ARTICLE:

# FORENSIC DOCUMENT EXAMINATION OF ELECTRONICALLY CAPTURED SIGNATURES

By **Heidi H. Harralson**

**Biodynamic signature systems are a means by which a person provides a signature in electronic format that is reproduced on the screen as a representation of their manuscript signature. These systems use software to record measurements when a person uses the device to produce a digital version of their handwritten signature. The measurements recorded include dynamic time-based measurements such as duration, velocity, air strokes, and pressure as well as static form-based measurements such as slant, length, height and shape. The combined data recorded establishes a unique signature profile of the person at the time of writing. The temporal, time-based features differ significantly from the static ink traces on paper documents that forensic document examiners typically analyze. Recommended procedures in forensic analysis include the acquisition of computer files and analysis of temporal features. Due to the varying quality of the data acquired by electronic signature systems, not all systems produce reliable information to support forensic opinions. A recent legal ruling in the U.S. underscores the need for forensic document examiners to examine electronic evidence in biodynamic signature cases. Working collaboration between forensic document examiners and computer experts is recommended.**

## Introduction

The electronic capture of handwritten signatures presents novel opportunities and challenges in forensic signature analysis. Biodynamic signatures allow for the analysis of temporal handwriting characteristics, characteristics not previously possible in the examination of traditional manuscript signatures signed with an inking pen on paper. Historically, forensic document examiners have focused on the examination of manuscript signatures. With the increasing use of electronic signatures, document examiners need to develop methods of analysis in order to reliably conduct examinations of these new technology-based signatures. Research into temporal handwriting features presents a new level of forensic identification previously unknown in the analysis of manuscript signatures. While temporal features add a deeper, more significant level of identification to handwriting, the devices used to record the measurements of the manuscript signature differ widely in technology. Temporal features such as the speed, pressure, and velocity are not available in all electronic signature cases – an inhibiting factor in forensic analysis. Some biodynamic systems incorporate computer-based biodynamic analysis of signatures. However, experimental research needs to be conducted to establish whether these systems are adequate in capturing handwriting features that would allow forensic document examiners to recognize the possible false negatives caused by handwriting variables (i.e., illness, disguise) or the possibility of false positives resulting from system attacks (simulation, forgery). The low resolution images recorded by many biodynamic signature systems make forensic analysis of biodynamic signatures either difficult or indeterminable. If these concerns are not addressed, the increasing use of biodynamic electronic signatures may create significant forensic problems in signature identification cases, in that document examiners may not have the expertise or methods to examine biodynamic electronic signatures; and forensic analysis may not be reliable because of the low resolution graphic images with limited or no temporal data.

Because of the onset of this new signature technology, document examiners have little in the way of published methods or procedures in the analysis of biodynamic

signatures, and little experimental research has been published about this in the field of document examination. Some biodynamic handwriting research has been used to detect differences between genuine and forged signatures or healthy handwriting compared to handwriting that indicates the person has a movement disorder, but biodynamic information is rarely available in forensic casework. Although temporal information is sometimes accessible in examining biodynamic signatures, document examiners have limited information about the technology and temporal features that can be analyzed. Some biodynamic systems perform automatic computerized signature analysis and verification. These types of systems are used for obtaining access or entry and are sometimes used instead of fingerprint, iris, or facial scans, because signatures cannot be replicated and are more user-friendly. However, there may be limitations in automatic signature verification with respect to system attacks (forgeries), handwriting variation, and data transmission loss.

## Applications

The applications for electronic signature technology are extensive, and they are in widespread use at an international level. Biodynamic signature software and hardware is manufactured and marketed by major corporations to areas such as finance, banking, health care, and mortgage lenders. Biodynamic signatures are used for access control, network access control, client identification purposes, document workflows, and electronic transaction security. Since the enactment of electronic signature legislation, the use of digital and other forms of electronic signature has increased significantly. They are used for contractual agreements, delivery verification, biometric security checkpoints, bank signature cards, and point-of-sale transactions. Traditional business has incorporated them into use for contractual negotiations, even in conservative business markets. It is inevitable that various forms of electronic signature technology will increase internationally as it maintains popularity over other forms of biometric analysis. Because signatures are intuitively associated with identity and are unique to the individual, they are more user-friendly and less invasive than other forms of biometric identification such as fingerprint, iris, facial, and gait recognition.

