Forensics for Managers

Ryan Washington
MBA, CISSP, CCE, CEH, NSA/IAM

703-961-9456
Extension 128

Introduction

- US Marines, Special Intelligence Communicator
- Bachelors in Management
- Masters of Business Administration
- Solaris Administrator
- Computer Nerd

National-Louis University
Access. Innovation. Excellence.

SOLARIS™

KELLEY
School of Business

Crucial SECURITY

Purpose of Presentation

- Awareness
- Knowledge
- Attributes
- Key Terminology

MANAGER

SET LIST

1. berate anyone who's slightly late
2. unnecessary meeting
3. promote the unqualified
4. duck out at 3pm to play golf

NO ENCORE

What is/are Forensic(s)?

- "Computer Forensics is the application of the scientific method to **digital media** in order to establish **factual information** for judicial review. This process often involves investigating computer systems to determine whether they are or have been used for illegal or unauthorized activities. Mostly, computer forensics experts investigate **data storage devices**, either fixed like hard disks or removable like compact disks and solid state devices.

Southeast Computer Forensics and Security
http://secomputerforensics.com/index.php?option=com_content&task=view&id=20&Itemid=48

What is/are Forensic(s)? (continued)

Computer forensics experts:

- Identify sources of documentary or other digital evidence
- Preserve the evidence
- Analyze the evidence

What is it ***REALLY?***

- "Find Stuff"
- Deleted Files
- Corporate Theft

Crucial SECURITY

Key Terminology …sound like a pro

- Image
  - E01
  - .dd
- Unallocated Space
- Unused Space
- Carve
- Mount
- Logs
- Partition
- Root Kit
- Malware
- Steg
- Dongle
- Header
- Backdoor
- Hash
- Logical
- Physical

Why Do We *Need* Forensics?

- You Don't…
  - Or…DO you?
- Different Skill Set
- Intrusions
- Employee Theft
- Corporate Malfeasance
- Human Resources Matters

Who Wants Our Information?

- Governments
  - **Contractors**
  - **Secrets**
- Corporations
  - **Contractors**
  - **Secrets**
- Thieves
  - **Information**
  - **MONEY**

Crucial SECURITY

Why Would Someone Attack Us?

- Angry
- Make a Statement
- Random
- Weak Security
- Strong Security
- Paid

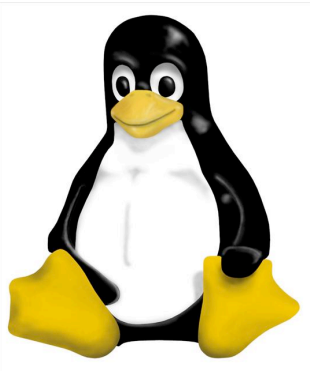
Crucial SECURITY

Tools

- Sleuthkit/Autopsy
- Wetstone Technologies
- ProDiscover
- Encase
- Forensic Toolkit (FTK)
- Paraben

Crucial SECURITY

Pricing on $oftware



Linux and Freeware

- PRO
  - Free
  - Open Source
  - Distributed
- CON
  - No Technical Assistance
  - More Man-hours
  - Deeper Trouble…

http://www.securityfocus.com/infocus/1503
http://www.tucofs.com/tucofs/tucofs.asp?mode=mainmenu
http://www.e-fense.com/helix/
http://fire.dmzs.com/
http://s-t-d.org/
http://www.opensourceforensics.org/tools/unix.html

F.I.R.E.

Wetstone Technologies

- PRO
  - Price
  - Easy to Use
  - Malware/Stego
- CON
  - Hashing
  - Basic

http://www.wetstonetech.com/f/index.htm

GEM-	**$995**
FPro-	**$1095**
Livewire	**$8995**

WetStone
A Division of Allen Corporation

Prodiscover

- PRO
  - Price
  - Perl *
- CON
  - "Pay per filesystem"
  - Pay for Perl ability
  - Pay for More

