SUMURI

CARBON

MANUAL

SUMURI.COM

Table of Contents

1. Introduction

CARBON is a forensic virtualization application contained within a bootable forensic Linux distribution based on Ubuntu. CARBON is designed for both novice and advanced users.

CARBON has the ability to virtualize a Windows computer, bypass login credentials allowing access to a user's desktop for triaging and documentation without the need for imaging or disassembly.

CARBON can also virtualize a variety of forensic image formats and virtual hard disk formats in a forensically sound environment. This is done within a protected environment without making any changes to the image file or the host system.

CARBON contains automated plugins that can parse thousands of artifacts from popular Windows applications. Examiners can triage internal disks, disk images, or attached media that contains a Windows operating system with CARBON and get answers in seconds. Examiners have advanced reporting capabilities, which include the ability to capture screenshots and videos of the original user's system to make reports easier to understand for non-technical readers.

CARBON includes imaging and built-in write blocking for internal and attached devices with the PALADIN Toolbox.

1.1 Virtualization without Imaging

Virtualizing with CARBON gives the examiner the ability to view and create documentation of a user's desktop and stored data safely without the need for creating a forensic image which can take hours.

Virtualizing only takes minutes and an examiner can navigate the system without having to worry about altering the original data.

See **Section 15** for more information on how to virtualize a Windows computer.

1.2 Virtualization of a Forensic Image

CARBON allows users to create a virtual environment of most Windows computers that have been imaged using popular forensic formats without compromising the original data.

See **Section 15.1** for more information on how to virtualize a forensic image.

1.3 Snapshot Comparison - Differential Analysis

SnapCompare is a tool within CARBON that allows the examiner to compare a Windows environment from two different states of time using differential analysis.

SnapCompare will take a snapshot of the files currently on the Windows system being examined. It will then compare the file modified, accessed, and created (MAC) timestamps of a second snapshot from a different date to identify what has changed. The Snapshot Comparison feature of CARBON is perfect for incident response and malware analysis specialists. Examiners can easily study malware's effects on a system in a sandboxed environment.

See **Section 17** for more information on how to use SnapCompare within CARBON.

1.4 Triage of Windows Artifacts

CARBON has the ability to perform automated forensic analysis on Windows images and internal devices using RECON for Windows. Examiners can triage any internal disk, disk image, or attached media that contains an operating system.

CARBON supports Windows 7, Windows 8, and Windows 10 and includes over 40 automated plugins capable of recovering thousands of artifacts for quick and easy analysis.

See **Section 16** for more information on how to use RECON for Windows to triage Windows artifacts.

1.5 Advanced File Search

CARBON includes advanced search features. The examiner can create and save configuration files containing keywords allowing a search of media to be conducted by content, name, or file signatures.

See **Section 18** for detailed information about Advanced Search.

1.6 Data Carving

CARBON has built-in and customizable data carving capabilities.

Examiners can carve data from mounted volumes, the booted device, or added forensic images to locate deleted files using predefined or custom file signatures. Data can also be carved from the unallocated or physical space.

See **Section 19** for detailed information about Data Carving.

2. Recommended System Requirements

2.1 Hardware Requirements

As CARBON is a Linux distribution based on Ubuntu, CARBON can only run on hardware that Ubuntu supports. This includes most PCs and some Macs. Please refer to help.ubuntu.com to find additional information on supported hardware.

2.2 Supported Operating Systems and File Systems

CARBON supports a variety of common and uncommon file systems. However, for virtualization CARBON currently supports Windows 7 through Windows 10 operating systems.

3. Key Concepts to Understand

Before using CARBON, it is helpful to understand some key concepts.

3.1 What is Virtualization

Virtualization is the process of creating a representation of an operating system or file system in an environment using virtual hardware.

Examiners can use CARBON to create a forensically sound environment (virtual machine) and analyze internal disks or images by viewing the live environment without making changes to the original data.

3.2 Uses of Virtualization - Why Virtualize?

3.2.1 Seeing the Live Environment

Presenting evidence visually aids in comprehension as compared to traditional documentation and reporting.

CARBON's virtualization capabilities allow examiners to present their audience with exactly what the suspect sees and how the environment operates. Presenting information in this manner provides a more in-depth understanding of documented scenarios, which are easier for the audience to understand.

3.2.2 True Triage without Changes

CARBON has true triaging capabilities with RECON for Windows. Most other triaging tools require examiners to collect data and import it to a separate tool for analysis.

CARBON's triage capabilities let examiners get answers quickly by performing advanced analysis without having to export the data first.

RECON for Windows allows examiners to triage a Windows operating system and generate reports without making changes to the original data.

3.2.3 Malware Analysis

Malware is any malicious software designed to exploit or harm data on a computer that damages a computer. Malware varies in functionality from simple key loggers to ransomware that locks users out of their machines. Understanding how malicious software functions is important for examiners to recognize how malware may be impacting a device.

Virtualization is commonly used to analyze or examine malware in a secure environment that is isolated (sandboxed) from the host machine. Within a secure environment, an examiner can analyze how malware interacts with an infected machine.

Examiners using CARBON have the ability to learn what malware does to an infected computer in a safe and controlled virtual environment.

CARBON's snapshot comparison features allow an examiner to quickly identify changes made by malware.

3.3 What is a LINUX Bootable ISO

Linux is an open-source operating system that is highly customizable and able to run on various hardware. A bootable ISO contains all of the information needed to run an operating system in one file.

If an examiner's agency requires a pristine environment before starting every case, then a bootable ISO can help satisfy this requirement as the forensic environment is reset each time it is booted.

3.4 PALADIN

PALADIN is a modified “live” Linux distribution that simplifies various forensic tasks in a forensically sound environment. The CARBON application is included in PALADIN. PALADIN includes helpful forensic tools such as the PALADIN Toolbox which allows examiners to triage, image, search, and more with built-in open-source tools, write-blocking, and BitLocker decryption capabilities. Examiners can also analyze images using Autopsy, a full GUI forensic suite that is included with PALADIN.

PALADIN has its own manual, which can be found on the SUMURI website here: **https://sumuri.com/paladin-manual/**

3.5 Legacy BIOS Mode vs. UEFI BIOS Boot Mode

The BIOS and UEFI are firmware that is used to assist in the startup operations of a computer.

Legacy BIOS Boot Mode - The traditional booting process typically used by systems prior to Windows 8.

UEFI Boot Mode - The current mainstream boot mode and successor of Legacy BIOS that includes better performance and higher security.

Depending on hardware configurations, examiners may need to enable the Legacy Boot Mode in order to see CARBON as a boot option.

In order to start CARBON, a few settings in each computer’s BIOS/UEFI may need to be changed:

- Disabling Secure Boot
- Enabling Virtualization
- Changing the boot order to prioritize CARBON

Note: BIOS Keys, BIOS/UEFI Setup Utility interfaces, and Boot Menu interfaces will differ based on the machine’s motherboard manufacturer.

3.5.1 Secure Boot

Secure Boot is a security feature found in most modern computers that only allows a computer to start using software trusted by the PC manufacturer. The examiner will need to disable Secure Boot within the BIOS/UEFI in order to boot CARBON successfully.

If Secure Boot is enabled within the BIOS/UEFI, the examiner will not be able to boot into CARBON.

- To disable Secure Boot, access the **BIOS/UEFI Setup Utility** by pressing the motherboard manufacturer's BIOS/UEFI Key on startup.
- Navigate to the **Security** menu.
- Select **Secure Boot**, click **Disable**, and **Save**.

3.5.2 Enabling Virtualization

After disabling Secure Boot, ensure that the Virtualization settings are Enabled in the BIOS/UEFI Virtualization settings. If Virtualization is disabled, the examiner cannot use CARBON virtualization capabilities.

3.5.3 Boot Order

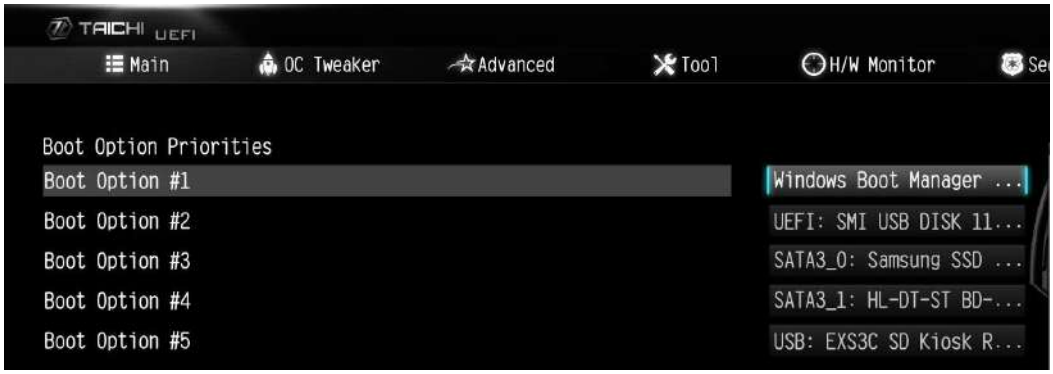
There are two ways to boot to CARBON successfully:

1. Change the Boot Order in the BIOS/UEFI
2. Access the Boot Menu during Start-Up.

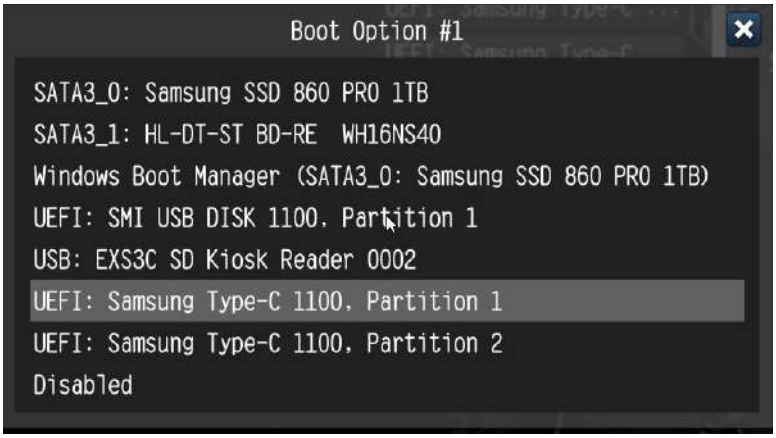
3.5.3.1 Changing the Boot Order in the BIOS/UEFI

Examiners can change the BIOS/UEFI's boot order to alter the sequence of how the motherboard loads bootable media. Altering the boot order to set the CARBON USB as the first boot option will allow the examiner to boot CARBON automatically when powered-on.

If CARBON is not the first boot option, the machine will automatically load the installed operating system, as the screenshot below indicates.



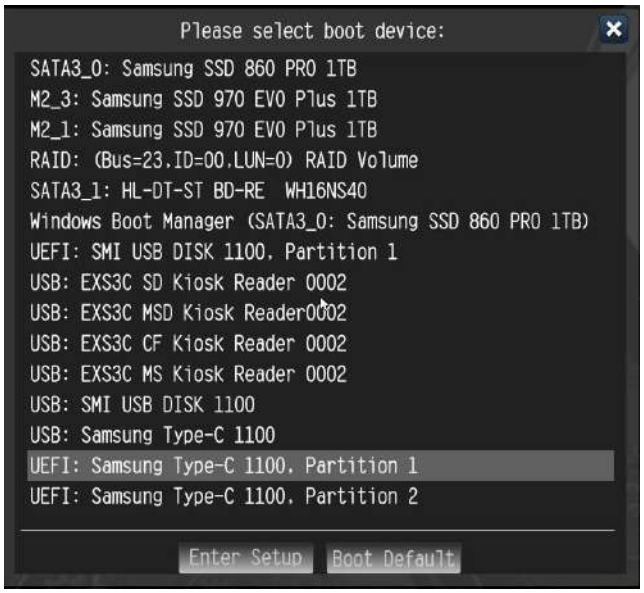
To change the boot order, navigate to the BIOS/UEFI **Boot** section.



Select **Boot Option #1** and change it to the USB device containing CARBON. Once changed, the computer will automatically boot to CARBON when the computer is powered on.

3.5.3.2 Accessing the Boot Menu Upon Startup

The Boot Menu is typically accessed by pressing the motherboard manufacturer's BIOS/UEFI key and allows for one-time overrides of the boot order. Once the examiner



is in the Boot Menu, select the USB containing CARBON. Once selected the machine will automatically boot CARBON.

3.6 Bitlocker

BitLocker is a Windows full volume encryption feature that can be decrypted using a Password or Recovery Key.

The CARBON forensic suite has the ability to virtualize either the image or volume containing BitLocker. CARBON identifies BitLocker volumes that will prompt the examiner with a window for the Password or Recovery Key. Entering the BitLocker key or password will allow CARBON to continue virtualizing the image or volume.

4. Getting Support

Support for CARBON is available via our Online Support site where you can submit a ticket. The ticket allows us to track your support request until it is solved.

https://helpdesk.sumuri.com/

During regular business hours, we strive to respond in less than one hour but no longer than 24 hours.

SUMURI is based in the state of Delaware, USA (Eastern Time Zone – EST/EDT).

Our office hours are 0900-1700 (9 AM – 5 PM). SUMURI is closed for US Federal Holidays.

For comments or feature requests, please email us at:

hello@sumuri.com

Law Enforcement Emergency Support

If you are law enforcement and are in need of immediate emergency assistance with any of our products, please contact us anytime at +1 302.570.0015.

5. Renewing CARBON

CARBON comes with one full year of support and updates. Once CARBON expires, its license will need to be renewed in order to continue to receive updates and support.

https://sumuri.com/product/carbon-vfs-renewal/

Click the **About CARBON** button in CARBON's Main Interface to find the expiration date. For more information, see **Section 9.1**.

5.1 Downloading CARBON Updates

CARBON updates can be found here:

https://sumuri.awsapps.com/workdocs/index.html#/share/document/9121e9463a137279c02f12dbf8cf59e79e379bf08ce3695e3f62f487ca5f78f2

To ensure that our customers can always access updates, we have alternative links for all downloads.

Download from this alternative link if the primary link is unavailable.

http://gofile.me/5dMCE/NJbmrqF6I

5.2 Updating CARBON

To properly update CARBON, please follow the steps below:

1. Download the latest version of CARBON from the link above.
2. Delete the old CARBON.iso from the root of the CARBON drive.
3. Copy the new CARBON.iso file to the root of the CARBON drive.
4. Once booted into the CARBON environment, confirm that the version number has been updated in the About CARBON section. See **Section 9.1** for information on where to locate the About CARBON menu.

5.2.1 Updating the CARBON Grub Configuration

For examiners with version 4.0.3 or older of CARBON, follow the steps below to properly update CARBON on PALADIN PRO:

1. Download the latest version of CARBON from the link above.
2. The Google Drive Link will contain a folder that says CARBON Update Guide. Navigate to that folder.
3. Download the file that says grub.fg.
4. Delete the old CARBON.iso from the root of the CARBON drive.
5. Copy the new carbon-paladin.iso to the root of the CARBON drive.
6. Navigate to the following directories and replace the grub.cfg file:
    a. boot > grub
    b. boot > grub > i386-pc
    c. boot > grub > 86_64-efi
7. Once booted into the CARBON environment, confirm that the version number has been updated in the About CARBON section. See **Section 9.1** for information on where to locate the About CARBON menu.

These instructions only need to be done once--when updated once, the examiner does not need to follow these steps again.

6. Booting CARBON

CARBON presents the following boot options:

- CARBON-PALADIN – Forensic Mode
- CARBON-PALADIN – Forensic Mode (nomodeset)
- CARBON-PALADIN – Forensic Mode (acpi=off)
- CARBON-PALADIN – Non-Forensic Mode
- CARBON-PALADIN – Non-Forensic Mode (nomodeset)
- CARBON-PALADIN – Non-Forensic Mode (acpi=off)
- PALADIN EDGE 64 - Forensic Mode -64 bit

- PALADIN EDGE 64 - Forensic Mode -64 bit (nomodeset)
- PALADIN EDGE 64 - Forensic Mode -64 bit (acpi=off)
- PALADIN EDGE 64 - Non-Forensic Mode -64 bit
- PALADIN EDGE 64 - Non-Forensic Mode -64 bit (nomodeset)
- PALADIN EDGE 64 - Non-Forensic Mode -64 bit (acpi=off)
- PALADIN EDGE 32 - Forensic Mode - 32-bit

Forensic Mode – A forensically sound environment that does not mount internal drives, attached media, or swap files with networking disabled. Once booted, the mounting of devices is controlled by the PALADIN Toolbox or the CARBON Device Manager.

Non-Forensic Mode – Not forensically sound with networking disabled. Booting to non-forensic mode allows mounting and writing to internal drives, attached media, or swap files as normal.

(nomodeset) - This setting can help when encountering video issues when attempting to boot CARBON.

(acpi=off) - Advanced Configuration and Power Interface is a standard that is used for power management. Some older systems may not support ACPI, so disabling it can help boot older systems.

7. Desktop Layout

Upon starting CARBON, the examiner will be presented with the desktop and dock.

The dock displays shortcuts for:

CARBON Forensics Suite — CARBON allows examiners to virtualize computers or forensic images, has Snapshot Comparison capabilities, data carving, advanced search, and Windows triage tools.

PALADIN Toolbox — The PALADIN Toolbox is included with CARBON Forensic Suite. PALADIN Toolbox simplifies and combines a majority of basic and advanced forensic tasks into a simple-to-use graphical user interface.

PALADIN QuickStart Guide — A PDF that contains the links for the PALADIN Manual and CARBON Manual.

Autopsy — Autopsy is included as a part of CARBON and allows examiners to image, virtualize, and analyze all in the same tool.

Open-Source Tools — A suite of over 100 pre-installed open-source forensic tools.

Google Chrome — Chrome Chrome is included in CARBON to review reports in HTML format and access the Internet when networking is enabled.

Terminal — Allows the examiner quick access to a command-line interface.

Screenshot — Allows examiners to document their findings with a built-in screenshot tool.

Mounted Media — Allows for quick access to any mounted volumes.

7.1 Start Menu

CARBON uses XFCE Desktop for fast and light navigation. Click on the **App Menu** to search for installed applications or select categories on the right.

For the examiner's convenience, some quick links to useful applications have been provided.

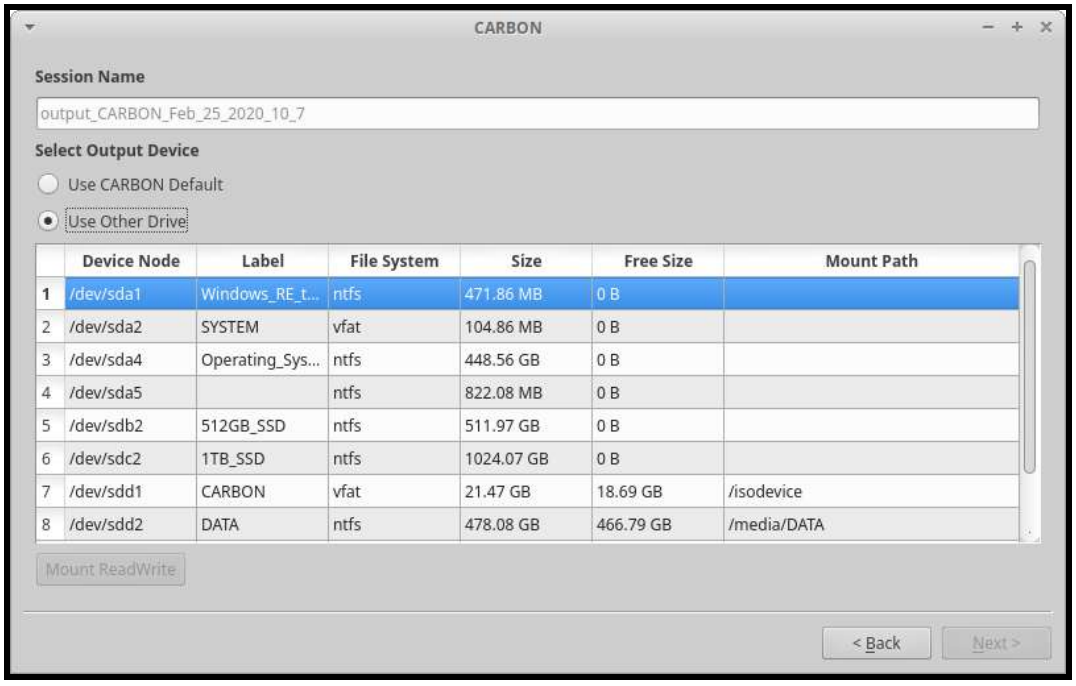
- **RecordMyDesktop** — Allows the examiner to record a video of the desktop or specific window and save it as a .ogv file
- **Web Browser** — Opens Google Chrome
- **File Manager** — Opens the file manager application to browse the file system
- **LibreOffice Writer** — A word processor that allows the examiner to create and edit text and graphics in letters, reports, documents, and web pages
- **LibreOffice Calc** — A spreadsheet that allows the examiner to perform calculations, analyze information, and manage lists
- **Terminal Emulator** - Opens the command line
- **Screenshots** - Allows the examiner to take screen captures of the desktop or specific window and save a .png file

7.2 Shutting Down CARBON

To shut down CARBON, click the **Power Button** in the upper right-hand corner of the App Menu.

8. Starting the CARBON Application

To begin, click the CARBON application icon in the dock.

