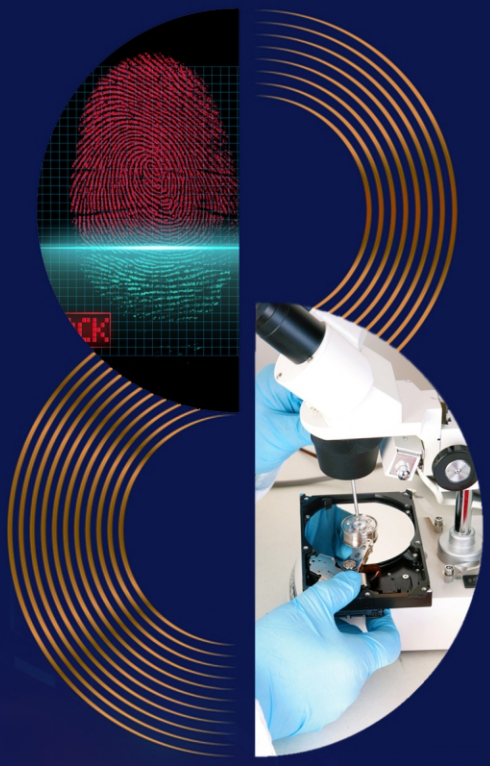
Volume 8 | Issue 3 | August 2023 https://doi.org/10.46293/4n6 | ISSN : 2582-1172

DIGITAL FORENSICS (4N6)

INDIA'S 1st DIGITAL FORENSICS PUBLICATION



8th YEAR OF

PUBLICATION

digital4n6journal.com /d4n6j @d4n6j @d4n6j

500/-

OUR SPONSORS & PARTNERS

DIGITAL FORENSICS(4N6)

INDIA'S 1st DIGITAL FORENSICS PUBLICATION

PARTNERS

CYBERFRAT
AN ERM COMMUNITY

NISC

NATIONAL CYBER DEFENCE RESEARCH CENTRE

Be The Change That You Wish To See In The Forensic Science
NYAYIK VIGYAN

StraightArc
Technologies Pvt. Ltd.

FORENSICS GURU .COM

CYSINFO

BRISK INFOSEC

Digital Investigators
DIA
Association

ninja
Information Security Seriously
ISO- 27001:2013 & 9001:2008 Certified

ARROW

TechLaw

INDIAN INFOSEC CONSORTIUM

CyberShrishti
For the Noobs by the Noobs

CYBER SECURE INDIA

CPC

ARNE
Advance Research Network

Cyber Katta

JEMISTRY
INFO SOLUTIONS

ARISTI NINJA

SAM
OFFENSIVE
TECHNOLOGIES

CyberHex

CopConnect
National Security Database

India Watch

DARK EYE
INTELLIGENCE

DIPLOMADS

SkillsDA®
Center for advance training

ISAC

CONFERENCE PARTNERS

ifip

2nd World Conference and Exhibition on
Forensic Science
June 11-12, 2018 Rome, Italy

DICE
DIGITAL INVESTIGATIONS
CONFERENCE & EXHIBITION

ASIA'S FOREMOST INFORMATION SECURITY CONFERENCE
GROUND ZERO
SUMMIT

HACKERS DAY

OUR TEAM

Our Founders
Lt. Col. (Dr.) Santosh Khadsare (Retd.)
Prince Boonlia

Our Mentors
Mr. Omveer Singh
Mr. Rakshit Tandon
Dr. Gaurav Gupta
Mr. Nilay Mistry

Technical Committee
Mr. Deepak Kumar (D3)
Mr. Tanmay Dikshit
Mr. Smith Gonsalves
Mr. Hriday Raval
Mr. Yugal Pathak
Mr. Ankit Bhisnoi
Mr. Deepanshu Sharma

Design and Development Committee
Mr. Aman Agarwal
Mr. Kritharth Jhala
Mr. Rishabh Sovani
Mr. Shubham Singh

Editor-In-Chief
Ms. Rakhi R Wadhwani
Mrs. Seema Khadsare

Editorial Board
Mr. Deep Shankar Yadav
Ms. Evita K. Breukel
Ms. Sneha Joshi

Managing Editor
Ms. Jyoti Nene

Content Reader Committee
Mr. Rajesh Sharma
Ms. Sunita N
Ms. Anjali Chouhan
Ms. Vaishali Wahi

DIGITAL FORENSICS (4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

Volume 8 | Issue 3 | August 2023

EDITORIAL NOTE

Dear Readers of 4N6,

If you are anything like us, you probably picked up our latest issue and immediately began flipping through the pages. It's a whole new package that's focused on the specific aspects of cyber security and digital forensics that you need in your work lives. We've remade the magazine to make it visually pleasing, easy to read and graphically informative. As much as the words, we want the photos, charts and figures to tell a story. As you read this issue, you'll be able to glean the information you need quickly and clearly.

At the outset, we would like to thank our writers, readers, partners and sponsors who have helped us sustain, grow and make our effort to spread knowledge on cyber security and digital forensics a success. In the present scenario, there is no crime which does not have digital forensics associated with it. The importance of digital forensics as a post-mortem tool that helps design the protection has increased enormously. Investigating various types of crime are a challenge to the forensic investigator because of difficulty in identification of the digital artefacts, shortage of storage space and its inter-connectivity.

In this issue, we have touched upon variety of topics which are less talked about such as WhatsApp Forensics. Keep Reading...

It is heart-warming to see the younger generation coming forward with articles and researches on forensics. We thank them for their efforts. For those whose articles have not been included in this issue due to some reason, do make the amendments and send us again so that we include in our next issue. Please read the authors guidelines before submission.

We look forward to the suggestions from the readers to improve upon and bring a better magazine. Keep writing to us at rakhi.r.wadhwani@gmail.com. Keep visiting our website www.digital4n6journal.com for updates. We would also love it if you join and follow us on social media – we're on LinkedIn, Twitter, Facebook and Instagram for our latest updates.

Seema Khadsare
Editor-in-Chief

Rakhi R. Wadhwani

Rakhi R Wadhwani
Editor-in-Chief

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

Volume 8 | Issue 3 | August 2023

INDEX PAGE

DIGITAL FORENSICS (4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

Volume 8 | Issue 3 | August 2023

https://doi.org/10.46293/4n6/2023.08.01.01

DEEPFAKE – A NEW TECHNOLOGY WITH OLD CONCEPT

Author/Writer: Dr. Bhagyashri R Hanji, Professor, Dept. of CSE, DSATM, Bengaluru.

Email: Bhagyashri-cse@dsatm.edu.in

Article/Paper Highlights:

The authors cover the evolving digital crime in recent times called Deepfakes, in which manipulated content spreads for spreading fake news, misinformation, digital kidnapping and lots more. It also highlights the process to analyse such crime and some areas where these crimes were used to spread and to create propaganda campaigns for/against.

– Editorial Team, Digital Forensics (4N6)

Abstract

In recent days tampered content is progressively increasing and is being used in a wide range of cybercrime activities. The spread of fake news, misinformation, digital kidnapping, and ransomware-related crimes are the most repeated crimes in which manipulated digital content is being used as an attacking vector.

Introduction

Deepfakes started with the Video Rewrite program, created in 1997 by Christoph Bregler, Michele Covell, and Malcolm Slaney. The existing video was altered to create new content and it was the first system to automate facial reanimation completely. Without precautionary measures, deepfakes can be used to harm organizations and their stakeholders. Deepfake can lead to Extortion, fraud, authentication failures and risk of losing reputation.

Machine Learning and Deep Learning algorithms are used to detect manipulated content. The retrenchment of deep learning and fake content involved in the creation of false multimedia content, computer-generated content, to make new content from existing old content is deepfake. Deepfakes cause major problems such as violation of human rights, privacy rights, personal data protection and copyright violations.

The amount of deepfake content online is rapidly growing. The scope of political and social dangers that deepfakes present is: "twisting functions talk; controlling elections; disintegrating trust in establishments; weakening journalism; intensifying social divisions; sabotaging public security and incurring hard-to-fix harm on the reputation of prominent people including elected officials and candidates for office.

Deepfakes can be identified by inadequacies incorporated. For example, occurrence of strange jewellery, facial expression, movement of mouth while talking, blinking of eyes, wrinkles, etc. Other indicators of a deepfake video include: The skin- Does it appear wrinkly or smoothed, consistency of skin texture all over the person's face, facial hair. Person's mouth or lips- Does it match the rest of their facial image, the person's voice. The shadows- Missing shadows in places where they would normally appear.

Deepfake content can be formed using face swap, expression swap and Generative Adversarial Networks following three steps- Extraction, Training and Creation. Deepfake does not require huge data sets, a small amount of data is quite enough to create deepfake contents.

Cybercrime is thought provoking and challenging national security systems all over the world, with malicious users taking advantage and exploiting human and technical vulnerabilities.

The similarity and resemblance of a person can be replaced by another in digital media, using artificial intelligence. The reachability of social media is a major concern impacting millions of people negatively and spreading severe damage to the sufferers within no time. The manual analysis of deepfakes is ineffective and time consuming in categorizing and gathering complete and meaningful digital evidence of such criminalities.

Effective forensic tools that are capable of reconstructing evidence are required. The cybercriminals life is at more ease because of the availability of sophisticated tools for complex digital attacks, at the same time challenging the criminal investigators' work.

Autopsy is a digital forensic open-source tool widely accepted by investigators to carry out the analysis and collect proof of doubtful happenings, through processing digital objects.

Machine learning algorithms and techniques have enhanced the detection and classification of digital objects. It involves two important steps. Firstly, data pre-processing and secondly justification and authentication of data.

Advances in video editing software have made it easy to fit the face of one person for another and alter the expressions on original faces. This brings researchers more challenges to move a step closer in developing automated tools for detecting manipulated data.

The competition between creation, detection and prevention of deepfakes makes this area of research more thought-provoking and inspiring. Advancement in technology makes it much harder to identify deepfake.

Blockchain technology can be used which allows storing of data online without centralized servers. Security concepts of blockchain can be used to confirm the validity of digital content which comes with additional requirements.

The main steps taken to create deepfakes include: Gathering your source material, Aligning the images and pixels with the target object in the video, training a deep neural network and encoders to learn the difference between the two sources, Converting the content into the deepfake, Finally, processing the output into a finished product through final edits.

How can we protect ourselves against Deepfake?

Legislation is already beginning to address the threats of Deepfake videos

companies are coming up with more and better detection algorithms all the time. These algorithms analyse the video image and spot the tiny distortions which are created in the 'faking' process. Deepfake videos are still at a stage where you can spot the signs yourself. Look for the following characteristics of a Deepfake video: jerky movement, shifts in lighting from one frame to the next, shifts in skin tone, strange blinking or no blinking at all, lips poorly synched with speech and digital artifacts in the image. But as Deepfakes get better, you'll get less help from your own eyes and more from a good cyber-security program. Good security procedures are the best means of protection.

Why is Deepfake Technology Dangerous?

In the best case scenario, it can be a fun joke between yourself and friends. Worst case scenario, someone has projected your likeness onto another or produced content of you doing or saying things you have not done. The potential to create fake news, violate someone's privacy or obtain secure information is much more at risk now than ever before.

Applications

- **Blackmail -** Deepfakes can be used to generate blackmail materials that falsely incriminate a victim.
- **Politics -** Deepfakes have been used to misrepresent well-known politicians in videos.
- **Art -** Deepfakes is used to publish video artwork with change of face and body creating a synthetic version.
- **Acting -** Deepfakes have been used for creating digital actors. Deepfake technology has already been used by fans to insert faces into existing films
- **Internet meme -** An internet meme emerged utilizing deepfakes to generate videos of people.
- **Social media -** Deepfakes have begun to see use in popular social media platforms.
- **Sock Puppets -** Deepfake photographs can be used to create sock puppets, non-existent people, who are active both online and in traditional media.

References

[1]. https://ercim-news.ercim.eu/en129/special/digital-forensics-for-the-detection-of-deepfake-image-manipulations

[2]. https://news.ucr.edu/articles/2022/05/03/new-method-detects-deepfake-videos-99-accuracy

[3]. https://blog.imatag.com/how-to-detect-deepfakes-using-media-forensics-techniques

[4]. https://www.internetjustsociety.org/legal-issues-of-deepfakes

[5]. https://www.analyticsinsight.net/best-ways-prevent-deepfakes/

[6]. https://q5id.com/blog/a-quick-history-of-deepfakes-how-it-all-began#:~:text=Deepfakes%20started%20with%20the%20Video,speak%20in%20the%20original%20version.

[7]. https://www.kaspersky.co.in/resource-center/threats/protect-yourself-from-deep-fake

[8]. https://securityintelligence.com/articles/how-protect-against-deepfake-attacks-extortion/

[9]. https://en.wikipedia.org/wiki/Deepfake

[10]. https://inspiredelearning.com/blog/the-biggest-trends-in-deepfake-detection-in-2022/

[11]. https://mobilityquotient.com/article/deepfake-technology-what-is-it-and-how-can-you-protect-yourself

Volume 8 | Issue 3 | August 2023

ABOUT THE AUTHOR:

Dr. Bhagyashri R Hanji
Professor, Computer Science and Engineering
Dayananda Sagar Academy of Technology and Management,
Bengaluru

Expertise:

Her areas of interest include Mobile Ad-hoc Networks, Wireless Networks, Information and Network Security.

Credentials: She currently works as a Professor in the Department of Computer Science and Engineering, Dayananda Sagar Academy of Technology and Management, Bengaluru, India.

DIGITAL FORENSICS (4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

Volume 8 | Issue 3 | August 2023

https://doi.org/10.46293/4n6/2023.08.01.02

DRONE FORENSICS - SERIES 2

Author/Writer: Ankit Bishnoi

Article/Paper Highlights:

In this article, we shall look at the digital forensic process for drones and drone controllers. If there are associated devices such as laptops, mobile phones or tablets, their examination process is covered in this article. There is a need for proper guidelines for First Responders and Digital Forensics Practitioners on how to respond to a drone incident. The article is intended to provide technical guidance in managing and processing an incident from a digital forensic point of view.

– Editorial Team, Digital Forensics (4N6)

Abstract

Drone forensics is a specialized field that involves the meticulous processing, examination, and analysis of unmanned aerial vehicles (UAVs). The primary goal of this practice is to extract and secure evidence from drones in a forensically sound manner.

Also known as UAV forensics, this discipline is focused on recovering crucial data such as recorded footage, flight history, geo-locations, and unique identification codes. By carefully analyzing this information, experts can gain valuable insights into the activities and intentions of drone operators.

In today's world, where drones are becoming increasingly prevalent, drone forensics is a critical tool for law enforcement agencies, private investigators, and other professionals. By leveraging the latest technologies and techniques, drone forensics experts can help to uncover the truth and bring justice to those who have been wronged.

Chapter 2

Drones and Other Associated Evidence Sources

Drones, unlike many other electronic devices, do require supporting devices for appropriate operational capability. These associated devices could include the following components:

Remote Controller

These are used to control the drone remotely. With the help of a controller, the direction and speed of the flight by radio signals is operated. It is usually operated with a mobile phone.



Mobile/Tablet Device

These devices are needed to view the live camera/video feed captured from the drone.


First Person View (FPV) Goggles

FPV goggles are used to view the live camera/video feed coming from the drone, and this may also be used to control the drone by head movements or gesture controls.

Memory Cards

Removable media/Memory cards are used to hold pictures and videos taken using the drone. They will also have files containing the flight path data and geotagging of photographs by using exchangeable image file (EXIF) data within the photographs and much more evidence. Photos and videos taken by When the drone is on a flight the videos and photos are stored in an SD card. In the internal storage of the drone, the flight log data in the form of TXT files or DAT files that record GPS (Global Positioning System) coordinates, timestamps, motor speed, and other data are stored.

Cloud Storage

Most of the drones may utilize the associated mobile handset to store photographs or video in cloud storage services such as iCloud or Google Photos, or a few directly communicate with the cloud via APIs.

Flight Control System

Network information of a drone is often set or modified Through a flight control system. The flight data files can be downloaded and found in the drone's internal SD card storage. The function of flight settings is provided by a flight control system.

Sensors

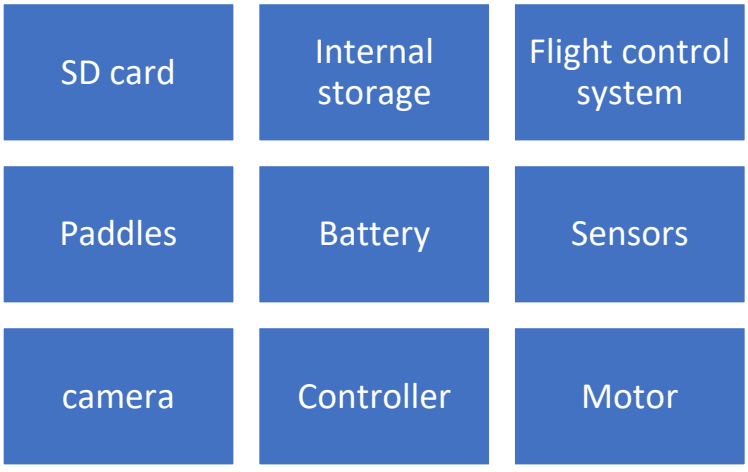
The sophisticated drone system relies on many sensors which act as controllers; they include gyroscopes, accelerometers, and barometers to stabilize the drone's body in the air. The drone is locked up in the air at a specified position and height. With the help of all handset above-mentioned sensors using GPS and barometer data, a drone also contains logs for the same.

Types of Data held on Drone Remote Controllers	
Telemetry	This data will be related to the drones' flights such as GPS, time and date (from GPS signal), velocity, direction, altitude, motor speeds, and user inputs.
Associated Devices	Any devices that have been paired or connected to the controller such as a mobile handset or tablet. This may be the IMEI of the handset or the unique hardware ID of the device.
Registered User Accounts	The user account may be a registered email address or registered account name that has been created with the drone manufacturer.
Communication Signal Parameters Between Drone and RC	These logs should contain signalling data which logs the signal strength between the drone and the RC

When two objects come into contact with each other, the Locard Exchange Principle clearly says that information is transferred from one object to the other in a mutual manner. While this concept was developed for physical forensics, it can also be applied to digital forensics. A drone and a controller/mobile phone depend on Wi-Fi signal at the crime scene, the need for drone forensic analysis has increased dramatically. After the data from the controller or cell phone is processed, forensic investigation may include a variety of details about a possible suspected drone communication to communicate with one another in drone forensics. The drone flies under control due to data transference. Using Wireshark, we can capture packets send by mobile to the drone, it contains the MAC address of the network interface card.

Digital Forensic Lab Process

The following items are basic equipment inside the drone.



Physical extraction

It is acquisition of raw binary data from the media storage device, with help of this method one can access live data, operating system files and the other data which is not accessible to all users.

File System Dump (FSD)

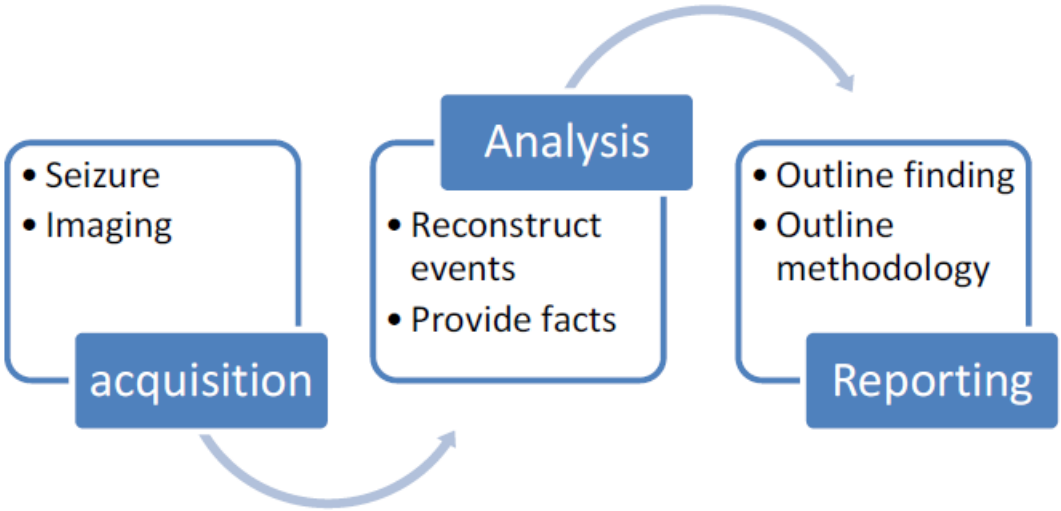
This allows the examiner to retrieve the file system and it interoperates the data, for example, databases holding deleted telematics/media data that may not be available at a logical extraction and may not be accessible during a physical extraction.

Logical extraction

This method allows the examiner to work with live data available on drone. Most drone device forensic software offers this type of feature if the data is not contained on a removable media card. It also involves receiving information from the drone and allowing the device to present the data for analysis.

Chiff-off

For drones that have on-board memory or are damaged, Chip-Off methods can be used to extract the data. Chip-Off also allows the extraction of raw binary data from the device's storage, but it requires the permanent removal of the device's memory chip from the memory board.



To get desired results of my study I retrieved data for different DJI and other make and model to study the variation in the information available, Additional artifacts include user information, credit card information, PCAP file, and the sign of any anti-forensic techniques.

I have divided the possible data outcomes into three categories, based on what the data describes, and then performed comparative analysis from different drones.

User-Created Data

- Digital image, video, or audio files.
- Waypoints of flight used by the user

User-Activity Data

- Dates and times of operation
- Flight logs
- Navigational waypoints utilized
- Motor speeds
- Height reached during flight
- GPS coordinates
- Directional information
- Flight route or path
- Launch location, landing location
- Mission-specific payload information (such as audit logs)
- Configuration files
- PCAP files

Device Operating Data

- FAA Registration Number
- Associated devices (mobile phones, online accounts, connected controller, previous computer connections, battery serial numbers)
- Software versions/firmware versions

Forensic Significance

- Understanding important acronyms used to describe drone components and their functions.
- Understand proper Drone evidence handling, labelling, preservation and seizure.
- Identify what information can be stored in a drone and associated equipment.
- Identify what information can be stored on a memory card.
- Identify other locations where information can be stored.
- Understand that placing memory cards in different computers, mobiles or drones may modify the data
- Identify the following types of drones: multi-copters and fixed-wing.
- Gap analysis in digital forensics of a drone concerning different techniques.
- Determining the accuracy of different drone forensic tools.
- Understanding different types of common tools to be used for analysis.

First of all, the file type, file path and default name comparison were done by manually dumping the data and understanding the core structure of each make and model. We can see the variation in all the different parameters chosen with different UAVs. Mostly the flight log of DJI is found in encrypted .dat files either internal or external media.

Drone Make/ Model	Data Location	File type	Default Name
DJI Phantom 3	Internal SD	.dat	FLYXXX
DJI Phantom 4 Pro	Internal SD	.dat Two additional logs were generated named 'PHARM.LOG' and 'USER.LOG'	FLYXXX
JI MAVIC 2	INTERNAL eMMC	.dat	
YNEEX Q500 4K	SD CARD (when saved on Controller)	.csv	Remote/RemoteGPS/Telemetry
Parrot ANAFI	External SD (or iPhone when used with controller)	.bin (.json)	Log.bin (XXDate&TImeXX.json)
DJI mavic			
DJI Spark			

Drone Make/ Model	Data Location	File Path	File type	Default Name
 **DJI Phantom 3**				
 **Photos**	External SD	\DCIM\	.jpg/.dng	FLYXXX
 **Video**	External SD	\DJI\dji.pilot\DJI_RECORD\	.mp4/.mov	FLYXXX

Drone Make/ Model	Data Location	File Path	File type	Default Name
 **DJI Phantom 4 pro**				
 **Photos**	External SD	\DCIM\	.jpg/.dng	FLYXXX
 **Video**	External SD	\DCIM\	.mp4/.mov	FLYXXX

Drone Make/ Model	Data Location	File Path	File type	Default Name
 **DJI Mavic 2**				
Photos	Internal eMMC/External SD	\DCIM\	.jpg/.dng	FLYXXX
Video	External SD	\DCIM\	.mp4/.mov	FLYXXX

Drone Make/ Model	Data Location	File Path	File type	Default Name
 **YUNEEC Q500 4K**				
Photos	Camera SD	\DCIM\	.jpg/.dng	Log bin
Video	Camera SD	\DCIM\	.mp4/.mov	FLYXXX

Drone Make/ Model	Data Location	File Path	File type	Default Name
 **Parrot ANAFI**				
 **Photos**	External SD	\DCIM\100MEDIA	.jpg/.dng	Log bin
 **Video**	External SD	\DCIM\100MEDIA	.mp4/.mov	FLYXXX

Potential illegal activities and dangers drones could represent where we might need to do Drone Forensics.

