

Mobile communications security



Matej Kovačič, (CC) 2017
Jozef Stefan Institute

Part I:
Identity spoofing

CallerID spoofing

The screenshot shows a web browser window displaying the TrixBox administration interface. The browser's address bar shows the URL `192.168.56.101/maint/index.php?`. The page title is "TrixBox [Running] - Oracle VM VirtualBox". The interface includes a "PBX Status" section with the following details:

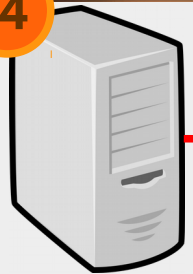
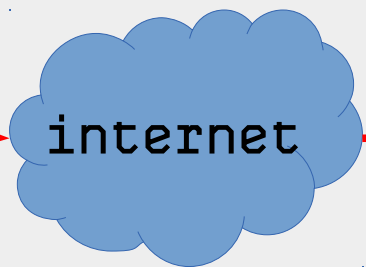
- Version: Asterisk 1.6.0.26-FONCORE-r78 built by...
- Uptime: System uptime: 6 minutes, 9 seconds; Last reload: 6 minutes, 9 seconds
- Active Channel(s): 0 active SIP dialogs
- SIP Peers: 3 sip peers [0 online, 2 offline Unmonitored: 1 online, 0 offline]
- IAX2 Registry: 0 IAX2 registrations.
- IAX2 Peers: 0 iax2 peers [0 online, 0 offline, 0 unmonitored]

Overlaid on the browser is a terminal window showing the following output:

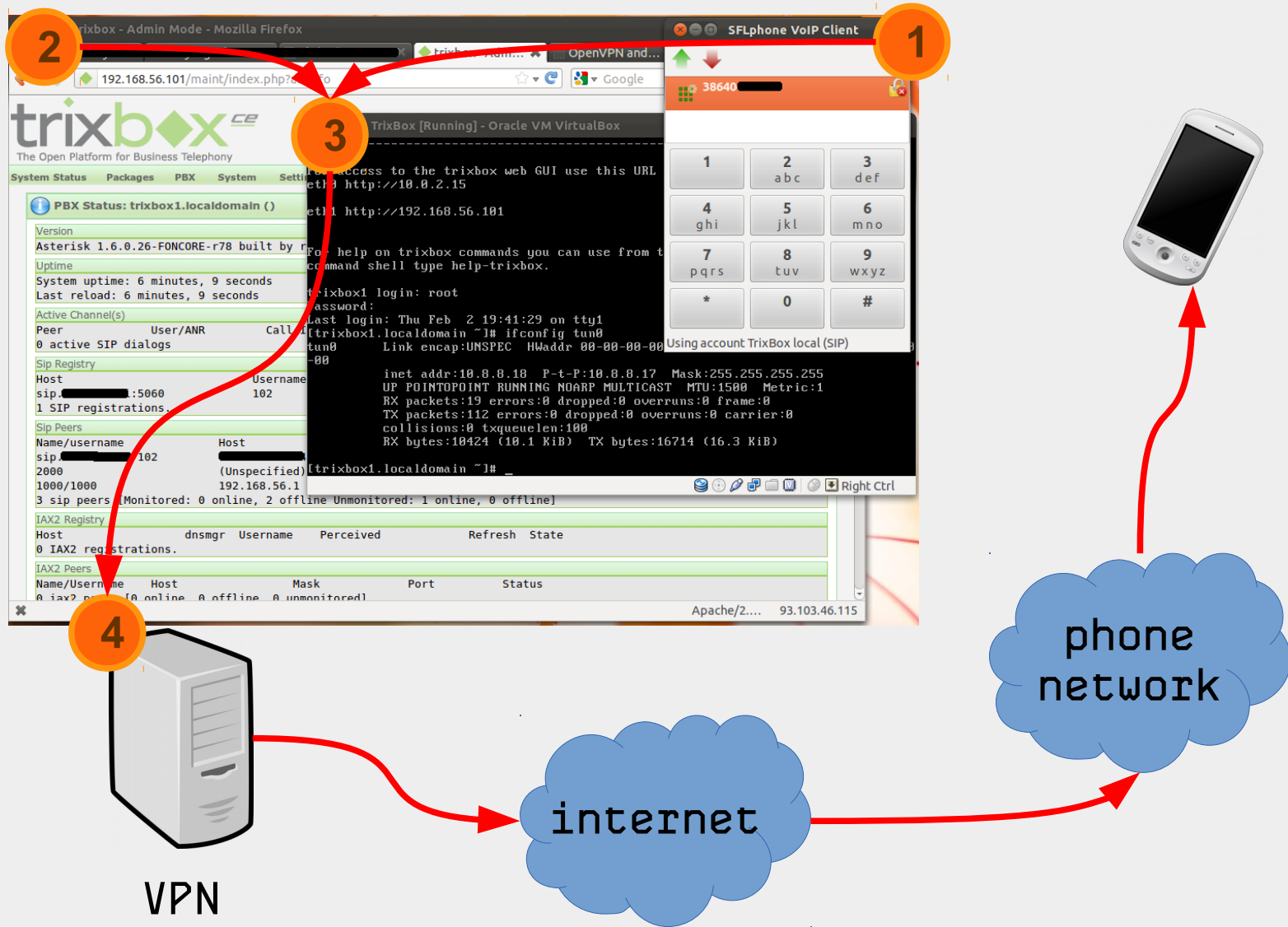
```
trixbox1 login: root
Password:
Last login: Thu Feb  2 19:41:29 on tty1
trixbox1.localdomain ~# ifconfig tun0
tun0    Link encap:UNSPEC HWaddr 00-00-00-00-00-00
        inet addr:10.0.0.10  P-t-P:10.0.0.17  Mask:255.255.255.255
        UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
         RX packets:19 errors:0 dropped:0 overruns:0 frame:0
         TX packets:112 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:100
         RX bytes:10424 (10.1 KiB)  TX bytes:16714 (16.3 KiB)

trixbox1.localdomain ~# _
```

