Computer Forensic Essentials - Final Project

SSH[ghost]

The University

Executive Summary

On today’s date, 7 February 2016, Draft Jeweler’s security guard, Paul Mitchell, contacted me in regards to imaging an SD card employee, Danny Jones, had tried to hide in his shoe as he exited the store. Paul Mitchell informs me that Danny Jones may have blueprints of the store on the SD car. As per store policy, Danny Jones has violated the rule against using removable media without management authorization and bringing in or leaving with removable media. Paul Mitchell has requested a full forensic examination and report to see what store files are included on the drive for possible criminal charges and civil litigation. Paul Mitchell has removed the SD card from the store safe where it has been stored undisturbed since confiscation as per store security camera footage.

The tools I used include Nikon Coolpix L340 Digital Camera, Asus N76VJ laptop, Linux Mint 17 operating system, UltraBlock USB 3.0 Forensic Card Reader and Writer, GParted, Linux terminal, Guymager, Firefox web browser, and Autopsy.

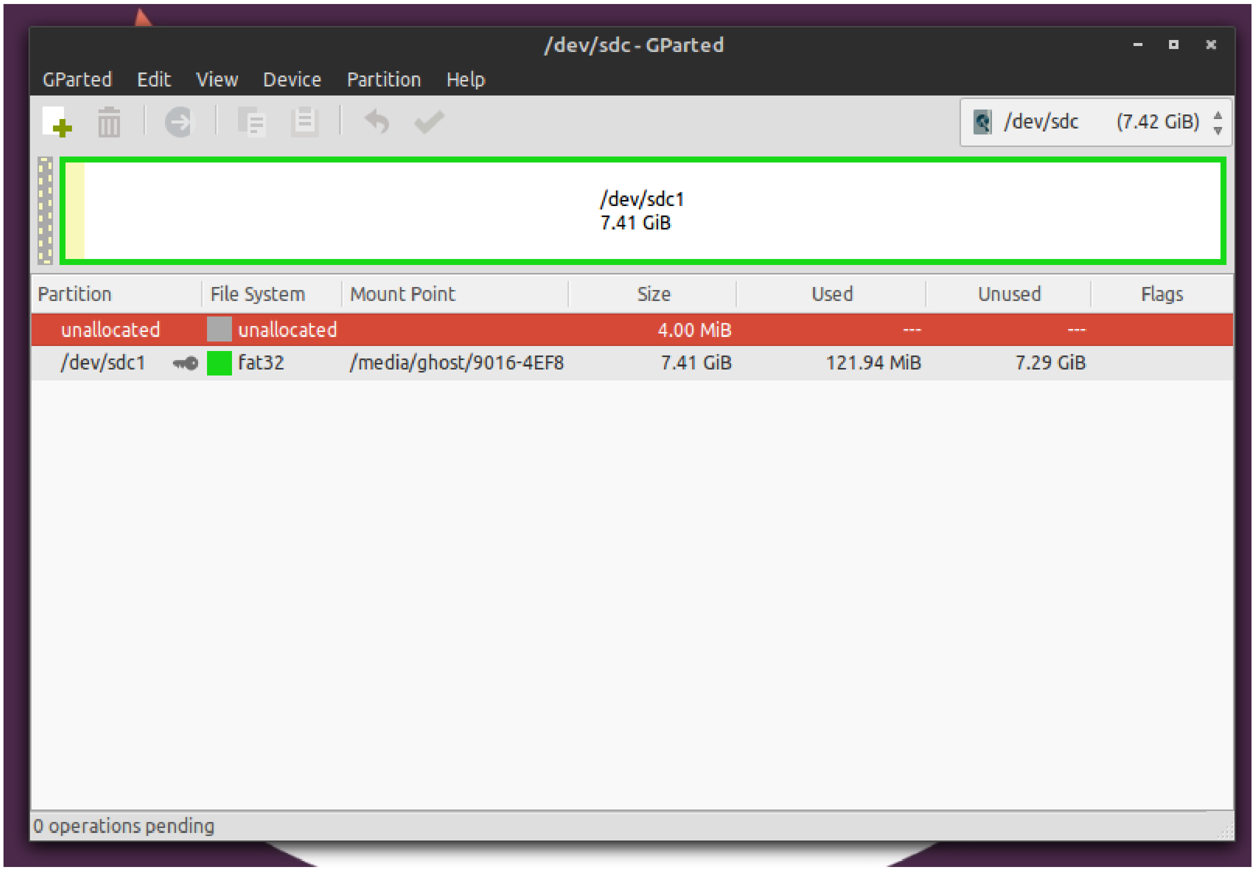
Table of Contents

Draft Jewelry SD Card Investigation

Forensic Acquisition / Examination Preparation

On today's date, 7 February 2016, I began the forensic acquisition, imaging, and examination of the confiscated SD card. Prior to acquisition, I took one front and one back photo of the SD card with my Nikon Coolpix L340 Digital Camera. As can be seen in the front photo on the left, this is a SanDisk SDHC, or Secure Digital High Capacity, SD card with 8GB of storage capacity and colored blue. As can be seen in the back photo on the right, this SD card was made in China and bares the serial number BI0827813483G. The back appears to be translucent while the front is opaque, as per the norm for SanDisk SD cards. The write-block lock is disengaged. The SD cards appears a little dirty indicating it's been used, but it shows no visible markings or damage indicating it's been under good care.

