The Forensics of Plagiarism: A Case Study in Cheating

Tim Ball, PhD
22 June 2017

Introduction

What this is:

- **A real case**
  - Actual events
  - Names changed
- **An application of common tools and techniques**

What this isn't:

- **Highly technical**
- **Personal**
- **The first time this has happened!**

Background

- **Student A was caught/accused of plagiarism**
  - In a Computer Forensics class!!
- **Used Student B's work from a previous semester**
- **Received a grade of "F for Cheating" in the class.**
- **Student A denied any wrongdoing**
  - Adamantly denied!
  - Got the parents involved
- **Student A was supposed to graduate, but ...**

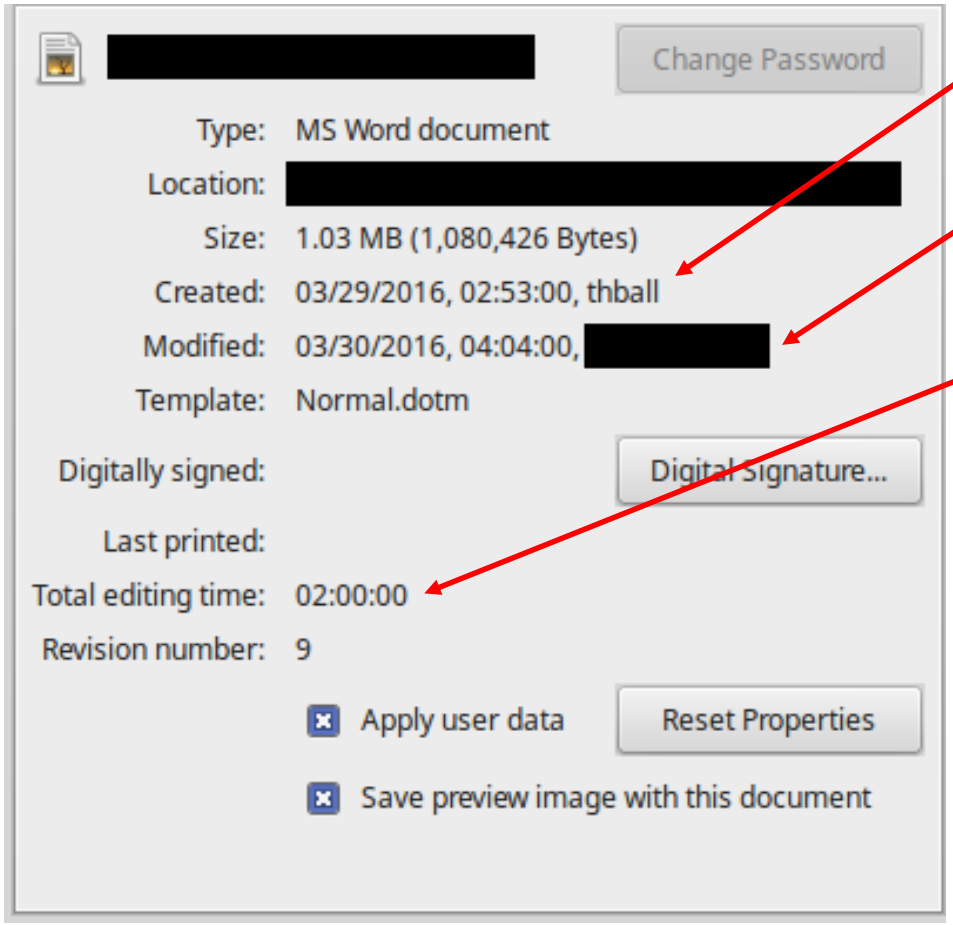
The Informant

- **Original "tip" came from Turnitin**
  - Originality report - 36% overall
  - 18% similar to Student B
- **Some crossover expected from template**
- **High percentage required investigation**
- **Student B was in the same class previous semester**
  - A copy of Student B's paper could easily be retrieved

Initial Investigation: Visual Inspection

- The first step was to compare the papers side-by-side
- File properties of Student A's were suspicious
- Wording was similar, exact in some places
- Screen shots appeared to be the same

Visual Inspection: File Properties



- **Created by me**
- **Last modified by Student A**
- **2-hour editing time!!**
  - This was an extensive investigation
  - Given 2 weeks before it was due
- **Started the day before it was due**

A Word About File Properties

- **This has happened before**
- **Same course, online version**
- **Ice Ice Baby!**

http://wecastmusic.tumblr.com/post/124255489761/ice-ice-baby-vanilla-ice-1990

Visual Inspection: Text

Student A (Copy)

"In world we live in, many crimes are committed with the use of computer systems. In order to help solve many investigations of computer systems, many programs are developed in order to make the process a simpler. FTK Imager, Forensic Toolkit, Autopsy, and Encase, are all of the forensic programs that were made to help the process of examining hard drives and computer systems for law enforcement use and private use."

