CIS-387: Digital Forensics (4 credits)

With Dr. Jinhua Guo

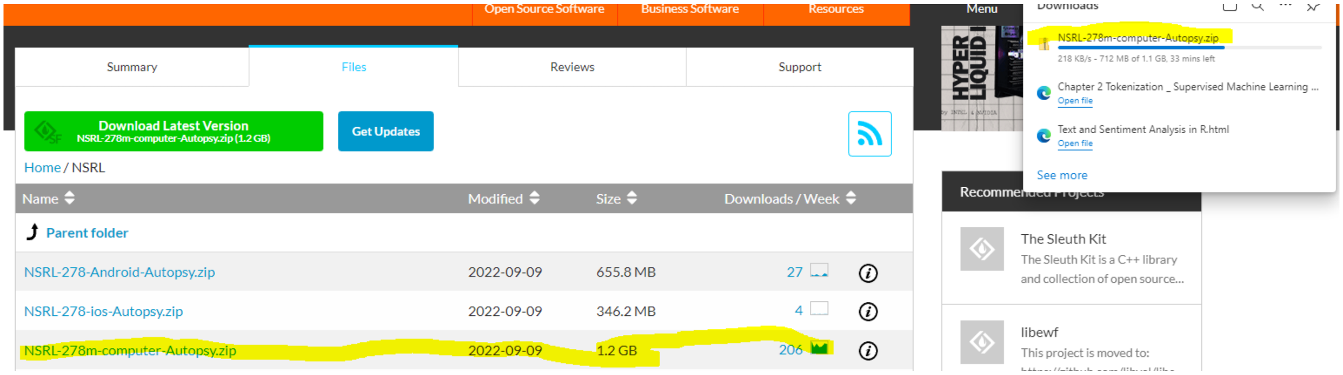
Lab 7 - National Software Reference Library (NSRL) Hash Analysis

Demetrius Johnson

November 16, 2022

INSTRUCTIONS

Downloading NSRL index file from http://sourceforge.net/projects/autopsy/files/NSRL/:



Home / NSRL

Name	Modified	Size	Downloads / Week
Parent folder			
NSRL-278-Android-Autopsy.zip	2022-09-09	655.8 MB	27
NSRL-278-ios-Autopsy.zip	2022-09-09	346.2 MB	4
NSRL-278m-computer-Autopsy.zip	2022-09-09	1.2 GB	206

Downloads

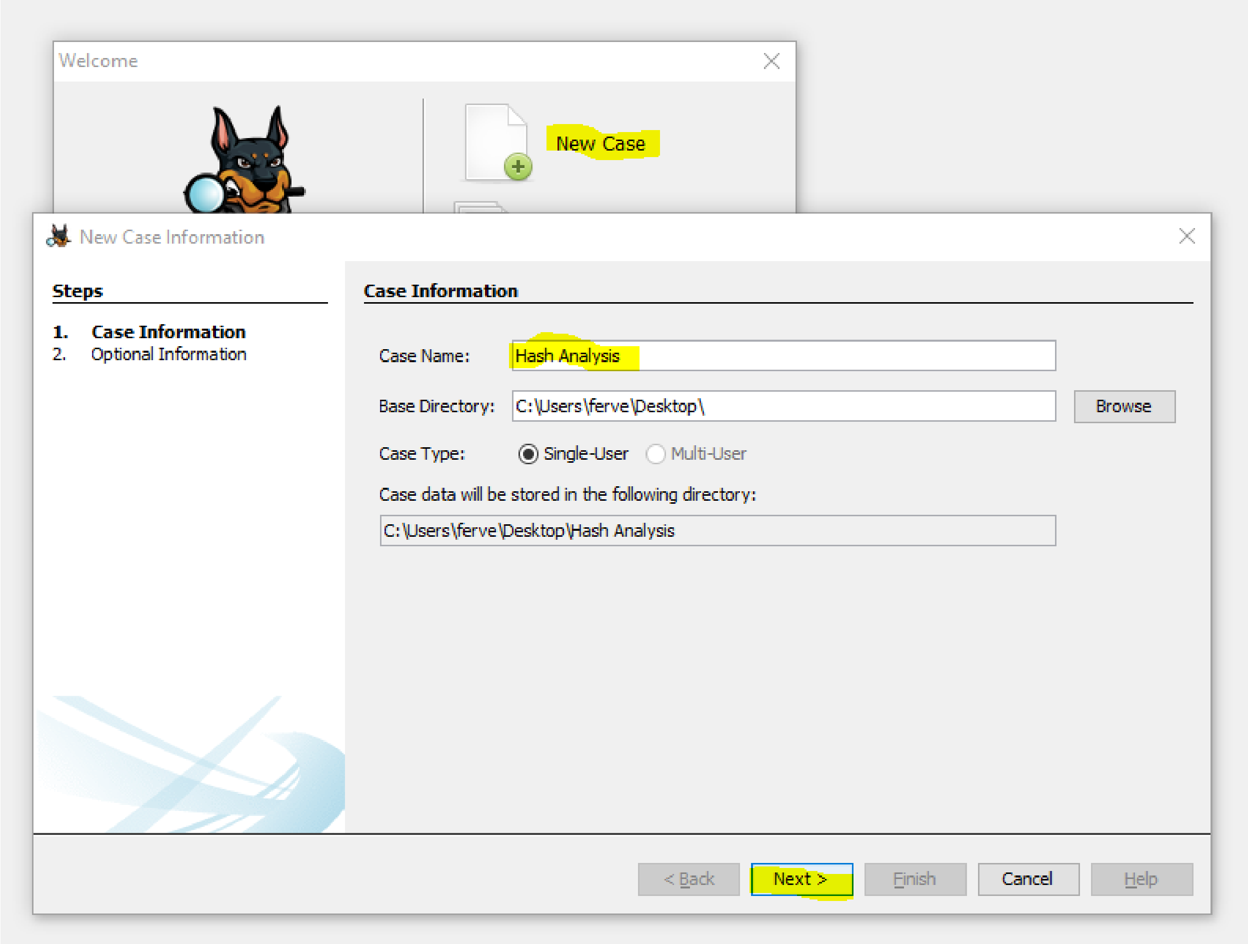
NSRL-278m-computer-Autopsy.zip
218 KB/s - 712 MB of 1.1 GB, 33 mins left

Chapter 2 Tokenization _ Supervised Machine Learning ...
Open file

Text and Sentiment Analysis in R.html
Open file

See more

1. Launch Autopsy and create a case, Create New Case and name it as "Hash Analysis".



Case Information

Case Name: Hash Analysis

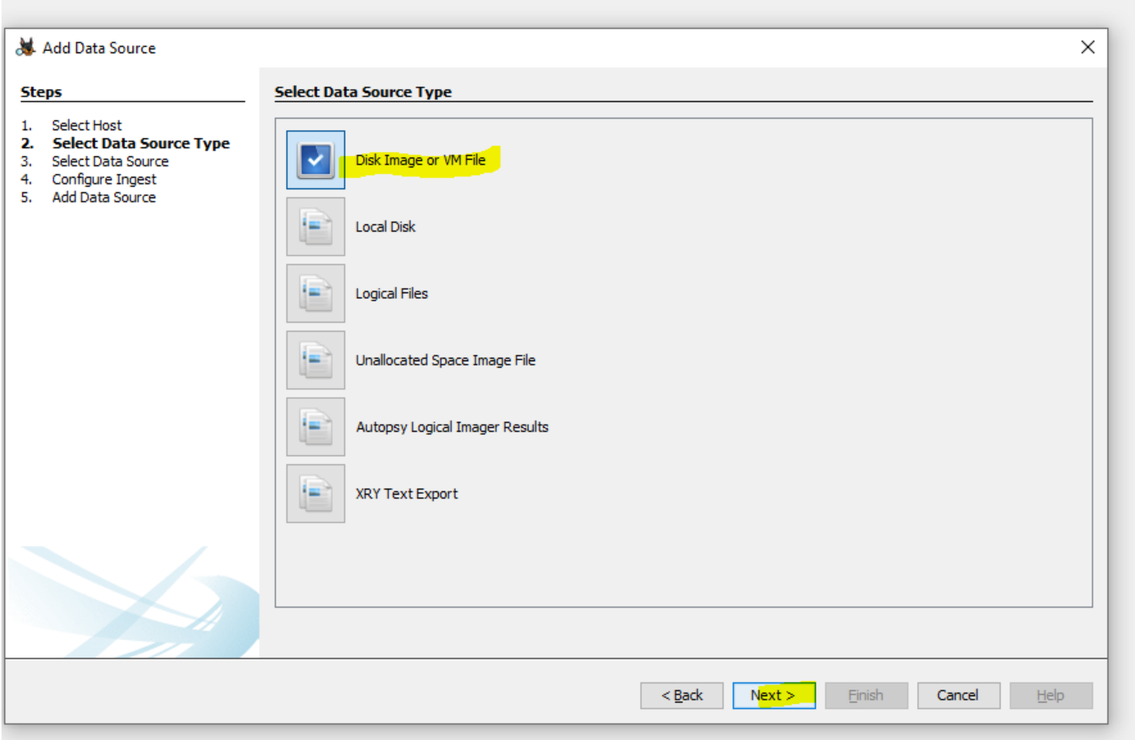
Base Directory: C:\Users\ferve\Desktop\

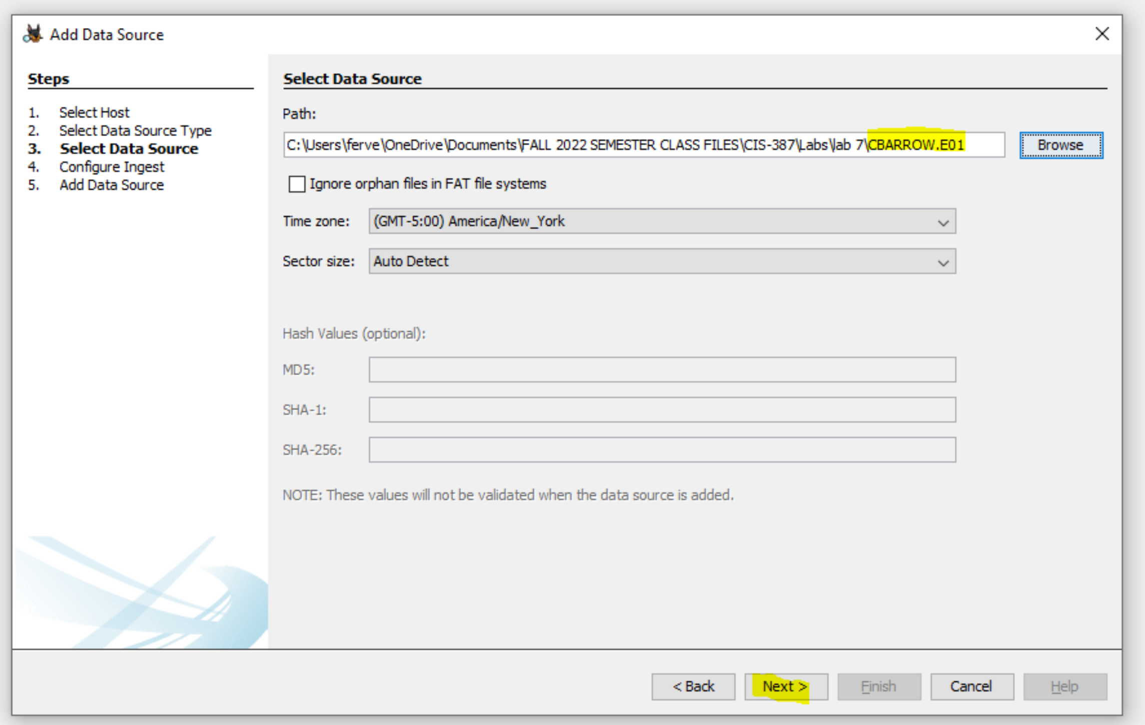
Case Type: ● Single-User ○ Multi-User

Case data will be stored in the following directory:

