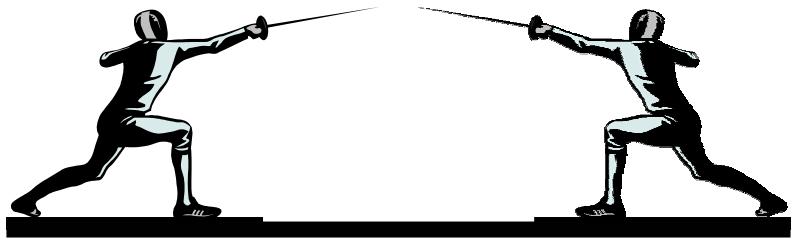
Putting the Horse Back in Front of the Cart

At The Crossroads: Taking Our Rightful Place in the Forensic Community

Peter Stephenson, CPE, CISSP, CISM, CIFI, FICAF
Executive Director, The International Institute for Digital Forensic Studies

The International Institute for Digital Forensic Studies

There is a religious war raging in the digital investigative community:



Is digital forensics art, technology or science?

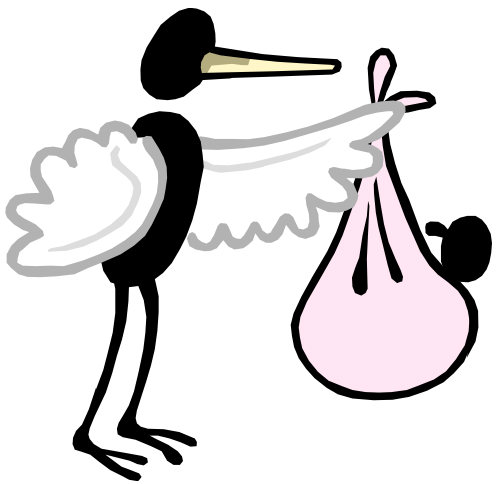
Specific Problems We Want to Solve

- Inconsistency in forensic analysis of digital events
- Inconsistencies in interpreting digital evidence in complex attacks
- Inconsistencies in representing results of digital investigations
- Incomplete or unsupported evidence chains in complex digital investigations possibly leading to erroneous conclusions
- Current tendency to focus upon specific platforms or environments instead of a generalized process

The Challenges

1. Nature of digital forensics and digital investigation
2. To certify or not to certify
   - Labs and practitioners
3. Education and training at all levels
4. The communities we serve
5. A common language
6. Consistency of process

Challenge #1: Science - Returning to First Principles



- Agreed-upon characteristics[1]
  - Theory: *a body of statements and principles that attempts to explain how things work*
  - Abstractions and models: *considerations beyond the obvious, factual, or observed*
  - Elements of practice: *related technologies, tools, and methods*
  - Corpus of literature and professional practice
  - Confidence and trust in results: *usefulness and purpose*
- Common ground between theoretical and forensic science is reliable methods of inquiry[2]
  - Integrity
  - Competence
  - Defensible technique
  - Relevant experience

[1] "A Road Map for Digital Forensic Research" 6th November 2001, The Digital Forensic Research Work Shop

[2] Forensic Science – An Introduction to Scientific and Investigative Techniques ed. James and Nordby

Reliable Methods[2]

- Help distinguish evidence from coincidence without ambiguity.
- Allow alternative results to be ranked by some principle basic to the sciences applied.
- Allow for certainty considerations wherever appropriate through the ranking of relevant available alternatives.
- Disallow hypotheses more extraordinary than the facts themselves.
- Pursue general impressions to the level of specific details.
- Pursue testing by breaking hypotheses (alternative explanations) into their smallest logical components, risking one part at a time.
- Allow tests either to prove or disprove alternative explanations (hypotheses).

"Whatever the scientific investigation at issue, how one's scientific opinion is constructed mirrors the certainty of the result.

Certainty, in the medical and scientific sense, Remains determined by the method of derivation applied in the investigation.

Medical and scientific certainty remains distinctly independent from either absolute certainty or mere mathematical probability."

