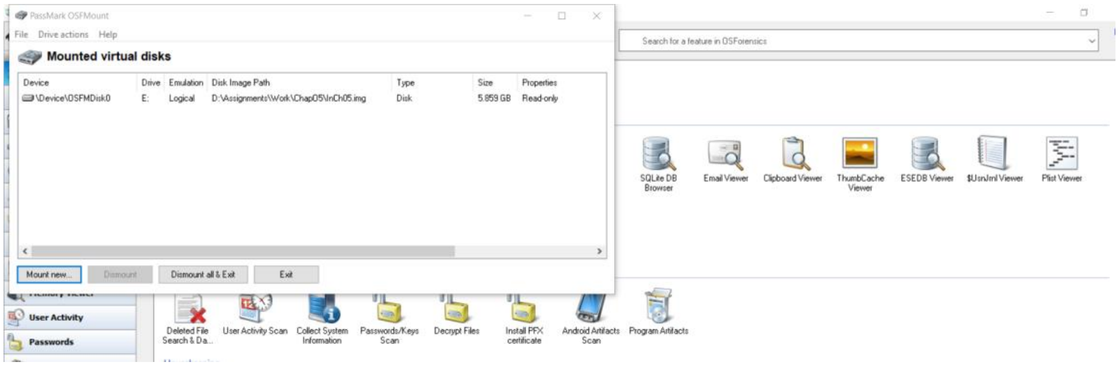
Hands-On Project 13-1

You have been asked to identify any files that might have been uploaded from Denise Robinson’s computer to the Dropbox cloud service. To determine whether files were uploaded, you must find the Dropbox folder where files are synchronized to see what it contains. For this project, you examine the InCh05.img image file you used in the in-chapter activity. Follow these steps:

1. Start OSForensics with the Run as administrator option, and click Continue Using Trial Version. If you dismounted the InCh05.img image file after the in-chapter activity, mount it again.

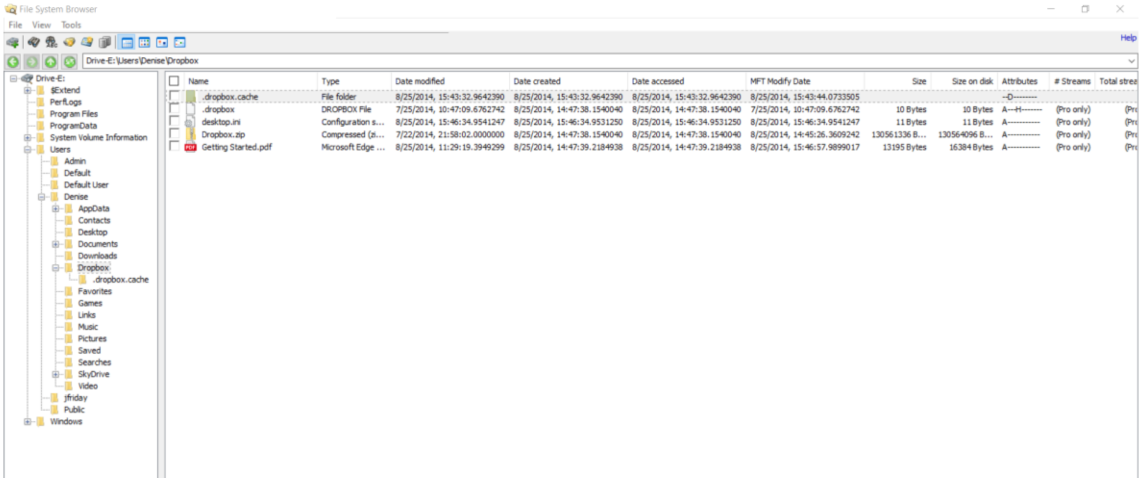


Device	Drive	Emulation	Disk Image Path	Type	Size	Properties
\Device\OSFMDisk0	E:	Logical	D:\Assignments\Work\Chap05\InCh05.img	Disk	5.859 GB	Read-only

2. Click the Manage Case button, and verify that the InChap13 case has a green check mark next to it in the Select Case window. If not, right-click the case name and click Open. If the case isn’t displayed, click Import Case, navigate to and click the case location folder, and then click OK.

3. You need to find Denise Robinson’s account name listed in drive:\Users\username\ Dropbox. To find this information, click File System Browser in the left pane. In the “Select device to add” dialog box, click the Drive Letter option button, if necessary. Click the Drive Letter list arrow (see Figure 13-3), click the drive letter assigned to the InCh05.img file, and then click OK.

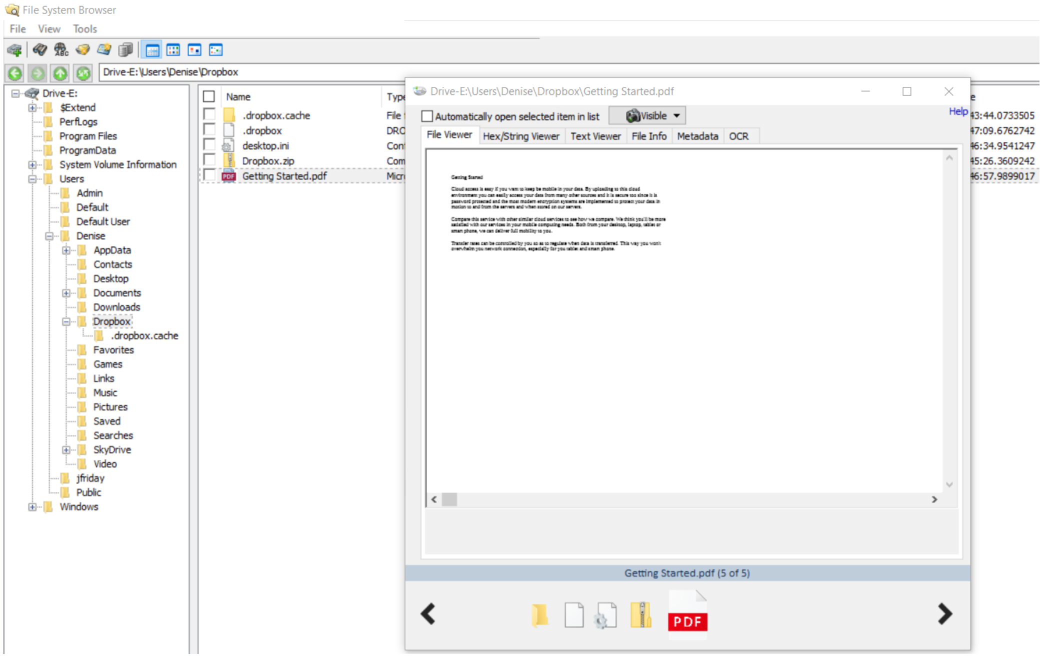
4. In the File System Browser window, navigate to drive\Users (substituting the correct drive letter for drive) and expand the file listings. Click to expand the Denise user account folder, and then click the Dropbox subfolder, as shown in Figure 13-4.



