# Digital Evidence: Disclosure and Admissibility in the United Kingdom Jurisdiction

Reza Montasari(✉)

Department of Computing and Mathematics, University of Derby, Derby, UK
r.montasari@derby.ac.uk

**Abstract.** Digital forensics, originally known as computer forensics, first presented itself in the 1970s. During the first investigations, financial fraud proved to be the most common cause on suspects' computers. Since then, digital forensics has grown in importance in situations where digital devices are used in the commission of a crime. The original focus of digital forensic investigations was on crimes committed through computers. However, over the past few years, the field has extended to include various other digital devices in which digitally stored information can be processed and used for different types of crimes. This paper explores how the admissibility of digital evidence is governed within the United Kingdom jurisdictions.

**Keywords:** Digital forensics · Digital evidence · Admissibility · Disclosure · Digital investigation · U.K. jurisdiction

## 1 Introduction

Digital forensics, originally known as computer forensics, first presented itself in the 1970s [1]. During the first investigations, financial fraud proved to be the most common cause on suspects' computers [2]. Since then, digital forensics has grown in importance in situations where digital devices are used in the commission of a crime [3]. The original focus of digital forensic investigations was on crimes committed through computers [4]. However, over the past few years, the field has extended to include various other digital devices in which digitally stored information can be processed and used for different types of crimes [5]. Palmer defines digital forensics as,

> *The use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorised actions shown to be disruptive to planned operations [6].*

This definition is widely accepted within the digital forensic community [2, 4, 7, 8] and is therefore adopted within this paper. A digital forensic investigation (DFI) is the process of linking extracted information and digital evidence in order to establish factual information for review by the judiciary [4, 9]. Cohen [10] highlights the need to establish factual information as the outcome of such an investigation. A DFI is carried out as an investigation after the occurrence of an incident [11, 12]. It is therefore a


H. Jahankhani et al. (Eds.): ICGS3 2017, CCIS 630, pp. 42–52, 2016.
DOI: 10.1007/978-3-319-51064-4_4

distinct type of investigation "where the scientific procedures and techniques used will allow the results, in other words digital evidence, to be admissible in a court of law" [13]. Due to the fact that digital evidence is contained in a digital device and cannot be observed by the naked eye, forensic tools such as Encase [14] and FTK [15] are used to extract and examine data representing potential digital evidence. The extent of the value of the digital evidence is based not only on the extent to which a tool is trusted [16, 17], but also on the competence and experience of the investigator carrying out the digital investigation [18, 19].

There are four basic principles of DFIs which must be considered. These are auditability, repeatability, reproducibility and justifiability. Auditability refers to the need for an independent investigator to be able to evaluate the activities performed by other investigators to determine whether or not a suitable scientific method was followed [20]. Repeatability requires one investigator to be able to arrive at the same conclusion as another under similar conditions [8, 21]. Reproducibility is established when the same test results are produced using the same method, but with different instruments and under different conditions, and can be reproduced at any time after the original test [18]. Justifiability refers to an investigator being able to justify all the actions and methods they used during the course of a digital investigation [18]. A DFI is often initiated in order to ascertain certain facts after an incident has occurred. It must be conducted in such a methodical manner that it can withstand scrutiny by the court and defence team [4]. There exist various types of DFIs, including live forensics, static forensics, proactive forensics and cloud forensics [22, 23]. The fundamental point of any DFI is to answer 'what', 'why', 'how', 'who', 'where' and 'when' type questions in relation to the data analysis and evidence in order to confirm or refute allegations of suspicious activity [9, 24]. 'What' refers to the data attributes or metadata, 'why,' the motivation [25], 'how,' the manner in which the incident was initiated or the way in which the necessary evidence was isolated [23], 'who,' the people involved [26], 'where,' the location of the potential digital evidence [4] and 'when,' the time of occurrence [27].

The remainder of this paper focuses only on the question of "how", which must be addressed by the steps of the investigative process undertaken to acquire digital evidence in a forensically sound manner.

