*International Journal of Computer Trends and Technology- volume3Issue2- 2012*

# Survey on Computer Crime Scene Investigation Forensic Tools

Dr.A.S.N.Chakravarthy [#1]
*Professor*
*Dept. of E C M*
*K.L.University,*
*A.P. India*

T.V.Sarath Kumar[*2]
*Research Scholar*
*Dept. of E C M*
*K.L.University,*
*A.P. India.*

***Abstract*— In the day to day life, the crime is becoming a big issue in the computer field. So to avoid and to protect from crime, Computer Forensics is used. This paper describes different tools that are used in the Computer Forensics. These tools are used to recover the data that is lost (ex., Hard disks).The universal truth says that the coin has two sides where as the technology also has both good and bad. We need to protect the technology by minimizing the impact of threat.**

***Keywords*— Computer Forensics, The Coroners Tool, Win Hex, The free Hex Editor, Mazu Enforcer.**

## I. INTRODUCTION

Now-a-days Forensics plays the main role. The American Heritage Dictionary defined as "Relating to the use of Science or Technology in the investigation and establishment of Facts or Evidence in court of Law" .Here we mainly discuss about computer Forensics which can be used as an evidence in the court for legal cases(1).

Computer Forensics involves the Identification, Documentation and Interpretation of computer media for using them as evidence and to rebuild the crime scenario (2). Computer Forensics includes several areas, Such as: Digital Forensics, System Forensics, Network Forensics, Cyber Forensics, Forensics Analysis, Enterprise Forensics, Proactive Forensics, etc…….

In the year 2008,CSI Computer Crime & Security has done the survey and published a report that the average loss is $500,00 with corporations experiencing Financial fraud and extra average of $350,00 losses at companies experienced by "BOT attacks(3)".

Different types of tools are used for the recovery of Computer Forensics.While Recovering, Each and every data should be maintained perfectly until the investigation completes.The Forensics analysis tools are used for recovering hard disk information.Forensic tool analyses hard-disk/hard-disk images from different operating systems to provide an explorer-style interfaces. When seizing evidence from a computer related crime,the investigator should collect each and every physical evidence.Such as peripherals, documentation, hard-disk generated evidence, etc….

Some of the tools that are used in Computer Forensics are described briefly in this paper.

## II. THE CORONERS TOOL(TCT):

The TCT plays a main role while gathering of evidences.The platform used is UNIX. It is the "collection of programs used for performing post-mortem Forensic analysis of UNIX disks after breaking(4).TCT is composed of four primary tools i.e., Grave-Robber,Unrm,Lazarus&Mac time.The Coroners toolkit is a collection of free tools designed to be used in the forensic analysis of a UNIXmachine. The Coroner's Toolkit is a good second product to back up your primary IT forensic tool. A serious knowledge of UNIX is a prerequisite for success, but if you can manage it, this is an extremely powerful set of tools. We can see the complete slides about TCT from a class taught in the year 1999.There is no support for this product.It is specifically designed for the purpose of investigation in computers break-in. These tools include reconstructing the activities of an intruder. Images are taken in the form of DD, and in UNIX environment.

## III. THE FREE HEXEDITOR

The hex editor tool is one of the tools that are used for recovering the data in the Forensics. Hex editors are the programs which we can view or edit data in its raw form. Rather than accessing data through files, we are able to modify individual bytes. Many hex editors display both binary and ASCII interpretations of the data in addition to the regular hexadecimal, or base. Data stored in the hard drives, thumb drives, memory cards, RAM and other sources can be accessed easily by hex editor tool. Though the file is deleted by the user, the operating system does not remove the original data. The use of a hex editor provides forensics experts with the possibility of recovering deleted information. Free hex editor is supplied on an as-is basis. The author offers no warranty of its fitness for any purpose whatsoever, and accepts no liability whatsoever for any loss or damage incurred by its use. Free hex editor is not a supported product. The author accepts no commitment or liability to address any problems that may be encountered in using it; however, free hex editor is continually being developed and improved, so he is always interested to hear about any bugs or deficiencies.may be freely used for any purpose. You may use it privately or in the course of your work; there is no fee, and no registration is required. You may distribute it to anyone,

and you may place it on any archive or bulletin board system. You may not charge anyone for it other than a reasonable fee to cover your distribution costs. Normally, you should distribute free hex editor in the form as supplied by the author; however, you may repackage it to suit the conventions and needs of an archive or bulletin board system. Free hex editor may be distributed as part of any commercial product without a prior licence agreement, although no extra cost should be charged for inclusion of free hex editor.The below mentioned screen-shots describes the Hex editor tool while installation.

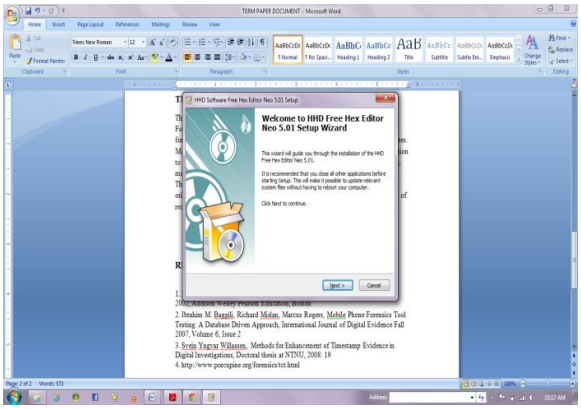


Fig.1 screen shots of free hex editor while installation

Free hex editor was compiled using Microsoft Visual C++ 4.0. Under newer compilers there might be some error messages;these usually mean that somewhere a typecast is needed that wasn't necessary under the old compiler. The release v1.0.156 beta 1 contains a .mak-file that might be helpful in resolving some other problem with linking to the right libraries, for example under 4.0 the comctl32.lib had to be added manually in the linker settings. Free hex editor is distributed under GNU General Public License (GPL), similar to Emacs, Linux etc. So you can modify the source code or incorporate portions of the free hex editor source code in your own programs and distribute the results, provided that they are also then released under GNU GPL.

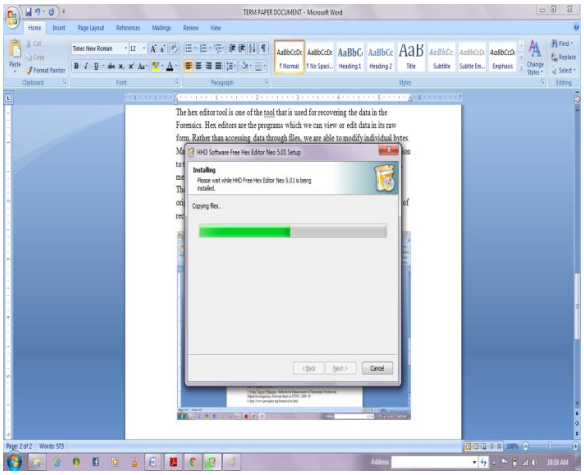

Fig.2 screen shots of free hex editor installation process

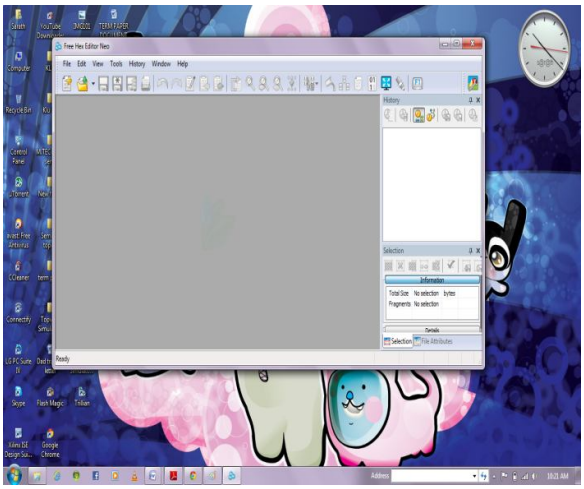

Fig.3 Screen shot of free hex editor after installation

## IV. MAZU ENFORCER

Mazu Enforcer (5) builds a statistical model of Web site traffic when no attack is occurring, says “Carty Castaldi, vice president of engineering at the company”. During a DDOS attack, Enforcer identifies data packets associated with the attack based on their statistical differences from the norm and recommends a filter that typically blocks 80% of the attack packets and about 5% of non-attack packets. Enforcer is one of the tools used in the crime Forensics. Some attackers switch the packet type’s mid-attack, reducing Enforcer's effectiveness until it can re-analyse the situation and recommend a different filter. New York-based MTV Networks is protecting its 15 entertainment Web sites with Enforcer, a defensive tool from Mazu Networks Inc. in Cambridge.

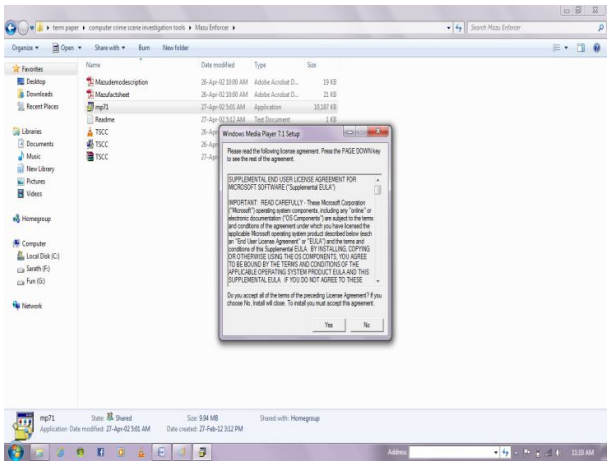

Fig.4 Screen shots of Mazu enforcer

If an attack has just been launched,The Network administrator is immediately alerted of this via the 'attack suspected 'alert that appears in red at the top of the page. The triggers that have been set off appear in red on the left. The graphs also reflect the surge in 'other' traffic type, while the tcp traffic curve remains steady. Within 30 seconds, suspected attack traffic characteristics appear on the lower right cornerof the overview page. The Mazu enforcer computes these characteristics using anomaly based methods, advanced heuristics and in depth packet inspection. The current attack is a randomized UDP flood of about 40,000 pps. Within a minute of attack detection, a Mazu surgical filter recommendation appears as shown by the yellow line above the attack characteristics section.

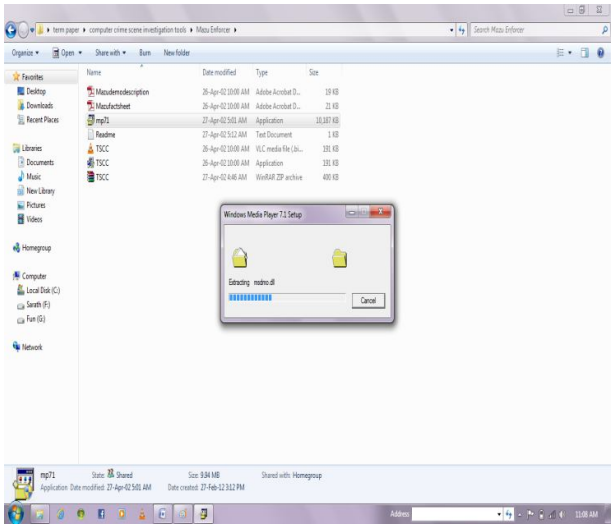

Fig.5 Screen shots of Mazu enforcer while installation

We can use the Traffic Analysis page to further analyse the attack traffic. The Traffic Analysis page provides a flexible and convenient tool for obtaining in depth informationabout current and past traffic. As shown in the graph setting options, it provides graphical views, by various packet parameters, for different traffic types and time periods. By selecting 'packet view', we can see individual packet details.

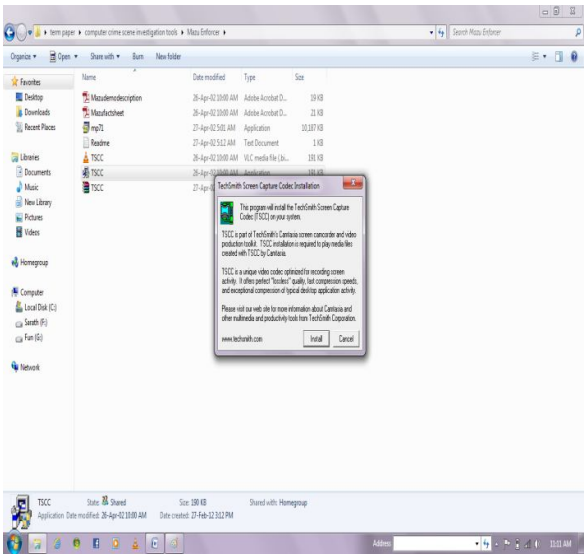

Fig.6 Screen shots of TSSCC

## V. WIN HEX

It is an advanced tool that is used in day to day life and in emergency cases. The main aim of this tool is to repair all kind of filesand to recover the data that is deleted or lost (ex. hard drives, digital cameras).So it can be used in the Forensics for recollection of data i.e., lost or removed. The win hex features include Disk editor for hard disks, floppy disks, CD-ROM & DVD, ZIP, Smart Media, Compact Flash memory cards, and more. FAT12, FAT16, FAT32, NTFS, CDFS RAM editor, providing access to other processes' virtual memory. While installing the Win hex tool, the below shown screen shots are appeared.(6)

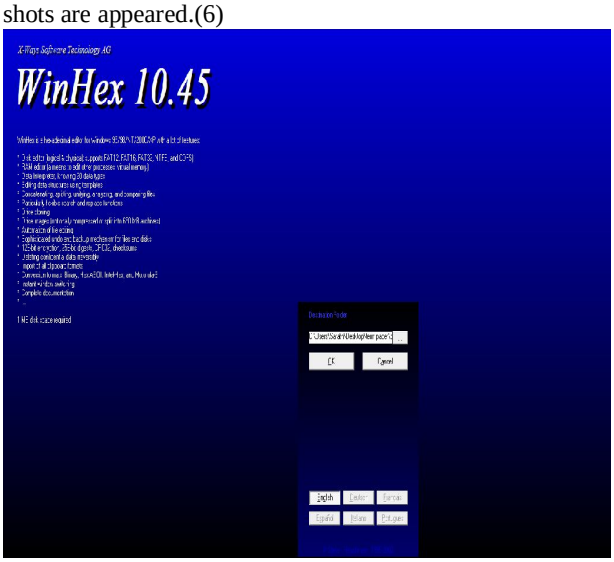


Fig.7 Screen shots of Win hex 10.45

The character Sets of win hex are ANSI ASCII, IBM ASCII, EBCDIC, (Unicode) Instant window switching. Printing. Random-number generator.It supports file greater than 4GB.Very fast and very easy to use. WinHex is a universal hexadecimal editor, and at the same time possibly the most powerful system utility ever.

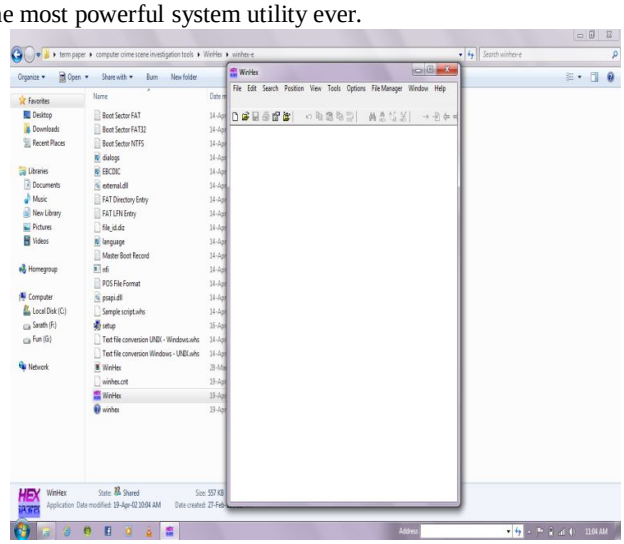

Fig.8 Screen shots of Win Hex after installation

## VI. Conclusion

Now a day's Crime Scene investigation is an integral part of computer forensics and we could give some tools used for it. Many enhancements can be made in the available tools in terms of performance, accuracy and speed. In the future we are trying to implement a new forensics tool which will have all the positives of present tools.

## Acknowledgment

The authors would like to thank everyone, whoever remained a great source of help and inspirations in this humble presentation. The authors would like to thank K.L. University management for providing necessary facilities to carry out this work.

## References

[1] Kruse W.G and Heiser J.G, Computer Forensics Incident Response Essentials, 2002, Addison Wesley Pearson Education, Boston

[2] Ibrahim M. Baggili, Richard Mislan, Marcus Rogers, Mobile Phone Forensics Tool Testing: A Database Driven Approach, International Journal of Digital Evidence Fall 2007, Volume 6, Issue 2

[3] SveinYngvarWillassen, Methods for Enhancement of Timestamp Evidence in Digital Investigations, Doctoral thesis at NTNU, 2008: 19

[4] http://www.porcupine.org/forensics/tct.html

[5] www.mazunetworks.com

[6] http://www.x-ways.com

### *Author Details*

Dr.A. S .N. Chakravarthy,currently works as Professor in Dept. of Electronics and Computer Engineering in K.L. University, Guntur. He has 21 papers published in various International journals and conferences. His research areas includeCryptography, Biometrics, and Digital Forensics. He is Reviewer and Editorial board member for various International Journals.

T.V.Sarath Kumar, currently pursuing M.Tech Degree in the Department of Electronics & Computer Engineering in K.L.University, Guntur.