Comprehensive Analysis and Forensic Recovery of Vipasana Ransomware

Francis Byabazaire^{1*}, Parag H. Rughani²

¹Institue of Forensic Science, Gujarat Forensic Sciences University, Gandhinagar, India ²Institue of Forensic Science, Gujarat Forensic Sciences University, Gandhinagar, India

*Corresponding Author: frankb0178@gmail.com

Available online at: www.ijcseonline.org

Received: 16/Mar/2018, Revised: 24/Mar/2018, Accepted: 18/Apr/2018, Published: 30/Apr/2018

Abstract— Ransomware is a malware that either encrypts files with specific extension on the system or locks the user out of the system demanding for the ransom in exchange of decryption key. The approach used here is to assess numerous aspects of ransomware so as to comprehend different techniques utilized by it. Ransomware has rapidly affected individuals, public and private organizations across the globe. This occurs due to system flaws and lack of recovery mechanisms. The challenging part is to recover vital data from the encrypted files. This has created severe security issues to companies of all sizes as several have lost valuable data and business proprietary information. Considering the above information, this research paper aims at examining the characteristics of a Microsoft Windows-based ransomware and potential recovery of encrypted files from the ransomware affected system. The sample was examined in an isolated environment using static and dynamic analysis techniques with open source tools. The results were encouraging as we were able to recover encrypted files with specific extensions.

Keywords— Vipasana Ransomware, Ransomware Forensics, Ransomware Analysis, Offline Ransomware, Static Analysis, Dynamic Analysis.

I. INTRODUCTION

Ransomware is one of the widest spread and damaging cyber threats faced by the world today. Different types of malware were designed to achieve different objectives such as disruption, modification, data theft, deletion of files or services and terrorist attacks. In all these cases, malware writers' goal is to receive a reward in form of financial benefits or money in different forms like digital currency. Ransomware is not a new type of malware, it has been around for more than two decades, but during the last 3 years, there has been a huge increase of infections which targeted almost every system it could reach and compromise.

According to statistics, more than 140 million new malware samples were discovered in 2015 and a large portion was ransomware. Many new ransomware variants emerged in first quarter of 2017 as represented in the graph (Fig 1).

The study aims at analyzing Vipasana, the well-known Windows based Ransomware. An attempt had been made to ensemble integrative analysis of ransomware variants functionality. This research work contributes to recovery of user encrypted files using forensic methods and tools without paying the ransom to cyber criminals.

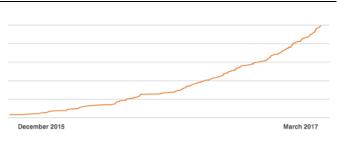


Figure 1: Growth in ransomware variants since Dec'15-Mar'17 Source: https://blog.barkly.com/ransomware-statistics-2017

This research paper aims at analysing one of the known Windows based ransomware namely Vipasana. The work carried out during the study is aimed at providing a detailed analysis of the functioning of the sample - a variant of a ransomware. This research contributes to the society by helping forensic investigators to recover important user data encrypted by Vipasana ransomware.

II. RELATED WORK

This section deals with the work carried out by researchers on different aspects of malware forensics.

The extent of the damage caused by ransomware attack is in high range at present. It is suggested that ransomware and

Vol.6(4), Apr 2018, E-ISSN: 2347-2693

similar cyber-criminal activities affect end users for digital extortion at a scale never seen before [1].

As reported by Ali et al. American Bankers Association estimated \$18 million loss to ransomware attacks for individuals and businesses and Cyber Threat Alliance reported that, 7.1 million attempted infections spread across the globe between 2015 to June 2016. The peak of one day of ransomware hit reached 228,496 [2].

Noted that the number of ransomware attacks were doubled in the past twelve months compared to a year earlier and predicted that it will double again the following year. The author explained that ransomware is precise in selecting targets. For example, they select florist shops before Valentine's Day because they know the heavy traffic these shops experience in that period forces them to pay the ransom [3].

Kharraz et al. conducted a study noting that ransomware attacks increased by 500% in 2013 compared to the 2012. It further gsuggested that this malware infected around 250,000 computers including a police department that ended paying a ransom to decrypt their computers and return their data [4].

Literature reports related to ransomware forensics are discussed as they worked on ransomware detection techniques and proposed some mechanisms to detect the presence of ransomware [5-8]. The work on the comparative analysis of various ransomware variants has been carried out [9-11]. As wannacry created havoc recently, substantial work is published about it by various authors [12, 13]. On the other hand, different authors worked on different ransomware variants such as cryptowall, locky, IoT based ransomware and Manamecrypt [14-17]. There is minimal research on ransomware forensics though plenty of data is published on different aspects of malware forensics [18-20].

Despite tremendous progress in research on other variants of Ransomware, the work done on Vipasana ransomware has been dealt marginally. Owing to higher rate of damage caused by Vipasana in present scenario, it might hamper the economy. Therefore the present work was conducted to elucidate the recovery of user data affected by Vipasana ransomware.

III. METHODOLOGY

III.I. **TOOLS AND ENVIRONMENTAL SETUP**

A physical standalone machine running Windows 10 Operating System was set up as a target machine.

The target machine was isolated to prevent the sample from infecting the entire network. Static and dynamic analysis tools were installed for the analysis of the sample.

Few files with extensions .doc, .ppt, .jpg, .mp4, .pdf, .PNG, .txt, .xls, .zip were stored in the C drive of the target machine to analyze complete execution and satisfy core dependency of the sample.

