Post Incident Analysis Framework for Automated Video Forensic Investigation

Abdullah AlShaikh
Faculty of Computing, Engineering and Sciences, Staffordshire University, United Kingdom

Mohamed Sedky
Faculty of Computing, Engineering and Sciences, Staffordshire University, United Kingdom

ABSTRACT
The need for proper and acceptable forensic process is necessary due to the proliferation and advancement of high digital technology in all aspect of our life. Also the desire and needs for optimizing time and cost of doing things push humans to deeply depend on digital data for decision making. The legal system has also been investing heavily on this area to develop a framework and technology improvement. Therefore there is a need for an automated video forensic investigation tool and a proper development of a framework that can address the sensitive issues associated with this application. A crime culprit may walk scot-free or an innocent suspect may suffer negative consequences, both monetary and otherwise, simply on account of a forensics process or investigation that was inadequate or improperly conducted. Computer related crime are on the rise and skipping one aspect of forensic process or step may result into incomplete or inconclusive result of investigation that may affect interpretation and conclusions in a court of law. In this paper, we propose a novel automated post incident analysis framework which is able to tackle the challenges of video, realistic and practical outdoor surveillance scenarios.

General Terms
Computer Forensics, Digital Video, Incident Analysis, Digital Investigation.

Keywords
Video Forensic Investigation, Post Incident Analysis, Evidence Collection, Automated Video Analysis.

1. INTRODUCTION
Digital Video generally refers to the capturing, manipulating and storage of moving images that can be displayed on computer screen [1]. The word digital refers to a system based on discontinuous events as opposed to analogue. Prior to digital era, to display analogue video images on a computer, the video signal had to first be converted from analogue to digital [2]. However, camera and a microphone capture the picture and sound of a video session and send analogue signals to a video-capture adapter board. The board only captures half of the number of frames per second that movies use in order to reduce the amount of data to be processed. Second, there is an analog-to-digital converter chip on the video-capture adapter card, and it converts the analogue signals (waves) to digital patterns (0s and 1s). Third, a compression/decompression chip or software reduces the data to a minimum necessary for recreating the video signals [3].

What makes video so attractive to many, particularly digital is becoming more popular than ever, is as a result of being easy to manipulate. The difference between analogue and digital is like comparing a typewriter with a word processor. Digital video files can be very large. For example, one single frame from a television image with a resolution of 720 x 576 pixels and a color depth of 16 bits has a size of 1.35MB [4].

Digital videos are becoming more popular and accessible through the various media technology advances which enable users to capture, manipulate and store video data in efficient and inexpensive ways. With the increasingly efficient compression formats and easiness of integrating videos in web pages, more people are able to enjoy producing and publishing movies in the digital world.

Digital video is video recorded as digital data which can be stored, manipulated and edited on a computer. Digital video differs from analogue video in a number of important ways: Digital video cameras are smaller and lighter than VHS camcorders, and have better picture quality. The key difference however, is the ease with which digital video can be edited. This enables users to produce video of a higher standard in a shorter time. Digital video is also easier to share via the Internet and integrate with other ICT applications, such as presentation software. With this development the need for digital or analogue video forensic as legal evidence as well as detection of forgery is necessary and important. This study thus presents a post incident analysis framework that can be used for digital video forensic investigation.

2. PREVIOUS WORK
In literature, combination of video fingerprints and registration in a fully automatic semi-blind forensic scheme is promising for forensic analysis [5]. Most organizations underestimate the demand for digital evidence [6]. Ttraditionally, the digital forensic process begins with the collection, duplication, and authentication of every piece of digital media prior to examination, these first three phases of the digital forensic process are by far the most costly [7]. Computer evidence is becoming a routine part of criminal cases with nearly 85% of current caseloads involving digital evidence [8]. Computer crimes are on the rise and unfortunately less than two percent of the reported cases result in conviction [9]. Computer forensics can be traced back to as early as 1984 when the FBI laboratory and other law enforcement agencies begun developing programs to examine computer evidence. Research groups like the Computer Analysis and Response Team (CART), the Scientific Working Group on Digital Evidence (SWGDE), the Technical Working Group on Digital Evidence (TWGDE), and the National Institute of Justice (NIJ) have since been formed in order to discuss the computer forensic science as a discipline, including the need for a standardized approach to examinations. Some previous work in the literature conclude that computer and network forensics frameworks consist of three basic components that [10] refer to as the basic building blocks in computer forensics investigations. These are: acquiring the evidence while ensuring that the integrity is preserved; authenticating the validity of the extracted data, which involves making sure that it is as valid as the original

and analyzing the data while keeping its integrity. Some process models that put the three factors into consideration include the Forensics Process Model [11], the Abstract Digital and the Integrated Digital Investigation Model popularly called IDIP which organized the process into five phases: Readiness phase, Deployment phase, Physical Crime Scene Investigation phase, Digital Crime Scene Investigation phase and the Review phase. All these phases have specific roles to play in ensuring reliable digital data forensic evidence. The objective of the Readiness phase is to ensure operations and infrastructure are able to fully support an investigation, while the Deployment phase is to provide a mechanism for an incident to be detected and confirmed. The main objective of Physical Crime Scene Investigation phase is to collect and analyze the physical evidence and reconstruct the actions that took place during the incident. The goal of Digital Crime Scene Investigation phase is to collect and analyze the digital evidence that was obtained from the physical investigation phase and or through any other future way round, and finally, Review phase reviews the whole investigation and identifies areas of improvement if necessary. This proposal was later enhanced and came up with Enhanced Digital Investigation model EIDIP, which separates the investigations at the primary and secondary crime scenes while depicting the phases as iterative instead of linear. It is based on the IDIP model and expands the deployment phase in the IDIP model to include the physical and digital crime investigations, while introducing a new phase dedicated to tracing back to the computer (the primary crime scene) that was used as a tool to commit the offense.

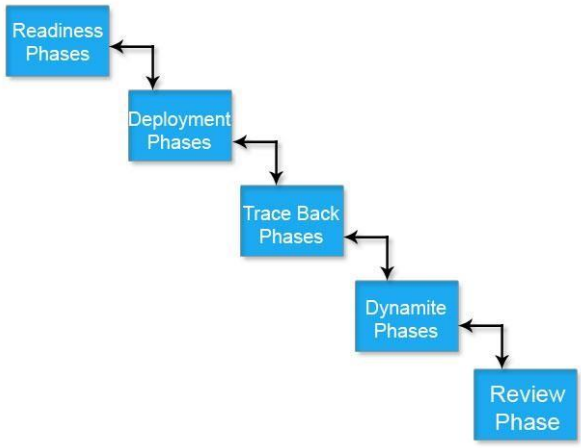

Fig 1: Enhanced Digital Investigation model (EIDIP)

2.1 Video forensics and interviews

Video forensics as a discipline demands specially trained personnel, support from management, and the necessary funding to keep a unit operating, and this can only be attained by constructing a comprehensive training program for examiners, which is mostly police personnel by providing sound digital video evidence recovery techniques, and a commitment to keep any developed unit operating at maximum efficiency [12]. The ability of Police personnel to follow the standard approach to video classification involves three major stages [12]: First, local visual features that describe a region of the video are extracted either densely [13] or at a sparse set of interest points [14] and [15]. Next, the features get combined into a fixed-sized video-level description. One popular approach is to quantize all features using a learned k-means dictionary and accumulate the visual words over the duration of the video into histograms of varying spatiotemporal positions and extents [16] Lastly, a classier (such as an SVM) is trained on the resulting "bag of words" representation to distinguish among the visual classes of interrogation. Participation in the legal system and testifying in court are associated with poorer mental health outcomes, especially when the experiences are particularly stressful for the individuals concerned [17]. It is difficult to estimate the time required to complete a full investigation. Information gained in investigative interviews thus plays a crucial role in the investigation of a crime. Fortunately, more than 30 years of research on crime interviewing clearly shows how investigative interviews should, and should not, be conducted [17]. The most reliable information is obtained when interviewers use open-ended prompts for information such as "tell me what happened?" and "tell me more about that;" such prompts also yield information that is most likely to be accurate. Professionals have also translated research findings into guidelines for interviewers such as the Memorandum of Good Practice, Achieving Best Evidence, the NICHD Protocol and the Guidance for Interviewing Child Witnesses and Victims in Scotland. The survey yielded further support for suggestions that investigative interviews with children should be electronically recorded [18]. Furthermore, the quality of interviews must be independently and regularly checked to ensure that standards are achieved and maintained. Make an initial assessment about the type of case being investigated. The interviewer or investigator should systematically follow the following [19].

