Digital Forensics Tutorials – Analyzing a Disk Image in Kali Autopsy

Explanation Section

About Disk Analysis

Once the proper steps have been taken to secure and verify the disk image, the actual contents of the image must be analyzed for suspicious or incriminating evidence. When looking at the contents of an image, it is necessary to not only look at the clearly visible contents such as folders on the desktop and images in user files, but the image must also be checked for hidden, encrypted, or deleted files. It is always better to assume that a suspect may have known that they were to be investigated and took steps to hide, delete, or otherwise make it difficult to find the information they had been storing on their USB or computer.

About Kali Linux Sleuth Kit and Autopsy

Autopsy and Sleuth Kit are open source digital investigation tools that run on Windows, Linux, OS X, and other Unix systems. Autopsy is the custom front-end application of Sleuth Kit. They can be used to analyze disk images and perform in-depth analysis of file systems (such as NTFS, FAT, Ext3) and several volume system types.

Examiners and analysts can use the Autopsy graphical interface or the Sleuth Kit command line tools to conduct an investigation. In this case, we will be launching the Autopsy graphical interface via the Sleuth Kit command line. Autopsy/Sleuth Kit allow for an examiner to open a .dd or other type of disk image file, hash the file, and search for files and other information contained within the file. It is also possible to produce reports of searches, results, and comments and notes in HTML and Excel.

The following features are available through Autopsy/Sleuth Kit:

- Timeline Analysis - Graphical event viewing interface.
- Hash Filtering - Flag known bad files and ignore known good.
- File System Forensic Analysis - Recover files from most common formats.
- Keyword Search - Indexed keyword search to find files that mention relevant terms.
- Web Artifacts - Extract history, bookmarks, and cookies from Firefox, Chrome, and IE.
- Multimedia - Extract EXIF from pictures and watch videos.
- Email Analysis: Parses MBOX format messages, such as Thunderbird.

In This Tutorial

Once a disk image has been created, hashed, and write-blocked to prevent changes, it is necessary to analyze the image. During the analysis process, the investigator must search for information pertinent to the case being compiled. This means not only looking for current contents on the drive, but also searching for deleted files, missing or hidden information, and hidden partitions that may not appear at first glance. Oftentimes a suspect will attempt to hide and delete information as a precaution. We will be able to see some of this information within Autopsy/Sleuth Kit.

Since Autopsy/Sleuth Kit is a free tool, it is a good option for disk image analysis within Linux, and even Windows systems. In this tutorial we will focus on some of the more basic functions of Autopsy/Sleuth Kit since we only have one file written to our “suspect’s” drive.

Tutorial Section

LEARNING OBJECTIVES:

- Launch Autopsy
- Start a new case and add the appropriate disk image file
- Review the contents of the disk image file
- Print out a basic report
- Use the search feature to search by keyword

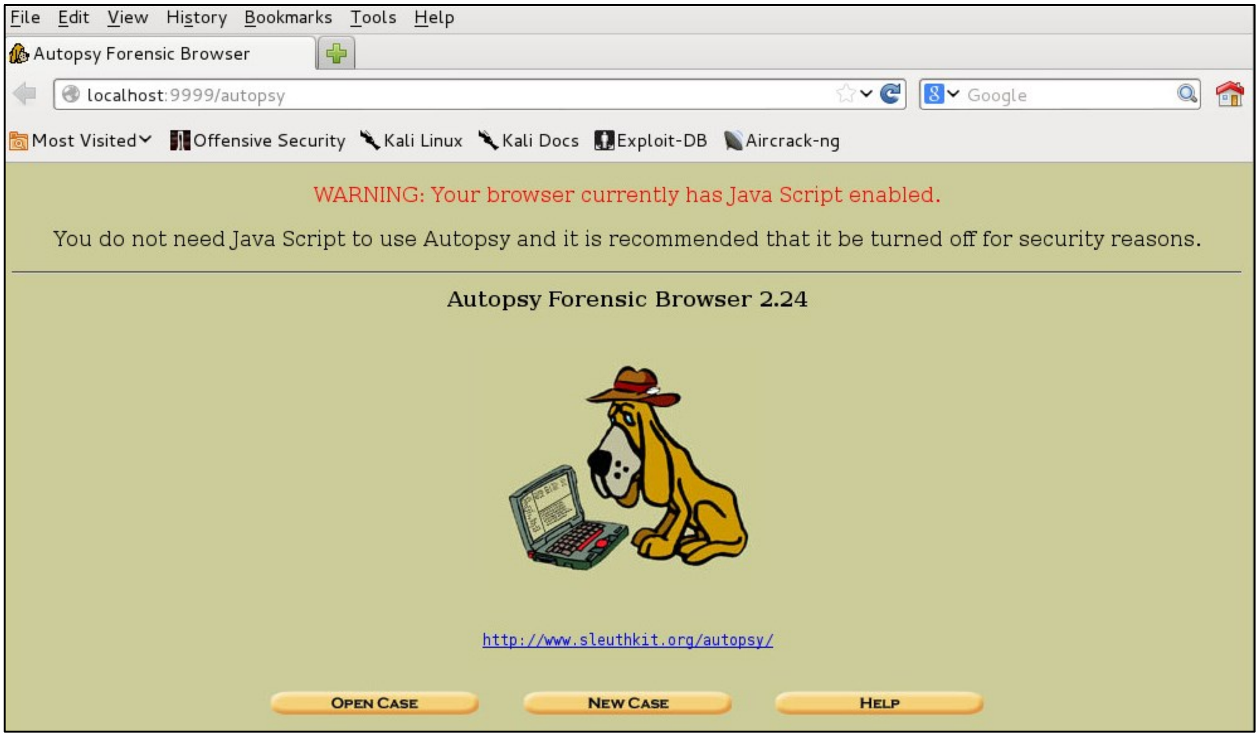
Part 1 – Launch Sleuth Kit/Autopsy

1. Login to the Virtual Lab website (https://v5.unm.edu/cloud/org/ialab), and enter the 'NEST Digital Forensics vApp'. Click on the **Kali Linux machine** to open the VM.