Overlaid on the terminal is the SFLphone VoIP client interface, showing a numeric keypad and the text "Using account TrixBox local (SIP)".



VPN



CallerID spoofing



CallerID spoofing

	25.02.2012	11:11:02	1 E	0	SVNSM-Si.mobil	SMS_poslan / 38631595xxx	Out
	25.02.2012	11:57:43	0:01:00	0	SVNSM-Si.mobil		In
	25.02.2012	13:07:13	0:00:41	0	SVNSM-Si.mobil		In
	25.02.2012	15:39:09	0:02:05	0	SVNSM-Si.mobil		In
	25.02.2012	16:37:28	0:00:50	0	SVNSM-Si.mobil		In
	25.02.2012	23:41:22	0:00:04	0	SVNSM-Si.mobil	38640222xxx	In
					SVNSM-		

25.02.2012	23:41:22	0:00:04	0	SVNSM-Si.mobil	38640222xxx	In
25.02.2012	23:43:21	0:00:02	0	SVNSM-Si.mobil	38640444xxx	In
25.02.2012	23:45:04	0:00:02	0	SVNSM-Si.mobil	38640666xxx	In
25.02.2012	23:46:37	0:00:02	0	SVNSM-Si.mobil	38640888xxx	In

	27.02.2012	9:51:56	1 E	0	SVNSM-Si.mobil		Out
	27.02.2012	9:53:05	1 E	0	SVNSM-Si.mobil		In
	27.02.2012	12:02:08	0:02:44	0	SVNSM-Si.mobil		Out
	27.02.2012	12:06:54	0:00:20	0	SVNSM-Si.mobil		Out
	27.02.2012	12:36:34	0:00:42	0	SVNSM-Si.mobil		Out
	27.02.2012	12:46:55	1 E	0	SVNSM-Si.mobil		Out
	27.02.2012	12:49:48	1 E	0	SVNSM-Si.mobil		In

Practical use of spoofing :-)

GSM module to open garage or front door

We offer a useful device with a simple phone call opens or closes the automated garage or front door.

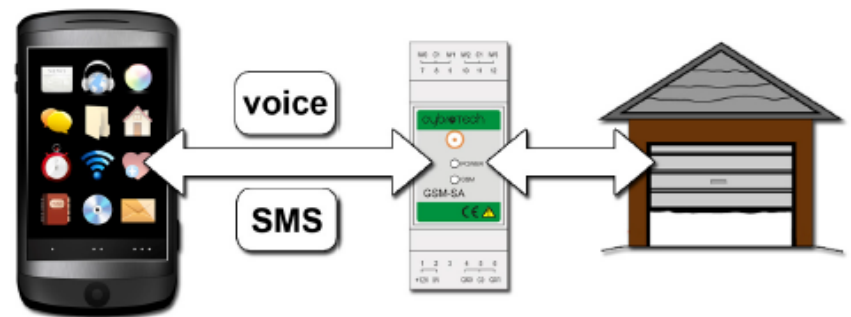
GSM module is a device which allows an authorized user to open or close the door. Device recognizes up to five specific phone numbers from which they can call on a GSM module which opens or closes the door.

Iku d.o.o. offers you:

- delivery of a package with instructions for use,
- mounting points agreed upon (please call us and we will send you the offer).

Using the GSM module to open the door:

on automated garage, front door or other GSM module is installed, in which the records are up to five phone (mobile) numbers, which is possible with a quick phone call, in order to door opened or close the door. This method accounts for the use of remote controls or additional equipment and appliances, because we assume that the mobile phone is already



Part II:
Intercepting (VoIP)
communications

Unencrypted vs. encrypted phone call

The image displays a network analysis session with several overlapping windows:

- Wireshark (sip.pcap):** Shows a list of captured packets. A filter is applied: `VoIP Calls`. The packet list table is as follows:

