

# 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 University'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 you've been given.

In addition to the USB key drive image, three network traces are also available—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.

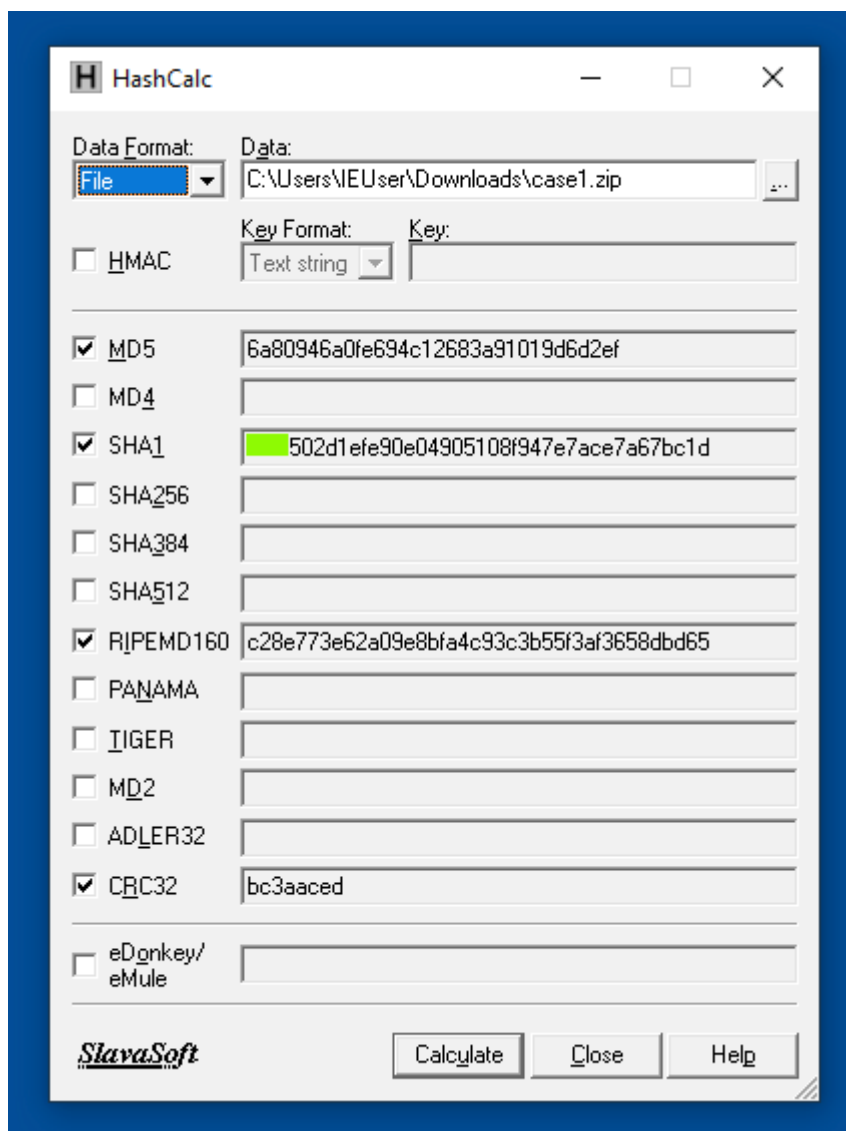
Drag the **case1.zip** file and drop it on the Hashcalc window.

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.

