

Computer Forensics

Doug White, PhD, CCE, CISSP
Roger Williams University
Networking and Security -- CIS

What do forensic examiners do?

- Collect Electronic evidence
- Examine Computers and other technology for clues
- Explain that evidence to others

Why do they do it?

- It's fun
- It solves crimes
- It develops complex evidence that would otherwise be missed

A quick example

- An employee of a company in a Western State is being stalked. She receives many initial offers of interest from aFriend@buhaoren.com.
- When she declines, the emails turn to threats and she disappears. There are no clues in her home or office and police are baffled as to where she went or why.

A quick example

- A review of her company account reveals the threats but who is aFriend?
- Example of samspace.org

What else?

- Did you know...
 - When you delete a file in windows it is not really deleted?
 - What happens to it?
 - Most people say, the trash can which is absolutely correct but what if you empty the trash can?

Surprise?

- Files in Microsoft systems (windows, etc.) are simply *Marked* for deletion.
- Now they look like
 - σyFile.doc instead of myFile.doc
- When the operating system sees this, it simply ignores files marked for deletion.
- When the space on the media is needed again, it may be used but until that time, the file is likely still there all we have to do is recreate it and we may be able to recover an entire disk if someone recently deleted everything on it.

Ok, but What else?

- How about Spy stuff?
- Forensics specialists often have to break passwords so they need to understand cryptography and how secrets are kept.
- Consider this secret message?
- ZHOFR PHWRU RJHUZ LOOLD PVXQL
YHUVL WBXXX
- Most people can figure this one out.

Answer

- It's a Caesar Cipher!
- This is a three letter shift so if we shift every letter by three:
 - Welcome to Roger Williams University.
- Computers can quickly try every combination of letters and see if any words emerge so cracking codes like this takes almost no time at all for a computer. Even more complex codes are quickly broken.

So can you crack a password?

- How do we get someone's password
 - Guess it or find it written down.
 - Use a dictionary attack (demo)
 - Use Brute Force – substitute every possible combination until something works.

One last spy trick

- Steganography – hiding something in plain site inside of something else.
- For instance, say you write a secret message on a canvas and then you paint a picture of puppies in oil on the canvas. Wipe away the oil and there is the message.

Steganography made simple

- Today, think about a digital file. It's made up of zeros and ones. What if not all the zeros and ones are important to the file?
- In most graphic files, music files, and other electronic storage, we can find areas that are unused. I can write messages in that space and hide things pretty well.
- Steganography example

Tools used today

- samspace.org
- passwordservice.com excel module
- wbstego4
- Contact me: doug.white@acm.org
- My Classes: cisweb.rwu.edu/dwhite
- My Company: www.whitehatresearch.com