A Framework for Digital Forensic Science

By

Mark Pollitt

Presented At

The Digital Forensic Research Conference

DFRWS 2004 USA Baltimore, MD (Aug 11th - 13th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

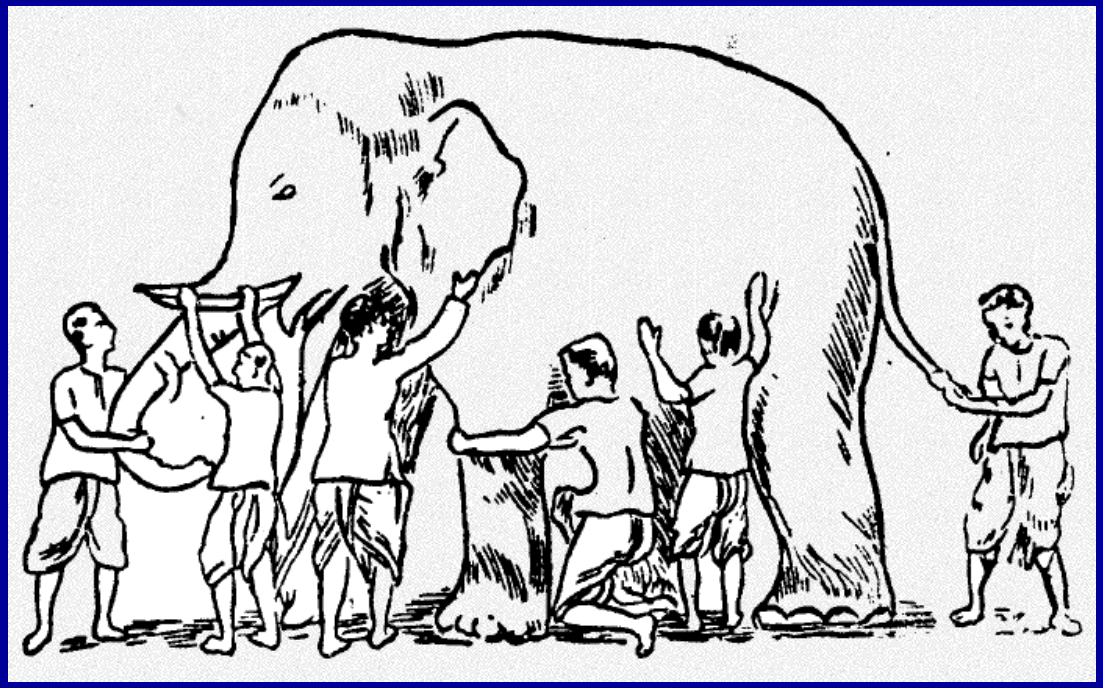
http:/dfrws.org

Six Blind Men from Indostan

Mark M. Pollitt

Digital Evidence Professional Services, Inc.

Once upon a time, there were six blind men from Indostan…



- One thought that the elephant looked like a snake
- Another a leaf
- Another a spear
- Another a wall
- Another a rope
- Another a tree trunk

So what does that have to do with digital forensics?

- We approach DF from different perspectives and with different goals
- Is DF:
  - An investigative task?
  - A forensic science?
  - Sensors for computer security?
  - Part of incident response?