## The technology

There are several points that forensic document examiners need to consider when encountering an electronic signature. In understanding the technological aspects of electronic signatures, forensic document examiners would benefit by working with digital evidence specialists and obtain relevant training in areas specific to understanding the technology associated with electronic signature technology. There is considerable variety in the methods used to capture electronic signatures, which brings into question issues concerning external factors in signature production (such as using a stylus or mouse to write the signature), the sampling rate and accuracy to record the signature (Hertz[1]), tablet quality, and transmission of data.

One of the issues associated with the recording of the measurements of a manuscript signature is how the document examiner obtains access to the computer file containing the electronic signature. Many forensic document examiners may not be aware that when a person signs their manuscript signature with such a device, their actions are converted into measurements, as instructed by the writer of the software, and the data is then, in turn, translated into a series of digital data which is capable of being replicated on the screen in the form of a human-readable representation of the manuscript signature. The human-readable representation of the manuscript signature is not the only data that the forensic document examiner should be reviewing. If the forensic document examiner is provided with a hard copy of the static signature image for examination, this may not be the best evidence that should be examined or presented to the court. Many of these signatures are recorded at a low resolution with a pixelization effect replacing the smooth line quality of a manuscript signature. Sometimes the digital data comprising the signatures are affixed or incorporated into the document on a signature line in an unnatural way, or the signature's natural size may be significantly reduced – or both of these effects might occur. If the forensic document examiner receives a print-out of an electronic signature, such indications will be obvious that the signature was recorded electronically. If these factors are present, the forensic document examiner should make inquiries about how the signature was produced and require a copy of the electronic signature file, because it is the digital data that must be examined,

1 *Hans-Leo Teulings and Frans J. Maarse, 'Digital recording and processing of handwriting movements', Human Movement Science, Volume 3, 1984, 193-217.*

 

not only its representation. If the digital data exists, these need to be examined, because they provide the relevant information about the biodynamic properties of the purported signer, not the static image reproduced on paper.

Aside from examining the handwriting features that may have been recorded, some of the first steps in examining digital signature files is to inquire whether the file has been stored and processed in a way that allows for forensic signature analysis. Certain computer processing procedures are carried out in order to facilitate the feature extraction process. For example, different digital renditions of signatures, no matter how poor, may need to be moved, rescaled, and rotated to allow optimal comparison, thereby further cumulating the coarseness of pixilation.[2]

Packet loss or the loss of digital data transmitted over the internet can occur in some biodynamic signature verification systems.[3] There may have been distortion or loss of data during the transmission or processing of the data. During recording, ideally a signature is recorded at a constant sampling rate. However, the computer processor may miss sequences of samples. This implies that small parts of the signature may be missing purely due to the technology and not because the writer was omitting an essential part of the signature. The limit or threshold of information recorded or maintained in a signature that allows for forensic analysis has not been established in research. With respect to biodynamic systems in general, it has been commented that 'prior work on quality evaluation is limited'.[4]

The analysis of biodynamic electronic signatures involves an understanding of the software and hardware used to acquire the signature, especially in the way the purported signer may have interacted with the hardware. Additionally, the tablet and stylus used to produce biodynamic electronic signatures can significantly affect the way the signature is produced. For example, in an experiment comparing two comparable brand name Tablet PCs, one Tablet PC sensor provided less reliable sampling rate information than the other, which affected the performance of the signature verification system used on the Tablet PC for enrollment.[5]

Aside from the variables associated with tablets, significant changes in temporal and spatial dimensions occur when signatures are written with digital writing implements in comparison to signatures written with ink and paper. These differences are caused both by the writing device and the writer's response to the writing device. Hardware factors such as the enlarged tip of a digital writing pen and the lack of friction on a digital tablet can cause changes to a writer's natural signature. The size of the writing tablet box or pad and other conditions associated with biodynamic electronic signature capturing devices can have a varying effect on the way people respond to the device. Some web-based software programs instruct the signer to use a mouse or the tip of a finger while signing their signature into a box on a computer screen. Other devices have delayed visual feedback, or poor resolution (or both) when signing on a signature pad. Some devices provide instructions related to writing within the parameters of a box, or require that the signature be captured within a certain time frame (or both). Frustration with rejected signatures and responding to annoying instructions may cause some people to alter their natural signature in order to fit within the box and within specified time limits. Some devices are handheld, which creates another factor pertaining to awkward posture while signing on a device.

