FORENSICS V2 LAB SERIES

Lab 14: Timeline Analysis

Document Version: 2021-01-14

Contents

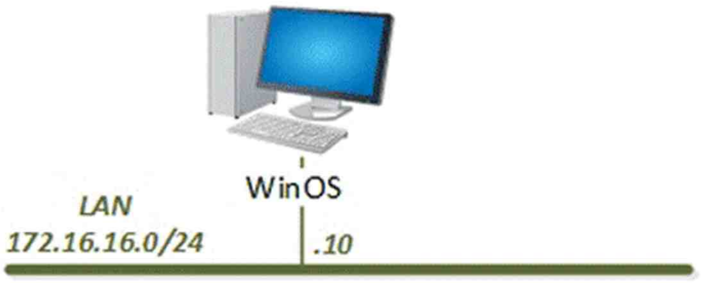
Introduction

It is often useful to review a data set based on temporal metadata. Organizing the information by dates and times can provide endless insights into user behavior.

Objectives

- Learn what a timeline analysis is
- Learn how to review a case based on different types of file system dates and times
- Learn how to access additional metadata that can be used to assist in the timeline analysis

Lab Topology



Lab Settings

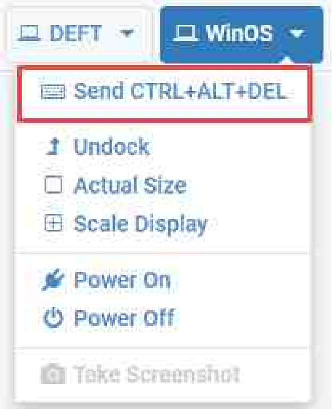
The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	**IP Address / Subnet Mask**	**Account** (if needed)	**Password** (if needed)
Caine	172.16.16.30	caine	Train1ng$
CSI-Linux	172.16.16.40	csi	csi
DEFT	172.16.16.20	deft	Train1ng$
WinOS	172.16.16.10	Administrator	Train1ng$

1 Getting Familiar with Autopsy Timeline

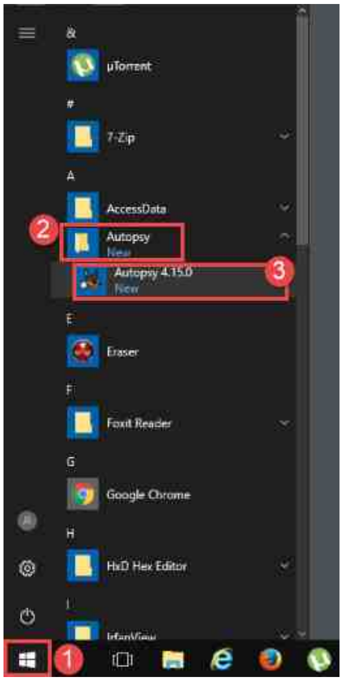
Timeline analysis is a useful investigative technique that involves sorting the data by their timestamp. The typical file tree navigation is helpful and can be used to quickly access known areas and review files within the selected folders. It is less helpful when you are examining a case where you need to track all the files that were affected within a certain timeframe. This is where timeline analysis comes in handy. Some forensic tools allow you to view all the data within a directory and its subdirectories, which is great for sorting by different dates and times. Other tools have timeline features that allow you to do the same thing but are a bit more intuitive and flexible. Autopsy contains the latter. It has a very useful timeline feature, which we will be using in this lab. In this exercise, we will get you familiar with the timeline and its features.

1. To begin, launch the WinOS virtual machine to access the graphical login screen.
   a. Select Send CTRL+ALT+DEL from the dropdown menu to be prompted with the login screen.

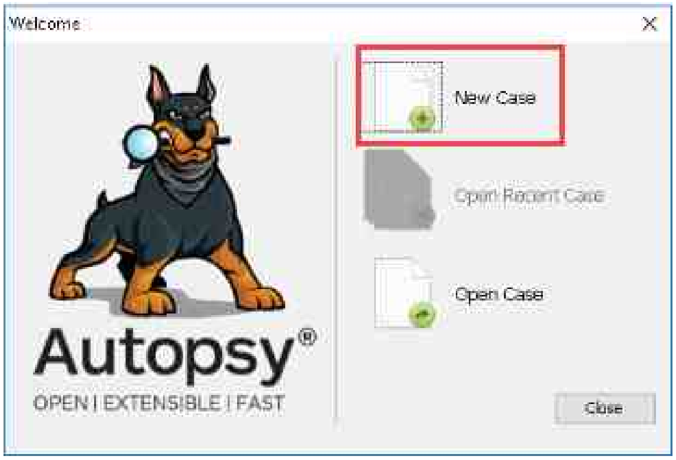


   b. Log in as `Administrator` using the password: `Train1ng$`

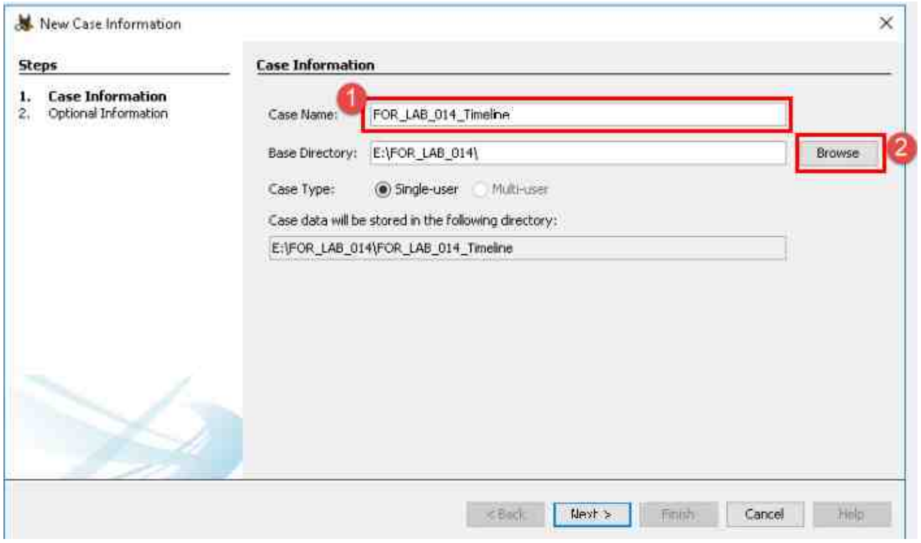
2. Launch the Autopsy program from the start menu by navigating to Start > Autopsy > Autopsy 4.15.0, as seen in items 1, 2, and 3 below. Alternatively, you can open Autopsy from the Desktop by clicking the Autopsy icon.



3. The Welcome screen will appear. Click New Case as highlighted below. This will open the New Case Information window.



4. In the New Case Information window, enter the name `FOR_LAB_014_Timeline` as the Case Name, as highlighted in item 1 below. Next, let’s change the Base Directory by clicking Browse as highlighted in item 2.



Case Name: FOR_LAB_014_Timeline

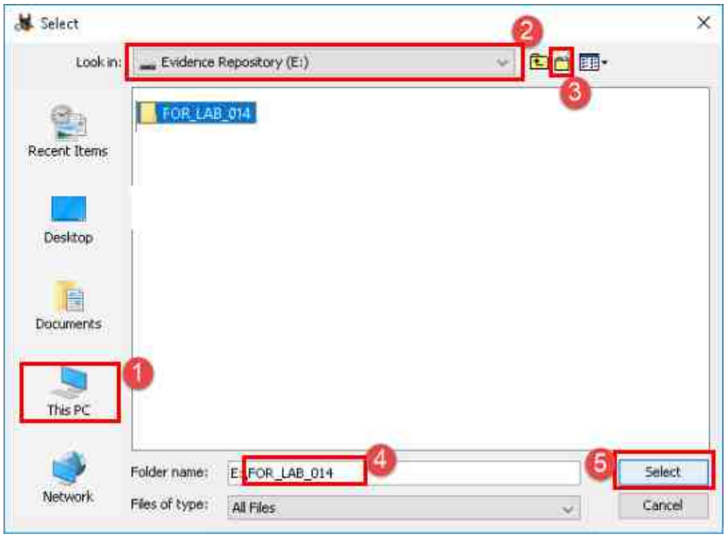
Base Directory: E:\FOR_LAB_014\

Case Type: ● Single-user ○ Multi-user

Case data will be stored in the following directory:

E:\FOR_LAB_014\FOR_LAB_014_Timeline

5. In the Select window, we can browse to the location where we want to create our case folder. Let’s do this by browsing to This PC > Evidence Repository (E:), as highlighted in items 1 and 2 below. Once there, create a new folder by clicking the Make New Folder button highlighted in item 3. Name this new folder `FOR_LAB_014` and then select it by clicking it once and then click the Select button as highlighted below. This will add the location to the Base Directory field in the New Case Information window.

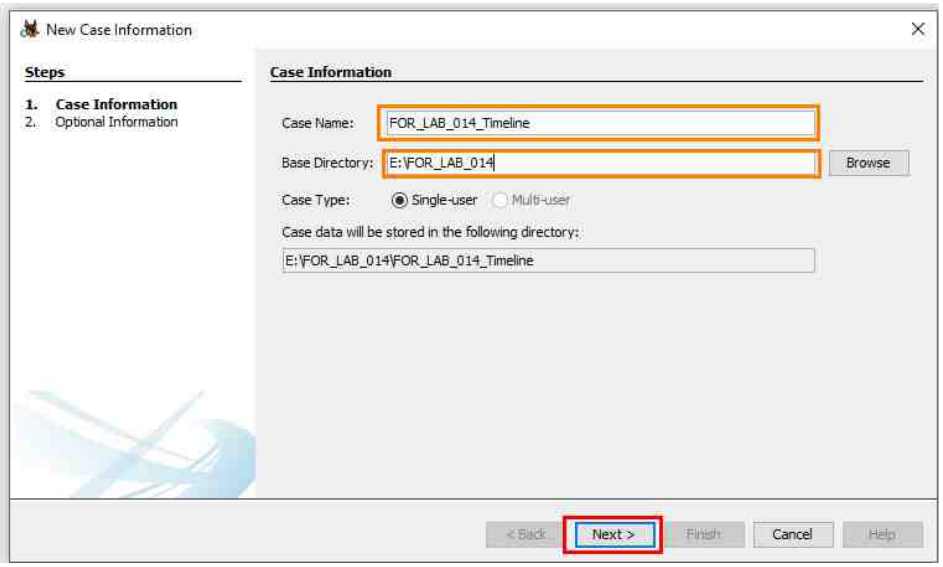


Look in: Evidence Repository (E:)

Folder name: E:\FOR_LAB_014

Files of type: All Files

6. Once you are back to the New Case Information window, verify that all the fields are correct and then click Next as highlighted below.



New Case Information

Steps
1. Case Information
2. Optional Information

Case Information

Case Name: FOR_LAB_014_Timeline

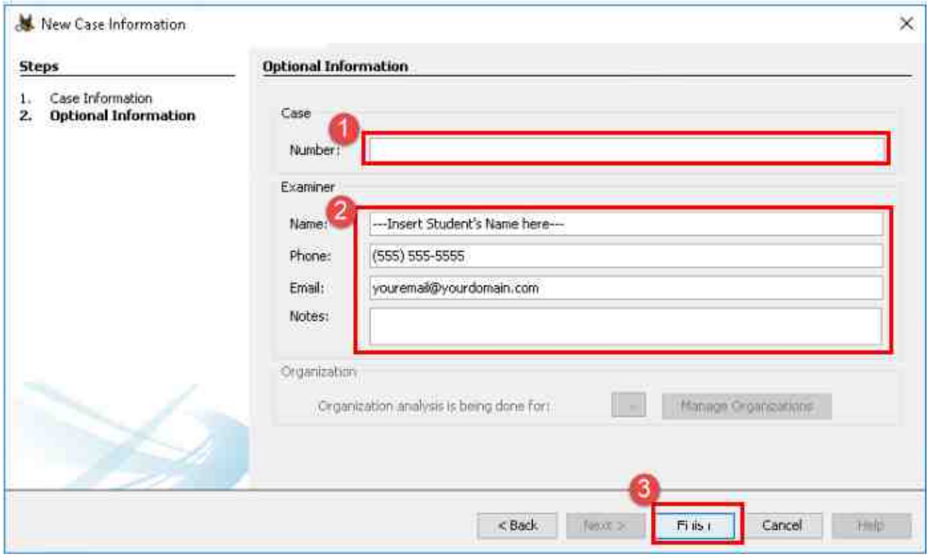
Base Directory: E:\FOR_LAB_014

Case Type: ● Single-user ○ Multi-user

Case data will be stored in the following directory:

E:\FOR_LAB_014\FOR_LAB_014_Timeline

7. The next window in the New Case wizard is the Optional Information window. Here you can type more information about the case and examiner. Fill out the information with your details as highlighted in items 1 and 2 below, and click Finish as highlighted at item 3.



