International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 10 Issue: 12 | Dec 2023 www.irjet.net p-ISSN: 2395-0072

Emerging Trends In Cryptography And Digital Forensics

Mr. Sneh Shrimankar[1], Mr. John Bright Raj[2], Mrs. Abhilasha Maurya[3]

[1]Dept. of Information Technology ,SVKM'S Shri Bhagubhai Mafatlal Polytechnic, Maharashtra, India
[2]Dept. of Information Technology ,SVKM'S Shri Bhagubhai Mafatlal Polytechnic, Maharashtra, India
[3]Professor, [1]Dept. of Information Technology ,SVKM'S Shri Bhagubhai Mafatlal Polytechnic, Maharashtra, India

---

Abstract - *With the internet reaching a level that merges with our lives, growing explosively during the last several decades' data storage usage and data security which has become a main concern due to increase in risk of misuse of data. This paper gives the overall emerging trend and the devastating changes in these 2 crucial fields in the IT environment. The two crucial components of cybersecurity are the fields of digital forensics and cryptography together working & ensuring integrity, confidentiality of digital information. In today's world there are lot of digital forensics tools used to gather the evidence of the investigations done combined with the cryptography tools used to cipher the data gathered.*

Key Words: confidentiality, data security, cipher, investigations, data gathering.

1.INTRODUCTION

In the last few years, computers have avoidably become the emerging field record keepers of the human activity. The trend has been accelerated with the emergence of PC's, handheld devices, multimedia and telecommunications. In today's digitally developing world, it presents opportunities and challenges for criminals. The proof of crime in the courtroom can be presented as the events recorded as per the sequence, recording artifacts which comprises of collection, review and evaluation. Cryptography plays a significant role in digital forensics by presenting unique challenges and opportunities such as Encryption Techniques, Password Cracking, Anti-Forensics Techniques etc. Cryptography is very necessary everywhere in communicating over any untrusted transmission system. It's a very crucial sector in information system security, and now in these modern technologies days, cryptography is worked everywhere from browsing the web to phone chat calls. The needy for a better cryptosystem keeps increasing because the enhancement of the recent generation of computers improved the backdated cryptosystems.

2. LITERATURE SURVEY

This study presents a review of cryptography research and digital forensics , explores the functioning of diverse cryptographic algorithms designed for various security purposes. Cryptography's significance remains evident in its alignment with IT and business strategies, safeguarding sensitive data like personal, financial, medical, and e-commerce information, and preserving privacy at a significant level.

3. CRYPTOGRAPHY CONCEPT

Cryptography is a new tactic through which the confidentiality and circumspection of the messages can be achieved. In Greek cryptography has a special and specific meaning known as "Secret Writing". The basic notion of the cryptography system is to cipher the information in the form of the transmission of data through the internet (insecure channel) or to ensure that the unauthorized people do not understand the information accessed through any scenario or through any other unusual forms. In this concept, the enshrouded information is termed as "plaintext" and the disguising process of plaintext is called as "ciphertext". The process through which the information is concealed is achieved through various "encryption algorithms". There is a concept of "encryption key" on which the encryption process relies, which is given as an input to the encryption algorithms along with the information. On other side the "decryption key" is used to retrieve the information on the receiver side [1].

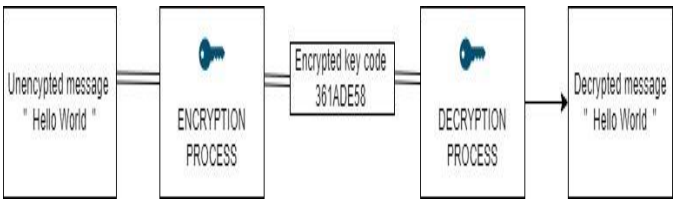

Fig-1: Cryptography Concept

3.1 Classification Of Cryptography

3.1.1 Symmetric Key Cryptography

It is also known as Secret Key or Conventional Cryptography. Symmetric Key Cryptography is an encryption system in which the sender and receiver share the common key which they use to encrypt the plaintext and decrypt the ciphertext information. The algorithm used is also known as secret key algorithm or sometimes called symmetric algorithm.

