IJournals: International Journal of Software & Hardware Research in Engineering
ISSN-2347-4890
Volume 4 Issue 11 November, 2016

FORENSIC APPLICATIONS AS A TOOL FOR HELPING CYBER CRIME INVESTIGATION

Henry Kristian Siburian

Lecturer, STMIK Budidarma, Jl. Sisingamangaraja XII No.338, Siti Rejo I, Medan Kota, Kota Medan, Sumatera Utara 20216, Indonesia, siburianhk@gmail.com

KEYWORD
Cyber Crime Investigation, Digital Forensic, Forensic Application, Technology Forensic, Victim Scene, Cyber Crime, Evidence

ABSTRACT
Digital Forensics in proving a crime these days is increasingly being used by the police or other authorities in proving the crimes committed, the use of digital forensics is not limited to accessing digital data that is in communication media contained on the perpetrator or of the victims, but also the proceeds of crime were abandoned or other authentic evidence that can be proved with the help of information technology in this case is a forensic applications.

1. INTRODUCTION
As the seriousness and scope of crimes involving computers increases, greater attention is being focused on apprehending and prosecuting offenders. New technologies and legislation are being developed to facilitate the investigation of criminal activities involving computers. More organizations are seekingqualified practitioners to conduct digital investigations. In addition, increased awareness of digital forensics has drawn many people to the field [1].

In this modern age, it is hard to imagine a crime that does not have a digital dimension. Criminals, violent and white collar alike, are using technology to facilitate their offenses and avoid apprehension, creating new challenges for attorneys, judges, law enforcement agents, forensic examiners, and corporate security professionals[1]. As a result of the large amounts of drugs, child pornography, and other illegal materials being trafficked on the Internet, the U.S. Customs Cybersmuggling Center has come to view every computer on the Internet in the United States as a port of entry. Organized criminal groups around the world are using technology to maintain records, communicate, and commit crimes. The largest robberies of our time are now being conducted via computer networks[1].

The main purpose of the use of IT in the field of forensics to determine the extent of proving process of a criminal case can be traced back to be used as one evidence of a crime to arrest suspects [2].
Forensic applications is a tool that can be used to conduct an examination of the evidence that there is good evidence of physical and non-physical, crime certainly can not interact directly with the victim but could also use technologies such as hackers who steal information of victims and use for personal purposes or also spammers who send chain emails that inserted the trojan with the same goal, to identify these crimes need help mengidentidikasi pattern forensic applications for criminal acts committed, so in this research the author tries to give some forensic applications use to assist in the investigation.

2. THEORY
2.1 CYBER CRIME
Computer-related crime or “cybercrime” or “e-crime” or “digital technology crime” is a long-established phenomenon, but the growth of global connectivity is inseparably tied to the development of contemporary cybercrime. Any criminal activity that involves a computer either as an instrument, target or a means for

perpetuating further crimes comes within the ambit of cybercrime. A generalized definition of cybercrime may be "unlawful acts wherein the computer is either a tool or target or both".

The proliferation of digital technology and the convergence of computing and communication devices have transformed the way in which we socialise and do business. While overwhelmingly positive, there has also been a dark side to these developments. Crime follows opportunity; virtually every advance has been accompanied by a corresponding niche to be exploited for criminal purposes. "Cybercrime" has been used to describe a wide range of offences, including offences against computer data and systems (such as "hacking"), computer-related forgery and fraud (such as "phishing"), content offences (such as disseminating child pornography), and copyright offences (such as the dissemination of pirated content)[1][3].

Generally speaking, computers play four roles in crimes: They serve as objects, subjects, tools, and symbols [3]. Computers are the objects of crime when they are sabotaged or stolen. There are numerous cases of computers being shot, blown up, burned, beaten with blunt instruments, kicked, crushed and contaminated (Ibid). The damage may be intentional, as in the case of an irate taxpayer who shot a computer four times through the window of the local tax office; or unintentional, as in the case of a couple who engage in sexual intercourse while sitting on computer sabotage and destroy information, or at least make it unavailable. Computers play the role of subjects when they are the environment in which technologies commit crimes. Computer virus attacks fall into this category. When automated crimes take place, computers will be the subjects of attacks. The third role of computers in crime is as tools, enabling criminals to produce false information or plan and control crimes. Finally, computers are also used as symbols to deceive victims. In a $50 million securities-investment fraud case in Florida, a stock broker deceived his victims by falsely claiming that he possessed a giant computer and secret software to engage in high-profit arbitrage. In reality, the man had only a desktop computer that he used to print false investment statements. He deceived new investors by paying false profits to early investors with money invested by the new ones [3].

