International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-3S, February 2019

An Automated Evaluation of Live Forensic Approach

Swarna Poojithakolli, K.V.D.Kiran

Abstract: ***Live forensics is an enlarging branch of digital forensics that carryout the analysis on live system. The enlightened attack on computer that needs the support of live forensics to discover the evidence because traditional forensics will not gather volatile data. To collect the volatile data we are performing Memory dump, to analyze that it has different plugins and tools. In this part of research we will generate an automation tool which saves the output data in particular file. This paper presents a design to resolve the difficulty by automating the process of acquisition and analyzing the data.***

Keywords: Live Forensics, memory dump, live acquisition, live analysis, forensics evidence

I. INTRODUCTION

Live Forensics observes the collection of live evidence at the time of a current attack with a limited live investigation. The first point in evidence gathering is the selection of procedure to procure live evidence from a distrust computer. All of the data can help the investigator in finding forensics evidence. The live forensics is the only way to acquire the data but that need to be considered during acquisition is very large and spread over the various locations on a computer. It usually become invariable and time consuming for an investigator to gather the data directly since investigator has informed of multiple tools with their availability and capability to perform a successful live forensics. To acquire volatile data the computer system must be powered on. Volatile data is stored in digital format that has the contents of getting deleted, overwritten or altered[1]. After considering the time complexity and enormous data involved in live forensics the only solution to the problem is to provide a tool that can automate the process of acquiring and analyzing evidence data. This tool can be easily deploy the memory dump and it is capable of maintaining integrity and reliability towards evidence data throughout the process.

II. LITERATURE SURVEY

Live forensic methodology allows forensic investigator to run programs on suspect's system to extract RAM dump and unencrypted files. Random Access Memory commonly known as RAM is the main form of computer storage. In today's world it is in the form of integrated circuits which stores data and allows the system to access it in any random manner. By stating random it is meant that any data in RAM can be retrieved in a constant time. The other important property of RAM is it stores the data in it only till a power supply exists. Hence it is also referred to as volatile memory.

Despite the fact that power is evacuated, the information put away on the drive isn't lost in light of the fact that the storage is not unstable unlike volatile memory. Live forensics solves the problems which are able to acquire unencrypted data.

This paper represents a design of infraction that reconstructs by memory correlation analysis, and provides a complete design and implementation of memory forensics. The tentative result shows the elucidation that perform multiple memory images correlation analysis based on the extracted memory information. Based on the results, investigators may determine the case occurrence. The proposed design may contribute to cross-platform the digital forensic research and responsible analysis for evidence information.

Some of the live forensic process are:

- Acquire the evidence without damaging the original
- Authenticate the recovered evidence as it is same as the originally seized data
- Analyse the data without modifying content.

In this research, forensics Investigator performs ram dump analysis using volatility framework. The best way to avoid all these issues is to provide an automation tool that can automate task and provide integrity towards data.

III. LIVE FORENSICS

Live forensics acquires data from running systems and provide the information like running processes, Ram dump and system states which cannot be extracted through static forensics. The information extracted from the evidence will be more and accurate of the system's live condition. Turning off the system may loss the data such as running processes, network connections and mounted file systems. Leaving a running computer may cause evidence to be altered or deleted [3]

The examination of computers to extract evidence within the operating system using sysadmin tools. The investigator deploys the target system and gain access to the user interface and getting the correct responses.

Memory acquisition will enable to clean snapshots of memory in the operating system. The responsibility of an forensic investigator is to acquire the evidence about the attacker's activities when the attack was performed.

Manuscript published on 28 February 2019.
* Correspondence Author (s)
SwarnaPoojithakolli, M.Tech Student, Department of Computer Science and Engineering, Koneru Lakshmaiah Educational Foundation, Vaddeswaram, Guntur, A.P, India. (swarna2015pujitha@gmail.com)
Dr.K.V.D.Kiran, Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Educational Foundation, Vaddeswaram, Guntur A.P, India.(swarna2015pujitha@gmail.com)

The investigator will have a control on the system configuration rather than system environment. The best approach to perform live analysis is to hide the live monitoring processes. [6]

Performing live accretion will collect information about the state of running systems and data about running processes as well the files accessed by them. It also acquires the network information which used for to and fro communication from the system.

