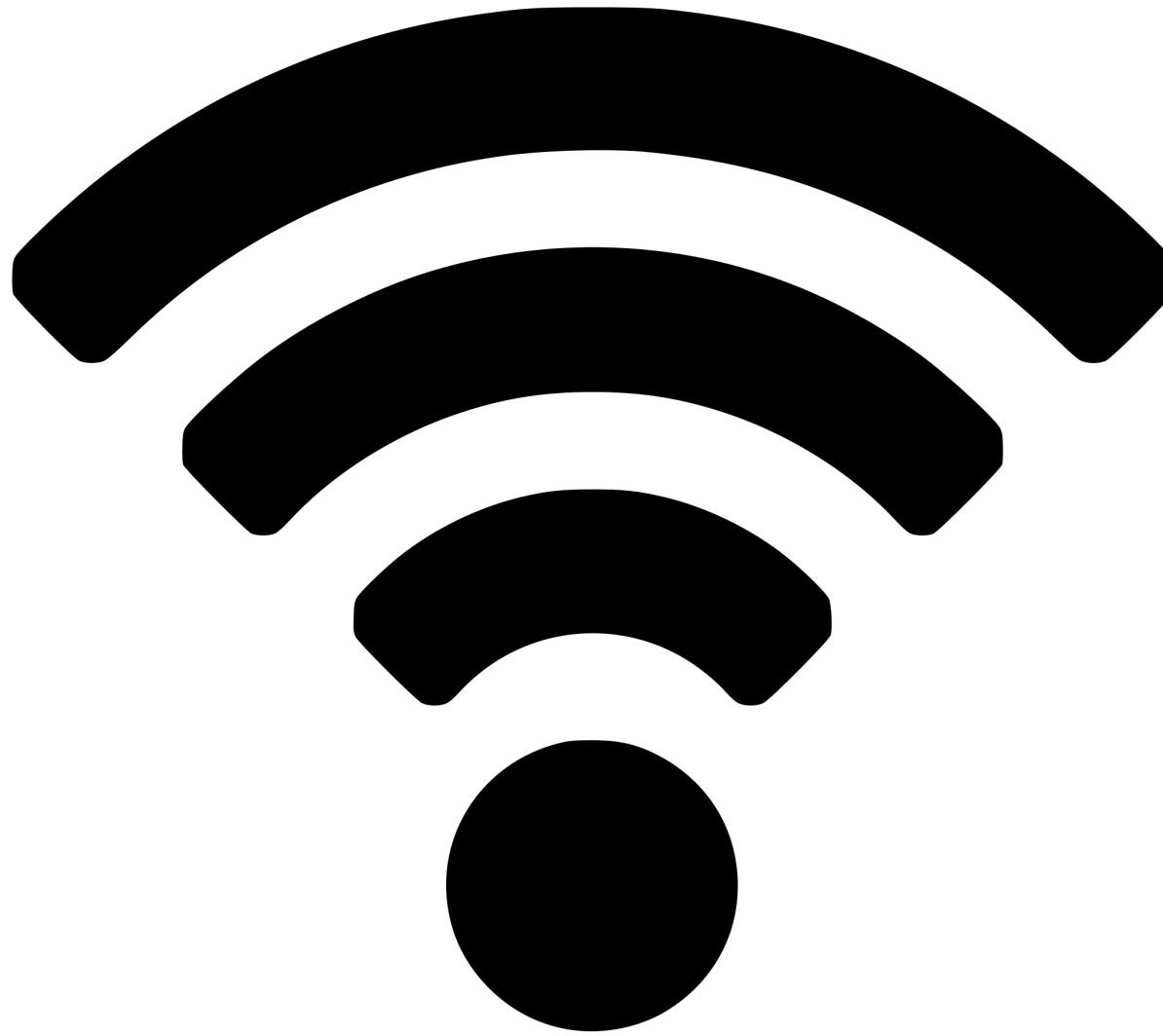




GAMAKER



Auditoría de WIRELESS:



Recopilación de recursos en WiFi arsenal <https://github.com/0x90/wifi-arsenal>

- **Aircrack-ng** <https://www.aircrack-ng.org/> es un programa de descifrado de claves 802.11 WEP y WPA y WPA2-PSK. <https://github.com/aircrack-ng/aircrack-ng> para poner a prueba la fuerza de nuestras redes WiFi. <https://tools.kali.org/wireless-attacks/aircrack-ng>

<https://gbhackers.com/aircrack-ng-wifi-password-cracker/>

- **Kismet** <https://kismetwireless.net/> es un detector de red inalámbrica (WiFi y Bluetooth), sniffer e IDS.
- **Krackattacks** <https://www.krackattacks.com/> es el ataque a redes WPA2 con los scripts disponibles <https://github.com/vanhoefm/krackattacks-scripts>

Auditoría de WIRELESS:



- **Reaver** <https://tools.kali.org/wireless-attacks/reaver> es el ataque de fuerza bruta contra WPS (WiFi Protected Setup).
<https://kali-linux.net/article/reaver/>
- **Fluxion** <https://github.com/FluxionNetwork/fluxion> es una herramienta empleada para atacar la seguridad de redes inalámbricas por ingeniería social. <https://gbhackers.com/cracking-wpa2-passwords-fluxion/> muy similar a los scripts Python de Wifite <https://github.com/derv82/wifite2>



Legislación sobre la seguridad de las comunicaciones:

En el estado es un **derecho constitucional**:

- Título I / Capítulo 2º / Sección 1ª / Artículo 18 / Apartado 3º:


<http://www.congreso.es/consti/constitucion/indice/titulos/articulos.jsp?ini=10&fin=55&tipo=2>

“Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.”

Legislación sobre la seguridad de las comunicaciones:

¿Por qué otras legislaciones se ve afectado?

- Artículo 8 del Convenio Europeo de Derechos Humanos:

https://www.echr.coe.int/Documents/Convention_SPA.pdf

...”sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.”



Legislación sobre la seguridad de las comunicaciones:

¿Por qué otras legislaciones se ve afectado?

- LECrim del RD de 14 de septiembre de 1882 Título VIII / artículo 579
 - Nueva redacción art.2 LO 4/1988 de 25 mayo de 1988
 - Nueva redacción LO 3/2015 de 5 de octubre de 2015 -> "Ley Torquemada"



Legislación sobre la seguridad de las comunicaciones:

¿Por qué otras legislaciones se ve afectado?

- LO 3/2015 de 5 de octubre de 2015:
 - Capítulo III: Correspondencia escrita o telegráfica. Artículo 579:



https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10725

“...siempre que la investigación tenga por objeto alguno de los siguientes delitos:

1. Delitos dolosos castigados con pena con límite máximo de, al menos tres años de prisión.
2. Delitos cometidos en el seno de un grupo u organización criminal.
3. Delitos de terrorismo.”

Legislación sobre la seguridad de las comunicaciones:

¿Por qué otras legislaciones se ve afectado?

- LO 3/2015 de 5 de octubre de 2015:
 - Capítulo III: Correspondencia escrita o telegráfica. Artículo 579:

https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10725

“... no se requerirá autorización judicial en los siguientes casos:

1. Envíos postales que.... no sean usualmente utilizados para contener correspondencia individual sino para servir al transporte y tráfico de mercancías...
2. Aquellas otras formas de envío... en las que resulte obligatoria una declaración externa de contenido o que incorporen la indicación expresa de que se autoriza su inspección.
3. ... de acuerdo con la normativa aduanera o proceda con arreglo a las normas postales que regulan una determinada clase de envío.”

Legislación sobre la seguridad de las comunicaciones:

¿Por qué otras legislaciones se ve afectado?

- LO 3/2015 de 5 de octubre de 2015:
 - Capítulo IV: ...interceptación de las comunicaciones telefónicas y telemáticas.
 - Artículo 588:

https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10725

“... podrá acordar alguna de las medidas de investigación reguladas en el presente capítulo siempre que medie autorización judicial.”

“En caso de urgencia, cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas o elementos terroristas y existan razones fundadas que hagan imprescindible la medida prevista en los apartados anteriores de este artículo, podrá ordenarla el Ministro del Interior o, en su defecto, el Secretario de Estado de Seguridad. Esta medida se comunicará inmediatamente al juez.”

Legislación sobre la seguridad de las comunicaciones:

¿Por qué otras legislaciones se ve afectado?

- Directiva 95/46/CE de 24 de octubre de 1995
https://www.urjc.es/images/proteccion_datos/B.4-cp--Directiva-95-46-CE.pdf
- Directiva 2002/58/CE de 12 de julio de 2002
<https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:es:PDF>
- Directiva 2006/24/CE de 15 de marzo de 2006
<https://www.boe.es/doue/2006/105/L00054-00063.pdf>
- Ley 34/2002 de 11 de julio de 2002
<https://www.boe.es/buscar/pdf/2002/BOE-A-2002-13758-consolidado.pdf>
- Ley 9/2014 de 9 de mayo 2014
<https://www.boe.es/boe/dias/2014/05/10/pdfs/BOE-A-2014-4950.pdf>

... y muchas más.