## 2 Background to Digital Evidence

Nowadays, almost all transactions from the commercial world, government and private individuals exist only in digital form [4, 28, 29]. In such cases it is only through digital evidence that one can demonstrate that something did or did not happen [22, 30]. Digital footprints of individuals' activities are left in the digital world, from which their actions and intentions can be deduced [29]. Digital evidence is the product of the digital forensics process [10, 30, 31] and can be extracted from various sources, including digital devices (such as desktop and laptop computers, thumb drives, mobile devices, digital cameras and tablets), network servers (such as supporting applications including Web sites, e-mail and social networks) and network hardware (such as routers) [4, 32, 33]. "Forensics" refers to the application of scientific evidence in courts of law, where

judges play a vital role as gatekeepers in deciding what evidence is and is not admissible [10, 30, 31, 34, 35]. Authors in [4, 6] argue that while the actual mechanics of digital forensics are different from the better-known physical and medical forensics, the processes of all forensic sciences are fundamentally the same. Each phase in the process must be performed in such a way that the integrity of the evidence is preserved and its admissibility assured. Digital evidence can be employed in many types of criminal investigations, such as homicide, sex offences, missing persons, child abuse, drugs, fraud and theft of personal information [4]. Digital evidence can show how a crime was perpetrated, provide investigative leads, prove or refute witness statements and identify potential suspects. Various similar definitions of digital evidence have been proposed in the literature [12, 36, 37]. However, for the purposes of this paper, the following definition given by Casey [4], which is widely accepted within the digital forensic community, is used:

> *any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi.*

The term "computer" in the above definition can be replaced with 'digital device' to cover various types of devices, such as computers, laptop computers, tablets and smart mobile devices. Data in Casey's [4] definition of digital evidence essentially refers to numbers that represent information of various types such as text, images, audio and video. A simple computer file can contain incriminating information and have corresponding properties that are useful in an investigation. For instance, details such as when a file was created, who may have created it, or that it was created on another computer, can all be essential. Notwithstanding its pervasiveness, few people are well-acquainted with the evidential, technical and legal issues associated with digital evidence. Consequently, digital evidence is often disregarded, acquired incorrectly or examined and analysed ineffectively. Digital evidence is often challenged in court because of the ease with which it can be altered, which is due to poor handling. The manner in which searches of digital evidence are authorised and carried out, the way in which it is handled, received and rejected, and the various legal issues associated with digital evidence, all differ from one jurisdiction to another. The topic of digital evidence explored in this paper focuses on the United Kingdom jurisdiction, occasionally incorporating the United States jurisdiction for the purposes of comparison.

## 3 Background to Digital Evidence

Digital evidence is increasing in both size and significance in criminal and civil trials [4, 10, 30–32, 38–40]. It is latent in the same way as a fingerprint or DNA sample [19]. However, digital evidence is more complex and volatile as it can be accidently or improperly modified, damaged or destroyed during the investigative process [41–45]. Due to its fragility, courts pay close attention to the process in which the digital evidence was acquired and stored [30]. Investigators' methods in carrying out digital investigations are often scrutinised by the courts [7, 46]. Therefore, to be admissible in court, digital evidence must have all the characteristics of other types of scientific and technical evidence and fulfil the standards associated with them [4, 30]. However,

electronic-based evidence presents far greater challenges, both for the courts and in relation to the procedures [29, 30]. The manner in which it is extracted plays a significant role in weighing the probative and prejudicial value of the evidence when presented in court [10, 31, 35, 47]. To withstand the stringent admissibility requirements, the evidence produced by law enforcement agencies must be robust. Evidence presented in court can be "real", "documentary", "technical", "expert" and "derived" and must satisfy two criteria of "admissibility" and "weight" [29]. To be admissible, it must fulfil legal acceptability tests. This is a function of jurisdiction which derives from English common law rather than European civil codes. The following three sections discuss the practices carried out by courts in relation to the admissibility of digital evidence. Emphasis is placed on the U.K. courts, but comparisons are also made with the U.S. jurisdiction.

### 3.1 Challenges Facing Judiciary

Judges play a vital role in protecting the legal system from the impacts of flawed evidence [10]. Just as judges need to remove "junk science" from the courtroom, so they need to keep out poor-quality digital evidence [10, 31]. They play the role of gatekeeper, determining what evidence is and is not admissible in their courtrooms [10, 30, 31, 34, 35]. Judges weigh the evidentiary value against the prejudicial effect of any evidence produced [10, 31]. However, their role has various subtleties and complications. One of the greatest challenges facing both judges and juries (lay audiences) is their lack of proper understanding of digital technology. Kessler [30] states that for a judge to be able to fairly assess the merits of digital evidence, they need to have some understanding of basic ICTs and the applications from which digital evidence is extracted [30]. Other researchers have raised this issue, arguing that a lack of familiarity with digital technology and the subsequent detrimental effect on court cases might indicate the necessity for "new laws of evidence" or "specialist judges" [5, 48].

