Module B3: Recover Deleted File and Lost Password

Pre-requisite Knowledge and Skills:

1. Understand basic of forensics investigation process

Learning Objectives

1. Be familiar with the process of setup a digital forensics case.
2. Be proficient with the basis of deleted file recovery.
3. Be familiar with the process of recover password from file slacks.

Recommended Running Environment/Tools:

1. Windows OS
2. FTK 1.86.1

Material:

1. image 1
2. image 2

Video Lecture:

1. Forensics Case and deleted file recovery

Lab Assessment:

1. Forensics Case and deleted file recovery Quiz

Acknowledgement:

The image 1 and image 2 are downloaded from DFRWS 2003 Challenge, https://www.dfrws.org/search

Lab Instructions:

Scenario Description

Your homework file (a precious picture of your high school graduation with your best friend) was stored on your thumb drive but your little brother played with it on computer and deleted the picture by accident.

And then, he was so panic and tried to save the picture, but accidently formatted the thumb drive. You were so angry and your little brother was crying.

- What you can do? Can you get your picture back?
- If you can get the picture back, what would be your approach?

<u>Tasks</u>

The thumb drive is now imaged and you have the image files, image1 and image2.

- Setup a case by using FTK 1.8.6 and image1 and image2

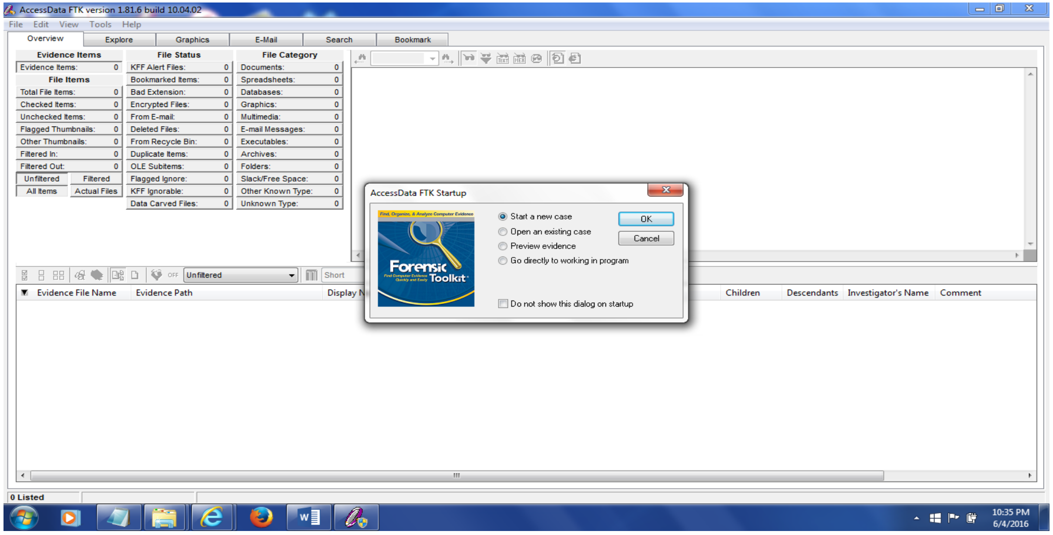
- Narrow down the search focus by using index search, live search, and bookmark
- Find out at least 1 password in the disk image
- Recover the following file
    - Cover page.jpg

Assessment – Students tasks

- Recover a jpeg based map.
- Recover a bmp based map.

Instructions

1. Run FTK 1.8.6 on your desktop by double click on the icon



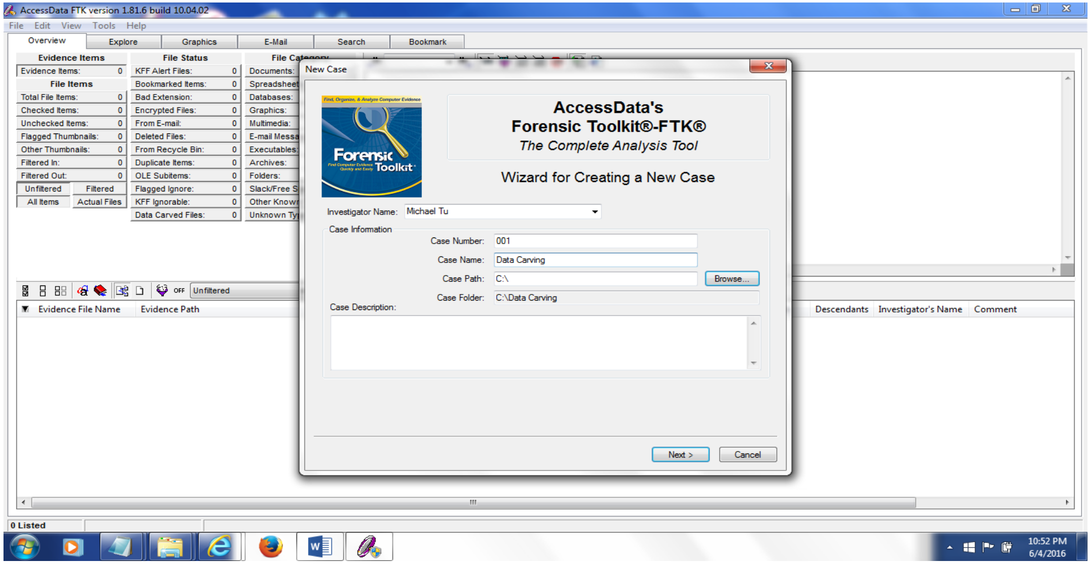
AccessData FTK Startup

- ● Start a new case
- ○ Open an existing case
- ○ Preview evidence
- ○ Go directly to working in program

□ Do not show this dialog on startup

OK | Cancel

2. Build a case of Data carving by using the default case setting (run in demo version)



AccessData FTK version 1.81.6 build 10.04.02
File Edit View Tools Help
Overview Explore Graphics E-Mail Search Bookmark
10:52 PM
6/4/2016

