F 201: Rhino Hunt with Autopsy

What You Need for This Project

- A Windows machine with Autopsy installed

Purpose

To practice basic forensic techniques:

- Reading a scenario
- Verifying a hash value
- Extracting files from a disk image with Autopsy

Scenario

The city of New Orleans passed a law in 2004 making possession of nine or more unique rhinoceros images a serious crime. The network administrator at the University of New Orleans recently alerted police when his instance of RHINOVORE flagged illegal rhino traffic. Evidence in the case includes a computer and USB key seized from one of the Universityâ€™s labs. Unfortunately, the computer had no hard drive. The USB key was imaged and a copy of the dd image is the case1.zip file youâ€™ve been given.

In addition to the USB key drive image, three network traces are also availableâ€”these were provided by the network administrator and involve the machine with the missing hard drive. The suspect is the primary user of this machine, who has been pursuing his Ph.D. at the University since 1972.

Downloading the Evidence File

On your Windows machine, download this file:

case1.zip (3.4 MB)

Verifying the Hash Value

If you don't already have it, download Hashcalc from

https://www.slavasoft.com/download.htm

Install Hashcalc. Launch it.

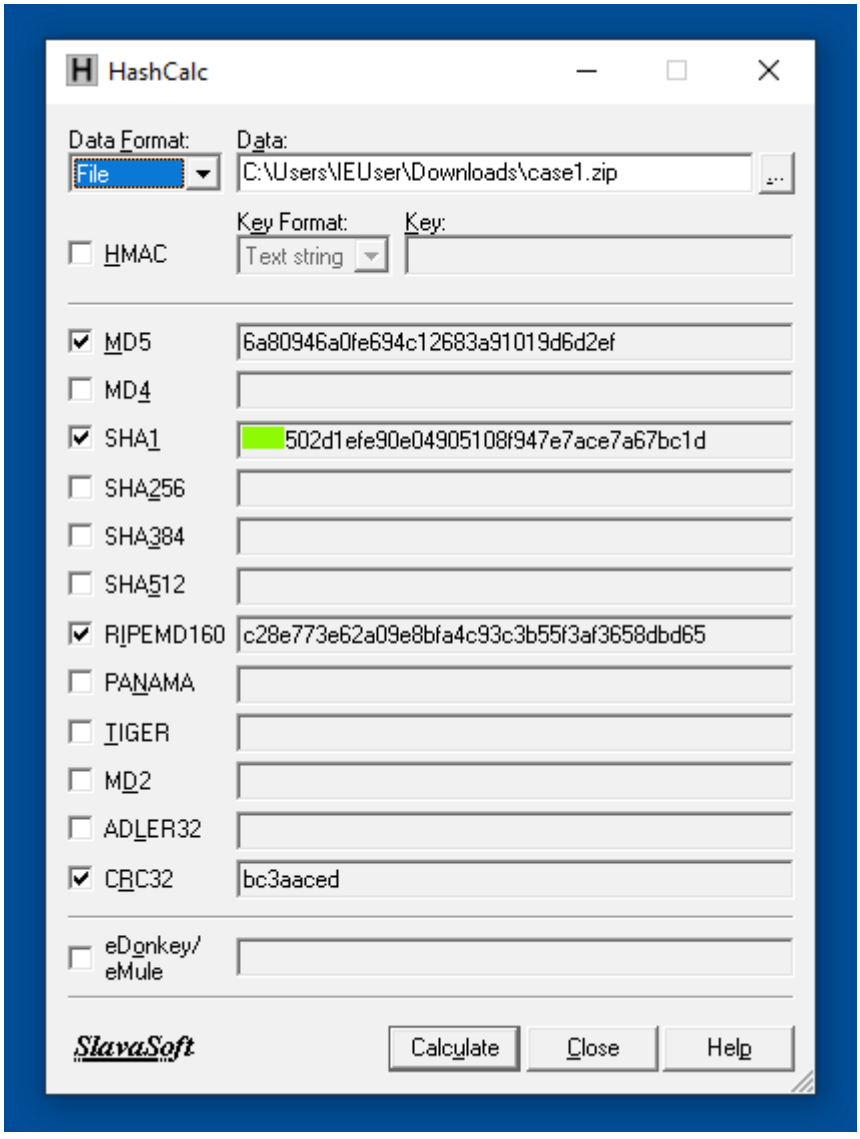
Drag the **case1.zip** file and drop it on the Hashcalc window.

