The Next Generation for the Forensic Extraction of Electronic Evidence from Mobile Telephones

Hayson K. S. Tse, K. P. Chow and Michael Y. K. Kwan
Department of Computer Science
The University of Hong Kong, Pokfulam
Hong Kong, Republic of China
{hkstse, chow, ykkwan}@cs.hku.hk

***Abstract*—Electronic evidence extracted from a mobile telephone provide a wealth of information about the user. Before a court allows the trier of fact to consider the electronic evidence, the court must ensure that the subject matter, testimony of which is to be given, is scientific. Therefore, regard must, at the investigation stage, be given to fulfill the requirements of science and law, including international standards. Such compliance also moves the extraction of electronic evidence from mobile telephones into the next generation, a more rigorous position as a forensic science, by being able to give in court well- reasoned and concrete claims about the accuracy and validity of conclusions.**

Keywords—electronic evidence; science and law; mobile telephone; international standards.

I. INTRODUCTION

In 1857, Clark Maxwell propounded the theory of electromagnetic radiation. In 1901, G. Marconi invented trans-Atlantic radio transmission by the use of electromagnetic waves. In the late 1940s in the United States, and in early 1950s in Europe, the first systems offering mobile telephone service in cars were introduced. Now, the Fourth Generation (4G) systems are being rolled out by some companies.

The use of mobile telephones has increased significantly which resulted in creation of new lifestyles. According to a worldwide report in 2012 [18], there were fewer than 1 billion mobile subscriptions in use worldwide in 2000. But in 2011, there were over 6 billion mobile subscriptions. That means three out of every four human beings use a mobile telephone in 2011 worldwide. Further, more than 30 billion mobile applications were downloaded in 2011. According to a 2013 report in China [8], China had 420 million mobile Internet users by the end of December 2012. Those who used mobile telephones to access the Internet increased from 69.3% at the end of 2011 to 74.5%. On the other hand, the ratio of Internet users using desktop computers dropped to 70.6% by nearly 3% over the end of 2012. The ratio of Internet users using laptop computers also dropped slightly to 45.9% when compared with the figure at the end of 2012. Compared with 2011, the proportion of mobile telephone Internet users shopping online via mobile telephones grew by 6.6%. In addition, the proportion of mobile telephone group shopping users went up 1.7%. Mobile telephone online payment also went up 4.6%. Mobile telephone online banking went up 4.7%. The users of these three types of mobile applications grew by more than 80%.

Due to the prevalence and proliferation of mobile telephones, forensic extraction of electronic evidence from mobile telephones has grown in scope and size. As the use of mobile telephones grows, more electronic evidence and information which are important to investigations will be found on them. Further, each technical advance in the capabilities of mobile telephones from the first generation to 4G offers greater opportunity for the extraction of additional electronic information.

Extraction of electronic evidence for the purpose of crime detection has been argued as still in its infancy [17]. Modi operandi of cyber criminals change. These have led to debates regarding the adequacy of current technical investigation models, examination tools and the capability of law enforcement to tackle cybercrime. The process or procedure adopted in performing extraction of electronic evidence has a direct influence on the outcome of the extraction. Choosing inappropriate processes may lead to incomplete or missing electronic evidence. Bypassing one step or interchanging any of the steps may lead to inconclusive results and invalid conclusions. Electronic evidence which are non-scientifically captured may become inadmissible in the court of law [32] [25].

A number of requirements are to be met before a court considers admissible electronic evidence extracted from mobile telephones, including the expert opinion given on the bases of those evidence. It must be demonstrated to the court that the subject matter, extraction of electronic data from mobile telephones, falls within a scientific domain. This requires interactions amongst electronic data, science and legal jurisprudence. By satisfying the requirements of science and law, including international standards, practitioners of extraction of electronic evidence from mobile telephones will move mobile telephones investigation into the next generation, a more rigorous position as a forensics science. Practitioners will be able to make well-reasoned and concrete assertions about the accuracy and validity of hypotheses presented in court.

