Fusion of Forensic Analysis of Mobile Devices: Integrating Multi-Criteria Decision Methods and Case Study Insights

Jorge B. Rubio Peñaherrera*[,1], Kevin Mauricio T. Diaz[1], Adam Marks[2]

[1]Technical University of Cotopaxi, Cotopaxi, Ecuador
[2]University of Sharjah, Sharjah, UAE

Email : jorgerubio@utc.edu.ec; kevin.tipanta4612@utc.edu.ec; Amarks@sharjah.ac.ae

Abstract

This study employed a Multi-Criteria Decision Analysis (MCDM) approach, utilizing the DEMATEL and TOPSIS methodologies, to assess the effectiveness of forensic tools designed for mobile devices, with a specific emphasis on Android and iOS platforms. The investigation evaluated technologies used for collecting, retrieving, and validating data in the Cyber Forensic Field Triage paradigm, with a focus on rapidly identifying and interpreting digital evidence. The study incorporated several factors and expert preferences, concluding that the Android Triage and Andriller tools were the most efficient.

Keywords: Forensic Analysis; Mobile Devices; Multi-Criteria Decision Analysis; DEMATEL; TOPSIS.

1. Introduction

Mobile devices are being used more and more by the workforce as powerful platforms for accessing large amounts of information. Mobile devices are constantly being upgraded with new technological improvements with each new generation [1]. These gadgets are always evolving, offering consumers increased storage capacity for activities such as text messaging, multimedia playback, instant chat, email, and internet browsing. These gadgets gather substantial data about their owner and the activities they engage in over a period [2]. Although mobile gadgets can enhance convenience in our lives, they also pose a heightened risk by providing additional capabilities for engaging in illicit actions. This research demonstrates how computer professionals may securely acquire information, examine evidence, and provide reports using an advanced forensic methodology [3].

Although there is no single, universal methodology in forensic analysis, with the existing documentation and taking into consideration the legal regulations and international standards currently in place, it can be said that there are a series of phases or important points that must be considered for forensic analysis to be adequate and serve as evidentiary support in the event of an incident, rights violation, and flagrant case [1]. Figure 1 shows the structure of the General Forensic Methodology.

Phases of the General Forensic Methodology [4]:

- ✓ **Acquisition:** Obtain copies of the suspicious information that must be relevant to the incident. In this way, data modification of any kind can be avoided by always copying one-to-one with the appropriate tools and equipment. The use of gloves, anti-static bags, and Faraday cages is recommended (to place devices that can interact with electromagnetic waves such as cell phones).
- ✓ **Preservation:** It must be ensured that the collected information will not be destroyed or altered. In other words, no analysis should be performed on a confiscated sample; it should

Doi: https://doi.org/10.54216/FPA.160203
Received: July 06, 2023 Revised: November 15, 2023 Accepted: May 26, 2024

be copied, and the expertise carried out on that copy. The concept of chain of custody is recommended (except for using the Triage model), minutes in which the place, date, analyst, and other actors who handled the sample are recorded; using hashing techniques; it is not valid to freeze neither date nor time; video of everything that is done.

- ✓ **Analysis:** The analysis can be said to be the most complicated part of the process because it is a purely technical phase, using hardware and software specifically designed for forensic analysis. Some metrics and methods help to build the fieldwork, but there can be many variations depending on the tools used and the skill and experience of the analyst. The tools recommended are Autopsy, FTK, and Win–X.
- ✓ **Documentation:** All actions must be recorded as they occur. We must cite and attach all obtained information and establish a logical relationship between the evidence obtained and the tasks performed, ensuring the admissibility of the investigation.
- ✓ **Presentation:** An executive report must be presented that shows the most important features in a summarized and weighted manner in the investigation without going into technical details.

