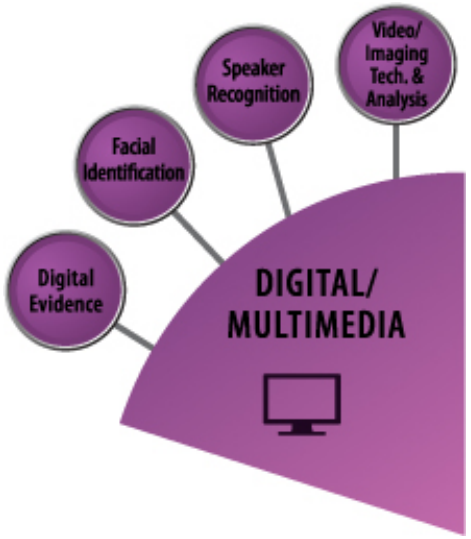


Is Digital & Multimedia Science Really "Forensic Science"?

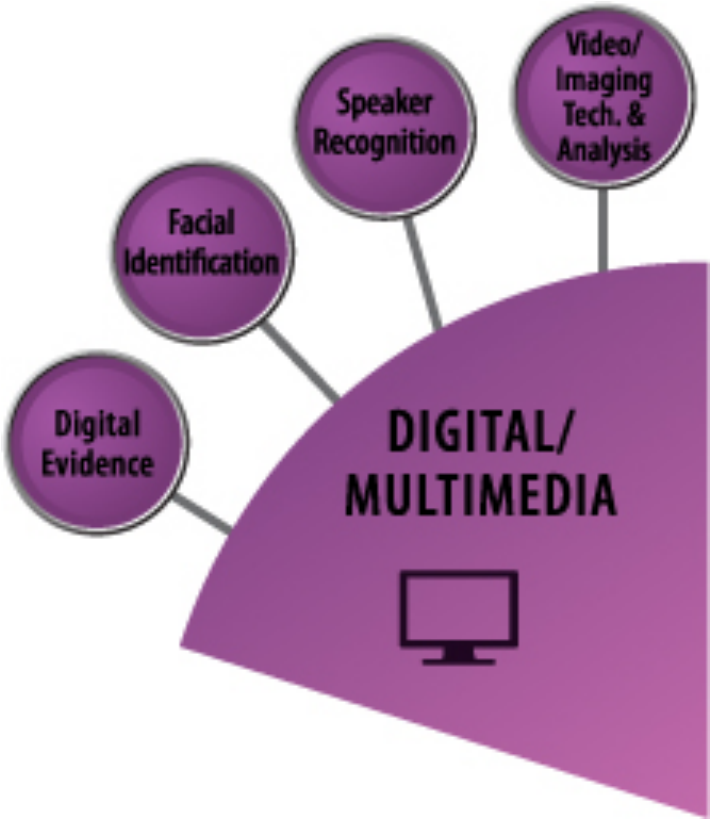
Richard W. Vorder Bruegge, Ph.D.
Digital/Multimedia SAC Chair
Federal Bureau of Investigation
February 20, 2017

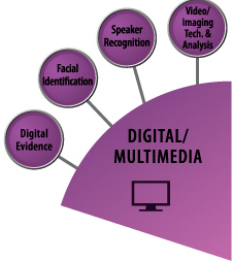
Agenda

- **DMSAC Organization and Status**
- **Focus Areas and Challenges**
- **Framework for Harmonizing Forensic Science Practices and Digital/Multimedia Evidence**

DMSAC Organization

- DMSAC Chair
  - **Richard W. Vorder Bruegge**, FBI
- DMSAC Vice Chair
  - **Lam Nguyen**, Mandiant
- Executive Secretary
  - **Douglas Lacey**, BEK TEK LLC
- Subcommittee Chairs
  - **James Darnell**, U.S. Secret Service
  - **Lora Sims**, Ideal Innovations Inc.
  - **James Wayman**, San Jose State University
  - **Julie Carnes,** Target





DMSAC Organization

- DMSAC Members
  - **Eoghan Casey, Ph.D.**, University of Lausanne, School of Criminal Sciences
  - **Matthew Graves**, United States Army Criminal Investigation Laboratory
  - **Abhyuday Mandal, Ph.D.**, University of Georgia
  - **P. Jonathon Phillips, Ph.D.**, National Institute of Standards and Technology
  - **Michael Piper**, Target Corporation
  - **Mark Pollitt, Ph.D.**, Digital Evidence Professional Services, Inc.
  - **Lawrence M. Solan**, Brooklyn Law School

- DMSAC Ex-Officio Members
  - **John F. Holloway,** Associate Dean and Exec. Dir., Quattrone Center for the Fair Administration of Justice, University of Pennsylvania (HFC)
  - **Henry R. Reeve**, Denver District Attorney's Office (LRC)
  - **Christopher Krug**, Quality Assurance Manager, Johnson County Sheriff's Office Criminalistics Laboratory (QIC)

DMSAC Status

Proposed New DMSAC Standards at ASTM E30

WK56121 * Standard Practice/Guide for Facial Recognition Systems: Capture Equipment and Specification

WK57017 * Standard Practice/Guide for Facial Recognition Systems: Guidelines for Postmortem Facial Image Capture