In the ensuing section, this paper examines the common requirements of forensic extraction of electronic evidence from

Sponsored by IEEE Louisville Chapter.
978-1-4799-4061-5/13/$31.00 ©2013 IEEE

mobile telephones in various jurisdictions and international requirements. Next, the challenges are discussed. Finally, this paper concludes with the way forward.

II. Mobile Telephone Forensics And Requirements

For extraction of electronic evidence from mobile telephones to grow and to be accepted as part of forensics science, regard must be given to the requirements of science and law, including international standards. There are reasons for this assertion.

A. *"Forensics"*

First, the word "forensics" is intertwined with the requirements of law. The word "forensics" derives from the Latin word "forensis", which means "forum". "Forum" means "in open court or public" [28] and refers to a location, a public square or market- place used for judicial and other business. The contemporary use of the word "forensics" has been developed to its usage in relation to law. The word refers to the scientific tests or techniques which are used for the detection of crimes for the purpose of court proceedings.

The purpose of court proceedings has always been highlighted in relation to "forensic". Many computer scientists described the word "forensics" as "a process of logging, collecting, and auditing or analyzing data in a post hoc investigation" [24]. Reference [12] defined computer forensic as the identification, preservation, and the analysis of information stored, transmitted, or produced by a computer system or computer network. Its main purpose is to establish the validity of the hypotheses used in an attempt to explain the circumstances or the cause of an activity under investigation. Reference [7] described "forensic" as any professional practice that provides scientific knowledge to the court or trier of fact.

The phrase "digital forensics" is largely used interchangeably with computer forensics. But the former term implies the inclusion of devices other than general-purpose computer systems, such as network devices, mobile telephones, and other devices with embedded systems.

B. *Similarity between Science and Law*

Second, reference [27] found a fundamental similarity of thought, amongst differences, between the field of science and law. Science and law have used completely different language to describe the same things when they explain decision-making under uncertainties. Despite the differences in language, science and law have also recognized, formalized and adopted approaches that are identical in important aspects. One example cited by [27] is the model of hypothesis testing, which is one of the methods common to crime investigation and judicial proof. The process of judicial proof is the accruing of evidence to confirm or deny hypotheses about current or past events relevant to a legal case [20]. Accordingly, scientific attitude should be applied to all phases of a crime investigative process and presentation of evidence in courts. As an example, mobile forensics investigators answered scientific and legal questions [24] in the course of investigation and analysis:.

- Who attacked this device?
- What actions did the attacker take?
- What was the consequence of each of those actions?
- With what degree of certainty, and under what assumptions, were these assertions made?
- Will these assertions be acceptable in a court?

Third, we can observe the developments of computer forensics. Computer scientists have taken steps to turn computer forensics into a more rigorous position as a science. Scientific disciplines carry out researches in ways that are scientifically valid. The scientific process adopted to validate computer forensics research techniques are [24]:

- Define the question;
- Form a hypothesis;
- Perform an experiment and collect data;
- Analyze the data;
- Interpret the data and draw conclusions that serve as a starting point for new hypotheses;
- Publish the results (return to item 3 and iterate).

Similarly, mobile telephone investigators must make well-reasoned and concrete claims about the accuracy and validity of conclusions presented in court [24]. In so doing, mobile telephone investigators attempt to answer questions including [24]:

- How accurate is the method used to produce the data?
- How accurate is the method used to analyze the data?
- What claims can be made about the data?
- What assumptions must be made to make those claims?
- What can be done to reduce the amount of assumptions that must be made to use the data?

On the bases of the answers to the above questions, a trier of fact determines the evidence to be believed, the weight to be assigned to the evidence, and the conclusion to be reached on the bases of the evidence.

C. *Scientific, independence and reviewability*

Fourth, courts are "gatekeepers". A trier of fact considers the relevance and weight of evidence. But before the evidence can be placed before the trier of fact, the proponent must prove that the evidence is authentic, which means "evidence sufficient to support a finding that the matter in question is what the proponent claims" [26]. Courts must ensure that the subject matter, testimony of which is to be given, is genuinely scientific. The question, regarding whether or not a domain is considered as an admissible subject of evidence to be given by an expert, is distinct from the question of whether or not a witness qualifies as an expert. We summarize the principles in four legal jurisdictions, the United States, the United Kingdom, Hong Kong and China. They have the common requirements of scientific, independence and reviewability.

