

Larry E. Daniel, EnCE, DFCP, BCE



Digital Forensics for Attorneys - Part 2

Experts, Analysis, Challenging Evidence

Digital Forensics For Attorneys

Part 1

- **Overview of Digital Forensics**

- Types of Digital Evidence
- Acquisition (Collection) and Preservation

Part 2

- **Experts, Evidence and Analysis**

- Understand Forensic Experts vs. Computer Experts
- Digital evidence: discovery and usage
- Overview of Digital Forensics – Analysis
- Challenging Digital Evidence



Experts



Defendant as Expert



Why a Forensics Expert?

Computer Forensics Expert

- Should have comparable or better training and experience than the other expert.
- Should have specific training and experience as a digital forensics expert
- Should have access to the same tools as the opposing expert
- Must be able to qualify as a forensic expert in court





Technical Expertise Comparison

Computer Expert	Forensic Expert
<ul style="list-style-type: none"> • Installation and setup of computers, software and networking • Disaster recovery of failed systems from backups • Troubleshooting and repairing computer problems • Removal of virus, malware, and Trojan horse software from infected computers, not the evidentiary effect of such programs. • Installation and maintenance of software applications for the end user. • Installation and setup of networking and Internet access for the purpose of allowing the end user to access the Internet or work network. 	<ul style="list-style-type: none"> • Forensically sound acquisition of digital evidence • Forensic data recovery from multiple media types, including backups • Forensic data analysis • Determination of the effect of virus, malware, and Trojan horse software on digital evidence, not for the purpose of removing such programs. • Examination of artifacts left behind by software applications for the purpose of determining the effect on evidence. • Examination of Internet artifacts in investigations for the purpose of determining their evidentiary value.



Technical Expertise Comparison

<ul style="list-style-type: none"> • Formatting and using various file systems for the purpose of installing operating systems such as Windows, Mac OS, or Linux. • Works with common file formats such as DOS, Windows, Linux, Mac for the purpose of installing software, finding files, and making backups. • Can make backups of hard drives, files and directories; does not include deleted data, for the purpose of recovery of lost documents for business continuation. 	<ul style="list-style-type: none"> • In-depth knowledge of how file systems work at the lowest level for the purpose of locating and examining artifacts recorded by the operating and file systems. • Understands and can use forensic file formats such as Expert Witness, DD Images, Access Data Images, and Smart Images for the purpose of chain of custody, authentication, and verification of evidence • Can make forensic copies of entire physical media including all deleted data for the purpose of forensic analysis
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



Legal Expertise Comparison

Table 8.2 Legal Expertise Comparisons

Forensic Expert	Computer Expert
<ul style="list-style-type: none"> • Chain of custody • Search warrant affidavits • Discovery motions and subpoenas • Assist with trial preparation. • Can qualify as a computer forensic expert in court • Adheres to ethics guidelines for forensic examiners 	<ul style="list-style-type: none"> • Unlikely • None • None • Unlikely • May qualify as a computer expert in court • Not applicable



Selecting a Digital Forensics Expert



Reasonable Costs

Table 9.1 General Time Estimates by Case Type

Case Type	General Estimate of Hours Required
Simple domestic case: Forensic copying of original evidence in the lab, recovery of Internet history, e-mail, chat logs, pictures. Forensic software-based single cell phone examination.	10 to 20 hours
Manual examination of a single cell phone.	4+ hours
Civil case.	4 to 8 hours
Criminal case.	10 to 50+ hours depending on complexity.
Child pornography case.	15 to 50+ hours depending on complexity and location. Cost is higher due to Adams Walsh Act requirement that has the examiner onsite during the entire process. Additionally, travel cost to and from the location is required if it is not local to the examiner.
Simple hard drive imaging: A single hard drive in a computer that is easy to access.	2 hours if done in lab (many examiners charge a flat fee for making forensic images of hard drives).
Complex hard drive imaging: Complex RAID setups, odd formatting, extremely large size (multiple terabytes).	3 to 12 hours if onsite (depends on size of drive). 2 to 25 hours depending on size, hardware type, operating system, and formatting.

Certifications

- **EnCase Certified Examiner (EnCCE)**
 - This is probably the most widely known and recognized certification. This is a vendor-specific certification that is provided through Guidance Software, the publishers of the EnCase Forensic Software. EnCase is widely used in law enforcement and in the private sector. (www.encase.com)
- **Access Certified Examiner (ACE)**
 - This is the vendor-specific certification for the Forensic Tool Kit (FTK) software by Access Data Corporation. FTK is widely used in law enforcement and in the private sector. (www.accessdata.com)
- **Certified Computer Examiner (CCE)**
 - This is a vendor-neutral certification administered by The International Society of Forensic Computer Examiners. The CCE is one of the oldest certification programs. (www.isfco.com)
- **GIAC Certified Forensic Examiner (GCFE) and GIAC Certified Forensic Analyst (GCFE)**
 - These are vendor-neutral certifications administered by SANS Institute and are supported by extensive training programs. (www.giac.org)
- **Certified Forensic Computer Examiner (CFCE)**
 - These certifications are offered by the International Association of Computer Investigative Specialists (IACIS). Until recently the certification has been open only to active or retired law enforcement officers. As of July 2011, the certification is open to the general public. (www.iacis.com)

Forensic Tools

Do they have appropriate forensic tools?

