**International Journal of Electrical and Computer Engineering (IJECE)**
Vol. 8, No. 5, October 2018, pp. 3179~3186
ISSN: 2088-8708, DOI: 10.11591/ijece.v8i5.pp3179-3186 

# Invesitigation of Malware and Forensic Tools on Internet

**Tarun Kumar, Sanjeev Sharma, Ravi Dhaundiyal, Parag Jain**
Department of Computer Science & Engineering, Uttrakhand Technical University, India

**Article Info**

***Article history:***

Received Nov 24, 2017
Revised Jan 13, 2018
Accepted Aug 5, 2018

***Keyword:***

Analysis tools
Cyber crimes
Forensic intelligence
Malware detection

**ABSTRACT**

Malware is an application that is harmful to your forensic information. Basically, malware analyses is the process of analysing the behaviours of malicious code and then create signatures to detect and defend against it.Malware, such as Trojan horse, Worms and Spyware severely threatens the forensic security. This research observed that although malware and its variants may vary a lot from content signatures, they share some behaviour features at a higher level which are more precise in revealing the real intent of malware. This paper investigates the various techniques of malware behaviour extraction and analysis. In addition, we discuss the implications of malware analysis tools for malware detection based on various techniques.

*Copyright © 2018 Institute of Advanced Engineering and Science.*
*All rights reserved.*

***Corresponding Author:***

Tarun Kumar,
Department of Computer Science & Engineering,
Uttarakhand Technical University,
Suddhowala, Dehradun, Uttarakhand-248007, I ndia.
Email: taretechcse14@gmail.com

## 1. INTRODUCTION

The word malware is the combination of two word such as malicious and software. Malware indicates the malicious content deployment with software [1]. Deployment of malware is easy but, source of the malware is difficult to track. The use of malware is to collect the confidential information and send to the black market. Basically, malware is demanded specifically for organized crime and state sponsored espionage agents. Financial services are the key targets of the malware enabled attacks [2]. The finance industry is also target by cyber criminals through the malware attacks. Malware enabled crime is not a new way to disturb the life of peoples. Software enabled crimes are the going parallelly with the information technology. Since the development of mainframe based automated bank accounts, financial services are the victims of malware enabled attacks [3].

In addition, criminals change the software with malware facility to transfer the money from one-person account to another account, which is happens during the internet connectivity or shared network. The parallel evolution of information technology and malware enabled crimes have created a big problem with respect to the security of information and in financial industry [4]. Those who have no great knowledge of technology, for them it is difficult to understand the side effects of software conciliation. In general, malware enabled criminals are working based on the hit and trials basis to find out any soft target. These types of incidentsaffectsome part of public as bad luck. But in some cases, cybercrimes are targeted as well [5].

In general, the analysis of malware has been required due to the computer security incidents, malware research and indicator of compromise extraction [6]. Malware analysis can be categorized into two classes such as static malware analysis and dynamic malware analysis.Static analysis has been achieved by dismembering the diverse resources of the binary file without executingit and studying each component. Dynamic analysis has been done through the observation of malware behaviour while it is actually running on a host system, which is basically used in sandbox environment to prevent the malware [7].

For any common person, news about the malware enabled attacks seems not so related to him/her. The malware enabled attackers are scattered around the globe [7]. They are working with various companies and nationalities. Only a few years ago, cyber security standards published about the malware to indicate as a security threat. In addition, they also agreed that malware is a black-hole in cyber security. The cyber criminals are working at a great level of cooperation to make a crime pattern [8].

Today security investigators consent that different sorts for malware need aid utilized within conjunction [9]. Collaboration also coordinated effort around cyber-criminals bring made wrongdoing designs that advance in show for developing technology and at clients about developing innovation organization would casualties. There will be also confirmation that cyber-criminals work clinched alongside geopolitically-identifiable bunches [10].