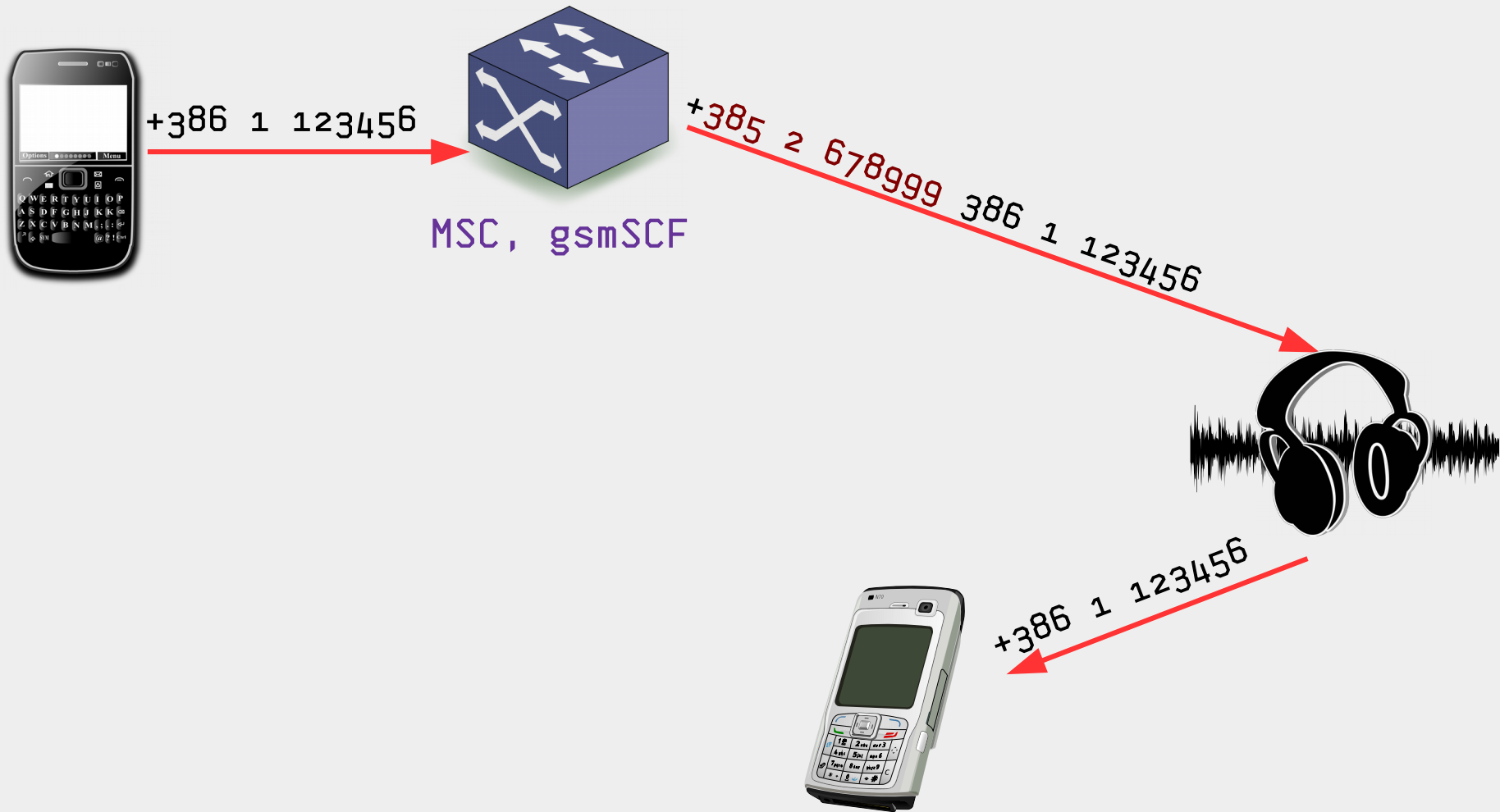
No.	Time	Source	Destination	Length	Protocol	Info
1	20:10:32.318				VoIP Calls	
2	20:10:32.318					
3	20:10:32.667					
4	20:10:32.669					
5	20:10:33.454					
6	20:10:33.454					
7	20:10:39.671					
8	20:10:40.173					
9	20:10:41.175					
10	20:10:42.669					
11	20:10:42.671					
12	20:10:43.179					
13	20:10:47.665					
14	20:10:47.667					
15	20:10:50.715					
16	20:10:50.777					
17	20:10:52.669					
18	20:10:52.670					
- Detected 2 VoIP Calls, Selected 1 Call:** A summary table showing call details:

Start Time	Stop Time	Initial Speaker	From	To	Protoco	Packets	State	Comments
21,162982	88,346119		<sip:031		SIP	7	COMPLETE	
102,384695	160,364970	172.16.0.116	"Matej Kovaric" <sip:csip:031		SIP	14	COMPLETE	
- pcap - VoIP - RTP Player:** Shows a waveform of RTP audio. A red box highlights a segment with the following details:
 - From 172.16.0.116:5062 to [redacted] Duration:64,04 Drop by Jitter Buff:0(0,0%) Out of Seq: 0(0,0%) Wrong Tim
- encrypted_srtp_audio:** A dedicated audio player window showing a waveform of encrypted audio. The title bar reads "encrypted_srtp_audio". The interface includes playback controls, volume sliders, and a frequency spectrum display.
- Packet Details:** On the right, the details pane shows SIP message headers, with several lines highlighted in red:
 - Content-Disposition: PUBLISH sip:[redacted]@212.1
 - Content-Type: application/sdp
 - Content-Length: 503
 - From: INVITE sip:015805373@212.1, with
 - To: 100 Trying
 - From: ACK sip:015805373@212.1
 - To: INVITE sip:015805373@212.1 with
 - From: 100 Trying
 - To: 180 Ringing
 - From: CANCEL sip:015805373@212.1
 - To: 200 OK
 - From: 487 Request Cancelled
 - To: ACK sip:015805373@212.1

