

# Understanding Computer Forensics

Cape Cod Technology

Council – 03 – March - 06

Doug White, Phd, CISSP, CCE

Roger Williams University

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

# The emergence of forensics

- Previously digital evidence was a minor component as digital evidence was admissible as hearsay evidence only (if at all).
- As more cases have **ONLY** digital components, both civil, criminal, and in-house issues will **HAVE** to involve digital evidence.

# Imagine

- An employee at your company has continually harassed and abused another employee by sending pornographic emails and chats to her.
- She complains and he is reprimanded.
- He continues the behavior and is fired.
- She quits files a Hostile Workplace suit.
- After 6 months, he files a wrongful termination suit.

# What happened?

- Did you maintain images of both machines that are admissible?
- Do you have any evidence in either case?
- If you don't you will be paying two settlements in the near future.

# What really happened?

- The company had an examiner review the material on the image of the employee's disk. They were able to prove that he had sent the emails and found vast amounts of pornography.
- This was used to convince the employee to reconsider his suit.

# Basic Ideas of Forensics

- Data Recovery
  - Undeletes and recovers
  - Analysis of Hidden Files
  - Analysis of Secured Files
    - Passwords
    - Encryption
  - Analysis of Damaged Media

# Using this in your company

- Collect Images of Drives
  - An image is a bit by bit copy (mirror image) of the drive.
  - Done for ALL separations of any kind.
- Monitor activity
  - Review Logs
  - Review file management
  - Review Anomalies
- Preservation of evidence

# BTK

- BTK eluded the authorities for 30+ years.
- He was completely unknown but had a habit of taunting the police with letters and notes.
- When he reemerged he was rapidly captured.  
Why? He didn't understand computer forensics.
- Information about his church was found on the diskette he sent police! This led to his arrest.

# Cleaning Disks

- DOD Wipes
  - Write 0s to entire disk
  - Write 1s to entire disk
  - Write random 0s and 1s to entire disk
  - Repeat 7 times
- You should be doing this to any drive that is being reused (well, at least, in some form)
- A single wipe of all 0's will produce the same results if security is not the real issue.

# What else does Forensics do

## ■ Password cracking

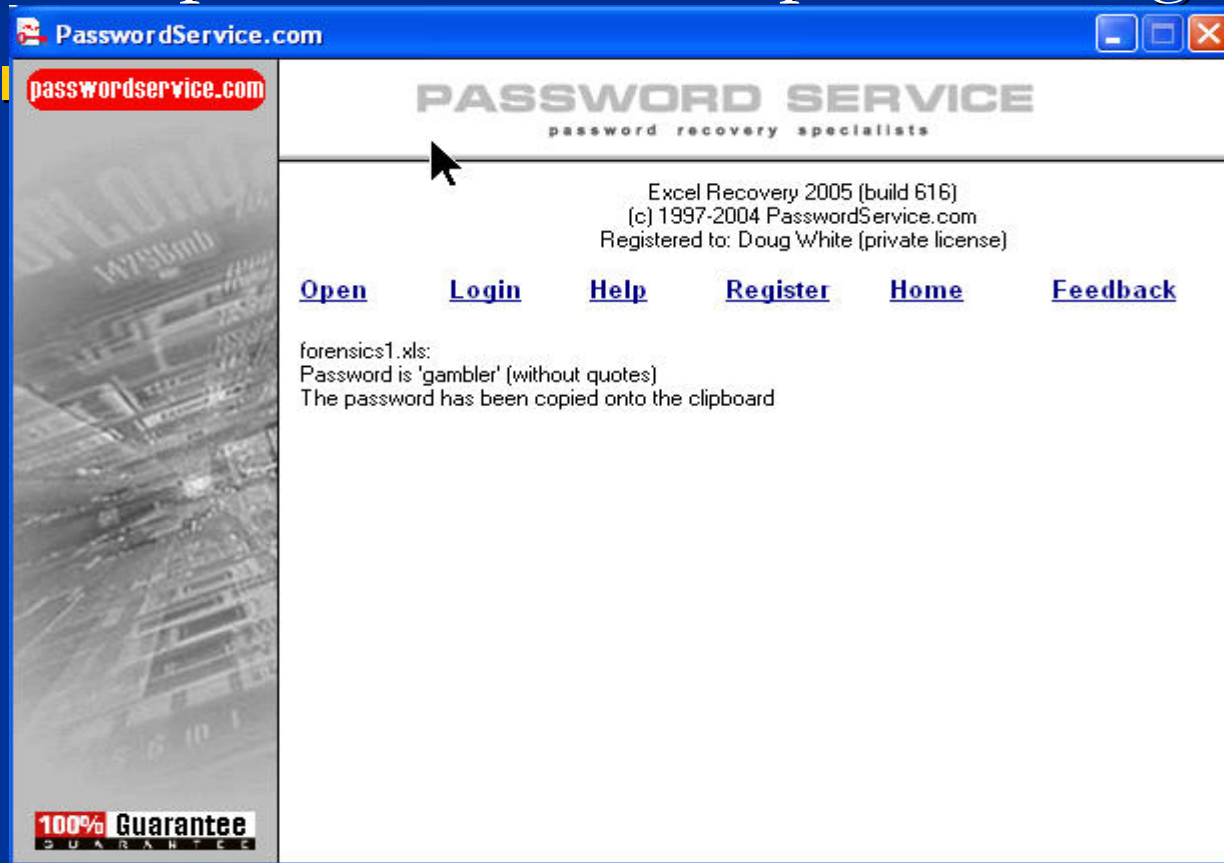
- Most files can be stored with a password to prevent their being opened.
- Most passwords can be cracked if you have enough time and computing power
  - Weak password – mypass
  - Strong password – h1yn\*YYmaiu90

