A Review on Legal and Ethical Principles of Computer Forensics

Abstract:

Since computers and information systems have evolved so rapidly in the late 20th century and the early 21st century, computer systems have become more so than ever capable of storing, accessing and processing data. New areas of expertise have also emerged such as the field of ethical hacking and cloud forensics which require specialists. But this ultra-fast emergence of technologies makes us overlook the controversies that have emerged with these advances, like the frequent violation of the Intellectual Property laws i.e. the copyright laws, patent laws, etc and other violations such as the privacy laws, laws related to misuse of business property, etc. These emerging controversies need to be contained by the introduction of legal and ethical principles to the fields of digital forensics.

I. INTRODUCTION

Digital Forensics is lately being in the public eye, it is an investigative field and like any other investigative field has its ethical issues. Computer forensics includes the gathering, storing and presenting digital pieces of evidence in a manner that is considered acceptable legally. It is a very complex process and can involve a huge number of activities. The evidence must be handled very carefully and must not be tampered with at any cost. This puts pressure on the investigator to be very careful with his job, and if he is not, he would be risking the entire case.

To counter these kinds of problems a few guidelines are provided by the ACPO and the NIST of England and the United States respectively. These guidelines, however, can only address the legal and logical issues but not the ethical and moral ones. Like any other profession, the field of computer forensics must also have an established ethical framework. Ethics in the field of digital forensics is defined as the set of definitive principles that define how a computer system should be used.

The Digital Forensic System is a specialized information system which helps us better understand events in electronic devices, the data gathered can then be used to identify and disapprove the people who do not maintain proper conduct on the internet and electronic devices. The data gathered can further be used in the future to avoid such events from happening again.

Digital forensics is defined by legal requirements, it's growth is effected by the various types of cases it receives year after year. Hence it is difficult to make progress in the field of Digital Forensics without critical examination and guidance from legal scholars.

The ethics of Digital forensics also include how a professor must approach his students on topics related to ethical hacking. This also includes what topics are to be considered when designing the curriculum for the students. [2] Students should be taught about hacking and also lab component which should also include the knowledge of destructive actions. Students should also be taught about ethical hacking and its principles in detail.

There are many issues associated with teaching ethical hacking. To understand the true intentions of students is very hard to identify and the reason why ethical hacking should be used is a very much a debate.

As mentioned before, since the field of digital forensics is an investigative one, a forensic analyst will most probably be confronting ethical dilemmas sometime while performing their job. These dilemmas might include serious issues like threats to national security, extremely personal information like photographs, etc, trade secrets, etc. The evidence which might be simply overlooked, found or not found by the forensic analyst might determine the outcome of the case he is working on, which can be related to a person's imprisonment or maybe a case involving huge amounts of money. If the forensic analyst is ethically not strong, simply accept to be handsomely paid to ignore the evidence.

According to the research conducted by various papers [4] forensic analysts are very ill-prepared to deal with these ethical dilemmas. This is because of various reasons like lack of regulation by the industry, very little to no attention given towards the teaching of these ethics in the fields related to forensic analysis. The field of forensic analysis requires professionals with a very strong and good moral character. [5]

