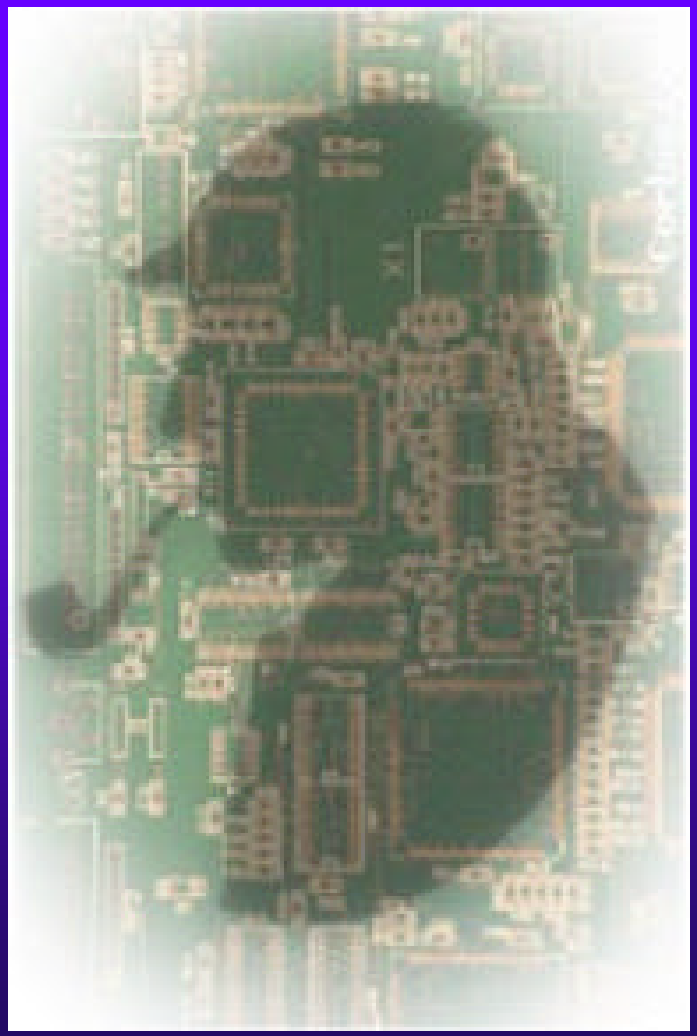
Introduction to Forensics 101

Joseph A. Juchniewicz
Security Analyst
AmeriCredit

The Game's Afoot…..



Today's Topics

- What is Forensics
- Is it right for your company's
- What are your company's needs
- Internal group vs. external contractor
- Training levels
- Available tools
- Computer Emergency Response Team

Forensics

Forensic – adj

[< Latin / forensis, public, of a forum]

1. Relating to, used in, or appropriate for courts of law or for public discussion or argumentation.

2. Of, relating to, or use in debate or argument; rhetorical.

Modern Forensics

- The examination of material and or data.
- To determine essential features and their relationship.
- A manner that is admissible in a court of law; post-mortem examination.

What is Forensics?

- History
  - China 700
  - China 1248
  - France 1609
  - Paris 1813

History….

- 1784 first documented use
- 1835 Scotland Yard's original Bow Street Runners
- 1860 Jack the Ripper

How to fight crime from TV

TV and Culture

- **The Nightly News**
- **Quincy**
- **Law and Order**
- **Homicide**
- **CSI**
- **24**

Different Names for Computer Forensics

- Computer forensic analysis
- Electronic discovery
- Electronic evidence discovery
- Digital discovery
- Data discovery
- Computer analysis
- Computer examination

Computer Crime

- Computer Assisted Crime
- Computer Specific or Targeted Crime
- Incidental

What Are Your Company's Needs

- Big, Small, Mom and Pop
- One building, Multiple campuses
- Continental US, International

What's Right for Your Company

The size of your organization should not determine whether or not you use computer forensics.

