Including Stakeholder Perspectives in Digital Forensic Programs

Colin Armstrong
School of Information Systems
Curtin University of Technology
colin.armstrong@curtin.edu.au

Abstract

An investigation due to adverse outcomes in a computer incident encapsulates stakeholders acting in specific roles. These stakeholders will have a unique worldview, based upon their association with other actors or the items of evidence. The worldviews of each actor will lean either side of neutrality towards either the prosecution or defense perspective. This paper discusses the inclusion of stakeholder perspectives into a traditional university program for a digital forensic curriculum.

1. Introduction

Traditional digital forensic programs include such essential topics as: forensic procedures, understanding the different levels of data abstraction such as binary hexadecimal and GUI, disk geometry, file systems, operating systems and the applicability of Unix command line options, forensic acquisition techniques, and password cracking.

This paper discusses a university business school postgraduate computer forensic program where the focus extends beyond the immediacy of computer science to include an appreciation for stakeholder perspectives in order to prepare students to adopt a broader view of the environment in which adverse outcomes associated with computer related incidents occur. This program does not assume that all instances requiring the intervention of a digital forensic investigation relate to criminal activities and may be of a lesser civil or administrative disciplinary nature. There is however an assumption that a computer incident resulting in adverse outcomes has initiated an investigation requiring the application of traditional digital forensic techniques. The majority of students enrolling in this program are expected to seek employment careers in security related roles within the corporate business sector and not in law enforcement agencies.

This holistic approach to teaching digital forensics within a business school incorporates three distinct topic areas: technology, investigations, and the law. Stakeholder perspectives are drawn from these three topic focus areas. The purpose for including stakeholder perspectives is to promote an understanding of the perceptions of bias and prejudice that can infringe onto an investigation and its findings. Also, because different stakeholders may be interested in different aspects of an investigation, their perceptions can influence the nature of the investigation. Nance et al [1] argue that research in education for digital forensics is necessary in order to understand the diverse worldviews of constituent perspectives before further progressing with assistance to educators in developing educational and training methodologies, and materials.

Various stakeholders become involved during an investigation initiated due to adverse outcomes caused during a computer incident. Such an incident may or may not be related to criminal activity. The causes for computer incident related adverse outcomes are numerous, some intentional, others simply seem to happen.

Investigations of computer related adverse outcomes tend to differ from other types of investigation in that normally, the perpetrator and the victim are among the most prominent of these stakeholders. While in the virtual networked world of computer incidents where a perpetrator or a victim may be difficult to identify, they none the less exist. There may also be an extensive list of stakeholders. An incomplete list of stakeholders includes: family and friends of a perpetrator, family and friends of a victim, corporate businesses, witnesses, first responders, law enforcement officers, investigators, forensic and other experts, vendors of information technology tools, defense and prosecution lawyers, judges and jury members. The stakeholders associated with any serious adverse computer event, whether personal, corporate, civil, or criminal, or whether of a digital or physical nature, may have an influence on the investigation of that incident. They may also influence the determination of guilt or innocence and the determinations for subsequent consequences if an accused is found guilty. Each stakeholder sees their world through a perspective that is unique to them and
these worldviews are reflected in their involvement with the investigation and presentation of evidence.

This paper introduces the incorporation of stakeholder worldviews to traditional digital forensic curricula and discusses the different perceptions of those people associated with investigations of adverse computer incidents. An overview of the influencing attitudes perceived to be associated with the various stakeholder perspectives follows discussion that includes aspects of social network analysis inherent in a computer incident investigation.

2. Worldviews

A worldview is the structure and filter through which an individual or society interprets and interrelates with the world. Our knowledge, experience, intuition, beliefs, values and many other factors combine to form a view of the world that is unique. Descartes thought deeply about the influence of our preconceptions on the truth, believing our worldview is built from infancy (Descartes, 1637: translated by Cottingham, [2]).

“We’re bound to have many preconceived opinions that keep us from knowledge of the truth, because in our infancy, before we had the full use of our reason, we made all sorts of judgments about things presented to our senses.”

Immanuel Kant had a strong influence on the development of the concept of worldview as we understand it today, through his work on objective rationality. Kant combined the previously opposing rationalist and empiricist perspectives (where all knowledge is based upon reasoning versus perception and direct sensory experience respectively). Kant [3] states:

“But even though all our cognition starts with experience, that does not mean that all of it arises from experience. For it might well be that even our experiential cognition is composite, consisting of what we receive through impression and what our own cognitive power supplies from itself, sense impressions merely prompting it to do so.”

Kant believed that we all have the same fundamental cognitive framework through which we construct a subjective model of reality. Every individual’s worldview is based upon this subjective model. An individual processes an external event through a filter to arrive at a subjective reality through which he or she can understand this event. The subjective nature of an individual’s interpretation of reality has been the focus of much discussion in the area of psychology, but can be summarized succinctly by proposing that a subjective reality is a best approximation of an external event and is the only reality a person has [4].

The subjective reality has several names depending upon the discipline in which it is presented, including not only worldview, but also weltanschaung and mental construct. In his writing on the role of a problem solver Jayaratna [5], describes the world view of an individual as their “mental construct” which is comprised of the following nine elements: perceptual processes, values and ethics, motives and prejudices, reasoning ability, experiences, skills and knowledge, structuring processes, roles, and models and frameworks.

**Perceptual processes**: these act as a filter to determine what information is to be significant together with interpretation of that information by assembling it and making comparisons with materials previously stored. In effect it shapes whatever comes in from the world outside. Jayaratna also points out that one perception may not be seen as valid or consistent with the perceptions of another.

**Values and ethics**: values are beliefs we consider to be good without question, and are inherited from parents, peer groups and the media, and others are formed from life experiences and observations. Values help us to pass judgment on situations or to assess the actions, behaviour, output and performance of others. Ethics, Jayaratna explains, relates to the standards we place on a person’s expected behaviour and provides a minimum tolerance limit for expected behaviour. Both individuals and groups set, accept, and abide by sets of rule by which we agree to live. A truth for one individual or group may not be considered a truth by others. Perceptions of being wronged can be deeply personal. A perception of wrong can be a primary instigator for commencing an investigation, an investigation that may be of a criminal nature, or not.

**Motives and prejudices**: “Motives are those needs that we try to satisfy in a given situation but keep private to ourselves” [5]. Most people have personal motives which they try to satisfy either consciously or unconsciously. Prejudices are persistent opinions which are formed from values, experiences or needs. Jayaratna goes on to state most prejudices have a harmful effect as they prevent the search for valid information, and act as mental blockages.

**Reasoning ability**: is an individual’s capacity to extract the essential aspects from any situation and to understand the notions upon which our thought processes are based, in other words to examine what makes us reason in a particular way.

**Experiences**: allow us to develop knowledge and skills and help to “form implicit models for structuring our understanding of situations” [5], and these will
dictate the information looked for and actions taken in a specific situation.

Skills and knowledge: are proficiencies and background knowledge obtained from education, training and experience.

Structuring processes: relate to the way we analyze and synthesize and are unique to each individual, structuring the way we think and act.

Roles: are “explicit behavioural character sets attributed to someone responsible for performing a set of tasks” [5]. Humans are happy to adopt any role behaviour and value set as long as it helps to maximize an individual’s needs and motives. In many instances an individual’s particular set of ethical and moral values may conflict with the politics inherent in different roles.

Models and frameworks: originate from experience, conscious training and by discussion, debate and reflection, and assist in the development of an individual’s reasoning abilities.

Jayaratna [5] also suggests that “contrary to popular belief, the secret manipulation of other human beings is not a sign of our problem solving ability, but visible evidence of our sense of insecurity and our lack of confidence in our own ability to pursue desirable actions.” The above listed elements interact in a dynamic way to form the ‘mental construct’. Our mental construct helps us to not only make sense of situations and manage our relationships with others, but also to take action and to identify and solve problems. Humans tend to select given elements of a situation as being relevant and useful. “Some of this selection is implicit and unconscious (based on gut feelings, hunches, assumptions), but at other times the selection is prompted by explicit concepts, models and methodologies that are employed” [5].

Other authors present similar messages. For example, Naugle [6] explains worldview as an emphasis on the various ways in which human beings seek to depict reality. How rational is an individual’s subjective reality? The non rationality of the thought process underlying a worldview is highlighted by Cobern [7] who states:

“Worldview provides a non rational foundation for thought, emotion, and behavior. Worldview provides a person with presuppositions about what the world is really like and what constitutes valid and important knowledge about the world.”

