RESEARCH ARTICLE

Development of Xiaomi Product Mobile Forensic Acquisition Framework on Second Space Features Based on SNI/ISO 27037:2014

Amru Rizal Fakhriansyah[1,*], Ahmad Luthfi[2]

[1,2]Fakultas Teknologi Industri, Universitas Islam Indonesia, Yogyakarta 55584, Indonesia

*Corresponding email: 21917002@students.uii.ac.id

Abstract: In conducting digital forensic activities, references or standards that must be followed serve as guidelines for the processes performed by investigators. One of the frameworks that can be adhered to is the SNI ISO 27037, which constitutes Indonesia's digital forensic standard governing the guidance for identification, collection, acquisition, and preservation of digital evidence, adopted from ISO 27037:2012. Mobile forensics, a branch of digital forensics, deals with the examination of mobile devices, and one such mobile device vendor is Xiaomi. Xiaomi offers a unique "Second Space" feature that segregates and divides internal storage. This feature poses a challenge for investigators in forensic activities as the SNI ISO 27037 does not explicitly regulate how to obtain digital evidence from a phone equipped with such a unique feature. The existence of the Second feature in Xiaomi products becomes a challenge for investigators to acquire legally admissible evidence in court by lawful means. The method employed in this research is a quantitative approach involving direct analysis (live forensics) to gather evidence from Xiaomi's Second Space feature. The outcome of this study is a workflow or framework designed to procure digital evidence from Xiaomi's Second Space feature, utilizing MobilEdit Forensic Express Pro, one of the digital forensic tools for mobile forensics. The constructed framework can be implemented for other phones featuring a similar Second Space function; however, as of now, only a limited number of phones possess this feature. Thus, establishing this framework can assist future investigators in acquiring digital evidence from mobile devices equipped with specialized features.

Keywords: framework, second space, sni iso 27037:2014, xiaomi.

1   Introduction

The evolution of technology poses a significant challenge within the realm of forensics [1]. Among the continually advancing technologies, mobile devices stand out as electronic tools facilitating the exchange of information, encompassing data, audio, and video. Besides serving communication purposes, mobile devices are increasingly prominent in cybercrime scenarios cases [2]. One of the mobile device vendors is Xiaomi. In its development, Xiaomi provides special features for its users, namely the unique feature of the Second Space. This Second Space feature is only developed by Xiaomi on Android smartphones; this Second Space feature can be activated on Xiaomi smartphones that have MIUI version 8 and above. Xiaomi stands as one of the prominent vendors in the mobile device industry. Throughout its evolution, Xiaomi has introduced distinct functionalities for its users, notably the unique feature known as the "Second Space." This specific attribute is exclusively incorporated into Xiaomi's Android smartphones, available for activation on devices running MIUI version 8 and higher.

The Second Space represents a feature that Xiaomi's smartphone developers crafted, enabling users to establish two distinct mobile environments within one device. Within this Second ary Space, users can share storage space, offering different access privileges and distinct storage locations. This particular feature was devised to uphold the data security of its users, mandating authentication measures such as lock screen passwords, MIUI account passwords, Second Space access passwords, and fingerprint verification for access. Notably, this Second Space feature significantly influences the handling process of digital evidence from mobile devices, an area commonly referred to as mobile forensics. Mobile forensics is a specialized field within digital forensic science, focusing on analyzing and exploring digital traces within mobile devices.

One of the processes of handling electronic evidence on mobile devices is acquisition [3]; acquisition is a process carried out to obtain digital traces on a device, which will later be used as evidence at trial [4]. To carry out the acquisition, a standard procedure is needed that can be a reference for investigators in carrying out the acquisition process. One of the standards that can be used as a standard or acquisition procedure is SNI ISO 27037. SNI ISO 27037 is a guideline for handling electronic evidence recognized in Indonesia as SNI (Indonesian National Standard), which was approved on 28 November 2013 in Bogor. SNI ISO 27037: 2014 is allowed to perform logical acquisitions carried out by investigator officers, namely Digital Evidence First Responders (DEFR) [5].

There are four stages in searching for evidence: Acquisition, Preservation, Analysis, and Presentation [6]. The SNI ISO/IEC 27037:2014 document has provided a complete explanation of each process of handling electronic evidence by definition, but there are areas for improvement in technical terms. Each step that must be taken in carrying out the digital forensic process must be explained in detail. Because each device has different characteristics, the investigator must be able to find an appropriate and suitable method in carrying out the digital forensic process according to the device being analyzed and can be accounted for in every process [7].

However, looking at the development of existing mobile devices, SNI ISO 27037 still needs to cover the acquisition process by the characteristics of Xiaomi devices. Xiaomi mobile devices have different storage characteristics that require investigators to find a framework that is suitable for Xiaomi devices. As explained, Xiaomi has a Second Space feature that separates storage media but remains on one device; thus, to perform acquisi-

tion on Xiaomi devices requires two acquisition processes, resulting in two extractions obtained from one device.SNI ISO 27037, which constitutes Indonesia's digital forensic standard governing the guidance for identification, collection, acquisition, and preservation of digital evidence, adopted from ISO 27037:2012. SNI ISO 27037 has provided guidelines for investigators to carry out the acquisition process, namely in clause 7.1.3 Acquisition, there are three scenarios where the acquisition is carried out, namely: when the digital device is turned on, when the digital device is turned off and when the digital device is turned on and cannot be turned off [8]. The acquisition process that is suitable for Xiaomi mobile devices is the acquisition of digital devices in the on state, because the Second Space has different characteristics from other devices in terms of data storage, the acquisition process must be adjusted.

By considering the existing problems, this research will develop a workflow as a guideline for the DEFR in acquiring Xiaomi mobile devices with the unique features of the Second Space based on SNI ISO 27037:2014. To support the preparation of this research, the author reviews previous methods conducted by Aji *et al.* [3], who developed a workflow or workflow in conducting logical acquisitions on smartphones using the live forensic method using the Laron application, which is adjusted to SNI ISO/IEC 27037:2014 with several requirements, research conducted by Sudyana *et al.* [9] explains that the current framework has shortcomings where there are stages in the framework that are not by SNI ISO 27037 [10]. The difference between this research and previous research lies in the object of research, namely the Xiaomi mobile device with unique features of the Second Space, which has different characteristics from mobile phones in general, so it requires the development of a workflow/framework in the acquisition process.