C:\Users\ferve\Desktop\Hash Analysis

2. Add data source type: choose Disk Image; browse and select the path to "CBARROW.E01".





Path: C:\Users\ferve\OneDrive\Documents\FALL 2022 SEMESTER CLASS FILES\CIS-387\Labs\lab 7\CBARROW.E01

☐ Ignore orphan files in FAT file systems

Time zone: (GMT-5:00) America/New_York

Sector size: Auto Detect

Hash Values (optional):

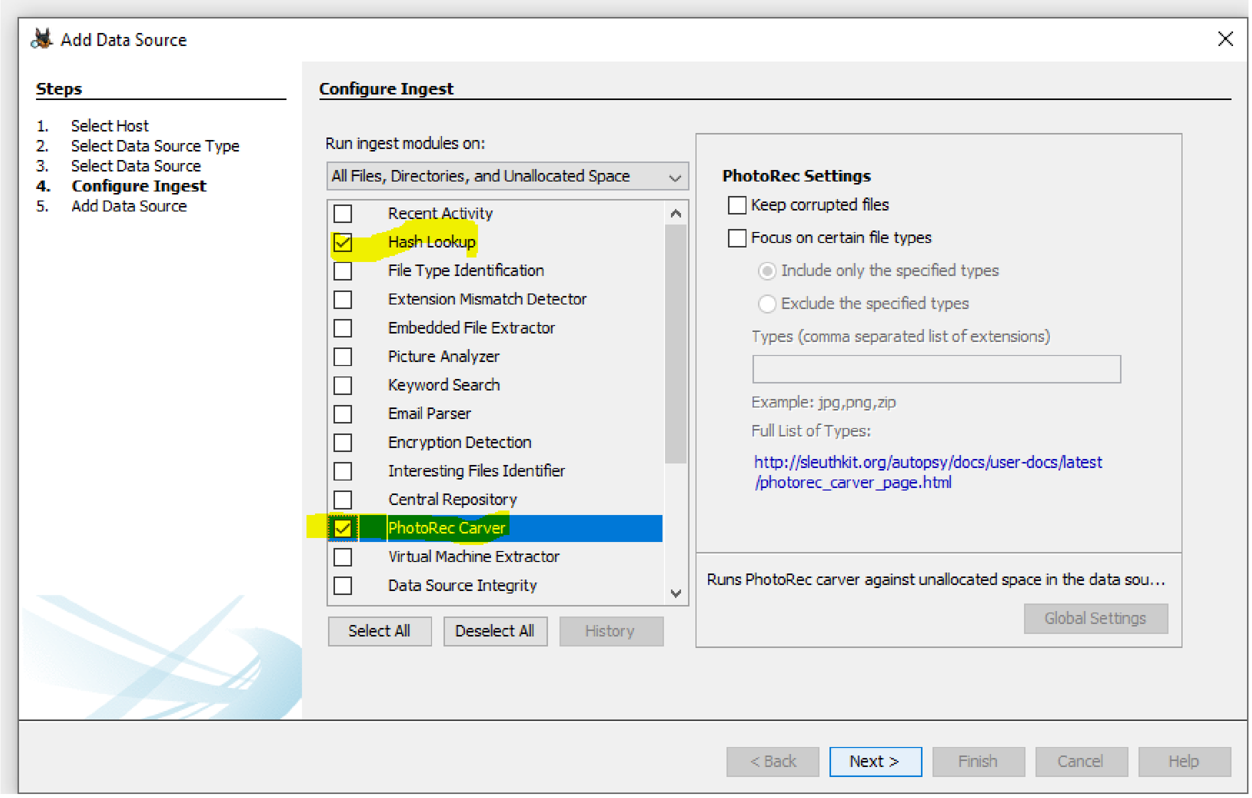
MD5:

SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

3. In the Ingest (processing) modules window, uncheck all modules except the “Hash Database Lookup Module” and “PhotoRec Carver Module”;



Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. **Configure Ingest**
5. Add Data Source

Configure Ingest

Run ingest modules on: All Files, Directories, and Unallocated Space

□ Recent Activity
☑ Hash Lookup
□ File Type Identification
□ Extension Mismatch Detector
□ Embedded File Extractor
□ Picture Analyzer
□ Keyword Search
□ Email Parser
□ Encryption Detection
□ Interesting Files Identifier
□ Central Repository
☑ PhotoRec Carver
□ Virtual Machine Extractor
□ Data Source Integrity

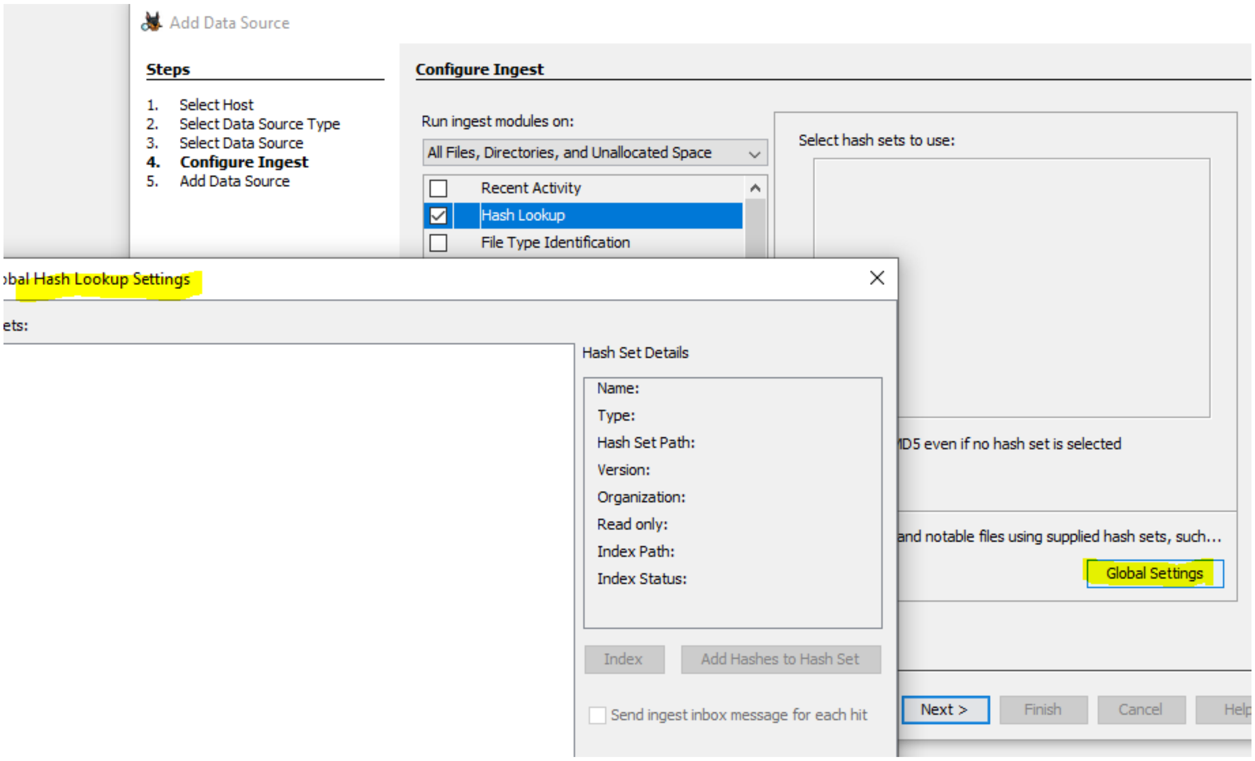
PhotoRec Settings

□ Keep corrupted files
□ Focus on certain file types
● Include only the specified types
○ Exclude the specified types
Types (comma separated list of extensions)

Example: jpg,png,zip
Full List of Types:
http://sleuthkit.org/autopsy/docs/user-docs/latest/photorec_carver_page.html

Runs PhotoRec carver against unallocated space in the data sou…

4. Click “Hash Database Lookup Module” and the click Global Setting.



Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. **Configure Ingest**
5. Add Data Source

Configure Ingest

Run ingest modules on:

All Files, Directories, and Unallocated Space

□ Recent Activity
☑ Hash Lookup
□ File Type Identification

Select hash sets to use:

ıbal Hash Lookup Settings

ets:

Hash Set Details

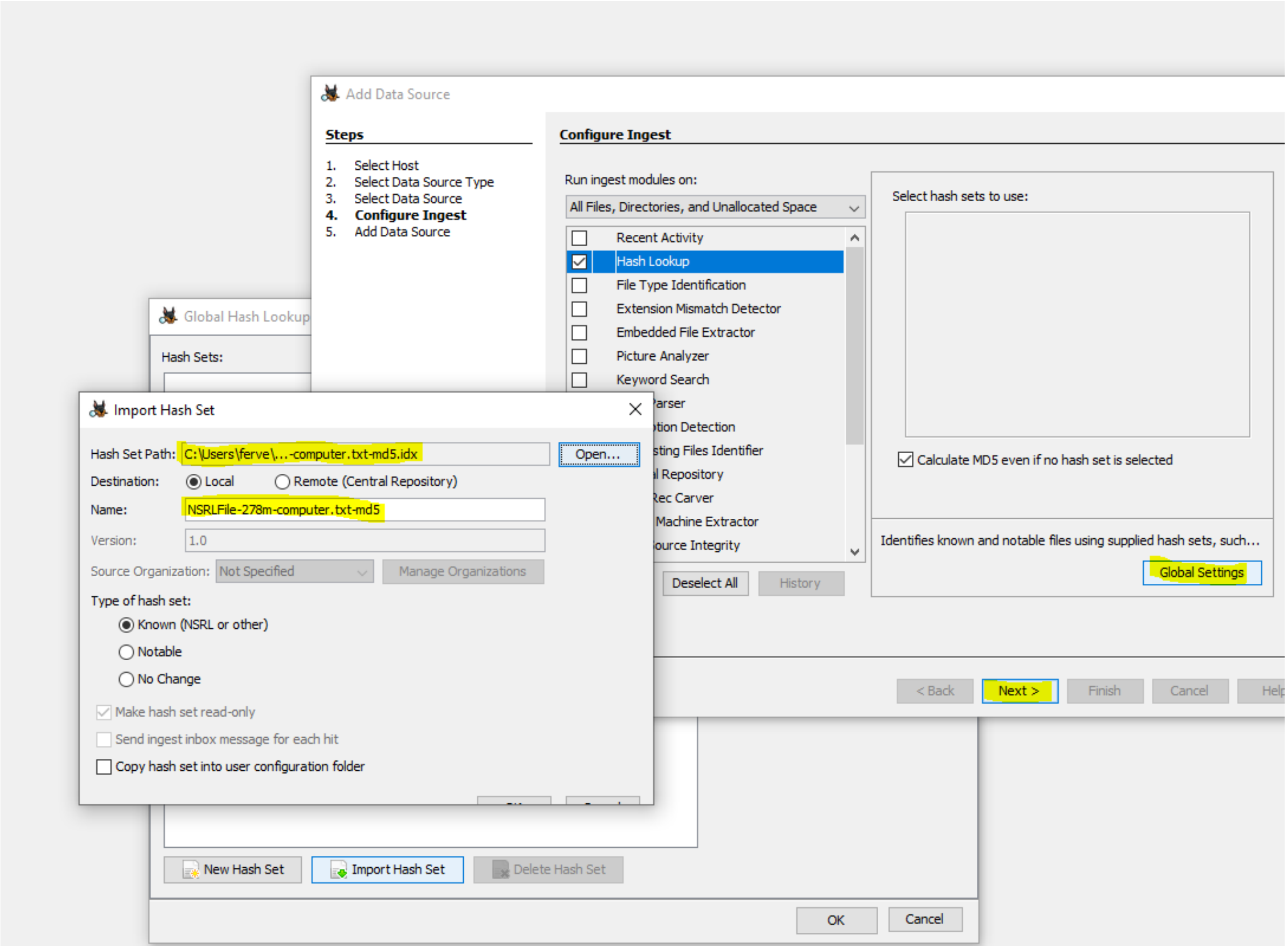
Name:
Type:
Hash Set Path:
Version:
Organization:
Read only:
Index Path:
Index Status:

□ Send ingest inbox message for each hit

ID5 even if no hash set is selected

and notable files using supplied hash sets, such…

5. At the “Global Hash Lookup Setting” window, click “Import Hash Set”, open your downloaded NRSL hash set index file (.idx), and check the “Known” option under the Type of Hash Set.



Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. **Configure Ingest**
5. Add Data Source

Configure Ingest

Run ingest modules on: All Files, Directories, and Unallocated Space

- □ Recent Activity
- ☑ Hash Lookup
- □ File Type Identification
- □ Extension Mismatch Detector
- □ Embedded File Extractor
- □ Picture Analyzer
- □ Keyword Search

Select hash sets to use:

☑ Calculate MD5 even if no hash set is selected

Identifies known and notable files using supplied hash sets, such...

Global Settings

< Back | Next > | Finish | Cancel | Help

Global Hash Lookup

Hash Sets:

New Hash Set | Import Hash Set | Delete Hash Set

OK | Cancel

Import Hash Set

Hash Set Path: C:\Users\ferve\...-computer.txt-md5.idx | Open...

Destination: ● Local ○ Remote (Central Repository)

Name: NSRLFile-278m-computer.txt-md5

Version: 1.0

Source Organization: Not Specified | Manage Organizations

Type of hash set:

● Known (NSRL or other)

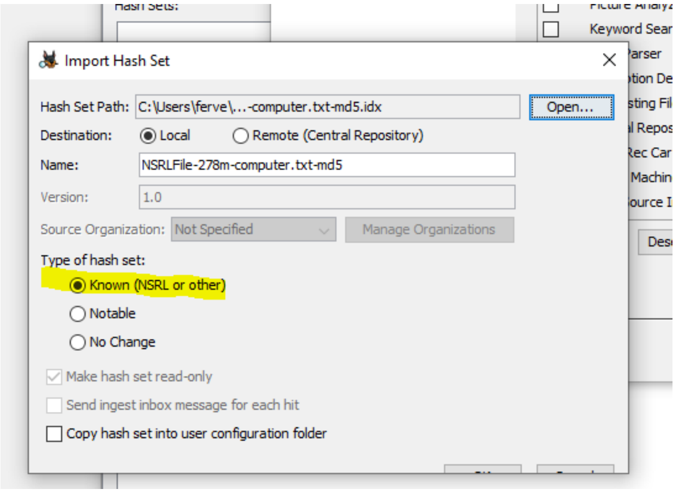
○ Notable

○ No Change

☑ Make hash set read-only

□ Send ingest inbox message for each hit

□ Copy hash set into user configuration folder



Import Hash Set

Hash Set Path: C:\Users\ferve\...-computer.txt-md5.idx | Open...

Destination: ● Local ○ Remote (Central Repository)

Name: NSRLFile-278m-computer.txt-md5

Version: 1.0

Source Organization: Not Specified | Manage Organizations

Type of hash set:

● Known (NSRL or other)

○ Notable

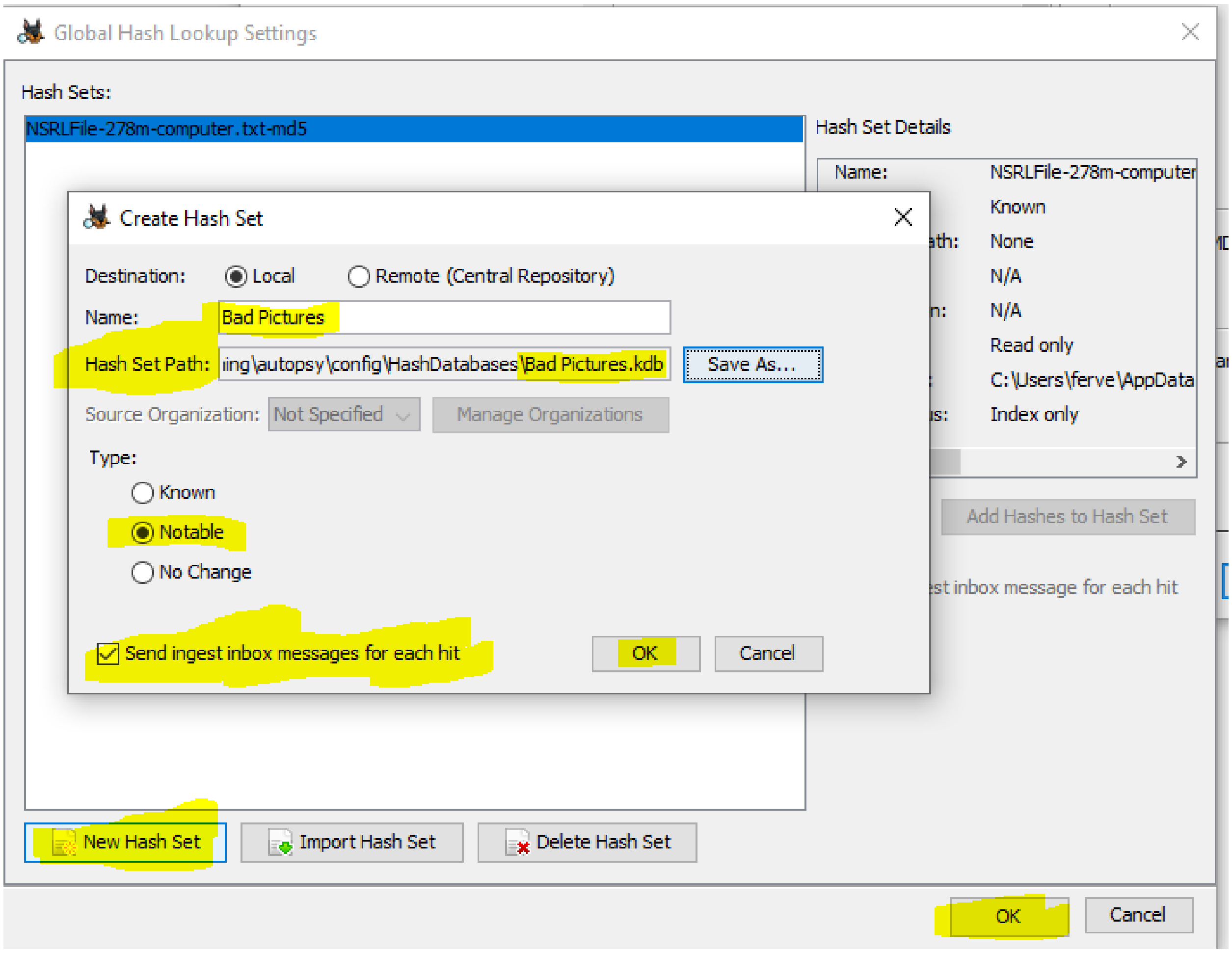
○ No Change

☑ Make hash set read-only

□ Send ingest inbox message for each hit

□ Copy hash set into user configuration folder

6. Click “New Hash Set” and then input “BadPictures” in the name field and choose a “Hash Set Path”, and, and check “Notable” type, and check “send ingest inbox messages for each hit”.



Hash Sets:
NSRLFile-278m-computer.txt-md5

Hash Set Details
Name: NSRLFile-278m-computer
Known
th: None
N/A
n: N/A
Read only
: C:\Users\ferve\AppData
s: Index only

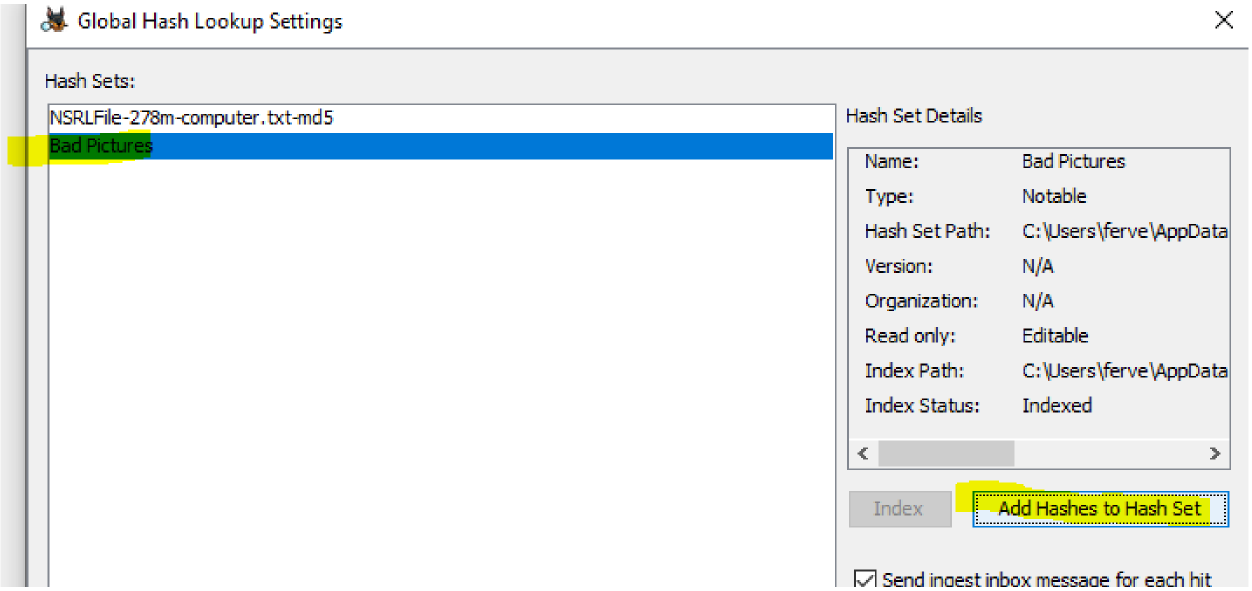
st inbox message for each hit

Destination: ● Local ○ Remote (Central Repository)
Name: Bad Pictures
Hash Set Path: ing\autopsy\config\HashDatabases\Bad Pictures.kdb
Source Organization: Not Specified
Type:
○ Known
● Notable
○ No Change
☑ Send ingest inbox messages for each hit

7. Click “OK”; and click “Add Hashes to Hash Set” and then copy and paste the following MD5 hashes:

1. 7d97aa329fe261c90bf68ee4104d4b85
2. 74a61bd54942d7e68fa0748e29dae219
3. 324c5372431efb4e01aa4849f3f0cb18
4. 2f649e8bb4ac958fd9ae8295da15200a
5. a58012d0bc57365fd58e975761fca8b9