So where does this leave us in the consideration of ultimate truth in the deliberations associated with a criminal event? While a simplistic view of evidence might be that it is anything that persuades one of a truth, the subjective worldview of stakeholders could be viewed as a praejudice and this bias or prejudice may influence the outcome of a hearing associated with any criminal event.

3. Stakeholder Groups

The nature of wrong doing and crime, while nefarious, is determined according to the laws, statutes, and policies of a community jurisdiction. The jurisdiction may reside within a corporate organisation at one level or a country at another level. A wrong doing or a crime in one jurisdiction may be acceptable conduct in another. Throughout this paper there is an assumption that any wrong doing may be escalated to being considered a crime and therefore warrant being treated as a crime from the commencement of digital forensic processing.

The investigation of an adverse outcome, or a more serious digital crime encompasses the following stakeholder groups:

- Victim group and associates of the victim
- Law enforcement
- Forensic scientists and experts
- Witnesses
- Perpetrator group and associates of the perpetrator
- The Judiciary
- Technology providers
- The Media
- The Public

The above stakeholder group perspectives vary in complexity with some being readily recognised as polarized towards either prosecution or defense. A third perspective, neutral, is also included in analysis of worldviews. The perspectives of each stakeholder listed may be described as follows:

Victim and Associates of the Victim

Human nature dictates that the victim of a crime can reasonably be expected to lean towards a prosecution perspective simply due to a desire to see justice done, for compensatory reasons, or revenge. While victims may be engaged by various other psychological postures this paper restricts considerations of perspectives to the prosecution, neutral finders of fact, and defense. There is also an assumption that family and friends being supportive of the victim will hold similar perspectives towards prosecution. It is important to remember that the victim may be difficult to identify. The victim may be an individual, a group, an organisation, or even a whole country. The victim may have been subjected to criminal activity, or to a lesser degree hold some perception of being wronged.
Law Enforcement

The law enforcement group may be considered from two views. Firstly, it is the role and responsibility of law enforcement personnel to investigate incidents and to determine the veracity of a claimed activity. During this phase of an investigation law enforcement personnel determine the basis for pursuing the matter dependent on the surmised guilt of the accused. Secondly, law enforcement personnel are required to discover sufficient evidence to pursue a prosecution. No other group of society is authorized to undertake this task. This role by definition places upon law enforcement personnel a perceived bias towards prosecution. Within law enforcement, but separate from law enforcement investigation personnel, prosecution officers examine the case materials and decide whether or not to pursue with a prosecution before a court of law and finders of fact.

Law enforcement offices in Australia, USA and Britain individually state that they see their role as seekers of evidence to support fact and as such are unbiased. They reject observations that their roles lead to the adoption of a bias towards prosecution. There is, therefore, a subtle difference of perspectives within the law enforcement group where their role has a bias towards prosecution yet their individual actions in carrying out their role claim to maintain no bias. The subtle difference of perspective within this group is not clearly seen by those outside of the group.

Forensic Scientists and Experts

Due to the specialist knowledge and experience gained through undertaking education and training the forensic scientist is perceived to have less bias towards either the prosecution or defense. Digital forensic investigation practitioners however are yet to be considered forensic scientists. While many practitioners possess academic qualifications, there are few that could justify the forensic scientist title. Many practitioners, because of their roots in military, corporate, or law enforcement are considered as persons with a level of expertise that likely retain a bias or prejudice aligned with their former role. The general perception is that scientists conduct their work in accord with the scientific method, producing repeatable experiments to ensure their scientific findings possess validity and reliability and thus be free of a prosecution or defense prejudice.

Occasionally this perception of forensic scientists is shaken when the media reports undesirable behaviour and outcomes when things go wrong. Oliver Mackson, a reporter with the USA Times-Herald Record newspaper published a report on 18th October 2008 to this effect [8]. In essence the expert testimony that helped convict Victor Valdes of murder did not withstand the rigor of an audit and the scientist Gary Veeder had committed suicide because of the shame resulting from his failure to meet the requirements of his job. Prosecution officials in New York State now face the task of re-examining every case involving Veeder expert testimony and determining whether retrials will be necessary.

There are situations where forensic scientists are called to interpret scientific finding on behalf of either the prosecution or the defense. This may present those that testify with a dilemma and beg the question, ‘Do they lean towards the bias that is paying for their services at court?’ It is the manner in which they present their interpretations of scientific finding that others may perceive a bias.

