Laboratorij za sigurnost i forenzičku analizu informacijsko-komunikacijskog sustava

Sveučilište u Zagrebu
Fakultet prometnih znanosti

Doc. dr. sc. Ivan Cvitić

Područja rada Laboratorija

- Sigurnost informacijsko-komunikacijskog sustava
  - mrežna sigurnost
  - sigurnost uređaja (mobilnih/nosivih/IoT)
- Forenzička analiza informacijsko- komunikacijskog sustava
  - mrežna forenzika
  - forenzika uređaja (mobilnih/nosivih/IoT)

O laboratoriju

- izvođenje nastave i vježbi za kolegije na smjeru
- izrada završnih i diplomskih radova
- znanstvena istraživanja
- dostupna oprema za eksperimentiranje u izoliranom okruženju

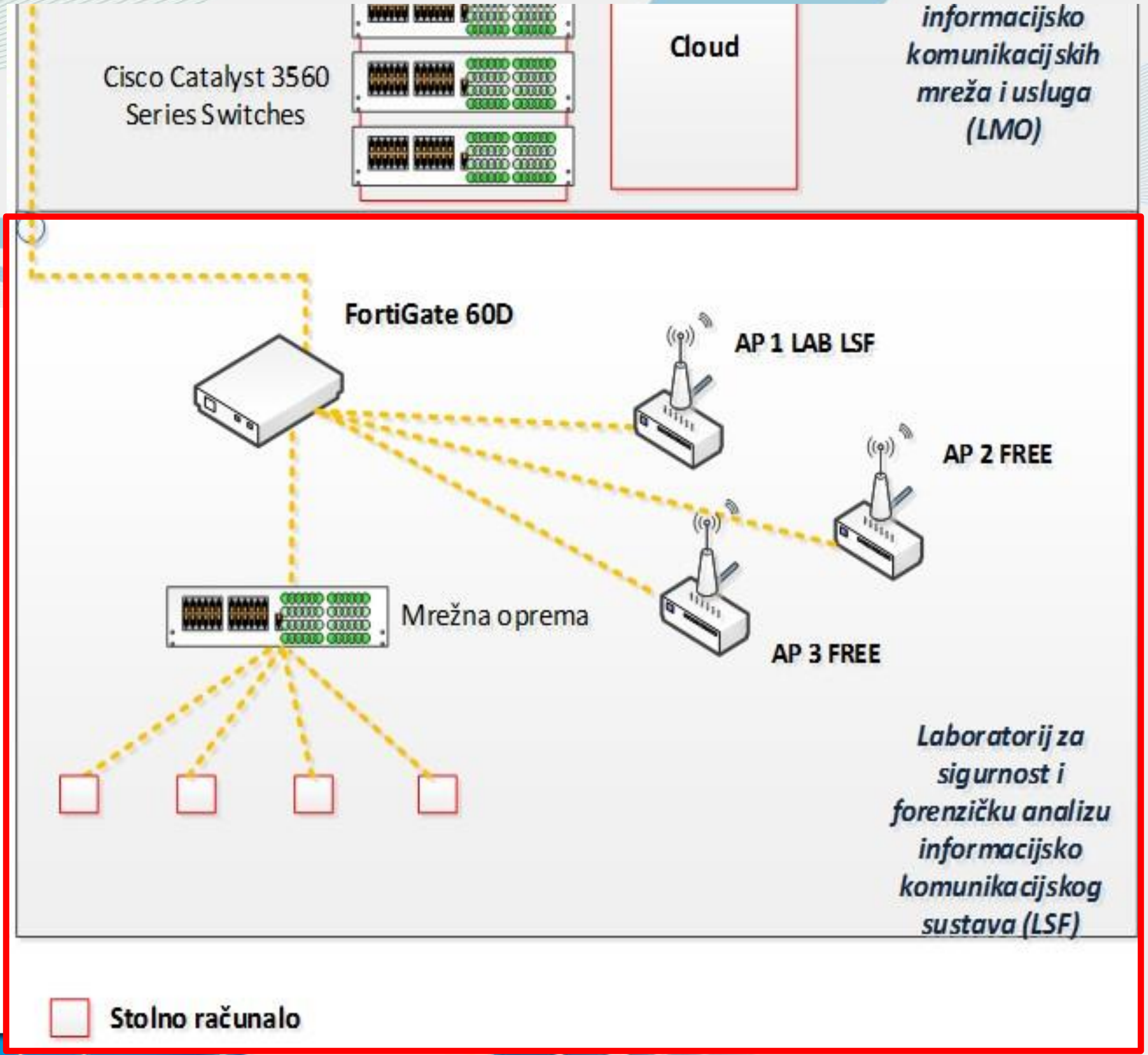
Opremljenost laboratorija

- **FortiGate 60D i FortiAP 221C**
- **Aktivna mrežna oprema**

- **Cellebrite UFED Touch 2**
- **SPF Pro mobile forensics**

- **pokretne i nepokretne radne stanice**
- **tablet računala, pametni telefoni**
- **IoT i nosivi uređaji**