Examples :-

Lucifer - Madryga

FEAL – REDOC
LOKI – GOST

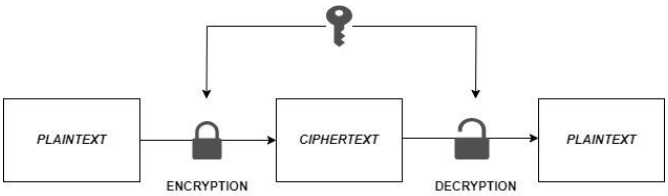

Fig-2: Symmetric Key Cryptography

3.1.2 Asymmetric Key Cryptography

Asymmetric Cryptography , also known as Public-Key cryptography , requires two separate keys indicating to a cryptographic algorithm , of which one is public and one is private. The encryption of the message is done using public key and decryption of the message is done using private key. Public key cryptography is a very advanced form of cryptography. Although the fundamental principles of public key cryptography were initially unearthed in 1973 by Clifford Cocks, a British researcher at the Communications-Electronics Security Group (CESG) within the Government Communications Headquarters (GCHQ), this breakthrough remained classified until 1997.[2]

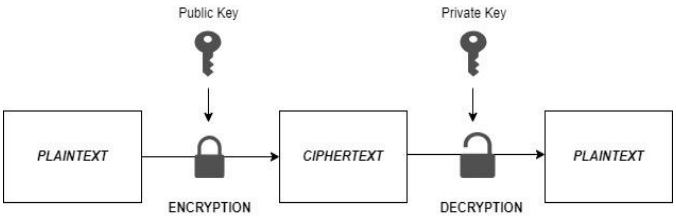

Fig-3: Asymmetric Key Cryptography

Examples :-

RSA Cryptanalysis
Digital Signature Standard (DSS)
ElGamal

3.2 Encryption And Decryption In Cryptography

When information is easily readable without requiring any specific actions, it is referred to as plaintext or cleartext. The practice of concealing the actual content of plaintext through various techniques is known as encryption. The outcome of encrypting plaintext is the creation of incomprehensible ciphertext, resembling jumbled text. Encryption serves the purpose of ensuring that data remains concealed from individuals who are not the intended recipients, even if they have access to the encrypted data. The procedure of converting ciphertext back to its initial plaintext form is termed decryption [3].

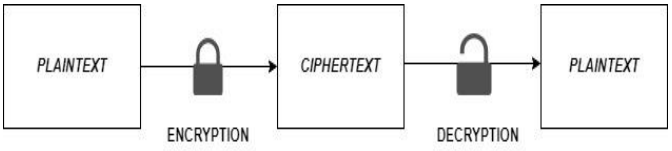

Fig-4: Encryption And Decryption

3.3 Suggested Methodology

As depicted in Figures 2 and 3, we have outlined the flowchart and operational process of our recently developed data encryption and decryption system. The process initiates with the encryption of plain text, yielding the formation of cipher text. Following this step, the resulting cipher text is securely transmitted to the recipient's endpoint, where our sophisticated data decryption system is utilized to decode and recover the original plain text, as cited in reference [4].

3.4 Hash Functions

In the realm of cryptography, a cryptographic hash function stands as a fundamental tool. It operates by accepting any arbitrary block of data and, in response, produces a bit string of fixed size known as the cryptographic hash value. Crucially, even the slightest alteration to the input data, whether inadvertent or deliberate, will almost certainly result in a significant change to the hash value. [2]. The compression technique employed here differs from that of .zip or .rar files; it's not an invertible mapping but rather a non-invertible one. In order to be valuable, a hash function must adhere to two essential properties[1]:

- The first property is that it must be one-way.
- The second property is that it must be collision resistant.

Suggesting that the unidirectional nature of a hash function's output is a significant attribute, alongside its ability to resist collisions, is essential. Collision resistance pertains to the challenge of finding another input that yields the same output, and there are two distinct forms in which this resistance can be introduced.

3.4.1 Preimage Collision Resistance

This form of hash function operates on an output Y, which is given by finding another input M in such a way that the hash of M is the same as Y, nontrivially.

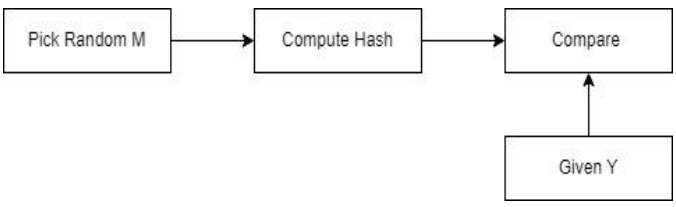

Fig-5: Preimage Collision Resistance

3.4.2 Second Preimage Collision Resistance

This the second form of hash function in which two messages are given (M1 and another, M2 that is chosen randomly) in which the match would be nontrivial [1].

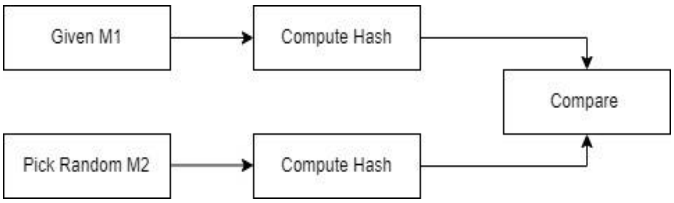

Fig-6: Second Preimage Collision Resistance

3.5 Generating Keys

To establish a robust and secure key for our system, we employ a random character generator. This generator produces characters with a minimum bit size of 208 bits, ensuring a strong foundation for our key. Following this, we select a minimum of four characters, each comprising 32 bits, through a random process. Once these characters are obtained, we arrange them into an array of characters .This meticulous approach guarantees the reliability and security of the key that underpins our desired system[4].

