International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-3, January 2020

Forensic Analysis of a Ransomware

Animesh Kumar Agrawal, Sumit Sah, Pallavi Khatri

Abstract*: In the present digital world malware is the most potent weapon. Malware, especially ransomware, is used in security breaches on a large scale which leads to huge losses in terms of money and critical information for big firms and government organisations. In order to counter the future ransomware attacks it is necessary to carry out a forensic analysis of the malware. This experiment proposes a manual method for dynamic malware analysis so that security researchers or malware analyst can easily understand the behaviour of the ransomware and implement a better solution for reducing the risk of malware attack in future. For doing this experiment Volatility, Regshot and FTK Imager Lite Forensics toolkit were used in a virtual and safe environment. The forensic analysis of a Ransomware is done in a virtual setup to prevent any infection to the base machine and carry out detailed analysis of the behaviour of the malware under different conditions. Malware analysis is important because the behavioral analysis helps in developing better mitigation techniques thereby reducing infection risks. The research can prove effective in development of a ransomware decryptor which can be used to recover data after an attack has encrypted the files.

***Keywords* : Malware Analysis, FTK Imager, Volatility, Virtual Box, Ransomware.**

I. INTRODUCTION

Malware is also known as malicious software. It is basically a file or program which is causes harm to the digital device be it a PC or a mobile. Malware has malicious code embedded in it which when executed leads to compromise of the device. Malware includes computer viruses, worms, bots, Spyware, adware, Trojan horses, etc. The latest addition in the family of malwares is Ransomware, which has infected large number of systems and led to loss of data and revenue. Every malware has a different behaviour which is basically dependent on how it is coded. One of the most dangerous and famous ransomware is Wannacry. It is a type of malware which infects the system and encrypts every folder and file and then locks the user screen, thereby preventing the user from accessing the system. In order to access the system and decrypt the files, the user has to pay a ransom in the form of digital currency called bitcoins. It was originally named as wanacrypt and also knows wanacrypt0r and wanadecrypt0r. The wannacry worldwide attack happened on May 2017 and affected more than 3 lakh computers. It basically targeted the computers which were running on Windows Microsoft Operating System.

Revised Manuscript Received on January 30, 2020.
***** Correspondence Author
Animesh Kumar Agrawal*, Computer Science Department, ITM University Gwalior, India. Email: akag9906@gmail.com
Sumit Sah, Computer Science Department, ITM University Gwalior, India. Email: sumitsah18@gmail.com
Dr Pallavi Khatri, Computer Science Department, ITM University Gwalior, India. Email: pallavi.khatri.cse@itmuniversity.ac.in

In the ransomware family one of the most famous ransomware is Locky Ransomware which primarily encrypts the files of the Windows OS and seeks ransom from the user for decrypting/unlocking the files. It was discovered in early 2016 and become most significant malware of Ransomware family. Another reputed ransomware is Cryptolocker 2 whose primary function is to lock files in a Windows machine through the use of Gameover Zeus botnet. It uses RSA & AES cipher for encrypting files and demands ransom in hundreds of dollars. Petya 1 ransomware active in early 2016 infected master boot record of Windows OS.

II. RELATED WORK

The work described in [1] discusses dynamic malware analysis using Cuckoo Sandbox environment. This is a virtual setup which is isolated to prevent any chance of infection due to execution of malware. The automatic report generated by this framework is utilised to carry out analysis of the bad as well as good samples using Machine Learning algorithms.

In [2] the authors have proposed a new algorithm for malware analysis called TFDROID. Based on the behaviour an application is categorised as malicious and benign. Clustering algorithm has been used in the presented approach but it is unable to do dynamic analysis of the apps and hence this approach needs to be improved. Using Machine Learning approach, malwares could be detected with 93.7% accuracy.

The research in [3] describes the method to detect malware for Windows as well as android apps. Different approaches were described to identify the signature and the behaviour of apps in order to detect the malware. The authors have proposed a solution named DERBIN which is capable of detecting malwares in runtime in an android phone. The proposed approach was not applicable to all situations though it did achieve an accuracy of 97%. New malwares could not be detected through the method described in the research.

