Retruth Reconnaissance: A Digital Forensic Analysis of Truth Social

Joseph Brown(✉) and Ibrahim Baggili

College of Engineering, Division of Computer Science, Center for Computation and Technology, Baggil(i) Truth (BiT) Lab Louisiana State University, Baton Rouge, USA
{jbro571,ibaggili}@lsu.edu

Abstract. Truth Social is a social media platform founded by former President Donald J. Trump as an alternative to mainstream social media platforms. Like other alt-tech social media, such as Parler or MeWe, Truth Social's looser content moderation rules may encourage more extreme user-based content. This includes biased language- posts with racist, sexist, ableist, or other discriminatory intent- and calls for violence. Digital forensic analysis can be useful in such cases, where law enforcement seeks to prevent or investigate extremist threats associated with a platform. This research fills a gap in the extant literature by offering a novel forensic analysis of Truth Social, based on established techniques. First, using mobile devices, account and application metadata was discovered. Next, network traffic analysis using a desktop computer revealed plaintext usernames and passwords. A detailed depiction of the forensic analysis performed for this paper is presented to aid future investigators.

Keywords: Digital forensics · Mobile network · Artifacts · Alternative social media · Truth Social

1 Introduction

Truth Social is an "alt-tech" social media platform, or one designed as an alternative to major platforms like Twitter and Facebook. It exists as a direct result of former President Donald Trump being banned from those platforms [10]. It has a format similar to Twitter. Truth Social shows character-limited text posts called "truths" which users can like, comment on, quote- which includes the text of one user's post onto another user's feed with additional input by the second user- or post the truth directly onto their own feed, called a "retruth" on the platform (See Fig. 1 for a sample Truth Social feed). This paper focuses on Truth Social because of its storied origins, its recent release, and because of the presence of extremist views on the platform, including calls for violence and even civil war [18]. Forensic analysis of this activity may provide valuable insight to

BiT Lab || Baggil(i) Truth (BiT) Lab.

S. Goel and P. R. Nunes de Souza (Eds.): ICDF2C 2023, LNICST 570, pp. 96–113, 2024.
https://doi.org/10.1007/978-3-031-56580-9_6

investigators and could even contain links to other individuals who may be on the brink of committing a violent act. Truth Social is also a new platform that launched February 12, 2022. Because it is a new platform, no digital forensic analysis has been conducted.

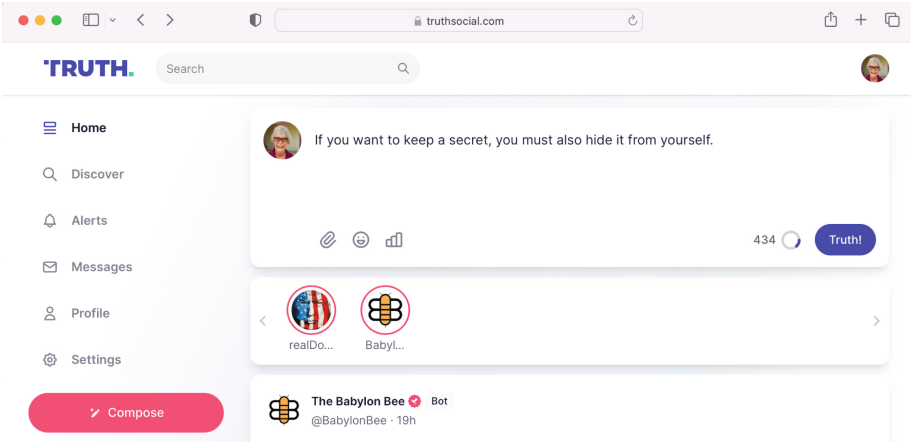

Fig. 1. Truth Social Feed

The source code of Truth Social is forked from Mastodon Social, an open-source social media platform. The code was originally copied without complying with the open source licensing requirements, leading Mastodon to threaten a lawsuit [21]. Details of the roll-out led one privacy researcher to question the safety of its data [16]. The circumstances behind the application's development may make it susceptible to security flaws. Analyzing this application is salient and novel because of its development history.

Truth Social markets itself as a free speech platform in reference to its content moderation policies. Other platforms with similar policies have had content eventually tied to criminal investigations. Less moderation tends to mean more of all types of content, including content linked to criminal behavior. For example, one Truth Social user lost his life after attacking an FBI office in response to an FBI raid of Mar-a-lago. The user posted about his attack on Truth Social while he was fleeing [17], creating what is known in the digital forensics world as artifacts. Artifacts are individual pieces of information (e.g., an image, post, or message) potentially of use in an investigation [15]. This instance illustrates how Truth Social could be of interest to investigators.

This paper seeks to provide three contributions to the digital forensics literature. Our contributions include:

- A novel forensic analysis of the application Truth Social.
- A guideline for future investigators to analyze the platform.
- A collection of discovered digital forensic artifacts shared on the Artifact Genome Project.

This paper is organized into the following sections. Section 1: Introduction describes Truth Social, its origins, and our motivations for investigating it. Section 2: Related Work presents a review of the relevant literature, with a focus on digital forensics investigations of social media applications. Section 3: Limitations briefly introduces some limitations considered before our research began. Section 4: Methodology reviews the actions taken to produce data within Truth Social, the steps to acquire data, and provides an overview of the tools used for acquisition and analysis. Section 5: Artifact Retrieval goes into detail how we took the raw data acquired in Sect. 4 and used to it to find relevant artifacts. Section 6: Discussion presents and considers the implications of the acquired artifacts. Section 7: Future Work provides recommendations for subsequent research. Section 8: Conclusion provides our final thoughts on this work.