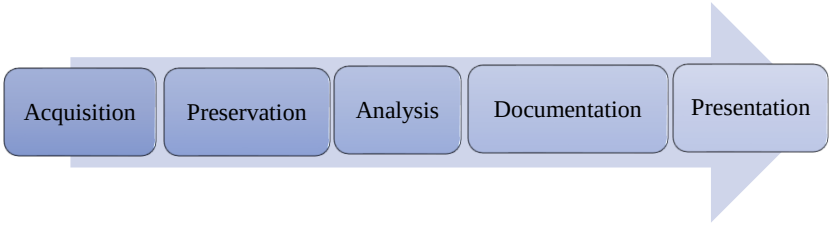

Figure 1: Structure of the General Forensic Methodology

2. The Computer Forensics Field Triage Process Model (CFFTPM)

This model is used in investigations that require immediate results because it involves analyzing data at the scene of the incident, which prevents a detailed analysis from being carried out. The application of this model will depend on the case to be analyzed using mobile device analysis tools. This model is very versatile because it adapts correctly to the tools used in the analysis of mobile devices [5].

Consequently, this methodology will allow:

- ✓ Analyze and collect evidence immediately.
- ✓ Identify victims at risk.
- ✓ Assess the offender's threat to affected individuals.

Phases of the model (CFFTPM):

Planning: In this initial stage, a quantification matrix of the elements of the event must be created to specify what is known and unknown. This matrix will contain the events, the offenders, and digital evidence.

Triage: This phase is fundamental to the process model, and together with planning, it forms the basis on which the other phases are built. It is characterized by highlighting the physical and digital evidence presented by users.

User Profile: With the combination of the previously named phases put into execution, the reconstruction of events is carried out, and a relationship with the victim of the digital evidence to be presented is established. This will lead to the filling out of an informed consent declaration where the user expresses their willingness and allows for the continued analysis of user profiles contained on the mobile device.

Startup Directory: In Microsoft Windows operating systems, the startup directory contains several folders such as documents, desktop, pictures, music, etc., for a specific user because each user has a structure of subdirectories and only the user who logs in will have access to the files.

Doi: https://doi.org/10.54216/FPA.160203
Received: July 06, 2023 Revised: November 15, 2023 Accepted: May 26, 2024

File Properties: These are very useful because they reveal information about the user who created them, meaning each file that is generated is saved with the data of the user who logged in and is not modified unless they have administrative rights.

Timeline: The chronological scope of the investigation can be defined by the intelligence case. In an investigation, digital evidence is defined by its MAC time without going into the narrative details of the MAC times specifically for each operating system, as follows:

- ✓ Modification when the content of a file is changed.
- ✓ Access time is defined by when a file was viewed.
- ✓ Creation time is defined by when a file was created.

Internet: Not in all cases, but a small part of mobile device analysis will require an examination of artifacts associated with Internet activity, such as instant messaging, email, and web browsing. The value, time cost, and time criticality will vary widely, depending on circumstances, including specific requests, and types of activity.

Browser: It is important to analyze the information contained in the browser, for example, cookies that show the Uniform Resource Locator (URL) of the visited site, which indicates the date and time of access. Also, evidence is found in the browser cache, where information such as images of visited pages is downloaded. The index.dat file also contains relevant information such as visited sites and web-based email.

Email: Emails can be of enormous evidentiary value but may require a costly investment in time. Procedures for examining emails and extracting useful data are usually specific to the particular email client.

Instant Messaging: Messaging applications generally save information on their servers, making direct access to the data difficult, which complicates the extraction of these data. In certain applications, information records are maintained that are analyzed by the investigator [6].

Through this chapter, relevant aspects of the General Forensic Methodology have been explored, which provide important data for the objective of the research. The goal is to compare the tools used in the Forensic Analysis of Mobile Devices. For the development of this goal, the following specific objectives are proposed:

a) Determine the tools to be evaluated.
b) Evaluate through a Multi-Criteria Decision Analysis the most feasible tools that provide better quality in the process. For this, the methods described in the following section will be applied.
c) Conduct a case study where the tool selected by experts is applied to demonstrate its reliability and validity.

3. Methods

DEMATEL: (Decision Making Trial and Evaluation) is a decision-making technique based on pairwise comparisons. The DEMATEL method can be used to identify the model of causal relations between the variables. It shows causal relations and the factors' exerted influences. The advantage of this method is that experts can be more fluent in expressing their opinions about the effects (direction and severity of effects) between factors [7, 8].