Part III:
Rerouting outgoing calls

Example: intercepting outgoing calls

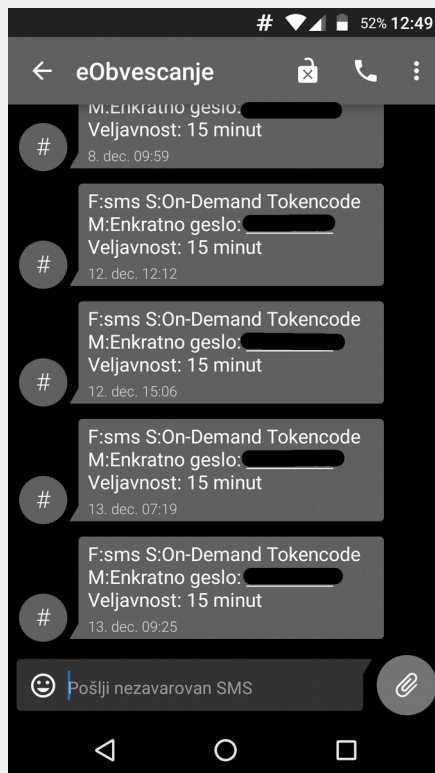
SS7 attacks.



Part IV:
Rerouting incoming
calls/SMS messages

Example: intercepting incoming calls

An attacker pretends that a subscriber is roaming in his network... From this point on, all calls and SMS messages for that subscriber are routed to the attacker.



Now a victim logs into his bank account, and since he is using two-factor authentication, his bank sends SMS to his number with mTAN access code...

How to obtain SS7 access?

Posing as a potential customer, this reporter registered an email domain—“smsrouter.co”— and, acting as a new text-message routing service, approached a division of a large-scale, legitimate telecommunications provider in Western Europe.

After exchanging emails over a weeklong period (and specifying the fake company would need coverage in Europe), the telco provided a quote: a one-time setup fee of around \$2,650, with 50 percent paid upfront and the rest with the first invoice after testing, and then a \$6,600 monthly rental fee for a so-called global title (GT)—a designated address for routing messages. The telco also offered to connect The Daily Beast’s imaginary company over a SIGTRAN link.

-- <https://www.thedailybeast.com/you-can-spy-like-the-nsa-for-a-few-thousand-bucks>

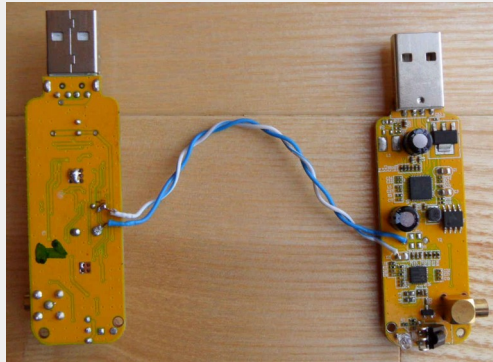
Part V: GSM Interception

gr-gsm

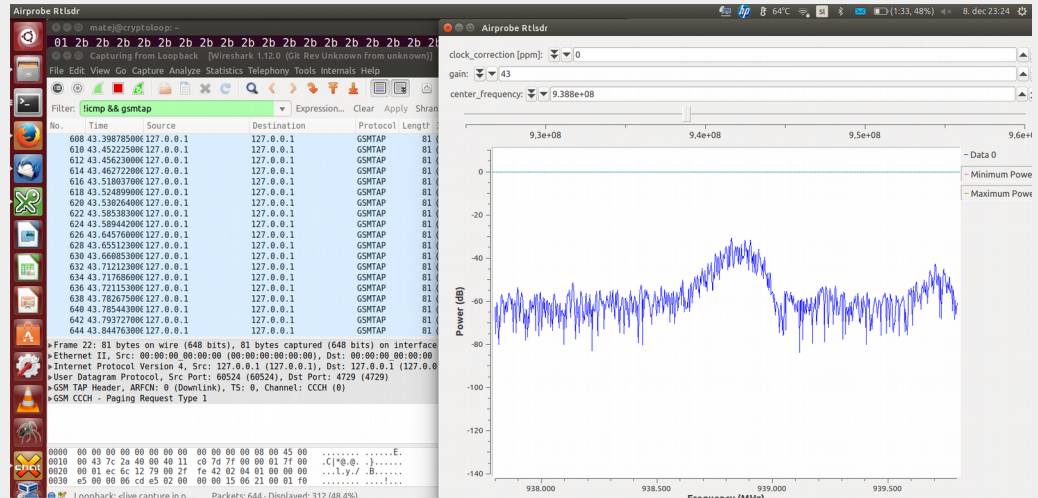
Toolset for capture and analysis of GSM signals.

```
grgsm_livemon -p 35 -f 938.8M
```

```
wireshark -k -Y '!icmp && gsmtap' -i lo
```



```
grgsm_scanner -p 35
```

