Alt-Tech Social Forensics: Forensic Analysis of Alternative Social Networking Applications

By:
Hailey Johnson (University of New Haven), Karl Volk (University of New Haven), Robert Serafin (University of New Haven), Cinthya Grajeda-Mendez and Ibrahim Baggili (University of New Haven)

From the proceedings of

The Digital Forensic Research Conference

DFRWS USA 2022

July 11-14, 2022

TECH THROUGH
THE LENS OF
SECURITY

Alt-Tech Social Forensics: Forensic Analysis of Alternative Social Networking Applications

HAILEY JOHNSON
KARL VOLK
ROBERT SERAFIN
CINTHYA GRAJEDA
DR. IBRAHIM BAGGILI






University of New Haven
CONNECTICUT INSTITUTE OF TECHNOLOGY
UNHcFREG

This material is based upon work supported by the National Science Foundation under Grant Numbers 1900210 and 1921813.
Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Support

University of New Haven

AUTHOR INFORMATION

Hailey Johnson

M.S. Cybersecurity & Networks, Class 2022
hjohn5@unh.newhaven.edu

Karl Volk

B.S. Cyber Systems

Robert Serafin

M.S. Cybersecurity & Networks
B.S. Computer Engineering

Cinthya Grajeda

Cybersecurity Lab & Grants Manager
The Artifact Genome Project Manager

Dr. Ibrahim Baggili

Elder Family Endowed Chair
Director, Connecticut Institute of Technology

Agenda

- Introduction
- Research Questions & Contributions
- Review of Methodology
- Discussion of Results and Findings
- Analysis / Presentation of Tool
- Conclusion

Introduction

- The research conducted is based on forensic analysis of 9 alternative social networking applications: Parler, MeWe, CloutHub, Minds Mobile, Minds Chat, SafeChat, GETTR, Wimkin, and 2nd1st
  - Testing and analysis performed on Android and iOS mobile phones
- A command-line tool was developed to facilitate the automated retrieval of relevant artifacts from forensic images

Motivation and Research Questions

Motivation

- Alternative social media applications such are growing in popularity and have existing links to extremist individuals and recent threats to the United States government
  - Individuals were being restricted on mainstream applications, and these applications market themselves as providing a "free speech" platform and using little censorship
  - January 6th insurrection at the Capitol building
- Law Enforcement need a reliable and fast method to obtain data from phones using these newer applications

Research Questions

- What data can be found related to these applications?
- How can we extract the most relevant information investigators need?
- Can there be an automated tool built from this investigation that could help investigators extract and organize the major evidence in a fast and reliable manner?

Application Downloads

Table 1: Application capabilities, tests performed, and retrieved data

Application	Downloads	Capabilities	Performed tests	Retrieved artifacts
MeWe (2.18.30)	*5M+	Post, comment, chat	Post on feed Comment on posts Sent/received private messages Voice/video call	Message, post, contact and account information, cached images, device fingerprint/ID
CloutHub (1.19.7-Android) & (2.0.41-iOS)	*100k+	Post, comment, chat, and groups	Post on feed Comment on posts Post and comment in group Sent/received private messages	Message, post, and user information, and cached images
Minds (Mobile) (4.14.2-Android) & (4.20.0-iOS)	*500k+	Post & react to posts	Post on feed Comment on posts	Comment and post and cached images
Minds (Chat) (1.1.7-dev-Android) & (1.6.6-iOS)	*5k+	Chat and groups	Sent/received private messages	Videos, images, and emojis related to chat
SafeChat (0.9.46-Android) & (0.9.66-iOS)	*100k+	Post, comment, chat, voice/video call	Post on feed Commented on posts Sent/received private messages on feed	Message, post, and user information
GETTR (1.0.7-Android) & (1.2.7-iOS)	*5M+	Post & comment	Post on feed Commented on posts on feed	User, post, and comment information
Wimkin (2.1)	*5k+	Post, comment, chat, and groups	Post on feed Commend on posts Post and comment in group Sent/received private messages	Message, post, comment, user, and account information, and cached images
2nd1st (1.2.21)	**N/A	Post, comment, chat	Post on feed Comment on posts Sent/received private messages	Image posted
Parler (3.0.1-Android) & (2.50-iOS)	***16M	Post & comment	Post on feed Comment on posts	Image posted and account email

Where information on downloads was retrieved: *Google Play Store, **Download information not found, ***TechCrunch article (Silberling, 2022)

Related Work

- Work was conducted on social media applications:
  - Al Mutawa et al (2012) conducted manual forensics as well as the acquisition of logical images for Facebook, Twitter, and MySpace on BlackBerrys, Androids, and iPhones.
  - Walnycky et al. (2015) performed network and device forensic analyses of 20 Android social messaging applications, including Instagram, Facebook, and Viber.
  - Alisabeth and Pramadi (2020) also performed a forensic analysis on Instagram and was able to recover user account information and activity information, such as uploads and private message traces.
  - Menahil et al (2021) performed forensic analyses on Instagram, LINE, Whisper, WeChat, and Wickr.

Related Work Cont.