CIS-387 – LAB 7 – MEECH



Global Hash Lookup Settings

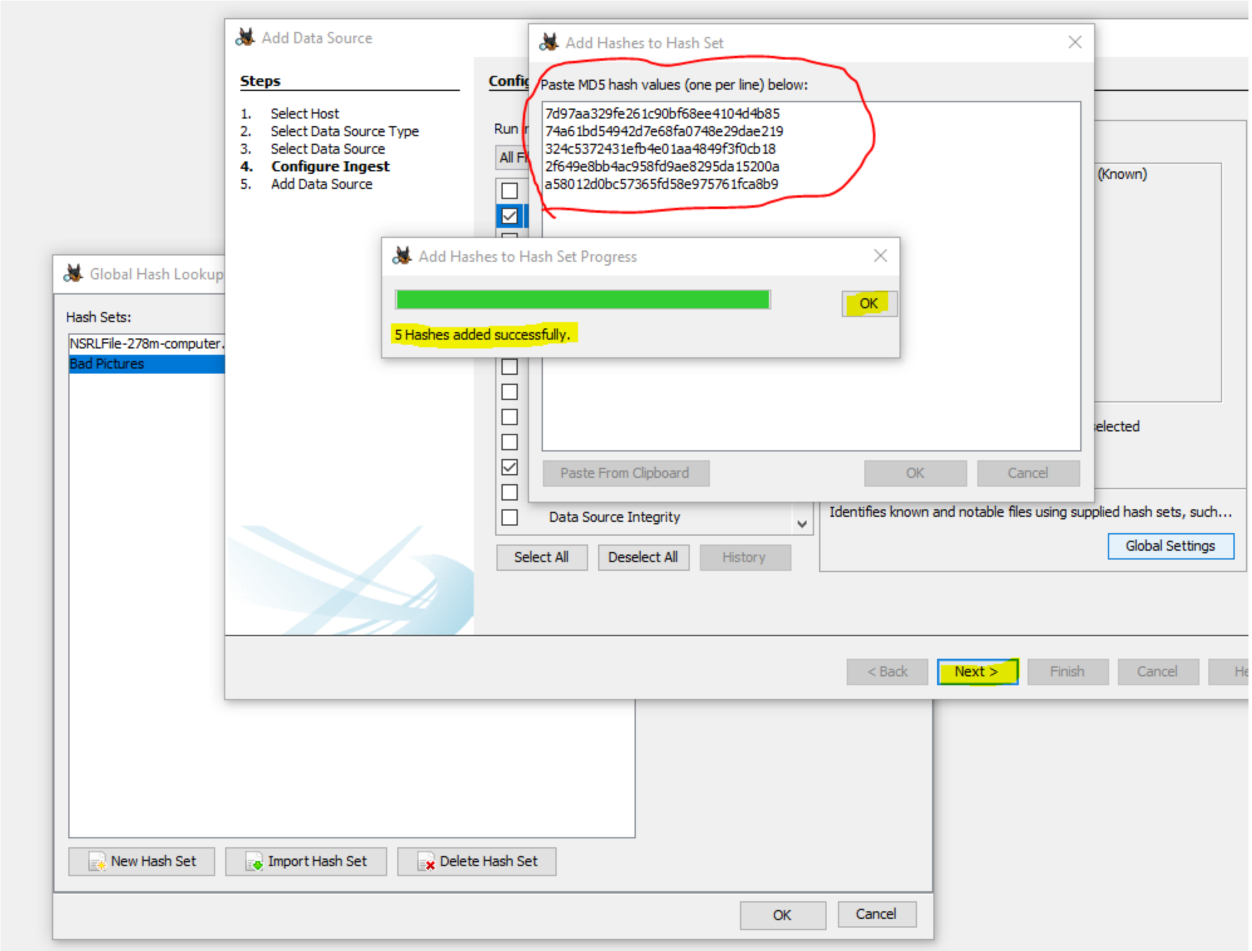
Hash Sets:

- NSRLFile-278m-computer.txt-md5
- Bad Pictures

Hash Set Details

Name:	Bad Pictures
Type:	Notable
Hash Set Path:	C:\Users\ferve\AppData
Version:	N/A
Organization:	N/A
Read only:	Editable
Index Path:	C:\Users\ferve\AppData
Index Status:	Indexed

☑ Send ingest inbox message for each hit



Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. **Configure Ingest**
5. Add Data Source

Add Hashes to Hash Set

Paste MD5 hash values (one per line) below:

```
7d97aa329fe261c90bf68ee4104d4b85
74a61bd54942d7e68fa0748e29dae219
324c5372431efb4e01aa4849f3f0cb18
2f649e8bb4ac958fd9ae8295da15200a
a58012d0bc57365fd58e975761fca8b9
```

Add Hashes to Hash Set Progress

5 Hashes added successfully.

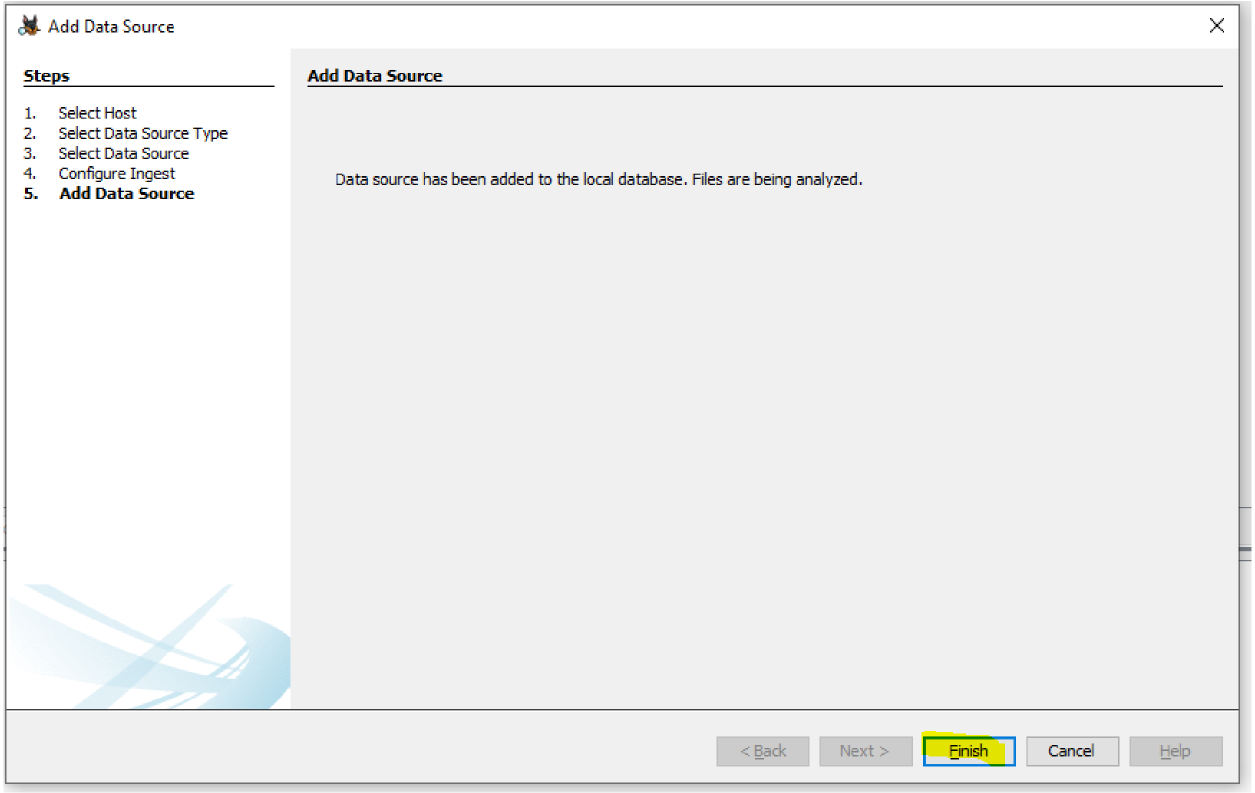
Identifies known and notable files using supplied hash sets, such...

Global Hash Lookup

Hash Sets:

- NSRLFile-278m-computer.
- Bad Pictures

8. Click “OK” twice; click Next and then click Finish.



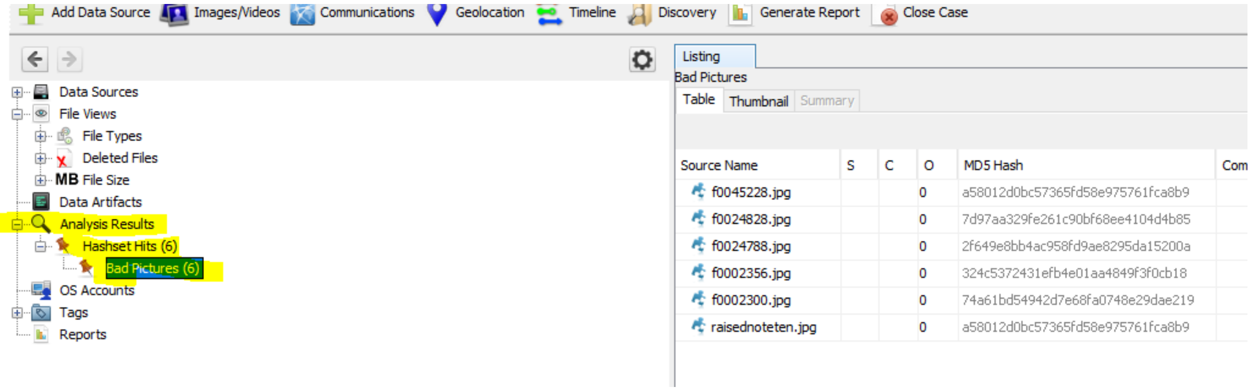
Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. **Add Data Source**

Add Data Source

Data source has been added to the local database. Files are being analyzed.

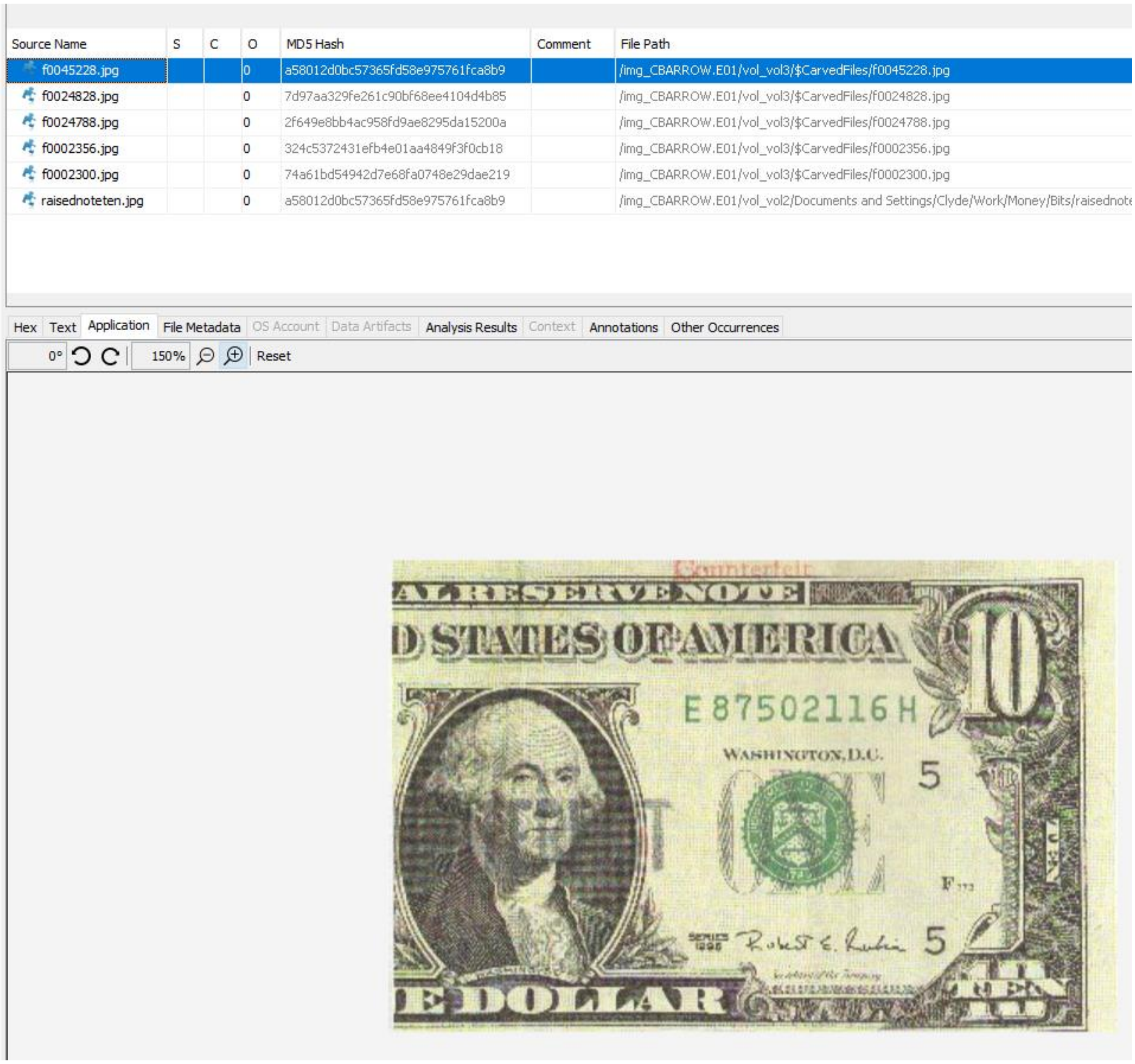
9. Review the search results under Results > Hashset Hits > BadPictures, and find all the hits.