Criminals often use these modern devices to conduct a myriad of illegal activities, including:

- Piloting them to smuggle drugs, mobile phones, guns, knives, and other weapons, illegal substances, and objects into prisons.
- Using them as a tool to conduct terrorism by planting explosives into stadiums and other public venues.
- Corporate and government espionage, unauthorized monitoring and intelligence gathering.
- Voyeurism and invasion of people's privacy by trespassing on private property
- Disrupting the workflow of airports and distracting air traffic
- International espionage and unauthorized trans-border supervision
- Stalking, harassment, and invasion of privacy by paparazzi or unethical journalists and reporters
- War crimes such as launching aerial missile attacks.
- Physical attacks on unsuspecting citizens
- Smuggling of contraband items between minors
- Property vandalism
- Violation of no-fly zones

ABOUT THE AUTHOR:

Ankit Bishnoi
DFIR Analyst – eSec Forte Technologies
Email Address: alstonbishnoi29@gmail.com
LinkedIn: https://www.linkedin.com/in/ankit-bishnoi-0819

Expertise:
Ankit is enthusiast in the field of Incident Response & DFIR Specialist, and Infosec Trainer. He is well experienced in managing projects from the blue team to the purple team.

Credentials:

Ankit is currently working as DFIR Specialist. Also, he holds many certifications like CHFI, CEH, CCIO, Paloalto, LogRhytm, Eset Certified, etc. He is targeting several assignments in Threat Analysis, Cyber Security, Incident Response, and DFIR.

DIGITAL FORENSICS (4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

Volume 8 | Issue 3 | August 2023

https://doi.org/10.46293/4n6/2023.08.01.03

DATABASE SECURITY: A TECHNICAL ANALYSIS AND BEST PRACTICES

Authors/Writers: Parth Trilokchandani, Shubham Pareek

Article/Paper Highlights:

This article briefs about the concepts of *Database Security* with some technical examination of multiple types of databases and highlights the useful strategies for enhancing database security. It also covers some best practices required in database security.

– Editorial Team, Digital Forensics (4N6)

Abstract:

In today's digital landscape, where data breaches and cyber-attacks pose major dangers to enterprises, database security is critical. This article examines the important components and best practices for developing a strong security framework, providing a technical study of database security. Access control, data encryption, auditing, vulnerability management, secure configuration, and data masking are all covered in the investigation. The importance of these procedures in protecting sensitive data, preventing illegal access, and limiting the dangers of data breaches is highlighted in the article. Organizations may strengthen their database security, maintain regulatory compliance, and preserve the integrity and confidentiality of their essential data assets by following the best practices suggested in this article.

1. Introduction

Database security is a significant consideration for businesses that handle sensitive data. With the rising prevalence of cyber hazards and data breaches, it is vital to have robust security measures to protect databases against unauthorized access [1], data theft, and malicious acts. This article provides a technical examination of database security as well as useful strategies for enhancing database security [2].

2. Methodology

Database security comprises a variety of procedures used to secure data confidentiality, integrity, and availability. Access control, data encryption, auditing, and vulnerability management are all important components of database security. These elements collaborate to create a tiered protection system against potential attacks.

2.1 Access Control:

The core of database security is access control. It entails putting in place procedures for user identification, authorisation, and permission control. Best practices include using secure passwords, following least privilege principles, and assessing user access privileges on a regular basis. To assign specific privileges based on job duties and responsibilities, role-based access control (RBAC) can be used.

2.2 Data Encryption:

Data encryption is critical for safeguarding sensitive data stored in databases. To encrypt data at rest and in transit, encryption techniques such as Transparent Data Encryption (TDE) and column-level encryption can be utilized. To prevent unauthorized access to encrypted data, encryption keys must be properly managed.

2.3 Auditing and Monitoring:

Effective auditing and monitoring techniques are essential for recognizing and analyzing questionable database activity. Database activity monitoring (DAM) technologies can monitor user behaviors in real-time, detect anomalies, and produce alerts. To handle any potential security problems as soon as possible, regular log analysis and security incident response protocols should be in place.

2.4 Vulnerability Management:

Regular vulnerability assessments and patch management are essential for identifying and correcting security flaws in the database management system (DBMS) and related software. It is critical to keep security updates up to date and to use vulnerability scanning tools to detect and repair potential flaws.

2.5 Secure Configuration:

It is critical to implement secure configuration settings for the DBMS and other components. This involves adopting secure network configurations, using vendor-recommended security settings, eliminating superfluous services and features, and using vendor-recommended security settings. To ensure compliance with security requirements, regular security assessments and configuration audits are advised.

2.6 Data Masking:

Data masking involves obfuscating sensitive data within databases, making it unreadable for unauthorized users while maintaining its functional integrity for legitimate use cases. Techniques such as tokenization and data redaction can be employed to protect sensitive data and reduce the risk of data exposure.

3. Conclusion

Database security is an ongoing endeavour that requires a combination of technical measures, processes, and best practices. By implementing robust access control, data encryption, auditing, and vulnerability management practices, organizations can strengthen the security posture of their databases. Regular security assessments, proactive monitoring, and staying updated with the latest security advancements are essential for maintaining an effective database security strategy.

References

1. A. Mousa, M. Karabatak and T. Mustafa, "Database Security Threats and Challenges," *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*, Beirut, Lebanon, 2020, pp. 1-5, doi: 10.1109/ISDFS49300.2020.9116436.

2. Z. S. Zubi, "On distributed database security aspects," *2009 International Conference on Multimedia Computing and Systems*, Ouarzazate, Morocco, 2009, pp. 231-235, doi: 10.1109/MMCS.2009.5256696.

ABOUT THE AUTHOR:

Parth Trilokchandani

M.Sc. In cyber-Security & Digital Forensics

SITAICS, Rashtriya Raksha University

Only.project.2021@gmail.com

Expertise:

Parth has good understanding of the Cyber Security and Digital Forensics

Credentials:

Parth is currently pursuing his M.Sc. in Cyber Security & Digital Forensics from Rashtriya Raksha University. He wants to make his career in the Cyber Security field and serve the nation in the same.

Shubham Pareek

MSc. In cyber-Security & Digital Forensics

SITAICS, Rashtriya Raksha University

Shubhampareek2023@gmail.com

Expertise:

Shubham has good expertise in the concepts of Cyber Security and he has completed some research in Cyber Security and Digital forensics.

Credentials:

Shubham is currently pursuing his M.Sc. in Cyber Security & Digital Forensics from Rashtriya Raksha University.

DIGITAL FORENSICS (4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION
Volume 8 | Issue 3 | August 2023
https://doi.org/10.46293/4n6/2023.08.01.04

INTRODUCTION TO MOBILE FORENSICS

Author/Writer: Vaibhav Kulshrestha

Article/Paper Highlights:

This article enlightens the mobile forensics concepts and importance of forensics in investigation of collecting data, mobile file system hierarchy, methods of data extraction from devices and challenges that come during the investigation of mobile devices.

– Editorial Team, Digital Forensics (4N6)

1. ABSTRACT

Mobile devices, which hold very large quantities of personal as well as sensitive data, have become an essential part of lives. Mobile forensic investigations are crucial to retrieving and analyzing data evidence from these devices. This assists in crime resolution, cyber risk prevention, and cyber-crimes. In this article, we need to focus on the evolution of upcoming technological challenges, and potential solutions. In order to adapt to the ever-changing digital world, examiners and practitioners need to investigate and understand these advancements. Further, it provides insight into the challenges associated with obtaining evidence from mobile devices, as well as the methods to overcome them.

1.1 KEYWORDS

Data collection, Data analysis, Investigation Processes, Verification, and location-based analysis.

2. INTRODUCTION

Are you curious to know about this technology? Why does it appear so frequently in the investigation process? Why do multiple organizations use this method of collecting data from mobile devices? If you are familiar with mobile forensics, you will be able to solve a variety of additional problems that arise in today's digital age. In today's world, all technology, including mobile devices are interconnected with one another. It provides investigators with additional information that may be useful for the analysis of artifacts during their investigation proceedings.

3. WHAT DO U MEAN BY MOBILE FORENSICS?

Mobile forensics is the practice of extracting, analyzing, and interpreting data from mobile devices such as smartphones, tablets, and portable GPS devices for investigative purposes. It entails capturing, preserving, and analyzing digital evidence obtained on mobile devices in order to unearth information useful to criminal investigations, legal disputes, or intelligence gathering. Mobile forensics is the extraction and analysis of data stored on mobile devices using various techniques, tools, and approaches. This can include call logs, text messages, emails, contacts, browsing history, multimedia files, app data, GPS location data, and other information. To obtain and analyze this data while retaining the integrity and validity of the evidence, forensic examiners employ specialized software and hardware technologies.

The technologies can assist in the creation of a report, data decryption, password cracking, and data analysis. There are some well-known tools available such as the Celebrate U FED and Physical Analyzer, MSAB-XRY, Magnet AXIOM, and others. To acquire the greatest results with the right evidence, accurate documentation, the chain of custody, and a methodology that can be followed are required. Data is extracted from a mobile device's memory as well as any type of storage media, such

as a SIM-Card, IMEI, SD card, using specialized tools and methodologies in mobile device forensics. The incoming data may involve text messages, call logs, contact, picture, video etc. The use of mobile device forensics to find evidence of fraud, cybercrime, and other wrongdoing is frequent in both criminal and civil investigations. It basically is used to recover hidden or deleted data or unallocated data space.

4. WHY IS IT MORE IMPORTANT IN MOBILE FORENSICS?

Mobile devices have transformed the way we interact, work, and save data. They have become an essential aspect of criminal investigations, giving crucial evidence that can lead to truth and justice. In multiple ways, mobile forensics advice to law enforcement agencies and forensic professionals as below: -

- **Criminal and Civil Investigations:** Mobile devices frequently carry critical information such as phone records, text messages, GPS data, and multimedia files that can aid in the reconstruction of events and the establishment of timelines.
- **Cybersecurity Detection methods:** Mobile forensics provides cyber threat detection and prevention by inspecting mobile devices for indicators of malware, unauthorized access, or data breaches.
- **Fraud and Financial Related Crimes:** Mobile devices frequently include proof of financial transactions, fraudulent activity, and identity theft.

5. WHAT ARE THE PHASES OF MOBILE FORENSICS?

6. IN MOBILE FORENSICS, WHERE CAN I FIND DATA STORED ON DEVICES?

Data can be kept in numerous locations on a mobile device in mobile forensics, depending on the operating system (e.g., iOS, Android) and the sort of data being studied. Here are some examples of frequent data storage locations:

- **Internal storage**: Internal storage in mobile devices stores apps, system files, and user data. Photos, movies, documents, and application data are all included. The location of these files varies depending on the operating system and device model.

- **External storage:** Some devices, such as SD cards, feature extended storage choices. If the device has an SD card, its contents must be examined because it may include more user data.

- **Directories on the system:** System folders house critical files related to the operating system and system settings. These directories may contain logs, configuration files, and other system-related data pertinent to the investigation.

- **Programme-specific directories:** Each installed programme on the device has its directory in which it saves data. User preferences, cached files, chat logs, and other application-specific data are all included. These folders are usually found in internal storage.

- **Databases**: Many programmes, particularly those that handle large volumes of data, store information in databases. Contacts, messages, call logs, surfing history, and other forms of data can be stored in these databases.

- **Cloud storage:** Mobile devices frequently sync data with cloud services like iCloud, Google Drive, and Dropbox. Accessing and analyzing cloud storage may yield new evidence and insights.

7. WHAT IS THE METHOD TO EXTRACT DATA FROM MOBILE FILE SYSTEM DURING PROCESS OF INVESTIGATION?

- **Physical extraction:** This includes creating a bit-by-bit copy of the entire storage partition. It allows for a comprehensive analysis of the file system, including deleted files and hidden files.
- **Logical extraction**: In a logical extraction, only specific files or paths are extracted from the file system. It is more convenient and faster than physical extraction.

- **File carving** is a method for recovering deleted or fragmented files from unallocated or free space on the Android file system. To detect and recover erased files, it searches for file signatures or certain file structures.

- **SQLite database analysis:** These databases can be analyzed by forensic software to extract information like contacts, messages, call logs, browser history, and application-specific data.

7.1 FILE SYSTEM IS AVAILABLE MOBILE DEVICES: -

- **System Configuration:** This directory contains a variety of system-level configuration files and settings that provide information on the device's setup and customization.

- **Logs**: System logs such as kernel logs (dmesg), system event logs (logcat), and debug logs can help you analyze device activity and potential problems.

- **Cache:** The cache directory contains temporary files that may provide valuable evidence containing cached data from apps, web browsers, and the system.

- **Miscellaneous:** Other critical system files, such as boot configurations, system binaries, and device-specific settings, may be found under the root directory.

- **Partitioning Data (/data):** It will contain details of partition of specific drive.

- **Applications:** The /data/app directory contains installed applications, as well as their accompanying APK files. These files may be useful for confirming the presence of specific apps on the system.

7.2 WHAT ARE THE MOBILE FORENSICS FILES TO CHECK DURING THE PROCESSING OF REPORTS?

The following categories are involved in checking files in mobile devices such as images, videos, audio and voicemail messages. Browsing history, content data, history searches, and analytics information. To-do lists, notes, calendar entries, ringtones. Documents, presentation files and other created data.

7.3 MOBILE FILE SYSTEM HIERARCHY?

- **/system: -** It involves both the system apps that come pre-installed apps on Android devices and the Android GUI based.
- **/recovery: -** This partition may be used to take backups.
- **/data: -** This partition contains the user's entire data collection, including contacts, settings, apps, and messages.
- **/cache: -** It helps to clean the entire disk partition of the system.
- **/misc.: -** the miscellaneous system may include settings for various options such as on/off switches.
- **/SD card: -** It is a storage part of media in which data can be stored as information.

8. THE EXAMINER FACED CHALLENGE DURING MOBILE FORENSICS PROCESS?

The major technical challenges in mobile forensics are as follows: - Technology is rapidly evolving, with new models, operating systems, and applications for mobile devices being produced on a regular basis. Forensic examiners must face the challenge of staying current with new breakthroughs and updating their abilities and equipment as needed. As user privacy and security become more important, modern Android handsets typically include increased encryption and security protection. Without the proper passwords or encryption keys, accessing data stored on the device can be challenging. Many Android mobiles contain secure enclaves or dedicated hardware for storing sensitive data and performing cryptographic operations. These security features make it difficult to circumvent or directly extract data from these protected locations, necessitating the use of certain techniques or weaknesses. Users often backup their data to the cloud, and Android devices are tightly connected with cloud storage providers. Mobile devices are widely utilized for a variety of reasons, and a wide range of third-party applications are available. Each programme may employ its own distinct data storage mechanisms, encryption algorithms, and security safeguards. Data extraction from these apps can be difficult and time-consuming, necessitating specialized knowledge and equipment. Furthermore, certain programmes may store data in the cloud or employ end-to-end encryption, complicating the investigation even further. Mobile devices have the ability to store huge amounts of data, such as call logs, texts, photographs, videos, social network activity, app data, and more. Analyzing such enormous amounts of data manually can be exceedingly time-consuming and may necessitate the use of specialized tools and techniques. It is critical to identify important information from this massive volume of data.

9. CONCLUSION

Mobile forensic science is a distinct and specialized profession with unique barriers compared to other fields of digital forensic science. Mobile forensics is a difficult and dynamic scope because of quickly expanding technology, encryption and security measures, fragmented data, cloud-based storage, data volume and complexity, anti-forensic strategies, and legal and privacy concerns. To solve the obstacles of mobile forensics, practitioners must have a thorough understanding of mobile technology, operating systems, and security procedures. To stay up with the ever-changing landscape of mobile devices and apps, they must constantly update their knowledge and skills. Collaboration and information exchange among forensic professionals, researchers, and law enforcement agencies is also essential to address growing challenges and develop effective solutions.

REFERENCES

- Kostadinov, D. (2016, July 06). The mobile forensics process: steps and types. Retrieved from Infosec Resources: https://resources.infosecinstitute.com/topic/mobile-forensics-process- steps-types/
- Heather Mahalik and Rohit Tamma. (2016, April 25). Mobile Forensics and Its Challenges. Retrieved from packthub: https://hub.packtpub.com/mobile-forensics-and-its-challanges/

ABOUT THE AUTHOR:

Vaibhav Kulshrestha
Digital Forensic (Intern) at eSec Forte Technologies.
Digital Forensic and Incident Response and Cyber Security
Email Address: - vaibhavkulshrestha65@gmail.com.
LinkedIn
https://www.linkedin.com/in/Vaibhav-Kulshrestha-275344ab

Expertise:
Software development, digital forensics, incident response, cyber security, cyber law and ethics, ethical hacking, and information security are all areas in which Vaibhav is very interested.

Credentials:
Vaibhav is competent, deserving of being allowed to concentrate on his task, and enthusiastic about learning new technology in the context of the digital world. He is presently working as an Intern at eSec Forte Technologies in Digital Forensics and Incident Response. Previously, he was employed in a private corporation as an Information Technology (IT) Engineer. He has also received training from the Ministry of Home Affairs', Central Forensic Science Laboratory's Digital Forensic Unit in New Delhi.

NSD CERTIFIED
National Cyber Security Scholar

Learn to strengthen enterprise cybersecurity, explore emerging trends, and transform them into actionable insights.

24th Sept to 10th Dec, 2022

www.isacindia.org

The cybersecurity scholar program is a comprehensive and insightful course for CISOs, CIOs, CXOs, Senior/Middle-level management professionals, and faculty members with seven or more years of experience and responsible for driving cyber security.

Program Outcomes

Why do certain companies win against hackers, and why do others fail? What will state-sponsored attacks in the global economy mean for your organization? How can you defend against next-generation cyber-attacks by continually being one step ahead? The NCSS Program will immerse you in new ways of thinking and provide insights that will significantly enhance your company's defenses against emerging cyber-attacks and propel your career.

On-Campus - 3 Days, 24 - 26 Sept, Mysuru

Immerse in three-day on-campus training (Includes stay and meals) at Cyberverse Foundation, Mysuru, with hands-on sessions on the Phygital Lab and SOC Simulation Center. Interact with the Karnataka Digital Economy Mission (KDEM) team and visit Lahiri's state-of-the-art ESDM facility.

Online Sessions - 12 Weeks, 8 Oct - 10 Dec (online)

Week 01: CII & National Security
Week 02: Smart Cities and Homeland Security
Week 03: CII Focus: Power Sector
Week 04: CII Focus: Transport Sector
Week 05: CII Focus: BFSI Sector
Week 06: CII Focus: Telecom Sector
Week 07: CII Focus: Defence Sector
Week 08: Next-Generation SOC
Week 09: Economy, Intelligence & Cyber Warfare
Week 10: DFIR, Cyber Insurance, & Legal Challenges
Week 11: AI, ML, & Quantum Computing Trends
Week 12: Capstone Project Briefing and Discussions

Weekly Cyber Crisis Wargame

Every Thursday, experience a real-world case study in form of a cyber emergency wargame activity. Play the table-top exercise game from the perspective of the Attacker, SOC teams, Forensicators, CISO, and the CEO.

Sector Specific Site Visits


New Delhi Airport


Modern Power Plant


SOC / Datacenter

ESDM Lahari

+91 8882-560-560
+91 8800-880-757

DIGITAL FORENSICS(4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

Volume 8 | Issue 3 | August 2023

https://doi.org/10.46293/4n6/2023.08.01.05

LIVE SYSTEM ANALYSIS USING AUTO TRIAGE IN OS FORENSICS

Author/Writer: Anubhav Varshney

Email: riishiivarshney01@gmail.com

Article/Paper Highlights:

This article highlights the Digital forensics tool and explains the step-by-step procedure in live system analysis with all the features including in the tool for Auto Triage in OS Forensics. Recently, digital attacks have become far more frequent as a result of the worldwide Internet user population growing quickly. Also, covers the detailed analysis steps of effective approaches and tools to quickly identify these attacks and prioritize the necessary actions.

– Editorial Team, Digital Forensics (4N6)

Abstract

The Internet is spreading at a tremendous speed due to the increase in the use of computers or crimes against computers. The field of computer crime emerged as a reaction to the growth of computer crime. Computer forensics is the careful collection and examination of electronic evidence, which not only analyzes the damage caused to a computer as a result of an electronic attack, but also recovers the data lost by such a system in order to convict the criminal. Therefore, the normal forensic process required after a cyber-attack involves collecting evidence from a computer system, analyzing it and presenting the collected evidence in court of law. Digital Forensic is primarily concerned with the collection and analysis of hidden evidence. The growth of digital forensics has greatly increased the need for effective tools. There are a number of tools available today that are used to examine the operating system of a particular computer. In this paper, we present a review of the triage in live forensic. This paper discusses Auto triage being used for performing live forensic analysis and critically evaluating their efficacy in terms of their applicability and reliability. We present the findings of our study in the section of live acquisition of current machines.

Keywords: Computer forensic, electronic evidence, auto triage, live analysis.

Introduction - PassMark Software OSForensics is a versatile, robust, and versatile computer forensics software used by the computer forensic experts and DFIR researchers worldwide. The latest release is more powerful and full of more features than ever before and adds new industry-leading features technology, such as new forensic virtual environment feature that automatically creates a virtual machine for your forensic disc images (e.g., E01). Imagine being able to see the system through the eyes of the suspect and capture him with a screenshot or video recording to add to your screen a report. This feature is especially good for:

- Analyzing desktop layout
- Deeper analysis of software applications
- Accessing cloud account content
- Courtroom presentation of evidence
- And much more!!!

OSForensics, Auto Triaze (AT) provides users with a complete automated and simple solution for Electronic Evidence Triage (EET). AT allows users of all levels complete EET with incredible speed and ease of use.What exactly is Electronic Evidence Triage (EET)? – EET aims to quickly find,

identify and capture (in a forensic manner), basic system information, user activity and other files and interesting artifacts from digital media sources.
Although useful for users of all skill levels, AT is for first responders and other "entry-level" users OSForensics, which may lack traditional forensic education and/or work experience in the field collection and processing of digital evidence. That is, non-forensic personnel can now get much the same traditional evidence from a full forensic investigation of the case in minutes and with one click of a mouse.

In addition to file recovery items of interest including AT automatically creates an initial case in HTML and/or PDF formats.
By default, these reports and everything else related to case files are automatically saved in the case folder on the OSForensics USB device. Users can get a list of all running processes, create a memory dump ("RAM Dump"), collect all network and user activities, passwords, user accounts, deleted files, system data, detect BitLocker encryption and more. AT also takes a screenshot target system and creates a searchable spreadsheet of all files in the file system, inclusive paths and date/time stamps.

AT can literally be launched with a single mouse click. Collection times vary, however if "Memory Dump" is not selected it usually only takes a few minutes.

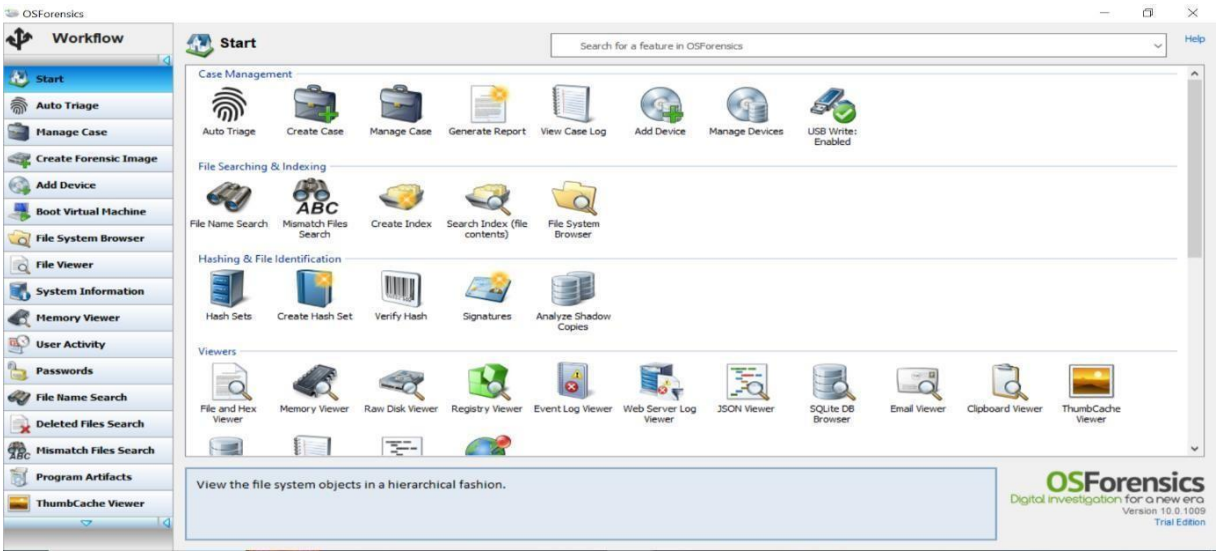
Features – OSForensics includes a collection of digital evidence search, identification, collection, preservation, analysis & recovery of the artifacts that can be used as evidence in the court of law. The main features of OSForensics are described below:

- **Auto Triage -** Automate common forensic tasks in order to triage the most relevant evidence data in time-limited situations. Auto Triage allows non- forensics trained personnel to acquire intelligence on-site which can be volatile and high-risk.

