

# Forensics, Report & Presentation

## Technical Scope:

- Hashing, Autopsy case setup,
- Autopsy hash verification,
- Analysis,
- hidden images discovery and recovery.

## Tasks:

1. Generate MD5 hash of an image file, store the hash in a file.
2. Create a new Autopsy case with the image in question, verify the hash with Autopsy.
3. Verify that the hash in Autopsy matches the original hash taken.
4. Perform file analysis. Search & recover the 5 hidden JPG image files.
5. Analyze findings: explain why these artifacts are significant from a forensic perspective.
6. Finalize VAPT report.
7. Work on the presentation deck.

## Hashing & Integrity

**MD5sum correctly run, hash saved to a file.**

```
md5sum 8-jpeg-search.dd

# Save hash to evidence file
md5sum 8-jpeg-search.dd > evidence_md5_hash.txt

# Verify against expected value
EXPECTED="9bdb9c76b80e90d155806a1fc7846db5"
```

```
(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]
$ md5sum 8-jpeg-search.dd > evidence_md5_hash.txt

(kali㉿attacker)-[~/Desktop/8-jpeg-search]
$ cat evidence_md5_hash.txt
9bdb9c76b80e90d155806a1fc7846db5  8-jpeg-search.dd
```

```
cp 8-jpeg-search.dd 8-jpeg-search-forensic-copy.dd

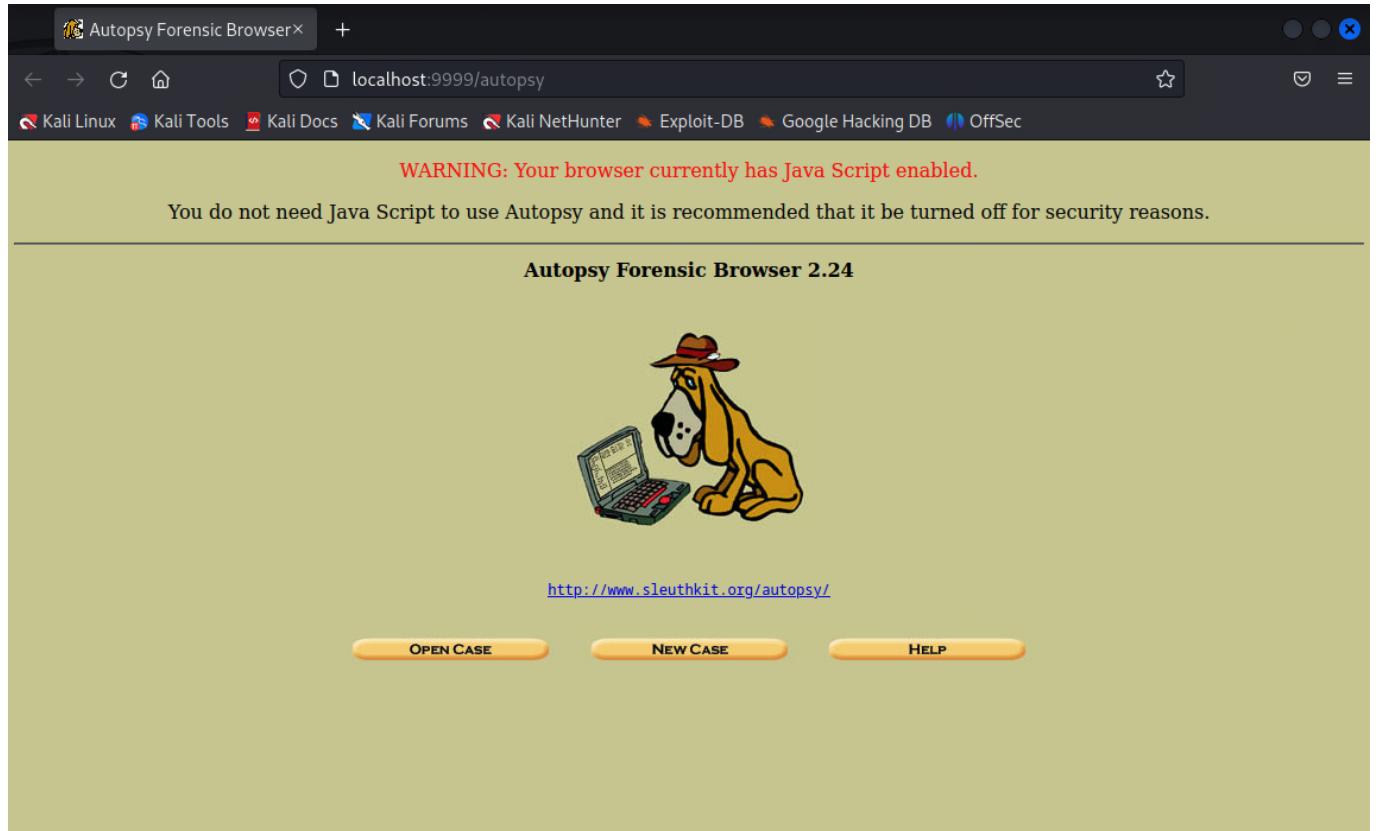
# Verify copy integrity
md5sum 8-jpeg-search_forensic_copy.dd > copy_md5_hash.txt
```

```
[kali㉿attacker] - [~/Desktop/8-jpeg-search]
$ cat evidence_md5_hash.txt
9bdb9c76b80e90d155806a1fc7846db5 8-jpeg-search.dd

[kali㉿attacker] - [~/Desktop/8-jpeg-search]
$ cat evidence_md5_hash_copy.txt
9bdb9c76b80e90d155806a1fc7846db5 8-jpeg-search-forensic-copy.dd
```

```
diff 8-jpeg-search.dd otro 8-jpeg-search_forensic_copy.dd
```

autopsy



```
File Actions Edit View Help
[sudo] password for kali: _____
_____
Autopsy Forensic Browser
http://www.sleuthkit.org/autopsy/
ver 2.24
You do not need Java Script to use Autopsy and it is recommended.

Evidence Locker: /var/lib/autopsy
Start Time: Mon Feb 2 15:09:50 2026
Remote Host: localhost
Local Port: 9999

Autopsy Forensic Browser
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
[ ]
```

```
/home/kali/forensics/
└── 8-jpeg-search-forensics/
    ├── evidence/
    ├── reports/
    └── screenshots/
```

```
[kali㉿attacker] - [~/Desktop/8-jpeg-search]
$ mkdir forensics

[kali㉿attacker] - [~/Desktop/8-jpeg-search]
$ mkdir forensics/case-8-jpeg-search

[kali㉿attacker] - [~/Desktop/8-jpeg-search]
$ mkdir forensics/case-8-jpeg-search/evidence

[kali㉿attacker] - [~/Desktop/8-jpeg-search]
$ mkdir forensics/case-8-jpeg-search/reports

[kali㉿attacker] - [~/Desktop/8-jpeg-search]
$ mkdir forensics/case-8-jpeg-search/screenshots
```

## Autopsy Case Setup

Case created with correct metadata (case name, description, investigator's name).

## CREATE A NEW CASE

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

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

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

|  |                         |
|--|-------------------------|
| a. <input type="text" value="Esperanza Buitrago"/> | b. <input type="text"/> |
| c. <input type="text"/>                            | d. <input type="text"/> |
| e. <input type="text"/>                            | f. <input type="text"/> |
| g. <input type="text"/>                            | h. <input type="text"/> |
| i. <input type="text"/>                            | j. <input type="text"/> |

**NEW CASE**      **CANCEL**      **HELP**

Forensic image added successfully.

### Creating Case: forensics

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

We must now create a host for this case.

**ADD HOST**

Add host

**ADD A NEW HOST**

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

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

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.

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.

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.