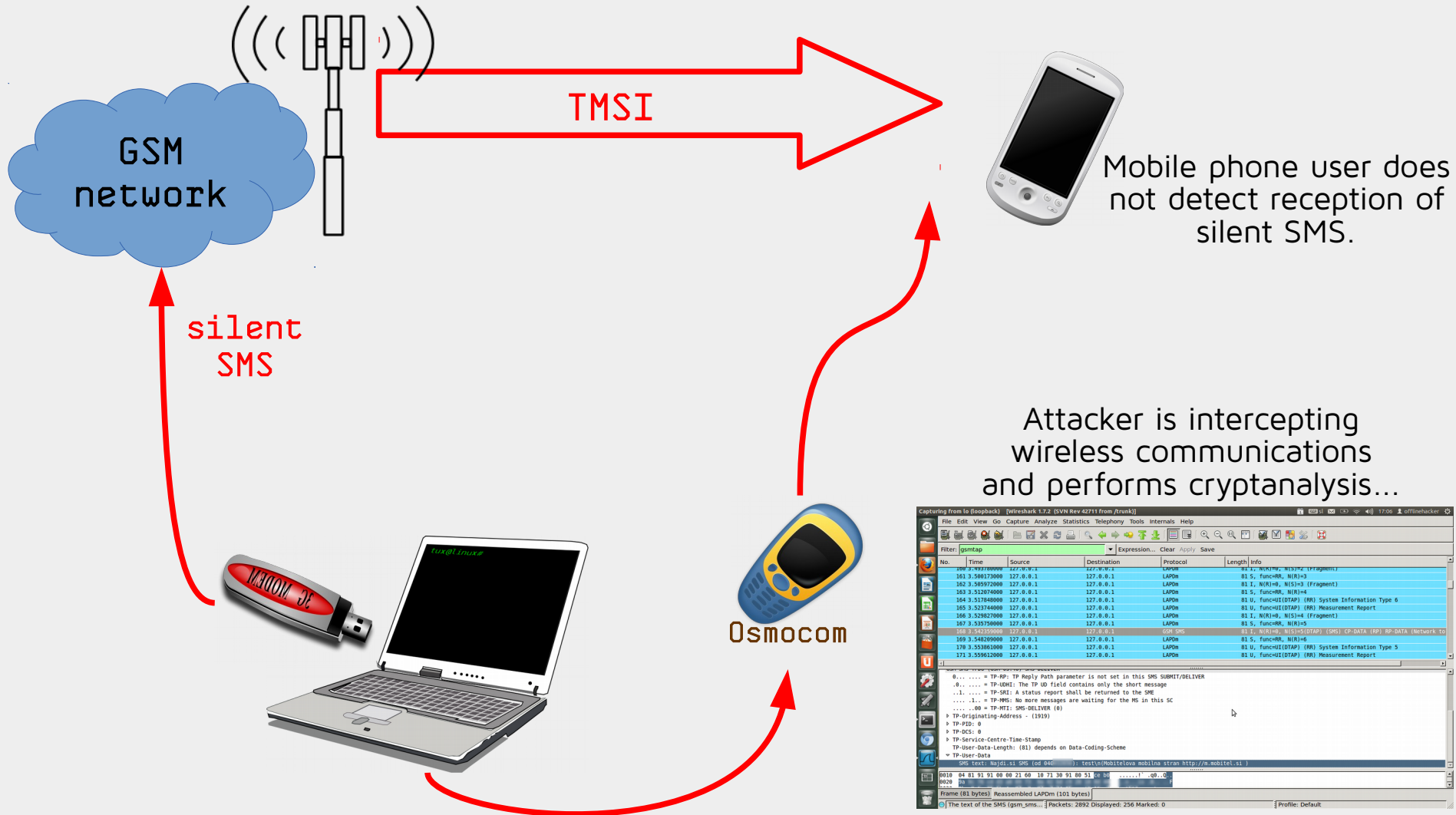


```
linux; GNU C++ version 4.9.1; Boost_105500; UHD_003.007.003-0-unknown
```

```
ARFCN: 18, Freq: 938.6M, CID: 0, LAC: 100, MCC: 293, MNC: 40, Pwr: -35  
ARFCN: 24, Freq: 939.8M, CID: 1313, LAC: 100, MCC: 293, MNC: 40, Pwr: -33  
ARFCN: 26, Freq: 940.2M, CID: 501, LAC: 100, MCC: 293, MNC: 40, Pwr: -27  
ARFCN: 124, Freq: 959.8M, CID: 0, LAC: 0, MCC: 0, MNC: 0, Pwr: -29
```

Osmocom/gr-gsm

Typical (passive) attack setup...



Part VI: IMSI Catchers

IMSI Catchers

Basically, they are fake base stations...



Alibaba.com Global trade starts here

Sourcing Solutions Services & Membership Help & Community

Categories Products What are you looking for... Search

About 2325 results: Other Telecommunications Products (47), VoIP Products (1694), Wireless Networking Equipment (408)

Home > Products > Telecommunications > Communication Equipment > Other Telecommunications Products (103492) [Subscribe to Trade Alert](#)

IMSI catcher

FOB Reference Price: [Get Latest Price](#)

US \$1,800 / Unit | 1 Unit/Units (Min. Order)