This paper [4] described static and dynamic analysis of the apps using ML approach. Obfuscated and non-obfuscated type of malware was analysed using dynamic analysis and the performance was found to be satisfactory. The experiments conducted proved that code obfuscated samples worked well in dynamic analysis whereas non-obfuscated ones in static analysis.

In [5] anomaly based malware detection framework has been proposed by the authors for an android device. Benign and malicious apps were installed in an android phone and their behaviour pattern was analysed. Various ML based algorithms were used to classify the apps in the two broad categories. Signature based malware detection could not be done via the proposed framework thereby limiting its applicability in malware analysis. The work in [6] measured the decay in performance of the samples both benign and malicious over time. For this the samples taken were stamped with dates so that the performance decay could be quantified accurately.

In order to do this study different Machine Learning classifiers were used. The authors concluded from the study that benign samples were wrongly classified as malicious in comparison to correctly classifying the malicious ones.

The research proposed in [7] and [8] describes ways to create a virtual environment and carry out analysis. While the papers describe the android phone environment, the concept is same and can be applied to carry out the malware analysis.

In [9], the basics of virtual machine creation and usage including its architecture have been described. The importance of emulator environment and the file structure has been elaborated along with the methodology to analysis a forensic image created on an emulator.

The research presented in [10] talks about a malware detection system called SIGPID which can help in differentiating between a malicious and benign app. The authors claim that the proposed system is efficient in identifying the malwares.

The work in [11] describes malware analysis in android setup. Two static analysis approaches has been presented in the paper. ML techniques have been used to compare the efficacy of the two approaches.

III. METHODOLOGY

This research focuses on dynamic malware analysis of a Wannacry ransomware in a virtual environment. Virtual box and Microsoft Windows 7 have been used to carry out the forensic analysis of the malware. One important pre-requisite was internet connection during analysis so that the malware could communicate with C&C server thereby depicting its true behaviour. Non-availability of internet prevents the malware from executing because it is unable to download the encryption keys, etc. The system and software specification used for this work is mentioned below in Table I and II.

Table I. Specification for host machine

System and software specification	
CPU	Sixth-Gen i3 core processor
RAM	4 GB DDR4, 2133MHz (min. requirement)
GPU	Intel Integrated HD 520
Host OS	Kali Linux 2019
HDD	1Tb SATA hard drive

Table II. Specification for virtual machine

System and software specification	
Software Required	Virtual box
OS	Windows 7/8/10
RAM	Minimum 2 GB
VDD	Minimum 30 GB

In this experiment virtual machine was used and the virtual OS was manually infected. But in case the host machine is already compromised by ransomware, there is a need to identify the file extensions created by ransomware. These file extensions are hidden and hence need to be searched. Some of the ransomware file extensions are .ecc, .ezz, .exx, .zzz, .xyz, .aaa, .abc, .ccc, .vvv, .xxx, .ttt, .micro, .encrypted, .locked, .crypto, _crypt, .crinf, .r5a, .XRNT, .XTBL, .crypt, .R16M01D05, .pzdc. We can also look for ransom note file if our system is infected by ransomware good, .LOL!, .OMG!, .RDM, .RRK, .encryptedRSA. If any of the file extensions are present on the machine it means our machine is infected. Usually the ransomware creates a ransom note, generally on the desktop and from the ransom note we can identify the source of the attack. Some of the ransom note files are help_decrypt.txt, help_your_files.txt, help_to_decrypt_your_ files.txt, recovery_key.txt, help_restore_files.txt,help _recover_files.txt, help_to_save_files.txt, DecryptAllFiles. txt. We can find the file owner domain by checking the property of ransom note.