2 Related Work

Digital forensics analysis has been performed on a wide variety of social media applications across many platforms, using many methodologies, and producing a cornucopia of artifacts. This work was instructive for investigation of Truth Social A brief survey of this analysis is presented in Subsect. 2.1. Each artifact is a potential piece of evidence in an investigation, providing potential motives, alibis, or proof of criminal activity. The relation of social media forensics to investigations is explored in Subsect. 2.2, which also tracks how digital forensic investigations have had to change with technology and discusses previous work focusing on criminal behavior and misinformation. In addition to the major social media platforms, a selection of alt-tech social media applications has been analyzed. A review of this analysis and its links to this paper's analysis of Truth Social are presented in Subsect. 2.3.

2.1 Social Media Forensics

There are many different ways to perform a forensic analysis of social media applications, or Social Media Forensics, which has become an increasingly useful tool for law enforcement and investigations. Though there are many hurdles to obtaining social media evidence in a manner that is legal and permissible in court [6], a variety of tools and techniques have been developed and successfully applied. Images recovered from social media have been analyzed to determine which application they were posted to [5] and for the integrity of the images or their presentation [25]. Methods for identifying anonymous authors through text posts have been developed and tested [4,26]. An earlier work in the field assesses the use of web crawlers to gather evidence from Facebook [19].

Many studies have taken advantage of the ubiquitous use of smart phones, capturing data images and using them in their analysis. A steady stream of researchers have been able to recover posted pictures and account information pulling data from phones [2,24,27]. Wu et al. use a combination of phones and

network traffic to extract data from a device but also include information gathered online [28]. Phone and desktop data has also been used to analyze social media applications developed as alternatives to the "Big Tech" platforms, finding not only artifacts but also large security flaws in the storage and transfer of data [20]. Each of these approaches uses different methodologies and tools to gather a variety of information potentially useful to an investigation. Some of these differences emerge from desired results, but the ever-changing nature of the internet also necessitates forensics methodologies to change.

2.2 Investigative Motivation

Digital Forensics have exited the "Golden Age" where collection and analysis of data was relatively easy [12]. Technology in general is constantly evolving, and the last decade has seen a tremendous shift from traditional computing to mobile use. Social media use is a large part of this; according to the Pew Research center, 72% of Americans reported using a social media site in 2021 [7]. Computing is shifting to mobile devices which constantly add or change data; this data can be harder to obtain than traditional computer data [24]. As social media platforms constantly update their underlying code, policies, and security, the methods with which to perform digital forensics have also had to evolve.

At the start of the decline from the Golden Age of Digital Forensics, Huber et al. were able to use add-ons and a web crawler to obtain evidence from Facebook including contact lists, "liked" posts, and limited data on photos, videos, and messages [19]. The authors note limitations- high levels of traffic proved hard to store and catalog, and metadata containing information potentially useful to investigators is often missed. They note traditional computer forensics is often inadequate in the age of the internet- criminals can completely bypass their own hardware, making the collection of evidence more difficult. Being able to obtain and parse information from an individual that does not reside on their computer is an increasingly important part of computer forensics [19].

Pasquini et al., concerned about the integrity of media such as images and videos disseminated on social media, used forensics to gather data proving a file's authenticity. They note that images uploaded to Facebook are commonly compressed and resized, and these changes are well known and easily verifiable forensically. Through further analysis, the authors reconstructed the URLs of images and identified the operating system used in some cases. They collected metadata that gave clues to the state of an image. Altered images, or even unaltered images presented in an untruthful way, can be tools of criminals or indicators of criminal activity [25].

Much of the focus of digital forensics is on the collection of inculpatory evidence, but other facets have been considered as well. Digital forensics of some social media sites have confirmed alibis [19], and in other cases is designed to help identify a suspect [4,26]. A person using tools like prepaid phones and TOR, a browser designed for anonymity, could make a post linking them to criminal activity. Considering these anonymous tools and the 140-character limit Twitter had at the time, researchers had little data to work with; however, they were

able to use machine learning to identify the authors of a post even with limited data [26]. By analyzing word use, organization, and style, they tagged posts and associated them with writings of current suspects or helped identify suspects by matching the post to another writing, such as an email or a tweet from a public account. Alfonso-Fernandez et al. similarly looked at identifying authors from Twitter posts, and found that they could do so with over 80% accuracy given a large enough number of tweets to analyze [4]. Rocha et al.'s specific motivation is to unveil perpetrators of misinformation campaigns conducted by individuals, corporations, or governments. Misinformation, criminal evidence, and extremist views exist on all social media platforms, but there are many emerging sites whose positions on "free speech" and moderation make them more common.

2.3 Alt-tech Extremism and Forensics

In the last five years, there has been a growing group of social media users who feel dissatisfied with the popular platforms. Some report feeling their views are unfairly targeted or censored. Several social media applications that position or market themselves as alternatives to mainstream companies like Facebook and Twitter have been released. They are commonly referred to as alt-tech social media [3]. One of the most popular is Parler, which has made claims of having up to 20 million users. Parler has deep ties to the attack on the U.S. Capitol on January 6, 2021, was taken down in response to those ties and moderation issues, and was only recently returned to the Google Play store [1]. Evidence from Parler and other alt-tech platforms has been used in the trials of some of the participants in the events of January 6th [8]. As these platforms are new, little extant analysis exists. Digital forensic analysis of these platforms could provide more tools for investigators and security professionals.