Topologija i lokacija



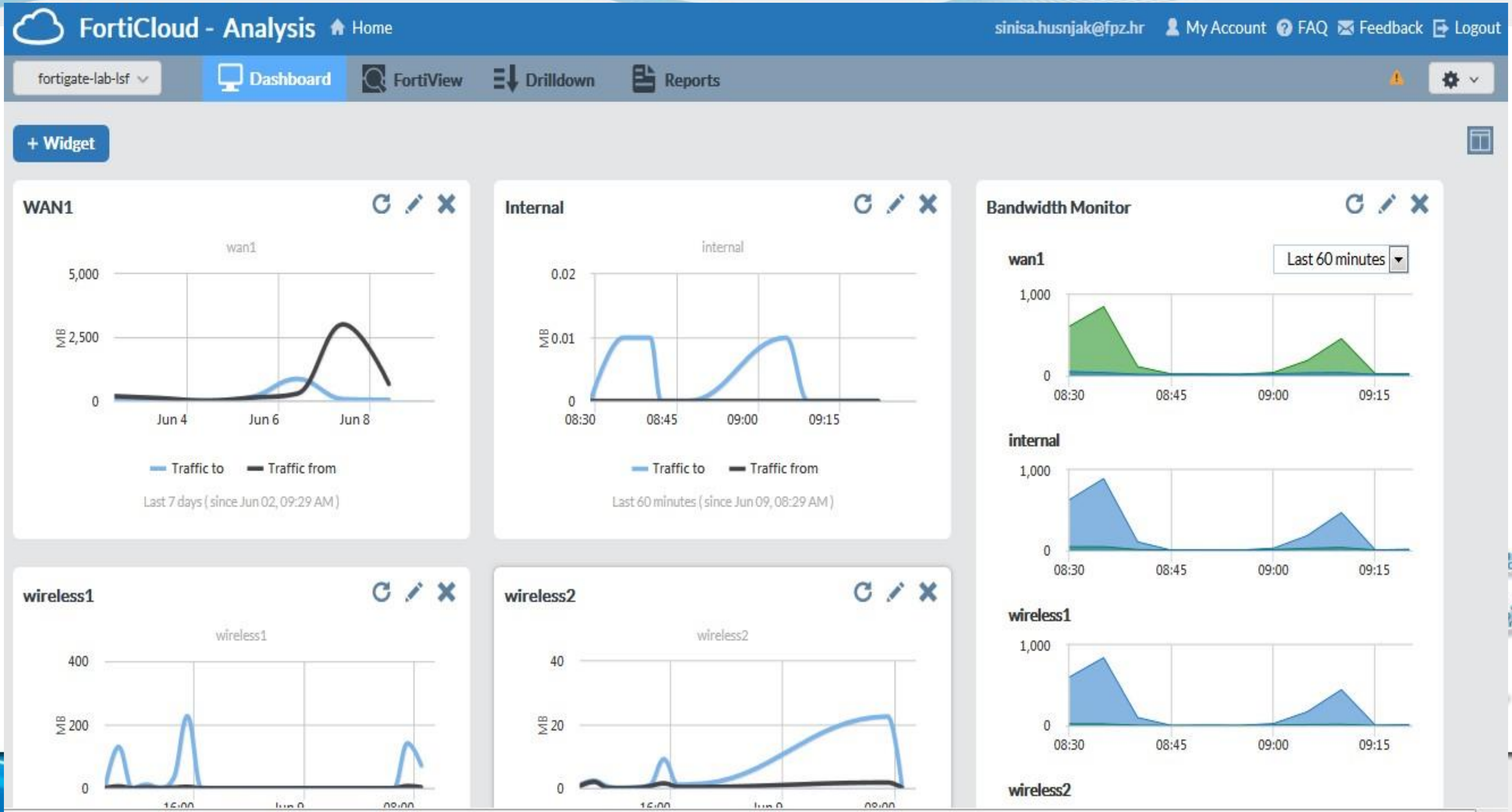
FortiGate 60D

- sigurnost, zaštita i forenzička analiza mrežnog informacijsko-komunikacijskog prometa
- vatrozid, kontrola aplikativnih paketa
- virtualne privatne mreže
- filtriranje web sadržaja
- upravljanje pristupom i sigurnosnim politikama (BYOD)

FortiAP 221C

- sigurnosna testiranja, zaštitu i forenzička analizu informacijsko komunikacijskog prometa
- siguran pristup Wi-Fi mreži temeljen na identitetima
- dubinska (L7) analiza za preciznu kontrolu aplikacija
- identifikacija gostujućih Wi-Fi pristupa
- središnje upravljanje

FortiCloud

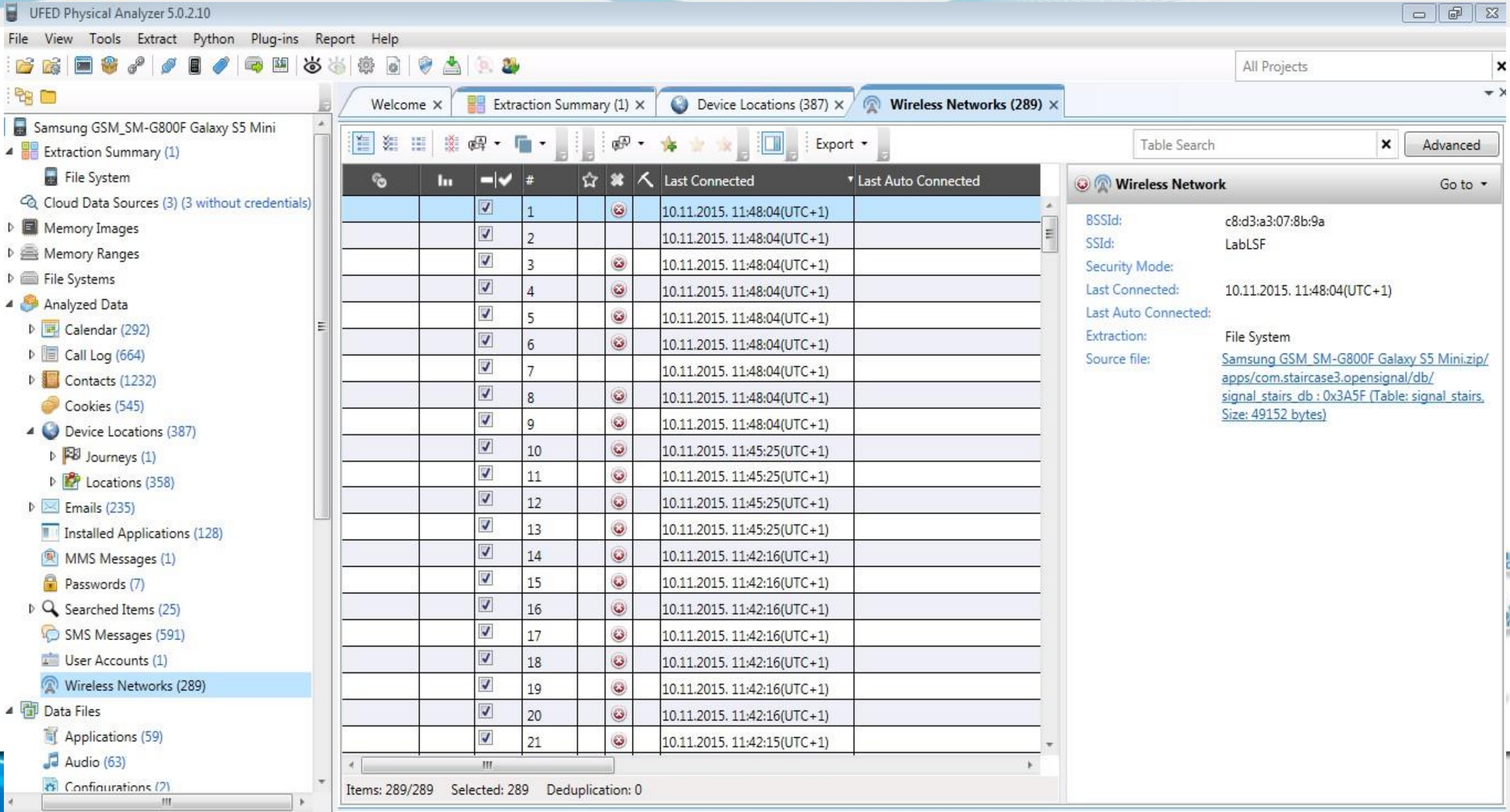


FortiCloud - Analysis
Home
sinisa.husnjak@fpz.hr
My Account
FAQ
Feedback
Logout
fortigate-lab-lsf
Dashboard
FortiView
Drilldown
Reports
+ Widget
WAN1
wan1
5,000
MB 2,500
0
Jun 4
Jun 6
Jun 8
Traffic to
Traffic from
Last 7 days (since Jun 02, 09:29 AM)
Internal
internal
0.02
MB 0.01
0
08:30
08:45
09:00
09:15
Traffic to
Traffic from
Last 60 minutes (since Jun 09, 08:29 AM)
Bandwidth Monitor
wan1
Last 60 minutes
1,000
0
08:30
08:45
09:00
09:15
internal
1,000
0
08:30
08:45
09:00
09:15
wireless1
1,000
0
08:30
08:45
09:00
09:15
wireless2
wireless1
wireless1
400
MB 200
0
16:00
Jun 9
08:00
wireless2
wireless2
40
MB 20
0
16:00
Jun 9
08:00

Cellebrite UFED Touch 2

- forenzička analiza mobilnih uređaja
- ekstrakcija, dekodiranje, analiza i izvještavanje o podacima na mobilnim uređajima
- fizička, logička, datotečna ekstrakcija podataka
- Smartphone uređaji, prijenosnih GPS uređaji, tablet uređaji, *chineset* uređaji, dronovi
- UFED Physical Analyzer, UFED Phone detective, UFED Reader

Cellebrite Physical Analyser



Samsung GSM_SM-G800F Galaxy S5 Mini
- Extraction Summary (1)
  - File System
- Cloud Data Sources (3) (3 without credentials)
- Memory Images
- Memory Ranges
- File Systems
- Analyzed Data
  - Calendar (292)
  - Call Log (664)
  - Contacts (1232)
  - Cookies (545)
  - Device Locations (387)
    - Journeys (1)
    - Locations (358)
  - Emails (235)
  - Installed Applications (128)
  - MMS Messages (1)
  - Passwords (7)
  - Searched Items (25)
  - SMS Messages (591)
  - User Accounts (1)
  - Wireless Networks (289)
- Data Files
  - Applications (59)
  - Audio (63)
  - Configurations (2)