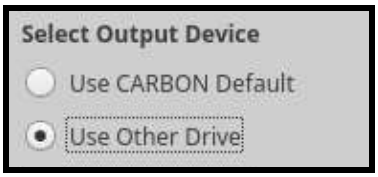


	Device Node	Label	File System	Size	Free Size	Mount Path
1	/dev/sda1	Windows_RE_t...	ntfs	471.86 MB	0 B	
2	/dev/sda2	SYSTEM	vfat	104.86 MB	0 B	
3	/dev/sda4	Operating_Sys...	ntfs	448.56 GB	0 B	
4	/dev/sda5		ntfs	822.08 MB	0 B	
5	/dev/sdb2	512GB_SSD	ntfs	511.97 GB	0 B	
6	/dev/sdc2	1TB_SSD	ntfs	1024.07 GB	0 B	
7	/dev/sdd1	CARBON	vfat	21.47 GB	18.69 GB	/isodevice
8	/dev/sdd2	DATA	ntfs	478.08 GB	466.79 GB	/media/DATA

Examiners can choose to use the default **Session Name** created by CARBON or input a custom Session Name. In the example above, the default Session Name's naming convention starts with "output_CARBON" followed by the date and time.

8.1 Setting the Cache Drive (NTFS, default, external)

Examiners can choose to **Use CARBON Default** to output the case folder to the Data Partition of the CARBON drive or select **Use Other Drive** to choose an attached device as an output device.

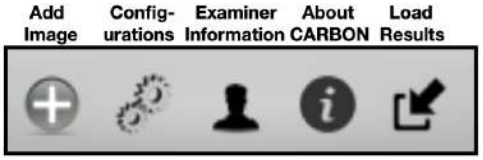


Note: Before processing, make sure that the output drive has enough free space. For more information about Attached Media, see ***Section 12****.*

After selecting the output device, click **Next**, and a message window will appear as in the screenshot below. Click **Launch CARBON** when ready.

Note: If the examiner has a demo license for CARBON and wants to use a created PALADIN USB, add the demo license on a separate drive and select the drive with the CARBON license as the Output Device.

9. CARBON Main Interface

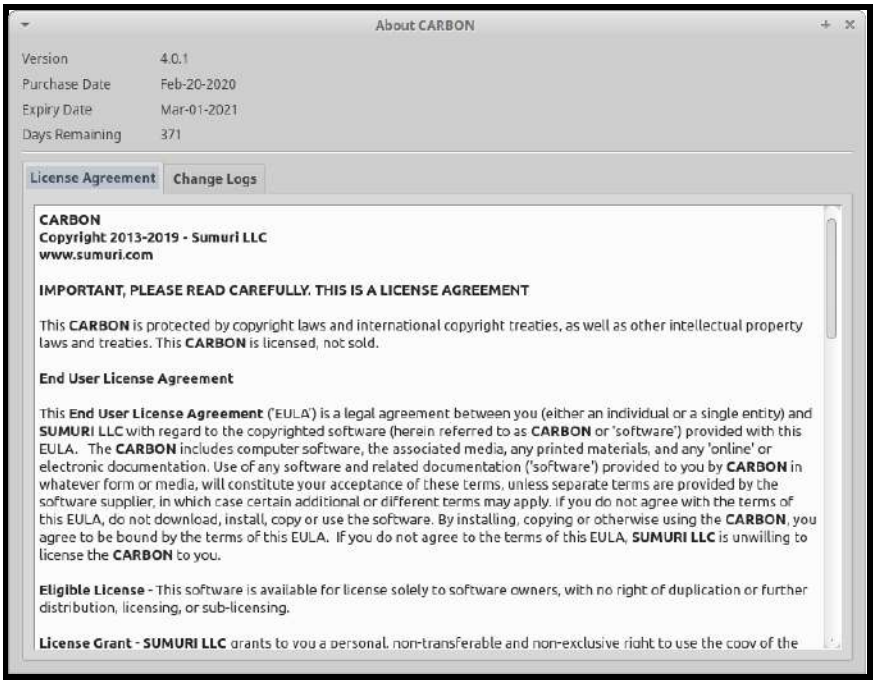


9.1 About CARBON

The **About CARBON** icon lists will show the Version number, Purchase and Expiration dates, and the number of days remaining until the license expires when selected.

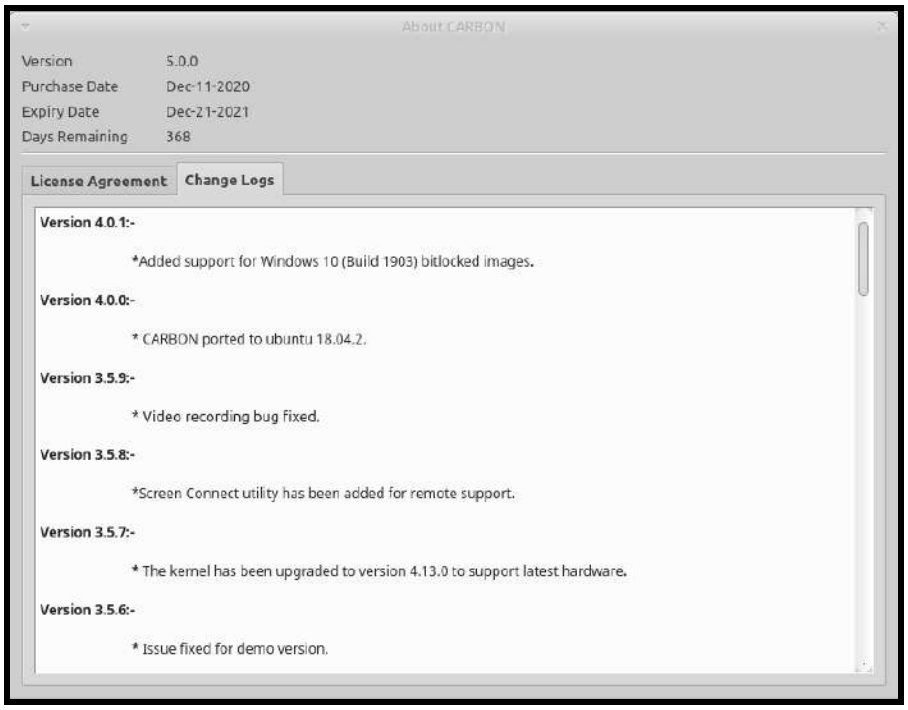
9.1.1 License Agreement

The License Agreement tab displays the End User License Agreement (EULA) which can also be found in **Section 20**.



9.1.2 Change Logs

Click on **Change Logs** for a description of the changes and updates made with each newly released version of CARBON.

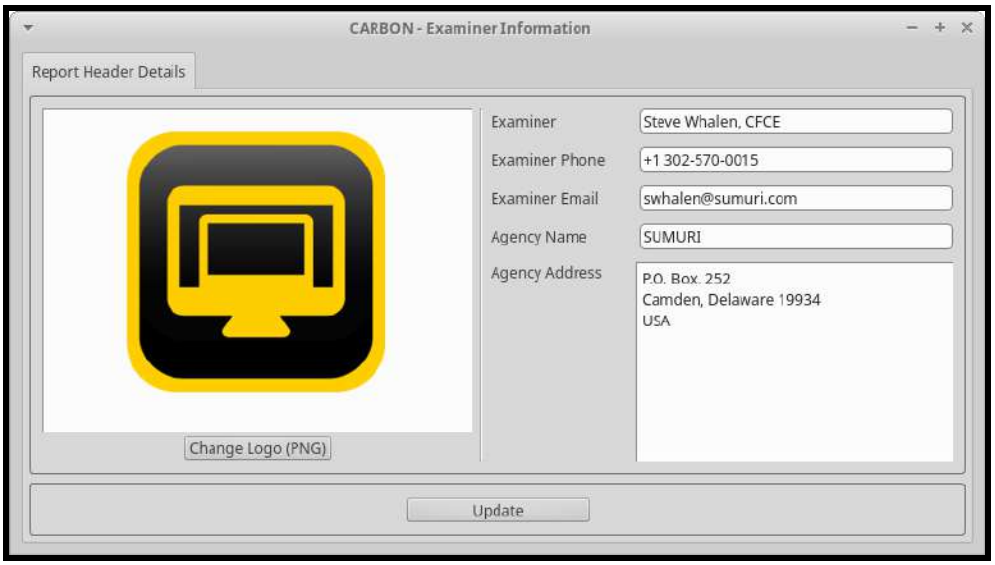


10. Adding Examiner Information

Examiner Information can be entered by selecting the Examiner Information icon in the Toolbar. Details entered here will auto-populate in CARBON where applicable.

When the Examiner Information window appears, an agency logo and examiner details can be added.

Fill in the appropriate information and click **Update**.



11. Search and Carving Configuration

File Search and Data Carving configuration files must be created before using these features in CARBON.

File Search Configuration - Allows examiners to add and edit unique records to search for File Names, Keywords, File Signatures, and Custom File Signatures.

File Signature for Carver - Allows examiners to add or edit the file signature records for Data Carving

When clicking on the **CARBON - Configuration** button, it automatically opens to the File Search Configuration window.

11.1 Loading a Configuration File

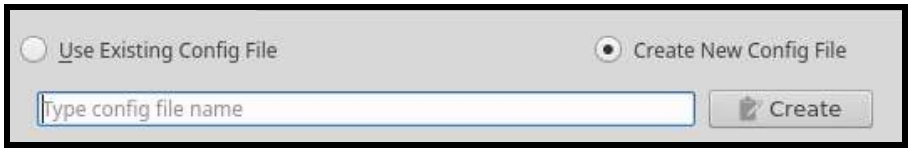
Loading a configuration file is the same process for both the File Search Configuration and File Signature for Carver windows.

Select **Use Existing Config File** to access or load a configuration file.

The dropdown menu will automatically show the examiner's previously created configuration files and allow the examiner to edit them in the window.

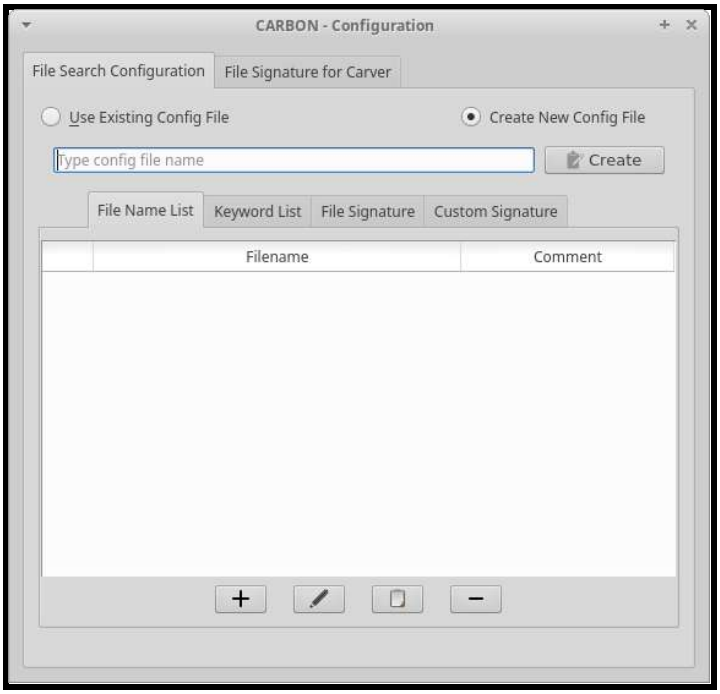
11.2 Creating a Configuration File

Creating a new configuration file is the same process in both of the File Search Configuration and File Signature for Carver windows.



Select **Create New Config File**, type in a configuration file name, and click **Create** to create a new configuration file for File Searches or File Signatures for Carver.

11.2.1 File Search

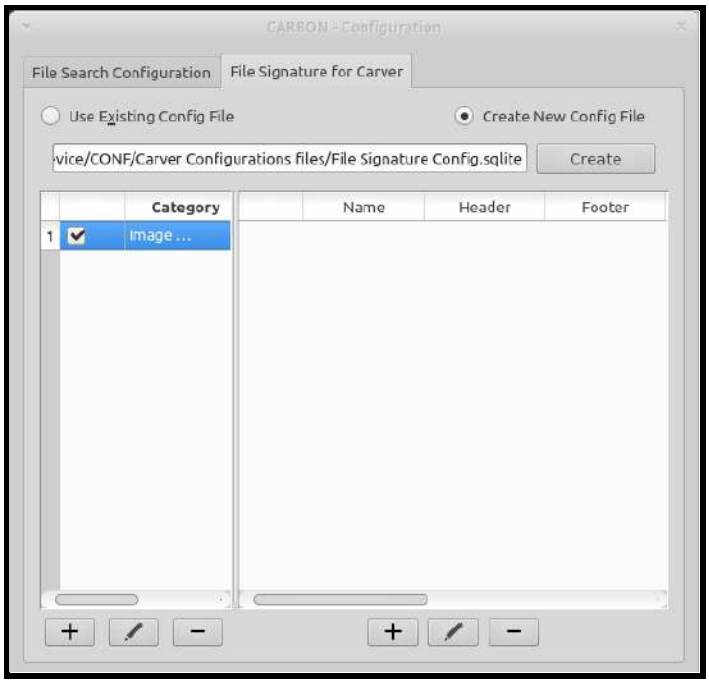


Add, edit, and delete new records for File Searching.

- **Plus icon** — add new records to search for
- **Pencil icon** — edit created records
- **Clipboard icon** — choose specific files and make records for all of their contents
- **Minus icon** — deletes records no longer needed

11.2.2 File Carving

Navigate to the **File Signature for Carver** to add configuration parameters for Data Carving.

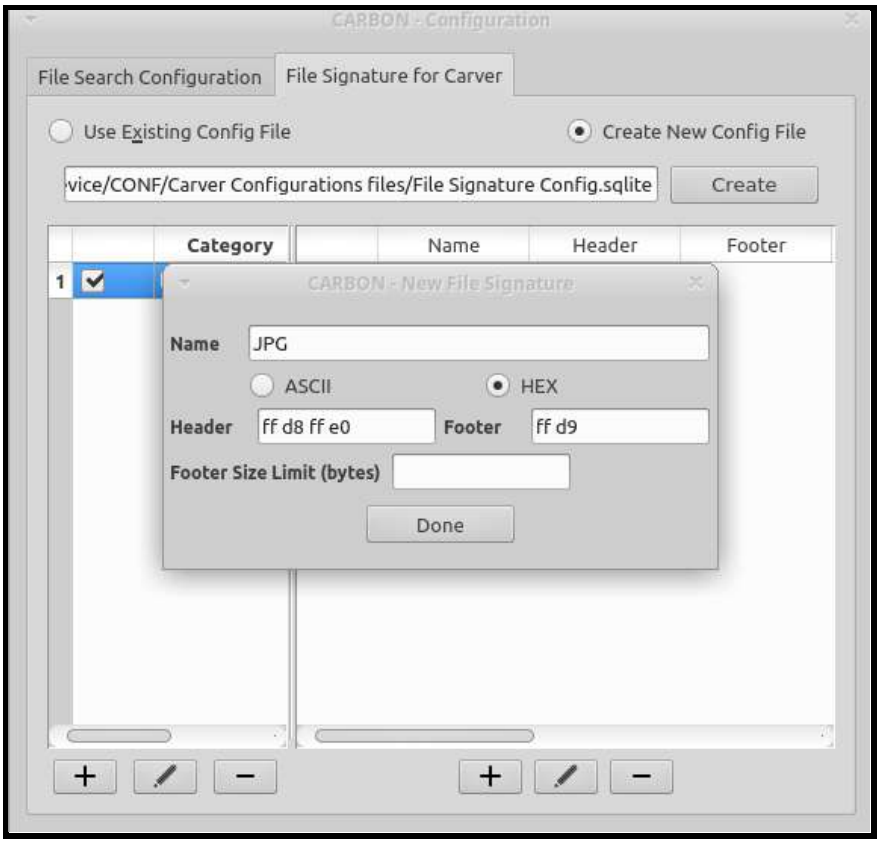


In the **File Signature for Carver** tab:

- **Plus icon** — create a new category.
- **Pencil icon** — to edit the name of a selected category.
- **Minus icon** — to delete a selected category.

After selecting the category, click the **Plus icon** on the right side of the window to add a new file signature.

Add a File Signature **Name**, **Header**, **Footer**, and **Footer Size Limit (bytes)**. The screenshot below displays creating a New File Signature with a JPG, the Header, the and Footer, and as HEX.



File Signatures can be added in either ASCII or Hex format.

12. Mounting Attached Media or Internal Drives

The default forensic mode for CARBON protects both internal and external drives and media. If you want to process a forensic image or virtual disk image of a hard drive the examiner must first mount the volume containing those images.

Two methods of mounting internal and external drives are the PALADIN Toolbox (may be more familiar to some examiners) or the Attached Media window via CARBON's Main Interface.

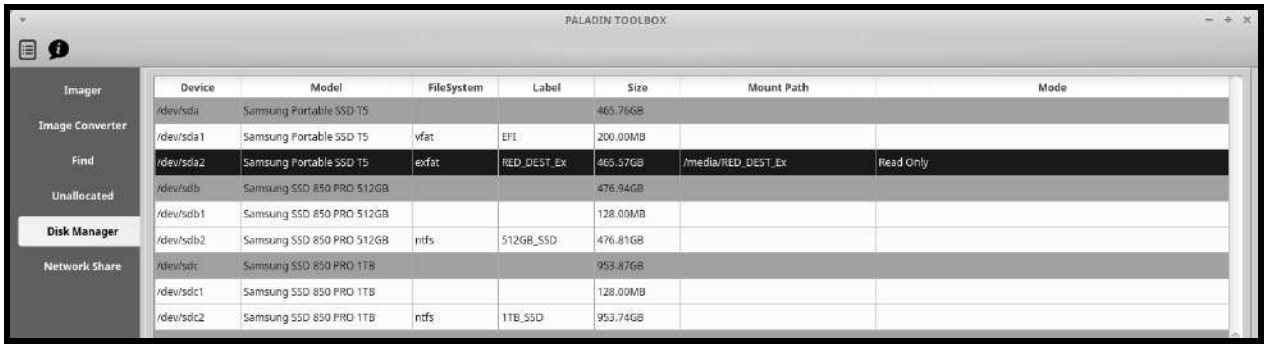
Examiners have two options for mounting drives:

- **Mount RW** - mounts the drive as Read-Write and allows changes to the drive. This is ideal for outputting to destination drives or interacting with CARBON's interface.
- **Mount R** - mount the drive as Read-Only to ensure that there are no changes to the data. This is ideal for attaching evidence drives for virtualization and triage.

12.1 Mounting Using the PALADIN Toolbox

Click the **PALADIN Toolbox** shortcut on the Dock.

Select **Disk Manager** to see information on all the connected drives and click on the desired partition.

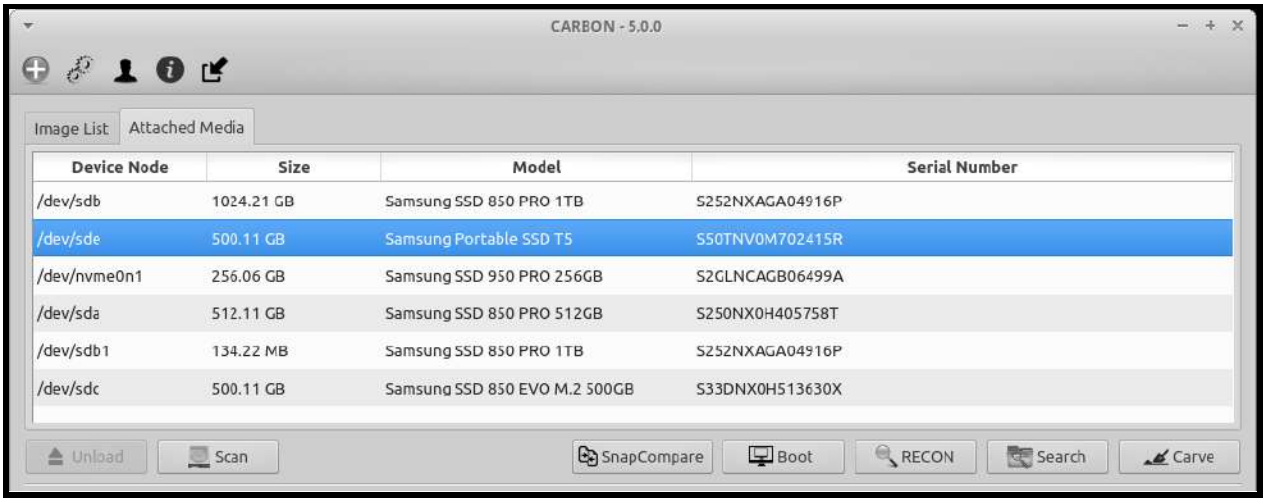


Choose either Read-Write or Read-Only depending on your preference.

12.2 Mounting Using CARBON

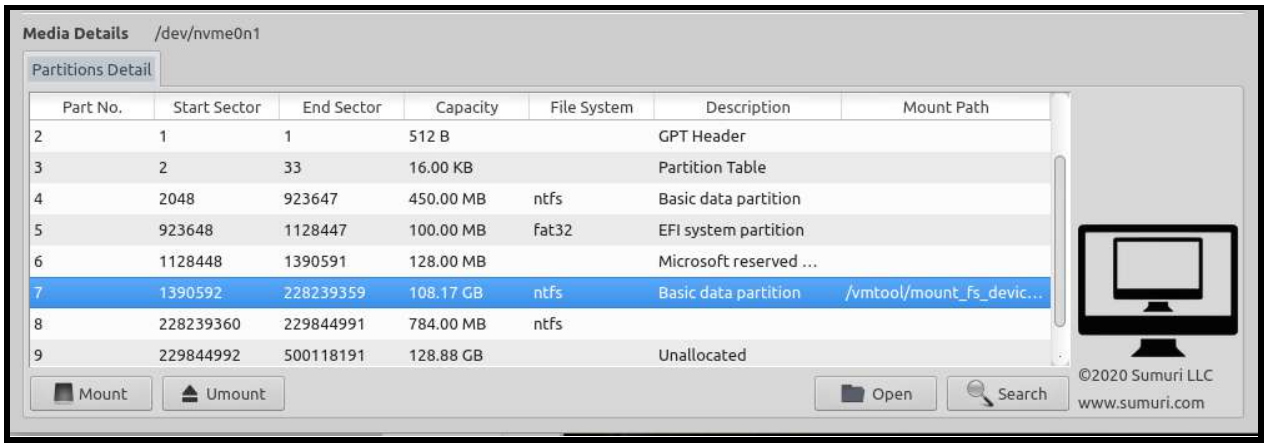
Click on the **CARBON** application, and the CARBON Main Interface will open.

