# A CASE STUDY OF THE CHALLENGES OF CYBER FORENSICS ANALYSIS OF DIGITAL EVIDENCE IN A CHILD PORNOGRAPHY TRIAL.

**Richard Boddington**
School of IT
Murdoch University
Perth, WA 6150
Australia.
r.boddington@murdoch.edu.au
Tel: +61 893602801. Fax: +61 89360 2941.

## ABSTRACT

Perfunctory case analysis, lack of evidence validation, and an inability or unwillingness to present understandable analysis reports adversely affect the outcome course of legal trials reliant on digital evidence. These issues have serious consequences for defendants facing heavy penalties or imprisonment yet expect their defence counsel to have clear understanding of the evidence. Poorly reasoned, validated and presented digital evidence can result in conviction of the innocent as well as acquittal of the guilty. A possession of child pornography Case Study highlights the issues that appear to plague case analysis and presentation of digital evidence relied on in these odious crimes; crimes increasingly consuming the time, resources and expertise of law enforcement and the legal fraternity. The necessity to raise the standard and formalise examinations of digital evidence used in child pornography seems timely. The case study shows how structured analysis and presentation processes can enhance examinations. The case study emphasises the urgency to integrate vigorous validation processes into cyber forensics examinations to meet acceptable standard of cyber forensics examinations. The processes proposed in this Case Study enhance clarity in case management and ensure digital evidence is correctly analysed, contextualised and validated. This will benefit the examiner preparing the case evidence and help legal teams better understand the technical complexities involved.

**Keywords:** Digital evidence, evidence analysis, evidence validation, presentation of evidence, digital evidence standards.

## 1. INTRODUCTION

Because the legal fraternity generally understands little about computer science, the potential for miscarriages of justice are great. The cyber forensics community sometimes exploits this situation and obfuscates the environment by focusing on issues such as preserving, collecting, and presenting digital evidence with evidence validation under-stated or ignored (Caloyannides, 2003). Ultimately, juries must evaluate the evidence and if they misread or misunderstand it because of inadequate forensics analysis and presentation, and faulty validation processes, unreliable decision as to the guilt of those accused are inevitable. The disappearance of baby Azaria Chamberlain at Ayres Rock more than thirty years ago and subsequent coronial inquests, a court case featuring controversial forensics evidence, and the subsequent Royal Commission into her sad death, resulted in a fundamental reconsideration of forensic practices in Australia (Carrick, 2010). Digital evidence may on occasions, also be failing to meet the same high standards expected of more established forensics regimes.

Criminal trials relying on digital evidence are increasingly common and regrettably, trials where innocents are convicted are not rare (George, 2004; Lemos, 2008). Defendants are pleading guilty based on what appears to be overwhelming hearsay evidence, mainly digital evidence without robust defence rebuttal. Reasons for this may be the evidence is compelling, the defendant may have limited

financial resources, the defence lawyers misread the evidence, plea-bargaining offers lesser sentences, etc. Various factors can affect the validity of the evidence, including failure of the prosecution or a plaintiff to report exculpatory data, evidence taken out of context and misinterpreted, failure to identify relevant evidence, system and application processing errors, and so forth (Cohen, 2006; Palmer, 2002).

Since 2008, the author has provided expert analysis of digital evidence to defence criminal lawyers in Western Australian. This involved re-examination and validation of digital evidence presented in state and federal law enforcement cases. A number of defendants were able to convince the jury of their innocence, partly with the assistance of the author's re-examination and testing of the digital evidence. The selected Case Study, a possession of child pornography, highlights the incomplete and incorrect analysis common in cyber forensics analysis of child pornography cases in Western Australia.

According to the Australian Federal Police, possession of and trafficking in child pornography cases are more frequent in Australia with a 30% increase arrests for child pornography offences in 2011 compared with 2010 (Sydney Morning Post, 2012). Child pornography cases are technically complex and require analysis of evidence that supports claims of criminal intent including knowledge and control of offensive materials. Locating evidence that proves more than simple possession of the materials requires skill and expertise in presenting evidence to prove deliberate actions by suspects. Linking the user to the crime may happen too quickly on some occasions without sound validation of the evidence.

Officers who undertake these important but tedious tasks may well be under-resourced, over-burdened with complex cases, sometimes made more difficult by inexperienced analysts and communicators. There is some anecdotal evidence suggesting that these prosecutions are in response to political lobbies determined to eradicate any form of immoral cyber behaviour through draconian, result-oriented legislation. The inherent problem with such an approach is too much pressure on examiners who put at risk the innocent inadvertently caught up in criminal investigations. These problems are not unique to Western Australia and the Case Study is not intended to criticise law enforcement agencies. What it attempts is to identify some common problems affecting their forensics examinations and suggests enhancements to improve outcomes. What is evident to the author, and his fellow workers in the field, are two related problems, 1) faulty case management through inadequate analysis and presentations of the digital evidence, and 2) incomplete and incorrect validation of the digital evidence. The Case Study highlights typical problems, identifies best standards, and offers processes to achieve outcomes that are more acceptable and helpful to the examiners and legal practitioners.

## 2. INTRODUCTION TO THE CASE

The case selected is the State of Western Australia versus Buchanan (2009) on a charge of possession of child pornography, an indictable offence usually resulting in imprisonment on conviction in the jurisdiction. The defendant's computer was seized and he was charged with possession of offensive photographs and movies contrary to the Western Australian Criminal Code Section 321. The offence of possession is contingent on the images being of an offensive nature of a person under sixteen years, purporting to be, or depicting a person under the statutory age. Mere possession is not sufficient to convict under the legislation and some degree of knowledge, control of the offensive material, and criminal intent has to be proven by the prosecution. Nevertheless, in reality, it is a reversal of the presumption of innocence and possession carries more weight than perhaps it should. On occasion, disproportionate onus is placed on a defendant to explain away incriminating digital evidence that is sometimes indiscriminate in signifying blame. It is easy to overlook the gap between possession and possession with criminal intent. Ownership or possession of a computer is tantamount to criminal guilt in some mindsets, yet it ignores the requirement to link a specific computer user with the evidence.

A number of computers were seized and examined and a perfunctory analysis report was produced describing the digital evidence clearly of an offensive nature located on one of the computers. The

defence team was instructed by the defendant to analyse the digital evidence and seek a better understanding of the nature of the prosecution's evidence and to develop a possible defence strategy.

During the re-examination of the forensic image, exculpatory digital evidence exhibits were identified and tendered at the trial. This new evidence and demonstrations of the unreliability of some existing evidence, challenged some key prosecution assertions and contributed to the defendant's swift acquittal by the jury.

## 3. PROBLEMS OF ANALYSIS AND PRESENTATION

Forensics examiners overlooking or mis-reading evidence, and worse still, resorting to 'cherry-picking' when choosing or omitting evidence to gain legal advantage, is a common phenomenon of the digital domain (Berk, 1983: Flushe, 2001; Koehler & Thompson, 2006). Moreover, bias, examiner inexperience and pressures to process cases with limited time resources can also explain the phenomenon. The reasoning used in the analysis may be faulty, lacking any safeguards to ensure complete and thorough analysis occurs. If abductive reasoning was used in the case presented for study, and it probably was as it is commonly used in such circumstances, then it seems to have been done poorly.