Johnson et al. looked specifically at social media platforms cast as alternatives to the established social media giants. Parler is the most widely used of the analyzed applications. The authors create multiple accounts on each platform and use them to communicate with each other, and then create images of the phones used and gather evidence from these images. Using a tool they developed and other open source tools, they were able to find a plethora of information, including phone numbers, users IDs, and other account information, content of posts and messages, cached images, and in some cases, security flaws allowing them to access data without authentication [20]. This approach opens new avenues of evidence collection and is directly applicable to Truth Social.

Truth Social is similar to Parler in many ways. Both platforms were created in response to alleged mistreatment from larger social media companies. Each has their own issues with extremist views, likely tied to their moderation policies. These views, the posts expressing them, and the moderation policies have affected the presence of both in the major online stores like Google Play and the Apple Store. Truth Social was only recently allowed into the Google Play store. Truth Social is unique in its direct ties to a former president of the United States, whose influence on supporters is strong and has been tied to illegal activity [9]. The platform not only exists because of him but also has him serve as

the anchor for the platform, with his account having roughly 4 million followers, the most of any Truth Social user. Because of its similarities to existing alt-tech platforms, novel ties to a former world leader, potential investigative use, and the newness of the application, Truth Social is ideally situated to undergo an initial digital forensic analysis.

3 Limitations

While we consider our analysis of Truth Social robust, there are some potential limitations. This paper considers only a single alt-tech social media application and is thus limited in scope. Truth Social is also a fledgling application, a little over a year old, has not undergone many updates, and is missing some functionality. At the time of this writing, the application has only recently introduced a direct messaging feature[1]. Its private nature may be of increased investigative interest, but it still lacks some of the features of other messaging clients, most notably the ability to attach or send images in direct messages. Finally, while the application does have millions of users, its base appears to be much smaller than Facebook or Twitter. Data on Truth Social users is opaque, with some reports indicating roughly 2 million active users. Donald Trump has around 4 million followers, which is substantial but also much lower than his 88 million follower count at Twitter.

4 Methodology

This section details our methodology for obtaining and analyzing the Truth Social data. It is broken into 3 Subsections. 4.1: Scenario Creation looks at the steps taken to produce data using Truth Social accounts. 4.2: Data Acquisition details how the data was retrieved from the mobile devices and networks. 4.3: Apparatus lists the tools we used in a table format and briefly discusses the major tools.

Forensic analysis of Truth Social included the following steps: scenario creation and execution, data acquisition, and data analysis. Multiple accounts were created on Truth Social using an Android phone, an Apple iPhone, and desktop computers. These accounts were then made to perform like regular accounts. They made posts, shared each other's posts, uploaded and shared images and videos, messaged each other, and utilized other miscellaneous functions, such as a polling feature. The scenario was completed over several weeks using natural spacing, with some days having multiple posts and some days with none. Additional scenario steps were completed as new functionality, such as the direct messaging feature, were added. Once the scenario was completed, a variety of tools were used to get images or backups from the phones, including Magnet Acquire, iPhone Backup Extractor, and a Cellebrite UFED. These images were then analyzed manually and using a variety of analysis tools.

[1] Truth Social's direct messaging feature became available 12/19/2022.

4.1 Scenario Creation

Scenario creation and execution consisted of testing each of Truth Social's features with a pair of accounts. An Android and Apple mobile device were factory reset and then tested with their out-of-the-box settings to mimic how an actual user may have their devices. Truth Social was not allowed in the Google Play store due to content moderation issues, [14] and the application was installed by downloading the APK file and installing from this file[2]. Once the application became available in the Google Play store, it was deleted and then reinstalled with that method. Truth Social was also downloaded from the Apple App store.

The scenario was meant to mimic the behavior of an actual user and to test all available functionality on the application and website. Fake email accounts were set up and used to create both profiles on the mobile devices and user accounts on Truth Social under the pseudonyms Jimmy Orange (Android) and Rebecca Red (iOS). Profile photos were AI-generated using the tool Dream by Wombo. These accounts posted "truths" with text, images, video, and polls. The accounts then interacted with each other, "retruthing", quoting, replying, voting in polls, liking comments, and later sending messages back and forth. At the time of the initial scenario, the direct messaging feature was not available, displaying a page stating "A new direct messaging experience will be available soon. Please stay tuned". The messaging feature has since been added and another round of testing followed. Scenario creation and execution were carried out September through November of 2022, with additional scenario work for the direct messaging feature occurring in December of 2022. Data acquisition and analysis then occurred.

4.2 Data Acquisition

In the data acquisition phase, Truth Social data had to be retrieved from the mobile devices, and data images were captured on the Android and iOS devices. Two software tools, Magnet Acquire and iPhone Backup Extractor, and one hardware tool, a Cellebrite Universal Forensic Extraction Device (UFED), were used to gather different types of data. Logical images came from the initial scenario completed on the out-of-the-box phones. The UFED produced "advanced logical" images, which the manufacturer claims combines features of both logical and physical images.

