DIGITAL FORENSIC ANALYSIS OF RANSOMWARE INFECTED WINDOWS SYSTEM

[1] Diana Rathod [2] Dr. Priyanka Sharma

[1] Post Graduation, Cyber Security, M.Tech, Raksha Shakti University, Ahmedabad, Gujarat, India

[2]Professor and Head, Information Technology & Telecommunication Department, Raksha Shakti University, Ahmedabad, Gujarat

ABSTRACT

Malware is one of the most serious threats to system security. It causes complex problems and issues on the system. Purpose of this research work is to forensically analyze and investigate a malware infected windows system. Windows operating system is infected with a ransomware. Forensic artifacts are obtained using various digital forensic tools and techniques such as recovery of lost and encrypted data, volatile memory analysis using memory forensics and registry analysis. Behaviour of the malicious code is analyzed in a controlled sandbox environment. Here, we are using various open source tools such as FTK Imager, Autopsy, Volatility Framework and open source cuckoo sandbox environment.

Keywords- Digital Forensics, Encrypted Data Recovery, Memory Forensics, Malware analysis, Cuckoo Sandbox, Ransomware, Windows Operating System.

I. INTRODUCTION

In recent times, malware is one of the serious threats to computer security. It is software or a program which causes harm to the computer. This malicious program can perform variety of different functions such as stealing, encrypting or deleting sensitive data, monitoring user's activity without their permission. Commonly used types of malware are virus, worms, Trojan, spyware, ransomware etc. Most of the malwares are spread through internet or through USB devices. Traces of malicious activity in any system can be identified through digital forensic techniques. Digital forensics is collection, analysis and preservation of the digital evidences. Digital forensics is law based method for investigation. Forensics tools are now used to examine and analyze any crime and malicious activity in the organization which is done by attacker, hacker or criminal.

In this paper we focus on the digital forensic Investigation of ransomware infected Windows operating system and find the artifacts using various open source forensic tools and techniques. We provide an efficient approach and methodology to investigate and analyze malware in forensic manner. Also, the behaviour of malicious program is analyzed in a controlled sandbox environment. We focused on encrypted data recovery, volatile memory analysis, registry artifacts, static and dynamic analysis in sandbox environment and analyzing the results for understanding the behaviour of malicious program. This Investigation and analysis of malware may help in preventing more infections and enhances the security of the system.

II. RELATED WORKS

Digital forensic is a science and process of collecting, preserving, analyzing and reporting legally admissible evidence to court. Different cybercrimes result in different Digital evidences. Digital forensic Investigation procedure includes following steps:

1. Acquiring the evidence: Acquire the evidence using standardized and accepted procedures and techniques. It includes duplication that is imaging or cloning of the hard drive of the system. Also, includes acquisition of volatile memory data.
2. Preserving the evidence: Evidence must be secured and preserved in its original state. It must be authentic and unaltered. For preserving and authenticating evidence cryptographic hash algorithms are used.
3. Analysis of the evidence: Find relevant artifacts and draw conclusion from the acquired evidence.
4. Reporting and presentation: Summarize and provide explanations of the conclusions, Tools and methodologies used, steps followed in lay person's terms.

Now, Malware analysis is the art of analyzing malicious program in order to understand how it works, how to identify it and how to eliminate it. There are two basic techniques for malware analysis:

1. Static analysis: Static analysis involves going through the code in order to discover what the program does. It is performed in non-runtime environment.it examines strings, imports, exports etc.
2. Dynamic analysis is process of running the malware and observing its behaviour. It monitors system memory, functions behaviour and overall performance of the system.

Volatile memory analysis: Memory forensic is a art of analyzing volatile memory data of computer. It is used to identify and analyze the malicious behaviour that do not leave any trace on hard drive data.

We have used the above methodologies and techniques for a effective and efficient investigation and analysis of windows system infected with ransomware. Digital forensic open source tools and procedure is used to analyze and obtain forensic artifacts, recover encrypted and deleted data from infected windows system. The malicious program is analyzed in a cuckoo sandbox environment. Thus, by performing both this techniques gives a effective approach to analyze ransomware infected system and provides better and reliable results.

III. PROPOSED METHODOLOGY

The proposed work of our research is explained in this section. We use an effective methodology to analyze the windows 7 operating system which is infected with the Wannacry ransomware. First, the forensic investigation of the system is carried out in which relevant forensic artifacts are extracted from the image of the system, along with this its volatile memory is also analyzed using volatility framework and then malicious executable is executed in a cuckoo sandbox environment. We executed the malware to understand its actual behaviour.

A. Digital Forensic Investigation:

In this approach the image of the infected system is taken along with its RAM Memory. The investigation is conducted in two stages:

Stage 1: Collection of digital Evidence.

Stage 2: Analysis of collected Evidence.

Collection of Evidence:

For collecting the evidence we are taking an image of the hard disk drive of the infected windows 7 system using open source FTK Imager tool. The image is taken in a standard E01 format.

Steps to create image using FTK Imager.

1. Open FTKImager.exe and Go to File menu
2. Select Create Disk Image option
3. Select the source of evidence. Physical Drive in our case.
4. Select the source Drive.
5. Select the format in which you want to create Image. E01 in our case.
6. Fill evidence information.
7. Select Image destination path, image name and Image fragment size and compression level.
8. Start creating the Image.