As there has been no such initiative to date, such a lack of appreciation could prevent judges from critically assessing the evidence submitted to them [49]. There is currently no study in the literature in relation to judges' perceived knowledge of digital evidence within the U.K. jurisdiction [30, 49–51]. This must be considered an imperative subject area for future research. Technical terms have also proved challenging for judges and juries. For instance, the forensic copy of an evidentiary medium was previously called a "mirror image" [52]. Whilst researchers in the field of computer science understand this terminology, it has been misinterpreted by "lay audiences" to denote a reverse copy, as mirrors reflect an opposite image [30, 32]. To remove such confusion, the process is now called a bit-by-bit forensic copy [4].

### 3.2 United States Jurisdiction

As with any evidence, the proponent of digital evidence has to lay an appropriate foundation in relation to its reliability [53]. Various practices are carried out across different jurisdictions in terms of laying such a proper foundation. In the United States,

the admission in a federal court of scientific evidence (including digital evidence) is governed by the Federal Rules of Evidence (FRE) [29, 54]. These rules require the trial judge to act as a gatekeeper, determining, prior to its admission, whether the evidence is scientifically valid and relevant to the case [30]. Across the U.S. federal courts, judges employ the Daubert Test [55] in order to determine the admissibility of the scientific or technical evidence. The Daubert Test includes the following five assessments [55]:

(1) whether the theory or technique in question can be and has been tested;
(2) whether it has been subjected to peer review and publication;
(3) its known or potential error rate;
(4) the existence and maintenance of standards controlling its operation; and
(5) whether it has attracted widespread acceptance within a relevant scientific community.

Using the Daubert Test, a judge can objectively determine the reliability of any digital evidence presented in the courts. The Kumho Tire v. Carmichael [56] decision extended the Daubert guidelines to any form of technical evidence. In addition, FRE Rule 702 provides guidelines for qualifying expert witnesses and minimizing adversarial bias in expert testimony [54]. The Rule 702 requirement for reliability may work against its design to balance "the imperatives of maintaining an adversarial system and mitigating bias" [30]. In particular, Rule 702 can be employed to prevent the admission of an expert's assumptions, which a judge might otherwise find useful, as assumptions cannot be considered to be reliable [57]. In conclusion, the Daubert Test and Rule 702 are employed in the U.S. courts to determine the admissibility of digital evidence as well as any other types of scientific and technical evidence [30, 58–60].

### 3.3 United States Jurisdiction

In the United Kingdom, judges can exercise their discretion within the boundaries of U.K. law (discussed in this section) to dismiss evidence that has been acquired unfairly. In many cases, digital evidence is ruled inadmissible in the U.K. courts if it has not met certain conditions (also discussed in this section). The concept of admissibility requires courts to establish whether evidence is "safe" to place before a jury and whether it will provide a solid foundation for arriving at a decision in the case. In practice, admissibility amounts to a set of legal tests performed by a judge to evaluate an item of evidence [4]. This evaluation process can be complex, especially when evidence has not been handled properly or has characteristics that make it less reliable or more prejudicial. In the U.K. legal system, "admissibility" refers to legal rules that are applied to an item of potential evidence prior to a court considering the value of the fact that it claims to offer [29]. There exist various laws and rules that govern the admissibility of digital evidence in U.K. courts.

The most important laws associated with the admissibility of digital evidence are the Criminal Justice Act 2003 [61], the Regulation of Investigatory Powers Act 2000 [62], the Computer Misuse Act 1990 [63] and the Police and Criminal Evidence Act 1984 [64]. For instance, section 117 of the Criminal Justice Act 2003 [61] regulates the

admissibility of communication data that has been obtained under warrant. Under section 17 of the Regulation of Investigatory Powers Act 2000 [62] content is not admissible. However, it will become admissible if it has been acquired from a foreign law enforcement agency within its own jurisdiction and is available to an investigator to be presented in the U.K. court [29]. Another example is section 78 of the Police and Criminal Evidence Act 1984 [64], according to which intercepted data content can only be used for intelligence purposes; it cannot be admitted as evidence. Also relevant to the issue of the admissibility of digital evidence is whether the material is a "business record," as outlined under section 117 of the Criminal Justice Act 2003 [61], an "expert report," defined under section 118(8) and 127 of that Act, or "real evidence". Importantly, under section 78 of the Police and Criminal Evidence Act 1984 [64], courts can reject any evidence deemed to have been acquired unfairly.

