

# Factorizing 2FA: Forensic Analysis of Two-Factor Authentication Applications

JESSICA BERRIOS  
ELIAS MOSHER  
SANKOFA BENZO  
CINTHYA GRAJEDA  
DR. IBRAHIM BAGGILI



# AUTHOR INFORMATION

## **Jessica Berrios**

SFS Scholar  
M.S. Cybersecurity 2025  
B.S. Cybersecurity 2023

## **Elias Mosher**

B.S. Computer Science  
M.S. Cybersecurity 2023

## **Sankofa Benzo**

SFS Scholar  
B.S. Cybersecurity 2024

## **Cinthya Grajeda**

Cybersecurity Lab &  
Grants Manager  
The Artifact Genome  
Project Manager

## **Dr. Ibrahim Baggili**

Former Director, UNHcFREG  
AGP Grant PI  
Director, BiT Lab  
Professor of Cybersecurity & Computer  
Science at LSU



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.

# Agenda

- Introduction
- Motivation & Research Questions
- Review of Methodology and Approach
- Discussion of Results and Findings
- 2FA Bypass
- Conclusion

# Introduction

- The growing need for Two-Factor Authentication (2FA).
- This research focuses on Time-based One-Time Password (TOTP) authentication.
  - 15 2FA applications were tested.
- To have a broad set of artifacts, the experiments were performed on three operating systems.
- How 2FA works: Enable a second factor of verification during the login process.

# Motivation and Research Questions

## Motivation

- Due to its growing nature 2FA has attracted adversaries.
- There is a growing need to understand what kind of data is being stored.
  - In 2021, Google enrolled 150 million of its users in 2FA & consequently 50% of those avoided being compromised.
  - In 2022, according to the ICR there have been 3.36 million cybercrime complaints, which resulted in \$27.6 billion in total losses.

## Research Questions

- What user data can be found from the 2FA applications through memory, network, & disk forensics?
- Who finds the information useful?
- Are organizations implementing accurate and extensive security measures to keep users' data protected?

# Previous Work

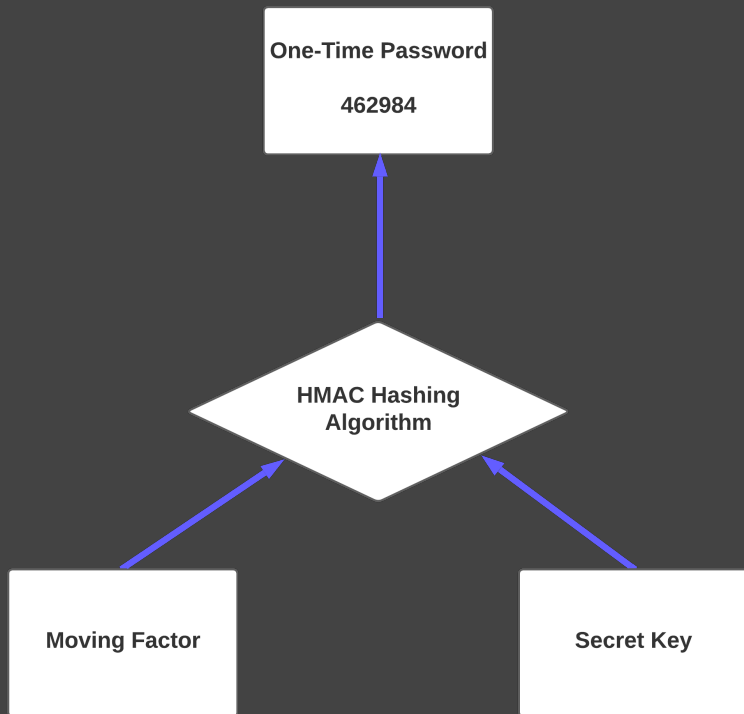
- Ozcan and Bicakci's "Security analysis of mobile authenticator applications" (2020).
  - Showcased what 2FA artifacts could be located on an Android device.
  - Utilized simple Android RE techniques to acquire Artifacts.
  - Explained the underlying algorithm of TOTP.

# Background Info

HMAC and TOTP







# HMAC

- The Hash-Based Authentication Code.
- Generates One-Time Passwords (OTP).
- Hashes the moving factor & a secret key.
- Output is a fixed length.
- For 2FA there are two major forms of HMAC.
- TOTP (Time-based One-Time Password).
- HOTP (HMAC-based One-Time Password).