1. Determine a preliminary design or approach to the case
2. Create a detailed design
3. Determine the resources you need
4. Obtain and copy an evidence
5. disk drive
6. Identify the risks
7. Mitigate or minimize the risks
8. Test the design
9. Analyze and recover the digital evidence
10. Investigate the data you recovered
11. Complete the case report
12. Critique the case

3. DEVELOPMENTS IN VIDEO FORENSICS

Several methods which are camera-based, coding-based, and geometrical/physical inconsistencies are used to assist in video forensics. With consideration to camera-based video forensics, some artifacts left behind are exploited for both camera identification and tampering detection [20]. Photo Response Non-Uniformity (PRNU) fingerprint technique was proposed by [21] which aids in detecting different kind of attacks. Other works in this area include the use of noise acquisition device to detect tampered regions in static scenes carried out by [13]. Even though there are several research in this area generally, this method works better when the video under consideration is uncompressed. Practically, most videos recovered from recording devices are usually compressed and as such, this method may not be effective and applicable to compressed video.

Considering coding-based video forensics, forensic experts exploit the presence or irregularities in coding artifacts to assist in detecting tampering in videos. Research done by [15] exploited tampering detection, focusing on the assumption of double and single compression of videos. Several other works are done in this area but it should be noted that most of the assumptions carried out by researchers do not apply in real life situations and up till now, there is no clear standard as to what extent using coding-based techniques could assist in presenting evidence in the court room.

For detection considering geometry or physical lighting properties of a crimes scene, it is very difficult to justify as whether such a scene is consistent or not. Several algorithms have been developed over the years considering this method including [22], which considers "ghost shadows" and [16] who are concerned with three-dimensional parabolic trajectory with considering of objects in a video. The above mentioned methods are useful in handling particular tasks. However, there are no defined patterns as to how these methods may assist in presenting the evidence recovered from such videos in the court of law. We hereby propose a video analytic-based video forensic framework showing how the evidence could be analysed in order to be acceptable in the court of law.

3.1 Legal Requirements

Digital forensic as a discipline comprises Information Assurance, and is perhaps one most closely defined by legal requirements and one whose growth and evolution is informed and guided by case law, regulatory changes, and the ability of cyber lawyers and digital forensics experts to take the products of forensic tools and processes to court. The tension between privacy rights and law enforcement's need to search and seize digital evidence sometimes mirrors, and frequently extends, the extant tensions inherent in rules of evidence. Technology is present in every aspect of modern life. At one time, a single computer filled an entire room. Today, a computer can fit in the palm of your hand. Criminals are exploiting the same technological advances which are driving forward the evolution of society, today, virtually every business and personal document is prepared on a computer and mobile, hand-held devices, it is the use of specialized techniques for recovery, authentication and analysis of electronic data when a case involves issues relating to reconstruction of computer usage, examination of residual data, and authentication of data by technical analysis or explanation of technical features of data and computer usage. Computer and digital forensics is useful for the detection and investigation of crime committed on computers, computer networks, the internet and other digital devices with the intent of giving digital evidence in law courts and tribunals [23]. It is also the professional extraction and handling of potential electronic evidence from any digital device or digital storage media to assist investigators, prosecutors, and the trier of fact (Judges, magistrates and members of tribunals) in a criminal justice system in arriving at the right judgment in litigation. In July, 2011, Nigeria as an African Country, signed into law her Evidence Act, 2011which recognizes electronic, digital and computer generated evidence. No doubt that this singular act has the capability to transform our legal and judicial systems. As electronic evidence grows in both volume and importance in criminal and civil courts, judges and magistrates need to fairly and justly evaluate the merits of the offered evidence. To do so, prosecutors, investigators, judges and magistrates need a general understanding of the underlying technologies and applications from which forensic evidence is derived and the appropriate standards that must be met. There is need for standards document aimed principally for the police officers, law-enforcement and security agents, military officers, prosecutors, anti-corruption agencies, regulatory agencies, other public sector investigators and private sector investigators working for their organizations and those working in conjunction with law enforcement. However, some work in the literature indicate pointed out that, every investigative process that reach the point where specific competency questions are answered, digital evidence must survive the threshold test posed by [18] of its competency as a class of evidence. The Court further clarified that the admissibility inquiry must focus "solely" on the expert's "principles and methodology," and "not on the conclusions that they generate. So, digital forensic evidence proposed for admission in court must satisfy two conditions: it must be (1) relevant, arguably a very weak requirement, and (2) it must be "derived by the scientific method" and "supported by appropriate validation. Digital forensics is, of course, highly technical, and therefore grounded in science, computer science, mathematics, physics, and so forth. It is also a discipline that requires knowledge of engineering, particularly electrical, mechanical and systems engineering. And applying the science and engineering in specific investigations is a complex process that requires professional judgment that is sometimes more art than science.