Student B (Original)

"In today's technological world, many crimes are committed with the help of computer systems. To help aid in investigations on computer systems, programs are developed to make the process a simpler. FTK Imager and ProDiscover Basic are two of the forensic programs that were made to aid in the process of examining hard drives and computer systems."

Visual Inspection: List of Figures

Student A (Copy)

Figures

Student B (Original)

Figures

Figure 9: Check Washing Gogle Search

Visual Inspection: Screen Shots

Student A (Copy)

```
google_ad.visible_url = "www.escapemeth.com";
google_ad.line1 = "Meth addiction video tool";
google_ad.line2 = "Graphic images, police footage used";
google_ad.line3 = "for education, treatment \x26amp; training";
google_ad.regionname = "";
google_ads[0] = google_ad;
google_ad = new Object();
google_ad.n = 2;
google_ad.type = "text";
google_ad.bidtype = "CPC";
google_ad.targeting_type = "contextual";
google_ad.url = "http://pagead2.googlesyndication.com/pagead/ic
google_ad.visible_url = "meth-wipe.com";
google_ad.line1 = "Detect Meth On-site";
google_ad.line2 = "MethAlert - Detects meth residue";
google_ad.line3 = "MethChek - Checks meth cleanup";
google_ad.regionname = "";
google_ads[1] = google_ad;
google_ad = new Object();
google_ad.n = 3;
google_ad.type = "text";
google_ad.bidtype = "CPC";
google_ad.targeting_type = "contextual";
google_ad.url = "http://pagead2.googlesyndication.com/pagead/ic
google_ad.visible_url = "www.eBay.com";
google_ad.line1 = "Crystal meth";
```

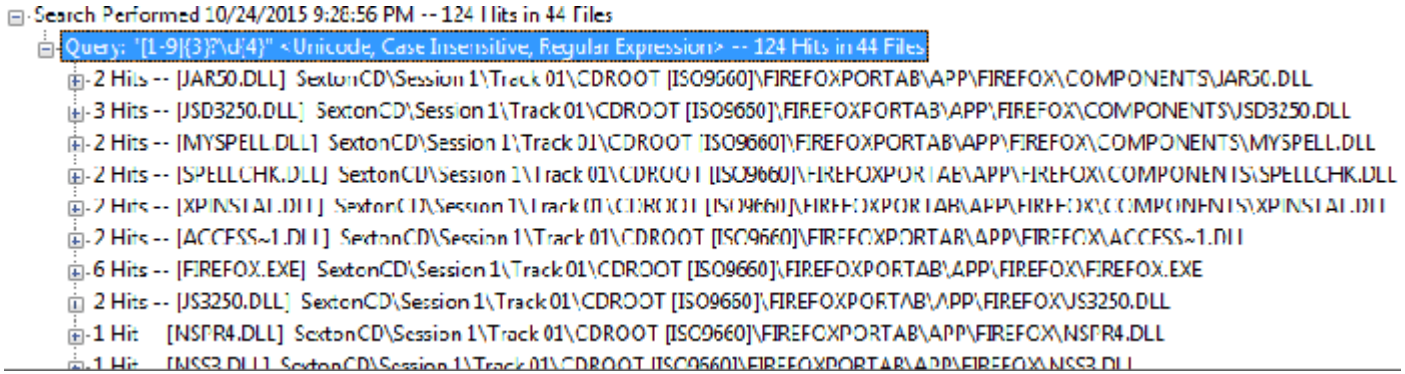
Student B (Original)

```
google_ad.visible_url = "www.escapemeth.com";
google_ad.line1 = "Meth addiction video tool";
google_ad.line2 = "Graphic images, police footage used";
google_ad.line3 = "for education, treatment \x26amp; training";
google_ad.regionname = "";
google_ads[0] = google_ad;
google_ad = new Object();
google_ad.n = 2;
google_ad.type = "text";
google_ad.bidtype = "CPC";
google_ad.targeting_type = "contextual";
google_ad.url = "http://pagead2.googlesyndication.com/pagead/ic
google_ad.visible_url = "meth-wipe.com";
google_ad.line1 = "Detect Meth On-site";
google_ad.line2 = "MethAlert - Detects meth residue";
google_ad.line3 = "MethChek - Checks meth cleanup";
google_ad.regionname = "";
google_ads[1] = google_ad;
google_ad = new Object();
google_ad.n = 3;
google_ad.type = "text";
google_ad.bidtype = "CPC";
google_ad.targeting_type = "contextual";
google_ad.url = "http://pagead2.googlesyndication.com/pagead/ic
google_ad.visible_url = "www.eBay.com";
google_ad.line1 = "Crystal meth";
```