New Case Information

Steps
1. Case Information
2. Optional Information

Optional Information

Case

Number:

Examiner

Name: ---Insert Student's Name here---

Phone: (555) 555-5555

Email: youremail@yourdomain.com

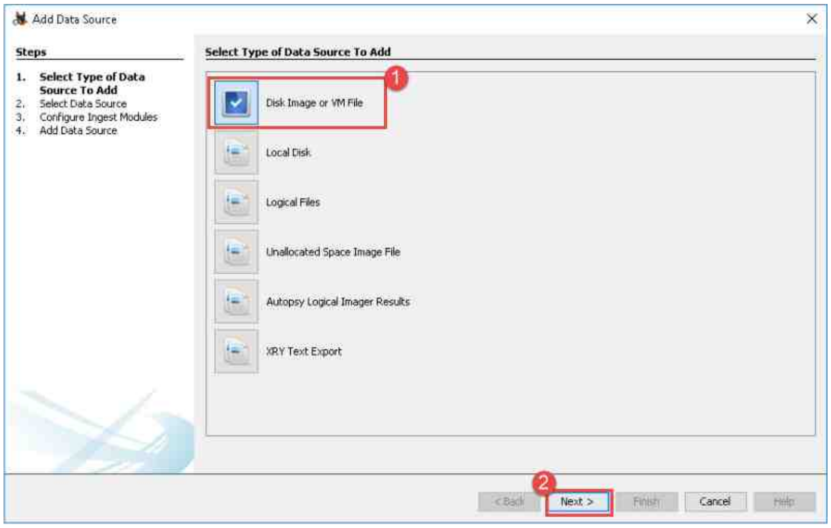
Notes:

Organization

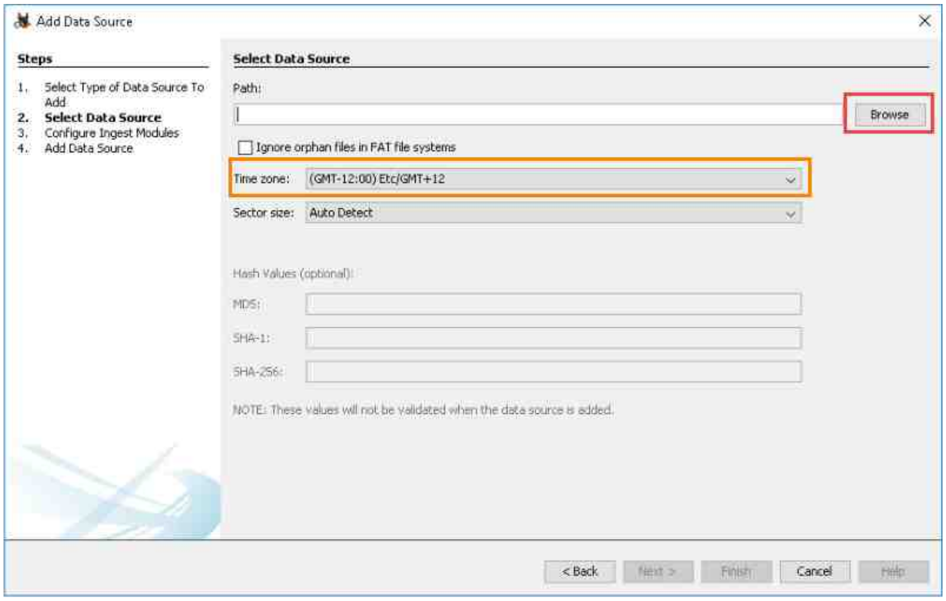
Organization analysis is being done for:

Even though this section is for optional information, case notes are always important.

8. You will now be taken to the Add Data Source window. Here you can choose between different evidence sources. In this exercise, we will be using an FEF so let's leave that as default and click Next as highlighted below.


Add Data Source
Steps
1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source
Select Type of Data Source To Add
1
Disk Image or VM File
Local Disk
Logical Files
Unallocated Space Image File
Autopsy Logical Imager Results
XRY Text Export
2
< Back
Next >
Finish
Cancel
Help

9. The next window will allow you to choose the image you want to add to the case. Click the Browse button highlighted below to open the Open window that allows you to browse for the FEF.



Path:

□ Ignore orphan files in FAT file systems

Time zone: (GMT-12:00) Etc/GMT+12

Sector size: Auto Detect

Hash Values (optional):

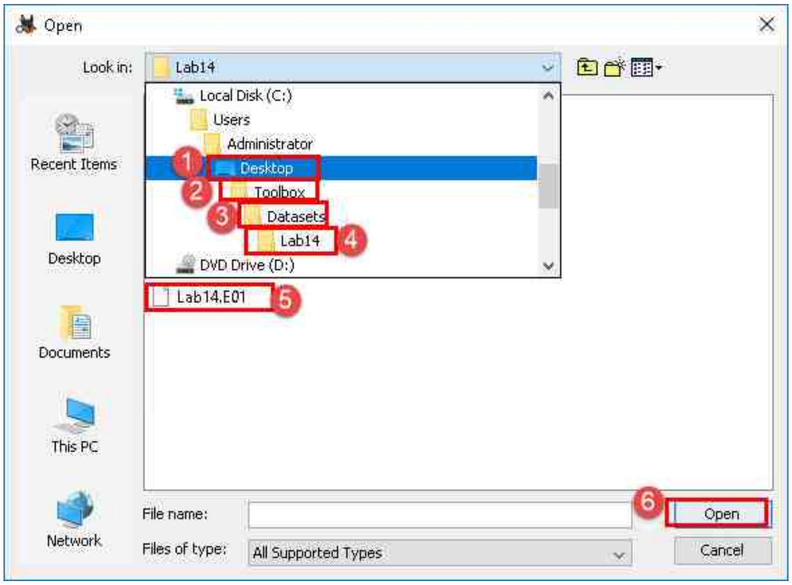
MD5:

SHA-1:

SHA-256:

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

10. In the Open window, browse to Desktop > Toolbox > Datasets > Lab 14 and click the file called Lab14.E01, as highlighted in items 1, 2, 3, 4, and 5, and then click Open as highlighted in item 6 below.



Open

Look in: Lab14

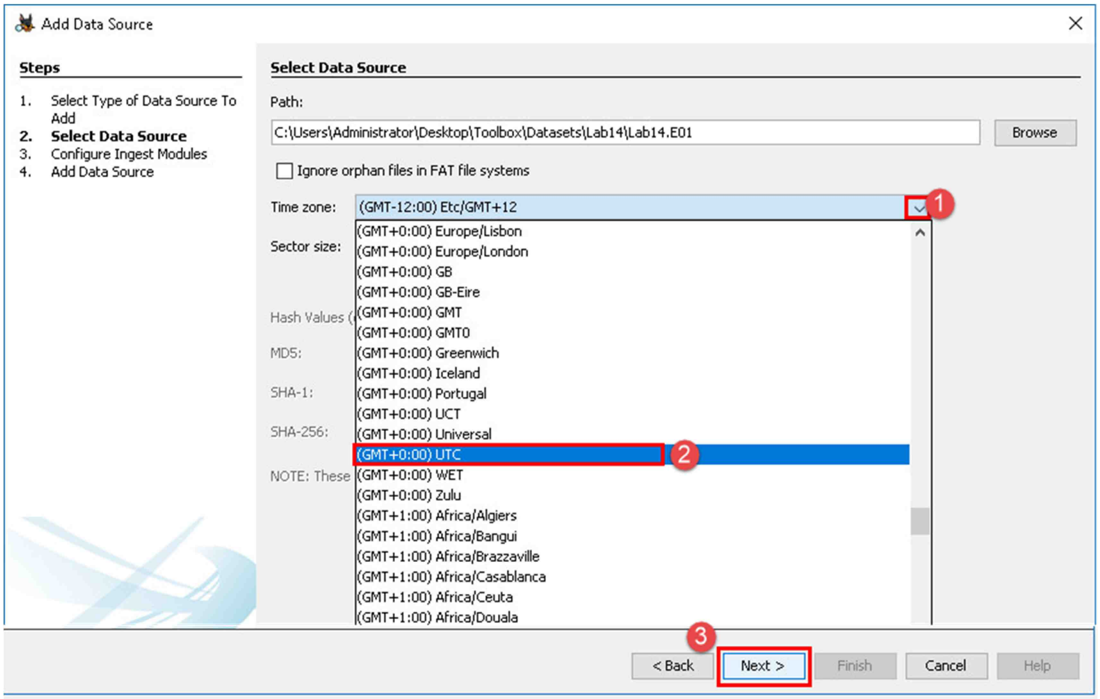
Local Disk (C:)
Users
Administrator
Desktop
Toolbox
Datasets
Lab14
DVD Drive (D:)

Lab14.E01

File name:

Files of type: All Supported Types

11. The image path will now appear in the Path field highlighted as item 1 below. Next, use the dropdown menu to select the (GMT+0) UTC time zone, as seen in item 2. We will leave the other options as is and click Next, as highlighted in item 3 below.



Add Data Source

Steps

1. Select Type of Data Source To Add
2. **Select Data Source**
3. Configure Ingest Modules
4. Add Data Source

Select Data Source

Path:

C:\Users\Administrator\Desktop\Toolbox\Datasets\Lab14\Lab14.E01

☐ Ignore orphan files in FAT file systems

Time zone: (GMT-12:00) Etc/GMT+12

(GMT+0:00) Europe/Lisbon
(GMT+0:00) Europe/London
(GMT+0:00) GB
(GMT+0:00) GB-Eire
(GMT+0:00) GMT
(GMT+0:00) GMT0
(GMT+0:00) Greenwich
(GMT+0:00) Iceland
(GMT+0:00) Portugal
(GMT+0:00) UCT
(GMT+0:00) Universal
(GMT+0:00) UTC
(GMT+0:00) WET
(GMT+0:00) Zulu
(GMT+1:00) Africa/Algiers
(GMT+1:00) Africa/Bangui
(GMT+1:00) Africa/Brazzaville
(GMT+1:00) Africa/Casablanca
(GMT+1:00) Africa/Ceuta
(GMT+1:00) Africa/Douala

Sector size:

Hash Values (

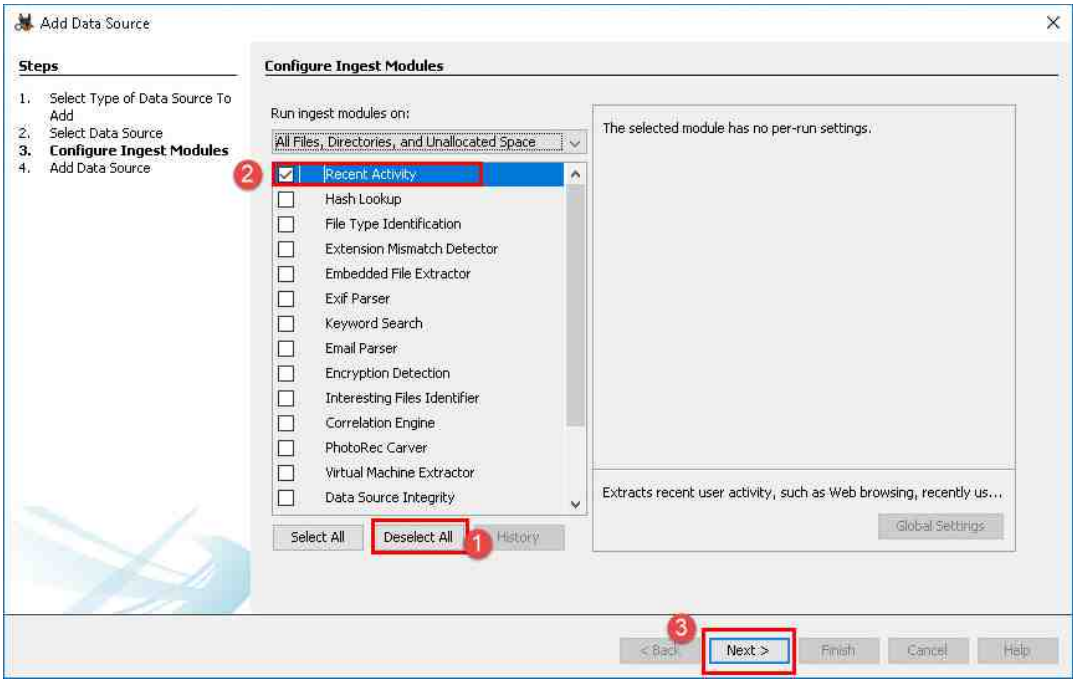
MD5:

SHA-1:

SHA-256:

NOTE: These

12. You will be taken to the Configure Ingest Modules step of the case creation process. We will be using the Recent Activity Ingest Module in this exercise, so uncheck any other selected Ingest Module by clicking the Deselect All button, then click the checkbox beside Recent Activity, and then click Next, as highlighted in items 1, 2, and 3 below.



