Securing Software Applications: E2EE Practices for API EndPoints

Justice Owusu Agyemang

PRESENTATION OUTLINE

- Introduction
- Client-Server Architecture
- Securing API EndPoints
- Conclusion

$WHOAMI

- Justice Owusu Agyemang
- DPhil Student / Researcher at KNUST
- Huawei Certified Network Associate
- Huawei Certified Academy Instructor
- **Research Areas**: Internet of Things (IoT), Network and Application Security, Artificial Intelligence and Applied Cryptography.

INTRODUCTION

"..... Let's create an App"

INTRODUCTION

"..... coding begins."

INTRODUCTION

..... app completed.

..... people start using the app.

INTRODUCTION

We recently discovered that some user data was compromised as a result of unauthorized access to one of our systems by a malicious third party. We are working rapidly to investigate the situation further and take the appropriate steps to prevent such incidents in the future.

We also want to be as transparent as possible without compromising our security systems or the steps we're taking, and in this post we'll share what happened, what information was involved, what we're doing, and what you can do.

We're very sorry for any concern or inconvenience this may cause.

..... the sad story 😔.

INTRODUCTION

What information was involved

For approximately 100 million Quora users, the following information may have been compromised:

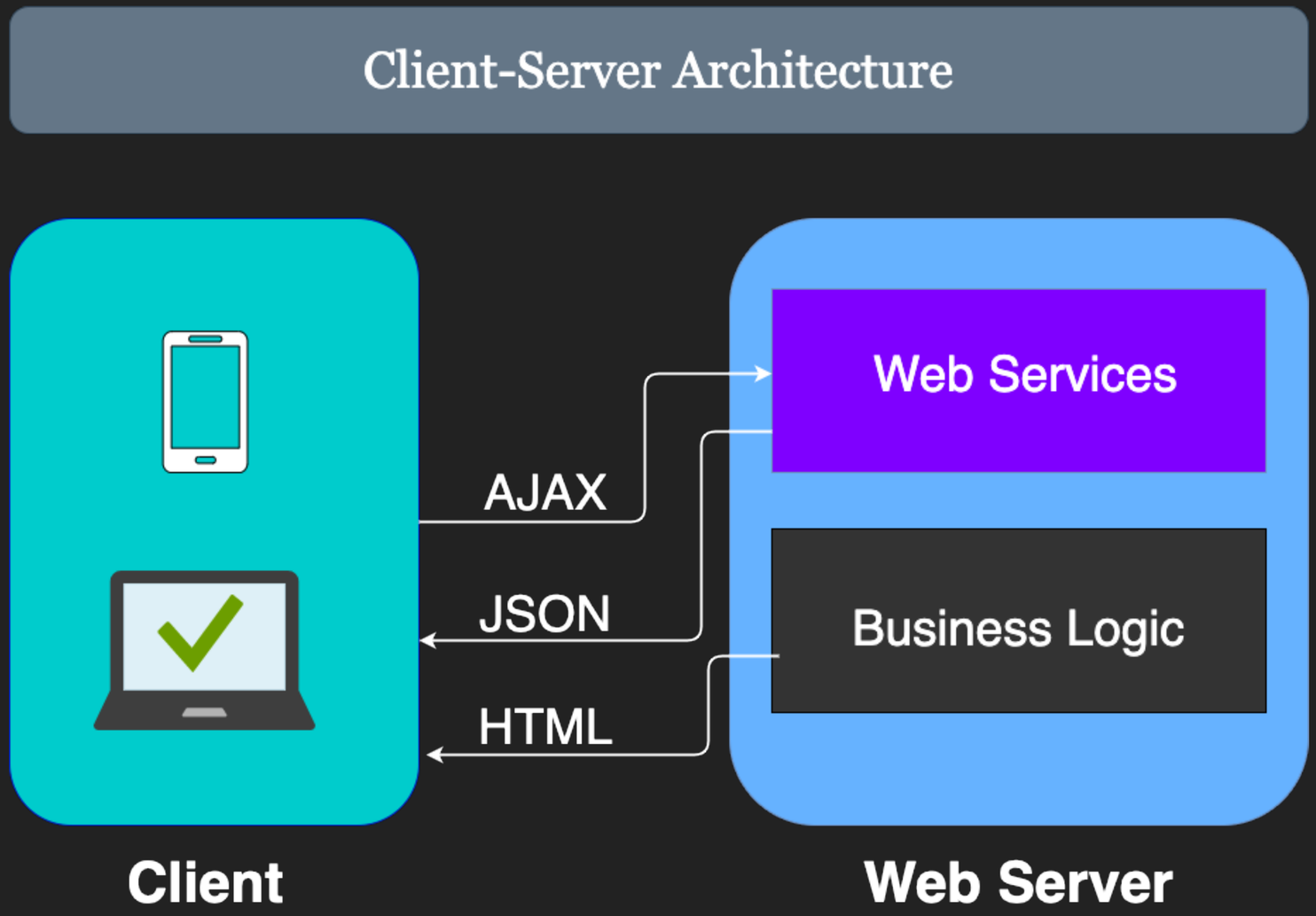
- Account information, e.g. name, email address, encrypted password (hashed using bcrypt with a salt that varies for each user), data imported from linked networks when authorized by users
- Public content and actions, e.g. questions, answers, comments, upvotes
- Non-public content and actions, e.g. answer requests, downvotes, direct messages (note that a low percentage of Quora users have sent or received such messages)

..... the sad story 😔.

INTRODUCTION

WHAT WENT WRONG?

