Criminal Investigations in an Automated Environment

Oct. 27-Nov. 6, 1997
Jefferson County Courthouse

Notes from Cmdr. Dave Pettinari

(This is the same course offered in Glynco, Ga.,
at the Federal Law Enforcement Training Center (FLETC).

DOS Programs
Darrell Lee, FLETC instructor

Reach him through Lisa Schaffer (912) 267-2604

Stored in RAM memory are DOS commands: dir, cd, md, rd, del. If it doesn't find these in RAM, it searches in the current directory, then in the "path." Hackers can change the name of these commands to reformat the hard disk. Lesson: Always boot from a safe, sterile DOS disk, not from the suspect's hard drive. Could run Norton Utilities Wipe-Info, which destroys hard drive and all information.

You want to use DOS for examining floppies and hard disks because you should not be executing programs on the suspect's hard drive that could change the suspect system.

List.com – shareware that helps you navigate and find things in DOS. Can look at all the directories and subdirectories, click on the file and read the contents.

In the DOS subdirectory, type HELP, gives help for a DOS commands. Notes, examples, and syntax for every command. As you process a hard drive, refer here often for fine shades of meaning and "switches" that will allow you to accomplish what you want to do.

With Doskey, up arrow brings up previous commands; down arrow commands that follow.

Dir /? – brings up all the commands to sort in this command, search other directors, displaying files in their compressed ratios, etc.

Dir /ah (finds hidden files)

Attrib command – r= read only, s=system file, h=hidden file. Executing this command will provide you with the attributes to see what has been made read only, hidden, etc.

To find all hidden files: **dir /s /ah** (search all subdirectories for hidden files)

Copy con test.dat – creates a file on your screen. Ctl Z to save what you have typed to a file.

To hide this file from DOS: attrib +h test.dat.

To find all files that begin with t: dir t*.* -- won't find test.dat

Go out to the root drive: cd \

Dir s/ /ah should find the test.dat file

Attrib –h c:\dos\test.dat – **Removes the hidden file attributes so you can see the file.**

Dir \dos\t*.* will find test.dat file that was unhidden.

To change this to a read-only file: attrib +r test.dat
This protects the file from being deleted. (del test.dat gives you "access denied")

Attrib –r turns off the read-only command so that you can copy the file or do something else with it.

Dir /s /ahd finds all hidden directories

To hide a directory, use the attrib command: attrib +h dos (hides the DOS directory); to unhide it, attrib –h dos

Crooks might have a directory called "cocaine," that you might not find unless you do this routine initially.

To see contents of files, if you don't have the list.com program:

Type test.dat

To check for files with list.com program:

C:\dos\List
W=wide
f-find
f bat – finds batch files

copy test.dat +f-i.dat merge.dat – copies both files to a merge file.

You can **sort contents of the file** with DOS's sort option.

Type merge.dat|sort (pipes data into a file in alphabetical order)
To send to printer: type merge.dat|sort >prn
To send to a file on a drive: type merge.dat|sort >a:

Sort <merge.dat will do the same thing.

Type merge.dat >prn copies a file to printer. For example, redirect a copy of all hidden files to the printer: dir /s /ah >prn.

You can date and time this printout: dir /s /ah >a:hidfiles.dat (labels with date and time)

Dir /p – info page by page
Dir /w – info wide across the screen
Redirect these to a printer or a file to keep a record of what the suspect had on his computer.

Tree |more – shows you all directories and subdirectories screen by screen.
Tree |more >prn sends it to a printer. Tree /A |more >prn looks better to some printers without good graphics capability.

Tree /f |more – shows all the files in the root, and each directory and subdirectory with all files, except hidden and system files. Tree /f |more >prn to print.

Dir /p .. – gives you a directory of the root directory.

To make a directory one level up: md ..\fake

Dir *.d* **Find all the data files.**

Attrib /? -- gives you help screen for attribute command.

Attrib *.dat – gives you the attributes of all the .dat files.

Cannot delete hidden files, but can print them or type them to the screen.

Dir /od – order by date
Dir /os – order by size
Dir /on – order by name (alphabetically)

Chkdsk c:

Tells you size of hard disk, **how many hidden files there are**, how many directories. Provides good summary of what's on the disk. Do at beginning of investigation. If hard disk looks too small, is rest of information hidden in a hard disk partition? 1.2-gig hard drive that is only a 540 meg hard drive, for example.

Be careful because chkdsk can be renamed to format the drive.

/v option under chkdsk shows displays everything on hard drive, including hidden files and directories. Send to a printout, as it scrolls too quickly on screen.

Chkdsk /v >prn.

Mem – memory command: mem/c|more tells what is loaded into standard and upper memory. Summary of memory, and how much is allocated to extended and expanded memory, and free memory.

If a file is too large to fit on one screen by using "type" command:
Type readme.txt|more or type more <readme.txt

Prompt can be changed so it doesn't appear as c:. If you run across anything cryptic, you can cancel it with prompt pg.

xcopy will copy things much more quickly from a directory, and copy the directory structure.
/s copies directories and subdirectories, unless empty
/e copies all dirs and subdirs, even the empty ones

deltree dirname – will delete that directory and all its subdirectories

If suspect formats a diskette with kiddie porn on it to erase the evidence, a newer version of DOS will allow you to unformat and recover this information, unless he did the /u unconditional format switch.

To give a volume label to a formatted disk -- label a:

To see label, vol a:

ver command – tells you what version of DOS the suspect's computer is doing. But don't boot with suspect's version of DOS until much later in the investigation.

diskcopy command – Copy all the dat files: copy \dos*.dat a: Diskcopy will copy over all the hidden files too.

/m option – Force multi-pass copy using memory only. If you don't use this option, it will run out of memory, altering the suspect's hard drive. MUST USE THIS OPTION.

Move command – moves the copy, but then deletes source files.

