Digital Forensics In Child Pornography Cases

GUARDIAN
DIGITAL FORENSICS

Larry E. Daniel, DFCP, EnCE
Digital Forensics Examiner
Guardian Digital Forensics

About Your Presenter

- **Began working with personal computers in 1982**
  - 29 years of experience in troubleshooting, networking, administration, programming and repair of computers starting with MS DOS 1.3.
- **Began in computer forensics in 2001**
  - 190+ hours of training specifically in computer and cell phone forensics
  - Testified as an expert witness 13 times.
  - Qualified and testified as an expert in three areas:
    - Computer Forensics
    - Cell Phone Forensics
    - Cellular Technology and Cell Tower Forensics
  - Worked over 500 cases, including Casey Anthony and other high profile cases.
  - Digital Forensic Certified Practitioner, Encase Certified Examiner and Blackthorn GPS Certified Examiner
  - Co-Author of the book; “Digital Forensics for Legal Professionals”

GUARDIAN DIGITAL FORENSICS

Special Issues

2007 – Adam Walsh Child Protection and Safety of 2006

- Makes is a Federal Crime to allow child pornography to be given to anyone outside of law enforcement
  - Some local states and laws allow this in spite of (Virginia)
- Impact is that case work must be done at a law enforcement facility.
  - Increases the cost of doing these cases

GUARDIAN DIGITAL FORENSICS

Special Discovery Issues

- **Cases involving child pornography.**
  - Possession, duplication and distribution of child pornography is illegal in most states and at the federal level.
    - This means that evidence containing contraband images cannot be given to attorneys, prosecutors or experts.
    - Police officers are not allowed to duplicate the evidence beyond the single copy on their computer forensics analysis computer unless ordered by the court to make a copy for purposes outlined in the court order.

GUARDIAN DIGITAL FORENSICS

Special Discovery Issues

- **Cases involving child pornography.**
  - State protective orders may not be recognized by federal agencies, leading to charges of possession at the federal level.
  - The defense expert must work under the supervision of law enforcement.
  - Need a Motion to Compel Access to Evidence
    - Can be provided as needed.

- **Defines the parameters for the analysis by the defense expert for all parties involved even if not ruled on by a Judge.**
  - Defines a date and time for the expert to access the evidence for analysis.
  - Defines the methods the expert will use to prevent accidental copying of contraband

GUARDIAN DIGITAL FORENSICS

Performing the Analysis

- **Analysis**
  - 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?

GUARDIAN DIGITAL FORENSICS

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.

GUARDIAN DIGITAL FORENSICS

Child Pornography Cases

- **The Players**
  - ICAC (Internet Crimes Against Children Task Force)
    - Funds and trains local and state law enforcement
- **The Progression**
  - Police get trained first in Internet Predator Investigations
  - Federal grants to fund computer forensics
    - Police get a one week class on computer forensics
    - Focus on peer to peer investigations
    - They get a computer and a copy of the Encase Software
    - Now they are computer forensics experts

GUARDIAN DIGITAL FORENSICS

Child Pornography Cases

- **Typical Scenario**
  - Police find CP on a computer
  - Submit images or movies to prosecutor
  - Charges are filed
  - Suspect is arrested
  - Defense attorney reviews images
  - Defendant takes a plea

GUARDIAN DIGITAL FORENSICS

Child Pornography Cases

- **Police examiners count on not being challenged**
  - Attitude is:
    - It is either there or not. What is there to investigate?
  - No motivation to perform a full examination.
    - Don't care where it came from
    - How it got there
    - No interest in exculpatory evidence

- **In 90% of cases, I am the first defense expert they have ever seen.**

GUARDIAN DIGITAL FORENSICS

How people get caught

- Peer to peer investigations (File Sharing)
- CP found subsequent to other computer forensic examinations
- Reported by someone who is using their computer
- Reported by a third party (concerned citizen)
- Reported by an ISP (AOL, Yahoo, Picasa (Google))
- Computers seized as part of a sex crime investigation

GUARDIAN
DIGITAL FORENSICS

Internet Predator Investigations

- **Police officer sits in a chat room and masquerades as an underage girl or boy**
  - Must not initiate chats
  - Can say anything they want to entice, as long as they remain "passive"
    - Roisman Case
  - Goal is to set up a meeting for an arrest.
- **Normal time to get a hit in a chat room:**
  - Under five minutes
- **Collects the evidence via chat logs and screen shots**
  - Logs need to be authenticated
  - Logs should be examined for anything that can be considered entrapment.

