Northwestern Journal of Technology and Intellectual Property

Volume 12 | Issue 2 Article 5

Spring 2014

Digital Forensic Evidence in the Courtroom: Understanding Content and Quality

Daniel B. Garrie
Law and Forensics.com

J. David Morrissy
Zeichner Ellman and Krause LLP

N O R T H W E S T E R N
JOURNAL OF TECHNOLOGY
AND
INTELLECTUAL PROPERTY

Digital Forensic Evidence in the Courtroom: Understanding Content and Quality

Daniel B. Garrie & J. David Morrissy

April 2014 VOL. 12, NO. 2

Northwestern Journal of Technology and Intellectual Property
Volume 12, Number 2 (April 2014)

Digital Forensic Evidence in the Courtroom: Understanding Content and Quality

By Daniel B. Garrie & J. David Morrissy*

¶1 With the widespread permeation of continually advancing technologies into our daily lives, it is inevitable that the product of those technologies, i.e., digital information, makes its way into the courtroom. This has largely occurred in the form of electronic discovery, or "e-discovery", where each party involved in an action provides the relevant information they possess electronically. However, in cases where information is hidden, erased, or otherwise altered, digital forensic analysis is necessary to draw further conclusions about the available evidence.[1] Digital forensic analysis is analogous to more traditional forensic analysis. For example, in criminal cases where a firearm was used in the commission of the crime, but the gun is not readily admissible,[2] forensic science is necessary to trace the origin of the weapon, perform fingerprint analysis on it, and compare fired bullet casings to ensure the weapon used and the weapon analyzed are one and the same.[3]

---

* Daniel B. Garrie is a Partner at Law and Forensics.com, where he focuses on e-discovery and forensics and acts as Special Counsel to the law firm of Zeichner Ellman & Krause (www.zeklaw.com), specializing in e-discovery and cyber-security matters. For more information, or with questions and comments, please email at Daniel@lawandforensics.com. J. David Morrissy is an attorney with Zeichner Ellman & Krause. The views of the authors are their own, and do not represent the views or opinions of Law and Forensics or Zeichner Ellman & Krause LLP.

[1] *See generally*, PETER STEPHENSON, INVESTIGATING COMPUTER RELATED CRIME (2000).

[2] *See, e.g.*, *Pistorius murder trial postponed until August 19*, FRANCE 24 (Apr. 6, 2013), http://www.france24.com/en/20130604-pistorius-due-court-murder-charges-steenkamp.

[3] *See* Saby Ghoshray, *Untangling the CSI Effect in Criminal Jurisprudence: Circumstantial Evidence, Reasonable Doubt, and Jury Manipulation*, 41 NEW ENG. L. REV. 533 (2006-2007).

¶2 In sum, digital forensics is the preservation and analysis of electronic data.[4] These data include the primary substantive data (the gun) and the secondary data attached to the primary data, such as data trails and time/date stamps (the fingerprints).[5] These data trails and other metadata markers are often the key to establishing a timeline and correlating important events.[6]

I. A BRIEF HISTORY OF DIGITAL FORENSICS

¶3 A forensic report, whether for digital evidence or physical evidence, must have conclusions that are reproducible by independent third parties.[7] So, facts discovered and opinions formed need to be documented and referenced to their sources. Why? Ones and zeros do not lie. Therefore, forensic reports that contain opinions based upon properly documented digital sources are much more likely to withstand judicial scrutiny than are opinions based on less reliable sources.[8]

¶4 The reigning case in scientific evidence admission is *Daubert v. Merrell Dow Pharmaceuticals Inc*., 509 U.S. 579, 595 (1993). The decision in *Daubert* set forth a five-pronged standard for judges to determine whether scientific evidence is admissible in federal court. The *Daubert* standard applies to any scientific procedure used to prepare or uncover evidence and comprises the following factors:

(1) Testing: Has the scientific procedure been independently tested?
(2) Peer Review: Has the scientific procedure been published and subjected to peer review?

---

[4] This article recognizes that e-discovery and computer forensics are not co-extensive. Whereas e-discovery is typically sufficient, forensics offers more detail and should be viewed as complementing e-discovery in many cases. Lynn Roth, *Introduction to Computer Forensics*, NEV. LAW., June 2009, at 12, 15. *See also*, *Daubert* Evidentiary Hr'g Tr. at 170-71, U.S. v. Gardner, 2:10-CR-551-TC, Dec. 3, 2012 (Docket No. 262), ("[Experts defined digital forensics as] a specialized practice in investigating computer media for the purpose of discovery, analyzing available hidden or deleted data information that may serve as useful evidence in a legal matter.").