I placed the SD card into a transparent, SD card cartridge, placed the cartridge in my tech bag, placed my tech bag in my car, and drove straight home to conduct the forensic analysis. Once home, I removed the SD card from the cartridge and I enabled the write-block lock on the SD card, but I wanted to ensure write-blocking was enabled with community-accepted tools of the computer forensics field. I entered the SD card into my UltraBlock USB 3.0 Forensic Card Reader and Writer with read-only mode enabled and plugged the UltraBlock into one of my workstation’s USB 3.0 ports. I opened up GParted to find the SD card (it was mounted at “/dev/sdc” (without quotes)) and to unsure it was unmounted.



Partition	File System	Mount Point	Size	Used	Unused	Flags
unallocated	▨ unallocated		4.00 MiB	---	---	
/dev/sdc1	🟩 fat32	/media/ghost/9016-4EF8	7.41 GiB	121.94 MiB	7.29 GiB	

0 operations pending

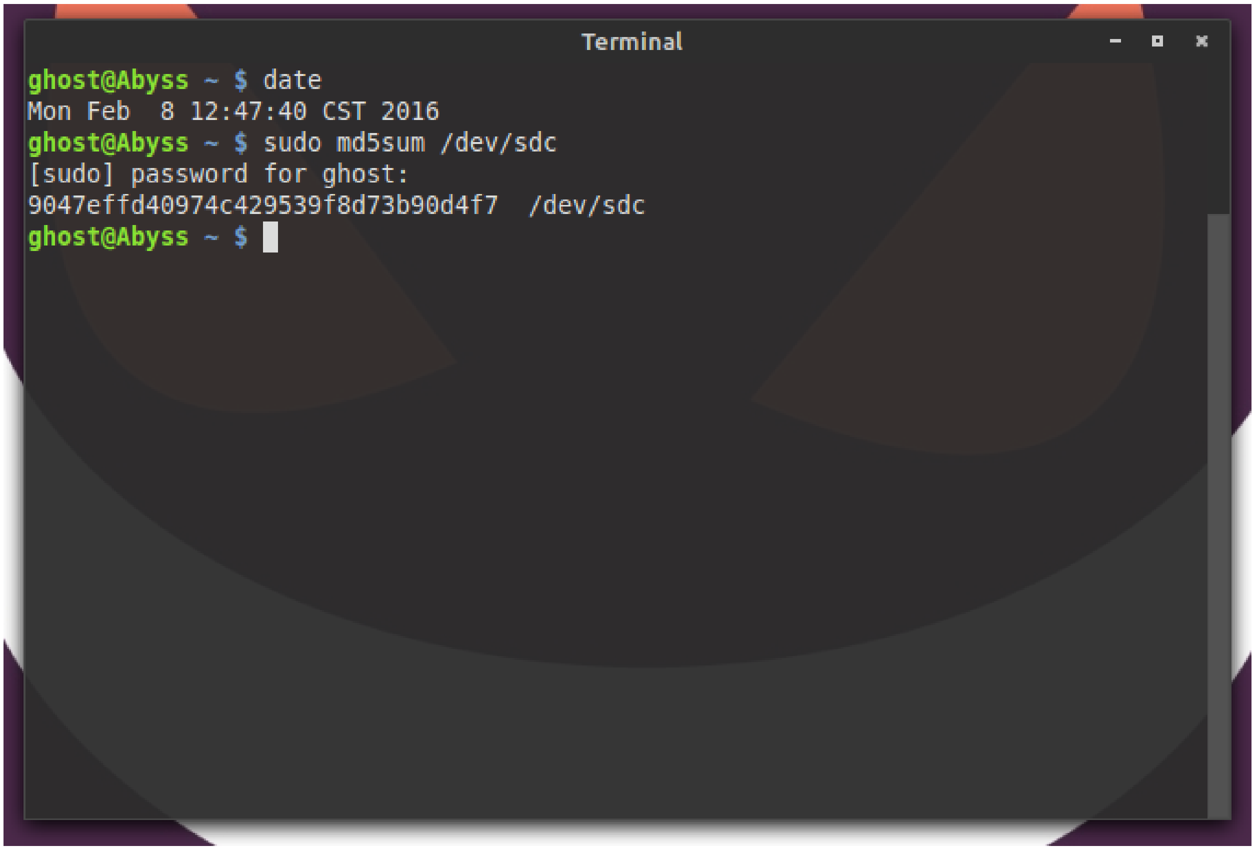
I then opened up the terminal and entered the following to check the MD5 hash value and time of checking hash value:

```
date

sudo md5sum /dev/sdc
```

The terminal responded with the hash value as seen in the screenshot below:

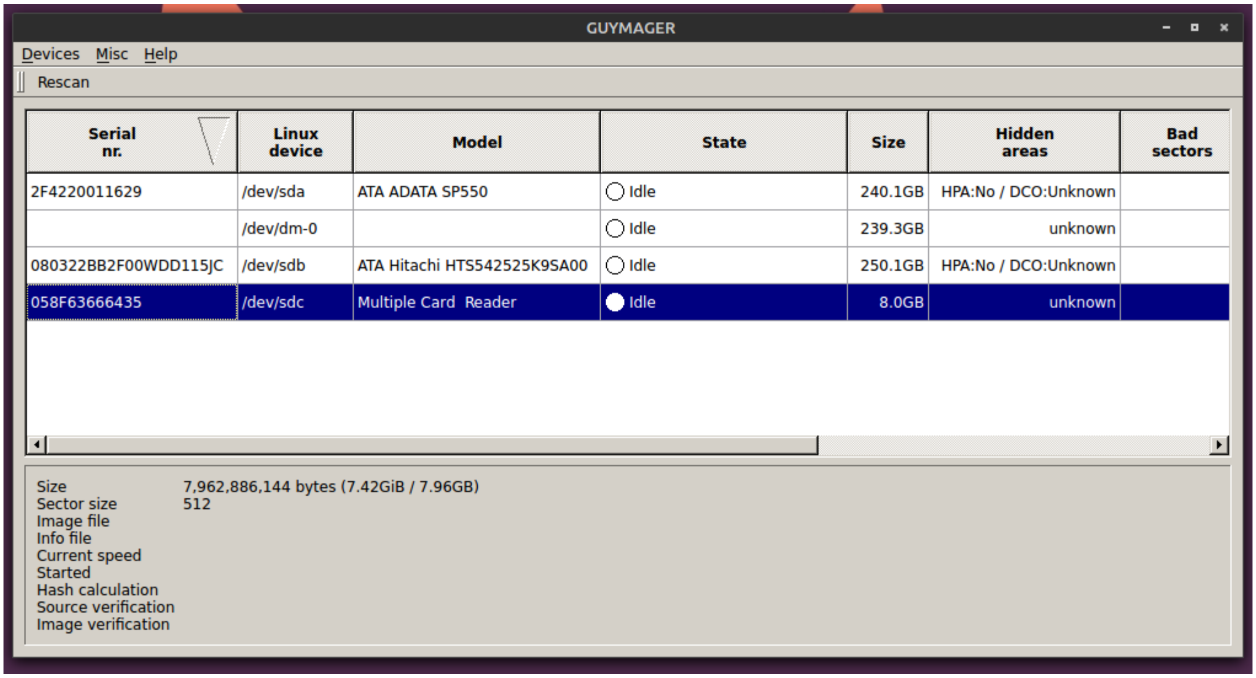
```
9047effd40974c429539f8d73b90d4f7
```



```
ghost@Abyss ~ $ date
Mon Feb  8 12:47:40 CST 2016
ghost@Abyss ~ $ sudo md5sum /dev/sdc
[sudo] password for ghost:
9047effd40974c429539f8d73b90d4f7  /dev/sdc
ghost@Abyss ~ $ 
```

Imaging

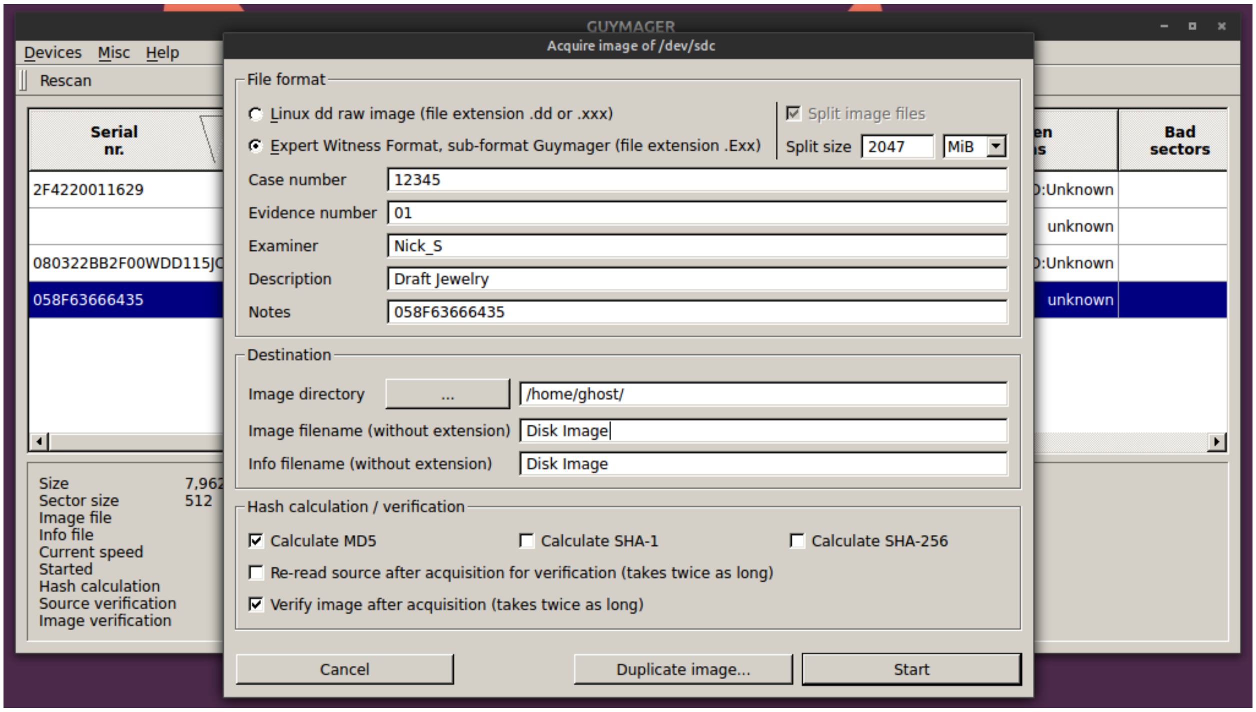
I mounted the partition and opened up Guymager. I selected the SD card mounted at "/dev/sdc" (without quotes), right-clicked, and clicked Acquire image.