The answer to these questions is

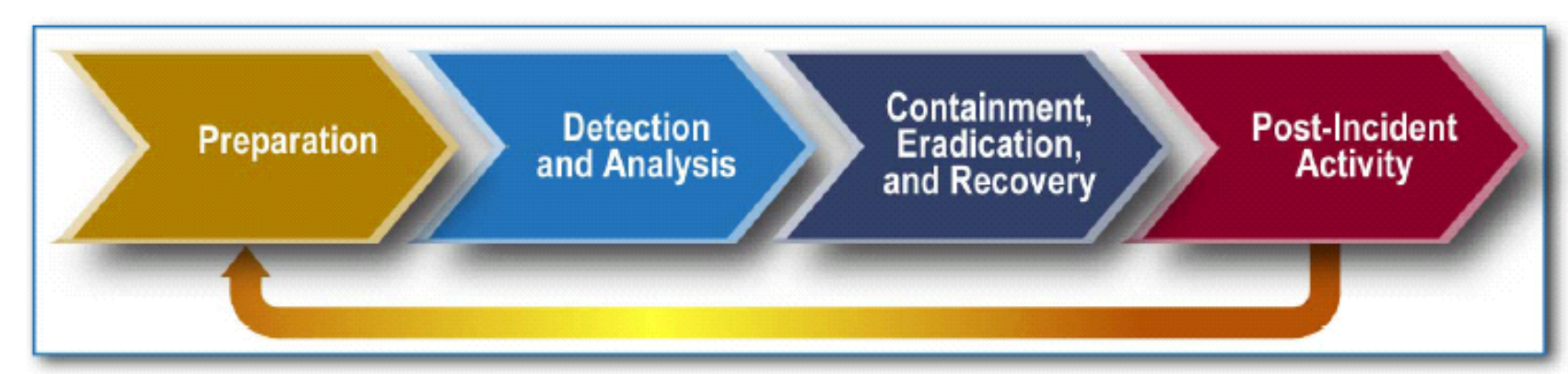
The answer to these questions is

But…

Forensics is not an elephant,
it is a **process**!

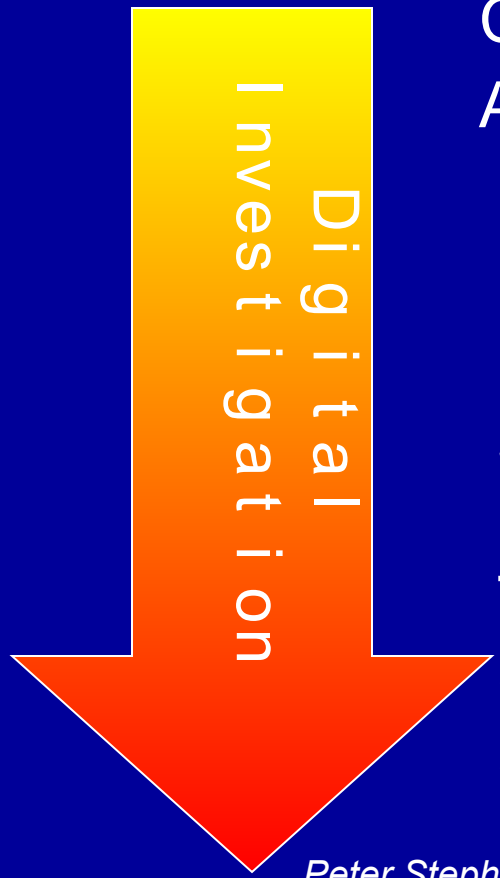
But, we just can't seem to agree
on what the process is…