There are many ways by which our machine can be infected by the ransomware malware. One of the spread mechanisms is phishing through email. If some infected links are sent via mail and clicked by the recipient inadvertently, the ransomware malware is downloaded automatically and starts spreading in the background.. Another way is exploitation of vulnerability in the OS, like the way Petya 1 ransomware infects. Another method is drive-by download in which hackers use online ads to upload malicious code in victims system. For dynamic malware analysis, software's and tools used are Virtual box, Regshot, FTK Imager Lite and Volatility. Ram dump is taken with the help of FTK Imager and then analysed with the help of Volatility. FTK Imager stands for Forensics Tool Kit. As the name suggests, it is basically a tool which comes with two versions FTK Imager Lite and FTK Imager. FTK Imager Lite is free of cost. On the other hand FTK Imager is paid version. It is used for taking RAM dump, obtaining protected files like hiber, page and SAM file and it is also used for making image of any physical drive/logical drive. Regshot is an open source utility which is used for taking the image of the registry. Two registry images taken through Regshot can then be compared. It allows user to take 1st shot of registry and then a 2nd shot and it gives comparative results and by this user can easily see the changes that happened between 1st and 2nd registry shot primarily due to some malware execution. Volatility is an open source memory forensics tool which is implemented in python. The main purpose of this tool is to find and extract digital artifacts from volatile memory (RAM) dump. The process for doing this work is divided into four parts. First phase is virtual machine setup phase on the host machine. In the second phase Regshot of the image is taken and then the malware is executed. In the third phase RAM dump of virtual machine is taken with the help of FTK Imager Lite. In the fourth phase memory forensics is done with the help of Volatility on RAM dump and digital artifacts are extracted.

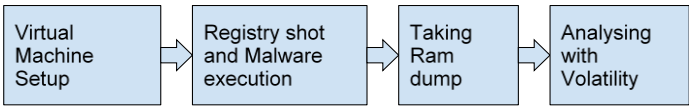


Fig 1. Flow chart of Methodology

IV. EXPERIMENTATION AND RESULTS

The first important step in dynamic malware analysis is to create a virtual machine on a host machine because in dynamic malware analysis we have to execute the real malware in machine and then we have to analyse its behaviour.

It is very risky to execute the malware on the host machine because it would lead to infection of the base OS. Hence, the malware analysis is done by creating a virtual machine in either Virtual Box or VMware environment.

We create a Windows 7 virtual machine and assign 2 GB RAM and 30 GB virtual disk space to it. After creating a virtual machine the second step is to run Windows and then take a snapshot of the machine by clicking on the button which is mentioned in Fig 2.

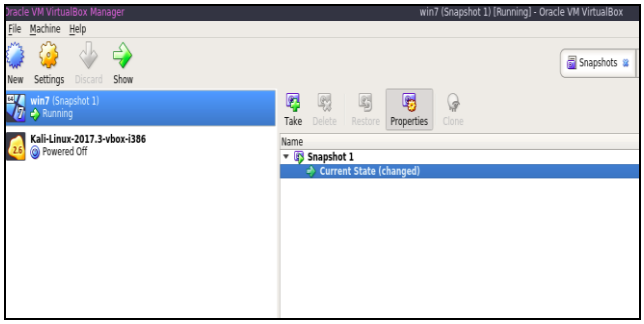
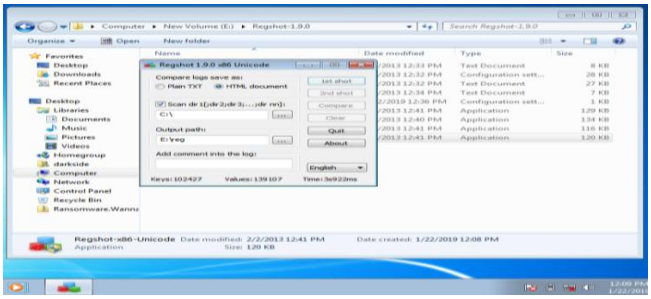


Fig 2. Win 7 Virtual machine

Fig 2 shows the Windows 7 virtual machine and we can see that a snapshot is also present. After taking snapshot next step is to take the first registry shot with the help of Regshot utility tool. Since it is utility tool so installation is not



required, so after opening Regshot click on the HTML document and provide the first output path then click on the 1st Regshot.

Fig 3. Taking 1st registry shot

Fig 3 shows the process of taking 1st Regshot. After successfully taking the 1st registry shot the next step is to execute the malware as an administrator manually. Generally we have to unzip the malware file first then we have to make it executable by adding .exe after the name of malware. Wannacry ransomware was executed and its effect on the resident data was seen in a couple of minutes. Fig 4 shows the screen after executing ransomware.

