I.J. Wireless and Microwave Technologies, **2015, 6, 11-18**
Published Online November 2015 in MECS(http://www.mecs-press.net)
DOI: 10.5815/ijwmt.2015.06.02

Available online at http://www.mecs-press.net/ijwmt

Cybercrimes Solutions using Digital Forensic Tools

Dhwaniket Ramesh Kamble[a], Nilakshi Jain [a], Swati Deshpande [a]

[a] *Faculty of Information Technology, Shah and Anchor Kutchhi Engineering College, University of Mumbai, India.*

Abstract

The crimes using computers is growing with rapid speed. As computer crimes have hit up to a high mark, the tools used to fight such crimes is budding faster. In today's world the use of Digital Forensics have also become vital. Digital Forensics is a step-by-step process of scientific methods and techniques to investigate crime obtained from digital evidences. For investigating the digital evidence there are many Digital Forensic tools which are used to investigate digital crimes by identifying the digital evidences. The study results in giving the solutions for Digital Forensic tools for investigators looking to spread out their serviceability in using Digital Forensic tools.

Index Terms: ISafe, Recuva, USBDeview, WinHex.

1. Introduction

Digital Forensics is defined as the use of precisely derived and proven methods toward the conservancy, endorsement, proof of identity, scrutiny, elucidation, documentation and appearance of digital evidence derived from digital sources for the purpose of enabling or broadening the reestablishment of events found to be criminal, or helping to expect unapproved actions shown to be troublesome to prearranged tasks[1].

Today the Internet is an integral part of our life. The internet is fact for virtually unlimited possibility for all of us but despondently also for criminals. Every day they attack our computers steal personnel and confidential information or send false messages from banks. This term is known as Cyber crimes. The Cyber crimes may affect the governments, businesses as well as common people. Cyber crimes are performed by the use of botnets which are network compromised computers that are been affected by computer viruses. To avoid being a victim of Cyber crimes, the use of different Digital Forensic tools should be adapted to minimize system vulnerability. There are many Digital Forensic tools implemented till now. Using Digital Forensic tools makes the investigation process more easier and understandable and it reduces the complexity of investigation that can

* Corresponding author
E-mail address:

occur. It helps in finding out the digital evidences from various digital sources that can play a vital part in committing a computer crime.

2. Brief Study on Digital Forensic Tools

There are four Digital Forensic tools taken into consideration to recognize how these tools works to minimize the Cyber threats. The four Digital Forensic tools are iSafe, USBDeview, Recuva and WinHex.

2.1. ISafe

ISafe is a network and system monitoring digital forensic tool[2] which records keystroke, captures the screenshots of the system, shows which application is running on the system, records mouse click events, analyses the network and gives us the details of the websites visited.

The Advantages of iSafe are as follows:

- ISafe monitors most actions, including websites visited, print jobs, attached drives, microphones and file sharing[3].
- ISafe has tools for blocking activities, and it supplies secure AES 1,024-bit encrypted log files.
- ISafe monitoring software is simple to install and use, even for those with no IT experience.
- It tracks almost all types of activities and provides content-based blocking[3].

The Disadvantages of iSafe are as follows:

- ISafe does not include advanced features that many IT teams desire, such as alerts for excessive bandwidth usage or port monitoring.

2.2. USBDeview

The USBDeview digital forensic tool detects and lists all the USB devices that are connected to the systems and reports are generated on the basis of device type, serial number, date created, last plug/unplug date etc[4]. USBDeview also permits you to uninstall USB devices earlier used, cut off USB devices that are at present connected to our computer, as well as to deactivate and facilitate USB devices. The USBDeview can be used on a remote computer, as long as we login to that computer with admin user.

The Advantages of USBDeview as follows:

- The main advantage of USBDeview is that we can govern tainted USB devices info like USB flash drives so after we know the ruined flash drive info, we can patch-it up by updating process.
- USBDeview is user-friendly and is simple to use.

The Disadvantages of USBDeview as follows:

- USBDeview does not allow to enable or disable USB devices on 32-bit system.
- The 'Created Date' column doesn't show precise principles on Windows 7/8/Vista/2008.
- Some USB devices with bad driver may cause USBDeview to suspend [4].

2.3. Recuva

Recuva is an chief file recovery software used to back up deleted file data material unintentionally done by

the user from their Windows PC, recycle bin or from an MP3 player [5]. It recuperates all our data, files, pictures and media subjects. It supports our PC, and also maintenance extension to memory cards, USB flash drives and iPods.

The Advantages of Recuva are as follows:

- Recuva restores all the important write ups we had written in our word file formerly in last 5 hours of time. The software is tremendously convenient to recuperate word file write ups mainly when it's not being saved.
- The exercise is to a certain extent effortless and somewhat at the requirement of an backup on other devices rather than our own device, we can use it with straightforwardness without setting up on the other device.
- It supplies the info of the electronic mail before we can in point of fact delete it. It is based on that foundation of material which was saved last, to omission of the file, which recuperates our data. When we use Recuva to bring back the electronic mail, it recuperates in form of .ZIP file format.

The Disadvantages of Recuva are as follows:

- Recuva's main disadvantage is that it has no filters.
- Recuva will not recover files deleted with Ccleaner.
- Scans for about 6 hours a 80Gb Partition (C:)[5].
- Recuva doesn't shelter many layouts and can't examine transportable media.
- It does random crashes.
- Recuva doesn't administer to find some of the pictures.

2.4. Winhex

Winhex is a Digital Forensic tool which is a universal hexadecimal editor[6][7]. Winhex lends a hand to the digital forensic features such as recovery of information, processing of information at low-level and provides IT safety measures[6][7]. Winhex scrutinizes and revise all types of files and recuperate deleted files from hard disk with damaged file which is obtained from any digital sources.

The Advantages of Winhex are as follows:

- Quick to create, particularly when obtaining remote hard disks through a slow network connection using F-Response[8].
- Transports/reveals only particularly targeted data, excludes dissimilar data, as may be compulsory by commandment, or the customer.
- Ability to attain all critical file system data.
- Result works accurately like a straight raw image of the disk for all the projected purposes if satisfactorily prepared, with original offsets and comparative distances between data structures preserved.

The Disadvantages of Winhex are as follows:

- Authorization expenditure could have been brought down for individual procedure.
- WinHex does not hold up the possessions of System Console.
- WinHex is not executable on Macintosh and Linux systems.

3. Results and Discussions

Solutions for Digital Forensic tools: ISafe, Recuva, USBDeview and WinHex on the basis of different criminal cases from the attackers point of view, how to identify the theft and how to remove the threat are given and discussed.

3.1. Case 1

Defendant pleads guilty in brokerage case, stealing money [9]

One of three conspirators in a computer-fraud scheme that used Trojans to steal funds from brokerage accounts has pleaded guilty to federal charges in New York [9]. The three men installed key logging Trojans onto victim's computers, according to an outcome, which did not describe how they accomplished this [9]. When victims logged onto their brokerage accounts, their credentials were stolen and used by the defendants to access the accounts. [9]

Tool applied to the case: ISafe.
Steps:

- **From Attackers Point of View**

1. Install ISafe to the victims computer.
2. Click Start to monitor the victims computer
3. After clicking start button restart the computer.
4. The tool will be completely hidden on the victims computer, as to unhide it a shortcut key is to be pressed which is only known to the attacker.
5. The attacker gets each and every information what the victim does through the snapshot he gets to his email.

- **Identification and Removal of Theft**

Neuber's Security Task Manager is a software that gives us background information on current visible and hidden process on our computer. Security Task Manager detects unknown malware and rootkits hidden from our antivirus software.

1. Download and install Security Task Manager software to the victims computer**.**
2. After installation completes, run Security Task Manager on the victims computer.
3. Security Task Manager will scan each and every services and drives on the victims computer including the current and hidden process.
4. After scanning the services and drives it will show the visible as well as hidden process and will state its threat through ratings.
5. Right click on the hidden process, check the file location where the program is installed and delete the program and click remove to end the hidden process.

3.2. Case 2

Cyber Criminals Use USB Sticks to Empty ATMs running on Windows XP robbed with infected USB sticks (most ATMs still run Windows) [10]

The scam to be uncovered saw numerous cash machines belonging to an unnamed European bank targeted during 2013 with the cyber criminals using a humble USB stick to allow them to steal money from the

machines[10]. The gang behind the attacks, which had very intimate knowledge of the technical details of the cash machines, cut holes in the ATMs to allow them to insert a USB stick which was infected with specially written malware. [10]

Tool applied to the case: USBDeview.
Solution:

1. Install and run USBDeview on the system.
2. Analyze the date and time when the incident occurred and check all the USB drives that where connected on that particular date and time through the USBDeview Interface.
3. Check whether the USB drive was previously plugged.
4. Identify the files which were created on the incident date and time in the system in each and every drive.
5. Examine the files if it matches with the incident date and time on the system and delete it because the attacker must have installed the malicious application to attack and steal the money.
6. Investigate the CCTV camera footage on the basis of date and time when the incident occurred.
7. Identify and arrest the suspect through police investigation.

3.3. Case 3

Learning from the natural disaster Hurricane Katrina [11].

Hurricane Katrina created a number of challenges for Gulf Coast businesses, chief among them being data protection [11]. While many companies utilized remote data backup services or had the foresight to ensure that their backups were completely safe - others were left with submerged computers and no backups [11]. Katrina proved that natural disasters have a way of putting our best laid plans to waste, so data recovery was an essential option when all others had been exhausted [11]. Unfortunately, a high level of data protection can be very expensive and therefore out of reach for many small businesses, leaving them in a difficult position [11]. If they didn't have defined backup methods in place, some companies had to face the possibility of losing all of their critical data potentially putting out of business [11].

Tool applied to the case: Recuva.
Solution:

1. Install and run Recuva software tool.
2. Select option you want to recover and click Next.
3. Specify the location from where the files were deleted and click Next.
4. Put a check mark on Enable Deep Scan and click Start.
5. Right click on the file we want to recover and click Recover Highlighted.
6. Select the same drive location from where the file was deleted to recover or else there is a chance of unsuccessful recovery.
7. After successful recovery the task reports are generated and the file gets recovered at the destination drive.

3.4. Case 4

Hackers Target Video Games for Fun, Profit and Better Scores[12].

In the past year alone, Nintendo reported that it had been a victim of an attack in which hackers managed to gain unauthorized access to a Nintendo members reward site 23,000 times, after some 15 million attempts[12].

Japanese game maker Konami said hackers had tried to gain access to its systems some 4 million times and were successful in 35,000 cases[12]. Crytek, the game developer, also reported a breach. Bohemia Interactive, a Czech game developer, confirmed that it too had been hacked after the source code for its DayZ game appeared on a game-hacking forum[12].

Tool applied to the case: WinHex
Solution:

1. Install and run WinHex software tool, and side by side run the game we want to manipulate.
2. Go to the website 'webcheats.com.br' and copy the code to register into WinHex.
3. Click Help option from WinHex and click Register, paste the copied code from the site and click Ok.
4. Click Tools option from the menu of WinHex and then click Open RAM to open processes that are running on the system.
5. Browse the game process that will say Point Blank and select the primary memory and then click Ok.
6. Hex values of the game will then be visible, find the hex value on the website 'webcheats.com.br' that we want to manipulate and then copy the hex value.
7. Click Search button on menu bar of WinHex and then click 'Find Hex Values', paste the copied hex value and then click Ok.
8. Modify the hex value for unlimited ammo in the game.
9. Open the game and select any shooting weapon it will be recognized that while we shoot the ammo remains the same.
10. This way a game is manipulated with Hex values.

To protect our organization's confidential data or our personal privacy, first the data should be strongly backed up and the hard drive cleansing solution should be used. As computer crimes is budding in a hurry, the tools used to fight such crimes is developing and growing faster. The Percentage of Cybercrimes in Top 20 Countries is shown in Figure 1.

