Usability of Cloud-Based Applications in Digital Forensics: An Experimental Study on Image Acquisition and Digital Evidence Preservation Processes

Zöhre Serttaş[1], Fadi Al-Turjman[2]

[1] *Artificial Intelligence and Informatics Faculty, Research Center for AI and IoT, Near East University, Nicosia, Mersin 10 /Turkey* zohre.serttas@neu.edu.tr

[2] *Artificial Intelligence and Informatics Faculty, Research Center for AI and IoT, Near East University, Nicosia, Mersin 10 /Turkey* fadi.alturjman@neu.edu.tr

ABSTRACT

While cloud computing's dynamic structure brings significant conveniences and access to information from anywhere in our professional and personal lives, this same dynamic structure also provides certain advantages in the field of digital forensics. Cloud forensics differs from traditional digital forensics in some physical and technical aspects. The physical and technical differences of cloud services have introduced new dimensions to the legal field, particularly concerning the concept of electronic evidence, its collection, ensuring its admissibility in court, and conducting these processes through scientific methods. As part of the study, the image acquisition process, which constitutes the first response to digital evidence, was performed by creating physical copies from external storage devices. Access to data stored in the cloud can be obtained by activating mutual legal assistance agreements, collecting user information with consent, and utilizing indicators and user information gathered during electronic evidence examinations. For testing purposes, a user account was created through Gmail's online drive, and certain user activities were conducted to enable data uploads to the accounts. To conduct examinations, a physical image of a Kingston DataTraveler G4 USB Device flash drive was obtained using the AccessData FTK Imager software.The purpose of this study is to create a preservation model that experts using cloud computing storage services, as a developing subfield of digital forensics, should follow during the image acquisition process the first response to digital evidence and its preservation during the analysis process. The digital evidence image acquisition processes within cloud storage services are presented as examples.

Keywords: Digital Forensics, Cloud Computing, Digital Evidence, Image Acquisition

1. INTRODUCTION

When interpreted as defined or understood today, digital forensics can be described as the field of study that analyzes evidence of crimes by processing numerical and logical data obtained from electronic environments, revealing the connections of crimes and examining evidence (Önel & Irmak, 2021). All processes in digital forensics share interconnected and similar characteristics. The occurrence of crimes involving electronic devices and environments has led to various types of digital forensics due to suspects' attempts to destroy evidence (Barbaros, 2016). These include:

- Static Data Forensics (Disk Forensics)

- Live Forensics

- Network Forensics

- Mobile Device Forensics

- Computer Forensics

- Database and Log Forensics

To establish a foundation for digital forensics applications in electronic environments, ISO 27037 standards outline the steps of identifying, collecting, and preserving evidence in the digital forensics process. In addition, analyzing, interpreting, and reporting evidence have also become essential components of this process, forming its core structure (Özkaya, 2021).

The general aim of our study involves integrating cloud computing technologies into digital forensics, embodying the philosophy of a new field known as cloud forensics. Due to its architectural structure, consisting of networks and devices connected to these networks, cloud forensics is considered a subfield of network forensics (Oğuz & Eryiğit, 2024). The integration of cloud forensics into network forensics, considering the advancements in data storage capabilities within cloud systems, leads to the belief that evidence obtained from cloud environments can be effectively preserved through virtualization technologies and service provider features such as log reporting (Kılıç, 2016). Additionally, these processes facilitate the use of data forensics. Accordingly, cloud storage capabilities provide significant convenience in preserving data related to crime evidence.

1.2. LEGAL ASPECT OF CLOUD COMPUTING

The preservation of digital evidence image files in cloud computing systems differs from the rules applied in physical systems. In our country, the legal basis for digital forensics is primarily governed by Articles 134 of the Criminal Procedure Code (CMK). According to CMK 134, data acquisition in digital forensics must be performed physically (Kara, 2019; Keskin, 2021). This makes evidence collection and image acquisition in cloud-based forensic cases more challenging compared to physical structures. However, since the resolution process will still involve physical analysis, storing image files is not expected to pose a security issue.The use of cloud systems’ network structures, data virtualization, and encryption of storage locations may enhance the security of image file preservation.

Defining the legal rules applicable to cloud forensics depends on the development scale of digital forensics in the respective country. Since digital forensics is still an emerging field, ongoing studies continue to shape its legal framework. While setting these rules, countries must also consider their "Personal Data Protection Law" provisions (Henkoğlu & Külcü, 2013). In this context, taking into account personal data protection regulations, storing digital evidence image files in cloud systems while conducting physical analyses can provide significant convenience.

