# A Hierarchical, Objectives-Based Framework for the Digital Investigations Process

*By*

**Nicole Beebe, Jan Clark**

*Presented At*

The Digital Forensic Research Conference

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

# A Hierarchical, Objectives-Based Framework for the Digital Investigations Process

Nicole Beebe & Jan Guynes Clark

University of Texas at San Antonio

DFRWS 2004

UTSA THE UNIVERSITY OF TEXAS AT SAN ANTONIO

# Discussion Topics

- Framework goals
- Framework components
- Proposed framework
- Framework discussion
  - Benefits
  - Limitations

# General Framework Goals

- Overarching purpose
  - Achieve scientific rigor and relevance
  - Provide structure; understand and define the underlying structure of a complex process
  - Delineate assumptions, concepts, values, and practices (standards, guidelines, procedures)
  - Simplify the complex without losing granularity

# Digital Investigations Process Framework Goals

- Carrier and Spafford (2003)
  - Basis in existing investigation theory
  - Practicality for usability
  - Technology neutrality
  - Specificity to facilitate R&D
  - Wide applicability
    - User communities
    - Layers of abstraction (Carrier 2003)
    - Types of digital crime scenes

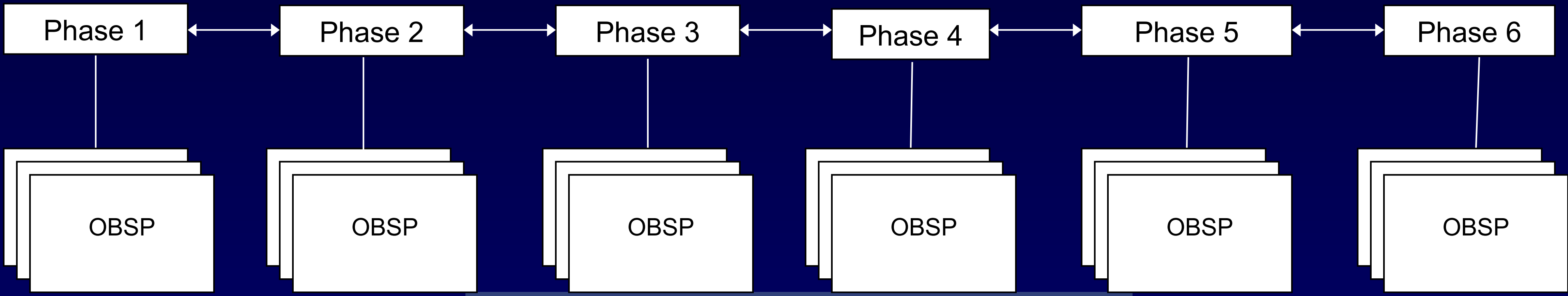
# Creation of the Framework

- Integrate previous frameworks
  - DFRWS (2001)
  - DoJ (2001)
  - Reith et al (2002)
  - Mandia et al (2003)
  - Carrier and Spafford (2003)
  - Nelson et al (2004)

  ... others should integrate well
- Emphasis on improving levels of practicality and specificity
  - Increased level of detail needed for examiners, investigators, researchers, and tool developers

# Framework Components

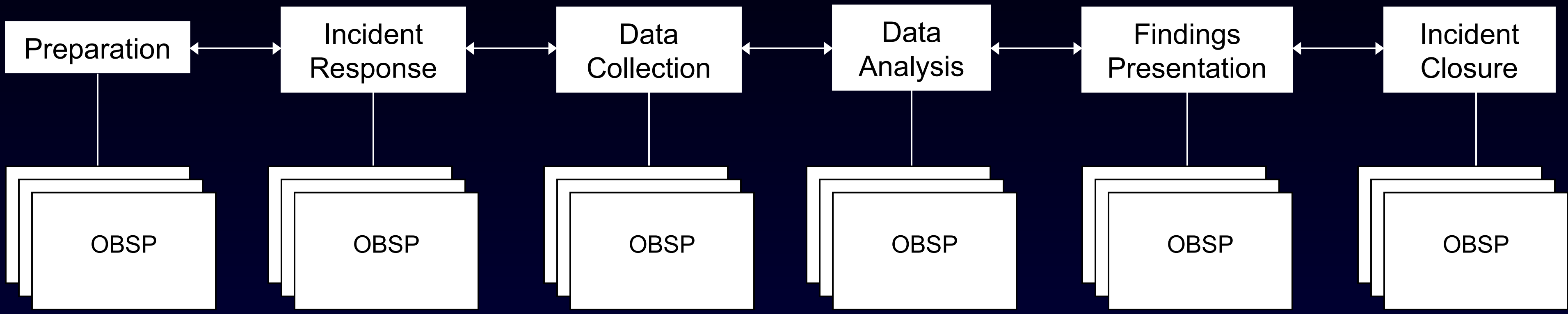
- Hierarchical phase structure
  - Phases
    - Distinct, discrete, and sequential
    - Predominantly, but not exclusively non-iterative
  - Sub-phases
    - Objectives-based (OBSP)
    - Supported by hierarchical, matrixed task structures
    - Highly iterative in nature



