
CS3 SECURITY SERVICES
https://cs3group.com
WHERE IS WALLY?
Pedro C. aka s4ur0n
SH3LLCON
Security Hell Conference

Whoami

```
class PedroC:
    def __init__(self):
        self.name =  'Pedro Candel'
        self.email =  's4ur0n@s4ur0n.com'
        self.web =    'https://www.s4ur0n.com'
        self.nick =   '@NN2ed_s4ur0n'
        self.role =   'Security Researcher'
        self.work =   [ 'Reversing', 'Malware',
                        'Offensive Security', '...' ]
        self.groups = [ 'mlw.re', 'OWASP', 'NetXploit', '...' ]
```

mlw.re

OWASP Open Web Application Security Project

© 2018 CS3 Group. Todos los derechos reservados.

CS³ SECURITY SERVICES
https://cs3group.com

Portfolio

Formación en Seguridad

Cursos presenciales a medida impartidos en las instalaciones del cliente o las concertadas con prácticas reales desde el primer momento

Hacking Ético

Auditorías de caja negra, gris o blanca para aplicaciones web, sistemas y redes de comunicaciones

Análisis de Malware

Análisis de Malware automatizados y manuales con completos informes de comportamiento e indicadores de compromiso (IOC)

Ingeniería Inversa

Ingeniería Inversa para binarios de sistemas Windows de 32/64 bits, GNU/Linux de 32/64 bits, OSX Mach-O de 64 bits, ARM y firmwares

Exploiting

Desarrollo y adaptación de exploits para sistemas Windows de 32/64 bits, GNU/Linux de 32/64 bits, OSX Mach-O de 64 bits y Android

Desarrollo Seguro

Auditoría SAST, DAST, IAST y RASP para análisis de vulnerabilidades en el código de proyectos en Java, .Net, PHP, C/C++ y Cobol

Hardware Hacking

Análisis de vulnerabilidades en dispositivos hardware, sistemas embebidos y firmware con técnicas de ingeniería inversa

Seguridad en dispositivos móviles

Análisis estático, dinámico e instrumentación dinámica de aplicaciones Android (APK), iOS (IPA) y Windows Mobile (APPX)

Respuesta ante incidentes

Investigación remota de incidentes de seguridad, análisis de las situaciones y respuesta inmediata ante las amenazas

Forense

Adquisición y elaboración de informes periciales con garantía de imparcialidad y objetividad para todo tipo de sistemas de información

DevSecOps

Desarrollo, Seguridad y Operaciones en CSI (Continuous Security Integration) con pruebas automatizadas de seguridad para CI/CD

Intelligence

Recopilación, análisis y explotación de datos a gran escala con fuentes OSINT, SIGINT, HUMINT, Deep Web, redes P2P, etc.

SIGINT

Inteligencia de comunicaciones, análisis y auditoría de seguridad en señales y protocolos de radiofrecuencia (RF)

T.S.C.M.

Technical Surveillance Counter-Measures: Contramedidas electrónicas para detección y localización de dispositivos de escucha

Telecom

Análisis y auditoría GSM/3G/4G, implementación de servicios de operadores móviles virtuales (HLR, VLR, GGSN, Roaming voz y datos)

ATM

Análisis de vulnerabilidades, auditoría, forense, skimming, shimming y pruebas de blackbox para NCR, Hyosung, WRG, Diebold Nixdorf e Hitachi

PoS/TPV

Auditoría y cumplimiento de controles en terminales Verifone e Ingenico. Monitorización y transaccionabilidad completa según ISO 8583

LOPD/GPDR/Cumplimiento

LOPD, adaptación GPDR, ISO 27000, SGSI, análisis y gestión de riesgos, Políticas de seguridad, continuidad de negocio, ITIL, PCI DSS

© 2018 CS3 Group. Todos los derechos reservados.

Agenda

- Introducción
- Instalación
- DEMO
- Conclusiones

© 2018 CS3 Group. Todos los derechos reservados.