3.2 Legal Evidence

As technology advance hence the need for dealing with digital evidence, to achieved the process general forensic and procedural principles should be applied like actions taken, Persons conducting an examination of digital evidence and activity relating to the seizure, examination, storage, or transfer of digital evidence should be documented, preserved, and available for review. The digital forensic process is a recognized scientific and forensic process used in digital forensics investigations [11]. Digital forensics process is defined as a number of steps from the original incident alert through to reporting of findings. The process is predominantly used in computer and mobile forensic investigation and consists of three steps: acquisition, analysis and reporting.

Digital media seized for investigation is usually referred to as an "exhibit" in legal terminology. Investigators employ the scientific method to recover digital evidence to support or disprove hypothesis, either for a court of law or in civil proceedings. Various types of techniques are used to recover evidence, usually involving some form of keyword searching within the acquired image file; either to identify matches to relevant phrases or to parse out known file types. Certain files (such as graphic images) have a specific set of bytes which identify the start and end of a file, if identified a deleted file can be reconstructed. Many forensic tools use hash signatures to identify notable files or to exclude known (benign) ones; acquired data is hashed and compared to pre-compiled lists such as the Reference Data Set (RDS) from the National Software Reference Library. On most media types including standard magnetic hard disks, once data has been securely deleted it can never be recovered. SSD Drives are specifically of interest from a forensics viewpoint, because even after a secure-erase operation some of the data that was intended to be secure-erased persists on the drive. Once evidence is recovered the information is analysed to reconstruct events or actions and to reach conclusions, work that can often be performed by less specialist staff [24].

3.3 Video Forensic Framework Review

Frequently cited definition for Digital Forensic Science is that of the Digital Forensic Research Workshop (DFRWS) of 2001: 'The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations' [25]. But as a result of advancement in technology most organization especially business firms relies heavily on software application and internet technology to operate and improve their business, and these businesses depend on the digital devices to process, store and recover data. A large amount of information is produced, accumulated, and distributed via electronic means. Recent study demonstrates that in 2008 98% of all document created in organization were created electronically [6] and approximately 85% of 66 million U.S. dollars was lost by organizations due to digital related crime in 2007. In 2008, Ehud Tenenbaum was extradited from Canada on suspicion of stealing $1.5million from Canadian bank through stolen credentials and infiltrated computers. Cybercrime reports indicates a complex online fraud which scammed over £1 million pounds from taxpayers in 2009. Some work in the literature defined digital forensic as the use of scientifically derived and proven methods toward the identification, preservation, collection, validation, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations. Digital evidence derived not only from computer devices such as hard drive and memory chip generic media, like mobile phones, portable computers, PDA's, network traffic contents can certainly be used to represent digital evidence before the court of law. However, in some study it was proved that methodologies from physical forensics is possible to be adopted into digital forensics, specific forensic software is created, and comprehensive knowledge is obtained by digital forensic specialist to defeat digital criminality. The use of digital device to carryout criminal activity, evidence or otherwise known as digital evidence can be obtain from fraud, theft of or destruction of intellectual property. This evidence is any data that can provide a significant link between the cause of the crime and the victim. Digital evidence is naturally fragile because it is easily altered, modified, copied and damaged or destroyed as a result of improper handling or analysis. This may influence the result of its original state, thus precaution should be taken when documenting, collecting, preserving and examining digital evidence [26]. Digital evidence is a data of investigative value that is stored on or transmitted by a digital device. Therefore digital evidence is hidden evidence in the same way that Deoxyribonucleic Acid (DNA) or fingerprint evidence is hidden. In its natural state, digital evidence cannot be known by the content in the physical object that holds such evidence. Investigative reports may be required to explain the examination process and any limitation [26].

