International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 11 Issue 1 –NOVEMBER 2014.

Digital Forensic Investigation Model

Ch. Pavani

Dept. of M.Sc (CS), K.B.N P.G College, Vijayawada

chitrapu.pavani@gmail.com

***Abstract*— Digital Forensics is the science of obtaining, preserving, and documenting evidence from digital electronic storage devices, such as computers, PDAs digital cameras, mobile phones, and various memory storage devices. All must be done in a manner designed to preserve the probative value of the evidence and to assure its admissibility in a legal proceeding. Computer forensics emerged in response to the escalation of crimes committed by the use of computer systems either as an object of crime, an instrument used to commit a crime or a repository of evidence related to a crime. Digital forensics is a branch of forensic science concerned with the use of digital information produced, stored and transmitted by computers as source of evidence in investigations and legal proceedings. Digital forensic science provides tools, techniques and scientifically proven methods that can be used to acquire and analyse digital evidence. The digital forensic investigation must be retrieved to obtain the evidence that will be accepted in the court. Digital forensics has existed for as long as computers have stored data that could be used as evidence. For many years, digital forensics was performed primarily by government agencies, but has become common in the commercial sector over the past several years. In this paper we provide a brief overview of digital forensics Process, the need of the "Digital Forensic Investigation Model" which is currently an active area of research in the academic world, which aims to ameliorate procedures followed in this field. At last, we discuss challenges and future scope of digital forensics.**

Keywords
Cyber Crime, forensics models, Investigation, Analysis, digital devices, Digital forensics, Investigation model, forensics process, digital crime, digital devices.

I. INTRODUCTION

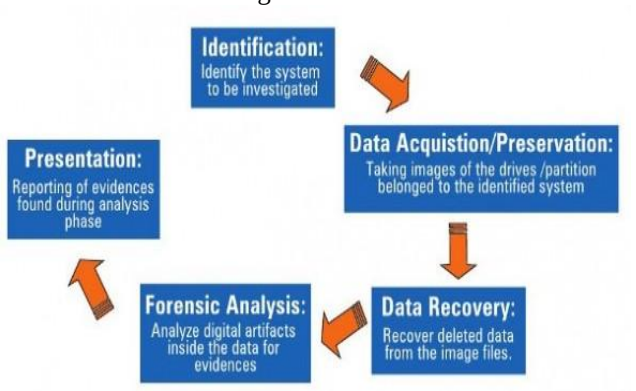
Digital Forensic Research Workshop has defined digital forensics as "The use of scientifically derived and proven methods toward the preservation, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations."

Digital Forensic Investigation Model

The preceding section discussed the basic concepts of an investigation and it never used the word forensic. To determine where, if at all, the term forensic can be applied we will first consult its definition. The American Heritage Dictionary defines forensic as an adjective and "relating to the use of science or technology in the investigation and establishment of facts or evidence in a court of law." Therefore, to be considered forensic, a process must use science and technology and the results must be able to be used in a court of law. With digital evidence, technology is always needed to process the digital data and therefore the only difference between a forensic and a non-forensic investigation of digital data is whether or not the evidence can be used in a court of law. A forensic investigation is a process that uses science and technology to develop and test theories, which can be entered into a court of law, to answer questions about events that occurred.

Digital Analysis Types

A digital investigation may encounter many formats of digital data and therefore there exist several types of analysis. The different analysis types are based on interpretation, or abstraction, layers, which are generally part of the data's design. For example, consider the data on a hard disk, which has been designed with several interpretation layers. The lowest layer may contain 3 partitions or other containers that are used for volume management.



Media Analysis: The analysis of the data from a storage device. This analysis does not consider any partitions or other operating system specific data structures. If the storage device uses a fixed size unit, such as a sector, then it can be used in this analysis.

Media Management Analysis: The analysis of the management system used to organize media. This typically involves partitions and may include volume management or RAID systems that merge data from multiple storage devices into a single virtual storage device.

File System Analysis: The analysis of the file system data inside of a partition or disk. This typically involves processing the data to extract the contents of a file or to recover the contents of a deleted file.

Application Analysis: The analysis of the data inside of a file. Files are created by users and applications and the format of the contents are application specific.

Network Analysis: The analysis of data on a communications network. Network packets can be examined using the OSI model to interpret the raw data into an application-level stream.

Application analysis is a large category of analysis techniques because there are so many application types.

Some of the more common ones are listed here:
OS Analysis: An operating system is an application, although it is a special application because it is the first one that is run when a computer starts. This analysis examines the configuration files and output data of the OS to determine what events may have occurred.

Executable Analysis: Executables are digital objects that can cause events to occur and they are frequently examined during intrusion investigations because the investigator needs to determine what events the executable could cause.

Image Analysis: Digital images are the target of many digital investigations because some are contraband. This type of analysis looks for information about where the picture was taken and who or what is in the picture. Image analysis also includes examining images for evidence of steganography.

Video Analysis: Digital video is used in security cameras and in personal video cameras and web-cams. Investigations of on-line predators can sometimes involve digital video from web-cams. This type of analysis examines the video for the identify of objects in the video and location where it was shot.

