Cyber Forensic

Sidhartha Mojumdar
HIT

Abstract- This research paper deals with military requirements and tough challenges that have been faced so far. In the context of military activities, cyber forensics is defined in a good manner. After hearing the term, something comes to mind those cyber forensic deals with the investigation of crimes. But recently, it is being used as a promising tool and process for cyber jobs. It mainly deals with the protection and preservation of data from the past. The main unit abstract with the evolution of IT and the increasing technology growth adopted for the communication and networking facilities. The deeds of criminals can be got against an organization or an individual. Military laws are done by cyber forensic system. It is actually a new way to deal with challenges in investigations, including challenges analyzing specific technologies. In this particular report I will discuss cyber cyber forensics and its impact on society and the field of military.

INTRODUCTION

There are many complex parts in cyber forensics and are managed by typical raw data, which are really too tedious for humans to understand. Information technology has really eased all the cumbersome jobs to an extent and cyber forensics also helps to analyze various typical data. To solve complex problems, some tools are used to transfer the information between different abstraction layers. Some non-file abstraction parts of the studies are also included, like: ASCII, HTML files, Windows Registry, Network Packages and source code. Cyber forensics mainly handles both criminal and normal private investigation, but traditionally it is actually associated with criminal laws. It is widely used in criminal law because a large number of crime reports and data are collected before the courts. As for example, we can say that network intrusion is a very common civil litigation and hack the data that are stored on the server. It is the field which deals with forensic science and applied to the extent of the attack and is managed by some proper process.

The main objective of this research paper is to find its investigation process and tools that are actually needed for the physical seizure and imaging of the suspect storage, which are related to the hardware specifications. Sometimes, automated data recovery is also needed for the analysis tools that are used for crime suspects. Apart from the part of legal forensic analysis, current forensic methods for detecting and identifying cocaine and other drugs that used to abuse a lot and are more destructive in nature.

Everything cannot be re-analyzed and cannot be figured out in the proper way. There are some processes such as Raman spectroscopy that is based on inelastic light that are scattered and rapidly allow the non-destructive analysis that is done in forensic science (Garfinkel, 2016). In the contemporary period, forensic science has been used for investigation purposes to solve different crimes. It is also used for some defensive purposes to stop all crime. In investigation, it is widely used with the help of information technology and communication with the help of forensic science.

It is assumed that cyber forensics is one of the most important parts of security that is now automatically used to protect data. In military words, the main concept of digital forensic analysis has already done in previous intrusion detection works. Protecting military data from all types of fatal intrusion is very much needed for the security of a country. Real-time assessment and analysis of data that are perceived and actual cyber-attacks and without being deactivated the attack to the victim's computer. When we hear about the term forensics, what first comes into our mind is the purpose of investigation of crime. Mainly deals with the protection and the preservation of data that are used in the field of investigation. In this particular report we will have a report that are of divarication of objects. Digital forensics has some impact on society and the future will be on safer way.

Computer forensics tends to focus on specific methods that encompass all types of report that including technologies for the digital world. Some of the digital legal actions cover the aspects that are acquired from digital forensics. So I can conclude that digital forensics have a great impact on society and its structure. As digital forensic science advances, information about methodology should become available in more ways.

BACKGROUND

All the techniques that are used for the purpose of investigation are non-destructive and they can perform rapid analysis for military purposes (Ashcroft, Daniels, & Hart, 2016). So, in the form of enforcement and law forensics are used in terms of activities that have an impact on society and business. In this particular topic, I have focused on the cyber forensic part and some destructive parts that can be fetched out with the help of technology and enhancement. (Dezfoli, Dehghantanha, Mahmoud, Sani, & Daryabar, 2013). So this has wide impact on the society and investigation can be done with proper way with some process that may be defensive or offensive according to the situation (Computer Forensics, 2016)

The main goal of the research is to directly address law enforcement needs in cyber forensics. It is also needed for military personnel to take tough decisions on how to manage all sorts of situations in cyberspace. They may be civilian enemies and can rather than be combat attacks. Commanders must know who the actual attackers are prior to taking any action that would be seen as violation of international protocols.. (James & Williams, 2008)

There are not any actual rules for recovering any digital data and information. But there are many practices in the cyber field for the recovery of data and maintaining its proper security. (Whitcomb, 2002). This competitive nature and varied process with all other techniques maintains the main fundamentals of cyber enforcement. The research we have done on this particular project by studying various journals and papers that are available in universal resource locaters. (Meyers & Rogers, 2004)

Some additional parts have also been added to make the system more specific in cyber forensics are the in the contemporary period, forensic science is used for investigation purposes to solve different crimes (Mitchell, 2016). . It is also used for some defensive purposes to stop all crime. In investigation, it is widely used with the help of information technology and communication with the help of forensic science. Defense is why we protect society from ill systems and crime by the use of such system by investigation and methodologies (Brown, 2015). Some commercial software, like SSPS and SAS, and some of the open source tools, including Rapid Miner and the extension of Weka and Gate in JAVA. Some of the mining multimedia is also observed that can be said as a defensive forensics pattern by some of the heterogeneous sources of information. (Garrie & Morrissy, 2014). Data security is much more important part that to be considered because electronic data are always prone to be tampered (Irons & Lallie, 2014). So in this context I would like to define two main points for security like conditional and unconditional scheme. It actually defines the unconditional scheme that secures the cryptography system and cannot be broken even with infinite computational resources after taking time. Information theory security sometimes shows unconditional security.it is not based on the unproven computational process.

