ISSN 2278-3091

Volume 9, No.1, January – February 2020

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse03912020.pdf

https://doi.org/10.30534/ijatcse/2020/03912020

Automated Collection of Artifacts from a Live Windows System using e-Triage Tool

Sri Parvathi Kota[1], Vijaya Sri Kompalli[2]

[1]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India, kotasriparvathi@gmail.com

[2]Associate Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India, kompallivsri@gmail.com

ABSTRACT

The evolution of computers and technology is outpacing the effectiveness of forensic techniques. In traditional computer forensic methodology, when an organization is effected by a cyber-attack, the systems were plugged off at the scene which results in loss of acquiring volatile memory and further seized media are analyzed at forensic laboratories to get report. In the current work, a novel e-Triage tool is developed which extracts artifacts present within a defined live windows system. It yields on-site identification and interpretation of digital evidences in a short period of time. The e-Triage tool follows live forensic methodology and facilitates to extract and collect artifacts related to system information, registry, events and network information, Random Access Memory, browsing history, shell bag, page file, hibernation file, swap file and also records the changes done by tool on registry whose novelty improves the forensic report. The current proposed e-Triage tool carries out prioritizing and collecting artifacts in preliminary investigation until a potential source is being identified and from then it accelerates further investigation.

Key words : artifacts, cyber-attack, digital evidence, live forensics, traditional forensics.

1. INTRODUCTION

Any aspect that has potential to jeopardize the confidentiality, availability and integrity of an information system and which violates or even compromises the security policies and procedures of an organization is considered as an incident. As cyber-attacks are increasing significantly in present technologically evolving world, the lack of skilled digital forensic investigators and efficient tools are at scarce.

The goal of digital forensics is to conserve evidence in its authentic form while achieving a deliberate investigation by collecting, identifying and validating the evidence for the purpose of rejuvenate previous events[4].

Forensics now-a-days are enforcing its impact and need in many diverse areas like software affected during natural disasters [14], cloud applications where the third party storage kind of works related [16], medicine [17][19] and other diverse application areas[15][18][19][20].

Forensic can be performed by following two approaches. Traditional or dead forensics and live forensics approach.

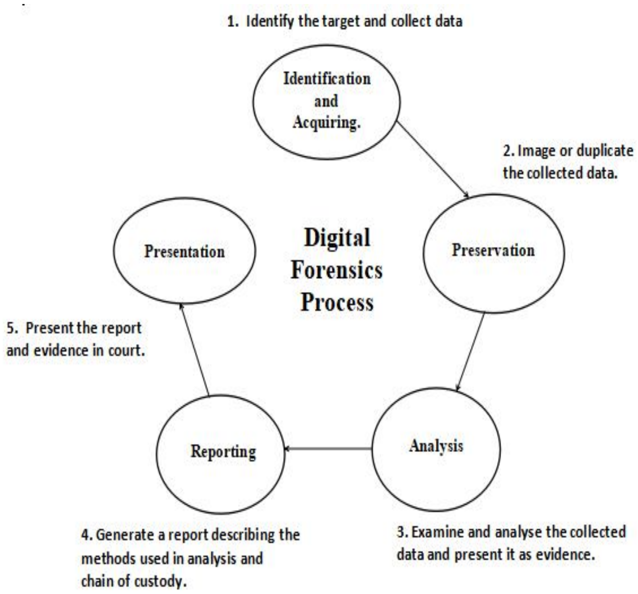

1. Identify the target and collect data
Identification and Acquiring.
2. Image or duplicate the collected data.
Preservation
Digital Forensics Process
Presentation
5. Present the report and evidence in court.
Reporting
Analysis
4. Generate a report describing the methods used in analysis and chain of custody.
3. Examine and analyse the collected data and present it as evidence.

Figure 1: Digital forensic process.

Dead Forensics is a process in which forensic investigator approach the system and checks the power status. If the system is powered on then the investigator shut downs or pulls out the plug and copies the hard disk data. Sometimes s/he bag the entire system as evidence and analyzes the data in laboratories. [6]

Live Forensics is a process in which the investigator conducts forensics on powered on systems. It provides access to collect more artifacts from RAM and running processes in the system. [5]

Live forensics follows 3 main principles. They are:

- Acquire the digital data from the system without modification.
- Authenticate the recovered data.
- Analyze the data while maintaining its integrity.

