



COMPUTER
FORENSIC
SERVICES, LLC

Computer Forensics
"Top 10 List"
- Things to avoid

Warren G. Kruse II, CISSP, CFCE
wgkruse@computer-forensic.com
<http://www.computer-forensic.com>
732-544-8080

Copy on www.computer-forensic.com/presentations/)

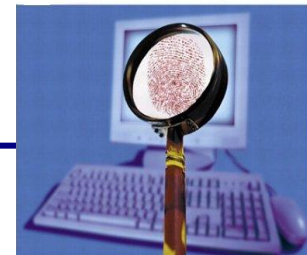
A little about me

● Warren G. Kruse II

- Certified Information Systems Security Professional (CISSP)
- Certified Forensic Computer Examiner (CFCE)
- Partner: Computer Forensic Services, LLC
- Instructor: Intenseschool.com
- Coauthor: Computer Forensics: Incident Response Essentials
- 2004 HTCIA International 1st VP
- Recipient 2001 HTCIA “Case of the Year Award”
- Member USSS NY and European Electronic Crimes Task Forces
- Previous Experience:
 - Lucent Technologies
 - Police Officer in NJ

Computer Forensics
Incident Response Essentials

Warren G. Kruse II
Jay G. Heiser



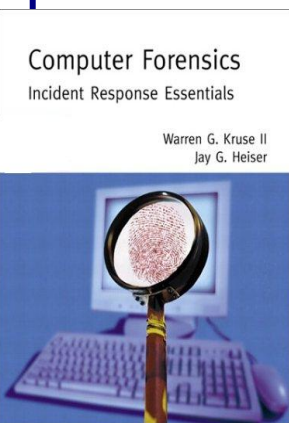
Computer Forensics

What the book says:

“Computer forensics involves the preservation, identification, extraction, documentation and interpretation of computer data. It is often more of an art than a science, but as in any discipline, computer forensic specialists follow clear, well-defined methodologies and procedures, and flexibility is expected and encouraged when encountering the unusual.”

From: “Computer Forensics: Incident Response Essentials”

Computer forensics is closely associated to law enforcement for retrieving evidence, but it could AND should be used to retrieve data for other reasons as well.



Terminology

- Image: exact copy of a hard drive including deleted files and areas of the hard drive that a normal backup would not copy



What Computer Forensics is used for:

- High Tech Investigations
- Incident Response
- E-mail recovery and analysis
- Document & File Discovery
 - Locating and recovering previously inaccessible files.
- Data Collection
 - Collecting data while preserving vital date and time stamps, temporary files and other volatile information.

What Computer Forensics is used for:

- **Preservation of Evidence**
 - Adherence to carefully developed set of procedures that address security, authenticity, and chain-of-custody.
- **Analysis of User Activity**
 - Reporting of all user activity on computer and company network including, but not limited to, e-mail, Internet and Intranet files accessed, files created and deleted, and user access times.
- **Password Recovery**
 - Accessing and recovering data from password protected files.





Top 10 Mistakes

1. Not having a plan before an incident.
2. “Looking around”
3. Reversing the master and slave at acquisition
4. Not using “forensically sterile” media
5. No or inadequate documentation

Top 10 Mistakes

6. Not having a good, unbroken chain of custody.
7. Not asking for help/ or asking too late
8. Using pirated / unlicensed software to conduct an examination
9. Using an examiner who misrepresents their background, training, etc.
10. Not reading my book :-)



1. Not having a plan before an incident.

- Logs don't last
- Core team has to be identified before the worst happens
- Federal rules state an expert must be selected for electronic discovery requests



2. "Looking around"

- Just booting a computer changes files
- Opening or printing files changes the files
- Deleted data, and data in unallocated clusters should be examined



3. Reversing the master and slave at acquisition or don't image physical drive

Use “forensically sterile” media
+ Image in the wrong direction
= “Nothing of evidentiary value”

- If you don't image the entire physical drive you will be losing data
 - 4 gig drive - 2 gig image example

4. Not using “forensically sterile” media

- Data contamination
 - Lawyers will love to bring up a “reasonable doubt” that the data was from a previous case.
- Example: had a person who was a Firewall admin send me an image of a drive, since the drive was not wiped there were thousands and thousands of IP's and hacker tools on the drive.

5. Inadequate documentation

- Average civil case in NJ take 2 ½ years.
 - Comtraid criminal case from 1999 court date Oct 2004
- Recent court case other sides report inadequate and anything testified to that wasn't in their report objected to.