NIST Incident Response Model



NIST SP 800-61

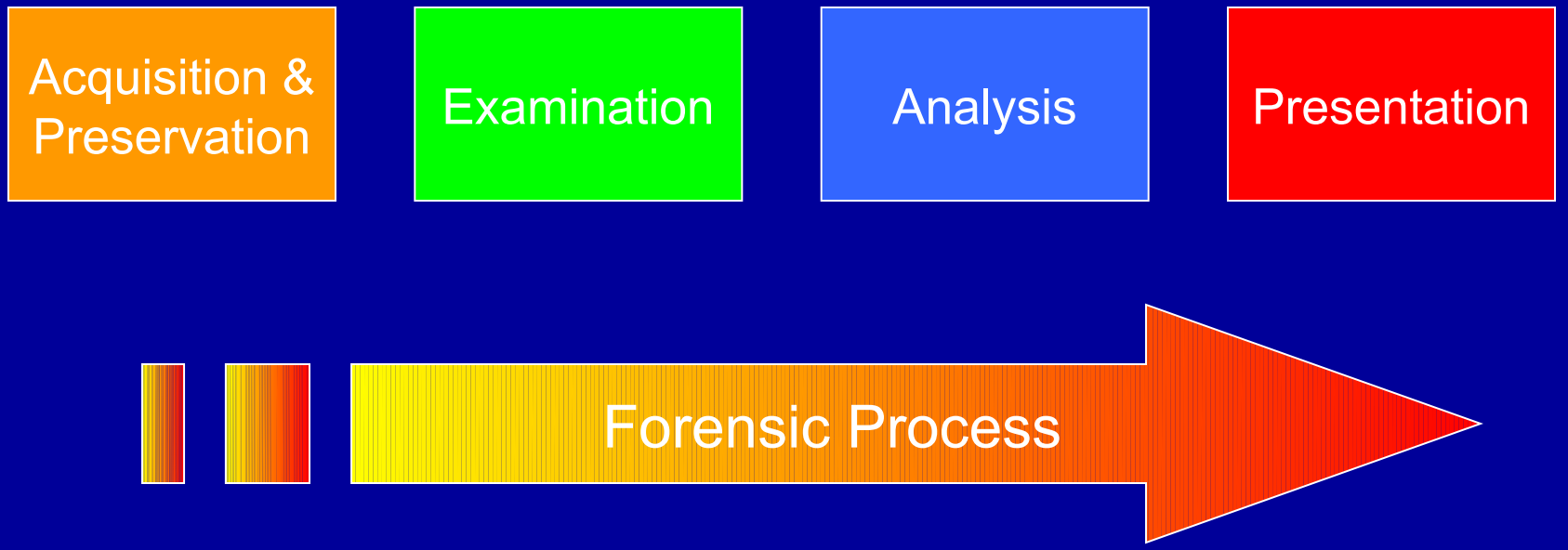
End to End Digital Investigation



- Collecting Evidence
- Analysis of individual events
  - Preliminary correlation
  - Event normalizing
  - Event deconfliction
  - Second level correlation (normalized and non-normalized events)
  - Timeline analysis
  - Chain of evidence construction
  - Corroboration (non-normalized events)

