**COMPUTER FORENSICS INVESTIGATION**

CASE 2005-45, Linda Johnson

Prepared for West Flint Library

DATE

December 20 2016

Examiner:

Mr. Christian Hill

Forensics Limited, INC.

(Comp Forensics Div. Section 9 of Weyland-Yutani Co.)

THIS DOCUMENT IS FOR INTERNAL USE ONLY. ALL INFORMATION CONTAINED WITHIN IS CONSIDERED CONFIDENTIAL.

Table of Contents

[Case History: 3](#_Toc470044527)

[Investigation Log: 3](#_Toc470044528)

[Evidence List Summary: 8](#_Toc470044529)

[Evidence: 8](#_Toc470044530)

[Investigational Summary: 11](#_Toc470044531)

[Case Log of Forensic Examination of subject Drive: 11](#_Toc470044532)

[Case Summary and Documentation: 14](#_Toc470044533)

[Drive image documentation and verification is as follows: 14](#_Toc470044534)

[Chain of Custody: 14](#_Toc470044535)

[Receipt: 17](#_Toc470044536)

[Exhibit A – Sanitization Policy 17](#_Toc470044537)

[Exhibit B – FORENSIC HANDLING POLICY 12-20-16 18](#_Toc470044538)

[Exhibit C – HASH IMAGE VALIDATION POLICY 12-20-16 18](#_Toc470044539)

# Case History:

This Examiner was called by Librarian Linda Johansen of West Flint Library located at 3601 Beecher Road, Flint MI 48503 on the evening of April 27, 2016. She asked that we examine a computer that a patron had used earlier that