2. At the login screen of the Kali Linux machine use the username **root** and the password **letmein**.

3. Navigate to **Applications>>Kali Linux>>Forensics>>Digital Forensics>>autopsy**.

4. A new window will open. **CTRL + click** on the provided link within the window to launch the **Autopsy Forensic Browser**.



WARNING: Your browser currently has Java Script enabled.

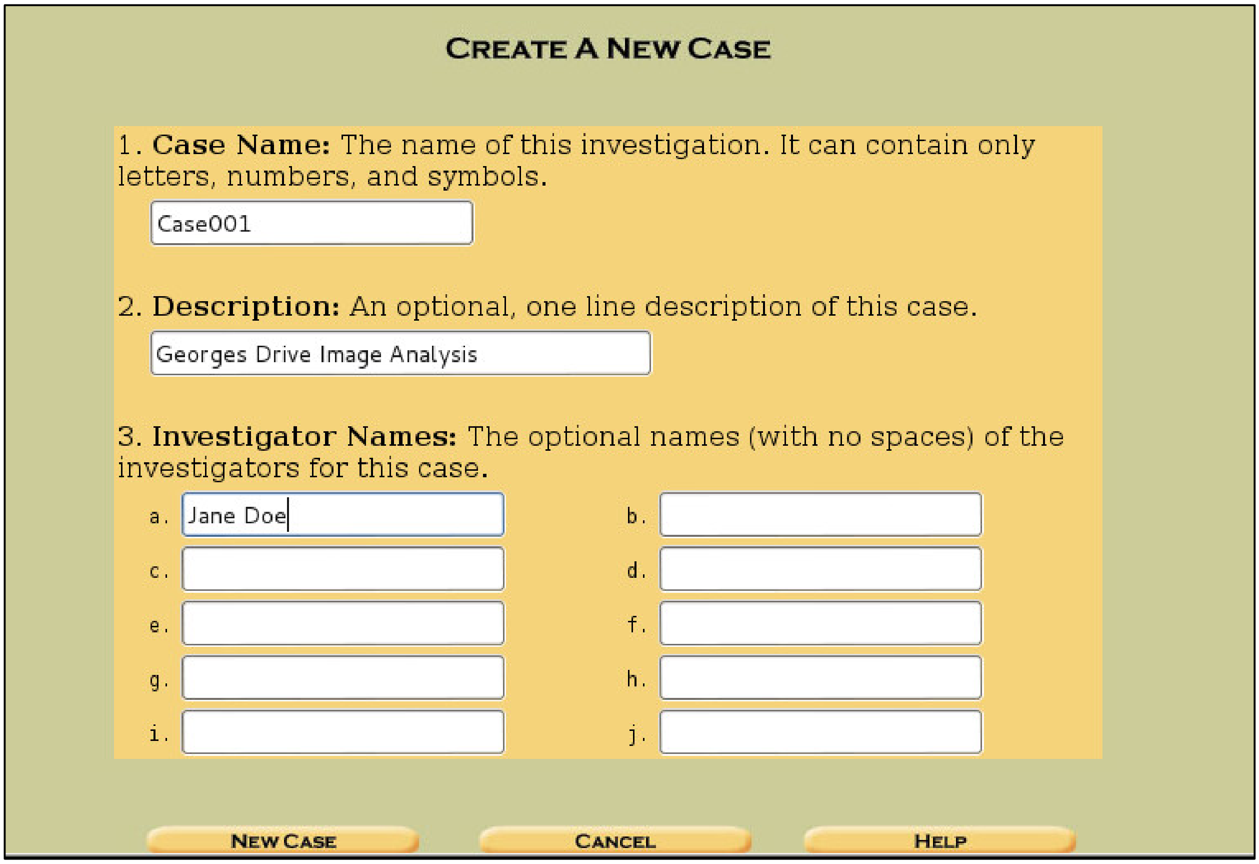
You do not need Java Script to use Autopsy and it is recommended that it be turned off for security reasons.

Autopsy Forensic Browser 2.24

http://www.sleuthkit.org/autopsy/

Part 2 – Create a New Case

1. Click **New Case**. The ‘Create a New Case’ page will open. Fill in the ‘Case Name’, ‘Description’, and ‘Investigator Name’. Then select ‘**New Case**’ near the bottom of the screen.



CREATE A NEW CASE

1. **Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.

Case001

2. **Description:** An optional, one line description of this case.