In the preparation of this research, the author is also not far from the previous researcher's review of the acquisition framework based on SNI ISO/IEC 27037; the following is a brief description of the studies that have been summarised: One of the frameworks developed using the Laron application as a logical acquisition application licensed by MIT [6]. According to the author's observation data, evidence in the form of smartphones always increases every year, so it is possible to increase crimes using smartphones in the future. So, the author built an acquisition framework using the Laron application based on SNI ISO 27037:2014. With the construction of this research, it is hoped that it can help DEFR's task in conducting smartphone acquisitions based on SNI ISO 27037:2014.

Previous research discussed the logical acquisition process on Android devices using open-source applications. The study discusses open-source applications that can be used as tools in the acquisition process of Android devices by paying attention to recognized standards, namely SNI ISO 27037:2014 [3]. The applications used in this study are AFLogical OSE and Laron, which consider the logical acquisition framework and use requirements such as mobile phones being on, unlocked, and ADB enabled. The results show that the AFLogical OSE application can obtain digital artifacts in the form of SMS, MMS, Contact List, and Call Log, while the Laron application obtains digital artifacts in the form of a database installed on the mobile phone.

Related research conducts digital artifacts searches on smartphones with unique features, namely Dual App on Xiaomi phones [11]. Due to the development of mobile cellular devices that continue to grow with increasingly varied innovations, special handling is needed. Rapid actions in the mobile cellular world significantly affect the forensic process regarding rules, procedures, and handling. By conducting an analysis using Andriller and Laron, it turns out that the location of the database in the Dual App feature cannot be de-

tected automatically, so a manual search is carried out to find the artifacts sought. Because the Andriller and Laron applications are still open-source, it is hoped that in the future, it will be possible to search for digital artifacts with a logical acquisition application in the application that runs on the Dual App.

To support this research, the author takes the same research object as the previous author, who discussed the search for digital artifacts in the Mi Video application on Xiaomi phones using the Live Forensic method [12]. Xiaomi smartphones are growing yearly, both in terms of sales and production. The UI design update on Xiaomi phones called MIUI in version 9 has many changes, especially in added features such as Mi Drop, Mi Music, Mi Video, and Special Features. Besides being a tool for playing videos, Mi Video also has a Log that stores user activity on the device. So, the author investigates the Mi Video application to get digital artifacts stored in the Mi Video Log. The results of this study are digital artifacts found in the Mi Video Log that can be used as evidence, but to gain access to the Log requires root access. Due to the unique structure of Xiaomi mobile phones, the device must be on to carry out this investigation process using the Live Forensic method [13].

Previous research has discussed technology development on mobile devices and their features. Still, earlier research has yet to discuss the unique features of the Second Space on Xiaomi. Due to the rapid development of technology on mobile devices, this research is essential and can be helpful for investigators in conducting digital forensic processes on mobile devices. The kedia Space feature has different specifications from other devices in terms of storage, so it requires some additions to the acquisition process of the Second Space feature Xiaomi device based on SNI ISO 27037:2014.

2   Research Method

2.1   Research Flow

At this stage, the flow of the research process that will be carried out will be explained; the process in this research is Literature Study, Problem Identification, Framework Identification, and Framework Evaluation with SNI ISO 27037:2014. SNI ISO 27037 framework SNI 27037 is an Indonesian digital forensics standard regarding guidelines for identifying, collecting, acquiring, and preserving digital evidence adopted from SNI ISO 27037:2012, Building Framework, Framework Implementation, Framework Implementation Evaluation, and Conclusion. This research was built by conducting a framework development study and adjusting digital forensic standards in carrying out the process of investigating digital evidence; this research focuses on the unique features of Xiaomi mobile phones, namely Second Space, by adjusting the SNI ISO 27037:2014 standard which is used as a reference or measure in conducting digital forensic activities in Indonesia. Each process or flow of this research has been summarized and will be explained in Figure 1.

As in Figure 1, this research is built from a literature review collected and analyzed by the object of study, namely, the acquisition framework and special features of Second Space on Xiaomi Android devices.

Problem identification is determining the formulation of problems by adjusting the object of research, namely Xiaomi smartphones and Second Space features. Identification of the issues taken from previous research related to storage on mobile devices that will be analyzed according to research needs.
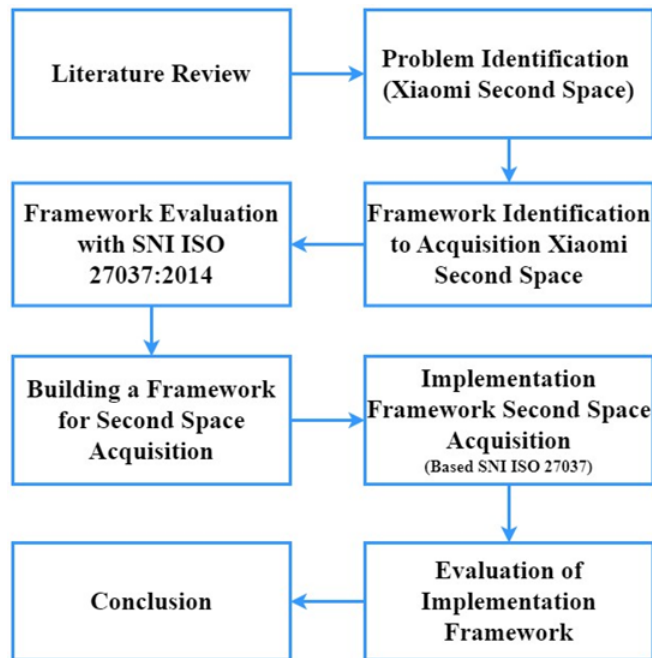
Figure 1: Research flow of second space acquisition.