P R I S M

O n e N a t i o n U n d e r S u r v e i l l a n c e

Seguridad vs privacidad:

- *No tengo nada que ocultar...*



- <https://www.youtube.com/watch?v=J1EKvWot-3c>
- [https://commons.wikimedia.org/wiki/File:Anonymus_text_message_received_by_many_participants_of_clashes_at_Dynamivska str.- Dear subscriber, you are under arrest as a partisipant of mss protests.- Euromaidan Protes ts.jpg](https://commons.wikimedia.org/wiki/File:Anonymus_text_message_received_by_many_participants_of_clashes_at_Dynamivska_str.-_Dear_subscriber,_you_are_under_arrest_as_a_partisipant_of_mss_protests.-_Euromaidan_Protes_ts.jpg)
- <https://www.wired.com/2013/06/why-i-have-nothing-to-hide-is-the-wrong-way-to-think-about-surveillance/>
- <https://theintercept.com/2015/11/15/exploiting-emotions-about-paris-to-blame-snowden-distract-from-actual-culprits-who-empowered-isis/>
- http://www.ugr.es/~aquiran/cripto/enigma/boletin_enigma_15.txt

BYOD

Bring Your Own Device



BYOD...

Peligros:

- Uso de canales de comunicación no seguros.
 - Redes wifi abiertas o poco fiables.
- Apps que utilizan nuestra localización.
- Envío de fotos con metadatos de localización.
- Pérdida o robo del dispositivo.
- Malware.



BYOD...

Buenas prácticas

- No hacer jailbreak o rootear el móvil.
- No utilizar aplicaciones desconocidas.
- Activar el GPS sólo para las aplicaciones de “confianza”.
- Disponer de mecanismos de borrado remoto del dispositivo en caso de pérdida.



UNA AVENTURA DE MORTADELO y FILEMÓN

El pinchazo TELEFÓNICO

GUIÓN E ILUSTRACIONES DE
F. IBÁÑEZ



Auditoría de comunicaciones móviles:

Sistema de comunicación	Terminal móvil	"Antenas"/Estaciones		Sistema conmutador entre móviles/core		
2G/GSM	MS	BSS BTS + BSC		NSS MSC/VLR HLR/AuC		
"2.5G"/GPRS	UE	BSS BTS+BSC		SGSN	NSS MSC /VLR HLR/AuC	GGSN
3G/UMTS	UE	BSS BTS+BSC	RNS Node B+ RNC	SGSN	NSS MSC /VLR HLR/AuC	GGSN
4G/LTE	UE	eNodeB		EPC MME+HSS+SGW+PGW		

Tabla 1: Equivalencia de elementos de los distintos sistemas de comunicación.

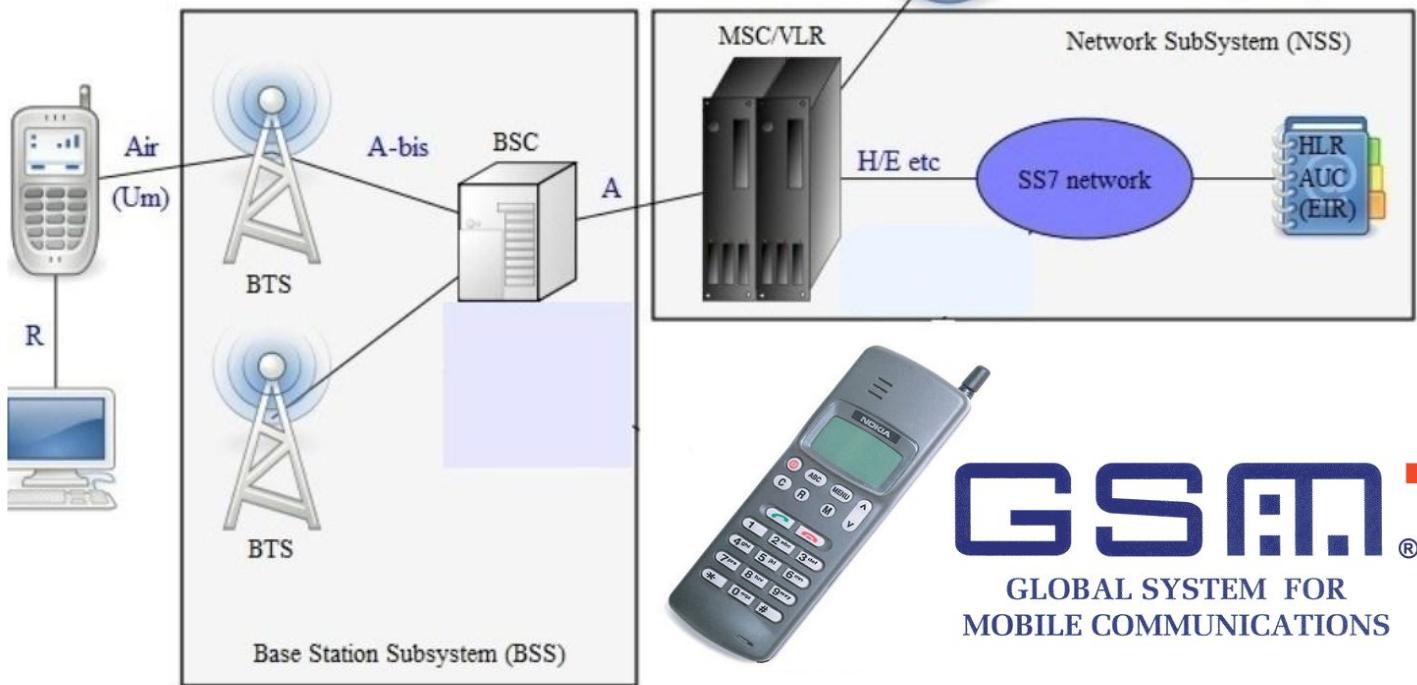
Auditoría de comunicaciones móviles:

Seguridad de telefonía móvil: https://www.owasp.org/images/0/0b/OWASP_MCT.pdf

- GSM,
- GPRS,
- UMTS,
- 4G,
- 5G.

Auditoría de comunicaciones móviles:

- GSM



Auditoría de comunicaciones móviles:

Seguridad del protocolo **GSM**:

Principales aspectos y requerimientos de seguridad:



- Confidencialidad del IMSI, es decir, del suscriptor. Esta información se considera confidencial y sensible ya que puede permitir la geolocalización de una persona.
- Validación de la autenticación del suscriptor, evitando el fraude y falsificación.
- Confidencialidad de las comunicaciones mediante mecanismos de cifrado.

Auditoría de comunicaciones móviles:

Seguridad del protocolo GSM:

- <http://www.tierradelazaro.com/criptoanalisis-del-gsm-para-moviles>
- https://www.etsi.org/deliver/etsi_ts/100900_100999/100929/08.06.00_60/ts_100929v080600p.pdf#page=25



Seguridad en comunicaciones móviles:

Infiltración en la red del operador:

El atacante ha conseguido comprometer la infraestructura de la red del operador:



- Soborno o extorsión de algún empleado.
- Acceso físicamente a la infraestructura.
- Introduciendo algún tipo de malware.



Seguridad en comunicaciones móviles:

Infiltración en la red del operador:

- En marzo 2005 se descubre que más de un centenar de políticos griegos, incluido el primer ministro, habían sido objeto de escuchas.
- El día anterior, Kostas Tsalikidis, trabajador de Vodafone Grecia, aparece suicidado en su apartamento. Se le vincula con la instalación de un malware en la red del propio operador que afectaba a los sistemas Ericsson AXE que utilizaba la compañía.



<https://spectrum.ieee.org/telecom/security/the-athens-affair>

<https://theintercept.com/2015/09/28/death-athens-rogue-nsa-operation/>

Seguridad en comunicaciones móviles:

Escucha del canal de radio:

(Señalización):



- Información sobre la red para luego elaborar un ataque.
- Información sobre usuario: su presencia o no en la red, si genera tráfico o su localización geográfica.



Seguridad en comunicaciones móviles:

Escucha del canal de radio:

(Datos):



- Ataque centrado en las comunicaciones de datos, cifradas normalmente en A5/1.
- La conversación puede ser grabada completamente para descifrarla posteriormente.

