Upload this document as a pdf.

## Name: Student ID:

## Q1) The Order of Volatility

How does the effect of time on volatile data cause problems for the forensics process?

Why does the first responder consider volatility before executing any command?

# Q2) Live or Post Mortem?

Indicate what is the worry with the effect of a live analysis on disk based evidence.

What is the advantage of a remote live analysis when you are not sure if an intrusion has happened?

Why is a Live Analysis the best option when you suspect the files on disk may be encrypted?

**Q3) Capturing an image using ProDiscover**

**C) Analysis**

**1) Search for a keyword in text files.**

The search results appear.

Click the matching file in the work area.

The matching pattern will be shown in the data area.

Inset here your screen shot showing the work area and the data area result.

**2) Search for a deleted file on disk**.

Note the red cross indicating the file has been deleted.

Click the matching file.

The matching pattern will be shown in the data area.

Insert your work area and data area screen shot here.

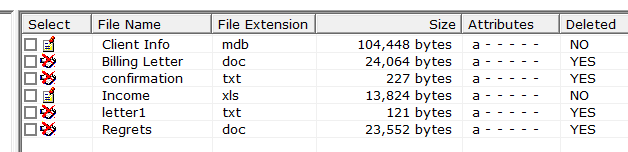
**3) Search for a cluster on disk**.

When finished, the Cluster Search Results will list any matches.

Insert your screen shot showing the word MSDOS here.

What does FAT16 (or FAT32) mean? How does it relate to clusters? Add your answer here.

**Q4) Advanced – Optional - Analysing an image using ProDiscover**

 **B) Acquisition**

Select Letter1.

Note its contents in the data area.

Insert your screen shot of the letter 1 contents here.

**C) Analysis**

Insert here a screen shot of the spreadsheet.

Examine enough files to determine if the allegation is proven or not.

**D) ProDiscover Report**

When finished, right click the ProDiscover report, and copy only the useful items here.

Indicate here why the allegation is proven or not.

## For all Questions - Report Submission.

Save this report as a single pdf.

Upload this pdf to Canvas.