UNIVERSITY OF CENTRAL OKLAHOMA

JACKSON COLLEGE OF GRADUATE STUDIES

THIRD-PARTY APPLICATION BURNER PHONE ANALYSIS

A THESIS

SUBMITTED TO THE GRADUATE FACULTY

in partial fulfillment of the requirements for the

Degree of

MASTER OF SCIENCE IN FORENSIC SCIENCE – DIGITAL FORENSICS

By

MAGALI HERNANDEZ
Edmond, Oklahoma
2025

THIRD-PARTY APPLICATION BURNER PHONE ANALYSIS

By: MAGALI HERNANDEZ

A THESIS

APPROVED FOR THE W. ROGER WEBB FORENSIC SCIENCE INSTITUTE

Dr. Mark McCoy Committee Chairperson

Ms. Rachael Elliott Committee Member

Dr. Grace Park Committee Member

Acknowledgements

First and foremost, I would like to thank Professor Elliott for taking the time to guide me through this process. Although this whole process was unfamiliar to me, with Professor Elliott's guidance, I was able to accomplish it. I also want to thank Dr. McCoy and Dr. Park for taking the time to be a part of my committee.

I want to give a huge thank you to my fiancé and my two boys for supporting me through this journey. Thank you to my parents and my in-laws for being there for me and being a part of my journey.

Abstract

In today's day and age, how people communicate is changing. Communication is often done using cell phones, specifically among users through multiple third-party applications. Although the options available to communicate are endless, they are also becoming a very dangerous tool. A third-party communication application is an application that is downloaded by a user to communicate with friends and family or socialize, separate from the mobile device text messaging. However, third-party applications are often used in criminal activities. Users' need for privacy also pushes manufacturers to improve and impose strong security features in their software. These improvements make forensic examinations and recovery of such data on mobile devices more difficult. This study explores the recovery of data from disposable numbers offered by the Burner application. The mobile devices utilized in the study differentiate in operating systems to compare data recovered in an Android operating system and an iOS operating system. Within the Burner Application, three lines will be used to exchange messages, photos, and videos. Data extraction and parsing will be conducted with Cellebrite UFED 4PC version 7.73.0.68 and Cellebrite Physical Analyzer Inseyets version 10.5.0.1016. The research demonstrated that the different operating systems contribute to how much data is recovered. In this study, the amount of data recovered from the Apple iPhone 15 Plus, an iOS device associated with the Burner application, was more significant than the Samsung Galaxy S23 Ultra, Android operating system. Future research should utilize various Android devices as they differ based on manufacture and service provider. Data associated with the Burner application is recoverable depending on the operating system. Using different mobile devices forensic tools could also yield different results. This research applies methods for recovering disappearing messages to recover digital artifacts created by Burner's disposable number feature, an area not previously studied or published.

Table of Contents

List of Figures

List of Table

Introduction

A burner phone is a mobile phone with a temporary disposable number. Burner phones are used to avoid contracts with specific cell phone providers, keep personal numbers private, and for illicit purposes, such as criminal activities (Hanna & Wigmore, 2022). Once a user is done with the burner phone, they can discard it, which is the end of that phone number. Burner phones can range from inexpensive to costly. On average, burner phones can cost between $15 to $150. Like everything, there are advantages and disadvantages to using burner phones; for instance, keeping personal information private is an advantage. On the downside, it sometimes requires carrying two devices versus one, a personal phone and a burner (Ramirez, 2025). The Burner application provides the functionality of a burner phone without having to purchase a secondary phone. The application allows users to have more than one disposable number while keeping their personal contact information private, all on the same device.

Technology advancement has had a significant impact on communication. Communication has gone from in-person, snail mail, and fax to telephonic to text message communications (Kavaturi, 2023). Although one would think that text messages would be enough, the need for private messaging is in high demand. Privacy in private messaging allows users to have more control. It also gives consumers peace of mind that their communication and information are not easily accessible to hackers by having end-to-end encryption. Privacy in private communication gives users more discretion when using communication applications. Private messaging is crucial for some users, whether that be for criminal activity, working-related reasons, or simply private use. A text message sends electronic messages between two or more mobile devices. Private messaging allows users to communicate in real-time through a software application (Chantel, 2023). Different messaging applications have been developed to

allow people to communicate and keep their personal numbers private. For example, Facebook, Snapchat, and Instagram are social media platforms providing instant user communication. Facebook and Instagram offer end-to-end encryption and their own form of disappearing messages. Facebook allows users to select their messages to be on a timer and disappear once time has lapsed (Meta, 2025). Instagram offers a vanish mode, which deletes the message after it has been seen or once the chat has been closed (Meta, 2025). Snapchat is different because it provides more privacy because of its known feature of messages being deleted after being read and photos expiring as the timer has run out (Snap Inc, 2025). Social media platforms are not private enough for businesses and users who want increased privacy. From a business perspective, client information and communication are meant to be private and confidential. Using a communication platform that offers privacy and protection would be ideal, leading businesspeople to seek third-party applications that would fulfill those requirements. Not all social media platforms offer end-to-end encryption; they are designed to keep users connected with their friends and family. This created the need for applications like WhatsApp and Burner to provide security.

This literature review will address the relationship between technology in crime and private communication applications. The first section will address the relationship between technology and crime. The second section will discuss forensic analysis and extraction in other private communication applications with similar security features. Lastly, section three will discuss the security features of the Burner app and why digital forensic investigators need to know how to analyze and extract data forensically.

Literature Review

Technology in Crime

Prior to the 1990s, drugs would be sold in specific locations, making it easier for suppliers and customers to have access. Before technology, drug dealers would sell drugs in "open-air markets," which at this time would be public places (Moyle et al., 2019). Now, with technology, drug dealers no longer need to be in one place. Deals can be anywhere at any given time. Locations are now more discrete and private, also known as "closed" markets or "lounge room dealing (Moyle et al., 2019)." With the click of a button, a drug dealer's potential customer can send a message requesting what type of product they want. Technology has allowed drug dealers to expand their business, become more accessible, and move more product. Before, a consumer would need to have some connection in order to have access to drugs. Now, technology allows consumers to make quick connections but also have multiple connections, making it easier to have access to drugs.

Moyle et al. conducted a study to demonstrate the ways applications like Snapchat, Instagram, and WhatsApp are utilized to access and supply drugs. This study gave more of an understanding of the motivations, barriers, and anxieties of users who choose to use or are thinking of using an app to get access to drugs. This study conducted an online survey, rapid face-to-face, and in-depth interviews. A sample size of 358 users was used; 228 indicated they were app users, and 70 indicated they would consider using an app.

Qualitative research in this study demonstrated that customers prefer to make a transaction anonymously to avoid any problems arising from an in-person transaction. The most common reason users opted to use a third-party application as their source to access drugs was because it

is easier to organize a transaction. This study examined multiple private messaging applications and identified their security features, security issues, and drug supply facilitation methods.