Abductive reasoning is inferential reasoning based on a set of accepted facts from which infers the most likely explanation for them and is most commonly used in legal proceedings (Australian Law Dictionary, 2012). In contrast, deductive reasoning abstracts directly from data while inductive reasoning is based on but extrapolates partially beyond data. Abductive reasoning extrapolates inductive reasoning even further (Walton, 2004, p. 13). Abductive reasoning is used to develop plausible hypotheses and evaluate candidate hypotheses to seek the best explanation based on a preponderance of supporting facts (Walton, 2004, pp. 22, 174). Walton (2004, pp. 1, 4, 20 and 33) asserts that logic is expected to be exact whereas abduction is inexact, uncertain, tentative, fallible, conjectural, variable and presumptive, labelling it as, *". . . the judgment of likelihood"*. Abductive reasoning draws its conclusions from incomplete evidence; a guess but an, *". . . intelligent guess. . ."* according to Walton (2004. pp. 3, 215).

Abductive reasoning involves a series of questions and answers and eliciting and ultimately evaluating competing explanations that emerge from the process (Walton, 2003, p. 32). Such legal debate and opinion of the hypotheses are passed to the jury for their consideration but of concern is the likelihood that incorrect and incomplete reasoning, abductive or otherwise, of technically complex digital evidence, hardly serves the course of justice. Certainly, no questioning or answering process was shared with the defence team involved in the Case Study, and guesswork seemed banal not intelligent.

Cases relying on digital evidence are often complex and involve various groups of related and unrelated evidence that make up the various threads of evidence that form part of the rope of evidence. The problem confronting the examiner is locating and selecting the evidence which requires careful, unbiased reasoning. Each thread complements the whole but often important threads are subject to misinterpretation or are overlooked. Pulling the threads a together then requires validation to check and test the evidence. That accomplished, the evidence must be presented in an easily understood form which defines the evidence, explains its relevance and evidentiary strength, and includes potential rebuttal based on validation and other issues that may challenge the claim.

## 4. ANALYSIS AND PRESENTATION ISSUES IN THE CASE STUDY

Subjective assumptions, evidently based on a perfunctory understanding of the evidence, with no attempt to ensure its completeness and correctness in the Case Study were also common to other child pornography case examined by the author, even though the innocence of those defendants was less clear than in the Case Study.

The prosecution analyst's original analysis report provided no narrative on the groups of catalogued evidence or the relationship between them or their combined contribution to the criminal charge. The

report lacked complete contextualisation to help the legal teams and defendant understand the significance of the evidence. No timeline, no storyboard, and no detailed explanation of the significance of the exhibits were provided. The prosecution analyst's lack of reliable case analysis, an absence of evidence validation, and confusing analysis presentation was problematic for the defence lawyers. The prosecution lawyer seemed to misunderstand the digital evidence based on weak cross-examination of the defence expert.

Expedient use of the evidence selected by the prosecution analyst, combined with questionable inferences about the probity of the evidence, suggested a disregard about the defendants' presumed innocence in the selected case. The charge of possession with intent, hinged on the defendant's ownership and exclusive access to the computer. No explicit evidence was offered to support the truth of the contention nor was any attempt made to show others had access of the computer. Offensive pictures and video files and access to child pornography websites was offered as *prima facie* evidence of guilt, presumably based on abductive reasoning. Whatever reasoning was used to determine the merit of the cases from a prosecution perspective, it appeared cursory and little thought given to the possibility of any alternative hypotheses. The power of the 'smoking gun' alone was enough to lay charges.

Exculpatory digital evidence recovered from extant and carved files, earlier identified but disregarded by the prosecution analyst's seemingly Procrustean disposition as "being irrelevant", suggested that the defendant was not the only suspect, nor the most obvious one. This evidence was not catalogued, nor was it voluntarily shared with the defence team, yet its existence was acknowledged prior to the trial and during cross-examination of the prosecution analyst. It is common for the re-examination of the evidence in these cases, to identify extra incriminating evidence as well providing helpful analysis presentation that sometime benefits the prosecution at monetary cost to the defendant and disadvantage to the defence strategy. It seems unjust that defence analysts are required to complete and improve the case evidence because of the shoddy work of the prosecution. In this case vital exculpatory evidence was recovered and inculpatory evidence was challenged.

Although unlikely to face the same charge as the defendant, or for perjuring themselves during their testimony, others were the likely culprits. Other witness testimony further implicated one or more of these persons who were tenants in the defendant's home at the time of the offence. Why the defendant was charged and not others, when available evidence contradicted the evidence of two of the prosecution witnesses, remains puzzling to the author. This was an exceptional case and even the prosecutor intimated its likely collapse but the judge directed the proceedings continue and allow the jury the final decision.

In this and other cases, the problem seems that the forensics examiners provide statements of evidence selection but no explanation why exhibits were selected in terms of their relevance and significance to the cases. Nonetheless, examiners should possess the experience and expertise to state the relevance of the evidence and its relationship to other evidence in the case. It seems this task is for the legal teams to elicit through various means; hardly efficacious case management. This raises problems of evidence reliability; notably its accuracy, authenticity, corroboration, consistency, relevance, etc. From this morass, some formal process is required to convey the gist of the examiner's analysis and conclusions.

## 5. POTENTIAL SOLUTIONS TO ANALYSIS AND PRESENTATION ISSUES IN THE CASE STUDY

Inman and Rudin (2001) state, "*Before the criminalist ever picks up a magnifying glass, pipette or chemical reagent, he must have an idea of where he is headed; he must define a question that science can answer*", neatly defining a basic cyber forensics case management problem. According to Pollitt (2008), this places the forensics examiner in a quandary who must have a sound understanding of defining investigative or legal questions and be able to convert them into scientific questions. Pollitt (2008) stresses the importance of first defining the legal and investigative questions before defining

the digital forensic (scientific) questions. If that advice were heeded in the Case Study, the prosecution analyst would have benefited from more direction from the outset of the examination and probably be more inclined to use more reliable logic in assembling the case. Assuming sound scientific logic is applied during analysis, presenting the evidence requires some dedicated thought. Yet there are various simple, effective processes such as Toulmin's model, discussed below that can help organise analysis and presentation of digital evidence.

Toulmin's model based on his theory of *The Layout of Argumentation* (1958) has been used to construct arguments at various stages of litigation and works for legal argument because of its accuracy, flexibility, and effectiveness, according to Saunders (1994, p. 169). Toulmin (1958, p. 7) was concerned that sound claims should be based on solid grounds and backed with firmness to support claims used in arguments. The model accommodates lawyers' reliance on precedential and statutory authority and incorporates the elements inference and uncertainty in judicial reasoning and decision-making (Saunders, 1994, p. 169). Most importantly it includes in the argument the element of rebuttal; anticipating refutation of counter arguments by lawyers. The same process is just as relevant to the forensics examiner.

Toulmin (1958) asserted that formal rules of logic were incompatible with common practices of argument as a means of critiquing and analysing public argument and has been used by lawyers to understand the constraints in legal cases when defining reasonableness standards. Toulmin's theory (1958) defines six aspects of argument common to any type of argument as described below and illustrated in Figure 1:

**Data (Object)** is the evidence, facts, data and information for the claim. It establishes the basis of the argument. Data can be grounded in anecdotal evidence and a specific instance can provide the basis for the argument. Data can be human testimony or grounded in statistical data.