Visual Inspection: Screen Shots

Search Performed on 10/24/2015???

Student A



Search Performed 10/24/2015 9:28:56 PM -- 124 Hits in 44 Files
Query: "[1-9]{3}?\d{4}" <Unicode, Case Insensitive, Regular Expression> -- 124 Hits in 44 Files
2 Hits -- [JAR50.DLL] SextonCD\Session 1\Track 01\CDROOT [ISO9660]\FIREFOXPORTAB\APP\FIREFOX\COMPONENTS\JAR50.DLL
3 Hits -- [JSD3250.DLL] SextonCD\Session 1\Track 01\CDROOT [ISO9660]\FIREFOXPORTAB\APP\FIREFOX\COMPONENTS\JSD3250.DLL
2 Hits -- [MYSPELL.DLL] SextonCD\Session 1\Track 01\CDROOT [ISO9660]\FIREFOXPORTAB\APP\FIREFOX\COMPONENTS\MYSPELL.DLL
2 Hits -- [SPELLCHK.DLL] SextonCD\Session 1\Track 01\CDROOT [ISO9660]\FIREFOXPORTAB\APP\FIREFOX\COMPONENTS\SPELLCHK.DLL
2 Hits -- [XPINSTAL.DLL] SextonCD\Session 1\Track 01\CDROOT [ISO9660]\FIREFOXPORTAB\APP\FIREFOX\COMPONENTS\XPINSTAL.DLL
2 Hits -- [ACCESS~1.DLL] SextonCD\Session 1\Track 01\CDROOT [ISO9660]\FIREFOXPORTAB\APP\FIREFOX\ACCESS~1.DLL
6 Hits -- [FIREFOX.EXE] SextonCD\Session 1\Track 01\CDROOT [ISO9660]\FIREFOXPORTAB\APP\FIREFOX\FIREFOX.EXE
2 Hits -- [JS3250.DLL] SextonCD\Session 1\Track 01\CDROOT [ISO9660]\FIREFOXPORTAB\APP\FIREFOX\JS3250.DLL
1 Hit -- [NSPR4.DLL] SextonCD\Session 1\Track 01\CDROOT [ISO9660]\FIREFOXPORTAB\APP\FIREFOX\NSPR4.DLL