day. The patron had exhibited suspicious activity as the patron kept closing the browser anytime she would come near the computer. The librarian stated that after the suspicious acting patron left the premises, she brought up the browser and tried to see where he had been but all history has been deleted. I arrived at the library at 8:05 AM on Tuesday, April 28 and discovered the computer in question in a powered off state. I removed the drive from the computer, placed it into a secure container, and left a note on the computer that it was out of service. This Examiner provided the librarian with a receipt and began a chain-of-custody form.

# Investigation Log:

* 5:30 PM 04/27/16: Interview with Linda Johnson, Librarian at West Flint Library:

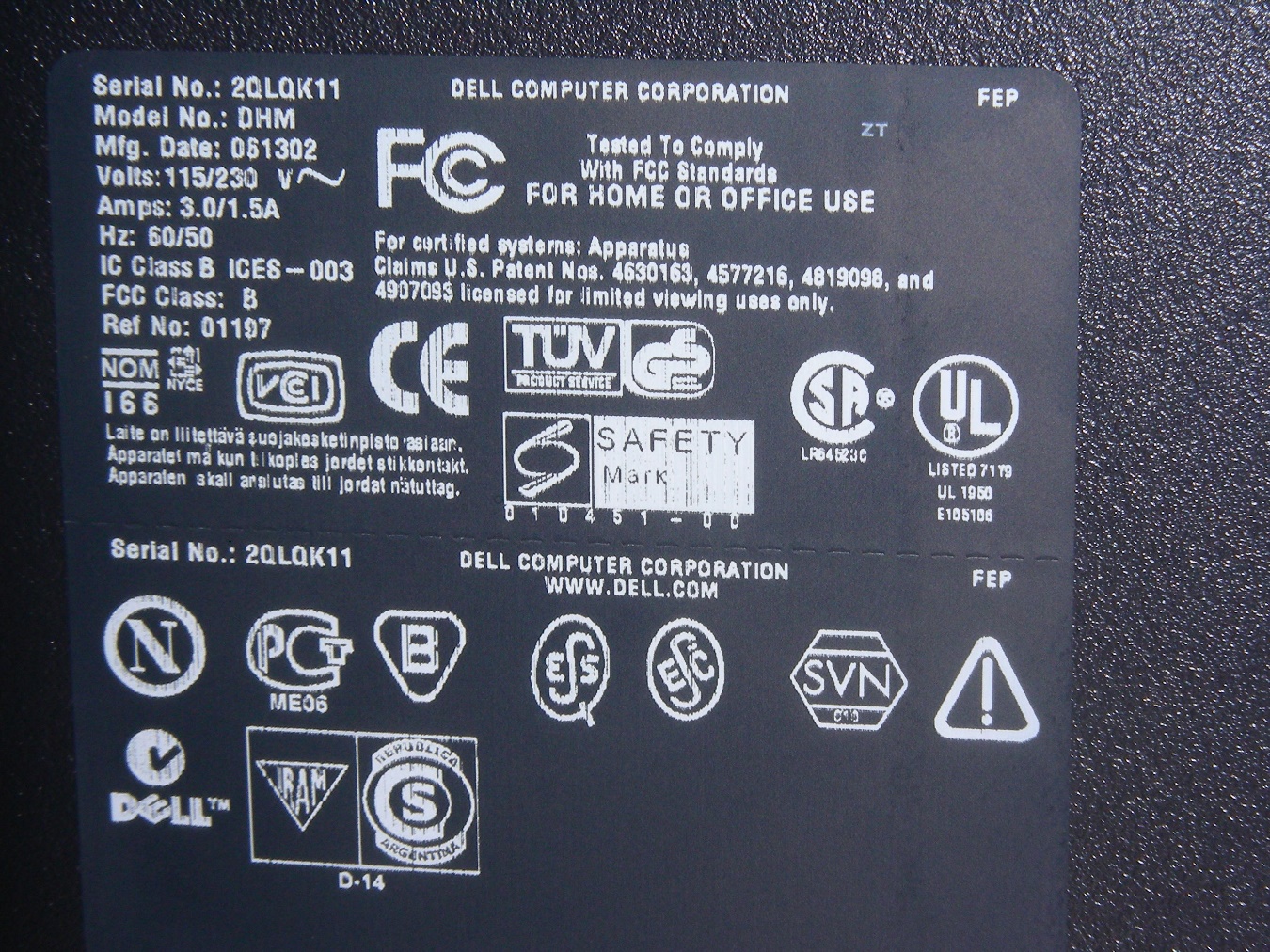
Linda Johnson reported top this investigator that a patron of the library was exhibiting suspicious activity on a public computer. She stated that the patron kept closing the browser anytime she would come near the computer. The librarian stated that after the suspicious acting patron left the premises, she brought up the browser and tried to see where he had been but all history has been deleted. Investigation was arranged for the following morning before opening hours.