THE THREAT LANDSCAPE



SECURING API ENDPOINTS

BASIC SECURITY REQUIREMENTS

SECURING API ENDPOINTS

SECURITY RISKS

BROKEN AUTHENTICATION

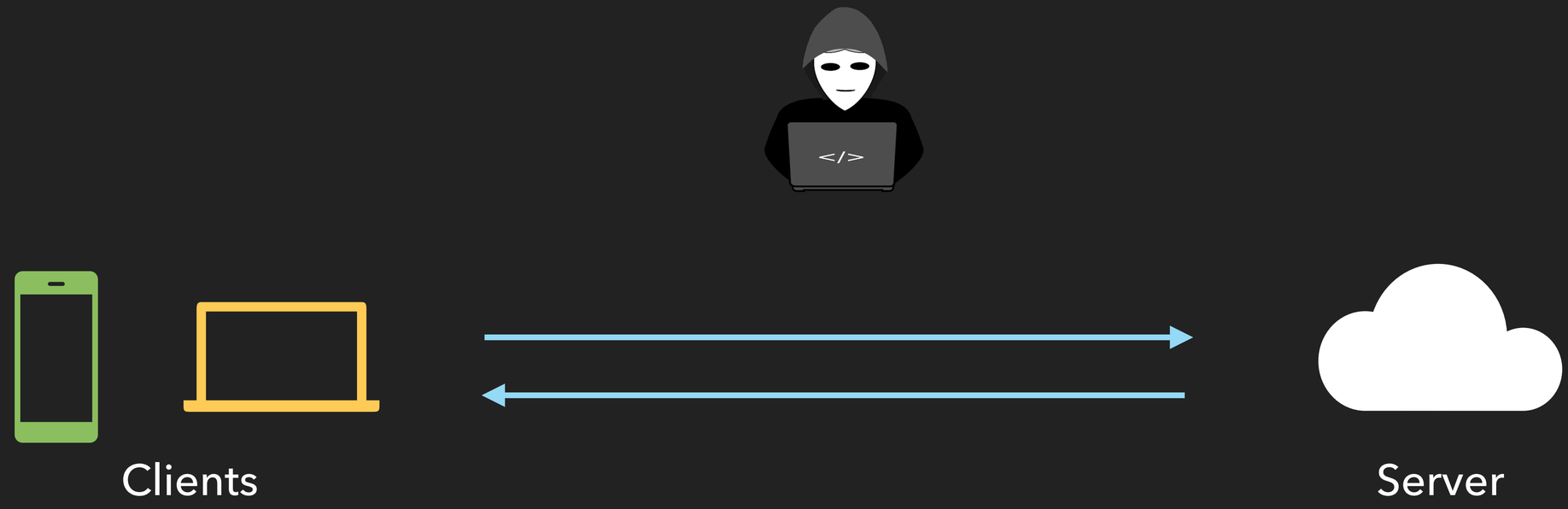
SENSITIVE DATA EXPOSURE

SECURITY MISCONFIGURATIONS

USING COMPONENTS WITH KNOWN VULNERABILITIES

SECURING API ENDPOINTS

SECURITY RISKS

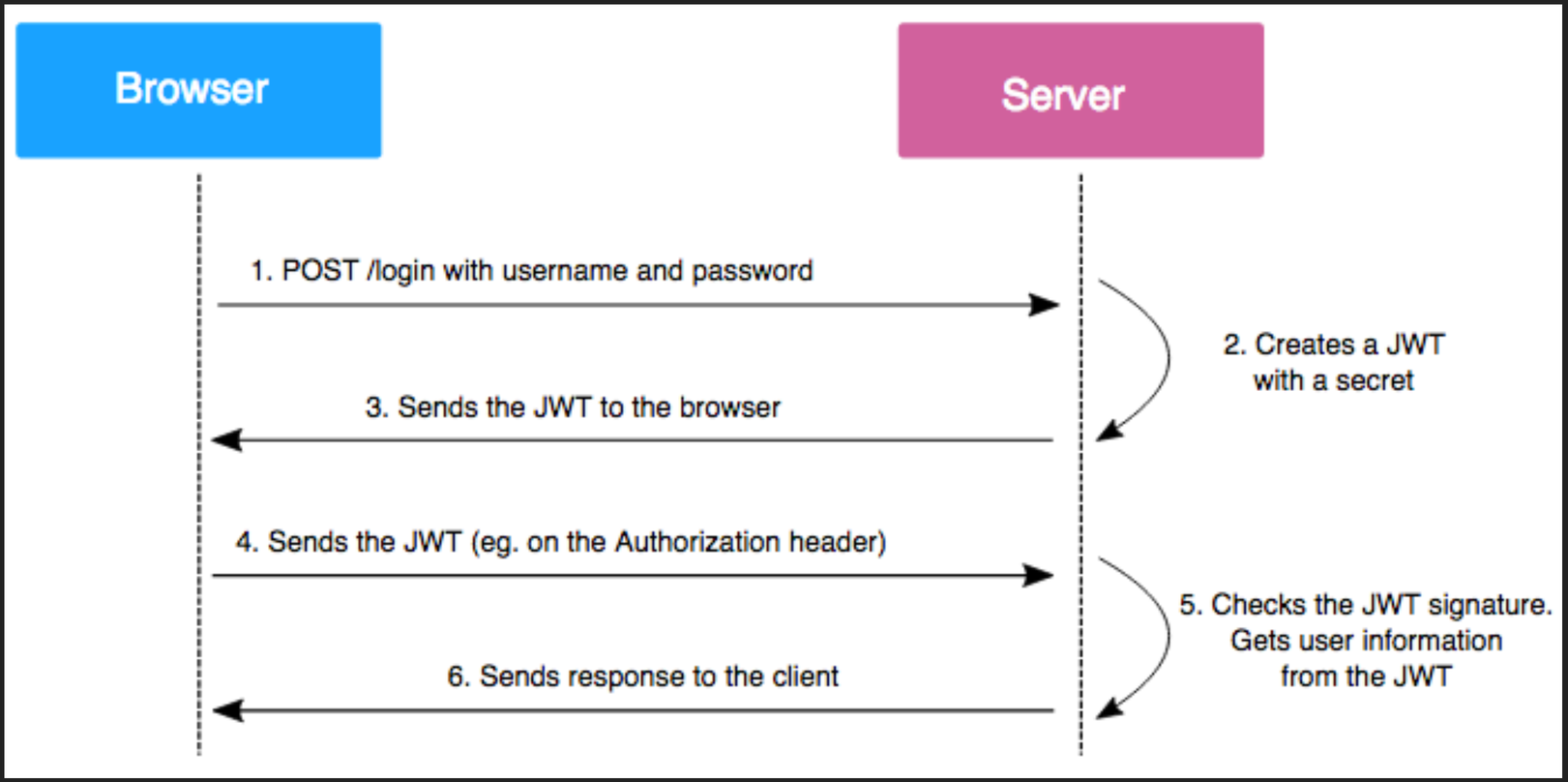


DEMO 1

ECG Prepaid App & KNUST AIM App

SECURING API ENDPOINTS

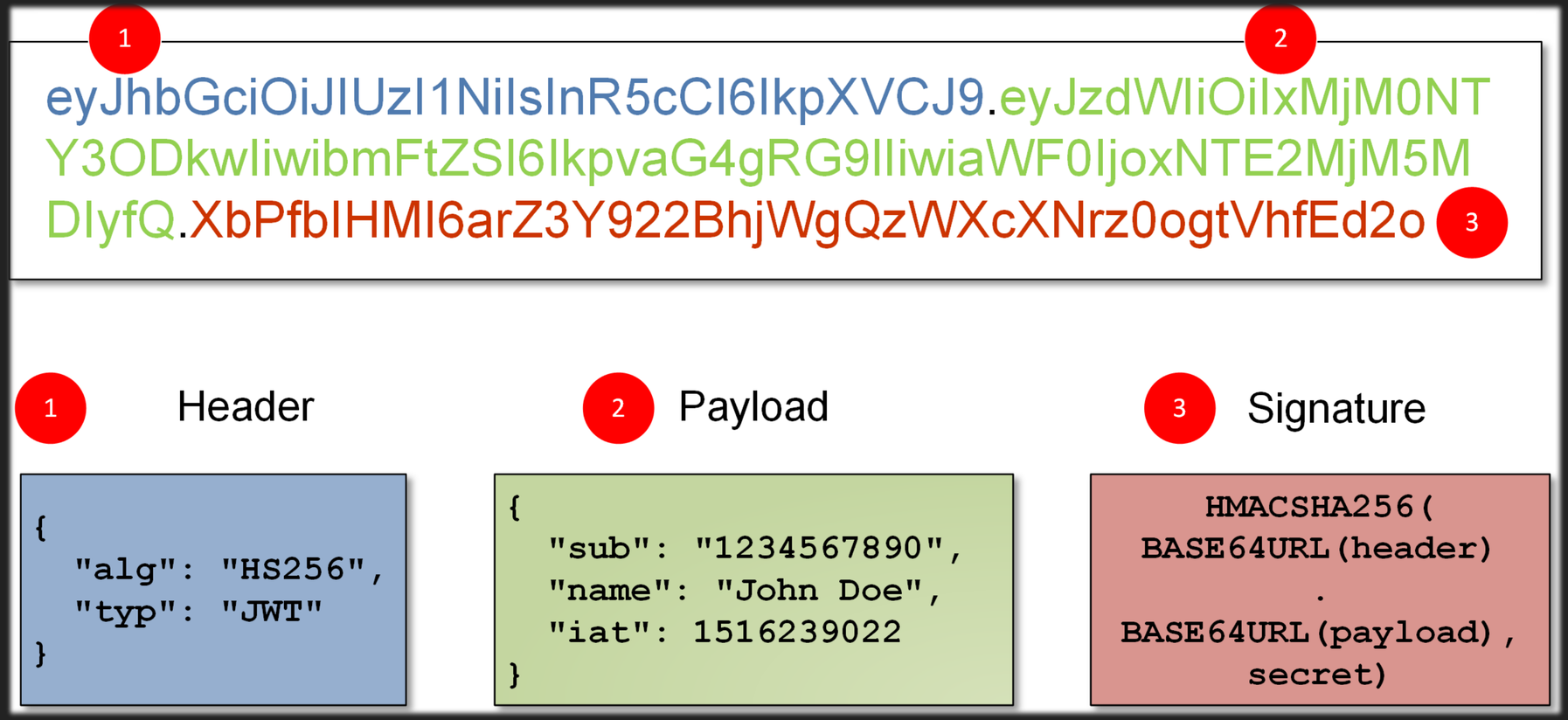
AUTHENTICATION



JWT authentication

SECURING API ENDPOINTS

AUTHENTICATION



JWT Structure

SECURING API ENDPOINTS

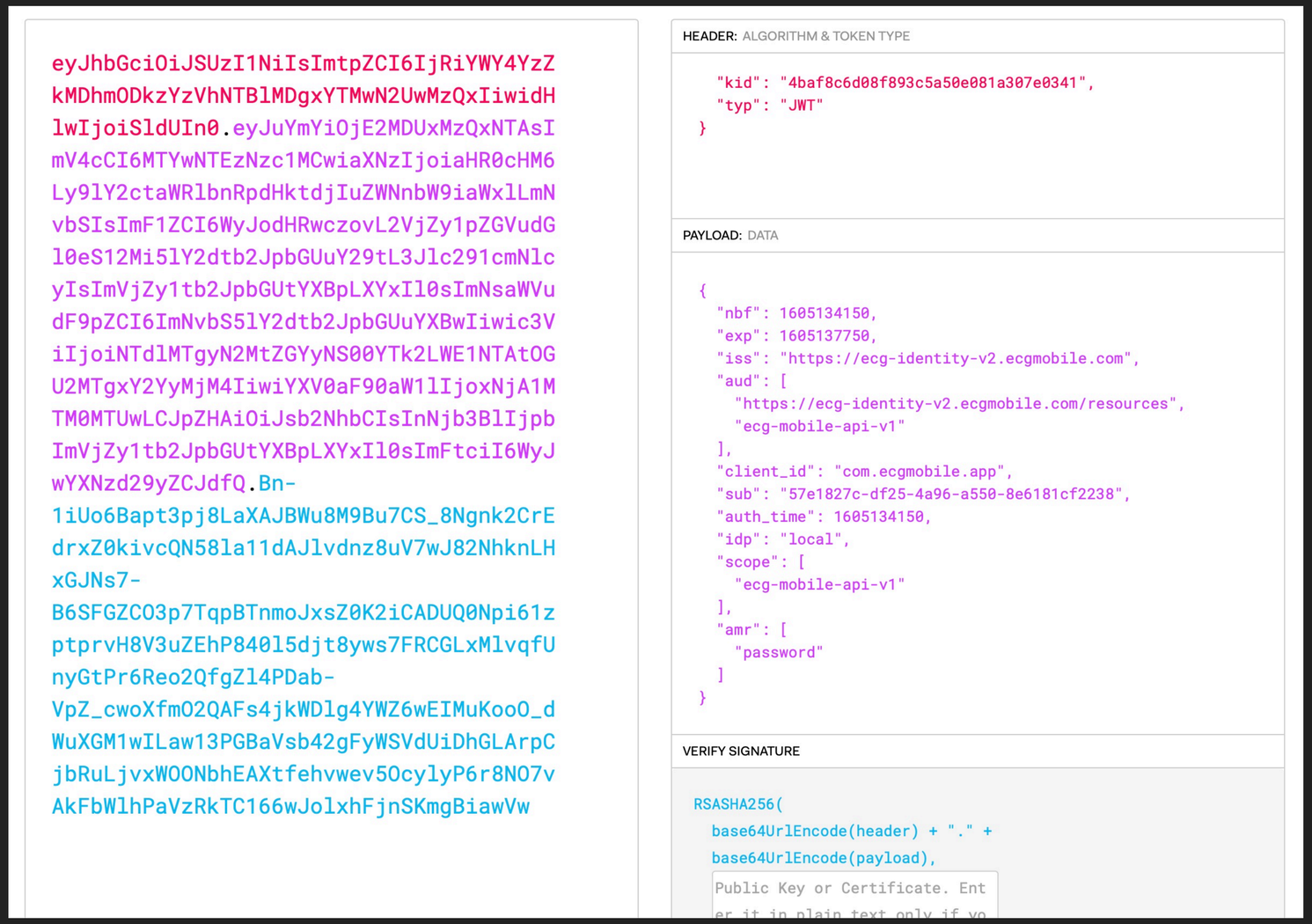
AUTHENTICATION - ECG PREPAID APP


```
{
    "access_token": "eyJhbGciOiJSUzI1NiIsImtpZCI6IjRiYWY4YzZkMDhmODkzYzVhNTBlMDgxYTMwN2UwMzQxIiwidHlwIjoiSldUIn0.
        eyJuYmYiOjE2MDUxMzQxNTAsImV4cCI6MTYwNTEzNzc1MCwiaXNzIjoiaHR0cHM6Ly9lY2ctaWRlbnRpdHktdjIuZWNnbW9iaWxlLmNvbSIsImF1ZCI6WyJodHRwczovL2VjZy1pZGVudGl0eS12Mi5lY2dtb2JpbGUuY29tL3Jlc291cmNlcyIsImVjZy1tb2JpbGUtYXBpLXYxIl0sImNsaWVudF9pZCI6ImNvbS5lY2dtb2JpbGUuYXBwIiwic3ViIjoiNTdlMTgyN2MtZGYyNS00YTk2LWE1NTAtOGU2MTgxY2YyMjM4IiwiYXV0aF90aW1lIjoxNjA1MTM0MTUwLCJpZHAiOiJsb2NhbCIsInNjb3BlIjpbImVjZy1tb2JpbGUtYXBpLXYxIl0sImFtciI6WyJwYXNzd29yZCJdfQ.
        Bn-1iUo6Bapt3pj8LaXAJBWu8M9Bu7CS_8Ngnk2CrEdrxZ0kivcQN58la11dAJlvdnz8uV7wJ82NhknLHxGJNs7-B6SFGZCO3p7TqpBTnmoJxsZ0K2iCADUQ0Npi61zptprvH8V3uZEhP840l5djt8yws7FRCGLxMlvqfUnyGtPr6Reo2QfgZl4PDab-VpZ_cwoXfmO2QAFs4jkWDlg4YWZ6wEIMuKooO_dWuXGM1wILaw13PGBaVsb42gFyWSVdUiDhGLArpCjbRuLjvxWOONbhEAXtfehvwev5OcylyP6r8NO7vAkFbWlhPaVzRkTC166wJolxhFjnSKmgBiawVw",
    "expires_in": 3600,
    "token_type": "Bearer"
}
```


JWT access token

SECURING API ENDPOINTS

AUTHENTICATION - ECG PREPAID APP



JWT structure

SECURING API ENDPOINTS

BROKEN AUTHENTICATION - AUDITING KNUST AIM

```
private static Retrofit.Builder getBuilder(String str) {
    return new Retrofit.Builder().baseUrl(str).addConverterFactory(GsonConverterFactory.create(gson));
}

public static <S> S createService(Class<S> cls) {
    return getBuilder().client(httpClient.build()).build().create(cls);
}

public static <S> S createServiceWithApiBaseUrl(Class<S> cls, String str) {
    return getBuilder(str).client(httpClient.build()).build().create(cls);
}

public static <S> S createService(Class<S> cls, final String str) {
    if (str != null) {
        httpClient.addInterceptor(new Interceptor() {
            public Response intercept(Chain chain) throws IOException {
                Request request = chain.request();
                StringBuilder sb = new StringBuilder();
                sb.append("Bearer ");
                sb.append(str);
                return chain.proceed(request.newBuilder().header("Authorization", sb.toString()).method(request.
            }
        });
    }
    return getBuilder().client(httpClient.build()).build().create(cls);
}
```

```
getAccessToken(@Field("grant_type") String str, @Field("username") String str2, @Field("password") String str3);
```

SECURING API ENDPOINTS

BROKEN AUTHENTICATION - AUDITING KNUST AIM

{"access_token":"uHYgmM184qnbcTdYIsBxCaDmsfGUVWaCBmhtj_Ipf9vMJK1Sav0hYiYFolvFNgm
cAlVedGJumHZo1U04Ye84ZJXOXKugOhIN1Add7se5qB6YPyxX7ESml8UjpBhUXQ_d041Ia-_v98SKYDP
FQswHyfRdivUG-FSxXNPeyyMWI75dVxtKjsXSiolUy8WKID-YxHdaE82PvBzP7iogmfYroz4GAh6JsVw
oi00AMlWp24Rg-mBsGyILX2oK43cxaTbXTwRSTaUoMIGRUZ6ib6-_fluxnBgV0GS-b4HxRGCIR3ZLgwr
a6RjRRmOCpEpHvLX4GgeejM8dlf04YGr6lyRfUHrdfD3sXHj4ZB7DfO2HzaTNPitv0d8bU8YVR_d5gk3
vjMsR7D-aerFTArLBJkjWJ5fQloXL_Z822G_j3yFHJU03IbH9Zx8fKDLdzwa9Q03iEvXm7OHwUAhVHMb
baDuDZKSXx3mdNRJLq7vgOfxm0lwdmK5v-1xbvS0f7U5LTdDAPJsuoSa8w-VsdRfmX0rliA","token_
type":"bearer","expires_in":7775999,"refresh_token":"8c8b8714-9062-4f52-811a-95f
62338f3e6","userName":"ojagyemang",".issued":"Sun, 14 Jul 2019 13:02:50 GMT",".e
xpires":"Sat, 12 Oct 2019 13:02:50 GMT"}

"Photo": "/9j/4AAQSkZJRgABAgAAAQABAAD
/2wCEABALDA4MChAODQ4SERATGCgaGBYWGDEjJR0oOjM9PDkzODdASFxOQERXRTc4UG1RV19iZ2hnPk1xeXBkeFxlZ2MBERISGBUYLxoaL2NC
OEJjY2NjY2NjY2NjY2NjY2NjY2NjY2NjY2NjY2NjY2NjY2NjY2NjY2NjY2NjY2NjY//AABEIAdMB4QMBIgACEQEDEQH
/xAGiAAABBQEBAQEBAQAAAAAAAAAAAQIDBAUGBwgJCgsQAAIBAwMCBAMFBQQEAAABfQECAwAEEQUSITFBBhNRYQcicRQygZGhCCNCscEVUtHw
JDNicoIJChYXGBkaJSYnKCkqNDU2Nzg5OkNERUZHSElKU1RVVldYWVpjZGVmZ2hpanN0dXZ3eHl6g4SFhoeIiYqSk5SVlpeYmZqio6Slpqeoq
aqys7S1tre4ubrCw8TFxsfIycrS09TV1tfY2drh4uPk5ebn6Onq8fLz9PX29/j5
+gEAAwEBAQEBAQEBAQAAAAAAAAECAwQFBgcICQoLEQACAQIEBAMEBwUEBAABAncAAQIDEQQFITEGEkFRB2FxEyIygQgUQpGhscEJIzNS8BVic
tEKFiQ04SXxFxgZGiYnKCkqNTY3ODk6Q0RFRkdISUpTVFVWV1hZWmNkZWZnaGlqc3R1dnd4eXqCg4SFhoeIiYqSk5SVlpeYmZqio6Slpqeoqa
qys7S1tre4ubrCw8TFxsfIycrS09TV1tfY2dri4+Tl5ufo6ery8/T19vf4+fr/2gAMAwEAAhEDEQA/AOmBIHrS55
/CkGcEUoHrW6Pn2KCKdTMClHQVQrCmg0nNL3oAB1pM88U7IzSdTRceiClpBxRSELRxiij60ytQopMYHFFArMWjHFJSjpSGBoxRmkz1piFpKWk
oEw70HpS0mRigaAUtKB6Vm6nrVnpkZMsgeTtEp5NIpRb0Ro0Y4zXH3njUklbW3ZMjgvzzzWHLruoys7NNgv1xwKXMjaOGnI9HluIYATLIqYGeT
VN9c0wKCb2LH1rzZ5ppGDPPI3HOWpnA4PrnFS59jZYLuz0OXxRpyfckD
/Q0P4m04dJASfQ9K874zwBS5HoOtLnZX1Ndz0pNf011yLqMY7E1agvba5KeVMrl
+VAPWvKwBycU5XkUho5XUr0w2MU1PuS8F2Z61yMZoBrzm18RalabAJVkRTnDck10Fl4xtpdy3ELxMBncTwapSTOeeGqRn70VXtLy3vYhbSK
6n0qxmmY7bi0lANJmgGwoxRS0xWEOf0pDnbjNO70nUUh7CDJxzRjnrlaNAHU9XSdcSkMc0BYWijFAFAwPSkJFKelI3UGgAzim5pTSY59
KBB1BpeDSHpxRjmgLAfamkDNOIowN2DQxbyKDnpSbuBjrRyTQIjWSfB5NYuteLQp8jTAGJHM
h5GPauPd2fJkJdj3bk1DnbY66WFcYc1G1qPifULsyLGwihzFQOGA