WK58704 * Facial Comparison Methods

WK60382 * Forensic Audio Laboratory Setup and Maintenance

WK61709 * Standard Practice for Data Retrieval from Digital CCTV System

DMSAC Status

Existing ASTM E30 Documents to be promoted to OSAC

E3016-15e1 Standard Guide for Establishing Confidence in Digital Forensic Results by Error Mitigation Analysis

E2825-12 Standard Guide for Forensic Digital Image Processing

DMSAC Status

<u>Other Priorities for 2018</u>

Posting Baseline Speaker Recognition Documents

Process Map for Speaker Recognition

Seeking Liaison Status for Speaker Recognition Subcommittee with ISO/IEC JTC1 SC37 WG

Training Standard across multiple OSAC Disciplines

Focus Areas and Challenges

- **Some Key DMSAC (& OSAC) Challenges:**
  - **Accreditation**
  - **Conclusion Scales – Coordinate with P/PESAC**
  - **Terminology – Discipline-specific vs. Global**
  - **Error Rates through Testing Examiners**
  - **Foundations**

- **Scientific Paradigm for Digital/Multimedia Forensics**

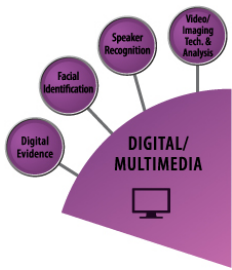
A Framework for Harmonizing Forensic Science Practices and Digital/Multimedia Evidence

Motivation, Background and Highlights

Mark Pollitt, Eoghan Casey, David-Olivier Jaquet-Chiffelle, Pavel Gladyshev

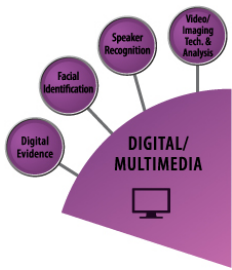
OSAC Task Group on Digital/Multimedia Science

- Primary Authors of this document:
  - Mark Pollitt
  - Eoghan Casey
  - David-Olivier Jaquet-Chiffelle
  - Pavel Gladyshev
- Contributing Members of the Task Group:
  - Martin Olivier, Michael Piper, Lam Nguyen, Henry Reeve, Marcus Rogers
- All of the DMSAC and Sub-committees participated
- The TG worked extensively with the FSSB and several members made substantial contributions to the final document.



TG Mission

- Answer the question: Where is the science in digital/multimedia (DM) forensics?
- Quest began at the very first public presentation at AAFS in Orlando (2015).
- The work continues both internally and in collaboration with the rest of OSAC