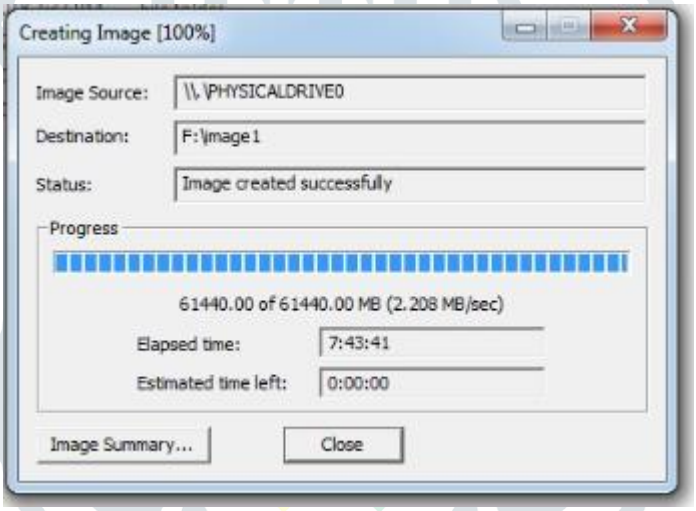

Figure 1: Creating Image of Hard drive

Also, we need to acquire Volatile memory data for more effective and efficient analysis of the compromised system. For this we are capturing the memory of the windows 7 system using FTK imager tool.

Steps to capture Memory in FTK Imager:

1. Open FTKImager.exe go to file menu.
2. Select Capture memory.
3. Browse to the destination path for dump file.
4. Enter filename for dump file.
5. Start capturing memory.

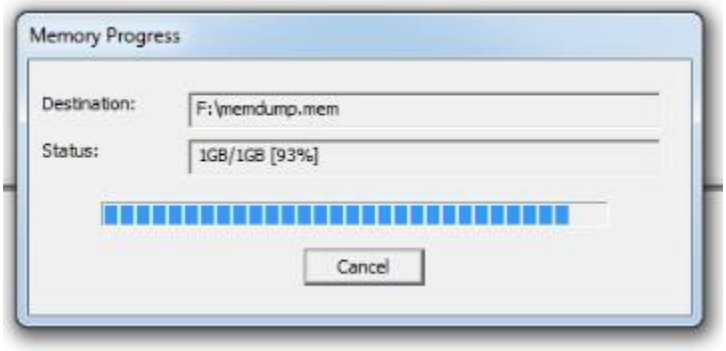

Figure 2. Memory Capture

Analysis of Collected Evidence:

The image of the ransomware infected machine is opened using Autopsy open source tool. We can go through the image and find out which files are present and/or deleted on the infected machine. Autopsy works on the basis of modules. It has many in-built modules which are useful and helpful in forensic investigation. It uses PhotoRec carver for recovering deleted data from the hdd. Some other modules are timeline analysis, keyword search, web artifacts, indicators of compromise etc. It is easy to use and cost effective tool.