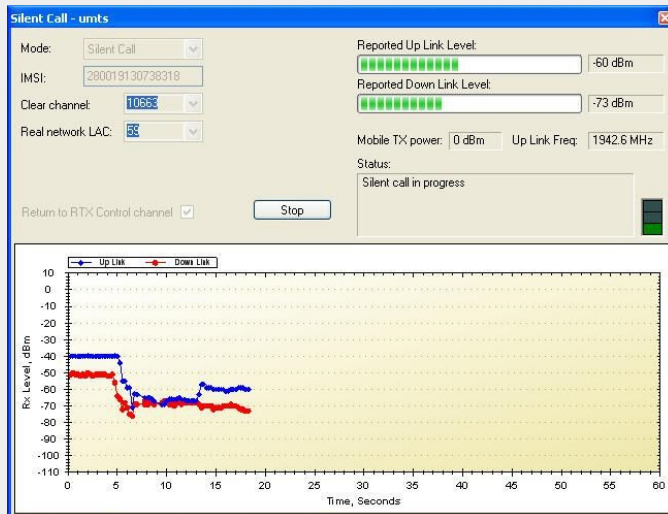
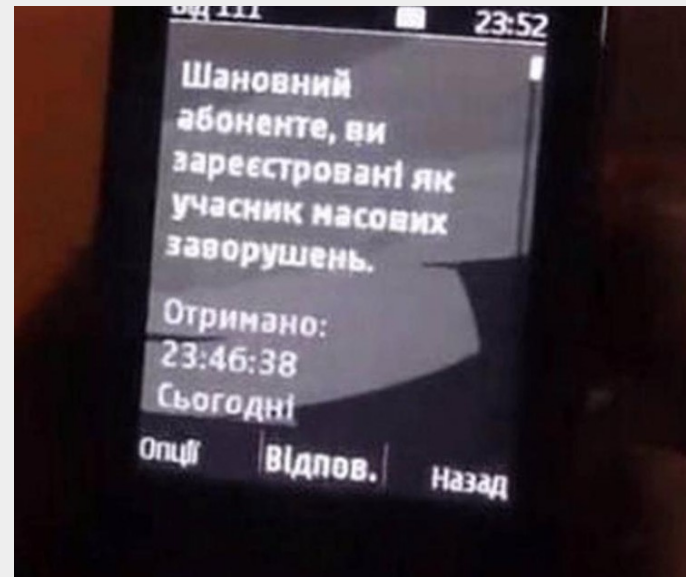
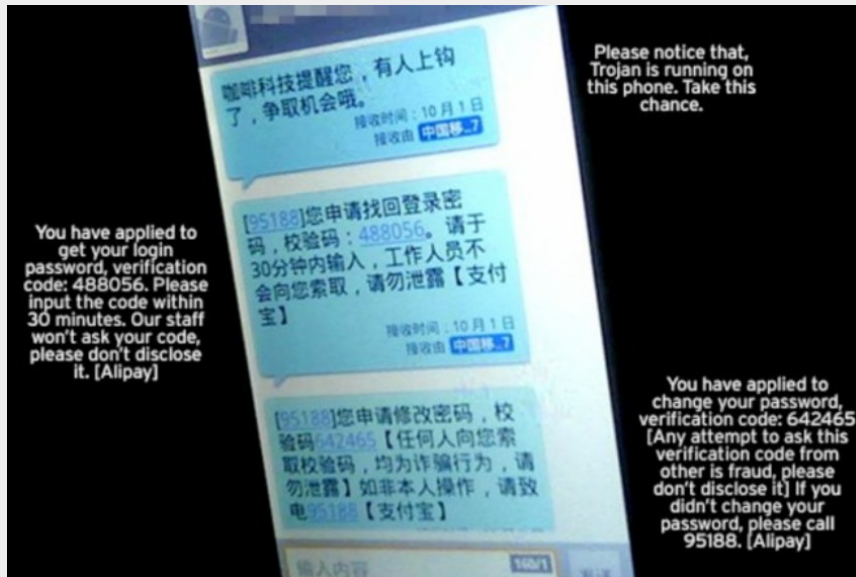
Contact Supplier

Leave Messages Add to My Cart

Payment: This supplier also supports Western Union payments for offline orders.

[View larger image](#) ZOOM

IMSI Catchers



UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

----- X

IN THE MATTER OF AN APPLICATION FOR :
THE UNITED STATES OF AMERICA FOR :
AUTHORIZATION TO CONTINUE TO :
INTERCEPT ORAL COMMUNICATIONS :
OCCURRING AT (i) THE SEATING AREA :
INSIDE BRUNELLO TRATTORIA, 227 EAST :
MAIN STREET, NEW ROCHELLE, NEW YORK :
10801; (ii) THE SEATING AREA INSIDE :
MARIO'S RESTAURANT, 2342 ARTHUR :
AVENUE, BRONX, NEW YORK 10458; :
(iii) THE SEATING AREA INSIDE :
AGOSTINO'S RESTAURANT, 969 BOSTON :
POST ROAD, NEW ROCHELLE, NEW YORK :
10801; AND (iv) THE SEATING AREA :
INSIDE THE MARINA RESTAURANT, WRIGHT :
ISLAND MARINA 280 DRAKE AVENUE, NEW

APPLICATION FOR AN :
ORDER AUTHORIZING THE :
INTERCEPTION OF ORAL :
COMMUNICATIONS

IMSI Catcher (when it is caught :-)

Wireshark interface showing network traffic analysis for `e212.imsi`.

