January – February 2020
ISSN: 0193-4120 Page No. 13757 – 13764

A Walkthrough of Digital Forensics and its Tools

Bhawna Narwal[1], Nimisha Goel[2]

[1,2]Department of IT, Indira Gandhi Delhi Technical University for Women (IGDTUW), Delhi, India
[1]bhawnanarwal@igdtuw.ac.in, [2]goelnimisha1@gmail.com

Article Info
Volume 82
Page Number: 13757 – 13764
Publication Issue:
January-February 2020

Article History
Article Received*: 18 May 2019*
Revised*: 14 July 2019*
Accepted*: 22 December 2019*
Publication*: 24 February 2020*

Abstract

The accelerated pace in technological advances and pervasive usage of digital assets has manifested the value of Digital Forensics. The operations of global phenomena are confronting a risk of exposure and threats from cyber penetrators as they are posing challenges towards everyone through anti-forensic techniques. This requires effective process and specialized digital forensics tools to acquire digital evidences to serve as an aid to justice. This paper provides a brief on digital forensics process, its evaluation metrics, and proposes a taxonomy of digital forensics tools which provides a detailed overview and comparison among different forensics tools based on different features in their categories. Furthermore, we identified several indispensable challenges in this fascinated area.

Keywords; *Digital Evidence, Digital Forensics, Digital Forensics Tools, Information Security*

I. INTRODUCTION

The technical advances in digital technology has brought advantages to the mankind as the evolution has greatly contributed in providing smooth conduct of business, comfortable life and streamlined processes which has automated thanks to such advances. Consequently, the technical development comes at the cost of breach in security of information stored or exchanged digitally. The dramatic rise in digital technology gives rise to new avenues for digital penetrators to devise new and sophisticated attack methods in order to bypass security defense, trap the victim and breach the security setups. Across the globe, digital attacks performed by these determined cyber penetrators have impacted huge masses and nagged billions of dollars [1]. Almost every corporate and organization is spending huge amount in safeguarding their digital assets and to avoid being victim of the attacks. The emergence of digital crimes and dependence on technology has lead to the development of Digital Forensics which acts as an armor in this battlefield. The intervention of Digital Forensics is paramount as the forensic process and multitude of tools provided a streamlined manner to extract evidence and provides a way to combat and protect from numerous cyber crimes [2]. The more agile and automated forensic process gives us the tools we require to investigate the extracted evidence to make it admissible to the court. The data storage platforms varies from computers, IoT, database, email, network, mobile, memory and cloud and for the better extraction and investigation of these storage platforms different tools are needed. To serve this purpose we proposed a taxonomy of digital forensics and further extending this we described in detail each category in the taxonomy [54-58].

Published by: The Mattingley Publishing Co., Inc.