## ■ Encryption cracking

- Encryption is a means of not only preventing the file from being opened but that actually transforms the plain text in a file into cipher text.
- Cracking encryption is the same as passwords only may take even more time to break depending on the algorithm used to encipher the text.

# First Example

- A spreadsheet with a password “gambler”



The screenshot shows a web browser window with the address bar displaying "PasswordService.com". The website header includes the logo "passwordservice.com" and the text "PASSWORD SERVICE password recovery specialists". A mouse cursor is positioned over the header. Below the header, the text reads: "Excel Recovery 2005 (build 616)", "(c) 1997-2004 PasswordService.com", and "Registered to: Doug White (private license)". A navigation menu contains links for "Open", "Login", "Help", "Register", "Home", and "Feedback". The main content area displays the results for "forensics1.xls": "Password is 'gambler' (without quotes)" and "The password has been copied onto the clipboard". A "100% Guarantee" badge is visible in the bottom left corner of the page.

# Why do you need this?

- Hostile employee encrypts a collection of spreadsheet as they depart
- A password is forgotten
- Data is being sent out to others via company mail and we need to determine it's nature.
- Hackers often password protect files they leave on your system. You may need to break the files just to see what they are ( be careful, it could be a trap!)

# Other cool stuff

- Steganography – Hiding information in image or other files.
- Take a JPG graphic and hide a text file in the graphic.
- This is an easy technique that can be done using s-tools, or any of the many other products floating around.
- Uses the bits in the colors that won't really impact the way it looks to store info.
- Hard to detect and requires much analysis to find the files. Not that likely due to technical issues but every 12 year hacker in the world knows how to steg a file on their website!

# Why Steg?

- Well, what if you could hide something in a picture on the web.
- You could hide gambling information, child pornography, drug information, or whatever you like on a completely innocent picture.

# Steg Example



# So what can forensics do for you

- Maintains images of employee media in a sound fashion
- Examines data to determine its legitimacy
- May assist in recovery of lost data or passwords
- May be required (imaging and wiping) to meet legal requirements
- May be the only option in the future

# Certifications

- CCE – Certified Computer Examiner
- [whitehatcce.com](http://whitehatcce.com) for online training

# Policy, policy, policy

- You must have existing policy in place to prevent issues.
  - Security policy – All material on company equipment may be reviewed at any time.
  - Imaging policy – All separations result in an image prior to the disk being wiped.

# Thanks

- [Doug.white@whitehatresearch.com](mailto:Doug.white@whitehatresearch.com)
- [www.whitehatresearch.com](http://www.whitehatresearch.com)
- [whitehatcce.com](http://whitehatcce.com)