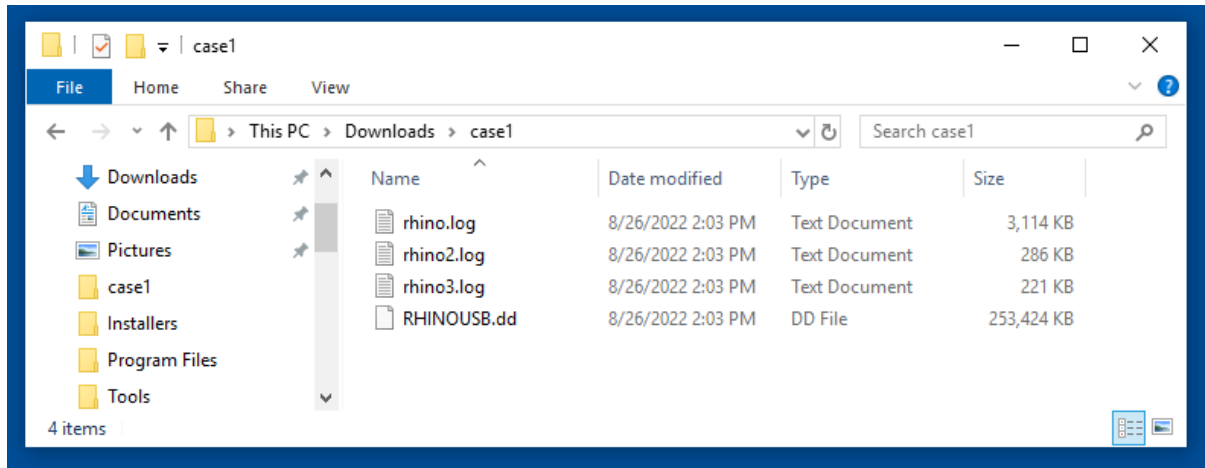
The flag is the first portion of the SHA1 address, covered by a green rectangle in the image below.