- Required to perform many digital forensic functions
 - Computer Forensics (EnCase, FTK)
 - Cell Phone Forensics (CelleBrite, Paraben, Susteen)
- Almost always needed to perform forensically sound acquisitions and examinations.



Selecting an Expert: Overview

1. Actual training in digital forensics and sub-disciplines?
2. Digital Forensics certifications? Or just computer based certifications?
3. Actual case experience?
4. Recommendation letters from other professionals, particularly attorneys?



Selecting an Expert: Overview

RALEIGH (WTVD) -- The defense asked for a mistrial Tuesday in the Brad Cooper murder trial. The move came as the first witness for the defense endured a withering examination by the prosecution on his qualifications to testify as an expert. James Ward of WireGhost Security told the court he was an expert in computer network security, but the prosecution questioned his qualifications to testify about Cooper's computers as a forensics expert.



Defense computer expert James Ward (WTVD Photo)



Selecting an Expert: Overview

Arguing before Gessner Tuesday, the prosecution said Ward lacked the proper education and experience to say there was evidence of computer tampering.

"He has a home lab. He borrowed his tools from Cisco. He doesn't know what software he used," said prosecutor Boz Zellinger.

Zellinger said the prosecution and defense should be held to the same standards on expert witnesses, and Ward falls short. "I would be laughed out of this building," said Zellinger.

Gessner ruled that Ward could testify about network security, but he could not testify about the FBI reports on Cooper's computers.



Spotting a Problem Expert

- Attitude: How does the expert interact with your team?
 1. Arrogant or superior?
 2. Does he or she take the time to explain to properly explain technical concepts in easy to understand language?
- The Bull Factor
 1. If an expert does not have the answer to a question, does he or she try to convince you that they do anyway?
 2. Great risk when testifying.
 3. Use of jargon to cover up ignorance.



Spotting a Problem Expert

- Does the Examiner Have Time?
 1. Does the examiner have time to work the case?
 - Some cases (particularly Child Pornography) can require travel.
 - Is Forensics a second job? Avocation?



Expectations of a Forensics Expert

Computer Forensics Expert

- Expected to
 - Anticipate testimony of opposing expert based on the forensic reports and discovery.
 - Duplicate and verify the opposing expert's work.
 - Assist the attorney in preparation for trial
 - Advise the attorney as to the merits of the case in regards to the digital evidence presented.



Expectations of a Forensics Expert

Computer Forensics Expert

- Expected to testify if needed as to:
 - Various files on the client's computer.
 - Ownership of the computer and files.
 - Forensic processes used to extract and verify data.
 - Handling and collection of the evidence.
 - Specifics relating to software installed, dates and times of computer activities



Analysis



Analyzing the Case

- Approaching the case holistically
 - Digital evidence can reach into all corners of a case:
 - » Cell records
 - » Email
 - » Pictures
 - » Timelines
 - » Internet Activity



Analyzing the Case

Always work the case like you are the primary examiner.
Never assume anything.

Check all the points in the case where mistakes are normally made:

Chain of custody.

Examination standard procedures.

RTC verified for all evidence containing clocks.

Evidence handling at the scene.

Was everything examined.

Claims made in the forensics report.

Pay particular attention to keyword search results, internet history results, link files, etc.

Placing the defendant at the computer.



Performing the Analysis

- **Step one:**
 - Duplicate the other side's work.
 - Verify the accuracy of their findings
 - Did they represent their findings correctly?
 - How thorough was the examination?
 - Verify the completeness of their report
 - Is everything they found in the report?
 - » Why or why not?
 - Was exculpatory evidence ignored or missed?



Establishing a framework for analysis

- Reading discovery documents
- Reading the computer forensics reports
 - What claims are being made?
 - What statements were made?
 - What facts support the claims and which do not?



What clues can lead to a more thorough digital analysis?

- Defendant's statements
- Witness statements
- Police statements and interviews
- Call center records
- Search warrants and subpoenas
- Other supporting documents
- Law Enforcement's computer forensics report



Case Analysis

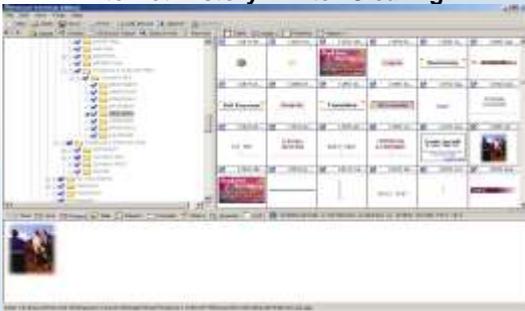
Examples



Internet History – Before Clearing



Internet History – After Clearing



Challenging the evidence

- **Common mistakes that open digital evidence to challenges**

- Failing to verify clock times
 - Computer Clocks (Real Time Clock Setting)
 - Affects everything related to time lines:
 - » Internet history
 - » Emails
 - » Computer activity
 - Digital Cameras
 - Affects the metadata inside the digital images.



