
# Quick Start Guide

SUMURI.COM

# Dedication and Credits

*This manual is dedicated to those who have tirelessly devoted their time, sacrificed moments with their loved ones, and risked their lives to protect our communities and make the world a safer place. Your dedication and service are deeply appreciated.*

**CREDITS**

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

A heartfelt thank you to the forensic community and all those who continue to make PALADIN possible. Your work has helped fight terrorism, bring criminals to justice, and protect children from exploitation across the globe.

Steve Whalen
SUMURI LLC - Co-Founder



SUMURI LLC
P.O. Box 121
Magnolia, Delaware 19962
USA
www.sumuri.com

# Quick Start Guide

SUMURI®

# 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 ensure 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 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: The Ultimate Forensic Swiss Army Knife

**PALADIN Toolbox** is one of the most **trusted and widely used** digital forensic tools available today—an essential companion for investigators worldwide.

Now, with the **latest version of Autopsy** integrated into PALADIN, forensic examiners have even more power at their fingertips. Autopsy, a full-featured forensic suite with an intuitive **graphical user interface (GUI)**, allows you to conduct **in-depth file system analysis, keyword searching, timeline examination, and more—all while maintaining forensic integrity** (no changes are ever made to the original evidence). Combined with PALADIN's bootable environment, this makes it easier than ever to **safely examine computers in the field or in the lab**.

## New: Persistent Storage for Investigations

PALADIN LTS now includes a **persistent partition**, allowing you to **store case files, keyword lists, and hash sets directly on your bootable drive**. This means you can save your Autopsy investigations, forensic notes, and custom configurations—bringing even more efficiency and convenience to your workflow.

## New: Enhanced Compatibility with Modern NVIDIA GPUs

The latest release of **PALADIN** now includes updated NVIDIA drivers, expanding compatibility with newer graphics hardware—including the 50-series NVIDIA GPUs. This upgrade ensures smoother operation on modern systems and allows forensic examiners to take full advantage of accelerated performance where available. By integrating the latest drivers, **PALADIN** is better equipped to run efficiently on a wider range of current-generation machines, making it even more adaptable to today's investigative environments.

## A Comprehensive Collection of Open-Source Forensic Tools

PALADIN includes a wide range of **open-source forensic applications** to assist with every stage of an investigation. These tools span multiple forensic disciplines, including:

- **Computer Forensics** – File system analysis, disk imaging, and evidence preservation.
- **Memory Forensics** – Extraction and analysis of volatile memory.
- **Network Analysis** – Capturing and examining network traffic and wireless activity.
- **Password Recovery & Cryptography** – Password cracking, encryption analysis, and decryption tools.
- **Metadata & Timeline Analysis** – Extraction of file metadata and forensic timeline reconstruction.
- **Mobile & Vehicle Forensics** – Investigation of mobile devices and automotive data.

- **Open-Source Intelligence (OSINT)** – Digital footprint analysis and intelligence gathering.
- **Email & Log Analysis** – Examination of email archives, system logs, and event records.
- **Forensic Imaging** – Acquisition and verification of digital evidence.
- **Steganography & Data Obfuscation** – Detection and analysis of hidden or altered data.

And much more! PALADIN's extensive toolkit ensures that forensic examiners have access to **powerful, field-tested tools**—all in a **bootable, forensically sound environment**.

## Now Available as a Dual-Boot Option on TALINO Forensic Workstations

For the **ultimate forensic workstation experience**, **PALADIN is now included as a dual-boot option on all TALINO Forensic Workstations**—exclusively from SUMURI. This means all of PALADIN's powerful features, open-source forensic tools, and time-saving automation are **pre-installed and ready to go right out of the box**.

With PALADIN built directly into TALINO, forensic professionals **save thousands on forensic software and tools** while also eliminating the hassle of manual setup. From advanced forensic imaging to in-depth analysis, PALADIN on TALINO ensures **you have everything you need in one powerhouse forensic workstation**.

## A Forensic Suite You Can Trust

Whether you're conducting **on-site investigations, analyzing digital evidence, or preserving forensic integrity**, PALADIN gives you the flexibility and power you need—all in a **bootable, easy-to-use package**.

And now, with **TALINO + PALADIN**, you get a **seamless, cost-effective, and fully integrated forensic solution—available only on TALINO Forensic Workstations**.

If you're interested in a **dual-boot TALINO Forensic Workstation from SUMURI**, reach out to us at **hello@sumuri.com** to learn more!

# 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 .dmg. |
| Ability to clone devices. |
| Ability to convert from one forensic image format to another. |
| 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). |
| A vast collection of pre-compiled open-source forensic tools and applications across multiple categories. |
| Bitlocker support for Windows 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** for digital forensics, eDiscovery, and the investigation of digital evidence worldwide.

Founded in **2010 by Steve and Ailyn Whalen**, SUMURI LLC is headquartered in **Delaware, USA**. Our mission is to deliver innovative and cost-effective forensic solutions while upholding the highest standards of integrity and service.

## About Our Founder

**Steve Whalen** has been a pioneer in the field of **computer forensics** since 1997. He has trained thousands of investigators and forensic examiners worldwide—both individually and through esteemed organizations such as the **International Association of Computer Investigative Specialists (IACIS)**, where he is a **Lifetime Member**, the **High Technology Cyber Investigation Association (HTCIA)**, and the **U.S. Department of State Anti-Terrorism Assistance Program**.

Steve is also the creator of several groundbreaking forensic solutions, including:

- **PALADIN** (formerly Raptor) – A powerful bootable forensic Linux distribution.
- **RECON ITR & RECON LAB** – Advanced macOS forensic tools designed for seamless acquisition and analysis.
- **Certified Forensic Mac Examiner (CFME)** – The **only vendor-neutral Mac forensic training and certification**, ensuring forensic professionals are equipped with unbiased, industry-standard expertise.
- **Macintosh Forensic Survival Course (MFSC)** – A widely recognized training program for Mac forensic investigations.
- **TALINO Forensic Workstations** – High-performance forensic systems that meet the needs of modern forensic examiners.

His expertise has taken him across **North America, Central America, Asia, Europe, the Middle East, the Caribbean, Africa, and Oceania**, where he has provided training to law enforcement agencies, government institutions, and forensic professionals.

## Law Enforcement Background

Prior to founding SUMURI, Steve served **over 15 years as a Delaware State Trooper**, where he worked as a detective in the **Criminal Investigations Unit** and became the agency's first **full-time forensic examiner for digital evidence**. In 2001, he played a key role in developing the **Delaware State Police High Technology Crimes Unit**, processing thousands of digital evidence items from cases involving **cyber intrusions, financial crimes, child exploitation, narcotics, stalking, and homicides**.

## Our Core Values

SUMURI was built on the same core principles that guided Steve throughout his law enforcement career:

- **Honor**
- **Integrity**
- **Courage**
- **Loyalty**
- **Attitude**
- **Discipline**
- **Service**

These values define every aspect of our work, from the **cutting-edge forensic solutions we develop** to the **trusted relationships we build with our clients**. At SUMURI, we don't just provide tools—we offer **customized solutions tailored to your needs, backed by a team that treats every client like family**.

Our team is made up of **leading experts in digital evidence, computer forensics, and eDiscovery**, with **real-world experience** in **law enforcement, military, and corporate investigations**. As **active practitioners**, we bring firsthand knowledge and expertise to every case, tool, and training we provide.

We have trained **thousands of forensic examiners and investigators** from **Fortune 500 companies, local and federal law enforcement agencies, and government organizations worldwide**—ensuring they have the skills and tools needed to uncover the truth.

At SUMURI, we are committed to delivering **unparalleled forensic solutions and services across the globe**.

We look forward to assisting you and hope you enjoy using **PALADIN!**

# Differences Between PALADIN Versions
## (PALADIN LTS vs. PALADIN 32)

There are **two versions** of PALADIN available:

- **PALADIN LTS (64-Bit Architecture)** – Based on the most current **LTS (Long-Term Support) version of Ubuntu** for maximum stability. In addition to the **PALADIN Toolbox**, it includes a collection of **pre-compiled open-source forensic tools and applications**.
- **PALADIN 32 (32-Bit Architecture)** – A lightweight version of PALADIN that **only includes the PALADIN Toolbox** without additional forensic tools. This makes it **smaller, faster to boot**, and ideal for older hardware with **32-bit architecture**.

### Available Boot Modes

Both PALADIN LTS and PALADIN 32 offer **two boot modes**, selectable from the splash screen:

- **Live Session - Forensic Mode**
- **Live Session - Non-Forensic Mode**

**Forensic Mode (Forensically Sound)**

- **Networking is disabled** for forensic integrity.
- **PALADIN does not mount** internal drives, external media, or swap files.
- Once booted, device mounting is controlled by the **PALADIN Toolbox**.
- Designed for **forensic investigations** where maintaining data integrity is critical.

**Non-Forensic Mode (Not Forensically Sound)**

- **Networking enabled** for standard system use.
- **Automatically mounts** internal drives, attached media, and swap files.
- Ideal for general system access **without forensic restrictions**.

# How Can I Get PALADIN?

The PALADIN ISO (used to create a PALADIN USB) is provided as a courtesy to the forensic community by SUMURI and is available as donationware for non-commercial use.

🚨 **Important: Commercial Use Policy**

For commercial use, a minimum donation of $25.00 USD per user per version is required. When a new version of PALADIN is released, we ask that you donate again to continue using the latest version.

**Using PALADIN commercially without the required donation is a violation of our End User License Agreement (EULA) and U.S. copyright law.**

## Why Does This Matter?

Unauthorized commercial use of PALADIN may constitute software piracy, copyright infringement, or breach of contract under U.S. law.

We appreciate the forensic community's support in keeping PALADIN available and evolving. If you use PALADIN commercially, please donate to help sustain development.

**PALADIN Pro – Pre-Compiled & Ready to Use**

For a ready-to-go solution, you can purchase PALADIN Pro, a pre-compiled USB that includes both PALADIN LTS and PALADIN 32, directly from SUMURI:
🔗 Get PALADIN Pro

**Download PALADIN**

Need PALADIN right away? You can download it instantly from our website:
🔗 Download PALADIN

**Support the PALADIN Project**

If you find value in PALADIN, please consider making a donation to help keep the project alive. Every contribution is greatly appreciated!

🔹 If you donate and download the ISO from our website, you will need to create your own PALADIN USB.

## How Can I Download the PALADIN ISO?

Follow these steps to download the PALADIN ISO from SUMURI:

1. Visit [www.sumuri.com](http://www.sumuri.com).
2. Sign in to your account via the **"My Account"** menu. If you do not have an account, you must register for a **free account**.
3. Navigate to the **PALADIN page** via the **"Products"** menu.
4. **Select the version of PALADIN you wish to download.**
5. **Choose your usage type:**
    - **Commercial Use** (Requires a minimum donation of **$25.00 per user per version**)
    - **Non-Commercial Use** (Donation appreciated)
6. **Enter your donation amount** and select **"Add to Cart."**
7. Review your **Cart** and select **"Proceed to Checkout."**
8. Provide the requested information and select **"Place Order."**

## 📌 Important Information – Please Read Carefully

🔹 **You must complete this process to obtain any PALADIN ISO, even if the entered amount is zero.**
🔹 **Providing false or anonymous information may result in your request being discarded** and could prevent you from downloading PALADIN.
🔹 **If you select Commercial Use, a minimum donation of $25.00 USD per user per version is required.** When a **new version of PALADIN is released**, you must **donate again** to continue using the latest version.
🔹 **Using PALADIN commercially without the required donation is a violation of our End User License Agreement (EULA) and U.S. copyright law.**

Thank you for supporting the continued development of PALADIN!

**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 dual-boot, professional-grade solution that includes the latest versions of PALADIN—trusted by forensic examiners worldwide:

- **PALADIN LTS (64-bit**) – A long-term support version packed with stable, pre-compiled open-source forensic tools.
- **PALADIN 32 (32-bit)** – A lightweight build of the PALADIN Toolbox, specifically optimized for legacy 32-bit systems.

### Key Advantages of PALADIN PRO:

- **Two versions, one device** – No need for multiple USBs. Run either 32-bit or 64-bit PALADIN environments from a single drive.
- **Extra storage partition** – Conveniently store case files, hash sets, keyword lists, logs, and other critical resources directly on the USB.
- **Universal system support** – Seamlessly operates across both modern UEFI and older BIOS-based systems.
- **Optimized for speed** – Fast boot times ensure you get to work quickly, even under tight deadlines.
- **High-quality USB** – Durable, reliable, and built for frequent field use.
- **Supports the PALADIN Projec**t – Your purchase helps keep this powerful forensic tool freely available to the digital forensics community.

---

# Introducing the New PALADIN PRO USB

**A Smarter, More Powerful Forensic Toolkit**

With the release of PALADIN 9.0.0, the PALADIN PRO USB marks a leap forward in how forensic examiners deploy and manage their tools. Designed with modern forensic workflows in mind, PALADIN PRO eliminates manual configuration and streamlines updates.

### Multi-ISO Boot Capability

Run multiple forensic environments—such as WinFE, Kali, SIFT Workstation, or any other custom ISO—from a single USB. Your entire toolkit, ready whenever and wherever you need it.

### Effortless Drag-and-Drop Updates

When a new version of PALADIN is released, simply drag and drop the ISO file onto the USB—no reformatting, no reconfiguration. It's the easiest way to stay current.

### Persistent Storage & Customization

Save logs, settings, and evidence securely with built-in persistent storage. Your tools and data remain intact between sessions, so you're always ready to resume your work.

### Broad File System Compatibility

Full support for FAT32, exFAT, and NTFS file systems allows you to use the drive across a variety of platforms and storage sizes without limitations.

### Integrated Forensic Utilities

Go beyond PALADIN. Use your PALADIN PRO USB to host additional forensic and recovery tools such as Clonezilla, SystemRescueCD, or your custom utilities—all from one device.

---

## Why PALADIN PRO USB Stands Out

In the fast-paced world of digital forensics, having a reliable, flexible, and up-to-date toolkit is critical. The **PALADIN PRO USB** is engineered to meet those demands:

- One USB, multiple environments
- Easy updates with zero downtime
- Built-in storage for critical case data
- Compatible with virtually any hardware
- High-quality USB for daily field use
- Directly supports ongoing PALADIN development

## Order Your PALADIN PRO USB Today

The PALADIN PRO USB is available for $99.99 USD and can be ordered directly from SUMURI.

# 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/how-to-make-your-own-PALADIN-usb/

# Troubleshooting PALADIN

There are two options for obtaining support with PALADIN:
- Ubuntu Forums and Community Support
- SUMURI Single Support Session

**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 on 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 when 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 $75 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 (With or Without Secure Boot)

PALADIN is designed to work on a wide range of PC hardware—both modern and legacy. To safely boot PALADIN on a standard PC (non-Mac), you may need to adjust the system's firmware settings depending on whether **Secure Boot** is enabled and if **BitLocker** protection is active.

---

## 🔑 Key Preparation Steps

Before booting PALADIN, be sure you're familiar with:

- ✅ Disabling Secure Boot (if necessary)
- ✅ Selecting boot options in BIOS/UEFI (Option 1)
- ✅ Using the Boot Manager (Option 2)
- ✅ Backing up the BitLocker Recovery Key (if applicable)

---

## 🔐 Secure Boot and BitLocker: What You Need to Know

**Secure Boot** is a UEFI firmware feature that blocks unsigned or untrusted software from loading during startup.
**BitLocker** is Microsoft's full-disk encryption. If boot behavior changes (such as inserting an external USB), BitLocker may trigger recovery mode.

> Most modern PCs ship with both features enabled by default.

---

## ⚠️ Common Issues

On systems with Secure Boot or BitLocker, you may encounter:

- ❌ **PALADIN fails to boot**, displaying a Secure Boot violation or security error.
- 🔒 **BitLocker Recovery Mode**, requiring the recovery key to access the encrypted drive.

---

### ✅ Recommended Pre-Boot Steps

1. **Back Up the BitLocker Recovery Key**
   The key may be stored in:
   - The user's **Microsoft account**
   - **Active Directory** (on domain-joined systems)
   - A **USB key**, printed copy, or exported file
2. **Test PALADIN on a Non-Critical System**
   Before using PALADIN on a system containing evidence, test it on similar hardware to confirm how Secure Boot and BitLocker behave.

---

## 🚀 Booting PALADIN: Step-by-Step

1. **Insert the PALADIN USB drive**
   Use any standard USB 3.0 or 2.0 port.
2. **Reboot the system**
   Immediately press the appropriate key to access the boot menu or BIOS/UEFI setup (typically `ESC`, `F1`, `F2`, `F10`, `DEL`, or `F12`).

---

### 🧭 Boot Scenarios Based on Secure Boot

| System Type | Secure Boot Status | PALADIN Compatibility |
|---|---|---|
| Legacy/Older UEFI systems | 🔓 No Secure Boot | ✅ PALADIN boots normally |
| Secure Boot + Standard PALADIN | ✅ Enabled with 3rd Party UEFI CA | ✅ Boots without changes |
| Secure Boot + PALADIN PRO | ✅ Enabled | ⚠️ Disable Secure Boot **or** enroll MOK (advanced) |

---

## Option A: Disable Secure Boot (Recommended for PALADIN PRO)

Disabling Secure Boot ensures compatibility, especially with PALADIN PRO.

**Steps to disable Secure Boot:**

- Enter BIOS/UEFI Setup
- Navigate to **Security**, **Boot**, or **Authentication**
- Set **Secure Boot** to `Disabled`
- Save and reboot

This method is forensically sound if documented and authorized on evidence systems.

---

## Option B: Use Microsoft 3rd Party UEFI CA (For Standard PALADIN Only)

If using **Standard PALADIN** (created via Rufus or Etcher), most UEFI systems will allow it to boot with Secure Boot enabled.

**If needed:**

- Enter BIOS/UEFI Setup
- Enable **“Microsoft 3rd Party Certificate”** or **“Allow 3rd Party UEFI CA”**
- Save and reboot

⚠️ This does **not** apply to PALADIN PRO.

## ⚠️ CAUTION: Rufus & Secure Boot Compatibility

If you are using **Rufus** to create a PALADIN bootable USB on a computer that currently runs **Windows 10 or 11**, you may encounter a boot failure. Recent Windows security updates have blacklisted older Linux bootloaders to prevent security bypasses.

**Signs of this issue:**

- A blue screen error stating: **"Security Policy Violation"**.
- An error stating: **"SBAT self-check failed"**.
- A warning from Rufus during the creation process that the ISO contains a **revoked UEFI bootloader**.

**Verified Solutions (as of 2026):**

- **Use BalenaEtcher:** This tool is currently the most recommended alternative as it performs a direct "clone" of the ISO, preserving the original signatures that are more likely to pass Secure Boot checks.

- **Rufus "DD Image Mode":** If using Rufus, you **must** select **"Write in DD Image mode"** when prompted after clicking "Start." The default "ISO Image mode" modifies the bootloader, which triggers the security violation.
- **Manual Override:** If the solutions above do not resolve the issue and the system remains inaccessible, you may need to **temporarily disable Secure Boot** within the BIOS/UEFI settings to successfully boot PALADIN and proceed with your investigation.

---

### 🧭 Selecting the Boot Device

If PALADIN does not boot automatically:

**Option 1: Set USB as First Boot Device**

- Access BIOS/UEFI
- Navigate to Boot Order/Priority
- Move the USB to the top
- Save and exit

**Option 2: Use Boot Menu Shortcut**

- Reboot and press the Boot Menu key (`F10`, `F11`, or `F12`)
- Select the PALADIN USB from the list
- Press `Enter` to boot

---

### 🔐 BitLocker Recovery (If Triggered)

If triggered:

- A blue screen will appear asking for the **BitLocker Recovery Key**
- Enter the key to unlock and continue with your forensic tasks

---

## 🔑 Optional: MOK Enrollment for PALADIN PRO

If you **must boot PALADIN PRO** on a system where Secure Boot **cannot** be disabled, MOK (Machine Owner Key) enrollment may allow the system to trust the PALADIN PRO boot environment.

> ⚠️ Only perform MOK enrollment on systems **you own or control**.
> Do **not** enroll a MOK on evidence systems unless:
>
> - You have proper forensic authority
> - The action is documented

- It complies with your jurisdiction's forensic standards

### How It Works

- If Secure Boot is enabled and MOK enrollment is required, you'll see a **blue MOK management screen**
- Follow the prompts to enroll the key and reboot
- PALADIN PRO should now boot fully under Secure Boot

---

### ✅ Final Reminders

- PALADIN is fully compatible with legacy systems and modern UEFI systems when properly configured.
- Always test boot behavior before examining evidence.
- Document any changes made to Secure Boot or BIOS settings.
- When in doubt, **disable Secure Boot for PALADIN PRO**, or use **Standard PALADIN** on systems that support third-party certificates.

---

# Booting PALADIN USB on a Macintosh

PALADIN can only boot on **Intel-based Macs** (non-PowerPC). It **will not boot Apple Silicon Macs** with **M-series processors**. If you need to image an **Apple Silicon Mac**, use **RECON ITR**—SUMURI's **forensically sound solution for macOS imaging and triage**.

Before attempting to boot PALADIN on a **supported Intel Mac**, ensure you are familiar with:

✅ **Checking for a Firmware Password**
✅ **Accessing Boot Options**
✅ **Identifying Macs with a T2 Security Chipset**

---

## Checking for a Firmware Password

Similar to **Secure Boot on PCs**, Macs can have a **Firmware Password (boot-level password)** that restricts startup commands. N**o startup key combinations will work** if set except **Option (⌥) / ALT**. Instead, the Mac will boot to the login screen.

To check for a Firmware Password:

1. **Restart the Mac and hold down the Option (⌥) / ALT key immediately.**
2. If a **lock icon** appears, a **Firmware Password is set**, and you **cannot boot to PALADIN** without unlocking it first.
3. The screen will display available **bootable drives**, including PALADIN, if no password is set.

---

## Accessing Boot Options

If no Firmware Password is set, follow these steps to boot PALADIN:

1. **Insert the PALADIN USB.**
2. **Power on the Mac and hold down the Option (⌥) / ALT key.**
3. A list of boot options will appear. The PALADIN USB may be labeled as:
    - **"Windows"**
    - **"EFI Boot"**
4. Select the appropriate icon to boot into PALADIN.

---

## Macs with a T2 Security Chipset

Macs with a **T2 Security Chip** have **Secure Boot enabled by default**, which **prevents booting from external devices like** PALADIN.

- If the **T2 Mac's Secure Boot settings have not been modified**, it **cannot boot PALADIN**.
- If Secure Boot was **manually disabled**, it may still be possible to boot from USB.

For forensic imaging of **T2 Macs and Apple Silicon (M-series) Macs**, SUMURI **recommends** using **RECON ITR**.

---

## Quick Summary: How to Boot PALADIN on a Supported Mac

1. **Insert the PALADIN USB.**
2. **Check for a Firmware Password** by holding **Option (⌥) / ALT** at startup.

- If a **lock icon appears**, a Firmware Password is set, and booting to an external drive, like PALADIN, is not possible.
  3. **If no Firmware Password is set, select the PALADIN USB**, which may be labeled as **"Windows"** or **"EFI Boot."**

# Using PALADIN Persistent Mode

## What Is Persistent Mode?

PALADIN's new **Persistent Mode** allows you to save settings, data, configurations, and installed tools between reboots. This means you can now:

- Configure your toolset once (e.g., set up Autopsy the way you like it)
- Install extra utilities
- Save case notes or scripts ...and have it **all ready to go** the next time you boot.

This is a major leap forward from traditional "live" boot environments that start fresh every time.

---

## 🔧 How It Works

PALADIN looks for a **specially named storage volume** labeled either:

- `writable` (recommended), or
- `casper-rw`

This volume can be located on:

- The same USB drive as PALADIN
- A **separate external USB drive**
- An **internal hard drive or SSD** partition

As long as the volume is available at boot and properly labeled, PALADIN will detect it automatically when you choose the **Persistent Mode** option from the boot menu.

---

## ✅ Setting Up the Persistence Volume (Recap)

> If you've already created the persistence volume using the PALADIN Toolbox, you can skip this step.

To set up persistence:

1. **Boot PALADIN in Live mode (non-persistent)**
2. Open the **PALADIN Toolbox**
3. Go to the **Partition Formatting** section
4. Select the USB drive or other device/partition to use
5. Format it as **ext4**
6. Set the **volume label** to either `writable` or `casper-rw`
7. Apply the changes

Once this is complete, you're ready to boot into Persistent Mode.

---

## 🚀 Booting into Persistent Mode

1. **Insert the PALADIN USB drive** (and external persistence device, if applicable)
2. Reboot the computer
3. At the **PALADIN boot menu**, use the arrow keys to select the option labeled **"Persistent Mode"**
4. Press `Enter` to boot

> ⏳ **Helpful Tip**: After selecting Persistent Mode, wait **about 5 minutes** for everything to load—especially on slower or older hardware. You'll notice a brief delay as PALADIN mounts the persistence volume and loads saved data.

---

## 💾 Using Persistence Mode

Once booted:

- All **changes to system settings**, desktop preferences, or application configurations (like Autopsy) will be saved.
- **Files saved in your home folder**, logs, and small scripts remain after reboot.
- The persistence volume acts like a miniature user environment, separate from the system core.

You can:

- Pre-configure toolkits
- Save case files in progress (on non-evidence devices)
- Maintain preferred layouts or language settings

---

## ⚠️ Things to Remember

- You **must select "Persistent Mode" at boot** each time to access your saved environment.
- Booting in standard **Live Mode** will ignore the persistence partition and start a clean session.
- Avoid storing actual evidence or large case data on the persistence partition; use external media for evidence handling.

---

## 🔒 Pro Tip for Forensic Workflow

Persistence is especially useful for:

- **Custom pre-configured environments** (e.g., Autopsy tuned for your lab)
- Training environments or classroom use
- Quick field use where you don't want to reconfigure tools each time

# PALADIN OS Overview

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

- PALADIN Dock
- Activities Overlay/Forensic Tools
- PALADIN Toolbox

**PALADIN Dock**

The PALADIN Dock can be accessed along the left side of the Desktop, by default. From here you access and manage common applications that have been pinned there: Google Chrome, Terminal, PALADIN Toolbox, and Autopsy, by default.

**Shutting Down PALADIN**

To shut down PALADIN, you can press the power button on the device to bring up the shutdown/reboot menu overlay. To find the button within the OS, you can click in the top right corner of the Desktop, where the battery indicator is. Then, click the power icon in the top right of the dropdown menu.

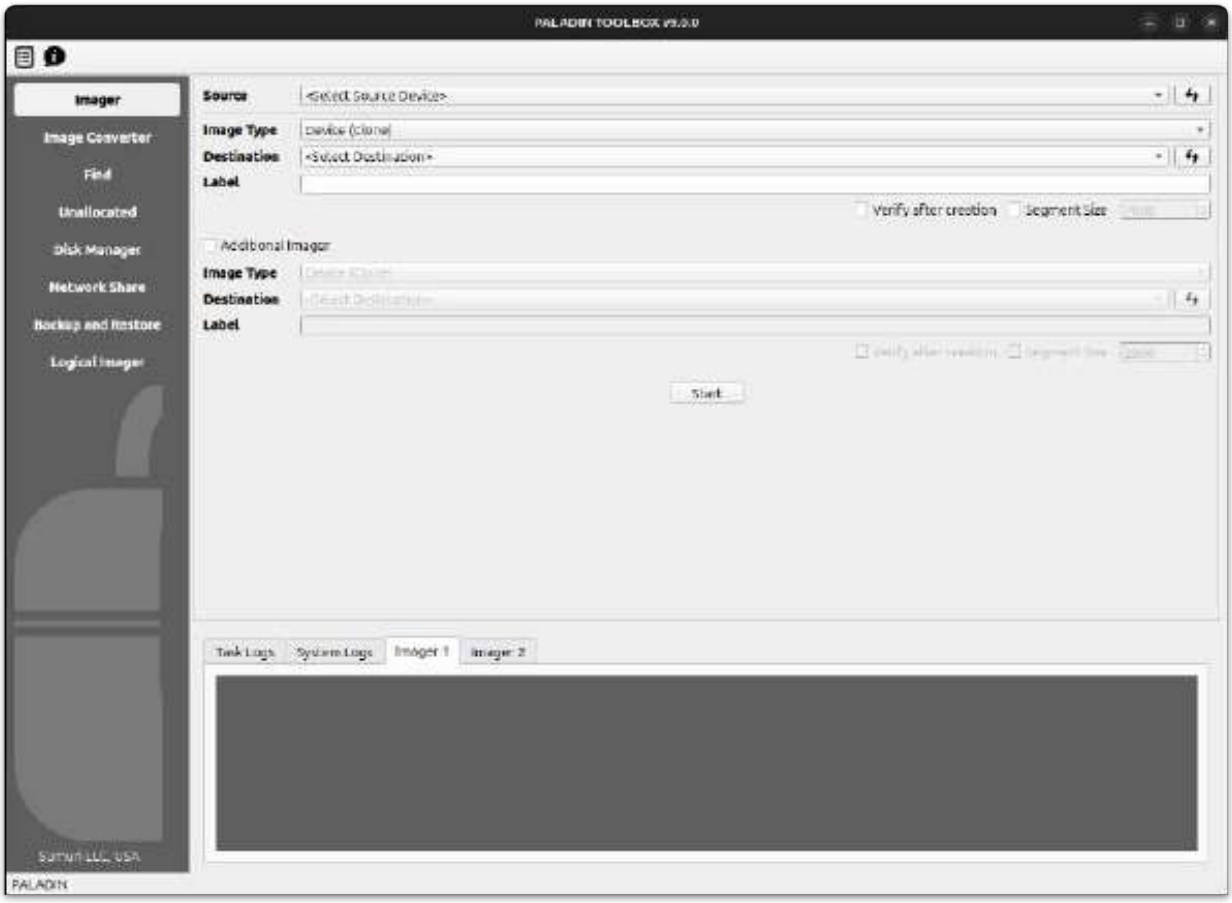
**PALADIN Toolbox**

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.

**Activities Overlay/Forensic Tools**

To access other applications and tools besides those pinned to the dock, you can click the shield icon in the bottom left of the Dock, or click the Windows button on a Windows keyboard, or the Command button on an Apple keyboard, to bring up the Activities overlay. This view will show you all the currently open applications as well as allow you to navigate and search for the other installed tools.

# 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 rewritten to account for technology changes and continues to be updated.

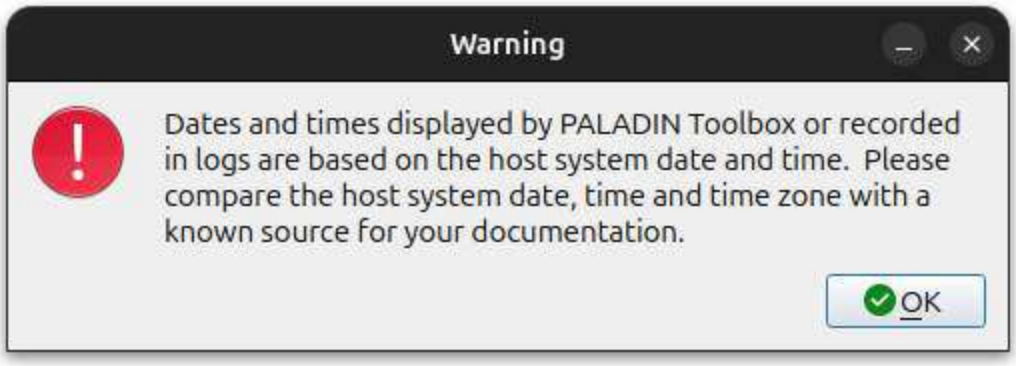
The PALADIN Toolbox has combined and simplified multiple forensic tasks into one easy-to-use GUI (graphical user interface) that requires minimal training and does not require users to utilize the command line.

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 before 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).

In this section, we will be covering the following:

- Date and Time Settings
- Logging
- Preparing Media (Drives) - Sterilize, Format
- Mounting Media (Drives)
- Imaging and Cloning
- Imaging Across a Network
- Converting an Image
- Imaging Unallocated and Free Space Only
- Hashing and Verification
- Mounting a Logical Forensic Image
- Logical Imaging and Bitlocker Encryption

## Date and Time Settings



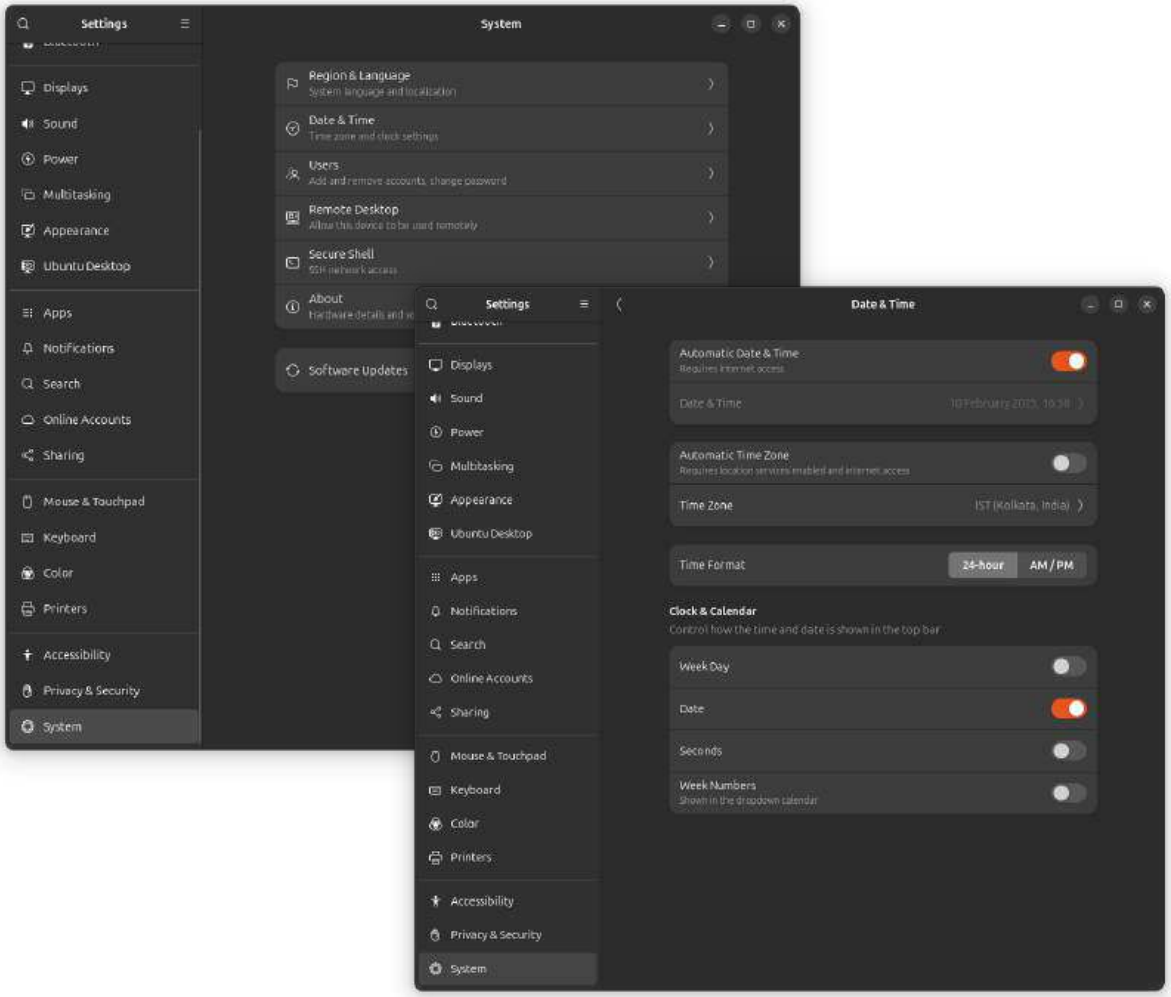

When the PALADIN Toolbox is first started, a warning message appears.

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 in the top-right corner of the Desktop (usually where the Battery Icon is located) and then on the Gear Icon to open the Settings application.

Inside Settings, you'll need to navigate to System > Date & Time to find the settings to change these values.




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

## Logging

There are three 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.

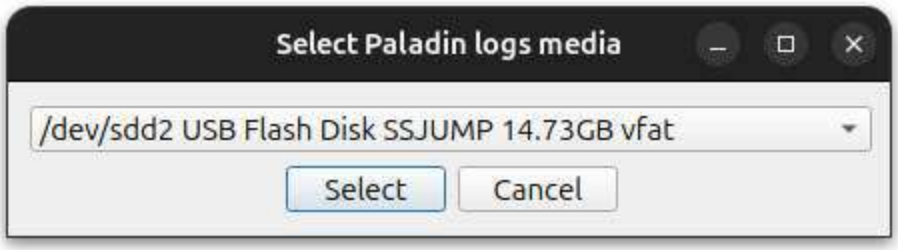
**Module-specific logs** show information relating to the current module being used and typically show live information. For example, in the image below, you are seeing Module-specific Logs for the Disk Manager Module (“Verify” and “Wipe”).

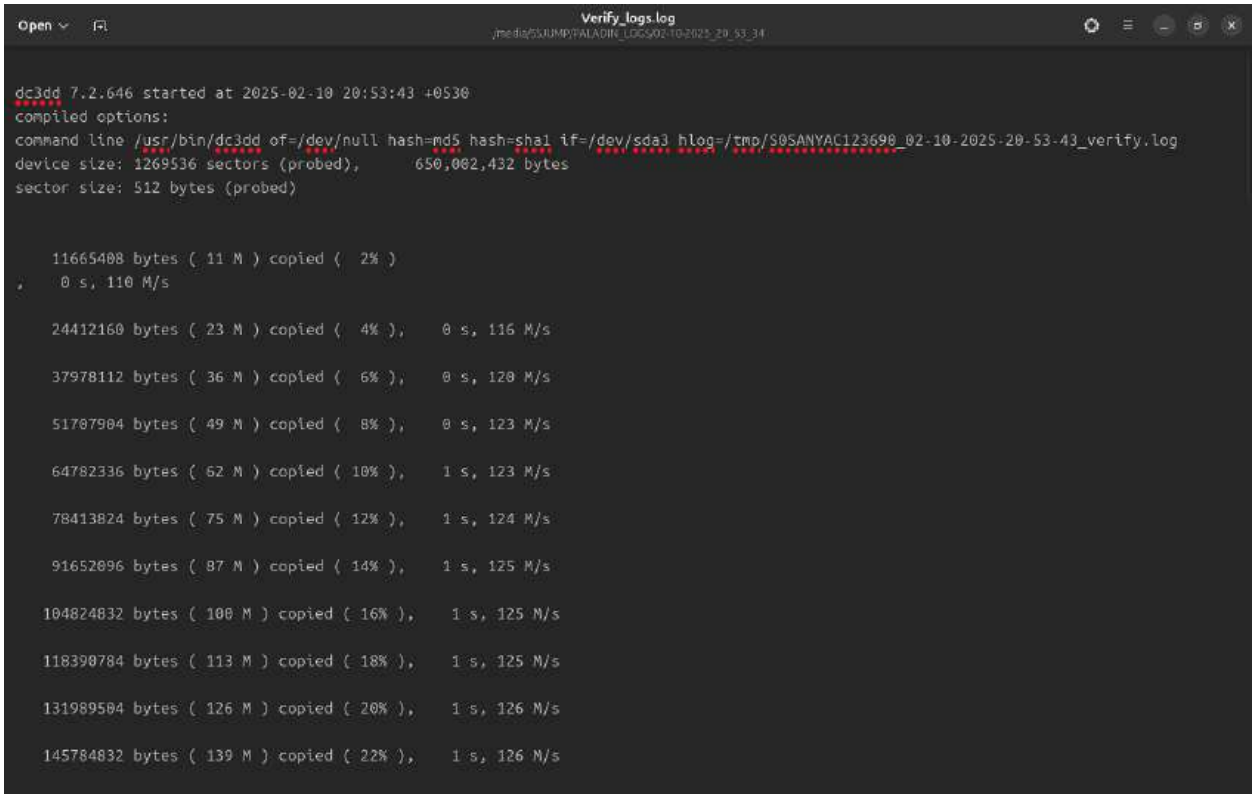

Logs in the PALADIN Toolbox can be saved automatically to a destination drive of your choice. Insert and mount a drive where you would like your logs to be stored. If necessary, you can prepare the drive using the Disk Manager in the PALADIN Toolbox.