GUARDIAN DIGITAL FORENSICS

Peer to Peer Investigations

- **Uses a special version of LimeWire modified for law enforcement or other tools.**
  - Peer Spectre, GNU Watch, or other
  - Can “see” child pornography being transferred over the Gnutella network
  - Can see the IP address of ROUTER sharing or downloading contraband
  - Can connect directly to a suspect computer on the network
  - Uses a WHOIS lookup to see where the IP is located
  - Subpoena to the ISP for subscriber information
  - Captures a list of files being shared or downloaded
  - Progresses to a warrant from there

GUARDIAN DIGITAL FORENSICS

The Questions To Be Answered

- What is present?
- Where is it?
- When was it put there?
- How did it get there?
- Who put it there?

GUARDIAN
DIGITAL FORENSICS

The Questions

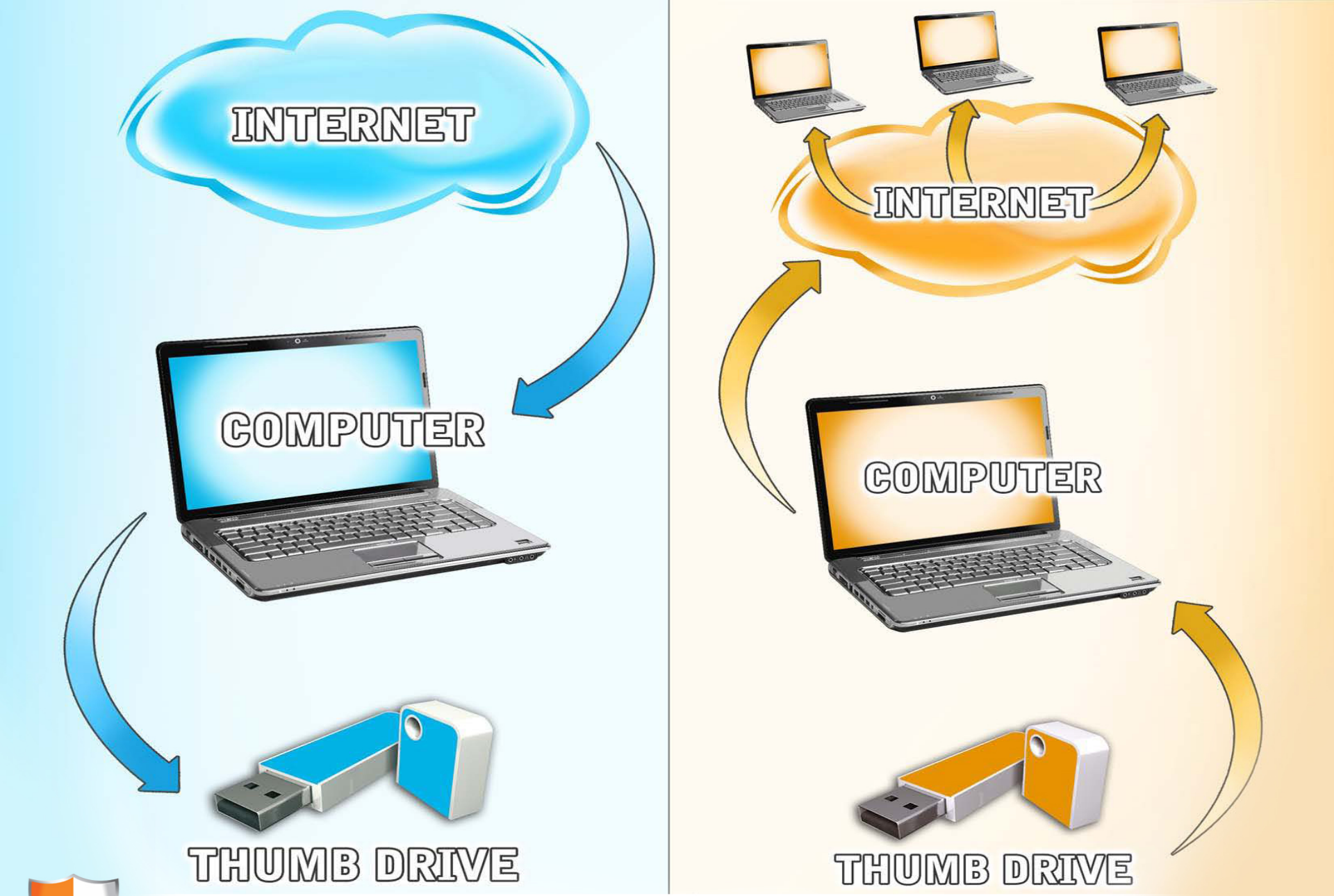
- **What is present?**
  - Pictures
    - Thumbnails
    - Full size images
  - Movies
    - Is the CP embedded in the middle or it is all CP?
    - Are the movies complete or incomplete?
- **Has it been deleted?**

GUARDIAN DIGITAL FORENSICS

The Questions

- **Where is it?**
  - Only on the computer drive?
  - On other devices as well?
    - Thumb drives
    - External hard drives
    - CDs and DVDs
    - Cell Phone
    - Media Player

GUARDIAN DIGITAL FORENSICS



GUARDIAN
DIGITAL FORENSICS

The Questions

- **When was it put there?**
  - Did the defendant have access to the computer during these times?
    - Do we know the whereabouts of the defendant?
      - At work?
  - Did others have access to the computer at these times?
  - (Alabama Case)
    - Ex Husband set up the boyfriend.