After analyzing as needed, the researcher analyzed the framework used in the acquisition process using the SNI ISO 27037:2014 standard in many digital forensic acquisition processes. This standard was chosen because it already has SNI, is recognized in Indonesia as one of the standards that DEFR can use in carrying out digital forensic processes, and has the power to prove cases in court. SNI ISO 27037, a guideline for investigators used in this research, will be evaluated with the needs of the research so that the requirements in SNI ISO 27037 are met, and the framework built has strength in the process of proof for investigators and is valid in court.

After analyzing the appropriate framework, the researchers built a framework based on the SNI ISO 27037:2014 standard by paying attention to each clause contained in SNI ISO 27037:2014 so that the framework built has a strong foundation and has the proper basis for carrying out the digital forensics process.

After building the framework and having the appropriate case scenario, the framework implementation process in the file acquisition process in the Second Space can be carried out. When implementing the framework on the object of research, researchers also carry out documentation, which is one of the requirements in the SNI ISO 27037:2014 clause.

After the implementation process was completed, the researcher used an observational method approach to evaluate the effectiveness of the framework built by paying attention to the acquisition results; observations were made by paying attention to the requirements in the SNI ISO 27037:2014 clause and the obstacles that occurred during the implementation of the framework. Evaluation of the framework is carried out by analyzing each process, which must be by SNI ISO 27037 standards to recognize the framework's application. The framework built is a development of the acquisition process of SNI ISO 27037 clause 7.1.3,

which is the process of acquiring digital evidence of the device; this acquisition process was chosen because, in the process of acquiring the Xiaomi device, the Second Space feature must be done in the state of the device on. The Second Space is a sensitive feature; if the acquisition process is carried out on a dead Xiaomi device, the Second Space cannot be connected. Observations are also made on the acquisition results; this research discusses the development of the framework and the characteristics of the Second Space, which is considered a gap for criminals in hiding digital evidence.

After the evaluation, it will conclude that the framework built is practical based on the standards and requirements needed in the file acquisition process on the unique features of the Second Space/Second Space of Xiaomi mobile devices.

2.2   Case Scenario

In accordance with Figure 1 where the case scenario is built in the problem identification process to be carried out. The case scenario built in this study aims to analyze the Second Space acquisition process, so that the file to be acquired must be in the Second Space. To clarify the case to be built, it is explained in Figure 2.
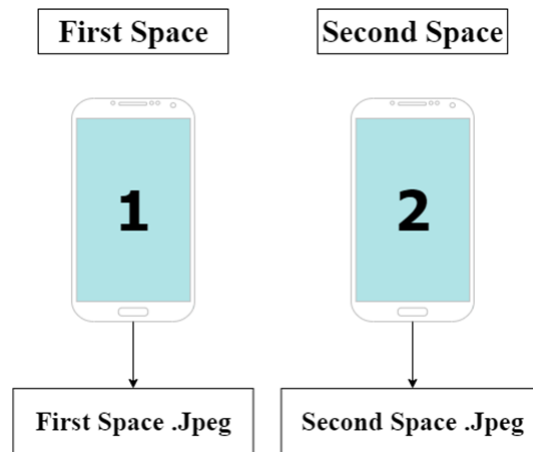

Figure 2: Case scenario.

The case scenario built in this study will perform two storage of image files with .Jpeg format stored in the First Space and the Second Space, the purpose of storing in both Space s to be analyzed in the acquisition process. The Second Space storage is a separate storage with the main Space, to get files in the Second Space must get access to the First Space First, so with this different storage, it will be possible to analyze the storage Space. The acquisition process carried out using the MobilEdit application will detect the storage on the mobile phone, the file stored in the First Space is stored with the file name First Space .Jpeg and the file in the Second Space with the file name Second Space .Jpeg.

First Space .Jpeg file stored in the First storage is located in the internal storage folder/FILE EVIDENCE 1/First Space .Jpeg, while the Second Space .Jpeg. file is stored in the internal storage folder/FILE EVIDENCE SECOND SPACE /Second Space .Jpeg. To be able to access the Second Space, First Space access is needed such as, lock screen password,

MI account, Fingerprint (if needed), developer mode or developer access, and password login Second Space. In this case, the Second Space feature has been activated on a Xiaomi device with specifications as shown in Figure 3.
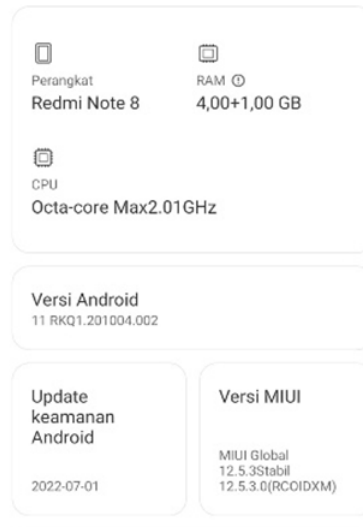

Figure 3: Mobile phone specifications.

The First and Second Space storage on Xiaomi phones have separate jolly that can be done manually analyzed on the primary storage; there is a difference before and after the Second Space is activated; on the First Space before the Second Space is made, the storage used on the phone is 33.7 GB / 64 GB, but after activating the Second Space the storage becomes 35.1 GB / 64 GB it can be seen that the main repository has been used 1.4 GB, the difference can be seen in Figure 4.