Frye v. United States [13] was the first American appellate decision to set out a special standard to decide whether or not a subject matter was an area of scientific expertise. Frye was a case concerning the admissibility of blood pressure deception tests. In 1923, scientists had not generally accepted those tests. In 1923, the United States Court of Appeals for the D.C. Circuit held that the evidence of a scientific expert was admissible if the subject of the evidence was based on a discovery or principle that had gained general acceptance in the field in which it belonged. This "general acceptance test" is a stringent admissibility standard.

Years later, rule 702 of the 1975 United States Federal Rule of Evidence set down a more liberal standard. According to rule 702, expert scientific or technical opinions are admissible in evidence if they are relevant and helpful to the judge or a trier of fact in deciding the facts of the case. Rule 702 provides that an expert (by knowledge, skill, experience, training, or education) may testify about scientific, technical, or other specialized knowledge if:

- The testimony is based upon sufficient facts or data;
- The testimony is the product of reliable principles and methods; and
- The witness has applied the principles and methods reliable to the facts of the case.

Who should prevail, Frye or rule 702? In 1993, in *Daubert v. Merrell Dow Pharmaceuticals, Inc.* [10], the issue was whether or not evidence, on the bases of the methodologies in animal studies and pharmacological studies which had not gained acceptance within general scientific areas, was admissible. The U.S. Supreme Court held that, on a proper interpretation, rule 702 of the 1975 Federal Rules of Evidence had superseded Frye. The U.S. Supreme Court also endorsed an alternative approach for deciding the admissibility of scientific evidence under the Federal Rules. In order to be reliable, expert testimony must be derived by scientific method and supported by appropriate validation. The Supreme Court set out several non-exclusive factors that courts may consider in deciding what amounts to "scientific knowledge" and in evaluating the reliability of scientific, technical and other evidence supported by expert evidence:

- Whether the theories and techniques employed by the scientific expert have been tested;
- Whether they have been subjected to peer review and publication;
- Whether the techniques employed by the expert have a known error rate;
- Whether they are subject to standards governing their application; and
- Whether the theories and techniques employed by the expert enjoy widespread acceptance.

In the United Kingdom, the judicial approach to the admissibility of expert evidence is one of laizzez-faire. Expert opinion is admissible without adequate scrutiny. No clear test is being applied to determine whether the evidence is sufficiently reliable. In 2011, the United Kingdom Law Reform Commission published a report to explain the recommendations for reforming the law relating to expert evidence in criminal proceedings [29]. The Commission also provided a draft Criminal Evidence (Experts) Bill which, if enacted, would give effect to the principal recommendations.

Section 4 of the draft bill provides:

"1. Expert opinion evidence is sufficiently reliable to be admitted if:

a) the opinion is soundly based, and

b) the strength of the opinion is warranted having regard to the grounds on which it is based.

2. Any of the following, in particular, could provide a reason for determining that expert opinion evidence is not sufficiently reliable

a) the opinion is based on a hypothesis which has not been subjected to sufficient scrutiny (including, where appropriate, experimental or other testing), or which has failed to stand up to scrutiny;

b) The opinion is based on an unjustifiable assumption;

c) The opinion is based on flawed data;

d) The opinion relies on an examination, technique, method or process which was not properly carried out or applied, or was not appropriate for use in the particular case;

e) The opinion relies on an inference or conclusion which has not been properly reached.

3. When assessing the reliability of expert opinion, the court must have regard to

a) Such of the generic factors set out in Part 1 of the Schedule as appear to the court to be relevant;

b) If any factors have been specified in an order made under Part 2 of the Schedule in relation to a particular field, such of those factors as appear to the court to be relevant;

c) Anything else which appears to the court to be relevant."