New Case

AccessData's
Forensic Toolkit®-FTK®
The Complete Analysis Tool

Wizard for Creating a New Case

Investigator Name: Michael Tu

Case Information

Case Number: 001

Case Name: Data Carving

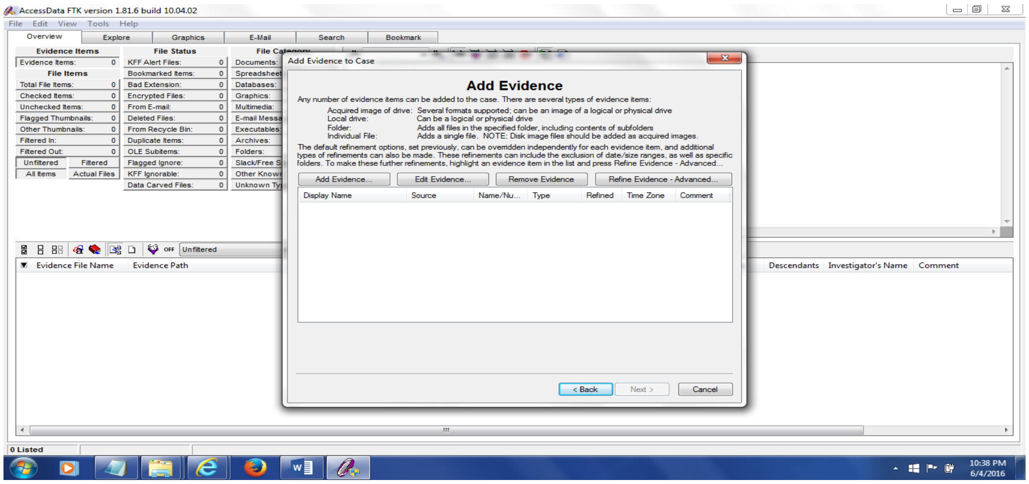
Case Path: C:\

Case Folder: C:\Data Carving

Case Description:

Browse... | Next > | Cancel

3. Using default settings of FTK by clicking the next button till this "Add Evidence"


AccessData FTK version 1.81.6 build 10.04.02
File Edit View Tools Help
Overview Explore Graphics E-Mail Search Bookmark
Add Evidence to Case

Add Evidence

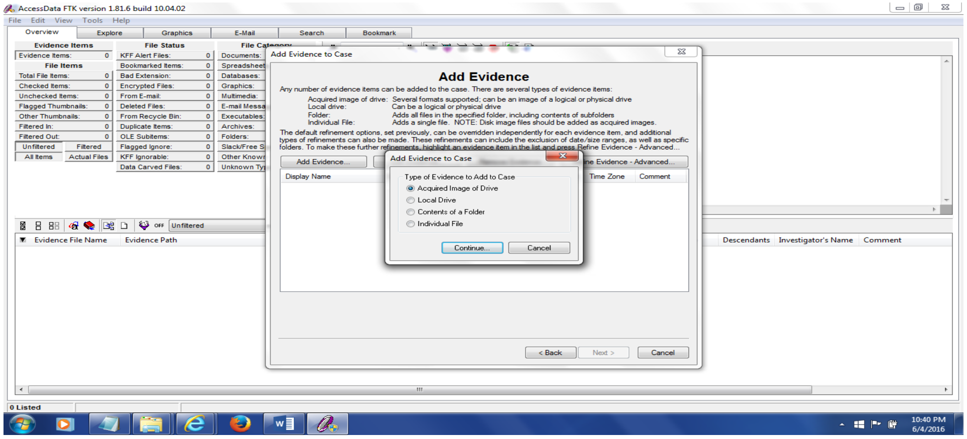
Any number of evidence items can be added to the case. There are several types of evidence items:

Acquired image of drive:	Several formats supported; can be an image of a logical or physical drive
Local drive:	Can be a logical or physical drive
Folder:	Adds all files in the specified folder, including contents of subfolders
Individual File:	Adds a single file. NOTE: Disk image files should be added as acquired images.

The default refinement options, set previously, can be overridden independently for each evidence item, and additional types of refinements can also be made. These refinements can include the exclusion of date/size ranges, as well as specific folders. To make these further refinements, highlight an evidence item in the list and press Refine Evidence - Advanced...

Add Evidence... Edit Evidence... Remove Evidence Refine Evidence - Advanced...
Display Name Source Name/Nu... Type Refined Time Zone Comment
< Back Next > Cancel
10:38 PM
6/4/2016

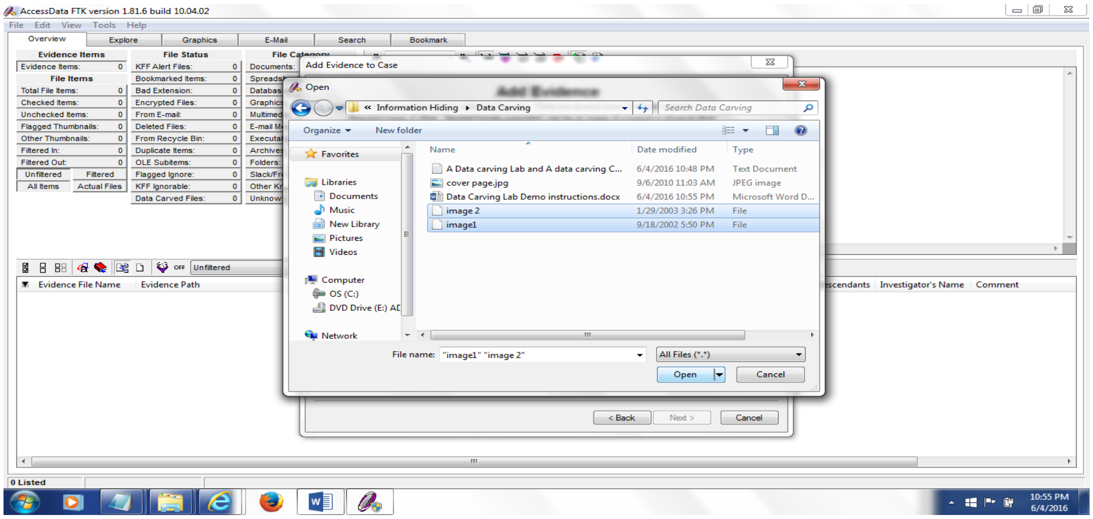
4. Click on "Add Evidence" button to add choose the **acquired image of a drive**