CS3 SECURITY SERVICES
https://cs3group.com

SH3LLCON
Security Hell Conference



© 2018 CS3 Group. Todos los derechos reservados.

1 Introducción

- An **International Mobile Subscriber Identity-catcher**, or IMSI-catcher, is a telephone eavesdropping device used for intercepting mobile phone traffic and tracking location data of mobile phone users.
- Essentially a **"fake"** mobile tower acting between the target mobile phone and the service provider's real towers, it is considered a man-in-the-middle (MITM) attack.

© 2018 CS3 Group. Todos los derechos reservados.

1 Introducción

- The **3G wireless** standard **mitigates some risk** due to mutual authentication required from both the handset and the network.
- However, sophisticated attacks may be able to **downgrade 3G and LTE to non-LTE** network services which ***do not require mutual authentication***.
- Source: https://en.wikipedia.org/wiki/IMSI-catcher

© 2018 CS3 Group. Todos los derechos reservados.

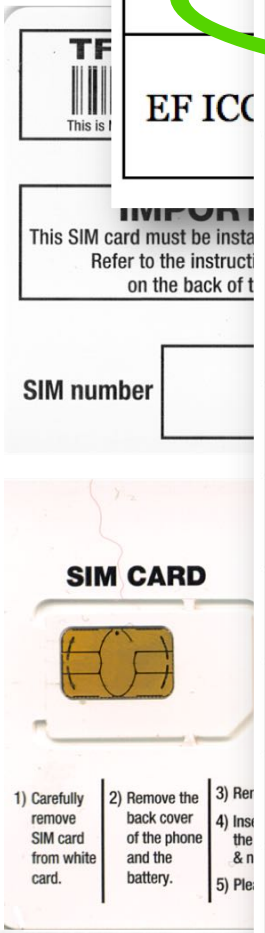
1 Introducción

- Tip
- **Pas**
- **Act**



© 2018 CS3 Group. Todos los derechos reservados.

- SIM 1



File Name	File ID	Size
EF LP	6F05	1-n bytes nth language code
EF IMSI	6F07	9 bytes
EF KC	6F20	9 bytes
EF HPPLMN	6F31	1 byte
EF SST	6F38	X bytes X >= 2
EF BCCH	6F74	16 bytes
EF ACC	6F78	2 bytes
EF FPLMN	6F7B	12 bytes
EF LOCI	6F7E	11 bytes
EF AD	6FAD	3 + X bytes
EF Phase	6FAE	1 byte

R FILE (MF)

© 2018 CS3 Group. Todos los derechos reservados.

