Mystery Master File Forensics Report

Examiner name: Timothy Kang

Date of submission: 4/2/18

Number of Pages: 19

Index

[Summary: 3](#_Toc510451421)

[Authentication: 4](#_Toc510451422)

[Physical Image Layout: 5](#_Toc510451423)

[Analysis Table: 9](#_Toc510451424)

[Item Details: 11](#_Toc510451425)

# Summary:

Before analyzing the master image which is called mysteryMaster.dd, a bit-by-bit copy is necessary. Unlike a normal backup which would only involve known files, this copy would contain everything ranging from deleted files to space that is considered empty. In order to do so, AccessData FTK Imager 3.1.2.0 was used. This software allowed me to create a physical copy called PhyMystery.001 and use forensic tools such as ProDiscover Basic and WinHex. In addition to creating this copy, it provides a verification window that shows a comparison of the MD5 and SHA1 Hash of both the master and physical copy. In this case, both hashes match so it is time to begin analyzing the image. This proves that the image file that I will be adding to the forensic tools is exactly the same as the master dd image.

First tool that was used was ProDiscover Basic. A new project was created and the image file was added. Once that has been done, ProDiscover allows you to view either the contents or clusters of the image file. One can see many files when looking at content view; 8 files of different file types can be seen. These file types include txt, zip, doc, jpg, flv, and bmp. In addition to this, the size of the files, the creation/modification/accessed date, parent folder, and whether or not the file has been deleted can be seen. For example, womanOfMystery.bmp, theTurtle.txt, and DietCoke+Mentos.flv have been deleted. However, ProDiscover is still able to show that these files once existed within the image. By double clicking the files, you are able to open the file and see the contents directly. Unfortunately, certain files such as womanOfMystery.bmp and DietCoke+Mentos.flv could not be opened at all. A perk of using ProDiscover is that by right clicking a file and doing “copy file,” you can save it on a desktop or a USB to easily transfer and open the file on a different computer. Since some of these files would not open, an attempt was made to extract as much information as possible from these files. I used Kali Linux and a tool called Foremost to do so. This allowed me to extract a zip file from the womanOfMystery.bmp file and an ole file from the DietCoke+Mentos.flv file. The zip file contained a document of the Declaration of Independence and the ole file contained the story of the Pied Piper. I was unable to succeed in figuring out what the contents of theTurtle.txt file was. This file opened properly in notepad but was filled with gibberish. Right clicking a file and clicking “Show Cluster Numbers” allow you to see the clusters associated with each file. Cluster view allows you to take a more indepth look at the clusters in hexadecimal and ASCII. ProDiscover shows the byte size of each file which can be really handy in calculating the cluster size and sector size. Sector size is the byte size divided by 512. Since sectors cannot be a decimal number, it is necessary to round up to the nearest ones place. Cluster size can be calculated once you have the sector size since cluster size is sector size divided by 32. This should also be rounded up to the nearest ones.

Using one tool is not enough. At least two forensic tools should be used to ensure that results match. I used WinHex for my second tool. Once you open a new case and put in the image file, this tool gives a very simple look at how the partitions are divided. In this case, there is unpartitioned space, a partition gap, unpartitionable space, and 1 partition with the FAT16 filesystem. To confirm the filesystem, I looked at the clusters, found the MBR partition table and signature value, and found the filesystem ID that confirmed that it was indeed FAT16. WinHex helped with understanding the physical image layout by showing the 1st sector location of each file, partition, and any space within the image. By observing these values, one can see that the deleted files share a 1st sector location with an undeleted file. This is why I predict that the “JFIF” within the gibberish of theTurtle.txt file could possible be referring to the iitRice.JPG file. In addition, since this tool also shows things like volume slack and boot sector of partition 1, we can see some ASCII values that we never would’ve seen. These interesting findings will be shown in the analysis table and item details section. For example, in the volume slack, there is a story that can be seen within this section that is unrelated to any of the 8 main files that we saw on ProDiscover.

# Authentication:

The program AccessData FTK Imager 3.1.2.0 was used to create a physical image file. As you can see in both the “Drive/Image Verify Results” and image summary text file screenshots, both files (mysteryMaster.dd and its physical image copy) have been verified to have the same MD5 Hash and SHA1 Hash.

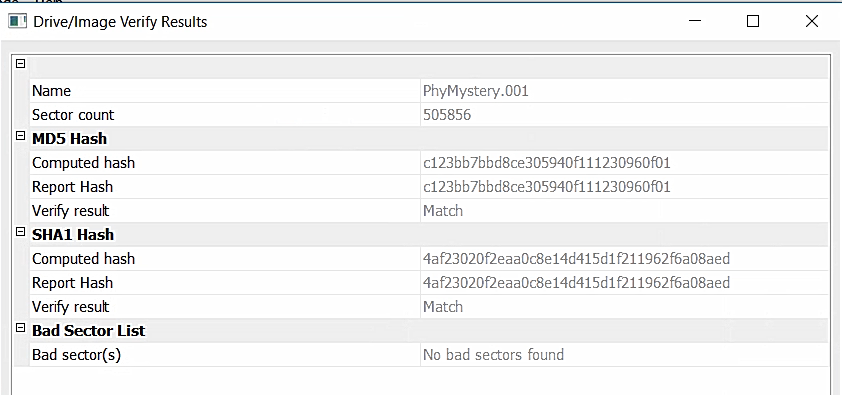


Fig 1.1: Screenshot of the “Drive/Image Verify Results” box after physical image has been created



Fig 1.2: Screenshot of the image summary text file once physical image was created.