[5] For an in-depth discussion of secondary data, otherwise known as metadata, see Philip J. Favro, *A New Frontier in Electronic Discovery: Preserving and Obtaining Metadata*, 13 B.U. J. SCI. & TECH. L. 1 (2007), available at https://www-dr.bu.edu/law/central/jd/organizations/journals/scitech/volume131/documents/Favro_WEB.pdf.

[6] Momah v. Albert Einstein Med. Ctr., 164 F.R.D. 412, 418 (E.D. Pa. 1996) (ordering production of a document with metadata that was potentially relevant to establishing plaintiff's claim); *In re* Telxon Corp. Sec. Litig., No. 5:98CV2876, 1:01CV1078, 2004 WL 3192729, at *34 (N.D. Ohio July 16, 2004) ("[M]issing metadata [...] suggest[ed] that PwC may be withholding or has improperly destroyed discoverable information."); Wild v. Alster, 377 F. Supp. 2d 186, 194-95 (D.D.C. 2005) (denying motion for a new trial in a malpractice suit where metadata linked to photographic evidence showed date uploaded, not the date the photograph was taken).

[7] Simson Garfinkel et al., *Bringing Science to Digital Forensics with Standardized Forensic Corpora,* 6 DIGITAL INVESTIGATION S2 (Supp. 2009), *available at* http://www.dfrws.org/2009/proceedings/p2-garfinkel.pdf; Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, *Strengthening Forensic Science in the United States: A Path Forward*, THE NATIONAL ACADEMIES PRESS (Aug. 2009), https://www.ncjrs.gov/pdffiles1/nij/grants/228091.pdf.

[8] Daubert v. Merrell Dow Pharms., Inc., 509 U.S. 579, 595 (1993). *See* NutraSweet Co. v. X-L Eng'g Co., 227 F.3d 776, 788–89 (7th Cir. 2000) ("The district court did not abuse its discretion in concluding that the common and official acceptance of photographic analysis made it sufficiently reliable."); Clark v. Takata Corp., 192 F.3d 750, 758–59 (7th Cir. 1999) (holding proper the exclusion of expert opinion that was based only on experience or training with no scientific data or supporting research material or other rigorous methodology).

(3) Error rate: Is there a known error rate, or potential to know the error rate, associated with the use of the scientific procedure?
(4) Standards: Are there standards and protocols for the execution of the methodology of the scientific procedure?[9]
(5) Acceptance: Is the scientific procedure generally accepted by the relevant scientific community?

¶5 The *Daubert* standard provides judges with an objective set of guidelines for accepting scientific evidence. Following *Daubert*, the decision in *Kumho Tire v. Carmichael,* 526 U.S. 137 (1999) extended the *Daubert* standard to the qualification of expert witnesses by its interpretation of Federal Rule of Evidence ("FRE") 702. FRE 702 provides guidelines for qualifying expert witnesses, stating that the expert can have "scientific, technical, or other specialized knowledge." The *Kumho Tire* court extended the *Daubert* standard to apply to experts with technical or specialized knowledge, and not simply those called to testify regarding their scientific knowledge.

¶6 The majority of jurisdictions in the country favor the *Daubert* standard over the "general accepted practices" standard set forth in *Frye v. United States*, 293 F. 1013 (1923).[10] For jurisdictions in which *Daubert* is followed, there are a number of practical points that both attorneys and judges will benefit from knowing, in order to understand and effectuate the guidelines set forth in the *Daubert* standard. This article's goal is to elucidate those practical high-level points, thereby allowing counsel or judge to review technical expert reports and spot potential weaknesses.[11]

II. THE *DAUBERT* STANDARD IN THE CONTEXT OF THE EXPERT-REPORT DRAFTER

¶7 A digital forensics expert can be used in a variety of ways: as an expert witness,[12] for litigation support,[13] "to conduct Non-Invasive Data Acquisition (NIDA), to proactively investigate potential disputes . . . [prior to litigation], [and] to recover data negligently or intentionally destroyed."[14] Whether or not a digital forensics expert is retained to testify in court proceedings, a written report is still mandatory unless otherwise stipulated or ordered by the court.[15] This written report, if properly done, practically negates the need to provide expert testimony.[16]

---

[9] The fourth factor arose more explicitly through the evolution and interpretation of the case law surrounding evidence-based trial findings.