**Warrant** is the component of the argument that establishes the logical connection or reasoning process between the Data and the Claim:

- *Authoritative warrants* rely on expert testimony offering conclusions about the Data to support the Claim.
- *Motivational Warrants* rely on appeals to the audience offering conviction, virtues and values to support the claim.
- *Substantive warrants* more closely resemble traditional forms of logical reasoning, including Cause-Effect/Effect-Cause, and generalisation based on example and classification.

**Claim** is the point of an argument and represents the conclusion advocated by the arguer based on the Data linked to the Warrant.

**Backing** is the material that supports the Warrant and explains the reasoning used in the Warrant. Backing adds credibility to an argument; without it the arguments seems lacking:

- *Statistical Backing* relies on numbers to quantify information but can create an allusion of truth.
- *Example Backing* are concrete instances that illustrate the Warrant and provide a real world view but caution is required when using generalised examples that may not be true in a given argument.
- *Testimony Backing* is based on expert opinion and personal experience which adds credibility to the argument.

**Qualifier** represents the soundness, the strength and worthiness of an argument.

**Reservation (Rebuttal)** is an exception to the claim made by the arguer as arguments may not be universally true.

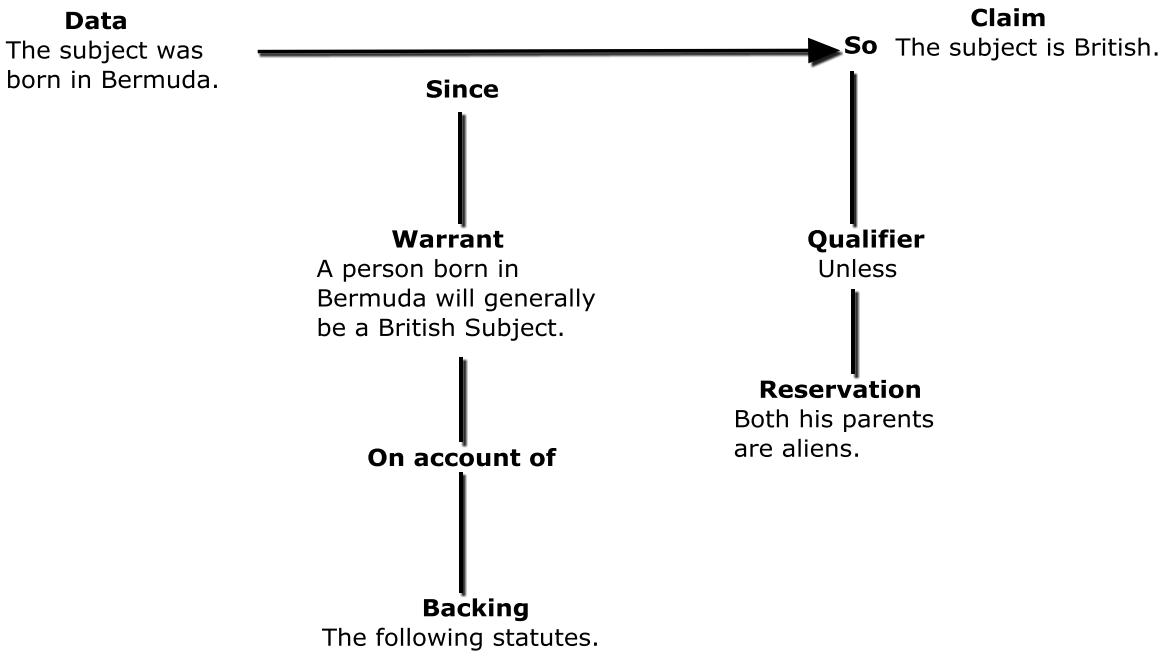


Figure 1. Toulmin's Model of Argumentation (Toulmin, 1958, p. 105)

The flexibility of Toulmin's model is that it can be used to take a top down view of the case based on validation of the combined evidence as well as individual and clusters of related evidence at an elementary level. The model offers the opportunity to present the evidence (Data), explain the reasoning for the Claim (Warrant). As highlighted in Toulmin's example, providing explanation and credibility in support of the Warrant (Backing) offers some measurement of the claim (Qualifier), and permits a rebuttal of the Claim (Reservation), all which promote a better understanding of the argument inherent in the Claim.

The Case Study suggests no consideration was expressed that exculpatory evidence may exist, that the evidence may not be correct and no validation was undertaken. Toulmin's model offers the opportunity to develop templates to ensure that more complete and vigorous examination of the evidence occurs. If Toulmin's model is applied to the Case Study, it replaces the disorder with a thorough, complete and structured perspective of the elements of the charge against the defendant. Taking an overview of the Case Study, the prosecution claim and the defence rebuttal is illustrated in Figure 2. The model shows assertions made by the prosecution, such as the defendant had sole access to the computer based on witness testimony. This appears false, as exculpatory evidence suggested the witness testimony was dubious based on other digital evidence that was valid and which contradicted their perjuries.

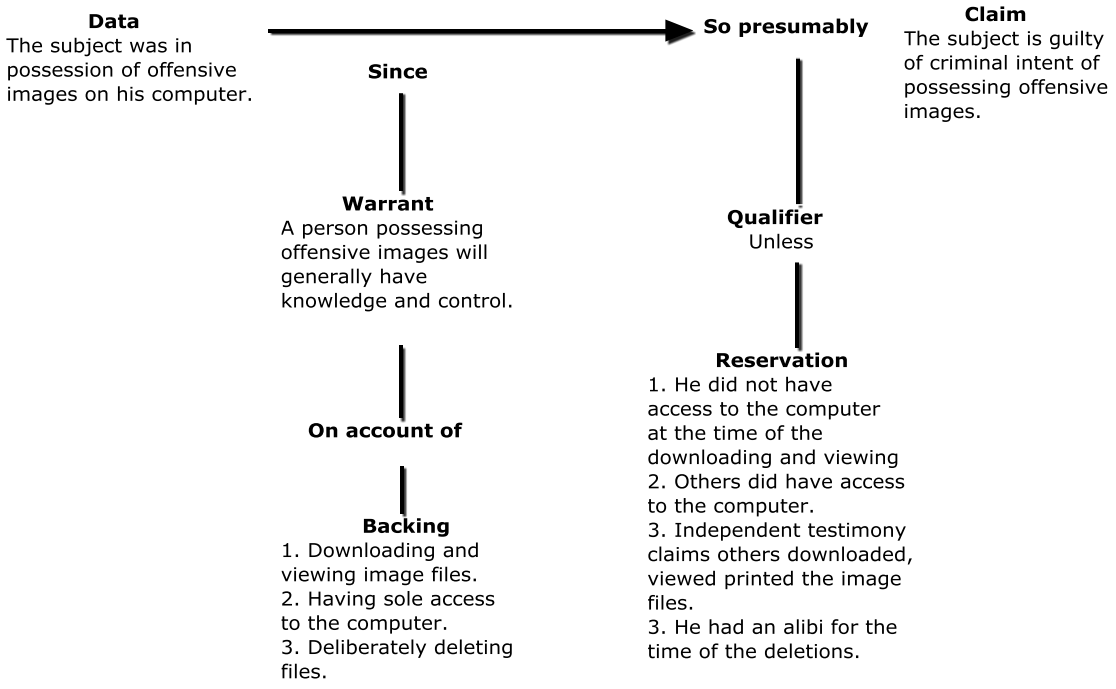


Fig. 2. An overview of the Case Study case using Toulmin's Model.