No.	Time	Source	Destination	Protocol	Length	Info
24...	56.627398...	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH)	(RR) Paging Request Type 1
34...	81.125671...	127.0.0.1	127.0.0.1	GSMTAP	81 (CCCH)	(RR) Paging Request Type 1

Packet Details:

- User Datagram Protocol, Src Port: 57272, Dst Port: 4729
- GSM TAP Header, ARFCN: 0 (Downlink), TS: 0, Channel: CCCH (5)
- GSM CCCH - Paging Request Type 1
 - L2 Pseudo Length
 - ... 0110 = Protocol discriminator: Radio Resources Management messages (0x6)
Message Type: Paging Request Type 1
 - Page Mode
 - Channel Needed
 - Mobile Identity - Mobile Identity 1 - IMSI ([REDACTED])
Length: 8
 - 0010 = Identity Digit 1: 2
 - ... 1... = Odd/even indication: Odd number of identity digits
 -001 = Mobile Identity Type: IMSI (1)
 - IMSI: [REDACTED]**
 - Mobile Country Code (MCC): Slovenia (293)
 - Mobile Network Code (MNC): SI Mobil (40)
 - P1 Rest Octets

Packet Bytes:

```
0010 00 43 70 31 40 00 40 11 cc 76 7f 00 00 01 7f 00 .Cp1@.@. .v.....
0020 [REDACTED] [REDACTED]
0030 [REDACTED] [REDACTED]
0040 [REDACTED] 2b 2b [REDACTED] +++++
0050 2b +
```

International mobile subscriber identity(IMSI) (e212.imsi), 8 bytes

Packets: 4196 · Displayed: 2 (0.0%) · Load time: 0:0.83 · Profile: Default

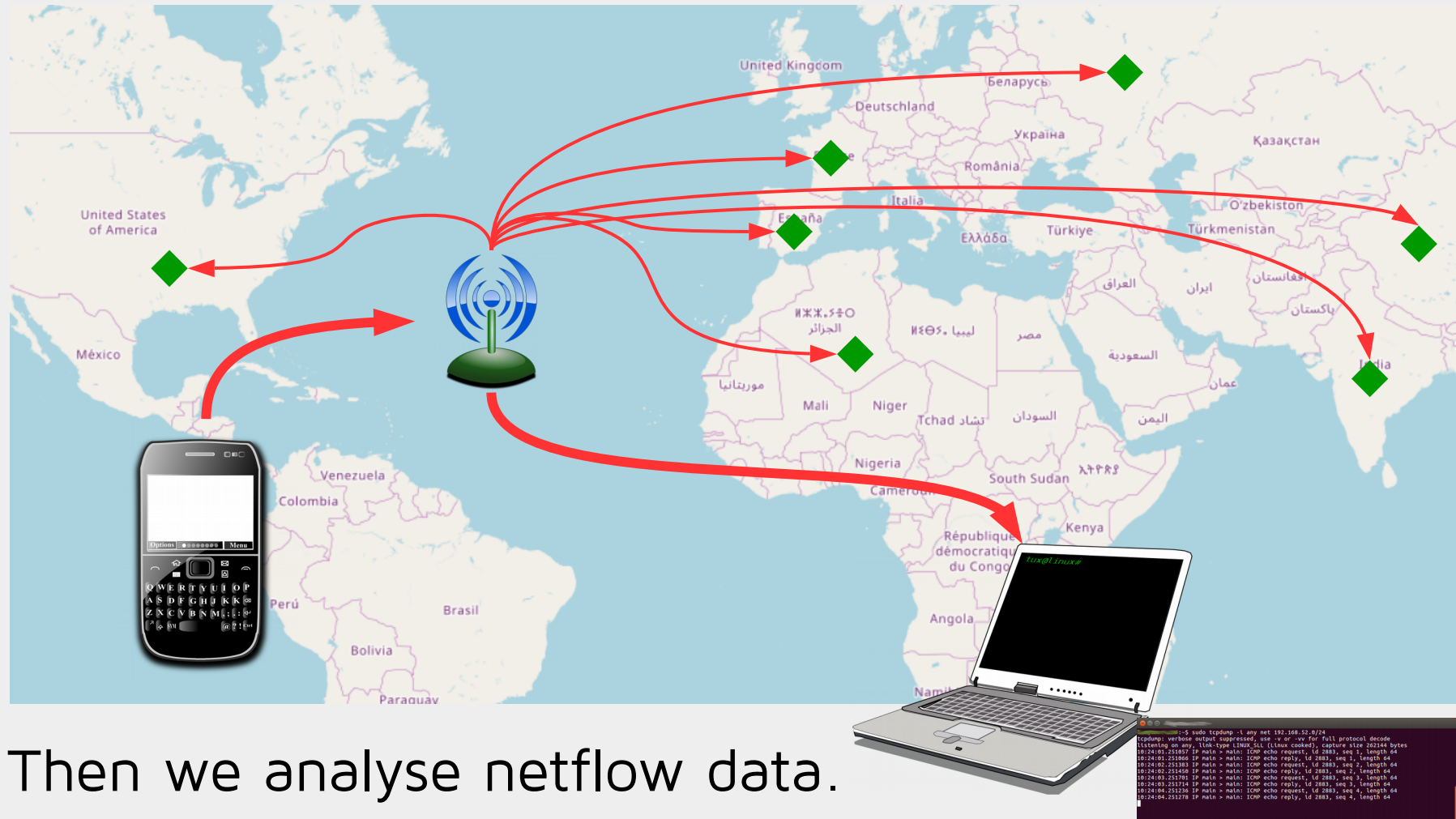
Part VII:

Mobile Phone Infection

[via "classical" malware or via baseband attack]

Real Case [Netflow Analysis]


First we intercept mobile phone network connections and collect IP network traffic.



