve Whalen, CFCE'. At the bottom of the dialog are five buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

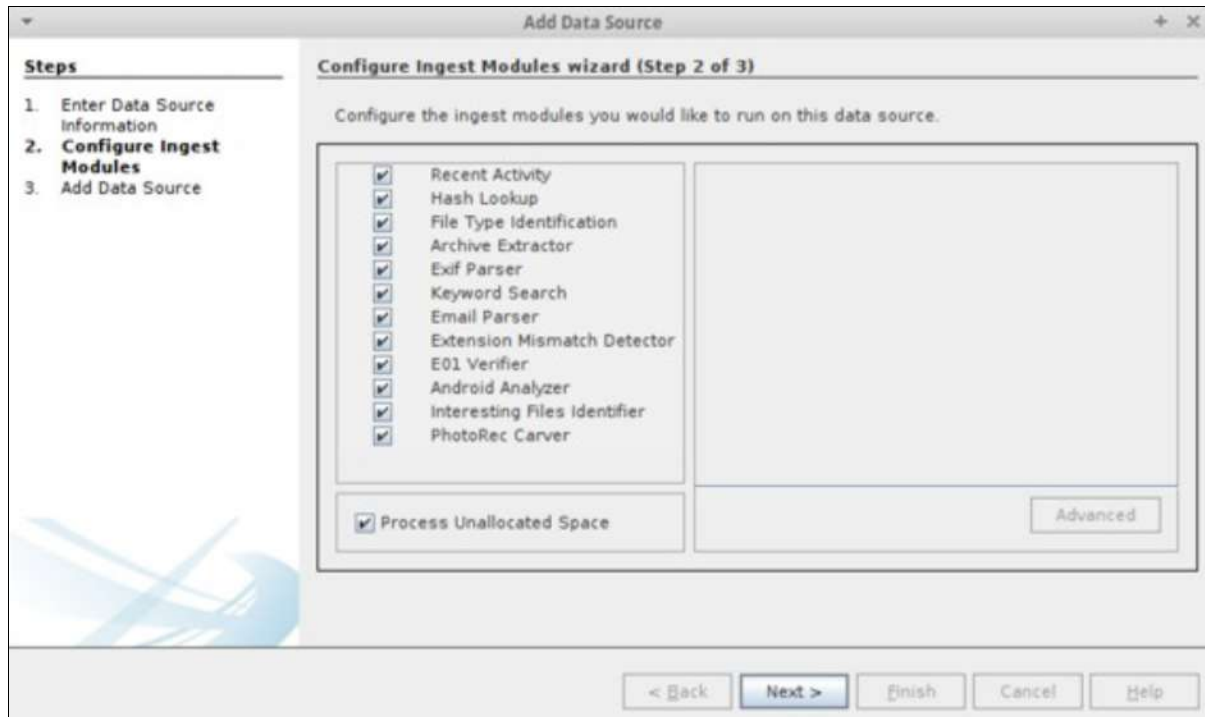
Select “Image File” for your source and navigate to the forensic image file.



