Volume 2, No. 3, May-June 2011
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

E-mail Forensics For Real Life Application in Evidence Building

Lokendra Kumar Tiwari*
PhD Research Scholar,
Department of Electronics and Communication,
University of Allahabad,
Uttar Pradesh, India.
lokendra.kt@gmail.com

Shefalika Ghosh Samaddar
Assistant Professor
(ISEA) Project, Department of Computer Science and Engineering Motilal Nehru National Institute of Technology,
Allahabad, Uttar Pradesh, India.
shefalika99@yahoo.com

Chandra Kant Dwivedi
Professor,
Department of Electronics and Communication,
University of Allahabad,
Uttar Pradesh, India
ckdwivedi@gmail.com

***Abstract*:** Computer Forensic, the upcoming branch of forensic science where acquiring, preserving, retrieving and presenting content processed electronically and stored digitally, is used for legal evidence in computer related crimes or any other unethical practice involving manipulation of digital content. Such digital content may take many forms which are manifested by different file formats and digital artifacts.
This paper concentrates on evidential usage of recovered deleted e-mail from off-line mail boxes to provide digital evidence in case of non-repudiation either by the sender or by the receiver. This is simply accomplished by using a digital forensic tool Encase 6.0 and applying a capturing mechanism to prove legitimacy of the evidence. The step-by-step procedure is able to increase the practical insight in the capturing of deleted e-mail as digital evidence of non-repudiation and is able to provide an example for preparing evidentiary e-mail for presentation in the Court of Law or for preparation of any legal procedure. Recovery of deleted e-mails in the form of digital evidence requires certain legal bindings which may be provided under this mechanism. This paper contributes to that extent that recovered files are ready digital evidence in the Court of Law.

***Keywords*:** E-mail recovery, E-mail forensic visualization, File recovery, .DBX file recovery, EnCase 6.0, Outlook Express mail recovery, Evidentiary e-mail.

I. INTRODUCTION

Forensics is the process of using deductive scientific knowledge in the collection, analysis, and presentation of legally valid evidence to the court of law. The goal of cyber technology in forensics is to explain the current state of various digital artifacts [1]. Another definition is "computer forensics is considered to be the use of analytical and investigative techniques and tools to identify, collect, examine and preserve evidence/information which is magnetically stored or encoded" [2]. It provides a procedure to systematically identify or capture the digital evidence as a sequence of events responsible for a particular arrangement of bits at a specified time instance [3].

The major steps of computer forensic analysis can be presented through the following block diagram (**figure 1**).

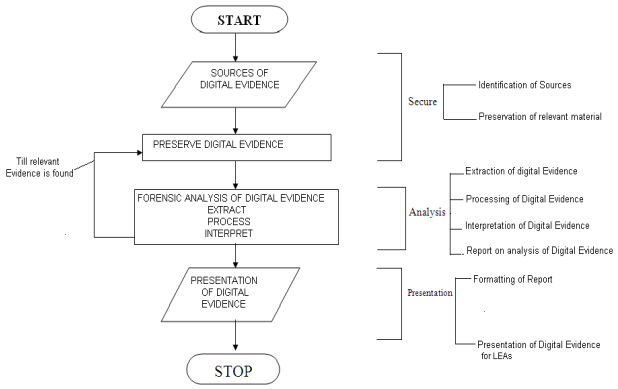

Figure 1 Generic Computer Forensic Methodology (LEA: Legally Enabled Authorities)

Any computer forensic method including evidentiary usages of E-mail Forensic visualization is performed through the stages as given in figure 1.

A. Role of Computer Forensic in Data Recovery

Contents of computer (available in primary or secondary storage) can be considered as a source of evidence. This evidence can be extracted by the forensic investigators with the technical tools available as a proprietary and open source computer forensic mechanism. Computer forensic mechanism makes use of analytical and investigative techniques to identify, collect, examine and

preserve evidence in the form of crime-related content information. A forensic investigation can be initiated as typical criminal investigation or civil litigation using sophisticated digital forensic techniques.

