



# Computer Forensics: Error in Judgment

---

By

Scott A. Moulton

Forensic Strategy Services, LLC



# Case Experience

---

- Types of Cases:
  - Civil
  - Corporate
  - Law Enforcement
    - Secret Service
    - ICE (Immigrations and Customs)
    - State Agencies
    - Local Law Enforcement

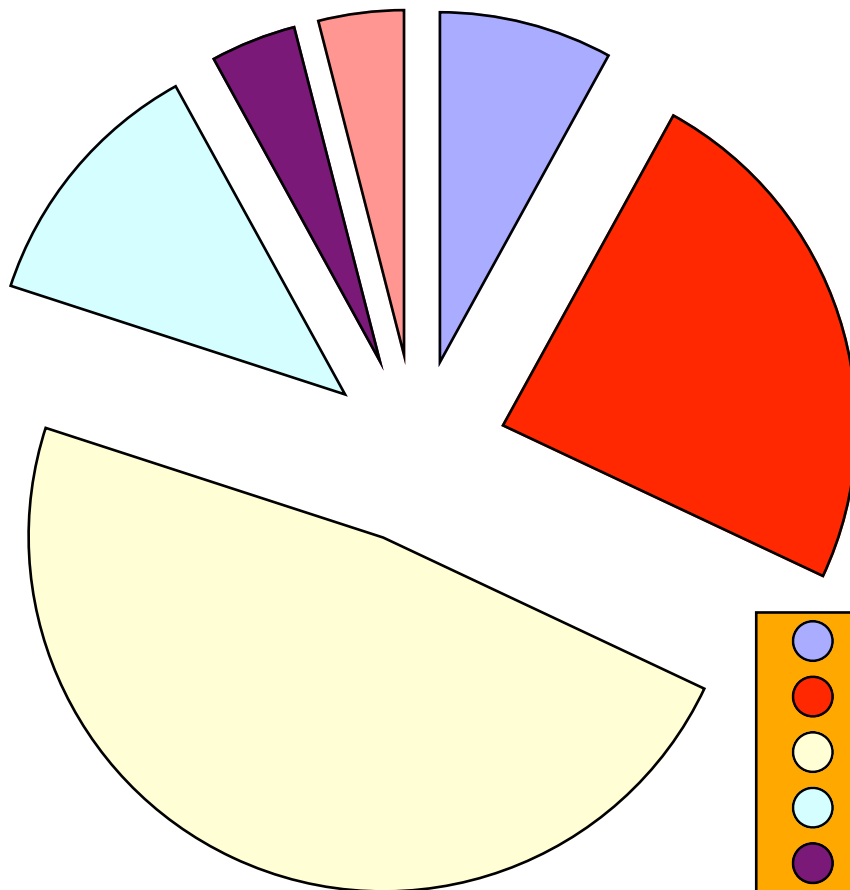


# Expanding The Role

---

## The First Responder

# Examining the Data from 25 Cases



50% First Responder Issues

35% Data Retention Issues

15% Quality Control Issues

- Corrupted the Image and Turn on
- Backup Problems
- Imaging done incorrectly
- Gave us the wrong Image
- Encase Data was Incorrect
- Log files never reviewed



# Why “Error in Judgment?”

---

If these issues are not addressed,  
one day soon there will be someone pointing  
a finger at you stating that YOU made an

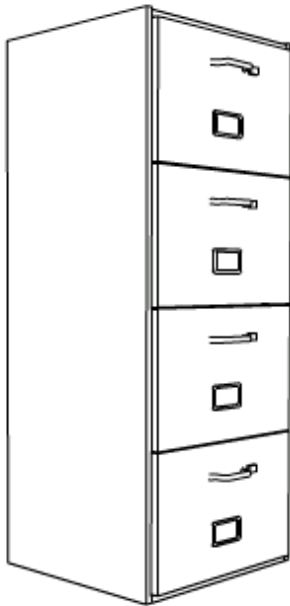
“Error in Judgment!”

- 
- [ **First Responder**
  - [ **Data Retention**
  - [ **Quality Control**

# Why I am telling you this?

---

- Not enough attention is being paid to the position of the first responder and the plan supporting the categories that effect that job.



- This will cause major problems as laws and compliance issues come into play and you will not be able to defend your case.
- You can benefit by knowing and addressing the issue BEFORE they are a problem for you!



## Scary Conversation

---

- Q: Have you assigned and trained someone as a first responder.
- Hospital IT Admin A: What's that?

— [ **First Responder**

— [ **Data Retention**

— [ **Quality Control**



# What is a First Responder?

---

Refers to the first person that will approach and access the system once the incident or event has been reported. That person is responsible for containment and integrity of system/s for examination.