Malware is typically used to steal information that can be readily monetized, such as login credentials, credit card and bank account numbers, and intellectual property such as computer software, financial algorithms, and trade secrets [11]. Although many cyber-criminal groups are trafficking in commodities shared by multiple industry sectors, such as credit card numbers, there are some situations wherein a single company is obviously the target of a single adversary, whether it be an organized crime syndicate, nation-state, or a single operative [12]. For example, the work of a single nation-state adversary was evident to Google upon analysis of its 2009 cyber-attack. Just as information technology software tools and techniques have become more proficient, more effective and more economical over time and malware crime patterns have become more finely tuned [13].

## 2. MALWARE CLASSIFICATION

Malware might take concerning illustration numerous structures such as programming. It might deployed around desktops, servers, portable phones, printers and programmable electronic circuits [14]. Complex publicizing strike bring affirmed information camwood a chance to be stolen through elegantly composed malware residing just on framework memory without abandoning any foot shaped impression in the manifestation about constant information [15]. Basically, malwares can be classified into two categories such as Rootkit and Keylogger as shown in Table 1.

Table 1. Malware Classification

| Malware | Propagation | Infection | Self-Defence | Capabilities |
|---|---|---|---|---|
| Rootkit | Infected websites and/or installs on servers by hackers or insiders | Exploited trusted admin access, vulnerable browsers, or unpatched OS or application | Replacing OS kernel-level API routines | Collect data and impersonate user activity for entire machine and its interfaces |
| Keylogger | Infected websites and/or USB or other media | Vulnerable browsers or unpatched OS or application | Replace IO device drivers or APIs | Collect user keystrokes including credentials |

The Table 1 illustrated the malware classification through propagation, infection, self-defence and their capabilities. Malware has been known to incapacitate majority of the data securitycomponents for example, desktop firewalls and anti-virus projects [16]. A percentage considerably needs the capacity to subvert authentication, authorization and review capacities. It need arranged introduction files on support hold on in Indeed following a contaminated framework will be rebooted. Upon execution, complex malware might self-replicate or lie lethargic until summoned through its summon features should extricate information alternately eradicate files [17], [18].

## 3. MALWARE IN CYBER THREAT INTELLIGENCE

The digital risk sagacity analytics showcase will be developing quickly. Instruments such as Palantir Gotham and IBM i2 need aid utilized by discernment action investigators. Mostly, digital danger defenders for an everyday premise should help in the extraction of significant brainpower from limitless information collections comprised from claiming majority of the data acquired starting with a number divergent sources [19]. This may be attained by encouraging the revelation from claiming concealed inter-relationships the middle of cyber-artifacts, for example, components starting with organized organize logs, proxy Furthermore IDS systems, VPN, anti-virus, DLP, DNS queries. In addition, more provision logs are from relevant data such as like email, print logs, office get logs and inside talk logs, which are mankind's assets information [20], [21]. Malware analysis process has been presents by Figure 1.

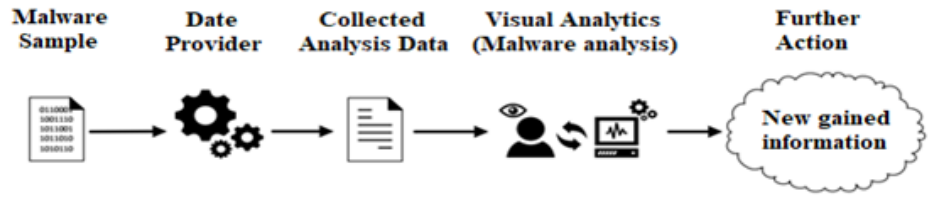


Figure 1. Malware analysis process

As shown in Figure 1 that presents the overall process flow of the malware analysis performed on malware sample. Computer helped enormous information visualization, which is a step towardsthe risk discernment action instruments facilitates revelation for associations between apparently inconsequential digital occasions and entities, and in addition the capacity to guide pernicious action should a normal root [22], [23]. To instance, programmed association finding in digital artifacts pulled from a corporate system under constant strike enabled security examiners should fast find at influenced machines. Furthermore to identify those foundation utilized by their attackers [20], [23], [24].