2.3   Xiaomi's Second Space

Second Space / Second Space is a unique feature developed by Xiaomi developers for users who have mobile specifications that have MIUI updates above version 9. This Second Space is here to provide more access to users in storing files that are more secure by utilizing storage that can be divided into two different Spaces with different access; the principle of this Second Space is the same as the open-source virtualization process on Windows, where an installed OS can create a new OS that has different storage with different access, conceptually this is almost the same as what Samsung has, namely Samsung Knox [14]. The difference between Second Space and Samsung Knox is in the access; Xiaomi provides more special access for users who have MIUI accounts and must have more access to be able to operate Second Space, while Samsung Knox is a feature where control of a mobile phone can be monitored or controlled by other parties who have the same network and have IP control. To access Second Space, Xiaomi phone users only need to activate it in settings - special features - Second Space, see Figure 5.
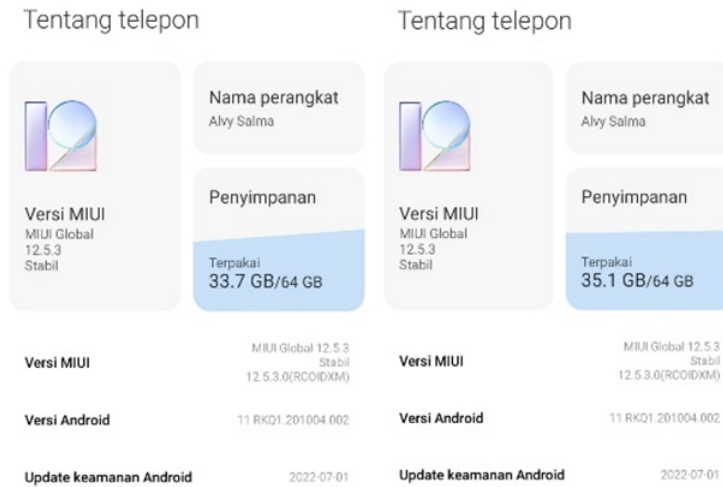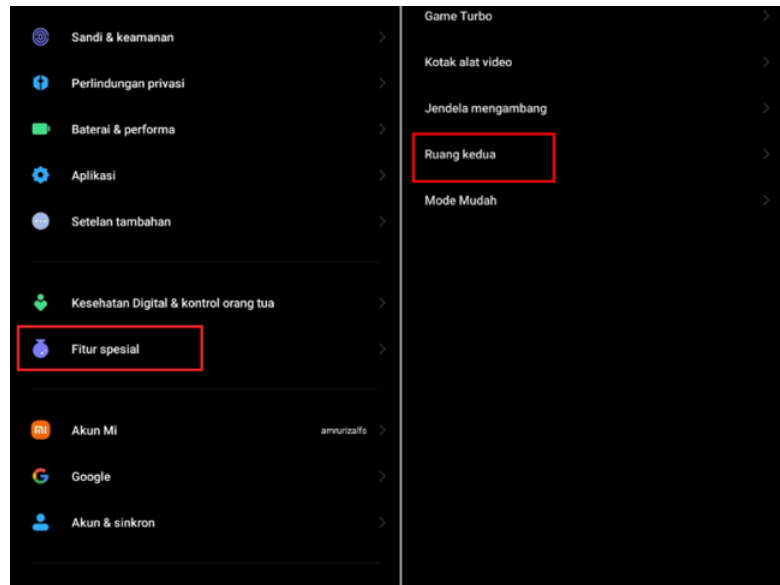
Figure 4: Storage size difference.

Figure 5: Second space.

2.4 Framework

NI ISO 27037:2014 is a standard procedure that is a reference for digital forensic practitioners in analysing and investigating digital evidence [9]. SNI ISO 27037 explains the procedures in handling digital evidence including the handling of mobile devices [15].

But in practice, SNI ISO 27037 only provides general procedures in handling electronic evidence that is universal; of course, this is a new challenge for digital forensic practition-
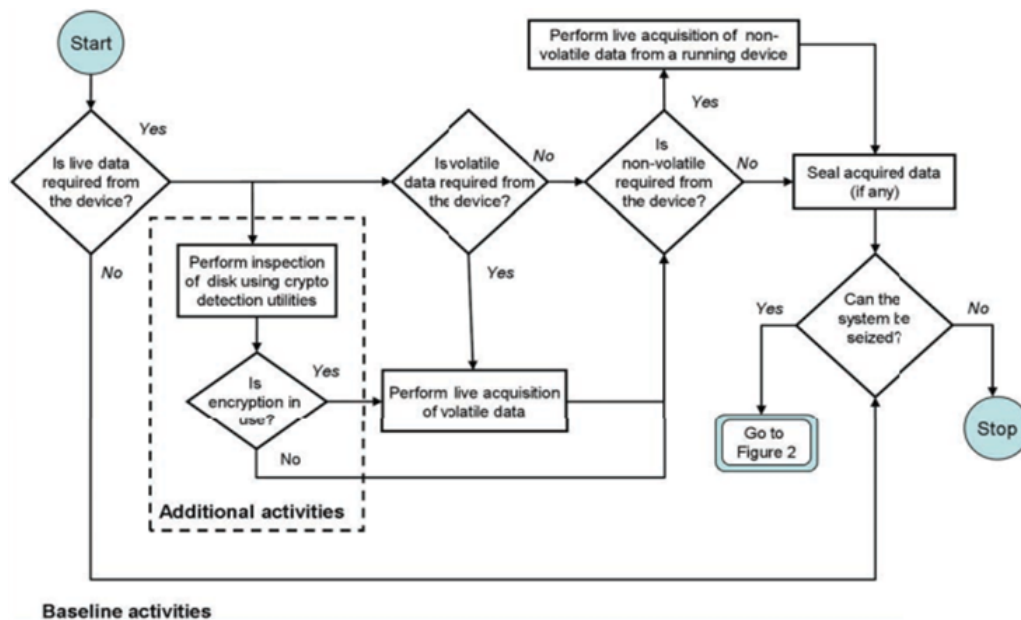
Figure 6: SNI ISO 27037 acquisition process (document SNI ISO-IEC 27037-2014 clause 7.1.3).