Type of Evidence to Add to Case

● Acquired Image of Drive
○ Local Drive
○ Contents of a Folder
○ Individual File

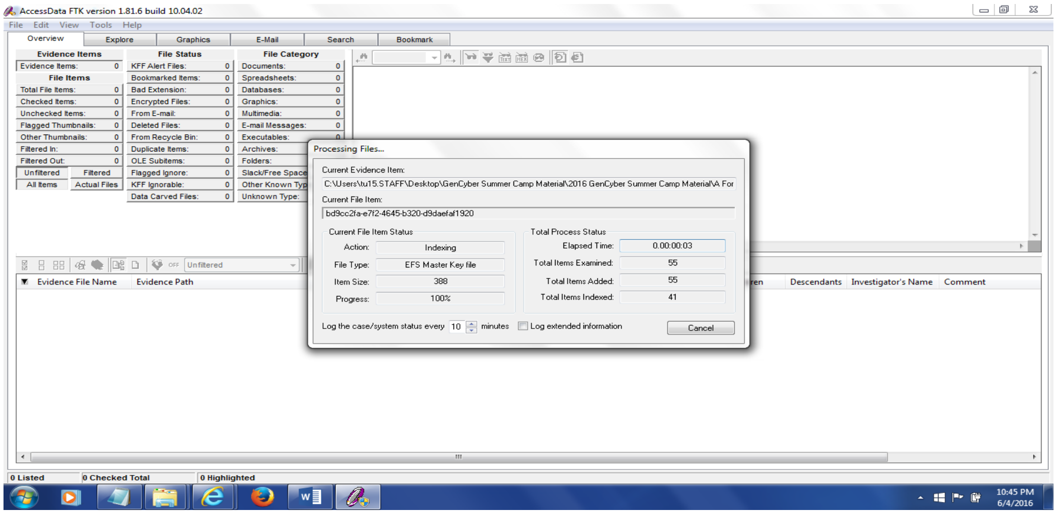
5. Click on continue and next to navigate to the image1 and image2 file on your data carv folder, then add the two files


Open
« Information Hiding ▸ Data Carving
Search Data Carving
Organize New folder
Favorites Libraries Documents Music New Library Pictures Videos Computer OS (C:) DVD Drive (E:) AD Network
Open Cancel
10:55 PM
6/4/2016

Name	Date modified	Type
A Data carving Lab and A data carving C...	6/4/2016 10:48 PM	Text Document
cover page.jpg	9/6/2010 11:03 AM	JPEG image
Data Carving Lab Demo instructions.docx	6/4/2016 10:55 PM	Microsoft Word D...
image 2	1/29/2003 3:26 PM	File
image1	9/18/2002 5:50 PM	File

File name: "image1" "image 2"   All Files (*.*)

6. Click on open and then click on OK, and then next and finish, till finished.



AccessData FTK version 1.81.6 build 10.04.02

Evidence Items		File Status		File Category	
Evidence Items:	0	KFF Alert Files:	0	Documents:	0
File Items		Bookmarked Items:	0	Spreadsheets:	0
Total File Items:	0	Bad Extension:	0	Databases:	0
Checked Items:	0	Encrypted Files:	0	Graphics:	0
Unchecked Items:	0	From E-mail:	0	Multimedia:	0
Flagged Thumbnails:	0	Deleted Files:	0	E-mail Messages:	0
Other Thumbnails:	0	From Recycle Bin:	0	Executables:	0
Filtered In:	0	Duplicate Items:	0	Archives:	
Filtered Out:	0	OLE Subitems:	0	Folders:	
		Flagged Ignore:	0	Slack/Free Space	
		KFF Ignorable:	0	Other Known Typ	
		Data Carved Files:	0	Unknown Type:	

Processing Files...

Current Evidence Item:
C:\Users\tu15.STAFF\Desktop\GenCyber Summer Camp Material\2016 GenCyber Summer Camp Material\A For

Current File Item:
bd9cc2fa-e7f2-4645-b320-d9daefaf1920

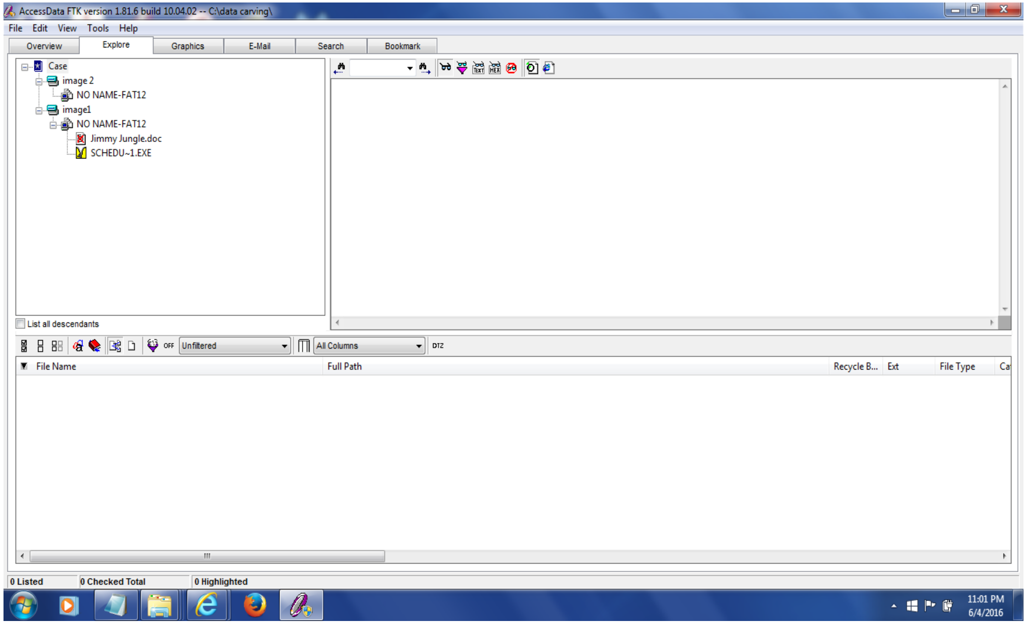
Current File Item Status
Action: Indexing
File Type: EFS Master Key file
Item Size: 388
Progress: 100%