**ADD HOST**      **CANCEL**      **HELP**

**Adding host: host1 to case forensics**

Host Directory (`/var/lib/autopsy/forensics/host1/`) created

Configuration file (`/var/lib/autopsy/forensics/host1/host.aut`) created

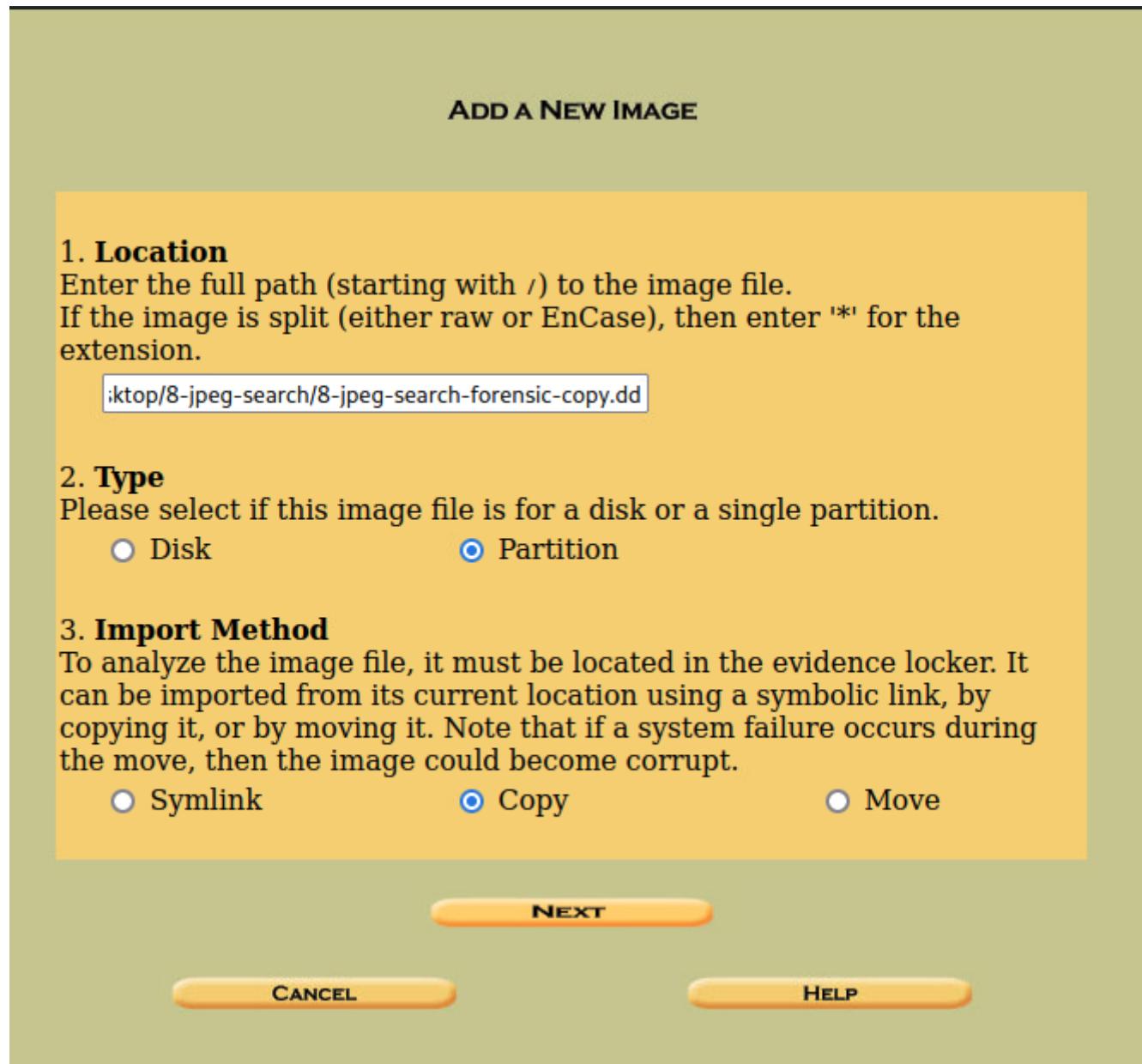
We must now import an image file for this host

**ADD IMAGE**

Add directory

```
(kali㉿attacker) [~/Desktop/8-jpeg-search]
$ pwd
/home/kali/Desktop/8-jpeg-search
Start Time: Wed Feb 4 08:27:59 2026
(kali㉿attacker) [~/Desktop/8-jpeg-search]
$ ls -al
total 20148
drwxr-xr-x 2 kali kali 4096 Feb 4 08:16 .
drwxr-xr-x 3 kali kali 4096 Jan 16 2025 ..
-rw-r--r-- 1 kali kali 10289152 Jun 10 2004 8-jpeg-search.dd
-rw-r--r-- 1 kali kali 10289152 Feb 2 14:47 8-jpeg-search-forensic-copy.dd
-rw-r--r-- 1 kali kali 18009 Jun 9 2004 COPYING-GNU.txt
-rw-r--r-- 1 kali kali 65 Feb 2 14:49 evidence_md5_hash_copy.txt
-rw-r--r-- 1 kali kali 51 Feb 2 14:41 evidence_md5_hash.txt
-rw-r--r-- 1 kali kali 5615 Jun 10 2004 index.html
-rw-r--r-- 1 kali kali 799 Jun 9 2004 README.txt
-rw-r--r-- 1 kali kali 2368 Jun 10 2004 results.txt
```

We are going to use `8-jpeg-search-forensic-copy.dd`, to preserve the integrity of the original image `8-jpeg-search.dd`.



## Same hash verified in Autopsy.

We should have the same hash that we already calculated before:

9bdb9c76b80e90d155806a1fc7846db5.

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

Volume image (0 to 0 - ntfs - C:) added with ID vol1
```

## Evidence Recovery

Analysing the image:

| mount | name                               | fs type | details                 |
|-------|------------------------------------|---------|-------------------------|
| C:/   | 8-jpeg-search-forensic-copy.dd-0-0 | ntfs    | <a href="#">details</a> |

Analysis succeeded:

localhost:9999/autopsy?mod=1&submod=2&case=forensics&host=host&inv=unknown&vol=vol1

**FILE ANALYSIS** **KEYWORD SEARCH** **FILE TYPE** **IMAGE DETAILS** **META DATA** **DATA UNIT** **HELP** **CLOSE**

| DEL  | Type     | NAME            | WRITTEN                   | ACCESSED                  | CHANGED                   | CREATED                   | SIZE     | UID | GID | META    |
|--|----------|-----------------|---------------------------|---------------------------|---------------------------|---------------------------|----------|-----|-----|---------|
|  | dir / in |                 |                           |                           |                           |                           |          |     |     |         |
| Error Parsing File (Invalid Characters?):<br>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 |          |                 |                           |                           |                           |                           |          |     |     |         |
|  | r / r    | \$attrpref      | 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) | 2560     | 48  | 0   | 4-12B-4 |
|  | r / r    | \$BadClus       | 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) | 0        | 0   | 0   | 8-12B-2 |
|  | r / r    | \$BadClus:\$Bad | 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) | 10289152 | 0   | 0   | 8-12B-1 |
|  | r / r    | \$Bitmap        | 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) | 2512     | 0   | 0   | 6-12B-1 |
|  | r / r    | \$Root          | 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) | 8192     | 48  | 0   | 7-12B-1 |

**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 for hidden JPG files performed correctly and discovered.

### Extraction in deleted files

```
All deleted files
>> file6.jpg
>> file7.hmm
```

localhost:9999/autopsy?mod=1&submod=2&case=forensics&host=host&inv=unknown&vol=vol1

**FILE ANALYSIS** **KEYWORD SEARCH** **FILE TYPE** **IMAGE DETAILS** **META DATA** **DATA UNIT** **HELP** **CLOSE**

| DEL               | Type     | NAME              | WRITTEN                   | ACCESSED                  | CHANGED                   | CREATED                   | SIZE   | UID | GID | META     |
|-------------------|----------|-------------------|---------------------------|---------------------------|---------------------------|---------------------------|--------|-----|-----|----------|
|                   | dir / in |                   |                           |                           |                           |                           |        |     |     |          |
| All Deleted Files |          |                   |                           |                           |                           |                           |        |     |     |          |
|                   | - / r    | C:/del1/file6.jpg | 2004-06-10 02:48:08 (EDT) | 2004-06-09 23:28:00 (EDT) | 2004-06-09 23:28:00 (EDT) | 2004-06-09 23:28:00 (EDT) | 175630 | 0   | 0   | 32-12B-3 |
|                   | - / r    | C:/del2/file7.hmm | 2004-06-10 02:49:18 (EDT) | 2004-06-09 23:43:38 (EDT) | 2004-06-09 23:43:44 (EDT) | 2004-06-09 23:28:00 (EDT) | 326859 | 0   | 0   | 31-12B-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