Some crooks can rename file extensions so that you will think they are something else:
.wpd WordPerfect
.xls – Excel
.ppt – PowerPoint
.doc – Word document
.dbf – database file
.exe might not be an executable file, but a document

Practical Exercise 2

To list all files on a disk, including files in subdirectories, not necessarily erased or hidden files:
Use list.com
Dir /s
Tree /f |more

If you want to see hidden files:
Chkdsk /v |more

To see if any files have been deleted:
Undelete command

To copy all files from one subdirectory to another, use the xcopy command. Xcopy /s \stuff*.* junk. The /s gives you all the files in all subdirectories and files in them. Xcopy is better than copy command in that it gives you the option to copy subdirectories. The destination directory does not have to be created before you execute the command, as xcopy gives you this option too. Neither copy nor xcopy can copy hidden files or erased files. But the diskcopy command allows you to copy hidden files and erased files (copies information sector by sector, track by track). (Older versions of xcopy allowed you to copy hidden files, but not MS-DOS ver. 6.22). Diskcopy must be used on the same drive, and with the same density disk.

Read only files:
Can't be deleted in DOS
Can be copied
Can see in a directory listing
If it's a program, you can run it.

If a file is hidden:
You can delete it.

You can copy it.
You cannot see it in a directory listing, unless you use the /ah switch.

- It is a program, you can run it.
- If it is a file, you can read it.

The command to display all hidden files on a:
Attrib *.* /s
Dir /ah a:

To rename a directory:

Move a:\subdir1 a:\subdir2

Allows you to give a more logical name to directories you find on a suspect's machine.

To get a printed list of all files and subdirectories on a diskette (not hidden files):
Dir /s >prn
Tree /f |more >prn

To get a printed list of all files and subdirectories on a diskette (including hidden files)
Dir /s /ah >prn
Chkdsk /v >prn

Viruses

Virus check at the search site if your warrant doesn't allow you to take the computer, and definitely do prior to analysis back at the shop.

(See handout in FLETC manual)

File Compression

Compress files to save disk space/storage. Can transmit more quickly by e-mail over the Internet.

PKZIP, PKUNZIP are the most commonly used programs. Shareware. Has .zip extension.

Zip2.exe – end up with one self-extracting file with .exe extension.

PKUNZIP separates one compressed .zip file into the number of files that were zipped into it in the first place.

Running PKZIP brings up a help screen. Go to option 2 for switches.

To run command:

PKZIP zipfile files (you want to compress)

PKZIP manual.zip manual.doc (file stored in current directory)

To put it in another directory:
PKZIP c:\stuff\manual.zip manual.doc

To view contents:
PKZIP manual.zio –v

means this file is password protected.

To compress all of the .doc files:

Pkzip docs *.docs

If want to see what's in that file to make sure you have enough space to explode it:

Pkzip docs.zip –v

Can't compress hidden files unless you use the appropriate switch.

Can use a switch to tell the computer to switch to another floppy after one is full. -&

To uncompress, view the file you want to decompress:
Pkunzip file.zip –v

To unzip into another directory:

Pkunzip manual.zip subdir (create subdirectory in advance)

To zip up stuff in a subdirectory, use –rp switch:
Pkzip –rp subdir This puts all those files into a single zip drive, subdir. To view this file, pkzip –v subdir

-s Put in a password.

Pkunzip –s allows you to unzip with a password.

Winzip

New, name the archive, browse to select files to archive. Ctl click on to do more than one. Go to add to select more files.

QuickView Plus!

Very intuitive. If you look at it through file manager or Windows Explorer, you can see the hidden files too.

Software to Use in Computer Crime Investigations

Available on Zip Disk or Hard Drive in these Directories

18 USC -- federal computer crimes statutes, compressed and hypertext
CShow – graphics viewer
DOJ – Guidelines for search and seizure
DOJ.IDX – Hypertext version
FCIC – Federal Computer Investigations Committee – good organization to belong to. Newsletter, web site (FCIC-USA.ORG)
List – Newer version of the program that lists files on a disk/hard drive
Mars.zip
Nscape.zip – Netscape ver. 3.0
PES – Practical exercises
PGP – Pretty Good Privacy with a Windows front end
PK – PKWare compression/uncompression utilities
Sample.syd – Safeback sampler
State.sts – Map of U.S. If you are working on a joint cases, click on that state for its computer crimes statutes.
SW – I.R.S. agent-proof program that documents equipment seizure. Good to use if you have lots of evidence to seize.
Thumbs – Thumbs Plus graphics viewer put out by Naval Criminal Investigative Service
Virus – virus scanners
WinZip 95 –
Zip.drv – zip drive drivers
Walt – Lead seizure person for Defense Investigative Services – his utilities.

Disk Analysis Boot-Up Process

Have to disable passwords if can't get into the computer. Discharge battery, find jumper to discharge battery (call computer company). CMOS, a volatile memory that requires battery power, it will forget what it used to know, such as a password. Will also forget what hard drive you have and what floppy drives are installed.

To get into CMOS, Ctl Alt Del, hold del key down. Record all the info you find in he CMOS. Use what is called a POST card; plugs into the computer, a smaller computer that records data from the hard drive.

Another way if you can't get password from the suspect is to take the hard drive out and run it in another machine to search. Or write a Rule 41.1 and have a judge order them to reveal the password.

Boot disk
Format /s to put system files on it
Command.com
Tree
Chkdsk
Undelete
MSD
Attrib
More
Find
Edit
Qbasic (edit won't run without)
DM-COM (Directory Magic; don't need attrib command, and many others)
List.com

Automate disk by creating batch files ,and an autoexec.bat since you are booting up with this disk.
Edit a:autoexec.bat
F-prot /hard
PAUSE
Dir /s /ah c: >prn (or save to file on disk if you don't have >hidfiles.c) (put separate lines for e drive, f drive, etc.)
Tree /f |more
chkdsk to send to printer, etc.

REM command for reminders to you.

Config.sys file

DEVICE=DOS\SETVER.EXE --- JOIN, STORE, and other older DOS versions can run on updated software. Include this command if suspect's computer has a program, such as older version of Lotus, that runs on previous DOS version.

DEVICE=DOS\HIMEM.SYS Gives computer access to higher memory.

