Automatic Eforensic Analysis System

User Manual & Technical Documentation

Contents

Introduction to AEAS

The Automatic Eforensic Analysis System (AEAS) provides a collection of eForensic scanning features requiring minimal configuration, and a scriptable interface to reduce the repetitive manual labour of eForensic analysis.

AEAS will interrogate a disk image to find:

- Image hash
- Partition information
- Deleted files
- Renamed files
- Carved files
- Files containing keywords
- A timeline of file timestamps

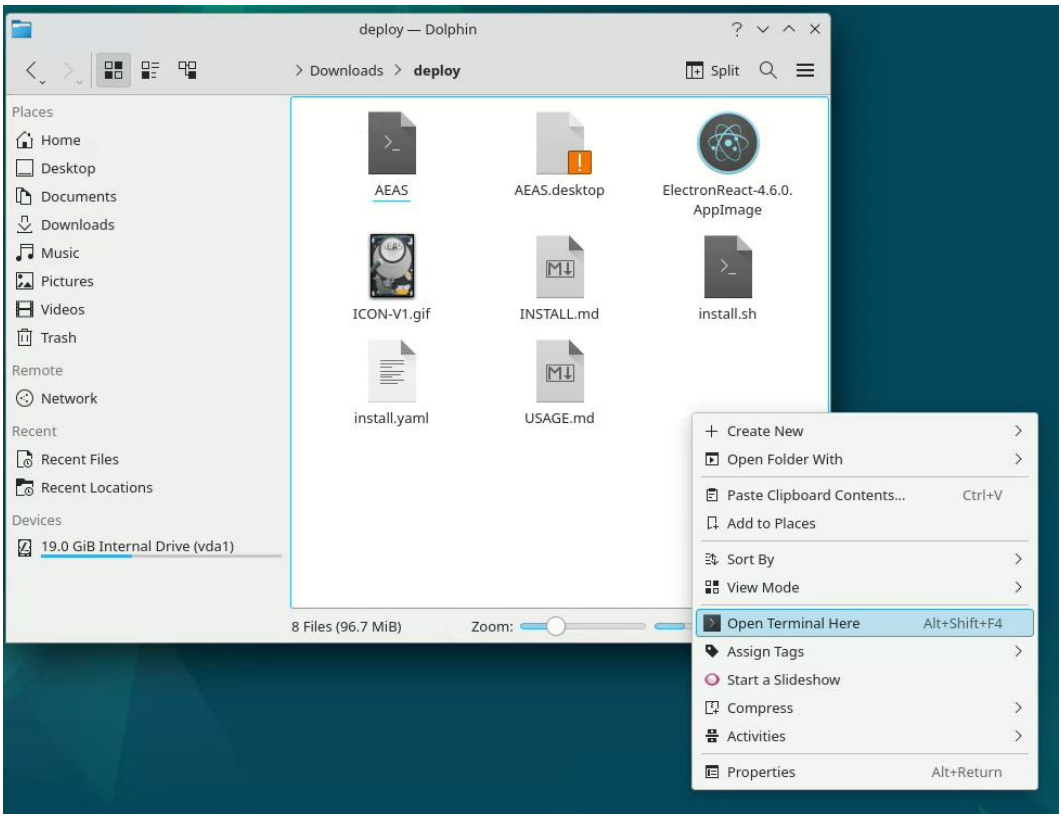
This document contains the information needed to install and operate AEAS on your Debian 12 system.

Installation of AEAS

Before you install AEAS, ensure that your target machine is running Debian 12. For your convenience it is also recommended to use a desktop environment that you are comfortable with, as AEAS should work on all popular desktop environments.

AEAS is provided with a convenient installation script (install.sh) that will pull in all necessary dependencies and install AEAS on your system. To begin the installation process, extract the provided ZIP file. Ensure to take note of where you extract these files.