You see various hash values, including MD5 and SHA1, as shown below.

F 201.1: SHA1 (5 pts)

Verify that the MD5 value matches the value shown below. If it does not, re-download the evidence file.

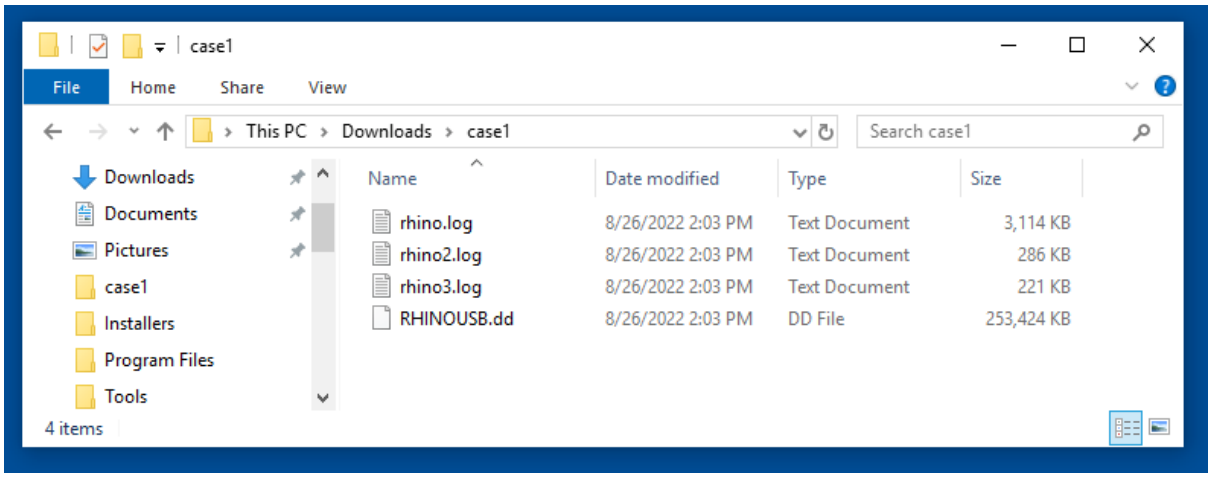
The flag is the first portion of the SHA1 address, covered by a green rectangle in the image below.



Unzipping the Evidence File

Right-click the **case1.zip** file and click "**Extract All...**". Click the **Extract** button.

You see four files, as shown below.