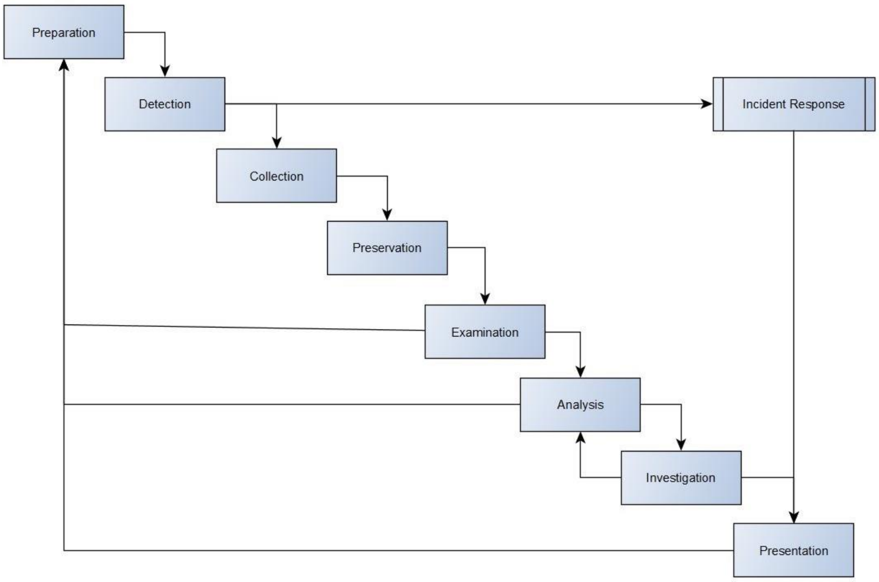


Fig.1: Process flow of Forensic investigation in which every phase has its respective rules and principles

II. Computer Forensics

A. Introduction

Computer forensics is a detailed application of investigation and complete analysis techniques to retain and preserve collected evidence from a particular electronic computing device in a way that is suitable for presentation during a court of law. It often involves electronic data storage extractions for legal purposes. Cybercrimes cover a broad spectrum, from email scams to downloading copyrighted works for distribution, and are fuelled by a desire to profit from another person's intellectual property or private the information.

Computer forensics can show a digital audit trail for analysis which will be done by experts or law enforcement. Developers often build program applications to combat and capture online criminals; these applications are the crux of computer forensics.

A computer forensic examination may gave you information like when a document first used on a computer, when it was last edited, when it was last printed and which user carried out of these particular actions.[6]

Computer Forensics is derived as a synonym for cyber forensics, but its definition has expanded to include the forensics of all digital technologies . A digital forensic investigation can be widely classified into three stages:

- preservation of evidence,
- analysis and
- presentation/reporting.

Digital evidence can be there in either of open computer systems, communication systems, or in embedded computer systems.

Digital evidence can be duplicated exactly and it will be very difficult to destroy and they can be found in hard drive, flash drive, phones, mobile devices, routers, tablets, and instruments such as GPS. To be admissible during a court of law, evidence must be strictly both relevant and reliable. upto date, there have been a few legal challenges to compete digital evidence. These also include Criminal investigations, Civil investigations, Intelligenceinvestigations.

B. Benefits

- With computer forensics, a business is suitable to mitigate the risk of sampling. While an organization can always use other auditors or cyber forensics professionals, this is one benefit that it can acquire using the on-board forensic team.
- The procedure enables the team to compare similar data collected from different sources or symptoms. This comparison helps to complete the huge picture when investigating on a cybercrime case.
- Through investigation, the team can relate the trends related to the relevant data. The patterns can also help understand the fluctuations. Also, the team is able to determine potential risk factors and false positives.

- There are identifying trends that enable the team to acquire more details about the consultants, company personnel, and forensic accountants.
- The reports and investigation may help the team understand the control environment. The enterprise teams will learn about policies to identify the attributes that violate rules.
- Training the team on board to carry out the cyber forensics also help contain less network costs.
- The team is trained to recommend budget-friendly system upgrades and other relevant implementations.
- Helps identify the increased threats, crimes and security vulnerabilities.
- There square measure distinctive trends that alter the team to amass additional details regarding the consultants, company personnel, and forensic accountants.
- The reports and investigation might facilitate the team perceive the management atmosphere. The enterprise groups can find out about policies to spot the attributes that violate rules.
- Coaching the team on board to hold out the cyber forensics additionally facilitate contain less network prices.
- The team is trained to advocate budget friendly system upgrades and different relevant implementations.
- Helps establish the inflated threats, crimes and security vulnerabilities.