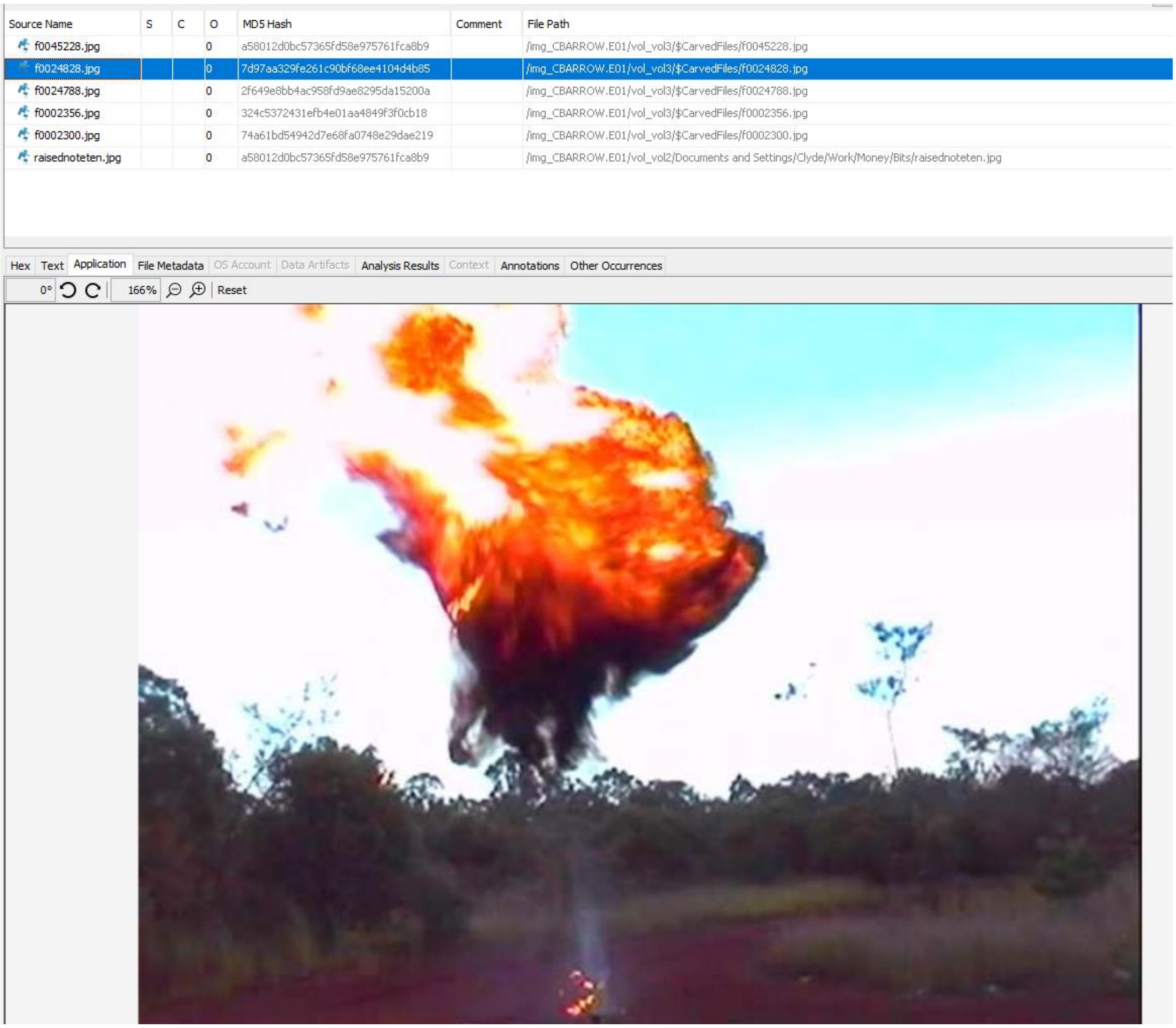
Bad Pictures

Source Name	S	C	O	MD5 Hash	Com
f0045228.jpg			0	a58012d0bc57365fd58e975761fca8b9	
f0024828.jpg			0	7d97aa329fe261c90bf68ee4104d4b85	
f0024788.jpg			0	2f649e8bb4ac958fd9ae8295da15200a	
f0002356.jpg			0	324c5372431efb4e01aa4849f3f0cb18	
f0002300.jpg			0	74a61bd54942d7e68fa0748e29dae219	
raisednoteten.jpg			0	a58012d0bc57365fd58e975761fca8b9	

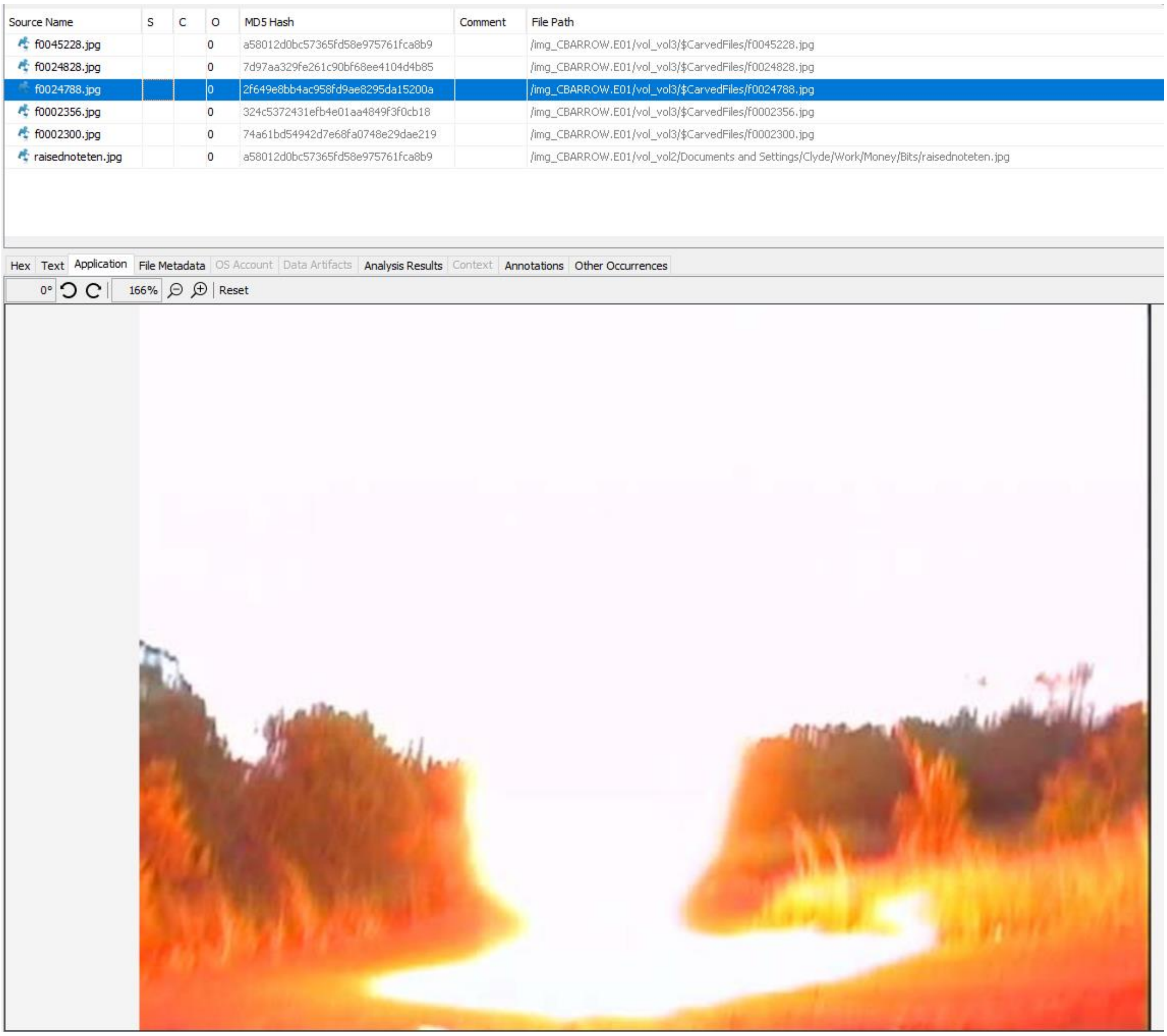
It appears that 5 out of 6 hashes from BadFile Hash set has made a hit:



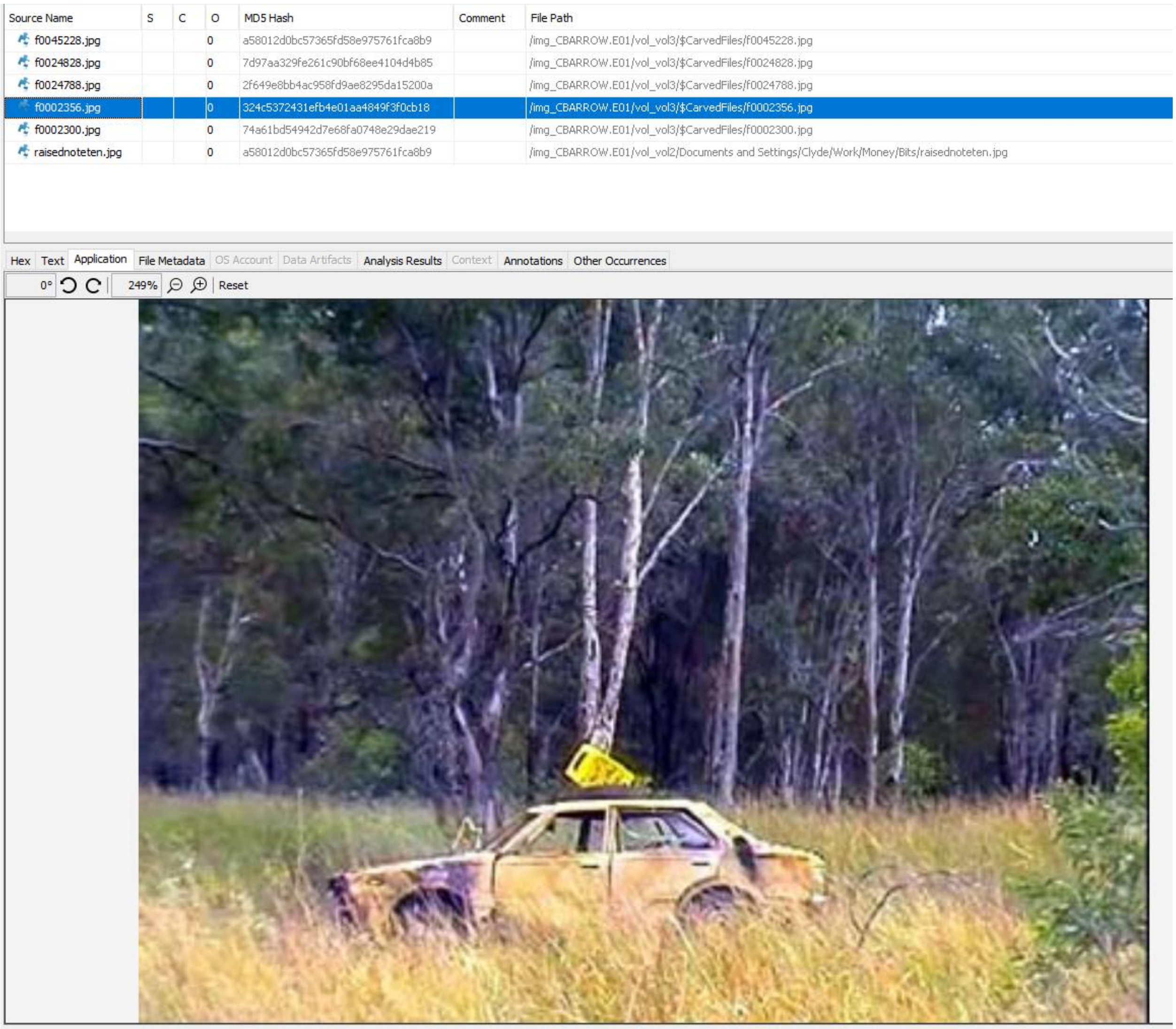
Source Name	S	C	O	MD5 Hash	Comment	File Path
f0045228.jpg			0	a58012d0bc57365fd58e975761fca8b9		/img_CBARROW.E01/vol_vol3/$CarvedFiles/f0045228.jpg
f0024828.jpg			0	7d97aa329fe261c90bf68ee4104d4b85		/img_CBARROW.E01/vol_vol3/$CarvedFiles/f0024828.jpg
f0024788.jpg			0	2f649e8bb4ac958fd9ae8295da15200a		/img_CBARROW.E01/vol_vol3/$CarvedFiles/f0024788.jpg
f0002356.jpg			0	324c5372431efb4e01aa4849f3f0cb18		/img_CBARROW.E01/vol_vol3/$CarvedFiles/f0002356.jpg
f0002300.jpg			0	74a61bd54942d7e68fa0748e29dae219		/img_CBARROW.E01/vol_vol3/$CarvedFiles/f0002300.jpg
raisednoteten.jpg			0	a58012d0bc57365fd58e975761fca8b9		/img_CBARROW.E01/vol_vol2/Documents and Settings/Clyde/Work/Money/Bits/raisednote