6. Not having a good, unbroken chain of custody.

Standard Evidence Form.doc - Microsoft Word

File Edit View Insert Format Tools Table Window Help

Type a question for help

75% Block Line + Le Times New Roman 12

COMPUTER FORENSIC SERVICES, LLC

Evidence Property Custody Document

Office	Serial Number:	
Location	Investigator Assigned To:	
Name and Title of Person from whom received <input type="checkbox"/> Owner <input type="checkbox"/> Other	Address (include zip code)	
Location from where obtained	Reason Obtained	Date:

Item No.	Quantity	DESCRIPTION OF ARTICLE(S) (include model, serial number, condition and visible marks or scratches)

CHAIN OF CUSTODY				
Item No.	Date	Released By	Received By	Purpose of Change of Custody
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	
		SIGNATURE	SIGNATURE	

Page 1 Sec 1 1/2 At 2.1 Ln 2 Col 2 REC TRK EXT OVR English (U.S.) Standard Evidence Form.doc - Microsoft Word

- From who, to whom, when, where, why and how.
 - i.e. Civil Case where all they asked the court was for chain of custody forms and inspect the storage of evidence

7. Not asking for help or asking too late

- Believing that all cases can be handled internally

- **Hypothetical** Sys admin e-mail:

The compromised system was running some hacker tools, apparently probing the University of [blank] (found running: .bla -s 123.456.*.*)

Unfortunately I removed the probe tool before determining exactly what it was doing, sorry. Additionally, there were outbound telnet connections from the compromised system to University of [someplace else] & State University of (some state).

The hackers also altered the inetd config to install a high-port telnetd and a backdoor for unauthenticated root access on an alternate TCP port.

Naturally I have re-secured our system and have stepped up monitoring for unauthorized access.

Using pirated / unlicensed software to conduct an examination

- “A leading computer-security company is accused of software piracy.”
- First question you will get now on cross is “are you licensed to use the software you conducted the examination with? Have you ever used unlicensed software?”

<http://www.fortune.com/fortune/technology/articles/0,15114,457276,00.html>

Using an examiner who misrepresents their background

- Using an examiner who misrepresents their background, training, etc.
 - Many unemployed people switching to forensics
 - Many companies adding forensics as another service
- Not checking certifications
 - Mail order certs
 - Certs not recognized
- Where will they be 2 ½ years from now?

Alternate # 10: Not following the cardinal rules

- The four “Cardinal Rules” per IACIS for Digital Forensics are as follows:
 1. Never Mishandle Digital Evidence
 2. Never Work On Original Digital Evidence
 3. Never Trust The Subject’s Operating System
 4. Document Everything

Trace Information May Exist From:

- Email
- PDA/Blackberry
- Temp Files
- Recycle Bin
- Info File Fragments
- Recent Link Files
- Spool (printed) files
- Internet History (index.dat)
- Registry
- Unallocated Space
- File Slack



The File Lives On...

- This is possible only through the forensic practice of treating the entire physical disk as evidence (rather than just files) and handling it as evidence.

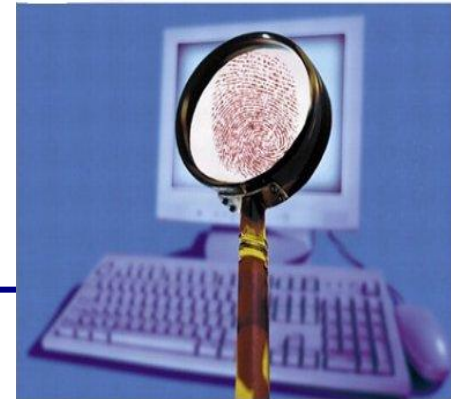


Where to go from here

- www.virtuallibrarian.com/legal/
- www.htcia.org
- www.intenseschool.com
- **Shameless Plug Warning:**
 - Computer Forensics:
Incident Response Essentials
 - **Paperback:** 416 pages
 - **Publisher:** Addison-Wesley Pub Co
 - **ISBN:** 0201707195

Computer Forensics
Incident Response Essentials

Warren G. Kruse II
Jay G. Heiser



Questions?



Computer Forensic Services, LLC

Copy on www.computer-forensic.com/presentations/
www.computer-forensic.com/newsletter/Feb-newsletter.htm

Warren Kruse
20 Industrial Way
Eatontown, New Jersey
(732) 544-8080
Email: wgkruse@computer-forensic.com