It is believed that malware has been extremely under-represented for digital danger brainpower. Malware give adequate methods to disclosure for inter-relationships around particular case. In turn like ID number from claiming concealed connections around malware empowers investigators to reason around whole malware battles[3, 8].Yet, this possibility need run generally undiscovered. For instance, concerning illustration of writing, it seems that those just malware majority of the data ordinarily contemplated something like for digital risk sagacity [24].

The reason for virus battle after that may be achieve state-of-theart malware analyses under the overlay of digital danger brainpower. So as will encourage this goal, three criteria must be met. Firstly, in artifacts from claiming malware suitableness for utilization over finding malware interrelationships must be distinguished[9, 25]. Second, malware analyses must make produced and utilized to naturally extricate these sorts of malware artifacts. Third, to every sort from claiming malware relic considered, versatile method for correlation must make created to use done finding malware interrelationships [7], [20], [25].

## 4. FORENSIC MALWARE ANALYSIS TOOLS

Each tool, we provide a short outline judgment describing, which of the systems starting with segment would actualized [7], [26], [27]. An exchange on the approaches, could be allowed avoidance techniques, In addition, more preferences over other methodologies may be provided. The investigation reports are also created eventually for the tools in this segment provide for an investigator important knowledge under movements performed by a test. These reports lay the establishment to a quick point by point comprehension of the test [3], [8], [28]. The section provides a review of the existing methodologies and tools that settle on utilization of those introduced strategies for forensic in malware investigation as shown in Figure 2.

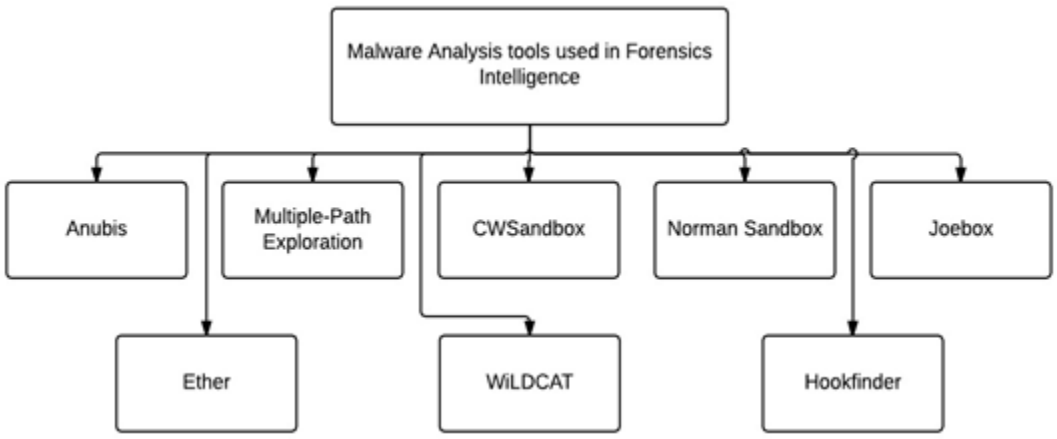


Figure 2. Forensic malware analysis tools

### 4.1. Anubis

The examination from claiming obscure binaries (Anubis) was introduced by Bayer et al. in 2006. Anubis executes the example under examination clinched alongside an emulated surroundings comprising of Windows XP working framework running as the guest over the Qemu (proposed by Bellard in 2005)[29, 30]. The investigation will be performed by checking the conjuring of Windows API functions and framework administration calls of the Windows local APIs [31]. The parameters passed should these capacities would analyse and followed. Since Anubis executes those investigated test to a completeWindows working system, it is imperative with concentrate on the operations that are executed ahead sake of the test and preclude operations that happen concerning illustration ordinary conduct of alternately different running forms[13]. At this point, Anubis makes utilization of the information that Windows assigns each running transform its identity or page registry.