While conducting forensic investigation, the investigators face challenges in prioritizing the collection of artifacts and also due of lack of technical experience they fail to investigate the evidence at the crime scene. The proposed tool automates the artifacts collection process and helps the investigator to spot and prioritize systems with the potential supply of evidence.

2. LITERATURE SURVEY

The purpose of this survey is to identify and analyse the techniques and approaches used in performing investigation on live windows systems.

Table 1: Literature Survey

S.No	*Author(s), Year*	*Reference*	*Description*	*Technique Used*
1	SWARNA PUJITHAKOLLI, 2019.	[4]	The author proposed an automated tool designed to perform live volatile memory analysis to resolve the difficulty in acquisition and analysis process.	Volatility and Sleuth kit Plugins.
2	VACIUS JUSAS, ELVAR GAHRAMANOV, DARIUS BIRVINKAS, 2017.	[1]	The discussion about different triage models and tools. The authors identified some common defects in tools that include lack of extracting browser artifacts and the accountability of registry changes done by too on examination system.	Cyber Forensic Field Process Model and DC3, GRR tools
3	NISARG TRIVEDI, 2014.	[9]	Nisarg Trivedi represented different tools to acquire pagefile.sys from a system and how to analyse it.	Linux Reader Software, HxD Software.
4	VINCENT LO, 2014.	[7]	Vincent lo identified the shellbag structure and location of shellbag in different windows OS. He also explained the importance of shellbag information in forensic investigation.	Registry Editor.
5	MARUS K. ROGERS, 2014.	[3]	Marus k. Rogers proposed a triage model to identify digital evidence in short period of time.	Computer Forensics Field Triage Process Model.
6	RAIHANA MD SAIDI, SITI ARPAH AHMAD, NORHAYATI MOHAMED NOOR, 2013.	[12]	This paper exhibit the grandness of registry analysis by performing forensic investigation and detecting the illegal activities of a key logger.	FTK image, Windows Registry File Viewer

S.No	***Author(s), Year***	***Reference***	***Description***	***Technique Used***
7	CHRISTOPHER HARGREAVES AND JONATHAN PATTERSON, 2012.	[13]	By using the pattern matching technique, the author automatically constructed a high level timeline. The author has also stressed that this method should not be intended as full forensic analysis.	Utilised log2timeline features.
8	JUNGHOON OH, SEUNGBONG LEE, 2011.	[10]	The authors shown how browser records are stored in different windows operating systems. They also provided study on different tools used for web browser artifact analysis.	Web Browser Forensic Analyzer Tool
9	MARTHIE LESSING, 2008.	[6]	Author has presented the key differences between live and dead forensic acquisition process. She explained how to ensure evidence's forensic soundness.	Live and Dead Forensic approaches.

3. ARCHITECTURE

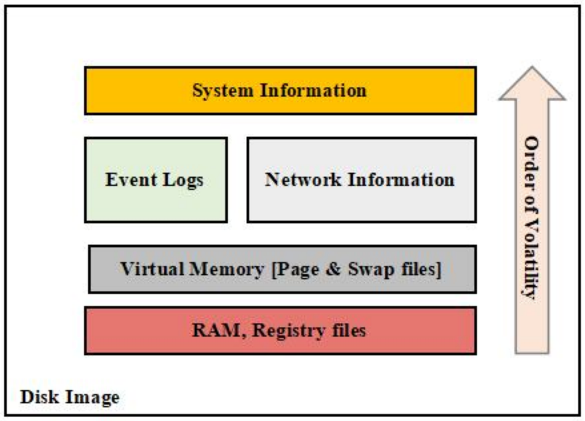


Figure 2: Architecture of tool

The investigator need to capture data that is most volatile in nature. S/he may comply the order of volatility. It defines which data must be collected first.

Registry is a jackpot of evidence. IT stores configuration information of all users, software and hardware present in the system. Registry has the tendency to change. Thus on execution, the e-Triage tool automatically collects the data of default, system, software, SAM and security hives.

Network information enables to collect artifacts like IP configuration, ARP Data, sessions and shared files within a network. On selecting the specific options, the e-Triage tool collects and stores the details in evidence folder.

Memory is another aspect with high priority in the order of volatility. RAM is a temporary memory which is lost on system power off state.

Virtual Memory is a capacity allotment scheme in which auxiliary memory can be tended to just as it were a piece of main memory. The memory framework uses to recognize physical storage sites, and program produced addresses are made an interpretation of the related machine addresses.