2.2 TYPES OF CYBER CRIMINALS

The cyber criminals consist of various groups and category. This division may be justified on the basis of the object that they have in their mind. The category of cyber criminals are shown below in Table 1 [3] [4] Criminal profiling is the art and science of developing a description of a criminal's characteristics (physical, intellectual, and emotional) based on information collected at the scene of the crime. A criminal profile is a psychological assessment made before the fact—that is, without knowing the identity of the criminal [3] [4]. The profile consists of a set of defined characteristics that are likely to be shared by criminals who commit a particular type of crime. It can be used to narrow the field of suspects or evaluate the likelihood that a particular suspect committed the offence [1][3].Though not quite that easy or certain in real life, criminal profiling is a valuable tool that can give investigations many clues about the person who commits a specific crime or series of crimes. Nonetheless, it's important to understand that a profile—even one constructed by the top profilers in the field—will provide only an idea of the general type of person who committed a crime [1] [3] [4] a profile will not point to a specific person as the suspect. Although good profiles can be amazingly accurate as to the offender's occupation, educational background, childhood experiences [3].

Table 1. Classification Cyber Criminals

No	Category	Explanation
1	Children	The simple reason for this type of delinquent behaviour pattern in children is seen mostly due to the inquisitiveness to know and explore the things. Other cognate reason may be to prove themselves to be outstanding amongst other children in their group. Further, the reasons may be psychological even
2	Organized Hackers	These kinds of hackers are mostly organised together to fulfil certain objective. The reason may be to fulfil their political bias, fundamentalism etc.
3	Profesional Hackers	Their work is motivated by the colour of money. These kinds of hackers are mostly employed to hack the site of the rivals and get credible, reliable and valuable information. Further, they are even employed to crack the system of the employer basically as a measure to make it safer by detecting the loopholes
4	Discontented Employees	This group include those people who have been either sacked by their employer or are dissatisfied with their employer. To avenge they normally hack the system of their employee

2.3 FORENSIC APPLICATION

forensic applications are the tools used in the field of forensic science that combines several different disciplines that can be used fatherly help the process of identifying, evaluating cases that required judicial system, There are some abstraction that is used to model forensic applications [5], which are as follows:

- Identification
- Preparation
- Approach strategy
- Preservation
- Collection
- Examination
- Analysis

the use of forensic applications in digital forensics also has advantages and disadvantages, the advantages of the use of digital forensics [6]:

- Comprehension Increase
- Efficiency – Reconstruction technology can improve the speed
- Persuasiveness
- Attention Increase,

The following is a disadvantage of the use of forensic applications [6] :

- Prejudice, visual displays when used can introduce levels of prejudice, if one side has such evidence and the other does not.
- Bias, Graphics based reconstruction technology is potentially prone to allowing bias into the presentation, whether that is conscious bias (a form of evidence tampering) or subconscious bias. In an attempt to reduce this, all computer-generated graphical evidence must be backed up with a comprehensive audit trail, and the expert witness presenting such evidence must be able to substantiate the accuracy of the reconstruction, both in terms of the original data used to reconstruct the incident, and the accuracy of the reconstruction.
- Relaxation of Critical Faculties – this is an issue of the 'persuasiveness' of the technology. It is possible that when a subject is shown a 'realistic' computer-generated reconstruction of an event they may feel mesmerised, or believe that they are seeing the actual event happen.Jurors may hence adopt a 'seeing is believing' attitude, as has beenshown to sometimes be the case

  with television viewing. There is therefore apotential reduction in their level of critical appraisal of the reconstructedevidence.

It does not make sense to use technology just for the sake of using something new[6]. However, as many lawyers and expert witnesses continue to push towards the dynamic presentations of video, text, documents and other forms of evidence, it seems likely that these complex data visualisations and forensic virtual models will become a more pervasive and effective alternative to the sketches, drawings and photographs traditionally used to portray demonstrative evidence in the courtroom [6].