```
>> - /r C:/del1/file6.jpg
```

localhost:9999/autopsy?mod=1&submod=2&case=forensics&host1=inv=unknown&vol=vol1

**FILE ANALYSIS** **KEYWORD SEARCH** **FILE TYPE** **IMAGE DETAILS** **META DATA** **DATA UNIT** **HELP** **CLOSE**

| Type  | dir / in          | NAME | WRITTEN                   | ACCESSED                  | CHANGED                   | CREATED                   | SIZE   | UID | GID | META     |
|-------|-------------------|------|---------------------------|---------------------------|---------------------------|---------------------------|--------|-----|-----|----------|
| - / r | C:/del1/file6.jpg |      | 2004-06-10 02:48:08 (EDT) | 2004-06-09 23:28:00 (EDT) | 2004-06-09 23:28:00 (EDT) | 2004-06-09 23:28:00 (EDT) | 175630 | 0   | 0   | 32-128-3 |
| - / r | C:/del2/file7.hmm |      | 2004-06-10 02:49:18 (EDT) | 2004-06-09 23:43:38 (EDT) | 2004-06-09 23:43:44 (EDT) | 2004-06-09 23:28:00 (EDT) | 326859 | 0   | 0   | 31-128-3 |

**Directory Seek**  
Enter the name of a directory that you want to view.  
C:/  
**VIEW**

**File Name Search**  
Enter a Perl regular expression for the file names you want to find.

**SEARCH**

**ALL DELETED FILES**

**EXPAND DIRECTORIES**

ASCII (display - report) \* Hex (display - report) \* ASCII Strings (display - report) \* Export \* View \* Add Note  
File Type: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 563x527, components 3  
Deleted File Recover Mode

C:/del1/file6.jpg

**Thumbnail:** [View Full Size Image](#)

## Metadata:

**MFT Entry Number:**  
32-128-3  
**VIEW**

**ALLOCATION LIST**

**Pointed to by file:**  
C:/del1/file6.jpg (deleted)

**File Type (Recovered):**  
JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 563x527, components 3  
**MD5 of recovered content:**  
afdf55222024a4e22f7f5a3a665320763 -

**SHA-1 of recovered content:**  
21cbafed3ff928f247f301c9a26bc5319d20a13 -

**Details:**

MFT Entry Header Values:  
Entry: 32 Sequence: 2  
\$LogFile Sequence Number: 1116754  
Not Allocated File  
Links: 1

\$STANDARD\_INFORMATION Attribute Values:  
Flags: Archive  
Owner ID: 0  
Security ID: 259 ()  
Created: 2004-06-09 23:28:00.862830400 (EDT)  
File Modified: 2004-06-10 02:48:08.000000000 (EDT)  
MFT Modified: 2004-06-09 23:28:00.912902400 (EDT)  
Accessed: 2004-06-09 23:28:00.912902400 (EDT)

\$FILE\_NAME Attribute Values:  
Flags: Archive  
Name: file6.jpg  
Parent MFT Entry: 30 Sequence: 1  
Allocated Size: 0 Actual Size: 0  
Created: 2004-06-09 23:28:00.862830400 (EDT)  
File Modified: 2004-06-09 23:28:00.862830400 (EDT)  
MFT Modified: 2004-06-09 23:28:00.862830400 (EDT)  
Accessed: 2004-06-09 23:28:00.862830400 (EDT)

**REPORT** **VIEW CONTENTS** **EXPORT CONTENTS** **ADD NOTE**

```
>> - /r C:/del1/file7.hmm
```



## Metadata:

**MFT Entry Number:** 31-128-3

**Pointed to by file:** C:/del2/file7.hmm (deleted)

**File Type (Recovered):** JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 698x752, components 3

**MD5 of recovered content:** 0c452c5800fcfa7c66027ae89c4f068a -

**SHA-1 of recovered content:** 7fe0602ea83956867553fa3ca98d03d90e675866 -

**Details:**

MFT Entry Header Values:  
Entry: 31 Sequence: 2  
LogFile Sequence Number: 1117937  
Not Allocated File  
Links: 1

\$STANDARD\_INFORMATION Attribute Values:  
Flags: Archive  
Owner ID: 0  
Security ID: 262 ()  
Created: 2004-06-09 23:28:00.742657600 (EDT)  
File Modified: 2004-06-10 02:49:18.000000000 (EDT)  
MFT Modified: 2004-06-09 23:43:44.157187200 (EDT)  
Accessed: 2004-06-09 23:43:38.899627200 (EDT)

\$FILE\_NAME Attribute Values:  
Flags: Archive  
Name: file7.hmm  
Parent MFT Entry: 47 Sequence: 1  
Allocated Size: 327168 Actual Size: 326859  
Created: 2004-06-09 23:28:00.742657600 (EDT)  
File Modified: 2004-06-10 02:49:18.000000000 (EDT)  
MFT Modified: 2004-06-09 23:28:00.842801600 (EDT)  
Accessed: 2004-06-09 23:28:00.842801600 (EDT)

## Searching files

Let's search for jpgs:

**Keyword Search of Allocated and Unallocated Space**

Enter the keyword string or expression to search for:

ASCII       Unicode  
 Case Insensitive       grep Regular Expression

**SEARCH**

**EXTRACT STRINGS**      **EXTRACT UNALLOCATED**

[Regular Expression Cheat Sheet](#)

**NOTE:** The keyword search runs grep on the image.  
A list of what will and what will not be found is available [here](#).

**Searching for ASCII: Done****Saving: Done**5 hits- [link to results](#)**Searching for Unicode: Done****Saving: Done**20 hits- [link to results](#)[\*\*New Search\*\*](#)**5 occurrences of jpg were found**

Search Options:

ASCII

Case Insensitive

Cluster 10672 ([Hex](#) - [Ascii](#))

1: 451 (\*jpG)

Cluster 10810 ([Hex](#) - [Ascii](#))

2: 36 (ile8.jpgUX)

Cluster 11464 ([Hex](#) - [Ascii](#))

3: 417 (ile8.jpgUX)

Cluster 11466 ([Hex](#) - [Ascii](#))

4: 36 (ile9.jpgUX)

Cluster 12040 ([Hex](#) - [Ascii](#))

5: 130 (ile9.jpgUX)

**20 occurrences of jpg were found**

Search Options:

Unicode

Case Insensitive

Cluster 2728 ([Hex](#) - [Ascii](#))

1: 182 (ile1.jpg)

After checking on the data that was found, we see the following results:

Occurrences of jpg were found with search options ASCII:

1. 451 (\*jpg)  
>> C:/archive/file10.tar.gz  
    Cluster: 10672  
    MFT Entry: 38-128-4
2. 36 (ile8.jpgUX)  
>> C:/archive/file8.zip  
    Cluster: 10810

```
MFT Entry: 39-128-3
3. 417 (ile8.jpgUX)
>> C:/archive/file8.zip
    Cluster: 11464
    MFT Entry: 39-128-3
4. 36 (ile9.jpgUX)
>> C:/archive/file9.boo
    Cluster: 11466
    MFT Entry: 40-128-3
5. 130 (ile9.jpgUX)
>> C:/archive/file9.boo
    Cluster: 12040
    MFT Entry: 40-128-3
```

Occurrences of **jpg** were found with search options **Unicode**:

```
1: 182 (ile1.jpg)
>> C://LogFile
    Cluster: 2728
    MFT Entry: 2728
2. 30 (ile1.jpg)
>> C://LogFile
    Cluster: 2729
    MFT Entry: 2-128-1
3. 462 (ile6.jpg)
>> C://LogFile
    Cluster: 2796
    MFT Entry: 2-128-1
4. 310 (ile6.jpg)
>> C://LogFile
    Cluster: 2797
    MFT Entry: 2-128-1
5. 214 (ile3.jpg)
>> C://LogFile
    Cluster: 2857
    MFT Entry: 2-128-1
6. 62 (ile3.jpg)
>> C://LogFile
    Cluster: 2858
    MFT Entry: 2-128-1
7. 198 (ile4.jpg)
>> C://LogFile
    Cluster: 2865
    MFT Entry: 2-128-1
8. 46 (ile4.jpg)
>> C://LogFile
    Cluster: 2866
    MFT Entry: 2-128-1
9. 134 (ile6.jpg)
>> C://LogFile
    Cluster: 3652
    MFT Entry: 2-128-1
```

```
10. 414 (ile1.jpg)
>> C://$MFT
    Cluster: 6753
    MFT Entry: 0-128-1
11. 254 (ile1.jpg)
>> C://$MFT
    Cluster: 6757
    MFT Entry: 0-128-1
12. 414 (ile6.jpg)
>> C://$MFT
    Cluster: 6759
    MFT Entry: 0-128-1
13. 254 (ile6.jpg)
>> C://$MFT
    Cluster: 6763
    MFT Entry: 0-128-1
14. 414 (ile3.jpg)
>> C://$MFT
    Cluster: 6765
    MFT Entry: 0-128-1
15. 6 (e4.jpg)
>> C://$MFT
    Cluster: 6766
    MFT Entry: 0-128-1
16. 254 (ile3.jpg)
>> C://$MFT
    Cluster: 6769
    MFT Entry: 0-128-1
17. 254 (ile4.jpg)
>> C://$MFT
    Cluster: 6771
    MFT Entry: 0-128-1
18. 240 (ict9.jpg)
>> C:/misc/file12.doc
    Cluster: 12583
    MFT Entry: 43-128-3
19. 0 (ict9.jpg)
>> C:/misc/file12.doc
    Cluster: 12818
    MFT Entry: 43-128-3
20. 300 (ile6.jpg)
>> Inode not found
```

This data gives us the idea of looking up on the following directories:

```
>> C: /archive/
>> C://LogFile
>> C://$MFT
>> C:/misc/
```

and the following files:

```
>> ile1.jpg
>> ile3.jpg
>> ile4.jpg
>> ile6.jpg
>> ile8.jpgUX

>> e4.jpg
>> ict9.jpg

>> C:/archive/file8.zip
>> C:/archive/file9.boo
>> C:/archive/file10.tar.gz
```

This data gave us compressed with hidden images:

1. 451 (\*jpg) >> C:/archive/file10.tar.gz
2. 36 (ile8.jpgUX) >> C:/archive/file8.zip
3. 417 (ile8.jpgUX) >> C:/archive/file8.zip
4. 36 (ile9.jpgUX) >> C:/archive/file9.boo
5. 130 (ile9.jpgUX) >> C:/archive/file9.boo

Where the attackers are using compressed files (**ZIP**, or **TAR**) to hide images. And the extension **boo** suggests that there is a possible obfuscation. More especifically:

- **file10.tar.gz**: This contains references to **JPG** files with possible objective files.
- **file8.zip**: Appears in multiple clusters and could contain **file.8.jpg**.
- **file9.boo**: Possible intentional obfuscation.

```
>> C://LogFile
- ile1.jpg (clusters 2728–2729)
- ile6.jpg (clusters 2796–2797)
- ile3.jpg (clusters 2857–2858)
- ile4.jpg (clusters 2865–2866)

>> C://$MFT
- ile1.jpg (clusters 6753, 6757)
- ile6.jpg (clusters 6759, 6763)
- ile3.jpg (clusters 6765, 6769)
- ile4.jpg (clusters 6771)
- e4.jpg (cluster 6766)
```

Where **\$LogFile** is the registry file of **NTFS** that shows operations with files. **MFT**: contains metadata of all files. So, the references in **\$LogFile** and **\$MFT** indicates that those **JPG** existed in the system and were

accessed to or modified. This will help us to rebuild the timeline of these files.

Also,

```
18. 240 (ict9.jpg) >> C:/misc/file12.doc  
19. 0 (ict9.jpg) >> C:/misc/file12.doc
```

indicates that **file12.doc** is a Word document that contains references to **file9.jpg**, this could indicate that it has malicious documents with macros that downloads/opens images.

Finally, the reference

```
20. 300 (ile6.jpg) >> Inode not found
```

Could indicate that the file was deleted, or overwritten, or the file system is corrupted.

So,

- **file1.jpg** >> references in **\$LogFile** and **\$MFT**.
- **file3.jpg** >> references in **\$LogFile** and **\$MFT**.
- **file4.jpg** >> references in **\$LogFile** and **\$MFT**.
- **file6.jpg** >> references in **\$LogFile** and **\$MFT**.
- **file8.jpg** >> contained in **file8.zip** and **\$MFT**.
- **file9.jpg** >> references in **file12.doc**, and contained in **file9.boo**.
- **file10.jpg** >> possibly contained in **file10.tar.gz**.

Possibly existed in the system, but we already found **file6.jpg** in deleted files. We need to look for the others.

### Extractionn of compressed files in **C://archive/**

```
>> C://archive/  
- file8.zip  
- file9.boo  
- file10.tar.gz
```

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

**FILE ANALYSIS** | **KEYWORD SEARCH** | **FILE TYPE** | **IMAGE DETAILS** | **META DATA** | **DATA UNIT** | **HELP** | **CLOSE**

| DEL. | Type   | Name          | WRITTEN                   | ACCESSED                  | CHANGED                   | CREATED                   | SIZE   | UID | GID | META     |
|------|--------|---------------|---------------------------|---------------------------|---------------------------|---------------------------|--------|-----|-----|----------|
|      | d / in | .wl           | 2004-06-09 23:59:10 (EDT) | 2004-06-09 23:59:10 (EDT) | 2004-06-09 23:59:10 (EDT) | 2004-06-09 23:22:22 (EDT) | 56     | 48  | 0   | 5-144-6  |
|      | d / d  | .wl           | 2004-06-09 23:28:51 (EDT) | 2004-06-09 23:28:52 (EDT) | 2004-06-09 23:28:51 (EDT) | 2004-06-09 23:28:37 (EDT) | 472    | 0   | 0   | 37-144-1 |
|      | r / r  | 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  | file8.zip     | 2004-06-10 03:16:42 (EDT) | 2004-06-09 23:28:51 (EDT) | 2004-06-09 23:28:51 (EDT) | 2004-06-09 23:28:51 (EDT) | 335371 | 0   | 0   | 39-128-3 |
|      | r / r  | file9.boo     | 2004-06-10 03:17:46 (EDT) | 2004-06-09 23:28:54 (EDT) | 2004-06-09 23:28:54 (EDT) | 2004-06-09 23:28:51 (EDT) | 294124 | 0   | 0   | 40-128-3 |

**File Name Search**  
Enter a Perl regular expression for the file names you want to find.  
   
 ALL DELETED FILES  
 EXPAND DIRECTORIES

**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