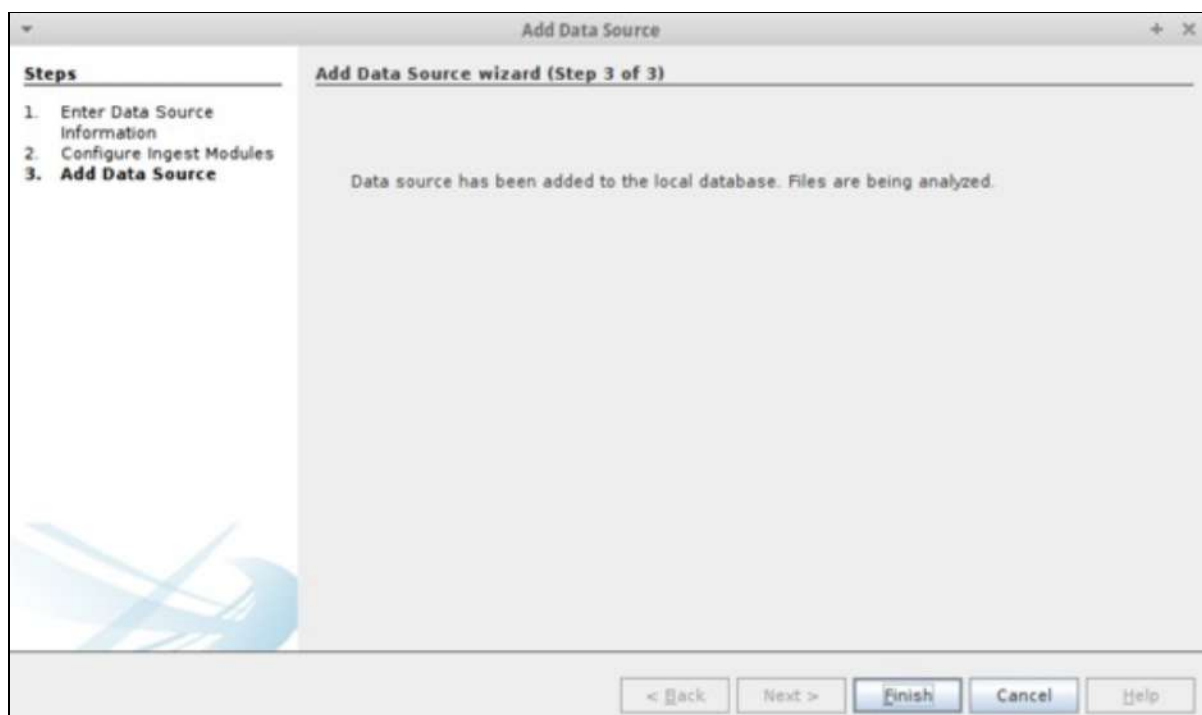
The screenshot shows the 'Add Data Source' dialog box, titled 'Enter Data Source Information wizard (Step 1 of 3)'. On the left, a 'Steps' pane lists '1. Enter Data Source Information', '2. Configure Ingest Modules', and '3. Add Data Source'. The main area contains a 'Select source type to add:' dropdown menu with 'Image File' selected. Below this is a 'Browse for an image file:' section with a text input field containing '/media/AUTOPSY_OUTPUT/BADGUY/BADGUY.000' and a 'Browse' button. Further down is a 'Please select the input timezone:' dropdown menu with '(GMT+0:00) Etc/UTC' selected. A checkbox labeled 'Ignore orphan files in FAT file systems' is checked, with a note '(faster results, although some data will not be searched)' below it. At the bottom, there is a text instruction: 'Press "Next" to analyze the input data, extract volume and file system data, and populate a local database.' At the very bottom are five buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

PALADIN and Autopsy - Starting a Case

Select and configure your “Ingest Modules”.