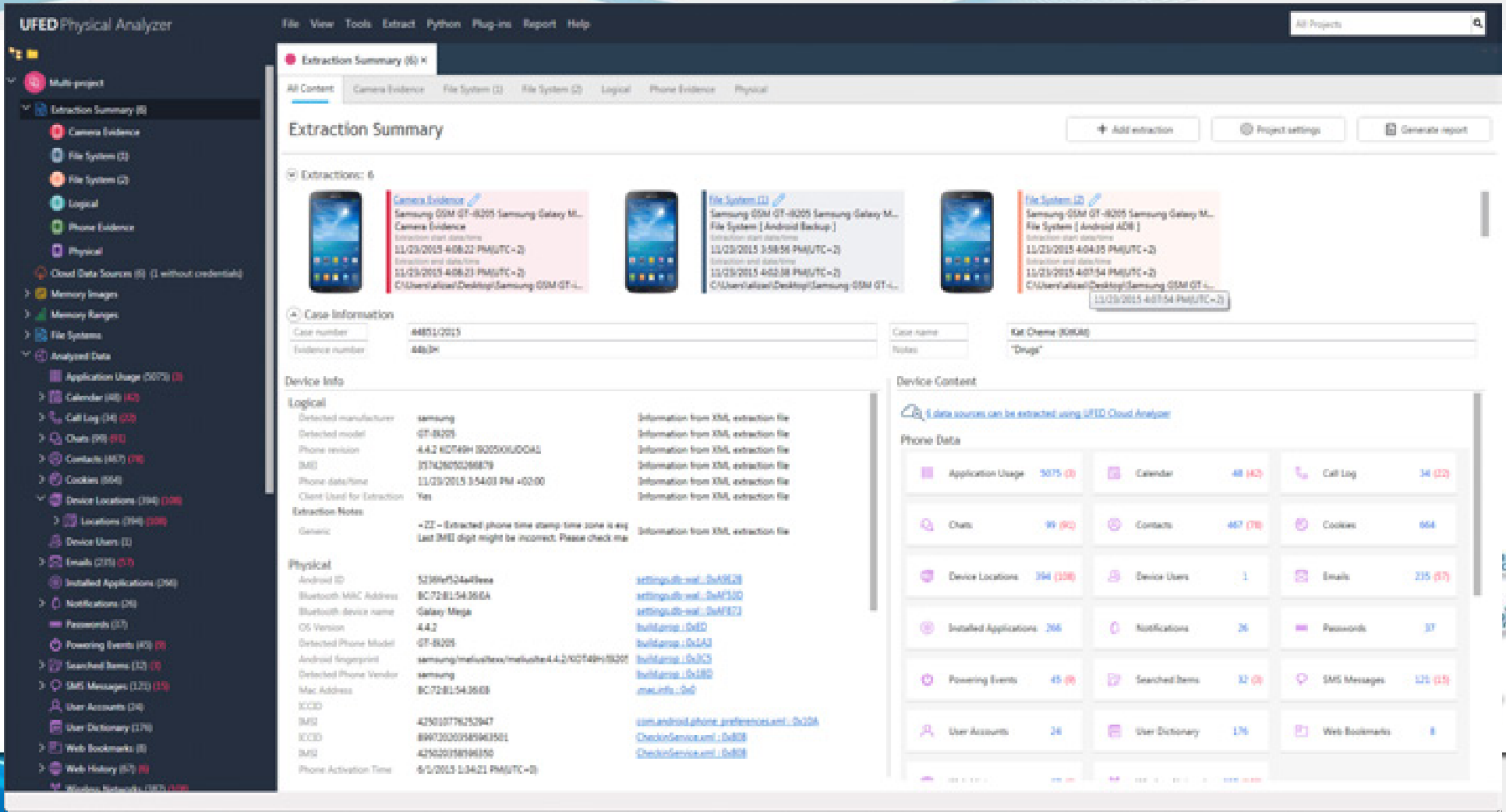
			#	☆	✖		Last Connected	Last Auto Connected
		☑	1		⊗		10.11.2015. 11:48:04(UTC+1)	
		☑	2				10.11.2015. 11:48:04(UTC+1)	
		☑	3		⊗		10.11.2015. 11:48:04(UTC+1)	
		☑	4		⊗		10.11.2015. 11:48:04(UTC+1)	
		☑	5		⊗		10.11.2015. 11:48:04(UTC+1)	
		☑	6		⊗		10.11.2015. 11:48:04(UTC+1)	
		☑	7				10.11.2015. 11:48:04(UTC+1)	
		☑	8		⊗		10.11.2015. 11:48:04(UTC+1)	
		☑	9		⊗		10.11.2015. 11:48:04(UTC+1)	
		☑	10		⊗		10.11.2015. 11:45:25(UTC+1)	
		☑	11		⊗		10.11.2015. 11:45:25(UTC+1)	
		☑	12		⊗		10.11.2015. 11:45:25(UTC+1)	
		☑	13		⊗		10.11.2015. 11:45:25(UTC+1)	
		☑	14		⊗		10.11.2015. 11:42:16(UTC+1)	
		☑	15		⊗		10.11.2015. 11:42:16(UTC+1)	
		☑	16		⊗		10.11.2015. 11:42:16(UTC+1)	
		☑	17		⊗		10.11.2015. 11:42:16(UTC+1)	
		☑	18		⊗		10.11.2015. 11:42:16(UTC+1)	
		☑	19		⊗		10.11.2015. 11:42:16(UTC+1)	
		☑	20		⊗		10.11.2015. 11:42:16(UTC+1)	
		☑	21		⊗		10.11.2015. 11:42:15(UTC+1)	

Items: 289/289 Selected: 289 Deduplication: 0

Wireless Network

BSSId:	c8:d3:a3:07:8b:9a
SSId:	LabLSF
Security Mode:	
Last Connected:	10.11.2015. 11:48:04(UTC+1)
Last Auto Connected:	
Extraction:	File System
Source file:	Samsung GSM_SM-G800F Galaxy S5 Mini.zip/apps/com.staircase3.opensignal/db/signal_stairs_db : 0x3A5F (Table: signal_stairs, Size: 49152 bytes)

Cellebrite Physical Analyser



Multi-project
- Extraction Summary (6)
  - Camera Evidence
  - File System (1)
  - File System (2)
  - Logical
  - Phone Evidence
  - Physical
- Cloud Data Sources (6) (1 without credentials)
- Memory Images
- Memory Ranges
- File Systems
- Analyzed Data
  - Application Usage (5075) (3)
  - Calendar (48) (42)
  - Call Log (34) (22)
  - Chats (99) (91)
  - Contacts (467) (78)
  - Cookies (664)
  - Device Locations (394) (108)
    - Locations (394) (108)
  - Device Users (1)
  - Emails (235) (57)
  - Installed Applications (266)
  - Notifications (26)
  - Passwords (37)
  - Powering Events (45) (9)
  - Searched Items (32) (3)
  - SMS Messages (121) (15)
  - User Accounts (24)
  - User Dictionary (176)
  - Web Bookmarks (8)
  - Web History (67) (6)
  - Wireless Networks (387) (108)

Extraction Summary

Extractions: 6

Camera Evidence
Samsung GSM GT-I8205 Samsung Galaxy M...
Camera Evidence
Extraction start date/time
11/23/2015 4:08:22 PM(UTC+2)
Extraction end date/time
11/23/2015 4:08:23 PM(UTC+2)
C:\Users\alizaz\Desktop\Samsung GSM GT-i...

File System (1)
Samsung GSM GT-I8205 Samsung Galaxy M...
File System [Android Backup]
Extraction start date/time
11/23/2015 3:58:56 PM(UTC+2)
Extraction end date/time
11/23/2015 4:02:38 PM(UTC+2)
C:\Users\alizaz\Desktop\Samsung GSM GT-i...

