



## Computer Investigative Specialists Forms

---

*Please turn on Adobe Bookmarks*

The following forms were developed with input from numerous computer investigative specialists in the IRS CIS program as well as from other computer specialists from several law enforcement agencies. Additionally, information regarding control disks are included in this document, as well as some overall comments on analysis software. The control disks were developed for presentation in the CIS2000 training program. The CIS2000 program is a program initiated in 1997 to train special agents of US Treasury agencies - US Customs, US Secret Service, ATF, IRS Inspection and IRS Criminal Investigation Division - in the preservation, authentication and examination of electronic evidence.

The forms are presented in the order normally encountered when examining a seized computer - inventory, documenting original access, documenting all activities performed on an original machine, examination of the drive for integrity issues (hidden partitions, incorrect drive sizes, fats marked BAD, etc), examination of the drive for evidence, and finally a summary report on the findings of the examination.

The forms can be used as guidelines or reminders of activities to be performed when examining computer evidence. They should in no way be considered required steps to be performed in each and every encounter of a computer for examination. Each machine is unique and needs to be treated as such.

Modify any parts of these forms to meet your needs. As new operating systems develop and new analysis software becomes available, these forms will require update. Again, they are intended merely as a guide or reminder to assist in the examination of computers. Nothing substitutes for the training and knowledge of an experienced computer investigator.

It is recommended that whenever possible (always), work from an image copy.

Also included in this document is a summary of control disks that were recommended in the CIS 2000 program (as well as a modified alternative setup). Properly prepared control disks are extremely important to the preservation of evidence. It is important that the investigator using a control disk fully understand all commands being called in the autoexec.bat and config.sys files located on these disks.

Finally, there is a small section briefly comparing various software programs available to the law enforcement community.

Please contact me should you have any questions.

Dave Messinger  
Special Agent, IRS  
Rocky Mountain District  
Denver, Colorado  
303.446.1851

[denverdp@sprynet.com](mailto:denverdp@sprynet.com) OR [david.messinger@ci.irs.gov](mailto:david.messinger@ci.irs.gov)



# Computer Investigative Specialists Forms

## **Table Of Contents:**

<b>EVIDENCE INVENTORY WORKSHEET .....</b>	<b>3</b>
<b>INTERNAL PARTS INVENTORY SHEET .....</b>	<b>5</b>
<b>ORIGINAL MEDIA ACCESS WORKSHEET.....</b>	<b>6</b>
<b>ACTIVITIES PERFORMED ON ORIGINAL MEDIA .....</b>	<b>7</b>
<b>DISK INTEGRITY WORKSHEET .....</b>	<b>12</b>
<b>EXAMINATION FOR EVIDENCE .....</b>	<b>16</b>
<b>ANALYSIS OF COMPUTER SUMMARY.....</b>	<b>24</b>
<b>CONTROL BOOT DISKS OVERVIEW .....</b>	<b>29</b>
[EXCERPTS FROM CIS2000 CONTROL DISKETTE COURSE].....	29
CONTROL BOOT DISKS:.....	29
UTILITY DISKS:.....	30
CREATION OF DISKETTES:.....	30
CONTROL BOOT DISK USE PROCESS:.....	32
CONTENT OF AUTOEXEC.BAT AND CONFIG.SYS .....	32
SUMMARY OF FILES ON CONTROL DISKS: .....	38
<b>ALTERNATIVE BOOT DISKS .....</b>	<b>43</b>
SUMMARY OF AUTOEXEC.BAT ON DOS 622 AND WIN95B CONTROL DISKETTES: .....	43
SUMMARY OF CONFIG.SYS ON DOS CONTROL DISKETTES: .....	46
FILES THAT ARE ON ALTERNATIVE CONTROL DISK.....	49
SUMMARY OF MSDOS.SYS ON WIN95B CONTROL DISKETTE:.....	51
SUMMARY OF FILES ON WIN95B CONTROL DISKETTE: .....	52
<b>COMMENTS ON OTHER SOFTWARE: .....</b>	<b>54</b>





# Computer Investigative Specialists Forms

Evidence Tag #	Descriptions	Markings on Front	Manufacturer	Serial #	Model #

Additional Comments:



# Computer Investigative Specialists Forms

## Internal Parts Inventory Sheet (CIS Use Only - Detail of Inside Components)

				Date: _____		Initials: _____	
				Computer ID: _____			
Evidence Tag #	Qty	Computer	MB	Manufacturer	Model #	Serial #	
		Fixed Drive					
		Fixed Drive					
		Fixed Drive					
			Occupied				
			YES	NO			
		Slot 1	<input type="checkbox"/>	<input type="checkbox"/>			
		Slot 2	<input type="checkbox"/>	<input type="checkbox"/>			
		Slot 3	<input type="checkbox"/>	<input type="checkbox"/>			
		Slot 4	<input type="checkbox"/>	<input type="checkbox"/>			
		Slot 5	<input type="checkbox"/>	<input type="checkbox"/>			
		Slot 6	<input type="checkbox"/>	<input type="checkbox"/>			
		Slot 7	<input type="checkbox"/>	<input type="checkbox"/>			
		Slot 8	<input type="checkbox"/>	<input type="checkbox"/>			
			<input type="checkbox"/>	<input type="checkbox"/>			

Additional Comments: (switch settings, markings, listing of bad tracks, monitor switches, etc. ) (Continued comments on back or continuation sheets)



# Computer Investigative Specialists Forms

## ORIGINAL MEDIA ACCESS WORKSHEET

TO DOCUMENT EACH ACCESS TO ORIGINAL MEDIA

COMPUTER ID: \_\_\_\_\_

### LOG OF EVERY ACCESS TO ORIGINAL MEDIA

(Complete the following every time you access the Original Media)

1.	Access Date:		System Date: (Optional)
	Access Time:		System Time:
<input type="checkbox"/>	<b>Boot with Control Government Disks Virus Free</b>	3.5 or 5.25	Control Disk operating system: DOS 622 WIN95B
<input type="checkbox"/>	<b>WriteBlock Installed</b>		<b>Writes may occur unless booting with DOS 622</b>
<input type="checkbox"/>	<b>System info - saved as xxyy_Sl.n (see pg 3)</b>	3.5 or 5.25	Apparent OS System (see pg 2) DOS WIN95A WIN95B NT
<input type="checkbox"/>	<b>Evidence Lock (if applicable)</b>	3.5 or 5.25	Attached: <input type="checkbox"/> APEX <input type="checkbox"/> Jaz <input type="checkbox"/> SCSI Card:
Comments:			
2.	Access Date:		System Date: (Optional)
	Access Time:		System Time:
<input type="checkbox"/>	<b>Boot with Control Government Disks Virus Free</b>	3.5 or 5.25	Control Disk operating system: DOS 622 WIN95B
<input type="checkbox"/>	<b>WriteBlock Installed</b>		<b>Writes may occur unless booting with DOS 622</b>
<input type="checkbox"/>	<b>System info - saved as xxyy_Sl.n (see pg 3)</b>	3.5 or 5.25	
<input type="checkbox"/>	<b>Evidence Lock (if applicable)</b>	3.5 or 5.25	Attached: <input type="checkbox"/> APEX <input type="checkbox"/> Jaz <input type="checkbox"/> SCSI Card:
Comments:			
3.	Access Date:		System Date: (Optional)
	Access Time:		System Time:
<input type="checkbox"/>	<b>Boot with Control Government Disks Virus Free</b>	3.5 or 5.25	Control Disk operating system: DOS 622 WIN95B
<input type="checkbox"/>	<b>WriteBlock Installed</b>		<b>Writes may occur unless booting with DOS 622</b>
<input type="checkbox"/>	<b>System info - saved as xxyy_Sl.n (see pg 3)</b>	3.5 or 5.25	
<input type="checkbox"/>	<b>Evidence Lock (if applicable)</b>	3.5 or 5.25	Attached: <input type="checkbox"/> APEX <input type="checkbox"/> Jaz <input type="checkbox"/> SCSI Card:
<input type="checkbox"/>	<b>Evidence Lock (if applicable)</b>	3.5 or 5.25	Attached: <input type="checkbox"/> APEX <input type="checkbox"/> Jaz <input type="checkbox"/> SCSI Card:
Comments:			

Comments:



# Computer Investigative Specialists Forms

## ACTIVITIES PERFORMED ON ORIGINAL MEDIA

COMPUTER ID: \_\_\_\_\_

DATE: \_\_\_\_\_

INITIALS: \_\_\_\_\_

**Initial Drive Information: - Observation of boot Process**

**Bootng** – BIOS, Memory and other Screen Information:

Wrblk installed

**Initial view of Computer's Drives - Using Norton Commander -**

Drives	C:	D:	E:
Size			
Free Space <CTL +L>	% free _____	% free _____	% free _____

Comments: **CONFIG..SYS; AUTOEXEC.BAT; MSDOS.SYS** (and other observations)

**yes** -  **no** Compressed Drive - (DoubleSpace, Stacker, SuperStor, Drvspace, other)

**yes** Optional Reboot with proper drivers loaded

**Determine Operating System: <Check One>** The OS should be determined as soon as possible. This may effect further examination of Original Media. This can usually be accomplished by looking at Command.com and IO and OS system files in root. This should always be initially done using the DOS Sterile Control disk. Unless it is required that examination take place immediately, the system should not be booted with WIN95 or the DBLSPACE Control Boot disk. A FAT 32 WIN95 drive may not show up at all, but Safeback will be able to make a Physical Copy.

File Dates:	Date:	Time:	
IO.SYS			( 6:22am- DOS 622, 9:50am is 95, 11:11am is 95B -OSR2)
OS.SYS			(12:12am - 95B OSR2.1)
Command.Com			

Other Steps to help determine:	Generally DOS if	Probably 95 if
1st unsorted files	<input type="checkbox"/> - IO.SYS	<input type="checkbox"/> - IO.DOS
2nd unsorted (system) files	<input type="checkbox"/> - OS.SYS	<input type="checkbox"/> - MSDOS.DOS

View Command Com in root– search for "version"

**Version Identified:**

<input type="checkbox"/> DOS version _____	<input type="checkbox"/> DOS / Win 31	<input type="checkbox"/> WIN95 (a)	<input type="checkbox"/> WIN95 B (OSR2)
<input type="checkbox"/> NT 3.51 4.0 5.0		<input type="checkbox"/> WIN98	<input type="checkbox"/> FAT16 <input type="checkbox"/> FAT32
<input type="checkbox"/> Other (and comments)			

Note: if not determinable using steps above, run system info, diskedit, partnbl or fdisk to identify partitions



# Computer Investigative Specialists Forms

**Network Computers** - description and comments:

**IMAGE COPY and Review of Drive Integrity for Partitions / Logical Drives:** Safeback in the DIRECT mode allows you to review the disk for possible irregularities such as variances in partition sizes that could indicate further examination is needed. If Safeback indicates irregularities, you may need to explore further using FDISK, DISKEDIT, and PARTNTBL

SAFEBACK	DRIVE	CAPACITY	CYLINDERS	HEADS	SECTORS	SPECIAL
DIRECT	0					
DIRECT	C					
	0					
	C					
	D					
	E					

<input type="checkbox"/> <b>Image Copy</b>	SAFEBACK version <u>2.0</u>	Audit file YYXX.AUD		
<input type="checkbox"/> Physical <input type="checkbox"/> Logical <input type="checkbox"/> /FI 630  Output to <device>: <input type="checkbox"/> Jaz <input type="checkbox"/> Apex <input type="checkbox"/> Tape <input type="checkbox"/> Other -	<b>Other Options:</b> <input type="checkbox"/> Verify RAN  <input type="checkbox"/> Direct Access used <input type="checkbox"/> Use Extended Bios <input type="checkbox"/> Adjust Partitions (Comments)	Backup File Name:*.sfb/.001 (YYXX_C or YYXXDRV0)	CRC value yyxx_JAZ.crc or yyxxAPEX.crc (CD=YYXX_CD.CRC)	CDTransfer & verified
				<input type="checkbox"/>

**Note:** If a Logical Image is made – be sure to examine track 0 and test cylinders for data if appropriate

<input type="checkbox"/>	<b>FDISK</b> (to check if irregularities show up above)
	Findings:

<input type="checkbox"/>	<b>PARTNTBL</b> (to check if irregularities show up above)
	Findings:

<input type="checkbox"/>	<b>DISKEDIT</b> (to check if irregularities show up above)
	Findings:



# Computer Investigative Specialists Forms

**SYSTEM INFORMATION** – SI documents the condition of the computer, allows examination of various system areas and provides hardware and software information. When the machine is released from custody, another SI report (.2) documents the condition at time of return.