Education

- Education of management
- Education of employees/team members
- Don’t use scare tactics

Internal Group
vs.
External Contractor

Finding the Right Person for the Job

- Right person
- Background
- Training
- Equipment
- Cost

Pro's for Internal Personnel

- A trusted individual
- Always Available
- Flexible schedule
- Local law enforcement contacts

Pro's for Internal Personnel

- Part of training certification
- Knowledge of company network
- Knowledge of company's policy and procedures
- Quick response time
- Able to use as needed for other tasks

Con's for Internal Personnel

- Costly setup
- Have to purchase equipment
- Have to keep up certification
- Limited networking (at first)
- Have to play office politics
- Peer or management pressure

Pro's for Contract Personnel

- Don't have to pay for training
- Don't have to keep up certification
- Don't have to play office politics
- Don't have to purchase equipment

Pro's for Contract Personnel

- Have access to other specialized team members, or associations for additional help
- No peer or management pressure
- Software Knowledge

Con's for Contract Personnel

- Does not know the network
- Will have to relearn your systems every time
- Response time
- Limited use

Con's for Contract Personnel

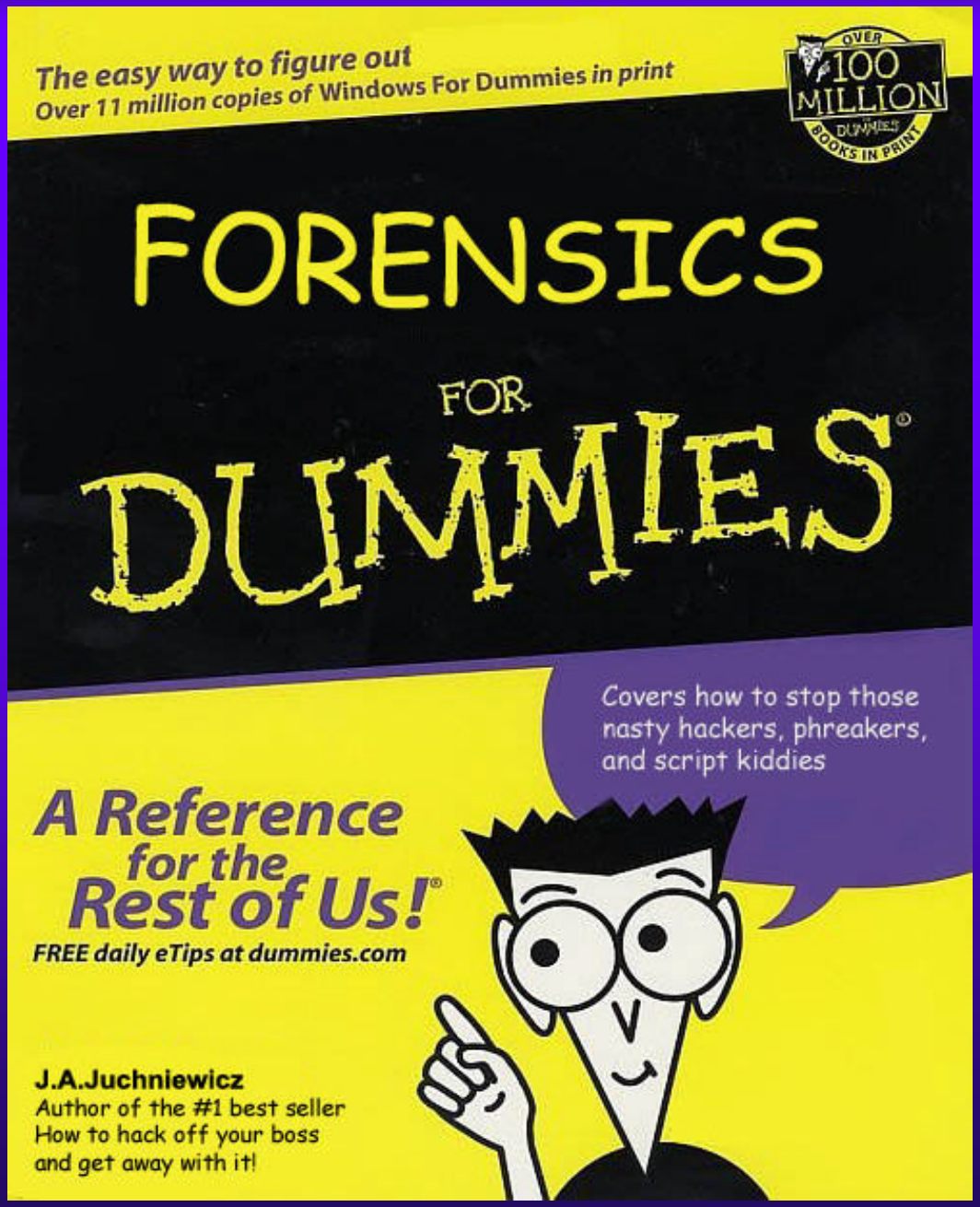
- Cost for service (per incident or on call)
- Restrictive time schedules
- Company software knowledge