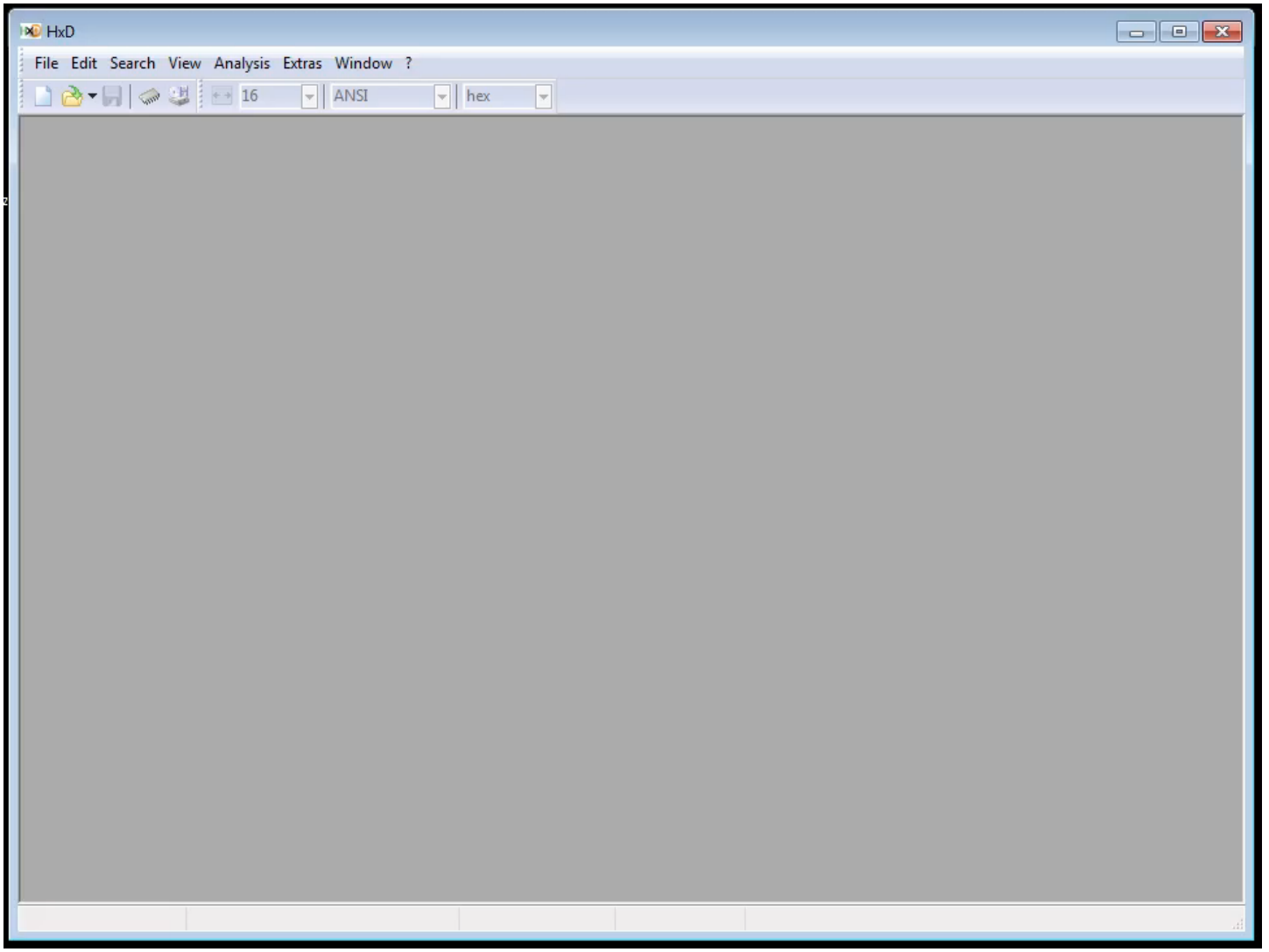
Accusation & Appeal

- **Student A was given an "F for Cheating" in the class**
  - Goes on permanent record
  - Given in extreme cases of cheating
- **Student decided to appeal the grade**
- **Because of appeal, an air-tight case was needed**
  - Appeal could go to committee

Forensics Tools & Techniques

- **7-Zip for file extraction**
  - Similar to WinZip, WinRar, etc.
- **HxD for a hex editor**
  - View the hex representation of a file
  - Perform file comparisons with hash values
- **File Hashing**
  - Technique for comparing files, file integrity
  - Creates a "message digest"
  - Unique value generated from the file contents