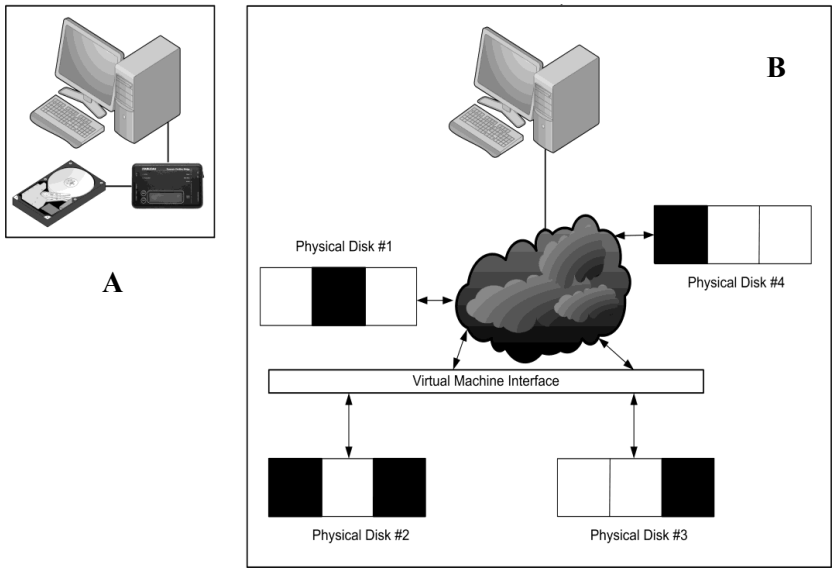

Figure 1: (A) Traditional One-to-One Copying (B) Copying in a Cloud Environment (Grispos, Storer ve Glisson, 2012).

In Section A of Figure 1, the process of traditional image acquisition involves copying data in a physical structure and transferring it to an external physical storage device. In Section B, the process illustrates transferring image files obtained in a physical environment to a cloud system, indicating an interactive process between systems. In cloud computing, there is also the possibility of re-transferring data back to a physical environment. Based on these processes, the primary objective of our study is to conduct a test on image acquisition of digital evidence and its preservation in cloud computing environments. Data security measures, including encryption fields, are integral to the evidence preservation process. All procedural steps involved in the test study are explained in detail in the second section of our study.

2. FIRST RESPONSE TO DIGITAL EVIDENCE: IMAGE ACQUISITION PROCESSES

The image acquisition processes were carried out using the AccessData FTK Imager software. The physical specifications of the imaged device are listed in Table 1. This section also provides a detailed explanation of the image acquisition process steps.

Table 1. Specifications of the Imaged Device

Device Information	Kingston DataTraveler G3 USB Device
Memory Capacity	4 GB

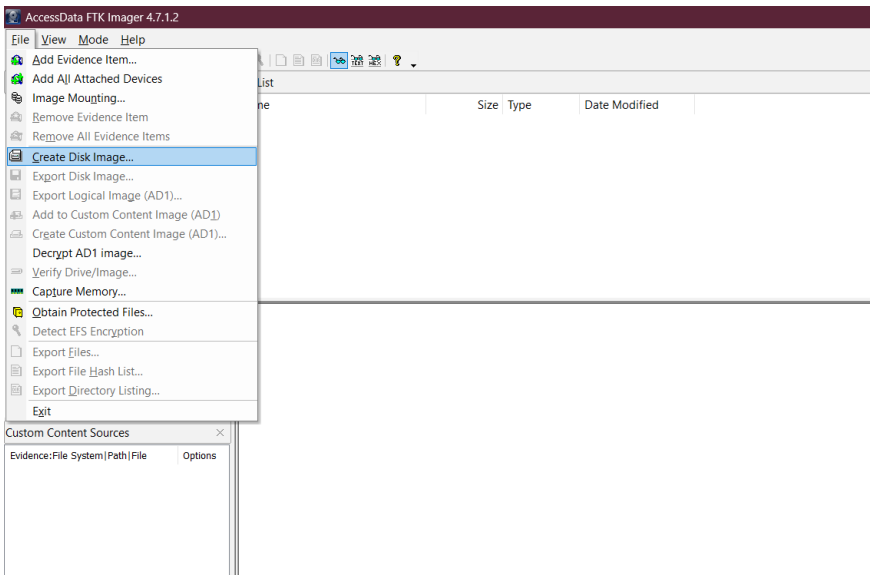

Figure2. AccessData FTK Imager application

Figure 2 shows the first part of the image acquisition process. In the AccessData FTK Imager program, the "create disk image" section is first selected for the image acquisition process.

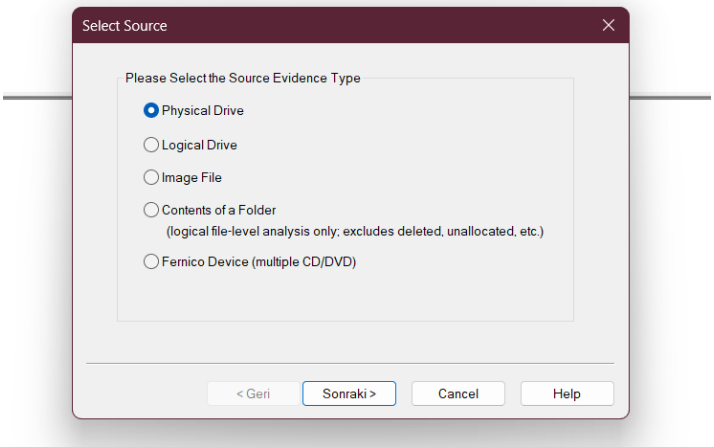

Figure3. Choosing to take images with the AccessData FTK Imager application

Figure 3 shows information on how to obtain digital evidence. In this section, it is stated that the image will be taken in physical form.