# Physical Image Layout:

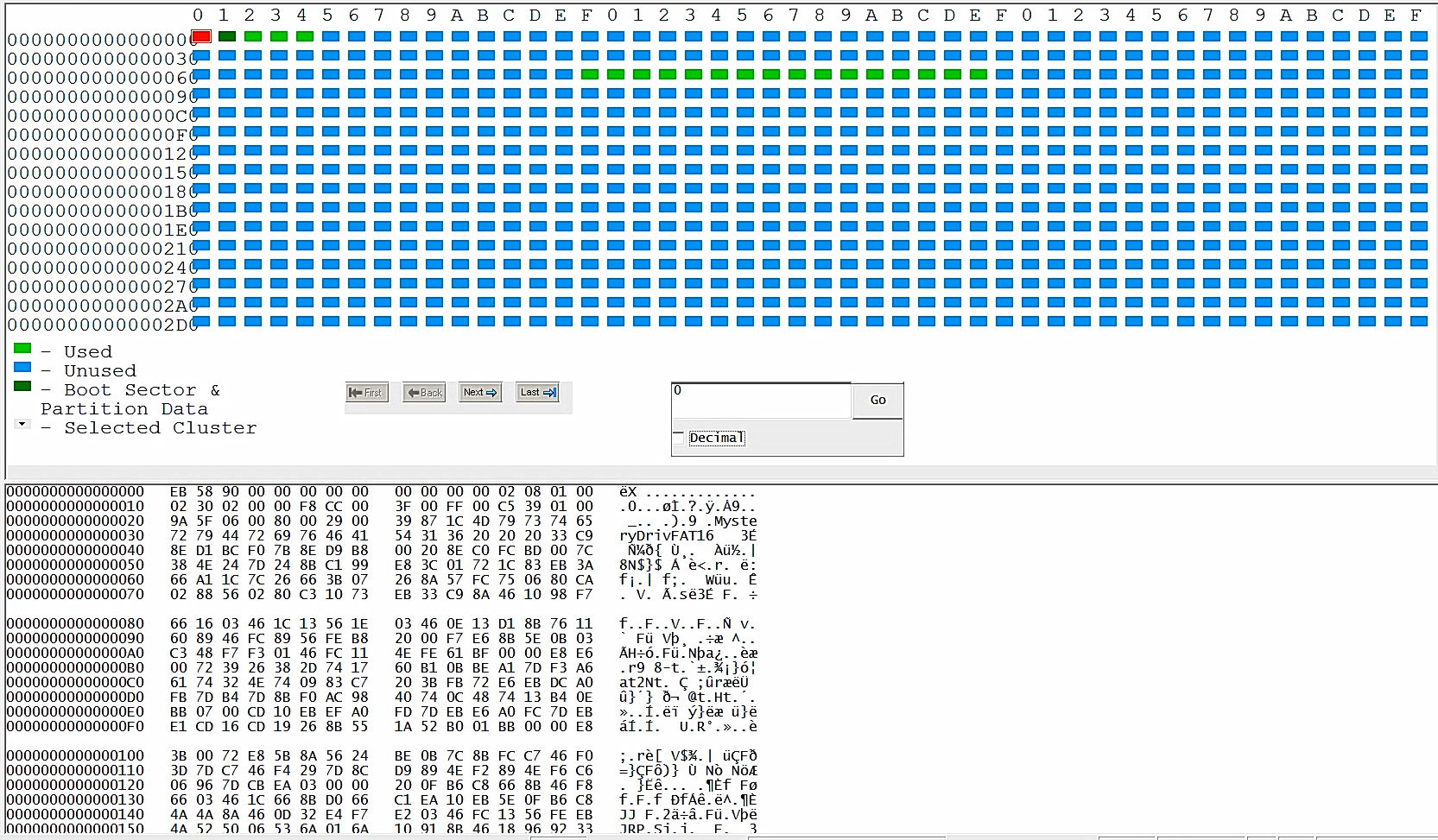


Fig 2.1: Cluster view in ProDiscover Basic

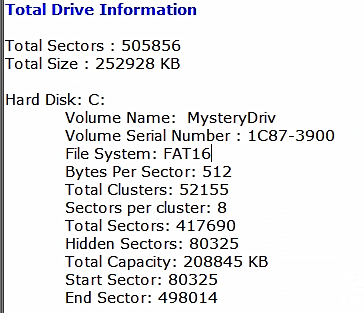


Fig 2.2: Basic Drive Information from Report in ProDiscover Basic

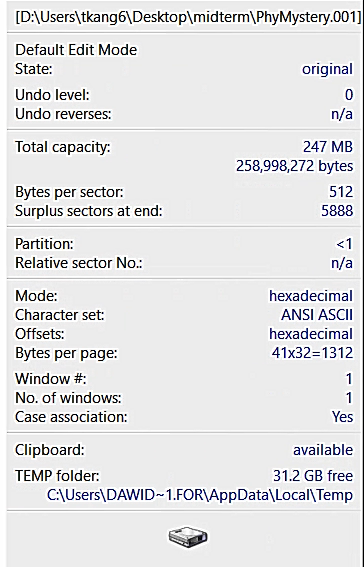


Fig 2.3: Basic Drive Information Report in WinHex

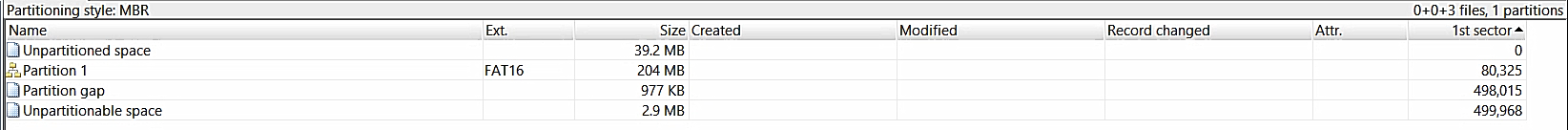


Fig 2.4: Layout information in WinHex

Based on the screenshot above, you can see the partitions and the starting locations of each; there is an unpartitioned space, partition 1 with the file system FAT16, a partition gap, and space that is unpartitionable. The next 3 images highlight the 3 parts of the MBR which are the boot code, partition table, and signature value