* 8:05 AM 04/28/2016: On site of West Flint Library:

Arrived on site before opening hours of Library. The computer area looked as follows:



Photographed the computer in question



Photographed the back Label

* + Identified System as a Dell OptiPlex GX260, which is the standard machine at the library.
  + The PC serial number was: 2QLQK11. The system was in a powered off state.
* 8:25 AM, 04/28/16:

Disconnected the machine’s power source, removed the cover, photographed the inside, then removed the hard drive. The hard drive was placed into a static-free evidence bag, labeled Case 2005-45, West Flint Library-Dell. A receipt for the removal of property was signed by and given to Linda Johansen, Librarian, as was the Chain of Custody form. No other items were seen in the library that would be known to contain electronic data or information related to the investigation, and no other items were removed.

Photographed the Open computer system

* + Opened the system and removed the Hard Drive. Left a note on the computer stating it was out of service.
* 8:45 AM 04/28/2016: Transport of Hard Drive to my Forensics Limited Analysis Lab.
* 9:30 AM 04/28/16: Arrival at Analysis Lab, imaging of drive for analysis:

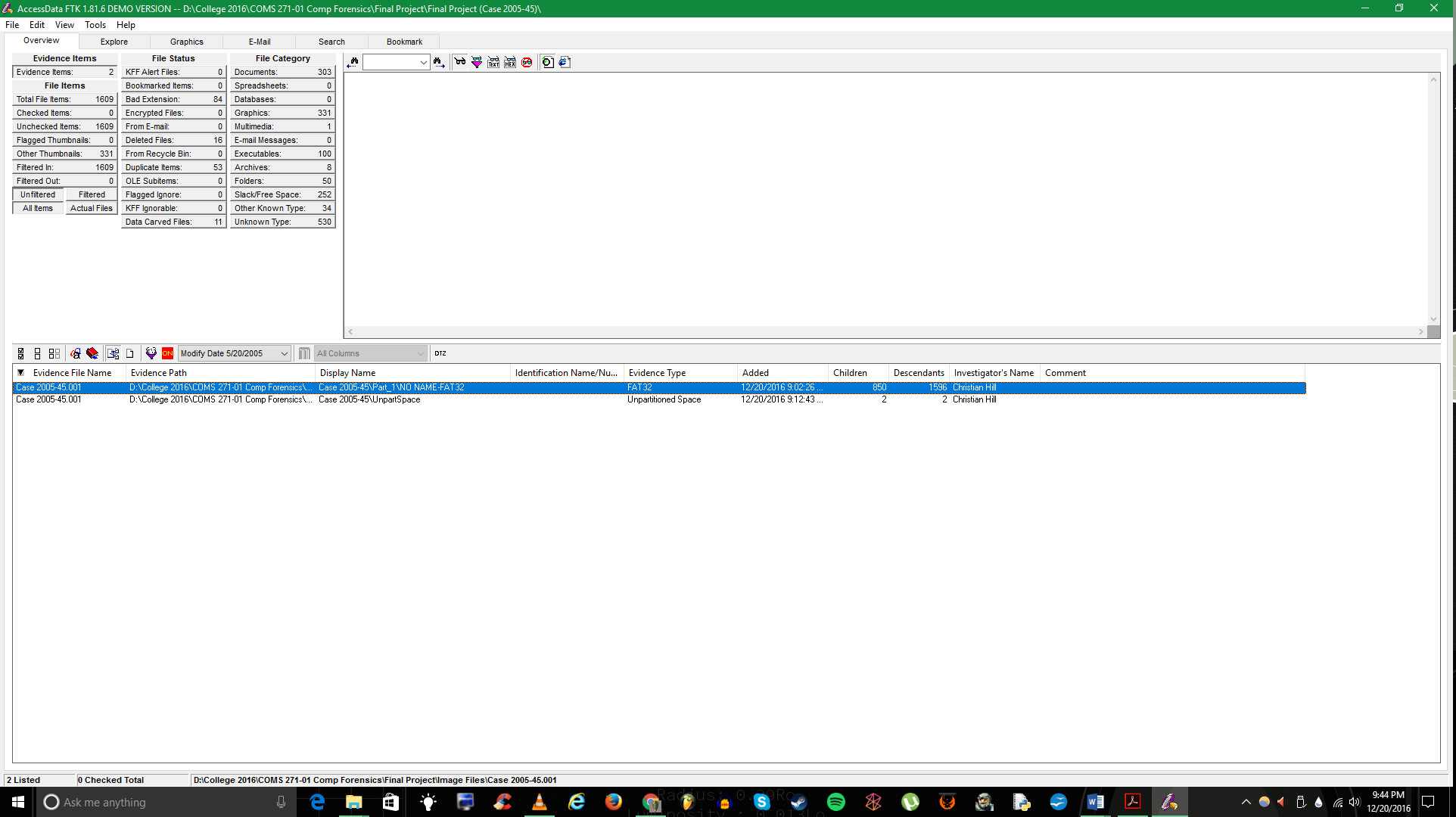
Upon arrival at the Forensics Limited Analysis Lab, the subject hard drive was readied for analysis by the attachment of a write-blocking device. This Investigator then made a bit-by-bit image of the subject drive using AccessData FTK 1.81.6, ProDiscover Basic 64, and OSForensics. All registered to Forensics Limited, Inc. Analysis of the drive revealed it to be a Standard disk drives 20GB hard drive, model Maxtor 6E 020L0, and serial number SG-02w647-24951-359-AOXW, formatted as FAT 32 and an Un-Partitioned Space.

* The Following is a photograph of the subject drive taken before imaging:



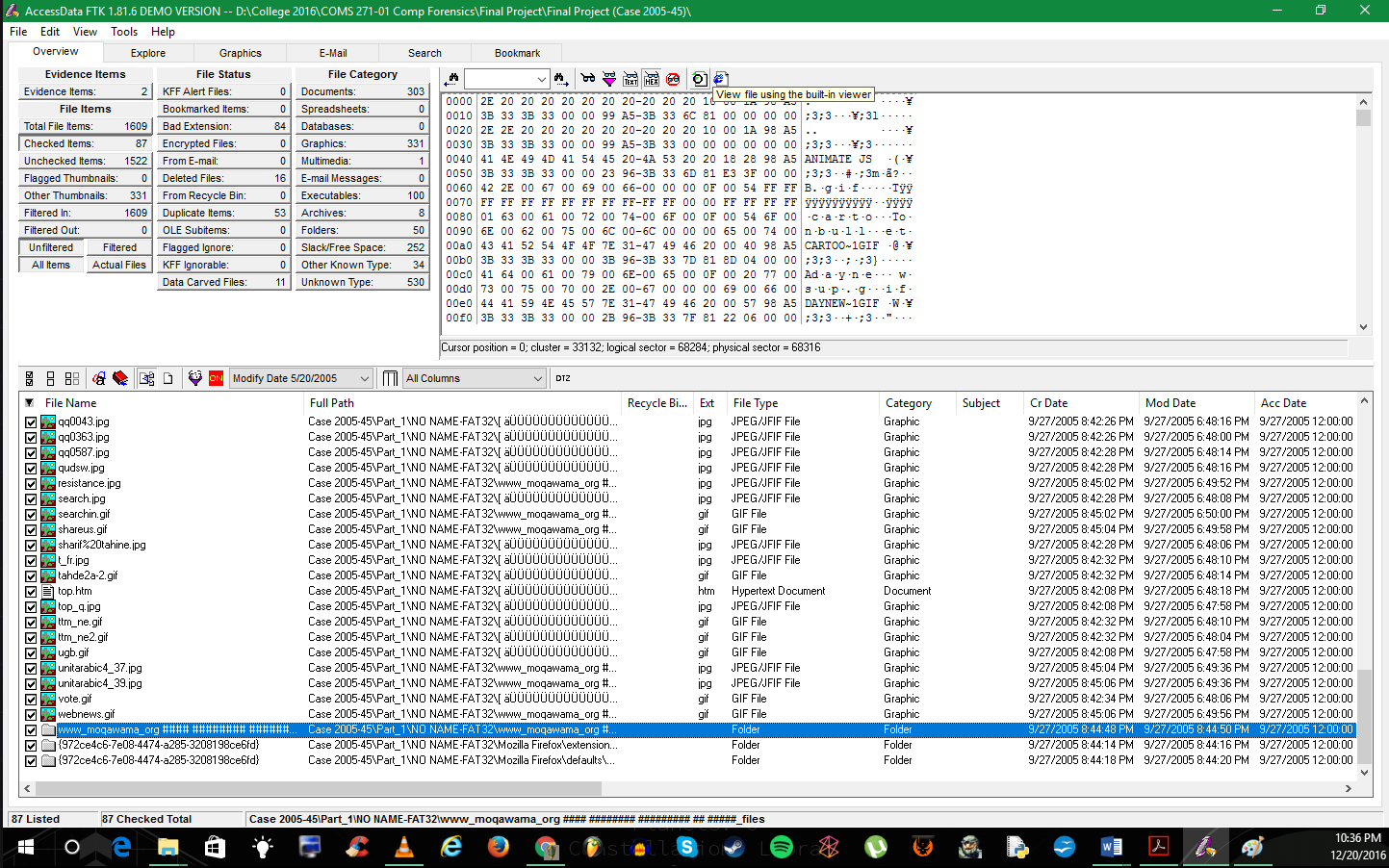
# Evidence List Summary:

* The following screenshot shows a listing of all items recovered during analysis:



# Evidence:

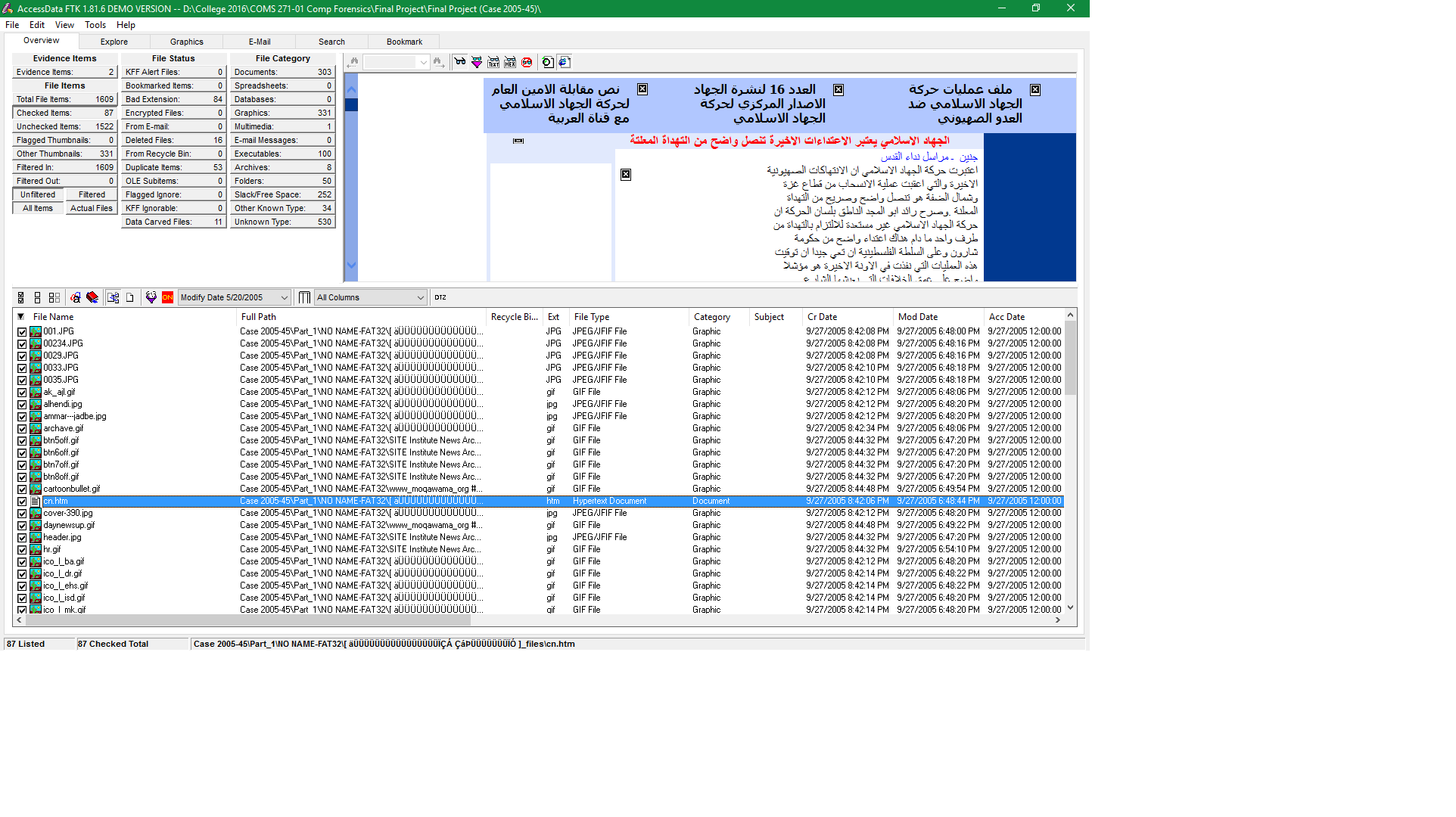
* Upon examination, the hard drive was found containing 1609 files total including a downloaded file containing graphic image files from a website with possible jihadist affiliation. All files and Images were exported from the drive using AccessData FTK 1.81.6.

