

The Realm of Digital Forensics

ISACA – Malta Chapter
26th March 2009

Donald Tabone

Agenda

- Introducing Computer Forensics
- **Computer Forensics in the Real World**
- The cost vs. benefit perspective
- **Modern day challenges**

Digital Forensics

Where do we begin?

Introducing Computer Forensics..1

- Defining Computer Forensics
 - Is the systematic accumulation of digital evidence
- More than
 - Investigating computer-related incidents
 - Incident Response
- But
 - Collecting evidence and building a story that can be used in court – and if necessary lead to a conviction

Introducing Computer Forensics..1

- Laws for digital evidence were established in the late 1980's
- Identification, collection, preservation and analysis of digital information
- Information class: stored, transmitted and produced

Introducing Computer Forensics..2

- Defining the scope for CF
 - Disaster recovery vs. computer forensics
 - Fraud, embezzlement, pedophilia, harassment, industrial espionage, policy breaches
 - Email recovery and analysis
 - Preservation of evidence
 - Analysis of user activity
 - Password recovery
 - Tracing web browsing activities

Four Major Stages

- Acquisition
 - Admissible, Authentic, Complete, Reliable, Believable
- Identification
 - Cataloguing Digital Evidence, Bag-and-tag
- Evaluation
 - Searching for keywords, detecting file signatures, steganography, sector level analysis
- Presentation
 - Reporting without making assumptions,
 - Producing chain of custody log documentation,
 - Presentation in a court of law as an expert / technical witness

Computer Forensics in the real world

- Real world examples
 - TJX
 - The hackers who ransacked TJX Companies Inc.'s computer network and exposed at least 45.7 million credit and debit card holders to identity fraud reportedly began their assault by exploiting Wi-Fi weaknesses at a Marshalls clothing store near St. Paul, Minn.
 - Heartland Payment Systems
 - Heartland Payment Systems, a credit card processor, on January 20th, that up to 100 Million credit cards may have been disclosed in what is likely the largest data breach in history.
 - If accurate, such figures may make the Heartland incident one of the largest data breaches ever reported.
 - State Bank of India (SBI)
 - Mumbai: The State Bank of India, the country's largest bank, has had to shut down its corporate website after overseas hackers tried to break in.
 - The local scene?

The Cost vs. Benefit perspective

- Conducting digital forensics is expensive and time consuming and not always conclusive
- Companies must stand to gain from CF
 - Reputation. Bad publicity? e.g. credit card rating
 - Justice through the legal system for fraud
 - Reducing liability
- Political reasons
 - Official recording of events

Bottom line – how much do you stand to lose?

The Cost vs. Benefit perspective

“When it comes to creating adequate security **incident response procedures**, creating a feedback link that will lead to improving existing security practices and closing the gap between security policy creation and its enforcement, the answer is **yes** – investing in an enterprise electronic forensics program is probably the right thing to do.”

Milen Nikolov, IT consultant and trainer, Etisalat Academy

Modern day challenges..1

- Time is money!
 - And hard drives are becoming huge
- Technology evolutions
 - MD5 hash algorithm cracked!
 - The move to smarter mobile devices
 - The cost of keeping abreast with investigation hardware & software
- Multiple writes to secure delete, a myth?
 - Craig Wright, a forensics expert, claims to have put this legend finally to rest
- Anti-forensics groups and software
 - People are becoming a lot smarter as anti-forensic tools become more available

Modern day challenges..2

- Finding the right skills for an investigator
 - Intuitive and able to think outside the box
 - Technical expertise – a jack of all trades
 - Legal term understanding
 - Being a technical / expert witness in court
 - Discretion
 - Ethical
 - The ability to convey the concept to various individuals
- Full Disk Encryption (FDE)
 - Microsoft Bitlocker / PGP WDE
- Security concerns
 - Plausible Deniability e.g. Truecrypt

The keys to successful

Computer Forensics

- Informative documentation throughout
 - Transparent forensic procedures
 - Accuracy of process and content
- Preservation of evidence and chain of custody
- Continual research
- An aptitude towards being dynamic
- TIME!

Conclusion..

- The word 'forensics' literally means
 - A science that deals with the relation and application of a particular field
- Computer forensics is the science and discipline that is concerned with the relation and application of computers and legal issues
- The computer forensic professional...
 - ... is a cross between technician, programmer and investigator
 - a curiosity-oriented person who determines why and how past events occurred
- Computer forensics is used to uncover the proverbial 'smoking-gun'
- Changes to technology will cause growing pains for the profession

Food for thought..

- As the digital evolution becomes ever more predominant in today's world, can companies afford to not be diligent about evaluating risk?
- How much does your company stand to lose?

Understanding how records can be retrieved is instrumental in reducing the risk from unwanted discovery.

Can you anticipate your companies reaction?

Questions?

Thank you!

References

- (Craig Wright, Dave Kleiman, Shyaam Sundhar R. S.: Overwriting Hard Drive Data: The Great Wiping Controversy) <http://www.springerlink.com/content/408263ql11460147/>
- <http://www.h-online.com/security/Secure-deletion-a-single-overwrite-will-do-it--/news/112432>
- Digital Forensics Handout – Dr. Guillermo Francia III – Jacksonville State University
- Community of Computer Forensic Professionals <http://www.computerforensicsworld.com>
- Introducing Digital Forensics – Peter Sommer, London School of Economics
- Law, investigations and ethics – Kelly J Kuchta <http://www.lazarusalliance.com/horsewiki/images/d/d4/Computer-Forensics-Today.pdf>
- Is it really worth it? - Milen Nikolov, IT consultant and trainer, Etisalat Academy, 2007 <http://www.cpilive.net/v3/print.aspx?NID=1872>