Compared with the U.K. legal system, admissibility rules in other European counties are much more relaxed and, although admissibility rules in the United States follow the English common law model, they have evolved differently. For instance, authorisations to seize evidence in the U.S. must be drawn up with far greater precision than in the U.K. [29] and any material acquired outside the warrant is likely to be considered inadmissible. Another deviation relates to the way in which technical evidence is handled. Within the U.K. courts, the jury is simply provided with opposing expert witnesses, while in the United States, technical evidence is an admissibility issue with the judge acting as a gatekeeper to protect the jury from scientific evidence which has not been established as "generally accepted" [55].

U.K. judges often consider three issues before deciding whether or not to admit digital evidence. These can be classified as issues relating to search warrants, reliability and best evidence.

(1) **Search Warrants**

Acquiring digital evidence under "proper authorisation" is vital for its admission in the U.K. legal system. Investigators must obtain a search warrant or subpoena before they can search, seize or examine digital devices. Subpoenas are employed to seize a company's business records, while search warrants are needed to access more detailed information such as customer-owned files [4]. For instance, in circumstances involving an Internet Service Provider (ISP), a subpoena might be required to identify the name of an individual owning a specific e-mail account and a search warrant used to extract the contents of e-mail or user profiles [35]. As already stated, digital evidence acquired without authorisation will not be admitted in courts. In order to acquire the necessary warrant, investigators must demonstrate to a judge that a crime has been committed, evidence of the crime exists and the evidence is likely to exist at the place to be searched. Search warrants in the United Kingdom can be more loosely defined than in the United States. In the U.K. legal system, there are several types of warrants such as a "specific premises warrants", all-premises warrants" and "multiple entry warrants" [4]. Even when investigators have obtained authorisation to search a computer, they must focus only on the crime under investigation. If they identify evidence of other crimes during their investigation, that evidence will not be admissible as it is outside the scope of the warrant. In such circumstances,

investigators would have to obtain a second warrant before being able to use evidence to charge the offender [4, 29].

Furthermore, investigators may need to acquire two separate warrants for a seized computer: one for the computer itself and one for the files contained in it. Seized computers usually constitute 'real' evidence for admissibility purposes, with individual files having to be admitted separately in accordance with section 117 of Criminal Justice Act 2003 [61]. This is of particular importance where more than one individual has had access to a computer. In such situations, in order to adhere to Computer Misuse Act 1990 [63], investigators must prove that they are authorised to access the computers.

(2) **Best Evidence**

The "best evidence" rule refers to a legal principle that an original copy of a document is superior evidence. In the past, based upon this rule, secondary evidence such as a copy or "facsimile" would not be admissible if an original document was in existence and could be acquired [68]. The original purpose of the rule was to ensure that decisions reached in courts were based on the best available information [4]. However, with the arrival of photocopiers, scanners, computers and other technology that can produce effectively identical replicas, duplicates became acceptable instead of the original. According to Blackstone's Criminal Practice [68], the best evidence rule in England and Wales is now all but defunct. Therefore, evidence that is not an original will be admitted provided it meets other admissibility requirements. If a question is raised in relation to the authenticity of the original or the accuracy of the copy, or if the circumstances dictate that it would be unfair to admit the copy in place of the original, the best evidence rule will still apply. As most forms of digital evidence can be duplicated exactly, this issue does not often arise and copies are usually admitted in the U.K. courts. In fact, producing a duplicate of digital evidence is often preferred as it removes the possibility of the original being accidently modified.

According to the "Hearsay Rule", digital evidence would not be admissible if the witness (the digital forensic analyst) was not present in court to verify its truthfulness. Under section 114(1) of the Criminal Justice Act 2003 [61], "hearsay" in criminal proceedings is "a statement not made in oral evidence in the proceedings that is evidence of any matter stated." There are exceptions for evidence that describes events accurately and is simpler to authenticate, but the discussion of these is outside the scope of this research.