Forensic investigation provides digital evidence when data loss occurs in the following manner:

a. Internet abuse by way of spam, denial of service by an imposter etc.
b. Unauthorized disclosure of corporate information and data to a third party; intentionally or unintentionally; by internally or externally controlled accessibility
c. Damage of the system (intentional or unintentional) resulting in financial loss and loss of goodwill as well.
d. Criminal fraud and deception cases through e-mail exchange
e. Recovery of deleted e-mail to prove the existence of e-mail to legally enabled authorities and visualizing the total process in the Court of Law by recreating the evidentiary environment and data

The last point has been taken care in this paper by suggesting a tool usage so that it can be used as digital evidence in case of intentionally deleted emails.

[a] Genesis of the Problem

The deleted file recovery allows the forensic investigators to collect deleted file from incident node and present the report by following national evidentiary standards. This will provide evidence which could be found directly or indirectly [4] and by presenting them as evidence beyond any doubt.

[b] Encase for E-mail Recovery

There are many tools available for email recovery like Email Detective, Recover My Email etc. but Encase Forensic Suite developed by Guidance Software is having the facility of parsing commercials mails like yahoo and hotmail. These mails are among the most common e-mail usages. Data recovery process of Encase has been verified by NIST (National Institute of Standard and Technology) through its project CFTT (Computer Forensic Tool Testing). **Table no 1** recompiled and reproduced here shows comparison of different email recovery tools and some of their important features.

. **Table 1: Comparison of Email Recovery Tools**

Sr. No	Features	Encase	Email-Detective	Recover my Email
1.	Commercial Tool	Yes	Yes	Yes
2.	*Integrated	Yes	No	No
3.	Recovery From offline mail boxes	Yes	Yes	Yes
4.	Recovery of Commercial Email (yahoo, hotmail, AOL, Netscape etc)	Yes	No	No
5.	Validation by NIST	**Yes(Image Engine)**	No	No
6.	**Multiplatform support	Yes	No	No

[c] Method of operation of Encase Forensic

The first Step in Encase Forensic is to create images of suspect media (hard drives, CDs etc). Images are stored in proprietary formats and contain an MD5 or SHA-1 Hash to validate their authenticity. Encase makes images that are exact copies of the original, byte for byte, in order to be able to fully examine unused parts of the media for deleted files [5]. The method is very much similar to "dd" command [3].

The next step after imaging, EnCase can be used to examine the files stored in the image using common tools such as a document viewer and hex editor. It can also examine parts of the file system not normally exposed to the user, such as deleted file entries, on-disk checksums and log/journaling data. It can also search for and attempt to recover deleted files.

The last step is any relevant files can be saved to the hard disk of the evidence collector along with checksums and other metadata, for use as evidence.

EnCase only uses common tools to perform its analysis. The tools are all tied together and are of supposedly forensic (i.e. verifiable) quality [5].

Data recovered by EnCase has been used successfully in various court systems around the world. For example, the BTK Killer (Dennis Rader) was caught by FBI investigators using this software for evidence creation. Interested reader may have a look at Appendix-1 provided for such purpose.

[d] Contribution of the Paper

Implementation of deleted e-mail recovery as presentation of evidence is achieved by using Encase 6.0. A running example will lead to recovery of evidentiary data which can be accepted in judiciary for any legal proceeding.

II. RELATED WORK

E-mail forensics has its basis in e-mail tracking; especially malicious e-mail tracking. In the initial days of e-mail forensic, a number of malicious e-mails tracking system (MET) was designed. These systems are designed to automatically report statistics on the flow behavior of malicious software delivered via e-mail attachment [6]. The system used to take care of self-replicating virus providing some futuristic insight by detecting suspicious, otherwise new e-mail viruses that may go undetected as these signatures are not available in the antivirus software. However, even detection and tracking of these emails having malicious attachments, are of no help when it come to produce evidence in the Court of Law for the damage caused to the victim. In other words, the systems like MET may be used for evidentiary usage.