Steps of DEMATEL Method:

Step 1: Generate the direct relation matrix: To identify the model of the relations among the n criteria, an n × n matrix is first generated. The effect of the element in each row is exerted on the element of each column of this matrix. If multiple experts' opinions are used, all experts must complete the matrix. The arithmetic means of all of the experts ' opinions is used and then a direct relation matrix X is generated.

$$X = \begin{bmatrix} 0 & \cdots & x_{n1} \\ \vdots & \ddots & \vdots \\ x_{1n} & \cdots & 0 \end{bmatrix} \quad (1)$$

Doi: https://doi.org/10.54216/FPA.160203
Received: July 06, 2023 Revised: November 15, 2023 Accepted: May 26, 2024

To normalize, the sum of all rows and columns of the matrix is calculated directly. The largest number of the row and column sums can be represented by k. To normalize, each element of the direct-relation matrix must be divided by k.

$$k = max\left\{max\sum_{j=1}^{n} x_{ij}, \sum_{i=1}^{n} x_{ij}\right\} \quad (2)$$

$$N = \frac{1}{k} * X \quad (3)$$

Step 3: Compute the total relation matrix: After calculating the normalized matrix, the fuzzy total-relation matrix can be computed as follows:

$$T = \lim_{k\to+\infty}(N^1 + N^2 + \cdots + N^k) \quad (4)$$

In other words, an n × n identity matrix is first generated, then this identity matrix is subtracted from the normalized matrix and the resulting matrix is reversed. The normalized matrix is multiplied by the resulting matrix to obtain the total relation matrix.

$$\mathrm{T} = \mathrm{N} \times (I - N)^{-1} \quad (5)$$

Step 4: set the threshold value: The threshold value must be obtained in order to calculate the internal relations matrix. Accordingly, partial relations are neglected, and the network relationship map (NRM) is plotted. Only relations whose values in matrix T are greater than the threshold value are depicted in the NRM. To compute the threshold value for relations, it is sufficient to calculate the average values of the matrix T. After the threshold intensity is determined, all values in matrix T that are smaller than the threshold value are set to zero, that is, the causal relation mentioned above is not considered.

Step 5: Final output and create a causal diagram: The next step is to find out the sum of each row and each column of T (in step 3). The sum of rows (D) and columns (R) can be calculated as follows:

$$D = \sum_{j=1}^{n} T_{ij} \quad (6)$$

$$R = \sum_{i=1}^{n} T_{ij} \quad (7)$$

Then, the values of D+R and D-R can be calculated by D and R, where D+R represents the degree of importance of factor i in the entire system and D-R represents the net effects that factor *i* contributes to the system [9].

TOPSIS: Hwang and Yoon developed a technique to resolve MCDM known as the TOPSIS method. To support the shortest Euclidean distance, they proposed the PIS and NIS and each criterion needs to be maximized or minimized [10]. They claimed that the TOPSIS method helps rank alternatives closeness based on the optimum ideal solution and obtained the maximum level from available alternatives. The best alternative has rank one and the worst alternative approaches rank zero. For every alternative, there is an intermediate ranking between the best answer extremes. An identical set of choice criteria permits correct weighting of relative disease and therefore the optimum disease is alarming and needs attention. Here are presented the steps for the TOPSIS technique. TOPSIS views an MCDM problem with m-alternatives as a geometric system with m points in the n-dimensional space. The core concept of this technique is that the chosen alternative should have the smallest geometrical distance from the PIS and the largest geometrical distance from the NIS. To apply TOPSIS [54], a common assumption is that criteria should be either monotonically increasing or decreasing so that PIS and NIS can be easily identified [11].

The construction of the normalized matrix will be as follows:

$$r_{ij} = \frac{f_{ij}}{\sqrt{\sum_{j=1}^{n} f_{ij}^2}} \quad (8)$$

Where: r_{ij} is the normalized value for the qualification of alternative i against criterion j and f_{ij} is the indicator of each alternative i against each indicator j.