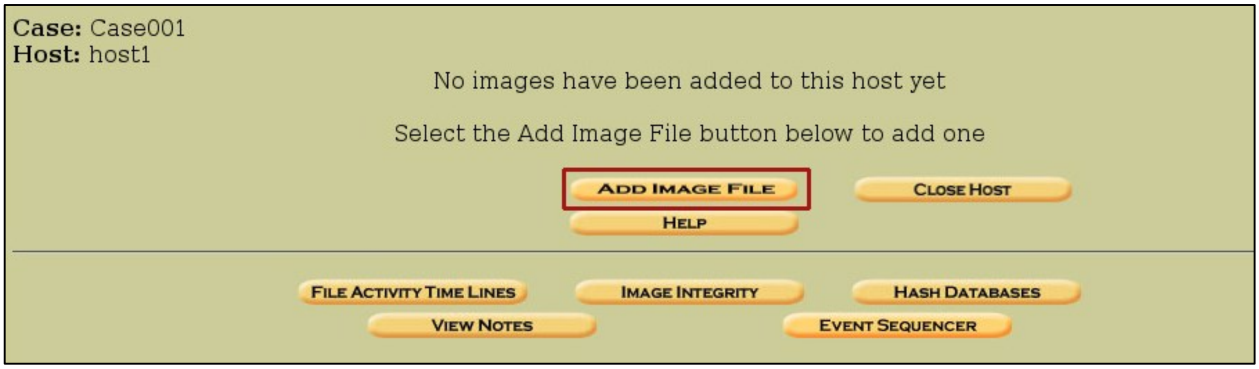
Georges Drive Image Analysis

3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.

a. Jane Doe
b.
c.
d.
e.
f.
g.
h.
i.
j.

2. Click ‘**Add Host**’ on the following page. Leave the defaults on the ‘Add a New Host’ page and select ‘**Add Host**’ at the bottom of the page.

3. On the following page, select ‘**Add Image**’. On the following page, select ‘Add Image File’.

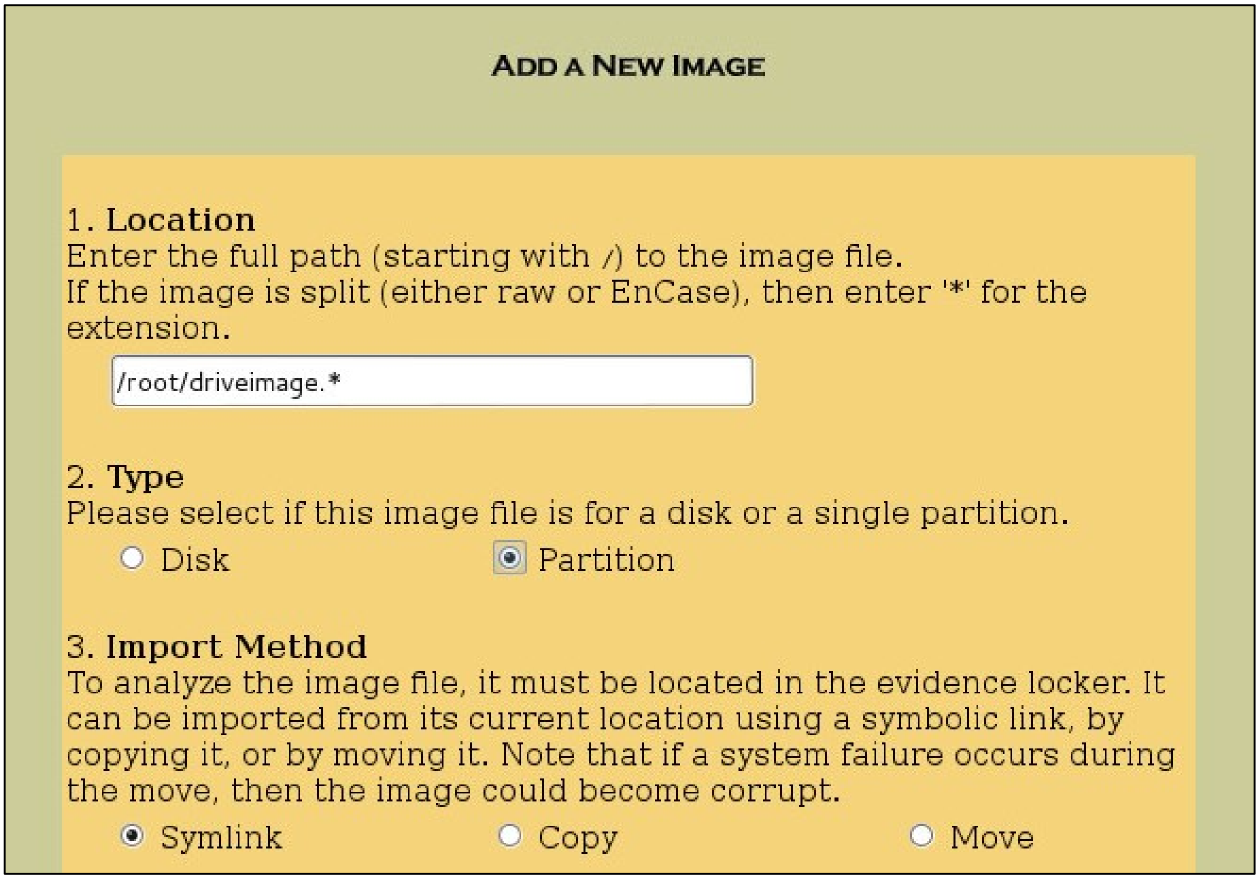


Case: Case001
Host: host1

No images have been added to this host yet

Select the Add Image File button below to add one

4. To add the image file for analysis, enter the path of the image file, /root/driveimage.*. The * will select any file with an appropriate disk image extension. Since this image drive is from one partition, select the ‘Partition’ radio button. Click **Next**.



