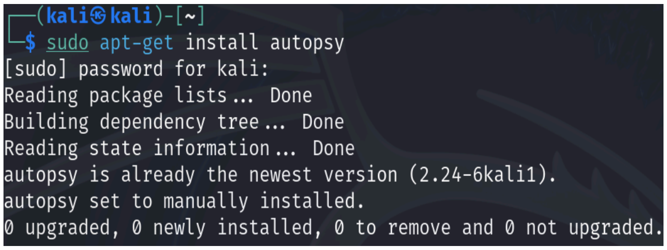
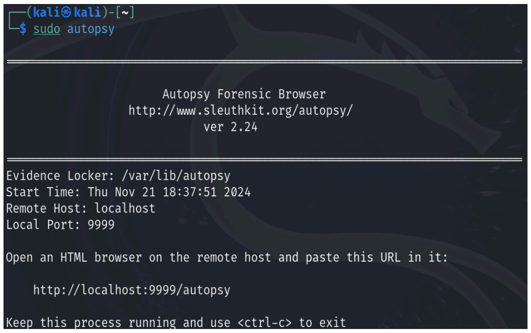


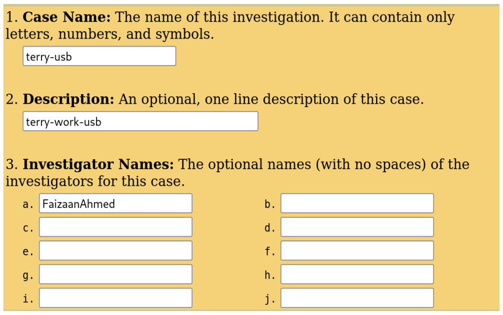
```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install autopsy
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
autopsy is already the newest version (2.24-6kali1).
autopsy set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

In this screenshot, we see the process of installing Autopsy on a Kali Linux system using the apt-get package manager. The command entered is sudo apt-get install autopsy, which prompts the user to enter their password for elevated privileges. The system then proceeds to read the package lists, build the dependency tree, and read state information. The output indicates that Autopsy is already the newest version available (2.24-6kali1) and is set to be manually installed. No packages were upgraded, newly installed, removed, or held back. This confirms that Autopsy was already installed on the system and was up to date. It shows the initial setup step necessary for using the Autopsy tool, ensuring that the software is available and ready to be used for forensic analysis. This step is essential for verifying the installation status and version of Autopsy before proceeding with further forensic tasks.



```
┌──(kali㉿kali)-[~]
└─$ sudo autopsy

============================================================================

                       Autopsy Forensic Browser
                  http://www.sleuthkit.org/autopsy/
                               ver 2.24

============================================================================
Evidence Locker: /var/lib/autopsy
Start Time: Thu Nov 21 18:37:51 2024
Remote Host: localhost
Local Port: 9999

Open an HTML browser on the remote host and paste this URL in it:

    http://localhost:9999/autopsy

Keep this process running and use <ctrl-c> to exit
```

We began by launching Autopsy as a root user using the command sudo autopsy. This initiated the Autopsy platform and provided details such as the Evidence Locker location, start time, remote host, and local port (9999). Keeping the terminal running was crucial to maintaining the server's activity, enabling us to access the Autopsy web interface. We saw the terminal output, which included the URL http://localhost:9999/autopsy. We pasted this URL into firefox to access the Autopsy interface. The terminal continued running, showing that the process should remain active to keep the server running. The purpose of this step was to establish a connection to the Autopsy web interface, which is essential for conducting forensic analysis.



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

terry-usb

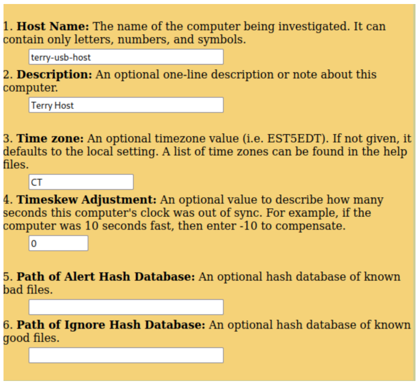
2. **Description:** An optional, one line description of this case.

terry-work-usb

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

a.	FaizaanAhmed	b.	
c.		d.	
e.		f.	
g.		h.	
i.		j.	

We see a form within the Autopsy web interface for creating a new forensic case. The form includes fields for the case name, description, and investigator names. The form asks for the name of the investigation. It specifies that the case name can contain only letters, numbers, and symbols. In this example, the case name is entered as "terry-usb". An optional one-line description of the case is requested. Here, the description is entered as "terry-work-usb". This field helps provide a brief summary of the investigation's focus or context. The form allows the entry of multiple investigator names, with instructions to avoid spaces in the names. The purpose is to demonstrate the setup process for a new forensic case in Autopsy. By filling out the case name, description, and investigator names, we establish a structured and documented environment for the investigation. This step ensures that all relevant information is recorded and organized, facilitating effective case management and collaboration among investigators.



1. **Host Name:** The name of the computer being investigated. It can contain only letters, numbers, and symbols.
terry-usb-host

2. **Description:** An optional one-line description or note about this computer.
Terry Host

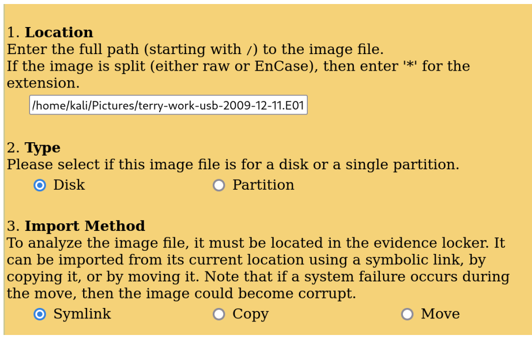
3. **Time zone:** An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.
CT

4. **Timeskew Adjustment:** An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.
0

5. **Path of Alert Hash Database:** An optional hash database of known bad files.

6. **Path of Ignore Hash Database:** An optional hash database of known good files.

This is another form within the Autopsy web interface, this time for adding a new host to a case. This form collects information about the computer being investigated. The form asks for the name of the computer being investigated. It specifies that the host name can contain only letters, numbers, and symbols. This step is important for uniquely identifying the system under investigation. An optional one-line description or note about the computer can be provided. This field helps provide additional context or notes about the host, aiding in the clarity of documentation. An optional timezone value can be entered. If not given, it defaults to the local setting. Specifying the timezone is important for accurate time-based analysis, ensuring that all timestamps are correctly interpreted. An optional value to describe how many seconds the computer's clock was out of sync. For instance, if the computer was 10 seconds fast, then entering -10 would compensate. Here, the adjustment is set to "0", indicating no adjustment is needed. This field is significant for correcting any discrepancies in timekeeping, which can affect the interpretation of forensic data. This is to demonstrate the detailed setup process for adding a new host in Autopsy. By filling out these fields, we ensured that the investigation was well-documented and that the system's time settings were accurately configured. Specifying hash databases helped optimize the forensic analysis by quickly identifying known good or bad files. This step is essential for organizing the investigation and ensuring that all relevant parameters are set correctly for a thorough forensic examination.