Costs

- Classes $3,000 – $5,000
- Software $25,000
- Certifications and testing $150 - $1000
- Start up equipment $10,000 - $20,000
- External contractor $125-$200 an hour

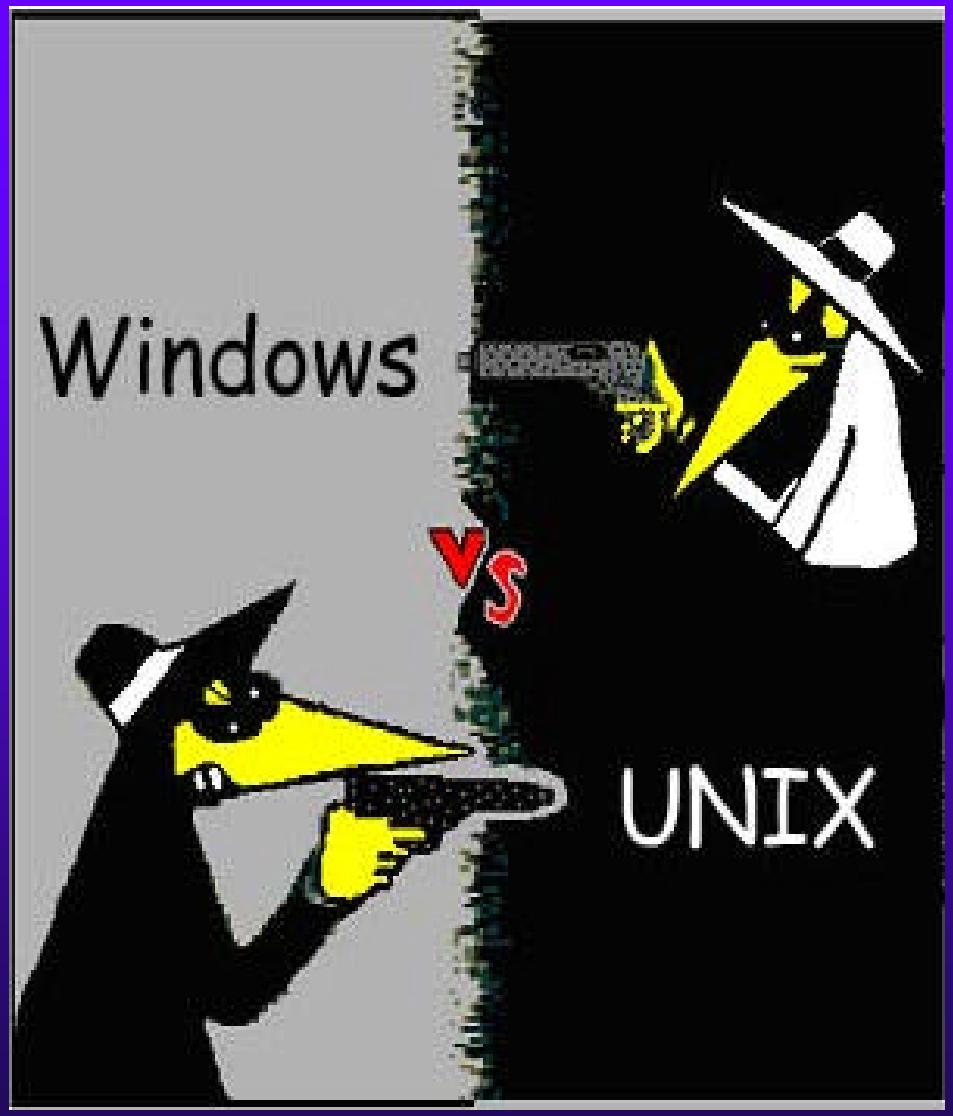
Training

- Traditionally, limited to law enforcement and special government agencies.
- A limited number of individuals in the corporate sector allowed to participate.
- Currently opened up to the corporate world.



