

# WhatsApp Forensics

## Advanced acquisition and decryption techniques

Tanya Pankova, Oxygen Forensics



Over **2 billion** users globally



**5.5 billion** messages per day



**4.5 billion** photos shared per day



**1 billion** videos shared per day



# Plan

- Extraction from **Mobile Devices**
- Extraction from **Cloud**
- WhatsApp backup **decryption**
- Access to **WhatsApp Server**
- WhatsApp from **Computer**



# From where do you extract WhatsApp?



Apple  
Android  
Windows Phone

iCloud  
Google Drive

Computers

# WhatsApp security



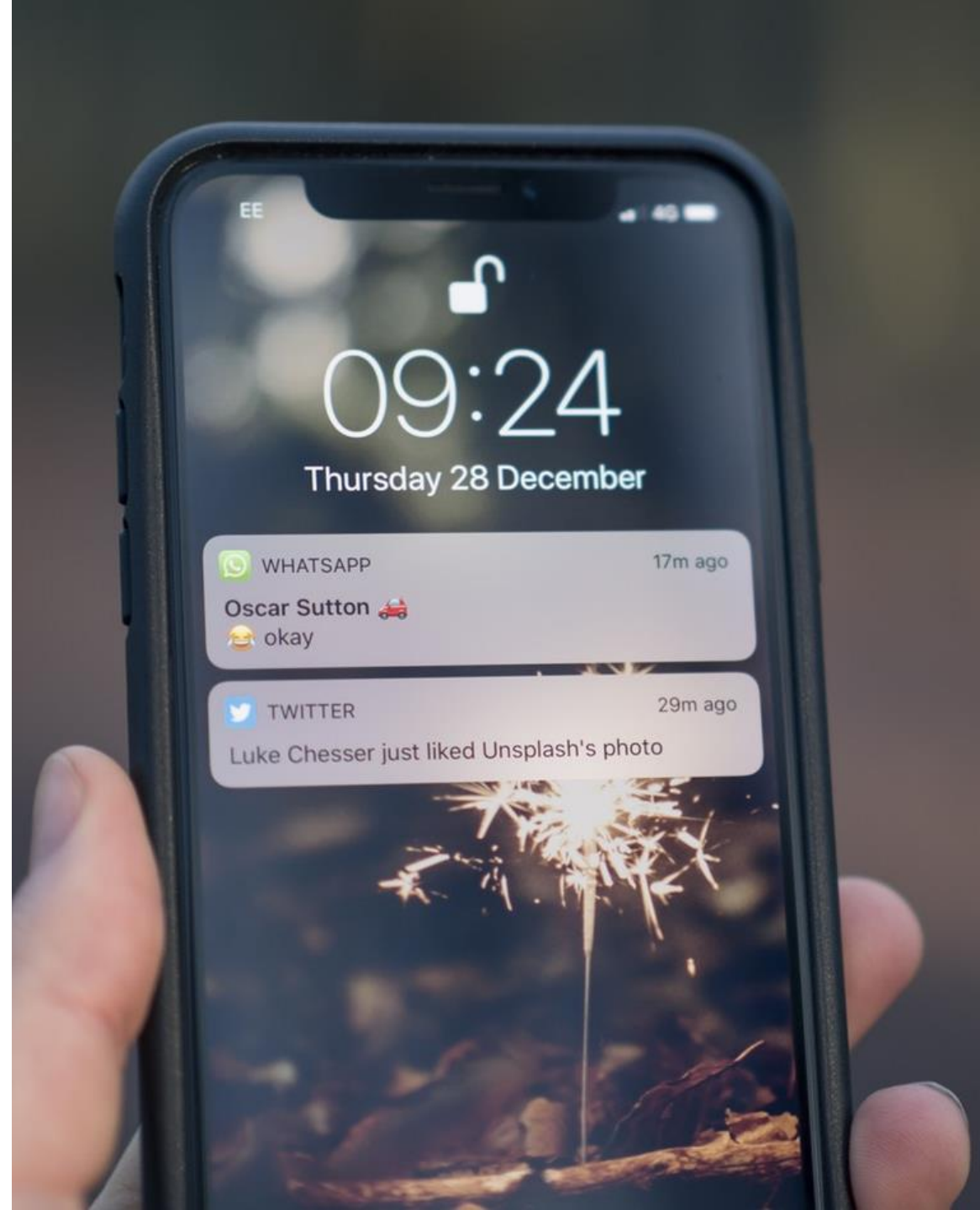
All messages are always end-to-end encrypted. Decryption keys are not stored on the server.



Messages are stored on the server until they are received by the addressee.

# WhatsApp encryption

- Data on device is **not encrypted**
- Backup in iCloud is **encrypted**
- Media files in iCloud are **not encrypted**





# Device

Oxygen Forensic® Detective

File View Tools Service Help

All devices > Amy > Apple iPhone 8 - 15.08.2018 15:30:06 [353001096358800] > Messengers > WhatsApp Messenger

Connect device Export Print Recovery Show viewer Set time zones Reset Filters Help

Information << User data (472) Application files (51) Application information (25)


Keywords Copy to clipboard Show thumbnails Maps and Routes Export to KML Autosize

**Application information**

**WhatsApp ...**  
472 items  
net.whatsapp.W...

Container:  
/private/var/mobile/Applications...

**Details:**  
Source table: ZWAMESSAGE  
Source file: ChatStorage.sqlite  
Message ID: 382  
Direction: Outgoing message  
Remote party: 79850235190  
Remote party name: Colette Béland  
Time stamp (Device time):  
26.06.2018 22:44:37  
Content:  
Media/79850235190@s.whatsa...