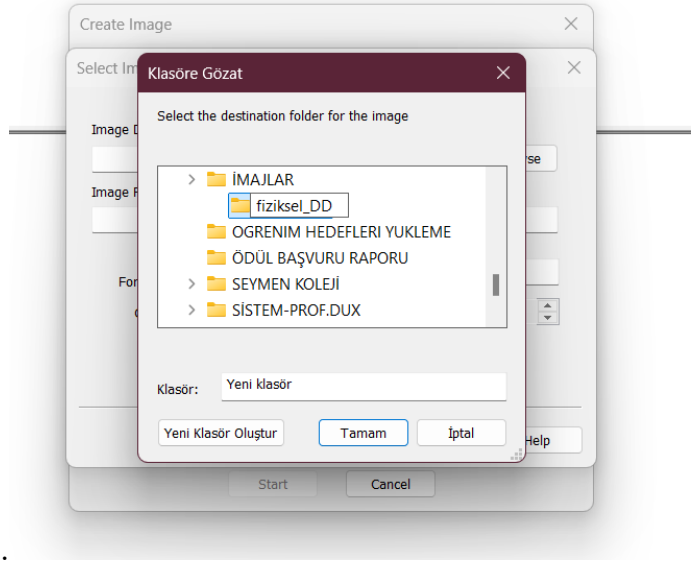

Figure4. Choosing to take images with the AccessData FTK Imager application

A section on which file the image file planned to be physically imported will be transferred to on the computer has been created.

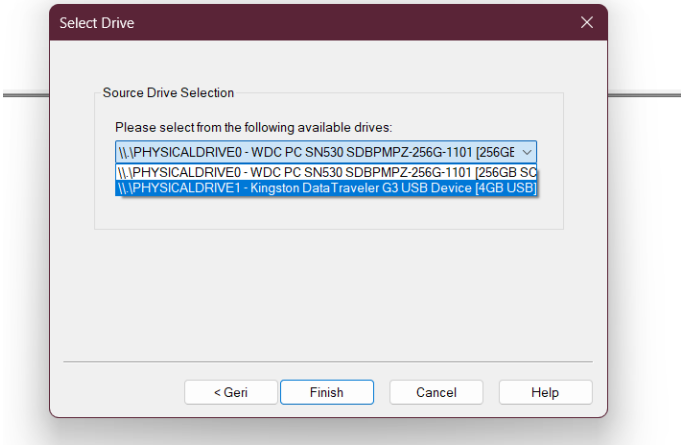

Figure5. Choosing to take images with the AccessData FTK Imager application

This section contains the section on which device the image will be taken. The options include the physical space of the computer and the information of the USB memory. Since the device to be imaged is a USB memory, the process continued by selecting the USB memory information.

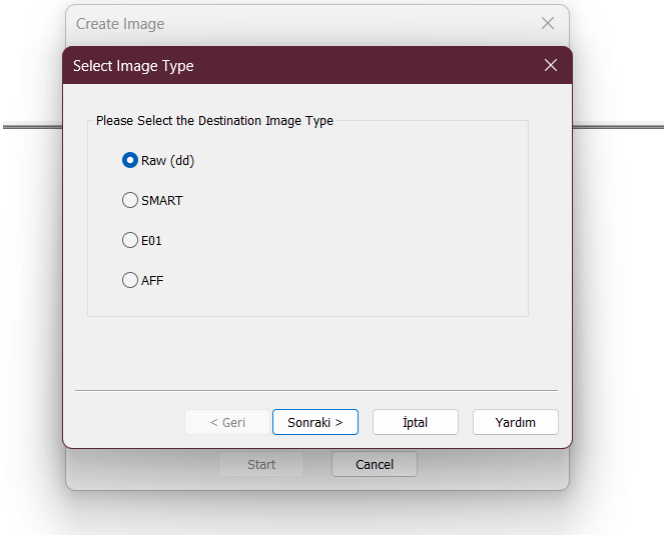

Figure6. Choosing to take images with the AccessData FTK Imager application

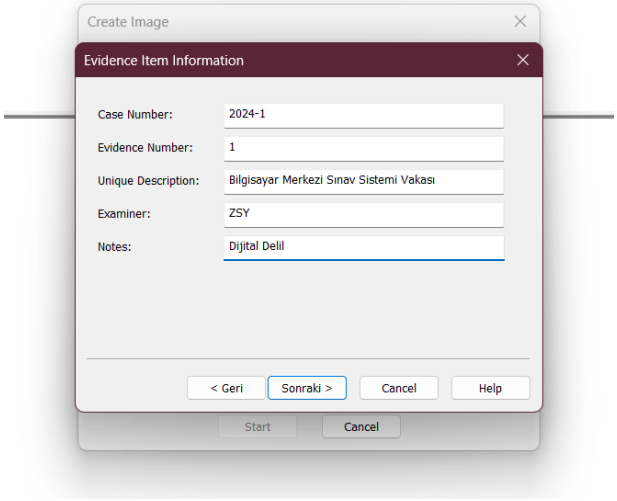

Figure7. Image acquisition and explanations with the AccessData FTK Imager application

In this section, the processing of digital evidence is explained. The reason for doing this is that it is important to include in the reports why and by whom the image was taken. After this information is entered, the image acquisition process begins.

