

PRESENTATION TO CLASSICAL HIGH SCHOOL

Doug White
PhD, CISSP, CCE, PI(RI)
Director, Forensics, Applied Networking, and Security
Roger Williams University

COURT

- Witnesses

- Experts

- Daubert - You need to be able to be admitted as an expert in court.
 - Daubert means the judge decides if you will contribute something useful.
 - This could mean that a psychic is admitted

- Hearsay Evidence

- Can be inadmissible but it's complicated

THE CASE OF THE NAKED FISH MAN



CASE BREAKDOWN

- ⦿ Two parties - One male one female
- ⦿ Female complains of harassment by male
- ⦿ Male claims that female is a psycho stalker
- ⦿ Corporation wants to figure out who is the bad guy and fire them
- ⦿ Both parties are planning to sue for wrongful termination and hostile workplace

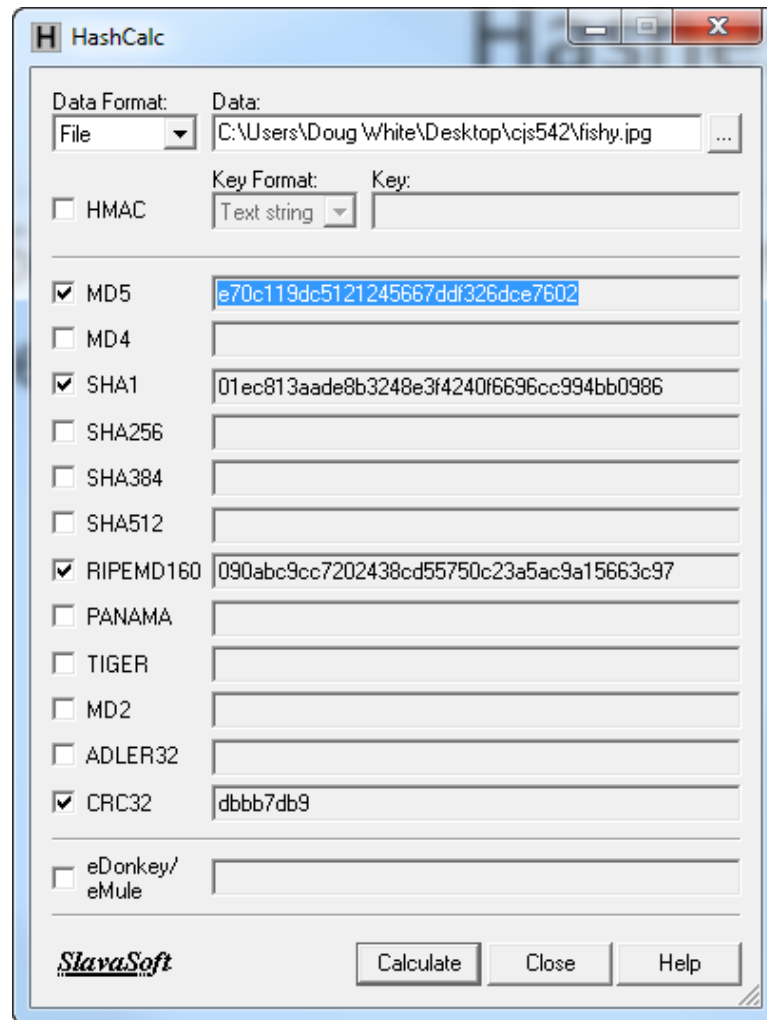
THE MAIN EVIDENCE

- A nude photo with the head replaced with a fish.
- Can we find this photo and prove that it belongs to someone?
- Female allows us to have a copy of her home system which contains one of the photos.
 - Male refuses
- Note: We were able to get a copy of the male's work machine since it belonged to the company.

HASHES

- MD5 hashes are like fingerprints of digital evidence.

HASHES OF FISHY



WHAT HAPPENED?

- On the males machine from work, we found a deleted file in the email folders which contained the fishy picture. The hashes match.

WHAT DO DIGITAL FORENSICS EXPERTS DO?

- ◉ Recover hidden, deleted data
- ◉ Open locked files
- ◉ Recover data from cell phones and other hand helds
- ◉ Preserve evidence for presentation later
- ◉ Analyze evidence to provide opinions

THE CASE OF THE BAD CEO

- ◉ Corporate Employee is under scrutiny for doing something possibly illegal.
- ◉ Claim is the CEO ordered him to hide the info from everyone so he did it!

WHAT HAPPENED?

- ◉ Obnoxious CEO in multi million dollar apartment tells us, “go ahead look at my laptop, you won’t find anything”.
- ◉ I ask for his phone and he calls his attorney
- ◉ I looked at the laptop and it looks like the drive has been wiped.
- ◉ We get tossed
- ◉ At the company we use a court order to obtain all his emails from the server.

EMAIL MESSAGE

- ⦿ “If you don’t put that under a stack of paper somewhere, we will both be looking for a job. Just do it” - CEO
- ⦿ “You understand this could be really bad if anyone finds this?” - Corporate Flunky
- ⦿ “Why do you think we’re using email, stupid.” -- CEO

TRAINING THAT MIGHT WORK

○ Typical

- Some sort of certification like the Certified Computer Examiner (ISFCE.ORG)
 - GCFA (sans.org)
 - CCFE (infosec.org)
 - Others
- Advanced Degrees
- Years and Years of Experience

CREDENTIALS FOR DFI

- ◉ CCE - Certified Computer Examiner
(isfce.org)
- ◉ CCFE - infosec.org
- ◉ GCFA - sans.org
- ◉ Etc.
- ◉ Advanced Degrees
- ◉ Work experience

WHERE DO YOU WORK?

- ◉ Police Agencies
- ◉ Corporations
- ◉ Law Firms
- ◉ Self Employed Consultants

DOUG WHITE

- ◉ First Programming Job in 1977 as a FORTRAN II programmer (part time high school job)
- ◉ Pen Tester and C Programmer Federal Reserve Bank of Atlanta
- ◉ President, Secure Technologies, LLC.
- ◉ PHD in Computer Information Systems and Statistics
- ◉ CCE (#30)
- ◉ CISSP - Certified Information Systems Security Professional
- ◉ Private Investigator (RI)

CONTACT

- ◉ dwhite@whitehatresearch.com
- ◉ 4016629781 text
- ◉ Slides @ www.whitehatresearch.com