  
Type: Image  
File size: 269,79 KB

**Evidence note**

Enter a note for the evidence

Direction	Remote party	Remote party name	Time stamp (Device time)	Content	Caption	Categories
✓	79850235190	Colette Béland	12.07.2018 11:07:56	N/A	N/A	All categories 472
✓	923313526901	Laraib Shah	10.07.2018 19:49:21	Hey	N/A	Account 1
✓	79850235190	Colette Béland	05.07.2018 17:48:45	Talk to me	N/A	Media statuses 6
✓	79850235190	Colette Béland	05.07.2018 17:48:40	Haha heyyyyyy	N/A	Contacts 6
✓	15852859781	Philip Tinder	04.07.2018 14:50:45	Sorry I was traveling	N/A	لارب شاه 6
✓	79850235190	Colette Béland	26.06.2018 22:45:13	Are you envious ?	N/A	Contacts 73
✓	79850235190	Colette Béland	26.06.2018 22:44:37	Media/79850235190@s.whatsapp.net/c/6/c6ecc9d...	N/A	WhatsApp Messenger 11
✓	79850235190	Colette Béland	26.06.2018 22:44:26	Media/79850235190@s.whatsapp.net/c/a/ca4920a...	In Italia si mangia bene 😊	Phonebook 62
✓	923313526901	Laraib Shah	26.06.2018 18:21:18	Going for some work?	N/A	Group chats info 1
✓	923313526901	Laraib Shah	26.06.2018 18:20:18	Ahan	N/A	Chats 371
✓	923313526901	Laraib Shah	26.06.2018 17:48:18	Italy	N/A	Private 368
✓	923313526901	Laraib Shah	26.06.2018 11:28:04	Where are you going?	N/A	2. Colette Béland 62
✓	13103840289, 79...	13103840289, 7...	25.06.2018 22:16:57	Hey guys	N/A	3. Guilherme 97
✓	79998411697	79998411697	25.06.2018 22:16:46	Group	N/A	4. Tyron Ryland 156
✓	79998411697	79998411697	25.06.2018 22:16:46	N/A	N/A	5. Laraib Shah 45
✓	79850235190	Colette Béland	25.06.2018 20:50:01	41.8224678039551;12.4755754470825	Villa Eur Parco dei PiniRome, L	6. Philip Tinder 8
✓	79850235190	Colette Béland	25.06.2018 20:49:43	Guess where I'm	N/A	Group 3
✓	61498091317	Tyron Ryland	20.06.2018 14:17:27	Haha	N/A	9. Group 3
✓	61498091317	Tyron Ryland	20.06.2018 14:17:22	47.3157005310059;8.55022716522217	C. G. Jung Institut Zürich	Calls 11
✓	61498091317	Tyron Ryland	20.06.2018 14:16:03	Heyyyy	N/A	5521994797272 1
✓	61498091317	Tyron Ryland	18.06.2018 13:59:31	Nothing special actually	N/A	79850235190 10
✓	61498091317	Tyron Ryland	18.06.2018 13:59:24	Oh great!	N/A	Shared data 9
✓	61498091317	Tyron Ryland	18.06.2018 11:59:23	Yeah was all good just relaxed lol wat did you get u...	N/A	Locations 3
✓	61498091317					
✓	61498091317					
✓	61498091317					
✓	61498091317					
✓	61498091317					
✓	61498091317					
✓	61498091317					
✓	61498091317					
✓	61498091317					
✓	923313526901					
✓	923313526901					

Version: 10.4.0.54 Apple iPhone 8 Total: 371 Filtered: 371

- Extraction via iTunes backup procedure
- GrayShift's images are also supported
- Contacts, chats, calls, shared data

# WhatsApp encryption

- Data on device is **not encrypted**
- Backup on device and in Google Drive is **encrypted**  
Encryption key is in  
`/data/data/com.whatsapp/files/key`
- Media files in backup are **not encrypted**







# Device

Oxygen Forensic® Detective

File View Tools Service Help

← → All devices ▶ Brooklyn maniac ▶ Stephen Bremer's Samsung phone - 02.03.2016 14:21:27 [354017050438270] ▶ Messengers ▶ WhatsApp Messenger Filtering criteria ...

Connect device Export Print Recovery Show viewer Show viewer Set time zones Reset Filters Help

Information << User data (191) Application files (88)

Keywords Copy to clipboard Show thumbnails Maps and Routes Export to KML Autosize

**Application information**

**WhatsApp ...**  
191 items  
com.whatsapp

Container:  
/data/data/com.whatsapp

**Details:**  
Source table: messages  
Source file: msgstore.db  
ID: 106  
Direction: Incoming message  
Remote party: 79639955252  
Remote party name: Alison 79639955252  
Time stamp (Device time): 24.04.2015 14:17:20  
Content: [Emojis]  
Type: Text  
Received (Device time): 24.04.2015 14:12:19  
BaseName: databases  
AccountID: 79035569010

**Evidence note**

Enter a note for the evidence

Remote party	Remote party name	Time stamp (Device time)	Content	Type
79639955252,79680289231	Alison 79639955252,Barbara Dudek	24.04.2015 14:36:44	Great see you	Text
79680289231	Barbara Dudek	24.04.2015 14:33:25	Yes near central park entrance	Text
79639955252	Alison 79639955252	24.04.2015 14:32:55	So we meet tomorrow at 12	Text
79680289231	Barbara Dudek	24.04.2015 14:32:24	Cute	Text
79639955252,79680289231	Alison 79639955252,Barbara Dudek	24.04.2015 14:32:12	IMG-20150424-WA0000.jpg	image/jpeg
79639955252,79680289231	Alison 79639955252,Barbara Dudek	24.04.2015 14:32:01	Found his photoc	Text
79639955252	Alison 79639955252	24.04.2015 14:28:50	♥♥♥♥♥♥♥♥	Text
79639955252	Alison 79639955252	24.04.2015 14:28:28	Oh I remember him nice guy	Text
79639955252,79680289231	Alison 79639955252,Barbara Dudek	24.04.2015 14:26:00	John Leach	Contact
79639955252,79680289231	Alison 79639955252,Barbara Dudek	24.04.2015 14:25:42	My friend john leach	Text
79680289231	Barbara Dudek	24.04.2015 14:25:23	Who is John?	Text
79639955252,79680289231	Alison 79639955252,Barbara Dudek	24.04.2015 14:25:07	Probably john will join us	Text
79639955252,79680289231	Alison 79639955252,Barbara Dudek	24.04.2015 14:21:49	Some nice cafe	Text
79639955252,79680289231	Alison 79639955252,Barbara Dudek	24.04.2015 14:21:36	Ok and then?	Text
79680289231	Barbara Dudek	24.04.2015 14:21:09	The weather is nice	Text
79680289231	Barbara Dudek	24.04.2015 14:20:55	Yes lets go cycling	Text
79639955252	Alison 79639955252	24.04.2015 14:20:36	Cycling?	Text
79639955252,79680289231	Alison 79639955252,Barbara Dudek	24.04.2015 14:19:50	[Emojis]	Text
79639955252,79680289231	Alison 79639955252,Barbara Dudek	24.04.2015 14:19:18	I suggest some outdoor activity	Text
79639955252,79680289231	Alison 79639955252,Barbara Dudek	24.04.2015 14:18:39	Mmmm you have nice plans	Text
79639955252	Alison 79639955252	24.04.2015 14:17:20	[Emojis]	Text
79639955252	Alison 79639955252	24.04.2015 14:16:40	Let's discuss what we will do this weekend	Text
79639955252	Alison 79639955252	24.04.2015 14:16:27	Hi guys	Text

Categories >>

- All categories 191
- Account 1
- Contacts 25
  - WhatsApp Messenger 10
  - Phonebook 15
- Groups 1
  - WhatsApp Messenger 1
- Group chats info 1
- Messages 142
  - Group chat 25
    - Weekend plans 25
  - Private chat 117
    - 79263487243 1
    - Barbara Dudek 71
    - Alison 79639955252 42
    - 36203312436 1
    - 998943894265 1
    - 998939413243 1
- Calls 10
  - Alison 79639955252 10
- Media 7
- Logs 4

Version: 10.4.0.54 Stephen Bremer's Samsung phone Total: 142 Filtered: 142

- Our own physical extraction
- UFED/XRY images are supported
- Contacts, chats, calls, shared data



# WhatsApp backup in Android

## How to backup

- Settings/Chats/Backup chat in WhatsApp app

## How it looks like

- WhatsApp\_backup\_PHONENUMBER\_DATE\_TIME

## Where to find

- WhatsApp\Databases folder on SD card or other location

## How to extract

- Available via MTP protocol, no physical extraction needed

## How to decrypt

- Using key file from the internal memory (common method)



So you have an encrypted WhatsApp backup from Android device (WhatsApp is deleted or you have no access to the internal memory)

**What will you do to decrypt it?**

# WhatsApp backups decryption

exclusive

## Decrypt WhatsApp backup files

### Step 1. Specify the encrypted databases

Please specify the WhatsApp backup encrypted databases retrieved from SD-card or the internal memory of an Android device.

