DATA ACQUISITION REPORT

By: Team 6 -Lam Luong, William Zaourbekov, Lima Sin, Sam Zheng

CASE #: CIS 481-006
SUSPECT NAME: BAD HACKER
LOCATION SEIZED: CAL POLY POMONA
COLLECTED BY: PROFESSOR TOBI WEST

Abstract

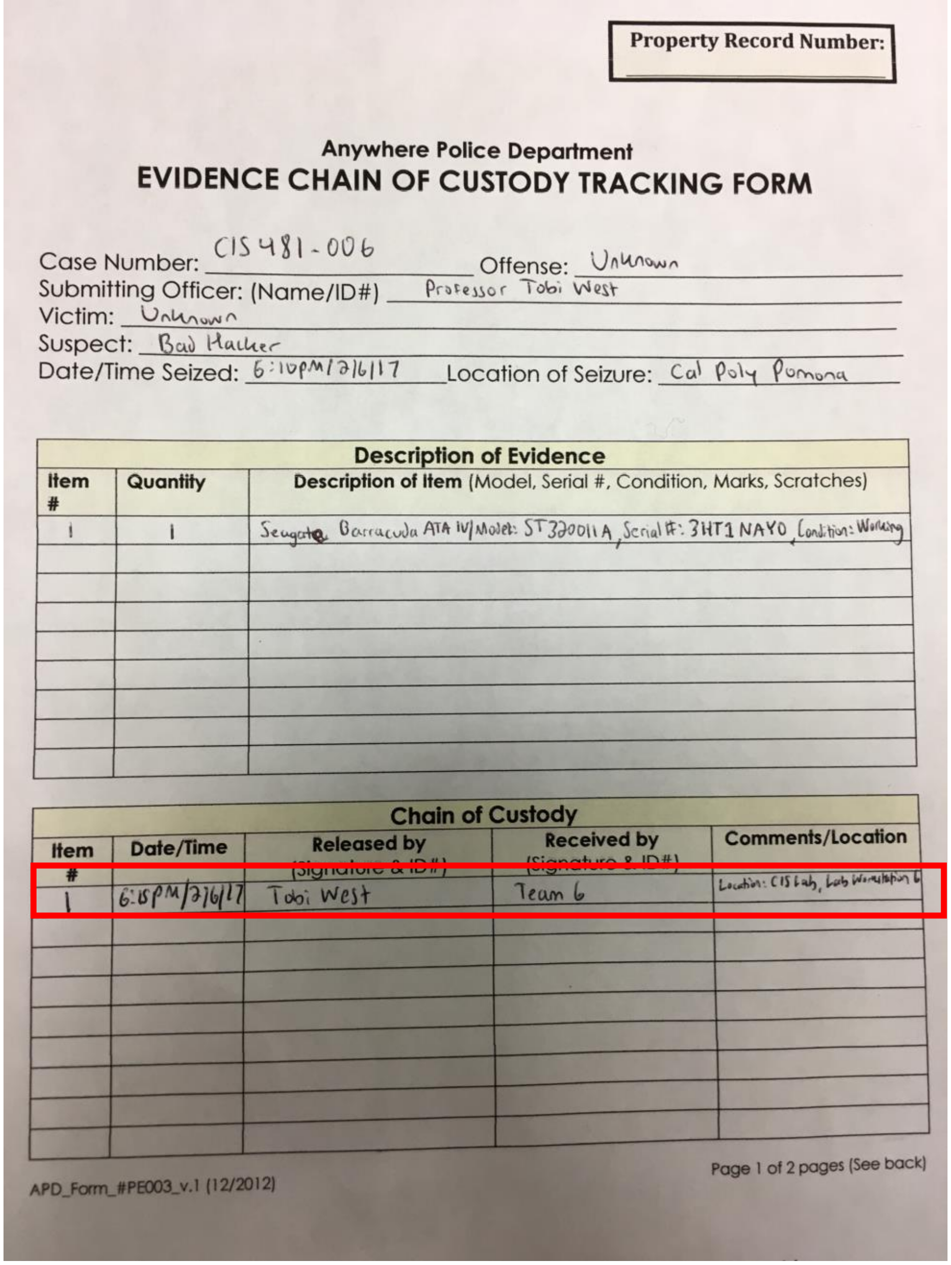
This report outlines the chain of custody we used to systematically acquire the evidence, create and validate a bit stream image (exact copy) of the Hard Disk Drive (HDD, Storage Device), and lastly how we transferred custody of the evidence once we were done with creating the bit stream image of the Hard Drive.

Table of Contents

Chain of custody form filler page

Acquisition of the Evidence

We began the preparation for our data acquisition by first having Professor West sign off on our "Evidence Chain of Custody Tracking Form." as shown below in *Photo 1*. This form is especially important to ensure that we keep track of the what, who, and where of the evidence. Without this, the evidence is more than likely going to be inadmissible in court.



Property Record Number: ____

Anywhere Police Department

EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: CIS 481-006 Offense: Unknown
Submitting Officer: (Name/ID#) Professor Tobi West
Victim: Unknown
Suspect: Bad Hacker
Date/Time Seized: 6:10pM/2/6/17 Location of Seizure: Cal Poly Pomona

Description of Evidence

Item #	Quantity	Description of Item (Model, Serial #, Condition, Marks, Scratches)
1	1	Seagate Barracuda ATA IV/Model: ST320011A, Serial #: 3HT1 NAY0, Condition: Working

Chain of Custody

Item #	Date/Time	Released by (Signature & ID#)	Received by (Signature & ID#)	Comments/Location
1	6:15PM/2/6/17	Tobi West	Team 6	Location: CIS Lab, Lab Workstation 6

APD_Form_#PE003_v.1 (12/2012)

Page 1 of 2 pages (See back)

Photo 1: Chain of custody form documenting the transfer of the evidence from Tobi West to Team 6. We later obtained her signature as seen in Photo 21.

The hard disk drive obtained is as described:

Manufacturer: Seagate Barracuda ATA IV
Model: ST320011A
Serial: 3HT1NAY0
Condition: Working Condition with no visible damages

Photos 2, 3, & 4 shown below are of the front & back of the HDD released by Tobi West with a phone for scale and to time stamp it.

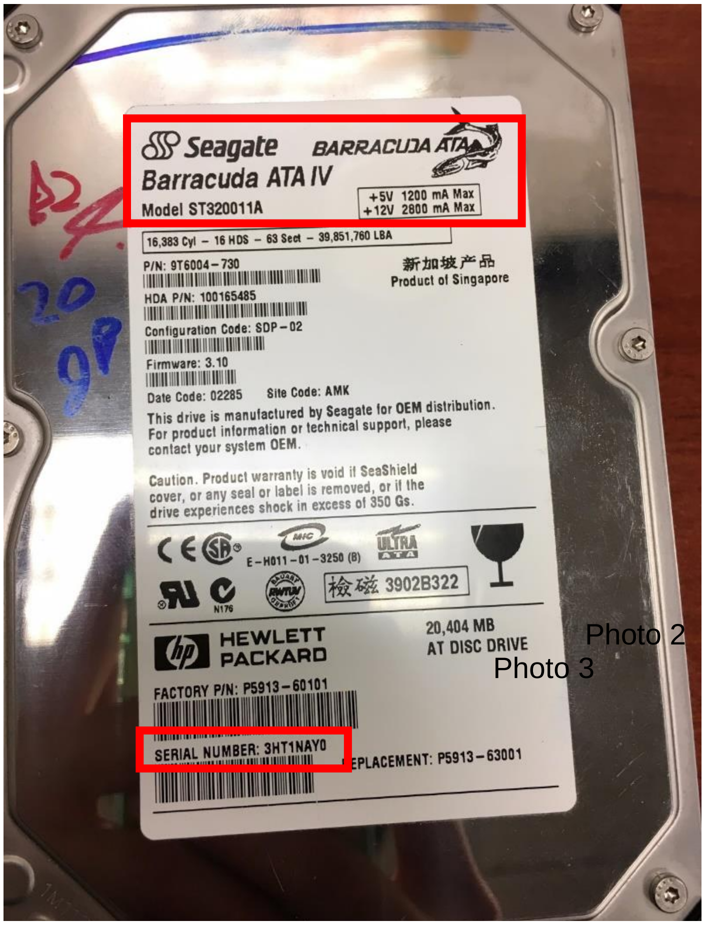

Seagate
BARRACUDA ATA
Barracuda ATA IV
Model ST320011A
+5V 1200 mA Max
+12V 2800 mA Max
16,383 Cyl – 16 HDS – 63 Sect – 39,851,760 LBA
P/N: 9T6004–730
新加坡产品
Product of Singapore
HDA P/N: 100165485
Configuration Code: SDP–02
Firmware: 3.10
Date Code: 02285 Site Code: AMK
This drive is manufactured by Seagate for OEM distribution. For product information or technical support, please contact your system OEM.
Caution. Product warranty is void if SeaShield cover, or any seal or label is removed, or if the drive experiences shock in excess of 350 Gs.
E–H011–01–3250 (B)
ULTRA ATA
檢磁 3902B322
HEWLETT PACKARD
20,404 MB AT DISC DRIVE
FACTORY P/N: P5913–60101
SERIAL NUMBER: 3HT1NAY0
REPLACEMENT: P5913–63001
Photo 2
Photo 3

Photo 2: Front of the Hard Drive.

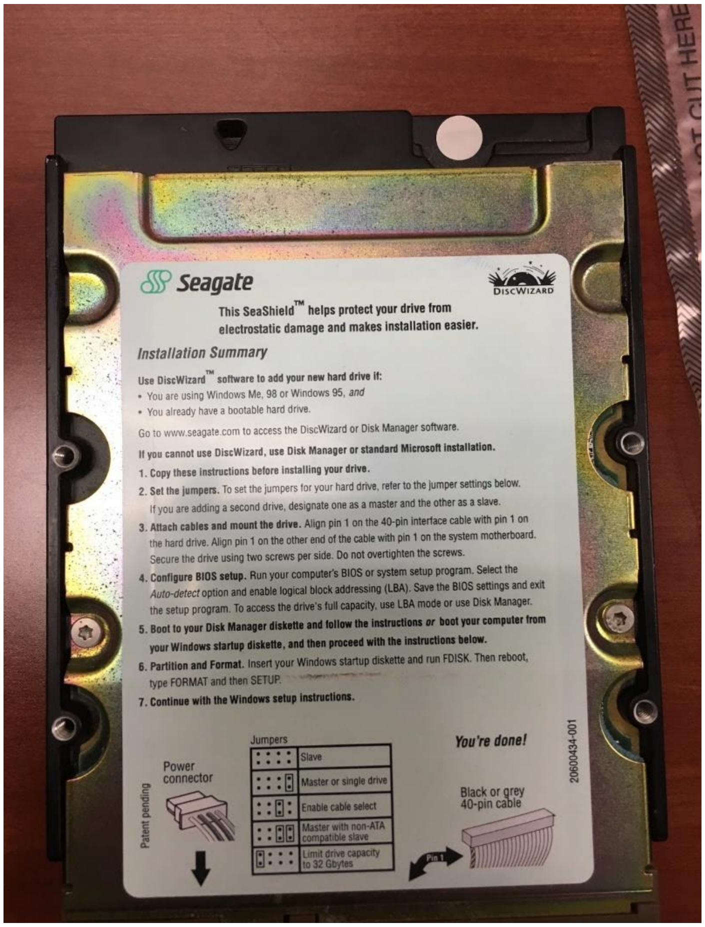

Seagate
DiscWizard
This SeaShield™ helps protect your drive from electrostatic damage and makes installation easier.
Installation Summary
Use DiscWizard™ software to add your new hard drive if:
You are using Windows Me, 98 or Windows 95, and
You already have a bootable hard drive.
Go to www.seagate.com to access the DiscWizard or Disk Manager software.
If you cannot use DiscWizard, use Disk Manager or standard Microsoft installation.
1. Copy these instructions before installing your drive.
2. Set the jumpers.
3. Attach cables and mount the drive.
4. Configure BIOS setup.
5. Boot to your Disk Manager diskette and follow the instructions or boot your computer from your Windows startup diskette, and then proceed with the instructions below.
6. Partition and Format.
7. Continue with the Windows setup instructions.
You're done!
Jumpers
Slave
Master or single drive
Enable cable select
Master with non-ATA compatible slave
Limit drive capacity to 32 Gbytes
Power connector
Black or grey 40-pin cable
Pin 1
Patent pending
20600434-001

Photo 3: Back of the Hard Drive.