The benefit of representing the argument in this format should be evident to the reader. Backing and for that matter Reservation, can contain expert opinion and statistical research, but both should be validated. The model allows the examiner to build a simple list of facts from which assertions are derived and check those against a list of facts that may exist and used in the reservation to test the original argument. This visual aid encourages rebuttal of the counter claim to complete analysis and show the lines of reasoning; a simple yet powerful model. The model can be used to show an overview of the case evidence and broken down into individual evidence exhibits or groups.

Computer events should be checked and tested to avoid ambiguous, inaccurate and irrelevant outcomes and this can also be represented in the model.

## 6. VALIDATION PROBLEMS

The International Standards ISO/IEC DIS 27037 sets broad guidelines to validate forensics tool and processes used in the evidence retrieval stages with an expectation that the evidence is what it purports to be. The Standards Australia International's Guidelines for the Management of IT evidence: A handbook (2003) states that, *"The objective of this stage of the lifecycle is to persuade decision-makers (e.g. management, lawyer, judge, etc.) of the validity of the facts and opinion deduced from the evidence."* The guidelines were intended to assist a range of stakeholders, including investigators and the legal fraternity, who rely on digital evidence held in electronic records in various legal cases. These standards are broad but offer no formal validation process of digital evidence *per se* during the analysis stage.

Dardick (2010) offers guidance, stressing the need for standards of assurance required and asserts that digital evidence validation requires a rigorous examination of the quality of evidence available and proposes a checklist that ensures cases are thoroughly validated through examination of: accuracy, authenticity, completeness, confidentiality, consistency, possession, relevance and timeliness. Certainly, digital evidence validation requires more study and research as it underpins a crucial

forensic tenet. Defining validation and testing applicable processes that make it useful to examiners and lawyers seems overdue.

A definition of validation or correctness in the context of cyber forensics may be taken from Sippl & Sippl (1980, p. 608) as being a relative measure of the quality of being correct, sound, efficient, etc., and defining data validity as a relation or measure of validity. Such relations and measures based on specific examination must rely on tests and checks to verify the reliability of the data, thereby validating the data or determining a degree of acceptability of the evidence (Sippl & Sippl, 1980, p. 140). The Dictionary of Psychology (2009) defines validation as, *". . . soundness or adequacy of something or the extent to which it satisfies certain standards or conditions."* The Oxford Dictionary of English (2005) defines validation as, *". . . The process of establishing the truth, accuracy, or validity of something. The establishment by empirical means of the validity of a proposition.*"

More relevant to digital evidence is a legal definition of validity and soundness of judicial inference that involves conceptualisation of the actual event described by language for the trial, while abstract law approaches actuality as it is interpreted for application in the verdict (Azuelos-Atias, 2007). Consequently, to apply an abstract law to a concrete occurrence, the occurrence is abstracted and the law is interpreted.

Verification of the evidence involves complete, objective checking of conformity to some well-defined specification, whereas validation refers to a somewhat subjective assessment of likely suitability in the intended environment (A Dictionary of Computing, 2008). If the verification and validation of the existing digital and the extra digital evidence had provided contradictory or ambiguous findings, the case may not have proceeded to trial because of the weakness of the evidence to link the defendant to the crime.

According to Cohen (2006), incomplete scrutiny of the available evidence during the validation stage of the investigative process and failure to validate the evidence at that point is where the investigation can fail. But what is sometimes missing in cyber forensics is some formal and practical process of validating evidence to measure the extent to which the evidence is what it purports to be: a simple, reliable, validation test. The introduction of validation standards and compliance to such standards should encourage correctness and completeness in cyber forensics analysis. Selecting evidence relevant to only one party to a case contravenes legal discovery requirements. Failing to validate that same evidence is unacceptable neglect.

## 7. VALIDATION ISSUES IN THE CASE STUDY

The prosecution analyst in the Case Study did establish implicit relationships between each exhibit but failed to describe the relationship in full, meaningful terms and certainly provided no proof of comprehensive evidence validation. These issues seem to be an inherent deficiency in other child pornography cases examined by the author.

One argument presented by the prosecution analyst in the Case Study suggested the defendant installed software to delete browser cookies and history cache files automatically and opined this was done to conceal browsing for child pornography. The general assumption that computer users install such software for anti-forensics purposes was based on the expert opinion of the analysts and not backed with any meaningful statistics which may have been admissible had they been available. It was guesswork and well outside proper expert opinion. The defendant's explanation, never sought by the prosecution, and later examination of the computer confirmed conclusively the software related to a browser not installed on his computer; the validity of the claim never being tested before being presented to the jury. Use of such 'proclivity' evidence in child pornography trials is always controversial and on occasions introduced under legislation to bolster prosecution cases. Had it not been challenged by the defence it is likely that the argument would have been accepted at face value by the jury. More properly, this evidence should have been debated and rejected as inadmissible in the absence of the jury based on the outcome of argument between the prosecution analyst and defence

expert and not been allowed to influence the jury unnecessarily.

The prosecution analyst argued that the Internet browser was uninstalled just prior to the seizure of the evidence to conceal wrongdoing but the files were recovered from the Recycler. The prosecution lawyer made much of the allegation that the defendant had attempted to uninstall the browser based on the prosecution analyst's testimony. The matter of whether the browser was uninstalled or deleted was patently irrelevant to the argument; the fact that the application was removed was a strong claim the prosecution could use without needlessly obfuscating the issue. What the prosecution failed to validate was whether the time of deletion corresponded with the defendant's access to the computer. The deletion timestamp was never validated nor was it used to check the defendant's alibi that he was elsewhere when the deletion occurred. As it transpired, the browser uninstall operation was a deletion; appearing to be a panic reaction by the real culprits who were inadvertently warned of the raid during the absence of the defendant and later most likely perjured themselves when denying all access to the computer. The reader can be forgiven for believing the prosecution analyst was determined to secure conviction on clearly dubious facts.

Significantly, the exculpatory evidence located on the computer included correspondence and browser events that pointed to the use of the computer by the defendant's tenants who rented an adjacent building with free and open access to the defendant's residence. Some of this evidence was recovered from unallocated space and contained little or no temporal metadata. What it did contain was content linking it to the tenants, notably Internet access logs and cookies and private documents and photographs exclusive to the tenants and their friends. It was also possible to calculate the creation dates of recovered job applications, school projects, photographs of school parties and curriculum vitae. The creation dates of more than twenty of these files corresponded with periods when the computer was used to browse for child pornography. This required corroboration and validation of the evidence against known events in the lives of the tenants. This information was known to the prosecution analyst but for some reason discounted and ignored.

Browsing activities for child pornography may be corroborated through search histories, downloaded files, browser caches, and viewing and storage behavior by the user. There was no attempt made to link the browsing activities to known or suspected users of the computer, despite the defendant's explanation provided at the time of his arrest and subsequent interview. A simple validation check would have identified exculpatory evidence raising the possibility that others were involved in illicit browsing and downloading offensive material. Reconstruction of browsing activities is part of the validation process, checking and testing each file is crucial to measure the truth of the matter. This must be done before any attempt can be made to test the weight of the evidence.