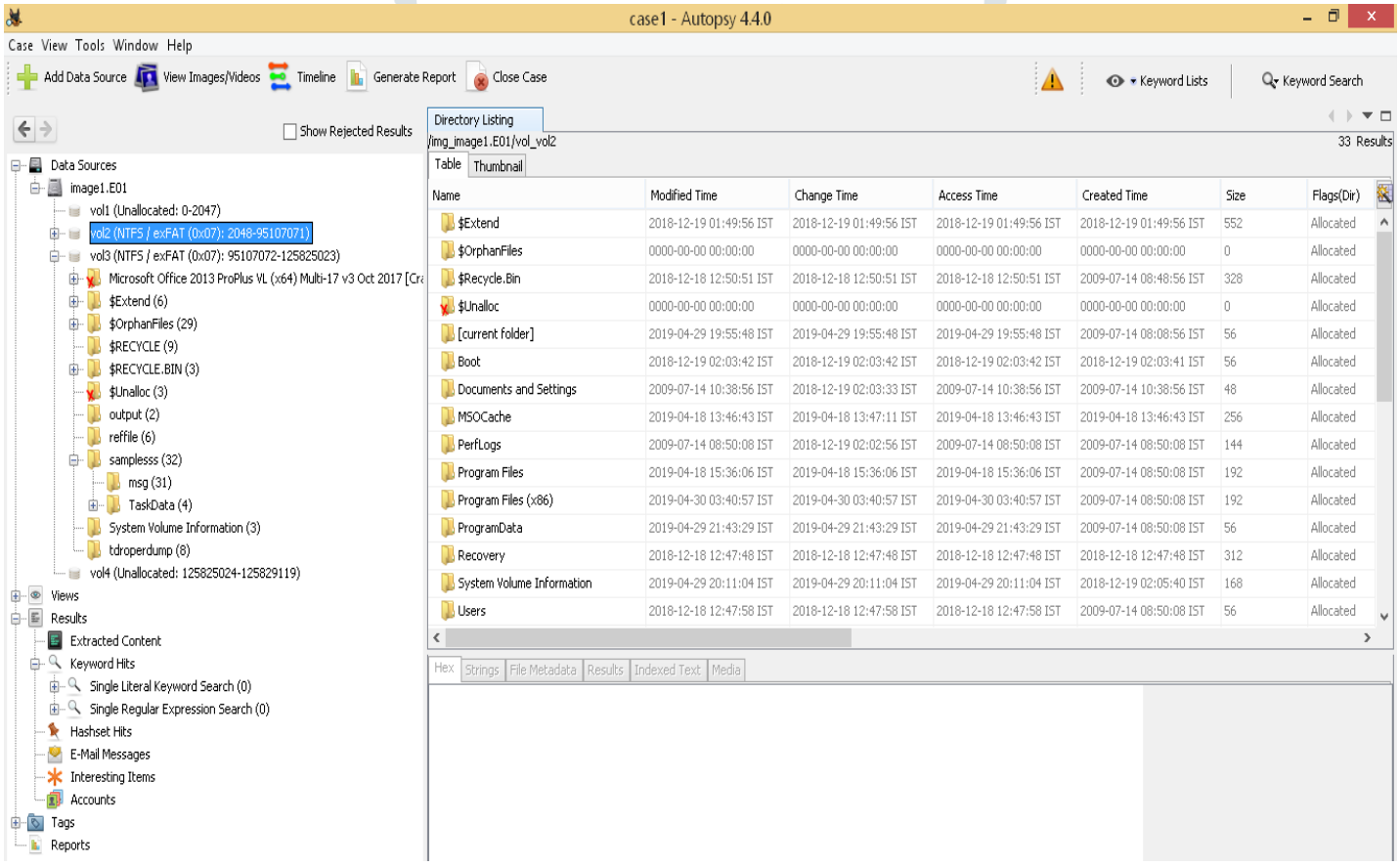

Figure 3: Analysis of image file using Autopsy

Now, by analyzing the image in autopsy, we can observe that every file on the system is encrypted by the Wannacry ransomware. The ransomware encrypts the file and changes their extension to .WNCRY. This .WNCRY files are not accessible and user cannot open this files. We have lost access to data of the infected

system. User can get the key for decryption only after the ransom is paid to the attacker. Wannacry ransomware demands ransom in bitcoins.

Steps to analyze e01 image file in autopsy:

1. Open a new case from file menu.
2. Enter the information such as case name, path, examiner name, case number etc.
3. Add data source. Image file in our case.
4. Browse and select data source.
5. Configure ingest modules.
6. Autopsy will start analyzing the image file and run the modules.

Analyzing memory artifacts:

The ram memory dump collected is parsed using volatility a open source memory analysis tool for parsing and analyzing memory dump files. It supports 32-bit and 64-bit windows, Linux kernels and MacOS X and android phone memory dump. Volatility has many plugins useful for identifying the malware infection.

Some of them are:

1. Pslist: to print list of loaded processes.
2. Pstree: to show processes in parent child tree.
3. Psscan: to scan for hidden or terminated processes.
4. Dlllist:to list loaded dll's for each process.
5. Connscan: to test tcp connections.
6. Malfind: detect hidden and injected code.
7. Psxview: Identifies process trying to avoid detection.

Steps:

Open Command prompt and go to directory, where volatility framework is present.

Run the volatility.exe file in command prompt with respective options.

Command: **D:/Volatility.exe -h**

We have a memory dump of infected system with file name memdump1.mem; we get the image information using imageinfo command.

Command: **D:/volatility.exe -f memdump1.mem imageinfo**

```
D:\>volatility.exe -f memdump1.mem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (D:\memdump1.mem)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf80002a030a0L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff80002a04d00L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2019-04-30 17:35:46 UTC+0000
     Image local date and time : 2019-04-30 23:05:46 +0530
```

Figure 4: Image Information

To know the processes that were running during the RAM Capture pslist plug-in is used. It lists the running processes.

