2

Standards and Best Practices in Digital and Multimedia Forensics

Shujun Li[1], Mandeep K. Dhami[2] and Anthony T.S. Ho[1]
[1]*Department of Computing and Surrey Centre for Cyber Security (SCCS), University of Surrey, Guildford, UK*
[2]*Department of Psychology, Middlesex University, London, UK*

2.1 Introduction

One of the main goals of digital forensics is to produce digital evidence admissible to the court, which requires that the digital forensic process or techniques used are not flawed in such a way that the evidence or intelligence generated can be questioned. This requirement is normally described as 'forensic soundness' (Casey 2007; McKemmish 2008). While the exact meaning of forensic soundness depends on the underlying jurisdiction and forensic techniques involved, there are established standard procedures and best practices around how digital forensic examinations should be conducted and managed to ensure forensic soundness for every step of the chain of custody.

This chapter provides a comprehensive review of important international, regional and national standards relevant to digital forensics and electronic evidence in general, as well as many best practice guides produced by different bodies. Some standards and best practice guides are not directly related to digital forensics; however, they are still important to digital forensics laboratories and law enforcement agencies because they define formal management procedures that help guarantee soundness of forensic examinations conducted. In addition, this chapter also covers standards and best practice guides on training and education in the digital forensics sector, with some training and certification programs which are well recognized among forensic practitioners.

Handbook of Digital Forensics of Multimedia Data and Devices, First Edition.
Edited by Anthony T.S. Ho and Shujun Li.

Companion Website: www.wiley.com/go/digitalforensics

Most standards and best practice guides covered in this chapter are about digital forensics in general, but they can be applied to multimedia forensics as well since they often define steps of the general procedure rather than how a specific technique should be used in practice. There are also standards and best practice guides dedicated to digital forensics of multimedia data and devices, many of which are focused on a specific type of multimedia data or devices. We however do not cover standards and best practice guides falling more into traditional forensic sciences, such as those on fingerprint and facial image recognition systems and processes.[1]

It deserves mentioning that this chapter should not be considered as a complete list of all standards and best practice guides in digital and multimedia forensics fields, due to the fact that a large number of nations and regional/international bodies have their own standards and best practice guides. Therefore, the main areas that this chapter focuses on are a number of important regional/international bodies and representative nations such as the United States, the United Kingdom and the European Union. We plan to cover more regional/international bodies and nations on the website and future editions of this book.

The rest of this chapter is organized as follows. In the next section we will give an overview of most important standards and best practice guides covered in this chapter, in order to show a big picture of what has been happening in this space since the early 1990s when electronic evidence started becoming an important area for law enforcement and forensic practitioners to look at seriously. This section will give a complete list of all standards and best practice guides covered in this chapter. After the overview a number of sections are dedicated to different groups of standards and best practice guides according to their contents: Section 2.3 covers electronic evidence and digital forensics in general, Section 2.4 focuses on multimedia evidence and multimedia forensics, Section 2.5 looks at digital forensics laboratory accreditation, Section 2.6 focuses on general quality assurance (management) procedures important for digital forensics laboratories and finally Section 2.7 covers training, education and certification. The last section concludes this chapter with a summary of existing standards and best practices and also future trends.

2.2 Overview

Figure 2.1 provides a diagrammatic representation of the historical development of selected standards and best practice guides for digital forensics. It also illustrates how those standards and best practice guides are related to each other.[2] Largely speaking,

[1] Note that those systems are highly digitized as well, but we consider them less relevant for the context of digital forensics and electronic evidence due to their closer link to physical means of conducting forensic analysis and preserving the evidence.

[2] Only major dependencies among standards and best practice guides are shown to enhance readability of the diagram. It is not uncommon for one standard or best practice guide to refer to many other ones.

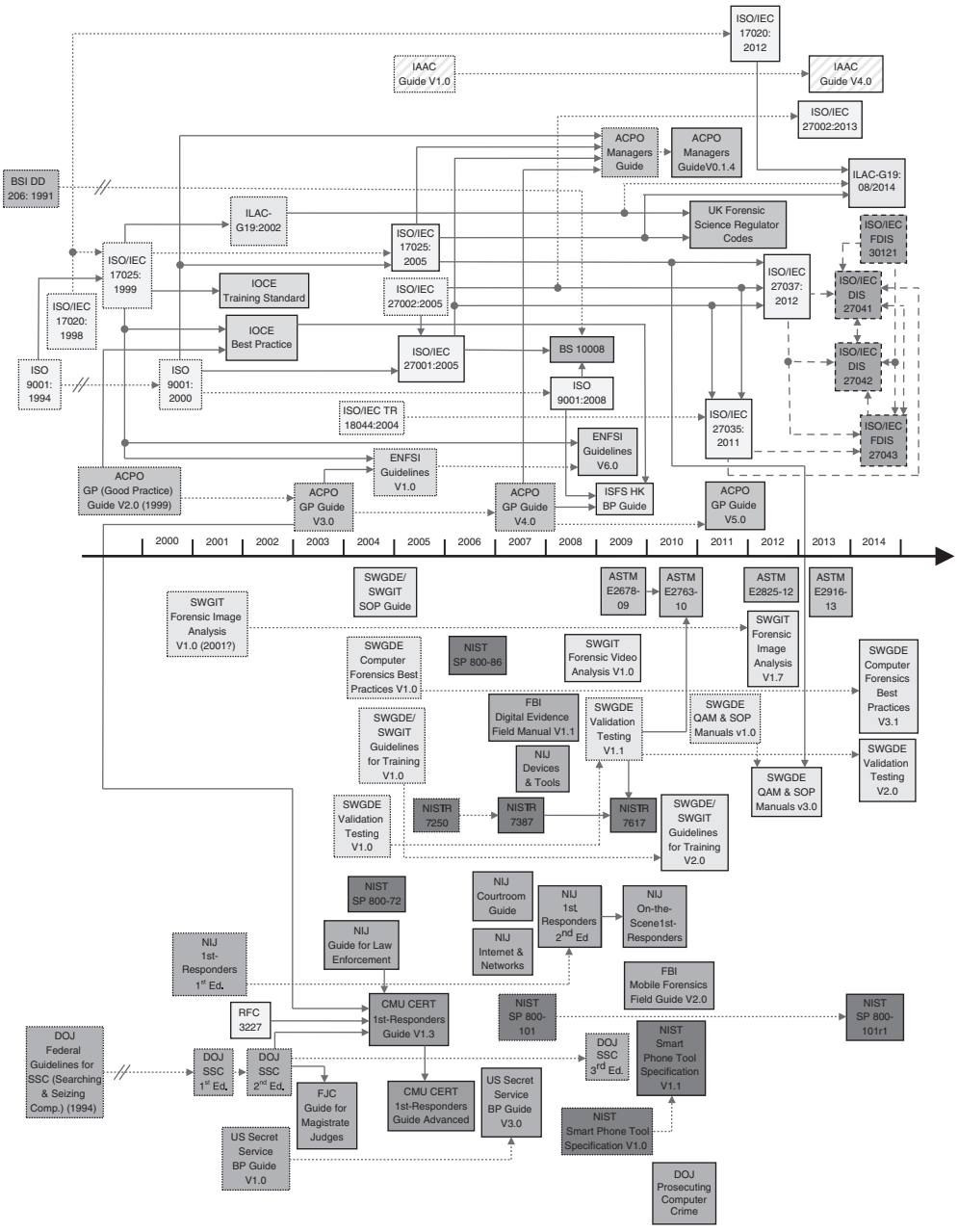

Figure 2.1 Time line and relationships of selected standards and best practice documents on digital forensics. Dotted boxes denote superseded early editions and dotted lines link these with their latest editions. The dashed boxes denote four ISO standards to be published. The Information Assurance Advisory Council (IAAC) forensic-readiness guide refers to many standards and best practice guides, so the links are omitted.

there are two subsets of standards and best practice guides: those with a closer link with ISO standards (above the time axis), and those without a link or with a very loose link with ISO standards (below the time axis). The first subset is more about quality assurance and the second is more about technical/legal/judicial processes. Most standards and best practice guides in the second subset (as covered in this chapter) are made by US bodies, which is mainly due to the leading roles of three key US bodies, National Institute of Standards and Technology (NIST) and two SWGs (Scientific Working Groups), in the digital forensics field. This partitioning has its root in the fact that ISO standards are more about quality assurance procedures, so standards and best practice guides more related to technical/legal/judicial procedures are less dependent on ISO standards.

While ISO standards are the most important ones among all digital forensics standards, the IAAC forensic-readiness guide is the most comprehensive non-standard guide and also the most recent as its latest edition was published in November 2013. The UK ACPO (Association of Chief Police Officers) 'Good Practice Guide' is probably the most cited non-standard guide, which can be explained by its long history since the 1990s.[3]

In the remaining part of this section, we list all standards and best practice guides covered in this chapter according to the following grouping:

- ISO standards
- Other international/regional standards and best practice guides
- US standards and best practice guides
- UK standards and best practice guides
- Other standards and best practice guides

The aforementioned grouping is more based on the bodies making/publishing the standards and best practice guides. In Sections 2.3–2.7 we will discuss all the standards and best practice guides in detail according to the following content-based grouping:

- Electronic evidence and digital forensics
- Multimedia evidence and multimedia forensics
- Digital forensics laboratory accreditation
- General quality assurance (management)
- Training, education and certification

It will be a very long list if we try to cover all relevant standards and best practice guides in all countries and regions. The language barrier and difficulties in accessing the fulltexts of standards from non-English-speaking regions have limited our ability to

[3] The authors were unable to obtain the first edition of the *ACPO Good Practice Guide*, but it must have appeared before 1999 when the second edition was published.

review other potentially relevant standards. Therefore, this chapter covers only some selected standards and best practice guides which we had access and considered more important for the digital and multimedia forensics fields. In future we plan to include a page on the book's website to (i) provide updates on new changes to standards and best practice guides covered in this chapter and (ii) cover more standards and best practice guides which are nor covered in the printed edition of this chapter.

2.2.1 ISO Standards

A number of ISO standards are important in the field of digital forensics:

- ISO/IEC 27037:2012 'Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence' (2012)
- ISO/IEC 27035:2011 'Information technology – Security techniques – Information security incident management' (2011)
- ISO/IEC 17025:2005 'General requirements for the competence of testing and calibration laboratories' (2005)
- ISO/IEC 17020:2002 'General criteria for the operation of various types of bodies performing inspection' (2002)
- ISO/IEC 27001:2013 'Information technology – Security techniques – Information security management systems – Requirements' (2013b)
- ISO/IEC 27002:2013 'Information technology – Security techniques – Code of practice for information security management' (2013a)
- ISO 9001:2008 'Quality management systems – Requirements' (2008)

There are also several other new standards that have not been officially published but are in the final stage of being finalized:

- ISO/IEC 27041 'Information technology – Security techniques – Guidelines on assuring suitability and adequacy of incident investigative methods' (2014a): DIS (draft international standard) as of April 2014
- ISO/IEC 27042 'Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence' (2014b): DIS (draft international standard) as of April 2014
- ISO/IEC 27043 'Information technology – Security techniques – Incident investigation principles and processes' (2014c): FDIS (final draft international standard) as of September 2014
- ISO/IEC 30121 'System and software engineering – Information technology – Governance of digital forensic risk framework' (2014d): FDIS (final draft international standard) as of September 2014

These to-be-published standards will also be covered in this chapter because they are important new progresses and no major changes are expected in their contents (DIS and FDIS are both in voting stages).

2.2.2 Other International/Regional Standards and Guides

There are some other international/regional standards and best practice guides, although some of them (i.e. those made by ASTM International) appear to be more geared to the US digital forensics community. For regional standards and best practice guides we focused mainly on European ones.

- ASTM International Standards[4]:
  - ASTM E2678-09 'Guide for Education and Training in Computer Forensics' (2009)
  - ASTM E2763-10 'Standard Practice for Computer Forensics Guide' (2010)
  - ASTM E2825-12 'Standard Guide for Forensic Digital Image Processing' (2012)
- A best practice guide from the IETF (Internet Engineering Task Force): RFC 3227 'Guidelines for Evidence Collection and Archiving' (2002)
- International best practice guides:
  - ILAC-G19:2002 'Guidelines for Forensic Science Laboratories' (2002)
  - ILAC-G19:08/2014 'Guidelines for Forensic Science Laboratories' (2014)
  - IOCE (International Organization on Computer Evidence) 'Guidelines for Best Practice in the Forensic Examination of Digital Technology' (2002a)
  - IOCE 'Training Standards and Knowledge Skills and Abilities' (2002b)
- European best practice guides:
  - ENFSI (European Network of Forensic Science Institutions) 'Guidelines for Best Practice in the Forensic Examination of Digital Technology' Version 6.0 (2009)
  - ENFSI Forensic Speech and Audio Analysis Working Group (FSAAWG) 'Best Practice Guidelines for ENF Analysis in Forensic Authentication of Digital Evidence' (2009)

2.2.3 US Standards and Best Practice Guides

There are a large number of US standards and best practice guides. Some of these were produced by the NIST, the measurement standards laboratory of the US Department of Commerce. NIST produces Federal Information Processing Standard publications (FIPS PUB), NIST special publications (SPs), technical reports and specifications in

[4] ASTM International is a US-based standardization body making international voluntary consensus standards. While this body calls itself 'ASTM International', the standards it makes are more like regional standards for digital forensics practice in North America (especially in the United States).

different technical fields. Some of these can be used as guidelines for digital forensics. Many other best practice guides have been produced by the Scientific Working Group on Digital Evidence (SWGDE), which was formed by the Federal Crime Laboratory Directors in 1998[5] and the Scientific Working Group on Imaging Technology (SWGIT) formed by the US Federal Bureau of Investigation (FBI) in 1997.[6] Both SWGs produce documents regarding standard procedures for many aspects about handling digital and multimedia evidence. Finally, best practice guides have also been produced by US law enforcement bodies such as the Department of Justice (DOJ) and its research, development and evaluation agency, National Institute of Justice (NIJ). US standards and best practice guides covered in this chapter are listed in the following[7]:

- NIST special publications (SPs), interagency reports (IRs) and other publications:
  - NIST SP 800-101 Revision 1 'Guidelines on Mobile Device Forensics' (Ayers *et al.* 2014)
  - NIST SP 800-72 'Guidelines on PDA Forensics' (Jansen and Ayers 2004)
  - NIST SP 800-86 'Guide to Integrating Forensic Techniques into Incident Response' (Kent *et al.* 2006)
  - NISTIR 7387 'Cell Phone Forensic Tools: An Overview and Analysis Update' (Ayers *et al.* 2007)
  - NISTIR 7617 'Mobile Forensic Reference Materials: A Methodology and Reification' (Jansen and Delaitre 2009)
  - NIST 'Smart Phone Tool Specification' Version 1.1 (NIST 2010)
- SWGDE and SWGIT best practice guides:
  - SWGDE/SWGIT 'Recommended Guidelines for Developing Standard Operating Procedures' Version 1.0 (2004)
  - SWGDE/SWGIT 'Guidelines & Recommendations for Training in Digital & Multimedia Evidence' Version 2.0 (2010)
  - SWGDE/SWGIT 'Proficiency Test Program Guidelines' Version 1.1 (2006)
  - SWGDE 'Model Standard Operation Procedures for Computer Forensics' Version 3.0 (2012d)
  - SWGDE 'Model Quality Assurance Manual for Digital Evidence Laboratories' Version 3.0 (2012c)
  - SWGDE 'Minimum Requirements for Quality Assurance in the Processing of Digital and Multimedia Evidence' Version 1.0 (2010)
  - SWGDE 'Digital Evidence Findings' (2006)
  - SWGDE 'Focused Collection and Examination of Digital Evidence' Version 1.0 (2014h)

[5] See http://www.swgde.org/.

[6] See https://www.swgit.org/history.

[7] NIST published other publications related to digital forensics, but in this chapter we only consider those more relevant as standards and best practice guides.