D:\Oxygen backups\WhatsApp backup\



One encrypted file found. Click "Next" to decrypt.

D:\Oxygen backups\WhatsApp backup\msgstore-2018-05-16.1.db.crypt12

## Decrypt WhatsApp backup files

### Step 2. Log in WhatsApp account associated with the backup

1. Select the authentication type.

Phone number

WhatsApp Cloud token

2. Type the phone number associated with the WhatsApp backup.

**Warning:** if you authenticate via phone number the associated device will be logged out of the WhatsApp account.

+18383902020

3. Specify the output folder and click the "Decrypt backup" button.

D:\



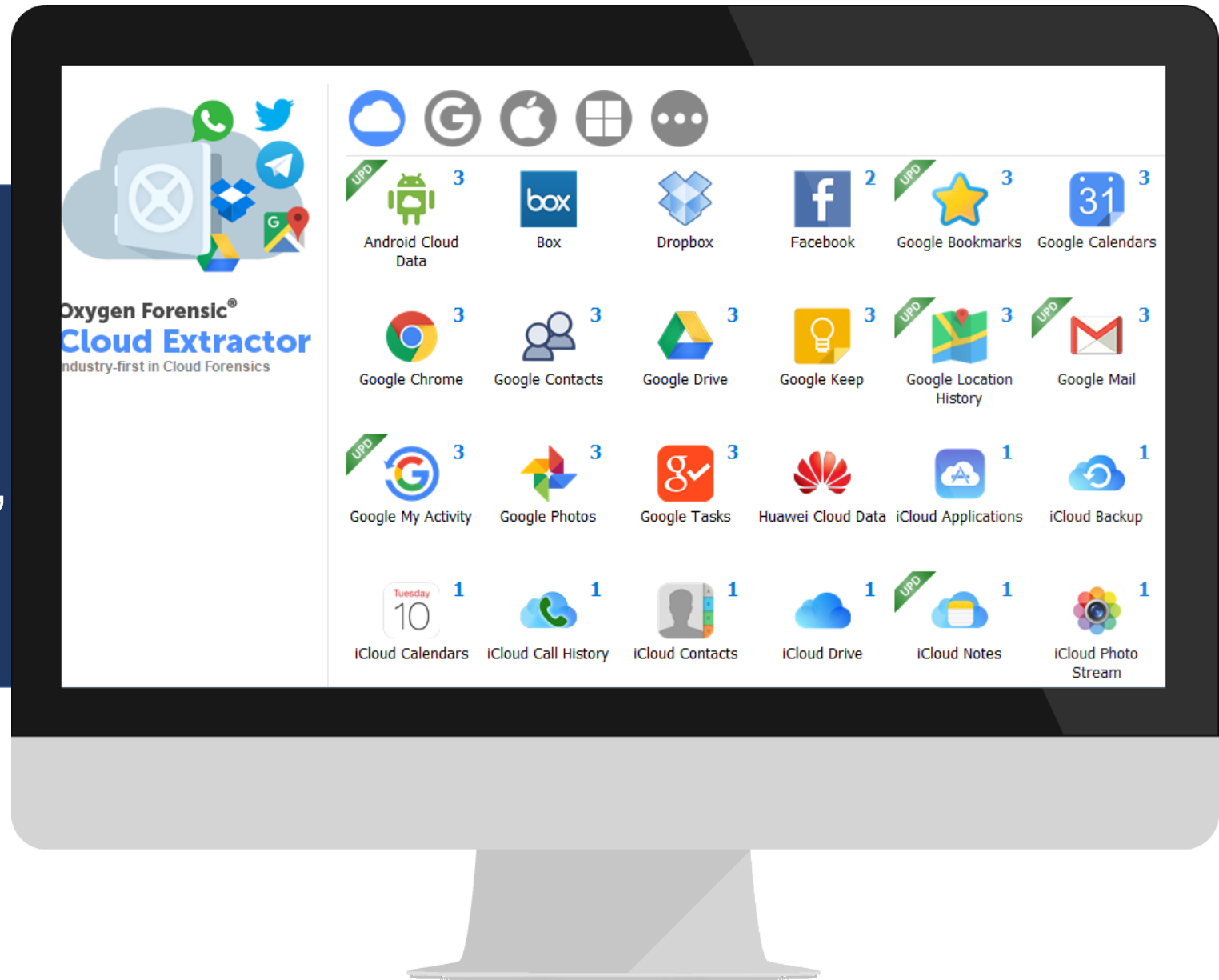
Decrypt backup

# The first in cloud forensics

65 cloud services

Free of charge

Exclusive support Samsung,  
Mi Cloud, Huawei, DJI, etc



# How to access?

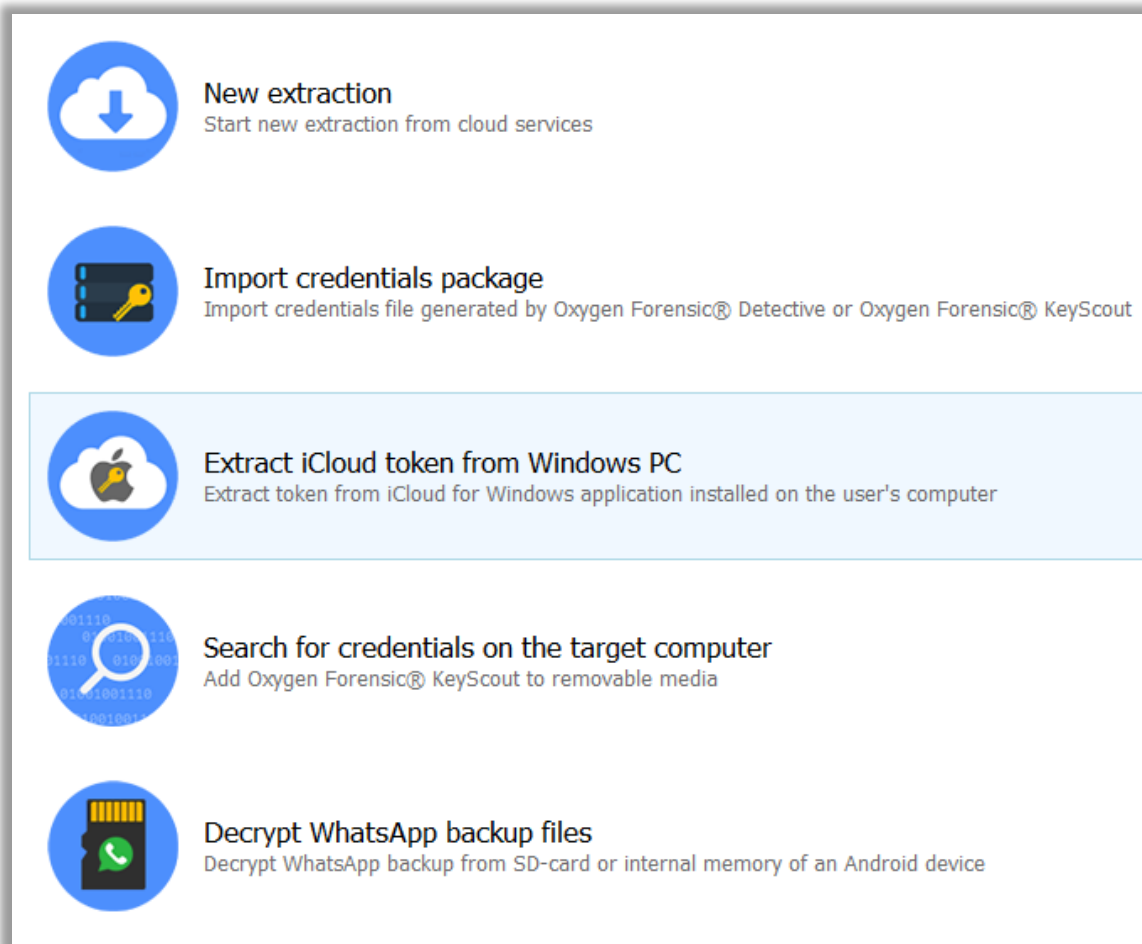
- Login and password
- Token

# Where to find?

- Mobile device
- Computer (KeyScout utility)
- Social analysis



# iCloud and Google Drive credentials



**New extraction**  
Start new extraction from cloud services

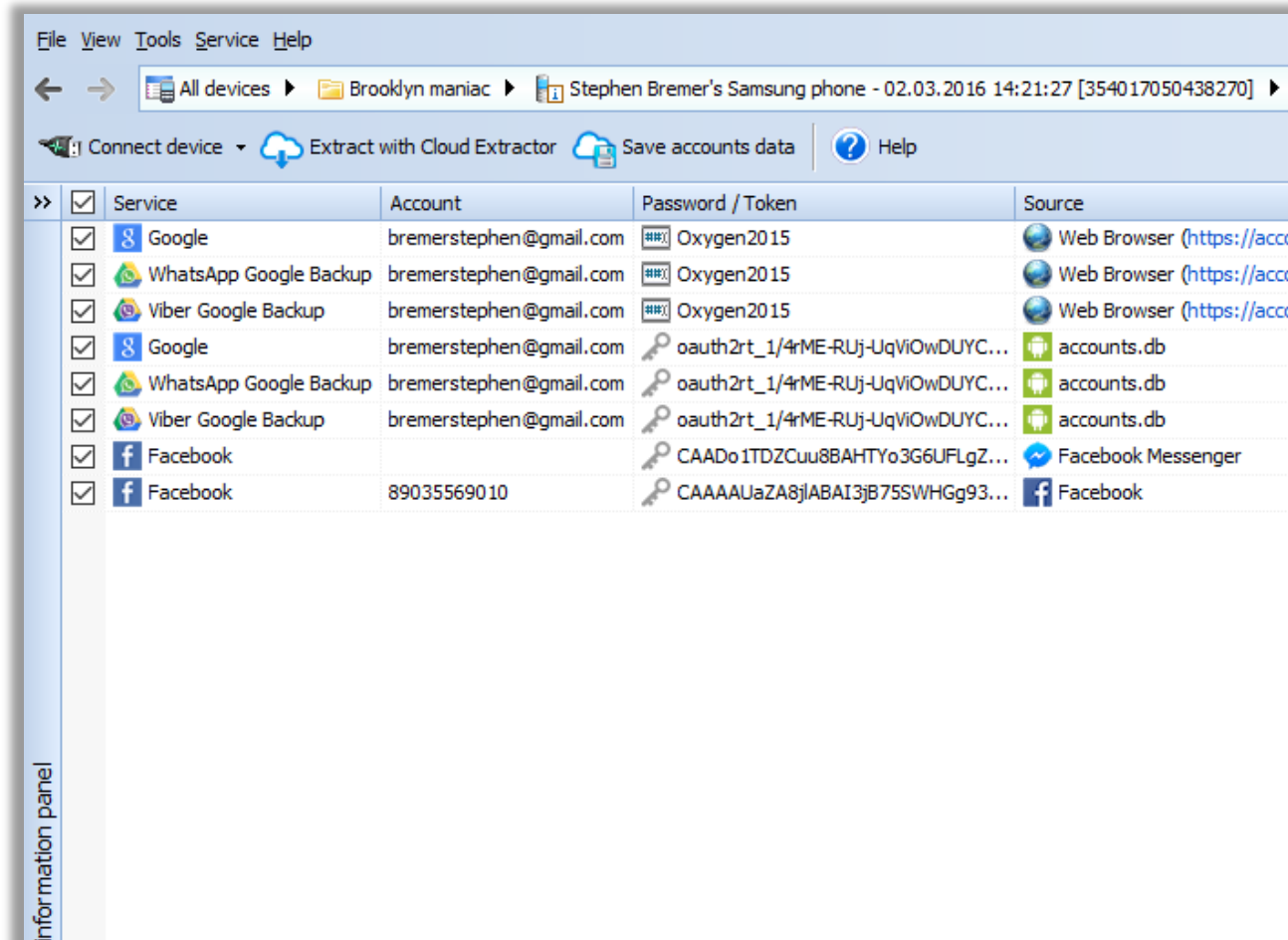
**Import credentials package**  
Import credentials file generated by Oxygen Forensic® Detective or Oxygen Forensic® KeyScout

**Extract iCloud token from Windows PC**  
Extract token from iCloud for Windows application installed on the user's computer

**Search for credentials on the target computer**  
Add Oxygen Forensic® KeyScout to removable media