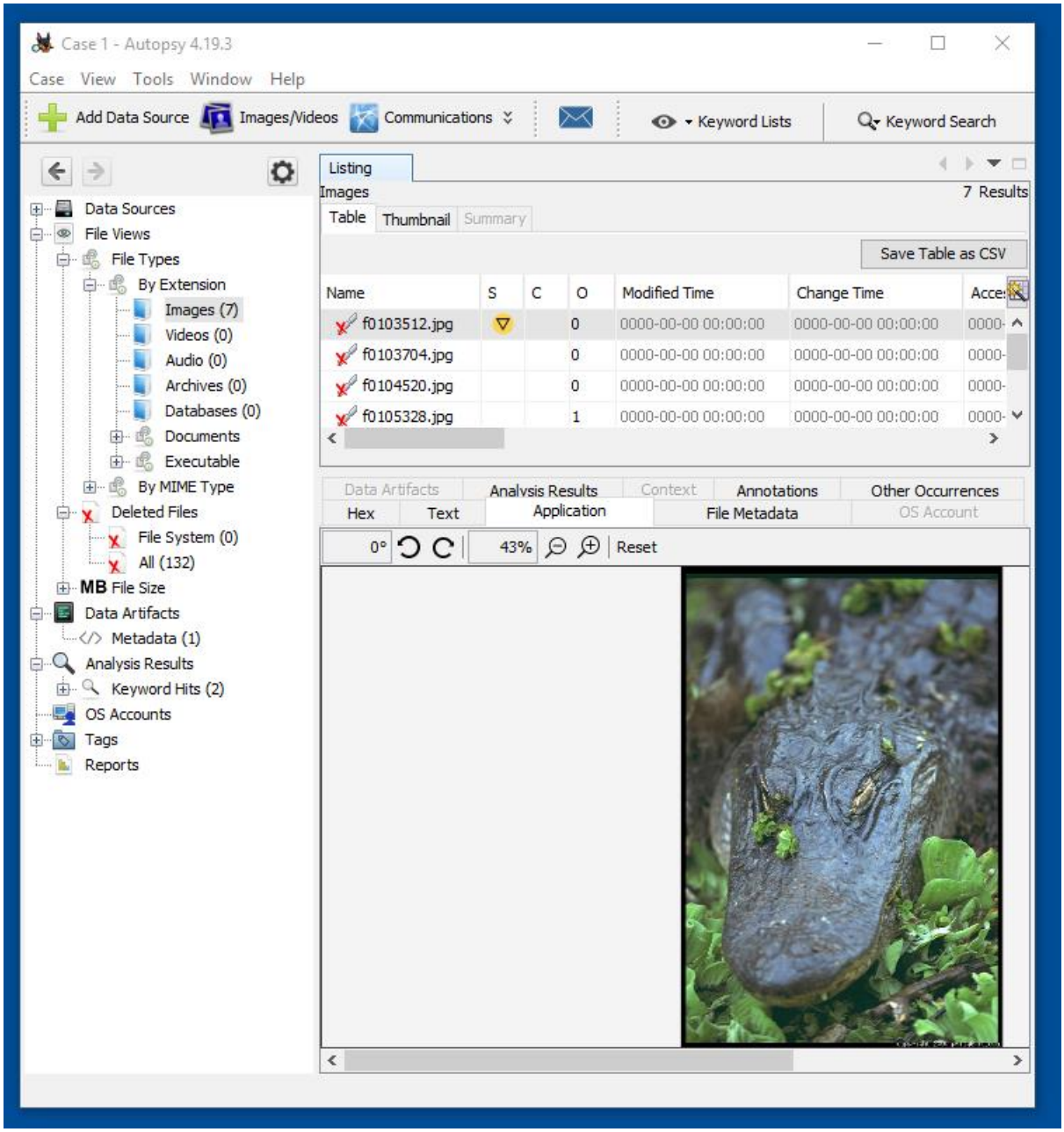
Creating an Autopsy Case

Launch Autopsy. In the Welcome box, click "**New Case**".

Make these selections:

- Case Name: Name your case **F201**
- Base Directory: Select your Documents folder and click **Next**.
- Assign it a case number of **F201** and click **Finish**.
- In the "1. Select Host" page, click **Next**.
- In the "2. Select Data Source Type" page, accept the default of "**Disk Image or VM File**" and click **Next**.
- In the "3. Select Data Source" page, click **Browse**, navigate to the **RHINOUSB.dd** file, and double-click it. Then click **Next**.
- In the "4. Configure Ingest" page, click the "**Select All**" button and click **Next**.
- In the "5. Add Data Source" page, Click **Finish**.

