Forensic Examination of Digital Evidence: A Guide for Law Enforcement comprises public domain material from the U.S. Department of Justice. UMGC has modified this work.

Case brief 1 report

REPORT OF MEDIA ANALYSIS

MEMORANDUM FOR: County Sheriff's Police
Investigator Johnson
Anytown, USA 01234

SUBJECT: Forensic Media Analysis Report
SUBJECT: DOE, JOHN
Case Number: 012345

1. Status: Closed.

2. Summary of Findings:

- 327 files containing images of what appeared to be children depicted in a sexually explicit manner were recovered.
- 34 shortcut files that pointed to files on floppy disks with sexually explicit file names involving children were recovered.

3. Items Analyzed:

TAG NUMBER:	**ITEM DESCRIPTION:**
012345	One Generic laptop, Serial # 123456789

4. Details of Findings:

- Findings in this paragraph related to the Generic Hard Drive, Model ABCDE, Serial # 3456ABCD, recovered from Tag Number 012345, One Generic laptop, Serial # 123456789.

  1) The examined hard drive was found to contain a Microsoft® Windows® 98 operating system.

  2) The directory and file listing for the media was saved to the Microsoft® Access Database TAG012345.MDB.

  3) The directory C:\JOHN DOE\PERSONAL\FAV PICS\, was found to contain 327 files containing images of what appeared to be children depicted in a sexually explicit manner. The file directory for 327 files disclosed that the files' creation date and times are 5 July 2001 between 11:33 p.m. and 11:45 p.m., and the last access date for 326 files listed is 27 December 2001. In addition, the file directory information for one file disclosed the last access date as 6 January 2002.

  4) The directory C:\JOHN DOE\PERSONAL\FAV PICS TO DISK\ contained 34 shortcut files that pointed to files on floppy disks with sexually explicit file names involving children. The file directory information for the 34 shortcut files disclosed

the files' creation date and times are 5 July 2001 between 11:23 p.m. and 11:57 p.m., and the last access date for the 34 shortcut files was listed as 5 July 2001.

5) The directory C:\JOHN DOE\LEGAL\ contained five Microsoft® Word documents related to various contract relationships John Doe Roofing had with other entities.

6) The directory C:\JOHN DOE\JOHN DOE ROOFING\ contained files related to operation of John Doe Roofing.

7) No further user-created files were present on the media.

5. Glossary:

Shortcut File: A file created that links to another file.

6. Items Provided: In addition to this hard copy report, one compact disk (CD) was submitted with an electronic copy of this report. The report on CD contains hyperlinks to the above-mentioned files and directories.

IMA D. EXAMINER
Computer Forensic Examiner

Released by_____

Case brief 2 report

Department of State Police
Computer Crimes Unit
Computer Forensics Laboratory
7155-C Columbia Gateway Drive
Columbia, MD 21046
(410) 290-0000

April 19, 1999

MEMO TO FILE

FORENSIC EXAMINER PROCESSING NOTES: **SGT. David B. Smith (5555)**
FORENSIC CASE NUMBER: **99-03-333-A**

REQUESTER:	TFC. Brian Jones State Police Auto Theft Unit (310-288-8433)
OFFENSE:	Auto Theft, Forgery
CASE NUMBER:	01-39-00333
RECEIVED:	March 19, 1999
OPENED:	March 24, 1999
COMPLETED:	April 19, 1999
FORENSIC HOURS:	40 hours
OS EXAMINED:	Microsoft® Windows® 98
FILE SYSTEM:	[FAT32]
DATA ANALYZED:	7,782 MB

Evidence Description: Item 1: One Gateway Solo® 9100 Notebook Computer, Serial Number 555-Z3025-00-002-0433.

Action Taken:

March 24, 1999

1600 hours: I retrieved the original digital evidence from the CCU Property Room. I inventoried, marked, and cataloged the evidence described on the MSP Form 67. All original evidence listed on the Chain of Custody Form was accounted for.