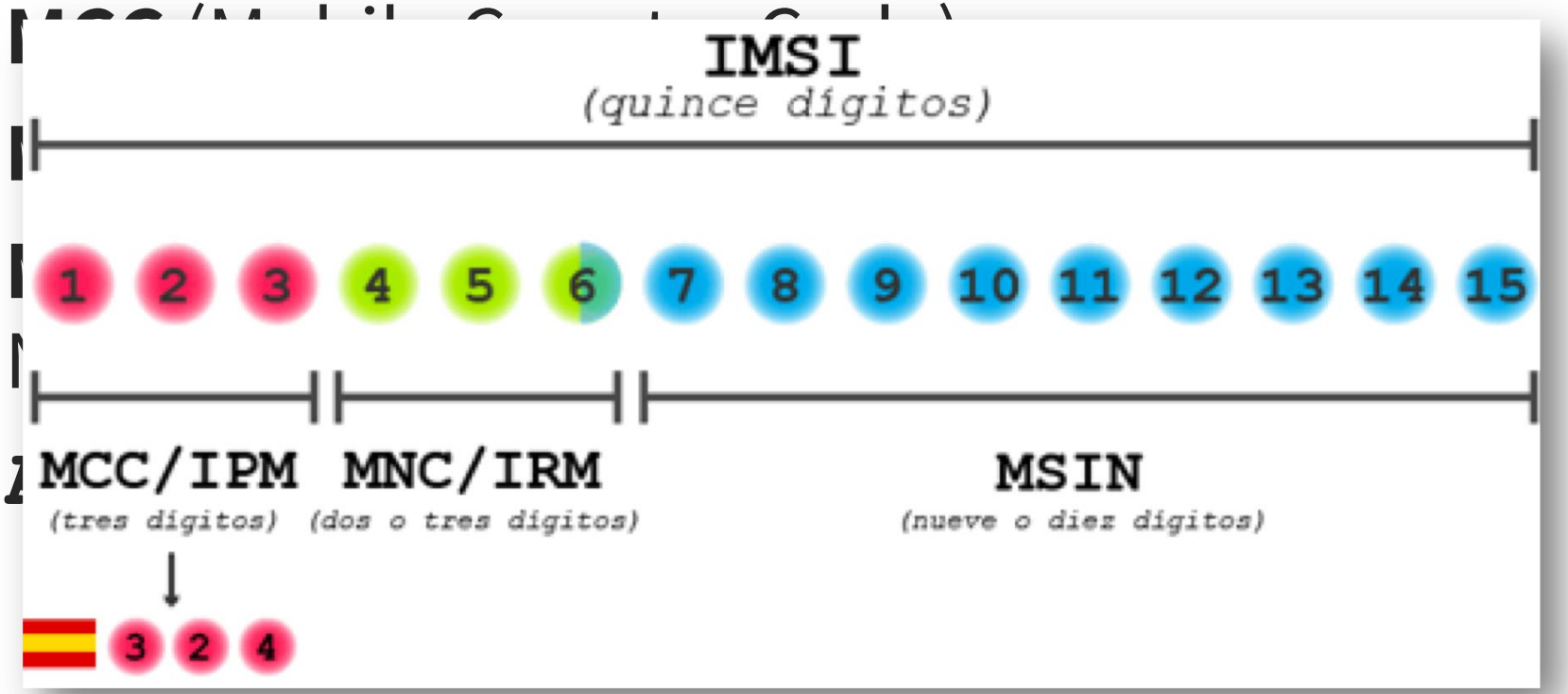
1 Introducción

- IMSI 101 (**International Mobile Subscriber Identity**)
- Es un número de 15 dígitos que reconoce el operador que está usando su teléfono.
- Cada IMSI es un **código único**.
- El dispositivo lo **almacena** y lo **envía** de **forma segura** a su red ***para identificarlo***.
- Los números IMSI están asociados a redes móviles, tanto GSM como UMTS.

© 2018 CS3 Group. Todos los derechos reservados.

1 Introducción

- Compuesto por **3 partes**:
- **M**
- **I**
- **I**
  N
- **A**



© 2018 CS3 Group. Todos los derechos reservados.

1 Introducción

- IMEI 101 (**Int**[illegible]**tional Mobile** Station **Equipm**[illegible])
- **Identif**[illegible] pero [illegible]**iza** para estable[illegible]cación
- Los opera[illegible]**ben d**[illegible]**r** que el terminal es válido y no h[illegible]nciado.
- **`AT+CGSN`**
- **`*#06#`**



© 2018 CS3 Group. Todos los derechos reservados.

1 Introducción

- Conexión 101
- La **conexión inicial** le da al dispositivo móvil un **código temporal de identidad de abonado móvil** (**TMSI**).
- Se utiliza para las identificaciones de suscriptores **cada vez que accede a la red móvil**.
- El número temporal **se genera** mientras el teléfono se está inicializando.

© 2018 CS3 Group. Todos los derechos reservados.

1 Introducción

- El número IMSI original **no se puede transmitir**.
- El teléfono solo genera un número temporal de TMSI y **la red lo usa para identificarlo**.
- Las bases de datos de suscriptores permanentes incluyen **HLR** (**Home Location Register**) y **VLR** (**Visitor Location Register**).
- El código IMSI obtiene la información detallada sobre el dispositivo móvil en la base de datos HLR y VLR.

© 2018 CS3 Group. Todos los derechos reservados.