Pagefile.sys or the Page File is the PC paging document that your Windows utilizes as Virtual memory. PageFile.sys holds objects in an over-utilized memory that has not been gotten to for a significant stretch of time. At the point when Windows comes up short on physical memory, it resorts to utilizing the Page File, writing a few contents of RAM on the disk.

The Swap file holds objects which have been launched out from memory and are not expected to be gotten to quite a while and enables a framework to employ disk space to re-enact additional memory at whatever point the framework comes up short on memory, by swapping segment of RAM that an inactive program is utilizing onto the hard disk to free up the memory for different projects.

Every action triggers an event in the windows system. The application, system and security windows logs are extracted. They provide a detailed information on significant events in the system.

Device information collects system information, running services, process and account settings of the device. Along with device information and archive media are considered as the least volatile data in the order of volatility.

4. WORKFLOW OF TOOL

The first step is to make a prior planning. Consider the potential legal issues. Make sure that the warrant supports to seize the systems or allows to conduct on site examination. The responder or the investigator should have access to admin privileges of systems from the organization or the admin should be with the responder throughout the collection process. Technical operations are conducted after fulfilling the planning. Assess the situation and decide the effective method to complete the process.

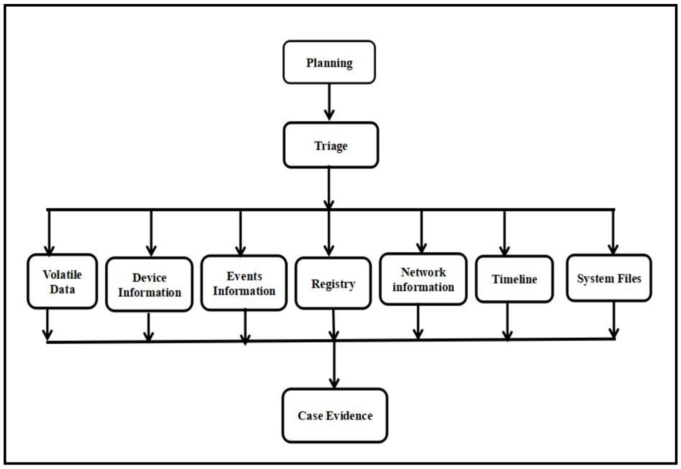


Figure 3: Tool work flow

Copy e-Triage tool into a clean USB drive or any external drive with high storage capacity. Execute the tool in host system. Select features based on the reported incident. The result will be automatically stored in a single folder in tool running device. Further in-depth analysis is performed based on the acquired evidence folder.

e-Triage tool also supports imaging the windows system. Imaging is a process to capture the entire disk data which can be mounted on examiner system to conduct further in-depth examination and analysis of evidence. This feature is only used when the system does not support the live forensics.

In e-Triage, hashing of files is used to maintain the integrity of collected evidence. Md5 and SHA-1 hashes of every file in the collected evidence folder is extracted and saved in the evidence folder itself.

5. RESULTS

Experimentation is carried out in virtual machine on windows 10x64 bit operating system with 8GB RAM capacity. Data theft using external drive scenario is created and artifacts are collected from the system.

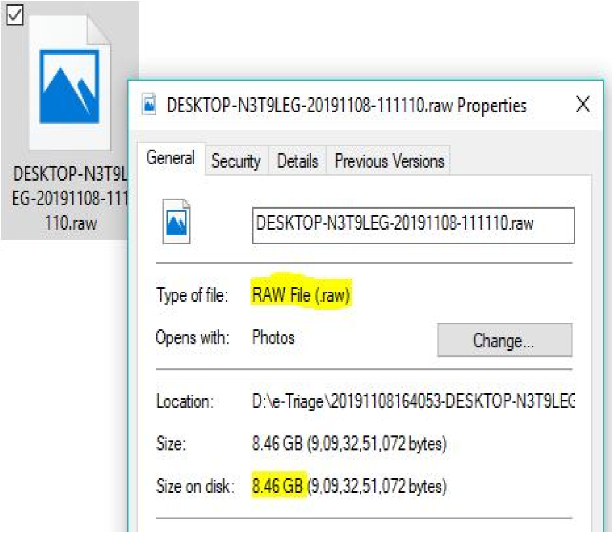
The e-triage tool collects the device related artifacts like system information, version number, build type, owner name. It captures the running process and services information.

It collects windows event logs especially Application, system and software logs. Inclusion of every result screenshot is hectic so only few artifacts result are included in the paper. Collecting the following artifacts strengthened the investigation process.

