

Electronic Discovery

Doug White, PhD, CISSP, CCE

www.whitehatresearch.com

Roger Williams University

Why is Electronic Discovery Important to Trial Lawyers?

- In the 2000 Census, the US Commerce Department reports 51% of all households in the U.S. have computers.
 - 65% of all children lived in a household with a computer.
 - 30% of the children used the internet.
 - Among people 3 years and older, 36% (94 million people!) used the internet at home.

And that was in 2000!

Think about the next 20 Years

- My daughter is 5.
- She uses a computer to send email
- She uses a computer for entertainment
- She uses a computer for projects
- Her Generation will do most of their activities electronically.

Think about today

- You pay your bills electronically
- You send and receive email instead of traditional correspondance
- You use GPS to locate a hotel
- You use a blackberry to schedule appointments.
- You use a laptop for work

So what should your firm be doing with Electronic Discovery?

Everything it Can!

- Acquire Information
- Reengineer your approach
- Implement

Acquisition of Knowledge

- Develop contacts with CCE and CFCE certified individuals
 - CCE is Certified Computer Examiner
 - CFCE is Certified Forensics Computer Examiner (law enforcement)
- Use CPEs to study Electronic Resources
- Get a computer and use the internet

Reengineer Your Approach

- Professionals become entrenched in methodology
- Think outside the box
- Don't forget technology when you consider the case!

Implement

- Develop experts you can work with regularly
- Acquire all electronic media in each case

Components of Discovery

- Computers
 - Laptops, Desktops, Servers
- Networking Devices
 - Routers, Switches, Firewalls, Hubs
 - WIFI!!!
- Personal Tools
 - Cell Phones, PDAs, Cameras, MP3 players
 - GPS, Printers and Fax machines, digital recorders
- Odds and Ends
 - Flash memory sticks, other media

Soft Components

➤ Chat Rooms

- Chats can be recovered from the disk in part.
- Instant messages (IM) also fall into this category
- These may fall under wiretap laws

➤ VOIP (Voice over IP)

- This may be recoverable depending on how it is managed on the system.
- This may fall under wiretap laws.

➤ Backup Copies of Hardware Devices

- Tapes, et. al.

What can you recover?

➤ Evidence

- Deleted Files!
- Erased Disks!
- Cached Web Pages!
- Cached emails from web based mail
- Photographs
- Address Books
- Calendars
- Etc.

Primary Services of Experts

- Acquire Images of Media in a Sound Fashion
- Analyze and develop evidence discovered
- Open encrypted and password protected media
- Recover hidden and deleted files
- Develop expert testimony about electronic media and devices

Consider a Case:

- A company terminated an employee as a result of a hostile workplace charge.
- The employee filed a wrongful termination suit against the company.
- All of the evidence the hostile workplace charge was electronic.
 - The employee had used a web based email service to send pornographic photos to another employee who filed the complaint.
 - The terminated employee denied the charge.

Electronic Discovery

- An Image of the employees disk was obtained.
- The image was examined and initially the disk had nothing of consequence.
- Examination of the slack space on the disk revealed the web based email and several of the photos sent.
- Examination of deleted files and folders revealed massive amounts of pornography as well as the photos sent to the employee.

Wrapping it Up

- Data is tied together with Windows log to show who was on the machine with dates and times of creation of photos, emails etc.

Bottom Line

- Both sides need to be fully evaluated by experts to determine how the case should proceed.

Future

- Every case will likely have a technology component.
- Many cases will be entirely reliant on electronic evidence
- Electronic discovery is critical to your firm.
Critical!

Q&A

- Slides are available at:
 - www.whitehatresearch.com
 - Doug.white@whitehatresearch.com