



## **Information Forensics and Electronic Investigation:**

### **Identifying Sources and Roles of Digital Evidence in an Investigation**

**Aaron Hughes, CISSP  
Vidoc Razor, LLC**



# DEFINITIONS

**Incident Response**

**Forensics**

Network Forensics

Live Stream

Processing Stream

Data Forensics v. Information Forensics

**Digital Investigation**



# It's Cool - But Is It Science?

Characteristics of Science:

Can be replicated  
(Same skill, equipment, etc.)

Uses Scientific Method

- Observation,
- Hypothesis,
- Prediction,
- Experimentation,
- Conclusion/Reporting





# It's Cool - But Is It Science?

## **Characteristics of Data Forensics:**

Replication is critical

Testing is most often “non-destructive”  
(Some notable exceptions)

Results and locations should remain the same



# Where the Data Things Are...

## Information Sources and What they Might Mean:

File and Email Servers, Network Infrastructure –

Mostly safe from a privacy standpoint (except email)

Investigative Role:

Typically Focused on Organization behaviors: Useful for determining WHO to start with



# Where the Data Things Are...

## Information Sources and What they Might Mean:

PCs, Laptops

Getting Risky

- State of Mind” Behavior: File access, Network Activity, Internet Activity

**Focused on the Individual's Behavior**



# Where the Data Things Are...

## Information Sources and What they Might Mean:

Cell Phones, PDAs, Other Mobile Devices (may include a laptop or desktop if home use is involved)

High Risk

Shows the user in their “Natural Environment”



# It Can Be So Much More

## **Forensics Beyond the Hard Drive**

- Email
- Webmail
- Newsgroups/Social Networking Sites
- Posted pictures
- Personal Mobile Devices (iPhones, Cell Phones, Kindles)
- Other electronic devices: Gaming Systems, Electronic Recorders, ???



# State of the Science...

Your Forensic-Fu might be bad if:  
(recognize any of these?)

10. No chain of custody
9. No evidence preservation steps (multi-layered)
8. Lack of “approach” strategy
7. Incomplete reporting
6. Lack of inventory control
5. Vague references with no backing



# State of the Science...

Your Forensic-Fu might be bad if:  
(recognize any of these?)

4. PI License (If private company)
3. “Single Prong Approach”
2. Lack of understanding of basic legal principles
1. Incomplete reporting  
(I know - I mentioned this already... but it is important!)



Aaron Hughes, CISSP  
Vidoc Razor, LLC

[Aaron.Hughes@VidocRazor.com](mailto:Aaron.Hughes@VidocRazor.com)

[www.VidocRazor.com](http://www.VidocRazor.com)

[Inforensics.VidocRazor.com](http://Inforensics.VidocRazor.com)

[www.Twitter.com/VidocRazor](http://www.Twitter.com/VidocRazor)