

# Computer Forensics

Doug White, PhD, CISSP, CCE

[www.whitehatresearch.com](http://www.whitehatresearch.com)

Roger Williams University

# Where is Forensics going to be Used?

- We all know about law enforcement!
  - Did you look at something illegal?
  - Did you buy something illegal?
  - Did you sell something illegal?
- But what about the everything else in LIFE?...

# Consider a Case: NOT Zubulake v. Warburg

- 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 cache 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.

# The Super Chinese Hack

- Broken Firewalls and a destroyed website
- Failed Backups
- Tracing someone
- Finding that someone across the internet
- Crime and Punishment!
- Translating all the findings to something that a manager can understand.

# Why is Computer Forensics Important?

- 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 *your* life today

- Your calendar is electronic
- 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

# Components of Forensics

- 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

# What can you recover?

## ➤ Evidence

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

# Forensics Examiners

- Certified Computer Examiner and Certified Forensic Computer Examiner (CCE and CFCE)
  - Premier Certifications that require both practical examination and general knowledge examination
  - Requires renewal every two years with a new practical

# What do examiners do?

- Collect evidence in a usable manner (admissible)
- Recover exculpatory or inculpatory evidence from media and hardware devices
- Present the evidence in an manner which will assist attorneys in the case
- Act as experts at trial and present complex material in a manner a jury can comprehend and use.
- Preserve and maintain evidence for later use

# Q&A

- Slides are available at:
  - [www.whitehatresearch.com](http://www.whitehatresearch.com)
  - Training for CCE at whitehatcce.com
  - Doug.white@whitehatresearch.com