

Understanding Computer Forensics

Doug White, Phd, CISSP, CCE

Roger Williams University

Basic Ideas of Forensics

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

Some Basic Ideas About Files

- Microsoft
 - NTFS, FAT 32, and others
 - Files are not necessarily deleted when someone hits “delete”.
 - The first character in the collection of data is changed to a NULL and the section of storage is marked for deletion
 - Until that area of the media is needed, the file is still sitting there

Some Basic Ideas about Files

- Linux
 - EXT2, EXT3
 - EXT3 actually removes the files from the disk, thus no undelete. EXT2 works about like Windows

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

More Basic File Info

- Files are just long patterns of zeros and ones.
- If you process the pattern for a given file, you can obtain a “HASH” for that file.
- A HASH is a mathematical computation that results in a number, the hash, that is reproducible only for an identical file.
- Hashes created using the MD5 and SHA algorithms are admissible in court

So What does a HASH do for you

- A HASH validates evidence as being unchanged.
- If you confiscated my laptop and immediately hashed the hard drive, you could later prove, in court, that the hard drive had not been changed even if it was a copy!
- A HASH may be used to locate a known file, kiddie porn, that is on a disk. If the hash matches a known KP file, you have solid evidence.

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.

Example of Encryption

- Caesar Cipher – Shift all letters in the alphabet three spaces to the right
 - Plaintext: A B C D E F G H I J K L M N O P Q R
S T U V W X Y Z
Ciphertext: T U V W X Y Z A B C D E F G H I J
K L M N O P Q R S
- Time to break this with a modern cracker, about .01 seconds.
- Enigma and Purple

Example of CC

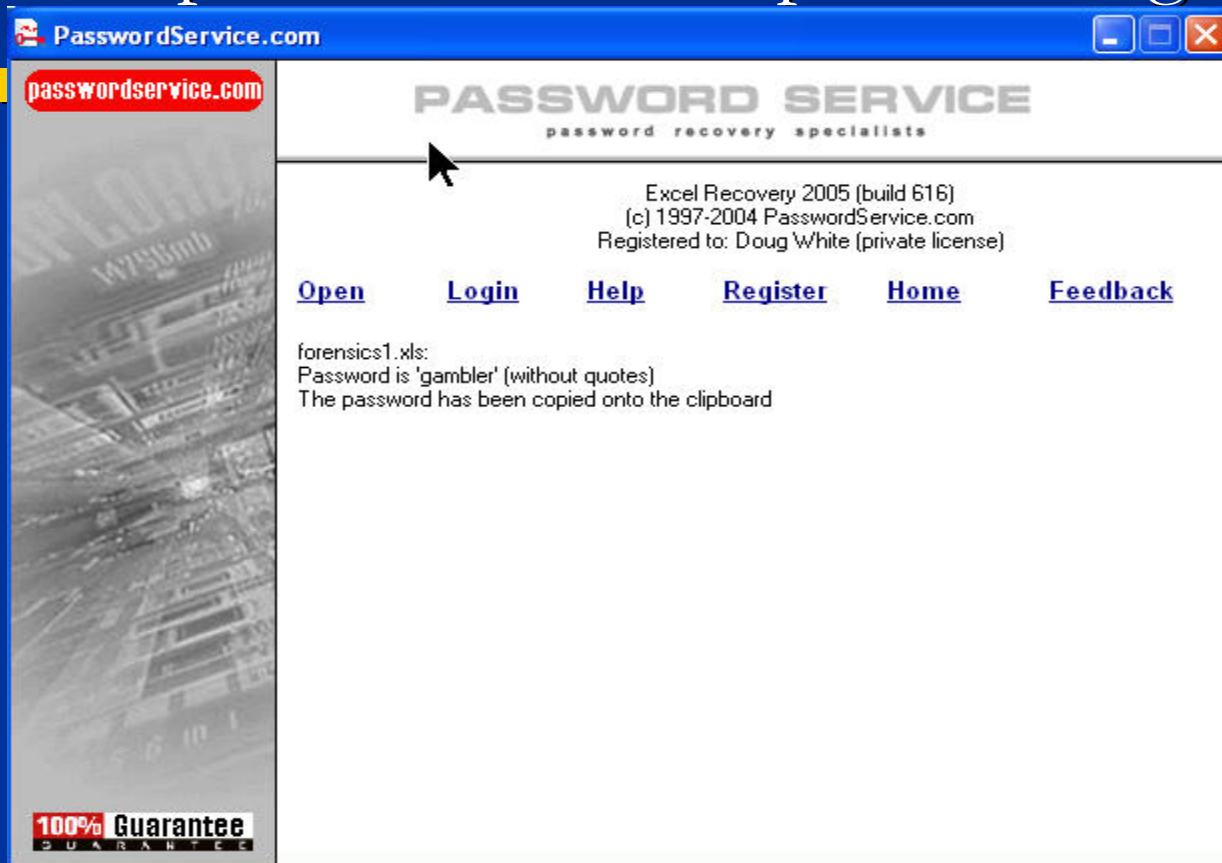
- I will attack at midnight
- B pbee tmmtvd tm fbwgbzam
- Bpbee tmmtv dtmfb wgbza mghfg

On the Other Hand

- Elliptic Curve Encryption – May take years to break depending on the amount of computing power brought to bear on the problem.

First Example

- A spreadsheet with a password “gambler”



Types of Cracking

- Dictionary Attacks
- Brute Force (substitution) attacks
- Gambler vs. G6mbl3R&

Other cool stuff

- Steganography – Hiding information in image or other files.
- Take a JPG graphic and hide a text file in the graphic.
- Consider the file stegtest and forensics.txt.
What if I hid the message in the seemingly harmless graphic, mysteg.bmp.
- Wbstego will let me extract the message file.

So what can forensics do for you

- Opens up new avenues of evidence
- Provides analysis of electronic media of all types
- May create additional/critical support for the case
- May create new leads
- May be the only option in the future

Certifications

- CCE – Certified Computer Examiner
- <http://www.certified-computer-examiner.com/>

Cautions

- *Verify Credentials*
- *Verify Degrees*

Thanks

- Doug.white@whitehatresearch.com
- www.whitehatresearch.com