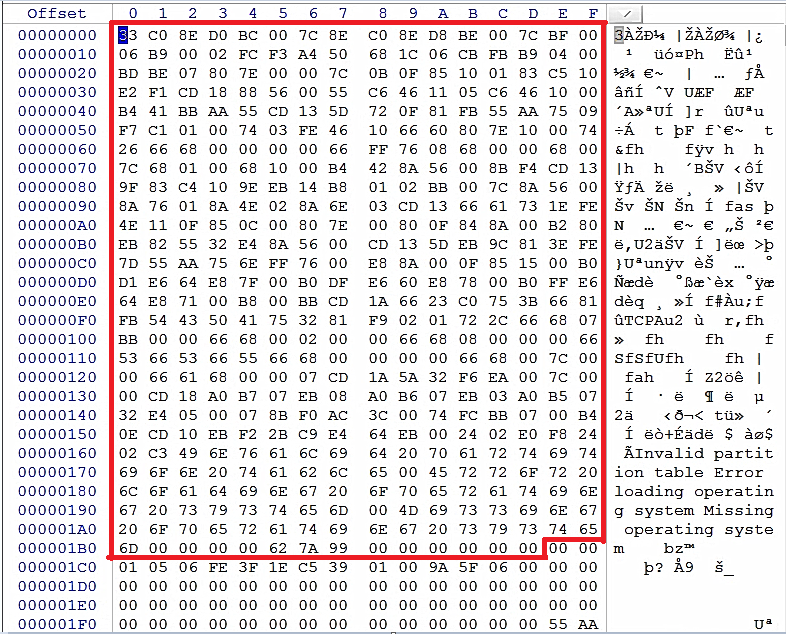


Fig 2.5: Boot code of MBR (Bytes 00 – 445 🡪 0x00 – 0x01BD

(highlighted in red)

This part of the MBR processes the partition table and allows the partition to be located.

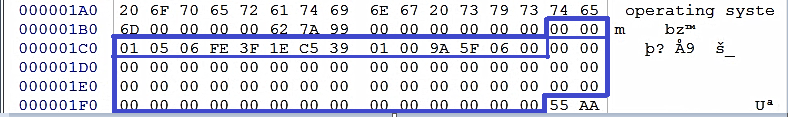


Fig 2.6: Partition Table (Bytes 446 – 509) 🡪 0x01BE – 0x01FD

(highlighted in blue)

First partition entry is highlighted using a thin blue line. There are no other partitions since the rest are 00s. This partition table entry reveals the file system ID. It is the 5th number on the entry so in this case, it is 06 which is a known system ID for FAT 16 (>=32MB).