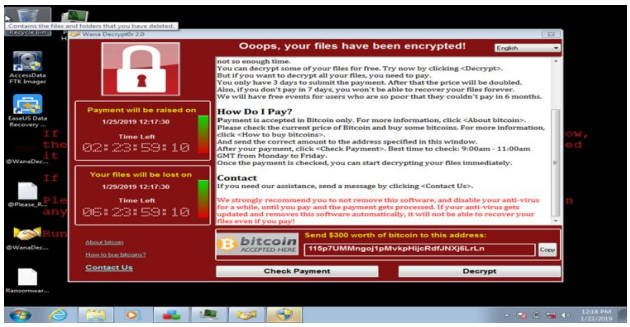


Fig 4. Screen Hijacking by Ransomware

After successful execution of ransomware, the control of the user screen was taken over by the malware and it encrypted all the files and folders so that they were not accessible by user. In order to allow the user to decrypt his files a ransom of $300 in the form of bitcoins was asked.

The next step is to take 2nd registry shot with the help of Regshot and then compare it with the previous one. We do this because after comparing we can easily say that what types of changes malware does on the machine and where it's executed, where from where the new files are created and deleted by the malware. We can see all the directory changes by comparing the result by simply clicking on compare button. Fig 5 shows the step for taking 2nd registry shot.

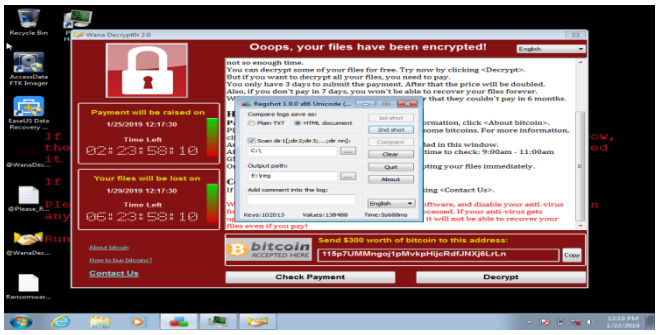


Fig 5. Taking second registry shot

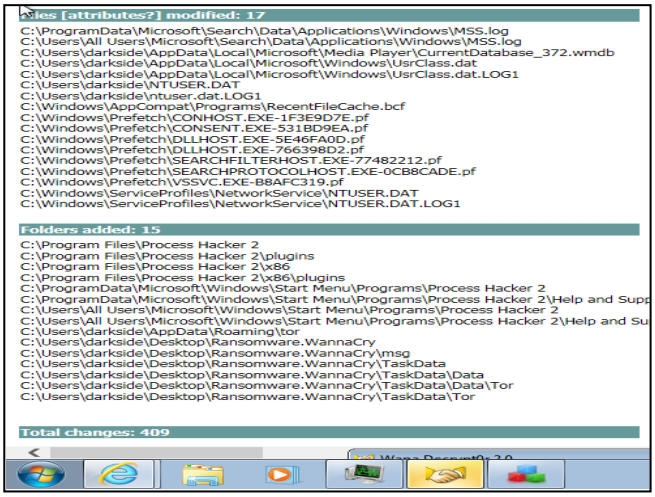


Fig 6. Result of Regshot

Regshot gives the result in HTML document to compare it because we already selected HTML document. After analyzing the result we can easily see that in Fig 6 that ransomware makes total 409 changes and it modified 17 attributes and in 15 folders. It added folders and files on desktop as depicted in Fig 6 but these folders are not visible on the desktop. After completing the Regshot related processes, the next step is to do memory forensics on volatile memory in order to find the process id and process name of ransomware malware. In order to do this, RAM dump of compromised virtual Windows machine with the help of FTK Imager Lite tool is taken. Fig 7 shows the process of taking RAM dump. Then the virtual machine needs to be reverted back to its original state by clicking on restore button on virtual box. After reverting it, we can use snapshot of the VM which we created earlier.

