Modeling Forensic Evidence Systems Using Design Science

Colin Armstrong, Helen Armstrong

17 MODELING FORENSIC EVIDENCE SYSTEMS USING DESIGN SCIENCE

Colin Armstrong
Helen Armstrong
School of Information Systems
Curtin University of Technology
Bentley, WA, Australia

Abstract *This paper presents an overview of the application of design science research to the tactical management of forensic evidence processing. The opening discussion addresses the application of design science techniques to specific socio-technical information systems research in regard to processing forensic evidence. The discussion then presents the current problems faced by those dealing with evidence and a conceptual meta-model for a unified approach to forensic evidence is developed. Any practical application of the suggested model would be predominantly law enforcement driven; evaluation of sections of the model has been carried out by law enforcement participants in several international jurisdictions.*

Keywords Design science research, socio-technology, forensic evidence

1 INTRODUCTION

Design science is not just a methodology for devising solutions utilizing technology. It is an approach that offers the researcher the ability to investigate problem spaces and devise theories and designs that could address such problem spaces. Most problem spaces encompass various stakeholders, each with a particular perspective on that problem. The field of forensic evidence is no different, with three main stakeholder groups: law enforcement, the first responders to a crime situation; forensic scientists,

who take physical items (DNA, weapons, disk drives, mobile phone, etc.) and, using scientific standards and methodologies, form opinions and interpretations of the evidence; and the judiciary, who employ information about the evidence derived from law enforcement and forensic science to present arguments for either the prosecution or defense.

Electronic devices are increasingly appearing as important items of evidence in criminal investigations, due to the spread of technology and society's dependence upon that technology in everyday life. Although digital forensics is a frequent topic in information systems security research, the focus in this area is broadening to consider the links between all types of forensic evidence (digital and otherwise) for many types of traditional crime, not just computer crime. This is due to the increasing amount of potential evidence stored electronically on devices such as computers, Internet and ISP servers, mobile phones, portable storage devices, and other electronic devices and media for traditional and digital crimes.

Investigation of the area of evidence illustrates a number of problems emerging as technology becomes more pervasive. Using design science as the chosen research approach, this paper describes a study of the forensic evidence problem space through the perspectives of the three main stakeholder groups and the design of a meta-model for the effective management of forensic evidence at the tactical level. The meta-model presented provides an opportunity to employ a number of different technological solutions, depending upon the perspective and needs of the interested party. As law enforcers are the stakeholders with the majority of exposure to, and interaction with, evidence, the evaluation of the suggested processes and models has been undertaken by a focus group of experienced law enforcement officers.

2 WHY DESIGN SCIENCE?

Evidence takes the form of both physical objects and information about those objects. Evidence can be comprised of fragments of disparate data that combine to produce something larger and more meaningful in the context of the investigation. So why design science? In design science research, "knowledge and understanding of a problem domain and its solution are achieved in the building and application of the designed artifact" (Hevner et al. 2004, p. 75). Furthermore, design science attempts to create things that serve human needs (March and Smith 1995) and benefits those affected by the problem situation. With the focus on designing solutions Design Science is an ideal approach for the analysis of the forensic evidence problem space and the design of a model to eliminate or reduce that problem domain.

3 DESIGN SCIENCE AND SOFT APPROACHES

Much of the literature in support of design science focuses on the engineering or "hard" side involving scientific rigor pertaining to the physical artifact and technology (together with the associated systems development). However, the "soft" side of information systems recognizing the social and organizational aspects is also emerging.

Baskerville et al. (2007) highlight the need for a soft design science research approach to accommodate IT/IS artifacts in natural organizational settings. Information systems encompass both social, human, and organizational aspects, as well as tools and technology, and all of these aspects need to be considered in problem studies and the associated solution design. Checkland and Scholes (1990) discuss the need to recognize that problems are seen through the world view of an individual, which they refer to as the *weltanschauung*. Human beings "interpret what they perceive. Moreover, the interpretation may, in principle, be unique to a particular observer. This means that multiple perspectives are always available" (Checkland and Scholes 1990, p. 25). In the context of this research the authors propose that world views can be either individual or group perspectives, depending upon the nature and scope of the problem domain under consideration. A full understanding of the problem situation incorporating the perspectives of the different stakeholders provides a holistic view for those attempting to design solutions. Softer approaches also permit the consideration of social and political issues that form an integral part of problem situations. The consideration of human and organizational issues is crucial for the design and implementation of effective solutions.

March and Smith (1995) and March and Storey (2008) propose the two cornerstones of design science as building and evaluating artifacts. In order to design, build, and evaluate artifacts, it is necessary to understand the problem causes and impact to ensure that the artifact does actually address the problem.

4 THE PROBLEM SPACE

A problem exists when a stakeholder in a given situation perceives there is a difference between the desired state and the current state (Checkland and Scholes 1990; Jayaratna 1999; Jonassen 2000). Key to the recognition of a problem is that a stakeholder group affected by the situation perceives a gap between the two states. The same problem can be perceived differently by each stakeholder group within the problem situation based upon their perspective of the world. In order to fully understand a problem situation, the perspectives of different stakeholder groups must be considered. To be of value and significance, design science should address a class of problem (faced by a collection rather than by one individual), be nontrivial in nature (significant), as well as relevant (germane and useful).

A clear understanding of the problem and its causes is needed in order to develop a theory relating to the design of a solution and also before an in-depth design of a solution is embarked upon. As the aim is to reduce or eliminate the problem space, interaction with theory conceptualization and development, the solution design process, plus the solution evaluation is essential.

5 THE SOLUTION SPACE

Inextricably linking the problem and solution spaces is the theory space. Walls et al. (1992) differentiated design theory from scientific theory by considering the overall

objectives of each. While scientific theory seeks to understand and predict natural phenomenon, the aim of design theory is to guide artifact creation. March and Smith (1995) and later also Venable (2006) note the interchangeable nature of models and theories as forms for representing knowledge

Venable highlights the importance and inclusion of theory building as a specific component of the design science research process, claiming that theorizing and theory building actually occur before, during, throughout, at the end, and as a result of design science research. Venable proposes a cyclic approach that recognizes the central role played by theory and theorizing.