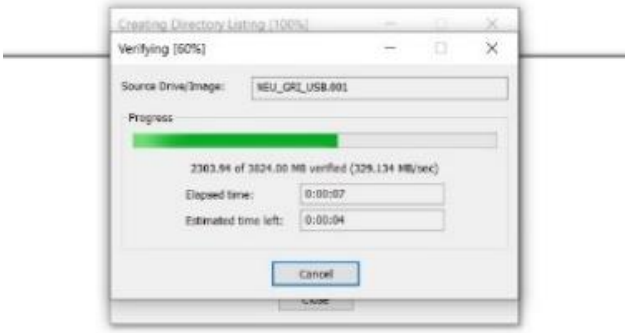

Figure8. Verification step of the image acquisition process with the AccessData FTK Imager application

The received image process is verified. This verification is called “Verifiying process”. After the verification process is completed, the hash information of the received image file is revealed.

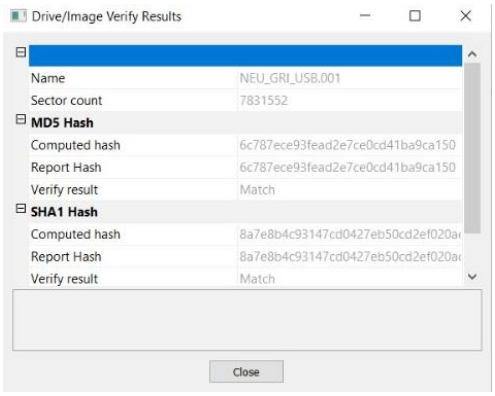

Figure9. HASH values of image files received from AccessData FTK Imager application

In this section, the image file is ready and the Hash values (MD5 and SHA1) are created.

2.1. Cloud Service Used in the Test Study: Gmail Drive Online

Gmail Drive is a file storage and synchronization service created and managed by Google. This service allows users to store documents in the cloud, share files, and edit documents collaboratively with others (Microsoft).

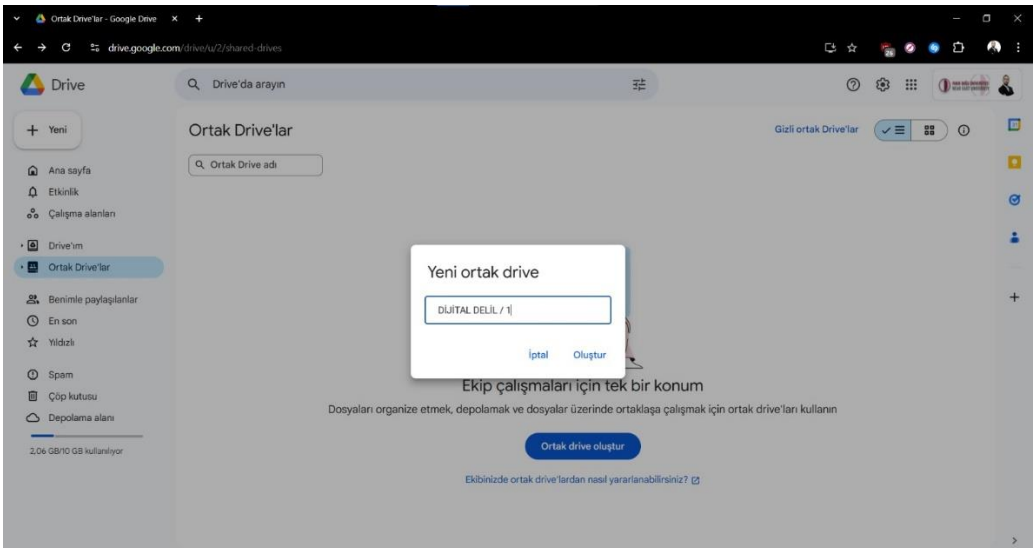

Figure9. Creating the Google Online Drive Storage Folder

In this section, a folder has been created in Google Online Drive to store the image file of the acquired digital evidence. The folder is named “Digital Evidence /1.”