January – February 2020
ISSN: 0193-4120 Page No. 13757 – 13764

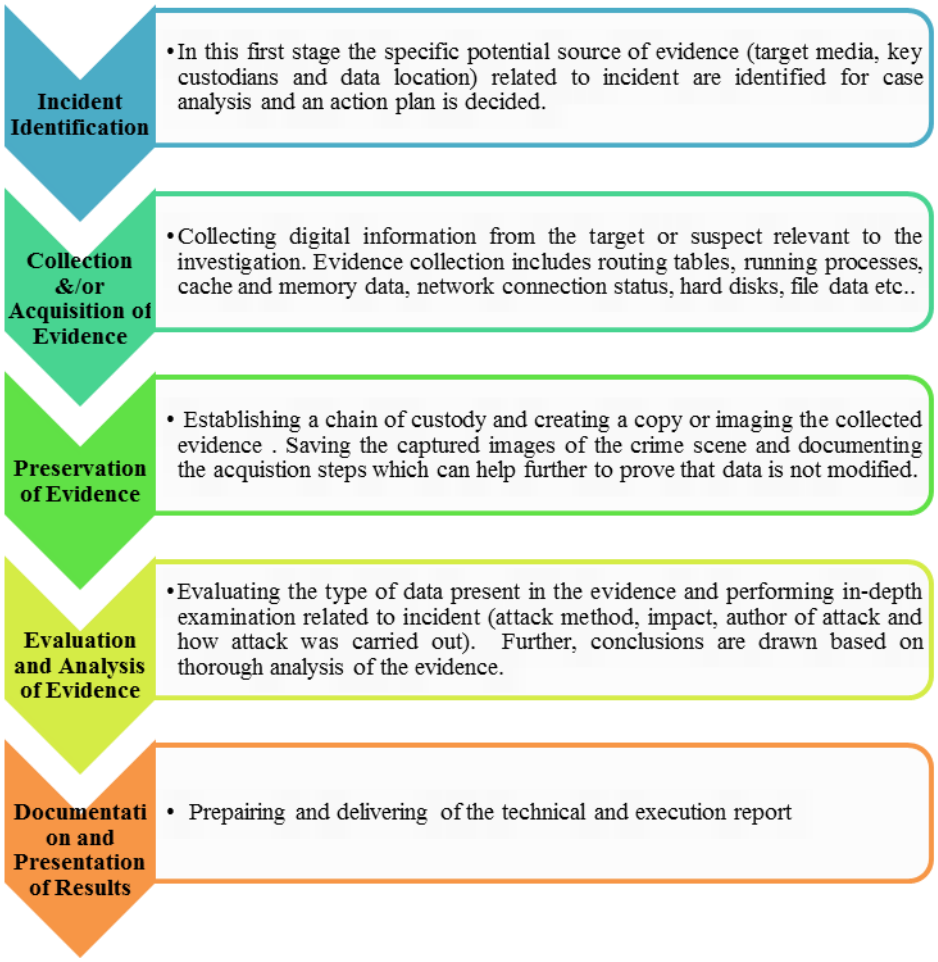

Fig. 1. Digital Forensic Process

II. EVALUATION METRICS FOR DIGITAL FORENSICS TOOLS

For validation of forensics tools it is important to assess them based on the evaluation metrics which can help community to select the tool with no bias and can help the vendors knowing the scope of improvement. These evaluation metrics cover all properties that can help in judging the capacity of the tool [3].

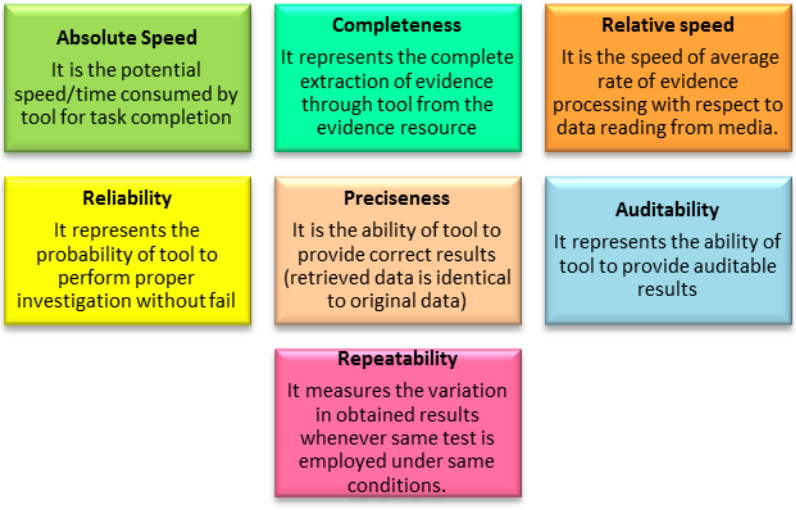

Fig. 2. Seven Evaluation Metrics for Digital Forensics Tools

Published by: The Mattingley Publishing Co., Inc.