[10] Edward Cheng & Albert Yoon, *Does* Frye *or* Daubert *Matter? A Study of Scientific Admissibility Standards*, 91 VA. L. REV. 471, 473 (2005); Cassandra H. Welch, *Flexible Standards, Deferential Review:* Daubert*'s Legacy of Confusion*, 29 HARV. J. L. & PUB. POL. 1085, 1087-88 (Summer 2006).

[11] For a detailed article analyzing an expert report, see Robert Lerner & Althea Nagai, *A Critique of the Expert Report of Patricia Gurin in* Gratz v. Bollinger, CENTER FOR EQUAL OPPORTUNITY (May 7, 2001), http://50.116.98.17/~ceousa/attachments/article/534/Gurin%20Critique.pdf.

[12] *See, e.g.*, Craig Ball, *Cross-examination of the Computer Forensics Expert*, CRAIGBALL.COM (2004), http://www.craigball.com/expertcross.pdf.

[13] Sean L. Harrington, *Collaborating with a Digital Forensics Expert: Ultimate Tag-Team or Disastrous Duo?*, 38 WM. MITCHELL L. REV. 353, 367-69 (2011) (discussing the litigation support role of digital forensics experts).

[14] *See* Lynn Roth, *Introduction to Computer Forensics*, NEV. LAW., June 2009, at 12, 13.

[15] FED. R. CIV. P. 26(a)(2)(B).

[16] *See generally*, Ronald L. Carson, *Policing the Bases of Modern Expert Testimony*, 39 VAND. L. REV. 577 (1986).

¶8 Over the last several years, commercial hardware and software vendors who specialize in digital forensic analysis tools and applications have made significant improvements in the methodologies necessary to analyze digital evidence.[17] As a result, what was once an almost entirely *ad hoc* manual-analysis process is now structured to a point where years of experience and training are no longer necessary for the production of a digital forensic report.[18] This trend increased the number of forensic examiners and lowered costs, but also reduced the depth of knowledge held by the average forensic examiner.[19]

¶9 As a result, the reviewer of a forensic expert report should scrutinize the qualifications of a forensic examiner to avoid the unfortunate scenario wherein an unqualified forensic examiner produces a flawed or unreliable report.[20] While no uniform set of standards exists to gauge the competency of a digital forensic examiner, reviewers should consider the most appropriate combination of certification, education, and real-world experience, given the case at hand.[21] The examiner's training will likely include a number of hours in the classroom as well as practical experience in the real world and in the lab. This training should be considered in the context of the levels of experience and quality of the instructors and institutions administering such training.[22]

¶10 While individual vendor certifications can have value, the education marketplace is seeing the emergence of vendor-neutral certification programs to validate technology skills of varying levels.[23] Accordingly, as certification programs become more salable, the value of any particular certification must be assessed in the context of a growing industry in which establishing credentials is simply the monetization of a product.[24] The true measure of expertise goes well beyond certification and solidly into the realm of actual field experience in real-world situations and/or years of study. Thus, the bench and the bar should interpret a forensic certification only as an indication of additional testing that the forensic examiner navigated in a particular area, or in a specific type of software, that is particular to that examiner's education and experience.[25]

---

[17] Ewa Huebner et al., *Computer Forensics – Past, Present And Future*, 8 INFO. SECURITY TECHNICAL REP. 32, 54 (2007).

[18] This is not to say there are no hurdles or impediments to successfully training experts. For a thorough discussion of these difficulties, see Gal Shpantzer & Ted Ipsen, Law Enforcement Challenges in Digital Forensics, 6th Nat'l Colloquium Information Systems Security Education (June 6, 2002), available at http://www.isat.jmu.edu/common/Projects/NCISSE/2002presentations/shpantzer.pdf.

[19] For an exploration of the costs of digital forensic investigations, see Tyler Moore, The Economics of Digital Forensics, Fifth Workshop on The Econ. of Info. Sec. (June 26, 2006), available at http://weis2006.econinfosec.org/docs/14.pdf.