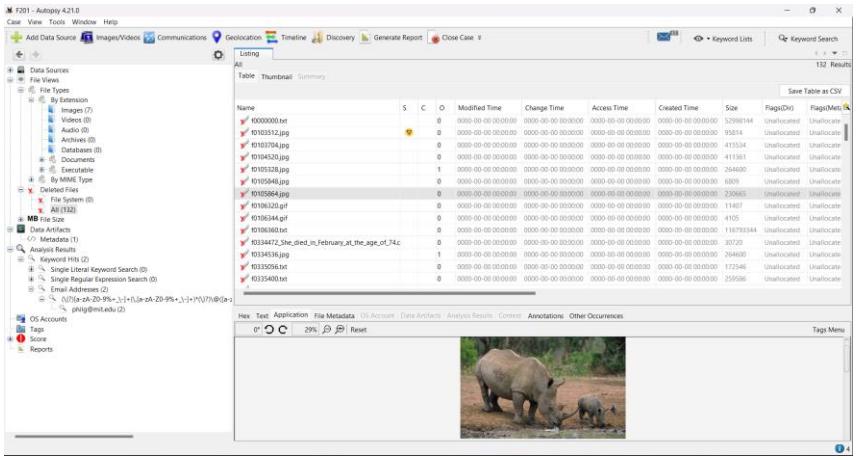
When the data file is imported and processed, in the left pane of Autopsy, expand the containers to see the **Images** and "**Deleted Files**", as shown below.



F 201.2: Mother and Child (5 pts)

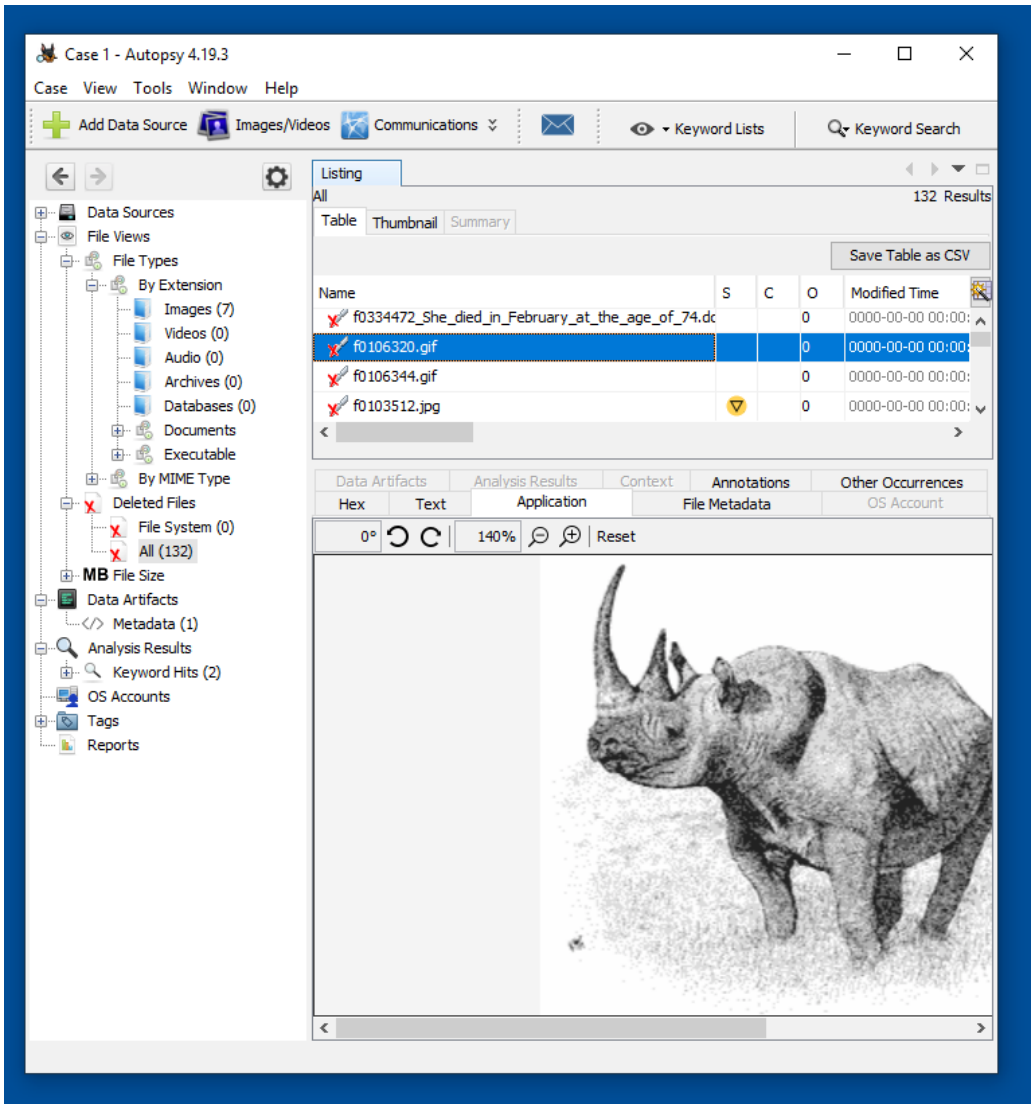
Find the image of a mother rhinoceros and her child. That's the flag.