Part 1 of the Schedule provides:

"1. The factors referred to in section 4(3)(a) are as follows:

a) The extent and quality of the data on which the opinion is based, and the validity of the methods by which they were obtained.

b) If the opinion relies on an inference from any findings, whether the opinion properly explains how safe or unsafe the inference is (whether by reference to statistical significance or in other appropriate terms).

c) If the opinion relies on the results of the use of any method (for instance, a test, measurement or survey), whether the opinion takes proper account of matters, such as the degree of precision or margin of uncertainty, affecting the accuracy or reliability of those results.

d) The extent to which any material upon which the opinion is based has been reviewed by others with relevant expertise (for instance, in peer-reviewed publications), and the views of those others on that material.

e) The extent to which the opinion is based on material falling outside the expert's own field of expertise.

f) The completeness of the information which was available to the expert, and whether the expert took account of all relevant information in arriving at the opinion (including information as to the context of any facts to which the opinion relates).

g) Whether there is a range of expert opinion on the matter in question; and, if there is, where in the range the opinion lies and whether the experts' preference for the opinion proffered has been properly explained.

h) Whether the experts' methods followed established practice in the field; and, if they did not, whether the reason for the divergence has been properly explained.

2. These factors are not arranged in any hierarchical order."

In Hong Kong, if a court is to accept the evidence of a scientific theory, novel or not, four principles must be fulfilled. The principles are summarized by the Court of First Instance of the High Court of Hong Kong in [31]. We set them out below:

- The person propounding the scientific theory must have the necessary qualifications, expertise, experience and integrity to ensure that the Court can have confidence that his testimony is worthy of consideration.
- The theory must have a sound scientific basis, comprehensible to the Court.
- The theory should have gained widespread support amongst that sector of the scientific community which would be likely to utilize it or its results.
- The methods used to carry out the scientific test should be safe and reliable, and follow an established protocol, i.e. one that has been published, disseminated and acknowledged to be reproducible.

In China, articles 239 to 247 of the Rules for the Procedures for Public Security Departments to Handle Criminal Cases [35], articles 84 to 87 and articles 92 to 94 of the Judicial Interpretations of the Supreme People's Court of the People's Republic of China regarding the Law of Criminal Litigations of the People's Republic of China [36], and article 48, articles 144 to 147 of the Law of Criminal Litigations of the People's Republic of China [37] made provisions for the admissibility of expert opinion on electronic evidence. In particular, article 242 of the Rules for the Procedures for Public Security Departments to Handle Criminal Cases [38] requires a forensics expert to use scientific methods to independently carry out examinations and validations. All these provisions came into effect on 1 January 2013. They also provide for the exclusion of improperly obtained or unreliable electronic evidence.

D. International Standards

Fifth, in order for courts to determine the reliability of electronic evidence presented to them, international standards may be considered.

The ISO (International Organization for Standardization) is the world's largest developer of International Standards. ISO works closely with two other international standards development organizations, the International Electrotechnical Commission (IEC) and International Telecommunication Union (ITU). China is one of the 35 participating countries of the Joint ISO/IEC Technical Committee created in 1987 (JTC 1: Information Technology). The ISO standards give state of the art specifications for products, services and good practice.

On 15 October 2012, JTC 1 published the digital forensics standards ISO/IEC 27037:2012 - Guidelines for identification, collection, acquisition, and preservation of digital evidence (first edition) [2]. ISO/IEC 27037:2012 provides guidelines for the processes adopted to identify, collect, acquire and preserve digital evidence. Whether or not digital evidence is admissible in legal proceedings depends on the methodology used in obtaining the evidence. These processes are the bases of acceptable methodology. The standard gives guidelines to individuals such as Digital Evidence First Responders (DEFRs), Digital Evidence Specialists (DESs), incident response specialists and forensic laboratory managers. The standard also helps courts to decide the admissibility and weight of digital evidence obtained by DEFRs and DESs, including electronic evidence extracted from mobile telephones.

International standardization for electronic evidence is still lacking [16]. JTC 1 is still developing three other digital forensic standards (drafts). They are:

- ISO/IEC 27041: Guidance on assuring suitability and adequacy of investigation method [3];
- ISO/IEC 27042: Guidelines for the analysis and interpretation of digital evidence [4]; and
- ISO/IEC 27043: Digital evidence investigation principles and processes [5].