There was a paradigm shift in the year 2009 when e-mail forensic analysis was considered from the perspective of visualization. The rich personal information hidden in e-mail was required to be trapped for investigation and evidence collection. The paradigm shift was also evident from the types of the considered e.g. E-mail client data files, databases as well as text files [7]. The sequence of stand-alone methods like parsing the data files, pre-processing the data, keyword searching using KMP algorithm [8] are applied to classify E-mail collection into different category. An association frequency mining technique would be applied to obtain the associative features behind various e-mails account that are

matched with personal information. These efforts in e-mail forensics were more directed towards visualization and illustration for making it more understandable and comprehensive.

There was a probable approach for investigating the e-mail databases of various format including attachments, this is unacceptable in legal procedure where understanding or evidence production will be in purely black and white, suspected e-mail account may be examined to gather evidence to prosecute criminals in the Court of Law. This requirement calls for an efficient automated and techniques to perform multi-staged analysis of e-mail ensembles with a high degree of accuracy. A number of frameworks for preparing such tools have been suggested e.g. Inter-database browser, Statistics Explorer, Data Mining Explorer, Weka Sub module, E-mail Explorer, Details Editor, Map Viewer, Statistics Viewer, Social Network Viewer and Data Mining Viewer [9].

A number of open source tools are also available to recover the deleted emails [10]. Most of the tools are meant for casual users and therefore, cannot be used by authorities for any legal purpose. Such tools are not considered as weapon in the arsenal of Computer Forensic. Computer forensic, by rule, avoids working directly on the supposed-to-be evidentiary material. This stems from the fact that physical evidence to be produced at the Court of Law, should always be held pristine. The need for excellent disk imaging process using relevant tools is paramount. The National Institute of Standards and Technology (NIST) has developed several tools used for disk drive imaging tool evaluation [11]. The Institute's requirements for disk imaging tools should cover a number of essential information, evidential and legal parameters.

The tools should be able to make bit stream duplicate of an image of an original disk or of required partition. The tool should never alter the original disk and require assuring that technically in a full-proof manner. The tool should be able to log I/O errors, in case it is detected.

The tool should provide correct documentation and visualization of forensic processes involved and performed on the evidentiary material [11]. Disk imaging tools, both open-source and commercial types, can be used for evidence-on disk preservation [12]. The "dd" (data dump) command is one of the original UNIX utilities that is used for disk cloning or duplication [13]. But such method of SSH port forwarding fails to provide due visualization due to its operating system based features [3]. All these works place due importance on the deleted file recovery and the collection of information is of paramount importance to an event. However, the legal usage of digital data happens to be a new addition in the jurisprudential technique. The tools are viewed from an angle of legal validity rather than the simple object, proving or disproving some information for public/general consumption.

With the view of a legal evidentiary usage, deleted e-mail recovery technique has been performed using Encase 6.0. EnCase Enterprise closely maps to generally accepted best practices put forth by the National Institute of Standards and Technology and its imaging engine is certified by NIST[14] and has worldwide court acceptance record.

III. Proposed Legally Validated E-mail Recovery Technique using Encase 6.0

Analysis of metadata related to email provides greater insight in formulation and presentation of digital evidence. EnCase 6.0 has a number of powerful features that facilitate efficient examinations and analysis, including recognition of the various files typically associated with email metadata. E-mail metadata collection is a pre-recovery process to get insight into the piece of evidence in the form of e-mail.