III. LITERATURE SURVEY

Digital forensics will be outlined as cluster of tasks and processes that involve in digital investigation which in the main involves technical implementation details and investigation procedures that square measure intensively developed by the normal forensics scientists. On the opposite hand, legal practitioners might have difficulties in applying the forensics strategies or even they may face drawback in understanding the processes and tasks.

A digital forensics investigator has to applyvarious strategies for implementing the tools in an exceedingly particular state of affairs. The investigator has to collect, recover, decode, discover, extract, analyse and convert the info and at last preserve it in an exceedingly totally different storage media to legible proof. regardless of the location wherever the info is hold on the investigator should be revealing and focusing retrieval of the truth behind the info.

The data extraction doesn't mean to easily copy the data with Windows human or storing files to a disk. In general, chain of proof, time, integrity of the proof and therefore the person relationship with the evidence can be conjointly thought-about because the non-repudiated and rebutted, then the digital evidence would be reliable and admissible for judicial review.

The connexion of the proof with the case would finally have an effect on the burden and importance of the evidence. If the legal professional will counsel on what should be extracted, time and price spent within the present information will be controlled in a good approach.

The IT Security fundamentals are:

- Confidentiality
- Availableness
- Integrity

In a typical digital forensics investigation method the homeowners along side the investigators and practitioners square measure expected to be concerned and square measure requested to follow on the case. There are typically eight individual roles of participants in investigation. the various roles are:

- Case Leader
- System/business owner
- Legal consultant
- Security
- Digital Forensics specialist
- Investigator/administrator
- Analyst
- Legal prosecuting officer

No framework can be applied while not the testing of its pertinence. [3] The FORZA model has different layers.

They are:

- discourse Investigation Layer
- discourse Layer
- Legal consultatory Layer
- abstract security Layer
- Technical presentation Layer
- information acquisition Layer
- information analysis Layer
- Legal presentation Layer

The forza framework are going to be developed as a semiautomatic investigation tool chest. [2] because the apply of "ethical hacking" has reached worldwide attention, several companies square measure advocates of teaching workers however hackers suppose and add an endeavor to see whether or not a corporate network has been attacked yet on determine potential weaknesses and stop future hacking.

Moreover consulting corporations exist whose main aim is to instruct data technology connected professionals on the practices of moral hacking.

[2] University level courses square measure offered that concentrate on hacking and train the scholars a way to hack yet because the legal and moral implication of such practices.

A person World Health Organization accesses computers and knowledge hold on on computers while not legal permission of the owner.

Hackers are typically divided into several categories where some are ethical and others are unethical. White hat hackers are those who use their skill in a manner that most would clearly define as ethical. Black hat hackers are those individuals who are highly skilled but they use their skills in criminal and other activities.

Ethical hacking can be defined as the practice of hacking without malicious intent. They use the same tools and techniques as the intruders, but they neither damage the target systems nor steal information. Their main motto is to evaluate the target systems' security and report the same back to the concerned owners.

A particular student just can be taught how to hack but it is finally in their hands if they put their knowledge in a good practice or not.

Many universities and colleges must be aware of the risk and legal issues of adding ethical hacking courses to the curriculum. Moreover the concerned faculty must be help liable for the actions of their students. All the legal students must be considered when conducting penetration tests, in order to protect the universities' data. Colleges must take measures to guarantee the availability, confidentiality and integrity of data or to ensure access for authorized persons only. In addition schools that facilitated the creation of malware would be liable for damages from malware released from their laboratories.

Once a student is well trained about all the hacking skills certain policies must be applied at the University level to address certain issues about students conducting malicious acts.

Ethical concerns regarding obtaining consent from the original owner and the scenarios under which data could be obtained are identified.

The Digital Forensics field is still very young. At one extreme there are highly skilled researchers with strong background in computer science and mathematics pondering the esoteric inner working of technology in order to develop new forensic tools and techniques.