The software Magnet Acquire provides data imaging functionality for mobile devices and was used to retrieve logical images on each device. This is an enterprise software, but is free for members of the forensic community. The tool is UI-based and user friendly. The version used produces archived zip files by default. After image acquisition, the initial analysis showed more artifacts in the Apple image than in the Android image and included text files and some database files.

iPhone Backup Extractor is an inexpensive, freely available software tool used to backup Apple phones and explore the backups. Like Magnet Acquire, it

[2] Truth Social became available in the Google Play store 10/13/2022.

is easy to use and UI-based. iPhone Backup Extractor can use existing iTunes backups stored on a computer or device. The software can also create its own backups from the mobile device. Initial analysis showed preference list files and one database file for the Apple device. This software was only used with the Apple devices, as it has no functionality for Android phones.

The final data acquisition was completed using a Cellebrite UFED, a hardware device designed for mobile device forensic analysis. The UFED is a common tool in investigations, and tens of thousands of devices are deployed to law enforcement agencies worldwide [13]. It is capable of producing several data image types, including logical and physical images. In this round of analysis, logical and advanced logical (also called filesystem) images were acquired for both devices. The images gathered using the UFED were the largest collected from all the tools used.

In addition to the device images, the network protocol analyzer Wireshark was used to record network traffic during access and use of the Truth Social website. The captured packets were then imported into the application NetworkMiner to undergo analysis. The packets appear to be properly encrypted; no passwords or other identifying information was discovered, nor were any images or other media. However, using the web debugging proxy tool Fiddler Everywhere, HTTPS traffic was captured that produced a number of valuable artifacts.

Table 1. Apparatus

Hardware/Software	Use	Company	Version
Agent Ransack	Search tool	Mythicsoft	3389
Autopsy	Image viewer used for analysis	The Sleuth Kit	4.19.3
Burp Suite Community Edition	Capture/Analyze network traffic	PortSwigger	2022.9.6
UFED	Forensic image acquisition	Cellebrite	7.53
DB Browser for SQLite	View databases	DB	3.12.2
Fiddler Everywhere	Capture/Analyze network traffic	Progress Software Corporation	4.0.1
iPhone Backup Extractor	iOS image acquisition and analysis	Reincubate	7.7.40.8353
Magnet Acquire	Image acquisition for Android and iOS	Magnet Forensics	2.56.0.31667
Network Miner	Analyze network traffic	Netresec	2.7.3.0
Safari	Desktop Truth Social use	Apple	16.0
Wireshark	Capture/Analyze network traffic	Wireshark	4.0.1-0-ge9f3970b1527
iPhone 6 s	Truth Social accounts	Apple	iOS 15.7.1
Galaxy S6	Truth Social accounts	Samsung	Android 7.0
Macbook Pro	Acquisition and analysis	Apple	macOS Monterey 12.6
Windows 10	Acquisition and analysis	Microsoft	OS Build 19043.2130
Truth Social	Android and iOS Truth Social accounts	Truth Social	0.1.7 (Android) & 1.3.8 (iOS)
VirtualBox	Host VMs for testing and analysis	Oracle	6.1.38 r153438

4.3 Apparatus

A variety of software and hardware devices were used during this research. Much of the software was chosen because it is either free or inexpensive, allowing investigators at various levels to recreate this analysis. Only the UFED is of significant cost, and it is already ubiquitous with law enforcement agencies. The individual items are discussed in more depth where relevant. For instance, network analysis tools like Wireshark and Fiddler Everywhere are discussed in Sect. 5.4, Network Traffic Analysis. The full list of hardware and software used, including version numbers and the function of the item, is presented in Table 1.

5 Artifact Retrieval

Table 2. Artifacts Found

Path	Origin	Tool	Description
/LogicalFileSet3/samsung SM-G920V Quick Image/Live Data/Dumpsys Data/activity.txt	Android	Autopsy	Application launch time
/LogicalFileSet3/samsung SM-G920V Quick Image/Live Data/Dumpsys Data/dbinfo.txt	Android	Autopsy	Process ID numbers
/LogicalFileSet1/Backup/698e7bc1d5360fe396cef329bcd1fd9a18b21256-2022101-130616/2c/2c9c9fa7711487633029ec6a83873dfddf5d08a	Apple	Autopsy	Application launch time
https://truthsocial.com/api/v1/accounts/verify_credentials	Macbook Pro	Burp Suite	User biography
https://truthsocial.com/api/v1/timelines/home	Macbook Pro	Burp Suite	User timeline
https://static-assets-1.truthsocial.com/tmtg:prime-ts-assets/accounts/avatars/107/780/257/626/128/497/original/0806c7e6b4c33703.jpeg	Macbook Pro	Burp Suite	Static profile image example
https://truthsocial.com/users/rebeccared/statuses/109277563934729421	Macbook Pro	Burp Suite	Static post example
https://truthsocial.com/oauth/token	Macbook Pro	Fiddler Everywhere	Static post example
https://truthsocial.com/api/v1/pleroma/chats/399834/messages	Macbook Pro	Fiddler Everywhere	Direct message example
https://static-assets-1.truthsocial.com/tmtg:prime-ts-assets/media_attachments/files/109/832/912/972/151/117/original/d1c95ca8589ad450.png	Macbook Pro	Fiddler Everywhere	Static photo link that works after deletion
https://rumble.com/embed/v1l3yk8/	Macbook Pro	Fiddler Everywhere	Static video link
https://rumble.com/embed/v26c34u/	Macbook Pro	Fiddler Everywhere	Static video link that works after deletion