```
>> C://archive/file8.zip
```

vol1-C..archive.file8.zip

Archive Edit View Help

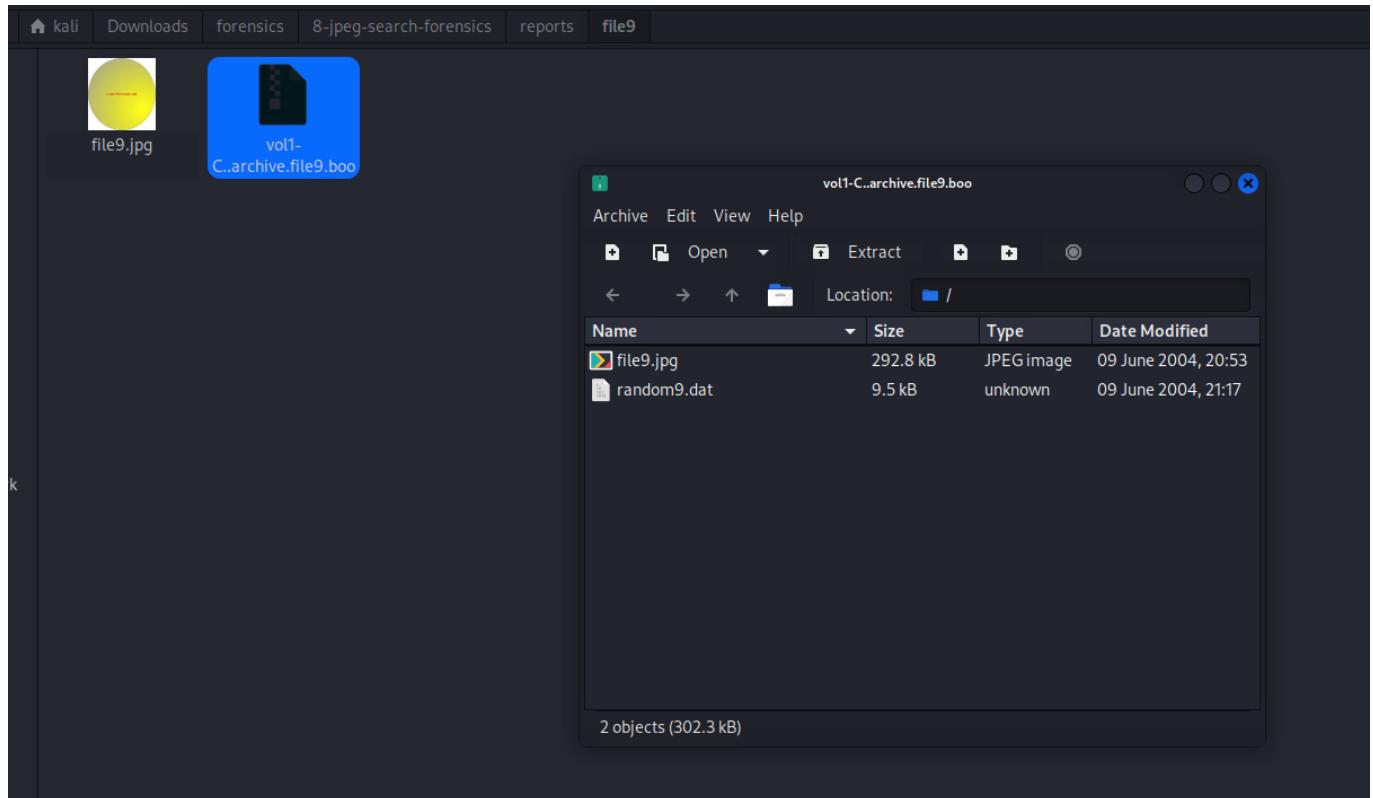
Open Extract

Location: /

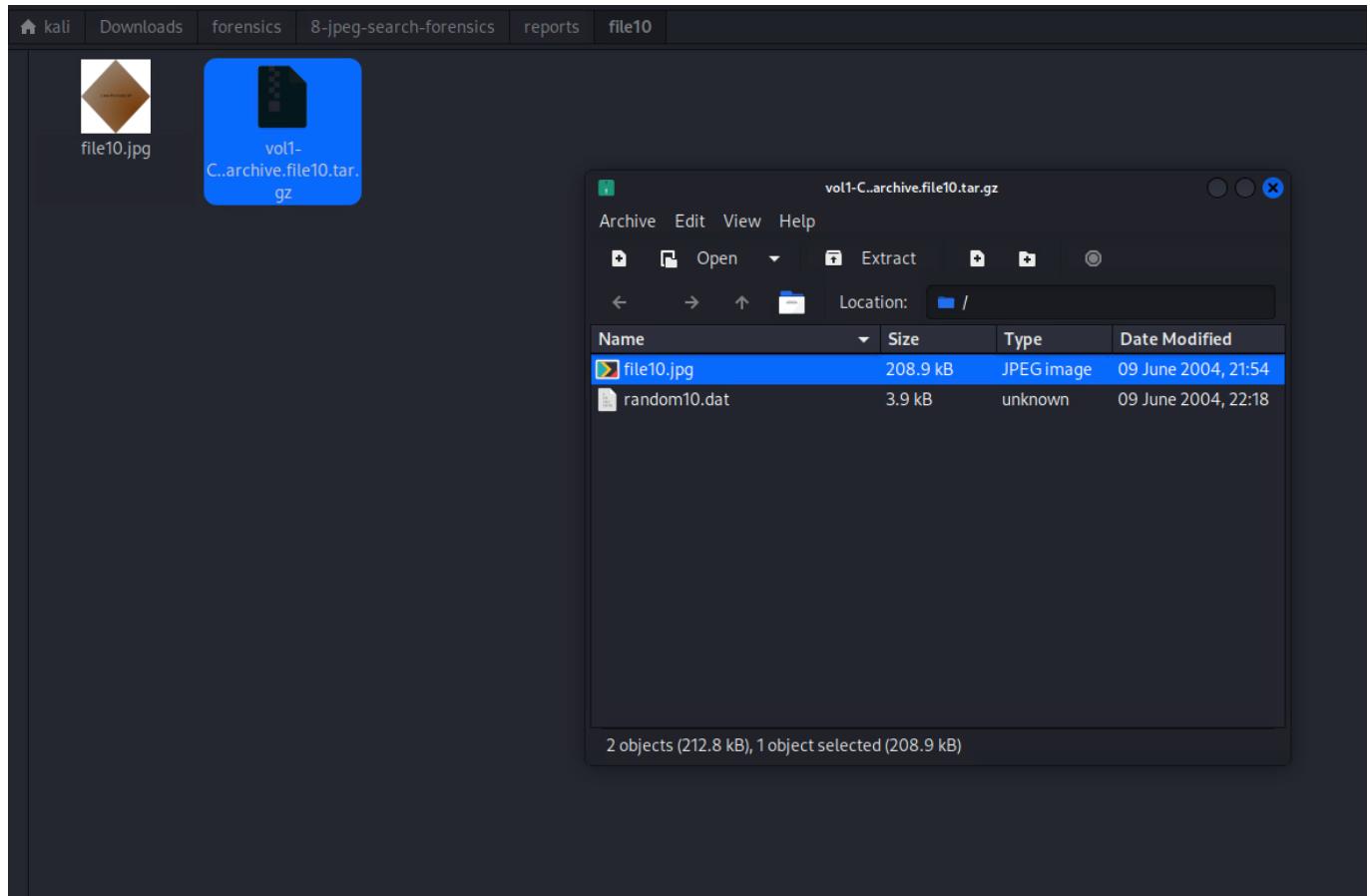
| Name        | Size     | Type       | Date Modified       |
|-------------|----------|------------|---------------------|
| file8.jpg   | 337.7 kB | JPEG image | 09 June 2004, 20:52 |
| random8.dat | 4.1 kB   | unknown    | 09 June 2004, 21:06 |

2 objects (341.8 kB)

```
>> C://archive/file9.boo
```



```
>> C://archive/file10.tar.gz
```



## Extractionn of compressed files in C://alloc/

```
>> C://alloc/
- file1.jpg
- file2.dat
```

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

**FILE ANALYSIS** **KEYWORD SEARCH** **FILE TYPE** **IMAGE DETAILS** **META DATA** **DATA UNIT** **HELP** **CLOSE**

| DEL | Type     | Name      | WRITTEN                   | ACCESSED                  | CHANGED                   | CREATED                   | SIZE   | UID | GID | META     |
|-----|----------|-----------|---------------------------|---------------------------|---------------------------|---------------------------|--------|-----|-----|----------|
|     | dir / in | ..        | 2004-06-09 23:59:10 (EDT) | 2004-06-09 23:59:10 (EDT) | 2004-06-09 23:59:10 (EDT) | 2004-06-09 23:22:22 (EDT) | 56     | 48  | 0   | 5-144-6  |
|     | d / d    | ..        | 2004-06-09 23:27:36 (EDT) | 2004-06-09 23:27:36 (EDT) | 2004-06-09 23:27:36 (EDT) | 2004-06-09 23:27:06 (EDT) | 256    | 0   | 0   | 27-144-1 |
|     | r / r    | 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    | 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 |

**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.

**SEARCH**

**ALL DELETED FILES**

**EXPAND DIRECTORIES**

**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