Drive-E:\Users\Denise\Dropbox

Name	Type	Date modified	Date created	Date accessed	MFT Modify Date	Size	Size on disk	Attributes	# Streams	Total strea
.dropbox.cache	File folder	8/25/2014, 15:43:32.9642390	8/25/2014, 15:43:32.9642390	8/25/2014, 15:43:32.9642390	8/25/2014, 15:43:44.0733505			--D--------		
.dropbox	DROPBOX File	7/25/2014, 10:47:09.6762742	8/25/2014, 14:47:38.1540040	8/25/2014, 14:47:38.1540040	7/25/2014, 10:47:09.6762742	10 Bytes	10 Bytes	A---H-------	(Pro only)	(Pr
desktop.ini	Configuration s...	8/25/2014, 15:46:34.9541247	8/25/2014, 15:46:34.9531250	8/25/2014, 15:46:34.9531250	8/25/2014, 15:46:34.9541247	11 Bytes	11 Bytes	A-----------	(Pro only)	(Pr
Dropbox.zip	Compressed (zi...	7/22/2014, 21:58:02.0000000	8/25/2014, 14:47:38.1540040	8/25/2014, 14:47:38.1540040	8/25/2014, 14:45:26.3609242	130561336 B...	130564096 B...	A-----------	(Pro only)	(Pr
Getting Started.pdf	Microsoft Edge ...	8/25/2014, 11:29:19.3949299	8/25/2014, 14:47:39.2184938	8/25/2014, 14:47:39.2184938	8/25/2014, 15:46:57.9899017	13195 Bytes	16384 Bytes	A-----------	(Pro only)	(Pr

5. Right-click the Getting Started.pdf file in the right pane and click View with Internal Viewer to display its contents. In the viewer window, click the File Viewer tab (see Figure 13-5), if necessary, and scroll through the document, which is a welcome notice from Dropbox. Close this viewer window, and repeat this step for other files in this folder to determine their contents.



Drive-E:\Users\Denise\Dropbox

Drive-E:\Users\Denise\Dropbox\Getting Started.pdf

□ Automatically open selected item in list

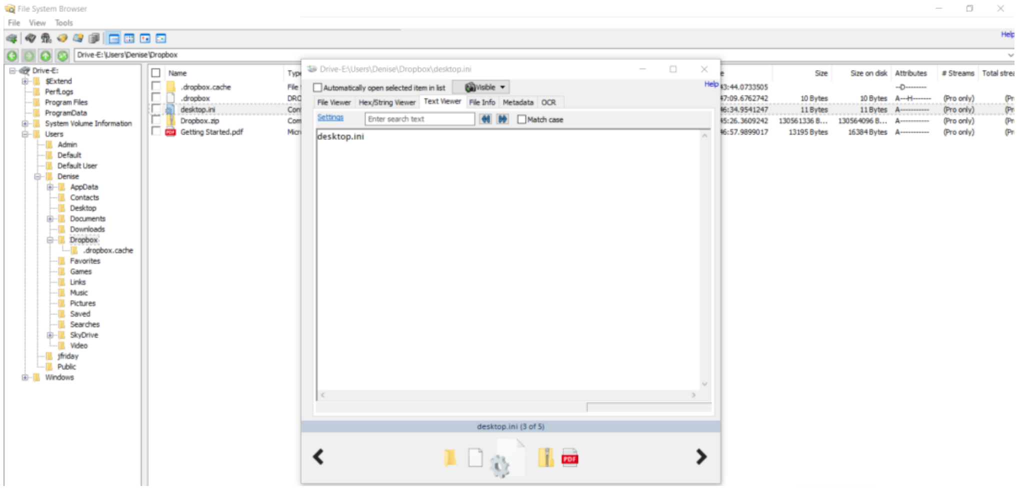
Getting Started

Cloud access is easy if you want to keep be mobile in your data. By uploading to this cloud environment you can easily access your data from many other sources and it is secure too since it is password protected and the most modern encryption systems are implemented to protect your data in motion to and from the servers and when stored on our servers.

Compare this service with other similar cloud services to see how we compare. We think you'll be more satisfied with our services in your mobile computing needs. Both from your desktop, laptop, tablet or smart phone, we can deliver full mobility to you.

Transfer rates can be controlled by you so as to regulate when data is transferred. This way you won't overwhelm you network connection, especially for you tablet and smart phone.

Getting Started.pdf (5 of 5)



```
desktop.ini
```

6. In the File System Browser window, right-click the Dropbox.zip file and click Save to disk. In the “Save file as” dialog box, navigate to your work folder, click Save, and then click OK. Close the File System Browser window.

7. Open File Explorer, navigate to your work folder, and extract (unzip) Dropbox.zip. Examine the extracted data and write a memo to the attorney stating that you recovered the Dropbox.zip file and describing its contents.

Report:

This project is about recovering files that may have been posted to the Dropbox cloud service from Denise Robinson's PC. I used the OSforensic forensics tool to mount the given image file InCh05.img and discovered many files in the user directory. I was able to extract the Dropbox.zip file from the image file, and after decompressing it, I discovered 23 image files. Following more study, I discovered that the image files belong to the San Francisco de Asis Church. The image includes shots of many parts of the edifice, and it's possible that photos of artwork and adobe structures were uploaded from there.

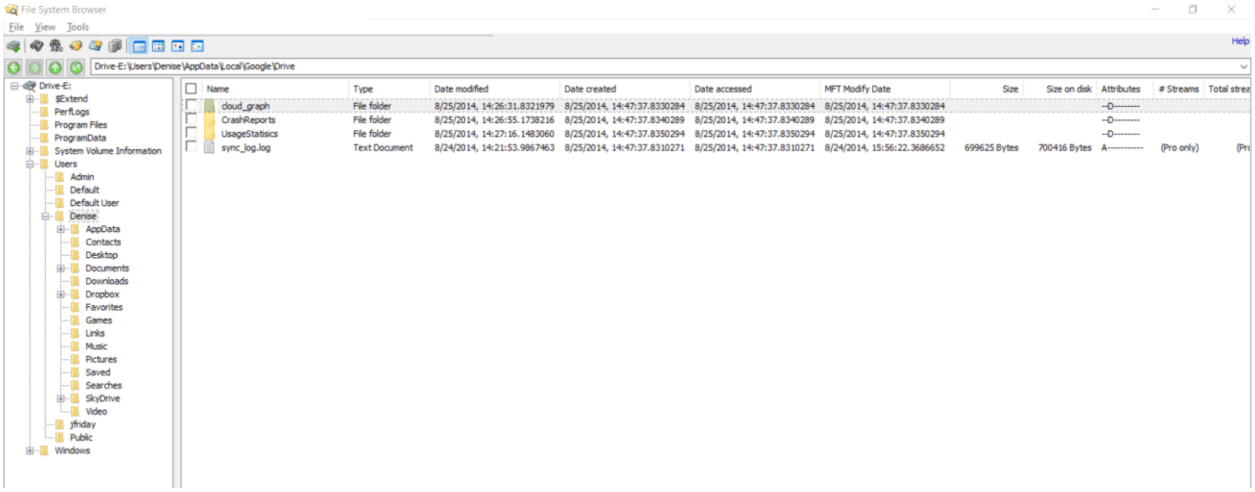
8. Leave the InChap13 case open and OSForensics running for the next project.

