Network security Forensic revised-1.docx

Assignment

Class

Organization

Document Details

Submission ID

trn:oid:::1:2975081485

Submission Date

Jul 30, 2024, 6:02 PM UTC

Download Date

Jul 30, 2024, 6:03 PM UTC

File Name

2024_07_30_Network_security_Forensic_revi_4605455a1a5cad06.docx

File Size

3.5 MB

22 Pages

4,714 Words

28,237 Characters

79% detected as AI

The percentage indicates the combined amount of likely AI-generated text as well as likely AI-generated text that was also likely AI-paraphrased.

Caution: Review required.

It is essential to understand the limitations of AI detection before making decisions about a student's work. We encourage you to learn more about Turnitin's AI detection capabilities before using the tool.

Detection Groups

1 AI-generated only 79%
Likely AI-generated text from a large-language model.

2 AI-generated text that was AI-paraphrased 0%
Likely AI-generated text that was likely revised using an AI-paraphrase tool or word spinner.

Frequently Asked Questions

How should I interpret Turnitin's AI writing percentage and false positives?
The percentage shown in the AI writing report is the amount of qualifying text within the submission that Turnitin's AI writing detection model determines was either likely AI-generated text from a large-language model or likely AI-generated text that was likely revised using an AI-paraphrase tool or word spinner.

False positives (incorrectly flagging human-written text as AI-generated) are a possibility in AI models.

AI detection scores under 20%, which we do not surface in new reports, have a higher likelihood of false positives. To reduce the likelihood of misinterpretation, no score or highlights are attributed and are indicated with an asterisk in the report (*%).

The AI writing percentage should not be the sole basis to determine whether misconduct has occurred. The reviewer/instructor should use the percentage as a means to start a formative conversation with their student and/or use it to examine the submitted assignment in accordance with their school's policies.

What does 'qualifying text' mean?
Our model only processes qualifying text in the form of long-form writing. Long-form writing means individual sentences contained in paragraphs that make up a longer piece of written work, such as an essay, a dissertation, or an article, etc. Qualifying text that has been determined to be likely AI-generated will be highlighted in cyan in the submission, and likely AI-generated and then likely AI-paraphrased will be highlighted purple.

Non-qualifying text, such as bullet points, annotated bibliographies, etc., will not be processed and can create disparity between the submission highlights and the percentage shown.

Digital & Network Security Forensics

Case Study

Table of Contents

Executive Summary:

In the current assessment an evidence image file is provided downloaded by given link to perform further digital forensic analysis solve the criminal activities. The evidence file contains all type of sensitive information to provide case solution in further steps all sensitive and suspected data found given in report with supported information.

https://myaru-my.sharepoint.com/:f:/g/personal/aw21_aru_ac_uk/Eqd01XMa2spLmIvVb5rDwQABydVlZ2fr0_5CZDiCi1DFdw?e=BOE32S

During digital forensic process working as investigation officer need to find criminal evidence using small level of digital information. In the past there was no concept of digital forensic tools however using latest techniques and tools finding of criminal activities has become easy to solve the complex level challenges After working in current assessment multiple sensitive information found to solve the criminal activities where list of installed operating system found, time zone settings and software program installations, list of hardware devices and volumes connected with operating system, user profile details and other sensitive information etc. After the evidence analysis a strong and reliable browsing forensics field. If the desired success is achieved with this model, maybe a new study field such as search engine data computer forensics will be able to be produced. After working in assessment now everyone can perform digital forensics of any images for organization to solve criminal activities. During the work initial step was involve to open the case image file in investigation tool therefore a technical person should have strong level knowledge about the cyber activities in such way a person can find the sensitive information easily to solve the case.

Objectives:

In the field of information technology negative use of internet technology is increase therefore risk level of cyber threat never come to zero level. Therefore, after cyber-attack every organization try to recover data and other sensitive information another important point company also need to find the multiple attacking activities and directions in details for this purpose digital forensic process start in computing infrastructure. Therefore, importance of forensic process cannot deny for small to large level financial organizations. Normally digital forensic process contains complex level challenges therefore current process performed using a team of specialists and experts with process and digital evidence regarding cybercrime. A technical person needs to specialists in performing investigation of encrypted data using different types of forensic application and techniques. In some cases, need to crack passwords, recover deleted data or files to find supporting evidence therefore complete process included with investigation of digital level information [1]. After the analysis process assessment collect the digital evidence and facts to report digital crime or cybercrime activities. The complete findings of digital forensics report need to compiles according necessary actions. It also provides standard support about cyber regulate authorities and exploring of forensic investigations to support cybercrime incidents. During investigation process a digital forensics person is someone who has a desire to follow the multiple evidence and solve a crime based virtually based with imagine a security breach happened art a company or organization resulting of data stolen in specific situation [2]. However, the main responsibility of forensic analyst to determines the cyber attacker objectives and collection of malicious activities and get information about planted malware, emails and other sensitive information. In the past history of digital forensics law enforcement during the specific age has a minimal understanding of the application of digital techniques. Similarly,

during the forensic team were mostly representatives of government law commencement agencies with different computing background [3]. The main concerns of current data for law enforcement were data storage as most documentation happened digitally.

Computer evidence analyzed:

In current assessment an employ from the well-respected financial institute bank with six years ago convinced the following criminal activities.

- Viewing and possessing conspiracy to distribute indecent pictures of naughty girls and bad boys
- Embezzlement from bank customer funds and conspiracy to defraud the banks.
- During the criminal activity an employee convicted of viewing and possessing indecent pictures conspiracy to distributed such pictures, embezzlement and conspiracy to defraud with bank like data breach, fraudulent remove of deposits is noted but not confirmed as art of his convictions.
- Checking and processing indecent pictures
- Conspiracy to distribute indecent pictures
- Embezzlement from bank customer funds
- Conspiracy to defraud the banks

Adding data source:

Digital forensics involves identifying, preserving, analyzing, and presenting electronic evidence in a way that is legally acceptable. Given the increasing use of technology in almost all aspects of life, criminal activities often leave behind digital traces. This makes digital forensics crucial in solving crimes, as it can uncover valuable information from computers, mobile devices, and other digital storage media. Digital forensics provides critical assistance to law enforcement agencies, enabling them to recover deleted files, trace the origin of cyber-attacks, analyze communication records, verify the authenticity of digital documents, and identify unauthorized access to systems. Such expertise is invaluable not only for solving crimes but also for presenting evidence in court. The data collected through digital forensics can be pivotal in proving guilt or innocence, making it a fundamental part of modern legal proceedings. In the role of a forensic analyst, one of the primary tools used is Autopsy, a well-known digital forensics platform. To start an investigation with Autopsy, the first step is to download and install the software from the official Autopsy website. Once installed, the forensic analyst sets up a new case by entering essential details such as the case name, case number, and examiner name. These details help in organizing and managing the investigation process. After setting up the case, the next step is to add the evidence by specifying the location of the forensic image, which is a complete copy of the digital storage media being analyzed. Autopsy supports various types of evidence, including disk images, local drives, and remote data. With the evidence added, the analyst can then use Autopsy's user-friendly interface to navigate through the data and perform various analyses, such as recovering deleted files, analyzing file structures, and more. This streamlined process allows for efficient and thorough examination of digital evidence, making it an essential tool in modern forensic investigations.

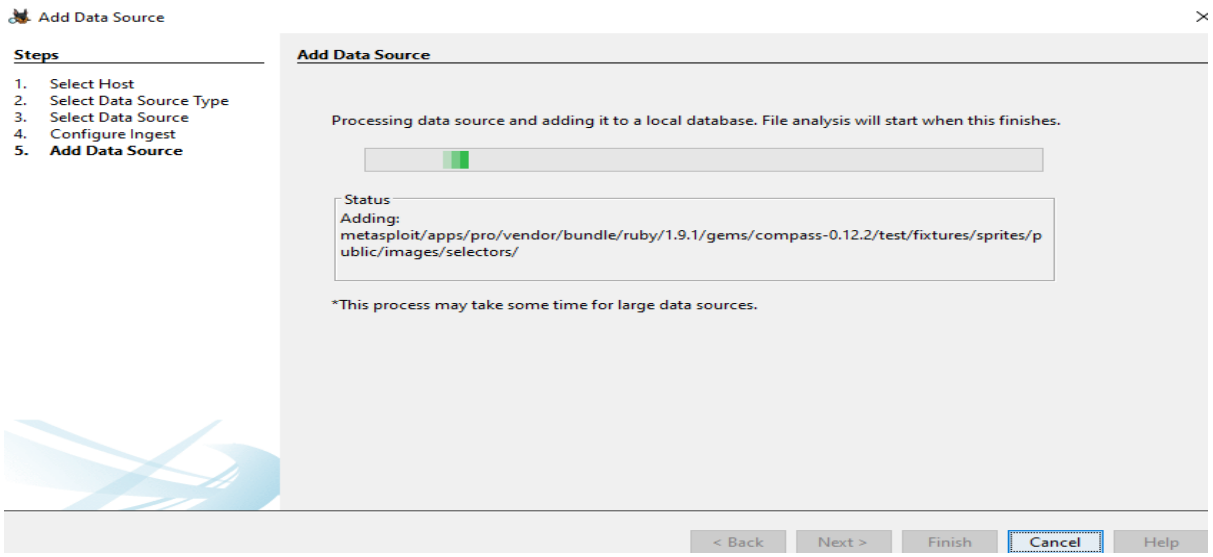

Figure: add data source

In the second step of a forensic analysis using Autopsy, the disk image is thoroughly examined with all its available properties, including data size, disk volumes, and file systems. During this analysis, Autopsy processes the data, indexing and categorizing files to make them easier to navigate and analyze. This step may take a few minutes to several hours, depending on the size and complexity of the data. The tool systematically scans for artifacts such as deleted files, internet history, email archives, and other potentially incriminating information. Once the analysis is complete, Autopsy generates a detailed report summarizing the findings. This report serves as crucial supporting material, documenting the evidence in a structured format that can be used in court proceedings or further investigative steps. The report typically includes information on the discovered files, their metadata, and any relevant connections or patterns that may aid in solving the case.

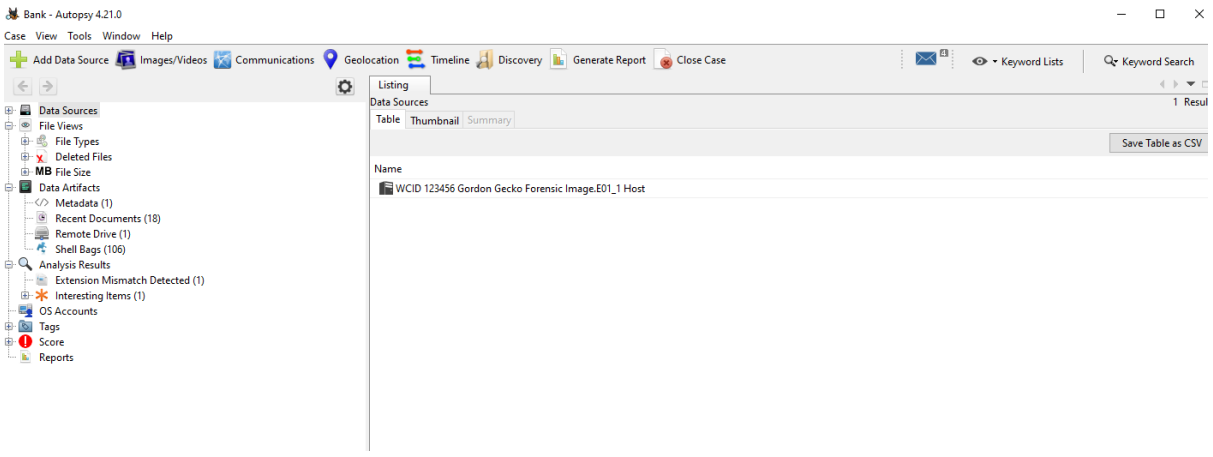

Figure: disc image file

In the current disk image file, three types of disk volumes containing sensitive information are available. Each volume is meticulously analyzed to reveal details such as sector status, length, and flags. These volumes contain critical data that is essential for solving the criminal case. The correct values of sector status, length, and flags provide insights into the structure and integrity of the data, ensuring that the information extracted is accurate and reliable. Each disk volume holds sensitive information that can significantly aid in the investigation,

uncovering evidence that may not be immediately apparent but is crucial for building a comprehensive understanding of the case.

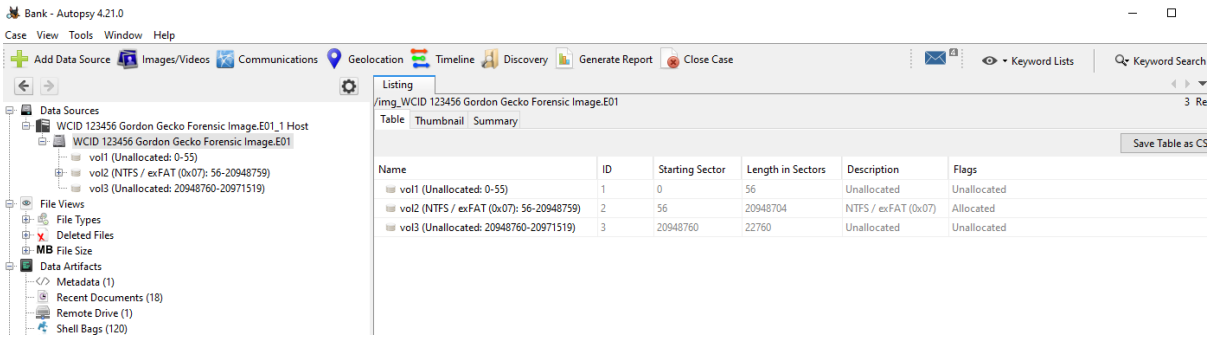

Figure: Disc image volumes

Relevant Findings:

As a forensic analyst, accessing suspected information is crucial for solving criminal activities and aiding investigation officers. The list of sites in the given figure showcases the browsing activities performed by the attacker, highlighting various criminal operational actions within the computing environment. This data reveals patterns and specific actions taken by the attacker, which are essential for understanding the extent and nature of the criminal activities. These browsing activities demonstrate how attackers exploit device access to make unauthorized changes, posing significant risks, particularly to financial organizations. Such institutions hold sensitive customer information, making them prime targets for cybercriminals. Unauthorized access and manipulation of this data can lead to severe financial and reputational damage. Therefore, the insights gained from analyzing these browsing activities are invaluable for identifying the methods and tools used by the attacker, ultimately contributing to a comprehensive understanding of the case and supporting law enforcement efforts.

Operating system information:

In every computing environment, the operating system plays a crucial role as it contains all the essential functionalities needed for computers to operate. During an investigation, details about the operating system are vital as they provide critical context and insights into the computing environment being analyzed. The operating system information includes the name, version, and source details, which help forensic analysts understand the structure and configuration of the system in question. This information is important because it can reveal specific system vulnerabilities that might have been exploited by attackers. Additionally, knowing the operating system helps in identifying the appropriate forensic tools and methods for data extraction and analysis. By understanding the operating system details, forensic analysts can more effectively trace the steps taken by an attacker and reconstruct the sequence of events leading up to the incident. This, in turn, supports the broader investigation and aids in developing a comprehensive understanding of the criminal activity being examined.

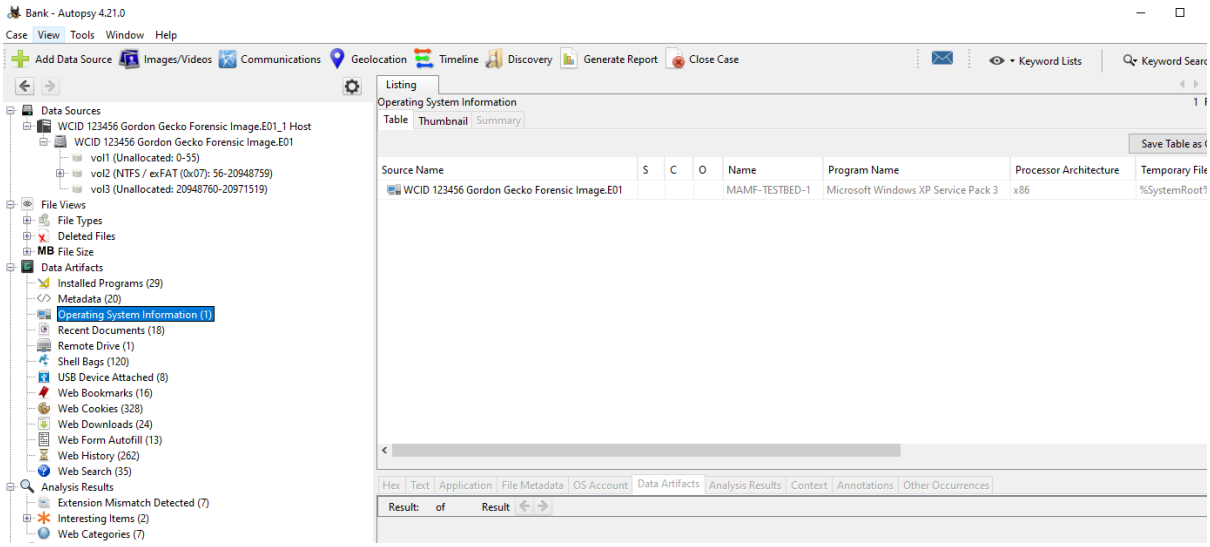

Figure: operating system information

Recent documents:

In the current forensic analysis, the details of recent documents are provided below, where a list of computing devices is available in the image files. These recent documents offer valuable insights into the activities and operations performed on the suspect's device. By examining these documents, forensic analysts can trace the user's actions, understand the nature of their activities, and gather evidence that might be crucial for solving the case. This information is essential as it can help link the suspect to specific actions and provide a timeline of events that are critical for the investigation.

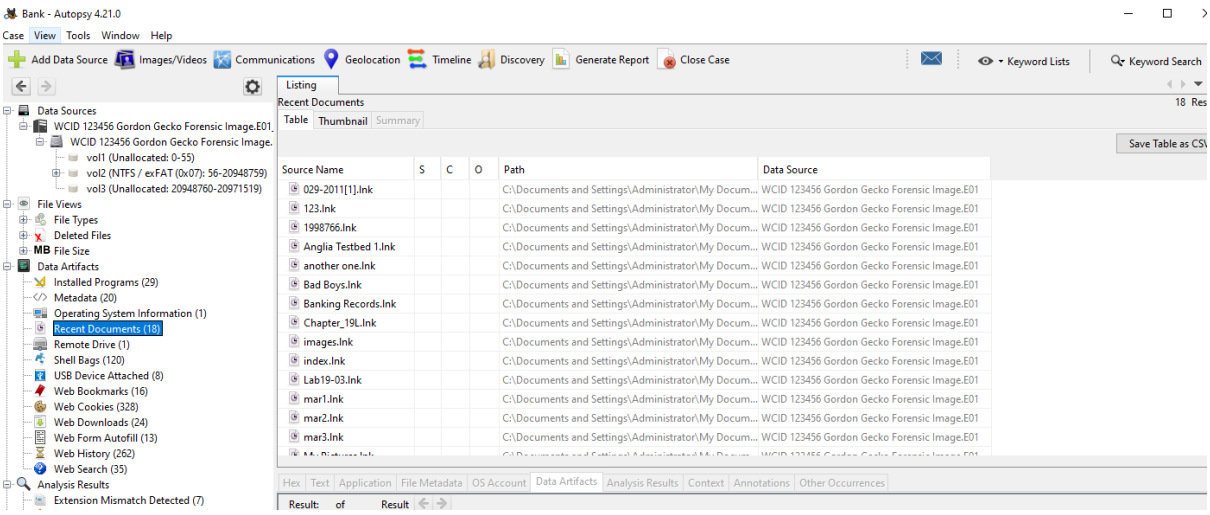

Figure: list of recent documents

Remote devices:

In the given figure, a set of remote device details is provided below with local path and ID values. During these days, remote access to networking resources is not a significant challenge. For example, using various simple tools and applications, employees of any organization can easily access system resources for activities like remote meetings without needing additional resources. However, in some cases, employees require specific types of training and need to attend cybersecurity awareness training programs. This is crucial to

ensure they are well-equipped to handle potential security threats and understand the best practices for maintaining a secure computing environment. The ability to access remote devices can be beneficial for operational efficiency but also poses security risks if not managed properly. Therefore, the details of these remote devices are critical in the forensic analysis as they can provide insights into unauthorized access and potential security breaches.

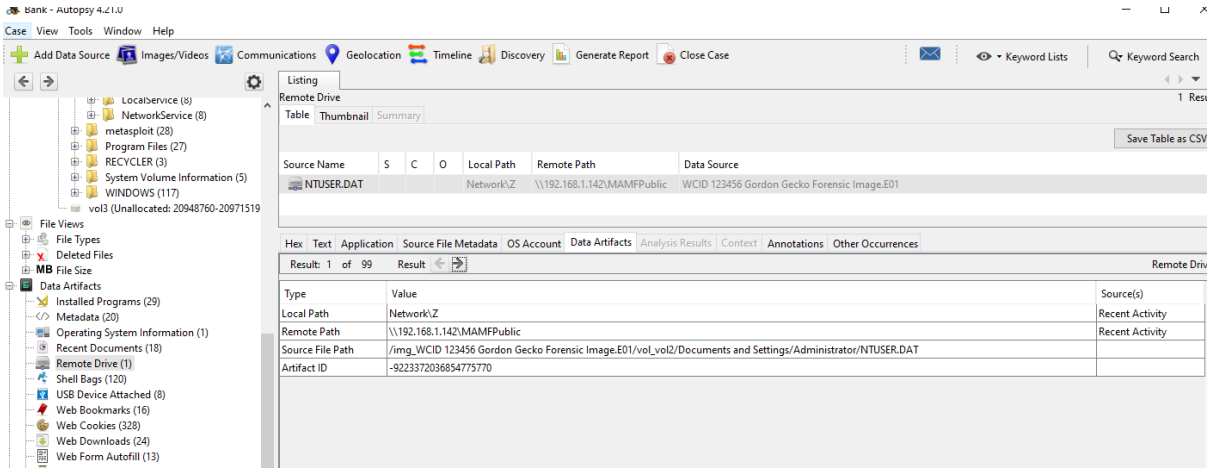

Figure: remote device

Suspected shell bags:

In the given figure, a set of system files is provided, which are stored in the image data for future use. Shell bags are system artifacts in Windows operating systems that store information about the folders and files accessed by the user, including details such as folder views and file locations. These artifacts can be crucial in forensic investigations as they provide insights into the user's interactions with the file system.

The shell bags can reveal patterns of usage and access to specific files and directories, which might be relevant in identifying suspicious activities or unauthorized access. Analyzing these files helps in reconstructing the timeline of user activities and understanding the context of the evidence. This information is essential for determining how and when files were accessed, which can be valuable for solving the case and providing critical evidence for legal proceedings.

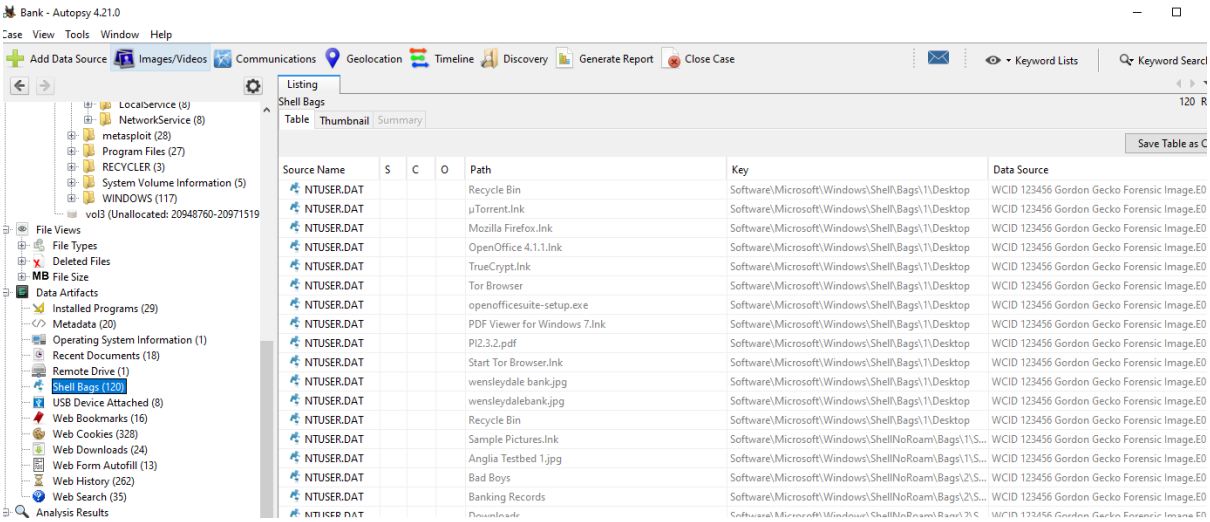

Figure: shell bags

USB devices attached:

USB devices are significant components in computing environments, often used for data transfer and storage. In forensic analysis, information about USB devices connected to a system can provide valuable insights into potential security breaches. Cyber attackers frequently use USB devices to transfer malicious files, exploit vulnerabilities, or execute unauthorized operations. An attacker might target newly hired employees within an organization, as they may be less familiar with security protocols and more susceptible to malicious tactics. This makes USB device information crucial for identifying and understanding the methods used by attackers. By analyzing the details of connected USB devices, forensic investigators can uncover traces of malicious activities and determine the extent of any potential security incidents. This analysis helps in addressing the breach, mitigating future risks, and enhancing overall cybersecurity measures.

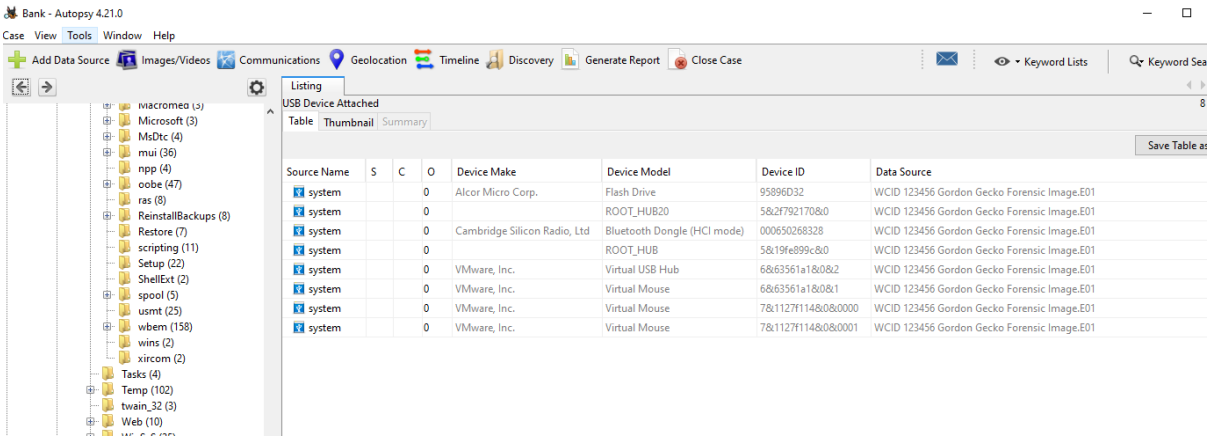

Figure: devices attached

Web bookmarks:

Bookmarks are a common feature in web browsers that allow users to save URLs of frequently visited or important websites for easy access in the future. In the context of digital forensics, analyzing web bookmarks can provide critical insights into a user's online activities and interests. Bookmarks stored within image files can reveal significant information about the user's browsing habits, preferred websites, and potential areas of interest. For investigators, these bookmarks can serve as a useful resource in understanding the suspect's online behavior, identifying any malicious sites visited, or discovering connections to criminal activities. This analysis helps in constructing a clearer picture of the suspect’s digital footprint, supporting the overall investigation and aiding in the resolution of the case.

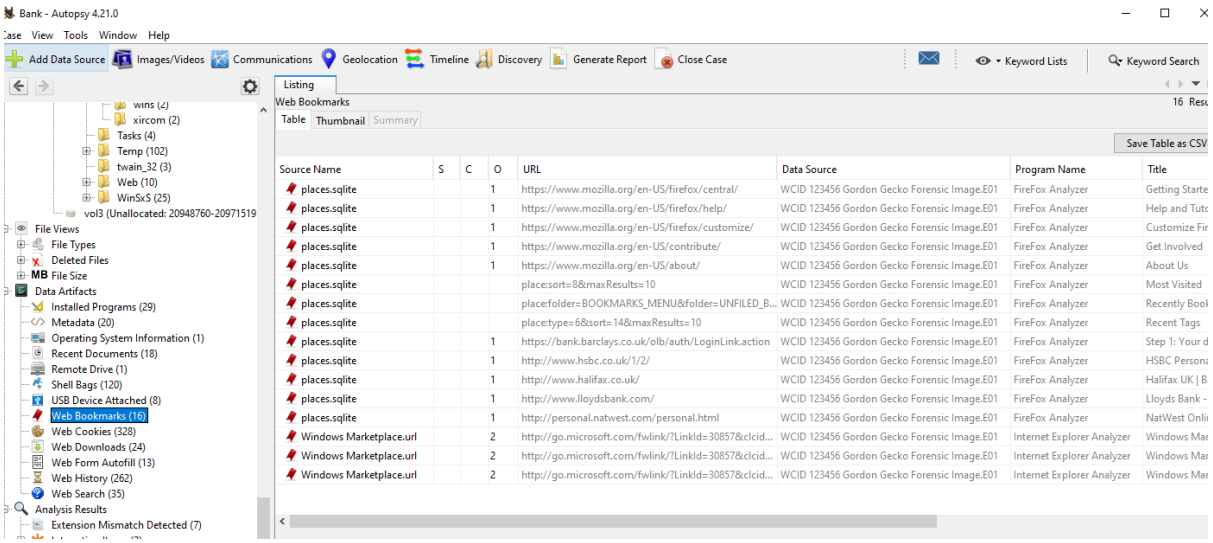

Figure: bookmarks details

Web cookies:

Web cookies are small pieces of data generated by web servers and stored by web browsers. They serve various purposes, such as maintaining user sessions, tracking user preferences, and enhancing the browsing experience. Cookies can include information like session identifiers, user settings, and tracking data that persists across browsing sessions. In digital forensics, analyzing web cookies from image files can provide valuable insights into user interactions and browsing habits. Cookies can reveal details about the websites visited, the user's login sessions, and their online behavior. For investigators, this information can be crucial for identifying patterns, understanding user activities, and uncovering potential evidence related to criminal activities. By examining the cookies attached to the image files, forensic analysts can gain a deeper understanding of the suspect's digital footprint and support the investigation with relevant data.

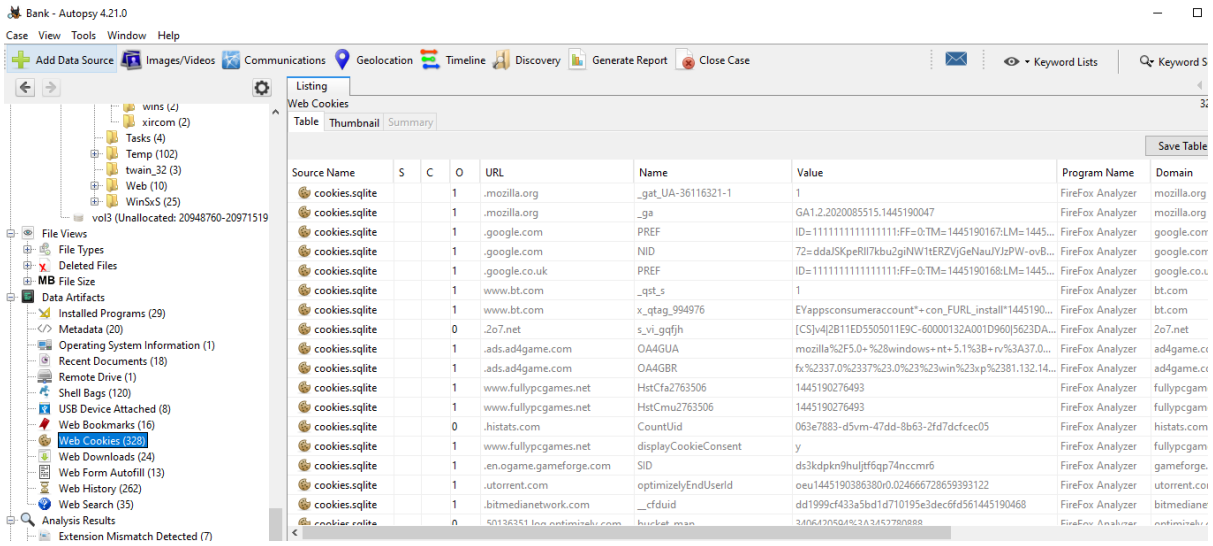

Figure: web cookies

Web downloads:

Web downloads are a crucial aspect of digital activity, as they involve the transfer of files and data from the internet to a local system. This can include various types of files, such as documents, executables, and media. For attackers, web downloads can be a method to acquire or distribute sensitive or malicious content. In the current forensic analysis, web download activities are particularly significant. The image files contain evidence of suspected web downloads, which can provide insights into the nature of files being transferred and the methods used by the attacker. By examining these downloads, forensic analysts can trace the source and destination of the files, identify potentially harmful content, and understand how it might have been used in the criminal activity. The details of these downloads, such as file names, sources, and timestamps, can help establish a timeline of events and provide critical evidence in the investigation. This information is valuable for understanding the attacker's actions and motives, and it can support legal proceedings by linking the digital evidence to the criminal case.

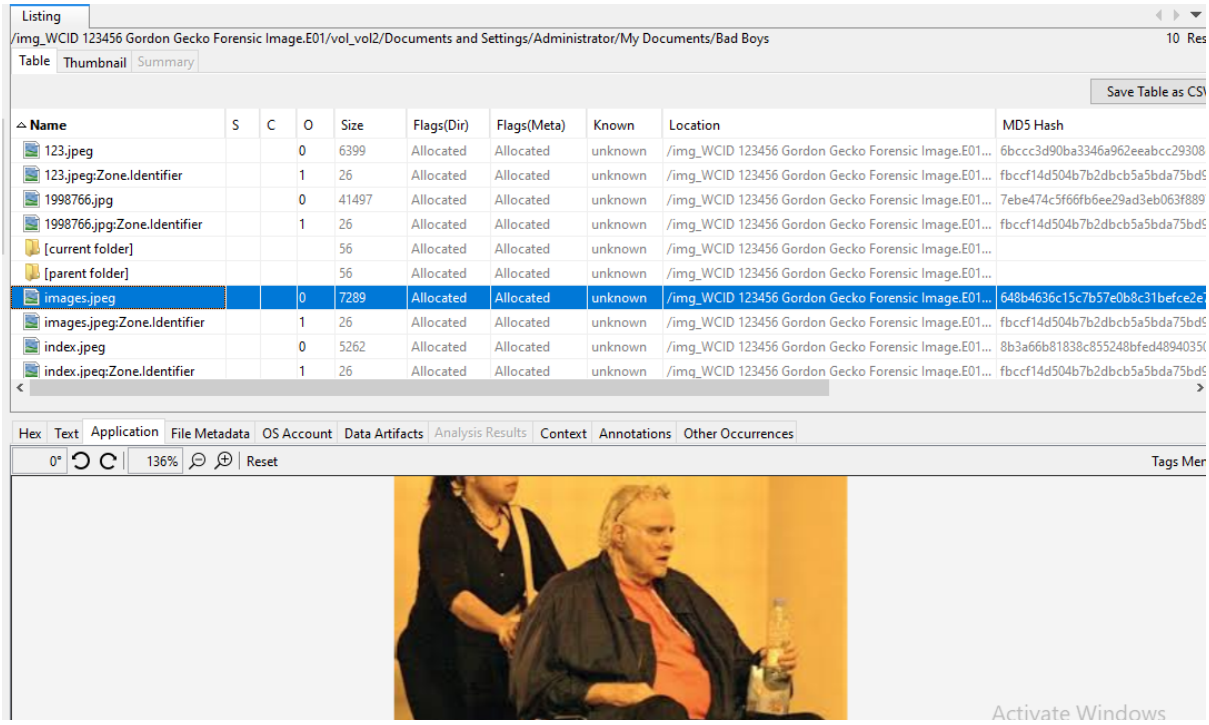

Figure: web downloads

Web links:

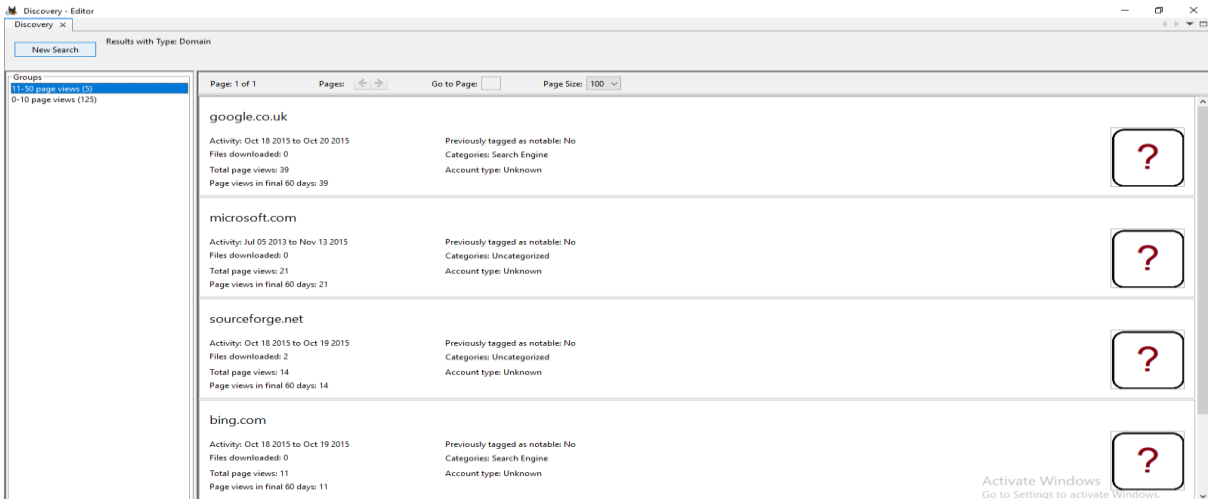

Figure: List of web links discovered

Web links, or URLs, play a significant role in digital forensics as they often provide pathways to where sensitive information has been accessed, shared, or exploited. Attackers frequently use web links to facilitate fraudulent activities, leveraging stolen data to carry out scams or other malicious actions. These links can lead to phishing sites, malicious downloads, or other compromised resources designed to further the attacker's objectives. In the current forensic analysis, the investigation has revealed web links that are critical to understanding the attacker's operations. These links may include references to malicious code, fraudulent websites, or other sources used by the attacker to achieve their goals. By examining these links, forensic analysts can trace the activities of the attacker and uncover connections between different elements of the crime.

The web links found in the current image files provide evidence of how the attacker may have exploited customer information or executed malware-based instructions. This information is instrumental in piecing together the attacker's methods and intentions, and it helps in assessing the scope and impact of the criminal activities.

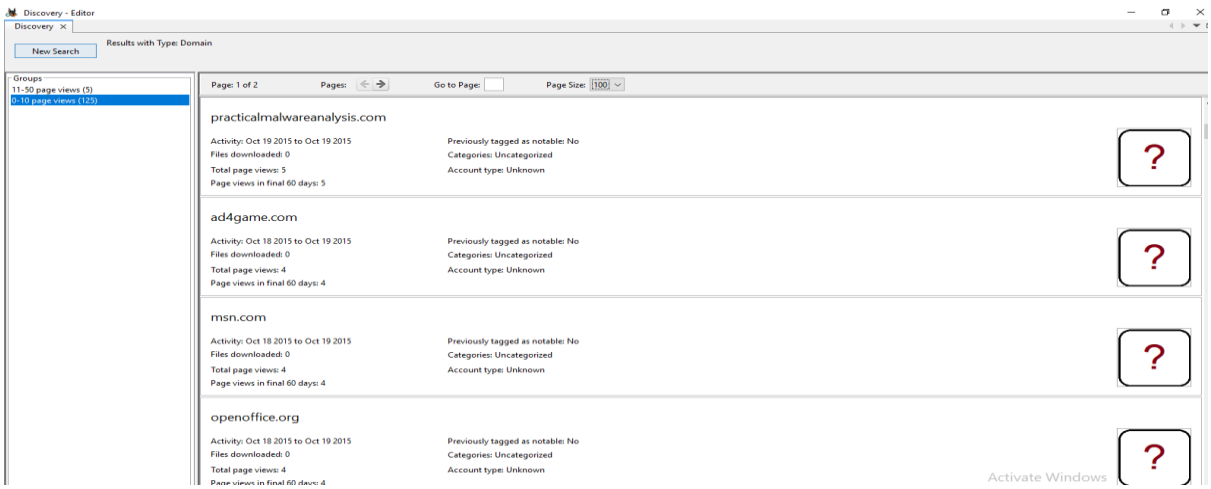

Figure: List of web links discovered

In the forensic analysis, a set of images with associated metadata has been identified as part of the investigation. These images are crucial as they may contain evidence related to the criminal activities under review. The metadata associated with these images can provide valuable context, such as timestamps, file origins, and modification history, which are essential for understanding the role these images played in the case. The images discovered in the Autopsy tool's discovery option are particularly noteworthy. They require further examination to establish their relevance to the investigation. To fully uncover their significance, it is necessary to conduct a detailed analysis with the suspected individual to obtain additional insights and corroborate findings. This step is vital for validating the evidence and linking it to the broader context of the criminal activity being investigated.

Suspected criminal images:

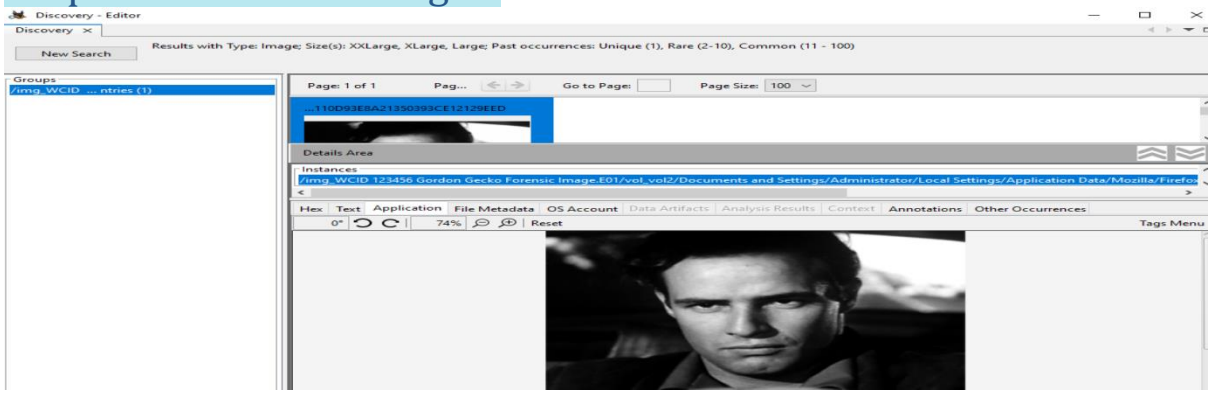

Figure: Suspected criminal image

In the provided figure, a document associated with fraudulent activities has been identified. This document exhibits a strong connection to the criminal activities under investigation. It appears to be used by the perpetrator to facilitate attacks on banks or other financial institutions. The document's contents suggest it may contain plans, instructions, or other details pertinent to executing financial crimes. This document's significance lies in its potential role in orchestrating or supporting attacks on sensitive financial systems. Further examination and analysis are required to understand how this document was used and its impact on the criminal operations. This step is crucial for linking the document to specific incidents and establishing its relevance in the broader scope of the financial attack investigation.

Discovery fraud documents:

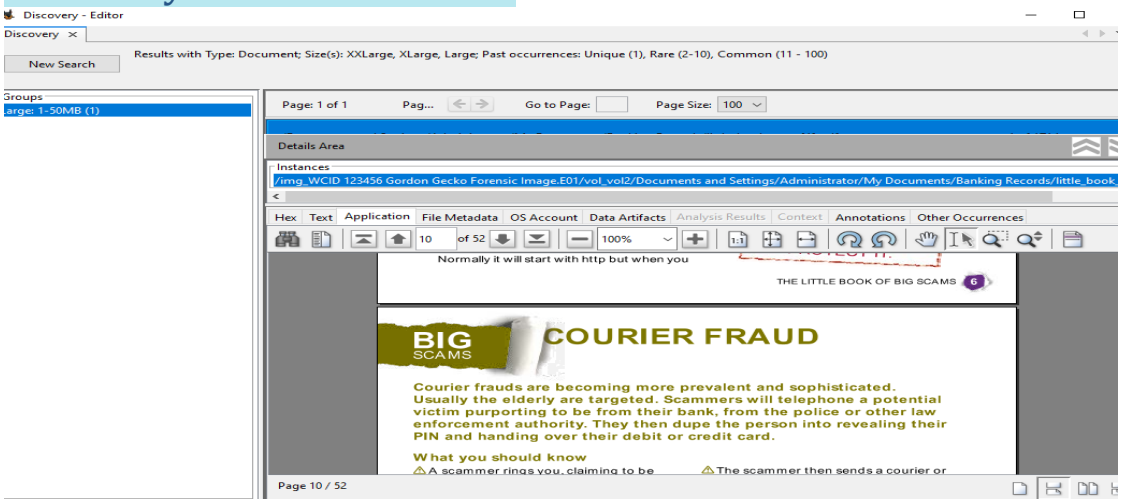

Figure: Discovery fraud document

In the provided figure, a document associated with fraudulent activities has been identified. This document reveals a significant link to the criminal activities under investigation, indicating its use by the perpetrator to facilitate attacks on banks or other financial institutions. The contents of the document suggest it may include plans, instructions, or other crucial details relevant to executing financial crimes. The importance of this document lies in its potential role in orchestrating or supporting attacks on sensitive financial systems. To fully understand its impact, further examination and analysis are necessary. This process is essential for linking the document to specific incidents and assessing its relevance within the broader context of the financial attack investigation.

Figure: Activity timeline

Supporting Information:

Audio/Video and images gallery:

The provided figure includes information from an audio/video and images gallery. This data consists of details such as tags, creation time, modification time, and hash-based values. These elements are essential for verifying the authenticity and integrity of the multimedia files. The tags and timestamps offer insights into the context and timeline of the content, while the hash values are crucial for ensuring that the files have not been tampered with. This supporting information aids in the investigation by providing additional context and verification for the multimedia evidence.

Figure: calls image

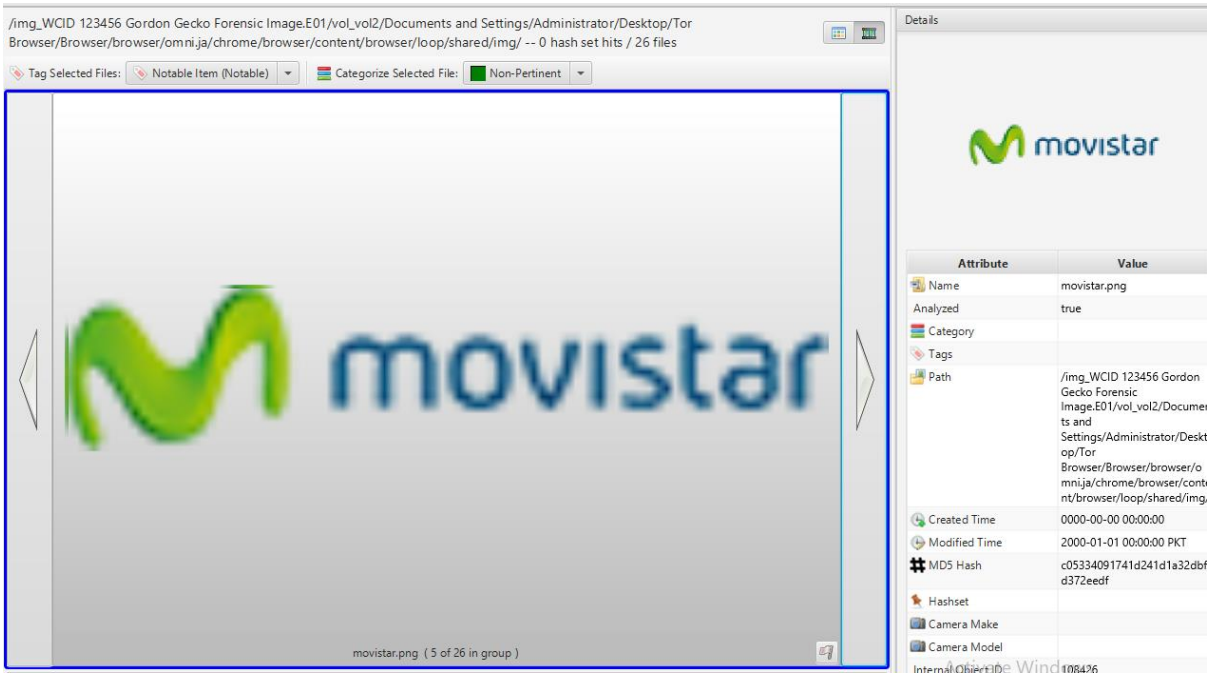

Figure: desktop icon

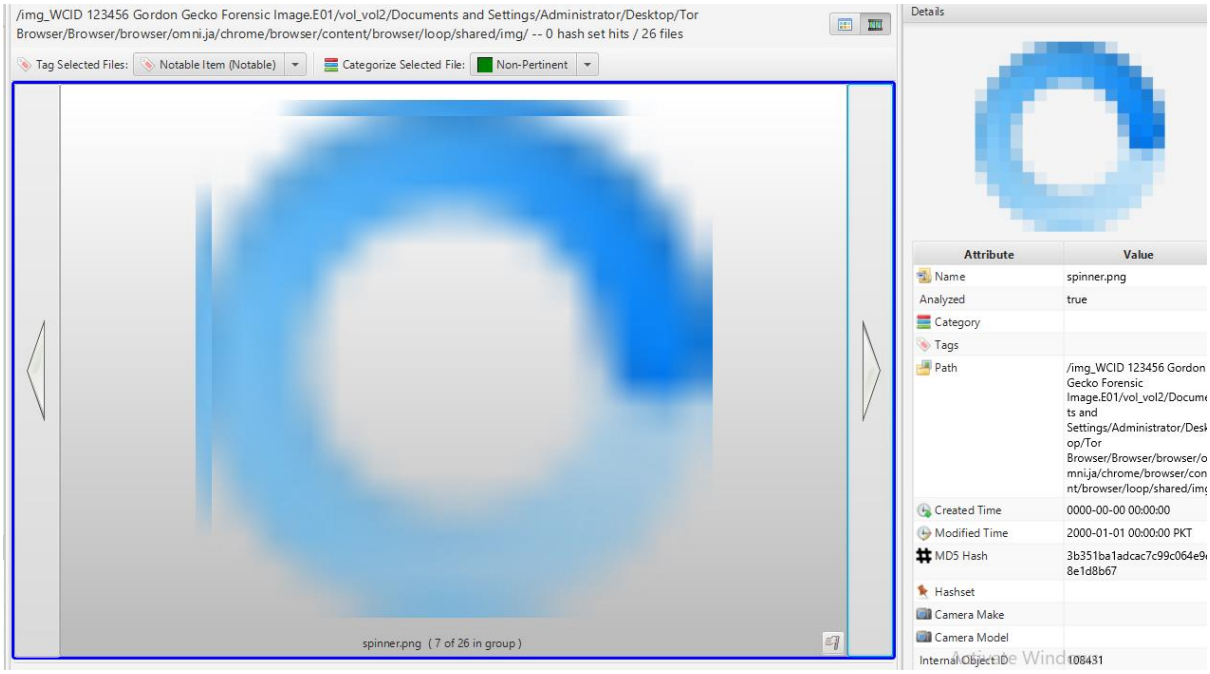

Figure: desktop icons

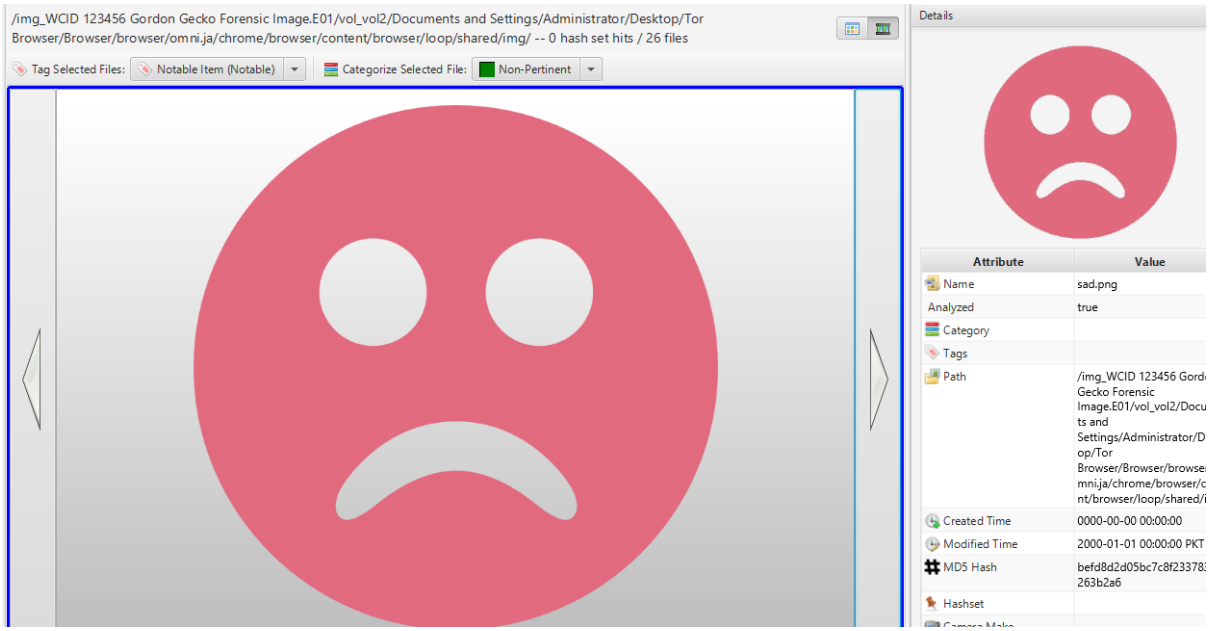

Figure: desktop pictures

In the provided figure, a deleted item has been identified. Recovering this item is crucial as it may contain sensitive information pertinent to solving the case. Deleted files can often hold valuable evidence that could shed light on the criminal activities under investigation. By recovering and analyzing this item, we can uncover additional details that might be instrumental in building a comprehensive understanding of the case and advancing the investigation.

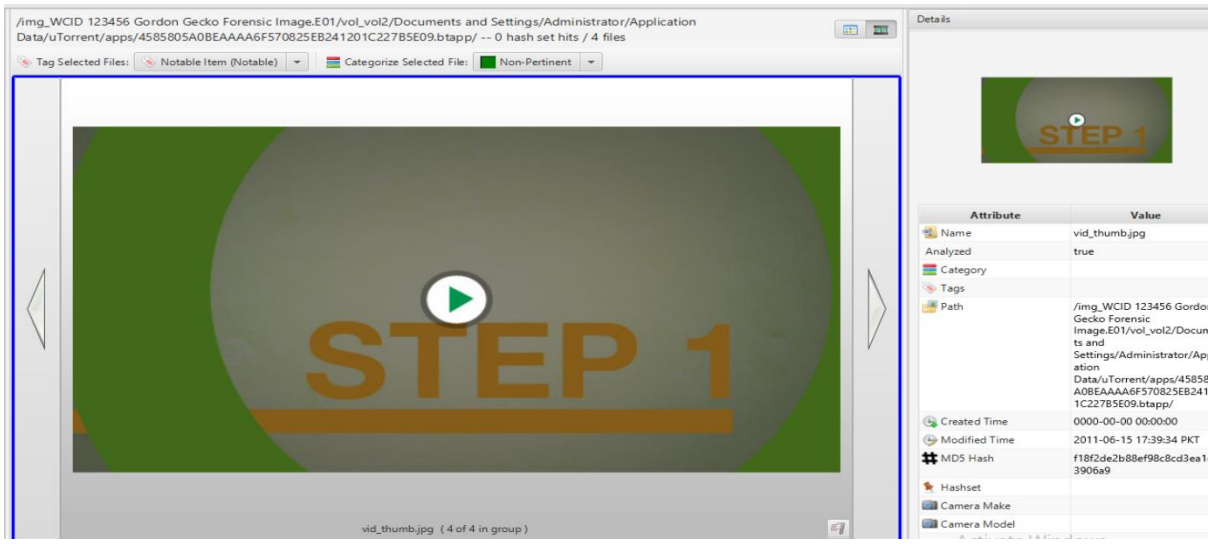

Figure: suspected deleted video

Investigative leads:

Bank Fraud Loss Details:

During the investigation, a detailed analysis of bank fraud loss data for a specific period was conducted. This analysis revealed key patterns and insights into the financial losses incurred due to fraudulent activities. By examining the timeline, amounts, and affected accounts, we can identify potential links to the criminal activities under investigation. This information helps in tracing the financial impact of the fraud, understanding the scale of the attack, and correlating it with other evidence collected. Further scrutiny of these details could provide crucial leads on the perpetrators' methods, targets, and potential accomplices, aiding in the comprehensive resolution of the case.

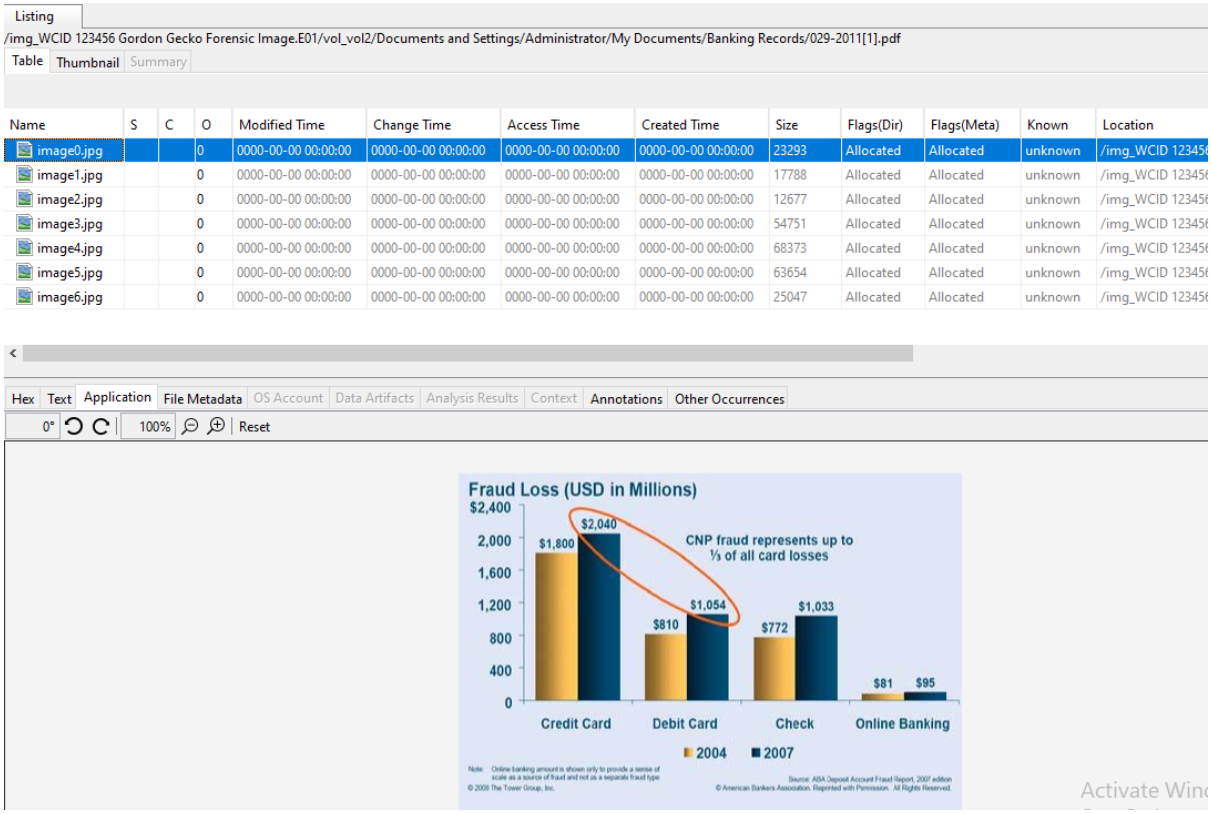

Figure: Bank fraud loss

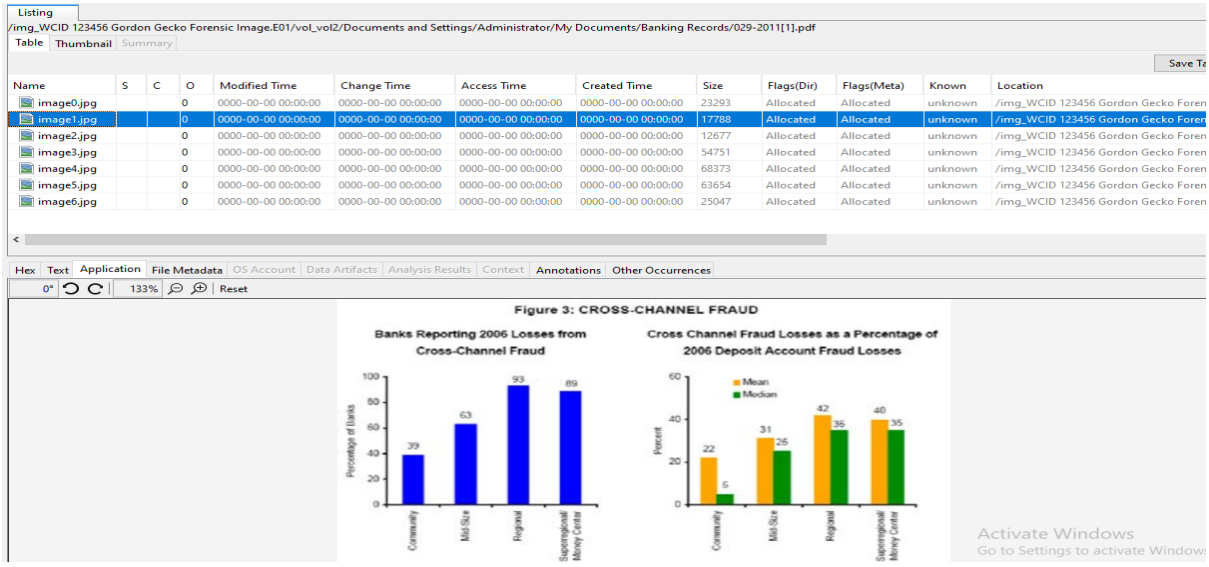

Figure: cross channel fraud

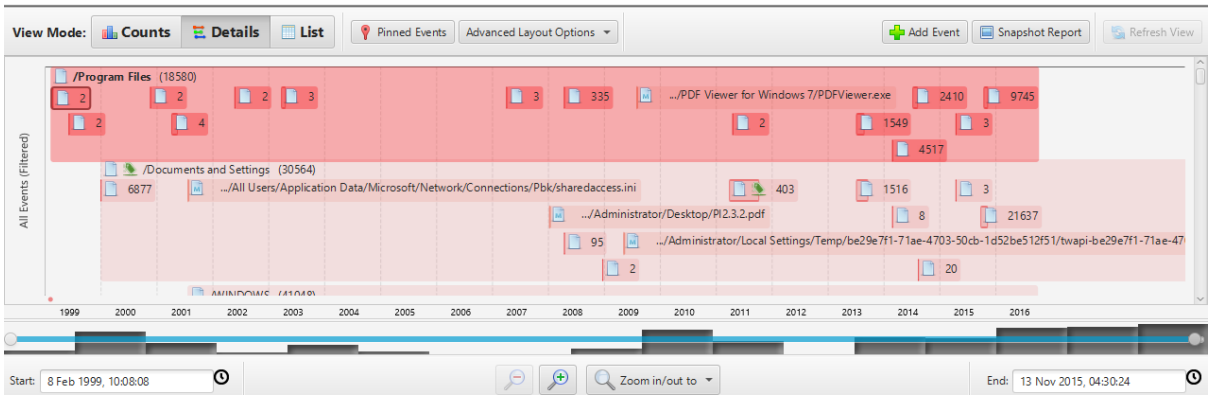

Figure: forensic activity details

In the provided image, a series of malicious activities are documented, complete with all pertinent properties and specific numerical identifiers. These activities showcase various forms of cyber-attacks or illicit operations conducted by the perpetrator. The detailed properties associated with each activity, such as timestamps, involved systems, and activity types, offer critical insights into the attacker's methods and operational patterns. By analyzing this data, we can track the sequence of malicious actions, identify targeted systems, and correlate these activities with other evidence in the case. This information is essential for understanding the full scope of the cyber-attack and for developing strategies to prevent future incidents.

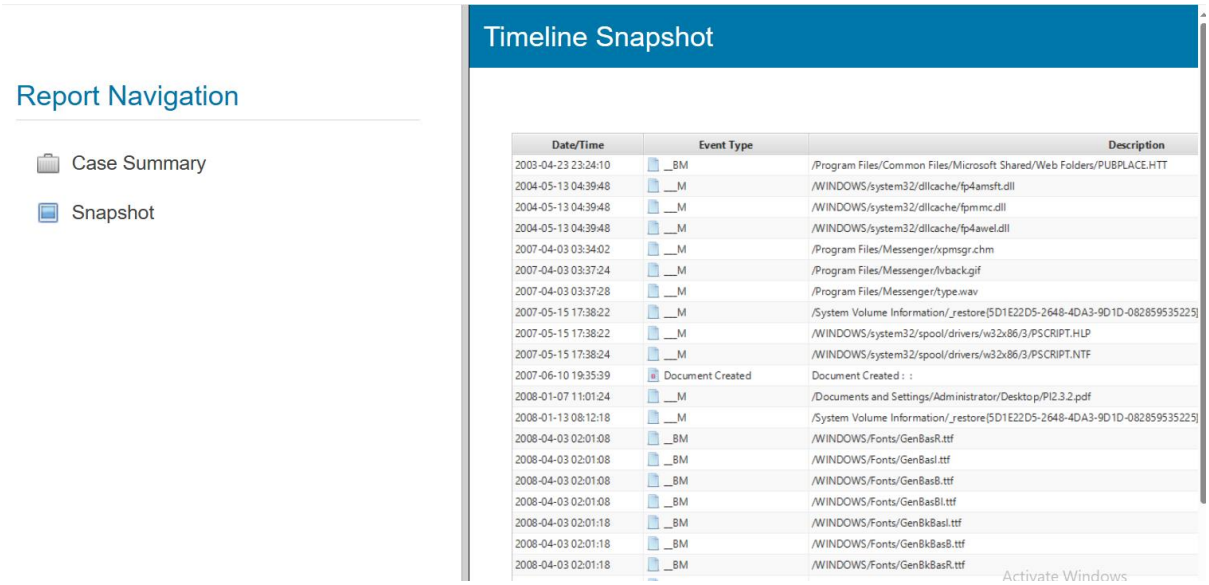

Figure: timeline details

Figure: case report details

During the forensic investigation, several risks are inherent that could inadvertently lead an organization towards vulnerabilities or an attacking platform. Firstly, incomplete or improper handling of sensitive data during the investigation can result in unintentional exposure of confidential information. Additionally, the use of compromised or outdated forensic tools may introduce new risks or fail to detect advanced threats. Mismanagement of evidence, such as failing to securely document or store digital artifacts, could also lead to evidence tampering or loss. Furthermore, inadequate understanding of the attacker's techniques or failing to keep up with evolving cyber threats may leave the organization unprotected against similar future attacks. Ensuring rigorous protocols, continuous updates of forensic tools, and comprehensive risk management strategies are crucial to mitigate these risks and safeguard the organization throughout the investigation process.

Cyber security risk details:

Cybersecurity risks often involve attackers seeking unauthorized access to systems to achieve specific malicious objectives. For instance, an attacker might aim to access sensitive information or critical systems to exploit them for various purposes. One common risk is data exfiltration, where attackers steal confidential data for use in extortion or other forms of exploitation. Another risk involves attackers implanting malware or backdoors to maintain persistent access and control over compromised systems. These attacks can lead to severe consequences, such as financial losses, reputational damage, and disruption of operations. To mitigate these risks, organizations must implement robust security measures, including strong access controls, continuous monitoring, and prompt incident response strategies. Awareness and proactive measures are essential in protecting against the evolving landscape of cyber threats.

Compliance based risk:

Compliance-based risks occur when an organization's use of technology deviates from established security controls and standards, potentially leading to significant vulnerabilities. In a standard technological environment, this can happen when technological solutions or practices fail to adhere to regulatory requirements or industry standards, exposing the organization to legal and financial repercussions. For example, non-compliance with data protection regulations like GDPR or HIPAA can result in penalties and reputational damage if sensitive data is mishandled. Similarly, inadequate implementation of security controls, such as failing to encrypt sensitive data or not enforcing proper access controls, can undermine the organization's ability to safeguard information. These compliance-based risks highlight the importance of integrating robust security practices with regulatory requirements to ensure that technology use aligns with both legal and industry standards, thereby minimizing potential threats and enhancing overall security posture.

Third party-based risks:

Outsourcing to third-party vendors or service providers introduces several risks for banks, primarily concerning network vulnerabilities, proprietary data, financial customer information, and other sensitive data. Banks often handle highly sensitive customer information, and delegating tasks or functions to external parties can expose this data to potential breaches or misuse. One significant risk is that external vendors may not adhere to the same stringent security protocols as the bank, leading to vulnerabilities that could be exploited by cybercriminals. Additionally, since third parties may have access to critical data, there is a risk that they could inadvertently or maliciously alter or compromise this information, affecting the bank's performance and customer satisfaction. It is crucial for banks to carefully manage these relationships by avoiding the assignment of sensitive information to third parties unless absolutely necessary. Strong due diligence and robust security measures must be in place to mitigate these risks. Establishing clear roles and responsibilities for all employees, including those hired newly, and ensuring comprehensive decision-making protocols can help minimize these risks and maintain data integrity. By implementing stringent oversight and maintaining tight control over sensitive information, banks can safeguard their operations and protect customer trust.

Concluding Statement:

After working in current assessment working as forensic analysis solving of any criminal case has become easy now. In this bank more complex, interconnected supply chains with customers, partners and software vendors are involved also exposes the digital assets to attack. Therefore, organization also need to deploy standard level secure computing environment to produce safe and secure working platform for the end users. Therefore, in my opinion every organization should spend heavy budget for the security of networking environment because it is necessary to produce positive results. A company like financial organization should hire network security officer the person should have strong level knowledge about cyber security because in case of any attacking activity such person can response quickly against any illegal activities. The digital forensic report on current case provides the complete details about the crime objectives in results investigation process completed by supporting legal actions and professional level decision making with all type of stakeholders.

There are multiple challenges are occurred during forensic process in today computing environment filled with high ratio of malicious items so financial organization should move towards cloud computing environment because cloud service provider organizations contain multi layers of authentication. In cloud-based banking like internet banking chances of cyber-attack is low because multi factor authentication is involved. For example, in current method end user easily can access the account from any location where specific number of OTP generated for user level account authentication after success of verification user can access the bank services easily. This is the simple and powerful techniques for the data protections.

References:

[1] M. Orta, Bilişim Suçlarında Adli Analiz, Konya: Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Doktora Tezi, 2015.

[2] M. D. Kohn, M. Eloff and J. Eloff, "İntegrated Digital Forensic Process Model," Computers&Security, cilt 38, pp. 103-115, 2013.

[3] A. S. Şirikçi and N. Cantürk, "Adli Bilişim İncelemelerinde Birebir Kopya Alınmasının (İmaj Almak) Önemi," Bilişim Teknolojileri Dergisi, cilt 5, no. 3, pp. 29-34, 2012.

[4] D. Quick and K.-K. R. Choo, "Dropbox Analysis: Data Remnants on User Machines," Digital Investigation 10, pp. 3-18, 2013.

[5] M. Z. Gündüz, Bilişim suçlarına yönelik IP tabanlı delil tespiti- IP-based evidence detection, Elazığ: Fırat Üniversitesi Fen Bilimleri Enstitüsü Yüksek Lisans Tezi, 2013.

[6] E. Şahin, "Sayısal Delilin Ortaya Çıkarılması Kapsamında Koruma Tedbirleri," İnternational Journal of Legal Progress, cilt 1, no. 2, pp. 88 106, 2015.

[7] A. Emekçi and E. Kuğu, "Adli Bilişim ve Etmen Tabanlı Sistemler," İstanbul/Türkiye, 2014.

[8] S. Mascarnes, P. Lopes and P. Sakhare, "Search Model for Searching the Evidence in Digital Forensic Analysis," Green Computing and Internet of Things (ICGCIoT), 2015 International Conference, pp. 1353-1358, 2015.

[9] M. Al Fahdi, N. Clarke, F. Lİ and S. M. Furnell, "A Suspect-Oriented Intelligent and Automated Computer," Digital Investigation, pp. 65-76, 2016.

[10] J. Wang and Z. Xu, “Bayesian Inferential Reasoning Model for Crime Investigation,” China, 2014.