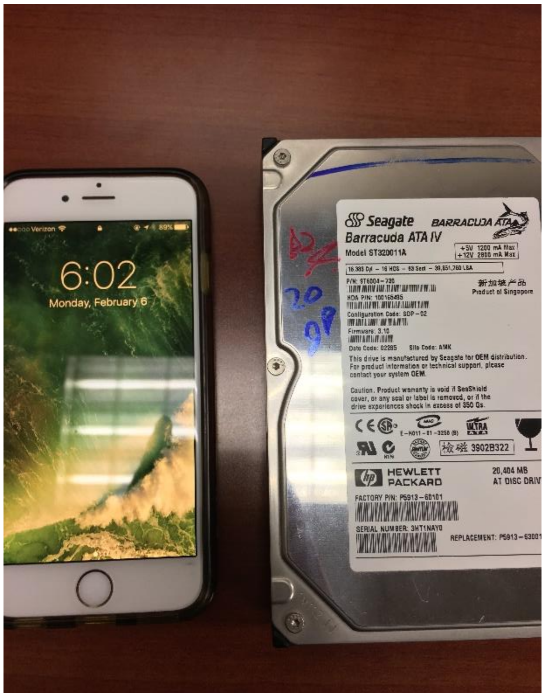


Photo 4: Hard Drive with Phone for Scale & Time.

Workstation Setup

After documenting the process of receiving the evidence, inspecting it for damages, taking pictures and getting a detailed description of it, we began to set up our workspace to prepare for the data acquisition. Below is a photo of the workstation with all the equipment used in the data acquisition process laid out. A time stamp is provided on the laptop to the left, and a phone is included to provide scale.

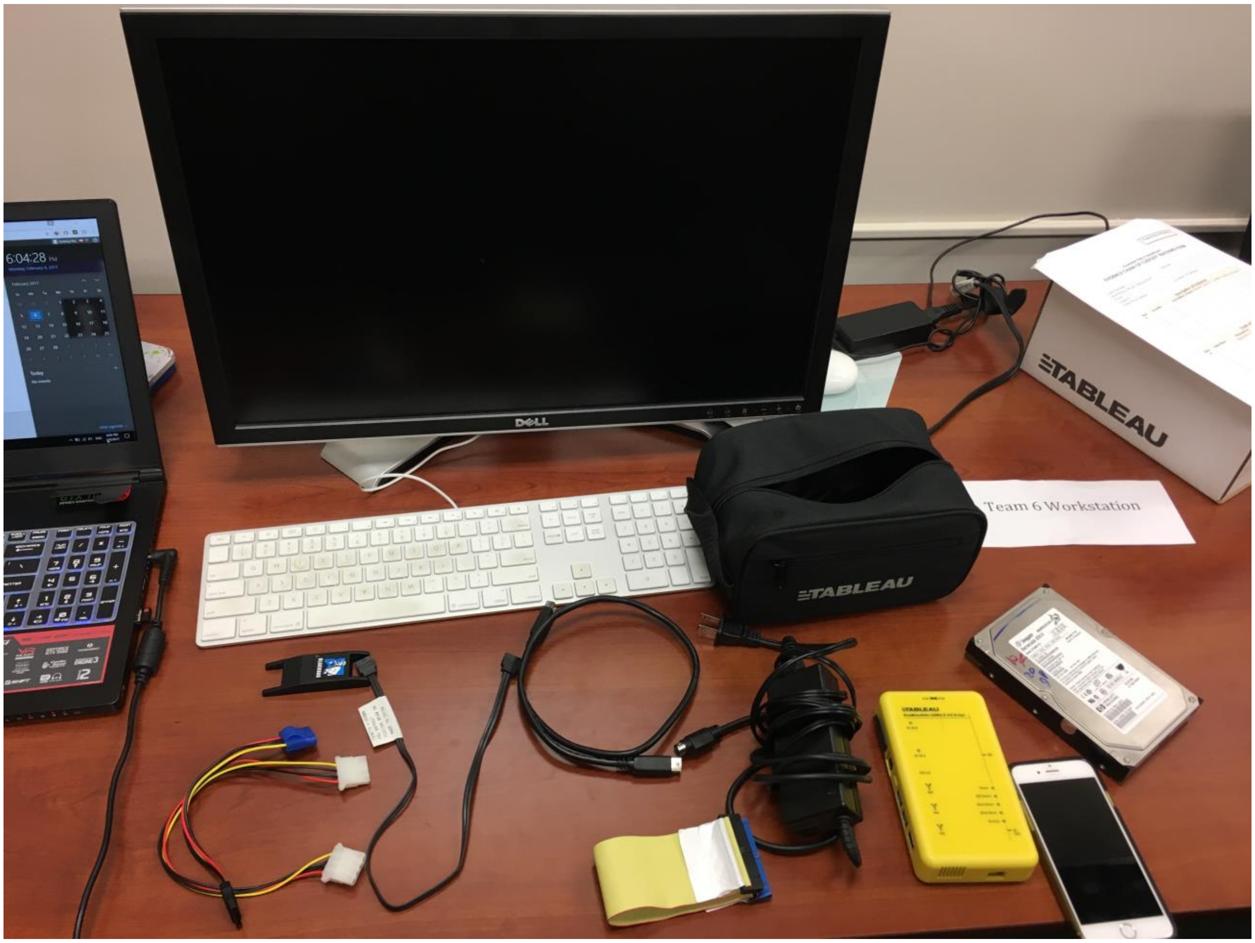


Photo 5: Workstation setup with all the equipment used laid out.

Assembling the Hardware

We then started to carefully connect all the cables to the correct ports as shown in the YouTube video on blackboard. After we finished plugging everything in, we connected the write blocker (a physical device that prevents modifications or edits to the evidence drive) to the computer on one end and the hard drive on the other. To finish the setup, we flipped the switch to turn on the write blocker. The setup we used with everything properly connected is shown on *Photo 6*.

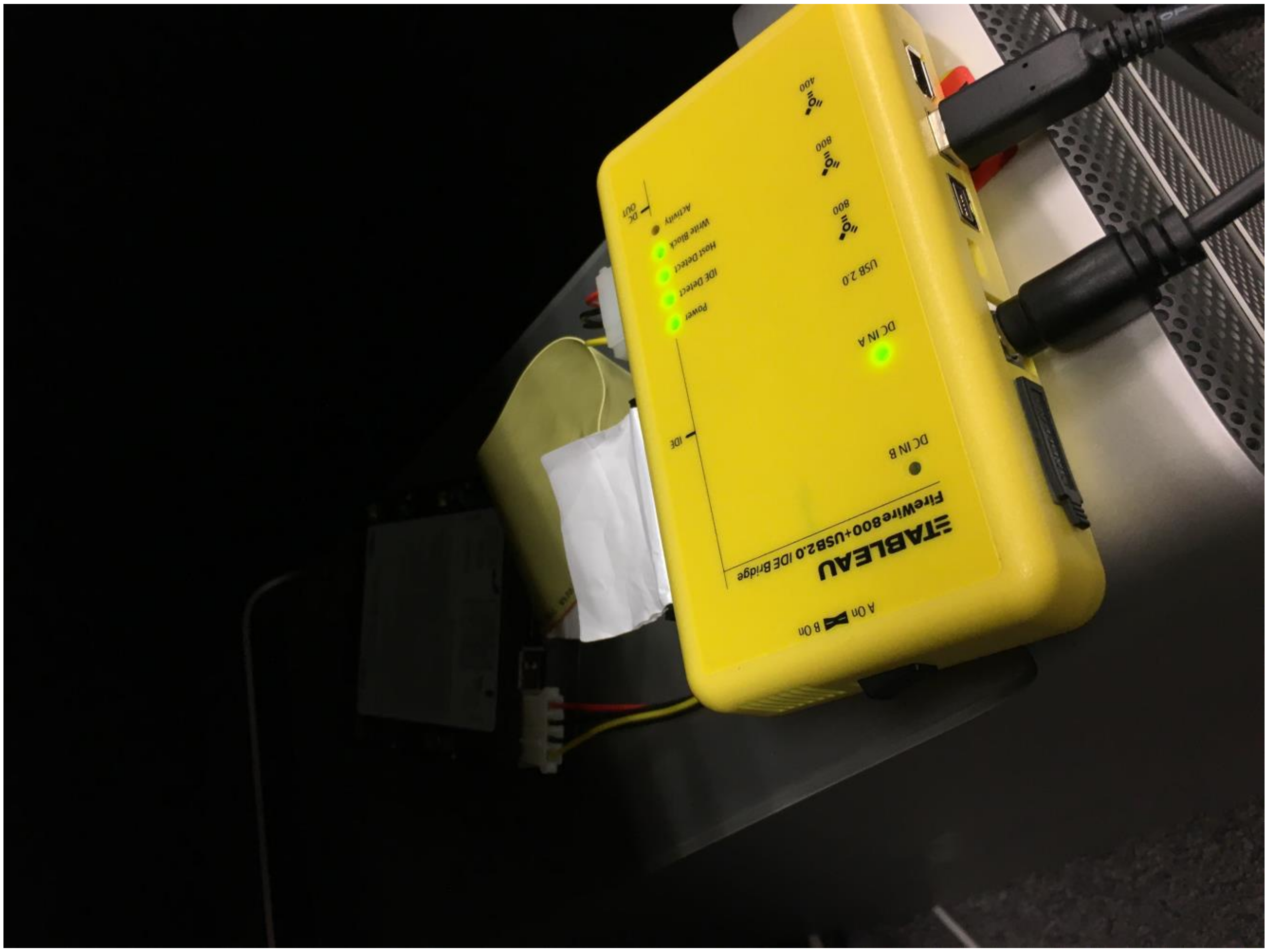
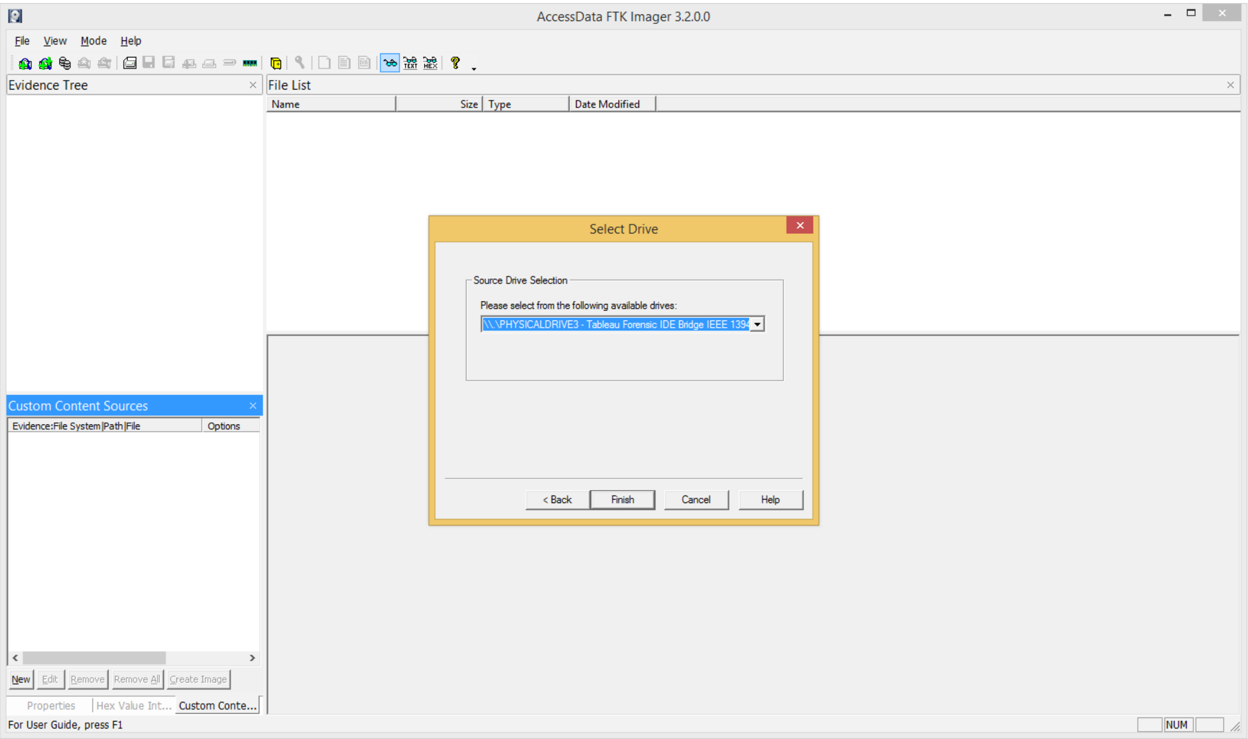


Photo 6: Full setup of the write blocker connected to the hard drive on one end and the computer on the other.