Doi: https://doi.org/10.54216/FPA.160203
Received: July 06, 2023 Revised: November 15, 2023 Accepted: May 26, 2024

For the minimum distance to the positive ideal solution and maximum distance to the negative ideal solution, it is carried out according to the following equations [12].

$$A^+ = (x_1^+, x_2^+, \dots x_{j+l}^+) \quad (9)$$

$$A^- = (x_1^-, x_2^-, \dots x_{j+l}^-) \quad (10)$$

With the normalized values, the Euclidean distances for each of the alternatives to the positive ideal solution and the negative ideal solution are calculated, as explained in [13]:

$$\rho(A^k, A^+) = \|w * (TA^k - TA^+)\| \quad (11)$$

$$\rho(A^k, A^-) = \|w * (TA^k - TA^-)\| \quad (12)$$

Finally, the calculation of the Relative Proximity Index (Ri) is done as follows:

$$Ri(A^k, A^i) = \frac{\rho(A^k, A^+)}{\rho(A^k, A^+) + \rho(A^k, A^-)} \quad (13)$$

4. Results

The following criteria will be analyzed by a group of 4 experts, following the DEMATEL method, for their evaluations and weightings:

1) **Data Extraction Capability:** measures the tool's ability to perform physical, logical, and system file extractions from mobile devices. A forensic tool must be able to extract as much information as possible from the device.
2) **Operating System Compatibility:** evaluates the number of versions and variety of mobile operating systems (such as Android and iOS) with which the tool is compatible.
3) **Ease of Use** considers how intuitive and easy to use the tool's interface is for users, including the documentation and technical support provided.
4) **Analysis and Reporting Capability:** measures the tool's ability to analyze extracted data and generate detailed and clear reports.
5) **Data Recovery Capability:** measures the effectiveness of the tool in recovering data that has been deleted from the device. Recovering deleted data can be crucial for uncovering relevant information in forensic investigations.

Table 1: Direct relation matrix

	Criterion1	Criterion2	Criterion3	Criterion4	Criterion5
Criterion1	0	0.9	0.9	0.875	0.975
Criterion2	0.55	0	0.575	0.65	0.625
Criterion3	0.85	0.9	0	0.8	0.9
Criterion4	0.575	0.55	0.625	0	0.675
Criterion5	0.875	0.85	0.925	0.675	0

Source: consultation with experts. DEMATEL method. Note: own elaboration.

Table 2: The normalized direct-relation matrix

	Criterion1	Criterion2	Criterion3	Criterion4	Criterion5
Criterion1	**0**	**0.247**	**0.247**	**0.24**	**0.267**
Criterion2	**0.151**	**0**	**0.158**	**0.178**	**0.171**
Criterion3	**0.233**	**0.247**	**0**	**0.219**	**0.247**
Criterion4	**0.158**	**0.151**	**0.171**	**0**	**0.185**
criterion5	**0.24**	**0.233**	**0.253**	**0.185**	**0**

Source: consultation with experts. DEMATEL method. Note: own elaboration.

Table 3: Final output

	R	D	D+R	D-R
Criterion1	4,744	5,824	10,568	1.08

Doi: https://doi.org/10.54216/FPA.160203
Received: July 06, 2023 Revised: November 15, 2023 Accepted: May 26, 2024

Criterion2	5,222	4,081	9,302	-1,141
Criterion3	4,977	5,558	10,535	0.581
Criterion4	4,936	4,153	9.09	-0.783
Criterion5	5,171	5,434	10,605	0.263

Source: consultation with experts. Note: own elaboration.

According to the table above, each factor can be assessed based on the following aspects:

- ✓ Horizontal vector (D + R) represents the degree of importance between each factor plays in the entire system. In other words, (D + R) indicates both factors i's impact on the whole system and other system factors' impact on the factor. In terms of degree of importance, criterion5 is ranked in the first place, and criterion1, criterion3, criterion2 and criterion4, are ranked in the next places.
- ✓ The vertical vector (D-R) represents the degree of a factor's influence on the system. In general, the positive value of D-R represents a causal variable, and the negative value of D-R represents an effect. In this study, criterion1, criterion3, criterion5 are considered to be a causal variable and criterion2, and criterion4 are regarded as an effect.