On the other end we have a frenzied market filled with service providers, software vendors and other specialists offering and every service that can even remotely be branded Digital Forensics by some contrition of logic.The background and related work include:

- Privacy Statistics
- Filesystem and Usage Statistics
- Existing Ethical codes
- Existing ethical quandaries and violations

[1] We must define the general issues and circumstances under which hard drives may be acquired for analysis.

These aspects are best summarized by asking four questions:

- Who is the seller?
- Is the seller the real data owner?
- How is the device being sold?
- What impediments does the selling method make to obtaining consent?

There are many scenarios where the general interaction between different types of media owners and methods of exchange. The further removed from direct exchange with the original owners and methods of exchange.

Here the media is not solicited by the researcher, but is instead offered for sale in general purposes. The sale is not generated because of media's research potential itself and is incidental.

The data already exists in the wild and is transferred to a third party would occur whether the researcher purchases it or someone else does.

The main areas of concern are:

- Privacy
- Ethics
- Mainstream cognizance

There are a lot of ethical tests to determine the need for consent and define how the data can and cannot be used to absent consent.

The tests are presented as a sequence of questions which guide the interpretation of a scenario to determine to what extent acquired data may be ethically used if at all.

Few questions that can help us when there is a breach are:

- Is it possible to determine whose consent is required?
- Does the effort of identifying the original owner negate the purpose of obtaining consent?
- Has the original owner forfeited an expectation of privacy?
- Is there any potential benefit gained from the violation?
- What steps will be taken to secure the data's confidentiality?
- To how many others will potentially private data be exposed?
- Will the data itself be made public?
- Will any monetary gain come from the data itself rather than from the research?

[4] As computer forensics plays a crucial role in crime investigation related to online, all the forensic investigators need to follow some rules and procedures in making the investigation process.

Although there are many approaches to get results, one who follows the rules and procedures in investigation process will be getting the efficient results. It is the professional responsibility to follow those rules as a forensic investigator. There exist different societies in making the investigation of digital crime which includes American Board of Criminalistics (ABC), American Academy of Forensic Science (AAFS), International Association of Computer Investigation Specialists (IACIS), SANS Institute etc. Different societies had different set of rules and procedures.

All those rules are certified as entities and any set of rules by those societies leads to the efficient and better investigation. Reviewing the primary reason for the expert guideline, advanced legal social orders are relied upon to have separate by-laws that direct the moves made upon expert misconduct. Nonetheless, the unimportant presence of an enforceability approach and procedures concentrated on the examination of a supposed moral code's infringement does not suggest that their execution, for example the real requirement, is a strategy inflexibly pursued by the legal science social orders. While the motivation behind the requirement is for the most part to the related activities of gathering proof supporting the unfortunate behaviour, deciding a real infringement of the code of morals, hearing and forcing approvals, and dealing with reestablishment strategies requires executional limit that not very many criminology associations have.

Legal Aspects n Digital Forensics is a major attention in todays world. Due to the lack of care as well as attention to the rules or legal aspects resulting in wastage of evidence. It also makes the users and stakeholders vulnerable. Since legal aspects in case of computer forensic investigation is most important. For any case related to cyber-crime, computer or digital forensics can make a solution and detects the hackers or intruders if any. But for each case one should have to submit the evidences to the court. Hence, without the attention and care towards legal aspects no one can make those evidences worth. Those evidences are worthless. Also, it leads to insecurity in terms of user security. But also, it will leave the officer who is investigating into vulnerability.

Generally Digital forensics itself a discipline. Digital Forensics involves many technological fields such as Computer Science, Maths, Physics etc. Hence it is a discipline. For the judgement related to this it will be very difficult. As the judgement involves many evidences related to science, one had to integrate and understand those evidences and gives judgement based on some disciplines. Also, in case of collection of data from the system, investigator had to be disciplined and ethical. Any abnormalities lead to trash/erase of data from the system which results in the destroy of digital evidence. Hence, all the process of investigations to be disciplined for better results. Hence, Digital Forensics itself a discipline.