A. Preparation of Digital Evidence

"Digital evidence is the information of probative value that is stored or transmitted in a binary form" [15]. This definition covers any piece of digital resources including audio, multimedia, video and hypertext. These digital evidences pertain to digital (e.g. spam, DoS attack, hacking of passwords) and physical crime (spying, planning to hatch conspiracy and implementation of fraudulent). With Cyber terrorism and child pornography facilitated by advance communication technology, digital evidence amount to a major part of evidence in all facets of crime [16]. Digital evidence must support or refute a pre-conceived template of crime framed by the investigators. The Digital evidence should be admissible to the Court of Law and therefore it is necessary that at should be legally acquired [17]. The acquirer of evidence is authorized to acquire evidence in a lawful manner. A data object or any other physical item becomes evidence when it is deemed by a Court of Law or its assignee. The data (digital) object and physical (compact disk, hard disk, pen drive etc.) object becomes inseparable while preserving evidence in the form of object. The physical media may store data objects or information and provide accessibility to the digital items. The physical and digital item together at the time of acquisition or seizure is considered original and an accurate digital reproduction of all data objects contained in the original physical items is called a duplicate or a copy of the original digital evidence.

Digital evidence consists of a set of approving or disapproving statements of a party in a legal dispute. Along with such statements comes the concept of non-repudiation. Non-repudiation is the process or method of ensuring that a party in a dispute cannot refute (or repudiate) the validity of the statement. These statements may be in the form of a legal contract. In that case, non-repudiation ensures the validity of the legal contract. One of the common applications of non-repudiation is the verification and trust of signatures.

Digital evidences considered in the light of non-repudiation mean providing proof of integrity and origin of data and an authentication technique with legal assurance that the evidence (e.g. in the form of a signature, digital signature, authenticated digital document etc) can be asserted to be genuine.

Data integrity is one of the requirements of non repudiation. This is achieved by several hash techniques like MD-51, SHA-256 etc. However data integrity alone is not a full proof security as data may be tampered while being communicated due to man- in- the middle attack [18] or phishing. Verification at the other end of communication is a must as a safeguard.

Assertion of digital origin of data is other requirement. This can be achieved by digital certificates issued by various certification authorities (CAS).

The verification of digital origin allows that the certified /signed data with acceptable certainty can be trusted to be received from somebody having the secret key corresponding to the signing certificate. The secret key is required to be safeguarded by the sign on against all odds.

An e-mail in the form of digital evidence is subjected to all the above applications of digital security.

Preparation of digital evidence consists mainly of the stages related to imaging or getting a copy for working out analysis, analysis of data and metadata for building up evidence and presentation of the recovered e-mail in the Court of Law by enacting the total process involved to create a situation claiming non repudiation.

[a] Email Analysis

EnCase 6.0 has the ability to find, parse, analyze, display documents of various email formats, including Outlook PSTs/OSTs ('97-'03), Outlook® Express DBXs, Lotus Notes NFS, webmail such as Hotmail, Netscape and Yahoo; UNIX mbox files e.g. files used by Mac OS X; Netscape; Firefox; UNIX email applications; and also of the format AOL 6, 7, 8, 9. In most of these file formats, EnCase 6.0 can recover deleted files successfully but the status of the machine can only be obtained in certain cases of selected email format. This is a problem area where case based probe generates viable results through a conversion of format.

[b] Presentation

Email analysis results are presented through in a common EnCase 6.0 format where examiners can navigate through the information, necessary to support the most complex investigations. The steps may be captured in a sequential manner for further analysis and presentation.

B. Real Life Design of a Case: Recovery of Deleted E-mail

Purposeful deletion of email can be recovered using a number of email forensic or forensic tools. Recovery feature of Encase is considered to be very strong. The usages of Encase in email recovery are considered legally acceptable in Court of Law as per standard direction of Department of Defense (DoD) [19]. Table-1 supports to this fact too. The facts are presented through a very common scenario in corporate world. In fact, some of the major implications for organizational security results from unscrupulous employees' online behavior. Inappropriate online behavior calls for a complex set of technical, legal and organizational issues [9]. Employees who may deliberately exploit technical and managerial weaknesses to engage in inappropriate and often illegal online activity are not very difficult to locate but it is difficult to provide legally valid evidence. Let us consider the case of a Telecom company X.