SYSINFO saved as report (YYXX\_SI.x) – for example 9810\_SI.1 YY=year, XX=job number, x=si report # per this computer

Report Name \_\_\_\_\_

**SYSTEM / System Summary:**

Built IN BIOS	Main Processor	Bus Type	Serial Ports	Parallel Ports

**SYSTEM / CMOS VALUES**

SYSTEM / CMOS VALUES				DISK / Disk Characteristic	
	HD Size	HD Type	Floppy Size	RAM MEMORY	Model
Primary				Base:	
Secondary				Extended:	

**DISKEDIT- Capture / Review of System Areas** (particularly if only logical drive image made)

**DISKEDIT /M** to create SAFETY NET diskette)

Track 0 Examined - Comments:

Track 0 to saved to disk DRV0\_TRK.0

**IDENTIFICATION of TEST Cylinder(s)** Last # of CYLINDERS (Logical Drive) ALT+P

Switch to Logical Drive - Last # of CYLINDERS (Logical Drive) ALT+P

Test Cylinder Examined - Comments:

Test Cylinders saved to disk DRV0\_TST.CYL

CAPTURE SYSTEM AREA - boot, fat & dir areas to disk (filename- A:sysarea.c (etc.) )

Partition Table Information

Hard Disk #	Start side	End Side	Start Track	End Track	# of sectors	Total Size
						x512
						x512

Comments

**Creation of RESCUE DISK** - Rescue Disks are created to save CMOS and other vital areas should those areas become corrupted – generally, if an image copy has been made only CMOS needs saving

Copy system files to a blank diskette - Copy IO, OS, and command.com to disk in that order

Run RESCUE to save CMOS, BOOT, & PART info to disk – Files Saved to: 3.5 5.25 APEX or JAZ

Comments

**Additional Examination of Original Drive**

**VIRUS CHECK** – If found, extra precautions are taken during examination. Agent should be notified and consideration given to notifying owner. Viruses will be noted and documented.



# Computer Investigative Specialists Forms

<b>Virus Found: Y or N</b>	Program Used:	F-PROT	Other:
Report saved as : yyxx_VIR.RPT -	Version # :		
<input type="checkbox"/> Memory <input type="checkbox"/> Boot <input type="checkbox"/> Files <input type="checkbox"/> Packed <input type="checkbox"/> Docs			
Comments			

**CRC – File CRC's should be documented on the original computer if possible. Access to the original files may not be available if the OS is WIN95 or NT**

CRC File Name (yyxxCorg.crc)		
CRC /s /h C:\*.* >> A:CRC.C1 or RUNCRC <drive> <yyxxCorg.crc < xxyyCorg.crc>		
Comments		

**DiskSearch – Searching for word strings can pinpoint files or areas of the drive that contain relevant information to the search. The CIS should insure that searches are conducted within the limits of the search warrant**

Output file saved as (ex. A:dsout.c)    Disk No.		
Comments		

### Additional Examination of Original Drive

<input type="checkbox"/> Copy Autoexec.* and Config.*	3.5	5.25	Apex / Jaz		
<input type="checkbox"/> <b>TREE &gt;&gt; A:TREE.C (etc.)</b>	3.5	5.25	Apex / Jaz		
<input type="checkbox"/> <b>DISKINFO &lt;drive&gt;</b> - gathers chkdsk info and hidden/readonly/system file info <DISKINFO> for Guest Driver					
<input type="checkbox"/> <b>CHKDSK (Copy to disk CHKDSK C: &gt;&gt; A:)</b>	3.5	or 5.25	Disk No.:		
	Total Size	Bytes Free	Hidden Files	Errors	Bad Bytes
Drive C:					
Drive D:					
Drive E:					
Comments					

**ERASED files** – while generally erased files will be examined on the image copy, there may be times when examination will take place on the original media. Using Norton Unerase <View All Directories> and PRN2FLE to redirect screen outputs - along with searching for Lost File Names and Data Types can assist in reviewing the computer for erased files.

	3.5	or 5.25	Disk No.:
	erased files	lost names	data type
Comments			



# Computer Investigative Specialists Forms

<input type="checkbox"/>	<b>LAPLINK PRO</b>		
	Comments		
<input type="checkbox"/>	<b>HEADS PARKED &amp; SHUTOFF</b>	3.5 or 5.25	Disk No.:
	Comments		

**ADDITIONAL COMMENTS & OBSERVATIONS**



# Computer Investigative Specialists Forms

## DISK INTEGRITY WORKSHEET

Case Information / Number	Date:	Initials:
		Computer ID:

Note: This worksheet is intended to assist the CIS in an in-depth analysis of disk structure. All steps may not be required depending on the analysis required. Some steps may have been performed during other analysis processes.

<input type="checkbox"/> Establish the scope of examination with agent
<input type="checkbox"/> Control Disk used - ID:
<input type="checkbox"/> Working on Original Media <input type="checkbox"/> Working from Restored Image - ID:
Examination DISK OS Version used <input type="checkbox"/> 622 <input type="checkbox"/> 95 - v7.0 <input type="checkbox"/> 95B v 7.1 <input type="checkbox"/> Other:
<input type="checkbox"/> 95 - GUI <input type="checkbox"/> 95B - GUI
Note: All 95 OS will change Last Accessed File Date if file viewed 95B partitions are not accessible without 95B boot disk or LINUX OS
<input type="checkbox"/> Writeblock installed (if needed for documentation)

**SYSTEM AREAS via Diskedit**  
 To Save system areas as workpapers:  
 PRN2FILE DISKSTRU.C to redirect printer writes to file or use Diskedit print functions under tools and print each disk area separately to file.  
 CTRL + P to saved as system workpapers

C		Area	Activity (hex and area view)
<input type="checkbox"/>	<input type="checkbox"/>	PARTITION RECORD    ALT + A	Cylinder gaps (use 1st page for recording if needed)
<input type="checkbox"/>	<input type="checkbox"/>	BOOT RECORD          ALT + B	Unusual names / entries (& in HEX for IO & OS files before 55 AA)
<input type="checkbox"/>	<input type="checkbox"/>	FAT1                    ALT + F1	Bad Clusters (F7 FF), gaps, fat slack
<input type="checkbox"/>	<input type="checkbox"/>	FAT2                    ALT + F2	same
<input type="checkbox"/>	<input type="checkbox"/>	ROOT                    ALT + R	inspect unused directory area, directory slack, hidden , split, ALT255, attributes
<input type="checkbox"/>	<input type="checkbox"/>	SUB-DIR                ALT + R	systematically go through each sub-dir for above

Observation of Partition and Boot Areas

Observation of FATS (gaps, bad clusters, slack etc) (Hex and as FAT)

Observation of Root and Sub-Directory areas: (gaps, split, or locked directories, ALT 255 (HEX FF), unusual entries, review past "unused directory areas" in HEX):

Observation of Track 0



# Computer Investigative Specialists Forms

## Boot Process: (to verify that boot files do not appear to have been tampered with)

No	
<input type="checkbox"/>	1st file in root directory is an IO system file
<input type="checkbox"/>	2nd file in root directory is an OS system file
<input type="checkbox"/>	The IO system file calls config.sys (at approx 95%)
<input type="checkbox"/>	The IO system file calls command.com
<input type="checkbox"/>	Review config.sys (print out and note observations)
<input type="checkbox"/>	Review Autoexec.bat (print out and note observations)
<input type="checkbox"/>	Locate command.com's call to autoexec.bat (at approx 15%)
<input type="checkbox"/>	Review command.com's internal commands - "dir,type,copy, rename,date,time" (at approx. 70%)
<input type="checkbox"/>	Locate command.com's ".com.exe.bat" order (at approx 90%)
<input type="checkbox"/>	Check for multiple command.com's - review each one (use Norton commander to find them and use CRC's to eliminate dups)

Virus detection (if not done on Original Media)  
 Program Used \_\_\_\_\_ Version \_\_\_\_\_ Results filename (X:\<filename.c, etc)  
 Clean  Infected

CRC verification - Verify restored files (Word - Options/compare version) (CRC\_DS.exe)  
 Compares or explanation:

DS (Disksearch) (look for keywords save as file - X:\DS.C) (Contact case agent)

CHKDSK (save as file X:\CHKDSK.C)

10. TREE (TREE C: >> X:\TREE.C)

11. File Attributes  
 DIR C:\\*.\* /S/AH >> X:\DIR.HID  
 DIR C:\\*.\* /S/AS >> X:\DIR.SYS



## Computer Investigative Specialists Forms

DIR C:\\*. \* /S/AR>> X:\DIR.RO

Don't forget other drives

12. HEADER.EXE for 1st line header check (look for MZ in .EXE files)

13. .COM files less than (<) 64K (use CRC\_C.DBF for review) (if > 64K, explain)

Batch file comments Number of batch files (use CRC\_C.DBF to find): \_\_\_\_\_

Erased files:  Writeblock on reminder

a. Deleted Directories first (document by print screens or using Norton Unerase (prn2file undir.c)

b. Deleted Files (document ) (option - DOS UNDELETE (sweep undelete /list >> X:\undel.c)  
Number of deleted files: \_\_\_\_\_

c. Undelete the Files

Norton Unerase for directories

Option - DOS Undelete for files (sweep undelete \*.\* /all)

Option - Number of auto recovered files: \_\_\_\_\_

Option - Number of auto non-recoverable: \_\_\_\_\_

d. Recover partial .WK1, .DBF, and .TXT files

Norton Unerase (Search /Data Type and Lost Names)

Observations:

Notes: (Names of deleted directories, etc.)



## Computer Investigative Specialists Forms

DISKEDIT Drive Partition Information- The following can be used if drive size / partition info requires additional examination

Hard Disk #		Size	Type	Heads/Sides	Cylinders/Tracks	Sectors
	C:					
	D:					
	E:					

Partition Table Info:

Hard Disk #	Start side	End Side	Start Track	End Track	# of sectors	Total Size
					x512	
					x512	
					x512	



# Computer Investigative Specialists Forms

## EXAMINATION FOR EVIDENCE

Case Information / Number

DATE:

INITIALS:

COMPUTER ID:

Note: This worksheet can be used to assist the CIS in the analysis process of examining a computer for evidence. It will usually be used when working on a restored image of the original computer. All steps may not be required depending on the depth of analysis required. Some steps may have been performed during previous analysis processes. You may wish to modify this worksheet to meet your documentation process.