Understanding the software and system used to capture the biodynamic measurements is critical in the examination. Some systems do not record biodynamic data, while other systems capture varying degrees of biodynamic data.[6] Some systems may only record a few measurements, while others may record the measurements of several handwriting features that would allow for a comprehensive forensic analysis of temporal and form-based elements. One study examined the reliability of digital data captured by biodynamic verification systems and found that some measures

2 *Fayyaz A. Afsar, M. Arif and U. Farrukh, 'Wavelet Transform Based Global Features for Online Signature Recognition', 9th International Multitopic Conference, IEEE INMIC 2005, pp 1-6, Karachi, Pakistan, December 2005.*

3 *Jonas Richiardi, Julian Fierrez-Aguilar, Javier Ortega-Garcia and Andrzej Drygajlo, 'On-line signature verification resilience to packet loss in IP networks' IP Networks', 2nd COST275 Workshop on Biometrics on the Internet: Fundamentals, Advances and Applications, pp 11-16, Vigo, Spain, March 2004.*

4 *Fernando Alonso-Fernandez, Julian Fierrez and Javier Ortega-Garcia, 'Quality Measures in Biometric Systems', Security & Privacy, IEEE Computer Society Digital Library, IEEE Computer Society, 99 (2011).*

5 *Fernando Alonso-Fernandez, Julian Fierrez-Aguilar and Javier Ortega-Garcia, 'Sensor Interoperability and Fusion in Signature Verification: A Case Study Using Tablet PC', Advances in Biometric Person Authentication, Lecture Notes in Computer Science, 2005, Vol. 3781/2005, pp 180-187.*

6 *There are serious issues concerning data protection and privacy and how systems protect signature data. To illustrate, a 2002 legal case in Canada involved the standard practice of a courier service that published electronic signatures on its website without the consent of the signers (Stephen Mason, Electronic Signatures in Law (3rd edn, Cambridge University Press, 2012) 353-355).*

*Without an adequate understanding, background and knowledge of the software of the device, the image of the signature provided to an examiner cannot be accurately analyzed*

provide more consistent and discriminating data than others. For example, it was found that speed and angle are more reliable handwriting features. [7]

In reviewing a few of the systems that are offered in the marketplace, it is evident that there is little standardization with respect to the way a signature is recorded. Topaz recommends software and hardware guidelines for the recording of a signature. Part of Topaz's signature recording process includes binding the signature to the document using a secure hash 'which forms a direct cryptographic relationship between the signature and a single document or aggregated data message, and security data.'[8] Topaz also records biodynamic signature measurements in some of its software packages.

SOFTPRO GmbH software examines both static and biodynamic information from signatures including location, pressure, and time signals.[9] WonderNet's Penflow system requires users to enroll into the database by providing a total of six signatures, three of which are for training purposes. Once a user is enrolled into the system, the system continues to collect signatures and increases the size of the database of the measurements that are recorded.[10] Penflow also includes additional security features such as a hash in order to invalidate the signature if the document is altered. Instead of writing a manuscript signature, the Biometric Signature ID software instructs users to sign into the system drawing a password with a mouse. The measurements that are recorded and analyzed include speed, direction, length, height, width, angle, and number of strokes.[11]

Cyber-SIGN affixes biodynamic signatures into PDF documents with the intention that the document and its associated signature cannot be altered without changes being detected. This is an example of a system where affixing the signature into the document is an important process in the act of 'signing'. Signature authentication and verification is achieved through Cyber-SIGN's 'four-dimensional dynamic signature verification algorithm [that] examines the changes in speed, shape, pressure and strokes (including strokes in the air).'[12]

DocuSign, Inc. includes affixing the signature measurements and other security features, but does not record a signature in a way that is a graphic representation of the handwritten signature. The user types in his or her name and can select a cursive-type font style in order to make the name look like a signature when it is affixed or logically associated with the document.[13]

## Standardization

Establishing inter-writer and intra-writer variability has always been an issue of concern in the field of forensic handwriting examination. With the onset of biodynamic electronic signatures, the issue of variability increases due to the numerous software, tablet, and stylus types currently being used to produce signatures. Without an adequate understanding, background and knowledge of the software of the device, the image of the signature provided to an examiner cannot be accurately analyzed. This means that standardization in the methodology of forensic analysis of biodynamic electronic signatures is necessary.