DEVICE=DOS\EMM386.EXE NOEMS Let's you get into extended memory.

DOS=HIGH,UMB Loads DOS into upper memory and upper memory blocks.

DEVICEHIGH=DOS\ANSI.SYS Puts colors into DOS screen and certain prompts. Keyboard driver.

SHELL=C:\DOS\COMMAND.COM C:\DOS\ /P /E:512 Sets up environment and tells the computer where to look for command.com.

FILES=64 Need up to 50 files open for some Windows programs.

STACKS=9,256

LASTDRIVE=Z If more than 5 devices, a-e, can't see zip drive or another hard drive, unless set up. Lastdrive will give you 26 drives you can access. If you can't access a drive, make sure this statement is in there.

devicehigh command allows you to load devices into upper memory, like old WordPerfect, etc., which carve into DOS's required 640K.

deskcan\mini4001.sys – driver for a scanner

sb16 – SoundBlaster driver

mscd0001-Miscrosoft CD compact disk driver of some kind

DOS Disk Structures

and Recovery of Erased Data

Can tell the difference between a high-density (1.4 meg) disk and a low-density (730 meg) disk by the lack of a notch opposite the write-protect notch. Or run chkdsk on it to see total disk space.

If you are changing from DD to HD, or HD to DD…
Or
Id adding /s
Or
If disk is almost full… (no room to store unformatting information – boot record, FAT, directory)
"Cannot format, continue? Y N

format /u treats the disk as if it is being formatted for the first time.

Unerase – Shows prognosis for recovery. Get information on the erased file. Next to get information on the next file. View shows you what's in the file. You can read it. Alt F to go to UnErase to, send to a file. Search for text. File directory, View All Directories, shows you all deleted files on the hard disk. Select Group, highlights all the files. To recover a subdirectory, first recover the subdirectory itself, then the files inside of it.

Disk Editor program – recovers deleted files. Diskedit to activate. Object menu, pick a drive, directory, file, cluster, sector, partition table, etc. Change to drive, replace hex character with letter to recover any document. Then note clusters file was occupying, then go to Object menu, FAT. "Changes made to Sector 19". Write. Cluster at bottom right. Clusters linked together to form files are in red against blue background. Page down, where red ends and white begins is unallocated space. Beginning of new red block is a new file. See a couple of zeroes interspersed among other white numbers, where data was erased. To link these clusters together, go back to first zero and type in the cluster number at bottom, e.g. 1,989, and EOF where the end of the file should be. Now save your changes. Alt E for edit, write changes. Synchronize FATS (update both copies). Rescan to reflect that changes were made.

Alt View as FAT to go back to the FAT table.

If Unerase cannot find, use Disk Editor to view the files, go to Object FAT, and look for zeroes (unallocated between allocated data). This might be remnants of the file partially overwritten. Find out what clusters those are. Look at lower right to determine which clusters these are. Go to Object menu and tell it to bring up data by cluster. Pick Cluster. Fill in starting and ending clusters. Actually brings up the file so you can read it.

To save portions of that file, Object menu, Sector, type in the sector numbers to save (73-79). Alt T for Tools, Write object to… (file). Enter file name. NEVER write to SECTOR 0 on the hard drive, which messes up your computer boot record.

If you don't get the entire file, you might have to run Disk Edit on that file and remove the single control character that tells DOS to stop displaying the file. Go to hex view, overwrite that code with a letter, and save. Or use the edit program to see the entire document. The control character will not stop it from displaying.

Use erased information as investigative leads.

Do NOT use as evidence in court, because it becomes very sticky to explain it. Not very successful.

To explain to a jury: "It's like writing on a page, erasing part of it, and writing over the erasures."

If you wanted to hide a password on a disk, you could go into the FAT, and write "BAD" over several clusters, and put that information here. Disk will never write over this information, and an investigator might miss it, thinking BAD means they are damaged clusters.

Slack

Area between the end of the file and the end of the buffer (RAM saves bits of file and other stuff in the buffer). Slack is everything in that file that doesn't belong to that file. It is the stuff between the end of the file and the end of that cluster. Might contain erased information. On high density disks, the ONLY slack that exists comes from RAM. RAM can only write 512K to the buffer.

If you do a simple copy or xcopy, you don't get the slack area. But if you image a file (diskcopy or Safeback program) you get the slack.

A manual way to look at the data in slack is to use Disk Editor, go into the FAT, make a list of the clusters that have EOF, and look in them. You can print it, document where it is in your notes, or save to a file on another disk. Tell computer to save the clusters you wish to refer to, or save it in context of what you found in the EOF file.

Orphan cluster – has information in them, but marked as 0. Slack erased file is in EOF.

Seejunk is a shareware program that you can use to get at slack. A special form of Unerase can get you orphan clusters. Seejunk shows, in standard DOS debug dump format, the data actually present after the end of the file. Doesn't change the file, but opens it for reading and writing. Seejunk has a web site for more info.

Seejunk /s a:*.* |more (or redirect to a file – seejunk /a a:*.* >report; use Edit program to read this report, use find or search commands) Printable characters in ASCII appear in the right-hand column, so you can read what is in slack. Sometimes trying to print this output crashes, because there are control characters. Don't print the entire thing, just the portion you need. (Computer ASCII codes are on Page 10 of your blue book, Pocket PCRef.).

To make a directory on your hard drive where the directory name is not visible – md alt 255 (or any other number on the numeric keypad). It appears as a directory, but directory name is not visible. Can't get in through DOS, but can see it with QuickView. Can still get into it with Windows Explorer. Network administrators use this to hide directories so others don't get into it.

Set temp filename in autoexec.bat file (subdirectory where you can put information created by using the |more command).

Unerase features –

Use Unerase in a standard mode to bring back anything you can't see. Then use these search features. Might make more than one original copy of your diskette to use different procedures.

- File, View All Directories **(shows all unerased files**).