ers where in the development of existing technology, investigators are required to be able to find methods that are suitable for the device being analyzed. In this case, the forensic process that will be developed is the acquisition process, according to SNI ISO 27037:2014 clause 7.1.3 in section 7.1.3.1.1.1 Summary, it has been explained that "DEFR can follow several guidelines for acquisition when the device is found to be turned on. Not all guidelines are ideal and appropriate for all cases; some guidelines are only relevant for certain cases." This is the basis and reason for investigators to develop suitable acquisition methods for the case being handled. On the other hand, SNI ISO 27037 also provides guidelines for acquiring active digital devices, see Figure 6. Figure 6 explains how the acquisition process is carried out on an active digital device. Of course, this should be a guideline for investigators in carrying out the acquisition process, but on the other hand, a new problem is found where the device is. The object to be acquired has different specifications, whereas the Xiaomi mobile phone has different storage and other potential storage gaps. Xiaomi provides a feature for users to separate the central repository from personal storage, and this will undoubtedly be a different process when performing the acquisition process by the SNI ISO 27037 standard in Figure 6. The difference in the acquisition process is in the results/output of the imaging file; when extracting a mobile phone, it will produce an extraction file which will later be analyzed, in contrast to Xiaomi, which has a Second Space feature, when the investigator analysis this phone it is possible that it will produce two extraction files with the same extension and have the same file contents, but the study will produce different conclusions.

To get extraction results that are in accordance with the SNI ISO 27037:2014 standard, the framework built will be adjusted to the features and processes on the mobile phone

because Xiaomi has a unique feature, namely the Second Space, to separate the storage media, the process will be carried out for file acquisition twice, see Figure 7.
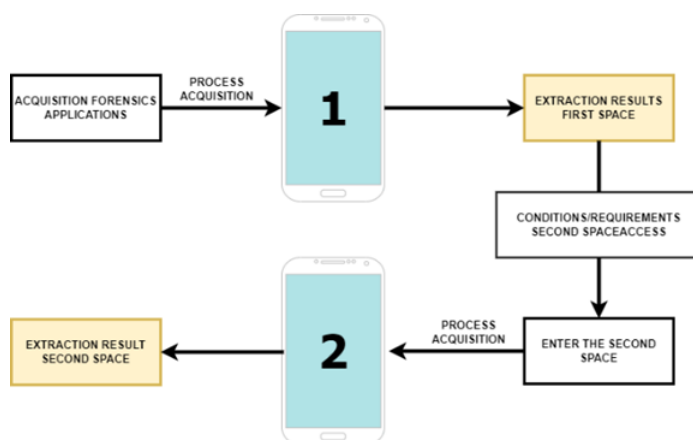

Figure 7: Xiaomi's acquisition process.

Figure 7 shows how the acquisition process is carried out. To perform the acquisition process in the Second Space, Xiaomi mobile phones must undergo two acquisition processes in one mobile phone. The process carried out to carry out the acquisition in the First Space can be done using the reference or standard SNI ISO 27037:2014, which can be a reference for investigators, but in carrying out the acquisition process of the Second Space, the same thing must also be done. There are several requirements in conducting the acquisition of the Second Space: 1. The Second Space acquisition process must be done after the First Space acquisition process is complete 2. The process to access the Second Space must go through the First Space. 3. Some authentication requirements are needed, such as the First Space password/key, Second Space key, and fingerprint to enter the Second Space. 4. A USB Debug is required in the Second Space to be able to perform acquisition, USB Debug is not valid if it is only done in the First Space. 5. Additional processes can occur if problems are found during the acquisition process, such as rooting the mobile phone in certain circumstances, the process fails because the mobile phone sleeps, if the mobile phone sleeps, the Second Space will automatically lock the mobile phone will automatically open the First Space.

2.5   Acquisition Process

The acquisition process is carried out by connecting the Xiaomi Redmi Note 8 mobile phone to the MOBILedit Forensic Express Pro v7.4.0.20393 acquisition application; as previously explained that to carry out the acquisition process must go through two methods, namely, the First Space is acquired, and the acquisition is carried out in the Second Space. Process for acquiring Xiaomi devices with the MobilEdit application can be seen in Figure 8 [16]. Still, before making an acquisition, several requirements must be made, namely: activate developer mode to be able to activate USB Debugging; after USB debugging is activated, then activate the install application via USB; this is done to allow the mobile phone to install the connector application needed by the MobilEdit application, see Figure 8.

Figure 8: Install connector MobilEdit.

After the connector is successfully installed, the next step is to carry out the acquisition process in the First Space; the steps in this process include selecting what you will extract, configuring the results to select the output of the imaging file, filling in the extract result form, select the format of the extracted file, select the destination of the imaging result storage location and the last step is to wait for the imaging results to be completed. In this research, the extraction results are selected in the form of .pdf files, and the file analysis carried out by imaging is selected image files because this research aims to develop a framework. While the acquisition process until the extract results are obtained will not affect the file type, the difference from the file acquisition to imaging will depend on the size of the file; the larger the file size, the longer the imaging process will take, but for the procedure from the beginning until the extraction process is complete there is no difference. The results of the extraction file can be seen in Figure 9, and the .pdf report can be seen in Figure 10.

Figure 9: Imaging results with MobilEdit.

Figure 10: Report Pdf imaging results.

2.6 Evaluation

After analyzing the object of research, namely the unique features of the Xiaomi Second Space, and paying attention to the standards used in this study, it can be concluded that it is necessary to build a framework that can be utilized in carrying out the Xiaomi Second Space acquisition process. Considering the acquisition process guidelines from SNI ISO 27037:2014, the process is to the Xiaomi mobile phone situation. Still, it is necessary to add several approaches to the framework due to several circumstances. After doing some analysis on the Xiaomi Second Space, some additional requirements need to be considered in the acquisition process, namely:

1. To access the Second Space, we need: First Space password, MIUI account access, Second Space password, and fingerprint (if needed).

2. The Second Space is a very power-sensitive feature, if the acquisition is done in the Second Space, the mobile phone must be on. The acquisition process will fail because if the Second Space is off/sleep then the Second Space will automatically be locked and the process for acquisition must be repeated.

3. The settings in the First Space and the Second Space are different, this greatly affects the mobile phone settings where the required USB debug and application connectors must be installed in both Spaces.

4. To enable USB debugging in the Second Space, developer mode must be enabled in the First Space. Despite having different settings, the settings in the Second Space are not as complete as in the First Space. Some accesses such as developer mode are only available in the First Space.

Considering this, the researcher will develop an acquisition method in the Second Space. The acquisition process is based on SNI ISO 27037:2014; the acquisition process that suits the requirements of the Second Space is the acquisition process of active digital devices (clause 7.1.3 SNI ISO 27037:2014) by performing several additional functions according to the state of the mobile phone. The acquisition process is carried out using the MOBILedit Forensic Express Pro v7.4.0.20393 application; investigators can utilize this application to conduct easy-to-use mobile device acquisitions. This MOBILedit application has a connector that must be installed on the connected mobile phone with USB Debugging requirements and permission to install applications via USB [17].

This research produces two extraction files with different storage from one mobile phone, with the process repeated but with the same mobile phone, making the extraction results questionable. In general, a device that is analyzed will produce one extraction file; even though it has different file storage, it still produces one file after being extracted with the application, but it is different from the Xiaomi phone, which can separate the central repository with the Second storage when an analysis is carried out using the application to get the file being searched, the file cannot be found, there must be an additional process carried out to access the file stored in the Second Space. After analyzing the details of the First Space device and the Second Space, the difference in detailed properties can be seen in Figure 11.

From Figure 11. It can be seen that there are some differences from the device properties analyzed with the MobilEdit application. The same manufacturer description and the same

Device Properties	
Manufacturer	Xiaomi
Product	Redmi Note 8
HW Revision	RKQ1.201004.002
Platform	Android
SW Revision	11 (30)
Android ID	922f77786c951928
Serial Number	13cbf4ff
Device Time	2023-02-16 17:00:25 (UTC+7)
Manual Time	No
Time Zone	Asia/Jakarta
Manual Time Zone	No
Device Storage Encrypted	Yes
IMEI	863144045275213
Rooted	No
Communication Type	ADB Connector
SIM Card	No
SIM Card Country	Indonesia
Operator	3, MCC: 510, MNC: 89
Total Storage	48.9 GB
Used Storage	18.3 GB

Device Properties	
Manufacturer	Xiaomi
Product	Redmi Note 8
HW Revision	RKQ1.201004.002
Platform	Android
SW Revision	11 (30)
Android ID	f4756eae96ea2c64
Serial Number	13cbf4ff
Device Time	2023-02-16 17:44:10 (UTC+7)
Manual Time	No
Time Zone	Asia/Jakarta
Manual Time Zone	No
Device Storage Encrypted	Yes
IMEI	863144045275213
LACCID	LAC: 42087, CID: 145996320
Rooted	No
Communication Type	ADB Connector
SIM Card	Yes
IMSI	510897288697258
SIM Card Country	Indonesia
Operator	3, MCC: 510, MNC: 89
Total Storage	48.9 GB
Used Storage	18.5 GB

Figure 11: Analysis result device propoerties.

product, namely Redmi Note 8, but the Android ID has a different description [18], this is because the Second storage Space is a different storage as if the same mobile phone has been created with a different ID but has the same Hardware (HW) Revision [19], and the same serial number. In addition, the IMEI of the two identification results gives the same results, this indicates that the product being analyzed is the same product where the IMEI is the identity of a device where there is no same IMEI for each device [20]. In addition, in the device properties of the Second Space there is a description of LACCID which is not found in the device properties of the First Space [21], LACCID is a combination of LAC (Location Area Code) and CID (Cell ID) [22], LAC is a unique code of the detected location and can change while CID is a unique number or code that identifies the BTS (Base Transceiver Station) tower in the location area which can also change according to location [23]. In addition, there is IMSI (International Mobile Subscriber Identify) information which is the identity of the GSM network [24], the First three numbers 510 are MCC (Mobile Country Code) identifying that the network connected to the device is in Indonesia, and the next two numbers are MNC (Mobile Network Code) the identity of the operator connected, 89 is the identity for operator 3 (Three) [25].

3   Result

After analyzing the Xiaomi Second Space storage and determining suitable methodologies, this research yielded a method development for acquiring data within the Xiaomi Second Space to support the admissibility of digital evidence in court. The evaluation
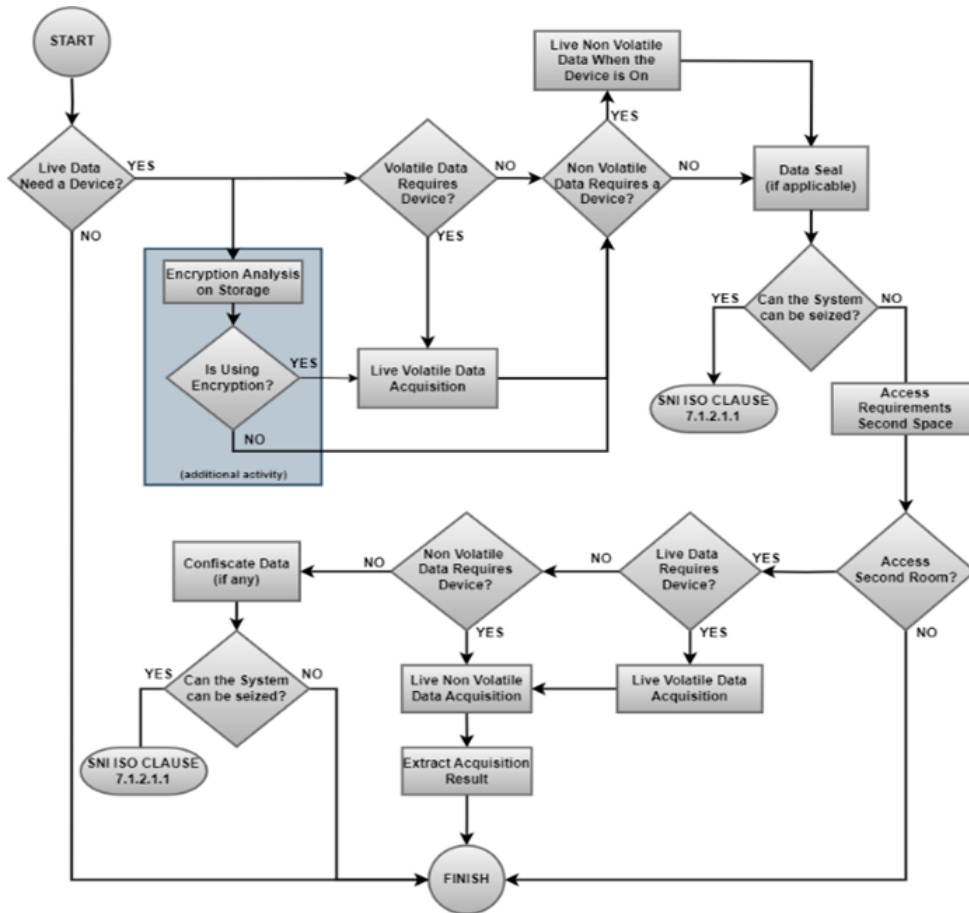
Figure 12: Proposed second space acquisition framework.