## 4 Concluding Remarks

Digital evidence has been presented in a growing number of criminal and civil court cases over the last decade. In order to be admissible in courts of law, digital evidence needs to meet the standards of other scientific and technical evidence. The lay audience (judges and jury) decide cases based on their understanding of evidence that is presented at trial. Knowledge of ICTs because of everyday use of computers, smart mobile devices, and other digital devices and network services might be understood by the lay

audience as interpreting how digital evidence is extracted from digital sources. A knowledge of how digital evidence is acquired determines the way in which judges and jury weigh the probative and prejudicial value of this evidence when presented in court. In order to assess the value of digital evidence fairly and impartially, judges and jury will need to have some understanding of the fundamental ICTs and applications from which digital evidence is extracted such as computers, the Internet and e-mail. However, there is no study in the literature revealing the judges' perceived knowledge of digital evidence. Thus, investigating judges' perceived knowledge of digital evidence within the U.K. jurisdiction must be considered an imperative subject area for future research.

## References


1. Pollitt, M.: A history of digital forensics. In: Chow, K.-P., Shenoi, S. (eds.) DigitalForensics 2010. IAICT, vol. 337, pp. 3–15. Springer, Heidelberg (2010). doi:10.1007/978-3-642-15506-2_1
2. Kohn, M., Eloff, M., Eloff, J.: Integrated digital forensic process model. Comput. Secur. **38**, 103–115 (2013)
3. Garfinkel, S.: Digital forensics research: the next 10 years. Digit. Invest. **7**, 64–73 (2010)
4. Casey, E.: Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 3rd edn. Elsevier Academic Press, New York (2011)
5. Nance, K., Hay, B., Bishop, M.: Digital forensics: defining a research agenda. In: 42nd Hawaii International Conference on System Sciences, pp. 1–6 (2009)
6. Palmer, G.: A road map for digital forensic research. In: 1st Digital Forensic Research Workshop (DFRWS), pp. 27–30 (2001)
7. Montasari, R., Peltola, P., Evans, D.: Integrated computer forensics investigation process model (ICFIPM) for computer crime investigations. In: Jahankhani, H., Carlile, A., Akhgar, B., Taal, A., Hessami, A.G., Hosseinian-Far, A. (eds.) ICGS3 2015. CCIS, vol. 534, pp. 83–95. Springer, Heidelberg (2015). doi:10.1007/978-3-319-23276-8_8
8. Valjarevic, A., Venter, H.: A comprehensive and harmonized digital forensic investigation process model. J. Forensic Sci. **60**(6), 1467–1483 (2015)
9. Ieong, R.: FORZA - digital forensics investigation framework that incorporate legal issues. Digit. Invest. **3**, 29–36 (2006)
10. Cohen, F.: Toward a science of digital forensic evidence examination. In: Chow, K.-P., Shenoi, S. (eds.) DigitalForensics 2010. IAICT, vol. 337, pp. 17–35. Springer, Heidelberg (2010). doi:10.1007/978-3-642-15506-2_2
11. Freiling, C., Schwittay, B.: A common process model for incident response and computer forensics. In: 3rd International Conference on IT-Incident Management and IT-Forensics, pp. 19–40 (2007)
12. Rowlingson, R.: A ten step process for forensic readiness. Int. J. Digit. Evid. **2**(3), 1–28 (2004)
13. Agarwal, A., Gupta, M., Gupta, S., Gupta, C.: Systematic digital forensic investigation model. Int. J. Comput. Sci. Secur. **5**(1), 118–130 (2011)
14. Guidance Software: EnCase Forensics (2016). https://www.guidancesoftware.com/encase-forensic. Accessed 11 June 2016
15. AccessData: Forensic Toolkit (FTK) (2016). http://accessdata.com/products/computer-forensics/ftk. Accessed 09 June 2016