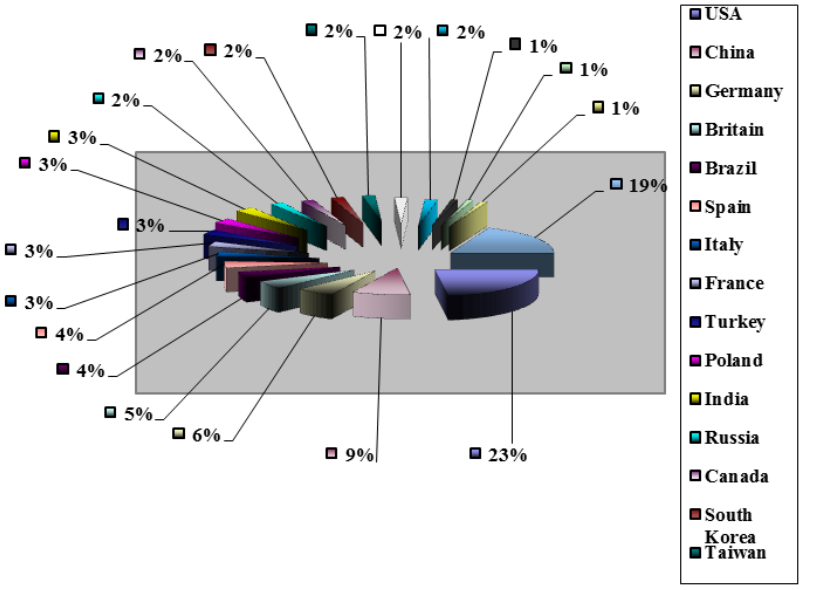

Fig.1. Percentage of Cybercrimes in Top 20 Countries.

4. Conclusion

Taking into consideration the increase in the rate of crimes using computers, we have studied the various Digital Forensic tools which plays an crucial role in finding the digital evidences from digital sources**,** based on different criminal cases **,** we can see that each tool is better to utilize in some or the other area to investigate Cybercrimes. As Cybercrimes is spreading out and speeding up very quickly in various well known countries, the use of Digital Forensic tools should be specially made to minimize this increasing rate of computer crimes. Therefore Digital Forensic tools are needed to prepare solutions for uncovering and thievery deduction purpose. We conclude that the Digital Forensic tools is good to use in Cybercrime investigation process and in future will prove better tools in finding the vital Digital evidence.

References

[1] Ravneet Kaur, Amandeep Kaur, "Digital Forensics". International Journal of Computer Applications, Volume 50 – No.5, India, 2012.
[2] Preeti Tuli, Priyanka Sahu, "System Monitoring and Security Using Keylogger". International Journal of Computer Science and Mobile Computing, Vol. 2, Issue. 3,pp. 106-111, Chhattisgarh, 2013.
[3] ISafe. [Online]. Available: http://employee-monitoring-software-review.toptenreviews.com/ ISafe-review.html. [Accessed: May. 27, 2015].
[4] USBDeview. [Online]. Available: http://www.nirsoft.net/utils/usb_devices_view.html. [Accessed: May. 30, 2015].
[5] Recuva. [Online]. Available: https://www.piriform.com/recuva. [Accessed: May. 23, 2015].
[6] K. K. Sindhu, Dr. B. B. Meshram, " Digital Forensic Investigation Tools and Procedures". International Journal of Computer Network and Information Security,4, 39-48, 2012.
[7] WinHex. [Online]. Available: http://www.WinHex.com. [Accessed: May. 26, 2015].
[8] Tweakers. [Online]. Available: http://tweakers.net/downloads/30694/winhex-171.html. [Accessed: May. 26, 2015].
[9] SC Magazine. [Online]. Available: http://www.scmagazine.com. [Accessed: May. 27, 2015].
[10] IBTimes UK. [Online]. Available: http://www.ibtimes.co.uk. [Accessed: May. 30, 2015].
[11] Kroll Ontrack. [Online]. Available: http://www.krollontrack.com. [Accessed: May. 23, 2015].
[12] Technology-Bits-NYTimes.com. [Online]. Available: http://bits.blogs.nytimes.com. [Accessed: May. 26, 2015].

Author(s) Profiles

Dhwaniket Kamble is currently working as Assistant Professor in Information Technology Department at Shah and Anchor Kutchhi Engineering College, Mumbai. He has done B.E in Information Technology and currently pursuing M.E in Information Technology. His email id is sakec.dhwaniketk@gmail.com.

Nilakshi Jain is currently working as Assistant Professor in Information Technology Department at Shah and Anchor Kutchhi Engineering College, Mumbai. She is having 6 years of teaching experience. She has done M Tech in computer Engineering and currently pursuing Ph.D in Digital forensic field under computer engineering. Her email id is sakec.nilakshij@gmail.com.

Swati Deshpande is currently working as Assistant Professor in Information Technology Department at Shah and Anchor Kutchhi Engineering College, Mumbai. She has completed her M.E. (Electronics).Her teaching experience is almost 17 years. She is also acting as in Charge Head of Department for more than.

How to cite this paper: Dhwaniket Ramesh Kamble, Nilakshi Jain, Swati Deshpande,"Cybercrimes Solutions using Digital Forensic Tools", IJWMT, vol.5, no.6, pp.11-18, 2015.DOI: 10.5815/ijwmt.2015.06.02