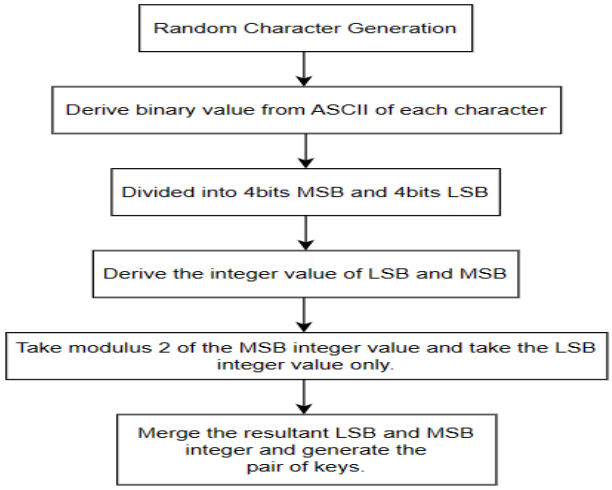

Fig-7: Flowchart of Proposed key generation technique

The whole process of key generation is given below.
Random Character = ADYX . . . . . n

Array of Character = [A, D, Y, X . . . . . n]

Input: S ← {Random string of n characters}
Output: *K[n]* ← {Array of the nth generated keys}
Generate random string S
for *i* ← 0 to *n-1* do
  Divide *S* into nth characters: *C[i]* ← *S[i]*
  Compute ASCII value for each character: A[i] ← *C[i]*
  for *j* ← 0 to 7 do
    Compute binary bits for *A[i]*
    Store binary bits to *B[i][j]*
  end for
  Divide the 4 bits LSB and MSB
  Compute *MSB_val* from *B[i][0..3]*
  Compute *LSB_val* from from *B[i][4..7]*
  MSB_val ← *MSB_val* % 2
  KEY ← Merge *MSB_val*, *LSB_val*
  K[i] ← *KEY*
end for

Fig-8: Proposed Algorithm for Key generation

First, each character is converted into its corresponding ASCII value, from which we derive binary representations. This binary transformation involves separating each binary number into two parts—specifically, the 4 least significant bits (LSB) and the 4 most significant bits (MSB). Subsequently, we calculate the integer values corresponding to these 4-bit LSBs and MSBs. This allows us to create an array for each character, pairing them with these two-digit integers. Now, for a crucial step in enhancing the security of our technique, we apply a modulus operation to the first digit of each pair, ensuring it is limited to either 0 or 1. This manipulation becomes instrumental in determining the character's position within a block during both data encryption and decryption processes. The pair of digits in our array forms the final key in our innovative approach. To clarify, the first digit signifies the character's position within the corresponding block of plaintext, while the second digit represents the number of bits that will undergo circular shifting—a crucial aspect of our encryption and decryption method[4].
Array of decimal value = [41, 44, 59, 58, ... n]

Key = [01, 04, 19, 18, ... n]

Table -1: Key Generation of Proposed Technique

A		D		X		Y	
65		68		89		88	
01000001		01000100		01011001		01011000	
0100	0001	0100	0100	0101	1001	0101	1000
4	1	4	4	5	9	5	8
4%2=0	1	4%2=0	4	5%2=1	9	5%2=1	8
01		04		19		18	

3.6 Working of PGP

PGP is a cryptographic system that combines the strengths of both traditional and public key encryption which makes it a hybrid approach.

When PGP is used to encrypt plaintext, process of compressing the text starts. This compression serves multiple purposes, such as conserving modem transmission time, reducing disk space usage, and most crucially, bolstering cryptographic security. The primary aim is to thwart cryptanalysis techniques that thrive on detecting patterns in plaintext. By compressing the text, PGP effectively diminishes these discernible patterns, thereby significantly enhancing resistance against cryptanalysis. [3].

Following the compression step, PGP generates a unique session key, which is a one-time-only secret code. The session key works in conjunction with a highly secure and rapid conventional encryption algorithm to transform the plaintext into ciphertext, ensuring confidentiality. Once the data is successfully encrypted, the session key undergoes another layer of encryption, this time using the recipient's public key. This public key-encrypted session key is then bundled with the ciphertext and sent to the intended recipient[3].

