Forensic Evidence Collection and Analysis

Scope

This report details a forensic analysis of an image file, including hash generation, case setup in Autopsy, hash verification, and the discovery and recovery of hidden image files. A pre-created forensic challenge image file, obtained from Techshied's environment after an incident, was used to create a new autopsy case. And the goal is to ensure all investigative actions are performed on a preserved copy of the data.

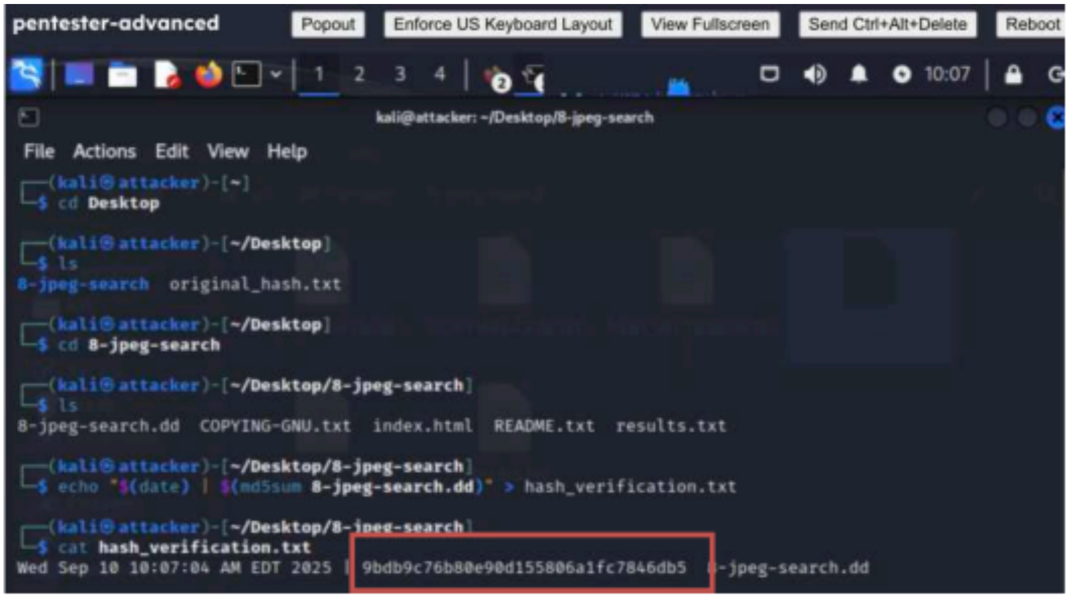
Verification of Forensic Image Test File

Step 1: MD5 Hash Creation and Storage

To maintain the integrity of the evidence, an MD5 hash of the original image file created, which creates a unique digital fingerprint that will be used to verify that the file is unmodified or hasn't been altered during the forensic process. It is just simply a fingerprint of the given input.

Process:

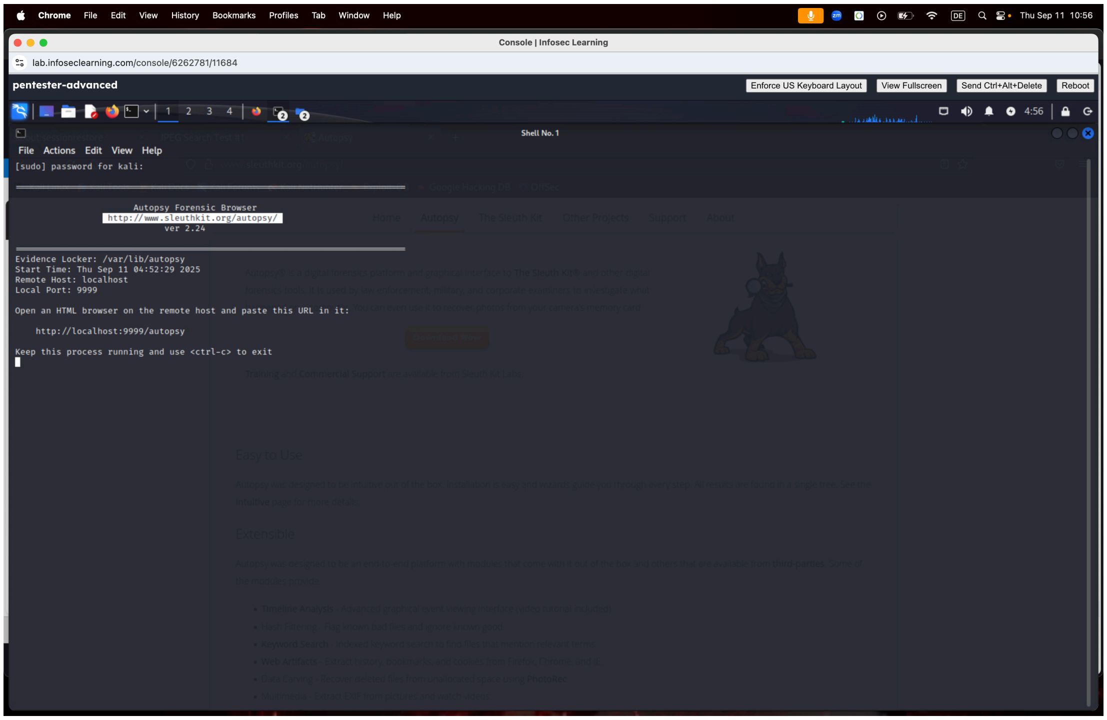
A command-line tool like ***md5sum (Linux/macOS) echo $"(date) $(md5sum 8-jpeg-search.dd)" > hash_verification.txt*** is used. The generated hash value is then saved to a separate text file with the command-line ***cat hash_verification.txt***, which serves as a record of the original state of the evidence.



```
┌──(kali㉿attacker)-[~]
└─$ cd Desktop

┌──(kali㉿attacker)-[~/Desktop]
└─$ ls
8-jpeg-search  original_hash.txt

┌──(kali㉿attacker)-[~/Desktop]
└─$ cd 8-jpeg-search

┌──(kali㉿attacker)-[~/Desktop/8-jpeg-search]
└─$ ls
8-jpeg-search.dd  COPYING-GNU.txt  index.html  README.txt  results.txt

┌──(kali㉿attacker)-[~/Desktop/8-jpeg-search]
└─$ echo "$(date) | $(md5sum 8-jpeg-search.dd)" > hash_verification.txt

┌──(kali㉿attacker)-[~/Desktop/8-jpeg-search]
└─$ cat hash_verification.txt
Wed Sep 10 10:07:04 AM EDT 2025 | 9bdb9c76b80e90d155806a1fc7846db5  8-jpeg-search.dd
```

MD5 Hash Creation

Step 2: Prior to setting up the autopsy case**,** the command ***sudo autopsy*** was used to be directed to http://localhost:9999/autopsy