PC > Local Disk (C:) > Test_Files > File.doc

Name	Date modified	Туре	Size
🔁 Assignment	1/17/2017 10:09 AM	Microsoft Word D	31 KE
Documentation	8/27/2017 6:07 AM	Microsoft Word D	4,316 KE
🗐 MAC Flooding	7/20/2017 2:20 AM	Microsoft Word D	17 KE
🖤 TA2	3/31/2017 11:13 AM	Microsoft Word D	11 KE

PC > Local Disk (C:) > Test_Files > File.jpg



Figure 3: jpg files

PC >	Local Disk	(C:) →	Test Files	>	File.pdf	
------	------------	--------	------------	---	----------	--

Name	Date modified	Туре	Size
🗾 Learning Pentesting for Android Devices	8/14/2017 10:28 AM	Adobe Acrobat D	14,517 KB
🗾 Learning-Android-Forensics	8/14/2017 10:28 AM	Adobe Acrobat D	13,783 KB
🗾 Network Forensics 2012	6/22/2017 11:41 AM	Adobe Acrobat D	20,281 KB
🔁 Packt.Mastering.Mobile.Forensics	8/14/2017 10:29 AM	Adobe Acrobat D	16,049 KB
🔁 Practical_Malware_Analysis	8/24/2017 1:07 AM	Adobe Acrobat D	9,426 KB

Figure 4: pdf files

PC > Local Disk (C:) > Test_Files > File.txt						
Name	Date modified	Туре	Size			
Game	1/18/2017 1:22 PM	Text Document	37 KB			
MD5	1/18/2017 5:01 PM	Text Document	1 KB			
pslist	1/18/2017 2:29 PM	Text Document	45 KB			

Figure 5: txt files

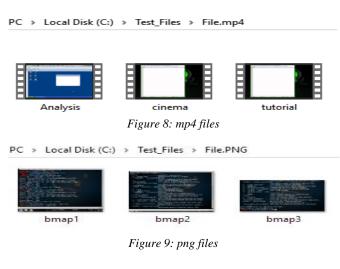
Name	Date modified	Туре	Size
🔊 Data	8/29/2017 5:42 PM	Microsoft Excel W	9 K
🔄 Items	8/29/2017 5:42 PM	Microsoft Excel W	9 K
Terms	8/29/2017 5:42 PM	Microsoft Excel W	9 k

Figure 6: xls files

PC > Local Disk (C:) > Test Files > File.ppt

Name	Date modified	Туре	Size
🖭 Francis	8/29/2017 6:13 AM	Microsoft PowerP	35 KB
🖳 LAND IN WORLD	8/29/2017 6:13 AM	Microsoft PowerP	35 KB
SKYPE	8/29/2017 6:13 AM	Microsoft PowerP	35 KB

Figure 7: ppt files



III.II. INFECTING THE TARGET MACHINE

- The sample was copied to the target machine using a pen drive.
- Zip file containing sample was extracted on the desktop of the target machine.
- Static analysis of the sample was done.
- Windows security features like Windows defender, Windows firewall were disabled.
- The sample was then run by right clicking on the executable file.
- The machine was infected by the sample; files encrypted and desktop wallpaper changed with the infection details.

IV. RESULTS AND DISCUSSION

This section consists of the summary and report on the findings. It includes results of the analysis of data, presentation of findings and summary with interpretations on findings in relation to the sample.

IV.I. STATIC ANALYSIS

1) FileAlyzer tool

Using FileAlyzer, brief details about the sample were obtained as shown below:

MD5	: 2AEA3B217E6A3D08EF684594192CAFC8
Size	: 379392 bytes
File Name	: 1.exe
File Type	: Portable Executable
Last Write	: Thursday, February 18, 2016 2:44:22 AM

Vol.6(4), Apr 2018, E-ISSN: 2347-2693

Proof of concept:

FileAlyzer 2.0.5.	57 - [C:\Users\WINDOWS_M	MALWARE	Desktop\	1]		
🗋 File Edit Wi	ndow Report Help					
🚹 🖌 🗅 🚺	280					
Disa	ssembler		Com	patibility		
General Hex	Anomalies OpenSBI	Мар	Bitmap	Streams	Security	Hashes
1						
Location:	C:\Users\WINDOWS_MAL\	WARE\Desk	top\			
Size: Version:	379392 000000000	005CA00				
CRC-32:	A3F98B0B					
<u>M</u> D5:	2AEA3B217E6A3D08EF684	1594192CA	-C8			
S <u>H</u> A-1:	3A0B855DD052B2CDC645	3F6CBDB85	8C7855762	280		
Read only	Directory					
System file	Symbolic link					
Creation:	Sunday, November 19, 20	17 3:45:24	PM	2017-1	1-19 15:45:2	4
Last access:	Sunday, November 19, 20	17 3:45:24	PM	2017-1	1-19 15:45:2	4
Last write:	Thursday, February 18, 20	16 1:14:22	AM	2016-02	2-18 01:14:2	2
Creation (UTC):	Sunday, November 19, 20	17 10:15:24	1 AM	2017-1	1-19 10:15:2	4
Last access (UTC):	Sunday, November 19, 20	17 10:15:24	1 AM	2017-1	1-19 10:15:2	4
Last write (UTC):	Wednesday, February 17,	2016 7.44	00.014	2045 01	2-17 19:44:2	-

Figure 10: FileAlyzer

2) Dependency walker tool

List of DLLs imported: Details of Dynamic Link Libraries from where the sample imported functions were discovered.

Proof of concept:					
Dependency Walker - [1]					
🔩 File Edit View Options Profile Window Help					
🖻 📕 🔎 🖹 斗 🖭 💭 🔐 🗒 関	18	II N?			
8- 0	PI	Ordinal ^	Hint	Function	Entry Point
È In the second sec		N/A	0 (0x0000)	ExitProcess	Not Bound
🗄 🔤 📲 🖬 USER32.DLL		N/A	0 (0x0000)	WriteFile	Not Bound
		N/A	0 (0x0000)	UnhandledExceptionFilter	Not Bound
H Q OLEAUT32.DLL		N/A	0 (0x0000)	SetFilePointer	Not Bound
🛐 🕯 KERNEL32.DLL		N/A	0 (0x0000)	SetEndOfFile	Not Bound
ADVAPI32.DLL		N/A	0 (0x0000)		Not Bound
		N/A	0 (0x0000)		Not Bound
		N/A		RaiseException	Not Bound
🗄 📲 GDI32.DLL		N/A		GetStdHandle	Not Bound
🚮 🛱 USER32.DLL		N/A	0 (0x0000)		Not Bound
🚮 KERNEL32.DLL		N/A		GetFileType	Not Bound
🚮 OLEAUT32.DLL		N/A	0 (0x0000)	CreateFileA	Not Bound
⊞ 🔤 SHELL32.DLL	<				
🗄 🔲 🛱 WININET.DLL	E	Ordinal ^	Hint	Function	Entry Point
	C	1 (0x0001)	0 (0x0000)	AcquireSRWLockExclusive	NTDLL.RtIA
	0	2 (0x0002)	1 (0x0001)	AcquireSRWLockShared	NTDLL.RtIA
		3 (0x0003)	2 (0x0002)	ActivateActCtx	0x0001EB

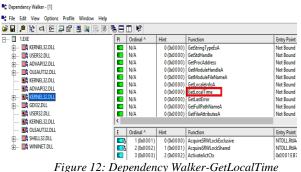
Figure 11: Dependency Walker - Imported DLLs

Some of the important function calls related to the sample being ransomware were observed as shown below:

a. GetLocalTime function

Contains ability to query machine time, this seems to be used by the sample to start the timer for the duration by which victim needs to pay the money or ransom.