Serial nr.	Linux device	Model	State	Size	Hidden areas	Bad sectors
2F4220011629	/dev/sda	ATA ADATA SP550	○ Idle	240.1GB	HPA:No / DCO:Unknown	
	/dev/dm-0		○ Idle	239.3GB	unknown	
080322BB2F00WDD115JC	/dev/sdb	ATA Hitachi HTS542525K9SA00	○ Idle	250.1GB	HPA:No / DCO:Unknown	
058F63666435	/dev/sdc	Multiple Card Reader	● Idle	8.0GB	unknown	

Size	7,962,886,144 bytes (7.42GiB / 7.96GB)
Sector size	512
Image file	
Info file	
Current speed	
Started	
Hash calculation	
Source verification	
Image verification	

I left the default file format at Expert Witness Format, or Exx, where the number of disk images created would change the xx to that number. Since this is my first disk image for the day, the disk image will be saved as E01. I then added information to the image as seen in the screenshot below. The Case Number is 12345, the Evidence number is 01, the examiner, me, is Nick_S, the description is Draft Jewelry SD Card, and the Image filename is Disk Image.



Acquire image of /dev/sdc

File format

○ Linux dd raw image (file extension .dd or .xxx)

● Expert Witness Format, sub-format Guymager (file extension .Exx)

☑ Split image files

Split size 2047 MiB

Case number	12345
Evidence number	01
Examiner	Nick_S
Description	Draft Jewelry
Notes	058F63666435

Destination

Image directory	/home/ghost/
Image filename (without extension)	Disk Image
Info filename (without extension)	Disk Image

Hash calculation / verification

☑ Calculate MD5 □ Calculate SHA-1 □ Calculate SHA-256

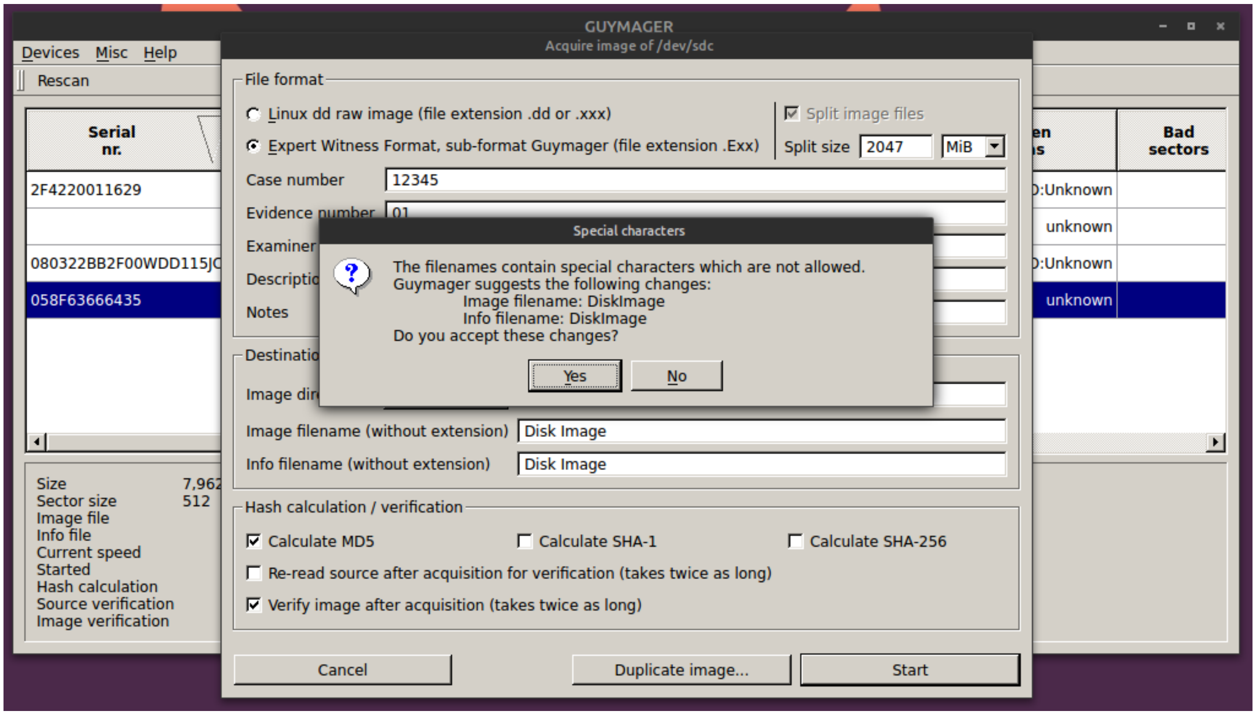
□ Re-read source after acquisition for verification (takes twice as long)

☑ Verify image after acquisition (takes twice as long)

Serial nr.	...
2F4220011629	):Unknown
	unknown
080322BB2F00WDD115JC	):Unknown
058F63666435	unknown

Size 7,962
Sector size 512
Image file
Info file
Current speed
Started
Hash calculation
Source verification
Image verification

Guymager changed file name to DiskImage.