- **Android Artifacts**
- **Boot Virtual Machine**
- **ESE Database Viewer**
- **Case Management**
- **Deleted Files Search**
- **Email Viewer**
- **Event Log Viewer**
- **Drive Preparation**
- **Signature**
- **ThumbCache Viewer**
- **User Activity**
- **Signatures**
- **Verify/Create Hash**
- **Web Browser**
- **Web Server Log Viewer**
- **$UsnJrnl Viewer**
- **File Name Search**
- **Hash Sets**
- **Internet Viewer**
- **Map Viewer**
- **Memory Viewer**
- **Mismatch Search**
- **Image Analysis**
- **Indexing**
- **Clipboard Viewer Passwords**
- **Plist Viewer**
- **Program Artifacts**
- **Raw Disk Viewer**
- **File System Browser**
- **Forensic Imaging**
- **SQLite Database Browser**
- **System Information**

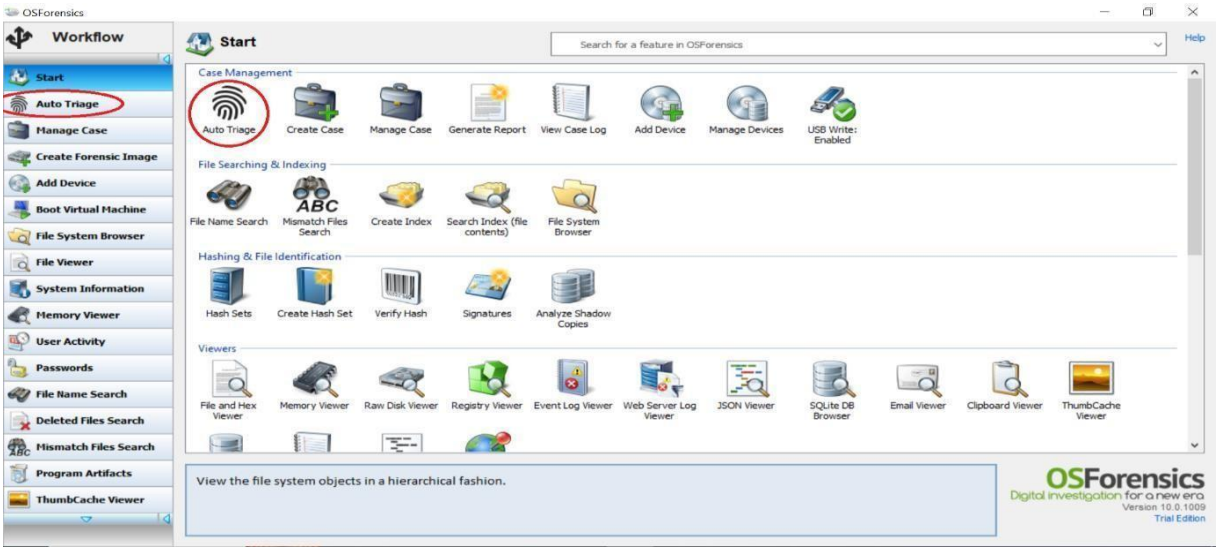
Purpose – Forensic triage is the process of taking key evidence from an information system limited time frame. This is especially true for field investigators with limited forensic expertise of gathering forensic information in a time-critical situation. This procedure is useful for those with non-forensic trained personnel, initial investigators, military personnel tasked with obtaining intelligence on the ground, especially in potentially volatile situations (e.g., probation officers and parole officers during home visits).
By collecting and prioritizing the most valuable evidence on the ground, field investigators do not need to get consent for large volumes of data for research and can therefore quickly focus on a specific area of interest (e.g., Internet and application history for probation officers).

Quick start of the Auto Triage for live system analysis!



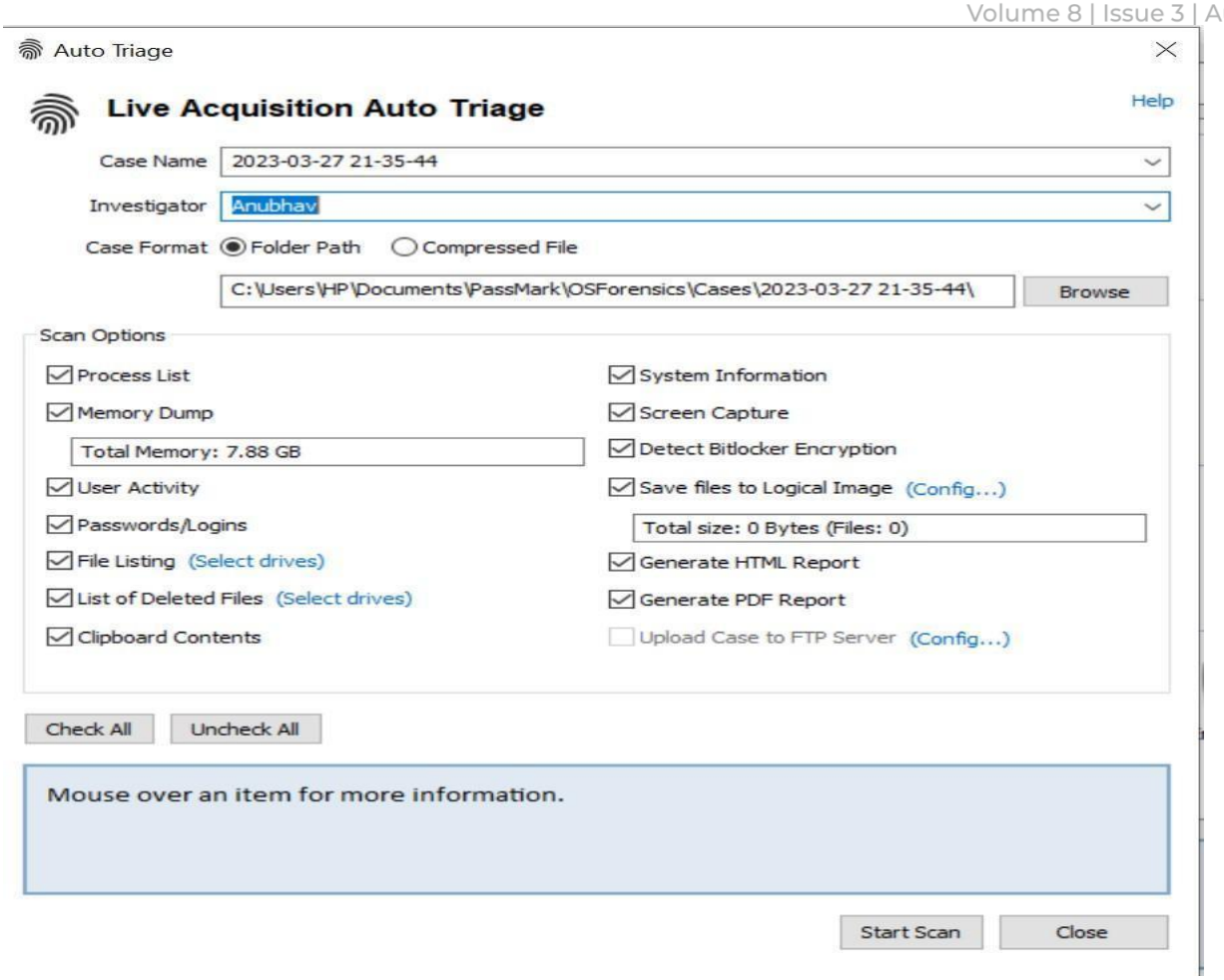
The start window contains a brief description of each feature on mouse over.

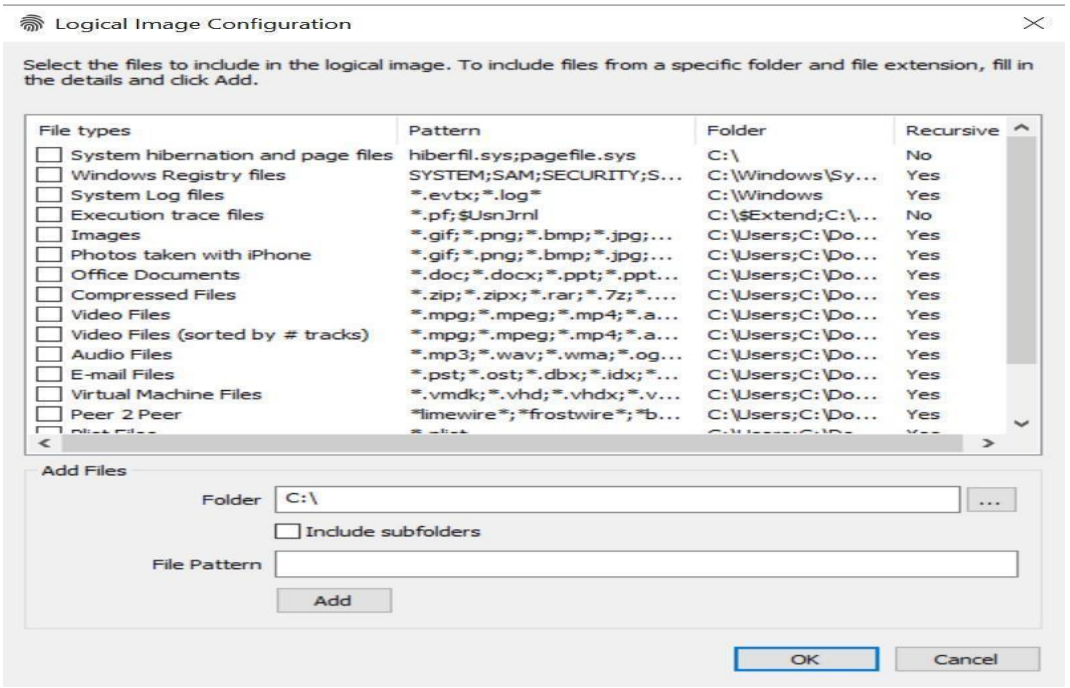
Step 1: Launch the Auto Triage - Open the OSForensics app and click the "Auto Triage" icon on the home screen. You can also click the "Auto Triage" workflow module as shown below.



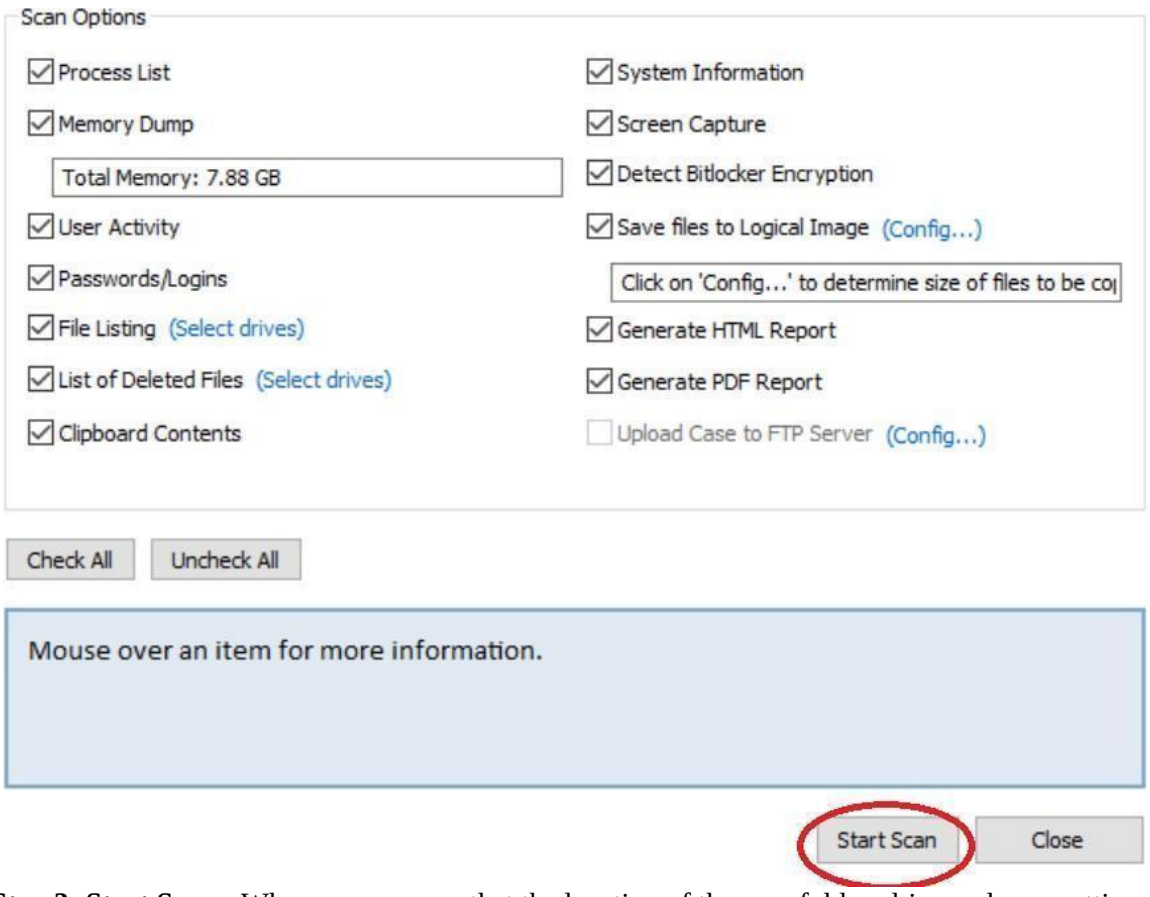
Step 2: Review Default Settings - The Auto Triage window appears.

Before starting the scan, check the settings and make the necessary changes to the default settings.
By default, the triage scan is pre-configured with the most common settings so that the investigator can create a new case and immediately start gathering evidence. However, the investigator can configure the files saved as a logical image by clicking the link (Configuration).


Auto Triage
Live Acquisition Auto Triage
Help
Case Name
2023-03-27 21-35-44
Investigator
Anubhav
Case Format
Folder Path
Compressed File
C:\Users\HP\Documents\PassMark\OSForensics\Cases\2023-03-27 21-35-44\
Browse
Scan Options
Process List
Memory Dump
Total Memory: 7.88 GB
User Activity
Passwords/Logins
File Listing (Select drives)
List of Deleted Files (Select drives)
Clipboard Contents
System Information
Screen Capture
Detect Bitlocker Encryption
Save files to Logical Image (Config...)
Total size: 0 Bytes (Files: 0)
Generate HTML Report
Generate PDF Report
Upload Case to FTP Server (Config...)
Check All
Uncheck All
Mouse over an item for more information.
Start Scan
Close

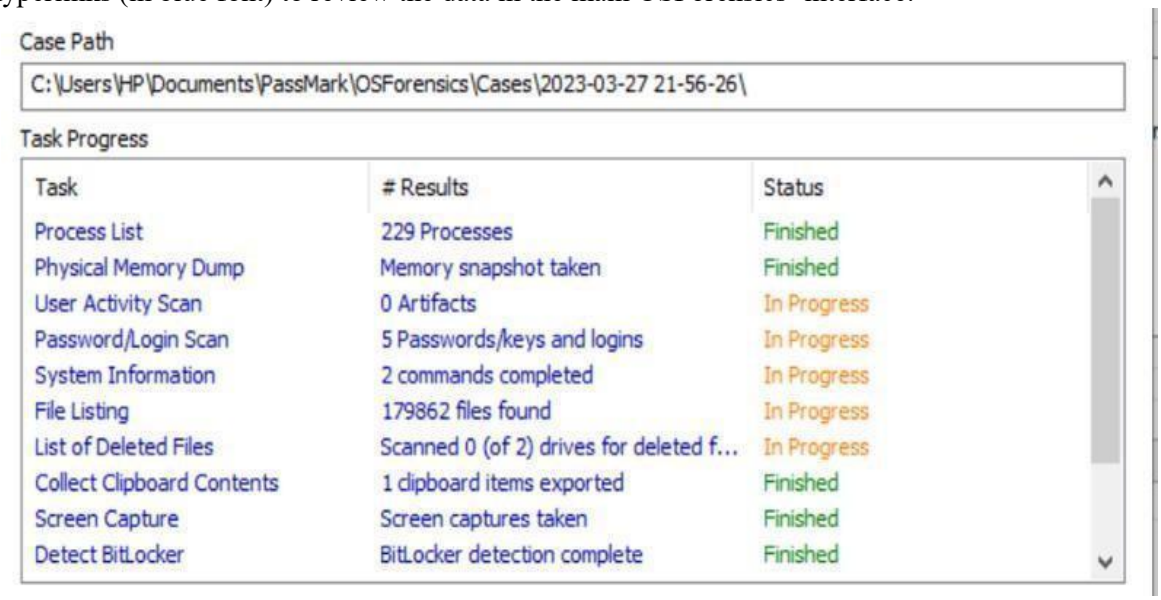

Logical Image Configuration
Select the files to include in the logical image. To include files from a specific folder and file extension, fill in the details and click Add.
File types
Pattern
Folder
Recursive
System hibernation and page files
hiberfil.sys;pagefile.sys
C:\
No
Windows Registry files
SYSTEM;SAM;SECURITY;S...
C:\Windows\Sy...
Yes
System Log files
.evtx;.log*
C:\Windows
Yes
Execution trace files
*.pf;$UsnJrnl
C:\$Extend;C:\...
No
Images
.gif;.png;*.bmp;*.jpg;...
C:\Users;C:\Do...
Yes
Photos taken with iPhone
.gif;.png;*.bmp;*.jpg;...
C:\Users;C:\Do...
Yes
Office Documents
.doc;.docx;*.ppt;*.ppt...
C:\Users;C:\Do...
Yes
Compressed Files
.zip;.zipx;*.rar;*.7z;*....
C:\Users;C:\Do...
Yes
Video Files
.mpg;.mpeg;*.mp4;*.a...
C:\Users;C:\Do...
Yes
Video Files (sorted by # tracks)
.mpg;.mpeg;*.mp4;*.a...
C:\Users;C:\Do...
Yes
Audio Files
.mp3;.wav;*.wma;*.og...
C:\Users;C:\Do...
Yes
E-mail Files
.pst;.ost;*.dbx;*.idx;*...
C:\Users;C:\Do...
Yes
Virtual Machine Files
.vmdk;.vhd;*.vhdx;*.v...
C:\Users;C:\Do...
Yes
Peer 2 Peer
limewire;*frostwire*;*b...
C:\Users;C:\Do...
Yes
Add Files
Folder
C:\
Include subfolders
File Pattern
Add
OK
Cancel

In this dialog, the files to be saved to a logical image can be selected from a default list or a user specified start folder and file pattern to match.

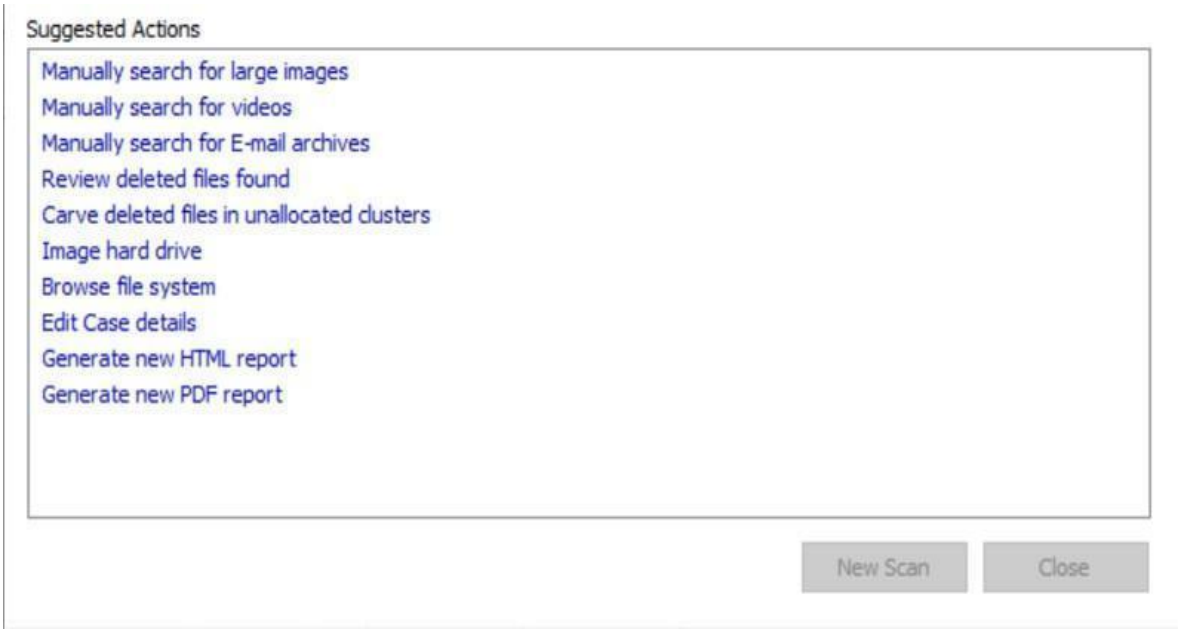


Step 3: Start Scan - When you are sure that the location of the case folder, drive and scan settings are correct, click "Start Scan" to start the Auto Triage.

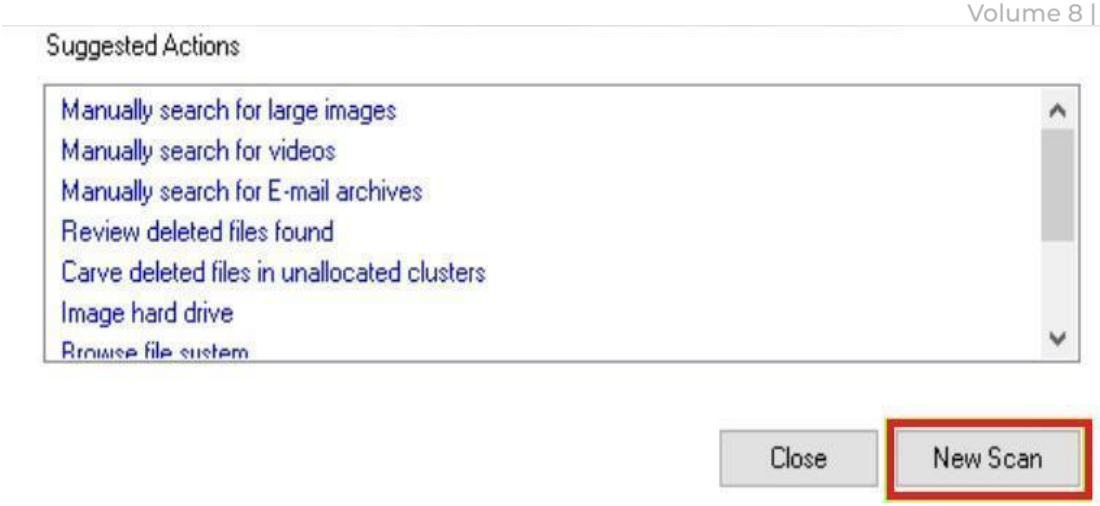
Step 4: Review Results: You can see the status of each scan in real time under the "**Status**" column. The process is complete when all scans show "**Finished**". To review results, simply click on the hyperlinks (in blue font) to review the data in the main OSForensics' interface.



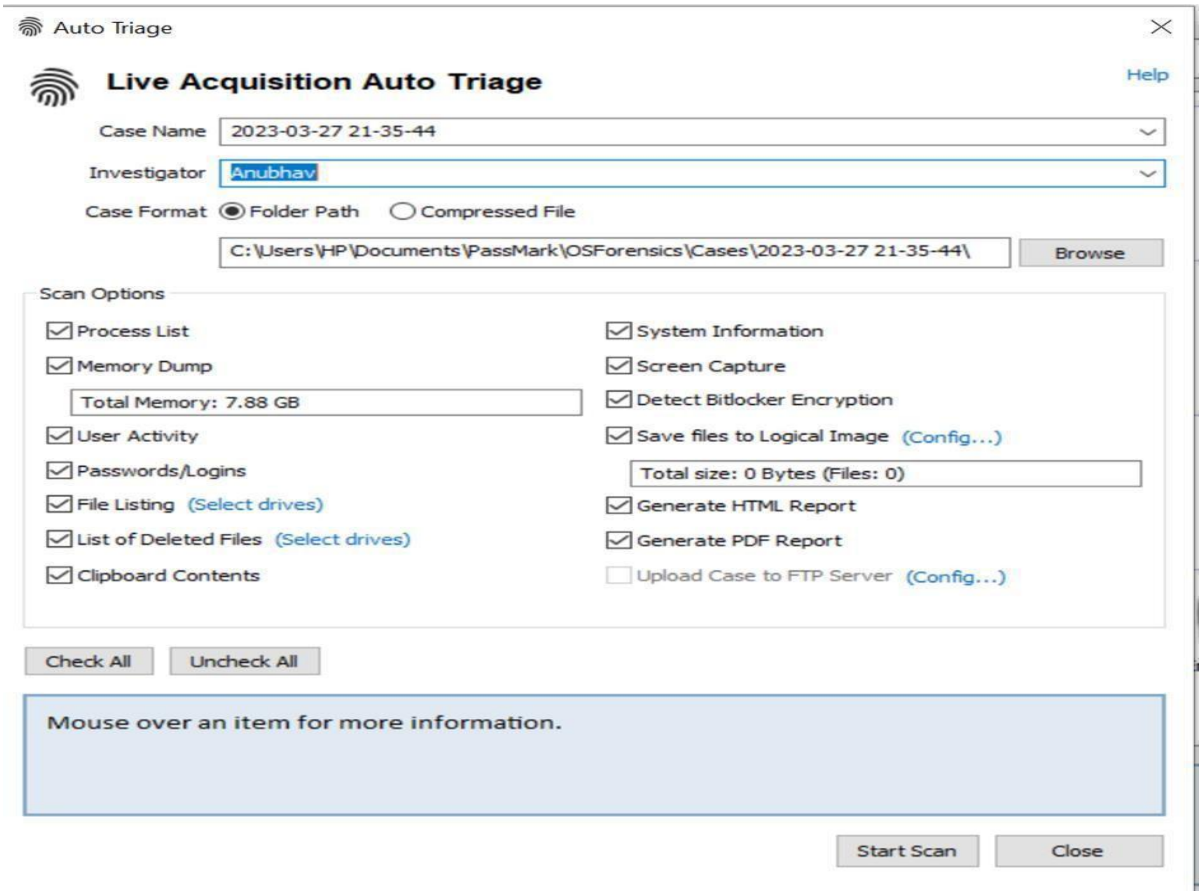
Step 5: Choose Additional Actions - In addition to creating a new report, users can take additional actions after the first AT scan. These additional features are shown in the image below.