A leading telecom company X (say) was desirous of expanding its business in Middle East countries. The company prepared their bid for purchase of a tender to further its objective. The bid contained the ceiling i.e. maximum and minimum price for the tender along with other required details. The bid was confidential and only the General Manager of the company and his personal assistant were aware of it. The bid details were stored in the personal computer system of the General Manager which was password protected and only his personnel assistant and he himself were aware of the password. The personnel assistant leaked the bid details to other telecom company by way of email from his personal account and thereafter to escape the guilt he deleted the email from the 'sent' folder of the email where the pristine copy of sent mail is automatically stored. Due to leakage of bid details the company fails to secure the tender as the other company quoted a better bid for the same. Such an unscrupulous deal puts the company at a huge financial loss. The copy in the sent folder is able to give the digital evidence of the leakage of information to the other rival company. But as it was deleted and the trash was emptied, therefore the obvious evidence is now difficult to make it available before the authority. The cyber investigator was called to recover evidence in order to prosecute the personnel assistant.

IV. DELETED E-MAIL RECOVERY : A CASE

Let us consider a situation where the Personnel Assistant has sent his mail from his personal account. This may be considered as a running example in order to showcase usage of a forensic tool in context. His activities are traced through the following steps:

Step 1: Assuming that he has sent the mail through his account configured on outlook mail express, he must have allowed himself to generate a window **(Figure 2).**

The screen shows such an email has been sent to the contact in rival company.

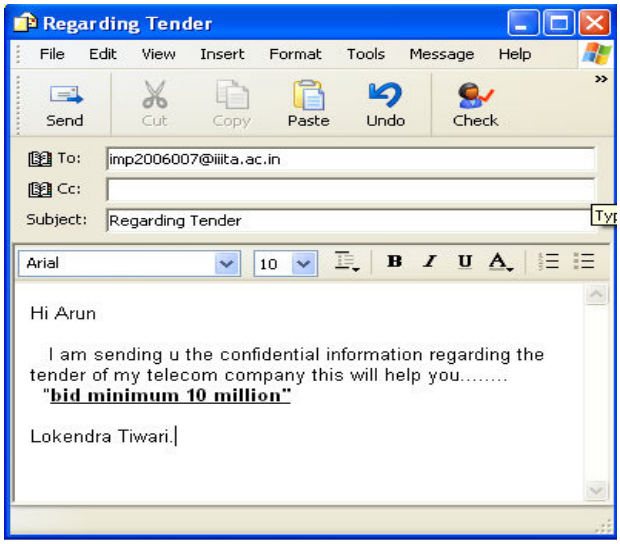

Figure 2 Sending email from personal account

Step 2: The copy of the mail is available in the 'sent item' folder. The sender intentionally wants to delete the mail to remove all the evidences of his fraudulent activity. The file has been deleted as shown in Figure 3. (by emptying the trash bin).

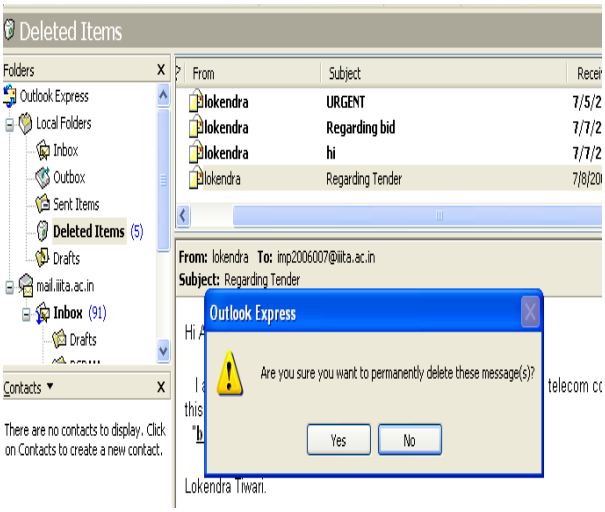

Figure 3 Complete deletion of e-mail

The investigator comes to probe on becoming suspicious as there was no third person who can avail such confidential information. The forensic experts use review tools to make copies and search of e-mails and their attachments looking for incriminating evidence using keyword searches. E-mails may contain *In-Reply-To* headers that allow to be reconstructed by tool application.