1. Memory dump
2. Registry hives
3. Browser history
4. USB Artifacts
5. Shell Bag
6. MFT Timeline

1. Memory dump:

The RAM is collected in .raw format. It helps in conducting memory analysis. Malicious process activities, saved passwords, console data can be identified from memory dump.



DESKTOP-N3T9LEG-20191108-111110.raw Properties

DESKTOP-N3T9LEG-20191108-111110.raw

Type of file: RAW File (.raw)

Opens with: Photos

Location: D:\e-Triage\20191108164053-DESKTOP-N3T9LEG

Size: 8.46 GB (9,09,32,51,072 bytes)

Size on disk: 8.46 GB (9,09,32,51,072 bytes)

Screenshot 1: Captured memory properties.

2. Registry:

The windows registry stores settings information and configurations of operating system, hardware devices, user preferences and software programs.

'%SYSTEMROOT%\System32\Config\' folder holds the registry files in windows. The registry hives contains keys which holds the registry values.

The following registry hives are collected:

HKLM\SYSTEM,

HKLM\SECURITY,

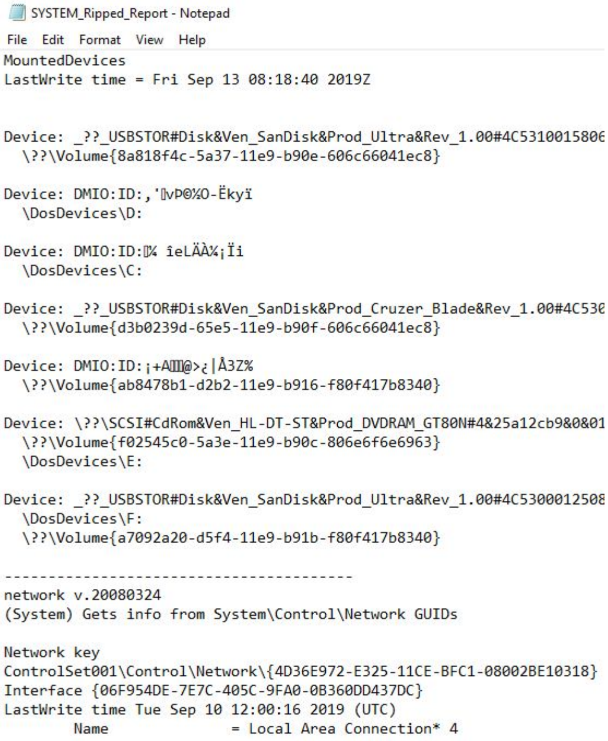
HKLM\SAM,

HKLM\SOFTWARE,

HKCU and

HKU\.DEFAULT.

Regripper plugin is used to parse the collected registry data into a legible format.

