

Mystery Master File Forensics Report

Examiner name: Timothy Kang

Date of submission: 4/2/18

Number of Pages: 19

Index

Summary:	3
Authentication:	4
Physical Image Layout:	5
Analysis Table:.....	9
Item Details:	11

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 the `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 the `theTurtle.txt` file could possibly 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.

Drive/Image Verify Results	
Name	PhyMystery.001
Sector count	505856
MD5 Hash	
Computed hash	c123bb7bbd8ce305940f111230960f01
Report Hash	c123bb7bbd8ce305940f111230960f01
Verify result	Match
SHA1 Hash	
Computed hash	4af23020f2eaa0c8e14d415d1f211962f6a08aed
Report Hash	4af23020f2eaa0c8e14d415d1f211962f6a08aed
Verify result	Match
Bad Sector List	
Bad sector(s)	No bad sectors found

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

```

Created By AccessData® FTK® Imager 3.1.2.0

Case Information:
Acquired using: ADI3.1.2.0
Case Number:
Evidence Number:
Unique Description:
Examiner:
Notes:
-----

Information for D:\Users\tkang6\Desktop\midterm\PhyMystery:

Physical Evidentiary Item (Source) Information:
[Device Info]
Source Type: Physical
[Drive Geometry]
Bytes per Sector: 512
Sector Count: 505,856
[Image]
Image Type: Raw (dd)
Source data size: 247 MB
Sector count: 505856
[Computed Hashes]
MD5 checksum: c123bb7bbd8ce305940f111230960f01
SHA1 checksum: 4af23020f2eaa0c8e14d415d1f211962f6a08aed

Image Information:
Acquisition started: Wed Mar 28 12:22:21 2018
Acquisition finished: Wed Mar 28 12:22:23 2018
Segment list:
D:\Users\tkang6\Desktop\midterm\PhyMystery.001

Image Verification Results:
Verification started: Wed Mar 28 12:22:23 2018
Verification finished: Wed Mar 28 12:22:25 2018
MD5 checksum: c123bb7bbd8ce305940f111230960f01 : verified
SHA1 checksum: 4af23020f2eaa0c8e14d415d1f211962f6a08aed : verified

```

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

Physical Image Layout:

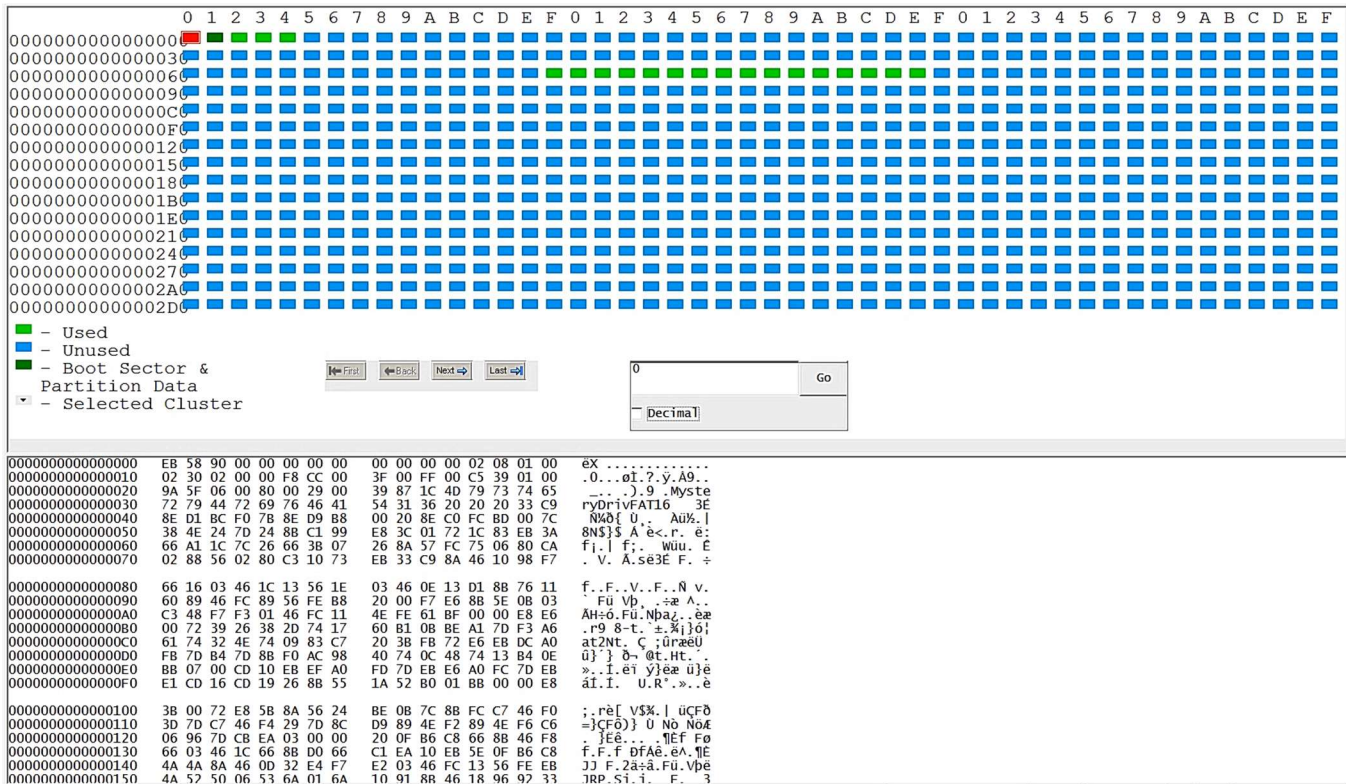


Fig 2.1: Cluster view in ProDiscover Basic

Total Drive Information

Total Sectors : 505856

Total Size : 252928 KB

Hard Disk: C:

Volume Name: MysteryDriv

Volume Serial Number : 1C87-3900

File System: FAT16|

Bytes Per Sector: 512

Total Clusters: 52155

Sectors per cluster: 8

Total Sectors: 417690

Hidden Sectors: 80325

Total Capacity: 208845 KB

Start Sector: 80325

End Sector: 498014

Fig 2.2: Basic Drive Information from Report in ProDiscover Basic

[D:\Users\tkang6\Desktop\midterm\PhyMystery.001]

Default Edit Mode	
State:	original
Undo level:	0
Undo reverses:	n/a
Total capacity: 247 MB 258,998,272 bytes	
Bytes per sector:	512
Surplus sectors at end:	5888
Partition:	<1
Relative sector No.:	n/a
Mode:	hexadecimal
Character set:	ANSI ASCII
Offsets:	hexadecimal
Bytes per page:	41x32=1312
Window #:	1
No. of windows:	1
Case association:	Yes
Clipboard:	available
TEMP folder:	31.2 GB free C:\Users\DAWID~1\FOR\AppData\Local\Temp




Fig 2.3: Basic Drive Information Report in WinHex

Partitioning style: MBR							0+0+3 files, 1 partitions
Name	Ext.	Size	Created	Modified	Record changed	Attr.	1st sector
Unpartitioned space		39.2 MB					0
Partition 1	FAT16	204 MB					80,325
Partition gap		977 KB					498,015
Unpartitionable space		2.9 MB					499,968

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

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	33	C0	8E	D0	BC	00	7C	8E	C0	8E	D8	BE	00	7C	BF	00	3ÅŽĐ¼ žÀž0¾ ç
00000010	06	B9	00	02	FC	F3	A4	50	68	1C	06	CB	FB	B9	04	00	¹ üó=Ph Ěú¹
00000020	BD	BE	07	80	7E	00	00	7C	0B	0F	85	10	01	83	C5	10	¼¼ e~ ... fÅ
00000030	E2	F1	CD	18	88	56	00	55	C6	46	11	05	C6	46	10	00	añí ^v UeF EF
00000040	B4	41	BB	AA	55	CD	13	5D	72	0F	81	FB	55	AA	75	09	'A>ªUí]r ûUªu
00000050	F7	C1	01	00	74	03	FE	46	10	66	60	80	7E	10	00	74	÷Á t pF f`e~ t
00000060	26	66	68	00	00	00	00	66	FF	76	08	68	00	00	68	00	&fh fyv h h
00000070	7C	68	01	00	68	10	00	B4	42	8A	56	00	8B	F4	CD	13	h h 'BŠV <óí
00000080	9F	83	C4	10	9E	EB	14	B8	01	02	BB	00	7C	8A	56	00	ŸfÅ žē , » ŠV
00000090	8A	76	01	8A	4E	02	8A	6E	03	CD	13	66	61	73	1E	FE	Šv ŠN Šn í fas p
000000A0	4E	11	0F	85	0C	00	80	7E	00	80	0F	84	8A	00	B2	80	N ... e~ e „š ºe
000000B0	EB	82	55	32	E4	8A	56	00	CD	13	5D	EB	9C	81	3E	FE	ě,U2äŠV í]ěœ >p
000000C0	7D	55	AA	75	6E	FF	76	00	E8	8A	00	0F	85	15	00	B0	}Uªunÿv èš ... °
000000D0	D1	E6	64	E8	7F	00	B0	DF	E6	60	E8	78	00	B0	FF	E6	Nædè °œ`èx °ÿæ
000000E0	64	E8	71	00	B8	00	BB	CD	1A	66	23	C0	75	3B	66	81	dèq , »Í f#Àu;f
000000F0	FB	54	43	50	41	75	32	81	F9	02	01	72	2C	66	68	07	ûTCPAu2 ù r,fh
00000100	BB	00	00	66	68	00	02	00	00	66	68	08	00	00	00	66	» fh fh f
00000110	53	66	53	66	55	66	68	00	00	00	00	66	68	00	7C	00	sfsfUfh fh
00000120	00	66	61	68	00	00	07	CD	1A	5A	32	F6	EA	00	7C	00	fah í z2öê
00000130	00	CD	18	A0	B7	07	EB	08	A0	B6	07	EB	03	A0	B5	07	í · e ¶ e µ
00000140	32	E4	05	00	07	8B	F0	AC	3C	00	74	FC	BB	07	00	B4	2ä <ð-< tü» ´
00000150	0E	CD	10	EB	F2	2B	C9	E4	64	EB	00	24	02	E0	F8	24	í èð+Éädè \$ àø\$
00000160	02	C3	49	6E	76	61	6C	69	64	20	70	61	72	74	69	74	ÅInvalid partit
00000170	69	6F	6E	20	74	61	62	6C	65	00	45	72	72	6F	72	20	ion table Error
00000180	6C	6F	61	64	69	6E	67	20	6F	70	65	72	61	74	69	6E	loading operatin
00000190	67	20	73	79	73	74	65	6D	00	4D	69	73	73	69	6E	67	g system Missing
000001A0	20	6F	70	65	72	61	74	69	6E	67	20	73	79	73	74	65	operating syste
000001B0	6D	00	00	00	00	62	7A	99	00	00	00	00	00	00	00	00	m bz™
000001C0	01	05	06	FE	3F	1E	C5	39	01	00	9A	5F	06	00	00	00	p? Å9 š_
000001D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000001F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	55	AA	Uª