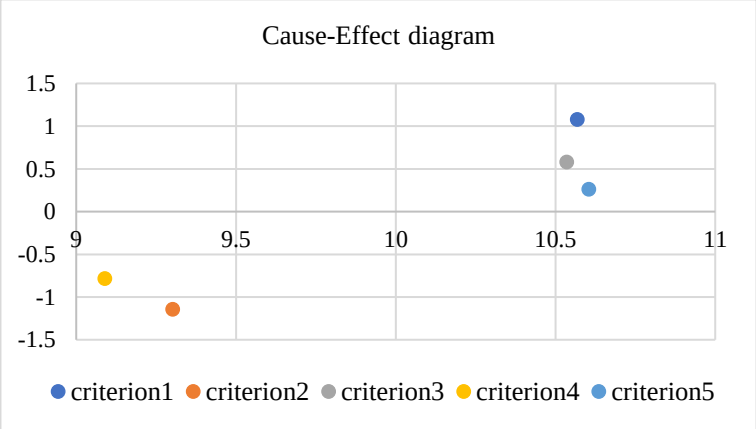

Figure 2: Causal relationships. Source: DEMATEL Method.

Figure 2 shows a causal relationship diagram among the five criteria evaluated in the forensic analysis of mobile devices. This type of diagram is useful for understanding the internal dynamics among the factors (criteria) and how each one contributes to the overall system, allowing for the identification of the most influential factors and those that are more influenced.

- Criterion 1 (D+R = 10.568, D-R = 1.08): This criterion has the highest D+R, indicating that it is the most prominent in the system. The positive value of D-R suggests that it is also a net influencer. This means that the Data Extraction Capability is not only important in itself, but it also significantly affects other criteria.
- Criterion 2 (D+R = 9.302, D-R = -1.141): Although this criterion has high importance (D+R), its negative D-R indicates that it is more of a recipient of influences. Operating System Compatibility is more affected by other criteria than it affects them.
- Criterion 3 (D+R = 10.535, D-R = 0.581): Similar to Criterion 1 in terms of prominence but with a lower positive D-R. Ease of Use is important and acts more as an influencer within the system, although not as much as Criterion 1.
- Criterion 4 (D+R = 9.09, D-R = -0.783): This criterion is important but, similar to Criterion 2, acts more as a recipient. The Analysis and Reporting Capability is influenced by the capabilities and compatibilities of other areas.
- Criterion 5 (D+R = 10.605, D-R = 0.263): This criterion is the most prominent after Criterion 1, indicating its high relevance. Its positive D-R, although lower, shows that the Data Recovery Capability of Deleted Data also plays an influencing role in the system.

Doi: https://doi.org/10.54216/FPA.160203
Received: July 06, 2023 Revised: November 15, 2023 Accepted: May 26, 2024

To compare the tools used in the Forensic Analysis of Mobile Devices using the TOPSIS method, the criteria previously processed in the DEMATEL method, and their corresponding weights will be taken. The proposed tools to be analyzed are as follows:

1. Android Triage; 2. iOS Triage; 3. Andriller Triage; 4. Magnet Acquire

Table 4: Characteristics of Criteria

	Name	Type	Weight
1	Criterion1	+	0.2109
2	Criterion2	+	0.1856
3	Criterion3	+	0.2102
4	Criterion4	+	0.181
5	Criterion5	+	0.211

Source: consultation with experts. TOPSIS method. Note: own elaboration.

Table 5: Decision Matrix

	Criterion1	Criterion2	Criterion3	Criterion4	Criterion5
Alternative1	0.9075	0.875	0.9375	0.9	0.9125
Alternative2	0.62	0.4525	0.5625	0.4875	0.275
Alternative3	0.9	0.825	0.9	0.8325	0.85
Alternative4	0.6125	0.6	0.6375	0.425	0.3

Source: consultation with experts. TOPSIS method. Note: own elaboration.

Table 6: The normalized matrix

	Criterion1	Criterion2	Criterion3	Criterion4	Criterion5
Alternative1	0.587	0.617	0.604	0.649	0.696
Alternative2	0.401	0.319	0.362	0.352	0.21
Alternative3	0.582	0.582	0.58	0.601	0.648
Alternative4	0.396	0.423	0.411	0.307	0.229

Source: consultation with experts. TOPSIS method. Note: own elaboration

Table 7: The weighted normalized matrix

	Criterion 1	Criterion 2	Criterion 3	Criterion 4	Criterion 5
Alternative1	0.124	0.115	0.127	0.118	0.147
Alternative2	0.085	0.059	0.076	0.064	0.044
Alternative3	0.123	0.108	0.122	0.109	0.137
Alternative4	0.084	0.079	0.086	0.055	0.048