**Decrypt WhatsApp backup files**  
Decrypt WhatsApp backup from SD-card or internal memory of an Android device

*On computer*



File View Tools Service Help

← → All devices ▶ Brooklyn maniac ▶ Stephen Bremer's Samsung phone - 02.03.2016 14:21:27 [354017050438270] ▶

Connect device Extract with Cloud Extractor Save accounts data Help

Service	Account	Password / Token	Source
Google	bremerstephen@gmail.com	### Oxygen2015	Web Browser (https://acco
WhatsApp Google Backup	bremerstephen@gmail.com	### Oxygen2015	Web Browser (https://acco
Viber Google Backup	bremerstephen@gmail.com	### Oxygen2015	Web Browser (https://acco
Google	bremerstephen@gmail.com	oauth2rt_1/4rME-RUj-UqViOwDUYC...	accounts.db
WhatsApp Google Backup	bremerstephen@gmail.com	oauth2rt_1/4rME-RUj-UqViOwDUYC...	accounts.db
Viber Google Backup	bremerstephen@gmail.com	oauth2rt_1/4rME-RUj-UqViOwDUYC...	accounts.db
Facebook		CAADo1TDZCuu8BAHTYo3G6UFLgZ...	Facebook Messenger
Facebook	89035569010	CAAAAUaZA8jABAI3jB75SWHGg93...	Facebook

information panel

*In mobile device*



# Extracting WhatsApp iCloud backups

## Login/password

Authentication parameters

WhatsApp iCloud Backup

Username/Password **Token**

Username  
peterm@gmail.com

Password  
●●●●●●●●●●●●●●●●●●

Apply Close

1. **Overcome 2FA** (verification code)
2. **Overcome 2-step verification** (enter PIN or reset it)
3. **Decrypt backup** (SMS, phone call)

