



The Power of Simple Hands-On Cyberforensics Exercises: A Guide for Faculty

12th Colloquium for Information Systems
Security Education

Dallas, TX
June 3, 2008

Gary C. Kessler & Jim Hoag
Champlain College
Burlington, Vermont, U.S.A.

Overview

- Introduction
- Pedagogy issues and hands-on exercises
- The role of hands-on exercises
 - » Detailed view of sample exercise
 - » Other exercises
- Conclusion

What Did I Learn From This?

- Lectures are well-suited to the transfer and exchange of information
- Hands-on tasks cement the concepts
 - » Students do not need an instructor or proctor hovering while they exercise hands-on skills
 - » Students need someone to go to for questions, problems, etc. but that resource does not need to be geographically or temporally local
 - In fact, students are not so quick to ask questions when the resource is *not* right there
 - » Students do not need to practice hands-on skills in a central facility
 - Not everything in computer forensics needs to be done on a FRED

Why Hands-On Exercises Are So Important

- **Active learning** is a critical component in technology education
 - » Constructivism
 - Cognitive structures are the building block of learning
 - » Resource-based learning
 - Engages students in active learning, enables their curiosity and investigative skills, and demands critical thinking
 - » Problem-based learning
 - Ill-defined problems allow students to synthesize information and build their own problem-solving skills

Program Philosophy

- We are trying to educate students about the digital investigations process rather than train them about any individual product
 - » They will build their own tool kits
 - They will determine which tools excel at which functions
 - » Education = life-long learning
 - Product training expires with new versions

© 2008, Gary C. Kessler/Jim Hoag

4

Burning Issue

- *Critique:* "You can't teach computer forensics online because you have to have students do hands-on exercises."
 - » *Corollary:* "You need to teach computer forensics in a laboratory environment."

© 2008, Gary C. Kessler/Jim Hoag

5

Our Response...

- *Yes* -- computer forensics education requires hands-on tasks
- *No* -- you don't need a lab; students can do the work on their own systems
 - » Not only is this possible, it probably enhances their (current and future) education
 - » Not limited to college's tools
 - » Not limited to lab hours

© 2008, Gary C. Kessler/Jim Hoag

6

The (abbreviated) Computer Forensics Process

1. Identification -- An incident occurred
2. Preservation -- Freeze the state of the scene
3. Collection -- Create the examination media
4. Examination -- Gather pertinent data
5. Analysis -- Interpret findings
6. Presentation -- Report the results

*Digital Forensics Research
Workshop, 2001*

© 2008, Gary C. Kessler/Jim Hoag

7

Hands-On Forensics Exercises

- Focus of exercises is on *process* rather than specific tools
 - » Homework exercises emphasize *examination, analysis, and presentation*
 - » Exercises employ many tools
 - Shareware, freeware, demo versions
 - EnCase, FTK, Helix, ProDiscover, WinHex, ...
 - » Evidence images come from a variety of sources
 - » Network-based analysis uses Internet tools

Sample Hands-On Exercise

Analysis of a Floppy Disk That
Contains Deleted Files

Project Outline

- Students start with a floppy disk image file
 - » There are reportedly three files on the floppy
- Examine floppy to find an address, an image, some passwords, some other data, and verify the MD5 hash of the distribution medium
- This project is based on a forensic challenge posted on the Internet, October 2002

DOS Floppies Use FAT12

- Sector 0 is the Boot Sector
 - » B/S points to FATs and Root Directory
- Primary and Secondary FATs follow Boot Sector
 - » FATs contain linked lists indicating clusters assigned to files
- Root Directory follows Secondary FAT
 - » Contains names of files (and directories), starting cluster, length, MAC times, etc.
 - » The starting cluster points to a cluster of data on the medium **and** an entry in the FATs
- Data Area follows Root Directory
 - » Data area always starts in *logical* cluster 2
 - » In FAT12 on a floppy, data area starts in *physical* cluster 33

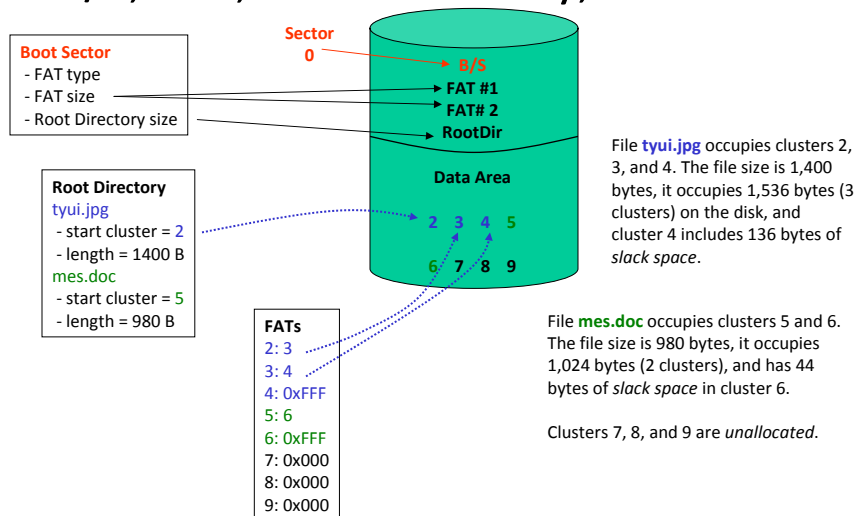
Capacity of this Medium

- FAT12 allocates 12 bits per FAT entry
 - » Limits addressing to 4,096 (2^{12}) clusters
- This floppy is configured so that:
 - » 1 cluster = 1 sector
 - » 1 sector = 512 B
- This FAT12 table is limited in capacity to 2,097,152 bytes (2 MB)
 - » The device itself is only 2880 sectors (1.44 MB)

© 2008, Gary C. Kessler/Jim Hoag

12

B/S, FAT, Root Directory, & Files



© 2008, Gary C. Kessler/Jim Hoag

13

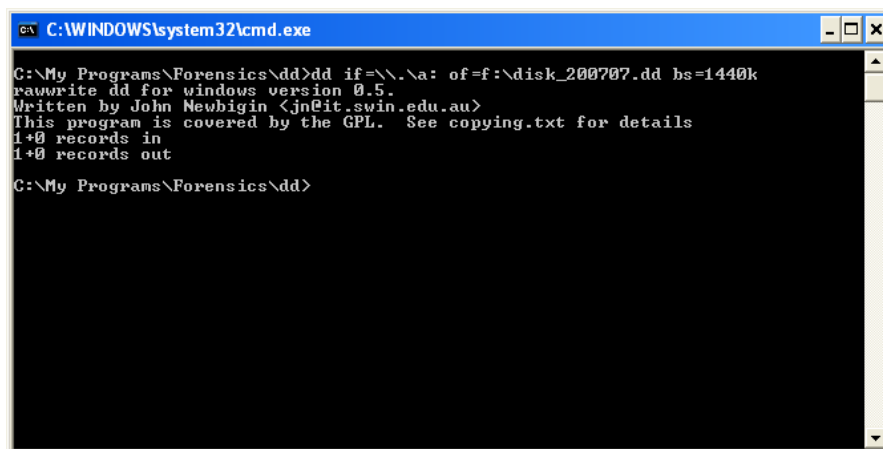
Forensic Process Redux

- It is **imperative** that the integrity of the original evidence medium be maintained
 1. Make a forensically correct image (copy) of the evidence medium
 2. Put the evidence medium in a safe place
 3. Do the analysis on the image *or* on a restored version of the original
 4. Verify that the examination copy is the same as the original evidence