The physical delivery of the page registry of the right now running procedure is continuously introduced in the CR3 CPU register. Thus, upon those conjuring of the broke down sample, Anubis records the quality of the CR3 registers and performs those dissections best for this procedure. By screening the APIs that would answerable for making new courses[32]. Anubis has the capacity should screen all techniques that need aid made by those first example. That loader might choose all load those library at an alternate deliver over the favoured base address. Thus, those genuine entrance purpose will be a main workunder those process' memory space. In addition, Anubis tracks the greater part invocations of the progressive loader in the connection of the test under investigation[33].

### 4.2. Multiple-Path Exploration

Programmed element malware-analysis tool produce their reports to indicate the absolute execution follow of the example under dissection. The utilization from claiming rationale bombs permits malware should main uncover its pernicious self-destructive considerations and conduct In view of discretionary imperatives [34]. For example, a malware example might postpone its pernicious exercises until a sure date will be arrived at or stop executing whether important files can't be discovered on the contaminated framework [35]. To succeed this shortcoming exhibit an instrument fit from claiming exploring different execution ways to Windows binaries. This tool distinguishes an expanding purpose at any point [35].

This approach extends Anubis that applies dynamic corrupt following to dissect how information come back starting with framework calls may be manipulated, which is compared eventually those transform under investigation. The framework calls would answerable for presenting those taint-labels handle-file framework [35]. At manipulating the quality upon resetting those framework states, uncommon forethought will be made. This implies that not just the worth straightforwardly included in the correlation must be changed. To attain this, the framework saves a set from claiming memory areas to each expanding perspective that relies on the compared quality joined together with a set of straight imperatives describing these dependencies. Throughout the situated of imperatives may be assessed. A demand solver to process the qualities that require on be substituted on power execution down alternate way. Whether a reliance cannot make displayed as a straight demand [36].

### 4.3. Cwsandbox

CWSandbox executes the example under dissection possibly natively alternately on a virtual Windows domain. Those examination purpose will be actualized works that perform the following on the API level[37]. Additionally, checking of the framework call interface may be actualized. The framework will be planned with catch those conduct ofmalicious programming specimens for admiration to file-system. In addition, registry manipulation, organize communication and working framework interactional [38].

The virtual framework is a full establishment from claiming aWin32-class working framework under, which has the capability to do the test under examination, may be executed with the dissection segments. API snaring may be performed toward changing those examples under examination also quickly as it is stacked under memory. Those connected snaring technological installs following the work that camwood perform those dissections previously, and then afterward each API brings. To this end, the malware procedure is began on the suspended state, implying that those example with every last one of libraries[32, 38]. It relies looking into would stacked on memory anyway no execution need taken put yet. Throughout the initialization, CWSandbox analyses the exported APIs work for stacked libraries[32].

A procedure could inquiry those working framework to running courses and in addition for stacked libraries. Since this data might uncover those vicinity of the investigation schemes. The CWSandbox applies rootkit systems will hiddenite the sum framework queries that might uncover the vicinity of the investigation skeleton starting with the transform under dissection [38], [39].

### 4.4. Norman Sandbox

Norman sandbox is a dynamic malware-analysis tool, which executes the test previously on the firmly regulated virtual surroundings that simulates a Windows working framework [38]. These surroundings will be used to mimic a host machine and also a connected neighbourhood and, should a portion extent, web connectivity. The centre clue behind the Norman sandbox may be to displace constantly on purpose needed toward an analysed test for a mimicked versify thereof [34]. The mimicked system needs the backup for operating system-relevant mechanisms such as memory security and multithreading help. Moreover, every last bit obliged APIs must have a chance to be introduce on provide for those test those fake feeling that it may be running on a true framework. A direct result those malware will be executed in a mimicked system, stuffed alternately obfuscated executables don't ruin the examination itself [40].