FTK Imager Software

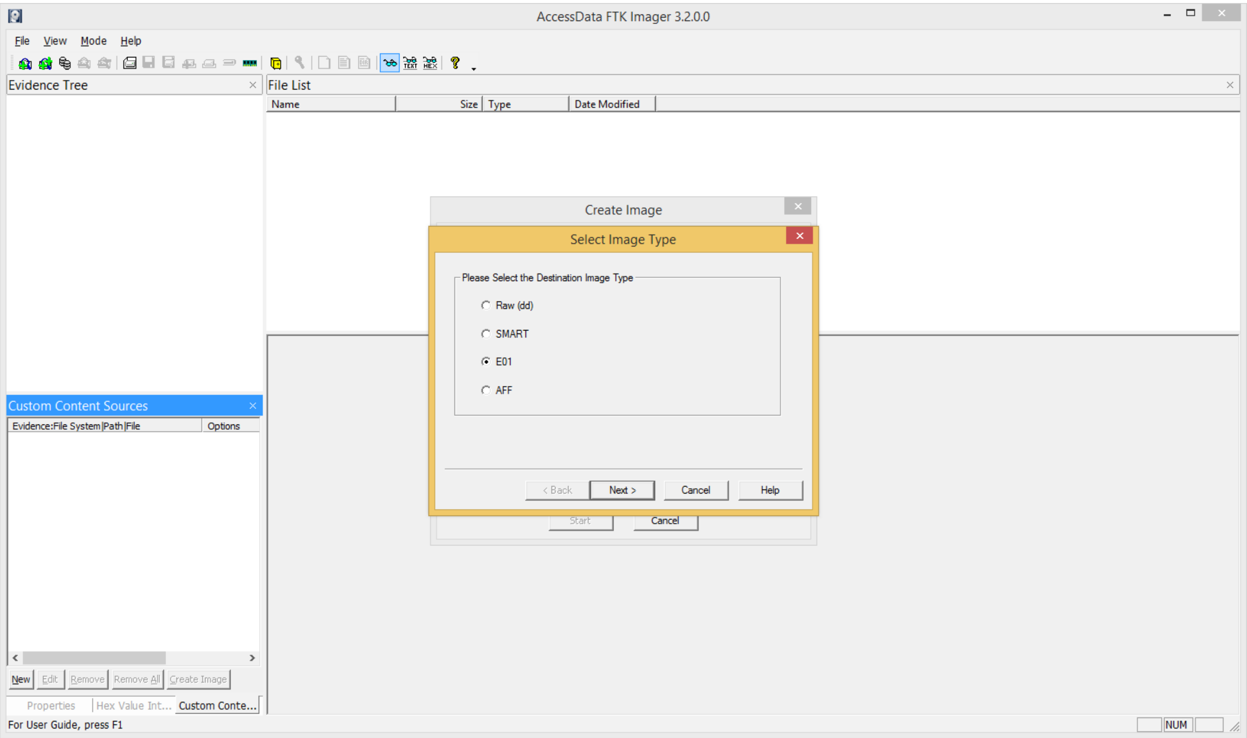
When we first logged in, we ran FTK and needed the Admin password so we had Professor West come over and input it for us. Afterwards, the following images are of the process, step by step that we went through from start to finish without omitting a single frame to create the bit stream image. This image is important because we will not want to be ever working with the evidence besides to create a copy. It is very dangerous to do so because if we were to change even a single bit on the drive, it may render the evidence inadmissible in court, therefore we will want to create a bit stream image to work on instead. We will do this using FTK software alongside a write blocker to prevent any alterations to the evidence, then afterwards validate the integrity of the bit stream image with the evidence HDD to ensure the integrity of the cloned image.



Source Drive Selection

Please select from the following available drives: \\.\PHYSICALDRIVE3 - Tableau Forensic IDE Bridge IEEE 1394

Photo 7: We first selected the physical device as the source drive to create the bit stream image.


AccessData FTK Imager 3.2.0.0
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
Create Image
Select Image Type
< Back Next > Cancel Help
Start Cancel
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value Int... Custom Conte...
For User Guide, press F1
NUM

Please Select the Destination Image Type

○ Raw (dd)
○ SMART
● E01
○ AFF

Photo 8: We selected “E01” as the destination image type so that we can import the image onto EnCase Forensic.

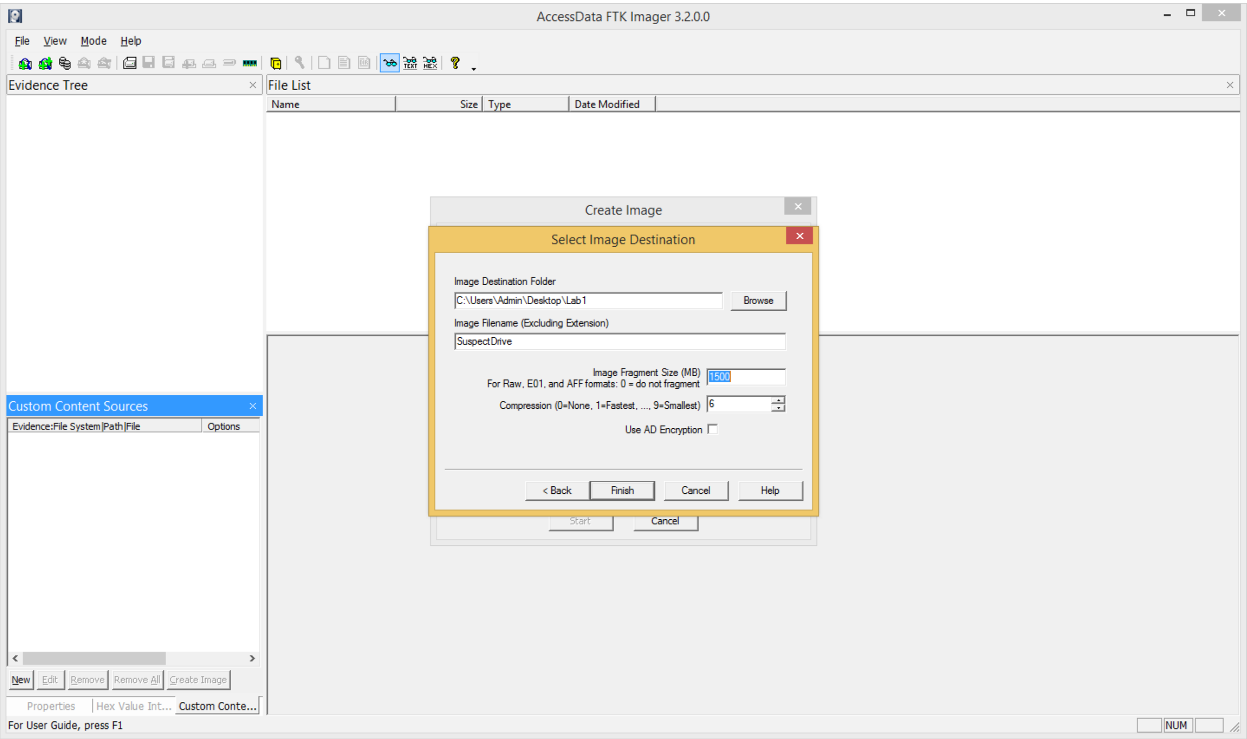

AccessData FTK Imager 3.2.0.0
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
Create Image
Select Image Destination
Browse
< Back Finish Cancel Help
Start Cancel
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value Int... Custom Conte...
For User Guide, press F1
NUM

Image Destination Folder: C:\Users\Admin\Desktop\Lab1

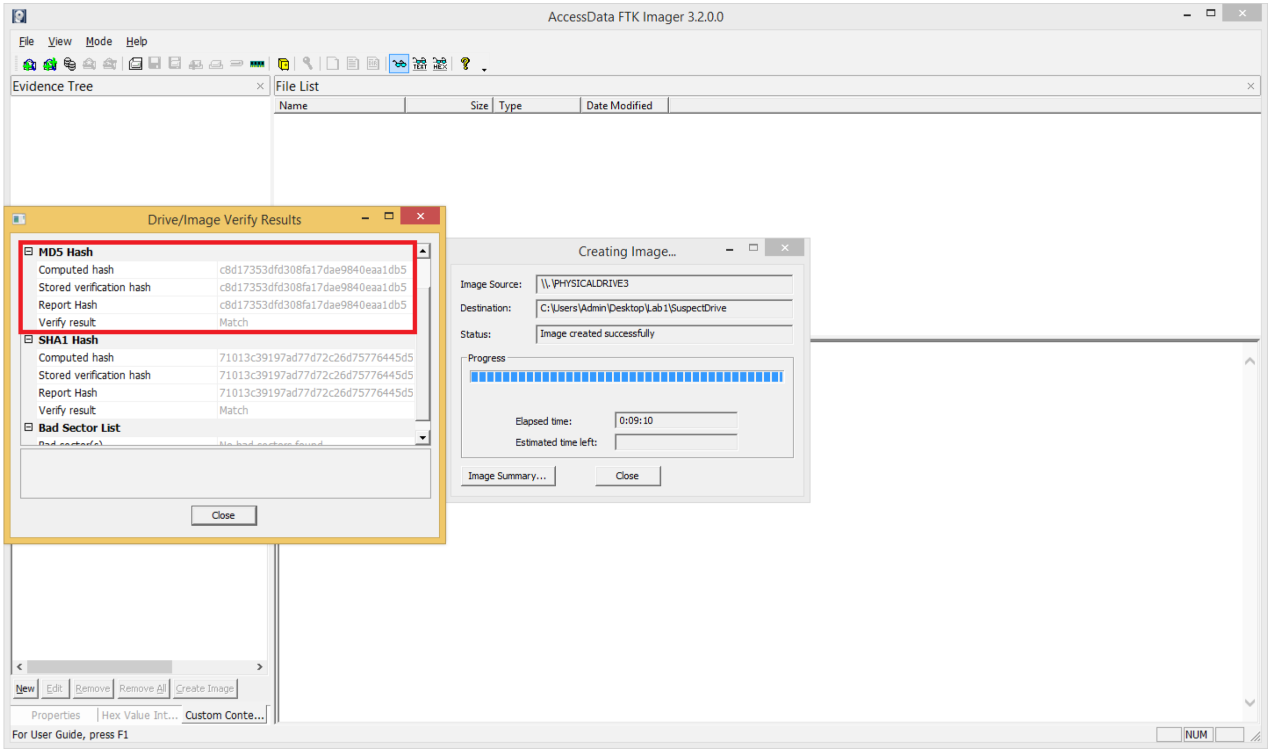
Image Filename (Excluding Extension): SuspectDrive

Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment: 1500

Compression (0=None, 1=Fastest, ..., 9=Smallest): 6

Use AD Encryption □

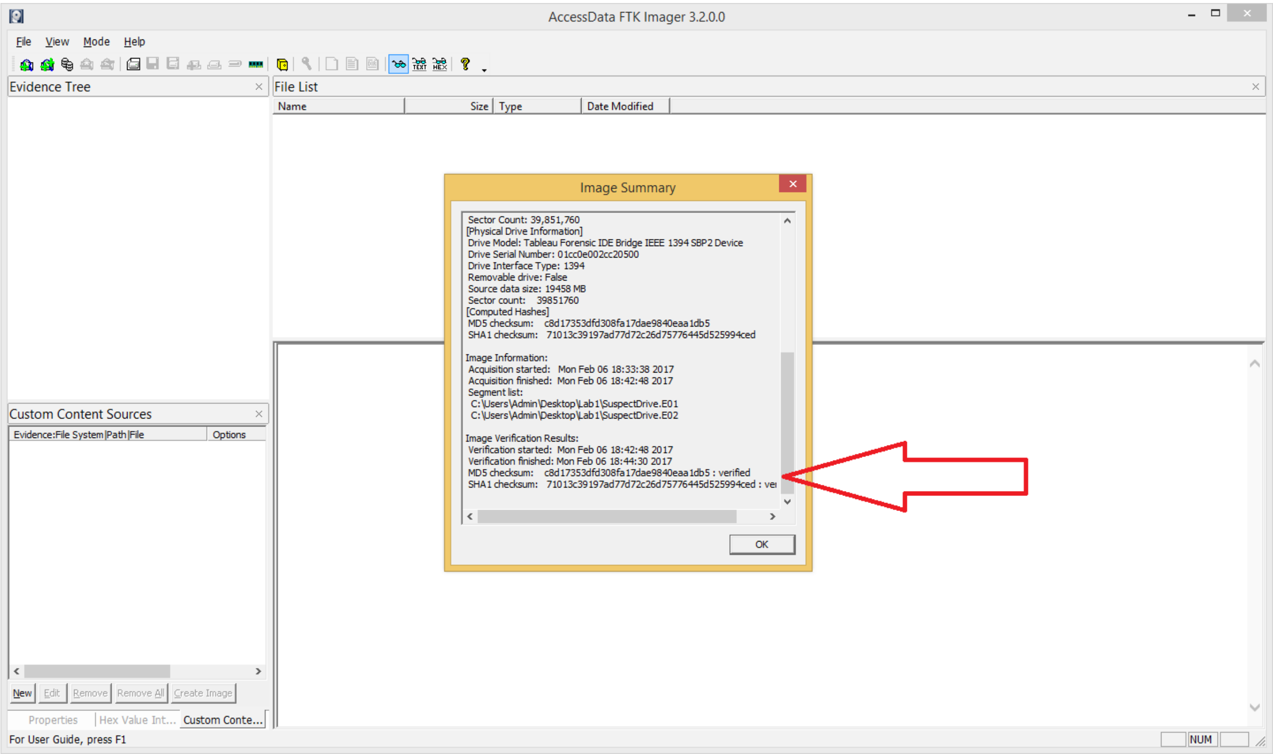
Photo 9: We are then about to start the process, with an image fragment size of 1500MB.



```
MD5 Hash
  Computed hash              c8d17353dfd308fa17dae9840eaa1db5
  Stored verification hash   c8d17353dfd308fa17dae9840eaa1db5
  Report Hash                c8d17353dfd308fa17dae9840eaa1db5
  Verify result              Match
SHA1 Hash
  Computed hash              71013c39197ad77d72c26d75776445d5
  Stored verification hash   71013c39197ad77d72c26d75776445d5
  Report Hash                71013c39197ad77d72c26d75776445d5
  Verify result              Match
Bad Sector List
  Bad sector(s)              No bad sectors found
```

```
Image Source:  \\.\PHYSICALDRIVE3
Destination:   C:\Users\Admin\Desktop\Lab1\SuspectDrive
Status:        Image created successfully

Elapsed time:          0:09:10
Estimated time left:
```

Photo 10: The bit stream image is successfully created, generating the
MD5 hash value: *c8d17353dfd308fa17dae9840eaa1db5*
SHA-1 hash value: *71013c39197ad77d72c26c2675776445d5*

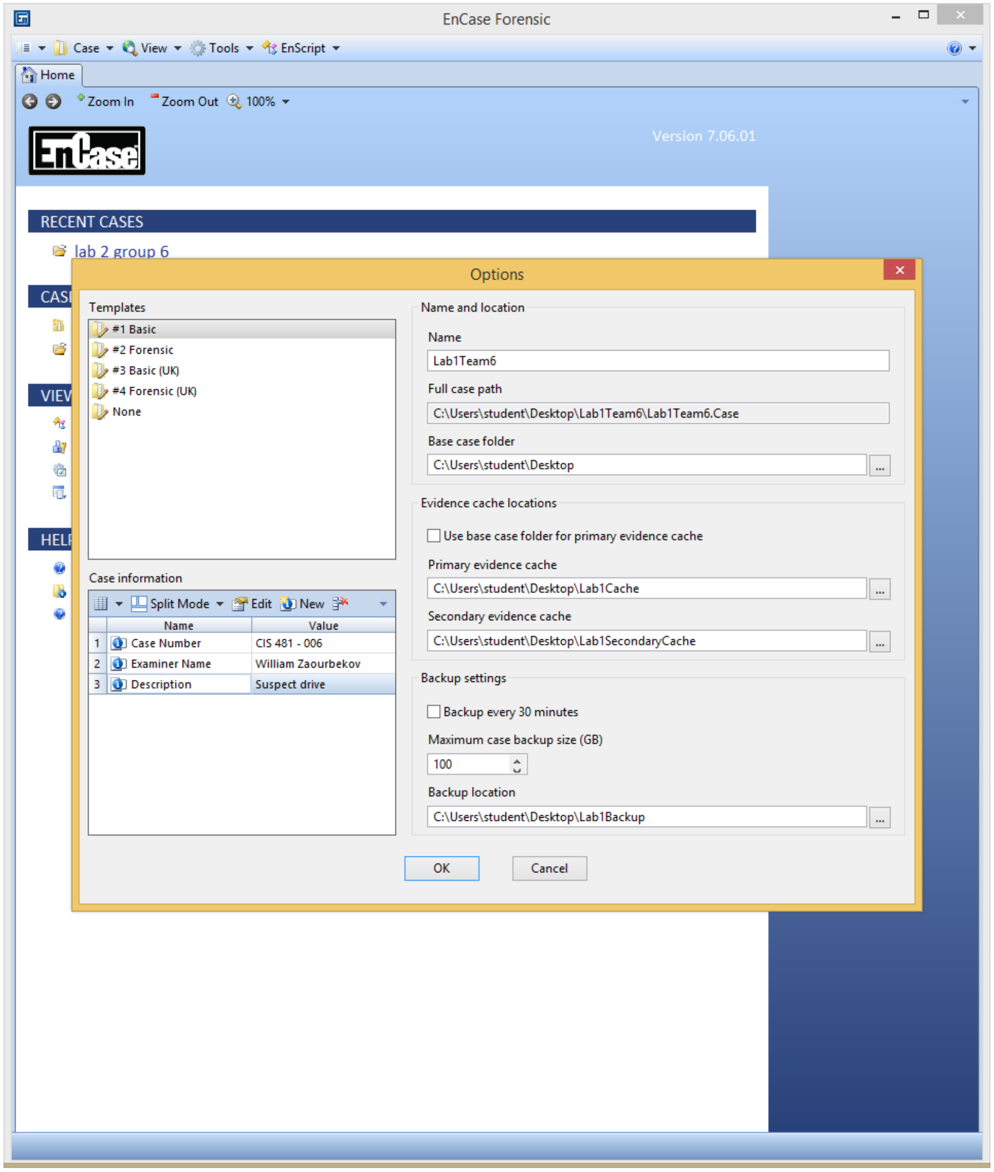


```
 Sector Count: 39,851,760
[Physical Drive Information]
 Drive Model: Tableau Forensic IDE Bridge IEEE 1394 SBP2 Device
 Drive Serial Number: 01cc0e002cc20500
 Drive Interface Type: 1394
 Removable drive: False
 Source data size: 19458 MB
 Sector count:    39851760
[Computed Hashes]
 MD5 checksum:    c8d17353dfd308fa17dae9840eaa1db5
 SHA1 checksum:   71013c39197ad77d72c26d75776445d525994ced

Image Information:
 Acquisition started:   Mon Feb 06 18:33:38 2017
 Acquisition finished:  Mon Feb 06 18:42:48 2017
 Segment list:
  C:\Users\Admin\Desktop\Lab1\SuspectDrive.E01
  C:\Users\Admin\Desktop\Lab1\SuspectDrive.E02

Image Verification Results:
 Verification started:  Mon Feb 06 18:42:48 2017
 Verification finished: Mon Feb 06 18:44:30 2017
 MD5 checksum:    c8d17353dfd308fa17dae9840eaa1db5 : verified
 SHA1 checksum:   71013c39197ad77d72c26d75776445d525994ced : ve
```

Photo 11: Image summary. Both MD5 and SHA1 checksums are verified.

EnCase Forensic Software

We then created another copy of the bit stream image to have a “Master Copy” (That we will never touch unless we need it for a new copy) in case we accidentally change the data on the image we are working on, we will have a backup without having to go back to the evidence locker to create another image. This master copy should be locked up or properly stored with restricted access as well. If the copy we are working on becomes unusable and we need to go back to our master copy and it turns out that the master copy was tampered with (and hopefully we catch that is was), we would have to go back to the evidence locker to request the original HDD to create a new image. We wouldn’t want to go back to the locker because this creates additional windows for error in some way. We want to minimize contact with the evidence as much as we can to reduce the chance of any tampering or damage to the evidence. If the evidence becomes tampered with, damaged, or if there is an error with the chain of custody form or with the process of documenting it, there is a good chance the evidence will become inadmissible in court.



Case information

	Name	Value
1	Case Number	CIS 481 - 006
2	Examiner Name	William Zaourbekov
3	Description	Suspect drive

Name and location

Name: Lab1Team6

Full case path: C:\Users\student\Desktop\Lab1Team6\Lab1Team6.Case

Base case folder: C:\Users\student\Desktop

Evidence cache locations

□ Use base case folder for primary evidence cache

Primary evidence cache: C:\Users\student\Desktop\Lab1Cache

Secondary evidence cache: C:\Users\student\Desktop\Lab1SecondaryCache

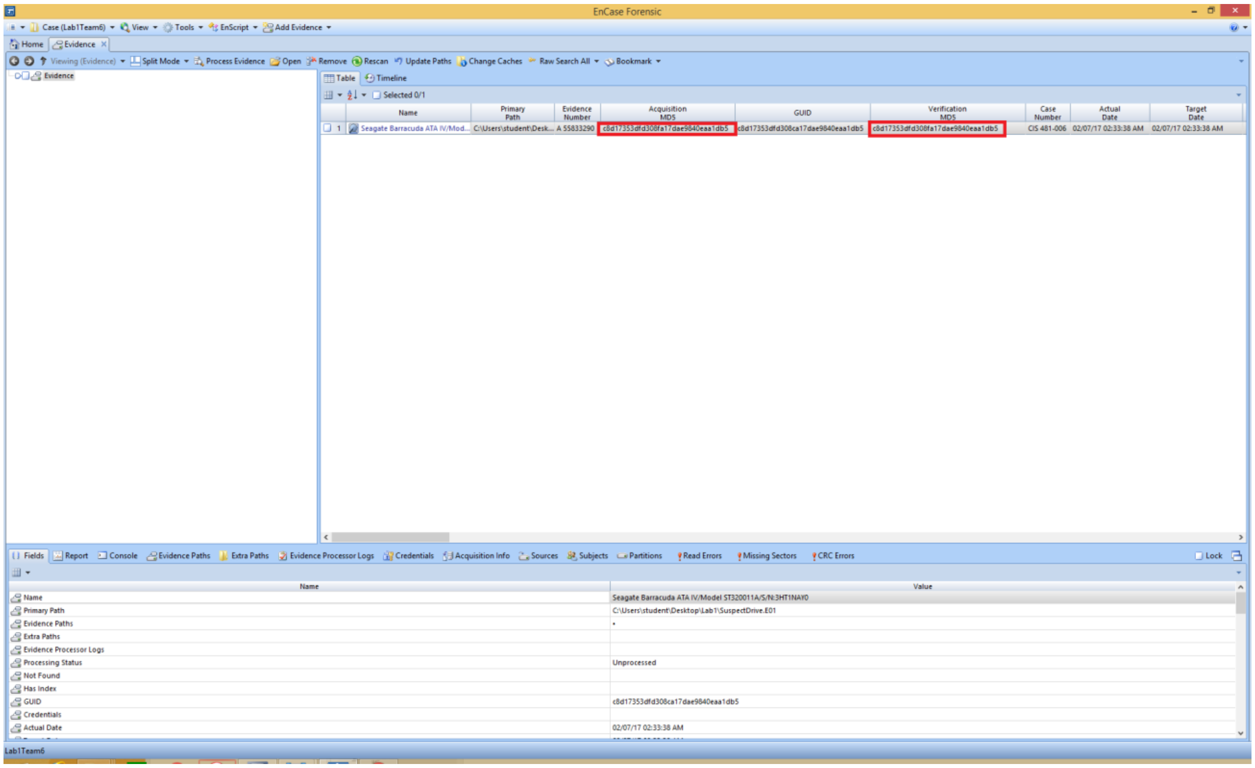
Backup settings

□ Backup every 30 minutes

Maximum case backup size (GB): 100

Backup location: C:\Users\student\Desktop\Lab1Backup

Photo 12: We then move onto EnCase *Forensic to perform the image acquisition/hash value verification processes. We start out by creating a new case with these* specified parameters.