Because of his reputation during the early 20th century, the testimony of Sir Bernard Henry Spilsbury, a British pathologist was accepted without question. Spilsbury was considered at the time to be the most powerful forensics expert in the world and his influence extended into every judicial corner [9]. In the words of one contemporary: “He could achieve single-handed all the legal consequences of homicide – arrest, prosecution, conviction and final post-mortem – requiring only the brief assistance of the hangman” [9]. The mere fact that Spilsbury was to appear for the prosecution or the defense often determined the guilt of an accused. Spilsbury presented evidence for the prosecution in the infamous Hawley Harvey Crippen murder trial. As great a scientist as he was, Spilsbury was not, however, infallible. Recently forensic scientists, Trestrail and Foran, published their finding relating to this 1910 case stating that DNA evidence now calls into doubt the court’s determination of Crippen’s guilt [10].

These cases suggest that the perception of forensic scientist testimony may be either neutral, or possibly lean towards either of the adversarial opponents, prosecution or the defense. Fortunately it is the role of the finders of fact to determine outcomes of guilt.

Witnesses

The witness group may reflect any of the three perspectives, and may be intentionally or accidentally erroneous. Friends and family of both the victim and the perpetrator are commonly interviewed early in the investigative process as witnesses. Fortunately, because of the manner well conducted investigations follow, associates of the perpetrator will not necessarily be fully aware of investigation progress. This awareness also applies but to a lesser degree with associates of the victim. It is essential to interview witnesses as early as possible and away from the influences of people associated with the incident. Once witnesses become aware of the relationships within an incident their testimony could begin to exhibit a particular spin.
Witnesses may provide unbiased testimony or possess either a sense of loyalty due to friendship or another desire to influence outcomes. Examining witness testimony predominantly displays neutral perspective statements and a few that hold a bias towards either the prosecution or defense. These statements tend to either support or devalue the reasons surrounding incident occurrences.

It may be important therefore to understand who is providing testimony and their relationship with the victim or perpetrator in order to ascertain the presence of bias.

**Perpetrator and Associates of the Perpetrator**

The perpetrator of a crime could have any number of reasons for undertaking their actions. Their reasons may be based on; political and or religious motivations, revenge, financial gain or personal benefit, to list but a few. The reason for committing the inappropriate or illegal act may not be apparent. There will, in most instances, be an understandable desire to not be found out. This could be because the incident is not discovered or recognised, or because they have hidden or destroyed evidence. Few wish to be caught and punished. There is therefore a presumption that whatever they tell as their side of the story will possess a strong defense bias. When conducting illegal activities most perpetrators focus on the primary objective of achieving their desired task. Secondary considerations after the event may be towards self-preservation by dispersing or destroying evidence and distancing themselves from the incident. Certainly a perpetrator must possess three essential characteristics; opportunity, capacity, and motive. Naturally, the perception held by a perpetrator has a strong focus on defense as would associates, family and friends.

Perpetrators of digital crime may possess an element of heroism because of their motivations, and physical separation from the victim and the crime scene environment. Perpetrators may justify their actions because of their perception that there is no loss to the victim, the victim is faceless and therefore a lessened sense of victim suffering than a crime involving direct physical trauma to a victim. Because of their isolation from the crime scene and the victim a perpetrator may believe that have not hurt anyone.

Often the friends and family of a perpetrator have little or no idea about the crime and disbelief leads to a lack of understanding of the repercussions and impacts of committing actions in the virtual world because the effects on the victim are not obvious. There is a natural tendency by friends and family of a perpetrator to support the perpetrator and to hold a biased perspective of events towards defense.

**Judiciary**

The judiciary group may be viewed as possessing three perspectives; prosecution and defense plus the neutral finders of fact being a judge, a tribunal of judges or magistrates, or the members of the jury. As it is the prosecutor’s duty on behalf of the State and public to gain a conviction over the accused, a natural bias towards achieving that goal is expected. It is the role of their opponent to defend the issues of fact before the court contesting interpretations of prosecution evidence seeking loopholes in the evidentiary processes to gain an acquittal for their client. It is not normally the role of the defense to prove innocence. The burden of proof resides with the accuser. As the prosecution’s opponent there is a natural bias away from a prosecution perspective.