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

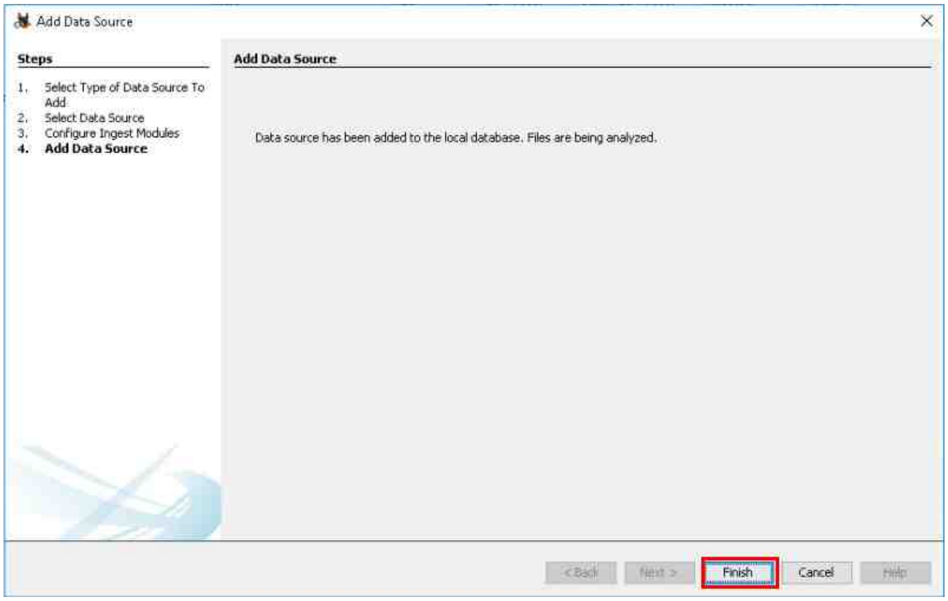
☑ Recent Activity
□ Hash Lookup
□ File Type Identification
□ Extension Mismatch Detector
□ Embedded File Extractor
□ Exif Parser
□ Keyword Search
□ Email Parser
□ Encryption Detection
□ Interesting Files Identifier
□ Correlation Engine
□ PhotoRec Carver
□ Virtual Machine Extractor
□ Data Source Integrity

The selected module has no per-run settings.

Extracts recent user activity, such as Web browsing, recently us...

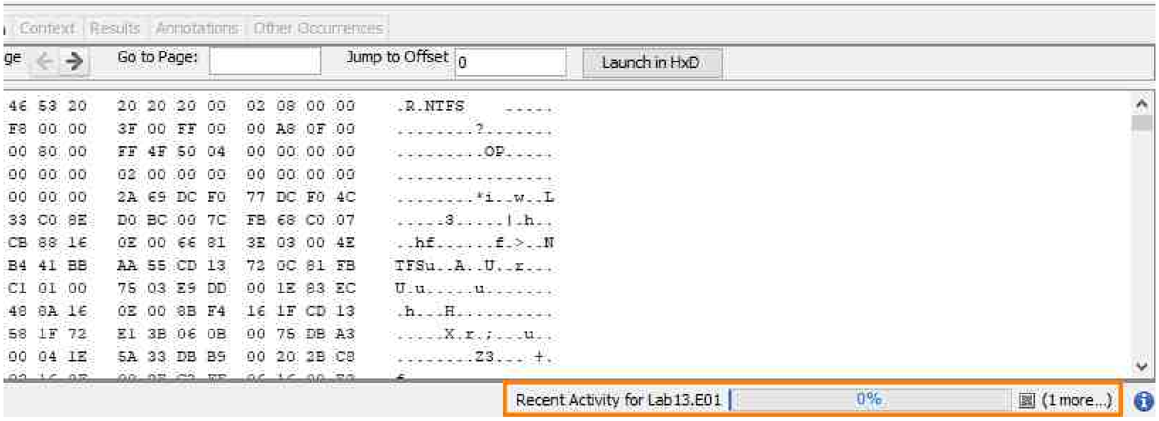
The Recent Activity Ingest Module is not mandatory for the timeline analysis. We are using it in this exercise to help populate the timeline.

13. You will be presented with the final screen, indicating that the files are being analyzed. Click Finish as highlighted below.



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

14. You will now be taken to the Autopsy main window. Before opening the timeline, ensure that the ingest module has finished running or the timeline will be incomplete. Pay attention to the status bar at the bottom right-hand corner of the window, as highlighted below. We can move on once the status bar completes and disappears.

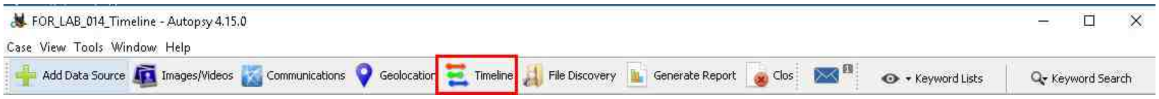


Jump to Offset 0

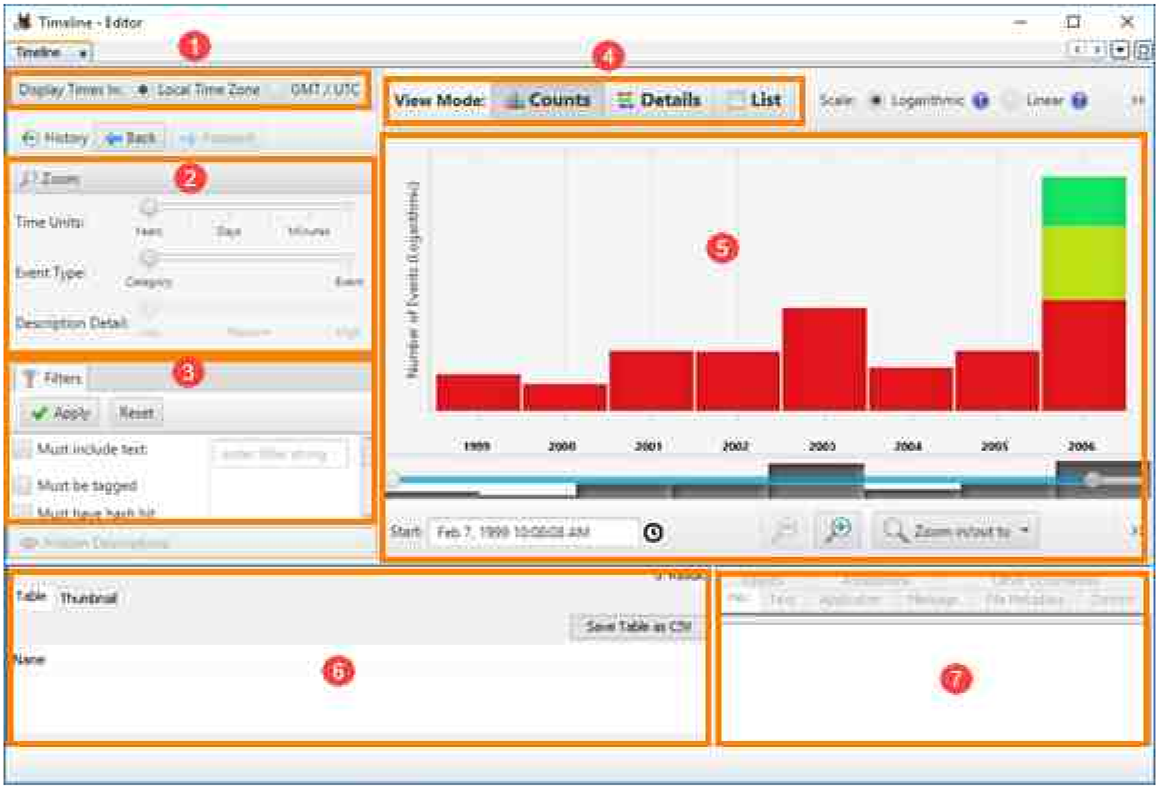
```
46 53 20   20 20 20 00   02 08 00 00   .R.NTFS    .....
F8 00 00   3F 00 FF 00   00 A8 0F 00   .........?.......
00 80 00   FF 4F 50 04   00 00 00 00   ..........OP.....
00 00 00   02 00 00 00   00 00 00 00   .................
00 00 00   2A 69 DC F0   77 DC F0 4C   .........*i..w..L
33 C0 8E   D0 BC 00 7C   FB 68 C0 07   .....3.....|.h..
CB 88 16   0E 00 66 81   3E 03 00 4E   ..hf.......f.>..N
B4 41 BB   AA 55 CD 13   72 0C 81 FB   TFSu..A..U..r...
C1 01 00   75 03 E9 DD   00 1E 83 EC   U.u......u.......
48 8A 16   0E 00 8B F4   16 1F CD 13   .h...H..........
58 1F 72   E1 3B 06 0B   00 75 DB A3   ......X.r.;...u..
00 04 1E   5A 33 DB B9   00 20 2B C8   .........Z3... +.
```

Recent Activity for Lab13.E01 0% (1 more...)

15. Once the ingesting is done, open the timeline feature by clicking the Timeline icon from the toolbar as highlighted below.



16. When the timeline opens, you will see the interface below. This is what the timeline view looks like. It seems complicated at first, but it is actually easy to use. The table below the screenshot will outline some of the features we will be using in this lab.


Timeline - Editor
Timeline
1
Display Times In: ● Local Time Zone ○ GMT / UTC
4
View Mode: Counts Details List
Scale: ● Logarithmic ○ Linear
History Back Forward
2
Zoom
Time Units: Years Days Minutes
Event Type: Category Event
Description Detail: Low Medium High
5
Number of Events (Logarithmic)
1999 2000 2001 2002 2003 2004 2005 2006
3
Filters
Apply Reset
Must include text:
Must be tagged
Must have hash hit
Hidden Descriptions
Start: Feb 7, 1999 10:00:00 AM
Zoom in/out to
Table Thumbnail
Save Table as CSV
Name
6
7

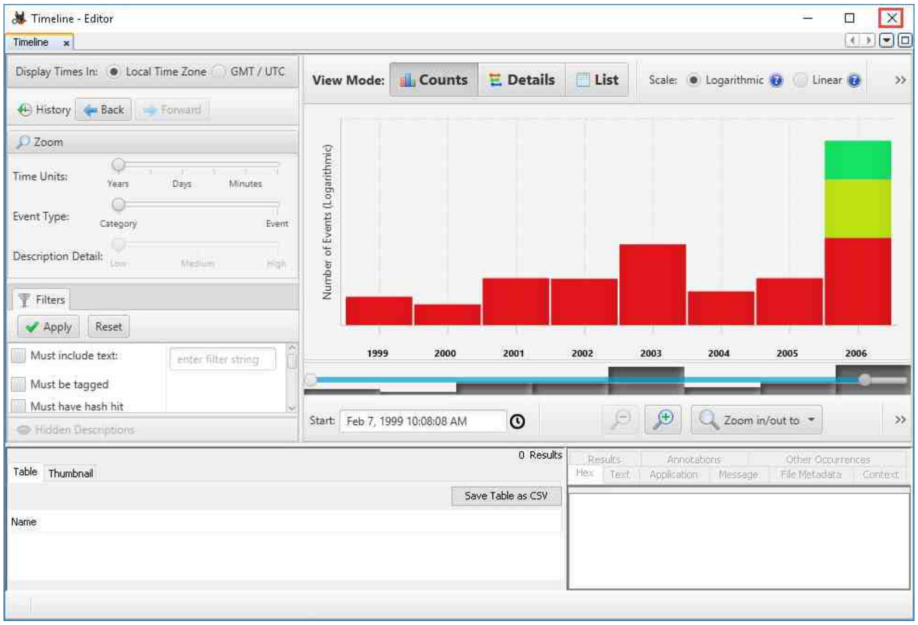
1	Display Time	This contains options that allow you to switch between the local time zone or UTC.
2	Zoom	This provides controls that allow you to narrow or widen the amount of data shown in the view area. This data can be sorted by time, date, category, event, and description.
3	Filters	This contains a wide variety of categories to sort and filter data. Filters are enabled by selecting the checkboxes beside the intended option.
4	View Mode	This allows you to change the way the data in the *Data View* area is represented. You can choose between Bar Chart, Detailed Timeline, or File List.
5	Data View	This displays the data in chronological order.
6	Table/Thumbnail View	This allows you to view any data selected from the *Data View* area in a list or thumbnail format.
7	Data Interpreter	This shows the contents of specific files selected in the *Table/Thumbnail* pane.