http://www.techpathways.com/DesktopDefault.aspx?tabindex=0&tabid=1

PD Win- $995
PD Forensic- $2195
PD Invest- $9995
PD IR- $12995

Crucial SECURITY

Technology Pathways ProDiscover® Computer Forensics

EnCase

- PRO
  - Robust
  - Market Share
  - Training
- CON
  - Price
  - Support
  - Enscript
  - Training

http://www.guidancesoftware.com/

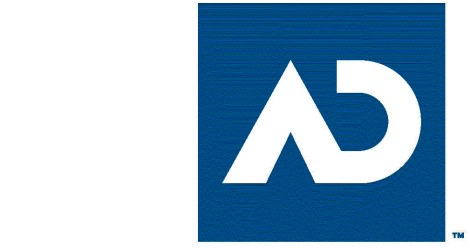
Forensic- $3700-7200
Enterprise- ~$200,000

AccessData FTK/UTK

- PRO
  - Price
  - Index
  - "Dummy Proofing"
- CON
  - False Sense of Completeness/Security
  - Heavy Upfront

http://www.accessdata.com/

FTK- $1095
UTK- $1949



AccessData®

Paraben

- PRO
  - Distributed
  - Price
- CON
  - Distributed
  - Training

http://www.paraben-forensics.com

Modules- $99-895
P2- $1495
P2 Enterprise $6995

Why Do These Tools Cost So Much?

- Cover Costs (of course…)
- Profit (of course…)
- Multi-Tasking
- Powerful
- "Easy to Use"
- Court Tested!!!
- Technical Assistance

mail is any indicator, users defend with religious zeal.

Since many organizations use multiple computer forensic tools, which one is "best" almost no longer matters. If you can afford the tool, it meets your needs, it produces acceptable results in the venue in which you are using it, and you have training and experience on it, then that tool probably is your best buy.

Where we are beginning to see real innovation is in what

Forensics Salaries ($USD)

- Junior
  - $60,000 - $80,000
- Mid-Level
  - $75,000 - $100,000
- Senior
  - $90,000 - $150,000
- "Well Known" Senior
  - $110,000 - $300,000