ADD A NEW IMAGE

1. **Location**
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.

/root/driveimage.*

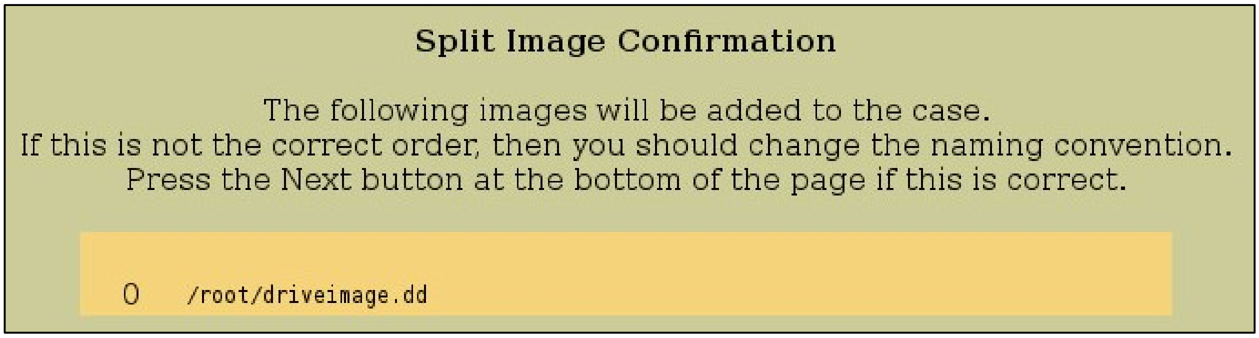
2. **Type**
Please select if this image file is for a disk or a single partition.

○ Disk ● Partition

3. **Import Method**
To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.

● Symlink ○ Copy ○ Move

5. The next page will verify that the correct image file has been selected. Click **Next**.



Split Image Confirmation

The following images will be added to the case.
If this is not the correct order, then you should change the naming convention.
Press the Next button at the bottom of the page if this is correct.

```
0   /root/driveimage.dd
```

6. Select the hashing option on the next page. This will verify the integrity of the disk image, and will allow you to check this hash value against the ones created in the imaging process. Leave the other defaults as they are and click ‘**Add**’.

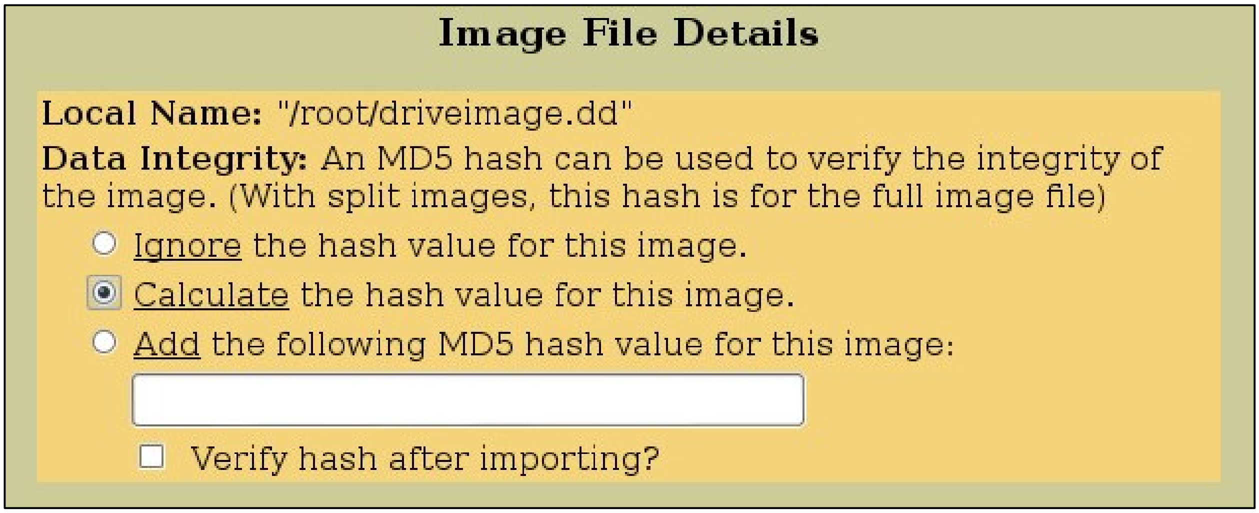


Image File Details

Local Name: "/root/driveimage.dd"

Data Integrity: An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)

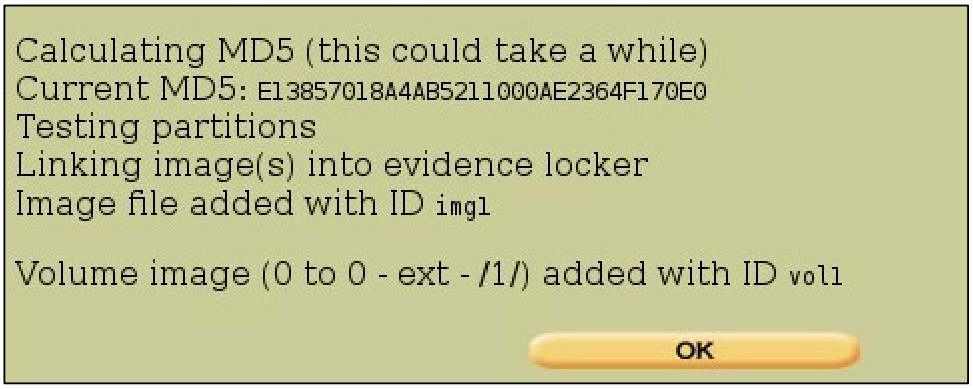
○ Ignore the hash value for this image.