The neutral perspective resides with the finders of fact. In the situation where a judge alone or a tribunal of judges fulfils this role there is a requirement to undertake two responsibilities. Firstly, that responsibility is to ensure legal requirements of evidence before the court comply with accepted rules. Secondly there is responsibility to determine believability of presented argument based on evidence available to the court before deciding whether the appropriate burden of proof is achieved.

Although dependent on the jurisdiction and legal system, a tribunal setting provides an opening for different determinations of believability between sitting judges and in those instances majority rules. Where the matter in dispute is heard before a jury the role changes slightly in that the judge solely ensures compliance of legal requirements and the jury determines the believability of evidence. Upon deciding whether the burden of proof is achieved the jury pass their finding to the judge and the matter of punishment resides with the judge.

It could therefore be assumed that the perception of the judiciary group may fall towards either the prosecution, defense, or remain neutral. It should be noted that the mere fact that a decision of guilt is made does not indicate a bias and that in the ideal world those called to hold office in determining guilt rise above natural inclinations of guilt or innocence based on anything but the ‘unbiased facts of the matter’.

**Technology Providers**

Digital evidence tends to have a strong reliance on specialised knowledge and skill in the application of processes and tools. Matters in dispute relating to information technology are not dissimilar to other forensic disciplines in the use of specialised processes and tools to facilitate discovery of facts. A significant difference between digital forensic evidence and other forensic evidence is that the physical machinery pertaining to digital evidence may be captured and
readily replicated in a manner where copies of the evidence are identical to the original evidence. The tools used to capture and analyse digital evidence tend to be provided by corporate organisations. Also, the applications that permit the operation of computing systems to perform various functions tend to be proprietary in nature. The proprietary nature of digital world applications tends to cause problems because the inner machinations of these applications are shrouded in secrecy. Unless the application in question is open source where many experts can validate how the application truly functions it may be necessary to rely on vendors to provide validation that the application actually does exactly as it is claimed. In these situations there is likely to be a bias regarding the application that is not related directly to the outcome of the case at question and therefore considered neither for the prosecution nor the defense.

Whereas early in the history of digital forensic evidence tools there was a tendency for digital forensic practitioners to validate the tools they used, with the advent of more complex ‘black box’ tools we now see a reliance placed on vendors to provide that validation and vendors now regularly appear before a court to verify that the tool does not produce any adverse changes to the evidence. While there is an expectation that a competent practitioners will ensure the tool chosen for a task performs as the vendor claims, it is not practical for the practitioner to fully validate the ‘black box’ tool. Information technology vendors therefore are expected to be bias towards the benefits of their particular tool but tend not be perceived as being bias towards the outcomes of the case before a finder of fact.

The Media

The media through television, radio, and newspaper reporting have the potential to influence community attitudes and ultimately shape the modifications of community rules and laws. In some situations the media picks up on community attitudes and pushes stories to accentuate societal change leading politicians to enact legislation. The media is a powerful influence within society and the manner in which it pursues a story can present an accused to be guilty in the eyes of the public before due process of the courts, particularly when jurisdictional boundaries hinder State legal processes. On the other hand the media may chose to not run with a story and thereby severely limit public awareness of selected situations.

The media can affect public attitudes to the extent that a hostile and enraged community results, having an impact on the behaviour and decisions of otherwise neutral actors. This may present difficulties with jury selection and is one reason why the ‘Law’ sometimes appears to function very slowly. In today’s society this is particularly relevant to investigations of paedophilia. Many personnel involved in the investigative and judicial process have young children or grandchildren. Each will have their own personal beliefs and opinions relating to the care of children. The nature of their work may demand a close association with people and evidence relating to distasteful and emotionally disturbing illegal activities. They may also have friends and family that have been subjected to the traumas of incidences similar to those being worked on.

The Public

Among the public at large many will not be aware of, or be interested in, particular criminal activities or specific events. There are, however, sub groups that may have an interest and that might influence an outcome. The courts exist to satisfy the demands for justice by ‘the people’. The laws that form the foundations upon which a justice system is built exist because ‘the people’ have caused the rules by which society agrees to live to be formalized into those laws. At this point there is possibly a leaning towards either a defense or prosecution perspective but predominantly a neutral perspective would be expected. An example of the influence of the public on the formation of laws is the recent move to change smoking in the workplace from a norm to becoming socially unacceptable to then becoming an illegal activity.