In live response, the first thing is to collect is the contents from RAM. According to Locard's Exchange Principle, the contents of RAM first collected so that we can minimize the impact which we have on it. If any other tools run to collect volatile information they are going to be loaded into memory and modify the contents of memory.

3.1 Importance of Live Data Forensics:

RAM contents are fading fastly and investigator cuts the power supply from the system. At that time data will be stored in temporarily in RAM or remotely. All the data is not stored in Hard drive then data will be loss without Live Forensics.[1]

3.2 Live forensics Benefits:

- Investigation processes will be shotrend.
- Cost efficiency
- More evidence collection.
- Proper acquisition and analysis.
- Improved chances for successful lawsuit.

IV. DEAD FORENSICS

Dead Forensics involves the analysis of a suspect system which is shut down condition through the normal administrative procedures. When the system is in dead state it doesn't provide the information of any malicious process running on the system, as the system in shut down condition erases the volatile data. The investigator can access the data resides in the system and can analysis on the data available while the system is in offline condition.

If the computer is in switch on condition, then the system has to be turn off by shut down or by either pulling out the power plug. After system shut down the forensic investigator pulls out the hard drive from the system and attaches it as an external media of an forensic system and start the analysis [2]. The forensic investigator will safeguard the evidence that no data tampering may takes place on the external drive. Before starting the analysis the write blocker is used to avoid any type of data tampering, and allows only read access. [7]

4.1 Positive aspects:

1. Forensics is the ability to retrieve hidden and deleted data.
2. No need of overwriting or modifying the evidentiary data obtained from a forensics acquisition

4.2 Limitations:

1. Many unique practical constraints and legal procedure makes the appliance of digital forensics both interesting and complex.
2. As there is a lack of effectiveness in the present forensic investigative techniques which leads to the uncertainties.
3. Investigators need passwords to access the system.

V. STATIC ANALYSIS

In static analysis the target system was freeze for analysis of an attached storage media to perform forensic imaging or copy of the system data. For forensic investigative analysis, investigators utilize both open source tools and commercial products. Static analysis involves effective data recovery from storage media. It can identify the files which are present in file systems such as deleted files, file using keywords, pattern matches, or modification, access, and creation times [6].

Static analysis commonly presents an investigator with a single snapshot of the storage media. At the time of force shutdown the investigator will not have restraint over the file system and results might be inconsistent.Some file systems need additional efforts from the investigator to rectify.

VI. LIVE FORENSICS ACQUISTION

It considers the retention of volatile data. Investigator will report the chain of custody from the first approaches of computer and determines its power status. To initiate acquisition, the investigator needs to activate the forensics agent and the forensics agent is placed within the kernel space of the computer system giving the forensics investigator administrative rights to the suspect machine.

It was developed in response to the forensic acquisition techniques will retent the volatile data.

To perform the Live Acquisition first disconnect the system from the network to track an active attack, if any damage or loss of valuable information then automatically it will stop [2]. Live forensics will record the time, date, who discovered the problem and how much information was known. Each and every time we must make an note of an situation of what type of actions were taken and what type of results were found. Evidence Forensics will be ready for action to collect information and determine that Action based on the data collected.

Run a network to capture communication flows to and from a compromised system. Tcpdumpraw format will reduce the performance issues. Create a paper copy of data collection and record the results of commands running at the time of data gathering while sending the digital data to a remote host or storing it on external media.

When the computer is powered on, then investigator will collect the data locally, or through the network. The investigator will attach a write blocker system to the suspect machine of a forensic system.

Live forensics may be altered the data and continuously processed. Powering off the system may loss the volatile data like running processes, network connections and file systems.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

6.1 Positive aspects:

1. It allows forensics investigators to recover the volatile information to the suspect's system network settings and shared files and folders.
2. Collects information about the running state of the system.

6.2 Limitations:

1. Data modification during the acquisition process and the dependencies of the forensics acquisition on the suspects system.