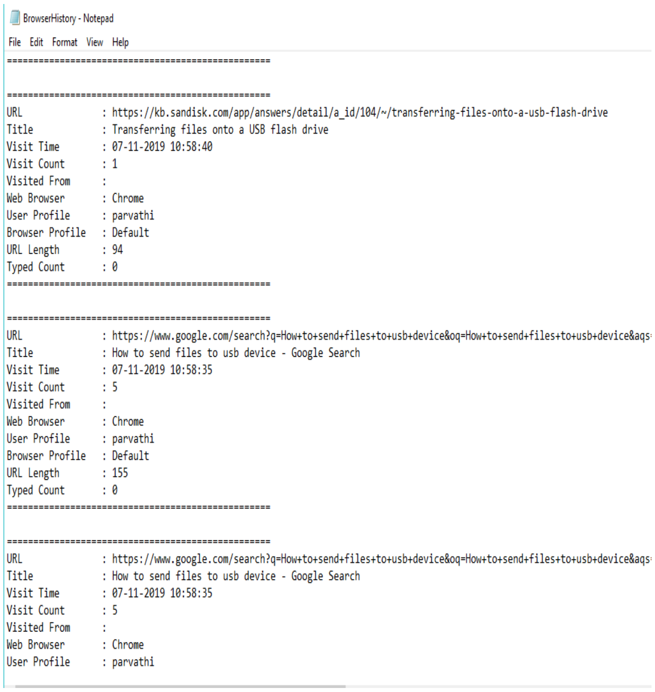


```
MountedDevices
LastWrite time = Fri Sep 13 08:18:40 2019Z


Device: _??_USBSTOR#Disk&Ven_SanDisk&Prod_Ultra&Rev_1.00#4C531001580€
  \??\Volume{8a818f4c-5a37-11e9-b90e-606c66041ec8}

Device: DMIO:ID:,'▯vÞ©½O-Ëkyï
  \DosDevices\D:

Device: DMIO:ID:▯¼ îeLÄÀ¼¡Ïi
  \DosDevices\C:

Device: _??_USBSTOR#Disk&Ven_SanDisk&Prod_Cruzer_Blade&Rev_1.00#4C53€
  \??\Volume{d3b0239d-65e5-11e9-b90f-606c66041ec8}

Device: DMIO:ID:¡+A▯▯@>¿|Å3Z%
  \??\Volume{ab8478b1-d2b2-11e9-b916-f80f417b8340}

Device: \??\SCSI#CdRom&Ven_HL-DT-ST&Prod_DVDRAM_GT80N#4&25a12cb9&0&01
  \??\Volume{f02545c0-5a3e-11e9-b90c-806e6f6e6963}
  \DosDevices\E:

Device: _??_USBSTOR#Disk&Ven_SanDisk&Prod_Ultra&Rev_1.00#4C530001250€
  \DosDevices\F:
  \??\Volume{a7092a20-d5f4-11e9-b91b-f80f417b8340}

----------------------------------------
network v.20080324
(System) Gets info from System\Control\Network GUIDs

Network key
ControlSet001\Control\Network\{4D36E972-E325-11CE-BFC1-08002BE10318}
Interface {06F954DE-7E7C-405C-9FA0-0B360DD437DC}
LastWrite time Tue Sep 10 12:00:16 2019 (UTC)
        Name                = Local Area Connection* 4
```

Screenshot 2: HKLM\SYSTEM Report

3. *Browser history:*

Users depend on web browsers to carry on their internet activities. e-Triage tool collects all users history of Google, opera, safari , Mozilla and internet explorer web browsers. The visited URLs , visited time and visited count of all users in the system is extracted and parsed into human readable format.



```
==================================================


==================================================
URL             : https://kb.sandisk.com/app/answers/detail/a_id/104/~/transferring-files-onto-a-usb-flash-drive
Title           : Transferring files onto a USB flash drive
Visit Time      : 07-11-2019 10:58:40
Visit Count     : 1
Visited From    :
Web Browser     : Chrome
User Profile    : parvathi
Browser Profile : Default
URL Length      : 94
Typed Count     : 0
==================================================


==================================================
URL             : https://www.google.com/search?q=How+to+send+files+to+usb+device&oq=How+to+send+files+to+usb+device&aqs
Title           : How to send files to usb device - Google Search
Visit Time      : 07-11-2019 10:58:35
Visit Count     : 5
Visited From    :
Web Browser     : Chrome
User Profile    : parvathi
Browser Profile : Default
URL Length      : 155
Typed Count     : 0
==================================================


==================================================
URL             : https://www.google.com/search?q=How+to+send+files+to+usb+device&oq=How+to+send+files+to+usb+device&aqs
Title           : How to send files to usb device - Google Search
Visit Time      : 07-11-2019 10:58:35
Visit Count     : 5
Visited From    :
Web Browser     : Chrome
User Profile    : parvathi
```

Screenshot 3: Browser Activity

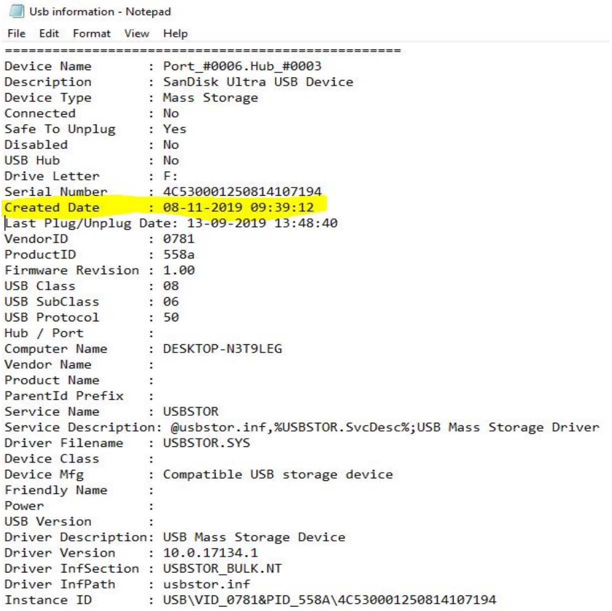
4. *USB Artifacts:*

Whenever a USB device is connected or removed to/from the system, it leaves traces in the system. The USB information extracted from the system includes device name, vendor, product number, serial number, computer name.