© 2008, Gary C. Kessler/Jim Hoag

14

Imaging a Floppy With dd



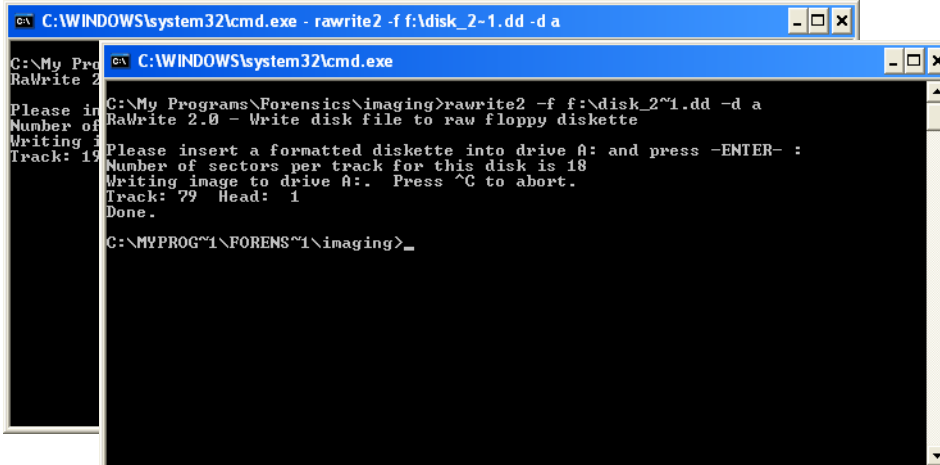
```
C:\WINDOWS\system32\cmd.exe
C:\My Programs\Forensics\dd>dd if=\\.\a: of=f:\disk_200707.dd bs=1440k
rawwrite dd for windows version 0.5.
Written by John Newbiggin <jn@it.swin.edu.au>
This program is covered by the GPL. See copying.txt for details
1+0 records in
1+0 records out
C:\My Programs\Forensics\dd>
```

This use of dd creates an image file called disk_200707.dd on the f: drive.

© 2008, Gary C. Kessler/Jim Hoag

15

Restoring the Floppy With rawrite

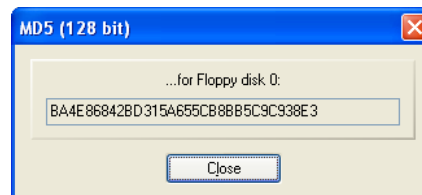


```
C:\WINDOWS\system32\cmd.exe - rawrite2 -f f:\disk_2-1.dd -d a

C:\WINDOWS\system32\cmd.exe
C:\My Programs\Forensics\imaging>rawrite2 -f f:\disk_2~1.dd -d a
RaWrite 2.0 - Write disk file to raw floppy diskette
Please insert a formatted diskette into drive A: and press -ENTER- :
Number of sectors per track for this disk is 18
Writing image to drive A:. Press ^C to abort.
Track: 79 Head: 1
Done.
C:\MYPROG~1\FORENS~1\imaging>
```

This use of rawrite2 writes the image file to a floppy. **NOTE** that rawrite2 requires use of short file names.

Verifying the Copy



WinHex calculated the same MD5 has for both the original evidence and examination media.

A DOS View of the Floppy

```
C:\WINDOWS\system32\cmd.exe
C:\MYPROG~1\FORENS~1\imaging>dir a:
Volume in drive A has no label.
Volume Serial Number is A4B6-0974

Directory of A:\

11/20/2002  01:20 PM                2,560 schedules.exe
             1 File(s)                2,560 bytes
             0 Dir(s)                1,455,104 bytes free

C:\MYPROG~1\FORENS~1\imaging>
```

Note that DOS sees only one file although we have been led to believe that there are three files on the floppy...

Let the Examination Begin...



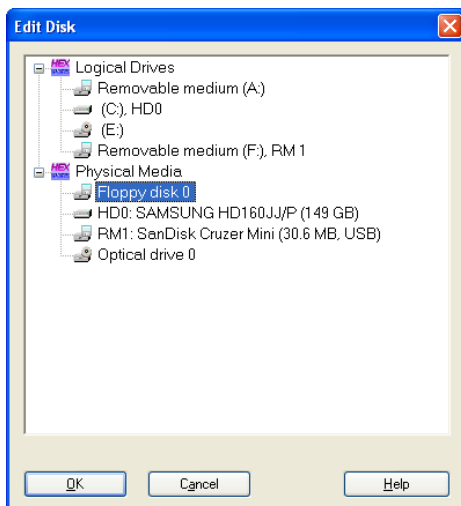
Examination/Analysis Software

- The examination of this floppy could employ any number of tools, including FTK, EnCase, or any hex editor
 - » FTK or Encase could work with the dd image
 - » Editor could be used with the examination floppy
- Examples that follow employ WinHex

© 2008, Gary C. Kessler/Jim Hoag

20

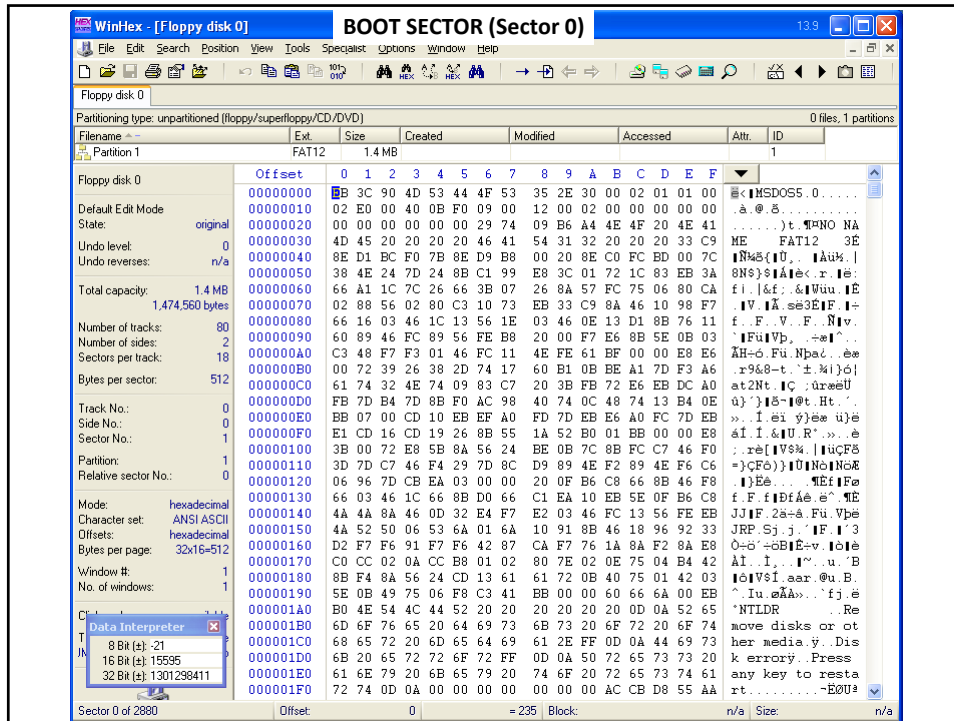
Physical vs. Logical



- Logical view
 - » Examiner sees what the file system sees
 - » I.e., we won't see deleted files, and slack and unallocated space
- Physical view
 - » Examiner sees everything on the medium
- We want the **physical** view!!