Then we analyse netflow data.

```
root@kali:~# sudo tcpdump -l any net 192.168.52.0/24
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 262144 bytes
00:24:00.251877 IP main > main: ICMP echo request, id 2883, seq 0, length 64
00:24:00.251886 IP main > main: ICMP echo reply, id 2883, seq 1, length 64
00:24:00.251983 IP main > main: ICMP echo request, id 2883, seq 2, length 64
00:24:00.251990 IP main > main: ICMP echo reply, id 2883, seq 2, length 64
00:24:00.252091 IP main > main: ICMP echo request, id 2883, seq 3, length 64
00:24:00.252100 IP main > main: ICMP echo reply, id 2883, seq 3, length 64
00:24:00.252200 IP main > main: ICMP echo request, id 2883, seq 4, length 64
00:24:00.252208 IP main > main: ICMP echo reply, id 2883, seq 4, length 64
```

Real Case (Netflow Analysis)


Welcome Guest: [Manual](#) - [Status](#)

Data Sets | telefon

Flows [2] | Overview | Statistics | Per Hour | GeoMAP | IPs Source [1] | IPs Destination [1] | Protocols | Timeline

Date ↑	Time	Source IP	Destination IP	Destination Name	Source Port	Destination Port	L4	Protocol	Country
2017-██	10:25:10	192.168.160.251	██	██	50280	443	TCP	SSL	██
2017-██	10:25:09	192.168.160.251	██	██	50277	443	TCP	SSL	██

Wireshark · Packet 201114 · 2017

▼ **TLSv1.2 Record Layer: Handshake Protocol: Certificate**

Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 2805

▼ **Handshake Protocol: Certificate**

Handshake Type: Certificate (11)
Length: 2801
Certificates Length: 2798

▼ **Certificates (2798 bytes)**

▼ Certificate Length: 1685

▼ Certificate: 38 ██████████ (id-at-██████████)

▼ signedCertificate

version: v3 (2)
serialNumber: 0x██████████

signature (sha256WithRSAEncryption)
Algorithm Id: 1.2.840.113549.1.1.11 (sha256WithRSAEncryption)

issuer: rdnSequence (0)

▼ rdnSequence: 3 items (id-at-commonName=██████████)

- ▶ RDNSequence item: 1 item (id-at-countryName=██████████)
- ▶ RDNSequence item: 1 item (id-at-organizationName=██████████)
- ▶ RDNSequence item: 1 item (id-at-commonName=██████████)

▶ validity

- ▶ subject: rdnSequence (0)
- ▶ subjectPublicKeyInfo

▼ extensions: 9 items

▼ Extension (id-ce-subjectAltName)

Extension Id: 2.5.29.17 (id-ce-subjectAltName)

GeneralNames: 6 items

- ▶ GeneralName: dNSName (2)
dNSName: ██████████
- ▶ GeneralName: dNSName (2)
dNSName: ██████████
- ▶ GeneralName: dNSName (2)
dNSName: ██████████
- ▶ GeneralName: dNSName (2)
dNSName: ██████████
- ▶ GeneralName: dNSName (2)
dNSName: ██████████
- ▶ GeneralName: dNSName (2)
dNSName: ██████████
- ▶ GeneralName: dNSName (2)
dNSName: ██████████
- ▶ Extension (id-ce-basicConstraints)
- ▶ Extension (id-ce-kevUsage)

USER	PID	PPID	VSIZE	RSS	WCHAN	PC	NAME
root	1	0	23296	972	SyS_epoll_	000000000	S /init
root	2	0	0	0	kthreadd	000000000	S kthreadd
root	3	2	0	0	smpboot_th	000000000	S ksoftirqd/0
root	7	2	0	0	rcu_gp_kth	000000000	S rcu_preempt
root	8	2	0	0	rcu_gp_kth	000000000	S rcu_sched
root	9	2	0	0	rcu_gp_kth	000000000	S rcu_bh
root	10	2	0	0	smpboot_th	000000000	S migration/0
root	11	2	0	0	smpboot_th	000000000	S watchdog/0
root	12	2	0	0	smpboot_th	000000000	S watchdog/1
root	13	2	0	0	smpboot_th	000000000	S migration/1
root	14	2	0	0	smpboot_th	000000000	S ksoftirqd/1
root	17	2	0	0	smpboot_th	000000000	S watchdog/2
root	18	2	0	0	smpboot_th	000000000	S migration/2
root	19	2	0	0	smpboot_th	000000000	S ksoftirqd/2
root	22	2	0	0	smpboot_th	000000000	S watchdog/3
root	23	2	0	0	smpboot_th	000000000	S migration/3
root	24	2	0	0	smpboot_th	000000000	S ksoftirqd/3
root	27	2	0	0	smpboot_th	000000000	S watchdog/4
root	28	2	0	0	smpboot_th	000000000	S migration/4
root	29	2	0	0	smpboot_th	000000000	S ksoftirqd/4
root	32	2	0	0	smpboot_th	000000000	S watchdog/5
root	33	2	0	0	smpboot_th	000000000	S migration/5
root	34	2	0	0	smpboot_th	000000000	S ksoftirqd/5

No.: 201114 · Time: 1552.980957 · Source: 217.20.156.148 · Destination: 192.168.160.251 · Protocol: TLSv1.2 · Length: 1282 · Info: Certificate

[Help](#)

Questions?



Matej Kovačič
matej.kovacic@ijs.si



<https://telefoncek.si>