Of more importance are those smaller sub-groups comprised of associates of the victim and the accused perpetrator. Each may influence the initial investigation process by either encouraging or disrupting law enforcement procedures. Helpful friends and family of a victim can assist police by making it easy for them to do their job. Similarly friends and family of an accused may be uncooperative, disruptive, even to the point of hiding and destroying evidence and telling their side of the story with a defensive slant.

Communities endeavour to create rules and laws to protect themselves from such harsh incidents. The US State of Nebraska, for example as of 1st July 2008, has implemented unique safe haven laws to protect children. In Nebraska it is now legally possible for distressed care providers of children, not always a parent, to abandon children at State Health Care Centers. As a result disgruntled parents are travelling to Nebraska to abandon their children. How much of this is attributable to the power of the media is undetermined. There is clearly the need to recognise the media’s ability to influence perspectives of investigatory processes and outcomes.

3.1. Misaligned Incentives

It is apparent when considering the perspectives of these various stakeholders that evidence and the
understanding of how evidence might explain what and how something occurred is subjected to differing levels of bias and prejudice.

The postgraduate computer forensic program taught in this university business school encourages students to adopt a holistic approach to understanding digital evidence and to recognise the benefits of considering the misaligned incentives of stakeholders. All too often students tend to adopt the view that there can only be one answer to what the digital evidence means. Such an immature attitude subjects the integrity of the investigator to adverse personal and professional risk on the one hand, and on the other an inability to correctly explain the incident in question.

4. Stakeholder Perspectives in Digital Evidence Forensics

In line with technological progress, law enforcement and the judiciary are increasingly faced with digital evidence in relation to cases of both digital crime as well as other physical crimes. Digital evidence is often sought to strengthen a case involving physical crimes, particularly in cases of homicide, child sex offences and financial fraud.

Any incident of crime happens within a domain, not necessarily at a single location. While in general physical crimes occur in a geographic location and are readily accommodated within a legal jurisdiction, cyber crime often has no single jurisdictional boundary. This presents some stakeholders with difficulties while protecting others. Jurisdictional issues relating to the nature of offences, the accepted elements of an offence, and who has authority to conduct various tasks can hinder investigations proceeding to a court. In the corporate world there is often a reluctance to acknowledge an incident has occurred, and these attitudes tend to protect the perpetrator.

Evidence may be considered in two parts: in the first exhibits are collected and ultimately may be presented to a court, and secondly there is testimony. Testimony is gathered from witnesses who may be directly associated with the incident or alternately have an indirect association, such as expert testimony provided by investigators and forensic scientists. All expert testimony is opinion-based, and no exhibit is presented to a court without accompanying testimony. Other evidence and exhibits result from further analysis of collected evidence examined beyond the boundaries of the incident.

Considering the various stakeholders as actor nodes of a social network facilitates visualising the context of those people associated with an investigation. This technique provides insights as to the interrelationships between stakeholders within the incident environment.

Rarely does the Judiciary Group venture into the incident environment. One would expect both the victim and the perpetrator to be strongly represented at the core of the incident as would most witnesses. Law enforcement and forensic scientist practitioners may be found working throughout the whole environment. And, the media, public and both associates of victim and perpetrator reside in the outside world environment.

At the core of understanding the views expressed by actors, which is dependent on their respective perspectives, is realising the range of philosophies for truths and defining how truth is associated with the concept of evidence. The philosophy of truth is a complex matter and entering a discussion on this topic is beyond the scope of this paper. However, a range of levels of believability will aid the comprehension and measurement of believability within situation in dispute. Founded on the principles of logic, a test of the truth as stated in testimonial evidence may be applied. There is a need to distinguish factual truths from comments of belief truths and there are accepted criteria of truths established by philosophers that we may adopt. Sahakian and Sahakian, [11] discuss the rules by which the accuracy of statements and opinions may be judged, thus providing the criteria for standards of verification.

Levels of believability are presented by Sahakian and Sahakian [11] ranging from approximately 0% to approximately 100%. These authors recognise seventeen levels ranging from the most to least believable as being; Coherence, Rigorous Consistency, Loose (or Mere) Consistency, Pragmatic Truth, Authority (ipse dixit), Correspondence, Naive Realism, Consensus Gentium, Majority Rule, Revelation, Intuition, Hunch, Instinct, Feelings (Emotions), Time, Tradition, and Custom. These seventeen levels of truth...
have been used as a basis to map the relative approximate percentages to the burden of truth as shown in Figure 1.