[20] *See* U.S. v. Bryan James Gardner, 2:10-CR-551-TC (D. Utah Dec. 21, 2012) (granting a motion in part to limit testimony by the expert as his report provided information and opinions outside of the realm of his designated expertise).

[21] R.E. Overill & R.I. Ferguson, Does Computer Forensics belong to Computer Science or Forensic Science?, 3d HEA ICS Workshop on Teaching Computer Forensics (Nov. 22, 2007), *available at* http://www.ics.heacademy.ac.uk/events/presentations/736_HEA-ICS-TchCompFor_paper.pdf.

[22] Philip Anderson et al., A Comparative Study of Teaching Forensics at a University Degree Level, Internat'l Conference on IT Security and Incident Management, IMF (2006).

[23] Matthew Meyers & Marc Rogers, *Computer forensics: The need for standardization and certification*, 3 INT'L J. DIGITAL EVIDENCE 1 (2004).

[24] *See generally*, LAW TECHNOLOGY NEWS (Aug. 2011), http://www.eddupdate.com/2011/08/sham-exam-.html (devoting an entire issue to the conundrum of vendor certification criticism and issues).

[25] Meyers & Rogers, *supra* note 24, at 10.

¶11 Finally, in addition to technical expertise, an ideal expert will have experience on the witness stand.[26] Although direct examination will set out the baseline requirements of a competent expert, the ability to calmly and confidently relay findings while undergoing rigorous cross-examination is critical.

III. Framework for Evaluating a Forensic Report

¶12 The sections below provide an evaluation framework that should be adjusted in accordance with the underlying facts of the dispute.

A. Examine the Mechanism Used to Collect the Digital Evidence

¶13 To begin, the reviewer should focus on the manner in which the evidence was acquired. The report should establish if the original evidence was acquired by a duplicate bit-by-bit image of a hard drive[27] or by live acquisition.[28] While the manner of acquisition is dictated by the circumstances, a bit-by-bit acquisition is generally more reliable than a live acquisition because there are fewer moving parts, reducing the opportunities for error or failure.[29]

¶14 In addition to the means of acquiring a digital image, reviewers should be aware of the format of the imaged data.[30] The primary format for images is E01.[31] E01 format is created using Encase software by Guidance Systems, and is the most popular software used for imaging,[32] although other programs can also create images in this format.

---

[26] Cornell Walker, *Computer Forensics: Bringing the Evidence to Court*, InfoSec Writers (Aug. 17, 2005), http://www.infosecwriters.com/text_resources/pdf/Computer_Forensics_to_Court.pdf.

[27] Orin S. Kerr, Searches and Seizures in a Digital World, 119 Harv. L. Rev. 531 (2005) (discussing bit-by-bit images, also known as bitstream copying as a copy of "every bit and byte on the target drive including all files, the slack space, Master File Table, and metadata in exactly the order they appear on the original"). See also, Bill Nelson et. al., Guide to Computer Forensics and Investigations 50 (2004) (discussing bit-by-bit images).

[28] "Live Acquisition refers to the acquisition of a machine that is still running and can retrieve both static and dynamic, volatile data." M.M. Grobler & S.H. von Solms, A Best Practice Approach to Live Forensic Acquisition Information Security South Africa Conference 2009 (July 2009), available at http://icsa.cs.up.ac.za/issa/2009/Proceedings/Full/1_Paper.pdf; Dario V. Forte, Volatile Data vs. Data at Rest: The Requirements of Digital Forensics, Network Security, June 2008, at 13-15. In a live acquisition, "computer forensic practitioners . . . run programs on [the target's] computers to acquire RAM, unencrypted files and any other data." Ryan Jones, Safer Live Forensic Acquisition, University of Kent Canterbury (Nov. 2007), http://www.cs.kent.ac.uk/pubs/ug/2007/co620-projects/forensic/report.pdf).

[29] For a step-by-step guide on authenticating digital forms of evidence, including audio and video, see Tom Owen et al., The Expert Witness – The Admissibility of Recorded Evidence, Law and the Expert Witness, AES 26/h International Conference (2005), available at http://tapeexpert.com/pdf/owendenver2005.pdf.

[30] For sample protocols for collecting forensic images, see North Carolina State Bureau of Investigation, *Computer Forensics Discipline*, Technical Procedure Manual, available at http://www.ncids.com/forensic/sbi/digital/computer_forensics_tech._proc._manual.pdf.