● Calculate the hash value for this image.

○ Add the following MD5 hash value for this image:

□ Verify hash after importing?

7. The hash may take a moment to calculate, especially if the disk image file is large. The hash value will be printed out. Be sure to copy it a text file for comparison. Click **OK**.

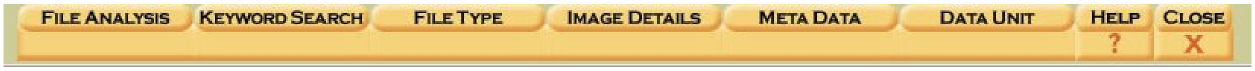


```
Calculating MD5 (this could take a while)
Current MD5: E13857018A4AB5211000AE2364F170E0
Testing partitions
Linking image(s) into evidence locker
Image file added with ID img1

Volume image (0 to 0 - ext - /1/) added with ID vol1
```

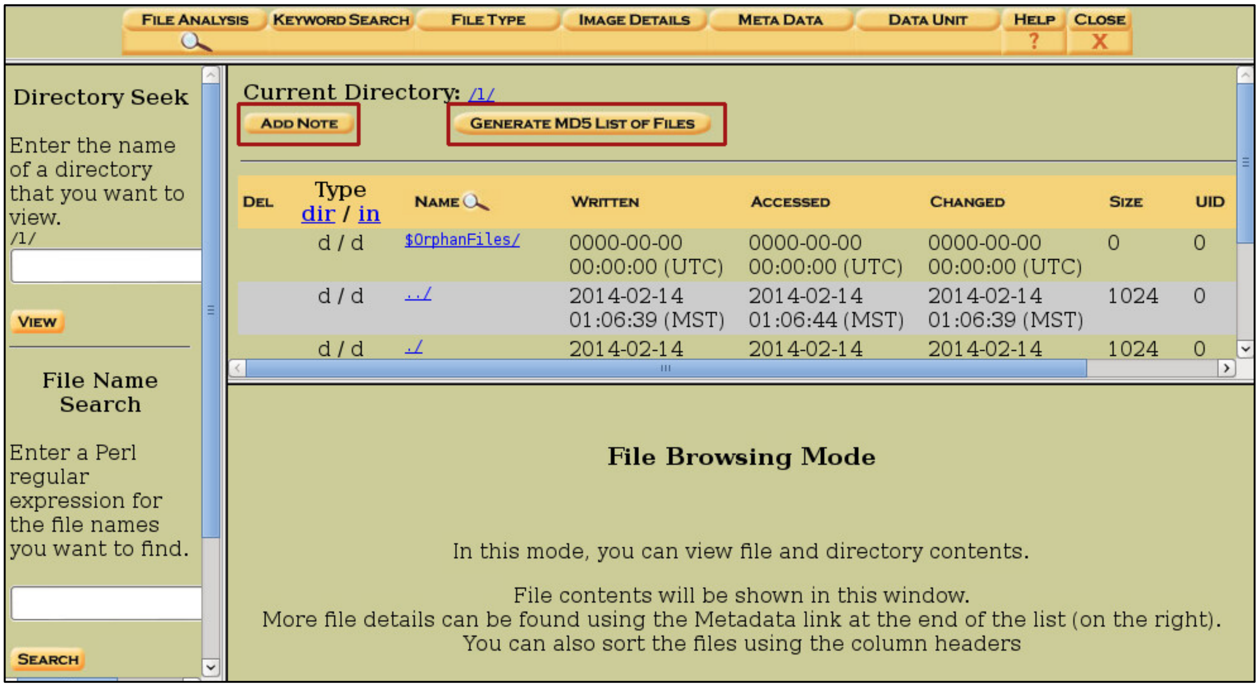
Part 3 – Analyze the Image File

1. On the following page, click '**Analyze**'. Note the other possible options, such as 'View Notes', 'File Activity Time Lines', 'Event Sequencer', and 'Image Integrity'.
    - Image Integrity allows you to verify the hash value of the image file at any time.
    - File Activity Time Lines allows you to create a timeline of file activities. This is highly useful, as it provides a report of exactly what was found on the image file.
    - Event Sequencer allows you to add new events in the course of the investigation

2. To complete the file analysis, select one of the tabs from the top of the screen. Start with '**File Analysis**'.



3. A new window will open that displays the full contents of the disk image file. Since there is only one file on this partition, it will not take long to display. Note that to make hashing easier, there is an option to make an md5 list of all files on the image file. It is also possible to add a note at this point.