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.

000001A0	20	6F	70	65	72	61	74	69	6E	67	20	73	79	73	74	65	operating syste
000001B0	6D	00	00	00	00	62	7A	99	00	00	00	00	00	00	00	00	m bz™
000001C0	01	05	06	FE	3F	1E	C5	39	01	00	9A	5F	06	00	00	00	p? Å9 š_
000001D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000001F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	55	AA	Uª

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).

000001C0	01 05 06 FE 3F 1E C5 39 01 00 9A 5F 06 00 00 00	p? Å9 š _
000001D0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
000001E0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
000001F0	00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA	Uª

Fig 2.7: MBR Signature (Bytes 510 – 0511)→ 0x01FE – 0x01FF
(highlighted in green)

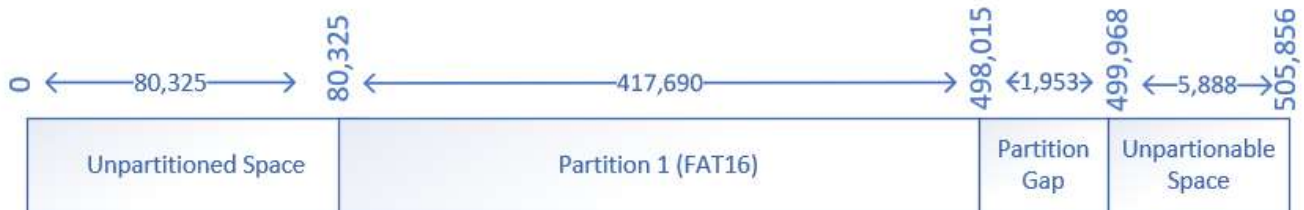


Fig 2.8: MBR partition layout

Name	Ext.	Size	Created	Modified	Record changed	Attr.	1st sector
(Root directory)		17.5 KB					409
declarationOfIndependence.zip	zip	10.3 KB	02/24/2018 22:23:58.6	02/24/2018 20:08:20		A	444
womanOfMystery.bmp	bmp	434 KB	02/24/2018 22:01:51.3	02/24/2018 21:54:08		A	444
iitRice.JPG	JPG	3.9 KB	02/24/2018 22:20:30.3	02/24/2018 21:44:32		A	1,316
theTurtle.txt	txt	168 B	02/24/2018 22:02:22.0	02/24/2018 20:22:32		A	1,316
theTermite.txt	txt	172 B	02/24/2018 22:02:29.6	02/24/2018 20:24:48		A	1,324
thePurist.txt	txt	380 B	02/24/2018 22:02:35.8	02/24/2018 20:29:28		A	1,332
DietCoke+Mentos.flv	flv	6.9 MB	02/24/2018 22:07:58.6	02/24/2018 21:39:36		A	1,340
piedPiper.doc	doc	48.5 KB	02/24/2018 22:19:28.8	02/24/2018 21:31:20		A	1,340
Free space (net)		204 MB					
Idle space							
Boot sector		0.5 KB					0
FAT 1		102 KB					1
FAT 2		102 KB					205
Volume slack		3.0 KB					417,684

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	womanOfMystery.bmp	C:\womanOfMystery.bmp Partition 1	2 (2) 3 (3) 4 (4) / 28	444 / 868	444,054
2	theTurtle.txt	C:\theTurtle.txt Partition 1	6f (111) / 1	1316 / 1	168
3	theTermite.txt	C:\theTermite.txt Partition 1	70 (112) / 1	1324 / 1	172
4	thePurist.txt	C:\thePurist.txt Partition 1	71 (113) / 1	1332 / 1	380
5	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	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	iitRice.JPG	C:\iitRice.JPG Partition 1	6f (111) / 1	1316 / 8	3,970

8	declarationOfIndependence.zip	C:\declarationOfIndependence.zip Partition 1	2 (2) 3 (3) 4 (4) / 1	444 / 21	10,525
9	Unpartitioned Space	Unpartitioned Space			39,200,000
10	Boot sector	Partition 1			500
11	Volume slack	Partition 1			3,000

Item Details:

Select	File Name	File ...	Size	Attributes	Deleted	Created Date	Modified Date	Accessed Date	Parent Folder
<input type="checkbox"/>	All Files			- d - - - -	NO	12/31/1969 18:00:00	12/31/1969 18:00:00	12/31/1969 18:00:00	D:\Users\kang6\Desktop\midterm\PhyMystery.001\C:
<input checked="" type="checkbox"/>	womanOfMystery	bmp	444,054 bytes	a - - - - -	YES	02/24/2018 22:01:50	02/24/2018 21:54:08	02/24/2018 00:00:00	D:\Users\kang6\Desktop\midterm\PhyMystery.001\C:
<input checked="" type="checkbox"/>	theTurtle	txt	168 bytes	a - - - - -	YES	02/24/2018 22:02:22	02/24/2018 20:22:32	02/24/2018 00:00:00	D:\Users\kang6\Desktop\midterm\PhyMystery.001\C:
<input checked="" type="checkbox"/>	theTermite	txt	172 bytes	a - - - - -	NO	02/24/2018 22:02:28	02/24/2018 20:24:48	02/24/2018 00:00:00	D:\Users\kang6\Desktop\midterm\PhyMystery.001\C:
<input checked="" type="checkbox"/>	thePurist	txt	380 bytes	a - - - - -	NO	02/24/2018 22:02:34	02/24/2018 20:29:28	02/24/2018 00:00:00	D:\Users\kang6\Desktop\midterm\PhyMystery.001\C:
<input checked="" type="checkbox"/>	DietCoke+Mentos	flv	7,266,804 bytes	a - - - - -	YES	02/24/2018 22:07:58	02/24/2018 21:39:36	02/24/2018 00:00:00	D:\Users\kang6\Desktop\midterm\PhyMystery.001\C:
<input checked="" type="checkbox"/>	piedPiper	doc	49,664 bytes	a - - - - -	NO	02/24/2018 22:19:28	02/24/2018 21:31:20	02/24/2018 00:00:00	D:\Users\kang6\Desktop\midterm\PhyMystery.001\C:
<input checked="" type="checkbox"/>	itRice	JPG	3,970 bytes	a - - - - -	NO	02/24/2018 22:20:30	02/24/2018 21:44:32	02/24/2018 00:00:00	D:\Users\kang6\Desktop\midterm\PhyMystery.001\C:
<input checked="" type="checkbox"/>	declarationOfIndependence	zip	10,525 bytes	a - - - - -	NO	02/24/2018 22:23:58	02/24/2018 20:08:20	02/24/2018 00:00:00	D:\Users\kang6\Desktop\midterm\PhyMystery.001\C:

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.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	50	4B	03	04	14	00	00	00	08	00	2D	9D	68	3E	6E	31	PK - h>n1
00000010	4A	61	81	28	00	00	00	AC	00	00	1D	00	00	00	64	65	Ja (- de
00000020	63	6C	61	72	61	74	69	6F	6E	4F	66	49	6E	64	65	70	clarationOfIndep
00000030	65	6E	64	65	6E	63	65	2E	64	6F	63	EC	5B	7D	8C	1D	endence.doci[]E
00000040	D7	55	BF	6B	3B	8E	3F	B2	76	52	67	13	27	29	64	08	xU;k;Z?vRg ')d
00000050	AE	43	DB	C7	3A	A5	69	12	6C	51	BA	DE	64	BD	DE	F8	@CÛç:¥i lQ°Pd½Pø
00000060	63	B3	EB	62	02	25	E9	7D	6F	EE	7B	6F	76	E7	E3	E5	c³eb ¢é}oi{ovçãã
00000070	CE	CC	3E	BF	A8	A4	4A	15	04	02	41	01	81	48	FF	03	Îî>ç"=J A Hÿ
00000080	A9	08	8A	D4	3F	F8	68	11	08	09	2A	50	A2	BA	94	04	© ŠÔ?øh *Pç°"
00000090	A9	41	2D	A2	51	1A	51	41	81	3F	0C	A5	22	09	10	F3	©A-çQ QA ? ¥" ó
000000A0	3B	E7	DC	3B	6F	DE	DA	26	21	53	A1	56	CD	28	C7	F3	;çÛ;øPÛ&!S;VÍ(çó
000000B0	E6	CE	CC	B9	E7	9E	F3	3B	5F	77	B2	CF	3E	73	DD	0B	æÎî¹çžó;_w²î>sÝ

Fig 3.3: Beginning hex figures of womanOfMystery.bmp

IN CONGRESS, JULY 4, 1776
The unanimous Declaration of the thirteen united States of America

When in the Course of human events it becomes necessary for one people to dissolve the political bands which have connected them with another and to assume among the powers of the earth, the separate and equal station to which the Laws of Nature and of Nature's God entitle them, a decent respect to the opinions of mankind requires that they should declare the causes which impel them to the separation.

We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness.

- That to secure these rights, Governments are instituted among Men, deriving their just powers from the consent of the governed,

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

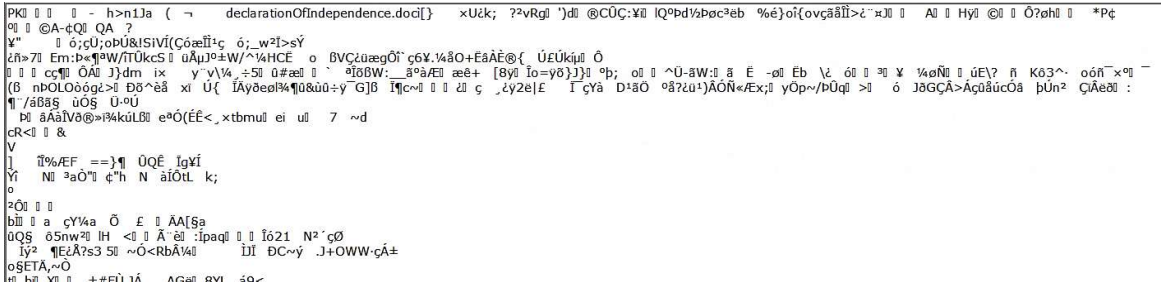


Fig 3.5: Partial screenshot of womanOfMystery.bmp on ProDiscover Basic

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.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	EF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	01	00	82	yøÿà JFIF ,
00000010	00	82	00	00	FF	DB	00	43	00	08	06	06	07	06	05	08	, yÛ c
00000020	07	07	07	09	09	08	0A	0C	14	0D	0C	0B	0B	0C	19	12	
00000030	13	0F	14	1D	1A	1F	1E	1D	1A	1C	1C	20	24	2E	27	20	\$. '
00000040	22	2C	23	1C	1C	28	37	29	2C	30	31	34	34	34	1F	27	",# (7),01444 '
00000050	39	3D	38	32	3C	2E	33	34	32	FF	DB	00	43	01	09	09	9=82<.342yÛ c
00000060	09	0C	0B	0C	18	0D	0D	18	32	21	1C	21	32	32	32	32	2! !2222
00000070	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	2222222222222222
00000080	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	2222222222222222
00000090	32	32	32	32	32	32	32	32	32	32	32	32	32	32	FF	C0	2222222222222222ÿÀ
000000A0	00	11	08	00	3D	00	CB	03	01	22	00	02	11	01	03	11	= È "

Fig 3.6: Beginning hex figures theTurtle.txt



Fig 3.7: Screenshot of theTurtle.txt on notepad

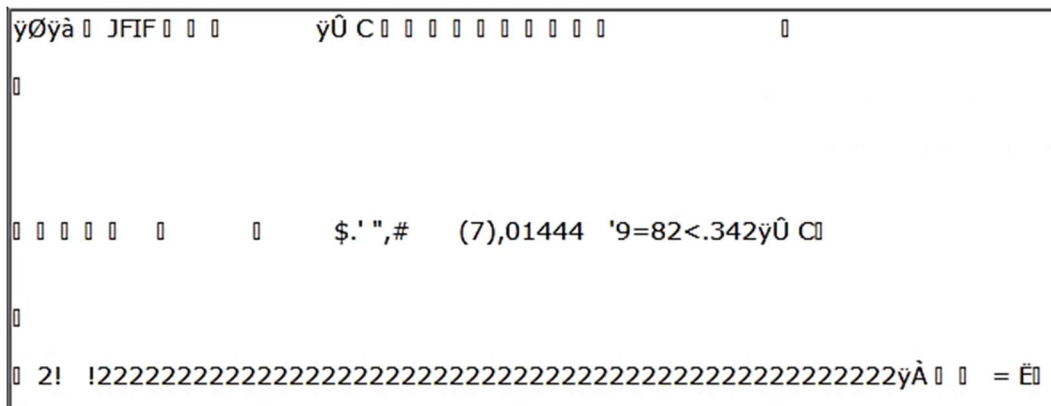


Fig 3.8: Screenshot of theTurtle.txt on ProDiscover Basic

Item #3:

Filename: theTermite.txt

Deleted: No

Simple text file that opened without any problems.