```
>> C://alloc/file1.jpg
```

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

**FILE ANALYSIS** **KEYWORD SEARCH** **FILE TYPE** **IMAGE DETAILS** **META DATA** **DATA UNIT** **HELP** **CLOSE**

| DEL | Type     | Name      | WRITTEN                   | ACCESSED                  | CHANGED                   | CREATED                   | SIZE   | UID | GID | META     |
|-----|----------|-----------|---------------------------|---------------------------|---------------------------|---------------------------|--------|-----|-----|----------|
|     | dir / in | ..        | 2004-06-09 23:59:10 (EDT) | 2004-06-09 23:59:10 (EDT) | 2004-06-09 23:59:10 (EDT) | 2004-06-09 23:22:22 (EDT) | 56     | 48  | 0   | 5-144-6  |
|     | d / d    | ..        | 2004-06-09 23:27:36 (EDT) | 2004-06-09 23:27:36 (EDT) | 2004-06-09 23:27:36 (EDT) | 2004-06-09 23:27:06 (EDT) | 256    | 0   | 0   | 27-144-1 |
|     | r / r    | 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    | 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 |

**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.

**SEARCH**

**ALL DELETED FILES**

**EXPAND DIRECTORIES**

ASCII (display - report) \* Hex (display - report) \* ASCII Strings (display - report) \* Export \* View \* Add Note  
File Type: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 696x752, components 3

C:/alloc/file1.jpg

**Thumbnail:** [View Full Size Image](#)

```
>> C://alloc/file2.dat
```

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

**FILE ANALYSIS** **KEYWORD SEARCH** **FILE TYPE** **IMAGE DETAILS** **META DATA** **DATA UNIT** **HELP** **CLOSE**

| DEL | Type     | Name      | WRITTEN                   | ACCESSED                  | CHANGED                   | CREATED                   | SIZE   | UID | GID | META     |
|-----|----------|-----------|---------------------------|---------------------------|---------------------------|---------------------------|--------|-----|-----|----------|
|     | dir / in | .1        | 2004-06-09 23:59:10 (EDT) | 2004-06-09 23:59:10 (EDT) | 2004-06-09 23:59:10 (EDT) | 2004-06-09 23:22:22 (EDT) | 56     | 48  | 0   | 5-144-6  |
|     | d / d    | .1        | 2004-06-09 23:27:36 (EDT) | 2004-06-09 23:27:36 (EDT) | 2004-06-09 23:27:36 (EDT) | 2004-06-09 23:27:06 (EDT) | 256    | 0   | 0   | 27-144-1 |
|     | r / r    | 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    | 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 |

ASCII (display - report) \* Hex (display - report) \* ASCII Strings (display - report) \* Export \* View \* Add Note  
File Type: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 437x365, components 3

C:/alloc/file2.dat

**Thumbnail:** [View Full Size Image](#)

I AM PICTURE #2

## Extractionn of compressed files in C://misc/

```
>> C://misc/
- file12.doc
- file13.dll:here
```

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

**FILE ANALYSIS** **KEYWORD SEARCH** **FILE TYPE** **IMAGE DETAILS** **META DATA** **DATA UNIT** **HELP** **CLOSE**

| DEL | Type     | Name            | WRITTEN                   | ACCESSED                  | CHANGED                   | CREATED                   | SIZE   | UID | GID | META     |
|-----|----------|-----------------|---------------------------|---------------------------|---------------------------|---------------------------|--------|-----|-----|----------|
|     | dir / in | .1              | 2004-06-09 23:59:10 (EDT) | 2004-06-09 23:59:10 (EDT) | 2004-06-09 23:59:10 (EDT) | 2004-06-09 23:22:22 (EDT) | 56     | 48  | 0   | 5-144-6  |
|     | d / d    | .1              | 2004-06-09 23:29:18 (EDT) | 2004-06-09 23:29:18 (EDT) | 2004-06-09 23:29:18 (EDT) | 2004-06-09 23:29:00 (EDT) | 360    | 0   | 0   | 41-144-1 |
|     | r / r    | file11.dat      | 2004-06-10 03:44:46 (EDT) | 2004-06-09 23:29:17 (EDT) | 2004-06-09 23:29:17 (EDT) | 2004-06-09 23:29:17 (EDT) | 272753 | 0   | 0   | 42-128-3 |
|     | r / r    | file12.doc      | 2004-06-10 03:20:58 (EDT) | 2004-06-09 23:29:18 (EDT) | 2004-06-09 23:29:18 (EDT) | 2004-06-09 23:29:17 (EDT) | 131584 | 0   | 0   | 43-128-3 |
|     | r / r    | file13.dll      | 2004-06-09 23:29:45 (EDT) | 2004-06-09 23:29:45 (EDT) | 2004-06-09 23:29:45 (EDT) | 2004-06-09 23:29:45 (EDT) | 58391  | 0   | 0   | 44-128-3 |
|     | r / r    | file13.dll:here | 2004-06-09 23:29:45 (EDT) | 2004-06-09 23:29:45 (EDT) | 2004-06-09 23:29:45 (EDT) | 2004-06-09 23:29:18 (EDT) | 124038 | 0   | 0   | 44-128-5 |

ASCII (display - report) \* Hex (display - report) \* ASCII Strings (display - report) \* Export \* Add Note  
File Type: data

```
>> C://misc/file13.dll:here
```

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

**FILE ANALYSIS** **KEYWORD SEARCH** **FILE TYPE** **IMAGE DETAILS** **META DATA** **DATA UNIT** **HELP** **CLOSE**

| DEL | Type     | Name            | WRITTEN                   | ACCESSED                  | CHANGED                   | CREATED                   | SIZE   | UID | GID | META     |
|-----|----------|-----------------|---------------------------|---------------------------|---------------------------|---------------------------|--------|-----|-----|----------|
|     | dir / in | .1              | 2004-06-09 23:59:10 (EDT) | 2004-06-09 23:59:10 (EDT) | 2004-06-09 23:59:10 (EDT) | 2004-06-09 23:22:22 (EDT) | 56     | 48  | 0   | 5-144-6  |
|     | d / d    | .1              | 2004-06-09 23:29:18 (EDT) | 2004-06-09 23:29:18 (EDT) | 2004-06-09 23:29:18 (EDT) | 2004-06-09 23:29:00 (EDT) | 360    | 0   | 0   | 41-144-1 |
|     | r / r    | file11.dat      | 2004-06-10 03:44:46 (EDT) | 2004-06-09 23:29:17 (EDT) | 2004-06-09 23:29:17 (EDT) | 2004-06-09 23:29:17 (EDT) | 272753 | 0   | 0   | 42-128-3 |
|     | r / r    | file12.doc      | 2004-06-10 03:20:58 (EDT) | 2004-06-09 23:29:18 (EDT) | 2004-06-09 23:29:18 (EDT) | 2004-06-09 23:29:17 (EDT) | 131584 | 0   | 0   | 43-128-3 |
|     | r / r    | file13.dll      | 2004-06-09 23:29:45 (EDT) | 2004-06-09 23:29:45 (EDT) | 2004-06-09 23:29:45 (EDT) | 2004-06-09 23:29:45 (EDT) | 58391  | 0   | 0   | 44-128-3 |
|     | r / r    | file13.dll:here | 2004-06-09 23:29:45 (EDT) | 2004-06-09 23:29:45 (EDT) | 2004-06-09 23:29:45 (EDT) | 2004-06-09 23:29:18 (EDT) | 124038 | 0   | 0   | 44-128-5 |

ASCII (display - report) \* Hex (display - report) \* ASCII Strings (display - report) \* Export \* View \* Add Note  
File Type: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 518x563, components 3

C:/misc/file13.dll:here

**Thumbnail:** [View Full Size Image](#)

## Extractionn of compressed files in C://invalid/