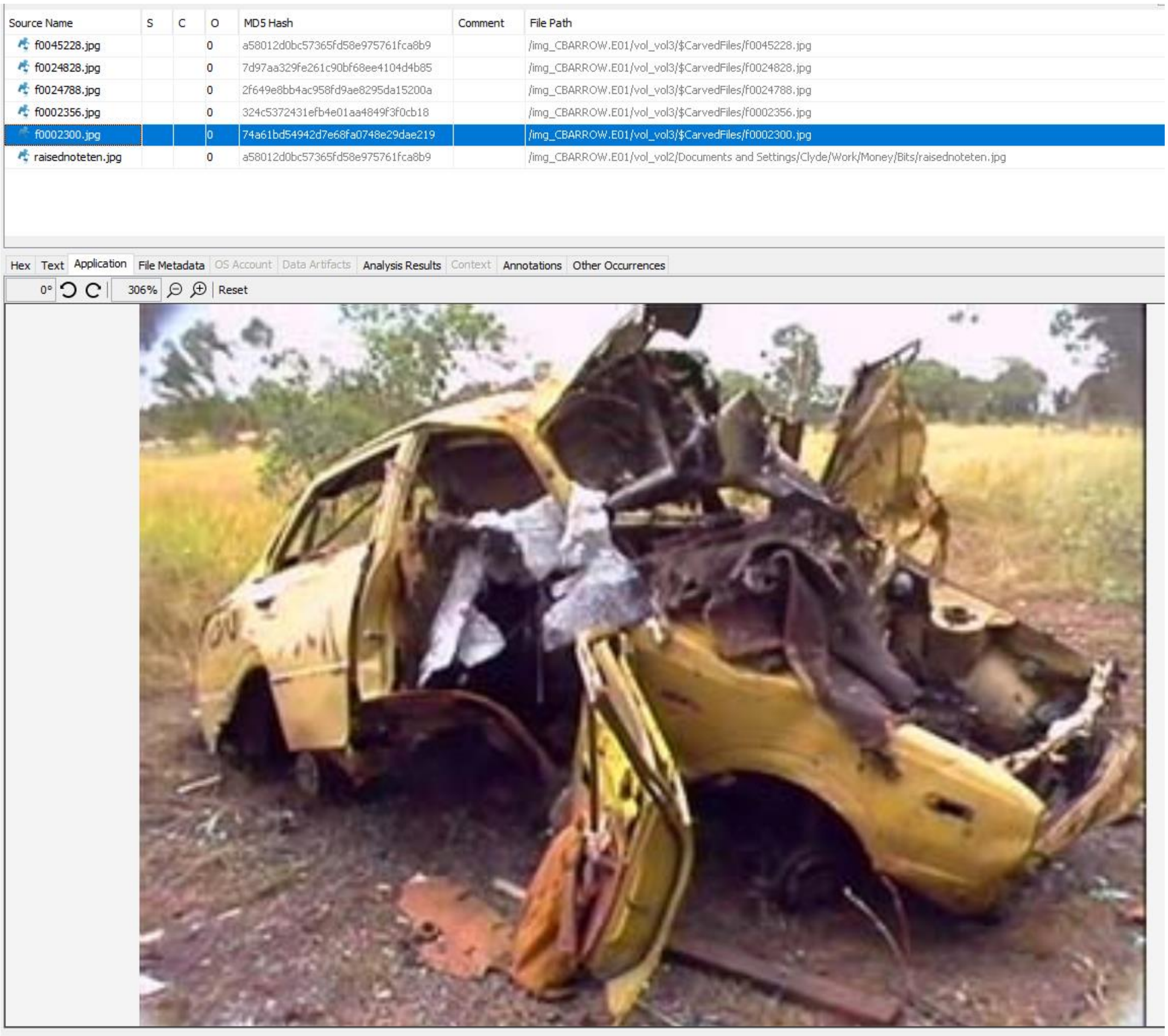
Source Name	S	C	O	MD5 Hash	Comment	File Path
f0045228.jpg			0	a58012d0bc57365fd58e975761fca8b9		/img_CBARROW.E01/vol_vol3/$CarvedFiles/f0045228.jpg
f0024828.jpg			0	7d97aa329fe261c90bf68ee4104d4b85		/img_CBARROW.E01/vol_vol3/$CarvedFiles/f0024828.jpg
f0024788.jpg			0	2f649e8bb4ac958fd9ae8295da15200a		/img_CBARROW.E01/vol_vol3/$CarvedFiles/f0024788.jpg
f0002356.jpg			0	324c5372431efb4e01aa4849f3f0cb18		/img_CBARROW.E01/vol_vol3/$CarvedFiles/f0002356.jpg
f0002300.jpg			0	74a61bd54942d7e68fa0748e29dae219		/img_CBARROW.E01/vol_vol3/$CarvedFiles/f0002300.jpg
raisednoteten.jpg			0	a58012d0bc57365fd58e975761fca8b9		/img_CBARROW.E01/vol_vol2/Documents and Settings/Clyde/Work/Money/Bits/raisednoteten.jpg



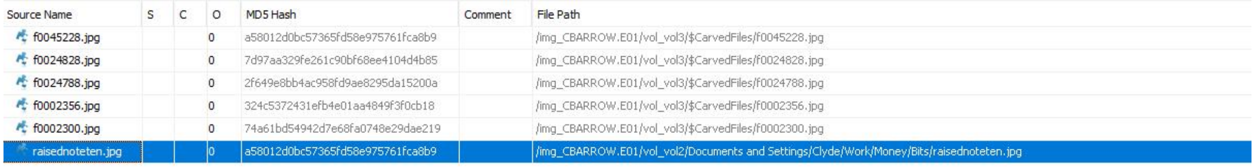
Source Name	S	C	O	MD5 Hash	Comment	File Path
f0045228.jpg			0	a58012d0bc57365fd58e975761fca8b9		/img_CBARROW.E01/vol_vol3/$CarvedFiles/f0045228.jpg
f0024828.jpg			0	7d97aa329fe261c90bf68ee4104d4b85		/img_CBARROW.E01/vol_vol3/$CarvedFiles/f0024828.jpg
f0024788.jpg			0	2f649e8bb4ac958fd9ae8295da15200a		/img_CBARROW.E01/vol_vol3/$CarvedFiles/f0024788.jpg
f0002356.jpg			0	324c5372431efb4e01aa4849f3f0cb18		/img_CBARROW.E01/vol_vol3/$CarvedFiles/f0002356.jpg
f0002300.jpg			0	74a61bd54942d7e68fa0748e29dae219		/img_CBARROW.E01/vol_vol3/$CarvedFiles/f0002300.jpg
raisednoteten.jpg			0	a58012d0bc57365fd58e975761fca8b9		/img_CBARROW.E01/vol_vol2/Documents and Settings/Clyde/Work/Money/Bits/raisednoteten.jpg



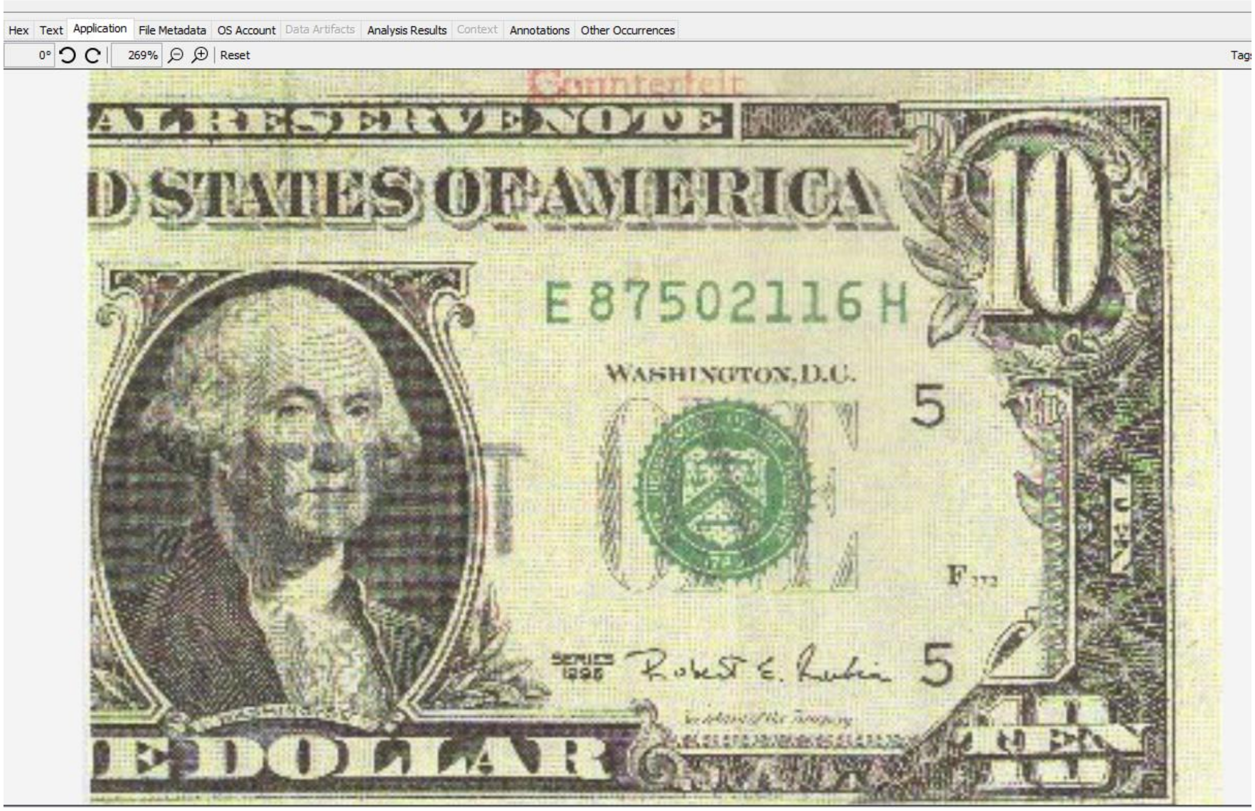
Source Name	S	C	O	MD5 Hash	Comment	File Path
f0045228.jpg			0	a58012d0bc57365fd58e975761fca8b9		/img_CBARROW.E01/vol_vol3/$CarvedFiles/f0045228.jpg
f0024828.jpg			0	7d97aa329fe261c90bf68ee4104d4b85		/img_CBARROW.E01/vol_vol3/$CarvedFiles/f0024828.jpg
f0024788.jpg			0	2f649e8bb4ac958fd9ae8295da15200a		/img_CBARROW.E01/vol_vol3/$CarvedFiles/f0024788.jpg
f0002356.jpg			0	324c5372431efb4e01aa4849f3f0cb18		/img_CBARROW.E01/vol_vol3/$CarvedFiles/f0002356.jpg
f0002300.jpg			0	74a61bd54942d7e68fa0748e29dae219		/img_CBARROW.E01/vol_vol3/$CarvedFiles/f0002300.jpg
raisednoteten.jpg			0	a58012d0bc57365fd58e975761fca8b9		/img_CBARROW.E01/vol_vol2/Documents and Settings/Clyde/Work/Money/Bits/raisednoteten.jpg