Total Process Status
Elapsed Time: 0.00:00:03
Total Items Examined: 55
Total Items Added: 55
Total Items Indexed: 41

Log the case/system status every 10 minutes □ Log extended information

0 Listed | 0 Checked Total | 0 Highlighted

7. Click on the explore tab, nothing found for the cover.jpg file!!!



AccessData FTK version 1.81.6 build 10.04.02 -- C:\data carving\

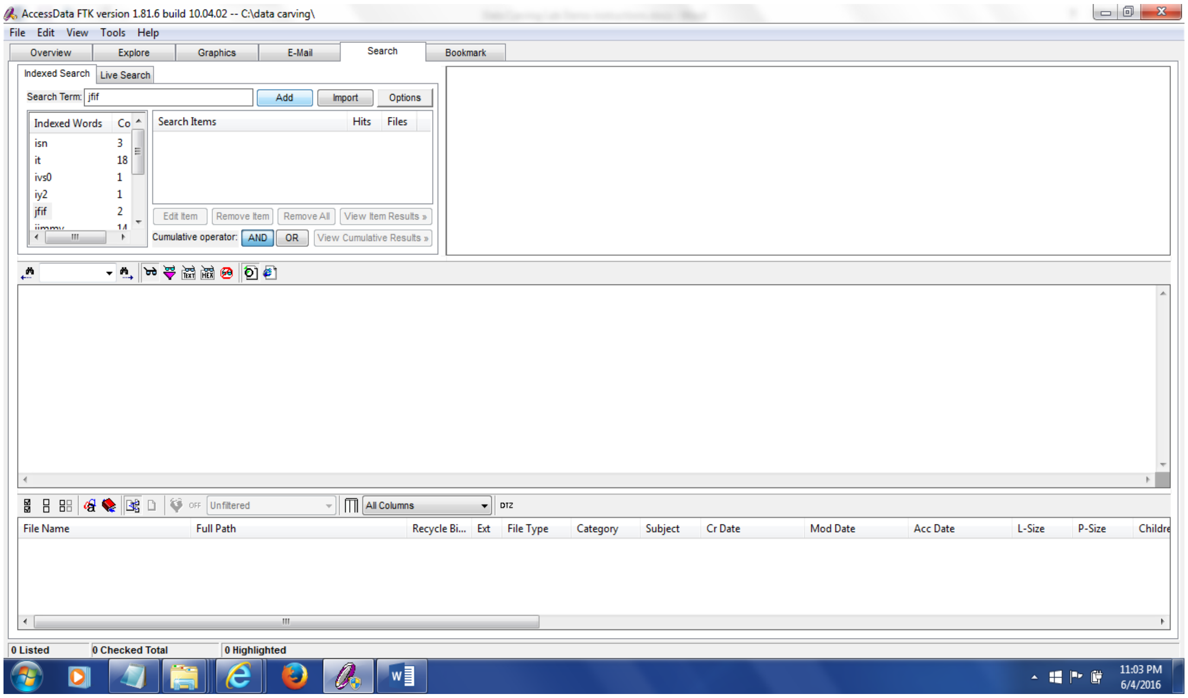
- Case
  - image 2
    - NO NAME-FAT12
  - image1
    - NO NAME-FAT12
      - Jimmy Jungle.doc
      - SCHEDU~1.EXE

□ List all descendants

Unfiltered | All Columns

0 Listed | 0 Checked Total | 0 Highlighted

8. The file signature of the .jpg file is JFIF, so let’s search it by clicking on search tab



AccessData FTK version 1.81.6 build 10.04.02 -- C:\data carving\

Search Term: jfif

Indexed Words	Co
isn	3
it	18
ivs0	1
iy2	1
jfif	2
jimmy	14

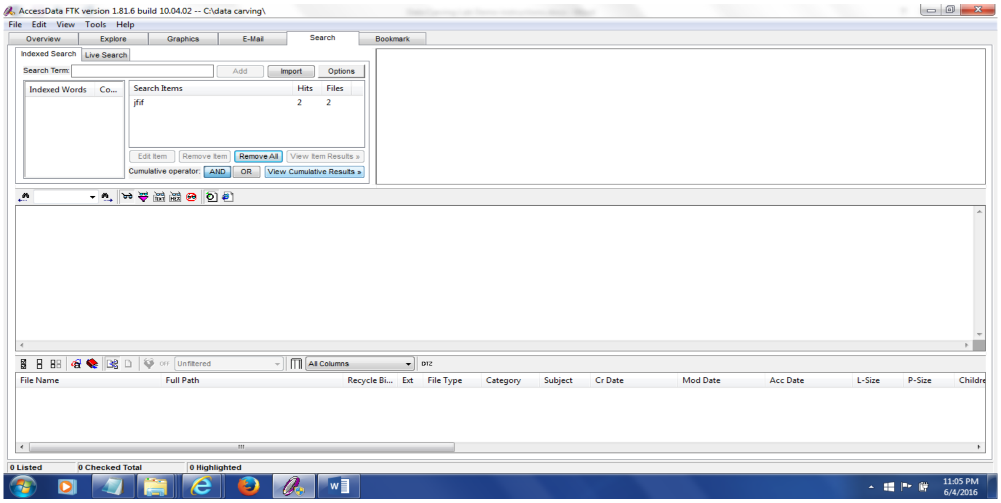
Search Items	Hits	Files

File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject	Cr Date	Mod Date	Acc Date	L-Size	P-Size	Childre

0 Listed | 0 Checked Total | 0 Highlighted

11:03 PM
6/4/2016

9. Add the search terms and click on “**view cumulative results**”



AccessData FTK version 1.81.6 build 10.04.02 -- C:\data carving\

Search Term:

Indexed Words	Co...