January – February 2020
ISSN: 0193-4120 Page No. 13757 – 13764

III. DIGITAL FORENSICS TOOLS CHALLENGES

• Encryption

•Volume of Investigation data

• Evidence Size and its volatility

• Remarkable growth and sophistication in digital crimes

• Legal Issues (Jurisdiction, Privacy, Legal Process, Acceptability of forensics tools and mechanisms)

• Proliferation in digital media types and their life span

• Anti Digital Forensics

• Scarcity of Resources

• Emerging technologies, applications and devices

• Shortage of trained and certified personnel

•Incompatibility or automation absence among varied forensics tools

• Ethical Issues

• Trust in the Audit Process

• Manual Interventions

• Lack of Standardization

• Testing and Validation

• Malicious Programs

IV. TAXONOMY OF DIGITAL FORENSICS

A Taxonomy of Digital Forensics is highlighted through Figure 3 and detailed explanation of different types of Digital forensics is provided in following sub-sections where ✓ means supported feature, × means non-supported, W stands for Windows, M stands for MAC OS, L stands for Linux, A stands for Android, I stands for iOS, BB stands for BlackBerry and U stands for Unix.

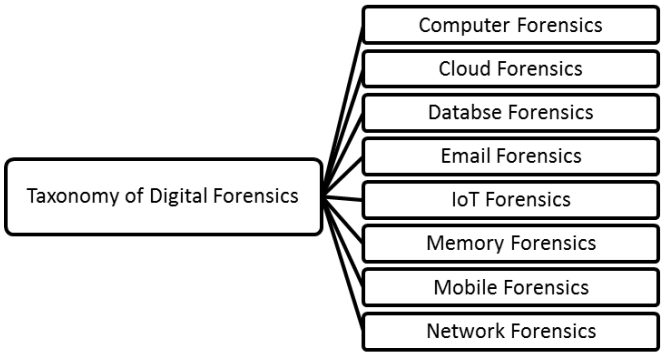

Fig. 3. Taxonomy of Digital Forensics

4.1 Computer Forensics and its Tools

Computer forensics is a vital form of digital forensics which investigates the evidential information extracted from computing devices, networks, storage elements and wireless communication and later analyzes it and preserves it for making it admissible in the court. The investigation is aimed towards collection of latent data. The tools are used to extract deleted data, password cracking, keyword searches, evaluation of windows registry and physical file data construction. The tools used for performing Computer Forensics with their features are highlighted in Table 1.

Table 1. Computer Forensics Tools

Features/Tool	Internet Evidence Finder [4]	X-Way Forensics [5]	FTK Imager [6]	EnCase [7]	The Sleuth Kit [8]	Helix [9]	Live View [10]
Identifying threats	✓	✓	✓	✓	✓	✓	×
User-friendly GUI	✓	✓	✓	✓	✓	×	✓
Protocols support like HTTP/POP	×	×	×	✓	✓	✓	×
Decryption for password recovery	✓	✓	✓	✓	✓	✓	✓
Data visualization	✓	✓	✓	✓	✓	✓	✓
Hash databases	✓	✓	✓	✓	✓	×	×
Supported Platforms	W/M	W	W	L	W /L	W /L	W /L

Published by: The Mattingley Publishing Co., Inc.

January – February 2020
ISSN: 0193-4120 Page No. 13757 – 13764

4.2 Cloud Forensics Tools

Cloud Forensics Tools perform investigation on Cloud i.e. forensic acquisition of cloud. The tools perform data acquisition only on the area where some false action has been performed (to collect evidence against attacker) as data on cloud is stored in logical pools which spans multiple servers containing vast and humongous amount of data. The tools can extract data from API logs, virtual disks, guest firewall logs, private social media accounts, mails, user location, etc. The tools used for performing Cloud Forensics with their features are highlighted in Table 2.