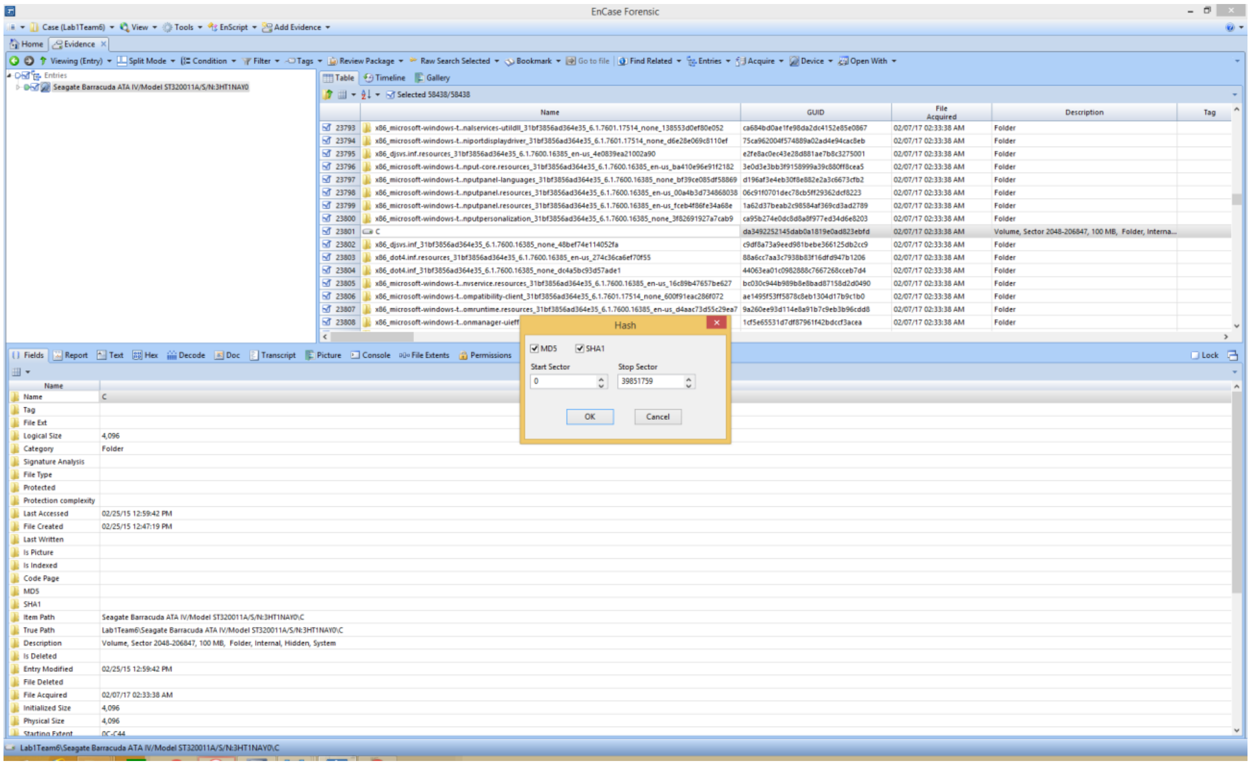

EnCase Forensic
Case (Lab1Team6) View Tools EnScript Add Evidence
Home Evidence
Viewing (Evidence) Split Mode Process Evidence Open Remove Rescan Update Paths Change Caches Raw Search All Bookmark
Evidence
Table Timeline
Selected 0/1
Fields Report Console Evidence Paths Extra Paths Evidence Processor Logs Credentials Acquisition Info Sources Subjects Partitions Read Errors Missing Sectors CRC Errors Lock
Lab1Team6

	Name	Primary Path	Evidence Number	Acquisition MD5	GUID	Verification MD5	Case Number	Actual Date	Target Date
1	Seagate Barracuda ATA IV/Mod...	C:\Users\student\Desk...	A 55833290	c8d17353dfd308fa17dae9840eaa1db5	c8d17353dfd308ca17dae9840eaa1db5	c8d17353dfd308fa17dae9840eaa1db5	CIS 481-006	02/07/17 02:33:38 AM	02/07/17 02:33:38 AM

Name	Value
Name	Seagate Barracuda ATA IV/Model ST320011A/S/N:3HT1NAY0
Primary Path	C:\Users\student\Desktop\Lab1\SuspectDrive.E01
Evidence Paths	•
Extra Paths	
Evidence Processor Logs	
Processing Status	Unprocessed
Not Found	
Has Index	
GUID	c8d17353dfd308ca17dae9840eaa1db5
Credentials	
Actual Date	02/07/17 02:33:38 AM

Photo 13: After dragging the image file onto EnCase it verifies the E01 file and then generates a verification MD5 hash value.

This value has the same MD5 hash value as the acquisition files (c8d17353dfd308fa17dae9840eaa1db5). It is very important that these two values match as it means that the bit stream image was not tampered with or altered between the time it was acquired and the time it was verified by EnCase.


EnCase Forensic
Case (Lab1Team6) View Tools EnScript Add Evidence
Home Evidence
Viewing (Entry) Split Mode Condition Filter Tags Review Package Raw Search Selected Bookmark Go to file Find Related Entries Acquire Device Open With
Entries
Seagate Barracuda ATA IV/Model ST320011A/S/N:3HT1NAY0
Table Timeline Gallery
Selected 58438/58438
Fields Report Text Hex Decode Doc Transcript Picture Console File Extents Permissions Lock
Hash
OK
Cancel
Lab1Team6\Seagate Barracuda ATA IV/Model ST320011A/S/N:3HT1NAY0\C

	Name	GUID	File Acquired	Description	Tag
23793	x86_microsoft-windows-t..nalservices-utildll_31bf3856ad364e35_6.1.7601.17514_none_138553d0ef80e052	ca684bd0ae1fe98da2dc4152e85e0867	02/07/17 02:33:38 AM	Folder	
23794	x86_microsoft-windows-t..niportdisplaydriver_31bf3856ad364e35_6.1.7601.17514_none_d6e28e069c8110ef	75ca962004f574889a02ad4e94cac8eb	02/07/17 02:33:38 AM	Folder	
23795	x86_djsvs.inf.resources_31bf3856ad364e35_6.1.7600.16385_en-us_4e0839ea21002a90	e2fe8ac0ec43e28d881ae7b8c3275001	02/07/17 02:33:38 AM	Folder	
23796	x86_microsoft-windows-t..nput-core.resources_31bf3856ad364e35_6.1.7600.16385_en-us_ba410e96e91f2182	3e0d3e3bb3f9158999a39c880ff8cea5	02/07/17 02:33:38 AM	Folder	
23797	x86_microsoft-windows-t..nputpanel-languages_31bf3856ad364e35_6.1.7600.16385_none_bf39ce085df58869	d196af3e4eb30f8e882e2a3c6673cfb2	02/07/17 02:33:38 AM	Folder	
23798	x86_microsoft-windows-t..nputpanel.resources_31bf3856ad364e35_6.1.7600.16385_en-us_00a4b3d734868038	06c91f0701dec78cb5ff29362dcf8223	02/07/17 02:33:38 AM	Folder	
23799	x86_microsoft-windows-t..nputpanel.resources_31bf3856ad364e35_6.1.7600.16385_en-us_fceb4f86fe34a68e	1a62d37beab2c98584af369cd3ad2789	02/07/17 02:33:38 AM	Folder	
23800	x86_microsoft-windows-t..nputpersonalization_31bf3856ad364e35_6.1.7600.16385_none_3f82691927a7cab9	ca95b274e0dc8d8a8f977ed34d6e8203	02/07/17 02:33:38 AM	Folder	
23801	C	da3492252145dab0a1819e0ad823ebfd	02/07/17 02:33:38 AM	Volume, Sector 2048-206847, 100 MB, Folder, Interna...	
23802	x86_djsvs.inf_31bf3856ad364e35_6.1.7600.16385_none_48bef74e114052fa	c9df8a73a9eed981bebe366125db2cc9	02/07/17 02:33:38 AM	Folder	
23803	x86_dot4.inf.resources_31bf3856ad364e35_6.1.7600.16385_en-us_274c36ca6ef70f55	88a6cc7aa3c7938b83f16dfd947b1206	02/07/17 02:33:38 AM	Folder	
23804	x86_dot4.inf_31bf3856ad364e35_6.1.7600.16385_none_dc4a5bc93d57ade1	44063ea01c0982888c7667268cceb7d4	02/07/17 02:33:38 AM	Folder	
23805	x86_microsoft-windows-t..nvservice.resources_31bf3856ad364e35_6.1.7600.16385_en-us_16c89b47657be627	bc030c944b989b8e8bad87158d2d0490	02/07/17 02:33:38 AM	Folder	
23806	x86_microsoft-windows-t..ompatibility-client_31bf3856ad364e35_6.1.7601.17514_none_600f91eac286f072	ae1495f53ff5878c8eb1304d17b9c1b0	02/07/17 02:33:38 AM	Folder	
23807	x86_microsoft-windows-t..omruntime.resources_31bf3856ad364e35_6.1.7600.16385_en-us_d4aac73d55c29ea7	9a260ee93d114e8a91b7c9eb3b96cdd8	02/07/17 02:33:38 AM	Folder	
23808	x86_microsoft-windows-t..onmanager-uieff	1cf5e65531d7df87961f42bdccf3acea	02/07/17 02:33:38 AM	Folder	

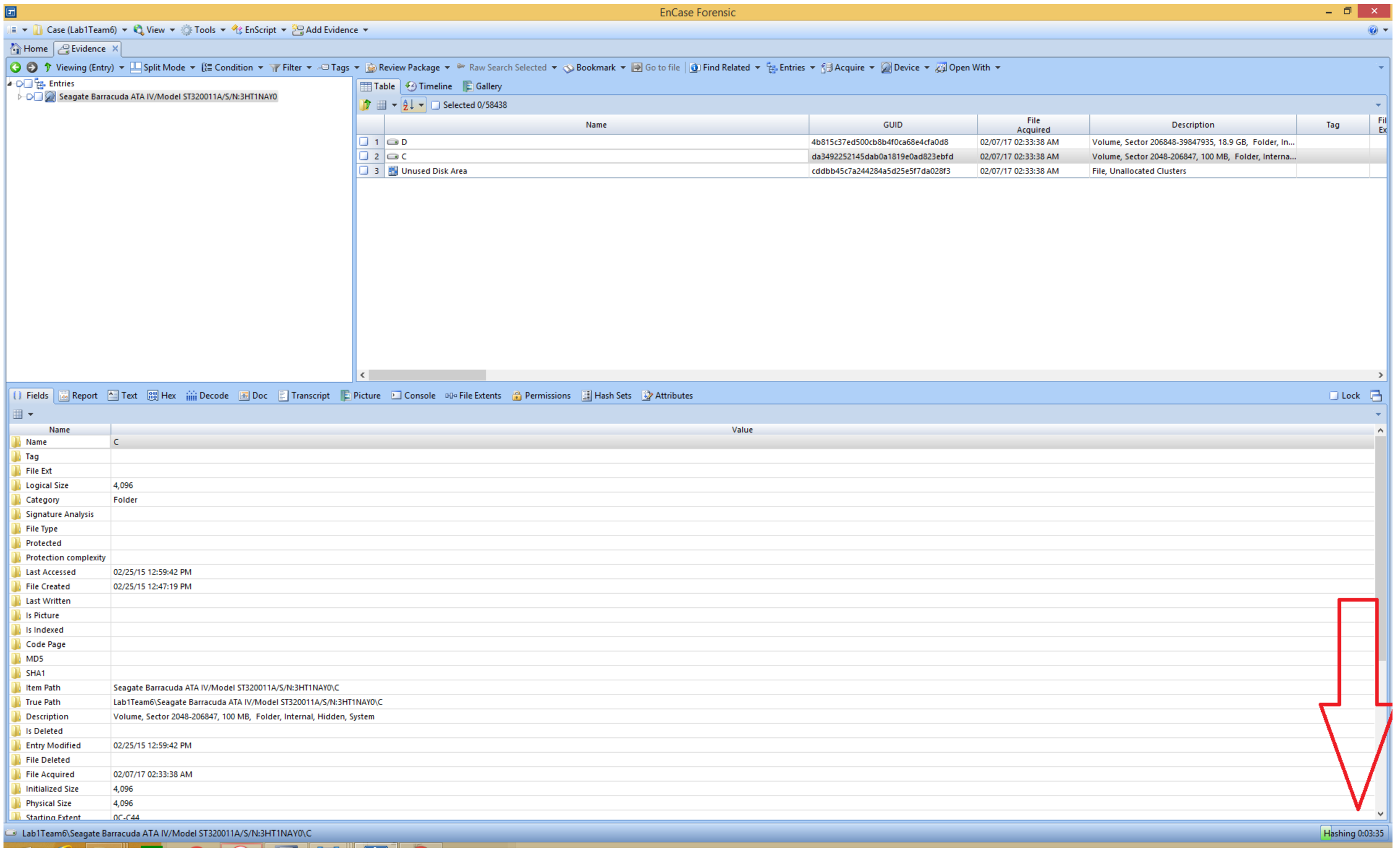
Hash

☑ MD5 ☑ SHA1

Start Sector: 0
Stop Sector: 39851759

Name	
Name	C
Tag	
File Ext	
Logical Size	4,096
Category	Folder
Signature Analysis	
File Type	
Protected	
Protection complexity	
Last Accessed	02/25/15 12:59:42 PM
File Created	02/25/15 12:47:19 PM
Last Written	
Is Picture	
Is Indexed	
Code Page	
MD5	
SHA1	
Item Path	Seagate Barracuda ATA IV/Model ST320011A/S/N:3HT1NAY0\C
True Path	Lab1Team6\Seagate Barracuda ATA IV/Model ST320011A/S/N:3HT1NAY0\C
Description	Volume, Sector 2048-206847, 100 MB, Folder, Internal, Hidden, System
Is Deleted	
Entry Modified	02/25/15 12:59:42 PM
File Deleted	
File Acquired	02/07/17 02:33:38 AM
Initialized Size	4,096
Physical Size	4,096
Starting Extent	0C-C44

Photo 14: We then generate MD5 and SHA1 hash values from the physical drive, so we can compare it to the hash values that were generated by FTK Imager.