File Hashing Example



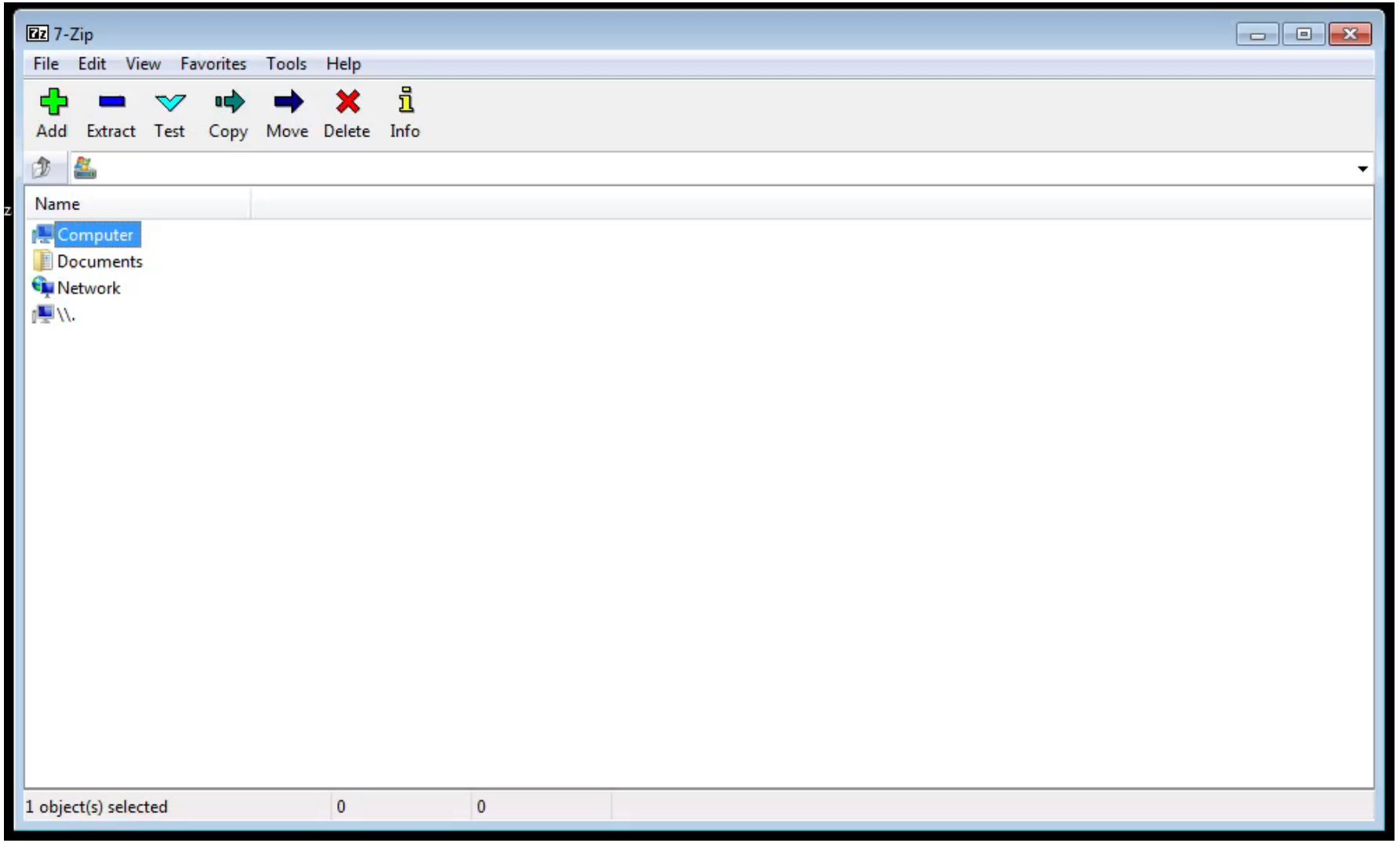
File Hashing Sample

- **Hello World.**
  - DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
- **Hello World!**
  - 2EF7BDE608CE5404E97D5F042F95F89F1C232871

Building the Case: Extracting the Evidence

- **Both Student A & B turned in Word docs**
  - docx file format is a container
- **Used 7-Zip to extract the docx files**
- **Accessed the original image files from the documents**
- **Created hashes of screen shots from both papers**

Extracting the Evidence with 7-Zip



Building the Case: Hashing the Images

Student A (Copy)

```
google_ad.visible_url = "www.escapemeth.com";
google_ad.line1 = "Meth addiction video tool";
google_ad.line2 = "Graphic images, police footage used";
google_ad.line3 = "for education, treatment \x26amp; training";
google_ad.regionname = "";
google_ads[0] = google_ad;
google_ad = new Object();
google_ad.n = 2;
google_ad.type = "text";
google_ad.bidtype = "CPC";
google_ad.targeting_type = "contextual";
google_ad.url = "http://pagead2.googlesyndication.com/pagead/ic
google_ad.visible_url = "meth-wipe.com";
google_ad.line1 = "Detect Meth On-site";
google_ad.line2 = "MethAlert - Detects meth residue";
google_ad.line3 = "MethChek - Checks meth cleanup";
google_ad.regionname = "";
google_ads[1] = google_ad;
google_ad = new Object();
google_ad.n = 3;
google_ad.type = "text";
google_ad.bidtype = "CPC";
google_ad.targeting_type = "contextual";
google_ad.url = "http://pagead2.googlesyndication.com/pagead/ic
google_ad.visible_url = "www.eBay.com";
google_ad.line1 = "Crystal meth";
```

