"Cyber Forensics"

Jitendra Kumar, Jutirani Talukdar
Student (Ballb 4th Year) Symbiosis Law School, Pune Symbiosis International (Deemed University) Maharashtra, India

Abstract

This study presents a quantitative assessment of the cyber forensics which is also known as computer forensic the usage of Computer Forensics in solving cases. In modern time our whole world is centred on computers even criminals have started taking help of computers in committing crimes. Cyber Forensics is simply application of computer investigation and analysis techniques in the interest of determining potential legal evidence. Basically, Forensic computing is the process of identifying preserving, analysing and presenting the digital evidence in a manner that is legally acceptable. It also symbolizes the study of evidence from attacks on computer system in order to learn what has occurred, how to prevent it from recurring and the extent of the damage. Corporate world is most affected with computer based crimes as their whole business is done with the help of computers. Digital evidence was not considered as tangible evidence in courts until recently but now they are gaining importance. This research paper is an attempt to understand the scope of cyber forensics and its Indian scenario.

Keywords: cyber forensics, Computer Forensics, investigation, criminals, crimes, digital evidence, Indian scenario.

INTRODUCTION

The computer is becoming a weapon in the arsenal of the everyday criminal. Drug users are becoming more sophisticated by using computers to keep track of "customers," shipments, and money. Hackers are shutting down university computer systems, airports, and other systems, sometimes resulting in millions of dollars in losses and the threat of fatalities. As a new century begins, so does the problem of computer criminals for the probation and parole system. Cybercrime trials often turn on a battle between competing computer forensic experts. As a result, both prosecutors and defence attorneys are asking: What types of evidence can computer forensic experts provide? How can computer evidence be recovered and preserved? How should an attorney go about finding a qualified expert? How should the expert's testimony be presented at trial? What issues do experts commonly contest in cybercrime cases? This article attempts to answer each of these questions[1].

The ancient world lacked standardized forensic practices, which aided criminals in escaping punishment. Criminal investigations and trials relied on forced confessions and witness testimony.[2] In ancient India too, medical opinion was frequently applied to the requirements of the law. By law the minimum age for the marriage of girls was

[1] The Federal Law Enforcement Training Center (http://www.fletc.gov/, accessed April 02, 2019

[2] RK Tewari, *History and Development of Forensic Science*, 46 J Postgrad Med 303-305 (2000).

fixed at 12 years; the duration of pregnancy was recognized as being between 9 and 12 lunar months and there is evidence that doctors had to opine on such cases.[3]***In 1968, the Ministry of Home Affairs, Government of India, set up the first Forensic Science Laboratory for Delhi Police and the Central Bureau of Investigation under the administrative control of the Central Bureau of Investigation.*** Forensic Science, an amalgamation of almost all faculties of knowledge is an essential and efficient enabler in the dispensation of justice in criminal, civil, regulatory and social contexts.[4]Thus a need is felt for the development of cyber/digital forensics to combat the evil of the cybercrimes. However, the field of cyber forensics is still in its nascent stage and there is a lot that needs to be done in order to achieve the desired results.

SCOPE

The ever evolving nature of Internet and computers has paved the way for several cybercrimes across the globe. Cyber Crimes provides for a peculiar field of criminal law jurisprudence. Consequently, for the sake of investigating these crimes, digital evidence assumes the centre stage. Although, ***Section 65-B of the Indian Evidence Act provides for admissibility of electronic evidence, however there is lack of jurisprudence on the import of the electronic evidence in the criminal jurisprudence and the specific contours which corroborate their admissibility***.

The lecture also focused on the developments in cyber forensics and provide for the current position on the admissibility of digital evidence along with the various challenges faced in Indian Jurisprudence.

ANALYSIS

- **DEFINITION OF CYBER FORENSICS**

Cyber Forensics is not explicitly defined in Indian laws. However, cyber forensics could be conveniently defined as[5]

> *The usage of apt forensic tools and technical knowledge to recover the electronic evidence within the contours of the rules of evidence, for it to be admissible before the court of law.*

The electronic evidence so obtained has to satisfy the criteria of crime attribution to the perpetrator by tracing its digital footprints by preservation, extraction, interpretation, and documentation of digital evidence.