2 Reviewing the Timeline to Find Evidence

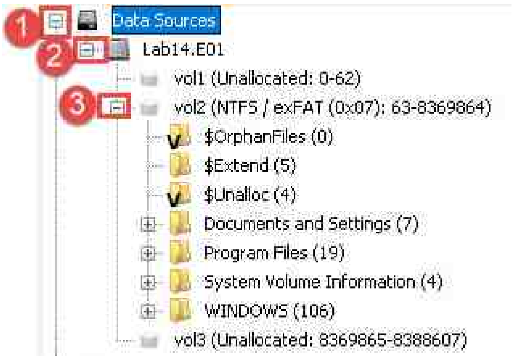
1. Now that you are familiar with the interface, we will take a look at the different ways we can review and identify data of evidentiary value using timeline analysis. In this specific exercise, we will use a simple scenario:

   The user of the computer was accused of downloading illegal pictures of cartoon characters. When questioned, they stated that they did not know how the pictures got there. Let us look at the evidence to see if we can determine how the pictures ended up on the device.

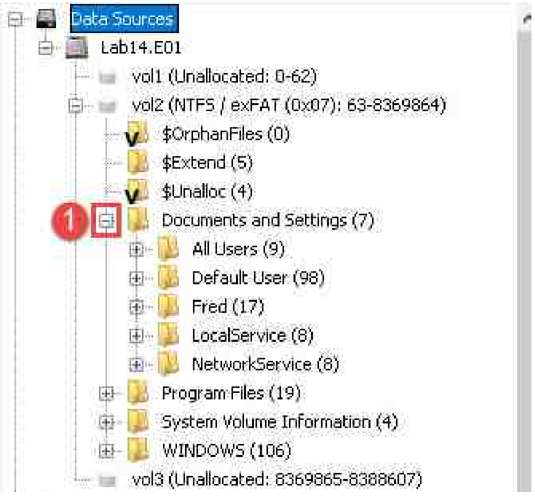
2. Let us begin by looking at the pictures in the My Pictures folder. Let's start by closing the Timeline window by clicking the X at the top-right corner of the window, as seen below.



3. Now let's first take a look at the name of the Users folder so that we can learn the operating system age and the path to the My Pictures folder. As seen in items 1, 2, and 3 below, begin by clicking the + beside the following folders to get to the root of the main drive: Data Sources > Lab14.E01 > vol2.

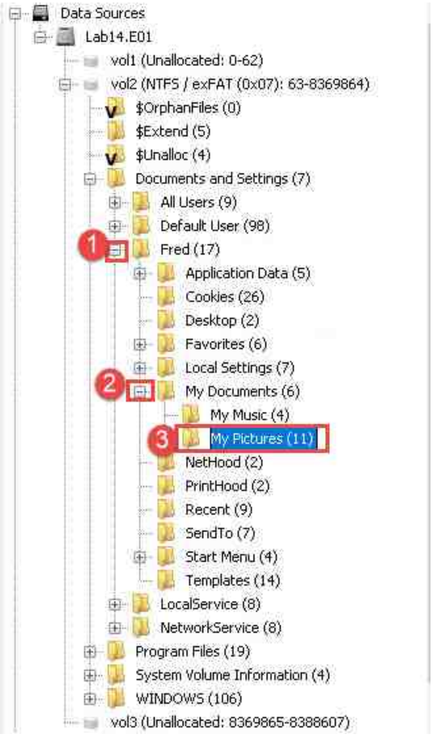

1
2
3
Data Sources
Lab14.E01
vol1 (Unallocated: 0-62)
vol2 (NTFS / exFAT (0x07): 63-8369864)
$OrphanFiles (0)
$Extend (5)
$Unalloc (4)
Documents and Settings (7)
Program Files (19)
System Volume Information (4)
WINDOWS (106)
vol3 (Unallocated: 8369865-8388607)

4. We are now in the root directory or the C:\ folder. As you can see, there is no folder called Users, but one called Documents and Settings. This means the operating system is Microsoft Windows XP or older. It also means the My Pictures folder is found in the My Documents folder. In newer operating systems, the My Pictures and My Videos folders are renamed to Pictures and Videos and are located within the root of each user's folder. Let's expand the Documents and Settings folder by clicking the + beside it, as seen in item 1 below.



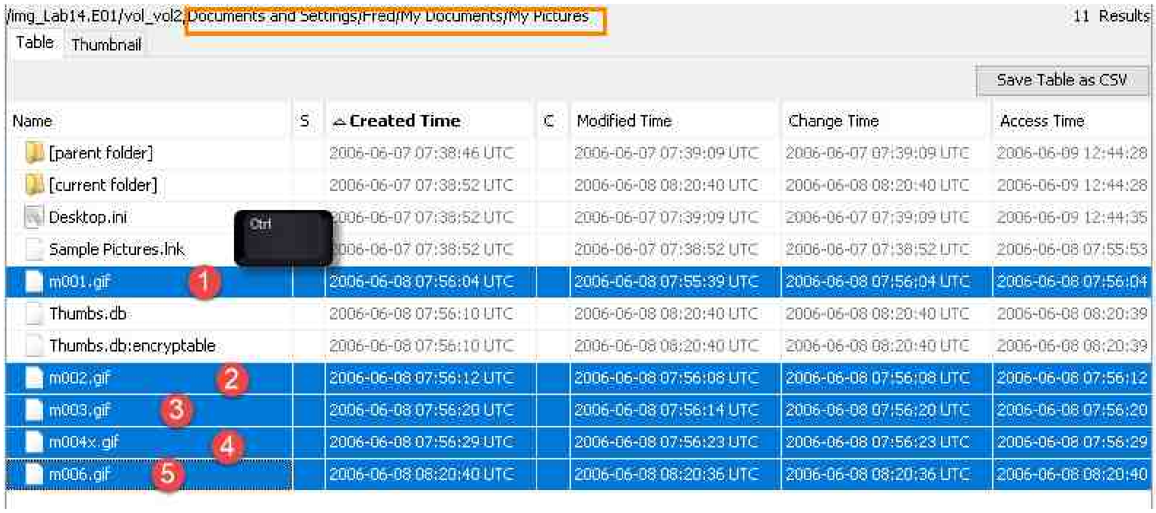
Data Sources
Lab14.E01
vol1 (Unallocated: 0-62)
vol2 (NTFS / exFAT (0x07): 63-8369864)
$OrphanFiles (0)
$Extend (5)
$Unalloc (4)
Documents and Settings (7)
All Users (9)
Default User (98)
Fred (17)
LocalService (8)
NetworkService (8)
Program Files (19)
System Volume Information (4)
WINDOWS (106)
vol3 (Unallocated: 8369865-8388607)

5. Now that you can see the current user folders, you can assume that only the user folder called Fred is a user-created folder based on the names of each. This is not a rule, however, and should be confirmed by reviewing the registry files to learn the RIDs and review their activity. It is also a good idea to review those folders for content, unless you are sure you don't need to. Since we will be using the Fred account, let's navigate to My Pictures by clicking the + sign beside the following folders, as seen in items 1, 2, and 3 below: Fred > My Documents > My Pictures.



```
Data Sources
  Lab14.E01
    vol1 (Unallocated: 0-62)
    vol2 (NTFS / exFAT (0x07): 63-8369864)
      $OrphanFiles (0)
      $Extend (5)
      $Unalloc (4)
      Documents and Settings (7)
        All Users (9)
        Default User (98)
        Fred (17)
          Application Data (5)
          Cookies (26)
          Desktop (2)
          Favorites (6)
          Local Settings (7)
          My Documents (6)
            My Music (4)
            My Pictures (11)
          NetHood (2)
          PrintHood (2)
          Recent (9)
          SendTo (7)
          Start Menu (4)
          Templates (14)
        LocalService (8)
        NetworkService (8)
      Program Files (19)
      System Volume Information (4)
      WINDOWS (106)
    vol3 (Unallocated: 8369865-8388607)
```

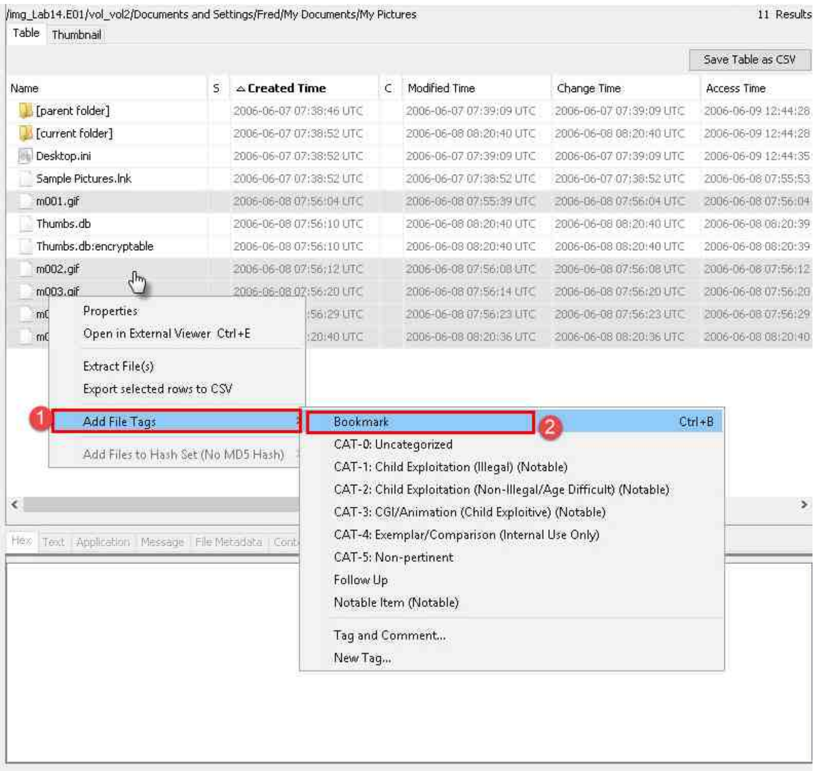
6. There are 5 GIF picture files inside the My Pictures folder, as highlighted below. Let's review each one to see their content by clicking them. Select them all by holding Ctrl + clicking on each file, as seen in items 1, 2, 3, 4, and 5 below.



/img_Lab14.E01/vol_vol2/Documents and Settings/Fred/My Documents/My Pictures   11 Results

Name	S	Created Time	C	Modified Time	Change Time	Access Time
[parent folder]		2006-06-07 07:38:46 UTC		2006-06-07 07:39:09 UTC	2006-06-07 07:39:09 UTC	2006-06-09 12:44:28
[current folder]		2006-06-07 07:38:52 UTC		2006-06-08 08:20:40 UTC	2006-06-08 08:20:40 UTC	2006-06-09 12:44:28
Desktop.ini		2006-06-07 07:38:52 UTC		2006-06-07 07:39:09 UTC	2006-06-07 07:39:09 UTC	2006-06-09 12:44:35
Sample Pictures.lnk		006-06-07 07:38:52 UTC		2006-06-07 07:38:52 UTC	2006-06-07 07:38:52 UTC	2006-06-08 07:55:53
m001.gif		2006-06-08 07:56:04 UTC		2006-06-08 07:55:39 UTC	2006-06-08 07:56:04 UTC	2006-06-08 07:56:04
Thumbs.db		2006-06-08 07:56:10 UTC		2006-06-08 08:20:40 UTC	2006-06-08 08:20:40 UTC	2006-06-08 08:20:39
Thumbs.db:encryptable		2006-06-08 07:56:10 UTC		2006-06-08 08:20:40 UTC	2006-06-08 08:20:40 UTC	2006-06-08 08:20:39
m002.gif		2006-06-08 07:56:12 UTC		2006-06-08 07:56:08 UTC	2006-06-08 07:56:08 UTC	2006-06-08 07:56:12
m003.gif		2006-06-08 07:56:20 UTC		2006-06-08 07:56:14 UTC	2006-06-08 07:56:20 UTC	2006-06-08 07:56:20
m004x.gif		2006-06-08 07:56:29 UTC		2006-06-08 07:56:23 UTC	2006-06-08 07:56:23 UTC	2006-06-08 07:56:29
m006.gif		2006-06-08 08:20:40 UTC		2006-06-08 08:20:36 UTC	2006-06-08 08:20:36 UTC	2006-06-08 08:20:40

7. There is not much we can learn by looking at the content of the pictures. We will be better able to determine their source by reviewing the metadata associated with them. Let’s tag these files so we can retain their information for reference. Note the dates and times that the files were created, accessed, and modified, as these will help us learn more about them. To tag the files, right-click on the highlighted area and navigate to Add File Tags > Bookmark on the context menu that appears, as seen in items 1 and 2 below.

