INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

A REVIEW ON USB DEVICE FORENSICS

MS. SHRADDHA H. INGLE[1], ARVIND S. KAPSE[2]

1. Student of M. E. CSE, P. R. Patil COE&T, Amravati.
2. Assistant Professor, Department of Computer Science & Engineering, Amravati.

Accepted Date: 15/03/2016; Published Date: 01/05/2016

Abstract*:* Now a days most of data is stored digitally on hard disk, USB drive, compact disk (CD) ,DVD. If small storage device like USB containing important information is lost then lots of problems arises like security of that data. As USB is plug-n-play technology has becomes problamistic. It becomes risky for individuals, businesses, government and institutions with respect to data loss. In this paper we are discussing about with the help of digital forensics it becomes easier to retrieve data by using USB device forensics.

Keywords: Digital Forensics, USB Device Forensics

PAPER-QR CODE

Corresponding Author: MS. SHRADDHA H. INGLE

Access Online On:

www.ijpret.com

How to Cite This Article:

Shraddha H. Ingle, IJPRET, 2016; Volume 4 (9): 1299-1303

INTRODUCTION

As per advancement in technology the use of USB drive also known as flash drive increases to store the data. As USB are easily available, having large storage capacity (10 Mb to 64 Gb), robust and small in size so it becomes easily carried but it can be easily lost or stolen. As information technology reaches to advancement in data storing, sharing. Crimes committed with technology also becomes intensive.

When the crime involves the use of digital devices then the investigation categorized under digital forensics [3]. Digital Forensics is the recovery of data from any type of digital device or media that is retrievable through professional analysis, scientific processes and methodologies that can be validated and potentially utilized in a court of law as evidence [2]. Digital Forensics covers device forensics, database forensics, computer forensics, network forensics. In this paper we study about USB device forensics with the help of Digital Forensics. The purpose of the research is to gain anunderstand how much information that remains on the USB storage devices and to determine the level of damage that could potentially, be caused if that information fell into the wrong hands [7]. USB device may contain personal information of owner like name, address, email ID, password.

So it becomes essential to protect data in USB memory security function. The increase in use of USB security is effective in protecting against leakage of private information, but creates difficulties in obtaining evidence during digital forensic investigations.

1.1 Objective

- To discover the files and recover the data
- To get the data ready for analysis
- To carry out an analysis of the Sensitive data.
- To save the time for the Forensic and analysis of computer sensitive data.

1.2 Scope

Computer forensics*:* Investigation by searching through computer hard drives and other information devices.[4]

1.3 Motivation

Identifying the link between a physical USB device, computer system and associated user account is the primary goal of USB forensic examinations. The recovery of USB link data can take the form of device information such as the USB serial number, past USB connection information left in the Windows Registry of a computer system and file metadata (i.e. information data).

1. LITERATURE REVIEW

1. Jewan Bang, ByeongyeongYoo, Sangjin Lee: Explains how security functions can be bypassed using USB controller commands and presents the design and implementation of a secure USB bypassing tool that bypass the USB security functions.[1]

2. A. Adam and N. L. Clarke: This project investigate whether it is possible to retrieve data from USB storage disks bought second-hand, to try to evaluate the sensitivity of the retrieved data and finally to understand the consequences of a possible disclosure of the restored data.[3]

3. Mark Simms: The problem area is USB memory storage device forensics. The purpose of this research was to provide a formal toolset evaluation of existing USB device analysis tools, and to develop a working prototype tool for use in future digital forensic examinations.[4]

4. Andy Jones, Craig Valli, G Dabibi:

The study examined USB storage devices that had been obtained in the UK to determine whether the way that the disposal of USB storage devices is addressed achieved the desired result, to determine the level of information remaining on the devices and the level of risk that this may create.[8]

2.1 Related work

a. The German security company O&O Software conducted several times a study (Kehrer, 2007) on second-hand hard disk drives leakages. 115 storage media were bought via online auctions coming both from Germany and from the USA. If 32 devices were securely deleted, 72.2% of the other disks presented recoverable data [3].