6.3 Live forensics process diagram:

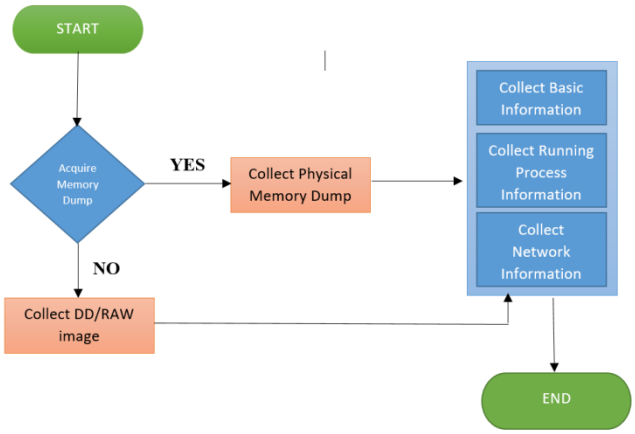

***Figure 1*: live forensics process**

VII. LIVE FORENSICS ANALYSIS& RESULTS

The ability to collect the information from RAM often to be gathered from non-volatile analysis but it may require acquisition training and hardware.

RAM allows analysis to occur the first response of an acquisition and enables RAM to view the data of an static evidence item to which duplicate validation techniques can be applied [3].

The necessity of analysis has been demonstrated by reiterate the weaknesses in forensic computing methodologies, tools and techniques [4].

The acquisition of an physical memory was verified to the various levels by comparing MD5 hashes. The time taken to produce the memory dumps of physical hardware was found to be significantly longer than on simulated hardware.

Uncertainty if the input for imaging is actually the RAM as malware cane be utilised to prevent RAM access or incorrect representation of RAM to prevent detection.

Analysis assumptions on process structure's doubly linked list does not take unlinked ones such as old and hidden processes into account

RAM in certain cases can be present in spite of loss in power supply up to certain periods of time. Hence, its volatility comes into question.

7.1 LIVE FORENSICS ANALYSIS WORKFLOW

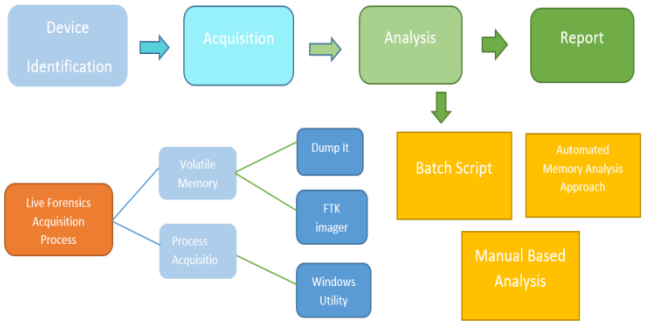

Figure 2: live forensics workflow

VIII. MEMORY FORENSICS

Memory Forensics is a procedure to captures the memory dump, and list the analyses of an information obtained from systems memory. Numerical analysis is used to collect the volatile data of evidence in practical time.

Data captured from memory dump is further analyzed in forensic laboratory. It was stacked into a memory when user types the password, or data is decrypted [9].

Traditional analysis has the inefficiency of the physical disk to reveal information about processes that were running in memory.

The investigator intuition has the utilization was used on the system of attack. It is possible to open the hide data in memory who will negotiate the system to store data on the system's drive.

- Viruses and Worms exist in memory that's why Forensics analysis is hard to perform as the malicious activities couldn't be captured.
- Forensics evidences are extracted from volatile memory which reside in system.
- Examination of activities such as login, internet, usage history uninstalled programs, deleted files can be found in volatile memory.
- Network information of currently logged on user, processes and services can be found in volatile memory.

Carrying out a Memory Forensics investigation will require in-depth knowledge of the most recent trends in the field. Here are the six main stages that an investigation should cover:

- Identifying the rogue processes posing as legitimate processes by heuristic methods
- Detecting anomalies in the treatment of objects being processed (DLLs, Registers, Threads, etc.),
- Examining the network artefacts and the communication ports used by the processes of the system in memory to determine the suspect elements;
- Searching for evidence of code injection and methods of obfuscation
- Searching for signs of the presence of a rootkit by the hooking detection method;
- Making a copy of the process in memory and the drivers of the suspect system