```
>> C://invalid/
- file3.jpg
- file4.jpg
- file5.rtf
```

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

**FILE ANALYSIS** **KEYWORD SEARCH** **FILE TYPE** **IMAGE DETAILS** **META DATA** **DATA UNIT** **HELP** **CLOSE**

| DEL | Type     | Name      | WRITTEN                   | ACCESSED                  | CHANGED                   | CREATED                   | SIZE   | UID | GID | META     |
|-----|----------|-----------|---------------------------|---------------------------|---------------------------|---------------------------|--------|-----|-----|----------|
|     | dir / in | .1        | 2004-06-09 23:59:10 (EDT) | 2004-06-09 23:59:10 (EDT) | 2004-06-09 23:59:10 (EDT) | 2004-06-09 23:22:22 (EDT) | 56     | 48  | 0   | 5-144-6  |
|     | d / d    | .1        | 2004-06-09 23:28:20 (EDT) | 2004-06-09 23:28:21 (EDT) | 2004-06-09 23:28:20 (EDT) | 2004-06-09 23:28:08 (EDT) | 360    | 0   | 0   | 33-144-1 |
|     | r / r    | file3.jpg | 2004-06-10 03:27:02 (EDT) | 2004-06-09 23:28:20 (EDT) | 2004-06-09 23:28:20 (EDT) | 2004-06-09 23:28:20 (EDT) | 214228 | 0   | 0   | 35-128-3 |
|     | r / r    | file4.jpg | 2004-06-10 03:38:06 (EDT) | 2004-06-09 23:28:22 (EDT) | 2004-06-09 23:28:22 (EDT) | 2004-06-09 23:28:20 (EDT) | 189021 | 0   | 0   | 36-128-3 |
|     | r / r    | file5.rtf | 2004-06-10 03:41:54 (EDT) | 2004-06-09 23:28:20 (EDT) | 2004-06-09 23:28:20 (EDT) | 2004-06-09 23:28:20 (EDT) | 148102 | 0   | 0   | 34-128-3 |

**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

```
>> C://invalid/file3.jpg
```

>> C://invalid/file4.jpg

>> C://invalid/file5.rtf

The screenshot shows the Autopsy Forensic Browser interface. The top navigation bar includes links for Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The main title is "localhost:9999/autopsy?mod=1&submod=2&case=forensics&host=host1&inv=unknown&vol=vol1". Below the title is a toolbar with buttons for FILE ANALYSIS, KEYWORD SEARCH, FILE TYPE, IMAGE DETAILS, META DATA, DATA UNIT, HELP, and CLOSE.

**Directory Seek**: A sidebar with the text "Enter the name of a directory that you want to view." and a "VIEW" button.

**File Name Search**: A sidebar with the text "Enter a Perl regular expression for the file names you want to find." and a "SEARCH" button.

**All Deleted Files**: A sidebar with the text "EXPAND DIRECTORIES".

**Current Directory:** C:/invalid/ (highlighted in yellow). Buttons for "Add Note" and "GENERATE MD5 LIST OF FILES".

**File List Table:**

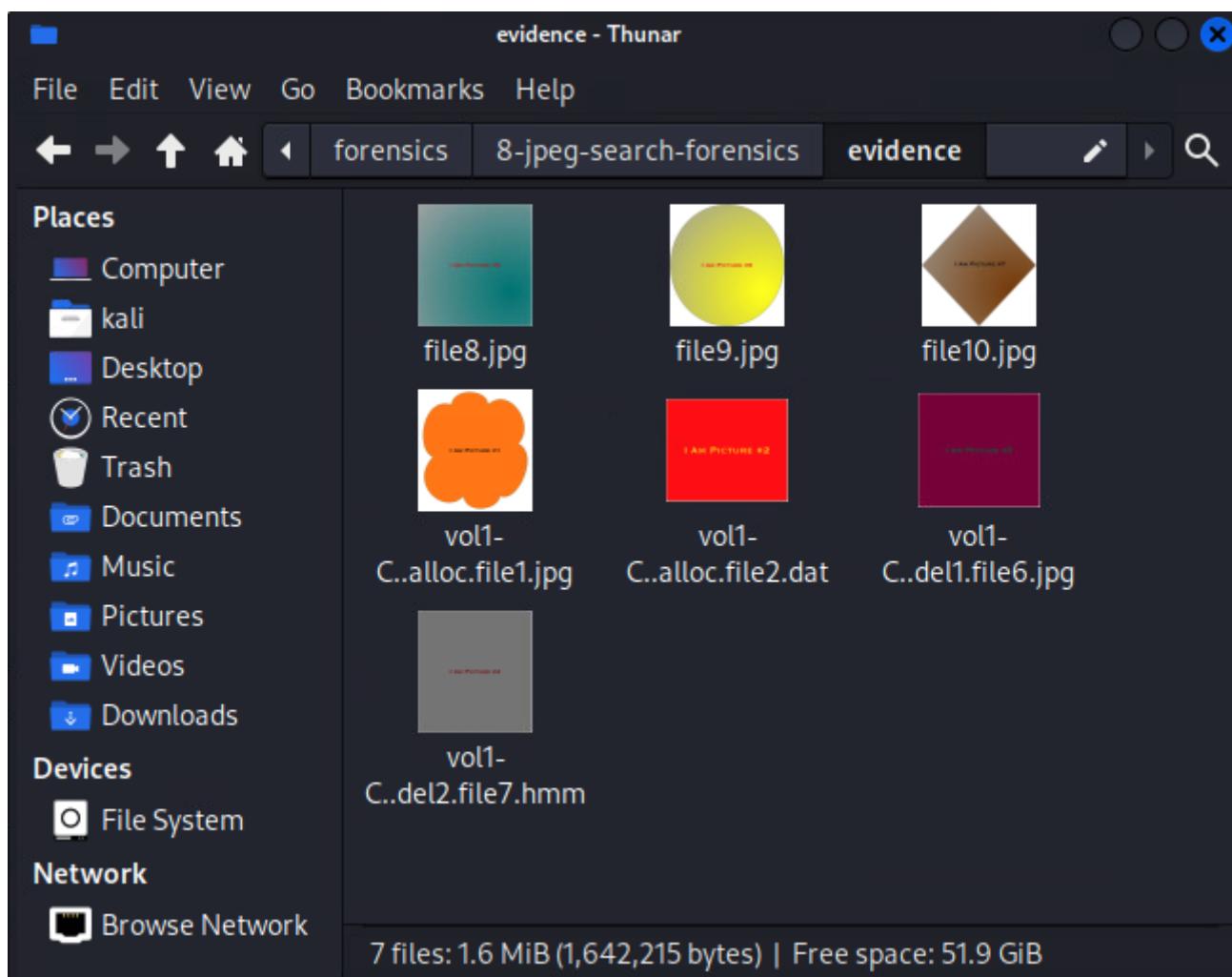
| DEL   | Type      | Name      | Written                   | Accessed                  | Changed                   | Created                   | Size   | UID | GID | META     |
|-------|-----------|-----------|---------------------------|---------------------------|---------------------------|---------------------------|--------|-----|-----|----------|
| d / d | dir / in  | ..        | 2004-06-09 23:59:10 (EDT) | 2004-06-09 23:59:10 (EDT) | 2004-06-09 23:59:10 (EDT) | 2004-06-09 23:22:22 (EDT) | 56     | 48  | 0   | 5-144-6  |
| d / d | dir / in  | ..        | 2004-06-09 23:28:20 (EDT) | 2004-06-09 23:28:21 (EDT) | 2004-06-09 23:28:20 (EDT) | 2004-06-09 23:28:08 (EDT) | 360    | 0   | 0   | 33-144-1 |
| r / r | file3.jpg | file3.jpg | 2004-06-10 03:27:02 (EDT) | 2004-06-09 23:28:20 (EDT) | 2004-06-09 23:28:20 (EDT) | 2004-06-09 23:28:20 (EDT) | 214228 | 0   | 0   | 35-128-3 |
| r / r | file4.jpg | file4.jpg | 2004-06-10 03:38:06 (EDT) | 2004-06-09 23:28:22 (EDT) | 2004-06-09 23:28:22 (EDT) | 2004-06-09 23:28:20 (EDT) | 189021 | 0   | 0   | 36-128-3 |
| r / r | file5.rtf | file5.rtf | 2004-06-10 03:41:54 (EDT) | 2004-06-09 23:28:20 (EDT) | 2004-06-09 23:28:20 (EDT) | 2004-06-09 23:28:20 (EDT) | 148102 | 0   | 0   | 34-128-3 |

**File Content Preview:** ASCII (display - report) \* Hex (display - report) \* ASCII Strings (display - report) \* Export \* Add Note  
File Type: data

Contents Of File: C:/invalid/file5.rtf