© 2008, Gary C. Kessler/Jim Hoag

21



Offset	Title	Value
0	JMP instruction	EB 3C 90
3	DEM	MSDOS5.0
BIOS Parameter Block		
B	Bytes per sector	512
D	Sectors per cluster	1
E	Reserved sectors	1
10	Number of FATs	2
11	Root entries	224
13	Sectors (under 32 MB)	2880
15	Media descriptor (hex)	F0
16	Sectors per FAT	9
18	Sectors per track	18
1A	Heads	2
1C	Hidden sectors	0
20	Sectors (over 32 MB)	0
24	BIOS drive (hex, HD=8x)	00
25	(Unused)	0
26	Ext. boot signature (29h)	29
27	Volume serial number (decimal)	2763393396
27	Volume serial number (hex)	74 09 B6 A4
2B	Volume label	NO NAME
36	File system	FAT12
1FE	Signature (55 AA)	55 AA

Boot Sector Template (WinHex)

© 2008, Gary C. Kessler/Jim Hoag

23

12

Sector Assignments

Sector(s)	Offset	Function
0	0x0000-0x01FF	Boot Sector
1-9	0x0200-0x13FF	File Allocation Table (primary)
10-18	0x1400-0x25FF	File Allocation Table (secondary)
19-32	0x2600-0x41FF	Root Directory
33-2879	0x4200- 0x167FFF	Data area (cluster 2)

NOTES:

- Boot Sector is 1 sector (0x200 bytes)
- There are two FATs, each 9 sectors (0x1200 bytes)
- The Root Directory can contain 224 entries, each 32 bytes (7168, or 0x1c00, bytes; 14 sectors)
- File storage starts at sector #33 (1+9+9+14), byte #0x4200 (0x200+0x1200+0x1200+0x1c00)

© 2008, Gary C. Kessler/Jim Hoag

24

Root Directory (1)

- The Root Directory starts at sector 19, byte offset 0x2600.
- Each entry is 32 B and contains the short (8.3) filename, attributes, MAC times, start cluster, and file size.
 - » Short file names (SFN) are preceded by the file's long filename (LFN), if appropriate.
 - » LFN entries have a sequence number in the first byte of the name and are stored in reverse order, 13 characters/entry
 - » SFNs use ASCII (8-bit) characters; LFNs use Unicode (16-bit)
 - » Example.... file named *ThisIsAReallyVeryLongName.html* would be stored in four entries:

html	(LFN entry, seq. 0x43)
VeryLongName.	(LFN entry, seq. 0x02)
ThisIsAReally	(LFN entry, seq. 0x01)
THISIS~1HTM	(SFN entry, 8.3 format)

© 2008, Gary C. Kessler/Jim Hoag

25

Root Directory (2)

- The first byte of the SFN entry is either the first character of the file name or a usage indicator:
 - » 0x00 - entry has never been used
 - » 0xE5 - file has been deleted
- The start cluster in the directory entry points to the first cluster of the data on the medium **and** acts as a pointer to the cluster linked list in the FAT.

© 2008, Gary C. Kessler/Jim Hoag

26

WinHex - [Floppy disk] ROOT DIRECTORY (Sector 19/Offset 0x2600)

Partitioning type: unpartitioned (floppy/superfloppy/CD/DVD) 0 files, 1 partitions

Filename	Ext.	Size	Created	Modified	Accessed	Attr.	ID
Partition 1		FAT12	1.4 MB				1

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Hex	ASCII
00002600	5	64	00	6F	00	63	00	00	00	FF	FF	0F	00	BC	FF	FF	5d	.o.c...
00002610	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	00	00	FF	FF	FF	FF	yy	.yy
00002620	E5	6A	00	69	00	6D	00	6D	00	79	00	0F	00	BC	20	00	aj	.i.a.m.y...
00002630	6A	00	75	00	6E	00	67	00	6C	00	00	00	65	00	2E	00	j	.u.n.g.l...
00002640	E5	49	4D	4D	59	4A	7E	31	44	4F	43	20	00	2F	40	BA	IMMYJ	~IDOC
00002650	EC	36	EC	36	00	00	0E	6C	74	2D	02	00	00	50	00	00	i6i6	...lt...
00002660	E5	63	00	6F	00	76	00	65	00	72	00	0F	00	F4	70	00	ac	.o.v.e.r...
00002670	61	00	67	00	65	00	2E	00	6A	00	00	00	70	00	67	00	a.g.e...	.j.p.g
00002680	E5	4F	56	45	52	50	7E	31	4A	50	47	20	00	BF	59	BA	OVERP	~IJPG
00002690	EC	36	EC	36	00	00	66	8A	6D	2D	2A	00	00	3E	00	00	i6i6	...flm*
000026A0	41	73	00	63	00	68	00	65	00	64	00	0F	00	55	75	00	As	.c.h.e.d.u.
000026B0	00	65	00	73	00	2E	00	00	65	00	00	00	78	00	65	00	l.e.s...	.e
000026C0	53	43	48	45	44	55	7E	31	45	58	45	20	00	80	75	BA	SCHEDU	~LEXE
000026D0	EC	36	EE	36	00	00	9A	6A	74	2D	49	00	00	0A	00	00	i6i6	... jt-I
000026E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000026F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

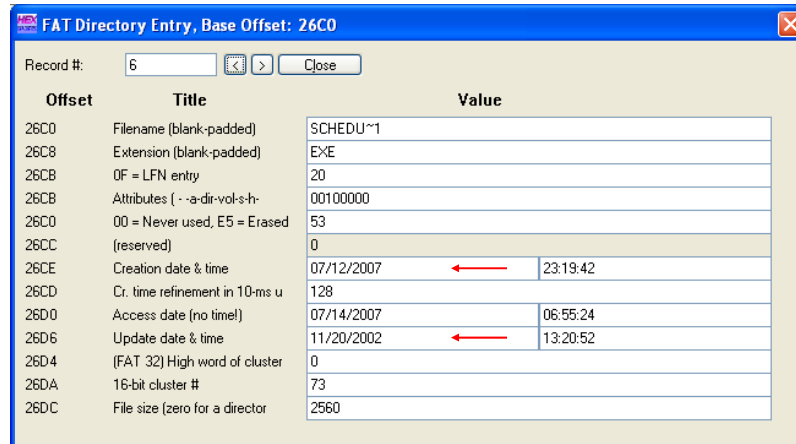
Mode: hexadecimal
Character set: ANSI ASCII
Offset: hexadecimal
Bytes per page: 32x16=512

