

results from keyword searches

The screenshot shows the Malware1 - Autopsy 4.4.1 interface. The left sidebar displays a tree view of data sources, including 'Extracted Content', 'Keyword Hits', and 'Tags'. The main pane shows the results of a keyword search. The search results are displayed in a table with columns: Name, Location, Modified Time, Change Time, Access Time, Created Time, and Size. Two results are shown, both for the file 'Reply to August 20 2005 order.bt' located at '/img_MaryvilleP_1.E01/vol2/Documents and...'. The search results are filtered by 'Keyword search 1 - 1ZA307F3024565...' and 'Keyword search 2 - hide_folder'.

Name	Location	Modified Time	Change Time	Access Time	Created Time	Size
Reply to August 20 2005 order.bt	/img_MaryvilleP_1.E01/vol2/Documents and...	2005-08-20 11:08:02 CDT	2005-08-20 11:08:02 CDT	2015-05-01 09:01:24 CDT	2015-05-01 09:01:24 CDT	495
Reply to August 20 2005 order.bt	/img_MaryvilleP_1.E01/vol2/Documents and...	2005-08-20 11:08:02 CDT	2005-08-20 11:08:02 CDT	2015-05-01 09:03:56 CDT	2015-05-01 09:03:56 CDT	495

1ZA307F30245655391 is the tracking number for the august order.

The screenshot shows the Malware1 - Autopsy 4.4.1 interface. The left sidebar displays a tree view of data sources, including 'Extracted Content', 'Keyword Hits', and 'Tags'. The main pane shows the results of a keyword search. The search results are displayed in a table with columns: Name, Location, Modified Time, Change Time, Access Time, Created Time, and Size. Two results are shown, both for the file 'Reply to August 20 2005 order.bt' located at '/img_MaryvilleP_1.E01/vol2/Documents and...'. The search results are filtered by 'Keyword search 1 - 1ZA307F3024565...' and 'Keyword search 2 - hide_folder'.

Name	Location	Modified Time	Change Time	Access Time	Created Time	Size
Reply to August 20 2005 order.bt	/img_MaryvilleP_1.E01/vol2/Documents and...	2005-08-20 11:08:02 CDT	2005-08-20 11:08:02 CDT	2015-05-01 09:01:24 CDT	2015-05-01 09:01:24 CDT	495
Reply to August 20 2005 order.bt	/img_MaryvilleP_1.E01/vol2/Documents and...	2005-08-20 11:08:02 CDT	2005-08-20 11:08:02 CDT	2015-05-01 09:03:56 CDT	2015-05-01 09:03:56 CDT	495

The 'Indexed Text' tab is selected, showing the following text:

```
>>Please sent me 80 Per**a to my regular address
>>The money is being sent to you via WU.
>>The WU is 800-789-1234 and the amount of $999.00
>>Secret question: What color is the sky?
>>Answer: Green
>>When you receive funds, please mail my order ASAP along with tracking number.
>>Ab
August 20, 2005 reply:
Your funds were received and your order is on its way via brown shorts.
Tracking number is: 1ZA307F30245655391
If problems, let me know . . .
Tessy
```

No hits for hide_folder within unallocated space.