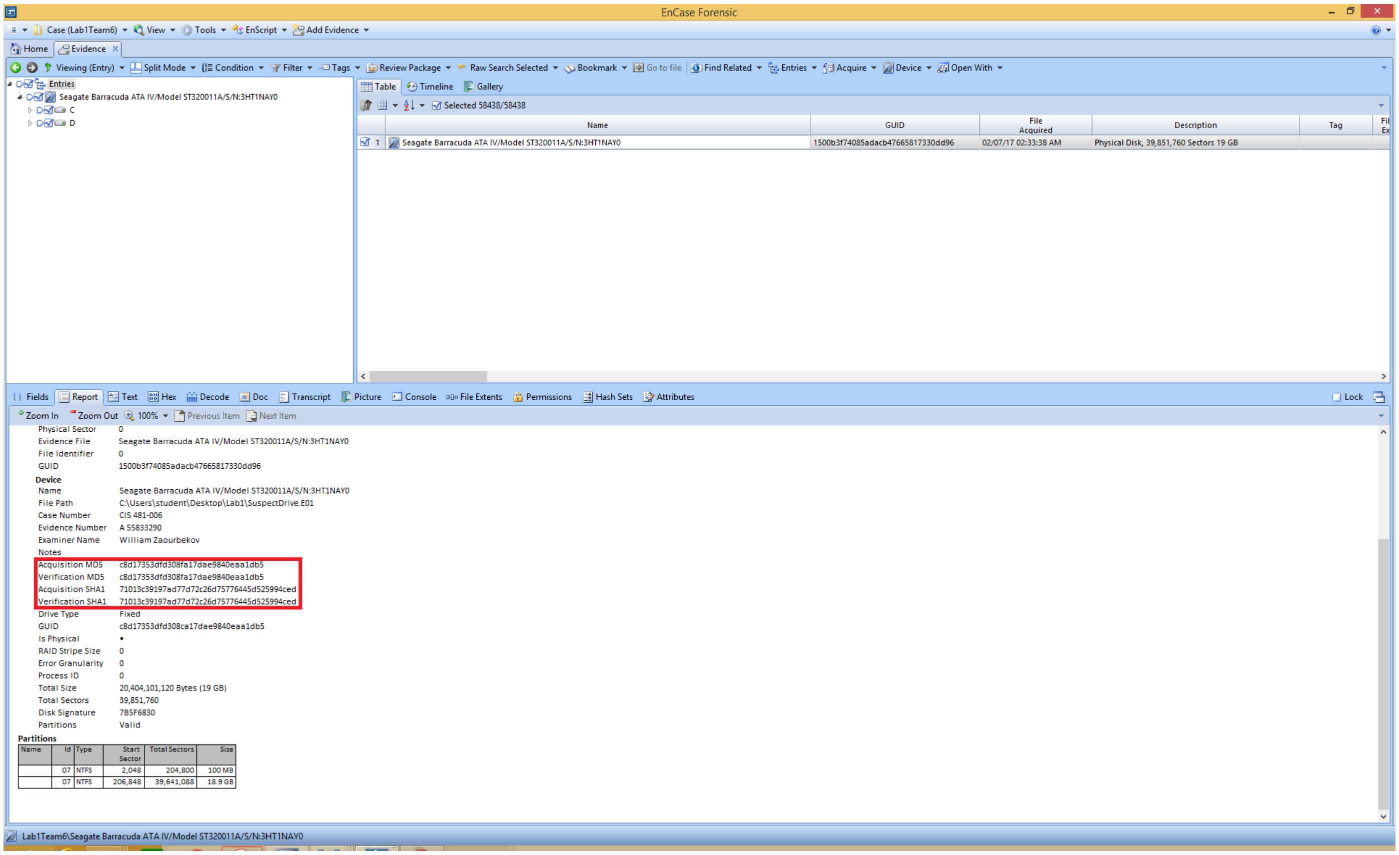


	Name	GUID	File Acquired	Description	Tag
1	D	4b815c37ed500cb8b4f0ca68e4cfa0d8	02/07/17 02:33:38 AM	Volume, Sector 206848-39847935, 18.9 GB, Folder, In...	
2	C	da3492252145dab0a1819e0ad823ebfd	02/07/17 02:33:38 AM	Volume, Sector 2048-206847, 100 MB, Folder, Interna...	
3	Unused Disk Area	cddbb45c7a244284a5d25e5f7da028f3	02/07/17 02:33:38 AM	File, Unallocated Clusters	

Name	Value
Name	C
Tag	
File Ext	
Logical Size	4,096
Category	Folder
Signature Analysis	
File Type	
Protected	
Protection complexity	
Last Accessed	02/25/15 12:59:42 PM
File Created	02/25/15 12:47:19 PM
Last Written	
Is Picture	
Is Indexed	
Code Page	
MD5	
SHA1	
Item Path	Seagate Barracuda ATA IV/Model ST320011A/S/N:3HT1NAY0\C
True Path	Lab1Team6\Seagate Barracuda ATA IV/Model ST320011A/S/N:3HT1NAY0\C
Description	Volume, Sector 2048-206847, 100 MB, Folder, Internal, Hidden, System
Is Deleted	
Entry Modified	02/25/15 12:59:42 PM
File Deleted	
File Acquired	02/07/17 02:33:38 AM
Initialized Size	4,096
Physical Size	4,096
Starting Extent	0C-C44

Lab1Team6\Seagate Barracuda ATA IV/Model ST320011A/S/N:3HT1NAY0\C

Photo 15: EnCase then starts to generate the hash values, note the arrow pointing to “Hashing”



	Name	GUID	File Acquired	Description	Tag
1	Seagate Barracuda ATA IV/Model ST320011A/S/N:3HT1NAY0	1500b3f74085adacb47665817330dd96	02/07/17 02:33:38 AM	Physical Disk, 39,851,760 Sectors 19 GB	

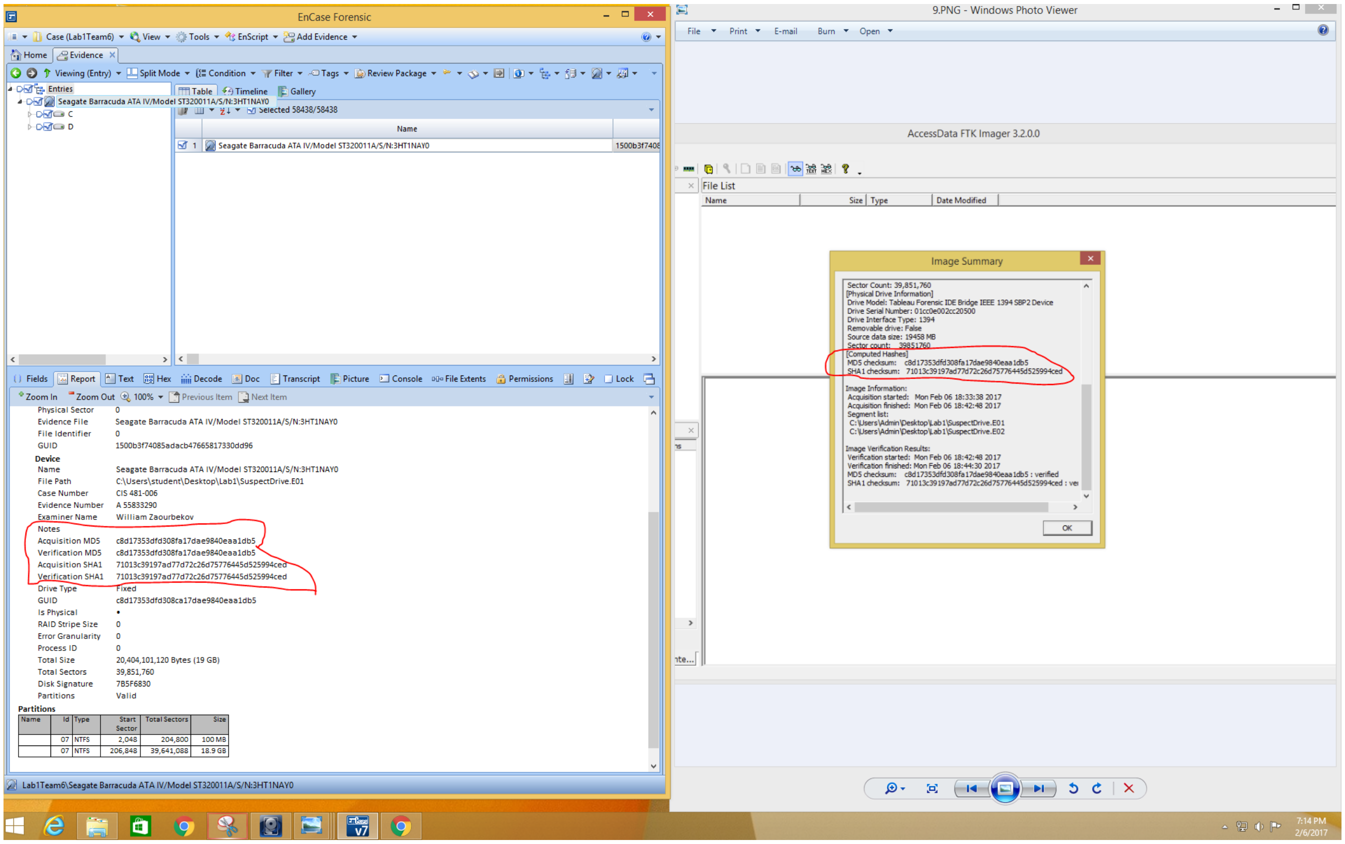
```
 Physical Sector      0
 Evidence File        Seagate Barracuda ATA IV/Model ST320011A/S/N:3HT1NAY0
 File Identifier      0
 GUID                 1500b3f74085adacb47665817330dd96
Device
 Name                 Seagate Barracuda ATA IV/Model ST320011A/S/N:3HT1NAY0
 File Path            C:\Users\student\Desktop\Lab1\SuspectDrive.E01
 Case Number          CIS 481-006
 Evidence Number      A 55833290
 Examiner Name        William Zaourbekov
 Notes
 Acquisition MD5      c8d17353dfd308fa17dae9840eaa1db5
 Verification MD5     c8d17353dfd308fa17dae9840eaa1db5
 Acquisition SHA1     71013c39197ad77d72c26d75776445d525994ced
 Verification SHA1    71013c39197ad77d72c26d75776445d525994ced
 Drive Type           Fixed
 GUID                 c8d17353dfd308ca17dae9840eaa1db5
 Is Physical          •
 RAID Stripe Size     0
 Error Granularity    0
 Process ID           0
 Total Size           20,404,101,120 Bytes (19 GB)
 Total Sectors        39,851,760
 Disk Signature       7B5F6830
 Partitions           Valid
```

Partitions

Name	Id	Type	Start Sector	Total Sectors	Size
	07	NTFS	2,048	204,800	100 MB
	07	NTFS	206,848	39,641,088	18.9 GB