- **TECHNIQUES GOVERNING CYBER FORENSICS**

The findings of a cybercrime investigation will be admissible in a court of law only if these three basic rules are followed:[6]

---

[3] IshaTyagi and Nivedita Grover, *Development of Forensic Science and Criminal Prosecution-India*, 2 IJSRP 1-3 (2014).

[4] Dr. Gopal Ji. Misra & Dr. C. Damodaran, *Perspective Plan for Indian Forensics*, MINISTRY OF HOME AFFAIRS GOVERNMENT OF INDIA, (April 02, 2019, 10:04 AM), https://mha.gov.in/sites/default/files/IFS%282010%29-FinalRpt_3.pdf

[5] Ramanuj, *Cyber Forensics: Law and Practice in India*, I-Pleaders (April 02, 2019, 10 AM), https://blog.ipleaders.in/cyber-forensics-law-and-practice-in-india/

1. The cybercrime investigators must be skilled competent professionals.
2. The original digital evidence must never be tampered with or altered. As far as practical, investigators must work on the image/clone of the original evidence. If that is not practical, then extreme care and caution must be taken while working on the original evidence.
3. A detailed and accurate audit trail must be maintained. The chain of custody forms and other audit trail documents must be meticulously maintained. Any lacuna in these documents casts suspicion on the entire findings of the investigation.

There are two basic forms of collection "freezing the scene" and "honey potting".[7] The two are not mutually exclusive. They are briefly described as under:

FREEZING THE SCENCE

The necessary authorities should be notified (for instance the police and our incident response and legal teams) but we should not go out and tell the world just yet. Next, one should then start to collect whatever data is important onto removable non-volatile media in a standard format and make sure that the programs and utilities used to collect the data is also collected onto the same media as the data.

HONEYPOTTING

Honey potting is the process of creating a replica system and luring the attacker into it for further monitoring. A related method—sandboxing—involves limiting what the attacker can do while still on the compromised system so they can be monitored without much further damage. The placement of misleading information and the attacker's response to it is a good method for determining the attacker's motives.

- **VOLATILE DATA THAT YOU LOSE**

- Running Processes
- Password in Clear Text
- Executed Control Command
- Instant Messages
- Unencrypted Data
- Trojan Horse

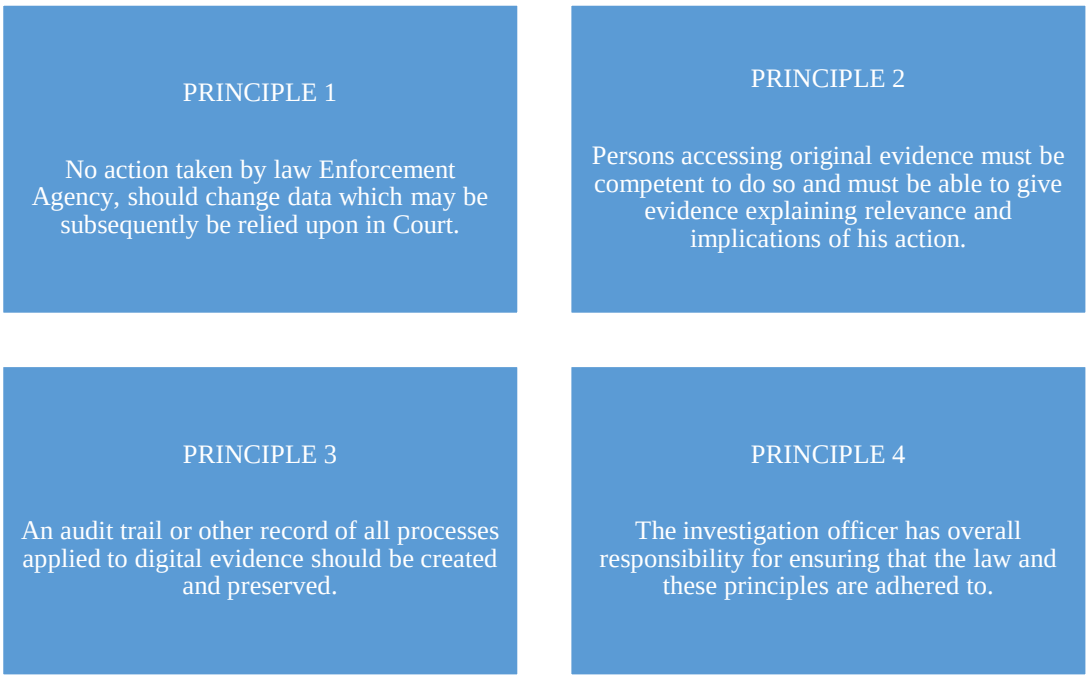
These are the kind of data that may be lost when anyone hack or enter your computer, computer here include mobile phone or any other electronic device which is capable of storing or retaining data. These are the data which the computer stores when we enter them into it using them in any kind.