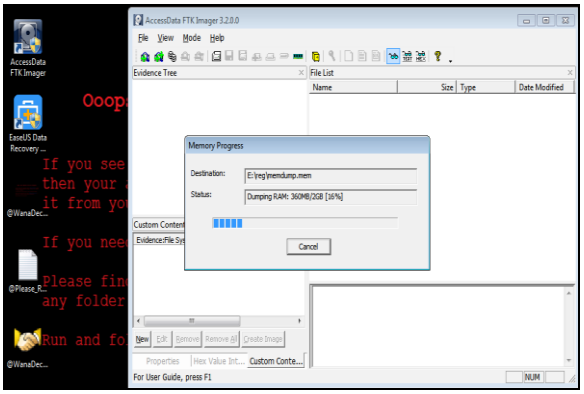
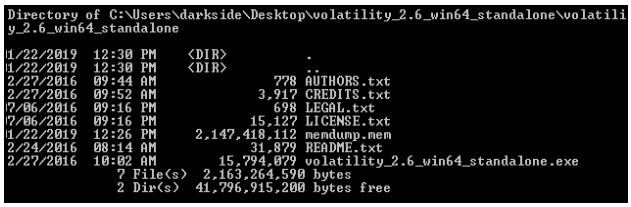


Fig 7. Taking RAM dump with FTK Imager Lite

After reverting the VM, the next step is to do memory forensics with the help of volatility tool. For doing this we have to paste the RAM dump file which was taken by the FTK Imager Lite in the same folder where volatility.exe file is residing. Subsequently, a command prompt is opened in administrator mode and the command as depicted in Fig 9 is required to be entered.

The first process in Volatility is profiling where we find the profile of RAM dump. For this imageinfo command is used as mentioned in Fig 8.



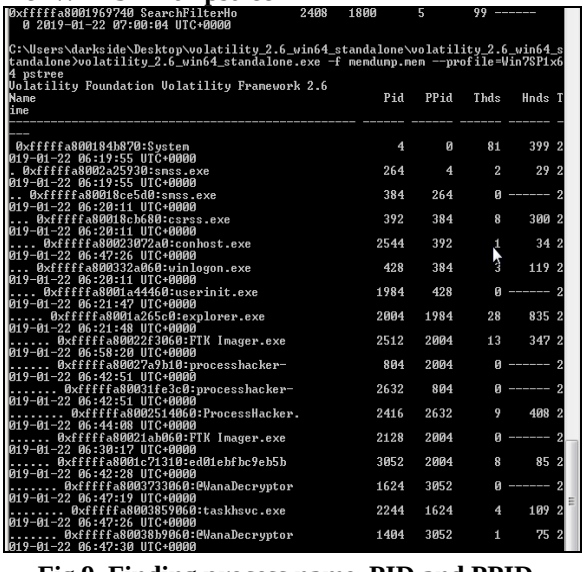
```
Directory of C:\Users\darkside\Desktop\volatility_2.6_win64_standalone\volatili
y_2.6_win64_standalone

01/22/2019  12:30 PM    <DIR>          .
01/22/2019  12:30 PM    <DIR>          ..
2/27/2016   09:44 AM               778 AUTHORS.txt
2/27/2016   09:52 AM             3,917 CREDITS.txt
7/06/2016   09:16 PM               698 LEGAL.txt
7/06/2016   09:16 PM            15,127 LICENSE.txt
01/22/2019  12:26 PM     2,147,418,112 memdump.mem
2/24/2016   08:14 AM            31,879 README.txt
2/27/2016   10:02 AM        15,794,079 volatility_2.6_win64_standalone.exe
               7 File(s)  2,163,264,590 bytes
               2 Dir(s)  41,796,915,200 bytes free
```

Fig 8. Profiling of RAM dump

After profiling, Volatility suggests a no of profiles from which we have to choose the correct profile based on the OS being used (Win7SP1x64 profile in the present case). After that all the processes, process ID (PID) and parent process ID (PPID) are required to be found out. This helps in identifying the ransomware process real name and we can find process id with the help of pslist or pstree plugin as given in Fig 9. For doing this we have to execute the command