Proof of concept:



GetVersionExA function b.

The sample contains ability to query the machine version which is a basic requirement for any malware. Sample retrieves information about which version of Windows is currently running on victim machine; this can be used as part of a victim's machine survey.

Proof of concept:

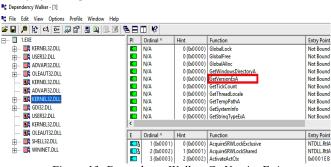


Figure 13: Dependency Walker-GetVersionExA

GetDiskFreeSpaceA function c.

The sample contains ability to query volume size of the victim's machine.

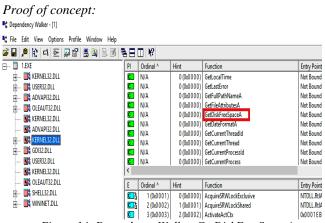


Figure 14: Dependency Walker-GetDiskFreeSpaceA

© 2018, IJCSE All Rights Reserved

WININET.DLL d.

Contains ability to read and download files from the Internet. The sample possibly once connected to internet communicates with command and control server for key exchange.

Circle Edit View Options Profile Window Help					
🗳 🖬 🔎 🖹 🕬 🖭 🖉 🖓 💷 🕷	58	II 149			
= 🔲 1.EXE	PI	Ordinal ^	Hint	Function	Entry Point
🗄 🧱 KERNEL32.DLL		N/A	0 (0x0000)	InternetReadFile	Not Bound
🛱 🧱 USER32.DLL		N/A	0 (0x0000)	InternetOpenUrIA	Not Bound
ADVAPI32.DLL	C	N/A	0 (0x0000)	InternetOpenA	Not Bound
🛱 📲 OLEAUT32.DLL		N/A	0 (0x0000)	InternetCloseHandle	Not Bound
KERNEL32.DLL					
ADVAPI32.DLL					
E B KERNEL32.DLL					
⊞ 🚮 KERNEL32.DLL ⊞ 🗐 GDI32.DLL					
⊞ 30\$ KERNEL32.DLL ⊞ ■\$ GDI32.DLL 30\$ USER32.DLL					
B 35 KERNEL32.DLL B 35 GDI32.DLL 55 KERNEL32.DLL 56 KERNEL32.DLL					
B - 31 ⁸ KERNEL32.DLL B - 11 ⁸ GO132.DLL - 31 ⁸ KERNEL32.DLL - 31 ⁸ KERNEL32.DLL - 31 ⁸ OLFAUT32.DLL	E	Ordinal ^	Hint	Function	Entry Point
⊕- 35 KERNEL32.DLL ⊕- 11 KG082.DLL 36 USER3.DLL 36 KERNEL32.DLL 36 KERNEL32.DLL ⊕- 11 KSHEL32.DLL	E	Ordinal ^ 101 (0x0065)		Function N/A	Entry Point 0x00112250
→ ■			N/A		
	0#	101 (0x0065)	N/A N/A	N/A	0x00112250

Figure 15: Dependency Walker-WININET

3) Virus Total tool

The sample was then uploaded to Virus Total and was identified as malicious by a large number of antivirus engines. The antivirus engines identified the sample as Vipasana.

	50 engines d	etected this file		
	SHA-256	0442cfabb3212644c4b894a7e4a	7e84c00fd23489cc4f96490f9	988e6074b6ab
	File name	vipasana1.exe		
	File size	370.5 KB		
50/64	Last analysis	2017-10-25 01:48:11 UTC		
	Community score	-261		
tection Det	ails Relations	Behavior Community 6		
Ad-Aware	🛕 Ger	eric.Ransom.Cryak.CD721E02	AegisLab	Troj.W32.Scartc
AhnLab-V3	A Tro	an/Win32.Agent.C1172414	ALYac	Generic.Ransom.Cryak.CD721
				•
Antiy-AVL	🛕 Troj	an/Win32.Scar	Arcabit	Generic:Ransom.Cryak.CD721
Avast	A Wir	32:Malware-gen	AVG	Win32:Malware-gen
11030		Service Se		A mischainere gen
Avira	🛕 TR/	ATRAPS.A.14311	AVware	Trojan.Win32.Generic!BT
D .:1	A		BitDefender	
Baidu	A ***	32.Trojan.WisdomEyes.16070401	bitbeiender	Generic.Ransom.Cryak.CD721
Bkav	🛕 W3	2.RansomCriaklB.Trojan	CAT-QuickHeal	Ransom.Vipasana.PR8
	-			• • • •
Comodo	A Tro	Ware.Win32.TrojanDownloader.De	CrowdStrike Falcon	malicious_confidence_90% (W
		afe		W32/Criakl.A.gen!Eldorado

4) Resource Hacker tool

Resource hacker clearly displayed desktop wallpaper image with a ransom note suspected to appear after target machine gets infected.



Figure 17: Resource Hacker

IV.II. Dynamic Analysis

Static analysis of the sample discovered many important details and evidences of the sample being a ransomware, but the dynamic analysis is required to get more concrete information on the same. On the other hand as the paper aims at recovery using forensic techniques, the sample needs to be executed. In this part of the experiment, the sample was executed in an isolated machine as mentioned earlier and observations were made.

1. Process Monitor

The sample, upon execution copied itself in the Program Files directory of the target machine.