[6] Steve Romig, *Forensic Computer Investigations*, OHIO STATE.EDU, (April 02, 2019 6:10 pm), http://www.net.ohio-state.edu/security/talks/2001-10_forensic-computerinvestigations/

[7] *Investigations Involving Computer and Computer Networks*, UNITED STAES DEPT. OF JUSTICE, (April 02, 2019, 4:10 PM), https://www.ncjrs.gov/pdffiles1/nij/210798.pdf

Printers also save the data that we print on it. The storage chip on the printer saves all the data that is printed on it. The only way to getting removed this kind of data is to override the data printed on printer. The other way to recover this sensitive data is to not use the devise and seek expert available.

- **PRINCIPLES OF DIGITAL EVIDENCE**

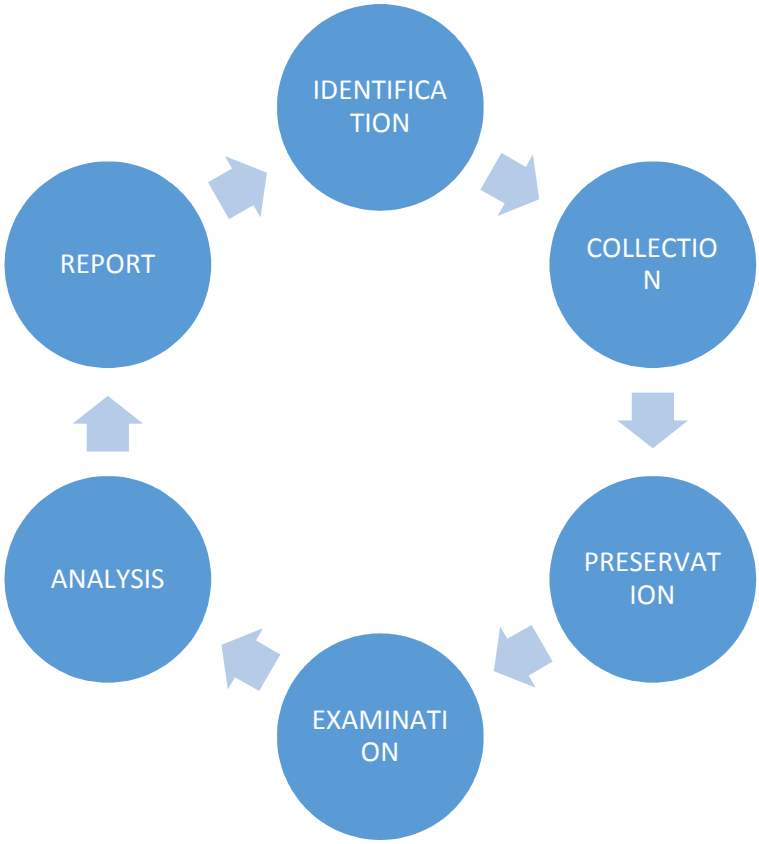


- **LOCARDS EXCHANGE PRINCIPLE**

"***It is impossible for a criminal to act, especially considering the intensity of a crime, without leaving traces of this presence***."

Although Locard's exchange principle is generally understood as the phrase "with contact between two items, there will be an exchange," Edmond Locard never actually wrote down those words in the vast amount of material he produced, nor did he mention anything concerning a principle.A criminal can leave all sorts of evidence, including fingerprints, footprints, hair, skin, blood, bodily fluids, pieces of clothing and more. By coming into contact with things at a crime scene, a criminal also takes part of that scene with him, whether it's dirt, hair or any other type of trace evidence.

STEPS IN EVIDENCE COLLECTION



Identification

The first process of computer forensics is to identify the scenario or to understand the case. At this stage, the investigator has to identify the purpose of investigation, type of incident, parties that involved in the incidence, and the resources that are required to fulfill the needs of the case.