Norman sandbox concentrates on the identification of worms that spread by means of email alternately P2P networks, and also infections that attempt to replication over system greater part. Previously a nonexclusive malware-detection procedure tries should catch other pernicious product. The Norman sandbox gives a mimicked surroundings of the example under investigation comprising of uniquely designed variants about user-land APIs fundamental for executing the test [40]. The works giving work to these APIs need aid intensely instrumented with those comparing investigation abilities. To stay with those reproductions self-contained, these reinstatement APIs do not perform any associations with the imaginable execution of the genuine framework. Uncommon consideration is brought with admiration to systems administration APIs. At systems administration solicitations issued toward the test under investigation are redirected to mimic parts to test the SMTP server with send email. The association endeavour with TCP/IP port 25 will be detectedas opposed to opening an association of the genuine server and the association is redirected should a recreated mail server [40], [41].

### 4.5. Joebox

Throughout those progressive examination of a conceivably pernicious sample, Joebox makes a log that holds high-keyed majority of the data of the performed activities in regards file-system, registry and framework exercises [42]. Joebox is particularly outlined on run on genuine hardware, not relying ahead any virtualization or copying system. The framework will be intended concerning illustration a client-server model clinched alongside which is an absolute controller example camwood coordinate numerous customers that are answerable for performing the dissection [42]. Thus, it may be clear on build those throughput of the complete framework toward including additional examining customers of the framework [43]. Joebox captures user-mode API calls and system-call invocations. Each library gives work to the API, which holds a word reference name. The directoryknown as the fare deliver table used to queried toward a procedure that wishes should bring a work in that library [36], [44].

### 4.6. Ether: Malware Analysis Via Hardware Virtualization Extensions

Dinaburg et al. in 2008 recommended a transparent malware-analysis skeleton in the reference fittings virtualization. They inspires the existent examination instruments endure starting with detectability issues that permit pernicious code should identify [45]. Ether's transparency property comes from the reality that it will be executed for a hypervisor resides over a higher benefit level over the monitored guest working framework [46]. Ether helps to observe the executed instructions, memory writes, and framework calls. Furthermore, Ether gives instruments to the Windows XP versify will limit the investigation for a particular procedure main. This strategy best meets the expectations of framework calls through SYSENTER direction [20], [46].

### 4.7. Wildcat

WiLDCAT is a structure to coarse- fine-grained malware investigation. It comprises of various segments that actualize all the stealth breakpoints, double defiant. The improvements of stealth breakpoints may be inspired toward the perception that huge numbers malware specimens utilize code confirmation alternately dynamic code generation, which renders product breakpoints pointless[47]. Vampire executes breakpoints setting the not-present banner of the memory page holding the direction book on which it break [48]. A page-fault handler is introduced that handle the shortcoming, which rose in the direction book about that page may be executed. Assuming those direction books triggered those flaw line matches with memory area of the breakpoint, vampire stops execution. Joined together with a debugger, this framework might a chance to be used in single-step through those provision starting with the side of the point around [49]. The most recent part for theWiLDCAT is cobra, which is an arrangement that helps confined executions. An essential piece will be an arrangement of educational that is possibly ended for a control flow-modifying direction book or the point when a sure greatest period may be arrived [48, 49].

### 4.8. Hookfinder

A malware gathers data from a contaminated system, it will be vital from an attacker's perspective that happens in a stealthy manner, so as with avoid identification. Commonly, pernicious programs such as spyware or rootkits, insert snares under the framework with be notified when occasions from claiming their enthusiasm [50]. For example, a keylogger to theWindows nature's domain could make a snare utilizing those SetWindowHookEx API functions, which is notified at present point. Hookfinder may be an arranged skillof identifying such snaring strategies and produces reports around the place these attacks[36].Hookfinder executes toward utilizing information and deliver anti-tracking systems over a changed rendition of the Qemu full-system emulator. All memory areas composed the methodology under examination need to be tainted and in addition, the obtained corrupt status may be propagated through those frameworks[36]. Also similarly as with display, Hookfinder utilizes a portion module that executes in the emulated working framework will span semantic hole. This module may be answerable for gathering those vital high-keyed data (such as stacked libraries, presently executing process, and so on) and conveying the information of the underlying dissection framework [51], [52].