Window #: 1
No. of windows: 1

Data Interpreter: 8 Bit [a]: -27, 16 Bit [a]: 25829, 32 Bit [a]: 1862296805

Sector 19 of 2880 Offset: 2600 = 229 Block: n/a Size: n/a

Root Directory Template (WinHex)



FAT Directory Entry, Base Offset: 26C0

Record #: 6

Offset	Title	Value
26C0	Filename (blank-padded)	SCHEDU~1
26C8	Extension (blank-padded)	EXE
26CB	OF = LFN entry	20
26CB	Attributes { - a-dir-vol-s-h	00100000
26C0	00 = Never used, E5 = Erased	53
26CC	(reserved)	0
26CE	Creation date & time	07/12/2007 23:19:42
26CD	Cr. time refinement in 10-ms u	128
26D0	Access date (no time!)	07/14/2007 06:55:24
26D6	Update date & time	11/20/2002 13:20:52
26D4	(FAT 32) High word of cluster	0
26DA	16-bit cluster #	73
26DC	File size (zero for a director	2560

© 2008, Gary C. Kessler/Jim Hoag

28

An Aside on MAC Times

- Modified (M) time is the actual time that the file was last written
- Access (A) time is the time that the file was last accessed
 - » This time is set by the application, not all of which do this accurately
 - » FAT file systems only maintains the **date** with A-time
- Creation (C) time is the time when the file was created *in this directory*

© 2008, Gary C. Kessler/Jim Hoag

29

What the Root Directory Tells Us

Short File Name	?IMMY~1.DOC	?OVERP~1.JPG	SCHEDU~1.EXE
Long File Name	Jimmy Jungle.doc	cover page.jpg	schedules.exe
Starting Cluster (logical)	0x0002 (2)	0x002A (42)	0x0049 (73)
Starting Cluster (physical)	0x0021 (33)	0x0049 (73)	0x0068 (104)
Byte Offset (physical)	0x4200	0x9200	0xD000
File Size (bytes)	20,480	15,072	2,560
File Size (clusters)	40	31	5
Offset Into FAT	0x004 (4)	0x03F (64)	0x06E (110)

Offset into FAT is $(\text{starting_cluster} * 3/2 + 1)$. This is where the link to the next cluster in the file is located.

The Actual Analysis

- We know that there are at least three files on the floppy. How do we get to them?
 - » ?IMMYJ~1.DOC
 - » ?OVERP~1.JPG
 - » SCHEDU~1.EXE

?IMMYJ~1.DOC

- The Root Directory tells us that the file starts at cluster 2 (i.e., sector 33, offset 0x4200)
 - » Scrolling down through the disk or image file would tell us the save thing
- Pertinent information:
 - » 0x4200: File header for MS Office document
 - » 0x4400: File subheader for Word file
 - » 0x905D: End of data
- Some text and a lot of metadata found!

© 2008, Gary C. Kessler/Jim Hoag

32

WinHex - [Floppy disk] ?IMMYJ~1.DOC (Sector 33/Offset 0x4200) 13.9

Partitioning type: unpartitioned (floppy/superfloppy/CD/DVD) 0 files, 1 partitions

Filename	Ext.	Size	Created	Modified	Accessed	Attr.	ID
Partition 1		FAT12	1.4 MB				1

Floppy disk 0

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00004200	D0	CF	11	E0	A1	B1	1A	E1	00	00	00	00	00	00	00	00
00004210	00	00	00	00	00	00	00	00	3E	00	03	00	FE	FF	09	00
00004220	06	00	00	00	00	00	00	00	00	00	00	00	01	00	00	00
00004230	23	00	00	00	00	00	00	00	00	10	00	00	25	00	00	00
00004240	01	00	00	00	FE	FF	FF	FF	00	00	00	00	22	00	00	00
00004250	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
00004260	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
00004270	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
00004280	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
00004290	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000042A0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000042B0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000042C0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000042D0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000042E0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000042F0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
00004300	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
00004310	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
00004320	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
00004330	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
00004340	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
00004350	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
00004360	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
00004370	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
00004380	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
00004390	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000043A0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000043B0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000043C0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000043D0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000043E0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
000043F0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF

Sector 33 of 2880 Offset: 4200 = 208 Block: n/a Size: n/a

WinHex - [Floppy disk 0] Sector 34/Offset 0x4400

File Edit Search Position View Tools Specialist Options Window Help

Floppy disk 0

Partitioning type: unpartitioned (floppy/superfloppy/CD/DVD) 0 files, 1 partitions

Filename	Ext.	Size	Created	Modified	Accessed	Attr.	ID
Partition 1	FAT12	1.4 MB					1

Floppy disk 0

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00004400	BC	A5	C1	00	35	40	09	04	00	00	F0	12	BF	00	00	00	5@ . . . 8 . 0 . .
00004410	00	00	00	10	00	00	00	00	00	06	00	00	9D	0B	00	00
00004420	0E	00	62	6A	62	6A	CF	32	CF	32	00	00	00	00	00	00	. . . bjbjI2I2
00004430	00	00	00	00	00	00	00	00	00	00	00	00	09	04	16	00
00004440	22	12	00	00	AD	58	00	00	AD	58	00	00	9D	03	00	00
00004450	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00004460	00	00	00	00	00	00	00	00	00	00	00	00	FF	FF	0F	00
00004470	00	00	00	00	00	00	00	00	FF	FF	0F	00	00	00	00	00
00004480	00	00	00	00	FF	FF	0F	00	00	00	00	00	00	00	00	00
00004490	00	00	00	00	00	00	00	00	88	00	00	00	00	00	32	01
000044A0	00	00	00	00	00	00	32	01	00	00	32	01	00	00	00	00
000044B0	00	00	32	01	00	00	00	00	00	32	01	00	00	00	00	00
000044C0	00	00	32	01	00	00	00	00	00	32	01	00	00	14	00	00
000044D0	00	00	00	00	00	00	00	00	00	46	01	00	00	00	00	00
000044E0	00	00	2A	03	00	00	00	00	00	2A	03	00	00	00	00	00
000044F0	00	00	2A	03	00	00	00	00	00	2A	03	00	00	0C	00	00
00004500	00	00	36	03	00	00	0C	00	00	46	01	00	00	00	00	00
00004510	00	00	70	07	00	00	B6	00	00	4E	03	00	00	00	00	00
00004520	00	00	4E	03	00	00	00	00	00	4E	03	00	00	00	00	00
00004530	00	00	4E	03	00	00	00	00	00	4E	03	00	00	00	00	00
00004540	00	00	4E	03	00	00	00	00	00	4E	03	00	00	00	00	00
00004550	00	00	4E	03	00	00	00	00	00	EF	06	00	00	02	00	00
00004560	00	00	F1	06	00	00	00	00	00	F1	06	00	00	00	00	00
00004570	00	00	F1	06	00	00	00	00	00	F1	06	00	00	00	00	00
00004580	00	00	F1	06	00	00	00	00	00	F1	06	00	00	24	00	00
00004590	00	00	26	08	00	00	52	02	00	78	0A	00	00	52	00	00
000045A0	00	00	15	07	00	00	15	00	00	00	00	00	00	00	00	00
000045B0	00	00	00	00	00	00	00	00	00	32	01	00	00	00	00	00
000045C0	00	00	11	06	00	00	00	00	00	00	00	00	00	00	00	00
000045D0	00	00	00	00	00	00	00	00	00	4E	03	00	00	00	00	00
000045E0	00	00	4E	03	00	00	00	00	00	11	06	00	00	00	00	00
000045F0	00	00	11	06	00	00	00	00	00	15	07	00	00	00	00	00