Step 3: Outbox.dbx is likely to provide clue on the desired e-mail (if any) as can be visualized in Figure 4.

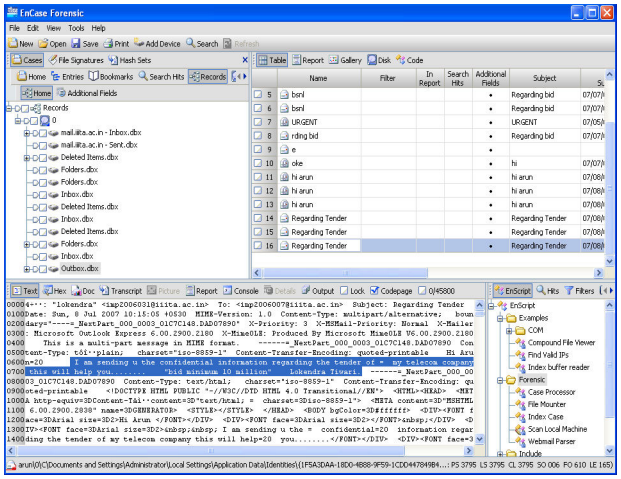

Figure 4 Outbox.dbx

The corresponding code-page in figure 5 delivers the piece of information related to evidentiary material. This can either be recorded as presented here in a sequence by capturing screen shots or should be obtained live after making the account inaccessible to the account holder. Hash matching of the original mail received and recovered mail from sending machine will prove the authenticity of the data recovered.

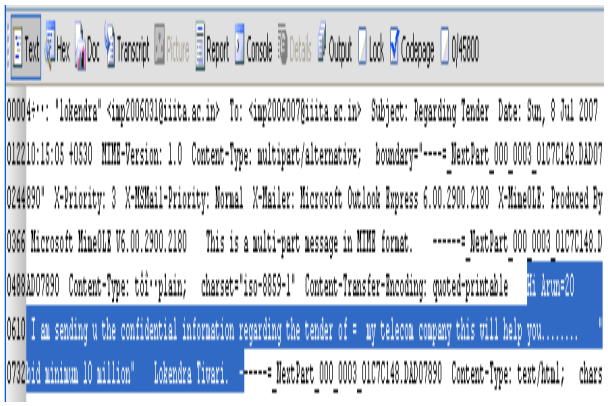

Figure 5 Code page of the recovered email

The evidentiary e-mail and the related information through EnCase 6.0 can be stored with all related metadata information in a suitable storage media for the purpose of re-creation of total non-repudiation method, presentation and visualization for convincing the parties concerned through such evidence. The metadata helps to formulate legally enabled evidence preparation which includes matching of the hash value of recovered e-mail and presented evidentiary e-mail. Another important evidentiary proof is matching of file signature. The date-time stamp recovered is also able to prove the sequence of events leading to the leaking information from the personnel assistant's personal account (Figure 5). The information recovered can be sealed as well till the presentation of the evidentiary material in the court of Law in a full-proof manner.

V. LIMITATIONS

This method may not work in case of counter forensics. For example, let us consider MAFIA (Metaspoilt Anti-Forensic Investigation Arsenal) [20]. Users in the mode of crime take each and every possible precaution. This may be the scripts that run on shutdown to erase evidence of crime, or any other pre-programmed method to cover-up the crime. In the case of MAFIA, users are allowed to alter time-stamps and there are also tools that will leave their imprint only on RAM and will not create a copy by writing anything to disk. In such a case, the cyber investigator may fail to recover the evidence. Recovery of files fails or of no use in case some shredding software shreds the file before deletion. Success of recovery in such cases depends on the understanding of the working of the shredding software.

In case of use of EE, the disk becomes redundant to be used as evidence. This opens up loopholes on evidence of deleted files beyond recovery.