Table 2. Cloud Forensics Tools

Features/Tools	FROST[11]	UFED Cloud Analyzer[12]
Extraction of data from OpenStack cloud	✓	×
Compatibility with forensic formats	✓	✓
Infrastructure-as-a-Service (IaaS)	✓	×
Data sharing	✓	✓
Supported Platform	W	W

4.3 Database Forensics Tools

Database Forensics tools involve extraction and investigation of databases and their related metadata, where the tools after a critical failure/attack inspect changes in hard disk, perform kernel recovery (lost tables, stored procedures, quick scan, tracing of files, views and keys). The tools can recover deleted, damaged and hidden data. In addition to this, file comparing, disk cloning, file encryption and checksum creation are some of the features provided by these tools. The tools used for performing Database Forensics with their features are highlighted in Table 3.

Table 3. Database Forensics Tools

Features/Tools	IDEA[13]	ACL Audit exchange [14]	Arbutus[15]	SQL CMD [16]	Windows Forensic Toolchest [17]	Systools SQL Log Analyzer [18]
Data analysis	✓	✓	✓	✓	✓	✓
Visualization of data	✓	✓	✓	×	✓	×
Read only access	✓	✓	✓	✓	✓	✓
Audits	✓	✓	✓	×	✓	✓
SQL support	✓	✓	✓	✓	✓	✓
Supported platforms	W	W	W	W	W	W

4.4 Email Forensics Tools

Email forensics tools offer diverse and detailed information related to source and content of Email. To investigate the attacker's intent behind the attack, these tools helps in tracing the path followed by the email, its source and destination, sent and receipt date and time, transaction details, and are able to locate the phishing and spam networks. To extract the aforesaid information there is a need to perform header analysis, bait tactics, keyword searching, port scanning, sender mailer fingerprint identification etc. The tools used for performing Email Forensics with their features are highlighted in Table 4.

Table 4. Email Forensics Tools

Features/Tools	MailXaminer [19]	eMailTracker Pro [20]	EmailTracer [21]	Adcomplain [22]	Add4Mail Forensic [23]	AbusePipe [24]	Final eMail [25]	Paraben (Network) E-mail Examiner[26]	Forensics Investigation Toolkit (FIT) [27]
Analysis and investigation of e-mails	✓	✓	✓	✓	✓	✓	✓	✓	✓
Abuse Reporting	×	✓	×	✓	✓	✓	×	✓	×
Spam filter	✓	✓	×	✓	✓	✓	×	✓	×

Published by: The Mattingley Publishing Co., Inc.

January – February 2020
ISSN: 0193-4120 Page No. 13757 – 13764

Recovery of lost e-mails and databases	✓	×	✓	×	✓	×	✓	✓	✓
Boolean searching	✓	×	✓	×	✓	×	×	✓	✓
Export format support	✓	✓	✓	✓	✓	✓	×	✓	✓
Visualisation support	✓	✓	×	×	×	✓	✓	×	✓
Platforms supported	W/M	W	Content analysis	U/W	L/W/M	W/M/U	W/L	W	W

4.5 IoT Forensics Tools

The IoT forensics tools involves investigation of vast real time data collected from crime scene which involves variety of smart and communication capable IoT devices such as home appliances, embedded systems, mobile devices, sensors, etc. The area of region covered by these devices in the crime scene could be LAN, MAN, WAN or PAN. These tools after context establishment perform data, file and images extraction which is further followed by its investigation, analysis and reporting. The tools used for performing IoT Forensics with their features are highlighted in Table 5.

Table 5.IoT Forensics Tools

Features/Tools	Bulk Extractor [28]	CAINE [29]	NUIX [30]	RegRipper [31]	Pajek64 [32]
Scanning and extraction of information	✓	✓	✓	✓	×
Analysis of forensic images, data and files	✓	✓	✓	✓	✓
GUI Support	✓	×	✓	×	✓
Windows registry files	×	×	✓	✓	×
Supported Platforms	W/L/M	L/W/ U	W/ M/ L	W/ L	W/ M

4.6 Memory Forensics Tools

Memory Forensics Tools involves investigation of current status of system's memory/memory dump. The memory dump is captured (volatile information) to form a real time image of the system which is later analyzed for investigation. This file contains information about running processes, running exe files, file related information, logged in users, network related information, user activity, timestamp comparison and decoded applications in memory. For live acquisition Process Hacker, Helix ISO etc. tools can be used. The tools used for performing Memory Forensics with their features are highlighted in Table 6.