[31] Simson Garfinkel, *Digital forensics research: The next 10 years*, 7 Digital Investigation S64 (Supp. 2010), *available at* http://www.dtic.mil/dtic/tr/fulltext/u2/a549288.pdf.

[32] Vishal Ambhire & Dr. B.B. Meshram, *Digital Forensic Tools*, 2 IOSR J. Eng. 392 (Mar 2013), *available at* http://www.iosrjen.org/Papers/vol2_issue3/D023392398.pdf.

B. Forensic Report Should Provide Sufficient Details to Replicate Findings

¶15 A digital forensic report should document with sufficient detail the steps undertaken by the examiner so that an independent third-party could replicate the conclusions.[33] This also means that the forensic images should be available for copying by a third-party.[34]

¶16 In *Nucor Corp v. Bell*, 2008 WL 4442571 (D.S.C. Jan. 11, 2008), an expert offered testimony on evidence that the opposing party had used a non-traceable wiping program to clear evidence from a laptop. The spoliation case was based on the examination of a hard drive with large blocks of zeros surrounded by data.[35] The court denied a motion to exclude the expert's testimony, finding that the method used by the expert sufficiently filled the analytical gap between the data and the opinion.[36] With a nod to the *Daubert* factors, the court noted that the expert had tested a hypothesis as to how the blocks of zeroes had appeared on the drive, and had replicated the pattern of zeros.[37] The court also admitted evidence resulting from a testing that was found capable of repetition, because the expert had thoroughly documented each step in the test to establish that data had been written to the hard drive in the predicted manner.[38]

¶17 Generally, when the forensic images are not available to replicate the findings of a digital forensic report, the report is less dependable because of the inability to assess its accuracy or the reliability of its methodology. Reports with conclusions that are not reproducible using copies of the forensic images and similar analysis software should be granted little credence, and only reviewed in extraordinary circumstances.

C. Structure of a Digital Forensic Report

¶18 Generally, the forensic report is outlined as follows:

(1) Brief summary of information
(2) Tools used in the investigation process, including their purpose and any underlying assumptions associated with the tool
(3) Evidence Item #1 (For example: Employee A's work computer)
    (a) Summary of evidence found on Employee A's work computer
    (b) Analysis of relevant portions of Employee A's work computer
        (i) Email history
        (ii) Internet search history
        (iii) USB registry analysis
    (c) Repetition of above steps for other evidence items (which may include other computers and mobile devices, etc.)
(4) Recommendations and next steps for counsel to continue or cease investigation based on the findings in the report

---

[33] CHRIS DAVIS ET AL., HACKING EXPOSED COMPUTER FORENSICS SECRETS & SOLUTIONS 12-14 (2009).
[34] Jim Bates, *Fundamentals of Computer Forensics*, 3 INFO. SECURITY TECHNICAL REP. 75 (1998).
[35] Nucor Corp. v. Bell, 2008 WL 4442571 (D.S.C. Jan. 11, 2008).
[36] *Cf.* U.S. v. Bryan James Gardner 2:10-CR-551-TC (D. Utah Dec. 21, 2012) (limiting the scope of testimony by an expert after finding an expert's report to be conclusory and potentially confusing to a jury).
[37] Nucor Corp. v. Bell, 2008 WL 4442571 (D.S.C. Jan. 11, 2008).
[38] *Id*.

¶19 Generally speaking, the report should not volunteer superfluous information that may be vulnerable to scrutiny under cross-examination.[39] Further, all findings should be accurately qualified as to the limitations of the particular tool(s) used, the applicability of the current technology and industry-standard best practices, the methodology or techniques (such as search criteria or formulae), and the scope of the investigation.

¶20 The scope of the investigation is limited by relevancy and also by budget (a factor of which is the time necessary to conduct the investigation), which almost always places significant constraints on what data is found or not found and the inferences to be drawn therefrom. Moreover, the digital forensic report only investigates those areas where responsive evidence can be found. For example, in a case investigating the theft of proprietary software code, it would be outside the scope of the report to discuss a search for child pornography on the hard drive in question.[40]

¶21 Further, when evaluating a digital forensic report, a reviewer should evaluate the substance of the report to ascertain if information overload exists. The digital forensic report should provide a cohesive and logical framework on its face and not delve into the underlying technical minutiae. In this context, information overload rests on whether the report contains hundreds of pictures, documents, or other such digital items in the body of the report that distract from the underlying conclusions.

¶22 Examiners must resist overtures by attorneys, however well-intended or abstract, to submit any testimony or work product that is disrespectful of the truth, including overstating, understating, or omitting findings. The findings should be concise and carefully circumscribed. The report cannot be tailored to support a particular outcome, as a material omission may constitute fraud.[41]

D. The Forensic Report Should Establish the Tools Used and Assumptions Made by the Forensic Examiner

¶23 Many examiners use a variety of tools and it is important that the reviewer understands their genesis and purpose. The tools a forensic examiner uses should be explicitly stated in the report to assist the reviewer in understanding potential issues surrounding the conclusions the forensic tool is being used to support them.[42] For example, UNIX system log entries and X-Ways have similar capabilities, but the former was developed for programming purposes, such as debugging, and the latter for purposes of forensics analysis.

---

[39] *See* U.S. v. Bryan James Gardner 2:10-CR-551-TC (D. Utah, Dec. 21, 2012) (granting a motion in part to limit testimony by the expert as his report provided information and opinions outside of the realm of his designated expertise).

[40] Further, a shift in focus of an investigation may require a separate warrant if law enforcement officials are conducting the search. *See* United States v. Carey, 172 F.3d 1268 (10th Cir. 1999) (court suppressed discovery of child pornography where investigators were initially searching for evidence of narcotics transactions); *cf.* United States v. Walser, 275 F.3d 981, 986-87 (10th Cir. 2001) (during investigation of drug transactions, officer discovered child pornography, then suspended search for drug transactions, obtained warrant to search for child pornography, which was upheld by the court).

[41] For an international common law perspective, see Lirieka Meintjes-van der Walt, *Expert Odyssey: Thoughts on the Presentation and Evaluation of Scientific Evidence*, 120 S. AFR. L.J. 352 (2003).

[42] Brian Carrier, *Open Source Digital Forensics Tools: The Legal Argument*, STAKE RESEARCH REPORT (2002), http://dl.packetstormsecurity.net/papers/IDS/atstake_opensource_forensics.pdf.

IV. CONCLUSION

¶24 As the use of technology becomes increasingly ubiquitous, it is likely that digital forensic experts and their reports will become increasingly important to litigation.

¶25 Commentators have expressed the view that rather than asking whether the expertise presented is "science" or "non-science," courts should inquire into the methods that the experts are using, and when considering an expert's experience, "the existence of data showing that engineers, or physicians, or psychologists, or forensic scientists can measure or diagnose or predict or correct certain conditions does little if anything to support an inference that they possess the requisite expertise for another task or condition for which there are no data."[43] This means that reviewers should engage in an analysis that identifies the nature of the problem at issue and assesses whether data supports a conclusion that "necessary expertise exists to offer a dependable opinion on that problem."[44] Additionally, to the extent that forensic science methods have been tested in similar factual circumstances, and that those methods have been subjected to peer-review, and/or have a known error rate, it is appropriate for a court take those factors into account when such methods are presented as digital forensic expert evidence.

¶26 As digital forensic science advances, information about methodology should become more available as common techniques mature.[45] General acceptance of a technique may be relevant in the types of cases that arise repeatedly, such as spoliation of evidence cases requiring file recovery or forensic comparison. Nonetheless, cases involving the expert testimony of computer scientists are rife with unique factual situations that may require an innovative approach by the expert. Consequently, it is critical that the bench and the bar determine whether the facts of a case are such that a traditional technique can be applied before determining whether a *Daubert* analysis is necessary.

---

[43] DAVID L. FAIGMAN ET AL., MODERN SCIENTIFIC EVIDENCE: THE LAW AND SCIENCE OF EXPERT TESTIMONY § 1:25, at 70 (2008-2009 ed.).

[44] *Id*.

[45] Colin Armstrong, Developing a framework for evaluating computer forensic tools, Evaluation in Crime Trends and Justice: Trends and Methods Conference in Conjunction with the Australian Bureau of Statistics (Mar. 24-25, 2003), *available at* http://www.aic.gov.au/media_library/conferences/evaluation/armstrong.pdf.