ISSN:2320-0790

COMPUSOFT
An International Journal of Advanced Computer Technology

Data Wiping and Anti Forensic Techniques

Dr. AJEET SINGH POONIA

Govt. College of Engineering and Technology, Bikaner, India

Abstract: In the era of information technologies every one using the smart phone, laptop, and many other electronic gadgets. These all have high storage capacity, so people use these devices to store photos, videos, music files, contacts details, calendar and even personal information also. People when see the new brands or new technologies in the market they just sell their old phones or electronic gadgets. While selling their gadgets, people behave like smart person and delete all information containing in it and in the memory card, hard disk etc. and they feel secure after deleting or formatting the data contained in that devices. Now as we know that deleting the information which is stored in smart electronic gadgets is not so easy. When we format or delete the information from the media storage it actually deletes the links of data blocks not the actual data residing in it. So it can be easily recovered your data by the help of some data recovery tools. When we sell our electronic gadgets to the shopkeeper, he can recover your personal photos, videos, important information, contact details etc. using the tools available in the market. So beware while selling your smart phone, laptops and other electronic gadgets those have storage capacity as other person can miss use it. In this paper we will cover how to efficiently wipe the memory, so that another person can't recover the required data/information.

Keyword: Data Sanitization Methods; Metadata; Cryptography; Stegnography; Electronic Gadgets:

I. INTRODUCTION

Wiping means erasing the memory content and after overwriting the memory with some character like null character and randomized character. After wiping it become impossible to recover the data existing previously because it deletes the links to memory blocks and also replace the memory content with some new character value. There are various data wiping and anti forensics techniques available in the market by which we can avoid these mishappining. Anti forensics techniques also works in similar way as data wiping does. By mean of anti forensics techniques we use some techniques on the storage devices that data can't recovered. For example meta data can be erased from the media, so it become impossible to read that type of file or we can change first 4 byte of a file that having information about file type after that we can't identify that which type of file is this.[1]

Main difference between anti forensics and data wiping techniques is that in anti forensics technique we don't delete the data from the storage device we change or encrypt the information so that data can't be recovered. In data wiping techniques we overwrite the existing data by some special character like null or any random character so we can't recover that data.

A. *Differences between Data Wiping and Anti Forensics Techniques*

There are major following differences exist between these two –

S.No.	*Data Wiping*	*Anti Forensics*
1.	In these techniques exiting data is overwritten from some special character or randomized character.	The meta data or file structure is changed so user is not able to read the data.
2.	In the data wiping, more than one pass can be used, means	In these techniques data can be encrypted so that

	many times data can be overwritten for the safe deletion.	data can't be recovered without having the encryption key.
3.	It is possible through some tools.	By tools we can perform encryption but we have to manually change the meta data of the storage device.
4.	It is very hard to recover data after wiping.	From some tools we can recover data even after anti forensics.

Table I Differences between Data Wiping and Anti Forensics Techniques

II. ANTI FORENSICS TECHNIQUES

A. ***Cryptography:*** Cryptography is the traditional method of anti forensics. In this method, data is encrypted using some encryption methods using a private key. In future, anyone wants to access the data needs that private key otherwise data is not recovered in human readable format. Now days some tools are available in market by which we can recover encrypted data also like Encase higher versions. [3]

B. ***Stenography:*** Stenography also can be used as anti forensics techniques. In this technique we can hide our sensitive data with the image or video file. Because in the image file some spaces are always available in that space we can put our message. So only the receiver knows about the message. Receiver can easily extract the message attached to the image file. [3]

C. ***Generic Data Hiding:*** In the storage media there may be slack areas that are due to fragmentation of the disk. So we store some data in those slack areas from that area forensics tools can't recover data. In addition to this host protected areas can be use for hide the data. [3]

D. ***Overwriting Metadata:*** Meta data is the most important data about data. It helps lot to read the content of the file. If the Meta data of a file is altered then it becomes hard to read that file. Every file structure initial four bytes uses as the Meta data of a file. If we change or alter this data then we can't read that file. [3]

III. DATA WIPING TECHNIQUES

Also called data clearing, is a software based method of overwriting the data that completely destroys all electronic data residing on the storage device. Data wiping is method of overwriting the existing data by null character or some random character. The following method can be used for data wiping: [2]

A. ***Data Sanitization Method:*** In data sanitization method data on hard drive is overwritten by data destruction program or file shredder program. If the overwriting is done through the software then it comes under the category of data sanitization method.[4]

B. ***File shredder:*** File shredder is a method that deletes the files permanently from hard disk or any storage device. Now it is clear that what is the data wiping and anti forensics techniques so it is better that we should use data wiping techniques for permanently erasing the data. We will discuss some tools that are open source and can be used for data wiping. Our problem is how to wipe the data while selling the mobile phones, computer etc. those having memory them. Here we will discuss both types of methods for non technical person and technical person.

IV. DATA WIPING TOOLS AND TECHNIQUES

A. ***For Non-Technical Person:*** In era of internet every one having smart phone and computer and also switch from one model to another model after selling the old without wiping it. So best way to erase or overwrite your personal information from your mobile phone memory just store another data like you can store a movie or music anything. Now your mobile data or personal information is overwritten and can't be recovered. So this method is useful for every person but not a standard method.

B. ***For Technical Background Person:*** There are various data wiping software is available on the internet. We can use open source software for wiping the storage devices.

1) ***DBAN (Darik's Boot and Nuke) :***It is free data destruction tool. We can create a ISO bootable CD or flash drive as pendrive and then we can boot the computer directly from the these bootable CD or Pendrive. It uses following data sanitization methods DoD 5220.22-M, RCMP TSSIT OPS-II, Gutmann, Random Data, Write Zero. [5]
2) ***CBL Data Shredder:*** It also can be used in two forms we can boot it from the CD or Pendrive for wiping the hard disk or we can run it as a regular program for wiping another storage devices. It uses following data sanitization methods DoD 5220.22-M, Gutmann, RMCP DSX, Schneier, VSITR. We can also select random data or no of passes for data overwriting. [5]
3) ***ErAce:*** ErAce is very easy to use because you simply boot from it and then press one button to wipe all the data from a drive. Data Sanitization Methods: DoD 5220.22-M [4]
4) ***HDShredder:*** HDShredder [5] is a data destruction program that's available in two forms, both of which work with one data wipe method. Data Sanitization Methods: Write Zero
5) ***HDDErase:*** HDDErase [5] is probably the best Secure Erase based data destruction software available.Data Sanitization Methods: Secure Erase

V. CONCLUSION

Data wiping techniques are most useful when we want to permanently erase the data from the storage devices as compared to Anti Forensic Techniques. After erasing permanently we can sell our mobile or computer so that no one can recover our personal information. So this type of cyber crime can be controlled if we are little bit aware about these techniques. Otherwise we have lots of personal information in our mobile phone and computer and we delete the entire information without knowing that it can be recovered from the recovery software.

VI. REFERENCES

[1] Defcon paper “Anti-forensics Techniques and Anti-Anti-Forensics” by Michael Perklin.

[2] “Counter forensics techniques –a brief overview” By Grant Thornton.

[3] Modern Anti-Forensics “A Systems Disruption Approach”.

[4] “Data Sanitization Method A List of Software Based Data Sanitization Methods” By Tim Fisher

[5] Data Destruction Software Programs By Tim Fisher