```
...RTF content in hex and ASCII representation...
```

JPG files recovered.



All the **ASCII** and **Hex** reports may be found in the folder **8-jpeg-search** folder:

```
L$ tree .
```

```
.
```

```
+- 8-jpeg-search.dd
+- 8-jpeg-search-forensic-copy.dd
+- COPYING-GNU.txt
+- evidence_md5_hash_copy.txt
+- evidence_md5_hash.txt
+- forensics/
   +- 8-jpeg-search-forensics
      +- evidence
         +- file10.jpg
         +- file8.jpg
         +- file9.jpg
         +- vol1-C..alloc.file1.jpg
         +- vol1-C..alloc.file2.dat
         +- vol1-C..del1.file6.jpg
         +- vol1-C..del2.file7.hmm
      +- reports
         +- file1
            +- ASCII-filename=vol1-C..alloc.file1.jpg.txt
            +- Hex-filename=vol1-C..alloc.file1.jpg.txt
            +- vol1-C..alloc.file1.jpg
            +- vol1-meta29-128-3.raw
         +- file10
            +- ASCII-filename=vol1-C..archive.file10.tar.gz.txt
            +- file10.jpg
            +- Hex-filename=vol1-C..archive.file10.tar.gz.txt
            +- vol1-C..archive.file10.tar.gz
         +- file13
            +- ASCII-filename=vol1-C..misc.file13.dll.here.txt
            +- Hex-filename=vol1-C..misc.file13.dll.here.txt
            +- vol1-meta44-128-5.raw
         +- file2
            +- ASCII-filename=vol1-C..alloc.file2.dat.txt
            +- Hex-filename=vol1-C..alloc.file2.dat.txt
            +- vol1-C..alloc.file2.dat
            +- vol1-meta28-128-3.raw
         +- file3
            +- ASCII-filename=vol1-C..invalid.file3.jpg.txt
            +- Hex-filename=vol1-C..invalid.file3.jpg.txt
            +- vol1-meta35-128-3.raw
         +- file5
            +- ASCII-filename=vol1-C..invalid.file5.rtf.txt
            +- Hex-filename=vol1-C..invalid.file5.rtf.txt
            +- vol1-meta34-128-3.raw
         +- file6
            +- ASCII-filename=vol1-C..vol1-meta-32-128-3.txt
            +- hex-filename=vol1-C..vol1-meta-32-128-3.txt
            +- vol1-C..del1.file6.jpg
            +- vol1-meta32-128-3.raw
         +- file7
            +- ASCII-filename=vol1-C..del2.file7.hmm.txt
            +- hex-filename=vol1-C..del2.file7.hmm.txt
            +- vol1-C..del2.file7.hmm
            +- vol1-meta31-128-3.raw
         +- file8
            +- ASCII-filename=vol1-C..archive.file8.zip.txt
            +- file8.jpg
            +- Hex-filename=vol1-C..archive.file8.zip.txt
            +- vol1-C..archive.file8.zip
         +- file9
            +- ASCII-filename=vol1-C..archive.file9.boo.txt
            +- file9.jpg
            +- Hex-filename=vol1-C..archive.file9.boo.txt
            +- vol1-C..archive.file9.boo
      +- screenshots
+- index.html
+- README.txt
+- results.txt
```

```
8-jpeg-search/
+- 8-jpeg-search.dd
+- 8-jpeg-search-forensic-copy.dd
+- COPYING-GNU.txt
+- evidence_md5_hash_copy.txt
+- evidence_md5_hash.txt
+- forensics/
```

```
└── 8-jpeg-search-forensics/
    ├── evidence/
    │   ├── file0.jpg
    │   ├── file8.jpg
    │   ├── file9.jpg
    │   ├── vol1-C..alloc.file1.jpg
    │   ├── vol1-C..alloc.file2.dat
    │   ├── vol1-C..del1.file6.jpg
    │   └── vol1-C..del2.file7.hmm
    ├── reports/
    │   ├── file1/
    │   │   ├── ASCII-filename=vol1-C..alloc.file1.jpg.txt
    │   │   ├── Hex-filename=vol1-C..alloc.file1.jpg.txt
    │   │   ├── vol1-C..archive.file1.jpg
    │   │   └── vol1-meta29-128-3.raw
    │   ├── file10/
    │   │   ├── ASCII-filename=vol1-C..archive.file10.tar.gz.txt
    │   │   ├── file10.jpg
    │   │   ├── Hex-filename=vol1-C..archive.file10.tar.gz.txt
    │   │   └── vol1-C..archive.file10.tar.gz
    │   ├── files/
    │   │   ├── ASCII-filename=vol1-C..misc.file13.dll.here.txt
    │   │   ├── Hex-filename=vol1-C..misc.file13.dll.here.txt
    │   │   └── vol1-meta44-128-5.raw
    │   ├── file2/
    │   │   ├── ASCII-filename=vol1-C..alloc.file2.dat.txt
    │   │   ├── Hex-filename=vol1-C..alloc.file2.dat.txt
    │   │   ├── vol1-C..alloc.file2.dat
    │   │   └── vol1-meta28-128-3.raw
    │   ├── files/
    │   │   ├── ASCII-filename=vol1-C..invalid.file3.jpg.txt
    │   │   ├── Hex-filename=vol1-C..invalid.file3.jpg.txt
    │   │   └── vol1-meta35-128-3.raw
    │   ├── file6/
    │   │   ├── ASCII-filename=vol1-C..invalid.file5.trf.txt
    │   │   ├── Hex-filename=vol1-C..invalid.file5.trf.txt
    │   │   └── vol1-meta34-128-3.raw
    │   ├── file6/
    │   │   ├── ASCII-filename=vol1-C..vol1-meta-32-128-3.txt
    │   │   ├── Hex-filename=vol1-C..vol1-meta-32-128-3.txt
    │   │   ├── vol1-C..del1.file6.jpg
    │   │   └── vol1-meta32-128-3.raw
    │   ├── file7/
    │   │   ├── ASCII-filename=vol1-C..del2.file7.hmm.txt
    │   │   ├── Hex-filename=vol1-C..del2.file7.hmm.txt
    │   │   ├── vol1-C..del2.file7.hmm
    │   │   └── vol1-meta31-128-3.raw
    │   ├── files/
    │   │   ├── ASCII-filename=vol1-C..archive.file8.zip.txt
    │   │   ├── Hex-filename=vol1-C..archive.file8.zip.txt
    │   │   └── vol1-C..archive.file8.zip
    │   ├── file9/
    │   │   ├── ASCII-filename=vol1-C..archive.file9.b00.txt
```

```
    └── Hex-filename=vol1-C..archive.file9.b00.txt  
        └── vol1-C..archive.file9.b00
```

## Findings Summary:

| Files           | Original location | State   |
|-----------------|-------------------|---|
| file1.jpg       | C:\alloc\         | Recovered from assigned space                                   |
| file2.dat       | C:\alloc\         | Recovered (extension <b>dat</b> ) - possible <b>jpg</b> renamed |
| file3.jpg       | C:\invalid\       | Marked as "invalid" - damaged/corrupted format                  |
| file4.jpg       | Not found         | Unexistent, overwritten or obfuscated file                      |
| file5.trf       | C:\invalid\       | Extension <b>.trf</b> - unknown format                          |
| file6.jpg       | C:\del1\          | Recovered from deleted space                                    |
| file7.hmm       | C:\del2\          | Recovered (extension <b>hmm</b> ) - unknown format              |
| file8.zip       | C:\archive\       | Contains <b>file8.jpg</b>                                       |
| file9.boo       | C:\archive\       | Contains <b>file9.jpg</b> (obfuscated extension)                |
| file10.tar.gz   | C:\archive\       | Contains <b>file10.jpg</b>                                      |
| file13.dll.here | C:\misc\          | Suspicious <b>dll</b> file - suspicious executable file         |