The rationale of persons carrying out activities the public understands to be undesirable is varied. Many activities conducted in the digital world may be seen by the public as being of little consequence because the digital world is a virtual world where there is little, if any, perceived impact on the physical world. The acquisition of entertainment data in the form of digital reproductions of music sound and movie vision without depriving the owner of the actual material downloaded may be considered a personal gain without robbing the owner. Similarly the manipulation of data in the form of numbers may not be considered financial theft or fraud because it is only data and not physical cash.

Likewise it may be difficult for the public to appreciate or understand the significance of digital data being transferred from one virtual location to another. These activities relate to such crimes as identity theft, intellectual property theft, or industrial espionage. There is a belief held by some that it is not possible to steal a thought because it is not physical and that rationale seems to be readily applied by some to objects in the digital world. There is, of course, a basic flaw to this form of logic. Underlying all of these is the rationale of personal gain which may be achieved through a conduit of political, religious, corporate, or organised crime justifications.

Perpetrators of digital crime may possess an element of heroism because of their physical separation from the victim and the crime scene environment. Perpetrators may justify their actions because of their perception that there is no loss to the victim. The victim is faceless and there is a lessened sense of victim suffering in comparison to committing a crime involving physical trauma to a victim. Because of their isolation from the crime scene and victim a perpetrator of digital crime may believe they have not hurt anyone. Often the friends and family of such a perpetrator have little or no understanding of the crime and disbelief leads to a lack of comprehension of the repercussions and impacts of committing actions in the virtual world because the effects on the victim are not obvious.

In order to analyse the relationships and possible biases within a digital crime evidence in a network, the evidence is categorized in two ways; the method of generation, and purpose. The three basic types of digital evidence generations are:

1. Computer generated records, where the output of computer programs are created without human intervention such as in the form of log files, telephone records, and automated teller machine receipts;

2. Computer stored records, where documentary files contain human input or writings in the form of word processed files, e-mail, and internet chat messages; and

3. Combined computer records where both computer-generated and computer-stored records are differentiated depending on whether a person or a computer created the records’ substantive contents as in the form of financial spreadsheet where part is human and part machine input is resultant from mathematical calculations.

The two focuses on digital evidence purpose may be described as:

1. Computer focused crime, where illegal acts are committed within the virtual world using computer systems. Examples of computer focused crime are hacking, cyber stalking, and cyber identity theft;

2. Computer assisted crime, where illegal acts are committed without the need for computer systems for the committing of the criminal act but where computers may be used to record or manage illegal acts. Examples of computer assisted crimes include fraud, prostitution, homicide, and drug related crimes.

To assist this analysis it is helpful to model and visualise the relationships between actors and evidence items, to indicate an inherent bias, however this is a complex operation. In this paper the relationships are reduced to simple generalisations in order to provide an overview of the interplays between the various nodes of the perspectives in a digital evidence network.

Figure 2 represents an example of a Network of Actors and Offence displaying three levels of relationship. This network has both actors and offences represented by nodes, with links between them showing a three level rating of their relationships. The rating apportioned to a link has been based on actual data collected by the authors from three sources: direct interviews with law enforcement, judiciary and forensic scientists, analysis of documentation, and discussions with colleagues relating to evidence attitudes and understanding during doctoral research. The three-level rating illustrates the level of importance placed on the crime and associated evidence which vary according to personal experiences, understanding of the offences and more significantly on the perspective of the offence taken by the particular actor.
The three levels of crime and evidence relationships shown represent High, Low, and Medium appreciation of the consequences and seriousness of the crime. The shadings used in Figure 2 are broad light grey to show a low appreciation or understanding, dark grey to shown medium understanding, and narrow black shading to show strong understanding. For example, there are three different levels of links attached to The Media node:

1. Four narrow black shaded links to Copyright, Identity Theft, Hacking, and Industrial Espionage: indicating a strong appreciation of the crime’s seriousness and consequences.
2. A single medium dark grey link to Intellectual Property: indicating a lesser but medium appreciation, and
3. A single broad light grey link to Industrial Espionage: indicating a poor appreciation of the crime’s seriousness and consequences.

It becomes apparent that even at this simple level of modelling there is a wide divergence of attitudes between actors of these basic criminal activities. The perspective of actors is swayed by not only their appreciation of the activity and associated evidence but also by their personal associations within the community and their leanings towards prosecution, defense, or neutrality through lack of interest in the activity.