Select the **Attached Media** tab at the top of the window as shown in the screenshot below.



Select the **Scan** button to detect any media attached to the device.

When selecting a drive, the **Partition Details** tab will display information about the selected drive.



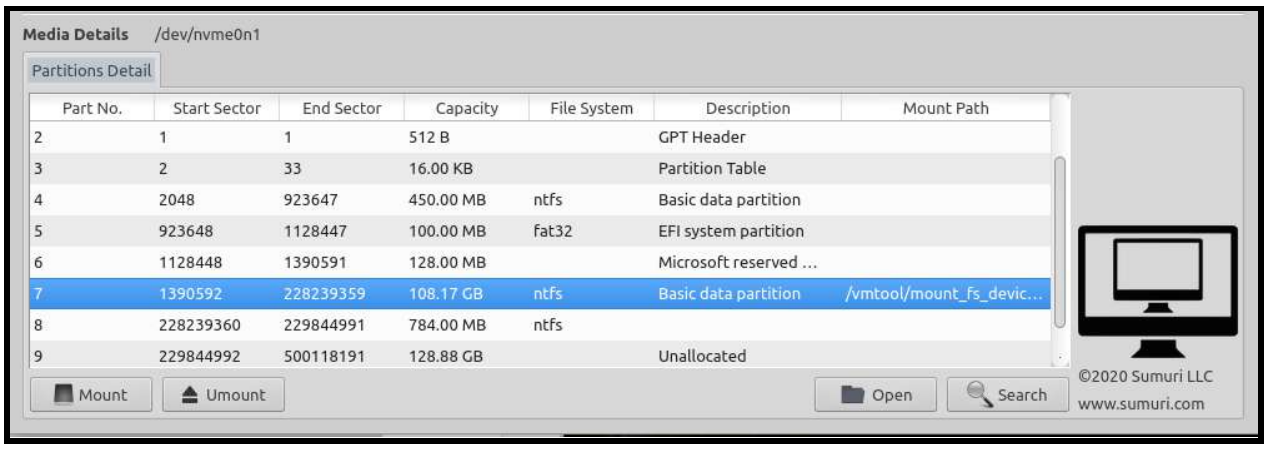
13. Partition Details

The Partition Details tab allows examiners to view details based on the selected source.

CARBON has four options available for viewing Partition Details:

- **Mount** - Mounts the drive as Read-Write
- **Unmount** - Unmounts the previously mounted drive
- **Open** - Opens the selected previously mounted partition to browse its contents
- **Search** - Allows the examiner to perform a search of individual partitions of the drive

The screenshot below displays the Partition Details of the Basic data partition with its Mount Path.

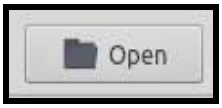


13.1 Mounting a Partition

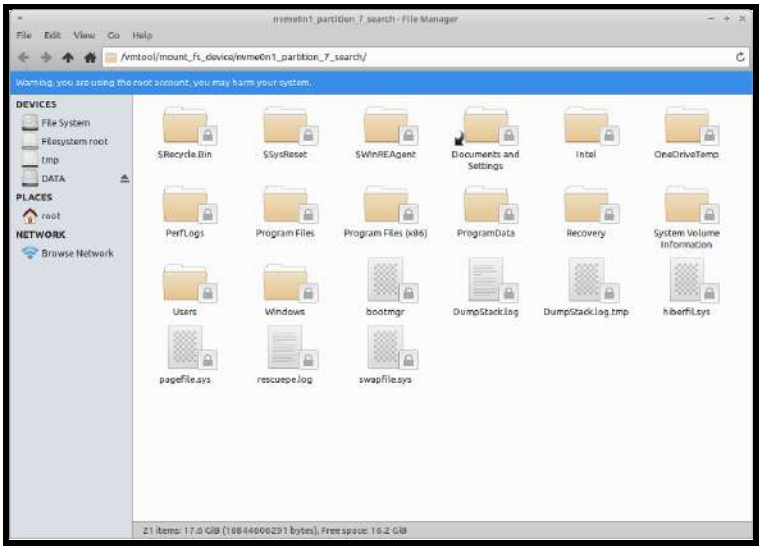
Select the desired partition and click **Mount** to mount a drive as Read-Only which does not allow the examiner to make changes to the partition and its contents.

13.1.1 Opening a Partition

Select a previously mounted partition and click **Open**.



The File Browser window will open to allow the examiner to browse the mounted partition file contents.



13.2 Search a Partition

Click the **Search** button to activate the File Search interface to search individual

partitions of the selected partition.

For more information on how to use File Search, please see ***Section 19****.*

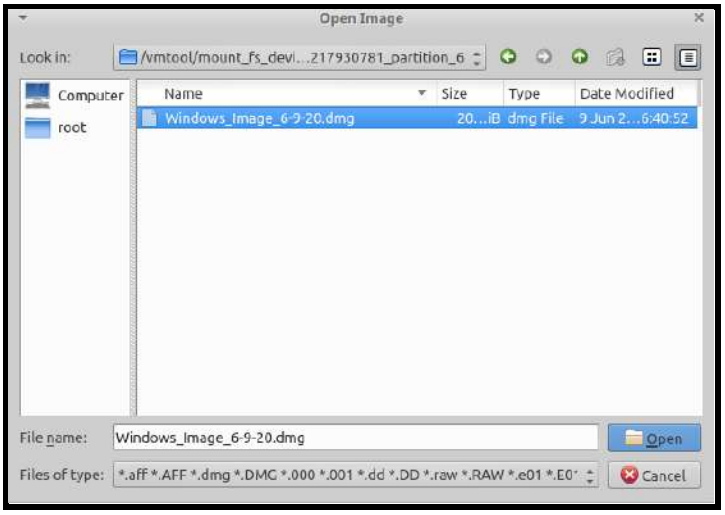
13.3 Unmounting a Partition

Click **Unmount** to eject a previously mounted partition.

14. Selecting an Image to Process

Click the **Plus** icon at the top of CARBON's Main Interface to add a forensic or virtual hard disk image. The **Open Image** window will launch.

Note: Before mounting an image, first mount the drive that contains the desired image. For more information about Attached Media, see ***Section 12****.*



Select an image and click **Open** to add the image to CARBON.

15. Virtualization

CARBON's virtualization capabilities allow examiners to create a forensically sound virtual environment of the attached drives or images with a Windows operating system. The created virtual machine can bypass user login credentials without making changes to the source media.

Virtualization is a powerful tool that gives examiners the chance to see the system as the original user did.

The following information can be entered in the Virtual Machine configuration window:

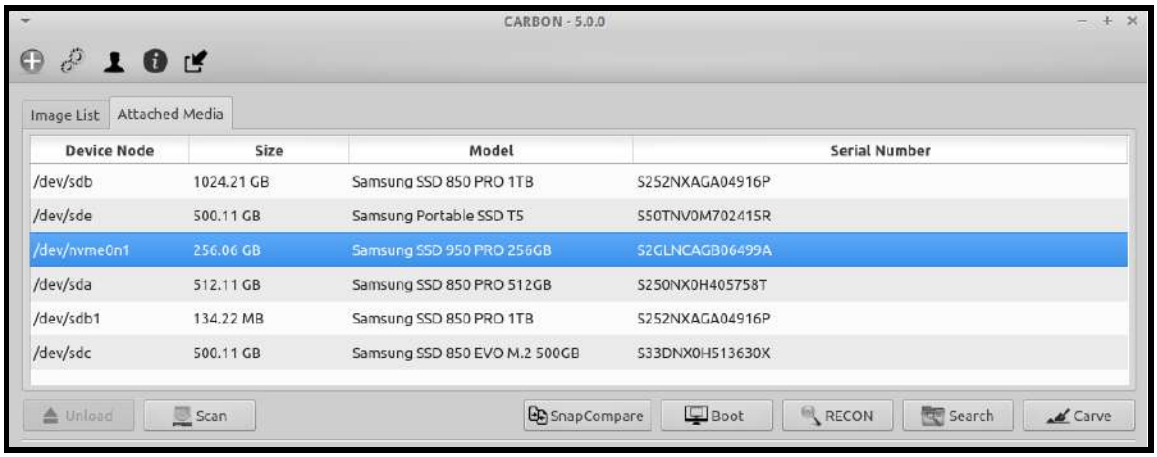
Virtualization Modules	Summary of Module
Device Name	Name of the device node
VM Name	Virtual Machine name
VM RAM Size*	Virtual Machine memory size
VM CPUs*	Number of cores the virtual machine runs
VM Video Memory*	Amount of video memory the virtual machine can support
Clear User Passwords	Check the Clear User Passwords box to bypass the need to enter the User's login credentials.
Output as SAMBA SHARE	Networking standard for Windows
Enable Network	Allows the virtual machine to connect to the network utilizing Network Address Translation (NAT) with the host machine. The host machine must be connected to the network prior to booting the image.
Activate USB Filters	Allows USB support (Non-Forensic Mode only)
Domain User List	Active Directory users
Save Snapshot	Snapshots and video captures of the virtualized machine
Saved Snapshot List	Location of output device with saved snapshots
Dual Boot	Displays whether or not the VM has more than one operating system
Operating System	Displays the current operating system being examined
Hard Disk Controller	Type of Hard Disk Controller emulated. Examiners can choose between SATA, IDE, and SCSI
Comments	A text box for any comments (These comments can be found on the output drive under the CARBON_Output/VMNotes folder.)

*Many of these settings can be adjusted to allow for more RAM, CPU cores, and Video Memory to increase the performance of the VM.

15.1 Selecting a Source

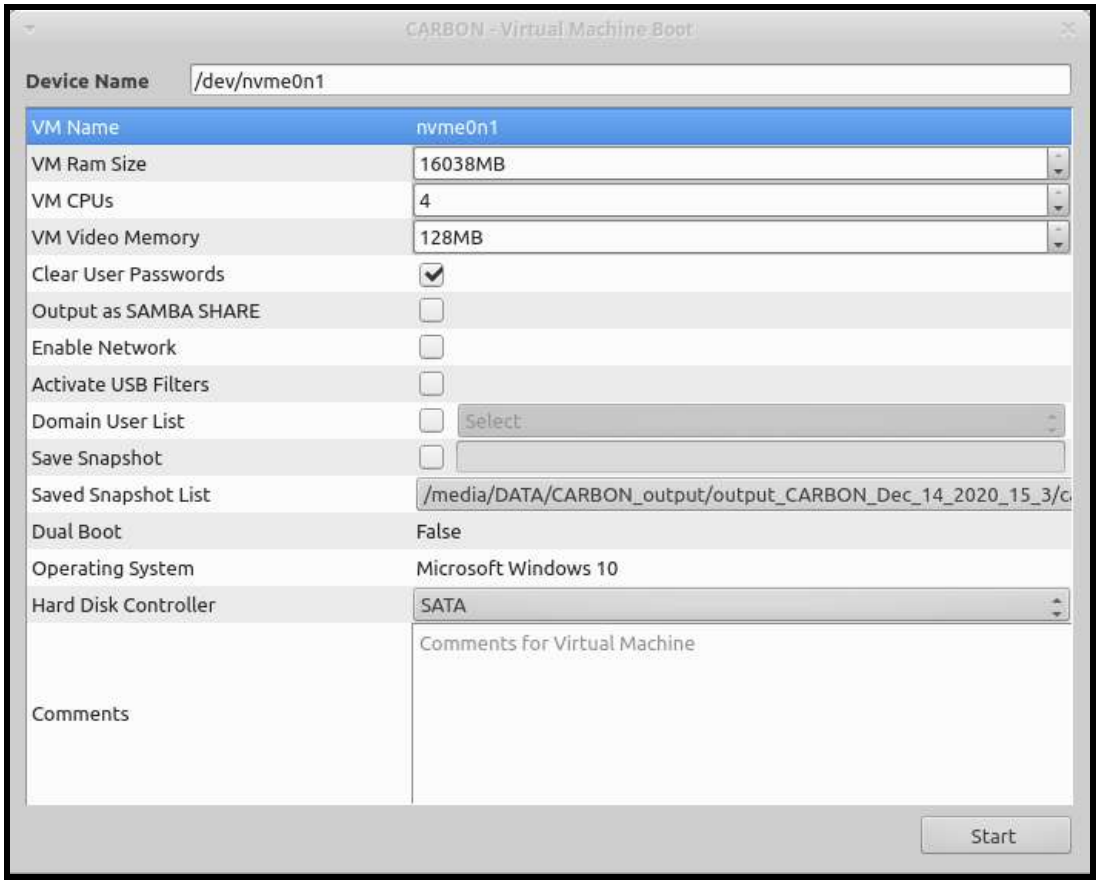
Before starting Virtualization, select the desired partition, drive, or image that contains the operating system from the **Image List** or **Attached Media** tabs.

*For more information about Attached Media, see **Section 12**.*



15.2 Starting Virtualization

To begin the virtualization of a drive or image select **Boot** in CARBON's Main Interface to access the Virtual Machine Boot configuration window.



15.3 Device Name

CARBON lists the **Device Name** based on the selected source.

15.4 Default Settings

By default, CARBON lists the **VM RAM Size**, **VM CPUs**, and **VM Video Memory** settings based on the virtual machine.

- **VM RAM Size** - Virtual Machine memory size
- **VM CPUs** - Number of cores the virtual machine runs
- **VM Video Memory** - Amount of video memory the virtual machine can support

15.4.1 Adjusting Default Settings

Examiners can adjust the default settings to increase the RAM, CPU cores, and Video Memory for better performance of the Virtual Machine.

15.5 Clearing User Passwords

Check the **Clear User Passwords** box to bypass the need to enter the User's login credentials.

15.6 Output as SAMBA SHARE

SAMBA SHARE allows the examiner to share files across a network.

Check the **Output as SAMBA SHARE** box to output cache files via SAMBA SHARE to the output directory.

15.7 Enable Network

Check the **Enable Network** box allows the virtual machine to connect to the network utilizing Network Address Translation (NAT) with the host machine. The host machine must be connected to the network prior to booting the image.

15.8 Activate USB Filters

Check the **Activate USB Filters** box to allow USB support.

15.9 Domain User

The **Domain User List** will display the list of available domain if the machine is set up to have.

15.10 Saving Snapshot

Check the **Save Snapshot** box to enable saving snapshots of the Windows environment being examined. Name the snapshot in the text box.

Select **New Cache** to create a new snapshot before booting in the Virtual Machine. Changes in the Windows environment will be saved in the snapshot as caches files located in the Output Directory.

For more information about the Output Directory, see **Section 8.1**.

15.10.1 Selecting a Saved Snapshot

Select previously saved snapshots from the **Saved Snapshot List** dropdown menu to boot the saved snapshot.

15.10.2 Use in Snapshot Comparison

Snapshots of the Windows environment being examined can be used in CARBON's Snapshot Comparison feature to compare files changes from two different states of time using differential analysis.

Examiners need to create two snapshots in order to use Snapshot Comparison:

Base Snapshot - the first snapshot of the machine's original state

Secondary Snapshot - the second snapshot of the machine with changes to its file system

For more information about Snapshot Comparison, see **Section 17**.

15.11 Dual Boot Detected

CARBON displays whether or not the VM has more than one Windows operating system.

15.12 Operating System Detected

CARBON lists the **Operating System** based on the current operating system being examined.

15.13 Hard Disk Controller Setting

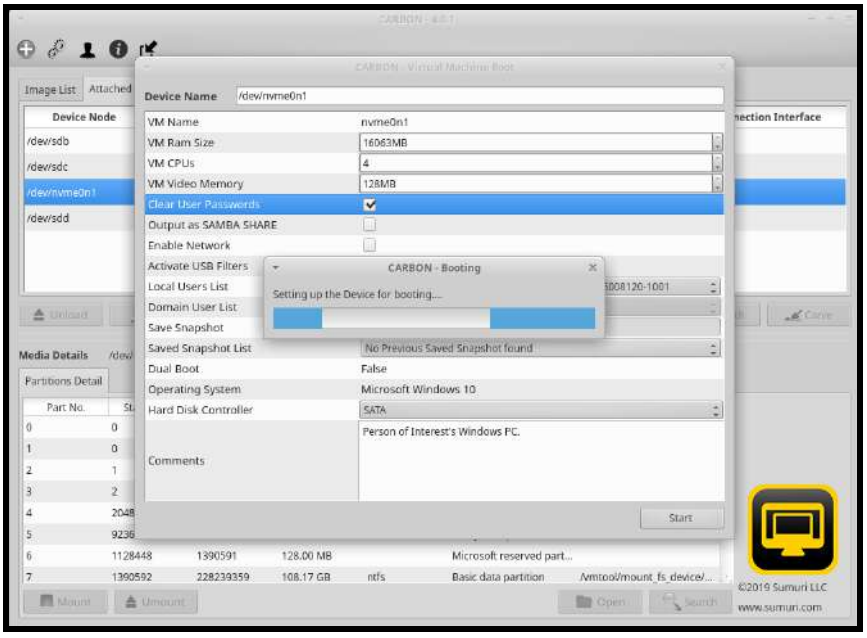
In the **Hard Disk Controller** drop down menu, choose the type of Hard Disk Controller to be emulated. Examiners can choose from SATA, IDE, and SCSI.

15.14 Entering Comments/Notes

Enter any comments or notes in the **Comments** text box (These comments can be found on the output drive under the CARBON_Output/VMNotes folder.)

15.15 Start

Once the Virtual Machine settings are properly configured, click **Start**, and CARBON will begin the Virtualization process.



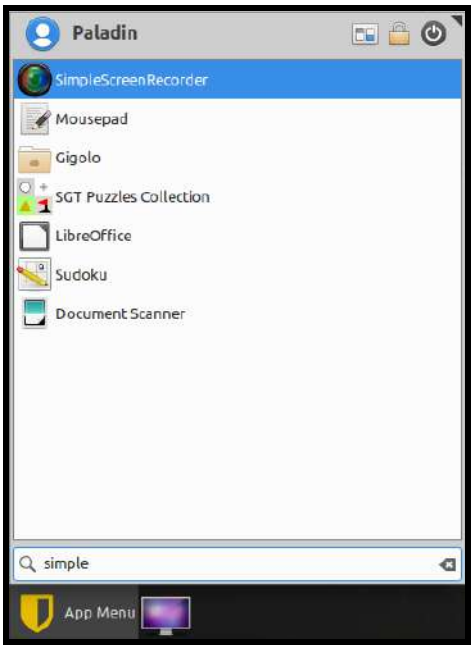
15.16 Documentation

SUMURI has included tools in CARBON to help examiners properly document important events observed in the Virtual Machine.

15.16.1 Video Capture

Click the **App Menu** and search for **SimpleScreenRecorder**.

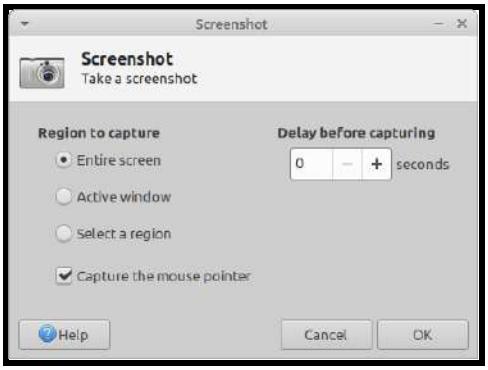
A window will appear to configure the settings for the recording and save the recording to an output drive.



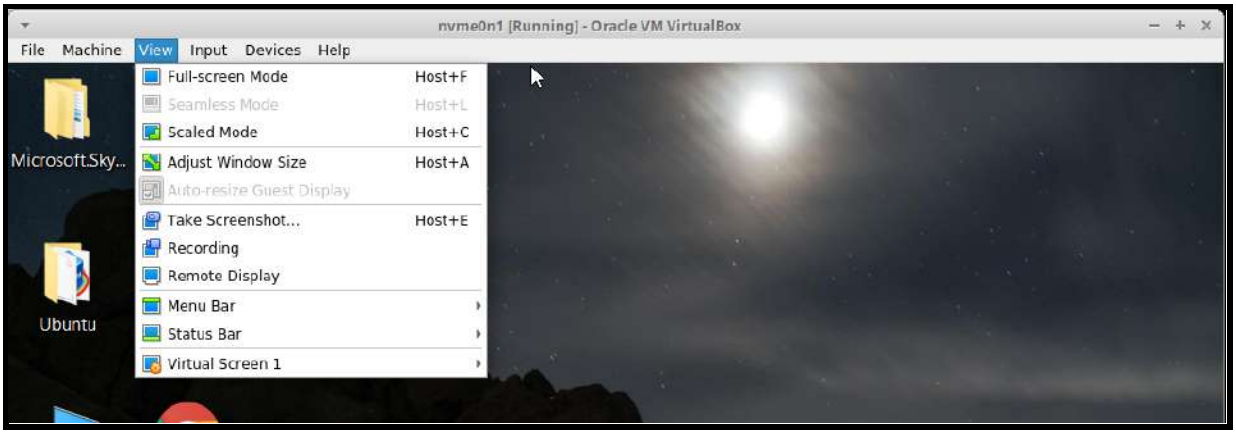
15.16.2 Screenshot Capture

Click the **Screenshot** shortcut on the Dock.