Fig 2.7: MBR Signature (Bytes 510 – 0511)🡪 0x01FE – 0x01FF

(highlighted in green)

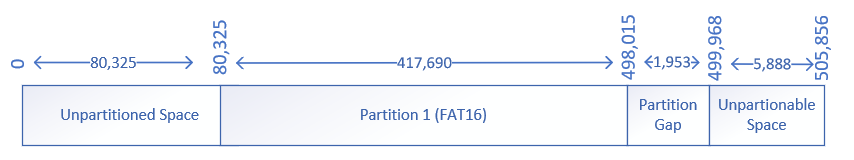


Fig 2.8: MBR partition layout

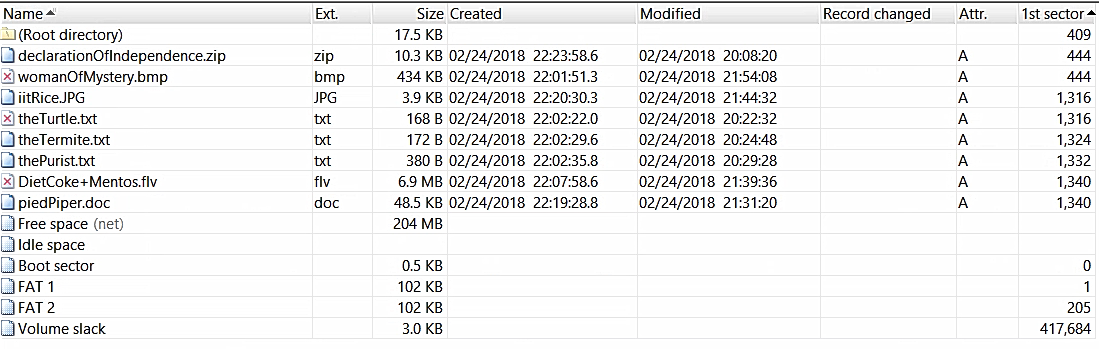


Fig 2.9: Screenshot of Partition 1 on WinHex

By using WinHex, you can see the various items that make up Partition 1. It includes the items that can also be seen in ProDiscover but also show things like Free space, Idle space, Boot sector, FAT 1, FAT 2, and Volume slack. One thing to note is that every deleted item has the same 1st sector location as another undeleted item on the list.

# Analysis Table:

(Hold Ctrl and left click the item # in order to find out more details about that specific item)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Item #** | **Item Description** | **General Location** | **Cluster Location /Size** | **Sector Location /Size** | **Size in bytes** |
| [1](#item1) | womanOfMystery.bmp | C:\womanOfMystery.bmp  Partition 1 | 2 (2)  3 (3)  4 (4)  / 28 | 444 / 868 | 444,054 |
| [2](#item2) | theTurtle.txt | C:\theTurtle.txt  Partition 1 | 6f (111)  / 1 | 1316 / 1 | 168 |
| [3](#item3) | theTermite.txt | C:\theTermite.txt  Partition 1 | 70 (112)  / 1 | 1324 / 1 | 172 |
| [4](#item4) | thePurist.txt | C:\thePurist.txt  Partition 1 | 71 (113)  / 1 | 1332 / 1 | 380 |
| [5](#item5) | DietCoke+Mentos.flv | C:\DietCoke+Mentos.flv  Partition 1 | 72 (114)  73 (115)  74 (116)  75 (117)  76 (118)  77 (119)  78 (120)  79 (121)  7a (122)  7b (123)  7c (124)  7d (125)  7e (126)  / 444 | 1340 / 14193 | 7,266,804 |
| [6](#item6) | piedPiper.doc | C:\piedPiper.doc  Partition 1 | 72 (114)  73 (115)  74 (116)  75 (117)  76 (118)  77 (119)  78 (120)  79 (121)  7a (122)  7b (123)  7c (124)  7d (125)  7e (126)  / 4 | 1340 / 97 | 49,664 |
| [7](#item7) | iitRice.JPG | C:\iitRice.JPG  Partition 1 | 6f (111)  / 1 | 1316 / 8 | 3,970 |
| [8](#item8) | declarationOfIndependence.zip | C:\declarationOfIndependence.zip  Partition 1 | 2 (2)  3 (3)  4 (4)  / 1 | 444 / 21 | 10,525 |
| [9](#item9) | Unpartitioned Space | Unpartitioned Space |  |  | 39,200,000 |
| [10](#item10) | Boot sector | Partition 1 |  |  | 500 |
| [11](#item11) | Volume slack | Partition 1 |  |  | 3,000 |

# Item Details:

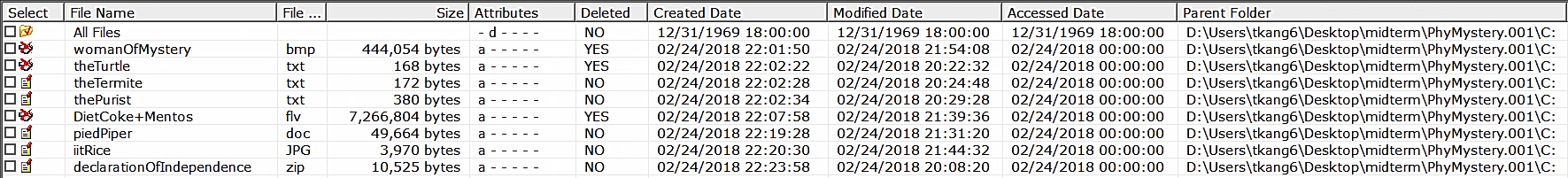


Fig 3.1: Screenshot of content view on ProDiscover Basic



Fig 3.2 Gallery view of Content on ProDiscover Basic

**Item #1:**

Filename: womanOfMystery.bmp

Deleted: Yes

The bmp file could not be opened but I was able to extract a declarationOfIndependence.doc file from it.

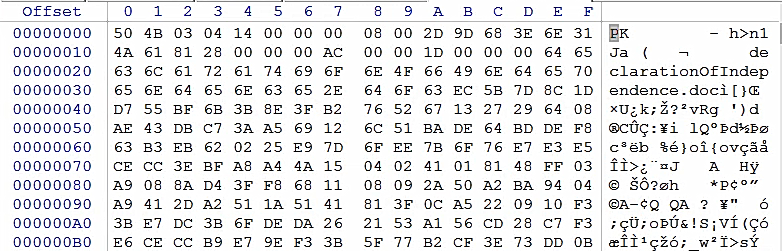


Fig 3.3: Beginning hex figures of womanOfMystery.bmp

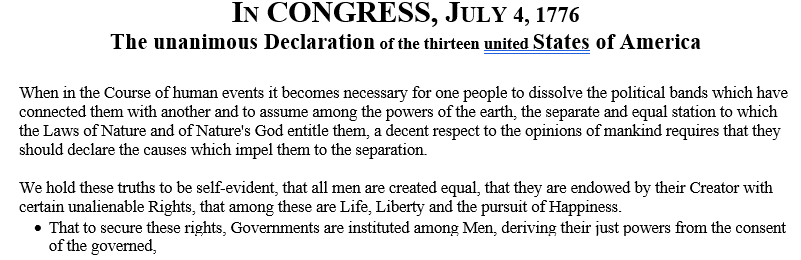


Fig 3.4: Partial screenshot of declarationOfIndependence.doc that was extracted from the bmp file

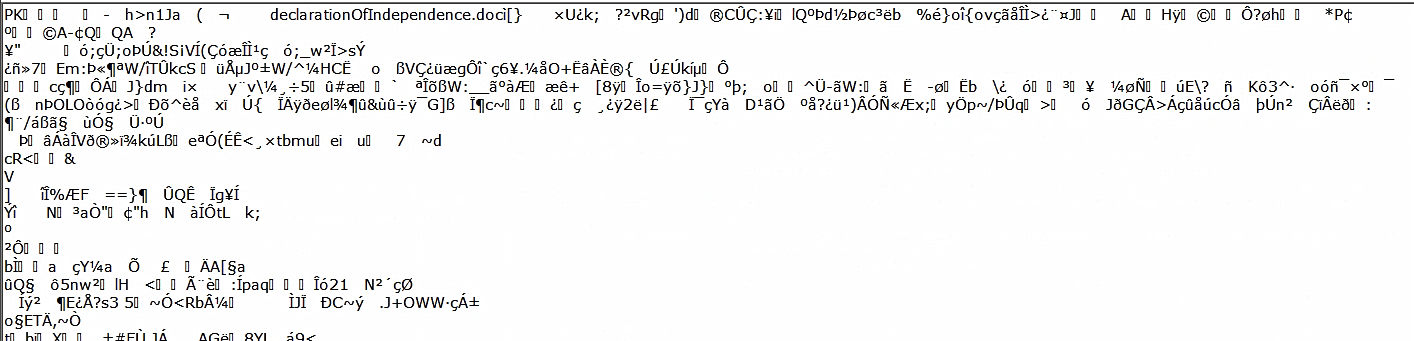


Fig 3.5: Partial screenshot of womanOfMystery.bmp on ProDiscover Basic

**Item #2:**

Filename: theTurtle.txt

Deleted: Yes

As you can see in both screenshots below, not much can be understood from this text file but it does say JFIF which is a file extension which involves JPEG compression and JPEGs are linked with images. Unfortunately, I was not successful in extracting any image but based on the sector locations of other files, it is possible that this JFIF may be referring to iitRice.jpg file.