Step 6: New Scan - Closing the AT window does not reset/delete results. Simply closing OSForensics or running a secondary scan will do it. However, this does NOT affect the generated reports. If you need to make a further check of the same drive or a different drive. Repeat steps 2–5 and choose the "New Scan" button as displayed below.

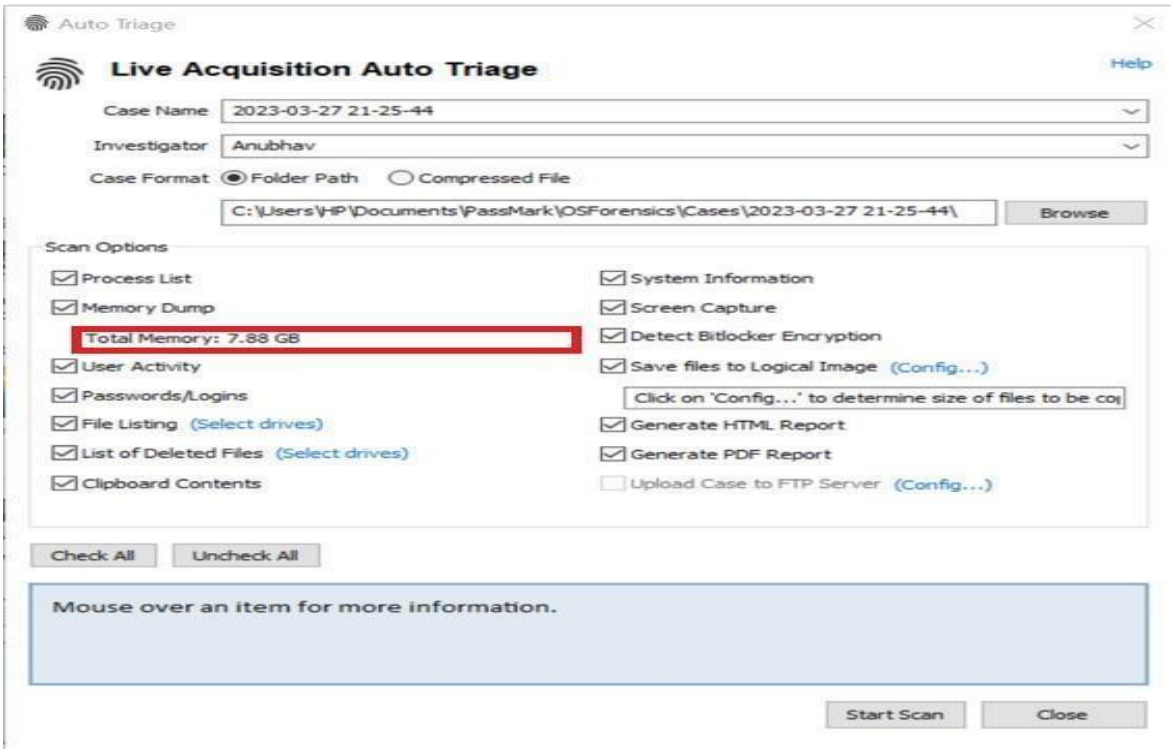


Step 7: Configurable Options - The user has the option to modify the case name that is automatically assigned. The system clock's current date and time are used as the default naming convention, which is shown as "YEAR-MONTH-DAY HOUR-MINUTE-SECOND." The user has the option to use the default configuration or insert their own name in the "Investigator" section and select a specific place to store the case data.

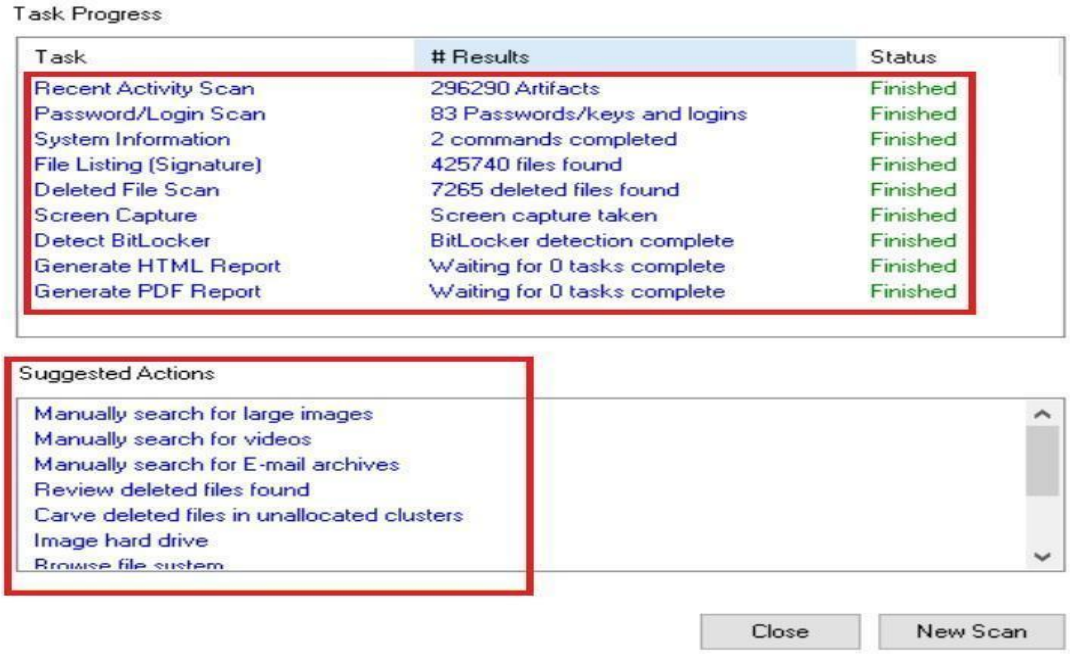


As the operating system drive and the drive where you will most likely find user activity and other interesting artefacts, the C: drive is selected as the default drive.

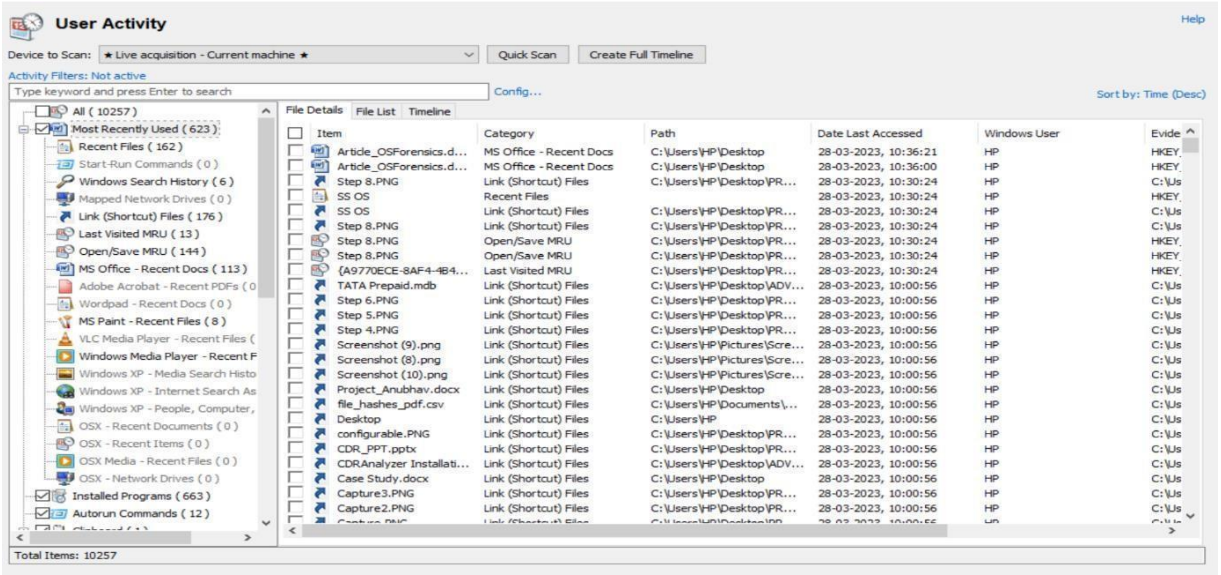
All settings are checked by default when OSF is operating. Before starting the scan, the AT will display the total amount of RAM memory on the system, as seen in the image below.

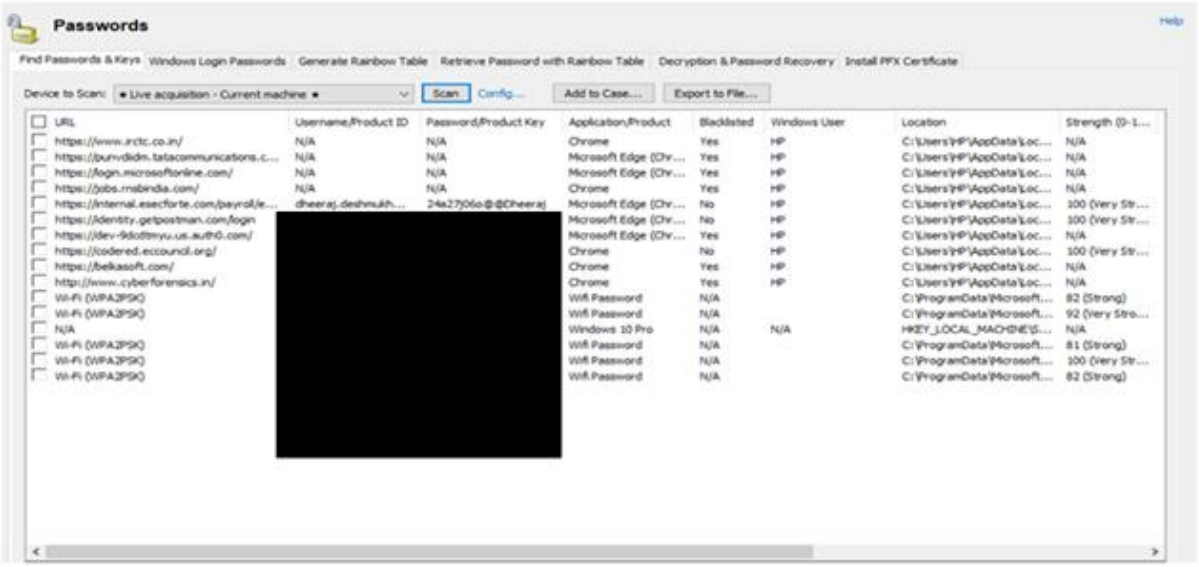


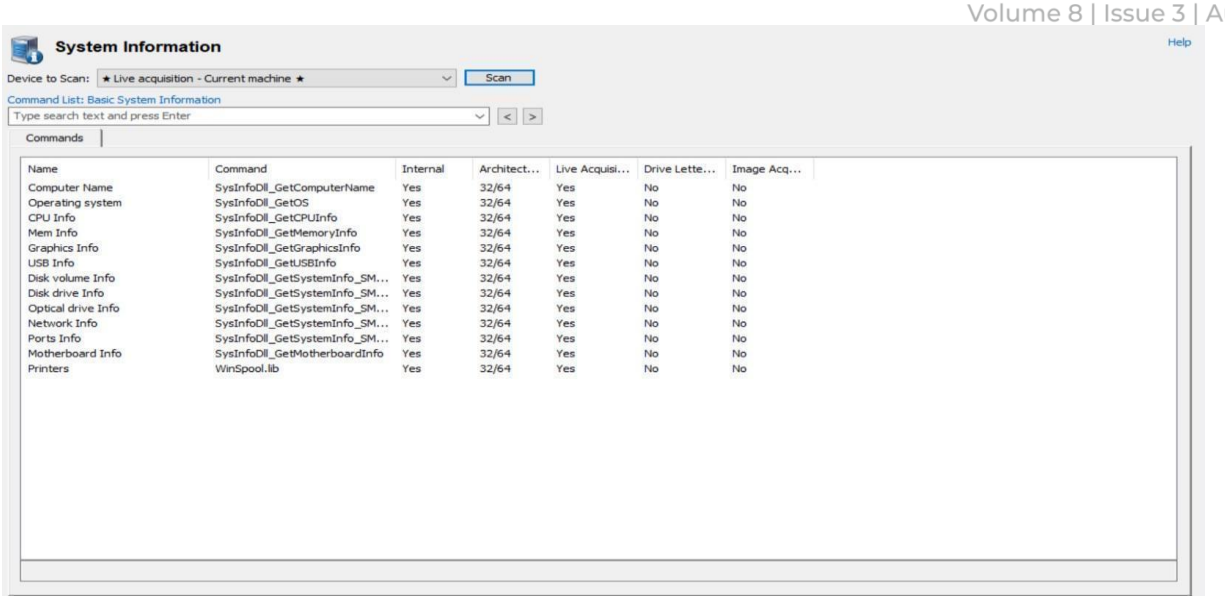
Step 8: Reviewing Results - After finished, you can either select from a variety of further options in the "Suggested Actions" pane or click on the individual scans to evaluate the results in the main OSForensics interface. You can easily shut down OSForensics if a review will be done by viewing the generated reports at a later time and date.

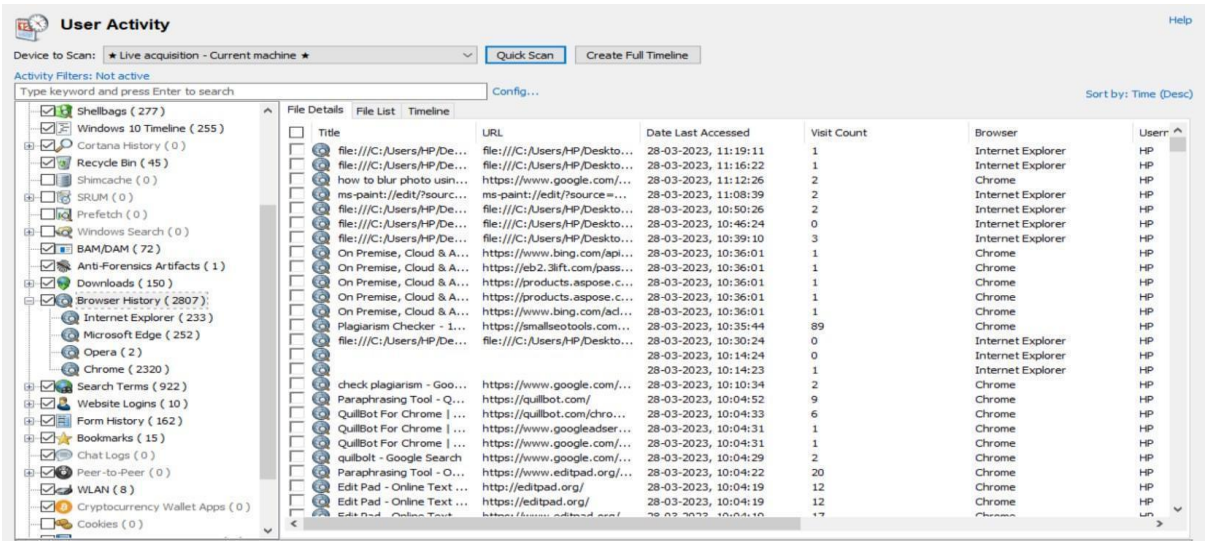


Step 9: Results - In the example given below, you can see that after the user clicked on the "Recent Activity Scan" in the AT window, the findings are displayed in the main OSForensics' interface for inspection. By clicking on the blue hyperlinks in the AT window, users may now study all of the scan's findings (such as Recent Activity, Passwords and User Accounts, System Information, Deleted Files, Browse History etc.).









During the review, users can add files of interest to the case using the tick and right-click options, and then create a new report by clicking "Create New HTML/PDF Report" in the Advanced Features list.

Conclusion - It is impossible to prevent memory content modification when conducting live forensic analysis to gather evidence. Advanced forensic tools are needed in live forensic analysis not only to gather and analyse data but also to resolve any ambiguity or conflicts that may have been introduced by their implementation. Tools used to capture memory images, for instance, can swap or reassign the memory addresses. Calculating the effects of memory changes brought on by the use of forensic tools is extremely challenging but not impractical. Therefore, it is more crucial to quantify the amount of volatile memory material that has been altered as a result of the use of forensic tools; as a result, the information gathered by memory analysis tools must be accurate and consistent with the actual data at the time it was acquired. One of the many causes of memory change is the loading and operation of memory content gathering tools, which have an impact on the key traces.

Digital attacks have become far more frequent as a result of the worldwide Internet user population growing quickly. Consequently, it is necessary to build effective approaches and tools to quickly identify these attacks and prioritize the necessary actions without interfering with the functionality of the current system. Developing relevant triage for live digital forensic analysis requires a lot of work. In this article, we have critically analysed findings using a live forensic analysis method. This article uses auto triage in OSForensics to create a live system analysis.

ABOUT THE AUTHOR:

Anubhav Varshney
Digital Forensic Trainee at eSec Forte Technologies

Email: riishiivarshney01@gmail.com
LinkedIn: https://in.linkedin.com/in/anubhav-varshney-4391a41a2

Expertise:

Researcher & enthusiast in the field of digital forensics, mobile forensics, crime scene investigation and with knowledge in the fields of Cyber Crime Investigation & Digital Fraud Investigation.

Credentials:

He is currently Digital Forensic Intern at eSec Forte Technologies. Previously he was an intern at CFSL CBI New Delhi in the Computer Forensic Division. He has also worked for a year as Cyber Crime Investigator (Intern) in Cyber Crime Branch, (Mathura Uttar Pradesh Police) in the year 2021. He is currently pursuing his post-graduation in MBA Cyber Security Management from National Forensic Science University, Gujarat and is looking for opportunities in the field of digital forensics & cyber-crime investigation.

DIGITAL FORENSICS (4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

Volume 8 | Issue 3 | August 2023
https://doi.org/10.46293/4n6/2023.08.01.06

INTRODUCTION TO MAC FORENSICS

Author/Writer: Shrey Sharma
Email: shreyshaurya13@gmail.com

Article/Paper Highlights:

The author highlights the Mac Forensics investigation of the devices, explains the utility tools available in Mac devices for security enhancement and covers the Apple device architecture for the forensics analysis and briefs about multiple artifacts paths with explanation.

– Editorial Team, Digital Forensics (4N6)

I. INTRODUCTION

With the recent introduction of Apple's new silicon chips, the MacBook has once again emerged as a leading contender in the market. As the Mac user base continues to grow, it's natural to see an increase in cases involving this state-of-the-art device.

The MacBook stands out from traditional laptops due to its robust security measures and Apple's sophisticated ecosystem-. In macOS 10.13, Apple made a significant shift from the HFS+ file system to the advanced APFS file system, which we will explore in detail in this article. In 2020, Apple made a momentous decision to transition from Intel chips to their high-performance silicon-based chips. The first of these chips, the M1 chip, boasts impressive features such as ARM architecture, delivering faster and more efficient performance compared to Intel's x86 chips. However, this transition presented challenges as numerous companies and tools struggled to adapt to the new Mac architecture. Consequently, forensic analysis of Mac devices became more complex, as not many software solutions fully support and keep up with macOS.

This article serves as a foundational guide to Mac Forensics, highlighting the distinctions between analyzing a MacBook and a Windows laptop. We will explore the fundamental elements of macOS, including its built-in features like Keychain, FileVault, and Time Machine. Additionally, we will delve into alternative approaches to the Windows registry and introduce essential files that can uncover critical information during forensic analysis.

II. THE MAC

As of July 2023, the most recent version of macOS is Ventura 13.4.1. Unlike Windows, macOS is built on a UNIX kernel and adopts a different approach to storage. Instead of using drives, everything in a macOS computer is considered as a file organized under directories in a B-Tree structure hierarchy. It's important to note that macOS doesn't run '.exe' files like Windows does, but instead utilizes the '.app' and '.dmg' extensions for its applications.
MacOS comes with several built-in programs designed to enhance the security of the laptop. Here are a few noteworthy examples:

- **Console:** Console is an application that provides forensic investigators with access to system logs, allowing them to analyze and troubleshoot macOS issues and investigate potential security incidents.

- **Disk Utility:** Disk Utility is a valuable tool for forensic analysis as it enables investigators to examine and manipulate storage devices, including creating disk images for forensic preservation and analysis of data.

Fig. 1. Pre-installed apple softwares

- **FileVault:** From a forensic standpoint, FileVault encryption adds an extra layer of security to the Mac's storage. It presents a challenge for investigators as they need to employ specialized techniques to decrypt and analyze the encrypted data during forensic examinations.
- **Gatekeeper:** Gatekeeper plays a role in forensic investigations by helping to prevent the execution of potentially malicious software. Investigators need to consider Gatekeeper's settings and any exceptions made to ensure a thorough analysis of the system.
- **macOS Firewall:** The built-in macOS Firewall serves as an important component in network forensics, allowing investigators to analyze incoming and outgoing network connections, detect unauthorized access attempts, and identify potential communication with malicious entities.
- **XProtect:** XProtect's role in forensic investigations is crucial as it acts as a baseline defense against known malware. Investigators need to consider XProtect's logs and database updates to identify any malware that may have been present on the system.
- **Keychain Access:** Keychain Access is a valuable resource for forensic examiners as it stores passwords and certificates. Investigators can analyze the Keychain to uncover stored credentials, encryption keys, and other sensitive information relevant to their investigation.
- **Time Machine:** Time Machine presents forensic opportunities by providing investigators with the ability to restore files and recover system configurations from backups. It can be used to analyze changes over time and recover important data in the event of data loss or system com- promise.
- **Terminal:** The Terminal offers forensic analysts a command-line interface for conducting advanced forensic tasks. It allows them to execute commands, run scripts, and perform various security-related tasks for in-depth analysis and investigation.

III. APPLE FILE SYSTEM

The file system in macOS is divided into various domains that categorize files and resources according to their intended use. Through a focus on a certain group of files, this division streamlines the user experience. Additionally, access privileges are set to each domain to protect files from illegal changes.

The User Tree, also known as the ”home” folder, is a user's profile in macOS, containing separate applications, settings, documents, and temporary files. Each user account operates within their own isolated environment, with read and execute access to applications and capabilities within the Local and System Trees. The home directory is portable and can be easily transferred between systems, making it relevant during forensic investigations. Users can create an ”Applications” directory within their home directory, enabling installation and running without administrative privileges. The User Tree is fully owned and controlled by the user, and administrative users can access it through the Terminal with proper authentication.

The Local Tree is a directory system that contains files and folders that are significant for daily computer use and are accessible to all users. It includes the /Applications/ and /Library/ folders, and if present, the /Developer/ folder. Administrative group users can modify files and folders within the Local Tree, but must authenticate their actions. The Tree includes applications, utilities, and library resources, and is subject to frequent modifications by users, such as software installations, preference adjustments, and shared spaces like the Documents folder. Users may not always be aware of these changes, even if prompted to provide their username and password.

Resources shared by users on a local area network (LAN) are included in the network tree. This domain mostly consists of network file servers that store programs and data that network users can access. Everything in this domain remains under the administrator's control.

The system tree contains essential system software installed by Apple. These resources are vital for the proper functioning of the operating system and cannot be modified, added, or removed by users.

By organizing files and resources into distinct domains, macOS ensures a structured and secure environment while al- lowing users to manage their own files within the user domain. The local and network domains provide shared resources, while the system domain remains immutable to maintain system stability and integrity.

In addition to these common directories, the Finder has a large number of files and directories that are hidden from the user. When the finder is open, you can inspect these by hitting Command + Shift + '.' or by using the Terminal (Apple's command prompt) using Linux commands like 'ls'. These concealed folders and files are now visible in a gray font. This is because changing these files could cause the system to behave improperly.

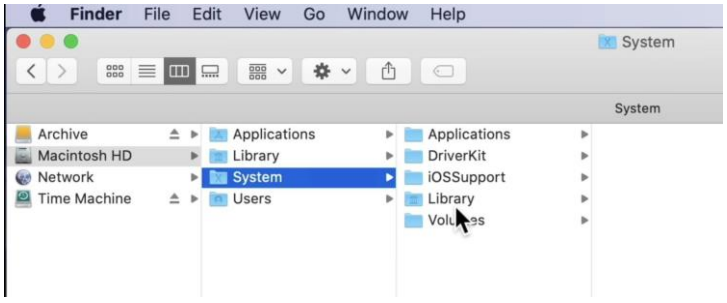


Fig. 2. Standard Directories

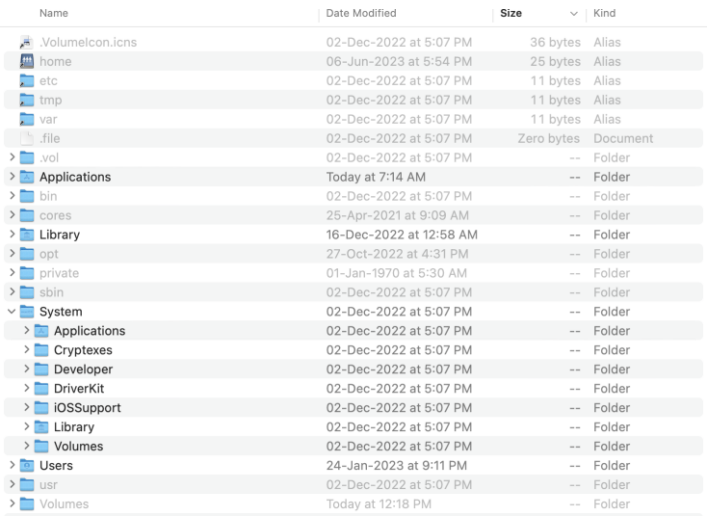


Fig. 3. Standard Directories

IV. IMPORTANT ARTIFACTS

During the forensic analysis of a MacBook, various directories hold crucial information for uncovering evidence. The ".Trashes" directory at "/Volumes/[VolumeName]/.Trashes" contains Trash folders for different mounted volumes, potentially revealing remnants of deleted files from external drives, network shares, or other storage devices.