The study used the following applications: Snapchat, Instagram, Wickr, WhatsApp, Kik, Telegram, Facebook Messenger, Tinder, Whisper, Grinder, and Yik Yak. Many applications, such as Instagram, Tinder, Whisper, and Grindr, offer no security features. Applications like Wickr, WhatsApp, Facebook, and Telegram offer end-to-end encryption for messaging. Overall, each of the applications selected has other security features, such as disappearing messaging, while others share information with parent companies and/or third-party advertising companies. Kik, Tindr, and Grinder kept track of IP addresses, and Whisper kept a rough map of the user's location even if their geo-location services were off. An ephemeral message, also known as a disappearing message, is a multimedia message sent by a mobile device received by the recipient and deleted after being viewed (Heath et al., 2023). Different kinds of mobile phone applications are used to connect with drug suppliers. Users gain access by connecting with pre-existing customers and using emojis to signify a supplier's account (Moyle et al., 2019). Mobile phone applications are a popular form of communication in today's society. Users use applications like Snapchat, Instagram, and WhatsApp either because they simply have access to that particular application or because they do not want to use their personal phones to communicate.

Difference in Applications

In 2020, WhatsApp released its 'Disappearing Messages' feature for its platform (Heath et al., 2022). WhatsApp also offers end-to-end encryption, chat lock, silence unknown callers, encrypted backups, and much more (WhatsApp LLC, 2025). Although the disappearing messages are meant to give users more privacy, the sender and recipient cannot be guaranteed to be the only ones to see the messages. The methods used to preserve disappearing messages, such

as replying to or, forwarding or altering the original data, are not ideal for a forensic examination and are an Association Chief Police Officers (ACPO) guidelines violation.

Instant messages have become a popular form of communication. It is inexpensive and does not require a SIM card like regular text messages. A few popular instant message communications are WhatsApp, Facebook Messenger, and WeChat. WhatsApp's Disappearing Messages feature gives its users more privacy by allowing them to have their messages "deleted" after a specific period. They can select from 24 hours, seven days, or 90 days. More recently, other popular instant communication applications have followed with their own 'Disappearing Messages' features, such as Instagram and Facebook. Instagram offers a vanish mode; the message will disappear once the message is seen or when the user closes out of the chat. Facebook allows the user to select a timer for the message, and the message will disappear after the time has expired.

In the Heath et al. study, researchers seek answers to the question of 'disappearing messages' and how they can be forensically recovered, how they work, and their impact on criminal investigation for forensic investigators. This study used tools such as Cellebrite's UFED 4 PC version 7.50.0.137 - 7.52.0.152, MSAB's XRY, and Magnet's AXIOM version 5.6.0.26839 on Android, Apple, and Windows devices to see what data they can recover. WhatsApp was the primary focus of the study, but they also analyzed data recovered from Snapchat and Telegram. This study involved seven groups, all using different messaging applications, and four images and videos were created. Two images and two videos were used for each group. A pre-disappearing extraction was completed and compared with post-disappearing extractions for all groups.

Group 1 analyzed WhatApp's treatment of disappearing messages. It used XRY and Cellebrite software to compare recovered data results on both pre-and post-disappearing messages on iOS and Samsung devices. XRY and Cellebrite had better results in recovering disappearing messages on iOS than Samsung. In the pre-disappearing stage, XRY had a 50% success rate, and Cellebrite had a 75% success rate. In the post-disappearing messages stage, XRY could not recover any messages, and Cellebrite could only recover 42% of the messages. A manual review of the data through Cellebrite's built-file system browser and database viewer was able to recover the expiration timestamp. It also proves that the expiration timestamp is stored in the application's database and does not require an internet connection to recover the expiration timestamp. Overall, Cellebrite recovered more messages, videos, and photos than XRY.

In group 2, WhatsApp's rollforward disappearing date method was tested. This method determined whether the disappearing timer works based on a server or localized timestamp check. The time was changed to the time the messages were set to disappear. Forcing the time to change forward caused a forced wipe. Cellebrite UFED 4PC was used to extract data from iOS and Samsung devices. After the forced wipe, there was no data recovery on disappearing messages on iOS. Only messages and system messages set on standard settings were recovered. Cellebrite UFED 4PC could recover more data, including message data, but not the attachment data from Samsung.

In group 3, WhatsApp's rollback disappearing date method was tested. For this method, messages were allowed to expire. After messages expired, the phone system clock was rolled back for both iOS and Samsung. After rolling back time, 100 percent of the data created before the expiration time was recovered. WhatsApp does not have any procedure regarding rolling

back the time after the expiration time. It also determined that if isolated from the network, the application relies on a localized clock.

Group 4 used UFED Cloud Analyzer to recover disappearing messages from WhatsApp Cloud and Google Drive/iCloud backups. The backups are created after messages have been created. This method also requires a connection to the network, which is not a common practice. Post-disappearing messages were not recovered, but in the pre-disappearing stage, some data was recovered: time/date sent or received, but the actual content of the messages was not.

Group 5 tested whether performing a live acquisition (RAM dump) on a WhatsApp Desktop computer with disappearing messages enabled provides any forensic benefit. A memory dump was taken pre- and post-disappearing messages. During the analysis, a few file paths were identified as interesting: Root/Users/%USER%/AppData/Local/WhatsApp/. This path contained files pertaining to installation and updates files and the setup log "SquirrelSetup.log." No data was found. The path Root/Users/%USER%/AppData/Roaming/WhatsApp contained databases, cache folders, cookies, and main-process log files. The "databases.db" contained no message data, only a table with mmap_status, version, and last compatible version. The Root/Users/%USER%/AppData/Roaming/WhatsApp/LocalStorage/leveldb/000003.log path contained a lead to a file of interest. The log file did not contain any message but contained what appeared to be keys that encrypt/decrypt messages and data identify devices that were paired with the application. The data recovered with this method was very limited. This method is ideal for law enforcement in cases where a suspect is caught in the act of viewing or sending material and the device is still active.

Group 6 performed a standard mobile extraction on the device, focusing on both 'unsaved' and 'saved' messages from Snapchat on iOS and Samsung. Data extraction from iOS

was unsuccessful, while the Samsung device recovered all but three artifacts: one timed photo and two messages. The Samsung device recovered data regardless of whether or not the messages were saved. The iOS device has more success when it comes to data sanitization than a Samsung device.

Group 7 performed a standard mobile extraction on Telegram to see whether messages or data can be recovered in 'secret' mode. In an iPhone, no chats were recovered; only application data was collected in both regular chat and 'secret' chat. The "preferences.plist" file was recovered but contained no data related to the disappearing messages. On the Samsung device, regular chat was recovered, limited data was recovered from the 'secret' chat, and incorrect metadata was also recovered. (Heath et al., 2022).