SECURING API ENDPOINTS

BROKEN AUTHENTICATION - AUDITING KNUST AIM


```
"UserName": "g
"StudentId": "
"IndexNo": "39
"Surname": "ZI
"OtherName": "
"FullName": "G            ara",
"Title": "Mr."
"Gender": "Mal
"BirthDate": "            00:00:00",
"Country": "Gh
"RegionId": 8,
"Region": "UPP
"SchoolEmail":            @st.knust.edu.gh",
"OtherPhone":             ",
"OtherEmail":             orge@gmail.com",
"PrimaryMobile": null,
"SchoolMobile": null,
"ResAdd": "AHANSOYEWO                    r",
"ResAdd1": "AHANSOYEW
"ResAdd2": "53C",
"ResAdd3": "OBUASI",
"ResAdd4": null,
"PostAdd": "KUKPIENG                     COMPANY OF G                    \nOBUASI\r",
"PostAdd1": "KUKPIENG
"PostAdd2": "ELECTRIC                    ,
"PostAdd3": "P.O.BOX
"PostAdd4": "OBUASI",
"PassportNo": null,
"ProgrammeStreamId":
"ProgrammeStream": "B                    ING",
```


[redacted]

COURSE CODE	COURSE NAME	CREDITS	MARKS	GRADE
PL 357	AGRICULTURAL AND INDUSTRIAL DEVT POLICY	3	63	B
PL 359	RESOURCE ASSESSMENT TECHNIQUES	3	52	C
PL 361	HOUSING POLICY PLANNING	3	45	D
PL 351	DISTRICT DEVELOPMENT PLANNING WORKSHOP I	6	36	F
PL 355	TRANSPORTATION PLANNING	3	76	A

Courses Trailing:

PL 351(F)

	Semester	Cumulative
Credits Registered:	18	18
Credits Obtained:	12	12
Credits Calc:	18	18
Weighted Marks:	924	924
Weighted Average:	51.33	51.33

Student's Signature

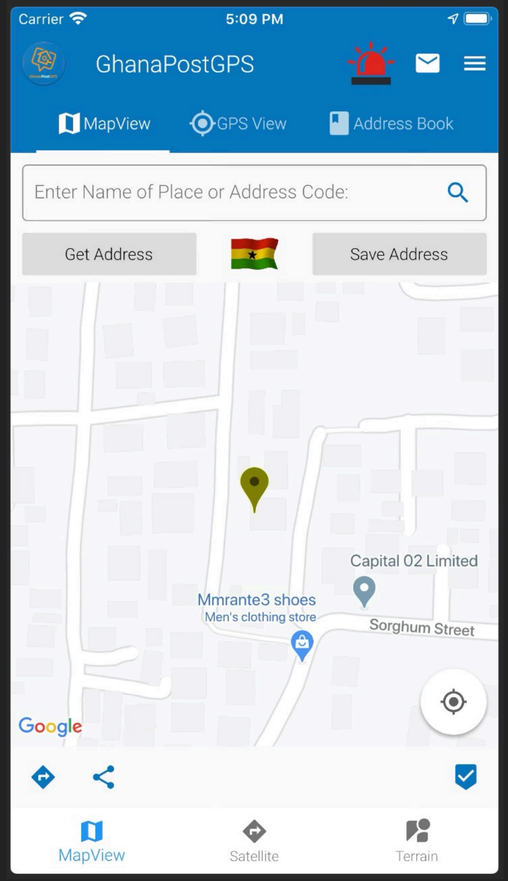
Academic Supervisor/Exams Officer's Signature

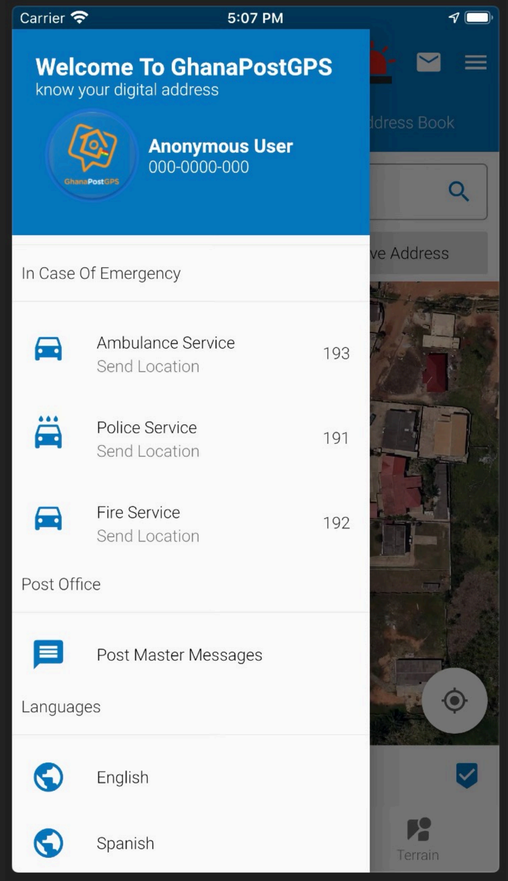
DEMO 2

GHANAPOST GPS APP

SECURING API ENDPOINTS

AUDITING GHANAPOST GPS APP

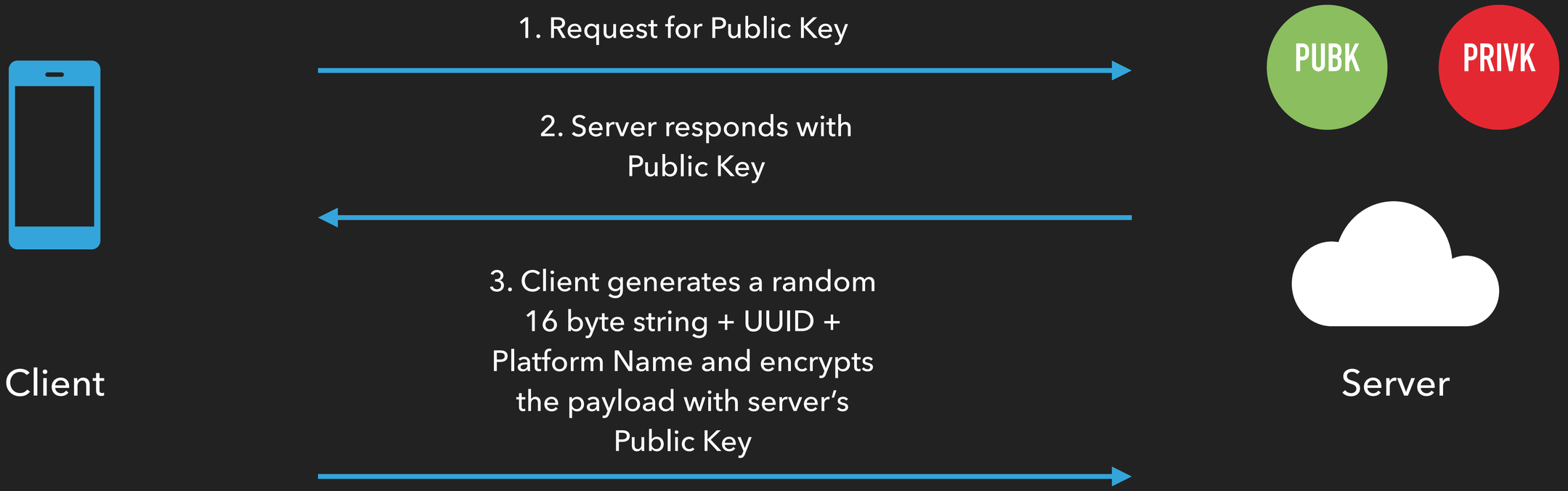




Client-Server uses asymmetric encryption

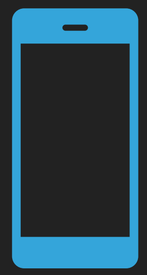
SECURING API ENDPOINTS

AUDITING GHANAPOST GPS APP

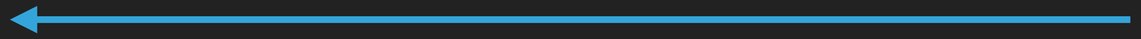


SECURING API ENDPOINTS

AUDITING GHANAPOST GPS APP

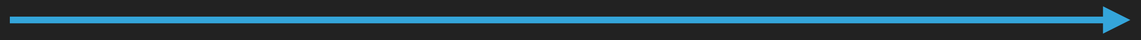


5. Server responds with encrypted API Endpoint URL



6. Client decrypts any subsequent payload with the generated 16 bytes string.

AES Encryption/Decryption (Symmetric Key)



Client

Server

SECURING API ENDPOINTS

AUDITING GHANAPOST GPS APP

Communication between the clients and the web service uses asymmetric encryption. When the application is launched for the first time, the mobile client connects to the endpoint https://api.ghanapostgps.com/GetAPIData.aspx to get the server's public key (a sample is shown below).

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAlO6O2gAGlT4+YP+evP9c
9qynWdv/qIAx5Jc4kp+UTmrsn8wJn4bD9H8rynSvepH0navZiDwYvioAPbIcR6cG
MMFnP5/2wN9zrBFZtnofcpSrk4q9/GRHj4IuHheQjvMiislrRdIEgqxjMQ1aaiG7
+MeoeQuHzO8O+aecHuMtJTXzcIQDqkMHkeA/yt/ge/ASDqSRn0Hdpa/4OA/ZtVpT
8Ph2lLgMv+O5Iz11UIwSqyewSdAZzX0H4jUPKCCfnhgWsS+7WJU6KufYptvl0/P4
NSdJKSdYg/y44pWiPxlgMUf6s1nOXJJ0vSi0zrDFjx+y+GD2h+dMBRWe9nym+NmJ
1QIDAQAB
-----END PUBLIC KEY-----
```

SECURING API ENDPOINTS

AUDITING GHANAPOST GPS APP

Upon getting the public key, the mobile client generates a random string (using the method below) of length 16 characters.

```
private static final String ALLOWED_CHARACTERS = "0123456789qwertyuiopasdfghjklzxcvbnm!@$#^&*()";
public static String getRandomString(int i) {
  Random random = new Random();
  StringBuilder sb = new StringBuilder(i);
  for (int i2 = 0; i2 < i; i2++) {
     sb.append(ALLOWED_CHARACTERS.charAt(random.nextInt(ALLOWED_CHARACTERS.length())));
  }
  return sb.toString();
}
```

SECURING API ENDPOINTS

AUDITING GHANAPOST GPS APP

The generated random string becomes a symmetric key that is used in the encryption and decryption of data between the client and the server. The client sends the generated random string (16 bytes) together with a universally unique identifier (UUID) and the operating system's name (Android or iOS) to the server. This data is encrypted (using RSA) and encoded in base64 using the server's public key before it is sent. A sample is shown below:

```
TiJ/O4d2rFzaR046lLMYBJ6yU3e+vqDjkrYNVrhFm9K+jLXbMzTB6xAdtz/f/Rx+Nyw5ZB64ok3v8MRJq9jf8NwpYeFQZUGROUzMmg
EgYR3MlAgFz7vRkQtOGGt/BwEaKO81PJKxnqVqqXjr3NqNbfJr3GDDkfIfVKT4xOZRZbcCFdPpDD6Ofb5RD7mL8LQLvwOPOUVq3+/
MlNDVhxOD4Osq0PqWh8CvrZY8y2Q1sDJYDTUsKFnOChxFNtJhso1ImtqLBkNFZbrWUXn6NbHV+p3HBJVeZNcJxlWPPHaBh8Ip7
qPOnnMww4ZXWC88/tWTlScFemwTcyGpT58T9rMySA==
```

SECURING API ENDPOINTS

AUDITING GHANAPOST GPS APP

The server responds by sending a base64 encoded data which can be decrypted using the client's symmetric key. The decrypted data is shown below.

```
PlsUseYourOwnKey||https://api.ghanapostgps.com/PublicGPGPSAPI.aspx
```

The decrypted data contained a new endpoint https://api.ghanapostgps.com/PublicGPGPSAPI.aspx through which all subsequent communications were made. The symmetric encryption used is advanced encryption standard (AES).

Made API Publicly available: https://jayluxferro.github.io/ghpgps/

SECURING API ENDPOINTS

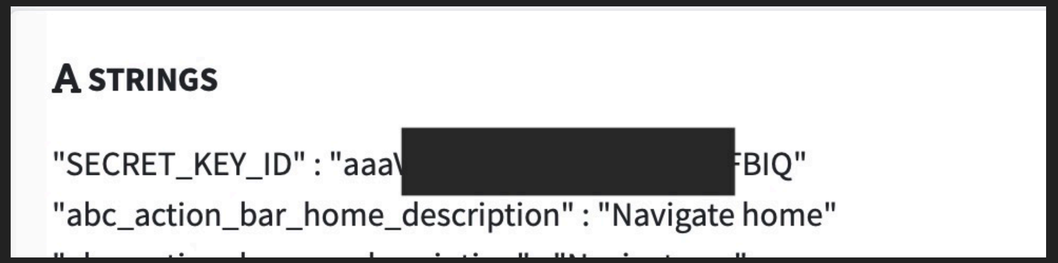
AES ENCRYPTION/DECRYPTION