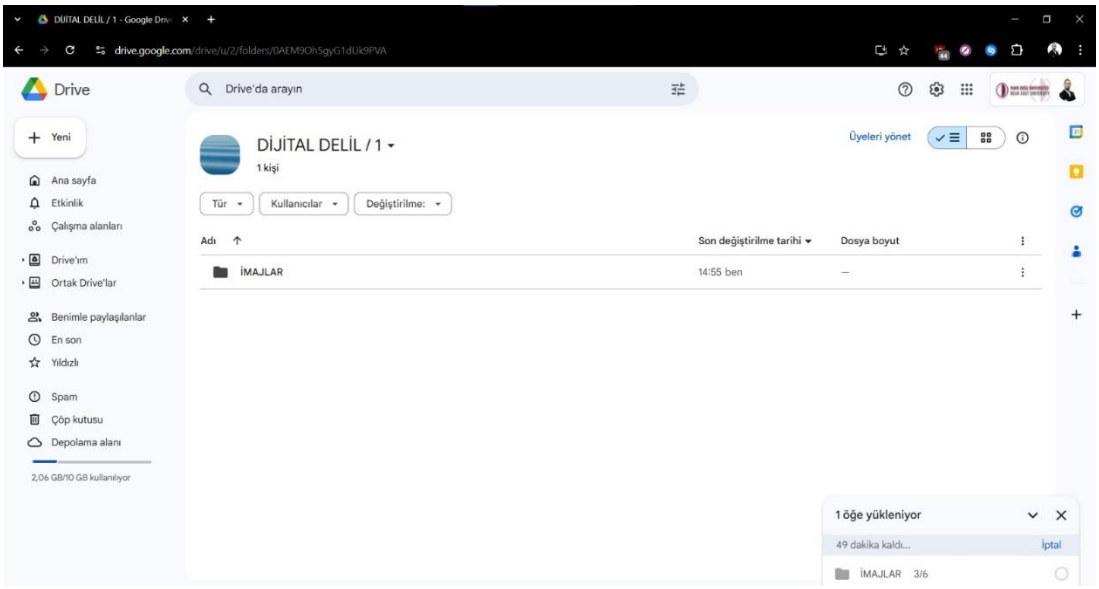

Figure10. Transferring the Image File to the Google Online Drive Storage Folder

The image file located in the physical environment is transferred to the Google Online Drive area.

Figure11. Transferring the Image File to the Google Online Drive Storage Folder

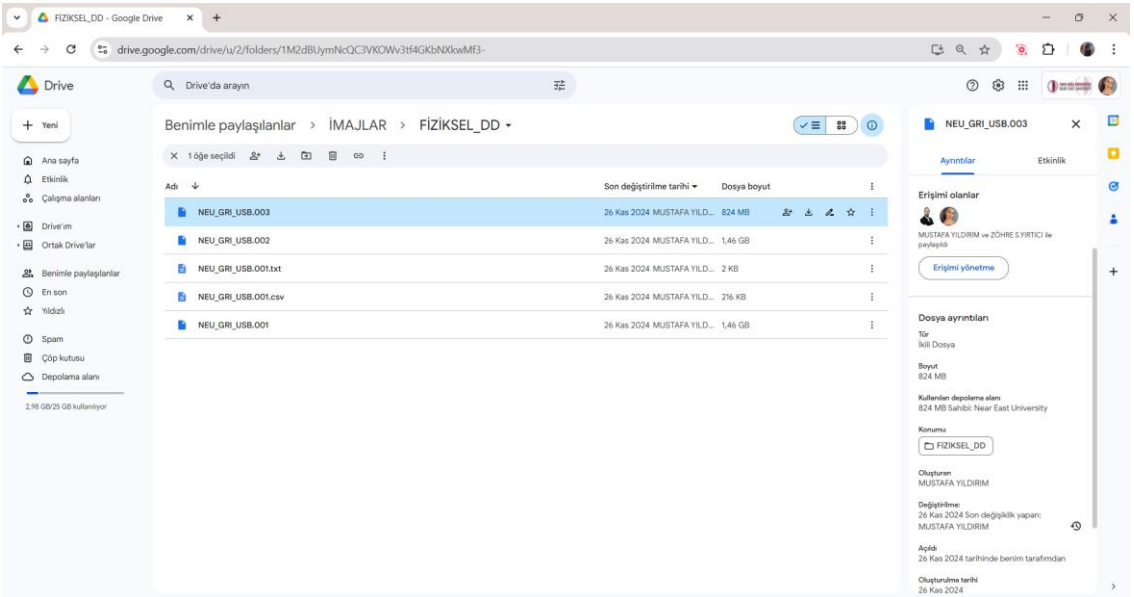

Figure12. Transferring the Image File to the Google Online Drive Storage Folder

The details of the transferred image files are stored in the cloud system. This information includes an explanation section that answers questions such as who transferred the file, what actions were performed, and whether any changes were made to the file. The importance of this section lies in the fact that any modification to the image file would render it invalid. Therefore,

including these explanations is crucial for the security of storing the image file. It is believed that this will enhance trust in the use of cloud-based digital forensics.

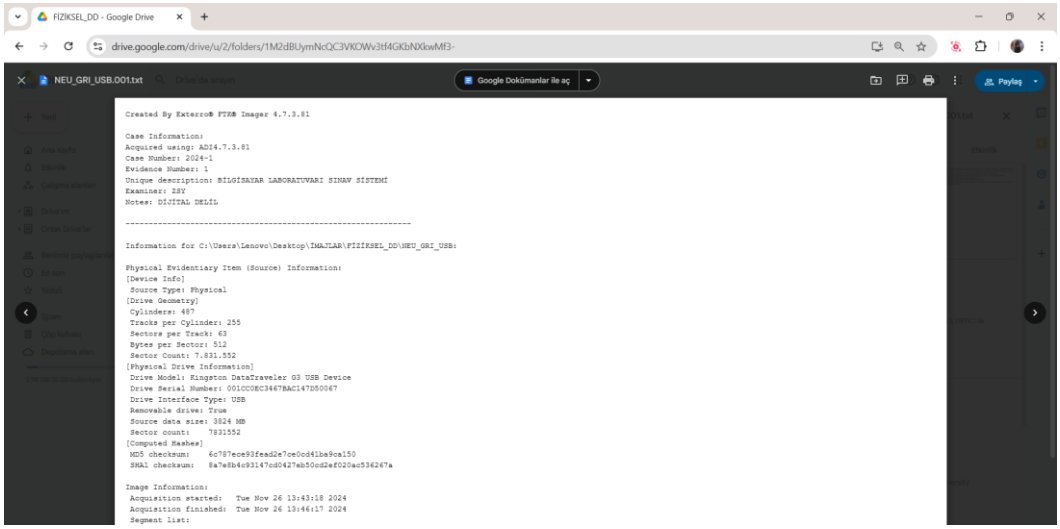

Figure 13. Process Report of the Image File in the Google Online Drive Storage Folder