Standardization is a critical issue in terms of handwriting examination as well as in forensic applications in the court. If manufacturers and users of the

7 *Hansheng Lei and Venugopal Govindaraju, 'A comparative study on the consistency of features in on-line signature verification', Pattern Recognition Letters, Volume 26, Issue 15, 2005, 2483-2489.*

8 *Topaz Systems, Inc., available from http://www.topazsystems.com/signaturecapture/guidelines.htm.*

9 *http://www.softpro.de/en/signature-verification/biometric-authentication.aspx.*

10 *WonderNet Ltd at http://www.penflow.com/index.php?option=com_content&task=view&id=36&Itemid=45.*

11 *J C Lads Corporation d/b/a Biometric Signature ID (BSI), at http://www.biosig-id.com/products/.*

12 *Cyber-SIGN (a wholly owned subsidiary of Witswell Consulting and Services, Inc., based in Japan), at http://www.cybersign.com/com/CSIacrobat.html.*

13 *DocuSign, Inc., at http://www.docusign.com/.*

 

technology do not comply with the minimum standards established within the industry, the signature produced by this type of technology could be deemed to be unreliable. Even when manufacturers state that they meet the requirements established by the Electronic Signatures in Global and National Commerce Act[14] or ISO/IEC 27001:2005,[15] these standards or minimum requirements for compliance apply to all forms of electronic signatures and may mean little to the handwriting expert examining a static or biodynamic signature. From a practical standpoint, the level of awareness that the legal system, and even forensic examiners have regarding the minimum standards and procedures required for capturing and authenticating an electronic signature is questionable. This is a critical point, because in establishing procedures for handwriting examiners in evaluating these types of signatures, it may be necessary to first establish whether the signature recording procedure was reliable. In this sense, it may be necessary for legal professionals to consult with both a digital evidence specialist and a document examiner.

## Forensic analysis

It would seem that forensic analysis of electronic signatures would only be necessary in examining important financial documents such as loan transactions. In reality, from a forensic perspective, every signature that is signed may have forensic relevance. A poorly recorded electronic signature taken on a point-of-sale device at a retail store may place a suspect at the scene of a crime. Or a signature recorded on the device of a courier service connected to a package containing illegal materials also has forensic relevance. This means that the corresponding deterioration or complications involved with recording electronic signatures compounds issues involved in forensic handwriting identification both in civil and criminal proceedings.

Most document examination casework involves static analysis of manuscript signatures. The features examined for signatures committed to a piece of paper differ from biodynamic methods of signature, yet information obtained from biodynamic features could help facilitate or validate static observations. For example, characteristics typical of forgery include pen lifts and slow drawn line quality.[16] These can be recorded, measured, and recovered through biodynamic methods. Pen speed is measured, but only guessed at when analyzing manuscript signatures on paper. Biodynamic methods not only enhance, but are superior to analysis of physical signature characteristics because of the temporal information that can be calculated and recorded.

There has been considerable research on the use of biodynamic signatures for identity validation and verification.[17] Some studies have shown that current signature verification systems may have weaknesses that allow for devices to be subject to successful forgery attacks.[18] A comparison of biodynamic and manuscript signature verification system methods showed that the performance between both approaches was small, which is surprising considering how much temporal information can be extracted from biodynamic data.[19]

Review of temporal handwriting feature extraction studies can be used as a starting point in establishing what can be forensically analyzed from biodynamic signature analysis. From a practical perspective, however, many biodynamic electronic signatures encountered in document examination cases are static images rather than the original digital data which means that the best evidence available may not be provided to the document examiner.

## Legal implications

For both document examiners and lawyers, it is important to understand that electronically-captured signatures use processes that materially alter the dynamic movement of handwriting. These differences occur at the beginning of the process (when the purported signer is using the equipment such as a stylus or tablet), as well as the method in which the measurements of the signature are recorded and processed in accordance with the instructions set out in the software. A proper analysis of the signature must not only examine the printed version

14 *(E-SIGN), 15 U.S.C. §§ 7001-7003.*

15 *ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements.*

16 *American Standards for Testing and Materials International, ASTM E2290 - 07a Standard Guide for Examination of Handwritten Items.*