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


## 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.

## Preparing Media

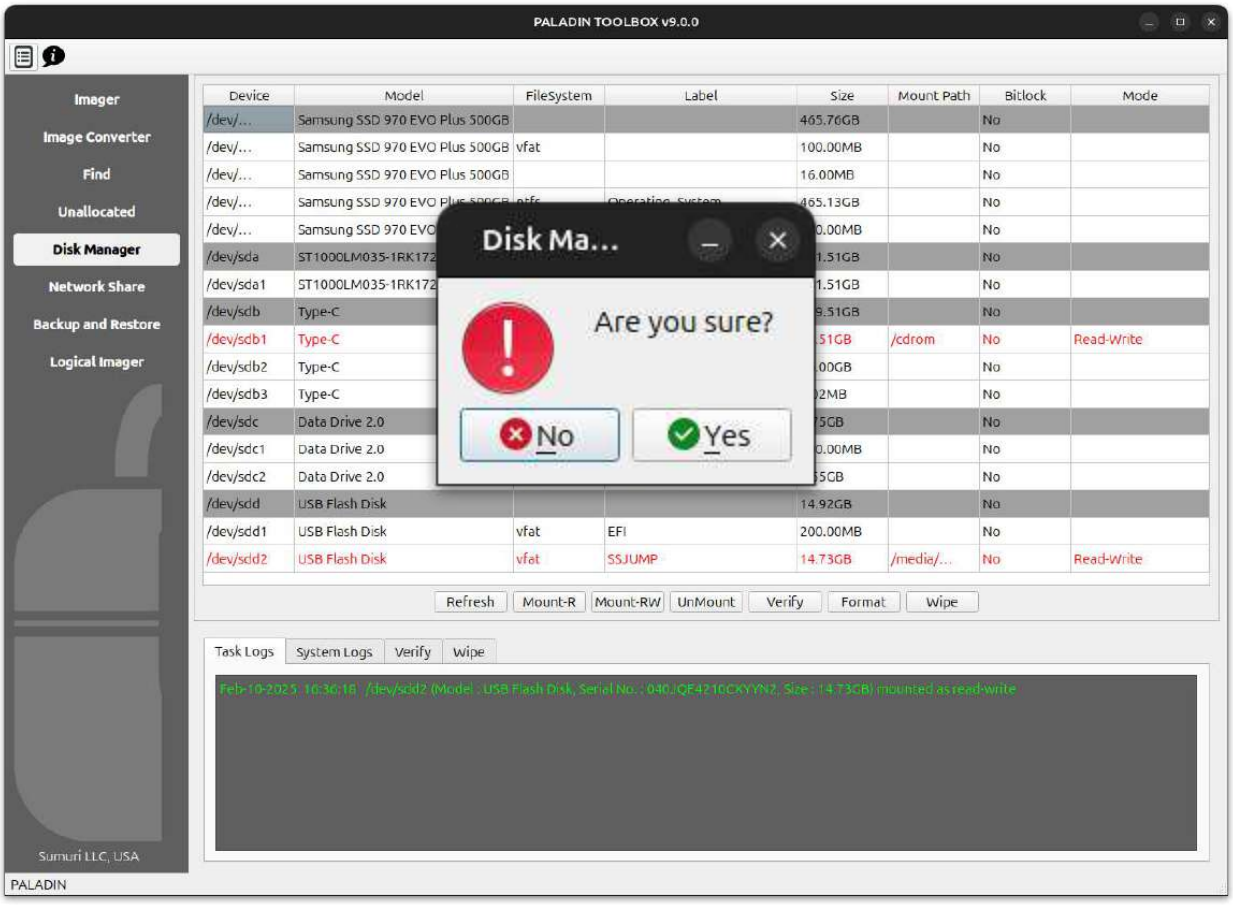
### Sterilize (Wiping)

Many agencies require that the media being 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. The 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.

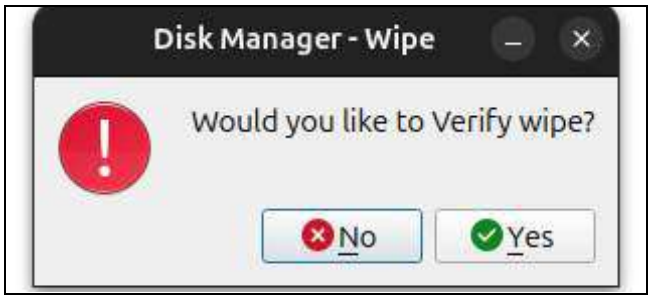
The PALADIN Toolbox speeds up the process of verification by simply scanning the device for anything that is not a zero, which is much more efficient and faster. The results of this scan are either pass or fail.

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

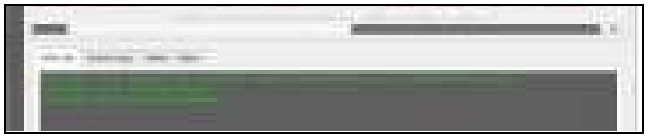


Once you have clicked “Wipe,” the Toolbox will ask you if you are sure ... ONCE!

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




Wiping of the device that you selected now begins.



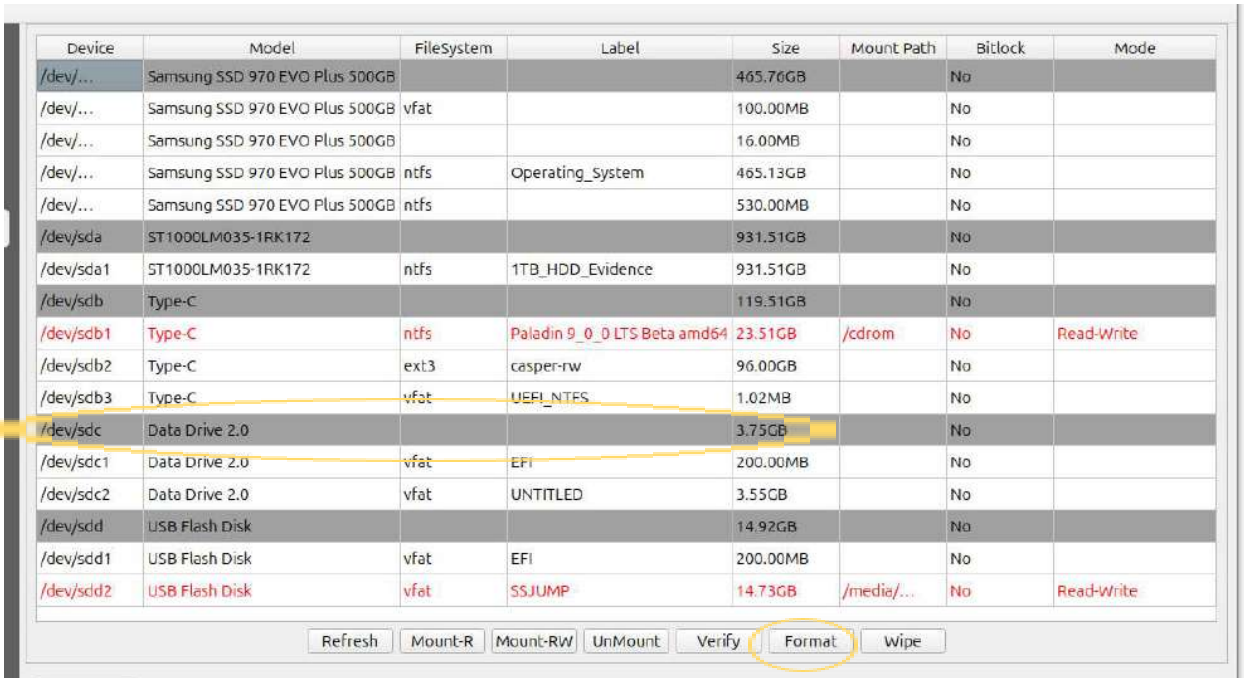
“Device Wiped successfully” message appears after successful verification. The device is now ready for formatting if desired.

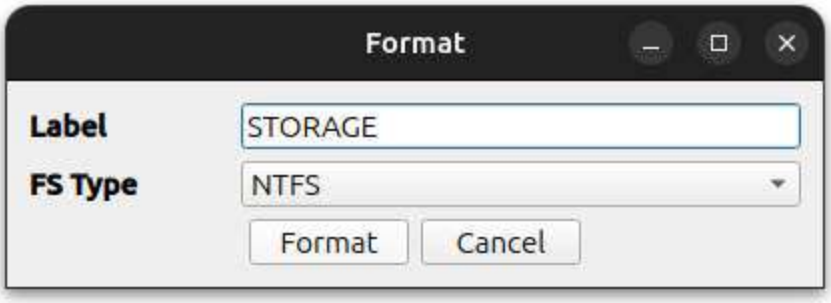
## Formatting

PALADIN Toolbox makes it easy to format a device with any of the following 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.






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 has 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).

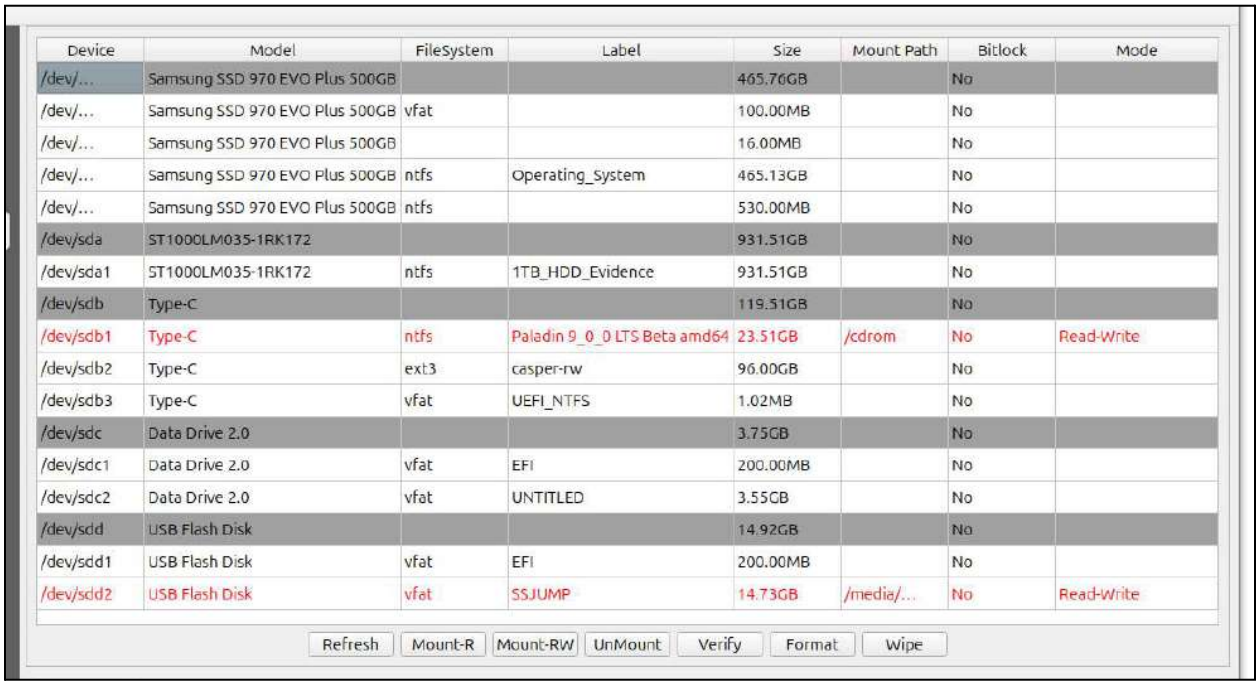
PALADIN Toolbox supports the following forensic image formats (types):

- **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)
- **Device** (for device cloning, to be discussed later)

## Hashing

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

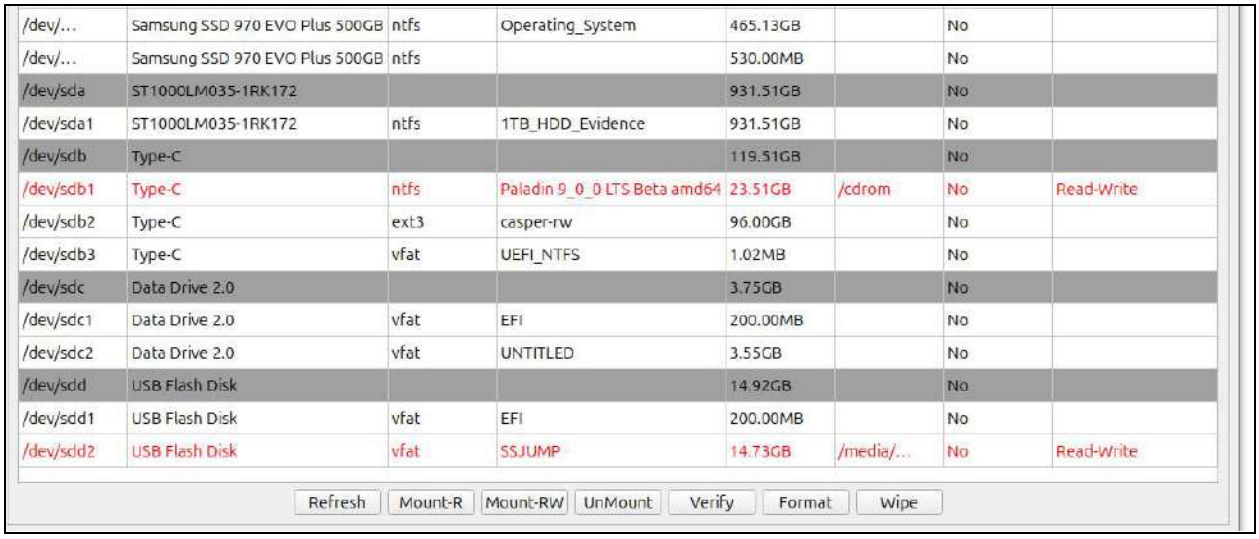
For physical devices or logical volumes, select the device or volume to be hashed and click “Verify” to begin.




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

## 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 that attached devices are not accidentally altered. The mounting and unmounting of disks occurs in the Disk Manager module. Simply highlight a device or volume and click the appropriate button.

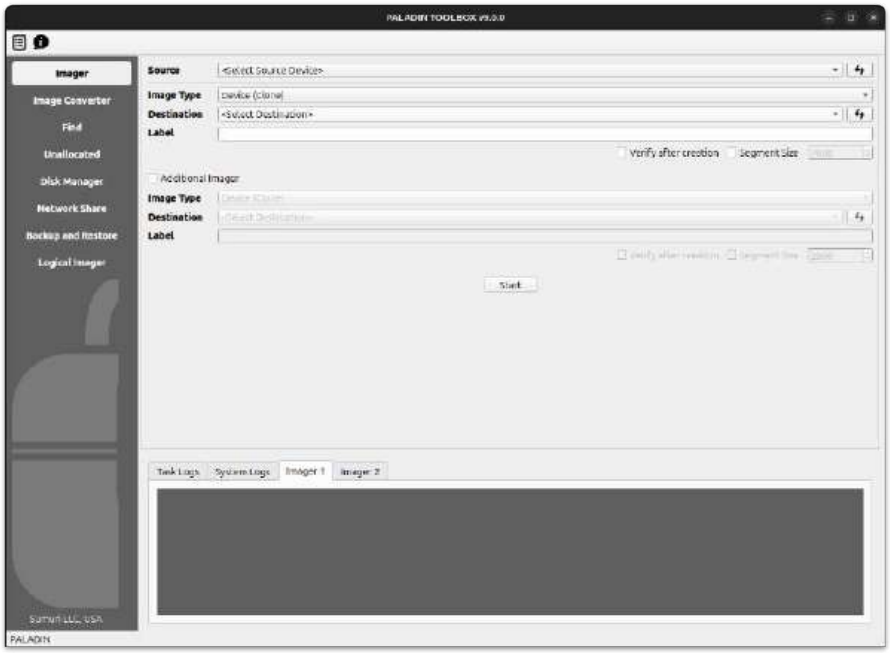



| GREEN - mounted read-only | RED - mounted read-write |
|---|---|

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

## Imaging a Drive

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



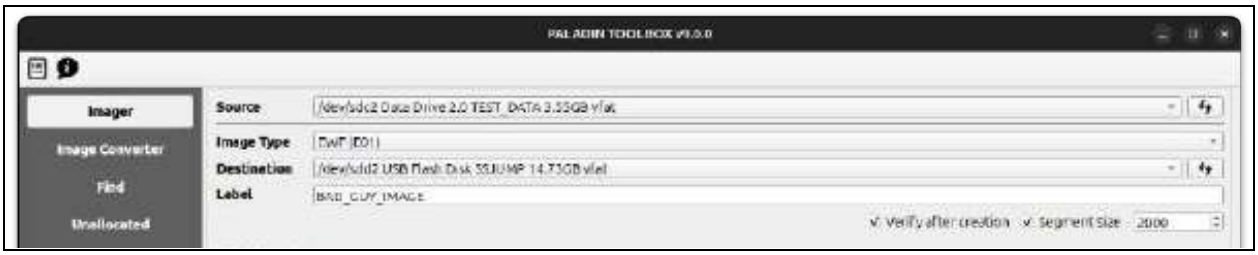

- **Source** - Select the physical or logical drive that you want to image.
- **Image Type** - This is where you select the type of forensic image for the output or select “Device” to make a clone.
- **Destination** - This is the volume where you want your forensic image to go.
- **Label** - Name for 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** - Start imaging once your parameters are set.