1620 hours: I examined the Gateway Solo® 9100 notebook computer and completed an **Initial Computer Evidence Processing** form (see attached). The computer contained one fixed disk. The notebook case was not opened to expose the drive (Original Digital Evidence# hdd01). I inserted a controlled boot disk in the notebook computer floppy drive and powered on the computer. I pressed F1 to enter the setup utility. I documented the BIOS settings:

State Police - Computer Forensics Laboratory
Forensic Report - Laboratory Case Number 99-03-333-A

BIOS	System Date	System Time	Memory	Boot Order
Award 4.5 pg	3/24/1999	16:30:03	128 MB	Floppy Drive Hard Drive
	Actual Date 3/24/1999	Actual Time 16:30:08	CPU Intel PII 300	

EnCase® (1.998) (DOS Version 7.10)

1 Physical Disks					1 Logical Volumes				
Disk 0	Size 7.6GB		CHS 7480:16:63		LP	LABEL	SYSTEM	FREE	SIZE
Lock	Code	Type	Sectors	Size	C0	NONAME	FAT32	5.5GB	7.6GB
80	0B	FAT32	16,000,740	7.6GB					

Server Mode
Connected...!

En.exe was executed on the laboratory computer; EnCase® reported:

EnCase® (1.998) Client Mode (DOS Version 7.10)

1 Physical Disks					1 Logical Volumes				
Disk 0	Size 7.6GB		CHS 7480:16:63		LP	LABEL	SYSTEM	FREE	SIZE
Lock	Code	Type	Sectors	Size	C0	NONAME	FAT32	5.5GB	7.6GB
80	0B	FAT32	16,000,740	7.6GB					

State Police - Computer Forensics Laboratory
Forensic Report - Laboratory Case Number 99-03-333-A
3 of 6 Initials **DBS**

1750 hours: Acquisition of a compressed evidence file was started.

File Name & Path:	F:\hdd01
Case #:	01-39-00333
Examiner:	Sgt. David B. Smith
Evidence #:	99-03-333-A
Description:	555-Z3025-00-002-0433.

March 25, 1999

0900 hours: EnCase® reported: "An evidence file for drive 0 was successfully created . . . Elapsed Time 11:14:00, 7.6GB read, 0 errors, 11:14:00 elapsed, 0:00:00 remaining."

0910 hours: I exited EnCase® on the laboratory computer and returned to the A:\ prompt. The computer was powered off, the Sony MO disk containing the evidence files was removed from the MO drive unit and write protected and placed into evidence. A State Police Chain of Custody Form was completed.

March 30, 1999

1400 hours: The laboratory Gateway GX-450XL computer was equipped with a Sony MO drive unit connected to an AHA 2940UW SCSI adapter card. A controlled boot disk was placed in drive A:. The computer was powered on and the system booted to the A:\ prompt. The DOS copy command was used to copy the EnCase® evidence files from the Sony MO Dsk drive F: to "Data" hard drive, E:. The files were successfully copied. The computer was powered down and the Sony MO disk was returned to evidence.

April 1, 1999

0800 hours: The laboratory Gateway GX-450XL computer was booted to Windows® 98. EnCase® for Windows® 98 (version 1.999) was launched. I opened a new EnCase® case, titled *99-03-333-A*. I added the previously acquired evidence file into the case. EnCase® file Signatures was run.

0900 hours: I began a logical analysis of the data contained in the EnCase® case.

1000 hours: A data wiping utility was used to wipe removable drive I: on the laboratory Gateway GX-450XL computer. The drive was wiped to U.S. Department of Defense recommendations (DoD 5200.28-STD). Unallocated clusters and file slack from the evidence file space were then copied from the EnCase® case to drive I:. The files were divided into seven folders, each folder holding a maximum of 1,048MB. 575 files containing 5,944MB were copied.

State Police - Computer Forensics Laboratory
Forensic Report - Laboratory Case Number 99-03-333-A
4 of 6 Initials **DBS**

1220 hours: NCIS DIGit© [Version 1.08] was executed. The files that had been copied from the evidence file to drive I: were examined. The files included both unallocated clusters and file slack. 5,944MB of data were processed in seven (7) batches. DIGit© reported extracting:

Files Extracted From Unallocated Space
DIGit© (Version 1.08)

Batch	HITS	Jpg	Bmp	Gif	Tif	Pcx	HTML	Word8	Total Megs Examined
1	5,378	197	82	4,908	11	16	66	98	1,048
2	2,499	53	48	2,258	14	3	76	47	1,048
3	599	0	6	550	4	6	11	22	1,048
4	0	0	0	0	0	0	0	0	1,048
5	0	0	0	0	0	0	0	0	1,048
6	0	0	0	0	0	0	0	0	704
7	0	0	0	0	0	0	0	0	512 bytes
Total	8,476	250	136	7,716	29	25	153	167	5,944MB

The extracted graphic files were viewed using Quick View Plus®.