17 *Anil K. Jain, Friederike D. Griess and Scott D. Connell, 'On-line signature verification', Pattern Recognition, Volume 35, Issue 12, 2002, 2963-2972; Alisher Kholmatov and Berrin A. Yanikoglu, 'Identity authentication using improved online signature verification method' Pattern Recognition Letters, Volume 26, Issue 15, 2005, 2400-2408.*

18 *Daniel P. Lopresti and Jarret D. Raim, 'The effectiveness of generative attacks on an online handwriting biometric', in Takeo Kanade, Anil Jain and Nalini K. Ratha, editors, Audio- and Video-Based Biometric Person Authentication, Lecture Notes in Computer Science, Volume 3546 (Berlin: Springer, 2005) 1090-1099; Lucas Ballard, Daniel Lopresti and Fabian Monrose, (2006) 'Evaluating the security of handwriting biometrics', Tenth International Workshop on Frontiers in Handwriting Recognition, http://www.cs.jhu.edu/~lucas/papers/iwfhr.pdf.*

19 *Gerhard Rigoll and Andreas Kosmala, 'A systematic comparison between on-line and off-line methods for signature verification with hidden Markov values', Proceedings of the Fourteenth International Conference on Pattern Recognition, Volume 2, 1998, 1755-1757.*

of the signature measurements, but must include the digital data and software that causes the measurements to be recorded, such as speed and pressure.

One of the potential problems that can occur in the analysis of biodynamic electronic signatures involves the comparison of an electronically-recorded signature with traditional manuscript signatures. Forensic cases involving this type of analysis have begun to occur, and present several problems. First, writing with a stylus on a tablet in a box or onto a computer screen is a different writing environment compared to writing on paper with a pen. Experimental studies have shown significant differences in the way a person writes his or her signature electronically in comparison to writing a manuscript signature. For example, handwriting measurements or characteristics that changed between electronic signing and manuscript signing included the writers, velocity and size.[20] Additionally, a detailed analysis of the form characteristics between the two conditions showed differences. The differences were significant, in that the form details that changed between the signature conditions could be attributed to either an altered writing environment or could be mistakenly attributed to the effect of forgery.

There are many limiting factors to consider when comparing an electronic signature to samples of manuscript signatures. These limiting factors include the differences in writing surface and writing instrument as well as the quality in which the signature was electronically recorded in comparison to manuscript signatures. While some qualified opinions may be possible, unqualified opinions are probably not advisable, and inconclusive opinions are probably the safest approach for these types of comparisons.

For other types of examination, such as the comparison of an electronic signature that is disputed to a set of recorded electronic signature samples, the analysis is dependent upon the sophistication of the biodynamic data captured and available for analysis. Some handwriting verification systems perform an automated analysis of the signature. Others provide biodynamic data that can be independently examined. There are verification systems that advertise varying claims, such as 'forgery proof', which are questionable claims at best, especially given the considerable variables involved in handwriting examination. While proficiency among forensic document examiners in signature examination has been established in the academic literature, not all handwriting variables have been independently tested.[21] Computerized handwriting analysis has also received academic recognition, but again, not all variables have been tested.[22] Certain variables that need further research in the field include health factors, effect of medications, whether a person is left-handed or right-handed, and intentional disguise on the part of the signer, to name a few. It is difficult to imagine that commercially available handwriting verification systems have taken the considerable research time necessary to account for all handwriting variables, let alone the problems inherent in a writer's natural range of variation. For example, if a handwriting verification system recorded a minimum number of base comparison signatures (such as five), this number may not be sufficient for verification, especially since most forensic document examiners require more than five signatures for the purposes of comparison. Additionally, there may be an unintended training effect associated with the collection of signatures for verification in a signature security system. In order to pass the 'test', the person signing may adapt to an unnaturally consistent version of his or her signature. This could have potential implications, because it might assist in the ease of forgery, rather than hindering forgery.