The theory realm holds value as the theory or hypothesis is expressed in a design with particular application to the given problem space. The theory realm also is dependent on the stakeholder's perspective. Where particular stakeholder groups are removed from consideration, there will be no debate or understanding of the holistic situation. A holistic viewpoint facilitates and promotes a successful solution design and ownership of the artifact.

The design is a conceptualization of a specified solution that is one of many potential solutions envisaged to reduce or eliminate the problem. Each potential solution is an instantiation of a conceptualization and, in information systems terms, a solution design could be a detailed physical model illustrating application in a specific *in situ* or a logical model that could be applied in a number of physical modes.

A project to investigate the problem space in forensic evidence management and the design of a socio-technological solution space has been undertaken. With a strong socio-political element, the solution design devised took the form of a meta-model enveloping, a number of lower-level interactive models to shape a management system. An iterative approach was employed in this research using three main stages of data collection and analyses (see Figure 1). The stakeholders were interviewed in three groups over a period of two years, with participants in the judiciary, forensic practitioners, and law enforcement stakeholder groups interviewed in each period. This enabled a gradual development of the model together with solutions on a progressive basis. The data gathered in stages 2 and 3 was used to confirm the findings from the interviews in earlier stages and further develop the new model and solutions.

6 FORENSIC EVIDENCE PROBLEM SPACE

The essence of the forensic evidence problem space is the disparate conceptualization of the usage and tactical management of evidence. Exposure and association with forensic evidence by the three primary perspective groups is sequential in nature and the three groups do not enjoy forensic evidence associations equally. A simplistic observation would describe law enforcement as the first responders, forensic scientists as the experts, and the judiciary as that highly respected independent determinator of an accused's fate. The problem space of the forensic evidence management project is illustrated in the rich picture presented in Figure 2. The nature, purpose, and importance of forensic evidence is viewed differently by each of the stakeholder groups and, with no common understanding or standards to underpin the realm, misunderstandings commonly arise.

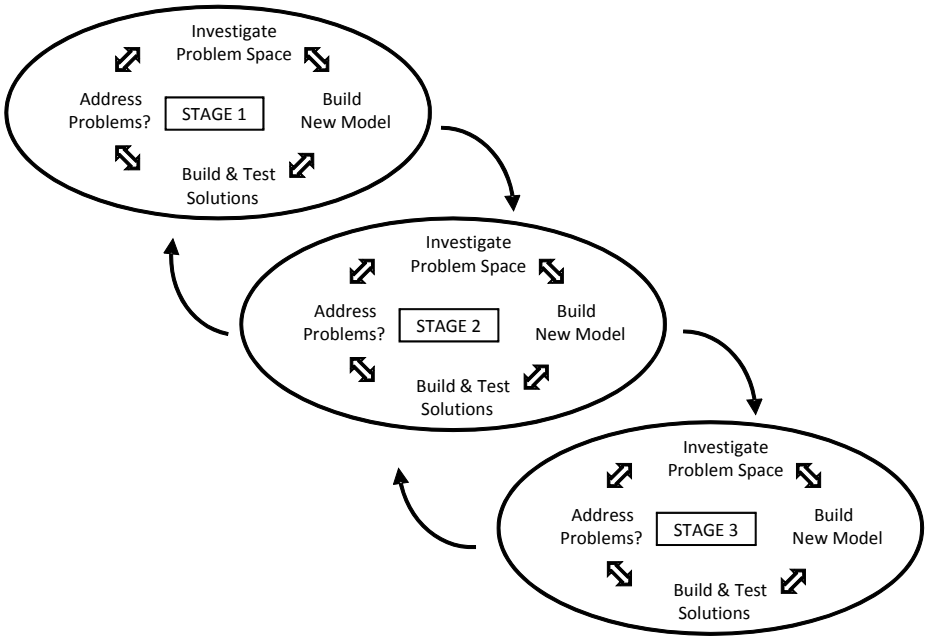

Figure 1 Iterative Approach Employed in the Research

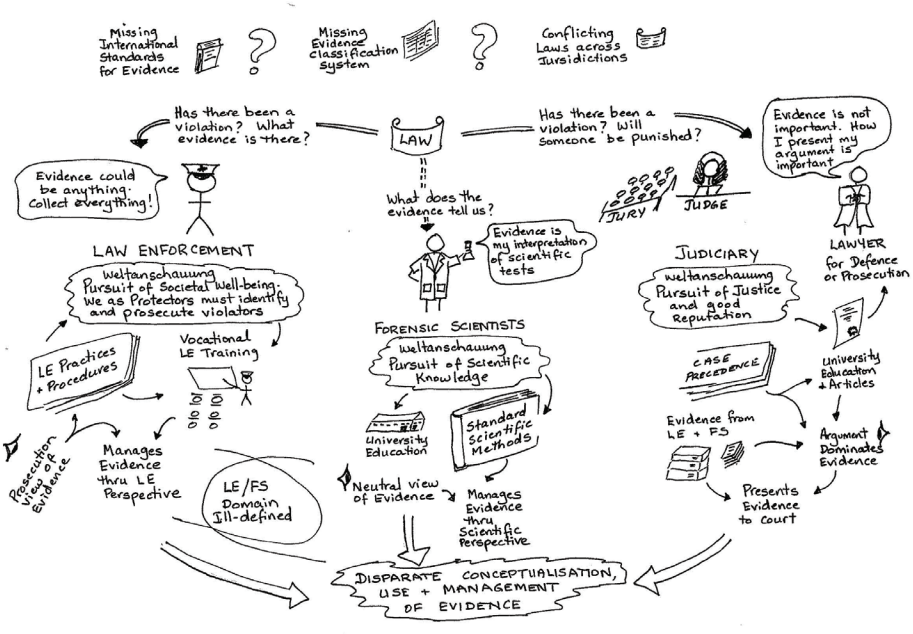

Figure 2 Forensic Evidence Management Problem Space

Once a perceived wrong has been brought to the attention of the enforcers of law, an enquiry may commence and, to discover the facts behind the perceived wrong, evidence is sought. To better interpret and understand the meaning of evidence, we rely on scientific expertise. Finally, when sufficient information is gathered, it is presented in order to persuade the finder of fact in determining an accused's guilt. The association between evidence and each of these three perspectives reflects very different relationships, as can be seen in Figure 2.