# facebook

Mary Smith token is:

726 410

Your token expires in **24**




## TOTP

- Time-based One-Time Password.
- HMAC with time as the moving factor.
- The 2FA type focused on in this paper.
- Supported by all major social media outlets.
- Major company applications use TOTP (e.g. Microsoft, Google).

# TOTP User Experience

← Two-factor authentication



## Help protect your account

If we notice an attempted login from a device or browser we don't recognize, we'll ask for your password and a verification code.


## Select a security method

**Authentication app**  
**Recommended** · Use an app like Google Authenticator or Duo Mobile to generate verification codes for more protection.

← Two-factor authentication

### Set up via third party authenticator

Please use your authentication app (such as Duo or Google Authenticator) to scan this QR code.



Set up on same device

Or enter this code into your authentication app  
**K4JU JOVS DELG QTGN RU34 AXEE MVR6 HCLN**

× Add Key

ACCOUNT NAME  
agp.unh@gmail.com


ACCOUNT KEY  
K4JU JOVS DELG QTGN RU34 AXEE MVR6 HCLN

ISSUER NAME  
Facebook

ACCOUNT LABEL  
Entertainment

☰ Accounts 🔍 📄

Social



936 366  
agp.unh@gmail.com  
Facebook





















# Methodology



# Apparatus

Table A.4: Apparatus

Hardware/Software	Use	Company	Software Version
Galaxy S6	2FA Accounts	Samsung	7.0
iPhone 7	2FA Accounts	Apple	14.7.1
Android Debug Bridge (ADB)	Data Extract	Android Studio Developers	N/A
Magnet Acquire	Data Extract	Magnet Forensics	2.56.0.31667
FTK Imager	Data Extract	AccessData	4.7.1
ArtEx	Data Extract	DoubleBlak	2.4.12
Autopsy	Data Analysis	Basis Technology	4.19.3
Wireshark	Network Extract/Analysis	Wireshark, Inc	3.6.6
Fiddler	Network Extract/Analysis	Telerik, Inc	v5.0.20211
DB Browser for SQLite	File Analysis	DB	N/A
Instagram	2FA Testing	Meta Platforms, Inc.	254.0.0.19.109
Facebook	2FA Testing	Meta Platforms, Inc.	386.0.0.35.108
Twitter	2FA Testing	Twitter, Inc.	9.61.0-release.0
Dropbox	2FA Testing	Dropbox, Inc.	298.2.2
Snapchat	2FA Testing	Snap, Inc.	12.01.0.33
VMware Fusion	Platform to Host VM	VMware, Inc.	12.2.4
Windows 10 Education	Windows VM for Testing	Microsoft, Inc.	21H2
Bulk Extractor	Memory Analysis	N/A	2.0.0
Linux Strings Command	Memory Analysis	N/A	N/A

Application	Version	Platform	Downloads
Aegis	2.0.3		100K+
FreeOTP	1.5		1M+
TOTP	1.89		100K+
Google	5.20R4	 / 	100M+
Microsoft	6.2207.4624	 / 	50M+
2FAS	3.17.0	 / 	1M+
Twilio Authy	4.8.8	 /  / 	10M+
Okta Verify	7.9.0		36K
Two-Factor	1.5		25
FIS Authenticator	4.4.6		120
Epic Authenticator	1.0		21
IBM Verify	2.5.2		72
Authenticator+	2.0.4		N/A
WinAuth	3.5.1		N/A
2 Factor Auth	2.5.1804		N/A

Key: : Android, : iOS, : Windows

# Phase One & Two

- Fifteen total applications were tested across three different operating systems.

## Environment Set-up

- The devices used were factory reset and rooted.
- Device was sanitized of any unnecessary applications.
- Accounts were created for the applications 2FA was tested against.

## Data Acquisition

- A diverse set of tools were used in order to acquire disk and memory.
- Hotspot was set-up in order to collect network traffic.

# Contributions

- A peer-reviewed paper discussing the structure of 2FA and the artifacts found through the analysis of memory, network, and disk.
- A presentation of digital artifacts found within forensic images, and an educational module as a case scenario—free access through **the Artifact Genome Project @**  
**agp.newhaven.edu**

# Findings





# Results Overview

- Android Device rendered most results.
- Secret Keys were found across the network, memory, & disk.
- PII was located across all three devices.
- Passwords were stored in plain-text on disk artifact.

# 2FA Important Artifacts Found Across All Acquisition Types

	Issuer Name	Account Name	Email	Secret Keys	Timestamps	Encrypted Secret Keys	Salt	Phone Number	Application Lock Pin
Aegis Locked				A			A		
Aegis Unlocked	A	A	A	A					
Authenticator+	I	I		I	I				
Epic Authenticator		I		I					
FIS Authenticator	I	I		I					
FreeOTP	A	A				A			
Google Authenticator	A	A			A	A			
IBM Verify	I	I		I					
Microsoft Authenticator	A	A		A					
Okta Verify	I	I							
TOTP Locked	A	A	A		A	A			A
TOTP Unlocked	A	A	A		A	A			
Twilio Authy Locked	A		A	A	A	A	A	A	A
Twilio Authy Unlocked	A		A	A	A/W	A	A	A	
Twilio Authy Memory*	W		W			W		W	
Twilio Authy Network*	W		W	W					
Two-Factor	I	I		I	I				
WinAuth	W			W	W				
WinAuth Memory*	W		W			W			
WinAuth Network*	W			W					
2FAS Locked					A	A			
2FAS Unlocked	A/I	A/I			A	A			
2 Factor Authenticator Memory*	W	W	W	W		W			
2 Factor Authenticator Network*	W			W					

Key: A: Android Mobile, I: iOS Mobile, W: Windows, Memory\* or Network\*: Memory or network acquisition only.

# Sample Artifacts

```
"type": "totp",
"uuid": "8d5f9ef6-f01f-4fd2-b0b8-4503f26c3d96",
"name": "agp.unh@gmail.com",
"issuer": "Facebook",
"note": "",
"icon": null,
"info": {
  "secret": "043RIEYICE2QLPE5S2J0CB23E4QFDUUJ",
  "algo": "SHA1",
  "digits": 6,
  "period": 30
}
```

Figure 1: JSON file artifact from Aegis

nts 5 entries Page 1 of 1 Export to CSV

group_key	name	username	paws_url	oath_secret_key
00000000...	Facebook	Facebook		AJAS ANIK I7CG 573V 6JHK TK4Q RJNI W16E
00000000...	Twitter	Twitter		EXTRM6UPQ536YPTP
00000000...	Snapchat	jess_c2022328		UTWCDBR4PIBPWGGZDCH2OMRI6C5ONOAU
00000000...	Dropbox	Dropbox		6a2ni2bovtkq6uximxcui7la6u
00000000...	Instagram	instagram		MEMA ABNO QBIZ RHEU NSMK MNZM 7G4Z P5LG

Figure 2: Database artifact from Microsoft Authenticator



# Sample Artifacts

```
AuthyFBCode.txt
1  YA6BTLFJGANJFV3RVVHVNKSFINMQNX3HL
2
```

Figure 3: Desktop memory artifact from Authy

```
ail":"benzotesting@gmail.com","countryCode":1,"cellphone":"754-242-5457","userId":"618627374","multiDevicesEnabled":true}TBYYr8Z53YZHRz"}
Temail":"benzotesting@
https://www.dropbox.com/benzotesting@gmail.com
https://accounts.snapchat.com/benzotesting@gmail.com
https://twitter.com/benzotesting@gmail.com
{"email":"benzotesting@gmail.com","countryCode":1,"cellphone":"754-242-5457","userId":"618627374","multiDevicesEnabled":true}
login_emailbenzotesting@gmail.com
textbenzotesting@gmail.com
benzotesting@gmail.com
benzotesting@gmail.com
https://www.dropbox.com/benzotesting@gmail.com
https://accounts.snapchat.com/benzotesting@gmail.com
https://twitter.com/benzotesting@gmail.com
benzotesting@gmail.com
login_emailbenzotesting@gmail.com
textbenzotesting@gmail.com
benzotesting@gmail.com
":"benzotesting@
ail":"benzotesting@gmail.com","cellphone":"754-242-5457","country_code":1,"multidevice_enabled":true,"multidevices_enabled":true,"primary_email_verified":false,"success":true}
{"email":"benzotesting@gmail.com","countryCode":1,"cellphone":"754-242-5457","userId":"618627374","multiDevicesEnabled":true}
benzotesting@gmail.com
{"email":"benzotesting@
login_emailbenzotesting@gmail.combenzotesting@gmail.comc
textbenzotesting@gmail.combenzotesting@gmail.comc
ail":"benzotesting@gmail.com","countryCode":1,"cellphone":"754-242-5457","userId":"618627374","multiDevicesEnabled":true}HRz"}439522e1fd31c82
{"email":"benzotesting@gmail.com","countryCode":1,"cellphone":"754-242-5457","userId":"618627374","multiDevicesEnabled":true}HRz"}

```

Figure 4: Memory artifact from Authy

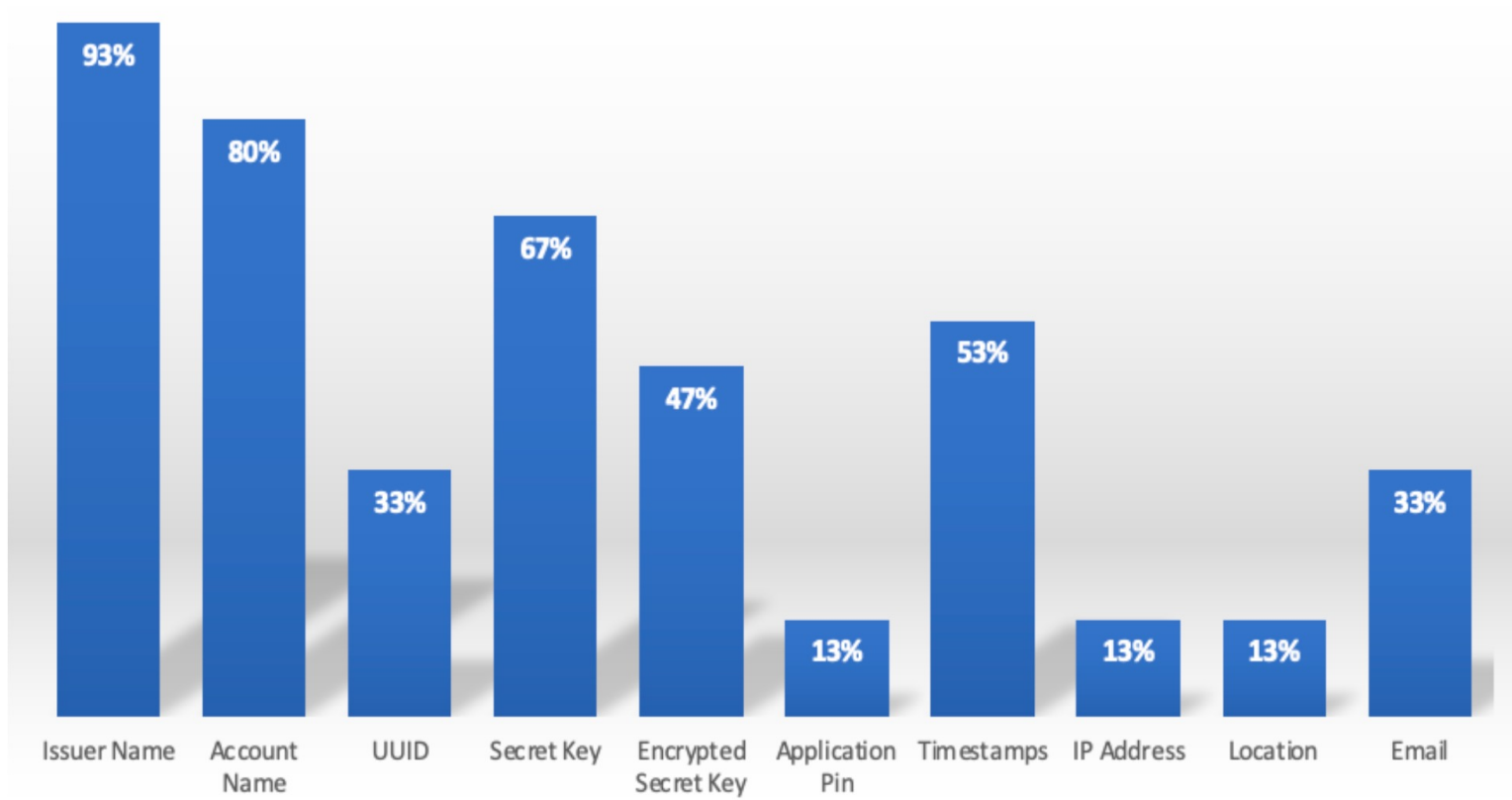


# Data Analysis

The graph shown is a summary of the number of applications containing important information.