File System (2)
Samsung GSM GT-I8205 Samsung Galaxy M...
File System [Android ADB]
Extraction start date/time
11/23/2015 4:04:25 PM(UTC+2)
Extraction end date/time
11/23/2015 4:07:54 PM(UTC+2)
C:\Users\alizaz\Desktop\Samsung GSM GT-i...
11/23/2015 4:07:54 PM(UTC+2)

Case Information

Case number	#4851/2015	Case name	Kat Cheme (KiKAt)
Evidence number	44b3H	Notes	"Drugs"

Device Info

Logical

Detected manufacturer	samsung	Information from XML extraction file
Detected model	GT-I8205	Information from XML extraction file
Phone revision	4.4.2 KOT49H I8205XXUDOA1	Information from XML extraction file
IMEI	357426050266879	Information from XML extraction file
Phone date/time	11/23/2015 3:54:03 PM +02:00	Information from XML extraction file
Client Used for Extraction	Yes	Information from XML extraction file
Extraction Notes		
Generic	<22 – Extracted phone time stamp time zone is eq Last IMEI digit might be incorrect. Please check me	Information from XML extraction file

Physical

Android ID	5236fef524a4feea	settings.db-wal : 0xA9628
Bluetooth MAC Address	BC:72:B1:54:36:0A	settings.db-wal : 0xAF53D
Bluetooth device name	Galaxy Mega	settings.db-wal : 0xAF873
OS Version	4.4.2	build.prop : 0xED
Detected Phone Model	GT-I8205	build.prop : 0x1A3
Android fingerprint	samsung/meliusltexx/meliuslte:4.4.2/KOT49H/I8205	build.prop : 0x3C5
Detected Phone Vendor	samsung	build.prop : 0x180
Mac Address	BC:72:B1:54:36:0B	.mac.info : 0x0
ICCID		
IMSI	425010776252947	com.android.phone_preferences.xml : 0x10A
ICCID	8997202035859963501	CheckinService.xml : 0x808
IMSI	425020358596350	CheckinService.xml : 0x808
Phone Activation Time	6/1/2013 1:34:21 PM(UTC+0)	

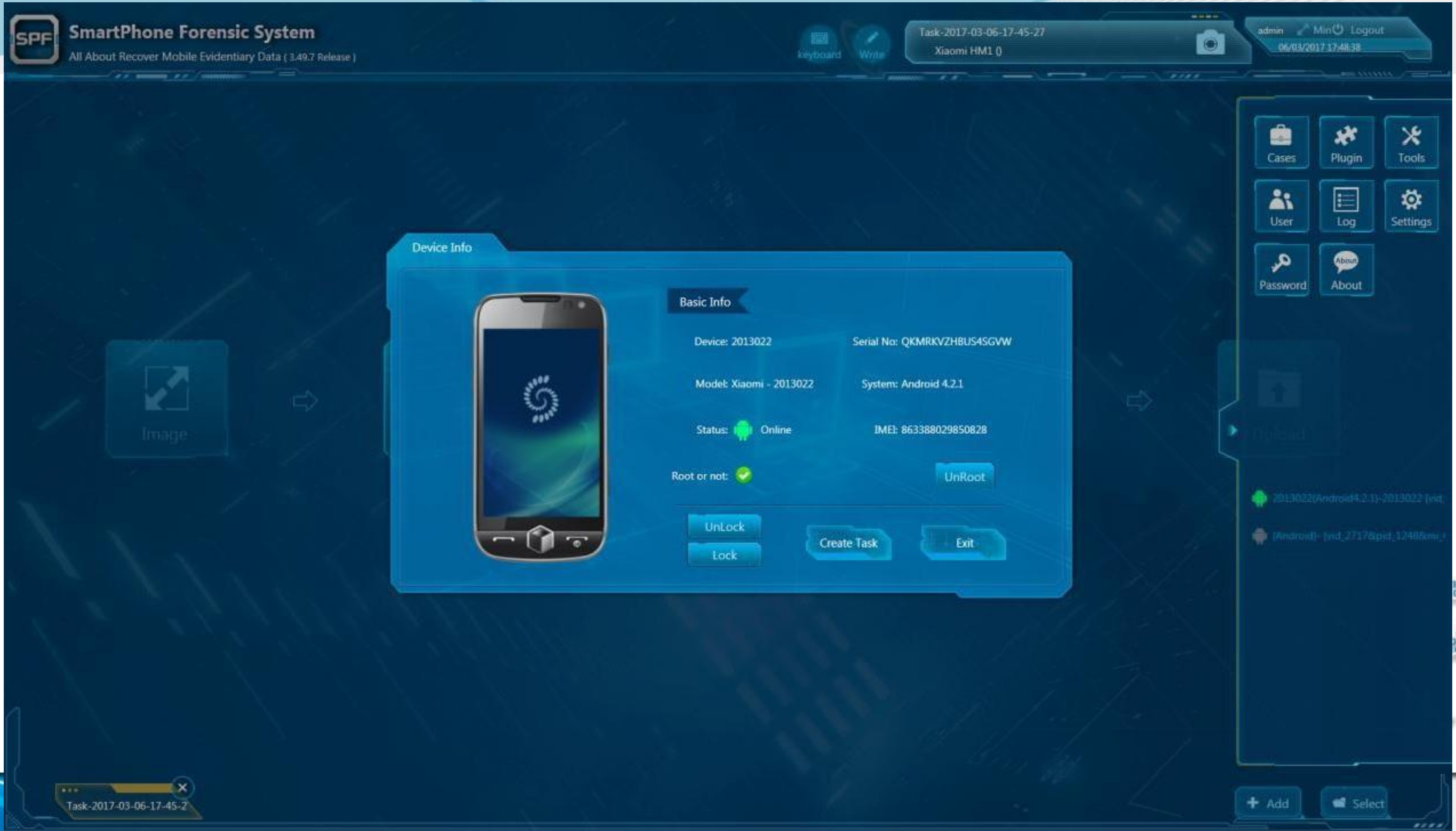
Device Content

6 data sources can be extracted using UFED Cloud Analyzer

Phone Data

Application Usage	5075 (3)	Calendar	48 (42)	Call Log	34 (22)
Chats	99 (91)	Contacts	467 (78)	Cookies	664
Device Locations	394 (108)	Device Users	1	Emails	235 (57)
Installed Applications	266	Notifications	26	Passwords	37
Powering Events	45 (9)	Searched Items	32 (3)	SMS Messages	121 (15)
User Accounts	24	User Dictionary	176	Web Bookmarks	8

SPF Pro



SmartPhone Forensic System

All About Recover Mobile Evidentiary Data (3.49.7 Release)

Task-2017-03-06-17-45-27

Xiaomi HM1 ()

admin

06/03/2017 17:48:38

Device Info

Basic Info

Device: 2013022

Serial No: QKMRKVZHBUS4SGVW

Model: Xiaomi - 2013022

System: Android 4.2.1

Status: Online

IMEI: 863388029850828

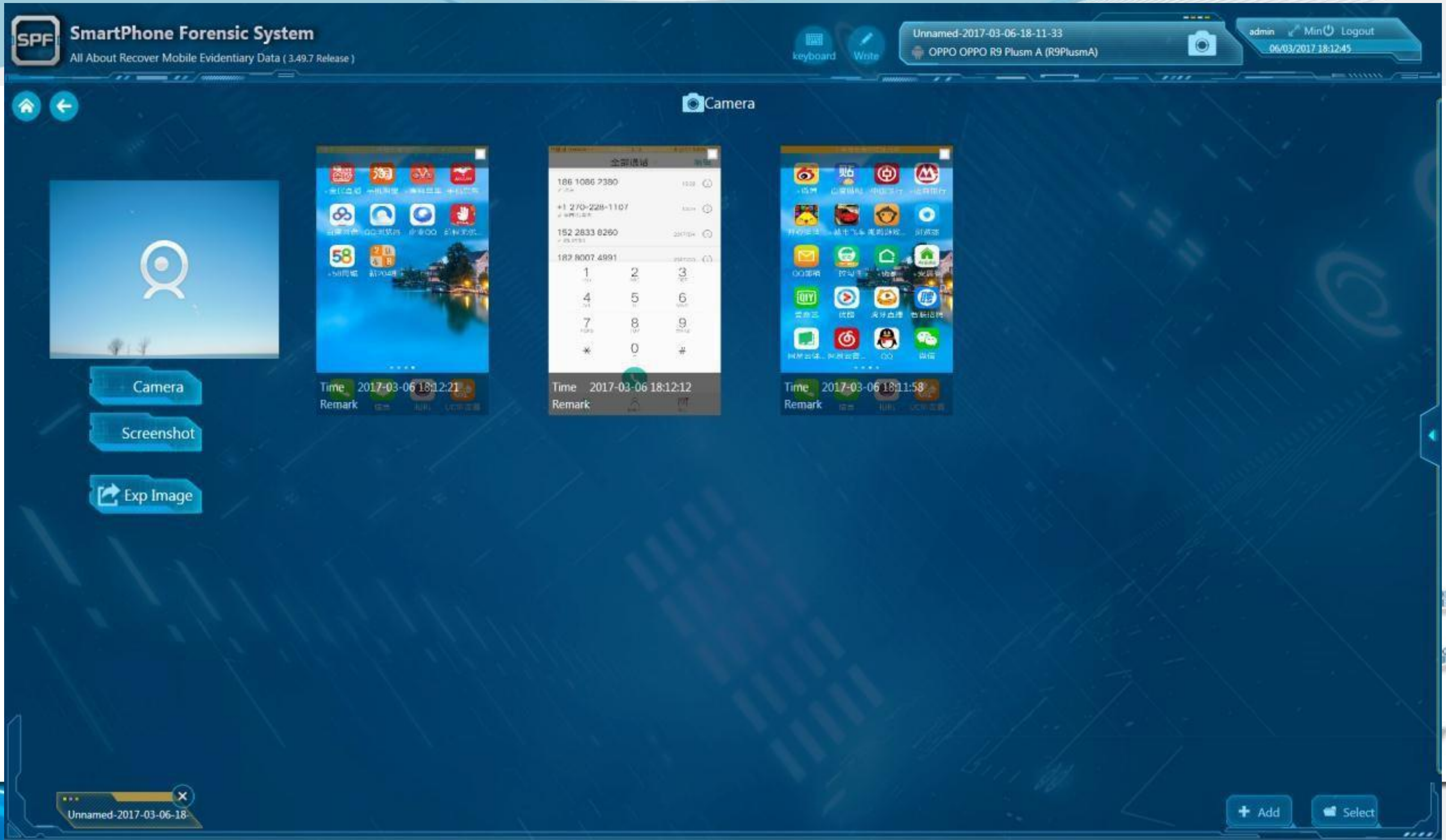
Root or not: ✓

2013022(Android4.2.1)-2013022 (vid_

(Android)- (vid_2717&pid_1248&mi_

Task-2017-03-06-17-45-2

SPF Pro

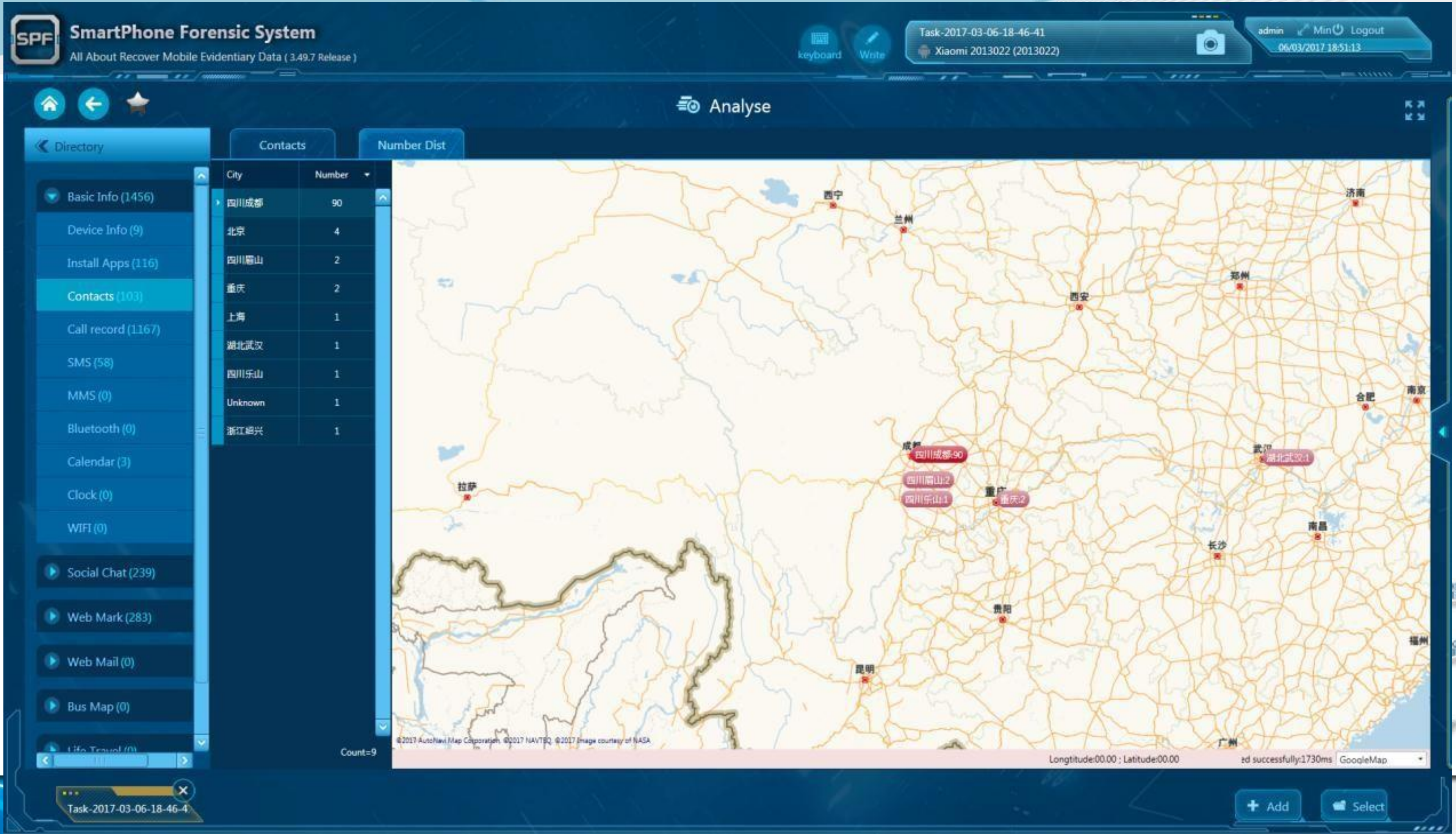


Time 2017-03-06 18:12:21
Remark

Time 2017-03-06 18:12:12
Remark

Time 2017-03-06 18:11:58
Remark

SPF Pro



City	Number
四川成都	90
北京	4
四川眉山	2
重庆	2
上海	1
湖北武汉	1
四川乐山	1
Unknown	1
浙江绍兴	1

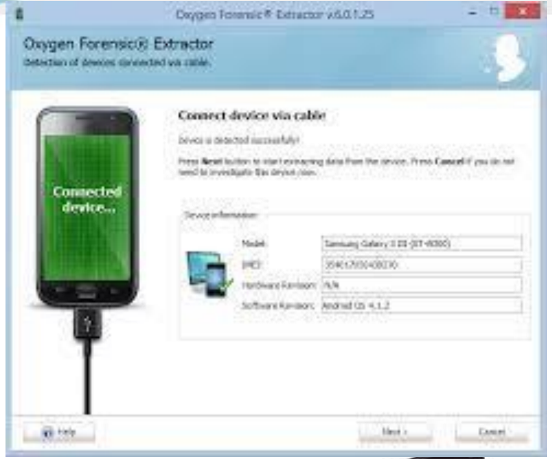
Count=9

©2017 AutoNavi Map Corporation ©2017 NAVTEQ ©2017 Image courtesy of NASA

Nosivi i IoT uređaji

- Mogućnosti primjene
- Generiranje prometa
- Forenzika
- Sigurnost (DDoS)
- Detekcija anomalija

Radne stanice i alati



Oxygen Forensic® Extractor v6.0.1.25

Oxygen Forensic® Extractor

Detection of devices connected via cable.

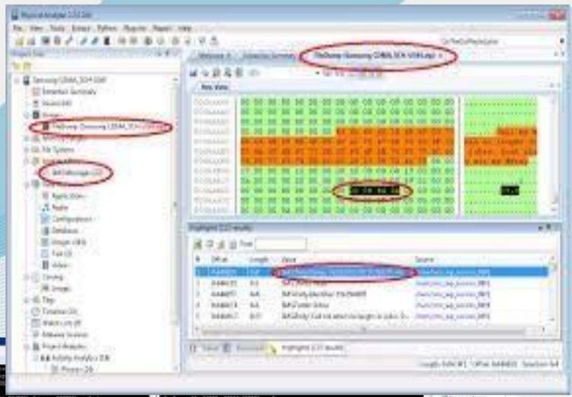
Connect device via cable

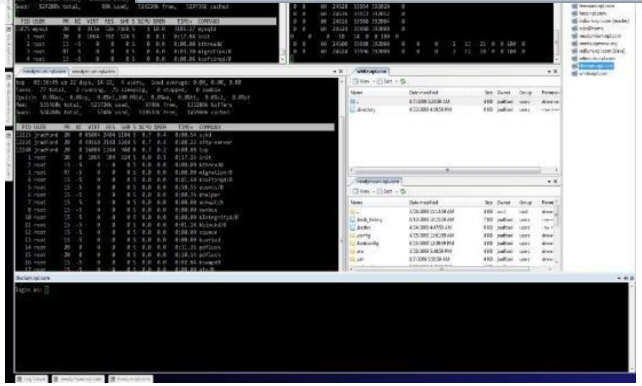
Device is detected successfully!

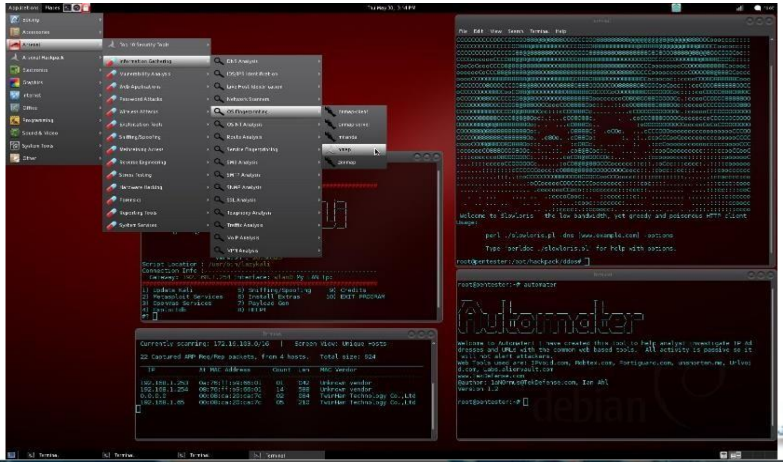
Press **Next** button to start extracting data from the device. Press **Cancel** if you do not need to investigate this device now.

Device information

Model:	Samsung Galaxy S III (GT-I9300)
IMEI:	354017050400230
Hardware Revision:	N/A
Software Revision:	Android OS 4.1.2





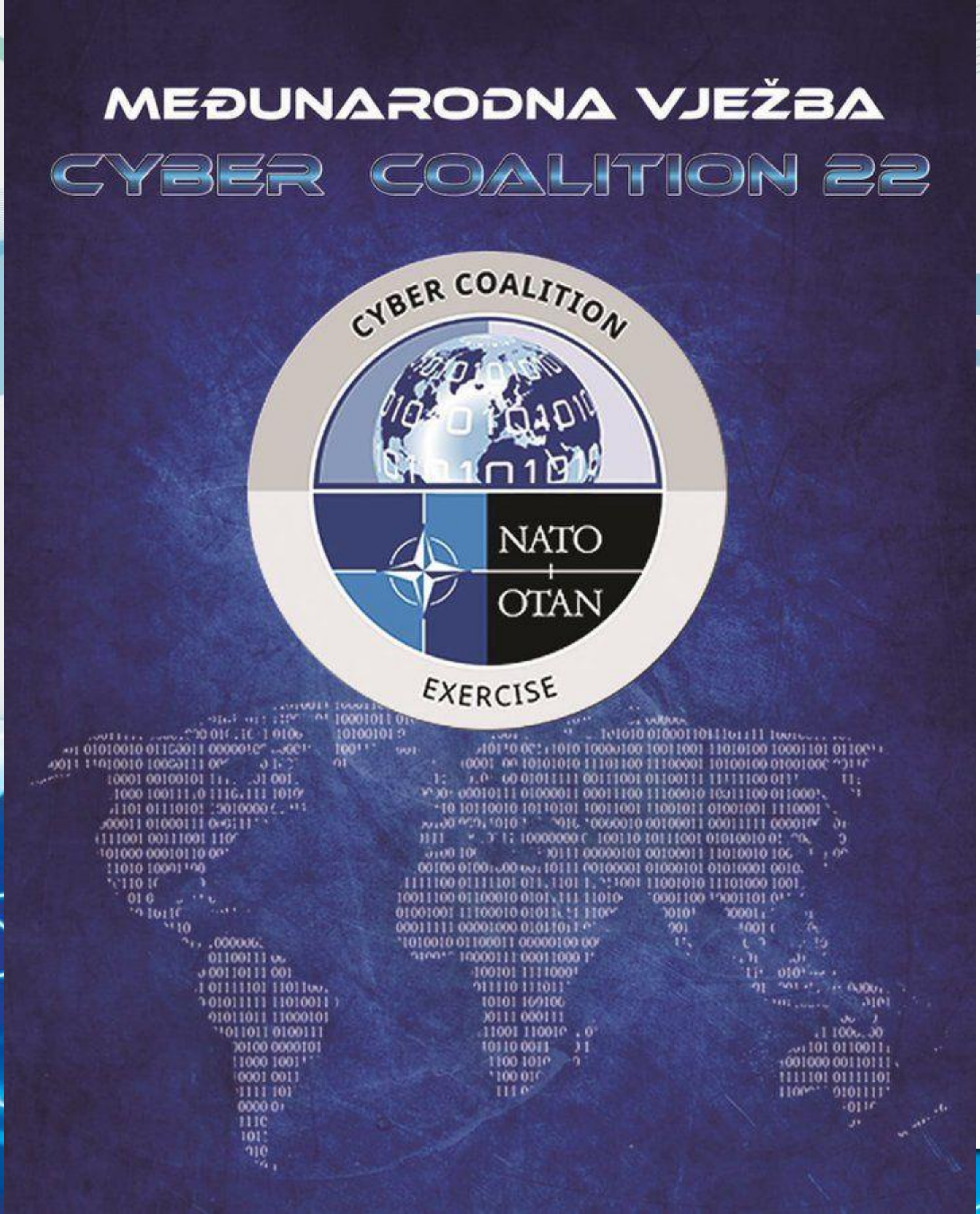


```
Script Location : /usr/bin/lazykali
Connection Info :
  Gateway: 192.168.1.254 Interface: wlan0 My LAN Ip:
1) Update Kali             5) Sniffing/Spoofing     9) Credits
2) Metasploit Services     6) Install Extras       10) EXIT PROGRAM
3) OpenVas Services        7) Payload Gen
4) Exploitdb               8) HELP!
#?
```

```
Currently scanning: 172.16.183.0/16   |   Screen View: Unique Hosts

22 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 924

  IP             At MAC Address     Count   Len   MAC Vendor
192.168.1.253   0a:78:ff:b9:88:01    01     042   Unknown vendor
192.168.1.254   08:70:ff:b9:88:01    14     588   Unknown vendor
0.0.0.0         00:08:ca:28:ca:7c    02     084   TwinHan Technology Co.,Ltd
192.168.1.85    00:08:ca:28:ca:7c    05     210   TwinHan Technology Co.,Ltd
```