<https://www.youtube.com/watch?v=4jfpeQcOmHI>



Seguridad en comunicaciones móviles:

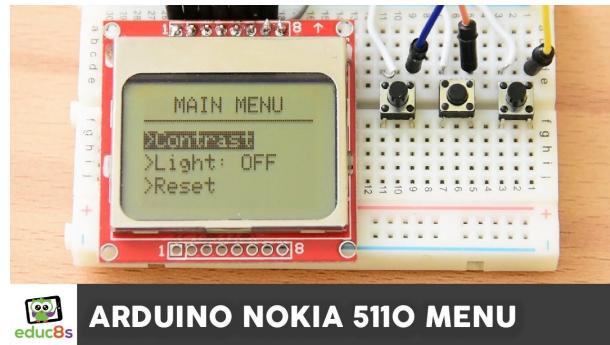


Cifrado en GSM:

- **A3**: Es el algoritmo de autenticación. Es el que hace que cada teléfono móvil sea “único”. Identifica al móvil y con la base de datos de la operadora se puede asociar al usuario propietario (SIM -> BBDD -> Operador -> Factura).
- **A5**: para cifrado de voz. Existen versiones:
 - A5/0: Sin cifrado.
 - A5/1: Desarrollado 1987. Considerado “fuerte”.
 - A5/2: Desarrollado en 1989. Versión del A5/1 deliberadamente debilitada para su exportación fuera de Norte América y Europa. Retirado en 2006.
 - A5/3: No obligatorio en GSM.
 - A5/4



Seguridad en comunicaciones móviles:



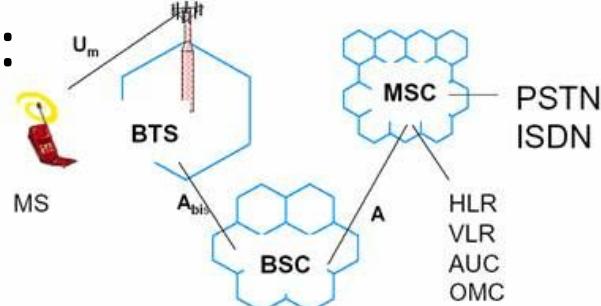
Cifrado en GSM:

- A8: Genera las claves de autenticación usadas por A3 y A5. De manera interna se suele hacer uso del algoritmo COMP128.

Ataques sobre el cifrado COMP128:

- Abril 1998: Investigadores de Berkeley y la Smartcard Developer Association publican el conocido como “narrow pipe attack”. El ataque aprovecha una debilidad en una función compresión.
 - Enviaba consultas a la SIM (hasta 2^{19} consultas) hasta detectar una colisión, lo que usa para obtener la clave, lo que implicaba la duplicación de la SIM.
 - Tiempo aproximado: 6 horas.

Seguridad en comunicaciones móviles:



Cifrado en GSM:

- Mayo 2002: Ataques sobre el cifrado COMP128: Investigadores de IBM publican el “partitioning attack”. Mejora de manera sustancial la velocidad.
- 2003: Ataques sobre el cifrado A5/2: Investigadores del Instituto Israelí de Tecnología y la Universidad de Jerusalén publican un estudio que conlleva la retirada del algoritmo A5/2. Aprovecharon los códigos de corrección de errores de los que hacía uso y un texto conocido, demostrando que era posible sacar el texto del tráfico y la clave de sesión.

<http://www.cs.technion.ac.il/users/wwwb/cgi-bin/tr-get.cgi/2006/CS/CS-2006-07.pdf>

Seguridad en comunicaciones móviles:

Cifrado en GSM:

- 2009: Ataques sobre el cifrado A5/1: A5 Security Project, proyecto para sistema asequible para realizar ataques y hacerlos públicos. Estos ataques están basados en criptoanálisis y se implementan mediante un proceso de pre-computación en tablas de aproximadamente 2TB, que supone un trabajo de unos 3 meses. Actualmente las tablas están disponibles en BitTorrent.



Seguridad en comunicaciones móviles:



- **Ataques mediante SMS:**
 - Cambio de número origen: El sistema no verifica el origen, por lo que puede ser modificado.
- **Ataques mediante SMS/MMS/WAP:**
 - Ataque OTA: Se recibe un mensaje en modo binario de manera que la interfaz inicia el acceso a la SIM, lo que puede producir denegación de servicio o la introducción de un código malicioso.



<https://media.blackhat.com/us-13/us-13-Nohl-Rooting-SIM-cards-Slides.pdf>

<https://media.blackhat.com/us-13/us-13-Nohl-Rooting-Sim-Cards.m4v>

Auditoría de comunicaciones móviles:

Seguridad del protocolo **GSM**:



De las especificaciones los algoritmos de cifrado del GSM se pueden sacar las siguientes **debilidades**:

- El IMSI puede ser enviado en texto claro en numerosas ocasiones.
- Los móviles soportan A5/0 como método de “cifrado”.
- Los algoritmos A5 son débiles en cuanto a la robustez del cifrado.
- La autenticación es unilateral desde la estación móvil a la red.
- La obtención de la clave de autenticación (KC) entre estación móvil y red permite descifrar cualquier conversación grabada con anterioridad de ese usuario de la estación móvil.

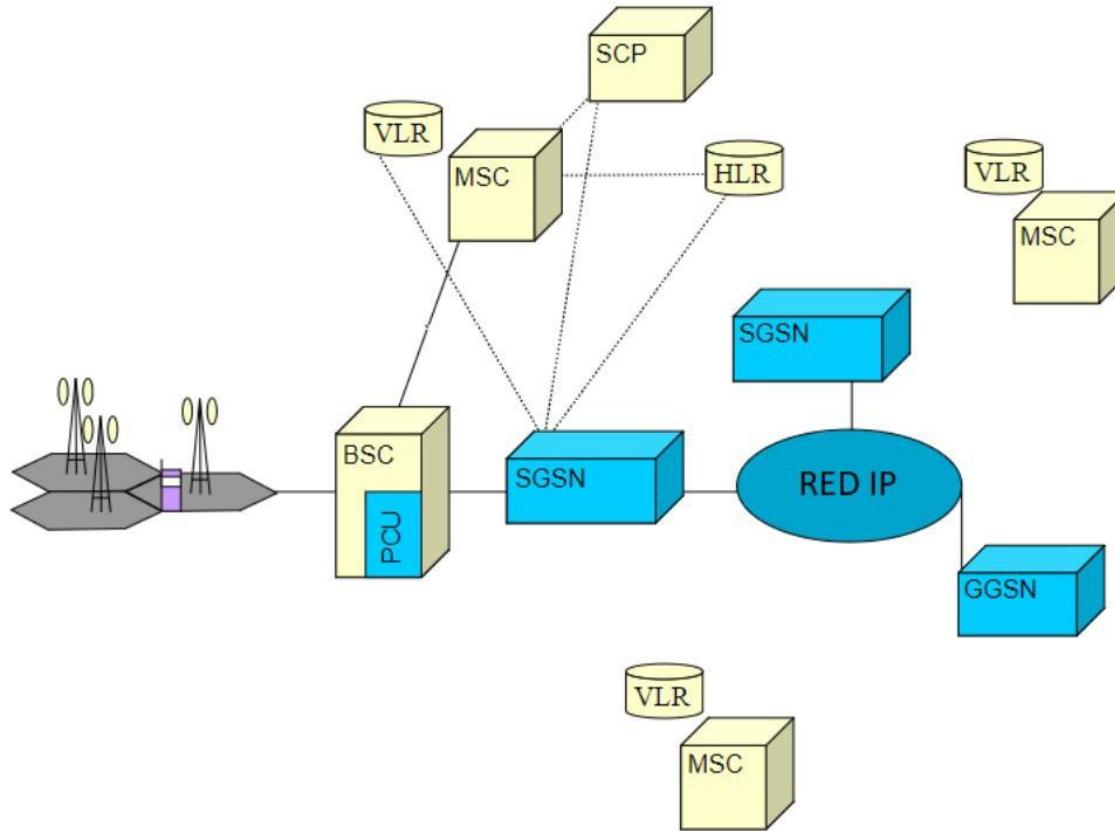
Auditoría de comunicaciones móviles:

Posibles ataques en redes GSM

- Infiltración y suplantación de la NSS
- Escuchas del canal de radio <https://z4ziggy.wordpress.com/2015/05/17/sniffing-gsm-traffic-with-hackrf/>
- Ataques al cifrado
https://fahrplan.events.ccc.de/congress/2009/Fahrplan/attachments/1519_26C3.Karsten.Nohl.GSM.pdf
- Suplantación de estación móvil
- Suplantación de estación base falsa
<http://blog.taddong.com/2011/05/selective-attack-with-rogue-gsmgprs.html>
<https://es.wikipedia.org/wiki/OpenBTS>



Auditoría de comunicaciones móviles:



Auditoría de comunicaciones móviles:



Posibles ataques en redes GPRS

- Overbilling attack (ataque de sobrefacturación.)
 - <http://cgi.di.uoa.gr/~xenakis/Published/23-CRITIS'06/CRITIS2006-Vul&Att-GPRS-backbone.pdf>
 - https://www.theregister.co.uk/2003/10/02/official_crackers_have_broken_into
- Ataques a las interfaces Gn y Gp
- Ataques pasivos
- Ataques mediante estación base falsa
 - https://media.blackhat.com/bh-dc-11/Perez-Pico/BlackHat_DC_2011_Perez-Pico_Mobile_Attacks-wp.pdf
 - <http://www.taddong.com/docs/RootedCon2011-AtaquePracticoGPRS.pdf>

