Required Elements For Constructing A Highly Adoptable And Adaptive Digital Forensic Model

Ken Rodgers - Dissertation

Agenda

- Problem Statement
- Purpose of the Research
- Research Question
- Summary of Research Design
- Core Authors and their Contribution
- Data Collection Process
- Data Analysis Techniques
- Summary of Findings
- Summary of Conclusions
- Summary of Implications
- Recommendation for Future Research

Problem Statement

The field of digital forensics has failed to unilaterally accept a digital forensic process model, despite the availability of over 25 models since 1995 (Bulbul et al., 2013; Casey, Katz, & Lewthwaite, 2013; Mushtaque, Ahsan, & Umer, 2015; Park, Kim, Park, & Chang, 2018).

Research Purpose

- To establish a comprehensive list of elements that are required to create a widely accepted digital forensic model since a widely accepted digital forensic model has not yet been adopted

- This research contributes to the broader knowledge of digital forensic model requirements and can later be used to develop a model which is widely appealing in the digital forensic community.

Research Question

- What acceptable digital forensic model elements are required to create a widely accepted digital forensic model with a high degree of usefulness, a low degree of difficulty, and the capability of organizational acclimation through adaptation?

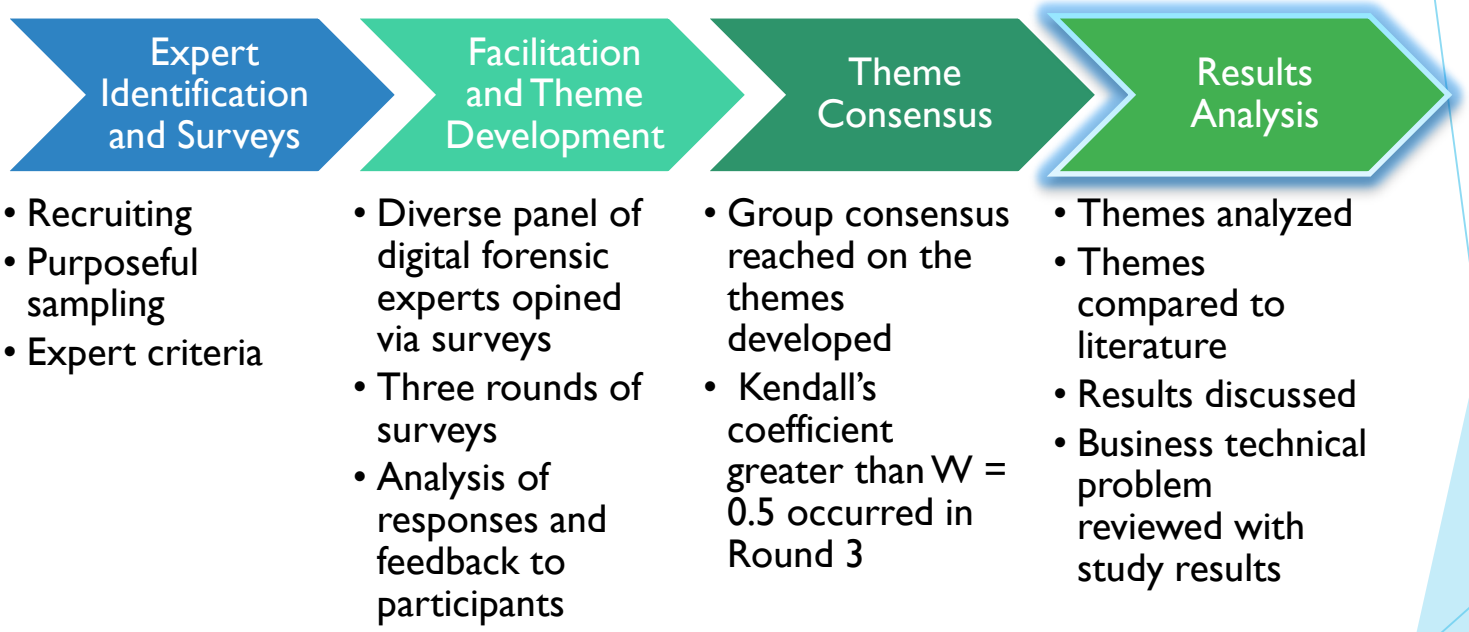
Research Design and Methodology

- Method: Qualitative
- Design: Modified Delphi