Artifacts Location:

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrenControlSet\Services\USBSTOR

C:\Windows\system32\drivers\USBSTOR.SYS



```
==================================================
Device Name        : Port_#0006.Hub_#0003
Description        : SanDisk Ultra USB Device
Device Type        : Mass Storage
Connected          : No
Safe To Unplug     : Yes
Disabled           : No
USB Hub            : No
Drive Letter       : F:
Serial Number      : 4C530001250814107194
Created Date       : 08-11-2019 09:39:12
Last Plug/Unplug Date: 13-09-2019 13:48:40
VendorID           : 0781
ProductID          : 558a
Firmware Revision  : 1.00
USB Class          : 08
USB SubClass       : 06
USB Protocol       : 50
Hub / Port         :
Computer Name      : DESKTOP-N3T9LEG
Vendor Name        :
Product Name       :
ParentId Prefix    :
Service Name       : USBSTOR
Service Description: @usbstor.inf,%USBSTOR.SvcDesc%;USB Mass Storage Driver
Driver Filename    : USBSTOR.SYS
Device Class       :
Device Mfg         : Compatible USB storage device
Friendly Name      :
Power              :
USB Version        :
Driver Description: USB Mass Storage Device
Driver Version     : 10.0.17134.1
Driver InfSection  : USBSTOR_BULK.NT
Driver InfPath     : usbstor.inf
Instance ID        : USB\VID_0781&PID_558A\4C530001250814107194
```

Screenshot 4: USB Device information

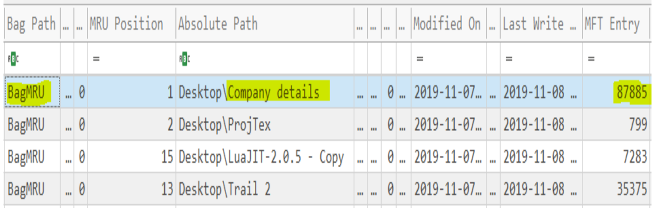
5. Shell Bag:

Shell bags are registry keys which store meta data of folders which were accessed through the file explorer. It also stores data about folders accessed through external drives and remote systems[7]. Timeline explorer is used to get a better view of output CVS file.

Artifacts collected from the below locations.

Computer\HKEY_USERS\{User-SID}\Software\Microsoft\Windows\Shell\Bags

Computer\HKEY_USERS\{User-SID}\Software\Microsoft\Windows\Shell\BagMRU

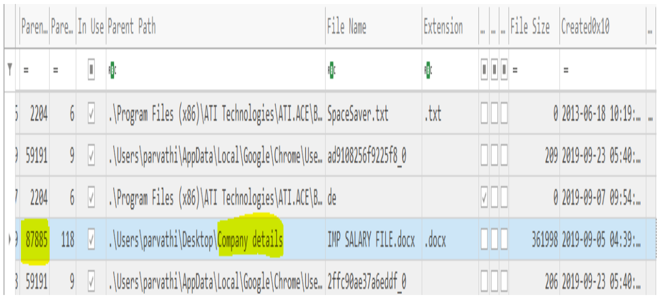


Bag Path	…	…	MRU Position	Absolute Path	…	…	…	…	Modified On	…	Last Write …	MFT Entry
BagMRU	…	0	1	Desktop\Company details	…	…	0	…	2019-11-07…	…	2019-11-08 …	87885
BagMRU	…	0	2	Desktop\ProjTex	…	…	0	…	2019-11-07…	…	2019-11-08 …	799
BagMRU	…	0	15	Desktop\LuaJIT-2.0.5 - Copy	…	…	0	…	2019-11-07…	…	2019-11-08 …	7283
BagMRU	…	0	13	Desktop\Trail 2	…	…	0	…	2019-11-07…	…	2019-11-08 …	35375

Screenshot 5: Shell bags data

6. MFT Timeline:

MFT is a vital file in NTFS file system. It records the meta data of all files present in the windows. It records the MACB time of a file. For effective incident response and forensics, organizing the collected pieces of information in a chronological manner avoids wasting of investigator's time. This feature helps to identify what events are occurred after or before specific time. The activity is extracted, sorted based on time and saved in a CSV file.