Lab1Team6\Seagate Barracuda ATA IV/Model ST320011A/S/N:3HT1NAY0

Photo 16: Hashing process is completed; these MD5 and SHA-1 hash values are then *generated*



```
Physical Sector      0
Evidence File        Seagate Barracuda ATA IV/Model ST320011A/S/N:3HT1NAY0
File Identifier      0
GUID                 1500b3f74085adacb47665817330dd96
Device
Name                 Seagate Barracuda ATA IV/Model ST320011A/S/N:3HT1NAY0
File Path            C:\Users\student\Desktop\Lab1\SuspectDrive.E01
Case Number          CIS 481-006
Evidence Number      A 55833290
Examiner Name        William Zaourbekov
Notes
Acquisition MD5      c8d17353dfd308fa17dae9840eaa1db5
Verification MD5     c8d17353dfd308fa17dae9840eaa1db5
Acquisition SHA1     71013c39197ad77d72c26d75776445d525994ced
Verification SHA1    71013c39197ad77d72c26d75776445d525994ced
Drive Type           Fixed
GUID                 c8d17353dfd308ca17dae9840eaa1db5
Is Physical          •
RAID Stripe Size     0
Error Granularity    0
Process ID           0
Total Size           20,404,101,120 Bytes (19 GB)
Total Sectors        39,851,760
Disk Signature       7B5F6830
Partitions           Valid
```

Partitions

Name	Id	Type	Start Sector	Total Sectors	Size
	07	NTFS	2,048	204,800	100 MB
	07	NTFS	206,848	39,641,088	18.9 GB

Lab1Team6\Seagate Barracuda ATA IV/Model ST320011A/S/N:3HT1NAY0

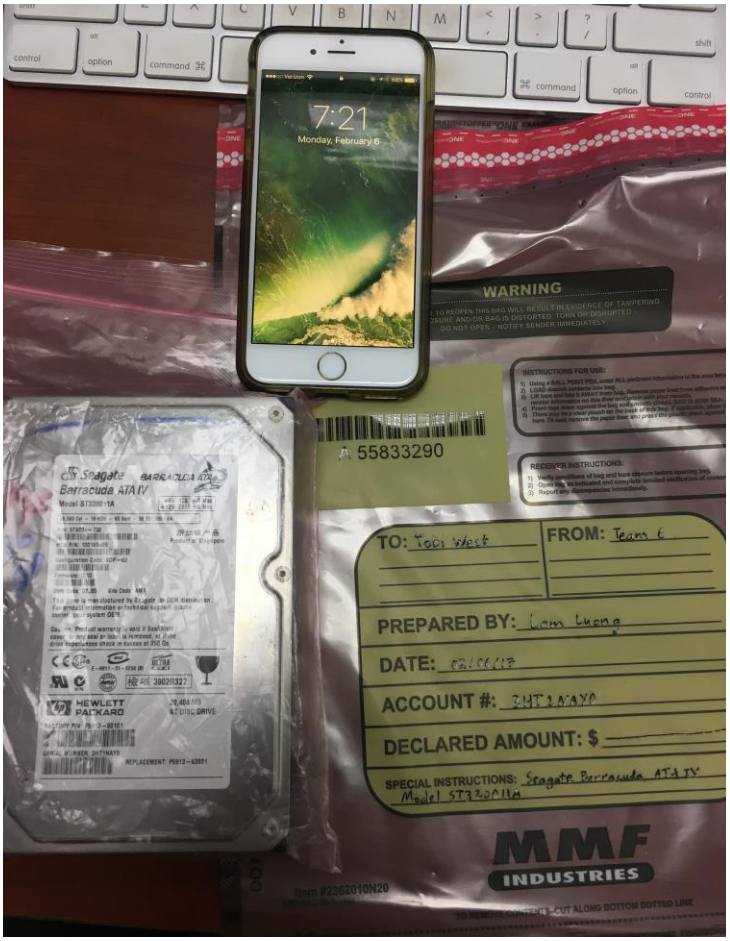
```
Sector Count: 39,851,760
[Physical Drive Information]
 Drive Model: Tableau Forensic IDE Bridge IEEE 1394 SBP2 Device
 Drive Serial Number: 01cc0e002cc20500
 Drive Interface Type: 1394
 Removable drive: False
 Source data size: 19458 MB
 Sector count:    39851760
[Computed Hashes]
 MD5 checksum:    c8d17353dfd308fa17dae9840eaa1db5
 SHA1 checksum:   71013c39197ad77d72c26d75776445d525994ced

Image Information:
 Acquisition started:   Mon Feb 06 18:33:38 2017
 Acquisition finished:  Mon Feb 06 18:42:48 2017
 Segment list:
  C:\Users\Admin\Desktop\Lab1\SuspectDrive.E01
  C:\Users\Admin\Desktop\Lab1\SuspectDrive.E02

Image Verification Results:
 Verification started:  Mon Feb 06 18:42:48 2017
 Verification finished: Mon Feb 06 18:44:30 2017
 MD5 checksum:    c8d17353dfd308fa17dae9840eaa1db5 : verified
 SHA1 checksum:   71013c39197ad77d72c26d75776445d525994ced : ve
```

Photo 17: Comparing the hash values, and since they match, we can say now say that we have created a bit stream image of the evidence drive.

After comparing the hash values to FTK imager, we notice that they both match with each other, meaning that the image has not been tampered and therefore a correct copy of the physical drive. This means that the image can be provided as admissible evidence in court.

Preparing the Evidence for Release

After completing our hash validation, we proceeded to carefully disassemble our set up from *Photo 6,* placed the hard drive into its original zip lock bag and sealed it. We then had Lam fill out the evidence bag with the proper and sufficient information, enough to ensure that the evidence would not be misplaced, and is easily identifiable. *Photos 18, 19, & 20* below shows the HDD & evidence bag side by side, the receipt of the evidence bag in one picture, and the last shows a precisely placed HDD in a way to see easily see the serial number within the post-sealed bag. The receipt was then safely stored.



A 55833290

TO: Tobi West

FROM: Team 6

PREPARED BY: Lam Luong

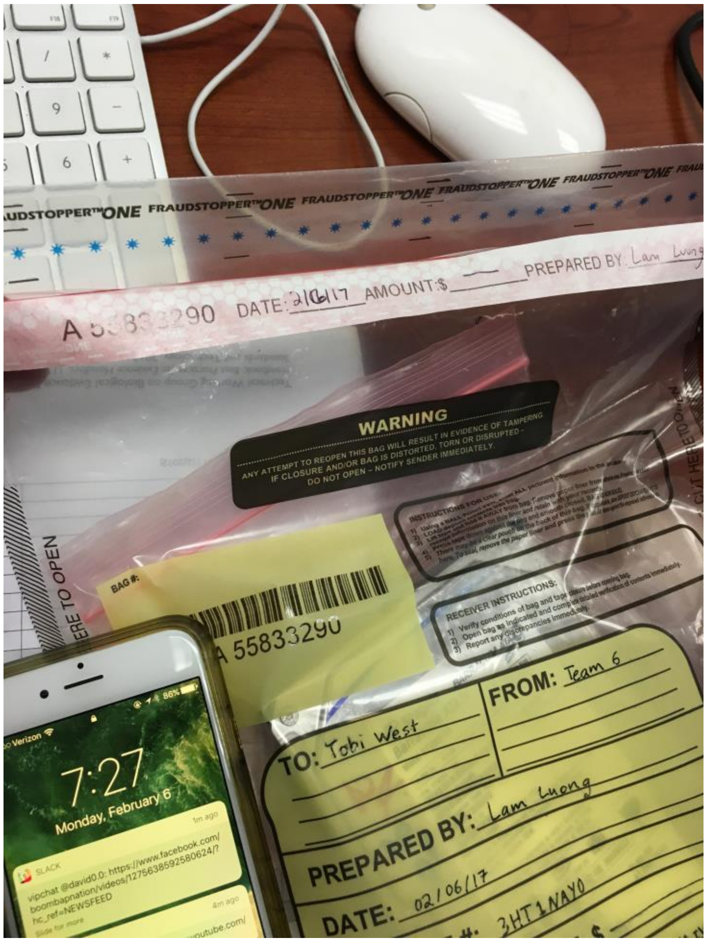
DATE: 02/06/17

ACCOUNT #: 3HT1NAYO

DECLARED AMOUNT: $

SPECIAL INSTRUCTIONS: Seagate Barracuda ATA IV Model ST320011A

Photo 18: Original HDD in its bagging, filled out evidence bag & a phone for Scale & the time Stamp.



A 55833290 DATE: 2/6/17 AMOUNT $ ______ PREPARED BY: Lam Luong

A 55833290

TO: Tobi West

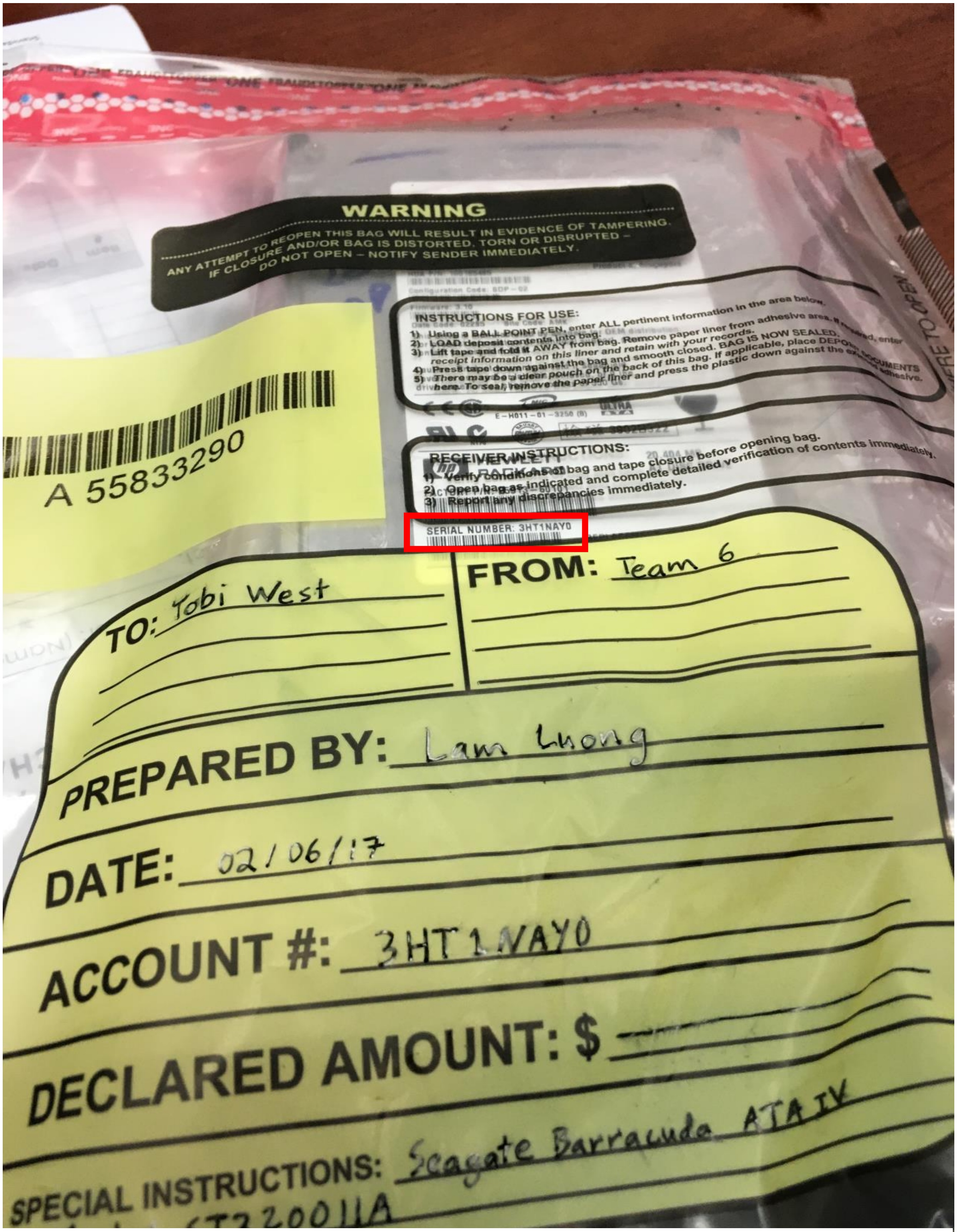
FROM: Team 6

PREPARED BY: Lam Luong

DATE: 02/06/17

#: 3HT1NAYO

Photo 19: Receipt seal & phone for the time stamp.