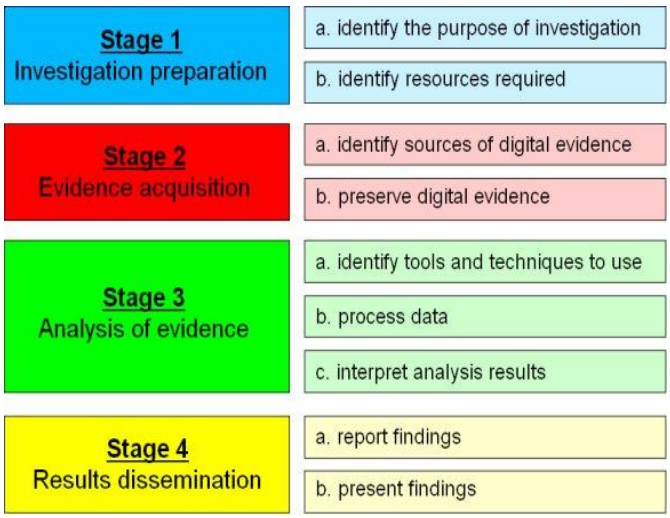
II. NEED FOR DIGITAL FORENSIC INVESTIGATION MODELS

It is important to understand the need of the "Digital Forensic Investigation Model" which is currently an active area of research in the academic world, which aims to ameliorate procedures followed in this field. The way Digital Forensic Science is implemented has a direct impact on the prevention of further malicious events occurring against the intended "target".

The successful tracing back of the events that occurred which led to the crime, and determining the guilty parties involved. Bringing the perpetrators of the crime to justice. The improvement of current prevention mechanisms in place to prevent such an event from occurring again.

III. PHASES OF DIGITAL FORENSIC INVESTIGATION MODEL

Drawing from the previous forensic protocols, there exist common steps that can be abstractly defined to produce a model that is not dependent on a particular technology or electronic crime. The basis of this model is to determine the key aspects of the for mentioned protocols as well as ideas from traditional forensics, in particular the protocol for an FBI physical crime scene search This proposed model can be thought of as an enhancement of the DFRW model since it is inspired from it. The key components of this model include the following:



Identification – recognizing an incident from indicators and determining its type. This is not explicitly within the field of forensics, but significant because it impacts other steps.
Preparation – preparing tools, techniques, search warrants, and monitoring authorizations and management support.
Approach strategy – dynamically formulating an approach based on potential impact on bystanders and the specific technology in question. The goal of the strategy should be to maximize the collection of untainted evidence while minimizing impact to the victim.

Preservation – isolate, secure and preserve the state of physical and digital evidence. This includes preventing people from using the digital device or allowing other electromagnetic devices to be used within an affected radius.

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

Examination – in-depth systematic search of evidence relating to the suspected crime. This focuses on identifying and locating potential evidence, possibly within unconventional locations. Construct detailed documentation for analysis.

Analysis – determine significance, reconstruct fragments of data and draw conclusions based on evidence found. It may take several iterations of examination and analysis to support a crime theory. The distinction of analysis is that it may not require high technical skills to perform and thus more people can work on this case.

Presentation – summarize and provide explanation of conclusions. This should be written in a layperson's terms using abstracted terminology. All abstracted terminology should reference the specific details.

Returning evidence – ensuring physical and digital property is returned to proper owner as well as determining how and what criminal evidence must be removed. Again not an explicit forensics step, however any model that seizes evidence rarely addresses this aspect.

Advantages

• Create consistent and standardized framework for digital forensic development.

• Mechanism for applying the same framework to future digital technologies.

• Generalized methodology that judicial members can use to relate technology to non-technical observers.

• Identifies the need for specific technology-dependent tools while providing insight from previously defined tools of the same category.

• Potential for incorporating non-digital, electronic technologies within the abstraction

Disadvantages

• Categories may be defined as too general for practical use.

• No easy or obvious method for testing the model

• Each sub-category added to the model will make it more cumbersome to use.

IV. CONCLUSION

Each year, there is an increase in the number of digital crimes worldwide. As technology evolves, software changes, and users become digitally savvy, the crimes they commit are becoming more sophisticated. Law enforcement is in a perpetual race with these criminals to ensure that the playing field remains level. Part of this race includes developing tools that have the ability to systematically search digital devices for pertinent evidence. As more devices become digitalized, the tool development should also progress to include these as well. Another part of this race, and perhaps more crucial, is the development of a methodology in digital forensics that encompasses the forensic analysis of all genres of digital crime scene investigations. This methodology must be applicable to all current digital crimes, as well as any unrealized crimes of the future. Many current methods are simply too technology specific. The proposed model attempts to improve upon existing models through the amalgamation of common techniques while trying to ensure method shortfalls are addressed.

V. REFERENCES

[1] [RCG02] Mark Reith, Clint Carr, and Gregg Gunsch. An Examination of Digital Forensics Models.International Journal of Digital Evidence, Fall 2002.

[2] [Ryn02] Joseph Rynearson. Evidence and Crime Scene Reconstruction. National Crime Investigation and Training, 6 edition, 2002.

[3] [Saf00] Richard Saferstein. Criminalistics: An Introduction to Forensic Science. Pearson, 7 edition, 2000.

[4] [SB03] Fred Smith and Rebecca Bace. A Guide to Forensic Testimony. Addison Wesley, 2003.

[5] [Ste03] Peter Stephenson. Modelling of Post-Incident Root Cause Analysis. International Journal of Digital Evidence, Fall 2003.

[6] [Tec01] Technical Working Group for Electronic Crime Scene Investigation. Electronic Crime Scene Investigation: A Guide for First Responders, July 2001.