File Analysis
Keyword Search
File Type
Image Details
Meta Data
Data Unit
Help
Close
Directory Seek
Enter the name of a directory that you want to view.
/1/
View
File Name Search
Enter a Perl regular expression for the file names you want to find.
Search
Add Note
Generate MD5 List of Files

Current Directory: /1/

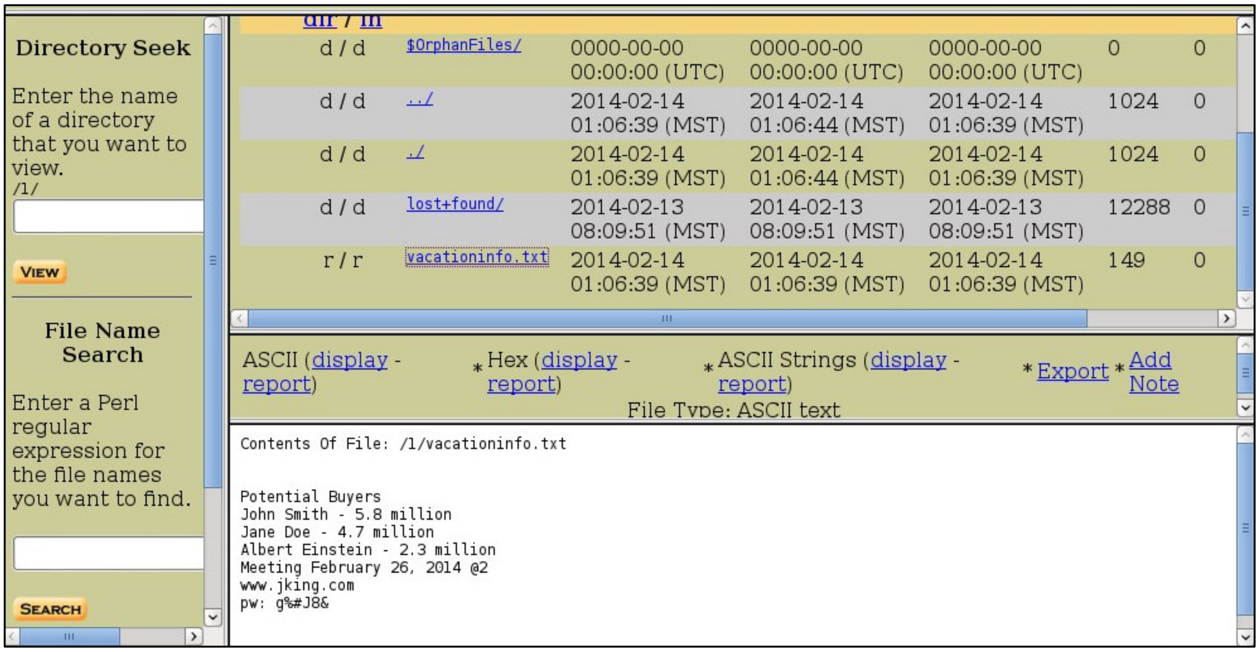
Del	Type dir / in	Name	Written	Accessed	Changed	Size	UID
	d / d	$OrphanFiles/	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0	0
	d / d	../	2014-02-14 01:06:39 (MST)	2014-02-14 01:06:44 (MST)	2014-02-14 01:06:39 (MST)	1024	0
	d / d	./	2014-02-14	2014-02-14	2014-02-14	1024	0

File Browsing Mode

In this mode, you can view file and directory contents.

File contents will be shown in this window.
More file details can be found using the Metadata link at the end of the list (on the right).
You can also sort the files using the column headers

4. Scroll down to find our file, ‘**vacationinfo.txt**’. Click on the file. Notice that the contents of the file will populate in the space below. You can also view information about the file, including the size, when it was created, the last time it was accessed, and the last time it was changed. In the next section, you will create a basic report about this file.


Directory Seek
Enter the name of a directory that you want to view.
/1/
View
File Name Search
Enter a Perl regular expression for the file names you want to find.
Search
ASCII (display - report)
* Hex (display - report)
* ASCII Strings (display - report)
* Export * Add Note