Previous research output present a number of published model or frameworks in the area of digital forensic, many of this output fundamentally used the concept or ideas derived from traditional methodology popularly known as physical forensic evidence collection of digital evidence strategy as practice by police or any law enforcement agent. Such frameworks are previously examined by [24] for digital forensics. The authors argued that the proposed model can be term as an enhancement of the Digital Forensic Research Workshops (DFRWS) 2001 therefore their model involves nine components such as:

Identification – it recognises an incident from indicators and determines its type. This component is important because it impacts other steps but it is not explicit within the field of forensic.

Preparation – it involves the preparation of tools, techniques, search warrants and monitoring authorization and management support.

Approach strategy – formulating procedures and approach to use in order to maximize the collection of untainted evidence while minimizing the impact to the victim.

Preservation – it involves the isolation, securing and preserving the state of physical and digital evidence.

Collection – This is to record the physical scene and duplicate digital evidence using standardized and accepted procedures.

Examination – An in-depth systematic search of evidence relating to the suspected crime. This focuses on identifying and locating potential evidence.

Analysis – This determines importance and probative value to the case of the examined product.

Presentation - Summary and explanation of conclusion.

Returning Evidence – Physical and digital property returned to proper owner.

4. PROPOSED FRAMEWORK

Currently, forensic research focuses mainly on identification, individualisation and association at the source level. Even though a forensic expert aims at achieving any of these, considering video forensics, the court of law finds it difficult accepting evidence which they are not so sure how it was handled. Figures 2 and 3 give a description of our proposed framework.

The Ten (10) steps are explained below:

Evidence collection:

Devices that contain video footages should be identified and acquired from all the relevant sources. Digital Video Recorders (DVRs) and Network Video Recorders (NVRs) serve as a source of input evidence. For this input to be used as legal evidence, which is the focus of this research, it is important that the recording device includes embedded proof of authentication. Recordings such as DVR4C cannot be manipulated/altered without being noticed, and as such can guarantee the authenticity or integrity of the recording. Most DVRs has the capability to perform the above tasks successfully.