Regarding laboratory accreditation, ISO 17025:2005 General requirements for the competence of testing and calibration laboratories [1] specifies the general requirements for the competence to carry out tests and/or calibrations, which are performed using standard methods, non-standard methods, and laboratory-developed methods.

ISO 17025:2005 consists of two core chapters on management and technical requirements. They define the essential aspects of accreditation. The management requirements section reflects the requirements of ISO standard 9001 and details the assessment criteria for the effectiveness of the quality management system of the laboratory. The technical requirements sections address the competence of staff, the testing methodologies, estimations of uncertainty, traceability and the reporting of results. There is also a requirement to maintain records of any non-conformances and the actions taken to deal with them. Non-conformances include unexpected results, exceptions to normal working. If it is

necessary to use a process that has not been validated against a particular set of requirements, it should be acknowledged that the work is "out of scope" or carry out a validation exercise to extend the scope of the process.

Reference [7] identified the challenges posed by ISO 17025 to digital forensics laboratory. The main challenges are education, validation of tools and methods. To the best of our knowledge, Hong Kong law enforcement agencies have not yet applied to be certified under the digital forensics standards ISO/IEC 27037:2012, or the laboratory accreditation standards ISO 17025:2005. On the other hand, the Computer Forensic Laboratory of the Hong Kong Customs and Excise Department has been awarded ISO 9001 on quality management and ISO 27001 on information security.

Other than international standards, there are other practical guidelines. The Association of Chief Police Officers (ACPO) guidelines [6] provided principles to be followed when officers examine computer devices, including mobile telephones. The National Institute of Standards Technology (NIST) Guidelines on Cell Phone Forensics [19] explained mobile device forensics. It did not set out procedures for law enforcement to follow during an investigation. Reference [22] provided a comparison and contrast between the two guidelines and concluded that:

- The forensic analysis of mobile device is heavily reliant on the methods and tools that relate to specific manufacturer;
- Both NIST and ACPO guidelines in 2007 need to be frequently updated to meet evolving mobile device and their ubiquitous features.

E. Testing of tools

Finally, it is important for a forensic tool user to test the performance of a variety of tools against each other. Questions regarding the validity and reliability of digital forensic software tools used in an investigation are often asked by lawyers in the courtroom [23]. Some official organizations had carried out testing work for digital forensic tools. Reference [23] gave a survey of them. The Computer Forensic Tool Testing (CFTT) group at NIST had tested disk imaging tools and write blocking tools. The Scientific Working Group on Digital Evidence (SWGDE) had also tested some forensic tools. But the results are unavailable to the public. The Department of Defense in the United States had launched a test and evaluation project. The results are available to law enforcement only. In Australia, the Electronic Evidence Specialist Advisory Group (EESAG) had carried out tests on image and audio processing tools only. EESAG reports to the Senior Managers of Australian and New Zealand Forensic Laboratories, which had proposed to establish the National Association of Testing Authorities (NATA) accreditation criteria for the inclusion of digital evidence as a class of examination for the discipline of forensic science. These testing works cannot satisfy the increasing needs for the testing of digital tools built for different purposes for mobile telephones.

The use of recognized standards or protocol in a court of law to determine admissibility and reliability is not novel. One example is the distributed digital forensics mini-lab project linked to the Kentucky Regional Computer Forensic Laboratory (Kentucky RCFL) implemented and monitored by the University of Louisville. For the purpose of triage, the RCFL program of the United States Federal Bureau of Investigation (FBI) has promoted regional collaborations of the FBI with state, regional and local law enforcement. In this regard, the University of Louisville has implemented and monitors the mini-lab project which requires adherence to a set of protocols of the participating agencies to control quality of the investigation [34].

Another example is sections 31.1 to 31.8 of the Canada Evidence Act 1985 of the Revised Statutes of Canada which bring important improvements to the evidence law of business records in Canada. Section 31.5 specifically provides [33]:

"For the purpose of determining under any rule of law whether an electronic document is admissible, evidence may be presented in respect of any standard, procedure, usage or practice concerning the manner in which electronic documents are to be recorded or stored, having regard to the type of business, enterprise or endeavor that used, recorded or stored the electronic document and the nature and purpose of the electronic document."