The "/Volumes/[VolumeName]/.Spotlight-V100" directory pertains to the Spotlight indexing system, which maintains indexes of file metadata and content. Deleted files may leave residual metadata in the Spotlight index files, particularly if they were indexed prior to deletion.

In case Time Machine backups are enabled, the "/Volumes/[VolumeName]/Backups.backupdb/[ComputerName]" directory stores older backup snapshots that could facilitate the recovery of deleted files.

For tracking file changes and maintaining consistency, ma- cOS utilizes journaling and metadata systems, which store relevant information related to file access, timestamps, and other metadata. While not directly equivalent to ShellBag, these systems, located at "/private/var/db," can offer valuable insights.

Additionally, application-specific caches and logs found at '/Users/[Username]/Library/Caches' and '/Users/[Username]/Library/Logs' may contain traces of recent file activity and usage. Alongside these, the analysis of user account artifacts, such as user home directories at '/Users/[Username]' and user-specific configuration files like '/Users/[Username]/.bash_profile' '/Users/[Username]/.bashrc' and '/Users/[Username]/.zshrc' provides valuable information.

Browser profiles and data, including Safari and other apps, can be found at "/Users/[Username]/Library/Application Support/Google/Chrome" and "/Users/[Username]/Library/ Safari," respectively.

Furthermore, mail data resides at "/Users/[Username]/Library/Mail." System configuration and logs, system preferences and configurations, and network information and settings are located at "/var/log," "/Library/Preferences," "/System/Library/Preferences," and "/Library/Preferences/SystemConfiguration," respectively.

Web browsing artifacts, including caches, histories, cook- ies, and DNS cache, can be examined at various paths such as ”Application Support/Google/Chrome,” and ”/pri- vate/var/db/dnsleaktest.” File and file system artifacts, network artifacts, and system metadata also contribute to the forensic analysis. These include file system metadata, file access logs, deleted files and remnants, network connections, network interface configurations, DHCP lease information, serial numbers, hardware information, system startup and shutdown logs. Lastly, the ”securityd” process, responsible for user authentication and security, can be found at ”/usr/sbin/securityd.” By examining these directories and artifacts, forensic analysts gain insights into file deletion, metadata, backups, application behavior, system configurations, network activity, and user authentication within the macOS environment.

REFERENCES

[1] https://developer.apple.com/library/archive
[2] http://files.peelman.us/BasicMacForensics.pdf
[3] https://ieeexplore.ieee.org/document/8530928
[4] https://www.ijrte.org/wp-content/uploads/papers/v7i6s/F02090376S19.pdf
[5] https://www.dataforensics.org/mac-os-x-forensics-analysis/
[6] https://www.ntfs.com/index.html

ABOUT THE AUTHORS:

Shrey Sharma
DFIR (intern), eSec Forte Technologies

LinkedIn -https://www.linkedin.com/in/shrey-sharma-13a09323a/

Expertise:

With a passion for cyber security, Shrey aspires to establish himself as a renowned expert in the field. He possesses a deep-seated determination to delve into the intricacies of the Apple environment, seeking to acquire profound knowledge and expertise in this domain.

Credentials:

Shrey Sharma is an accomplished student currently pursuing a Bachelor of Technology degree in Computer Science Engineering from the esteemed Shiv Nadar Institute of Eminence.

Lab Systems

Request a Demo

NEW AGE AUDIO & VIDEO FORENSICS LABORATORY

Image Enhancement & Authentication

Audio Analysis & Authentication

Video Enhancement & Authentication

CORE SERVICES

- Network & Cloud Forensics
- Mobile Forensics
- Audio Forensics
- CDR/IPDR Forensics
- Disk Forensics
- Video Forensics

OUR PARTNERS

FOCLAR
FORENSIC MULTIMEDIA ANALYSIS

Anubhooti Solutions

LABSYSTEMS.CO.IN | CONTACT@LABSYTEMS.CO.IN | (022) 28794636

DIGITAL FORENSICS (4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

Volume 8 | Issue 3 | August 2023

https://doi.org/10.46293/4n6/2023.08.01.07

CRITICAL ANALYSIS OF MALWARE FROM DIGITAL FORENSIC VIEWPOINT

Authors/Writers: Avinash Kumar, Parth Trilokchandani, Shubham Pareek

Article/Paper Highlights:

This article enlightens analysis of malware artifacts, aiming to explore their types, generation methods, and significance in the field of cyber security. It also explores both static and dynamic malware artifacts in the analysis.

– Editorial Team, Digital Forensics (4N6)

Abstract

Malware continues to pose significant threats to the security and integrity of computer systems and networks worldwide. To effectively combat these threats and investigate cybercrime incidents, it is crucial to analyze malware from a forensic perspective. This article presents a comprehensive analysis of malware artifacts, aiming to explore their types, generation methods, and significance in the field of cyber security. Furthermore, by offering a complete review of malware artifacts and their significance in the broader context of cyber security, this article adds to the field of malware analysis.

1. Introduction

The procedure to preserve, to identify, to extract and to make a document of computational storage media that could be produced in legal institutions is termed as digital forensics [1]. Malware is a crafted code that is created to compromise computer systems, networks or devices without the consent of the owner [2]. Malware forensics is the study and analysis of malicious software (malware) using forensic methodology and techniques. It entails the methodical analysis of malware samples to acquire data, comprehend its behaviour, and pinpoint the malware's origin, function, and effect [3]. In this article, we explore static and dynamic malware artifacts.

2. Methodology

The below subsections explore the Static and dynamic malware artifacts. Artifacts are terms used to describe different types of evidence or indicators related to malicious software.

2.1 Static Malware Artifacts

Static malware artifacts refer to the characteristics and properties of malware that can be analyzed without executing or running the actual malicious code. These artifacts can be observed or extracted from the malware file itself or its associated components. Some common static malware artifacts include:

- **File Hashes:** Cryptographic techniques (such as MD5, SHA-1, or SHA-256) that generate unique identifiers that represent the content of a file. They can be used to identify previously identified malware samples.

- **File Structure:** The malware file's internal structure and organization, which can give information about its capabilities, code sections, or embedded resources.
- **Strings:** Textual data encoded in malware files that may contain recognized patterns, URLs, command and control server addresses, encryption keys, or other evidence of malicious intent.
- **Metadata:** Information about the file, such as the file name, creation date, author, version, or other embedded metadata that can reveal more about the malware.
- **Pack/Obfuscation Techniques:** Malware authors use techniques such as file packers, encryption, or obfuscation to conceal or protect malicious code. Identifying these strategies can aid in understanding the malware's intricacy and sophistication.

2.2 Dynamic Malware Artifacts

The actions and behaviors of malware that have been detected during its execution or runtime are referred to as dynamic malware artifacts. The majority of the time, these artifacts are gathered via dynamic analysis approaches, such as executing the malware in a sandbox or seeing how it behaves on an infected device. Here are a few examples of dynamic malware artifacts:

- **Network Traffic:** The communication patterns, network connections, protocols utilized, and data transferred between the malware and other systems infected with it.
- **Process Behavior:** The malware's interactions with the host system, such as generating or editing files, changing system settings, injecting code into other processes, or manipulating registry data.
- **System Calls and APIs:** Malware function calls used to interface with the operating system or other software components. The analysis of these calls can offer information about the malware's capabilities and objectives**.**
- **Memory Artifacts:** Data and structures left in the system's memory by the malware during execution, which might include injected code, hooks, or other runtime alterations.
- **Malware Persistence Mechanisms:** Malware techniques used to keep malware present on an infected system after a reboot or system shutdown, such as adding startup entries, altering system settings, or installing rootkits.

3. Conclusion:

Understanding static and dynamic malware artifacts is critical for malware detection, analysis, and mitigation. While static artifacts can provide preliminary information about the type of malware, dynamic artifacts provide a more in-depth knowledge of its activity and possible impact on a system or network.

References

1. K. Bellin and R. Creutzburg, "Conception of a Master Course for IT and Media Forensics Part II: Android Forensics," *2015 Ninth International Conference on IT Security Incident Management & IT Forensics*, Magdeburg, Germany, 2015, pp. 96-105, doi: 10.1109/IMF.2015.19.

2. R. R. Branco and G. N. Barbosa, "Distributed malware analysis scheduling," *2011 6th International Conference on Malicious and Unwanted Software*, Fajardo, PR, USA, 2011, pp. 34-41, doi: 10.1109/MALWARE.2011.6112324.

3. P. Ren, W. Liu, D. Sun, J. -p. Wu and K. Liu, "Analysis and forensics for Behavior Characteristics of Malware in Internet," *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, Auckland, New Zealand, 2016, pp. 637-641, doi: 10.1109/PST.2016.7906999.

ABOUT THE AUTHORS

Mr. Avinash Kumar, Assistant Professor,
SITAICS, Rashtriya Raksha University, India.

Expertise:

Avinash Kumar is NCSC Certified (GCHQ) Certified and EC Council - Certified Ethical Hacker (CEH). Also, he has worked as a Security Analyst. His area of interest is Reverse Engineering.

Credentials:

Avinash Kumar is Assistant Professor at SITAICS, Rashtriya Raksha University and completed his M.Sc. in Cyber Security from the United Kingdom.

Parth Trilokchandani

M.Sc. In Cyber Security & Digital Forensics

SITAICS, Rashtriya Raksha University

Only.project.2021@gmail.com

Expertise:

Parth has good understanding of the Cyber Security and Digital Forensics

Credentials:

Parth is currently pursuing his M.Sc. in Cyber Security & Digital Forensics from Rashtriya Raksha University. He wants to make his career in the Cyber Security field and serve the nation in the same.

Volume 8 | Issue 3 | August 2023

Shubham Pareek

MSc. In Cyber Security & Digital Forensics

SITAICS, Rashtriya Raksha University

Shubhampareek2023@gmail.com

Expertise:

Shubham has good expertise in the concepts of Cyber Security and he has completed some research in Cyber Security and Digital forensics.

Credentials:

Shubham is currently pursuing his M.Sc. in Cyber Security & Digital Forensics from Rashtriya Raksha University.

OUR SPECIALISTS

CHFI XRY CERTIFICATION
CCSK CELLEBRITE CERTIFIED OPERATOR
ISO 27001:2013 LEAD AUDITOR OSCP
PALO ALTO CERTIFIED CISSP CEH
CISA CISM SALVATIONDATA CERTIFIED
PCI DSS QSA CERT-INDIA PMP
ACCESSDATA CERTIFIED CDFE

CASE STUDIES

Forensics Infrastructure Setup For State Law Enforcement Agency

Digital Forensic Lab Setup For Strategic Research Lab

Advanced Digital Forensic Setup For State Forensic Science Laboratory

Provided Advanced Forensic Training For Law Enforcement Officer

OUR PARTNERS

Atola TECHNOLOGY · opentext™ · BITMINDZ · SANDVINE · Crackbox · ELCOMSOFT DESKTOP, MOBILE & CLOUD FORENSICS
Cellebrite · MAGNET FORENSICS · hex-rays · MSAB · TEELtechnologies · Kinesense intelligent video analytics
exterro · INTEL471 · sixgill · ASI ASSISTANT INVESTIGATOR

New Delhi
A-2/10, A-2 Block, Rohini Sector- 5, New Delhi – 110085

Gurugram
Plot No. 285, Udyog Vihar, Phase- IV, Gurugram, 122015

Mumbai
Plot C-59, Bandra Kurla Complex, Bandra East, Mumbai – 400051

Bangalore
143, 3rd Floor, 10 th Cross, Indiranagar 1 st stage, Bangalore – 560038

Singapore
1 North Bridge Road, # 11-10, High Street Centre, Singapore - 179094

Sri Lanka
Level 26 & 34, East Tower, World Trade Center, Echelon Square, Colombo, 00100, Sri Lanka

www.esecforte.com contact@esecforte.com

DIGITAL FORENSICS (4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION
Volume 8 | Issue 3 | August 2023
https://doi.org/10.46293/4n6/2023.08.01.08

VITALITY OF DIGITAL FORENSICS IN ANALYSIS OF DARK WEB

Author/Writer: Hrutuja Kondre, Avinash Kumar, Tanmayee Tilekar

Article/Paper Highlights:

This article enlightens the role of Digital Forensics in analysis of Dark Web over TOR browser. Also, covers the various aspects of investigating dark web like crime committed in the Dark Web, types of evidence, role of forensics, analysis techniques and challenges to complete the investigation process of Dark Web.

– Editorial Team, Digital Forensics (4N6)

Introduction

The "dark web" refers to a section of the internet that is intentionally hidden and inaccessible to traditional search engines. It is a system of websites and online platforms that can only be accessed with specific software, authorization, or settings. On overlay networks like Tor (The Onion Router), which anonymize users and hide their identities and locations, the black web runs [1]. The dark web has become well-known because of the prevalence of illegal activities and anonymous marketplaces, despite the fact that it is not necessarily illegal. It is frequently linked to illicit products and services, such as illegal narcotics, weapons, fake money, stolen data, hacking tools, and dangerous software. The anonymity offered by the dark web facilitates these actions, making it challenging for law enforcement organizations to locate and identify those engaged. The vast majority of internet users do not need to visit the dark web, and doing so entails serious hazards, it is vital to remember. Users that browse the black web run the risk of coming across malware, frauds, and unlawful content. When using online spaces, including the dark web, it is typically encouraged to use caution and prioritize personal safety and cybersecurity [2].

I. Importance of Investigating Dark Web

Researchers claim that only 4% of the internet is accessible to the general public, with the remaining 96% being "The deep web". The Dark Web, also known as the dark net, can be said to be a subsection of the deep web that contains websites that provide or sell goods or services like illegal narcotics, hacking tools or services, fake cash, and weapons in exchange for payments made in the form of the anonymous cryptocurrency known as Bitcoin. Additionally, there is a financed "Assassination market" where anyone can pay to have someone killed. [2,3] The dark web has become a popular location for people or groups looking to avoid being discovered by national or local law enforcement because of its complete anonymity. Others converse with journalists to provide them with private information in an anonymous manner, on the other hand. Depending on the activity they intend to carry out on the dark web, users are recommended to tape over the webcam on their computer to prevent other users from viewing them. According to The Independent, British Prime Minister David Cameron established a new intelligence organization to monitor the "Dark Web" on December 10, 2014. "The dark net is the next side of the problem," claims Cameron, "where pedophiles and perverts are sharing images, not using the normal parts of the Internet we all use[2,4]."

Data that has been recovered from digital media and/or devices is examined scientifically as part of digital forensics, among other things. "Digital evidence" or "electronic evidence" refers to information

found on digital devices[5]. Hard discs and other storage devices are where digital evidence is most frequently located, but network traffic, mobile devices, and embedded systems can also include it [6]. As a result, any information gathered via the dark web may be considered to constitute evidence. Researchers have provided principles, techniques, models, and frameworks for structuring and optimizing digital forensics investigations over the years while keeping in mind that the field of digital forensics is still relatively "young" [7,8] Every organization tends to "develop its procedures" for investigations, according to Ieong, who claims that there are "over hundreds" of digital forensics investigation techniques. The 14-phase harmonized digital investigation process model described by Mumba & Venter [9] seeks to represent the gold standard for digital investigations. The dark web, being so indulged in helping criminals in committing numerous crimes, is a crucial aspect that needs to be investigated [1].

II. Crimes Committed with Dark Web

The following list of eight serious crimes, which can be viewed as the key justifications for the use of the dark web:

1. Human and Sex Trafficking:

With 2.5 million people globally ensnared in contemporary slavery, human trafficking and sex trafficking pose serious threats to human rights. Victims are coerced into working in slave-like conditions as domestic workers, factory employees, child soldiers, beggars, sex workers, and laborers in a variety of commercial businesses [10]. Trafficking networks can evade the government's and anti-human trafficking organizations' detection, censorship, and monitoring technologies. According to the International Labour Organisation (ILO), there were almost 40.3 million modern slaves in 2017, including 24.9 million who were subject to forced labor and 15.4 million who were forced into marriage. In the commercial sex sector, women and girls are exploited by 99% and 58%, respectively [11]. Over 21,000 people called a federally funded hotline for victims of trafficking in 2014, and the Department of Justice obtained 184 convictions for trafficking, up from 174 in 2013. The majority of victims are young, defenseless foreign females who are tricked, deceived, and frequently abducted before being forced into prostitution [12,13].

2. Pornography Industry:

Women, teen girls and children are primarily exploited by the pornographic industry through sex and human trafficking. Traffickers coerce victims into signing contracts for the creation of pornography, record movies without their knowledge, and then sell the content to the interested criminal parties. Recordings and pictures are also seen to be posted on their websites. These businesses conceal the identities of its victims and offenders while recruiting them or kidnapping them via the Dark Web, social media, and online forums. Videos and photographs of prostitution on the internet show new kinds of violent crimes being committed. Social media has increased the sophistication of prostitution monitoring, making it challenging to properly speak with victims and witnesses and monitor behavior[13,14].

3. Assassinations and its Marketing:

With websites like “MailOnline, White Wolves, and C'thuthlu” posting advertising for criminals with hiring rates ranging from $10,000 to $12,000 in the US and $12,000 in Europe, the Dark Web is a popular venue for criminals to market their assassin talents. Thirteen illegal onion sites, including the Silk Road forum, the Sheep Market forum, and the Black Market Reloaded forum, have been discovered by researchers[15]. The Silk Road was the most restricted Deep Web marketplace from 2011 to 2013 for purchasing drugs, exchanging political opinions, and advocating personal freedom, free markets, and minimal government[16,17,]. Despite being operational for less than three years,

members of Silk Road believed their transactions were anonymous because they used Tor's hidden service and bitcoin. However, on 1st October, 2013, the FBI, IRS, and DEA took control of the market and detained 'Silk Road's' founder 'Ross Ulbricht', putting an abrupt stop to the site's prominence. Ulbricht was charged with funding the attempted killings of two business partners who he thought had betrayed him. Bitcoins worth $3.6 million were seized by the Justice Department after it shut down the Silk Road website [18,19].

4. Drug Transactions:

Drug markets on the Deep Web can be divided into two categories: specialized markets for particular drugs like heroin, which are well-liked because of product expertise and vendor customer relationships, and general shops for customers offering all kinds of illicit goods, such as credit cards, stolen jewellery, credit cards, weapons, pornography, and stolen jewellery. A digital illicit market for drugs has emerged thanks to a huge increase in drug transactions on the Deep Web[20,21,22].

Popular Dark Web bazaar Silk Road sold drugs for over a billion dollars through drop shipment or DHL. Several additional cryptocurrency markets on the Dark Net have developed since Silk Road was shut down in 2013. From January 2014 to March 2015, Evolution, a well-known cryptocurrency market, discovered approximately 48,000 postings and over 2700 dealers claiming to send illicit drug products from 70 countries. However, despite exact digital information on concealment strategies and shipping nations, it was discovered that the quality of illicit narcotics varied from the data in the corresponding listings. Another darknet marketplace for narcotics including cocaine and marijuana, Mr. Nice Guy, has better security and registration protection than regular websites [23].

5. Child Pornography:

As more kids use social media and apps like Omegle and Ask.fm to conceal their identities, pedophiles are taking advantage of these sites to spread obscene photographs and engage in child pornography. With Freedom Hosting deploying 550 servers across Europe, pedophiles and criminals frequently use the Dark Web for child pornography. In Operation Pacifier, which involved 2 million users, 23 thousand explicit photos, and 9 thousand explicit video files, the FBI detained hundreds of pedophiles. The suicide of Canadian teenager Amanda Todd, 15, brought attention to the growing danger of child exploitation online. With victims making money by selling their live sexual photos through Voice-over-IP (VoIP) programmes, webcam child prostitution has grown to be a serious issue[24,25].

Around 100 sites with thousands of visitors were hosted by Freedom Hosting, which was identified as hosting 95% of the child porn on the TOR network in 2011[26]. Hackers who could identify the users in 2017 stated that over 50% of the content on Freedom Hosting II was related to child pornography[27]. At least 23 exploited children from the United States of America, Spain, and the United Kingdom were saved after Jong Woo Son, a 23-year-old South Korean who ran the largest child exploitation website Welcome to Video, was accused and detained in 2018.

6. Terrorist Markets for Cybercrime Tools and Stolen Data

The Deep Web is a major threat to the security of various nations because of terrorism and terrorist organizations there. Terrorist organizations like al-Qaeda/ISIS have reportedly been known to have utilized the Dark Web to spread propaganda, generate money, and transmit information when command changes. ISIS uses Bitcoins to pay for services on the Dark Web, and the US Military also monitors ISIS there. However, neither the military nor law enforcement have been able to track ISIS without violating the privacy rights of individuals. ISIS seeks for fighters from all over the world, transmits media, and uses the Dark Web as a weapon of terrorism by, among other things, streaming and recording the execution of prisoners. ISIS went to the Dark Net to shield its members' identities

and prevent hackers. Using DarkNet sites and other platforms, they disseminated news and misinformation following the Paris attacks in November 2015[29,30].

ISIS coordinates by organizing activities and talking about command and control in front of a large audience. Small drones are employed to gather real-time data for propaganda, while messaging apps like Skype and WhatsApp are utilized to relay messages across the battlefield. ISIS recruits by utilizing slickly produced online periodicals to spread its ideologies and create weapons for terrorist strikes. These five categories—propaganda, recruiting and training, funding, communications, and targeting—are used to classify terrorist activity on the Internet[31].

7. Markets for Cybercrime Tools and Stolen Data

Cybercriminals frequently purchase their tools for cybercrime from anonymous markets and sell stolen or leaked data on the Dark Web. Some of the most well-known and developing Dark Net markets are the Silk Road forum, Black Market Reloaded forum, and Sheep Market forum. These markets have changed over time, with a significant chunk of their ecologies being examined between 2013 and 2015[32]. Some of these marketplaces have had police seizures, voluntary closures, and closures that are thought to be fake. These online markets also offer for sale personal information, financial records, credit card information, cloned pins, and other information that has been stolen or leaked[33].

Darknet markets providing goods and services related to fraudulent hacking have been looked at utilizing various techniques that have been established. Data thieves and cybercriminals trade information about dangerous software and services that help assist online crime via forums and underground black markets. Empire Market, Wannabuy RDP, UAS Service RDP, Hydra, SLILPP, UNICC Shop, Cannazon, Monopoly Market and Tochka Market are among the rising and active marketplaces according to DNStat [34].

8. Dark Net Currency Exchange Using Bitcoin:

Silk Road made approximately $1.2 billion using Bitcoin, a cryptocurrency that permits anonymous transactions on dark net markets. Bitcoin's legal usage has been in question, yet money laundering has been encouraged by it[35]. Three steps are involved in money laundering: introducing illicit monies into the established financial system, hiding them behind further transactions, and integrating them into the system to provide the impression that the funds are legitimate. Between 2013 and 2016, The Elliptic forensics analysis tool was used to track down bitcoins coming from illegal sources[36]. Although the blockchain's publicly accessible data can be analyzed, fraudsters use the Escrow system to avoid being taken advantage of [36].

III. Role of Forensics in analysis of crimes

Given that anyone may access the dark web using the TOR browser and that the majority of dark web sites conduct transactions using Bitcoin, the proposed forensic methodologies for darknet forensics are divided into two categories: TOR forensics and Bitcoin forensics.

A. TOR browser Forensics: Forensics of the TOR browser Four alternative methods can be used to extract evidence relating to the TOR browser.

1. **The RAM Forensics:** Volatile memory forensics include RAM analysis. The RAM dump will be captured using the Belkasoft RAM capturer, and the hexadecimal view of the RAM dump will be seen using Hex dump. The goal of RAM forensics is to gather information about the file kinds and websites visited.

2. **Registry changes:** Regshot will do registry forensics, and the evidence it extracts will reveal information on the installation of TOR and the most recent access date.

3. **Network forensics:** Using network miner and wireshark, network forensics will be conducted, and the evidence that is gathered will reveal details about web traffic.

4. **Locations database:** Database viewer can be used to view the contents of the TOR browser database, which is located at \Tor Browser\Browser\TorBrowser\Data\Browser \profile.default.

B. Bitcoin Transaction Forensics: The user's system can be used to retrieve forensic artifacts from a Bitcoin wallet programme that has been installed. Bitcoin artifacts can be recovered by Internet Evidence Finder [37].

IV. Types of Evidences Found During Analysis of Dark Web

When a forensic investigation is carried out for analysis of evidences that are procured from the Dark web, the most common evidences that are looked for can be as follows:

- **Illicit Marketplaces:** Markets that facilitate the sale of unlawful products and services include dark web markets. Listings for narcotics, weapons, stolen data, hacking tools, fake money, false documents, and other items are examples of evidence. This information can be used to locate criminally linked sellers, buyers, and transactions.