	Paren…	Pare…	In Use	Parent Path	File Name	Extension	…	…	…	File Size	Created0x10	…
5	2204	6	☑	.\Program Files (x86)\ATI Technologies\ATI.ACE\B…	SpaceSaver.txt	.txt	□	□	□	0	2013-06-18 10:19:…	…
9	59191	9	☑	.\Users\parvathi\AppData\Local\Google\Chrome\Use…	ad9108256f9225f8_0		□	□	□	209	2019-09-23 05:40:…	
7	2204	6	☑	.\Program Files (x86)\ATI Technologies\ATI.ACE\B…	de		☑	□	□	0	2019-09-07 09:54:…	
9	87885	118	☑	.\Users\parvathi\Desktop\Company details	IMP SALARY FILE.docx	.docx	□	□	□	361998	2019-09-05 04:39:…	
3	59191	9	☑	.\Users\parvathi\AppData\Local\Google\Chrome\Use…	2ffc90ae37a6eddf_0		□	□	□	206	2019-09-23 05:40:…	

Screenshot 6: MFT Timeline.

Benefits of e-Triage tool.

i. Reduces the time of data extraction.

ii. Anyone with minimum computer knowledge and forensics can utilize the tool.

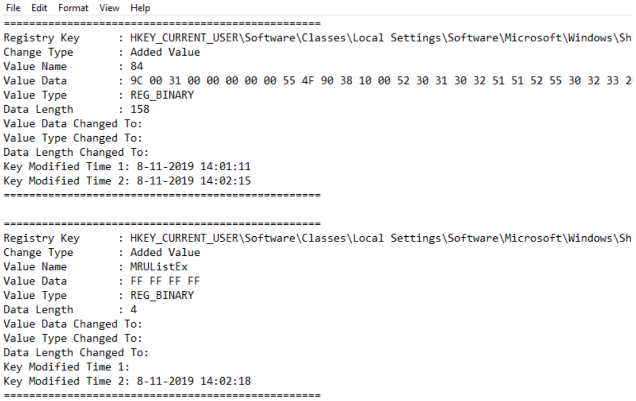
iii. Records all registry modifications.

iv. Generates hashes of evidence to maintain integrity.

v. It supports various windows versions XP, vista, 7, 8 and 10.

To ensure that the collected artifacts are not tampered and are pertinent in the court, the proposed automated tool guarantees the trustworthiness by saving the hashes of gathered data and furthermore by safeguarding the digitalized chain of custody.

Whenever a new software is executed in the system, It does changes to the system hard disk and registry. The proposed tool does not require installation setup in the host system. To maintain accountability, the tool records all the changes done to the registry.



```
==================================================
Registry Key       : HKEY_CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\Windows\Sh
Change Type        : Added Value
Value Name         : 84
Value Data         : 9C 00 31 00 00 00 00 00 55 4F 90 38 10 00 52 30 31 30 32 51 51 52 55 30 32 33 2
Value Type         : REG_BINARY
Data Length        : 158
Value Data Changed To:
Value Type Changed To:
Data Length Changed To:
Key Modified Time 1: 8-11-2019 14:01:11
Key Modified Time 2: 8-11-2019 14:02:15
==================================================

==================================================
Registry Key       : HKEY_CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\Windows\Sh
Change Type        : Added Value
Value Name         : MRUListEx
Value Data         : FF FF FF FF
Value Type         : REG_BINARY
Data Length        : 4
Value Data Changed To:
Value Type Changed To:
Data Length Changed To:
Key Modified Time 1:
Key Modified Time 2: 8-11-2019 14:02:18
==================================================
```

Screenshot 7: Registry changes

6. CONCLUSION

In traditional digital forensics, when an incident occurred in the organization, the investigator identifies the incident and conducts analysis in order to find the root cause of attack. As digital forensics and cyber-attacks are propagating rapidly, live monitoring and analysis is required to identify and mitigate the incident. This paper aims to present an automated tool which gathers artifacts from the windows system in short frame of time.