Collection

The collection (chain of custody) is one of the important steps because your entire case is based on the evidence collected from the crime scene. Collection is the data acquisition process from the relevant data sources while maintaining the integrity of data. Timely execution of the collection process is crucial in order to maintain the confidentiality and integrity of the data. Important evidence may have lost if not acted as required.

Imaging

Rule of Thumb: make 2 copies and don t work from the original (if possible)

• A file copy does not recover all data areas of the device for examination

• Working from a duplicate image

• Preserves the original evidence Preserves the original evidence

• Prevents inadvertent alteration of original evidence during examination during examination

• Allows recreation of the duplicate image if necessary

Digital evidence can be duplicated with no degradation from copy to copy

Examination

The aim of third process is to examine the collected data by following standard procedures, techniques, tools and methodology to extract the meaningful information related to the case. **Analysis**

Since all five processes are linked together, the analysis is the procedure to analyze the data acquired after examination process. At this stage, the investigator search for the possible evidence against the suspect, if any. Use the tools and techniques to analyze the data. Techniques and tools should be justified legally, because it helps you to create and present your report in front of the court.

Reporting

This is the final, but the most important step. At this step, an investigator needs to document the process used to collect, examine and analyze the data. The investigation report also consists the documentation of how the tools and procedures were being selected. The objective of this step is to report and present the findings justified by evidences.

CHANGES IN LAW FOR CYBER FORENSICS

Cyber forensics is a relatively new discipline to the courts and many of the existing laws used to prosecute computer-related crimes, legal precedents, and practices related to computer forensics are in a state of flux. The legislature has made changes to the acts to adapt to the changing scenario. Firstly, Section 3 of the Evidence Act has been amended to include electronic evidence as a part of the term evidence. The other parallel legal recognition appeared in Section 4, The Information Technology (Amendment) Act, 2008, with the provision for acceptance of matter in electronic form to be treated as “written” if the need arises. This shows that electronic evidence will now be accepted in a trial. Section 79A of the IT (Amendment) Act, 2008 defines electronic evidence as any information of probative value that is either stored, or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones and digital fax machines. Section 79A of the IT (Amendment) Act, 2008, empowers the Central government to appoint any department or agency of Central or State government as Examiner of Electronic Evidence. This particular agency will give expert opinion on the electronic evidence. Section 65B of the Indian Evidence Act, 1872 states certain conditions wherein any electronic record produced by a computer shall also be deemed to be evidence if it satisfies the conditions.

(i) The computer producing the information must be in use for the purpose of regular activities during that period.

(ii) The nature of information so extracted out of the computer must have been regularly fed in the computer.

(iii) During the said period, the computer must have worked properly and if not, then its non-operation shouldn’t have affected the accuracy of such information.

(iv) The information contained in the electronic record reproduces or is derived from such computer in the ordinary course of the business[8].

FORESNSIC SCIENCE IN INDIA

In India, forensic science was considered to be relevant and admissible in a limited arena of law. ***Previously it was an amalgamation efficient enabler in the dispensation of justice in criminal, civil and regulatory contexts only.***However, with the advent of time and surge of technological advancements various new forms of crimes occupied the landscape which reflected the need for cyber-forensics in Indian jurisprudence.

❖ Cyber forensics and Information Technology Act, 2000

Information and Technology Act, 2000 was enacted to cater to the growing demand of legislation in cyber space. ***For the first time it introduced the concept of 'digital signatures', 'encryption', 'electronic evidences' etc.*** These terms were foreign to the then law of evidence. No provision was there to adduce them as evidences in courts of law. Inevitably, certain changes were made in the Indian Evidence Act, 1872 to make it more contemporary and in tune with the changing times.[9] The Indian Evidence Act, 1872 and Information Technology Act, 2000 grants legal recognition to electronic records and evidence submitted in form of electronic records. According to section ***2(t)*** of the Information Technology Act, 2000 "***electronic record***" means