(If you are using an automated CTF scoreboard, enter the filename of the image as the flag.)



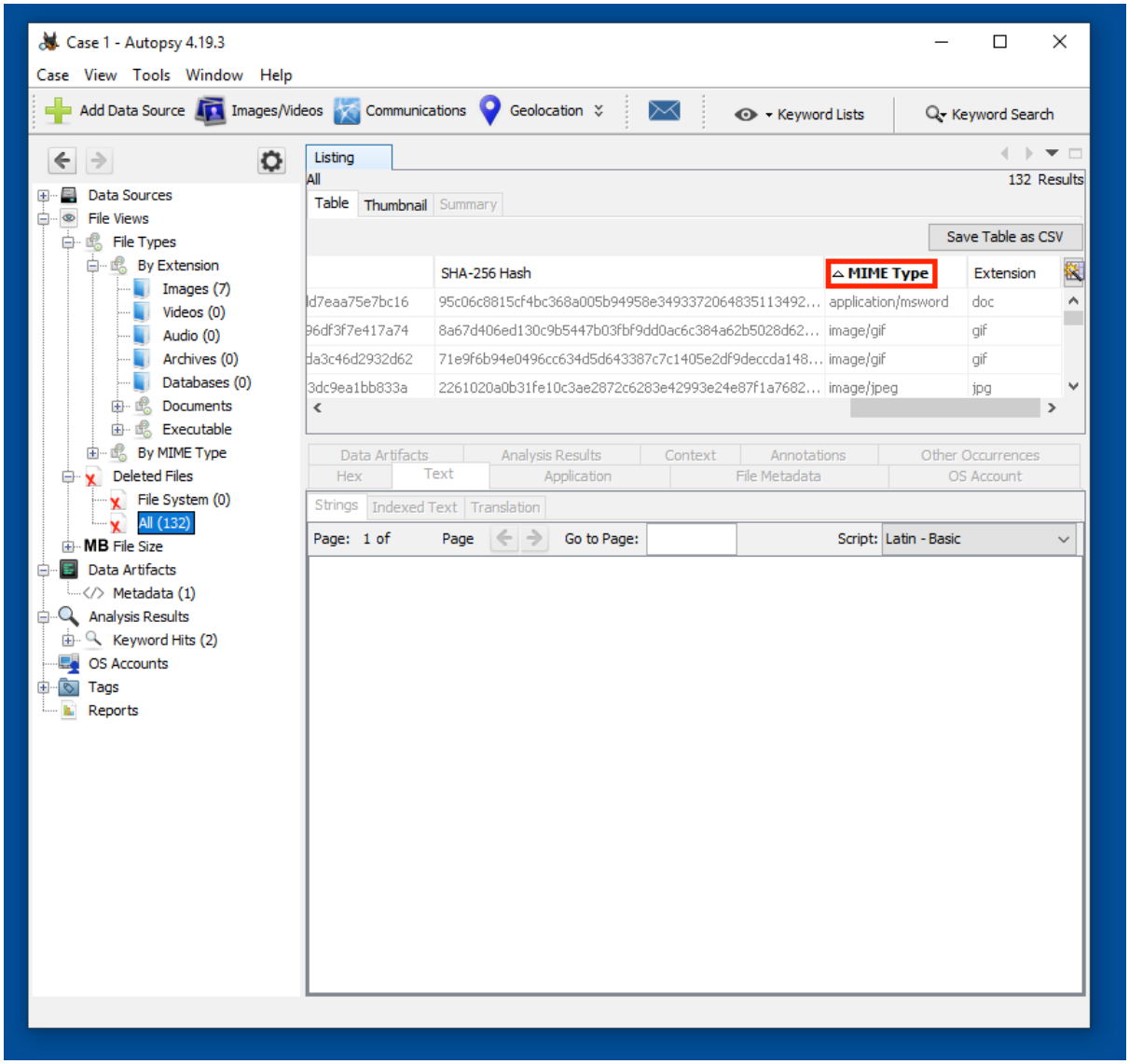
Examining Deleted Files

In the left pane, select **All**. The deleted files appear in the right pane, as shown below.



Sorting by File Type