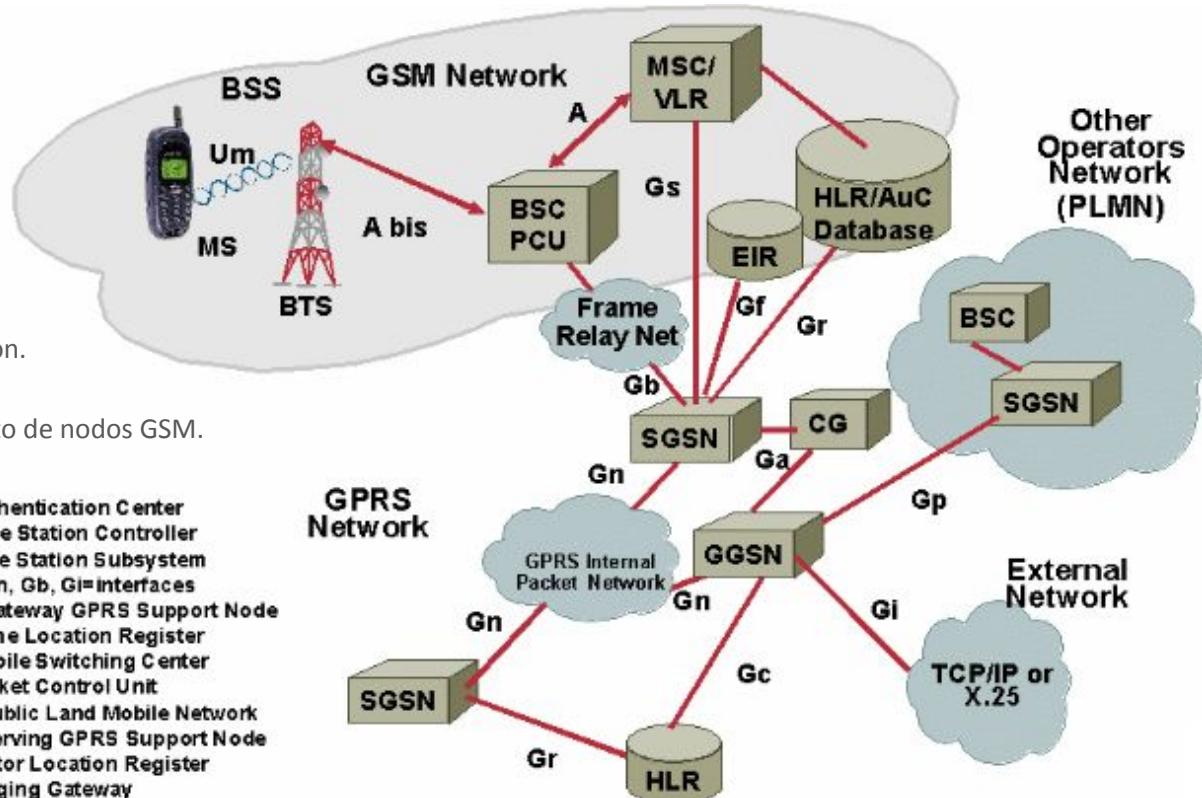
Seguridad en comunicaciones móviles:

Posibles ataques en redes GPRS

- Ataques a las interfaces Gn:

El SGSN:

- Identifica y registra usuarios.
- Realiza seguimiento de la localización.
- Funciones de movilidad
- Interactúa con redes externas y resto de nodos GSM.



Seguridad en comunicaciones móviles:

Posibles ataques en redes GPRS

- Ataques a las interfaces Gn:
 - Monitorización de tráfico de usuarios móviles.
 - Manipulación de tráfico de usuarios móviles.
 - Creación y utilización de túneles GTP.
 - Borrado selectivo de túneles GTP.
 - Borrado masivo de túneles GTP.
 - Envío de tráfico anómalo.



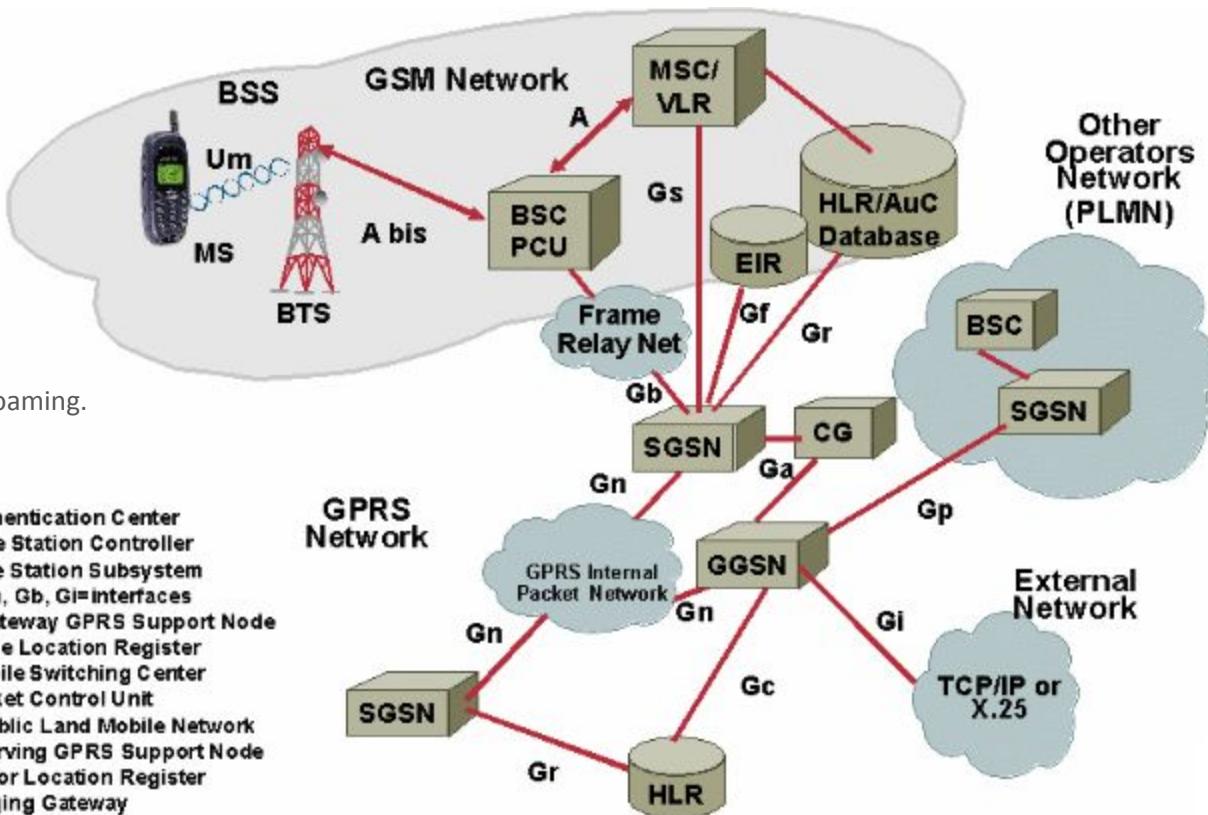
Seguridad en comunicaciones móviles:

Posibles ataques en redes GPRS

- Ataques a las interfaces Gp:

El GP:

- Toma parte para proporcionar servicios roaming.



AUC=Authentication Center
BSC=Base Station Controller
BSS=Base Station Subsystem
Gs, Gr, Gn, Gb, Gi=interfaces
GGSN=Gateway GPRS Support Node
HLR=Home Location Register
MSC=Mobile Switching Center
PCU=Packet Control Unit
PLMN=Public Land Mobile Network
SGSN=Serving GPRS Support Node
VLR=Visitor Location Register
CG=Charging Gateway

Seguridad en comunicaciones móviles:

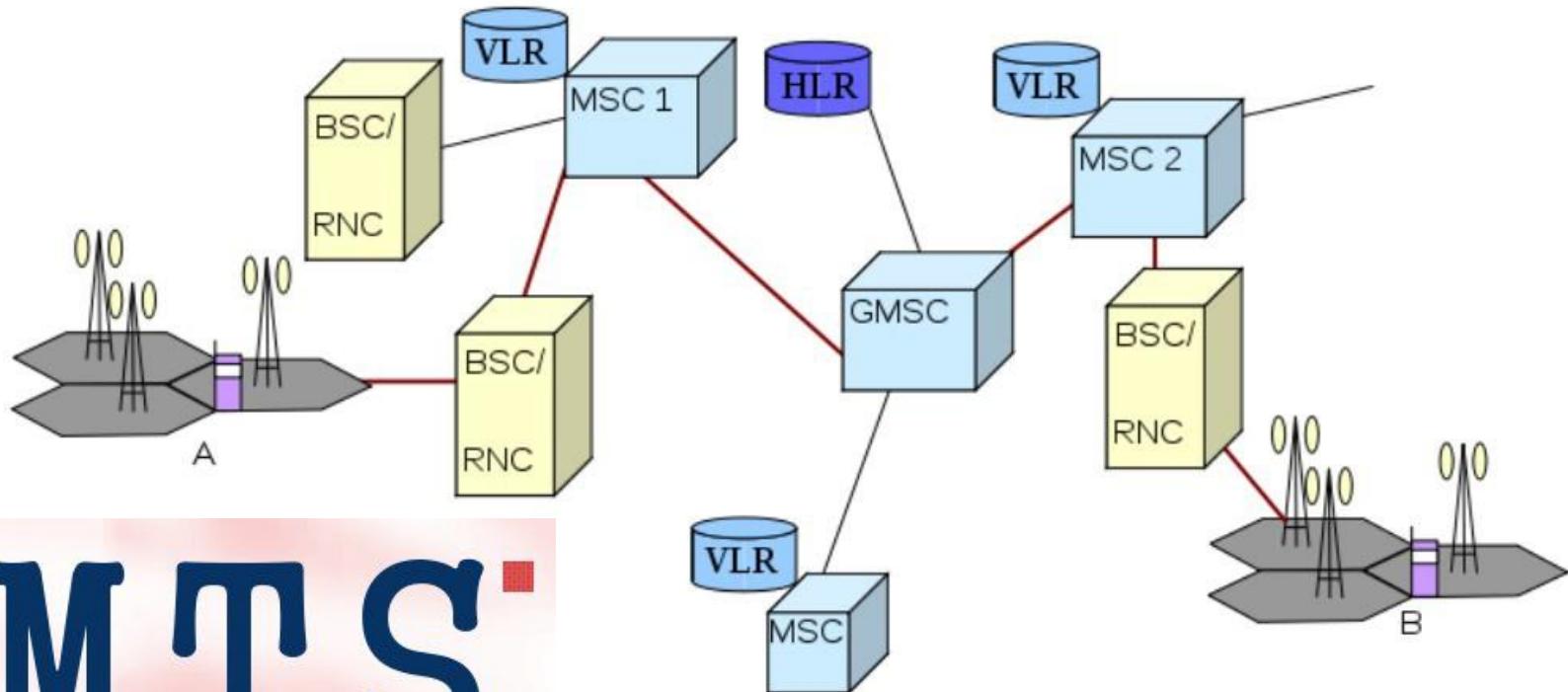
Posibles ataques en redes GPRS

- Ataques a las interfaces Gp:
 - Denegación de servicio.
 - Información sensible mediante escucha.
 - Modificación de datos.



Auditoría de comunicaciones móviles:

UMTS



U.M.T.S.

Auditoría de comunicaciones móviles:

Seguridad del protocolo UMTS:

- Seguridad en el acceso a la red.
- Seguridad en el dominio de la red.
- Seguridad en el dominio de usuario.
- Seguridad en el dominio de aplicación de la red.
- Visibilidad y configurabilidad de la seguridad.

Principales avances en seguridad conseguidos en UMTS:

- Los mensajes deben de ir protegidos en integridad. Con esta mejora, las estaciones falsas no podrían enviar mensajes firmados por una estación legítima.
- La criptografía 3G es más robusta que sus predecesoras y no ha sido descifrada en la actualidad.



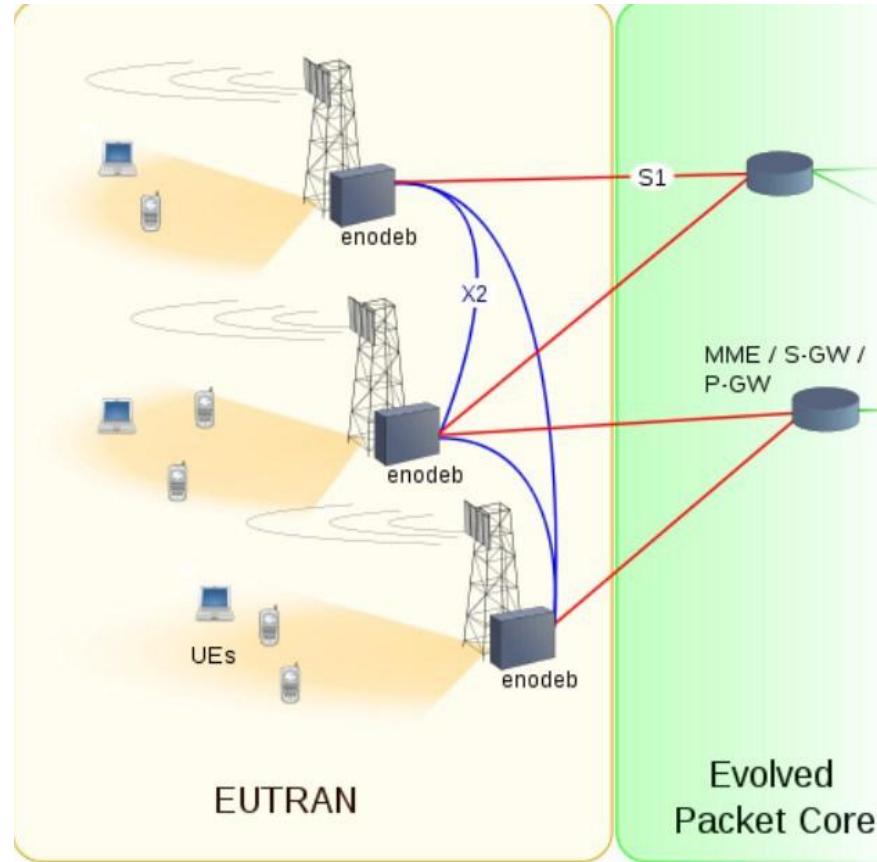
Auditoría de comunicaciones móviles:

Posibles ataques en redes UMTS

- Captura del IMSI
- Geolocalización
- Denegación de servicio
- Downgrade selectivo
- Ataque pasivo contra handover <https://www.cs.stevens.edu/~swetzel/publications/gsm.pdf>



Auditoría de comunicaciones móviles:



Auditoría de comunicaciones móviles:

Seguridad del protocolo 4G:

Estudio de las posibles amenazas, contramedidas y plan de seguridad para definir las especificaciones.

Este estudio se recoge en la norma 33.821 del 3GPP.

- <https://arxiv.org/pdf/1510.07563.pdf>

Posibles ataques en redes 4G:

- Downgrade a 3G



Auditoría de comunicaciones móviles:

Seguridad del protocolo 4G:

- Comparativa de ataques a la disponibilidad de la red:

Threat	Platform	Range	Difficulty	Impact
Smart Jamming	1 RF/SW-defined radio device	Local (cell/sector)	Low cost and complexity	High (but local)
Signaling amplification	Botnet of infected UEs	Large portion of a national network	Medium (10K-100K infected UEs)	High
HSS saturation	Botnet of infected UEs	Potentially global	Medium (10K-100K infected UEs, avoid attack throttled at EPC)	Very high
External DDoS	Botnet of infected UEs	DDoS target	Medium	Potentially high
APT	Insider	Local to global	Low	Very high

Auditoría de comunicaciones móviles:

Seguridad del protocolo 4G:



Artículo “Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems”

<http://www.tech-invite.com/3m33/tinv-3gpp-33-821.html>

Seguridad en comunicaciones móviles:

Posibles ataques de estación base falsa

- Denegación de servicio selectiva.
- Redirección de llamadas y tráfico.
- Suplantar número de origen en llamadas y SMS.
- Grabación de llamadas.
- Captura del contenido de cualquier SMS.
- Localización geográfica de dispositivo móviles.
- Explotación de un servicio vulnerable.



```
root@koala:~# airbase-ng -c 6 -a 00:1F:9F:FD:D9:A7 -e Bbox-3C3D8 -W 1 wlanmon0
15:02:22  Created tap interface ati
15:02:22  Trying to set MTU on ati to 1580
15:02:22  Access Point with BSSID 00:1F:9F:FD:A7 started.
15:02:58  Client 0C:84:DC:70:80:C7 associated (WPAP2;CCMP) to ESSID: 'Bbox-3C3D8'
15:02:59  Client 0C:84:DC:70:80:C7 associated (WPAP2;CCMP) to ESSID: 'Bbox-3C3D8'
15:03:00  Client 0C:84:DC:70:80:C7 associated (WPAP2;CCMP) to ESSID: 'Bbox-3C3D8'
15:03:01  Client 0C:84:DC:70:80:C7 associated (WPAP2;CCMP) to ESSID: 'Bbox-3C3D8'
15:03:02  Client 0C:84:DC:70:80:C7 associated (WPAP2;CCMP) to ESSID: 'Bbox-3C3D8'
15:03:03  Client 0C:84:DC:70:80:C7 associated (WPAP2;CCMP) to ESSID: 'Bbox-3C3D8'
15:03:03  Client 0C:84:DC:70:80:C7 associated (WPAP2;CCMP) to ESSID: 'Bbox-3C3D8'
15:03:04  Client 0C:84:DC:70:80:C7 associated (WPAP2;CCMP) to ESSID: 'Bbox-3C3D8'
15:03:05  Client 0C:84:DC:70:80:C7 associated (WPAP2;CCMP) to ESSID: 'Bbox-3C3D8'
15:03:06  Client 0C:84:DC:70:80:C7 associated (WPAP2;CCMP) to ESSID: 'Bbox-3C3D8'
15:03:09  Client 0C:84:DC:70:80:C7 associated (WPAP2;CCMP) to ESSID: 'Bbox-3C3D8'
15:03:10  Client 0C:84:DC:70:80:C7 associated (WPAP2;CCMP) to ESSID: 'Bbox-3C3D8'
15:03:11  Client 0C:84:DC:70:80:C7 associated (WPAP2;CCMP) to ESSID: 'Bbox-3C3D8'
15:03:12  Client 0C:84:DC:70:80:C7 associated (WPAP2;CCMP) to ESSID: 'Bbox-3C3D8'
15:03:13  Client 0C:84:DC:70:80:C7 associated (WPAP2;CCMP) to ESSID: 'Bbox-3C3D8'
15:04:31  Client 0C:84:DC:70:80:C7 associated (WPAP2;CCMP) to ESSID: 'Bbox-3C3D8'
15:04:32  Client 0C:84:DC:70:80:C7 associated (WPAP2;CCMP) to ESSID: 'Bbox-3C3D8'
15:04:33  Client 0C:84:DC:70:80:C7 associated (WPAP2;CCMP) to ESSID: 'Bbox-3C3D8'
15:04:34  Client 0C:84:DC:70:80:C7 associated (WPAP2;CCMP) to ESSID: 'Bbox-3C3D8'
15:04:35  Client 0C:84:DC:70:80:C7 associated (WPAP2;CCMP) to ESSID: 'Bbox-3C3D8'
15:04:36  Client 0C:84:DC:70:80:C7 associated (WPAP2;CCMP) to ESSID: 'Bbox-3C3D8'
15:04:36  Client 0C:84:DC:70:80:C7 associated (WPAP2;CCMP) to ESSID: 'Bbox-3C3D8'
15:04:36  Client 0C:84:DC:70:80:C7 associated (WPAP2;CCMP) to ESSID: 'Bbox-3C3D8'
15:04:37  Client 0C:84:DC:70:80:C7 associated (WPAP2;CCMP) to ESSID: 'Bbox-3C3D8'
15:04:38  Client 0C:84:DC:70:80:C7 associated (WPAP2;CCMP) to ESSID: 'Bbox-3C3D8'
15:04:39  Client 0C:84:DC:70:80:C7 associated (WPAP2;CCMP) to ESSID: 'Bbox-3C3D8'
15:04:40  Client 0C:84:DC:70:80:C7 associated (WPAP2;CCMP) to ESSID: 'Bbox-3C3D8'
15:04:41  Client 0C:84:DC:70:80:C7 associated (WPAP2;CCMP) to ESSID: 'Bbox-3C3D8'
```

Seguridad en comunicaciones móviles:

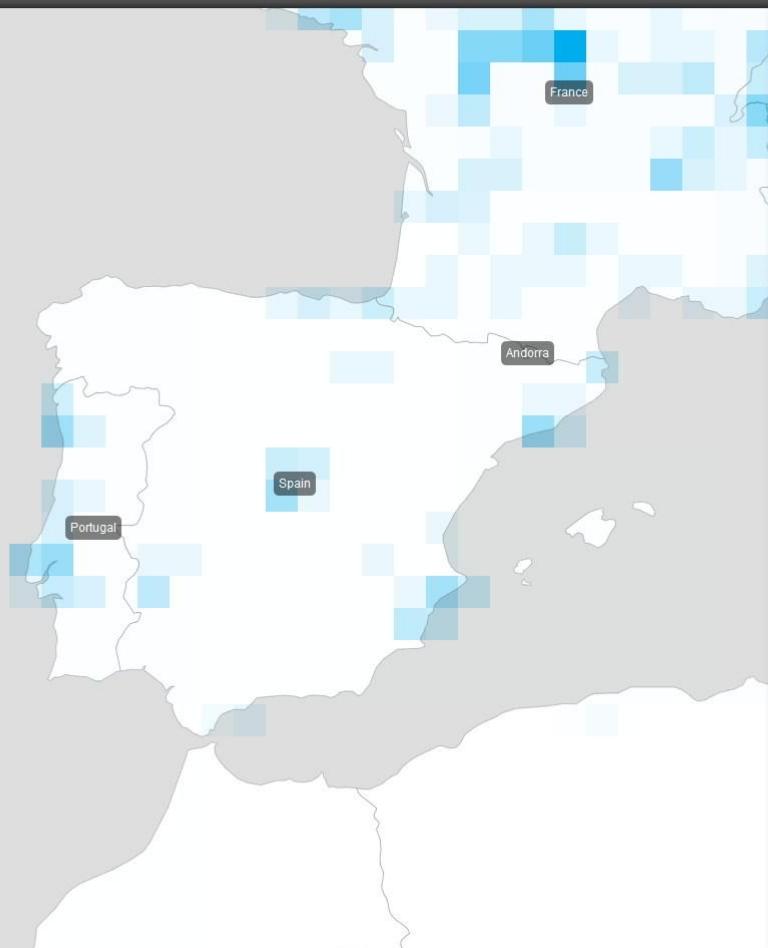
https://gs mmap.org/assets/pdfs/gs mmap.org-country_report-Spain-2018-06.pdf



All 3G networks in Spain implement sufficient 3G intercept protection.

Users of Orange are not sufficiently protected from 2G intercept. In all 2G networks, user impersonation is possible with simple tools. Movistar and Yoigo allow user tracking.

Operator		Protection dimension (higher means better)		
		Intercept	Impersonation	Tracking
Movistar	2G	53%	36%	11%
	3G	90%	-	
Orange	2G	46%	29%	63%
	3G	86%	-	
Vodafone	2G	59%	42%	81%
	3G	86%	-	
Yoigo	2G	53%	31%	44%
	3G	82%	-	



Spain

Country report (2018-06)

Vodafone

Orange

Yoigo

Movistar

Intercept

Impersonation

Tracking

USIM prevalence

2G both 3G



Auditoría de comunicaciones móviles:

Seguridad del protocolo 5G:



<https://www.itproportal.com/news/itu-reveals-5g-specs-including-20gbps-download-speeds-and-4ms-latency/>

http://www.3gpp.org/news-events/3gpp-news/1929-nsa_nr_5g

https://www.etsi.org/deliver/etsi_tr/138900_138999/138913/14.03.00_60/tr_138913v140300p.pdf

<http://www.tech-invite.com/3m33/tinv-3gpp-33.html>

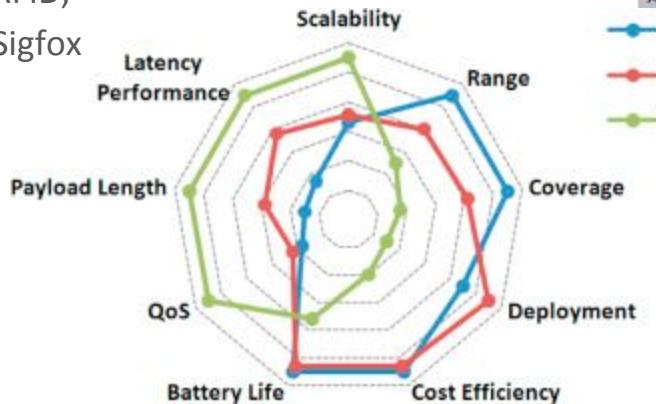
Auditoría de comunicaciones inalámbricas:

Seguridad en comunicaciones inalámbricas

- WiFi,
- Bluetooth,
- ZigBee,
- RFID,
- Sigfox

	SIGFOX	LoRa	clean slate	NB LTE-M Rel. 13	LTE-M Rel. 12/13	EC-GSM Rel. 13	5G (targets)
Range (outdoor) MCL	<13km 160 dB	<11km 157 dB	<15km 164 dB	<15km 164 dB	<11km 156 dB	<15km 164 dB	<15km 164 dB
Spectrum Bandwidth	Unlicensed 900MHz 100Hz	Unlicensed 900MHz <500kHz	Licensed 7-900MHz 200kHz or dedicated	Licensed 7-900MHz 200kHz or shared	Licensed 7-900MHz 1.4 MHz or shared	Licensed 8-900MHz 2.4 MHz or shared	Licensed 7-900MHz shared
Data rate	<100bps	<10 kbps	<50kbps	<150kbps	<1 Mbps	10kbps	<1 Mbps
Battery life	>10 years	>10 years	>10 years	>10 years	>10 years	>10 years	>10 years
Availability	Today	Today	2016	2016	2016	2016	beyond 2020

LPWA IoT connectivity overview



Auditoría de comunicaciones inalámbricas:



Seguridad en comunicaciones inalámbricas (WiFi)

Tipo	Frecuencia (GHz)	Velocidad (Mbps)	Rango (metros)
802.11a	5	54	23
802.11b	2,4	11	45
802.11g	2,4	11	45
802.11n	2,4/5	54	30
802.11ac	2,4/5	433-3,69 Gbps	30

Auditoría de comunicaciones inalámbricas:



Protocolo	Net bit rate [Mbps]	Frecuencia Operativa [GHz]	Compatibilidad	Channel Widths [Mhz]
802.11b	< 11	2,4	Compatible con 802.11g	22
802.11a	< 54	5	Incompatible con el resto	22
802.11g	< 54	2,4	Compatible con 802.11b (limitando redes g a b)	22
802.11g (Super-G)	< 108	2,4	Compatible con 802.11g	22
802.11n	< 600	2,4 y 5	Compatible con g en configuraciones MIMO	(10), 20, 40
802.11ac	< 1300	5	MIMO multi usuario	20, 40, 80, (160)

Auditoría de comunicaciones inalámbricas:



Seguridad en comunicaciones inalámbricas (WiFi)

<https://www.aircrack-ng.org/doku.php?id=Main>



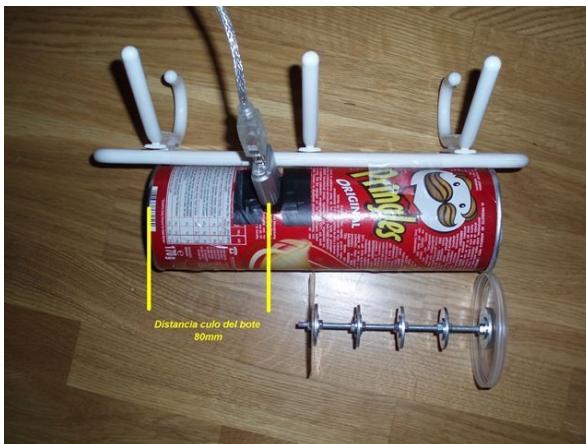
Auditoría de comunicaciones inalámbricas:



Auditoría en comunicaciones inalámbricas (WiFi)

<https://www.aircrack-ng.org/doku.php?id=es:aireplay-ng>

<https://www.aircrack-ng.org/doku.php?id=es:airodump-ng>



The screenshot shows the Wireshark 'Capture Interfaces' dialog box. It lists several network interfaces:

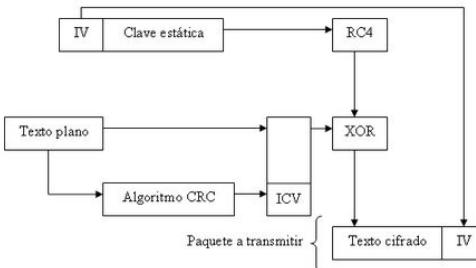
Interface	Traffic	Link-layer He	Promiscuous	Snaplen (B)	Buffer
> VirtualBox Host-Only Network #2	Ethernet	<input checked="" type="checkbox"/>	default	2	
> VPN - VPN Client	Ethernet	<input checked="" type="checkbox"/>	default	2	
> Ethernet 2	Ethernet	<input checked="" type="checkbox"/>	default	2	
> Wi-Fi	Ethernet	<input checked="" type="checkbox"/>	default	2	
> Ethernet	Ethernet	<input checked="" type="checkbox"/>	default	2	
> Conexión de área local* 3	Ethernet	<input checked="" type="checkbox"/>	default	2	

At the bottom, there is a checkbox labeled "Enable promiscuous mode on all interfaces" which is checked. Below it is a "Capture filter for selected interfaces:" field with the placeholder "Enter a capture filter ...".

Auditoría de comunicaciones inalámbricas:

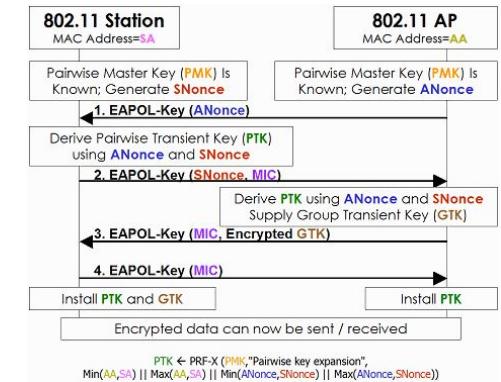
Seguridad en comunicaciones inalámbricas (WiFi)

- Ataques a redes WEP:
 - Ataque ChopChop de Korek.
- Ataques a redes WPA/WPA2
 - <https://www.krackattacks.com>

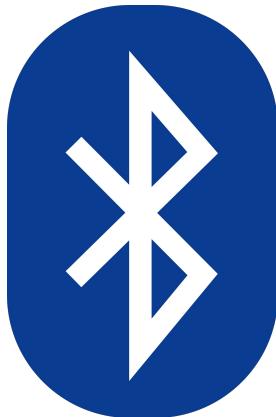


Artículo de la investigación: <https://papers.mathyvanhoef.com/ccs2017.pdf>

Herramienta utilizada en la demostración y utilizable para <https://github.com/vanhoefm/krackattacks-scripts> <https://github.com/kristate/krackinfo>



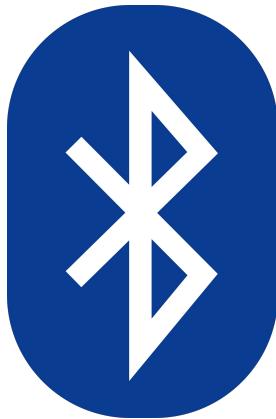
Auditoría de comunicaciones inalámbricas:



Seguridad en comunicaciones inalámbricas **Bluetooth**

- Bluelog: escáner y monitor de tráfico bluetooth <https://tools.kali.org/wireless-attacks/bluelog>
- BlueMaho: Herramienta de testeo de vulnerabilidades <https://tools.kali.org/wireless-attacks/bluemaho>
- Bluepot: Honeypot de bluetooth <https://tools.kali.org/wireless-attacks/bluepot>
- BlueRanger: Localizador de dispositivos <https://tools.kali.org/wireless-attacks/blueranger>
- Bluesnarfer: Herramienta para la realización de ataques Bluesnarfing (explicado más adelante) <https://tools.kali.org/wireless-attacks/bluesnarfer>
- Spooftooth: Herramienta para realizar clonados de la información del dispositivo o suplantaciones de identidad <https://tools.kali.org/wireless-attacks/spooftooth>

Auditoría de comunicaciones inalámbricas:



Posibles ataques en comunicaciones inalámbricas **Bluetooth**

- Bluejacking
- Bluesnarfing https://www.youtube.com/watch?v=jF9x61Rz_QI
- Bluebugging
- Bluetooth Honeypots <https://github.com/andrewmichaelsmith/bluepot>
- BlueBorne <https://www.armis.com/blueborne/>



A new attack vector exposes almost every connected device.

Auditoría de comunicaciones inalámbricas:

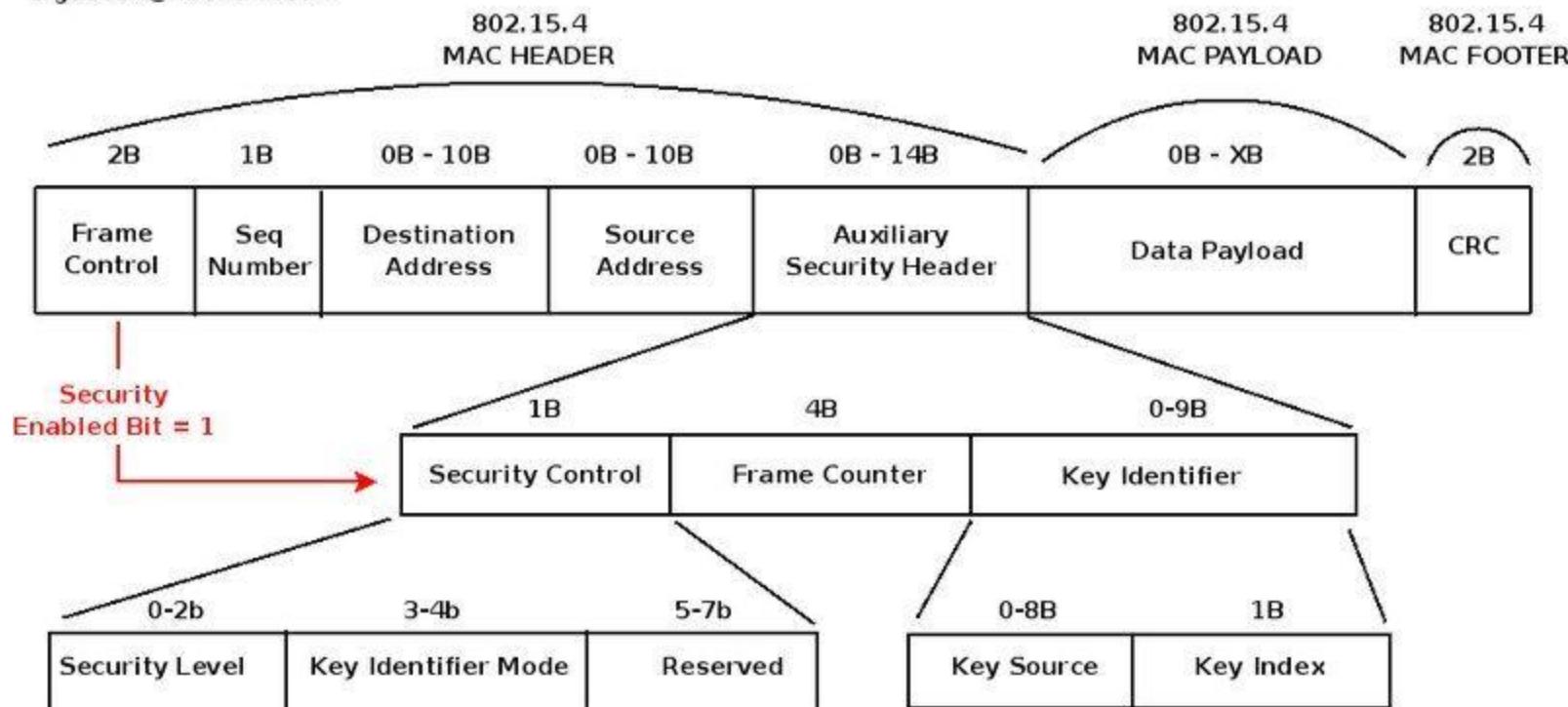
- ZigBee



Security in the IEEE 802.15.4 MAC FRAME

<http://www.sensor-networks.org>

Author: David Gascón
d.gascon@libelium.com



Auditoría de WIRELESS: Seguridad en comunicaciones inalámbricas.

