DIFO VT17 Lab #2

Group #21 Member 2, Member 3

Friday 6th October, 2017

Contents

CFIAR [insert case number]

Computer Forensic Investigative Analysis Report (CFIAR)

Incident Report Number	[2017,10,07, 1:st version]
Reported Incident Date	
Examiner(s)	Anton Fluch & Johan Bäckström
Requester(s)	N.N
Suspected Offence	N.N
Investigation Hours	N.N

CFIAR [insert case number]

Case [insert number]

Sample text:

SUBJECT owned a roofing company. SUBJECT gave his laptop computer to an employee to take to Mom & Pop's Computer Repair for monitor problems. Upon repairing the laptop, Mom of Mom & Pop's started the laptop to ensure the monitor had been fixed. A standard procedure of Mom & Pop's was to go to the Recent menu on the Start Bar of Windows® 98 systems and select files for viewing. Mom was presented with what appeared to be an image of a young child depicted in a sexually explicit manner. Mom telephoned the county sheriff. A sheriff's deputy responded and observed the image and confirmed it to be a violation of a State statute. The laptop was seized because it contained contraband. The seizure was performed in a manner consistent with recommendations found in Electronic Crime Scene Investigation: A Guide for First Responders. The laptop was entered into evidence according to agency policy, and a search warrant was obtained for the examination of the computer. The computer was submitted for examination.

Objective	[objective of forensics investigation]
Computer Type	[if known/needed]
Operating System	[if known/needed]
Offense	[if known/needed]
Case Agent	[if known/needed]
Evidence Number	#1234567
Where examination took place	[location]
Tools used:	[specify which tools were used]

Processing

Identification

Sample text: Reviewed the case investigator's request for service. The search warrant provided legal authority. The investigator was interested in finding all information pertaining to child pornography, access dates, and ownership of the computer. It was determined that the equipment needed was available in the forensic lab.

Acquisition

Sample text: The hardware configuration was documented and a duplicate of the hard drive was created in a manner that protected and preserved the evidence. The CMOS information, including the time and date, was documented.

Examination

Sample text: The directory and file structures, including file dates and times, were recorded. A file header search was conducted to locate all graphic images. The image files were reviewed and those files containing images of what appeared to be children depicted in a sexually explicit manner were preserved. Shortcut files were recovered that pointed to files on floppy disks with sexually explicit file names involving children. The last accessed time and date of the files indicated the files were last accessed 10 days before the laptop was delivered to Mom & Pop's.

Documentation and Reporting

Sample text: The investigator was given a report describing the findings of the examination. The investigator determined that he needed to conduct interviews.

CFIAR [insert case number]

Case X Brief Report

REPORT OF _____

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 #12345677

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.*

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

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

   (c) *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.*

   (d) *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.*

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

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

   (g) *No further user-created files were present on the media.*

5. **Glossary**

Term	**Explanation**
Shortcut File	*A file created that links to another file.*
Metadata	*Data associated with a file, such as timestamps.*

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
N.N Computer Forensic Examiner

Released by *Mr. X*

Funny Image

Figure 1: This is a caption.

Figure 2: This image is scaled down.

Table of Stuff

Table 1: This is a table.

Text goes here	& here	& here.
Here's a new line.		