In this section, we present the steps we used to take the raw data acquired in Sect. 4.2 and analyze it to discover artifacts. It is broken into 3 Subsections. 5.1: Manual Analysis of Logical Images details the investigation into the data before using sophisticated tools. This type of analysis is rudimentary and can be performed with little skill. 5.2: Tool Analysis of Logical Images explores the data found using industry standard tools common in most digital investigations. 5.3:

Source Code Analysis of Truth Social considers known or discovered software vulnerabilities using standard software security procedures. 5.4: Network Traffic Analysis covers items discovered using various packet capturing tools. Subsections here will detail each of the different categories of analysis performed and highlight important artifact types. A selection of the most significant artifacts is presented in Table 2.

5.1 Manual Analysis of Logical Images

Fig. 2. Plaintext User Information from Fiddler Everywhere

Manual analysis of the phones' logical images found small but significant artifacts possibly of use in a forensic investigation. This analysis consisted of using basic and advanced search methods, including using Microsoft and Apple's built-in search functionalities, command line searches, and open source or proprietary tools like Agent Ransack. Searches included looking for simple strings like "truth" or "social" as well as some keywords from posts, and then reviewing data in the files containing those strings. This type of analysis can be performed at little to no cost.

In the Android images, the vast majority of files found were simple text files. The main artifacts present in the Android logical image were references to the Truth Social app launcher. Some activity was visible, such as calls to login pages, but passwords, tokens, or other credentials were not viewable. The authors could see that the application requested direct boot access on the device, letting the application run while the phone is powered on but not unlocked.

The Apple phone's logical image proved more fruitful than the Android logical image. The iOS image obtained from Magnet Acquire was significantly larger than the Android image, 175 MB to 9.8 MB respectively[3]. A variety of files were present, including text files, database files, and list files. Artifacts discovered included Truth Social metadata, file system locations for the application, and database entries. Many of the files present in the Apple image were not easily readable in text editors, and artifacts of interest in these files were not found until tool analysis began.

[3] This held for the Cellebrite images, 135 MB to 25 MB.

5.2 Tool Analysis of Logical Images

After manual analysis, some digital forensics software applications were used for a more thorough search of the images and backups. iPhone Backup Extractor has some functionality to identify files and information associated with a particular application and was the first tool used to look at the Apple phone backups. The software Autopsy provides a wide variety of forensic analysis tools that can be used on many different image types for both Apple and Android devices, and was also used for further analysis.

Autopsy was able to identify many artifacts not discovered in manual analysis or using iPhone Backup Extractor. Many of these artifacts are not easily readable in their original forms- some were encrypted, while others were in hex or other representative forms- and the tool was able to convert them into more useful formats. String searches were performed within the cleaned up data to further narrow down the files of interest. Several of these files contained base64 segments of characters, which were run through an online base64 decoder for analysis; most contained little data to our interest.

5.3 Source Code Analysis of Truth Social

Truth Social was based on Mastodon, an open source social media platform. A requirement of the license Mastodon uses requires any organization using their code to make the alterations freely available[4]. As such, Truth Social's own source code is open source and available to the public for review. Code was analyzed for ease of artifact discovery and was run through software vulnerability scanners to look for any flaws making the application susceptible to attack.

Common Vulnerabilities and Exposures (CVEs) are an industry standard to track publicly exposed vulnerabilities in software packages. CVEs for Truth Social were not found in the National Vulnerabilities Database, but a number of CVEs associated with Mastodon's code are present. Vulnerabilities present when Truth Social cloned Mastodon's code may still be in the Truth Social codebase. For instance, CVE-2022-31263 concerns an email restriction bypass in the app/models/user.rb file of Mastodon. The same file is present in Truth Social's Github page with the last commit on February 21, 2022, but the CVE was logged on May 24th 2022. Comparing Mastodon's patched version of the file to Truth Social shows differences in how email validation is handled in the code. It is likely Truth Social has this vulnerability, and others from the original Mastodon clone.

5.4 Network Traffic Analysis

Wireshark, NetworkMiner, and Fiddler Everywhere were used to perform network analysis. The first two tools produced mostly encrypted traffic. The traffic captured by Fiddler during login attempts produced both the username and

[4] This technique is commonly called "Copyleft.".

password in plaintext (see Fig. 2). Posts from the main page, including from other users, were easily accessible, as was a plethora of metadata such as login times. Interaction between users was also easily obtainable using Fiddler. Direct messages in plaintext were also discovered, with each new message producing a JSON record with the full list of messages.

These findings were replicated using the community edition of Burp Suite, a security vulnerability scanner with network analysis functionality. Burp Suite also discovered static URLs for profile photos (see Fig. 3), which can be accessed directly without being logged into the platform, and profile demographic information such as a user biography. Static links for posted videos were also discovered. In addition, Burp Suite has functionality to brute force passwords through its Intruder feature by stepping through a character set and length range. Truth Social's server is using Cloudflare to handle incoming requests and serve content to visitors. Cloudflare is a popular Content Delivery Network provider meant to help improve performance, security, and reliability. It has built in Distributed Denial of Service protection, but did not immediately stop our slower, single origin brute force attack. Truth Social did send an HTTP 400 code for most entries, but it did not stop the traffic despite thousands of attempts. When using a simple password list including a correct username/password combination, a successful HTTP 200 was received.