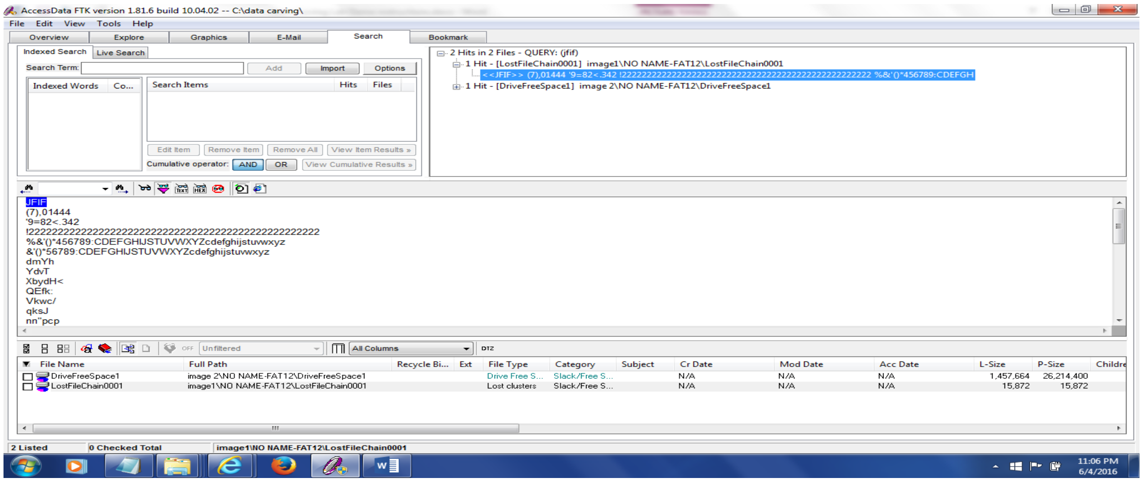
Search Items	Hits	Files
jfif	2	2

File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject	Cr Date	Mod Date	Acc Date	L-Size	P-Size	Childre

0 Listed | 0 Checked Total | 0 Highlighted

11:05 PM
6/4/2016

10. With 2 hits, expanded the first one



AccessData FTK version 1.81.6 build 10.04.02 -- C:\data carving\

```
2 Hits in 2 Files - QUERY: (jfif)
  1 Hit - [LostFileChain0001]  image1\NO NAME-FAT12\LostFileChain0001
    <<JFIF>> (7),01444 '9=82<.342 !22222222222222222222222222222222222222222222222222 %&'()*456789:CDEFGH
  1 Hit - [DriveFreeSpace1]  image 2\NO NAME-FAT12\DriveFreeSpace1
```

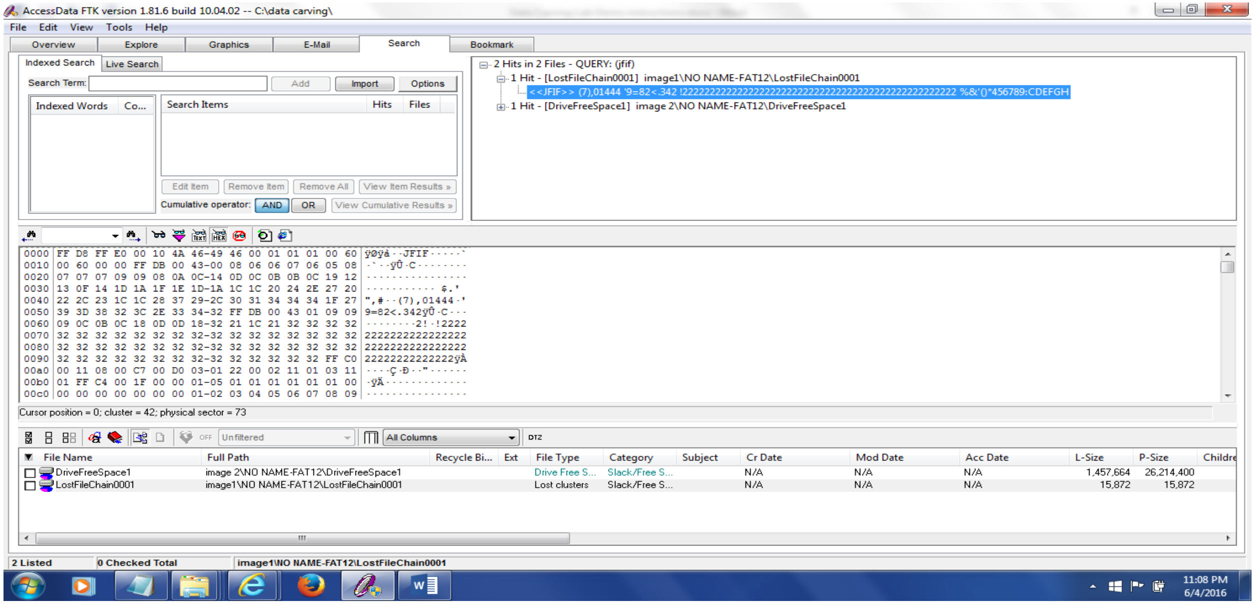
```
JFIF
(7),01444
'9=82<.342
!22222222222222222222222222222222222222222222222222
%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
dmYh
YdvT
XbydH<
QEfk:
Vkwc/
qksJ
nn"pcp
```

	File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject	Cr Date	Mod Date	Acc Date	L-Size	P-Size	Childre
□	DriveFreeSpace1	image 2\NO NAME-FAT12\DriveFreeSpace1			Drive Free S...	Slack/Free S...		N/A	N/A	N/A	1,457,664	26,214,400	
□	LostFileChain0001	image1\NO NAME-FAT12\LostFileChain0001			Lost clusters	Slack/Free S...		N/A	N/A	N/A	15,872	15,872	