[8] Forensic accounting is used in different fields like verifying and reporting of the financial data from the past and settling the current disputes that are faced based on that data. The main aim of forensic accounting is the elimination of fraud and its investigation.

The Forensic accountants provide the services like the net worth valuations and in asset valuations and they are helpful in the detection of fraudulent documents. Forensic accounting is helpful in the development of the evidence and to identify the perpetrator. There are different frauds in the criminology. The student should be capable of distinguishing the different crimes and should have clean observation of the cases.

Criminology is the study of the crime that enforces the laws. The study of criminology is mainly helpful in the crime rate detection and the trending analysis of the crimes in a particular region or culture.

[8] Criminal Fraud- Edwin H.Sutherland observed that white collar crime is identified as the common behaviour in the criminology.

Later Donald Cressey has developed the fraud triangle that describes the occurrence of the factors. The similar explanation is helpful in criminology and white-collar crime estimation. In the previous years the fraud that is done against any government agency is known as the criminal fraud and the one made against the non- government agencies are called tort law. In the present scenario the fraud done against non- government agencies is considered not only as a tort but also a crime. The topics like Information privacy, Interviewing, Regulatory and Professional Standards, Procedural law and evidence are discussed in this paper. Each forensic program should be allocated 2 distinct full-semester criminology courses. The ethics have to be developed among the students from these two courses that are merged in the curriculum.

The principles of digital evidence...

Principle 1: The action cannot be taken by the law enforcement agencies, The employees of these law enforcement agencies should change the data which is subsequently relied upon the court.

Principle 2: If a person needs to access the original data, the person must be able to give evidence explaining the implications of their actions

Principle 3: The processes applied to digital evidence have to be created and recorded. The third-party apps can be used to examine those applied processes and return the initial result.

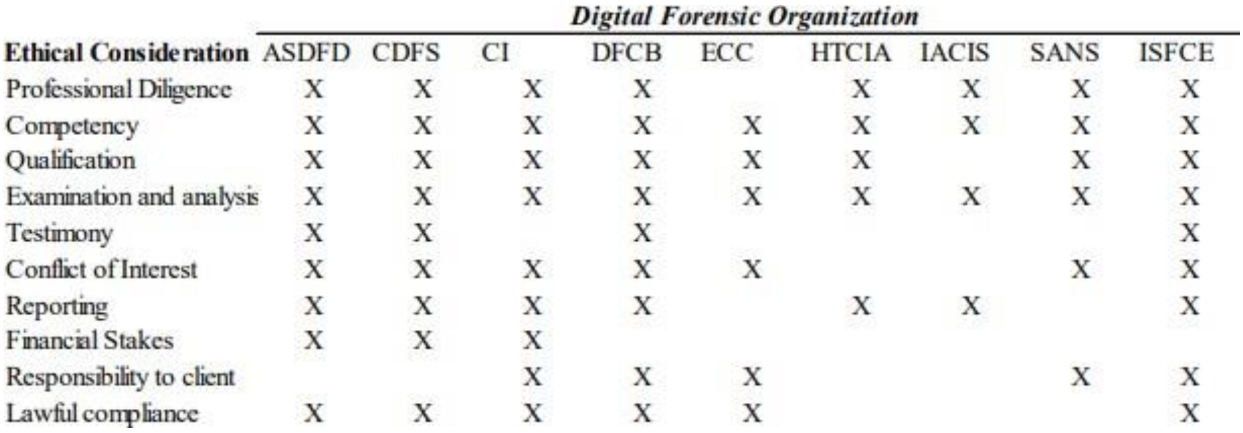
Principle 4: The investigation officer has all the responsibility to ensure that the law and principles must adhere.