Hash Value:
0DEC68AFE3ABD7FCFD8CA109D15B982F60AC6622

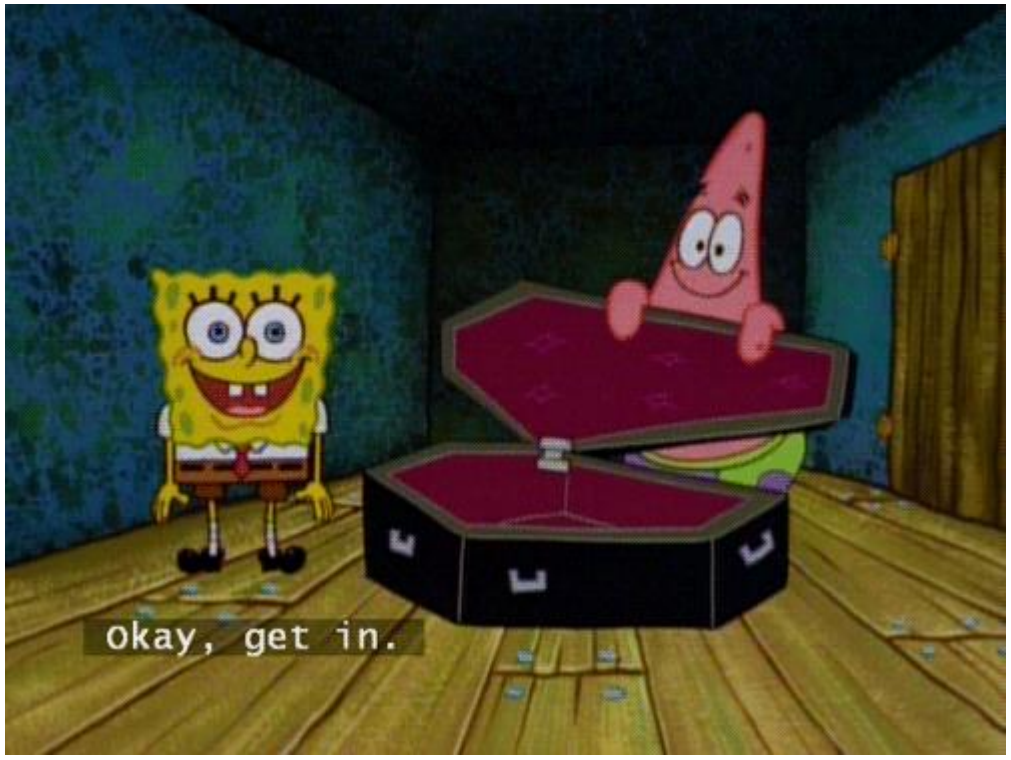
Student B (Original)

```
google_ad.visible_url = "www.escapemeth.com";
google_ad.line1 = "Meth addiction video tool";
google_ad.line2 = "Graphic images, police footage used";
google_ad.line3 = "for education, treatment \x26amp; training";
google_ad.regionname = "";
google_ads[0] = google_ad;
google_ad = new Object();
google_ad.n = 2;
google_ad.type = "text";
google_ad.bidtype = "CPC";
google_ad.targeting_type = "contextual";
google_ad.url = "http://pagead2.googlesyndication.com/pagead/ic
google_ad.visible_url = "meth-wipe.com";
google_ad.line1 = "Detect Meth On-site";
google_ad.line2 = "MethAlert - Detects meth residue";
google_ad.line3 = "MethChek - Checks meth cleanup";
google_ad.regionname = "";
google_ads[1] = google_ad;
google_ad = new Object();
google_ad.n = 3;
google_ad.type = "text";
google_ad.bidtype = "CPC";
google_ad.targeting_type = "contextual";
google_ad.url = "http://pagead2.googlesyndication.com/pagead/ic
google_ad.visible_url = "www.eBay.com";
google_ad.line1 = "Crystal meth";
```

Hash Value:
0DEC68AFE3ABD7FCFD8CA109D15B982F60AC6622

The Final Nail in the Coffin

The assignment Student A turned in was the assignment from the previous semester!



http://tumblr.com/

Verdict

- **Initial visit to Student Affairs**
  - Advised to not pursue appeal
- **Appeal to the Program Director**
  - Advised to talk to the Dean
- **Appeal to the Associate Dean**
  - Appeal denied
- **Appeal to the Provost**
  - Meeting with all three
  - Student finally admitted guilt

Questions?