Malware - Autopsy 4.4.1
Case View Tools Window Help

Listing Keyword search 1 - 12A307F3024565... Keyword search 2 - hide_folder

Keyword search

Name	Location	Modified Time	Change Time	Access Time	Created Time
hide_folder_ext_setup.exe	/img_MaryvilleXP_1 E01/vol_vol2/Documents and Settings/Administrator/My Documents/hide_folder_ext_setup.exe	2014-12-24 17:37:52 CST	2015-05-01 08:59:41 CDT	2015-05-01 08:59:41 CDT	2015-05-01 08:59:41 CDT
hide_folder_ext_setup.exe	/img_MaryvilleXP_1 E01/vol_vol2/Documents and Settings/Administrator/My Documents/hide_folder_ext_setup.exe	2014-12-24 17:37:52 CST	2015-05-01 08:59:41 CDT	2015-05-01 08:59:41 CDT	2015-05-01 08:59:41 CDT
hide_folder_ext_setup.exe	/img_MaryvilleXP_1 E01/vol_vol2/Documents and Settings/Administrator/My Documents/hide_folder_ext_setup.exe	2014-12-24 17:37:52 CST	2015-05-01 08:59:41 CDT	2015-05-01 08:59:41 CDT	2015-05-01 08:59:41 CDT
hide_folder_ext_setup.exe	/img_MaryvilleXP_1 E01/vol_vol2/Documents and Settings/Administrator/My Documents/hide_folder_ext_setup.exe	2014-12-24 17:37:52 CST	2015-05-01 08:59:41 CDT	2015-05-01 08:59:41 CDT	2015-05-01 08:59:41 CDT
NTUSER.DAT	/img_MaryvilleXP_1 E01/vol_vol2/Documents and Settings/Administrator/My Documents/hide_folder_ext_setup.exe	2015-05-01 09:29:02 CDT	2015-05-01 09:29:02 CDT	2015-05-01 12:59:53 CDT	2015-05-01 12:59:53 CDT
REGISTRY_MACHINE_SYSTEM	/img_MaryvilleXP_1 E01/vol_vol2/System Volume...	2015-05-01 12:59:53 CDT	2015-05-01 12:59:53 CDT	2015-05-01 12:59:53 CDT	2015-05-01 12:59:53 CDT
ntuser.dat.LOG	/img_MaryvilleXP_1 E01/vol_vol2/Documents and Settings/Administrator/My Documents/hide_folder_ext_setup.exe	2015-05-01 14:34:50 CDT	2015-05-01 14:34:50 CDT	2015-05-01 14:34:50 CDT	2015-05-01 14:34:50 CDT
REGISTRY_USER_NTUSER_S-1-5-21-144832229-195	/img_MaryvilleXP_1 E01/vol_vol2/System Volume...	2015-05-01 12:59:53 CDT	2015-05-01 12:59:53 CDT	2015-05-01 12:59:53 CDT	2015-05-01 12:59:53 CDT

Hex Strings File Metadata Results Indexed Text Media

Name	Value
Name	/img_MaryvilleXP_1 E01/vol_vol2/Documents and Settings/Administrator/My Documents/hide_folder_ext_setup.exe
Type	File System
MIME Type	application/x-dosexec
Size	3084824
File Name Allocation	Allocated
Metadata Allocation	Allocated
Modified	2014-12-24 17:37:52 CST
Accessed	2015-05-01 08:59:41 CDT