Although the amendments are not a mandatory requirement for the admissibility of electronic records, they do make compliance with them a relevant consideration by the courts.

In sum, in order for a court to conclude that the subject matter, testimony of which is to be given, is genuinely scientific, international high standards and stringent legal principles must be satisfied. If mobile phone investigators strive to fulfill these requirements, extraction of electronic evidence from mobile telephones will soon evolve to the next generation and becomes part of forensics science.

III. FURTHER ISSUES

The hurdles of meeting the above international standards or legal principles are higher for mobile telephones than traditional computers.

Mobile telephones remain active constantly. Therefore, their contents are continuously updated, unlike traditional computers. Reference [15] concluded that it was impossible to obtain a bit-wise copy of the whole data of the memory of a mobile telephone. Further, investigators, who have sound knowledge of computer operating systems, have limited knowledge and abilities to analyze electronic evidence extracted from mobile telephones. This is because of the lack of knowledge about and familiarity with operating systems and file systems of mobile devices.

Mobile telephone manufacturers use different proprietary operating systems instead of those more standardized operating systems for personal computers. There are five major operating systems, which are Android, Apple, Blackberry, Windows Mobile and Symbian, together with a dozen proprietary systems. The operating systems and forensic tool developers are reluctant to release information about the inner workings of their codes which are regarded as a trade secret. Reference [15]

concluded that this reluctance is the hurdle in developing efficient and reliable forensic analysis techniques. Consequently, the evidence extraction toolkits for mobile telephones are confined to distinct platforms for a manufacturer's product line, an operating system family, or a type of hardware architecture. On the other hand, new mobile telephones are constantly being developed. Toolkits manufacturers have to continually update their toolkits.

Whilst some of the operating systems versions were developed by well-known manufacturers, such as Nokia and Samsung, others were developed by little known Chinese, Korean and other regional manufacturers. This made developing forensics tools and testing them difficult. There are also pirated mobile telephones, referred to as

"Shanzhai phones", which were often used by criminals because they are inexpensive and easy to obtain. The varieties of Shanzhai phones and the absence of documentation hinder the forensic analysis of these mobile telephones [11].

Current mobile telephone forensic is still mainly restricted to the search and analysis of static data on the Subscriber Identity Module, memory cards and the internal flash memory. There are a number of methods to extract electronic evidence from mobile telephones [9]. The primary method is to physically access the telephone circuit board. This is done by removing the memory chip and extracting the data directly. The second method is to use JTAG test points which are found on the circuit board. The third method is to use unlock and reprogramming boxes. The three techniques produce a binary file known a Permanent Memory file. This file must be translated into a format that is easier recognized and is readable and true.

On the other hand, volatile information such as application data, internet browsing data, and instant messaging conversation histories may not be stored in the non-volatile storage media. Without the means to perform live memory forensics on mobile telephones, potentially incriminating evidence may be lost [30].

If extraction of electronic evidence fails, there are specially made screen-capturing tools to photograph the screen on the mobile telephone for preservation purposes [25].

Reference [14] summarized the history of extraction of electronic evidence, concluded that there was no standard way to extract evidence from mobile telephones, and identified a fundamental problem of forensics tools, i.e. the tools were designed to help investigators to find specific pieces of evidence and not to help the forming and evaluation of hypotheses to be presented in court.

In sum, it was difficult to use the current tools to reconstruct a unified timeline of past events or actions and assemble data into a narrative report [14] for the purpose of legal proceedings. The current tools are only able to extract the evidence residing in the telephone's non-volatile storage. The challenge arises when the application data are found in the volatile data only (e.g. in web-based applications) and no trace of evidence could be found in the non-volatile storage [30].

IV. The Way Forward

Common law legal system makes a distinction between technical evidence and expert evidence. A witness gives technical evidence if he or she carries out a technical investigation or procedure and then reports without comment on the findings. An example is the exercise of properly imaging a hard disk or producing the results of a keyword search. On the other hand, an expert witness gives evidence based on experience and opinion. The common requirement for the testimony of both type of witnesses is that the domain for which they testify must have a sound scientific basis, the scientific test should be safe and reliable, and follow an established protocol, i.e. one that has been published, disseminated and acknowledged to be reproducible, and conforms with international standards.