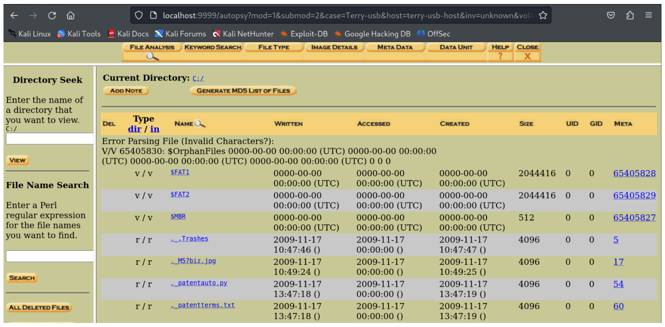
1. **Location**
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.
/home/kali/Pictures/terry-work-usb-2009-12-11.E01

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

In this screenshot, we see a form in the Autopsy web interface for adding an image file to the forensic case. The form includes fields for specifying the image file's location, type, and import method. We entered the full path to the image file, starting with '/'. If the image was split, we would have used '*' for the extension. In this case, my image file path is /home/kali/Pictures/terry-work-usb-2009-12-11.E01.

This step is crucial for identifying the exact file to be analyzed in the investigation. We specified whether the image file is for a disk or a single partition. To analyze the image file, it must be located in the evidence locker. We could import it using a symbolic link, by copying it, or by moving it. Here, Symlink is selected. Using a symlink minimizes disk space usage and preserves the original file's integrity, but it requires that the original location remains accessible. If copying or moving, there is a risk of corruption if a system failure occurs during the process. This helps us understand the process of adding an image file to a forensic case in Autopsy. Specifying the location, type, and import method ensures that the forensic software correctly identifies and accesses the image file for analysis. This step is a must for any digital forensic investigation, as it sets up the data source from which all subsequent analysis will be performed.



Directory Seek

Enter the name of a directory that you want to view.
C:/

File Name Search

Enter a Perl regular expression for the file names you want to find.

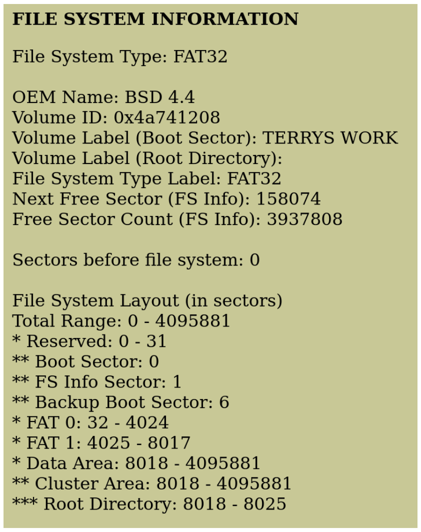
Current Directory: C:/

Del	Type dir / in	Name	Written	Accessed	Created	Size	UID	GID	Meta

Error Parsing File (Invalid Characters?):
V/V 65405830: $OrphanFiles 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0 0 0

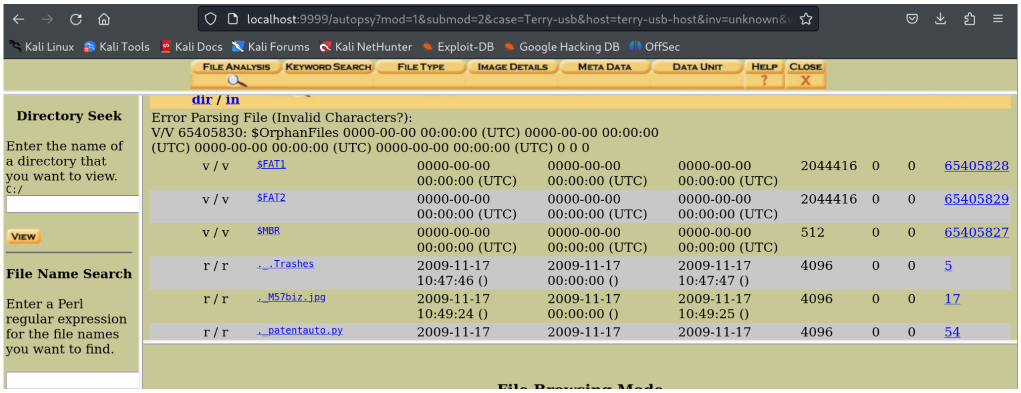
Del	Type dir / in	Name	Written	Accessed	Created	Size	UID	GID	Meta
	v / v	$FAT1	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	2044416	0	0	65405828
	v / v	$FAT2	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	2044416	0	0	65405829
	v / v	$MBR	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	512	0	0	65405827
	r / r	._.Trashes	2009-11-17 10:47:46 ()	2009-11-17 00:00:00 ()	2009-11-17 10:47:47 ()	4096	0	0	5
	r / r	._M57biz.jpg	2009-11-17 10:49:24 ()	2009-11-17 00:00:00 ()	2009-11-17 10:49:25 ()	4096	0	0	17
	r / r	._patentauto.py	2009-11-17 13:47:18 ()	2009-11-17 00:00:00 ()	2009-11-17 13:47:19 ()	4096	0	0	54
	r / r	._patentterms.txt	2009-11-17 13:47:18 ()	2009-11-17 00:00:00 ()	2009-11-17 13:47:19 ()	4096	0	0	60

In this screenshot, we see the Autopsy web interface displaying the contents of the root directory C:/ of the image file we previously added, used for analyzing the file system and identifying relevant files during a forensic investigation. The Directory Seek input field on the left allows the user to enter the name of a directory to navigate to it, with the current directory set to C:/. The table displays various details about the files and directories, including Type, Name, Written, Accessed, Created, Size, UID, GID, and Meta. The Type column indicates whether the entry is a directory (dir) or a file (r for regular file), and the Name column shows the file or directory names. The Written, Accessed, Created columns provide timestamps, though many show 0000-00-00 00:00:00 (UTC) due to parsing errors. The Size column indicates file size in bytes, while UID and GID show the User ID and Group ID of the file owner, and Meta contains metadata links. Parsing errors are noted with Error Parsing File, possibly due to invalid characters or corrupted data. The list includes special system files like $FAT1, $FAT2, $MBR, and other files like ._Trashes, ._M57biz.jpg, ._patentauto.py, ._patentterms.txt. Functional buttons like Add Note and Generate MD5 List of Files allow users to add notes and generate MD5 hash values for file integrity verification and identifying duplicates.



FILE SYSTEM INFORMATION