1 Introducción

- Para que ***no pueda ser obtenido***, el IMSI…
- Sólo se usa cuando el TMSI (Temporary Mobile Subscriber Identity) **no se encuentra disponible**, p.e. en la conexión inicial.
- El VLR es responsable de la **localización actual** de un suscriptor y **asigna** un TMSI.
- El terminal **almacena el TMSI en la SIM** y en el VLR
- Consulta al **HLR de origen** los permisos del usuario (si puede hacer llamadas o no).

© 2018 CS3 Group. Todos los derechos reservados.

1 Introducción

- **HLR** (Home Location Registrer)
- Almacena la posición del usuario dentro de la red, si está conectado o no y las características de su abono (servicios que puede y no puede usar, tipo de terminal, etc.)
- Es de carácter más bien permanente
- Cada número de teléfono móvil está adscrito a un HLR **determinado y único**, que administra su operador móvil.

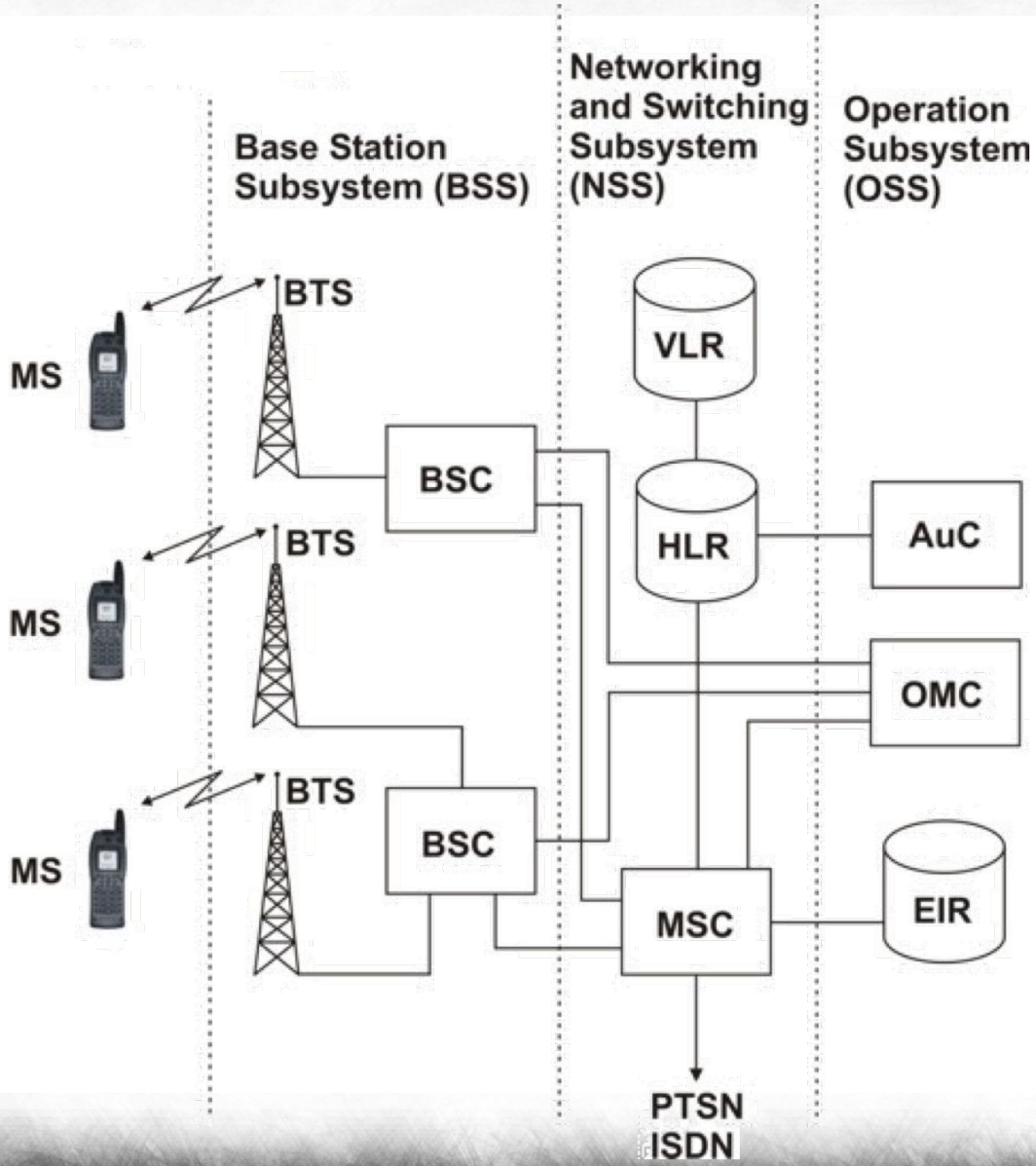
© 2018 CS3 Group. Todos los derechos reservados.

1 Introducción

- Al recibir una llamada, el **MSC** pregunta al HLR correspondiente al número llamado **si está disponible** y **dónde está** (es decir, a qué **BSC** hay que pedir que le avise) y ***enruta la llamada*** o da un ***mensaje de error***.

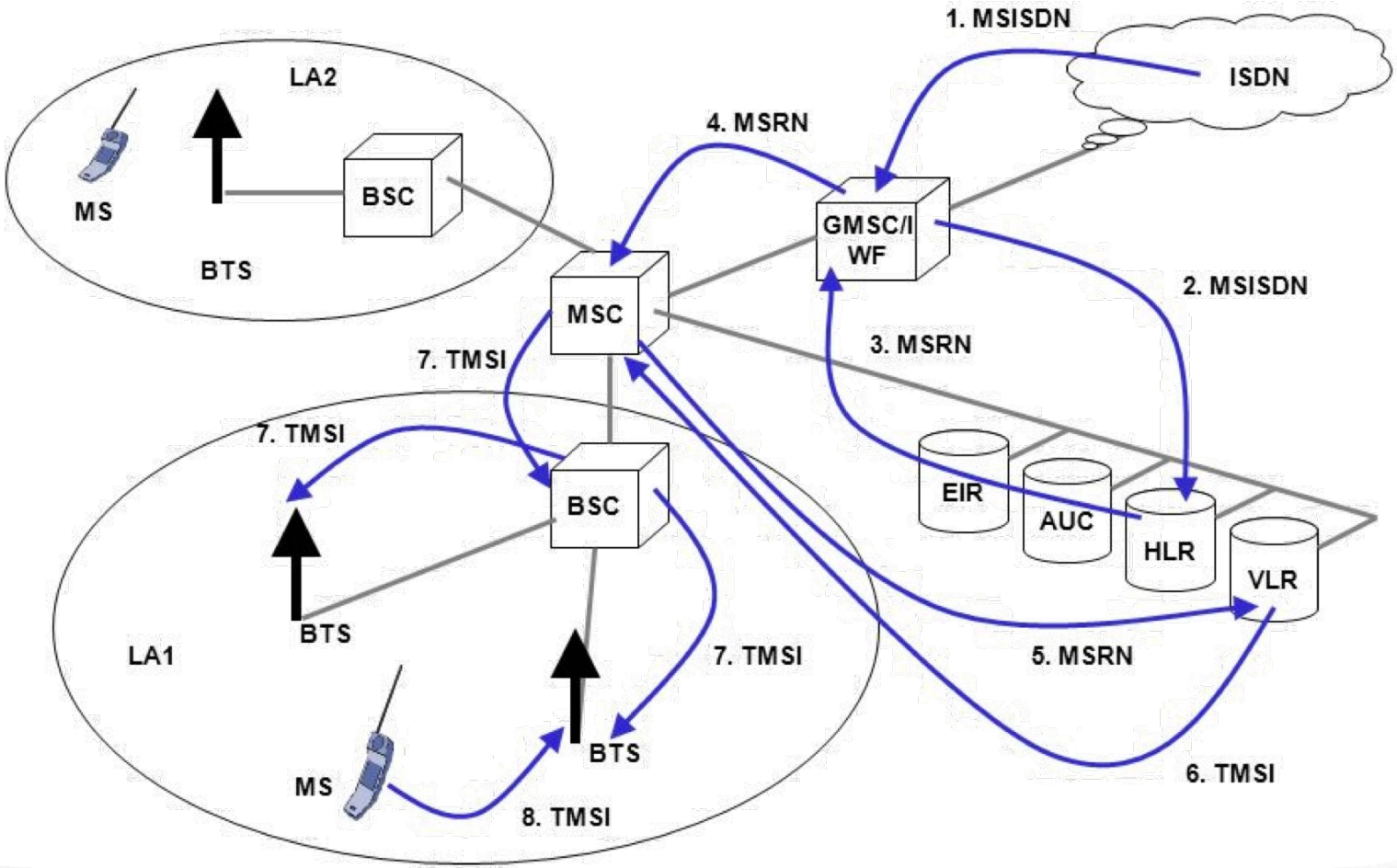
© 2018 CS3 Group. Todos los derechos reservados.