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

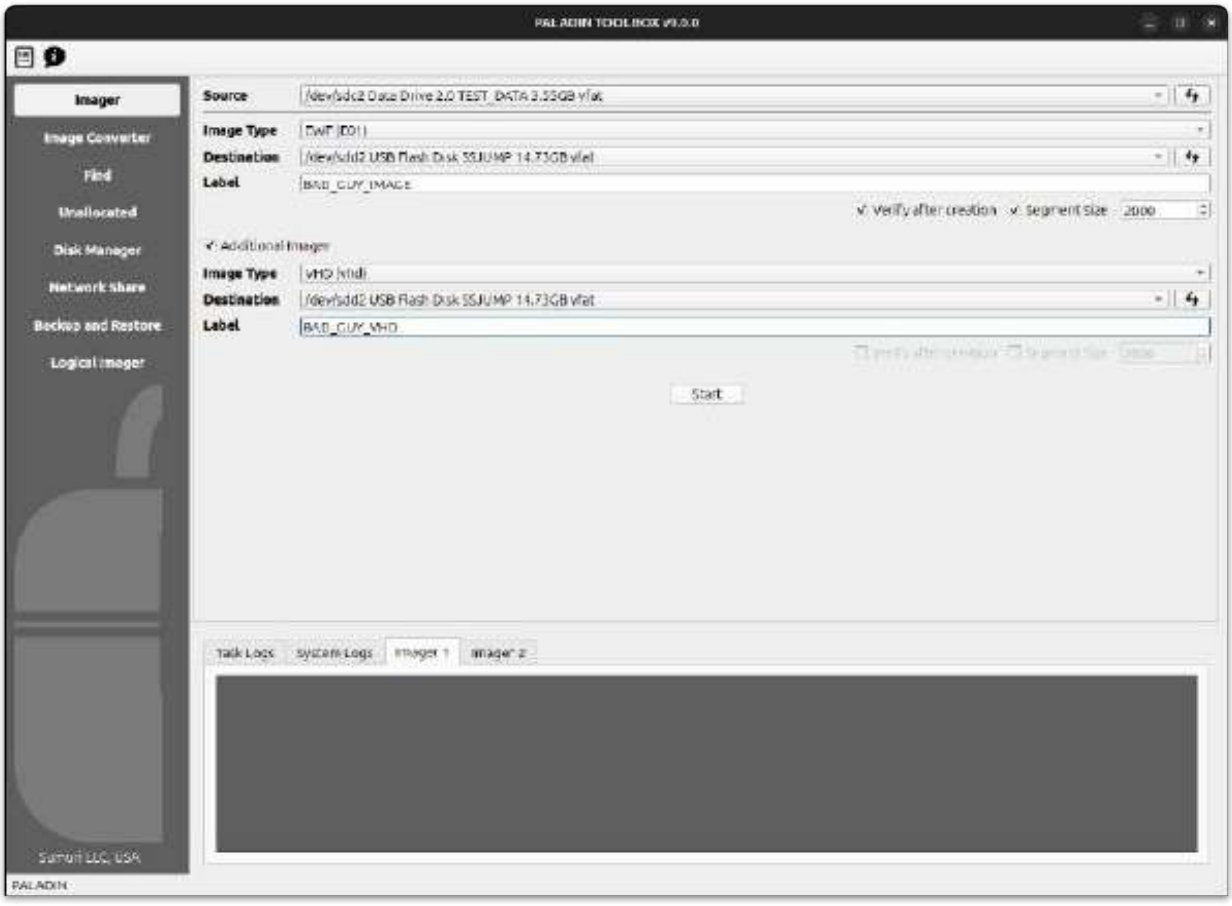
**There is no need to pre-mount any devices or drives for imaging**. PALADIN automatically mounts the destination drive that you have selected.

## Imaging to an Additional Drive or Creating Two Different Images

The 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 that if you are using the “Additional” image option, you must use a different “Label” for each image to avoid overwriting.



## Imaging Example




The example above shows the following configuration:

A single physical partition (/dev/sdc2 TEST_DATA) is being imaged to a collection drive (/dev/sdd2 “SSJUMP” volume) and then as a Virtual Machine image to the same drive.

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

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

## 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.

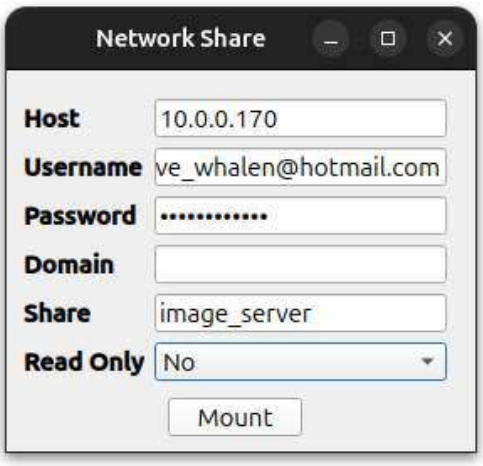

To create a device clone, choose the physical drive in the "Source" field. Under "Image Type," select "Device." Then, in the "Destination" field, specify the drive for the clone. Lastly, enter a label in the "Label" field and click "Start."

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

## Imaging Across a Network

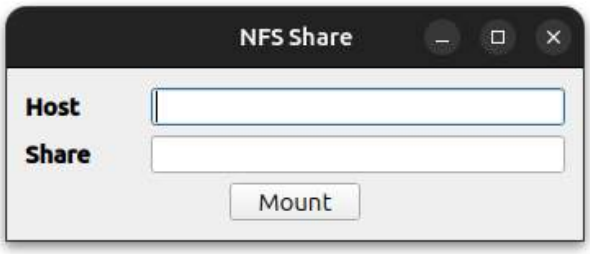
One of the coolest features of the PALADIN Toolbox is its ability to image across a network. This could be from your workstation to an Image Server, or it could be out in the field, imaging a large RAID or server to a NAS (Network-Attached Storage) that you brought along. As long as you have set up a 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 login.
- **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:



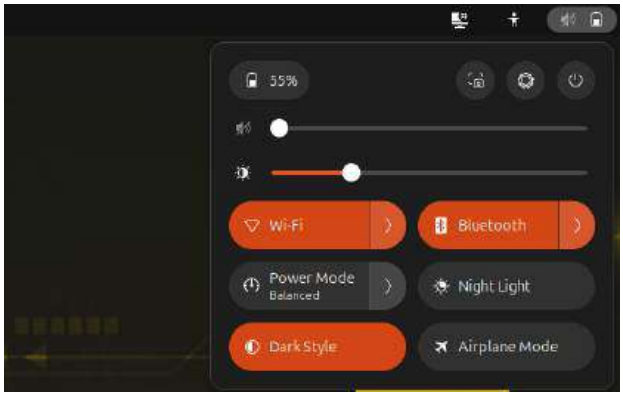

- **Host** - Typically, the IP Address of the server.
- **Share** - this is the drive or directory that you are sharing.

## 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 computer and globe icon in the top-right corner and click it to bring up the menu. Select “Enable Networking” from the menu.

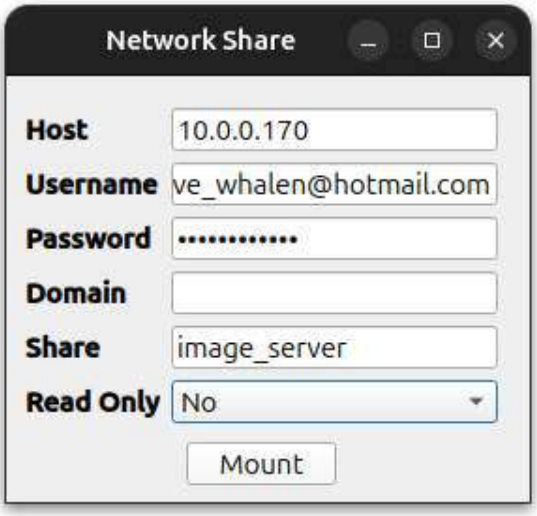
When selecting “Enable Networking,” there will be a warning message that pops up that must be accepted, or the command will be canceled.


Once the network is enabled, clicking on the same icon in the top-right will bring up options. 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 connect the PALADIN Toolbox to your server by using the “Network Share” module and entering your SMB or NFS connection settings and clicking “Mount”.

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



## 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 with read-write privileges with the images that you would like to convert.

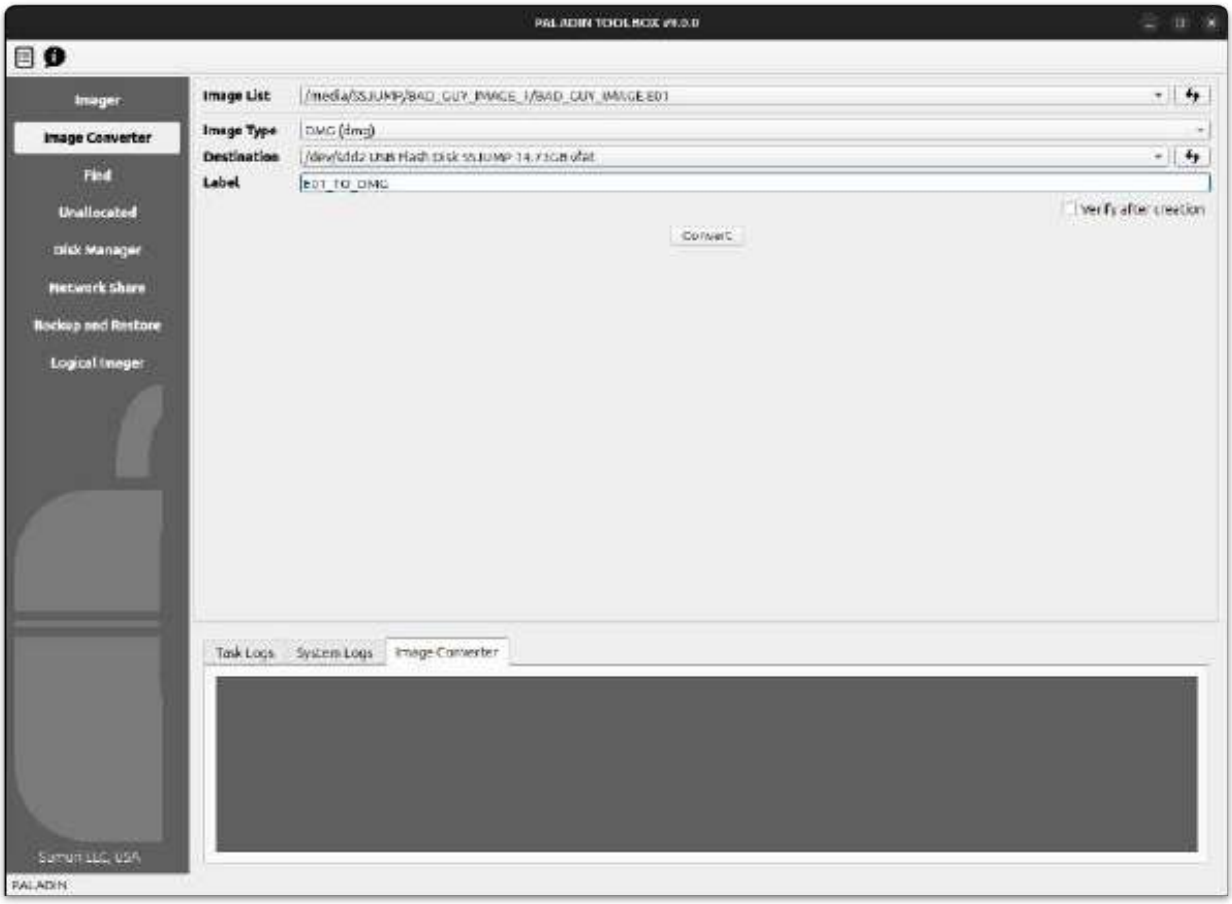



**Image List** - Your forensic images to convert. If you do not see your images, hit the "Refresh" button next to the dropdown box.

I**mage Type** - Select the new format for the forensic image.

**Destination** - Where to send the new image format.

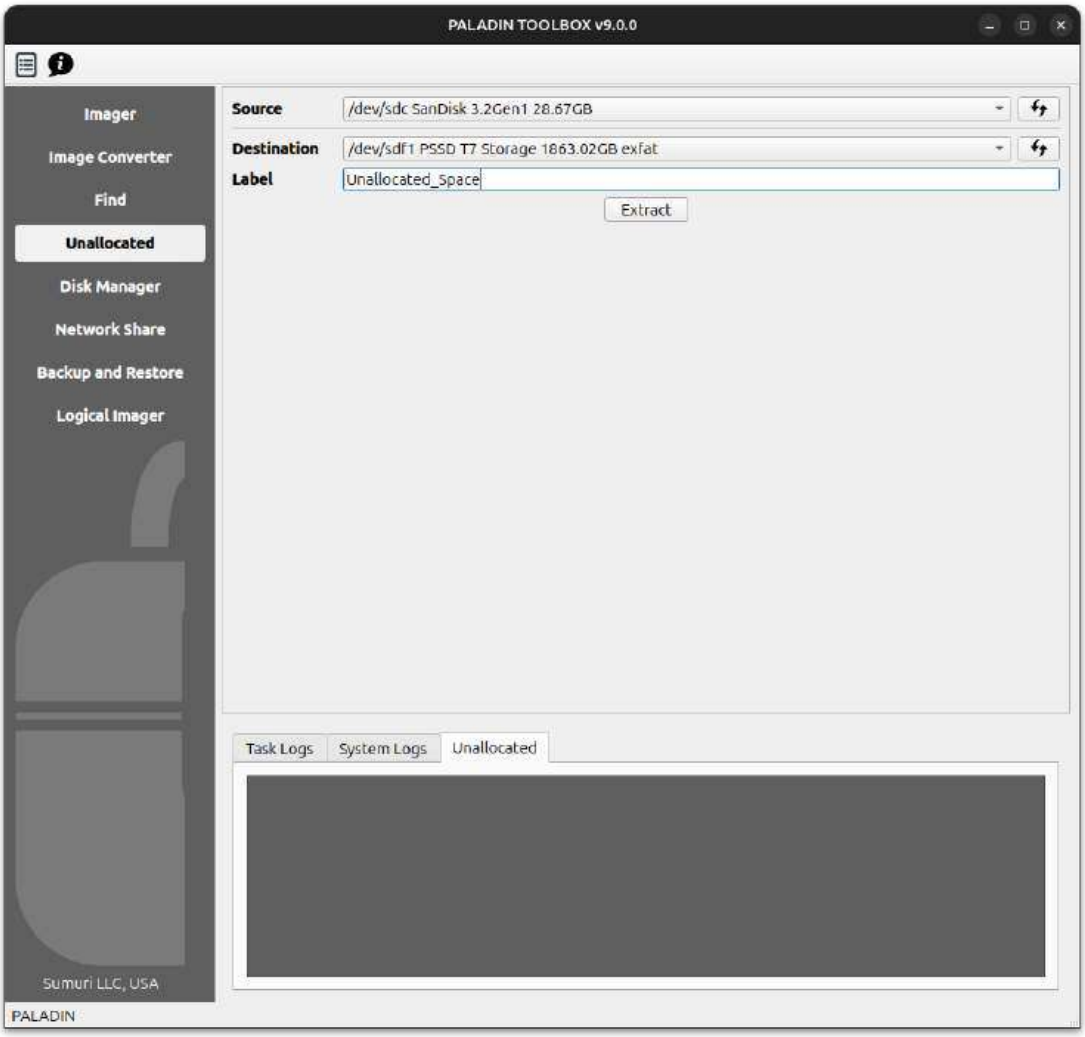
**Label** - Enter a name for the conversion.

Click "**Convert**" to begin.

## Imaging Unallocated Space

Another useful feature of PALADIN is its ability to image only the Unallocated Space and Free Space (unpartitioned space) as raw image files that can be carved later 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.



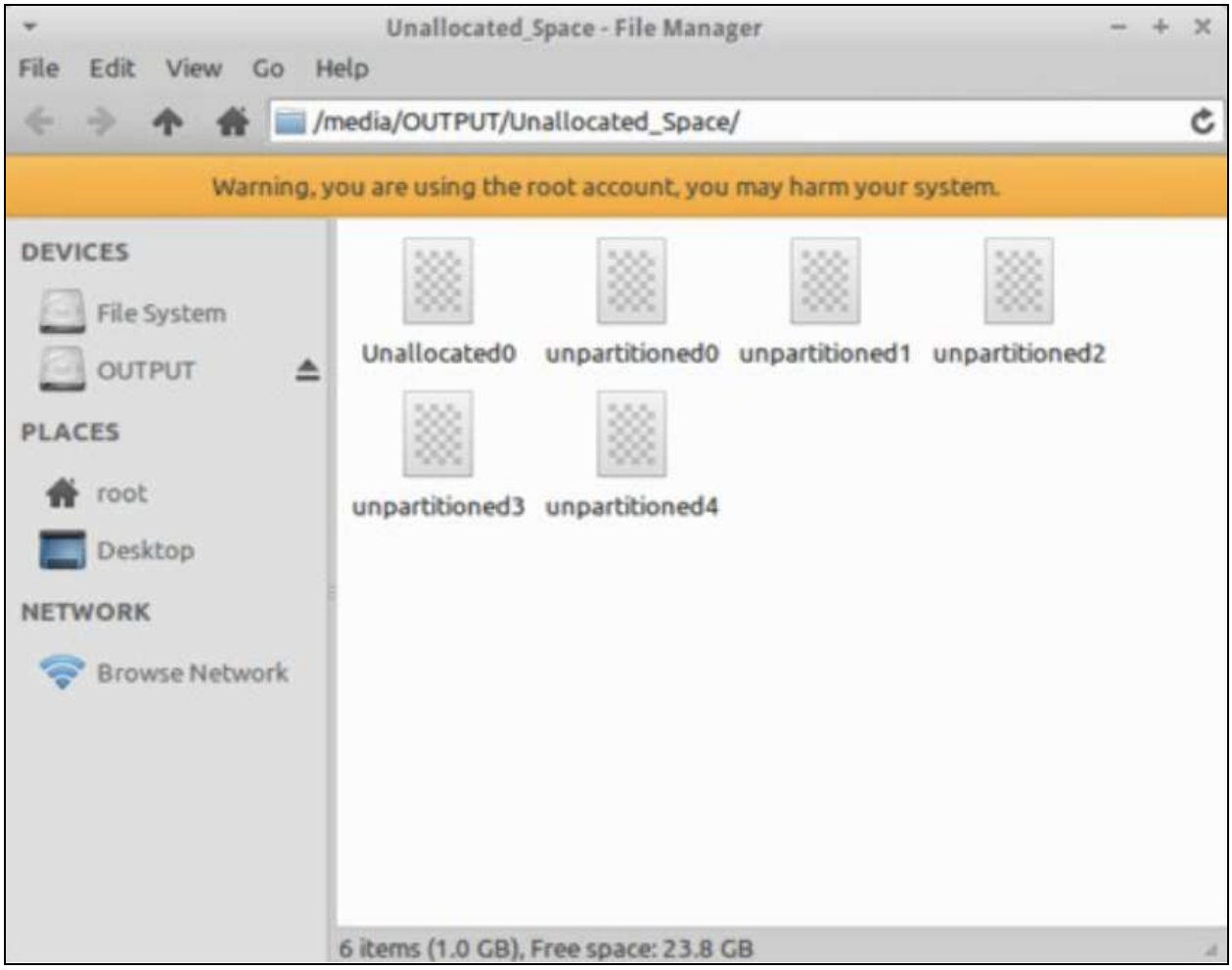

**Source** - Select the device for unallocated and free space extraction.

**Destination** - Select the drive that will store the extracted data.

**Label** - Enter a name for the session.

Click "**Extract**" to begin.