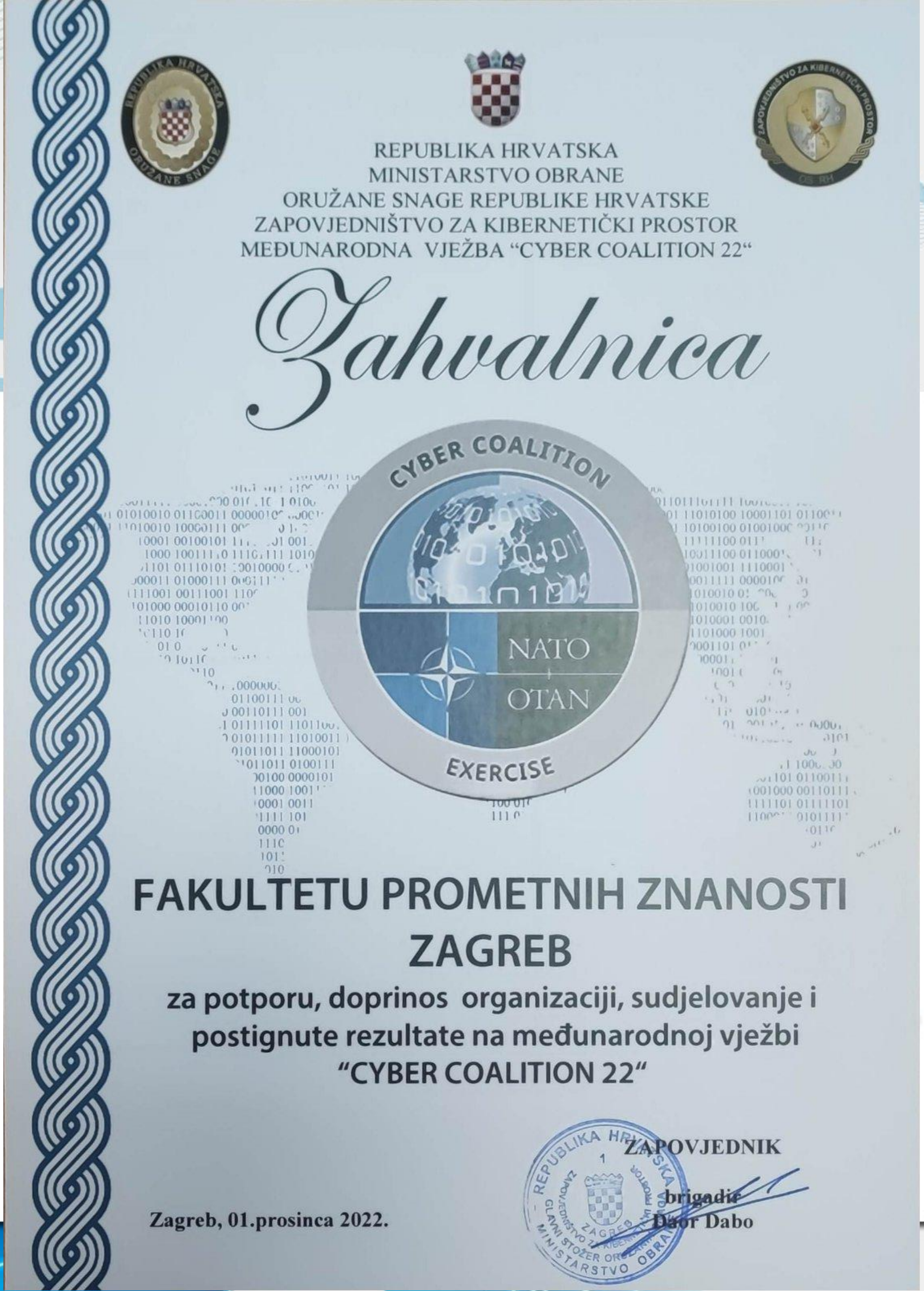
```
Welcome to Slowloris - the low bandwidth, yet greedy and poisonous HTTP client
Usage:

        perl ./slowloris.pl -dns [www.example.com] -options

        Type 'perldoc ./slowloris.pl' for help with options.

root@pentester:/opt/hackpack/ddos#
```

```
root@pentester:~# automater

Automater

Welcome to Automater! I have created this tool to help analyst investigate IP Ad
dresses and URLs with the common web based tools.  All activity is passive so it
 will not alert attackers.
Web Tools used are: IPvoid.com, Robtex.com, Fortiguard.com, unshorten.me, Urlvoi
d.com, Labs.alienvault.com
www.TekDefense.com
@author: 1aN0rmus@TekDefense.com, Ian Ahl
Version 1.2

root@pentester:~#
```



MEĐUNARODNA VJEŽBA

CYBER COALITION 22



REPUBLIKA HRVATSKA
MINISTARSTVO OBRANE
ORUŽANE SNAGE REPUBLIKE HRVATSKE
ZAPOVJEDNIŠTVO ZA KIBERNETIČKI PROSTOR
MEĐUNARODNA VJEŽBA "CYBER COALITION 22"

Zahvalnica

**FAKULTETU PROMETNIH ZNANOSTI
ZAGREB**

**za potporu, doprinos organizaciji, sudjelovanje i
postignute rezultate na međunarodnoj vježbi
"CYBER COALITION 22"**

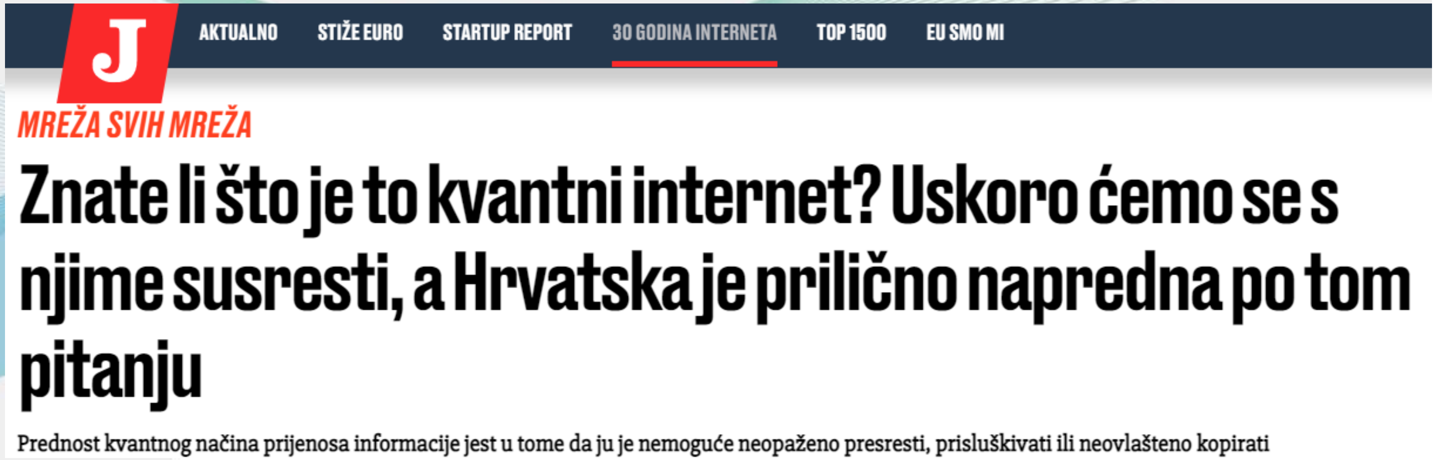
ZAPOVJEDNIK

**brigadir
Daor Dabo**

REPUBLIKA HRVATSKA
1
ZAPOVJEDNIŠTVO ZA KIBERNETIČKI PROSTOR
ZAGREB
GLAVNI STOŽER ORUŽANIH SNAGA
MINISTARSTVO OBRANE

Zagreb, 01.prosinca 2022.

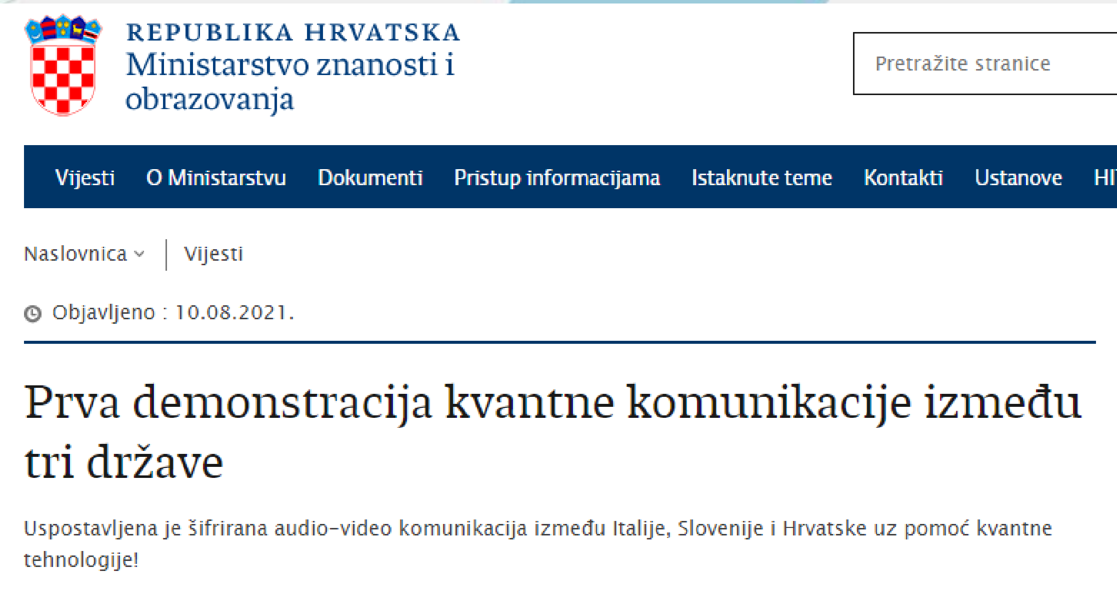
CYBER COALITION
NATO
OTAN
EXERCISE



MREŽA SVIH MREŽA

Znate li što je to kvantni internet? Uskoro ćemo se s njime susresti, a Hrvatska je prilično napredna po tom pitanju

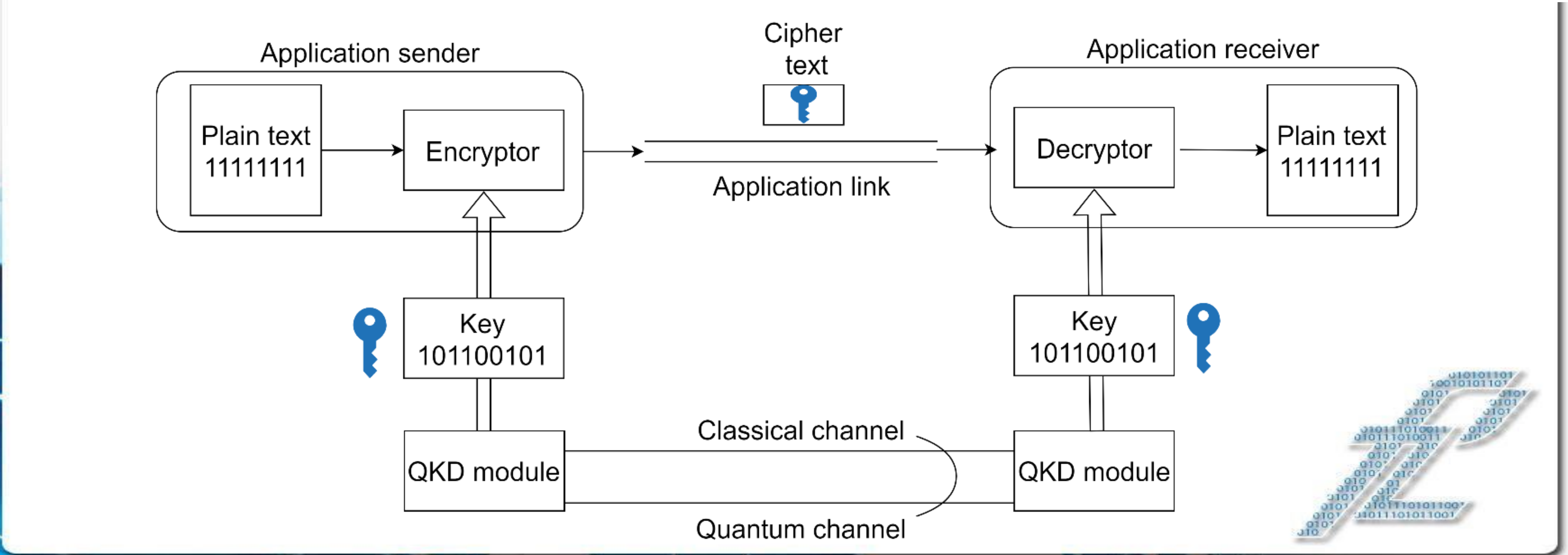
Prednost kvantnog načina prijenosa informacije jest u tome da ju je nemoguće neopaženo presresti, prisluškivati ili neovlašteno kopirati



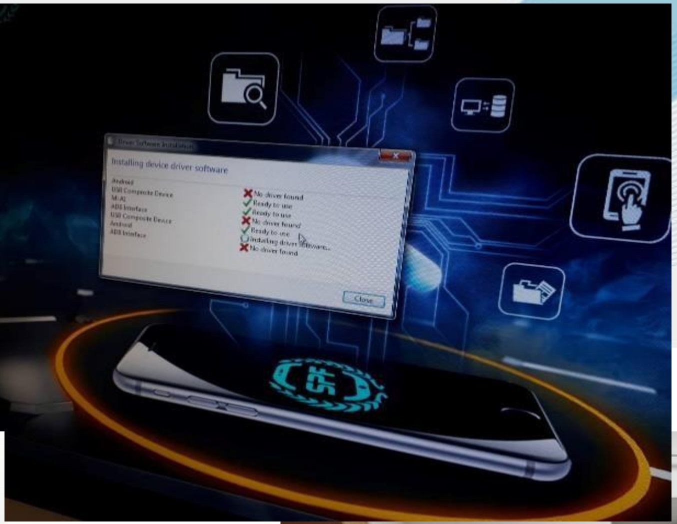
Objavljeno : 10.08.2021.

Prva demonstracija kvantne komunikacije između tri države

Uspostavljena je šifrirana audio-video komunikacija između Italije, Slovenije i Hrvatske uz pomoć kvantne tehnologije!



Laboratorij & studenti



```
Driver Software Installation

Installing device driver software

Android
USB Composite Device      ✗ No driver found
MI A1                     ✓ Ready to use
ADB Interface             ✓ Ready to use
USB Composite Device      ✗ No driver found
Android                   ✓ Ready to use
ADB Interface             ○ Installing driver software...
                          ✗ No driver found

                                        Close
```