## 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.



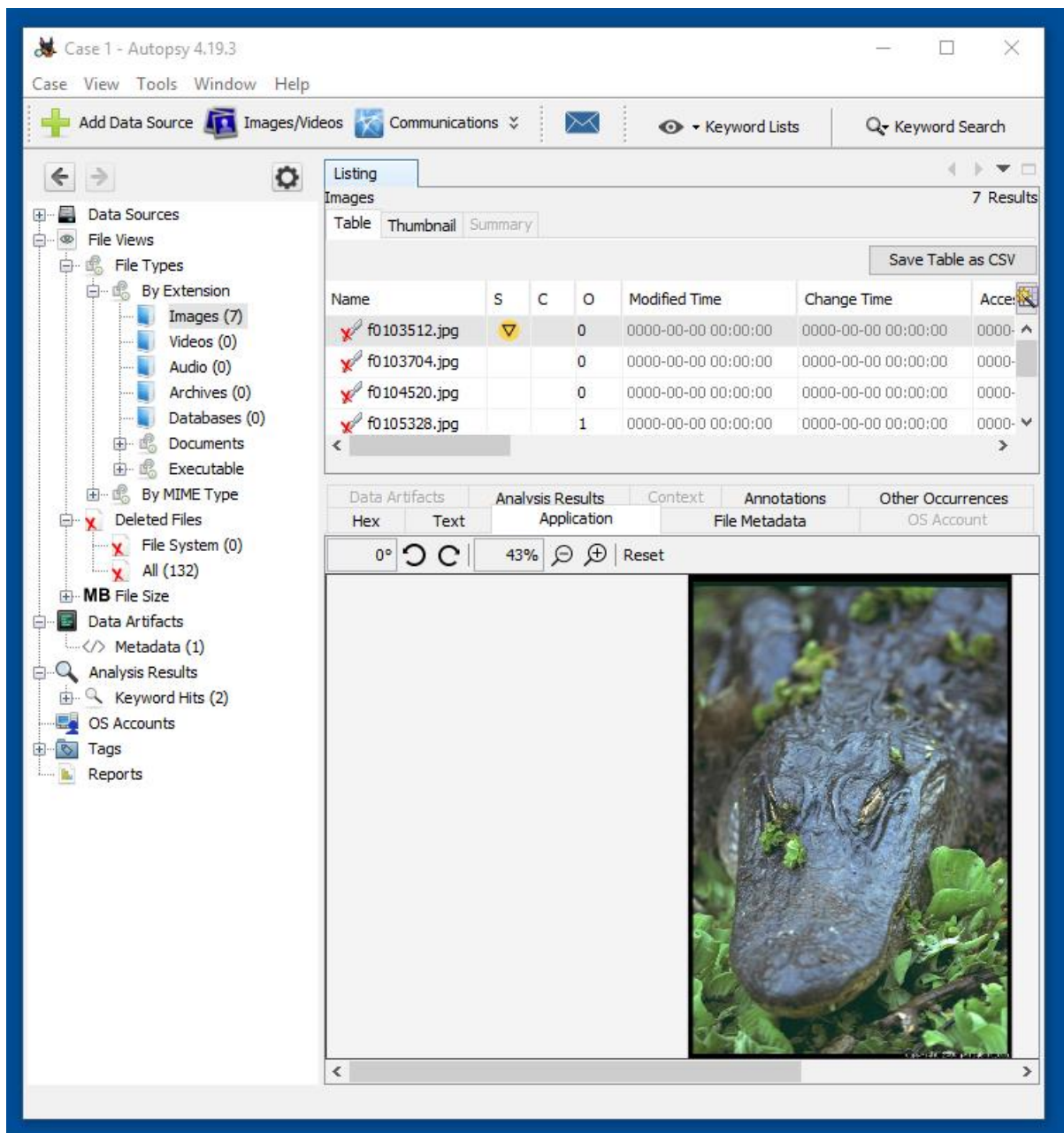
## Creating an Autopsy Case

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**.

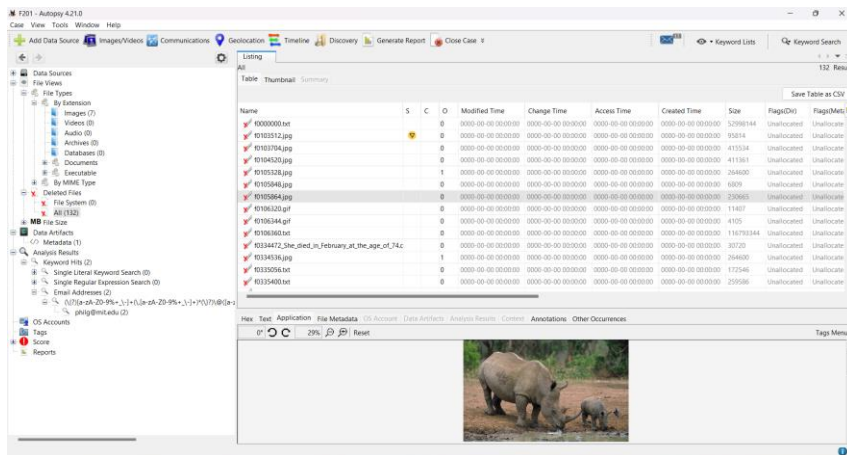
When the data file is imported and processed, in the left pane of Autopsy, expand the containers to see the **Images** and "**Deleted Files**", as shown below.