The law enforcement community has the greatest exposure to forensic evidence. It identifies and collects the evidence at the scene of a violation; it manages the safe handling of the evidence in order for it to be admissible to a court of law; it directs the appointment of forensic scientists for evidence analysis and collates forensic results; and finally, it presents evidence in court predominantly representing the prosecution. Forensic scientists carry out testing and analyses specific to the inquiry, and the judiciary presents evidence to support an argument of guilt or non-guilt.

The lack of standard procedures, underlying classifications, and international standards relating to evidence, as well as differing laws, has a major effect upon law enforcers, in comparison to the minor influence it plays for the judiciary and forensic scientists.

6.1 Law Enforcement

Law enforcers are held responsible, not only as first responders to secure evidence locations; in most situations, they are solely responsible for the collection and management of forensic evidence. Law enforcers are considered less-educated blue collar workers and, therefore, not as well qualified to assess issues as forensic scientists or the judiciary. They tend to be faced with the chaotic frontier of humanity at its worst and tasked with responsibility for forensic evidence management while being required to preserve peace and security in our communities. This situation results in little or no time for law enforcers to contemplate the intricacies of an incident and, because anything could be evidence, adopt the practice of collecting everything.

Law enforcers do not have internationally agreed standards ensuring unified best practices for forensic evidence processes, relying on jurisdictional policies and procedures. This does not suggest that law enforcers do a poor job. It does suggest, however, that even though there is a great deal of international cooperation and that enforcement agencies and personnel strive to provide the best service, there is little national or global agreement as to what constitutes best practice and service.

6.2 Forensic Scientists

Unless working alongside law enforcers, forensic scientists are not first responders, do not secure evidence locations, do not collect evidence, and are only responsible for the management of forensic evidence while it is in their care for analysis. Forensic scientists often become involved only after law enforcers have collected potential evidence. As forensic scientists usually have university education in a scientific field, they

are perceived to be educated and professional experts in their particular domain of research. This group is perceived to be experts without a bias toward either prosecution or defense because they pursue discovery of facts based on dispassionate scientific methods. Hence, forensic scientists are perceived to be divorced from determinations of guilt or otherwise.

Forensic experts are regularly afforded the luxury of retiring to a secured laboratory far from the influences of a chaotic world and, therefore, have more time and an environment more conducive to contemplating the meaning of evidence items. Forensic experts are often excluded from the rest of an enquiry and only called upon for specialized expert opinion. When granted access to complete case file information, forensic experts do have time to contemplate the intricacies of an incident. Generally, forensic scientists are only associated with particular items of case evidence and not with every collected item.

As scientists, forensic scientists are members of organizations that are international and that establish and maintain agreed standard practices for conducting scientific processes. Many fields within forensic science have their own classification systems or methods of categorizing objects; however, these are isolates and form well-defined boundaries resulting is discrete, unintegrated systems.

6.3 Judiciary

Although the judiciary group members fall into three separate subgroups—prosecution, defense, and finder of fact—they have yet another point of view relating to evidence. Judiciary group members tend to focus most strongly on interpretations of evidence that support their particular objective: either proving guilt, defending and disputing evidence interpretations, or passing culpability judgement. The judiciary are rarely first responders; they are not responsible for securing evidence locations or collecting evidence, but they are responsible for the management of forensic evidence if it is given into their care.

In contrast to the law enforcement and the forensic science stakeholders, the judiciary believe the evidence itself is not the key factor, but their presentation of the argument pertaining to that evidence in a court of law, or in other words their ability to persuade the finders of fact of guilt or innocence. The judiciary is perceived by society as being highly educated as well as respected, independent determiners of an accused's fate. The judiciary often deals with the worst results from the chaotic frontier of humanity, but does so in the comfort of a secured environment. The judiciary is not perceived as being expert in scientific matters but do have access to specialized publications relating scientific matters to the law and legal precedents. This group specializes in contemplation of evidence, its meanings, and the case in question before the courts and, by ensuring decisions are not hasty, engenders the perception that evidence matters are well and carefully contemplated. However, the judiciary only deals with a small but essential selection of the total collected case evidence and features only that evidence supporting the prosecution or defense case.

The judiciary maintains a deep abidance to rigorously established rules and procedures relating to evidence that are accepted internationally even though the same set of rules are not applied in the same manner in every jurisdiction.

6.4 Global and Local Problems

The resulting operational situation presents law enforcers with having to resolve a problem situation because it has greater impact on their operations than the other two perspective groups. The forensic scientists are, for the most part, isolated from the entire case under investigation and limited to providing an expert opinion of the evidence based on scientific principles. Finally, the judiciary determine justice based on only that small amount of evidence essential to argue their case.

The problems emerging from this consideration are both global and local, and include

- a lack of international standards, policies, and procedures for the identification, collection, analysis and presentation of evidence
- no classification systems for evidence, only classifications and categorization for certain types of objects that may be used as evidence
- the lack of tools and techniques to provide a big picture in the consideration of criminal cases, resulting in a piecemeal rather than informed, holistic approach to decision making about evidence
- the bias of perspective and the different perspectives of the stakeholders, resulting in the value of evidence being viewed differently by each of the stakeholder groups

7 FORENSIC EVIDENCE THEORY AND MODEL DESIGN

An extensive archival search was conducted to identify prior work done to address the above problems and any standards or models already developed in the area. The findings were that the work has been piecemeal with no interdisciplinary solutions proposed. In all, 52 professionals across the three domains were interviewed and data collected regarding the nature of evidence, the problems they faced, and a desired state. A set of models was then developed based on analyses of that data.