2 Listed | 0 Checked Total | image1\NO NAME-FAT12\LostFileChain0001

11:06 PM
6/4/2016

11. Change the hex view in the middle pane and then



AccessData FTK version 1.81.6 build 10.04.02 -- C:\data carving\

```
2 Hits in 2 Files - QUERY: (jfif)
  1 Hit - [LostFileChain0001]  image1\NO NAME-FAT12\LostFileChain0001
    <<JFIF>> (7),01444 '9=82<.342 !22222222222222222222222222222222222222222222222222 %&'()*456789:CDEFGH
  1 Hit - [DriveFreeSpace1]  image 2\NO NAME-FAT12\DriveFreeSpace1
```

```
0000  FF D8 FF E0 00 10 4A 46-49 46 00 01 01 01 00 60  ÿØÿà··JFIF·····`
0010  00 60 00 00 FF DB 00 43-00 08 06 06 07 06 05 08  ·`··ÿÛ·C········
0020  07 07 07 09 09 08 0A 0C-14 0D 0C 0B 0B 0C 19 12  ················
0030  13 0F 14 1D 1A 1F 1E 1D-1A 1C 1C 20 24 2E 27 20  ············ $.'
0040  22 2C 23 1C 1C 28 37 29-2C 30 31 34 34 34 1F 27  ",#··(7),01444·'
0050  39 3D 38 32 3C 2E 33 34-32 FF DB 00 43 01 09 09  9=82<.342ÿÛ·C···
0060  09 0C 0B 0C 18 0D 0D 18-32 21 1C 21 32 32 32 32  ········2!·!2222
0070  32 32 32 32 32 32 32 32-32 32 32 32 32 32 32 32  2222222222222222
0080  32 32 32 32 32 32 32 32-32 32 32 32 32 32 32 32  2222222222222222
0090  32 32 32 32 32 32 32 32-32 32 32 32 32 32 FF C0  22222222222222ÿÀ
00a0  00 11 08 00 C7 00 D0 03-01 22 00 02 11 01 03 11  ····Ç·Ð··"······
00b0  01 FF C4 00 1F 00 00 01-05 01 01 01 01 01 01 00  ·ÿÄ·············
00c0  00 00 00 00 00 00 00 01-02 03 04 05 06 07 08 09  ················
```

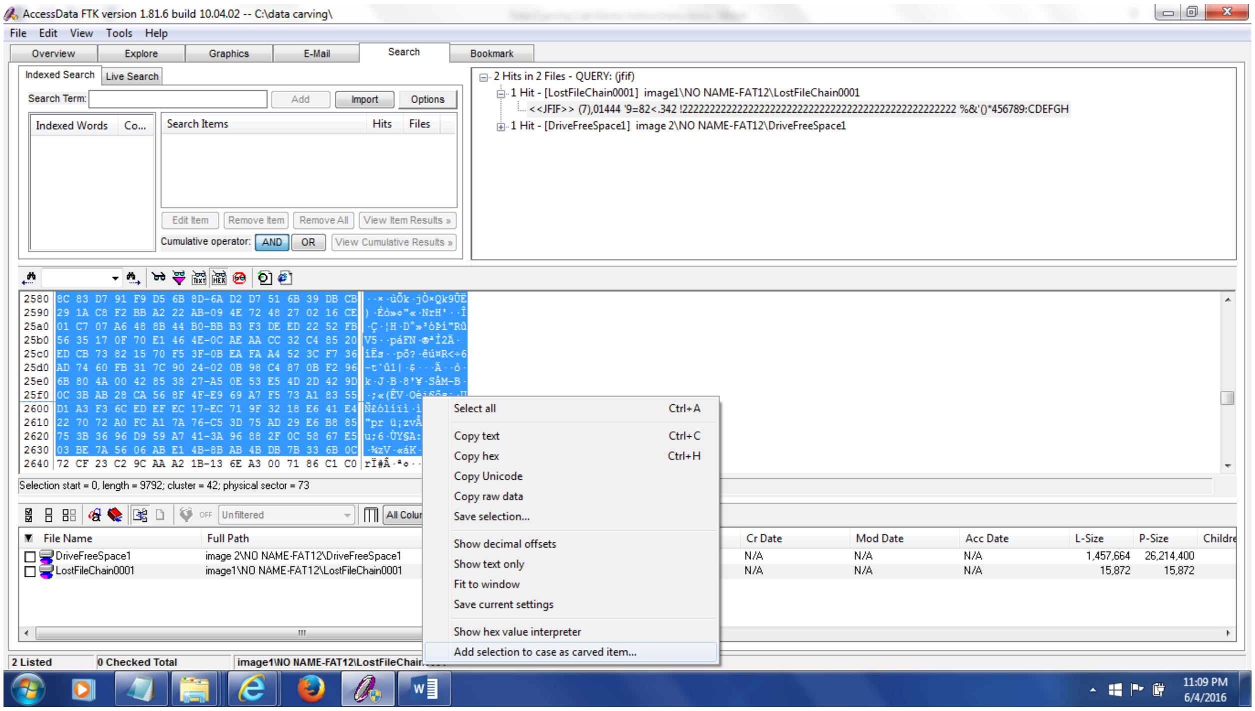
Cursor position = 0; cluster = 42; physical sector = 73

	File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject	Cr Date	Mod Date	Acc Date	L-Size	P-Size	Childre
□	DriveFreeSpace1	image 2\NO NAME-FAT12\DriveFreeSpace1			Drive Free S...	Slack/Free S...		N/A	N/A	N/A	1,457,664	26,214,400	
□	LostFileChain0001	image1\NO NAME-FAT12\LostFileChain0001			Lost clusters	Slack/Free S...		N/A	N/A	N/A	15,872	15,872	

2 Listed | 0 Checked Total | image1\NO NAME-FAT12\LostFileChain0001

11:08 PM
6/4/2016

12. Highlight the file from beginning, and then right click, then select the last menu



```
2 Hits in 2 Files - QUERY: (jfif)
  1 Hit - [LostFileChain0001]  image1\NO NAME-FAT12\LostFileChain0001
    <<JFIF>> (7),01444 '9=82<.342 !22222222222222222222222222222222222222222222222 %&'()*456789:CDEFGH
  1 Hit - [DriveFreeSpace1]  image 2\NO NAME-FAT12\DriveFreeSpace1
```