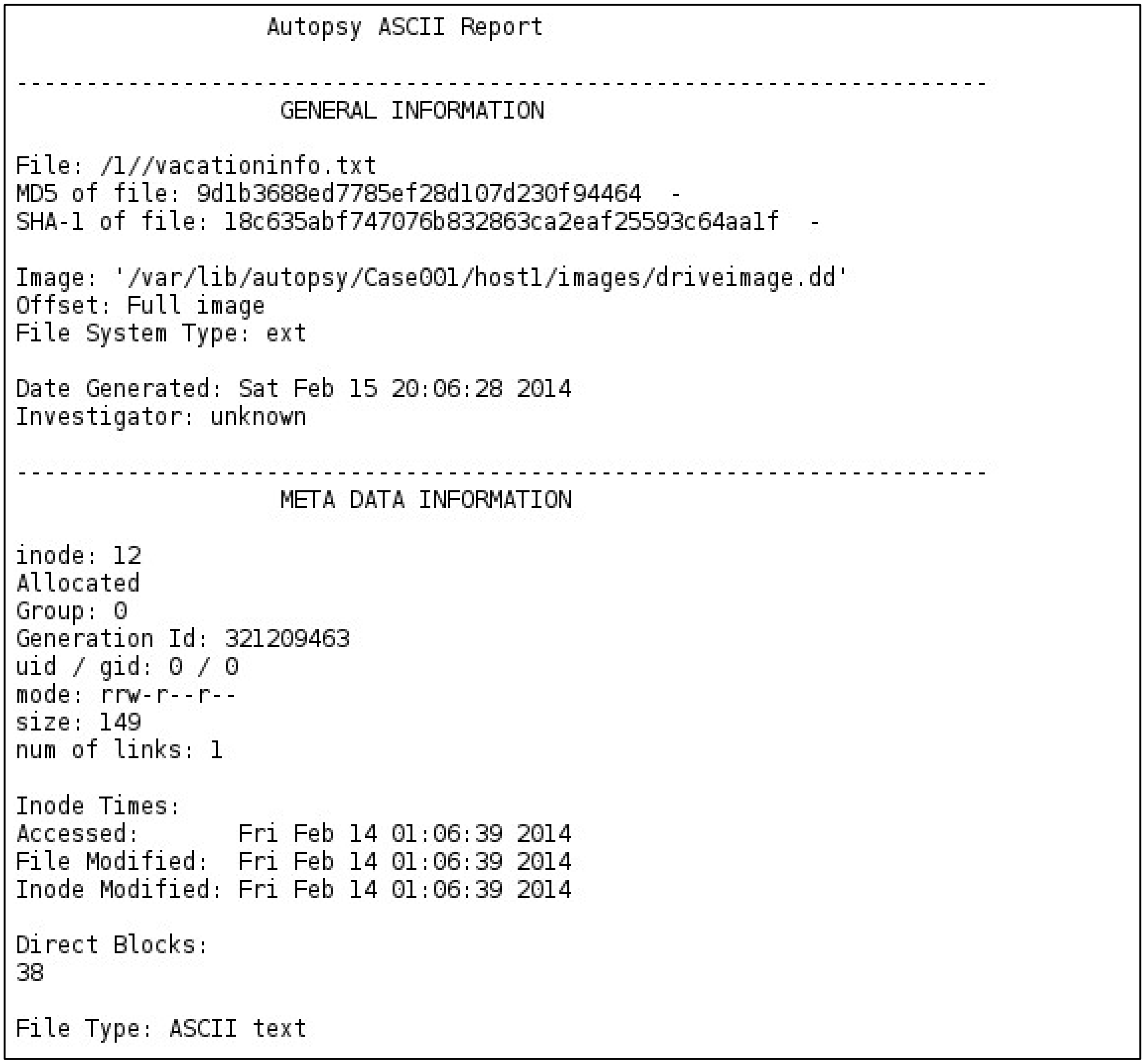
Type dir / in	Name	Written	Accessed	Changed	Size	UID
d / d	$OrphanFiles/	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0	0
d / d	../	2014-02-14 01:06:39 (MST)	2014-02-14 01:06:44 (MST)	2014-02-14 01:06:39 (MST)	1024	0
d / d	./	2014-02-14 01:06:39 (MST)	2014-02-14 01:06:44 (MST)	2014-02-14 01:06:39 (MST)	1024	0
d / d	lost+found/	2014-02-13 08:09:51 (MST)	2014-02-13 08:09:51 (MST)	2014-02-13 08:09:51 (MST)	12288	0
r / r	vacationinfo.txt	2014-02-14 01:06:39 (MST)	2014-02-14 01:06:39 (MST)	2014-02-14 01:06:39 (MST)	149	0

File Type: ASCII text

```
Contents Of File: /1/vacationinfo.txt


Potential Buyers
John Smith - 5.8 million
Jane Doe - 4.7 million
Albert Einstein - 2.3 million
Meeting February 26, 2014 @2
www.jking.com
pw: g%#J8&
```

Part 4 – Create a Basic Report with Autopsy

1. From the analysis page, it is possible to create a report about a file that can be used for later easy access. Click on ‘**ASCII report**’. This will create an easy-to-read report with all the information about ‘**vacationinfo.txt**’. Right click this report to save it as a .txt file.

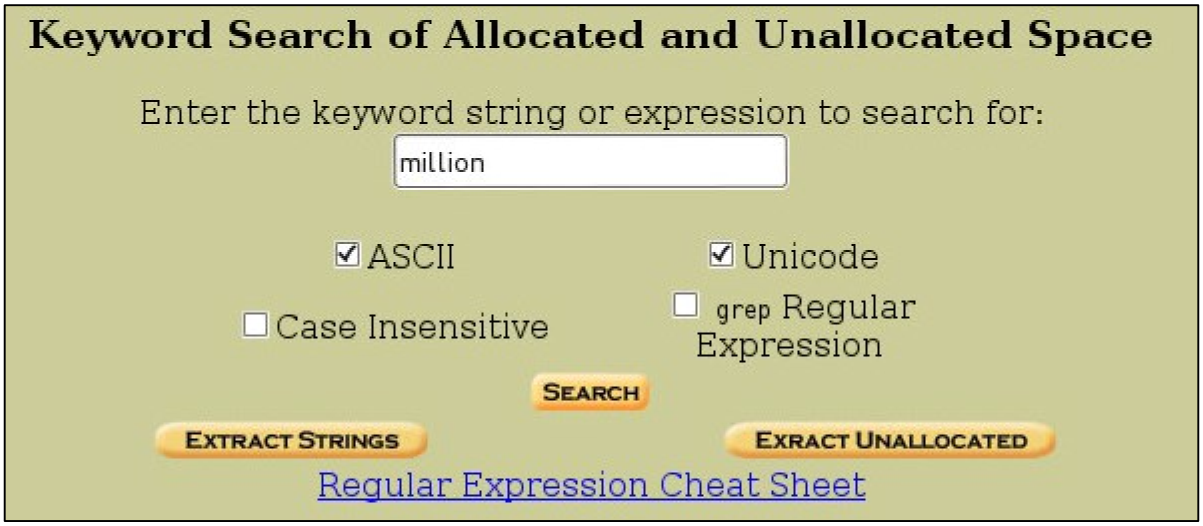


```
                  Autopsy ASCII Report

----------------------------------------------------------------------
                   GENERAL INFORMATION

File: /1//vacationinfo.txt
MD5 of file: 9d1b3688ed7785ef28d107d230f94464  -
SHA-1 of file: 18c635abf747076b832863ca2eaf25593c64aa1f  -

Image: '/var/lib/autopsy/Case001/host1/images/driveimage.dd'
Offset: Full image
File System Type: ext

Date Generated: Sat Feb 15 20:06:28 2014
Investigator: unknown

----------------------------------------------------------------------
                   META DATA INFORMATION

inode: 12
Allocated
Group: 0
Generation Id: 321209463
uid / gid: 0 / 0
mode: rrw-r--r--
size: 149
num of links: 1

Inode Times:
Accessed:       Fri Feb 14 01:06:39 2014
File Modified:  Fri Feb 14 01:06:39 2014
Inode Modified: Fri Feb 14 01:06:39 2014

Direct Blocks:
38

File Type: ASCII text
```