The models, designed to reflect perspectives in forensic evidence tactical management, draw upon established theories and modeling approaches. The journey along the evidence path from raw data to courtroom-presented evidence is at times complex and chaotic. No single theory adequately addresses the modeling of forensic evidence. There are two main streams of theory providing the elements underpinning such modeling. The first approach addresses the organization of evidence, which draws on theories associated with systems. The second approach accommodates the nature of evidence, which includes legal perspectives.

General systems theory is the overriding approach to the organization of evidence and associated information. To this are incorporated elements from a number of interconnected theoretical bases including chaos theory, complexity theory, network theory, social–network theory, and actor–network theory.

The overriding theories addressing the legal perspective are legal theory and evidence theory, which are strongly linked with justice and policing theories. As burdens of proof are not absolute they are dealt with as probability values. Probability theory is

in turn accompanied by Bayesian statistical theory and Dempster-Shafer theory. In addition to theories, principles such as Locard's exchange principle are applied to the analysis of crime scenes.

Other theories contributing to the design of these models include elements from Heisenberg's uncertainty principle, information theory, scientific theory, model theory, and stakeholder theory. The development of the designed models draws on elements from these theory foundations.

The aim was to design a high-level conceptual model that provided an interdisciplinary view of tactical management of forensic evidence. Such an approach offers a broad opportunity to satisfactorily address the challenges presented in the forensic evidence problem space. A unifying holistic forensic evidence model necessarily consists of components specifically designed to address both global and local problems. There are six components considered desirable for inclusion in a model for the tactical management of forensic evidence processing.

1. A method for understanding the transitional information flow as raw data related to forensic evidence changes to become evidence due to the information that practitioners extract from the raw collected data and convert into knowledge.
2. A method for determining the particular relationship between the enquirer and the evidence.
3. A system for examining the interrelatedness of forensic evidence in a network of case evidence.
4. A method of visualizing forensic evidence networks.
5. A repository for forensic evidence information.
6. A system to accommodate classification of forensic evidence, and provide standards and best practices.

The Armstrong forensic evidence meta-model (see Figure 3) brings together the six components identified as desirable for the tactical management of forensic evidence processing. Modeling the six components reveals that four components are processes and two are frameworks. Modeling also reveals that two components address sociological aspects and four components address technological aspects of forensic evidence. The six models forming the meta-model are

- evidence data to knowledge conversion
- evidence stakeholder perspective
- evidence relationships network
- evidence resource library
- evidence network analysis
- evidence classification scheme

The *evidence data to knowledge conversion* process (see Figure 4) models an entry point into the inquiry-related data and provides the mechanism for determining the status of evidence entering an inquiry. Some data is self evident in nature and less disputable than other data. During the processes inculcated in this model, initial statistical data col-

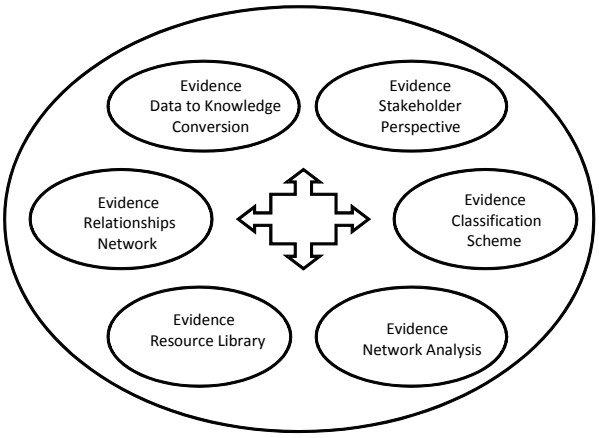

Figure 3 The Armstrong Forensic Evidence Meta-Model

lection commences and practitioners form conclusions based on the accumulation of data. The major contribution of this process is in the modeling of data integrity entering an inquiry.

During the inquiry process, all incoming evidence arrives, initially, as data, and in a spasmodic manner. Then, as reasoning and analysis commences, the data undergoes a transitional process that sees some data progress to become knowledge based on information processing while other data items may be held awaiting further clarification, discounted, or discarded.

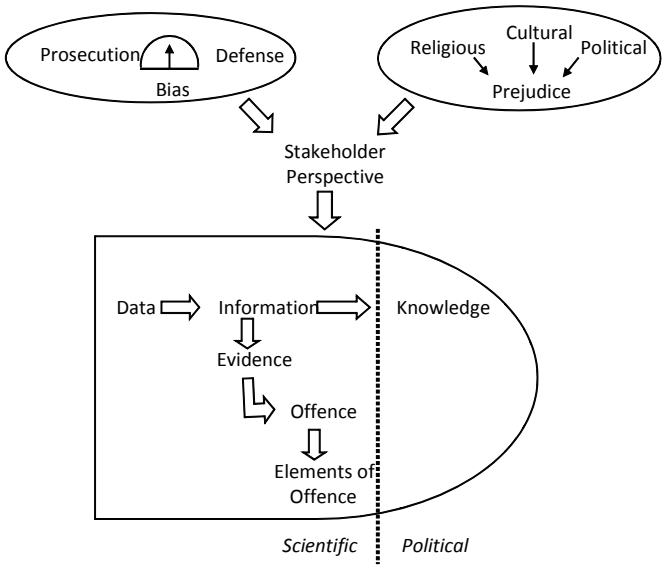

Figure 4 Evidence Data to Knowledge Conversion

Evidence can only exist in the human mind and it is that information that persuades. Forensic evidence is that information that persuades to a level determined by the court within a jurisdiction's legal system. Commonly in matters of civil dispute the burden of proof is "in all likelihood," and in criminal matters the burden of proof is "beyond a reasonable doubt."

This process models the data transition by requiring the inquirer to recognize the bias and prejudices they will be perceived to possess. Recognition of the inquirer's perceived associations to the evidence is essential in determining the meanings attributed to evidence interpretations. The purpose of establishing the inquirer's association to evidence is not to change the meanings attributed to evidence analysis but rather to better understand the reasoning processes that have lead to conclusions based on the analysis of evidence.