Next, open a command-line terminal to the folder where the files were extracted – in most desktop environments, this can be done by right clicking inside the folder within the file manager, and selecting the option like “open a terminal here”

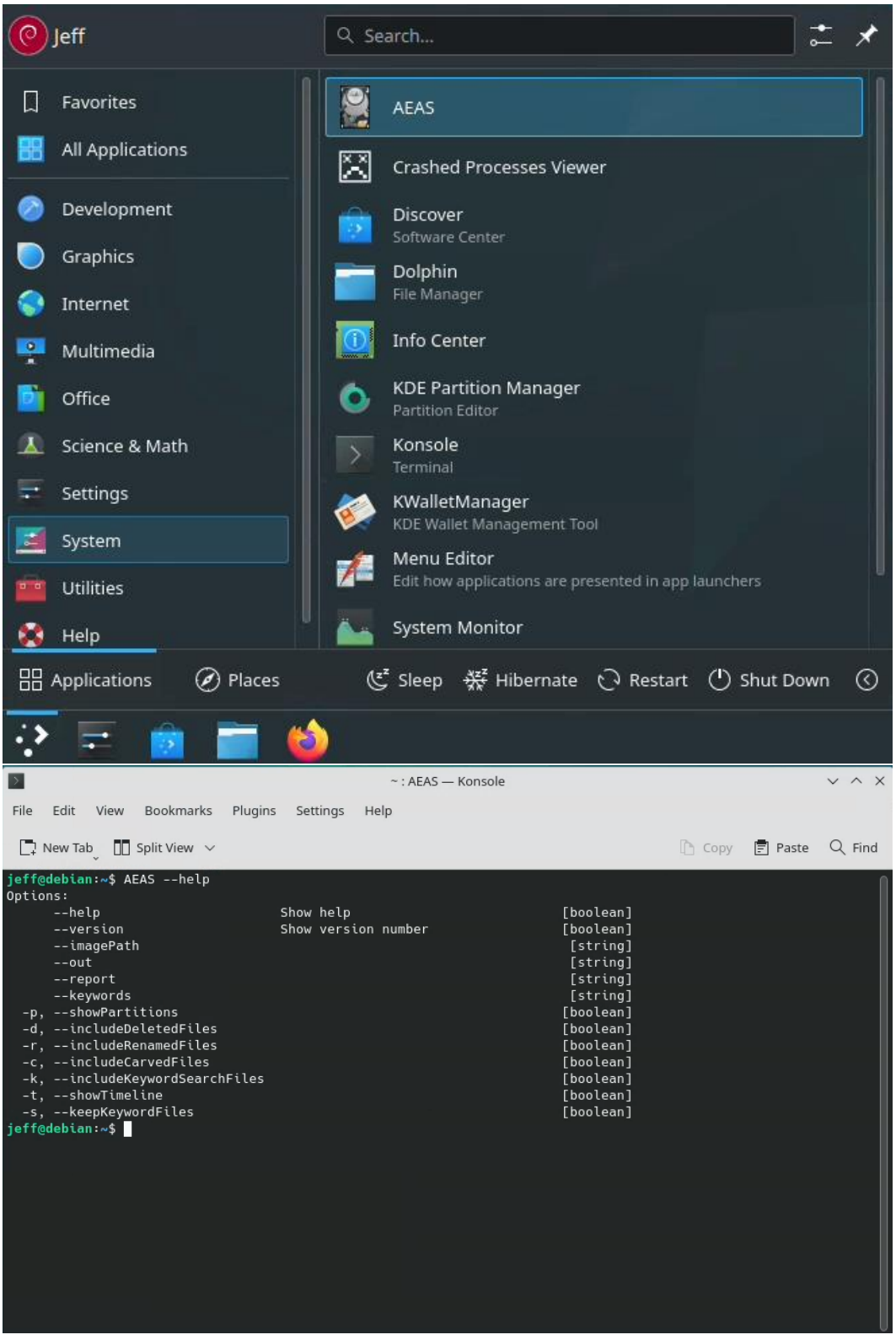


Within the terminal window ensure that the “install.sh” script is marked as executable. This can be done by running the command “chmod +x install.sh”. After this you should be able to run the script with the command “./install.sh”. Installation of AEAS will require superuser privileges, so enter your password when asked to do so.