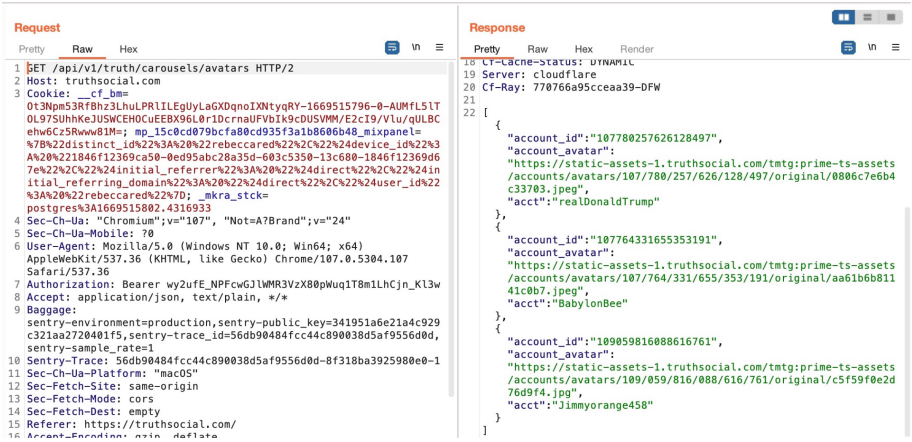

Fig. 3. Profile Photos' Static URLs

6 Discussion

This section considers the previous two sections and their implications. We consider how the data was acquired and how our process compares and differs to investigations academic, public, or private in nature. We also discuss the significance of the artifacts found and how they can aid an investigation.

We discovered a variety of information about the Truth Social application. Artifacts were recoverable using freely available and proprietary tools and from varying backup types. In contrast to previous alt-tech platform research, some expected artifact types were not recovered from the mobile devices and had to be found using network traffic analysis (e.g., images or text from posts). The types of artifacts discovered and the manner in which each type was found should provide guidance for anyone wishing to perform forensic analysis of Truth Social.

Every tool used found relevant artifacts from every data image or backup created. This includes tools freely downloaded from the world wide web and proprietary tools requiring licensing and payment, and also covers standard backups like ones from iTunes and ones produced by forensic tools like the Cellebrite UFED. This means that almost anyone with access to a mobile device will be able to conduct some level of forensic investigation regardless of position or means. It also indicates a level of ease for experienced, professional investigators with access to forensic tools, who should be able to recover artifacts from Truth Social with little difficulty.

No information about posts, replies, or other direct updates was found using the images from the mobile devices. Posts were visible while viewing network traffic. This may indicate that little to no activity information from Truth Social is stored on either Apple or Android devices. Source code analysis showed many references to Firebase, a Google platform that commonly stores data on the cloud, which may prevent local storage [22]. As such, investigators attempting data retrieval from Truth Social may need to actively track a person of interest's Truth Social use to discreetly acquire data. Despite the lack of direct post evidence found from the images, other important information was discovered.

Using the various data images and tools, enough information was found for an investigator to build a case against a suspect. Records of the application were present after deletion, so even if Truth Social was removed from a device, it could still be tied to a user. From application launch times, use of Truth Social can be matched to other known posts or users also known to be active at that time. Launch times also show the frequency of use on the devices.

The bulk of the more interesting artifacts were collected during network traffic analysis. Oauth tokens were found with usernames and passwords in plaintext. Full text of a user's biography was accessible, as well as their posts and information about followers. When logging into the application, all information presented on the user's feed was visible in the network traffic. This included recent posts by other users our test user followed. Direct messages were also viewable, as well as unique ID numbers for each chat.

In addition to the post and message information, static links for profile photos and photos posted to the timeline were also visible. The links for profile photos share a similar pattern, containing a series of nested directories with a three-digit numerical title. Each user is assigned an ID number, and the nested directories are composed of that ID split into triplets. For instance, the user Rebecca Red has an ID of 109145180605858911, and the static link to that profile photo includes this in its URL: 109/145/180/605/858/911. Notably, these links were directly

accessible even without authentication- logging out of the system did not prevent the photos from loading when navigating to the URLs. These static links work even after the post containing the photo is deleted, indicating an investigator could retrieve posts or photos a user attempts to hide.

Truth Social is hosted by Rumble, a cloud services provider and video platform positioning itself as an alt-tech alternative to YouTube. Network analysis with Fiddler revealed videos posted to Truth Social are stored to Rumble. Viewing a video-containing post produces a Rumble link in the traffic. Like the static photo links, these video links can be accessed unauthenticated. Deleting a post with a video removes it from a user's timeline, but does not remove the stored video- the Rumble links work post-deletion. With videos and images accessible even after deletion, most media posted to Truth Social could be recoverable by investigators even if a user tries to remove it.

Truth Social's codebase is largely written using the server-side web application framework Ruby on Rails (Github's languages breakdown indicates it accounts for 60% of the code). Using Burp Suite Community Edition, a number of potential security vulnerabilities were discovered, including a variety of injection risks, web cache poisoning, and cross-site scripting. The details of these vulnerabilities have not been explored. Earlier, since patched vulnerabilities in Mastodon may still be present in Truth Social's code. Future work may focus on attempts to exploit one of these vulnerabilities to gain access to artifacts.