## Token

Authentication parameters

1. **Overcome 2-step verification** (enter PIN or reset it)
2. **Decrypt backup** (SMS, phone call)

Only until Apple iOS 11.2





# iCloud

Oxygen Forensic Detective

File View Tools Service Help

All devices Case 24.08.2018 16:48:07 Jensen Arkles Clouds - 24.08.2018 16:49:51 Messengers WhatsApp Messenger Filtering criteria ...

Connect device Export Print Show viewer Set time zones Reset Filters Help

Information User data (55) Application files (23)

Application information

**WhatsApp Messenger**  
55 items  
57f9237fN3.net.whatsapp.Whats

Container: /57f9237fN3.net.whatsapp.WhatsApp

**Details:**  
Source table: zwaMessage  
Source file: ChatStorage.sqlite.enc  
Direction: Incoming message  
Remote party: 79151541872  
Remote party name: Mike  
Time stamp (Device time): 21.08.2018 08:58:07  
Text: I'm in Moscow

**Evidence note**  
Enter a note for the evidence

Direction	Remote party	Remote party name	Time stamp (Device time)	Text
Outgoing	79151541872	Mike	21.08.2018 09:01:37	No problem
Incoming	79151541872	Mike	21.08.2018 09:01:32	Sent you by mistake
Incoming	79151541872	Mike	21.08.2018 09:01:26	Oh sorry
Incoming	79151541872	Mike	21.08.2018 09:01:23	Media/79151541872@s.whatsapp.net/f/4/f4038f59-f03e-4863-a8e...
Incoming	79151541872	Mike	21.08.2018 09:01:04	You are welcome
Incoming	79151541872	Mike	21.08.2018 09:00:51	Thanks
Incoming	79151541872	Mike	21.08.2018 09:00:48	Thinks
Incoming	79151541872	Mike	21.08.2018 09:00:45	Piter
Incoming	79151541872	Mike	21.08.2018 09:00:36	Sure
Incoming	79151541872	Mike	21.08.2018 09:00:29	Need to contact hm?
Incoming	79151541872	Mike	21.08.2018 09:00:03	Do you have the contact of Piter?
Incoming	79151541872	Mike	21.08.2018 08:59:36	So cute
Incoming	79151541872	Mike	21.08.2018 08:59:26	Media/79151541872@s.whatsapp.net/2/3/23d420c7-d8b1-4657-b9...
Incoming	79151541872	Mike	21.08.2018 08:59:12	Haha
Incoming	79151541872	Mike	21.08.2018 08:59:01	Window
Incoming	79151541872	Mike	21.08.2018 08:58:58	Looking out of the windup
Incoming	79151541872	Mike	21.08.2018 08:58:46	Media/79151541872@s.whatsapp.net/2/1/21568747-46b5-47e5-a...
Incoming	79151541872	Mike	21.08.2018 08:58:30	Media/79151541872@s.whatsapp.net/5/3/538444aa-b683-464e-b...
Incoming	79151541872	Mike	21.08.2018 08:58:14	Too
Incoming	79151541872	Mike	21.08.2018 08:58:11	You ?
Incoming	79151541872	Mike	21.08.2018 08:58:07	I'm in Moscow
Incoming	79151541872	Mike	21.08.2018 08:57:42	Where are you now?
Incoming	79151541872	Mike	21.08.2018 08:57:30	How are you
Incoming	79151541872	Mike	21.08.2018 08:57:27	Hi Mike
Incoming	79670442810	Player 1	21.08.2018 08:40:35	Hi how are you
Incoming	0@status	WhatsApp	21.08.2018 08:39:24	Media/0@status/e/7/e7014aa1-06b2-439e-a264-2f966fc5cbf9.jpg
Incoming	0@status	WhatsApp	21.08.2018 08:39:24	Media/0@status/3/2/32aad891-963f-4cd9-ac09-abe35c3903af.jpg
Incoming	0@status	WhatsApp		
Incoming	0@status	WhatsApp		
Incoming	0@status	WhatsApp		
Incoming	0@status	WhatsApp		
Incoming	0@status	WhatsApp		

Categories

- All categories 55
- jensenadlesinlaw@gmail.com\_666... 48
  - Encrypted bases 6
    - 79055448310 6
      - BackedUpKeyValue.s... 1
      - calls.log.enc 1
      - ChatStorage.sqlite.enc 1
      - current\_walpaper.jp... 1
      - Sticker.sqlite.enc 1
      - UserDefaults.plist.enc 1
    - 79055448310 42
      - Calls 2
        - 79151541872 1
        - 79670442810 1
      - Chats 31
        - Private 31
          - Mike 24
          - Player 1 1
          - WhatsApp 6
        - Shared data 9
          - Locations 1
          - Contacts 1
          - Photos 7
        - Media 7

## Chats, calls, shared data, media



# Extracting WhatsApp Google backups

Login/password

Authentication parameters

WhatsApp Google Backup

Username/Password  Token

Username  
peters@gmail.com

Password  
●●●●●●●●●●

Upload key file Apply Close

1. **Overcome 2FA** (SMS, authenticator code, backup code, Google Prompt)
2. **Overcome 2-step verification** (enter PIN or reset it)
3. **Decrypt backup** (SMS, phone call)

Token

Authentication parameters

WhatsApp Google Backup

Username/Password   Token

Token  
t8msvxwdR-5kH9jSpCGTfw2w879ie8u08gMKME

Upload key file Apply Close

1. **Overcome 2-step verification** (enter PIN or reset it)
2. **Decrypt backup** (SMS, phone call)

***BUT: if you do physical acquisition of Android in OFD the backup is automatically decrypted via token!***



# Google Drive

Oxygen Forensic® Detective

File View Tools Service Help

← → All devices ▶ Case 24.08.2018 17:21:47 ▶ Bill Bobb Clouds - 24.08.2018 17:22:56 ▶ Messengers ▶ WhatsApp Google Backup Filtering criteria ...

Connect device ▶ Export ▶ Print ▶ Show viewer ▶ Set time zones ▶ Reset Filters ▶ Help

Information << User data (40) Application files (11)

Application information

**WhatsApp Google ...**  
40 items  
cloud.whatsapp.googledrive

Container: /cloud.whatsapp.googledrive

**Details:**  
Source table: messages  
Source file: msgstore.db.crypt12  
ID: 10  
Direction: Incoming message  
Remote party: 79998411697  
Time stamp (Device time): 17.08.2018 15:45:39  
Content: Hey there cutie  
Type: Text  
Received (Device time): 17.08.2018 15:44:50

Evidence note

Enter a note for the evidence

ID	Direction	Remote party	Time stamp (Device time)	Content	Type	Created (Device time)	Received	Categories
39	Outgoing	79998411697	22.08.2018 15:41:52	See ya	Text	N/A	N/A	All categories
38	Outgoing	79998411697	22.08.2018 15:41:49	That's the spirit!	Text	N/A	N/A	Encrypted bases
37	Incoming	79998411697	22.08.2018 15:41:29	Your wish is my command	Text	22.08.2018 15:41:30	22.08.	Backup 79850238613
36	Outgoing	79998411697	22.08.2018 15:41:10	I'm always happy to meet you at o...	Text	N/A	N/A	Account
35	Outgoing	79998411697	22.08.2018 15:40:48	You know I love parties	Text	N/A	N/A	Chats
34	Outgoing	79998411697	22.08.2018 15:40:30	BORING	Text	N/A	N/A	Private chat
33	Incoming	79998411697	22.08.2018 15:40:12	Just the two of us	Text	22.08.2018 15:40:12	22.08.	79998411697
32	Incoming	79998411697	22.08.2018 15:40:05	Let's go somewhere together	Text	22.08.2018 15:40:05	22.08.	Media
31	Outgoing	79998411697	22.08.2018 15:39:03	Join me 2nite? Harry's place	Text	N/A	N/A	
30	Outgoing	79998411697	22.08.2018 07:25:29	Thanks I guess	Text	N/A	N/A	
29	Outgoing	79998411697	22.08.2018 07:25:25	Aw	Text	N/A	N/A	
28	Incoming	79998411697	21.08.2018 09:08:06	Miss you A LOT♥	Text	21.08.2018 09:08:06	21.08.	
27	Incoming	79998411697	21.08.2018 09:07:24	I know @	Text	21.08.2018 09:07:24	21.08.	
26	Outgoing	79998411697	20.08.2018 15:56:18	U were nice	Text	N/A	N/A	
25	Outgoing	79998411697	20.08.2018 15:56:10	Thanks babe	Text	N/A	N/A	
24	Incoming	79998411697	20.08.2018 15:43:19	Yeah! Was nice to see you there, y...	Text	20.08.2018 15:43:19	20.08.	
23	Outgoing	79998411697	20.08.2018 07:17:46	Last night was WILD @DDD	Text	N/A	N/A	
22	Outgoing	79998411697	20.08.2018 07:17:24	Hey babe	Text	N/A	N/A	
21	Outgoing	79998411697	17.08.2018 16:02:13	Yay	Text	N/A	N/A	
20	Incoming	79998411697	17.08.2018 16:00:18	What you gonna drink?	Text	17.08.2018 16:00:18	17.08.	
19	Incoming	79998411697	17.08.2018 15:59:57	Hmmm why not?!	Text	17.08.2018 15:59:58	17.08.	
18	Outgoing	79998411697	17.08.2018 15:57:32	You coming?	Text	N/A	N/A	
17	Outgoing	79998411697	17.08.2018 15:50:22	Abby's place	Text	N/A	N/A	
16	Outgoing	79998411697	17.08.2018 15:50:17	Wanna join me 2nite?	Text	N/A	N/A	
15	Outgoing	79998411697	17.08.2018 15:50:01	Lighhhh	Text	N/A	N/A	
14	Incoming	79998411697	17.08.2018 15:47:35	Where've you been, long time no see	Text	17.08.2018 15:47:35	17.08.	
13	Incoming	79998411697	17.08.2018 15:47:05	Enjoying my life, too many parties! ...	Text	17.08.2018 15:47:05	17.08.	
12	Incoming	79998411697	17.08.2018 15:45:...					
11	Outgoing	79998411697	17.08.2018 15:45:...					
10	Outgoing	79998411697	17.08.2018 15:45:...					
9	Incoming	79998411697	17.08.2018 15:32:...					
8	Incoming	79998411697	17.08.2018 15:32:...					

Version: 10.4.0.54 Bill Bobb Clouds Total: 32 Filtered: 32

Chats, calls, shared data, media

# WhatsApp Server data

**Incoming messages with attachments**

**Original messages embedded into reply**

**Missed calls**

**Information about deleted messages**

**Information about account, groups, contacts**

**Broadcast messages**

# Access to the WhatsApp server

exclusive



Phone number



WhatsApp  
Cloud token

Authentication parameters

WhatsApp Cloud

Phone number Token

Phone number in international format

*e.g. +1703\*\*\*\*\*23*

Apply Close



# WhatsApp Server

Oxygen Forensic® Detective

File View Tools Service Help

← → All devices ▸ Neo Case 27.08.2018 10:46:57 ▸ Neo Steve Bobb Clouds - 27.08.2018 10:48:58 ▸ Messengers ▸ WhatsApp Cloud Filtering criteria ...

Connect device ▾ Export ▾ Print ▾ Show viewer Set time zones Reset Filters Help

Information << User data (14) Application files (4)

Application information

**WhatsApp Cloud**  
14 items  
cloud.whatsappcloud  
Container: /cloud.whatsappcloud

**Details:**  
Source table: Messages;ContactAttachments;Locatio...  
Source file: main.db3  
Direction: Message not delivered  
Decrypted: Data successfully decrypted  
Remote party: 79151541872  
Time stamp (Device time): 24.08.2018 14:01:35  
Time stamp (re-send) (Device time): 27.08.2018 07:40:02  
Text: Again some urgent issue  
Type: private  
ID: 06AB66879DA1EA94608CF3102DDDC

**Evidence note**

Enter a note for the evidence

		Direction	Decrypted	Remote party	Time stamp (Device time)	Text	Media file	Shared contact	Categories
<input checked="" type="checkbox"/>				79151541872	24.08.2018 14:11:07	Are you offline	N/A	N/A	All categories 14
<input checked="" type="checkbox"/>				79151541872	24.08.2018 14:04:34	Really very very urgent	N/A	N/A	Accounts 1
<input checked="" type="checkbox"/>				79151541872	24.08.2018 14:04:25	Contact him asap	N/A	N/A	79055448310 13
<input checked="" type="checkbox"/>				79151541872	24.08.2018 14:04:17	N/A	N/A	BEGIN:VCARDVERSION:3.0N:Pkant;Bot	Contacts 2
<input checked="" type="checkbox"/>				79151541872	24.08.2018 14:03:09	N/A	1ecc85eb264203810...	N/A	Private chats 8
<input checked="" type="checkbox"/>				79151541872	24.08.2018 14:01:35	Again some urgent issue	N/A	N/A	79151541872 8
<input checked="" type="checkbox"/>				79151541872	24.08.2018 14:01:18	Are you there	N/A	N/A	Statuses 1
<input checked="" type="checkbox"/>				79151541872	24.08.2018 14:01:10	Hi	N/A	N/A	23790889875 1

**Categories**

- All categories 14
  - Accounts 1
  - 79055448310 13
    - Contacts 2
  - Private chats 8
    - 79151541872 8
  - Statuses 1
  - 23790889875 1
  - Calls 1
    - hellenaabbers5 1
  - Attached files 1