April 4, 1999

0930 hours: I continued the examination of the graphics and HTML files previously extracted from unallocated clusters using DIGit©.

1000 hours: I used EnCase® version 1.999 to perform a keyword text string search of the entire case. All hits were examined and text with possible evidentiary value was extracted.

Search 1: **Keyword:** **honda** **Hits:** **433**

April 5, 1999

0700 hours: I continued the examination of HTML files previously extracted from unallocated clusters using DIGit©.

1354 hours I used EnCase® version 1.999 to perform a keyword text string search of the entire case. All hits were examined and text with possible evidentiary value was extracted.

Search 2:	**Keywords:**	**99985 (case)**	**Hits: 0**
		999886 (case)	**1**
		ZDF-3333 (case)	**0**
		39347618	**0**
		virginia	**212**
		georgia	**333**
		certificate of title	**0**
Search 3:	**Keyword:**	**motorcycle**	**Hits: 1,696**

State Police - Computer Forensics Laboratory
Forensic Report - Laboratory Case Number 99-03-333-A
5 of 6 Initials **DBS**

April 6, 1999

0800 hours: I used EnCase® version 1.999 to perform a keyword text string search of the entire case. All hits were examined and text with possible evidentiary value was extracted.

Search 4:	**Keywords:**	**suzuki gsxr**	**Hits: 2**
Search 5:	**Keyword:**	**brandell**	**Hits: 125**
Search 6:	**Keywords:**	**jh2sc3307wm20333**	**Hits: 5**
		..#..####..######(Grep)	**0**
Search 7:	**Keyword:**	**Jn8hd17y5nw011333**	**Hits: 0**

April 7, 1999

0800 hours: I continued the examination of the search results.

1333 hours: I used EnCase® version 1.999 to perform a keyword text string search of the entire case. All hits were examined and text with possible evidentiary value was extracted.

Search 8:	**Keywords:**	**9998##(Grep)**	**Hits: 5**
		hotmail	**19,465**
		chyma	**27,453**
		suzuki	**20**

April 19, 1999

0700 hours: I continued the file-by-file examination of the evidence files.

0900 hours: I completed the forensic examination. Documents, pictures, HTML files, and text fragments of investigative interest were located by utilizing individual file-by-file examination, EnCase® Keyword Text Searches, and NCIS DIGit©. The Keyword Text Searches are defined in the EnCase® Report. Files believed to be of investigative interest were bookmarked into categories as defined below. The files associated with the information described below were copied/unerased from the EnCase® case.

FINDINGS

The analysis of the notebook computer resulted in the recovery of 176 files of evidentiary value or investigative interest. The recovered files included:

1. 59 document files including documents containing the suspect's name and personal information; text included in the counterfeit documents; scanned payroll, corporate, and certified checks; text concerning and describing stolen items; and text describing the recovered motorcycle.

2. 38 graphics files including high-resolution image files depicting payroll, corporate, and certified checks; U.S. currency; vehicle titles; registration cards and driver's license templates from Georgia and other States; insurance cards from various

companies; and counterfeit certified checks payable to a computer company ranging from $25,000 to $40,000 for the purchase of notebook computers. Most graphics were scanned.

3. 63 HTML files including Hotmail® and Yahoo® e-mail and classified advertisements for the recovered motorcycle, other vehicles, and several brands of notebook computers; e-mail text, including e-mails between the suspect and the concerned citizen about the sale of the recovered motorcycle; e-mails between the suspect and a computer company concerning the purchase of notebook computers.

4. 14 graphics files carved from unallocated space depicting checks at various stages of completion and scanned images of U.S. currency.

5. Two password-protected and encrypted files.

   a. WordPerfect® document containing a list of personal information on several individuals including names, addresses, dates of birth, credit card and bank account numbers and expiration dates, checking account information, and other information. Password [**nomoresecrets**].

   b. Microsoft® Word document containing vehicle title information for the recovered motorcycle. Password [**HELLO**].

I created one compact disk containing copies of the above-described files, which will be maintained in the CFL case file. A copy of the compact disk was labeled and provided to the investigator.

1800 hours: The forensic examination was completed.

Sgt. David B. Smith (5555) [Signature]