## 5. CONCLUSION AND FUTURE WORK

In this paper, we described various malware detection and analysis tools based on API call sequences and opcode sequences. This paper provides an interesting review of the existing approaches to make the clear understanding. Future work could include a similar analysis involving additional features beyond API calls and opcodes. A comparisonofscoringtechniquesotherthangraphbased scores, structural scores, other machine learning and statistical scores and optimal combinations of static and dynamicscores like SupportVectorMachineswould beworthwhile.Finally, amorein-depthanalysisofimbalance issues in this context might prove interesting.

## ACKNOWLEDGEMENTS

The authors cordially thank the Uttaranchal University, Dehradun, INDIA for supporting this work.

## REFERENCES

[1] Distler, D. and C. Hornat, "Malware analysis: An introduction," SANS Institute InfoSec Reading Room, pp. 18-19.2007.
[2] Ligh, M., et al., "Malware analyst's cookbook and DVD: tools and techniques for fighting malicious code", Wiley, 2010.
[3] Taylor, R.W., E.J. Fritsch, and J. Liederbach, "Digital crime and digital terrorism," Prentice Hall Press, 2014.
[4] Sikorski, M. and A. Honig, "Practical malware analysis", William Pollock, San Francisco, CA, 2012.
[5] Burguera, I., U. Zurutuza, and S. Nadjm-Tehrani "Crowdroid: behavior-based malware detection system for android" 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices, 2011.
[6] Casey, E., "Digital evidence and computer crime", Elsevier book of Forensic science, computers, and the Internet, 2011.
[7] Malin, C.H., E. Casey, and J.M. Aquilina, "Malware forensics: investigating and analyzing malicious code", Elsevier Syngress, 2008.
[8] Li, F., A. Lai, and D. Ddl, "Evidence of Advanced Persistent Threat: A case study of malware for political espionage", 6th IEEE International Conferenc on Malicious and Unwanted Software (MALWARE) , 2011.
[9] Ligh, M.H., et al., "The art of memory forensics: detecting malware and threats in windows, linux, and Mac memory," ACM Digital Library, John Wiley & Sons, 2014.
[10] Hunt, R. and S. Zeadally," Network forensics: an analysis of techniques, tools, and trends," IEEE Xplore Digital Libraray, pp. 36-43, 2012.
[11] Vural, I. and H. Venter," Mobile botnet detection using network forensics," ACM Digital Library- Future Internet-FIS 2010, pp. 57-67, 2010.
[12] Malin, C.H., E. Casey, and J.M. Aquilina," Malware Forensics Field Guide for Windows Systems", Elsevier Digital Forensics Field Guides, 2012.
[13] Provataki, A. and V. Katos, "Differential malware forensics", Elsevier Digital Investigation, pp. 311-322, 2013.
[14] Nataraj, L., et al., "A comparative assessment of malware classification using binary texture analysis and dynamic analysis",4th ACM Workshop on Security and Artificial Intelligence, 2011.
[15] Yan, G., N. Brown, and D. Kong,"Exploring discriminatory features for automated malware classification", Springer International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, 2013.
[16] Dilek, S., H. Çakır, and M. Aydın, "Applications of artificial intelligence techniques to combating cyber crimes: A review", International Journal of Artificial Intelligence & Applications, Vol. 6, No. 1, January 2015.
[17] Rad, B.B., M. Masrom, and S. Ibrahim "Opcodes histogram for classifying metamorphic portable executables malware", IEEE International Conference on e-Learning and e-Technologies in Education (ICEEE), 2012.