In the top right pane, scroll to the right. Click "**MIME Type**", outlined in red in the image below, to sort the files, and put the "**application/msword**" file at the top.

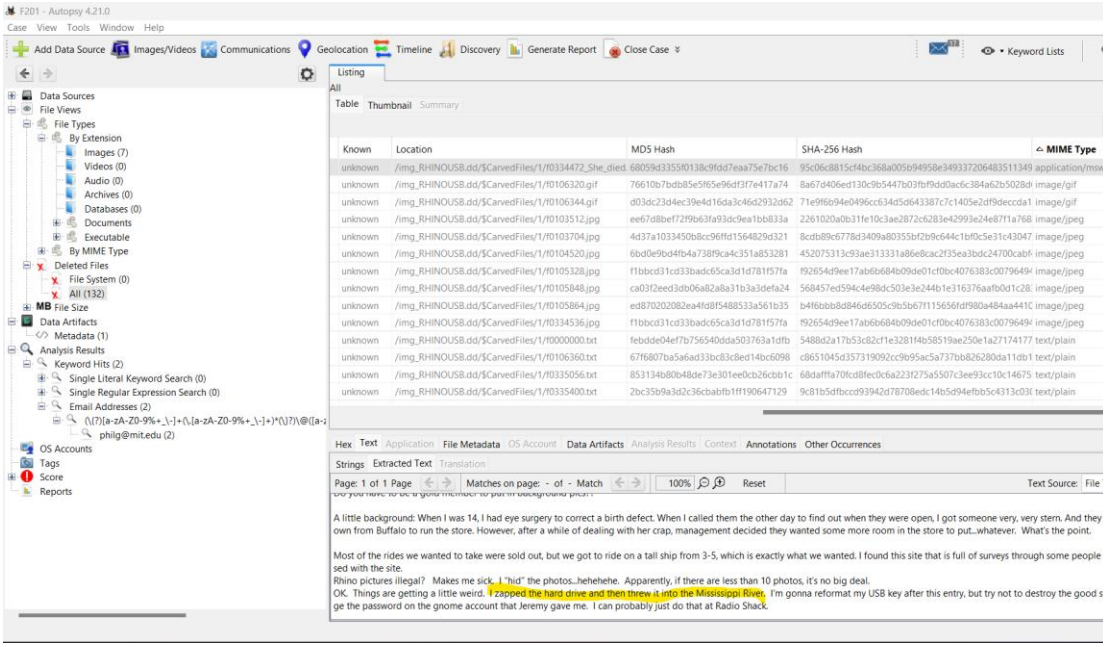


Reading the Diary

The "application/msword" file is a diary. Read through it and find the flag below.