Establish the scope of examination with agent (what are you looking for – is it included on the search warrant)

Examination taking place on:  Original Computer  Image

Writeblock (optional on image unless documenting unallocated areas)

Examination Boot or Fixed Disk OS Version used  622  95 – v7.0  95B v 7.1  Other:  
 95 – GUI  95B – GUI

Note: All 95/NT OS will change Last Accessed File Date if file viewed or CRCed  
95B partitions are not accessible without 95B boot disk or LINUX OS

**TREE** (TREE C: >> yyxx.tree.C) if needed - can record examination notes in tree structure using edit file  
 optional use of Norton Navigator – File / Print List (Generic printer, print to file, may need to change Courier font)

**DS (Disksearch)** (look for keywords save as file – X:\DS.C) (Contact case agent)  Writeblock on “reminder” if needed  
(if restore on SCSI drive, may have to enable drive bios)

**Review of Hidden/ System Files** [Advanced Recovery]

- DIR C:\\*\\*/S/AH >> X:\DIR.HID
- DIR C:\\*\\*/S/AS >> X:\DIR.SYS
- DIR C:\\*\\*/S/AR >> X:\DIR.RO
- Don't forget other drives

or  DISKCAT -d <drive> -f \*.\* -H -O <Yyxx\_Hid.Fil)

Comments on unusual Hidden/ System files:

**HEADER.EXE** for 1st line header check (look for MZ in .EXE files, other unusual headers) [Advanced Recovery]

<alt> DISKCAT -zh <fileheader file> -O header.out

**.COM** files less than (<) 64K (use sorted CRC listing for review) (if > 64K, explain) [Advanced Recovery]

<alt> DISKCAT -d c: \*.com -o com\_file.1

**CRC** - if not already done



# Computer Investigative Specialists Forms

**Erased files:**     Writeblock involved ? (a "reminder" if needed for evidentiary documentation)

Examination of erased files may prove beneficial and provide clues to files that were on the drive. Use of disk search programs may have already identified any data in unallocated areas that you may have interest in. However, examining for erased files may prove beneficial. Recovery of erased data is usually performed on the restored image copy. Data can be recovered directly on the drive or written to different drive location <Unerase To>.

Recovering erased files can be performed various ways. Here is one method using Norton UNERASE version 95. The 95 version is used because it works in conjunction with the recycle bin. The steps usually involve:

- Documenting the erased files (load PRN2FILE <filename> and <View All Directories>, then use PRINTSCREEN to redirect screen outputs to the documentation file
- Be sure to recover Directory areas first (if they contain directory entries)
- Recover files to a another destination (easiest way to find the files later)
- Then recover files automatically in their current directory (this allow for lost file name and data type searches)
- Search for Lost File Names and Data Types (can provide additional information about deleted files not available through normal unerase activities.)

Note: If restore is on a SCSI drive, may have to enable drive bios before Norton Unerase will recognize the drive. This may mean booting your system with a floppy to boot around the restored i mage operating system.

	Aprx # of erased files	Excellent	Good	Average	Poor
Drive C					
Drive D					
Recovered					
		Data Type -TXT	Data Type -WK1	Data Type - DBF	Lost Names
	# of Files				

Comments and notes erased files:

- Alternative documentation of Deleted Files (option - DOS UNDELETE (sweep undelete /list >> X:\undel.c)  
 DOS Undelete for files (sweep undelete \*.\* /all)

**Recycle BIN** (Note: EXPLORER does not always accurately show files in the recycle bin. Norton Navigator does)

- Review of Recycle Bin  
 Review of other SENTRY or RECYCLE data

**Comments:**

- Latest Dated Files** – determine and rewiev the files most recently saved for recent activity
- use CRC listingand print latest
  - <alt> DISKCAT C:\\*.\* -t 90 -O lastdate.fil  
(-t 90= no more than 90 days old)

- |                                                                                                                                                   |               |             |
|---------------------------------------------------------------------------------------------------------------------------------------------------|---------------|-------------|
| <input type="checkbox"/> <b>Directory Dates</b> – identifies when directories were created, programs installed, etc.                              | Earliest Date | Latest Date |
| <input type="checkbox"/> DIRBAT C: xxyy_dir.1 (DOS's DIR C: /AD >> xxyy_dir.1<br><input type="checkbox"/> <alt> DISKCAT -d C: -D -o dirlist.1 ??? |               |             |

- Last Access and File Created Dates needed ?** – 95 & NT contains additional dates in the Directory areas.
- Diskcat
  - Hash
  - CRCKit





## Computer Investigative Specialists Forms

**Summary of Programs located on Computer:** While examination of may not require identification of all programs on the computer, many times such identification is helpful in discussing the contents of computer with case agent. The summary can be an attachment to your summary report of examination, and it can be used as a refresher in reviewing the computer at a later time. If you are examining in a Windows environment, It may be helpful to have both Norton Navigator using the Viewer Pane (or Explorer with QV Plus) as well as the Tree directory file (if you use it) to record your comments.

\* **Appears Not Used:** While many programs may be on a computer, a "X" in this column identifies programs that have been installed by do not appear used – that is, no apparent data files other than sample files or when the program starts, screens for setting a first time user appears.

	Summary of Programs	Version	Appears not used *	Program Owner identified (if relevant) (using Help / About )	Multi-Purpose	Wordprocessing	Spreadsheet	Database	Presentation	Accounting	Investment Tracking	Communications	FAX	Publishing	Graphic	Internet	Disk Utilities	Games	Virus			
	Program Name																					
<input type="checkbox"/>	Microsoft Office																					
<input type="checkbox"/>	Word																					
<input type="checkbox"/>	Excel																					
<input type="checkbox"/>	Access																					
<input type="checkbox"/>	PowerPoint																					
<input type="checkbox"/>	MS APPS programs MSGraph, MSChart, etc)																					
<input type="checkbox"/>	Coral Office Suite																					
<input type="checkbox"/>	Word Perfect																					
<input type="checkbox"/>																						
<input type="checkbox"/>	Quicken																					
<input type="checkbox"/>	QuickBooks																					
<input type="checkbox"/>	Procomm																					
<input type="checkbox"/>	It's Legal																					
<input type="checkbox"/>	MS Works																					





## Computer Investigative Specialists Forms

Draw programs

( Latest files in <File> menu )

Communications

( Latest files in <File> menu )

Accounting programs

( Latest files in <File> menu )

Utility programs

( Latest files in <File> menu )

Database programs

( Latest files in <File> menu )

Backup programs

( Latest files in <File> menu )

Graphics files (View graphic files for contents)

Note: View graphic files using viewers or the native program. It is best to have the case agent view the files.

Other programs

**Internet Programs and Files** – Internet programs may be important to the investigation. As there are many programs used in connection with the Internet, a separate section is provided for their review and examination, if required. It may be that you are interested in URL's visited, or e-mail messages, or the History file. You may be interested in downloaded files. IPFILTER allows examination of single files for e-mail and URL addresses. It can be ran against any file – including cache and swap files.

		Ver	Used ?	Comments
	Internet <input type="checkbox"/> Explorer <input type="checkbox"/> Netscape <input type="checkbox"/> Other			



## Computer Investigative Specialists Forms

Identified ISP's programs <input type="checkbox"/> MSN <input type="checkbox"/> AOL <input type="checkbox"/> Compuserve <input type="checkbox"/> AT&T <input type="checkbox"/> Other			
Other Internet Programs: <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Ver	Used	Comments
Mail Programs: <input type="checkbox"/> Microsoft Mail <input type="checkbox"/> Exchange <input type="checkbox"/> Eudora <input type="checkbox"/>			If exchange
Mail - .PST for Exchange (32,768 k is default )			
Address Books - .PAB			
\system\FAVORITES folder			
History files (probably have to run specific program)			
Cache Files			
Downloaded files:			
Newsgroups			
<p><b>Swap File Review</b> (copy to another media – filter, search) The SWAP file can contain clues if an in-depth analysis is required. Capturing the SWAP file in 95 requires either pulling the plug at time of seizure. A normal shutdown will cause a dynamic SWAP file to become part of unallocated space.</p>			



# Computer Investigative Specialists Forms

---

## Additional Comments



# Computer Investigative Specialists Forms

## Analysis of Computer Summary

Date	
	Desk / Note / Net
MFG	
Model	
Evidence ID	
Job #	

### Summary of Computer:

Processor:		Date Seized	/ /
Operating System :		Date in CIS	/ /
<input type="checkbox"/> WIN95 <input type="checkbox"/> NT <input type="checkbox"/> DOS <input type="checkbox"/> WIN31 <input type="checkbox"/> Other :		Custody	
Disk Size	C:	D:	Date Returned
Disk Space Used (%)			/ /
Disk Structure	<input type="checkbox"/> OK <input type="checkbox"/> see comments below	# of 3.5" Floppies	
<input type="checkbox"/> Virus Checked	<input type="checkbox"/> OK <input type="checkbox"/> had infection	# of 5" Floppies	
<input type="checkbox"/> Owner notified		# of Tapes	
<input type="checkbox"/> Backup Image Made		Other:	
<input type="checkbox"/> image transferred to CD			

### Additional Comments:

### Summary of Findings and Explanation of Attachments:

TREE of All Directories (Attachment A) A "tree" gives you a graphical listing of the "directories" (also know as "folders"). The directories reflect how files are organized on the disk(s).

The TREE is basically an overview of how the computer is organized internally. There are comments on the tree report that explains the general content of the files located within most folders. You should review the entire tree listing to familiarize yourself with how the files were organized on this computer.

Data File Listing (Attachment B) This computer had over \_\_\_\_\_ files. There are lots of files on most computers. Generally most files on a computer are files needed or used by a program - HELP files, PROGRAM files, INDEX files, support files, etc. Those type of files generally contain meaningless or undecipherable information (at least to a user) and are usually identified by their extensions.

This DATA FILE LISTING report (ATTACHMENT B) summarizes only those files that appear to be DATA type files - that is files such as spreadsheets, databases, word processing, etc. The report is based on file extensions. The included data file extensions are in the header of this report. (Note: A complete listing of all files located on the computer will be provided upon request.)

Files that do not appear to be relevant may be crossed out and files identified as being possibly relevant may be highlighted in yellow or have other comments. **However, You should review all the file names listed in this report for any names that may be relevant to your investigation. You can also use this report as a workpaper in tracking your review of files provided to you on disk or CD.**

### Comments:



## Computer Investigative Specialists Forms

**Latest Dated Files (Attachment C)** is a short summary (usually three pages) of the most recent dated files and is an possible indication of how the computer was probably last used. Reviewing these files will familiarize you with the most current used files. Remember - DATES are not always accurate and could have been modified. This report includes all files and not just "data" files (see attachment B).

Latest Dated File \_\_\_\_/\_\_\_\_/\_\_\_\_

### Comments:

**Compressed Files Listing (Attachment \_\_\_\_)** Zipped or Compressed files are files that contain many files grouped together. Zip files are sometimes used to back up files onto one disk, or to keep certain files together. This attachment lists the names of files contained inside the Zipped files on the computer. They may require further examination if you determine they are relevant to the investigation. **If attached, you should review this report for any relevant file names**

Zipped files encountered? yes no

Report Attached ? yes no

Comments:

**Address/Pim/Script Files (Attachment \_\_\_\_)** These files are indicative of addresses or other contacts the users of the computer may have had. Any information that should be furthered examined are highlighted in yellow. Generally the CIS reviews this report to see if any address books should be printed, or if there are any password clues in the script files.

**Graphic Files (Attachment \_\_\_\_)** Graphic files include Newsletters, Signs, Drawings, Photos, etc. Many programs create graphic files and use graphic files (.JPG, .GIF, .DRW, .PCX, .CGM, .WPG, etc.) for clipart or drawings. Users can create these type of files. These files must be viewed using a "viewer" or the native program. **You may want to review the file names for pertinent or obvious names. Your CIS can assist you in reviewing such files.**

Graphic files (other than standard program files) located: yes no

Report Attached? yes no

Comments:

**Password Protected / Encrypted Files** - Passwords and encryption may indicate that the content of files were meant to be private. Most computer examinations are not a file by file examination, so it is difficult to determine all password protected files. Additionally, communications script files can contain passwords. If any passwords were encountered during examination, comments appear below.

Passwords encountered during examination? yes no

Comments:

**95/98/T Desktop (Attachment \_\_\_\_)** If the machine is a WIN95/98 or NT machine, this attachment reflects the Programs that are on the Desktop. They will probably be long file names and will give you an indication as to how the machine was used.