- Work was conducted on instant messaging applications:
  - Mahajan et al (2013), Karpisek et al (2015), and Arista Yuliani and Riadi (2019) all conducted research on and analyzed WhatsApp
  - Mahajan et al (2013) also conducted forensics on Viber
  - M. Ovens and Morison (2021) analyzed Wickr and the Private Text Messaging applications and detected cryptographic processes
- Extremist propaganda in social media:
  - Aliapoulious et al (2021) analyzed parler and presented an extensive dataset
  - Ferrara (2017) and Erbschloe (2019) examined how the spread of propaganda in social media has propelled radicalization
  - Longhi (2021) investigated the use of digital humanities and linguistics to assist with terrorism investigations

Contributions

- A primary mobile and network forensic analysis of the Parler, MeWe, SafeChat, Clouthub, Minds, 2nd1st, Wimkin, and GETTR applications.
- A collection of discovered digital forensic artifacts shared on the Artifact Genome Project – free access through **the Artifact Genome Project @ agp.newhaven.edu**
- An upgraded Python that can be used by digital forensic investigators to extract relevant data from the applications: https://github.com/unhcfreg/ASNAAT.git

Apparatus

Table A.3: Apparatus

Hardware/Software	Use	Company	Software Version
Galaxy S6	Application accounts (excluding 2nd1st)	Samsung	Nougat 7.0
Android ZTE	Application accounts (excluding 2nd1st)	Samsung	Nougat 7.1.1
iPhone 6s	Application accounts (excluding Wimkin)	Apple	iOS 14.4.2
iPhone 8	Application accounts (excluding Wimkin)	Apple	iOS 14.4.2
Thinkpad X1	Acquisition and analysis	Lenovo	Windows 10
Macbook Pro	Acquisition and analysis	Apple	macOS Big Sur 11.6
Ryzen Desktop PC	Acquisition and analysis	MSI	Windows 10 Education
Ubuntu Virtual Machine	Testing and analysis	Ubuntu	Ubuntu 20.04
Windows Virtual Machine	Testing and analysis	Windows	Windows 10
VirtualBox	Host VMs for testing and analysis	Oracle	6.1
Parler	Android and iOS Parler accounts	Parler	3.0.1 (Android) & 2.50 (iOS)
MeWe	Android and iOS MeWe accounts	MeWe	2.18.30
Clouthub	Android and iOS Clouthub accounts	Clouthub	1.19.7 (Android) & 2.0.41 (iOS)
Minds Mobile	Android and iOS Minds Mobile accounts	Minds Mobile	4.14.2 (Android) & 4.20.0 (iOS)
Minds Chat	Android and iOS Minds Chat accounts	Minds Chat	1.1.7-dev (Android) & 1.6.6 (iOS)
Safechat	Android and iOS Safechat accounts	Safechat	0.9.46 (Android) & 0.9.66 (iOS)
GETTR	Android and iOS GETTR accounts	GETTR	1.0.7 (Android) & 1.2.7 (iOS)
Wimkin	Android and iOS Wimkin accounts	Wimkin	2.1
2nd1st	Android and iOS 2nd1st accounts	2nd1st	1.2.21
Android Debug Bridge (ADB)	Communicate with tool and extract application data		1.0.41
Filza File Manager	File system manager	TIGI Software	3.8
DB Browser for SQLite	View databases	DB	3.35.5
iBackup Viewer	View iOS plists	iMacTools	4.22.1
Magnet Acquire	Physical acquisition for Android and iOS	Magnet Forensics	2.46.0.28200
Autopsy	Image viewer used for analysis	The Sleuth Kit	4.19.1
Wireshark	Capture and analyze network traffic	Wireshark	3.4.8
Fiddler	Analayze network traffic	Progress Software Corporation	3.0.1
Network Miner	Analyze network traffic	Netresec	2.7.1

Methodology & Approach

- Setup and scenario creation
  - The nine applications' features were tested with a user account. Devices were factory reset and rooted prior to use
  - A scenario was created that not only aimed to test the various functionalities within each application, but to also imitate realistic user activity
- Data acquisition
  - In this phase, in order to capture and analyze important artifacts in each application, data acquisition from mobile devices through device imaging was performed on the Android and iOS devices
  - Magnet acquire was used to acquire physical images of both devices after testing each application
  - Network traffic was captured while testing each application. It was noted that most of the traffic was encrypted and no essential artifacts were found
- Data analysis
  - To extract and analyze relevant artifacts from our data acquisition, tools and manual analysis were used
- Tool enhancement

Findings

Important Artifacts Extracted

Table 2: Important Artifacts Extracted Across All Forensic Acquisitions

Application, File ID & Artifact Name	Important Data Found in Disk										
	User ID	Name	Email	Phone #	Username	Timestamps	Posts/ comments	Media posted	Chats	Files sent/ received	Cached data
MeWe											
1.1 app_database, sgrouplesdb.sqlite	🤖, 🍎	🤖, 🍎			🤖, 🍎	🤖, 🍎	🤖, 🍎		🤖, 🍎		
1.2 Cache.db	🍎	🍎		🍎	🍎	🍎	🍎		🍎		
1.2 SGSession.xml	🤖	🤖		🤖	🤖	🤖					
1.3 tmp								🍎		🍎	
1.3 image_manager_disk_cache								🤖		🤖	🤖
1.4 default								🍎		🍎	🍎
Clouthub											
2.1 Clouthub.xml	🤖	🤖	🤖	🤖	🤖	🤖					
2.2 compressor								🤖		🤖	
2.1 Cache.db	🍎	🍎	🍎	🍎	🍎	🍎			🍎		
2.3 image_manager_disk_cache								🤖		🤖	🤖
2.2 tmp										🍎	
2.3 default											🍎
Minds Mobile											
3.1 minds1.db	🤖, 🍎				🤖, 🍎	🤖, 🍎	🤖, 🍎				
3.2 RKStorage	🤖				🤖	🤖					
3.3, 3.2 react-native-image-crop-picker								🤖, 🍎			
3.3 fsCachedData											🍎
3.4 image_manager_disk_cache								🤖			🤖
3.4 default											🍎
Minds Chat											
4.1 D										🤖	
4.1 Caches										🍎	
4.2 fsCachedData											🍎
4.2 emoji-recent-manager.xml						🤖			🤖		
4.3 image_manager_disk_cache										🤖	🤖