Table 6. Memory Forensics Tools

Features/Tools	Memoryze [33]	Belkasoft RAM Capturer [34]	Volatility Suite [35]	Windows SCOPE [36]	Rekall [37]
Live Acquisition	✓	✓	✓	✓	✓
Memory Image acquisition	✓	×	✓	✓	✓
Find Physical Address	×	×	✓	✓	×
Find Virtual Address	✓	×	✓	✓	×
Running Processes	✓	×	✓	✓	×
Malware detection	×	✓	✓	×	×
GUI Support	×	×	×	✓	✓
Command Line Support	✓	✓	✓	×	×
Paging file Inclusion	✓	×	×	×	×
Reporting device and driver layering	✓	×	×	×	×
Verify digital signature	✓	×	×	×	×
Images full system memory	✓	×	✓	✓	✓
Enumerating Running Processes	✓	×	✓	✓	×
Listing Network Sockets	✓	×	✓	✓	×
Bypass Active Anti-Debugging and Anti-Dumping Protection	×	✓	×	×	×
Analyze rootkits	✓	×	✓	×	×
Supported Platform	W	W	W/ L/ M/A	W	W

Published by: The Mattingley Publishing Co., Inc.

TEST Engineering & Management

January – February 2020
ISSN: 0193-4120 Page No. 13757 – 13764

4.7 Mobile Forensics Tools

Mobile Forensics deals with the potential recovery of digital evidence from different sources of mobile device (mobile phones, PDAs, GPS devices, Tablets) such as SIM card, SD card and Handset memory. The forensic process of a mobile device involves following stages: seizure, identification, acquisition, examination and reporting. The evidences such as contact list, messages (SMS and MMS), photos, videos, emails, notes, location information, social networking sites related and web browsing information are acquired using any of the data acquisition technique such as physical, manual, brute force and logical. The tools used for performing Memory Forensics with their features are highlighted in Table 7.

Table 7. Memory Forensics Tools

Features/Tools	MOBILed It Forensic Express [38]	Cellebrite UFED Ultimate [39]	Paraben E3:DS Mobile Forensic [40]	Secure View APEX [41]	Micro Systemation XRY/XACT [42]	Oxygen Forensic Suite [43]
Screen Lock Disabler	✓	✓	✓	✓	✓	✓
Password and PIN breaker	✓	✓	✓	×	✓	✓
Data Reports	✓	✓	✓	✓	✓	✓
Call Logs	✓	✓	✓	✓	✓	✓
Messages	✓	✓	✓	✓	✓	✓
User Data	✓	✓	✓	✓	✓	✓
Application Data	✓	✓	✓	✓	✓	✓
Internet Data	✓	✓	×	×	✓	×
Social Networking Data	✓	✓	`×	×	✓	✓
GPS data	✓	✓	✓	×	✓	✓
Drone Data	×	✓	✓	×	✓	✓
Cloud Data	✓	✓	✓	×	✓	✓
Keyword Search	✓	✓	✓	✓	✓	✓
IoT device support	×	×	✓	✓	×	✓
Organizer	✓	×	×	×	×	✓
Deleted data Recovery	✓	✓	×	✓	✓	✓
Logical Acquisition	✓	✓	✓	×	✓	✓
Physical Acquisition	✓	✓	✓	✓	✓	×
Hex Viewer	×	✓	✓	×	✓	✓
SQLite Databases	✓	✓	✓	✓	×	✓
GUI Support	✓	✓	✓	✓	✓	✓
Command Line support	×	×	×	×	×	×
Organizer	✓	✓	×	×	✓	✓
Timeline Support	✓	✓	✓	×	×	✓
Live Data Extraction	×	✓	✓	×	✓	✓
Backup and Image import	✓	✓	✓	×	✓	✓
Malware detection	✓	×	✓	×	×	✓
Supported Platform	W	i/A	A/i/ BB/ W	i	A/i	A/ W/ BB/ i, S