[18] Elizondo, D., A. Solanas, and A. Martinez-Balleste, "Computational Intelligence for Privacy and Security", Springer Book, Vol. 394, , 2012.
[19] Lee, K.-C., et al., "Sec-Buzzer: cyber security emerging topic mining with open threat intelligence retrieval and timeline event annotation", Springer Soft Computing Book, pp. 2883-2896, 2017.
[20] Miles, C., et al.,"VirusBattle: State-of-the-art malware analysis for better cyber threat intelligence", 7th IEEE International Symposium on Resilient Control Systems (ISRCS), 2014.
[21] Riccardi, M., "Applying intelligence analysis while attributing cyber attacks", research gate publications, 2016.
[22] Pahi, T., M. Leitner, and F. Skopik " Analysis and Assessment of Situational Awareness Models for National Cyber Security Centers", in ICISSP-University College, Dublin, Ireland, 2017.
[23] Jones, P.H. and K.M. Dye, "4-D COMMON OPERATIONAL PICTURE (COP) FOR MISSION ASSURANCE (4D COP) Task Order 0001", Air Force Research Laboratory (AFRL) Autonomy Collaboration in Intelligence, Surveillance, and Reconnaissance (ISR), Electronic Warfare (EW)/Cyber and Combat Identification (CID), Dialogic Design International Dayton United States, 2016
[24] Mandt, E.J.," Integrating cyber intelligence analysis and active cyber defense operations", Utica College, 2015.
[25] Carrier, B., "File system forensic analysis", Addison-Wesley Professional, 2005.
[26] Garfinkel, S.L., "Digital forensics research: The next 10 years", Elsevier digital investigation, pp. S64-S73, 2010.
[27] Petroni, N.L., et al., "FATKit: A framework for the extraction and analysis of digital forensic data from volatile system memory", Elsevier Digital Investigation, pp. 197-210, 2016.
[28] Egele, M., et al., "A survey on automated dynamic malware-analysis techniques and tools",ACM computing surveys (CSUR), pp. 6, 2012.
[29] Aminnezhad, A., A. Dehghantanha, and M.T. Abdullah, "A survey on privacy issues in digital forensics" International Journal of Cyber-Security and Digital Forensics (IJCSDF), pp. 311-323, 2012.
[30] Sanz, B., et al., "Puma: Permission usage to detect malware in android", Springer International Joint Conference CISIS'12-ICEUTE´ 12-SOCO´, 2013.
[31] Wagner, M., et al., "A survey of visualization systems for malware analysis" in EG Conference on Visualization (EuroVis)-STARs, 2015.
[32] Dai, S.Y., et al., "Holography: a behavior-based profiler for malware analysis", Software: Practice and Experience, pp. 1107-1136, 2012.
[33] Edem, E.I., et al., "Analysis of Malware Behaviour: Using Data Mining Clustering Techniques to Support Forensics Investigation", IEEE Cybercrime and Trustworthy Computing Conference (CTC), 2014.
[34] Choi, Y.H., et al., "Toward extracting malware features for classification using static and dynamic analysis", IEEE 8th International Conference on Computing and Networking Technology (ICCNT), 2012.
[35] Vidyarthi, D., et al., "Malware Detection by Static Checking and Dynamic Analysis of Executables", International Journal of Information Security and Privacy (IJISP), pp. 29-41, 2017.
[36] Gandotra, E., D. Bansal, and S. Sofat, "Tools & Techniques for Malware Analysis and Classification", International Journal of Next-Generation Computing, 2016.
[37] Huang, H.-D., et al.,"Applying FML and fuzzy ontologies to malware behavioural analysis", IEEE International Conference on Fuzzy Systems (FUZZ), 2011.
[38] Huang, H.-D., et al., "Malware behavioral analysis system: TWMAN", IEEE Symposium on Intelligent Agent (IA), 2011.
[39] Benenson, Z., et al., "Exploring the Landscape of Cybercrime", First IEEE Workshop on SysSec, 2011.
[40] Bhatkar, S.B., S. Nanda, and J.S. Wilhelm, "Techniques for behavior based malware analysis", Google Patents, 2013.
[41] Hoopes, J., "Virtualization for security: including sandboxing, disaster recovery, high availability, forensic analysis, and honeypotting," Springer Syngress, 2009..
[42] Vokorokos, L., Z. Dankovičová, and L.u. Leščišin,"Using of the forensic analyzing tools, code obfuscation," IEEE 15th International Symposium on Applied Machine Intelligence and Informatics (SAMI), 2017.
[43] Iqbal, M.S. and M. Sohail, "Runtime Analysis of Malware", School of Computing, Blekinge Institute of Technology, 2011.
[44] McDougal, M.D., W.E. Sterns, and R.S. Jennings, "System and method for malware detection using multiple techniques", Google Patents, 2015.
[45] Garfinkel, S. Anti-forensics, "Techniques, detection and countermeasures. in 2nd International Conference on i-Warfare and Security, http://www.simson.net/ref/2007/ICIW.pdf.
[46] Ahmed, I., et al., "Scada systems: Challenges for forensic investigators", IEEE Computer, pp. 44-51, 2012.
[47] VILCHEZ, S.D.L.S., et al., "Computer implemented method for classifying mobile applications and computer programs", Google Patents, 2015.
[48] Anderson, R., "Risk and Privacy Implications of Consumer Payment Innovation in the Connected Age", Consumer Payment Innovation, pp. 99, 2012.
[49] Weiss, D.R., "Handling Bad: Inside a Cyber Era Private Investigative Firm", Advantage Media Group, 2015.
[50] Ramani, R.G., S.S. Kumar, and S.G. Jacob., "Rootkit (malicious code) prediction through data mining methods and techniques", IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), 2013.
[51] Wang, C.-W., et al.," MrKIP: Rootkit Recognition with Kernel Function Invocation Pattern," J. Inf. Sci. Eng., pp. 455-473, 2015.
[52] Xie, X.,"Security Improvement in Cloud Computing Environment through Memory Analysis", The University of North Carolina at Charlotte, 2017.