The purpose of modeling the transitional nature of data into evidence is to understand better how the evidence explains what occurred.

The *evidence stakeholder perspective* (illustrated in Figure 5) provides the mechanism for assessing the justification of a practitioner entering the enquiry and illustrates the practitioner's relationship to evidence. This facilitates a mechanism for determining bias and defines the extent of the practitioner's engagement in the enquiry process. The major contribution of this process is the explicit statement of association between enquirer and evidence.

As an inquirer may enter the inquiry process at any time during the process, their entry should be justifiable, having a legitimate reason for being granted access to the case evidence. Without a clear purpose for entering the inquiry process, access should be denied. Each entrant to the inquiry process will possess attributes deemed desirable that will contribute to drawing the case to a satisfactory conclusion.

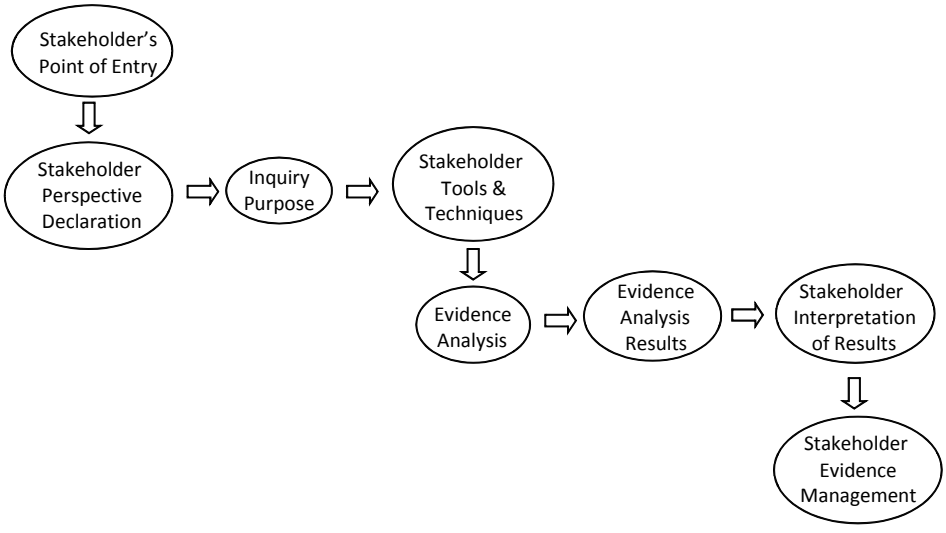

Figure 5 Evidence Stakeholder Perspective

Having been granted entry to an inquiry, the next step requires an explicit recognition of the bias and prejudices the entrant may be perceived to possess. The entrant will possess skills, knowledge, and qualifications considered worthy in furthering the progress of the inquiry but others may maintain an opinion as to how the entrant may conduct evidence analysis. As evidence may be defined as information possessing an ability to persuade, it is important to also understand the persuasive nature of the inquirer. The persuasive nature of the inquirer is directly associated with how others perceive them.

The next step in the inquiry process requires determining the purpose for which the entrant has been granted access to case evidence. The reason for entering the inquiry process designates the scope of conduct permitted to the inquirer. There are many reasons one may seek access to evidence, including: crime scene reconstruction based on forensic evidence, determining appropriate storage of evidence items, developing an evidence matrix for determining commonalities between witness statements, filing inquiry information, and determining appropriate methods of evidence analysis. The reason for limiting the scope of inquirer activity with the evidence is to assist in ensuring that the integrity of the evidence is not damaged during the progress of the investigation, and that the entrant only conducts those activities deemed necessary by their role.

Based on the entrant's skills, knowledge, and qualifications, together with a defined purpose, the inquirer may choose certain tools and techniques to apply to the evidence. It is important that the choice of tools and techniques are appropriate to the entrant's reason for accessing the evidence.

Once the preceding steps have been achieved to a level commensurate with the nature of the inquiry, the entrant may access the evidence. It is at this stage of the process that the inquirer shall conduct whatever examination of the evidence meets the specific needs of the inquiry. Following the examination and analyses of evidence, the results are produced, with such results varying dependent upon the nature of the examination process. Having obtained sets of analysis results, the inquirer sets about interpreting meanings to explain those particular aspects of the case being examined.

The final step in the inquiry process refers to evidence management. During a complex inquiry, there may be many subordinate inquiry processes, some conducted sequentially, others concurrent to the overall inquiry. Evidence management in this step relates only to the inquirer at hand and their management of the materials passing into their realm of responsibility. Most inquirers will only have access to small selections of the complete set of case related evidence. Having conducted their specific tasks with the evidence, the evidence continues along the inquiry process journey. Depending on the nature of the tasks conducted, the evidence may continue its journey, may have been subjected to destructive testing, or may transition into a case report.

The *evidence relationships network* (see Figure 6) process provides explanations for the linking relationships of categorized enquiry evidence discovered by practitioners when adopting a link perspective of evidence. As we tend to focus on what we can directly see, the major contribution of this process is directing the enquirer to examine the intangible links.

The purpose of this process is to understand the relationships between evidence, the inquiry domain, and other sets of information affecting evidence.