> *Data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche.*

❖ Legal Provisions

1. Firstly, the traditional law defining the term "***Evidence***" has been amended to include electronic evidence in Section 3, The Evidence Act, 1872. The other parallel legal recognition appeared in Section 4, The Information Technology (Amendment) Act, 2008, with the provision for acceptance of matter in electronic form to be treated as "***written***" if the need arises. These show a prima facie acceptability of digital evidence in any trial.
2. Further, ***Section 79A*** of the IT (Amendment) Act, 2008 has gone aboard to define electronic evidence as any information of probative value that is either stored, or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones and digital fax machines.
3. With regards to admissibility of electronic records, ***Section 65-B*** of the Evidence Act, 1872 enunciates various conditions for the same. Afzal guru case[10]. In this particular case importance, the collection, preservation and appreciation of electronic evidence was highlighted. This was first time admissibility of evidence under Section 65B of the Evidence Act was put under the test.
4. Since digital evidence ought to be collected and preserved in certain form, the admissibility of storage devices imbibing the media content from the crime scene is also an important factor to consider. Reading Section 3 and Section 65-B, The Evidence Act, 1872 cumulatively, it can be inferred that certain computer outputs

[8]Indian Evidence Act, 1872
[9] Swati Mehta, *Cyber Forensics and Admissibilty of Digital Evidence*, 5 SCC J-54, 56 (2011).
[10]State v. Mohd. Afzal&Ors. 107 (2003) DLT 385

of the original electronic record, are now made admissible as evidence "***without proof or production of the original record. Thus, the matter on computer printouts and floppy disks and CDs become admissible as evidence."***

5. Throughout the material part of such period, the computer must have been operating properly. In case the computer was not properly operating during such period, it must be shown that this did not affect the electronic record or the accuracy of the contents.
6. The information contained in the electronic record should be such as reproduces or is derived from such information fed into the computer in the ordinary course of such activities.

The apex court in ***State v Navjot Sandhu***[11], held that while examining the provisions of newly added section 65B that in a given case, it may be that the certificate containing the details in sub- section 4 of section 65B is not filed, but that does not mean that secondary evidence cannot be given. It was held by the court that the law permits such evidence to be given in the circumstances mentioned in the relevant provisions, namely, sections 63 and 65 of the Indian Evidence Act 1872.

Further in the case of ***State of Delhi v. Mohd. Afzal & Others***[12], it was held that electronic records are admissible as evidence. If someone challenges the accuracy of a computer evidence or electronic record on the grounds of misuse of system or operating failure or interpolation, then the person challenging it must prove the same beyond reasonable doubt.

Requirement for Computer Forensic Services: 2004 – 2014[13]

Year	***India Market US$ Million***
2004	***103.152***
2005	***137.641***
2006	***173.446***
2007	***208.279***
2008	***243.141***
2009	***278.109***
2010	***313.708***
2011	***349.845***
2012	***384.546***
2013	***421.925***
2014	***463.050***

[11] State v Navjot Sandhu, (2005) 11 SCC 600 (India).
[12]State of Delhi v. Mohd. Afzal &Others, 2003 (3) SCC 1669 (India).
[13] www.icongrouponline.com

USE OF CYBER FORENSICS

1. **Criminal prosecution**: Use electronic evidences in variety of crimes where incriminating evidences can be found.
2. **Civil prosecution:** Can make use of electronic evidences in unearthing business and personal records. Contracts, divorce, claims, harassment, defamation cases are some examples.
3. **Insurance cases**: Insurance companies may be able to successfully defend themselves from any claim by furnishing electronic records of possible fraud in accident and arson cases.
4. **Corporations** They also make use of these evidences to ascertain any possible linkups in blackmails, frauds, trade secret, misappropriation and other internal and external information.

    - Identify sources of documentary or other digital evidence
    - Understand the suspects
    - Secure the machine and the data
    - Examine the machine's surroundings
    - Examine the Live System and record open applications
    - Duplicate the electronic media evidence

Cluster:

Is also known as allocation blocks, a cluster is a contiguous group of sectors that is the smallest amount of space assigned to a file by an operating system such as Microsoft Windows.