PROPOSED APPROACH

Various types of research work are carried out for the field of forensic science, but some small numbers of vendors have built proprietary forensic tools that actually require the support of some expensive ones. Some ad hoc tools for cyber forensic purposes without good programming techniques sometimes require a standard for data integrity. It is also true that a toolbox cannot be assembled without any help of input from another. Commercial and private tools offering limited to post-attack analysis that as a result, is a law enforcement model of data collection and individuals. The most currently offered tools for analysis or imaging of a single computer and offline from the network environment.

Tools will need to address some of the impact that has been carried out for the purpose of the cyber forensic wing. Also, we have learned about the different types of security policy installed in a military forensic for protecting data and the service provided by the system. Above we have also learned that the security system uses in different sectors.

The above discussion is useful because of the different policies installed in the company. Then we have discussed the IT forensics analysis with respect to the security system in information technology. We discussed and also have gained knowledge about the different forensic analyses of the security system.

Solutions have also been developed after research for military operational capabilities like data protection, when candidate digital data information sources are identified and measuring must be put in some place for the prevention of information being destroyed because of its unavailability. Data Acquisitions is a process of transferring data from a venue out of the physical or administrative control of the investigators into some of the controlled locations. Data extraction is also a very important part that must be discussed in this context of matter for the identification and separating some potential data from some image dataset.

The proposed research agenda of this report is to describe the work that needs to be carried out for the purpose of military work so far. The overall concept is identifying, collecting, protecting and analyzing data from the distributed network system that is used for cyber forensic databases. After that, it was desperately needed to perform work that allows us to detect hidden data with network congestion. The art of hiding data is the process of steganography, which exactly means for cover writing.

Another part of the analysis for the forensic database is able for the reconstruction of past events and trace evidence to indicate them. Distributed systems in forensic analysis would be small and lightweight programs that are launched by the agent control center. The experiment type carried out in the research is in wide spectrum and in possibilities to protect data and information with the help of technology. It is seen in this part of the project that properly timeline events over any distributed network are all properly time synchronized. It is also natural that natural drift errors can sometimes happen in computer clocks, and this clock system can be changed by attackers. So a trusted part should be developed which can maintain the synchronization of clocks for the event occurring.

CONCLUSION

The report here represented for military forensic work and these capabilities will soon have direct applications to all real-time problems faced by federal laws. The system of using computers in their conventional manner are increasing their ability to surrender to hi-tech attackers. So, now government and all other industries are faced with new challenges in matching all capabilities towards all network-based cyber-attacks. Data preservation and recovery are two main facets of any repository system. It is so natural that data can be fetched in some authentic manner and the system has the ability to detect such with proper measurement methods.

The cyber forensic sections can be more enhanced by the initiation and sustainability of community experts in digital forensics. Ongoing research work should have been known to everybody with increased awareness. Every day, new tools are being generated for the protection of network security, such as monitoring and analysis of networks of computer traffic for the purpose of gathering information, evidence etc. Systems used to collect network data for forensic use usually come in two forms:

Catch-it-as-you-can and Stop look and Listen. USB device forensics can be challenging on a number of levels. USB device forensics is best known for its application to enforcement investigations, but it is also useful for addressing security concerns about information technology and also data related security concerns in any information-related organization. Improved industry investments are also required for proper research work in the digital forensics area through some proper guidelines and an agenda for tool development.

REFERENCE

[1] Computer Forensics. (2016). https://www.us-cert.gov/sites/default/files/publications/forensics.pdf.

[2] Ashcroft, J., Daniels, D. J., & Hart, S. V. (2016). Forensic Examination of Digital Evidence: A Guide for Law Enforcement. https://www.ncjrs.gov/pdffiles1/nij/199408.pdf.

[3] Brown, C. S. (2015). Investigating and Prosecuting Cyber Crime:Forensic Dependencies and Barriers to Justice. http://www.cybercrimejournal.com/Brown2015vol9issue1.pdf.

[4] Dezfoli, F. N., Dehghantanha, A., Mahmoud, R., Sani, N. F., & Daryabar, F. (2013). Digital Forensic Trends and future. http://usir.salford.ac.uk/34014/1/digital%20forensics.pdf.

[5] Garfinkel, S. L. (2016). Modern crime often leaves an electronic trail. Finding and preserving

that evidence requires careful methods as well as technical skill.http://www.americanscientist.org/issues/pub/digital-forensics.

[6] Garrie, D. B., & Morrissy, J. D. (2014). Digital Forensic Evidence in the Courtroom: Understanding Content and Quality. http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1218&context=njtip.

[7] Irons, A., & Lallie, H. S. (2014). Digital Forensic to Intelligent Forensics. https://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=0ahUKEwjJg96fzurRAhULLY8KHRN4DMYQFggnMAI&url=http%3A%2F%2Fwww.mdpi.com%2F1999-5903%2F6%2F3%2F584%2Fpdf&usg=AFQjCNH4HLzK3gYPcktMIf2YrGy_rvYL9g&sig2=HhT0Ww1EUKNC9aWL21JNEg&.

[8] James, & Williams, P. (2008). Digital forensics and the legal systems: A dillema of our time. http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1040&context=adf.

[9] Meyers, M., & Rogers, M. (2004). Computer Forensics: The Need for Standardization and certifications.https://utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf.

[10] Mitchell, J. (2016). Computer Forensics (Finding & Preserving the Hidden Evidence). http://lhscontrol.com/Computer%20Forensics%20Article.pdf.

[11] Whitcomb, C. M. (2002). An Historical Perspective of Digital Evidence: A Forensic Scientist's View. https://www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf.