FORENSAFE

Large Scale Digital Forensic Investigations

OSDFCon

İbrahim Halil Saruhan
ibrahimsaruhan@gmail.com

Story : Gülen Movement (AKA FETO) and Coup Attempt

FORENSAFE

Gulen Movement

- Religious group with more than 40 years of history
- Infiltrated into judicial, military and law enforcement organizations in Turkey
- International organization with highly educated people

Coup Attempt

- On 15 July 2016, attempted in Turkey against state institutions, government and president, was carried out by a faction within the Turkish Armed Forces and failed after forces loyal to the state and **people** defeated them
- Turkish Government accused coup leaders of being linked to the Gulen Movement
- During the coup attempt, over **240 people died,** more than **2,100 were injured,** many government buildings, including the **Turkish Parliament** were damaged and mass arrests followed, after 1 month, **81494** people are purged and **18756** people are arrested, in a year **80000** more people got arrested related to FETO, 75.000 of them due to **ByLock**

Digital Forensics

- **Number of evidence related to Coup attempt was huge (~430.000), after a year it became more than 1.600.000**

Digital Forensics Challenges

- Technology might prevent evidence being generated
- Technology is intentionally developed with antiforensics capabilities
- Technology might not be available for evidence gathering or analysis

- Number of evidence to be analyzed could be enormous
- Number of evidence increase continuously while investigation
- Not clear Scope, also not easy to clarify

- Encryption and AntiForensics

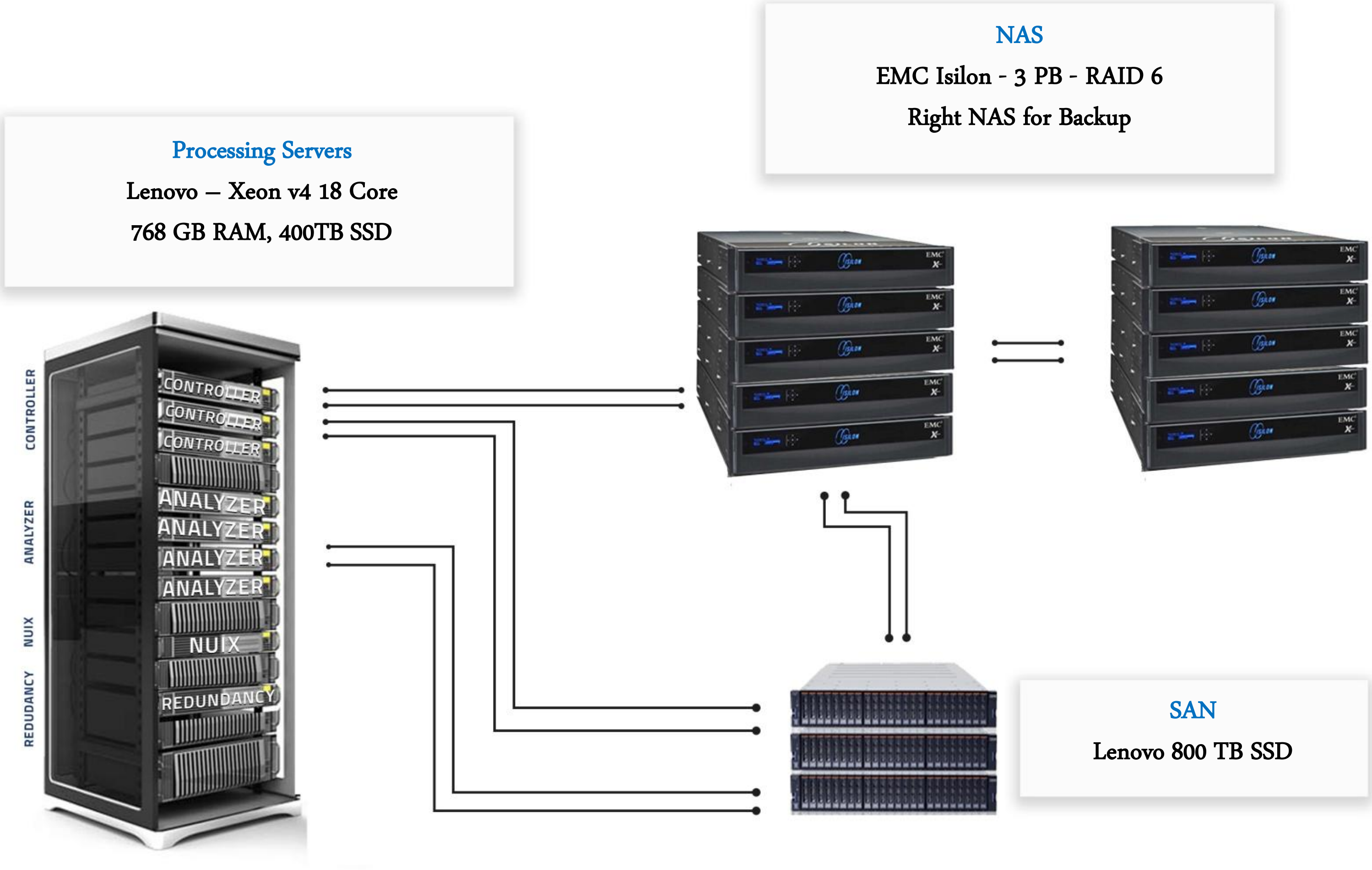
About the Case and Scope

- **Hundreds of thousands of disks → thousands of cases**
- **Hundreds of thousands of mobile devices and other media**
- Initially **430.000 disks/devices, currently 1.600.000 disks/devices**

- **Huge imaging and analysis task**

- Disk sizes are average
- Clear search criteria – FETO related information
- Legal requirements (Source of evidence, analysis steps)

Example System Room



Processing Servers

Lenovo – Xeon v4 18 Core

768 GB RAM, 400TB SSD

NAS

EMC Isilon - 3 PB - RAID 6

Right NAS for Backup

SAN

Lenovo 800 TB SSD

Some Statistics from Investigation

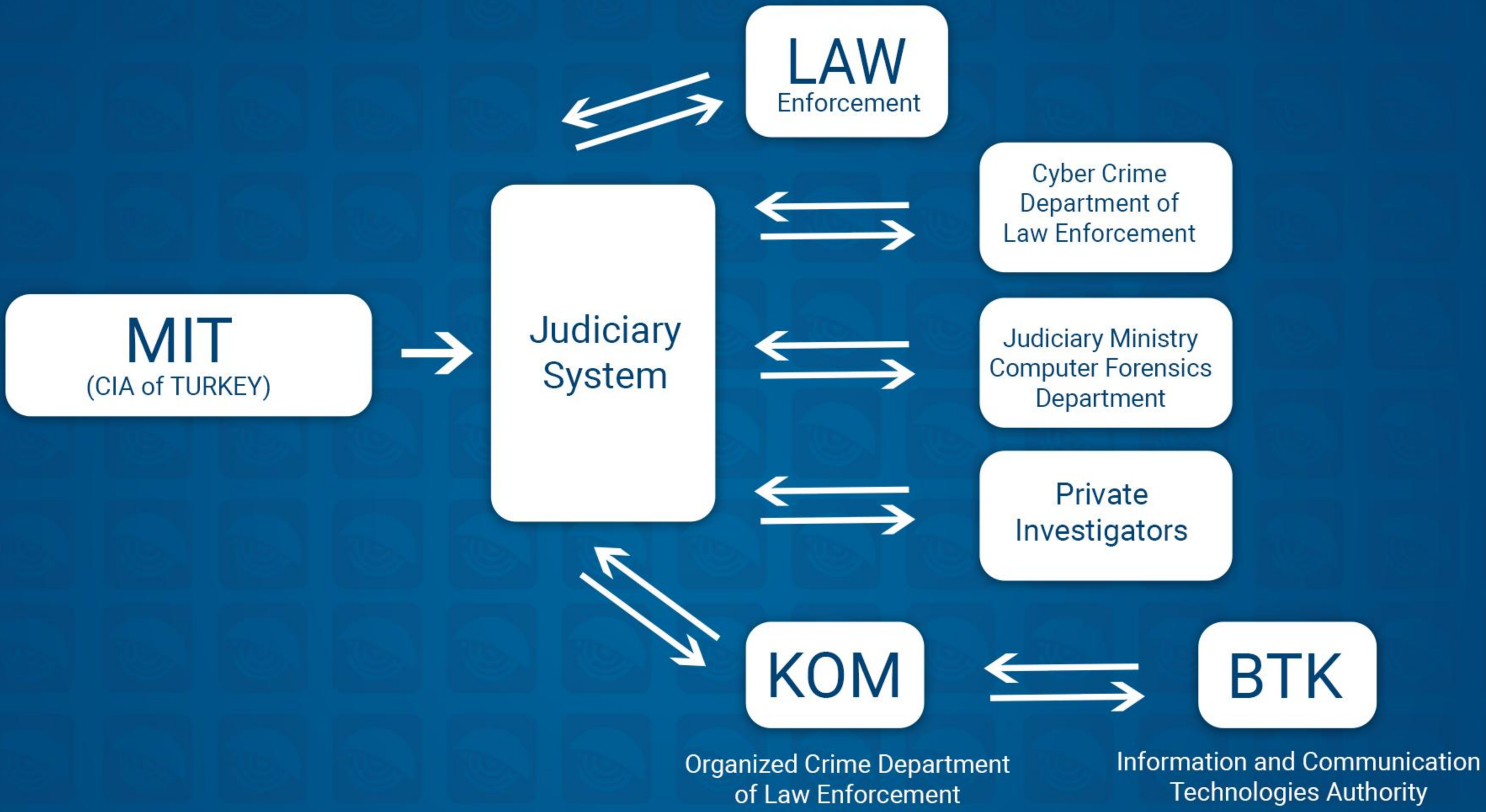
- Imaging speed with 16 Tableau devices and 16 people is ~1000 imaging per month, could be twice as much if needed
- ~1000 images are also analyzed monthly
- Multi million dollar purchase including digital forensics software
- Not a single digital forensics software can cover all the investigation requirements
- **Even planning is the key, anticipation is not as easy as it sounds**

Performance Statistics

- Commercial digital forensics software using only ~% 7 of CPU
- One Commercial Password Cracking Software using ~% 85 of CPU
- One Commercial Digital Forensics Software with 16 core can reach up to ~% 40 of CPU
- Reason seems to be **DTSearch**, which is used by most digital forensics software

One Example Action List

1. Get Information about **Operating System**
2. **Recover all** folders/files including **deleted** files and folders
3. **Extract** and **recover** all **compound** files
4. Calculate **Hashes** of all files and folders
5. Exclude **NSRL** (National Software Reference Library) List
6. **OCR** Process
7. **Keyword** Search
8. **Encrypted** Disk and File Analysis
9. **Internet Activity** Analysis
10. **Instant Messaging**
11. **Export** all results as **Portable Case** and optionally Report in case it is needed



MIT
(CIA of TURKEY)

Judiciary System

LAW
Enforcement

Cyber Crime Department of Law Enforcement

Judiciary Ministry Computer Forensics Department

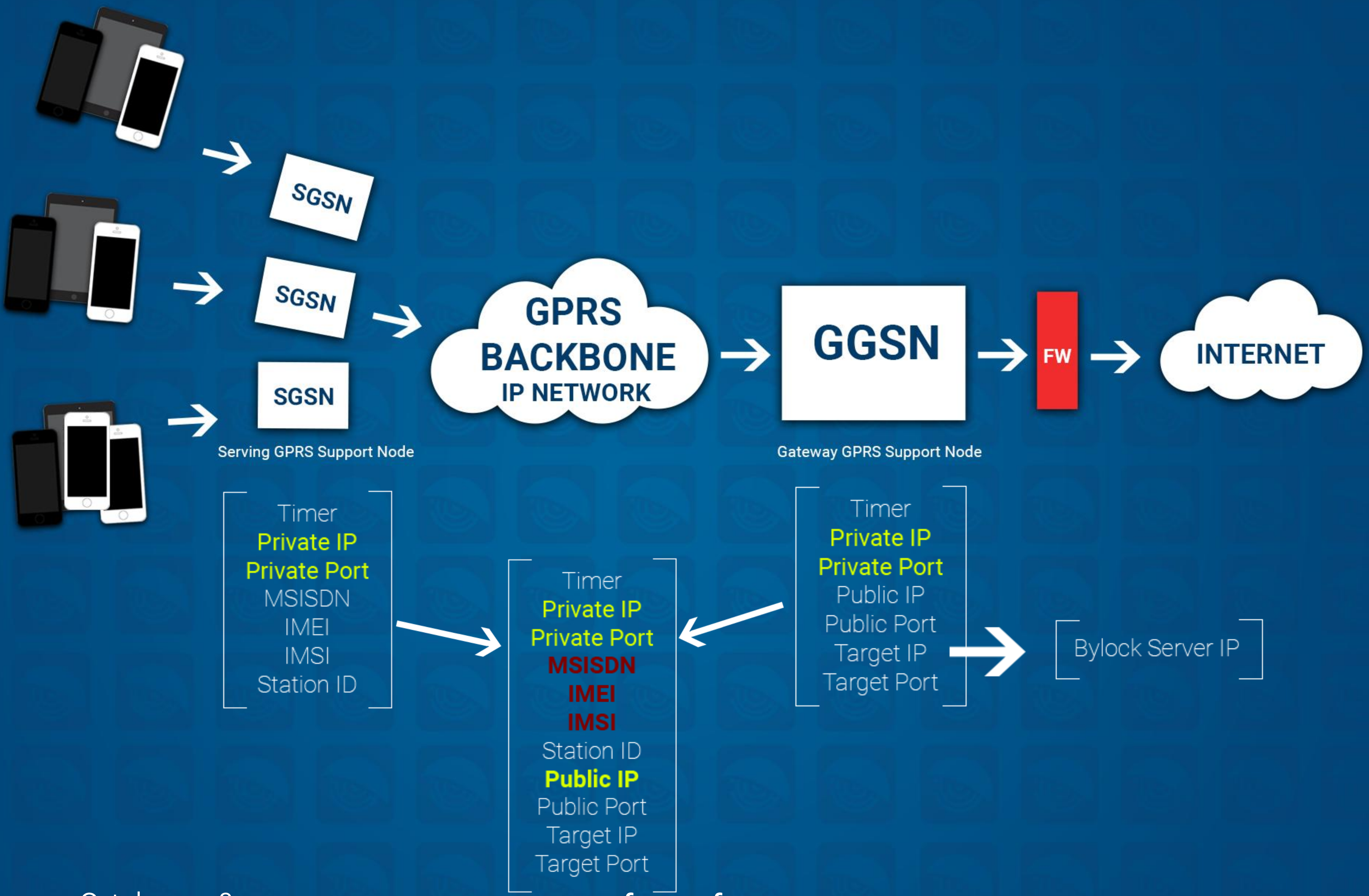
Private Investigators

KOM

Organized Crime Department of Law Enforcement

BTK

Information and Communication Technologies Authority



SGSN

SGSN

SGSN

Serving GPRS Support Node

GPRS
BACKBONE
IP NETWORK

GGSN

Gateway GPRS Support Node

FW

INTERNET

Timer
Private IP
Private Port
MSISDN
IMEI
IMSI
Station ID

Timer
Private IP
Private Port
MSISDN
IMEI
IMSI
Station ID
Public IP
Public Port
Target IP
Target Port

Timer
Private IP
Private Port
Public IP
Public Port
Target IP
Target Port

Bylock Server IP

Keyword List

ByLock Keyword List

- More than 100 words
- Sample Words
  - 46.166.164.137
  - 46.166.164.176
  - 46.166.164.177
  - 46.166.164.178
  - 46.166.164.179
  - 46.166.164.180
  - 46.166.164.181
  - 46.166.164.182
  - 46.166.164.183
  - ByLock.net
  - Bylock++
  - Bylock/net
  - Net.client.by.lock
  - Maindata.db
  - ***More than 100 words***

General Keyword List

- More than 100 words
- Sample Words
- ByLock Keyword List +
- Instant Messaging List
  - ➢ Eagle (…)
  - ➢ Viber
  - ➢ Other apps…
- FETO Investigative Words
  - ➢ People Names
  - ➢ Jargon

Issues

- **Worlds single biggest investigation ever**

- There needs to be full coordination between all organizations
- One organization finds evidence from ByLock Servers, another one finds different evidence from logs, ISP's support with their evidence data, other organizations actually perform investigation and analysis
- Enormous budget (Tens of millions dollars) has been spent and there will be more
- 2-3 more years planned ongoing investigation and analysis