Command: **D:/volatility.exe -f memdump1.mem --profile=Win7SP1x64 pslist**

```
D:\>volatility.exe -f memdump1.mem --profile=Win7SP1x64 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0xfffffa8000ca19e0 System                    4      0     88      507 ------      0 2019-04-30 17:15:40 UTC+0000
0xfffffa8001231590 smss.exe                220      4      2       29 ------      0 2019-04-30 17:15:40 UTC+0000
0xfffffa8001d6ea00 csrss.exe               312    304      9      466      0      0 2019-04-30 17:16:13 UTC+0000
0xfffffa8001dff060 csrss.exe               364    356      9      272      1      0 2019-04-30 17:16:18 UTC+0000
0xfffffa8001ff2910 wininit.exe             372    304      3       75      0      0 2019-04-30 17:16:18 UTC+0000
0xfffffa80024100c0 winlogon.exe            408    356      3      112      1      0 2019-04-30 17:16:20 UTC+0000
0xfffffa800240cb30 services.exe            472    372      8      211      0      0 2019-04-30 17:16:30 UTC+0000
0xfffffa8002419b30 lsass.exe               496    372      7      580      0      0 2019-04-30 17:16:32 UTC+0000
0xfffffa80024180f0 lsm.exe                 504    372     10      140      0      0 2019-04-30 17:16:32 UTC+0000
0xfffffa80024c6910 svchost.exe             596    472     10      348      0      0 2019-04-30 17:17:01 UTC+0000
0xfffffa80024dd2f0 vmacthlp.exe            660    472      3       63      0      0 2019-04-30 17:17:08 UTC+0000
0xfffffa8002505b30 svchost.exe             704    472      8      290      0      0 2019-04-30 17:17:17 UTC+0000
0xfffffa800252bb30 svchost.exe             764    472     20      450      0      0 2019-04-30 17:17:20 UTC+0000
0xfffffa8002447b30 svchost.exe             852    472     13      346      0      0 2019-04-30 17:17:39 UTC+0000
0xfffffa80024bcb30 svchost.exe             876    472     34     1078      0      0 2019-04-30 17:17:39 UTC+0000
0xfffffa800255a610 svchost.exe            1004    472     13      534      0      0 2019-04-30 17:17:46 UTC+0000
0xfffffa80025e1910 spoolsv.exe            1040    472     12      266      0      0 2019-04-30 17:17:59 UTC+0000
0xfffffa80025946f0 taskhost.exe           1064    472      7      192      1      0 2019-04-30 17:18:02 UTC+0000
0xfffffa80026017a0 svchost.exe            1128    472     18      315      0      0 2019-04-30 17:18:02 UTC+0000
0xfffffa8002652b30 svchost.exe            1200    472      9      312      0      0 2019-04-30 17:18:04 UTC+0000
0xfffffa8002699b30 VGAuthService.         1344    472      3       86      0      0 2019-04-30 17:18:06 UTC+0000
0xfffffa80026ec640 vmtoolsd.exe           1424    472     10      274      0      0 2019-04-30 17:18:08 UTC+0000
0xfffffa800272fb30 sppsvc.exe             1640    472      4      145      0      0 2019-04-30 17:18:13 UTC+0000
0xfffffa80027c0330 svchost.exe            1840    472      5       99      0      0 2019-04-30 17:18:18 UTC+0000
0xfffffa80027f8b30 dllhost.exe            2028    472     14      202      0      0 2019-04-30 17:19:21 UTC+0000
0xfffffa800283c630 msdtc.exe               896    472     14      154      0      0 2019-04-30 17:19:25 UTC+0000
0xfffffa80028c5b30 GoogleCrashHan         2120   1528      5      103      0      1 2019-04-30 17:19:34 UTC+0000
0xfffffa80028af060 GoogleCrashHan         2128   1528      6       90      0      0 2019-04-30 17:19:34 UTC+0000
0xfffffa8002728a70 svchost.exe            2200    472     11      136      0      0 2019-04-30 17:19:37 UTC+0000
0xfffffa80028eab30 WmiPrvSE.exe           2264    596      6      215      0      0 2019-04-30 17:19:38 UTC+0000
0xfffffa8002856ab0 dwm.exe                2328    852      5      136      1      0 2019-04-30 17:19:39 UTC+0000
0xfffffa8002854450 explorer.exe           2336   2320     28      769      1      0 2019-04-30 17:19:39 UTC+0000
0xfffffa8002d75060 vmtoolsd.exe           2476   2336      7      201      1      0 2019-04-30 17:19:49 UTC+0000
0xfffffa8002d78b30 ailiao.exe             2484   2336     16      353      1      1 2019-04-30 17:19:49 UTC+0000
0xfffffa8002d47b30 SearchIndexer.         2736    472     11      611      0      0 2019-04-30 17:19:56 UTC+0000
0xfffffa8002eef750 svchost.exe            2452    472     13      338      0      0 2019-04-30 17:21:17 UTC+0000
0xfffffa80028a8b30 wannacry.exe           1616   2336      8       86      1      1 2019-04-30 17:25:28 UTC+0000
0xfffffa8003071300 FTK Imager.exe         2324   2336      8      343      1      1 2019-04-30 17:29:26 UTC+0000
0xfffffa80030375f0 taskeng.exe            1232    876      5       86      0      0 2019-04-30 17:30:15 UTC+0000
0xfffffa8003024260 GoogleUpdate.e         1052   1232      5      131      0      1 2019-04-30 17:30:58 UTC+0000
0xfffffa8002ff3060 GoogleCrashHan          912   1052      3       90      0      1 2019-04-30 17:36:23 UTC+0000
0xfffffa8002ea0730 WmiPrvSE.exe            648    596     10      175      0      0 2019-04-30 17:36:32 UTC+0000
0xfffffa80027ed060 @WanaDecryptor         1764   1616      2        0      1      1 2019-04-30 17:37:23 UTC+0000
0xfffffa8002e33060 SearchProtocol         1980   2736      7      236      0      0 2019-04-30 17:37:26 UTC+0000
0xfffffa8002e99060 GoogleUpdate.e         2084   1052      1       28      0      1 2019-04-30 17:37:36 UTC+0000
0xfffffa8002ff0b30 SearchFilterHo         2768   2736      4       82      0      0 2019-04-30 17:37:40 UTC+0000
0xfffffa8003048060 @WanaDecryptor         1988   1616      1       67      1      1 2019-04-30 17:37:42 UTC+0000
0xfffffa8003011610 VSSVC.exe              2660    472      6      121      0      0 2019-04-30 17:38:06 UTC+0000
0xfffffa8002fbe060 taskhsvc.exe            980   1764      7      111      1      1 2019-04-30 17:38:09 UTC+0000
0xfffffa8002d61b30 conhost.exe            1716    364      1       34      1      0 2019-04-30 17:38:10 UTC+0000
0xfffffa8002ee8290 WmiPrvSE.exe           2004    596      7        8      0      1 2019-04-30 17:38:49 UTC+0000
```

Figure5: Running processes extracted from Image

From pslist command we get to know the process id for a particular process and also parent process which triggered it. From this info we can find if any suspicious process is triggered by a parent process.

Psscan plugin is used to find the processes that are hidden and terminated.