This process may take some time as the script will install all of the dependencies required for AEAS to function correctly, this is usually around 5 minutes. When the process is complete, you will receive a message stating that this is the case, and the terminal will have returned to the usual command-line prompt.

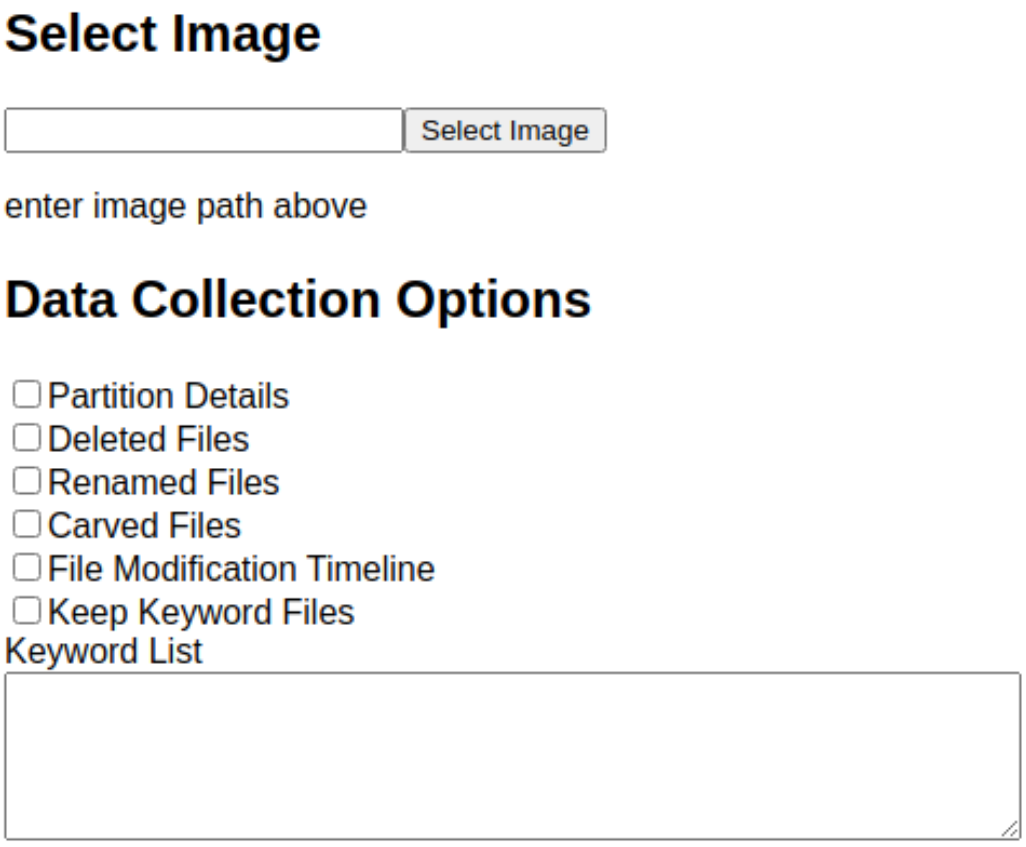
We recommend rebooting your system at this stage as the operating system may not update the start menu correctly, making the program inaccessible.

You may now start the program from either the start menu, or command line interface as shown in the screenshots below.



Starting an analysis

To start an analysis of a support disk image, you may either manually enter a path to the image in the text box or use the button to the right of the box to browse for a path. Using the file browser is the recommended way of doing this however it may be easier to manually enter the path to the image if you are working on the same file repeatedly or it is otherwise stored in a path that is more difficult to reach with a file browser.