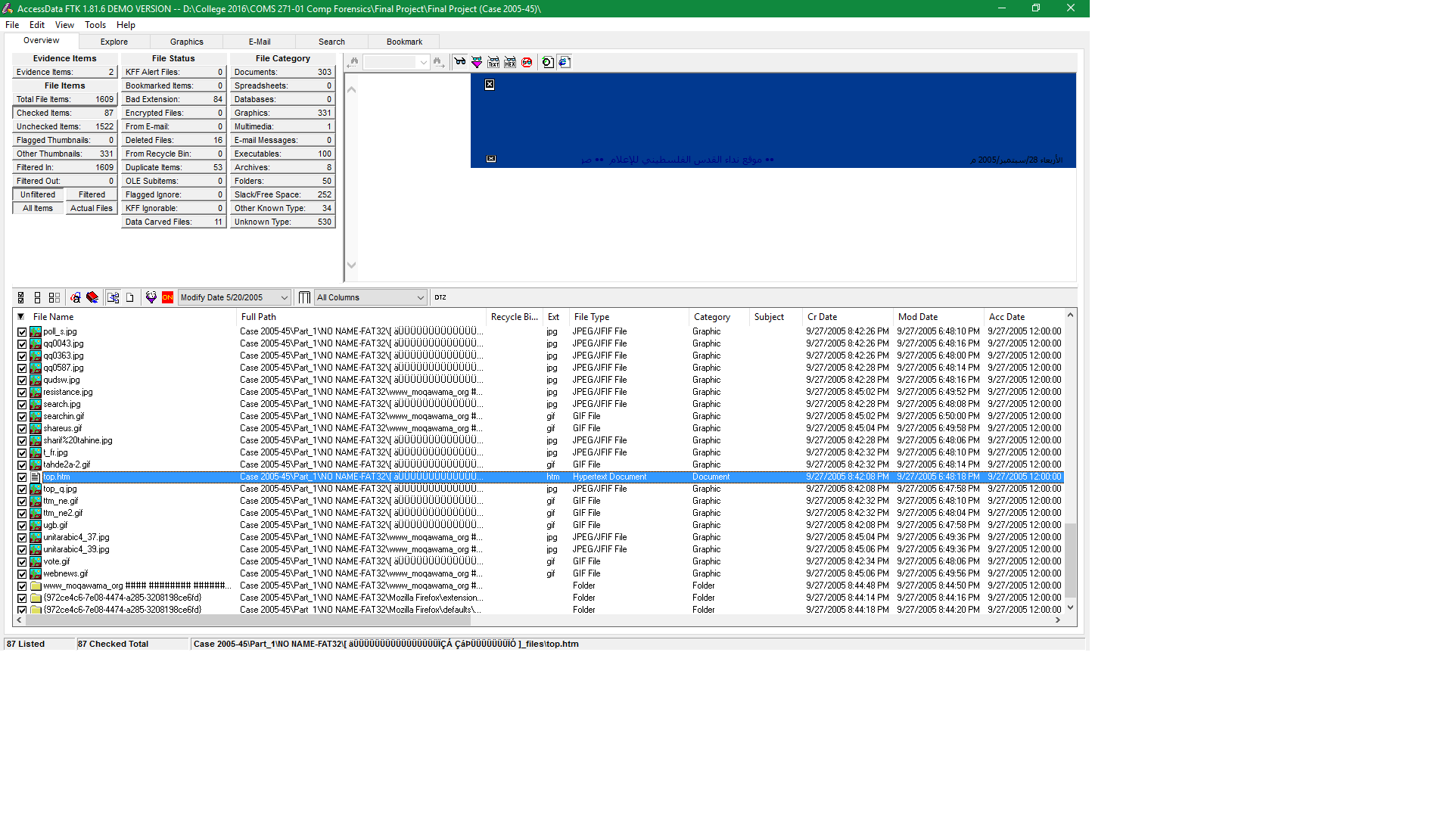












# Investigational Summary:

Examination of the suspect drive showed the presence of the following items:

1. 3 files were downloaded from the internet including 2 Firefox extensions and 1 website, www\_moqawama\_org.
2. 84 image files were also downloaded onto the hard drive such as, jihad-islam.jpg, jihad.jpg, Israel.jpg, and alhendi.jpg, etc.
3. 2 htm files were also downloaded containing images splashed in Arabic writing.

Based on the evidence uncovered, the Librarian was contacted at 10am on Wednesday, April 29th, and informed that there is a likelihood that the computer the patron was using was used in suspicious acts that may threaten national security. She was informed that she would have the full report later that evening.

# Case Log of Forensic Examination of subject Drive:

12/20/2016 9:02:26 PM -- FTK Version 1.81.6 build 10.04.02

FTK Exe Path: C:\Program Files (x86)\AccessData\AccessData Forensic Toolkit 1.81.6\Program\ftk.exe

Examiner's Machine:

Phys Mem: Total: 4,294,299,648 Available: 1,842,634,752 Used: 2,451,664,896

Virt Mem: Total: 4,294,836,224 Available: 3,466,301,440 Used: 828,534,784

Page File Available: 4,294,967,295

----------------------------------------------------

12/20/2016 9:02:26 PM -- KFF database being used: none

12/20/2016 9:02:26 PM -- Examiner's Local Machine Setting is time zone used for file times (create, modify, accessed) in file display and reports.

12/20/2016 9:02:26 PM -- New case started by examiner Christian Hill using FTK version 1.81.6 build 10.04.02

Investigator: Christian Hill

Case Name: Final Project (Case 2005-45)

Case Number: Case 2005-45

Case Folder: D:\College 2016\COMS 271-01 Comp Forensics\Final Project\Final Project (Case 2005-45)

Description: Image for Comp Forensics Final Project

Case Log Options (NOT Case Reviewer Logging Options):

Log case and evidence events: Yes

Log error messages: Yes

Log bookmarking events: Yes

Log searching events: Yes

Log special searching events: Yes

Log other events: Yes

Log extended information: No

Processes to be performed:

File Extraction: Yes

File Identification: Yes

MD5 Hash: Yes

SHA1 Hash: Yes

KFF (Known File Filter): Yes

Entropy Test: Yes

Full Text Index: Yes

Prerender Thumbnails: Yes

File Listing Database: Yes

DB Include OLE-embedded items: No

DB Include Slack Files: No

DB Include image name in filename: Yes

HTML File Listing: No

Data Carving: Yes

Preprocess Registry Files: No

Decrypt EFS Files: Yes

Default Case Refinement Settings:

Add files only if they satisfy BOTH the file status and the file type criteria as follows:

File Status Criteria:

Deletion status: any

Encryption status: any

From email status: any

Duplicate status: any

OLE stream status: any

File Type Criteria:

documents: yes

spreadsheets: yes

databases: yes

graphics: yes

email messages: yes

executables: yes

archives: yes

folders: yes

other recognized: yes

unknown: yes

Default Index Refinement Settings:

Don't index KFF ignorable files

Index files only if they satisfy BOTH the file status and the file type criteria as follows:

File Status Criteria:

Deletion status: any

Encryption status: any

From email status: any

Duplicate status: any

OLE stream status: any

File Type Criteria:

documents: yes

spreadsheets: yes

databases: yes

graphics: yes

email messages: yes

executables: yes

archives: yes

folders: yes

other recognized: yes

unknown: yes

-- Evidence 1 --

Name/Number:

Location: D:\College 2016\COMS 271-01 Comp Forensics\Final Project\Image Files\Case 2005-45.001

Display name: Case 2005-45\Part\_1\NO NAME-FAT32

Type: Raw Drive Image, Partition, FAT32

Time Zone: America/New\_York

Comment:

Evidence-specific Case Refinement Settings:

Add all files

Evidence-specific Index Refinement Settings:

Index all files

-- Evidence 2 --

Name/Number:

Location: D:\College 2016\COMS 271-01 Comp Forensics\Final Project\Image Files\Case 2005-45.001

Display name: Case 2005-45\UnpartSpace

Type: Raw Drive Image, Partition, FAT32Unpartitioned Space

Comment:

Evidence-specific Case Refinement Settings:

Add all files

Evidence-specific Index Refinement Settings:

Index all files

12/20/2016 9:02:26 PM -- Starting to add evidence items...

12/20/2016 9:03:02 PM -- The file Case 2005-45\Part\_1\NO NAME-FAT32\DELL\ATAPI.EXE failed Outside In filtering and was filtered manually.

12/20/2016 9:03:03 PM -- The file Case 2005-45\Part\_1\NO NAME-FAT32\DELL\BLDBUBG.EXE failed Outside In filtering and was filtered manually.

\*\*\*A full listing of the FTK Case Activity Log may be viewed when reviewing the full FTK Forensic Report.

# Case Summary and Documentation:

The investigation and analysis of the suspects drive was performed, using a dedicated analysis drive, with AccessData’s FTK toolkit 1.81.6, ProDiscover Basic 64, and OSForensics. All software is registered to Forensics Limited, Inc. and documentation can be obtained for all software from the Lab Administrator of Forensics Limited, Inc.

# Drive image documentation and verification is as follows:

* Drive Interface Type: USB
* Drive Model: Maxtor 6E 020L0
* Size: 19.41 GB (20,842,859,520 bytes)
* Partitions: 2
* [Drive Geometry]
* Bytes/Sector: 512
* Total Cylinders: 2,534
* Total Sectors: 40,708,710
* Total Tracks: 646,170
* Tracks/Cylinders: 255
* MD5 Checksum: 9218a94a80da18c8ec14b695063b67a
* SHA1 checksum: dcc4117a25db572bc05f6b4a9147b12c9d50c74f

The full report can be viwed upon documented request of an authorized individual at Forensics Limited, Inc. Analysis Lab.