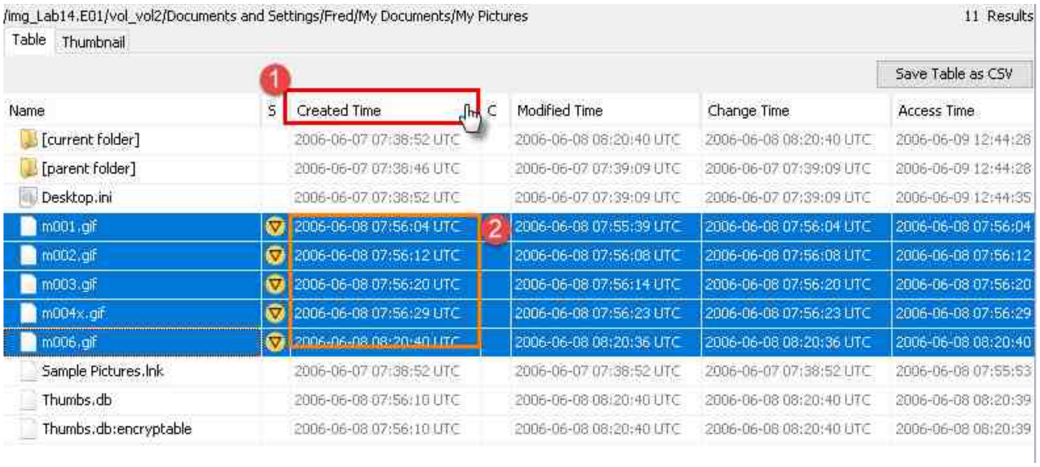


/img_Lab14.E01/vol_vol2/Documents and Settings/Fred/My Documents/My Pictures 11 Results

Name	S	Created Time	C	Modified Time	Change Time	Access Time
[parent folder]		2006-06-07 07:38:46 UTC		2006-06-07 07:39:09 UTC	2006-06-07 07:39:09 UTC	2006-06-09 12:44:28
[current folder]		2006-06-07 07:38:52 UTC		2006-06-08 08:20:40 UTC	2006-06-08 08:20:40 UTC	2006-06-09 12:44:28
Desktop.ini		2006-06-07 07:38:52 UTC		2006-06-07 07:39:09 UTC	2006-06-07 07:39:09 UTC	2006-06-09 12:44:35
Sample Pictures.lnk		2006-06-07 07:38:52 UTC		2006-06-07 07:38:52 UTC	2006-06-07 07:38:52 UTC	2006-06-08 07:55:53
m001.gif		2006-06-08 07:56:04 UTC		2006-06-08 07:55:39 UTC	2006-06-08 07:56:04 UTC	2006-06-08 07:56:04
Thumbs.db		2006-06-08 07:56:10 UTC		2006-06-08 08:20:40 UTC	2006-06-08 08:20:40 UTC	2006-06-08 08:20:39
Thumbs.db:encryptable		2006-06-08 07:56:10 UTC		2006-06-08 08:20:40 UTC	2006-06-08 08:20:40 UTC	2006-06-08 08:20:39
m002.gif		2006-06-08 07:56:12 UTC		2006-06-08 07:56:08 UTC	2006-06-08 07:56:08 UTC	2006-06-08 07:56:12
m003.gif		2006-06-08 07:56:20 UTC		2006-06-08 07:56:14 UTC	2006-06-08 07:56:20 UTC	2006-06-08 07:56:20
m0		:56:29 UTC		2006-06-08 07:56:23 UTC	2006-06-08 07:56:23 UTC	2006-06-08 07:56:29
m0		:20:40 UTC		2006-06-08 08:20:36 UTC	2006-06-08 08:20:36 UTC	2006-06-08 08:20:40

Table
Thumbnail
Save Table as CSV
Properties
Open in External Viewer Ctrl+E
Extract File(s)
Export selected rows to CSV
1
Add File Tags
Add Files to Hash Set (No MD5 Hash)
Bookmark Ctrl+B
2
CAT-0: Uncategorized
CAT-1: Child Exploitation (Illegal) (Notable)
CAT-2: Child Exploitation (Non-Illegal/Age Difficult) (Notable)
CAT-3: CGI/Animation (Child Exploitive) (Notable)
CAT-4: Exemplar/Comparison (Internal Use Only)
CAT-5: Non-pertinent
Follow Up
Notable Item (Notable)
Tag and Comment...
New Tag...
Hex
Text
Application
Message
File Metadata
Cont

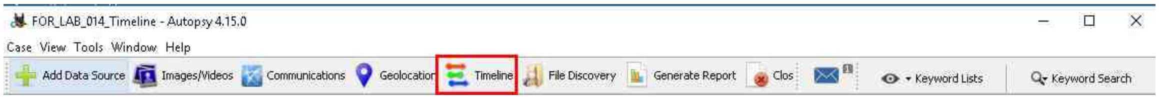
8. Now let’s sort the file by created time to learn the time that each file was placed on the drive. To sort by created time, click the column heading Created Time as highlighted in item 1 below. As you can see, when the column is sorted, it shows that the files were created between 07:56:04 and 08:20:40 on 2006-06-08. This shows that the files were created within half an hour of each other, as seen in item 2. Note these dates and times.



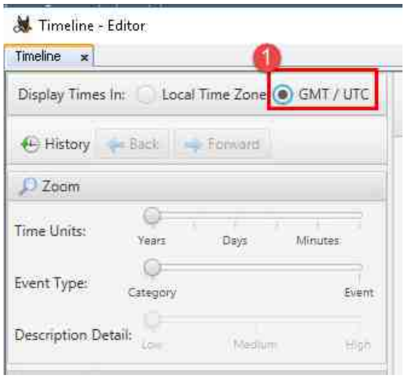
/img_Lab14.E01/vol_vol2/Documents and Settings/Fred/My Documents/My Pictures — 11 Results

Name	S	Created Time	C	Modified Time	Change Time	Access Time
[current folder]		2006-06-07 07:38:52 UTC		2006-06-08 08:20:40 UTC	2006-06-08 08:20:40 UTC	2006-06-09 12:44:28
[parent folder]		2006-06-07 07:38:46 UTC		2006-06-07 07:39:09 UTC	2006-06-07 07:39:09 UTC	2006-06-09 12:44:28
Desktop.ini		2006-06-07 07:38:52 UTC		2006-06-07 07:39:09 UTC	2006-06-07 07:39:09 UTC	2006-06-09 12:44:35
m001.gif	▽	2006-06-08 07:56:04 UTC		2006-06-08 07:55:39 UTC	2006-06-08 07:56:04 UTC	2006-06-08 07:56:04
m002.gif	▽	2006-06-08 07:56:12 UTC		2006-06-08 07:56:08 UTC	2006-06-08 07:56:08 UTC	2006-06-08 07:56:12
m003.gif	▽	2006-06-08 07:56:20 UTC		2006-06-08 07:56:14 UTC	2006-06-08 07:56:20 UTC	2006-06-08 07:56:20
m004x.gif	▽	2006-06-08 07:56:29 UTC		2006-06-08 07:56:23 UTC	2006-06-08 07:56:23 UTC	2006-06-08 07:56:29
m006.gif	▽	2006-06-08 08:20:40 UTC		2006-06-08 08:20:36 UTC	2006-06-08 08:20:36 UTC	2006-06-08 08:20:40
Sample Pictures.lnk		2006-06-07 07:38:52 UTC		2006-06-07 07:38:52 UTC	2006-06-07 07:38:52 UTC	2006-06-08 07:55:53
Thumbs.db		2006-06-08 07:56:10 UTC		2006-06-08 08:20:40 UTC	2006-06-08 08:20:40 UTC	2006-06-08 08:20:39
Thumbs.db:encryptable		2006-06-08 07:56:10 UTC		2006-06-08 08:20:40 UTC	2006-06-08 08:20:40 UTC	2006-06-08 08:20:39

9. Now that we have some dates of interest, let us look at what occurred between this time on the timeline. To do this, reopen the timeline by clicking the Timeline icon from the toolbar as highlighted below.

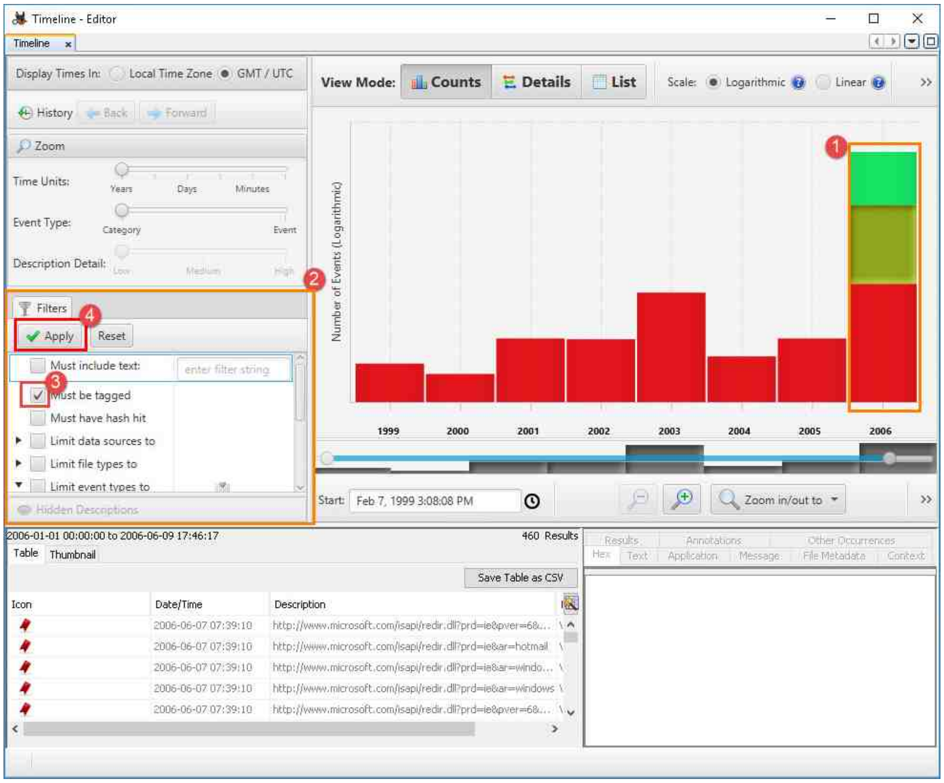


10. Now that the timeline is open, switch to the GMT/UTC time zone so that you will have the same time as we do. Do this by clicking the radio button beside GMT/UTC in the Display Times In field.



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

11. There are many ways we can approach the sorting of the data to view the dates in question. We can click the bar that is closest to our date of interest, we can change the view mode, or we can type the dates of interest in the Start and End fields. Let's use the bar graphs. The bar highlighted in item 1 labeled 2006 is split into 3 different colors. The legend in the Filters pane highlighted as item 2 below can let you know what type of data is in each colored block. Let's see which one of the bars contains our tagged items. To filter the data by tagged items, click the checkbox beside Must be tagged, as seen in item 3, and select Apply as seen in item 4.



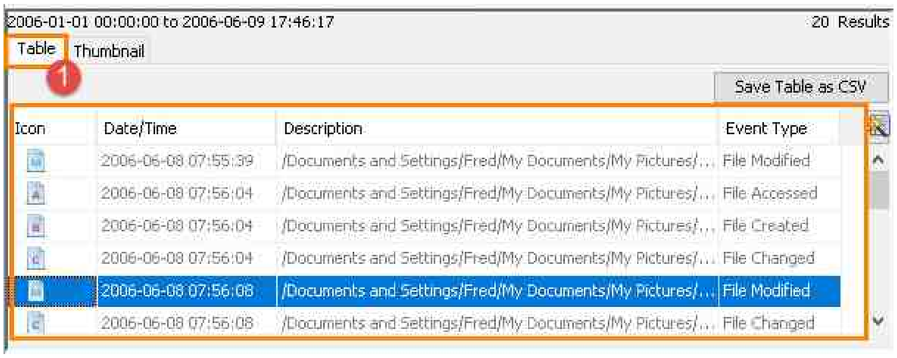
2006-01-01 00:00:00 to 2006-06-09 17:46:17 460 Results

Table | Thumbnail

Save Table as CSV

Icon	Date/Time	Description
	2006-06-07 07:39:10	http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&...
	2006-06-07 07:39:10	http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=hotmail
	2006-06-07 07:39:10	http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=windo...
	2006-06-07 07:39:10	http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=windows
	2006-06-07 07:39:10	http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&...

12. Now that you have filtered the data, you can click on the bar to see the tagged files in the Table/Thumbnail pane highlighted in item 1 below. Each entry in the table represents a different type of metadata, so this means the same file may be listed multiple times in the table with different Event Types.