```
File System Type: FAT32

OEM Name: BSD 4.4
Volume ID: 0x4a741208
Volume Label (Boot Sector): TERRYS WORK
Volume Label (Root Directory):
File System Type Label: FAT32
Next Free Sector (FS Info): 158074
Free Sector Count (FS Info): 3937808

Sectors before file system: 0

File System Layout (in sectors)
Total Range: 0 - 4095881
* Reserved: 0 - 31
** Boot Sector: 0
** FS Info Sector: 1
** Backup Boot Sector: 6
* FAT 0: 32 - 4024
* FAT 1: 4025 - 8017
* Data Area: 8018 - 4095881
** Cluster Area: 8018 - 4095881
*** Root Directory: 8018 - 8025
```



Directory Seek

Enter the name of a directory that you want to view.
C:/

File Name Search

Enter a Perl regular expression for the file names you want to find.

dir / in

Error Parsing File (Invalid Characters?):
V/V 65405830: $OrphanFiles 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0 0 0

v / v	$FAT1	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	2044416	0	0	65405828
v / v	$FAT2	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	2044416	0	0	65405829
v / v	$MBR	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	512	0	0	65405827
r / r	._.Trashes	2009-11-17 10:47:46 ()	2009-11-17 00:00:00 ()	2009-11-17 10:47:47 ()	4096	0	0	5
r / r	._M57biz.jpg	2009-11-17 10:49:24 ()	2009-11-17 00:00:00 ()	2009-11-17 10:49:25 ()	4096	0	0	17
r / r	._patentauto.py	2009-11-17	2009-11-17	2009-11-17	4096	0	0	54

Executive Summary: In this lab, we utilized the Autopsy platform for digital forensic analysis on a Linux system. First, we ensured that Autopsy was installed and then launched it using the command line, accessing it through a browser at localhost. We started a new case, entered necessary case details, and added a host to save the analysis results. We downloaded a USB image from Digital Corpora, specifically the "terry-work-usb-2009-12-11.E01" file, and provided its path in Autopsy. After mounting the image, we began our analysis by exploring various features of the Autopsy platform. We examined file system details, generated MD5 hash values for integrity verification, and sequenced events based on timestamps. We analyzed file metadata and generated reports for each file. Through Autopsy's interface, we identified and reviewed deleted files, expanded directories, and assessed timestamps for file activities. We delved into the meta information of files and directories to scrutinize their content. At the end, we generated detailed reports and visualized the findings, enhancing our understanding of the digital forensic process and Autopsy's capabilities in forensic investigations.