Legally admissible data are required to be authentic. It is really easy to alter real documents just by saving it another time. The computer forensic experts must ensure that no one else can break into their systems and change data that they are working on.

VI. CONCLUSION AND FUTURE DIRECTION OF WORK

This work has been able to prove beyond any doubt that non-repudiation can be enacted in the Court of Law on usages of Encase 6.0 and it is more convincing to visualize the total process rather than just to present documentary evidence. Such visualization technique can further be improved for different file system while taking case of portability and pluggability. A well-defined strategy of suitability of different file formats and forensic software can be obtained as a result. Such formulation will serve the purpose of a guide book for the investigators of e-mail forensic. This ability to provide empirical evidence and identification of original author of e-mail misuse is of prime importance in successful prosecution of an offender.

VII. REFERENCES

[1] Computer Forensics World and Recognizing Potential Evidence, http://www.worldcomputerforensic.com (Accessed on 10.01.2010).

[2] Liu Qian, Fredrik Hoglin, Patricia Alonso Diaz., Computer Forensics; Uppsala University, 2007.

[3] Mishra, Shivani and Ghosh Samaddar, Shefalika. Hard Disk Image Recovery Practices using SSH port forwarding; proceeding of the 12th IEEE International Conference on Information Technology ICIT 2009, Edited by Jargia P. Mohanti, Arindama Singh & Brayendra Panda, Tata McGraw Hill Education Pvt. Ltd. New Delhi ISBN 13978-07-068104-2, IEEE

[4] Computer Society, Bhubaneswar, India, December 21-24, 2009, page 85-89.

[5] Tiwari, Lokendra Kumar, Singh, Arun Kumar and Dwivedi, C.K. An Examination into Computer Forensic Tools: Proceeding of 1st International Conference on Management of Technology and Information Security ICMIS 2010 Edited by Anurika Vaish, Pratika Mishra, Abhishek Vaish, Pallavi Dixit and M.D. Tiwari, Shree Publisher and Distributers, New Delhi ISBN 978-81-8329-375-4, IIIT-Allahabad, India, January 21-24,2010, page 175-183.

[6] Guidance Software Encase "http://www.digitalintelligence.com/software/guidancesoftware/encase/ (Accessed on 15/7/2010).

[7] Mansi Bhattacharayya, Shlomo Hershkop, Eleazar Eskin, and Salvatore J. Stolfo, "MET: An Experimental System for Malicious Email Tracking," Proceedings of the 2002 workshop on New Security paradigms, pp 3-10, September 2002.

[8] Meng, Wu, Yang and Yu, "Research of an E-mail forensic and analysis system based on visualization" Asia-Pacific Conference on Computational intelligence and Industrial Application, 2009, PACIIA 2009

[9] TITAN Jun-feng, HUANG Jian-cai, DU Rui-zhong, ZHAI Jian-qiang (Institute of Computer Networks Technology, Hebei University, Baoding 071002, China)

[10] Rachid Hadjidj, Mourad Debbabi*, Hakim Lounis, Farkhund Iqbal, Adam Szporer, Djamel Benredjem, "Towards an integrated e-mail forensic analysis framework" digital investigation 5 (2009) pages 124 – 137

[11] Write Blocker Review in http:www.forensicfocus.com/write-blocker-review-230709 (Accessed on 11 September 2009).

[12] Open Source Forensic in http://www.opensourceforensics.org/ (Accessed on 11 September 2009).

[13] Linux "dd" command in www.redhat.com, (Accessed on 17 September 2009).

[14] Disk Imaging in http://www.cftt.nist.gov/disk imaging.htm, (Accessed on 23 December 2009).

[15] Encase Computer Forensic tool, http://en.wikipedia.org/wiki/EnCase (Accessed on 23/7/2010).