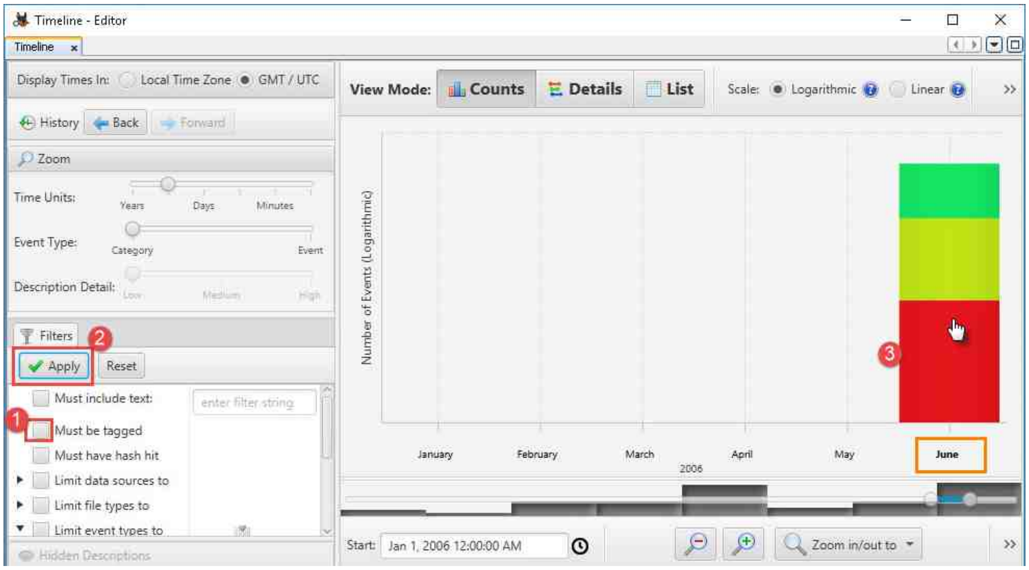
2006-01-01 00:00:00 to 2006-06-09 17:46:17 20 Results

Table | Thumbnail

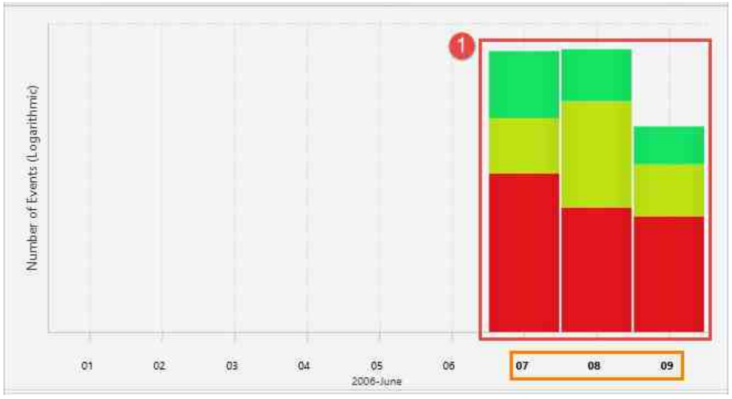
Save Table as CSV

Icon	Date/Time	Description	Event Type
	2006-06-08 07:55:39	/Documents and Settings/Fred/My Documents/My Pictures/...	File Modified
	2006-06-08 07:56:04	/Documents and Settings/Fred/My Documents/My Pictures/...	File Accessed
	2006-06-08 07:56:04	/Documents and Settings/Fred/My Documents/My Pictures/...	File Created
	2006-06-08 07:56:04	/Documents and Settings/Fred/My Documents/My Pictures/...	File Changed
	2006-06-08 07:56:08	/Documents and Settings/Fred/My Documents/My Pictures/...	File Modified
	2006-06-08 07:56:08	/Documents and Settings/Fred/My Documents/My Pictures/...	File Changed

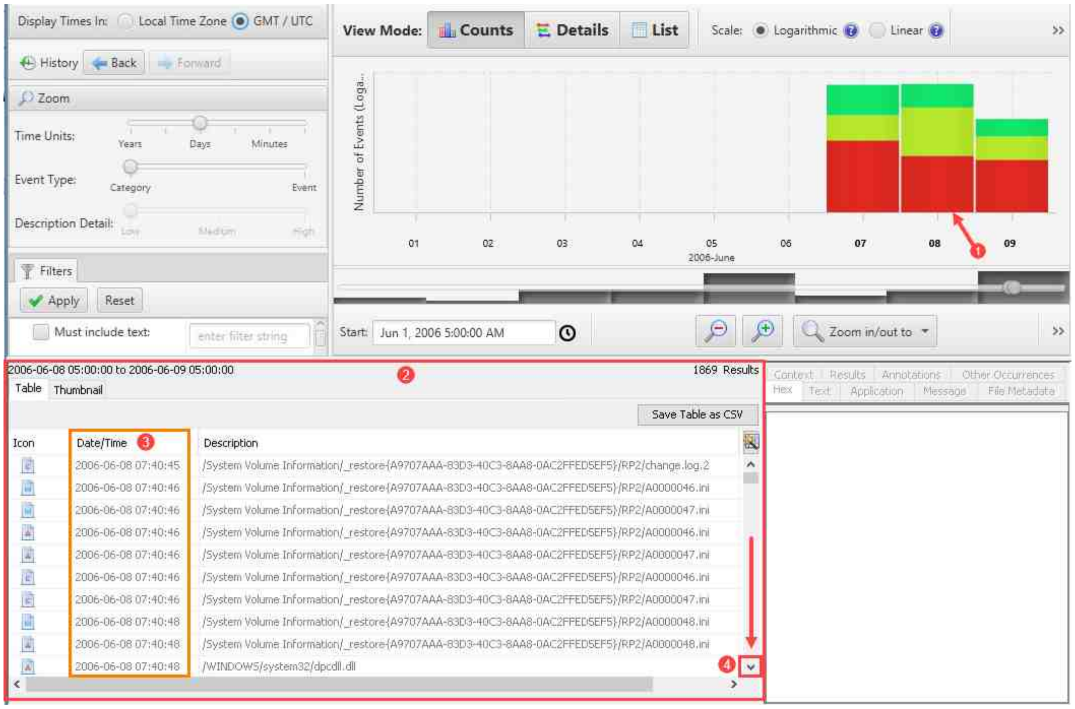
13. Now that we are sure our tagged items are in the 2006 bar, let’s uncheck the Must be tagged filter, as seen in item 1, and select Apply as seen in item 2. Now let us drill down a bit to get closer to the data we want. Do this by double-clicking the bar called 2006 to expand it and reveal the months, as seen in item 3 below.



14. Once there, double-click the month of interest, June, to reveal the dates of interest, as seen in item 1 below.



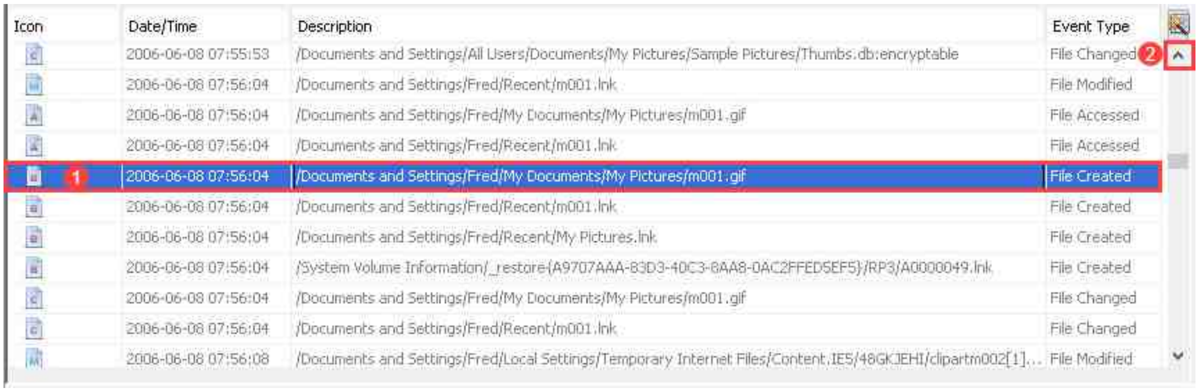
15. You will now see each date in the month and can determine the usage of the device by looking at the amount of data created, accessed, and modified on the different dates. You can dig deeper if you would like to but for now, let us click on the bottom segment of the bar called 08 as seen in item 1 below. The 08 represents the date we are interested in. This will reveal all the file system activity for 2006-06-08. This can be seen in the Table/Thumbnail view in the bottom-left corner, as highlighted in item 2 below. As you can see in item 3, the date and time that each timestamp was updated is in chronological order from oldest to newest. Since the first file was created at 7:56:04 let's look for that date first and then backtrack. Scroll down until you see 7:56:04 by clicking the arrow or dragging the scroll bar as seen in item 4 below.



2006-06-08 05:00:00 to 2006-06-09 05:00:00 1869 Results

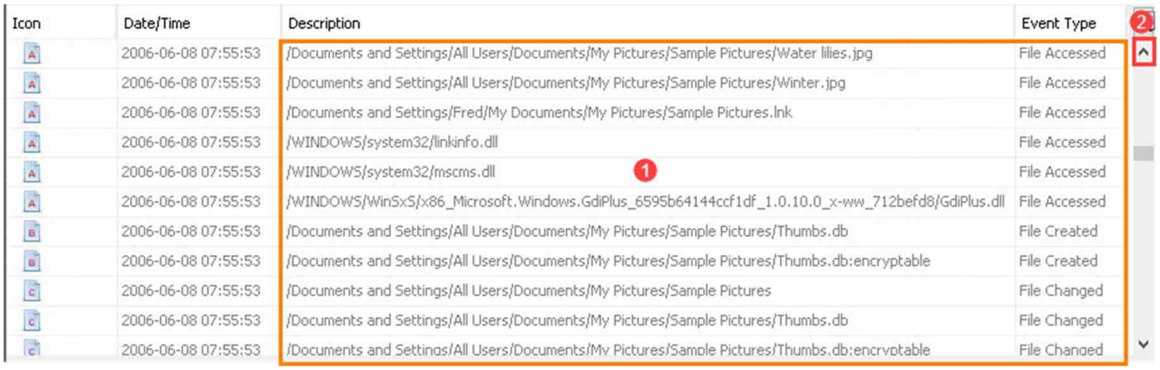
Icon	Date/Time	Description
	2006-06-08 07:40:45	/System Volume Information/_restore{A9707AAA-83D3-40C3-8AA8-0AC2FFED5EF5}/RP2/change.log.2
	2006-06-08 07:40:46	/System Volume Information/_restore{A9707AAA-83D3-40C3-8AA8-0AC2FFED5EF5}/RP2/A0000046.ini
	2006-06-08 07:40:46	/System Volume Information/_restore{A9707AAA-83D3-40C3-8AA8-0AC2FFED5EF5}/RP2/A0000047.ini
	2006-06-08 07:40:46	/System Volume Information/_restore{A9707AAA-83D3-40C3-8AA8-0AC2FFED5EF5}/RP2/A0000046.ini
	2006-06-08 07:40:46	/System Volume Information/_restore{A9707AAA-83D3-40C3-8AA8-0AC2FFED5EF5}/RP2/A0000047.ini
	2006-06-08 07:40:46	/System Volume Information/_restore{A9707AAA-83D3-40C3-8AA8-0AC2FFED5EF5}/RP2/A0000046.ini
	2006-06-08 07:40:46	/System Volume Information/_restore{A9707AAA-83D3-40C3-8AA8-0AC2FFED5EF5}/RP2/A0000047.ini
	2006-06-08 07:40:48	/System Volume Information/_restore{A9707AAA-83D3-40C3-8AA8-0AC2FFED5EF5}/RP2/A0000048.ini
	2006-06-08 07:40:48	/System Volume Information/_restore{A9707AAA-83D3-40C3-8AA8-0AC2FFED5EF5}/RP2/A0000048.ini
	2006-06-08 07:40:48	/WINDOWS/system32/dpcdll.dll

16. As highlighted in item 1 below, we identified the first file called m001.gif. Now let's backtrack to see what happened before this file got created. Let's scroll up until we get to 07:55:53 by using the scroll bar, the mouse wheel, or by clicking the arrow as seen in item 2.



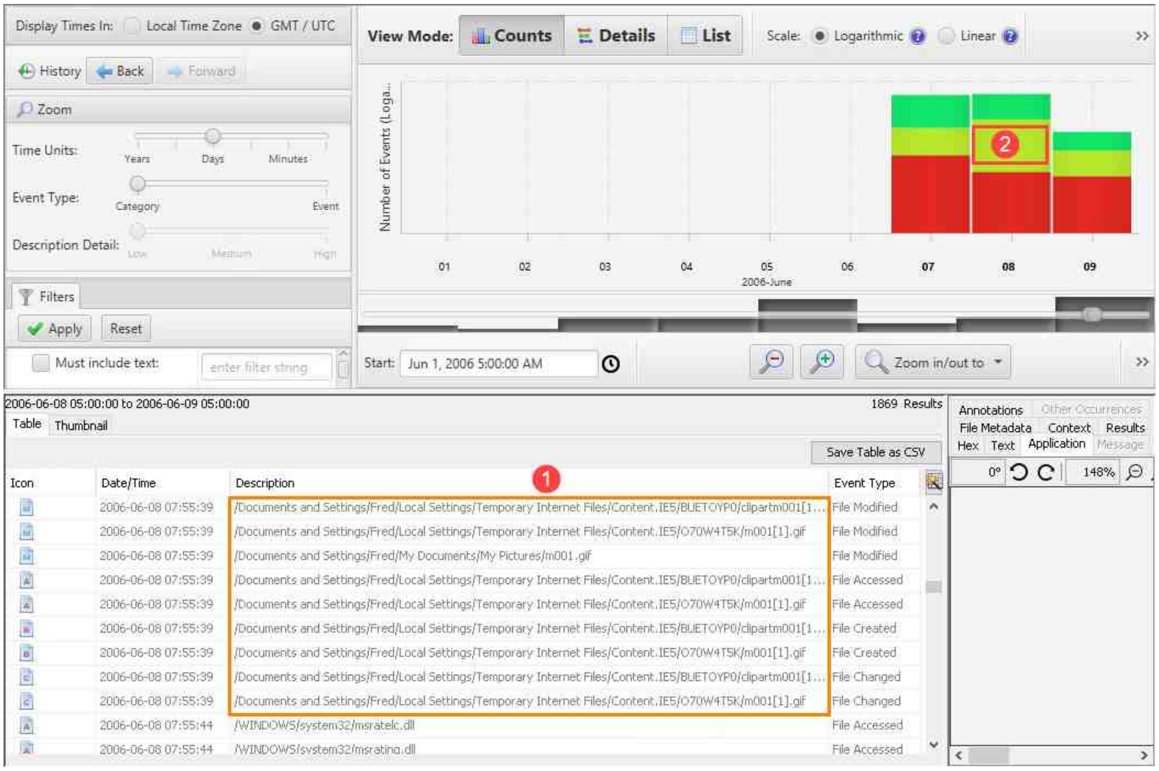
Icon	Date/Time	Description	Event Type
	2006-06-08 07:55:53	/Documents and Settings/All Users/Documents/My Pictures/Sample Pictures/Thumbs.db:encryptable	File Changed
	2006-06-08 07:56:04	/Documents and Settings/Fred/Recent/m001.lnk	File Modified
	2006-06-08 07:56:04	/Documents and Settings/Fred/My Documents/My Pictures/m001.gif	File Accessed
	2006-06-08 07:56:04	/Documents and Settings/Fred/Recent/m001.lnk	File Accessed
	2006-06-08 07:56:04	/Documents and Settings/Fred/My Documents/My Pictures/m001.gif	File Created
	2006-06-08 07:56:04	/Documents and Settings/Fred/Recent/m001.lnk	File Created
	2006-06-08 07:56:04	/Documents and Settings/Fred/Recent/My Pictures.lnk	File Created
	2006-06-08 07:56:04	/System Volume Information/_restore{A9707AAA-83D3-40C3-8AA8-0AC2FFED5EF5}/RP3/A0000049.lnk	File Created
	2006-06-08 07:56:04	/Documents and Settings/Fred/My Documents/My Pictures/m001.gif	File Changed
	2006-06-08 07:56:04	/Documents and Settings/Fred/Recent/m001.lnk	File Changed
	2006-06-08 07:56:08	/Documents and Settings/Fred/Local Settings/Temporary Internet Files/Content.IE5/48GKJEHI/clipartm002[1]...	File Modified

17. As you can see, there are several other files that are being created, accessed and changed from the Windows directory and the My Pictures directory for the All Users user account, seen in item 1 below. This could be either user, system or software activity. Let's scroll up a little more once again until we get to 07:55:39.



Icon	Date/Time	Description	Event Type
A	2006-06-08 07:55:53	/Documents and Settings/All Users/Documents/My Pictures/Sample Pictures/Water lilies.jpg	File Accessed
A	2006-06-08 07:55:53	/Documents and Settings/All Users/Documents/My Pictures/Sample Pictures/Winter.jpg	File Accessed
A	2006-06-08 07:55:53	/Documents and Settings/Fred/My Documents/My Pictures/Sample Pictures.lnk	File Accessed
A	2006-06-08 07:55:53	/WINDOWS/system32/linkinfo.dll	File Accessed
A	2006-06-08 07:55:53	/WINDOWS/system32/mscms.dll	File Accessed
A	2006-06-08 07:55:53	/WINDOWS/WinSxS/x86_Microsoft.Windows.GdiPlus_6595b64144ccf1df_1.0.10.0_x-ww_712befd8/GdiPlus.dll	File Accessed
B	2006-06-08 07:55:53	/Documents and Settings/All Users/Documents/My Pictures/Sample Pictures/Thumbs.db	File Created
B	2006-06-08 07:55:53	/Documents and Settings/All Users/Documents/My Pictures/Sample Pictures/Thumbs.db:encryptable	File Created
C	2006-06-08 07:55:53	/Documents and Settings/All Users/Documents/My Pictures/Sample Pictures	File Changed
C	2006-06-08 07:55:53	/Documents and Settings/All Users/Documents/My Pictures/Sample Pictures/Thumbs.db	File Changed
C	2006-06-08 07:55:53	/Documents and Settings/All Users/Documents/My Pictures/Sample Pictures/Thumbs.db:encryptable	File Changed

18. The data here looks slightly different. As you can see in item 1 below, there are now files being created, accessed, and changed within a folder called Temporary Internet Files. This is a folder used to store cached files for Internet Explorer in older operating systems. This means that a web browser may have been open at the time. Let's check out the web history for that day. Do this by clicking the middle section of the bar called 08 as seen in item 2 below.



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

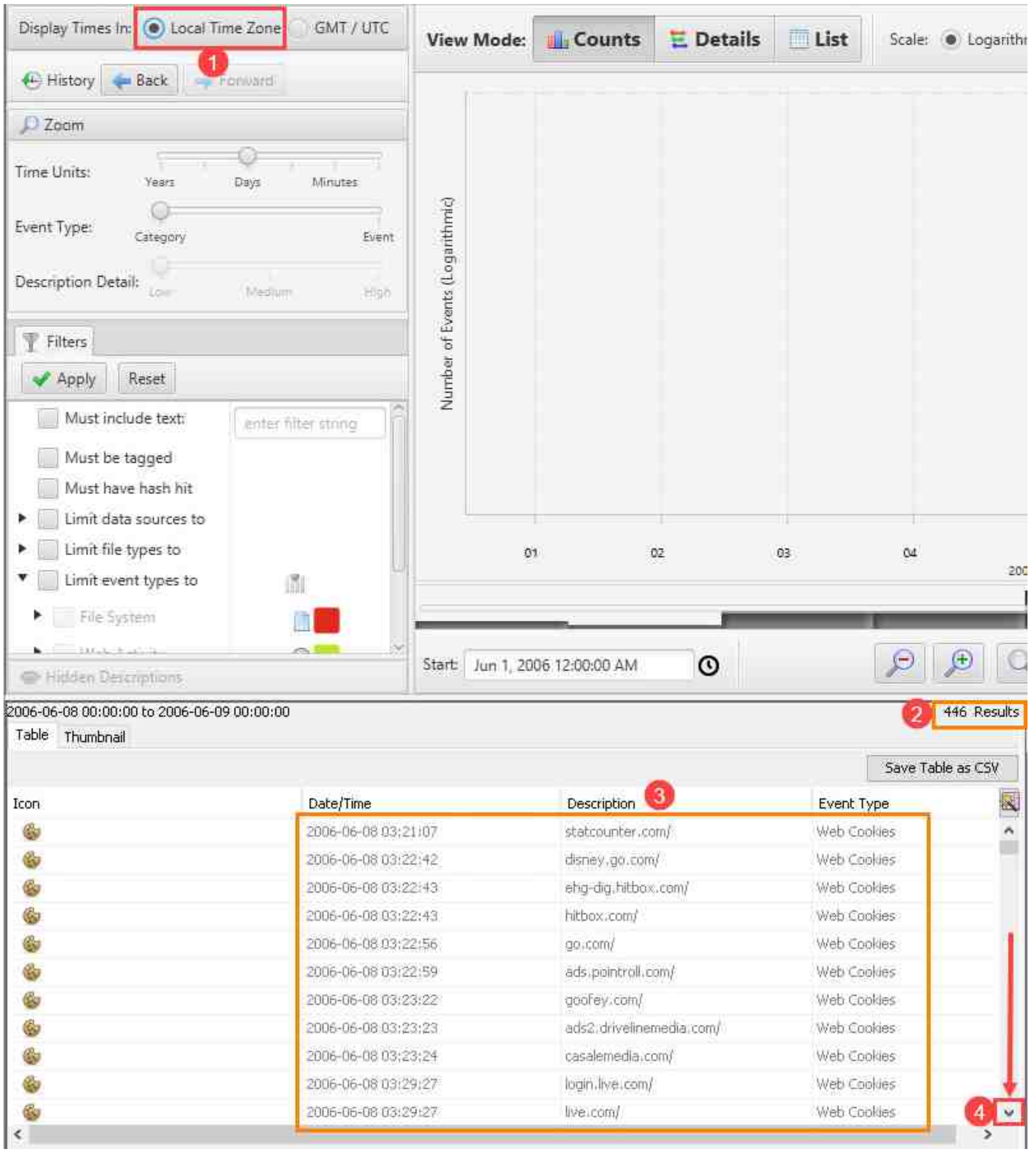
View Mode: Counts Details List Scale: ● Logarithmic ○ Linear

Start: Jun 1, 2006 5:00:00 AM

2006-06-08 05:00:00 to 2006-06-09 05:00:00 1869 Results

Icon	Date/Time	Description	Event Type
M	2006-06-08 07:55:39	/Documents and Settings/Fred/Local Settings/Temporary Internet Files/Content.IE5/BUETOYP0/clipartm001[1...	File Modified
M	2006-06-08 07:55:39	/Documents and Settings/Fred/Local Settings/Temporary Internet Files/Content.IE5/O70W4T5K/m001[1].gif	File Modified
M	2006-06-08 07:55:39	/Documents and Settings/Fred/My Documents/My Pictures/m001.gif	File Modified
A	2006-06-08 07:55:39	/Documents and Settings/Fred/Local Settings/Temporary Internet Files/Content.IE5/BUETOYP0/clipartm001[1...	File Accessed
A	2006-06-08 07:55:39	/Documents and Settings/Fred/Local Settings/Temporary Internet Files/Content.IE5/O70W4T5K/m001[1].gif	File Accessed
B	2006-06-08 07:55:39	/Documents and Settings/Fred/Local Settings/Temporary Internet Files/Content.IE5/BUETOYP0/clipartm001[1...	File Created
B	2006-06-08 07:55:39	/Documents and Settings/Fred/Local Settings/Temporary Internet Files/Content.IE5/O70W4T5K/m001[1].gif	File Created
C	2006-06-08 07:55:39	/Documents and Settings/Fred/Local Settings/Temporary Internet Files/Content.IE5/BUETOYP0/clipartm001[1...	File Changed
C	2006-06-08 07:55:39	/Documents and Settings/Fred/Local Settings/Temporary Internet Files/Content.IE5/O70W4T5K/m001[1].gif	File Changed
A	2006-06-08 07:55:44	/WINDOWS/system32/msratelc.dll	File Accessed
A	2006-06-08 07:55:44	/WINDOWS/system32/msrating.dll	File Accessed

19. The web activity will appear in the same Table/Thumbnail pane as before. Before we go any further, let's switch the time zone back to Local Time Zone to view the correct dates and times for this artifact. Do this by clicking the radio button beside Local Time Zone as seen in item 1 below. Now let's look at the web history. As you can see in items 2 and 3, there are lots of results for web activity for that day. Let's take a look at what happened around the same time that our file got created. Do this by scrolling to 07:56:04 using the mouse wheel, scroll bar, or the down arrow, as seen in item 4 below.