A window will appear to take a screenshot of the entire screen, an active window, or a specified region.



Examiners can also take screenshots with the built-in screenshot utility in the Virtual Machine Task Bar.

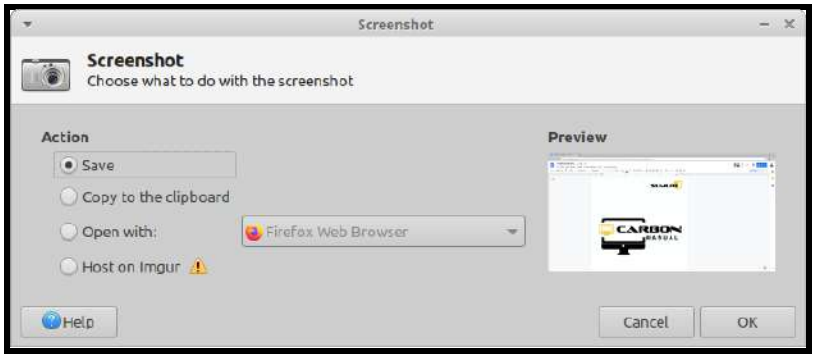


Navigate to the **View** tab and select **Take Screenshot**. This will automatically save a screenshot of the entire window as a PDF.

15.16.3 Reviewing Output

Select one of the following output options to save the screenshot:

- **Save -** Allows the examiner to select an output directory to save the screenshot
- **Copy to Clipboard -** Copies the taken screenshot to the clipboard
- **Open With -** Allows the examiner to select an application to open the screenshot.



16. Windows Triage - RECON

RECON for Windows allows the examiner to quickly scan a target machine's file system using automated plugins.

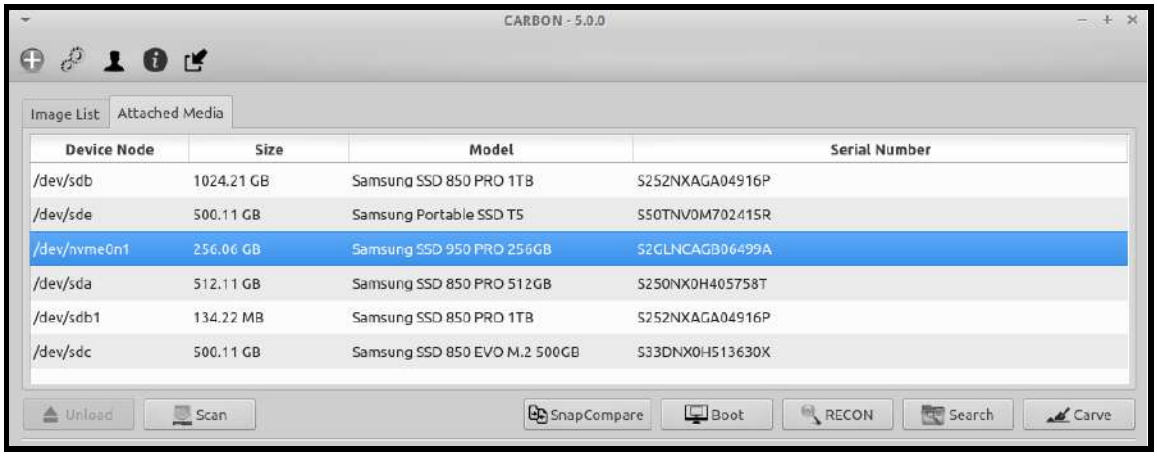
RECON for Windows features over 40 plugins that will automatically parse artifacts that can be instantly exported into a professional report.

Examiners have the ability to create custom templates.

Triage of Windows operating systems can be performed on internal disks or attached media.

16.1 Selecting a Source

Before starting RECON for Windows, select the partition, drive, or image from the **Image List** or **Attached Media** that contains a Windows operating system.

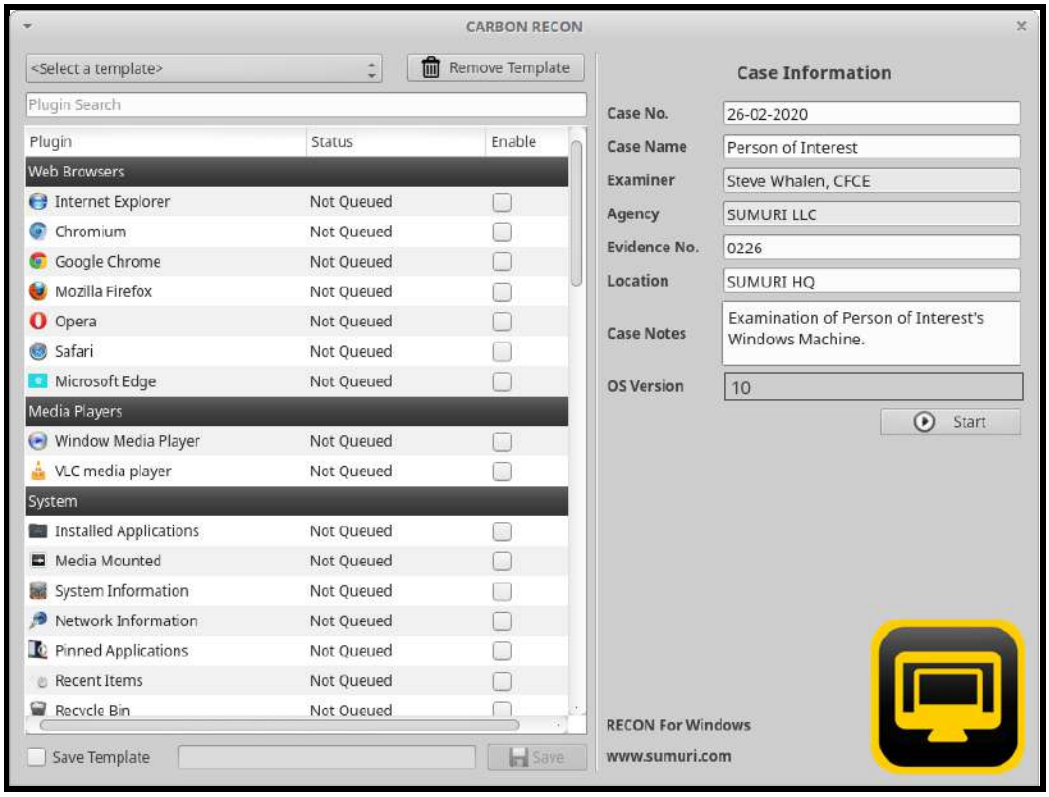


16.2 Starting RECON for Windows

Click the **RECON** button to start triaging a Windows device using RECON for Windows.

The RECON for Windows window will appear.

16.3 New Case Interface



16.3.1 Case Information

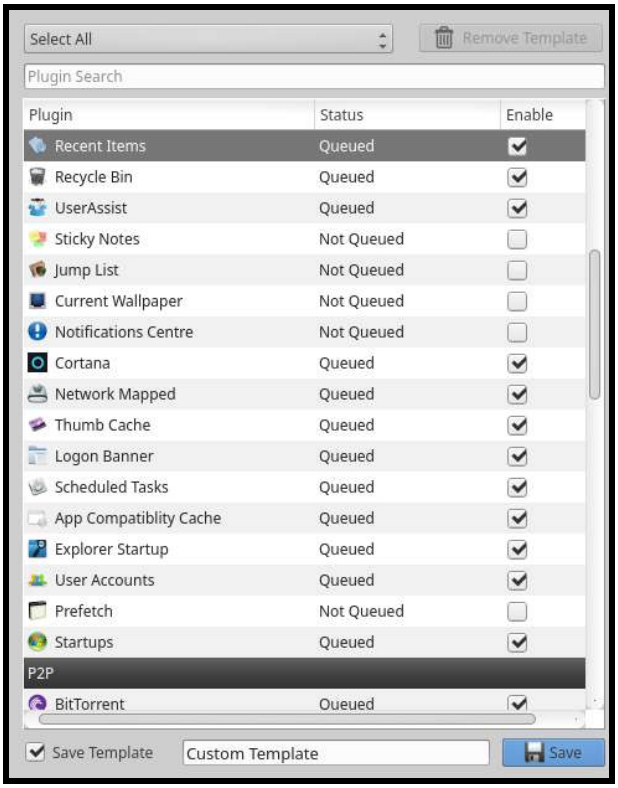
When the New Case window appears, start by entering the Case Information.

Note: The Examiner and Agency information must be set in the Configuration Module or these fields will remain blank. See ***Section 9.3*** *for information on how to add examiner information.*

- **Case No.** (mandatory) — A unique case number
- **Case Name** — Name for the case
- **Examiner** — Examiner name
- **Agency** — Agency name
- **Evidence No.** — A unique evidence number
- **Location** — Location of the incident or the exam
- **Case Notes** — Free form field
- **OS Version** — Automatically populated based on detected Windows OS version of the image

16.3.2 Selecting Plugins

Plugins can be selected and activated by checking the Enable box.

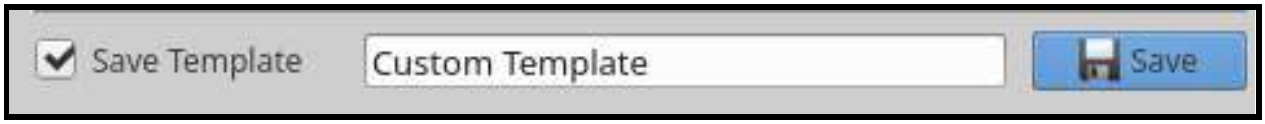


16.3.2.1 Plugin Search

The **Plugin Search** field can be used to filter the list of plugins quickly.

16.3.2.2 Saving a Template

A template for plugins can be created by selecting any number of plugins.



Once the plugins have been chosen for the template, activate the **Save Template** checkbox and provide a unique name. Click the **Save** button to save the template.

16.3.2.3 Loading a Template

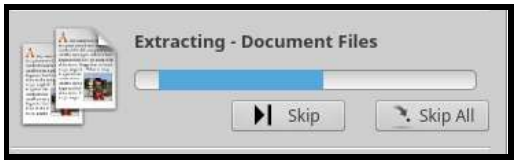
Once saved, templates will be available in the **<Select a Template>** dropdown list above the Plugin Search box.

To delete a template, pick a template from the list and click the **Remove Template** button.

16.3.3 Starting the Triage

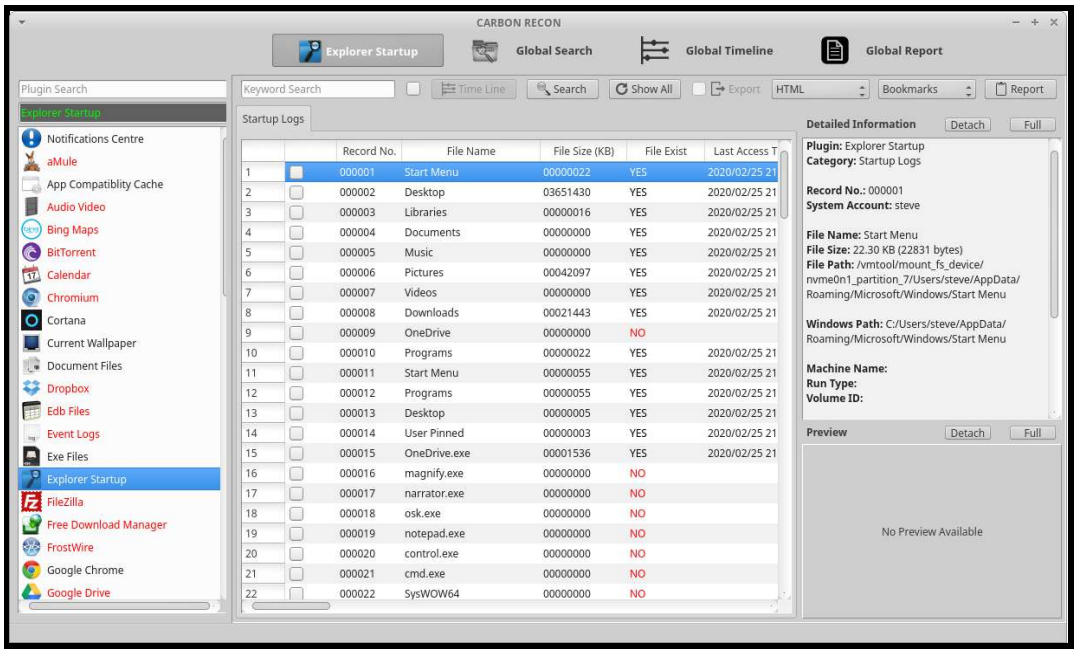
Once the Case Information and options have been set, click the **Start** button to begin the automated parsing and analysis of artifacts.

Once the processing starts, examiners can **Skip** individual processes or **Skip All** remaining processes if needed.



16.4 Results Window

After the data has been processed, selecting any plugin from the Plugin Sidebar will show records in the Records Window with Detailed Information.



16.5 Viewing Plugin Results

The Results Window will display a list of the plugins in the left pane and artifacts (records) in the center.

16.5.1 Red vs. Black

If there are artifacts for a plugin, the plugin will be in **black text.** If there are no artifacts for the plugin, the plugin will be in **red text**.

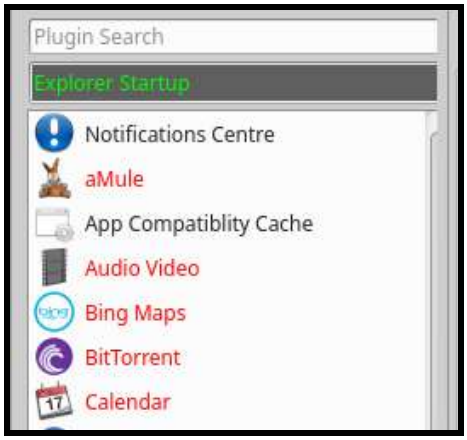
The **File Exist** field indicates whether or not that particular file is present on the media in its original location.

- **Yes** - the file exists in its original location
- **No** - the file does not exist in its original location

If a multimedia file is available, the examiner will be able to preview the file using the built-in viewer.

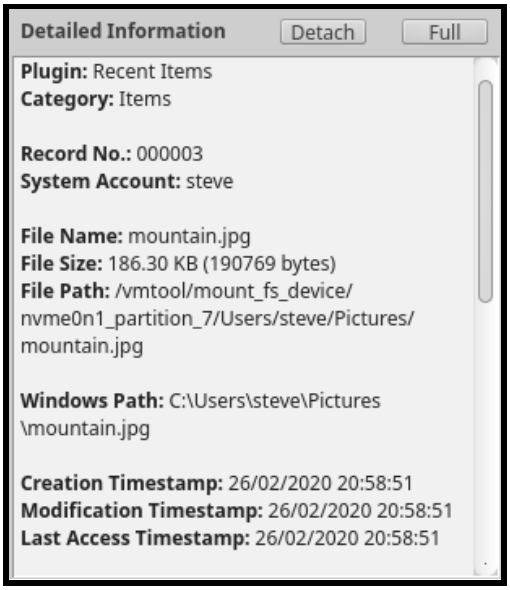
16.5.2 Plugin Sorting

The **Plugins Sidebar** is found on the left-side of the Results Window. Selecting a plugin will show records in the Records Window. The Plugins Sidebar also has a Plugin Search box to filter plugins quickly.



16.6 Detailed Information Window

The **Detailed Information Pane** can be found on the right-side of the Results Viewer window.



The Detailed Information shows additional information about any record selected in the Results Viewer window. The information will change based on the type of record that is selected.

Note: Timestamps of artifacts are formatted as yyyy/dd/mm hh:mm:ss.

16.6.1 Detach Button

Click the **Detach** to open a separate Detailed Information Window. Information changes when new records are selected.

16.6.2 Full Button

Click the **Full** button to open a separate Detailed Information Window with the current record information only.

16.7 Preview Window

The Preview Window is a multimedia viewer and supports the preview of most audio, video, and images. The Preview Window will show content when a supported file is selected.

There are two options for detaching the Preview Window using the buttons at the top.

16.7.1 Detach Button

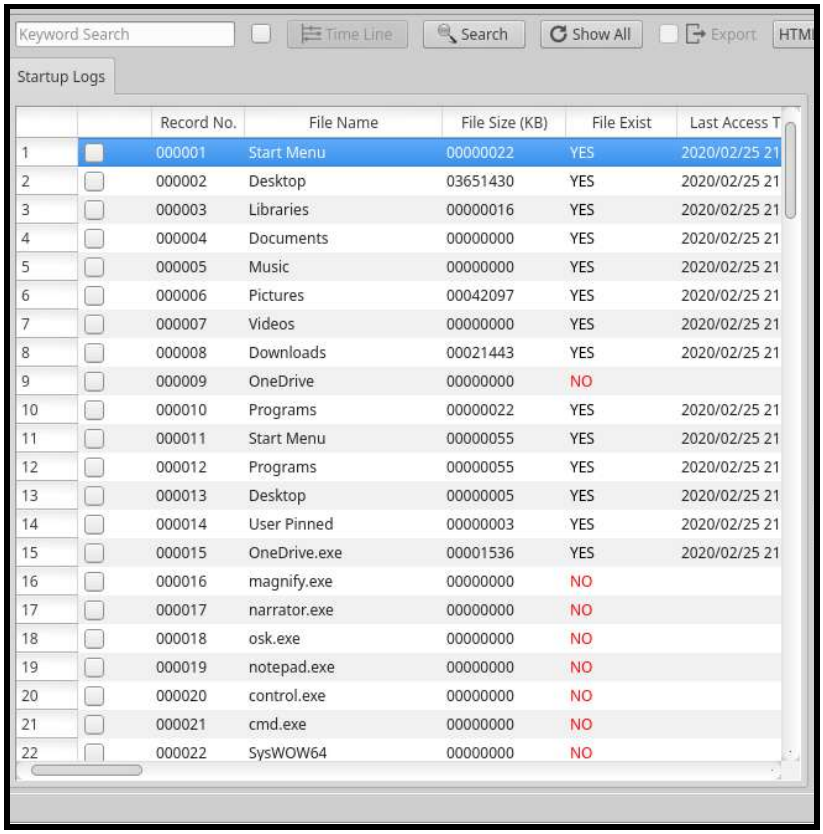
Click the **Detach** to open a separate Preview window. Information changes when new records are selected.

16.7.2 Full Button

Click the **Full** button to open a separate Preview Window with the current record information only.

16.8 Records Window

The Records Window allows the examiner to search, bookmark, add notes, and export records.



		Record No.	File Name	File Size (KB)	File Exist	Last Access T
1		000001	Start Menu	00000022	YES	2020/02/25 21
2		000002	Desktop	03651430	YES	2020/02/25 21
3		000003	Libraries	00000016	YES	2020/02/25 21
4		000004	Documents	00000000	YES	2020/02/25 21
5		000005	Music	00000000	YES	2020/02/25 21
6		000006	Pictures	00042097	YES	2020/02/25 21
7		000007	Videos	00000000	YES	2020/02/25 21
8		000008	Downloads	00021443	YES	2020/02/25 21
9		000009	OneDrive	00000000	NO	
10		000010	Programs	00000022	YES	2020/02/25 21
11		000011	Start Menu	00000055	YES	2020/02/25 21
12		000012	Programs	00000055	YES	2020/02/25 21
13		000013	Desktop	00000005	YES	2020/02/25 21
14		000014	User Pinned	00000003	YES	2020/02/25 21
15		000015	OneDrive.exe	00001536	YES	2020/02/25 21
16		000016	magnify.exe	00000000	NO	
17		000017	narrator.exe	00000000	NO	
18		000018	osk.exe	00000000	NO	
19		000019	notepad.exe	00000000	NO	
20		000020	control.exe	00000000	NO	
21		000021	cmd.exe	00000000	NO	
22		000022	SysWOW64	00000000	NO	

16.8.1 Record Tabs

Records will have different tabs, columns, and values based on the types of artifacts that were processed.

Selecting a different Tab will load new records. *Not all tabs will be populated with records.*

16.8.2 Records

Records will have multiple fields, columns, and values based on the type of artifacts that were processed. *Not all records will be populated with fields.*

16.8.3 Bookmarking Records

Bookmarking a record can help to identify items of interest. Reports can also be generated using bookmarked records.

Click the checkbox to the left of the record to bookmark the record.

16.8.3.1 Bookmark All

All records in the current Results Window can be bookmarked by right-clicking on any record and selecting **Bookmark All.**

16.8.3.2 Remove All Bookmarks

Bookmarks can also be removed all at once by right-clicking and selecting **Remove All Bookmarks.**

16.8.4 Adding Notes

The examiner can add notes to records. Right-click on a record and click **Add Note**.

16.8.4.1 Adding Notes to All Bookmarks

To add a note to a bookmark, make sure to bookmark the item first, and then select **Add Note to Bookmarks.**

Add the note and click **Save**.

A small icon will appear next to the checkmark box verifying that the note has been added and will be included in the report.

16.8.5 Exporting Individual Files

Files can be exported by right-clicking and selecting **Export File**.

16.9 Filtering Plugin Records

Examiners can apply two filter options to any displayed results and only show the files they are looking for quickly.