Listing Keyword search 1 - 12A307F3024565... Keyword search 2 - hide_folder

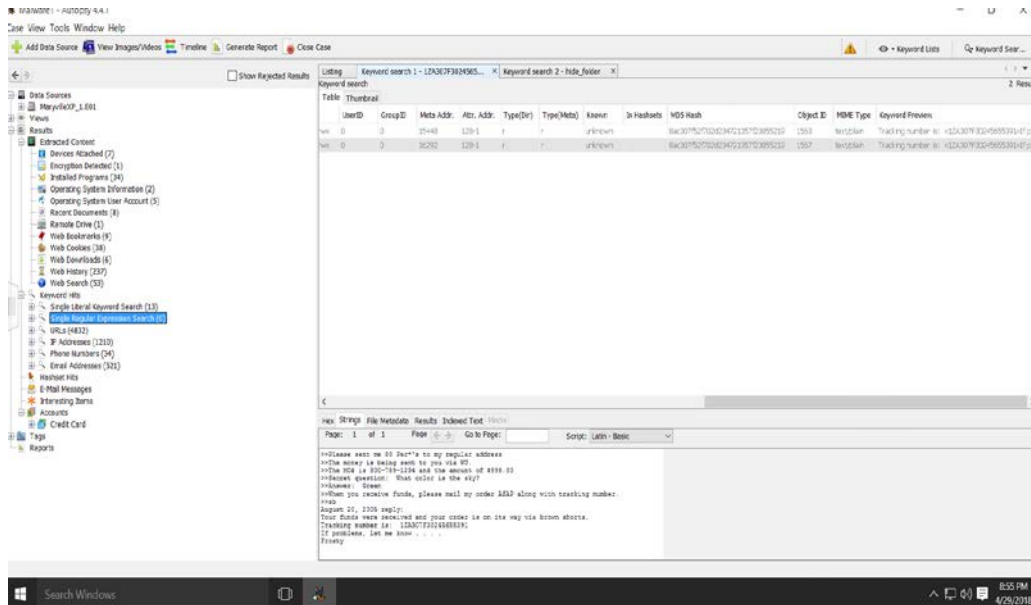
Keyword search

Name	Location	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Mode	UserID	GroupID
1.E01/vol_vol2/Documents and...	/img_MaryvilleXP_1 E01/vol_vol2/Documents and Settings/Administrator/My Documents/hide_folder_ext_setup.exe	2014-12-24 17:37:52 CST	2015-05-01 08:59:41 CDT	2015-05-01 08:59:41 CDT	2015-05-01 08:59:41 CDT	3084824	Allocated	Allocated	rw-rw-rw-	0	0
1.E01/vol_vol2/Documents and...	/img_MaryvilleXP_1 E01/vol_vol2/Documents and Settings/Administrator/My Documents/hide_folder_ext_setup.exe	2014-12-24 17:37:52 CST	2015-05-01 08:59:41 CDT	2015-05-01 08:59:41 CDT	2015-05-01 08:59:41 CDT	3560	Allocated	Allocated	rw-rw-rw-	0	0
1.E01/vol_vol2/Documents and...	/img_MaryvilleXP_1 E01/vol_vol2/Documents and Settings/Administrator/My Documents/hide_folder_ext_setup.exe	2014-12-24 17:37:52 CST	2015-05-01 08:59:41 CDT	2015-05-01 08:59:41 CDT	2015-05-01 08:59:41 CDT	3084824	Allocated	Allocated	rw-rw-rw-	0	0
1.E01/vol_vol2/Documents and...	/img_MaryvilleXP_1 E01/vol_vol2/Documents and Settings/Administrator/My Documents/hide_folder_ext_setup.exe	2014-12-24 17:37:52 CST	2015-05-01 08:59:41 CDT	2015-05-01 08:59:41 CDT	2015-05-01 08:59:41 CDT	3560	Allocated	Allocated	rw-rw-rw-	0	0
1.E01/vol_vol2/Documents and...	/img_MaryvilleXP_1 E01/vol_vol2/Documents and Settings/Administrator/My Documents/hide_folder_ext_setup.exe	2015-05-01 09:29:02 CDT	2015-05-01 09:29:02 CDT	2015-05-01 12:59:53 CDT	2015-05-01 12:59:53 CDT	1210720	Allocated	Allocated	rw-rw-rw-	0	0
1.E01/vol_vol2/System Volume...	/img_MaryvilleXP_1 E01/vol_vol2/System Volume...	2015-05-01 12:59:53 CDT	2015-05-01 12:59:53 CDT	2015-05-01 12:59:53 CDT	2015-05-01 12:59:53 CDT	3825664	Allocated	Allocated	rw-rw-rw-	0	0
1.E01/vol_vol2/Documents and...	/img_MaryvilleXP_1 E01/vol_vol2/Documents and Settings/Administrator/My Documents/hide_folder_ext_setup.exe	2015-05-01 14:34:50 CDT	2015-05-01 14:34:50 CDT	2015-05-01 14:34:50 CDT	2015-05-01 14:34:50 CDT	409576	Allocated	Allocated	rw-rw-rw-	0	0
1.E01/vol_vol2/System Volume...	/img_MaryvilleXP_1 E01/vol_vol2/System Volume...	2015-05-01 12:59:53 CDT	2015-05-01 12:59:53 CDT	2015-05-01 12:59:53 CDT	2015-05-01 12:59:53 CDT	1204704	Allocated	Allocated	rw-rw-rw-	0	0

Hex Strings File Metadata Results Indexed Text Media

Name	Value
Name	/img_MaryvilleXP_1 E01/vol_vol2/Documents and Settings/Administrator/My Documents/hide_folder_ext_setup.exe
Type	File System
MIME Type	application/x-dosexec
Size	3084824
File Name Allocation	Allocated
Metadata Allocation	Allocated
Modified	2014-12-24 17:37:52 CST
Accessed	2015-05-01 08:59:41 CDT

Compare the hashes of both text files.



Sort by specific fields within Autopsy to answer the following questions.

1. Conduct a keyword search of the entire drive for the following keywords.

a. 1ZA307F30245655391

b. hide_folder

2. How many .txt files did the keyword search hit on?

- a. 2 text files
- b. No text files

3. What are the names of the text files?

Reply to August 20 2005 order.txt

4. Use the review tab to review the hits within the text files. What is the number “1ZA307F30245655391”?

It is a tracking number for a an order.

5. Are there any hits for “hide_folder” within unallocated space? What do you think this represents? Do you know for sure?

No, there isn't any hits for hide_folder within unallocated space.

6. Analyze the text files titled “Reply to August 20 2005 order.txt” located in the “My Hidden Folder” directory and the Recycle Bin. Are these two files identical? (Hint: Hash both files and sort by hash value with the “C” drive homeplated).

Yes, both files are identical.