Hands-On Project 13-2

The attorney managing the case discovered that Denise Robinson’s computer contains the IMG_3646.png file that might have been uploaded to Google Drive. To determine whether it has, you need to examine the Google Drive file sync_log.log. For this project, you need a text editor (Notepad, WordPad, or any word processor), OSForensics, a Web browser, and the image file InCh05.img you saved in Hands-On Project 13-1. Follow these steps:

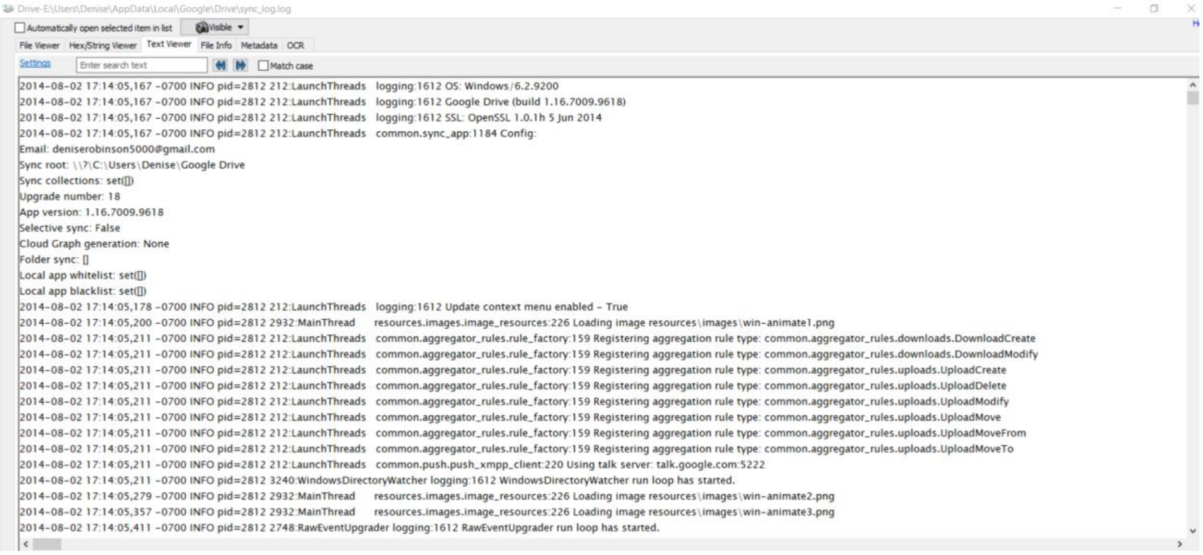
1. If you exited OSForensics, restart it, and open the InChap13 case and the InCh05.img file.

2. Click File System Browser in the left pane and navigate to C:\Users\Denise\AppData\Local\Google\Drive. Right-click sync_log.log and click View with Internal Viewer.



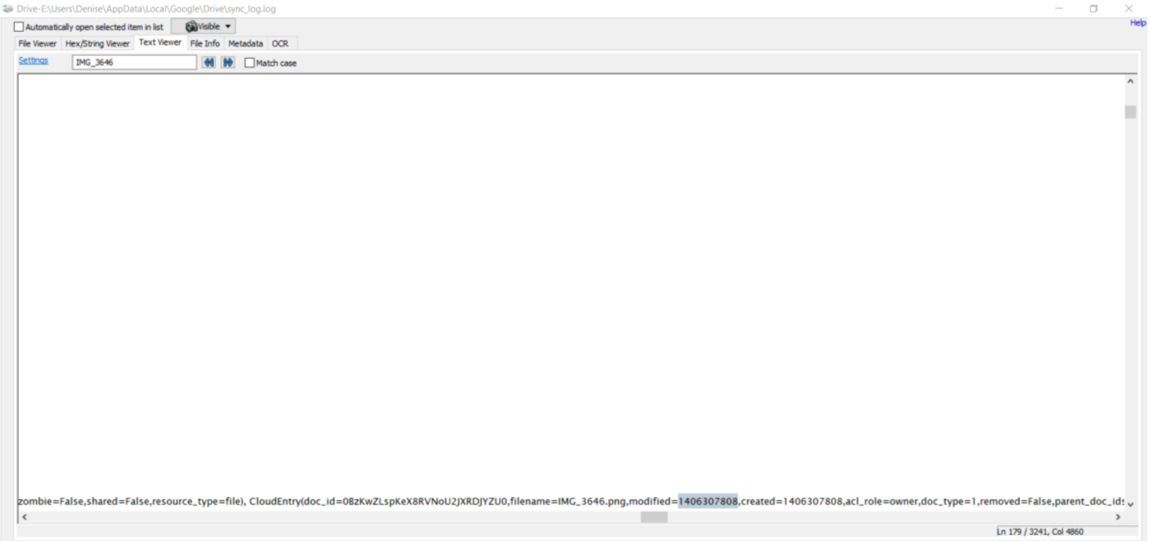
Name	Type	Date modified	Date created	Date accessed	MFT Modify Date	Size	Size on disk	Attributes	# Streams	Total strea
cloud_graph	File folder	8/25/2014, 14:26:31.8321979	8/25/2014, 14:47:37.8330284	8/25/2014, 14:47:37.8330284	8/25/2014, 14:47:37.8330284			--D--------		
CrashReports	File folder	8/25/2014, 14:26:55.1738216	8/25/2014, 14:47:37.8340289	8/25/2014, 14:47:37.8340289	8/25/2014, 14:47:37.8340289			--D--------		
UsageStatisics	File folder	8/25/2014, 14:27:16.1483060	8/25/2014, 14:47:37.8350294	8/25/2014, 14:47:37.8350294	8/25/2014, 14:47:37.8350294			--D--------		
sync_log.log	Text Document	8/24/2014, 14:21:53.9867463	8/25/2014, 14:47:37.8310271	8/25/2014, 14:47:37.8310271	8/24/2014, 15:56:22.3686652	699625 Bytes	700416 Bytes	A----------	(Pro only)	(Pr

3. In the viewer window, click the Text Viewer tab, if necessary. In the text box, type IMG_3646, and then click the >> button. Finding the file confirms that it was uploaded to Google Drive.