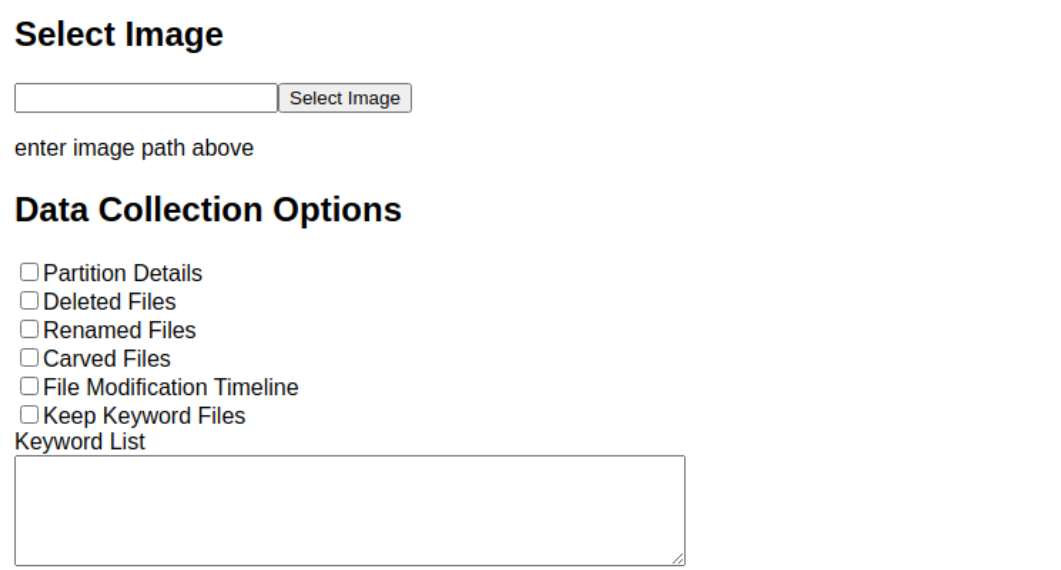
The message below the prompt to select an image will alert you if the disk image is a supported format. AEAS supports the following disk image formats:

Image Format	Extension	Notes
Encase Image File Format / Expert Witness Format	.E01	
Raw	.dd .img ...	Raw image formats can have a variety of extensions. AEAS will detect these based on support of the underlying library, so the extension matching is not critical.
ZIP	.zip	ZIP files are supported if they contain a valid forensic image. AEAS will automatically extract this compressed image and perform a normal check and analysis against it

It is generally recommended to use raw disk images where possible as these will reduce the amount of preprocessing, and often hold a complete bit-for-bit copy of the entire disk, which will lead to a more complete analysis.

Analysis options

The checkboxes on the first screen can be used to control what information will be included in the final report. Additionally, a short summary of what each checkbox does is included down the bottom of the window whenever an option is hovered over with the mouse. A summary of these is included below.



Option	Description
Partition Details	This will include a table showing all disk partitions found on the disk image, including their size and type
Deleted Files	This will include a summary of files that have been marked as deleted on the disk image, as well as some information about the file.
Renamed Files	This will include a summary of files whose extension does not match the expected file type – a technique often used to hide files. This will show the extension present on disk as well as what the extension should be based on the files' content.
Carved Files	This will include files that were detected without proper meta data structures on disk, requiring carving techniques to be used to locate them.
File Modification Timeline	This will include a timeline of files whose modification history can be traced via shell history files. Note: This will only work on operating system disk images extracted from Linux hosts.
Keep Keyword Files	This option is slightly different in that it does not modify the output of the report, but instead decides whether AEAS should keep a copy of files found on the disk with keyword matches.

Starting the Analysis

Once you are happy with your selection options, you only need to click the “Go” button in the top right-hand corner of the window to start the analysis. If the button is greyed out, the provided disk image may require some pre-processing. Once this is complete the button will become active again, and the analysis can begin. The status of the analysis is shown in the bottom left-hand corner. When the analysis is complete, the report will be automatically displayed on the window.

Viewing the report

Once the disk has been analysed, you will be shown a report that includes the items that were selected on the previous screen. It is important to note that the report will change depending on which items you select to include, however below is an example of a complete report with an explanation of all items that are included.