- Search for Lost Names (**look for hidden and erased files without recovering subdirectories first**)
- Locate orphan clusters that don't have a file (clusters they are chained to are overwritten):Search or Date Types (click or space bar on Other Data in the box). Looks for contiguous 0's in the FAT. Does not find any slack (clusters marked as EOF). Will even find one 0 if it has data in it. VIEW to see the information. Gives you .doc., .txt, .dbf extensions to indicate to you the type of file it has found. Look at them, unerase them, use Disk Edit to process and look at what clusters it is in.

To write a secret message in a FAT cluster: Diskedit, Alt O, 1st FAT, go to a 0 sector and type B for bad, Alt E, write changes. You can then write information into that "bad" cluster. Alt O, cluster, cluster number. To put a message in there, tab to right hand side where division symbols are. Save it. You can also Edit, Mark, Copy, copy to Windows clipboard, and paste it elsewhere. You could also copy a file into this FAT area from a Windows word processing program. To find, hit F7 FF in Disk Edit, or run chkdsk to see if there are any BAD files, then go to the FAT to look at them.

Disk Edit and Unerase are both on the Norton Utilities floppies you were given with Norton Utilities for Windows 95. Make sure these get into your "on-scene" kit.

To find out if a file is fragmented, run Disk Edit, go to Information, Object Information. To get to corresponding FAT, choose LINK, Cluster Chain FAT. Everything in red refers to the file and you will see the filename in lower right. Last number in this sequence is a pointer that points to the cluster where the file resumes. To go back, Link, File. View, Text. Scroll down to the end of where the pointer cluster is.

Fragmented Erased Files

To put a file back to about where it was before it was erased (a fragmented file will not all be there) – Use manual unerase. Highlight the file, File, **Manual Unerase**. Put in a letter to replace ?. Shows how many clusters needed due to file size. Add Cluster. Browse for clusters to add. Add. Next (if it looks like it goes with the previous cluster, Add). Escape to view list of clusters added to make sure you haven't skipped a cluster (remove, move cluster on menu). F to view the file again. Add all clusters if it looks as if the rest of the information belongs with the file. Save, and it recovers all of the file linked together.

Investigating Computer Crime on Networks

Rob Kipp, rkipp@arms.com – e-mail him if you need help.

Network: A file server controls all the other computers. WAN – Wide Area Network. Networks allow us to set access rights, security, etc. for many different users.

You can tell you are on a network simply by opening up File Manager or Windows Explorer; you will see a bunch of drives at the top or on a tree. Or you will find a network interface card in the CPU. Drivers for this card will be in your autoexec.bat file. For example, files start with NW, NWClient, NWServer, or end in .vlm extension.

You can seize a server and a workstation with a warrant and take it back to your shop to examine, or examine on sight with in-house assistance.

System administrator is your key person to help you in the investigation. After interviewing the suspect, draft some questions to ask the systems administrator, unless this person could possibly be the suspect, or another suspect. This person has superuser (supervisory) access. Control passwords, can read your e-mail, can see everything in a system, do everything on a system. Can help you examine the person's access rights, then run an audit trail to see if this person has been doing other things not within his or her access rights. If

he is a suspect, use the backup systems administrator.

If suspect won't give you a password, the systems administrator can cancel it and bypass it with another password.

Novell command examples

Map -- Command "map" tells you what different file servers are on line, and what different computer systems the computer is looking at. Will show you the "path" for the network.

Purge – Deleted files remain on a server. Purge command erases them off the disk forever. Someone can control a file server from a remote location. **Rconsole** – remote console. During a raid, it is easy and quick for someone in a back room to send a quick e-mail to a hacker friend in NewYork, who can then access the server and issue the purge command to delete everything. If the suspect is using rconsole, sysadmin can terminate his session, but he's alerted you are onto him.

Ask systems administrator to load Rconsole for you as the investigator.

Monitor – Load monitor. Connection information – brings up those currently using the file server. Is suspect online now? What is he doing now? What files is he looking at?

Salvaged -- Equals DOS undelete command.

whoami – Gives you the user ID; identifies the user. Could be logged in as another person.

Software on a LAN can look at hard drives of computers on the LAN. Can also "broadcast" software to all machines simultaneously. Not very commonly used yet, but is available; very expensive.

userlist /a – Lists all users online.

rights – What rights does that user have in the system?

Investigative Techniques at Search Sites

Chuck Davis, CBI

- Get intel beforehand
- "Photograph the hell" out of the scene and the computer, as if it were a homicide
- Shut down network – down command. In NT, file down.

It not what technique you use, but WHY you do it, and how you document it. One agency's checklist may not be anything like that of another.

Protocol checklist

Documentation (Use forms)

- "Reasonable expectation of privacy?" (Signed employee statement, disclaimer on screen at login "all files subject to security audits at any time" Signs displayed? Search warrant.
- Options for seizure:

1. Seize computer and return to office for detailed analysis. Used most often with home computers and standalone office computers. Enables us to carefully analyze the slack and orphan sectors, and look for erased files. Orphan clusters are those clusters on a disk that contain data but are not assigned to any file.
2. Seize computer, but leave copies of files with suspect. Officer should make copies, not the suspect.
3. Seize copies of the files, but leave originals. Used most often in multi-user environments such as mainframes. Search the computer for likely files, then copy to your medium and leave.

- Secure the system; make sure no one has access. Terminate users, lock them out.
- Header info: Case number, exhibit number, analyst, date
- System hardware description, SN,CPU type, system actual date and time, modem, sound, CD; visible devices (3.5 drive, 5.25 drive, tape, other), monitor, keyboard, mouse, printer. Internal parts inventory: fixed drives, slots (manufacturer, model, serial #)
- Hard drive architecture: manufacturer, model number, serial number, capacity
- Computer running at time of entry?
- Computer connected to network (disconnect)
- Phone line connected to computer? (modem disconnected)
- Photograph screen or note content
- Photograph connections; videotape scene
- Place blank diskettes in all drives and Safepark hard drive

1. Wear latex gloves at every scene to protect yourself. If fingerprint is absolutely necessary, do electronic exam first, then dust or fume hood. Data is more important. You can always tie the floppy to the suspect in other ways – Only one with access to computer, etc.
2. Document all components and peripherals (see above)
3. Mirror image and restore data to a second drive in your machine, or in a separate hard drive in an analysis machine that is separate from your system. It is usually not desirable to pull the hard disk from the seized computer and install it in another computer for analytical purposes. Most hard disks have a very dependent relationship on the drive controller and BIOS of the original machine and that relationship may be shattered when the disk is installed in a separate system.
4. Put in second drive. Main drive has mirroring program, Write Block, and other analysis utilities. Or use Mares' shareware HDSENTRY, which write-blocks the disk.
5. Boot system with Don Mares utilities and apply write block protection (HDSENTRY); run programs.