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 “File Carving”:

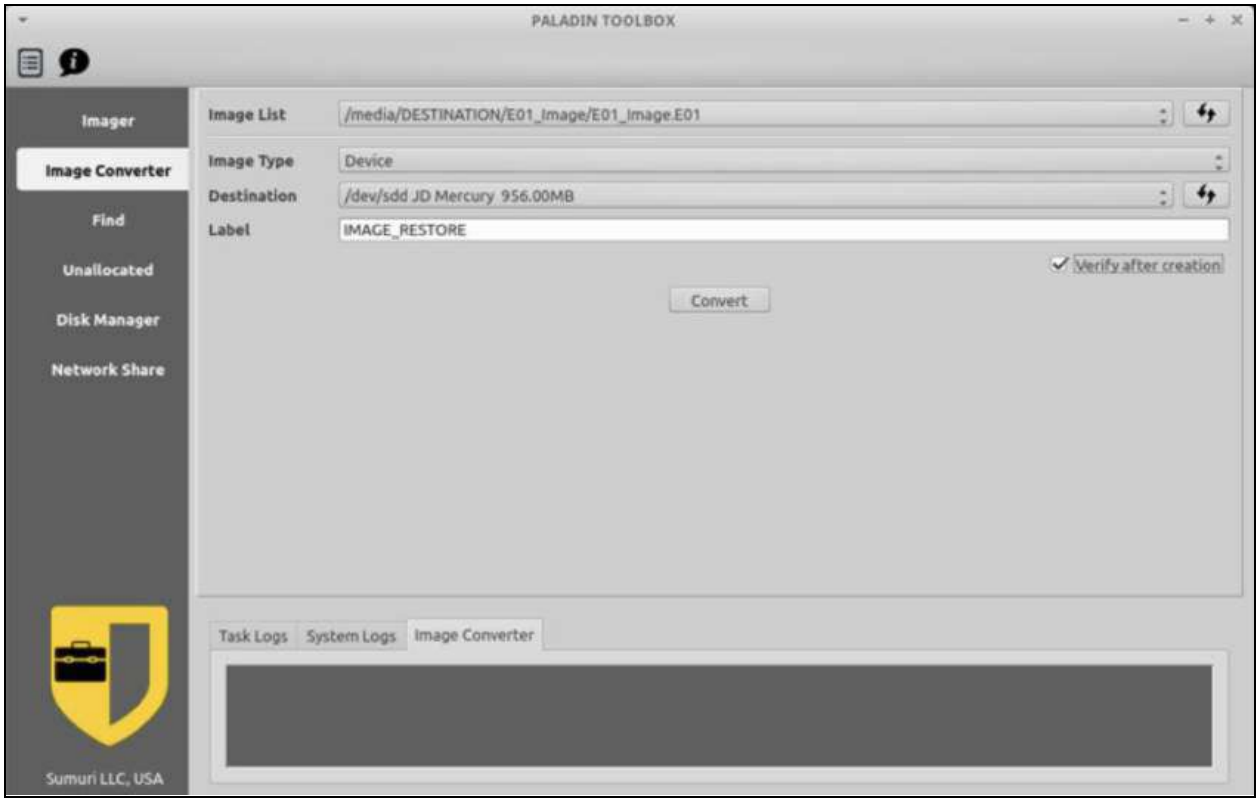
- Foremost
- Photorec
- Scalpel
- And more!

## Restoring a Forensic Image

To restore a forensic image to a physical disk, use the Backup and Restore Module.

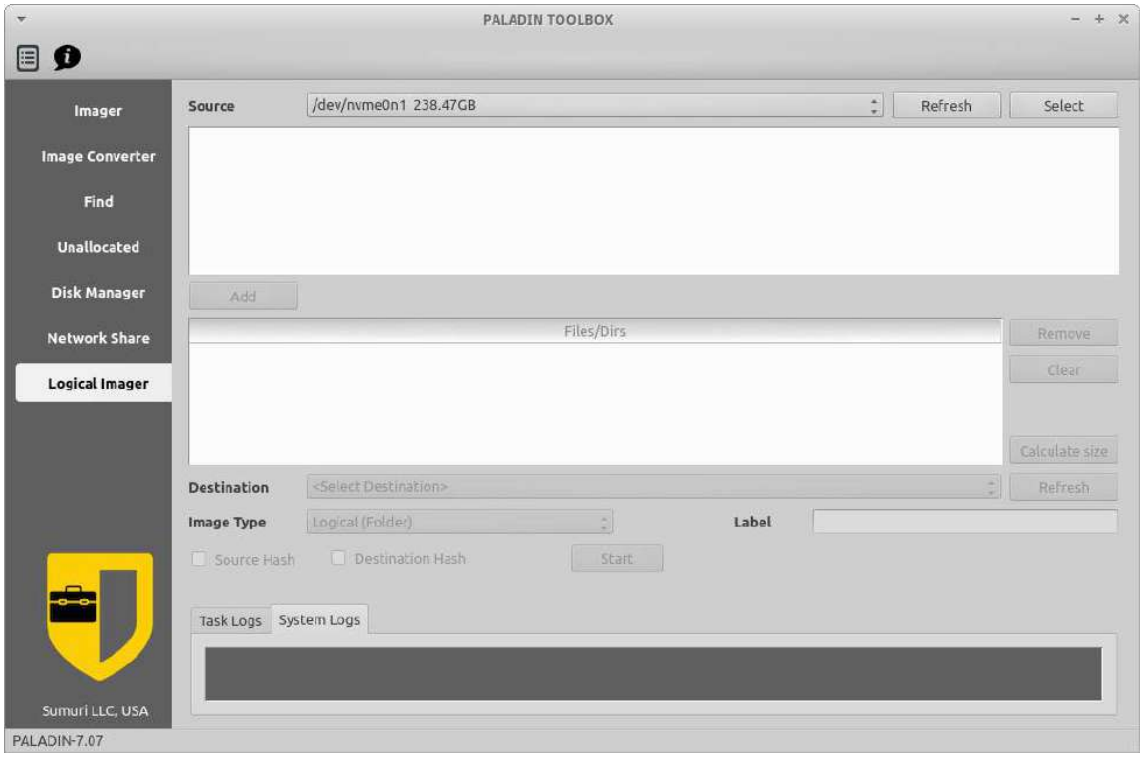
Select the Restore tab and make sure that the device containing the forensic image to be restored is mounted read-write. If you do not see your image in the drop-down list, please click the “Refresh” button. Select the forensic image to be restored from the “Image List.”

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

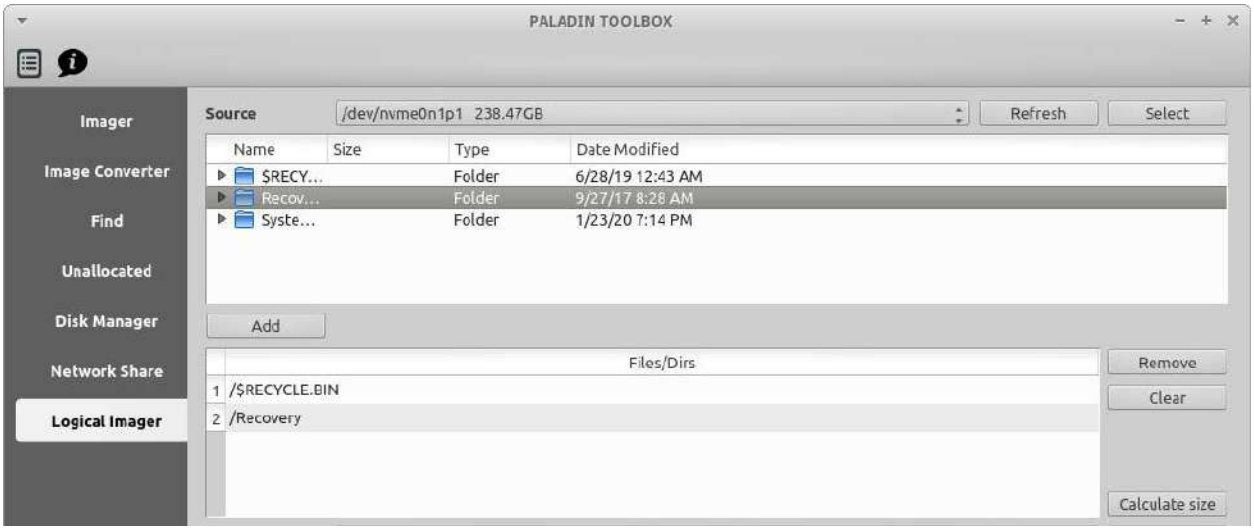


## Logical Imaging

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



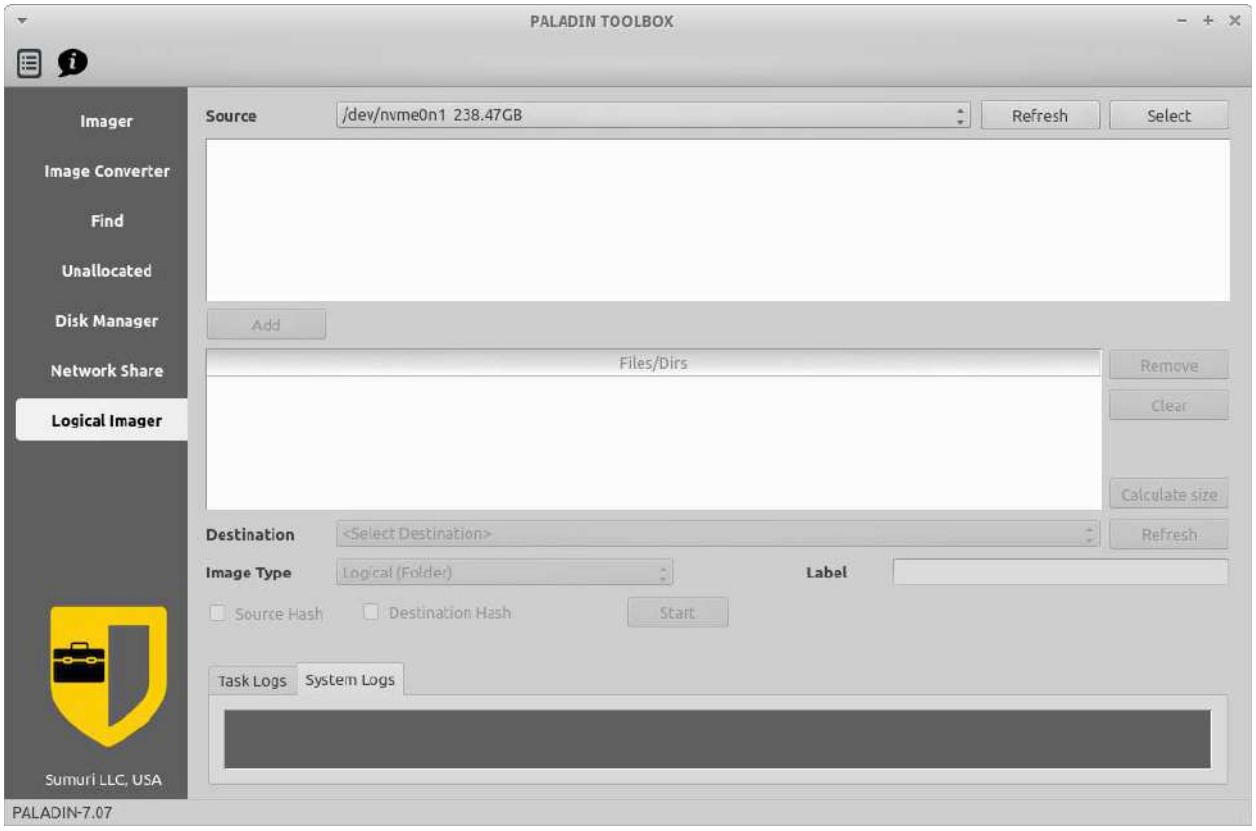

Once the source is selected, individual folders and/or files can be selected and sent to a destination. The image can also be hashed at both the source and destination.



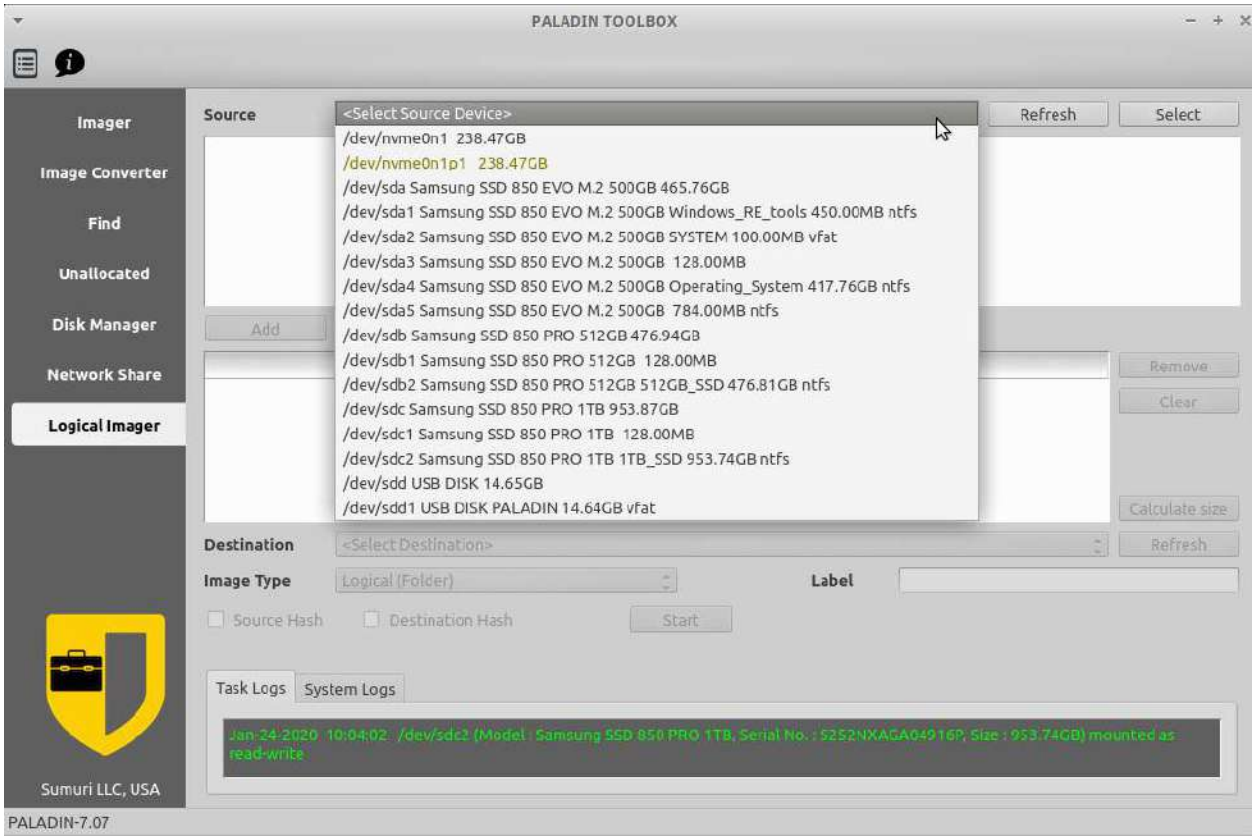
## Bitlocker Decryption

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

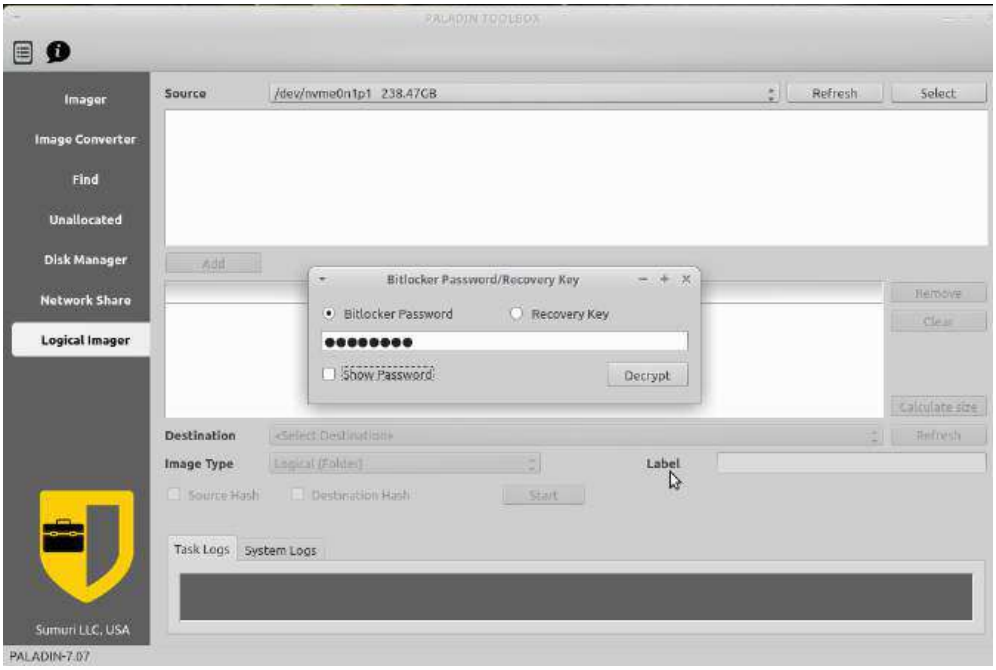
To decrypt a BitLocker partition in the PALADIN Toolbox, select the Logical Imager module.



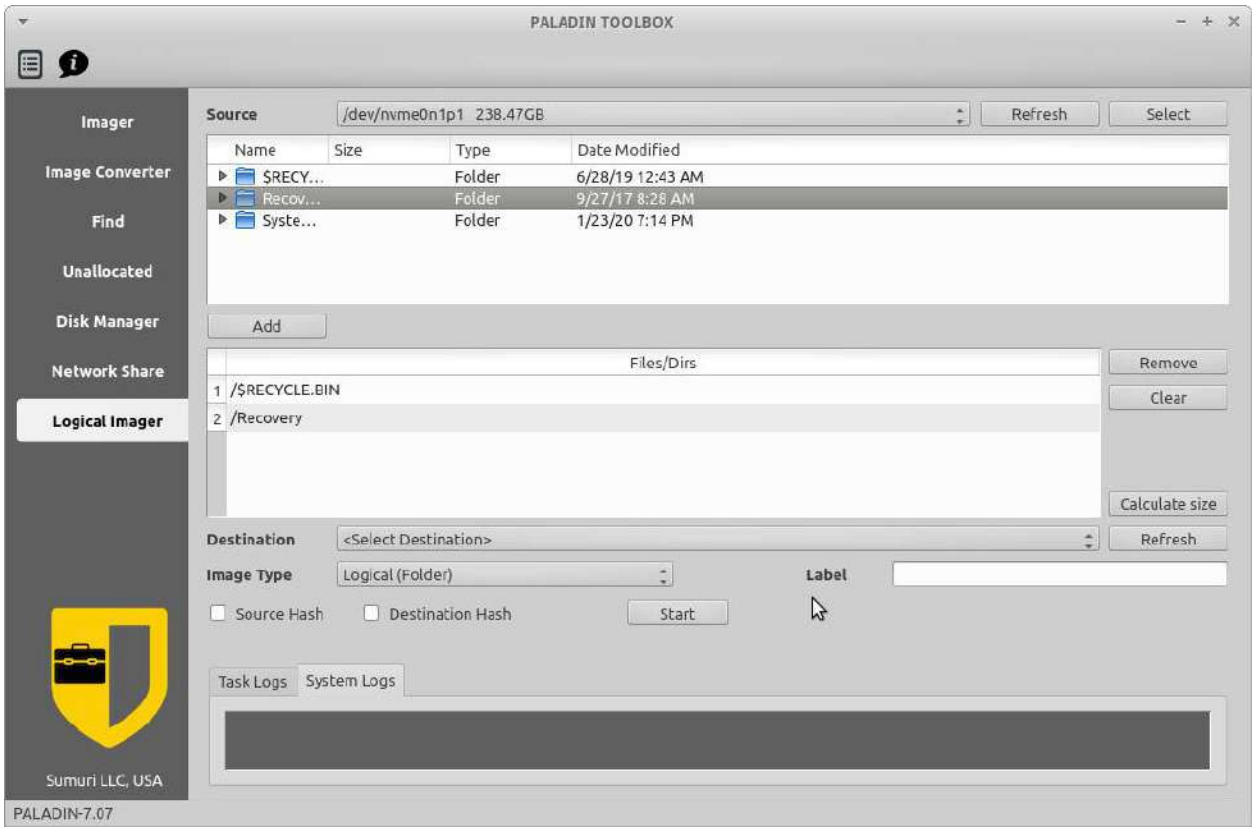

The source dropdown will display all the available partitions. BitLocker-encrypted partitions will have olive text.