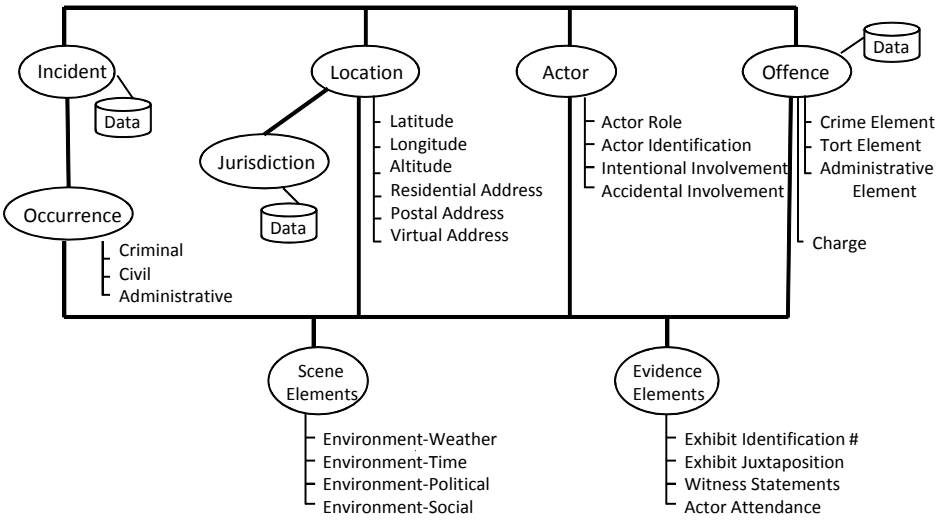

Figure 6 Evidence Relationships Network

Within the inquiry domain, certain common elements tend to be associated with an inquiry. The common elements are attributes associated with the incident, its location, the associated actors, and an offence. Evidence tends to be directly or indirectly linked to one or more of these four elements. This process draws the inquirer to identify the intangible links that exist between these four elements. The intangible links may exist between what, when, where, who, why, and how with incident, location, actor, and offence. The intangible links may relate to actions, inactions, ownership, possession, and knowledge of, or assist in explaining causes and effects.

The *evidence network analysis* (see Figure 7) process provides a network science perspective of an inquiry, thereby permitting visualizing the inquiry as an interrelated web and additionally providing a mathematical method for describing the relationships

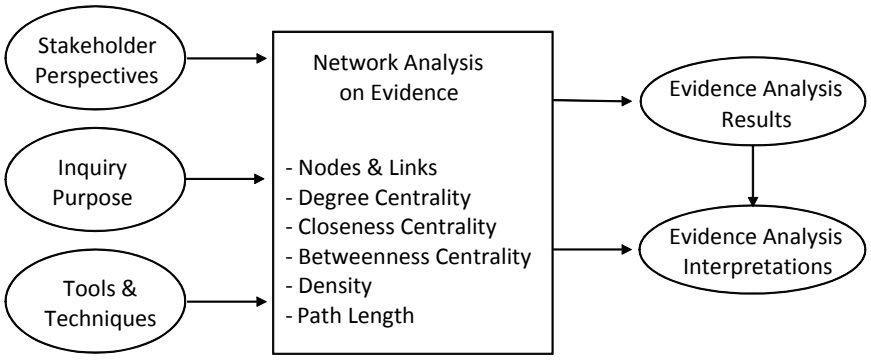

Figure 7 Evidence Network Analysis

between evidence items. The major contribution of this process is the statistical analyses and visualizations of links and the absence of links that are enabled by adopting network science techniques.

The network science approach models objects in a defined situation as nodes, joined by links or relationships. A network consists of nodes linked to other nodes. Network science provides the underlying theory, tools, and techniques for determining the strength of nodes and links, and analyzes the changes in network structure and linkages in a dynamic situation. The importance of a node is measured according to a few simple rules. Determining the importance of networked nodes is achieved by examining centrality measures of degree, closeness, betweenness, and path length, in addition to overall network density. These measures indicate the strength of a node based on how well it is connected to the rest of the network.

Network science is used to analyze and visualize evidence relating to an inquiry. Plotting the evidence associated to a particular inquiry offers a perspective that may be focused on individual evidence items, or to a case as a whole. The network nodes are representations of individual evidence items, and, at finer levels of granularity, of evidence item attributes, while the links between nodes represent relationships. Network visualizations may be of specific moments frozen in time, or chained together to illustrate a dynamic situation as it evolves.

The *evidence resource library* (illustrated in Figure 8) facilitates practitioners proactively building and managing a repository of evidence-related resources. The major contribution of this process is being a living library of enquiry-related information.

As the scientific and legal efforts supporting forensic evidence continue to progress and develop, consolidation of resources enhances forensic evidence practitioner capabilities. To date much of the work conducted has been restricted to silos of expertise. The resource library models an approach to facilitate interactive multidisciplinary progress of evidence processes. It comprises both social and technological elements, presenting an extensive repository of data in the form of the evidence information system (EIS). The overall motivations of the stakeholders are represented by the top block above the EIS and forms the objectives. Data is contributed by the three stakeholder groups shown on the left-hand side of the EIS, with the action represented by the right-hand block, the project and process management. The technologies applied are shown in the lower block.

The participants interviewed across the three domains agreed that the evidence resource library was the most important component as well as the most difficult to develop as all stakeholder groups need to agree upon the foundation theories, standards, and ontologies. However, the development of such an integrated resource for evidence practitioners is considered an integral component to a holistic model for the tactical management of forensic evidence.

The *evidence classification scheme* (see Figure 9) facilitates the various procedural practices for classifying physical evidence items and, more particularly, classifying forensic evidence relationships. The major contribution of this process is providing a basic foundation for the identification, organization, and categorization of evidence at a global level, for application in law enforcement, forensic science and judicial domains.