16. Wojcik, M., Venter, H., Eloff, J., Olivier, M.: Applying machine trust models to forensic investigations. In: Olivier, M.S., Shenoi, S. (eds.) Digital Forensics 2006. IAIC, vol. 222, pp. 55–65. Springer, Heidelberg (2006). doi:10.1007/0-387-36891-4_5
17. Ciardhuáin, O.: An extended model of cybercrime investigations. Int. J. Digit. Evid. **3**(1), 1–22 (2004)
18. SO/IEC: ISO/IEC 27037: Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence. British Standards Institution, London (2012)
19. ACPO: ACPO Good Practice Guide for Digital Evidence. U.K. Association of Chief Police Officers (2012)
20. ISO/IEC: ISO/IEC 27043: Incident Investigation Principles and Processes. British Standards Institution, London (2015)
21. Solms, S., Louwrens, C., Reekie, C., Grobler, T.: A control framework for digital forensics. In: Olivier, M., Shenoi, S. (eds.) DigitalForensics 2006. IAIC, vol. 222, pp. 343–355. Springer, Heidelberg (2006). doi:10.1007/0-387-36891-4_27
22. Rogers, M., Goldman, J., Mislan, R., Wedge, T., Debrota, S.: Computer forensics field triage process model. In: Conference on Digital Forensics, Security and Law, pp. 27–40 (2006)
23. Beebe, N., Clark, J.: A hierarchical, objectives-based framework for the digital investigations process. Digit. Invest. **2**(2), 147–167 (2005)
24. Kruse, W., Heiser, J.: Computer Forensics: Incident Response Essentials. Addison-Wesley, Boston (2001)
25. Grobler, C.P., Louwrens, C.P., Solms, S.H.: A multi-component view of digital forensics. In: ARES 2010 International Conference on Availability, Reliability and Security, pp. 647–652 (2010)
26. Carrier, B., Spafford, E.: Getting physical with the digital investigation process. Int. J. Digit. Evid. **2**(2), 1–20 (2003)
27. Mandia, K., Prosise, C., Pepe, M.: Incident Response and Computer Forensics, 2nd edn. McGraw-Hill/Osborne, Emeryville (2003)
28. Cohen, F.: Update on the state of the science of digital evidence examination. In: Proceedings of the Conference on Digital Forensics, Security, and Law, pp. 7–18 (2012)
29. Sommer, P.: Directors' and corporate advisors' guide to digital investigations and evidence. U.K. Information Assurance Advisory Council (2008). https://www.ucisa.ac.uk/~/media/Files/members/activities/ist/DigitalInvestigationsGuide.ashx. Accessed 17 June 2016
30. Kessler, C.: Judges' awareness, understanding, and application of digital evidence. Ph.D. thesis, Nova Southeastern University (2010)
31. Cohen, F.: Digital Forensic Evidence Examination, 2nd edn. Fred Cohen & Associates, Livermore (2009)
32. Brown, C.: Computer Evidence: Collection and Preservation, 2nd edn. Course Technology, Boston (2009)
33. Gonzales, A., Schofield, R., Hagy, D.: Digital evidence in the courtroom: a guide for law enforcement and prosecutors. U.S. Department of Justice (2007). https://www.ncjrs.gov/pdffiles1/nij/211314.pdf. Accessed 17 June 2016
34. Jones, A.: Computer science and the reference manual for scientific evidence: defining the judge's role as a firewall. Intellect. Prop. Law Bull. **14**(1), 23–40 (2009)
35. Kerr, O.: Computer Crime Law, 2nd edn. Thomson/West, St. Paul (2009)
36. Mason, S.: Electronic Evidence: Disclosure, Discovery and Admissibility. LexisNexis Butterworths, London (2007)
37. Whitcomb, C.: An historical perspective of digital evidence: a forensic scientist's view. Int. J. Digit. Evid. **1**(1), 1–9 (2002)
38. Kerr, O.S.: Fourth amendment seizures of computer data. Yale Law J. **119**(4), 700–724 (2010)