Important Artifacts Extracted

Table 2: Important Artifacts Extracted Across All Forensic Acquisitions

Application, File ID & Artifact Name	Important Data Found in Disk										
	User ID	Name	Email	Phone #	Username	Timestamps	Posts/ comments	Media posted	Chats	Files sent/ received	Cached data
SafeChat											
5.1 SafeChat								🤖		🤖	
5.1 .video								🍎		🍎	
5.2 cache										🤖	
5.2 tmp										🍎	
5.3, 5.4 SafeChat.db	🤖, 🍎	🤖, 🍎	🤖, 🍎	🤖, 🍎	🤖, 🍎	🤖, 🍎	🤖, 🍎		🤖, 🍎		
5.3 imagecache											🍎
5.4 download_tasks.db						🤖				🤖	
GETTR											
6.1 libCachedImageData.db								🤖			
6.2, 6.1 private_hughhen123.db, private_jmanny3.db	🤖, 🍎				🤖, 🍎	🤖, 🍎					
6.3, 6.2 g.db	🤖, 🍎				🤖, 🍎	🤖, 🍎					
6.3 Cache.db	🍎				🍎	🍎	🍎				
6.4, 6.8 libCachedImageData								🤖, 🍎			
6.4 flutter-images								🍎			
6.5 giphy_recents_file.xml								🤖			
6.5 .image								🍎			
6.6 giphy_searches_file.xml								🤖			
6.6 .video								🍎			
6.7 image_manager_disk_cache								🤖			🤖
6.7 fsCachedData											🍎
6.9 default								🍎			🍎

Important Artifacts Extracted

Table 2: Important Artifacts Extracted Across All Forensic Acquisitions

Application, File ID & Artifact Name	Important Data Found in Disk										
	User ID	Name	Email	Phone #	Username	Timestamps	Posts/ comments	Media posted	Chats	Files sent/ received	Cached data
Wimkin											
7.1 RKStorage	🤖	🤖	🤖		🤖	🤖					
7.2 v2.ols100.1								🤖		🤖	🤖
7.3 react-native-image-crop-picker										🤖	
7.4 cache										🤖	
7.5 rocketUser.xml	🤖										
7.6 io.invertase.firebase.xml	🤖	🤖			🤖	🤖	🤖		🤖		
7.7 chatplus-chat.wimkin.com.db.db	🤖	🤖			🤖	🤖			🤖		
2nd1st											
7.1 tmp								🍎			
Parler											
8.1 file_0.localstorage			🍎								
8.2 https_parler.com_0.localstorage			🍎								
8.3 tmp								🍎			

Key: 🤖: Android Mobile, 🍎: iOS Mobile

Important/interesting Artifacts

- MeWe - app_database

Table: CHAT_MESSAGE

Filter in any column

	createdAt	editedAt	textPlain	eventType	callWithVideo	callDuration	attachmentType	contentFeature	attachmentId	attachmentName
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1625259113	0	If we want to overthrow the government,we need to get ...	NULL	0	0	UNSUPPORTED	EMPTY	NULL	NULL
2	1625259123	0	How can I start spreading our message?	NULL	0	0	UNSUPPORTED	EMPTY	NULL	NULL
3	1625259132	0		NULL	0	0	PHOTO	EMPTY	60df7c7bcfe8c10387778326	image.jpg
4	1625259139	0	I have this bad boy!	NULL	0	0	UNSUPPORTED	EMPTY	NULL	NULL
5	1625259214	0	Nice pistol! To spread the message we can post stuff on ...	NULL	0	0	UNSUPPORTED	EMPTY	NULL	NULL
6	1625259289	0	https://www.openstreetmap.org/?...	NULL	0	0	UNSUPPORTED	EMPTY	NULL	NULL
7	1625259292	0	This is a secure location we can host meeting at.	NULL	0	0	UNSUPPORTED	EMPTY	NULL	NULL
8	1625259386	0	Cool that's perfect!	NULL	0	0	UNSUPPORTED	EMPTY	NULL	NULL
9	1625259407	0		NULL	0	0	PHOTO	EMPTY	60df7d8f6988ba61adcebd09	Screenshot_20210630-154408.jpg
10	1625259454	0	I have a guy who can get us stuff from the black market....	NULL	0	0	UNSUPPORTED	EMPTY	NULL	NULL
11	1625259515	0	https://www.cheaperthandirt.com/first-time-gun-buyer/...	NULL	0	0	UNSUPPORTED	EMPTY	NULL	NULL
12	1625259864	0	https://www.securityprousa.com/collections/body-armor-...	NULL	0	0	UNSUPPORTED	EMPTY	NULL	NULL
13	1625259885	0	https://thumbs.gfycat.com/HopefulVerifiableErmine-...	NULL	0	0	UNSUPPORTED	EMPTY	NULL	NULL
14	1625259887	0	Bail Organa is so done!!	NULL	0	0	UNSUPPORTED	EMPTY	NULL	NULL

Important/interesting Artifacts cont.

- Wimkin - io.invertase.firebase.xml


```
<map>
  <string name="0:1628524792446644%e15026a3e15026a3">{"sentTime":2147483647,"notification":{"body":"Sent an
  attachment","title":"Emmanuel Jones","android":
  {"sound":"default","clickAction":""}},"from":"826337191700","collapseKey":"com.wimkin.android","ttl":2419200,"messageId":"0:1628524
  {"roomName":"","payload":"{\"sender\":{\"name\":\"Emmanuel Jones\",\"_id\":\"CDyu4W2DtZg9AXNWk\",\"username\":\"profile-
  270131\"},\"host\":\"https:\\\/\\\/chat.wimkin.com\\\/\",\"messageId\":\"ph8i3krkRaHrwzs9K\",\"rid\":\"CDyu4W2DtZg9AXNWkZ27mpS8EDSL
  Jones","message":"Sent an attachment","username":"Emmanuel Jones","userId":"Z27mpS8EDSLQTY6c9","badge":"1"}}</string>
  <boolean name="crashlytics_auto_collection_enabled" value="true"/>
  <string name="0:1626304910633407%e15026a3e15026a3">{"sentTime":2147483647,"notification":{"body":"Emmanuel Jones commented on your
  status update Hi everyone! 😊","title":"","android":
  {"sound":"default","clickAction":""}},"from":"826337191700","collapseKey":"com.wimkin.android","ttl":2419200,"messageId":"0:1626304
  {"resource_link":"","web_link":"https:\/\/wimkin.com\/feed\/3575246\/?comment_id=1079581"}}</string>
  <string name="0:1628612039174101%e15026a3e15026a3">{"sentTime":2147483647,"notification":{"body":"Nicole Lahoud added you as a
  friend.","title":"New friend request","android":
  {"sound":"default","clickAction":""}},"from":"826337191700","collapseKey":"com.wimkin.android","ttl":2419200,"messageId":"0:1628612
  {"resource_link":"friend\/request\/6164348","web_link":"tab\/friend"}}</string>
  <string name="0:1628526225397853%e15026a3e15026a3">{"sentTime":2147483647,"notification":{"body":"Ok sounds good. Here is a helpful
  video I think we should all watch to learn some tactics for fighting","title":"Emmanuel Jones","android":
  {"sound":"default","clickAction":""}},"from":"826337191700","collapseKey":"com.wimkin.android","ttl":2419200,"messageId":"0:1628526
  {"roomName":"","payload":"{\"sender\":{\"name\":\"Emmanuel Jones\",\"_id\":\"CDyu4W2DtZg9AXNWk\",\"username\":\"profile-
  270131\"},\"host\":\"https:\\\/\\\/chat.wimkin.com\\\/\",\"messageId\":\"1b45877c-3b90-1f45-4a5d-
  7d5549a3fef4\",\"rid\":\"CDyu4W2DtZg9AXNWkZ27mpS8EDSLQTY6c9\",\"type\":\"d\"}","title":"Emmanuel Jones","message":"Ok sounds good.
  Here is a helpful video I think we should all watch to learn some tactics for fighting","username":"Emmanuel
  Jones","userId":"Z27mpS8EDSLQTY6c9","badge":"1"}}</string>
  <string name="0:1626301827056385%e15026a3e15026a3">{"sentTime":2147483647,"notification":{"body":"Emmanuel Jones added you as a
  friend.","title":"","android":
  {"sound":"default","clickAction":""}},"from":"826337191700","collapseKey":"com.wimkin.android","ttl":2419200,"messageId":"0:1626301
  {"resource_link":"","web_link":"https:\/\/wimkin.com\/user\/270131\/"}}</string>
  <string name="0:1626304887772891%e15026a3e15026a3">{"sentTime":2147483647,"notification":{"body":"Emmanuel Jones liked your photo
  Screenshot_20210702-151429","title":"","android":
  {"sound":"default","clickAction":""}},"from":"826337191700","collapseKey":"com.wimkin.android","ttl":2419200,"messageId":"0:1626304
  {"resource_link":"mobile\/photo\/1355628","web_link":"https:\/\/wimkin.com\/photo\/1355628\/"}}</string>
  <string name="0:1628526432005851%e15026a3e15026a3">{"sentTime":2147483647,"notification":{"body":"Sent an
  attachment","title":"Emmanuel Jones","android":
  {"sound":"default","clickAction":""}},"from":"826337191700","collapseKey":"com.wimkin.android","ttl":2419200,"messageId":"0:1628526
  {"roomName":"","payload":"{\"sender\":{\"name\":\"Emmanuel Jones\",\"_id\":\"CDyu4W2DtZg9AXNWk\",\"username\":\"profile-
  270131\"},\"host\":\"https:\\\/\\\/chat.wimkin.com\\\/\",\"messageId\":\"yxXJBoe3qaJcy28sb\",\"rid\":\"CDyu4W2DtZg9AXNWkZ27mpS8EDSL
  Jones","message":"Sent an attachment","username":"Emmanuel Jones","userId":"Z27mpS8EDSLQTY6c9","badge":"1"}}</string>
  <string name="0:1626304837322751%e15026a3e15026a3">{"sentTime":2147483647,"notification":{"body":"Emmanuel Jones liked your status
  update Hi everyone! 😊","title":"","android":
```

Vulnerabilities

- Vulnerabilities were found in three of the nine applications tested (33.3%), in which personal data was able to be accessed without expected authentication or authorization.
- Unencrypted links to media posted and sent through direct messages were stored in databases and were able to be accessed without proper authorization. Some were able to be accessed simply by copying and pasting the URL on the browser, while others required an account on the application to access the link.
- An application's database stored private information from channels that had been created. This included phone numbers, addresses, and emails that had been entered during the account creation.
- An application stored the password as an md5 hash

Md5 Hash


```
<map>
  <boolean name="First" value="true"/>
  <string name="password">050331835c451406a7098a69b46d9184</string>
  <string name="user_data_key">{"badgeType":"none","customTags":[{"a":"ironic","b":false},
  {"a":"imtired","b":false}],"defaultRoom":"main","displayname":"HughHen123","email":"hh8117505@gmail.com","facebookSyncStatus":"notsynced","firstname":"Hugh","followerCount":8
  05de-47e8-b411-38d46f10cbcb","jsonIssuesLocal":["Crime","Traffic","Over Development","Schools","Blight","Economic Development","Housing","Homelessness","Rent
  Control","Services","Infrastructure"],"jsonIssuesNtnl":["Economy","Jobs","Government Spending","Taxes","Immigration","Health Care","Mental
  Illness","Environment","Infrastructure","Protection of Faith","Drug Issues"],"jsonPolticlLeaning":["Conservative","Liberal","Middle of the Road","Decline to
  State"],"jsonPoltclRegstrtn":["Democrat","Republican","Independent","Green Party","Libertarian","Decline to State"],"lastname":"Henderson","mode":"sms","noticeSettings":
  {"connectionAccepted":true,"connectionRequested":true,"newComments":true,"newFollowers":true,"newLikes":true,"newMention":true,"newMessage":true,"newReplies":true,"newVotes":
  {"activityReadTime":"2021-06-30T15:06:32.258Z","glimpseReadTime":"2021-06-30T15:06:32.258Z","unreadGlimpse":false},"storageSettings":{"region":"us-west-
  1","forumBucket":"forum-clouthub","identityPoolId":"us-west-2:337e55d2-8df7-45da-a1de-83d437c8341b","identityRegion":"us-west-2","profileBucket":"profile-
  clouthub","provider":"login.clouthub.clouthub"},"token":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6IjM3MDY5ZmQ5LTA1ZGUtNDdlOC1iNDExLTM4ZDQ2ZjEwY2JjYiIsImlhdCI6MTYyNTUwMTAw
  D_44kGSEjfOz6M8oQHr1rR4b2Qf2-EBIf1hPD7qV4USXjBuK0RhS4dYTDUjEY98eSGW6CjhW22Q378YA7FknWe4_A87T4Z3QJufEshNtFXHy8gVIOQ4LtFT-1LWU_8kz4lgcEm6CFvVAs0NWkRY4iQZjFR-o3-
  jpzfe7NVdjb7hWAz1vITJ6Om2qAdQUmFqXSb-QZxmiPccHJdgPEdu1JXl39muySpJ61vAN_9lLoVUUIUZnNFfCkQg854VpKjfcUXVchHuLsBYSHb2AKlbotqJmX2wM5CXml_MU4nYC6zYb-
  Q","twitterSyncStatus":"notsynced","unreadActivities":7,"unreadBluePost":0,"unreadMainPost":0,"unreadMessages":false,"unreadRedPost":0,"unreadRequests":0,"userParameters":
  {"galleryVideoDuration":150,"messageCharacters":1000,"postCharacters":300,"quickVideoDuration":150},"username":"@HughHen123","verificationStatus":"none","viewVisibility":"all
  </string>
  <string name="app_setting__amplitude_api_key">afd905df6b6e94697b5c7a754c0ddccd</string>
  <boolean name="app_setting__amplitude_enable" value="true"/>
  <string name="setting_data_key">
  {"android_mandatory":2020020600,"android_recommended":2019110900,"channelsLink":"https://www.clouthub.com/more","extrasLink":"https://www.clouthub.com/extra","groupsLink":"ht
  {"blue":{"color":"#5BACAFFF","displayName":"Elect 2020","name":"blue"},"main":{"color":"#D8D8D8FF","displayName":"Main","name":"main"},"red":
  {"color":"#DFC7ABFF","displayName":"Fun \u0026 Sports","name":"red"}}}</string>
  <boolean name="firebase_token_ent_to_server" value="true"/>
  <string
  name="refresh_token">1ac2952477c154f5e5f3d4beba059250da71f5741eee891f23a6971064fe19db5531da0364adbf4845348b5f88e9d9b7727a866e2a60d8c07159cec512f17965f1928e9108d8fcb4f522a3998
  <string name="loginStatus">signin</string>
  <string name="app_setting__deeplink_domain_key">https://clthb.co</string>
  <string
  name="access_token">eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6IjM3MDY5ZmQ5LTA1ZGUtNDdlOC1iNDExLTM4ZDQ2ZjEwY2JjYiIsImlhdCI6MTYyNTUwMTAwNiwiZXhwIjoxNjI1NjczODA2fQ.agcKFGQ_jB
  D_44kGSEjfOz6M8oQHr1rR4b2Qf2-EBIf1hPD7qV4USXjBuK0RhS4dYTDUjEY98eSGW6CjhW22Q378YA7FknWe4_A87T4Z3QJufEshNtFXHy8gVIOQ4LtFT-1LWU_8kz4lgcEm6CFvVAs0NWkRY4iQZjFR-o3-
  jpzfe7NVdjb7hWAz1vITJ6Om2qAdQUmFqXSb-QZxmiPccHJdgPEdu1JXl39muySpJ61vAN_9lLoVUUIUZnNFfCkQg854VpKjfcUXVchHuLsBYSHb2AKlbotqJmX2wM5CXml_MU4nYC6zYb-Q</string>
  <string name="username">hh8117505@gmail.com</string>
  <string name=" id">37069fd9-05de-47e8-b411-38d46f10cbcb</string>
  <string name="app_setting__deeplink_weburl_key">https://app.clouthub.com</string>
</map>
```

Tool Development

- ASNAAT is the second generation of the original Python tool created in past research which was presented at the 2021 12th EAI International Conference on Digital Forensics & Cyber Crime and it will be published in the conference proceedings.
- The purpose of the Alternative Social Networking Applications Analysis Tool (ASNAAT) is to automatically aggregate the forensically relevant data from the researched alt-tech social applications.
- Extracting and presenting critical pieces of information in a report will assist investigators in triaging evidence found in forensic images acquired from Apple and Android smartphones.

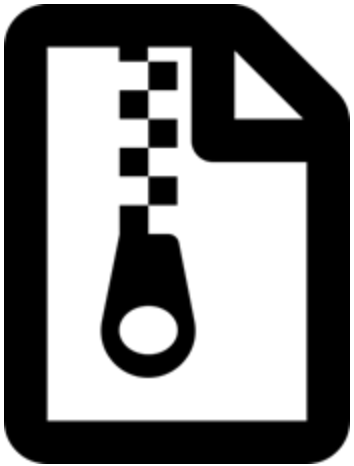
Algorithm 1 High-level Automation Algorithm

Requirements: Python3
Input: TAR image of a device.
Output: HTML Report

```
Select files to compare:
if "Help Option" then
 | show_manual();
else if "Apple Tar" then
 | A();
else if "Android Tar" then
 | B();

Select from installed apps (For terminal output):
if "All" then
 | AnalyzeApps = Installed;
else if "Specified" then
 | AnalyzeApps = Specified;

All apps analysis:
Initial_hash();
Search_archive();
extract_found();
analyze_files();
check_hashing();
generate_report();
```



Tool Output

Detailed Forensic Reports

Apple Forensics Report

Filename: 02-Apple
Case: 02
Timestamp: 02/10/2022-23:24:16 UTC
Examiner: Cinthya
Image Size: 12G
Extraction Time: 0:00:16
Before Analysis:
MD5: 35244f2ed0f59276767254fadd52341d
SHA256: 406e5b2f25d1bbaedb5924205df4e7ffaeb7c75dee41f208b3274c7bb20ee7a2
After Analysis:
MD5: 35244f2ed0f59276767254fadd52341d : Matched
SHA256: 406e5b2f25d1bbaedb5924205df4e7ffaeb7c75dee41f208b3274c7bb20ee7a2 : Matched

SafeChat.db - Conversation

serverId	ownerId	createdAt	localName	sharedKey	message
1414968261863211008	1410607368651767808	1626189697713	Hugh Henderson	siru1myEwH+oWbkc6IiPhZxewKIh3qX/|MHWL7OnkgDy3akLw8AB4/FBMLnaz/pNnQfNeMcDWGzk52Q3GqZNqb9Y6PynUBHJBiJcvv61FtuwHcPJG|0UfzQz6o3sNVHpEbR8zRIoE6e/kQ7cJGDYGAq+DMh2I=	Video call
1414981527800840192	1410607368651767808	1626192859713	None	xZzaA+xx64Fh3u824HcsltEn95PP1rEA|f+P2if0tPJ9lhXbtVA+1Q5t3qBkFhswAzzbxhLcUbNGoDfNHEow/Ht8R/8Wiogn6HsJhTR1STdSrMRqZ|5eTia9x4hOqvPIz0J/eNR5bWZUjilf23ojk5u2c+rio=	Global Training Center - rue habib themer, Tataouine, Tunisia

SafeChat.db - Message

senderId	conversationId	text	createdAt	encryptMode
1410642969231745024	1414968261863211008	Hi Emanuel! I saw you posted a pic about 2nd amendment rights. Nice. I stand by it	2021-07-13T15:29:26.7133+00:00	0
1410607368651767808	1414968261863211008	We need to stand together! Did you hear Bail Organa wants to take that right away from us?	2021-07-13T15:29:54.7133+00:00	0

.video Files

Filenames
1280x720_IMG_0010.mp4
1280x720_IMG_0011.mp4
IMG_0004.mp4
IMG_0011.mp4

Hash Table

Filename	SHA256
SafeChat.db	11b8e5508d1391ae9beff99750e77ccd6bd448f960bce89a690eca81c9f3e1cc
1280x720_IMG_0010.mp4	aa155a575084836e44a69e16f8572510a44ba0281edda5b119323d866daa5464
1280x720_IMG_0011.mp4	8de1566eaf5850728d79897c1b149d6042dc8f93af73891179934d15473e35bb
1626192834270.aac	4deb922535581b56e6bc62c20839ca04a4fdd45d7177edfe48605b6d4d390385
IMG_0004.mp4	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
IMG_0011.mp4	8aa328a67270764b6ef9f553aa944b35fe0d555776064814bb27fc516cac6ada
1280x720_IMG_0010.mp4	aa155a575084836e44a69e16f8572510a44ba0281edda5b119323d866daa5464
1280x720_IMG_0011.mp4	8de1566eaf5850728d79897c1b149d6042dc8f93af73891179934d15473e35bb
IMG_0004.mp4	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
IMG_0011.mp4	8aa328a67270764b6ef9f553aa944b35fe0d555776064814bb27fc516cac6ada

Android Forensics Report

Filename: 01-Android
Case: 01
Timestamp: 02/10/2022-23:18:03 UTC
Examiner: Cinthya
Image Size: 8G
Extraction Time: 0:00:02
Before Analysis:
MD5: bd06ea087217fd0ded0eb4a1dce10dea
SHA256: 7ef76004405052c6c5d78797d170efb0295f949f12ccf535d3a25933f855a777
After Analysis:
MD5: bd06ea087217fd0ded0eb4a1dce10dea : Matched
SHA256: 7ef76004405052c6c5d78797d170efb0295f949f12ccf535d3a25933f855a777 : Matched

Gettr | SafeChat | Minds Chat | Minds Mobile | Wimkin | CloutHub | MeWe

Direct Message Files

Filenames
Screenshot_20210630-105810.jpg
Screenshot_20210630-154408.jpg
Screenshot_20210702-151429.jpg

Clouthub.xml

Keys	Values
displayname	HughHen123
email	hh8117505@gmail.com
firstname	Hugh
followerCount	8

followingCount	1
friendCount	2
gender	Male
id	37069fd9-05de-47e8-b411-38d46f10cbcb
password	050331835c451406a7098a69b46d9184
phoneNo	**********
username	@HughHen123
app_setting__deeplink_weburl_key	https://app.clouthub.com

Hash Table

Filename	SHA256
Screenshot_20210630-105810.jpg	351a5bc5daaad17cdbffdcb5f381c972bc74c1979a508214e27c8aeaf786357a
Screenshot_20210630-154408.jpg	41514fe8cb5151823fdf026d81446ef7b0942ab575c047813d36df7524b2020f
Screenshot_20210702-151429.jpg	fe3d266c2d6d4ec5d54cee68cc742f799b0d72ded9b1cbbb7c4a7a69b4be67c1
Clouthub.xml	de8f338b0636e3d794064e27e92c9981d96afe4419c65d5e5b5cb8ccad619464

Conclusion

- Due to the increased popularity of social media applications, it is important to understand and have an effective way to extract digital artifacts that may be crucial to ongoing investigations.
- Information such as usernames, emails, full names, phone numbers, profile pictures, and more could be extracted, along with posts and comments and private messages.
- Through the usage of the ASNAAT tool, investigators can quickly obtain and analyze important information related to the applications.

Limitations/Future Work

- Not all artifacts are discussed in this paper, due to the vast number of data recovered and redundancy.
- Applications were updated during the testing phase. Although most did not alter the features, there were some significant changes between data found during preliminary testing and final testing.
- New applications are being developed more rapidly, and future work should explore updated versions of applications as well as new applications.
- In order to maintain the tool, future work should also include continual testing and improvements based on new and updated applications.

Credits

Thanks for listening!

We hope you learned something! Feel free to reach out with questions or ideas for improvement.

Contact

Hailey Johnson – hjohn5@unh.newhaven.edu

Karl Volk – kvolk1@unh.newhaven.edu

Robert Serafin – rsera1@unh.newhaven.edu

Tool: https://github.com/unhcfreg/ASNAAT.git

Artifact Genome Project – agp.newhaven.edu

References

Al Mutawa, N., Ibrahim, B. and Marrington, A. (2012), 'Forensic analysis of social networking applications on mobile devices', *Digital Investigation* **9**, 742–2876.

Aliaoulios, M., Bevensee, E., Blackburn, J., Bradlyn, B., De Cristofaro, E., Stringhini, G. and Zannettou, S. (2021), A large open dataset from the parler social network, *in* 'Proceedings of the International AAAI Conference on Web and Social Media (ICWSM2021)', pp. 943–951.

Alisabeth, C. and Pramadi, Y. R. (2020), Forensic analysis of instagram on android, *in* 'IOP Conference Series: Materials Science and Engineering', IOPscience.

Arista Yuliani, V. and Riadi, I. (2019), 'Forensic analysis whatsapp mobile application on android-based smartphones using national institute of standard and technology (nist) framework', *International Journal of Cyber-Security and Digital Forensics and The Society of Digital* **8**.

Baggili, I., Oduro, J., Anthony, K., Breitinger, F. and McGee, G. (2015), Watch what you wear: preliminary forensic analysis of smart watches, *in* 'Availability, Reliability and Security (ARES), 2015 10th International Conference on', IEEE, pp. 303–311.

Barrett, B. (2021), 'Whatsapp fixes its biggest encryption loophole'.
URL: *https://www.wired.com/story/whatsapp-end-to-end-encrypted-backups/*

Brown, A. (2021), 'Conservative social media app parler is pretty much dead'.
URL: *https://www.forbes.com/sites/abrambrown/2021/01/10/conservative-social-media-app-parler-is-pretty-much-dead/?sh=16396faf6a53*

Casey, P., Baggili, I. and Yarramreddy, A. (2019), 'Immersive virtual reality attacks and the human joystick', *IEEE Transactions on Dependable and Secure Computing* pp. 1–1.

Casey, P., Lindsay-Decusati, R., Baggili, I. and Breitinger, F. (2019), 'Inception: Virtual space in memory space in real space–memory forensics of immersive virtual reality with the htc vive', *Digital Investigation* **29**, S13–S21.