process determined the prerequisites required to develop the acquisition method, and the methodology employed was highly contingent on the device under scrutiny. In this study, a quantitative approach was utilized, involving formulating problem statements, hypothesis development, experimental design and execution, conclusion drawing, and result reporting.

The framework employed in this study was SNI ISO 27037:2014, an Indonesian digital forensic standard outlining guidelines for the identification, collection, acquisition, and preservation of digital evidence, adopted from ISO 27037:2012. The approach adopted in this research was Live Forensic, a process of digital device acquisition conducted while the device is powered on. This procedure was imperative as accessing the Second Space on Xiaomi devices is mandatory.

One of the applications used for Mobile Digital Forensics on mobile devices is MobilEdit Forensic Express Pro, which can acquire and generate image files from mobile devices. The requirements for accessing the Second Space were also detailed within this framework.

Currently, this framework cannot be universally applied to numerous types of phones, as the Second Space feature is exclusive to Xiaomi. However, there is a possibility that in the future, many mobile vendors will develop similar features. Hence, this research construction will aid researchers in acquiring insights into the specific Second Space feature. The developmental outcomes of the framework are illustrated in Figure 12.

Figure 12 is a proposed Framework that has been analyzed in each clause of SNI ISO 27037:2014 and is a contribution to this research; the framework built is a development of the SNI ISO 27037:2014 acquisition procedure where there are several additions in the SNI ISO 27037 procedure only one acquisition and imaging process is carried out by producing one extraction file, in contrast to the Second Space feature Xiaomi which will produce two extraction files with two acquisition processes on one mobile phone or mobile device. The additions contained in the acquisition procedure are:

1. Repeating the First process by enabling USB Debbug on the Second Space with developer mode access permission on the First Space.

2. Collecting data needed to access the Second Space such as the Second Space password and fingerprint.

Install the MobilEdit application connector on the Second Space by enabling the application to install via USB permission in the Second Space settings. The investigator can use this framework for some phones with special Second Space features, such as Samsung Knox, a special part built by Samsung to separate the main Space and the Second Space. This framework can also be used to anticipate the rapid development of technology, and there will be many possibilities that other cellphone vendors will provide special Second Space features.

4   Conclusion

After implementing the case and analyzing the SNI ISO 27037:2014 framework, it is concluded that the Second rack storage on Xiaomi phones has different specifications from other telephones held in the Second Space, has a different storage location from the First Space and separates RAM and ROM in different Spaces. The Second Space is a virtual machine built by Xiaomi developers to separate the Space on the primary storage, just like doing dual boot on a laptop, but there are differences in accessing it. When doing Space division on a laptop virtual machine, we can choose the size used in another Space, but in the Second Space, we cannot determine the storage size.

To perform the acquisition process in the First Space can be done with the acquisition process contained in the SNI ISO 27037:2014 standard, but to perform activities in the Second Space, some additional processes must be done. In carrying out the acquisition process in the Second Space, several requirements must be met, namely the First Space password, MIUI account access, Second Space password, and fingerprint (if needed), the Second Space is a feature that is very sensitive to power, if the acquisition is carried out in the Second Space, the mobile phone must be on. The acquisition process will fail because if the Second Space is off/sleep, the Second Space will automatically be locked and the process for acquisition must be repeated, the required USB debug and application connector must be installed in both Spaces, To enable USB debugging in the Second Space, you must activate the developer mode in the First Space.

After analyzing the Second Space, building a suitable case study, and adjusting to the SNI ISO 27037:2014 standard, the researcher created a framework based on SNI ISO 27037, as shown in Figure 12. The framework built is a development of the SNI ISO 27037 acquisition process clause 7.1.3, which is the acquisition process on a lit device. Several additional functions in the framework were built and contributed to this research, namely the process of accessing the Second Space to perform the acquisition. The further procedure is based on the analysis of the Second Space and the requirements needed to access the Second Space and adjusted to the application used. This framework was built using one test sample, namely the .Jpeg (image) format file, which was chosen because it is a file that is small enough to represent other files. The framework built can be used in the Second Space acquisition process on all files; the only difference is the file size, which will affect the acquisition process time in the application, but every operation carried out and the requirements needed are the same. The construction of this framework can help the DEFR carry out the Second Space acquisition process and have a strong legal basis for consideration before the trial. Investigators can also utilize this framework to search for digital evidence on other mobile phones with similar features. However, presently, this feature is only available on Xiaomi products.

References

[1] F. Yudha, E. Ramadhani, F. Rahma, and W. N. Hamzah, "Pendekatan dd sebagai salah satu teknik akuisisi perangkat android," *Cyber Security dan Forensik Digital*, vol. 3, no. 1, pp. 33–38, 2020.

[2] S. Madiyanto, H. Mubarok, and N. Widiyasono, "Mobile forensics investigation proses investigasi mobile forensics pada smartphone berbasis ios," *JRSI (Jurnal Rekayasa Sistem dan Industri)*, vol. 4, no. 01, pp. 93–98, 2017.