START MENU & DESKTOP (Programs on the computer)



## Computer Investigative Specialists Forms

Profiles (indicative of Users)  
Users indicated:

Recent and Personal (indicative of the latest and personal Document Files)  
Comments:

Favorite and History (indicative of Internet use)  
 internet activity indicated

Cache/Cookies Files (Attachment \_\_\_\_) - These files give a more detailed look at internet usage and normally are examined only by the CIS for review. If it appears they are relevant to the investigation, the report may be included.

Folder Created Dates (Attachment \_\_\_\_), if included, is a summary of the dates directories or folders were created. This would be important to establish timing of certain events or in determining the history regarding a computer's setup.

Recycle Bin (Attachment \_\_\_\_) On some computers, deleted files are kept in a "Recycle Bin". These files may also be included in other reports depending on the 3 character file extension. **You should review this report for any relevant file names.**

Comments:

Erased Files (Attachment \_\_\_\_) is a summary containing the names of files which can possibly be recovered. Generally, not all such files are recoverable. Erased files are normal on most computers. Normally (but not always) little information is contained in erased files that is not contained elsewhere on the computer. However, that is not always the case, and you may need to examine those files. **If this report is attached, you should review file names for relevancy.**

Approximate # of deleted files \_\_\_\_\_

Comments:

Key-Word Disk Search (Attachment \_\_\_\_) Searches of the computer using certain "key" words provided by the agent may have been made. This attachment contains a list of the words searched for as well as the names of files identified as containing these "key" words hits. **You should review the "key" word hits to determine if you need to look at the related files.**

Comments:

Existence of Unusual Hidden/Read-Only Files - Certain Hidden and Read-Only files generally exist on all computers. Unusual ones may be indicative of the user attempting to hide information.

Computer Examined for Unusual Hidden/Read Only files ? yes no

Comments:



## Computer Investigative Specialists Forms

---

**Printouts (Attachment I)** *During examination of the computer, the CIS may print out various information that is encountered. Generally this is for your examination and may be relevant to the investigation. Please review the items if included.*

**Other Attachments and comments:**





## Computer Investigative Specialists Forms

### Control Boot Disks Overview

*NOTE: There are two control disks formats included - the one that follows (from the CIS2000 class material), and an **Alternative Control Boot Disk** section found on page 43.*

#### **[Excerpts from CIS2000 Control Diskette course]**

The use of the control boot disk dates back to the beginning of the development of the computer seizure process known as the Safety Net. Without the use of a control boot disk, it is impossible to know exactly if a computer is booting (starting) in a manner which will not alter and/or destroy the data contained within. By using a control boot disk, as the name implies, the Computer Investigative Specialist (CIS) controls the boot process by providing known, good and clean system files for the computer to use in the boot process.

In order to truly control the boot process the CIS must ensure that the control boot disk used is in good working order, that the files contained on the disk are from a known source and are clean (both disk and files) of virus infection.

The following are steps to further insure that the boot process is controlled by the CIS agent:

All removable disk drives must either have controlled boot disks inserted in them or be removed from the system. (e.g. disconnect external devices such as Zip drives prior to booting)

The CMOS must be checked to verify the boot sequence as floppy drive first - hard drive second (typically A: / C:). This is to ensure that the system does not by-pass the floppy drive(s) and boot directly from a hard drive.

The CIS must closely monitor the boot process to ensure that the system is booting from the control boot disk. If it appears that the system is booting from another device, the boot process must be immediately terminated. (e.g. power off or Ctrl-Alt-Del keystroke sequence)

Once the system is booted, care must be taken to ensure that either a control boot disk or non-bootable utility disk is in the floppy drive(s) at all times. This is to ensure that the system is not accidentally re-booted from a system hard drive.

Your boot disks do not have to match these exactly, however, they must accomplish the same goal – the controlled boot of a suspect system.

#### **Control Boot Disks:**

Boot Disk #1 – Simple boot disk with no memory managers.

Boot Disk #2 – Simple boot disk with memory managers.

Boot Disk #3 – Boot disk with memory manager. Also runs Norton's System Information (sysinfo.exe) on boot and writes report to the "Rcv\_data" subdirectory on the control boot disk.

Boot Disk #4 – Boot disk with memory manager. Also runs Norton's System Information (sysinfo.exe) on boot, writes report to the "Rcv\_data" subdirectory, and loads device drivers for the Pinnacle APEX Optical hard drive and Adaptec Mini-SCSI cable.

Boot Disk #5 - Boot disk with memory manager. Also runs Norton's System Information (sysinfo.exe) on boot, writes report to the "Rcv\_data" subdirectory, and loads device drivers for the HD45 Quick Drive hard drive and HD45 cable.

Boot Disk #6 - Boot disk with memory manager. Also runs Norton's System Information (sysinfo.exe) on boot, writes report to the "Rcv\_data" subdirectory, and loads device drivers for the Pinnacle APEX Optical hard drive and Adaptec 2940 Wide SCSI card and SCSI cable.



## Computer Investigative Specialists Forms

All of the above listed boot disks load WriteBlock (wrblk.exe) on boot-up and set environments so that temporary files write to the "Temp" subdirectory on the control boot disk. Each disk also has a "Cr.txt" file, which contains a single carriage return (Enter). This file is piped into the "Date" and "Time" calls in the autoexec.bat file. The piping of this file allows the use of the internal DOS commands "date" and "time", but prevents the date and time from accidentally being changed by the CIS.

In addition to the above, disks #4, #5, and #6 also contain the CRC program (crc.exe) and Sydex's SafeBack Master (master.exe) program.

***Another Note : The Alternative Control Boot Disks use three boot diskettes:***

- ***DOS 622 Sterile (will not boot dblspace drive)***
- ***DOS 622 Control (will boot dblspace drive)***
- ***WIN95B - to access a FAT32 drive***

***In the alternative control boot disks, the Config.sys and autoexec.bat provide the features found in the six diskettes described here.***

### Utility Disks:

Util Disk #1 – Utility disk with Disk Search 2 (Ds2.exe) and Partition Table utility (partntbl.exe) which displays the hard drive partition table.

Util Disk #2 – Utility disk with Norton's Disk Editor (diskedit.exe).

Util Disk #3 – Utility disk with Norton Commander (Nc.exe) and file viewers for word processing, database, and spreadsheet files.

Util Disk #4 – Utility disk with Norton Commander (Nc.exe) and the remaining file viewers contained in the Norton Commander package.

Util Disk #5 – Utility disk with F-Prot virus checking software. Disk also contains a batch file (Go.bat) which executes the F-Prot software from the command line with all applicable switches.

Util Disk #6 – Utility disk with McAfee's virus checking software. Disk also contains a batch file (Go.bat) which executes the McAfee software from the command line with all applicable switches

While the Norton Commander program can fit on one high density diskette, all of the viewers will not fit on one diskette. Each diskette #3 and #4 contain all files necessary to run Norton Commander for ease of use.

All of the utility diskettes contain the MS-DOS version 6.22 command.com file. This must be the same command.com file on the control boot disk. DO NOT make utility diskettes bootable. The command.com file is added to the utility diskettes to make them easier to use during on-site examinations. If command.com is not loaded on the diskettes, the control boot disk would have to be re-entered in the drive each time the utility diskettes were changed.

### CREATION OF DISKETTES:

Creating each of the diskettes starts in the same manner. A diskette (any size and capacity) is first unconditionally formatted (format x: /u). Please note that special switches may have to be used to format double (low) density diskettes.

If the diskette is to be used as a control boot disk, then the system files must be added using the System (sys.com) command.



## Computer Investigative Specialists Forms

If the diskette is to be used as a utility disk, only the command.com file is copied to the diskette. DO NOT make utility diskettes bootable.

**[Note: the following two paragraphs have been modified slightly from the CIS2000 course material]**

You may choose to have two sets of bootable control disks:

- One that does not mount a doublespace (or drvspace) drive
- One that will mount a doublespace (or drvspace) drive

If you choose to make a diskette that does not mount a doublespace drive, you need to make some modifications to that diskette:

- Once the system is added, the hidden read-only system file Drvspace.bin SHOULD be deleted from the diskette.
- In order to protect against the diskette mounting a compressed drive on the suspect system, the IO.sys MUST be modified. (If you are uncomfortable doing this, only make a control disk that will mount a doublespace drive.) This is accomplished using Norton's Disk Editor program. The first modification is to change the file extensions on Dbldspace.bin, Drvspace.bin, and Drvspace.ini to "xxx". The file extension on all three files MUST be changed to "xxx". These calls (file names) are located at offset 33,098 in MS-DOS 6.22's IO.sys file.
- An additional modification is made in the IO.sys file. This change is made to the statement "Starting MS-DOS...". MS-DOS displays this message on the monitor at the start of boot-up. This statement is replaced with "STERILE BOOT DISK xxx". The "xxx" refers to the CIS's initials, and should be in lowercase letters. In MS-DOS version 6.22 IO.sys file, "Starting MS-DOS..." is located at offset 40,213. While this modification does not prevent the suspect system from completing some unwanted action, such as mounting a compressed drive, it does provide the CIS with verification that the system is booting from the control boot disk when it (STERILE DISK BOOT xxx) displays on the monitor during boot-up.

Once these modifications are completed and saved to the diskette, the diskette is ready to have the necessary file(s) copied to the diskette. Please see the attached sheets for a list of the files required by each diskette and the associated config.sys and autoexec.bat files for each diskette.

Once all the files are copied to the diskette, several other steps are necessary to make the diskette ready to use in the field. This process is called Stack, Clean and Pack.

**Stack** – Stacking the diskette is accomplished using Norton Utility Speed Disk (speedisk.exe) to optimize the diskette. This process will unfragment the files. Complete this process even if Speed Disk reports that no optimization is necessary. Also it is best to select "Full with Directories First" under Optimization Method prior to Beginning Optimization.

**Clean** – Cleaning refers to two processes. This first is to check each diskette for the presence of viruses. This should be completed using two different virus checking software packages. It is all very important that each program has up-to-date virus definition tables. If a virus is identified on the diskette, both the diskette and the source computer will have to be completely cleaned of any and all viruses and thoroughly re-checked prior to continuing.

The second part of the clean process is accomplished using Sydex's Prune (prune.exe) program. This program removes data from the slack areas (files and unallocated) on the diskette. The program should be used with both the /s and /u switches. These switches will instruct the prune.exe program to recursively scan subdirectories and clear out all unallocated file space.

**Pack** – Packing refers to making self-extracting image files of the control boot and utility diskettes. This is accomplished using Sydex's CopyQM program. Making self-extracting image files and storing them on a portable notebook computer, allows the CIS to easily make additional copies of the control boot and utility diskettes at a search site.

Once the Stacking, Cleaning, and Packing are complete, each diskette should be clearly labeled.

The diskettes are now ready for use.



## Computer Investigative Specialists Forms

### CONTROL BOOT DISK USE PROCESS:

The recommended control boot disk process is as follows:

Insert control boot disk #3 in primary (A:) floppy drive. If there is second floppy drive, insert either control boot disk #1, #2, or #3.

NOTE: In order for disks #3 - #6 to work properly, they can NOT be write protected when used. If the disk is write protected, Norton's System Information (sysinfo.exe) program will generate an error when it attempts to save the report file to the diskette. This error will prevent the report from being written.

It is for this reason (no write protection) that it is highly recommended that any non-write protected control boot or utility disk only be used in one machine.

Disconnect any attached removable disk drives.

Power-up system, while paying close attention, and switch to CMOS screen if possible.

If access to CMOS is gained, verify that system boot sequence is to floppy disk first.

Re-boot system paying close attention to process.

If system will not boot (freezes) attempt re-boot with control boot disk #2.

If system will not boot with control boot disk #2, attempt re-boot with control boot disk #1.