The digital evidence has to be subjected to the rules and the laws that are applied to documentary evidence. The dogma of documentary evidence has to be explained so that the onus is on the prosecution to show the court that evidence that is present now is not less at present compared to the evidence that was initially taken into the control of law enforcement. In an operating system, the other program may alter the data by adding, deleting the contents in the electronic storage.

This might happen without the knowledge of the user that the data is being changed. In order to control that and agree with the principles of the digital evidence, the relevant image of the deice has to be made. This will make us understand that the original data is stored safely and that enables the third-party apps to re-examine the data and ensure to achieve the same result that is required by the above principles

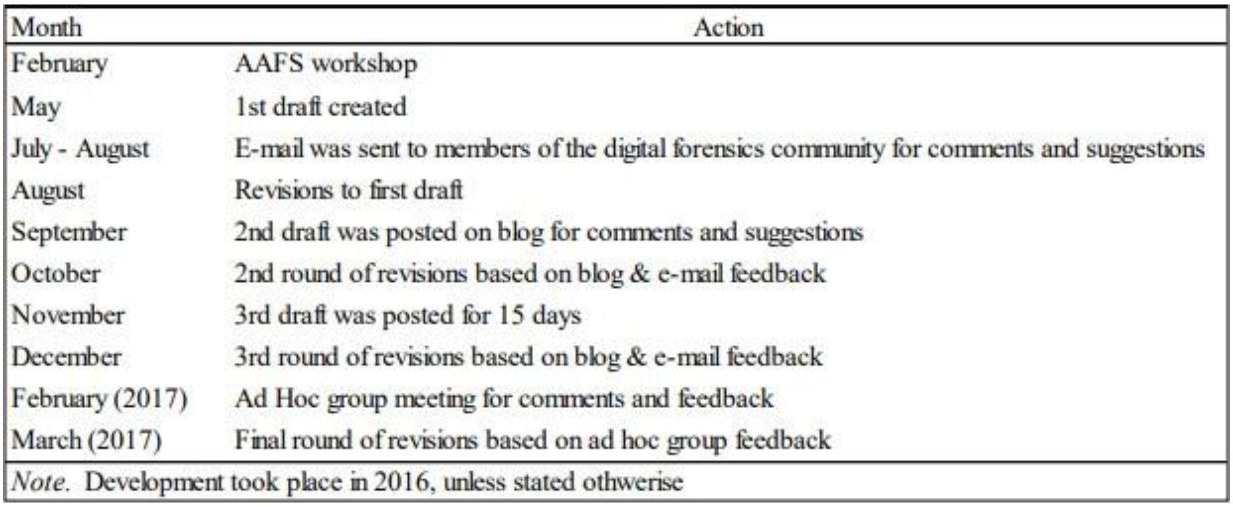
3. This is the logical file or the logical/physical block image of the device that contains the partial data which is captured by the triage process. The investigators should use their judgment to capture all the evidence that is relevant to the case if this approach is adopted. In cases like when we are dealing with the data at the remote but not stored locally and inaccessible in your location. In that case, it is not possible to obtain the image. There may be a situation to access to the original data to recover it. It is very essential that the person has to retrieve the data and able to give evidence to the court of law that makes any such access.

We need to display the objectivity in the court of law which is a very essential part as well as the integrity and the community of the evidence. There is also a necessary need for the evidence recovery demonstration which shows each process of how the evidence is recovered which shows each process by which the evidence is obtained.
The evidence has to be preserved so that when the third party is used it must be able to repeat the process and obtain the same result which was presented in the court. The application of these principles should not preclude the approach of the digital evidence examination.
The decision making of the conduct of digital investigation has the ability to make judgments regarding the focus and the scope of the investigation by considering the investigation resources. This also includes the risk assessment based on the non-technical and the technical factors, for example considering the potential evidence that is held by a particular type of device of the suspect, the process should be transparent and the decisions have to be justifiable and rationale recorded.