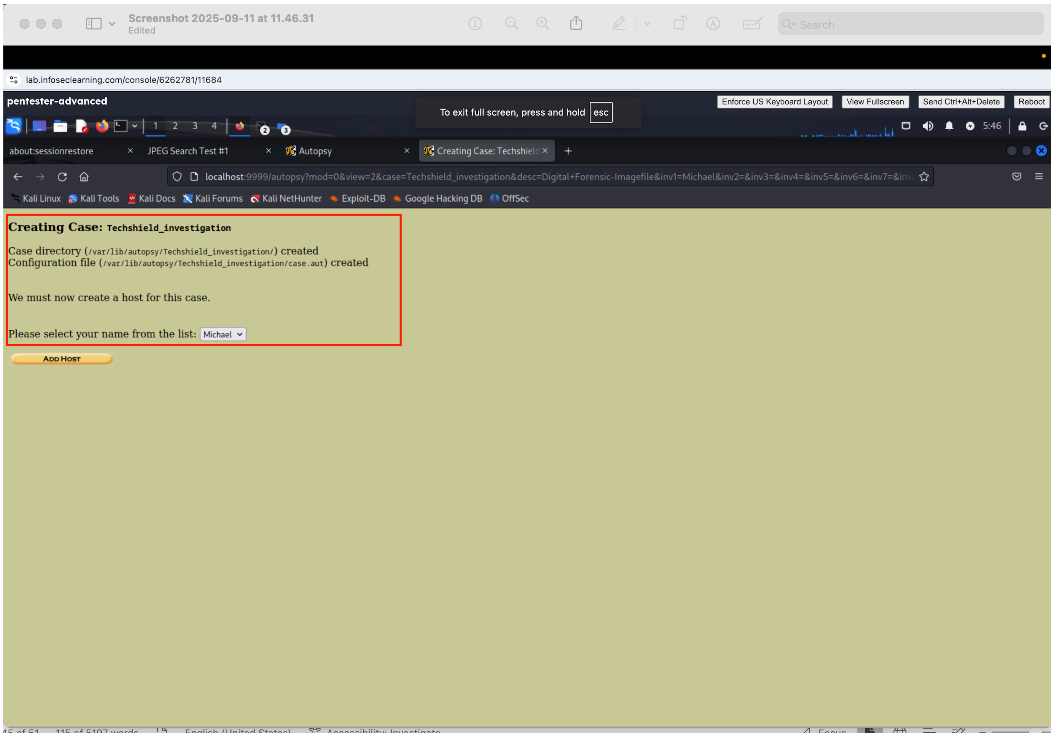
```
[sudo] password for kali:

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

Evidence Locker: /var/lib/autopsy
Start Time: Thu Sep 11 04:52:29 2025
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
```

Established Link to Localhost for Forensic Image creation and Importation

Autopsy Case Setup & Hash Verification

Autopsy is a powerful open-source digital forensics platform or a forensic browser used to analyze disk images and it enabled Michael Cyber Defense us to look at the content of the drive image, so within the case setup, the hash of the evidence file is verified to ensure that the file being analyzed is the same as the original, unaltered evidence.

Step 3: A new autopsy case was created, and the image file is added as a data source. During the data source addition process, Autopsy automatically calculates the MD5 hash of the added file. The calculated hash is, then, stored within the case database.