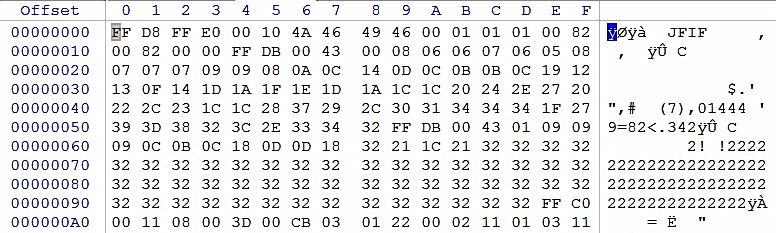


Fig 3.6: Beginning hex figures theTurtle.txt



Fig 3.7: Screenshot of theTurtle.txt on notepad

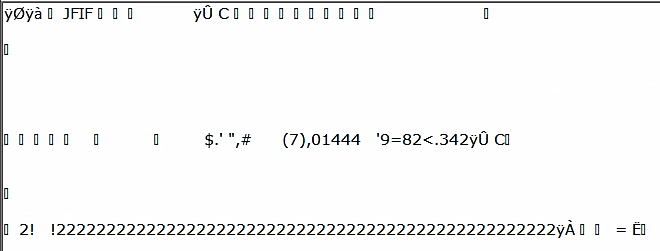


Fig 3.8: Screenshot of theTurtle.txt on ProDiscover Basic

**Item #3:**

Filename: theTermite.txt

Deleted: No

Simple text file that opened without any problems.

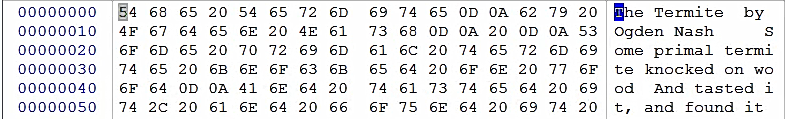


Fig 3.9: Beginning hex figures of theTermite.txt

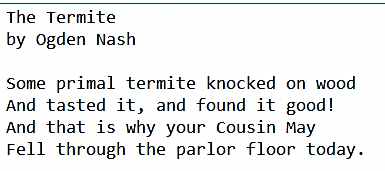


Fig 3.10: Screenshot of theTermite.txt

**Item #4:**

Filename: thePurist.txt

Deleted: No

Another text file that opened without any problems.

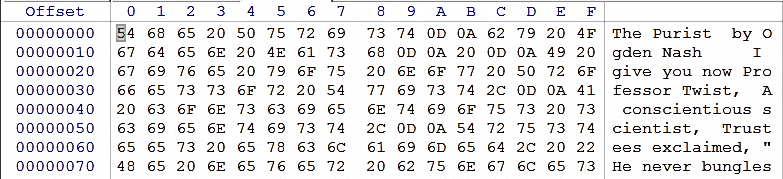


Fig 3.11: Beginning hex figures of thePurist.txt

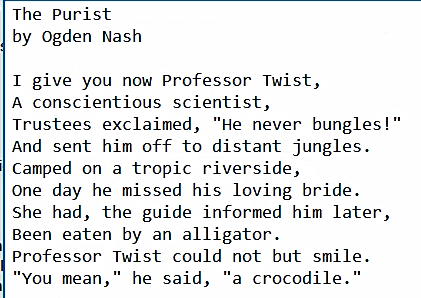


Fig 3.12: Screenshot of thePurish.txt

**Item #5:**

Filename: DietCoke+mentos.flv

Deleted: Yes

Could not open this video file. However, by using foremost on Kali, an OLE file was extracted from the flv file. The story within the file was the story of the Pied Piper.