WARNING

ANY ATTEMPT TO REOPEN THIS BAG WILL RESULT IN EVIDENCE OF TAMPERING. IF CLOSURE AND/OR BAG IS DISTORTED, TORN OR DISRUPTED – DO NOT OPEN – NOTIFY SENDER IMMEDIATELY.

A 55833290

INSTRUCTIONS FOR USE:

1) Using a BALL POINT PEN, enter ALL pertinent information in the area below.
2) LOAD deposit contents into bag.
3) Lift tape and fold it AWAY from bag. Remove paper liner from adhesive area. If required, enter receipt information on this liner and retain with your records.
4) Press tape down against the bag and smooth closed. BAG IS NOW SEALED.
5) There may be a clear pouch on the back of this bag. If applicable, place DEPOSIT DOCUMENTS here. To seal, remove the paper liner and press the plastic down against the exposed adhesive.

RECEIVER INSTRUCTIONS:

1) Verify conditions of bag and tape closure before opening bag.
2) Open bag as indicated and complete detailed verification of contents immediately.
3) Report any discrepancies immediately.

SERIAL NUMBER: 3HT1NAY0

TO: Tobi West

FROM: Team 6

PREPARED BY: Lam Luong

DATE: 02/06/17

ACCOUNT #: 3HT1NAY0

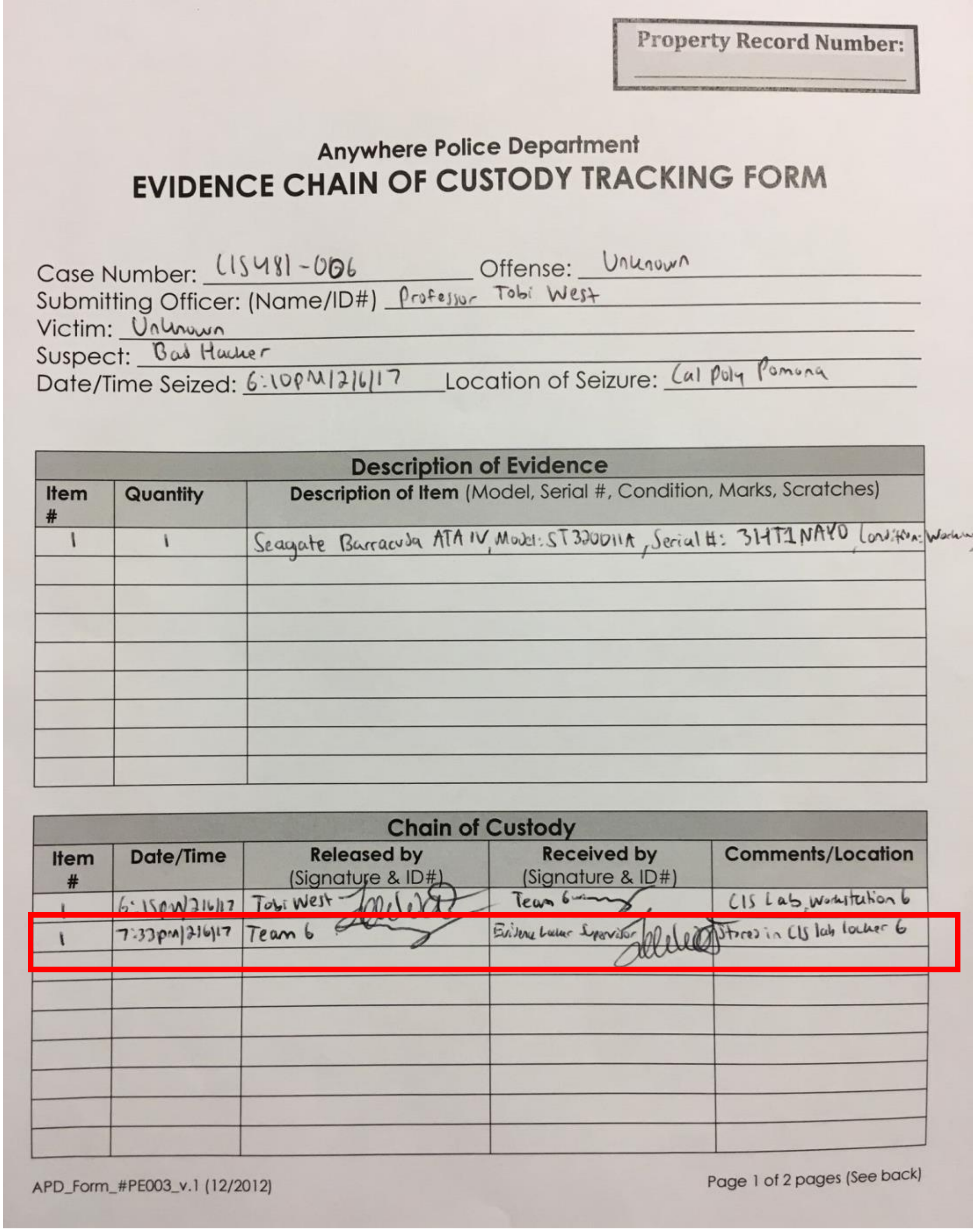
DECLARED AMOUNT: $ —

SPECIAL INSTRUCTIONS: Seagate Barracuda ATA IV ST320011A

Photo 20: Hard Drive sealed within the evidence bag with the serial # visible to prove the authenticity of the hard drive within the bag.

Releasing the Evidence

The next step was to place the evidence back in the locker for safekeeping. We were assigned the locker labeled as “Team 6” by the evidence locker supervisor. We were instructed that the person who received the evidence was not named Tobi West, but rather a generic evidence locker supervisor person, and so we had that person sign off on receiving the evidence we provided (*Photo 21*). Then, we asked the supervisor to watch us transfer custody of the evidence from our hands to the locker labeled “Team 6.” (*Photo 22*). Lastly, we locked up the evidence locker (*Photo 23*), and the proper process for the chain of custody was completed.



Property Record Number: ______

Anywhere Police Department

EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: CIS481-006 Offense: Unknown
Submitting Officer: (Name/ID#) Professor Tobi West
Victim: Unknown
Suspect: Bad Hacker
Date/Time Seized: 6:10pM|2/6/17 Location of Seizure: Cal Poly Pomona

Description of Evidence		
Item #	Quantity	Description of Item (Model, Serial #, Condition, Marks, Scratches)
1	1	Seagate Barracuda ATA IV, Model: ST320011A, Serial #: 3HT1NAYD, Condition: Working

Chain of Custody				
Item #	Date/Time	Released by (Signature & ID#)	Received by (Signature & ID#)	Comments/Location
1	6:15pM 2/6/17	Tobi West	Team 6	CIS Lab, workstation 6
1	7:33pm|2/6/17	Team 6	Evidence Locker Supervisor	Stored in CIS lab locker 6

APD_Form_#PE003_v.1 (12/2012) Page 1 of 2 pages (See back)

Photo 21: Chain of custody form documenting the transfer of the evidence from Team 6 to the evidence locker supervisor.

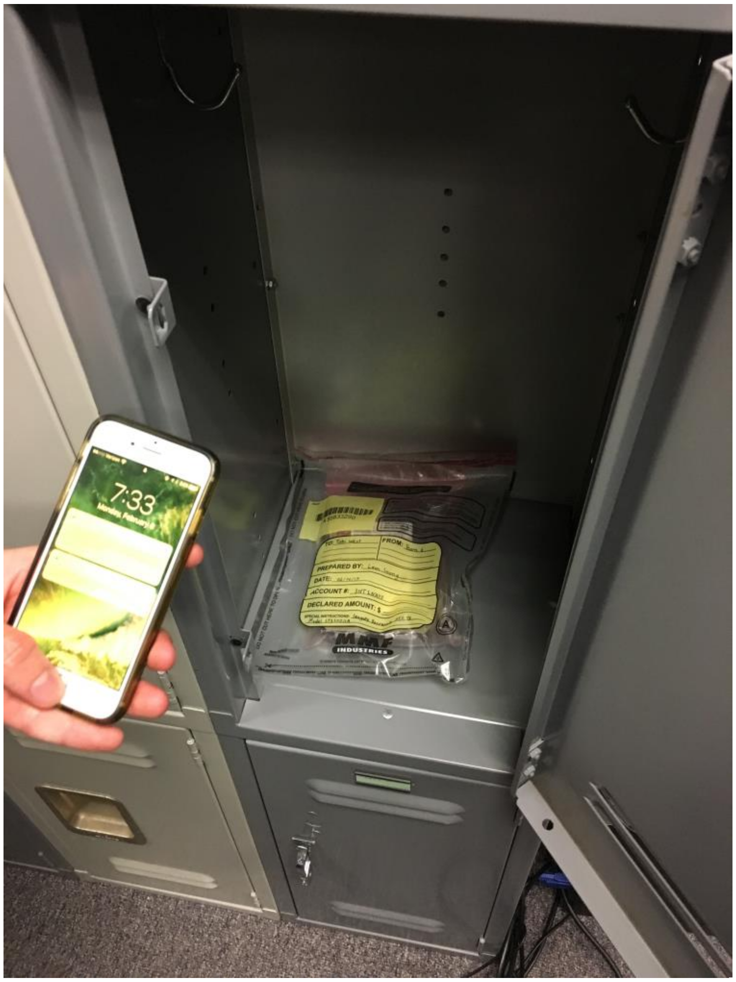


Photo 22: Placing the Evidence within the locker and the time stamp.

Photo 23: Locking up the evidence locker labeled Team 6.

Executive Summary

The process of creating an exact bit for bit copy of the hard drive began with the critically important step of documenting the chain of custody form in detail during the acquisition of the evidence. To have not done so correctly at the acquisition and release of the evidence would be a violation of the chain of custody. Not only may the evidence become inadmissible by the judge, it may establish a basis for the opposing court representative to dismiss, refute, or even use the evidence against our case. We used a write blocker (a piece of hardware that prevents modification to the evidence storage device) alongside FTK Imager (software that creates an exact cloned copy of the storage device) and went through the steps frame by frame to make visible the process in which we cloned the evidence. Afterwards, we used EnCase (software that compares 2 storage devices to ensure they are the same) to authenticate the integrity of our cloned copy of the evidence drive, again frame by frame to increase visibility and to allow easy replicability should our process be disputed. Once we knew the bit stream image was court admissible, we created a master copy and restricted access to it just in case we make a blunder in our analysis process so we will have a backup to fall back to. We were finished creating the copy and no longer had a need to hold onto the evidence so we followed the chain of custody in transferring the device back into the evidence locker and had it signed off, thus properly releasing the evidence from our custody.

Glossary

Hard Disk Drive (HDD) / Hard Drive / Disk Drive – A storage device used by a computer.

Bit Stream Image / Bit-by-bit Image – An exact cloned copy of a disk drive that is admissible in court.

Chain of Custody (CoC) – Refers to the chronological documentation or paper trail, showing the seizure, custody, control, transfer, analysis, and disposition of physical or electronic evidence.

Write Blocker – Are devices that allow acquisition of information on a drive without creating the possibility of accidentally damaging the drive contents. They do this by allowing read commands to pass but by blocking write commands, hence their name.

FTK Imager – A software used to create the bit stream image.

MD5 – A cryptographic hash (128 bits) that is used in this case to check the integrity of files.

SHA1 – A cryptographic hash (160 bits) that is used in this case to check the integrity of files.

Checksum – A 32 character hexdecimal number computed on a file. If two files have the same check sum, they are the same.

EnCase Forensic – A software used to validate the integrity of the bit stream image vs the original disk drive.

=

Evidence Bag Receipt

Team Contract

Project Name: CIS 481 Lab 1

Project Team Members Names and Sign-off:

Name	**Sign-off on Team Contract**
Lam Luong	
Sam Zheng	
William Zaourbekov	
Lima Sim	

Code of Conduct: As a project team, we will:

- Work together to complete the Forensics Project
- Keep all of the team members informed on project assignments and developments
- Respect other team members and their ideas

Participation: We will:

- Actively provide our input for the project
- Distribute project work equally among team members
- Provide quality work to complete the project
- Inform the team prior to an absence

Communication: We will:

- Make sure each team member is up to date with project status
- Actively discuss open issues
- Use email and group meetings as means of communication
- Inform each other of any problems encountered

Problem Solving: We will:

- Encourage team members to provide their view
- Make use of possible solutions brought up by team members
- Use positive attitude to benefit the team