Command: **D:/volatility.exe -f memdump1.mem --profile=Win7SP1x64 psscan**

```
D:\>volatility.exe -f memdump1.mem --profile=Win7SP1x64 psscan
Volatility Foundation Volatility Framework 2.6
Offset(P)          Name                PID   PPID PDB                Time created                   Time exited
------------------ ---------------- ------ ------ ------------------ ------------------------------ ------------------------------
0x000000003da11610 VSSVC.exe          2660    472 0x00000000032f5b000 2019-04-30 17:38:06 UTC+0000
0x000000003da24260 GoogleUpdate.e     1052   1232 0x00000000039bbf000 2019-04-30 17:30:58 UTC+0000
0x000000003da375f0 taskeng.exe        1232    876 0x000000000189e8000 2019-04-30 17:30:15 UTC+0000
0x000000003da48060 @WanaDecryptor     1988   1616 0x00000000039cd4000 2019-04-30 17:37:42 UTC+0000
0x000000003da71300 FTK Imager.exe     2324   2336 0x0000000006075000 2019-04-30 17:29:26 UTC+0000
0x000000003da71b30 taskeng.exe        2108    876 0x00000000117c2000 2019-04-30 17:29:05 UTC+0000   2019-04-30 17:30:19 UTC+0000
0x000000003dc33060 SearchProtocol     1980   2736 0x00000000023fc1000 2019-04-30 17:37:26 UTC+0000
0x000000003dc99060 GoogleUpdate.e     2084   1052 0x00000000014ffb000 2019-04-30 17:37:36 UTC+0000
0x000000003dca0730 WmiPrvSE.exe        648    596 0x000000002bf1f000 2019-04-30 17:36:32 UTC+0000
0x000000003dce8290 WmiPrvSE.exe       2004    596 0x00000000e8a5000 2019-04-30 17:38:49 UTC+0000
0x000000003dcef750 svchost.exe        2452    472 0x000000002acd6000 2019-04-30 17:21:17 UTC+0000
0x000000003dd23b30 OSPPSVC.EXE        3056    472 0x00000000013bd1000 2019-04-30 17:22:02 UTC+0000   2019-04-30 17:32:37 UTC+0000
0x000000003ddbe060 taskhsvc.exe        980   1764 0x000000000fceb000 2019-04-30 17:38:09 UTC+0000
0x000000003ddf0b30 SearchFilterHo     2768   2736 0x000000002ace1000 2019-04-30 17:37:40 UTC+0000
0x000000003ddf3060 GoogleCrashHan      912   1052 0x00000000036cd8000 2019-04-30 17:36:23 UTC+0000
0x000000003df47b30 SearchIndexer.     2736    472 0x00000000033ac3000 2019-04-30 17:19:56 UTC+0000
0x000000003df61b30 conhost.exe        1716    364 0x000000000c196000 2019-04-30 17:38:10 UTC+0000
0x000000003df75060 vmtoolsd.exe       2476   2336 0x000000000386af000 2019-04-30 17:19:49 UTC+0000
0x000000003df78b30 ailiao.exe         2484   2336 0x0000000038504000 2019-04-30 17:19:49 UTC+0000
0x000000003dfc68a0 taskse.exe         2244   1616 0x000000000d00f000 2019-04-30 17:38:53 UTC+0000   2019-04-30 17:38:54 UTC+0000
0x000000003e23c630 msdtc.exe           896    472 0x0000000007925000 2019-04-30 17:19:25 UTC+0000
0x000000003e254450 explorer.exe       2336   2320 0x000000003cc11000 2019-04-30 17:19:39 UTC+0000
0x000000003e256ab0 dwm.exe            2328    852 0x000000000c71000 2019-04-30 17:19:39 UTC+0000
0x000000003e2a8b30 wannacry.exe       1616   2336 0x0000000001206000 2019-04-30 17:25:28 UTC+0000
0x000000003e2af060 GoogleCrashHan     2128   1528 0x000000000585c000 2019-04-30 17:19:34 UTC+0000
0x000000003e2c5b30 GoogleCrashHan     2120   1528 0x0000000005855000 2019-04-30 17:19:34 UTC+0000
0x000000003e2eab30 WmiPrvSE.exe       2264    596 0x000000000f33000 2019-04-30 17:19:38 UTC+0000
0x000000003e4017a0 svchost.exe        1128    472 0x000000000e781000 2019-04-30 17:18:02 UTC+0000
0x000000003e452b30 svchost.exe        1200    472 0x000000000ddbc000 2019-04-30 17:18:04 UTC+0000
0x000000003e499b30 VGAuthService.     1344    472 0x000000000d28a000 2019-04-30 17:18:06 UTC+0000
0x000000003e4ec640 vmtoolsd.exe       1424    472 0x000000000cc10000 2019-04-30 17:18:08 UTC+0000
0x000000003e528a70 svchost.exe        2200    472 0x00000000004e33000 2019-04-30 17:19:37 UTC+0000
0x000000003e52fb30 sppsvc.exe         1640    472 0x000000000ab7d000 2019-04-30 17:18:13 UTC+0000
0x000000003e5c0330 svchost.exe        1840    472 0x000000002f500000 2019-04-30 17:18:18 UTC+0000
0x000000003e5ed060 @WanaDecryptor     1764   1616 0x0000000011cb5000 2019-04-30 17:37:23 UTC+0000
0x000000003e5f8b30 dllhost.exe        2028    472 0x00000000089dc000 2019-04-30 17:19:21 UTC+0000
0x000000003e60cb30 services.exe        472    372 0x0000000017816000 2019-04-30 17:16:30 UTC+0000
0x000000003e6100c0 winlogon.exe        408    356 0x0000000019906000 2019-04-30 17:16:20 UTC+0000
0x000000003e6180f0 lsm.exe             504    372 0x0000000017583000 2019-04-30 17:16:32 UTC+0000
0x000000003e619b30 lsass.exe           496    372 0x000000001747c000 2019-04-30 17:16:32 UTC+0000
0x000000003e647b30 svchost.exe         852    472 0x0000000012730000 2019-04-30 17:17:39 UTC+0000
0x000000003e6bcb30 svchost.exe         876    472 0x0000000012cb9000 2019-04-30 17:17:39 UTC+0000
0x000000003e6c6910 svchost.exe         596    472 0x0000000016a14000 2019-04-30 17:17:01 UTC+0000
0x000000003e6dd2f0 vmacthlp.exe        660    472 0x000000000160f4000 2019-04-30 17:17:08 UTC+0000
0x000000003e705b30 svchost.exe         704    472 0x0000000015e01000 2019-04-30 17:17:17 UTC+0000
0x000000003e72bb30 svchost.exe         764    472 0x000000000158a9000 2019-04-30 17:17:20 UTC+0000
0x000000003e75a610 svchost.exe        1004    472 0x0000000012icb000 2019-04-30 17:17:46 UTC+0000
0x000000003e7946f0 taskhost.exe       1064    472 0x000000000e86f000 2019-04-30 17:18:02 UTC+0000
0x000000003e798920 conhost.exe        2544    364 0x00000000033a9000 2019-04-30 17:37:51 UTC+0000   2019-04-30 17:38:50 UTC+0000
0x000000003e7e1910 spoolsv.exe        1040    472 0x000000000ee2b000 2019-04-30 17:17:59 UTC+0000
0x000000003edf2910 wininit.exe         372    304 0x000000001a10f000 2019-04-30 17:16:18 UTC+0000
0x000000003ef6ea00 csrss.exe           312    304 0x000000001aa09000 2019-04-30 17:16:13 UTC+0000
```

Figure6: processes extracted by psscan command

To identify rogue process in Ram Dump we use malfind Plugin. It extracts process dumps that are malicious. The processes produced by volatility framework are uploaded to “virustotal.com” to check if the processes present in the dump are infected with any malware.