- SWGDE 'Establishing Confidence in Digital Forensic Results by Error Mitigation Analysis' Version 1.5 (2015)
- SWGDE 'Best Practices for Computer Forensics' Version 3.1 (2014a)
- SWGDE 'Recommended Guidelines for Validation Testing' Version 2.0 (2014j)
- SWGDE 'Best Practices for Mobile Phone Forensics' Version 2.0 (2014e)
- SWGDE 'Core Competencies for Mobile Phone Forensics' Version 1.0 (2013b)
- SWGDE 'Best Practices for Handling Damaged Hard Drives' Version 1.0 (2014d)
- SWGDE 'Capture of Live Systems' Version 2.0 (2014f)
- SWGDE 'Best Practices for Forensic Audio' Version 2.0 (2014c)
- SWGDE 'Core Competencies for Forensic Audio' Version 1.0 (2011)
- SWGDE 'Mac OS X Tech Notes' Version 1.1 (2014i)
- SWGDE 'Best Practices for Vehicle Navigation and Infotainment System Examinations' Version 1.0 (2013a)
- SWGDE 'Best Practices for Portable GPS Device Examinations' Version 1.0 (2012b)
- SWGDE 'Peer to Peer Technologies' (2008)
- SWGDE 'Best Practices for Examining Magnetic Card Readers' Version 1.0 (2014b)
- SWGDE 'UEFI and Its Effect on Digital Forensics Imaging' Version 1.0 (2014k)
- SWGDE 'Electric Network Frequency Discussion Paper' Version 1.2 (2014g)
- SWGIT Document Section 1 'Overview of SWGIT and the Use of Imaging Technology in the Criminal Justice System' Version 3.3 (2010e)
- SWGIT Document Section 4 'Recommendations and Guidelines for Using Closed-Circuit Television Security Systems in Commercial Institutions' Version 3.0 (2012f)
- SWGIT Document Section 5 'Guidelines for Image Processing' Version 2.1 (2010d)
- SWGIT Document Section 6 'Guidelines and Recommendations for Training in Imaging Technologies in the Criminal Justice System' Version 1.3 (2010c)
- SWGIT Document Section 7 'Best Practices for Forensic Video Analysis' Version 1.0 (2009)
- SWGIT Document Section 11 'Best Practices for Documenting Image Enhancement' Version 1.3 (2010b)
- SWGIT Document Section 12 'Best Practices for Forensic Image Analysis' Version 1.7 (2012b)
- SWGIT Document Section 13 'Best Practices for Maintaining the Integrity of Digital Images and Digital Video' Version 1.1 (2012c)
- SWGIT Document Section 14 'Best Practices for Image Authentication' Version 1.1 (2013b)
- SWGIT Document Section 15 'Best Practices for Archiving Digital and Multimedia Evidence (DME) in the Criminal Justice System' Version 1.1 (2012a)

  - SWGIT Document Section 16 'Best Practices for Forensic Photographic Comparison' Version 1.1 (2013a)
  - SWGIT Document Section 17 'Digital Imaging Technology Issues for the Courts' Version 2.2 (2012d)
  - SWGIT Document Section 18 'Best Practices for Automated Image Processing' Version 1.0 (2010a)
  - SWGIT Document Section 19 'Issues Relating to Digital Image Compression and File Formats' Version 1.1 (2011)
  - SWGIT Document Section 20 'Recommendations and Guidelines for Crime Scene/Critical Incident Videography' Version 1.0 (2012e)
  - SWGIT Document Section 23 'Best Practices for the Analysis of Digital Video Recorders' Version 1.0 (2013c)
  - SWGIT Document Section 24 'Best Practices for the Retrieval of Digital Video' Version 1.0 (2013d)
- Best practice guides edited/published by US law enforcement agencies (mainly DOJ and NIJ):
  - *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, 3rd Edition (US DOJ's Computer Crime and Intellectual Property Section 2009)
  - 'Investigative Uses of Technology: Devices, Tools, and Techniques' (US NIJ 2007c)
  - 'Investigations Involving the Internet and Computer Networks' (US NIJ 2007b)
  - 'Forensic Examination of Digital Evidence: A Guide for Law Enforcement' (US NIJ 2004)
  - 'Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors' (US NIJ 2007a)
  - 'Electronic Crime Scene Investigation: A Guide for First Responders' Second Edition (US NIJ 2008)
  - 'Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders' (US NIJ 2009)
  - 'Digital Evidence Field Guide' Version 1.1 (US FBI 2007)
  - 'Mobile Forensics Field Guide' Version 2.0 (US FBI 2010)
  - 'Computer-Based Investigation and Discovery in Criminal Cases: A Guide for United States Magistrate Judges' (US Federal Judicial Center 2003)
  - 'Best Practices for Seizing Electronic Evidence: A Pocket Guide for First Responders' Version 3.0 (United States Secret Service, US Department of Homeland Security 2007)
- First responder training and education handbooks of Carnegie Mellon University (CMU) Computer Emergency Response Team (CERT):
  - 'First Responders Guide to Computer Forensics' (Nolan *et al.* 2005b)
  - 'First Responders Guide to Computer Forensics: Advanced Topics' (Nolan *et al.* 2005a)

2.2.4 UK Standards and Best Practice Guides

In the UK there is a national standard BS 10008:2008 'Evidential weight and legal admissibility of electronic information – Specification' (BSI 2008a) and a number of implementation guides of BS 10008:2008, all published by British Standard Institute (BSI):

- BIP 0008-1:2008 'Evidential weight and legal admissibility of information stored electronically. Code of Practice for the implementation of BS 10008' (BSI 2008c)
- BIP 0008-2:2008 'Evidential weight and legal admissibility of information transferred electronically. Code of practice for the implementation of BS 10008' (BSI 2008d)
- BIP 0008-3:2008 'Evidential weight and legal admissibility of linking electronic identity to documents. Code of practice for the implementation of BS 10008' (BSI 2008e)
- BIP 0009:2008 'Evidential Weight and Legal Admissibility of Electronic Information. Compliance Workbook for Use with BS 10008' (BSI 2008b)

There are also a number of best practice guides made by law enforcement including the ACPO (Association of Chief Police Officers of England, Wales and Northern Ireland), NPIA (National Policing Improvement Agency, dissolved in 2012), HOSDB (Home Office Scientific Development Branch, currently known as the CAST – Centre for Applied Science and Technology) and Forensic Science Regulator (FSR). Those best practice guides are listed in the following:

- Best practice guides on digital forensics or electronic evidence:
  - 'ACPO Good Practice Guide for Digital Evidence' Version 5.0 (UK ACPO 2011a)
  - 'ACPO Good Practice Guide for Managers of e-Crime investigation' Version 0.1.4 (UK ACPO 2011b)
  - Forensic Science Regulator (FSR) 'Codes of Practice and Conduct for forensic science providers and practitioners in the Criminal Justice System' Version 1.0 (UK Forensic Science Regulator 2011)
- Best practice guides on multimedia evidence handling:
  - 'Practice Advice on Police Use of Digital Images' (UK ACPO and NPIA 2007)
  - 'Storage, Replay and Disposal of Digital Evidential Images' (UK HOSDB 2007)
  - 'Digital Imaging Procedures' (Cohen and MacLennan-Brown 2007)
  - 'Retrieval of Video Evidence and Production of Working Copies from Digital CCTV Systems' (Cohen and MacLennan-Brown 2008)
  - 'Practice Advice on The Use of CCTV in Criminal Investigations' (UK ACPO and NPIA 2011)

In addition to the above, the Information Assurance Advisory Council (IAAC), a UK-based not-for-profit organization, also publishes a comprehensive guide on

digital investigations and evidence since 2005 (Sommer 2005) and the latest edition is the fourth edition published in 2013. The guide's title was originally 'Directors and Corporate Advisors Guide to Digital Investigations and Evidence' but was changed to 'Digital Evidence, Digital Investigations, and E-disclosure: A Guide to Forensic Readiness for Organizations, Security Advisers and Lawyers' since its third edition published in 2012.

2.3 Electronic Evidence and Digital Forensics

In this section, we describe standards and best practice guides about electronic evidence and digital forensics in general (excluding those focusing on multimedia evidence and multimedia forensics, which will be covered in the next section). While for most standards we only give a very brief description, for some very important standards we provide more details to reflect their importance for the digital forensics community.

2.3.1 International Standards

2.3.1.1 ISO/IEC 27037:2012 'Guidelines for identification, collection, acquisition and preservation of digital evidence'

This standard provides guidelines for the identification, collection, acquisition and preservation of digital evidence. The scope of the guidance provided concerns general circumstances encountered by personnel during the digital evidence handling process. This standard is part of the ISO/IEC 27000 series of standards on information security management, and should be used as an accompaniment to ISO/IEC 27001 and ISO/IEC 27002 (the two most important standards in the ISO/IEC 27000 series) since it provides supplementary guidance for the implementation of control requirements for digital evidence acquisition.

According to the standard, digital evidence is usually regulated by three central principles:

1. Relevance: digital evidence proves or disproves an element of a case, and be relevant to the investigation.
2. Reliability: digital evidence serves its purpose, and all processes used in the handling of it should be repeatable and auditable.
3. Sufficiency: a digital evidence first responder (DEFR) should gather enough evidence for effective investigation and examination.

In addition, all the tools to be used by the DEFR should be validated prior to use and the validation evidence should be available when a challenge of the validation technique is encountered.

As part of its coverage on the whole process of digital evidence handling, this standard also covers issues related to personnel, roles and responsibilities,

technical and legal competencies (core skills in Annex A), documentation (minimum requirements in Annex B), formal case briefing session, prioritization of potential digital evidence, among other important aspects.

The standard contains a detailed discussion on concrete instances of digital evidence identification, collection, acquisition and preservation. Such instances include computers, peripheral devices digital storage media, networked devices and also CCTV systems.

2.3.1.2 ISO/IEC 27035:2011 'Information security incident management'

This international standard provides techniques for the management of security incidents that are highly related to digital forensics, especially network forensics. It is also part of the ISO/IEC 27000 series and relies on the terms and definitions in ISO/IEC 27000. The standard overviews basic concepts related to security incidents, and describes the relationship between objects in an information security incident chain. It states that there should be a well-structured and planned approach to handle security incidents, and states the objectives of such an approach; which are beneficial for an organization to plan and establish its own security incident management approach. Moreover, it discusses the various benefits of having a structured approach. One of the key benefits is strengthening evidence and rendering it forensically sound and legally admissible. The standard also states that the guidance provided is extensive, and some organizations may vary in the need to deal with all of the issues mentioned depending on the size, nature of business conducted in the organization and complexity of mechanisms implemented within the organization.

Five main phases are identified that should constitute any information security incidence management. These are as follows:

1. Plan and prepare
2. Detection and reporting
3. Assessment and decision
4. Responses
5. Lessons learnt

The various procedures performed as part of the incident response to security incidents should handle and store digital evidence in a way to preserve its integrity in case it is later required for further investigation and legal prosecution.

The rest of the standard overviews key activities of each phase mentioned earlier. Moreover, Annex A provides a cross-reference table of ISO/IEC 27001 versus ISO/IEC 27035. Annex B provides examples of information security incidents and possible causes, while Annex C gives examples of sample approaches to categorization of security events and incidents. Annex D provides examples of incident and vulnerability reports and forms, while Annex E deals with legal and regulatory aspects.

This standard is to be split into three parts in future editions as currently planned by ISO/IEC JTC 1/SC 27 (the expert group editing ISO/IEC 27000 series standards): ISO/IEC 27035-1 'Principles of incident management', ISO/IEC 27035-2 'Guidelines to plan and prepare for incident response', ISO/IEC 27035-3 'Guidelines for incident response operations'. All the three parts are still in CD (committee draft) stage, so it is still too early to introduce them in this chapter.

2.3.1.3 ISO/IEC DIS 27041 'Guidance on assuring suitability and adequacy of incident investigative methods' (2014a)

This standard is also part of a set of new ISO/IEC standards to be published on investigation of information security incidents. As at the time of this writing, it is still in DIS stage, but it is expected that it will be officially published soon.

This standard is about providing assurance of the investigative process used and results required for the incident under investigation. It also describes the abstract concept of breaking complex processes into smaller atomic components so that simpler and robust investigation methods can be developed more easily. This standard is considered important for any person involved in an investigation ranging from authorizer, manager and the actual conductor. It is required that the standard is applied before an investigation starts so that all other relevant standards including ISO/IEC 27037, ISO/IEC 27042, ISO/IEC 27043 and ISO/IEC 27035 are all properly considered.

2.3.1.4 ISO/IEC DIS 27042 'Guidelines for the analysis and interpretation of digital evidence' (2014b)

This standard is also part of a set of new ISO/IEC standards to be published on investigation of information security incidents. Its current status is DIS.

This standard provides guidance on analysis and interpretation of potential digital evidence for identifying and evaluating digital evidence that may be used to investigate an information security incident. It is not a comprehensive guide, but provides some fundamental principles for ensuring that tools, techniques and methods can be selected and justified appropriately. This standard also aims to inform decision makers who need to determine the reliability of digital evidence presented to them. It is assumed to be used together with ISO/IEC 27035, ISO/IEC 27037, ISO/IEC 27041 and ISO/IEC 27043 in order to achieve compatibility.

2.3.1.5 ISO/IEC FDIS 27043 "Incident investigation principles and processes" (2014c)

This standard is also part of a set of new ISO/IEC standards to be published on investigation of information security incidents. Its current status is FDIS, the final

phase of an international standard so we do not expect any major changes to its contents once published.

This standard provides guidelines for common investigation processes across different investigation scenarios, covering pre-incident preparation up to and including returning evidence for storage or dissemination. It also provides general advice and caveats on processes and appropriate identification, collection, acquisition, preservation, analysis, interpretation and presentation of digital evidence.

A basic principle of digital investigations highlighted in this standard is repeatability, which means the results obtained for the same case by suitably skilled investigators working under similar conditions should be the same. Guidelines for many investigation processes are given to ensure clarity and transparency in obtaining the produced results. The standard also provides guidelines to achieve flexibility within an investigation so that different types of digital investigation techniques and tools can be used in practice. Principles and processes are specified and indications are defined for how the investigation processes can be customized for different scenarios. Guidelines defined in this standard help justify the correctness of the investigation process followed during an investigation in case the process is challenged.

This standard covers a rather wide overview of the entire incident investigation process. It it is supposed to be used alongside some other standards including ISO/IEC 27035, ISO/IEC 27037, ISO/IEC 27041, ISO/IEC 27042 and ISO/IEC 30121.

2.3.1.6 ISO/IEC FDIS 30121 'Governance of digital forensic risk framework' (2014d)

This standard is a forensic-readiness standard for governing bodies (e.g. owners, senior managers and partners) to prepare their organizations (of all sizes) for digital investigations before they occur. It focuses on the development of strategic processes and decisions relating to many factors of digital evidence disclosure such as availability, accessibility and cost efficiency. Currently this standard is in the FDIS stage, so its content can be considered stable.

2.3.1.7 IETF RFC 3227 'Guidelines for Evidence Collection and Archiving' (2002)

This IETF RFC (Internet standard) defines best practice for system administrators in collecting electronic evidence related to 'security incidents' as defined in RFC 2828 'Internet Security Glossary' (Shirey 2000). It is a short document covering some general guidelines on 'order of volatility', 'things to avoid', legal and privacy considerations, and discusses evidence collection procedure and evidence archiving procedure separately. It also lists a number of tools system administrators need to have for evidence collection and archiving procedures.

2.3.2 National Standards

2.3.2.1 US Standards

In this section we review two standards made by ASTM International. We categorize them as US standards because they are more US-facing and were developed based on some national best practice guides.

ASTM E2763-10 'Standard practice for computer forensics' (2010)
This standard is a best practice document briefing methods and techniques for seizure, proper handling, digital imaging, analysis, examination, documentation and reporting of digital evidence in the scope of criminal investigations. The standard comprises 11 brief sections, each providing direct steps on general guidelines for a specific process. Section 1 contains the scope of the document, mentioned above, while Section 2 mentions the reference documents that are the ASTM Guide for Education and Training in Computer Forensics, and the SWGDE Recommended Guidelines for Validation Testing. Section 3 mentions the significance and the use of this document, most importantly that the examiner should be trained in accordance with the previous ASTM guide. Section 4 provides very general guidelines on evidence seizure. Section 5 concerns evidence handling, and Section 6 outlines equipment handling. Section 7 outlines steps needed for forensic imaging, while Section 8 handles guidelines on forensics analysis and examination. Section 9 goes over the documentation process, and Section 10 briefly outlines the report and its main function. Section 11 covers review policy of the forensic examiners' organization.