# Framework Components (cont.)

- Principles
  - Overarching goals and objectives
  - Continuous; permeates multiple phases
  - Procedures and methodological approaches intended to meet standards and guidelines
  - Examples
    - Evidence preservation
      - Purpose is to maximize evidence availability & quality; and maintain evidence integrity during process
    - Documentation
      - Purpose is to record and preserve information generated during the process for variety of uses

# Proposed Framework – 1st Tier



- Preparation Phase
  - Forensic readiness (Rowlingson 2004)
  - Preparation by response/investigation personnel
- Incident Response Phase
  - Detection & initial, pre-investigation response
  - Validate, assess, determine response strategy

# Proposed Framework – 1st Tier (cont.)

- Proposed Framework – 1st TierData Collection Phase
  - After decision is made to investigate
  - Collect evidence in support of response strategy and investigative plan
  - Caveat: “Investigate” and “evidence” are defined loosely here; may not have a legal context per se.
- Data Analysis Phase
  - Confirmatory analysis and/or event reconstruction
  - Survey, extract, and examine data collected during Data Collection Phase

# Proposed Framework – 1st Tier (cont.)

- Presentation of Findings Phase
  - *Communicate* relevant findings to audiences
- Incident Closure Phase
  - Make and act upon decision(s)
  - Evidence disposition
  - Information retention
  - Identify, incorporate lessons learned

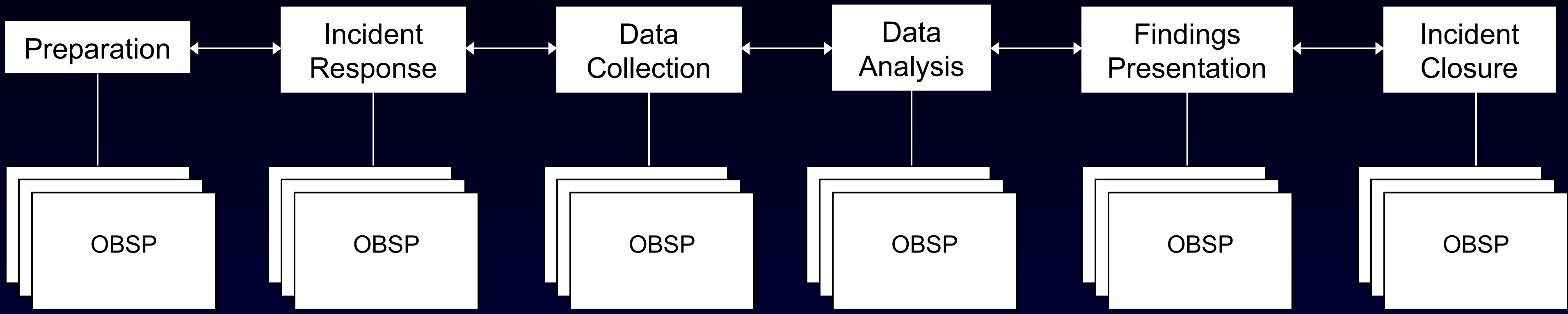
# Framework Principles

- Evidence Preservation
  - Purpose
    - Maximize evidence availability & quality
    - Maintain evidence integrity during process
  - Examples
    - Preparation Phase – enable logging
    - Incident Response Phase – minimize data alteration during “live response”
    - Data Collection Phase – forensic duplicates, hashes, etc.
    - Data Analysis Phase – forensic working copies, understanding of level of invasiveness of procedures
    - Presentation of Findings Phase – enable corroboration
    - Incident Closure Phase – information retention

# Framework Principles (cont.)

- Documentation
  - Purpose is to record and preserve information generated during the process for variety of uses
  - Examples
    - Preparation Phase – risk assessment info, policies, procedures, “known goods,” training, legal coord., etc.
    - Incident Response Phase – information obtained during “live response,” witness statements, damage info, etc.
    - Data Collection Phase – “state” info, evidence marking, chain of custody information, etc.
    - Data Analysis Phase – tools, processes, findings, etc.
    - Findings Presentation Phase – technical, non-tech. info
    - Incident Closure Phase – decisions, lessons, info retention