- **Keyword Search** - Allows the examiner to conduct keyword searches quickly within all artifacts
- **Time Line** - Allows an examiner to refine the results of a data query to a specific date range

16.9.1 Keyword Search

Enter a keyword into the Keyword Search bar, and then click the **Search** button.

16.9.1.1 Adding Multiple Keywords

Search for multiple terms simultaneously by separating each word with a comma and click **Search**. In the screenshot below, multiple search terms can be used at once by separating each word with a comma and no spaces (i.e. bitcoin,dropbox).

Click the **Show All** button to refresh the search bar and clear Keyword Search filters.

16.9.2 Applying a Timeline

Check the Time Line box to refine the results of a data query to a specific date range.

Data can be filtered by setting a **Start Time** and an **End Time**. Once the dates have been entered, click **Set**.

16.9.3 Show All Records

Click the **Show All** button to refresh the search bar and clear Timeline filters.

16.10 Generating a Plugin Report

Plugin Reports can be created within any Plugin. Report options can be found in the upper right hand corner of the Results Window.

16.10.1 Reporting Formats

RECON for Windows has the ability to create reports in four formats. Not all reporting formats will be available for all plugins.

The four formats include:

- **HTML** - A report that can be opened in a standard web browser
- **PDF** - A Portable Document Format report
- **CSV** - A report saved as a Comma Separated Value spreadsheet
- **XML** - A report saved in the Extensible Markup Language format for importing into other tools

Click on the first dropdown menu and choose the desired report format.

16.10.2 Scope of Report

Three options exist for including records in the Plugin Report.

The three options are:

- **Bookmarks** - Includes only the bookmarked records within the currently selected plugin
- **Screen Items** - Includes all records currently showing in the Results Window
- **Full** - Includes all records in the currently selected plugin

Click on the second dropdown menu and choose the desired scope of the report.

16.10.3 Including Exported Files in Report

Check the **Export** box next to the report button to export files at the same time the report is generated.

16.10.4 Saving a Report

To generate the Plugin Report after all the options have been selected, click **Report**.

A message will appear stating that the report was generated. To open the report, click **YES**.

16.10.5 Location of Report

Plugin Reports can be found in the Output Directory selected by the examiner when CARBON was started. For more information about the Output Directory, see **Section 8.1**.

16.11 Global Search

Global Search allows the examiner to quickly find information across all Plugins within seconds.

16.11.1 All Plugins

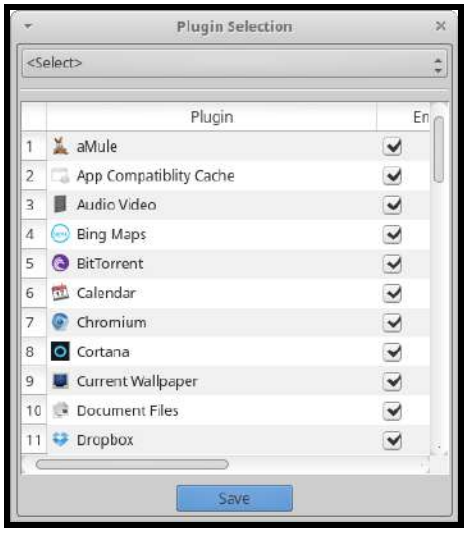
Select the **Global Search** button at the top of the results window to begin.

In the upper left-hand corner of the Global Search window, there are Plugin options.

By default, the **All Plugins** options will be checked. **All Plugins** will search through every artifact extracted from all processed plugins.

16.11.1.1 Filtering Plugins

To limit the Global Search to specific plugins, select the **Plugin List** button, and click **Select**. The Plugin Selection window will appear.

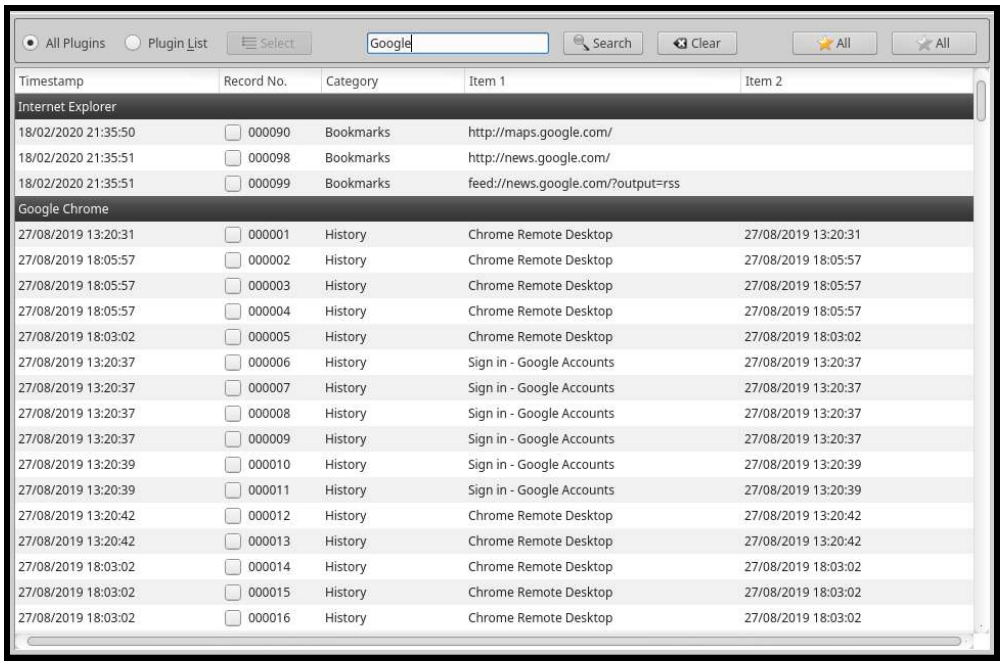


Choose the plugins to include in the Global Search, and click **Save**.

A Plugin Search box is available to quickly filter and find plugins to select. Only the plugins enabled will show results.

16.11.2 Keyword Search

Enter a keyword into the Keyword Search field, and then click the **Search** button to perform a Global Search. To reset and start a new search, click the **Clear** button.



Timestamp	Record No.	Category	Item 1	Item 2
Internet Explorer				
18/02/2020 21:35:50	000090	Bookmarks	http://maps.google.com/	
18/02/2020 21:35:51	000098	Bookmarks	http://news.google.com/	
18/02/2020 21:35:51	000099	Bookmarks	feed://news.google.com/?output=rss	
Google Chrome				
27/08/2019 13:20:31	000001	History	Chrome Remote Desktop	27/08/2019 13:20:31
27/08/2019 18:05:57	000002	History	Chrome Remote Desktop	27/08/2019 18:05:57
27/08/2019 18:05:57	000003	History	Chrome Remote Desktop	27/08/2019 18:05:57
27/08/2019 18:05:57	000004	History	Chrome Remote Desktop	27/08/2019 18:05:57
27/08/2019 18:03:02	000005	History	Chrome Remote Desktop	27/08/2019 18:03:02
27/08/2019 13:20:37	000006	History	Sign in - Google Accounts	27/08/2019 13:20:37
27/08/2019 13:20:37	000007	History	Sign in - Google Accounts	27/08/2019 13:20:37
27/08/2019 13:20:37	000008	History	Sign in - Google Accounts	27/08/2019 13:20:37
27/08/2019 13:20:37	000009	History	Sign in - Google Accounts	27/08/2019 13:20:37
27/08/2019 13:20:39	000010	History	Sign in - Google Accounts	27/08/2019 13:20:39
27/08/2019 13:20:39	000011	History	Sign in - Google Accounts	27/08/2019 13:20:39
27/08/2019 13:20:42	000012	History	Chrome Remote Desktop	27/08/2019 13:20:42
27/08/2019 13:20:42	000013	History	Chrome Remote Desktop	27/08/2019 13:20:42
27/08/2019 18:03:02	000014	History	Chrome Remote Desktop	27/08/2019 18:03:02
27/08/2019 18:03:02	000015	History	Chrome Remote Desktop	27/08/2019 18:03:02
27/08/2019 18:03:02	000016	History	Chrome Remote Desktop	27/08/2019 18:03:02

Within seconds, the Results Window will populate with search hits across all plugins.

16.11.2.1 Adding Multiple Keywords

To search for multiple keywords at the same time, enter the keywords separated with a comma and no space.

16.11.2.2 Clearing Keywords

To reset and start a new search, click the **Clear** button.

16.11.3 Bookmarking in Global Search

Bookmarking a record can help identify items of interest. Reports can also be generated using bookmarked records.

Click the checkbox next to each record or hit the spacebar while a record is highlighted to bookmark the records.

16.11.3.1 Bookmarking All Results

Click the **Gold Star All** button in the top right corner of the Global Search window to select ALL records to bookmark.

16.11.3.2 Removing All Bookmarks

Click the **Grey Star All** to deselect the bookmarked records in the current Results Window.

16.12 Global Timeline

All parsed artifacts with timestamps can be loaded within the Global Timeline Module to allow chronological analysis. Chronological, or historical, analysis enables the examiner to view data minute by minute or even second by second in order. The ability to place the artifacts in order by time can lead to a greater understanding of the case and can even change the outcome of an investigation.

16.12.1 Selecting Plugins

Select the **Global Timeline** button at the top of the results window.

In the upper left-hand corner of the Global Timeline window, there are Plugin options.

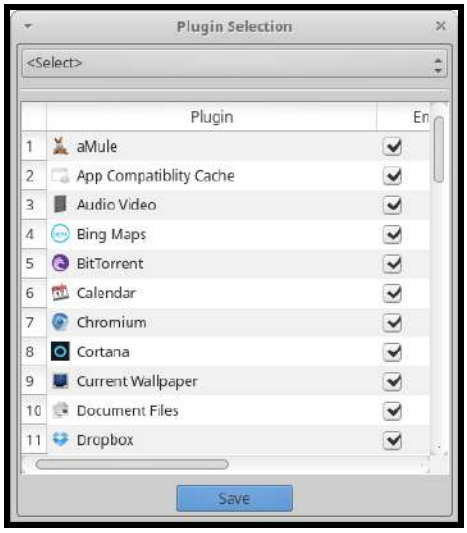
16.12.1.1 All Plugins

By default, the **All Plugins** options will be checked. **All Plugins** will search through every artifact extracted from all processed plugins.

16.12.1.2 Selecting Specific Plugins

To limit the Global Timeline to specific plugins, select the **Plugin List** button, and click **Select**.

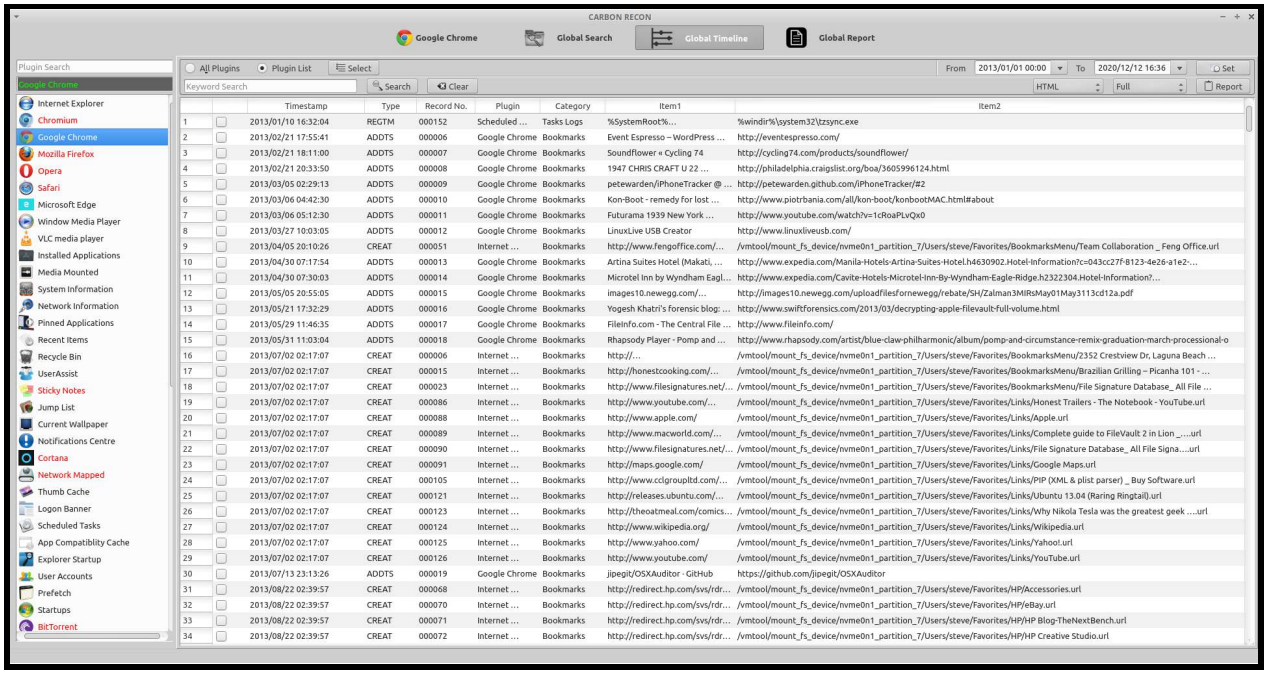
The Plugin Selection window will appear.



Choose the plugins to include in the Global Timeline, and click **Save**. A Plugin Search box is available to quickly filter and find plugins to select. Only the plugins enabled will show results.

16.12.2 Setting the Timeline

Data can be filtered by setting a **Start Time** and an **End Time**. Then, click **Set**.



16.12.3 Keyword Search

Enter a keyword into the Keyword Search bar, and then click the **Search** button in Global Timeline.

Within seconds, the Results Window will populate with search hits across all plugins.

16.12.3.1 Adding Multiple Keywords

To search for multiple keywords at the same time, enter the keywords separated with a comma and no space.

16.12.3.2 Clearing Keywords

To reset and start a new search, click the **Clear** button.

16.12.4 Bookmarking

Bookmarking a record can help to identify items of interest. Reports can also be generated using the bookmarks as a filter.

Click the checkbox to the left of the record to bookmark the record.

16.12.4.1 Bookmark All Results

All records in the current Results Window can be bookmarked by right-clicking on any record and selecting **Bookmark All.**

16.12.4.2 Remove All Bookmarks

Bookmarks can also be removed all at once by right-clicking and selecting **Remove All Bookmarks.**

16.12.5 Generating a Report

Reports can be generated from the Global Timeline by clicking the **Report** button at the top of the results window.

16.12.5.1 Reporting Formats

Global Timeline has the ability to create reports in four formats. Not all reporting formats will be available for all plugins.

The four formats include:

- **HTML** - A report that can be opened in a standard web browser

- **PDF** - A Portable Document Format report
- **CSV** - A report saved as a Comma Separated Value spreadsheet
- **XML** - A report saved in the Extensible Markup Language format for importing into other tools

Click on the first dropdown menu and choose the desired report format.

16.12.5.2 Scope of Report

Three options exist for including records in the Global Timeline Report.

The three options are:

- **Full Time**- Includes all records in Timeline
- **Screen Items** - Includes all records currently showing in the Results Window
- **Bookmarks** - Includes only the bookmarked records

Click on the second dropdown menu and choose the desired scope of the report.

To generate the Plugin Report after all the options have been selected, click **Report**.

A message will appear stating that the report was generated. To open the report, click **YES.**

16.12.5.3 Location of Report

Plugin Reports can be found in the Output Directory. For more information about the Output Directory, see **Section 8.1**.

16.13 Global Report

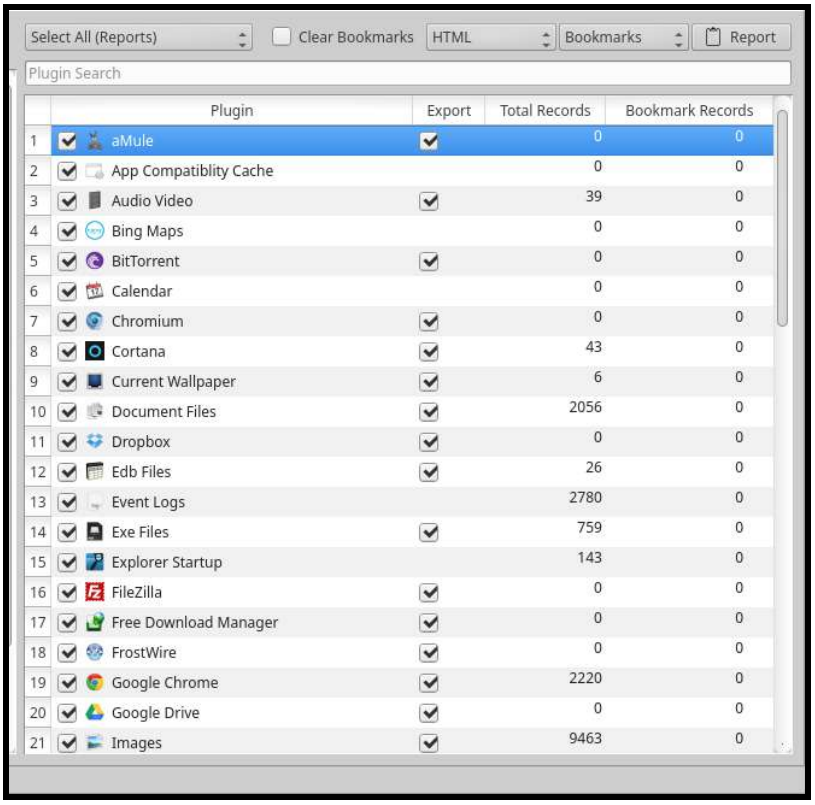
A master report containing artifacts from all the plugins can be created with **Global Reports** which can include data from every plugin processed or only the user's Bookmarks.

16.13.1 Selecting Plugins

Select the individual Plugins to include their records in the Global Report by checking the box within the **Plugin** column.

The examiner has the option to select one of the following Plugin Options:

- **Select All (Reports)** - Add all plugins to your report without exporting
- **Select All (Reports & Exports)** - Add all the plugin results and export all files
- **Deselect All** - Remove all selected items



A Plugin Search box is available to quickly filter and show plugins to select. Only the plugins enabled will show results.

16.13.2 Including Files to Export

To export files associated with the records during the report creating, check the Export button under the corresponding column.

16.13.3 Generating a Report

To generate a report, select the Report Format and the Scope of the Report.

16.13.3.1 Reporting Formats

Global Report has the ability to create reports in five formats using the dropdown list.

Not all reporting formats will be available for all plugins. The five formats include:

- **HTML** - A report that can be opened in a standard web browser
- **PDF** - A Portable Document Format report
- **CSV** - A report saved as a Comma Separated Value spreadsheet
- **XML** - A report saved in the Extensible Markup Language format for importing into other tools
- **Advanced HTML** - A report with navigation options that can be opened in a standard web browser

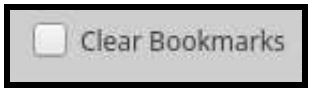
16.13.3.2 Scope of Report

Three options exist for including records in the Plugin Report. These can be selected using the second dropdown list. The three options are:

- **Full Plugin** - Includes all records in the currently selected plugin
- **Bookmarks** - Includes only the bookmarked records within the currently selected plugin

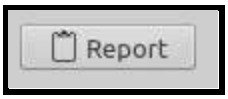
16.13.3.3 Clearing Bookmarks

Check the Clear Bookmarks option to clear selected records in Global Report after generating a report.



16.13.3.4 Generate a Report

Click **Report** to generate a report.



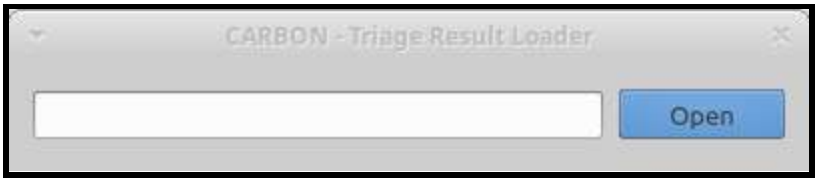
16.13.3.5 Location of Report

Global Reports can be found in the Output Directory. For more information about the Output Directory, see **Section 8.1**.

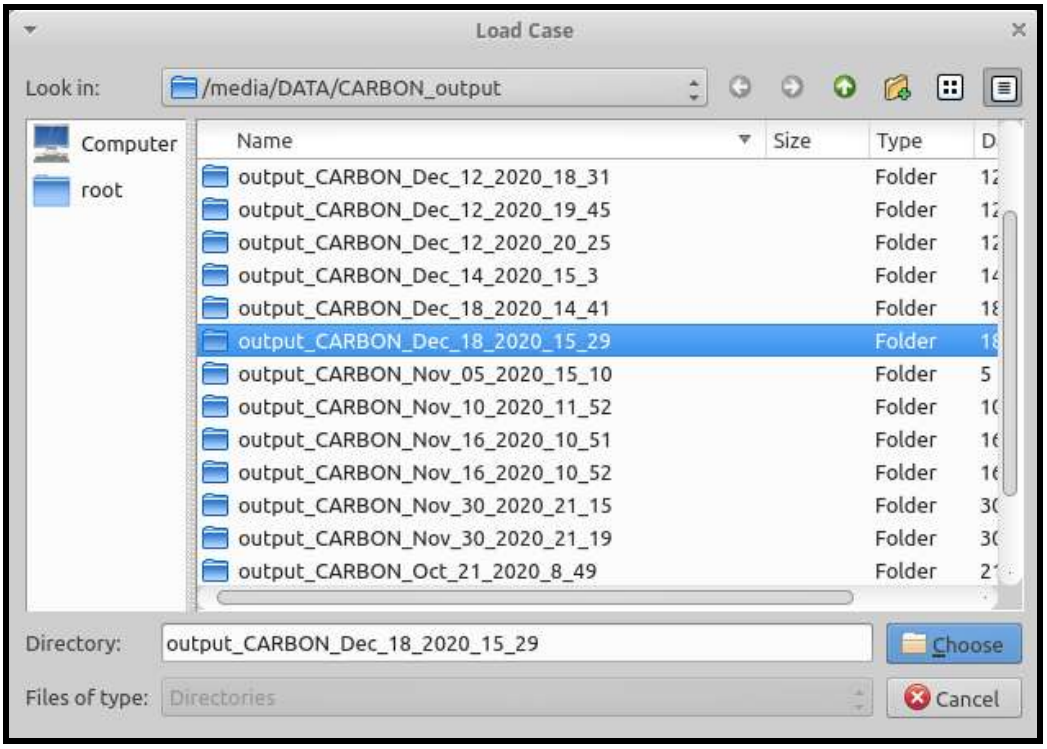
16.14 Load Previous Triage Results

Select the **Load Results** button at the top of the interface to open a previous RECON for Windows case.