## 8. POTENTIAL SOLUTION TO THE VALIDATION ISSUES IN THE CASE STUDY

Validation of the digital evidence presented in the Case Study and majority of prosecution cases examined by the author appeared superficial or absent. In themselves, the reports were meaningless to the non-technical lawyers requiring the author to translate and interpret the evidence for them in meaningful terms. The prosecution analyst corroborated some digital evidence exhibits presented in the case but not all, seemingly taking others at face value or interpreting their status to suit his viewpoint when testifying.

Digital evidence is circumstantial evidence and considered hearsay evidence that may only be admitted in legal proceedings under established procedures (Anderson & Twinning, 1991). Business records, including electronic records, are admissible in evidence as an exception to the hearsay rule but are subject to certain requirements such as those maintained in normal business activities and assurances that reasonable measures were taken to protect the authenticity and accuracy of the records (Chaikin, 2006).

In line with many other jurisdictions, Western Australian jurisprudence gives the benefit of doubt to accused parties when circumstantial evidence cannot be corroborated. For example, undated offensive

images recovered through data carving of unallocated space will be regarded as inadmissible during a trial if it cannot be corroborated by other evidence (SOWA versus Sabourne, 2010). Consequently, the corroboration of a digital evidence exhibit may be seen as a mandatory part of the validation process.

From a forensics perspective, the measurement of evidentiary weight requires validation checking and testing of the admissibility and plausibility of digital evidence, and then confirming corroboration. Admissible evidence means it was legally acquired; plausible evidence means that it is relevant, accurate and consistent with known facts; and corroboration means proving the existence of independent evidence to validate the exhibit and its relationship with the former exhibit.

Some structure is required if validation is to be attempted and here the author offers a formal, validation process, as distinct from an ad hoc, intuitive process, to measure the evidentiary weight of digital evidence through measurements of its admissibility, plausibility and corroboration. Evidentiary weight is the strength of the evidence against a pre-set threshold above which the evidence may be considered likely to be true in a specific legal case.

Validation requires checking and testing of each exhibit as well as the relationship between corroborating exhibits to measure their evidentiary weights:

**Checking** is examining an exhibit to measure validity of the data, metadata and relationships with other exhibits. For example, in the Case Study, the time of deletion of the Internet browser was obtained from the Recycler, compared with the defendant's alibi, triangulated with the computer clock and was then checked against other events to complete the validation process.

**Testing** uses experiments, existing experiment data or reliable statistics to measure the validity of the relationship between exhibits. Testing whether the browser was deleted, complemented the testing of the deletion and showed through modelling that deletion and uninstallation left different artefacts on a computer; a thorough and conclusive exercise that provided a more reliable and complete reconstruction of events compared with the prosecution analyst's report.

Using the process, validation is depicted as a three-step process consisting of an object (the evidence), a claim (statement about the evidence) and a test (to validate the claim). As shown in the example in Figure 3 the process would test the correctness of the timestamp of a photograph on a storage device. The process starts with a statement that the evidence (Object) was correct (Claim) and the claim was checked and tested (Test) and produced a result. In this example, six outcomes are offered but this may vary according to case context. Whether the weight of the evidence passes a predetermined, acceptable threshold will depend on the outcomes of the test.

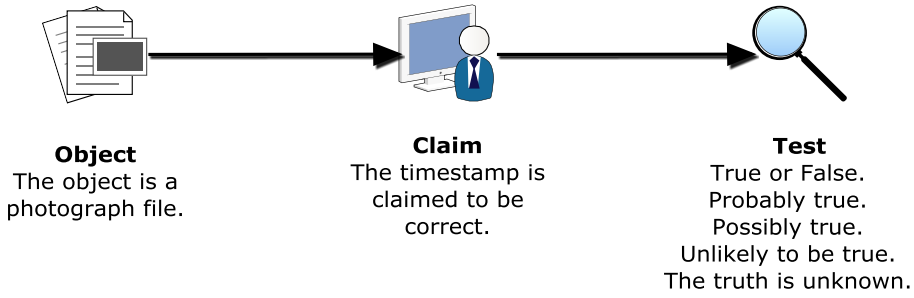


Fig. 3. Validation process to test the evidence.

The testing stages entails measuring the strength of the claim through checking and testing the admissibility of the evidence (o), the plausibility of the evidence (p) and corroboration of the evidence (c) to determine whether the strength of the evidence is higher than a predetermined threshold. A higher threshold would be appropriate in criminal cases where a greater the burden of proof is placed

on the prosecution, where the soundness of the evidence must be beyond reasonable doubt. In civil litigation the burden of proof is determined at a lower threshold based on a balance of probability.

The admissibility of the evidence requires confirmation that the evidence was obtained lawfully and is relevant to the case (claim, o,), although relevance issues may be decided during pre-trial 'hot-tubbing' of the analysts and during the trial. If the evidence fails this test the evidence is inadmissible and must be excised from the case. If the evidence is admissible the claim may be set alongside the plausibility test to determine its plausibility (claim, p). At this stage it does not matter whether plausibility is proved to be true or false as long as it is sufficiently reasonable to include it as part of the argument that will ultimately require validation of each supporting exhibit used in the claim.

Corroboration requires confirmation that the exhibit is corroborated with one other valid exhibit but a requirement for more than one corroborating exhibit may be factored in depending on the case type. The claim may then be set alongside corroboration (claim, c). Assuming the conditions of admissibility are met, examination of the results of the plausibility and corroboration tests can be used to measures whether the strength of evidence is higher or lower than the set threshold:

If (c,p) > threshold then the claim has a high degree of probability.

In the Case Study, the assertion was made that the defendant deliberately uninstalled the browser to conceal illegal browsing activity. An alibi confirmed that comparing the time of the removal (later confirmed to be deletion) of the browser with the whereabouts of the defendant established that the defendant was not present and could not have been involved. No further testing is required – the evidence is irrelevant and must be rejected. As shown in Figure 4 the evidence, while legally acquired under warrant, was irrelevant to the case although it was allowed to be presented to the jury. Plausible argument was demolished by a lack of corroboration and additional evidence that rebutted the original argument.

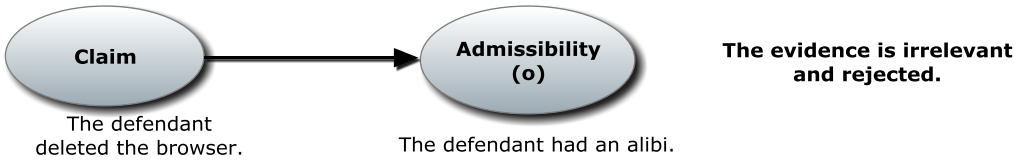


Fig. 4. Inadmissibility of the evidence.

If the evidence is admissible the plausibility and corroboration stages will test and check the evidence so that the two sets of results may be used to measure the strength of the evidence and determine the likelihood the claim is true. In the hypothetical example in Figure 5 the claim that the defendant deliberately deleted the browser to conceal evidence of a crime is a plausible assertion based on the presence of evidence of deletion and the defendant's ownership of the computer. It is not proven and still requires corroboration. Some other evidence, such as linking the defendant to the computer during the deletion process would bolster the strength of the evidence. If the plausibility and corroboration are calculated to be above the threshold then the claim is substantiated as being highly probable.