- **Records of Communication:** Discussions and conversations about criminal activity may be found on dark web forums and messaging services. Investigators can find chat records, messages, and posts that reveal details about upcoming criminal activity, criminal cooperation, or the trade of private information.

- **Stolen Data and Personal Information:** On the dark web, stolen credentials, compromised databases, and personal information are frequently traded. Evidence that forensic investigators can find includes credit card numbers, social security numbers, stolen login credentials, and other personally identifiable information (PII). This information may be essential for locating victims, determining the scope of data breaches, and connecting certain people to particular cybercrimes.

- **Malware and Exploit Kits:** The dark web is a major marketplace for the sale of hacking tools, malware, and exploit kits. Investigators could come across code fragments, malware settings, or even conversations about possible targets and attack strategies as proof of malicious software. This information can be used to track down offenders, comprehend attack methods, and gauge the severity of cybercrimes[38].

- **Cryptocurrency Transactions:** On the dark web, cryptocurrency is frequently used for anonymous transactions. Blockchain transactions may be analyzed by investigators to track the movement of money, spot wallets linked to unlawful activity and associate transactions with particular people or organized crime groups. By demonstrating financial linkages, this evidence strengthens the case against those engaged in illegal activity.

- **Digital Identity and Fraud:** These are two topics that are frequently covered in dark web marketplaces. Evidence may include false identification papers, credit cards that have been stolen, guides to fraud, or aid with identity theft services. The identification of those

participating in identity fraud and fraudulent schemes may be possible with the help of this data.

- **Materials Relating to Child Exploitation:** Sadly, the dark web is renowned for housing illicit material pertaining to child exploitation. Evidence of child abuse may be found by investigators in the form of graphic photographs, videos, chat logs, or discussion forums. These resources can be used to locate child exploitation offenders, victims, and networks [39].

V. Analysis Techniques

Due to its anonymous nature and the associated technical difficulties, investigating the dark web may be a complicated and difficult operation. Investigating the dark web can help law enforcement agencies, cybersecurity companies, and other organizations find illicit activity and identify those responsible. The following are some essential components of a dark web investigation:

- **Specialized Software and Tools:** In order to access the dark web safely and anonymously, investigators frequently employ specialized equipment and software. Tor is the most popular programme, which enables users to visit websites on the dark web while hiding their IP addresses.

- **Data Gathering and Monitoring:** Investigators collect information by keeping an eye on forums, markets, and communication channels on the dark web. For the purpose of spotting potential dangers or illegal activity, they might analyze conversations, deals, and encounters.

- **Collaboration:** For dark web investigations, cooperation between various agencies and organizations is essential. To increase the investigation's efficacy, this may entail pooling knowledge, resources, and skills[40].

- **Infiltration and Undercover Operations:** To infiltrate dark web groups, law enforcement organizations may send out undercover agents or use fictitious personas. These activities have the ability to gather evidence for judicial processes, identify important individuals, and gather intelligence.

- **Cryptocurrency Analysis:** Due to their perceived anonymity, cryptocurrencies like Bitcoin are frequently used for transactions on the dark web. Blockchain transactions are frequently analyzed by investigators to track the movement of money, pinpoint specific people, and connect transactions to unlawful activity[41].

- **Legal Challenges:** Investigating the dark web includes navigating the complexities of international law as well as crossing jurisdictional boundaries, which present legal obstacles. Investigations only succeed when law enforcement authorities from many nations work together.

- Finding a careful balance between privacy and security is necessary for dark web investigations. Investigators must protect the privacy of innocent users while searching for illegal activity. To keep the public's trust and make sure that investigations follow the law, it is crucial to strike this balance [42].

These law enforcement operations can be dangerous and might backfire into the investigators losing their own data to the offenders with their personal information, which can prove to be life threatening.

It is strongly advised that these operations and investigations be carried out only by technicians and authorities who are trained for such cybersecurity roles.

VI. Conclusion:

The articles focused on various aspects, though the dark web being a very complex process would always be an area for deep research and investigation. This article can also provide a platform for future analysis of the dark web.

VII. References:

[1] Popov, O., Bergman, J., & Valassi, C. (2018). A Framework for a Forensically Sound Harvesting the Dark Web. https://doi.org/10.1145/3277570.3277584

[2] Rafiuddin, M. F. B., Minhas, H., & Dhubb, P. S. (2017). A dark web story in-depth research and study conducted on the dark web based on forensic computing and security in Malaysia. https://doi.org/10.1109/icpcsi.2017.8392286

[3] Egan, M., 2017. What is the Dark web and Deep web? [Online] Available at: http://www.techadvisor.co.uk/howto/ internet/what-is-dark-web-deep-web-3593569/

[4] Glance, D., 2016. What is the Dark Web. [Online] Available at: http://www.iflscience.com/technology/what-darkweb/ all/

[5] M-H. Maras. 2015. Computer Forensics - Cybercriminals, Laws, and Evidence. Jones and Bartlett Learning, USA.

[6] E. Casey. 2010. Digital forensics investigation and handbook. Elsevier Academic Press, USA.

[7] R. S. Ieong. 2012. FORZA - Digital forensics investigation framework that incorporates legal issues. Digital Investigation: The International Journal of Digital Forensics and Incident Response archive 3, Supplement (2012), 29–36.

[8] A. Valjarevic and H. S. Venter. 2012. Harmonised Digital Forensic Investigation Process Model. In Information Security for South Africa (ISSA). IEEE, 1–10.

[9] E. R. Mumba and H. S. Venter. 2014. Testing and Evaluating the Hamonised Digital Forensic Investigation Process in Post Mortem Digital Investigations. In Fourth International Conference on Next Generation Mobile Applications, Services and Technologies (NGMAST). ADFSL, 85–99.

[10] L. Greenemeier. (Feb. 8, 2015). Human traffickers caught on hidden Internet. Scientific American. [Online]. Available: https://www.scientificamerican.com/article/human-traffickers-caughton- hidden-internet/

[11] Geneva. (Sep. 19, 2017). Forced Labour, Modern Slavery and Human Trafficking. [Online]. Available: https://www.ilo. org/global/topics/forced-labour/lang_en/index.html

[12] C. Reilly. (Jul. 29, 2015). Human Trafficking: A Crime Hard to Track Proves Harder to Fight. [Online]. Available: https://www.pbs. org/wgbh/frontline/article/what-is-human-traf_cking-and-why-is-it-sohard- to-combat/

[13] H. J. Clawson and N. Dutch, ``Addressing the needs of victims of human trafficking: Challenges, barriers, and promising practices: Department of health and human services, office of the assistant secretary," Dept. Health Hum. Services, Washington, DC, USA, Tech. Rep., 2008.

[14] ConvenantEyes. (Sep. 7, 2011). The Connections Between Pornography and Sex Trafficking. [Online]. Available: https://www. covenanteyes.com/2011/09/07/the-connections-between-pornographyand- sex-trafficking/

[15] M. Chertoff and T. Simon, ``The impact of the darkWeb on Internet governance and cyber security," Centre Int. Governance Innovation (CIGI), Waterloo, ON, Canada, Tech. Rep. 6, 2015.

[16] W. Li and H. Chen, ``Identifying top sellers in underground economy using deep learning-based sentiment analysis," presented at the IEEE Joint Intell. Secur. Informat. Conf., Sep. 2014, pp. 64_67.

[17] J. Lane, ``Bitcoin, silk road, and the need for a new approach to virtual currency regulation," Charleston L. Rev., vol. 8, no. 5, p. 511, 2013.

[18] S. Pfeifer, S. Li, and W. Hamilton. (Oct. 2, 2013). End of Silk Road for Drug Users as FBI Shuts Down Illicit Website. [Online]. Available: https://www.latimes.com/business/la-_-silk-road-bitcoin-20131003- story.html

[19] D. Moore and T. Rid, ``Cryptopolitik and the Darknet," Survival, vol. 58, no. 1, pp. 7_38, 2016.

[20] A. Celestini, G. Me, and M. Mignone, ``Tor marketplaces exploratory data analysis: The drugs case," presented at the Int. Conf. Global Secur., Saf., Sustainability, 2017.

[21] J. Van Buskirk, S. Naicker, R. Bruno, C. Breen, and A. Roxburgh, ``Drugs and the Internet," Nat. Drug Alcohol Res. Centre (NDARC), UNSW, Sydney, NSW, Australia, Tech. Rep. 7, 2016.

[22] D. Rhumorbarbe, L. Staehli, J. Broséus, Q. Rossy, and P. Esseiva, ``Buying drugs on a darknet market: A better deal? Studying the online illicit drug market through the analysis of digital, physical and chemical data," Forensic Sci. Int., vol. 267, pp. 173_182, Oct. 2016.

[23] DeepDotWeb. (2015). Interview: `Mr. Nice Guy' Market Admin Tells His Story. [Online]. Available: https://gir. pub/deepdotweb/2015/06/03/interview-with-mr-niceguy-market-admin/

[24] K. V. Açar, ``Webcam child prostitution: An exploration of current and futuristic methods of detection," Int. J. Cyber Criminol., vol. 11, no. 1,pp. 98_109, 2017.

[25] E. Puffer, K. McDonald, M. Pross, and D. Hudson, ``Webcam child sex tourism: An emerging global issue," Cedarville Univ., Cedarville, OH, USA, Tech. Rep., 2014.

[26] K. Poulsen. (Sep. 9, 2013). FBI Admits it Controlled Tor Servers Behind Mass Malware Attack. [Online]. Available: https://www.wired.com/2013/09/freedom-hosting-fbi/

[27] The Bitcoin News. (Feb. 9, 2017). Anonymous Hacks Freedom Hosting II, Bringing Down Almost 20% of Active Darknet Sites. [Online]. Available: https://thebitcoinnews.com/anonymous-hacks-

[28] L. H. Newman. (Oct. 16, 2019). How a bitcoin trail led to a massive dark Web child-porn site takedown. Wired. [Online]. Available: https://www.wired.com/story/dark-web-welcome-to-video-takedownbitcoin/

[29] P. W. Singer and E. T. Brooking, LikeWar: The Weaponization of social media. New York, NY, USA: Eamon Dolan Books, 2018.

[30] G. Weimann, ``Going dark: Terrorism on the dark Web," Stud. Convict Terrorism, vol. 39, no. 3, pp. 195_206, Mar. 2016.

[31] Zhou, E. Reid, J. Qin, H. Chen, and G. Lai, ``US domestic extremist groups on the Web: Link and content analysis," IEEE Intell. Syst., vol. 20, no. 5, pp. 44_51, Sep. 2005.

[32] K. Soska and N. Christin, ``Measuring the longitudinal evolution of the online anonymous marketplace ecosystem," presented at the 24th USENIX Secur. Symp., 2015.
[33] R. Koch, ``Hidden in the shadow: The dark Web A growing risk for military operations?" presented at the 11th Int. Conf. Cyber Convict (CyCon), 2019.

[34] DNStats. (2019). Dark Net Stats. [Online]. Available: https://dnstats.net/

[35] J. Lane, ``Bitcoin, silk road, and the need for a new approach to virtual currency regulation," Charleston L. Rev., vol. 8, no. 5, p. 511, 2013.\

[36] Y. Fanusie and T. Robinson, ``Bitcoin laundering: An analysis of illicit flows into digital currency services," Center Sanctions Illicit Finance Memorandum, Elliptic, London, U.K., Tech. Rep., Jan. 2018.

[37] https://www.magnetforensics.com/computerforensics/bitcoin-forensics-a-journey-into-the-darkweb/

[38] M-H. Maras. 2015. Computer Forensics - Cybercriminals, Laws, and Evidence. Jones and Bartlett Learning, USA.

[39] E. Nunes, A. Diab, A. Gunn, M. Ericsson, M. Vineet, V. Mishra, V. Paliath, J. Robertson, J. Shakarian, A. Thart and P. Shakarian. 2016. Darknet and Deepnet Mining for Proactive Cyber Treat Intelligence. Intelligence and Security Informatics (ISI) (2016), 7–12. https://doi.org/10.1109/ISI.2016.7745435

[40] H. Chen. 2012. Dark web: Exploring and data mining the dark side of the web. Springer-Verlag New York. https://doi.org/10.1007/978-1-4614-1557-2

[41] D. Bryans, ``Bitcoin and money laundering: Mining for an effective solution," Ind. LJ, vol. 89, no. 1, p. 441, 2014.

[42] M-H. Maras. 2015. Computer Forensics - Cybercriminals, Laws, and Evidence. Jones and Bartlett Learning, USA.

ABOUT THE AUTHORS

Hrutuja Kondre

M.Sc. in Forensic Science

SFRMNS, Rashtriya Raksha University

Expertise:

Hrutuja wants to make her career in the field of Information Security. Her area of interest is in Cyber Security.

Credentials:

Hrutuja is currently pursuing M.Sc. in Cyber Security from SFRMNS, Rashtriya Raksha University.

Avinash Kumar

Assistant Professor,
SITAICS, Rashtriya Raksha University, India.

Expertise:

Avinash Kumar is NCSC Certified (GCHQ) Certified and EC Council - Certified Ethical Hacker (CEH). Also, he has worked as a Security Analyst. His area of interest is in Reverse Engineering.

Credentials:

Avinash Kumar is Assistant Professor at SITAICS, Rashtriya Raksha University and completed his M.Sc. in Cyber Security from the United Kingdom.

Miss. Tanmayee Tilekar

Assistant Professor,
SITAICS, Rashtriya Raksha University, India.

tanutilekar9900@gmail.com

Expertise:

Tanmayee is Certified Ethical Hacker (CEH) from EC Council. Also, she has worked as a Digital Forensics investigator. Her keen area of interest is in Digital Forensics.

Credentials:

Tanmayee currently works as an Assistant Professor at SITAICS, Rashtriya Raksha University and completed her M.Sc. in Cyber Security from the United Kingdom.

eSec Forte®

DIGITAL FORENSICS

WE DO IT DIFFERENTLY

OUR CAPABILITIES

- FORENSIC LAB SETUP
- COMPUTER FORENSICS
- NETWORK FORENSICS
- MALWARE ANALYSIS
- MOBILE FORENSICS
- EMAIL FORENSIC SERVICES
- ADVANCED DIGITAL FORENSICS
- SOCIAL MEDIA MONITORING
- CDR & CELL SITE ANALYSIS
- DIGITAL FRAUD INVESTIGATION
- HARD DISK IMAGING SERVICES
- TAKEDOWN SERVICES
- THREAT INTELLIGENCE SERVICES
- INCIDENT & BREACH RESPONSE SERVICES

CAPACITY BUILDING

We impart training based on job profiles in addition to tool/technology based training.

First Responder	Lab Assistant	Lab Analyst / Examiner	Technical / Quality Manager	Expert Witness

FORENSIC CONSULTING

- Establishment/Upgradation of a Digital/Cyber Forensics Laboratory needs to be done with due thought process in adherence to global ISO/IEC standards and law of the land.
- In India IT Act under 79A mandates that government can notify labs as EEE (Examiner of Electronic Evidence) and Ministry of Information and Technology has a procedure which notifies government labs. **We at eSec Forte® Technologies will guide / consult / design lab provide services / provide products you need to meet the requirements so that your lab can be notified. We have all the experience and expertise to assist you.**

Lt Col (Dr.) Santosh Khadsare (Retd.)

VP-Digital Forensics and Incident Response (DFIR)

Drop a message at

forensics@esecforte.com

DIGITAL FORENSICS (4N6)
INDIA'S 1st DIGITAL FORENSICS PUBLICATION

Volume 8 | Issue 3 | August 2023

https://doi.org/10.46293/4n6/2023.08.01.09

A NOVEL FRAMEWORK FOR WHATSAPP FORENSICS USING OPEN-SOURCE TOOLS

Authors/Writers: Tusharanshu Deo, Manvjeet Kaur, Pooja Kaplesh

Article/Paper Highlights:

In this article, authors highlight the analysis of WhatsApp forensics using open-source tools available over the internet on publicly available resources. Author's covers the use of multiple tools for the WhatsApp forensics and explains the detailed analysis process for the extraction of data from WhatsApp using tools. Also, proposed the framework for the WhatsApp Forensics procedure.

– Editorial Team, Digital Forensics (4N6)

Abstract

The emergence of end-to-end encryption in widely-used messaging apps such as WhatsApp has transformed the aspect of communication by providing enhanced privacy and security for user conversations. However, this increased emphasis on robust encryption techniques has also posed significant challenges for digital forensics investigations. This paper aims to provide the analysis of different latest open-source tools that are available to perform forensic investigation on the encrypted social media platform like WhatsApp and Signal etc. The primary focus is on WhatsApp due to its worldwide popularity and the extraction of useful WhatsApp artifacts with the help of different tools. This analysis will evaluate the pros and cons of each of the tools and their effectiveness in performing the investigation and will contribute to the development of more effective methods for investigating WhatsApp data. The findings of this research will be of interest to law enforcement, intelligence agencies, and other investigators who often find themselves in difficult situations to extract evidence from WhatsApp. This paper proposes a framework for extracting the useful data from encrypted WhatsApp platforms by using the best combination of open-source tools which can be proved as cost effective and can be used as an alternative to commercial tools.

Keywords: WhatsApp, Open-source tools, Encryption, Forensic.

1. Introduction

Today's Digital world has changed our day to day lives in numerous ways. We usually store our sensitive information in our mobile devices and we tend to share them through different messaging platforms. Messaging platforms like WhatsApp, Signal, and Telegram etc. have shifted to encrypted versions now. They have introduced a new technique called End to End encryption which allows only communicating parties to view the messages even if someone tries to intercept the messages such as a government agency or any potential hacker, they will not be able to access it in clear text form. Although it has captured attention around the globe as WhatsApp is the largest messaging platform in the world and with this technique it enhances the privacy of its user, providing them a secure channel to communicate. But there is a downside of it which poses a serious threat to the society because recently we have seen a surge in crimes and illegal activities like drug dealing, terrorist acts and pornography which has been carried out through this platform. It has hindered the criminal investigation very severely. In earlier days it used to be very easy to get access to the messages but now investigating crimes that involve

WhatsApp messages is almost impossible in some cases. There are still numerous ways by which forensic investigators can get access to the messages but the amount of time it takes makes it a very complex process. WhatsApp can reveal a lot of information about a user or about any particular event, and with the ever-growing popularity of this platform it is likely that the impact of its encryption on forensics will become even more significant. So, there is a need to do a thorough analysis of different approaches available to handle this problem. There are some open-source tools which are being used by the investigators regardless of their inability to access encrypted messages. This paper will provide an efficient way of gaining access to the encrypted messages and many other artifacts which can be useful in solving complex cases by using a combination of open-source forensic tools.

2. Related Work

This section will provide us some previous research and analysis which reflects their effort to obtain useful artifacts from WhatsApp on mobile devices. It covers the brief description of the tools and techniques which were carried out by different forensic investigators. The following are some studies that are relevant to this research:

Mohammed et al. described the different ways to recover encryption keys from WhatsApp, to decrypt its encrypted databases without rooting the device. Different tools and software, both open source and commercial such as DB extractor and WhatsApp viewer to view and decrypt the WhatsApp database[1].

In 2022 Mohammed Moreb et al. discussed the ways to extract the encryption keys from the latest version of WhatsApp stored in both Android and iOS devices. Many commercial tools were used on a free trial basis like MOBILedit, Belkasoft and FINALMobile in combination with some open-source tools and a detailed comparison of forensics tools was also shown[2].

Dennis Wijnberg et al. proposed a real time approach to intercept the WhatsApp communication like decrypting WhatsApp databases, using OSINT, wiretapping and many more. These methods were evaluated with different scenarios to provide real time access to suspect WhatsApp data remotely, which can be proved as a very efficient method to Law Enforcement Agencies for their investigation[3].

Aya Fukami et al. in their research proposed a model to extract data from encrypted mobile devices. It covers the impact of increasing encryption on the forensics of latest mobile devices. It focuses on invasive techniques such as exploiting smartphone vulnerabilities, bypassing security features, Physical Chip-off analysis and the legal issues related to these techniques [4].

Nagendra Rao Koppolu, Inspector of police, Telangana Police Department performed a deep analysis of WhatsApp artifacts that are useful in investigating modern crimes. It discusses the overall structure of WhatsApp including its security features and different acquisition techniques that can be performed on Android and iOS platforms. Different mobile forensics software such as MOBILedit, Cellebrite UFED etc. was used to perform the study [5].

Khalid Alissa et al. proposed the detailed comparative analysis of different WhatsApp forensics tools. Various functionalities and features supported by tools were analyzed. It also discussed the complete internal structure of WhatsApp databases and its valuable artifacts.[6].

Hasan Fayyad-Kazan et al. addressed the analysis of decrypted WhatsApp databases without rooting the device using SQLite DB Browser tool. The complete study is done on Android Device and key is extracted using WhatsApp Key/DB extractor tool[7].

Vindy Arista Yuliani et al. performed a forensic analysis of WhatsApp using the NIST framework on Android devices. This study involves a combination of commercial and open-

source tools like Oxygen forensic and Andriller that were proved to be valuable in terms of extracting encrypted WhatsApp databases [8].

3. Research Problem

The usage of messaging platforms has become ubiquitous in recent years and sharing of information through them is very common and considered to be a more reliable form. WhatsApp is a popular medium for criminals, who use it to communicate with each other and to share sensitive information which makes it a valuable source of information for law enforcement and other investigators. But due to its encrypted nature it makes it difficult for them to access and analyze the data. There are a number of open-source forensic tools available that can be used to investigate WhatsApp data. Open-source tools are free to use and it can be a cost-effective way for investigators as relying only on commercial tools does not guarantee expected outcomes. However, these tools are often limited in their capabilities, and there is a lack of research on the combination of these tools that can lead to effective results. To address this problem, this research would need to explore the best ways that these forensic tools can be combined to meet the required result. There is also a need for more research on unexplored tools that can be used to investigate WhatsApp data. There are many open-source forensic tools that have not yet been fully explored by the digital forensic community. These tools have the potential to be valuable assets in investigations, but they can only be used if they are known about.

4. Research Objective

This paper aims to collect and analyze the artifacts on the latest WhatsApp version on the Android device. This study uses a different approach and tools to achieve the following goals:

- To propose an approach or framework of extracting data by using the best combination of open-source tools.
- To extract the cipher key that is present in the internal storage of the device and uses that key to decrypt the latest WhatsApp database version.
- To provide a comparative analysis of the latest open-source tools.

5. Proposed Methodology

To implement this research in an optimal way, there are a series of steps that need to be done in order to get the required result. The proposed methodology aims to extract the decrypted contents of WhatsApp present inside the internal memory in a forensically sound manner with the help of the right selection of tools. Below subsections details about the steps taken to accomplish this.

5.1 Understanding the Internal Structure of WhatsApp

First step is to get a clear understanding of the internal structure of WhatsApp in order to become familiar with its artifacts and to determine where it stores valuable data which might be of some use for the investigation. It is the mandatory step to dive deep in any investigation that involves WhatsApp data. WhatsApp data can be found inside the internal memory in *com.whatsapp* folder which contains files like msgstore.db, wa.db and many more.

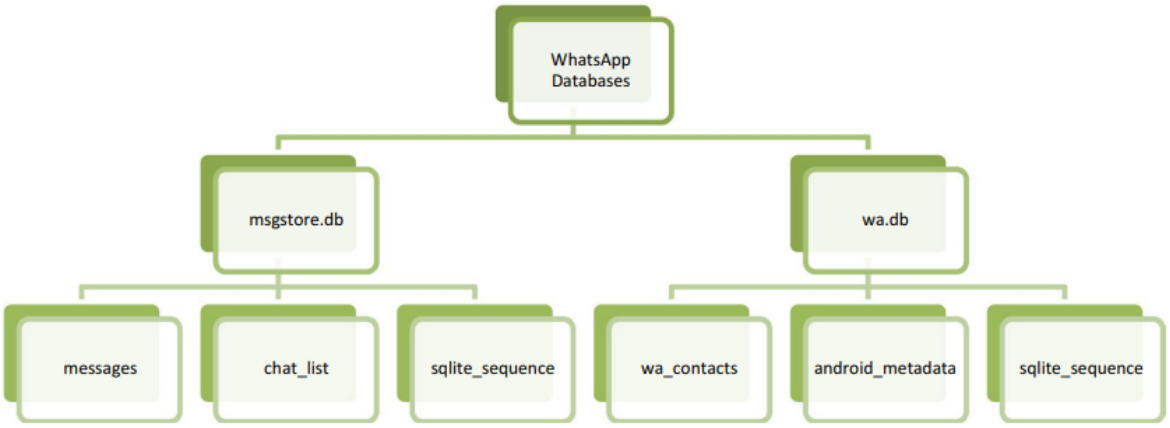


Fig.1 Internal Structure of WhatsApp[6]

Fig.1 illustrates the WhatsApp structure present inside the internal memory of the mobile devices. This is mainly divided into two parts: msgstore.db and wa.db. Msgstore.db contains the message exchanged between sender and receiver. It is also known as a chat database since it contains messages in different formats, especially text and multimedia [6]. It contains three tables namely messages, chat_list and SQLite sequence.

Messages: It contains the detailed information of the messages exchanged between communicating parties. Every message and its content are stored as record here [8]. It contains the different messaging attributes.

Chat_List: It stores the record regarding conversations where messages are classified based on the contact involved.