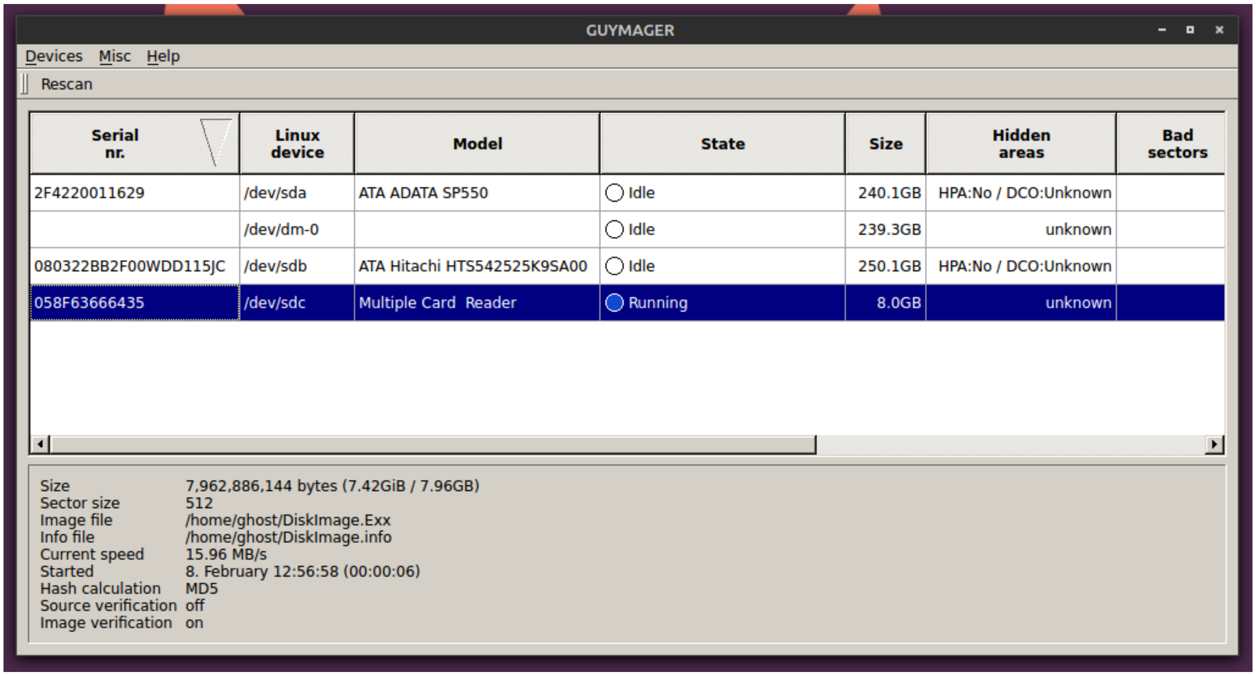


Acquire image of /dev/sdc

Special characters

The filenames contain special characters which are not allowed.
Guymager suggests the following changes:
Image filename: DiskImage
Info filename: DiskImage
Do you accept these changes?

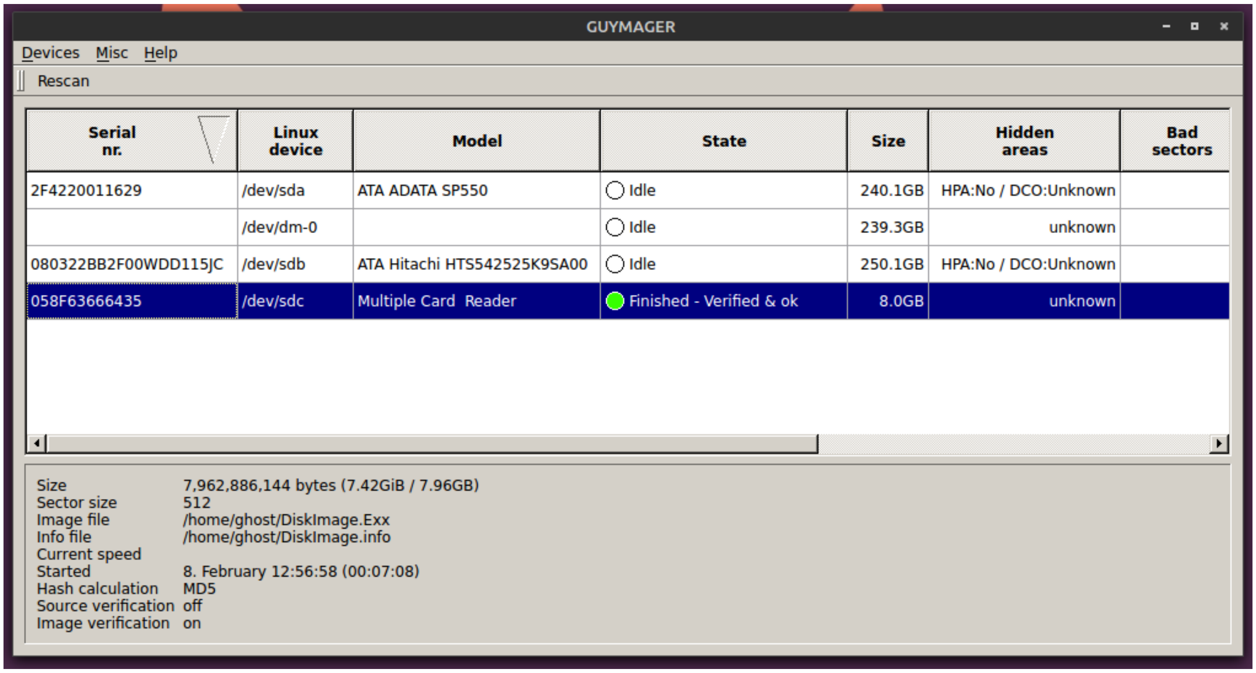
I clicked Yes and the imaging process started.