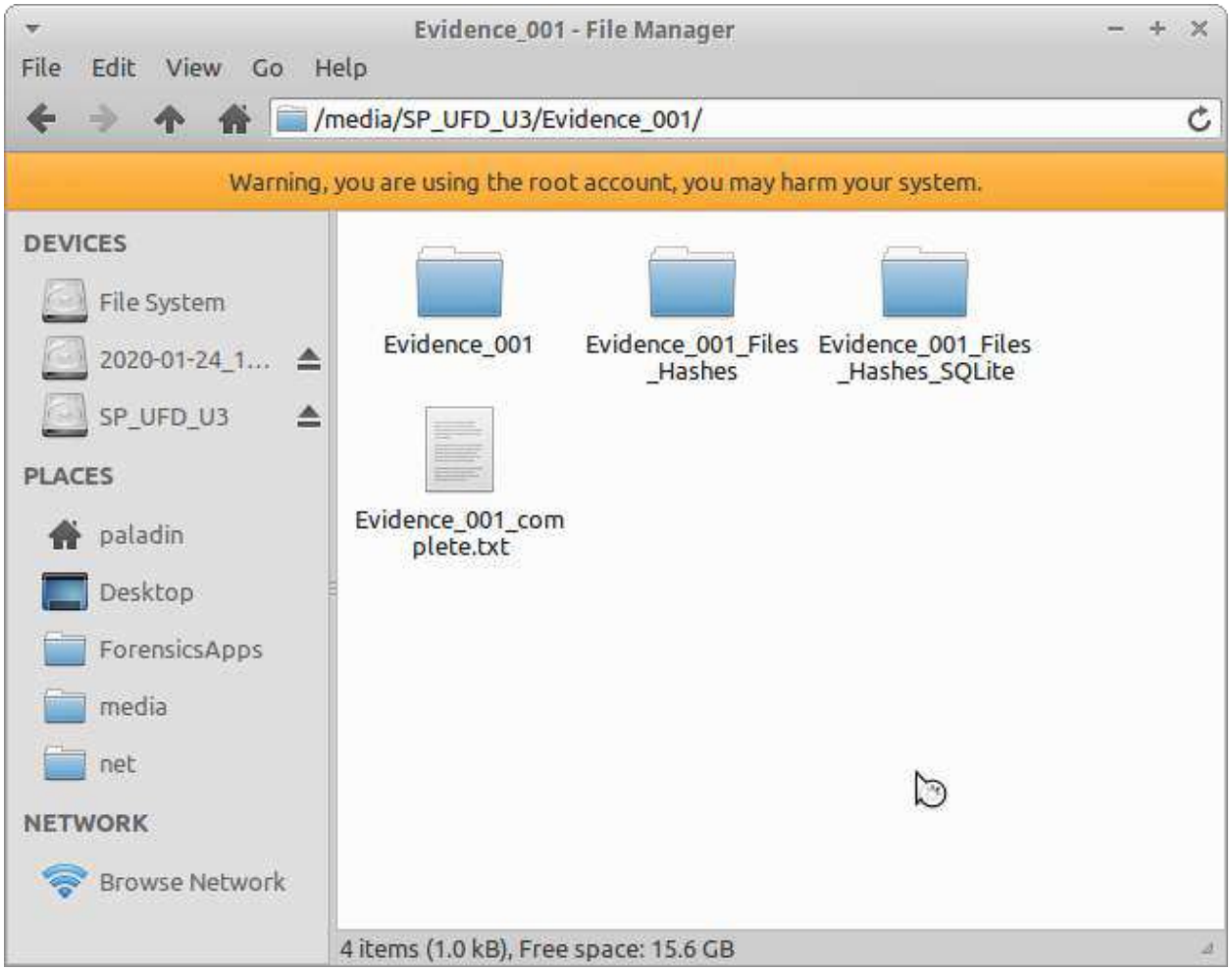

After selecting the BitLocker partition, enter the password and click decrypt.



After decryption finishes, select the folders or files to be recovered, select 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.

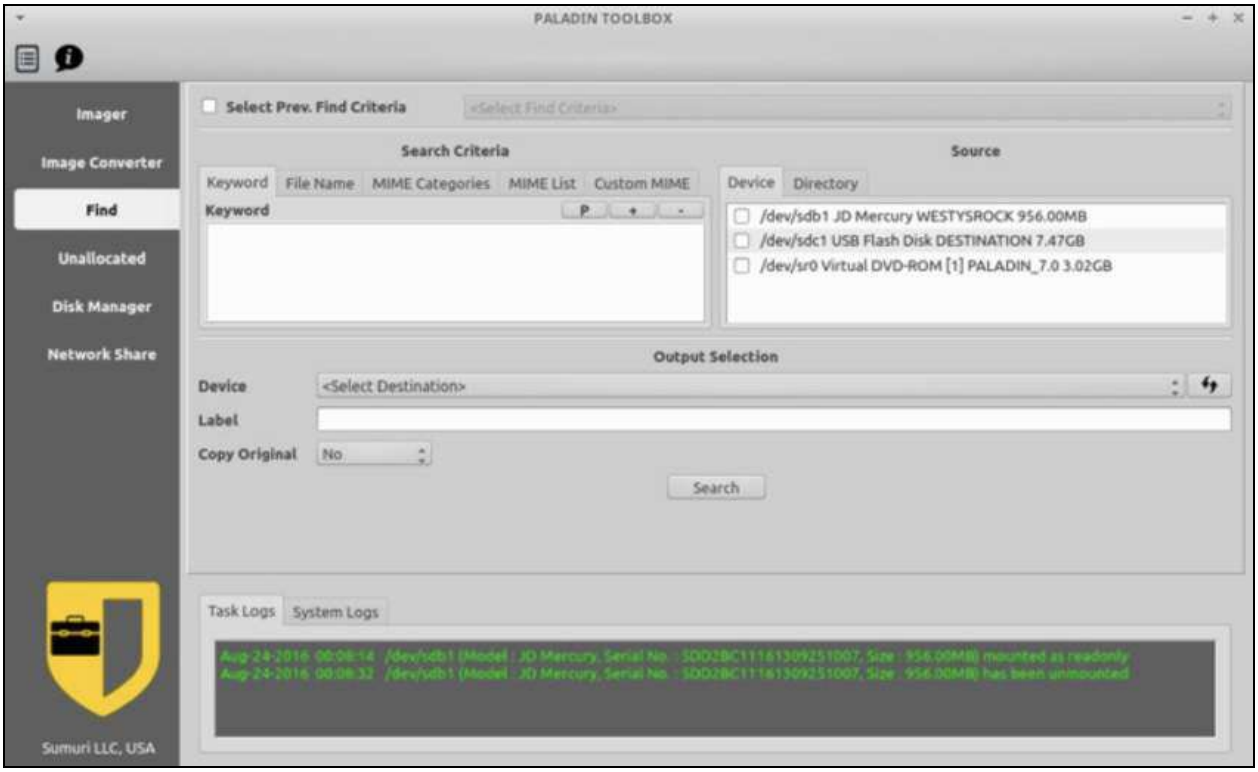


## TRIAGE with PALADIN

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 that 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.



## 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

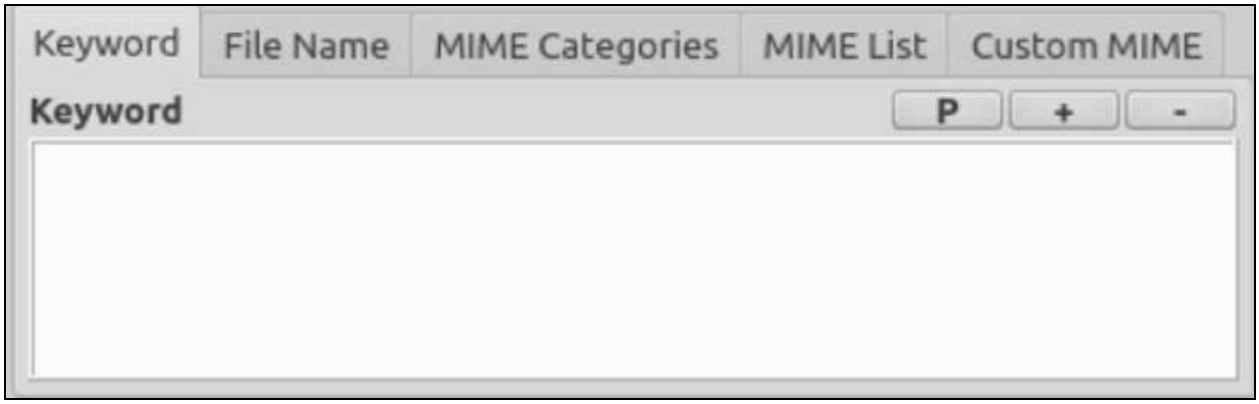
Attach a destination drive to save your search results and to optionally copy out files of interest and mount as read-write. PALADIN will remember your searches, which can then be reloaded later. This saves you from having to enter a large number of search parameters more than once.

“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 format your destination as HFSPLUS, NTFS, or EXT4. The FAT32 (VFAT) and ExFAT formats can be used for the destination drive, however, the files that are located will automatically be copied to your destination drive.

You are now ready to begin your Triage/Search.

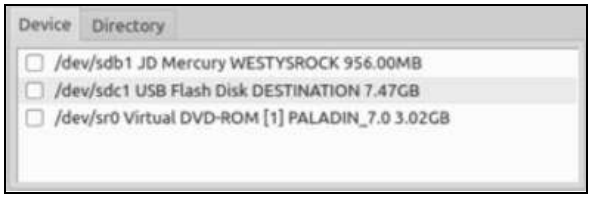
## Find Search Window

- **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.

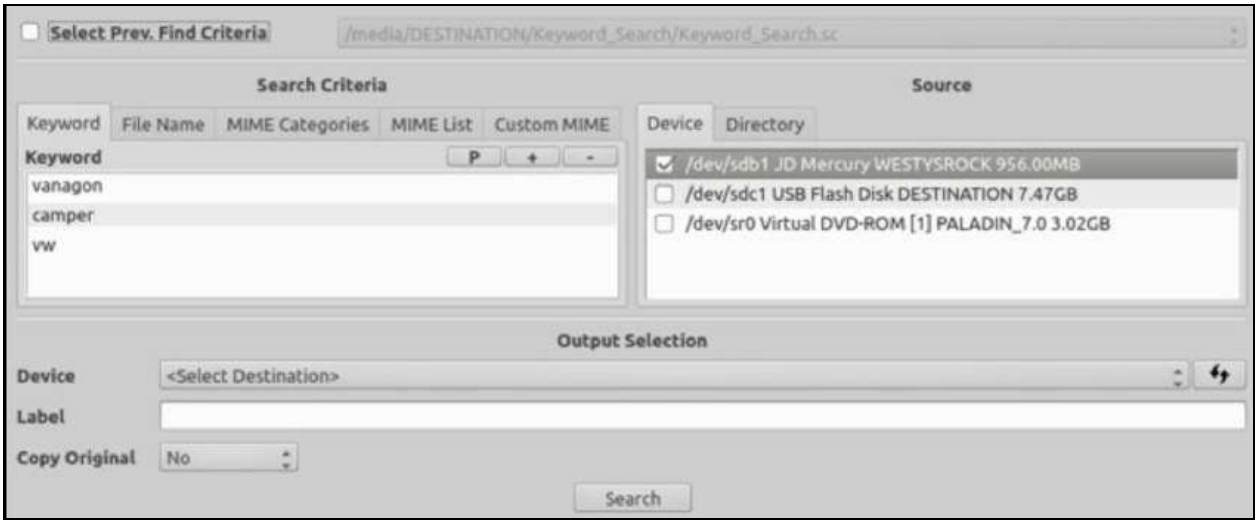
- **Device Tab** - Used to search full volumes.
- **Directory Tab** - Used to select single or multiple directories to search.




- **Device** - Select your Destination drive to store your 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 will be copied to your destination drive.

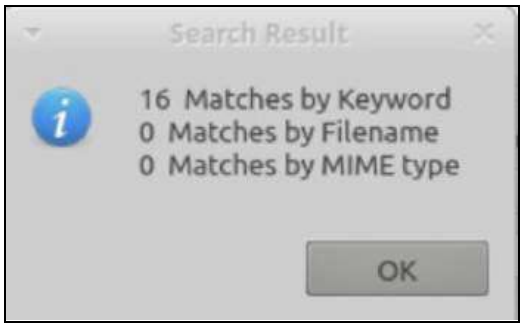
## Content Search

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



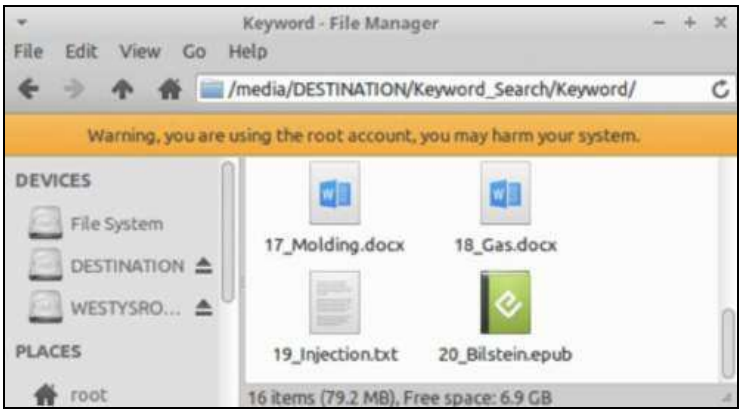

- Use the **“+” (plus) button in the Keyword** window to add keywords. To add multiple keywords all at once, use the clipboard to copy your single-spaced keyword list into the window with the “P” button. The example above is “vanagon”, “camper”, and “vw”.
- **Select the Device** or add directories to search. The volume /dev/sdb1 “WESTYSROCK” is used in this example.
- **Provide a “Label”** for your 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”** drop-down box.
- Click the **“Search”** button to begin your search.

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

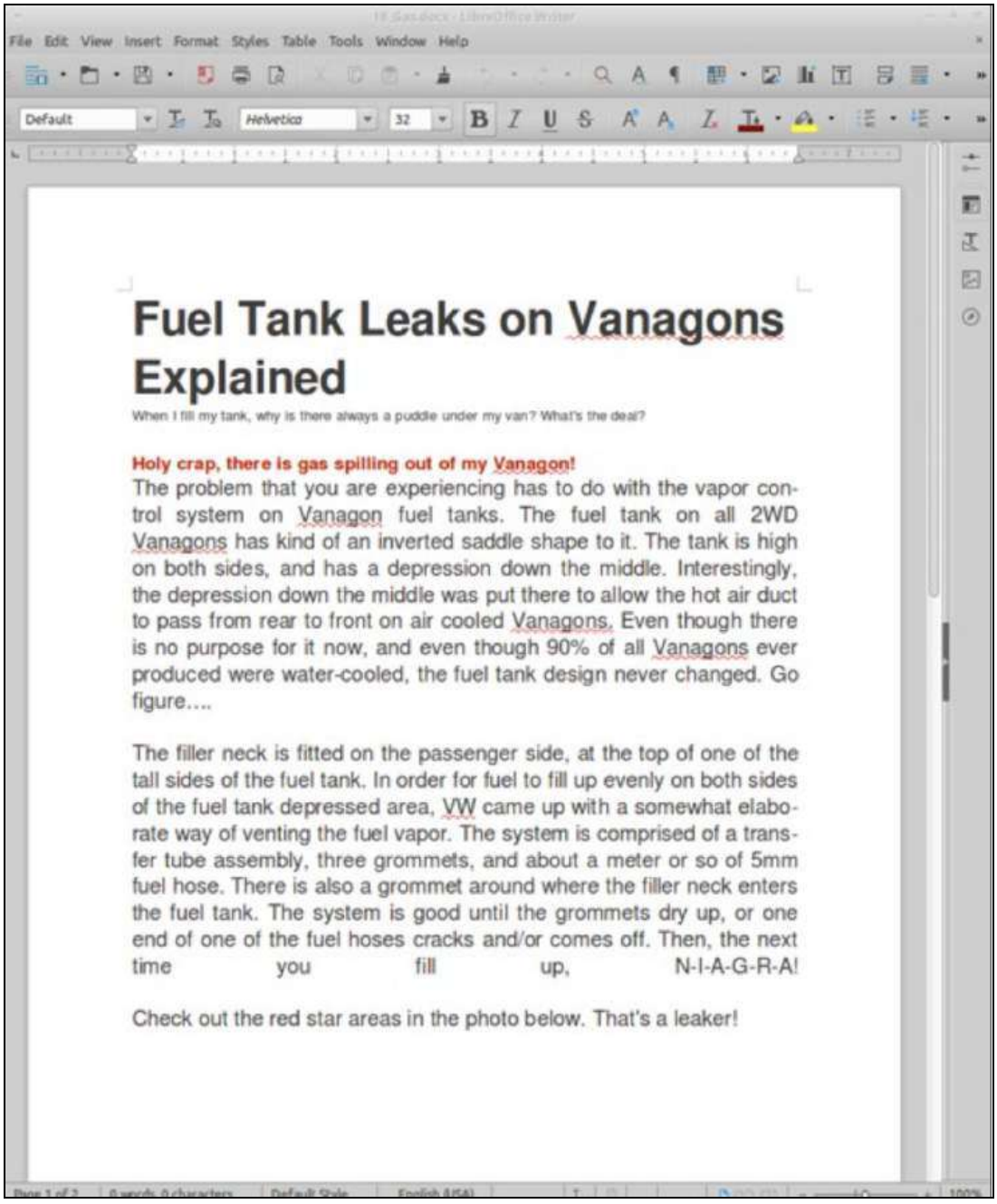




When the Find Result window appears, the search will be complete. Here, we see **“16 Matches by Keyword”**.

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

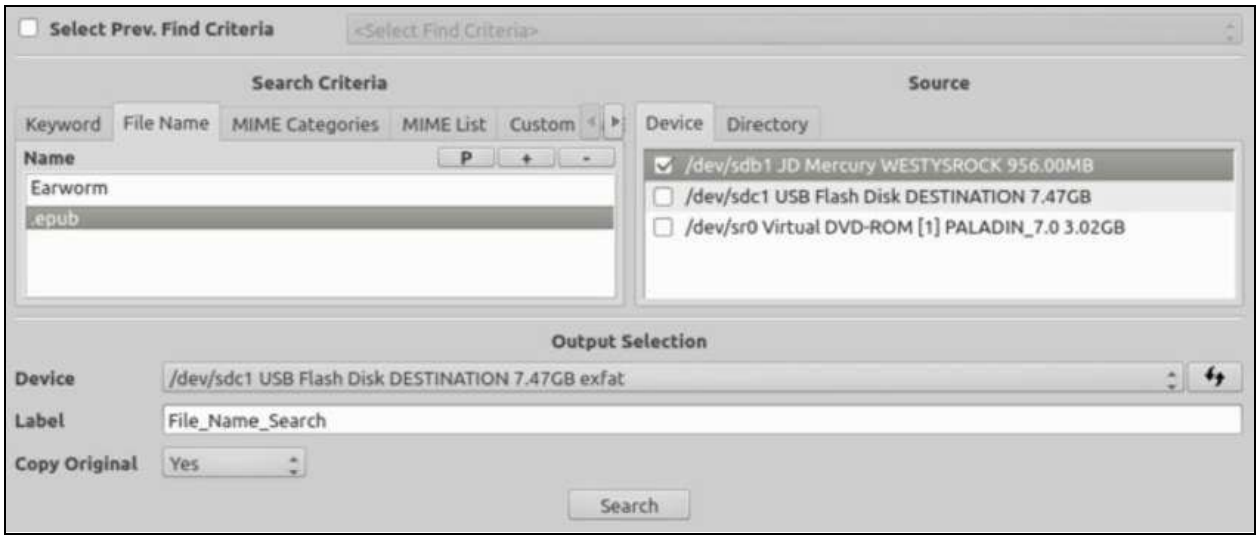


PALADIN includes multiple applications to open and view the files found. As seen below, “vanagon” was found inside the document.