- Contractor/Independent/Hourly
  - Over $200,000

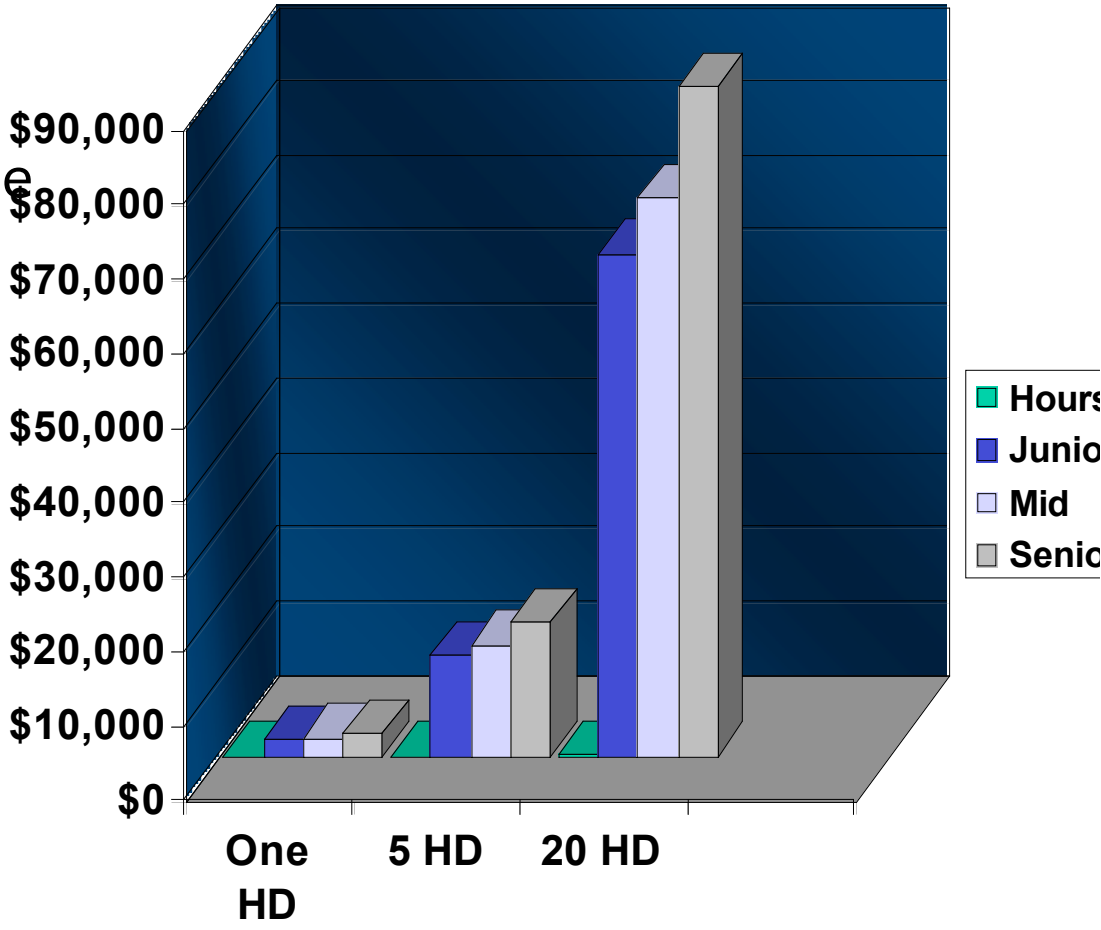
Hiring Considerations

- Experience
  - Where? When?
  - Commercial? Law Enforcement?
- Education
  - University? Learning Center? Discovery Channel?
- Certifications
  - CISSP, EnCE, ACE, GIAC, CCE, CFCE
- Personality
  - ?
  - Integrity
  - Honesty

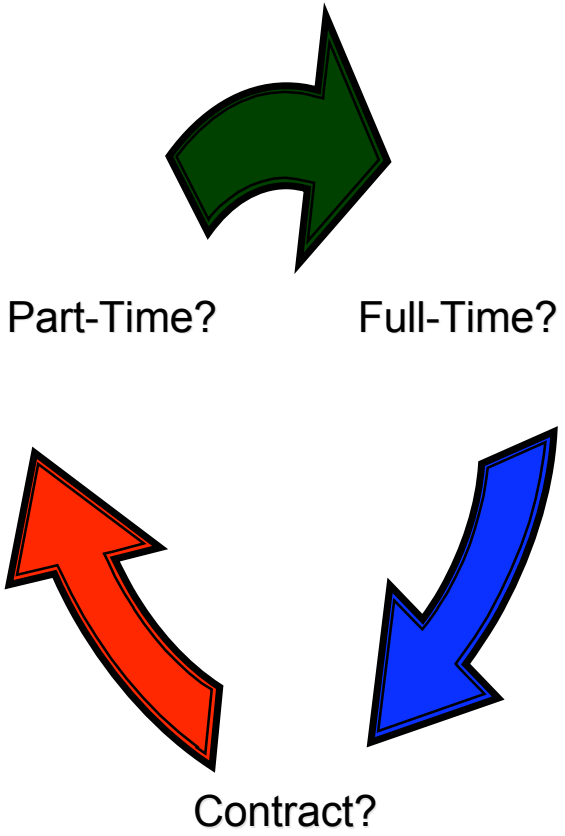
Crucial SECURITY

Time is Money… in a perfect world

- Hard Drive Size
- Expenses
- Level of Expertise
- Retainer
- Imaging Fee
- Admin Fee



Outsource or Hire?



Crucial SECURITY

“It wasn’t raining when Noah built the Ark.”

-Howard Ruff

Crucial SECURITY

Final Considerations

- How often are "Forensic Services" needed?
- Multi-tasked Person?
- Trusted Outsourced Company?
- Investigation Costs >, =, < Possible loss of data?

- Remember…You Get What You Pay For….

Crucial
SECURITY

Questions?

Crucial
SECURITY

Expertise. Integrity. Past Performance.

Ryan Washington
rwashington@crucialsecurity.com
Work 571-223-3426
Cell 571-437-3722