Serial nr.	Linux device	Model	State	Size	Hidden areas	Bad sectors
2F4220011629	/dev/sda	ATA ADATA SP550	○ Idle	240.1GB	HPA:No / DCO:Unknown	
	/dev/dm-0		○ Idle	239.3GB	unknown	
080322BB2F00WDD115JC	/dev/sdb	ATA Hitachi HTS542525K9SA00	○ Idle	250.1GB	HPA:No / DCO:Unknown	
058F63666435	/dev/sdc	Multiple Card Reader	● Running	8.0GB	unknown	

```
Size                 7,962,886,144 bytes (7.42GiB / 7.96GB)
Sector size          512
Image file           /home/ghost/DiskImage.Exx
Info file            /home/ghost/DiskImage.info
Current speed        15.96 MB/s
Started              8. February 12:56:58 (00:00:06)
Hash calculation     MD5
Source verification  off
Image verification   on
```

After 7 minutes, it completed creating an image of the SD card.



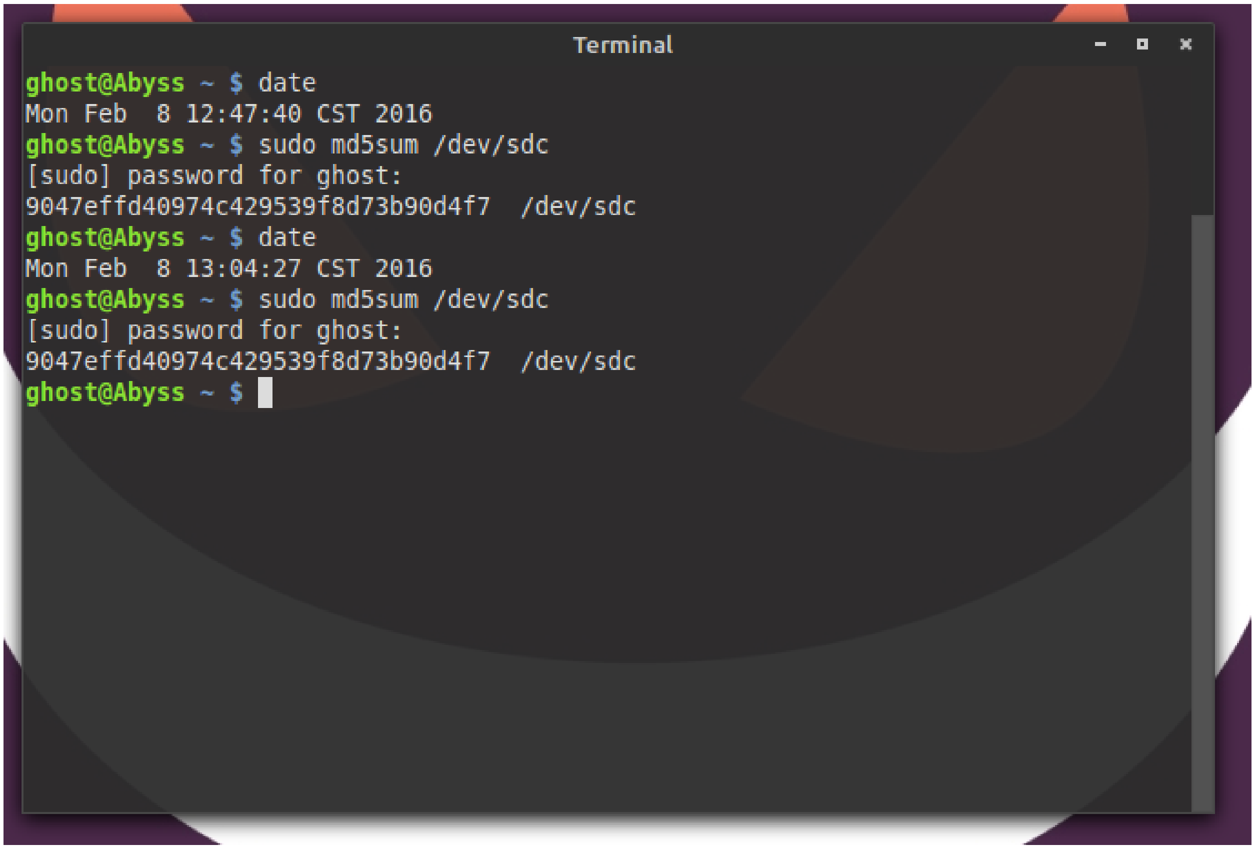
Serial nr.	Linux device	Model	State	Size	Hidden areas	Bad sectors
2F4220011629	/dev/sda	ATA ADATA SP550	○ Idle	240.1GB	HPA:No / DCO:Unknown	
	/dev/dm-0		○ Idle	239.3GB	unknown	
080322BB2F00WDD115JC	/dev/sdb	ATA Hitachi HTS542525K9SA00	○ Idle	250.1GB	HPA:No / DCO:Unknown	
058F63666435	/dev/sdc	Multiple Card Reader	● Finished - Verified & ok	8.0GB	unknown	

```
Size                 7,962,886,144 bytes (7.42GiB / 7.96GB)
Sector size          512
Image file           /home/ghost/DiskImage.Exx
Info file            /home/ghost/DiskImage.info
Current speed
Started              8. February 12:56:58 (00:07:08)
Hash calculation     MD5
Source verification  off
Image verification   on
```