[16] Scientific Working Group on Digital Evidence (SWGDE), http://www.swgde.org/, (Accessed on May 2010)

[17] Digital evidence and chain-of-custody framework, http://www.scribd.com/doc/37992079/ CECIIS-2010-Digital- evidence-chain-of-custody-framework (Accessed on 10 May, 2010)

[18] File System and Forensic Analysis by Brian carrier ISBN: 0-321-26817-2 Publisher: Addison Wesley March 17, 2005

[19] Nayak, Gopi Nath & Samaddar, Shefalika Ghosh (2010) Different Flavors of Man–In-The-Middle Attack, Consequences and Feasible Solutions, The 3rd IEEE International IEEE China council, Chengdu, China, July 09-11, 2010 (Accepted)

[20] United State Department of Defense www.defence.gov (Accessed on 15/7/2010).

[21] Metasploit penetration testing resources, www.metasploit.com/research/projects/antiforensics (Accessed on 23/7/2010)

APPENDIX 1

Dennis Lynn Rader (born March 9, 1945) is an American serial killer who murdered ten people in Sedgwick County (in and around Wichita, Kansas), between 1974 and 1991.

He was known as the BTK killer (or the BTK strangler), which stands for "bind, torture and kill" and describes his modus operandi. He sent letters describing the details of the killings to police and to local news outlets during the period of time in which the murders took place.

After a long hiatus in the 1990s through early 2000s, Rader resumed sending letters in 2004, leading to his 2005 arrest and subsequent conviction.

By 2004, the investigation of the BTK Killer had gone cold. Then, Rader sent a letter to the police, claiming responsibility for a killing that had previously not been attributed to him. DNA collected from under the fingernails of that victim provided police with previously unknown evidence. They then began DNA testing hundreds of men in an effort to find the serial killer. Altogether, some 1100 DNA samples were taken.

The police corresponded with the BTK Killer (Rader) in an effort to gain his confidence. Then, in one of his communications with police, Rader asked them if it was possible to trace information from floppy disks. The police department replied that there was no way of knowing what computer such a disk had been used on, when in fact such ways existed. Rader then sent his message and floppy to the

police department, which quickly checked the metadata of the Microsoft Word document. In the metadata, they found that the document had been made by a man who called himself Dennis. They also found a link to the Lutheran Church. When the police searched on the Internet for 'Lutheran Church Wichita Dennis', they found his family name, and were able to identify a suspect: Dennis Rader, a Lutheran Deacon. The police also knew BTK owned a black Jeep Cherokee. When investigators drove by Rader's house they noticed a black Jeep Cherokee parked outside.

The police now had strong circumstantial evidence against Rader, but they needed more direct evidence in order to detain him. They obtained a warrant to test the DNA of a Pap smear Rader's daughter had taken at the University of Kansas medical clinic while she was a student there. The DNA of the Pap smear was a near match to the DNA of the sample taken from the victim's fingernails indicating that the killer was closely related to Rader's daughter. This was the evidence the police needed to make an arrest.

On February 25, 2005, Rader was detained near his home in Park City and accused of the BTK killings. At a press conference the next morning, Wichita Police Chief Norman Williams announced, "the bottom line... BTK is arrested." Rader pleaded guilty to the murders on June 27, 2005, giving a graphic account of his crimes in court. On August 18, 2005, he was sentenced to serve 10 consecutive life sentences, one life sentence per murder victim. This included nine life sentences that each had the possibility of parole after 15 years, and one life sentence with the possibility of parole after 40 years. It meant that, in total, Rader would be eligible for parole after 175 years of imprisonment, in 2180.Rader was ineligible for the death penalty, because Kansas did not have a death penalty during the period of time in which he committed his crimes. Kansas reinstated death penalty laws in 1994.

NOTE: [Police found metadata embedded in a deleted Microsoft Word document that was, unbeknownst to Rader, on the disk. The metadata, recovered using the forensic software EnCase, contained "Christ Lutheran Church", and the document was marked as last modified by "Dennis". A search of the church website turned up Dennis Rader as president of the congregation council. Police began surveillance of Rader.]

Source: http://en.wikipedia.org/wiki/Dennis_Rader (Accessed on 23/7/2010)