00000000	54 68 65 20 54 65 72 6D 69 74 65 0D 0A 62 79 20	The Termite by
00000010	4F 67 64 65 6E 20 4E 61 73 68 0D 0A 20 0D 0A 53	Ogden Nash S
00000020	6F 6D 65 20 70 72 69 6D 61 6C 20 74 65 72 6D 69	ome primal termi
00000030	74 65 20 6B 6E 6F 63 6B 65 64 20 6F 6E 20 77 6F	te knocked on wo
00000040	6F 64 0D 0A 41 6E 64 20 74 61 73 74 65 64 20 69	od And tasted i
00000050	74 2C 20 61 6E 64 20 66 6F 75 6E 64 20 69 74 20	t, and found it

Fig 3.9: Beginning hex figures of theTermite.txt

The Termite
by Ogden Nash

Some primal termite knocked on wood
And tasted it, and found it good!
And that is why your Cousin May
Fell through the parlor floor today.

Fig 3.10: Screenshot of theTermite.txt

Item #4:

Filename: thePurist.txt

Deleted: No

Another text file that opened without any problems.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	54	68	65	20	50	75	72	69	73	74	0D	0A	62	79	20	4F	The Purist by O
00000010	67	64	65	6E	20	4E	61	73	68	0D	0A	20	0D	0A	49	20	gden Nash I
00000020	67	69	76	65	20	79	6F	75	20	6E	6F	77	20	50	72	6F	give you now Pro
00000030	66	65	73	73	6F	72	20	54	77	69	73	74	2C	0D	0A	41	fessor Twist, A
00000040	20	63	6F	6E	73	63	69	65	6E	74	69	6F	75	73	20	73	conscientious s
00000050	63	69	65	6E	74	69	73	74	2C	0D	0A	54	72	75	73	74	scientist, Trust
00000060	65	65	73	20	65	78	63	6C	61	69	6D	65	64	2C	20	22	ees exclaimed, "
00000070	48	65	20	6E	65	76	65	72	20	62	75	6E	67	6C	65	73	He never bungles

Fig 3.11: Beginning hex figures of thePurist.txt

```

The Purist
by Ogden Nash

I give you now Professor Twist,
A conscientious scientist,
Trustees exclaimed, "He never bungles!"
And sent him off to distant jungles.
Camped on a tropic riverside,
One day he missed his loving bride.
She had, the guide informed him later,
Been eaten by an alligator.
Professor Twist could not but smile.
"You mean," he said, "a crocodile."
    
```

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.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	D0	CF	11	E0	A1	B1	1A	E1	00	00	00	00	00	00	00	00	Ðï à;± á
00000010	00	00	00	00	00	00	00	00	3E	00	03	00	FE	FF	09	00	> by
00000020	06	00	00	00	00	00	00	00	00	00	00	00	01	00	00	00	\ ^
00000030	5C	00	00	00	00	00	00	00	00	10	00	00	5E	00	00	00	byyy l
00000040	01	00	00	00	FE	FF	FF	FF	00	00	00	00	5B	00	00	00	YYYYYYYYYYYYYYYY
00000050	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	YYYYYYYYYYYYYYYY
00000060	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	YYYYYYYYYYYYYYYY
00000070	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	YYYYYYYYYYYYYYYY

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

The Pied Piper of Hamelin: A Child's Story
Robert Browning

Hamelin town's in Brunswick,
By famous Hanover city;
The River Weser, deep and wide,
Washes its wall on the southern side;
A pleasanter spot you never spied;
But, when begins my ditty,
Almost five hundred years ago,
To see townsfolk suffer so
From vermin, was a pity.

Rats!
They fought the dogs, and killed the cats,
And bit the babies in the cradles,
And ate the cheeses out of the vats,
And licked the soup from the cook's own ladles,
Split open the kegs of salted sprats,
Made nests inside men's Sunday hats,
And even spoiled the women's chats,
By drowning their speaking
With shrieking and squeaking
In fifty different sharps and flats.