This study demonstrates that disappearing messages will be a challenge to digital forensic investigators and the importance of being up to date on the new security features of these applications. This demonstrates that operating systems behave differently and impact how much data can be recovered. Although this study is not associated with burner third-party applications, it has a similar concept that could be applied to recovering data from a burner third-party application.

Mobile Forensics: Burner

As the world becomes more digitized, people are becoming more dependent on their mobile devices to communicate. That said, instant messages have become a popular form of communication. Statista reported that as of February 2025, the most popular mobile messenger applications are WhatsApp, Weixin/WeChat, Facebook Messenger, Telegram, Snapchat, and QQ (Ceci, 2025). Application developers constantly update their applications to improve features and become more secure as private messaging applications become more popular.

In 2012, Ad Hoc Labs released an application called Burner. To date, the Burner application has been downloaded by 10 million consumers (Ad Hoc Labs, 2025). This application aims to keep personal numbers private by creating disposable numbers with an expiration date. With Burner, users can make calls and send text messages by purchasing credits (Etherington, 2012). Since Burner's release in 2012, the platform has changed users' options to utilize multiple disposable numbers and switch between numbers. Both iOS and Android users can purchase credit, which can be used to extend the life of temporary numbers, also known as Prepaid Burner. The Prepaid Burner numbers are meant to only last fifty (50) minutes and one hundred (100) texts and auto-burns in 30 days. Android and iOS devices have multiple subscription options; there are one-line, three-line, and ten-line options and a standard or premium option (Burner, 2025). The Burner application offers passcode protection. This is a separate passcode from the device passcode. It also offers unlimited calls and texts, mute and block numbers, and, most importantly, can delete numbers when done using them (Burner, 2023). Although Burner is not one of the top applications of 2024, it is still commonly used to communicate. Today's society believes no bad thing can come from using an application; however, there are inevitably users who intend to use these applications for illicit purposes.

In March 2022, the Federal Information & News Dispatch LLC reported about Matthew Anthony Marshall defrauding $2.3 million from a Montana investor. Marshall pleaded guilty to wire fraud, money laundering, and tax evasion with a sentence of six years in prison. Marshall claimed to be a former Recon Marine and CIA operative who defrauded John Doe by convincing Doe that Marshall needed funds for a CIA rescue mission. John Doe hired Marshall in the Spring of 2013. Marshall used lies, fake emails, and fake text messages to deceive John Doe. In three years, John Doe wired payments totaling $2,355,000. Marshall created phony text messages from

former CIA Officer Cofer Black. These messages were created through the Burner application. Marshall created two Virginia phone numbers to "receive" messages (Washington: Federal Information & News Dispatch, LLC, 2022). Details of how the data was recovered were not revealed in this article.

Goldstein et al. report that a dozen financial firms, as well as eight major Wall Street banks, were fined for not ensuring that their employees were using proper communication channels. Federal law requires financial firms and Wall Street banks to maintain records of employees' work-related messages. Sixteen firms, including five affiliates of the large banks, were fined $1.1 billion. It was discovered that between 2018 and 2021, bank employees communicated with WhatsApp and other third-party applications to avoid using work communication outlets. Banks must preserve communication correspondence, which is challenging when employees use third-party communication applications. Failure to keep accurate records could result in severe penalties (Goldstein et al., 2022).

Business Wire informs us that Burner offers iOS and Android users MMS support. This feature allows Burner users to send and receive to all U.S. and Canadian carriers. Burner offers a "Today" extension that allows users to separate contact lists from each line, a Touch ID-based privacy lock, and custom colors. Greg Cohn, co-founder and CEO of Burner, states, "We're seeing a huge expansion in use cases for secondary numbers, especially given the growth of online marketplaces and sharing-economy services." Burner also offers a Chrome extension allowing users to access Burner numbers online. Burner is designed to keep personal numbers private and create a temporary number that can be used for voice, SMS, and MMS (Business Wire; New York, 2014).

Summary

Humphries et al. said, "There have been several challenges which have grown due to technological advances: stronger security and the need for privacy of large quantities of data, new applications, and sensors" (Humphries et al., 2021). As a result of how fast technology advances, developers are constantly improving their applications. If not, a developer is trying to create an application that is better than anything else. Privacy has become very important for users. Privacy gives users peace of mind, and they can handle their business without worrying whether someone will have access to their private information.

Furthermore, private communication applications are becoming increasingly popular. Users communicate through private communication applications and social media, including but not limited to Facebook, Snapchat, WhatsApp, Telegram, Signal, and Burner. Users are also not just using one application to communicate. They communicate directly through mobile devices, social media, and private communication applications. One thing all of these social media and private communication applications have in common is that they have been keeping up with the demands of users and staying up to date with new technological advancements. Most social media and private communication applications have been designed or redesigned to offer end-to-end encryption, disappearing messages, self-destructing messages, and other privacy features. Studies have demonstrated that data recovery is possible when messages disappear from these applications. Still, contributing factors could impact the amount of data recovered from applications with disappearing message features.

Digital forensic examiners must familiarize themselves with all applications and security features within a mobile device and application. Digital forensic examiners never know what kind of device or application could become crucial in an investigation. Only some of these

applications can be forensically analyzed, especially if their security features are far more advanced than some of their counterparts. The Burner application is similar to other communication applications, but it differs because of its disposable number feature. Knowing whether messages can be forensically recovered after the disposable number has been deleted is essential. It is also important to determine if having multiple disposable numbers impacts how data is stored and if it can be forensically recovered.

Statement of the Problem

At the time of writing, only a few studies were published regarding the recovery of disappearing messaging. There were no studies regarding the recovery of data from disposable numbers offered by Burner. Compared to many third-party messaging applications, Burner allows users to use a number for as long as they need and dispose of it. This study aims to use the fundamental concept of recovering disappearing messages and apply it to recovering digital artifacts generated by the disposable numbers feature.

Research Questions

The research questions to be addressed are as followed:

1. Can data be recovered from using the Burner application that offers disposable numbers?
2. Does using multiple lines at the same time affect how data is recovered?
3. Does burning of a number eliminate the data stored?
4. Does having an Android device or iOS device affect data recovery?

Methodology

This study aimed to analyze digital artifacts recovered from the Burner application on a Samsung Galaxy S23 Ultra with Android OS version 14 and an Apple iPhone 15 Plus with iOS version 18.3.1. The primary concern with using this application is that data is not recoverable.