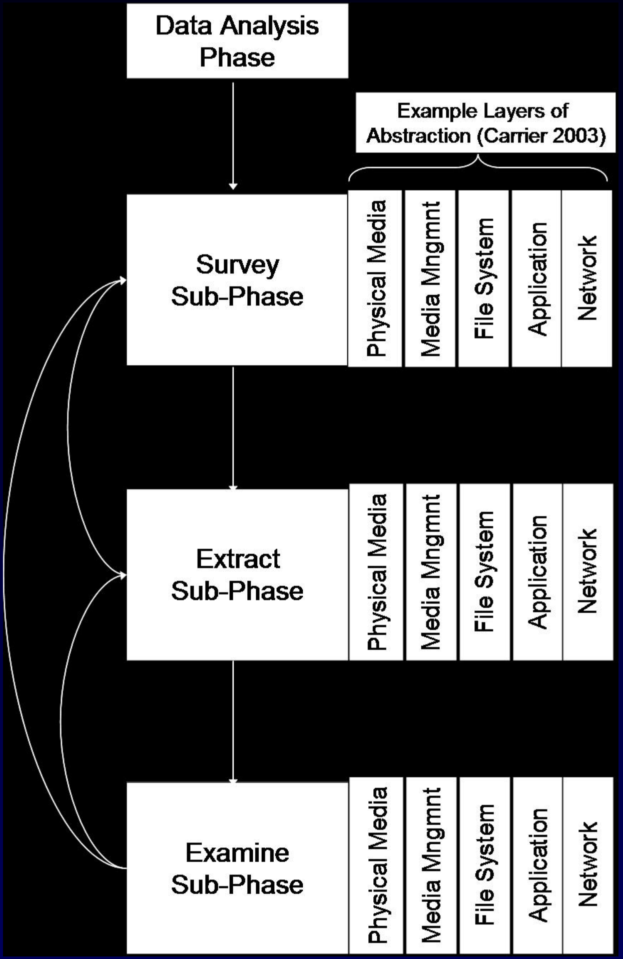
# Proposed Framework – 2nd Tier



- Each first-tier phase requires objectives-based sub-phase (OBSP) development
  - i.e. “Determine if unauthorized software was installed” instead of “examine the Registry key…”
  - User selects pertinent objectives and specific tasks are subsequently illuminated

# Example – Data Analysis Phase

- "SEE Data Analytical Approach"
  - Survey Sub-Phase
    - Describe digital object's "landscape"
    - i.e. file system mappings, partitioning, geometry, key objects
  - Extract Sub-Phase
    - Extract data for examination
    - i.e. keyword searches, data de/reconstruction, filtering, signature analysis, etc.
  - Examine Sub-Phase
    - Examine data for confirmatory and/or event reconstruction goals
    - Draw conclusions



# Data Analysis Objectives

- Apply “SEE Data Analytic Approach” to selected analytic objectives with subordinate task hierarchies
- Example analytic objectives
  - Reduce amount of data to analyze
  - Assess skill level of suspect(s)
  - Recover deleted files
  - Find relevant hidden data
  - Determine chronology of file activity

  … 14 objectives identified in paper

# Analytic Objective Task Hierarchy (Examples)

- Reduce amount of data to analyze
  - Signature analysis to filter out “known goods”
  - Chronological ordering and focus
- Assess skill level of suspect(s)
  - Look for evidence of data hiding/wiping utilities
  - Look for evidence of activity hiding (e.g. log alteration)
- Recover deleted files
  - ID & recover deleted files via file system info
  - ID & recover deleted files via Recycler
  - ID & recover temporary files
  - Rebuild deleted partitions

# Framework Discussion

- Multiple level task hierarchy is encouraged
  - Objective
    - Task
      - Sub-task
        - Sub-sub-task, etc.
- Benefits of the hierarchical, objectives based approach to framework development:
  - Meets Carrier and Spafford criteria (2003)
    - Specific improvements in the areas of practicality and specificity; more useful for entire community

# Framework Discussion (cont.)

- Approach enables matrices
  - Matrix sub-tasks to multiple tasks
  - Matrix tasks to multiple objectives
  - Matrix tools to tasks and sub-tasks
  - Matrix capabilities (objectives) to tools
- Matrices streamline complex, flexible processes
  - Provides “worksheets” and guidelines in place of impossible and impractical “checklists”
  - Handles task redundancies
  - Reduces complexity
  - Identify gaps

# Framework Discussion (cont.)

- Primary limitation
  - Framework is incomplete
    - Proposed data analytic objectives and task hierarchies in paper requires refinement
    - Remaining phases need sub-phase development
    - Cross-abstraction layer development needed
      - Different task hierarchies may need to be developed for different platforms and potentially media types
    - Empirical testing needed

# Summary

- Framework goals
- Framework components
- Proposed framework
- Framework discussion
  - Benefits
  - Limitations

# ? Questions ?

Nicole Lang Beebe, CISSP

nbeebe@utsa.edu

Jan Guynes Clark, PhD, CISSP

jclark@utsa.edu