GUARDIAN DIGITAL FORENSICS

The Questions

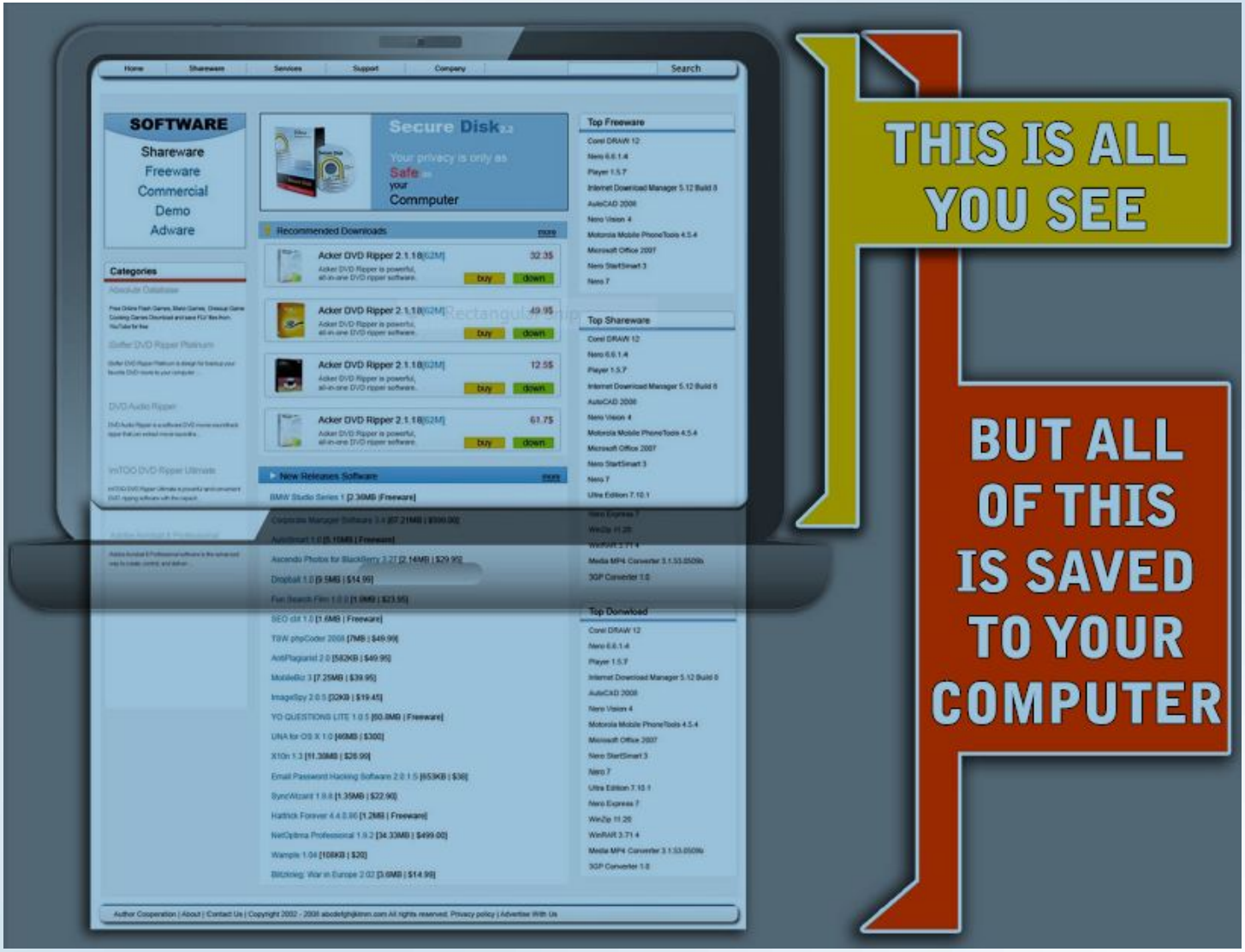
- **How did it get there?**
  - Was it downloaded as a result of using the Internet browser only?
  - Newsgroups?
  - Via Email?
  - Limewire or other peer to peer networks?
  - Chat rooms?