2. Note that it is possible to also print out HEX and String reports. Also note that it is possible to export the file for further analysis, just as in ProDiscover and FTK. You can also add a note about the individual file.

Part 5 – Using the Search Function

1. At the top of the screen, click the ‘**Keyword Search**’ tab. If you would like to search for individual keywords as we did in FTK, it is possible to do that from this location. Since the words within the image file have been indexed by Autopsy, typing in a work found within the ‘vacationinfo.txt’ file will result in hits leading to that file. Type **million** and select ‘**Search**’.



Keyword Search of Allocated and Unallocated Space

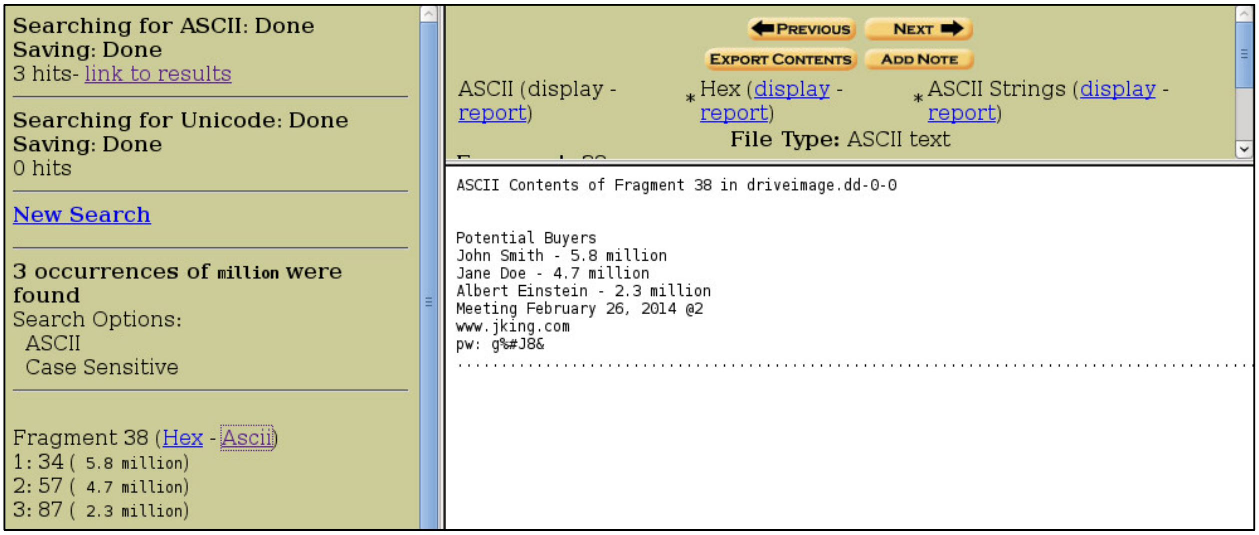
Enter the keyword string or expression to search for:

million

☑ ASCII ☑ Unicode

☐ Case Insensitive ☐ grep Regular Expression

2. A new page with the results will appear. Note that three occurrences of million were found in ASCII. The results will be printed out below. It is possible to click on ASCII to view the file in which the results were found. The file will be populated on the right side of the screen.



Searching for ASCII: Done
Saving: Done
3 hits- link to results

Searching for Unicode: Done
Saving: Done
0 hits

New Search

3 occurrences of million were found
Search Options:
ASCII
Case Sensitive

Fragment 38 (Hex - Ascii)
1: 34 (5.8 million)
2: 57 (4.7 million)
3: 87 (2.3 million)

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report)

File Type: ASCII text

```
ASCII Contents of Fragment 38 in driveimage.dd-0-0


Potential Buyers
John Smith - 5.8 million
Jane Doe - 4.7 million
Albert Einstein - 2.3 million
Meeting February 26, 2014 @2
www.jking.com
pw: g%#J8&
```

3. If there are additional results, use the ‘Previous’ and ‘Next’ buttons to navigate through the files in which the results were found. The report generators, add note, and export content options are also available on this page as well. If you would like further practice, feel free to write images to the sda3 partition and see how they can be viewed within Autopsy.

Conclusion

You should now have a general idea of how to create a disk image file, hash the file, write block the file, and perform a first-level analysis of the disk image in a Kali Linux environment. This is the basis of any digital forensics investigation. Knowing these basics will enable you to focus on learning more involved and advanced aspects of digital forensics. Since reports and notes are often used in court and to verify the integrity of evidence, it is important to keep a log of any changes made or anything noted during the course of the investigation. These reports and logs will potentially be used in a court of law.