Figure 3 displays the expected natural human bias to an adversarial dispute. This simple diagram displays a total of thirteen nodes, ten representing ‘actors’ and three nodes representing the choices; prosecution, defense, and neutrality. These three choices can readily be seen as the main centres of the network with links to nodes representing each of the ‘actors’: the Prosecution (links shown by light connecting lines), the Defense (shown by dark connecting lines), and Neutral (shown by medium shaded connecting lines). It becomes obvious that there is a natural bias in this network towards prosecution because the prosecution node possesses more links than either of the nodes representing defense or neutral. In network terms, the prosecution and defense nodes are ‘hubs’ due to the greater number of links. Hubs tend to carry more significance than do other nodes.

Analysis of the sample data forming the basis of figures 2 and 3 indicates that different perspectives are differentiable and automated tools can assist in providing a more comprehensive picture of the subjective realities of different actors in a crime scene environment. However, further research needs to be conducted in measuring the actual influence of such bias on the final decisions made by the finders of fact.

5. Conclusion

In many Societies, there resides a belief demanding the wrong-doer be punished. Fear of punishment is an important element of a society’s worldview for managing societal behaviours to reduce wrong doing. The role of law enforcement is to enforce the law and maintain the peace. On behalf of the people and the State, law enforcement investigates wrong-doing and prepares arguments explaining the wrong-doers’ activities. It is the State’s role to conduct these processes within the State’s legal system. Communities construct the rules by which they agree to live, progressing to become States that assume such responsibilities. Instruments of the State include law enforcement and the judiciary. Law enforcement, in addition to maintaining the peace and enforcing the community rules (State laws), have the added responsibility of obtaining the evidence of breaches to those rules and preparing the prosecution perspective’s argument. The processes conducted by the State on society’s behalf should be devoid of emotion and political interference. Beyond the State, one encounters the emotive and personal perspectives of stakeholders.

The family and friends of the victim are often well aware of the victim’s suffering. Apart from providing care towards the victim many are prompted to promote actions to rectify the matter or simply to seek revenge.

The family and friends of the perpetrator may believe that the perpetrator did not actually harm a
victim, or that the actions were justifiable. Often associates of the perpetrator have a distorted perspective about the crime such as disbelief due to lack of understanding the impact of digital actions because effects are not obvious. There may be attitudes towards heroism in digital crime or disbelief of victim impacts because the victim is faceless and perceptions of suffering are not the same as with a physical trauma.

The responsibility for exacting appropriate responses to criminal activities eventually falls at the feet of the finder of fact and the viewpoint of the judge must focus on the greater good of the community. Law may be considered a ‘fashion’ determined by the interactions of the community and reflects the desires of people. The peoples’ desires for justice lead to the formulation and changes of laws. Judges are conservative by nature and the quickly changing scene of the computing and communications environment leaves the lawmakers behind. Lawmakers attempting to pre-empt advancing technologies sometimes produce unusual results. In Australia the Cyber Crime Act of 1999 enacted in New South Wales contained a clause that made it illegal for anyone working in the cyber world “to attempt the impossible”. This was modified in the subsequent federal Australian Cyber Crime Act of 2001 and illustrates the general lack of understanding of digital crime and evidence.

Digital crime evidence is a challenging concept that is little understood by many of today’s community and yet that does not prevent actors from possessing strong attitudes. Further research using network science techniques could lead to the establishment of a method for determining how best to attribute a measure of believability to testimony. Being able to better assess the believability of testimonial statements using mathematically sound processes could reduce poor decision making based on erroneous analysis results. That the majority of testimony might appear to support a particular hypothesis does not necessarily make those statements factually true. If a measure may be applied to testimonial statements permitting the bias to be calculated then it will be possible to better understand the incident using a holistic perspective.

In summary, the corporate world uses information technology extensively. Corporations are subjected to adverse computer related incidents. It is considered important that doers of wrong be made accountable. Digital evidence provides the means for understanding how these wrongs occur. Without the inclusion of an understanding for how different stakeholders holding different perspectives can influence an understanding of digital evidence, there is a risk students entering corporate careers will be unaware of not only the expected behaviour of stakeholders based on their various perspectives, but will also be unaware of how their own perspective may be perceived by others to hold a bias or be prejudice.

7. References