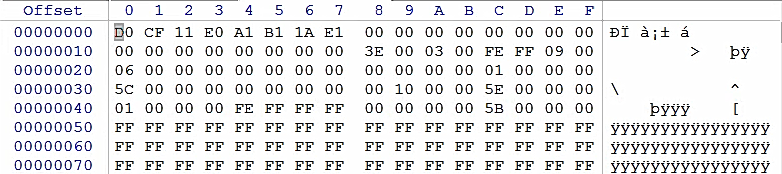


Fig 3:13: Beginning hex figures of DietCoke+mentos.flv

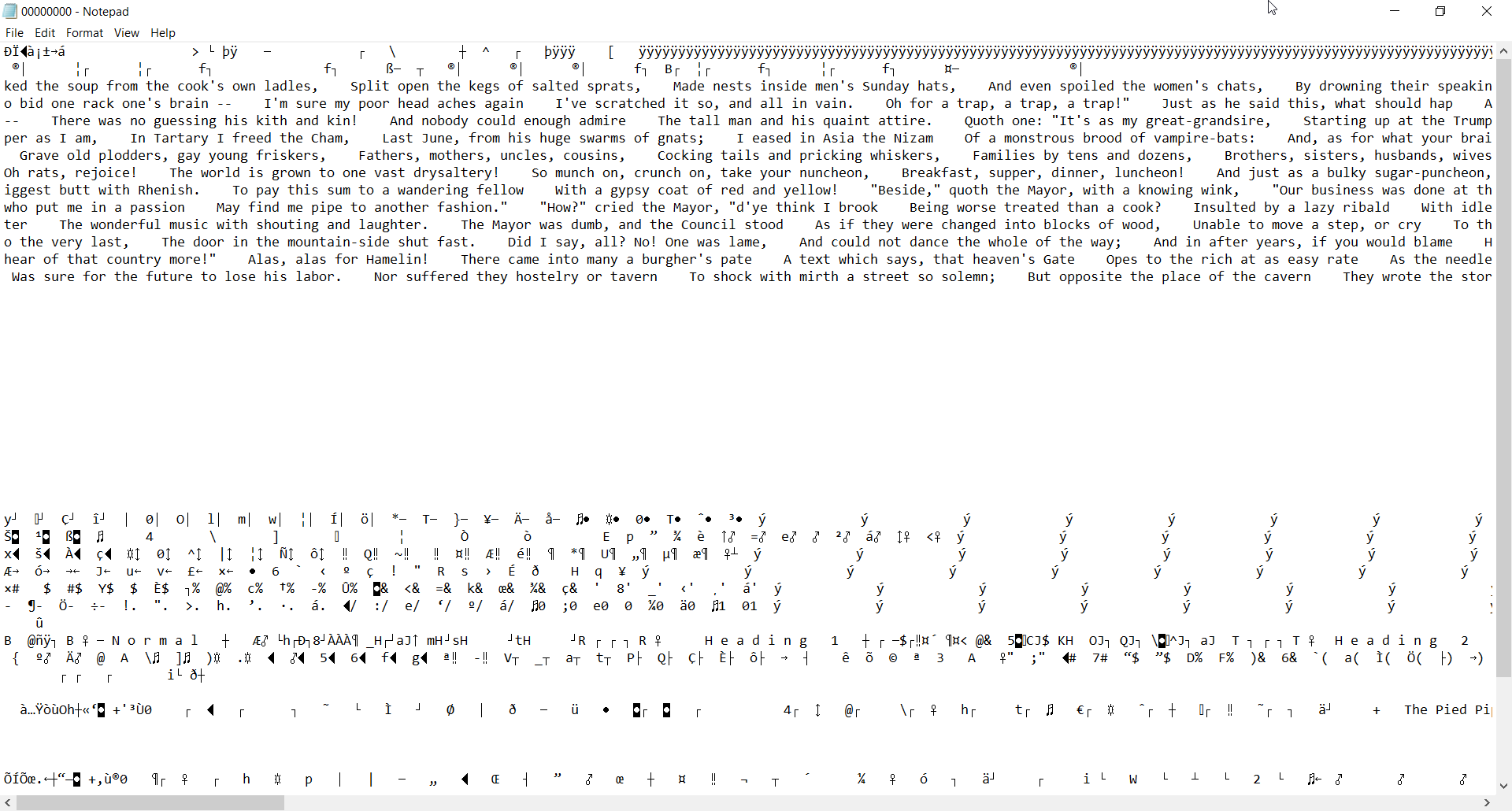


Fig 3.14: Screenshot of the OLE file

**Item #6:**

Filename: piedPiper.doc

Deleted: No

This document opened without any problems.

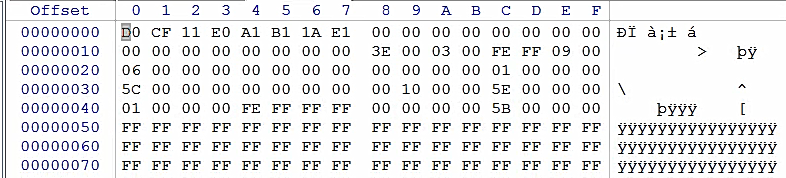


Fig 3.15: Beginning hex figures of piedPiper.doc

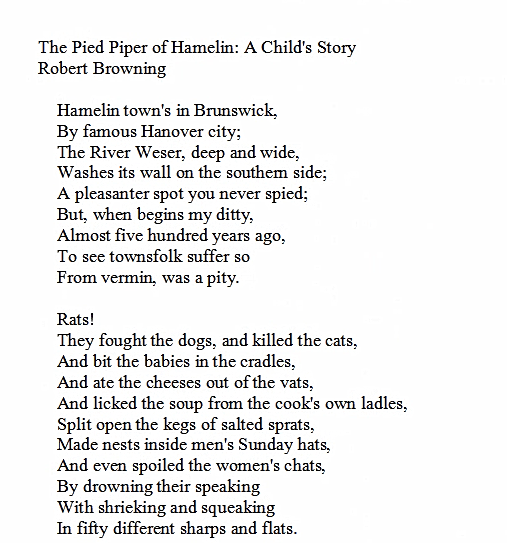


Fig 3.16: Screenshot of piedPiper.doc (only a small segment since total is 6 pages)

**Item #7:**

Filename; iitRice.JPG

Deleted: No

This image opened without any problems.

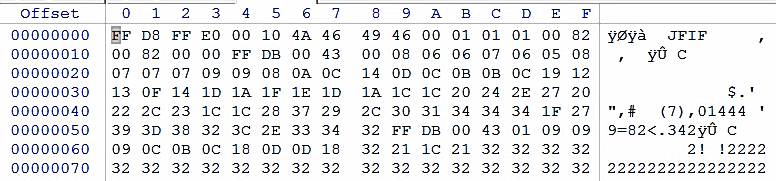


Fig 3.17: Beginning hex figures of iitRice.JPG



Fig 3.18: Screenshot of iitRice.JPG

**File #8:**

Filename: declarationOfIndependence.zip

Deleted: No

Within the zip file: declarationOfIndepedence.doc. There were no problems in unzipping the file and opening the document within.