If system will not boot with control boot disk #1, seizing machine may be only option.

If system boots with control boot disk #3, the system should be virus checked with two different (up-to-date) virus checking software programs. The results should be documented. If a virus or viruses are discovered, they should not be removed or altered. When the virus checks are completed, the on-site examination of the system should begin using the other utility disk(s).

Once it is determined that evidence is present and/or data image will be seized, re-boot system with control boot disk #4, #5 or #6 depending on the device(s) to be used to make the image.

Once the system is re-booted with either disk #4, #5, or #6, a CRC can be run on the files to be seized. When the CRC is completed, SafeBack Master (master.exe) can be executed and the image will be created and written to the device specified by the user.

### Content of Autoexec.bat and Config.sys

#### Disk #1 - Contents Of The Autoexec.bat File

```
@echo off
prompt=$p$g
a:\wrblk
echo.
echo.
echo This machine is booting from the 3 1/2" diskette.
echo.
echo.
echo ATTENTION:
echo.
echo This is the Control Boot Disk for NON-COMPRESSED drives.
pause
```



# Computer Investigative Specialists Forms

cls

```
echo *****
echo *****          DO NOT          *****
echo *****          TOUCH OR OPERATE THIS EQUIPMENT          *****
echo *****          THIS EQUIPMENT MAY CONTAIN EVIDENCE          *****
echo *****
pause
```

```
cls
set temp=a:\temp
set tmp=a:\temp
set nu=a:\temp
cls
echo.
echo.
echo.
date < a:\cr.txt
echo.
echo.
echo.
time < a:\cr.txt
echo.
```

(Continued on Next Page)

```
echo *****
echo *****          *****
echo *****          NOTE: Record the above listed dates and times.          *****
echo *****          These are the system clock settings          *****
echo *****          on the target machine.          *****
echo *****          *****
echo *****          DO NOT attempt to change.          *****
echo *****          *****
echo *****
echo.
echo.
echo.
a:
```

## Disk #1 - Contents Of The Config.Sys File

```
files=30
fcbs=4,0
stacks=9,256
buffers=40
lastdrive=z
shell=a:\command.com /p /e:1024
numlock=off
```

## Disk #2 - Contents Of The Autoexec.bat File

```
@echo off
prompt=$p$g
a:\wrblk
echo.
echo.
```



## Computer Investigative Specialists Forms

```
echo This machine is booting from the 3 1/2" diskette.
echo.
echo.
echo ATTENTION:
echo.
echo This is the Control Boot Disk for NON-COMPRESSED drives.
pause
```

```
cls
```

```
echo *****
echo *****          DO NOT          *****
echo *****          TOUCH OR OPERATE THIS EQUIPMENT          *****
echo *****          THIS EQUIPMENT MAY CONTAIN EVIDENCE          *****
echo *****
pause
```

```
cls
set temp=a:\temp
set tmp=a:\temp
set nu=a:\temp
```

```
cls
echo.
echo.
echo.
date < a:\cr.txt
echo.
echo.
echo.
time < a:\cr.txt
```

```
echo *****
echo ****          ****
echo ****          NOTE: Record the above listed dates and times.          ****
echo ****          These are the system clock settings          ****
echo ****          on the target machine.          ****
echo ****          ****
echo ****          DO NOT attempt to change.          ****
echo ****          ****
echo *****
```

```
echo.
echo.
echo.
a:
```

### Disk #2 & #3 - Contents Of The Config.Sys File

```
devicehigh=a:\dos\himem.sys /v
devicehigh=a:\dos\emm386.exe noems
dos=high,umb
files=30
fcbs=4,0
stacks=9,256
buffers=40
lastdrive=z
shell=a:\command.com /p /e:1024
numlock=off
```





# Computer Investigative Specialists Forms

```
date < a:\cr.txt
echo.
echo.
echo.
time < a:\cr.txt
echo.
```

```
echo *****
echo ****
echo **** NOTE: Record the above listed dates and times.
echo **** These are the system clock settings
echo **** on the target machine.
echo ****
echo **** DO NOT attempt to change.
echo ****
echo *****
echo.
echo.
echo.
a:\sysinfo\sysinfo /rep:a:\rcv_data\sysinfo.dat
a:
```

### Disk #3 - Contents Of The Config.Sys File

```
devicehigh=a:\dos\himem.sys /v
devicehigh=a:\dos\emm386.exe noems
devicehigh=a:\dos\ansi.sys
dos=high,umb
files=30
fcbs=4,0
stacks=9,256
buffers=40
lastdrive=z
shell=a:\command.com /p /e:1024
numlock=off
```

### Disk #4, #5, and #6 - Contents Of The Autoexec.bat File

**NOTE:** For disks #5, and #6, the file is the same except for line 16 and 17. Those lines must be changed to identify the particular device loaded by the config.sys file.

```
@echo off
prompt=$e[1;37;44m$p$g
@echo on
cls
@echo off
a:\wrblk
echo.
echo.
echo This machine is booting from the 3 1/2" diskette.
echo.
echo.
echo ATTENTION:
echo.
echo This is the Control Boot Disk for NON-COMPRESSED drives.
echo.
```



# Computer Investigative Specialists Forms

echo This disk also loads drivers for the Pinnacle APEX Optical Hard Drive  
 echo using the Adaptec Mini-SCSI (SCSI to Parallel) cable.  
 echo.

echo These drivers will not properly load other devices.  
 echo.

pause  
 lh /L:0;1,45456 /S a:\dos\smartdrv.exe /X  
 cls

```

echo *****
echo ***** DO NOT *****
echo ***** TOUCH OR OPERATE THIS EQUIPMENT *****
echo ***** THIS COMPUTER MAY CONTAIN EVIDENCE *****
echo *****
echo ***** The PC is booting from a 3 1/2" Diskette *****
echo *****
echo ***** Name of CIS Agent *****
echo ***** Title *****
echo ***** Title 2 *****
echo ***** Agency and Office *****
echo ***** Office Address *****
echo ***** Voice - (XXX) XXX-XXXX Pager - (XXX) XXX-XXXX *****
echo *****
echo *****
echo ***** DO NOT ATTEMPT TO USE THIS EQUIPMENT WITHOUT *****
echo ***** DIRECT AUTHORIZATION OF THE *****
echo ***** ABOVE LISTED CIS AGENT *****
echo *****
echo ***** DO NOT *****
echo ***** TOUCH OR OPERATE THIS EQUIPMENT *****
echo ***** THIS EQUIPMENT MAY CONTAIN EVIDENCE *****
echo *****
pause
  
```

```

cls
lh a:\mouse\mouse.exe
lh a:\dos\doskey /insert
set temp=a:\temp
set tmp=a:\temp
set nu=a:\temp
cls
  
```

```

echo.
echo.
echo.
date < a:\cr.txt
echo.
echo.
time < a:\cr.txt
echo.
echo *****
echo *****
echo ***** NOTE: Record the above listed dates and times. *****
echo ***** These are the system clock settings *****
echo ***** on the target machine. *****
echo *****
echo ***** DO NOT attempt to change. *****
echo *****
  
```



# Computer Investigative Specialists Forms

```

echo *****
echo.
echo.
echo.
a:\sysinfo\sysinfo /rep:a:\rcv_data\sysinfo.dat
a:

```

## Disk #4, #5, and #6 - Contents Of The Config.Sys File (See Note Below)

```

devicehigh=a:\dos\himem.sys /v
devicehigh=a:\dos\emm386.exe noems
devicehigh=a:\dos\ansi.sys
dos=high,umb
files=30
fcbs=4,0
stacks=9,256
buffers=8
rem The buffers statement is set to "buffers=8" to
rem enhance the operation of SafeBack Master.
lastdrive=z
shell=a:\command.com /p /e:1024
numlock=off

```

```

device=a:\apex\ma358.sys
device=a:\apex\aspidisk.sys

```

rem The device drivers called above will load a Pinnacle APEX drive using an  
rem ADAPTEC Mini-SCSI (SCSI to Parallel) cable.

### NOTE:

For disks #5, and #6, the first thirteen (13) lines of the above file remains the same for the config.sys file. The remaining lines (device drivers and "rem" statements) are changed to fit the particular device loaded.

### Device Drivers for Disk #5

```

device=a:\hd45qd\h45hd.sys
device=a:\hd45qd\aspihd.sys

```

### Device Drivers for Disk #6

```

device=a:\adc2940w\aspi8dos.sys
device=a:\adc2940w\aspidisk.sys

```

### Summary of Files on Control Disks:

#### Control Disk 1:

```

DOS          <DIR>      08/12/97   5:15p
TEMP        <DIR>      08/12/97   5:16p
WRBLK      RPL          99 08/21/97   3:57a
COMMAND    COM      54645 05/31/94   6:22a
AUTOEXEC   BAT      1498 08/17/97  12:39p
CONFIG     SYS        105 08/13/97  11:49a
CR         TXT          4 08/12/97   5:36p
Directory of A:\DOS
ATTRIB     EXE      11208 05/31/94   6:22a
CHKDSK     EXE      12241 05/31/94   6:22a

```



## Computer Investigative Specialists Forms

```
EDIT      COM      413 05/31/94   6:22a
FDISK     EXE     29336 05/31/94   6:22a
QBASIC    EXE     194309 05/31/94   6:22a
TREE      COM      6945 05/31/94   6:22a
XCOPY     EXE     16930 05/31/94   6:22a
Directory of A:\TEMP
```

### Control Disk 2:

```
DOS       <DIR>      08/12/97   5:15p
TEMP      <DIR>      08/12/97   5:16p
COMMAND   COM      54645 05/31/94   6:22a
CONFIG    SYS      187 08/13/97   1:06p
AUTOEXEC  BAT      1491 08/13/97  11:48a
CR        TXT       4 08/12/97   5:36p
WRBLK     RPL       99 08/21/97   3:57a
```

Directory of A:\DOS

```
ATTRIB    EXE     11208 05/31/94   6:22a
CHKDSK    EXE     12241 05/31/94   6:22a
EDIT      COM      413 05/31/94   6:22a
FDISK     EXE     29336 05/31/94   6:22a
QBASIC    EXE     194309 05/31/94   6:22a
TREE      COM      6945 05/31/94   6:22a
XCOPY     EXE     16930 05/31/94   6:22a
HIMEM     SYS     29136 05/31/94   6:22a
EMM386    EXE     120926 05/31/94   6:22a
```

Directory of A:\TEMP

### Control Disk 3:

```
DOS       <DIR>      08/12/97   5:15p
MOUSE     <DIR>      08/12/97   5:16p
TEMP      <DIR>      08/12/97   5:16p
SYSINFO   <DIR>      08/12/97   5:21p
RCV_DATA  <DIR>      08/12/97   5:23p
WRBLK     RPL       99 08/21/97   3:57a
AUTOEXEC  BAT     3061 08/17/97   4:45p
COMMAND   COM     54645 05/31/94   6:22a
CONFIG    SYS     218 08/12/97   5:35p
CR        TXT       4 08/12/97   5:36p
CRC       EXE     15877 07/25/94   8:49p
```

Directory of A:\DOS

```
ANSI      SYS     9065 05/31/94   6:22a
ATTRIB    EXE     11208 05/31/94   6:22a
CHKDSK    EXE     12241 05/31/94   6:22a
EDIT      COM      413 05/31/94   6:22a
EMM386    EXE     120926 05/31/94   6:22a
FDISK     EXE     29336 05/31/94   6:22a
HIMEM     SYS     29136 05/31/94   6:22a
QBASIC    EXE     194309 05/31/94   6:22a
SMARTDRV  EXE     45145 05/31/94   6:22a
TREE      COM      6945 05/31/94   6:22a
XCOPY     EXE     16930 05/31/94   6:22a
DOSKEY    COM     5861 05/31/94   6:22a
```

Directory of A:\MOUSE

```
MOUSE     DRV     11872 07/28/93   9:01a
MOUSE     EXE     93166 07/28/93   9:01a
MOUSE     INI     1270 09/24/96   1:10a
```

Directory of A:\RCV\_DATA

Directory of A:\SYSINFO

```
SYSINFO   EXE     96604 05/18/94   8:00a
NLIB200   RTL     200650 05/18/94   8:00a
```

Directory of A:\TEMP



## Computer Investigative Specialists Forms

### Control Disk 4:

```
Directory of A:\
DOS                <DIR>      08/12/97    5:15p
MOUSE              <DIR>      08/12/97    5:16p
TEMP              <DIR>      08/12/97    5:16p
SYSINFO           <DIR>      08/12/97    5:21p
RCV_DATA          <DIR>      08/12/97    5:23p
APEX              <DIR>      08/14/97    7:26a
WRBLK    RPL      99 08/21/97    3:57a
COMMAND  COM      54645 05/31/94    6:22a
AUTOEXEC BAT     3276 08/18/97    1:12p
CONFIG   SYS      404 08/14/97   10:52a
CR       TXT       4 08/12/97    5:36p
MASTER  RPL      157 08/21/97    4:26a
CRC     EXE     15877 07/25/94    8:49p
Directory of A:\APEX
ASPIDISK SYS     15054 11/11/96    4:01a
MA358    SYS     12316 11/11/96    4:01a
Directory of A:\DOS
ANSI     SYS      9065 05/31/94    6:22a
ATTRIB  EXE     11208 05/31/94    6:22a
CHKDSK  EXE     12241 05/31/94    6:22a
EDIT    COM      413 05/31/94    6:22a
EMM386  EXE    120926 05/31/94    6:22a
FDISK   EXE     29336 05/31/94    6:22a
HIMEM   SYS     29136 05/31/94    6:22a
QBASIC  EXE    194309 05/31/94    6:22a
SMARTDRV EXE    45145 05/31/94    6:22a
TREE    COM      6945 05/31/94    6:22a
XCOPY   EXE     16930 05/31/94    6:22a
DOSKEY  COM      5861 05/31/94    6:22a
Directory of A:\MOUSE
MOUSE    DRV     11872 07/28/93    9:01a
MOUSE    EXE     93166 07/28/93    9:01a
MOUSE    INI      1270 09/24/96    1:10a
Directory of A:\RCV_DATA
Directory of A:\SYSINFO
SYSINFO  EXE     96604 05/18/94    8:00a
NLIB200  RTL    200650 05/18/94    8:00a
Directory of A:\TEMP
```

### Control Disk 5:

```
Directory of A:\
DOS                <DIR>      08/12/97    5:15p
MOUSE              <DIR>      08/12/97    5:16p
TEMP              <DIR>      08/12/97    5:16p
SYSINFO           <DIR>      08/12/97    5:21p
RCV_DATA          <DIR>      08/12/97    5:23p
HD45QD           <DIR>      08/14/97    7:26a
WRBLK    RPL      99 08/21/97    3:57a
COMMAND  COM      54645 05/31/94    6:22a
AUTOEXEC BAT     3307 08/18/97    1:31p
CONFIG   SYS      422 08/14/97    1:32p
CR       TXT       4 08/12/97    5:36p
MASTER  RPL      157 08/21/97    4:26a
CRC     EXE     15877 07/25/94    8:49p
Directory of A:\DOS
ANSI     SYS      9065 05/31/94    6:22a
ATTRIB  EXE     11208 05/31/94    6:22a
```



## Computer Investigative Specialists Forms

CHKDSK	EXE	12241	05/31/94	6:22a
EDIT	COM	413	05/31/94	6:22a
EMM386	EXE	120926	05/31/94	6:22a
FDISK	EXE	29336	05/31/94	6:22a
HIMEM	SYS	29136	05/31/94	6:22a
QBASIC	EXE	194309	05/31/94	6:22a
SMARTDRV	EXE	45145	05/31/94	6:22a
TREE	COM	6945	05/31/94	6:22a
XCOPY	EXE	16930	05/31/94	6:22a
DOSKEY	COM	5861	05/31/94	6:22a

```
.. <DIR> 08/14/97 7:26a
ASPIHD SYS 17270 03/06/97 4:07p
H45HD SYS 56678 03/07/97 5:29p
4 file(s) 73948 bytes
```

Directory of A:\MOUSE

MOUSE	DRV	11872	07/28/93	9:01a
MOUSE	EXE	93166	07/28/93	9:01a
MOUSE	INI	1270	09/24/96	1:10a

Directory of A:\RCV\_DATA

Directory of A:\SYSINFO

SYSINFO	EXE	96604	05/18/94	8:00a
NLIB200	RTL	200650	05/18/94	8:00a

Directory of A:\TEMP

### Control Disk 6:

Directory of A:\

DOS	<DIR>		06/09/97	7:47p
IOMEGA	<DIR>		06/09/97	7:47p
TEMP	<DIR>		06/09/97	7:47p
MOUSE	<DIR>		06/10/97	10:25a
AUTOEXEC	BAT	3201	08/18/97	9:23a
COMMAND	COM	54645	05/31/94	6:22a
CR	TXT	4	06/10/97	7:30p
CONFIG	SYS	868	08/18/97	8:20a
README	TXT	453	08/18/97	10:34a
CRC	EXE	15877	07/25/94	8:49p
WRBLK	RPL	99	08/21/97	3:57a
MASTER	RPL	157	08/21/97	4:26a

Directory of A:\DOS

EMM386	EXE	120926	05/31/94	6:22a
SMARTDRV	EXE	45145	05/31/94	6:22a
HIMEM	SYS	29136	05/31/94	6:22a
FDISK	EXE	29336	05/31/94	6:22a
CHKDSK	EXE	12241	05/31/94	6:22a
XCOPY	EXE	16930	05/31/94	6:22a
ANSI	SYS	9065	05/31/94	6:22a
EDIT	COM	413	05/31/94	6:22a
QBASIC	EXE	194309	05/31/94	6:22a
DOSKEY	COM	5861	05/31/94	6:22a
TREE	COM	6945	05/31/94	6:22a
ATTRIB	EXE	11208	05/31/94	6:22a

Directory of A:\IOMEGA

SCSICFG	EXE	36461	11/03/95	3:03a
SCSIDRVR	SYS	67978	11/03/95	3:03a
D_ASPI	OP	361	11/03/95	3:03a
NIBBLE	ILM	1429	11/03/95	3:03a
D_ASPI	AT	4679	11/03/95	3:03a
ASPIPPM1	SYS	22575	11/03/95	3:03a
D_FLOP	DT	8349	11/03/95	3:03a



## Computer Investigative Specialists Forms

---

D_FLOP	OP	377	11/03/95	3:03a
D_GEN	DT	9784	11/03/95	3:03a
D_IBMHBA	AT	5425	11/03/95	3:03a
D_IBMHBA	OP	391	11/03/95	3:03a
D_IDE	AT	10028	11/03/95	3:03a
D_IDE	OP	401	11/03/95	3:03a
D_IHA90	AT	4663	11/03/95	3:03a
D_IHA90	OP	401	11/03/95	3:03a
D_ISDASD	DT	2653	11/03/95	3:03a
D_ISDASD	OP	482	11/03/95	3:03a
D_PPA	AT	3606	11/03/95	3:03a
D_PPA	OP	536	11/03/95	3:03a
SCSI	SCF	369	08/18/97	9:04a
ASPIPC16	SYS	21045	11/03/95	3:03a
Directory of A:\MOUSE				
MOUSE	EXE	93166	07/28/93	9:01a
MOUSE	INI	1270	09/24/96	1:10a
MOUSE	DRV	11872	07/28/93	9:01a
Directory of A:\TEMP				



## Computer Investigative Specialists Forms

### Alternative Boot Disks

I personally use a somewhat modified version of the above described boot disks. I carry three control disks:

- 622 Sterile Control Disk ( will not boot a dblspace drive)
- 622 Control Disk (will boot a dblespace drive)
- 95B Control Disk (with msdos.sys modified to boot to DOS Command Prompt only)

The balance of my utility disks are very similar to the disks described in the previous section. I use a MD5 HASH computation instead of the 32 bit CRC computation. I also carry Norton Diskedit 95 and Norton Unerase 95 on a utility disk in case I need to look at LFN directory areas on a 95 machine.

Following are summaries of the following:

- **Autoexec.bat on DOS622 and Win95B Control Diskettes**
- **Config.sys on DOS622 and Win95B Control Diskettes**
- **Files on DOS622 Control Diskettes**
- **Msdos.sys on Windows 95B Control Diskette**
- **Files on Win95B Control Diskette**

#### Summary of Autoexec.bat on DOS 622 and WIN95B Control Diskettes:

```
a:\wrblk /a
pause
prompt=3H622_1S $p$g    Note: Prompt will show computer booted from 3.5" High Density Control Disk 1S
path=a:\
@echo on
cls
@echo off
rem LH /L:0;1,45456 /S a:\smartdrv.exe /X /V
rem A:\SMARTDRV.EXE
rem a:\mouse.exe
a:\doskey /insert
set temp=a:\temp
set tmp=a:\temp
set nu=a:\temp

if %config%==cd_acer goto acer
if %config%==cd_atapi goto atapi
if %config%==cd_adap goto adap
if %config%==SCSI3_358 goto adaptec
if %config%==SCSI4_358 goto adaptec
if %config%==SCSI5_358 goto adaptec
if %config%==SCSI6_358 goto adaptec
if %config%==H45_aspidisk goto adaptec
if %config%==aspi2 goto adaptec
if %config%==aspi4 goto adaptec
if %config%==aspi8 goto adaptec
```



## Computer Investigative Specialists Forms

```
if %config%==mcam goto adaptec
if %config%==358_guest goto guest
if %config%==H45_guest goto guest
if %config%==as4_guest goto guest
if %config%==as8_guest goto guest
if %config%==mcam_guest goto guest
if %config%==sigg_guest goto guest
if %config%==ZIP_PAR goto guest
goto finish

:adap
mscdex aspicd /d:aspi_cd /L:M
goto finish

:atapi
A:\MSCDEX.EXE /D:mscd000 /V /M:12 /L:M
goto finish

:acer
a:mscdex /S /d:mtmide01 /m:10 /L:M
goto finish

:adaptec
if exist C:\SCERS.TXT SUBST Q: C:\
if exist D:\SCERS.TXT SUBST Q: D:\
if exist E:\SCERS.TXT SUBST Q: E:\
if exist F:\SCERS.TXT SUBST Q: F:\
if exist G:\SCERS.TXT SUBST Q: G:\
if exist H:\SCERS.TXT SUBST Q: H:\
if exist I:\SCERS.TXT SUBST Q: I:\
if exist J:\SCERS.TXT SUBST Q: J:\
if exist K:\SCERS.TXT SUBST Q: K:\
if exist L:\SCERS.TXT SUBST Q: L:\
if exist M:\SCERS.TXT SUBST Q: M:\
if exist N:\SCERS.TXT SUBST Q: N:\
set comspec=q:\dos622\command.com
path=q:;q:\DOS622;q:\win311;q:\util;q:\scers;q:\nc5;q:\nu
goto finish

:guest
a:\guest\guest letter=q
set comspec=q:\dos622\command.com
path=q:;q:\DOS622;q:\win311;q:\util;q:\scers;q:\nc5;q:\nu
goto finish

:finish
cls
```



# Computer Investigative Specialists Forms

```

echo *****
echo *****
echo ***** DO NOT *****
echo ***** TOUCH OR OPERATE THIS EQUIPMENT *****
echo ***** THIS COMPUTER MAY CONTAIN EVIDENCE *****
echo *****
echo ***** The PC is booting from a 3 1/2" Diskette *****
echo *****
echo ***** David P Messinger *****
echo ***** Special Agent *****
echo ***** US Treasury - IRS *****
echo ***** 600 17th Street, 15th Floor North *****
echo ***** Denver, Colorado 80202 *****
echo ***** Voice - (303) 446-1851 Pager - (303) 446-1851 *****
echo *****
echo *****
echo ***** DO NOT ATTEMPT TO USE THIS EQUIPMENT WITHOUT *****
echo ***** DIRECT AUTHORIZATION OF THE *****
echo ***** ABOVE LISTED SCERS AGENT *****
echo *****
echo ***** DO NOT *****
echo ***** TOUCH OR OPERATE THIS EQUIPMENT *****
echo ***** THIS EQUIPMENT MAY CONTAIN EVIDENCE *****
echo *****
pause

```

```

cls
echo.
echo.
echo.
date < a:\cr.txt
echo.
time < a:\cr.txt
echo.

```

```

echo *****
echo ***** Using Original Media Worksheet .... *****
echo ***** *****
echo ***** Record the above listed dates and times. *****
echo ***** These are the system clock settings *****
echo ***** on the target machine. *****
echo ***** *****
echo ***** DO NOT attempt to change. *****
echo ***** *****
echo ***** If using GUEST - Drive is letter "Q:" *****
echo ***** If using CD - CD drive letter "M:" *****
echo *****
echo.
echo.

```



## Computer Investigative Specialists Forms

```
echo.
PAUSE
CLS
echo.
echo.
echo.
echo.
echo *****
echo ****   Use Original Media Worksheet.....   ****
echo ****           ****
echo ****   Look at Disk using Norton Commander           ****
echo ****   Also check disk size using Direct Option on Safeback ****
echo ****   Run DISKINFO BAT for each drive           ****
echo ****   CRC the files on all drives           ****
echo ****   Image the disk using Safeback           ****
echo ****           ****
echo ****   Document condition of machine using Norton SI.EXE ****
echo ****   (System Information Program)           ****
echo ****           ****
echo ****   If using Removeable media - Drive is letter "Q" ****
echo ****   unless SCER.TXT is not in root of removeable media ****
echo *****
echo.
echo.

:end
```

### Summary of CONFIG.SYS on DOS Control Diskettes:

```
[MENU]
MENUITEM=VANILLA NO DRIVERS - A: boot only
SUBMENU=AHA358 358 MiniSCSI PPA
SUBMENU=H45 H45 SHUTTLE
SUBMENU=Guest_DRV Iomega GUEST drivers / ZIP & QUICK DRIVE Menu
MENUITEM=aspi4 aspi4dos - 1542 ISA SCSI cards
MENUITEM=aspi8 aspi8dos - 2940W & 7880 PCI SCSI cards
MENUITEM=mcam mcaml8xx - 2920 PCI SCSI cards
MENUITEM=siig aspiedos - SiiG PCI SCSI cards
submenu=CD CD Drivers
MENUITEM=1460 1460 PCMCIA card - aspi2dos

[CD]
menuitem cd_adap Adaptec CD
menuitem cd_atapi Atapi CD - ie, vectra
menuitem cd_acer Acer MTMCDAI.sys

[cd_adap]
device=a:\adaptec\aspicd.sys

[cd_atapi]
rem - atapi ide drive
Devicehigh=A:\cd\ATAPI_CD.SYS /D:mscd000 /i:0
```



## Computer Investigative Specialists Forms

```
[cd_acer]
rem atapi ide drive ??
DEVICEhigh=a:\cd\MTMCDAI.SYS /D:MTMIDE01

[GUEST_DRV]
MENUITEM=ZIP_PAR Parallel Port Zip using Guest
MENUITEM=as4_guest aspi4dos - 1542 ISA SCSI cards
MENUITEM=as8_guest aspi8dos - 2940W & 7880 PCI SCSI cards
MENUITEM=mcam_guest mcam18xx - 2920 PCI SCSI cards
MENUITEM=siig_guest aspiedos - Siig PCI SCSI card
MENUITEM=h45QD H45 Quick Drive

[H45]
MENUITEM=H45_guest SHUTTLE using GUEST->Q: (epst v4.44/guest v4.12)
MENUITEM=H45_aspi SHUTTLE using ASPIDISK (epst v4.44/aspdisk v4.01)
MENUITEM=H45_hdrm SHUTTLE using HDRM (epst v4.44/hdrm v3.51)
MENUITEM=H45_cdaspi SHUTTLE with CD using ASPIDISK (epst v4.44/aspdisk v4.01)
MENUITEM=H45_cdhdrm SHUTTLE with CD using ASPIHDRM (epst v4.44/hdrm v3.51)

[AHA358]
MENUITEM=358_guest, 358 MiniSCSI using GUEST->Q: (ma358 v3.10/guest v4.12)
menuitem=SCSI3_358, 358 MiniSCSI w/aspdisk - full handshaking (Default)
menuitem=SCSI4_358, 358 MiniSCSI w/aspdisk - Force Non-EPP;autodetect
uni/bidirectional
menuitem=SCSI5_358, 358 MiniSCSI w/aspdisk - Force Non-EPP and Force
unidirectional
menuitem=SCSI6_358, 358 MiniSCSI w/aspdisk - Force EPP

[COMMON]
shell=a:\command.com /p /e:1024
devicehigh=a:\himem.sys /v
devicehigh a:\emm386.exe noems
rem devicehigh=a:\ansi.sys
dos=high,umb
files=30
fcbs=4,0
stacks=9,256
buffers=8
lastdrive=z
numlock=off
rem break=on

[VANILLA]

[SCSI3_358]
DEVICEhigh=A:\adaptec\MA358.SYS
DEVICEhigh=A:\adaptec\ASPIDISK.SYS

[SCSI4_358]
DEVICEhigh=A:\adaptec\MA358.SYS /M04
DEVICEhigh=A:\adaptec\ASPIDISK.SYS

[SCSI5_358]
DEVICEhigh=A:\adaptec\MA358.SYS /M06
DEVICEhigh=A:\adaptec\ASPIDISK.SYS

[SCSI6_358]
DEVICEhigh=A:\adaptec\MA358.SYS /M08
DEVICEhigh=A:\adaptec\ASPIDISK.SYS
```



## Computer Investigative Specialists Forms

```
[358_guest]
rem Device=a:\adaptec\MA358ibm.sys /M07
Device=a:\adaptec\MA358.sys
```

```
[mcam_guest]
devicehigh=a:\adaptec\mcaml8xx.sys
```

```
[H45_guest]
device=a:\h45\epst.sys
```

```
[H45_aspi]
device=a:\h45\epst.sys
device=a:\adaptec\aspidisk.sys
```

```
[h45_hdrm]
device=a:\h45\epst.sys
device=a:\h45\aspihdrm.sys
```

```
[h45_cdaspi]
device=a:\h45\epst.sys
device=a:\adaptec\aspidisk.sys
device=a:\h45\aspicd.sys
```

```
[h45_cdhdrm]
device=a:\h45\epst.sys
device=a:\h45\aspihdrm.sys
device=a:\h45\aspicd.sys
```

```
[H45QD]
device=a:\h45\h45hd.sys
device=a:\h45\aspihd.sys
```

```
[aspi2]
devicehigh=a:\adaptec\aspi2dos.sys
device=a:\adaptec\aspidisk.sys
```

```
[aspi4]
devicehigh=a:\adaptec\aspi4dos.sys /D
rem /P334
device=a:\adaptec\aspidisk.sys
```

```
[mcam]
devicehigh=a:\adaptec\mcaml8xx.sys
device=a:\adaptec\aspidisk.sys
device=a:\adaptec\aspicd.sys
```

```
[aspi8]
devicehigh=a:\adaptec\aspi8dos.sys /d
device=a:\adaptec\aspidisk.sys
device=a:\adaptec\aspicd.sys
```

```
[siig]
devicehigh=a:\adaptec\advaspi.sys
devicehigh=a:\adaptec\aspidisk.sys
```

```
[siig_guest]
devicehigh=a:\adaptec\advaspi.sys
```

```
[as2_guest]
devicehigh=a:\adaptec\aspi2dos.sys
```



## Computer Investigative Specialists Forms

```
[as4_guest]
devicehigh=a:\adaptec\aspi4dos.sys /d

[as8_guest]
devicehigh=a:\adaptec\aspi8dos.sys

[aspimtm]
devicehigh=a:\adaptec\advaspi.sys
rem- next for cdrom
rem devicehigh=a:\adaptec\mtmcdai.sys

[zip_h45]
device=a:\h45\epst.sys
devicehigh=a:\guest\aspi16.sys
devicehigh=a:\guest\aspi16.sys file=nibble.ilm speed=10
devicehigh=a:\guest\scsicfg.exe
devicehigh=a:\guest\scsidrvr.sys

[zip_358]
rem Device=a:\adaptec\MA358ibm.sys /M07
Device=a:\adaptec\MA358.sys
devicehigh=a:\guest\aspi16.sys
devicehigh=a:\guest\aspi16.sys file=nibble.ilm speed=10
devicehigh=a:\guest\scsicfg.exe
devicehigh=a:\guest\scsidrvr.sys
```

### Files that are on Alternative Control Disk

#### Files that are on Control Disk 3H622\_1 (S and C)

```
Directory of A:\
VTREE      COM           512  12-10-85  2:54p  VTREE.COM
ADAPTEC    <DIR>             10-28-97  8:40a  ADAPTEC
GUEST      <DIR>             10-28-97  8:40a  GUEST
H45        <DIR>             10-28-97  8:41a  H45
TMP        <DIR>             05-29-98  2:11p  TMP
TEMP       <DIR>             10-28-97  8:41a  TEMP
CD         <DIR>             05-29-98  2:14p  CD
MSCDEX     EXE             25,361  05-31-94  6:22a  MSCDEX.EXE
COMMAND    COM             54,645  05-31-94  6:22a  COMMAND.COM
CR         TXT              4       06-10-97  7:30p  CR.TXT
TREE       COM             6,945  05-31-94  6:22a  TREE.COM
DOSKEY     COM             5,861  05-31-94  6:22a  DOSKEY.COM
EMM386     EXE            120,926  05-31-94  6:22a  EMM386.EXE
HIMEM      SYS             29,136  05-31-94  6:22a  HIMEM.SYS
NC         INI              1,592  09-12-97  7:56a  NC.INI
NTFSDOS    EXE             46,393  02-06-97  11:08p  NTFSDOS.EXE
NTFSHLP    VXD             8,812  09-10-96  9:50p  NTFSHLP.VXD
PATHQ      BAT              58     10-02-97  4:33p  PATHQ.BAT
PRINT      EXE            15,656  05-31-94  6:22a  PRINT.EXE
PRN2FILE   COM             1,386  06-01-88  12:00p  PRN2FILE.COM
FDISK      EXE             29,336  05-31-94  6:22a  FDISK.EXE
SMARTDRV   EXE            45,145  05-31-94  6:22a  SMARTDRV.EXE
SUBST      EXE            18,526  05-31-94  5:22a  SUBST.EXE
WRBLK      EXE            10,358  09-17-97  11:16a  WRBLK.EXE
FORMAT     COM            22,974  05-31-94  6:22a  FORMAT.COM
SYS        COM              9,432  05-31-94  6:22a  SYS.COM
DISKINFO   BAT             1,248  09-17-97  10:37a  DISKINFO.BAT
```



## Computer Investigative Specialists Forms

```
CHKDSK   EXE           12,241  05-31-94  6:22a  CHKDSK.EXE
EW       EXE          115,048  07-06-98  1:19p  ew.exe
AUTOEXEC BAT           5,843  06-15-98  8:50a  AUTOEXEC.BAT
CONFIG  SYS           5,359  10-22-98  11:12a  CONFIG.SYS
        25 file(s)          592,797 bytes
```

