



# **UNDERSTANDING COMPUTER FORENSICS**

**Doug White, PhD, CISSP, CCE**

**Security Assurance Studies**

**Roger Williams University**

## LET'S TALK ABOUT SERIAL KILLERS

- BTK – A serial killer who had numerous victims in the 70s and 80s and then disappeared.
- Taunted the police and media with letters but was not caught.
- When he returned in the 90s he sent taunts on a floppy disk. It was forensically examined and something that was hidden was found, the name of the church where Rader worked.



## WHAT ABOUT NOT SO SCARY STUFF?

- Have you ever taken a photo of something that happened:
  - An accident
  - A robbery
  - Two friends talking
- What about a text message?



# SUDDENLY...

- Almost any kind of legal case, civil or criminal, may have some kind of digital media involved.



## REAL EXAMPLE

- This was from a divorce case:
  - The husband was not only having an affair but was also slowly transferring funds from accounts he shared to off shore accounts.
  - How can you find this with computer forensics?
    - Evidence hidden on the disk
    - Evidence in chats, emails, files, letters, you name it.



# USB FORMAT EXAMPLE

- This USB key had a lot of files on it but now it's blank since I formatted it.
- If I use forensics techniques?



# WHAT DO EXAMINERS DO?

- Collect Forensics Evidence
- Attempt to find clues hidden or visible on digital media
- Interpret and explain evidence to non-technical persons



# WHAT HAPPENS WHEN YOU DELETE A FILE?

- Not much
- The file has the first letter of its name changed to  $\delta$
- It is marked for deletion. Even if you delete it from the trash can!
- The space on the disk may be used by other files now but not necessarily.



## WHAT ABOUT TEXTS?

- They may not be there, but we have often been able to recover parts of text messages as fragments on the hard drive.



# REAL WORLD

- How could someone recover a password from a program?
  - Software can allow you to perform
    - Dictionary Attacks – Trying words from the dictionary against the file
      - A password like hello will be pretty easy to break
      - A password like {mrSn00kum2sC@} will be really hard
    - Brute Force Attacks – Trying every possible combination of letters, symbols, and numbers until you get luck



## OTHER SPY STUFF

- What about secret codes?
  - ZHOFR PHWRU RJHUZ LOOLD PVXQL YHUVL  
WBABC
  - This is a secret code. Written in groups of 5 to make sure you can't guess letters.
  - Computers can quickly crack letter substitution codes (so can humans if they have that skill).
  - Let's try a caesar cipher
    - <http://secretcodebreaker.com/caesar.html>



# LETTER CIPHERS

- Crypto (cryptography) is the study of ciphers.
- Most any sort of substitution cipher can be broken quickly by computers who can try every letter until they start detecting legible words.
- When these ciphers were invented, most of the populace was illiterate so just writing something down was a kind of cipher.
- Today ciphers are very complex.



# MODERN CIPHERS

- Algorithms are used which are often math tricks to have a single input with a different output based on some key. The numbers and letters are processed as zeros and ones and shuffled, manipulated mathematically, shuffled some more, and then some ciphertext is output. This is called encryption.



## ONE MORE SPY TRICK

- Steganography – hiding things inside of other things.
- Consider you want to paint a picture making fun of fearless leader but if you get caught they send you to jail. So, what if you paint the picture and then paint another picture on top of it that will wash off?



## MODERN STEG

- Hide a file inside a file. There are often unused bits inside a file which are “reserved” or saved for future use.
- Consider the file icecream.txt
- What if I spent way too much time writing this nonsense and then used it to hide something.
- (the password is hellokitty and the algorithm is Rijndael)



# STEG

- Things can be hidden in pictures, music, video, anything if you have the right tool.



## SO WHAT DO FORENSICS EXAMINERS DO?

- In almost every court case, civil or criminal, they are involved in analysis of evidence and attempting to find the truth.
- Roger Williams offers a three course certification sequence in forensics and a major in security techniques (SAS) as well as a computer security major (Networking and Security)



# THANKS

## ○ We used:

- Passware toolkit ([www.lostpassword.com](http://www.lostpassword.com))
- Wbstego (<http://wbstego.wbailer.com/>)
- My Site ([www.whitehatresearch.com](http://www.whitehatresearch.com))
- Security Studies (SAS.RWU.EDU)
- My classes ([cisweb.rwu.edu/dwhite](http://cisweb.rwu.edu/dwhite))
- My email [doug.white@acm.org](mailto:doug.white@acm.org)
- Yvosyg kcf Hcanbu (Vigenere Cipher with foo for a cipher) <http://sharkysoft.com/misc/vigenere/>