Proof of concept:

👌 Process Monitor - Sysi	internals: www.sysinternals	s.com	
File Edit Event Filter	Tools Options Help		
🗃 🖬 🍳 🏽 🖄 🔤	🗟 🖗 🗊 🖊 🛓	s 🔐 🕞 🕰 🛺 📶	
Time Process Name	PID Operation	Path	Result
12:08: 🎩 1.exe	2512 🗟 CreateFile	C:\Windows\syswow64\imm32.dll	SUCCESS
12:08: 🎩 1.exe	2512 🗟 CreateFile	C:\Windows\syswow64\imm32.dll	SUCCESS
12:08: 🔳 1.exe	2512 🗟 CreateFile	C:\Windows\syswow64\imm32.dll	SUCCESS
12:08: 🎩 1.exe	2512 🛃 CreateFile	C:\Windows\syswow64\imm32.dll	SUCCESS
12:08: 🎩 1.exe	2512 🗟 CreateFile	C:\Windows\syswow64\ole32.dll	SUCCESS
12:08: 💶 1.exe	2512 🛃 Create File	C:\Windows\syswow64\ole32.dll	SUCCESS
12:08: 💶 1.exe	2512 🗟 CreateFile	C:\Users\WINDOWS_MALWARE\AppData\Local\Temp\1.ENU	NAME NOT
12:08: 🎩 1.exe	2512 🛃 CreateFile	C:\Users\WINDOWS_MALWARE\AppData\Local\Temp\1.ENU.DLL	NAME NOT
12:08: 🎩 1.exe	2512 🛃 CreateFile	C:\Users\WINDOWS_MALWARE\AppData\Local\Temp\1.EN	NAME NOT
12:08: 🎩 1.exe	2512 🛃 Create File	C:\Users\WINDOWS_MALWARE\AppData\Local\Temp\1.EN.DLL	NAME NOT
12:08: 🎩 1.exe	2512 🛃 CreateFile	C:\Program Files (x86)	SUCCESS
12:08: 🎩 1.exe	2512 🕂 CreateFile	C:\Users\WINDOWS_MALWARE\AppData\Local\Temp\1.exe	SUCCESS
12:08: 💶 1.exe	2512 🛃 CreateFile	C:\Program Files (x86)\1.exe	SUCCESS
12:08: 🎩 1.exe	2512 🛃 Create File	C:\Program Files (x86)\1.exe	SUCCESS
12:08: 💶 1.exe	2512 🛃 CreateFile	C:\Program Files (x86)\1.exe	SUCCESS
12:08: 💷 1.exe	2512 🗟 CreateFile	C:\Program Files (x86)	SUCCESS
12:08: 🎩 1.exe	2512 🗟 CreateFile	C:\Program Files (x86)\1.exe	SUCCESS
12:08: 💷 1.exe	2512 CreateFile	C:\Program Files (x86)\desktop.ini	SUCCESS
12:08: 🎩 1.exe	2512 🛃 CreateFile	C:\Program Files (x86)	SUCCESS
12:08: 🔳 1.exe	2512 CreateFile	C:\Program Files (x86)\ROTKXJYLPR.RYQ	SUCCESS
12:08: I.exe	2512 CreateFile	C:\Program Files (x86)\ROTKXJYLPR.RYQ	SUCCESS
12:08: I.exe	2512 CreateFile	C:\Users\WINDOWS_MALWARE\AppData\Local\Temp\iertutil.dll	NAME NOT
12:08: I.exe	2512 CreateFile	C:\Windows\syswow64\iertutil.dll	SUCCESS
12:08: 🎩 1.exe	2512 🛃 Create File	C:\Windows\syswow64\iertutil.dll	SUCCESS

Figure 18: Process Monitor

2. Reshot tool

The first shot was taken before running the sample on the target machine and the second shot was taken after the sample was executed. The result showed that a malicious Run key to the registry was added by the sample.

	es-x64.txt - Notepad
File	idit Format View Help
Val	es added: 1588
••••	
HKL	SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-21-2072349296-2157970859-38016
HKL	SOFTWARE\Microsoft\Windows\CurrentVersion\Run\pr: "C:\Program Files (x86)\1.exe"
HKU	\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore\Volatile\NestingLevel:
HKL	SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore\Volatile\StartNesting:
HKU	<pre>\SYSTEM\ControlSet001\Services\NcbService\NCB\KapiNlmCache\5\NumNetworks: 0x000000</pre>
HKL	<pre>\SYSTEM\ControlSet001\Services\NcbService\NCB\KapiNlmCache\5\Networks: 6E 21 76 0</pre>
HKL	<pre>\SYSTEM\ControlSet001\Service\NcbService\NCB\KapiNlmCache\5\Timestamp: 7C 78 84</pre>
HKL	<pre>\SYSTEM\ControlSet001\Service\NcbService\NCB\KapiNlmCache\5\KeySize: 0x00000000</pre>
	<pre>\SYSTEM\ControlSet001\Services\NcbService\NCB\KapiNlmCache\5\ValueSize: 0x00000008</pre>
	<pre>\SYSTEM\ControlSet001\Service\NcbService\NCB\KapiNlmCache\5\Value: 01 00 00 00 6</pre>
	<pre>\SYSTEM\ControlSet001\Services\VSS\Diag\ASR Writer\IDENTIFY (Enter): 48 00 00 00</pre>
	<pre>\SYSTEM\ControlSet001\Services\VSS\Diag\ASR Writer\IDENTIFY (Leave): 48 00 00 00</pre>
HKU	<pre>\SYSTEM\ControlSet001\Services\VSS\Diag\COM+ REGDB Writer\IDENTIFY (Enter): 48 06</pre>
	Figure 19: RegShot

3. ApateDNS tool

The sample made no relevant DNS request. Implying that it is an **offline** Ransomware; sample does not require internet in order to carry out its malicious activities on the victim's machine.