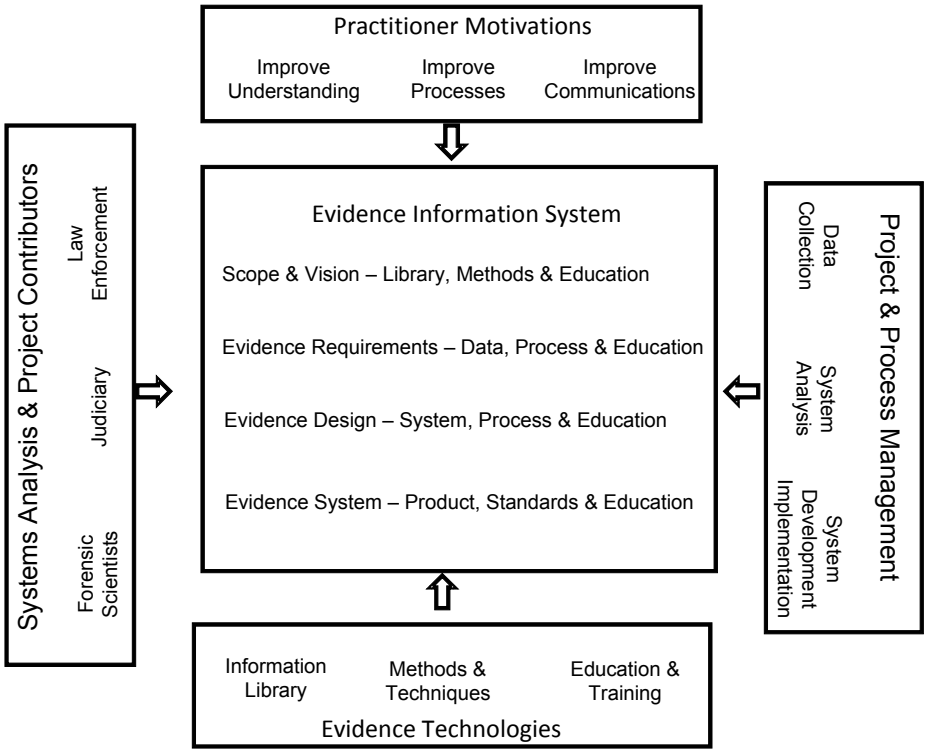

Figure 8 Evidence Resource Library

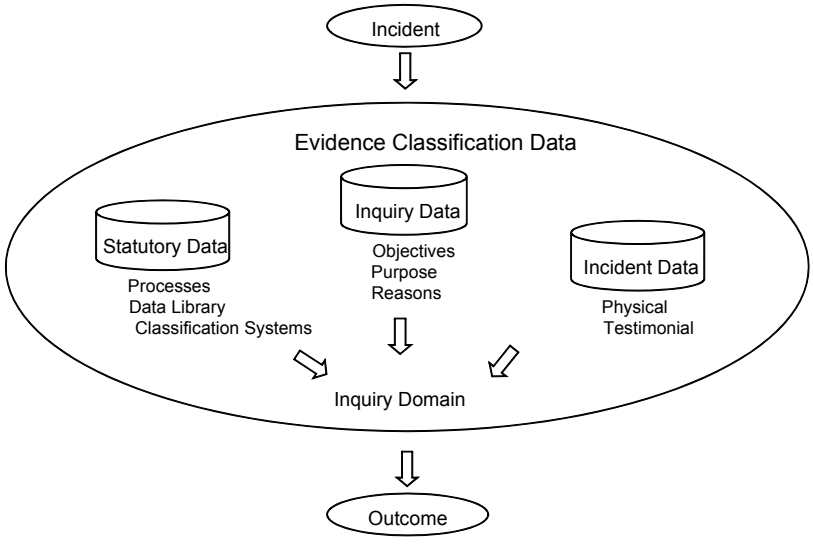

Figure 9 Evidence Classification Scheme

A complex inquiry is made up of diverse components. Apart from evidence associated with the case, there are people from different perspectives charged with undertaking different tasks. Each evidence practitioner, charged with different objectives to achieve, addresses evidence in a different manner. There is confusion arising from variations in terminologies and phrases applied to the same evidence. Legal requirements of evidence also vary between jurisdictions. This process presents a holistic approach to managing these diverse components.

Each evidence practitioner may require a system to organize the evidence set before them. Hence processes are defined to classify evidence items, and relationships between evidence items, according to the purpose of the inquiry.

The integration of the six processes presents a high-level meta-model for more effective handling of forensic evidence and its management across the three stakeholder domains. The meta-model exists only as a conceptual model as further analysis of component processes requires further detailed design before any prototype can be developed and tested in practice.

8 FORENSIC EVIDENCE MODEL EVALUATION

The building of the meta-model took place while interviews with the participants from the three stakeholder groups were in progress. This enabled a progressive development of processes to address problems and suggest potential solutions, moving between design of the new model, the underlying theories and considerations as to how it could be applied in practice. As the law enforcers were the drivers of the change, a focus group of law enforcement officers reviewed the meta-model and applied specific lower-level solutions to actual cases under investigation. A law enforcement focus group was chosen for the initial evaluation before progressing to the other two stakeholder groups. If the conceptual model cannot be applied in law enforcement, then no progression to the other stakeholder realms is justified. The focus group consisted of 10 law enforcement officers, each specializing in a different area and at varying levels of responsibility.

Earlier discussion in the forensic evidence problem space identified four broadly based local and global problems. Over one year, numerous situations were evaluated by the law enforcement focus group members; however, only a small portion of these implementations is reported in this discussion. Evaluation of the model by law enforcers has lead to many instances being suitable examples. These examples are taken from multiple international locations, but are considered to be representative of a local problem space.

8.1 Evaluation Example One

The identified problem was that there was no apparent formalized method or system for determining what the existence or nonexistence of evidence means to an investigation. A implementation of network science was applied to a cold case review instance. Instigating network science techniques raised a line of case-related questions regarding the existence of different evidence items, particularly in regard to information pertaining to bank account, cell phone, and family member contact activity currently as compared

to previous periods, and that at the time of the initial investigation. Analysis of the dynamic network over time was necessary for an informed analysis of the evidence.

Practitioner responses included

- This approach, when compared with our traditional methods, has resulted in significant differences in understanding about the whole case and lead to renewed enthusiasm because of the new lines of enquiry offered.
- The linking of evidence items and the absence of links provided direction for further investigation.

8.2 Evaluation Example Two

The identified problem was that investigators find that sorting and arranging forensic evidence in a meaningful manner is necessary yet impractical. A consideration of different stakeholder perspectives was needed. The model implemented showed that the researcher's association with the case evidence was different than that of investigating officers and that the detective has a different perspective than the police chief and other assisting officers. This implementation also highlighted that the purpose was to conduct a cold case review, examining the collected evidence, and asking questions about the evidence. The evidence had previously been collected and was assembled in one location and available for immediate examination and analysis. Those conducting the investigation were subject to limitations in that the evidence came to them in a piecemeal fashion, not in a sequential manner, and over different time periods. This caused the investigator to see the case evidence in small snapshots spread over a period of time in contrast to a situation where the evidence was available in its totality and sequentially arranged, offering a more holistic perspective.