Screenshot 2025-09-11 at 11.46.31
Edited
lab.infoseclearning.com/console/6262781/11684
pentester-advanced
To exit full screen, press and hold esc
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
about:sessionrestore
JPEG Search Test #1
Autopsy
Creating Case: Techshield
localhost:9999/autopsy?mod=0&view=2&case=Techshield_investigation&desc=Digital+Forensic-Imagefile&inv1=Michael&inv2=&inv3=&inv4=&inv5=&inv6=&inv7=&inv
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec

Creating Case: `Techshield_investigation`

Case directory (`/var/lib/autopsy/Techshield_investigation/`) created
Configuration file (`/var/lib/autopsy/Techshield_investigation/case.aut`) created

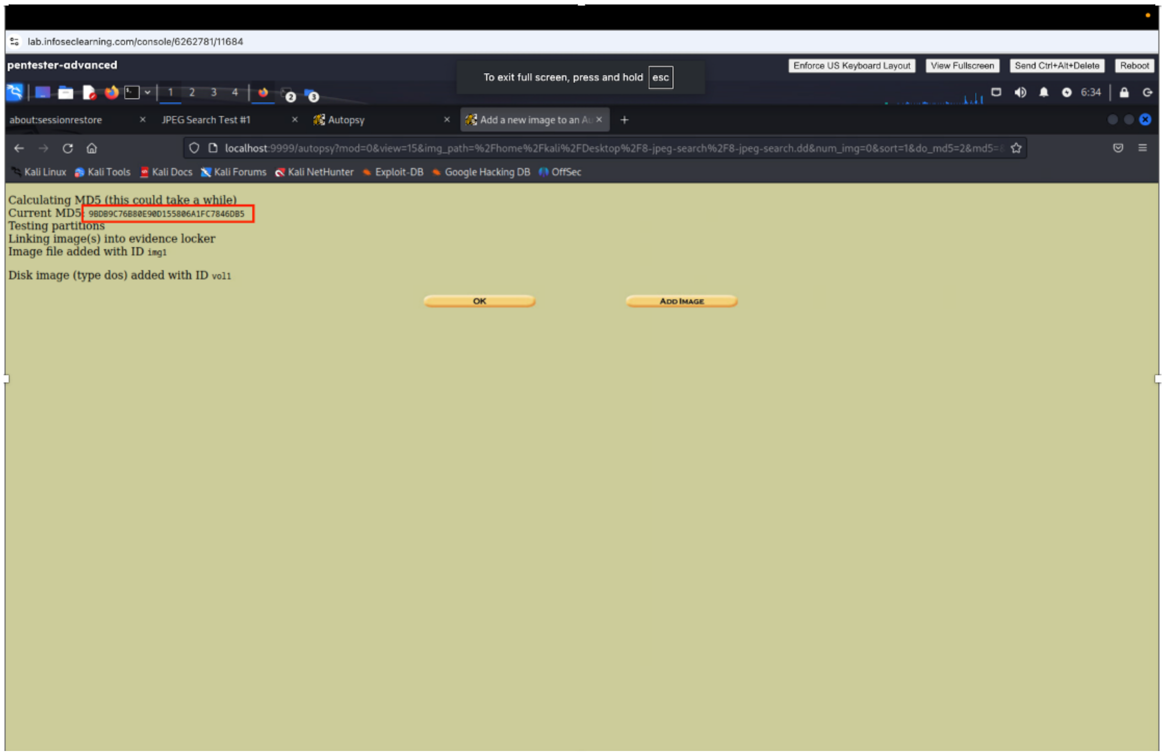
We must now create a host for this case.