Drive-E:\Users\Denise\AppData\Local\Google\Drive\sync_log.log
□ Automatically open selected item in list
Visible
File Viewer
Hex/String Viewer
Text Viewer
File Info
Metadata
OCR
Settings
Enter search text
□ Match case

```
2014-08-02 17:14:05,167 -0700 INFO pid=2812 212:LaunchThreads   logging:1612 OS: Windows/6.2.9200
2014-08-02 17:14:05,167 -0700 INFO pid=2812 212:LaunchThreads   logging:1612 Google Drive (build 1.16.7009.9618)
2014-08-02 17:14:05,167 -0700 INFO pid=2812 212:LaunchThreads   logging:1612 SSL: OpenSSL 1.0.1h 5 Jun 2014
2014-08-02 17:14:05,167 -0700 INFO pid=2812 212:LaunchThreads   common.sync_app:1184 Config:
Email: deniserobinson5000@gmail.com
Sync root: \\?\C:\Users\Denise\Google Drive
Sync collections: set([])
Upgrade number: 18
App version: 1.16.7009.9618
Selective sync: False
Cloud Graph generation: None
Folder sync: []
Local app whitelist: set([])
Local app blacklist: set([])
2014-08-02 17:14:05,178 -0700 INFO pid=2812 212:LaunchThreads   logging:1612 Update context menu enabled - True
2014-08-02 17:14:05,200 -0700 INFO pid=2812 2932:MainThread     resources.images.image_resources:226 Loading image resources\images\win-animate1.png
2014-08-02 17:14:05,211 -0700 INFO pid=2812 212:LaunchThreads   common.aggregator_rules.rule_factory:159 Registering aggregation rule type: common.aggregator_rules.downloads.DownloadCreate
2014-08-02 17:14:05,211 -0700 INFO pid=2812 212:LaunchThreads   common.aggregator_rules.rule_factory:159 Registering aggregation rule type: common.aggregator_rules.downloads.DownloadModify
2014-08-02 17:14:05,211 -0700 INFO pid=2812 212:LaunchThreads   common.aggregator_rules.rule_factory:159 Registering aggregation rule type: common.aggregator_rules.uploads.UploadCreate
2014-08-02 17:14:05,211 -0700 INFO pid=2812 212:LaunchThreads   common.aggregator_rules.rule_factory:159 Registering aggregation rule type: common.aggregator_rules.uploads.UploadDelete
2014-08-02 17:14:05,211 -0700 INFO pid=2812 212:LaunchThreads   common.aggregator_rules.rule_factory:159 Registering aggregation rule type: common.aggregator_rules.uploads.UploadModify
2014-08-02 17:14:05,211 -0700 INFO pid=2812 212:LaunchThreads   common.aggregator_rules.rule_factory:159 Registering aggregation rule type: common.aggregator_rules.uploads.UploadMove
2014-08-02 17:14:05,211 -0700 INFO pid=2812 212:LaunchThreads   common.aggregator_rules.rule_factory:159 Registering aggregation rule type: common.aggregator_rules.uploads.UploadMoveFrom
2014-08-02 17:14:05,211 -0700 INFO pid=2812 212:LaunchThreads   common.aggregator_rules.rule_factory:159 Registering aggregation rule type: common.aggregator_rules.uploads.UploadMoveTo
2014-08-02 17:14:05,211 -0700 INFO pid=2812 212:LaunchThreads   common.push.push_xmpp_client:220 Using talk server: talk.google.com:5222
2014-08-02 17:14:05,211 -0700 INFO pid=2812 3240:WindowsDirectoryWatcher logging:1612 WindowsDirectoryWatcher run loop has started.
2014-08-02 17:14:05,279 -0700 INFO pid=2812 2932:MainThread     resources.images.image_resources:226 Loading image resources\images\win-animate2.png
2014-08-02 17:14:05,357 -0700 INFO pid=2812 2932:MainThread     resources.images.image_resources:226 Loading image resources\images\win-animate3.png
2014-08-02 17:14:05,411 -0700 INFO pid=2812 2748:RawEventUpgrader logging:1612 RawEventUpgrader run loop has started.
```

4. Scroll to the right to view the modified=1406307808 and created=1406307808 values. Because both timestamp values are identical, you need to convert only one of them. Highlight the modified timestamp 1406307808, as shown in Figure 13-6, and then right-click it and click Copy.



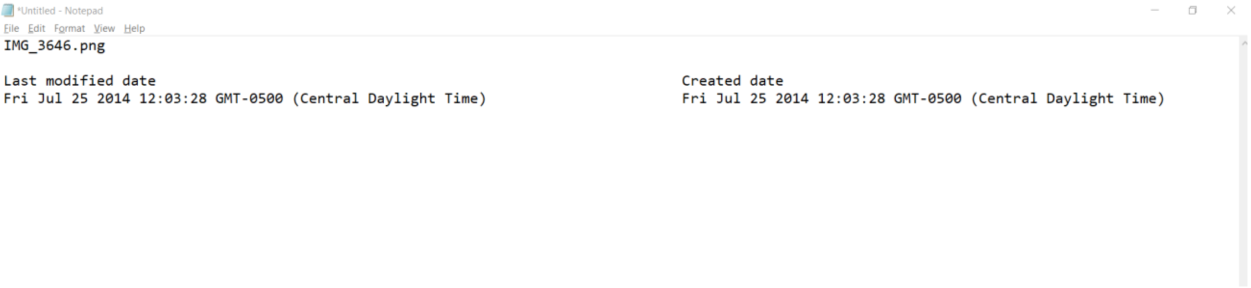
```
zombie=False,shared=False,resource_type=file), CloudEntry(doc_id=0BzKwZLspKeX8RVNoU2JXRDJYZU0,filename=IMG_3646.png,modified=1406307808,created=1406307808,acl_role=owner,doc_type=1,removed=False,parent_doc_ids
```

5. Start a Web browser, go to http://unixtime-converter.com, paste the numbers into the UNIX Timestamp text box, as shown in Figure 13-7, and click Convert. (Note: If you can't access this Web site, try www.onlineconversion.com/unix_time.htm.)