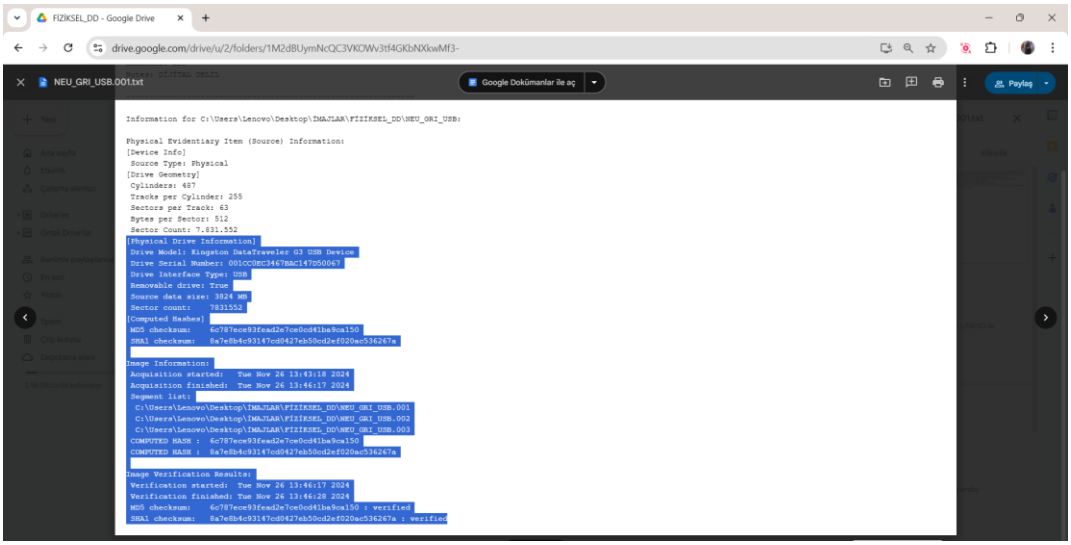

Figure14. Process Report of the Image File in the Google Online Drive Storage Folder

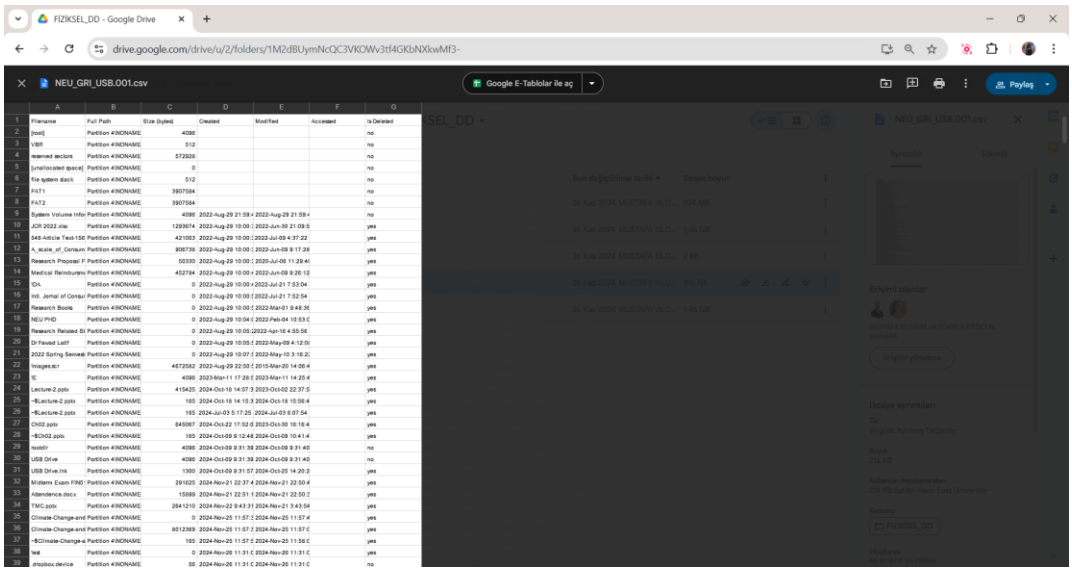

Figure15. Content File of the Image in the Google Online Drive Storage Folder

Images 13 and 14 depict the process of viewing the image file in the cloud system. These areas include information about who acquired the image, for what purpose, and the HASH values. Figure 15, on the other hand, provides details about the data stored on the USB device from which the image was acquired, including the dates when the data was transferred to the device. Additionally, there are sections containing information about deleted files on the device. This information can only be viewed in the cloud computing environment, and no data editing operations are performed on the file. It should also be noted that any intervention or modification to a file will render the image file invalid in the cloud computing environment, just as it would in a physical environment.