By doing memory dump analysis we can observe that a parent process explorer.exe(PID:2326) triggers the wannacry.exe(PID:1616) which in turn triggers taskse.exe (PID:2244) and @wanadecrypter(PID:1764) as shown in figure 5 & 6. This proves that the system is infected with Wannacry.exe ransomware.

IV. RESULTS

As we have seen that the Wannacry ransomware encrypts the data present on the system. By analyzing the e01 image we observed that the ransomware tries to delete the file after generating its .WNCRY copy. We can extract the encrypted data from autopsy as it uses data carving techniques. Thus, as shown in figure we recovered the encrypted data from autopsy.

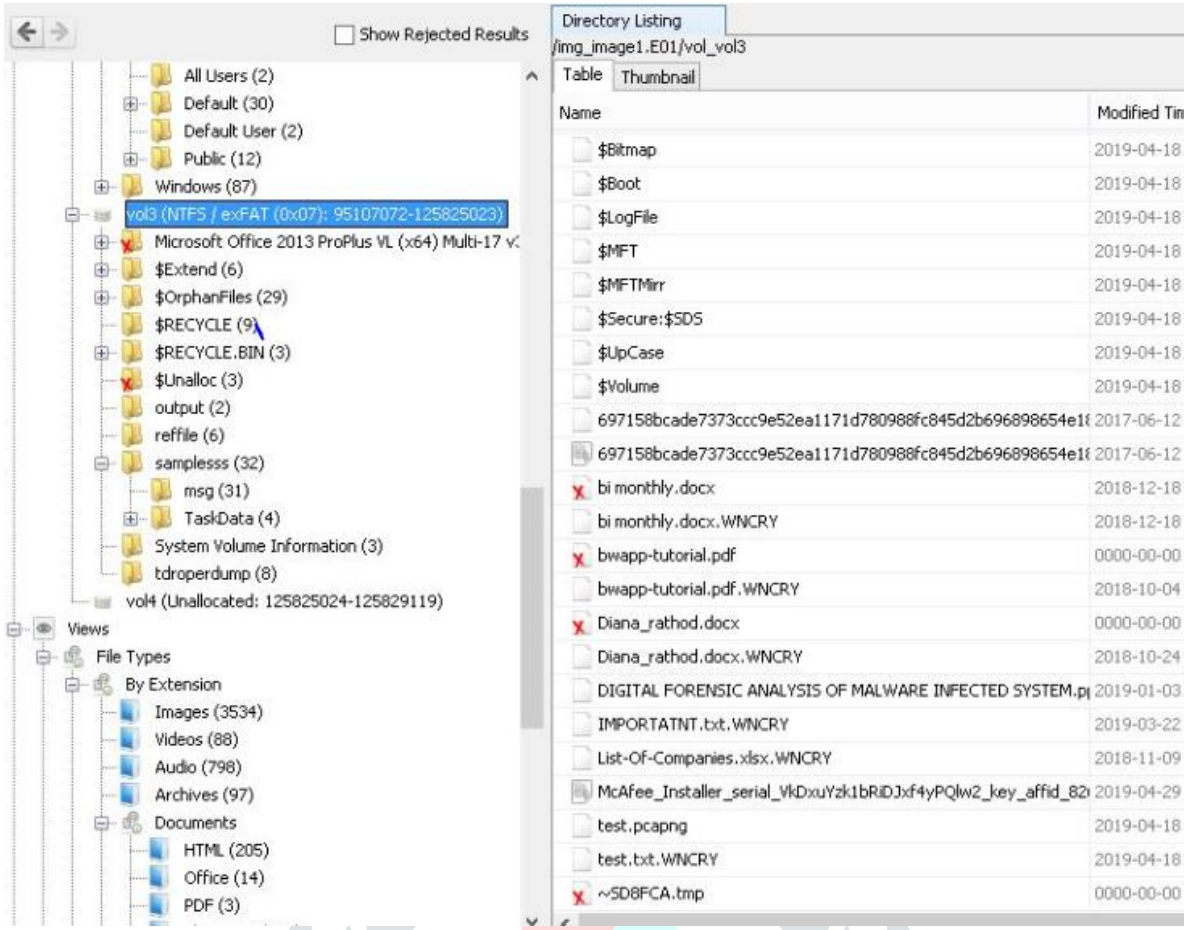

Figure7: encrypted files with extension .wncry

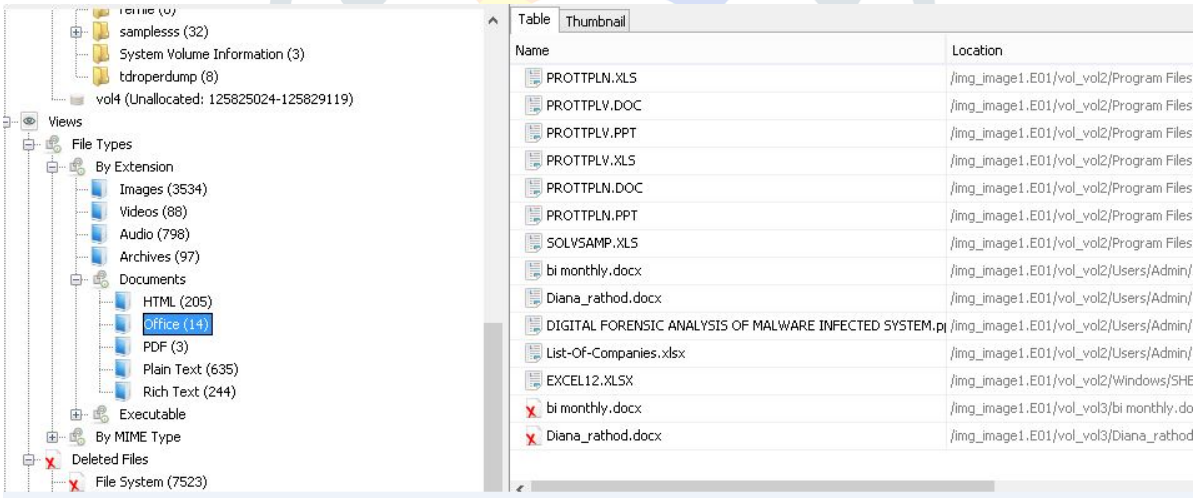

Figure8: Original files that can be recovered using autopsy

27619-340s.exe.zip	4/30/2019 2:38 PM	Compressed (zipp...	275 KB
27621-BlackDream.zip	4/30/2019 2:38 PM	Compressed (zipp...	167 KB
27623-smb-qua22o4u.7z	4/30/2019 2:38 PM	WinRAR archive	38 KB
27625-Trojan.Dropper.Gen.zip	4/30/2019 2:38 PM	Compressed (zipp...	1,588 KB
27627-Trojan.Kovter.zip	4/30/2019 2:38 PM	Compressed (zipp...	332 KB
27629-VBS.NoWarning.A.zip	4/30/2019 2:38 PM	Compressed (zipp...	2 KB
27631-WisdomEyes.7z	4/30/2019 2:38 PM	WinRAR archive	24 KB
bi monthly.docx	4/30/2019 2:34 PM	Microsoft Word D...	14 KB
bwapp-tutorial.pdf	4/30/2019 2:34 PM	Adobe Acrobat D...	8,947 KB
Diana_rathod.docx	4/30/2019 2:35 PM	Microsoft Word D...	59 KB
DIGITAL FORENSIC ANALYSIS OF MALW...	4/30/2019 2:35 PM	Microsoft PowerP...	66 KB
IMPORTATNT.txt	4/30/2019 2:37 PM	Text Document	1 KB
List-Of-Companies.xlsx	4/30/2019 2:36 PM	Microsoft Excel W...	26 KB

Figure9: list of original files extracted from autopsy

In memory analysis the ransomware Wannacry.exe infects the parent process “explorer.exe” and its child process are triggered “taskse.exe” & “@wanadecryptor.exe” as shown in above figure 5 & 6.

Now the Wannacry.exe executable is analyzed in a sandbox environment. The malware is executed in a controlled sandbox environment and its behaviour is observed, activities are logged and summarized report is generated. This report gives the findings of static and dynamic analysis of the ransomware. following snapshots shows the analysis done using cuckoo sandbox.

File *wannacry.exe*

Summary Download Resubmit sample

Size	3.4MB
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	84c82835a5d21bbcf75a61706d8ab549
SHA1	5ff465afaabcbf0150d1a3ab2c2e74f3a4426467
SHA256	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
SHA512	Show SHA512
CRC32	4022FCAA