Proof of concept:

captule will	ndow DNS Hex View		
Time	Domain Requested	DNS Returned	
12:07:39	5.8.d.1.d.d.f.6.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.b.9ff.4.6.0.0 ip6.arpa	FOUND	- 1
12:07:41	0.0.0.0.0.0.0.0.1.1.4.2.5.0.0.0.0.f.7.9f.1.0.0.0.0.0f.7.ip6.arpa	FOUND	
12:07:41	0.0.0.0.0.0.0.0.1.1.4.2.5.0.0.0.0.f.7.9.f.1.0.0.0.0.f.7.ip6.arpa	FOUND	
12:08:02	1.160.168.192.in-addr.arpa	FOUND	
12:08:02	1.160.168.192.in-addr.arpa	FOUND	
12:08:23	b.9.d.1.d.df.6.0.0.0.0.0.0.0.0.0.0.0.0.0.0.b.9ff.4.6.0.0.ip6.arpa	FOUND	
12:08:35	shopping-na-divane.ru	FOUND	
12:08:35	shopping-na-divane.ru	FOUND	
12:08:36	shoptorgvlg.ru	FOUND	
12:08:36	shoptorgvlg.ru	FOUND	
[+] DNS se	ammf.adobe.com 192.168.1.1 as return DNS IP! et to 127.0.0.1 on Remote NDIS based Internet Sharing Device.	FOUND	
<pre>(+] Using (+] DNS se (+] Sendin</pre>	192.168.1.1 as return DNS IP!	FOUND	
<pre>[+] Using [+] DNS se [+] Sendin [+] Server DNS Re</pre>	192_168_1.1 as return DNS IP! et o 127.0-0.1 on Remote NoIS based Internet Sharing Device. ng valid DNS response of first request. r started at 12:05:35 successfully.] keply IP (Default Current Gatway/DNS): 192_168_1.1	FOUND	
<pre>[+] Using [+] DNS se [+] Sendin [+] Server DNS Re</pre>	192.168.1.1 as return DNS TP to 127.04.1.1 as return DNS based Internet Sharing Device. ng valid DNS response of first request. r started at 12:05:56 successfully.		ver

Figure 20: ApateDNS

4. WireShark tool

No relevant hosts were contacted; no relevant HTTP requests were made. No communication between the sample and any external server like command & control were requested. This further confirms that the sample is an offline Ransomware and does not get the keys from any Command and Control server.

Vol.6(4), Apr 2018, E-ISSN: 2347-2693

File	Edit View	Go Capture	Analyze Stat	istics Telephony	Wireless Tools	Help	
1	i 🖉 🖲 🗌			₩ 🖉 🖉 🔳			
	polv a display filte						Expression
No.	Time	Source		Destination	Protoco	Length	
	344 268,187		68.1.1	192.168.1.1			443 → 49817 [RST, ACK] Seg=1 Ack=1 Win=0 Len=0
	345 268,187		68.1.1	192,168,1,1			Standard query response 0x607a AAAA dns.msftncsi
	346 268,699	354 192.1	68.1.132	192.168.1.1			[TCP Retransmission] 49817 → 443 [SYN] Seq=0 Wir
	347 268,700	221 192.1	68.1.1	192,168,1,1	32 TCP		443 → 49817 [RST, ACK] Seg=1 Ack=1 Win=0 Len=0
	348 269.211	991 192.1	68.1.132	192.168.1.1			[TCP Retransmission] 49817 → 443 [SYN] Seg=0 Wir
	349 269.212	886 192.1	68.1.1	192.168.1.1	32 TCP		443 + 49817 [RST, ACK] Seg=1 Ack=1 Win=0 Len=0
	350 269.218	666 192.1	68.1.132	192.168.1.1	DNS	91	Standard query 0x290e A settings-win.data.micros
	351 269.218	819 192.1	68.1.132	192.168.1.1	DNS		Standard query 0xe9ad AAAA dns.msftncsi.com
	352 269.219	000 192.1	68.1.132	192.168.1.1	TCP	66	49818 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
	353 269.219	785 192.1	68.1.1	192.168.1.1	32 DNS	282	Standard query response 0x290e A settings-win.d
	354 269.219	970 192.1	68.1.1	192.168.1.1	32 DNS	104	Standard query response 0xe9ad AAAA dns.msftncs
	355 269.220	118 192.1	68.1.1	192.168.1.1	32 TCP	54	443 → 49818 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
	356 269.727	026 192.1	68.1.132	192.168.1.1			[TCP Retransmission] 49818 → 443 [SYN] Seq=0 Wir
	357 269.727	917 192.1	68.1.1	192.168.1.1			443 → 49818 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
	358 270.228	995 192.1	68.1.132	192.168.1.1			[TCP Retransmission] 49818 → 443 [SYN] Seq=0 Wir
	359 270.230	036 192.1	68.1.1	192.168.1.1			443 → 49818 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
	360 270.247	554 192.1	68.1.132	192.168.1.1	. DNS	91	Standard query 0x69c4 A settings-win.data.micros
	361 270.247	998 192.1	68.1.132	192.168.1.1	DNS	76	Standard query 0x6e5c AAAA dns.msftncsi.com

Figure 21: WireShark

Status of Desktop after infection of the machine



Figure 22: Desktop status before infection

Status of Desktop after infection of the machine

After the sample was executed on the target machine, the desktop wallpaper was changed with a ransom message on it.

Proof of concept:



Figure 23: Desktop status after infection

As mentioned earlier, the test data used in this research was encrypted by the sample as shown in screenshots below.

Proof of concept:

PC > Local Disk (C:) > Test_Files > File.doc	νÖ	Search
Name	Date modified	Туре
email-Johnmen.24@aol.com.ver-CL 1.2.0.0.id-FGGHIJKKKLLMNNOPPPPQRRSTTTTUVVWXXYY-11@19@20	11/19/2017 6:24 PM	CBF File
email-Johnmen.24@aol.com.ver-CL 1.2.0.0.id-FGGHIUKKKLLMNNOPPPPQRRSTTTTUVVWXXYY-11@19@20	11/19/2017 6:24 PM	CBF File
email-Johnmen.24@aol.com.ver-CL 1.2.0.0.id-FGGHIUKKKLLMNNOPPPPQRRSTTTTUVVWXXYY-11@19@20	11/19/2017 6:24 PM	CBF File
email-Johnmen.24@aol.com.ver-CL 1.2.0.0.id-FGGHIJKKKLLMNNOPPPPQRRSTTTTUVVWXXYY-11@19@20	11/19/2017 6:24 PM	CBF File
Figure 24: Encrypted doc files		

PC > Local Disk (C:) > Test_Files > File.jpg	v 0	Search F
Name	Date modified	Туре
email-Johnmen.24@aol.com.ver-CL 1.2.0.0.id-FGGHIUKKKLLMNNOPPPPQRRSTTTTUVWXXXYY-11@19@201	7 11/19/2017 6:25 PM	CBF File
email-Johnmen.24@aol.com.ver-CL 1.2.0.0.id-FGGHIIJKKKLLMNNOPPPPQRRSTTTTUVWXXYY-11@19@201	7 11/19/2017 6:25 PM	CBF File
email-Johnmen.24@aol.com.ver-CL 1.2.0.0.id-FGGHIJKKKLLMNNOPPPPQRRSTTTTUVWXXXYY-11@19@201	7 11/19/2017 6:25 PM	CBF File
Figure 25: Encrypted jpg files		