This study used a new Seagate Backup Plus Slim 2TB hard drive. A full format was done to remove any residual data from the hard drive. A factory reset was done on the Samsung Galaxy S23 Ultra to return the phone to its original state, thus removing all user data and user-installed applications. The Apple iPhone 15 Plus was used without completing a factory reset. The Apple iPhone 15 Plus contained all data and installed applications prior to and during the experiment. Cellebrite UFED 4PC version 7.73.0.68 was used to acquire mobile acquisitions of both mobile devices. Cellebrite Physical Analyzer Inseyets version 10.5.0.1016 was used to parse data in each extraction.

An email was created to set up the Samsung Galaxy S23 Ultra: thesisproject2025@gmail.com. Once the Samsung Galaxy S23 Ultra was set up, the Burner application version 5.13.0.2530.5929016 was installed. The Galaxy S23 Ultra did not have a cellular plan and relied solely on Wi-Fi connectivity for service. The email thesisproject2025@gmail.com was also used to create an account on the Burner application. A monthly subscription for three lines was selected in the Burner application setup. Phone numbers were then selected; (405) 645-3492 and (210) 610-7460 were the first two numbers used. The phone number (405) 320-9589 will be the third phone number for the Samsung Galaxy S23 Ultra that will be activated once one of the current phone numbers is "burned."

The iPhone 15 Plus was already in use; therefore, it has an active cellular service. The Burner application version 5.14.1 was installed. The active number on the iPhone 15 Plus was

used to create an account on the Burner application. Once the account was created, a monthly subscription for three active lines was selected in the Burner application. Two numbers were selected: (405) 645-3559 and (726) 247-0113. The third number, (405) 279-9945, will later be activated on the Apple iPhone 15 Plus once one of the current phone numbers is "burned."

Once the phone numbers were selected, a total of fifty (50) messages, including ten (10) photos and ten (10) videos, were exchanged between the Samsung Galaxy S23 Ultra and the Apple iPhone 15 Plus per number using the Burner application. During the exchange of messages, photos, and videos, it was discovered that the Samsung Galaxy S23 Ultra could not send videos but could receive them. Because of this feature, the Samsung Galaxy S23 Ultra sent ten (10) images per number. The Apple iPhone 15 Plus had the capability to send videos in high-quality resolution via a link or low-quality resolution via message. The Apple iPhone 15 Plus sent ten (10) videos per number. Since the Samsung Galaxy S23 Ultra cannot send videos, it only sends photos to the Apple iPhone 15 Plus.

Once the two active phone numbers from the Samsung Galaxy S23 Ultra and iPhone 15 Plus reached 50 messages exchanged, one number was "burned" while the other line remained active. After the second number was "burned," a new line was activated: (405) 320-9589 for the Samsung Galaxy S23 Ultra and (405) 279-9945 for the Apple iPhone 15 Plus phone number, (405) 645-3492 and (405) 645-3559 are not burned but remained active, messages were no longer exchanged. The two new active lines exchanged fifty messages, including ten (10) photos and (50) videos. This information can be seen in Table 1 below.

Table 1:

List of numbers select for each device and status of numbers

Galaxy S23 Ultra Numbers	Status	iPhone 15 Plus Numbers	Status
(405) 645-3492	Active	(405) 645-3559	Active
(210) 610-7460	BURNED	(726) 247-0113	BURNED
(405) 320-9589	Active	(405) 279-9945	Active

Data Acquisition

In order to obtain an acquisition, Cellebrite UFED PC version 7.73.0.68 was used, while a physical acquisition is ideal but is not supported for either Samsung Galaxy S23 Ultra or Apple iPhone 15 Plus. A physical acquisition is only possible for the Galaxy S23 Ultra if the device is rooted, and rooting the device was not attempted due to the risk of wiping the phone's data. As a result, the device was not rooted. Both the Samsung Galaxy S23 Ultra and the Apple iPhone 15 Plus were disconnected from the network before the extraction; cellular connectivity, Bluetooth, and Wi-Fi were disabled, and airplane mode was enabled. Original cables used to charge mobile devices were used in the acquisition process. All acquisition files generated from the acquisition were stored on the Seagate Backup Plus Slim 2TB hard drive.

On the Samsung Galaxy S23 Ultra, an advanced logical and filesystem acquisition using Android backup was done. On the Apple iPhone 15 Plus, a logical acquisition and an advanced logical (filesystem) acquisition were done. Acquisitions were opened in Cellebrite Physical Analyzer Inseyets version 10.5.0.1016 for further analysis.

Galaxy S23 Ultra Results

The device data and device data file from the first extraction on the Galaxy S23 Ultra was thoroughly analyzed. It was discovered that no artifacts of the Burner application were detected. Summary of Samsung Galaxy S23 Ultra results can be seen below in Table 2.

Table 2:
Summary of Samsung Galaxy S23 Ultra Results

Artifacts Recovered	Messages	Photos	Videos
(405) 645-3492	None	None	None
(210) 610-7460	None	None	None
(405) 320-9589	None	None	None

A second acquisition was performed on the Galaxy S23 Ultra to verify the first acquisition results. The analysis of the second acquisition also showed that no digital artifacts associated with the Burner application were recovered. A thorough analysis was performed on the Galaxy S23 Ultra's file systems to determine if any databases associated with the Burner application were recovered. No databases were recovered, so a manual verification could not be conducted.

Samsung's foundation includes a secure hardware supply chain and manufacturing practice. Samsung Knox provides a strong security guarantee built on Samsung's foundation. Samsung Knox was introduced in 2013 by Samsung, an innovative mobile security platform that provides business-ready Android devices. Samsung Knox aimed to capitalize on mobile technology while maintaining control and protecting data. Since its introduction, Samsung Knox has been evolving in terms of technological advancement and consumer needs.

One of Samsung Knox's features included restricting unauthorized access and actions (Samsung, 2025). Samsung Knox security could be a factor in why data recovered from the Samsung Galaxy S23 Ultra was limited. A physical extraction could have recovered more data, but Samsung Knox has created an obstacle that limited the extractions to advanced logic and filesystems using Android backup. No information was found regarding the security features the Burner application uses. However, suppose its focus is to provide consumers with a safe and secure communication application. In that case, their security feature could likely factor in the amount of data recovered from the Samsung Galaxy S23 Ultra.

iPhone 15 Plus Results

After analyzing the parsed data associated with Apple iPhone 15 Plus, digital artifacts associated with Burner were found. At first, the only information found was that the application was installed, along with log entries and databases. The Burner application was detected as an installed application categorized under spoofing and social networking.

Within Cellebrite there is an "AppGenie" feature, which is a post-processing feature. AppGenie is a research tool that tries to automatically identify specific artifact types from device databases (Cellebrite, 2025). The data parsed from the AppGenie feature was verified by comparing the data found and manually verifying what it found on the iPhone.