- Delphi average panel of experts is somewhere between 10 and 100 panelists (Avella, 2016)
- Sixteen experts from the digital forensics field were solicited to obtain a sampling of opinions using the modified Delphi technique.
- Rational
  - The expert opinions are used to answer the research question and explore elements required for a new digital forensic model

Foundational Authors and Their Contributions

- Forensic Models & Elements
  - Bulbul et al., (2013) - Digital forensics: An analytical crime scene procedure model (ACSPM)
  - Adams, Hobbs, & Mann (2013) - The advanced data acquisition model (ADAM): A process model for digital forensic practice
  - Mushtaque, Ahsan, & Umer (2015) - Digital forensic investigation models: An evolution study
  - Satti & Jafari (2015) - Reviewing existing forensic models to propose a cyber forensic investigation process model for higher educational institutes.
- Design and Methodology
  - Avella (2016) - Delphi panels: Research design, procedures, advantages, and challenges
  - Creswell, J. W., & Creswell, J. D. (2018). Research design: Qualitative, quantitative, and mixed methods approaches. Sage publications

Data Collection and Analysis Techniques



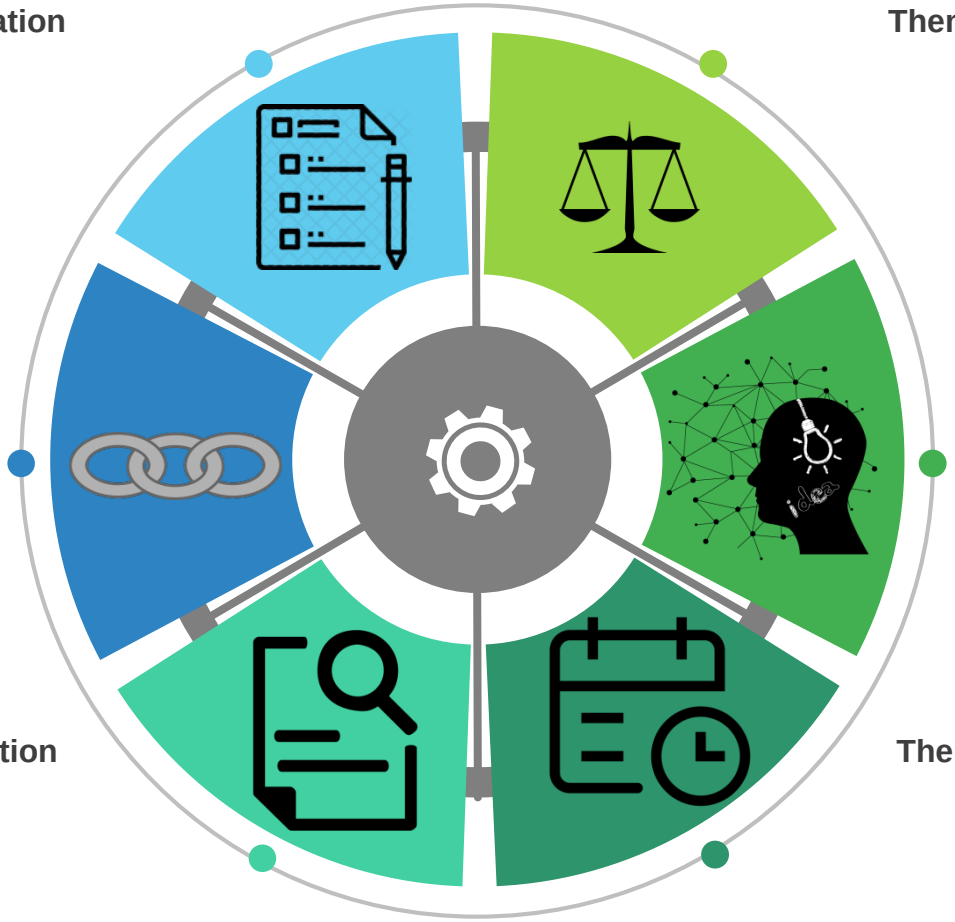
Summary of Findings: Modified Delphi

- Twenty experts recruited
- Actual sample size was 16 after attrition
- Consensus after 3 rounds of surveys
- Six themes emerged with consensus among the participants: Authority, Preparation, Triage, Examination, Chain of Custody, and Post Examination.