>>volatility_2.6_win64_standalone.exe-f memdump.mem profile=Win7SP1x64 pstree



```
0xfffffa80019697a0 SearchFilterHo        2408   1800      5       99 ------
  0 2019-01-22 07:00:04 UTC+0000

C:\Users\darkside\Desktop\volatility_2.6_win64_standalone\volatility_2.6_win64_s
tandalone>volatility_2.6_win64_standalone.exe -f memdump.mem --profile=Win7SP1x6
4 pstree
Volatility Foundation Volatility Framework 2.6
Name                                                 Pid   PPid   Thds   Hnds T
ime
-------------------------------------------------- ------ ------ ------ ------ -
---
 0xfffffa800184b870:System                             4      0     81    399 2
019-01-22 06:19:55 UTC+0000
. 0xfffffa8002a25930:smss.exe                        264      4      2     29 2
019-01-22 06:19:55 UTC+0000
.. 0xfffffa80018ce5d0:smss.exe                       384    264      0 ------ 2
019-01-22 06:20:11 UTC+0000
... 0xfffffa80018cb680:csrss.exe                     392    384      8    300 2
019-01-22 06:20:11 UTC+0000
.... 0xfffffa800230720:conhost.exe                  2544    392      1     34 2
019-01-22 06:47:26 UTC+0000
... 0xfffffa800332a060:winlogon.exe                  428    384      3    119 2
019-01-22 06:20:11 UTC+0000
.... 0xfffffa8001a44460:userinit.exe                1984    428      0 ------ 2
019-01-22 06:21:47 UTC+0000
..... 0xfffffa8001a265c0:explorer.exe               2004   1984     28    835 2
019-01-22 06:21:48 UTC+0000
...... 0xfffffa80022f3060:FTK Imager.exe            2512   2004     13    347 2
019-01-22 06:58:20 UTC+0000
...... 0xfffffa80027a9b10:processhacker-             804   2004      0 ------ 2
019-01-22 06:42:51 UTC+0000
...... 0xfffffa80031fe3c0:processhacker-            2632    804      0 ------ 2
019-01-22 06:42:51 UTC+0000
........ 0xfffffa8002514060:ProcessHacker.          2416   2632      9    408 2
019-01-22 06:44:08 UTC+0000
...... 0xfffffa80021ab060:FTK Imager.exe            2128   2004      0 ------ 2
019-01-22 06:30:17 UTC+0000
...... 0xfffffa8001c71318ed01ebfbc9eb5b             3052   2004      8     85 2
019-01-22 06:42:28 UTC+0000
....... 0xfffffa8003733060:@WanaDecryptor           1624   3052      0 ------ 2
019-01-22 06:47:19 UTC+0000
........ 0xfffffa8003859060:taskhsvc.exe            2244   1624      4    109 2
019-01-22 06:47:26 UTC+0000
....... 0xfffffa80038b9060:@WanaDecryptor           1404   3052      1     75 2
019-01-22 06:47:30 UTC+0000
```

Fig 9. Finding process name, PID and PPID

After doing this we find a process called @WanaDecryptor which was running on machine and process id (PID) was 1624 and parent process ID (PPID) was 3052. So with the help of this method we can analyse the behaviour of malware. For decrypting Wannacry ransomware encrypted files we can use WanaKiwi decryptor tool, which is free and easy to use.

Table III. Summary of results obtained

List of evidence	YES/NO
Ransom note found	YES
Malware Process name & process id found	YES
Malware Behaviour Found	YES
Ransom Demanded by Malware	YES
Registry Changes by Malware	YES

There are many benefits of doing dynamic malware analysis. Some of them are that we can understand the working and behaviour of the malware and it can also help the malware analyst or Incident responder to make a proper solution to mitigate this type of malware cyber-attack. In future and they can also analyse in a big network how many nodes are compromised by the malware. Dynamic malware analysis is also used for better.

V. CONCLUSION AND FUTURE SCOPE

The manual approach proposed in this work for forensic analysis of a ransomware is useful in carrying out a credible dynamic analysis. The examination of the various processes helped in understanding the infection process of the malware and thereby finding a remedy. The open source tools are effective in malware analysis and can be used to carry out a more in-depth analysis of more sophisticated ransomware samples and also help in developing an anecdote in the form of decryptor.