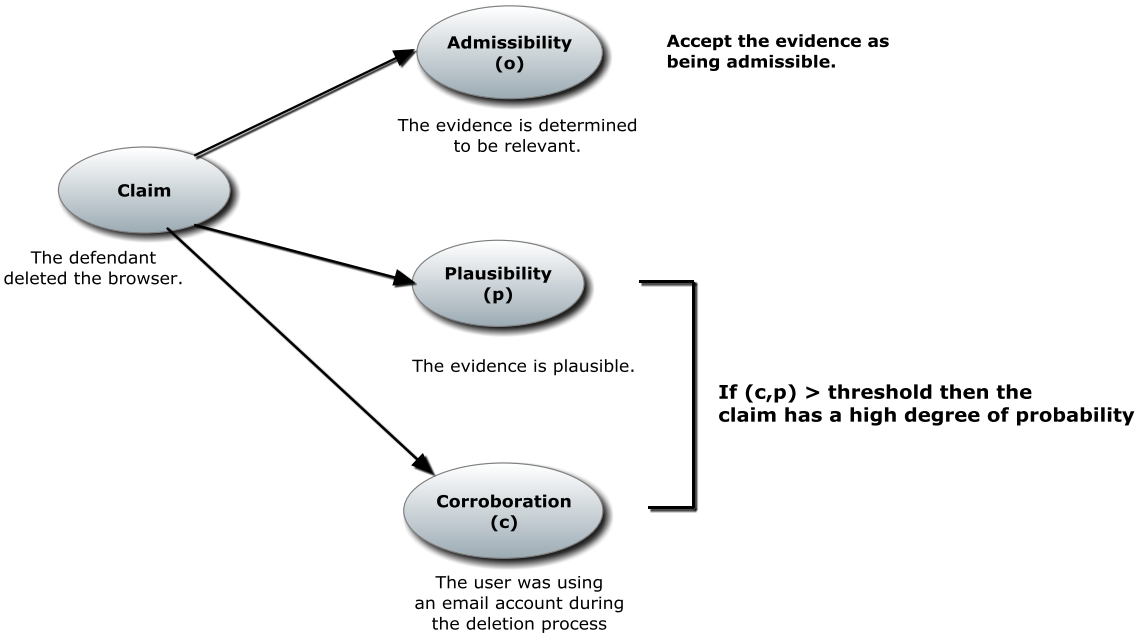


Fig. 5 Example of the plausibility and corroboration of digital evidence.

Testing and checking the validity of these exhibits might require comparison of the timestamps of the deleted files recovered from the Recycler and the sent email messages as illustrated in figure 6. The email messages would also require examination to determine the plausibility of the messages being created by the defendant or an impostor.

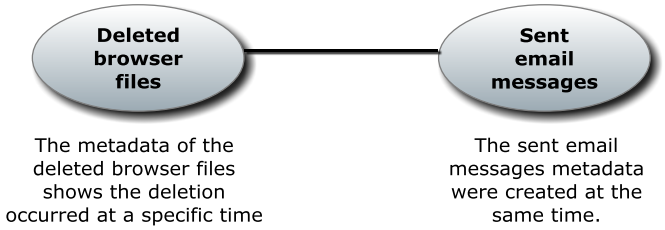


Fig. 6. Comparison of the corroboratory exhibit.

The process of admissibility checking of the primary exhibit is shown in Figure 7 which involves plausibility checking to determine the relevance, accuracy and consistency (unambiguity) of the evidence. For example: testing if the timestamps are relevant to a user of another user accessing the Internet; consistency checking to check for ambiguities timestamps that are unclear as to whether they were edited or the changed as a result of some other process; and checking the accuracy of time stamps to see if the files are relevant to the case.

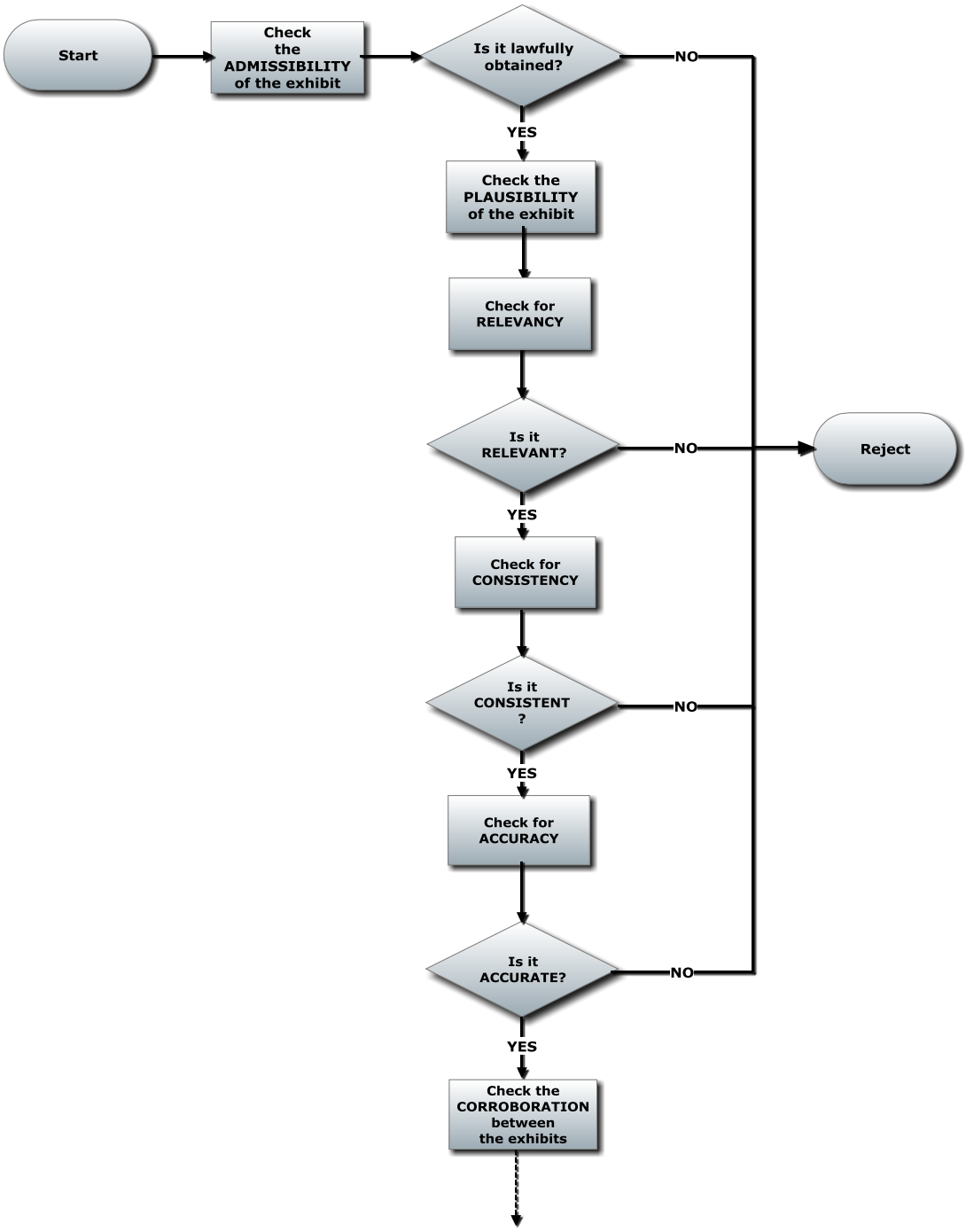


Fig. 7. Checking the relevance, accuracy and consistency during the plausibility stage.