- source: Win2K First Responder's Guide H. Carvey 2002-09-05

## What usually happens

---

An alarming number of admins tend to just run McAfee, SpyBot and AdAware when they receive a security notice from us. They don't think about the protected data on the machine (FERPA/HIPAA/etc) that may need to be analyzed to determine if it has been accessed. All that leads into the bigger issue of what if a security incident leads to a civil/criminal case.

Email from a System Admin....:)





## Why do you (should you) care?

---

- ..how **routine administrative tasks can affect both the forensic process** ability to recover data and analysis of a security incident.
- HIPAA, Sarbanes-Oxley, California Act 1798, FERPA, FRCP, compliance issues .... all of which hold **businesses civilly** and, in some cases, **criminally liable**



## Why does it go wrong?

---

- Inexperience & Distractions
- Proper Training & People
- Viewed as **GRUNT** Work!??



— [ **Case Examples** ]



## Case Examples: Names changed....

---

Three Letter Organizations/LE are now referred to as:

**"G-Man"**

Corporate IT Administrators are now referred to as:

**"Busy-Man"**



# First Responder Case Examples

---

## Install your OWN Rootkit!

- Fortune 500 company server had back door access on a separate T1 they did not know about and had IIS installed with no patches, no firewall.
- The Busy-Man searched and installed several rootkit detection tools to determine if access to the server was severe and went home as it was 5 pm.



# First Responder Case Examples

---

## Install your OWN Rootkit!

- One of the **rootkit detection** utilities the Busy-Man installed WAS **malware rootkit** and **rooted** the machine he installed it on.
- By the time it was realized there were additional compromises on the entire network originating from this one machine and they had to report on all the machines.



## Conclusion

---

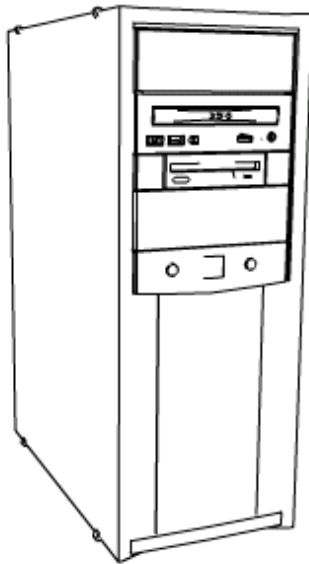
### Install your OWN Rootkit!

- The company had to report very negative findings that made the newspaper.
- The Busy-Man was fired and he is not busy anymore.

# First Responder Case Examples

---

## How NOT to RIP Some CDs!

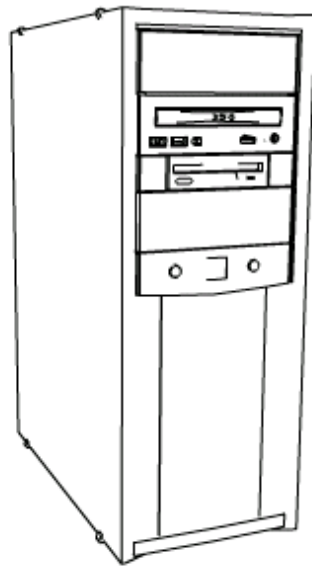


Before imaging a confiscated computer in a criminal case, a G-Man **turned the computer on**, copied files to a folder on the hard drive and used it to **burned several CD's**.

# Conclusion

---

## How NOT to RIP Some CDs!



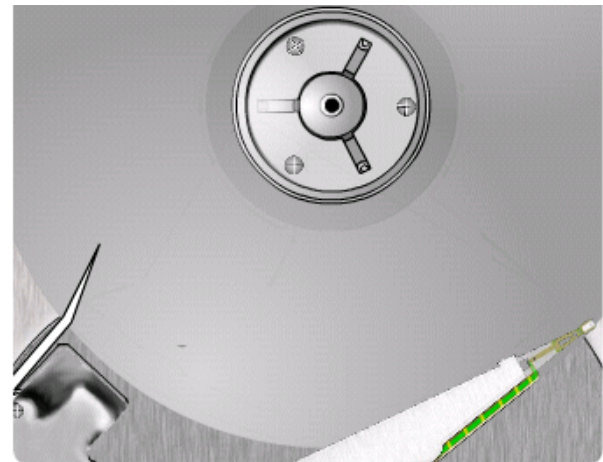
- The G-Man was rather embarrassed in court!
- The evidence was eliminated from court.

# First Responder Case Examples

---

## Go Clone Yourself!

- G-Man hooked up a drive to imaging machine and booted.
- G-Man then typed in the commands to image the drive.



# First Responder Case Examples

---

## Go Clone Yourself!

- G-Man then selected to image the evidence drive onto **itself** and did not realize this until all **free space** had been **overwritten** with itself.



# Conclusion

## Go Clone Yourself!

- The evidence was eliminated from court.