6. Run for viruses (do not disinfect original; Don't write to the hard drive unless you have to). Write Block is the one program you MUST own. Last line of defense; I know I didn't mess up the hard drive because I had a program preventing it.
7. Execute CRC – "What you had then is what you got now." The two match. CRCs are also memory joggers that the mirror backup was halfway decent.
8. Chkdsk and fdisk to take a quick look at the seized hard drive and its partitions. Run chkdsk for x-linked files. Is the hard drive on its last legs. Do text searches on .chk files.
9. DOS mem (memory) utility to give you a quick memory map of the seized system.
10. Ver command to learn version of DOS installed.
11. List of files, directory structure, files erased, files hidden.
12. Snapback restore of mirror image; Mares, Safeback.
13. Zip drives are cost effective. $150, Safeback, $250. Cartridges are $15 apiece. 20 cartridges for a 2 gig hard drive. $3,000 in zip disks for 10 cases.
14. Jazz drive $350, cartridges $90 apiece. Software $300. Two disks for a 2 gig hard drive.
15. Tape – Cheap but slow. Four hours to do a mirror image. $1,500 for the drive and Snapback; tapes are $7 apiece. $70 for 10 cases.
16. Boot system and write block
17. Execute CRC against restored image, and make it matches files in the other image.
18. Detailed file analysis (use original media access worksheet – Use Norton Commander to view the computer's hard drive (drives, size, free space, compressed, config.sys, autoexec.bat, MS-DOS.SYS, and other observations). Determine operating system DOS, NT, Win3.1, Win95, etc. Image copy with Safeback. Create rescue disk in case CMOS or other vital areas are corrupted.
19. Create CD-ROM
20. Complete systems analysis and hard disk analysis – Go from the most obvious to the least obvious. Automate, if at all possible. Use Norton's Text Search (ts.exe) to search all files for text strings. Can only search for one string at a time. Or search for text in Unerase. Strsrch (string search) in Mares software. Andy Fried utilities: hdsentry write protects hard drive; dospart tells you if partitions are there; hidden tells you if any hidden files; FDSR searches entire hard disk for key words; PC2UNIX and UNIX2PC translates Unix files to MSDOS and back. Dumpdisk dumps an entire disk to printer, making it easier for an investigative team to examine.
21. Examine autoexec.bat and config.sys files. Tells what applications the person uses most often. Gets into their head. What software can we expect to find. If PGP in path, be scared. If Norton Utilities, be concerned.
22. Examine partitions (Norton DiskEdit)
23. Examine disk for hidden files (Norton DiskEdit). Renamed files (Really a .doc file, but labeled an .xls file, or .dbf file). Check both copies of the FAT to ensure no illicitly stored data exists. Look for weirdly named files.
24. Check "BAD" sectors to ensure nothing is intentionally tucked inside.
25. Examine disk for and recover erased files (Norton Unerase)
26. Examine active files (QuickView). Thumbs Plus for .JPEG and .GIF files for pornography files. Norton Navigator. DiskSearch to search for word strings, or Mares STRSRCH.
27. Review slack space, which is the data between the end of the file marker and the end of the cluster. Examine slack areas with Seejunk. Many prosecutors won't take anything but active files. So you may not even want to try to explain allocated vs. unallocated; too complicated. Very time consuming.
28. Put all kinds of evidence in a format that the average case agent or prosecutor can read. Create CD-ROM of all evidence, rather than babysitting a printer and killing bunches of trees. $400 for a CD ROM burner. Teach case agent and prosecutor how to use QuickView, Thumbs Plus, or Adobe Acrobat. .pdf files look like printing, but on the screen. Put everything on one CD in the same format.
29. Keep analytical notes on every bit, bite, and picture. Document successes and failures. Fill out disk evidence worksheet (erased files, recycle bin, hidden/system files, latest dated files, summary of programs located on computer, passwords (menu, communications), run all programs for "clues." Most recent docs and programs show up under the "File" menu. Internet programs and files, downloaded files. Mail programs (.PST for Microsoft Exchange). Address books (.PAD). History files, cache files,

newsgroups. Review swap file (must pull plug at time of seizure on Win95 program). A normal shutdown will cause a dynamic SWAP file to become part of unallocated space.

30. Heads parked and shut off.
31. Floppy disk in floppy drive, tape shut.
32. Floppy disks labelled, and placed in paper bags with evidence tag attached.
33. Computer equipment packed in protective boxes.
34. Look for documents with passwords.
35. Check music CDs for computer CDs. Floppies taped to underside of drawer?
36. Ask questions -- programs, who owns, what type, passwords???
37. Check doorway for "degauzer" before taking media out the door. Use compass to detect electromagnetic currents that can destroy a hard drive or erase floppies as you leave.
38. Use surge protector back at the shop. Liable if damage.
39. When not examining seized machine, remove power cord to prevent unauthorized access.
40. Plan for the long haul. It takes one day per megabyte (1 million bytes or characters) to process. 100 MB takes 100 days.