Peter Stephenson, ***APPLICATION OF FORMAL METHODS TO ROOT CAUSE ANALYSIS OF DIGITAL INCIDENTS, 2003***

Forensic Science Process



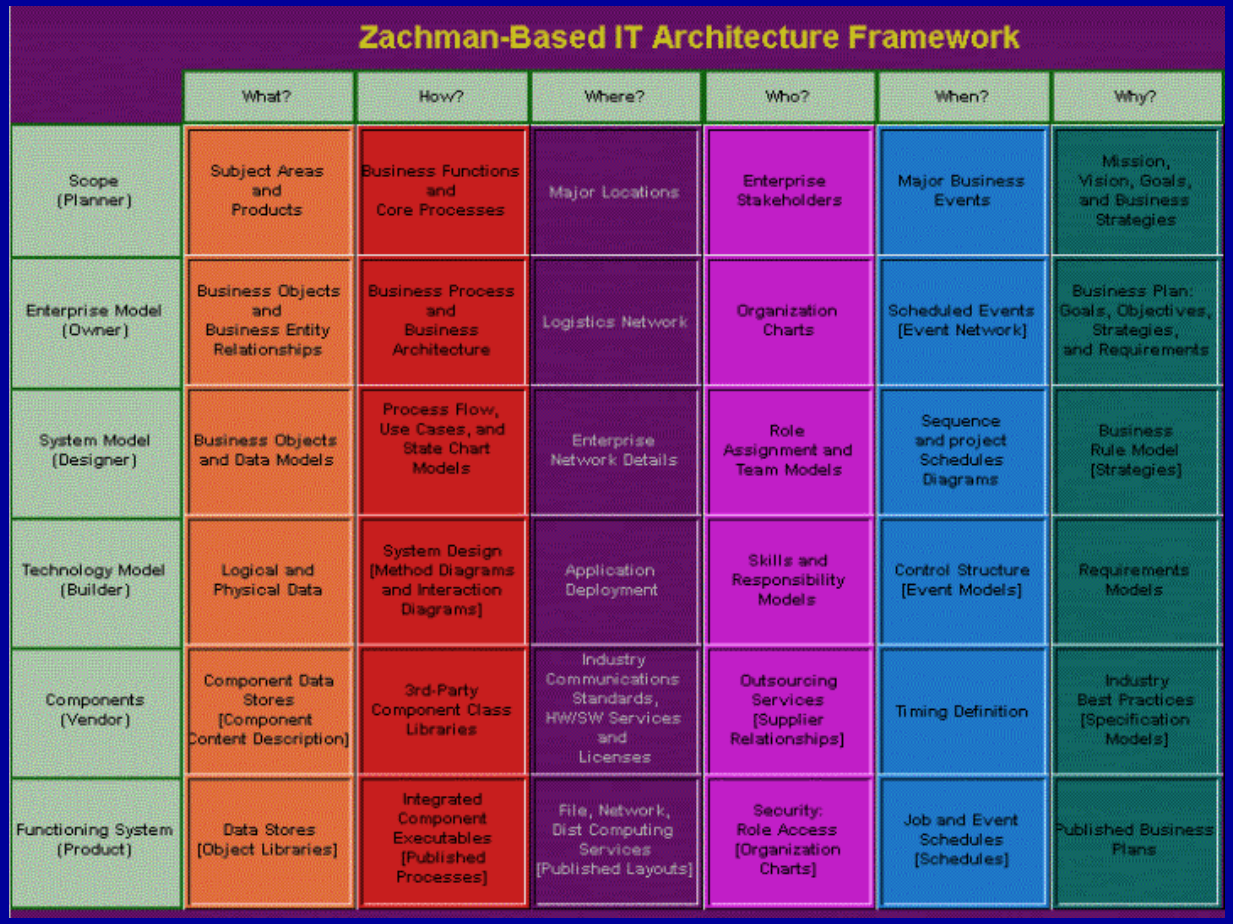
We just don't agree on what order the process takes...

The DFRWS 2001 “Process”

IDENTIFICATION	PRESERVATION	COLLECTION	EXAMINATION	ANALYSIS	PRESENTATION
Event/Crime Detection	**Case Management**	**Preservation**	**Preservation**	**Preservation**	Documentation
Resolve Signature	Imaging Technologies	**Approved Methods**	**Traceability**	**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 Statement
Complaints		**Legal Authority**	Pattern Matching	Data Mining	Recommended Countermeasure
System Monitoring		Lossless Compression	Hidden Data Discovery	Timeline	Statistical Interpretation
Audit Analysis		Sampling	Hidden Data Extraction	**Link**	
		Data Reduction		Spatial	
		Recovery Techniques			