6. In the Result text box, highlight the converted date and time value, and then right-click it and click Copy.

Detected timestamp is: Fri Jul 25 2014 12:03:28 GMT-0500 (Central Daylight Time)

7. Start a text editor and type IMG_3646.png in the first line. Press Enter to add a blank line, and then press Enter again. Create two columns by typing Last modified date, pressing Tab eight times, and typing Created date. Place the cursor under the "Last modified date" column, and then right-click and click Paste. Repeat to paste the same date and time value under the "Created date" column.



```
IMG_3646.png

Last modified date                                                                      Created date
Fri Jul 25 2014 12:03:28 GMT-0500 (Central Daylight Time)                               Fri Jul 25 2014 12:03:28 GMT-0500 (Central Daylight Time)
```

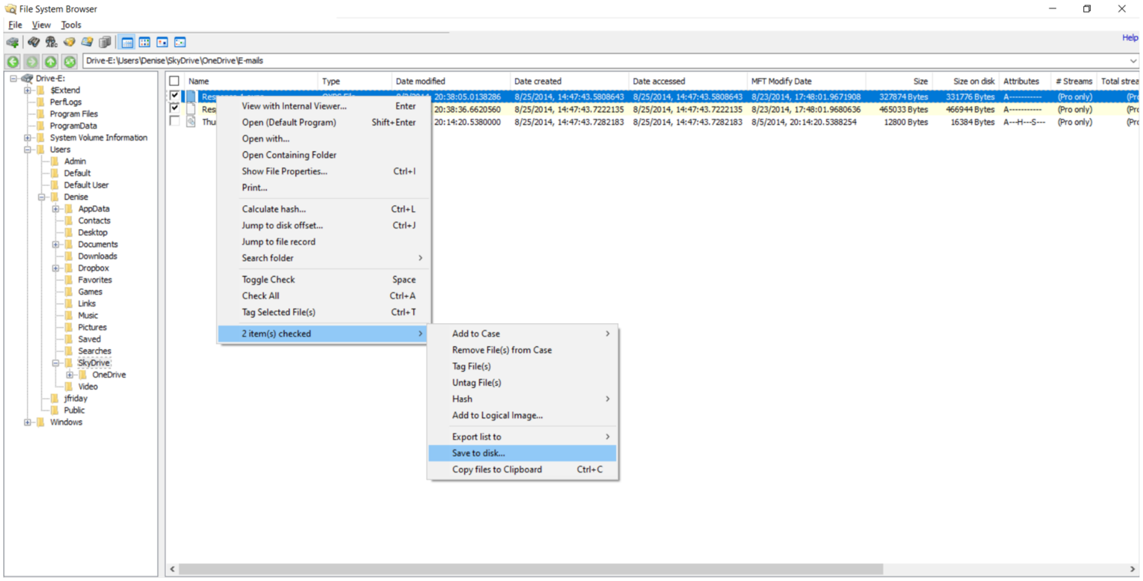
8. Save the file as Google Drive IMG_3646 date stamps.txt. Exit the text editor, and turn this file in to your instructor. Leave OSForensics running for the next project.

Hands-On Project 13-3

The case attorney asked you to examine the OneDrive synchronization folder for Denise Robinson to look for any e-mail correspondence. Follow these steps:

1. If you exited OSForensics, restart it, and open the InChap13 case and InCh05.img file. In the left pane, click File System Browser.

2. In the File System Browser window, navigate to drive:\Users\Denise\SkyDrive\ OneDrive\E-mails. Extract all files with the extension. oxps by right-clicking each file and clicking Save to disk, and then clicking OK in the message box about saving the file successfully. Exit OSForensics.



	Name	Type	Date modified	Date created	Date accessed	MFT Modify Date	Size	Size on disk	Attributes	# Streams	Total strea
☑	Res		20:38:05.0138286	8/25/2014, 14:47:43.5808643	8/25/2014, 14:47:43.5808643	8/23/2014, 17:48:01.9671908	327874 Bytes	331776 Bytes	A----------	(Pro only)	(Pr
☑	Res		20:38:36.6620560	8/25/2014, 14:47:43.7222135	8/25/2014, 14:47:43.7222135	8/23/2014, 17:48:01.9680636	465033 Bytes	466944 Bytes	A----------	(Pro only)	(Pr
□	Thu		20:14:20.5380000	8/25/2014, 14:47:43.7282183	8/25/2014, 14:47:43.7282183	8/5/2014, 20:14:20.5388254	12800 Bytes	16384 Bytes	A---H---S---	(Pro only)	(Pr

3. Open File Explorer, navigate to your work folder, and open each file to view its contents. Write a one-page memo describing the contents of each file you recovered, and then close File Explorer. Turn the memo in to your instructor.

Response 1 content

Sent: Friday, July 25, 2014 at 11:05 AM

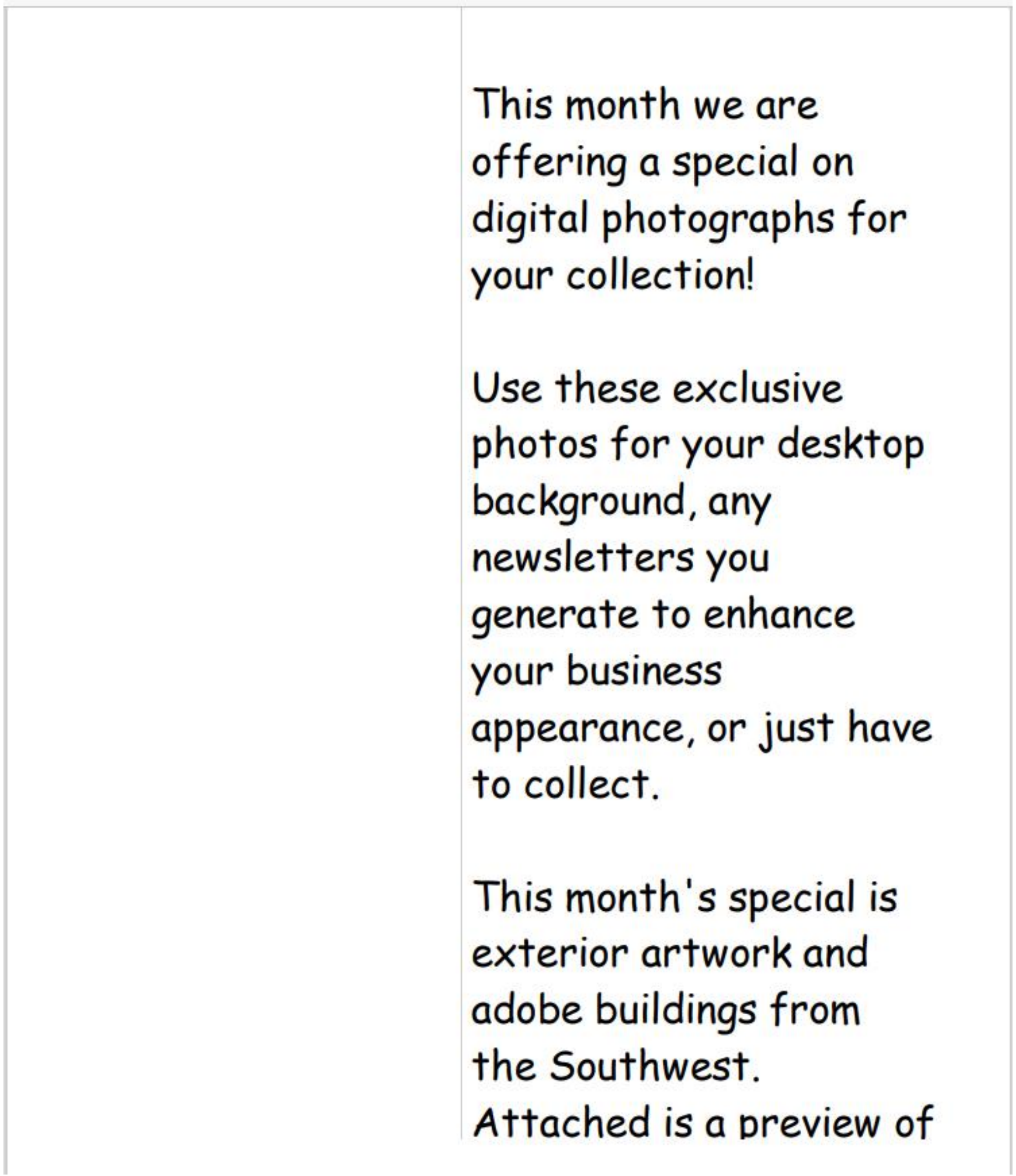
From: "Denise Robinson"