Challenging the evidence

- **Is there an attempt to place a person at a computer without adequate proof?**
 - How can you tell?
 - Did the analyst check for unique user accounts with passwords?
 - Is there evidence anyone else used the computer under that person's account or profile?
 - Was the computer in a common area?
 - Did others know the passwords to the user's account?
 - Was access to the computer restricted by physical boundaries or location?



Challenging the evidence

- **Games people play**
 - Stating facts out of context
 - Keywords
 - Keyword hits are not always relevant
 - » Murder case example
 - » Hits were found for the keywords murder (156), kidnapping (34), disposal (76), and death (273) on the subject's computer.



Challenging the evidence

- **Games people play**
 - Stating facts out of context
 - A Keyword hit is not always based on a User Search.
 - Context based ad services create searches automatically.
 - There must be evidence that the user created the search, not an automated process.



Challenging the evidence

- **Games people play**
 - Playing the techie game
 - Technical words no one understands
 - Unallocated space
 - Slack space
 - Browser cache
 - Typed URLs
 - Gnutella and Limewire
 - What does that mean?



Challenging the evidence

Listed below are the notable keyword searches and number of "hits" that FTK noted.

"Homicide" 230 hits	"Pheedo" 155903 hits
"Homicidal" 540 hits	"Kill" 9010 hits
"Insanity" 178 hits	"Police" 5788 hits
"Defense" 2429 hits	"Killer666vampire" 4863 hits
"Defense and Insanity" 871 hits	"Killer" 3872 hits
"Wikipedia" 6034 hits	"Insane" 4308 hits
"Murder" 2497 hits	"Death" 7745 hits
	"Deathblow" 16 hits
	"BTK" 1174 hits



User Inputted Search Terms?

```
\\Desktop\c:\386\apps\app00102\common\mshared\w\chared\msg3en.lex
instably $j $j lb instable == j l insanity $j j lb insanity l d 2 insanity $j
12/16/06 02:15:19PM 12/16/06 02:15:19PM 03/09/05 07:11:46PM
```

```
\\Desktop\l\Recovered Folders\aplico.exe
see me wrestle this Saturday afternoon :) A Fair Amount Of Insanity &#2A FAIR AMOUNT OF INSANITY" is an
annual wrestling event
Yes
11/30/06 05:47:01PM 11/30/06 05:47:01PM 11/30/06 05:47:01PM
```

```
\\Desktop\l\Recovered Folders\aplico.exe
afternoon :) A Fair Amount Of Insanity &#2A FAIR AMOUNT OF INSANITY" is an annual wrestling event put on by
MADMAN Entertainment
Yes
11/30/06 05:47:01PM 11/30/06 05:47:01PM 11/30/06 05:47:01PM
```

```
\\Desktop\l\Recovered Folders\Windows\SoftwareDistribution\DataStore\DataStore.edb
tely wasn't int s jeffdunham 0:39+ Jeff Dunham: spark of insanity bed scene, walte... 1,833,051 views hoppajinx
7:17+ Jeff D
Yes
12/16/06 02:37:14PM 12/16/06 02:37:14PM 08/08/10 01:42:15AM
```



Challenging the evidence

- What does that mean?
 - If it is in the browser cache, does that mean the user did it on purpose?
 - » How browser caching works.
 - » Federal courts have ruled that files:
 - » in the internet cache do not constitute possession unless the prosecution can prove the user knew about the files in the cache.
 - » In unallocated space do not constitute possession.
 - » Same ruling in Georgia in 2007.





Challenging the evidence

- What the heck is unallocated space?
 - » Unallocated space is areas on the hard drive that are available to store data.
 - » When a file is deleted, it is only marked as deleted, so the old data remains on the hard drive in the unallocated space.
 - » Forensic tools can recover files from this unallocated area of the hard drive.
- » Files recovered from unallocated space do not contain:
 - » Dates or times.
 - » Original file names
 - » Original location on the hard drive.



Challenging the evidence

- **Call Detail Records and Cell Phone Locations**
 - Help to establish the whereabouts of the defendant?
 - You cannot locate a cell phone using call detail records.
 - 90% of the cases reviewed contain serious flaws in the reports by law enforcement.
 - Be very careful of claims overstating the accuracy of this type of location information.
 - No such thing as triangulation of a cell phone from call detail records.



Questions?

Contact Information:

Email: lars@guardiandf.com
Web: www.guardiandf.com
Blog: www.exforensics.com
Phone: 919-868-6281

Coming soon:
Attorney Resource Center Online
www.attorneyresourcecenteronline.com

Book: Digital Forensics for Legal Professionals
May 2011, Syngress Publishing
Larry E. Daniel and Lars E. Daniel