Conversations from the Burner application were recovered. It appears that two numbers were recovered. The phone numbers recovered were the sender or the recipient. Cellebrite recovered 50 messages and detected 20 attachments. Summary of Apple iPhone 15 Plus results see Table 3 below. After further analyzing the conversations, although Cellebrite detected the attachments, the photos and video content were not recovered. See Figure 1 for message excerpts recovered but no photos or videos and Figure 2 for excerpts of attachments detected from iPhone

15 Plus. Messages that were recovered were also classified as "deleted" and "Message Deleted Reason: Unknown."

Table 3:

Summary of iPhone 15 Plus Results

iPhone 15 Plus Numbers (sender)	**Galaxy S23 Ultra Numbers (recipient)**	**Messages**	**Attachments**
(405) 645-3559	(405) 645-3492	50 Recovered	20 Detected/Not Recovered
(726) 247-0113	(210) 610-7460	Not Recovered	Not Recovered
(405) 279-9945	(405) 320-9589	50 Recovered	20 Detected/Not Recovered

Figure 1:
Excerpts of messages recovered from iPhone 15 Plus

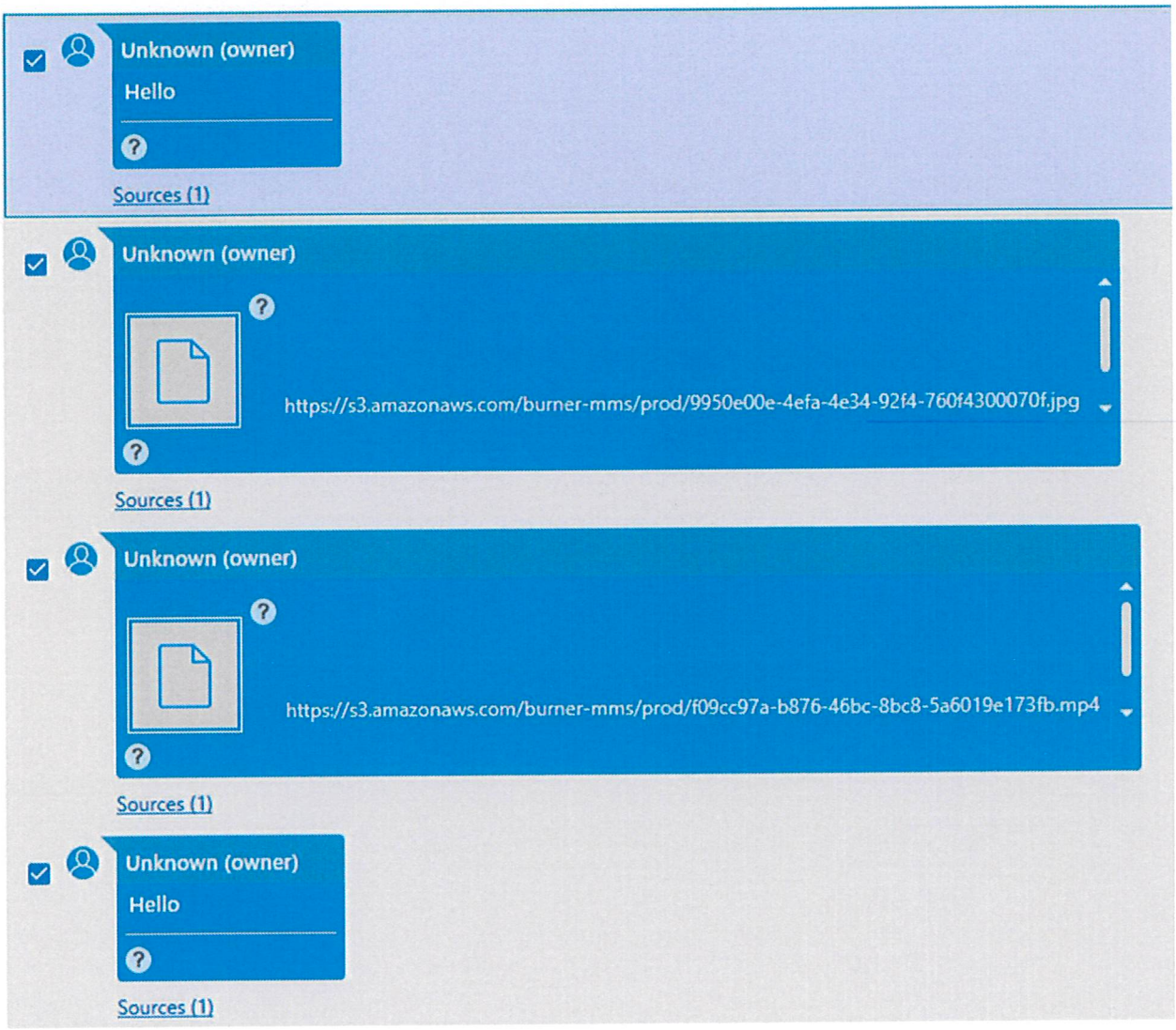
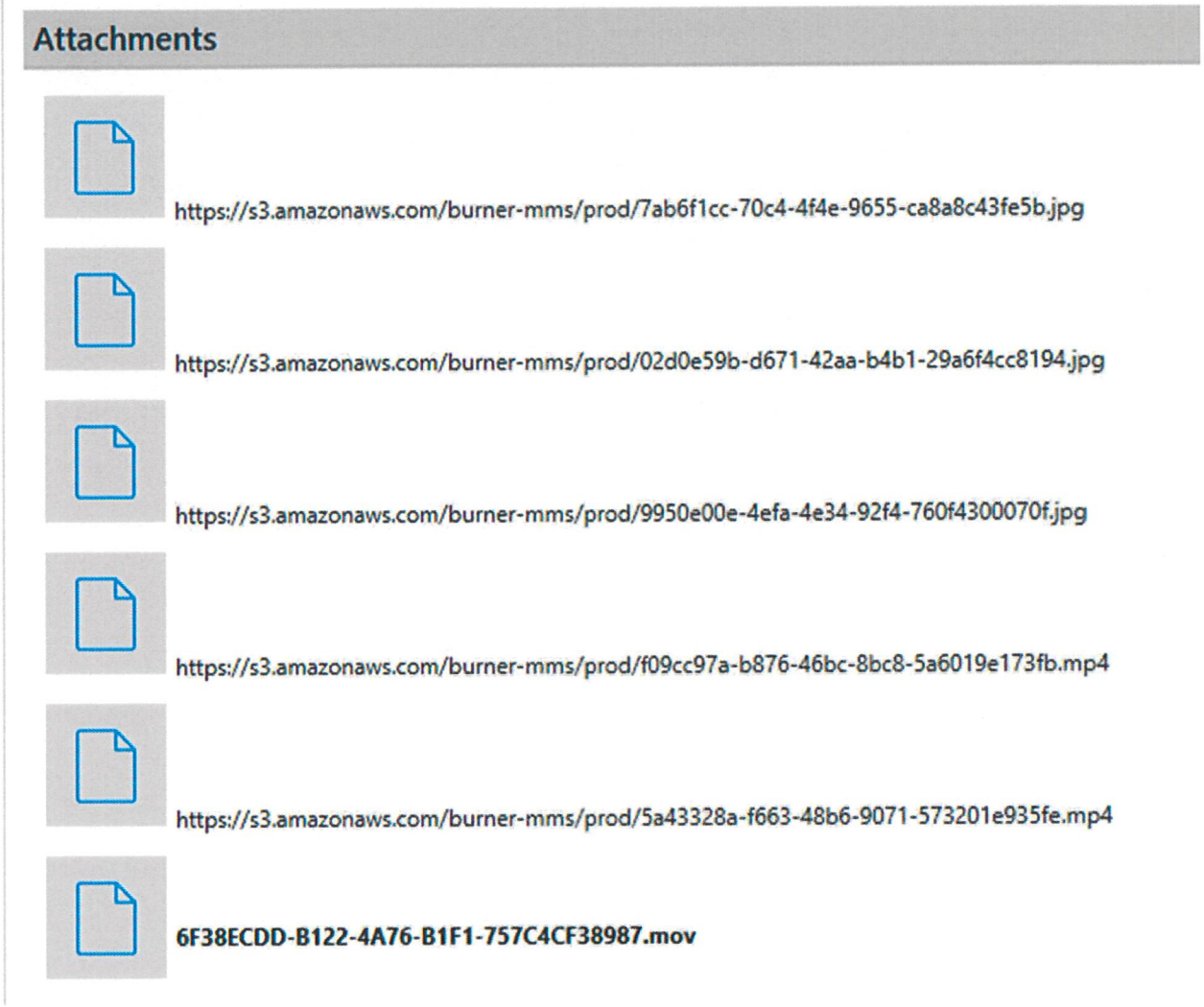