1 Introducción



© 2018 CS3 Group. Todos los derechos reservados.

GSM call routing



© 2018 CS3 Group. Todos los derechos reservados.

1 Introducción



© 2018 CS3 Group. Todos los derechos reservados.

CS3 SECURITY SERVICES
https://cs3group.com

SH3LLCON
Security Hell Conference



© 2018 CS3 Group. Todos los derechos reservados.



- **Ingredientes:**
  - SDR (RTL8232U)
  - Tiempo y ganas

© 2018 CS3 Group. Todos los derechos reservados.

CS3 SECURITY SERVICES
https://cs3group.com

2 SDR

IMSI-catcher

This program shows you IMSI numbers, country, brand and o

What you need

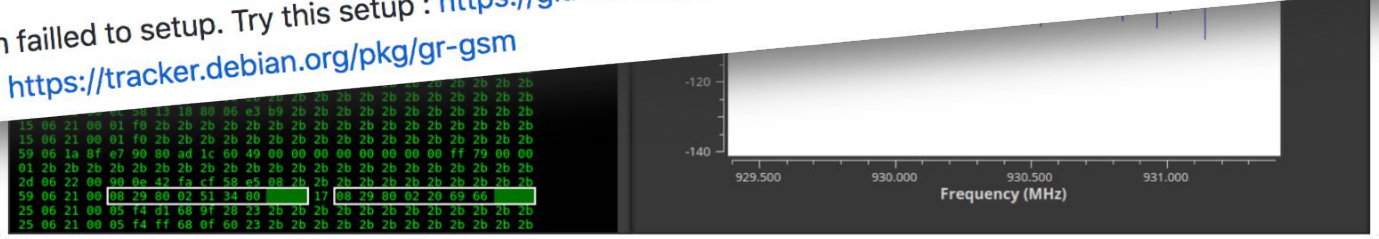
1 PC
1 USB DVB-T key (RTL2832U) with antenna (less than 15$) or a OsmocomBB phone or HackRF

Setup

```
sudo apt install python-numpy python-scipy python-scapy

sudo add-apt-repository -y ppa:ptrkrysik/gr-gsm
sudo apt update
sudo apt install gr-gsm
```

If gr-gsm failled to setup. Try this setup : https://github.com/ptrkrysik/gr-gsm/wiki/Installation
Debian : https://tracker.debian.org/pkg/gr-gsm



© 2018 CS3 Group. Todos los derechos reservados.

- **Dependencias:**
- apt-get update && apt-get upgrade apt-get -y install wim net-tools git python-pip gnutls-dev cmake libboost-all-dev libcppunit-dev swig doxygen liblog4cpp5-dev python-numpy python-scipy python-scapy automake autoconf libhackrf-dev wireshark sqlite3

© 2018 CS3 Group. Todos los derechos reservados.