4.8 Network Forensics Tools

Network forensics is a new area in Digital Forensics that discovers, monitors and analyzes the network traffic and its events for gathering information, tracking communication, identifying intrusions, anomalous behavior in traffic and source of attack. This pro-active investigation is performed either standalone or along with computer forensics process. The harvested information from the suspected network traffic needs to follow legal and technical aspects as well as general forensic aspects.

The tools used for performing Network Forensics with their features are highlighted in Table 8.

Table 8. Network Forensics Tools

Features/Tools	Network Miner [44]	Wireshark [45]	Security Onion [46]	NetVCR [47]	Xplico [48]	OmniPeek [49]	NIKSUN Netdetector [50]	Stenographer [51]	DSHELL [52]	Password Sniffer Console [53]
Intrusion detection	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

TEST Engineering & Management

January – February 2020
ISSN: 0193-4120 Page No. 13757 – 13764

Network Security monitoring	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Log management	✓	×	✓	✓	✓	✓	✓	×	×	✓
Offline analysis	✓	✓	✓	✓	✓	✓	✓	×	×	✓
Display Filters	✓	✓	✓	✓	×	✓	✓	×	×	×
GUI based	✓	✓	✓	✓	✓	✓	✓	✓	×	✓
Command Line based	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Full packet capture using WinPcap	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IPv4 and IPv6 support	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
VoIP call extraction	✓	✓	✓	✓	✓	✓	✓	×	×	✓
HTTP content extraction	✓	✓	✓	✓	✓	✓	✓	×	✓	✓
FTP login extraction	✓	✓	✓	✓	✓	✓	✓	×	×	✓
Web login extraction	✓	✓	✓	✓	✓	✓	×	×	✓	✓
Email extraction	✓	✓	✓	×	✓	✓	✓	×	×	✓
Supported Platform	W/L/M	W/L/M/U	L	W/L/U	L/W	W	W/L	W/L/U	L	W

V. CONCLUSION

The dramatic rise in digital technology gives rise to new avenues for digital penetrators to devise new and sophisticated attack methods in order to bypass security defense, trap the victim and breach the security setups. Across the globe, digital attacks performed by these determined cyber penetrators have impacted huge masses and nagged billions of dollars. The emergence of digital crimes and dependence on technology has lead to the development of Digital Forensics which acts as an armor in this battlefield. This paper provides a brief on digital forensics process, its evaluation metrics, and proposes a taxonomy of digital forensics tools which provides a detailed overview and comparison among different forensics tools based on different features in their categories. Furthermore, we identified several indispensable challenges in this fascinated area.

REFERENCES

1. Cameron, L. (2018). Future of digital forensics faces six security challenges in fighting borderless cybercrime and dark web tools.
2. Watson, S., &Dehghantanha, A. (2016). Digital forensics: the missing piece of the internet of things promise. Computer Fraud & Security, 2016(6), 5-8.
3. Baig, Z. A., Szewczyk, P., Valli, C., Rabadia, P., Hannay, P., Chernyshev, M., ... & Syed, N. (2017). Future challenges for smart cities: Cyber-security and digital forensics. Digital Investigation, 22, 3-13.
4. https://www.teeltech.com/mobile-device-forensic-tools/magnet-forensics/magnet-internet-evidence-finder-ief/
5. http://www.x-ways.net/forensics/
6. https://accessdata.com/product-download/ftk-imager-version-3-2-0
7. https://www.guidancesoftware.com/encase-forensic
8. https://www.sleuthkit.org/
9. https://www.e-fense.com/products.php
10. http://liveview.sourceforge.net/
11. Josiah Dykstra, Alan T. Sherman, Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform, Digital Investigation, Volume 10, Supplement, 2013, Pages S87-S95, ISSN 1742-2876, https://doi.org/10.1016/j.diin.2013.06.010.
12. https://www.cellebrite.com/en/ufed-cloud-analyzer/
13. https://idea.caseware.com/products/idea/
14. https://www.acl.com/
15. https://www.arbutussoftware.com/products-solutions/fraud-detection