# Chain of Custody:

Case Number: Case 2005-45 Offense: Suspicious behavior

Submitting Officer: (Name/ID#) Christian Hill

Victim: Linda Joh

Date/Time Seized: 04/28/16 8:25 am Location of Seizure: West Flint Library

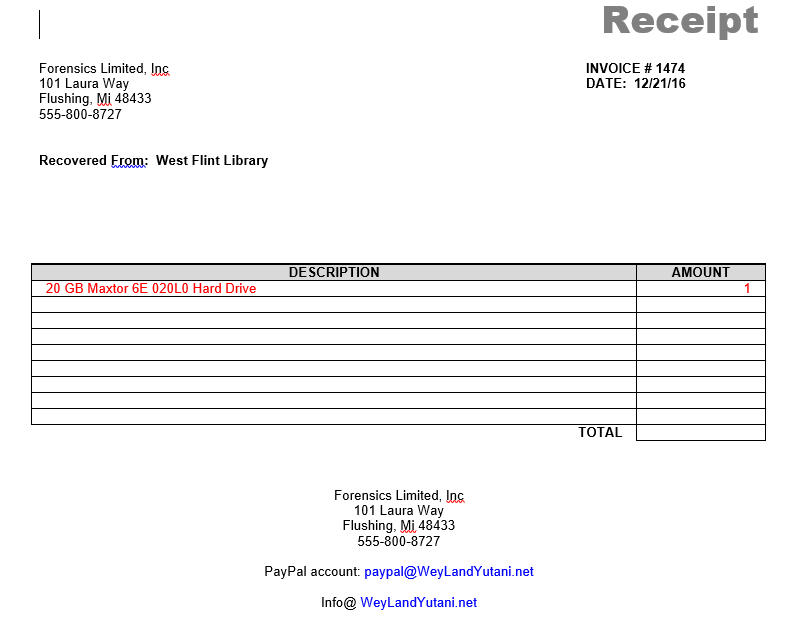
|  |  |  |
| --- | --- | --- |
| **Description of Evidence** | | |
| **Item #** | **Quantity** | **Description of Item** (Model, Serial #, Condition, Marks, Scratches) |
| 1 | 1 | 20 GB Maxtor 6E 020L0 hard drive |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Chain of Custody** | | | | |
| **Item #** | **Date/Time** | **Released by** (Signature & ID#) | **Received by** (Signature & ID#) | **Comments/Location** |
| 1 | 04/28/16 8:25 AM | Linda Johansen | Christian Hill | Analysis Lab 1 hour away from Library |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

APD\_Form\_#PE003\_v.1 (12/2012) Page 1 of 2 pages (See back)

|  |
| --- |
| **Final Disposal Authority** |
| **Authorization for Disposal**  Item(s) #: 1 item on this document pertaining to (suspect): Linda Johansen of West Flint Library\_ is(are) no longer needed as evidence and is/are authorized for disposal by (check appropriate disposal method) ☐ Return to Owner ☐ Auction/Destroy/Divert  Name & ID# of Authorizing Investigator: Christian Hill Date: 04/28/16 |
| **Witness to Destruction of Evidence**  Item(s) #: \_\_\_\_\_\_\_\_\_\_ on this document were destroyed by Evidence Custodian \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ID#:\_\_\_\_\_\_ in my presence on (date) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.  Name & ID# of Witness to destruction: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **Release to Lawful Owner**  Item(s) #: \_\_\_\_\_\_\_\_\_\_ on this document was/were released by Evidence Custodian \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ID#:\_\_\_\_\_\_\_\_\_ to  Name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ City: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_State: \_\_\_\_\_\_\_ Zip Code: \_\_\_\_\_\_\_\_\_\_ Telephone Number: (\_\_\_\_\_) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Under penalty of law, I certify that I am the lawful owner of the above item(s).  Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Copy of Government-issued photo identification is attached. ☐ Yes ☐ No |
| **This Evidence Chain-of-Custody form is to be retained as a permanent record by the Anywhere Police Department.** |
|  |

# Receipt:



# Exhibit A – Sanitization Policy

* All machines will be maintained with the latest anti-virus and anti-spyware patches from AVG, Avast, and Avira.
* Any drive to be used for forensics examination will be reformatted with a complete format before being used.
* All forensic machines will use an appropriate hardware based write blocker.

All forensic analysis workstations will not be connected to the Internet or to the company network in order to prevent any risk of being hacked.

# Exhibit B – FORENSIC HANDLING POLICY 12-20-16

to prevent cross contamination between cases and prior to use in any analysis or recovery, the working drive must be forensically sterile by performing a full reformat. The working drive is the drive used to store the target image. The working drive will have no other image files stored on it. After completion of each case, image files may be stored on an alternate data base system.

* Chain of Custody documentation must be maintained and accompany forensic recovery. Image files, original media or any other information is not to be disclosed to any third party unless required by law.
* All stored original media must be labeled by forensics case number.

# Exhibit C – HASH IMAGE VALIDATION POLICY 12-20-16

All recovered image Information must be validated as having an equivalent hash value with that of the original. The hash value may be either MD5 0r SHA-1 and must be included in the final report.