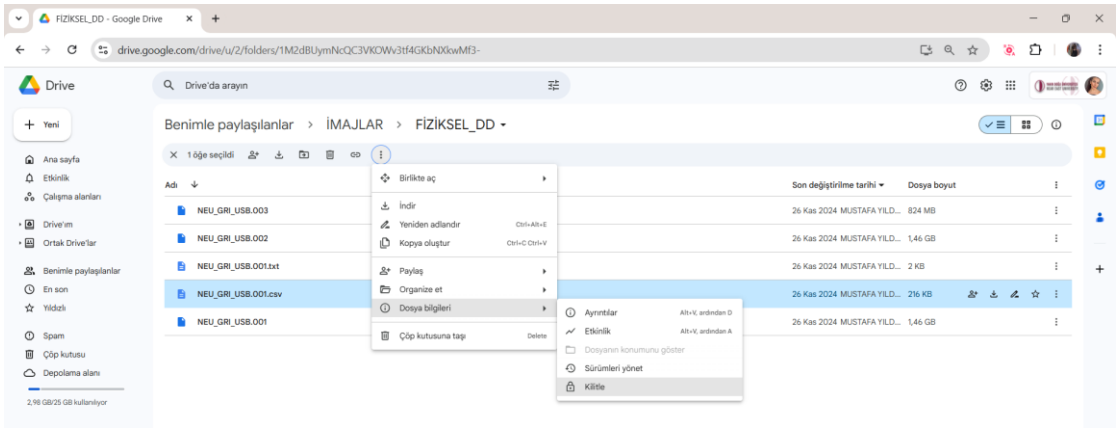

Figure16. Adding an Encryption Feature to the Image File in the Google Online Drive Storage Folder

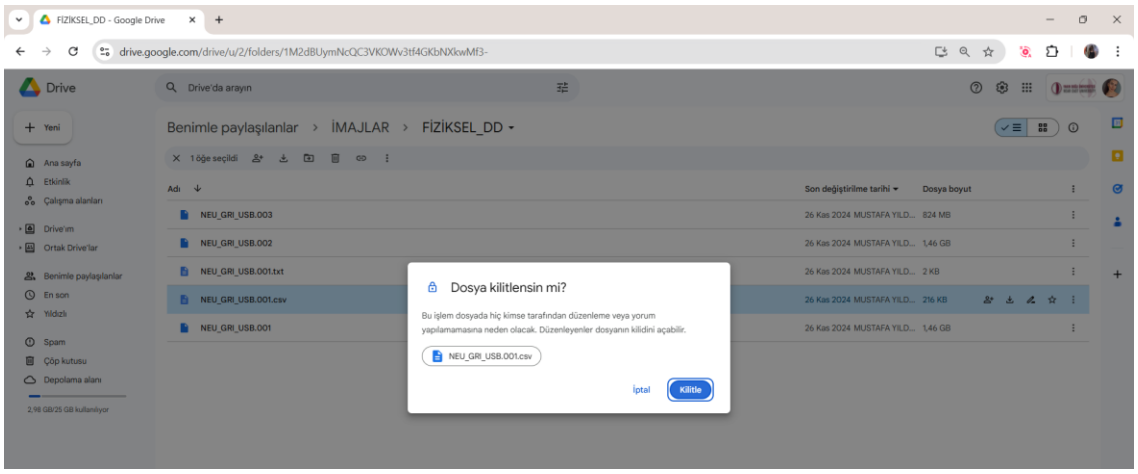

Figure17. Adding an Encryption Feature to the Image File in the Google Online Drive Storage Folder

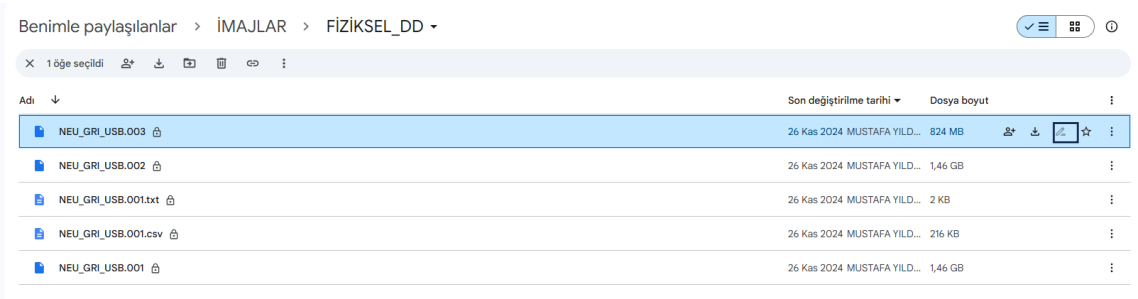

Figure18. Adding an Encryption Feature to the Image File in the Google Online Drive Storage Folder

In figure16, 17, and 18, a locking feature has been added to prevent interventions in the image files. With this feature, each file is individually locked, preventing any modifications to the file. This increases security by ensuring that encryption and file-locking sections are in place to prevent unauthorized interventions in the cloud computing environment.