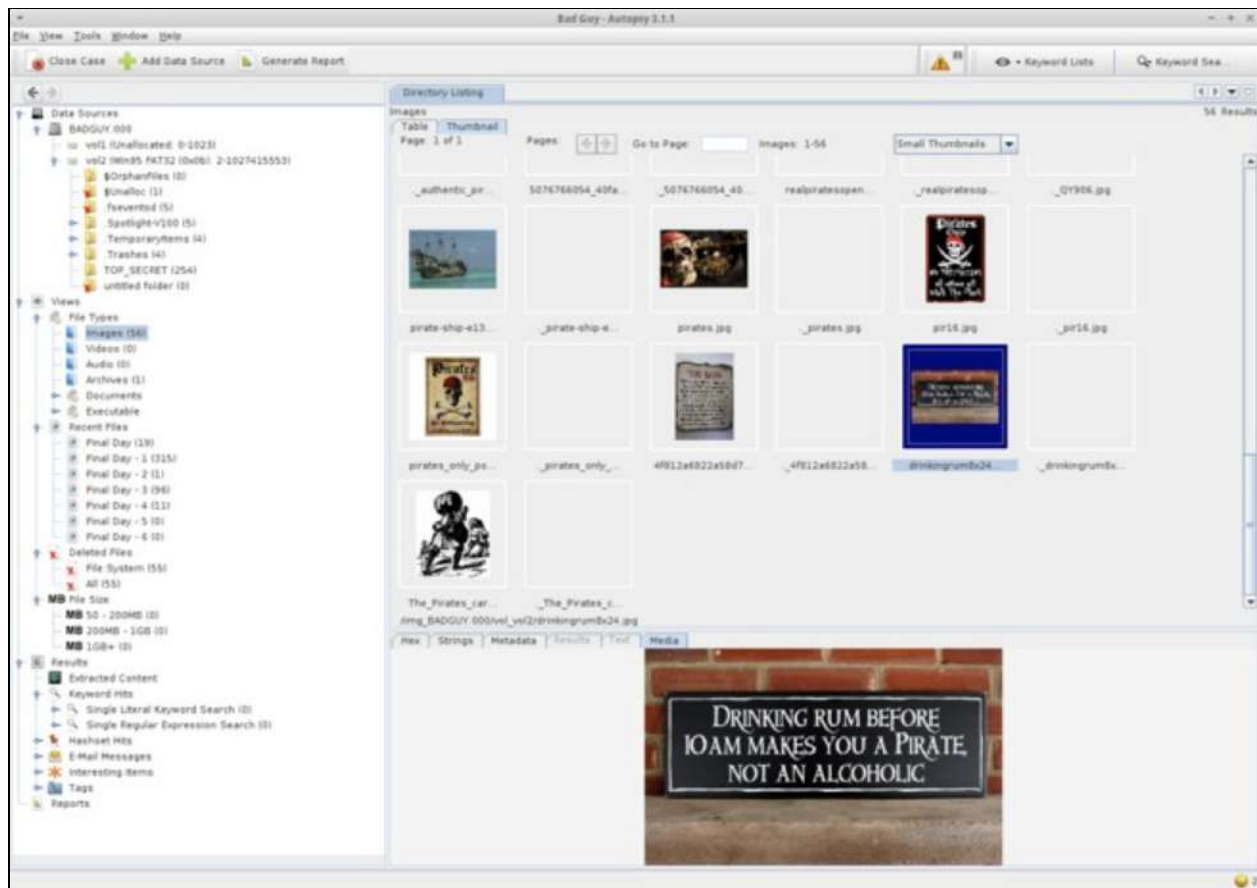
Click “Finish” to begin the processing.



PALADIN and Autopsy - Starting a Case

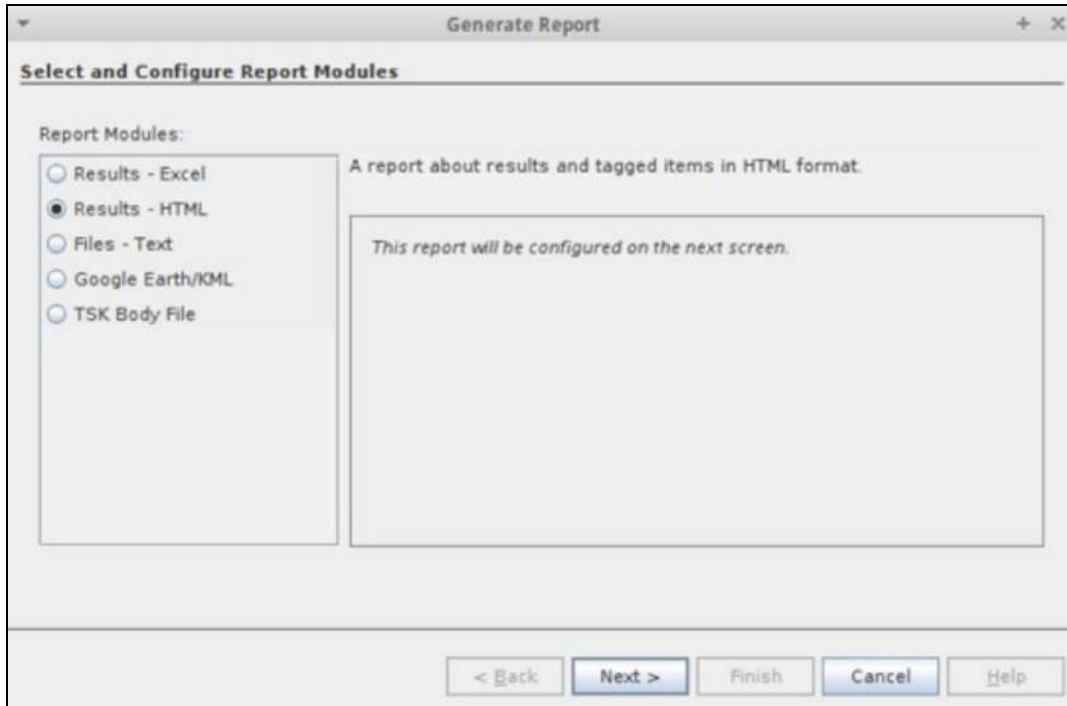
Autopsy provides an easy to use and intuitive interface that makes processing and finding data easy!