3. DISCUSSION

Forensic applications have many types and functions that can be used to audit evidence of the crime, some of the applications that are used can be found in the form of packages such as Oxygen Forensics, DEFT and also CAINE, there are some special software used for data recovery for restore data criminal acts such as Recover My Files, Easeus Data Wizard and so, in this study attempted outlines forensic applications using Easeus Data Wizard, The following is the interface of the application EASEUS Data wizard

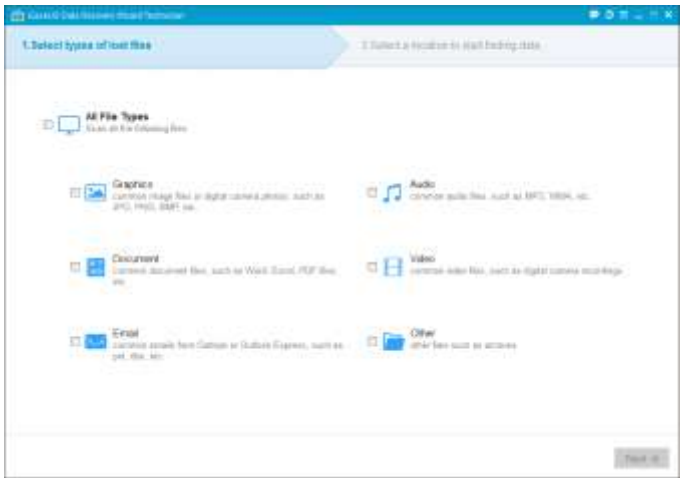

Fig 1. Easeus Data Wizard Interface

for testing of the recovery process is used as a criterion of digital forensic test is done to restore the file documents that have been deleted from the computer, here is the process

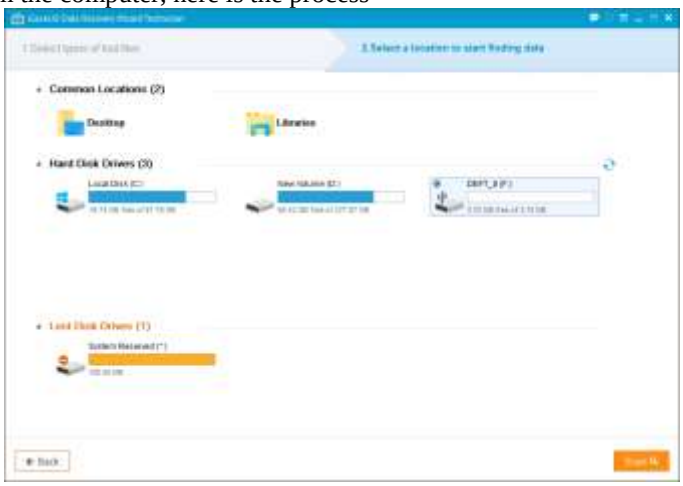

Fig 2. Choose Drive

Fig 2 displays the location of the drive that can be selected to determine which drive will be returned the documents, to the testing carried out select Drive F is a flash disk, after determining the file followed by pressing the Scan button

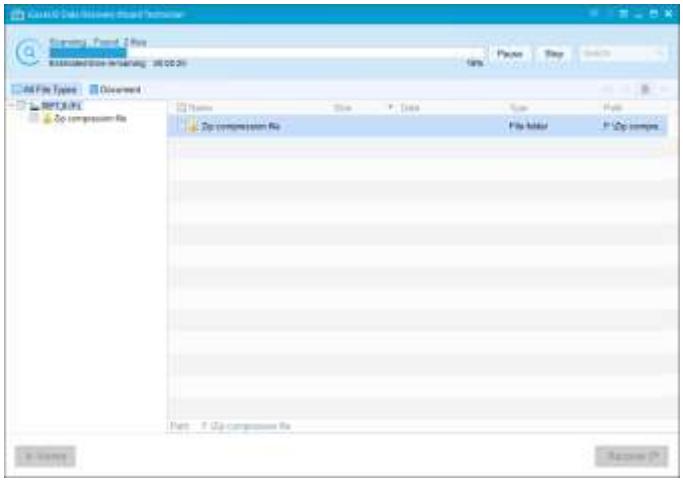

Fig 3. Process Scanning Document

The scanning process will take up all the deleted documents can be read to be returned in the form of a new file, after the process is completed the results are as follows