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

IX. ARCHITECTUTRE:

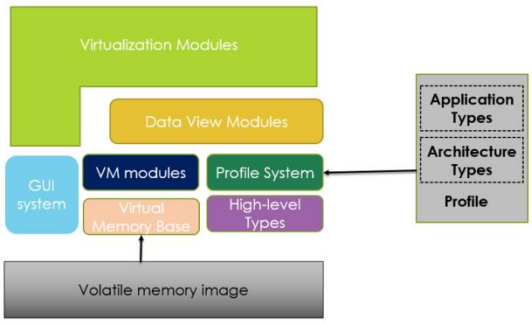

Figure 3: **Live forensics architecture**

- **Visualization Modules** contains two modules: Object Browser and Address Space Viewer.
- **Object Browser** will interpret the memory at abstraction level with the support for applications
- **Address Space** viewer will visualize the data which appears in virtual or physical address space.
- **Virtual Memory Base and Modules** will simulate to the random access of data and support to identify whether given data is accessible in memory.
- **High level types** contains objects which are an abstraction of data that was found in a Virtual Memory. Objects will have a Deep Member Access which provides a mechanism for the investigator to reference data. Allows a digital forensic investigator to perform objects operations in memor.
- **Data View Modules** Views the abstractions on address space and generally use profiles of a specific application that are present in address space.
- **Data Analysis Modules** Provides investigator with the potential to record and automate the tasks in data
- By using **GUI** Investigator will navigate and organize the data that are more likely to have the success at the time of investigation.

X. FORENSIC EVIDENCE COLLECTION

The memory is assigned to the application in the investigation of an extracted image captured. Strings are used to extract the text information from memory dump. Pattern matching is used to identify the precedent of user activity and approach takes the user input and test the image with the extracted memory dump.

The remnant of the user text the extracted information from the memory dump. The user input was stored on the applications of a user input and the data is retrieved from the volatile memory analysis of a Windows computer systems. The probe is focused on the information related to the user that application was recovered when the memory is grab at running application.

XI. TOOL IMPLEMENTATION

The automation tool used for analysis. The following plugin was utilised for obtaining the ***Profile*** which is necessary for executing further plugins:

```
     Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86
                AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                AS Layer2 : FileAddressSpace (C:\Users\Swarna\Desktop\Admin123.raw)
                 PAE type : PAE
                      DTB : 0x185000L
                     KDBG : 0x82962be8L
      Number of Processors : 1
Image Type (Service Pack) : 0
           KPCR for CPU 0 : 0x82963c00L
        KUSER_SHARED_DATA : 0xffdf0000L
      Image date and time : 2018-10-08 09:04:32 UTC+0000
Image local date and time : 2018-10-08 14:34:32 +0530
```

Screenshot 1: **List of profiles in memory dump**

11.1 DLLLIST

To view all the DLL's loaded by a process we use the plugin dlllistto verify if the process is calling its related DLL. It can be executed using the following plugin:

```
svchost.exe pid: 964
Command line: c:\windows\system32\svchost.exe -k dcomlaunch -p -s PlugPlay

Base                Size      Path
0x00000000256a0000  0x10000   c:\windows\system32\svchost.exe
0x00000000b7c0000   0x1e1000  C:\WINDOWS\SYSTEM32\ntdll.dll
0x00000000092e0000  0xb2000   C:\WINDOWS\System32\KERNEL32.DLL
0x00000000080a0000  0x273000  C:\WINDOWS\System32\KERNELBASE.dll
0x0000000008c80000  0x5b000   C:\WINDOWS\System32\sechost.dll
0x000000000ac30000  0x124000  C:\WINDOWS\System32\RPCRT4.dll
0x0000000007b90000  0xfa000   C:\WINDOWS\System32\ucrtbase.dll
0x0000000006b00000  0x22000   c:\windows\system32\umpnpmgr.dll
0x0000000009030000  0x9e000   C:\WINDOWS\System32\msvcrt.dll
0x0000000007540000  0x14000   C:\WINDOWS\SYSTEM32\WLDP.DLL
0x000000000ae10000  0x323000  C:\WINDOWS\System32\combase.dll
0x0000000007c90000  0x7a000   C:\WINDOWS\System32\bcryptPrimitives.dll
0x0000000007d10000  0x1e2000  C:\WINDOWS\System32\CRYPT32.dll
0x0000000007b70000  0x12000   C:\WINDOWS\System32\MSASN1.dll
0x0000000008ae0000  0x57000   C:\WINDOWS\System32\WINTRUST.dll
0x000000000b290000  0xa1000   C:\WINDOWS\System32\advapi32.dll
-------------------------------------------------------------------------------
svchost.exe pid: 984
Command line: C:\WINDOWS\system32\svchost.exe -k DcomLaunch -p

Base                Size      Path
0x00000000256a0000  0x10000   C:\WINDOWS\system32\svchost.exe
0x00000000b7c0000   0x1e1000  C:\WINDOWS\SYSTEM32\ntdll.dll
0x00000000092e0000  0xb2000   C:\WINDOWS\System32\KERNEL32.DLL
0x00000000080a0000  0x273000  C:\WINDOWS\System32\KERNELBASE.dll
0x0000000008c80000  0x5b000   C:\WINDOWS\System32\sechost.dll
Normal text file                                    length : 7,54,272  line
```