Mode: hexadecimal
Character set: ANSI ASCII
Offsets: hexadecimal
Bytes per page: 32x16=512

Window #1: 1
No. of windows: 1

Data Interpreter: 8 Bit [a]: 20, 16 Bit [a]: 23060, 32 Bit [a]: 12630924

Sector 34 of 2880 Offset: 4400 = 236 Block: n/a Size: n/a

WinHex - [Floppy disk 0] WinHex - [Floppy disk 0]

File Edit Search Position View Tools Specialist Options Window Help

Floppy disk 0

Partitioning type: unpartitioned (floppy/superfloppy/CD/DVD) 0 files, 1 partitions

Filename	Ext.	Size	Created	Modified	Accessed	Attr.	ID
Partition 1	FAT12	1.4 MB					1

Floppy disk 0

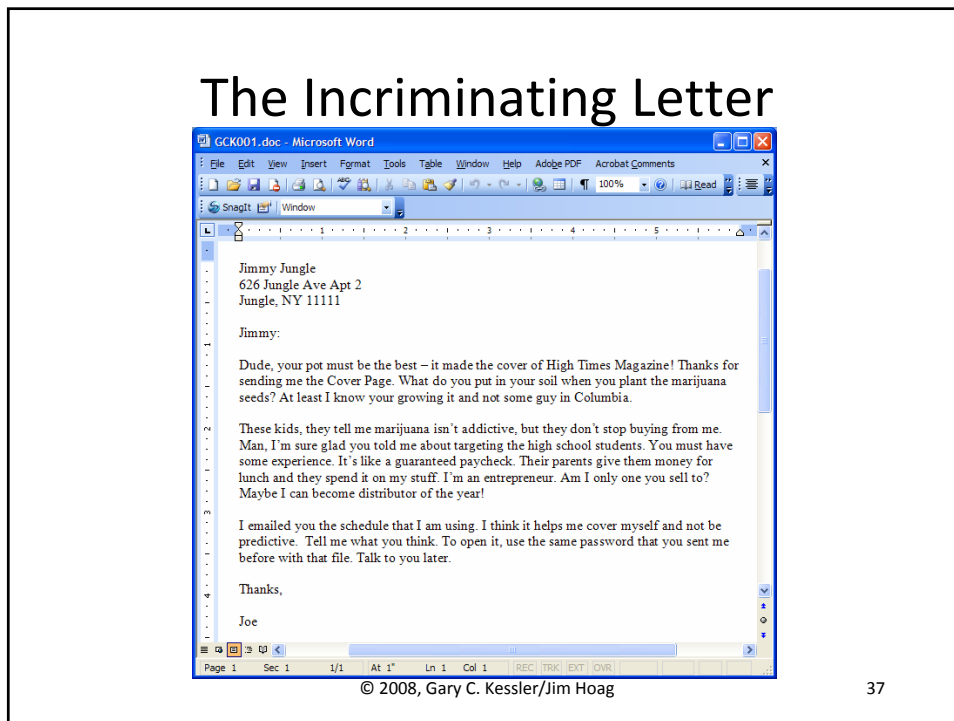
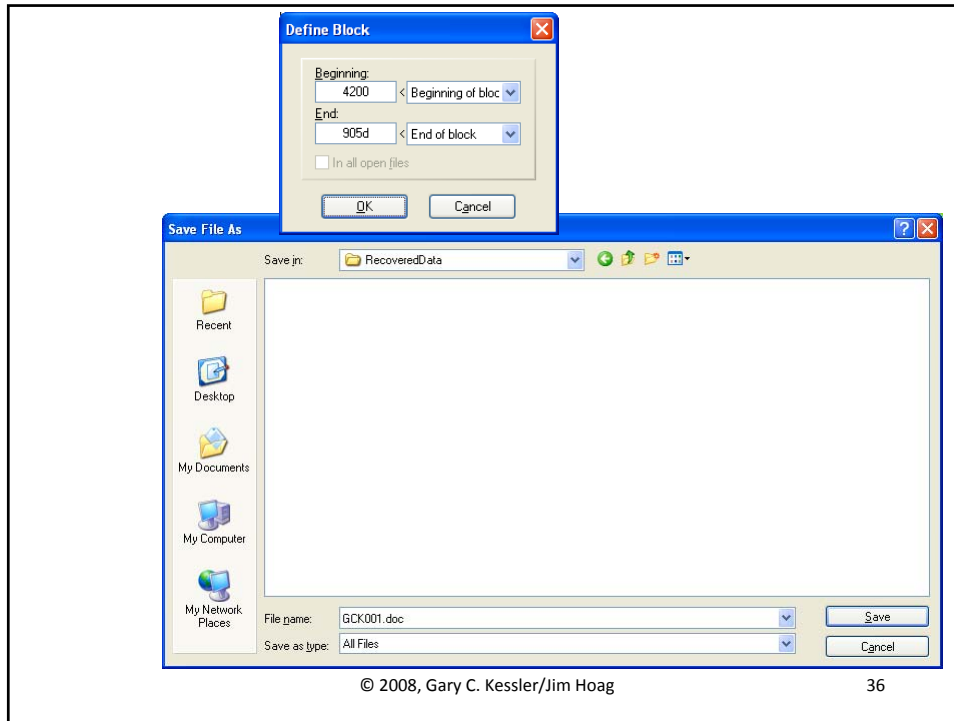
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00005800	14	00	0F	00	12	00	01	00	9C	00	0F	00	03	00	00	00
00005810	00	00	00	00	00	00	40	00	00	40	F1	FF	02	00	40	00
00005820	0C	00	00	00	00	00	00	00	00	00	06	00	4E	00	6F	00
00005830	72	00	6D	00	61	00	6C	00	00	02	00	00	00	18	00	00
00005840	43	4A	18	00	5F	48	01	04	61	4A	18	00	6D	48	09	04
00005850	73	48	09	04	74	48	09	04	00	00	00	00	00	00	00	00
00005860	00	00	00	00	00	00	00	00	00	00	44	00	41	40	F2	FF
00005870	A1	00	44	00	0C	01	00	00	00	00	00	00	00	00	16	00
00005880	44	00	65	00	66	00	61	00	75	00	6C	00	74	00	20	00
00005890	50	00	61	00	72	00	61	00	67	00	72	00	61	00	70	00
000058A0	68	00	20	00	46	00	6F	00	6E	00	74	00	00	00	00	00
000058B0	52	00	69	40	F3	FF	B3	00	52	00	0C	01	00	00	00	00
000058C0	00	00	00	00	0C	00	54	00	61	00	62	00	6C	00	65	00
000058D0	20	00	4E	00	6F	00	72	00	6D	00	61	00	6C	00	00	00
000058E0	1C	00	17	F6	03	00	34	00	D6	06	00	01	0A	03	6C	00
000058F0	34	D6	06	00	01	05	03	00	00	61	F6	03	00	00	02	00
00005900	0B	00	00	00	28	00	6B	40	F4	FF	C1	00	28	00	00	01
00005910	00	00	00	00	00	00	00	00	07	00	4E	00	6F	00	20	00
00005920	4C	00	69	00	73	00	74	00	00	00	02	00	00	00	00	00
00005930	00	00	00	00	00	00	9D	03	00	00	06	00	00	12	00	00
00005940	05	00	FF	FF	FF	FF	00	00	00	00	0D	00	00	22	00	00
00005950	00	00	33	00	00	00	34	00	00	00	3B	00	00	3C	00	00
00005960	00	00	2D	01	00	00	2F	01	00	00	B3	02	00	B4	02	00
00005970	00	00	8E	03	00	00	8F	03	00	00	97	03	00	98	03	00
00005980	00	00	9F	03	00	00	98	00	00	00	30	00	00	00	00	00
00005990	00	00	00	80	00	00	80	00	00	00	30	00	00	00	00	00
000059A0	00	00	98	00	00	00	30	00	00	00	00	00	00	00	00	00
000059B0	00	00	80	00	00	00	00	00	00	00	00	00	00	00	00	00
000059C0	00	00	00	30	00	00	00	00	00	00	80	00	00	00	00	00
000059D0	00	00	00	70	00	00	00	00	00	00	98	00	00	00	00	00
000059E0	00	00	00	00	00	00	80	00	00	00	80	00	00	00	00	00
000059F0	00	00	00	00	00	00	98	00	00	00	30	00	00	00	00	00