Procedures for Searching a Floppy Disk

1. Process hard drive first. Many of files could be there, floppies are used for backup.
2. Write protect the disk (don't want to change any data accidentally).
3. Virus scan (F-Prot a:)
4. Diskcopy to get exact mirror image, then write protect this copy. Diskcopy or Mares' Diskimag to copy erased files, orphan sectors, and slack space.
5. Secure the original, work on the exact copy.
6. Carefully document analysis for each disk. Use the form.
7. DOS examination
8. Look for any hidden files before you run programs, as they might be hidden. Run these programs from your C drive; that way you don't trigger anything
9. View list of files, dir, list.com, Windows Explorer. Print out a "tree" of the structure of the disk and look for pertinent directories.
10. Focus in on certain directories and subdirectories where the suspect information is likely to be.
11. Consider printing some of these things out
12. QuickView examination, if you can't pull it up any other way. Probably better than viewing in DOS with type command.
13. If you change anything, such as an attribute to make a hidden file visible, document it.
14. If hidden files, remove hide attribute if you are using QuickView (have to remove write protection temporarily, then put it back. Might be some files on that disk that, if run, could do some bad things).
15. Use Unerase
16. Use Unerase special features (check for Lost Names, etc.)
17. Run Seejunk to look for slack (EOF information)
18. Look for BAD cluster information. Whole documents can be written using Norton Disk Editor into a cluster that the suspect marks as "BAD" to try to fool investigators.
19. Check for compression utility – Stacker, SuperStor, Double Space, Drive Space. DOS, some programs, config.sys, autoexec.bat resident on the uncompressed portions, and the rest is a huge hidden systems file. If 150MB drive has only 25MB of data, you are missing the huge, hidden store of information. Easiest way to deal with is to use Windows 95. Use Microsoft Plus ($50 add-in program, with most recent version of Drive Space). Go into Explorer and format a floppy with systems files. Puts on latest and greatest compression drivers. Never have to worry about compression again. Can't find or restore erased files on a compressed drive. Worry only about active files.

Treat Windows 95 as a DOS box – don't use fancy graphics between you and the DOS files.

DDOs – dynamic drive overlays. DOS has problems with large drives. BIOS – Basic Input/Output System – tells computer what kind of keyboard, mouse, hard drive and floppy drives you have. Three modes – normal, large, and LDA. Install a new hard drive, and it tells the computer how many cylinders, heads, and sectors it has. Large=2.5 gig 4096 cylinders. Without this, you get all kinds of error messages such as "invalid media," "sector not found." DDO loaded on boot interfaces with drive to tell DOS how large a hard drive, and "this is how you can interface with it."

Each manufacturer has its own DDO. If you are not careful loading the hard drive from bad guy into your machine to mirror, you have to tinker with BIOS or DDO, which keeps changing based on changes with manufacturers. If you can't see all the drive, "Why is that?" Do I have to change the BIOS or load another DDO?

To configure a zip drive to use in computer crime investigations with Windows
To do mirror imaging and carry other investigative software¼

Get with Kirk McIntosh at Lakewood DPS. Unhook desktop computer hard drive. Boot with floppy disk. Go in with zip as "Guest." Install Windows to Drive k. Custom install. Runs a lot slower, but works.

A simple scheme to create "readable" CD ROM disk for case investigators, prosecutors and use in court.

Buy Adobe Acrobat ($190) software, and a CD "burner" ($400). Install Adobe printer on your machine. Select it as a printer to print everything to a CD, including .JPEG and .GIF files, Quicken files, and all kinds of word processing, spreadsheet and database files that can otherwise be printed out. Give to the case investigator or prosecutor with a zip file on the CD that, when exploded, gives them the free utility, Adobe Acrobat Reader. Call Chuck Davis at CBI for help. He uses this technique.

If the FAT is damaged

Power surge, turning computer off before shutting down Windows, or an incompleted write to the disk can damage the FAT. If the 1st FAT is damaged, you will see a bunch of zeroes in there. If you do a "type" command to read it, error message will come back, "Sector not found reading drive A." Can still use utility programs to view this information. 2nd FAT is still OK. Copy that on top of the 1st FAT, and the file will be OK.

Getting into Disk Edit at this point will give you the message, "Drive A has a file allocation error. Status line will only contain partial information." Disk Edit a:, alt Object, 2nd FAT. Either use Tools, Write Object, or mark, copy and paste to 1st FAT. Drag mouse al the way, Edit, Copy. Object, 1st FAT, Edit, Paste Over. Take synchronize FATs checkmark off, and write, sector by sector.

If the boot record on a disk is damaged

Formatted disks from same machine have the same boot record. Format a:/f:720 for a double density disk.

Even if you get error message: "failure reading drive a," you can still use Disk Edit to get at the disk with a damage boot record. If you use regular disk edit, you can't get in. So, at DOS prompt, diskedit/? To get help on switches. /M, maintenance mode, "bypass DOS and look at disk directly."

Diskedit a:/m. Select the size of diskette in Drive A.

When reformatting a disk, it checks for:

- Included /u (unconditional format)?
- Did you try to change from DD to HD?
- Did you use /s?
- Is there room on the disk for unformat information?

(Does above only after DOS ver. 5)

If any are true, it tells you it cannot reformat the disk. If none are true, then it proceeds to format your disk. Two files created – one stores the address of the data, the other stores the information: MIRROR.FIL and

MIRORSAV.FIL. Then it erases these files so that if the disk is unformatted, these addresses aren't available, but the data is.

Use Disk Edit to look at disk. Alt O, 1st FAT. Identify first unallocated cluster. That is where unformat information starts. Last cluster contains the address of where the unformat information is written.

format a:/f:720 – reformats DD disk as same density.

Hard disk structure and imaging

"Copy" copies files to the end of the file. Image copies that plus everything else, including system information.

- If only have one computer, one hard disk, you can partition it into logical drives (if 4 gig drive, 4 1-gig logical drives): c, d, e, f. One for regular information, one to mirror info, one to restore info, etc. If you have 800 meg of seized info, you can put it into a 1-gig partition. Image the logical drive.

- If you have one machine with two physical hard disks, restore to one of them. Utilities you need to examine are on one hard disk, then mirror to the other hard disk. C drive has utilities, image to d drive.

- Or use an external drive with utilities to do the analysis.