39. Ball, C.: What judges should know about computer forensics. National Workshop for District Judges II, pp. 1–19 (2008)
40. Manes, G., Downing, E., Watson, L., Thrutchley, C.: New federal rules and digital evidence. In: Conference on Digital Forensics, Security and Law, pp. 31–40 (2007)
41. Giova, G.: Improving chain of custody in forensic investigation of electronic digital systems. Int. J. Comput. Sci. Netw. Secur. **11**(1), 1–9 (2011)
42. Holder, E., Robinson, L., Rose, K.: Electronic crime scene investigation: an on-the-scene reference for first responders. U.S. Department of Justice (2009). https://www.ncjrs.gov/pdffiles1/nij/227050.pdf. Accessed: 11 June 2016
43. Mukasey, M., Sedgwick, J., Hagy, D.: Electronic crime scene investigation: a guide for first responders. U.S. Department of Justice (2008). https://www.ncjrs.gov/pdffiles1/nij/219941.pdf. Accessed 10 June 2016
44. Bem, D., Feld, F., Huebner, E., Bem, O.: Computer forensics - past, present and future. J. Inf. Sci. Technol. **5**(3), 43–59 (2008)
45. Ashcroft, J., Daniels, D., Hart, S.: Forensic examination of digital evidence: a guide for law enforcement. U.S. Department of Justice (2004). https://www.ncjrs.gov/pdffiles1/nij/199408.pdf. Accessed 10 June 2016
46. Rogers, M.: DCSA: A Practical Approach to Digital Crime Scene Analysis, vol. 3, 5th edn. Purdue University, West Lafayette (2004)
47. Frowen, A.: Computer forensics in the courtroom: is an IT literate judge and jury necessary for a fair trial? (2009). http://realestatearticles4u.com/computer-forensics-in-the-courtroom-is-an-it-literate-judge-and-jury-necessary-for-a-fair-trial/. Accessed: 17 June 2016
48. Shaw, B.: Judging juries: evaluating renewed proposals for specialized juries from a public choice perspective. UCLA J. Law Technol. **10**(2), 3–4 (2006)
49. Losavio, M., Wilson, D., Elmaghraby, A.: Prevalence, use, and evidentiary issues of digital evidence of cellular telephone consumer and small-scale digital devices. J. Digit. Forensic Pract. **1**(4), 291–296 (2006)
50. Scarborough, E., Rogers, M., Frakes, K., San Martin, C.: Digital evidence. In: Crimes of the Internet, pp. 477–488 (2009)
51. Rogers, M., Scarborough, K., Frakes, K., San Martin, C.: Survey of law enforcement perceptions regarding digital evidence. In: Craiger, P., Shenoi, S. (eds.) DigitalForensics 2007. ITIFIP, vol. 242, pp. 41–52. Springer, Heidelberg (2007). doi:10.1007/978-0-387-73742-3_3
52. Garber, L.: Computer forensics: high-tech law enforcement. IEEE Comput. Mag. **34**(1), 22–27 (2001)
53. Ryan, D., Shpantzer, G.: Legal aspects of digital forensics. In: Proceedings of Forensics Workshop, pp. 1–7 (2002)
54. U.S. Courts: Federal rules of evidence. Administrative Office of the U.S. Courts (2015). http://federalevidence.com/rules-of-evidence. Accessed 21 June 2016
55. Daubert v. Merrell Dow Pharmaceuticals, Inc. (92-102), 509 U.S. 579 (1993)
56. Kumho Tire v. Carmichael (97-1709), 526 U.S. 137, 131 F.3d 1433 reversed (1999)
57. Bernstein, D.: Expert witnesses, adversarial bias, and the (partial) failure of the Daubert revolution. George Mason Univ. Law Econ. Res. Pap. **93**(451), 100–137 (2008)
58. Rothstein, B., Hedges, R., Wiggins, E.: Managing discovery of electronic information: a pocket guide for judges (2007). https://bulk.resource.org/courts.gov/fjc/eldscpkt.pdf. Accessed 21 June 2016
59. Meyers, M., Rogers, M.: Digital forensics: meeting the challenges of scientific evidence. In: Pollitt, M., Shenoi, S. (eds.) DigitalForensics 2005. ITIFIP, vol. 194, pp. 43–50. Springer, Heidelberg (2006). doi:10.1007/0-387-31163-7_4

60. Noblett, M., Pollitt, M., Presley, L.: Recovering and examining computer forensic evidence. Forensic Sci. Commun. **2**(4), 1–13 (2000)
61. Criminal Justice Act 2003. Chapter 44. The Stationary Office, London
62. Regulation of Investigatory Powers Act 2003. Chapter 23. The Stationary Office, London
63. Computer Misuse Act 1990. Chapter 18. The Stationary Office, London
64. Police and Criminal Evidence Act 1984. Chapter 60. The Stationary Office, London
65. Adams, R.: The advanced data acquisition model (ADAM): a process model for digital forensic practice. Ph.D. thesis, Murdoch University (2012)
66. Steel, C.: Windows Forensics: The Field Guide For Conducting Corporate Computer Investigations. Wiley Publishing, Indianapolis (2006)
67. Buskirk, E., Liu, V.: Digital evidence: challenging the presumption of reliability. J. Digit. Forensic Pract. **1**(1), 19–26 (2006)
68. Ormerod, D., Perry, D.: Blackstone's Criminal Practice, 26th edn. Oxford University Press, Oxford (2015)