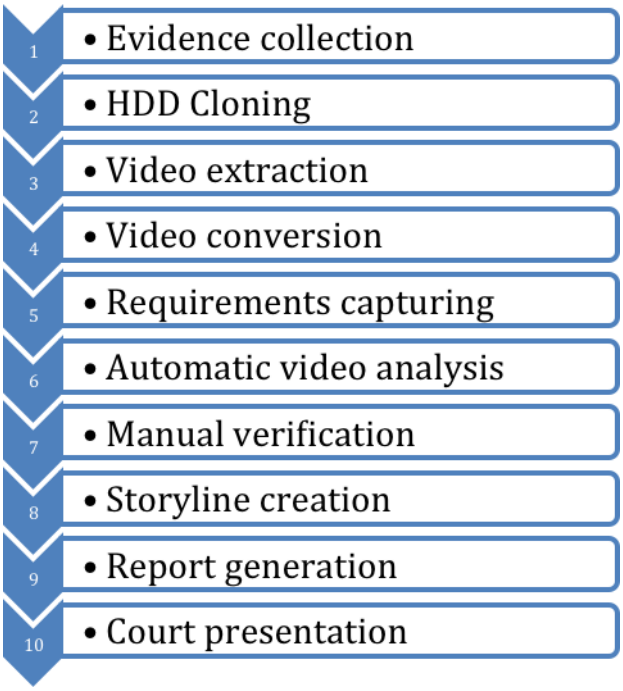

Fig 2: Evidence Analysis Framework

Hard Disk Drive (HDD) cloning:
Cloning the HDD means making an exact copy of the evidence collected in step 1 and saving to another storage media. This is done to avoid issues of manipulating the original evidence on the original HDD. The original HDD can be cloned as many times as possible without manipulating its contents. All experiments must be performed on the cloned HDD and not the original HDD.

Video extraction:
Retrieving the required evidence from the cloned HDD is carried out in this step. This is done to have access to the content of the cloned HDD. DVRs and NVRs can archive videos to a USB flash drive, external Hard Disk Drive (HDD), or other storage devices. This recording is usually in a digital format. Archiving the video and audio must be done consistently.

Video conversion
The video and audio must be converted to the right format for both viewing and analysis. Most of DVRs and NVRs store videos in their proprietary formats. There is every need to convert the collected evidence from the DVR/NVR proprietary format to a standard format in order to apply the video analytic tool.

Requirements capturing:
Police officers define the events to be detected from the video footages, by specifying area(s) as well as events that they want the video analytic tool to consider. For example, a suspect wearing red clothes and green hat, or a criminal walking or running in a particular direction or hanging around for the video length of time.

Automated video analysis:
A careful analysis of the evidence is important. This step automates the investigation process. A video analytic tool can generate a report detailing the start and end of each event. The list of events that happened per day, or per week, or per month, or even per year will be properly reported. Failure to properly analyse the evidence entails a miss of target for the evidence sought for.

Manual verification
In order not to take laws into their hands, the police officers manually verify and select relevant events from the events detected by the video analytic tool. Irrelevant events are not considered after careful examination by police experts.

Building a storyline
An investigation story board gives a sequence of events, typically with some directions and dialogue, representing the patterns of events.

Report generation
A report for the results of the analysis should be written down. This report should include issues like actions taken, why such actions were taken, findings made from the actions taken and recommendations for improvements to policies, guidelines and other aspects of forensic process amongst other issues.

Court presentation
The evidence in a DVD must be provided to the court. This helps the court to be sure that forensic expert and/or police officers are not formulating stories. The court has the right to get a clone of the DVD and give it to another expert to double check the evidence.