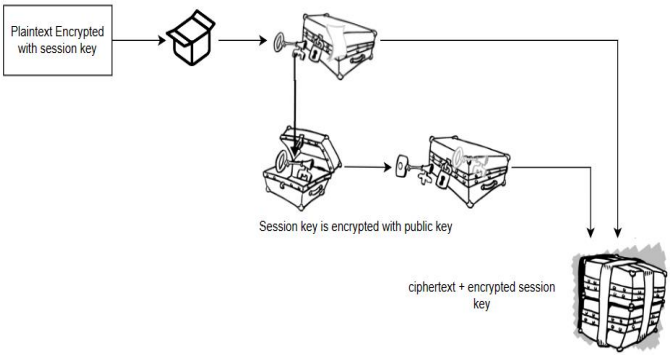

Fig-9: PGP Concept

3.7 Digital Signatures in Cryptography

Public key cryptography offers a significant advantage in its ability to implement digital signatures. These digital signatures play a crucial role in enabling recipients to authenticate the source of information and ensure that the data remained unaltered during transmission. Consequently, public key digital signatures deliver both authentication and data integrity. In essence, a digital signature fulfills the same function as a handwritten signature but with distinct advantages. While a handwritten signature can be relatively easy to forge, a digital signature holds the upper hand as it is exceptionally challenging to counterfeit.

Additionally, a digital signature not only vouches for the authenticity of the information but also verifies the identity of the signer. In practice, some individuals tend to rely more on digital signatures than encryption.

For instance, one might not be overly concerned about others knowing they deposited $1000 in their bank account, but they certainly want unequivocal confirmation that the transaction was indeed conducted with the authorized bank teller. The fundamental process of creating digital signatures is depicted in the accompanying figure. Instead of encrypting information using someone else's public key, the approach involves encrypting it with your private key. The assurance that the information can only be decrypted using your public key serves as irrefutable evidence of its origin, attributing it unequivocally to you[3].

Digital signatures are far more secure than handwritten ones, verifying both the content and the signer's identity. Some individuals prefer digital signatures over encryption for specific purposes, such as confirming bank transactions.

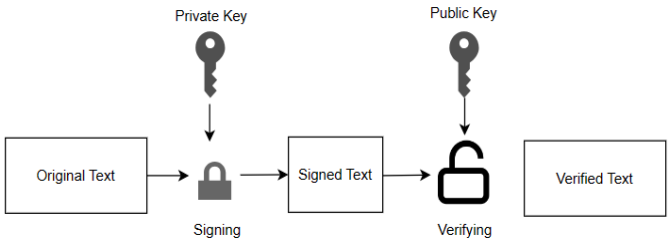

Fig-10: Digital Signature Process

4. DIGITAL FORENSICS CONCEPT

In investigations, digital forensics emerges as an indispensable facet where data is implicated following a security breach. The data in question could range from personal to business-related or highly sensitive information also. The root mission of digital forensics is to lawfully obtain and meticulously scrutinize the data under investigation [5]. The digital forensics domain spans across variety of disciplines with the guidelines needed in the acquisition, preservation, organization and also in examination of electronic data. Digital forensics is based on certain standards to qualify as admissible evidence in legal context of digital data. These admissible evidence include the data stored on electronic devices such as audio, video, and textual content, all of which are stored on electronic devices [6]. Within the realm of digital forensics, a cross-disciplinary science, protocols are established for collecting, storing, assembling, and evaluating electronic data. After collecting these data, to evaluate these in the judicial manner and information, we should have the proper standards decided that can be used and some proper case management tools that should be used by the investigators to manage the bits of every data and correlate with the evidence found in physical machines.

4.1 Digital Forensics Techniques

There are numerous types and ways used in anti-forensics; an ferocious check on the available tools were conducted to demonstrate the orders and subcategories, and the study told that there are many AFT available. AFT is divided into multiple orders according to the purpose of operation and type of attacks performed [5].

4.1.1 Artifact Wiping

When deleting a train or brochure from a storehouse device, the factual data remains on the storehouse device until it's overwritten by new data. The artifact wiping is considered an AF fashion designed to fully abolish and destroy data. Artifact wiping or secure wiping can be applied on lines, entire fragment, or partition. Available tools that serve the purpose are Eraser, External Examiner, Free Wipe Wizard, train Shredder, and Registry cleaner[5].

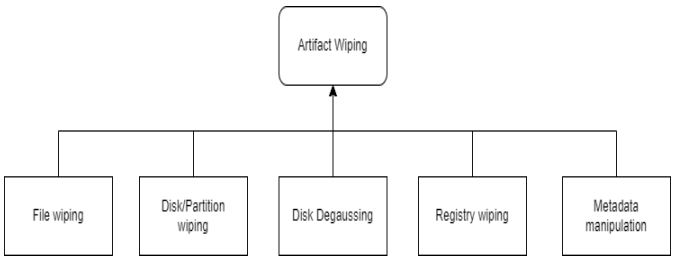

Fig-11: Artifact Wiping

File wiping - It is known as data shredding which is a process placed to obliterate all traces of information linked to a particular file.