## F 201.2: Mother and Child (5 pts)

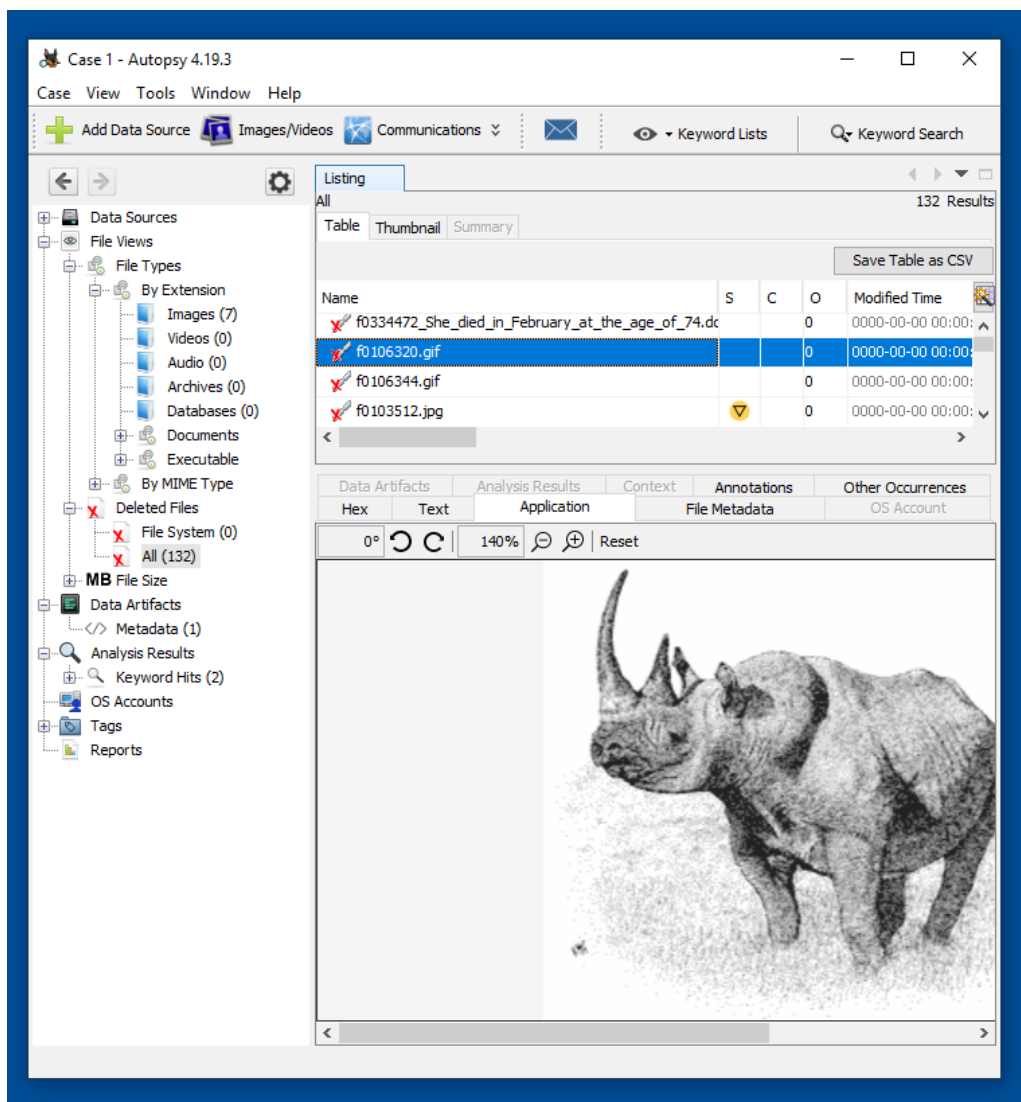
Find the image of a mother rhinoceros and her child. That's the flag.