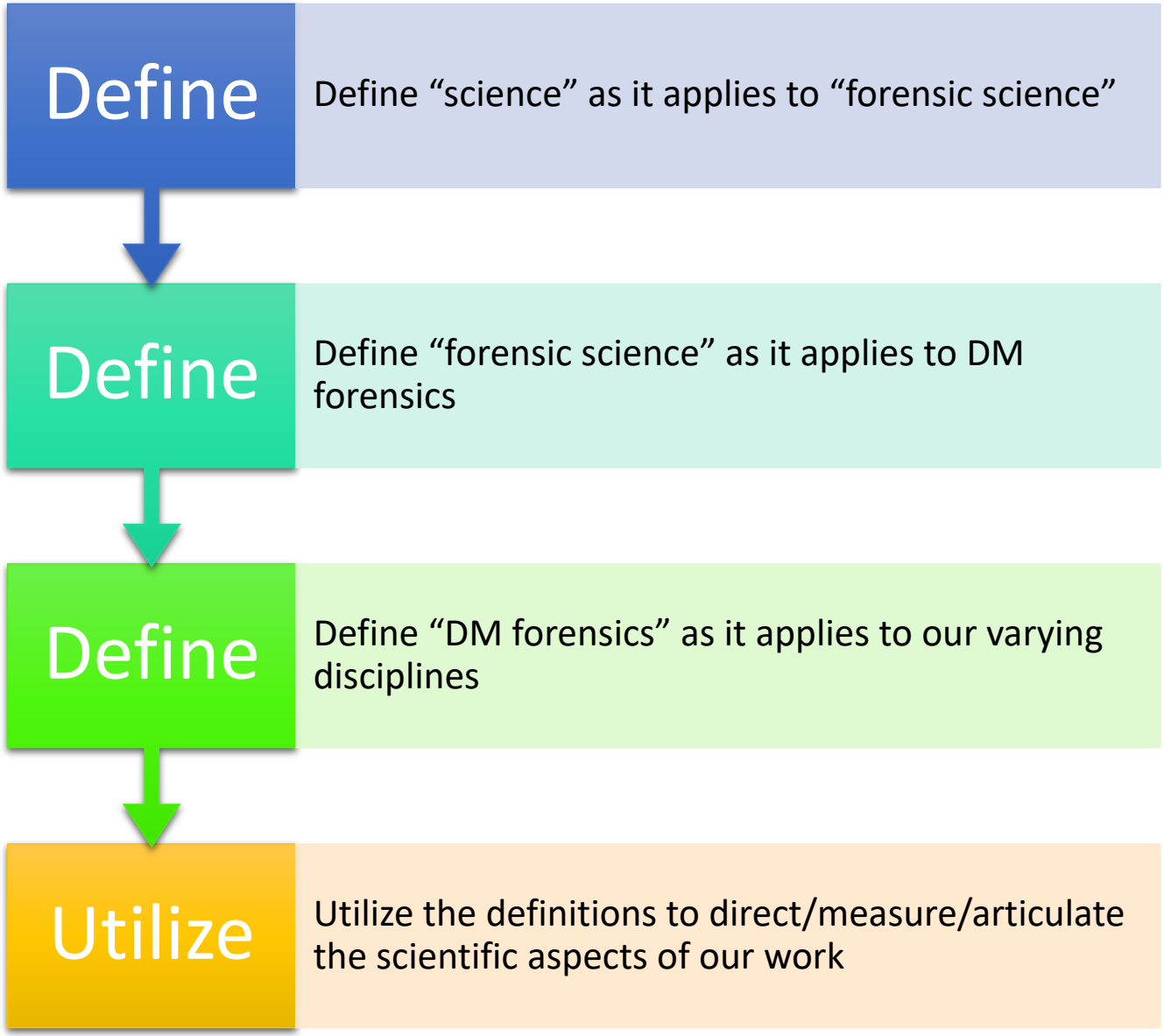


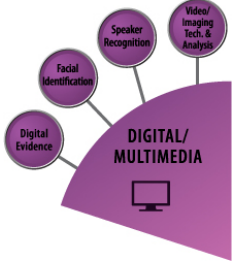
Motivation: demonstrate scientific basis

Case Example: Johnny Oquendo convicted of murdering Noel Alkaramla

- Defendant's attorney: “We're just asking for the courtroom to determine if this is good science”
- Judge: “[prosecution] failed to meet their burden of demonstrating that the science underlying Google location services has gained general acceptance in the in the relevant scientific community.”

DMSci TG Approach

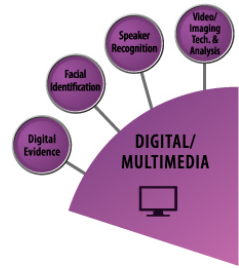




Gestalt: value of forensic science as a whole

<u>More than intersection of each forensic area & foundational sciences</u>

- Scientific reasoning and processes
- Address questions – specific to an event or a case – for legal contexts
- Provide decision-makers with trustworthy understanding of the traces
- Help decision-makers reach an informed decision



Goals: provide confidence and insights

<u>Give decision-makers confidence in & understanding of forensic results</u>

- Investigation
  - Assess evidence to guide investigative decisions
- Courtroom
  - Evaluate strength of evidence and help judge or jury reach a decision
- Research
  - Study evidence to establish generalized theories

Traces: what do we study?

Surveyed forensic practitioners & developed generalized definition

Any modification, subsequently observable, resulting from an event

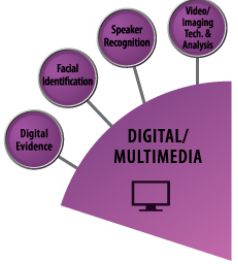
The nature of the modification can be	The trace can reveal itself
• physical or virtual • material or immaterial • analog or digital	• as a presence or • as an absence

Forensic questions: what are we asked?

<u>Surveyed forensic practitioners & categorized the questions (appendix)</u>

⇒ *Systematic and coherent study of traces to address questions for a legal context:*

- Authentication
- Identification
- Classification
- Reconstruction
- Evaluation



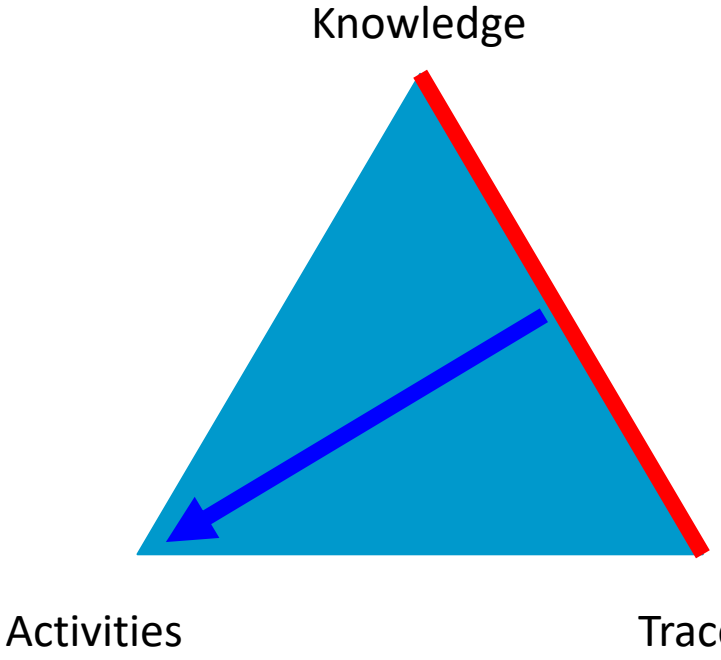
Addressing questions: scientific reasoning

1) Abductive Reasoning

Testimony: State claims

Investigation: Develop scenarios

Research: Form hypotheses

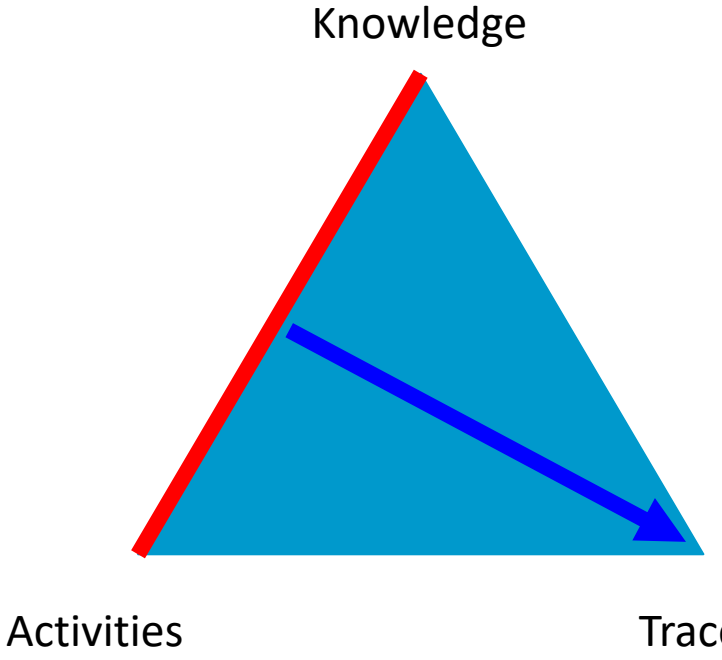


2) Deductive Reasoning

T) Fact-check claims

I) Fact-check scenarios

R) Test hypotheses

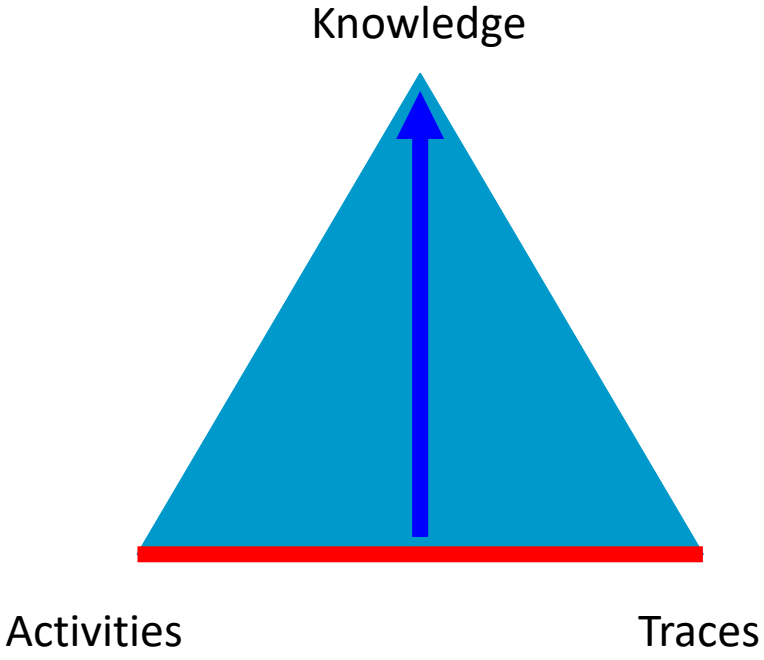


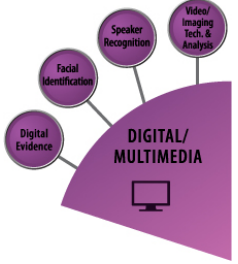
3) Inductive Reasoning

T) Evaluate traces apropos of the claims

I) Make investigative decisions

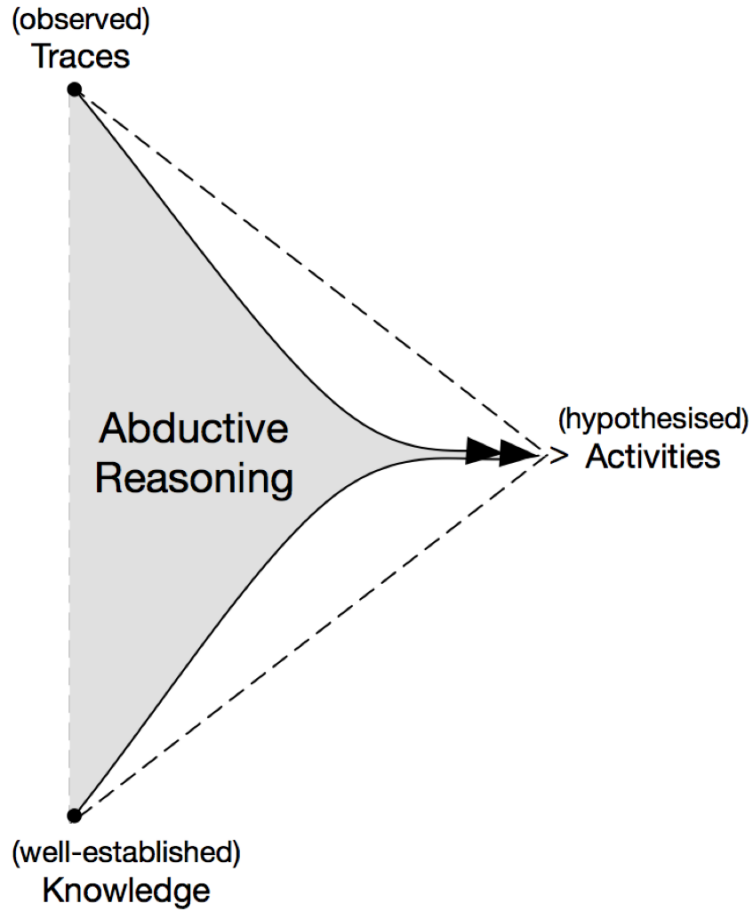
R) Establish general theories

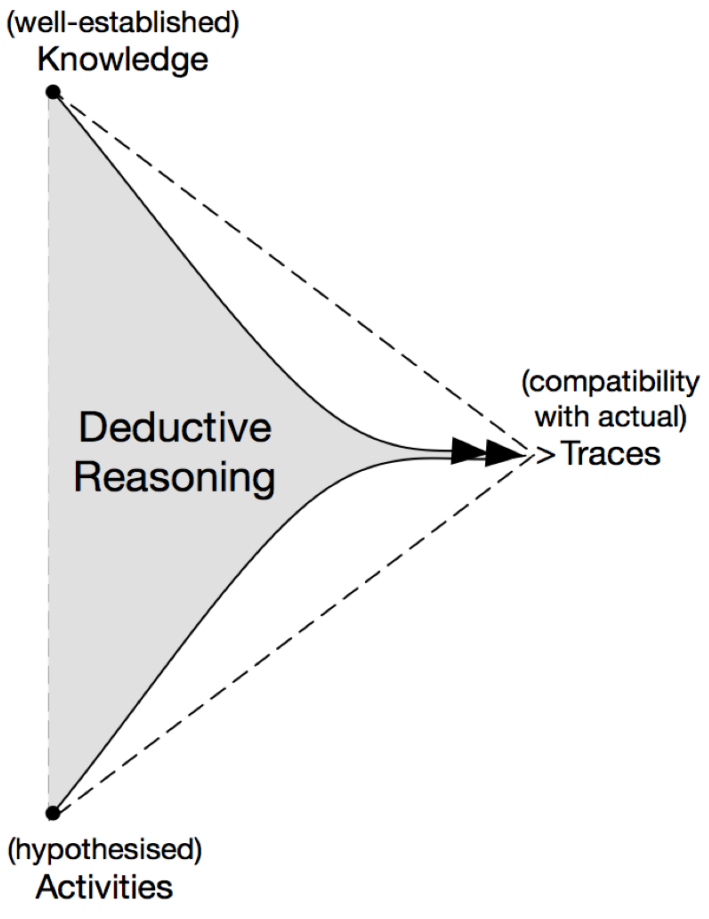


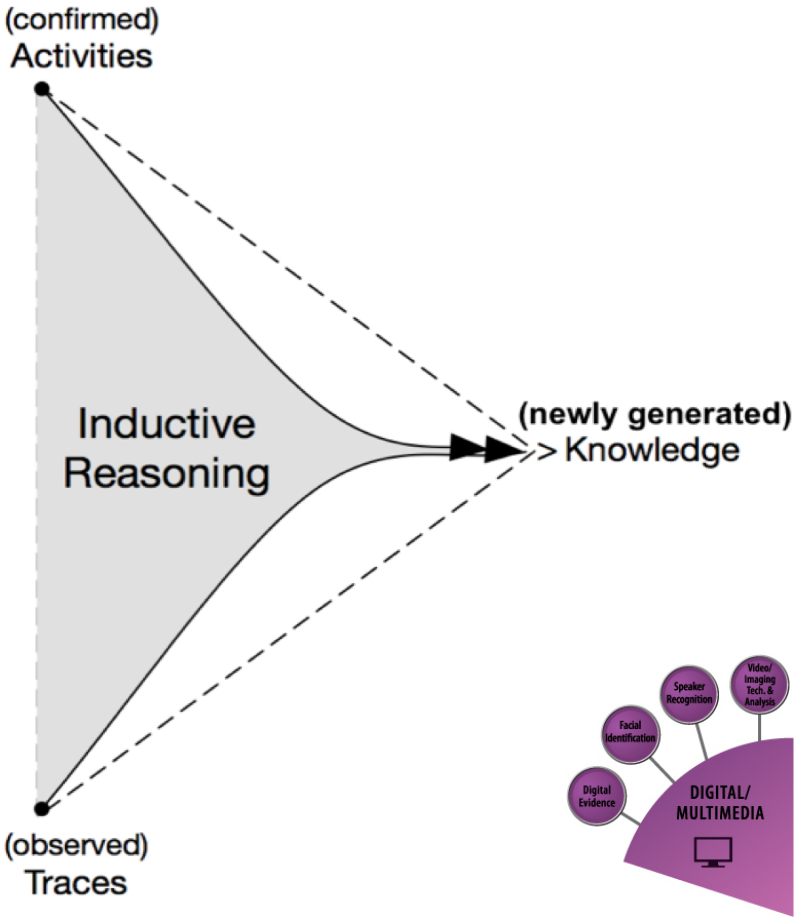


Scientific reasoning in forensic science

Takes into account uncertainties in activities, traces, or knowledge

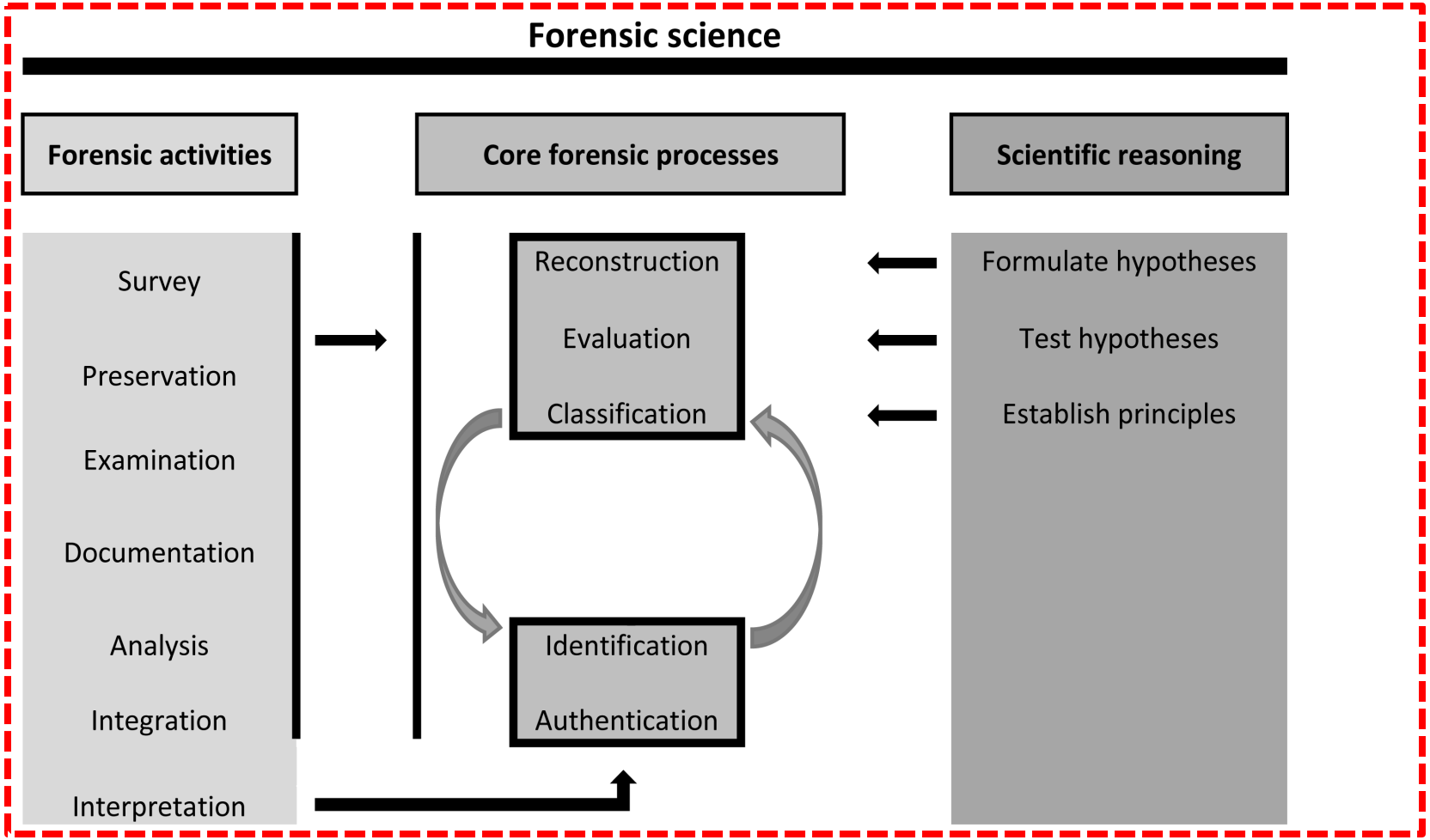






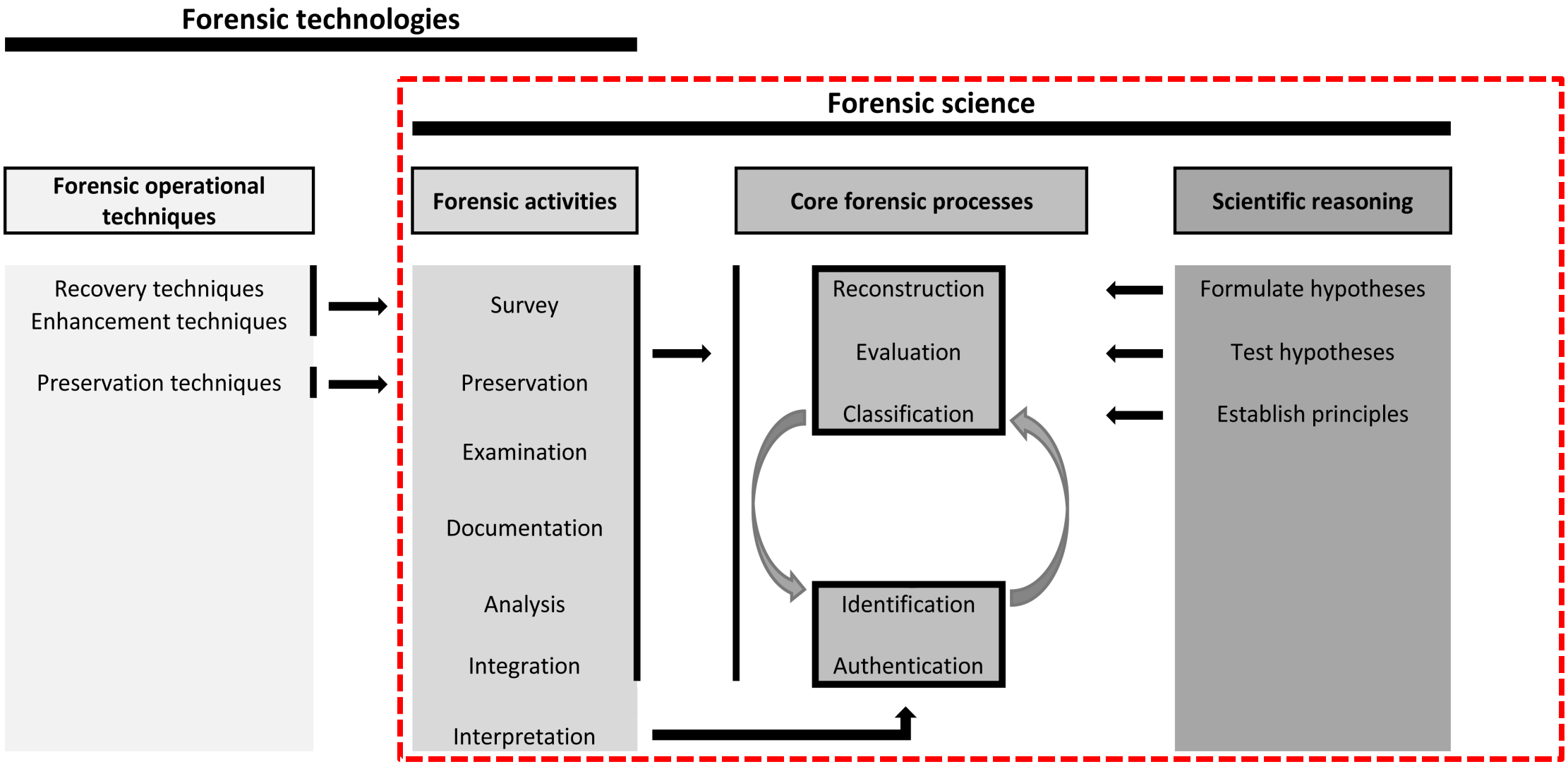
Processes and activities in forensic science

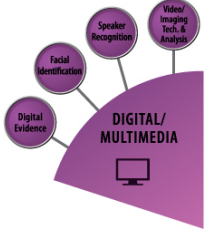
Reasoning applied to core forensic process, fed by forensic activities



(*Don't get hung up on labels!
Please refer to paper for context!)

Operational techniques in forensic science



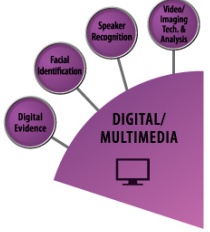


Core forensic processes: (1) Authentication

⇒ *Decision process attempting to establish sufficient confidence in the truth of some claim*

- The other four core forensic processes rely on the authentication of the trace(s) to be examined

- Example authentication claims:
  - This photograph is unaltered
  - This photograph was taken in Seattle
  - This photograph was taken on 30 January 2018
  - These two photos are identical at a binary level

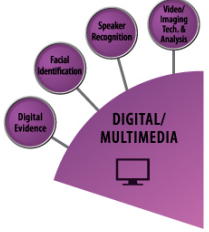


Core forensic processes: (2) Identification

⇒ *Decision process attempting to establish sufficient confidence that some identity-related information describes*

- *a specific entity*
- *in a given context*
- *at a certain time*

- Used within the authentication, classification, evaluation processes
- Applies to animate or inanimate entities, physical or virtual
  - The person in the images are the same person
  - This camera (specific) was used to take this photograph

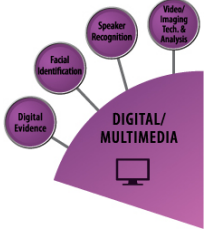


Core forensic processes: (3) Classification

⇒ *Development of taxonomies of traces and the decision process attempting to ascribe a trace with sufficient confidence to its class on the basis of characteristics that are common among traces of the same class, distinguishing them from traces of other classes*

Taxonomy	Ascription
• Scientific process that creates and defines classes	• Process that recognizes an element as belonging to a specific class

- Ascription can be considered as trace identification within the context of a taxonomy

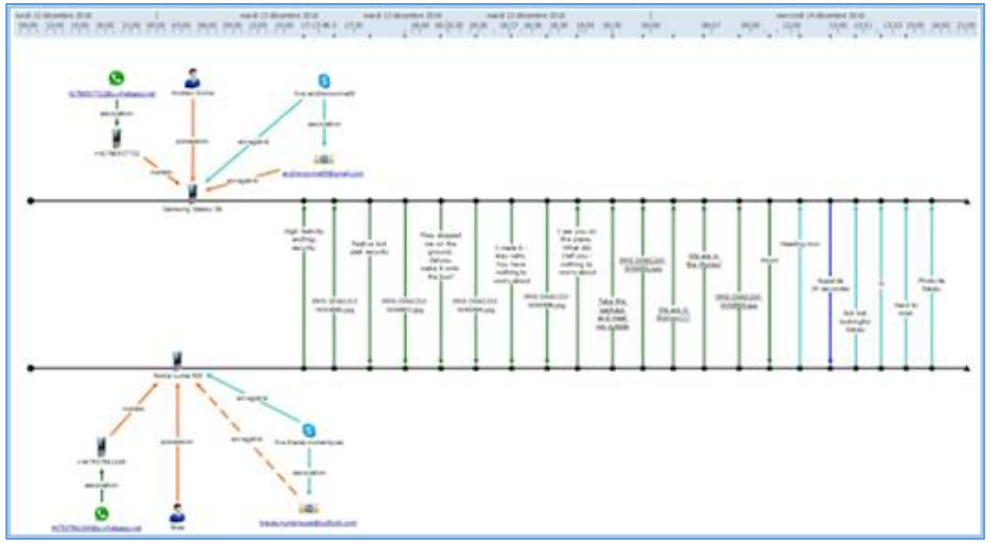


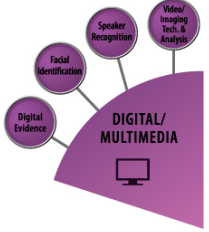
Core forensic processes: (4) Reconstruction