b. The research undertaken was sponsored by British Telecommunications (BT) which funded the purchase of the USB .To recover the files on the drives bought second-hand, the researchers used the commercial software program “Recover my files”. Results showed that data could be retrieved from 67% of the disks among which 26 disks contained the address of their owner. Concerning their domain of interest, they found out that 18% of the disks contained private information.

c. This study was conducted by academy 10USB devices were purchased from auction website out of 10 USB 2 devices did not present any data other 6 contains personal data and remaining 2 contains music, movie files which is retrieved by forensic software. From the retrieved data previous owner of second hand USB devices could have faced different treats like Identity theft, fraud and hacking attack.

3. TOOLS

1. USBDeview: This tool is used to keep record of all the USB devices that are connected to your computer currently and previously in the form of list. The list contains information such as device name,type,serial no, date/time when connected, product ID. USBDeview is free application for windows OS to show plugged USB devices

2. USBSTOR: It is also called as windows USB Storage parser. It can be run on windows, Linux, Mac OS-X. This tool is useful to view when a USB device was first installed on system and what has been access.

3. Tracking Data Theft via USB Devices with Windows Registry Forensics.

Registry is an important location in Windows system that contains footprints of user activities and other configuration data, which may be valuable for forensic investigators in collecting potential evidences from the system. This role played by Registry in tracking data theft from system to USB external devices.[7]

4. USB SECURITY

A secure USB offers a function that blocks an uncertified user from accessing data on the USB and allows use of the data only from a designated PC. Moreover, a secure USB provides various functions like IP tracking that can check the location information of a secure USB user[1].

5. CONCLUSION

In a recent study of USB flash memory examinations that there are still no frameworks or standardised methodologies for USB examinations compared to other accepted forensic standards. The use and disposal of information stored on USB storage devices will become security problem. A result of above survey says that data on USB storage Devices cannot be deleted effectively. This failure of removal of sensitive data from USB storage device can create the problem of misuse of data if it falls into wrong hand. So it is require to train staff to ensure the use of USB device is properly managed for organizations. For home users it is require to create awareness of potential dangers while storing personal data on USB devices. Recent industry research on USB forensic examinations has partially addressed the lack of development in USB based analysis frameworks.

REFERENCE:

1. Jewan Bang, Byeongyeong Yoo, Sangjin Lee:” Secure USB bypassing tool” Digital Investigation 7 (2010)

2. Veena H Bhat, Member, IAENG, Prasanth G Rao, Abhilash R V, P Deepa Shenoy, Venugopal K R and L M Patnaik :”A Data Mining Approach for Data Generation and Analysis for Digital Forensic Application” IACSIT International Journal of Engineering and Technology, Vol.2, No.3, June 2010

3. A. Adam and N. L. Clarke: “Information Security Leakage: A Forensic Analysis of USB Storage Disks” Section 2 – Information Systems Security & Web Technologies and Security

4. MARK SIMMS: “Portable Storage Forensics: Enhancing the Value of USB Device Analysis and Reporting”.

5. Conan C. Albrecht :”Fraud and Forensic Accounting In a Digital Environment”

6. Prof Sonal Honale , Jayshree Borkar: “Framework for Live Digital Forensics using Data Mining” International Journal of Computer Trends and Technology(IJCTT) – volume 22 Number 3–April 2015

7. Milind G. Meshram, Prof.Deepak Kapgate:” Investigating the Artifacts Using Windows Registry and Log Files” International Journal of Computer Science and Mobile Computing, Vol.4 Issue.6, June- 2015.

8. Andy Jones, Craig Valli, G.Dabibi:“The 2009 Analysis of InformationRemaining on USB Storage Devices Offered for Sale on the Second Hand Market” Dabibi3Proceedings of the 7th Australian Digital Forensics Conference