Screenshot 2: **DLL's loaded in process**

11.2 HANDLES

Handles are opened in a process and it applies to files, registry keys, and mutexes, named pipes, events.

```
System pid:  4 \<unable to open process>
    4: Process       System(4)
    8: Thread        System(4): 28
    C: Mutant        \KernelObjects\BcdSyncMutant
   10: Directory
   14: Directory     \GLOBAL??
   18: Partition     \KernelObjects\MemoryPartition0
   1C: Directory     \KernelObjects
   20: Event         \KernelObjects\LowPagedPoolCondition
   24: Event         \KernelObjects\HighPagedPoolCondition
   28: Event         \KernelObjects\LowNonPagedPoolCondition
   2C: Event         \KernelObjects\HighNonPagedPoolCondition
   30: Event         \KernelObjects\LowMemoryCondition
   34: Event         \KernelObjects\HighMemoryCondition
   38: Event         \KernelObjects\LowCommitCondition
   3C: Event         \KernelObjects\HighCommitCondition
   40: Event         \KernelObjects\MaximumCommitCondition
   44: Event         \KernelObjects\MemoryErrors
   48: Event         \KernelObjects\PhysicalMemoryChange
   4C: SymbolicLink  \GLOBAL??\ROOT#SYSTEM#0000#{53172480-4791-11d0-a5d6-28db04c10000}
   50: Thread        System(4): 80
   54: Process       Registry(96)
   58: SymbolicLink  \GLOBAL??\ACPI#PNP0C0B#2#{05ecd13d-81da-4a2a-8a4c-524f23dd4dc9}
   5C: Key           \REGISTRY
   60: Key           HKLM\SYSTEM\ControlSet001\Control\hivelist
   64: SymbolicLink  \GLOBAL??\ACPI#PNP0C0B#0#{05ecd13d-81da-4a2a-8a4c-524f23dd4dc9}
   68: SymbolicLink  \GLOBAL??\ACPI#PNP0C0B#1#{dbe4373d-3c81-40cb-ace4-e0e5d05f0c9f}
   6C: Key           HKLM\SYSTEM\ControlSet001\Control\Session Manager\Memory Management\PrefetchParameters
   70: SymbolicLink  \GLOBAL??\ACPI#PNP0C0B#0#{dbe4373d-3c81-40cb-ace4-e0e5d05f0c9f}
   74: Key           HKLM\SYSTEM\ControlSet001
   78: SymbolicLink  \GLOBAL??\ACPI#PNP0C0B#1#{dbe4373d-3c81-40cb-ace4-e0e5d05f0c9f}
Normal text file                                    length : 8,48,39,387  lines : 17,27,28  Ln : 1  Col : 1  Sel : 0 | 0
```

Screenshot 3: **Handles in process**

11.3 PSGETSIDS:

To view the Security Identifiers which is associated with a process. It identifies processes like malignant exemption and specific users.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-3S, February 2019

```

SID for \\SWARNA--PUJITHA:
S-1-5-21-49518011-4190476529-3160085385
```