2.3.2.2 UK Standards

BS 10008:2008 'Evidential weight and legal admissibility of electronic information – Specification'
This British standard, which has evolved from the early 1990s,[8] covers the requirements for the implementation and operation of electronic information management systems, including the storage and transfer of information with regard to this information being used as potential digital evidence. It focuses on 'potential' evidence as opposed to other ISO/IEC standards which normally focus on digital material already labelled 'evidence'. The standard states that the requirements covered are generic and can be used by any kind of organization regardless of size or nature of business and can be applied to electronic information of all types. Thus, the information provided in this standard is to a minor degree more generic compared with other ISO/IEC standards.

[8] The first of such early standards we identified is BSI DD 206:1991, titled 'Recommendations for preparation of electronic images (WORM) of documents that may be required as evidence'. It defines 'procedures for the capture and storage of electronic images of hardcopy documents to ensure the preservation and integrity of information recorded on them'.

This standard covers the scope of three BIP 0008 codes of practice on the same topic that have been published by the BSI Group since 1990s and been widely adopted. These three codes of practice are BIP 0008-1, BIP 0008-2 and BIP 0008-3. They cover evidential weight and legal admissibility of information stored electronically, transferred electronically, and linking electronic identity to documents, respectively. The latest version of the BIP 0008 provides more thorough guidance that will assist in the effective application of this standard. They are reviewed in the following.

BIP 0008-1:2008, BIP 0008-2:2008, BIP 0008-3:2008 and BIP 0009:2008

The British Standards Institution (BSI) issued codes of practice BIP 0008-1:2008 'Evidential Weight and Legal Admissibility of Information Stored Electronically', BIP 0008-2:2008 'Evidential Weight and Legal Admissibility of Information Transferred Electronically', and BIP 0008-3:2008 'Evidential Weight and Legal Admissibility of Linking Electronic Identity to Documents', to be used for the implementation of the British Standard 10008, which covers the scope of all these documents. BIP 0009:2008 'Evidential Weight and Legal Admissibility of Electronic Information' is a workbook that needs to be completed, and it aids in the assessment process of compliance with the BS 10008:2008 standard.

The BIP 0008-1:2008 code of practice explains the application and actions of information management systems that store information electronically via any storage media and using any type of data files, where the legal admissibility and evidential weight requirements include authenticity, integrity and availability (referred to 'CIA' in literature). Moreover, this code deals with features of information management processes that influence the usage of information in regular business operations where legal admissibility does not constitute an issue. This widens the applicability of this code of practice. Issues such as accuracy and wholeness of stored information and how information is transferred to other systems are covered, although in more detailed in the next code of practice.

The BIP 0008-2:2008 code of practice explains methods and procedures for transferring information between computer systems where confidentiality, integrity and authentication are required by the legal admissibility and evidential weight of the sent and/or received documents. This is especially when the transfer process occurs between organizations. The code is applied to any type of computer files containing all sorts of data ranging from text and images to video and software. The transmission media can be circuit-switched networks, telephone circuits, cable, radio or satellite technologies, or any other form of transmission networks.

The BIP 0008-3:2008 code of practice explains methods and processes that are associated with four authentication principles, namely electronic identity verification, electronic signature, electronic copyright, and linking the electronic identity and/or electronic signature and/or electronic copyright to the particular electronic document. This is useful when the identity of the sender needs to be proven in identity

theft cases. Moreover, the code provides guidelines on digital signatures and electronic copyright protection systems.

BIP 0009:2008 is a compliance workbook to be used with BS 10008:2008, which aids in the assessment of an information management system for compliance with the BS 10008:2008 standard. It should be completed and stored on the information management system under identical conditions by which other information on the system is stored. Moreover, it provides guidance on how to complete the workbook itself.

2.3.2.3 HB 171-2003 'Guidelines for Management of IT Evidence' (Australia)

This Australian standard provides guidance on managing electronic records that might be used as potential evidence in judicial and administrative procedures. It ensures the evidential value of records processed electronically.

It provides an overview of the management of IT evidence and the different uses of IT evidence for judicial, administrative and criminal proceedings. Moreover, it provides different principles for the management of IT evidence, and the IT evidence management lifecycle that consists of six stages: design for evidence, production of records, collection of evidence, analysis of evidence, reporting and presentation, and evaluating evidentiary weight.

2.3.3 Best Practice Guides

2.3.3.1 IOCE 'Guidelines for Best Practice in the Forensic Examination of Digital Technology' (2002a)

This document was made by the International Organization on Computer Evidence (IOCE). It presents requirements for systems, personnel, procedures and equipment in the whole forensic process of digital evidence. It provides a structure of standards, quality principles, and methods for processing digital evidence for forensic purposes in compliance with the requirements of an accreditation body or a prominent organization in the digital forensics community. It also promotes greater consistency in the methodology of processing digital evidence, which can yield equivalent results, thus enabling the interchange of data.

2.3.3.2 ENFSI 'Guidelines for Best Practice in the Forensic Examination of Digital Technology' Version 6.0 (2009)

This guide, produced by the European Network of Forensic Science Institutions (ENFSI), presents a structure for the standards and methods to be used for the detection, recovery and inspection of digital evidence for forensic objectives conforming to the standards of the ISO/IEC 17025 standard. Moreover, the guideline seeks to promote the level of efficiency and quality assurance in laboratories conducting forensic

investigations using digital evidence that can produce consistent and valid results as well as increase cooperation among laboratories.

The guide covers most of the procedures and phases in the digital forensic process from evidence recovery and examination to report presentation for the court. Moreover, the document states that participating laboratories should have achieved or be in the process of achieving ISO/IEC 17025 accreditation for laboratory testing events (by following ILAC G19:2002 implementation guidance). The document defines different terms and concepts necessary for forensic laboratory operation, and outlines the different types of personnel involved in the process, along with the qualifications and requirements to perform their respective roles. Moreover, it encourages the active participation of personnel in seminars, workshops and training sessions in order to maintain their level of competence if not increase it. It also mentions the importance of proficiency testing, and outlines the procedure of administering such tests and the personnel responsible for this testing.

This guide also includes details of complaint procedures, and outlines general procedures and guidelines for complaints, stressing the importance of prompt action when dealing with complaints and anomalies.

2.3.4 US Guides

2.3.4.1 NIST

NIST SP 800-101 Revision 1 'Guidelines on Mobile Device Forensics' (2014)

The National Institute of Standards and Technology (NIST) published this guide on mobile device forensics, a relatively new and growing area in digital forensics. It covers a wide range of examination techniques, including examining operation and features of cellular networks (e.g. GSM), that helps forensics examiners better understand cellular phone operation and subsequently improve their forensic analysis skills. Its first edition was published in 2007 with a slightly difference title 'Guidelines on Cell Phone Forensics' and the revision in 2014 contains mainly updated and augmented to reflect new development in this field especially smart phones (which also caused the change of the title to 'Guidelines on Mobile Device Forensics').

This guide covers procedures for the preservation, acquisition, examination, analysis and reporting of mobile device evidence. Moreover, one of the main aims of the guide is to enable organizations and personnel to make more educated decisions about mobile forensics and provide support for personnel performing this task. It also provides information that can be used as a basis for standard operating procedures (SOPs) and policy development in the organization. In fact, the guide expands on this issue by stating that an organization must have its own forensics procedures, which can be tailored to the nature of the business of that organization. To support this, the guide provides information regarding the level of detail needed for policy in order to maintain

a chain of custody. In addition, detailed information is provided for procedures and examinations of mobile phones to ensure successful policy production for an organization dealing with this task, along with how to perform proper evidence handling. Furthermore, different methods of data acquisition are discussed in detail, and the use of a cable is recommended in most situations. However, when this is not possible, the risk level of performing wireless acquisition is discussed.

This guide provides both coverage on physical and logical examinations, with detail on how to find evidence in memory. It also provides additional information on how to find and examine evidence on subscriber identity modules (SIM) cards, and discusses different types of data that can be extracted.

Legal practices are also considered, and the UK ACPO best practice guide (UK ACPO 2011a) is mentioned, along with the four principles that serve the goal of ensuring the integrity and accountability of evidence during an investigation. The Daubert standard originating in the United States (Project on Scientific Knowledge and Public Policy 2003) is also mentioned as a guide to be referred to when presenting evidence in a court of law.

Finally, this guide presents a variety of forensic tools evaluation: producing test results, reference data and proof of concept implementations and analysis. This tools evaluation has also resulted in the implementation of a test description and requirements document for a tool to be tested. The guide can provide aid to tool manufacturers so that they can improve their products. It also addresses the need for manufacturers to continuously update their products, since new mobile devices are being released very frequently.

NIST SP 800-72 'Guidelines on PDA Forensics' (2004)

This publication focuses on personal digital assistants (PDAs) and provides guidance on the preservation, examination and analysis of digital evidence on PDAs. It focuses on the properties of three families of PDAs:

1. Pocket PC
2. Palm OS
3. Linux-based PDAs

This guide also outlines actions to be taken during the course of evidence handling, device identification, content acquisition, documentation and reporting, in addition to forensic tools needed for such activities. The two main objectives of the publication are to aid organizations in gradually developing SOPs and strategies for forensic actions involving PDAs, and to prepare forensic examiners and first responders to effectively tackle any obstacles and challenges that might arise with digital evidence on PDAs. This guide is also intended to be used in addition with other guidelines to present more detailed insight into the issues associated with PDAs.

NIST SP 800-86 'Guide to Integrating Forensic Techniques into Incident Response" (2006)

This special publication is a detailed guide for organizations to help them build a digital forensic capability. It focuses on how to use digital forensic techniques to assist with computer security incident response. It covers not only techniques but also the development of policies and procedures. This NIST guide should not be used as an executive guide for digital forensic practices. Instead, it should be used together with guidance provided by legal advisors, law enforcement agencies and management.

The guide provides general recommendations for the forensic process in four phases: collection, examination, analysis and reporting. For the analysis phase, it covers four major categories of data sources: files, operating systems, network traffic and applications. For each category, it explains basic components and characteristics of data sources and also techniques for the collection, examination and analysis of the data. It also provides recommendations when multiple data sources need analyzing for a better understanding of an event.

The document also highlights four basic guidelines to organizations:

1. Organizations should establish policies with clear statements addressing all major forensic considerations and also conduct regular reviews of such policies and procedures.
2. Organizations should create and maintain digital forensic procedures and guidelines based on their own policies and also all applicable laws and regulations.
3. Organizations should ensure that their policies and procedures support use of the appropriate forensic tools.
4. Organizations should ensure that their IT professionals are prepared for conducting forensic activities.

NISTIR 7387 'Cell Phone Forensic Tools: An Overview and Analysis Update' (2007)

This interagency report (IR) of NIST is an overview of cell phone forensics tools designed for digital evidence acquisition, examination and reporting, which is an updated edition of NISTIR 7250 published in 2005. This document is not supposed to be a step-by-step guide, but serves to inform the digital forensic community about available tools and their performance.

NIST Smart Phone Tool Specification Version 1.1 (2010)

The purpose of this document is to specify requirements for mobile phone forensic tools that can be performed by obtaining internal memory from GSM smart phones and SIM cards and the internal memory of CDMA smart phones. Moreover it specifies test methods to verify if a certain tool meets the requirements.

The requirements which are specified are used to obtain test assertions. These are conditions that can be verified after tool testing, and these assertions produce at

least one test case which consists of a test protocol and associated parameters. The protocol provides measures for performing the test along with the associated results to be expected from the test. The test cases and associated assertions are specified in the 'Smart Phone Acquisition Tool Test Assertions and Test Plan' (2010) document published by NIST.

NISTIR 7617 'Mobile Forensic Reference Materials: A Methodology and Reification' (Jansen and Delaitre 2009)
This report from NIST considers validation of mobile forensics tools, focusing on the use of reference test data. It describes a computer program and a data set for populating mobile devices. The data set was used to analyze some existing mobile forensics tools and a variety of inaccuracies were identified. It highlights the importance and difficulties of conducting proper tool validation and testing.

2.3.4.2 SWGs (Scientific Working Groups)

SWGDE/SWGIT 'Recommended Guidelines for Developing Standard Operating Procedures' Version 1.0 (2004)
This document considers SOPs that refer to the procedures followed regularly by law enforcement agencies in their activities. Thus, when considering digital forensics and evidence, SOPs can include all the activities related to digital evidence ranging from evidence recovery and examination to analysis and court presentation. Since SOPs can basically cover the whole forensics process, SWGDE has recommended guidelines regarding developing such SOPs that should be reviewed annually, and should contain all the information needed for a specific task in relation to a case being investigated, type of evidence collected, and the type of agency conducting the investigation. General guidelines include the purpose of the SOP, definitions, equipment to be used and its type and limitations, detailed steps of the SOP, references, authorization information and any additional material required for the SOP (e.g. safety instructions). Two example SOPs are given, one for wiping media and the other for video processing.

SWGDE 'Model Standard Operation Procedures for Computer Forensics' Version 3.0 (2012d)
This document provides a model of SOPs for digital forensics that can be used by organizations as a template. It is designed to be functional for both a single person operation, multiple person units and laboratory organizations. The model was developed by SWGDE based on a variety of SOPs from a broad selection of federal, state and local organizations. The model follows a modular approach so that a digital forensics lab can include sections they want to implement. The focus of each module is the methodology to conduct a forensic examination properly, under the assumption

that the examiner is properly trained and competent in digital forensic analysis. The template SOPs are only examples and should not be used as mandatory step-by-step guides, and their contents must be revised to reflect an organization's policies and procedures.

SWGDE 'Minimum Requirements for Quality Assurance in the Processing of Digital and Multimedia Evidence' Version 1.0 (2010)

This document describes the minimum requirements for quality assurance when examining digital evidence as part of a forensic investigation. It outlines minimum requirements for the purposes of training, examiner certification, examination requirements, and laboratory requirements. Section 3 deals with educational aspects and training and discusses employment qualifications, training in areas related to duties, apprenticeship, on-going training, competency assessment and resources. Section 4 handles requirements for certification of digital evidence practitioners. Section 5 outlines laboratory standards in terms of personnel, facility design, evidence control, validation, equipment performance, examination procedures, examination review, documentation and reporting, competency testing, audits, deficiencies, health and safety. Policies for handling customer complaints, document control and disclosure of information are also mentioned in this section. Section 6 considers how to handle examination requests, examination and documentation.

SWGDE 'Digital Evidence Findings' (2006)

This is a very short document with the aim of ensuring that digital examination findings are presented to interested parties in an easily understandable format. It briefly lists what to include in a findings report and highlights the need to make such reports readable in non-technical terms and delivered on commonly accepted media supported by appropriate software. It also suggests that digital evidence laboratories educate people who review findings' reports. The document, however, does not cover laboratory specific topics and issues about providing digital evidence to defence representatives.

SWGDE 'Recommended Guidelines for Validation Testing' Version 2.0 (2014j)

This document is designed for all bodies performing digital forensic examinations, and it provides recommendations and guidelines for validation testing which is crucial for the results and conclusion of the examination process. It is stated that the testing should be applied to all new, revised and reconfigured tools and methods prior to their initial use in digital forensic processes. Such a validation testing process will guarantee the integrity of all the tools and methods used. The guideline outlines the process of validation testing, and also offers a sample test plan, a sample test scenario report and a sample summary report.

SWGDE 'Best Practices for Computer Forensics' Version 3.1 (2014a)
This document aims to outline best practices for computer forensics (forensics of normal computers like desktop PCs), starting from evidence collection and handling to report presentation and policy review. The sequence of information presented is very similar to that defined in ISO/IEC 27037, but it is more general in nature. However, an additional section of forensic imaging is included that briefly discusses how images should be taken.

SWGDE 'Focused Collection and Examination of Digital Evidence' Version 1.0 (2014h)
This document provides forensic examiners with a list of considerations when dealing with the review of large amounts of data and/or numerous devices so that they can focus their investigation on more relevant types of evidence. The main goal of this focused approach is to maximize efficiency and utilization of resources, so it can be considered as part of a generalized triage process.

SWGDE 'Establishing Confidence in Digital Forensic Results by Error Mitigation Analysis' Version 1.5 (2015)
This document provides a process for recognizing and describing errors and limitations associated with digital forensics tools. It starts with an explanation to the concepts of errors and error rates in digital forensics and highlights the differences of those concepts from other forensic disciplines. This document suggests that confidence in digital forensic results can be enhanced by recognizing potential sources of error and applying mitigating techniques, which include not only technical means but also trained and competent personnel using validated methods and following recommended best practices.