CONCLUSION AND DISCUSSION

In traditional forensic computing practices, methods developed for handling electronic evidence have been accepted in courts, and the accuracy of this information can be validated through repeatable tests/experiments. Barbaros (2016) stated in his study that when accessing cloud storage systems via remote connections to obtain images of evidence, it is not possible to determine whether the data has been tampered with or shared with another user. However, in the test processes covered in our study, we can report that all such situations can be documented. All steps related to the digital evidence are included in the Google Online Drive report, making it possible to access information on any sharing or tampering. This is explained in detail in the second part of our study.

When examining studies conducted in Turkey regarding cloud computing and forensic computing, no specific research has been found on preserving the images of digital evidence obtained through forensic processes. A comprehensive literature review revealed that Oktay (2013) conducted a thesis on *"cyberattacks targeting cloud systems,"* and Sevli and Küçüksille addressed *"problems encountered in cloud forensic computing and applicable methods."*

Additionally, Emekçi, Kuğu, and Temiztürk's 2016 study titled *"A Dimension Disrupting Forensic Computing Norms: Cloud Computing"* and Ateş's (2020) study on *"Forensic Computing, Digital Evidence, and Cybercrime Concepts"* were identified. From a forensic computing perspective, Henkoğlu's 2020 study titled *"Forensic Computing: Acquisition and Analysis of Digital Evidence"* aligns with the content of our work. Our study, however, is the first cloud forensic computing study conducted in the Turkish Republic of Northern Cyprus (TRNC).

On an international level, Chung et al. (2012) examined four different cloud computing storage applications: Amazon S3, Google Docs, Dropbox, and Evernote. Quick and Choo also studied the Dropbox and Skydrive cloud storage applications. The cloud computing application examined in our study is Google Online Drive. Similar to other researchers, we analyzed log records of stored data, folder structures, user information, as well as the structure of uploaded and shared files, and signature report formats.

In conclusion, our study conducted a test on the preservation of images obtained through forensic computing in cloud computing applications. This test demonstrates that cloud forensic computing, an emerging field, was utilized. The results confirm that there is no security vulnerability in storing image files obtained from digital evidence on Google Online Drive for further examination in physical environments. Of course, any tampering with the image would render the file invalid, just as in physical environments. However, documenting all log records could assist in applying legal sanctions in cases of file tampering.Finally, this study is expected to assist forensic computing specialists and researchers examining cloud computing, one of the newest topics in forensic computing, where storage methods are continually being developed. In future studies, tests can be conducted using other cloud computing applications such as Amazon, Dropbox, and Azure to ensure the validity and security of cloud digital forensics and to promote its widespread adoption.

REFERENCE

- Ateş, E. C. (2020). Examination of the Concepts of Digital Forensics, Digital Evidence, and Cybercrimes. 4th International Student Symposium of Future Engineers, 7-8.

- Barbaros, İ. Examination of Computers Using Cloud Storage Applications from a Digital Forensics Perspective.

- Chung, H., Park, J., Lee, S., Kang, C. (2012). Digital Forensic Investigation of Cloud Storage Services. *Digital Investigation,* Vol. 9, 81–95, 2012 Elsevier Ltd. DOI: http://dx.doi.org/10.1016/j.diin.2012.05.015

- Grispos, G., Storer, T., Glisson, W.B. (2012). Calm Before the Storm: The Challenges of Cloud Computing in Digital Forensics. *International Journal of Digital Crime and Forensics,* Volume 4, Issue 2, pp. 28-48.

- Hale, J.S. (2013). Amazon Cloud Drive Forensic Analysis. *Digital Investigation,* Elsevier Ltd., pp. 259-265. DOI: http://dx.doi.org/10.1016/j.diin.2013.04.006

- Henkoğlu, T. (2020). Digital Forensics: Acquisition and Analysis of Digital Evidence. Pusula.

- Kara, İ. (2019). Examination and Legal Dimension of Digital Evidence. *Journal of Yüzüncü Yıl University Institute of Science,* 24(3), 183-188.

- Keskin, S. (2021). Problems Encountered in the Implementation of Provisions in Article 134 of the Criminal Procedure Code in Cybercrimes. *Journal of Kırıkkale University Social Sciences,* 11(2), 649-667.

- Kılıç, A. F. Protection of Privacy and Security in Cloud Computing: Computational Defense and Legal Framework Dimensions.

- Oğuz, R., & Eryiğit, R. (2024). New Digital Forensics Examination Process (YABIS). *Journal of Fırat University Engineering Sciences,* 36(2), 717-724.

- Oktay, U. (2013). Proxy Network Intrusion Detection System in Cloud Computing. Master's Thesis, Air Force Academy, Institute of Aviation and Space Technologies, Istanbul.

- Quick, D., Choo, K.K.R. (2013b). Dropbox Analysis: Data Remnants on User Machines. *Digital Investigation,* Elsevier Ltd., pp. 3-18. DOI: http://dx.doi.org/10.1016/j.diin.2013.02.003

- Önel, B., & Irmak, E. (2021). Digital Forensics and Examination of Digital Evidence on the Windows Operating System. *Journal of Polytechnic,* 24(3), 1187-1196.

- Özkaya, P. (2021). Standardization, Certification, Accreditation, and Best Practices in Digital Forensics. Master's Thesis, Ankara University, Turkey.