Once the Window appears, click **Open**.



Select the desired previous **Case Folder**, and click **Choose**.



The RECON for Windows interface will open and display a previous case.

16.14.1 Loading a Case Saved on Another Drive

To load cases saved on another directory, mount the drive and select the case from the mounted drive.

For more information about Attached Media, see ***Section 12****.*

17. Snapshot Comparison - Differential Analysis

SnapCompare is a tool within CARBON that allows the examiner to inspect files on a Windows environment from two different states of time for modification or tampering using differential analysis.

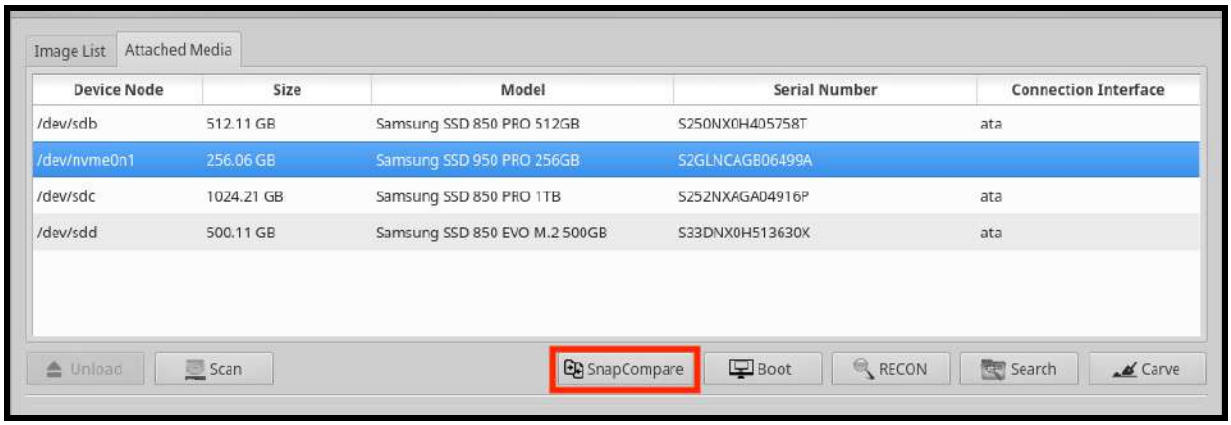
SnapCompare can be used to take a snapshot of files on the Windows system and compare the same file's modified, accessed, and created (MAC) timestamps to see the file changes between Snapshots.

This feature is especially useful for tasks like malware analysis. Examiners can take a Base Snapshot, launch the malware in the Windows environment using CARBON, take a Secondary Snapshot, and see how the malware affects the machine.

During the SnapCompare process, examiners can compare Selected Directories or the Complete Filesystem.

17.1 Selecting Base Snapshot

Snapshots are created using CARBON's Virtualization feature. For more information about creating Snapshots, see **Section 15.10**.

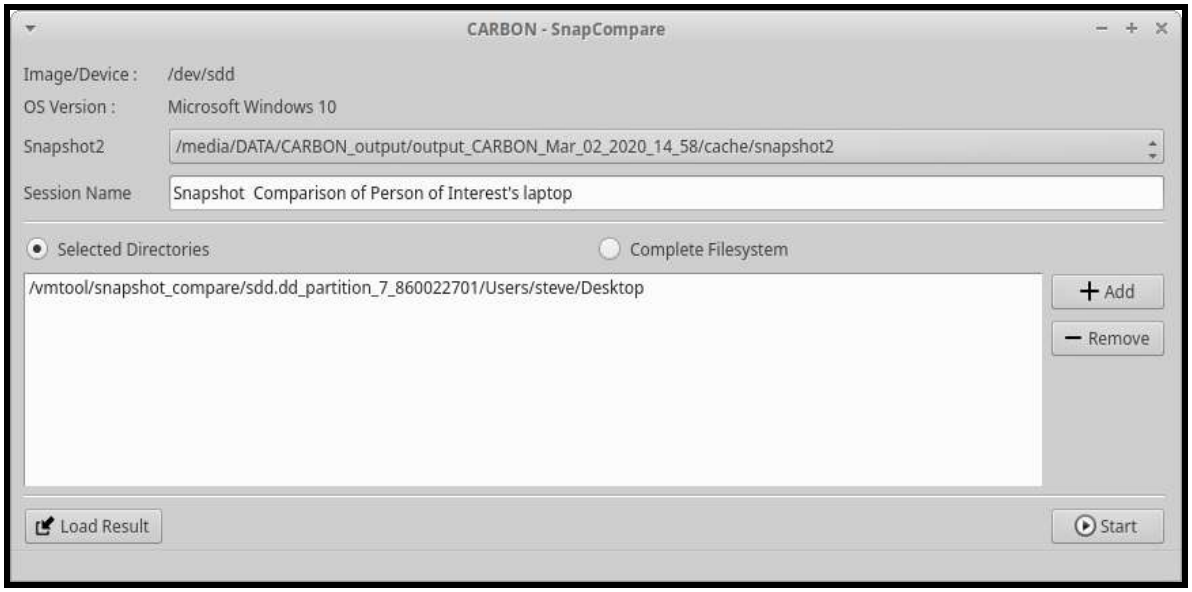


Select the desired Attached Media or Image in CARBON's Main Interface that contains the first snapshot, and then click **SnapCompare**.

Select the Base Snapshot (first snapshot) from the Attached Media or Image, and click on **Done**.

17.2 Selecting a Snapshot for Comparison

After clicking Done, the CARBON-SnapCompare window will appear. Identify the Secondary Snapshot (second snapshot) that will be used for the comparison.



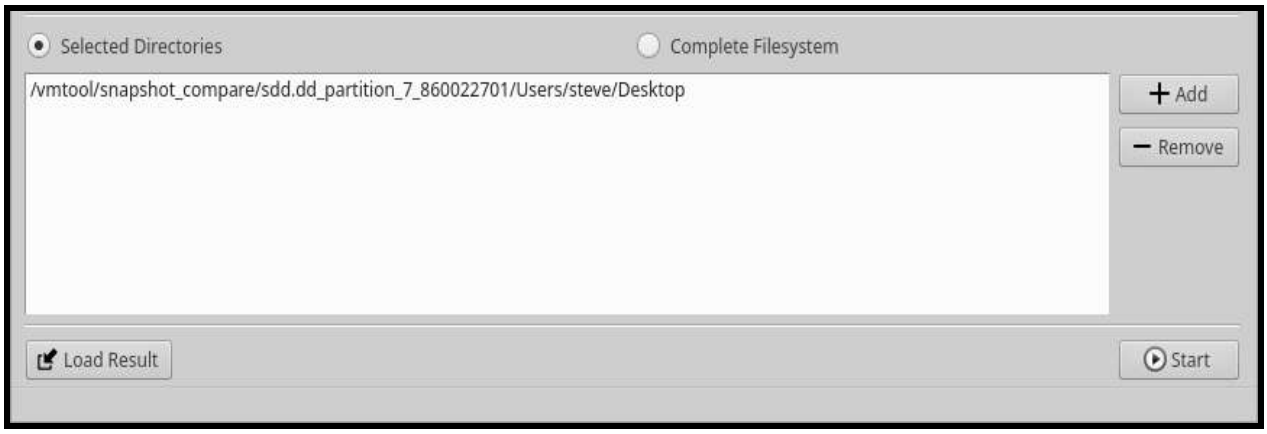
17.3 Naming the Session

Input a name in the following Session Name field.

17.4 Comparing Selected Directories

CARBON will have Selected Directories chosen by default. Examiners can compare directories of their choice from the Base Snapshot and Secondary Snapshot.

In the example below, the examiner is taking a snapshot comparison using the user's Desktop.

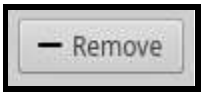


17.4.1 Adding a Directory

Click **+ Add** to add one or more directories to compare.

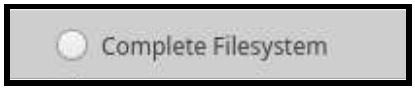
17.4.2 Removing a Directory

Click **- Remove** to remove an added directory.



17.5 Selecting Complete File System

Select **Complete Filesystem** to compare the entire file system.

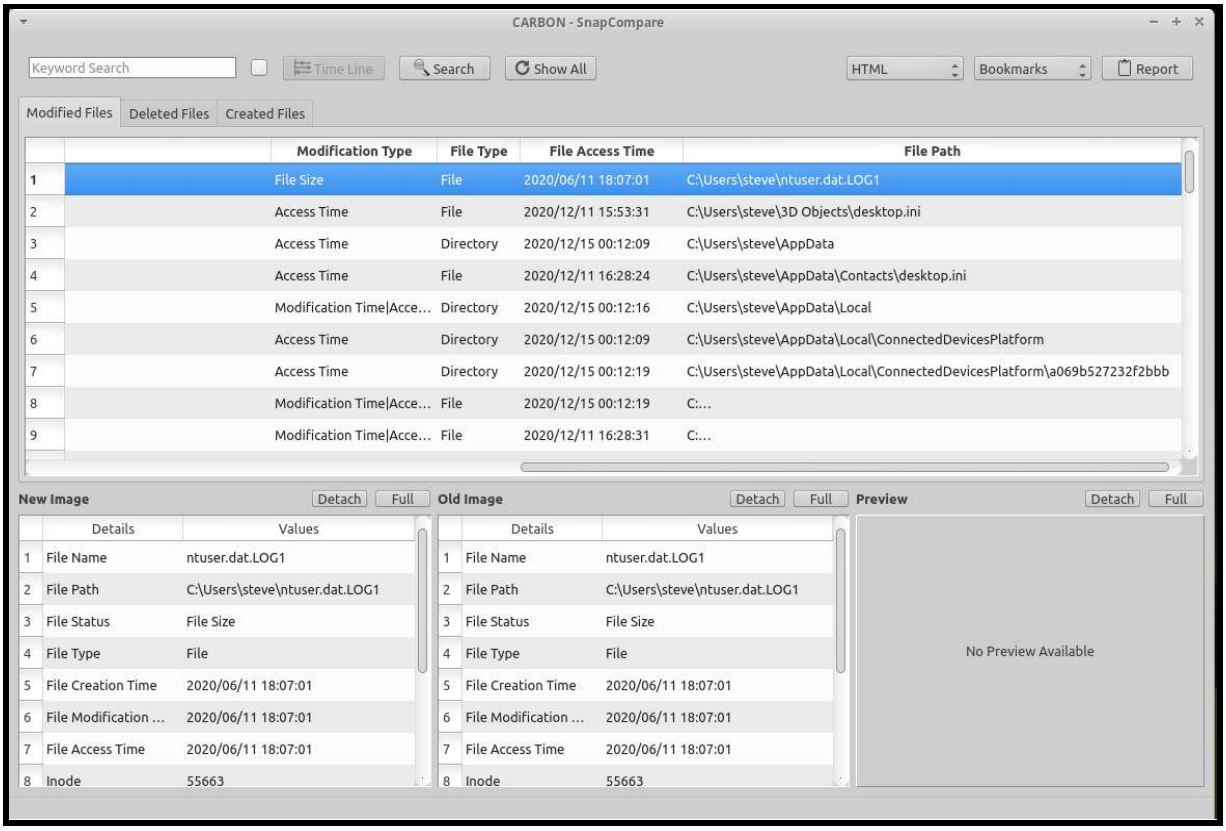


To begin comparing the user's file system Snapshots, click **Start**.

17.6 Results Window

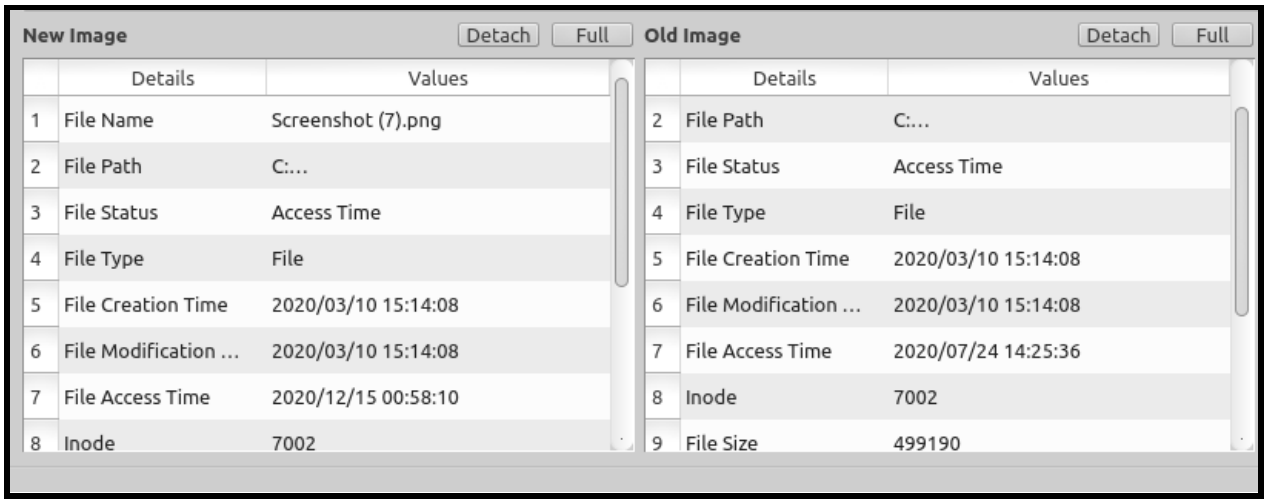
After the Snapshot Comparison is complete, the results will present Modified, Deleted, and Created Files.

Examiners have the option to perform Keyword Searches, Bookmark Records, Add Notes, Export Files, and Generate Reports.



17.6.1 Detailed Information Windows

The detailed information view shows all associated metadata with the selected record from both the New Image (Secondary Snapshot) and Old Image (Base Snapshot).

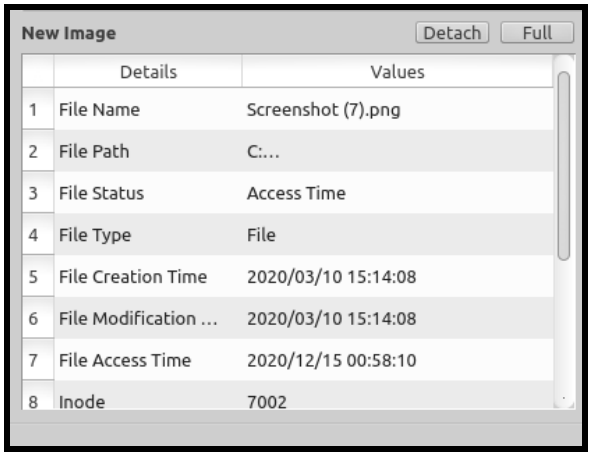


Select the **Full** button to enlarge the window.

Select the **Detach** button to enlarge the window and automatically update the window when another record is selected.

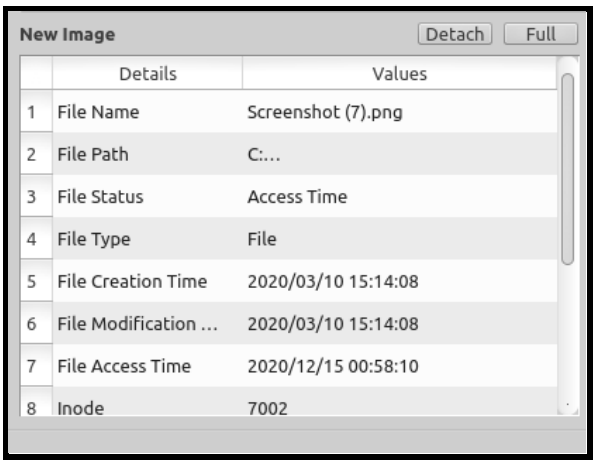
17.6.1.1 New Image

The **New Image** window lists the metadata of the Secondary Snapshot.



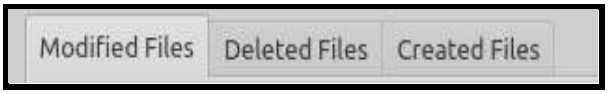
17.6.1.2 Old Image

The **Old Image** window lists the metadata of the Base Snapshot.

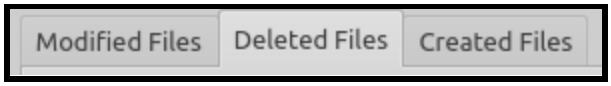


17.6.2 Modified Files

Select the **Modified Files** tab to display files that were changed or altered from the Base Snapshot to the Secondary Snapshot with its metadata.



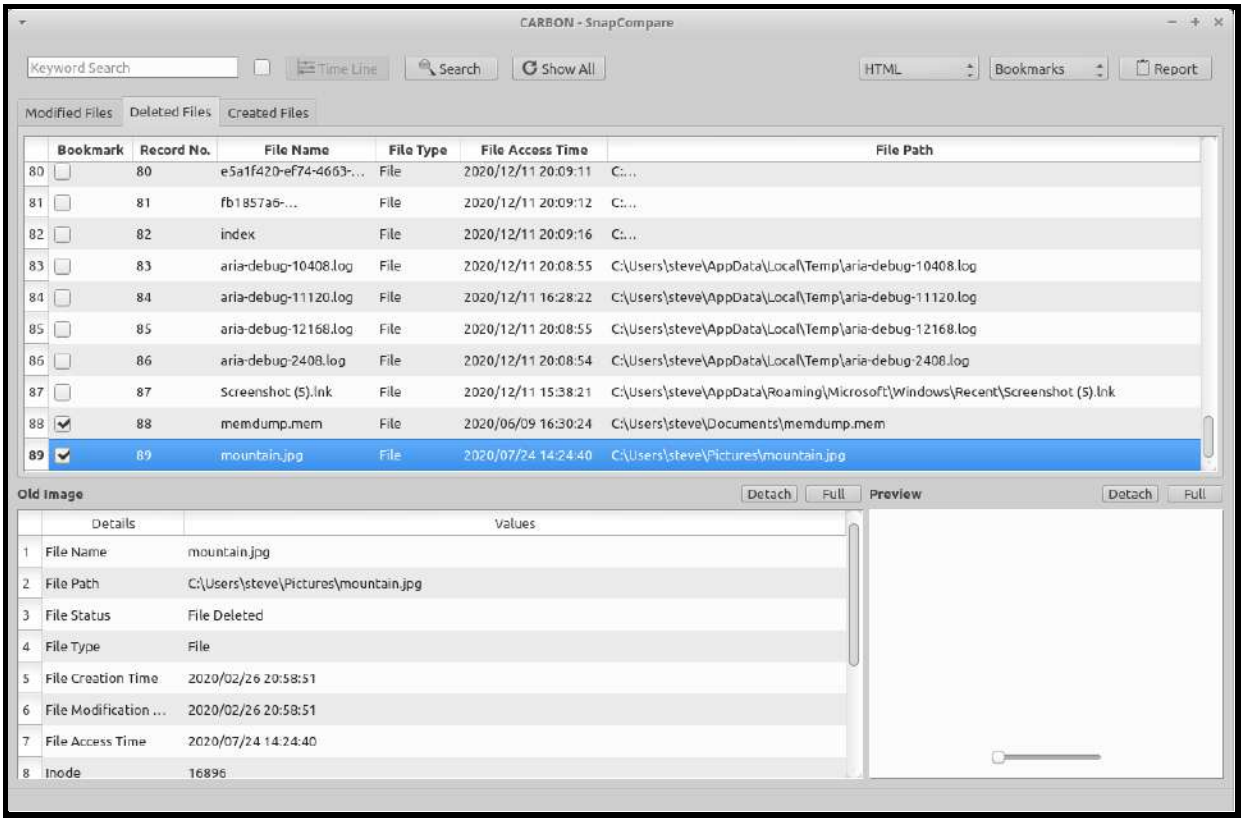
17.6.3 Deleted Files



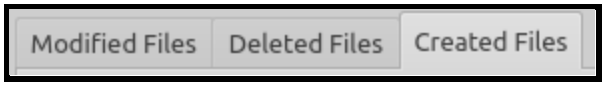
Select the **Deleted Files** tab to show all files deleted from the Secondary Snapshot compared to the Base Snapshot.

The Detailed Information view will only show associated metadata from the Base Snapshot.

In the screenshot below, CARBON lists the deleted .jpg from the Secondary Snapshot and displays its metadata taken from the Base Snapshot.