```
public final class Aes {
    private static final String AES_MODE = "AES/CBC/PKCS7Padding";
    private static final String CHARSET = "UTF-8";
    private static boolean DEBUG_LOG_ENABLED = false;
    private static final String HASH_ALGORITHM = "SHA-256";
    private static final String TAG = "Aes";
    private static final byte[] ivBytes = {0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0};

    private Aes() {
    }

    private static String bytesToHex(byte[] bArr) {
        char[] cArr = {'0', '1', '2', '3', '4', '5', '6', '7', '8', '9', 'A', 'B', 'C', 'D', 'E', 'F'};
        char[] cArr2 = new char[(bArr.length * 2)];
        for (int i = 0; i < bArr.length; i++) {
            byte b = bArr[i] & 255;
            int i2 = i * 2;
            cArr2[i2] = cArr[b >>> 4];
            cArr2[i2 + 1] = cArr[b & 15];
        }
        return new String(cArr2);
    }

    public static String decrypt(String str, String str2) {
        try {
            SecretKeySpec generateKey = generateKey(str);
            log("base64EncodedCipherText", str2);
            byte[] decode = Base64.decode(str2, 2);
            log("decodedCipherText", decode);
            byte[] decrypt = decrypt(generateKey, ivBytes, decode);
            log("decryptedBytes", decrypt);
            String str3 = new String(decrypt, "UTF-8");
            log(SettingsJsonConstants.PROMPT_MESSAGE_KEY, str3);
            return str3;
        } catch (UnsupportedEncodingException e) {
            if (DEBUG_LOG_ENABLED) {
                Log.e(TAG, "UnsupportedEncodingException ", e);
            }
            throw new GeneralSecurityException(e);
        }
    }
```



Avoid re-use of same symmetric key

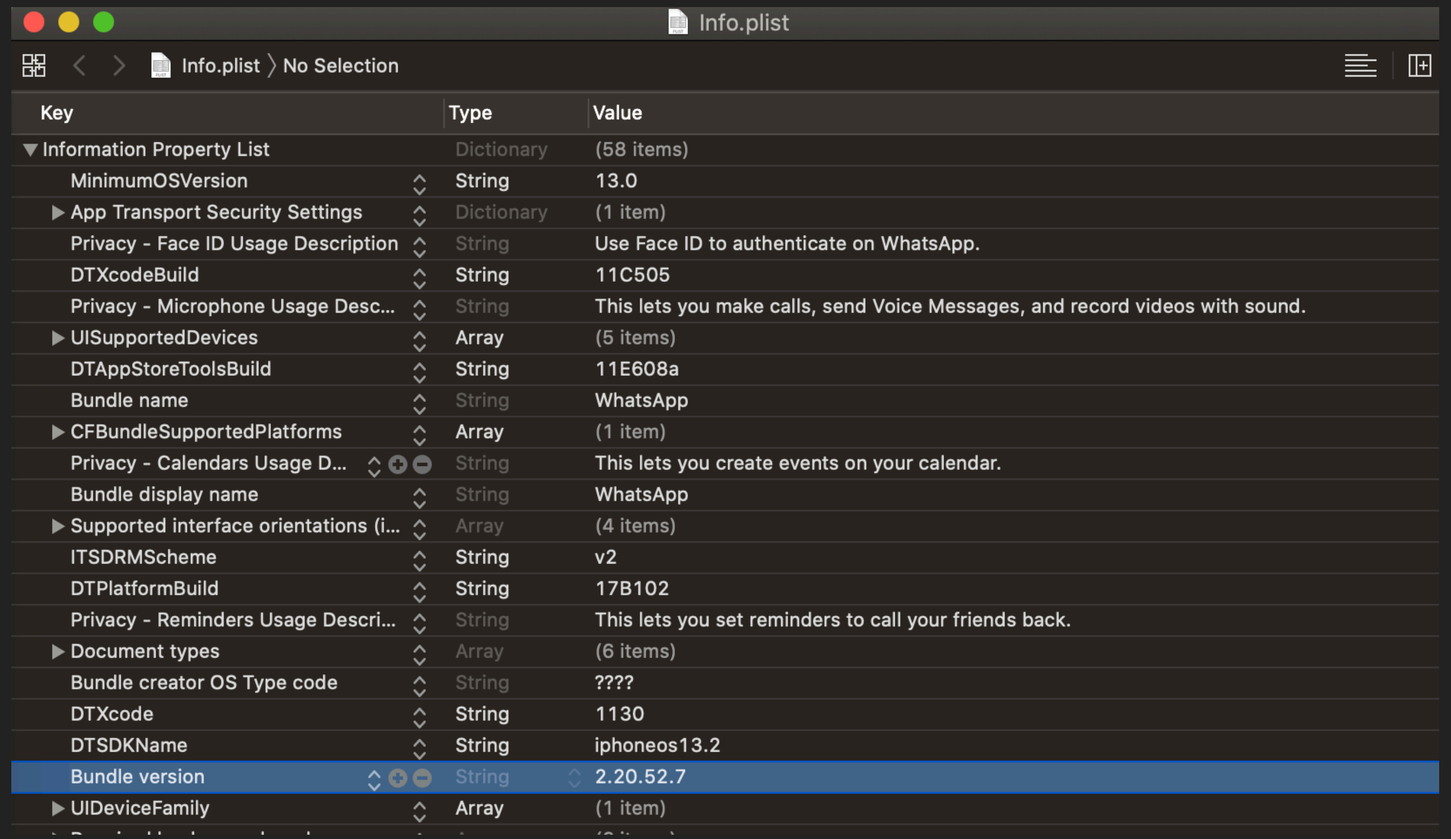
DEMO 3

WHATSAPP iOS App

SECURING API ENDPOINTS

AUDITING WHATSAPP IOS APP

The WhatsApp version used in this research was **2.20.52.7**. A brief content of the application's info.plist as shown below.



SECURING API ENDPOINTS

AUDITING WHATSAPP IOS APP

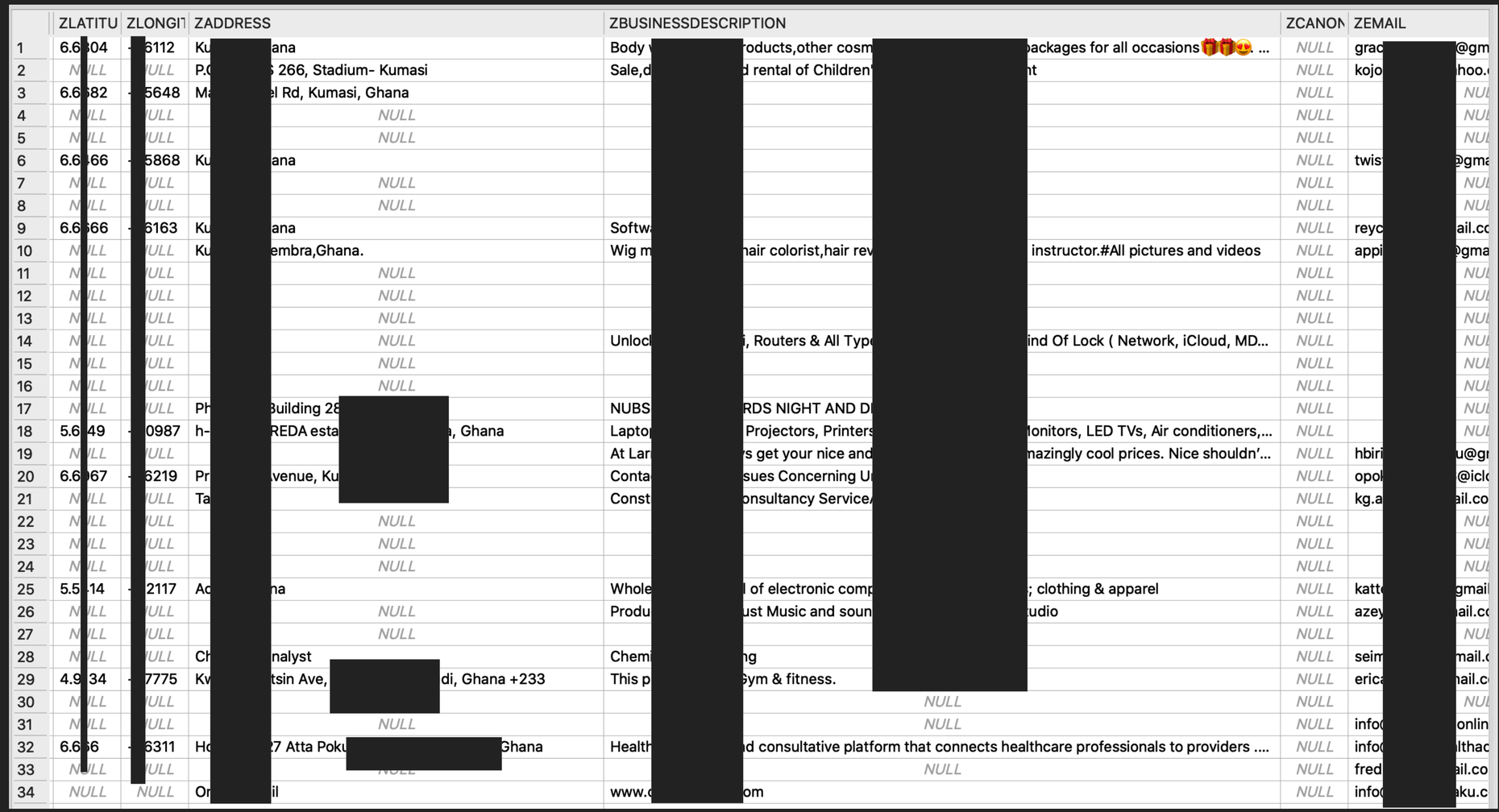
The content's of WhatsApp's application folder is shown below:

```
0x29a:~ root# cd /private/var/mobile/Containers/Shared/AppGroup/AAFA74A8-DD70-46BD-B175-F0F121446249/
0x29a:/private/var/mobile/Containers/Shared/AppGroup/AAFA74A8-DD70-46BD-B175-F0F121446249 root# ls
Axolotl.sqlite               ChatStorage.sqlite-wal    Logs/               connection.dlock
Axolotl.sqlite-shm           ContactsV2.sqlite         Logsv2/             connection_setup.dlock
Axolotl.sqlite-wal           ContactsV2.sqlite-shm     Media/              consumer_version
BackedUpKeyValue.sqlite      ContactsV2.sqlite-wal     Message/            current_wallpaper.jpg
BackedUpKeyValue.sqlite-shm  FieldStats2/              Outbox/             drestore.mark
BackedUpKeyValue.sqlite-wal  Library/                  Ranking.sqlite      emoji.sqlite
Biz/                         LocalKeyValue.sqlite      Ranking.sqlite-shm  fts/
CallHistory.sqlite           LocalKeyValue.sqlite-shm  Ranking.sqlite-wal  main_app.lock
CallHistory.sqlite-shm       LocalKeyValue.sqlite-wal  Sticker.sqlite      share_ext.lock
CallHistory.sqlite-wal       Location.sqlite           Sticker.sqlite-shm  status.blacklist
ChatStorage.sqlite           Location.sqlite-shm       Sticker.sqlite-wal  status.whitelist
ChatStorage.sqlite-shm       Location.sqlite-wal       cck.dat             stickers/
0x29a:/private/var/mobile/Containers/Shared/AppGroup/AAFA74A8-DD70-46BD-B175-F0F121446249 root#
```

SECURING API ENDPOINTS

AUDITING WHATSAPP IOS APP

The **Biz** folder contains an SQLite file; which stores the details of all WhatsApp Business clients that a user has in his/her contacts.

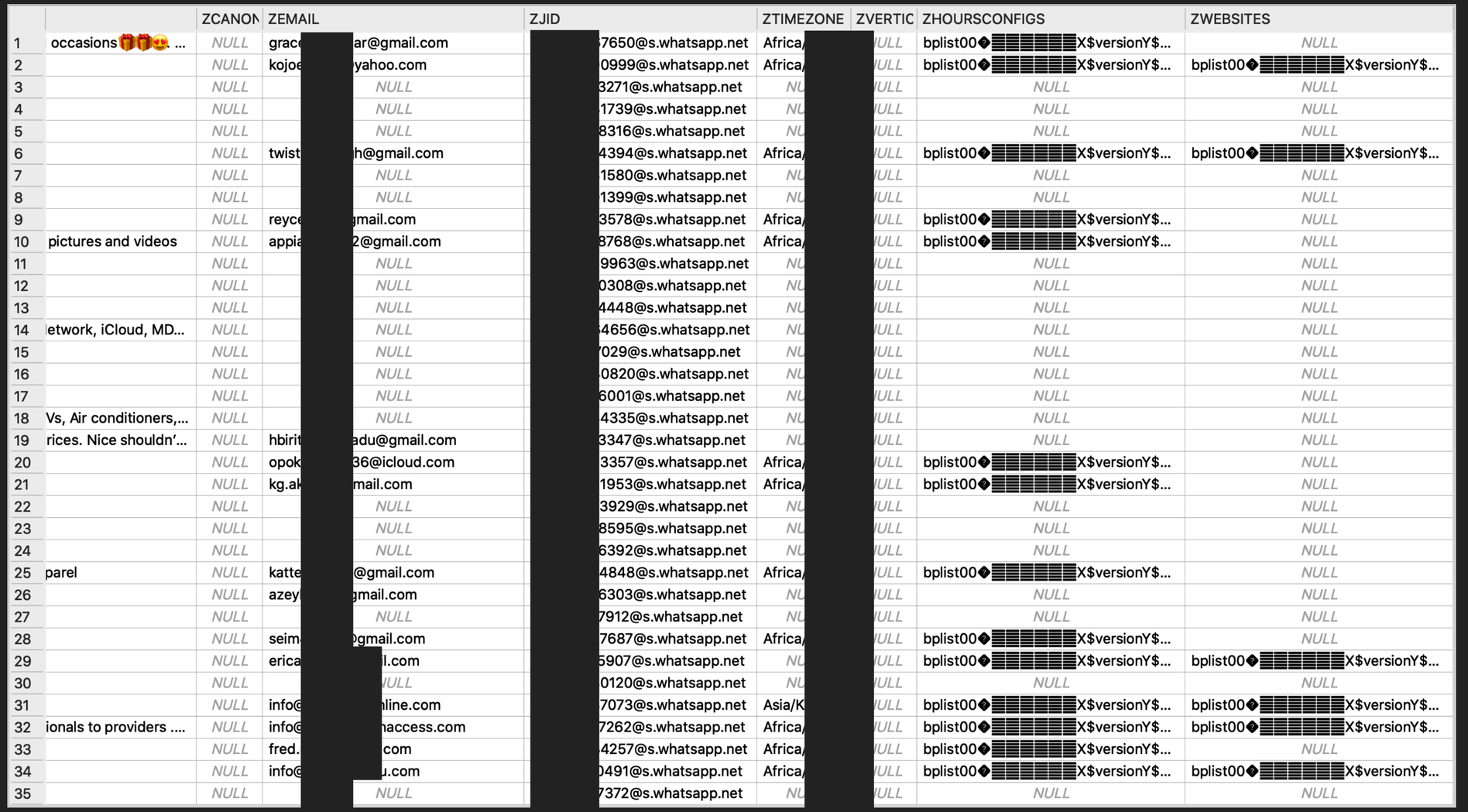


	ZLATITU	ZLONGI	ZADDRESS	ZBUSINESSDESCRIPTION	ZCANON	ZEMAIL
1	6.6	-1	Ku ana	Body products,other cosm packages for all occasions ...	NULL	grac @gm
2	NULL	NULL	P.O 266, Stadium- Kumasi	Sale,d d rental of Children' nt	NULL	kojo hoo.c
3	6.6	-1	Ma l Rd, Kumasi, Ghana		NULL	NUL
4	NULL	NULL	NULL		NULL	NUL
5	NULL	NULL	NULL		NULL	NUL
6	6.6	-1	Ku ana		NULL	twis @gma
7	NULL	NULL	NULL		NULL	NUL
8	NULL	NULL	NULL		NULL	NUL
9	6.6	-1	Ku ana	Softw	NULL	reyc ail.co
10	NULL	NULL	Ku embra,Ghana.	Wig m hair colorist,hair rev instructor.#All pictures and videos	NULL	appi @gma
11	NULL	NULL	NULL		NULL	NUL
12	NULL	NULL	NULL		NULL	NUL
13	NULL	NULL	NULL		NULL	NUL
14	NULL	NULL	NULL	Unloc , Routers & All Type ind Of Lock (Network, iCloud, MD...	NULL	NUL
15	NULL	NULL	NULL		NULL	NUL
16	NULL	NULL	NULL		NULL	NUL
17	NULL	NULL	Ph Building 28	NUBS RDS NIGHT AND D	NULL	NUL
18	5.6	-0	h- REDA esta , Ghana	Lapto Projectors, Printers Monitors, LED TVs, Air conditioners,...	NULL	NUL
19	NULL	NULL		At Lar 's get your nice and mazingly cool prices. Nice shouldn'...	NULL	hbiri u@gr
20	6.6	-1	Pr venue, Ku	Conta sues Concerning U	NULL	opol @icl
21	NULL	NULL	Ta	Const onsultancy Service/	NULL	kg.a ail.co
22	NULL	NULL	NULL		NULL	NUL
23	NULL	NULL	NULL		NULL	NUL
24	NULL	NULL	NULL		NULL	NUL
25	5.5	-2	Ac na	Whole l of electronic comp ; clothing & apparel	NULL	katt gmail
26	NULL	NULL	NULL	Produ ust Music and soun udio	NULL	azey ail.co
27	NULL	NULL	NULL		NULL	NUL
28	NULL	NULL	Ch nalyst	Chemi ng	NULL	seim mail.c
29	4.9	-7	Kv tsin Ave, di, Ghana +233	This p Gym & fitness.	NULL	erica ail.c
30	NULL	NULL		NULL	NULL	NUL
31	NULL	NULL	NULL	NULL	NULL	info onlin
32	6.6	-1	Ho 7 Atta Poku Ghana	Health d consultative platform that connects healthcare professionals to providers	NULL	info lthac
33	NULL	NULL	NULL	NULL	NULL	fred ail.co
34	NULL	NULL	Or il	www.c om	NULL	info aku.c

SECURING API ENDPOINTS

AUDITING WHATSAPP IOS APP

The **Biz** folder contains an SQLite file; which stores the details of all WhatsApp Business clients that a user has in his/her contacts.

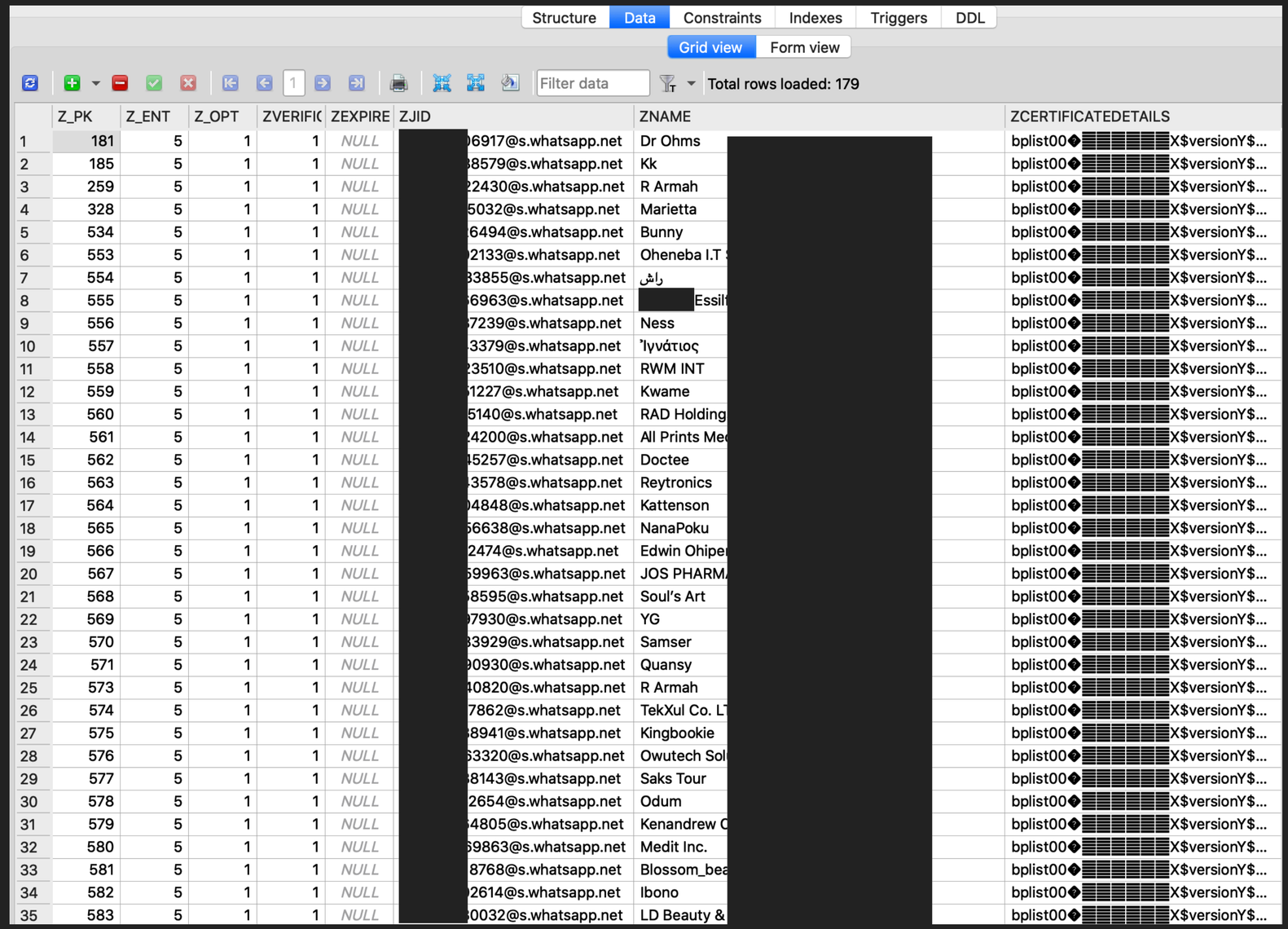


		ZCANON	ZEMAIL	ZJID	ZTIMEZONE	ZVERTIC	ZHOURSCONFIGS	ZWEBSITES
1	occasions🎁🎁😍. ...	NULL	grace[redacted]ar@gmail.com	[redacted]7650@s.whatsapp.net	Africa/[redacted]	NULL	bplist00[redacted]X$versionY$...	NULL
2		NULL	kojoe[redacted]yahoo.com	[redacted]0999@s.whatsapp.net	Africa/[redacted]	NULL	bplist00[redacted]X$versionY$...	bplist00[redacted]X$versionY$...
3		NULL	NULL	[redacted]3271@s.whatsapp.net	NU[redacted]	NULL	NULL	NULL
4		NULL	NULL	[redacted]1739@s.whatsapp.net	NU[redacted]	NULL	NULL	NULL
5		NULL	NULL	[redacted]8316@s.whatsapp.net	NU[redacted]	NULL	NULL	NULL
6		NULL	twist[redacted]h@gmail.com	[redacted]4394@s.whatsapp.net	Africa/[redacted]	NULL	bplist00[redacted]X$versionY$...	bplist00[redacted]X$versionY$...
7		NULL	NULL	[redacted]1580@s.whatsapp.net	NU[redacted]	NULL	NULL	NULL
8		NULL	NULL	[redacted]1399@s.whatsapp.net	NU[redacted]	NULL	NULL	NULL
9		NULL	reyce[redacted]gmail.com	[redacted]3578@s.whatsapp.net	Africa/[redacted]	NULL	bplist00[redacted]X$versionY$...	NULL
10	pictures and videos	NULL	appia[redacted]2@gmail.com	[redacted]8768@s.whatsapp.net	Africa/[redacted]	NULL	bplist00[redacted]X$versionY$...	NULL
11		NULL	NULL	[redacted]9963@s.whatsapp.net	NU[redacted]	NULL	NULL	NULL
12		NULL	NULL	[redacted]0308@s.whatsapp.net	NU[redacted]	NULL	NULL	NULL
13		NULL	NULL	[redacted]4448@s.whatsapp.net	NU[redacted]	NULL	NULL	NULL
14	letwork, iCloud, MD...	NULL	NULL	[redacted]4656@s.whatsapp.net	NU[redacted]	NULL	NULL	NULL
15		NULL	NULL	[redacted]7029@s.whatsapp.net	NU[redacted]	NULL	NULL	NULL
16		NULL	NULL	[redacted]0820@s.whatsapp.net	NU[redacted]	NULL	NULL	NULL
17		NULL	NULL	[redacted]6001@s.whatsapp.net	NU[redacted]	NULL	NULL	NULL
18	Vs, Air conditioners,...	NULL	NULL	[redacted]4335@s.whatsapp.net	NU[redacted]	NULL	NULL	NULL
19	rices. Nice shouldn'...	NULL	hbirit[redacted]adu@gmail.com	[redacted]3347@s.whatsapp.net	NU[redacted]	NULL	NULL	NULL
20		NULL	opok[redacted]36@icloud.com	[redacted]3357@s.whatsapp.net	Africa/[redacted]	NULL	bplist00[redacted]X$versionY$...	NULL
21		NULL	kg.ak[redacted]mail.com	[redacted]1953@s.whatsapp.net	Africa/[redacted]	NULL	bplist00[redacted]X$versionY$...	NULL
22		NULL	NULL	[redacted]3929@s.whatsapp.net	NU[redacted]	NULL	NULL	NULL
23		NULL	NULL	[redacted]8595@s.whatsapp.net	NU[redacted]	NULL	NULL	NULL
24		NULL	NULL	[redacted]6392@s.whatsapp.net	NU[redacted]	NULL	NULL	NULL
25	parel	NULL	katte[redacted]@gmail.com	[redacted]4848@s.whatsapp.net	Africa/[redacted]	NULL	bplist00[redacted]X$versionY$...	NULL
26		NULL	azey[redacted]gmail.com	[redacted]6303@s.whatsapp.net	NU[redacted]	NULL	NULL	NULL
27		NULL	NULL	[redacted]7912@s.whatsapp.net	NU[redacted]	NULL	NULL	NULL
28		NULL	seim[redacted]@gmail.com	[redacted]7687@s.whatsapp.net	Africa/[redacted]	NULL	bplist00[redacted]X$versionY$...	NULL
29		NULL	erica[redacted]l.com	[redacted]5907@s.whatsapp.net	NU[redacted]	NULL	bplist00[redacted]X$versionY$...	bplist00[redacted]X$versionY$...
30		NULL	[redacted]NULL	[redacted]0120@s.whatsapp.net	NU[redacted]	NULL	NULL	NULL
31		NULL	info@[redacted]nline.com	[redacted]7073@s.whatsapp.net	Asia/K[redacted]	NULL	bplist00[redacted]X$versionY$...	bplist00[redacted]X$versionY$...
32	ionals to providers	NULL	info@[redacted]naccess.com	[redacted]7262@s.whatsapp.net	Africa/[redacted]	NULL	bplist00[redacted]X$versionY$...	bplist00[redacted]X$versionY$...
33		NULL	fred.[redacted].com	[redacted]4257@s.whatsapp.net	Africa/[redacted]	NULL	bplist00[redacted]X$versionY$...	NULL
34		NULL	info@[redacted]u.com	[redacted]0491@s.whatsapp.net	Africa/[redacted]	NULL	bplist00[redacted]X$versionY$...	bplist00[redacted]X$versionY$...
35		NULL	NULL	[redacted]7372@s.whatsapp.net	NU[redacted]	NULL	NULL	NULL

SECURING API ENDPOINTS

AUDITING WHATSAPP IOS APP

The **Biz** folder contains an SQLite file; which stores the details of all WhatsApp Business clients that a user has in his/her contacts.

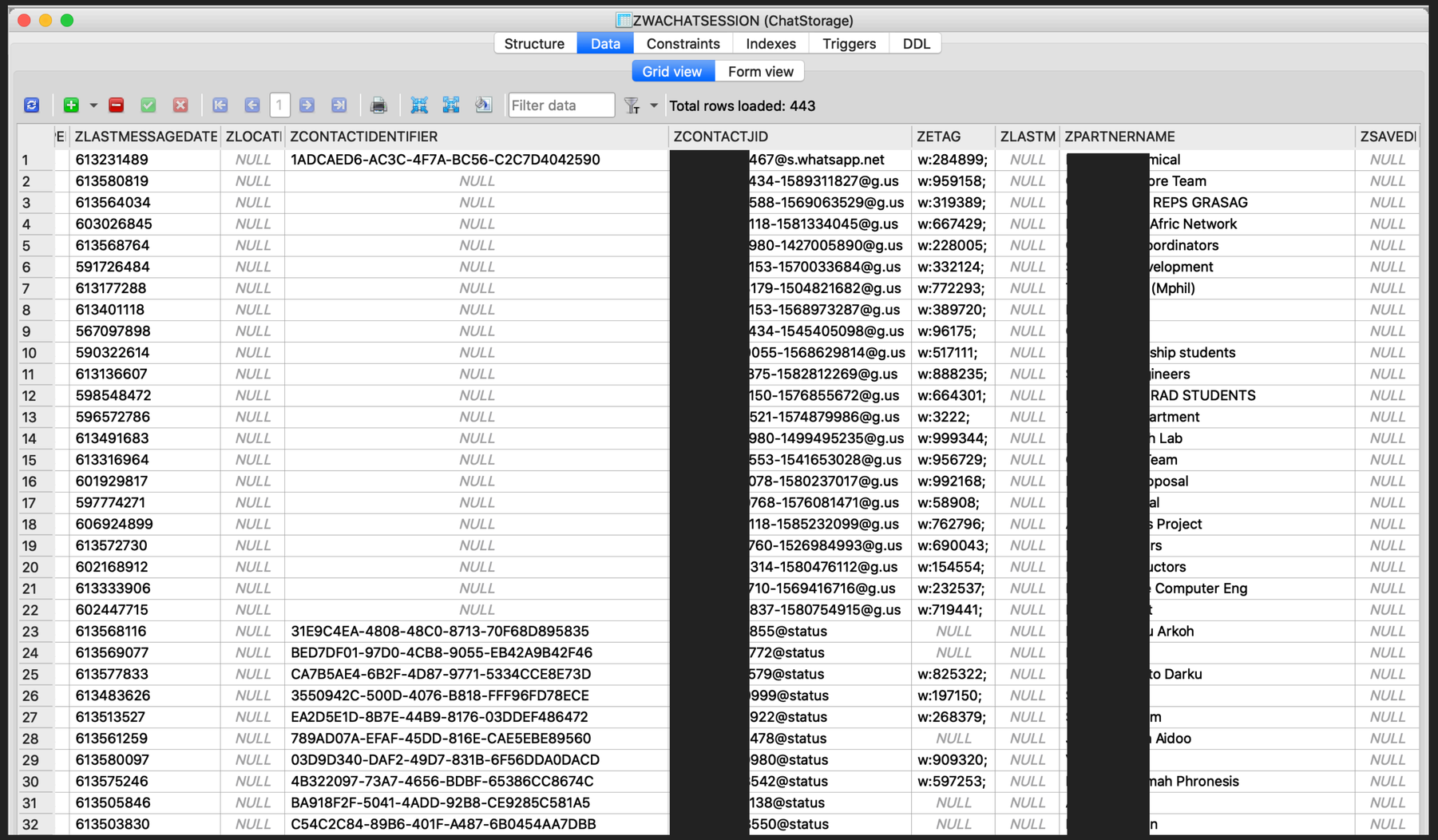


	Z_PK	Z_ENT	Z_OPT	ZVERIFIC	ZEXPIRE	ZJID	ZNAME	ZCERTIFICATEDETAILS
1	181	5	1	1	NULL	[redacted]	Dr Ohms	bplist00[redacted]X$versionY$...
2	185	5	1	1	NULL	[redacted]	Kk	bplist00[redacted]X$versionY$...
3	259	5	1	1	NULL	[redacted]	R Armah	bplist00[redacted]X$versionY$...
4	328	5	1	1	NULL	[redacted]	Marietta	bplist00[redacted]X$versionY$...
5	534	5	1	1	NULL	[redacted]	Bunny	bplist00[redacted]X$versionY$...
6	553	5	1	1	NULL	[redacted]	Oheneba I.T	bplist00[redacted]X$versionY$...
7	554	5	1	1	NULL	[redacted]	راش	bplist00[redacted]X$versionY$...
8	555	5	1	1	NULL	[redacted]	[redacted]Essil	bplist00[redacted]X$versionY$...
9	556	5	1	1	NULL	[redacted]	Ness	bplist00[redacted]X$versionY$...
10	557	5	1	1	NULL	[redacted]	Ἰγνάτιος	bplist00[redacted]X$versionY$...
11	558	5	1	1	NULL	[redacted]	RWM INT	bplist00[redacted]X$versionY$...
12	559	5	1	1	NULL	[redacted]	Kwame	bplist00[redacted]X$versionY$...
13	560	5	1	1	NULL	[redacted]	RAD Holding	bplist00[redacted]X$versionY$...
14	561	5	1	1	NULL	[redacted]	All Prints Me	bplist00[redacted]X$versionY$...
15	562	5	1	1	NULL	[redacted]	Doctee	bplist00[redacted]X$versionY$...
16	563	5	1	1	NULL	[redacted]	Reytronics	bplist00[redacted]X$versionY$...
17	564	5	1	1	NULL	[redacted]	Kattenson	bplist00[redacted]X$versionY$...
18	565	5	1	1	NULL	[redacted]	NanaPoku	bplist00[redacted]X$versionY$...
19	566	5	1	1	NULL	[redacted]	Edwin Ohipe	bplist00[redacted]X$versionY$...
20	567	5	1	1	NULL	[redacted]	JOS PHARM	bplist00[redacted]X$versionY$...
21	568	5	1	1	NULL	[redacted]	Soul's Art	bplist00[redacted]X$versionY$...
22	569	5	1	1	NULL	[redacted]	YG	bplist00[redacted]X$versionY$...
23	570	5	1	1	NULL	[redacted]	Samser	bplist00[redacted]X$versionY$...
24	571	5	1	1	NULL	[redacted]	Quansy	bplist00[redacted]X$versionY$...
25	573	5	1	1	NULL	[redacted]	R Armah	bplist00[redacted]X$versionY$...
26	574	5	1	1	NULL	[redacted]	TekXul Co. L	bplist00[redacted]X$versionY$...
27	575	5	1	1	NULL	[redacted]	Kingbookie	bplist00[redacted]X$versionY$...
28	576	5	1	1	NULL	[redacted]	Owutech Sol	bplist00[redacted]X$versionY$...
29	577	5	1	1	NULL	[redacted]	Saks Tour	bplist00[redacted]X$versionY$...
30	578	5	1	1	NULL	[redacted]	Odum	bplist00[redacted]X$versionY$...
31	579	5	1	1	NULL	[redacted]	Kenandrew C	bplist00[redacted]X$versionY$...
32	580	5	1	1	NULL	[redacted]	Medit Inc.	bplist00[redacted]X$versionY$...
33	581	5	1	1	NULL	[redacted]	Blossom_bea	bplist00[redacted]X$versionY$...
34	582	5	1	1	NULL	[redacted]	Ibono	bplist00[redacted]X$versionY$...
35	583	5	1	1	NULL	[redacted]	LD Beauty &	bplist00[redacted]X$versionY$...

SECURING API ENDPOINTS

AUDITING WHATSAPP IOS APP

Chat messages are stored in **CallHistory.sqlite**. This SQLite file stores names of groups a user belongs to, messages sent to and received in the group, messages sent/received from other users and links to encrypted images and videos sent/received.

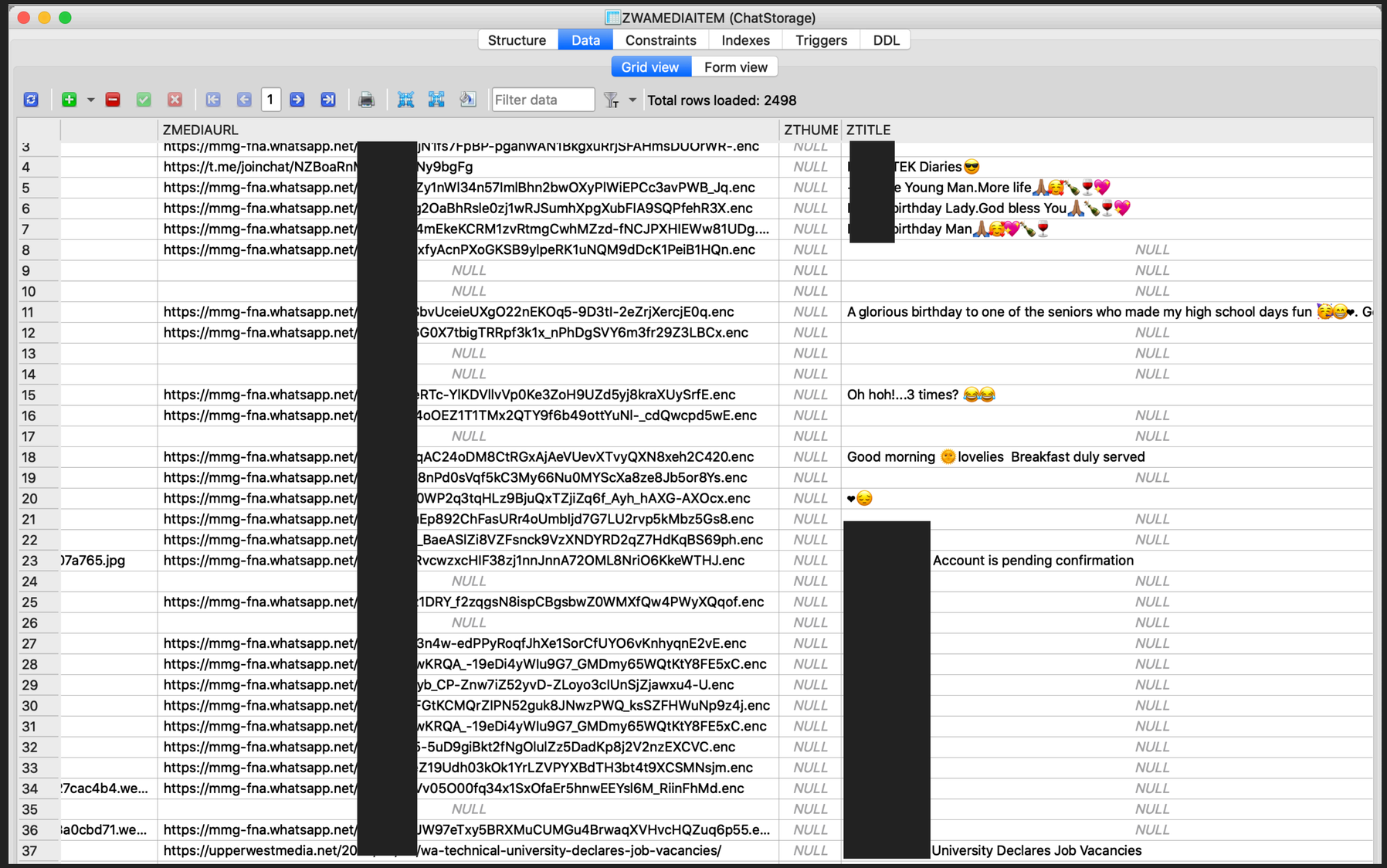


	E	ZLASTMESSAGEDATE	ZLOCATI	ZCONTACTIDENTIFIER	ZCONTACTJID	ZETAG	ZLASTM	ZPARTNERNAME	ZSAVEDI
1		613231489	NULL	1ADCAED6-AC3C-4F7A-BC56-C2C7D4042590	[redacted]467@s.whatsapp.net	w:284899;	NULL	[redacted]mical	NULL
2		613580819	NULL	NULL	[redacted]434-1589311827@g.us	w:959158;	NULL	[redacted]ore Team	NULL
3		613564034	NULL	NULL	[redacted]588-1569063529@g.us	w:319389;	NULL	[redacted] REPS GRASAG	NULL
4		603026845	NULL	NULL	[redacted]118-1581334045@g.us	w:667429;	NULL	[redacted]Afric Network	NULL
5		613568764	NULL	NULL	[redacted]980-1427005890@g.us	w:228005;	NULL	[redacted]ordinators	NULL
6		591726484	NULL	NULL	[redacted]153-1570033684@g.us	w:332124;	NULL	[redacted]velopment	NULL
7		613177288	NULL	NULL	[redacted]179-1504821682@g.us	w:772293;	NULL	[redacted] (Mphil)	NULL
8		613401118	NULL	NULL	[redacted]153-1568973287@g.us	w:389720;	NULL	[redacted]	NULL
9		567097898	NULL	NULL	[redacted]434-1545405098@g.us	w:96175;	NULL	[redacted]	NULL
10		590322614	NULL	NULL	[redacted]055-1568629814@g.us	w:517111;	NULL	[redacted]ship students	NULL
11		613136607	NULL	NULL	[redacted]375-1582812269@g.us	w:888235;	NULL	[redacted]ineers	NULL
12		598548472	NULL	NULL	[redacted]150-1576855672@g.us	w:664301;	NULL	[redacted]RAD STUDENTS	NULL
13		596572786	NULL	NULL	[redacted]521-1574879986@g.us	w:3222;	NULL	[redacted]artment	NULL
14		613491683	NULL	NULL	[redacted]980-1499495235@g.us	w:999344;	NULL	[redacted]n Lab	NULL
15		613316964	NULL	NULL	[redacted]553-1541653028@g.us	w:956729;	NULL	[redacted]eam	NULL
16		601929817	NULL	NULL	[redacted]078-1580237017@g.us	w:992168;	NULL	[redacted]oposal	NULL
17		597774271	NULL	NULL	[redacted]768-1576081471@g.us	w:58908;	NULL	[redacted]al	NULL
18		606924899	NULL	NULL	[redacted]118-1585232099@g.us	w:762796;	NULL	[redacted]s Project	NULL
19		613572730	NULL	NULL	[redacted]760-1526984993@g.us	w:690043;	NULL	[redacted]rs	NULL
20		602168912	NULL	NULL	[redacted]314-1580476112@g.us	w:154554;	NULL	[redacted]uctors	NULL
21		613333906	NULL	NULL	[redacted]710-1569416716@g.us	w:232537;	NULL	[redacted]e Computer Eng	NULL
22		602447715	NULL	NULL	[redacted]837-1580754915@g.us	w:719441;	NULL	[redacted]t	NULL
23		613568116	NULL	31E9C4EA-4808-48C0-8713-70F68D895835	[redacted]855@status	NULL	NULL	[redacted]u Arkoh	NULL
24		613569077	NULL	BED7DF01-97D0-4CB8-9055-EB42A9B42F46	[redacted]772@status	NULL	NULL	[redacted]	NULL
25		613577833	NULL	CA7B5AE4-6B2F-4D87-9771-5334CCE8E73D	[redacted]579@status	w:825322;	NULL	[redacted]to Darku	NULL
26		613483626	NULL	3550942C-500D-4076-B818-FFF96FD78ECE	[redacted]999@status	w:197150;	NULL	[redacted]	NULL
27		613513527	NULL	EA2D5E1D-8B7E-44B9-8176-03DDEF486472	[redacted]922@status	w:268379;	NULL	[redacted]m	NULL
28		613561259	NULL	789AD07A-EFAF-45DD-816E-CAE5EBE89560	[redacted]478@status	NULL	NULL	[redacted] Aidoo	NULL
29		613580097	NULL	03D9D340-DAF2-49D7-831B-6F56DDA0DACD	[redacted]980@status	w:909320;	NULL	[redacted]	NULL
30		613575246	NULL	4B322097-73A7-4656-BDBF-65386CC8674C	[redacted]542@status	w:597253;	NULL	[redacted]mah Phronesis	NULL
31		613505846	NULL	BA918F2F-5041-4ADD-92B8-CE9285C581A5	[redacted]138@status	NULL	NULL	[redacted]	NULL
32		613503830	NULL	C54C2C84-89B6-401F-A487-6B0454AA7DBB	[redacted]550@status	NULL	NULL	[redacted]n	NULL

SECURING API ENDPOINTS

AUDITING WHATSAPP IOS APP

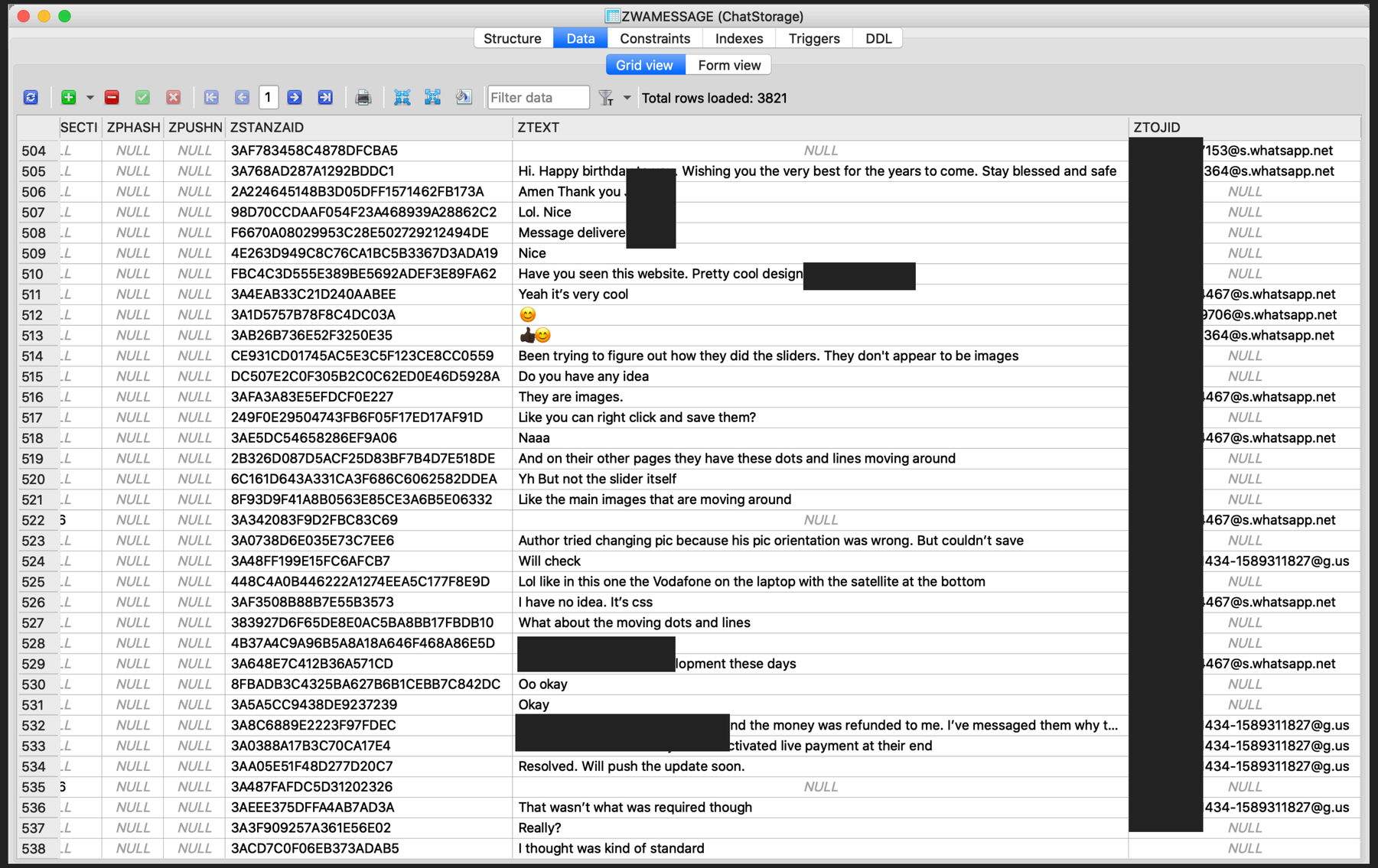
Chat messages are stored in **CallHistory.sqlite**. This SQLite file stores names of groups a user belongs to, messages sent to and received in the group, messages sent/received from other users and links to encrypted images and videos sent/received.



SECURING API ENDPOINTS

AUDITING WHATSAPP IOS APP

Chat messages are stored in **CallHistory.sqlite**. This SQLite file stores names of groups a user belongs to, messages sent to and received in the group, messages sent/received from other users and links to encrypted images and videos sent/received.

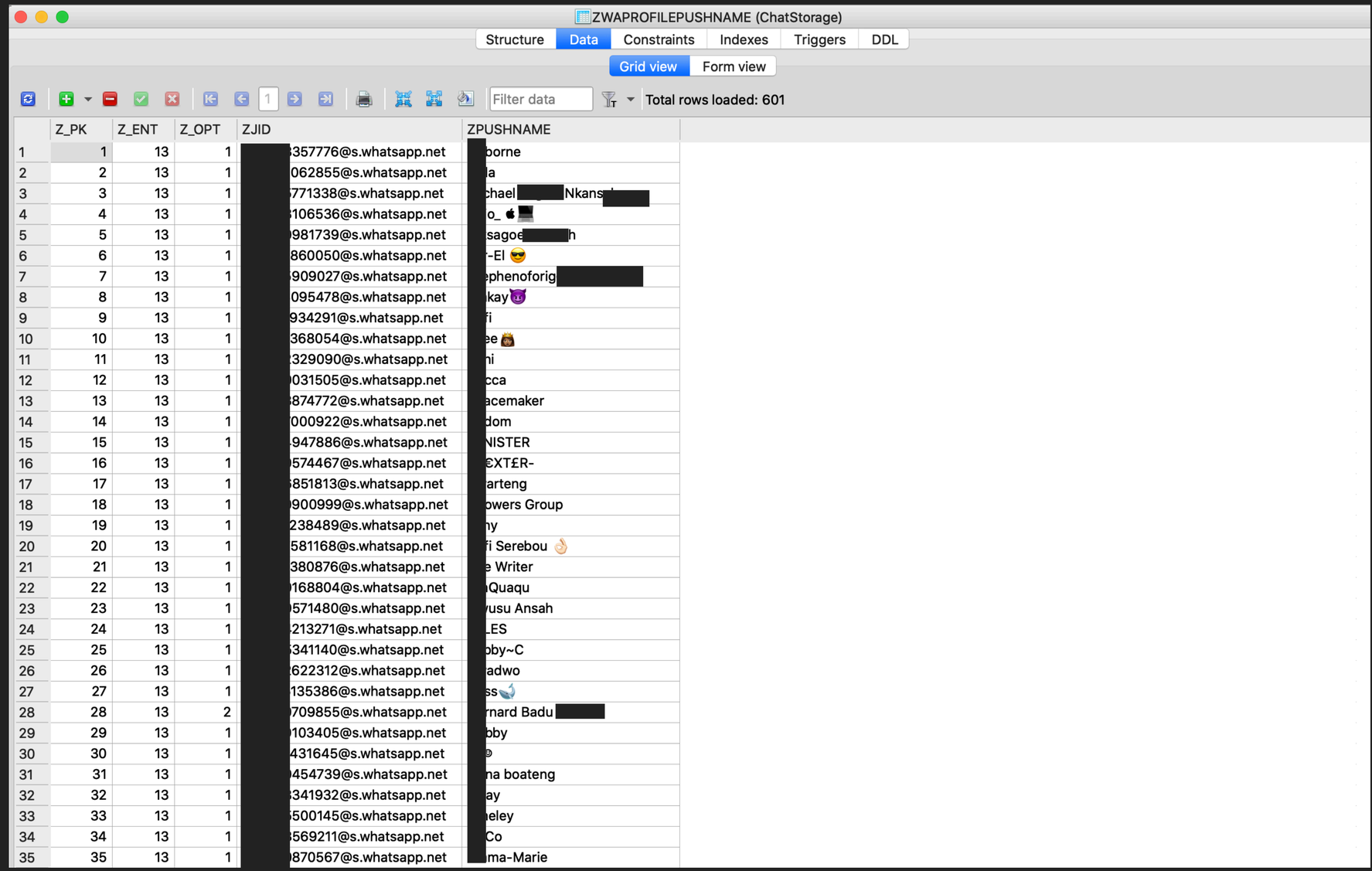


	SECTI	ZPHASH	ZPUSHN	ZSTANZAID	ZTEXT	ZTOJID
504	.L	NULL	NULL	3AF783458C4878DFCBA5	NULL	[redacted]153@s.whatsapp.net
505	.L	NULL	NULL	3A768AD287A1292BDDC1	Hi. Happy birthda[redacted]. Wishing you the very best for the years to come. Stay blessed and safe	[redacted]364@s.whatsapp.net
506	.L	NULL	NULL	2A224645148B3D05DFF1571462FB173A	Amen Thank you [redacted]	NULL
507	.L	NULL	NULL	98D70CCDAAF054F23A468939A28862C2	Lol. Nice	NULL
508	.L	NULL	NULL	F6670A08029953C28E502729212494DE	Message delivere[redacted]	NULL
509	.L	NULL	NULL	4E263D949C8C76CA1BC5B3367D3ADA19	Nice	NULL
510	.L	NULL	NULL	FBC4C3D555E389BE5692ADEF3E89FA62	Have you seen this website. Pretty cool design[redacted]	NULL
511	.L	NULL	NULL	3A4EAB33C21D240AABEE	Yeah it's very cool	[redacted]1467@s.whatsapp.net
512	.L	NULL	NULL	3A1D5757B78F8C4DC03A	😊	[redacted]9706@s.whatsapp.net
513	.L	NULL	NULL	3AB26B736E52F3250E35	👍😊	[redacted]364@s.whatsapp.net
514	.L	NULL	NULL	CE931CD01745AC5E3C5F123CE8CC0559	Been trying to figure out how they did the sliders. They don't appear to be images	NULL
515	.L	NULL	NULL	DC507E2C0F305B2C0C62ED0E46D5928A	Do you have any idea	NULL
516	.L	NULL	NULL	3AFA3A83E5EFDCF0E227	They are images.	[redacted]1467@s.whatsapp.net
517	.L	NULL	NULL	249F0E29504743FB6F05F17ED17AF91D	Like you can right click and save them?	NULL
518	.L	NULL	NULL	3AE5DC54658286EF9A06	Naaa	[redacted]1467@s.whatsapp.net
519	.L	NULL	NULL	2B326D087D5ACF25D83BF7B4D7E518DE	And on their other pages they have these dots and lines moving around	NULL
520	.L	NULL	NULL	6C161D643A331CA3F686C6062582DDEA	Yh But not the slider itself	NULL
521	.L	NULL	NULL	8F93D9F41A8B0563E85CE3A6B5E06332	Like the main images that are moving around	NULL
522	5	NULL	NULL	3A342083F9D2FBC83C69	NULL	[redacted]1467@s.whatsapp.net
523	.L	NULL	NULL	3A0738D6E035E73C7EE6	Author tried changing pic because his pic orientation was wrong. But couldn't save	NULL
524	.L	NULL	NULL	3A48FF199E15FC6AFCB7	Will check	[redacted]434-1589311827@g.us
525	.L	NULL	NULL	448C4A0B446222A1274EEA5C177F8E9D	Lol like in this one the Vodafone on the laptop with the satellite at the bottom	NULL
526	.L	NULL	NULL	3AF3508B88B7E55B3573	I have no idea. It's css	[redacted]1467@s.whatsapp.net
527	.L	NULL	NULL	383927D6F65DE8E0AC5BA8BB17FBDB10	What about the moving dots and lines	NULL
528	.L	NULL	NULL	4B37A4C9A96B5A8A18A646F468A86E5D	[redacted]	NULL
529	.L	NULL	NULL	3A648E7C412B36A571CD	[redacted]lopment these days	[redacted]1467@s.whatsapp.net
530	.L	NULL	NULL	8FBADB3C4325BA627B6B1CEBB7C842DC	Oo okay	NULL
531	.L	NULL	NULL	3A5A5CC9438DE9237239	Okay	NULL
532	.L	NULL	NULL	3A8C6889E2223F97FDEC	[redacted]nd the money was refunded to me. I've messaged them why t...	[redacted]434-1589311827@g.us
533	.L	NULL	NULL	3A0388A17B3C70CA17E4	[redacted]ctivated live payment at their end	[redacted]434-1589311827@g.us
534	.L	NULL	NULL	3AA05E51F48D277D20C7	Resolved. Will push the update soon.	[redacted]434-1589311827@g.us
535	5	NULL	NULL	3A487FAFDC5D31202326	NULL	NULL
536	.L	NULL	NULL	3AEEE375DFFA4AB7AD3A	That wasn't what was required though	[redacted]434-1589311827@g.us
537	.L	NULL	NULL	3A3F909257A361E56E02	Really?	NULL
538	.L	NULL	NULL	3ACD7C0F06EB373ADAB5	I thought was kind of standard	NULL

SECURING API ENDPOINTS

AUDITING WHATSAPP IOS APP

Chat messages are stored in **CallHistory.sqlite**. This SQLite file stores names of groups a user belongs to, messages sent to and received in the group, messages sent/received from other users and links to encrypted images and videos sent/received.



	Z_PK	Z_ENT	Z_OPT	ZJID	ZPUSHNAME
1	1	13	1	[redacted]357776@s.whatsapp.net	[redacted]borne
2	2	13	1	[redacted]062855@s.whatsapp.net	[redacted]la
3	3	13	1	[redacted]771338@s.whatsapp.net	[redacted]chael [redacted]Nkans[redacted]
4	4	13	1	[redacted]106536@s.whatsapp.net	[redacted]o_ 🍎💻
5	5	13	1	[redacted]981739@s.whatsapp.net	[redacted]sagoe[redacted]h
6	6	13	1	[redacted]860050@s.whatsapp.net	[redacted]-El 😎
7	7	13	1	[redacted]909027@s.whatsapp.net	[redacted]ephenoforig[redacted]
8	8	13	1	[redacted]095478@s.whatsapp.net	[redacted]kay😈
9	9	13	1	[redacted]934291@s.whatsapp.net	[redacted]fi
10	10	13	1	[redacted]368054@s.whatsapp.net	[redacted]ee 👧
11	11	13	1	[redacted]329090@s.whatsapp.net	[redacted]ni
12	12	13	1	[redacted]031505@s.whatsapp.net	[redacted]cca
13	13	13	1	[redacted]874772@s.whatsapp.net	[redacted]acemaker
14	14	13	1	[redacted]000922@s.whatsapp.net	[redacted]dom
15	15	13	1	[redacted]947886@s.whatsapp.net	[redacted]NISTER
16	16	13	1	[redacted]574467@s.whatsapp.net	[redacted]€XT£R-
17	17	13	1	[redacted]851813@s.whatsapp.net	[redacted]arteng
18	18	13	1	[redacted]900999@s.whatsapp.net	[redacted]owers Group
19	19	13	1	[redacted]238489@s.whatsapp.net	[redacted]ny
20	20	13	1	[redacted]581168@s.whatsapp.net	[redacted]fi Serebou 👌
21	21	13	1	[redacted]380876@s.whatsapp.net	[redacted]e Writer
22	22	13	1	[redacted]168804@s.whatsapp.net	[redacted]Quaqu
23	23	13	1	[redacted]571480@s.whatsapp.net	[redacted]usu Ansah
24	24	13	1	[redacted]213271@s.whatsapp.net	[redacted]_ES
25	25	13	1	[redacted]341140@s.whatsapp.net	[redacted]oby~C
26	26	13	1	[redacted]622312@s.whatsapp.net	[redacted]adwo
27	27	13	1	[redacted]135386@s.whatsapp.net	[redacted]ss🐋
28	28	13	2	[redacted]709855@s.whatsapp.net	[redacted]rnard Badu [redacted]
29	29	13	1	[redacted]103405@s.whatsapp.net	[redacted]bby
30	30	13	1	[redacted]431645@s.whatsapp.net	[redacted]®
31	31	13	1	[redacted]454739@s.whatsapp.net	[redacted]na boateng
32	32	13	1	[redacted]341932@s.whatsapp.net	[redacted]ay
33	33	13	1	[redacted]500145@s.whatsapp.net	[redacted]eley
34	34	13	1	[redacted]569211@s.whatsapp.net	[redacted]Co
35	35	13	1	[redacted]870567@s.whatsapp.net	[redacted]ma-Marie

DATA STORAGE

IOS

1. Data Protection key.
2. The Keychain.
3. NUSERDefaults*
4. CoreData*
5. SQLite Database**
6. Firebase Realtime Database.
7. Realm Database**

* - Stores data in plain text.

** - Encryption can be configured.

https://support.apple.com/guide/security/adopting-data-protection-in-apps-sec1a976c067/1/web/1

DATA STORAGE

ANDROID

1. Shared Preferences*,***
2. SQLite Database**
3. Firebase Realtime Database.
4. Realm Database**
5. Internal Storage***
6. External Storage****

* - Stores data in plain text.

** - Encryption can be configured.

*** - Accessible via root.

**** - World-readable

SECURING API ENDPOINTS

AUDITING WHATSAPP IOS APP

Failed Attempt:

MITM SSL decryption due to SSL pinning.

*Found a way.... TBD

APP TRANSPORT SECURITY

iOS & Android

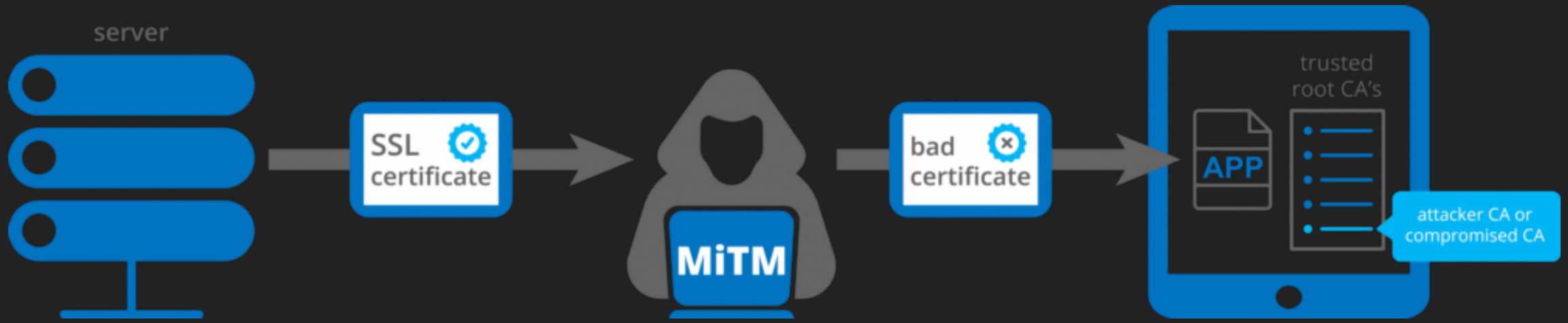
SECURING API ENDPOINTS

APP TRANSPORT SECURITY (ATS)

- No ‘HTTP’ connections.
- Transport Layer Security (TLS) version must be 1.2 or above and must support Perfect Forward Secrecy (PFS) through Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) key exchange and AES-128 or AES-256 symmetric ciphers.
- Mozilla provides SSL configuration generator for web services. https://ssl-config.mozilla.org

SECURING API ENDPOINTS

APP TRANSPORT SECURITY (ATS)



SECURING API ENDPOINTS

SSL PINNING

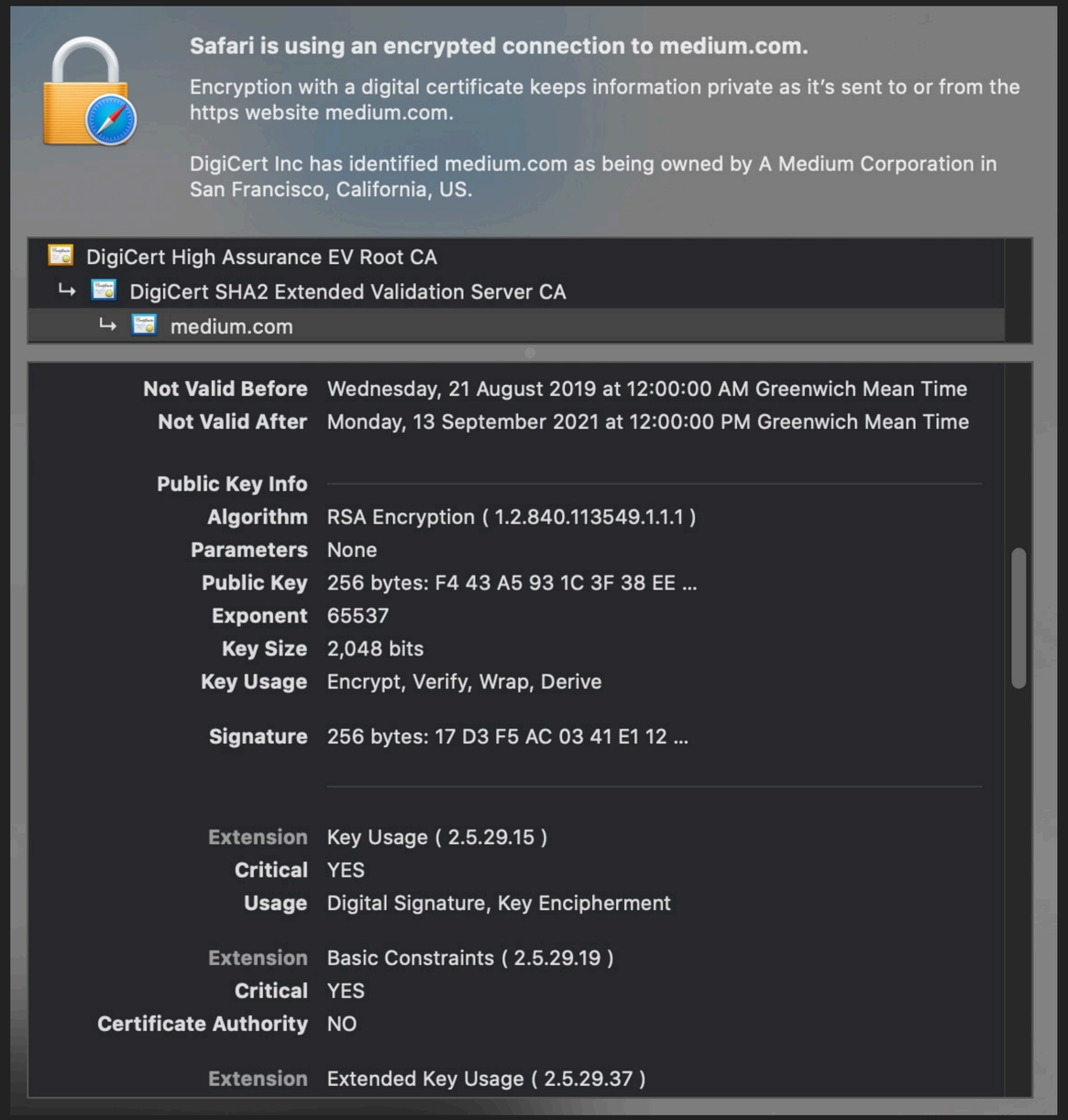
- Certificate Pinning
- Public Key Pinning
- Hash Pinning

SECURING API ENDPOINTS

SSL CERTIFICATE PINNING

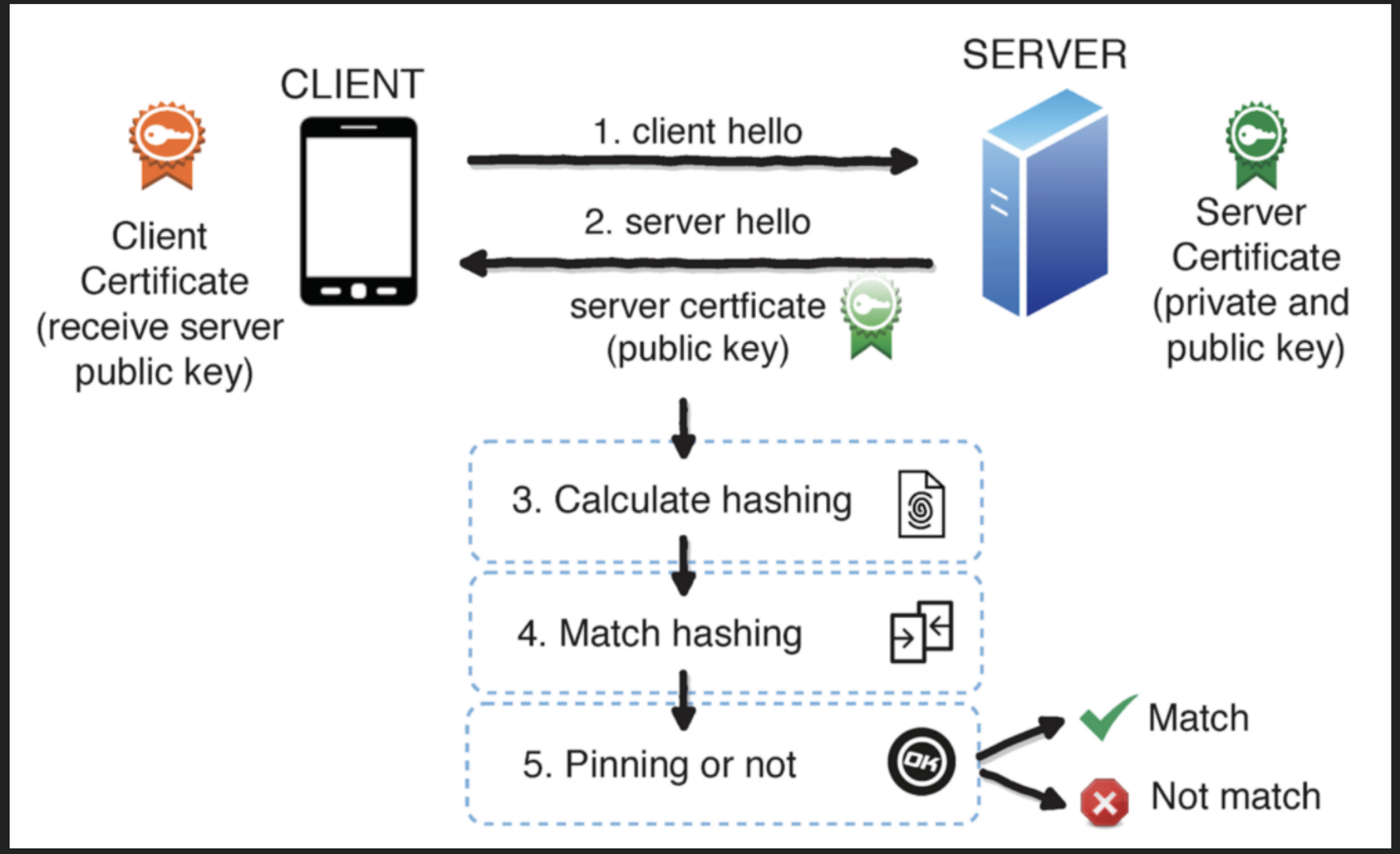
SECURING API ENDPOINTS

SSL PUBLIC KEY PINNING



SECURING API ENDPOINTS

SSL HASH PINNING



SECURING API ENDPOINTS

SSL PINNING

- Resource links:

  iOS https://medium.com/@andy.nguyen.1993/ios-ssl-pinning-bffd2ee9efc

  Android https://medium.com/@mailapurvpandey/ssl-pinning-in-android-90dddfa3e051

SUMMARY

SECURING API ENDPOINTS

SUMMARY

- Adopt standard ATS protocols.
- Use secure client-side databases.
- Do not implement your own encryption/decryption algorithms. Use approved standards.
- Adopt SSL pinning techniques.
- Ensure web services are configured correctly.
- Adopt efficient ACLs (such as using JWTs) for session authentication.
- Avoid re-using sessions keys and symmetric encryption/decryption keys.

THANK YOU

Q/A