I accessed the terminal previously used and entered the following to check the MD5 hash value and time of checking hash value as seen in the screenshot below:

```
date
```

sudo md5sum /dev/sdc



```
ghost@Abyss ~ $ date
Mon Feb  8 12:47:40 CST 2016
ghost@Abyss ~ $ sudo md5sum /dev/sdc
[sudo] password for ghost:
9047effd40974c429539f8d73b90d4f7  /dev/sdc
ghost@Abyss ~ $ date
Mon Feb  8 13:04:27 CST 2016
ghost@Abyss ~ $ sudo md5sum /dev/sdc
[sudo] password for ghost:
9047effd40974c429539f8d73b90d4f7  /dev/sdc
ghost@Abyss ~ $
```

Guymager did NOT change the hash values or violate the integrity of the SD card during the imaging process as seen in the SD MD5 Hash Check screenshots. I removed the SD card from my UltraBlock, removed the USB connection between my laptop, disabled the write-block lock on the SD card, placed it back in the cartridge, and placed the cartridge back in my tech bag. From this point forward, the investigation of the SD card data would only require the image taken and not the physical copy.

Examination Process / Report

Visual documentation for the examination process can be found in the Investigator Photos directory of the Evidence directory provided; they are labeled under Autopsy. The only screenshots taken during examination with Autopsy are the extraction screenshots of the images found on the SD card in place of the extracted photos shown on linked below.