AEAS Generated Report

Image:

This is the path to the image that you specified on the previous screen, if the image was extracted from a ZIP file this will be the path to the automatically extracted image, and not the path to the ZIP file itself

Timezone: If the disk image was taken from the system drive of a Linux-based operating system, the timezone will show up automatically here.

Image Hash

File	This is the same path as shown above
MD5 Hash	These are the hashes that were computed for the file. These are used to verify the integrity of the evidence (a hash is usually provided with the evidence), as well as to ensure that no changes are made during the analysis
SHA1 Hash	

Image Hash Post Analysis

File	This should be exactly the same as the table above
MD5 Hash	These are the hashes computed after the analysis has finished, if they have changed in any way it indicates that the disk image has been changed in some way during the AEAS' analysis
SHA1 Hash	

The result of the comparison between the hashes before and after analysis will be shown here for your convenience.

File Info

Partition Table

<table>
<tr><td colspan="4">Table Type: This is the partition table format used on the disk. The most common two are MBR (DOS) and GPT, with MBR being used by older operating systems and GPT being used by more modern ones</td></tr>
<tr><td colspan="4">Sector Size: This is the size of each sector on the disk. A sector is the smallest physical storage unit on the disk. For a forensic analysis, sector size is used to get data from an arbitrary position on disk (rather than the byte offset). This is relevant to you if you wish to perform further analysis with traditional forensic tools</td></tr>
<tr><td>Description</td><td>Start</td><td>End</td><td>Length</td></tr>
<tr><td>This is the partition type of the given partition. This is a byte at the beginning of the partition and is used by the operating system to determine how the disk should be handled. This may give some insight in to where the evidence originated – such as the origin operating system</td><td colspan="3">Thes describe the start, end and size of each partition in sectors (not bytes!). This is also useful if the user wishes to perform a manual forensic analysis against the disk, otherwise they may give an indication of the size of the disk or what partitions are likely to contain user data vs bootloader or recovery environment data.</td></tr>
</table>

Keyword Matched Files

These are files that were found to contain one or more of the keywords specified by the user.

iNode	File Path	Matched Keyword	Match	Match Offset From Beginning of Disk	Size	MAC Date	Hash
This is the metadata address of the file. This is how the file can be accessed using forensic tools	This is the path to the file on the filesystem. It is how the file would be accessed if the disk were to be mounted and browsed with a file explorer	This is the specific keyword that was found within the file. Can be used to differentiate which files contain which keyword	This is the portion of text that matched with the previous keyword	This is the location on the disk where the keyword was found. It is important to note that this offset is relative to the start of the disk image, rather than the start of the partition	This is the file's size in bytes	This is the modified accessed and created times for the file. Some filesystems do not store one or more of these dates, and thus may show "Invalid Date" in some fields	This is the SHA1 hash of the file. The hash can be used to compare two files found within the report or against the hash of a known file of interest

Renamed Files

These are files whose extension does not match the content of the file. This is a technique commonly used to hide files “in plain sight” (for example renaming a .zip file to .jpg to make it appear less suspicious)

iNode	File Path	True Ext.	Size	MAC Date	Hash
This is the metadata address of the file. This is how the file can be accessed using forensic tools	This is the path to the file on the filesystem. It also shows the file extension that the file is reporting to have	This is the actual filetype that has been detected based on the file’s signature – which is computed from its content	This is the file’s size in bytes	This is the modified accessed and created times for the file. Some filesystems do not store one or more of these dates, and thus may show “Invalid Date” in some fields	This is the SHA1 hash of the file. The hash can be used to compare two files found within the report or against the hash of a known file of interest

Deleted Files

These are files that have been removed from the filesystem, but still have metadata present on the disk.

iNode	File Path	Size	MAC Date	Hash
This is the metadata address of the file. This is how the file can be accessed using forensic tools	This is the path to the file on the filesystem. As the file does not exist on the filesystem anymore this is usually inaccessible by traditional means	This is the file’s size in bytes	This is the modified accessed and created times for the file. Some filesystems do not store one or more of these dates, and thus may show “Invalid Date” in some fields	This is the SHA1 hash of the file. The hash can be used to compare two files found within the report or against the hash of a known file of interest

Carved Files

These are files that no longer have metadata present on the disk and require carving techniques to access.