Fdisk shows you how the drive is organized. No. 4, display partition information. Partition status. Total disk space. Primary DOS partition is where utilities are stored. Actively boots the computer. Extended DOS partition, want to see the local drive info, Y for yes. Partition table defines how big the drives are and what operating systems they use.

Fdisk /status – tells how big physical disk is and how large logical drives are. If numbers don't add up, may be another drive you don't see.

Keep fdisk on the boot disk that you take to the crime scene.

Delete partition or logical disk drive – No. 3. Delete D drive and create two other smaller drives.
No. 1 Create logical disk drive; create logical DOS drive…ESC and reboot after making selections.

Then format logical drives you just created through partitioning.

Using a zip drive to image data:

When using a zip drive, don't put a disk into it while it is off, or it will ruin it. And always have a disk in it when transporting, or while it is sitting there, as it may fall off and get damaged.

Use utilities from FLETC to log you in as "Guest" and assign the next available logical drive to your zip drive (ziputil subdirectory). Saved under zip directory on Programs 2 disk.

Attach zip drive to host computer, and go in as guest, which assigns the next logical drive to the zip drive.

Util\sb.trn, program master, or take from the above disk. This is the Safeback program. Enter the name of the file to which audit data will be written (audit file has lots of good info in it).

Backup will take hard drive, with all hidden and deleted files, and make one huge file that you can then restore back at the office on your examination computer. "Copy" works like LapLink; you hook it up to another computer, and it transfers info exactly as it is, not just one large file. "Verify" creates a CRC to

ensure it is an exact copy.

Backup info to the drive designated as your zip drive. You will be prompted to put in another zip disk when it fills the first one.

Use Norton WipeInfo to wipe out every shred of info on the drive you plan restore the image to.

Everyday DOS, Dan Mares

(See the Everyday DOS class manual for more info)

Set dircmd=/ogn – Every time you issue dir command from then out, it will give you info sorted, subdirectories first. (GREAT TIME SAVER!). You could also set the command so that it always shows the hidden and deleted files. Put these in our boot disk.

In order to use batch files from anywhere in the system, put them in a "batches" subdirectory, and put the "batches" subdirectory in the path statement early.

e.g. "set path=ramdr:,c:\batches;c:\dos.."
Create a c:\batches subdirectory

If you consistently type the "type" command wrong, make batch files of various possible spellings, and the system will self-correct if you mistype it.

Has a program that, when you delete a file, no undelete program in the world can find it. It is totally gone. Cleans free space and slack space.

Crckit program batch file – tags your executable files, and determines whether they will launch a virus before you even run them.

Set Mares files in your path to find them.

DECLASFY – overwrites a hard disk to sanitize it before you mirror. Much faster than Norton's WipeInfo for sanitizing. Overwrites every sector up to nine times; hard drive is toast. 2 hours to overwrite 1 megabyte. Must do an fdisk on your hard drive. Doesn't even know it is out there any more. Use it when you finish a case and need to remove sensitive material to prepare for the next batch of mirrored evidence, to remove classified materials from your system, when your system has a virus and nothing else will do.

Declasfy –d a –w 1 (wipe floppy in a drive, one set of three overwrites)

Review by NSA, report available.

RMD

- Overwrites files
- Cleanses slack (empty space at end of file)
- Overwrites disk free space (where al your erased files are hiding). Do this after examining data all day so someone doesn't come in at night to read your files.
- Does simple DOS file deletion (unerasure is possible)
- Will remove everything below the subdirectory.
- RM * = del *.*
- Provides peace of mind that your erased data will not be recovered/stolen
- Use when you send disks out of the office – cleanses the slack space after the copy.
- Reviewed by NSA, report available.

RMD run by itself cleanses free space. RMD with a drive letter will cleanse that drive. RMD with file

names will erase those files. –s removes only slack. Help screen rmd –q.

MDIR program – enhancement to DIR (looks and feels like it) but sorts and shows attributes (hidden, etc.). Pauses ever screen by default.

Mdir *.com *.bat – shows two different kinds of files; DOS won't do.

Mdir –g 50000 – show me all the files over 50,000 bytes

DISKCAT

Disk cataloging programming. Output can be directed to a file Sorted output of every file. Can create a file inventory at same time you are disk imaging. Does CRC on every floppy automatically.

Can execute a DOS command on every file.

Can list only hidden/read-only files, files of a certain size, based on file types (*.exe, *.GIF, *.JPEG). Show type of file based on headers – what type of program produced it (document, zipped file, etc.). Does rely on the extension, but on the header, so that the software doesn't bypass files renamed to make them appear as if they are something else.

Does not create temp files on hard drives. Does not write to the hard drive unless asked for the output file.

Use this procedure for court validation of non-alteration of evidence. Do this as one of your first procedures.

Creates a disk label in sequence, indicating search site file it came from.

Diskcat –P – take it page by page on the screen.

Diskcat –q gives you options.

-o output file name to put listing to

diskcat –f *.zip – Shows all files.

–v command shows what is in zip files. To run the DOS command diskcat –f *.zip –e "PKZIPUNZIP –v%" –o a:zip.lis

Use RPSORT to sort this output.

CRCKIT – Creates CRC checksums (validity checkers to ensure files haven't been altered). Reads files and uses the same algorithm as PKZIP to calculate a 32-bit file CRC (checksum). Will only do one subdirectory at a time. Use HASH program if you want more. One in 4 billion chances that two dissimilar files could produce the same CRC. Creates CRCs of evidence to ensure integrity.

Crckit textfile

HASH – Companion program to CRCKIT. 32-bit CRC. Will do a file, directory, and subdirectories underneath. Finds all files, protected or not, creates short or long output record, guarantees file integrity.

Hash textfile –o text1

DISKIMAG creates floppy disk images, copy it to your hard drive to examine. Do fast search strings of imaged disk.

Places every sector of a floppy disk into a file on the hard drive. Similar to diskcopy. Will only process normal sized disks. Can call DISKCAT to catalog while you are imaging. Can call SEEJUNK to capture all slack on the disk.

Use when you need to image many seized diskettes to the hard drive. Automatically numbers each file in a sequence for easy association later on.