*- - Jon Nordby, PhD, D-ABMDI**

*Diplomate - American Board of Medicolegal Death Investigators

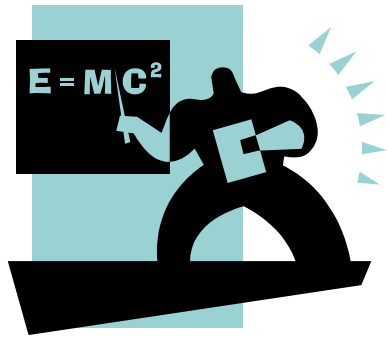
Digital Investigation Exhibits all Three Characteristics

- Art
  - The intuition of the investigator or analyst
- Technology
  - The reliable methods, tools and techniques used by practitioners
- Science
  - The well-spring of the technology
  - The structured approach used by practitioners
  - The structured framework of digital forensics and the digital investigative process
  - Integrity, competence, defensible technique, relevant experience
  - Court tested through Daubert and others

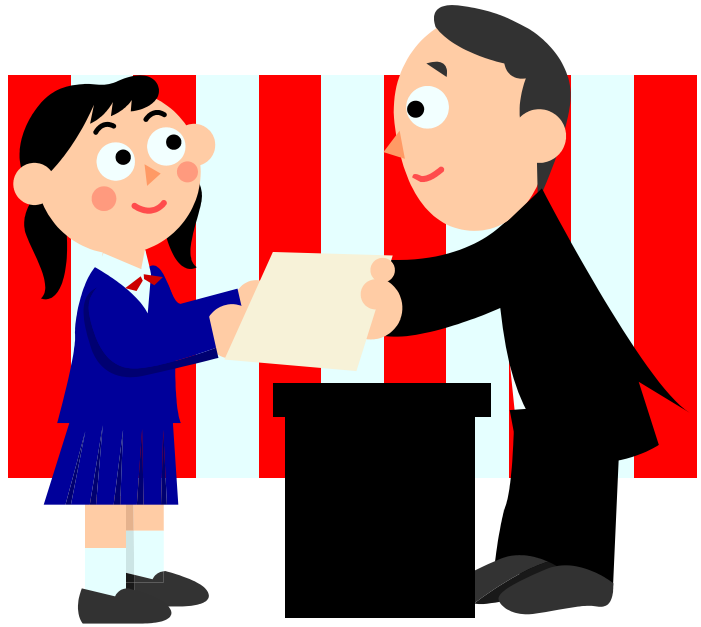
We Must, All of Us…

- …Exhibit the characteristics of integrity, competence, defensible technique and relevant experience
- …Depend upon reliable methods of inquiry
- …Strive for consistency and reliability in process
- …Apply the basic scientific method of forming an hypothesis and testing it with evidence

We Must, Therefore, All of Us, Become Scientists



Challenge #2: To Certify or Not To Certify



A Few Questions

- Can we have practitioners for whom the lay consumer has no reliable way of verifying experience?
- Can we have tools that the consumer has no way reliable way of verifying applicability to the forensic task?
- Can we have facilities for which there is reliable way to verify scope of true capability?

If our discipline permits any of these, can we truly take our place with the other forensic sciences?

Two Final Questions for this Challenge

1. What are the relative roles of vendor certification and industry certification
2. Who performs certification?

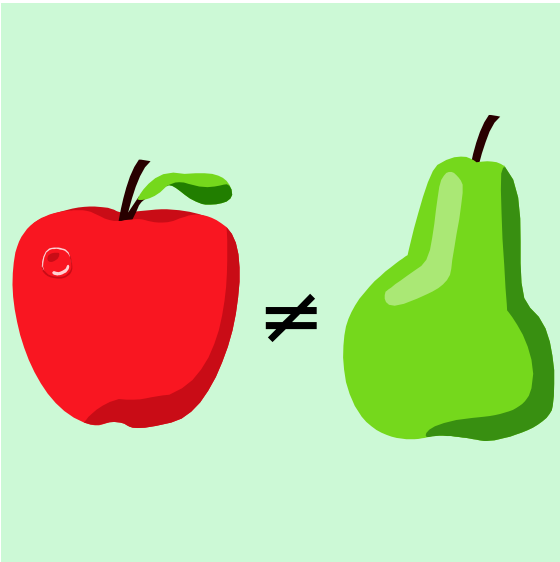
Challenge #3: Training and Education

Where Do Training and Education Come From?