Second is Wa.db which contains the contact database. Analyzing the contact list is considered to be a very crucial step in any investigation. It contains different tables like wa_contacts, android metadata, SQLite sequence.

Wa_contacts: The crucial information regarding the contacts is stored in this table. It is synced with the phonebook. It gets updated accordingly whenever a contact is added. It also reveals some important information about the contact like Blocked contact or if a contact is an active WhatsApp user or not.

Further sections will discuss this in detail by analyzing the type of information extracted from it.

5.2 Identifying tools based on the requirement

Now the next step is to identify and gather all the open-source tools based on the requirement and previous study, and which we are going to use and run experiments in the current study. Features of these tools are listed below in Table 1. Most of the tools listed are compatible with both Linux and Windows platforms.

Tools	Features	Open Source/Commercial
Andriller	Non- Destructive acquisition Powerful lock screen cracking	Open source

Avilla Forensics	ADB backup APK Downgrade WhatsApp Decryption Chat capture	Open source
WhatsApp Key Database Extractor	Extracting the WhatsApp database without rooting the device.	Open source
ADB Command Line	Android acquisition Used to backup the device	Open source
Whapa	Android WhatsApp database parser.	Open source
Whacipher	Allow decryption of WhatsApp database.	Open source
WhatsApp Viewer	Tool to display WhatsApp chats.	Open source
DB Browser for SQLite	High-quality tool to visualize WhatsApp database.	Open source
WhatsDump	Extract private keys from any Android device.	Open source

Table 1 Listing of tools

6. Experiment Setup and Analysis

This section details the device used for carrying out different experiments using different tools. It also discusses some prerequisites before performing any experiment. Table 2 highlights the mobile device used along with its specifications. This study is focused on Android devices of version 9 or higher.

Mobile Device	Specifications	WhatsApp Version
Samsung A9 Pro	Android version-9 RAM-4GB Storage-64GB	2.22.22.80

Table 2 Device Details

6.1 Prerequisites

- First you need to have a *USB cable* to connect your smartphone device to the forensic workstation which may vary according to the researcher.
- Second step is to enter the Developer mode. To do this you need to *Open your settings>>>System Settings>>>Tap 7 times on Build option*. You will enter into developer mode now.
- After entering into *Developer mode*, you need to enable *USB Debugging*. USB debugging is done to run commands on your device using your workstation (Laptop/Desktop) without rooting the mobile devices. You need to have your mobile device unlocked at any point of time to run this effectively.

6.2 Set of Experiments using Tools

Andriller-CE

Andriller is a very popular open-source forensic tool when it comes to smartphones. It performs read only non-destructive acquisition from Android devices. Although it offers a variety of features, here in this research it is used to take backup of the smartphone device in order to prevent any destruction or loss of data. It is always recommended to take backups prior to any kind of experiment. To use this tool, you need to visit this page: https://github.com/den4uk/andriller >>> Git clone the code file into your Kali Linux terminal. After running the tool, the next step is to connect the smartphone device using USB and complete the backup process. Fig. 2 and 3 represent the backup acquired of the device in (.ab) format.

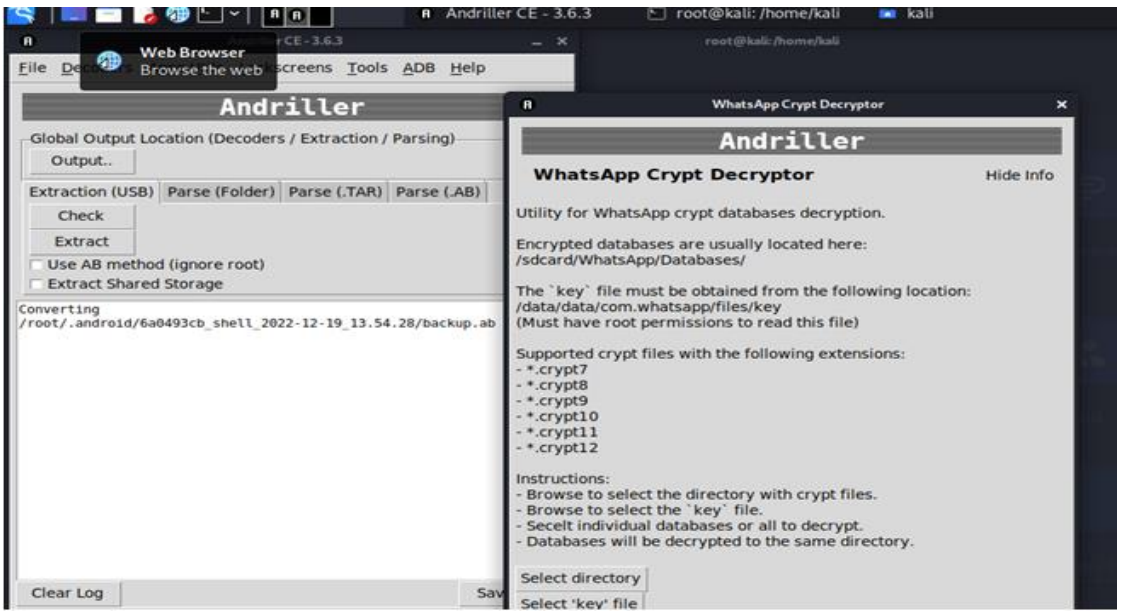


Fig. 2 Backup Operation

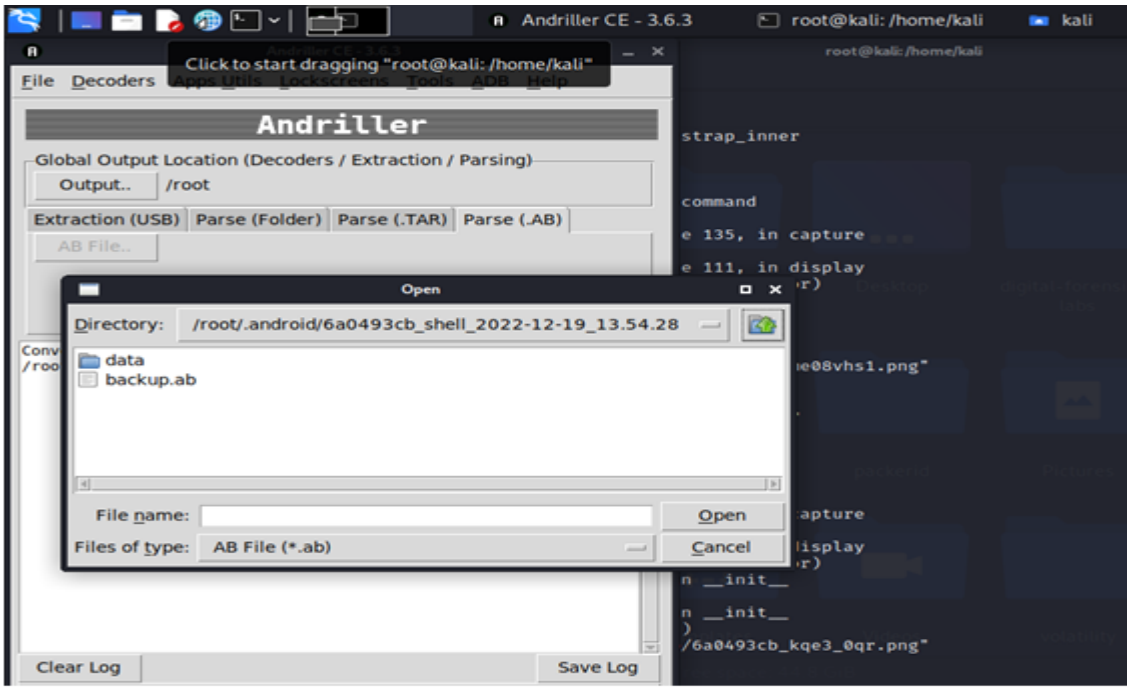


Fig. 3 Backup of the Device

ADB command line method used to be very popular for taking backup of the complete device but it's not working on the latest Android devices, that's why Andriller is preferred here. After performing the backups, the next step is to run the experiments and extract the cipher key which can be used to decrypt WhatsApp databases without rooting the device.

WhatsApp Key Database Extractor (WA-KDBE)

It is the most advanced and complete solution for extracting WhatsApp Key/DB from the package directory (*com.whatsapp*) without rooting the device. It can be installed on any platform, but usually, Kali Linux is recommended for its smooth functionality. Before running any script it's always better to take a backup of your chats and messages and store it somewhere safe. After running a few Python scripts, it can extract the cipher key present inside internal memory. Fig. 4 shows the complete key extraction process.

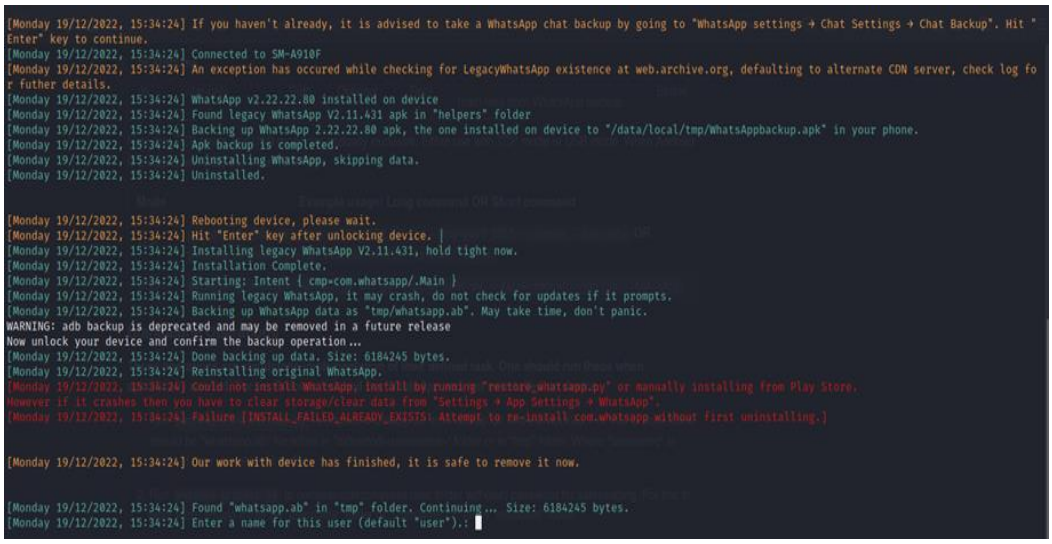


Fig.4 Extraction of the key

First it takes the backup of your installed WhatsApp and saves it in your internal storage. After the backup process is completed, it installs its legacy WhatsApp version to extract the *whatsapp.ab* folder to extract the cipher *key*. This process is known as Downgrading of Application. Finally, after the extraction, it again installs the original WhatsApp version on the device. You can find the extracted folder in Fig. 5.

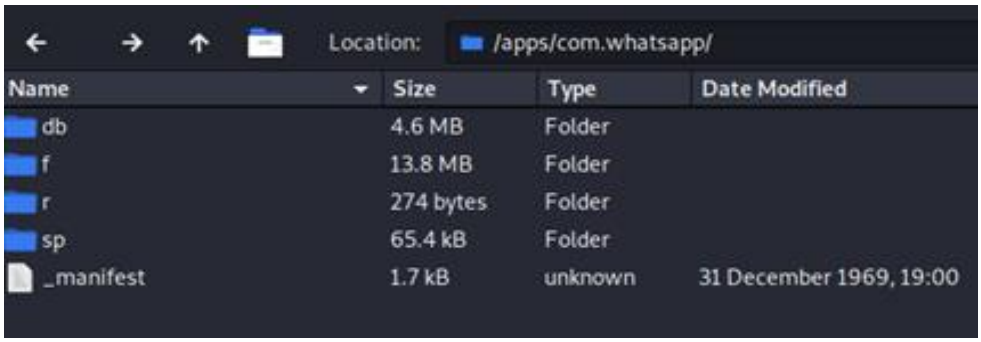


Fig.5 Extracted folder from the Device

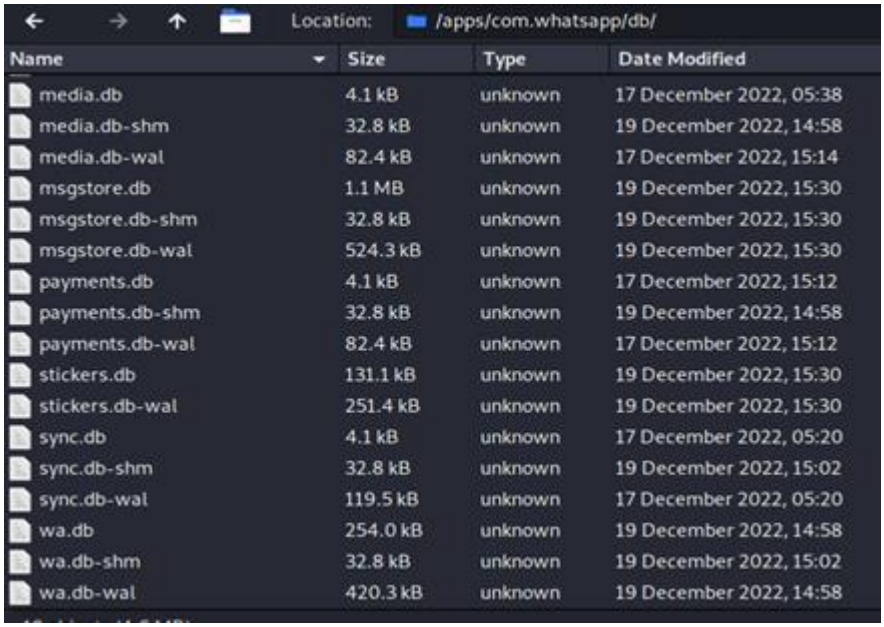


Fig.6 Extracted Database Folder

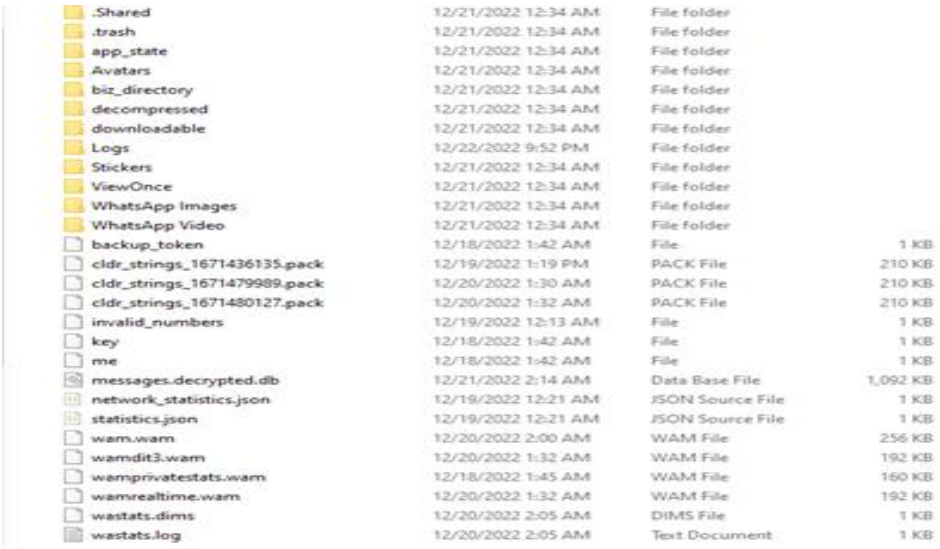


Fig.7 Extracted Key file

Here you can see the extracted database and key file which can be used to decrypt the encrypted WhatsApp database. This study aims to decrypt the latest encrypted database version: *crypt14/crypt15* which will be covered in the next sections. However (.db file) can be directly visualized using DB Browser for SQLite tool.

Avilla Forensics: Avilla forensic is an open-source forensic tool that can be used to extract data from android. It is one of the latest tools in mobile forensic which is still unexplored by the digital forensic community. It offers a lot of functionality like Backup ADB, APK Downgrade, Decrypting WhatsApp database crypt 14/15, merge WhatsApp database etc., but it is primarily used for decrypting crypt 14/15 WhatsApp databases and parsing WhatsApp chats in this study. To install this on your windows machine you need to visit this page https://github.com/AvillaDaniel/AvillaForensics.

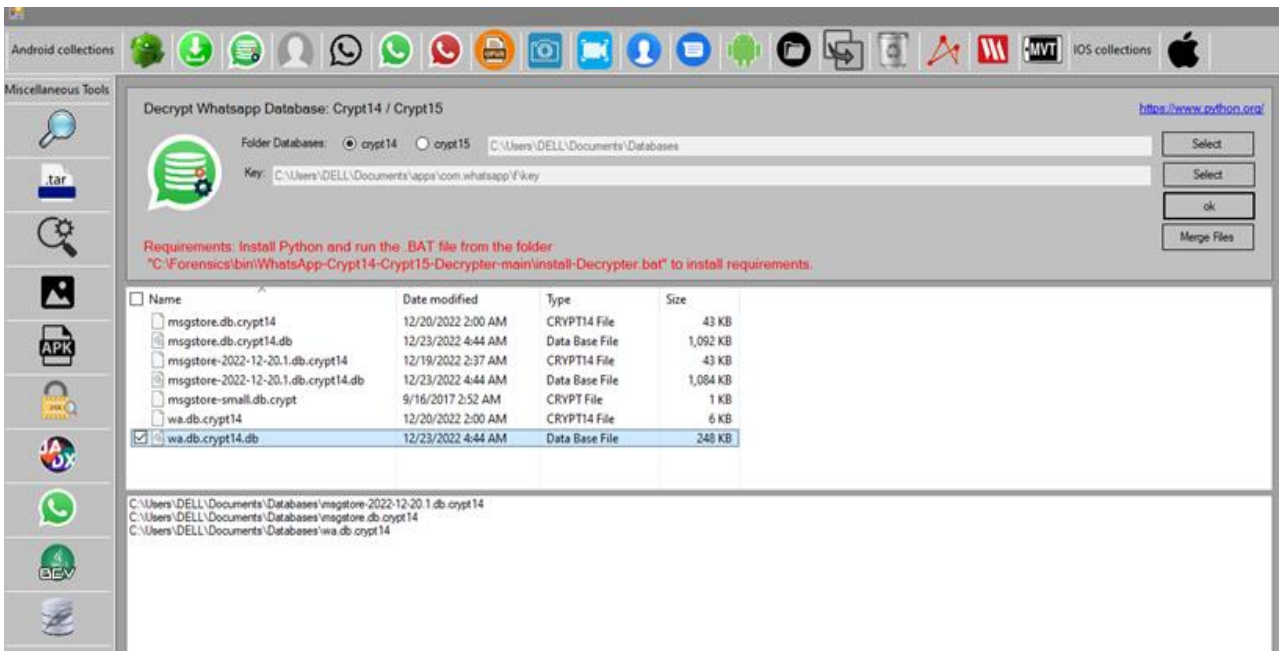


Fig.8 Decryption of WhatsApp Database

Above figure illustrates the decryption of WhatsApp database using the extracted key file. Here it is visible that *msgstore.db.crypt 14* changed to *msgstore.db.crypt 14.db* after decryption. It can now be visualized and analyzed using different tools.

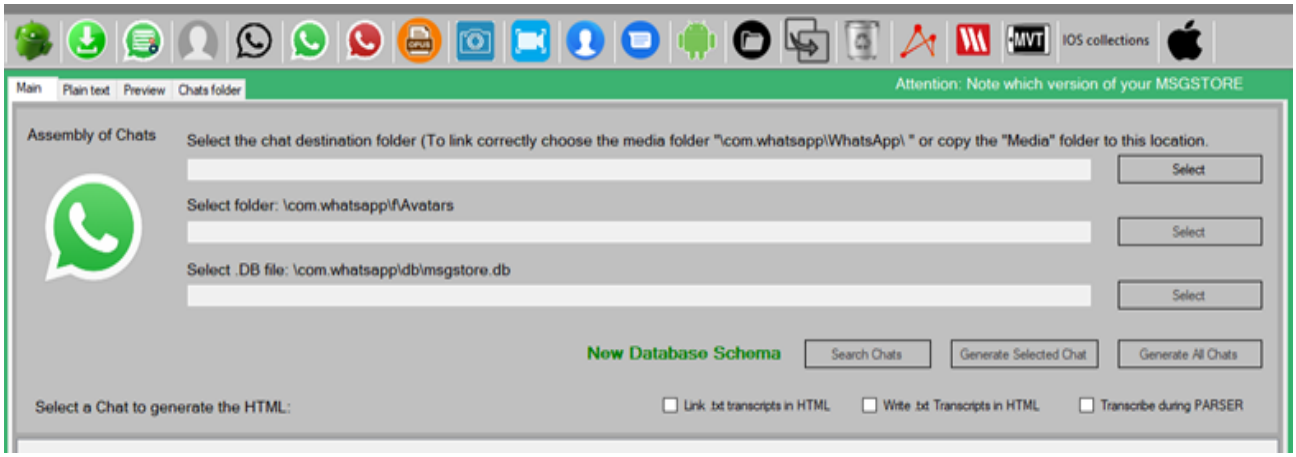


Fig.9 WhatsApp Chat Parser

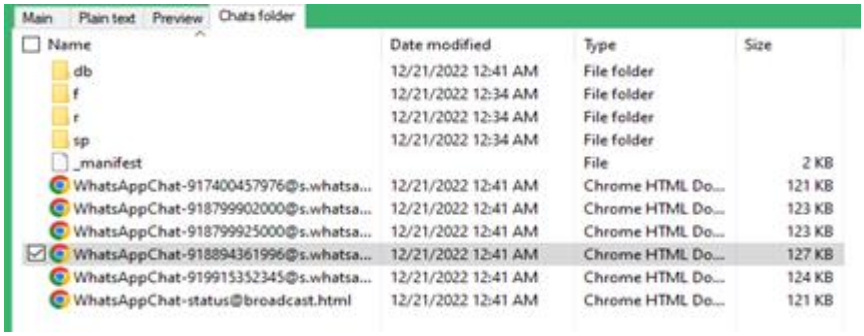


Fig.10 Parsed Chat Folder

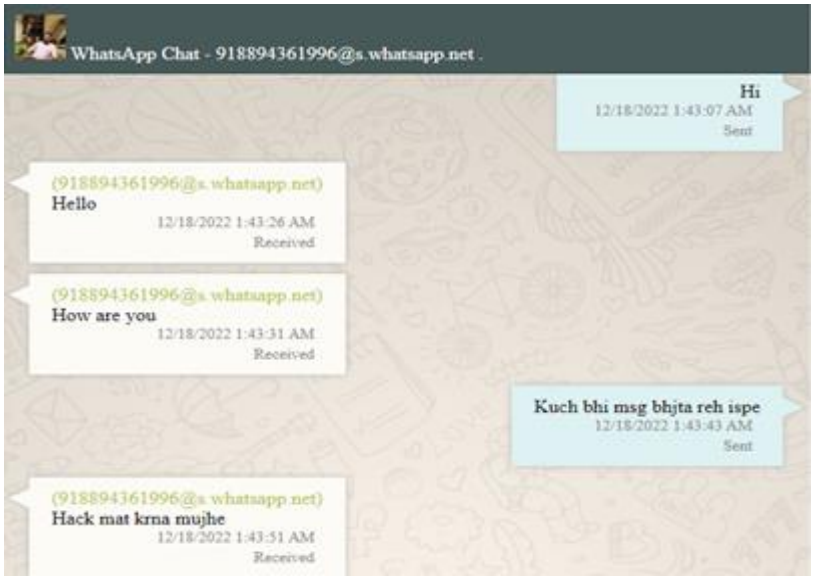


Fig.11 Extracted Chat

Another utility of Avilla Forensics is Parsing of WhatsApp chats. Fig.10 shows the chats stored in chrome HTML format. Fig.11 shows the extracted chats in the same WhatsApp format. Apart from this, Avilla Forensics has integrated all the tools which were being used independently like WhatsApp Viewer, DB Browser etc. This makes it a perfect and unique tool for the forensic investigators.

Whapa Toolset: Whapa toolset is a set of graphical forensics tools to analyze WhatsApp from Android devices. It works only on the Linux platform. It is one of the latest tools which are yet to be explored by the forensic investigators. It provides a GUI version which makes it very easy to operate. It is divided into 5 tools but only few are in the working stage at present. One of the tools is Whapa which is a WhatsApp chat parser which only works with older databases. It is used to get an active chat list on WhatsApp. Fig. 12 shows the active chat list extracted from *msgstore.db* database. Another tool is Whacipher which is used for decrypting the encrypted WhatsApp databases using key files; however, it does not support crypt15 databases.