Contacts, unanswered calls, undelivered messages, shared data

**Details**

Direction: (Message not delivered)  
Decrypted: (Data successfully decrypted)  
Remote party: 79151541872  
Time stamp: 24.08.2018 14:01:35  
Time stamp (re-send): 27.08.2018 07:40:02  
Text: Again some urgent issue  
Type: private  
ID: 06AB66879DA1EA94608CF3102DDDC328

# What about deleted data?



**Phone:** can be recovered from SQLite databases

**Cloud:** deleted from iCloud after the first synchronization



**Phone:** can be recovered from SQLite databases

**Backup:** the device locally stores up to 9 backups

**Cloud:** deleted from Google Drive after the first synchronization

# WhatsApp on computers

## WhatsApp Web and WhatsApp Desktop

- Settings -> WhatsApp Web/Desktop -> Scan QR code in a mobile device

## Any user data on PC?

- Logs (where app was launched, device model and OS)
- No messages and contacts
- Token



# WhatsApp QR token from PC



Using this token you can download chats from a locked device

Oxygen Forensic KeyScout - 2.0.0.243

User	Service	Credential Type	Source
<input checked="" type="checkbox"/>	Unknown	Password	Thunderbird
<input checked="" type="checkbox"/>	Unknown	Password	Thunderbird
<input checked="" type="checkbox"/>	Unknown	Password	Thunderbird
<input checked="" type="checkbox"/>	Unknown	Password	Thunderbird
<input checked="" type="checkbox"/>	WhatsApp QR	Token	WhatsApp Desktop
<input checked="" type="checkbox"/>	Telegram	Token	Telegram Desktop
<input checked="" type="checkbox"/> 115181012930083873894	Google	Google Refresh Token	Google Chrome
<input checked="" type="checkbox"/> 103677994952096780579	Google	Google Refresh Token	Google Chrome

Oxygen Forensic® Cloud Extractor - 4.5.0.11

### Credentials package viewer

Select services to load from credentials package

Services (1/23)	Credentials
<input type="checkbox"/> Google	Refresh token: GRT:MS9CTU5UcHFkLTZ2WU9pdVWVZTHFhTzFzUlp3XzRoazBMaGludH...
<input type="checkbox"/> Google	Refresh token: GRT:MS96eGZKRFE30HpMYThiY0hrajRCY3hSZ1hkSm42a2ZjY2VUNn...
<input type="checkbox"/> Google Home	Refresh token: GRT:MS9CTU5UcHFkLTZ2WU9pdVWVZTHFhTzFzUlp3XzRoazBMaGludH...
<input type="checkbox"/> Google Home	Refresh token: GRT:MS96eGZKRFE30HpMYThiY0hrajRCY3hSZ1hkSm42a2ZjY2VUNn...
<input type="checkbox"/> Telegram	Username: [redacted] Access token: TGT:ewogICAgImRlc2NyaXB0aW9uIjogIjRlbgVncmFtEjEpTT04gVG9rZ...
<input checked="" type="checkbox"/> WhatsApp QR	Username: [redacted] Access token: ewogICAgImJyb3dzZXJfaWQOIAIY2R10cVZXWTRMT1NFbndRdHJFYMZ...
<input type="checkbox"/> Unknown (mailbox://fs)	Username: tpankova 2 Password: *****
<input type="checkbox"/> Unknown (smtp://fs)	Username: tpankova Password: *****
<input type="checkbox"/> Unknown (smtp://fs)	Username: taniap Password: *****

Expand all Show passwords Save to file

Back Next Close



# WhatsApp QR Code

Oxygen Forensic® Detective

File View Tools Service Help

All devices Case 19.09.2018 18:03:09 WhatsApp QR 2 - 19.09.2018 18:07:13 Messengers WhatsApp QR Filtering criteria ...

Connect device Export Print Show viewer Set time zones Reset Filters Help

Information User data (63) Application files (2)

Keywords Copy to clipboard Show thumbnails Maps and Routes Export to KML Autosize

**Application information**

**WhatsApp QR**  
63 items  
cloud.whatsapp.qr  
Container: /cloud.whatsapp.qr

**Details:**  
Source table: messages;chats;peers  
Source file: main.db3  
Direction: Outgoing message  
Remote party: Colette Béland  
Time stamp (Device time): 14.09.2018 12:39:30  
Text: Whatever  
ID: 3AE4C51DF614A08E1F6D

**Evidence note**

Enter a note for the evidence

Direction	Remote party	Time stamp (Device time)	Text
Outgoing	J	19.09.2018 15:05:37	Where are u?
Outgoing	J	19.09.2018 15:05:29	Urgent issue
Outgoing	J	19.09.2018 15:01:07	You don't answer :(
Outgoing	J	19.09.2018 14:59:40	Me too
Incoming	Jensen Eye Candy	18.09.2018 08:54:30	Never mind
Incoming	J	18.09.2018 08:53:42	I miss those parties a lot
Incoming	J	18.09.2018 08:53:23	Just the three of us: you, me and some cocaine
Incoming	J	18.09.2018 08:52:47	I wanna meet you
Incoming	J	18.09.2018 08:52:40	Hey babe
Incoming	J	14.09.2018 12:39:53	RIGHT NOW
Incoming	J	14.09.2018 12:39:51	CALL ME
Incoming	J	14.09.2018 12:39:48	I NEED YOUR HELP
Incoming	J	14.09.2018 12:39:41	JAY!!!!!!
Incoming	Colette Béland	14.09.2018 12:39:30	Whatever
Incoming	J	14.09.2018 10:01:30	Me too
Incoming	J	14.09.2018 10:01:24	Me too babe
Incoming	J	14.09.2018 10:01:17	Awww
Incoming	J	14.09.2018 10:00:23	I can't wait to see you
Incoming	J	14.09.2018 10:00:15	Mm
Incoming	J	14.09.2018 09:55:13	How I wish that there would be only two of us...
Incoming	J	14.09.2018 09:54:54	You are a real treasure
Incoming	J	14.09.2018 09:54:39	
Incoming	J	14.09.2018 09:50:50	Yep