Chart courtesy of Peter Stephenson

Zachman EA Framework



Zachman-Based IT Architecture Framework

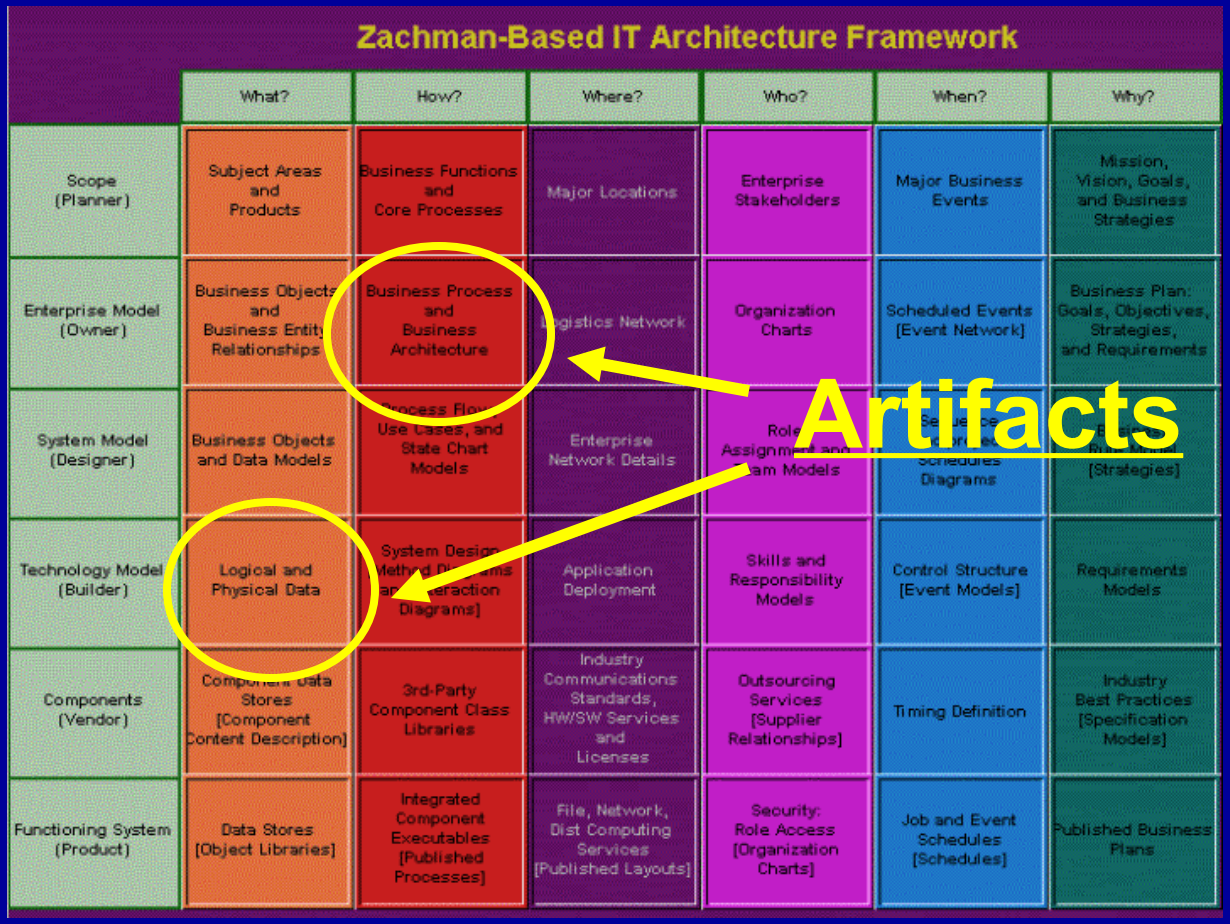
	What?	How?	Where?	Who?	When?	Why?
Scope (Planner)	Subject Areas and Products	Business Functions and Core Processes	Major Locations	Enterprise Stakeholders	Major Business Events	Mission, Vision, Goals, and Business Strategies
Enterprise Model (Owner)	Business Objects and Business Entity Relationships	Business Process and Business Architecture	Logistics Network	Organization Charts	Scheduled Events [Event Network]	Business Plan: Goals, Objectives, Strategies, and Requirements
System Model (Designer)	Business Objects and Data Models	Process Flow, Use Cases, and State Chart Models	Enterprise Network Details	Role Assignment and Team Models	Sequence and project Schedules Diagrams	Business Rule Model [Strategies]
Technology Model (Builder)	Logical and Physical Data	System Design [Method Diagrams and Interaction Diagrams]	Application Deployment	Skills and Responsibility Models	Control Structure [Event Models]	Requirements Models
Components (Vendor)	Component Data Stores [Component Content Description]	3rd-Party Component Class Libraries	Industry Communications Standards, HW/SW Services and Licenses	Outsourcing Services [Supplier Relationships]	Timing Definition	Industry Best Practices [Specification Models]
Functioning System (Product)	Data Stores [Object Libraries]	Integrated Component Executables [Published Processes]	File, Network, Dist Computing Services [Published Layouts]	Security: Role Access [Organization Charts]	Job and Event Schedules [Schedules]	Published Business Plans

http://www.feacinstitute.org/enterprise_architecture/federal_enterprise_architecture/index.htm#