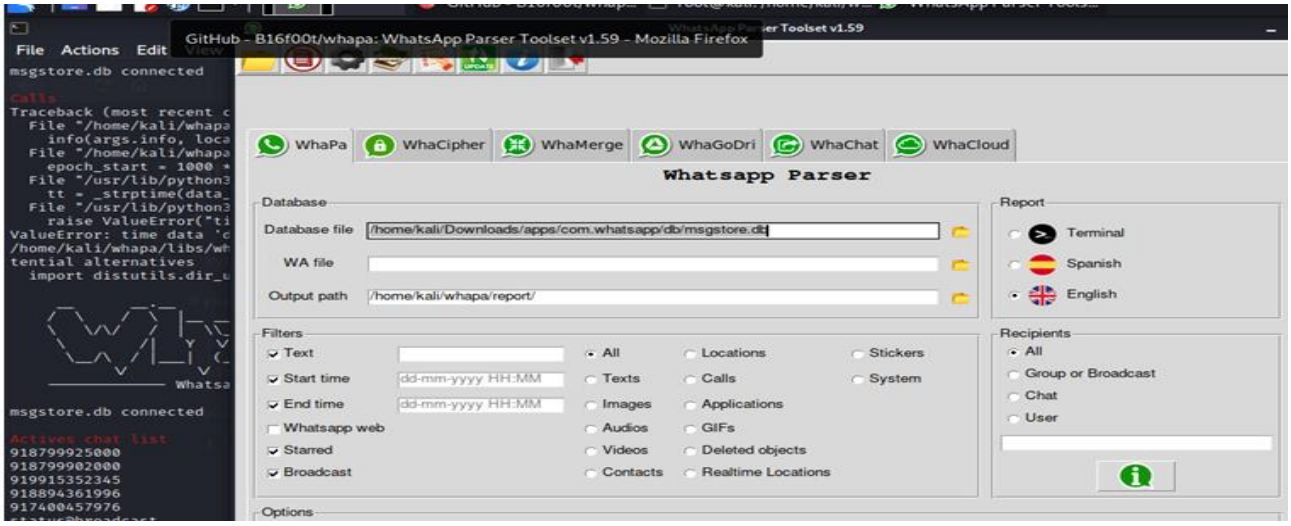


Fig.12 Active Chat List of WhatsApp

DB Browser: DB Browser for SQLite is a high-quality open-source tool to view and edit databases compatible with SQLite format. It can be used to visualize the WhatsApp chat in a very detailed format, as it provides a lot of fields which can play a very crucial role in an investigation. This tool can be used for any deep dive investigations. For using this tool, the database needs to be in decrypted form i.e. (.db extension). There is a lot of information that can be gathered from the *msgstore.db* and *wa.db* tables like key id of sender, status of the message, timestamp, geolocation, text data etc. which can be evident from Fig. 13 and 14. For more detailed information of each field of this table, research work of Hasan Fayyad et.al [7] can be referred to.

_me	key_id	sender_jid_row_id	sender_jid_raw_string	status	broadcast
	Filter	Filter	Filter	Filter	Filter
0	-1	NULL	NULL	NULL	NULL
1	BCF30DE7C21AAE2C4E1CB06BBD0A5B26	0	NULL	6	0
1	7CAFC83FA17E67B9CE73BA2CA974B1FD	0	NULL	6	0
1	76A1D85AB371B4CD89E0F9E51F95826B	0	NULL	6	0
0	6C744876D8D326DD75	0	NULL	0	0
1	0028A4C0B5304549545F9E157964FF59	0	NULL	6	0
1	E231629DFAE07A1A92F7CA2F28B9DBA2	0	NULL	13	0
1	992CE9F7E25071984E86ED435D1CFC6D	0	NULL	13	0
0	38A210EF528E4AD72758407C04B3D09D	0	NULL	0	0
0	A06E4C2808D0202A88B6D213216F57D6	0	NULL	0	0
1	BC889A73729E2C4AC4461863B8D80DA7	0	NULL	13	0

Fig.13 msgstore.db table

timestamp	received_timestamp	receipt_server_timestamp	message_type	text_data
Filter	Filter	Filter	Filter	Filter
1671307974530	0	1671307975000	0	Hii
1671307987728	0	1671307988000	0	Hi
1671308006000	1671308007149	-1	0	Hello
1671308011000	1671308011958	-1	0	How are you

Fig.14 available_msg_view_table

6.3 Comparative Analysis of Tools

Tools	Strength	Weakness	Platforms
Andriller	Used to complete backup to prevent data loss in the investigation.	Cannot be used to decrypt crypt 14/15. Not able to parse WhatsApp database.	Windows, Linux
WhatsApp Key Database Extractor	Extraction of the key is very easy with this tool. It also reinstalls your original WhatsApp after performing the operation.	Not able to downgrade WhatsApp on some devices. Data may be lost if you don't back it up.	Windows, Linux
Avilla Forensics	Able to decrypt crypt 14/15 database. Able to visualize chats.	Not able to downgrade the app to the Android 12 version.	Windows
Whapa and Whacipher	Used to extract active chat lists only. Can be used to decrypt	Not able to produce chats. Not able to decrypt	Linux

	crypt 14 databases.	crypt 15 databases.	
ADB Command Line	Android Acquisition. Used to back up the device.	Does Not support the latest Android versions.	Windows, Linux
WhatsApp Viewer	Able to decrypt the crypt14 database	Not able to visualize chats stored in the database	Windows

Table 3. Comparison of Tools

Table 3 illustrates the comparative analysis of different open-source tools which were used to extract some valuable information from WhatsApp. This table presents the pros and cons along with the platform operability of these tools. It is clearly shown in this table that a few tools like WhatsApp Viewer, ADB and Andriller have become obsolete and can no longer produce the expected outcomes as they lack the important features of WhatsApp forensic investigation. Whapa and Whacipher are still in their beta stages. Avilla Forensics is currently proven to be one of the best tools for WhatsApp forensics which can decrypt both crypt 14/15 databases and visualize messages. The below section represents the proposed framework based on this comparison table which can assist in any investigation effectively.

7. Proposed Framework

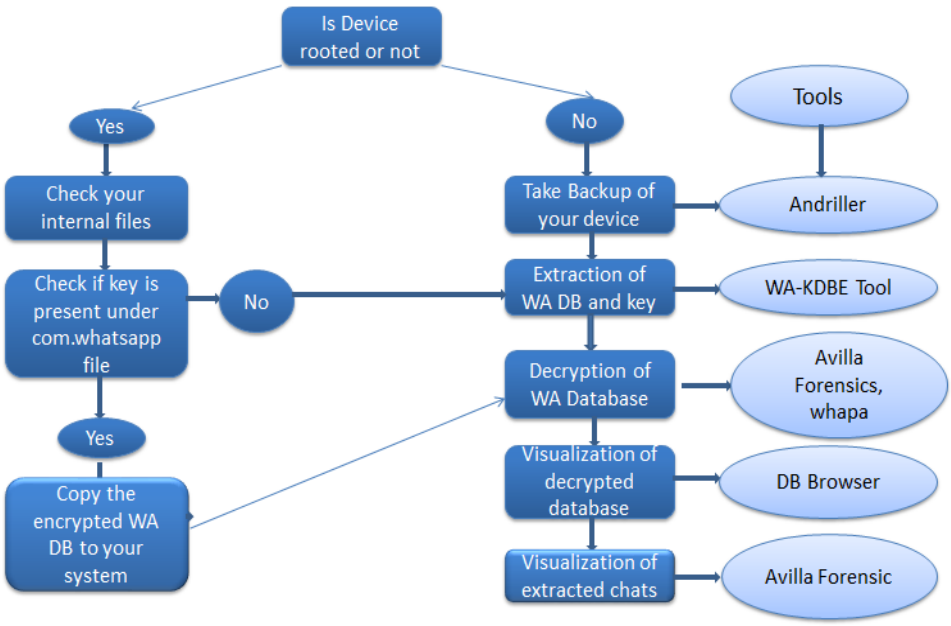


Fig.15 Proposed Framework

Fig.15 shows the framework proposed after doing a thorough and comparative analysis of different tools, which can be proved as the optimal way of doing WhatsApp investigation by law enforcement or any forensic investigators. It shows the step-by-step process of the WhatsApp forensic from extraction till visualization without rooting the device. It also specifies the tools used at each stage. This proposed framework is very efficient in terms of cost and time for unrooted devices as it provides the complete roadmap of encrypted WhatsApp forensics on latest devices. Avilla Forensics and Whapa are the two latest open-source tools that have not been previously used or explored by the forensics community. Both the tools have potential for uncovering the critical information for WhatsApp forensics if used properly.

8. Results and Conclusion

This research analyzed and compared the both latest and traditional WhatsApp forensics tools. The main reason behind this research is to provide a cost-effective way for forensic investigation using open-source tools as most of the forensic investigations currently are heavily dependent on commercial tools like MOBILedit, Belkasoft, Oxygen Forensics etc. Also, it has been observed in the previous studies that a similar set of open-source tools are being used repeatedly regardless of their incapabilities in extracting information. This research has revealed two new open-source tools namely Avilla Forensics and Whapa Toolset which are very efficient in investigations and very handy to operate. They offer a lot of functionalities which are very unique and have not been offered by any other tools previously. Moreover, a comparative analysis of tools has been proposed after performing the experiments using them. It gives an overall idea of the working of all the tools. Secondly a framework was also proposed on the basis of this comparative study to facilitate the investigation using the best tools. This framework is designed in such a way which will speed up the investigation process. In future more rigorous study can be done on the latest device or different operating system. Equivalence of commercial tools with open-source tools also need to be established.

References

[1] Shadeed, M., & Abu Arram, A. (2022). Forensic Analysis of "WhatsApp" Artifacts in Android without Root. *Advances in Science, Technology and Engineering Systems Journal*, *7*(2), 6. https://www.researchgate.net/publication/360055119_Forensic_Analysis_of_WhatsApp_Artifacts_in_Android_without_Root.

[2] Moreb, M. (2022). Mobile Forensic Investigation for WhatsApp. In *Practical Forensic Analysis of Artifacts on IOS and Android Devices: Investigating Complex Mobile Devices* (p. 48). Apress. https://link.springer.com/chapter/10.1007/978-1-4842-8026-3_9

[3] Wijnberg, D., & Khac, N. A. L. (2021). Identifying interception possibilities for WhatsApp communication. *Forensic Science International: Digital Investigation*, *38*(17), 8. https://doi.org/10.1016/j.fsidi.2021.301132.

[4] Fukami, A., & Stoykova, R. (2021). A new model for forensic data extraction from encrypted mobile devices. *Forensic Science International: Digital Investigation*, *38*(05), 10. https://doi.org/10.1016/j.fsidi.2021.301169

[5] Koppolu, N. R. (2021, June). A Deep-dive Analysis on WhatsApp Artifacts and their Relevance in Crime Investigation. *International Research Journal of Engineering and Technology*, *08*(06), 22. https://www.irjet.net/archives/V8/i6/IRJET-V8I6555.pdf.

[6] Alissa, K., & Almubairik, N. A. (2019, October). A comparative study of WhatsApp forensics tools. *SN Applied Sciences*, *1*, 10. https://doi.org/10.1007/s42452-019-1312-8

[7] Fayyad, H., & Kassem, S. (2022, June). Forensic Analysis of WhatsApp SQLite Databases on the Unrooted Android Phones. *HighTech and Innovation Journal*, *03*(02), 21. https://doi.org/10.28991/HIJ-2022-03-02-06

[8] Yuliani, V. a., & Riadi, I. (2019, September). Forensic Analysis WhatsApp Mobile Application on Android-Based Smartphones Using National Institute of Standard and Technology (NIST) Framework. *International Journal of Cyber-Security and Digital Forensics*, *08*(03), 9. http://dx.doi.org/10.17781/P002615.

[9] Sern, O. W., & Rahman, N. A. (2020, November). A forensic analysis visualization tool for mobile instant messaging apps. *International Journal on Information and Communication Technology (IJoICT)*, *6*(2). http://dx.doi.org/10.21108/IJOICT.2020.00.530.

[10] Umar, R., & Riadi, I. (2018, June). Mobile Forensic Tools Evaluation for Digital Crime Investigation. *International Journal on Advanced Science Engineering and Information Technology*, *08*(03), 7. http://dx.doi.org/10.18517/ijaseit.8.3.3591.

[11] Shidek, H., & Cahyani, N. (2020, June). WhatsApp Chat Visualizer: A Visualization of WhatsApp Messenger's Artifact Using the Timeline Method. i*nternational Journal on Information and Communication Technology (IJoICT*, *6*(1), 9. http://dx.doi.org/10.21108/IJOICT.2020.61.489.

[12] Irfandhia, M. D., & Satrya, G. B. (2022, November). Forensic Investigation Analysis of WhatsApp Messenger and Telegram Messenger on Android Based Device. *IEEE*, 6. https://doi.org/10.1109/ICoSEIT55604.2022.10030029.

ABOUT THE AUTHORS:

Tusharanshu Deo

Tusharanshudeo.mtcseis@pec.edu.in

https://www.linkedin.com/in/tusharanshu-deo-93316a171/

Expertise:

He is well versed in Cyber Security concepts and forensics overview and have completed some projects under Cyber Security domain during his degree.

Credentials:

Tusharanshu has completed his Bachelor's degree in 2020 in Cyber Security and Forensics. He is currently pursuing Masters in Computer Science and Information Security from Punjab Engineering College, Chandigarh.

Dr. Manvjeet Kaur

Manvjeet@pec.edu.in

Expertise:

Manvjeet's research interests include the areas of Medical Image processing, Biometrics and Biometric Security.

Credentials:

Dr. Manvjeet is currently working as an Assistant Professor in Cyber Security Research Centre, Punjab Engineering College, Chandigarh with an experience of more than 15 years.

Ms. Pooja Kaplesh

poojakaplesh.phd22csrc@pec.edu.in

Expertise:

Pooja's research area is information security, she has a good understanding in information security and has completed multiple research work in security.

Credentials:

Pooja has received M. Tech degree from Lovely Professional University Punjab. She is currently pursuing PhD from PEC.

eSec Forte®

Capacity Building In

Digital Forensics

First Responder (Onsite/CFL) – 05 Days

- Cardinal Rules of Digital Forensics
- Process, Tools & Techniques
- Volatile Memory Forensics
- Network Traffic Analysis
- Imaging Live Systems
- Documentation Preparation / Validation
- Seizure Procedure
- Packing and Transportation
- Preservation of Digital Assets

DF Assistant (CFL) - 05 Days

- Imaging of Digital Assets
- Cloning of Digital Assets
- Hash Verification
- Preservation of Digital Assets
- Maintenance of CFL
- Record Keeping

Expert Witness – 02 Days

- IT Act
- IEA (Relevant part)
- Moot Court
- 79A (Examiner of Electronic Evidence)

DF Examiner / Analyst – 10 Days

- Understanding Hard Disks and File Systems
- File Systems Analysis using FTK imager and open-source tools
- Volatile Memory Forensics
- OS Forensics
- Mobile Forensics
- Email Forensics
- Social Media Forensics
- Anti-forensics

Technical / Quality Manager – 03 days

- Report Writing
- IT Act
- CFTT (NIST)
- ISO/IEC 27037
- ISO/IEC 27041
- ISO/IEC 27042
- ISO/IEC 27043

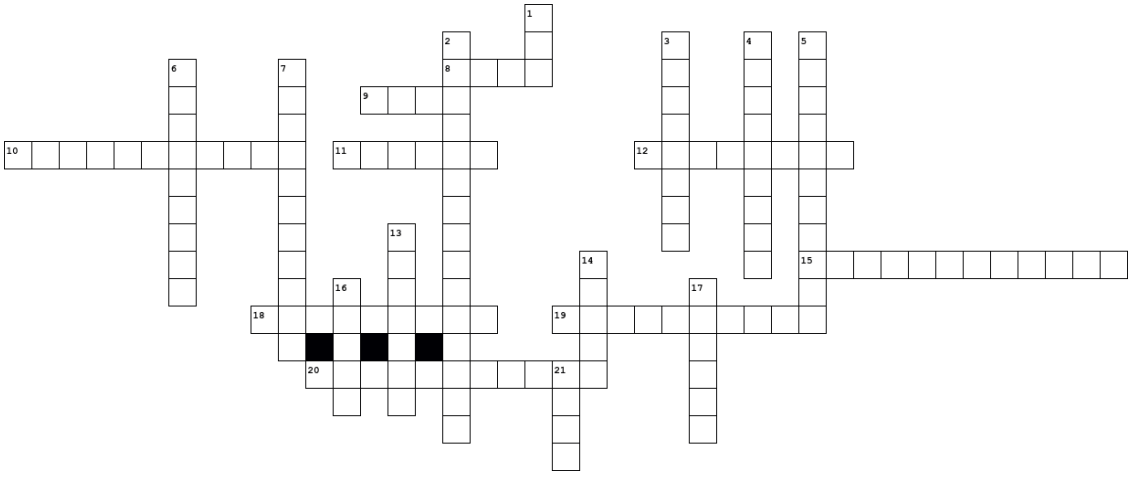
GURUGRAM | DELHI | MUMBAI | BANGALORE | SINGAPORE | SRI LANKA | DUBAI

Tel: +91 124 4264666 **Mail:** contact@esecforte.com **Web:** www.esecforte.com

Volume 8 | Issue 3 | August 2023

FORENSIC CROSSWORD

-Yugal Pathak



Across

8. The metadata standard used for digital images.

9. The metadata standard used for digital images

10. The first tool to focus on analyzing and recovering data from Linux file systems

11. A log file in Android that records system messages, debugging information, and application logs, which are vital in Android Forensics analysis

12. A folder in Windows contains information about recently executed programs.

15. A technique used to recover deleted files in Linux

18. A hardware device used to physically remove data from a hard drive

19. A feature in Ext4 systems that help maintain file system integrity and aid in Linux Forensics investigations.

20. The process of automatically transforming raw binary code into a more readable and understandable format.

Down

1. A device used to monitor and control industrial processes

2. The father of Computer Forensics started "Magnet Media Program".

3. A file that stores a snapshot of the computer's memory when it enters hibernation mode.

4. File encryption algorithm used by a built-in file encryption feature called FileVault in Apple devices.

5. The process of carefully removing the memory chip from a device without causing damage.

6. A tool used to extract data from Windows hibernation files.

7. A tool used for analyzing and recovering data from damaged or corrupted backup files

13. A type of attack that uses email attachments to deliver malware

14. A pioneering digital forensic tool developed by Fred Cohen

16. The first organization dedicated to advancing the field of digital forensics

17. Metadata about files, such as file creation and modification dates. obtained in Mac forensics.

21. An encryption standard commonly used for securing data on Linux systems poses a challenge in forensic analysis.

DRONA SERIES By eSec Forte

eSec Forte®

FORENSIC WORKSTATION SERIES

Developed to handle complex digital forensics processing and analysis and designed to ensure ease in operability.

PRODUCT DATASHEET

- **Biometric Access**
- **Persistent Memory**
- **Intel Dual Xeon Motherboard / AMD Dual EPYC compatible chipset**
- **1080p FHD Webcam with Autofocus**
- **27" LED FHD with Built-in Speakers mounted on Chassis**
- **20-Bay Proprietary Extended Frontal Cabinet with F-Mount**

Product Origin India

Technical Specifications

Model	EF-BEWS (BASIC)	EF-MEWS (MEDIUM)	EF-HEWS (HIGH END)
Series	Drona Series - I	Drona Series - P	Drona - X
Power Supply	Upto 1000W Modular	Upto 1600 Watts Fully Modular PSU	Upto 2200 Watts RPS
Cabinet	12-Bay Proprietary Cabinet	16-Bay Proprietary Extended Frontal Cabinet with F-Mount	20-Bay Proprietary Extended Frontal Cabinet with F-Mount
Chipset	Intel Z690 / AMD TRX40	Intel Xeon W or Dual Scalable Silver Series / AMD WRX80	Intel Dual Xeon Motherboard / AMD Dual EPYC compatible chipset
Processor	Intel Core i9 series / AMD Thread Ripper 3970 series	Intel Xeon W-3300 / AMD Thread Ripper 3990 series	Intel Xeon Scalable Gold or Platinum Series / AMD EPYC 7003 Series
No. of cores	Upto 16cores / Upto 32 cores	Upto 38 cores / Upto 64 cores	Upto 40cores / Upto 64 cores
RAM	Upto 256GB Non-ECC RAM	Upto 512 GB ECC RAM	Upto 4TB ECC RAM
OS Drive	500GB SATA SSD	1TB SATA SSD Plus / Pro Series	960GB Enterprise SATA SSD
Cache Drive	500GB NVMe M.2 SSD	1TB NVMe M.2 SSD Plus / Pro Series	960GB Enterprise NVMe M.2 SSD
Processing Drive	---	2TB NVMe NVMe M.2 SSD Plus / Pro Series	2 x 1.92TB Enterprise M.2 / U.2 SSD in RAID 0
Data Drive	4TB SATA HDD	12TB SATA Enterprise HDD in RAID 5 (4 x 4TB)	24TB SASIII/SATAIII Enterprise HDD in RAID 5 (4 x 8 TB)
Graphics Memory	6GB GDDR6	8GB GDDR6	14GB GDDR6
Standard HDD Bays	4 x 3.5" Removable 6Gbps HDD Hot-Swap Bays (compatible for SAS and SATA drives)		
	1 x 3.5" Removable IDE HDD Bay (optional)		
	1 x 3.5" Removable 68-pin SCSI HDD Bay (optional)		

Technical Specification

Model	EF-BEWS (BASIC)	EF-MEWS (MEDIUM)	EF-HEWS (HIGH END)
Series	**Drona Series - I**	**Drona Series - P**	**Drona - X**
Enterprise 12Gbps HD Mini-SAS Bays (Forensic)	---	4 x 3.5" Removable 12Gbps HD Mini-SAS HDD Hot-Swap Bays (Write Protected)	
	---	4 x 3.5" Removable 12Gbps HD Mini-SAS HDD Hot-Swap Bays (Read / Write)	
Forensic Card Reader	Supports read-only access to CF/UDMA, SDHC / SDXC, MicroSD, MS / DUO		
Forensic Bridge	5.25" Integrated Forensic Bridge with SAS/SATA/Firewire/USB/PCIe interfaces		
Ventilation Tray	Integrated Retractable Ventilation Tray with non-skid surface with dual performance fans along with auto on/off feature		
RAID Controller	---	8-port RAID Controller with 1GB Cache	8-port RAID Controller with 2GB Cache compatible with CacheVault supporting super capacitors
DVD Writer	Standard DVD Writer	Blue-Ray DVD Writer	Blue-Ray DVD Writer
Integrated System Security	---	Biometric System Power On	Biometric System Power On
Chassis KeyLock	Yes	Yes	Yes
Integrated System Performance Monitor	---	3.5" LCD For Performance Monitoring, System Info & Admin Control	3.5" LCD For Performance Monitoring, System Info & Admin Control
Integrated Biometric OS Login	---	---	Yes
Ports			
BackPanel USB (Rear)	4 x USB 3.2 Gen 1, 1 x USB 3.2 Gen (2 x2) / 3 x USB 3.2 Gen 2 / 4 x USB 3.2 Gen 2 & 6 x USB 3.2 Gen 1	6 x USB 3.2 Gen 2, 1 x 3.2 Gen 2 (2x2), 2 x 3.2 Gen 2, 4 x USB 2.0 / 6 x USB 3.2 Gen 1	6 x USB 3.2 Gen 1, 2 x USB 3.2 Gen 2 / 2 x USB 2.0, 4 x USB 3.0
Standard USB Bay (Lower Side Panel)	---	4-port USB 3.1 Gen 1 bay for charging phones	8-port USB 3.1 Gen 1 bay for charging phones
Rapid USB Bay (Lower Side Panel)	---	2-port USB 3.2 Gen 2 bay for rapid data transfer and charging (1 x Type A, 1 x Type C)	4-port USB 3.2 Gen 2 bay for rapid data transfer and charging (1 x Type A, 1 x Type C)
Bluetooth & Wifi	Dual- Band Wifi & Bluetooth 5.0		
Ethernet			
Gigabit NIC	Yes	Yes	---
10Gbps NIC	---	Yes	Yes
Fibre Channel NIC	---	---	Yes
Integrated Wireless Charging for mobile	---	Yes	Yes
System Integrated Webcam	---	720p HD Webcam	1080p FHD Webcam with Autofocus
System Cooling			
Air Cooling/Liquid Cooling	Compatible	Compatible	Compatible
Performance Cooling compatible	---	Compatible	
Standard System Peripherals	Membrane Keyboard & Mouse with backlit		Membrane Keyboard & Mouse with backlit embedded in Lapboard
Advanced System Peripherals	---	---	15-point Jog Shuttler embedded in lapboard (optional)
Audio	8-channel		
Remote Management	---	IPMI 2.0	
Adapter kits	PCIe Card SSD Adapter, PCIe M.2 SSD Adapter, PCIe Adapter for Apple SSD, PCIe U.2 SSD Adapter, Apple 2016+ PCIe SSD Adapter, 4" PCIe cable and Drive Adapter Kit		
Dimensions (W x H x D) in inches	30" x 28" x 12"	30" x 28" x 12"	30" x 28" x 12"

New Delhi
A-2/10, A-2 Block, Rohini Sector- 5, New Delhi – 110085

Gurugram
Plot No. 285, 2nd & 3rd Floor, Udyog Vihar, Phase- IV, Gurugram, 122015

Mumbai
Plot C-59, Bandra Kurla Complex, Bandra East, Mumbai – 400051

Bangalore
143, 3rd Floor, 10 th Cross, Indiranagar 1 st stage, Bangalore – 560038

Singapore
1 North Bridge Road, # 11-10, High Street Centre, Singapore - 179094

Sri Lanka
Level 26 & 34, East Tower, World Trade Center, Echelon Square, Colombo, 00100, Sri Lanka

Tel: +91 124 4264666 **Mail:** contact@esecforte.com **Web:** www.esecforte.com

Volume 8 | Issue 3 | August 2023 | INR 500

www.digital4n6journal.com

DIGITAL FORENSICS (4N6)

INDIA'S 1st DIGITAL FORENSICS PUBLICATION