Figure 2:
Excerpts of attachments detected from iPhone 15 Plus



To validate the data parsed, a manual examination of the databases associated with the Burner application was conducted. A few databases contained data; see Figure 3 for databases associated with the Burner application. From this analysis, another file of interest is "group.adhoclabs.Burners.plist." The data contained within this file is a path, domain, iTunes backup original file name, and encryption key. The Phoenix.sqlite database contains data relevant to this study, a table, ZMESSAGE, which contains the data that verifies the data parsed. Using Cellebrite's SQLite wizard feature, a select query was generated using the ZMESSAGE table

within the Phoenix.sqlite database. SQLite Wizard visually decoded the raw data from the Phoenix.sqlite database. An SQLite query was built, and the database field was mapped to a physical analyzer model. Then, A .csv report was generated from the query. See Figure 4 for an excerpt of .csv report with data generated from Phoenix.sqlite database from iPhone 15 Plus. The data manually verified included time created, body, asset URL, contact ID, and conversation ID.

Data recovered from the database pertinent to this study included the time created; the time created matched the date and time the messages were sent and received. The body contained the messages that were exchanged. High-resolution videos were sent as a link, and the link was recovered within the body. The Burner application utilizes an asset URL, a website linked to the photo or video sent, which is stored in the Burner application's server. The link associated with the photo or video includes a permanent URL that remains the same. The file name of the photo or video is the only change with the asset URL. If the photo or video was not successfully sent, an asset URL is not generated, and the filed name is the only thing recovered. In order to do the extraction, the Apple iPhone 15 Plus was disconnected from the next work, which could factor in why the content of the attachment was not recovered and only an asset URL.

Figure 3:
Databases associated with Burner application

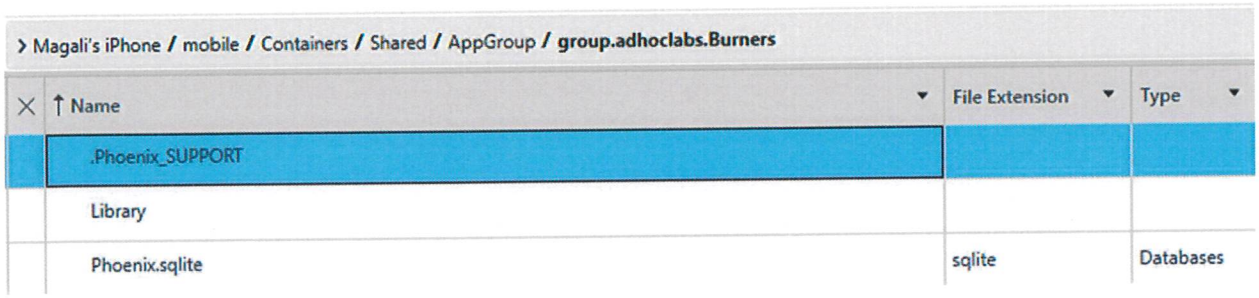


Figure 4:

Excerpt of .csv report with data generated from Phoenix.sqlite database from iPhone 15 Plus