File Name	Size	Sector	Modified Date	File Type
This is an automatically computed file name. Because the file no longer has any metadata present on disk, the file extension is computed based on the file type	This is the file size in bytes	This is the sector in which the file was found. Can be used to carve the file out of the disk for later analysis.	This is the date that the file was last modified, if it can be detected	This is the suspected file type based on the same signature algorithm as for renamed files

Timeline

This is a timeline of all suspicious files that have been detected in the previous tables. On supported Linux operating system disk images, the timeline will also show the user and operation (command) that was likely responsible for the change to the suspicious file.

Date	iNode	File Name	User	Operation
This is the date that the file was last modified	This is the iNode number that the file is located at	This is the name of the file on the filesystem	This is the user that is likely to have modified the file	This is the command/s that were run that were likely to modify the file

Exporting the Report

There are several formats that are supported to export the report to. JSON is a format used to store objects in a text-based format. This can be used by other programs to view the output of AEAS and parse them for further analysis. CSV is similar in this sense; however, it requires less computation to process and may be more applicable for simple scripts to perform additional analysis. Finally, PDF is a human readable format and can be used by other forensic analysts to visually see a summary of all of the findings generated by AEAS.

Advanced: CLI usage

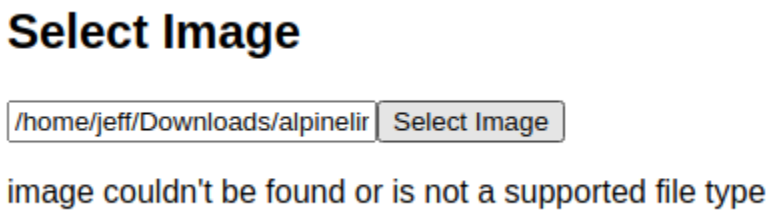
AEAS also provides a command-line interface to allow the output to be scripted into other tools, as well as for use on headless systems. This CLI can be accessed through your terminal with the command “AEAS”. The command “AEAS --help” will show an overview of all the commands that are available

```
jeff@debian:~$ AEAS --help
Options:
      --help                        Show help                          [boolean]
      --version                     Show version number                [boolean]
      --imagePath                                                       [string]
      --out                                                             [string]
      --report                                                          [string]
      --keywords                                                        [string]
  -p, --showPartitions                                                 [boolean]
  -d, --includeDeletedFiles                                            [boolean]
  -r, --includeRenamedFiles                                            [boolean]
  -c, --includeCarvedFiles                                             [boolean]
  -k, --includeKeywordSearchFiles                                      [boolean]
  -t, --showTimeline                                                   [boolean]
  -s, --keepKeywordFiles                                               [boolean]
jeff@debian:~$
```

An image can be passed to the command-line with the option --imagePath <path to your image>. Additionally, the format of the report can be selected with the argument --report <csv,json,pdf>. The folder where this report will be sent to is specified with --out, otherwise the report will be printed to stdout and can be processed by other scripts. It important to note that this is folder where the report will be located, and not the file name for the specific report.

Common Errors

The most common error to occur is that the image does not exist or is an incorrect format.



The easiest way to fix this is to convert the image to a format that is supported, and check that the file you have selected is correct.

Another rarer error is an error with a backend tool. These may occur if the image is corrupted. You can try restarting the application and running the analysis again with different options, however the best solution is to contact the software provider for additional support.

Command failed: icat -o 128 /home/jeff/Downloads/dfr-05-ntfs.dd 71 > .71 Invalid API argument (ntfs_load_attrs: attributes are NULL)