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.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	EF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	01	00	82	ÿøÿà JFIF ,
00000010	00	82	00	00	FF	DB	00	43	00	08	06	06	07	06	05	08	, ÿÛ C
00000020	07	07	07	09	09	08	0A	0C	14	0D	0C	0B	0B	0C	19	12	
00000030	13	0F	14	1D	1A	1F	1E	1D	1A	1C	1C	20	24	2E	27	20	\$. '
00000040	22	2C	23	1C	1C	28	37	29	2C	30	31	34	34	34	1F	27	",# (7),01444 '
00000050	39	3D	38	32	3C	2E	33	34	32	FF	DB	00	43	01	09	09	9=82<.342ÿÛ C
00000060	09	0C	0B	0C	18	0D	0D	18	32	21	1C	21	32	32	32	32	2! !2222
00000070	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	2222222222222222

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: declarationOfIndependence.doc. There were no problems in unzipping the file and opening the document within.

```

00000000 50 4B 03 04 14 00 00 00 08 00 2D 9D 68 3E 6E 31 PK      - h>n1
00000010 4A 61 81 28 00 00 00 AC 00 00 1D 00 00 00 64 65 Ja (  - de
00000020 63 6C 61 72 61 74 69 6F 6E 4F 66 49 6E 64 65 70 clarationOfIndep
00000030 65 6E 64 65 6E 63 65 2E 64 6F 63 EC 5B 7D 8C 1D endence.doci[]E
00000040 D7 55 BF 6B 3B 8E 3F B2 76 52 67 13 27 29 64 08 xU;k;Ž?²vRg ')d
00000050 AE 43 DB C7 3A A5 69 12 6C 51 BA DE 64 BD DE F8 @CÛÇ:¥i lQ°Pd²Bø
00000060 63 B3 EB 62 02 25 E9 7D 6F EE 7B 6F 76 E7 E3 E5 c°ëb %é}óí{ovçãâ
00000070 CE CC 3E BF A8 A4 4A 15 04 02 41 01 81 48 FF 03 îÏ>ç¨=J A Hÿ
00000080 A9 08 8A D4 3F F8 68 11 08 09 2A 50 A2 BA 94 04 © ŠÔ?øh *Pç°"

```

Fig 3.19: Beginning hex figures of declarationOfIndependence.zip

IN CONGRESS, JULY 4, 1776

The unanimous Declaration of the thirteen united States of America

When in the Course of human events it becomes necessary for one people to dissolve the political bands which have connected them with another and to assume among the powers of the earth, the separate and equal station to which the Laws of Nature and of Nature's God entitle them, a decent respect to the opinions of mankind requires that they should declare the causes which impel them to the separation.

We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness.

- That to secure these rights, Governments are instituted among Men, deriving their just powers from the consent of the governed,
- That whenever any Form of Government becomes destructive of these ends, it is the Right of the People to alter or to abolish it, and to institute new Government, laying its foundation on such principles and organizing its powers in such form, as to them shall seem most likely to effect their Safety and Happiness. Prudence, indeed, will dictate that Governments long established should not be changed for light and transient causes; and accordingly all experience hath shewn that mankind are more disposed to suffer, while evils are sufferable than to right themselves by abolishing the forms to which they are accustomed. But when a long train of abuses and usurpations, pursuing invariably the same Object evinces a design to reduce them under absolute Despotism, it is their right, it is their duty, to throw off such Government, and to provide new Guards for their future security.

Fig 3.20: Screenshot of declarationOfIndependence.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.”

00000140	32 E4 05 00 07 8B F0 AC 3C 00 74 FC BB 07 00 B4	2ä <ð-< tü» ´
00000150	0E CD 10 EB F2 2B C9 E4 64 EB 00 24 02 E0 F8 24	Í èð+Éädé \$ àø\$
00000160	02 C3 49 6E 76 61 6C 69 64 20 70 61 72 74 69 74	ÃInvalid partit
00000170	69 6F 6E 20 74 61 62 6C 65 00 45 72 72 6F 72 20	ion table Error
00000180	6C 6F 61 64 69 6E 67 20 6F 70 65 72 61 74 69 6E	loading operatin
00000190	67 20 73 79 73 74 65 6D 00 4D 69 73 73 69 6E 67	g system Missing
000001A0	20 6F 70 65 72 61 74 69 6E 67 20 73 79 73 74 65	operating syste
000001B0	6D 00 00 00 00 62 7A 99 00 00 00 00 00 00 00 00	m bz™
000001C0	01 05 06 FE 3F 1E C5 39 01 00 9A 5F 06 00 00 00	p? Å9 š_

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”

00000170	C0 CC 02 0A CC B8 01 02 80 7E 02 0E 75 04 B4 42	Àì ì, €~ u ´B
00000180	8B F4 8A 56 24 CD 13 61 61 72 0B 40 75 01 42 03	<ôŠV\$Í aar @u B
00000190	5E 0B 49 75 06 F8 C3 41 BB 00 00 60 66 6A 00 EB	^ Iu øÃA» `fj ë
000001A0	B0 4E 54 4C 44 52 20 20 20 20 20 0D 0A 4E 54	°NTLDR NT
000001B0	4C 44 52 20 69 73 20 6D 69 73 73 69 6E 67 FF 0D	LDR is missingÿ
000001C0	0A 44 69 73 6B 20 65 72 72 6F 72 FF 0D 0A 50 72	Disk errorÿ Pr
000001D0	65 73 73 20 61 6E 79 20 6B 65 79 20 74 6F 20 72	ess any key to r
000001E0	65 73 74 61 72 74 0D 0A 00 00 00 00 00 00 00	estart
000001F0	00 00 00 00 00 00 00 00 00 00 00 AC BF CC 55 AA	-¿ìUª

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.