- Training
  - Vendor training programs
  - Community colleges
  - Law enforcement academies
  - Law enforcement training organizations
- Education
  - Universities
- Who is training and certifying the trainers and educators?
- Where is the money for training and education coming from?
- Are we doing a good enough job of training and education? How would we know?

Challenge #4: What Communities Do We Serve?

Challenge #5: A Common Language



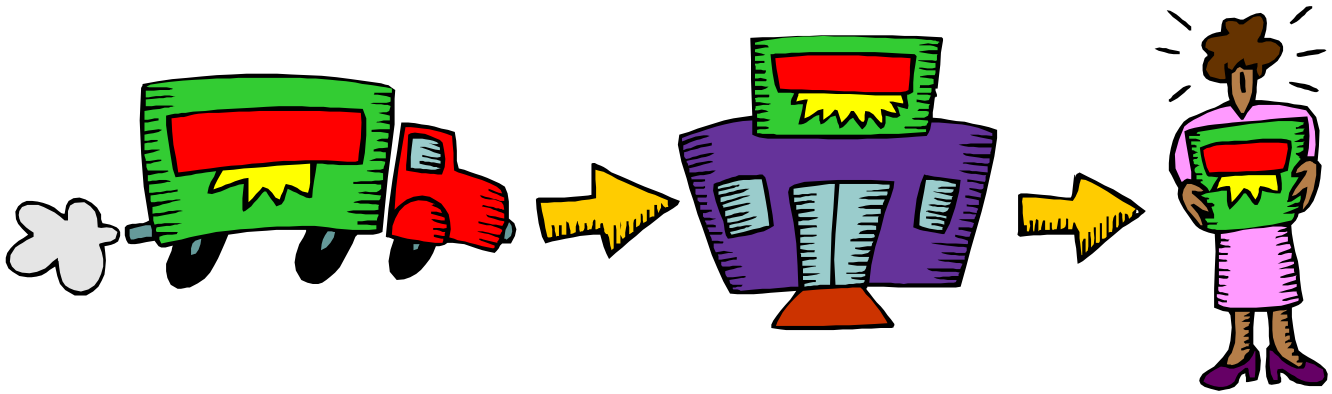
Starting Point: A Simple Definition

Digital Forensic Science is the Application of Computer Science and Mathematics to Matters of Law.