[53] Luis Miguel Acosta-Guzman, et al., "Network Activity Monitoring Against Malware in Android Operating System," International Journal of Electrical and Computer Engineering (IJECE), Vol 6, No 1, February 2016.
[54] Zahra Hakimi, Karim Faez, Morteza Barati, " A Flow-based Distributed Intrusion Detection System Using Mobile Agents", International Journal of Electrical and Computer Engineering (IJECE), Vol 3, No 6: December 2013.
[55] Alhamza Alalousi, et al.," A Preliminary Performance Evaluation of K-means, KNN and EM Unsupervised Machine Learning Methods for Network Flow Classification,"International Journal of Electrical and Computer Engineering (IJECE), Vol 6, No 2: April 2016.

## BIOGRAPHIES OF AUTHORS

Tarun Kumar is the Ph.D Scholar in computer science at Uttarkhand Technical University, Dehradun. He is working as research scholar under the guidance of Dr. Parag Jain, Professor Roorkee Institute of Technology, Roorkee. His areas of research are Malware Forensics and Moble Adhoc networks.

Sanjeev Sharma is the Assistant Professor in Computer Science Department at Uttaranchal University, Dehradun. His areas of research are Malware Forensics and Image Processing.

Ravi Dhaundiyal is the Assistant Professor in Computer Science Department at Uttaranchal University, Dehradun. His areas of research are Security and Image Processing.

Dr. Parag Jain is the Professor in Computer Science Department at Uttarakhand Technical University and Ph.D in Computer Science. He has the distinction of working as a research scholar under the guidance of internationally acclaimed emeritus Prof. Dr. S.C. Gupta, ex Professor Indian Institute of Technology, Roorkee. His areas of research are Cloud Computing and Security.