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



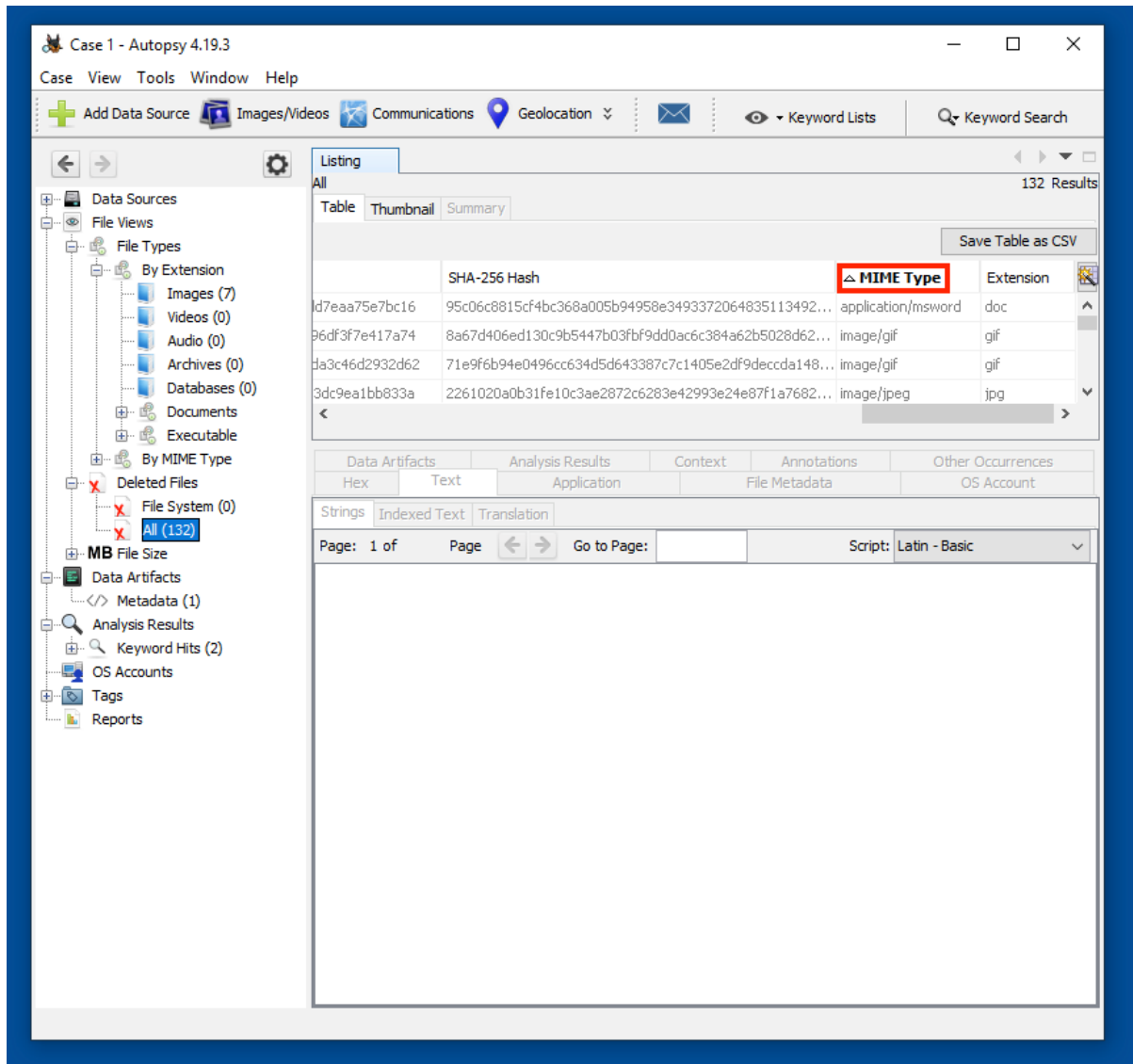
## Examining Deleted Files

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.

The screenshot shows the Autopsy 4.21.0 interface. The left sidebar displays the 'Data Sources' tree with 'File Views' expanded, showing 'File Types' and 'Deleted Files'. The main pane shows a 'Listing' table with the following columns: Known, Location, MD5 Hash, SHA-256 Hash, and MIME Type. The table lists various files from a forensic image, including images, executables, and text files. The bottom pane shows the 'Extracted Text' for a selected file, which contains a paragraph about eye surgery and a sentence that reads: 'I zapped the hard drive and then threw it into the Mississippi River'.