Figure 8 shows the process continued through to the corroboration stage where the corroborating exhibit and the relationship between the primary exhibit and the corroborating exhibit are checked and tested. Corroboration between exhibits may involve: relevance checking to show that the file accessed on the external drive was the same file shown in the Jump List Log; consistency checking to see if a deleted file was identical with a file shown in an application log or other files with the same name; and accuracy checking the timestamps to show a correlation between browsing and other critical user events.

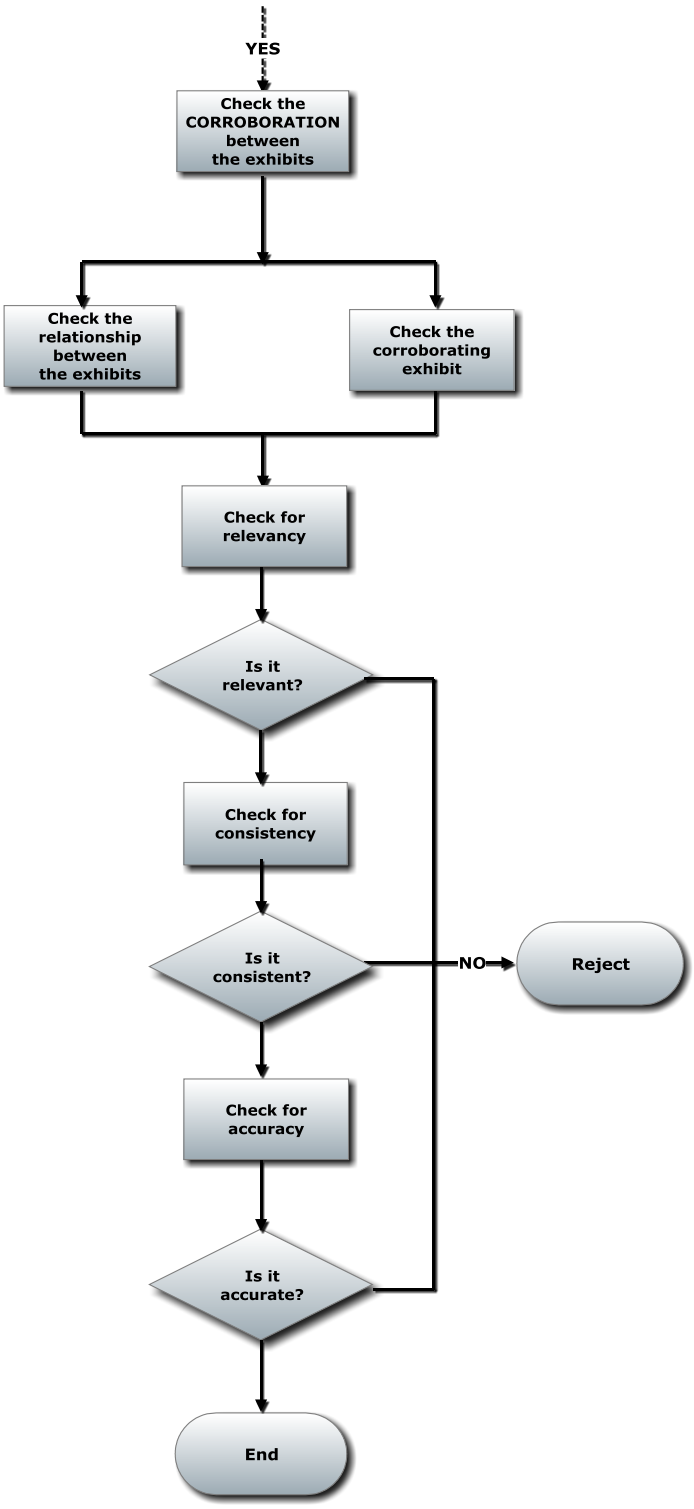


Fig. 8. Checking corroboration and relationships between exhibits.

Presenting the findings of the analysis and the validation checking on which the claims are evaluated confronts forensics examiners and prompts more thorough examination. This sub-argument, based on the validation testing in the Case Study could be represented using Toulmin's model as shown in

Figure 9. The reservation (rebuttal) statements are based on testing the plausibility and corroboration of relevant exhibits, and cast a different outlook on the case than that prosecution argument. Validation issues are shown such as evidence that the deletion of the browser was incompatible with the defendant's alibi.

Of course, if appropriate, the rebuttal may also be rebutted by the analyst and legal team and so forth. The point is, clarity of the argument is clearer and the evidence relied that much easier to understand and evaluate providing both parties a more reliable prognosis.