Screenshot 4: **Security identifiers**

11.4 PSINFO

PSINFO will gather the processes of a Virtual Address Descriptor and Process Environment Block information and displays the suspectable memory areas for running system.

```
System information for \\SWARNA--PUJITHA:
Uptime:                    19 days 6 hours 11 minutes 5 seconds
Kernel version:            Windows 10 Home, Multiprocessor Free
Product type:              Professional
Product version:           6.3
Service pack:              0
Kernel build number:       17134
Registered organization:
Registered owner:
IE version:                9.0000
System root:               C:\WINDOWS
Processors:                4
Processor speed:           2.3 GHz
Processor type:            Intel(R) Core(TM) i7-5500U CPU @
Physical memory:           2 MB
Video driver:
Volume Type       Format     Label                      Size        Free   Free
    C: Fixed      NTFS       Windows               455.94 GB   128.18 GB  28.1%

Installed     HotFix
n/a           Internet Explorer - 0
Applications:
Adobe Reader XI (11.0.23) 11.0.23
Adobe Refresh Manager 1.8.0
Advanced Port Scanner 2.4 2.4.2750
Advanced Port Scanner v1.3
AnyDesk ad 3.7.0
Autopsy 4.6.0
Bulk Extractor 1.5.5 1.5.5
Cisco Packet Tracer 6.0.1
CrypTool 1.4.40 1.4.40
GoTo Opener 1.0.470
Google Chrome 69.0.3497.100
Google Update Helper 1.3.33.17
HashCalc 2.02
Intel(R) Processor Graphics 20.19.15.4531
Java 8 Update 161 8.0.1610.12
Normal text file                                    length : 2,041    lines : 54
```

Screenshot 5: **Process information**

11.5 PSLIST

Pslist is a plugin used to obtain a list of processes running during imaging and provides information like process name, PID, PPID, threads, start and end time of process.

```
Process information for SWARNA--PUJITHA:

Name                          Pid Pri Thd  Hnd      VM      WS    Priv
Idle                            0   0   4    0       4       8      52
  System                        4   8 174 8151    3852     156     192
    smss                      412  11   2   61 4194303     216     500
    Memory Compression       1776   8 138    0  622080  459716    1488
Registry                       96   8   3    0  136656   23820    1716
csrss                         296  13  10  369 4194303      92    1712
csrss                         592  13  20  863 4194303    1516    2428
wininit                       700  13   1  174 4194303      36    1600
  fontdrvhost                  72   8   5   44 4194303     260    1932
  services                    816   9  11  740 4194303    7540    6500
    svchost                   356   8   5  152 4194303    4696    2336
    vmware-hostd              372   8  23  459  183016    3644   30596
    svchost                   384   8   4  117 4194303    5604    1476
    svchost                   668   8  29 1549 4194303   13628   12508
    svchost                   964   8   2   84 4194303     864     992
    svchost                   984   8  24 1471 4194303   29832   26248
      RuntimeBroker           328   8  40  972 4194303   34036   16676
      MicrosoftEdge          2288   8  24 1261 4194303   31132   32056
      WindowsInternal        3088   8  32  844 4194303     896   23184
      ShellExperienceHost    4164   8  38 1503 4194303    1368   53480
      unsecapp               4480   8   3  125 4194303    1812    1456
      SettingSyncHost        4488   6  10  719 4194303    3216   28264
      dllhost                4892   8   6  269 4194303    6388    4392
      MicrosoftEdgeCP        6056   8  32  833 4194303    8024   47588
      WmiPrvSE               6808   8   3  163   71320    1856    4408
      ApplicationFrameHost   7340   8   9  499 4194303   23996   16144
      MicrosoftEdgeCP        7832   8  14  523 4194303    6012    6160
      RuntimeBroker          8312   8   6  383 4194303    8408   12164
      MicrosoftEdgeCP        9224   8  14  514 4194303    5816    6088
      RemindersServer       10000   8   9  321 4194303   12924    7788
      RuntimeBroker         10636   8  26  769 4194303   21464   12420
        WINWORD             17720   8  23 1008 4194303   20176   84228
      WmiPrvSE              11076   8   8  470 4194303   19532    8028
      Video.UI              11688   8  22  725 4194303   10796   24240
Normal text file                                    length : 15,197    line
```

Screenshot 6: **List of Process**

11.6PSLOGGEDON

PSLOGGEDON can view the loaded profiles of a logged on users in the registry. It displays the locally logged users and logged users through local or remote computer [5].

```
Users logged on locally:
     31-10-2018 10:11:02          SWARNA--PUJITHA\Swarna

No one is logged on via resource shares.
```

Screenshot 7: **Logged on users**

11.7 CONSOLES

Consoles will find the commands in command prompt that attacker was typed and it scans the console information rather than command prompt. It collects the entire screen buffer and it displays the information like files, directories listed in directory command.

```
ipconfig /all
========================================
========================================

Windows IP Configuration

   Host Name . . . . . . . . . . . . : swarna--pujitha
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : 60-57-18-6E-CC-CA
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 4:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #3
   Physical Address. . . . . . . . . : 62-57-18-6E-CC-C9
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VMware Virtual Ethernet Adapter for VMnet1 #2
   Physical Address. . . . . . . . . : 00-50-56-C0-00-01
```