GUARDIAN DIGITAL FORENSICS

How browser caching works

Internet Browsers save everything

GUARDIAN
DIGITAL FORENSICS



GUARDIAN DIGITAL FORENSICS

Internet Cache

United States v. Kuchinksi, 469 F.3d 853 (9th Cir. 2006)

- "We held that we could not consider images recovered from the cache for purposes of a sentencing calculation when no evidence indicated that the defendant had tried to access the cache files or knew of their existence. *Id.* at 862.
- We reasoned:
- Where a defendant lacks knowledge about the cache files, and concomitantly lacks access to and control over those files, it is not proper to charge him with possession and control of the child pornography images located in those files, without some other indication of dominion and control over the images.

- To do so turns abysmal ignorance into knowledge."

GUARDIAN DIGITAL FORENSICS

The Questions

- **Who put it there?**
  - Who owns the computer?
  - Who's profile is it stored under?
  - Is the defendant's profile password protected?
  - Who has access to the defendant's account?
  - Who else uses the computer?
  - Did anyone witness the defendant viewing or downloading CP?

GUARDIAN DIGITAL FORENSICS

Unallocated Space

- **Users have no method for accessing files in unallocated space.**
- **Files recovered from unallocated space do not contain:**
  - Dates and times
  - File Names
  - Original Location (Where was it before it was deleted)

GUARDIAN
DIGITAL FORENSICS

Unallocated Space
United States v. Flyer (Feb 2011)

- Users have no method for accessing files in unallocated space.

- But deletion of an image alone does not support a conviction for knowing possession of child pornography on or about a certain date within the meaning of § 2252(a)(4)(B) (2004). No evidence indicated that on or about April 13, 2004, Flyer could recover or view any of the charged images in unallocated space or that he even knew of their presence there. Accordingly, the district court committed plain error, and we reverse Flyer's conviction on Count Three

GUARDIAN
DIGITAL FORENSICS

Are the images really chargeable?

WESTERN DIGITAL HARD DRIVE: 67 Possible Images and 17 Possible Movies located by Scott Slifer.

8 of the images tagged by Det. Slifer are not contraband. They depict people who are fully clothed in normal types of shots.

19 of the images depict older children and teens who are partially to fully nude and posing for the camera. There are no sex acts depicted in any of the images. Of these images, they were downloaded to the computer, probably from a web site as they are all thumbnail images. The creation date for these files was Mar. 9, 2005 and the Last Accessed Date, when they were deleted was Mar. 10, 2005.

The movies on this hard drive are from a modeling site. The movies do not depict any nudity.

The remaining 40 images tagged by Det. Slifer depict children and teens in various modeling poses. They do not contain any nudity or sexual activity.

GUARDIAN DIGITAL FORENSICS

Example from a Chat Session

Date	Time	From	To	Message
9/27/2004	12:25:00 AM	don heri	(ÇÄ®£Ø§) Tu CorAzÓn LO SaBe!!	hola
9/27/2004	12:25:04 AM	don heri	(ÇÄ®£Ø§) Tu CorAzÓn LO SaBe!!	quieres el video o no
9/27/2004	12:25:11 AM	(ÇÄ®£Ø§) Tu CorAzÓn LO SaBe!!	don heri	**si**
9/27/2004	12:25:12 AM	(ÇÄ®£Ø§) Tu CorAzÓn LO SaBe!!	don heri	**pero**
9/27/2004	12:25:13 AM	(ÇÄ®£Ø§) Tu CorAzÓn LO SaBe!!	don heri	**uvo falla**
9/27/2004	12:25:17 AM	(ÇÄ®£Ø§) Tu CorAzÓn LO SaBe!!	don heri	**no c pudo enviar**
9/27/2004	12:25:27 AM			don heri sends D:\New Folder (2)\!!boytied.wmv
9/27/2004	12:25:47 AM	(ÇÄ®£Ø§) Tu CorAzÓn LO SaBe!!	don heri	**manda varios**
9/27/2004	12:26:56 AM			Transfer of "!!boytied.wmv" is complete.
9/27/2004	12:27:00 AM	(ÇÄ®£Ø§) Tu CorAzÓn LO SaBe!!	don heri	**manda mas**
9/27/2004	12:29:00 AM	(ÇÄ®£Ø§) Tu CorAzÓn LO SaBe!!	don heri	**heyheri**

Key Points

- **Peer to Peer File Sharing**
  - What program was used? (Multi Select or Single Select Option)
  - How much was CP compared to legal pornography
  - Was it previewed?
  - Was consent given legally?
    - STATE OF MAINE v. JACK D. BAILEY II (Maine Supreme Court, March 2010)
      - Police used deceit to gain consent to search his computer.
      - Claimed to be searching for “problems” in the area with the internet and files.
      - Gained access then started searching for movie files.
    - Same in a recent case in NC (Not Argued)

GUARDIAN DIGITAL FORENSICS

Questions?

Contact Information:

Email: larry@guardiandf.com

Web: www.guardiandf.com

Blog: www.exforensis.com

Phone: 919-868-6281

Digital Forensics for Legal Professionals
By Larry E. Daniel and Lars E. Daniel