SWGDE 'Capture of Live Systems' Version 2.0 (2014f)
This document provides guidance on acquiring digital evidence from live computer systems. A primary concern is to capture and save data in a usable format. Factors that a forensic examiner should consider include the volatility or the volume of data, restrictions imposed by legal authority, and the use of encryption. It covers both volatile memory and data from mounted file systems as stored in a computer.

SWGDE 'Best Practices for Handling Damaged Hard Drives' Version 1.0 (2014d)
This document supplements the more general guide on best practices for computer forensics (SWGDE 2014a) by describing how to handle magnetic media hard drives when the data cannot be accessed using normal guidelines. It does not cover all storage media (e.g. solid-state drives, flash media and optical media). This document highlights that hard drive data recovery should be conducted by properly trained personnel only because traditional computer forensic software tools may destroy data stored on such hard disks.

SWGDE 'UEFI and Its Effect on Digital Forensics Imaging' Version 1.0 (2014k)
This document provides a general overview and guidance on Unified Extensible Firmware Interface (UEFI) used in media imaging. UEFI and its implementations are currently evolving so this document is expected to change as this technology and its standards become maturer. This document is for trained forensics professionals who may encounter UEFI for the first time.

SWGDE 'Best Practices for Examining Magnetic Card Readers' Version 1.0 (2014b)
This document describes best practices for seizing, acquiring and analyzing data contained within magnetic card readers used for illegal purposes (commonly called skimmers) to store personally identifiable information (PII). This document discusses different types of skimmers and explains the technical approaches to handling such devices for forensic investigation purposes.

SWGDE 'Best Practices for Mobile Phone Forensics' Version 2.0 (2014e)
This document provides best practice guidelines for the examination of mobile phones using hardware and software tools, including physical and logical acquisition. The target audiences include examiners in a laboratory setting and first responders encountering mobile phones in the field. It lists the most common limitations of mobile phones, ranging from dynamic and volatile data, to passwords and SIM cards. Guidelines for evidence collection are given in terms of evidence seizure and handling. The procedure for processing mobile phones in the laboratory is outlined in terms of equipment preparation, data acquisition, examination/analysis, documentation and archiving. Reporting and reviewing are also briefly mentioned at the end.

SWGDE 'Mac OS X Tech Notes' Version 1.1 (2014i)
This document describes the procedures for imaging and analyzing computers running Mac OS X (an operating system from Apple Inc.). It includes a discussion of OS X but does not cover iOS used by mobile devices and smart home appliance such as Apple TV. As a collection of technical notes, this document largely focuses on technical explanations to Mac OS and applications typically running from this platform.

SWGDE 'Best Practices for Portable GPS Device Examinations' Version 1.0 (2012b)
This document describes the best practices for handling portable GPS device examinations and provides basic information on the logical and physical acquisition of GPS devices. It also covers other steps of the whole evidence handling process including archiving and reporting.

SWGDE 'Best Practices for Vehicle Navigation and Infotainment System Examinations' Version 1.0 (2013a)
This document describes best practices for acquiring data contained within navigation and information and entertainment (Infotainment) systems installed in motor vehicles. It provides basic information on the logical and physical acquisition of such systems after physical access is obtained. It should be used in conjunction with the SWGDE document 'Best Practices for Portable GPS Devices'. It is limited to user data and does not cover information such as crash data.

SWGDE 'Peer-to-Peer Technologies' (2008)
This document is intended to provide guidelines when attempting to extract/recover evidence from peer to peer systems and associated files used in such systems for forensic purposes. The document provides results from a methodology used for testing peer to peer systems on different operating systems that was conducted by the US National White Collar Crime Center (NW3C), and the methodology is briefly outlined in the document.[9]

2.3.4.3 Department of Justice and Other Law Enforcement Agencies

DOJ 'Searching & Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations' 3rd Edition (2009)
This document deals with the laws that preside over digital evidence in criminal investigations that stem from two key sources: the Fourth Amendment and the statutory privacy laws like the Stored Communications Act, the Pen/Trap statute and the Wiretap statute. Moreover, it focuses on matters that arise in drafting search warrants, forensic analysis of seized computers, and post-seizure obstacles posed to the search process. Finally, in addition to discussing the applications of the above mentioned laws for searching and seizing digital evidence, it also deals with issues of seizure and search with and without a warrant.

NIJ Special Report 'Investigative Uses of Technology: Devices, Tools, and Techniques' (2007c)
This publication is intended to serve as a resource for law enforcement personnel dealing with digital evidence, including relevant tools and techniques. As most NIJ reports, it focuses on three pillars:

1. Preserving the integrity of digital evidence during collection and seizure.
2. Adequate training of personnel examining digital evidence.
3. Full documentation and availability of procedures involving seizure, examination, storage or transfer of digital evidence.

[9] It states that the results of the NW3C research can be found in a report titled 'Peer to Peer: Items of Evidentiary Interest' at the SWGDE website. However, our search into both SWGDE and NW3C websites did not provide any link to this report.

In addition to the above, care must be taken when seizing electronic devices since inappropriate data access may violate federal laws including the Electronic Communications Privacy Act of 1986 and the Privacy Protection Act of 1980. The report is structured into three chapters: Chapter 1 covers techniques, Chapter 2 covers tools and devices, and Chapter 3 covers legal issues for the use of high technologies.

NIJ Special Report 'Investigations Involving the Internet and Computer Networks' (2007b)

This report deals with investigations involving the Internet and other computer networks. It focuses on tracing an Internet address to a source, investigating emails, websites, instant message systems, chat rooms, file sharing networks, network intrusions, message and bulletin boards and newsgroups, and legal issues associated with performing these activities. The guide provides technical knowledge of how to handle digital evidence found on computer networks and on the Internet, ranging from chat rooms to information stored on the Internet Service Provider's records.

NIJ Special Report 'Forensic Examination of Digital Evidence: A Guide for Law Enforcement' (2004)

This report presents a guide for law enforcement on forensic digital examination. It also repeats the three pillars observed in most NIJ reports. It overviews how digital evidence is processed covering four essential steps, that is, assessment, acquisition, examination, and documentation and reporting. It discusses whether an agency is ready to handle digital evidence based on appropriate resources needed for that task. The report presents five basic steps for conducting evidence examination as follows: Policy and procedure development, evidence assessment, evidence acquisition, evidence examination, and documenting and reporting.

NIJ Special Report 'Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors' (2007a)

This report provides guidance on preparation of digital evidence for presentation in court. It details how to effectively present a case involving digital evidence, and suggests how to deal with a Daubert[10] gate-keeping challenge. In addition, it discusses challenges that face the process of maintaining the integrity of digital evidence along discovery and disclosure of the evidence. There is a chapter dedicated to child pornography cases that provides recommendations for law enforcement personnel on how to have a better understanding of the subculture of child pornographers to help with their investigation, since child pornographers are likely to be knowledgeable with the Internet, computers and technology.

[10] This refers to the Daubert Standard (Project on Scientific Knowledge and Public Policy 2003) following by US courts of law on scientific evidence. This is mentioned earlier in this chapter when NIST SP 800-101 (Ayers *et al.* 2014) is introduced.

NIJ Special Report 'Electronic Crime Scene Investigation: A Guide for First Responders' Second Edition (2008)

This report serves as a guide for law enforcement agencies and first responders in the tasks of recognition, collection and protection of digital evidence. In the introduction it defines digital evidence, and outlines how an agency can prepare for handling digital evidence investigations. It provides detailed information on different types of electronic devices on which potential evidence can be found, including computer networks and any investigative tools and equipment used in this process. Moreover, it outlines the process of securing and evaluating a crime scene, and instructs first responders on how to act when they arrive at the scene. There is also consideration of documentation, especially documenting the scene, and a list of what pieces of information to include. Evidence collection and transportation are also discussed towards the end, with the last chapter providing examples on categories and considerations given for specific crimes that can involve digital evidence.

NIJ Special Report 'Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders' Second Edition (2009)

This booklet style report is extracted from the above reviewed special report.

FBI 'Digital Evidence Field Guide' Version 1.1 (2007)

The guide starts out by mentioning five important facts about digital evidence that every law enforcement officer should be aware of including that most crimes involve digital evidence so that most crime scenes are digital crime scenes. Moreover, it states that digital evidence is usually volatile and can be easily modified if not handled with care. It also states that most digital evidence can be recovered even from damaged computers and other devices.

The guide focuses on explaining the role of a computer (or any other digital device in general) in a crime:

- Computers as the target of a crime, that is, related to the notion of unauthorized access to computer systems and hacking for specific aims like espionage, cyber terrorism and identity theft among others.
- Computers as the instrument of a crime, that is, using the computer to commit a specific crime, as above depending on the intention of the attacker including all of the above cases and additional cases like credit card frauds and child solicitations.
- Computer as the repository of evidence, that is, evidence on a computer can be found in various forms, like files, images, logs, etc. This is usually associated with crimes like frauds, child pornography, drug trafficking and email accomplices in traditional crimes.

Finally, the guide differentiates between the two types of digital evidence found on computers: universal (e.g. emails, logs, images) and case specific (e.g. for cyber

terrorism it would include computer programs making the user anonymous, IP addresses, source code, among others).

FBI 'Mobile Forensics Field Guide' Version 2.0 (US FBI 2010)
This guide is available to law enforcement only, and we were unable to get a copy. From its title we can however guess the contents are about guidelines for mobile forensic examiners in the field. If we get a copy of this guide later, we will add a more detailed description on the book's website (permission will be sought from the FBI).

United States Secret Service 'Best Practices for Seizing Electronic Evidence V.3: A Pocket Guide for First Responders' (2007)
This field guide is intended to provide law enforcement personnel and investigators with an explanation of the methods in which computers and electronic devices may be used in committing crimes or as an instrument of a crime, or being a storage medium for evidence in a crime. It also provides guidance for securing evidence and transporting it for further analysis and examination to be performed by a digital evidence forensic examiner.

US FJC 'Computer-Based Investigation and Discovery in Criminal Cases: A Guide for United States Magistrate Judges' (2003)
This guide is actually a mixture of slides for a workshop presentation, a list of annotated case laws, excerpts from the guide 'Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations' (US DOJ's Computer Crime and Intellectual Property Section 2002), a review of research on unresolved issues in computer searches and seizures (Brenner and Frederiksen 2002), and a draft report and recommendations for a working group on electronic technology in criminal justice system. The excerpts from the US DOJ guide and the review paper form the main body of the guide.

Compared with other guides and best practice documents, this one is less formal, and this may be explained by the fact that judges are much less familiar with electronic technologies than digital forensic examiners. In the draft report for the working group on electronic technology in criminal justice system, it is acknowledged that electronic data is pervasive and the lack of resources and training to handle electronic data. For the trial stage, it is also recommended that appropriate means should be taken to identify, preserve and present electronic evidence for the appellate record in an appropriate form.

2.3.4.4 CMU CERT

CMU CERT 'First Responders Guide to Computer Forensics' V1.3 (2005b)
This document highlights a serious training gap common to the fields of information security, computer forensics and incident response, which is performing basic forensic data collection. It comprises four modules:

- Module 1: Cyber laws and their influence on incident response
- Module 2: Understanding file systems and building a first responders toolkit
- Module 3: Volatile data, including tools for its collection, methodologies and best practices
- Module 4: Collecting persistent data in a forensically sound fashion

Of interest is that it quotes two related standards: ISO/IEC 17025 and RFC 3227. In addition, it also refers to the US DOJ guide 'Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations' (Version 2.0 published in 2002), NIJ guide 'Forensic Examination of Digital Evidence – A Guide for Law Enforcement' (2004) and the UK ACPO good practice guide (Version 3.0 published in 2003).

CMU CERT 'First Responders Guide to Computer Forensics: Advanced Topics' (2005a)

This guide builds on the technical data presented in the previous guide, with a special focus on advanced technical operations and procedures instead of methodology. It comprises five modules:

- Module 1: Log file analysis
- Module 2: Process characterization, analysis and volatile data recovery
- Module 3: Image management, restoration and capture, and a tool called dd
- Module 4: Capturing a running process
- Module 5: Identifying spoofed email and tracing it using various techniques

2.3.5 European Guides

2.3.5.1 UK ACPO Good Practice Guide for Digital Evidence (2011a)

This guide is the latest edition of a series of such guides started in the 1990s (UK ACPO 1999, 2003, 2007, 2011a). Its title was originally 'Good Practice Guide For Computer Based Evidence' and changed to 'Good Practice Guide for Digital Evidence' in its latest edition, which reflects a major change from focusing on normal computers to diverse computing devices that can generate evidence in digital form. It is the current 'gold standard' for digital forensic examiners in UK police forces and widely accepted in UK court.

The guide presents instructions on the handling and examination of digital evidence found on computer devices. It ensures the collection and recovery of evidence in an efficient and timely fashion. The guide presents four principles for the handling of digital evidence by law enforcement personnel, as follows (note that we reproduce wording from the guide itself to be more accurate):

- **Principle 1**: No action taken by law enforcement agencies, persons employed within those agencies or their agents should change change data which may subsequently be relied upon in court.
- **Principle 2**: In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
- **Principle 3**: An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
- **Principle 4**: The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

The main body of the guide covers planning, evidence capturing, analysis and presentation. Online evidence and mobile phone forensics are covered in this guide as well. For the presentation part, it covers different forms of presentation of digital evidence including verbal feedback, formal statements and reports, and as witness evidence. It also has a section on general issues such as training and education, welfare in the workplace, digital forensics contractors, disclosure and relevant legislation in the United Kingdom. The guide refers to another ACPO guide 'Good Practice Guide for Managers of e-Crime investigation' (UK ACPO 2011b) which covers more about managerial issues around e-crime investigation.

The guide also contains four appendices, one dedicated to network forensics covering wired and wireless networking devices and also live forensics, one dedicated to crime involving online evidence (websites, forums, blogs, emails, covert communications on the Internet, etc.), one dedicated to crime scene investigations and the last discussing how a law enforcement agency can develop a digital investigation strategy.

2.3.5.2 UK ACPO Good Practice and Advice Guide for Managers of e-Crime Investigation Version 0.1.4 (2011b)

This ACPO guide was produced in the context of the latest edition of the aforementioned best practice guide for digital forensic examiners. While the earlier one is for technical staff, the current one is mainly for managers of e-crime investigation laboratories/teams.

The guide consists of six sections. The first involves the initial setup, and it outlines issues such as role definitions: Roles of staff within e-crime units relating to the activities conducted that fall under two categories, that is forensic and network. This section also outlines key issues including training, budget, personnel and skill profiles, line managers within specialist investigation units, security of data and general points for consideration including accreditation. It encourages units to obtain ISO 9001 accreditation in the medium term, and ISO/IEC 17025 in the long term.

The second section of the guide involves management matters: where key issues such as business continuity are considered, including those for personnel and data, health and safety, and an example risk assessment policy developed by Sussex Police. Moreover, it also provides general advice on presentation of evidence, and on archiving and disposal.

The third section of the guide focuses on investigative matters, providing advice on balancing intrusion and privacy when conducting investigations and also outlining issues concerning intelligence acquisition and dissemination. Moreover, quality of process is covered, and the guide encourages units to implement different ISO standards including ISO 9001, ISO/IEC 17025, ISO/IEC 27001, and ISO/IEC 20000, advising managers to achieve this through the UKAS (United Kingdom Accreditation Service) while also considering the costs of such actions. In addition, it examines the different aspects related to defence 'experts', their instructions, and their use in the prosecution process, including the motivation for potential meetings to take place between defence experts and prosecution experts, with a description of the potential benefits.

The fourth section is about general issues, briefly providing recommendation for DNA profiling from keyboards, and also a review of recent changes in legislation and its impacts, including the Computer Misuse Act 1990 Amendments, Fraud Act 2006, and Part III RIPA 2000 – Investigation of Electronic Data Protected by Encryption, Powers To Require Disclosure. Moreover, it includes proposed amendments to the Obscene Publications Act 1959. It also mentions sources of advice including the NPIA, Serious Organised Crime Agency (SOCA) e-Crime, ACPO High-Tech Crime Sub-Group, Digital Evidence, The Centre for Forensic Computing, First Forensic Forum (F3), and the Internet Watch Foundation.

