Digital Forensic Analysis

Habib Zuberi

Title: Digital Forensic analysis

Abstract- Digital Forensics is a branch of Forensic Science which is used in crime investigation. People (or rather the relatives or friends of the criminals/accused persons) destroy the evidence inorder to save the accused person. The destruction/destroying of the forensic evidence from crime scene is called as anti-forensics. The main aim of this project is to create digital crime scenes and carry out forensic and anti-forensic analysis to check the cyber security. This project uses several tools and techniques to carry out the work. The outcome was that yes it is difficult to investigate digital crimes but every criminal drops down some or the other clue and by minute analysis the investigation can be successful.

Introduction

Forensic Science is the presenting the evidence/proof using scientific processes; while Digital forensic is a branch of Forensic Science that deals with careful extraction or mining of digital evidence that is accurate/valid and can be produced in the court. Like for example if there is a murder and if the victim had ordered something online then it will be recorded in the CCTV that this particular delivery person came at this this time and after that the murder happened. Andeven the notice that so and so product is to be delivered at this time (information from the online shopping site) can also be produced. The relatives/friends of the criminals or accused persons try to destroy the evidence / proofs from the crime scenes in order to save that particular person, due to human nature (relative’s or friend’s love for that accused person) and therefore destroy the evidence and as a result it gets difficult to investigate and justice is delayed. The measuresused to destroy the evidence from the crime scenes are called as anti- digital forensics or anti- forensics. Anti-forensics is thwarting/destroying the evidence from the crime scenes thereby making forensic processes difficult , impossible or by delaying it and frustrating the forensic investigators.

DOI: 10.55041/IJSREM15771

1 Related works

A) Enhanced Information through Forensics

We know that there are anti forensic tools that can eliminate attack footprints and make investigation difficult. The researchersChangwei, Anoop and Duminda in their research aimed to use attack graphs in forensic examinations. The methodology they used included anti-forensic capabilities into attack graphs, so that missing evidence can be explained. As a result, they were able to show how attack graphs could be used to help forensic investigators narrow down the attack scenarios, along with evidence left by attackers. Observable limitation of their work from anti forensic technique was that they used TrueCrypt as vulnerability tool, most attackers no longer use TrueCrypt it leavesas systems trace on the boot loader.

Balogun and Shao in their work examined what data encoding add to information security and then spotted out its influences onthe digital forensics of disk drives. The purpose was to converse the obtainable methods and tools to find solutions to the problems imposed by encryption. They used TrueCrypt as a study to illustrate their ideas. They further talked about some features of truecrypt that provides users with plausible deniability and nonrepudiation abilities. This makes digital forensics examinations of encrypted disk drives stiffer and less actualizable. The limitation intheir work is the Truecrypt boot loader traces.

Benjamin researched on “Modeling and refinement of forensicdata acquisition Specifications”, his aim was to define data acquisition tools. The approach which was used was the formal refinement language Event-B (Event B of the data acquisition functionality of digital forensics tools). Event B is an extension of Abrial’s B method Abrial for medeling distributed systems.

B) Enhanced Information Security through Anti-forensics

Researchers: Changwei, Anoop, Duminda

Work: Model using evidence from security events for networkanalysis

Aim: How to use data obtained from security events to constructan attack scenario and build evidence graph

Objective: To achieve the accuracy and completeness of the evidence graph, to correlate evidence by reasoning the casualty,and use an anti-forensic database and corresponding graph to find the missing evidence

Methodology: prolog inductive reasoning, abductive reasoning,global reasoning and mapping evidence to construct evidence graph

2 METHODOLOGY

Introduction

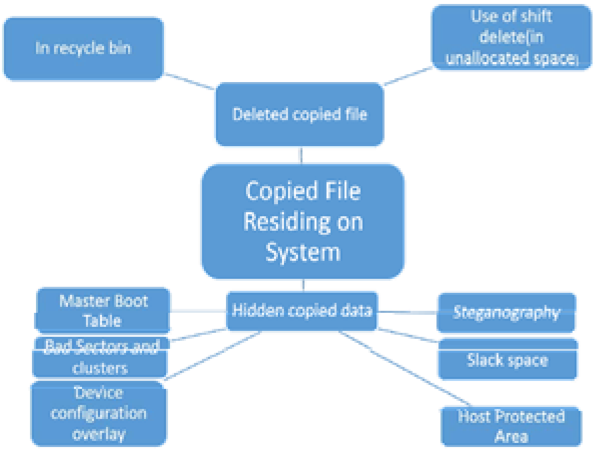
Before any forensic investigation can be carried out, there must have been a case at hand that needs evidence - especially evidence(s) relating to electronic media. Computer forensic examiners or investigators need to beware of possible circumvention techniques that computer criminals employ to defeat digital forensic approach known as Anti-forensic; but the aim of this work is to make the forensic examiner to be pro-active in investigations and to use reliable techniques. It will be un-wrapping some things the investigator has to put under consideration before, during and after forensic examination.

Assumed case

In Federal University of Technology Minna, there was a policy thatnobody should for any reason copy any of the institution's file without authorization, but a disgruntled employee who has being asked to resign was caught copying some relevant files into his personal laptop from one of his colleague's company computer whom he had quarrel with recently. When his colleague caught him, he denied it in the presence of others and when his system was searched by the rest colleagues they found nothing incriminating or any unauthorized file in his possession pertainingto FUT Minna, and now a forensic investigator has being brought to the scene to help out, with the analysis.

Virtual environment would be used to simulate this crime, and thetarget offender's machine would be assumed to be running Window 7, any windows operating system would work.

Methodology used in this work can be broken down into: Volatile data analysis and Non-volatile/persistent data analysis.



Pseudo Code

```
Seized System;

while Copied file resides on system The data is hidden;if data is
hidden
check:

- Master Boot Table,

-         Bad Sectors/clusters,

-         Device Configuration overlay,

-         Steganography,
```

- Slack Space, OR

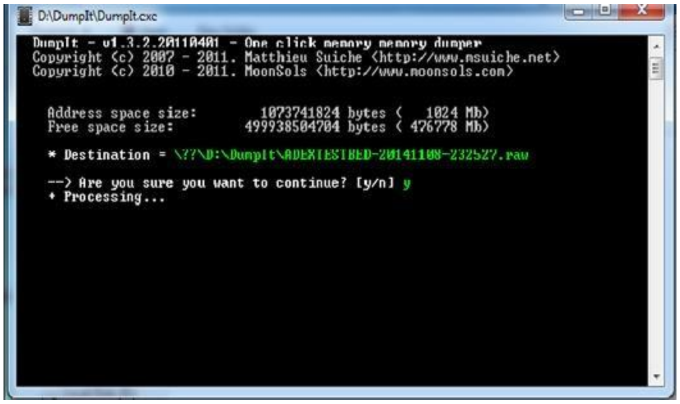
- Host Protected Area;Else

The data has been deleted

If the data has been deleted check recycle bin or unallocated space;

3 Experimental work

The experimental framework consists the use of forensic and anti-forensic tools and techniques to show how the digital forensic investigation works. It involves the installing of the test bed and the setup of test bed. The test bed used in this project is on virtual machine which utilizes the efficiency but yet less expensive forensic operation. VMware workstation 10 was used and window 7 ultimate was installed as guest operating system (OS) on the virtual machine, other forensic tools (FTs) were installed on the host OS while the Anti-Forensic tools (AFT) was ran on the guest OS. The figure below shows the different interface of the experiment



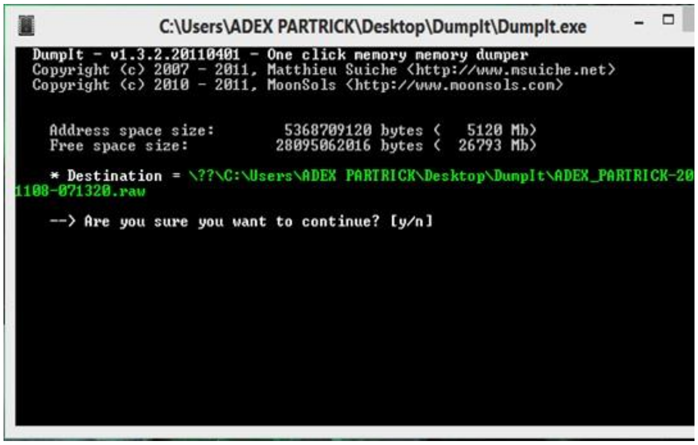
```
DumpIt - v1.3.2.20110401 - One click memory memory dumper
Copyright (c) 2007 - 2011. Matthieu Suiche <http://www.msuiche.net>
Copyright (c) 2010 - 2011. MoonSols <http://www.moonsols.com>


  Address space size:        1073741824 bytes (   1024 Mb)
  Free space size:         499938504704 bytes ( 476778 Mb)

  * Destination = \??\D:\DumpIt\ADEXTESTBED-20141108-232527.raw

  --> Are you sure you want to continue? [y/n] y
  + Processing...
```

DumpIt capturing RAM image



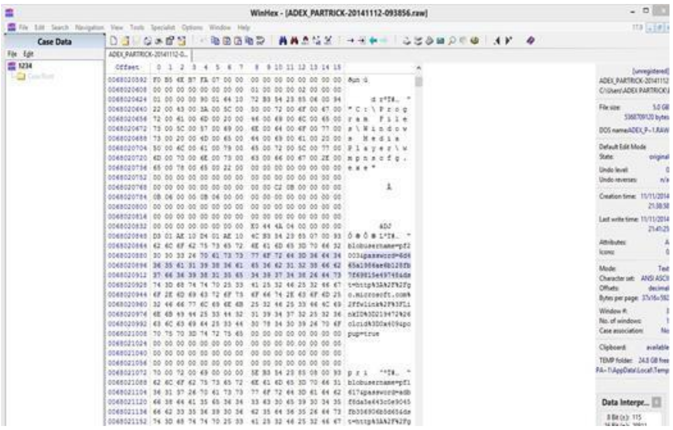
```
  DumpIt - v1.3.2.20110401 - One click memory memory dumper
  Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
  Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>


    Address space size:        5368709120 bytes (   5120 Mb)
    Free space size:          28095062016 bytes (  26793 Mb)

    * Destination = \??\C:\Users\ADEX PARTRICK\Desktop\DumpIt\ADEX_PARTRICK-20
1108-071320.raw

    --> Are you sure you want to continue? [y/n]
```