To: No recipient address

Subject: EXCLUSIVE OFFER! Photos for sale!

Dear Colleague: We're running a bargain on digital images for your collection this month! Use these exclusive photographs as a desktop wallpaper, in any newsletters you send out to improve your company's image, or simply to collect. This month's theme is Southwest exterior artwork and adobe structures. A sneak peek at this month's photographs is attached. Each photograph normally sells for $29.95. This month's special pricing is only $19.95 each plus tax and handling, only for you. Please reply to this e-mail message with the photo file number to place a purchase. Get your images as soon as possible before they are claimed by someone else.

Response 2 content



This month we are offering a special on digital photographs for your collection!

Use these exclusive photos for your desktop background, any newsletters you generate to enhance your business appearance, or just have to collect.

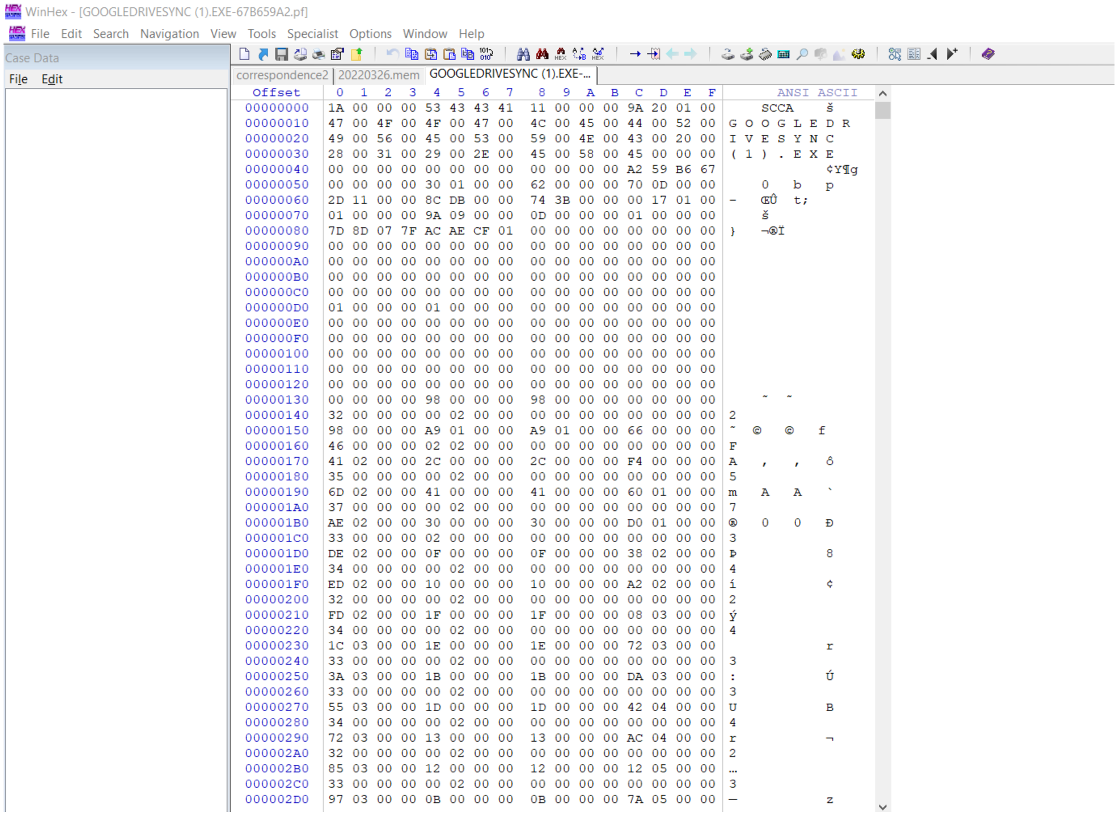
This month's special is exterior artwork and adobe buildings from the Southwest.
Attached is a preview of

Hands-On Project 13-4

The case attorney wants to know the last time Denise Robinson accessed Google Drive. To find this information, use the following steps. If you need help, refer to the in-chapter activity.

1.Start WinHex, and open the

drive:\Windows\Prefetch\GOOGLEDRIVESYNC(1).EXE67B59A2.pf file.