ZDATECREATED	ZBODY	ZASSETURL	ZCONTACTID	ZCONVERSATIONID
12/8/2024 8:45:36 PM(UTC-6)	Hello		+14056453492	+14056453492
12/11/2024 8:45:35 PM(UTC-6)	How are you doing		+14056453492	+14056453492
12/11/2024 8:47:38 PM(UTC-6)	I'm doing well. How are you doing??		+14056453492	+14056453492
12/11/2024 8:47:38 PM(UTC-6)	I'm doing well as well.		+14056453492	+14056453492
12/11/2024 8:48:58 PM(UTC-6)		https://s3.amazonaws.com/burner-mms/prod/7ab6f1cc-70c4-4f4e-9655-ca8a8c43fe5b.jpg	+14056453492	+14056453492
12/11/2024 8:50:05 PM(UTC-6)		https://s3.amazonaws.com/burner-mms/prod/02d0e59b-d671-42aa-b4b1-29a6f4cc8194.jpg	+14056453492	+14056453492
12/11/2024 8:50:57 PM(UTC-6)	Did you see the news today?		+14056453492	+14056453492
12/11/2024 8:56:43 PM(UTC-6)	No. Anything interesting?		+14056453492	+14056453492
12/11/2024 8:57:29 PM(UTC-6)	No, but there has been a lots of hit-and-runs.		+14056453492	+14056453492
12/11/2024 9:12:01 PM(UTC-6)	Well that's a shame.		+14056453492	+14056453492
1/8/2025 9:38:45 AM(UTC-6)	Hello		+14056453492	+14056453492
1/8/2025 9:41:28 AM(UTC-6)		https://s3.amazonaws.com/burner-mms/prod/9950e00e-4efa-4e34-92f4-760f4300070f.jpg	+14056453492	+14056453492
1/8/2025 9:43:16 AM(UTC-6)		https://s3.amazonaws.com/burner-mms/prod/f09cc97a-b876-46bc-8bc8-5a6019e173fb.mp4	+14056453492	+14056453492
1/8/2025 10:06:39 AM(UTC-6)	Hello		+14056453492	+14056453492
1/8/2025 12:57:39 PM(UTC-6)		https://s3.amazonaws.com/burner-mms/prod/5a43328a-f663-48b6-9071-573201e935fe.mp4	+14056453492	+14056453492
1/14/2025 4:25:46 PM(UTC-6)	Hello		+14056453492	+14056453492
1/14/2025 4:26:24 PM(UTC-6)	How are you?		+14056453492	+14056453492
1/14/2025 4:26:59 PM(UTC-6)		6F38ECDD-B122-4A76-B1F1-757C4CF38987.mov		+14056453492
1/14/2025 6:45:19 PM(UTC-6)	https://upload.pub/v/Axz6P3sk4K23aihqZm5xSV		+14056453492	+14056453492
1/14/2025 6:58:10 PM(UTC-6)		8B7BBBA8-9EE3-4FEC-8687-D1B055B141F0.mov		+14056453492
1/14/2025 7:01:07 PM(UTC-6)		01FB45B9-7DC6-4A3A-AA39-BD14E8835C44.mov		+14056453492
1/14/2025 7:05:29 PM(UTC-6)	https://upload.pub/v/4WLfo14ifbgWtqYmfmEv6h		+14056453492	+14056453492
1/14/2025 7:14:23 PM(UTC-6)		7BEAFEE9-09C3-428F-8107-89A6FC980C72.mov		+14056453492
1/14/2025 7:16:38 PM(UTC-6)		91AAAD28-CB72-4B1F-B3B6-AB3B13F8166C.mov		+14056453492
1/14/2025 7:18:35 PM(UTC-6)		38BBD4B9-562A-46CF-B20E-2A4A64909431.mov		+14056453492

The messages recovered do not indicate whether the message was sent or received. The automated data indicated the message was sent from "Unknown (owner)." See Figure 1 for an excerpt of messages recovered from the Apple iPhone 15 Plus. The database recovered the messages and the number associated with the iPhone 15 Plus, but the phone numbers recovered for "ZCONTACTID" and "ZCONVERSATIONID" were associated with the Samsung Galaxy S23 Ultra. During the message exchange, the Apple iPhone 15 Plus sent the Samsung Galaxy S23 Ultra low-quality videos, a .mov file. On the iPhone 15 Plus, the video showed a check mark but did not indicate whether or not the video was sent. The Galaxy S23 Ultra did not receive the

video sent as a low-quality video, a .mov file. The database recovered the asset URL, but the video not received by the Galaxy S23 Ultra did not recover the "ZCONTACTID" and "ZCONVERSATIONID" phone numbers. That also indicates that the messages were not successfully sent. Although data was not recovered from the "burned" phone number, the data associated with active lines contained the recipient's phone number.

Discussion

The Burner application is designed to mimic an actual burner phone without having to purchase a new phone every time a new number is needed. The purpose of a burner phone is to be untraceable and, for the most part, temporary use. This study aims to determine whether digital artifacts related to the Burner application could be recovered. More importantly, could digital artifacts be recovered once a number used in the Burner application has been "burned." A burner phone left behind could be a dead end or a crucial piece of evidence in a case. Users can decide to use the Burner application if they wish to keep personal information private; by using the Burner application, users have access to temporary numbers without having to purchase another mobile device and activate it. Once the user is done, they could "burn" the number without having any trace.

As demonstrated in Samsung Galaxy S23 Ultra results, no digital artifacts have been recovered. When the Android operating system was developed, it was designed with security in mind. Although it was possible to recover more data in previous years and previous versions of Android Operating systems, it is expected to get tougher as consumers desire more privacy regarding their mobile devices. Security weaknesses, once exploited to obtain data, are now patched and are no longer an option for forensic examiners or the tools they use.

In the Apple iPhone 15 Plus, the results of digital artifacts were recovered, but not fully. Two numbers remained active during extraction, but Cellebrite categorized them as deleted. Limited data would have been recovered if it wasn't for the AppGenie in Cellebrite Physical Analyzer Inseyets. Before running AppGenie, the only information found regarding the Burner application was that it was installed, as well as entry logs, databases, and some uncategorized data. This would then require examiners to search the database files manually for items of evidentiary value. This requires more time and increases backlogs as a result.

Limitations

Throughout this study, there are many limitations that need to be addressed. This study used the Samsung Galaxy S23 Ultra because it uses the Android operating system and was compared to the Apple iPhone 15 Plus iOS operating system. Android is open-source, meaning the software can be modified to fit any device and may vary depending on the manufacturer and cellular provider. This becomes problematic when a digital forensic tool can get into an Android device from one service provider but cannot access the data from the same device from a different service provider. Android devices are not the same across service providers. Android was designed with security in mind; multiple security layers must be penetrated to access users' data (Tamma et al., 2020). iOS operating systems are proprietary and remain the same across all devices regardless of service provider. No data was recovered using the Samsung Galaxy S23 Ultra in this study. Multiple extractions were attempted, manual examinations of the device's filesystem and databases were conducted, and no digital artifacts associated with the Burner application were found. Another factor to consider regarding the devices used in this study is that mobile devices were associated with T-Mobile. The service provider does not impact the Apple iPhone 15 Plus, but it does play a factor in the Samsung Galaxy S23 Ultra. With this in mind,

future research should consider using various Android device make and models from different manufacturers such as Samsung, Google, or Motorola.

Another limitation to consider is similar across all devices, no matter what the make of the device is automatic updates. After the Samsung Galaxy S23 Ultra device was set up, default settings were used. No changes to device settings were made, but the Burner application updated automatically without permission or prompting from the user. Initially, the Burner application was installed back in October 2024; it was later discovered that the application was updated in February 2025. At the start of this study, there were limited subscription options. Once the study was completed, the Burner application was updated, and new features were available for the Samsung Galaxy S23 Ultra. Options now available include but are not limited to credit purchases, as well as standard and premium subscriptions. As for the Apple iPhone 15 Plus, the user selected automatic updates for both applications and system updates.

Another limitation of this study was the limited use of forensic tools. Limiting to one forensic tool was primarily due to the focus on the comparison of digital artifacts recovered in an Android operating system device and an iOS operating system device. This study used Cellebrite since it is the most commonly used forensic tool for mobile forensics in digital forensic labs. Cellebrite was unsuccessful in recovering any data associated with the Burner application installed on the Samsung Galaxy S23 Ultra. Future research should consider using other forensic tools that support mobile devices. Not all forensic tools are made the same, and no one forensic tool is designed to do it all. One tool may work better on a specific operating system versus another or third-party applications. Using multiple forensic tools to do mobile acquisitions, as well as parsing, could result in different outcomes.