- pip install PyBOMBS
- pybombs auto-config
- pybombs recipes add-defaultspybombs prefix init /usr/local -a default -R gnuradio-default
- pybombs install **gr-gsm**

© 2018 CS3 Group. Todos los derechos reservados.

2 SDR

- cd /usr/local
- git clone https://github.com/pothosware/SoapySDR.git
- cd **SoapySDR**
- mkdir build
- cd build
- cmake ..make -j4
- make install
- ldconfig –v

© 2018 CS3 Group. Todos los derechos reservados.

- cd /usr/local
- git clone https://github.com/ptrkrysik/gr-gsm.git
- cd **gr-gsm**
- mkdir build
- cd build
- cmake ..
- Make
- make install
- ldconfig -v

© 2018 CS3 Group. Todos los derechos reservados.

2 SDR

- cd /usr/src
- git clone https://github.com/steve-m/kalibrate-rtl
- cd **kalibrate-rtl**/
- ./bootstrap
- ./configure
- Make
- make install

© 2018 CS3 Group. Todos los derechos reservados.

- cd /usr/src
- git clone git://git.osmocom.org/gr-osmosdr
- cd **gr-osmosdr**
- mkdir build
- cd build
- cmake ../
- make && make install
- ldconfig -v

© 2018 CS3 Group. Todos los derechos reservados.

- cd /usr/src
- git clone **https://github.com/Oros42/IMSI-catcher**



© 2018 CS3 Group. Todos los derechos reservados.

- cd /usr/src/IMSI-catcher
- **python simple_IMSI-catcher.py**
- **grgsm_livemon -f 925.4M --serverport=10000**
- **wireshark -k -Y '!icmp && gsmtap' -i lo**

© 2018 CS3 Group. Todos los derechos reservados.

- cd /u
- pyth py
- grgs
  serv
- wire
  gsmt



© 2018 CS3 Group. Todos los derechos reservados.

- **CONCLUSIONES: Problemas**
- `cmake ../ -DINSTALL_UDEV_RULES=ON -DDETACH_KERNEL_DRIVER=ON`
- Etc, etc, etc…

© 2018 CS3 Group. Todos los derechos reservados.

CS3 SECURITY SERVICES
https://cs3group.com

SHELLCON
Security Hell Conference



© 2018 CS3 Group. Todos los derechos reservados.

CS3 IIC (Interactive IMSI Catcher)



© 2018 CS3 Group. Todos los derechos reservados.

GRACIAS



CS³ SECURITY SERVICES
https://cs3group.com

© 2018 CS3 Group. Todos los derechos reservados.

Todas las demás marcas comerciales, productos, servicios, logotipos, imágenes, etc. referenciados aquí son propiedad de sus respectivos dueños. La información presentada es exclusivamente con propósitos informativos y únicamente expresa la opinión del autor en el momento de su publicación. CS³ GROUP no puede garantizar la veracidad y licitud del contenido o información aquí presentada. CS³ GROUP ofrece TODO EL MATERIAL Y EL CONTENIDO DE ESTA PRESENTACION "COMO ESTÁ", SIN NINGUNA GARANTÍA EXPRESA O TÁCITA DE NINGÚN TIPO, INCLUYÉNDOSE SIN LIMITACIÓN LAS GARANTÍAS DE QUE EL PRODUCTO O SERVICIO SEA COMERCIALIZABLE, NO INFRACTORA DE LA PROPIEDAD INTELECTUAL DE NADIE, O IDÓNEA PARA UN DETERMINADO PROPÓSITO. CS³ GROUP NO TIENE NINGUNA OBLIGACIÓN DE PAGAR INDEMNIZACIÓN POR DAÑOS Y PERJUICIOS DE NINGÚN TIPO (INCLUYENDO, ENTRE OTRAS, LA PÉRDIDA DE GANANCIAS, PÉRDIDA DE EXPLOTACIÓN, PÉRDIDA DE INFORMACIONES) PRODUCIDOS POR EL USO O POR LA INCAPACIDAD DE USAR EL MATERIAL Y/O INFORMACION AQUÍ PRESENTADA.