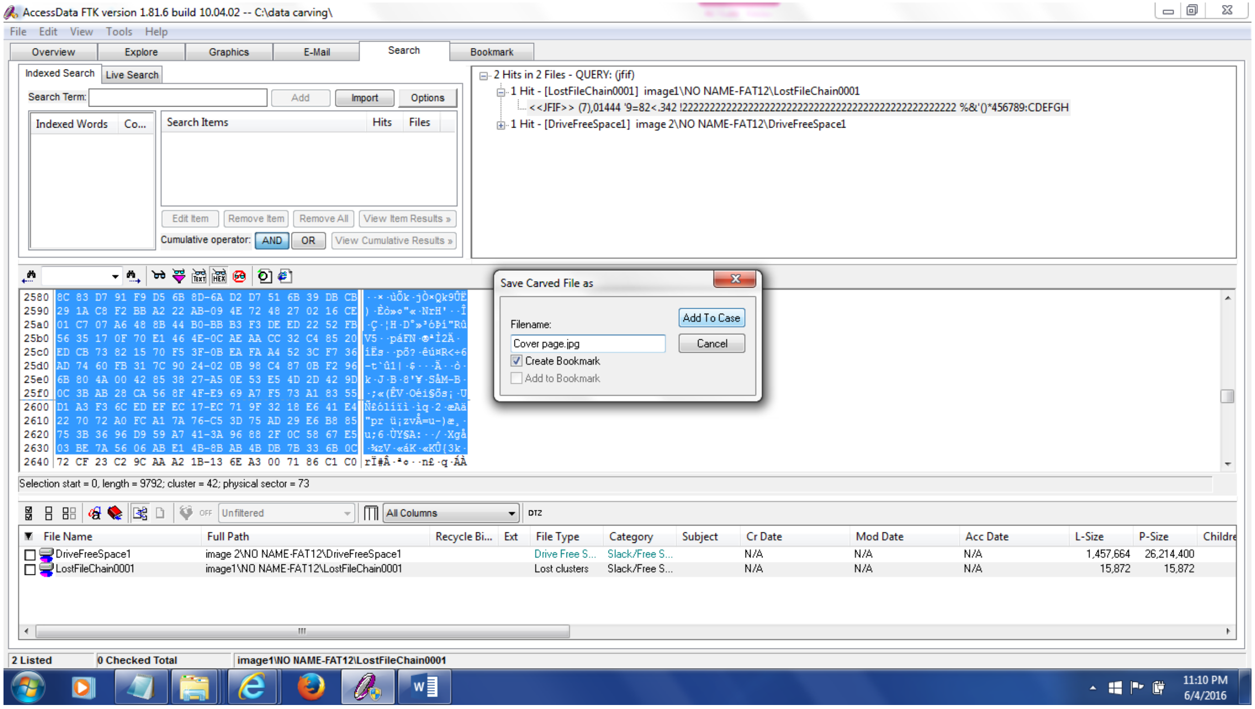
```
2580 8C 83 D7 91 F9 D5 6B 8D-6A D2 D7 51 6B 39 DB CB  ··×·ùÕk·jÒ×Qk9ÛË
2590 29 1A C8 F2 BB A2 22 AB-09 4E 72 48 27 02 16 CE  )·Èò»¢"«·NrH'··Î
25a0 01 C7 07 A6 48 8B 44 B0-BB B3 F3 DE ED 22 52 FB  ·Ç·¦H·D°»³óÞí"Rû
25b0 56 35 17 0F 70 E1 46 4E-0C AE AA CC 32 C4 85 20  V5··páFN·®ªÌ2Ä·
25c0 ED CB 73 82 15 70 F5 3F-0B EA FA A4 52 3C F7 36  íËs··põ?·êú¤R<÷6
25d0 AD 74 60 FB 31 7C 90 24-02 0B 98 C4 87 0B F2 96  -t`û1|·$···Ä··ò·
25e0 6B 80 4A 00 42 85 38 27-A5 0E 53 E5 4D 2D 42 9D  k·J·B·8'¥·SåM-B·
25f0 0C 3B AB 28 CA 56 8F 4F-E9 69 A7 F5 73 A1 83 55  ·;«(ÊV·Oéi
2600 D1 A3 F3 6C ED EF EC 17-EC 71 9F 32 18 E6 41 E4  Ñ£ólíïì·ì
2610 22 70 72 A0 FC A1 7A 76-C5 3D 75 AD 29 E6 B8 85  "pr ü¡zvÅ
2620 75 3B 36 96 D9 59 A7 41-3A 96 88 2F 0C 58 67 E5  u;6·ÙY§A:
2630 03 BE 7A 56 06 AB E1 4B-8B AB 4B DB 7B 33 6B 0C  ·¾zV·«áK·
2640 72 CF 23 C2 9C AA A2 1B-13 6E A3 00 71 86 C1 C0  rÏ#Â·ª¢··
```

Selection start = 0, length = 9792; cluster = 42; physical sector = 73

File Name	Full Path	Cr Date	Mod Date	Acc Date	L-Size	P-Size	Childre
□ DriveFreeSpace1	image 2\NO NAME-FAT12\DriveFreeSpace1	N/A	N/A	N/A	1,457,664	26,214,400	
□ LostFileChain0001	image1\NO NAME-FAT12\LostFileChain0001	N/A	N/A	N/A	15,872	15,872	