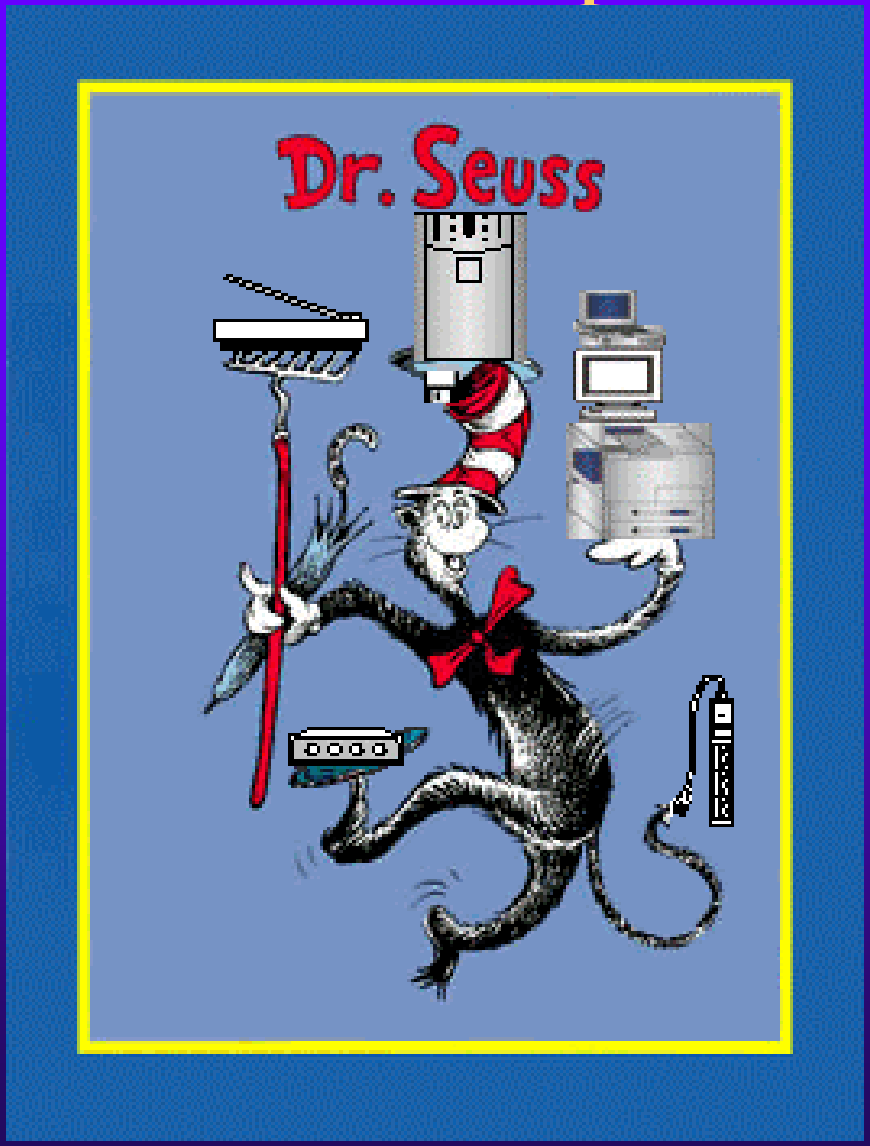
(The Dummies series of books is a trademark of IDG)

Windows vs. Unix



(Spy vs. spy is a trademark of Mad Magazine)

A Dr. Seuss Computer Story?



(Cat in the Hat is a trademark of Dr. Seuss)

Accrediting Organization and Accredited Classes

Your handout has a list of the different organizations.

Education

- John Hopkins University
- The University of Texas at Dallas
- Capital College
- University of Central Florida

Available Tools

A best of the best
list in your handout.

Computer Emergency Response Team

Friend or Foe??????????

Guidelines vs. Standards

- Establish a guideline and not standard.
- Standards are followed in a specific order (example items 1-10).
- Guideline is just that a guide, and you are not bound to follow them in any specific order.

Summary

Sun Tzu states

…if you know both the enemy and yourself, you will fight a hundred battles, without danger of defeat; if you are ignorant of the enemy but only know yourself, your chances of winning and losing are equal; if you know neither the enemy nor yourself, you will certainly be defeated in every battle.

(Sun Tzu, “The Art of War” p. 41)

Questions???

joe.juchniewicz@americredit.com