January – February 2020
ISSN: 0193-4120 Page No. 13757 – 13764

16. https://docs.microsoft.com/en-us/sql/tools/sqlcmd-utility?view=sql-server-ver15
17. http://www.foolmoon.net/security/wft/
18. https://www.systoolsgroup.com/sql-log-analyzer.html
19. https://www.mailxaminer.com/
20. http://www.emailtrackerpro.com/
21. http://www.cyberforensics.in/Products/emailtracer.aspx?AspxAutoDetectCookieSupport=1
22. http://www.rdrop.com/users/billmc/adcomplain.html
23. https://www.aid4mail.com/email-forensics
24. https://www.datamystic.com/abusepipe
25. http://finalemail.findmysoft.com/
26. https://paraben.com/email-forensics-emx/
27. http://www.edecision4u.com/FIT.html
28. https://dfir.training/dfirtools/tools/misc/273-bulk-extractor
29. https://www.caine-live.net/
30. https://www.nuix.com/
31. https://tools.kali.org/forensics/regripper
32. https://sites.google.com/site/shamshuritawati/home/pajek
33. https://www.fireeye.com/services/freeware/memoryze.html
34. https://belkasoft.com/ram-capturer
35. https://www.volatilityfoundation.org/24
36. http://www.windowsscope.com/windowsscope-cyber-forensics/
37. http://www.rekall-forensic.com/documentation-1/rekall-documentation/rekall-at-a-glance
38. https://www.mobiledit.com/forensic-express
39. https://www.cellebrite.com/en/products/ufed-ultimate/
40. https://paraben.com/mobile-forensics-software/
41. https://www.secureview.us/apex.html
42. https://www.msab.com/products/xry/
43. https://www.oxygen-forensic.com/en/
44. https://www.netresec.com/?page=NetworkMiner
45. https://www.wireshark.org/
46. https://securityonion.net/
47. https://www.phoenixdatacom.com/product/niksun-netvcr-proactive-network-service-application-monitoring/
48. https://www.xplico.org/
49. https://www.liveaction.com/products/omnipeek-network-protocol-analyzer/
50. https://www.niksun.com/product.php?id=112
51. https://www.dfir.training/resources/downloads/ctf-forensic-test-images/tools/incident-response/pcap-tools/599-stenographer
52. https://github.com/USArmyResearchLab/Dshell
53. https://www.nirsoft.net/utils/password_sniffer.html
54. Narwal, B., Mohapatra, A. K., &Usmani, K. A. (2019). Towards a taxonomy of cyber threats against target applications. Journal of Statistics and Management Systems, 22(2), 301-325.
55. Dhawan, S., &Narwal, B. (2019). Unfolding the Mystery of Ransomware.In International Conference on Innovative Computing and Communications (pp. 25-32).Springer, Singapore.
56. Narwal, B., &Mohapatra, A. K. (2017, October). Performance analysis of QoS parameters during vertical handover process between Wi-Fi and WiMAX networks.In International Conference on Recent Developments in Science, Engineering and Technology (pp. 330-344).Springer, Singapore.
57. Narwal, B. (2018, October). Fake News in Digital Media. In 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN) (pp. 977-981). IEEE.
58. Rani, S., Narwal, B., &Mohapatra, A. K. (2017, October). RREQ Flood Attack and Its Mitigation in Ad Hoc Network.In International Conference on Recent Developments in Science, Engineering and Technology (pp. 599-607).Springer, Singapore.

Published by: The Mattingley Publishing Co., Inc.