Abstract

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 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. Originally, much of the analysis software was custom and proprietary and eventually specialized analysis software was made available for both the private and public sectors. The first part of this paper provides a brief overview of digital forensics Process, followed by the models of digital forensics. In the further part of the paper, we consider 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.

References

- Mark Reith, Clint Carr and Gregg Gunsch, (2002) an Examination of Digital Forensic
- National Institute of Justice. (2002). Results from Tools and Technology Working Group, Governors Summit on Cybercrime and Cyberterrorism, Princeton NJ.
- Dr. Yong Guan, Digital Forensics: Research Challenges and Open Problems December 4, 2007

Index Terms

Computer Science Security

Keywords

Digital forensics Investigation model forensics process digital crime digital devices