Please select your name from the list: Michael

Autopsy Case Creation

Task 3: Verifying the hash

The figure below shows the MD5sum of the image and the hash calculated by Autopsy is then compared against the original hash value stored in the in the image file by manually comparing this hash against a known good fingerprint with the one in the image file. A perfect match confirms the integrity of the evidence. That's not a single file in the image, but that's the MD5sum for the entire image itself

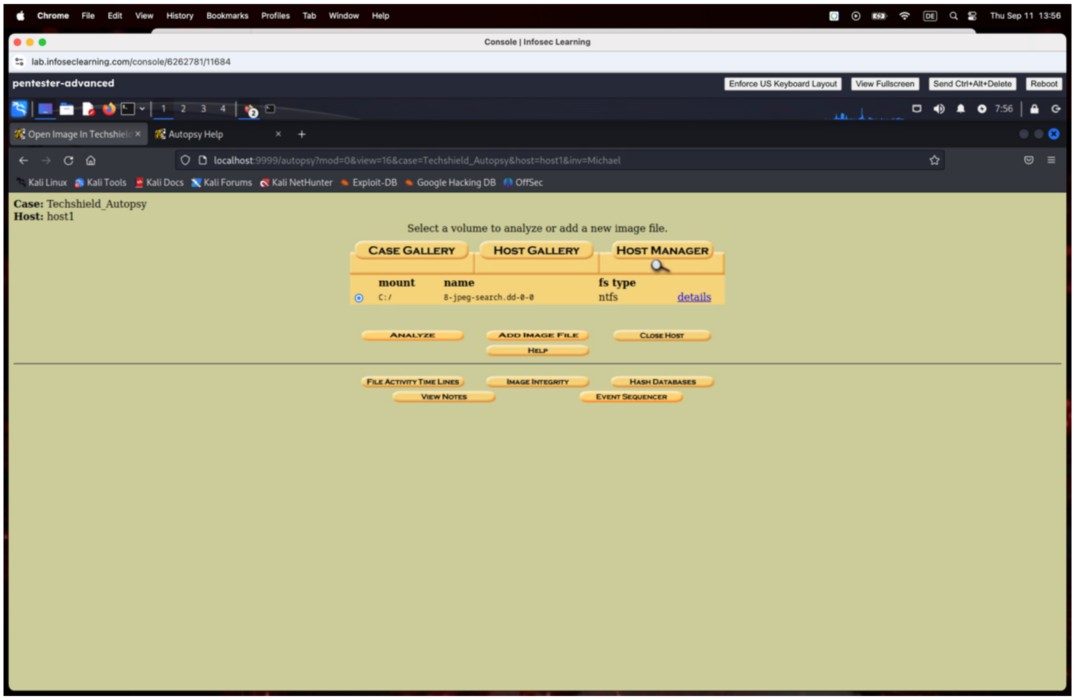


lab.infoseclearning.com/console/6262781/11684
pentester-advanced
To exit full screen, press and hold esc
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
about:sessionrestore
JPEG Search Test #1
Autopsy
Add a new image to an A
localhost:9999/autopsy?mod=0&view=15&img_path=%2Fhome%2Fkali%2FDesktop%2F8-jpeg-search%2F8-jpeg-search.dd&num_img=0&sort=1&do_md5=2&md5=
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec

```
Calculating MD5 (this could take a while)
Current MD5: 9BDB9C76B80E90D155806A1FC7846DB5
Testing partitions
Linking image(s) into evidence locker
Image file added with ID img1

Disk image (type dos) added with ID vol1
```

Correct MD5 Hash Calculation

From there, I am led to my main case management screen. My TechShield autopsy case.



Case: Techshield_Autopsy
Host: host1

Select a volume to analyze or add a new image file.

	mount	name	fs type	
●	C:/	8-jpeg-search.dd-0-0	ntfs	details

Case File Management screen before analysis

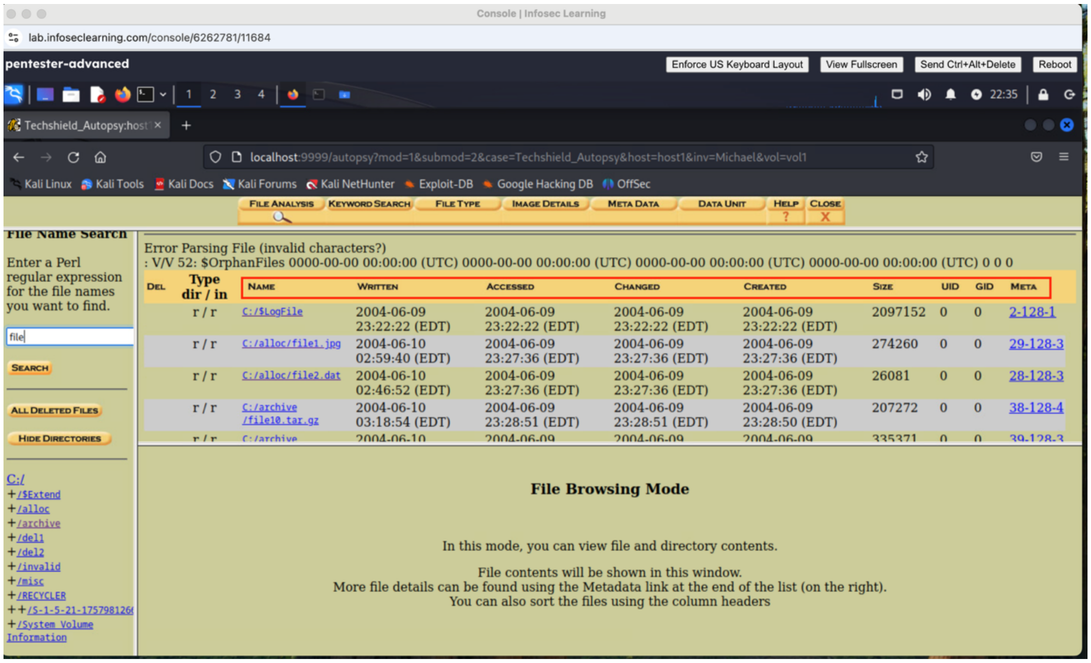
Task 4: File Analysis & Hidden Image Recovery

The last part of this section comprises of forensic discovery and Hidden image recovery. This is where File Analysis is conducted to discover and recover artifacts not immediately visible, such as hidden or deleted files. In this case, the objective is to find 5 hidden JPG images. The File Analysis gives me a list of files that are inside this image

Process:

File Type identification

- The search box was used to search for files because autopsy can identify files based on their digital signatures and it enables us to identify the timestamp of files written, access, changed, and created including their sizes. That can be broken down in three parts: The written time, which is sometimes called the M-Time, the access time, which is sometimes called the A-Time, and creation time, which is called the C-Time.



localhost:9999/autopsy?mod=1&submod=2&case=Techshield_Autopsy&host=host1&inv=Michael&vol=vol1

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

file

Error Parsing File (invalid characters?)
: V/V 52: $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	Changed	Created	Size	UID	GID	Meta
	r / r	C:/$LogFile	2004-06-09 23:22:22 (EDT)	2004-06-09 23:22:22 (EDT)	2004-06-09 23:22:22 (EDT)	2004-06-09 23:22:22 (EDT)	2097152	0	0	2-128-1
	r / r	C:/alloc/file1.jpg	2004-06-10 02:59:40 (EDT)	2004-06-09 23:27:36 (EDT)	2004-06-09 23:27:36 (EDT)	2004-06-09 23:27:36 (EDT)	274260	0	0	29-128-3
	r / r	C:/alloc/file2.dat	2004-06-10 02:46:52 (EDT)	2004-06-09 23:27:36 (EDT)	2004-06-09 23:27:36 (EDT)	2004-06-09 23:27:36 (EDT)	26081	0	0	28-128-3
	r / r	C:/archive /file10.tar.gz	2004-06-10 03:18:54 (EDT)	2004-06-09 23:28:51 (EDT)	2004-06-09 23:28:51 (EDT)	2004-06-09 23:28:50 (EDT)	207272	0	0	38-128-4
	r / r	C:/archive	2004-06-10	2004-06-09	2004-06-09	2004-06-09	335371	0	0	39-128-3

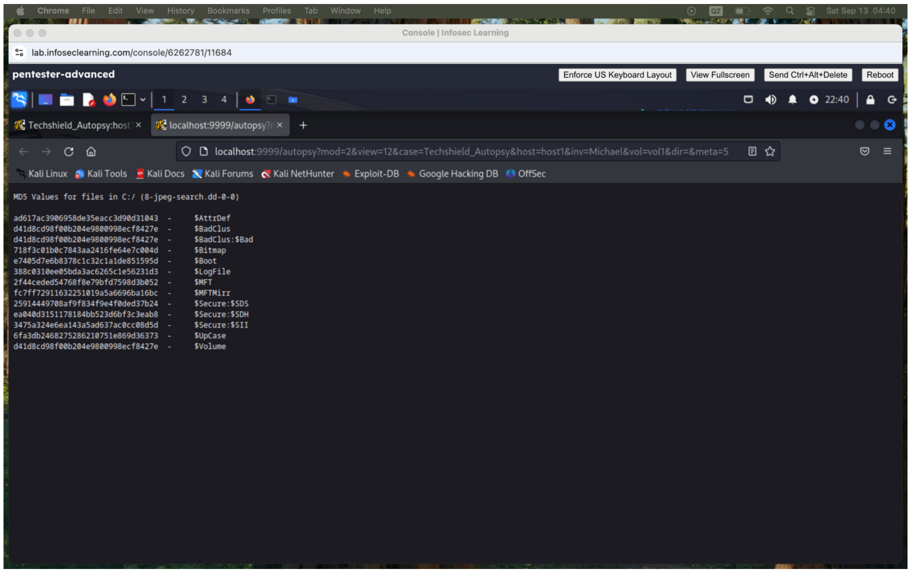
File Browsing Mode

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

Search Results

- Navigating to 14 File types > By MIME Type > image/jpeg revealed all files including those that had their extensions changed to conceal them.
- Before deciding to extract the contents from each file, I used the “Generate MD5 list of files” to button to have the calculated MD5sum values for each file in the current directory

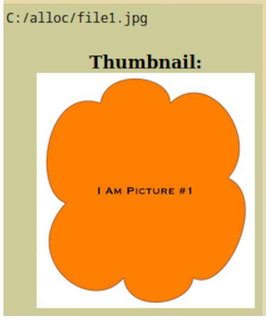


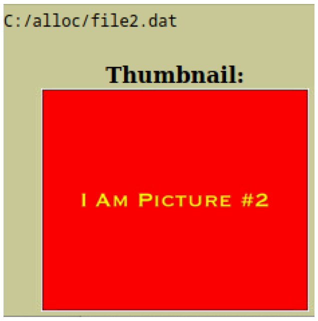
Chrome File Edit View History Bookmarks Profiles Tab Window Help
Sat Sep 13 04:40
Console | Infosec Learning
lab.infoseclearning.com/console/6262781/11684
pentester-advanced
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
22:40
Techshield_Autopsy:host1
localhost:9999/autopsy?m
localhost:9999/autopsy?mod=2&view=12&case=Techshield_Autopsy&host=host1&inv=Michael&vol=vol1&dir=&meta=5
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec

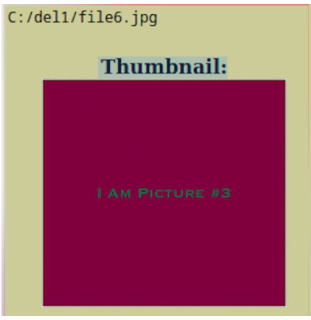
```
MD5 Values for files in C:/ (8-jpeg-search.dd-0-0)

ad617ac3906958de35eacc3d90d31043  -     $AttrDef
d41d8cd98f00b204e9800998ecf8427e  -     $BadClus
d41d8cd98f00b204e9800998ecf8427e  -     $BadClus:$Bad
718f3c01b0c7843aa2416fe64e7c004d  -     $Bitmap
e7405d7e6b8378c1c32c1a1de851595d  -     $Boot
388c0310ee05bda3ac6265c1e56231d3  -     $LogFile
2f44ceded54768f8e79bfd7598d3b052  -     $MFT
fc7ff72911632251019a5a6696ba16bc  -     $MFTMirr
25914449708af9f834f9e4f0ded37b24  -     $Secure:$SDS
ea040d3151178184bb523d6bf3c3eab8  -     $Secure:$SDH
3475a324e6ea143a5ad637ac0cc08d5d  -     $Secure:$SII
6fa3db2468275286210751e869d36373  -     $UpCase
d41d8cd98f00b204e9800998ecf8427e  -     $Volume
```

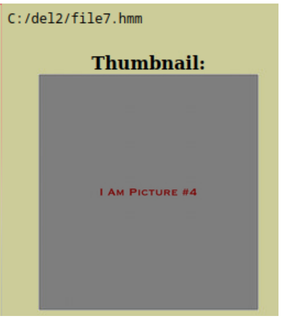
Calculated MD5sum Values

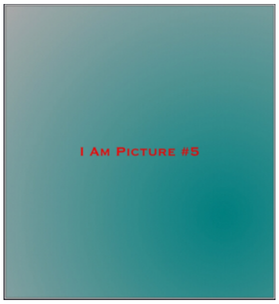
- Recovery: Using autopsy, the contents within each file are then extracted and the 6 discovered JPEG images are exported from the autopsy to a designated folder for further review.

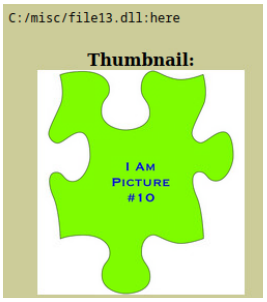












Task 5: Significance of Findings

The discovery and recovery of hidden images are significant from a forensic perspective for several reasons:

- **Intent to Conceal:** The act of hiding files, either by changing their extension or deleting them to leave them in unallocated space, strongly suggests a deliberate attempt to conceal information. This can indicate mens rea (guilty mind) on the part of the suspect.
- **Key Evidence:** The recovered images themselves can contain crucial evidence. They may be contraband, documents relevant to the case, or show a timeline of events. For example, the metadata (EXIF data) within the images could reveal the date, time, and even the geolocation where the picture was taken, providing a timeline and location for a specific event.
- **Attacker Behavior:** The methods used to hide the files (e.g., specific file names or directory structures) can reveal the suspect's level of technical sophistication and common operating procedures, which can be valuable for future investigations.
- **Link to Other Artifacts:** The recovered files can be linked to other artifacts in the case, such as web browser history showing where they were downloaded from or chat logs discussing their existence, helping to build a more complete picture of the events.