

# SIRT & Forensics



Chris Gibson  
Global eCrime Lab Manager  
eCrime Unit  
Citigroup Security and Investigative Services  
[chris.gibson@citigroup.com](mailto:chris.gibson@citigroup.com)

# Chris Gibson

- Who I am:
  - I am not a lawyer
    - I will tell you what my lawyer has told me
    - You need to ask your own lawyer
  - I am not law enforcement
  - I am a forensic investigator
    - Strong on Windows, DOS, networks
    - Weak on Macs, AppleTalk, IPX...

# Agenda

- Why do forensics?
- What is "Computer Forensics"?
  - Principles
  - Process involved
- What are the issues involved?
  - Seizure
  - Chain of Custody
  - Forensic Tools
  - Findings and Conclusions

# Why do forensics?

- Proactive not reactive
- Intelligence
- Who, why, when, how,

# What is "Computer Forensics" ?

"It deals with the preservation, identification, extraction and documentation of computer evidence."

*[Anderson, Michael R., New Technologies, Inc., "Computer Forensics Defined"]*

Or, in other words...

Looking at the information on a computer or network to determine what a person was doing in the "electronic world"



# Computer Forensics is NOT:

- "Data recovery"
- Something that can be done with software alone
- Something that can be performed by anyone other than a computer forensic specialist

# How do we approach the Computer ?

It's a piece of the **CRIME  
SCENE !**

It's just another piece of  
evidence - though it  
needs special handling.



## Identification ?

- We want to identify and analyse the evidence to form one or more chronological sequences that fit the evidence
  - There may be more than one !
- Can't always be conclusive as computer evidence is circumstantial in nature

# Identification ?

- It is a feed back loop
  - Analysis leads to more evidence which feeds analysis

We want to do this in a  
legally acceptable manner

*It is a capital mistake to theorize before one has data. Insensibly one begins to twist facts to suit theories, instead of theories to suit facts.*

**Sherlock Holmes - A Scandal in Bohemia**

# Evidence Considerations

- **Admissibility**
  - Conform to legal requirements
- **Authenticity**
  - Records must not be altered, manipulated or damaged after they were created
- **Completeness**
  - Complete record, not extracts!
- **Reliability**
  - Collected and handled appropriately
- **Believability**
  - Believable and understandable

# Computer Evidence Characteristics

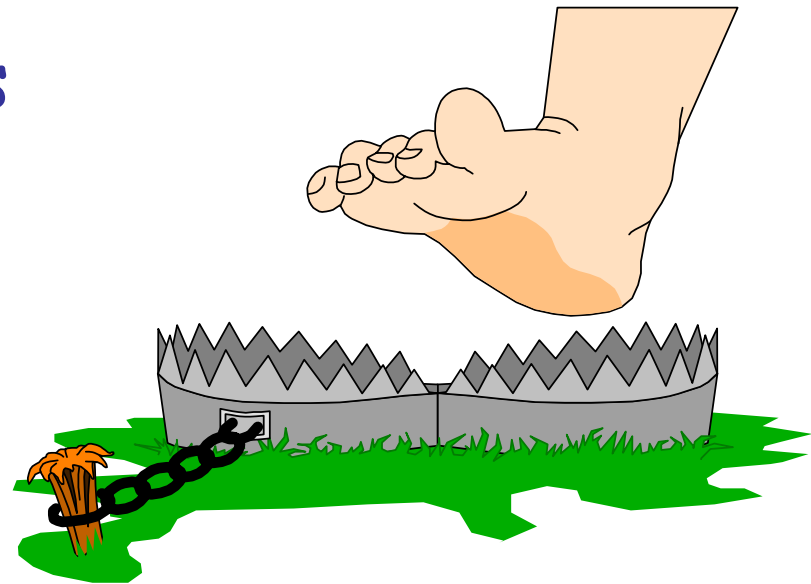
- Easily altered or deleted
- Invisibly and undetectably altered
- Stored in different format to that when it is printed or displayed (i.e. it is interpreted)
- Is generally difficult for a layman to understand

# Investigative Parameters

- Every investigation should be treated as if it will end in court
- The goals are:
  - Determine what happened
  - Determine the extent of the problem
  - Determine who was responsible

## So, where are the issues ?

- Seizure
- Chain of Custody
- Forensic Tools
- Findings and Conclusions



# Seizure?

- How do we “grab” the computer?
  - Is it turned on?
    - Is it doing anything?
  - Is it booby trapped?
  - Do we “Pull the Plug”?
    - What will we loose?

# Is it turned on ?

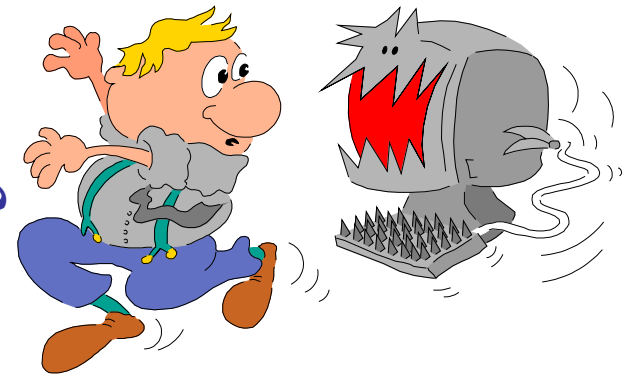
- What's it doing ?
  - Take a picture / notes of screen display / time (if possible)

- Is it booby trapped ?
  - Possibly set to erase data if

» a correct set of keys not used?