Chung, H., Park, J. and Lee, S. (2017), 'Digital forensic approaches for amazon alexa ecosystem', *Digital Investigation* **22**.

Clark, D. R., Meffert, C., Baggili, I. and Breitinger, F. (2017), 'Drop (drone open source parser) your drone: Forensic analysis of the dji phantom iii', *Digital Investigation* **22**, S3–S14.

Datareportal (2021), 'Global social media stats'.
URL: *https://datareportal.com/social-media-users*

Dickson, E. (2020), "free speech' social-media apps see enormous growth after the election'.
URL: *https://www.rollingstone.com/culture/culture-features/trump-election-facebook-twitter-mewe-parler-1088427/*

Dorai, G., Houshmand, S. and Baggili, I. (2018), I know what you did last summer: Your smart home internet of things and your iphone forensically ratting you out, *in* 'Proceedings of the 13th International Conference on Availability, Reliability and Security', ARES 2018, Association for Computing Machinery, New York, NY, USA.
URL: *https://doi.org/10.1145/3230833.3232814*

E. Salamh, F., Meraj Mirza, M., Hutchinson, S., Han Yoon, Y. and Karabiyik, U. (2021), 'What's on the horizon? an in-depth forensic analysis of android and ios applications', *IEEE Access* **99**, 1–1.

Erbschloe, M. (2019), *Extremist Propaganda in Social Media*, Taylor Francis Group.

Ferrara, E. (2017), 'Contagion dynamic of extremist propaganda in social networks', *Information Sciences* **418–419**, 1–12.

Greenberg, A. (2021), 'An absurdly basic bug let anyone grab all of parler's data'.

References Cont.

URL: *https://www.wired.com/story/parler-hack-data-public-posts-images-video/*

Johnson, D. (2020), 'What is a cache? a complete guide to caches and their important uses on your computer, phone, and other devices'.
URL: *https://www.businessinsider.com/what-is-cache*

Karpisek, F., Baggili, I. and Breitinger, F. (2015), 'Whatsapp network forensics: Decrypting and understanding the whatsapp call signaling messages', *Digital Investigation* **15**, 110–118.

Longhi, J. (2021), 'Using digital humanities and linguistics to help with terrorism investigations', *Forensic Science International* **318**.

M. Ovens, K. and Morison, G. (2021), 'Forensic analysis of instant messaging apps: Decrypting wickr and private text messaging data', *Digital Investigation* **17**, 40–50.

Mahajan, A., Dahiya, M. and Sanghvi, H. (2013), 'Forensic analysis of instant messenger applications on android devices', *International Journal of Computer Applications* **68**.

Mahr, A., Cichon, M., Grajeda, C. and Bagilli, I. (2021), 'Zooming into the pandemic! a forensic analysis of the zoom application', *Forensic Science International: Digital Investigation* **36**.

Mak, T. (2021), 'Across the internet, a game of whac-a-mole is underway to root out extremism'.
URL: *https://www.npr.org/2021/03/16/972519460/across-the-internet-a-game-of-whac-a-mole-is-underway-to-root-out-extremism*

Menahil, A., Iqbal, W., Iftikhar, M., Bin Shahid, W., Mansoor, K. and Rubab1, S. (2021), 'Forensic analysis of social networking applications on an android smartphone', *Wireless Communications and Mobile Computing* **2021**.

Newhouse, A. (2020), 'What to know about parler, the social-media platform that is now attracting millions of trump supporters'.
URL: *https://www.marketwatch.com/story/what-to-know-about-parler-the-social-media-platform-that-is-attracting-millions-of-trump-supporters-11606497149*

Richard Jones, K. (2017), 'Law enforcement use of social media as a crime fighting tool'.
URL: *https://core.ac.uk/reader/84755700*

Shalvey, K. (2021), 'Wimkin, a free speech network, says it was hit with a 'massive' ddos attack after being banned from apple's app store'.
URL: *https://www.businessinsider.com/apple-google-removed-wimkin-app-founder-reports-ddos-attack2021-1*

Silberling, A. (2022), 'Right-wing social app parler raises $20 million in funding'.
URL: *https://techcrunch.com/2022/01/07/right-wing-social-app-parler-raises-20m-in-funding/*

University, S. (2016), 'Fighting crime with mobile technology'.
URL: *https://www.southuniversity.edu/news-and-blogs/2016/08/fighting-crime-with-mobile-technology-137309*

Walnycky, D., Baggili, I., Marrington, A., Moore, J. and Breitinger, F. (2015), 'Network and device forensic analysis of android social-messaging applications', *Digital Investigation* .
URL: *https://www.sciencedirect.com/science/article/pii/S1742-287615000547*

Yarramreddy, A., Gromkowski, P. and Baggili, I. (2018), Forensic analysis of immersive virtual reality social applications: A primary account, *in* '2018 IEEE Security and Privacy Workshops (SPW)', IEEE, pp. 186–196.

Yurrieff, K., Fung, B. and O'Sullivan, D. (2021), 'Parler: Everything you need to know about the banned conservative social media platform'.
URL: *https://www.cnn.com/2021/01/10/tech/what-is-parler/index.html*

Yıldırım, , Bostancı, E. and Güzel, M. S. (2019), Forensic analysis with anti-forensic case studies on amazon alexa and google assistant build-in smart home speakers, *in* '2019 4th International Conference on Computer Science and Engineering (UBMK)', pp. 1–3.