The fifth section is brief and focuses on forensic matters. It is linked to Appendix G in the guide, and focuses on issues such as peer review, dual tool verification, horizon scanning, and preview of machines and triage.

The last section is involved with training; including where and when to do training, what courses to be provided. It provides a training matrix for digital evidence recovery personnel, network investigators and mobile phone examiners.

2.3.5.3 UK Forensic Science Regulator 'Codes of Practice and Conduct for Forensic Science Providers and Practitioners in the Criminal Justice System' Version 1.0 (2011)

This document defines codes of practices for providers of forensic services to the criminal justice system in the United Kingdom. The Forensic Science Regulator expects that all forensic laboratories handling digital data recovery should pass ISO/IEC 17025:2005 accreditation (supplemented by ILAC-G19:2002) by October 2015.[11] The codes are basically an implementation of ISO/IEC 17025 and

[11] For other types of forensic activities, there are different deadlines.

ILAC-G19:2002 for forensic laboratories providing services to criminal justice system. The main difference is that ISO/IEC 17025 and ILAC-G19:2002 are voluntary, but the codes are mandatory: 'All practitioners and providers offering forensic science services to the CJS are to be bound by these Codes' (Clause 2.3). In the codes, it is also made clear that the UKAS will be the accreditation body assessing all forensic laboratories. However, note that the official role of the UKAS is not defined by the Forensic Science Regulator or the Home Office. Rather, this is done by the Accreditation Regulations 2009 (No. 3155)[12] as the UK's response to Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008.[13]

2.3.5.4 Information Assurance Advisory Council (IAAC, Based in the United Kingdom) Digital Evidence, Digital Investigations, and E-disclosure: A Guide to Forensic Readiness for Organizations, Security Advisers and Lawyers (Fourth Edition, 2013)

This document is the fourth edition of a guide published by the IAAC whose first edition appeared in 2005. It stresses the importance of having a corporate forensic readiness program for an organization, and it is aimed at three types of audience who are involved in this process: Owners and managers of organizations, legal advisors and computer specialists. It seeks to provide information for the target audience on the various issues involved in evidence collection, analysis and presentation. This guide offers a rich amount of information about many standards and best practice documents, and also UK law enforcement resources and structures. Appendix 2 of this guide provides detailed individual procedures for the preservation of different types of evidence.

2.3.5.5 Information Security and Forensic Society (ISFS) Hong Kong 'Computer Forensics Part 2: Best Practices' (2009)

This document provides techniques and requirements related to the whole forensic process of providing digital evidence. It presents a deep level of examination of computer forensics from a technical aspect, along with an explanation underlying different procedures. It claims to be written in a neutral technological and jurisdictional manner, but with considerations in mind for readers from Hong Kong. The document is composed of the following five sections: Introduction to computer forensics, quality computer forensics, digital evidence, gathering evidence, and considerations

[12] The Accreditation Regulations 2009, No. 3155, Regulation 3, Appointment of UKAS as national accreditation body, 2009, http://www.legislation.gov.uk/uksi/2009/3155/regulation/3/made.

[13] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93, Official Journal of the European Union, L218, 30–47, 13 August 2008, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:218:0030:0047:EN:PDF.

of law. It also has four appendices providing further information: A sample statement of findings, a list of sources of data (potential evidence), additional evidence considerations covering admissibility of digital evidence in HK, and relevant selections from HK electronic transaction ordinance.

2.4 Multimedia Evidence and Multimedia Forensics

Compared to general digital forensics, we did not find any international standards focusing on multimedia evidence or multimedia forensics only. This is not surprising because most international standards look at procedural aspects covering digital evidence and digital forensics in general which can also be applied to multimedia evidence and multimedia forensics. There are however some national standards available. Particularly, we noticed that there are a large number of national standards published by Chinese standardization bodies and authorities. These standards cover different aspects of multimedia evidence and multimedia forensics such as crime-scene photography and videography, digital forensic imaging, multimedia evidence extraction, forensic audio/image/video evidence enhancement, image authenticity detection, photogrammetry, multimedia evidence recovery from media storage, etc.[14] We were unable to obtain most of these China standards as they are not freely available, so we will not cover them in this chapter.

2.4.1 ASTM E2825-12 'Standard Guide for Forensic Digital Image Processing' (2012)

This more US-facing standard addresses image processing and related legal considerations in image enhancement, image restoration, and image compression. It provides guidelines for digital image processing to ensure quality forensic imagery is used as evidence in court. It also briefly describes advantages, disadvantages and potential limitations of each major process. This standard is partly based on the best practice guides of SWGDE and SWGIT.

2.4.2 US SWGs (Scientific Working Groups)

A large number of best practice guides on multimedia evidence and multimedia forensics are published by SWGDE and SWGIT, the two SWGs based in the United States. SWGDE focuses on mainly computer forensics, and it traditionally also covers forensics audio since SWGIT only covers forensic imaging (images

[14] There are also a large number of national standards on digital forensics published by Chinese standardization bodies and authorities, many of which are not based on any existing international standards. The "national vs. international" issue is a topic for future research as we will discuss in Section 2.8.

and video evidence). The two SWGs also work very closely with each other to produce joint best practice guides on common issues covering both digital and multimedia evidence/forensics particularly on training (see Section 2.7 for some joint SWGDE/SWGIT guides in this area). In the following, we review selected best practice guides from SWGDE and SWGIT on multimedia evidence and multimedia forensics.

2.4.2.1 SWGDE 'Best Practices for Forensic Audio' Version 2.0 (2014c)

This document provides recommendations for the handling and examination of forensic audio evidence for successful introducing such evidence in a court of law. It covers best practices for receiving, documenting, handling and examining audio evidence, independent of the tools and devices used to perform the examination.

2.4.2.2 SWGDE 'Electric Network Frequency Discussion Paper' Version 1.2 (2014g)

This document describes the potential use of electric network frequency (ENF) analysis for forensic examinations of audio recordings. It explains the technology behind ENF analysis, what ENF analysis can address, and how to handle evidence using ENF analysis.

2.4.2.3 SWGIT Document Section 1: 'Overview of SWGIT and the Use of Imaging Technology in the Criminal Justice System' Version 3.3 (2010e)

Since digital imaging is a widely used practice in forensic science, it is important to focus on different issues arising in this field. The main objective of this document is to make readers accustomed to significant issues in the capture, preservation, processing and handling of images in digital format, analogue format or film format. The document defines each process, and mentions issues that ought to be taken into account in order to ensure the integrity and admissibility of the image in court. It also mentions that personnel should be familiar with the SOPs mentioned in the SWGDE/SWGIT 'Recommended Guidelines for Developing Standard Operating Procedures' (SWGDE and SWGIT 2004).

2.4.2.4 SWGIT Document Section 5: 'Guidelines for Image Processing' Version 2.1 (2010d)

This document provides guidelines for the use of digital image processing in the criminal justice system. The main objective is to ensure the quality forensic imagery for use as evidence in a court of law. It states the position of SWGIT on image processing for forensic purposes: changes made to an image are accepted if (i) the original image

is preserved, (ii) all processing steps are documented, (iii) the end result is presented as a processed or working copy of the original image and (iv) the recommendations laid out in this document are followed. This document describes advantages, disadvantages and potential limitations of each major process. It also provides guidelines for digital image processing SOPs with a sample SOP for latent print digital imaging.

2.4.2.5 SWGIT Document Section 7: 'Best Practices for Forensic Video Analysis' Version 1.0 (2009)

Forensic video analysis and the sub-discipline of forensic imaging were formally recognized by the International Association for Identification (IAI) in 2002 as a forensic science. The main purpose of this document is to establish suitable procedures for different processing and diagnostic tasks in video examination.

Forensic video analysis (FVA) consists of the examination, comparison and evaluation of video material and footage to be presented as evidence for legal investigations. The general tasks of FVA can be divided into three categories:

1. Technical preparation, which refers to the procedures and methods performed prior to examination, analysis or output (e.g. performing write-protection or visual footage inspections).
2. Examination, which involves the use of image science knowledge to obtain information from video materials (e.g. demultiplexing and decoding).
3. Analysis and interpretation, which are the use of specific knowledge to infer findings from video footage and their content.

The document describes best practice guidance for evidence management, quality assurance and control, security, infrastructure, work management, documentation, training, competency and SOPs. Moreover it describes the workflow for FVA that involves the sequence of all the events taking place during FVA. Finally, the document also presents a video submission form that contains sections necessary for all the information needed to be gathered from the scene and the victim for the investigation.

2.4.2.6 SWGIT Document Section 12: 'Best Practices for Forensic Image Analysis' Version 1.7 (2012b)

Image forensics is considered to be an important forensic discipline that has application in many domains other than the digital forensics field, including intelligence. This document provides personnel with direction regarding procedures performed when images represent the digital evidence under investigation.

Forensic image analysis involves analyzing the image and its content so it can be presented as evidence in court. Moreover, in law enforcement uses of forensic image analysis there are different sub-categories including photogrammetry and image

authentication. As previously mentioned in the forensic video analysis guidelines, forensic image analysis can be divided into three phases:

1. Interpretation, which involves the use of image analysis expertise and specific knowledge to gain insight and identify images themselves, or objects in images in order to produce conclusions about the image(s) which can be used in examination step.
2. Examination, which refers to using image domain expertise to excerpt information from images, or to further characterize the different attributes of an image in order to facilitate interpretation of the image. This ought to produce valid information and interpreted results that should be admissible in a court of law.
3. Technical preparation, which refers to preparing evidence in general for further steps (e.g. examination, analysis or output).

In addition to providing best practice guidelines for evidence management, quality assurance, security, infrastructure, work management, documentation, training and SOPs, the document also provides the workflow for forensic image analysis. Finally, the document provides three examples of how the different phases of image analysis should take place and what outcomes to expect. One is an example of photogrammetric analysis, another is an example of photographic comparison analysis and the last one is an example of content analysis.

2.4.2.7 SWGIT Document Section 13: 'Best Practices for Maintaining the Integrity of Digital Images and Digital Video' Version 1.1 (2012c)

This document presents an overview of different issues affecting digital media files, and lists different methods of maintaining and demonstrating the integrity of such files. Moreover, it offers five workflow examples for maintaining and demonstrating the integrity of digital media files.

2.4.2.8 SWGIT Document Section 15: 'Best Practices for Archiving Digital and Multimedia Evidence in the Criminal Justice System' Version 1.1 (2012a)

This document provides best practice guidelines for archiving digital and multimedia evidence. It discusses the issues involved and provides guidelines of developing an archiving program. It starts by stressing the importance of archiving and why it is needed in organizations handling digital evidence. Furthermore, it outlines the archive creation process and lists the key elements that should be taken into consideration in this process, from security of the archived material through different types of media that can be archived, to media preservation, transmission, management and compression. It also covers archive maintenance by suggesting that new versions of software and hardware should be regularly checked to ensure they can access archived

material which is usually of older versions, thus stressing the importance of reverse compatibility, interoperability and data migration. The last section of the document outlines archive retention periods that includes purging archived material.

2.4.2.9 SWGIT Document Section 16: 'Best Practices for Forensic Photographic Comparison' Version 1.1 (2013a)

This document outlines the appropriate practices to be followed when conducting photographic comparison in image analysis. It defines the purpose of photographic comparison, and emphasizes its importance as a forensic practice in various scientific fields ranging from medical applications to surveillance and intelligence. It also defines the scope of forensic photographic comparisons along with the validity of the comparison that could include a statistical model for reaching conclusions. It also discusses critical aspects of forensic photographic comparison; that include the class versus individual characteristics, the ACE-V protocol (Analysis, Comparison, Evaluation – Verification), recognition of imaging artefacts, and statistical versus cognitive evaluation. Moreover, the document provides guidelines on expertise and experience. It highlights training alone is not sufficient and translation of training into practice requires real-world expertise of qualified personnel. The document provides a rationale for best practices covering bias, selection of images for comparison, comparison processes, reconstruction, levels of findings, photogrammetry and forensic photographic comparison, and photographic documentation as a part of comparison/analysis. A brief outline of evidence management and quality assurance is provided at the end of this document.

2.4.2.10 SWGIT Document Section 17: 'Digital Imaging Technology Issues for the Courts' Version 2.2 (2012d)

This document discusses the proper use of digital imaging technology to judges and attorneys in court. It presents relevant issues in plain language to make them more understandable to the courts. It also covers case laws and research articles dealing with digital imaging technology used within the criminal justice system. In addition, it also addresses some common myths and misconceptions associated with digital imaging technologies.

2.4.2.11 SWGIT Document Section 20: 'Recommendations and Guidelines for Crime Scene/Critical Incident Videography' Version 1.0 (2012e)

This document provides recommendations and guidelines for using video camcorders to document crime scenes and critical incidents. It is suggested that videography be used a supplementary tool to still photography for investigative or demonstrative purposes. The document covers typical incidents that can be documented and equipment needed for the recording. It suggests general documentation and media-handling procedures, and also briefly covers maintenance and training.

2.4.3 ENFSI Working Groups

The only best practice guide from ENFSI on multimedia evidence and multimedia forensics we found is 'Best Practice Guidelines for ENF Analysis in Forensic Authentication of Digital Evidence' released by its Expert Working Group Forensic Speech and Audio Analysis (ENFSI-FSAAWG) in 2009. This was probably the only best practice guide on electric network frequency (ENF) analysis before SWGDE published its guide in 2014. ENF analysis is still a less mature research topic but has found its use in real-world digital forensics laboratories (see Section 1.2.4.2 of Chapter 1 of this book for its use at the Metropolitan Police Service's Digital and Electronics Forensic Service (DEFS) in the United Kingdom).

This ENFSI-FSAAWG ENF analysis guide aims to provide guidelines for FSAAWG members and other forensic laboratories for ENF analysis in the area of forensic authentication of digital audio and audio/video recordings. ENF analysis determines the authenticity of digital audio and video recordings. The document consists of four sections:

1. Quality assurance, which outlines requirements for a technical specialist dealing with ENF analysis, along with an overview of validation requirements for ENF analysis, different categories of software that can be used for forensic analysis, and the equipment to be used.
2. Case assessment, which outlines information requirements for determining authenticity of recorded evidence.
3. Laboratory examination, which outlines analysis protocols and standard procedures to be followed.
4. Evaluation and interpretation, which outlines considerations to be taken into account when handling ENF findings.

2.4.4 UK Law Enforcement

Some key UK law enforcement bodies have produced a number of best practice guides on handling multimedia evidence. They include Association of Chief Police Officers (ACPO), National Policing Improvement Agency (NPIA, ceased to exist in 2012 and most of its activities have been absorbed by the College of Policing), and the Home Office Scientific Development Branch (HOSDB, currently known as the CAST – Centre for Applied Science and Technology). Those guides are tailored to the law enforcement system in the United Kingdom, but can be reasonably generalized to other countries as well. For instance, some of the following reviewed guides are quoted by SWGIT in another guide we reviewed earlier (SWGIT 2012d).

2.4.4.1 ACPO and NPIA 'Practice Advice on Police Use of Digital Images' (2007)

This guide contains five main sections. Section 1 identifies the legal and policy framework within which digital images are managed as police information. Section 2

examines some of the police applications of digital imaging as an evidence resource (including third-party images that are given to the police for use as evidence). Section 3 defines and summarizes the functions of editing and processing images. One important principle is that any editing and processing should be done on a working copy of the original image. Both sections should be read in conjunction with another guide on digital imaging procedure (Cohen and MacLennan-Brown 2007) reviewed in the following text.[15] Section 4 describes the case preparation and disclosure of unused material relating to evidential digital images, and provides information for consideration when revealing exhibit images to the Crown Prosecution Service (CPS) and preparing for the court. Section 5 describes the decision-making process for retaining and disposing of police information, including associated images. This section should be read in conjunction with another guide 'Storage, Replay and Disposal of Digital Evidential Images' (UK HOSDB 2007) reviewed later on in this section.

2.4.4.2 HOSDB and ACPO 'Digital Imaging Procedures' Version 2.1 (2007)

This document is written for practitioners within the UK Police and Criminal Justice System (CJS) involved with the capture, retrieval, storage or use of evidential digital images. It is organized around a flowchart guiding the reader through the whole process including the following steps: (i) initial preparation and capture of images, (ii) transfer and designation of master and working copies, (iii) presentation in court and (iv) retention and disposal of exhibits. The first edition of this guide was published in 2002 and it has undergone a number of revisions. The latest edition recognizes the need to use a broader range of image capturing and storage techniques, and the allowance for the possibility that the Police can store master and working copies on a secure server rather than on physical WORM (write once, read many times) media such as CDs and DVDs.