ssdeep	98304:QqPoBhz1aRxcSUDk36SAEdhvxWa9P593R8yAVp2g3x:QqPe1Cxcxk3ZAEUadzR8yc4gB
Yara	• WannaDecryptor - Detection for common strings of WannaDecryptor • Wanna_Sample_84c82835a5d21bbcf75a61706d8ab549 - Specific sample match for WannaCryptor • ransom_telefonica - Ransmoware Telefonica • Wanna_Cry_Ransomware_Generic - Detects WannaCry Ransomware on Disk and in Virtual Page • WannaCry_Ransomware - Detects WannaCry Ransomware • WannaCry_Ransomware_Dropper - WannaCry Ransomware Dropper • CRC32_poly_Constant - Look for CRC32 [poly] • CRC32_table - Look for CRC32 table • RijnDael_AES - RijnDael AES

Figure10: brief info about the malicious executable

Figure11: Message on the screen when ransomware is executed

Behavioral Analysis:

Behavioral Analysis

Process Tree

- @WanaDecryptor@.exe (2656) @WanaDecryptor@.exe co
  - taskhsvc.exe (2060) TaskData\Tor\taskhsvc.exe
- cmd.exe (3768) cmd.exe /c start /b @WanaDecryptor@.exe vs
  - @WanaDecryptor@.exe (2832) @WanaDecryptor@.exe vs
    - cmd.exe (2748) cmd.exe /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} r
      wbadmin delete catalog -quiet
      - vssadmin.exe (3208) vssadmin delete shadows /all /quiet
      - WMIC.exe (3036) wmic shadowcopy delete
      - bcdedit.exe (3412) bcdedit /set {default} bootstatuspolicy ignoreallfailures
      - bcdedit.exe (1600) bcdedit /set {default} recoveryenabled no
      - wbadmin.exe (2640) wbadmin delete catalog -quiet
- taskse.exe (3060) taskse.exe C:\Users\ADMIN\AppData\Local\Temp\@WanaDecryptor@.exe
- @WanaDecryptor@.exe (836) @WanaDecryptor@.exe
- cmd.exe (2336) cmd.exe /c reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "swjwogwnbof758" /t REG_SZ /d "\"C:\Users\ADMIN\AppData\Local\Temp\tasksche.exe\"" /f
  - reg.exe (3096) reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "swjwogwnbof758" /t REG_SZ /d "\"C:\Users\ADMIN\AppData\Local\Temp\tasksche.exe\"" /f
- taskdl.exe (3020) taskdl.exe
- taskse.exe (3952) taskse.exe C:\Users\ADMIN\AppData\Local\Temp\@WanaDecryptor@.exe
- @WanaDecryptor@.exe (3600) @WanaDecryptor@.exe
- taskdl.exe (3212) taskdl.exe
- taskse.exe (2772) taskse.exe C:\Users\ADMIN\AppData\Local\Temp\@WanaDecryptor@.exe
- @WanaDecryptor@.exe (2932) @WanaDecryptor@.exe
- taskdl.exe (2952) taskdl.exe
- taskse.exe (2340) taskse.exe C:\Users\ADMIN\AppData\Local\Temp\@WanaDecryptor@.exe
- @WanaDecryptor@.exe (2684) @WanaDecryptor@.exe
- taskse.exe (2012) taskse.exe C:\Users\ADMIN\AppData\Local\Temp\@WanaDecryptor@.exe
- ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe (3080) "C:\Users\ADMIN\AppData\Local\Temp\ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
  - attrib.exe (3388) attrib +h .