## How to Fix the Problems?

---

- To save the best forensic people for reviewing evidence the task is assigned to the **newest person or lowest cost person.**
- Don't assign the person with the **least experience to first responder!**



— [ First Responder

— [ **Data Retention**

— [ Quality Control



# Why Data Retention is a problem!

---

- This is sometimes the most difficult job because you usually **don't realize** there is a problem until it is too late.
- Equipment for complete proper backup and long term storage is **expensive**.
- Very few **tests** are ever run to determine what is stored is able to be **restored!**



# Reasons it's a problem for First Responders!

---

- First Responders job is to secure evidence. That is really difficult if there is **NO** evidence to secure.
- Usually the first responder was **not included** in the process of what is being backed up, where it is being backed up and what is not being included. First Responder is treated as an **Outsider**.



# Federal Rules for Civil Procedure

---

- This will **require** that litigation **meet** early in any case to discuss **electronic discovery** and preservation.
- FRCP rules have a major impact on companies' storage and retention policies and it will be **contested in COURT** if it is found to be unreliable or incomplete.



## Who has reviewed FRCP?

---

- Poll taken by the American Bar Association on electronic data management, electronic discovery, and the proposed changes to the Federal Rules of Civil Procedure, over **80%\*** of Corporate Counsel members are **not aware of or familiar** with the e-discovery amendments.
- **77%** had at least one lawsuit since 2000 that involved an **e-discovery request** in which their organization was the **defendant**.

<http://www.pglewis.com/newsletter/mar05/mar2005recentdecision.html>



---

# [ Case Examples



## Data Retention Examples:

---

- Insurance Company where tape backups are not stored monthly but only in looped weekly cycles.
- A litigation case demanding emails back to last year, but they have all been overwritten.
- Busy-Man claims boss would not spend the money on the tapes to store them away.
- Now he spends money on **Lawyers.**



## Data Retention Examples:

---

- Financial stock company who had already been investigated by the SEC were ordered to keep copies of emails up to seven years.
- During upgrades to their servers, the company owner felt the IT person was expensive and fired them. No one was assigned or took over maintaining backup copies.
- Now being **fined by the SEC.**



## Data Retention Examples:

---

- Fortune 500 company in which HIPAA requires two hands on equipment at all times.
- Raid 5 drives failed and appeared to be forced back online causing corruption in financial files "interleaving" them together.
- Backup? Busy-Man says no one told them anything important was on this server so they never backed it up.
- They were **fin**ed for being late on their quarterly financials.



## How to Fix the Problems?

---

- No one conducts a complete inventory of DATA. **Someone needs to track DATA and document it!**
- All backups fail consistently. **Responsible review and often!**
- Tech / Legal / Management / HR camps are separated and seldom consolidate meetings on these topics. **Figure this out together!**



— [ **First Responder**

— [ **Data Retention**

— [ **Quality Control**



## Quality Control Issues

---

- No one is double checking all of these items and making sure that they are getting done.
- The person WHO is responsible for this process (if there is one), often reports to no one for review.
- There is never a simulation or “fire drill” to verify what is being done works.



---

# [ Case Examples



# Quality Control Case Examples

---

## Forget about it!

- G-Man had 10 drives on the evidence confiscation forms.
- Evidence had 10 images but one drive was **imaged twice** and one drive was just plain forgotten!
- One of the images provided was not even the client, **had nothing to do with the case** and was acquired in a completely different year.



## Now where was that evidence?

---

- Servers retain log files. An ISP viewed what they thought was a break-in at a government site and called the G-Man.
- G-Man took out a warrant based on the content of the log files.
- In **depositions** when asked where the log files were the G-Man said that **no one had ever seen them**.
- G-Man never even looked at the logs, he just took someone's word for it and arrested the person! Oops.



# Quality Control on User Accounts

---

- Government Facility could not find evidence of wrongdoing but something was going on when no one was in office. Security and permissions were changed and logs were destroyed on a daily basis.
- Every Users was setup as **Administrator** in the Domain. **Outbound** connections were not tracked at **ALL** and tools like LogMeIn and GoToMyPC were able to go outbound without notice.



## How to Fix the Problems?

---

Assign someone to be the control point and to schedule time for them to verify and review controls to make sure they are actually getting done.

**And NOT the lawyer!**



— [ **First Responder**

— [ **Data Retention**

— [ **Quality Control**



# Reviewing the Fixes!

---

- If the proper people were in place, with the proper education and experience, there would be far less errors in a crisis or in the event of litigation.
- Most problems can be solved by working with the divisions in the company and designing a plan and reviewing it often.
- If the plans were designed around an inventory of DATA and protecting it, the operation would be more effective.

EOF

**Scott A. Moulton**  
Forensic Strategy Services, LLC  
[www.ForensicStrategy.com](http://www.ForensicStrategy.com)