Source Name	S	C	O	MD5 Hash	Comment	File Path
f0045228.jpg			0	a58012d0bc57365fd58e975761fca8b9		/img_CBARROW.E01/vol_vol3/$CarvedFiles/f0045228.jpg
f0024828.jpg			0	7d97aa329fe261c90bf68ee4104d4b85		/img_CBARROW.E01/vol_vol3/$CarvedFiles/f0024828.jpg
f0024788.jpg			0	2f649e8bb4ac958fd9ae8295da15200a		/img_CBARROW.E01/vol_vol3/$CarvedFiles/f0024788.jpg
f0002356.jpg			0	324c5372431efb4e01aa4849f3f0cb18		/img_CBARROW.E01/vol_vol3/$CarvedFiles/f0002356.jpg
f0002300.jpg			0	74a61bd54942d7e68fa0748e29dae219		/img_CBARROW.E01/vol_vol3/$CarvedFiles/f0002300.jpg
raisednoteten.jpg			0	a58012d0bc57365fd58e975761fca8b9		/img_CBARROW.E01/vol_vol2/Documents and Settings/Clyde/Work/Money/Bits/raisednoteten.jpg

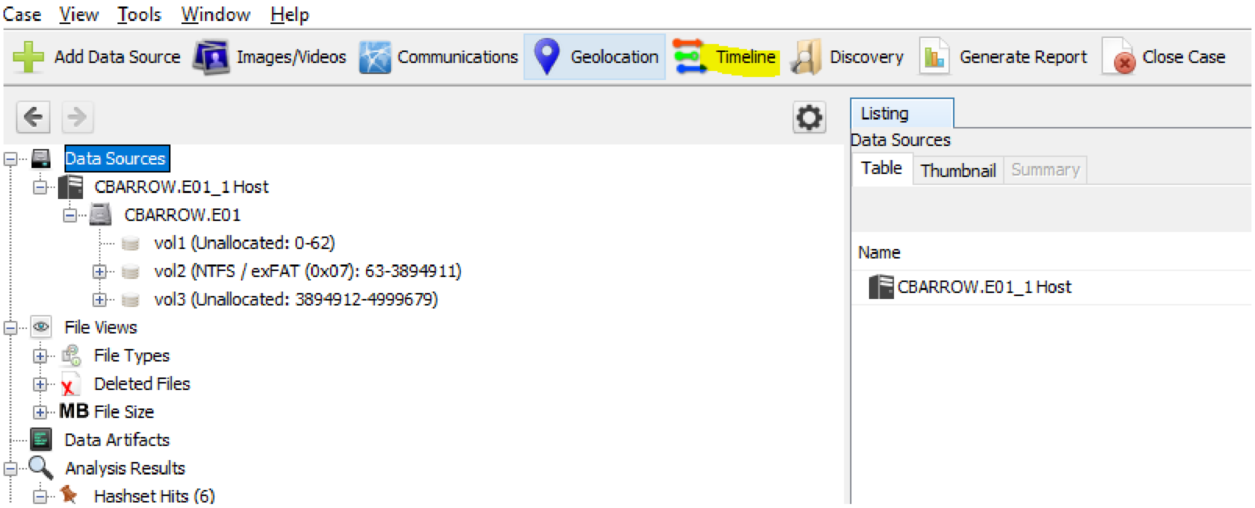


Source Name	S	C	O	MD5 Hash	Comment	File Path
f0045228.jpg			0	a58012d0bc57365fd58e975761fca8b9		/img_CBARROW.E01/vol_vol3/$CarvedFiles/f0045228.jpg
f0024828.jpg			0	7d97aa329fe261c90bf68ee4104d4b85		/img_CBARROW.E01/vol_vol3/$CarvedFiles/f0024828.jpg
f0024788.jpg			0	2f649e8bb4ac958fd9ae8295da15200a		/img_CBARROW.E01/vol_vol3/$CarvedFiles/f0024788.jpg
f0002356.jpg			0	324c5372431efb4e01aa4849f3f0cb18		/img_CBARROW.E01/vol_vol3/$CarvedFiles/f0002356.jpg
f0002300.jpg			0	74a61bd54942d7e68fa0748e29dae219		/img_CBARROW.E01/vol_vol3/$CarvedFiles/f0002300.jpg
raisednoteten.jpg			0	a58012d0bc57365fd58e975761fca8b9		/img_CBARROW.E01/vol_vol2/Documents and Settings/Clyde/Work/Money/Bits/raisednoteten.jpg

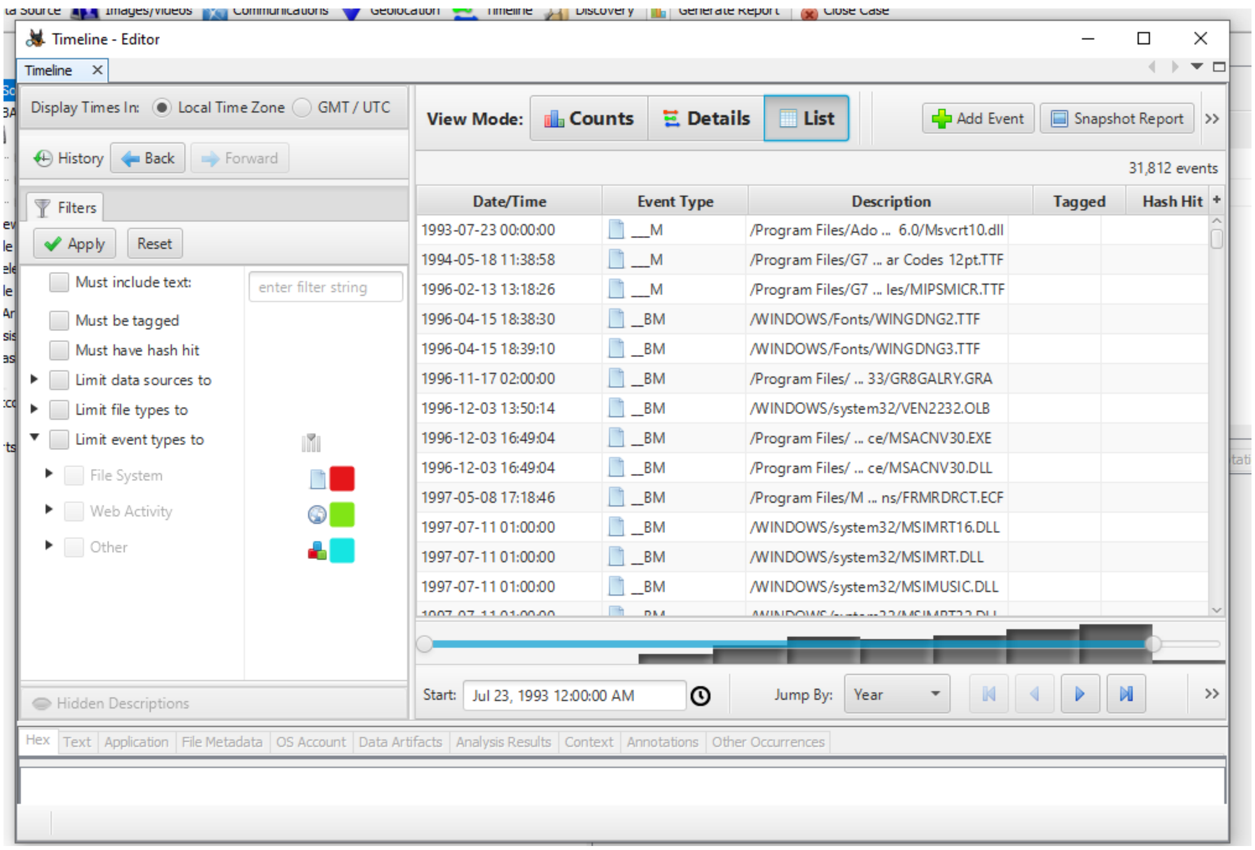


Notice this last file is the same file as the first file; they are exact matches, they just have different meta data (such as filename for example).

10. Click and Open “Timeline” window, select “List” view mode, and review some known files.



- Data Sources
  - CBARROW.E01_1 Host
    - CBARROW.E01
      - vol1 (Unallocated: 0-62)
      - vol2 (NTFS / exFAT (0x07): 63-3894911)
      - vol3 (Unallocated: 3894912-4999679)
- File Views
  - File Types
  - Deleted Files
  - MB File Size
- Data Artifacts
- Analysis Results
  - Hashset Hits (6)



Display Times In: ● Local Time Zone ○ GMT / UTC

□ Must include text:
□ Must be tagged
□ Must have hash hit
□ Limit data sources to
□ Limit file types to
□ Limit event types to
□ File System
□ Web Activity
□ Other