Disk/Partition - It used to destroy the data there on all the sectors of a specified disk or partition.

Disk degaussing - It is a procedure involving the electronic storage device to a magnetic field to neutralize and completely eliminate any data previously stored on it.

Registry wiping - It looks like a central repository to store the settings and related data to both the operating systems and the installed applications.

Metadata manipulation - Operating systems and software tools typically generate metadata for each file that is created and saved on a storage device. This metadata essentially serves as "information about information."[5]

4.1.2 Data Hiding

It is used to target the data on storage, which makes the analysis and examination of digital evidence, by forensics examiners, difficult or impossible to conduct. The data hiding includes steganography, data contraception, file system manipulation, hard disk manipulation, and network-based data hiding [5].

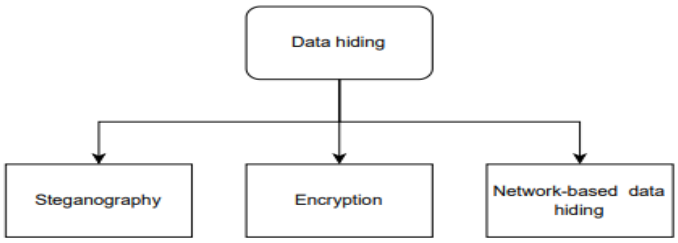

Fig-12: Data Hiding

Steganography - It is the concept of blocking out a hidden message within an ordinary message and not disclosing the fact that two parties are in communication with each other.

Encryption - Data encryption serves as a tool to safeguard stored information. It can be employed to protect individual files, databases, emails, or even entire disks, utilizing a range of encryption algorithms.

Network-based data hiding - Data encryption mirrors real-time encryption, safeguarding data as it moves between locations, rather than when it's stationary.

4.1.3 Trail Obfuscation

This method is commonly recognized as "counterfeiting." Hence, techniques like trail obfuscation or evidence counterfeiting are employed to confound and disorientate investigations. This can be accomplished through various means.It also refers to task of confusing the forensic process to hide the malicious behavior investigations. This can be accomplished through various means.It also refers to task of confusing the forensic process to hide the malicious behavior.

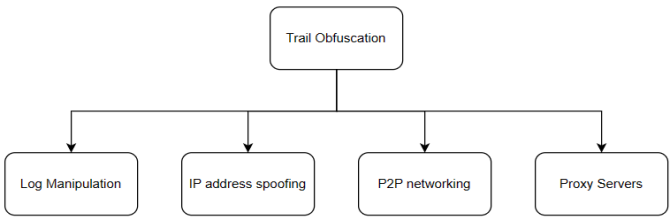

Fig-13: Trail Obfuscation

Log Manipulation:- Logs are stored on the compromised system as well as on external Syslog servers also.

IP address spoofing:- It is a common technic deployed by attackers in an attempt to either conceal their true identity or falsify the origin of the attack.

P2P networking:- It offers a decentralized data sharing approach, eliminating the need for a central host or server, and enabling rapid sharing of data among interconnected network nodes.

Proxy Servers:- Proxy servers are inherently designed to manage and limit access to predetermined URLs[5].

4.1.4 Attacks against forensic tools and processes

Forensic tools may come under attack as a means to deceive or distract investigators from accessing accurate information. Various methods and tools can be employed for this purpose, including those designed to reduce digital traces or render reverse engineering unfeasible. In more extreme cases, criminals may even attempt to undermine the credibility of the investigative teams. Program packers are employed to thwart forensic examiners from successfully implementing reverse engineering techniques on digital evidence, preventing them from gaining access to crucial information. Additionally, these packers serve as a means to evade detection during forensic examinations or scans of the digital environment. Criminals resort to these tactics to undermine the integrity of the investigative teams through malicious actions[5].

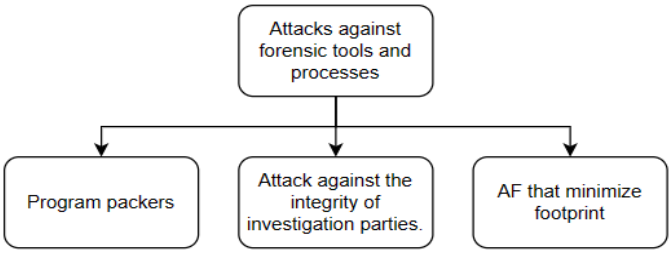

Fig-14: Attacks against forensics tools and processes

4.2 Digital Forensics Tools

As we go deep into the concept of digital forensics, it's essential to explore the necessary tools that investigators use for their investigations. So now we will take the overview of the various basic tools of digital forensics.