This implementation facilitated assessment of a solution based on a specific rather than a general evidence classification.

Practitioner responses included

- Until exposed to this concept, evidence was just evidence and we had not thought about the character of evidence.
- Evidence was always associated to a case and that was the end of the story.
- It was not that we did not do some of this stuff, it was just that we did not think about it nor fully understand our associations with the evidence.

8.3 Evaluation Example Three

The identified problem was that there is no apparent agreed method or system for describing or grouping types of relationships between evidence items. The network science process was undertaken, resulting in raising a line of case-related questions regarding evidence relationships. The problem relating to relationships pertained to current and previous activities of an actor in the investigation, highlighting the different types of relationships that could exist between things, between people, and between

people and things bought new perspectives to the investigators. This process brought about an appreciation regarding evidence connectedness. The relationships between evidence can be mutual (that is, in both directions), asymmetrical (either inward to an evidence node or outward away from an evidence node), or null (signifying no relationship exists), leading investigators to realize another perspective regarding evidence interrelatedness. Another informal trial confirmed results of a previous evaluation (example one above), which illustrated the differences in approach between investigating officers.

Practitioner responses included

- The difference in approach results in significant differences in understanding the whole case.
- The building of relationships between evidence items and between people and evidence items was improved and holistic views of the case were now possible.

8.4 Evaluation Example Four

The identified problem was that law enforcement officers were unaware of technology capacities because lack of financial support had lead to lack of technology-related training. The solution related to a specific and challenging instance. Use of a resource library system (limited in nature as compared to the theoretical model) showed that suitably arranged repositories of forensic evidence information can assist officers in resolving operational challenges. The demonstration assisted case resolution by taking paper-based GPS records and converting them into a digital format for storage and analysis in a database before plotting the recorded GPS coordinates onto a map, showing when and where a particular vehicle and person had traveled. This data was then able to be digitally compared with other information regarding mobile motor vehicle registration numbers stored in a computerized system.

Practitioner responses include

- This enabled us to visualize and link items of evidence from disparate sources.
- This shows interrelationships between different items of evidence not previously considered important.

The progressive nature of the movement between the problem space, theorizing about the design, and consolidating the design and application in a restricted event environment offered by design science provided a flexible approach for the research not available through other research methods.

9 LIMITATIONS

A major restriction in providing practicable solutions to the defined forensic evidence problem space is that the three stakeholder groups are not governed by an overarching body, so there is no direct enticement to view evidence holistically. With

such a large space under consideration, it is difficult to employ and evaluate solutions in order to address the global problems identified.

Although design science provided a suitable mechanism for the research process, this method does not provide a formalized set of steps for conducting the work. New researchers applying design science may have difficulty estimating how far through the process they have progressed. In addition, design science has not yet addressed the handling of different perspectives, a necessity when dealing with domains involving complex human interactions.

10 CONCLUSION

The research at hand involved designing a model for the management of forensic evidence. Design science was used as the research method with mixed results. It allowed the researcher to get down and dirty at the operational level and readily move between theorizing and building. Although the iterative nature of design science provides the opportunity to immerse into the problem and solution spaces at the same time, at times it can be too flexible.

The models developed by the researcher in conjunction with the participants from the three stakeholder groups provide a holistic framework for effective management of forensic evidence. The implementation of such a high-level model across three domains is fraught with difficulty. Initial evaluation carried out by law enforcers provided positive feedback for specific models. Further research is needed for the detailed design of the component models and their implementation across the three domains. With regard to design science, research is also needed in complex human activity systems in order to provide guidance in the accommodation of different stakeholder perspectives.

References

Baskerville, R., Pries-Heje, J., and Venable, J. 2007. "Soft Design Science Research: Extending the Boundaries of Evaluation in Design Science Research, in *Proceedings of the 2nd International Conference on Design Science Research in Information Systems and Technology*, Pasadena, CA, May13-15.

Checkland, P., and Scholes, J. 1990. *Soft Systems Methodology in Action*, Chichester, UK: John Wiley & Sons.

Hevner, A. R., March, S.T , Park, J., and Ram, S. 2004. "Design Science in Information Systems Research," *MIS Quarterly* (28:1), pp. 75-105.

Jayaratna, N. 1999. *Understanding and Evaluating Methodologies*, London: McGraw-Hill.

Jonassen, D. H. 2000. "Toward a Design Theory of Problem Solving," *Educational Technology, Research and Development* (48:4), pp. 63-85.

March, S. T., and Smith, G. F. 1995. "Design Science and Natural Science Research on Information Technology," *Decision Support Systems* (15), pp. 251-266.

March, S., and Storey, V. 2008. "Design Science in the Information Systems Discipline: An Introduction to the Special Issue on Design Science Research," *MIS Quarterly* (32:4), pp. 725-730.

Venable, J. 2006. "The Role of Theory and Theorising in Design Science Research," in *Proceedings of DESRIST*, February 24-25, Claremont Graduate University, Claremont, CA

Walls, J. G., Widmeyer, G. W., and El Sawy, O. A. 1992. "Building an Information Systems Design Theory for Vigilant EIS," *Information Systems Research* (3:1), pp. 36-59.

About the Authors

Colin Armstrong lectures in security subjects in the School of Information Systems at Curtin University. He works closely with law enforcement, government, and industry in consulting, teaching, and research in cyber-security and digital forensics. Colin can be contacted at colin.armstrong@cbs.curtin.edu.au.

Helen Armstrong coordinates higher degrees by research in the School of Information Systems at Curtin University in Perth, Western Australia. Helen's areas of interest in teaching and research include cyber-security and network science. Helen can be contacted at h.armstrong@curtin.eu.au.