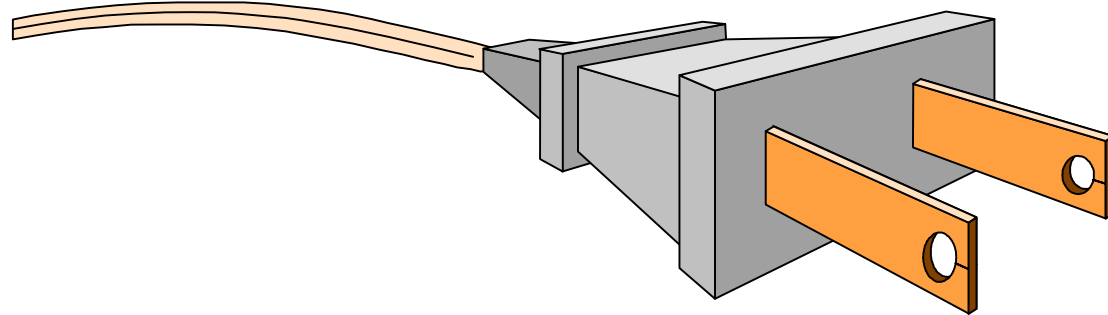
Or

» if network cable disconnected



# Pull the Plug?

- It depends.....
- What do we suspect the user of doing?
- What system is the user using?
- What's the level of competence of the user?



## Catch-22

- *Catch-22*: Anything and everything you do will change the state of the system
  - Power off? Changes it.
  - Take a a backup? Changes it.
  - Unplug the network? Changes it.
  - Even *Doing Nothing* will change the state of the system.

## What are the implications?

- Perform the analysis on a live system
  - OS/Utilities may have been modified
  - Least defensible in court
- But - *MAY* get more information
  - Connection status
  - Access to open data

## What are the implications?

- Perform the analysis on an image copy
  - Use known utilities
  - Most defensible in Court
- What if
  - the data is encrypted ?
  - the evidence was on a RAM drive?

## Chain of Custody

- Given the nature of the evidence (adaptable etc.) a common defence is to attempt to convince judge/jury that the data has been tampered with
- So you need a "rock solid" chain of custody

## Chain of Custody

- Who has had access to the evidence?
- What procedures did they follow in working with the evidence?
- How can we show that our analysis is based on copies that are identical to the original evidence?
- Answer: documentation, cryptographic hashes, timestamps

# Forensic Tools

- Many, many tools available
  - EnCase
    - [www.encase.com](http://www.encase.com)
  - Forensic Toolkit
    - [www.accessdata.com](http://www.accessdata.com)
  - New Technologies Inc. (NTI)
    - [www.forensics-intl.com/](http://www.forensics-intl.com/)
  - Forensic Toolkit
    - [www.foundstone.com/knowledge/forensics.html](http://www.foundstone.com/knowledge/forensics.html)
  - The Coroner's Toolkit
    - [www.porcupine.org/forensics/](http://www.porcupine.org/forensics/)
  - The @stake Sleuth Kit (TASK)
    - [www.atstake.com/research/tools/forensic/](http://www.atstake.com/research/tools/forensic/)
  - SMART
    - <http://www.asrdata.com/tools/>



# Tools

- Do these tools do what they say?
- Are they accepted within the forensic community?
- Are they accepted within the legal community?



## Have you tested them?

- Have you, personally, tested the tools?
- Do they do what they claim?

## Have you been trained in their use?

- Have you attended training?
- Do you understand how they work?
- Are you proficient in the use of the tool?

# Creating document findings and conclusions:

- Explaining findings in a way a judge and jury can understand
- Organizing data to clearly support conclusions
- Identifying and explaining exculpatory material
- Knowing how to address challenges to conclusions, software used, and processing methodologies

But, do not forget...

The evidence you may find implicates the computer - you still need to tie a person to the computer....

Whose fingers were on the keyboard...?



## Links

- Organisations
  - FIRST - [www.first.org](http://www.first.org)
- Web Sites
  - <http://www.ncjrs.org/pdffiles1/nij/187736.pdf>
  - <http://www.porcupine.org/forensics/>
  - <http://www.cftt.nist.gov/>
  - <http://staff.washington.edu/dittrich/forensics.html>
  - <http://www.crazytrain.com/content.html>
- Mailing Lists
  - <http://groups.yahoo.com/group/cftt/>



# Agenda

- Why do forensics?
- What is "Computer Forensics"?
  - Principles
  - Process involved
- What are the issues involved?
  - Seizure
  - Chain of Custody
  - Forensic Tools
  - Findings and Conclusions

# Questions?