Zachman EA Framework

Functions

Views



http://www.feacinstitute.org/enterprise_architecture/federal_enterprise_architecture/index.htm#

Viewing the DFRWS as a Framework

IDENTIFICATION	PRESERVATION	COLLECTION	EXAMINATION	ANALYSIS	PRESENTATION
Event/Crime Detection	**Case Management**	**Preservation**	**Preservation**	**Preservation**	Documentation
Resolve Signature	Imaging Technologies	**Approved Methods**	**Traceability**	**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 Statement
Complaints		**Legal Authority**	Pattern Matching	Data Mining	Recommended Countermeasure
System Monitoring		Lossless Compression	Hidden Data Discovery	Timeline	Statistical Interpretation
Audit Analysis		Sampling	Hidden Data Extraction	**Link**	
		Data Reduction		Spatial	
		Recovery Techniques			

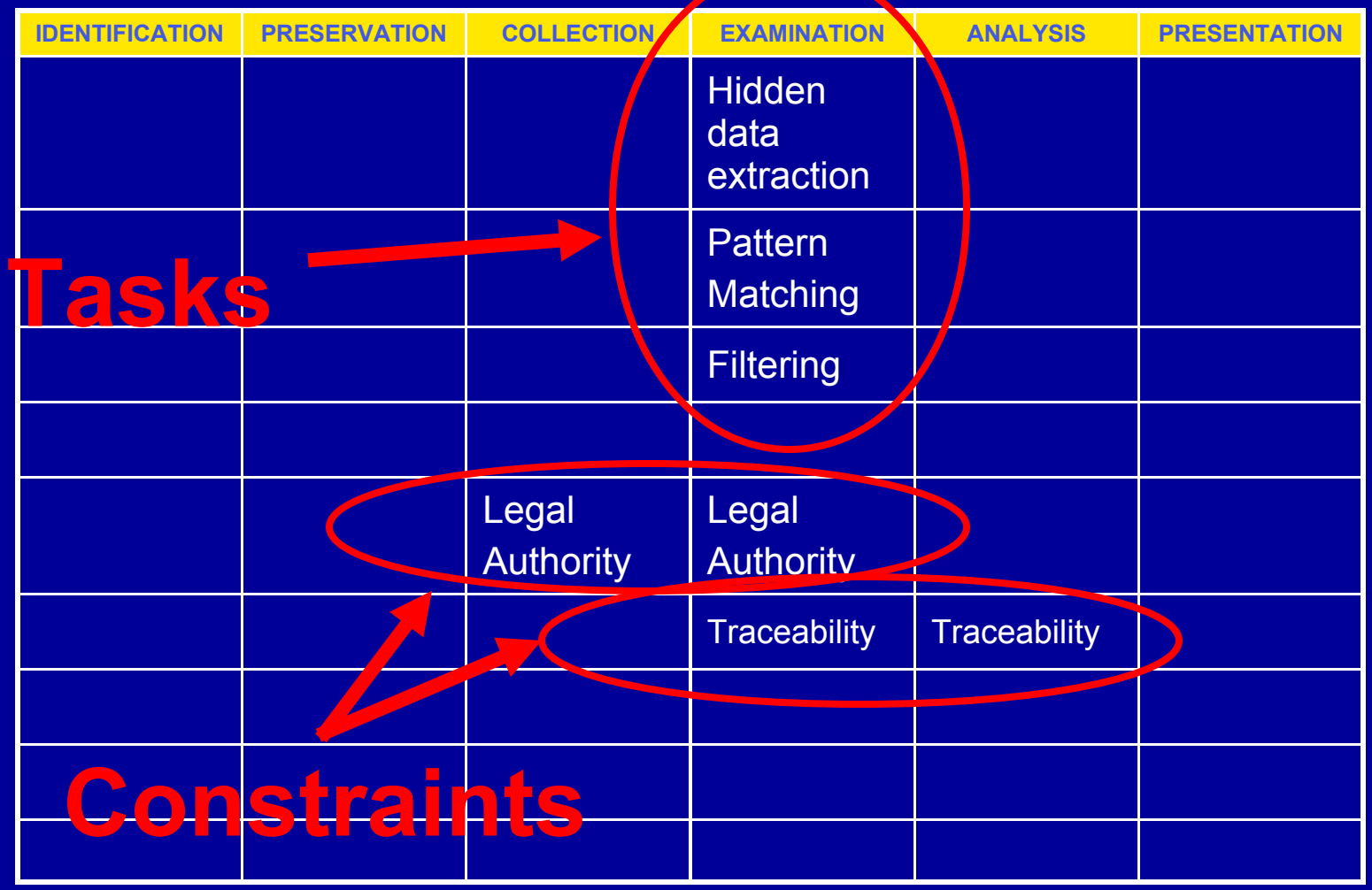
Chart courtesy of Peter Stephenson

IDENTIFICATION	PRESERVATION	COLLECTION	EXAMINATION	ANALYSIS	PRESENTATION

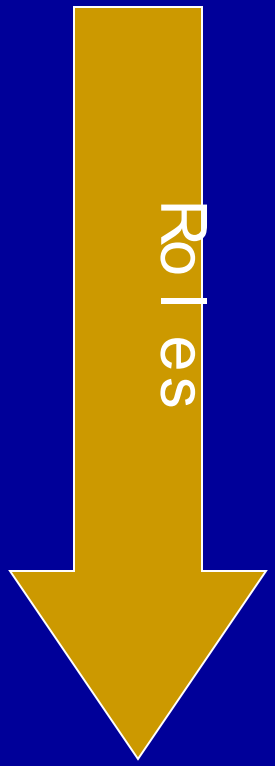
Functions

IDENTIFICATION	PRESERVATION	COLLECTION	EXAMINATION	ANALYSIS	PRESENTATION
			Hidden data extraction		
			Pattern Matching		
			Filtering		

Tasks


IDENTIFICATION
PRESERVATION
COLLECTION
EXAMINATION
ANALYSIS
PRESENTATION
Hidden data extraction
Pattern Matching
Filtering
Legal Authority
Legal Authority
Traceability
Traceability
Tasks
Constraints

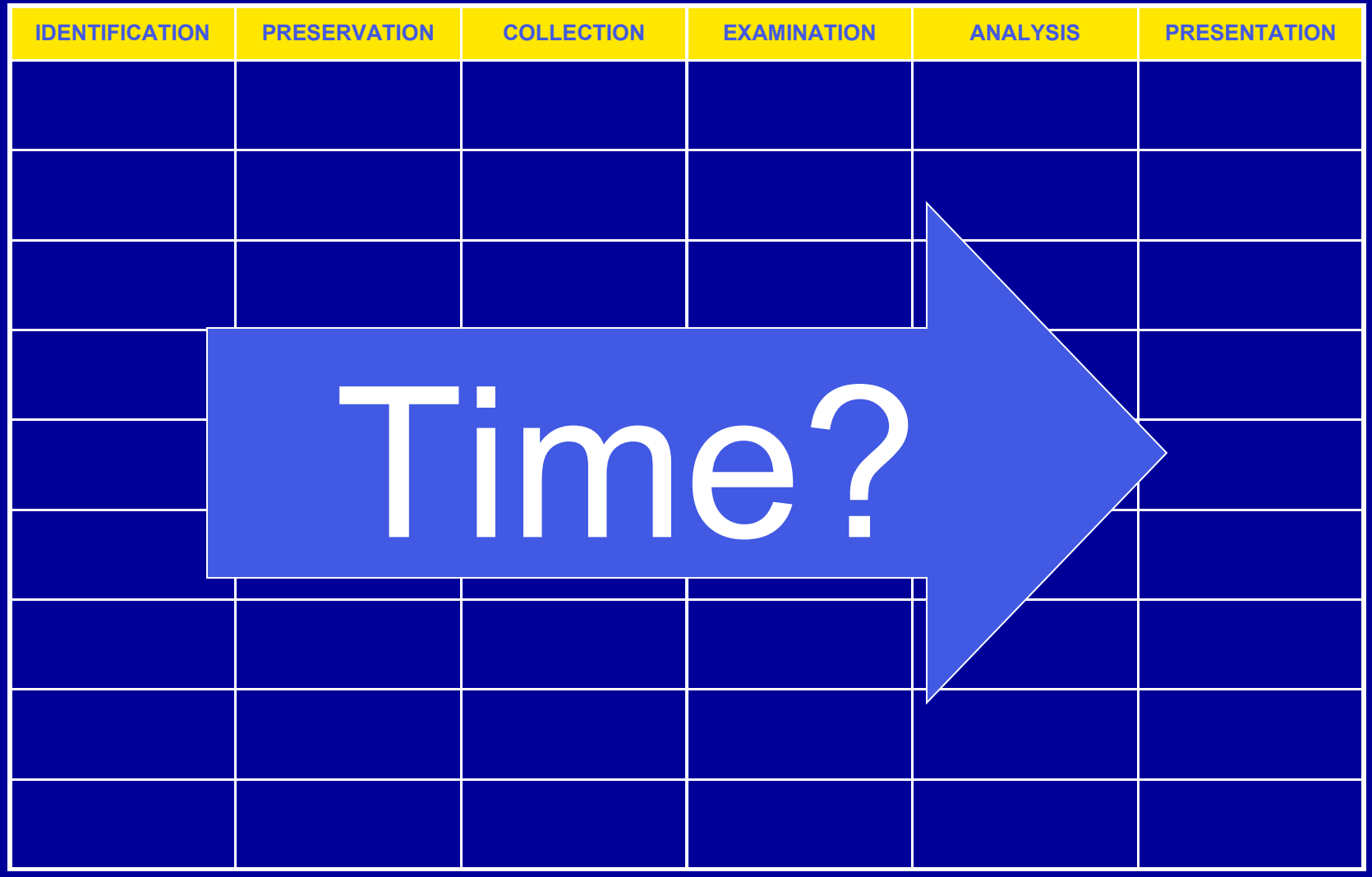
Roles, aka Views?



IDENTIFICATION	PRESERVATION	COLLECTION	EXAMINATION	ANALYSIS	PRESENTATION

Might look something like this:

Role	IDENTIFICATION	PRESERVATION	COLLECTION	EXAMINATION	ANALYSIS	PRESENTATION
Incident Response						
Security Management						
Criminal Investigations						
LE Forensic Examination						
Civil Discovery						
Intelligence						


IDENTIFICATION
PRESERVATION
COLLECTION
EXAMINATION
ANALYSIS
PRESENTATION
Time?

This is where it gets difficult, we don’t seem to agree on the same temporal order.

In fact, we don’t seem to use the same functions for each case/view/role.

Maybe we don’t have to…

The temporal order is not defined by “forensics”, as a process, but rather constrained by the role’s purpose for using forensics.

Another way to describe this:

- Forensics is not a single process, but is
- A set of tasks that can be grouped into
- Functions that are selected based upon
- The purpose for which the process is being applied (role) and are
- Bound by constraints that are
- Defined by either internal or external requirements

Another way to describe this:

- Forensics is not a single process, but is
- A set of tasks that can be grouped into
- Functions that are selected based upon
- The purpose for which the process is being applied (role) and are
- Bound by constraints that are
- Defined by either internal or external requirements

Is this THE answer?

- **Of course not!**
- Frameworks are always “works in progress”
- That should not stop us from taking new steps each day
- Frameworks get better with application

Applying this to Research Issues

- Research can be focused on:
  - Functions
  - Tasks
  - Constraints
  - Process
  - Roles
  - Or the interrelationships between these

Conclusion

- The core DFRWS framework is sound
- It can be developed, extended and refined
- It can be used as both a framework and a vocabulary for research and practice
- The next steps are in your hands!

I Sincerely Thank You for

- Your Time
- Your Attention
- Your Contributions to the field
- Your participation in the remainder of this conference

Mark M. Pollitt
President
Digital Evidence Professional Services, Inc.