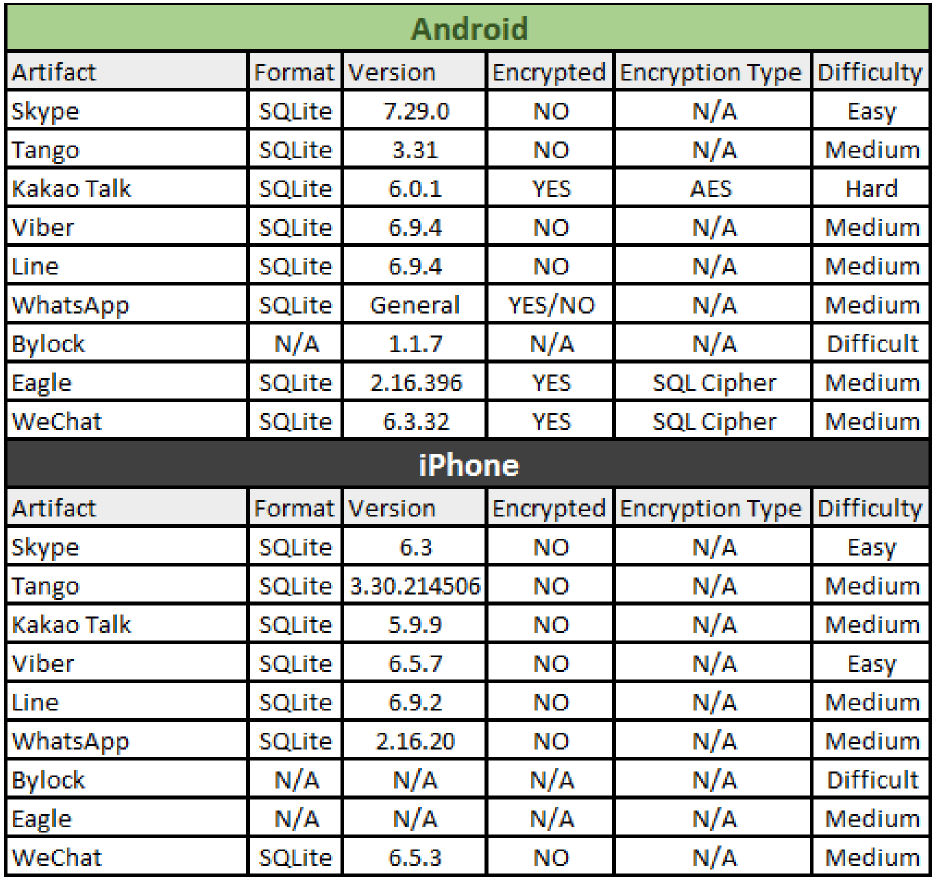
- What is more important? Evidence collection or evidence analysis?
- Digital forensics tool selection is critical since they come with licenses with time periods!
- Scope increased from **~430.000** devices to **1.600.000** devices

- **ByLock** and **Eagle** mobile IM applications become **critical** points in investigation

Thanks

ibrahimsaruhan@gmail.com

FETO Instant Messaging Applications



Android

Artifact	Format	Version	Encrypted	Encryption Type	Difficulty
Skype	SQLite	7.29.0	NO	N/A	Easy
Tango	SQLite	3.31	NO	N/A	Medium
Kakao Talk	SQLite	6.0.1	YES	AES	Hard
Viber	SQLite	6.9.4	NO	N/A	Medium
Line	SQLite	6.9.4	NO	N/A	Medium
WhatsApp	SQLite	General	YES/NO	N/A	Medium
Bylock	N/A	1.1.7	N/A	N/A	Difficult
Eagle	SQLite	2.16.396	YES	SQL Cipher	Medium
WeChat	SQLite	6.3.32	YES	SQL Cipher	Medium

iPhone

Artifact	Format	Version	Encrypted	Encryption Type	Difficulty
Skype	SQLite	6.3	NO	N/A	Easy
Tango	SQLite	3.30.214506	NO	N/A	Medium
Kakao Talk	SQLite	5.9.9	NO	N/A	Medium
Viber	SQLite	6.5.7	NO	N/A	Easy
Line	SQLite	6.9.2	NO	N/A	Medium
WhatsApp	SQLite	2.16.20	NO	N/A	Medium
Bylock	N/A	N/A	N/A	N/A	Difficult
Eagle	N/A	N/A	N/A	N/A	Medium
WeChat	SQLite	6.5.3	NO	N/A	Medium

Eagle

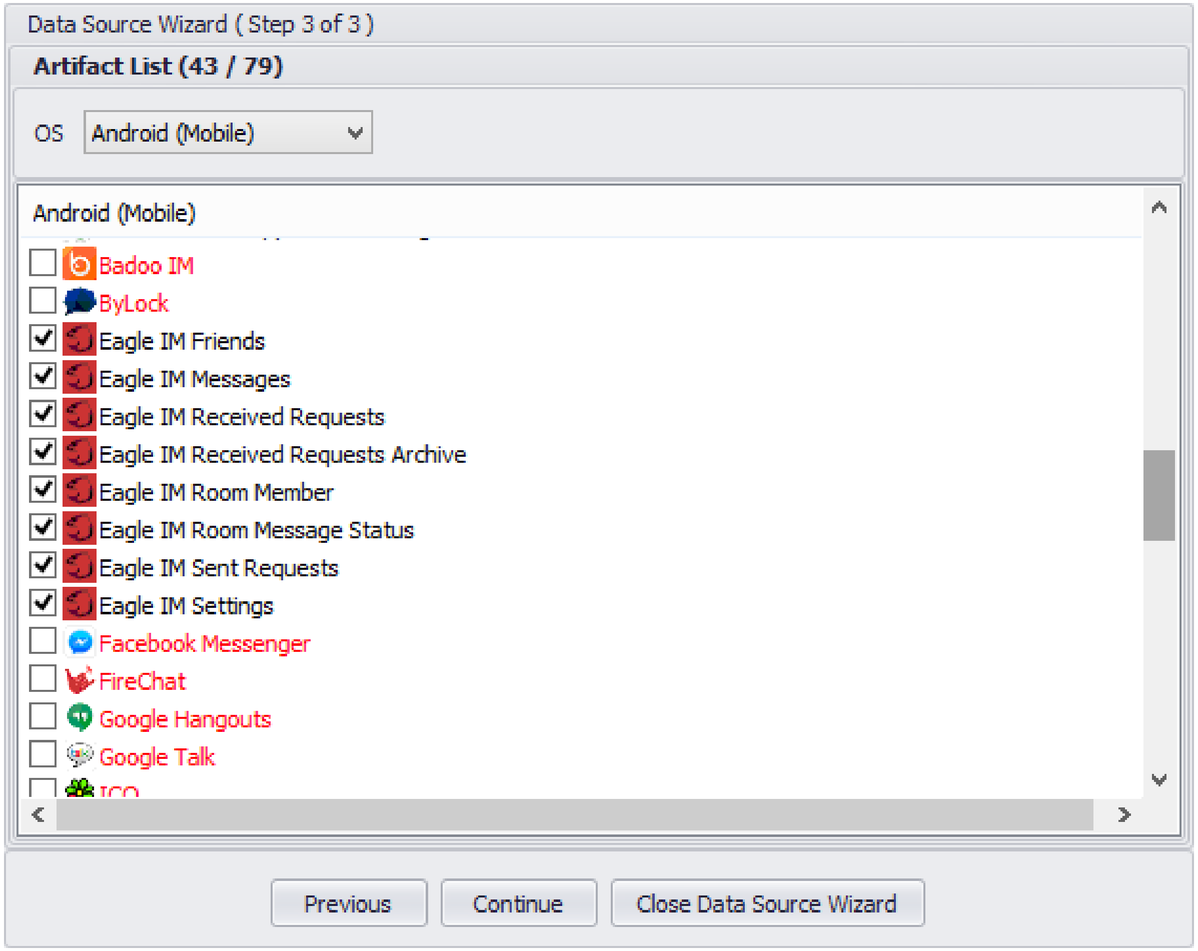
- Seems to be the most critical mobile IM application in FETO Investigation
- Creates random username, no option for selection
- When someone signs up, she will enter password and PIN code