**Categories**

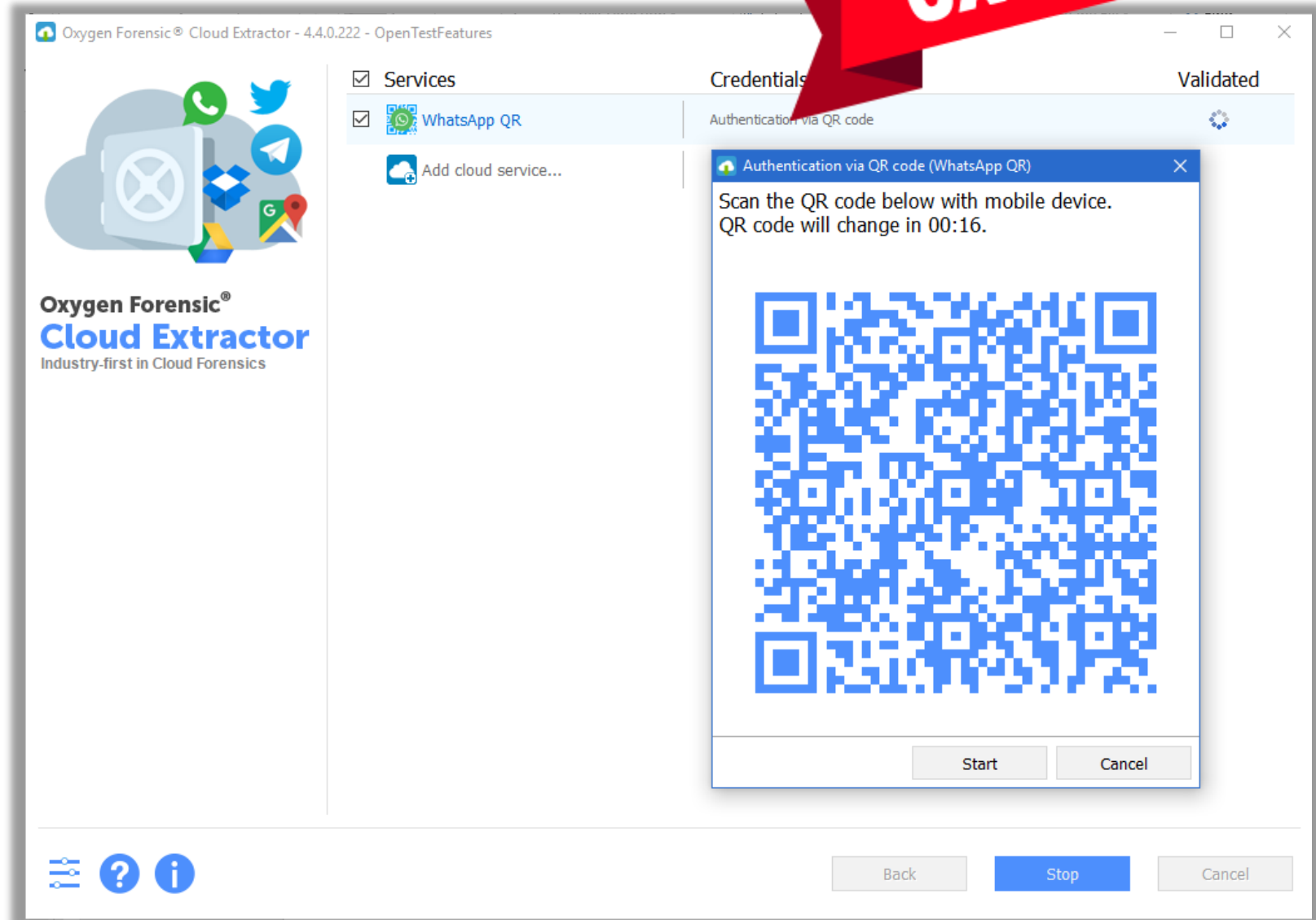
- All categories 63
  - Accounts 1
  - 79998411697\_9e0b20b39827f97f... 62
    - Contacts 12
    - Friends 12
    - Private chats 29
      - Colette Béland 1
      - J 24
      - Jensen Eye Candy 1
      - Laraib Shah 1
      - Philip Tinder 1
      - Tyron Ryland 1
    - Group chats information 6
      - Group 2
        - Members 1
      - Party makers 4
        - Members 3
    - Group chats 11
      - Group 1
      - Party makers 10
    - Missed calls 4
      - Guilherme 1
      - J 3

Device and account info, contacts, chats, missed calls, media files and other attachments

# WhatsApp QR code from a device

exclusive

- Android, Apple iOS, Windows Phone devices
- Scan QR-code from a device in Cloud Extractor



# How QR-code method can be used?



## If device is unlocked

1. Physical extraction fails
2. No possibility to decrypt iTunes backup
3. If your time for extraction is limited



## If device is locked

Use Oxygen Forensic KeyScout to detect a token on PC (if WhatsApp was used) and extract WhatsApp data from locked device

# Summary. How to extract?

## Apple iOS device

- Do logical device extraction
- Use credentials in Cloud Accounts section to access WhatsApp in iCloud

## Android device

- Do physical device extraction
- Check SD card for WhatsApp backups (up to 9 backups!)
- Use credentials in Cloud Accounts section to access WhatsApp in Google Drive

## Access WhatsApp Server via

- A phone number
- A WhatsApp Cloud token. Look for it in Cloud Accounts section.

## Access WhatsApp via QR-code or computer token

# Summary. How to decrypt?

## Apple iOS device

- Use available methods to decrypt cloud backups

## Android device

- Use available methods to decrypt cloud and SD card backups

## Available decryption methods

- Key file (commonly used)
- WhatsApp Cloud token (exclusive)
- Phone number (exclusive)

# Comparison chart (WhatsApp)

	OFD	Competitor
Device extraction	Yes	Yes
Cloud backups	Yes	Yes
Backup decryption via SMS	Yes	No
WhatsApp Server	Yes	No
WhatsApp QR code	Yes	No

# Other Messenger Support

	Device (Apple, Android)	Cloud
Facebook	Yes	Yes
Telegram	Yes	Yes
Viber	Yes	Yes
Skype	Yes	No
CoverMe	Yes	No
Signal	Yes	No
WeChat	Yes	No





# Telegram Messenger

- Extraction from Apple iOS (JB) and Android devices (physical dump)
  - Telegram app is not encrypted
  - Telegram X app needs decryption
- Extraction from Telegram cloud via phone number/token
- Token can be found in Android devices and on PC
- No secret chats are saved in cloud



# Facebook Messenger

- Extraction from Apple iOS (JB) and Android devices (physical dump)
- Complete extraction from Facebook cloud via login/password or token
- Token can be found in Apple iOS and Android devices
- This token lives a long life



# Viber Messenger

- Extraction from Apple iOS (even NJB) and Android devices (physical dump)
- Complete extraction from Viber cloud via login/password or token
- Token can be found in Apple iOS and Android devices



# Signal Messenger

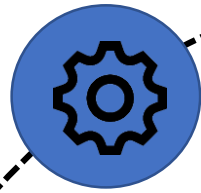
- Extraction and decryption of encryption keys from the Android Keystore
- Decryption of Signal Messenger from Android devices



# CoverMe Messenger

- Extraction and decryption from Apple iOS (even NJB) and Android devices (physical dump)

**Oxygen Forensic Extractor**  
(mobile and drone data)



**Oxygen Forensic KeyScout**  
(passwords and tokens  
collection on computer)

**Oxygen Forensic  
Cloud Extractor**



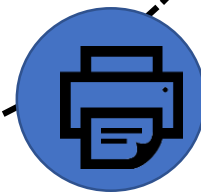
# Oxygen Forensic Detective

has FREE built-in modules



**Data Analysis  
Tools**

**Call Data Expert**



**Export Engine**



**Ask for a demo license to  
try all these great features**

**[tanya.pankova@oxygen-forensic.com](mailto:tanya.pankova@oxygen-forensic.com)**