000008E0	54 68 65 20 6E 61 6D 65 73 20 61 72 65 20 41 6E	The names are An
000008F0	6E 20 61 6E 64 20 41 6E 6E 65 20 61 6E 64 20 41	n and Anne and A
00000900	68 6E 20 61 6E 64 20 41 6E 2E 0D 0A 49 20 77 6F	hn and An. I wo
00000910	6E 64 65 72 20 77 68 65 6E 20 74 68 65 20 64 69	nder when the di
00000920	66 66 65 72 65 6E 74 20 73 70 65 6C 6C 69 6E 67	fferent spelling
00000930	73 20 62 65 67 61 6E 2E 0D 0A 44 69 64 20 74 68	s began. Did th
00000940	65 79 20 61 6C 6C 20 62 65 6C 6F 6E 67 20 74 6F	ey all belong to
00000950	20 74 68 65 20 73 61 6D 65 20 63 6C 61 6E 3F 0D	the same clan?
00000960	0A 0D 0A 4F 72 20 6D 61 79 62 65 20 74 68 65 79	Or maybe they
00000970	20 61 6C 6C 20 63 61 6D 65 20 66 72 6F 6D 20 4A	all came from J
00000980	61 70 61 6E 3B 0D 0A 4F 72 20 50 61 6B 69 73 74	apan; Or Pakist
00000990	61 6E 20 6F 72 20 4B 61 7A 61 6B 73 74 61 6E 3B	an or Kazakstan;
000009A0	0D 0A 4F 72 20 6D 61 79 62 65 20 4D 65 78 69 63	Or maybe Mexic
000009B0	6F 27 73 20 59 75 63 61 74 61 6E 2E 0D 0A 4F 72	o's Yucatan. Or
000009C0	20 6D 61 79 62 65 20 74 68 65 79 20 66 6C 65 64	maybe they fled
000009D0	20 66 72 6F 6D 20 53 75 64 61 6E 2C 0D 0A 41 6E	from Sudan, An
000009E0	64 20 74 68 65 6E 20 77 65 6E 74 20 74 6F 20 43	d then went to C
000009F0	61 6E 6E 65 73 0D 0A 57 68 65 72 65 20 74 68 65	annes Where the
00000A00	20 63 6F 6C 6F 72 20 6F 66 20 74 68 65 20 73 65	color of the se
00000A10	61 20 69 73 20 63 79 61 6E 2E 0D 0A 0D 0A 53 6F	a is cyan. So
00000A20	6D 65 6F 6E 65 20 73 61 69 64 20 74 68 61 74 20	meone said that
00000A30	74 68 65 79 20 77 65 72 65 20 61 6C 6C 20 62 6F	they were all bo
00000A40	72 6E 20 69 6E 20 4A 61 6E 2E 0D 0A 4F 72 20 64	rn in Jan. Or d
00000A50	75 72 69 6E 67 20 73 6F 6D 65 20 6F 74 68 65 72	uring some other
00000A60	20 61 73 74 72 6F 6C 6F 67 69 63 61 6C 20 73 70	astrological sp
00000A70	61 6E 2E 0D 0A 4D 61 79 62 65 20 74 68 65 79 72	an. Maybe theyr
00000A80	27 65 20 61 6C 6C 20 53 61 67 69 74 74 61 72 69	'e all Sagittari
00000A90	61 6E 2E 0D 0A 0D 0A 43 61 6E 20 49 20 63 6F 70	an. Can I cop
00000AA0	65 20 77 69 74 68 20 74 68 65 73 65 20 6E 61 6D	e with these nam
00000AB0	65 73 3F 20 20 49 20 63 61 6E 21 20 20 49 20 63	es? I can! I c
00000AC0	61 6E 21 0D 0A 42 75 74 20 6F 6E 6C 79 20 77 68	an! But only wh
00000AD0	69 6C 65 20 49 20 6C 69 65 20 6F 6E 20 6D 79 20	ile I lie on my
00000AE0	64 69 76 61 6E 20 2D 0D 0A 57 68 69 63 68 20 69	divan - Which i
00000AF0	73 20 6D 61 64 65 20 6F 66 20 72 61 74 61 6E 2E	s made of ratan.

Fig 3.23: Screenshot of part of Volume slack