Mode: hexadecimal
Character set: ANSI ASCII
Offsets: hexadecimal
Bytes per page: 32x16=512

Window #1: 1
No. of windows: 1

Data Interpreter: 8 Bit [a]: 74, 16 Bit [a]: 26954, 32 Bit [a]: 18358863

Sector 38 of 2880 Offset: 5800 = 20 Block: n/a Size: n/a



?OVERP~1.JPG

- The Root Directory tells us that the file starts at cluster 42 (i.e., sector 73, offset 0x9200)
 - » Scrolling down through the disk or image file would tell us the save thing
- Pertinent information:
 - » 0x9200: File header for JPEG file
 - » 0xCEDF: Two-byte trailer for JPEG file
- Character strings found in file's slack space!!

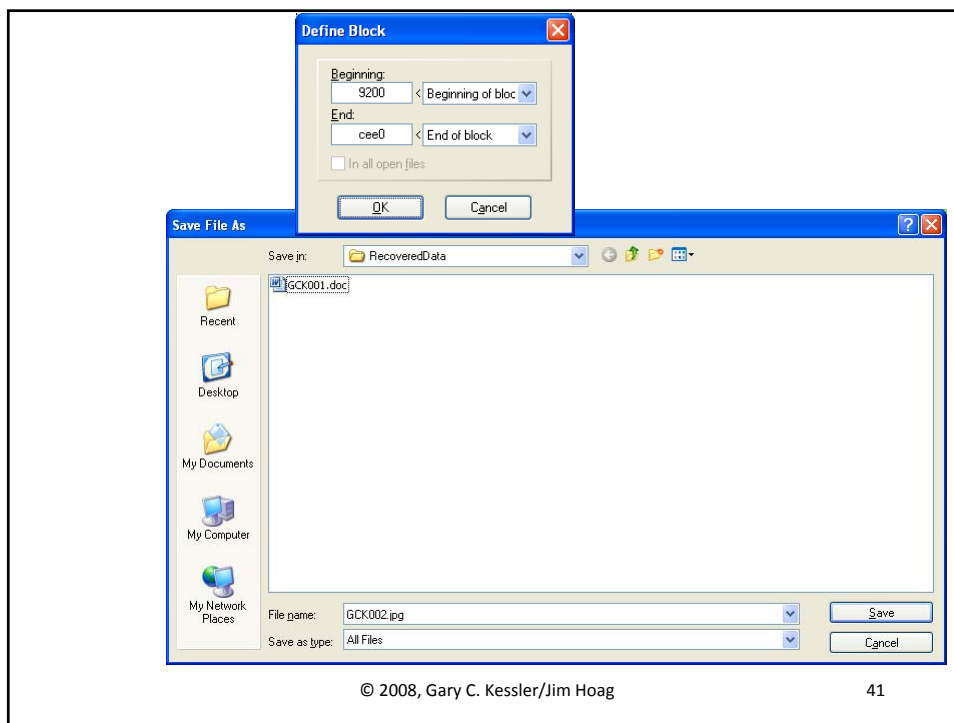
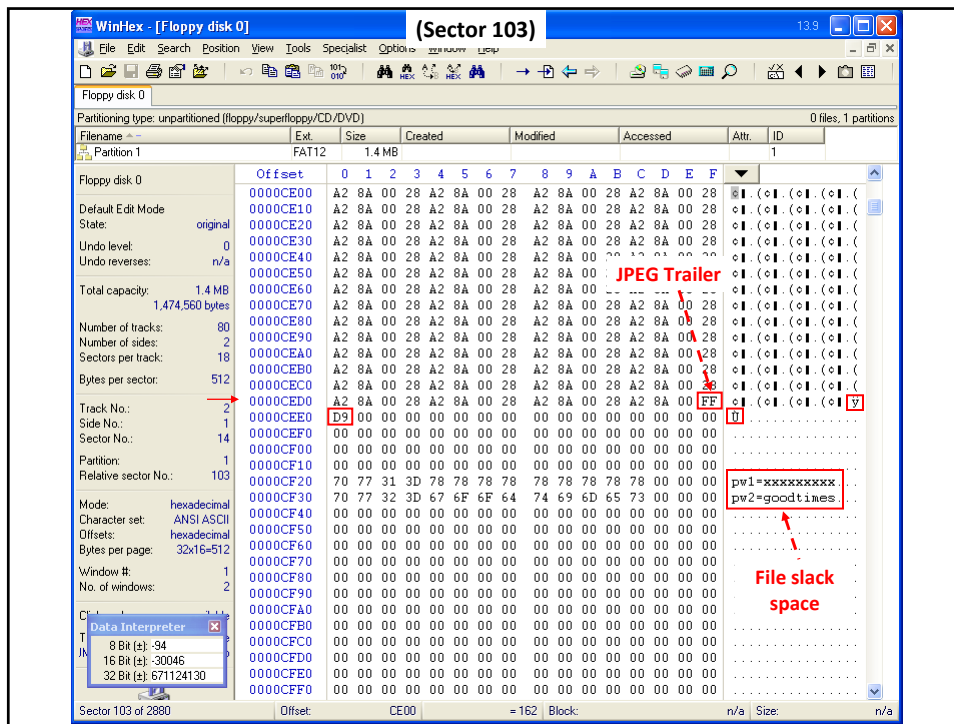
© 2008, Gary C. Kessler/Jim Hoag