Many artifacts were discovered in the course of this investigation. Some were redundant, while others may hold interesting information, but were too obscured for the scope of this study. All digital artifacts can be viewed at the Artifact Genome Project (https://agp.newhaven.edu).

6.1 Recommendations for Investigators

Based on our methodologies and findings, we have several recommendations for investigators.

Investigators need to acquire data from Truth Social in a forensically sound manner to ensure the data has not been tampered with and is admissible in court. This would involve using tools and techniques that can extract data from the platform's databases, file systems, and other storage locations. Our findings indicate network analysis is more fruitful, so investigators could focus on network sniffing tools like Wireshark or Fiddler. Network traffic associated with Truth Social, including traffic to and from the platform's servers and any third-party services it may use, should also be analyzed to identify potential evidence of data breaches, hacking attempts, or other types of cybercrime. Investigators would need to ensure that any data they collect from Truth Social complies with data privacy laws.

Most of the data acquired from the mobile devices was metadata. Investigators would need to analyze the metadata associated with any data collected from Truth Social. This would include creation and modification dates, geolocation data, and user IDs, which can provide valuable context for the data. Similarly, investigators can analyze user activity, including posts, comments, likes, and

other interactions to reconstruct user behavior and identify potential evidence of criminal activity, such as harassment, hate speech, or other types of online misconduct.

Since Truth Social allows users to share images and videos, investigators would need to analyze this media for potential evidence of criminal activity, such as child sexual abuse materials, terrorist propaganda, or cybercrime.

7 Future Work

We have noted some limitations and provided recommendations for investigators. In this section, we provide research ideas for future work in this area. By delving deeper into these areas, researchers can expand the current body of knowledge about Truth Social and alt-tech media in general. These ideas are intended to inspire and guide future research.

This paper has discussed artifacts the authors considered most important, but there are many artifacts that could be considered more closely. Some artifacts may contain important information, but were not able to be deciphered or otherwise identified as such within the scope of this research. The mobile devices used were not rooted or jailbroken, and performing a similar analysis with full access could produce interesting differences in obtained data. Truth Social is still new and going through major changes. New functionality may be introduced or be altered. For instance, the newly unveiled direct messaging lacks a key feature of its competitors- the ability to attach images or videos. Software updates may occur frequently as well, changing the type of artifacts and the manner in which they are discovered. These updates may mitigate previously discovered security vulnerabilities or introduce new ones.

This paper only considered a single alt-tech social media application. A comparison between Truth Social and other alt-tech social media, such as Parler or Gab, may provide interesting insight into the forensic techniques producing the best results. Finally, as Truth Social began as a branch of the Mastodon code, a full comparison between Mastodon and Truth Social could also be insightful, particularly in regard to the differences in protection of data and software security vulnerabilities.

8 Conclusion

Truth Social is quickly becoming one of the most important alternative social media applications. It was recently accepted into the Google Play store, and it became the most downloaded application in the store on that same day. More users are signing up daily, and as former President Donald Trump, founder of the site and the user with the most followers on the platform, has announced his 2024 presidential run, it is likely the application will continue to grow and gain media attention. Truth Social also may gain followers from the tumult occurring at its most similar rival, Twitter, which has undergone leadership change, massive layoffs, and behavior from its CEO that is alienating advertisers and users

alike [11]. Truth Social was founded in part as a response to President Trump's ban from Twitter, and even though his account was reinstated in November 2022, Trump claimed in a post on Truth Social he would remain on his own platform and has thus far stuck to that promise. Truth Social's looser content moderation has led to extremist users and its issues with violent, racist, misogynistic, and homophobic posts. With the recent 2022 United States Midterm elections finished and the upcoming 2024 presidential election, more users coupled with extremist views on Truth Social may lead to it being an area of focus for investigations.

According to testimony before Congress by a researcher for the Carnegie Endowment for International Peace, instances of politically-based violence are on the rise [23], and both perpetrators and bystanders often turn to social media to document their activities and observations. The January 6, 2021 attack on the US Capitol was discussed so much on some alternative social media sites that these posts were used in criminal trials of participants. As Truth Social becomes the dominant alternative, it is likely investigative reporting and civil or criminal investigations will often use the platform for evidence collection. This research seeks to identify what significant artifacts can be discovered and in what manner they can be discovered to benefit digital forensic investigations.

The preliminary digital forensic analysis of Truth Social performed in this paper shows many artifacts can be recovered from the application. Using various tools, techniques, and devices, a repository of these artifacts was created and includes user information, application information, install times, application launch times, post information, credentials, and permanent video and image links. Truth Social did prove resilient against mobile forensics, with most of the major discoveries occurring when monitoring network traffic. This is the exact opposite of the findings of previous alt-tech forensic research [20], where most artifacts were recovered from the mobile devices. This may be due to its origins as a Mastodon clone, which heavily utilizes cloud-based storage and network management.