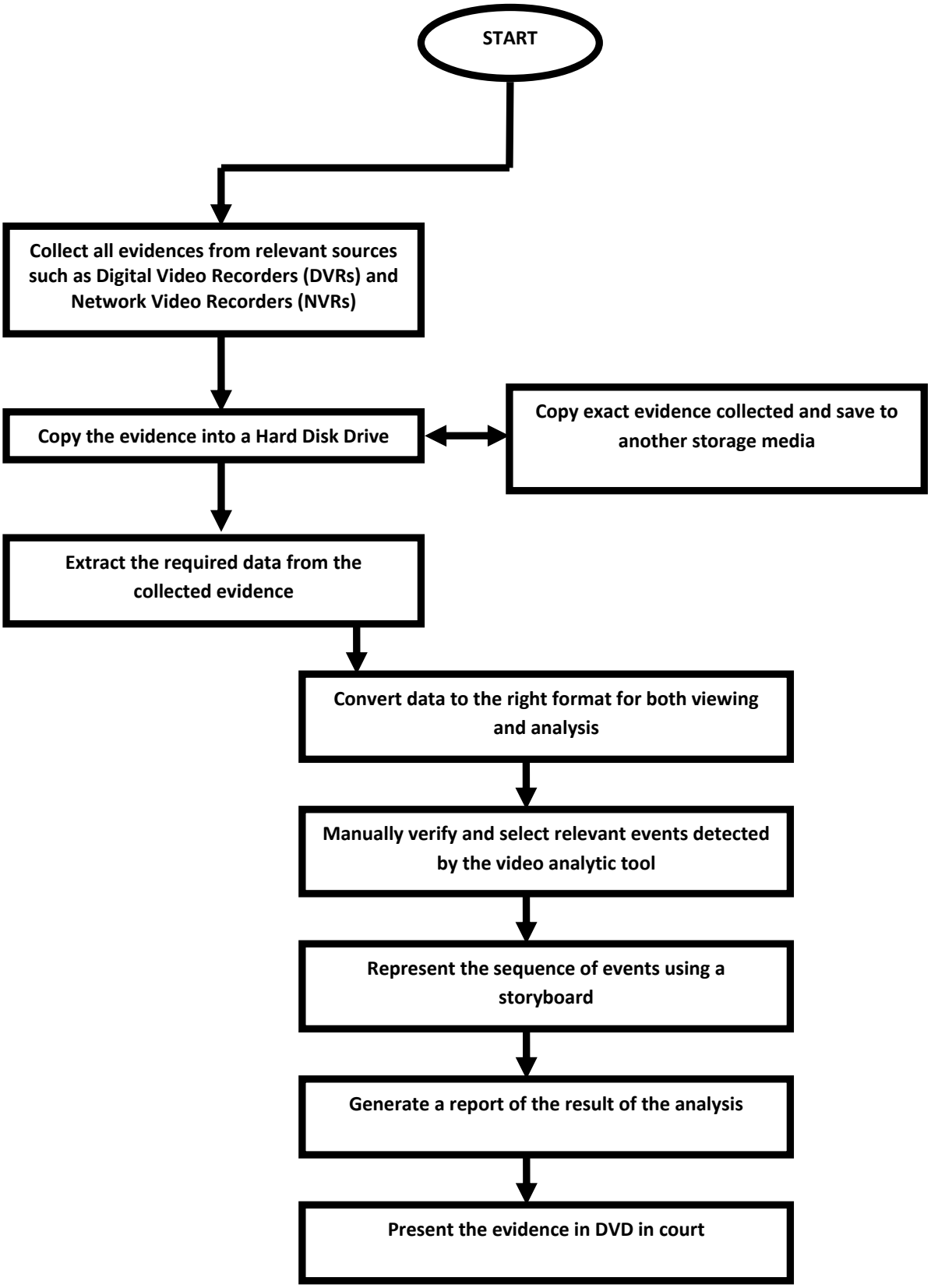

Fig 3: Detailed Workflow for the Proposed Framework

5. CONCLUSION

Digital evidence must be properly admissible, precise, authenticated and accurate in order to be accepted in the court of law. Because of fragile nature of digital evidence the process must be handled properly and carefully. A detailed digital forensic process provides important assistance to

forensic investigators in gathering evidence admissible in the court of law. In our study we conclude further that, there is need to have standard guideline for investigators. The digital forensic community needs a structured framework for rapid development of standard operational procedures that can be tested effectively and validated quickly. Digital forensic practitioners can benefit from the iterative structure proposed in this research to build forensically sound case and also for the development of consistent and simplified forensic guides on digital forensic investigation that can be a guideline for standard operational procedure and a model for developing future technology in digital forensic investigation.

Another important conclusion that can be drawn from this study is that Enhanced Integrated Digital Investigation Process is an improved version of Integrated Digital Investigation Process Model. This is because it is capable of describing the development right from the point when the initial infrastructure is put in place, to investigate when incident is reported through what it called trace back phase. In our study this improved version is tested and concludes that it is suitable for cyber crime investigation.

6. REFERENCES

[1] Lycos Tech Glossary. 1999. http://webopedia.lycos.com/Multimedia/Video/video.html

[2] Vaughan, T. 1998. Multimedia: Making it Work (4th ed.). Berkeley, CA: McGraw-Hill.

[3] White, R. (1999). How Computers Work. Indianapolis, IN: QUE

[4] Fisher, B. and Schroeder, U. 1999. http://www7.tomshardware.com/video

[5] Baudry, S., Chupeau, B. and Lefèbvre, F. 2008. "A Framework for Video Forensic base on Local and Temporal Fingerprint" Thomson R&D France Security Competence Center 1, avenue de Belle-Fontaine, 35576 Cesson-Sévigné Cedex, France

[6] Sommer, P. 2005. Directors and Corporate Advisors' Guide to Digital Investigations and Evidence. Information Assurance Advisory Council, http://www.iaac.org.uk, accessed 3 June 2014.