Screenshot 8: **List of commands in command prompt**

11.8 TCPVCON

It displays the list of all TCP and UDP endpoints of a system in local and remote addresses of TCP connections. It reports processes names and subset of netstat in windows.

```
TCP,svchost.exe,668,LISTENING,0.0.0.0,0.0.0.0
TCP,System,4,LISTENING,172.16.16.55,0.0.0.0
TCP,System,4,LISTENING,192.168.17.1,0.0.0.0
TCP,System,4,LISTENING,192.168.102.1,0.0.0.0
TCP,vmware-hostd.exe,372,LISTENING,0.0.0.0,0.0.0.0
TCP,vmware-authd.exe,3736,LISTENING,0.0.0.0,0.0.0.0
TCP,vmware-authd.exe,3736,LISTENING,0.0.0.0,0.0.0.0
TCP,svchost.exe,6408,LISTENING,0.0.0.0,0.0.0.0
TCP,TeamViewer_Service.exe,9784,LISTENING,127.0.0.1,0.0.0.0
TCP,AnyDesk.exe,3816,LISTENING,0.0.0.0,0.0.0.0
TCP,splunkd.exe,3728,LISTENING,0.0.0.0,0.0.0.0
TCP,python.exe,6156,LISTENING,127.0.0.1,0.0.0.0
TCP,splunkd.exe,3728,LISTENING,0.0.0.0,0.0.0.0
TCP,mongod.exe,4628,LISTENING,0.0.0.0,0.0.0.0
TCP,mongod.exe,4628,ESTABLISHED,127.0.0.1,127.0.0.1
TCP,mongod.exe,4628,ESTABLISHED,127.0.0.1,127.0.0.1
TCP,mongod.exe,4628,ESTABLISHED,127.0.0.1,127.0.0.1
TCP,mongod.exe,4628,ESTABLISHED,127.0.0.1,127.0.0.1
TCP,mongod.exe,4628,ESTABLISHED,127.0.0.1,127.0.0.1
TCP,mongod.exe,4628,ESTABLISHED,127.0.0.1,127.0.0.1
TCP,mongod.exe,4628,ESTABLISHED,127.0.0.1,127.0.0.1
TCP,mongod.exe,4628,ESTABLISHED,127.0.0.1,127.0.0.1
TCP,mongod.exe,4628,ESTABLISHED,127.0.0.1,127.0.0.1
TCP,vmware-hostd.exe,372,LISTENING,127.0.0.1,0.0.0.0
TCP,wininit.exe,700,LISTENING,0.0.0.0,0.0.0.0
TCP,svchost.exe,1400,LISTENING,0.0.0.0,0.0.0.0
TCP,lsass.exe,840,LISTENING,0.0.0.0,0.0.0.0
TCP,svchost.exe,1688,LISTENING,0.0.0.0,0.0.0.0
TCP,spoolsv.exe,3328,LISTENING,0.0.0.0,0.0.0.0
TCP,services.exe,816,LISTENING,0.0.0.0,0.0.0.0
TCP,splunkd.exe,3728,ESTABLISHED,127.0.0.1,127.0.0.1
TCP,splunkd.exe,3728,ESTABLISHED,127.0.0.1,127.0.0.1
TCP,splunkd.exe,3728,ESTABLISHED,127.0.0.1,127.0.0.1
TCP,splunkd.exe,3728,ESTABLISHED,127.0.0.1,127.0.0.1
TCP,splunkd.exe,7108,ESTABLISHED,127.0.0.1,127.0.0.1
TCP,splunkd.exe,7108,ESTABLISHED,127.0.0.1,127.0.0.1
TCP,splunkd.exe,7108,ESTABLISHED,127.0.0.1,127.0.0.1
```

Screenshot 9: TCP details

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

XII. ACKNOWLEDGEMENT

This work is supported by the Department of Science and Technology, India through the fund sanctioned for improvement of Science & Technology infrastructure, at department of CSE, K.L University, by order number SR/FST/ESI-332/2013.