References

1. Social media platform parler is back online on 'independent technology' (2021). https://www.cnbc.com/2021/02/15/social-media-platform-parler-back-online-after-being-banned-by-major-tech-companies.html
2. Al Mutawa, N., Baggili, I., Marrington, A.: Forensic analysis of social networking applications on mobile devices. Digit. Investig. **9**, S24–S33 (2012)
3. Aliapoulios, M., et al.: A large open dataset from the Parler social network. In: ICWSM, pp. 943–951 (2021)
4. Alonso-Fernandez, F., Belvisi, N.M.S., Hernandez-Diaz, K., Muhammad, N., Bigun, J.: Writer identification using microblogging texts for social media forensics. IEEE Trans. Biometr. Behav. Identity Sci. **3**(3), 405–426 (2021)
5. Amerini, I., Li, C.T., Caldelli, R.: Social network identification through image classification with CNN. IEEE Access **7**, 35264–35273 (2019)
6. Arshad, H., Jantan, A., Omolara, E.: Evidence collection and forensics on social networks: research challenges and directions. Digit. Investig. **28**, 126–138 (2019)

7. Auxier, B., Anderson, M.: Social media use in 2021. Pew Res. Cent. **1**, 1–4 (2021)
8. Billeaud, J.: Rioters accused of erasing content from social media, phones (2021). https://apnews.com/article/joe-biden-capitol-siege-business-electoral-college-media-efe0ea1092bc11c6d3f42ea4ef752d98. Section: Donald Trump
9. Byman, D.L.: How hateful rhetoric connects to real-world violence (2021). https://www.brookings.edu/blog/order-from-chaos/2021/04/09/how-hateful-rhetoric-connects-to-real-world-violence/
10. Clayton, J., Cabral, S.: Truth social: banned from twitter, trump returns with a new platform (2022). https://www.bbc.com/news/technology-60419008
11. Conger, K., Isaac, M., Mac, R., Hsu, T.: Two weeks of chaos: inside Elon Musk's takeover of twitter (2022). https://www.nytimes.com/2022/11/11/technology/elon-musk-twitter-takeover.html
12. Garfinkel, S.L.: Digital forensics research: the next 10 years. Digit. investig. **7**, S64–S73 (2010)
13. Goda, B.S., Bair, J.W., Costarella, C.E.: Cell phone forensics. In: Proceedings of the 16th Annual Conference on Information Technology Education, pp. 39–42. ACM (2015). https://doi.org/10.1145/2808006.2808022, https://dl.acm.org/doi/10.1145/2808006.2808022
14. Grant, N.: Google says trump's truth social must scrub violent content to join play store (2022). https://www.nytimes.com/2022/08/30/technology/google-trump-truth-social-violent-content.html
15. Harichandran, V.S., Walnycky, D., Baggili, I., Breitinger, F.: CuFA: a more formal definition for digital forensic artifacts **18**, S125–S137 (2016). https://doi.org/10.1016/j.diin.2016.04.005, https://www.sciencedirect.com/science/article/pii/S1742287616300366
16. Harwell, D.: Trump's truth social's disastrous launch raises doubts about its long-term viability (2022). https://www.washingtonpost.com/technology/2022/02/22/trump-truth-social-disaster/
17. Harwell, D., Kornfield, M.: FBI attacker was prolific contributor to trump's truth social website (2022). https://www.washingtonpost.com/technology/2022/08/12/shiffer-trump-truth-social-fan/
18. Hsu, T., Frenkel, S.: On truth social, F.B.I. search prompts talk of war, then conspiracy (2022). https://www.nytimes.com/2022/08/12/technology/truth-social-conspiracy-fbi-trump.html
19. Huber, M., Mulazzani, M., Leithner, M., Schrittwieser, S., Wondracek, G., Weippl, E.: Social snapshots: digital forensics for online social networks. In: Proceedings of the 27th Annual Computer Security Applications Conference, pp. 113–122 (2011)
20. Johnson, H., Volk, K., Serafin, R., Grajeda, C., Baggili, I.: Alt-tech social forensics: forensic analysis of alternative social networking applications. Forensic Sci. Int.: Digit. Investig. **42**, 301406 (2022)
21. Kan, M.: Mastodon threatens to sue trump's social media site for violating open-source license (2021). https://www.pcmag.com/news/mastodon-threatens-to-sue-trumps-social-media-site-for-violating-open-source
22. Khawas, C., Shah, P.: Application of firebase in android app development-a study. Int. J. Comput. Appl. **179**, 49–53 (2018). https://doi.org/10.5120/ijca2018917200
23. Kleinfeld, R.: The rise in political violence in the united states and damage to our democracy (2022). https://carnegieendowment.org/2022/03/31/rise-in-political-violence-in-united-states-and-damage-to-our-democracy-pub-87584
24. Menahil, A., Iqbal, W., Iftikhar, M., Shahid, W.B., Mansoor, K., Rubab, S.: Forensic analysis of social networking applications on an android smartphone. Wirel. Commun. Mob. Comput. **2021** (2021)

25. Pasquini, C., Amerini, I., Boato, G.: Media forensics on social media platforms: a survey. EURASIP J. Inf. Secur. **2021**(1), 1–19 (2021)
26. Rocha, A., et al.: Authorship attribution for social media forensics. IEEE Trans. Inf. Forensics Secur. **12**(1), 5–33 (2016)
27. Walnycky, D., Baggili, I., Marrington, A., Moore, J., Breitinger, F.: Network and device forensic analysis of android social-messaging applications. Digit. Investig. **14**, S77–S84 (2015)
28. Wu, S., Sun, W., Liu, X., Zhang, Y.: Forensics on Twitter and WeChat using a customised android emulator. In: 2018 IEEE 4th International Conference on Computer and Communications (ICCC), pp. 602–608. IEEE (2018)