For official training on Autopsy please contact Basis Technology (www.basistech.com).

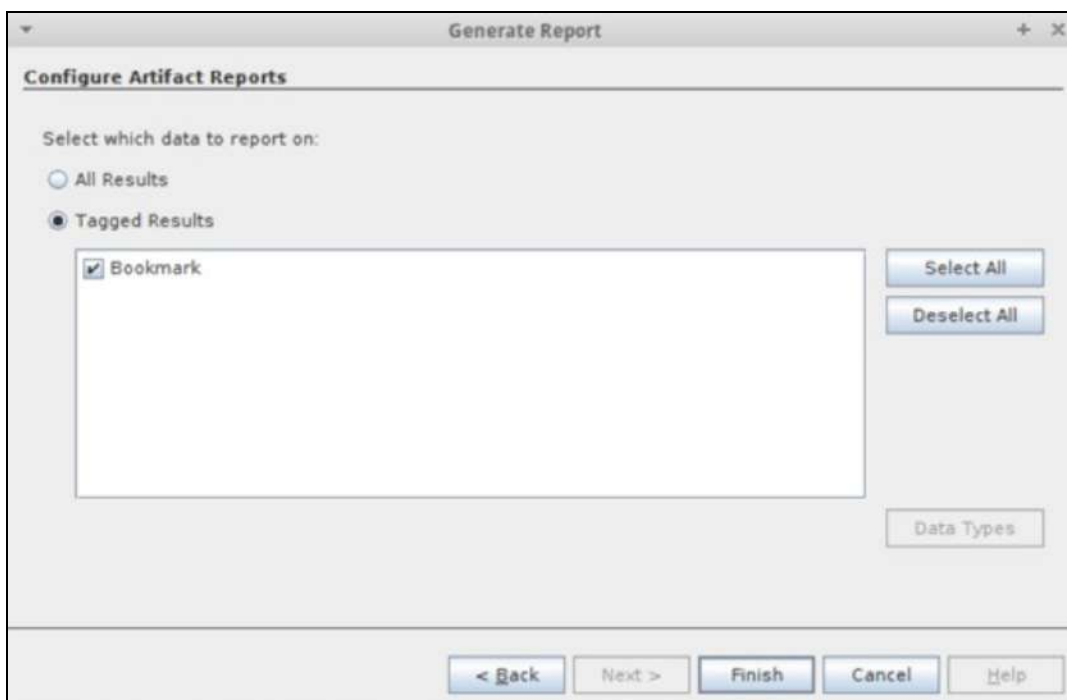


PALADIN and Autopsy - Reporting

After tagging and bookmarking data click the “Generate Report” button and select your report type.