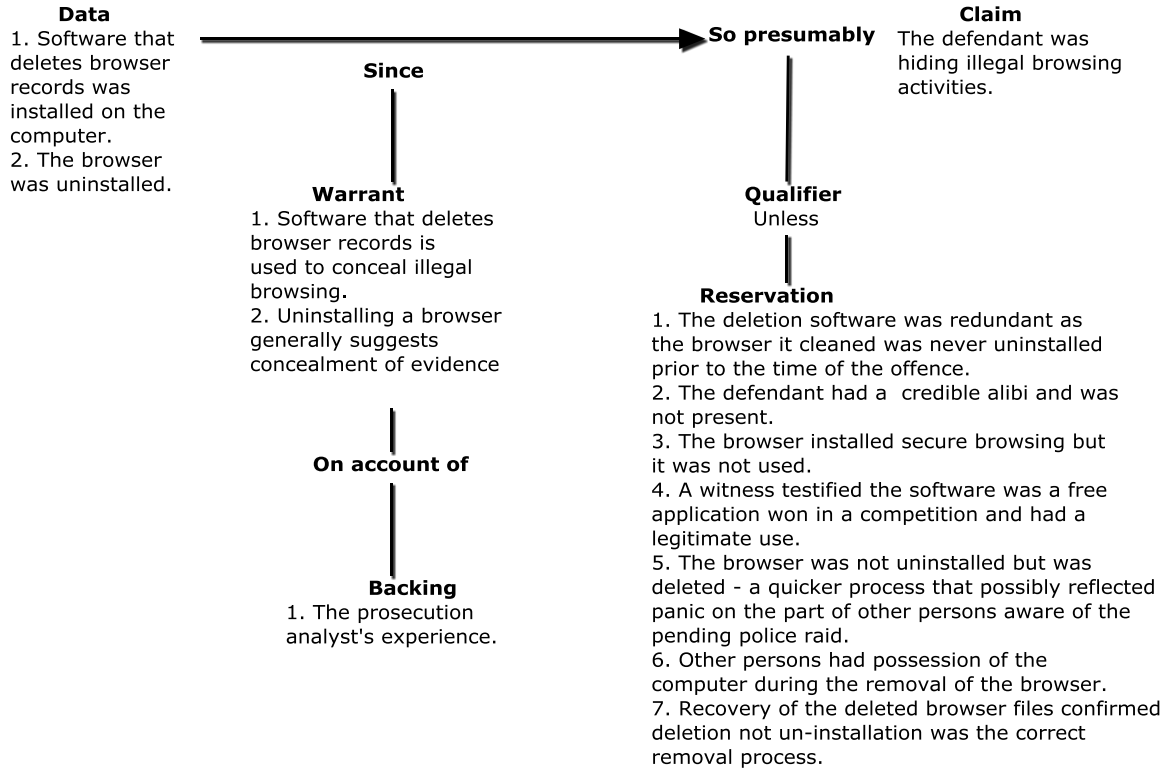


Fig. 9. A sub-argument showing a strong rebuttal

The process can be used to measure each individual thread of evidence as well as measuring the combined weight of evidence that comprises the trial case. The process offers some structural form to ensure that all relevant evidence is validated and presented with greater clarity in child pornography cases and potentially in a range of other digital evidence-based cases. The process minimises the chance that key validation issues are overlooked or trivialised. Ideally, it provides the means to measure the strength of each exhibit and evidence string that form part of the case, although this Case Study does not address the complexities of combining and measuring results of the process that affect the validity of the evidence.

## 9. CONCLUSION

The Case Study identifies issues of inadequate reasoning during analysis, compounded by poor presentation of even the basic facts, further degraded by inadequate validation of the digital evidence. Innocent or not, all facing the court should expect that the evidence presented is complete and correct. It is reasonable to expect that vigorous processes were used to measure its completeness and correctness; that the evidence is valid and is what it purports to be. Ideally, the trial should proceed with the best evidence available with a degree of confidence that it is what it purports to be.

Validation seeks a rigorous examination of the admissibility, plausibility and corroboration of the evidence. Presenting the evidence that has undergone complete validation using well-established argument models such as Toulmin's model has much to commend it. Correct and complete validation of digital evidence presented with clarity is so important and offers great benefits to the forensics examiner and the legal practitioner. It allows the evidence analysis to be independently scrutinised and audited; it makes the examiner accountable; and engenders thorough and diligent analysis of a high standard. Most importantly, it seeks the truth of the matter and without bias, a fundamental hallmark of forensics science.

The author has adopted Toulmin's model and the validation processes in case analysis presentations and already notes improved efficiencies in case management and communication with legal practitioners. Further research into refining the validation processes to serve a range of different case scenarios appears worthwhile.

## AUTHOR BIOGRAPHY

Mr. Richard Boddington holds a B.Sc (Hons) 1st Class and is completing Ph.D. research in digital evidence validation at Murdoch University, Australia where he teaches and researches information security and cyber forensics. He has a police and security intelligence background and provides cyber forensic analysis and expert testimony for the legal fraternity in a range of civil and criminal cases.

## ACKNOWLEDGEMENTS

Sincere thanks are extended to Drs. Valerie Hobbs and Graham Mann of Murdoch University for their support and feedback during the preparation of the paper.

## REFERENCES

A Dictionary of Computing. (2008). Eds. John Daintith and Edmund Wright. Oxford University Press, *Oxford Reference Online*. Accessed 21 December 2010 http://0-www.oxfordreference.com.prospero.murdoch.edu.au/views/ENTRY.html?subview=Main&entry=t11.e5680

A Dictionary of Psychology. (2010). Ed. Andrew M. Colman. Oxford University Press, *Oxford Reference Online*. Accessed 21 December 2010 http://0-www.oxfordreference.com.prospero.murdoch.edu.au/views/ENTRY.html?subview=Main&entry=t87.e8721

Anderson, T., & Twining, W. (1991). *Analysis of evidence: How to do things with facts based on Wigmore's Science of Judicial Proof*. Evanston, IL: Northwestern University Press. Australian Law Dictionary. (2012). Accessed 20 January 2012: http://0-www.oxfordreference.com.prospero.murdoch.edu.au/views/ENTRY.html?subview=Main&entry=t317.e10

Azuelos-Atias, S. (2007). *A pragmatic analysis of legal proofs of criminal intent*. Philadelphia: J. Benjamins Pub. Co

Berk, R. A. (1983). An introduction to sample selection bias in sociological data. *American Sociological Review, 48*, 386 - 398.

Caloyannides, M. A. (2003). Digital evidence and reasonable doubt. *IEEE Security and Privacy, 1*(6), 89 - 91.

Carrick, D. (2010). *The Chamberlain case: The lessons learned*. Melbourne: ABC Radio National.

Chaikin, D. (2006). Network investigations of cyber attacks: The limits of digital evidence. *Crime Law & Social Change, 46*, 239 - 256.

Cohen, F. (2006). Challenges to digital forensic evidence. Accessed 22 June, 2006, from http://all.net/Talks/CyberCrimeSummit06.pdf.

Dardick, G. S. (2010). *Cyber forensic assurance*. Paper presented at the 8th Australian Digital Forensics Conference.

Flusche, K. J. (2001). Computer forensic Case Study: Espionage, Part 1 Just finding the file is not enough! *Information Security Journal, 10*(1), 1 - 10.

George, E. (2004). Trojan virus defence: Regina v Aaron Caffrey, Southwark Crown Court. *Digital Investigation, 1*(2), 89.

Guidelines for the management of IT evidence: A handbook (HB171). (2003).

Inman, K., & Rudin, N. (2001), *Principles and Practices of Criminalistics: The Profession of Forensic Science.* CRC Press: Boca Raton, Florida.

Jones, A. (2011, November 2011). Meet the DF Professionals. *Digital Forensics, 9,* 37 – 38.

Koehler, J. J., & Thompson, William. C. . (2006). Mock jurors' reactions to selective presentation of evidence from multiple-opportunity searches: American Psychology-Law Society/Division 41 of the American Psychological Association.

Lemos, R. (2008). Lax security leads to child-porn charges [Electronic Version]. *Security Focus*. Accessed 22 November 2008 from http://www.securityfocus.com/brief/756.

Palmer, G. L. (2002). Forensic analysis in the digital world. *International Journal of Digital Evidence, 1*(1).

Pollitt, M. M. (2008). Applying traditional forensic taxonomy to digital forensics. *Advances in Digital Forensics IV IFIP International Federation for Information Processing, 285*, 17 - 26.

Saunders, K., M. (1994 ). Law as Rhetoric, Rhetoric as Argument. *Journal of Legal Education, 44*, 566.

State of Western Australia versus Sabourne. (2010). Perth District Court.

State of Western Australia versus Buchanan, 2009. Perth District Court.

Sippl, C. J., & Sippl, R. J. (1980). *Computer Dictionary* (3rd ed.). Indianapolis: Howard W Sams & Co.

Sydney Morning Herald. (2012). Accessed 8 February 2012 http://www.smh.com.au/national/growing-alarm-over-child-porn-epidemic-20120207-1r667.html

The Oxford Dictionary of English. (2010). (revised edition). Eds. Catherine Soanes and Angus Stevenson. Oxford University Press, *Oxford Reference Online*. Accessed 21 December 2010 http://0-www.oxfordreference.com.prospero.murdoch.edu.au/views/ENTRY.html?subview=Main&entry=t140.e85868

Toulmin, S. E. (1958). *The uses of argument*. Cambridge: University Press.

Walton, D. (2004). *Abductive Reasoning*. Tuscaloosa: The University of Alabama Press.