SUGGESTIONS

1. The first is creating a ***standard in the realization*** that it must have flexibility in order to allow for revisions. Because the world continuously changes, an inflexible standard is not practical and can become worthless. In attempting to ***create a standard for computer forensics, each phase of the forensic process must be analysed to determine the most practical method***. In search and seizure, the ***standard will need to effectively cover all aspects, including the warrant, preservation of evidence, on-scene forensics examination, transportation of evidence and documentation***.
2. The second area of concern, the ***qualifications of expert witnesses***, is an issue concerning experts of all fields. The computer forensic field is fairly unique, as it has no credentials or a formal educational process. Currently, the lower courts accept qualifications based on the skills and previous work experience of the experts. While this has been sufficient to date, it is anticipated that contesting the expertise and qualifications of expert witnesses will become more common in the future. Thus, ***the need for a national and internationally recognized certification and standardization for computer forensics is necessary***.
3. ***Cyber forensics is a branch of forensics relating to computer based evidences, their storage, collection and admissibility. It is also known as digital forensics.*** The reasons for employing cyber forensics techniques are manifold. ***Firstly***, analysis of computer systems belonging to accused; ***secondly***, recovery of data in

event of hardware/software failure; thirdly, to gather evidences against the employee or any person the organisation wish to terminate.

4. Cyber forensics as a discipline requires highly trained professional operating in an organized and comprehensive manner. The growing number of cybercrime indicates setting up of support group consisting of police officers in CBI, CID, state police headquarters and detective department of computer investigation. These ***trained police officers are needed to understand the nature of crime at the threshold.***
5. ***Special measure should be taken in conducting cyber forensics investigation***. It must be kept in mind that only collection of evidences is not required. ***The agency is required to ascertain that whether or not the evidences so gathered are admissible in the court of law***. For the purpose of admissibility, they are supposed to make provisions so that those evidences are not tampered or toyed. Evidences are to undergo a strict test of admissibility. Hence they must draw a clear picture of sequence of events leading to one and only one conclusion of the accused being guilty.
6. Another baffling aspect which is involved in these crimes is the intelligence of criminals. Those who commit these crimes are highly skilled persons especially trained in these fields. Hence their understanding of things is far more than what investigators can perceive. ***In order to match with the intellect and skill of criminals a hyper technical and sharp approach is needed.***
7. Although the problems of computer forensics can be correlated with the field being in its infancy, ***it is time to take decisive actions***. Computer forensics, as a field, has experienced events that should never be repeated (e.g., lack of standards and peer review). ***In order for the field of computer forensics to mature, there must be a national system for certifying individuals who claim to be professionals.***
8. Regarding the analysis, preservation, and presentation of the evidence, ***there should be rigorous standards, and requirements coupled with continual updates to the processes***. The common methodology used to analyze the evidence currently relies on proprietary software or hardware which does not allow experts to know exactly what is happening under the proverbial hood. This is a serious issue; ***the experts must be able to explain what is occurring at each step of the duplication and analysis process and why certain events are occurring*** (e.g., how data is being recovered and why it is possible to recover data).
9. Cyber forensics became more challenging since new forms and techniques of data storage are continuously being changed and new technologies are being developed. One of the major challenges faced by the investigators and law courts is the legal framework. In India after the enactment of Information and Technology Act, 2000 and consequential amendments in the Indian Evidence Act, 1872 and the Indian Penal Code, 1860, electronic record is admissible evidence criminal can be bringing to book. Thus law need to develop at the pace of technology. In ***State of Punjab v. Amritsar Beverages Ltd***.[14], the Supreme Court expressed that there are a lot of difficulties faced by investigating officers due to lack of scientific expertise and insight into digital evidences techniques. The court also noted that IT Act does not deal with all types of problems and hence the agencies are seriously handicapped in some respects.

[14] State of Punjab v. Amritsar Beverages Ltd, Case No. 2419 of 2006 (India).

CONCLUSION

Thus it may conclude that it is quite notable achievement for law enforcement agencies and legislators that India has kept pace with the changing technological trends and introduced extremely important amendments in its laws to cater to the demands of technology. ***The only thing which needs a special and urgent attention is the training imparted to the implementing authorities so that the provisions are adequately enforced.*** Hopefully in years to come this problem will also be redressed and the country will witness a totally new, refreshed and technologically sound legal and enforcement framework.

Maintaining the integrity of digital evidence throughout the process of examination presents different problems from those encountered when handling traditional physical or documentary evidence.

Mistakes in interpretation and analysis can be reduced by (i) rigorous application of the scientific method performing exhaustive investigation and research (ii) questioning all assumptions and (iii) developing a theory that explains the facts.

Ultimately, abiding by the scientific method will help forensic examiners to avoid egregious errors. Carefully exploring potential sources of error, hypothesis testing and qualifying conclusions with appropriate uncertainty will protect forensic examiners from overstating or misinterpreting the facts.