Doing a string search on the imaged copy on the hard drive is about 10 times faster than on the regular floppy. Use any time you need a blind diskcopy. Image a disk with key data on it, then zip it into a small file for storage.

A:>diskimag –d a: –o filename.

Disk_crc –d a: –I filename to check CRC

ALWAYS give the command from the subdirectory you are imaging to, e.g. c:\images. The command from there is diskimag –d a –o images –z.

DISKMAK – create disk from disk image.

Diskmak –d (drive) –i [input_file_name] –c# Floppy disk destination must be a formatted disk of the same size as the imaged file destined to be copied to the disk. –c# is the number of disk copies you want to make. Default is one disk image copied.

STRSRCH – searches files for strings of text. Provides 80 characters of surrounding text for context. If you make a text file with search strings in it (one per line, carriage return) and use the –s option, you can search up to 150 strings simultaneously.

Strsrch –f images.* -s strings –o strsrch.out –i
(-i=decode file position and show me exactly what sector and cluster it is in so I can look at it with Norton) strings is an ASCII search file

Write a batch file to image a number of disks, catalog the files on the disk using diskcat, and string search the disk images:

Disk.bat
Diskimag –d a: -o c:\diskimg
PAUSE
Diskcat –d a –o c:\diskcat
PAUSE
STRSRCH –d a-r –a –L
Ctl Z

SS – Searches physical disks for strings, sector by sector. Go back with Norton to verify.

DISABLE – Turns off keyboard. If someone tries to use, they cannot access. “Caution – This computer contains seized evidence. Do not touch the computer.”

SYSTEMS – Searching for operating systems and looks for partitions hidden from normal DOS operations.

DD – Disk Dump examines sectors of physical disks and shows both hex and ASCII values. Can scan for only text sectors, making evidence location easier. Can write selected sectors to files.

BRANDIT – Brand hard drives with identifying information. Distribute to colleges, companies, etc. free.

PROFILE
Dan Mares provided two Profile disks, one for 1.4meg and one for 720K to take to search sites and give an initial scan to a suspect's computer.

You can keep these profiles in separate subdirectories and boot with a sterile boot disk. Profile runs HDSentry to write block a hard disk, loads command.com, and captures CMOS data to files to regenerate CMOS if the battery dies. Get Boot captures the boot record, partitions and FAT to disk to preserve that. Checks for erased files and directories. Diskcat runs automatically to catalog the entire drive; you are prompted for a second diskette if it fills the first.

SS – Sector Search will search for strings that you enter into keyword.dat, or you can use something like DiskSearch. Add in MSD (Microsoft Diagnostics), which captures CMOS, boot record, autoexec.bat, etc.

Modify this batch file to run any other procedures you wish.

Dan Mares
IRS
P.O. Box 450168
Atlanta, Ga. 31145
(770) 986-6955
e-mail dmares@nocs.insp.irs.g

Legal Issues in Obtaining Computer Related Evidence

Issues you face:

- Educating prosecutors, judges and juries
- Strategies for search and seizure
- Taking a case to trial – breaking new ground. Law in this area is all brand new.

Lots of these cases being pleaded out. Lots of pressure to settle, "touchy-feely" white collar crime, even though they are doing some fairly nasty things. Porno cases at federal level (child porn) – strict liability based on victim's age and perpetrator's age.

Child porn cases – probably need to have a pediatrician testify that the people depicted in the images are children based on bone structure, size of arms, etc. As a matter of law, don't have to establish the identity of the child, it is a strict liability, per se prohibition. If you are charged federally, a simple depiction of a child's image is enough; doesn't have to be an actual child (could be a computer-generated morph image, make-believe kid who never existed). Will probably have a Colorado law like this soon. Even though there is no real child victim, we still don't want people trafficking in this stuff. (Fabiano is the only case that has gone through the process in Colorado thus far). Change in federal law means that they can't even bring up morphing as a defense.

If have problems proving that a photo is a non-morphed picture, contact Customs, which has printed library of child porn photos that might correspond with what you have in hand.

Expectation of Privacy – Any banners at the locality that say there is no expectation of privacy working on that company's computers or sending/receiving e-mail? E-mail seized without warrant and improperly, you can incur personal liability.

Advocate with your prosecutor's office that he have continuing legal education on this topic, or he will not be ready to take cases you produce.

Can't interfere with stuff destined for publication. If you seize the material, get back to them as soon as possible to avoid a large-scale civil rights action.

Ask for a Rule 41.1 to force criminal to reveal his PGP passphrase? If the act of producing this information is incriminating, under the 5th Amendment, you can't do it. This is testimonial in nature, and courts cannot compel this. Person could deny the computer and PGP software were not theirs, and you are taking this away from them if you compel them to reveal. You would be the only known person who would know this password, and that would be terribly incriminating. No federal cases or state/local cases on this topic.

Things to do to come "up to speed":

1. Copies of notes to investigators (including Mares' "Processing Floppy Disks"), sked training
2. Copies of notes to Sandy Wells, Vonda Mauro, Jerry Carleo
3. Create autoexec.bat for boot-up disk to automate processes. Look at Mares' checklist in "Processing Floppy Disks" handout. Add to Chuck Davis' protocol.
4. Purchase more zip disks
5. Purchase separate, external hard drive for data processing
6. Safeback for mirror imaging ($250)
7. Install QuickView Plus on all machines
8. Norton Utilities on all machines
9. Seejunk on master disk
10. Copy Messinger's evidence processing forms
11. Latex gloves for kit
12. Avery labels that fit disks for cataloging
13. Thumbs Plus for .JPEG/GIF files

144. CD burner ($400) and Adobe Acrobat ($190) to save .pdf files to give to investigator and prosecutor rather than printing out all content

155. Set dircmd=/ogn on all machines – sorts dir

166. Alta Vista to search hard drives with Boolean logic operators ($45)

177. Post "No Expectation of Privacy" signs at department; will be monitored.

.

“Accelerating Computer Learning Through Analogies” – a great little book for computer teachers. E-mail Lisa and ask her about it.