The artifact acquired and analyzed fell under one of the following categories:

- Secret/Encrypted Keys
- Account Information
- PII



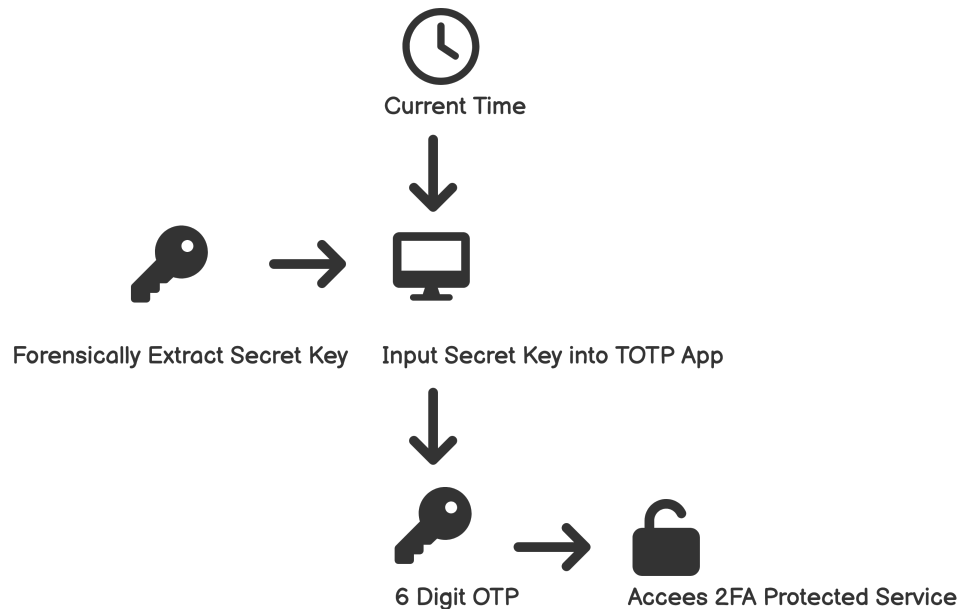
**Artifact Commonalities**

# 2FA Bypass



# 2FA Bypass

- Performing the bypass:
  - Extract a TOTP secret key from a disk image.
  - Input the key into the TOTP application of choice.
  - Use the valid token generated to authenticate.





1:47



## OTP Accounts



Twitter



John Doe 9

**789403** 

Time Remaining **7**

### My Accounts



Twitter

# Bypass Implications

## Criminal Activity

- Local bypass requires target phone to be stolen, unlocked, & rooted.
- A remote bypass is possible with network traffic sniffing.

## Law Enforcement

- Allows law enforcement to preserve 2FA tokens without the original device.
- Particularly useful if the original device is inaccessible.

# Conclusions

- Two-Factor Authentication is an ever-growing field which requires more forensic research to fully understand.
- TOTP applications store a plethora of useful artifacts across different operating systems.
- PII and secret keys were found in plain text on many of the 15 2FA apps tested.
- 10/15 secret keys, 12/15 usernames, 14/15 issuer names.
- Organizations developing 2FA apps may want to review how they secure data.



# Future Work

- Research alternative forms of 2FA.
  - HOTP
  - Push Mobile Authentication
  - Multi-Factor Authentication
- Continue research on new and updated TOTP applications.
- Analyze 2FA applications on other OS's such as MacOS & Linux.
- Further research on alternate methods to extract artifacts.
  - Reverse Engineering



# Thanks for listening!

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

# Contact

Jessica Berrios – [Jberr6@unh.newhaven.edu](mailto:Jberr6@unh.newhaven.edu)

Elias Mosher – [Emosh1@unh.newhaven.edu](mailto:Emosh1@unh.newhaven.edu)

Sankofa Benzo – [Sbenz1@unh.newhaven.edu](mailto:Sbenz1@unh.newhaven.edu)

Cinthya Grajeda– [Cgrajedamendez@newhaven.edu](mailto:Cgrajedamendez@newhaven.edu)

Dr. Ibrahim Baggili– [Ibaggili@lsu.edu](mailto:Ibaggili@lsu.edu)

Artifact Genome Project – [agp.newhaven.edu](http://agp.newhaven.edu)