1. I opened up a new terminal instance and ran Autopsy [screenshot]:

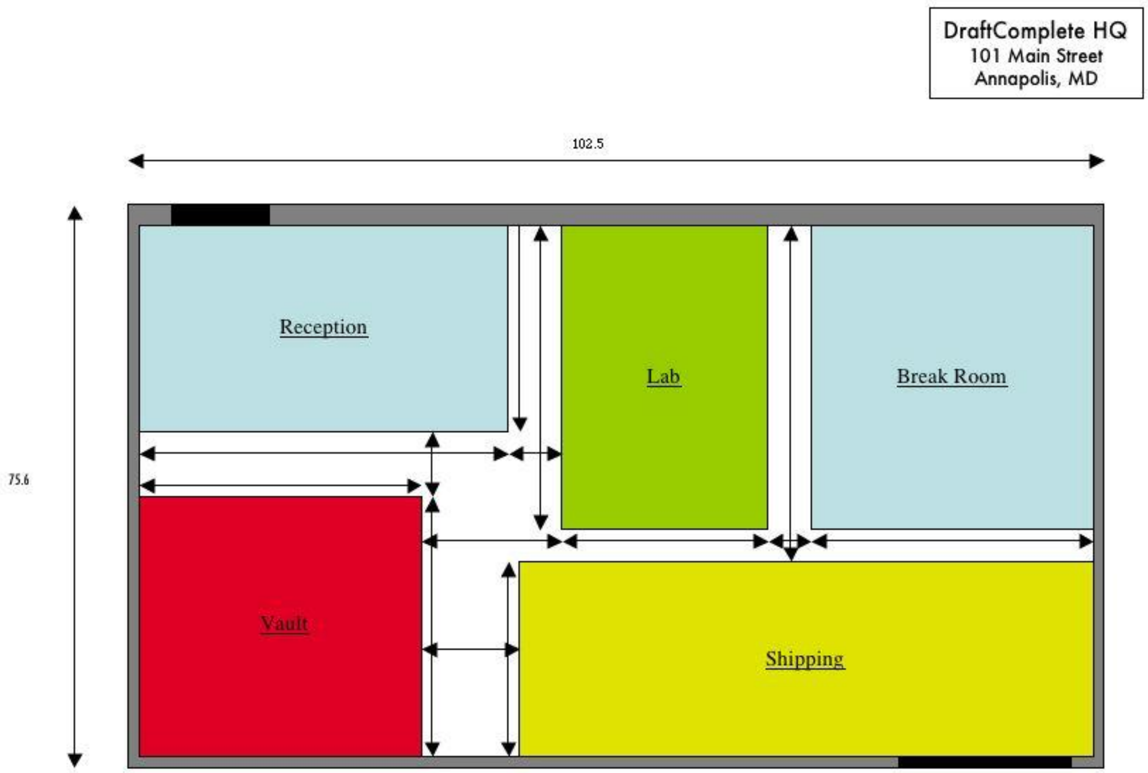
```
sudo autopsy
```

2. I opened up Firefox web browser and went to "localhost:9999/autopsy" (without quotes) [screenshot].
3. I clicked new case and added the same information as the SD image; Case Number is 12345, the description is Draft Jewelry SD Card, and the examiner/investigator is me, Nick_S [screenshot].
4. I clicked New Case, verified my name was selected, and click Add Host [screenshot].
5. I left host1 as the default host name and clicked Add Host again [screenshot].
6. I clicked Add Image at Adding Hosting screen [screenshot].
7. I clicked Add Image File [screenshot].
8. I entered the following in the image field I clicked copy in case of error with symlink [screenshot]:

```
/home/ghost/DiskImage.E01
```

9. I left the mount point at C: and changed the file system to FAT16; then clicked Add [screenshot].
10. I clicked OK at Testing partitions screen [screenshot].
11. I clicked the copy mounted at C: and clicked Analyze [screenshot].
12. I clicked the File Analysis tab in File Browsing Mode [screenshot].

Directory – Root. In the root directory, I clicked the "$FAT1" volume (without quotes) and clicked Report under Hex. The metadata offered no information beyond ASCII characters in metadata and mostly unallocated space [screenshot][screenshot]. This was the same for the “$FAT2” volume (without quotes) [screenshot][screenshot]. I clicked the MBR volume, clicked Report under Hex, and viewed the metadata to be a partition in F16 format [screenshot][screenshot]. These were the three volumes found in root directory. In addition, I found a file named “NIKON001.DSC” (without quotes). The Hex report generated no information, but the title indicates that the SD card is an external memory card for a Nikon digital camera [screenshot]. I was successfully able to cover two deleted photos with a JPG and TIF format. Both photos were titled “LUEPR~1” (without quotes) and consisted of blueprints to the Draft Jewelry store as indicated in the photo below.



In addition, I found two directories in the root directory. One was labeled “$OrphanFiles” (without quotes) and was empty. The other was labeled DCIM, a common folder in digital cameras, camera phones, smartphones, and other mobile devices with cameras, which stands for Digital Camera Images.

Directory – DCIM. The DCIM directory consisted of three directories. “..” (without quotes) brought me back to the previous directory and “.” (without quotes) brought me to the DCIM directory. The third directory is “100NIKON” (without quotes) [screenshot].

Directory – 100NIKON. The 100NIKON directory consisted of two directories. “..” (without quotes) brought me back to the previous directory and “.” (without quotes) brought me to the 100NIKON directory. In this directory, there was one file and there were five deleted files. The file not deleted was a TIF photo labeled “DSCN2065.TIF” (without quotes) of a gold necklace as seen below.

Four of the five deleted files were JPG photos. “SCN2066.JPG” (without quotes) was a deleted photo of a white pearl necklace, “SCN2067.JPG” (without quotes) was a deleted photo of a gold bracelet, “SCN2068.JPG” (without quotes) was a deleted photo of a gold ring with a dark-colored stone, and “SCN2069.JPG” (without quotes) was a deleted photo of a gold ring with a light-colored stone. These photos were extracted and can be found in the Extracted Photos directory of the Evidence directory provided; they contain their original names. The last deleted file is an NFO.TXT file of the photos taken in the Nikon digital camera and lists the metadata for said photos. This file states that the camera used was a Nikon Coolpix 5700 Digital Camera, that most of the photo settings were left at default, that the shutter and aperture varied on each photo, that the photo resolution was 2560x1920, and that all five photos were taken on 04 March 2004 between 9:12 and 9:15 [screenshot][screenshot][screenshot].

Conclusion

The facts from this investigation are as follows. The SD card is an 8GB San Disk SDHC card with a 122MB partition. It has been used in a Nikon Coolpix 5700 Digital Camera to take five photos of jewelry including gold rings (both JPG format), a gold bracelet (JPG format), a gold necklace (TIF format), and a pearl necklace (JPG format). The previously mentioned photos, excluding the gold necklace, were deleted. The previously mentioned photos were taken on 04 March 2004 between 9:12 and 9:15 and had resolutions of 2560x1920. The SD card also contained two deleted photos of blueprints to Draft Jewelry; one in JPG format and one in TIF format.

References

Garnett, B. (2010, Aug. 25). Intro to Report Writing for Digital Forensics [Web log]. Retrieved from https://digital-forensics.sans.org/blog/2010/08/25/intro-report-writing-digital-forensics/

Jarocki, J. (2009, Jun 18). Forensics 101: Acquiring an Image with FTK Imager [Web log]. Retrieved from https://digital-forensics.sans.org/blog/2009/06/18/forensics-101-acquiring-an-image-with-ftk-imager/