WinHex - [GOOGLEDRIVESYNC (1).EXE-67B659A2.pf]
File Edit Search Navigation View Tools Specialist Options Window Help
Case Data
File Edit
correspondence2
20220326.mem
GOOGLEDRIVESYNC (1).EXE-...

```
  Offset   0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F     ANSI ASCII
00000000  1A 00 00 00 53 43 43 41  11 00 00 00 9A 20 01 00      SCCA    š
00000010  47 00 4F 00 4F 00 47 00  4C 00 45 00 44 00 52 00  G O O G L E D R
00000020  49 00 56 00 45 00 53 00  59 00 4E 00 43 00 20 00  I V E S Y N C
00000030  28 00 31 00 29 00 2E 00  45 00 58 00 45 00 00 00  ( 1 ) . E X E
00000040  00 00 00 00 00 00 00 00  00 00 00 00 A2 59 B6 67              ¢Y¶g
00000050  00 00 00 00 30 01 00 00  62 00 00 00 70 0D 00 00      0   b   p
00000060  2D 11 00 00 8C DB 00 00  74 3B 00 00 00 17 01 00  -   ŒÛ  t;
00000070  01 00 00 00 9A 09 00 00  0D 00 00 00 01 00 00 00      š
00000080  7D 8D 07 7F AC AE CF 01  00 00 00 00 00 00 00 00  }   ¬®Ï
00000090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000D0  01 00 00 00 01 00 00 00  00 00 00 00 00 00 00 00
000000E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000110  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000120  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000130  00 00 00 00 98 00 00 00  98 00 00 00 00 00 00 00      ˜   ˜
00000140  32 00 00 00 00 02 00 00  00 00 00 00 00 00 00 00  2
00000150  98 00 00 00 A9 01 00 00  A9 01 00 00 66 00 00 00  ˜   ©   ©   f
00000160  46 00 00 00 02 02 00 00  00 00 00 00 00 00 00 00  F
00000170  41 02 00 00 2C 00 00 00  2C 00 00 00 F4 00 00 00  A   ,   ,   ô
00000180  35 00 00 00 00 02 00 00  00 00 00 00 00 00 00 00  5
00000190  6D 02 00 00 41 00 00 00  41 00 00 00 60 01 00 00  m   A   A   `
000001A0  37 00 00 00 00 02 00 00  00 00 00 00 00 00 00 00  7
000001B0  AE 02 00 00 30 00 00 00  30 00 00 00 D0 01 00 00  ®   0   0   Ð
000001C0  33 00 00 00 02 00 00 00  00 00 00 00 00 00 00 00  3
000001D0  DE 02 00 00 0F 00 00 00  0F 00 00 00 38 02 00 00  Þ           8
000001E0  34 00 00 00 00 02 00 00  00 00 00 00 00 00 00 00  4
000001F0  ED 02 00 00 10 00 00 00  10 00 00 00 A2 02 00 00  í           ¢
00000200  32 00 00 00 00 02 00 00  00 00 00 00 00 00 00 00  2
00000210  FD 02 00 00 1F 00 00 00  1F 00 00 00 08 03 00 00  ý
00000220  34 00 00 00 00 02 00 00  00 00 00 00 00 00 00 00  4
00000230  1C 03 00 00 1E 00 00 00  1E 00 00 00 72 03 00 00              r
00000240  33 00 00 00 00 02 00 00  00 00 00 00 00 00 00 00  3
00000250  3A 03 00 00 1B 00 00 00  1B 00 00 00 DA 03 00 00  :           Ú
00000260  33 00 00 00 00 02 00 00  00 00 00 00 00 00 00 00  3
00000270  55 03 00 00 1D 00 00 00  1D 00 00 00 42 04 00 00  U           B
00000280  34 00 00 00 00 02 00 00  00 00 00 00 00 00 00 00  4
00000290  72 03 00 00 13 00 00 00  13 00 00 00 AC 04 00 00  r           ¬
000002A0  32 00 00 00 00 02 00 00  00 00 00 00 00 00 00 00  2
000002B0  85 03 00 00 12 00 00 00  12 00 00 00 12 05 00 00  …
000002C0  33 00 00 00 00 02 00 00  00 00 00 00 00 00 00 00  3
000002D0  97 03 00 00 0B 00 00 00  0B 00 00 00 7A 05 00 00  —           z
```

2. Find the Windows date and time at offset 0x80 and the number of times this file has been run since it was installed at offset 0xD4.

3. Write a memo stating the date, time, and number of times this program has been run. Turn the memo in to your instructor, and exit WinHex.

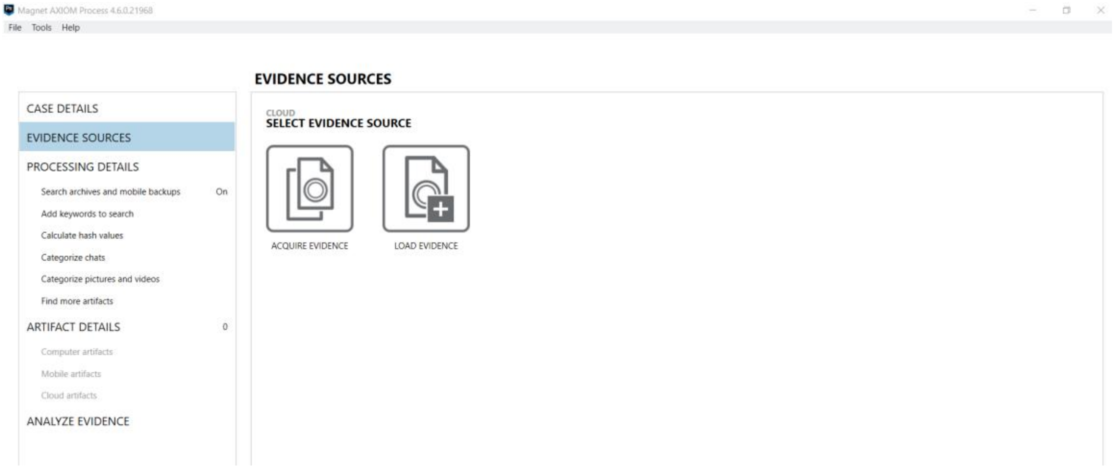
Report:

The date and time on Windows at offset 0*80 is 8/25/2014 17:20:54 PM, and the digit at 0*D4 is 0*01, thus the file has only been run once since it was installed at offset 0*D4.

Hands-On Project 13-5

Jim Shu has been using his phone to access his Facebook and Google Drive information. In this project, you use Magnet AXIOM to examine evidence stored in the cloud. 1. Start Magnet AXIOM Process, and click the CREATE NEW CASE button. In the Case number text box, type today's date followed by a hyphen and the number of the case you're working on that day. In the LOCATION FOR CASE FILES section, type Hands-On Project 13-5 in the Folder name text box. Click the BROWSE button next to the File path text box, navigate to and click your work folder, and click Select Folder. In the LOCATION FOR ACQUIRED EVIDENCE section, the folder name and file path should update automatically to be the same. If they don't, type Hands-On Project 13-5 for the folder name and select the path as described previously.