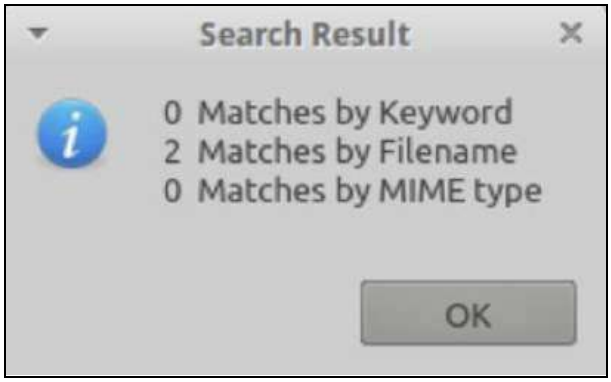
## Filename Search

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. The example above is “Earworm” and “.epub”.
- **Select the Device** or add directories to search. The volume /dev/sdb1 “WESTYSROCK” is used for this example.
- **Provide a “Label”** for your 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”** drop-down box.
- Click the **“Search”** button to begin your 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.

## 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 that identify file types have been built into PALADIN Find.

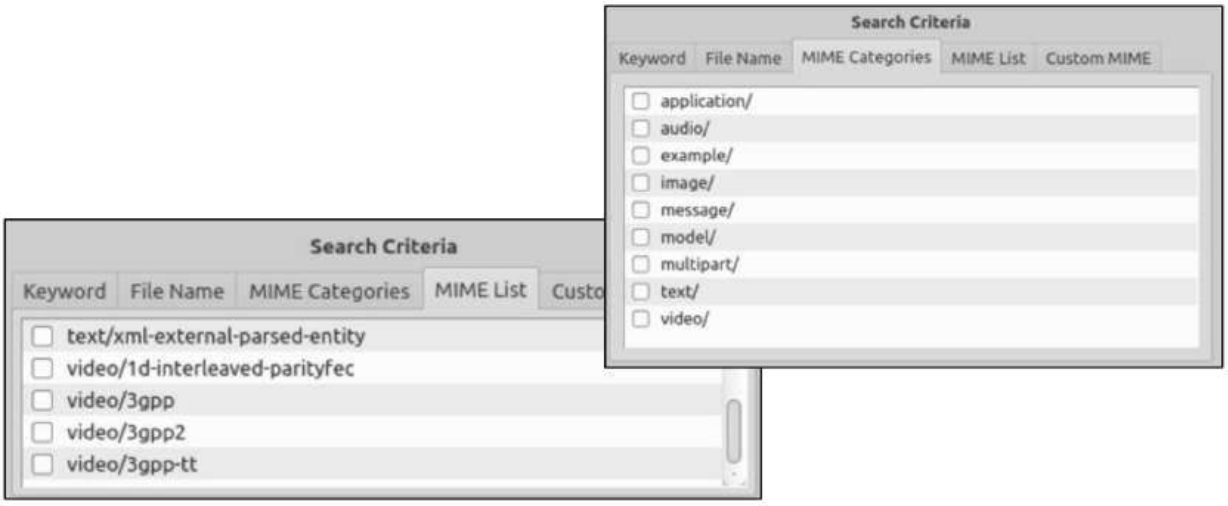
| File TYPE/S | MIME Code |
|---|---|
| JPEG Image | image/jpeg |
| Portable Document Format | application/pdf |
| MPEG-4 Video | video/mp4 |
| Find All Images | image/ |
| Find All Videos | video/ |

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

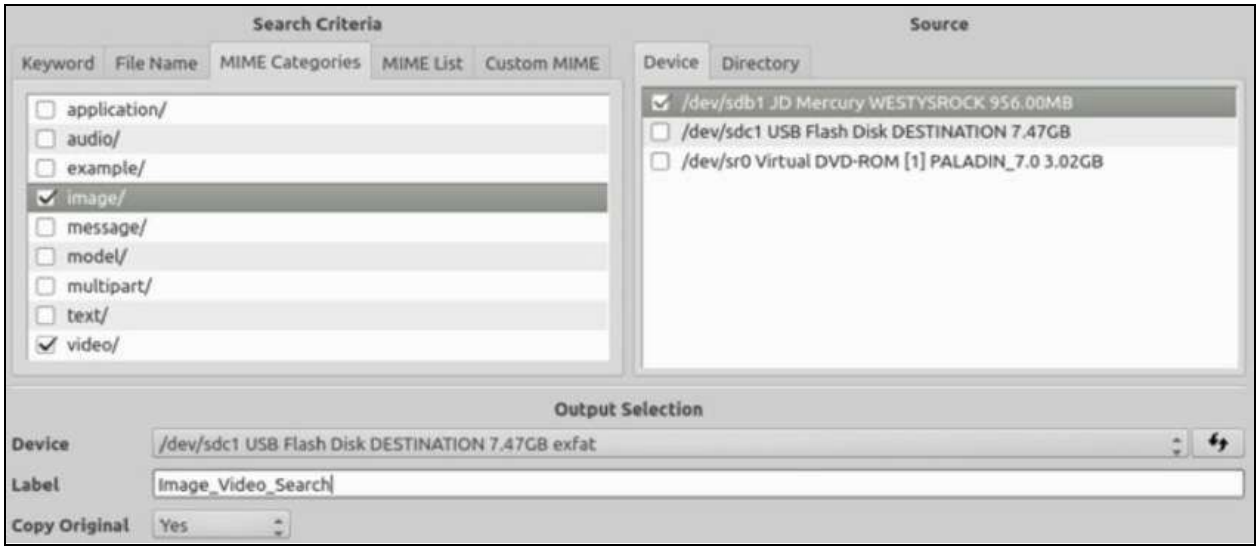
Several websites can be found that provide a list of MIME types.

We have included hundreds of MIME types in 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.

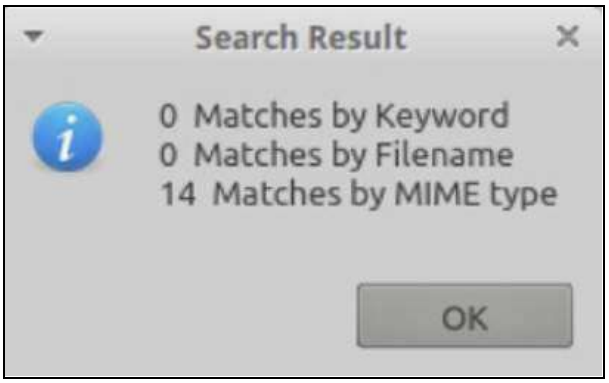


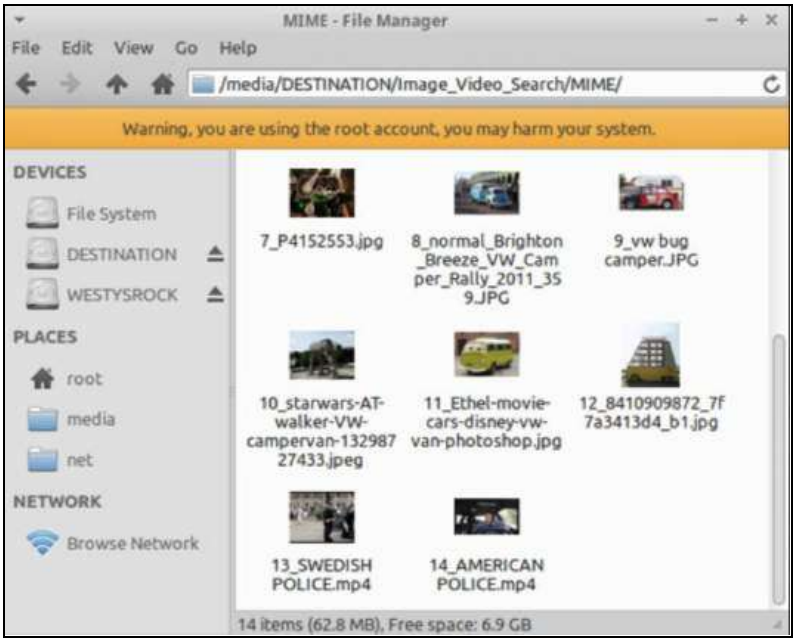
Example of a search based on MIME Categories for all Images and Videos.




- 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 in this example.
- **Provide a “Label”** for your 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.

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 that were provided.

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

## 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 previously saved searches is mounted with read-write privileges.

Click the box next to “Select Prev. Find Criteria”.

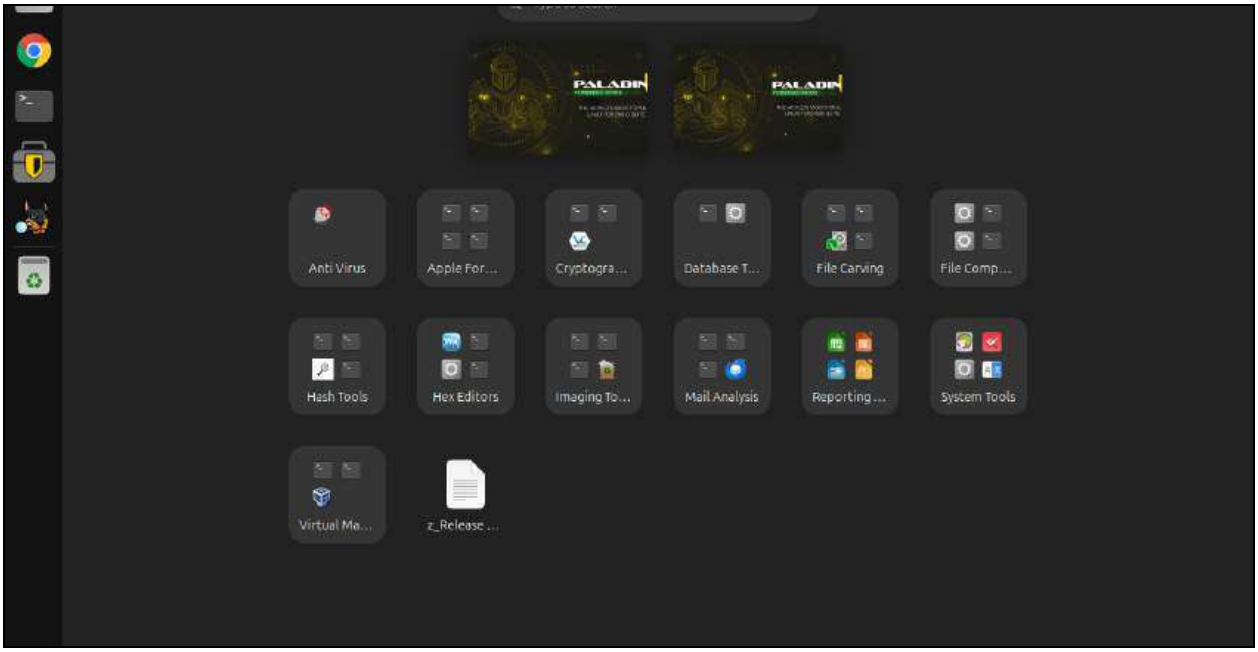
Once you have selected your previous search name, the keywords will automatically populate.

Edit the keywords or begin your search.

# Forensic Apps

PALADIN contains over a multitude of pre-compiled applications to assist with your forensic tasks, divided into various different categories. PALADIN is truly an all-in-one forensic suite!

The Forensic Apps can be accessed via the Activity Overlay by clicking the Shield Icon in the screen's bottom left corner on the sidebar. They can also be searched for or accessed by clicking the Windows Key or Apple Command Key on your keyboard to bring up the overlay and type your search terms.



## 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 that 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:

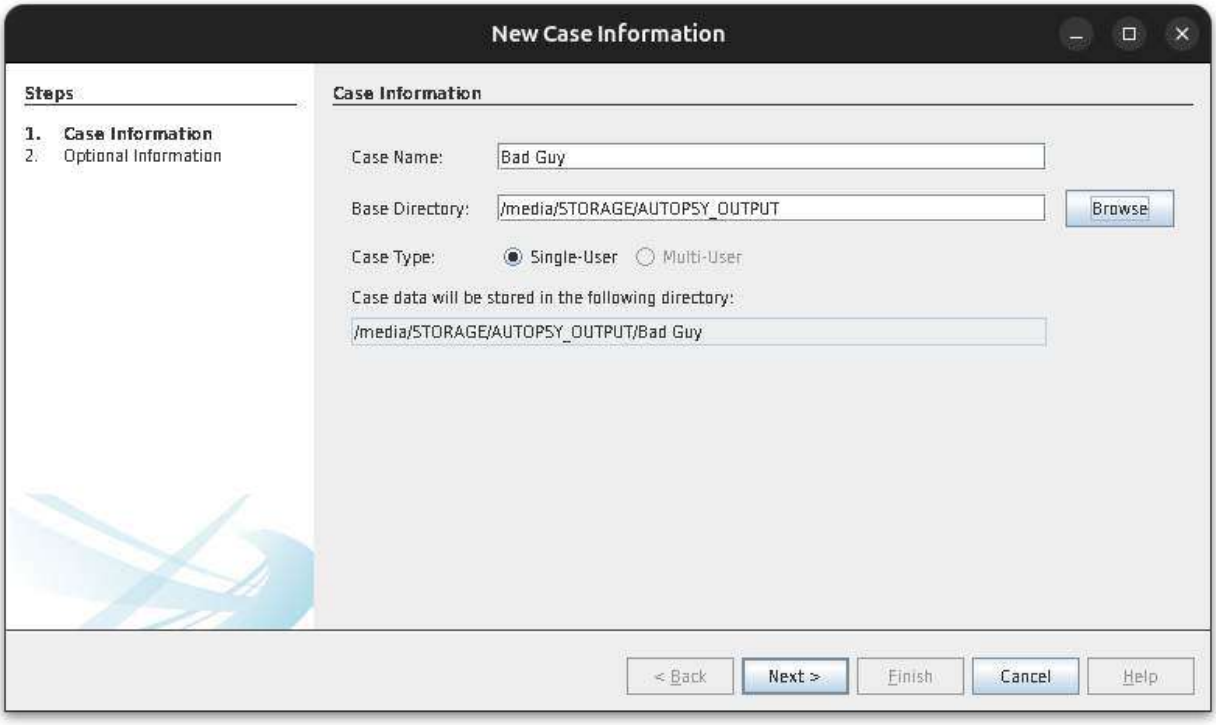
*"Autopsy® is the premier open-source digital forensics platform that has thousands of users worldwide. It has been developed by Basis Technology and an open-source community.*

*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.

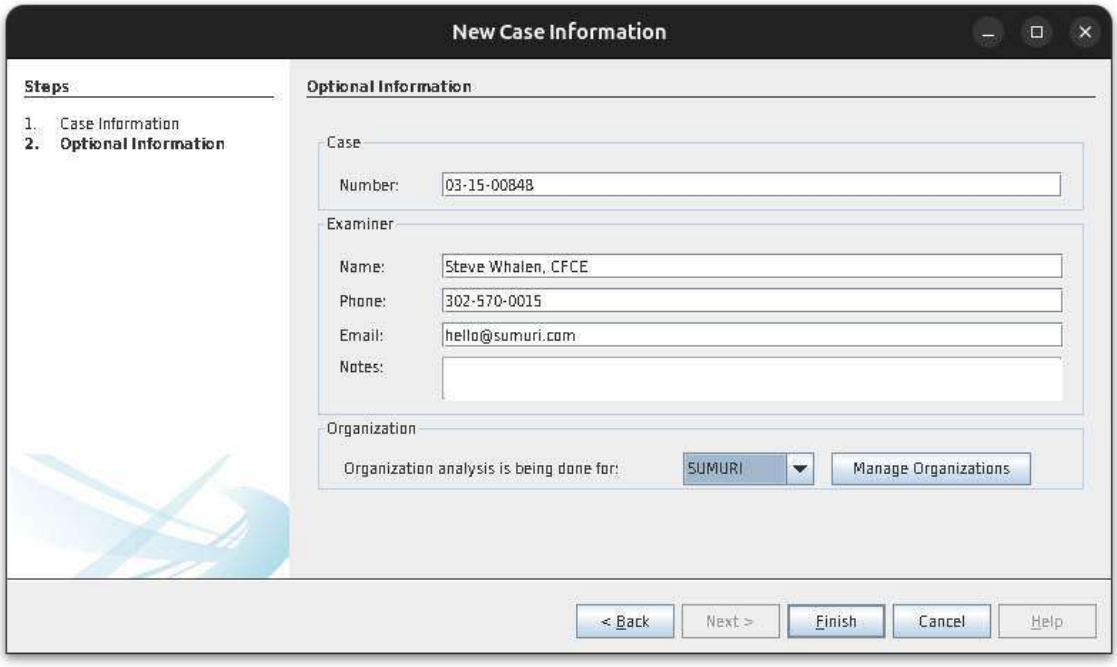

After imaging with PALADIN, start Autopsy and select "**New Case**".



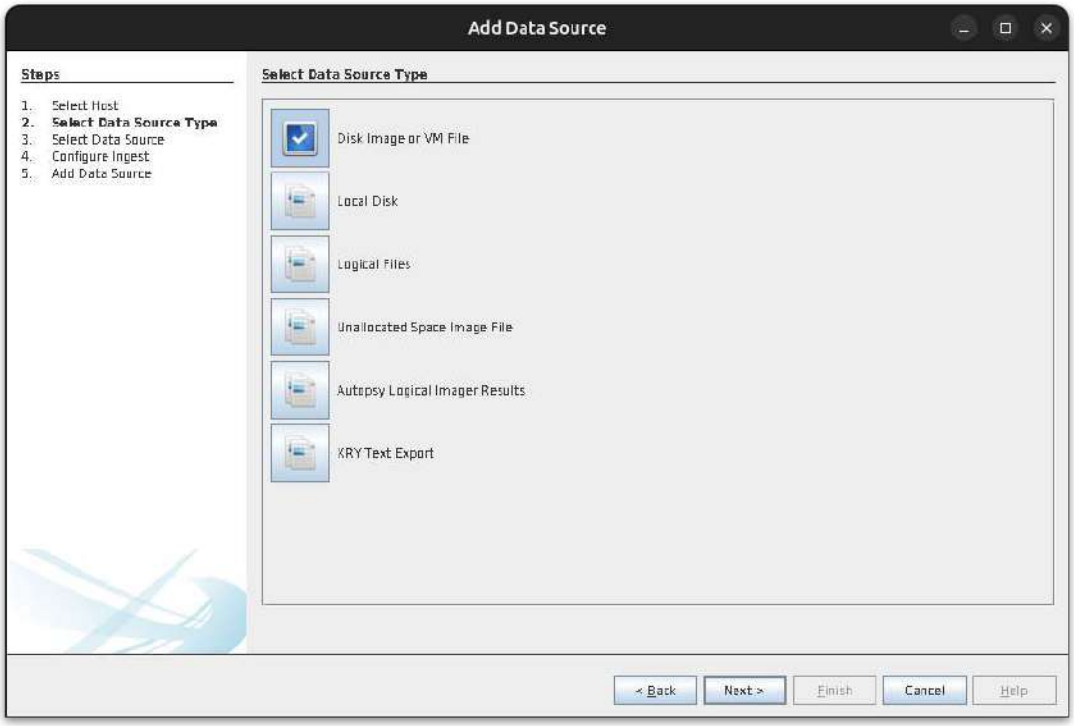

Enter a “Case Name” and select your **“Base Directory”** (it must be a drive that is mounted read-write) for output.