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

Time Units: Years Days Minutes

Event Type: Category Event

Description Detail: Low Medium High

□ 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

Scale: ● Logarithm

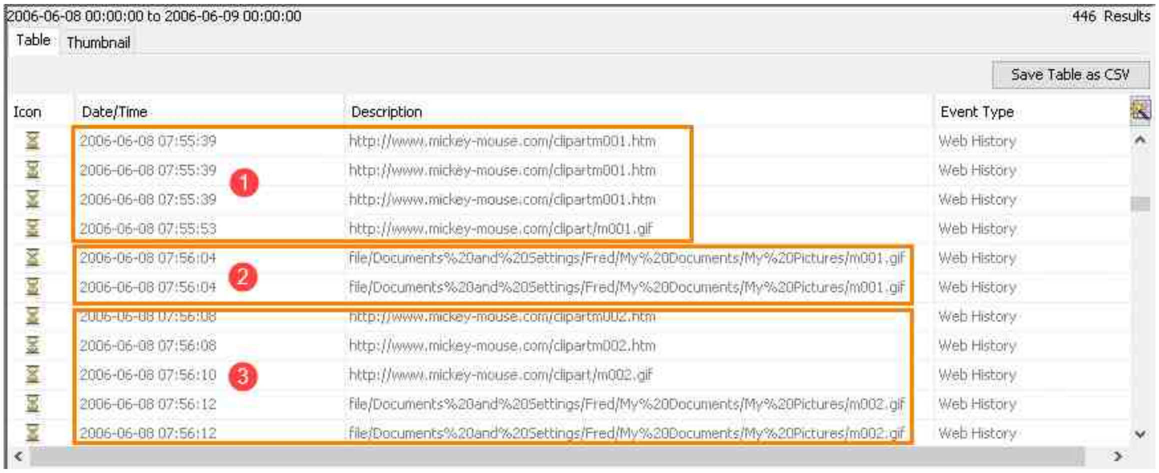
Start: Jun 1, 2006 12:00:00 AM

2006-06-08 00:00:00 to 2006-06-09 00:00:00

446 Results

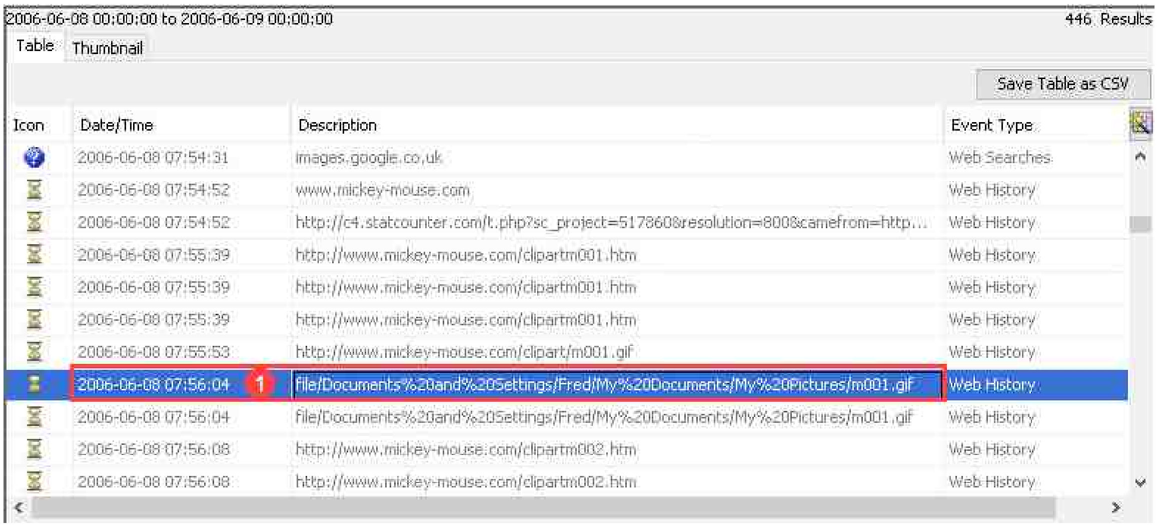
Icon	Date/Time	Description	Event Type
	2006-06-08 03:21:07	statcounter.com/	Web Cookies
	2006-06-08 03:22:42	disney.go.com/	Web Cookies
	2006-06-08 03:22:43	ehg-dig.hitbox.com/	Web Cookies
	2006-06-08 03:22:43	hitbox.com/	Web Cookies
	2006-06-08 03:22:56	go.com/	Web Cookies
	2006-06-08 03:22:59	ads.pointroll.com/	Web Cookies
	2006-06-08 03:23:22	goofey.com/	Web Cookies
	2006-06-08 03:23:23	ads2.drivelinemedia.com/	Web Cookies
	2006-06-08 03:23:24	casalemedia.com/	Web Cookies
	2006-06-08 03:29:27	login.live.com/	Web Cookies
	2006-06-08 03:29:27	live.com/	Web Cookies

20. As you can see in item 1 below, a file called m001.gif was accessed using a web browser at 07:55:53, which is 11 seconds before the file m001.gif was created. In item 2, we can see that at 07:56:04, a web browser interacted with the file m001.gif at the same path as the one for the files we tagged: Documents and Settings/Fred/My Documents/My Pictures/m001.gif. In item 3, another file we are familiar with is interacted with as well. This is the file called m002.gif that we tagged from the same directory as before.



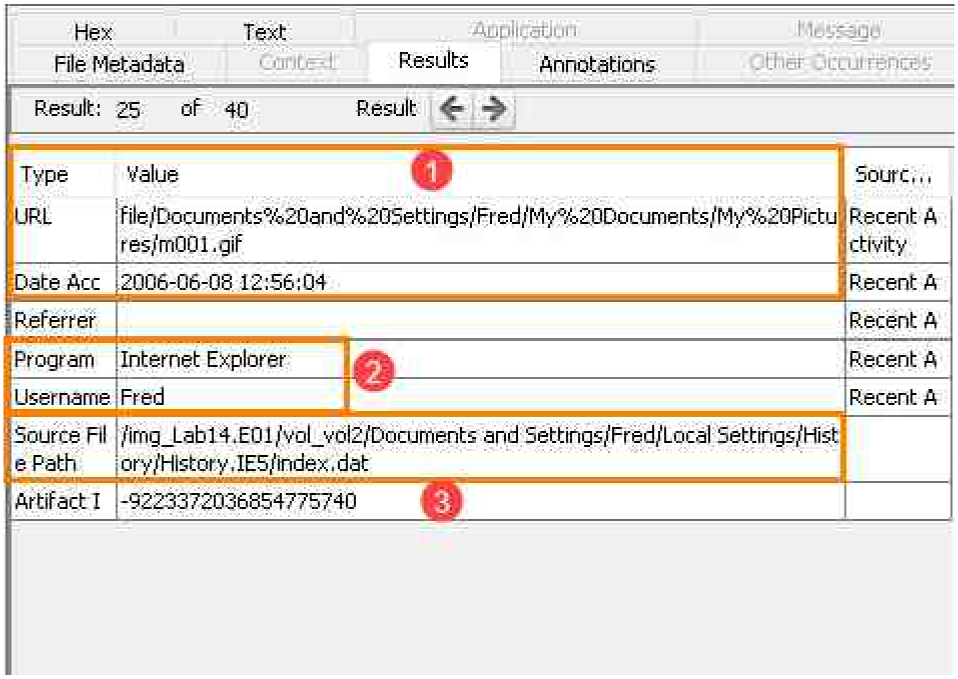
Icon	Date/Time	Description	Event Type
⌛	2006-06-08 07:55:39	http://www.mickey-mouse.com/clipartm001.htm	Web History
⌛	2006-06-08 07:55:39	http://www.mickey-mouse.com/clipartm001.htm	Web History
⌛	2006-06-08 07:55:39	http://www.mickey-mouse.com/clipartm001.htm	Web History
⌛	2006-06-08 07:55:53	http://www.mickey-mouse.com/clipart/m001.gif	Web History
⌛	2006-06-08 07:56:04	file/Documents%20and%20Settings/Fred/My%20Documents/My%20Pictures/m001.gif	Web History
⌛	2006-06-08 07:56:04	file/Documents%20and%20Settings/Fred/My%20Documents/My%20Pictures/m001.gif	Web History
⌛	2006-06-08 07:56:08	http://www.mickey-mouse.com/clipartm002.htm	Web History
⌛	2006-06-08 07:56:08	http://www.mickey-mouse.com/clipartm002.htm	Web History
⌛	2006-06-08 07:56:10	http://www.mickey-mouse.com/clipart/m002.gif	Web History
⌛	2006-06-08 07:56:12	file/Documents%20and%20Settings/Fred/My%20Documents/My%20Pictures/m002.gif	Web History
⌛	2006-06-08 07:56:12	file/Documents%20and%20Settings/Fred/My%20Documents/My%20Pictures/m002.gif	Web History

21. Let's take a look at the entry to see if we can learn more about the interaction. Do this by clicking the entry at 07:56:04 called Documents and Settings/Fred/My Documents/My Pictures/m001.gif, as seen in item 1 below, to view more details in the view pane.



Icon	Date/Time	Description	Event Type
❓	2006-06-08 07:54:31	images.google.co.uk	Web Searches
⌛	2006-06-08 07:54:52	www.mickey-mouse.com	Web History
⌛	2006-06-08 07:54:52	http://c4.statcounter.com/t.php?sc_project=517860&resolution=800&camefrom=http...	Web History
⌛	2006-06-08 07:55:39	http://www.mickey-mouse.com/clipartm001.htm	Web History
⌛	2006-06-08 07:55:39	http://www.mickey-mouse.com/clipartm001.htm	Web History
⌛	2006-06-08 07:55:39	http://www.mickey-mouse.com/clipartm001.htm	Web History
⌛	2006-06-08 07:55:53	http://www.mickey-mouse.com/clipart/m001.gif	Web History
⌛	2006-06-08 07:56:04	file/Documents%20and%20Settings/Fred/My%20Documents/My%20Pictures/m001.gif	Web History
⌛	2006-06-08 07:56:04	file/Documents%20and%20Settings/Fred/My%20Documents/My%20Pictures/m001.gif	Web History
⌛	2006-06-08 07:56:08	http://www.mickey-mouse.com/clipartm002.htm	Web History
⌛	2006-06-08 07:56:08	http://www.mickey-mouse.com/clipartm002.htm	Web History

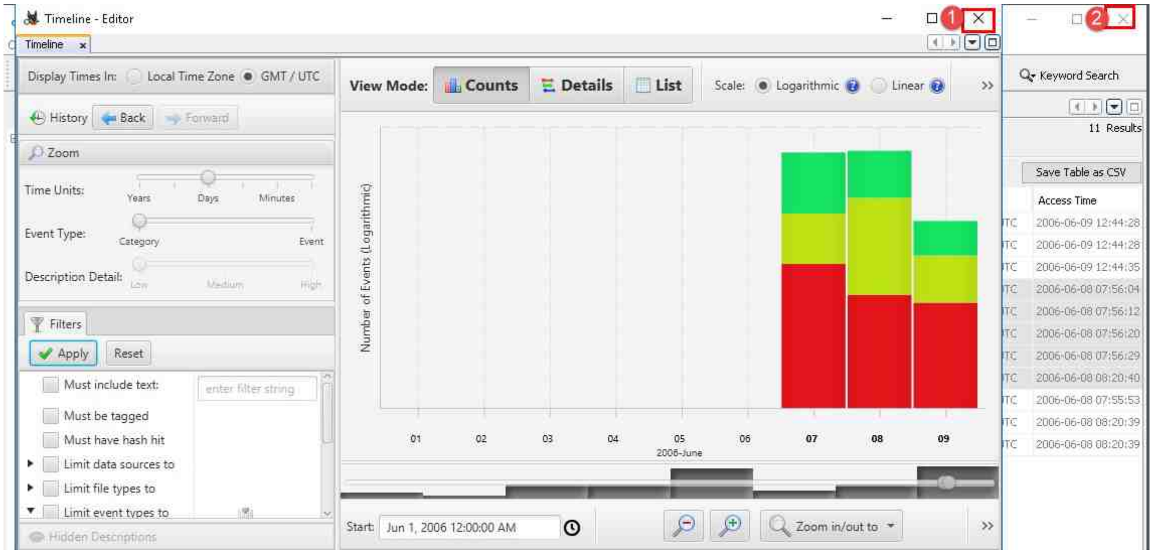
22. The view pane to the right of the Table/Thumbnail pane will populate with details about the selected file. As you can see in item 1 below, the file's path and access dates in UTC are listed. This shows us when the browser interacted with this file. Item 2 shows the name of the browser and the name of the user that was using the browser. Finally, the source of the data is listed in item 3. This is the path for the index.dat file, which is the location for internet history records for older versions of the Internet Explorer web browser.



Type	Value	Sourc...
URL	file/Documents%20and%20Settings/Fred/My%20Documents/My%20Pictures/m001.gif	Recent Activity
Date Acc	2006-06-08 12:56:04	Recent A
Referrer		Recent A
Program	Internet Explorer	Recent A
Username	Fred	Recent A
Source File Path	/img_Lab14.E01/vol_vol2/Documents and Settings/Fred/Local Settings/History/History.IE5/index.dat	
Artifact I	-9223372036854775740	

23. Based on the data we've seen, we can summarize that the user browsed the website www.mickey-mouse.com using the Internet Explorer web browser and downloaded the files m001.gif and m002.gif. You can scroll further down to look at the activity for the other files that we tagged earlier to determine when they were first accessed and then downloaded.
24. This exercise was a simple demonstration of a timeline analysis. Using dates and times from various artifacts, you can tell the story of how files were created, what a user was doing, and whether evidence can prove or disprove an allegation.

25. This lab is now complete. Close all open windows and programs by clicking the X at the top-right corner of each window as highlighted below.



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

Scale: ● Logarithmic ○ Linear

Start: Jun 1, 2006 12:00:00 AM

	Access Time
TC	2006-06-09 12:44:28
TC	2006-06-09 12:44:28
TC	2006-06-09 12:44:35
TC	2006-06-08 07:56:04
TC	2006-06-08 07:56:12
TC	2006-06-08 07:56:20
TC	2006-06-08 07:56:29
TC	2006-06-08 08:20:40
TC	2006-06-08 07:55:53
TC	2006-06-08 08:20:39
TC	2006-06-08 08:20:39