Figure 12: Process tree

Figure13: Tasks performed by Wannacry.exe on execution

Static Analysis:

Version Infos	
LegalCopyright	\xa9 Microsoft Corporation. All rights reserved.
InternalName	diskpart.exe
FileVersion	6.1.7601.17514 (win7sp1_rtm.101119-1850)
CompanyName	Microsoft Corporation
ProductName	Microsoft\xae Windows\xae Operating System
ProductVersion	6.1.7601.17514
FileDescription	DiskPart
OriginalFilename	diskpart.exe
Translation	0x0409 0x04b0

Figure14: Wannacry.exe info

Sections

Name	Virtual Address	Virtual Size	Size of Raw Data	Entropy
.text	0x00001000	0x000069b0	0x00007000	6.4042351061
.rdata	0x00008000	0x00005f70	0x00006000	6.66357096841
.data	0x0000e000	0x00001958	0x00002000	4.45574950787
.rsrc	0x00010000	0x00349fa0	0x0034a000	7.9998679751

Figure15: Sections

Imports

Library KERNEL32.dll:
- 0x40802c GetFileAttributesW
- 0x408030 GetFileSizeEx
- 0x408034 CreateFileA
- 0x408038 InitializeCriticalSection
- 0x40803c DeleteCriticalSection
- 0x408040 ReadFile
- 0x408044 GetFileSize
- 0x408048 WriteFile
- 0x40804c LeaveCriticalSection
- 0x408050 EnterCriticalSection
- 0x408054 SetFileAttributesW
- 0x408058 SetCurrentDirectoryW
- 0x40805c CreateDirectoryW
- 0x408060 GetTempPathW

Library USER32.dll:
- 0x4081d0 wsprintfA

Library ADVAPI32.dll:
- 0x408000 CreateServiceA
- 0x408004 OpenServiceA
- 0x408008 StartServiceA
- 0x40800c CloseServiceHandle
- 0x408010 CryptReleaseContext
- 0x408014 RegCreateKeyW
- 0x408018 RegSetValueExA
- 0x40801c RegQueryValueExA
- 0x408020 RegCloseKey
- 0x408024 OpenSCManagerA

Library MSVCRT.dll:
- 0x408108 realloc
- 0x40810c fclose
- 0x408110 fwrite
- 0x408114 fread
- 0x408118 fopen
- 0x40811c sprintf
- 0x408120 rand
- 0x408124 srand
- 0x408128 strcpy
- 0x40812c memset
- 0x408130 strlen
- 0x408134 wcscat
- 0x408138 wcslen
- 0x40813c __CxxFrameHandler
- 0x408140 ??3@YAXPAX@Z
- 0x408144 memcmp
- 0x408148 _except_handler3
- 0x40814c _local_unwind2
- 0x408150 wcsrchr
- 0x408154 swprintf

Figure16: Import functions

V. CONCLUSION

In this paper we presented the forensic analysis of ransomware infected windows system along with the forensic analysis of memory dumps and analysis of ransomware in a sandbox environment- Static & Dynamic Analysis. As the system is infected with Wannacry ransomware, data loss occurs as the ransomware encrypts the user data. With the help of this approach we were able to recover the encrypted data using forensic tool such as autopsy from infected system. Also, we performed memory dump analysis of the infected system. The traces of the malware were found in the memory dump which more effective technique for detecting malicious activity.Compared to static analysis, this method provides more features and artifacts for analysis because the dump is obtained after the real execution of the malware. Also, the Static and dynamic analysis performed in cuckoo sandbox environment helps us in understanding the actual behaviour of the Wannacry ransomware. Cuckoo sandbox provides integration with other tools such as Volatility, Yara, Virustotal, and Wireshark and provides an opportunity for better testing. Hence, by following digital forensic procedure and malware analysis techniques we were able to provide effective and more reliable results.

REFERENCES

[1] https://searchsecurity.techtarget.com/definition/malware

[2] Gursimran kaur,"Exploring the Malware Analysis Landscape for Forensic Investigation",2012

[3] https://github.com/fabrimagic72/malware-samples

[4] https://www.howtoforge.com/tutorial/how-to-install-and-use-volatility-memory-forensic-tool/

[5] Irfan Shakeel, " Computer Forensics: Overview Of Malware Forensic",2017

[6] J. Aquilina and C. Malin, "Malware Forensics_ Investigating and Analyzing Malicious Code-Syngress",2008

[7] Automated Malware Analysis - Cuckoo Sandbox. https://cuckoosandbox.org/

[8] https://www.fireeye.com/blog/threat-research/2017/05/wannacry-malware-profile.html