ACKNOWLEDGMENT

The authors would like to express sincere gratitude to ITM University Gwalior for providing the platform to work in machine learning as well as forensics analysis.

REFERENCES

1. H. Zhao, M. Li, T. Wu, and F. Yang, “Evaluation of Supervised Machine Learning Techniques for Dynamic Malware Detection,” International Journal of Computational Intelligence Systems, vol. 11, no. 1, p. 1153, 2018.
2. Songhao Lou, Shaoyin Cheng, Jingjing Huang (2019), TFDroid: Android Malware Detection by Topics and Sensitive Data Flows Using Machine Learning Techniques, IEEE 2nd International Conference on Information and Computer Technologies.
3. Syed Fakhar Bilal, Saba Bashir, Farhan Hassan Khan and Haroon Rasheed (2019), Malwares Detection for Android and Windows System by Using Machine Learning and Data Mining, INTAP 2018: Intelligent Technologies and Applications Communications in Computer and Information Science, Vol 932. Springer.
4. Alessandro Bacci, Alberto Bartoli,Fabio Martinelli (2018), Impact of Code Obfuscation on Android Malware Detection based on Static and Dynamic Analysis, 4th International Conference on Information Systems Security and Privacy.

5. Mariam Al Ali, Davor Svetinovic, Zeyar Aung, Suryani Lukman (2017), Malware Detection in Android Mobile Platform using Machine Learning Algorithms, IEEE International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS).
6. Yerima, S. and Khan, S. (2019) Longitudinal performance analysis of machine learning based Android malware detectors. International Conference on Cyber Security and Protection of Digital Services (Cyber Security 2019), Oxford, UK, June 3-4, 2019..
7. Sharma A., Agrawal A.K., Kumar B., Khatri P. (2019) Forensic Analysis of a Virtual Android Phone. In: Verma S., Tomar R., Chaurasia B., Singh V., Abawajy J. (eds) Communication, Networks and Computing. CNC 2018. Communications in Computer and Information Science, vol 839. Springer, Singapore.
8. Sumit Sah, Agrawal A.K., Pallavi Khatri (2019) Physical Data Acquisition from Virtual Android Phone using Genymotion. ICSCN 2019: International Conference on Sustainable Communication Networks and Applications Jul 30-31, 2019.
9. Brett Shavers," A Discussion of Virtual Machines Related to Forensics Analysis". {https://www.forensicfocus.com/downloads/virtual-machines-forensics-analysis.pdf}
10. Jin Li, Lichao Sun, Qiben Yan, Zhiqiang Li , Witawas Srisa and Heng Ye (2018) ,Significant Permission Identification for Machine Learning Based Android Malware Detection, IEEE Transactions on Industrial Informatics(Vol. 14.,Issue: 7 , July 2018).
11. N. Milosevic, A. Dehghantanha, and K.-K. R. Choo, "Machine learning aided Android malware classification," Computers & Electrical Engineering, vol. 61, pp. 266–274, Jul. 2017.

AUTHORS PROFILE

Animesh Kumar Agrawal is a Research Scholar who is currently pursuing his PhD from ITM University, Gwalior. His research interests are in the area of GPU programming, cyber security and mobile forensics. His papers have appeared in IEEE Conference on APSAR, Springer Lecture Note book in,, Advances in Data and Information Sciences".

Sumit Sah is a Computer Science Engineering student who is currently pursuing his Engineering from ITM University, Gwalior. His research interests are in the area of cyber security and cyber forensics. His papers have appeared in Springer Lecture Note book in "Data Engineering and Communication Technologies" and in IEEE Conference on ICICCS.

Pallavi Khatri is an Associate Professor of ITM university, Gwalior. Her research interests include mobile ad-hoc network, Wireless Sensor Networks. Her papers have appeared in IEEE Proceedings on Communication Networks (ICCN), Computing, Communication and Automation (ICCCA), Taylor n Francis Group, CRC Press, Balkema (ICCCS), International Conference on Information, Communication, Instrumentation and Control (ICICIC). Springer Lecture Note book ,,Advances in Data and Information Sciences.