- If left for 3 minutes application will ask for the PIN code
- If left for more than 30 minutes application will ask for the password

- Eagle will use password to encrypt the database artifact file, hence artifact is encrypted
- Seems to have inherent antiforensics capabilities
- UserID and secret are used together to start a session between 2 people

- For Eagle, 10.000-12.000 downloads is performed online (500.000 for ByLock)
- Download count might not indicate actual installation count as people can share APK

Eagle



Data Source Wizard (Step 3 of 3)

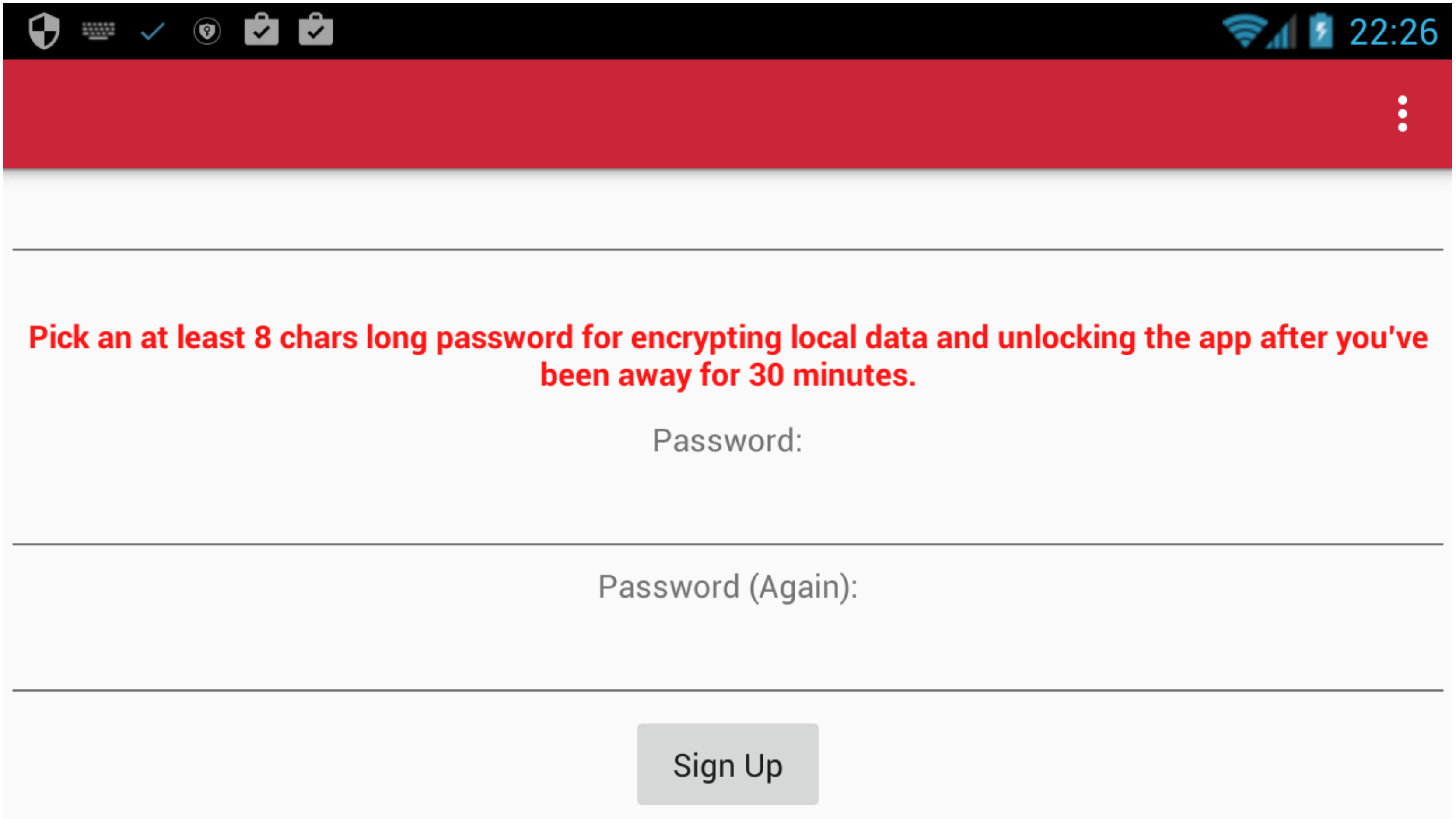
Artifact List (43 / 79)

OS: Android (Mobile)

Android (Mobile)