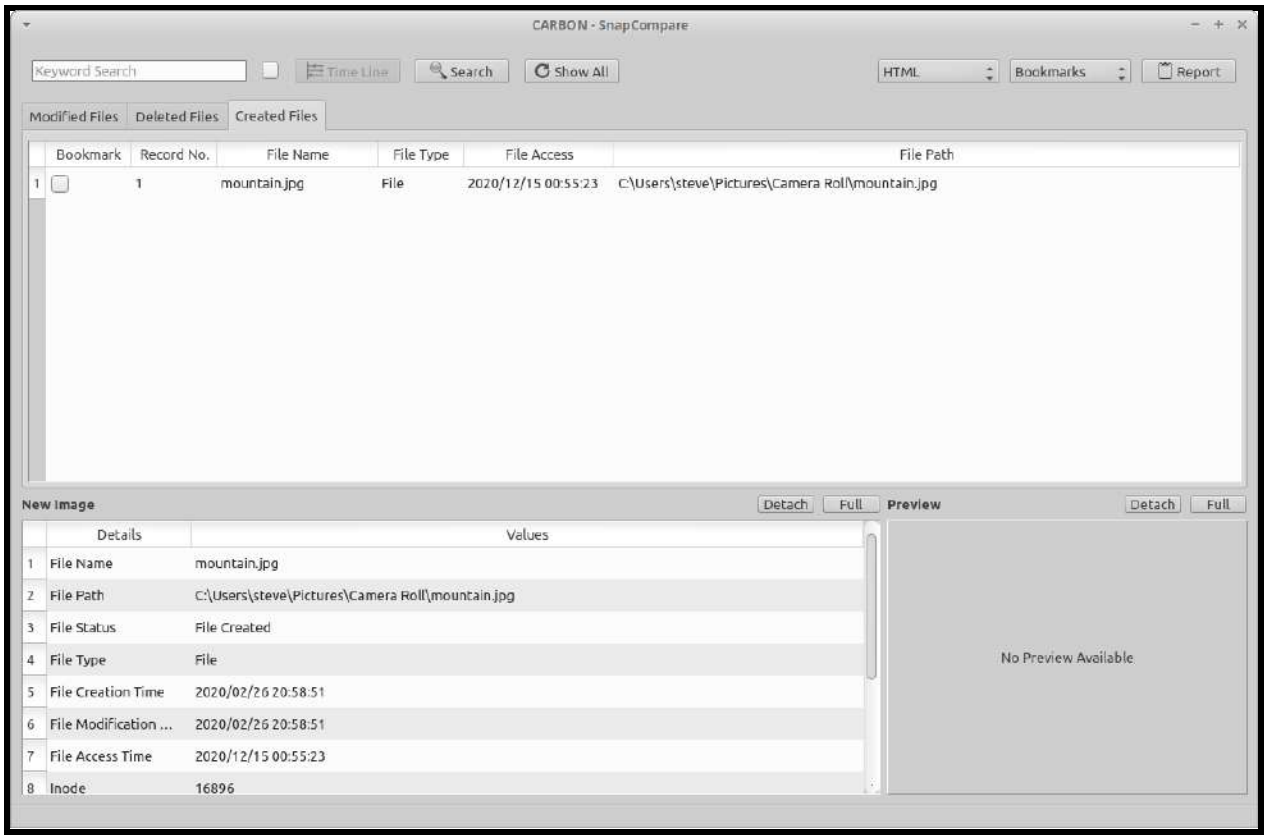


17.6.4 Created Files



Select the Created Files tab to show all files created from the Secondary Snapshot compared to the Base Snapshot.

The Detailed Information view will only show associated metadata from the Secondary Snapshot.



17.6.5 Bookmarking Records

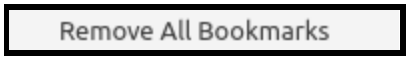
Select multiple artifacts in the first column to Bookmark Deleted Files and Created Files.

17.6.5.1 Bookmark All

Bookmark all results by right-clicking on any record in the Results Window and select **Bookmark All.**

17.6.5.2 Remove All Bookmarks

Right-click on any record and select **Remove All Bookmarks** to uncheck all of the bookmarks at once.

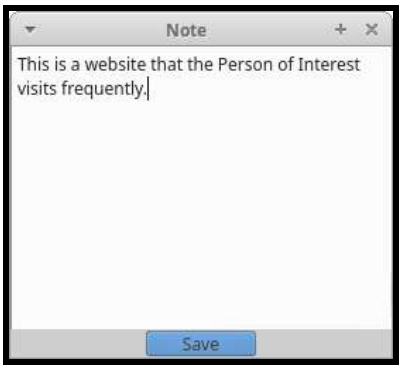


17.6.6 Adding Notes to Records

Right-click on a result record and click **Add Note**.

17.6.6.1 Add Note to Single Record

The Add Note window will open and examiners can add a note to a single Record.



When finished, click **Save**.

17.6.6.2 Add Note to All Bookmarks

Right-click on any record and click **Add Note to Bookmarks**. Bookmark the record before choosing to Add Note to Bookmarks.

When finished, click **Save**.

17.6.7 Exporting Files

Files can be exported by right-clicking and selecting **Export File**.

17.7 Filtering Plugin Records

Examiners can apply two filter options to any displayed results and only show the files they are looking for quickly.

- **Keyword Search** - Allows the examiner to conduct keyword searches quickly within all artifacts
- **TimeLine** - Allows an examiner to refine the results of a data query to a specific date range

17.7.1 Keyword Search

Enter a keyword into the Keyword Search bar, and then click the **Search** button.

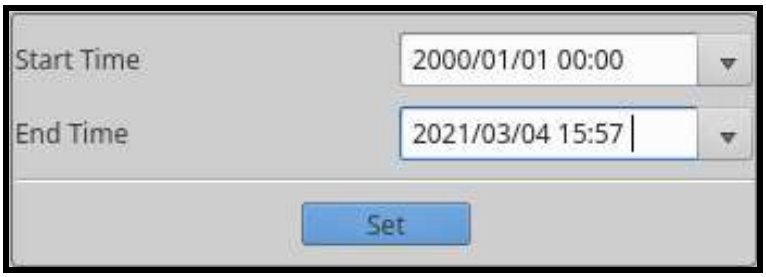
17.7.1.1 Adding Multiple Keywords

Search for multiple terms simultaneously by separating each word with a comma (with no space) and click **Search**. In the screenshot below, multiple search terms can be used at once by separating each word with a comma (i.e. bitcoin,dropbox).

17.7.2 Applying a Timeline

Check the TimeLine box to refine the results of a data query to a specific date range.

Data can be filtered by setting a **Start Time** and an **End Time**. Then, click **Set**.



17.7.3 Show All Records

Click the **Show All** button to refresh the search bar and clear Keyword Search filters.

17.8 Multimedia Preview Window

The Preview window is a multimedia viewer and supports the preview of most audio, video, and images. The Preview Window will show content when a supported file is selected.

There are two options for detaching the Preview window using the buttons at the top.

Click the **Detach** to open a separate Preview window. Information changes when new records are selected.

Click the **Full** button to open a separate Preview window with the current record information only.

17.9 Generating a Report

Reports can easily be generated from the top-right of the SnapCompare Window.

17.9.1 Reporting Formats

Reports can be in HTML or PDF formats that are saved to the output directory.

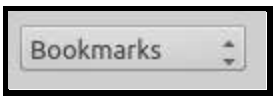
Click on the first dropdown menu to choose the Report Format.

17.9.2 Scope of Report

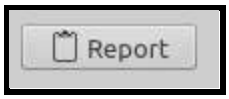
Reporting options include Full Plugin or Bookmarks.

- **Full Plugin** - Includes all of the data in SnapCompare
- **Bookmarks** - Includes only bookmarked results in the report

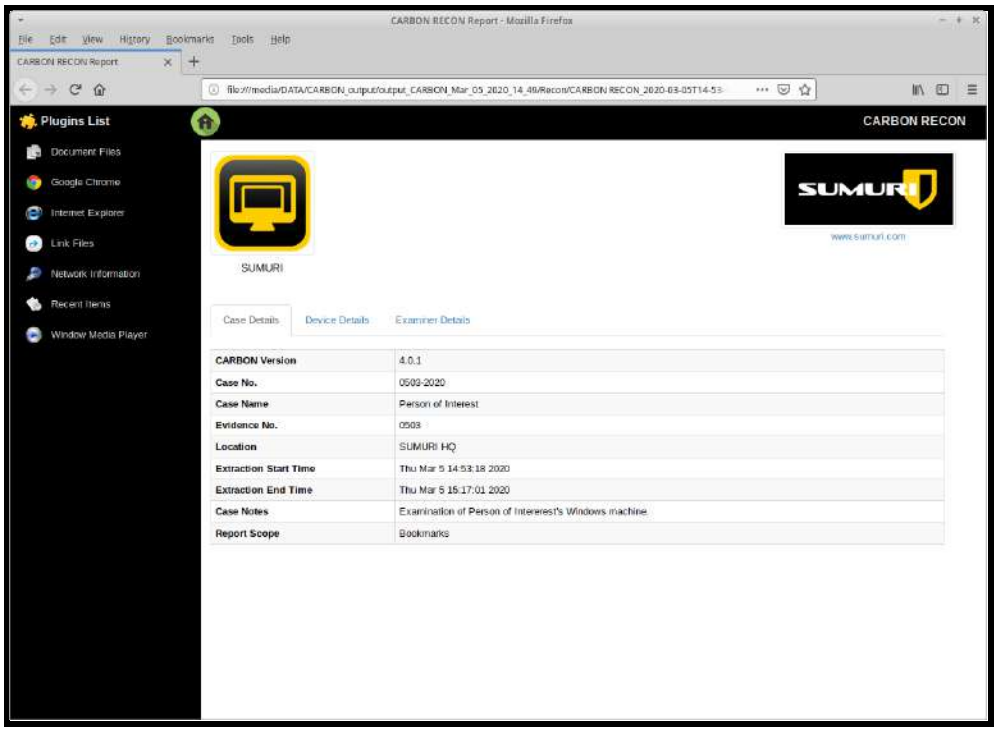
Click on the second dropdown menu to choose the scope of the report.



Click **Report** to generate a report.



The example below is an HTML of the SnapCompare Report that includes only Bookmarks with its Case Details, Device Details, Examiner Details, and Plugin Results.

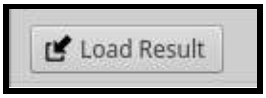


17.9.3 Location of Report

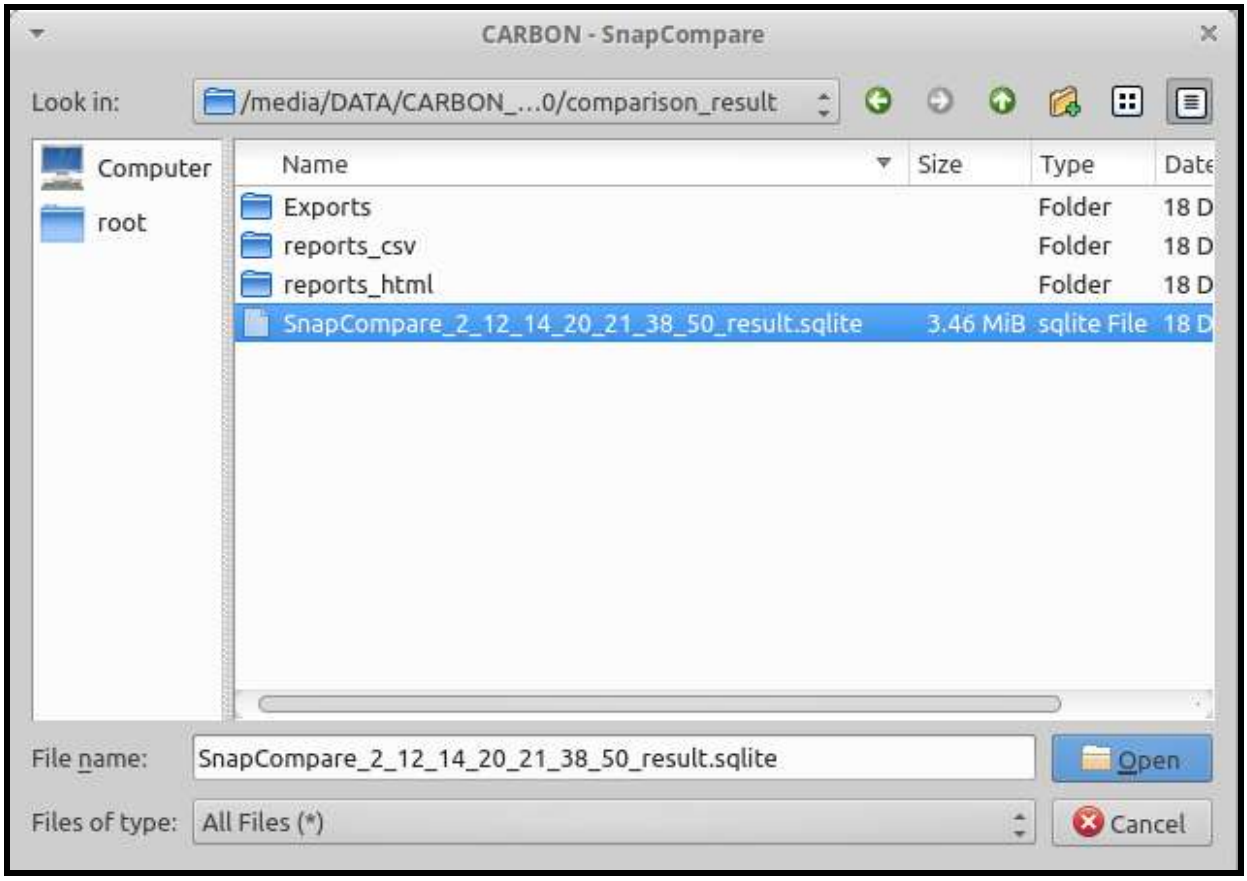
Reports are located in the Output Directory. For more information on the Output Directory, see **Section 8.1**.

17.10 Loading a Previous Result

Select the **Load Result** option at the bottom-left of SnapCompare's Main Interface.



A File Explorer window will appear. Navigate to the case folder, click on the SnapCompare sqlite file, and click **Open**.



18. Advanced File Search

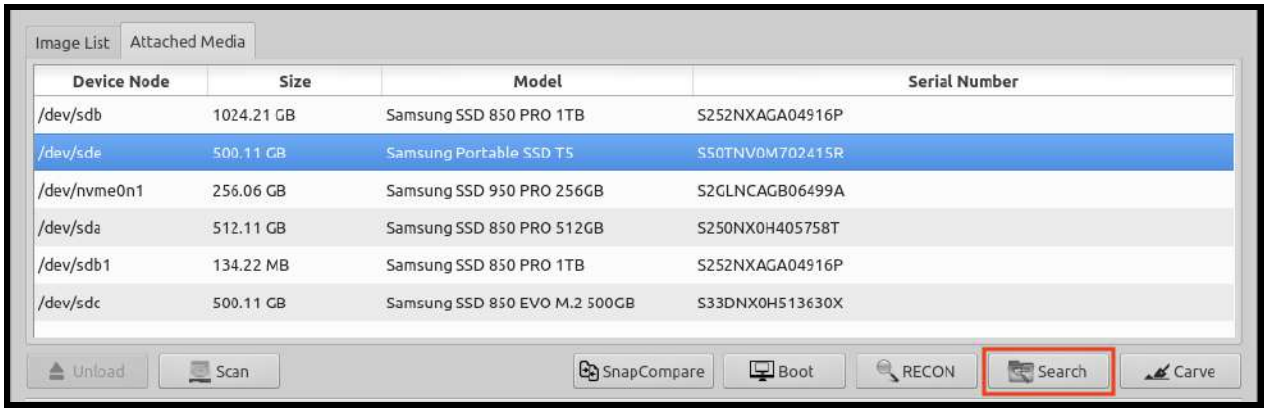
CARBON's File Search can be used to search for file and folder names along with their contents. In addition, CARBON supports all major file signatures for searching.

CARBON has four options available as searching parameters:

- **File Name Search** - Allows the examiner to add terms to find file names
- **Keyword Search** - Allows the examiner to add terms that will search for file contents
- **File Signature Search** - Allows the examiner to use CARBON's preloaded set of file signatures based on common file types
- **Custom Signature Search** - Allows the examiner to add file signatures in either ASCII or Hex with a Custom Offset

18.1 Selecting Media

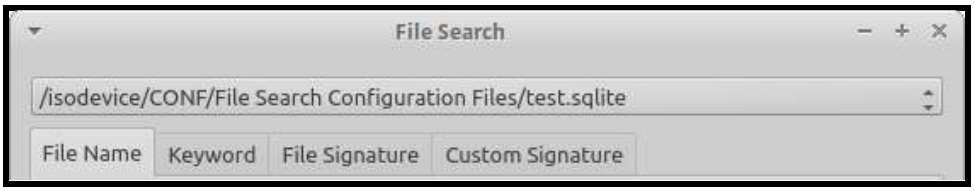
Select the desired source (Image List or Attached Media) to carve using CARBON's Main Interface, and click **Search**.



The **File Search** window will launch.

18.2 Loading a Configuration File

Use the drop-down menu to choose the existing File Search Configuration files created in the File Search Configuration.



*Note: If the File Search window does not display a file, see **Section 11** to create a new File Search Configuration.*

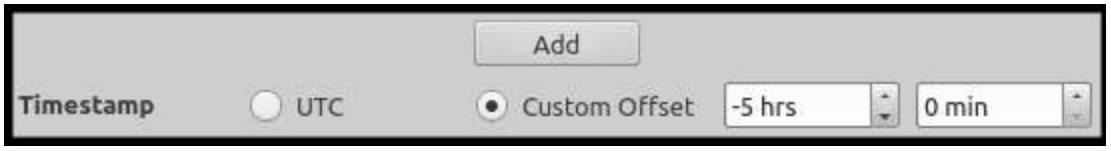
Click the **Add** button to include any additional search parameters based on the current tab outside the File Search Configuration.

18.3 Timestamp Options

Choose the preferred **Timestamp** format for the search (**UTC** or a **Custom Offset**).

18.4 Custom Offset Options

Custom Offset allows the examiner to set a timezone by inputting the offset of the desired timezone.



18.5 Output Directory

The File Search window lists the **Output Directory** with the location of the search results.

Note: The examiner can only change the output directory by restarting CARBON and setting a new output directory. See ***Section 8.1*** *for more information.*

18.6 Detail Window

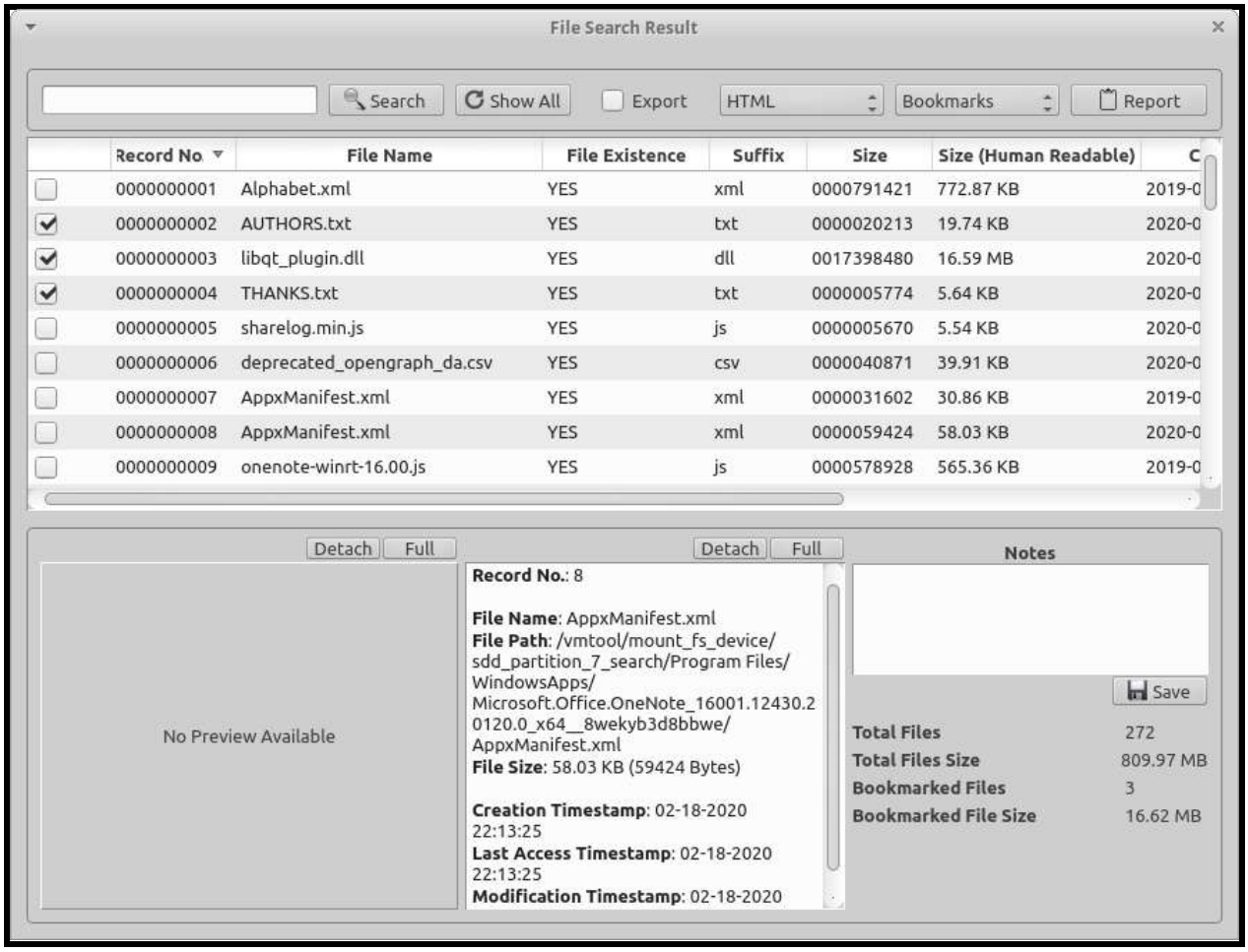
The Detail Window automatically displays information about the selected media.