38

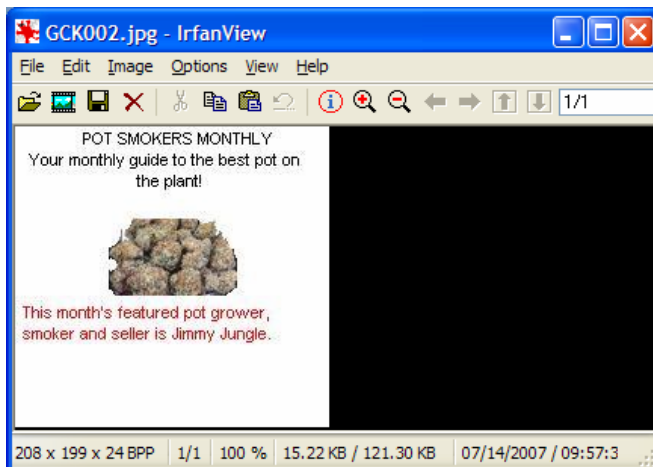
The screenshot shows the WinHex interface with the following details:

- Title Bar:** WinHex - [Floppy di] ?OVERP~1.JPG (Sector 73/Offset 0x9200)
- File Name:** ?OVERP~1.JPG
- Partition:** FAT12, 1.4 MB
- Offset:** 00009200
- Hex Dump (Sector 73):**

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00009200	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	01	00	60
- ASCII View:** 0va JFIF
- Data Interpreter:**
 - 8 Bit (±): -1
 - 16 Bit (±): -9985
 - 32 Bit (±): -520103681



The Incriminating Graphic



© 2008, Gary C. Kessler/Jim Hoag

42

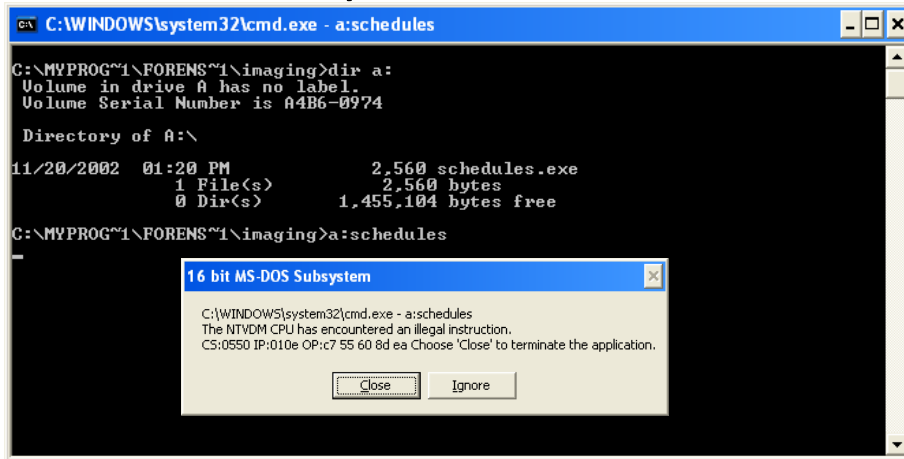
SCHEDU~1.EXE

- The Root Directory tells us that the file starts at cluster 73 (i.e., sector 104, offset 0xD000)
 - » Scrolling down through the disk or image file would tell us the same thing
- Pertinent information:
 - » 0xD000: File header for ZIP file (!!!)
- Why is there a .EXE extension?
 - » Because anyone can rename a file!