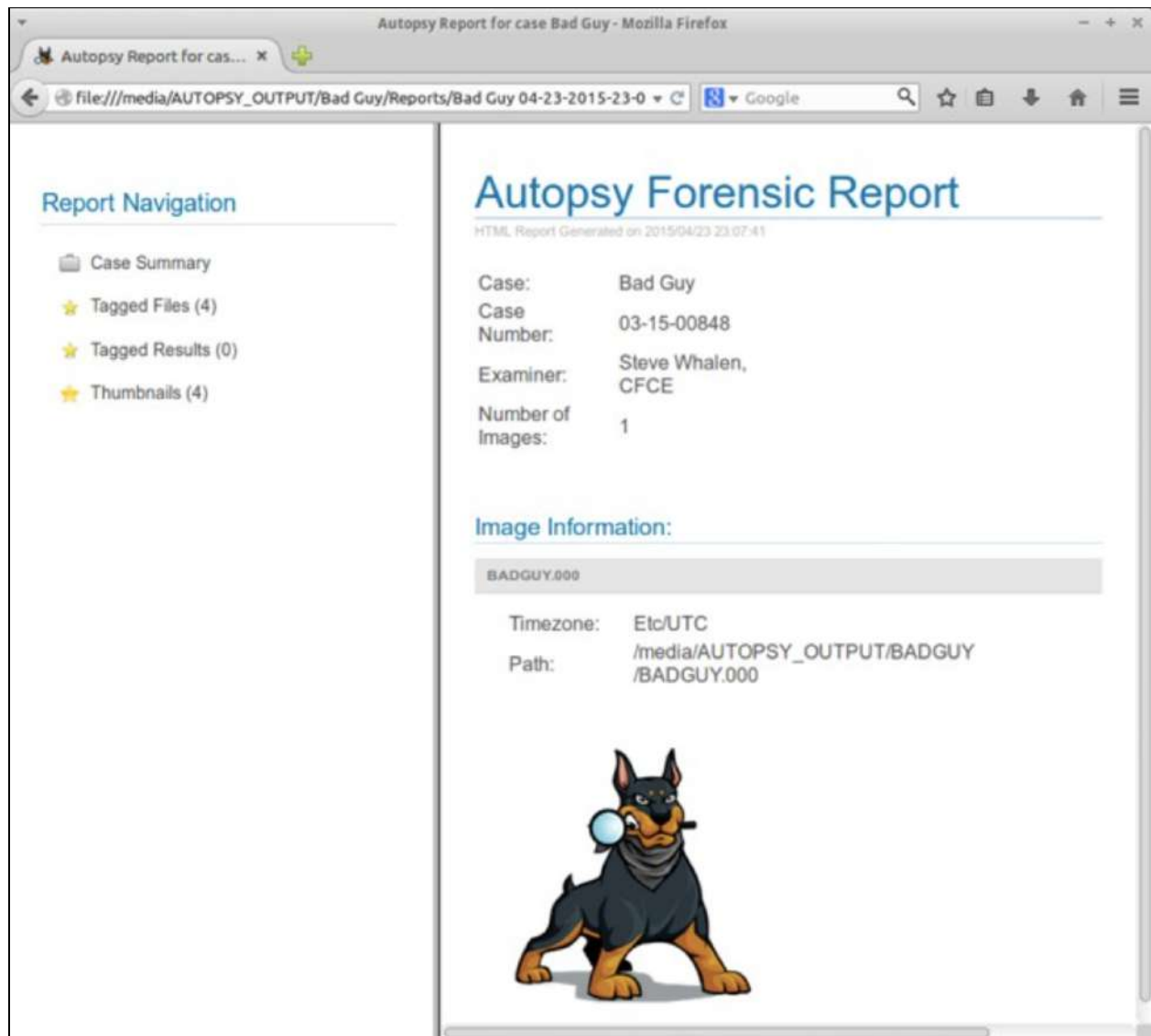


Select your artifacts to include in the report and click “Finish”.



PALADIN and Autopsy - Reporting

Your report is now ready!



For more information and to find additional Autopsy modules please visit Basis Technology's website here:

<http://www.basistech.com/digital-forensics/autopsy/modules/>