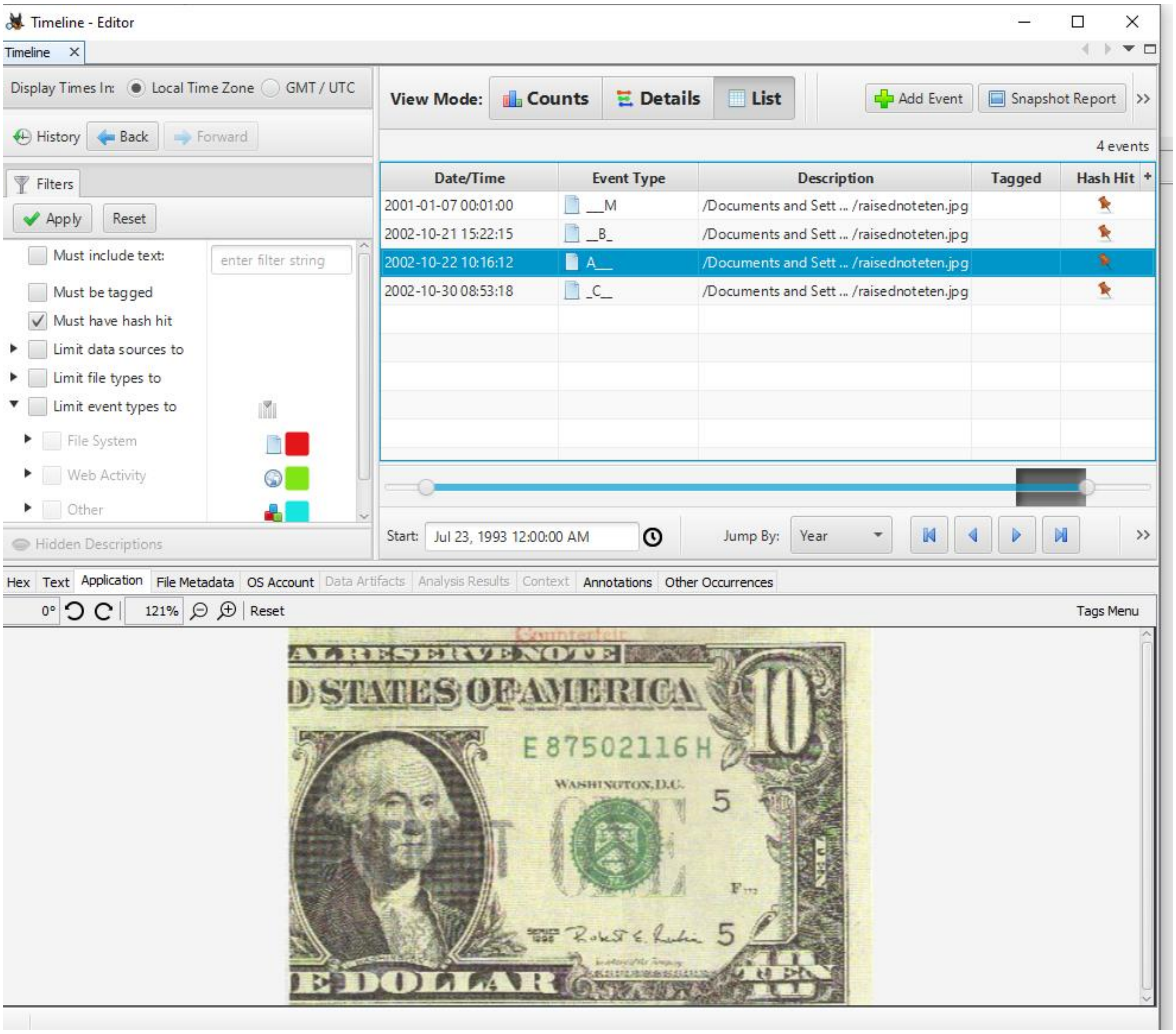
31,812 events

Date/Time	Event Type	Description	Tagged	Hash Hit
1993-07-23 00:00:00	__M	/Program Files/Ado ... 6.0/Msvcrt10.dll		
1994-05-18 11:38:58	__M	/Program Files/G7 ... ar Codes 12pt.TTF		
1996-02-13 13:18:26	__M	/Program Files/G7 ... les/MIPSMICR.TTF		
1996-04-15 18:38:30	_BM	/WINDOWS/Fonts/WINGDNG2.TTF		
1996-04-15 18:39:10	_BM	/WINDOWS/Fonts/WINGDNG3.TTF		
1996-11-17 02:00:00	_BM	/Program Files/ ... 33/GR8GALRY.GRA		
1996-12-03 13:50:14	_BM	/WINDOWS/system32/VEN2232.OLB		
1996-12-03 16:49:04	_BM	/Program Files/ ... ce/MSACNV30.EXE		
1996-12-03 16:49:04	_BM	/Program Files/ ... ce/MSACNV30.DLL		
1997-05-08 17:18:46	_BM	/Program Files/M ... ns/FRMRDRCT.ECF		
1997-07-11 01:00:00	_BM	/WINDOWS/system32/MSIMRT16.DLL		
1997-07-11 01:00:00	_BM	/WINDOWS/system32/MSIMRT.DLL		
1997-07-11 01:00:00	_BM	/WINDOWS/system32/MSIMUSIC.DLL		

Start: Jul 23, 1993 12:00:00 AM

Jump By: Year

So I have noticed if I filter the timeline by *must include hash hit*, it only shows 1 file (and different times the file meta data was updated). It is the raisedenoten.jpg file. The other files that had hash hits as seen in Analysis results did not show up in the timeline.



Timeline - Editor

Display Times In: ● Local Time Zone ○ GMT / UTC

View Mode: Counts | Details | List

4 events

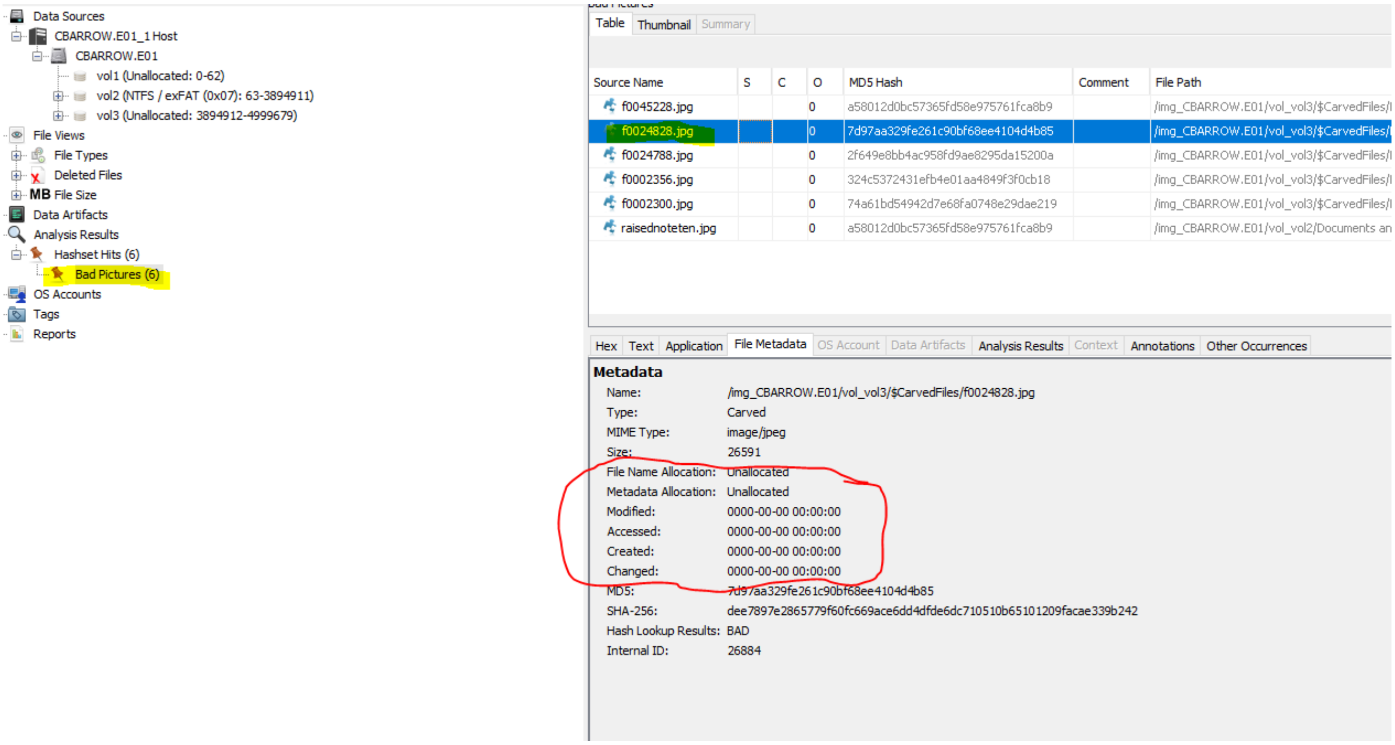
- □ Must include text: enter filter string
- □ Must be tagged
- ☑ Must have hash hit
- □ Limit data sources to
- □ Limit file types to
- □ Limit event types to
  - □ File System
  - □ Web Activity
  - □ Other

Date/Time	Event Type	Description	Tagged	Hash Hit
2001-01-07 00:01:00	__M	/Documents and Sett ... /raisednoteten.jpg		📌
2002-10-21 15:22:15	_B_	/Documents and Sett ... /raisednoteten.jpg		📌
2002-10-22 10:16:12	A__	/Documents and Sett ... /raisednoteten.jpg		📌
2002-10-30 08:53:18	_C_	/Documents and Sett ... /raisednoteten.jpg		📌

Start: Jul 23, 1993 12:00:00 AM

Jump By: Year

So I checked the meta data for the other files I was expecting to show up, since they are indeed hash hits. Turns out, it cannot appear on timeline because the meta data shows that for the other 5 hash hits they do not have any data modified/accessed/created times. The files may have been corrupted or purposely the metadata was deleted/nulled.

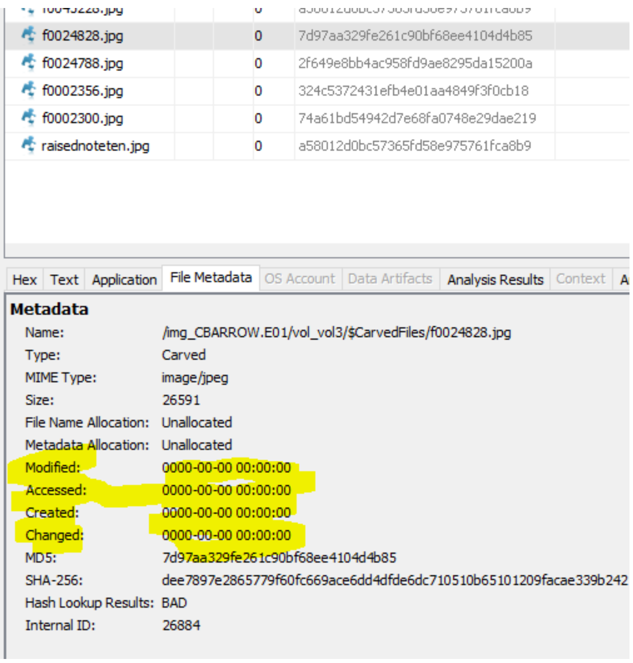


- Data Sources
  - CBARROW.E01_1 Host
    - CBARROW.E01
      - vol1 (Unallocated: 0-62)
      - vol2 (NTFS / exFAT (0x07): 63-3894911)
      - vol3 (Unallocated: 3894912-4999679)
- File Views
  - File Types
  - Deleted Files
  - MB File Size
- Data Artifacts
- Analysis Results
  - Hashset Hits (6)
    - Bad Pictures (6)
- OS Accounts
- Tags
- Reports

Source Name	S	C	O	MD5 Hash	Comment	File Path
f0045228.jpg			0	a58012d0bc57365fd58e975761fca8b9		/img_CBARROW.E01/vol_vol3/$CarvedFiles/
f0024828.jpg			0	7d97aa329fe261c90bf68ee4104d4b85		/img_CBARROW.E01/vol_vol3/$CarvedFiles/
f0024788.jpg			0	2f649e8bb4ac958fd9ae8295da15200a		/img_CBARROW.E01/vol_vol3/$CarvedFiles/
f0002356.jpg			0	324c5372431efb4e01aa4849f3f0cb18		/img_CBARROW.E01/vol_vol3/$CarvedFiles/
f0002300.jpg			0	74a61bd54942d7e68fa0748e29dae219		/img_CBARROW.E01/vol_vol3/$CarvedFiles/
raisednoteten.jpg			0	a58012d0bc57365fd58e975761fca8b9		/img_CBARROW.E01/vol_vol2/Documents an

Metadata

Name:	/img_CBARROW.E01/vol_vol3/$CarvedFiles/f0024828.jpg
Type:	Carved
MIME Type:	image/jpeg
Size:	26591
File Name Allocation:	Unallocated
Metadata Allocation:	Unallocated
Modified:	0000-00-00 00:00:00
Accessed:	0000-00-00 00:00:00
Created:	0000-00-00 00:00:00
Changed:	0000-00-00 00:00:00
MD5:	7d97aa329fe261c90bf68ee4104d4b85
SHA-256:	dee7897e2865779f60fc669ace6dd4dfde6dc710510b65101209facae339b242
Hash Lookup Results:	BAD
Internal ID:	26884



f0024828.jpg	0	7d97aa329fe261c90bf68ee4104d4b85
f0024788.jpg	0	2f649e8bb4ac958fd9ae8295da15200a
f0002356.jpg	0	324c5372431efb4e01aa4849f3f0cb18
f0002300.jpg	0	74a61bd54942d7e68fa0748e29dae219
raisednoteten.jpg	0	a58012d0bc57365fd58e975761fca8b9

Metadata

Name:	/img_CBARROW.E01/vol_vol3/$CarvedFiles/f0024828.jpg
Type:	Carved
MIME Type:	image/jpeg
Size:	26591
File Name Allocation:	Unallocated
Metadata Allocation:	Unallocated
Modified:	0000-00-00 00:00:00
Accessed:	0000-00-00 00:00:00
Created:	0000-00-00 00:00:00
Changed:	0000-00-00 00:00:00
MD5:	7d97aa329fe261c90bf68ee4104d4b85
SHA-256:	dee7897e2865779f60fc669ace6dd4dfde6dc710510b65101209facae339b242
Hash Lookup Results:	BAD
Internal ID:	26884

Summary/Reflection

Overall, I have gained a very valuable skill using the Autopsy digital forensic tool. Now, if I have a machine that has poor performance and I suspect that there may be a virus on the machine, I can capture an image of my entire disk drive and hash all files. Then, I can use the NSRL hash database set to compare to all of my files. The analysis done by the tool will automatically give me hash hits so that I can know if and which kind of known bad file is on my machine! Then I can proceed to the path of that hash hit on my actual machine that I made the disk image copy of and delete/remove the file/program! In essence, this lab helped me to be able to conduct digital forensic audits using the Autopsy tool more effectively and added to my knowledge of the use of the tool, and it has enabled me to do an autopsy of any of my everyday personal devices or for the devices of someone else to scan for viruses in a very effective, safe way (especially because the image file is read only as per the digital forensic software design).