Directory of A:\ADAPTEC - These are drivers for SCSI cards and SCSI parallel port cable

```
.          <DIR>           10-28-97  8:40a  .
..         <DIR>           10-28-97  8:40a  ..
MA358     SYS          12,316  11-11-96  4:01a  MA358.SYS
ASPIDISK  SYS          15,054  11-11-96  4:01a  ASPIDISK.SYS
ASPI2DOS  SYS          29,262  09-15-95  12:00a  ASPI2DOS.SYS
ASPI4DOS  SYS          14,314  11-11-96  4:01a  ASPI4DOS.SYS
ASPI7DOS  SYS          36,160  09-15-95  12:00a  ASPI7DOS.SYS
ASPI8DOS  SYS          36,756  11-21-96  5:20a  ASPI8DOS.SYS
ASPICD    SYS          29,564  09-15-95  12:00a  ASPICD.SYS
MTMCDAI   SYS          14,454  04-20-95  1:33a  MTMCDAI.SYS
MTMCDAI   386           5,449  02-23-95  1:20a  MTMCDAI.386
ASPIEDOS  SYS          10,704  06-10-94  1:31a  ASPIEDOS.SYS
MCAM18XX  SYS          19,872  11-11-96  4:01a  MCAM18XX.SYS
ADVASPI   SYS          53,654  04-23-96  9:04a  ADVASPI.SYS
        12 file(s)          277,559 bytes
```

Directory of A:\CD

```
.          <DIR>           05-29-98  2:14p  .
..         <DIR>           05-29-98  2:14p  ..
ATAPI_CD  SYS          15,022  03-16-95  2:10a  ATAPI_CD.SYS
MTMCDAI   386           5,449  02-23-95  1:20a  MTMCDAI.386
MTMCDAI   SYS          14,454  04-20-95  1:33a  MTMCDAI.SYS
        3 file(s)          34,925 bytes
```

Directory of A:\GUEST

```
.          <DIR>           10-28-97  8:40a  .
..         <DIR>           10-28-97  8:40a  ..
GUEST     EXE          31,948  11-21-96  5:20a  GUEST.EXE
ASPI1616  SYS          19,210  11-21-96  5:20a  ASPI1616.SYS
ASPI2930  SYS          23,804  06-04-96  5:00a  ASPI2930.SYS
ASPIIDE   SYS          23,098  11-21-96  5:20a  ASPIIDE.SYS
ASPIPC16  SYS          23,103  11-21-96  5:20a  ASPIPC16.SYS
ASPIPPM1  SYS          23,089  11-21-96  5:20a  ASPIPPM1.SYS
ASPIPPM2  SYS          25,957  11-21-96  5:20a  ASPIPPM2.SYS
ASPIPPA3  SYS          22,679  06-21-95  3:02a  ASPIPPA3.SYS
GUEST     INI             280    06-21-95  3:02a  GUEST.INI
ASPIPC2   SYS          16,866  06-04-96  5:00a  ASPIPC2.SYS
ASPIPC4   SYS          22,518  06-04-96  5:00a  ASPIPC4.SYS
ASPIPC8   SYS          17,974  06-04-96  5:00a  ASPIPC8.SYS
        12 file(s)          250,526 bytes
```

Directory of A:\H45 - these are drivers for the H45 parallel port cable

```
.          <DIR>           10-28-97  8:41a  .
..         <DIR>           10-28-97  8:41a  ..
ASPIHDMR  SYS          15,809  10-18-96  9:38a  ASPIHDMR.SYS
EPST      SYS          56,022  10-18-96  9:38a  EPST.SYS
ASPICD    EXE          20,588  09-12-96  7:25p  ASPICD.EXE
ASPICD    SYS          19,434  09-12-96  7:25p  ASPICD.SYS
ASPIHDMR  EXE          17,963  09-12-96  7:26p  ASPIHDMR.EXE
```







## Computer Investigative Specialists Forms

```
.. <DIR> 06-15-98 9:52a ..
GUEST EXE 31,948 11-21-96 5:20a GUEST.EXE
ASPI1616 SYS 19,210 11-21-96 5:20a ASPI1616.SYS
ASPI2930 SYS 23,804 06-04-96 5:00a ASPI2930.SYS
ASPIIDE SYS 23,098 11-21-96 5:20a ASPIIDE.SYS
ASPIPC16 SYS 23,103 11-21-96 5:20a ASPIPC16.SYS
ASPIPPM1 SYS 23,089 11-21-96 5:20a ASPIPPM1.SYS
ASPIPPM2 SYS 25,957 11-21-96 5:20a ASPIPPM2.SYS
ASPIPPA3 SYS 22,679 06-21-95 3:02a ASPIPPA3.SYS
GUEST INI 280 06-21-95 3:02a GUEST.INI
ASPIPC2 SYS 16,866 06-04-96 5:00a ASPIPC2.SYS
ASPIPC4 SYS 22,518 06-04-96 5:00a ASPIPC4.SYS
ASPIPC8 SYS 17,974 06-04-96 5:00a ASPIPC8.SYS
12 file(s) 250,526 bytes
```

### Directory of A:\H45

```
. <DIR> 06-15-98 9:53a .
.. <DIR> 06-15-98 9:53a ..
ASPIHDRM SYS 15,809 10-18-96 9:38a ASPIHDRM.SYS
EPST SYS 56,022 10-18-96 9:38a EPST.SYS
ASPICD SYS 19,434 09-12-96 7:25p ASPICD.SYS
ASPIHD SYS 17,270 03-06-97 4:07p ASPIHD.SYS
H45HD SYS 56,678 03-07-97 5:29p H45HD.SYS
5 file(s) 165,213 bytes
```

### Directory of A:\TEMP

```
. <DIR> 06-15-98 10:22a .
.. <DIR> 06-15-98 10:22a ..
0 file(s) 0 bytes
```

### Directory of A:\TMP

```
. <DIR> 06-15-98 10:22a .
.. <DIR> 06-15-98 10:22a ..
0 file(s) 0 bytes
```

### Total files listed:

```
49 file(s) 1,208,871 bytes
18 dir(s) 19,456 bytes free
```



## Computer Investigative Specialists Forms

### Comments on other Software:

*Note: The following comments are extracted from 2DBF.PDF. 2DBF is a text conversion program that converts text captured using several popular law enforcement documentation and analysis programs into DB3 format databases and also creates several analysis reports. The program also creates several analysis summary reports based on file dates and file extensions. If you are interested in a copy of this program please send e-mail to Dave Messinger.*

**[EXCERPT...]** Today's computer crime investigator is faced with myriad of complexities in choosing analysis software. It's not that there is a multitude of available software - even though there is quite a choice - but it is choosing the right software for the job.

We are now faced with 32 bit FAT, 32X FAT and NTFS systems not recognized by DOS622, NTFS systems not recognizing FAT32, FAT32 not recognizing NTFS ... and who knows what is in store down the road. Some of our analysis programs won't work on FAT32, some will partially work, some will work but only if the GUI is loaded, and some will work only if DOS71 (no GUI) is loaded. Some programs support Long File Names (LFN) and the three system dates - others don't. And some are year 2000 compliant (Y2K) and some aren't.

Computers have gotten too large for us to do in-depth analysis of the entire haystack - unless really essential for the investigation and unless someone creates more hours in the day. As computer forensic investigators, we need summary tools to quickly draw an overall picture of how the computer was used (programs, data, address books, etc.) and then present that picture in a clear and concise form to assist other investigators and prosecuting attorneys to assist them in identifying whether and where more in-depth analysis may need to be performed.

All of the above has to be happen within the limitations of the evidentiary process, including search warrant limitations, if applicable.

Included in this manual are my observations of various analysis software (see Comments about Various Programs) and an explanation of my attempt to somewhat standardize my analysis process (see Appendix D-Summary Analysis).

I believe that as seized computer specialists, our mission is to:  
insure that electronic evidence is properly and legally accessed and preserved  
analyze and summarize (report) the contents contained within the computer so that we (as investigators), other investigators responsible for the case (generally not us), and the prosecuting attorneys have an understanding of what is on the computer and how it was used.  
authenticate the evidence for court presentation

Being successful in court is the bottom line. Prosecuting attorneys need to understand the volume of information they could be dealing with and the importance of providing full discovery when it comes to electronic evidence - since it is nearly impossible to know every needle in that electronic haystack of needles. Even if only a few pieces of electronic evidence is being presented, the defense may have a right to review all the electronic evidence, and the prosecuting attorney needs to be able to make that decision knowledgeably.



## Computer Investigative Specialists Forms

My analysis approach is simple:

- Don't use analysis programs that you don't have a good basic understanding as to how they work (such as "proclaimed" fully automated analysis packages).
- Use a standard structured database to capture all the data so that you can optimize your report writers no matter what database program you are using.
- Do the analysis work yourself so you know what you have and can testify about it.

File Documentation Comments and Overview:

Where once I felt you only should run one file documentation program and use the output for documentation reports (sort of a one step does all), Long File Names, FAT 32 and other considerations have caused me to rethink this approach. Realizing that any comments made about various documentation programs will be outdated almost before the ink dries, here is my stab at describing my reasons for using various documentation programs. These program's nuances are described in greater detail in the "Comments on Various Program" section.

For initial file documentation performed on an original machine, I prefer FILELIST (NTI) since it gives you a 128 bit hash, long file names, erased files, can operate from a DOS or WIN95 non-GUI operating system, works on 32 bit fats and does not change the last date accessed. You can use CRC(32), but it will change the last date accessed in the directory area (if that is an important issue to you) on a Fat32 machine. And you don't get long file names. Also, the CRC is not as solid as a MD5 (128 bit) hash (see CRC, HASH, MD5 and SHA in Comments on Various Programs), HASH will not run out of a straight DOS 7.1 boot - needs to be run from inside a GUI DOS window.

Once restored (and lacking Filelist), I like Hash for file documentation and reports, particularly using the -w option. On restored 95 machines, I run the -hta option (no hash, all three dates & times) first (along with the -w option to widen the output file name field to 170 characters). I then will capture the hash values (this will change the last accessed date - hence the reason for doing the -hta option first). I don't like running Hash on 95 original machines if I don't have to - the GUI interface has to be running in order to do so - so you have to boot to GUI -I just prefer not to do that.

I have found that a handy report I sometimes like to review is a "date directory created" report - which gives me a good idea when programs were installed if I am trying to see how a machine was used and setup. Only RED and DIR capture "directory created dates". Although DIR has it's problems in capturing directory and file information located in or beneath hidden or system attributed directories (such as ...\\temporary internet files; ..\\recycle; ...\\recent), it does capture the directories long file name where RED does not (at least in a form that is convertible to a database) and for that reason I use DIR for capturing directory information and I don't worry about those few directories I miss.

If I want erased file documentation, FILELIST and RED both do a good job (you do get the deleted long file name with FILELIST). If I am really need to be looking at the data within the erased files (generally too time consuming and better served by a disk search), Norton Unerase with PRN2FILE loaded first is the better approach. Generally a search will lead me to where I need to look and I don't take the time to look at info inside deleted files, just document their names and inspect to see if anything attracts my attention..



## Computer Investigative Specialists Forms

---

As I see more and more files being zipped, I like documenting files contained within zipped files using pkunzip with the -v option and using the freeware sweep.com to automate recursive subdirectory searches.

If I need to look at headers, I prefer Mare's DISkCAT - although I do not examine headers that often - unless I have some suspicions. DISkCat does take a little work to configure it for all the files you may want to check the headers on - although there is a pretty good standard list. I keep hoping for someone to create the ultimate program - checks known CRC's against standard known files, checks for PGP, steganagraphy and encryption - all in one program.

Search programs are individual preferences. TXTSRCHP (NTI) probably is my favorite cause it runs on FAT32 logical drive (something that DiskSearch Mark II does not). RCMP's RED and DL and Mares' STRSRCH also work fine, although their output is more limited than TXTSRCHP and DiskSearch.