⇒ *Organize observed traces to disclose the most likely*

- *operational conditions or capabilities (functional analysis)*
- *patterns in time (temporal analysis)*
- *linkages between entities - people, places, objects - (relational analysis)*

- To ensure completeness & correctness, reconstruction typically relies on results from the other core forensic processes
- Reconstruction can support authentication, identification, classification, and evaluation



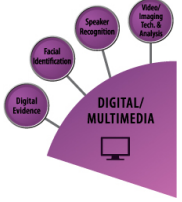


Core forensic processes: (5) Evaluation

⇒ *Produce a value that can be fed into a decision*

- Evaluation precedes every decision in the forensic lifecycle, including the other core forensic processes
- In a forensic context, at least two competing claims need to be evaluated and compared in order to prevent some forms of bias

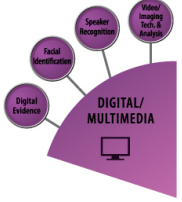
Evaluating Claim	Evaluating opposing claims
• The observed traces are more likely given one claim	• The observed traces are less likely given the other claims



Expressing probative value of forensic findings

Strength of evidence (appropriate)	Strength of hypothesis (inappropriate)
"The observed traces are more likely under the claim that the person depicted in image X is the same as the person depicted in image Y."	**"It is more likely that the person depicted in image X is the same as the person depicted in image Y given the observed traces."**

In courtroom contexts, to avoid encroaching upon the role of decision-maker, forensic scientists must exercise caution when expressing the probative value of forensic findings, concentrating on the well-established knowledge of traces in their domain of expertise rather than on the claim under consideration.



Supporting activities and techniques

Forensic activities

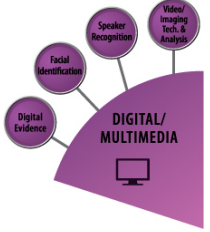
(feed core forensic processes)

- Survey
- Preservation
- Examination
- Documentation
- Analysis
- Integration
- Interpretation

Operational techniques

(support forensic activities)

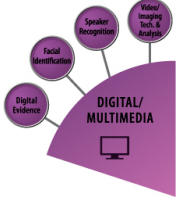
- Preservation
- Recovery
- Enhancement & restoration



Digital paradigm in forensic science

<u>The digital paradigm provides a unique opportunity</u>

- To revisit traditional and fundamental concepts in forensic science
- To harmonize forensic science disciplines
  - with common core principles and concepts
  - with unifying processes and definitions
- To strengthen the identity of forensic science as a whole



Recommendations

- There were seven specific recommendations articulated in this document. They revolve around three themes:
  - Discuss and develop the core concepts and terminology to further improve the framework described in this document.
  - Further explicate the scientific foundations of the processes, activities, and techniques utilized in forensic science.
  - Examine ways to minimize bias, improve the characterization of results, while improving the quality of the results.

Return to:
Focus Areas and Challenges

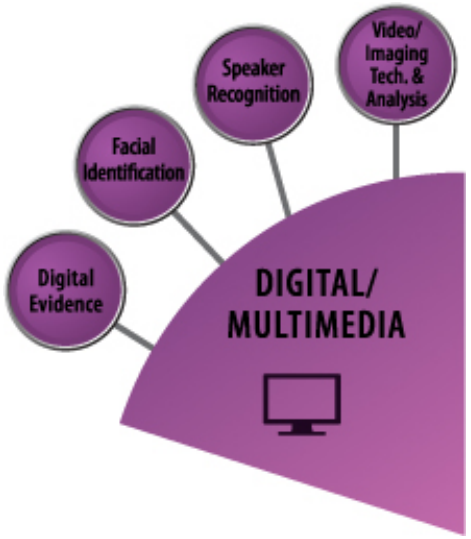
- **Some Key DMSAC (& OSAC) Challenges:**
  - **Accreditation**
  - **Conclusion Scales – Coordinate with P/PESAC**
  - **<u>Terminology</u> – Discipline-specific vs. Global**
  - **Error Rates through Testing Examiners**
  - **<u>Foundations</u>**

- **Scientific Paradigm for Digital/Multimedia Forensics**

Return to:
Focus Areas and Challenges

- **Some Key DMSAC (& OSAC) Challenges:**
  - **Accreditation**
  - **Conclusion Scales – Coordinate with P/PESAC**
  - **<u>Terminology</u> – Discipline-specific vs. Global**
  - **Error Rates through Testing Examiners**
  - **<u>Foundations – Questions asked and Answered</u>**

- **Scientific Paradigm for Digital/Multimedia Forensics**



QUESTIONS/DISCUSSION?

Richard W. Vorder Bruegge, Ph.D.
Digital/Multimedia SAC Chair
Federal Bureau of Investigation
February 20, 2017