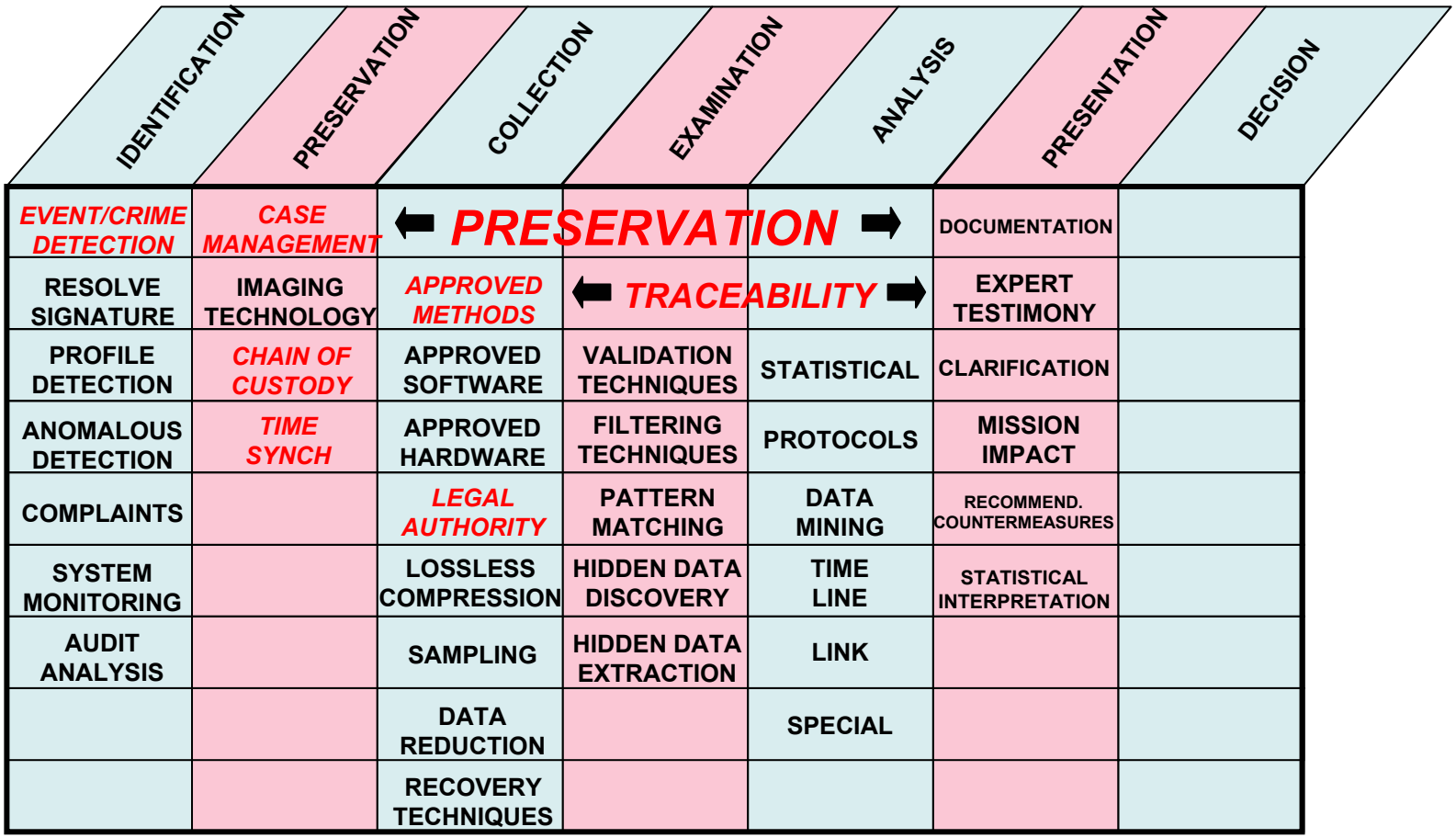
Semantically, digital forensic science includes:

- ✓ Computer forensics
- ✓ Network forensics
- ✓ Information forensics
- ✓ Software forensics

Challenge #6: Consistency of Process



Starting Point: A Comprehensive Framework[1]



IDENTIFICATION	PRESERVATION	COLLECTION	EXAMINATION	ANALYSIS	PRESENTATION	DECISION
EVENT/CRIME DETECTION	CASE MANAGEMENT	⬅ PRESERVATION ➡			DOCUMENTATION	
RESOLVE SIGNATURE	IMAGING TECHNOLOGY	APPROVED METHODS	⬅ TRACEABILITY ➡		EXPERT TESTIMONY	
PROFILE DETECTION	CHAIN OF CUSTODY	APPROVED SOFTWARE	VALIDATION TECHNIQUES	STATISTICAL	CLARIFICATION	
ANOMALOUS DETECTION	TIME SYNCH	APPROVED HARDWARE	FILTERING TECHNIQUES	PROTOCOLS	MISSION IMPACT	
COMPLAINTS		LEGAL AUTHORITY	PATTERN MATCHING	DATA MINING	RECOMMEND. COUNTERMEASURES	
SYSTEM MONITORING		LOSSLESS COMPRESSION	HIDDEN DATA DISCOVERY	TIME LINE	STATISTICAL INTERPRETATION	
AUDIT ANALYSIS		SAMPLING	HIDDEN DATA EXTRACTION	LINK		
		DATA REDUCTION		SPECIAL		
		RECOVERY TECHNIQUES				

Marching Orders for the Digital Forensic Community

- Distinguish between digital forensic science and the technology it spawns
- Establish a consistent digital forensic vocabulary
- Establish curricula for universally accepted education and training for various levels of digital forensic scientists, examiners and investigators
- Establish universally accepted practitioner certifications and academic credentials
- Establish research objectives and peer-review processes to assess research conclusions
- Establish standardized approaches to digital forensic processes, procedures and tool certification

Thank You for Considering These Important Issues With Me Today…

Peter Stephenson, CPE, CISSP, CIFI, CISM, FICAF
☎ 248-373-2813 or ☎ 248-760-1152 (mobile)
pstephenson@iidfs.infoforensics.org