Source: consultation with experts. TOPSIS method. Note: own elaboration

Table 8. Distance to positive and negative ideal points and order

	D+	D -	Ci	Rank
Alternative1	0	0.147	1	1
Alternative2	0.143	0.008	0.054	4
Alternative3	0.016	0.132	0.893	2
Alternative4	0.135	0.022	0.141	3

Source: consultation with experts. TOPSIS method. Note: own elaboration

A Multi-Criteria Decision Analysis (MCDM) using the TOPSIS method was employed to evaluate the effectiveness of various tools used in the forensic analysis of mobile devices. This analysis considered both the distance of each alternative from the positive ideal point and the distance from the negative ideal point. The goal was to identify the tool that offered the best performance according to the established criteria and expert evaluations.

Five main criteria were analyzed, and four forensic tool alternatives were compared. Each criterion was weighted according to its importance in forensic analysis. The initial decision matrix displayed

Doi: https://doi.org/10.54216/FPA.160203
Received: July 06, 2023 Revised: November 15, 2023 Accepted: May 26, 2024

the performance values of each tool in relation to each criterion. The study determined that the Android Triage and Andriller tools showed better performance. These tools reached the shortest distances to the positive ideal solution and the longest from the negative ideal solution, indicating that they closely align with the optimal criteria defined for the forensic analysis of mobile devices.

The AndroidTriage and Andriller tools from the Linux Operating System become the primary basis for information retrieval due to their specific features. AndroidTriage is a very powerful tool for forensic analysis, as it performs graphs about the collected information highlighting its social graph. This helps to see the links of the suspect with their contacts, as well as their conversation frequencies. In the case of Andriller, this tool allows the extraction of information from a mobile device. This application enables data acquisition from devices with Android operating systems using techniques that include access to system memory, extraction of application data, and password recovery.

A. Case study

Using the results from the Multi-Criteria Decision Analysis, for the following case study, the Tsurugi Linux Operating System will be used with the assistance of the two tools, AndroidTriage and Andriller, as they consume the least amount of time to obtain a forensic image, thereby starting the analysis of the evidence.

- ✓ **Comparison of forensic model phases**

CFFTPM	**DFRWS**	**GCFIM**
Planning	Identification	Pre-process
Triage	Preservation	Acquisition and preservation
User profile	Collection	
Timeline	Inspection	Analysis
Chronology	Analysis	Presentation
Internet	Presentation	Post-process
Specific Case	Decision	

As a result of the analysis, the **Triage model** was selected for application in the case study due to its characteristics.

"The practical case was carried out at the Technical Office of Violence 'Carcelén - Ecuador' in a controlled environment in the presence of staff from this department" (Kevin Tipanta; Rubio Jorge, 2023).

Planning: the first step involves filling out consent forms by the owner of the equipment to be analyzed.

Table 9: Characteristics of the received device

Device status and features			
Device status	Switched on **X**		Switched Off
Protected by some type of key	YES **X**		NO
In case of having protection (type)			
Pattern		---	
PIN		1971	
Password		---	
Fingerprint		--	
Facial Recognition		--	
Device Features			
Phone brand		SAMSUNG	
Phone model		J2 PRIME	
Phone number		0984943056	
Service operator		MOVISTAR	
IMEI serial number		358212080461584	
Extra device documentation			
	YES		NO
Removable memory (micro SD)	-----		X

Doi: https://doi.org/10.54216/FPA.160203
Received: July 06, 2023 Revised: November 15, 2023 Accepted: May 26, 2024

Charger	X	-----
Access codes	-----	X
Reception		
Received by:	Kevin Tipanta	
Reviewed by:	Eng. Jorge Rubio	
Approved by:	XXXXXXXXXX	

Triage

In this phase, it is necessary to create a table of data importance, so the user is informed about which data will be presented as evidence and where it is located. Next, a backup of the phone data is obtained.

It is required:

- ✓ The device to be unlocked.
- ✓ The device set to airplane mode.
- ✓ The device set in developer mode.
- ✓ USB debugging enabled.
- ✓ Prevent the device from locking during the backup.