4.2.1 Visual Time Analyzer

The Visual Time Analyzer is a software application that grants users complete control over a target computer. It provides comprehensive information about all active programs running on the computer, including details on the time users spend using each program and their internet activity. Additionally, it tracks working hours, breaks, and more. The program offers features such as software usage tracking, internet activity monitoring, computer supervision, project management, and more. An image of this program is provided below[7].

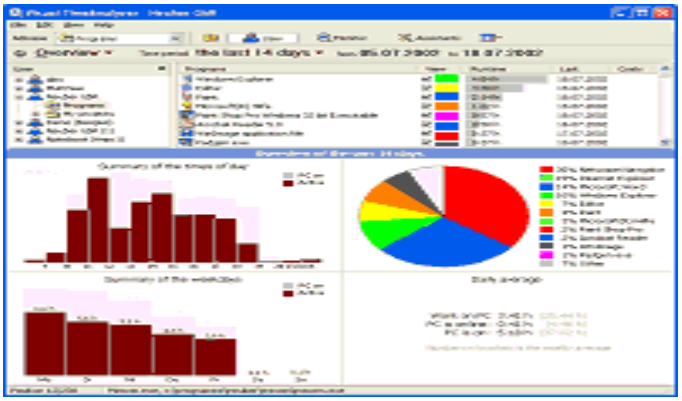

Fig-15: Visual Time Analyzer

4.2.2 X-Ways Forensics

X-Ways Forensics is a sophisticated forensic software application built upon the foundation of WinHex. Its primary purpose is to serve as an advanced tool for digital investigations. The program meticulously examines image files and all directories, providing investigators with detailed information if the directory is not a contiguous segment. It boasts compatibility with various file systems, including FAT, NTFS, CDFS, UDF, and more. Below, you'll find an image showcasing the program's interface[7].

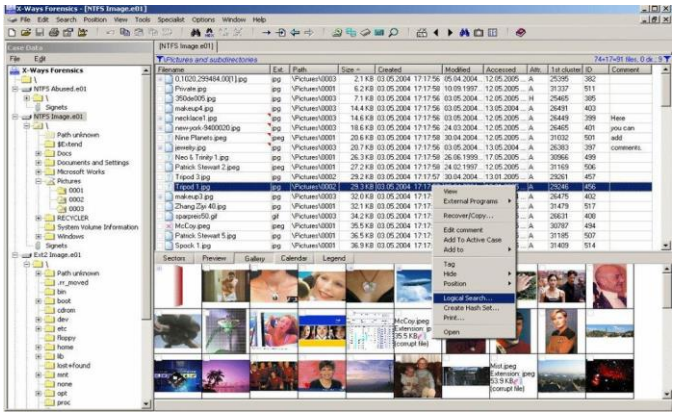

Fig-16: X-Ways Forensics

4.2.3 Evidor

Evidor is primarily employed for the analysis of text documents. Its core function involves selecting a specific keyword and initiating a systematic search within the system's memory. The program diligently retrieves any data containing the designated keyword and presents these findings to the investigator for further examination. Evidor's ability to pinpoint and extract data containing specific keywords from a system's memory aids investigators in uncovering valuable insights and evidence, making it a valuable asset in the field of digital investigations and forensics[7].

4.3 Using Digital Forensics Tools to deal with Images

The digital Forensics tools are not only used for identifying and analyzing the data during the investigations. These tools can also be used or are used to deal with the images also, generally known as "Image Digital Forensics". We will discuss some of the tools that deal with the images.

4.3.1 GFE- Graphic File Extractor

GFE stands for Graphic File Extractor, which is a software application with cross-platform compatibility. It can run on various OS which includes DOS, Windows, UNIX, and any INTL-compatible programs. The primary purpose of GFE is to facilitate the duplication of disk files while maintaining data integrity and without utilizing any compression techniques.

The core functionality of GFE involves copying files from one source, such as a disk, and creating an exact duplicate using a bitstream methodology called Safe back. This Safe back bitstream approach ensures that memory files are retrieved accurately, conserving their original size and structure. One of the key advantage of GFE is its ability to recover files from different storage media and generate reliable backups, regardless of the memory size. When dealing with small or large memory files, GFE ensures that the backup process remains efficient and comprehensive. A main aspect of GFE is its commitment to file recovery without any compression. This means that the program does not alter the data it copies; it maintains the original file size and content during the duplication process. This is particularly essential when preserving the integrity of graphics and other data that may be sensitive to compression artifacts [7].