## Starting a Case

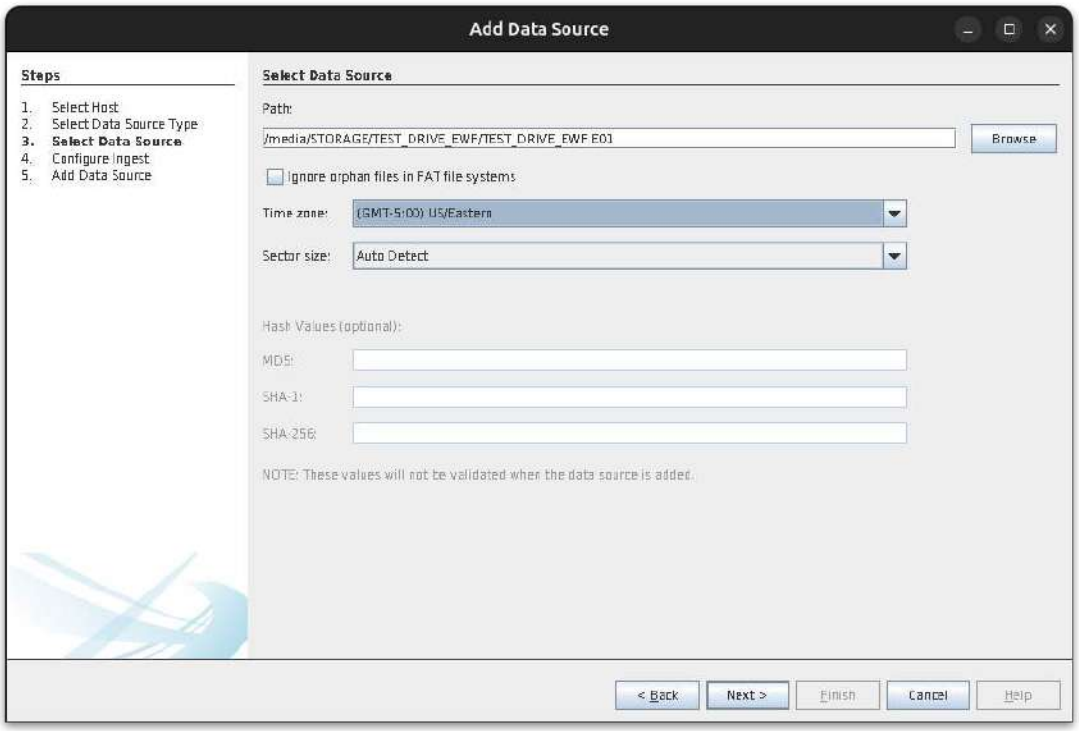
Add a “Case Number” and “Examiner” name.



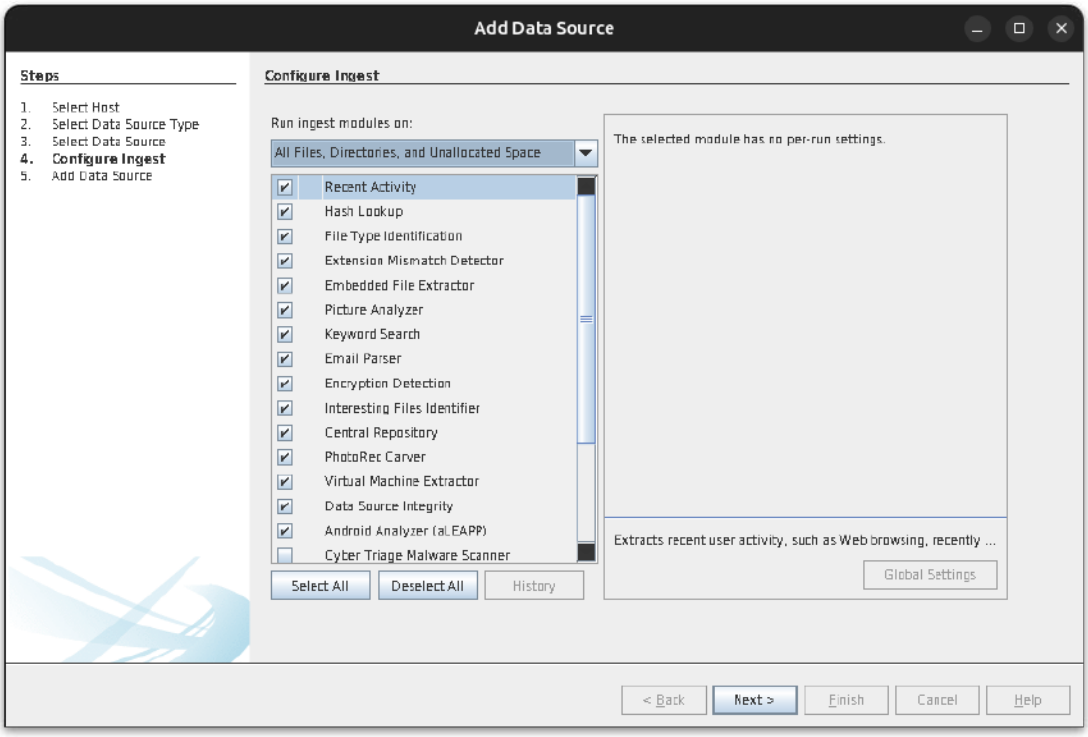

Next, select the type of image/source you will be using for your case.



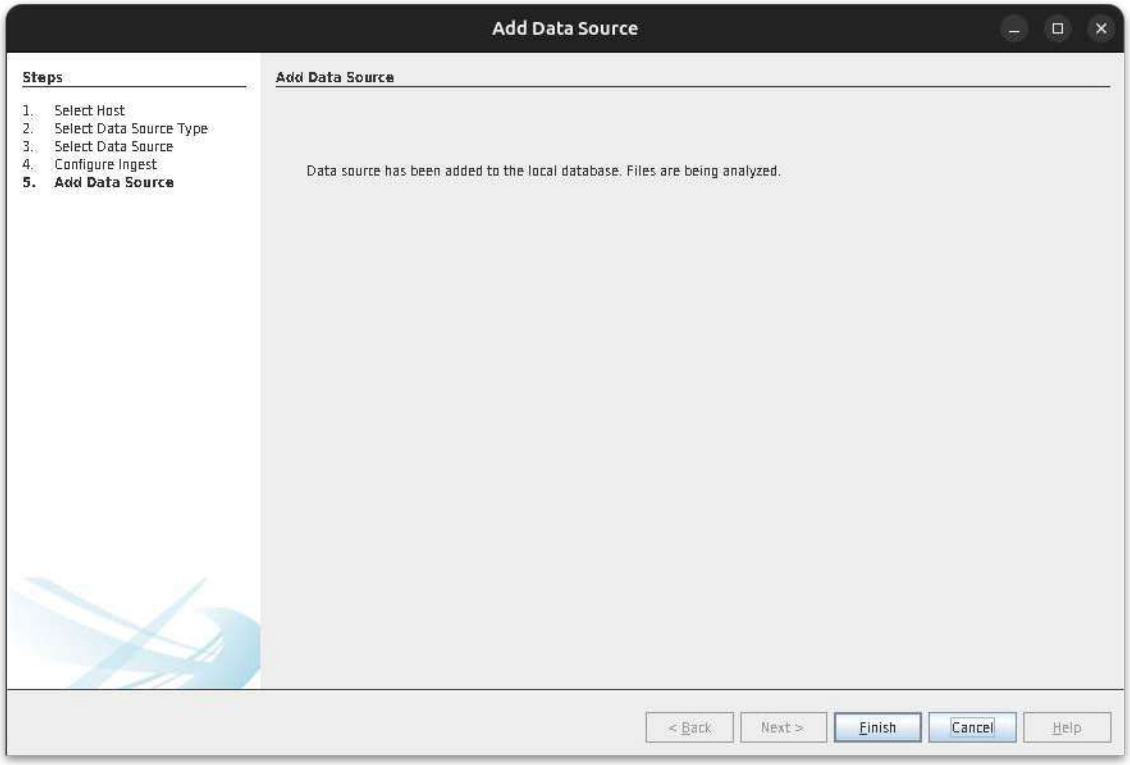
Select “Image File” for your source and navigate to the forensic image file.




Select and configure your “Ingest Modules”.

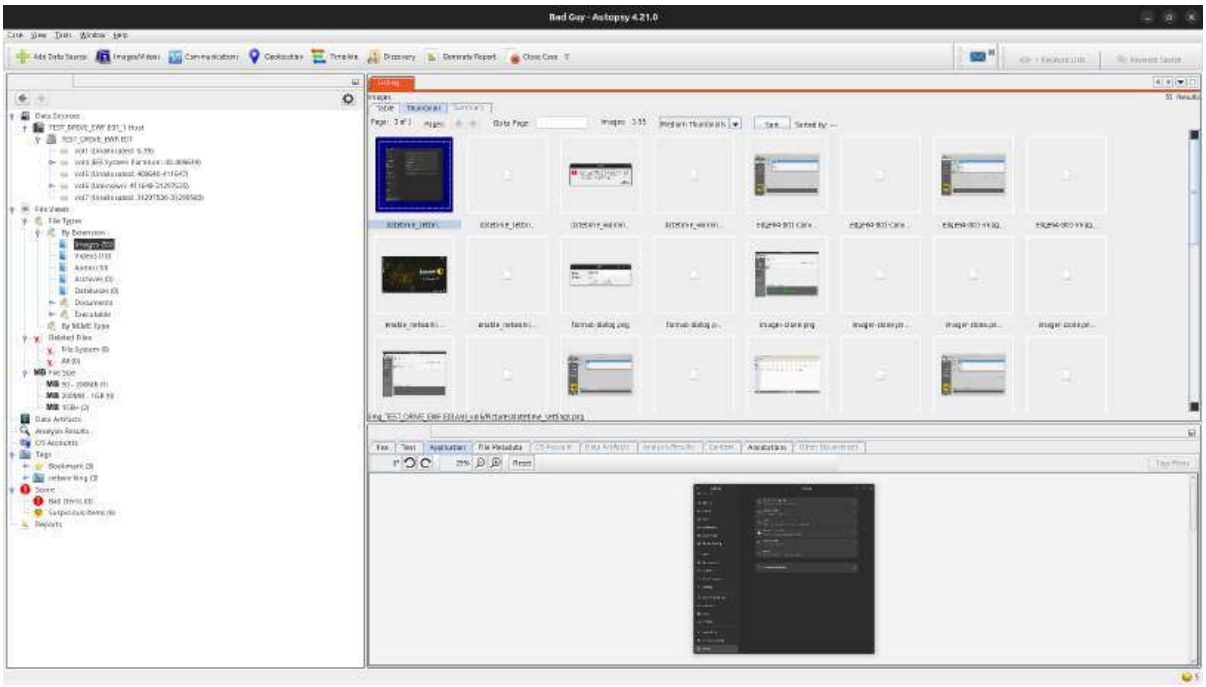


Click “Finish” to begin the processing.



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

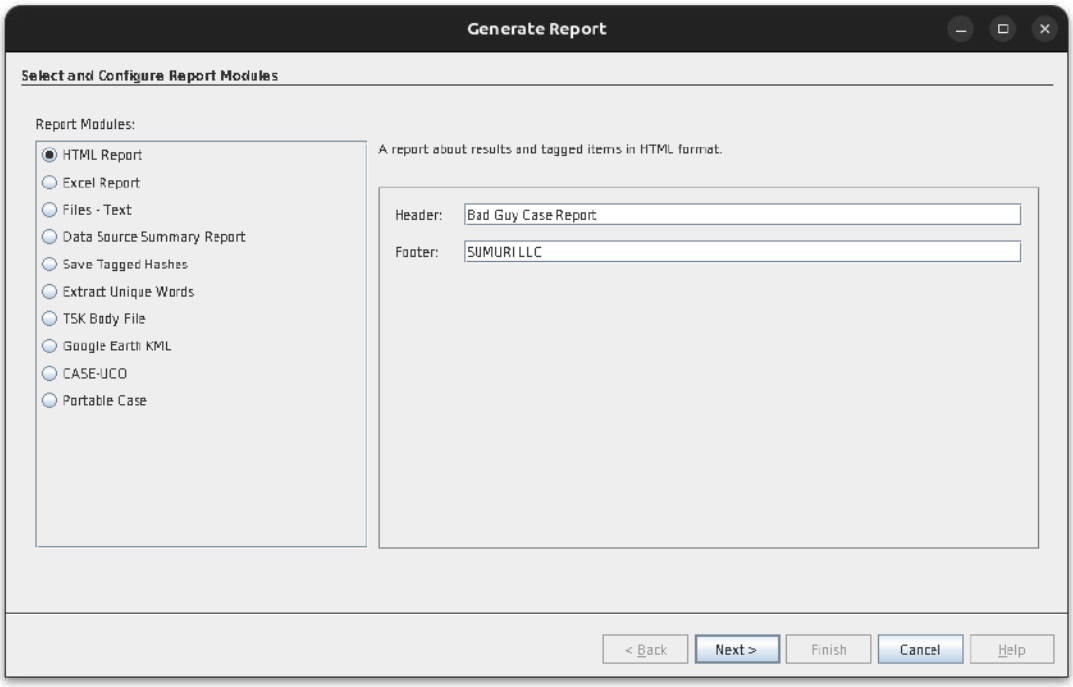
For official training on Autopsy, please contact Basis Technology (www.basistech.com).



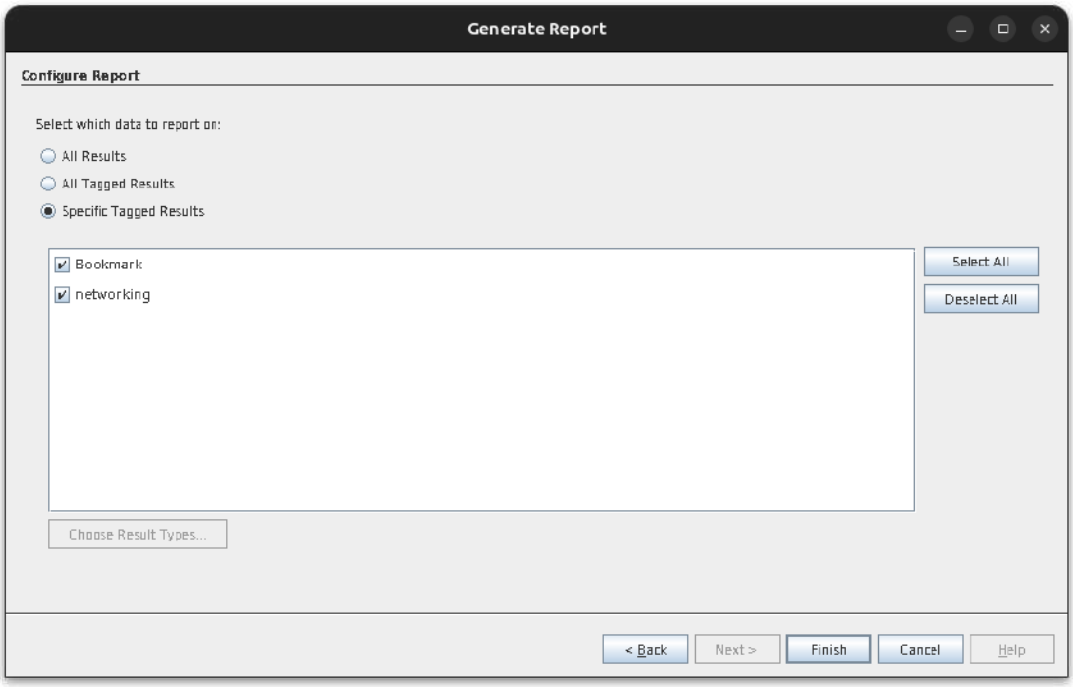

BASIS TECHNOLOGY

## Reporting

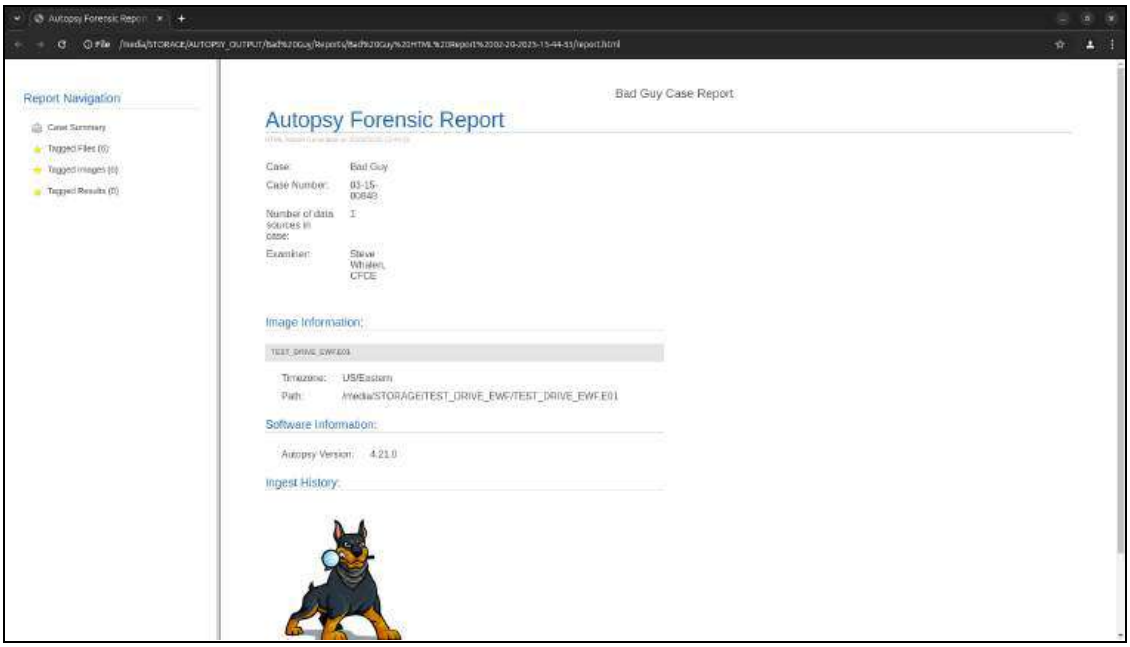
After tagging and bookmarking data, click the “Generate Report” button and select your report type.

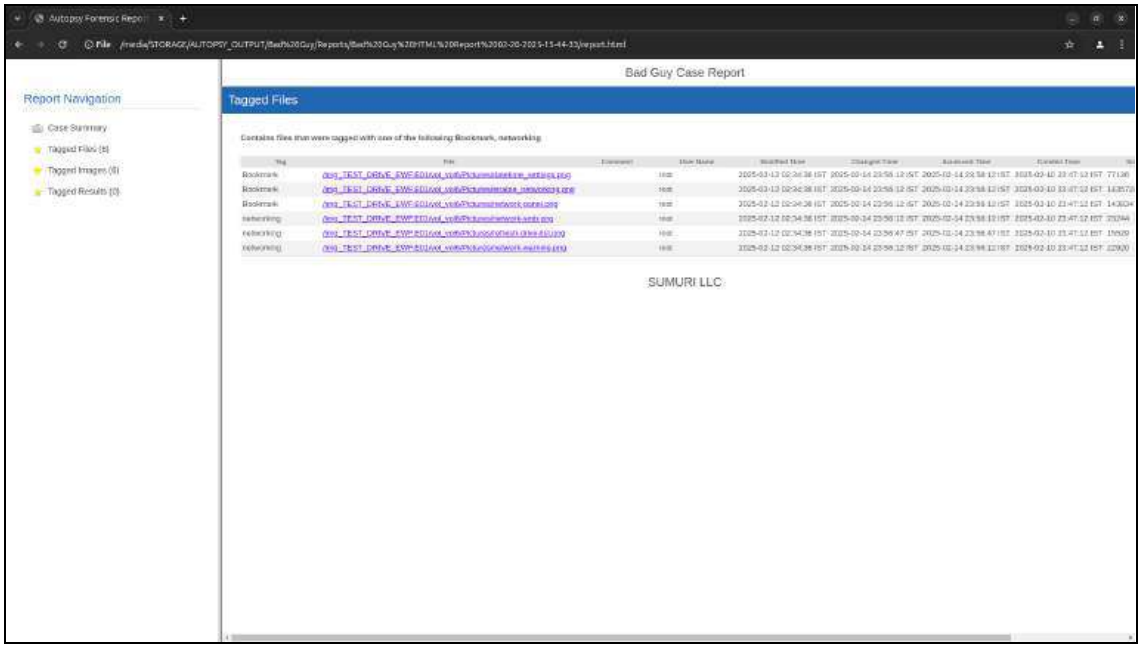



Select your artifacts to include in the report and click “Finish”.



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/