[3] M. P. Aji, D. Hariyadi, and T. Rochmadi, "Logical acquisition in the forensic investigation process of android smartphones based on agent using open source software," in *IOP Conference Series: Materials Science and Engineering*, vol. 771, p. 012024, IOP Publishing, 2020.

[4] F. E. Nastiti, N. D. Anggana, H. Gunawan, and U. Kristiana, "Akuisisi barang bukti digital pada smart cctv menggunakan standarisasi acpo dan sni iso/iec 27037: 2014," *Jurnal Informa: Jurnal Penelitian dan Pengabdian Masyarakat*, vol. 6, no. 2, pp. 23–27, 2020.

[5] V. Sargaiyan, M. Sapat, R. S. Yadav, S. Bhatele, S. S. Parihar, and A. H. Lanje, "Digital forensics," *Int. J. Oral Care Res.*, vol. 5, no. 4, pp. 335–337, 2017.

[6] D. Hariyadi and A. Akbarul, "Laron: Aplikasi akuisisi berbasis SNI 27037:2014 pada ponsel android," Unpublished, 2015.

[7] M. N. Faiz, "Studi komparasi investigasi digital forensik pada tindak kriminal," *Journal of Informatics Information System Software Engineering and Applications (INISTA)*, vol. 1, no. 1, 2018.

[8] I. Riadi, R. Umar, and I. M. Nasrulloh, "Analisis forensik digital pada frozen solid state drive dengan metode national institute of justice (nij)," *Elinvo (Electronics, Informatics, and Vocational Education)*, vol. 3, no. 1, pp. 70–82, 2018.

[9] D. Sudyana, B. Sugiantoro, and A. Luthfi, "Instrumen evaluasi framework investigasi forensika digital menggunakan sni 27037: 2014," *JISKA (Jurnal Informatika Sunan Kalijaga)*, vol. 1, no. 2, pp. 75–83, 2016.

[10] A. R. Supriyono, B. Sugiantoro, and Y. Prayudi, "Eksplorasi bukti digital pada smart router menggunakan metode live forensics," *Jurnal Infotekmesin*, vol. 10, no. 2, pp. 38–45, 2019.

[11] D. Hariyadi and I. Y. Pasa, "Identifikasi barang bukti percakapan aplikasi dual apps whatsapp pada ponsel xiaomi menggunakan metode nist mobile forensics," *INTEK Universitas Muhammadiyah Purworejo*, vol. 1, pp. 1–7, 2018.

[12] 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.

[13] M. M. A. S. Mushlich, M. A. Izzuddin, and M. Ridwan, "Analisis kinerja aplikasi forensik open-source pada ponsel cerdas berbasis android dalam mendapatkan bukti digital," *Jurnal Inovasi Informatika*, vol. 6, no. 2, pp. 86–97, 2021.

[14] U. Robustelli, J. Paziewski, and G. Pugliano, "Observation quality assessment and performance of gnss standalone positioning with code pseudoranges of dual-frequency android smartphones," *Sensors*, vol. 21, no. 6, p. 2125, 2021.

[15] R. Ruuhwan, I. Riadi, and Y. Prayudi, "Penerapan integrated digital forensic investigation framework v2 (idfif) pada proses investigasi smartphone," *JEPIN (Jurnal Edukasi dan Penelitian Informatika)*, vol. 2, no. 1, pp. 1–8, 2016.

[16] N. Nasirudin, S. Sunardi, and I. Riadi, "Analisis forensik smartphone android menggunakan metode nist dan tool mobiledit forensic express," *Jurnal Informatika Universitas Pamulang*, vol. 5, no. 1, pp. 89–94, 2020.

[17] M. Chopade, S. Khan, U. Shaikh, and R. Pawar, "Digital forensics: Maintaining chain of custody using blockchain," in *2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*, pp. 744–747, IEEE, 2019.

[18] A. Aldoseri, D. Oswald, and R. Chiper, "A tale of four gates,"

[19] A. Lutu, D. Perino, M. Bagnulo, E. Frias-Martinez, and J. Khangosstar, "A characterization of the covid-19 pandemic impact on a mobile network operator traffic," in *Proceedings of the ACM internet measurement conference*, pp. 19–33, 2020.

[20] W. A. Hammood, R. Abdullah, O. A. Hammood, S. M. Asmara, M. A. Al-Sharafi, and A. M. Hasan, "A review of user authentication model for online banking system based on mobile imei number," in *IOP Conference Series: Materials Science and Engineering*, vol. 769, p. 012061, IOP Publishing, 2020.

[21] W. A. Hammood, R. A. Arshah, S. M. Asmara, and O. A. Hammood, "User authentication model based on mobile phone imei number: a proposed method application for online banking system," in *2021 International Conference on Software Engineering & Computer Systems and 4th International Conference on Computational Science and Information Management (ICSECS-ICOCSIM)*, pp. 411–416, IEEE, 2021.

[22] A. Yudhana, A. Fadlil, M. R. Setyawan, *et al.*, "Analysis of skype digital evidence recovery based on android smartphones using the nist framework," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 4, no. 4, pp. 682–690, 2020.

[23] I. Zuhriyanto, A. Yudhana, and I. Riadi, "Analisis perbandingan tools forensic pada aplikasi twitter menggunakan metode digital forensics research workshop," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 4, pp. 829–836, 10 2020.

[24] S. Qin, J. Man, X. Wang, C. Li, H. Dong, X. Ge, *et al.*, "Applying big data analytics to monitor tourist flow for the scenic area operation management," *Discrete Dynamics in Nature and Society*, vol. 2019, 2019.

[25] F. Al Rasyid and B. P. Zen, "Dead forensic analysis of qutebrowser and librewolf browsers using the nist 800-86 method," *Jurnal Teknik Informatika (Jutif)*, vol. 4, no. 5, pp. 1009–1019, 2023.