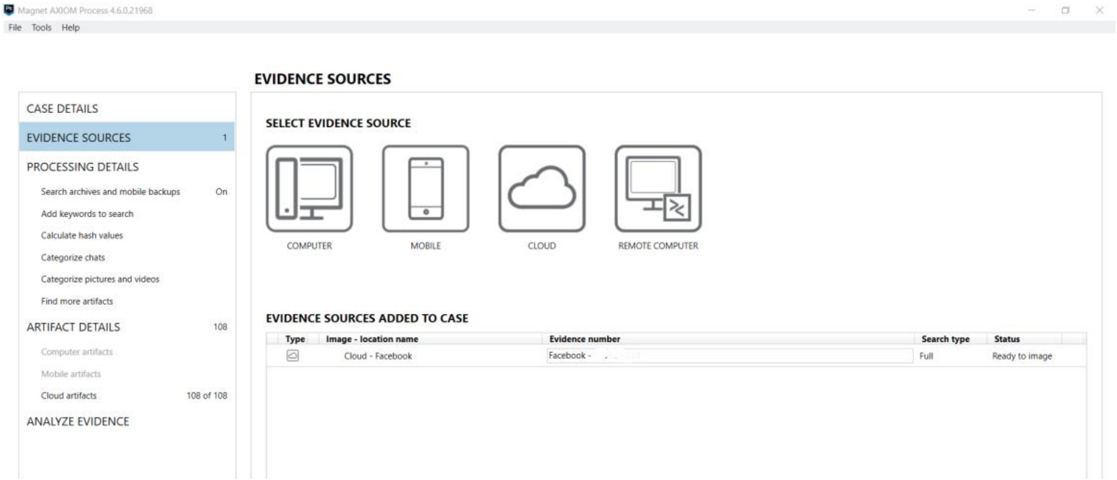
2. Click the GO TO EVIDENCE SOURCES button. In the SELECT EVIDENCE SOURCE section, click the CLOUD icon, and then click NEXT. In the EVIDENCE SOURCES window, click the ACQUIRE EVIDENCE icon (see Figure 13-8), and then click NEXT.



3. In the next window, click the I have proper search authorization to access the target's information stored in the cloud check box. The window shown in Figure 13-9 opens automatically, where you specify which platforms you want to access. (Note: For an actual case, you must sign in with victim or suspect's username and password.) Click the Facebook icon. In the SIGN IN TO FACEBOOK window, you select a sign-in method as well as your username and password. If you have a Facebook account, enter your login information and attempt to sign in. If you're successful, the SELECT DATE RANGE window opens.

4. Notice that you can set a date range or leave the default option, which is all dates. Your choice might depend on the warrant you have. Under it is the SELECT SERVICES AND CONTENT section with check boxes for Facebook Profile Info, Facebook Messenger Messages, and Facebook Timeline. All are selected by default, so leave them selected for this project. Click NEXT to go to

the PROCESSING DETAILS window, where you can add keywords or known hashes for media files, if needed. Click Cloud Artifacts on the left. Click GO TO ANALYZE EVIDENCE, and in the next window, click ANALYZE EVIDENCE.



EVIDENCE SOURCES

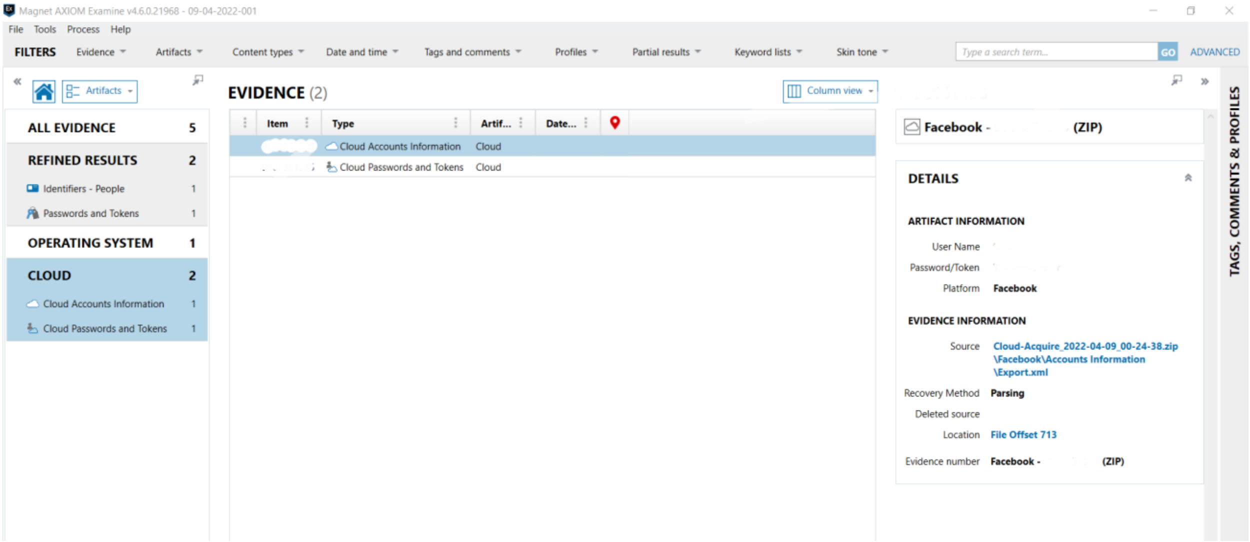
CASE DETAILS	
EVIDENCE SOURCES	1
PROCESSING DETAILS	
Search archives and mobile backups	On
Add keywords to search	
Calculate hash values	
Categorize chats	
Categorize pictures and videos	
Find more artifacts	
ARTIFACT DETAILS	108
Computer artifacts	
Mobile artifacts	
Cloud artifacts	108 of 108
ANALYZE EVIDENCE	

SELECT EVIDENCE SOURCE

EVIDENCE SOURCES ADDED TO CASE

Type	Image - location name	Evidence number	Search type	Status
	Cloud - Facebook	Facebook - [redacted]	Full	Ready to image

5. When it’s finished processing, start Magnet AXIOM Examine, if necessary. Review all the information on your Facebook account that’s available, and take screenshots. In the center pane, click the Column view down arrow and click Timeline view. Write a one- to two-page paper explaining what information on a suspect or victim could be found. Include your screenshots, and submit them with the paper to your instructor. Exit Magnet AXIOM.



ALL EVIDENCE	5
REFINED RESULTS	2
Identifiers - People	1
Passwords and Tokens	1
OPERATING SYSTEM	1
CLOUD	2
Cloud Accounts Information	1
Cloud Passwords and Tokens	1

EVIDENCE (2)

Item	Type	Artif...	Date...	
[redacted]	Cloud Accounts Information	Cloud		
[redacted]	Cloud Passwords and Tokens	Cloud		

Facebook - [redacted] (ZIP)

DETAILS

ARTIFACT INFORMATION

User Name [redacted]
Password/Token [redacted]
Platform Facebook

EVIDENCE INFORMATION

Source Cloud-Acquire_2022-04-09_00-24-38.zip \Facebook\Accounts Information \Export.xml
Recovery Method Parsing
Deleted source
Location File Offset 713
Evidence number Facebook - [redacted] (ZIP)