[7] Cantrell, G., Dampier, D.A., Dandass, Y.S., Niu, N. and Bogen, A.C.2012. Research toward a Partially-Automated, and Crime Specific Digital Triage Process Model. Computer and Information Science 5(2): 29-38 (2012)

[8] Meadaris. 2006. Grants to help develop ways to improve digital evidence collection. October 2006. Purdue University.

[9] Venansius Baryamureeba, Florence Tushabe. "The Enhanced Digital Investigation Process Model." *Digital Forensic Research Workshop* (2004): 1-9.

[10] Kruse II, Warren and Jay, G. Heiser. 2002. Computer Forensics: Incident Response Essentials. Addison-Wesley.

[11] National Institute of Justice. 2001. Electronic Crime Scene Investigation A Guide for First Responders. http://www.ncjrs.org/pdffiles1/nij/187736.pdf

[12] Dee, H. M., Velastin, S. 2008. 'How close are we to solving the problem of automated visual surveillance?' in Machine Vision and Applications, vol. 19, no. 5-6, pp. 329-343.

[13] Kobayashi, M., Okabe, T. and Sato, Y. 2010. Detecting forgery from static-scene video based on inconsistency in noise level functions, Information Forensics and Security, IEEE Transactions on 5 (4) (2010) 883{892.

[14] Wang, W. and Farid, H. 2006. Exposing digital forgeries in video by detecting double mpeg compression, in: Proceedings of the 8th workshop on Multimedia and security, ACM, 2006, pp. 37{47.

[15] Wang, W. and Farid, H. 2009. Exposing digital forgeries in video by detecting double quantization, in: Proceedings of the 11th ACM workshop on Multimedia and security, ACM, 2009, pp. 39{48.

[16] Conotter, V., O'Brien, J.F., and Farid, H. 2012. Exposing Digital Forgeries in Ballistic Motion, IEEE Transactions on Information Forensics and Security, v.7 n.1, p.283-296, February 2012

[17] Quas J.A, Goodman G.S, Ghetti S, Alexander KW, Edelstein R, Redlich A.D, Cordon I.M, Jones D.P.H, . 2005. Childhood sexual assault victims: Long-term outcomes after testifying in criminal court. Monographs of the Society for Research in Child Development. 2005;70:1–145.

[18] Scottish Executive. 2003. Guidance on Interviewing Child Witnesses and Victims in Scotland Edinburgh: Author.

[19] Sternberg, K. J., Lamb, M. E., Davies, G. A. & Westcott, H. L. 2001. The Memorandum of Good Practice: Theory versus application. Child Abuse and Neglect. 25,669-681.

[20] Farid, H. 2006. Exposing digital forgeries in scienti c images, in: Proceedings of the 8th workshop on Multi-media and security, ACM, 2006, pp. 29{36.

[21] Mondaini., 2007. Detection of malevolent changes in digital video for forensic applications. In: Proc. of SPIE Int. Conf. on security, steganography and watermarking of multimedia, pp. 65050

[22] Jing Zhang , Yuting Su , Mingyu Zhang,. 2009. Exposing digital video forgery by ghost shadow artifact, Proceedings of the First ACM workshop on Multimedia in forensics, October 23-23, 2009, Beijing, China

[23] NITDA. 2014. National Information Technology Development Agency. www.nitda.gov.ng

[24] Reith, M., Carr, C. and Gunsch, G. 2002. An Examination of Digital Forensic Models. International Journal of Digital Evidence, Vol. 1 No. 3. Online: http://www.ijde.org/docs/02_fall_art2.html [visited 30 June 2014]

[25] DFRWS. 2001. DFRWS Technical Report: A Road Map for Digital Forensic Research, Utica, New York.

[26] Carrier, B. and Spafford, E.H. 2003. Getting Physical with the Investigative Process International Journal of Digital Evidence, vol. 2, Issue 2.