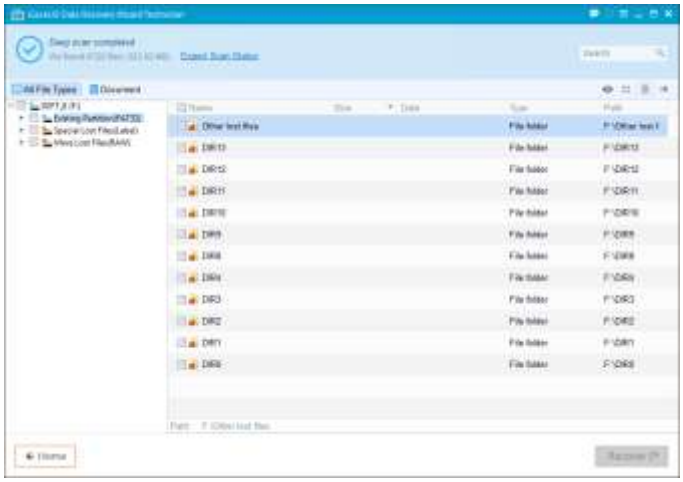

Fig 4. Finish Scanning

for more details, document files are successfully read by the forensic application EASEUS Data wizard can be seen in the picture below

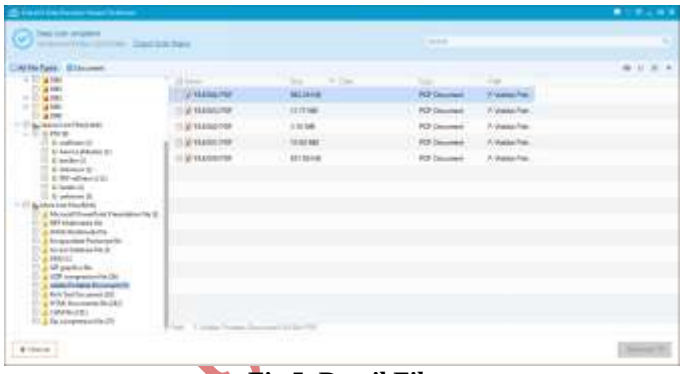

Fig 5. Detail File

to prove the file can be restored, all the files you want restored is given a checklist and then followed by pressing the recover, as follows image below

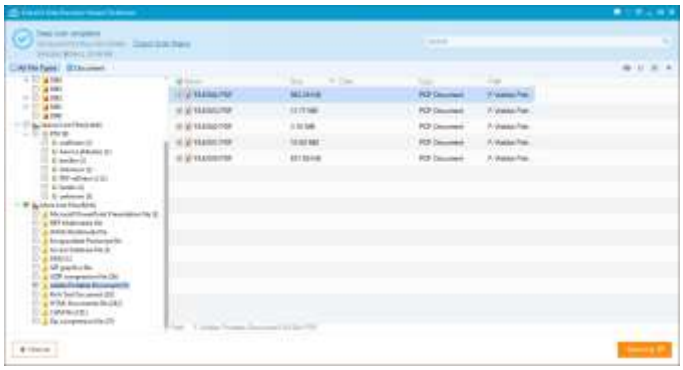

Fig 6. Recover File

after recovery, the results can be seen as follows

Fig 7. Result Recovery

4. CONCLUSION

The use of forensic applications can assist the authorities in restoring, identifying evidence of possible criminal so that the inspection process can be expected to be faster and better with the help of appropriate technology

5. REFERENCES

E. Casey, Digital Evidence and Computer Crime Forensic Science, Computers and the Internet, USA: Elsevier, 2011.

1]

G. S. Kearns, "A Curriculum for Teaching Information Technology Investigative Techniques for Auditors," *Journal of Digital Forensics, Security and Law,* vol. 1, no. 4, pp. 9-28, 2010.

2]

M. Chawki, A. Darwish, M. A. Khan and S. Tyagi, Cybercrime, Digital Forensics and Jurisdiction, Switzerland: Springer, 2015.

3]

J. Sammons, Digital Forensics Threatscape and Best Practices, USA: Elsevier, 2016.

4]

R. Kaur and A. Kaur, "Digital Forensics," *International Journal of Computer Applications* , vol. 50, no. 5, pp. 5-9, 2012.

5]

D. Schofield and K. Fowle, "Technology Corner Visualising Forensic Data : Evidence," *Journal of Digital Forensics, Security and Law,* vol. 8, no. 1, pp. 73-90, 2012.

6]