2.4.4.3 HOSDB 'Storage, Replay and Disposal of Digital Evidential Images' (2007)

This guide focuses on the storage, replay and eventual disposal of evidential digital images generated by the police or those transferred to them from a third party. The term 'evidential' in this guide includes any image generated by, or transferred to the police, even if it is not originally generated as evidence. This document limits its coverage to police units only and leaves the wider issues of transferring images between agencies of the CJS to other guides.

This document sets out a generic framework for thinking about how police units can store, replay and dispose of digital evidential images, and for encouraging a long-term approach to managing the technology. It also provides guidance on some technical issues and some templates for communicating requirements to the wider IT function.

[15] Appendix 1 of this guide also contains a diagram of the procedure (an older edition, Version 2.0).

2.4.4.4 ACPO and NPIA 'Practice Advice on the Use of CCTV in Criminal Investigations' (2011)

This document offers good practice to criminal investigators (who follow the Professionalising Investigation Programme Level 1 and 2) in the use of CCTV images as an investigative tool. Its aim is to provide a comprehensive set of fundamental processes and procedures for acquiring useful and usable CCTV material. This document does not cover roles/responsibilities, specialist techniques, real-time CCTV use or covert use of CCTV.

2.4.4.5 HOSDB and ACPO 'Retrieval of Video Evidence and Production of Working Copies from Digital CCTV Systems' Version 2.0 (2008)

This document provides guidance to technical staff in selecting CCTV methods and systems for effective retrieval and processing of video evidence. One key criterion is that the selected method should maintain evidential integrity so that maximum information is retained. The document is divided into two parts. The first part covers digital video retrieval in its native format from CCTV systems and the creation of master copies of the evidence. The second part focuses on the creation of working copies, particularly where a format conversion is required for further editing and processing purposes.

2.5 Digital Forensics Laboratory Accreditation

For most digital forensics laboratories, accreditation is an important issue because it can give the criminal justice system the needed confidence that the evidence presented in court is handled in a professional manner. According to Beckett and Slay (2011), 'laboratory accreditation is a system of peer assessment and recognition that a laboratory is competent to perform specific tests and calibrations'. The accreditation title does not automatically validate all results produced by an accredited laboratory, but it indicates that the laboratory has implemented a documented quality system so that the results of any forensic examination are repeatable. The core of the accreditation process is 'competence', and it applies to all types of forensic laboratories including the more recently developed digital forensics laboratories.

So far, there are only a few standards and best practice guides on accreditation of digital forensics laboratories. In this section we review those important ones for the digital forensics community.

2.5.1 International Standards

2.5.1.1 ISO/IEC 17025:2005 'General Requirements for the Competence of Testing and Calibration Laboratories'

This international standard is a general one for all types of laboratories, but the general principles can be applied to digital forensics laboratories. It has been followed

widely in the digital forensics community and is the standard selected by the UK Forensic Science Regulator (2011) and by the US ASCLD/LAB (American Society of Crime Lab Directors/Laboratory Accreditation Board). Essentially speaking, this standard is about proving compliance and focuses on documentation of the whole of life process of any analysis performed by a laboratory (Beckett and Slay 2011).

This standard stipulates the procedures and requirements for the competence of calibration and testing laboratories, and it covers procedures that use standard methods non-standards methods, and laboratory-developed methods. It is intended to be used as a sign of competence for laboratories by accreditation bodies, and not as the basis of certification for laboratories. Laboratories or any organization conducting testing and/or calibration that fulfil the requirements stated in this standard will also be conforming to the 'principles' of ISO 9001:2008 standard. Annex A in ISO/IEC 17025:2005 provides a cross-reference between this standard and ISO 9001:2008.

The standard describes the details of management requirements for laboratories, and the associated management system that should be followed in such settings. Moreover, it reviews the process of issuing and reviewing documents for personnel working in the laboratory, and considers the issues of subcontracting services from other parties (which is becoming common as the law enforcement agencies subcontract services from external providers), and the general procedure to be followed. Corrective actions and control of records used in the laboratories are also detailed, and the emphasis of management reviews is stressed (as in the BS 10008 standard reviewed before). In addition, the standard includes recommendations on subcontracting services by laboratories.

2.5.1.2 ISO/IEC 17020:2002 'General Criteria for the Operation of Various Types of Bodies Performing Inspection' (2002)

This international standard covers inspection bodies whose activities include the examination of materials, products, installations, plants, processes, work procedures or services, and the determination of their conformity with requirements and the subsequent reporting of results of these activities to clients and, when required, to authorities. Inspection bodies are different from normal laboratories because the former can actually accredit the latter on behalf of the standardization bodies and authorities. Such bodies are important because they are involved in the laboratory accreditation process and for conducting inspection of crime scenes the laboratory accreditation is insufficient (which means that ISO/IEC 17025 cannot be used).

2.5.1.3 ILAC-G19:2002 'Guidelines for Forensic Science Laboratories' (2002)

This document provides guidance for laboratories involved in forensic analysis and examination by providing application of ISO/IEC 17025. This is useful because ISO/IEC 17025 is not particularly defined for forensic laboratories. ILAC-G19:2002

follows the clause numbers in ISO/IEC 17025 but does not re-state all clauses, so it must be read as a supplementary material to the latter. Another goal of ILAC-G19:2002 is for accreditation bodies to provide appropriate criteria for the assessment and accreditation of forensic laboratories. Since ILAC-G19:2002 covers all forensic science activities, digital forensics is just part of its coverage mainly under the heading 'Audio, Video and Computer Analysis'. Digital forensics may also be involved in some other activities such as 'Computer Simulation', 'Photography' and 'Evidence recovery' under 'Scene Investigation' heading.

2.5.1.4 ILAC-G19:08/2014 'Modules in a Forensic Science Process' (2014)

This is the latest edition of the ILAC-G19 guide, but it is not just a simple extension of the above 2002 edition. Instead, it adds coverage of a new standard ISO/IEC 17020. The title of the guide was also changed to reflect the addition of ISO/IEC 17020. The addition of ISO/IEC 17020 was due to the need for bodies performing crime scene investigation to pass ISO/IEC 17020 rather than ISO/IEC 17025 because the latter is less relevant for crime scene inspection which is better covered by ISO/IEC 17020. For digital forensics laboratories ILAC-G19:08/2014 remains largely the same but the reference to ISO/IEC 17025 was changed from its older edition in 1999 to its latest edition in 2005.

2.5.1.5 SWGDE 'Model Quality Assurance Manual for Digital Evidence Laboratories' Version 3.0 (2012c)

This document provides a model of Quality Assurance Manual (QAM) for any entity performing digital and multimedia forensic examinations. It proposes minimum requirements pertaining to all quality assurance aspects for a forensic laboratory, and it is applicable to an organization of any size including a single examiner. It follows the international standard ISO/IEC 17025:2005, ASCLD/LAB-International 2006 Supplemental Requirements for the Accreditation of Forensic Science Testing Laboratories and American Association for Laboratory Accreditation's 'Explanations for the ISO/IEC 17025 Requirements'. While this document refers to some particular accreditation bodies, it does not endorse one accreditation body over another. Not all sections of the modal QAM are required to fulfil accreditation requirements and all sections are modifiable to suit an organization's need. This document can be used in totality or partially as needed by an organization.

2.6 General Quality Assurance (Management)

In addition to laboratory accreditation, there are also some general quality assurance (management) standards widely used in the digital forensics field because they provide an additional guarantee that the digital forensic process is managed properly. They

include mainly three ISO/IEC international standards which are also widely used in many other sectors.

2.6.1 ISO 9001:2008 'Quality Management Systems – Requirements'

This standard provides the requirements for a quality management system to be implemented by any type of organization, provided it is committed to showing its capability to constantly deliver services/products that conform to customer requirements and other statutory and regulatory requirements. In addition, organizations need to commit themselves to developing and advancing customer satisfaction via efficient implementation of the system. This standard mentions ISO 9000:2005 'Quality management systems – Fundamentals and Vocabulary' as an essential reference for its application.

2.6.2 ISO/IEC 27001:2005 'Information Security Management Systems – Requirements'

This standard presents a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management systems (ISMSs). The ISMSs can be tailored to the specific needs of an organization depending on the nature of business conducted, number of employees and the daily activities taking place in the organization. Moreover, the system should evolve over time to meet the changes in requirements and needs of the organization.

The standard uses the Plan–Do–Check–Act model for continual improvement and management of an ISMS, that also echoes the Organization for Economic Co-operation and Development (OECD) 'Guidelines for the Security of Information Systems and Networks' (2002). In relation to other international standards, this standard is compatible with ISO 9001:2000 reviewed earlier. ISO/IEC 27002 (formerly known as ISO/IEC 17799, see below) is crucial for the application of this standard, and Annex A in this standard derives a considerable amount of material from it.

2.6.3 ISO/IEC 27002:2013 'Code of Practice for Information Security Controls'

Historically, ISO/IEC 27002 was evolved from another standard in a different series and had a different reference number ISO/IEC 17799. After its second edition was published in 2013, the old reference number 17799 became outdated although it is still used in many other standards and documents including ISO/IEC 27001:2005 (which was published around the same time when the first edition of ISO/IEC 27002 was published based on ISO/IEC 17799).

This standard is concerned with all aspects of information security from introduction and implementation to maintenance and development of information security management in any organization. It includes control aims that are designed to be compliant with requirements resulting from a risk assessment. Moreover, it can be used for developing and implementing security management procedures for a given organization.

From a structural viewpoint, this standard is divided into 11 security control sections comprising 39 main security categories and one introductory section illustrating risk assessment and the handling of risks. The 11 security control sections refer to security policy, organizing information security, asset management, human resources security, physical and environmental security, communications and operations management, access control, information systems acquisition development and maintenance, information security incident management, business continuity management and compliance. Moreover, each of the 39 main security categories consists of a control aim outlining what the objectives are, and one or more controls that can be used to fulfil the aim.

Risk assessment plays a major part in this standard. Here, risk assessment is used for identifying and handling security risks in an organization, and should be performed in a systematic manner and regularly. Moreover, the standard contains useful sections for organizations trying to adapt their security controls, for example, Section 10.10 explains how audit logs should be used to monitor the usage of a system and also to assist in future investigations by providing reliable evidence. Finally, it is stated that such controls should be taken into account during the systems and projects requirement specification phase in order to optimize future costs and effective security solutions.

2.7 Training, Education and Certification on Digital and Multimedia Forensics

Training, education and certification of digital forensics examiners and any personnel working on cases involving digital and multimedia evidence are important for digital and multimedia forensics because of the need to ensure legal admissibility of evidence. Some standards and best practice guides particularly focus on these areas in order to provide guidance on how such programs can be managed. In the following, we first review those standards and best practice guides, and then briefly cover existing training, educational and certification programmes known in the digital and multimedia forensic community.

2.7.1 Standards and Best Practice Guides

2.7.1.1 ASTM E2678-09 'Standard Guide for Education and Training in Computer Forensics' (2009)

This standard provides guidance for individuals and students seeking academic and professional qualifications in the field of computer forensics, as well as academic

institutions concerned with introducing forensics programs, and employers who are interested in the academic background of graduates from the computer forensics field. The guide outlines the knowledge, skills, and abilities (i.e. KSAs) necessary for a career in computer forensics, and how academic institutions (in the United States) should aim to provide such elements, by providing a list of model curricula for a variety of degrees including 2-year associate degrees, bachelor degrees, and master degrees in addition to professional certifications. According to SWGDE (2012a), this standard was developed from an NIJ publication.

2.7.1.2 IOCE 'Training Standards and Knowledge Skills and Abilities' (2002b)

This brief document provides principles of training in terms of minimum recommendations for training, minimum training topics, costs and cooperation. It also outlines the core training standards in terms of personnel, qualifications, competence and experience, and the recommended knowledge base. Moreover, it mentions specialized training in terms of court training/legal issues, partnerships and management awareness. The document lists general recommendations regarding training in terms of recommendations for cooperation in training and training for the G-8 24/7 points of contact.

2.7.1.3 Best Practice Guides from US SWGs

SWGDE and SWGIT also published a number of guides on training, proficiency testing and definition of core competencies.

SWGDE/SWGIT 'Guidelines & Recommendations for Training in Digital & Multimedia Evidence' Version 2.0 (2010)
This document provides guidelines for building a suitable training program in forensic digital and multimedia evidence for personnel engaged in evidence handling, collection, analysis and examination. It defines the various job categories involved in such processes, and divides the categories of training into six main ones as follows:

1. Awareness
2. Skills and techniques
3. Knowledge of processes
4. Skills development for legal proceedings
5. Continuing education
6. Specialized applications and technologies

The document provides individual areas focused on training for each specific job category. Moreover, the document outlines aspects for consideration in respect to training needs such as on the job training, continuing education, testimony training, certifications, higher education and training documentation. The last section of the

document focuses on competency and proficiency testing, where it stresses that the examiner should be tested continuously whenever acquiring new skills and techniques for competency. The guidelines states that completed competency tests demonstrate proficiency in a given branch of knowledge.

SWGIT Document Section 6: 'Guidelines and Recommendations for Training in Imaging Technologies in the Criminal Justice System' Version 1.3 (2010c)
Different from SWGDE and SWGIT (2010), this document provides guidelines in proper training on imaging technologies for personnel or laboratories that are *not* performing image analysis or video analysis. This document defines various categories of training and different user categories that include ones unique to the criminal justice system. Moreover, it defines specific areas for focused training for each user category, and basically follows the same flow of information as in SWGDE and SWGIT (2010) for addressing aspects unique to training needs such as on the job training, continuing education, testimony training and certifications.

SWGDE/SWGIT 'Proficiency Test Program Guidelines' Version 1.1 (2006)
This document provides a proficiency test program for digital and multimedia evidence (DME) that would ascertain whether the technical methods used by a forensic examiner are valid and subsequently if the results produced by the examiner conform to a certain quality standard. It can be applied to the following fields: computer forensics, forensic audio, video analysis, and image analysis. This document provides advice on test preparation and design, and then briefly outlines test approval, distribution, testing process, review of test results, documentation and corrective action.

SWGDE 'Core Competencies for Mobile Phone Forensics' Version 1.0 (2013b)
This document identifies the core competencies necessary for handling and forensic processing of mobile phones. It applies to both first responders and laboratory personnel. It discusses different levels of cell phone analysis and the basic skills required at each level, but it does not address core competencies for chip-off or micro-read analysis. The elements covered in this document provide a basis for training, certification, competency and proficiency testing programs.

SWGDE 'Core Competencies for Forensic Audio' Version 1.0 (2011)
Similar to the aforementioned document, this one identifies core competencies necessary for conducting forensic audio functions. It covers the whole process of forensic audio from audio laboratory configuration, to audio evidence collection, to result reporting following needed legal standards. The elements covered in this document also provide a basis for training, certification, competency and proficiency testing programmes on forensic audio.

2.7.2 Certification, Training and Educational Programs

In addition to the above reviewed standards and best practice guides, there are many established training and certification programmes. Some such programmes are run by vendors of digital forensics software such as the EnCE Certification Program run by Guidance Software, Inc., the vendor of the widely used EnCase Forensics software tool, and AccessData BootCamp run by AccessData Group, LLC, the vendor of another widely used software tool Forensic Toolkit (FTK). Some other programs are run by law enforcement bodies such as the Core Skills in Data Recovery and Analysis program run by the UK College of Policing. Another example is the courses offered by the European Cybercrime Training and Education Group (ECTEG) which are for European law enforcement only. For multimedia evidence and forensics, one well-known program is the LEVA Certification Program (LEVA International, Inc. 2014) for forensic examiners handling video evidence.

For UK law enforcement, Appendix C of the ACPO guide (UK ACPO 2011b) contains a list of courses for assisting e-crime managers to train their staff, which include many digital forensics related training courses including higher education degree programs, general training course and product-oriented training programs. The list of courses is not exhaustive, but can reflect what UK law enforcement agencies are doing. Among all the training programs, those provided by National Policing Improvement Agency (NPIA), Centre for Forensic Computing (CFFC) of the Cranfield University, QinetiQ and 7Safe are the main highlights. NPIA was abolished in 2012 and its main activities were absorbed by the College of Policing (CoP) which is currently running former NPIA training courses. The NPIA/CoP Core Skills training courses are among the most fundamental ones in UK law enforcement, for example Surrey Police Digital Forensics Team requires all its technical staff to go through such training courses (see Section 1.3.3).

2.8 Conclusions

Digital and multimedia forensics is a fast evolving field both in terms of technologies involved and legal requirements forensic examiners need to follow. While a lot of international efforts have been made to provide international standards and best practice guides that can be applied to different jurisdictions, the majority of digital forensics practitioners and law enforcement bodies still follow a more national or local approach. For instance, most best practice guides covered in this chapter are made by UK or US law enforcement bodies and criminal justice system themselves, and to some extent the most followed international standards are those for general quality assurance (e.g. ISO/IEC 17025, ISO 9001 and ISO/IEC 27001/27002). This can be explained by the lack of international standards specially made for digital evidence and digital forensics.

The new international standards on digital forensics, that is ISO/IEC 27037, 27041, 27042, 27043, 30121 (most have been officially published as previously reviewed)

have started making a difference as the first set of ISO/IEC standards dedicated to digital evidence and digital forensics. For instance, the Cloud Security Alliance recently published a report on mapping the elements defined in ISO/IEC 27037 to cloud computing (Cloud Security Alliance 2013). We expect after all the above ISO/IEC digital forensics focused standards are officially published, they will play a more active role in digital forensics practice at the national and international levels. We also predict more interactions between international standardization bodies and national bodies which will further develop the above ISO/IEC standards and may also create new standards covering other areas which are currently left out, for example network and cloud forensics.

Four of the above five new standards on digital forensics are in the ISO/IEC 27000 series which is largely about information security management. Those standards are made in the context of information security incident investigation, which however does not cover all areas of digital and multimedia forensics. In addition, as far as we are aware of, currently we are still lacking an international standard on multimedia evidence and multimedia forensics (even though some national standards do exist). We therefore call for more standardization activities in broadening the scope of current/forthcoming ISO/IEC standards, potentially creating a new series covering digital and multimedia forensics which can be based on the rich set of best practice guides as reviewed in this chapter. Furthermore, as acknowledged in the report (UK Forensic Science Regulator 2011), the lack of a more relevant forensic laboratory accreditation standard led to the debate of if ISO/IEC 17025 (plus ILAC-G19) is the 'right' standard the community should go for. This calls the community to work more closely with each other to produce something more tailored towards the needs of digital forensics practitioners and law enforcement.

Another important area to look at is how national jurisdiction and digital forensics practice interact with international ones. Since national best practice guides are currently more accepted at the national level, we do not foresee a rapid change of such practice in the near future. Harmonizing national and international systems can be hard especially for countries following the civil law system. Since most countries following the civil law systems are non-English-speaking countries, we did not focus on any of such countries in this chapter. We plan to focus on non-English-speaking countries in our future research, especially on major European, Asian, Latin American and African countries such as Germany, France, China, Russian, Indian, Japan, Brazil and South Africa. Another interesting group of countries are those in the Middle East and Islamic countries in general as they have very different legal systems but many of them are active in accepting digital evidence. Our current plan is to make use of the book's website to report more about our future research along this line. We also hope this book will have printed future editions so that we can further extend this chapter to cover more national standards and best practice guides on digital and multimedia forensics.

Acknowledgements

Part of this chapter was funded by the UK Home Office's Centre for Applied Science and Technology (CAST) through its research project 'Digital Forensics: Scenarios and Standards' between 2011 and 2012. The authors would like to thank Mr. Ahmad al-Natour who was a research assistant of the UK Home Office funded project and contributed to its final report which covers many standards and best practice guides in this chapter.

References

AccessData Group, LLC 2013 AccessData BootCamp, http://marketing.accessdata.com/acton/attachment/4390/f-044b/1/-/-/-/-/ADBootCamp07-08-2013.pdf (Accessed 17 February 2015).

ASTM International 2009 Standard guide for education and training in computer forensics, ASTM E2678-09, http://www.astm.org/Standards/E2678.htm (Accessed 17 February 2015).

ASTM International 2010 Standard practice for computer forensics, ASTM E2763-10, http://www.astm.org/Standards/E2763.htm (Accessed 17 February 2015).

ASTM International 2012 Standard guide for forensic digital image processing, ASTM E2825-12, http://www.astm.org/Standards/E2825.htm (Accessed 17 February 2015).

Ayers R, Jansen W, Cilleros N and Daniellou R 2005 Cell phone forensic tools: An overview and analysis, NIST Interagency Report 7250, http://csrc.nist.gov/publications/nistir/nistir-7250.pdf (Accessed 17 February 2015).

Ayers R, Jansen W, Moenner L and Delaitre A 2007 Cell phone forensic tools: An overview and analysis update, NIST Interagency Report 7387, http://csrc.nist.gov/publications/nistir/nistir-7387.pdf (Accessed 17 February 2015).

Ayers R, Brothers S and Jansen W 2014 Guidelines on mobile device forensics, NIST Special Publication 800-101 Revision 1, http://www.nist.gov/manuscript-publication-search.cfm?pub_id=915021 (Accessed 17 February 2015).

Beckett J and Slay J 2011 Scientific underpinnings and background to standards and accreditation in digital forensics. *Digital Investigation* **8**(2), 114–121.

Brenner SW and Frederiksen BA 2002 Computer searches and seizures: Some unresolved issues. *Michigan Telecommunications and Technology Law Review* **8**(12), 39–114.

Brezinski D and Killalea T 2002 Guidelines for evidence collection and archiving, IETF RFC 3227, http://tools.ietf.org/html/rfc3227 (Accessed 17 February 2015).

BSI 2008a Evidential weight and legal admissibility of electronic information – Specification, BS 10008:2008, http://shop.bsigroup.com/ProductDetail/?pid=000000000030172973 (Accessed 17 February 2015).

BSI 2008b Evidential weight and legal admissibility of electronic information. compliance workbook for use with BS 10008, BIP 0009:2008, http://shop.bsigroup.com/ProductDetail/?pid=000000000030186720 (Accessed 17 February 2015).

BSI 2008c Evidential weight and legal admissibility of information stored electronically. code of practice for the implementation of BS 10008, BIP 0008-1:2008, http://shop.bsigroup.com/ProductDetail/?pid=000000000030186227 (Accessed 17 February 2015).

BSI 2008d Evidential weight and legal admissibility of information transferred electronically. code of practice for the implementation of BS 10008, BIP 0008-2:2008, http://shop.bsigroup.com/ProductDetail/?pid=000000000030186228 (Accessed 17 February 2015).

BSI 2008e Evidential weight and legal admissibility of linking electronic identity to documents. code of practice for the implementation of BS 10008, BIP 0008-3:2008, http://shop.bsigroup.com/ProductDetail/?pid=000000000030186229 (Accessed 17 February 2015).

Casey E 2007 Editorial: What does "forensically sound" really mean? *Digital Investigation* **4**(2), 49–50.

Cloud Security Alliance 2013 Mapping the forensic standard ISO/IEC 27037 to cloud computing, ISO/IEC 27037:2012, https://downloads.cloudsecurityalliance.org/initiatives/imf/Mapping-the-Forensic-Standard-ISO-IEC-27037-to-Cloud-Computing.pdf (Accessed 17 February 2015).

Cohen N and MacLennan-Brown K 2007 Digital imaging procedures, UK HOSDB Publication No. 58/07, Version 2.1, in association with ACPO, http://tna.europarchive.org/20100413151426/http:/scienceandresearch.homeoffice.gov.uk/hosdb/publications/cctv-publications/DIP_2.1_16-Apr-08_v2.3_%28Web%2947aa.html?view=Standard&pubID=555512 (Accessed 17 February 2015).

Cohen N and MacLennan-Brown K 2008 Retrieval of video evidence and production of working copies from digital CCTV systems, UK HOSDB Publication No. 66/08, Version 2.0, in association with ACPO, http://tna.europarchive.org/20100413151426/http:/scienceandresearch.homeoffice.gov.uk/hosdb/publications/cctv-publications/66-08_Retrieval_of_Video_Ev12835.pdf?view=Binary (Accessed 17 February 2015).

ENFSI 2009 Guidelines for best practice in the forensic examination of digital technology, Version 6.0, http://www.enfsi.eu/sites/default/files/documents/forensic_speech_and_autio_analysis_we_best_practice_guidence_for_enf_analysis_in_forensic_authentication_of_digital_evidence_0.pdf (Accessed 17 February 2015).

ENFSI-FSAAWG 2009 Best practice guidelines for ENF analysis in forensic authentication of digital evidence, http://www.enfsi.eu/sites/default/files/documents/forensic_speech_and_audio_analysis_wg_-_best_practice_guidelines_for_enf_analysis_in_forensic_authentication_of_digital_evidence_0.pdf (Accessed 17 February 2015).

European Cybercrime Training and Education Group 2014 E.C.T.E.G courses, http://www.ecteg.eu/courses.html (Accessed 17 February 2015).

Guidance Software, Inc. 2014 EnCE® certification program, https://www.guidancesoftware.com/training/Pages/ence-certification-program.aspx (Accessed 17 February 2015).

ILAC 2002 Guidelines for forensic science laboratories, ILAC-G19:2002, unavailable on ILAC website any longer, but still downloadable from http://www.nat.hu/dokumentumok/ilac-g19.pdf as of the date of this writing (28 September 2014).

ILAC 2014 Modules in a forensic science process, ILAC-G19:08/2014, http://ilac.org/?ddownload=805 (Accessed 17 February 2015).

Information Security and Forensics Society, Hong Kong, China 2009 Computer forensics Part 2: Best practices, http://www.isfs.org.hk/publications/ISFS_ComputerForensics_part2_20090806.pdf (Accessed 17 February 2015).

IOCE 2002a Guidelines for best practice in the forensic examination of digital technology, Draft V1.0, http://web.archive.org/web/20070812213853/http://www.ioce.org/fileadmin/user_upload/2002/Guidelines\%20for\%20Best\%20Practices\%20in\%20Examination\%20of\%20Digital\%20Evid.pdf (Accessed 17 February 2015).

IOCE 2002b Training standards and knowledge skills and abilities, Draft V1.0, http://www.ioce.org/.

ISO 2008 Quality management systems – Requirements, ISO 9001:2008, http://www.iso.org/iso/catalogue_detail?csnumber=46486 (Accessed 17 February 2015).

ISO/IEC 2002 Conformity assessment – Requirements for the operation of various types of bodies performing inspection, ISO/IEC 17020:2002, http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=52994 (Accessed 17 February 2015).

ISO/IEC 2005 General requirements for the competence of testing and calibration laboratories, ISO/IEC 17025:2005, http://www.iso.org/iso/catalogue_detail.htm?csnumber=39883 (Accessed 17 February 2015).

ISO/IEC 2011 Information technology – Security techniques – Information security incident management, ISO/IEC 27035:2011, http://www.iso.org/iso/catalogue_detail?csnumber=44379 (Accessed 17 February 2015).

ISO/IEC 2012 Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence, ISO/IEC 27037:2012, http://www.iso.org/iso/catalogue_detail?csnumber=44381 (Accessed 17 February 2015).

ISO/IEC 2013a Information technology – Security techniques – Code of practice for information security controls, ISO/IEC 27002:2013, http://www.iso.org/iso/catalogue_detail?csnumber=54534 (Accessed 17 February 2015).

ISO/IEC 2013b Information technology – Security techniques – Information security management systems – Requirements, ISO/IEC 27001:2013, http://www.iso.org/iso/catalogue_detail?csnumber=54534 (Accessed 17 February 2015).

ISO/IEC 2014a Information technology – Security techniques – Guidance on assuring suitability and adequacy of incident investigative methods, ISO/IEC DIS 27041, http://www.iso.org/iso/catalogue_detail.htm?csnumber=44405 (Accessed 17 February 2015).

ISO/IEC 2014b Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence, ISO/IEC DIS 27042, http://www.iso.org/iso/catalogue_detail.htm?csnumber=44406 (Accessed 17 February 2015).

ISO/IEC 2014c Information technology – Security techniques – Incident investigation principles and processes, ISO/IEC FDIS 27043, http://www.iso.org/iso/catalogue_detail.htm?csnumber=44407 (Accessed 17 February 2015).

ISO/IEC 2014d System and software engineering – Information technology – Governance of digital forensic risk framework, ISO/IEC FDIS 30121, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=53241 (Accessed 17 February 2015).

Jansen W and Ayers R 2004 Guidelines on PDA forensics, recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-72, http://www.nist.gov/manuscript-publication-search.cfm?pub_id=150217 (Accessed 17 February 2015).

Jansen W and Delaitre A 2009 Mobile forensic reference materials: A methodology and reification, NIST Interagency Report 7617, http://csrc.nist.gov/publications/nistir/ir7617/nistir-7617.pdf (Accessed 17 February 2015).

Kent K, Chevalier S, Grance T and Dang H 2006 Guide to integrating forensic techniques into incident response, NIST Special Publication 800-86, http://www.nist.gov/manuscript-publication-search.cfm?pub_id=50875 (Accessed 17 February 2015).

LEVA International, Inc. 2014 LEVA certification program, https://leva.org/index.php/certification (Accessed 17 February 2015).

McKemmish R 2008 When is digital evidence forensically sound? In *Advances in Digital Forensics IV* (ed. Ray I and Shenoi S), vol. 285 of *IFIP – The International Federation for Information Processing*, pp. 3–15, Springer.

NIST 2010 Smart phone tool specification, Version 1.1, http://www.cftt.nist.gov/documents/Smart_Phone_Tool_Specification.pdf (Accessed 17 February 2015).

Nolan R, Baker M, Branson J, Hammerstein J, Rush K, Waits C and Schweinsberg E 2005a First responders guide to computer forensics: Advanced topics, Carnegie Mellon Software Engineering Institute, CERT Training and Education Handbook CMU/SEI-2005-HB-003, http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=7261 (Accessed 17 February 2015).

Nolan R, O'Sullivan C, Branson J and Waits C 2005b First responders guide to computer forensics, Carnegie Mellon Software Engineering Institute CERT Training and Education Handbook, CMU/SEI-2005-HB-001, http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=7251 (Accessed 17 February 2015).

OECD 2002 Guidelines for the security of information systems and networks: Towards a culture of security, http://www.oecd.org/internet/ieconomy/15582260.pdf (Accessed 17 February 2015).

Project on Scientific Knowledge and Public Policy 2003 Daubert: The most influential supreme court ruling you've never heard of, http://defendingscience.org/sites/default/files/upload/Daubert-The-

Most-Influential-Supreme-Court-Decision-You-ve-Never-Heard-Of-2003.pdf (Accessed 17 February 2015).

Shirey R 2000 Internet security glossary, IETF RFC 2828, http://tools.ietf.org/html/rfc2828 (Accessed 17 February 2015).

Sommer P 2005 Directors and corporate advisors' guide to digital investigations and evidence, 1st edition, published by Information Assurance Advisory Council (IAAC), http://www.iaac.org.uk/media/1146/evidence-of-cyber-crime-v12-rev.pdf (Accessed 17 February 2015).

Sommer P 2012 Digital evidence, digital investigations, and e-disclosure: A guide to forensic readiness for organisations, security advisers and lawyers, 3rd edition, published by Information Assurance Advisory Council (IAAC), http://cryptome.org/2014/03/digital-investigations.pdf (Accessed 17 February 2015).

Sommer P 2013 Digital evidence, digital investigations, and e-disclosure: A guide to forensic readiness for organisations, security advisers and lawyers, 4th edition, published by Information Assurance Advisory Council (IAAC), http://www.iaac.org.uk/media/1347/iaac-forensic-4th-edition.pdf (Accessed 17 February 2015).

SWGDE 2006 SWGDE digital evidence findings, Version 1.0, https://www.swgde.org/documents/Current%20Documents/2006-04-12%20SWGDE%20Digital%20Evidence%20Findings (Accessed 17 February 2015).

SWGDE 2008 Peer to peer technologies, Version 1.0, https://www.swgde.org/documents/Current%20Documents/2008-01-30%20SWGDE%20Peer%20to%20Peer%20Technologies%20v1.0 (Accessed 17 February 2015).

SWGDE 2010 SWGDE minimum requirements for quality assurance in the processing of digital and multimedia evidence, Version 1.0, https://www.swgde.org/documents/Current%20Documents/2010-05-15%20SWGDE%20Min%20Req%20for%20QA%20in%20Proc%20Digital%20Multimedia%20Evidence_v1 (Accessed 17 February 2015).

SWGDE 2011 SWGDE core competencies for forensic audio, Version 1.0, https://www.swgde.org/documents/Current%20Documents/2011-09-15%20SWGDE%20Core%20Competencies%20for%20Forensic%20Audio%20v1.pdf (Accessed 17 February 2015).

SWGDE 2012a Foundational forensic science annotated bibliographies requested by RDT-E IWG SWGDE's reply to RDT&E IWG letter, https://www.swgde.org/documents/Current%20Documents/Foundational%20Forensic%20Science%20Annotated%20Bibliographies%20Requested%20by%20RDT-E%20IWG (Accessed 17 February 2015).

SWGDE 2012b SWGDE best practices for portable gps device examinations, Version 1.1, https://www.swgde.org/documents/Current%20Documents/2012-09-12%20SWGDE%20Best%20Practices%20for%20Portable%20GPS%20GPS%20Devices%20V1-1 (Accessed 17 February 2015).

SWGDE 2012c SWGDE model quality assurance manual for digital evidence laboratories, Version 3.0, https://www.swgde.org/documents/Current%20Documents/SWGDE%20QAM%20and%20SOP%20Manuals/2012-09-13%20SWGDE%20Model%20QAM%20for%20Digital%20Evidence%20Laboratories-v3.0 (Accessed 17 February 2015).

SWGDE 2012d SWGDE model standard operation procedures for computer forensics Version 3.0, https://www.swgde.org/documents/Current%20Documents/SWGDE%20QAM%20and%20SOP%20Manuals/2012-09-13%20SWGDE%20Model%20SOP%20for%20Computer%20Forensics%20v3 (Accessed 17 February 2015).

SWGDE 2013a SWGDE best practices for vehicle navigation and infotainment system examinations, Version 1.0, https://www.swgde.org/documents/Current%20Documents/2013-02-11%20SWGDE%20Best%20Practices%20for%20Vehicle%20Navigation%20and%20Infotainment%20System%20Examinations%20V1-0 (Accessed 17 February 2015).

SWGDE 2013b SWGDE core competencies for mobile phone forensics, Version 1.0, https://www.swgde.org/documents/Current%20Documents/2013-02-11%20SWGDE%20Core%20Competencies%20for%20Mobile%20Phone%20Forensics%20V1-0 (Accessed 17 February 2015).

SWGDE 2014a SWGDE best practices for computer forensics Version 3.1, https://www.swgde.org/documents/Current%20Documents/2014-09-05%20SWGDE%20Best%20Practices%20for%20Computer%20Forensics%20V3-1 (Accessed 17 February 2015).

SWGDE 2014b SWGDE best practices for examining magnetic card readers, Version 1.0, https://www.swgde.org/documents/Current%20Documents/2014-06-11%20SWGDE%20Best%20Practices%20for%20Credit%20Card%20Skimmers (Accessed 17 February 2015).

SWGDE 2014c SWGDE best practices for forensic audio, Version 2.0, https://www.swgde.org/documents/Current%20Documents/2014-09-08%20SWGDE%20Best%20Practices%20for%20Forensic%20Audio%20V2 (Accessed 17 February 2015).

SWGDE 2014d SWGDE best practices for handling damaged hard drives, Version 1.0, https://www.swgde.org/documents/Current%20Documents/2014-09-05%20SWGDE%20Best%20Practices%20for%20Handling%20Damaged%20Hard%20Drives (Accessed 17 February 2015).

SWGDE 2014e SWGDE best practices for mobile phone forensics, Version 2.0, https://www.swgde.org/documents/Current%20Documents/2013-02-11%20SWGDE%20Best%20Practices%20for%20Mobile%20Phone%20Forensics%20V2-0 (Accessed 17 February 2015).

SWGDE 2014f SWGDE capture of live systems Version 2.0, https://www.swgde.org/documents/Current%20Documents/2014-09-05%20SWGDE%20Capture%20of%20Live%20Systems%20V2-0 (Accessed 17 February 2015).

SWGDE 2014g SWGDE electric network frequency discussion paper, Version 1.2, https://www.swgde.org/documents/Current%20Documents/2014-02-06%20SWGDE%20Electric%20Network%20Frequency%20Discussion%20Paper%20v1-2 (Accessed 17 February 2015).

SWGDE 2014h SWGDE focused collection and examination of digital evidence, Version 1.0, https://www.swgde.org/documents/Current%20Documents/2014-09-05%20SWGDE%20Focused%20Collection%20and%20Examination%20of%20Digital%20Evidence (Accessed 17 February 2015).

SWGDE 2014i SWGDE Mac OS X tech notes, Version 1.1, https://www.swgde.org/documents/Current%20Documents/2014-09-05%20SWGDE%20Mac%20OS%20X%20Tech%20Notes%20V1-1 (Accessed 17 February 2015).

SWGDE 2014j SWGDE recommended guidelines for validation testing, Version 2.0, https://www.swgde.org/documents/Current%20Documents/2014-09-05%20SWGDE%20Recommended%20Guidelines%20for%20Validation%20Testing%20V2-0 (Accessed 17 February 2015).

SWGDE 2014k SWGDE UEFI and its effect on digital forensics imaging, Version 1.0, https://www.swgde.org/documents/Current%20Documents/2014-02-06%20SWGDE%20UEFI%20Effect%20on%20Digital%20Imaging%20V1 (Accessed 17 February 2015).

SWGDE and SWGIT 2004 SWGDE/SWGIT recommended guidelines for developing standard operating procedures, Version 1.0, https://www.swgit.org/pdf/Recommended%20Guidelines%20for%20Developing%20Standard%20Operating%20Procedures?docID=59 (Accessed 17 February 2015).

SWGDE and SWGIT 2006 SWGDE/SWGIT proficiency test program guidelines, Version 1.1, https://www.swgit.org/pdf/Proficiency%20Test%20Program%20Guidelines?docID=58 (Accessed 17 February 2015).

SWGDE and SWGIT 2010 SWGDE/SWGIT guidelines & recommendations for training in digital & multimedia evidence, Version 2.0, https://www.swgit.org/pdf/Guidelines%20and%20Recommendations%20for%20Training%20in%20Digital%20and%20Multimedia%20Evidence?docID=57 (Accessed 17 February 2015).

SWGIT 2009 Best practices for forensic video analysis, SWGIT Document Section 7, Version 1.0, https://www.swgit.org/pdf/Section%205%20Guidelines%20for%20Image%20Processing?docID=49 (Accessed 17 February 2015).

SWGIT 2010a Best practices for automated image processing, SWGIT Document Section 18, Version 1.0, https://www.swgit.org/pdf/Section%2018%20Best%20Practices%20for%20Automated%20Image%20Processing?docID=41 (Accessed 17 February 2015).

SWGIT 2010b Best practices for documenting image enhancement, SWGIT Document Section 11, Version 1.3, https://www.swgit.org/pdf/Section%2011%20Best%20Practices%20for%20Documenting%20Image%20Enhancement?docID=37 (Accessed 17 February 2015).

SWGIT 2010c Guidelines and recommendations for training in imaging technologies in the criminal justice system, SWGIT Document Section 6, Version 1.3, https://www.swgit.org/pdf/Section%206%20Guidelines%20and%20Recommendations%20for%20Training%20in%20Imaging%20Technologies%20in%20the%20Criminal%20Justice%20System?docID=50 (Accessed 17 February 2015).

SWGIT 2010d Guidelines for image processing, SWGIT Document Section 5, Version 2.1, https://www.swgit.org/pdf/Section%205%20Guidelines%20for%20Image%20Processing?docID=49 (Accessed 17 February 2015).

SWGIT 2010e Overview of swgit and the use of imaging technology in the criminal justice system SWGIT Document Section 1, Version 3.3, https://www.swgit.org/pdf/Section%201%20Overview%20of%20SWGIT%20and%20the%20Use%20of%20Imaging%20Technology%20in%20the%20Criminal%20Justice%20System?docID=35 (Accessed 17 February 2015).

SWGIT 2011 Issues relating to digital image compression and file formats, SWGIT Document Section 19, Version 1.1, https://www.swgit.org/pdf/Section%2019%20Issues%20Relating%20to%20Digital%20Image%20Compression%20and%20File%20Formats?docID=42 (Accessed 17 February 2015).

SWGIT 2012a Best practices for archiving digital and multimedia evidence (DME) in the criminal justice system, SWGIT Document Section 15, Version 1.1, https://www.swgit.org/pdf/Section%2015%20Best%20Practices%20for%20Archiving%20Digital%20and%20Multimedia%20Evidence%20%28DME%29%20in%20the%20Criminal%20Justice%20System?docID=55 (Accessed 17 February 2015).

SWGIT 2012b Best practices for forensic image analysis, SWGIT Document Section 12, Version 1.7, https://www.swgit.org/pdf/Section%2012%20Best%20Practices%20for%20Forensic%20Image%20Analysis?docID=38 (Accessed 17 February 2015).

SWGIT 2012c Best practices for maintaining the integrity of digital images and digital video, SWGIT Document Section 13, Version 1.1, https://www.swgit.org/pdf/Section%2013%20Best%20Practices%20for%20Maintaining%20the%20Integrity%20of%20Digital%20Images%20and%20Digital%20Video?docID=54 (Accessed 17 February 2015).

SWGIT 2012d Digital imaging technology issues for the courts, SWGIT Document Section 17, Version 2.2, https://www.swgit.org/pdf/Section%2017%20Digital%20Imaging%20Technology%20Issues%20for%20the%20Courts?docID=56 (Accessed 17 February 2015).

SWGIT 2012e Recommendations and guidelines for crime scene/critical incident videography, SWGIT Document Section 20, Version 1.0, https://www.swgit.org/pdf/Section%2020%20Recommendations%20and%20Guidelines%20for%20Crime%20Scene%20and%20Critical%20Incident%20Videography?docID=44 (Accessed 17 February 2015).

SWGIT 2012f Recommendations and guidelines for using closed-circuit television security systems in commercial institutions, SWGIT Document Section 4, Version 3.0, https://www.swgit.org/pdf/Section%204%20Recommendations%20and%20Guidelines%20for%20Using%20Closed-Circuit%20Television%20Security%20Systems%20in%20Commercial%20Institutions?docID=48 (Accessed 17 February 2015).

SWGIT 2013a Best practices for forensic photographic comparison, SWGIT Document Section 16, Version 1.1, https://www.swgit.org/pdf/Section%2016%20Best%20Practices%20for%20Forensic%20Photographic%20Comparison?docID=40 (Accessed 17 February 2015).

SWGIT 2013b Best practices for image authentication, SWGIT Document Section 14, Version 1.1, https://www.swgit.org/pdf/Section%2014%20Best%20Practices%20for%20Image%20Authentication?docID=39 (Accessed 17 February 2015).

SWGIT 2013c Best practices for the analysis of digital video recorders, SWGIT Document Section 23 Version 1.0, https://www.swgit.org/pdf/Section%2023%20Best%20Practices%20for%

20the%20Analysis%20of%20Digital%20Video%20Recorders?docID=117. The publication date of the document shown in the document itself (11 June 2012) does not match the one shown on the SWGIT general document page, https://www.swgit.org/documents/Current%20Documents (11 January 2013). We use the latter one because the PDF file was generated in June 2013.

SWGIT 2013d Best practices for the retrieval of digital video, SWGIT Document Section 24, Version 1.0, https://www.swgit.org/pdf/Section%2024%20Best%20Practices%20for%20the%20Retrieval%20of%20Digital%20Video?docID=141 (Accessed 17 February 2015).

UK ACPO 1999 ACPO good practice guide for computer based evidence, Version 2.0, http://www.swgit.org.history.

UK ACPO 2003 ACPO good practice guide for computer-based electronic evidence, Version 3.0, http://web.archive.org/web/20050525143019/http://www.acpo.police.uk/asp/policies/Data/gpg_computer_based_evidence_v3.pdf (Accessed 17 February 2015).

UK ACPO 2007 ACPO good practice guide for computer-based electronic evidence, Version 4.0, published by 7Safe, http://www.7safe.com/electronic_evidence/ (Accessed 17 February 2015).

UK ACPO 2011a ACPO good practice guide for digital evidence, Version 5.0, http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf (Accessed 17 February 2015).

UK ACPO 2011b ACPO good practice guide for managers of e-crime investigation, Version 0.1.4, http://www.acpo.police.uk/documents/crime/2011/201103CRIECI14.pdf (Accessed 17 February 2015).

UK ACPO and NPIA 2007 Practice advice on police use of digital images, http://www.acpo.police.uk/documents/crime/2011/20111014%20CBA%20practice_advice_police_use_digital_images_18x01x071.pdf (Accessed 17 February 2015).

UK ACPO and NPIA 2011 Practice advice on the use of CCTV in criminal investigtions, http://www.acpo.police.uk/documents/crime/2011/20110818%20CBA%20CCTV_Final_Locked.pdf (Accessed 17 February 2015).

UK College of Policing 2014 Core skills in data recovery and analysis, http://www.college.police.uk/en/1262.htm (Accessed 17 February 2015).

UK Forensic Science Regulator 2011 Codes of practice and conduct for forensic science providers and practitioners in the criminal justice system, Version 1.0, https://www.gov.uk/government/publications/forensic-science-providers-codes-of-practice-and-conduct (Accessed 17 February 2015).

UK HOSDB 2007 Storage, replay and disposal of digital evidential images, Publication No. 53/07, Version 1.0, in association with ACPO and NPIA, http://library.college.police.uk/docs/APPref/storage-replay-and-disposal.pdf (Accessed 17 February 2015).

United States Secret Service, US Department of Homeland Security 2007 Best practices for seizing electronic evidence: A pocket guide for first responders, Version 3.0, http://www.forwardedge2.com/pdf/bestPractices.pdf (Accessed 17 February 2015).

US DOJ's Computer Crime and Intellectual Property Section 2002 Searching and seizing computers and obtaining electronic evidence in criminal investigations, 2nd edition, http://cdn.ca9.uscourts.gov/datastore/library/2013/02/26/CDT_cyber.pdf (Accessed 17 February 2015).

US DOJ's Computer Crime and Intellectual Property Section 2009 *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* OLE Litigation Series 3rd edn.. Office of Legal Education (OLE) & Executive Office for United States Attorneys (EOUSA). http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf (Accessed 17 February 2015).

US FBI 2007 Digital evidence field guide, Version 1.1, http://www.rcfl.gov/downloads/documents/digital-evidence-field-guide/ (Accessed 17 February 2015).

US FBI 2010 Mobile forensics field guide, Version 2.0, http://www.rcfl.gov/continuing-education-series/products/field-guides (Accessed 17 February 2015).

US Federal Judicial Center 2003 Computer-based investigation and discovery in criminal cases: A guide for united states magistrate judges, National Workshop for Magistrate Judges II, http://www.fjc.gov/public/pdf.nsf/lookup/CompInve.pdf/$file/CompInve.pdf (Accessed 17 February 2015).

US NIJ 2004 Forensic examination of digital evidence: A guide for law enforcement, Special Report NCJ 199408, https://www.ncjrs.gov/pdffiles1/nij/199408.pdf (Accessed 17 February 2015).

US NIJ 2007a Digital evidence in the courtroom: A guide for law enforcement and prosecutors, Special Report NCJ 211314, https://www.ncjrs.gov/pdffiles1/nij/211314.pdf (Accessed 17 February 2015).

US NIJ 2007b Investigations involving the internet and computer networks, Special Report NCJ 210798, https://www.ncjrs.gov/pdffiles1/nij/210798.pdf (Accessed 17 February 2015).

US NIJ 2007c Investigative uses of technology: Devices, tools, and techniques, Special Report NCJ 213030, https://www.ncjrs.gov/pdffiles1/nij/213030.pdf (Accessed 17 February 2015).

US NIJ 2008 Electronic crime scene investigation: A guide for first responders, 2nd edition, Special Report NCJ 219941, http://www.nij.gov/publications/ecrime-guide-219941/ (Accessed 17 February 2015).

US NIJ 2009 Electronic crime scene investigation: An on-the-scene reference for first responders, Special Report NCJ 227050, https://www.ncjrs.gov/pdffiles1/nij/227050.pdf (Accessed 17 February 2015).