## A recent Daubert ruling

A 2011 *Daubert*[23] ruling in a U.S. district court underscores the need for document examiners to define the best evidence available when handling biodynamic electronic signature cases. In *American Family Life Assurance Company of Columbus (AFLAC) v. Glenda Biles*,[24] the defendant Biles claimed that signatures of the deceased had been forged on an insurance application and arbitration acknowledgement forms. The defendant retained a document examiner expert who was provided with a hard copy of the documents. The plaintiff, AFLAC, retained an expert who was provided with the digital data of the biodynamic electronic signature associated with the disputed documents. Motions to dismiss the affidavits produced by both experts were filed by the respective

20 *Heidi H. Harralson, H.-L. Teulings and L. S. Miller, 'Temporal and spatial differences between online and offline signatures', in Elana Grassi and José L. Contreras-Vidal, editors, Proceedings of the 15th International Graphonomics Society Conference, (2011) 34-37.*

21 *Bryan Found, Doug Rogers and Allan Herkt, 'The skill of a group of document examiners in expressing handwriting and signature authorship and production process opinions', Journal of Forensic Document Examination, Volume 14, 2001, 15-30; M. Kam, K. Gummadidala, G. Fielding and R. Conn, 'Signature authentication by forensic document examiners', Journal of Forensic Sciences, 46, 2001, 884-888.*

22 *Sargur N. Srihari, S.-H. Cha, H. Arora and S. Lee, 'Individuality of handwriting', Journal of Forensic Sciences, Volume 47, Issue 4, 2002, 1-17.*

23 *Daubert v Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993).*

24 *2011 WL 5325622 (S.D.Miss.), also available at http://law.justia.com/cases/federal/district-courts/mississippi/mssdce/3:2010cv00667/73831/80.*

 

parties and a Daubert hearing was conducted of each side's expert. The evidence provided by defendant's expert was deemed to be unreliable by the court.

In the court's memorandum, it was noted that the plaintiff's insurance agent had witnessed the deceased sign the contested signatures on a Topaz electronic signature pad. AFLAC contested that the defendant's expert had relied on a low resolution static image of the disputed signatures that was not an accurate representation of the data recorded. The defendant's expert admitted that he had not realized that he was examining a biodynamic electronic signature initially, nor did he subsequently examine the digital data that was available. The court found that defendant's expert did not rely on the best evidence available, while the document examination expert for AFLAC relied on the digital data of the disputed signatures. The court granted the motion to strike the affidavit of defendant's expert, and granted the plaintiff's motion for summary judgment.

The AFLAC ruling clearly demonstrates that static images of electronic signatures are not considered the best evidence available, and that testimony based on such evidence may be considered unreliable. In the court's memorandum, it was stated that the plaintiff's expert compared the recorded signature data to known exemplars of the deceased's signatures. The court did not mention in its ruling whether these comparison samples were also electronically-recorded signatures. Nor does the court's ruling state the reasons for the defendant's motion to dismiss the plaintiff expert's affidavit. The court was justified in its finding that plaintiff's expert relied on the best evidence available. However, if the plaintiff's expert was comparing biodynamic electronic signatures to manuscript signatures, the question remains whether the best evidence available was forensically reliable evidence to make claims regarding authenticity.

## Recommendations

Clearly, the challenges faced by documents examiners concerning biodynamic signatures require collaboration with computer forensics. The problems involved in the forensic analysis of biodynamic electronic signatures highlights the need to work within a framework such as computational forensics. Computational forensics is the application of a methodology to help quantify and standardize forensic analysis.[25] Other standardized guidelines for forensic collection and analysis of electronic evidence are outlined by Mason.[26] These types of guidelines would be useful for forensic document examiners to incorporate when handling electronic evidence in biodynamic electronic signature cases.

Further, forensic document examiner research in conjunction with computer forensics is necessary to more clearly define thresholds related to minimum levels of forensically reliable data. In working with biodynamic electronic signature technology, forensic document examiners need more than access to the best evidence available; they also need an understanding concerning the limitations of signatures captured with too little information.



**Heidi H. Harralson** MA, CDE, D-BFDE is a court-qualified, board-certified forensic document examiner maintaining a document examination practice in the US. Her research on document and handwriting examination, including electronic signatures, has been published in books and journal articles. She is an associate professor at East Tennessee State University where she teaches forensic document examination.

**harralson@spectrumforensic.com**

25 *Katrin Franke and Sargur N. Srihari, 'Computational forensics: Towards hybrid-intelligent crime investigation', Third International Symposium on Information Assurance and Security, (IEEE Computer Society, 2007), 383–386; Sargur N. Srihari, 'Beyond C.S.I.: The Rise of Computational Forensics', IEEE Spectrum, December 2010, December, 38-43, available on-line at http://spectrum.ieee.org/computing/software/beyond-csi-the-rise-of-computational-forensics/o.*

26 *Stephen Mason, general editor, Electronic Evidence (2nd edn, LexisNexis Butterworths, 2010), chapter 4.*