F 201.3: Hard Drive (5 pts)

Find the location of the missing hard drive. That's the flag.

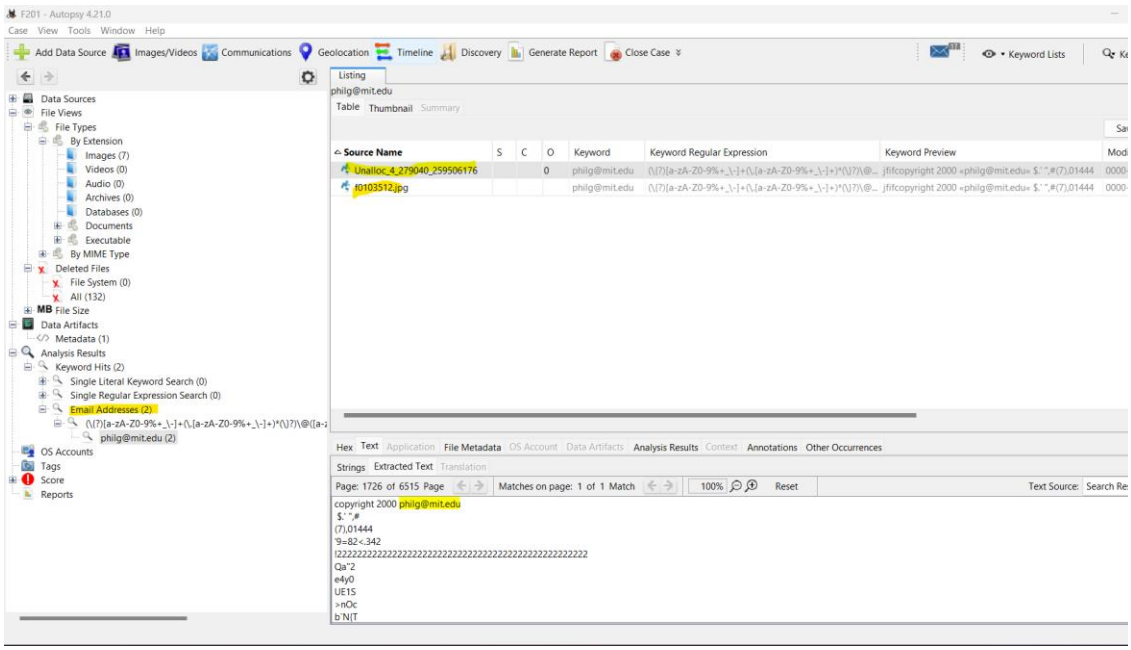


`I zapped the hard drive and then threw it into the Mississippi River`

F 201.4: Email Address (10 pts extra)

There are two files containing an email address at MIT. Only one of the files has a real filename. (A filename beginning with "Unalloc" is a fake filename generated by Autopsy for files recovered from unallocated clusters.)

That filename is the flag.


F201 - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Data Sources
File Views
File Types
By Extension
Images (7)
Videos (0)
Audio (0)
Archives (0)
Databases (0)
Documents
Executable
By MIME Type
Deleted Files
File System (0)
All (132)
MB File Size
Data Artifacts
Metadata (1)
Analysis Results
Keyword Hits (2)
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
Email Addresses (2)
philg@mit.edu (2)
OS Accounts
Tags
Score
Reports
Listing
philg@mit.edu
Table
Thumbnail
Summary
Source Name
S
C
O
Keyword
Keyword Regular Expression
Keyword Preview
Unalloc_4_279040_259506176
0
philg@mit.edu
f0103512.jpg
philg@mit.edu
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Strings
Extracted Text
Translation
Page: 1726 of 6515 Page
Matches on page: 1 of 1 Match
100%
Reset
Text Source:
copyright 2000 philg@mit.edu
$'.`"#
(7),01444
'9=82<.342
Qa"2
e4y0
UE1S
>nOc
b`N(T