This paper highlights the requirements to be fulfilled before the transition of extraction of electronic evidence from mobile telephone to the next generation, a true forensic science. Unification of standards and procedures and accreditation are required. There is also the challenge for law enforcement to prove compliance with the accreditation for forensic standards of investigation, analysis, interpretation and reporting, e.g. ISO/IEC 17025:2005 - General requirements for the competence of testing and calibration laboratories, and ISO/IEC 27037:2012 - Guidelines for identification, collection, acquisition, and preservation of digital evidence are two existing international standards. Soon, ISO/IEC 27041: Guidance on assuring suitability and adequacy of investigation method, ISO/IEC 27042: Guidelines for the analysis and interpretation of digital evidence; and ISO/IEC 27043: Digital evidence investigation principles and processes.

One of the biggest challenges concerning extraction of electronic evidence from mobile telephone is the differences in levels of technical expertise and a global skills shortage. At the moment, there is no minimum level of training and certification upon which are internationally agreed [16].

Digital Evidence First Responders, Digital Evidence Specialists, Incidence Response Specialists and Forensic Laboratory Managers should immediately take active steps to move extraction of electronic evidence from mobile telephone into a more rigorous position as a science, by compliance with the high legal requirements and international standards. Ideally, public forensic science laboratories should be independent of or autonomous within law enforcement agencies [21].

References

[1] ISO 17025:2005 - General Requirements for the Competence of Testing and Calibration Laboratories.

[2] ISO/IEC 27037:2012 Guidelines for Identification, Collection and/or Acquisition and Preservation of Digital Evidence (First Edition).

[3] ISO/IEC 27041: Guidance on Assuring Suitability and Adequacy of Investigation Method.

[4] ISO/IEC 27042: Guidelines for the Analysis and Interpretation of Digital Evidence.

[5] ISO/IEC 27043: Digital Evidence Investigation Principles and Processes.

[6] Association of Chief Police Officers and 7 Safe Information Security. Good Practice Guide for Computer-Based Electronic Evidence (version 4), July 2007.

[7] Jason Beckett and Jill Slay. Scientific Underpinnings and Background to Standards and Accreditation in Digital Forensics. Digital Investigation, 8(2):114 - 121, 2011.

[8] China Internet Network Information Center. The 31st Statistical Report on Internet Development in China, January 2013.

[9] Kevin Curran, Andrew Robinson, Stephen Peacocke and Sean Cassidy. Mobile Phone Forensic Analysis. International Journal of Digital Crime and Forensics, 2(3):15 - 27, July - September 2010.

[10] *Daubert v.Merrell Dow Pharmaceuticals Inc.* 509 U.S. 579 (1993).

[11] Junbin Fang, Zoe L. Jiang, Kam-Pui Chow, Siu-Ming Yiu, Lucas Chi Kwong Hui, Gang Zhou, Mengfei He and Yanbin Tang. Forensic Analysis of Pirated Chinese Shanzhai Mobile Phones. In IFIP Int. Conf. Digital Forensics, pages 129 - 142, 2012.

[12] Guillermo A. Francia and Keion Clinton. Computer Forensics Laboratory and Tools. Journal of Computing Sciences in Colleges, 20(6):143 - 150, June 2005.

[13] *Frye v. United States*. 293 F. 1013 (D. C. Cir 1923).

[14] Simson L. Garfinkel. Digital Forensics Research: The Next 10 Years. Digital Investigation, 7, Supplement (0): S64 - S73, 2010.

[15] Archit Goel, Anurag Tyagi and Ankit Agarwal. Smartphone Forensic Investigation Process Model. (6):322 - 341, 2012.

[16] Marthie Grobler. The Need for Digital Evidence Standardisation. International Journal of Digital Crime and Forensics, 4(2):1 - 12, April - June 2012.

[17] Paul Hunton. The Stages of Cybercrime Investigations: Bridging the Gap between Technology Examination and Law Enforcement Investigation. Computer Law & Security Review, 27(1):61 - 67, 2011.