REFERENCES

1. Vacius Jusas, Darius Birvinskas, and Elvar Gahramanov, "Methods and Tools of Digital Triage in Forensic Context: Survey and Future Directions", Symmetry 2017, 9, 49; doi: 10.3390/sym9040049.
2. Todd G. Shipley, Henry R. Reeve, "Collecting Evidence from a Running Computer: A Technical and Legal Primer for the Justice Community", Report Prepared by SEARCH, The National Consortium For Justice Information and Statistics.
3. Marcus K. Rogers, James Goldman, Rick Mislan, Timothy Wedge and Steve Debrota, "Computer Forensics Field Triage Process Model", Journal of Digital Forensics, Security and Law, Vol 1(2).
4. Swarna Poojitha Kolli, K.V.D.Kiran, 'An Automated Evaluation of Live Forensic Approach', International Journal of Engineering and Advanced Technology, ISSN:2249-8958, Volume-8, Issue-3S, February 2019.

5. Mahesh Kolhe, Purnima Ahirao, "Live Vs Dead Computer Forensic Image Acquisition",International Journal of Computer Science and Information Technologies, ISSN:0975-9646, Vol.8(3),2017.
6. Marthie Lessing, basie von Solms, "Live Forensic Acquisition as Alternative to Traditional Forensic Processes", Researchgate, september 2008.
7. Vincent Lo, "Windows ShellBag Forensics in Depth", SANS Institute Information Security Reading Room, 2014.
8. Rincy Roy Oommen, Princy Sugathan, "Recovering Deleted Files from NTFS", International Journal of Science and Research, ISSN:2319-7064.
9. Nisarg Trivedi, "Study on Pagefile.sys in Windows System", IOSR Journal of Computer Engineering, e-ISSN:2278-0661, Vol.16(2). https://doi.org/10.9790/0661-16251116
10. Junghoon Oh, Seungbong Lee and Sangjin Lee, "Advanced Evidence Collection and Analysis of Web Browser Activity", Digiital Investigation 8 (2011), S62-S70. https://doi.org/10.1016/j.diin.2011.05.008
11. Erhan Akbal, Fatma Gunes, Ayhan Akbal, "Digital Forensic Analysis of Web Browser Records", Journal of software, doi: 10.17706/jsw.11.7.631-637.
12. Raihana Md Saidi, Siti Arpah Ahmad, Norhayati Mohamed Noor, Rozita Yunos, "Windows Registry Analysis for Forensic Investigation", ISBN:978-1-4673-5613-8.
13. Christopher Hargreaves and Jonathan Patterson, "An Automated Timeline Reconstruction Approach for digital Forensic Investigations", Digital Investigation 9(2012), S69-S79. https://doi.org/10.1016/j.diin.2012.05.006
14. Kavitha, M., Manideep, Y., Vamsi Krishna, M., & Prabhuram. "Speech controlled home mechanization framework using android gadgets". International Journal of Engineering and Technology, 2018, 655-659.
15. Syed.Karimunnisa, Dr.Vijaya Sri Kompalli, "Cloud Computing: Review on Recent Research Progress and Issues", International Journal of Advanced Trends in Computer Science and Engineering, Vol 8, March-April 2019, ISSN 2278-3091. https://doi.org/10.30534/ijatcse/2019/18822019
16. Vijaya Sri Kompalli, K. Usha Rani, "Clusters of Genetic-based Attributes Selection of Cancer Data", Procedia Computer Science, 2016, Volume 89, Pages 534-539.
17. Kavitha, M., et al. "Wireless Sensor Enabled Breast Self-Examination Assistance to Detect Abnormality." International Conference on Computer, Information and Telecommunication Systems, IEEE, 2018.
18. Kompalli V.S., Kuruba U.R. "Combined Effect of Soft Computing Methods in Classification". Proceedings of the First International Conference on Computational Intelligence and Informatics. Advances in Intelligent Systems and Computing, vol 507, 2017. Springer. https://doi.org/10.1007/978-981-10-2471-9_49
19. Kavitha, Modepalli, P. Venkata Krishna, and V. Saritha. "Role of Imaging Modality in Premature Detection of Bosom Irregularity." Internet of Things and Personalized Healthcare Systems. Springer, Singapore, 2019, 81-92.
20. Ahmed Amer, Normaziah A. Aziz, "Malware Detection through Machine Learning Techniques", International Journal of Advanced Trends in Computer Science and Engineering, September- October 2016, 2408-2413. https://doi.org/10.30534/ijatcse/2019/82852019
21. Koduru Prasada Rao, Dr G Lavanya Devi, "Information Security Using Hilbert With Hash Value", International Journal of Advanced Trends in Computer Science and Engineering, September-October 2019, 2507-2511. https://doi.org/10.30534/ijatcse/2019/96852019