PC > Local Disk (C:) > Test_Files > File.pdf	v Ö	Search File
Name	Date modified	Туре
email-Johnmen.24@aol.com.ver-CL 1.2.0.0.id-FGGHIUKKKLLMNNOPPPPQRRSTTTTUWWXXYY-11@19@2017.6	11/19/2017 6:25 PM	CBF File
email-Johnmen.24@aol.com.ver-CL 1.2.0.0.id-FGGHIUKKKLLMNNOPPPPQRRSTTTTUWWXXYY-11@19@2017 6	11/19/2017 6:25 PM	CBF File
email-Johnmen.24@aol.com.ver-CL 1.2.0.0.id-FGGHIUKKKLLMNNOPPPPQRRSTTTTUWWXXYY-11@19@2017 6	11/19/2017 6:25 PM	CBF File
email-Johnmen.24@aol.com.ver-CL 1.2.0.0.id-FGGHIUKKKLLMNNOPPPPQRRSTTTTUVWWXXYY-11@19@2017.6	11/19/2017 6:25 PM	CBF File
email-Johnmen.24@aol.com.ver-CL 12.0.0:d+F66HIWXXLLMNV0PPPPQRISTITTUVWXXXY+11@19@20176 Figure 26: Encrypted pdf files	11/19/2017 6:25 PM	CBF File
PC > Local Disk (C:) > Test_Files > File.bt	v Ö	Search Fi
Name	Date modified	Туре
email-Johnmen.24@aol.com.ver-CL 1.2.0.0.id-FGGHIJKKKLLMNNOPPPPQRRSTTTTUVVWXXYY-11@19@2017	11/19/2017 6:25 PM	CBF File
email-Johnmen.24@aol.com.ver-CL 1.2.0.0.id-FGGHIIJKKKLLMNNOPPPPQRRSTTTTUVVWXXYY-11@19@2017	11/19/2017 6:25 PM	CBF File
email-Johnmen.24@aol.com.ver-CL 1.2.0.0.id-FGGHIUKKKLLMNNOPPPPQRRSTTTTUVVWXXYY-11@19@2017	11/19/2017 6:25 PM	CBF File
Figure 27: Encrypted txt files		

Name ^			
	Date modifier	d	Туре
email-Johnmen.24@aol.com.ver-CL 1.2.0.0.id-FGGHIUKKKLLMNNOPPPPQRRSTTTTUVWXXYY-11@19@2017	11/19/2017 6:	25 PM	CBF File
email-Johnmen.24@aol.com.ver-CL 1.2.0.0.id-FGGHIUKKKLLMNNOPPPPQRRSTTTTUVVWXXYY-11@19@2017	11/19/2017 6:	25 PM	CBF File
email-Johnmen.24@aol.com.ver-CL 1.2.0.0.id-FGGHIJKKKLLMNNOPPPPQRRSTTTTUVWXXYY-11@19@2017	11/19/2017 6:	25 PM	CBF File

C > Local Disk (C:) > Test_Files > File.zip	v	õ	Search File
lame ^	Date modifi	ed	Туре
email-Johnmen.24@aol.com.ver-CL 1.2.0.0.id-FGGHIUKKKLLMNNOPPPPQRRSTTTTUVVWXXYY-11@19@2017.6	11/19/2017	6:25 PN	A CBF File
email-Johnmen:24@aol.com.ver-CL 1.2.0.0.id-FGGHIJKKKLLMNNOPPPPQRRSTTTTUVVWXXYY-11@19@2017 6	11/19/2017	6:25 PN	A CBF File
email-Johnmen.24@aol.com.ver-CL 1.2.0.0.id-FGGHIJKKKLLMNNOPPPPQRRSTTTTUVVWXXYY-11@19@2017 6	11/19/2017	6:25 PN	A CBF File
Figure 29: Encrypted zip files			

IV. FORENSIC RECOVERY

The hard disk image of the infected machine was acquired using Forensic Falcon. Then Sleuthkit Autopsy was used to analyze the image. Following are a couple of important

Vol.6(4), Apr 2018, E-ISSN: 2347-2693

reasons behind selecting autopsy for analysis compared to other tools:

1. EnCase does not allow loading evidences having malicious files.

2. Autopsy is Open Source and the latest version of it is equally powerful and user-friendly.

Proof of concept:

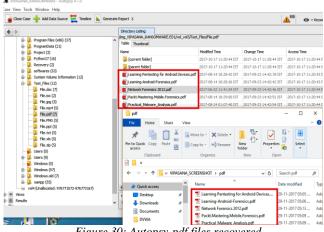


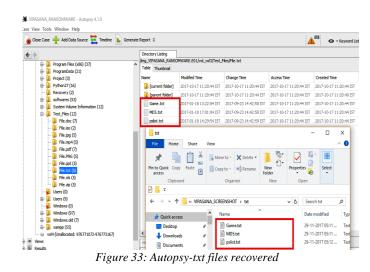
Figure 30: Autopsy-pdf files recovered

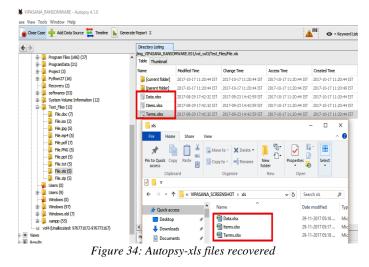
👩 Close Case 🕂 Add Data Source 🧮 Timeline	Generate Report 💲			A	 Keyword Lists
E ⇒	Directory Listing				
🕀 🐊 \$Recycle.Bin (4)	A Table Thumbhail	DMWARE.E01/vol_vol3/Test_	Files/File.jpg		
🕀 🔔 \$SysReset (6)					
SUnaloc (5)	Name	Modified Time	Change Time	Access Time	Created Time
🕀 🎉 \$WENDOWS.~BT (6)	[current folder]	2017-10-17 11:20:41 157	2017-10-17 11:20:41 IST	2017-10-17 11:20:41 IST	2017-10-17 11:20:41 15
Documents and Settings (2)	👘 😺 [parent folder]	2017-10-17 11:20:44 IST	2017-10-17 11:20:44 IST	2017-10-17 11:20:44 IST	2017-10-17 11:20:40 15
	📓 Kampala.jpg	2017-08-29 06:19:40 157	2017-09-23 14:42:04 IST	2017-10-17 11:20:41 IST	2017-10-17 11:20:41 157
Perfl.ogs (3)	Uganda.tpg	2017-08-29 06:18:14 157	2017-09-23 14:42:04 15T	2017-10-17 11:20:41 157	2017-10-17 11:20:41 15
Program Files (26)	Uganda2.pg	2017-08-29 06:19:08 151	2017-09-23 14:42:04 151	2017-10-17 11:20:41 151	2017-10-17 11-20-41 15
Program Files (x86) (37)					
🕀] ProgramData (21)					
⊕	Hex Strings File Ma	etadata Results Indexed T	ext Media		
	Hex Strings File Ma	etadata Results Indexed T			
🕀 🐊 Project (3)	Hex Strings File Ma	etadata Results Indexed T		ANDA &	
Project (3) Python27 (16) Recovery (2) softwares (53)	Hex Strings File Ma	etadata Results Indexed T		ANDA	
	Hex Strings File M	etadata Results Indexed T	U		
(1) Project (1) (1) (1) Prython 27 (16) (16) (16) (16) (16) (16) (12) (12) (12) (12) (12)	Hex Strings File M		EO	UATOR	
Project (3) Project (3) Protexn27 (6) Protexn27 (6) Softwares (53) Softwares (53) Softwares (53) Test_Files (12) File.Occ (7)	Hex Strings File No	etadata Results Indexed T	EO		
Project (3) Project (3) Project (3) Project (3) Project (3) Softwares (53) Softwares (53) Softwares (53) Test Files (12) Test Files (12) Files (12)	Hex Strings File Me		EO		
G G Priject (\$) G Priject (\$) G Priject (\$) G Priject (\$) G Softwares (\$3) G Softwares (\$3) G G Softwares (\$12) G G First (\$12) G G First (\$12) G First (\$2) First First (\$2) First First (\$2) First (\$2)	N Hex Strings File M		EO		
⊕	Nex Strings File Me		EO		
⊕ ⊕	Hex Strings File M		EO		
⊕ Project (1) ⊕ Project (2) ⊕ Proj	N Hex Strings File M		EO		
C C C C C	K Strigs FileM		EO		
⊕ The Project (1) ⊕ Project (2) ⊕ Project (2) ⊕ Rearvery (2) ⊕ Rearvery (2) ⊕ Project Volume Enformation (12) ⊕ Project (2)	K Strigs Field		EO		

Figure 31: Autopsy-jpg files recovered

lose Case	🕂 Add Data Source 🧮 Timeline 📔 Ge	nerate Report 🗧			<u>A</u> 83	Keyword Lists
	\$Recycle.5in (4) \$5ysReset (6)	Directory Listing /mg_VIPASANA_RANSOMM Table Thumbnail	ARE.E01/vol_vol3/Test_Files/	File.doc		
T- 🗸	sunaloc (5)	Name	Modified Time	Change Time	Access Time	Created Time
🖶 - 🚺	\$WINDOWS.~BT (6)	[current folder]	2017-10-17 11:43:52 IST	2017-10-17 11:43:52 IST	2017-10-17 11:43:52 15	T 2017-10-17 11:20:40
🔍	Documents and Settings (2)	[parent folder]	2017-10-17 11:20:44 IST	2017-10-17 11:20:44 IST	2017-10-17 11:20:44 15	T 2017-10-17 11:20:40
÷- 🔑	Intel (4)	Assignment.docx	2017-01-17 10:09:04 IST	2017-10-17 11:43:27 IST	2017-10-17 11:20:40 15	
ə 🏴	MSOCache (3)	Dog mentation docx	2017-08-27 06:07:46 151	2017-10-17 11:43:47 IST	2017-10-17 11:20:41 15	
- 1	PerfLogs (3)					
2	Program Files (26) Program Files (x86) (37)	MAC Flooding.docx	2017-07-20 02:20:16 IST	2017-09-23 14:42:04 IST	2017-10-17 11:20:41 15	
R	Program Hies (X86) (37) ProgramData (21)	TA2.docx	2017-03-31 11:13:08 IST	2017-09-23 14:42:04 IST	2017-10-17 11:20:41 IS	
ň	Project (3)	doc			-	□ × ^{20:00:00}
ñ	Python27 (16)	File Home S	hare View			~ 0
à.	Recovery (2)	The riving 2		_		
ġ.	softwares (53)	🚽 🖈 🗎 🚺	A Move to -	🗙 Delete 🔹 📜 🤨		H
8	System Volume Information (12)	Pin to Quick Copy Pa	ite 💼 🚺 Copy to -	Ti Rename New	Properties	Select
5	Test_Files (12)	access	ite 💽 🔛 Copy to 🕤	Rename folder	- Contraction of the second se	-
	File.doc (7)	Clipboard	Organi	ze New	Open	
	File.iso (2) File.jpg (5)	P 📑 =				
	File.mp4 (5)					
	File.odf (7)	← → * ↑	VIPASANA_SCREENSHOT	> doc	✓ Õ Search do	م
	File.PNG (S)		Name	^	Date modif	fied Typ
	File.ppt (5)	📌 Quick access				
	File.txt (5)	Desktop		nment.docx	29-11-2017	
	File.xls (5)	Downloads		mentation.docx	29-11-2017	05:00 Mic
1	File.zip (5)	 Documents 		Flooding.docx	29-11-2017	05:00 Mic
		Diawa	7 TA2.de	NCX .	29-11-2017	05:01 Mic

Figure 32: Autopsy-doc files recovered





In brief, during the analysis it was observed that the files encrypted by sample with extension .doc, .ppt, .jpg, .pdf, .txt, .xls were successfully recovered by autopsy. This was a big achievement as victims can rely on this uncommon technique to recover important documents without paying ransom to cyber criminals.

V. CONCLUSION AND FUTURE SCOPE

In conclusion, recovering files encrypted by the Ransomware is a great challenge to the Malware Analyst especially when the decryption key is not possible or difficult to identify. So, the present study demonstrated that digital forensic tools such as Autopsy can be used to recover user important files without paying a ransom.