	Digital Forensic Organization								
Ethical Consideration	ASDFD	CDFS	CI	DFCB	ECC	HTCIA	IACIS	SANS	ISFCE
Professional Diligence	X	X	X	X		X	X	X	X
Competency	X	X	X	X	X	X	X	X	X
Qualification	X	X	X	X	X	X		X	X
Examination and analysis	X	X	X	X	X	X	X	X	X
Testimony	X	X		X					X
Conflict of Interest	X	X	X	X	X			X	X
Reporting	X	X	X	X		X	X		X
Financial Stakes	X	X	X						
Responsibility to client			X	X	X			X	X
Lawful compliance	X	X	X	X	X				X

Table 1 Sub-categorization of the Digital Forensic Codes of Ethics in Respect to Ethicalconsideration {Sharevski,2015}



Month	Action
February	AAFS workshop
May	1st draft created
July - August	E-mail was sent to members of the digital forensics community for comments and suggestions
August	Revisions to first draft
September	2nd draft was posted on blog for comments and suggestions
October	2nd round of revisions based on blog & e-mail feedback
November	3rd draft was posted for 15 days
December	3rd round of revisions based on blog & e-mail feedback
February (2017)	Ad Hoc group meeting for comments and feedback
March (2017)	Final round of revisions based on ad hoc group feedback
Note. Development took place in 2016, unless stated othwerise	

Table 2 - Timeline of the Development p rocess j or th e P ro ,fi ess ional Code of Ethics

The Code of ethics plays a major role in digital forensics. This paper deals with the steps involved in the development of this code of ethics. The digital forensics helps in the collection and validation of the evidence that is found in an illegal activity due to unauthorized actions. The digital devices and evidence are helpful in solving many cases in the courts. This paper includes a case study on the case of Chester Kwitowski where he was found in obtaining child pornography and there is another case where a person gets a job by providing fake certificates to the institute. These cases are emerging as the digital forensics has a weak code of ethics, unlike the law and medicine which were supported by the state and the federal law. If a person is banned from the digital forensic community he can be certified under a different organization. So there is a need in unification of the code of ethics in all the communities in the forensic study. The lack of standards will lead to the weakness of digital evidence. This article describes the definitions made by different authors to explain how important the code of ethics in digital forensics. The licensure/certification in the medicine and law has unique nature whereas in the digital forensics there are different licensing and they are paid licenses. The medicine and law students have to be experienced whereas the forensic study does not require any evidence and it mainly depends on the individual interests. Problem-solving capability plays a major role in the digital forensics study. The students should have knowledge of forensic tools along with computer knowledge, unlike the law and medicine.

Development of the code of ethics:

The development was initated by the AAFS conference as mentioned in the table 2. The four drafts is provided to show how the development has begun in the field of the digital forensics.

1. The first draft of the Professional code of ethics was sent out between July-August in 2016. AAFS has made a feedback system and sent the link to different groups those who attended their workshops and also NIST. Later from the feedback they got 3 comments and rectified the errors.
2. On September 7 2016 the second draft is made available in WordPress as an opensource so that they can easily track the visitors and the count. The website has received the 321 visitors and with the view count of 500. After 30 days the WordPress site is made offline and the site received 11 different comments and a single comment via email. They removed clause VI, subsection a that mentions that lawyer shouldn’t favour a side in the side he is employed. This statement is not agreed by many people so they removed that subsection in a clause. They also made some changes in clause V and the clause III is made as a subset of clause II.
3. The 3rd draft is later made available in the same website and it receive the 83 visitors and a 141 views and 2 comments where one of the comment is via email.
4. In February 2017 the fourth draft is available for suggestions and feedback. There is a unique comment received here and this was not addressed in any other drafts. A new clause is added that describes that the " individuals should hold paramount the welfare of the public, and a member shall put individuals over personal gain, while prioritizing the pursuit of truth."