2 Listed | 0 Checked Total | image1\NO NAME-FAT12\LostFileChain...

13. Build a data carve file and named as cover page.jpg



```
2 Hits in 2 Files - QUERY: (jfif)
  1 Hit - [LostFileChain0001]  image1\NO NAME-FAT12\LostFileChain0001
    <<JFIF>> (7),01444 '9=82<.342 !22222222222222222222222222222222222222222222222 %&'()*456789:CDEFGH
  1 Hit - [DriveFreeSpace1]  image 2\NO NAME-FAT12\DriveFreeSpace1
```

```
2580 8C 83 D7 91 F9 D5 6B 8D-6A D2 D7 51 6B 39 DB CB  ··×·ùÕk·jÒ×Qk9ÛË
2590 29 1A C8 F2 BB A2 22 AB-09 4E 72 48 27 02 16 CE  )·Èò»¢"«·NrH'··Î
25a0 01 C7 07 A6 48 8B 44 B0-BB B3 F3 DE ED 22 52 FB  ·Ç·¦H·D°»³óÞí"Rû
25b0 56 35 17 0F 70 E1 46 4E-0C AE AA CC 32 C4 85 20  V5··páFN·®ªÌ2Ä·
25c0 ED CB 73 82 15 70 F5 3F-0B EA FA A4 52 3C F7 36  íËs··põ?·êú¤R<÷6
25d0 AD 74 60 FB 31 7C 90 24-02 0B 98 C4 87 0B F2 96  -t`û1|·$···Ä··ò·
25e0 6B 80 4A 00 42 85 38 27-A5 0E 53 E5 4D 2D 42 9D  k·J·B·8'¥·SåM-B·
25f0 0C 3B AB 28 CA 56 8F 4F-E9 69 A7 F5 73 A1 83 55  ·;«(ÊV·Oéi§õs¡·U
2600 D1 A3 F3 6C ED EF EC 17-EC 71 9F 32 18 E6 41 E4  Ñ£ólíïì·ìq·2·æAä
2610 22 70 72 A0 FC A1 7A 76-C5 3D 75 AD 29 E6 B8 85  "pr ü¡zvÅ=u-)æ¸·
2620 75 3B 36 96 D9 59 A7 41-3A 96 88 2F 0C 58 67 E5  u;6·ÙY§A:··/·Xgå
2630 03 BE 7A 56 06 AB E1 4B-8B AB 4B DB 7B 33 6B 0C  ·¾zV·«áK·«KÛ{3k·
2640 72 CF 23 C2 9C AA A2 1B-13 6E A3 00 71 86 C1 C0  rÏ#Â·ª¢··n£·q·ÁÀ
```

Selection start = 0, length = 9792; cluster = 42; physical sector = 73

Save Carved File as

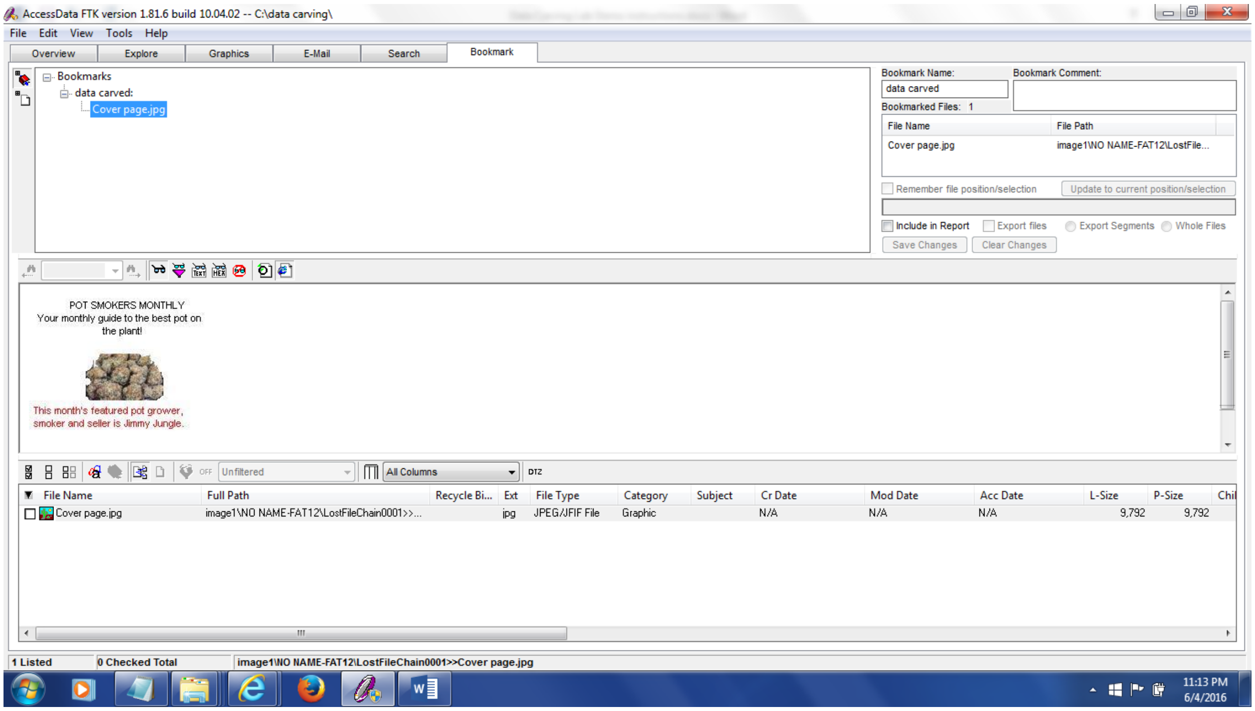
Filename: Cover page.jpg

☑ Create Bookmark
□ Add to Bookmark

File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject	Cr Date	Mod Date	Acc Date	L-Size	P-Size	Childre
□ DriveFreeSpace1	image 2\NO NAME-FAT12\DriveFreeSpace1			Drive Free S...	Slack/Free S...		N/A	N/A	N/A	1,457,664	26,214,400	
□ LostFileChain0001	image1\NO NAME-FAT12\LostFileChain0001			Lost clusters	Slack/Free S...		N/A	N/A	N/A	15,872	15,872	

2 Listed | 0 Checked Total | image1\NO NAME-FAT12\LostFileChain0001

14. Build a bookmark for the cover page file



AccessData FTK version 1.81.6 build 10.04.02 -- C:\data carving\

- Bookmarks
  - data carved:
    - Cover page.jpg

Bookmark Name: data carved

Bookmark Comment:

Bookmarked Files: 1

File Name	File Path
Cover page.jpg	image1\NO NAME-FAT12\LostFile...

☐ Remember file position/selection

☐ Include in Report ☐ Export files ○ Export Segments ○ Whole Files

POT SMOKERS MONTHLY
Your monthly guide to the best pot on the plant!

This month's featured pot grower, smoker and seller is Jimmy Jungle.

OFF Unfiltered

All Columns

	File Name	Full Path	Recycle Bi...	Ext	File Type	Category	Subject	Cr Date	Mod Date	Acc Date	L-Size	P-Size	Chi
☐	Cover page.jpg	image1\NO NAME-FAT12\LostFileChain0001>>...		jpg	JPEG/JFIF File	Graphic		N/A	N/A	N/A	9,792	9,792	

1 Listed | 0 Checked Total | image1\NO NAME-FAT12\LostFileChain0001>>Cover page.jpg

11:13 PM
6/4/2016