# CIS27A Course Project: Gathering and Reporting Digital Evidence

In this project, we will use the provide image gather digital artifacts and compose a report on the discovered evidence. Refer to below processes and project requirements.

## Case scenario

The city passed a law in making possession of nine or more unique rhinoceros images a serious crime.   The network administrator at the University  recently alerted police when his instance of RHINOVORE flagged illegal rhino traffic.  Evidence in the case includes a computer and USB drive seized from one of the University’s labs.  Unfortunately, the computer had no hard drive.  The USB drive was imaged and a copy of the *dd* image is provide.

 In addition to the USB 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 studies at the University.

**MD5 hashes for evidence:**

c0d0093eb1664cd7b73f3a5225ae3f30 \*rhino.log  
cd21eaf4acfb50f71ffff857d7968341 \*rhino2.log  
7e29f9d67346df25faaf18efcd95fc30 \*rhino3.log  
80348c58eec4c328ef1f7709adc56a54 \*CIS27A.dd

## Part 1: Gather Evidence and Report

### Tasks:

Use digital forensics tool to complete the following tasks.

1. Recover at least **nine rhino pictures** from the available evidence and include them in a report. Include screen capture and description of image in the report. (40 points)
2. Examine the network traffic and gather the evidence for the case including user account and file transfers. (60 points)
3. Who gave the accused a telnet/ftp account?
4. What’s the username/password for the account?
5. What relevant file transfers appear in the network traces?
6. Is there any evidence that connects the USB drive and the network traces?
7. If so, what type of evidence can you find?
8. Examine the image and determine what happened to the computer hard drive and USB drive. (50 points)
9. What happened to the hard drive in the computer? Where is it now?
10. What happened to the USB drive?
11. What is recoverable from the dd image of the USB drive?
12. Compose a detailed report to include tools you used, processes, timeline, evidence analysis from the requirements within tasks 1 – 3 (50 points).

### Part 2: Self Evaluation and E-Portfolio

### Tasks:

1. Complete a [Self-Evaluation](https://forms.gle/3Ky94ed7PHUu4x6T7) of the project. Submit a screen capture of the Completion page. (20 points)
2. Use [Google Sites](https://support.google.com/sites/answer/6372878?hl=en) to create a portfolio. Design your portfolio and add components of this project (Report) to the portfolio. Publish the portfolio and submit URL of your portfolio. (30 points)