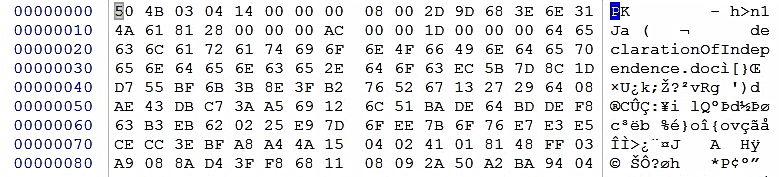


Fig 3.19: Beginning hex figures of declarationOfIndependence.zip

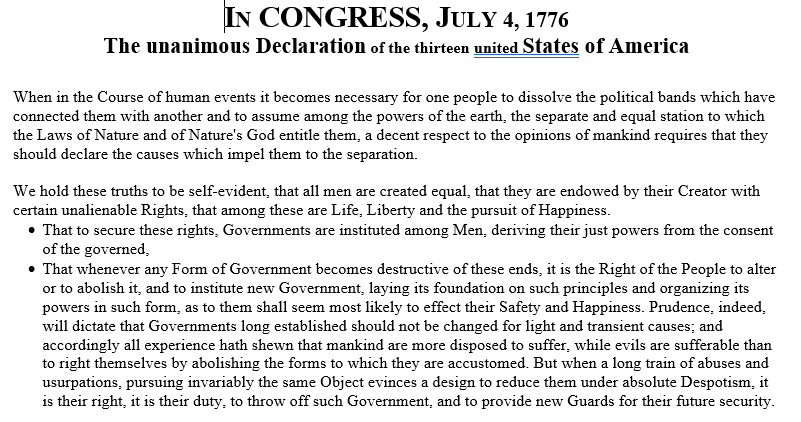


Fig 3.20: Screenshot of declarationOfIndepedence.doc (only a small segment since total is 3 pages)

**File #9:**

Interesting part of Unpartitioned space

It says “Invalid partition table Error loading operating system Missing operating system.”



Fig 3.21: Screenshot of part of Unpartitioned space

**File #10:**

Interesting part of Boot sector (within Partition 1)

It says “NTLDR is missing Disk error Press any key to restart”

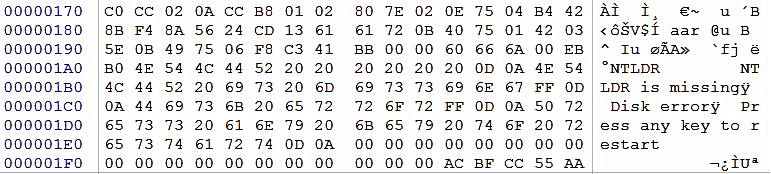


Fig 3.22: Screenshot of part of Boot sector

**File #11**

Interesting part of Volume slack (within Partition 1)

There is a small section within the Volume slack with a random story.

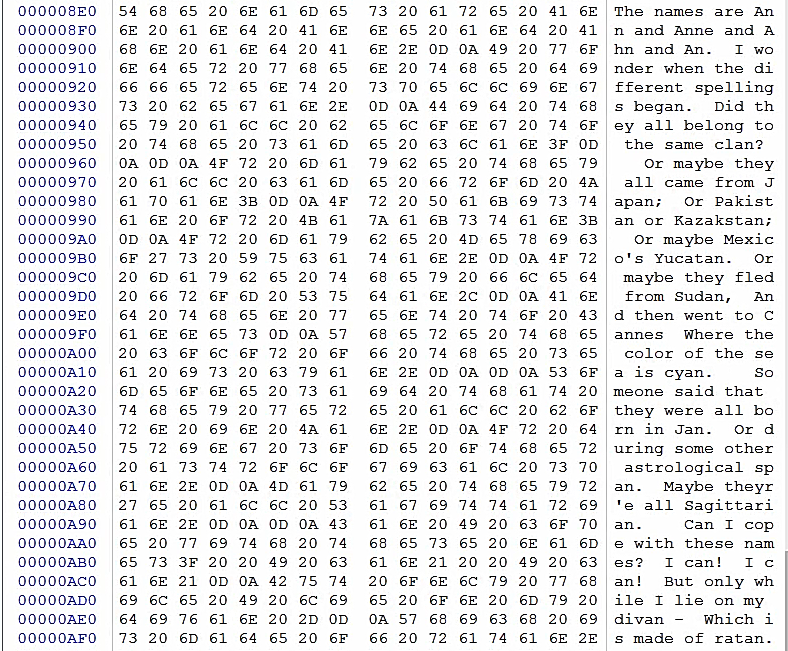


Fig 3.23: Screenshot of part of Volume slack