DumpIt asking to proceed for RAM image processing



```
Offset       0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15
0068020592  F0 B5 4E B7 FA 07 00 00  00 00 00 00 00 00 00 00  ðµN·ú
0068020608  00 00 00 00 00 00 00 00  01 00 00 00 02 00 00 00
0068020624  01 00 00 00 90 01 64 10  72 B3 54 23 85 06 00 94      d r³T#… ”
0068020640  22 00 43 00 3A 00 5C 00  50 00 72 00 6F 00 67 00  " C : \ P r o g
0068020656  72 00 61 00 6D 00 20 00  46 00 69 00 6C 00 65 00  r a m   F i l e
0068020672  73 00 5C 00 57 00 69 00  6E 00 64 00 6F 00 77 00  s \ W i n d o w
0068020688  73 00 20 00 4D 00 65 00  64 00 69 00 61 00 20 00  s   M e d i a
0068020704  50 00 6C 00 61 00 79 00  65 00 72 00 5C 00 77 00  P l a y e r \ w
0068020720  6D 00 70 00 6E 00 73 00  63 00 66 00 67 00 2E 00  m p n s c f g .
0068020736  65 00 78 00 65 00 22 00  00 00 00 00 00 00 00 00  e x e "
0068020752  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0068020768  00 00 00 00 00 00 00 00  00 00 C2 0B 00 00 00 00            Â
0068020784  0B 06 00 00 0B 06 00 00  00 00 00 00 00 00 00 00
0068020800  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0068020816  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0068020832  00 00 00 00 00 00 00 00  E0 44 4A 04 00 00 00 00          àDJ
0068020848  D3 01 AE 10 D4 01 AE 10  4C B3 54 23 85 07 00 93  Ó ® Ô ® L³T#… ”
0068020864  62 6C 6F 62 75 73 65 72  6E 61 6D 65 3D 70 66 32  blobusername=pf2
0068020880  30 30 33 26 70 61 73 73  77 6F 72 64 3D 36 64 34  003&password=6d4
0068020896  36 35 61 31 39 38 36 61  65 36 62 31 32 38 66 62  65a1986ae6b128fb
0068020912  37 66 36 39 38 31 35 65  34 39 37 34 38 26 64 73  7f69815e49748&ds
0068020928  74 3D 68 74 74 70 25 33  41 25 32 46 25 32 46 67  t=http%3A%2F%2Fg
0068020944  6F 2E 6D 69 63 72 6F 73  6F 66 74 2E 63 6F 6D 25  o.microsoft.com%
0068020960  32 46 66 77 6C 69 6E 6B  25 32 46 25 33 46 4C 69  2Ffwlink%2F%3FLi
0068020976  6E 6B 49 44 25 33 44 32  31 39 34 37 32 25 32 36  nkID%3D219472%26
0068020992  63 6C 63 69 64 25 33 44  30 78 34 30 39 26 70 6F  clcid%3D0x409&po
0068021008  70 75 70 3D 74 72 75 65  00 00 00 00 00 00 00 00  pup=true
0068021024  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0068021040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0068021056  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0068021072  70 00 72 00 69 00 00 00  5E B3 54 23 85 08 00 93  p r i   ^³T#… ”
0068021088  62 6C 6F 62 75 73 65 72  6E 61 6D 65 3D 70 66 31  blobusername=pf1
0068021104  36 31 37 26 70 61 73 73  77 6F 72 64 3D 61 64 62  617&password=adb
0068021120  66 38 64 61 35 65 34 34  33 63 30 65 39 30 34 35  f8da5e443c0e9045
0068021136  66 62 33 35 36 39 30 36  62 35 64 36 35 26 64 73  fb356906b5d65&ds
0068021152  74 3D 68 74 74 70 25 33  41 25 32 46 25 32 46 67  t=http%3A%2F%2Fg
```

[unregistered]
ADEX_PARTRICK-20141112
C:\Users\ADEX PARTRICK\

File size: 5.0 GB
5368709120 bytes

DOS name: ADEX_P~1.RAW

Default Edit Mode
State: original
Undo level: 0
Undo reverses: n/a

Creation time: 11/11/2014
21:38:58

Last write time: 11/11/2014
21:41:25

Attributes: A
Icons: 0

Mode: Text
Character set: ANSI ASCII
Offsets: decimal
Bytes per page: 37x16=592

Window #: 1
No. of windows: 1
Case association: No

Clipboard: available
TEMP folder: 24.0 GB free
PA~1\AppData\Local\Temp

8 Bit (±): 115

WinHex returning various password hashes

4 CONCLUSION AND RECOMMENDATIONS

In this paper, widely acceptable forensic methodology such as identifying, collecting, analyzing and reporting have been investigated.Hidden places on the logical and physical structure of the computer where evidence may reside were described and some forensic tools and their application to real life situation presented. Due to human inherent element such as being bias as a result of sentiment case measure should be put in place to avoid investigators handling casesthat he may pick interest in or that has to do with people that know him directly or indirectly, if such issue arises where investigator has interest in the case, it should be awarded to external professional examiner.

Reference

[1] L.Changwei, S. Anoop, & W. Duminda, (2014). A Model Towards Using Evidence From Security Events. A Model Towards Using EvidenceFrom Security Events, vol. 10, 103- 122

[2] M. Balogun & Y. Z. Shao, "Privacy Impacts of Data Encryption onthe Efficiency". International Journal of Advanced Computer Science and Applications, vol. 4, no. 5, 2013, pp. 36-40

[3] A. Benjamin, "Modelling and refinement of forensic data acquisition", Digital Investigation, vol. 11, no. 2, 2014, pp. 90- 101