Conclusion

Throughout this study, it is evident that consumers' increasing need for privacy affects how manufacturers are improving and implementing stronger security measures in their software and hardware. Mobile device use and third-party communication applications are more common among users and are on the rise. It is only a matter of time before consumers realize there are more efficient ways to keep their information private and not need so much software to do so. Mobile devices have expanded from what they were originally designed to do. In reality, mobile devices are both a useful and a dangerous tool. The Burner application has ultimately done what it was designed to do and then some. The Burner application gives users the capability of having many numbers within one device. The options include one line, three lines, or even ten lines.

After a complete analysis of the Burner application on the Galaxy S23 Ultra and iPhone 15 Plus, phone numbers (210) 610-7460 and (726) 247-0113 were "burned". The data associated with the "burned" phone numbers were not recovered on either phone. Data associated with the Galaxy S23 Ultra was not recovered, which included data associated with active phone numbers (405) 645-3492 and (405) 320-9589. A manual verification of the Galaxy S23 Ultra databases was conducted, and no database data was recovered. Data associated with active numbers (405) 645-3559 and (405) 279-9945 were recovered from the iPhone 15 Plus. The data included fifty (50) messages, ten (10) videos, and (10) photos from both phone numbers. All messages were recovered, but the photos and videos sent were detected and identified as attachments, but the content of those attachments was not recovered. The automated data did not indicate whether the message was sent, but the database data recovered indicates whether messages were sent. If the message was successfully sent, ZCONTACTID data is recorded; if the data is not sent, no data is recorded. Having multiple active lines did not affect the way data is stored. Data associated with

active numbers were stored in the Pheonix.sqlite database within the ZMESSAGE table. The data recovered did not include the active numbers used by the user but separated the message by the number of the recipient.

Many contributing factors played a part in the type of data recovered from the Burner application. The type of operating system on the device played a part in whether digital artifacts were recovered. In previous studies, Android devices had a higher success rate at recovering data, and iOS devices had no success recovering data. In this study, the iOS and Android operating system behaved differently. No data was recovered from the Android device, Samsung Galaxy S23 Ultra. The iOS device, Apple iPhone 15 Plus, recovered all messages, including indicators that attachments were sent, but the content was not recovered. The data recovered from the Burner application depends on the operating system. Overall, data is recoverable from iOS devices, but data associated with a "burned" number was not recovered.

This study is important in understanding the capabilities of a burner phone through third-party applications. Future research should continue analyzing issues emerging from the new capabilities of technology and security measures affecting mobile forensics.

References

Ad Hoc Labs. (2025, April 16). *About Ad Hoc Labs*. Retrieved from Ad Hoc Labs: https://www.adhoclabs.co/about

Burner. (2023, October 8). *How Burner works: Burner*. Retrieved from Burner: https://www.burnerapp.com/how-burner-works

Burner. (2025, February 20). *Purchasing credits: Burner*. Retrieved from Burner: https://support.burnerapp.com/article/233-purchasing-credits

Business Wire; New York. (2014, November 20). Burner app adds MMS and overhauls design; enables new features and faster, more integrated communications. *Article*. New York: Business Wire.

Ceci, L. (2025, February 21). *Most popular global mobile messenger apps as of February 2025, based on number of monthly active users: Statista*. Retrieved from Statista: https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/

Cellebrite. (2025, April 16). *Cellebrite digital intelligence glossary*. Retrieved from Cellebrite: https://cellebrite.com/en/glossary/appgenie-mobile-device-forensics/

Chantel, J. (2023, September 29). Texting vs. messaging: what's the difference? Textedly.

Etherington, D. (2012, October 18). *Burner app raises angel round, prepares to become the passbook for mobile privacy*. Retrieved from TechCrunch: https://techcrunch.com/2012/10/18/burner-app-raises-angel-round-prepares-to-become-the-passbook-for-mobile-privacy/

Goldstein, M., & Flitter, E. (2022, September 27). Texting on private apps costs Wall Street firms $1.8 billion in fines. *New York Times (Online); New York*. New York Times Company. Retrieved from New York Times (Online); New York.

Hanna, K. T., & Wigmore, I. (2022, October). *Burner phone*. Retrieved from TechTarget: https://www.techtarget.com/whatis/definition/burner-phone

Heath, H., MacDermott, A., & Akinbi, A. (2023). Forensic analysis of ephemeral messaging applications: Disappearing messages or evidential data? *Forensic Science International: Digital Investigation*.

Humphries, G., Nordvik, R., Manifavas, H., Cobley, P., & Sorell, M. (2021). Law enforcement educational challenges for mobile forensics. *Forensic Science International: Digital Investigation*. doi:https://doi.org/10.1016/j.fsidi.2021.301129

Kavaturi, G. (2023, April 07). *The rise Of messaging platforms in business communication*. Retrieved from Forbes: https://www.forbes.com/councils/forbestechcouncil/2023/04/07/the-rise-of-messaging-platforms-in-business-communication/

Meta. (2025, April 16). *Help center: Facebook*. Retrieved from Facebook: https://www.facebook.com/help/messenger-app/1084673321594605

Meta. (2025, April 16). *Help Center: Instagram*. Retrieved from Instagram: https://help.instagram.com/888592124998543

Moyle, L., Childs, A., Coomber, R., & Barratt, M. J. (2019). #Drugsforsale: An exploration of the use of social media and encrypted messaging apps to supply and access drugs. *messaging apps to supply and access drugs*. doi:https://doi.org/10.1016/j.drugpo.2018.08.005

Ramirez, X. (2025, April 16). *Flip phones at Walmart vs. burner: which is better?* Retrieved from Burner: https://www.burnerapp.com/blog/flip-phones-at-walmart-vs-burner-which-is-better

Samsung. (2025, March). *Introduction to Samsung Knox mobile security*. Retrieved from Samsung: https://docs.samsungknox.com/admin/fundamentals/whitepaper/samsung-knox-mobile-security/introduction/

Snap Inc. (2025, April 16). *Privacy: Snap Inc*. Retrieved from Snap Inc: https://values.snap.com/privacy/privacy-by-product

Tamma, R., Skulkin, O., Mahalik, H., & Bommisetty, S. (n.d.). In *Practical Mobile Forensics* (4 ed.). Packt Publishing.

Washington: Federal Information & News Dispatch, LLC. (2022, March 3). *Whitefish man sentenced to six years in prison for defrauding Montana investor of $2.3 million in scheme to fund fake CIA rescue missions.* Washington: Washington: Federal Information & News Dispatch, LLC.

WhatsApp LLC. (2025, April 16). *About WhatsApp*. Retrieved from WhatsApp: https://www.whatsapp.com/about