18.7 Starting the Advanced File Search

After selecting the search parameters, click **Start**, and CARBON will search for files and build results.

18.8 Results Window

The following is an example of the File Search Result window.



The first column with the checkbox can be used to bookmark a record.

- **Record No.** - This is a unique identifier assigned to a record by CARBON.
- **File Name** - The name of the file
- **File Existence** - This shows if the file still exists on the source
- **Suffix** - The File Signature associated with the file
- **Size** - Size of the file in Bytes
- **Size (Human Readable)** - Size of the file in a human-readable format (KB, MB, GB, TB, etc.)
- **Creation TS** - Timestamp for when the file was created
- **Last Access TS** - Timestamp for when the file was last accessed

- **Modification TS** - Timestamp for when the file was last modified

18.8.1 Keyword Search

Enter a keyword into the Keyword Search bar, and then click the **Search** button.

18.8.1.1 Adding Multiple Keywords

Search for multiple terms simultaneously by separating each word with a comma and no space (i.e. dog,cat,van) for a quick search.

18.8.1.2 Resetting Results (Show All)

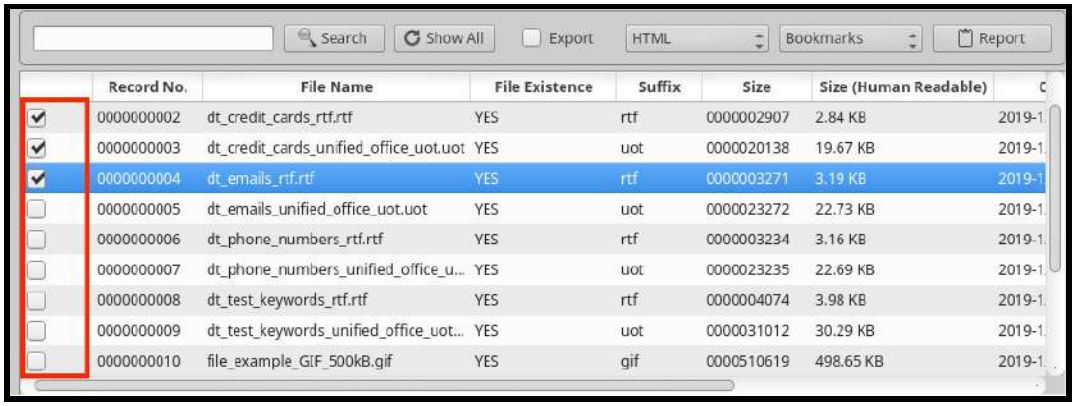
Click the **Show All** button to refresh the search bar and clear keyword search filters.

18.8.2 Bookmarking

Bookmarks are the easiest way to mark items of interest in CARBON. The examiner can bookmark all records or individual records.

18.8.2.1 Adding a Bookmark

To bookmark a file, **check the box** next to the file in the first column. Files can also be bookmarked via the right-click option or using the “Spacebar.”



To track the number of bookmarked files, check the **Results Summary** in the bottom-right corner of the window.

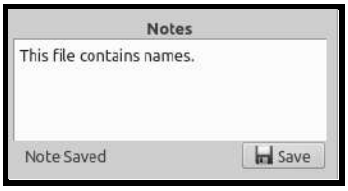
18.8.2.2 Bookmarking All Results

Right-click on a record and select **Bookmark All** to bookmark all results.

18.8.2.3 Removing all Bookmarks

Right-click on a record and select **Remove All Bookmarks** to deselect all results.

18.8.3 Adding Notes



Add notes to individual bookmarks by selecting the desired file and inserting any information in the Notes window. After adding the notes, click **Save**.

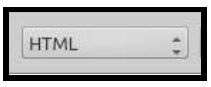
Notes will appear attached to each file in the auto-generated report.

18.8.4 Generating a Plugin Report

Reports can easily be generated from the Results Window.

18.8.4.1 Reporting Formats

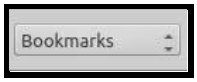
Reports can either be in HTML or PDF format and are saved to the output directory.



Click on the first dropdown button to choose the desired reporting format.

18.8.4.2 Scope of Report

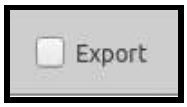
Reporting options include Bookmarks, Screen Items, or the Full module.



- **Bookmarks** - Includes only bookmarked File Search results in the report
- **Screen Items** - Includes only File Search results displayed on the screen
- **Full** - Includes all File Search results in the report

Click on the second dropdown button and choose the scope of the report.

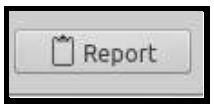
18.8.4.3 Including Exported Files in Report



Check the **Export** box to export the associated files in the File Search's output directory. Exporting also includes the Exported File Details and File Preview in the report. Not checking the export box will only include File Details in the report.

18.8.4.4 Saving a Report

Click **Report** after bookmarking all the items of interest and selecting the Report options.

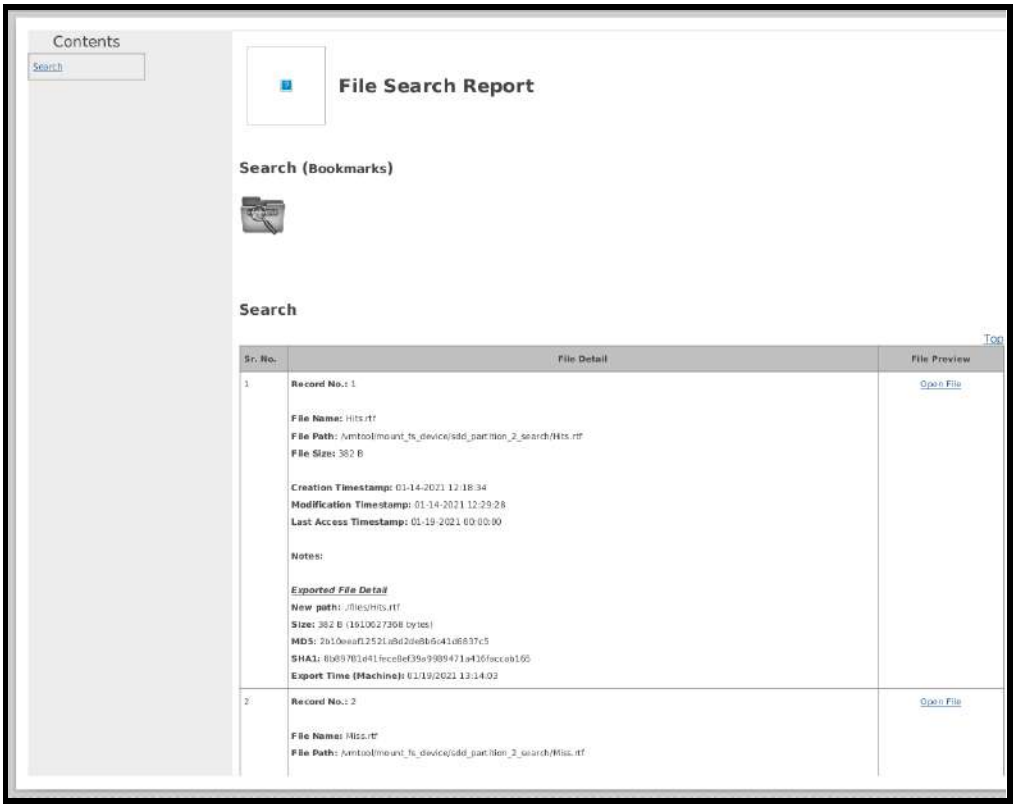


CARBON will generate the report and ask if the examiner would like to open the report.

The example below is a PDF of File Search Report that includes only Bookmarks with its File Details, Exported File Details, and File Preview.

18.8.4.5 Location of Report

Reports will be saved in the **Output Directory** listed in **Section 18.5** located in a Plugin Report folder.



19. Carving Data

Data carving is an integral part of the data recovery process that allows examiners to locate deleted files using file signatures.

CARBON has three options available for data carving:

- **File Carving** - carve data from a single file
- **Carving Unallocated Space** - carves the unallocated space of the attached media or image

- **Carving “Complete Space” (Physical)** - carves ALL of the Selected Image/Device, including the unallocated space

CARBON has two carving options:

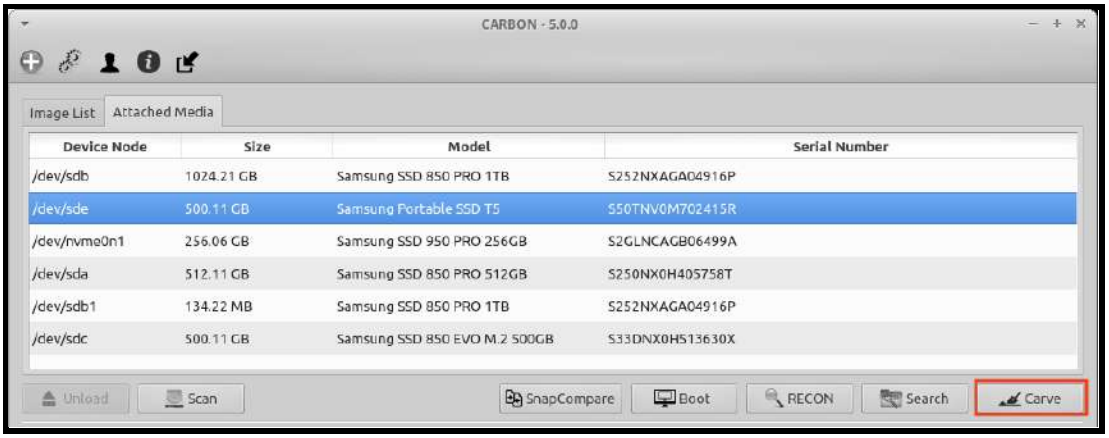
- **Built-in File Signatures** - a preloaded set of carving signatures based on common file types
- **Custom File Signatures** - allows examiners to set their own file type signatures to find proprietary files

The carving results will be displayed based on the carving parameters to quickly see each file type with a log file to show all the events during the carving session.

Log files contain the file name, extension, offset size, and exported file path for each carved file and a “sublog” in every file type directory. They also include SHA1 and MD5 hashes to identify each file.

19.1 Selecting Media

Select the desired source (imported images or attached media) to carve in CARBON’s Main Interface, and click **Carve** to begin. The **CARBON - Carver** window will launch.

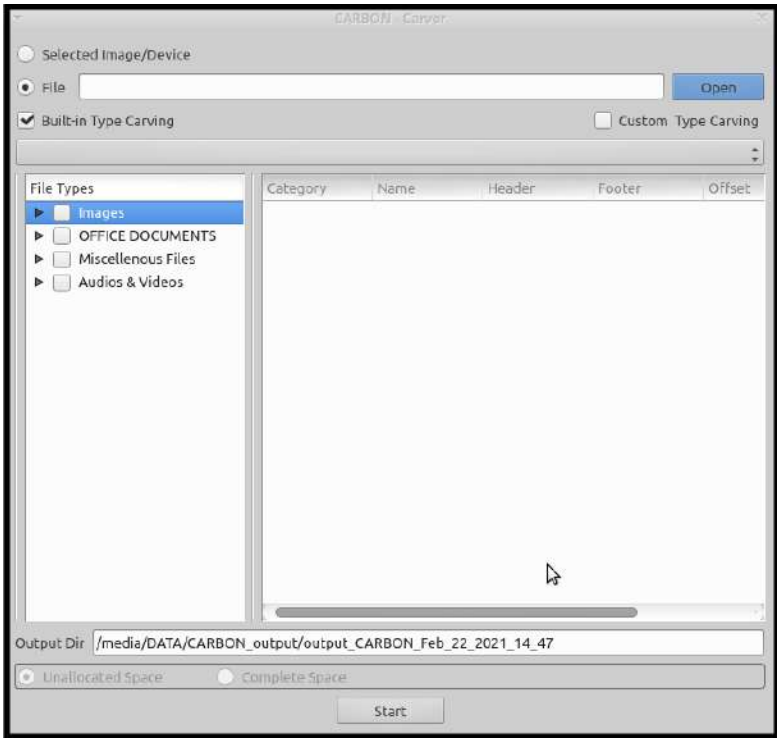


19.2 Selecting a File to Carve

Inside the Carver window,examiners have two options for file carving parameters. Choose either **Selected Image/Device** to carve data of the whole source or **File** to carve a specific file in the source.

Selected Image/Device - Carves the Unallocated Space or “Complete Space” (Physical) of an Image or Attached Drive

File - Carves different file types that are contained in a singular file (i.e., a word document that contains images and text will have the images and the text outputted separately)



19.3 Selecting a Custom Configuration File

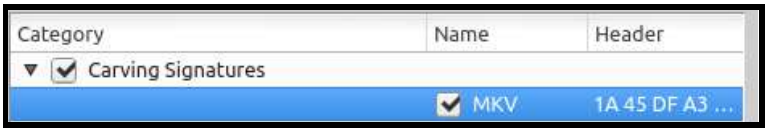
Select Custom Type Carving to use custom file type signatures created in the File/Custom Carving Configuration.

Note: Configure the Custom Type Carving option via the File/Custom Carving Configuration. For more information, see ***Section 11*****.**

19.4 Using Built-In Carving

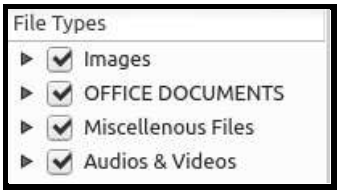
Select **Built-in Type Carving** to use CARBON's preloaded set of file signatures to carve based on common file types.

19.4.1 Activating File Categories



When selected Custom Type Carving, select the desired custom **Carving Signatures** listed under Category to carve.

19.4.2 Activating File Types



When selected Built-In Carving, select the desired preloaded set of **file signatures** listed under File Types to carve.

19.5 Setting Output Directory

Check if the **Output Directory** is correct to review results.

Note: The examiner can only change the output directory by restarting CARBON and setting a new output directory. See **Section 8.1** *for more information.*

19.6 Carving Unallocated Space

Check **Unallocated Space** to carve the unallocated space of the selected attached media or image.

19.7 Carving Allocated Space

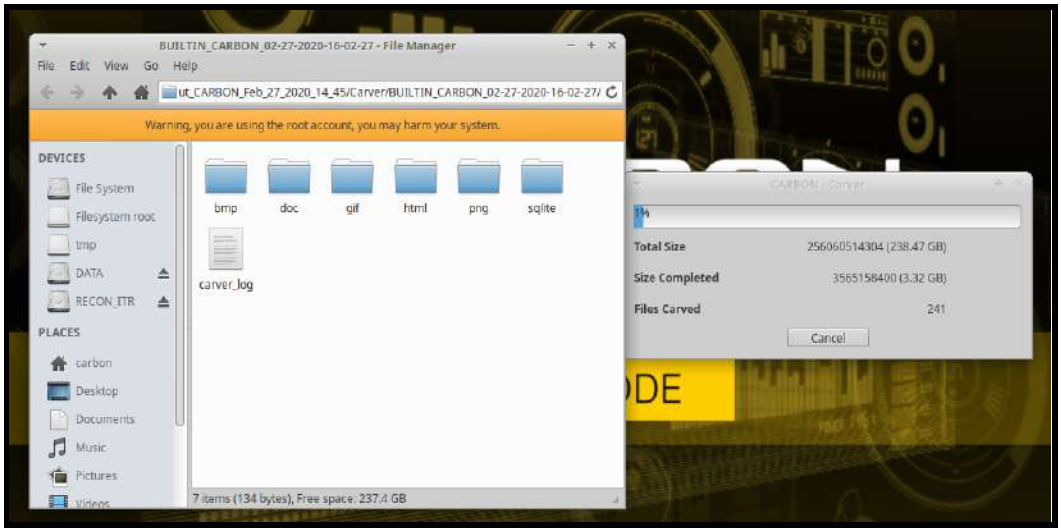
Check **Complete Space** to carve all of the selected attached media or image including unallocated space.

19.8 Start

After selecting the scope and carving settings, click **Start**, and CARBON will begin to carve for files and build results.

19.9 Reviewing Results

During the carving process, a window will appear with the live results and log file for analysis. Results can be found in the output directory selected during the initial setup of CARBON.



20. Terms and Conditions

CARBON

Copyright 2018-2021 – SUMURI LLC

www.sumuri.com

IMPORTANT! PLEASE READ CAREFULLY. THIS IS A LICENSE AGREEMENT.

This CARBON is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. This CARBON is licensed, not sold.

End-User License Agreement

This End User License Agreement (“EULA”) is a legal agreement between you (either an individual or a single entity) and SUMURI LLC with regard to the copyrighted software (herein referred to as CARBON or ‘software’) provided with this EULA. The CARBON includes computer software, the associated media, printed materials, and any ‘online’ or electronic documentation. Use of any software and related documentation (‘software’) provided to you by CARBON in whatever form or media, will constitute your acceptance of these terms unless separate terms are provided by the software supplier, in which case certain additional or different terms may apply. If you do not agree with the terms of this EULA, do not download, install, copy or use the software. By installing, copying or otherwise using the CARBON, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, SUMURI LLC is unwilling to license the CARBON to you.

Eligible License – This software is available for license solely to software owners, with no right of duplication or further distribution, licensing, or sub-licensing.

License Grant – SUMURI LLC grants to you a personal, non-transferable and non-exclusive right to use the copy of the software provided with this EULA. You agree you will not copy or duplicate the software. You agree that you may not copy the written materials accompanying the software. Modifying, translating, renting, copying, transferring or assigning all or part of the software, or any rights granted hereunder, to any other persons and removing any proprietary notices, labels or marks from the software is strictly prohibited. Furthermore, you hereby agree not to create derivative works based on the software. You may not transfer this software.

Copyright – The software is licensed, not sold. You acknowledge that no title to the intellectual property in the software is transferred to you. You further acknowledge that title and full ownership rights to the software will remain the exclusive property of SUMURI LLC and/or its suppliers, and you will not acquire any rights to the software, except as expressly set forth above. All copies of the software will contain the same proprietary notices as contained in or on the software. All title and copyrights in and to the CARBON (including but not limited to any images, photographs, animations, video, audio, music, text and "applets," incorporated into the CARBON), the accompanying printed materials, and any copies of the CARBON, are owned by SUMURI LLC. The CARBON is protected by copyright laws and international treaty provisions. You may not copy the printed materials accompanying the CARBON.

Reverse Engineering – You agree that you will not attempt, and if you are a corporation, you will use your best efforts to prevent your employees and contractors from attempting to reverse compile, modify, translate or disassemble the software in whole or in part. Any failure to comply with the above or any other terms and conditions contained herein will result in the automatic termination of this license and the reversion of the rights granted hereunder to SUMURI LLC.

Disclaimer of Warranty – The software is provided 'AS IS' without warranty of any kind. SUMURI LLC and its suppliers disclaim and make no express or implied warranties and specifically disclaim the warranty of merchantability, fitness for a particular purpose and non-infringement of third-party rights. The entire risk as to the quality and performance of the software is with you. Neither SUMURI LLC nor its suppliers warrant that the functions contained in the software will meet your requirements or that the operation of the software will be uninterrupted or error-free. SUMURI LLC is not obligated to provide any updates to the software for any user who does not have a software maintenance subscription.

Limitation of Liability – SUMURI LLC's entire liability and your exclusive remedy under this EULA shall not exceed the price paid for the software if any. In no event shall SUMURI LLC or its suppliers be liable to you for any consequential, special, incidental or indirect damages of any kind arising out of the use or inability to use the software, even if SUMURI LLC or its supplier has been advised of the possibility of such damages, or any claim by a third party.

Rental – You may not loan, rent, or lease the software.

Transfer – You may not transfer the software to a third party without written consent from SUMURI LLC and written acceptance of the terms of this Agreement by the transferee. Your license is automatically terminated if you transfer the software without

the written consent of SUMURI LLC. You are to ensure that the software is not made available in any form to anyone not subject to this Agreement. A transfer fee of $150 USD will be charged to transfer the software (not applicable to transfers associated with orders from distributors, or resellers or intra-company transfers).

Upgrades – If the software is an upgrade from an earlier release or previously released version, you now may use that upgraded product only in accordance with this EULA. If the CARBON is an upgrade of a software program that you licensed as a single product, the CARBON may be used only as part of that single product package and may not be separated for use on more than one computer.

OEM Product Support – Product support for the CARBON is provided by SUMURI LLC. For product support, please call SUMURI LLC. Should you have any questions concerning this, please refer to the address provided in the documentation.

No Liability for Consequential Damages – In no event shall SUMURI LLC or its suppliers be liable for any damages whatsoever (including, without limitation, incidental, direct, indirect, special and consequential damages, damages for loss of business profits, business interruption, loss of business information, or other pecuniary loss) arising out of the use or inability to use this 'SUMURI LLC' product, even if SUMURI LLC has been advised of the possibility of such damages. Because some states/countries do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

Indemnification By You – If you distribute the Software in violation of this Agreement, you agree to indemnify, hold harmless and defend SUMURI LLC and its suppliers from and against any claims or lawsuits, including attorney's fees that arise or result from the use or distribution of the software in violation of this Agreement.

Jurisdiction – The parties consent to the exclusive jurisdiction and venue of the federal and state courts located in the State of Delaware, USA, in any action arising out of or relating to this Agreement. The parties waive any other venue to which either party might be entitled by domicile or otherwise.