© 2008, Gary C. Kessler/Jim Hoag

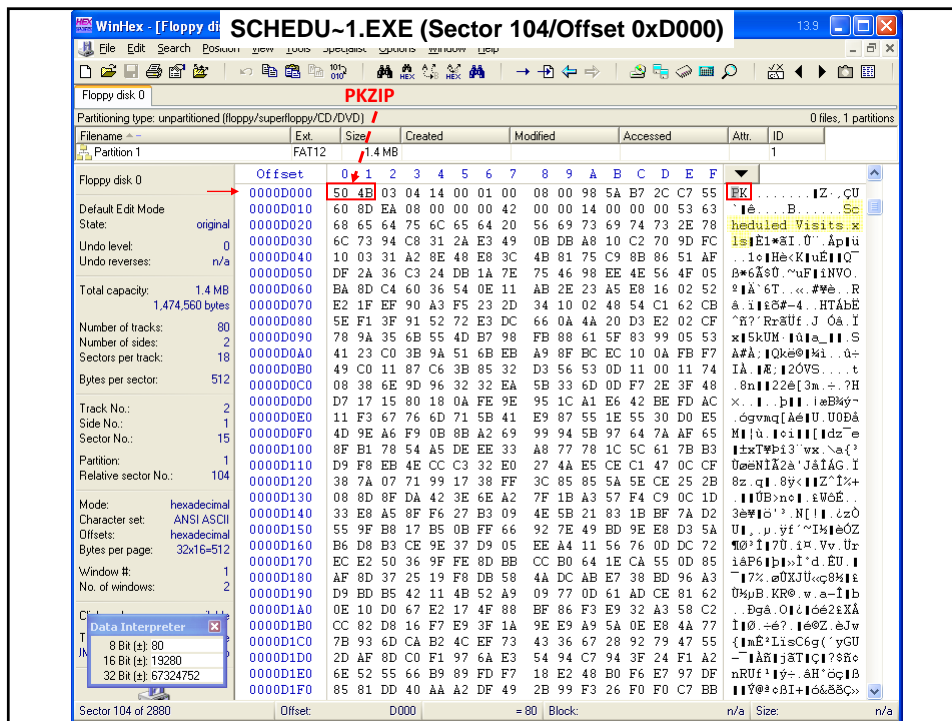
43

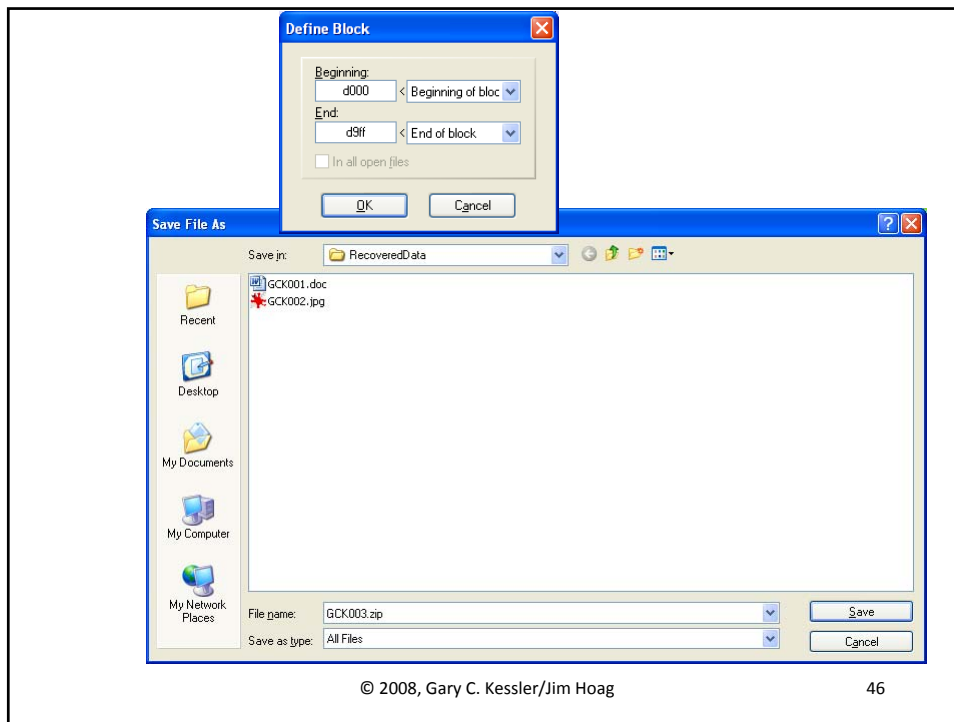
Definitely Not Executable...



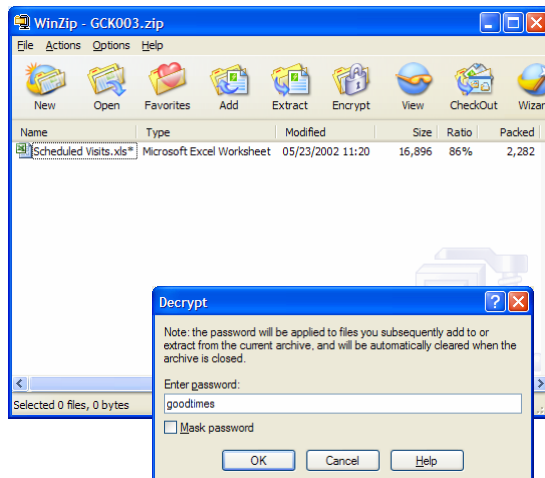
© 2008, Gary C. Kessler/Jim Hoag

44





Opening With WinZIP



Opening the file with WinZIP shows the name of the compressed file, "Scheduled visits.xls". The "*" indicates that the file is password protected.

The recovered letter alludes to a previously used password:

"I emailed you the schedule... To open it, use the same password that you sent me before with that file."

Recall our two character strings in the JPG file's slack space...

```
pw1=xxxxxxxxxxx
pw2=goodtimes
```

The Incriminating Spreadsheet

© 2008, Gary C. Kessler/Jim Hoag

48

Sector Assignments Finale

Sector(s)	Address	Function
0	0x0000-0x01FF	Boot Sector
1-9	0x0200-0x13FF	File Allocation Table (primary)
10-18	0x1400-0x25FF	File Allocation Table (secondary)
19-32	0x2600-0x41FF	Root Directory
33-72	0x4200-0x91FF	DATA: ?IMMYJ~1.DOC (deleted)
73-103	0x9200-0xCFFF	DATA: ?OVERP~1.JPG (deleted)
104-108	0xD000-0xD9FF	DATA: SCHEDU~1.EXE
109-2878	0xDA00-	
	0x167DFF	DATA: All bytes set to 0xF6
2879	0x167E00-	
	0x167FFF	DATA: All bytes set to 0x00

© 2008, Gary C. Kessler/Jim Hoag

49

Lessons Learned

- In-depth analysis of a floppy can be done manually... just barely
 - » File carving
- Analysis of a large hard drive requires automated tools

Project Files

- Digital Forensics Download Center
 - » <http://digitalforensics.champlain.edu/download/>
 - » dd
 - [dcfldd-1.3.4.x86win32.zip](#)
 - [dd-0.5.zip](#)
 - » rawrite: [rawrite2.zip](#)
 - » WinHex: [winhex.zip](#)
 - » Floppy disk image: [disk25.zip](#)
 - MD5: 391D4A30C29DA81D131DED2B1837B1A8
- http://www.garykessler.net/library/file_sigs.html

Other Hands-On Exercises

© 2008, Gary C. Kessler/Jim Hoag

52

Additional Hand-On Exercises

- Computer Forensics I
 - » Cell phone image analysis
 - » Web site and domain name information analysis
- Anti-Forensics and Network Forensics
 - » Photoshop and morphing images
 - » Cryptography/Steganography
 - » Packet sniffing
- Cybercrime
 - » Internet investigations
 - » E-mail, IRC, IM, and chat log analysis

© 2008, Gary C. Kessler/Jim Hoag

53

Hands-On Exercises Are Key

- Computer Forensics II
 - » Emphasis on reporting and building one's own tool kit
 - » Imaging and restoration exercises
 - Use of dd (and dcfldd), FTK Imager, and WinHex
 - Imaging CDs (multi-session) as well as "traditional" drives
 - » Analysis exercises using a variety of tools
 - Students build their own matrix of what software works best when doing what functions
 - » Live acquisition using Helix
 - Students image their own RAM to view contents

Conclusion

- Non-lab hands-on exercises can augment live classes and enable online classes
- Properly designed hands-on exercises -- with appropriate technology support -- can work as well as or better than in-lab exercises
 - » Most "hands-on" activities can be done as easily in a dorm room or at home as in a lab setting

Author Contact Information

Gary C. Kessler, Ed.S., CCE, CISSP

Associate Professor
Dir., Information Assurance Education & Research
Dir., Center for Digital Investigation
Champlain College
163 South Willard Street
Burlington, VT 05401

Adjunct Associate Professor
School of Computer and Information Science
Edith Cowan University
Joondalup, Western Australia

office: +1 802-865-6460
cell: +1 802-238-8913
fax: +1 802-865-6446
e-mail: gary.kessler@champlain.edu

<http://digitalforensics.champlain.edu>
<http://c3di.champlain.edu>
<http://www.garykessler.net>

Jim Hoag, M.S.

Assistant Professor
Prog. Dir., Computer Networking & Information Security
Champlain College
163 South Willard Street
Burlington, VT 05401

office: +1 802-865-6459
fax: +1 802-865-6446
e-mail: jhoag@champlain.edu

<http://cnis.champlain.edu>

This work was partially supported by Grant No. 2006-DD-BX-0282 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime. Points of view in this document are those of the author and do not represent the official position of the U.S. Department of Justice.

Acronyms and Abbreviations

ASCII	American Standard Code for Information Interchange
B	Byte
B/S	Boot sector
CD-ROM	Compact disc read-only memory
FAT	File allocation table
FRED	Forensic Recovery of Evidence Device
FTK	Forensic Toolkit (AccessData)
IM	Instant messaging
IRC	Internet Relay Chat
JPEG	Joint Photographic Experts Group
LFN	Long file name
MAC	Modified, access, and creation times
MB	Megabyte (millions of bytes, 2 ²⁰)
MD5	Message Digest 5
MS	Microsoft
RAM	Random access memory
SFN	Short file name