Next, the Android Triage tool is used to obtain a backup of the data. The first backup will be saved with the date and time it is being made as its name. Then, a folder will be created on the Tsurugi desktop to facilitate the creation of the hash; the folder will be called evidencia1 and will have the following path: **/home/tsurugi/Desktop/evidencia1**.

- ✓ Open the Tsurugi tools and select the hash option and the ssdeep tool.
- ✓ Enter the following command to access the created folder cd Desktop/evidencia1, then we enter an ls to see the files we have and verify that it is the backup.
- ✓ To obtain an md5 hash, enter the following code:
  md5sum* along with it to obtain in txt type enter **md5sum* >hash.txt**

User Profile

In this phase, the second backup will be performed, but this time the Andriller tool will be used since it includes an HTML report of the evidence found.

Proceed to select:

- ✓ - The path where the second backup will be saved.
- ✓ - Click on check and observe that a serial number is displayed.
- ✓ - Select the two options to extract all the data the device holds.
- ✓ - Ultimately, obtain a complete backup of the device along with an md5 hash as evidence.

Chronology

Case number 1 Android Triage

Backup Timeline
Computer Experts: Jorge Rubio
Case Number: 001
Date: 20/01/2023
Time: 17:35
Hash: d41d8cd98f00b204e9800998ecf8427e
Backup Status: Satisfactory
Tool Used: AndroidTriage and FuzzyHash ssdeep
Observations: None

Case number 1.1 Andriller

Backup Timeline
Computer Experts: Jorge Rubio
Case Number: 001.1
Date: 20/01/2023
Time: 23:35
Hash: 1276481102f218c981e0324180bafd9f
Backup Status: Satisfactory
Tool Used: Andriller, md5
Observations: None

Doi: https://doi.org/10.54216/FPA.160203
Received: July 06, 2023 Revised: November 15, 2023 Accepted: May 26, 2024

Internet
In this phase, it is crucial since the majority of data analyzed here are from instant messaging, for example, WhatsApp and Messenger, among the most recognized. Also included in this group are emails sent, received, and spam.

B. Discussion of the cases

The correct use of tools allowed for the collection, handling, and analysis of digital evidence stored on the mobile device, ensuring the forensic process. For the execution of this process, several tools were identified and selected; however, none of them proved to be optimal for analysis, with many exhibiting deficiencies when interacting with devices. Based on the analysis of Operating Systems and tools, AndroidTriage was used for evidence acquisition and Andriller for extracting information from a mobile device; these tools showed a performance of about 90% throughout the forensic analysis process, compared to other tools analyzed.

A methodology becomes a support tool for obtaining evidence that can clarify various types of illicit activities; if carried out appropriately, to not be considered a violation of privacy [14]. Although current mobile devices have similarities, the evidence found on these devices will be similar (images, files, exchanged emails, visited websites), but several additional elements can be obtained, such as:

- ✓ The contact list.
- ✓ Record of calls made and received.
- ✓ SMS, MMS.
- ✓ Data that allows determining the physical location of the mobile at the time of its acquisition.

To better understand these differences, they can be separated into 4 categories:

- ✓ File System.
- ✓ Memory states.
- ✓ Storage capacity.
- ✓ Data acquisition.

It is very likely that in the coming years, the operating systems of these devices, as well as their interfaces, will become standardized to facilitate investigative tasks. Meanwhile, the diversity of tools, and above all, the expertise of the computer forensic investigator, are key to the success of current investigations.

6. Conclusion

This study confirmed the effectiveness of using Multi-Criteria Decision Analysis (MCDM) methods, specifically DEMATEL and TOPSIS, to evaluate forensic tools for mobile devices. The findings highlighted the superior performance of Android Triage and Andriller tools in data collection, retrieval, and validation under the Cyber Forensic Field Triage model. The practical case study further validated these results, demonstrating the tools' efficiency and reliability in real-world forensic analysis scenarios. The integration of multiple criteria and expert preferences was crucial in identifying the most effective tools.

Future research should explore the application of these methods to a broader range of mobile operating systems and forensic tools to generalize the findings further. Additionally, developing automated systems that incorporate these MCDM methods could streamline the forensic analysis process, making it more efficient and accessible for practitioners. Enhanced collaboration between forensic experts and software developers is recommended to refine the tools and methodologies, ensuring they remain effective as mobile device technologies continue to evolve.