4.3.2 P2 eXplorer

P2 eXplorer is a software application that plays a crucial role in digital investigations. Its primary function is to enable the viewing and analysis of images extracted using the Safeback program. Investigators use this tool which helps them to uncover and explore the contents of these extracted images in a thorough and detailed manner. The Safeback program is renowned for its ability to create precise copies of disk files while maintaining data integrity and without resorting to any compression methods. It captures a snapshot of the original data, ensuring that every detail is faithfully preserved. However, when dealing with digital investigations, merely creating these copies is not sufficient; investigators need a means to delve into the contents of these images effectively. This is where P2 eXplorer comes into play. It acts as a dedicated image viewer, providing investigators with a comprehensive toolset to navigate and scrutinize the information contained within the Safeback-generated images[7].

4.3.3 ILOOK

ILook is a software application tailored to meet the needs of investigators in the field of digital forensics. It offers a user-friendly graphical interface that closely resembles Windows Explorer, making it accessible and intuitive for users familiar with the Windows operating system. The primary function of ILook is to empower investigators to conduct thorough examinations of a suspect's computer system. Investigators can delve into the system, meticulously extracting the data and information they require for their investigative purposes. Additionally, ILook provides a HEX viewer, which is a crucial tool for forensic analysis. A HEX viewer enables investigators to inspect the raw hexadecimal representation of data. This can be immensely helpful in identifying hidden or obscured information, as it provides a low-level view of the data that is independent of file formats or encoding schemes[7].

4.4 Existing Systems

This section aims to shed light on the ongoing efforts in the field by showcasing existing systems dedicated to digital investigation case management. A comprehensive examination of these systems will encompass an in-depth discussion of their features, benefits, and short comings [8].

4.4.1 AXXERA 4N6

Axxera's 4N6 system, serves as a robust solution for overseeing digital forensic cases and investigations. Users of the 4N6 tool enjoy the convenience of managing their cases within a single, integrated platform, streamlining the process of capturing, monitoring, and reporting on cases and their findings through its automated case workflow management capabilities. The Axxera 4N6 Integrated Case Management System was purpose-built to simplify the case creation procedure by seamlessly integrating data from diverse digital forensic tools into one centralized case management platform. Within this system, users have the capability to attach all evidence and associated documents to their respective cases. Additionally, the system provides a centralized repository for document management that accommodates various formats, including media files and tool-specific output formats. It offers users a unified interface with role-based access functions, providing a comprehensive global view for real-time access to analysis, case management, and reporting.

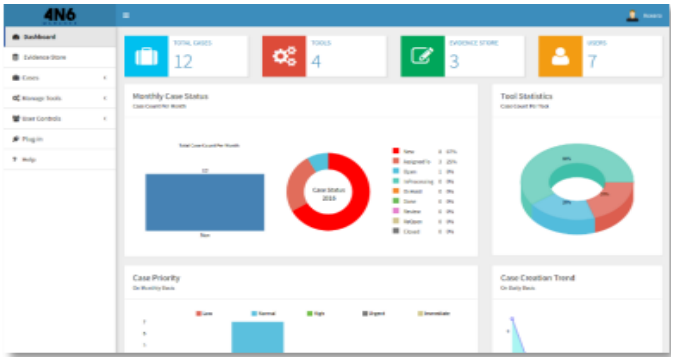

Fig-17: Main interface og Axxera 4N6[8]

4.4.2 xBit Digital Forensics Case Management

xBit stands out as specialized digital case management software tailored for the unique needs of digital forensic examiners. Its core objective is to assist digital forensic investigators in efficiently handling the typically daunting challenge of organizing and overseeing the multitude of case data associated with digital forensic investigations. Within this system, users have the capability to input comprehensive case and evidence details. xBit offers a range of control access features, including a role-based access model, enhancing security and user management. Additionally, this platform empowers investigators to document crucial notes and maintain a personal investigation journal, further streamlining the investigative process.

In a typical scenario, a single case often requires the collaborative efforts of multiple investigators, each contributing their expertise in areas such as data recovery, registry analysis, or network investigation. However, this particular case management tool falls short in terms of providing essential features for effectively monitoring and tracking tasks that are assigned to different investigators involved in the case[8].