- □ Badoo IM
- □ ByLock
- ☑ Eagle IM Friends
- ☑ Eagle IM Messages
- ☑ Eagle IM Received Requests
- ☑ Eagle IM Received Requests Archive
- ☑ Eagle IM Room Member
- ☑ Eagle IM Room Message Status
- ☑ Eagle IM Sent Requests
- ☑ Eagle IM Settings
- □ Facebook Messenger
- □ FireChat
- □ Google Hangouts
- □ Google Talk
- □ ICQ

Password Page

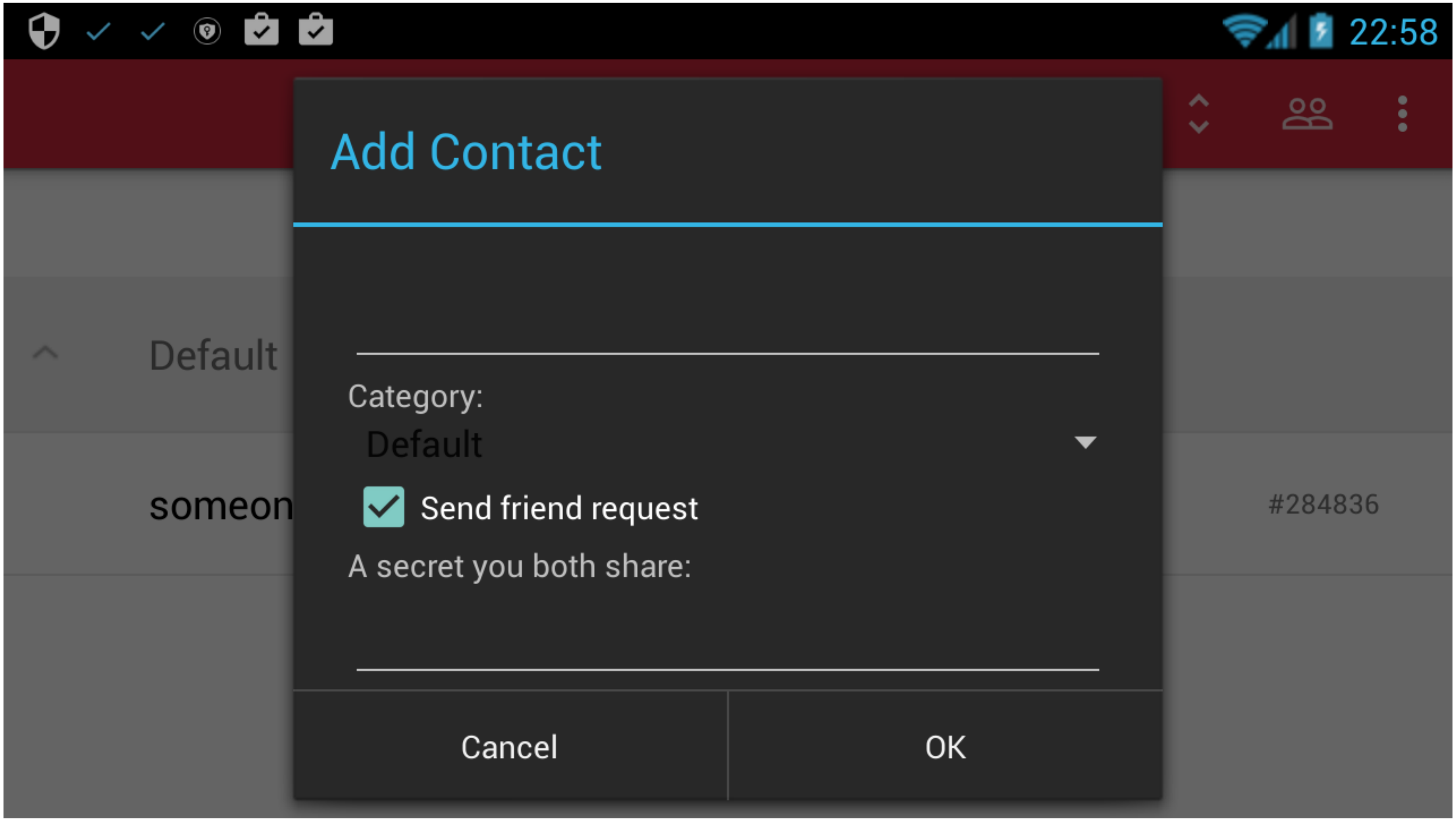


Pick an at least 8 chars long password for encrypting local data and unlocking the app after you've been away for 30 minutes.

Password:

Password (Again):

Authentication (Secret between User and Contact)



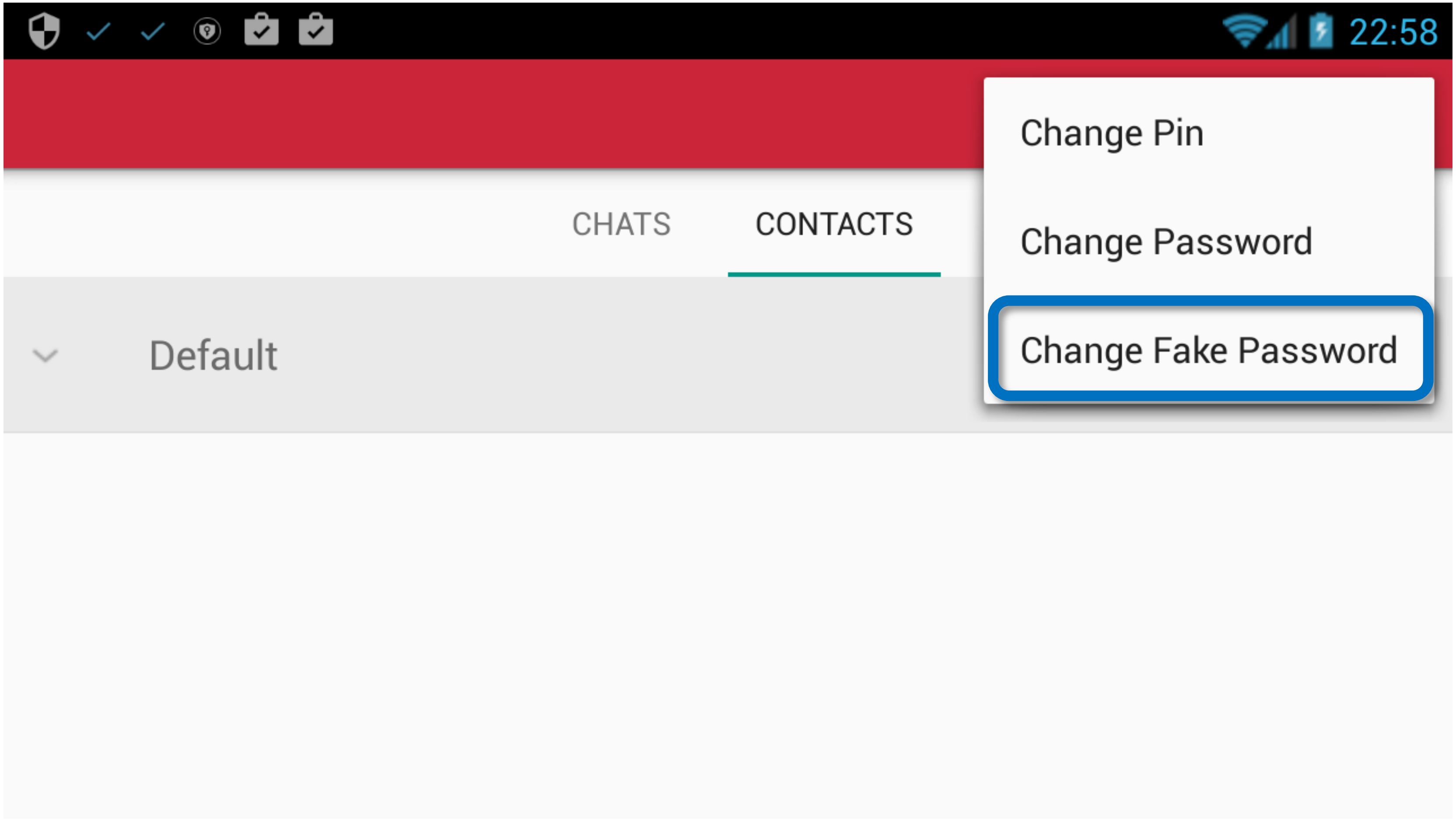
Add Contact

Category:
Default

☑ Send friend request

A secret you both share:

Security Options



22:58

CHATS

CONTACTS

Default

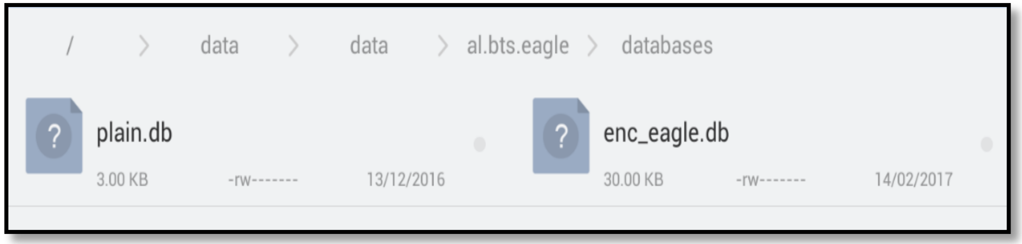
Change Pin

Change Password

Change Fake Password

Eagle Analysis

- Examining "databases" directory shows that Eagle IM uses two files:



/ > data > data > al.bts.eagle > databases

plain.db
3.00 KB -rw------- 13/12/2016

enc_eagle.db
30.00 KB -rw------- 14/02/2017

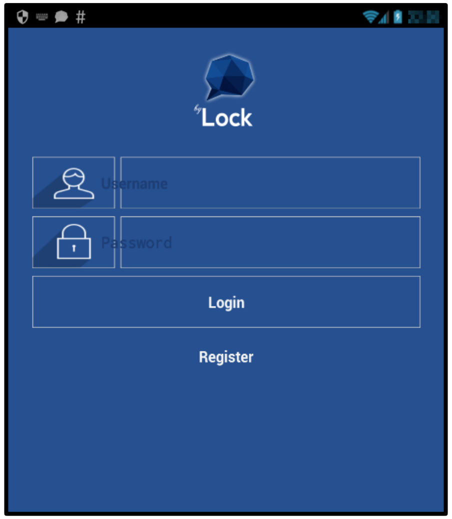
- **plain.db**: SQLite database file which contains one empty table that doesn't contain chat history
- **enc_eagle.db**: SQLite database tools do not open it (Its name indicates that this file might be encrypted)
- After analysis it become clear Eagle is using SQLCipher library, open source extension to SQLite which provides transparent 256-bit AES encryption for database files

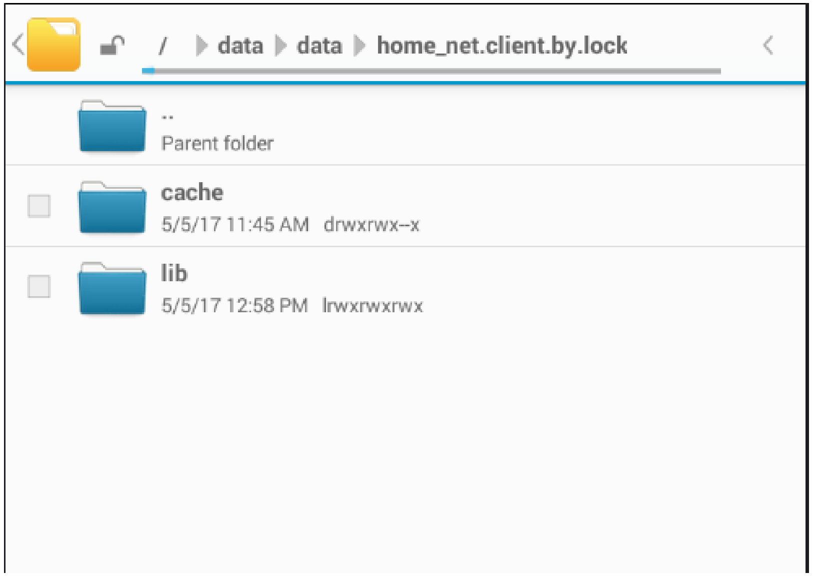
Why ByLock

- According to MIT (CIA of Turkey) ByLock IM application is used solely by FETO
- ByLock communication is encrypted
- ByLock doesn’t have commercial or corporate goals
- ByLock does not use phone numbers
- ByLock provides anonymity
- Content of most chat messages found at databases on ByLock servers shows activity related to FETO
- There are turkish words both on IM application and Server code

- **ByLock = Affiliation with an armed terrorist organization = 6 Years 3 months in Prison**

ByLock



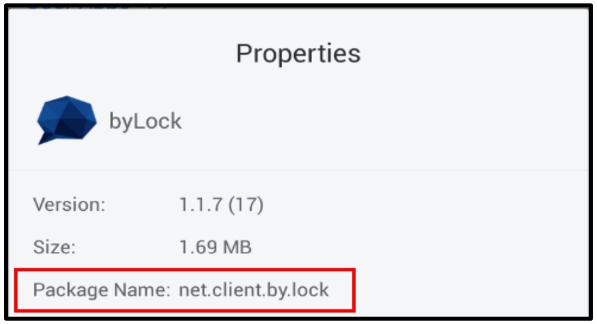


/ data data home_net.client.by.lock

..
Parent folder

cache
5/5/17 11:45 AM drwxrwx--x

lib
5/5/17 12:58 PM lrwxrwxrwx



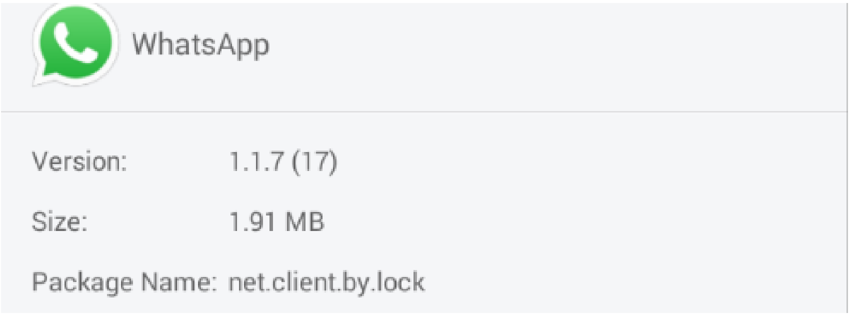
Properties

byLock

Version: 1.1.7 (17)

Size: 1.69 MB

Package Name: net.client.by.lock



WhatsApp

Version: 1.1.7 (17)

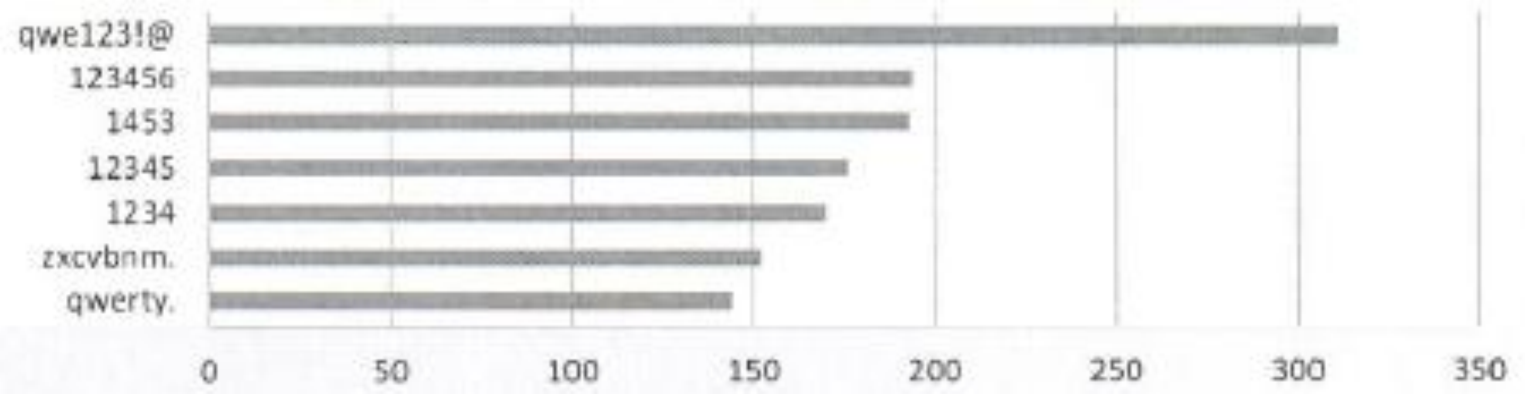
Size: 1.91 MB

Package Name: net.client.by.lock

Statistics from ByLock Server Database

Finding	Count
Registered Users	215.092
Users whose Password is decrypted	184.298
Groups	31.886
Chat Messages	17.169.632
Decrypted Chat Messages	15.520.552
E-mail Messages	3.158.388
Decrypted E-mail Messages	2.293.518
Users sent/received at least 1 message	60.473
Voice Communication Users	78.165
Only Voice Communication Users	46.799

Passwords from ByLock Server Database



Never ending Story

FORENSAFE

- Later ‘t become clear that some advertisement applications are actually connecting bylock.net before February 2016
- Checking only IP's without actual messages become part of investigation

Example Applications

- Best Free Music
  - Active date : 18.08.2014
  - Downloads : 100.000-500.000
- Mor German English Dictionary
  - Active date : 12.07.2014
  - Downloads : 10.000-50.000
- Freezy Play Free Music Online
  - Active date : 30.06.2014
  - Downloads : 10.000-50.000

Thanks

ibrahimsaruhan@gmail.com