V. Conclusion

Finally, the paper concludes on the note that the subject of forensic analysis requires the appending of the topic ‘legal and ethical principles of computer forensics’ to its curriculum. This will strengthen the character of individuals pursuing the carrier of forensic analysis and help them face any ethical dilemmas and take necessary action, or at-least refer the matter to a legal counsel.

VI. References

[1] Ethical Issues Raised by Data Acquisition Methods in Digital Forensics Research, Brian Roux and Michael Falgoust.

[2] Faculty Attitudes Toward Teaching Ethical Hacking to Computer and Information Systems Undergraduates Students. Aury M. Curbelo, Ph.D University of Puerto Rico, Mayaguez, Puerto Rico, aury.curbelo@upr.edu, Alfredo Cruz, Ph.D Polytechnic University of Puerto Rico, alcruz@pupr.edu.

[3] FORZA – Digital forensics investigation framework that incorporate legal issues. Ricci S.C. Ieong* eWalker Consulting Ltd, Unit 4 5/F, Block 2 Nan Fung Ind. City, 18 Tin Hau Road, Tuen Mun, Hong Kong, China.

[4] RULES OF PROFESSIONAL RESPONSIBILITY IN DIGITAL FORENSICS–A COMPARATIVE ANALYSIS Filipo Sharevski, Department of Computer and Information Technology, College of Technology Purdue, University West Lafayette, IN, 47906, fsharevs@purdue.edu.

[5] Legal Aspects of Digital Forensics, Daniel J. Ryan, The George Washington University, Washington_D.C., danjryan@gwu.edu. Gal Shpantzer, The George Washington University, Washington, D. C., gal@pikpuk.com.

[6] DIGITAL FORENSICS: OPERATIONAL, LEGAL AND RESEARCH ISSUES M. Pollitt, M. Caloyannides, J. Novotny and S. Shenoi.

[7] Research and Review on Computer Forensics∗ Hong Guo, Bo Jin, and Daoli Huang.

[8] Legal and Regulatory Environments and Ethics: Essential Components of a Fraud and Forensic Accounting Curriculum George E. Curtis.

[9] Development of A Professional Code of Ethics in Digital Forensics, Kathryn C. Seigfried-Spellar, Purdue University, kspellar@purdue.edu, Marcus Rogers, Computer Information & Technology, Purdue University, rogersmk@purdue.edu, Danielle M. Crimmins 2184089, Purdue University, dcrimmin@purude.ed.

[10] T. Clark. Designing Storage Area Networks: A Practical Reference for Implementing Fiber Channel and IP SANs. Addison-Wesley, Reading, Massachusetts, 2003.

[11] K. Egevang and P. Francis. RFC 1631: The IP network address translator. www.faqs.org/rfcs/rfc1631.html, 1994.

[12] M. Elmore. Big brother where art thou? Electronic surveillance and the Internet: Carving away Fourth Amendment privacy protections. Texas Tech Law Review, 32:1053–1083, 2001.

[13] Federal Bureau of Investigation. Digital evidence: Standards and principles. Forensic Science Communications, 2(2), April 2000.

[14] Federal Bureau of Investigation. Congressional Statement on Limited Expansion of the Predicate Offenses for Title III Electronic Surveillance. www.fbi.gov, 2001.

[15] A. Freier, P. Karlton and P. Kocher. The SSL Protocol Version 3.0. IETF (draft-ietf-tls-ssl-version3-00.txt), November 1996.

[16] K. Inman and N. Rudin. Principles and Practices of Criminalistics: The Profession of Forensic Science. CRC Press, Boca Raton, Florida, 2001.

[17] International Organization on Computer Evidence. G8 Proposed Principles for the Procedures Relating to Digital Evidence. www.ioce.org, 2000.

[18] C. Kirby. Cyber sleuths: Computer forensics booms as importance of electronic evidence grows. San Francisco Chronicle, February 26, 2001.