Known	Location	MD5 Hash	SHA-256 Hash	MIME Type
unknown	/img_RHINOUSB.dd/\$CarvedFiles/1/0034472_She_died	68059d33550138c9fdd7eaa75e7bc16	95c06d815c4fbc368a005b94958e349337206483511349	application/msn
unknown	/img_RHINOUSB.dd/\$CarvedFiles/1/00106320.gif	76610b7b0b85e5f6e96d37e417a74	8a67d406ed130c9b5447b03f9dd0ac6c384a62b5028d	image/gif
unknown	/img_RHINOUSB.dd/\$CarvedFiles/1/00106344.gif	d03dc23d4ec39e4d16da3c46a2932d62	71e9f6b94e0496cc34d5d643387c7c1405e2d9deccda1	image/gif
unknown	/img_RHINOUSB.dd/\$CarvedFiles/1/00103512.jpg	ee67d8bef72f9b63fa93dc9ea1bb833a	2261020a0b311e10c3ae2872c6283e42993e24e8711a768	image/jpeg
unknown	/img_RHINOUSB.dd/\$CarvedFiles/1/00103704.jpg	4d37a1033450b8cc96f6d1564829d321	8cdeb89c6778d3409a80355bf2b9c644c1bf0c5e31c43047	image/jpeg
unknown	/img_RHINOUSB.dd/\$CarvedFiles/1/00104520.jpg	6bd0e9b04fb4a738f9ca4c351a853281	452075313c93ae313331a86e8ac2f35ea3bd24700cab6	image/jpeg
unknown	/img_RHINOUSB.dd/\$CarvedFiles/1/00105328.jpg	1f1bbcd31cd33badc65ca3d1d781f57fa	f92654d9ee17ab6b684b09de01c0bc4076383c0079649	image/jpeg
unknown	/img_RHINOUSB.dd/\$CarvedFiles/1/00105848.jpg	ca03f2eed3db06a82a8a31b3a3defa24	568457ed594c4e98d503e3e244b1e316376aaf0d1c28	image/jpeg
unknown	/img_RHINOUSB.dd/\$CarvedFiles/1/00105864.jpg	ed870202082ea4f8f5488533a561b35	b4f62bb8d846cd6505c9b5b67115656fd980a484a441c	image/jpeg
unknown	/img_RHINOUSB.dd/\$CarvedFiles/1/00334536.jpg	1f1bbcd31cd33badc65ca3d1d781f57fa	f92654d9ee17ab6b684b09de01c0bc4076383c0079649	image/jpeg
unknown	/img_RHINOUSB.dd/\$CarvedFiles/1/00000000.txt	febdde04ef7b756540dda503763a1dfb	5488d2a17b53c62c1e328114b58519ac250e1a27174177	text/plain
unknown	/img_RHINOUSB.dd/\$CarvedFiles/1/00106360.txt	67f6807ba5a6ad33bc83cbed140c6098	c8651045d357319092cc9e95ac5a737b826280da11db1	text/plain
unknown	/img_RHINOUSB.dd/\$CarvedFiles/1/00335056.txt	853134b80b48de73e301ee0cb26cb01c	68dafffa70fcc8f8ec0c6a232f275a507c3ee93cc10c14675	text/plain
unknown	/img_RHINOUSB.dd/\$CarvedFiles/1/00335400.txt	2bc35b9a3d2c36cabfbf1f190647129	9c81b5dfbcc093942d78708edc14b5d94ef0b5c4313c03c	text/plain

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Strings Extracted Text Translation

Page: 1 of 1 Page Matches on page: - of - Match 100% Reset Text Source: File

A little background: When I was 14, I had eye surgery to correct a birth defect. When I called them the other day to find out when they were open, I got someone very, very stern. And they own from Buffalo to run the store. However, after a while of dealing with her crap, management decided they wanted some more room in the store to put...whatever. What's the point.

Most of the rides we wanted to take were sold out, but we got to ride on a tall ship from 3-5, which is exactly what we wanted. I found this site that is full of surveys through some people sed with the site.

Rhino pictures illegal? Makes me sick. I "hid" the photos..hehehehe. Apparently, if there are less than 10 photos, it's no big deal.

OK. Things are getting a little weird. I zapped the hard drive and then threw it into the Mississippi River. I'm gonna reformat my USB key after this entry, but try not to destroy the good s ge the password on the gnome account that Jeremy gave me. I can probably just do that at Radio Shack.

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.