XIII. CONCLUSION

In traditional digital forensics, when an incident has occurred the forensics investigator will identify the incident and perform forensic analysis to find the root cause of crime. Now-a-days digital forensics has developed in such a way that live monitoring is the main perspective to identify and mitigate the incident that happened. Live monitoring provides an in-depth analysis of identifying how the incident happened and what are the activities occur while the system is active. It's complicated to acquire a memory dump and perform the volatile analysis using the command line. So, to make it easier for analyzing the dump, the approach in this paper represents the automated analysis.

REFERENCES

1. Victor Voelzow "LIVE DATA FORENSICS - OR - WHY VOLATILE DATA CAN BE CRUCIAL FOR YOUR CASES" Blog on council of Europe Apr 30, 2013.
2. Mahesh Kolhe, PurnimaAhirao "LIVE VS DEAD COMPUTER FORENSIC IMAGE ACQUISITION" International Journal of Computer Science and Information Technologies, Vol. 8 (3), 2017, 455-457, ISSN: 0975-9646.
3. Lei Zhang, Dong Zhang, Lianhai Wang "LIVE DIGITAL FORENSICS IN A VIRTUAL MACHINE" International Conference on Computer Application 2010 Vol 4, 978-1-4244-7237-6.
4. C.L.T. Brown "COLLECTING VOLATILE DATA" Lecture Notes on Digital Forensics Aug 27, 2006.
5. Online "live-response-collecting-volatile-data-windows-forensic-analysis" tutorial on windows forensics analysis.
6. Pooja Gupta "CAPTURING EPHEMERAL EVIDENCE USING LIVE FORENSICS" IOSR Journal of Electronics and Communication Engineering, e-ISSN: 2278-2834,p- ISSN: 2278-8735, PP 109-113.
7. Brian Hay, Matt Bishop, Kara Nance "LIVE ANALYSIS: PROGRESS AND CHALLENGES" IEEE Xplore, 10.1109/MSP.2009.43, 2009.
8. Marthie Lessing, Asie Von Solms "LIVE FORENSIC ACQUISITION AS ALTERNATIVE TO TRADITIONAL FORENSIC PROCESSES" Research Gate, 30511418, 2008.
9. Martha Maria Grobler "LIFORAC – A MODEL FOR LIVE FORENSIC ACQUISITION" UJ Content UJ Institutional Repository, 2009.
10. Esan P. Panchal "EXTRACTION OF PERSISTENCE AND VOLATILE FORENISCS EVIDENCES FROM COMPUTER SYSTEM" International Journal of Computer Trends and Technology, V$(5):964-968, May Issue 2013, ISSN 2231-2803
11. K.V.D.KIRAN,"IntegratedDistributed Architecture to Integrate Wireless Sensor Networks (WSN) with Grid for Healthcare," International Journal of Bio-Science and Bio-Technology", Vol.7, No.3 (2015), pp.243-250, ISSN: 2233-7849 IJBSBT.
12. K.V.D.KIRAN,"A Critical study of information security risk assessment using fuzzy and entropy methodologies," International Journal on Computers and Communications", Pages: 17-22,Vol1,Isuue1,Dec-,12, ISSN: 2319 – 8869.
13. K.V.D.KIRAN," "Literature Review on RisK Literature Review on Risk and their Components"International Journal for Research in Emerging Science and Technology (IJREST) ",Volume-1, Issue-6, November 2014",(e-ISSN 2349-7610).
14. K.V.D.KIRAN,"Performance Analysis of Layered Architecture to Integrate Mobile Devices and Grid computing with a resource scheduling algorithm", IEEE CS'07, SIVAKASI, TAMIL NADU,India
15. K.V.D.Kiran "Risk Assessment in Distributed Banking System," International Journal of Applied Engineering Research(IJAER)", ISSN 0973-4562 Volume 9, Number 19 (2014) pp. 6087-6100
16. K.V.D.Kiran ,"Analysis and Classification Scheme of Risk Assessment Miniatures placed on Different Criteria for Reducing the Risk", International Journal of Applied Engineering Research"pp.12069-12085, ISSN 0973-4562 Volume 9, Number 22 (2014)
17. K.V.D.Kiran ,"Information Security risk authority in critical informative systems",CSIBIG 2014
18. K.V.D.Kiran ,"Survey on mobile malware analysis and detection", Volume 7, Issue 2.32 Special Issue 32, 2018, Pages 279-282, ISSN:2227524X

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)