Six Themes

Theme 6: Post Examination

Theme 1: Authority



Theme 5: Chain of Custody

Theme 2: Preparation

Theme 4: Examination

Theme 3: Triage

Expert Criteria and Demographics

100% Considered An Expert By Courts Under Rule 702

100% Have Testified In Actual Or Moot Court

100% Certified Though A Forensic Training Course

100% Are U.S Citizens

87.5% Work In The Public Sector

12.5% Work In The Private Sector

62.5% with 5-10 Years Experience

37.5% with 10+ Years Experience

Delphi Themes

- Theme 1: Authority
- Theme 2: Preparation
- Theme 3: Triage
- Theme 4: Examination
- Theme 5: Chain of Custody
- Theme 6: Post Examination

Summary of Findings and Contributions

- Theme 1 is Legal Authority such as consent or a search warrant. This theme suggests that any forensic models built should include permission for the examination to take place
- Theme 2 is Preparation. It includes, but it not limited to verification of authority (Theme 1), tested/verified equipment, and personnel training. Theme 2 contributes to the construction of a new digital forensic model by providing some areas of preparation to consider and allows for expansion to other areas of preparation when building a new model
- Theme 3 is the use of a Triage Process. Suggests a new model will need to give consideration to prioritizing what is actual digital evidence, which items need to be examined first, and the use of hashing for verification of digital evidence

Summary of Findings and Contributions

- Theme 4 is Examination. Including analyzing digital evidence and recording results in a report. These identified actions provide another area of substance that is needed for construction of a digital forensic model and can be further defined, expanded, and honed by anyone building their own model
- Theme 5 is Chain of Custody usage for evidence. This theme is relevant for inclusion in any new forensic model because in the United States, the Federal Rules of Evidence contains procedural rules guiding the usage of evidence, which includes ensuring evidence is authentic and identifiable
- Theme 6 is the Post Examination actions. What comes after the forensic examination is an important part for consideration in any new models. Whether this includes court prep, post exam hashing, or evidence destruction.

Summary of Conclusions

- The modified Delphi study was concluded showing 6 themes produced by digital forensic experts in the field, helping identify elements required for creating a digital forensic model identified in the research question
  - Supports prior research verifying the significance of some elemental areas (e.g., Adams, Hobbs, & Mann, 2013; Wilson-Wilde, 2018)
  - The participant's responses also supported the literature review in that there is no widely used digital forensic model, with only 37.5% of the participants using an official model of any kind at their organization
- The identified themes deliver a potential baseline for future development and construction of a highly adoptable and adaptive digital forensic model. Having a widely used digital forensic model can aid in cross jurisdictional cases and allow for more standardization in the field of digital forensics

Summary of Conclusions

- Identified themes also provided elements experts opined would have a high degree of usefulness, easy to incorporate, and likely adoption by organizations constructing a new digital forensic model.

Summary of Implications

- The study produced 6 elemental themes which can be used to form a baseline when producing a new digital forensic model. The 6 themes alone can potentially form a founding model that all subsequent new models could diversify from (if needed). Using Adaptive Radiation, organizations can expand and branch off from this baseline as needed for their required environments or challenges

Recommendations for Future Research

- Perform more studies to create an officail baseline digital forensic model that has the core theme elements, but can expand as needed to fit any situation or future technological advances plus take advantage of new technologies
- Studies to detail barriers to model adoptions to date and possible solutions
- Further studies seeking expansion and adaptation of these results to other countries and other legal environments

Questions?