On this basis, further studies can be implemented as: Reverse engineering the samples in order to obtain the decryption key, Analysis of the sample images using more Digital Forensics tools, Cuckoo Sandbox analysis technique,

Comprehensive RAM forensics analysis, Analysis and comparison of samples in bulk.

ACKNOWLEDGMENT

The authors are grateful to Dr. M.S. Dahiya, Director, Institute of Forensic Science, Gujarat Forensic Sciences University, Gandhinagar, for providing the infrastructure and the facilities for the completion of the project.

REFERENCES

- A. Bhardwaj, V. Avasthi, H. Sastry, G. V. B. Subrahmanyam, *"Ransomware Digital Extortion: A Rising New Age Threat"*, Indian Journal of Science and Technology, Vol.9, Issue.14, 2016.
- [2] A. Ali, "Ransomware: a research and a personal case study of dealing with this nasty malware", Issues in Informing Science and Information Technology, Vol.14, pp.087-099, 2017.
- [3] C. Everett, "Ransomware: to Pay or Not to Pay?" Computer Fraud & Security, Vol.2016, Issue.4, pp.8–12, 2016.
- [4] A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, E. Kirda, "Cutting the gordian knot: A look under the hood of ransomware attacks", In: M. Almgren, V. Gulisano, F. Maggi (eds) Detection of Intrusions and Malware, and Vulnerability Assessment. DIMVA 2015. Lecture Notes in Computer Science, Springer, Cham, Vol.9148, pp. 3-24, 2015.
- [5] S. Homayoun, A. Dehghantanha, M. Ahmadzadeh, S. Hashemi, R. Khayami, "Know abnormal, find evil: frequent pattern mining for ransomware threat hunting and intelligence", IEEE Transactions on Emerging Topics in Computing, pp. 1–1, 2017.
- [6] E. Kirda, "UNVEIL: a large-scale, automated approach to detecting ransomware (keynote)", In Software Analysis, Evolution and Reengineering (SANER-2017) IEEE 24th International Conference, pp.1-1, 2017.
- [7] K. Cabaj, M. Gregorczyk, W. Mazurczyk, "Software-Defined Networking-Based Crypto Ransomware Detection Using HTTP Traffic Characteristics", Computers & Electrical Engineering, Vol.66, pp.353–368, 2018.
- [8] J. K. Lee, S. Y. Moon, J. H. Park, "CloudRPS: a Cloud Analysis Based Enhanced Ransomware Prevention System", The Journal of Supercomputing, Vol.73, Issue.7, pp.3065–3084, 2017.
- [9] A. Gazet, "Comparative Analysis of Various Ransomware Virii", Journal in Computer Virology, Vol.6, Issue. 1, pp. 77–90, 2010.
- [10] V. U. Bala, B.D.C.N.Prasad "A Study on- Identifying and Evading Ransomware (Ransomware)", SSRG International Journal of Computer Science and Engineering (SSRG - IJCSE), Vol.5, Issue.2,pp.9-13, 2018
- [11] S. Mohurle, M. Patil, "A brief study of wannacry threat: Ransomware attack 2017", International Journal, Vol.8, Issue.5, pp.1938-1940, 2017.
- [12] "North Korea Blamed for WannaCry, PoS Attacks and Bitcoin Phishing", Network Security, Vol.2018, Issue.1, pp.1-2, 2018.
- [13] J. MacRae, V.N.L. Franqueira, "On Locky Ransomware, Al Capone and Brexit," In: P. Matoušek, M. Schmiedecker (eds) Digital Forensics and Cyber Crime (ICDF2C 2017) Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Springer, Cham, Vol.216, pp.33-45, 2017.
- [14] P. P. Kulkarni, T. Nafis, S.S. Biswas, "Preventive Measures and Incident Response for Locky Ransomware", International Journal of Advanced Research in Computer Science, Vol.8, Issue.5, 2017.

Vol.6(4), Apr 2018, E-ISSN: 2347-2693

- [15] A. Zahra, M.A. Shah "IoT Based Ransomware Growth Rate Evaluation and Detection Using Command and Control Blacklisting", In proceeding of 23rd International Conference on Automation and Computing (ICAC- 2017), pp.1-6, 2017.
- [16] S. Berkenkopf, "Manamecrypt–a ransomware that takes a different route", 2016. https://www.gdatasoftware.com/blog/2016/04/28234manamecrypt-a-ransomware-that-takes-a-different-route.
- [17] J. Li, D. Gu, Y. Luo, "Android malware forensics: Reconstruction of malicious events", In proceeding of 32nd International Conference on Distributed Computing Systems Workshops (ICDCSW-2012), IEEE, pp.552-558, 2012.
- [18] M. Brand, C. Valli, A. Woodward, "Malware Forensics: Discovery of the Intent of Deception", The Journal of Digital Forensics, Security and Law, Vol.5, Issue.4, pp.31, 2010.
- [19] B. Ruttenberg, C. Miles, L. Kellogg, V. Notani, M. Howard, C. LeDoux, A. Lakhotia, Pfeffer, "*Identifying Shared Software Components to Support Malware Forensics*", In: S. Dietrich (eds) Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA-2014), Lecture Notes in Computer Science, Springer, Cham, Vol.8550, pp.21–40, 2014.
- [20] Z. Deng, D. Xu, X. Zhang, X. Jiang, "Introlib: Efficient and transparent library call introspection for malware forensics", Digital Investigation, Vol.9, pp.S13-S23, 2012.

Authors Profile

Mr. Francis Byabazaire pursed Bachelor of Science from Kyambogo University, Uganda. He is currently pursuing Msc. Digital Forensics and Information Security from Gujarat Forensic Sciences University, Gandhinagar, India. His research area of interest are Malware Analysis, Digital Forensics, Cyber Forensic Analysis, Vulnerability Assessment and Penetration Testing.



Dr. Parag H. Rughani completed his Ph. D. in computer science from Saurashtra University. He is currently working as an associate professor in Digital Forensics and Information Security at Institute of Forensic Science, Gujarat Forensic Sciences University, Gandhinagar since November, 2014. He has 12 years of teaching experience and has published



more than 10 research papers in reputed international journals. His area of expertise include Digital Forensics, Memory Forensics, Android Forensics, Malware Analysis and IoT Security and Forensics.