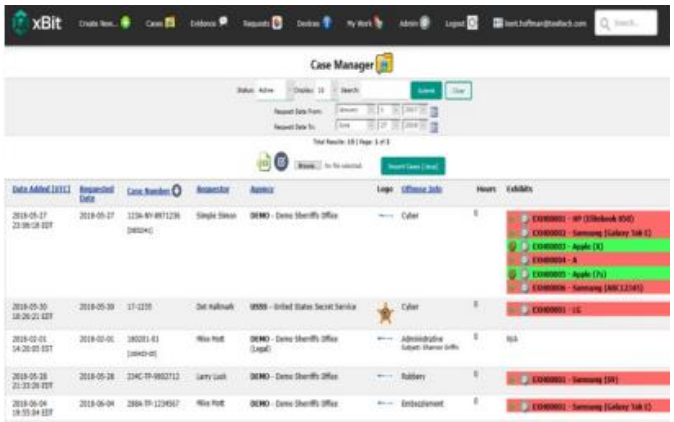

Fig-18: xBit Digital Forensic Case Management[8]

4.4.3 MagnetAtlas

It stands as a cutting-edge case management software developed by Magnet Forensics, a global leader renowned for crafting software solutions tailored for digital forensic professionals. This impressive tool encompasses digital evidence management and maintains the critical chain of custody. Operating as a web-based case management solution, it seamlessly consolidates all case-related information, spanning from evidence and lab resources to examination procedures. Its primary objective is to ensure the unbroken chain of custody while facilitating comprehensive case reviews. Moreover, administrators have the capability to delegate cases to other investigators, streamlining case distribution within the case management system. Users find ease in revisiting past investigations to validate adherence to appropriate procedures. Additionally,it boasts simplified reporting features, enabling any member of the investigative team to access and assess case information conveniently from any location and at any time[8].

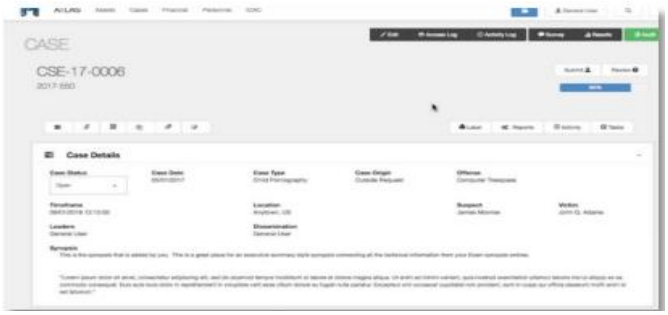

Fig-19: Case Details in MagnetAtlas[8]

However, it's worth noting that this particular case management tool was not structured in alignment with a digital forensics investigation framework, and its process flow lacks a solid theoretical foundation[8].

5. CONCLUSION

In conclusion, this research has put light on the evolving relationship between cryptography and digital forensics in the modern digital time. Cryptography plays a vital role in safeguarding data and communications, ensuring the privacy and security of individuals and organizations. However, this same technology can be leveraged to conceal criminal activities, necessitating the development of advanced digital forensics techniques to uncover hidden evidence. Furthermore, our study emphasizes the vital significance of collaborative efforts across different fields and the continuous enhancement of forensic techniques and tools to keep pace with the constantly evolving cryptographic environment. The researchers, professionals, and policy-makers join forces to devise creative approaches that uphold individuals' privacy rights while simultaneously enabling the efficient probing of cybercrimes.

With the continuous advancement of technology, the mutually dependent connection between cryptography and digital forensics is bound to endure and undergo further transformations. Our aspiration is that this research will become a valuable asset for individuals aiming to traverse this intricate junction and participate in the ongoing discussion about the most effective way to maintain a delicate equilibrium between personal privacy and collective security in the digital era.

REFERENCES

[1] Abdalbasit Mohammed Qadir and Nurhayat Varol,"A Review Paper On Cryptography", Firat University, Elazig, Turkey.

[2] Marcus K.G. Adomey, "Introduction to Cryptography," Chief Operations Manager, AfricaCERT.

[3] "An Introduction To Cryptography" by PGP Corporation,version 8.0.

[4] Khawja Imran Masud, Md Rakib Hasan, MD.Mozammel Hoque, Upel Dev Nath, Md.Obaidur Rahman,"A New Approach for data Encryption and Decryption",Department of CSE, Dhaka University, Gazipur, Bangladesh.

[5] Hussein Majed, Hassan Noura, Ali Chehab,"Overview of Digital Forensics and Anti-Forensics Techniques",Department of Computer Studies,Arab Open University, Beirut, Lebandon.

[6] Semih Ulupinar, Sengul Dogan, Erhan Akbal, Turker Tuncer,"The Importance of standardization in Biometric Data for digital forensics", Department of Digital Forensics Engineering, Technology faculty, Firat University, Elazig.

[7] Rayan Sulaiman Khalaf and Asaf Varol,"Digital Forensics: Focusing on Image Forensics", Software Engineering Department, Firat University, Elazig, Turkey.

[8] Vimal Raj Silvarajoo, Shu Yun Lim, Paridah Daud," Digital Evidence Case Management Tool for Collaborative Digital Forensics Investigation", Faculty of Business and Technology, UNITAR International University, Petaling Jaya, Malaysia.