Funding: “This research received no external funding”

Acknowledgement: The efficiency of the instruments in real-world forensic analysis was evaluated by a case study conducted at the Technical Office of Violence "Carcelén - Ecuador".

Conflicts of Interest: “The authors declare no conflict of interest.”

Doi: https://doi.org/10.54216/FPA.160203
Received: July 06, 2023 Revised: November 15, 2023 Accepted: May 26, 2024

References

[1] A. Al-Dhaqm, S. Abd Razak, R. A. Ikuesan, V. R. Kebande, and K. Siddique, "A review of mobile forensic investigation process models," IEEE access, vol. 8, pp. 173359-173375, 2020.

[2] A. Fukami, R. Stoykova, and Z. Geradts, "A new model for forensic data extraction from encrypted mobile devices," Forensic Science International: Digital Investigation, vol. 38, p. 301169, 2021.

[3] O. Osho, U. L. Mohammed, N. N. Nimzing, A. A. Uduimoh, and S. Misra, "Forensic analysis of mobile banking apps," in Computational Science and Its Applications–ICCSA 2019: 19th International Conference, Saint Petersburg, Russia, July 1–4, 2019, Proceedings, Part V 19, 2019, pp. 613-626.

[4] E. Abba, A. M. Aibinu, and J. Alhassan, "Development of multiple mobile networks call detailed records and its forensic analysis," Digital Communications and Networks, vol. 5, pp. 256-265, 2019.

[5] P. Sharma, D. Arora, and T. Sakthivel, "Enhanced forensic process for improving mobile cloud traceability in cloud-based mobile applications," Procedia Computer Science, vol. 167, pp. 907-917, 2020.

[6] H. H. Lwin, W. P. Aung, and K. K. Lin, "Comparative analysis of Android mobile forensics tools," in 2020 IEEE Conference on Computer Applications (ICCA), 2020, pp. 1-6.

[7] Y.-W. Du and X.-X. Li, "Hierarchical DEMATEL method for complex systems," Expert Systems with Applications, vol. 167, p. 113871, 2021.

[8] Leyva-Vázquez, M., Pérez-Teruel, K., Febles-Estrada, A., & Gulín-González, J. (2013). Causal knowledge representation techniques: A case study in medical informatics. Revista Cubana de Información en Ciencias de la Salud (ACIMED), 24(1), 73-83.

[9] D. R. Bonifaz Díaz, L. R. Ramírez López, and L. P. Advendaño Castro, "Neutrosophic DEMATEL to Prioritize Risk Factors in Teenage Pregnancy Sets," Neutrosophic Sets and Systems, vol. 37, pp. 24-30, 2020.

[10] I. F. B. Arias, J. M. M. Bermudez, and F. M. E. Gómez, "TOPSIS with a Neutrosophic Approach for a Study of Strategies to Confront the Crime of Feminicide in Ecuador," Neutrosophic Sets and Systems, vol. 37, pp. 347-354, 2020.

[11] Molina Manzo, A. D., Hernández Alvarado, V. J., & Nivela Ortega, E. S. (2022). AHP and TOPSIS methods for estimation in the humanitarian support law and the unconstitutionality of article 25 declared in the Ecuadorian constitutional court. Neutrosophic Computing and Machine Learning, 21, 87-98. https://doi.org/10.5281/zenodo.6772591

[12] Y. Çelikbilek and F. Tüysüz, "An in-depth review of theory of the TOPSIS method: An experimental analysis," Journal of Management Analytics, vol. 7, pp. 281-300, 2020.

[13] M. Y. L. Vazquez, L. A. B. Peñafiel, S. X. S. Muñoz, and M. A. Q. Martinez, "A Framework for Selecting Machine Learning Models Using TOPSIS," in Advances in Intelligent Systems and Computing vol. 1213 AISC, ed, 2021, pp. 119-126.

[14] R. Umar, I. Riadi, and B. F. Muthohirin, "Live forensics of tools on android devices for email forensics," TELKOMNIKA (Telecommunication Computing Electronics and Control), vol. 17, pp. 1803-1809, 2019.

Doi: https://doi.org/10.54216/FPA.160203
Received: July 06, 2023 Revised: November 15, 2023 Accepted: May 26, 2024