[18] International Bank for Reconstruction and Development / The World Bank, editor. 2012 Information and Communications for Development: Maximizing Mobile. International Bank for Reconstruction and Development / The World Bank, 2013.

[19] Wayne Jansen and Rick Ayers. Guidelines on Cell Phone Forensics - Recommendations of the National Institute of Standards and Technology. National Institute of Standards and Technology, 2007.

[20] Tod S. Levitt and Kathryn Blackmond Laskey. Computational Inference for Evidential Reasonings in Support of Judicial Proof. In Symposium - Artificial Intelligence and Judiciary Proofs, 2000.

[21] National Research Council of The National Academies. Strengthening Forensic Science in the United States: A Path Forward. U.S. Department of Justice and The National Academies Press, 2009.

[22] Paul Owen and Paula Thomas. An Analysis of Digital Forensic Examinations: Mobile Devices versus Hard Fisk Drives Utilising ACPO & NIST Guidelines. Digital Investigation, 8(2):135 - 140, 2011.

[23] Lei Pan and Lynn Margaret Batten. Robust Performance Testing for Digital Forensic Tools. Digital Investigation, 6(1 - 2):71 - 81, 2009.

[24] Sean Peisert, Matt Bishop and Keith Marzullo. Computer Forensics in Forensis. SIGOPS Operating Systems Review, 42(3):112 - 122, April 2008.

[25] Shafik G. Punja and Richard P. Mislan. Mobile Device Analysis. Small Scale Digital Device Forensics Journal, 2(1):1 - 16, June 2008.

[26] Chris K. Ridder. Evidential Implications of Potential Security Weakness in Forensic Software. International Journal of Digital Crime and Forensics, 1(3):80 - 91, 2009.

[27] Michael J. Saks and Samantha L. Neufeld. Convergent Evolution in Law and Science: the Structure of Decision-making under Uncertainty. Law, Probability and Risk, 10:133 - 148, 2011.

[28] C. Soanes and A. Stevenson, editors. Oxford Dictionary of English. Oxford University Press, 2005.

[29] The Law Reform Commission. Expert Evidence in Criminal Proceedings in England and Wales. The Stationery Office, 21 March 2011.

[30] Vrizlynn L. L. Thing, Kian-Yong Ng and Ee-Chien Chang. Live Memory Forensics of Mobile Phones. Digital Investigation, 7(Supplement):74 - 82, 2010.

[31] *Wang Din Shin v. Nina Kung alias Nina T.H. Wang*. High Court Probation Action No. 8 of 1999 (21 November 2002).

[32] Yunus Yusoff, Roslan Ismail and Zainuddin Hassan. Common Phases of Computer Forensics Investigation Models. International Journal of Computer Science & Information Technology, 3(3):17 – 31, June 2011.

[33] Canada Evidence Act, R.S.C., 1985, c. C-5, available at http://laws-lois.justice.gc.ca/eng/acts/C-5/FullText.html.

[34] Michael Losavio, Deborah Keeling and Michael Lemon, Models in Collaborative and Distributed Digital Investigation in the World of Ubiquitous Computing and Communication Systems, in Proceedings of The Memory of the World in the Digital Age: Digitization and Preservation (UNESCO 2013), pages 1079 – 1092.

[35] Zhonghuarenmingongheguo gonganjiguan banli xingshi anjian chengxu guiding, available at http://www.mps.gov.cn/n16/n1282/n3493/n3823/n442421/3486957.html.

[36] Zhonghuarenmingongheguo zuigaorenminfayuan guanyu shiyong Zhonghuarenmingongheguo xingshi susongfa de jieshi, available at http://www.court.gov.cn/qwfb/sfjs/201212/t20121228_181551.htm.

[37] Zhonghuarenmingongheguo xingshi susongfa, available at http://www.mps.gov.cn/n16/n1282/n3493/n3778/n4303/3170600.html.

[38] Gongan Jiguan Banli Xingshi Anjian Chengxu Guiding, available at http://www.mps.gov.cn/n16/n1282/n3493/n3823/n442421/3486957.html.