Para que a nivel 802.15.4 se pueda implementar seguridad, son necesarios una serie de campos en la cabecera de la trama.

- Para activar la seguridad a nivel MAC es necesario que el bit “Security Enabled” del campo “Frame Control” sea a 1.
- Si este campo se encuentra a 1, el campo “Auxiliary Security Header” de la cabecera se activa, permitiendo que la política de seguridad implemente cifrado AES según el nivel indicado en el campo “Security Level”.

<https://arxiv.org/pdf/1205.6678.pdf>

Auditoría de comunicaciones inalámbricas:

Posibles ataques en comunicaciones inalámbricas **ZigBee 802.15.4**

- Claves por defecto
- Killer Bee <https://github.com/riverloopsec/killerbee>

Estándar	ZigBee/802.15.4	Bluetooth	Wi-Fi	UWB
IEEE	802.15.4	802.15.1	802.11 a/b/g	802.15.3a
Banda de frecuencia	868/915 MHz ; 2,4 GHz	2,4GHz	2,4GHz ; 5GHz	3,1 - 10,6 GHz
Máxima tasa de transmisión	250 Kbps	1Mbps	54 Mbps	110 Mbps
Rango de alcance	10 - 20 m	10 - 100 m	100 m	10 m
Número de canales RF	1/10 ; 16	79	14 (2,4 GHz)	1-15
Ancho de banda de canal	0,3/0,6 MHz ; 2 MHz	1 MHz	22 MHz	500 MHz - 7,5 GHz

Auditoría de comunicaciones inalámbricas:

Seguridad en comunicaciones inalámbricas

- RFID

<https://es.wikipedia.org/wiki/RFID>



Guía sobre seguridad y privacidad
de la tecnología RFID



Auditoría de comunicaciones inalámbricas:

Posibles ataques en comunicaciones inalámbricas **RFID**:

- Robo contactless
- Clonado
- Rompiendo el cifrado

Contramedida:

- Bolsas de jaula de **Faraday**

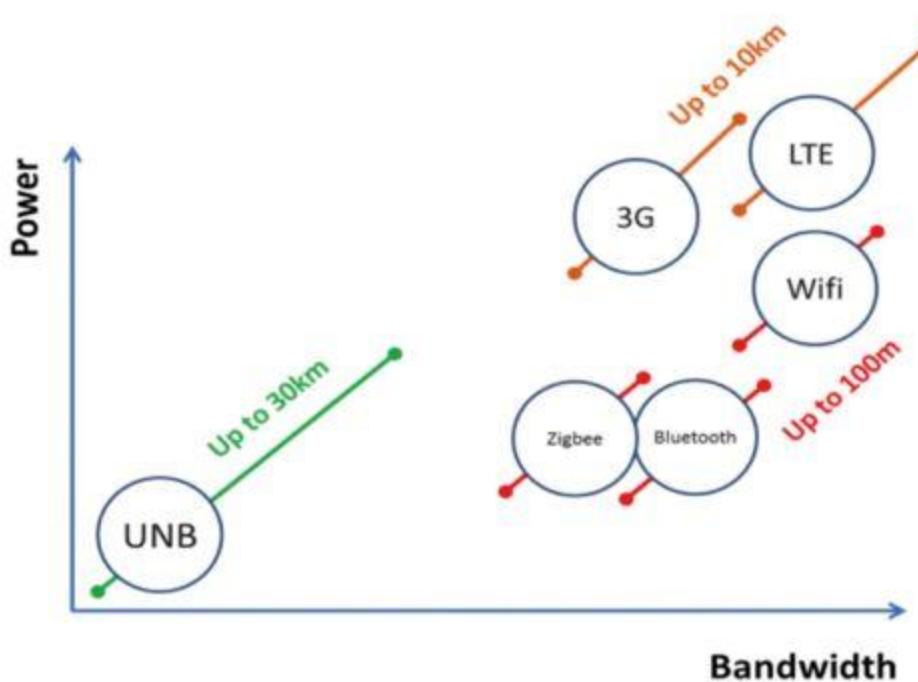


Auditoría de comunicaciones inalámbricas:

Seguridad en comunicaciones inalámbricas

- Sigfox





Auditoría de WIRELESS: Seguridad en comunicaciones inalámbricas.

Ataques de capa física:

- Jamming
- Tampering

Ataques en la capa de control de acceso al medio:

- Collision attack,
- Exhaustion attack
- Unfairness attack



Auditoría de WIRELESS: Seguridad en comunicaciones inalámbricas.

Ataques en la **capa de red**:

- Neglect and greed,
- Homing,
- Misdirection,
- Sinkholes,
- Sybil,
- Wormhole,
- Hello flood,
- Selective forwarding,
- Flooding,
- Node replication attack,
- Acknowledgement spoofing,
- Sniffing attack.



Auditoría de WIRELESS: Seguridad en comunicaciones inalámbricas.

Ataques en la **capa de transporte**:

- Session Hijacking
- SYN flooding.

Ataques en la **capa de aplicación**:

- ataque de corrupción de datos
- ataque de rechazo (repudiation)



http://www



World Wide Web

The WorldWideWeb (W3) is a wide-area [hypermedia](#) information retrieval initiative aiming to give universal access to a large universe of documents.

Everything there is online about W3 is linked directly or indirectly to this document, including an [executive summary](#) of the project, [Mailing lists](#) , [Policy](#) , November's [W3 news](#) , [Frequently Asked Questions](#) .

What's out there?

Pointers to the world's online information, [subjects](#) , [W3 servers](#), etc.

Help

on the browser you are using

Software Products

A list of W3 project components and their current state. (e.g. [Line Mode](#) ,X11 [Viola](#) , [NeXTStep](#) , [Servers](#) , [Tools](#) , [Mail robot](#) , [Library](#))

Technical

Details of protocols, formats, program internals etc

Bibliography

Paper documentation on W3 and references.

People

A list of some people involved in the project.

History

A summary of the history of the project.

How can I help ?

If you would like to support the web..

Getting code

Getting the code by [anonymous FTP](#) , etc.

Username

' OR 1=1; /*

Password

*/--

Log In

Pentesting WEB:

Estándar para la ejecución de pruebas de penetración <http://www.pentest-standard.org/>

- OWTF (Offensive Web Testing Framework)
https://www.owasp.org/index.php/OWASP_OWTF es el marco basado en Python para pentesting web. <https://github.com/owtf/owtf>
- ZAP (OWASP Zed Attack Proxy)
https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project es el framework de pruebas de penetración para Aplicaciones Web, disponible para Linux, Mac OS y Windows. <https://github.com/zaproxy/zaproxy/wiki/Downloads>
- PTF (Penetration Testers Framework) <https://github.com/trustedsec/ptf>

OWASP Zed Attack Proxy Project +

https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

Log in Request account

Page Discussion Read View source View history Search

OWASP Zed Attack Proxy Project

Main Screenshots Talks News ZAP Gear Supporters Functionality Features Languages Roadmap Get Involved

FLAGSHIP mature projects

Review this project.

The OWASP Zed Attack Proxy (ZAP) is one of the world's most popular free security tools and is actively maintained by hundreds of international volunteers*. It can help you automatically find security vulnerabilities in your web applications while you are developing and testing your applications. Its also a great tool for experienced pentesters to use for manual security testing.

ZAP 2.7.0 is now available!

[Download ZAP](#)

Please help us to make ZAP even better for you by answering the [ZAP User Questionnaire](#)!

For a quick overview of ZAP and an introduction to the [official ZAP Jenkins plugin](#) see these tutorial videos on YouTube:



Quick Download
[Download OWASP ZAP!](#)

Donate to ZAP
[Donate](#)

News and Events
Please see the [News](#) and [Talks](#) tabs

Change Log

- [zaproxy](#)
- [zap-extensions](#)

Code Repo

- [zaproxy](#)
- [zap-extensions](#)

Email List
Questions? Please ask on the [ZAP User Group](#)

Project Leader
Project Leader
Simon Bennetts @
Co-Project Leaders

Home About OWASP Acknowledgements Advertising AppSec Events Supporting Partners Books Brand Resources Chapters Donate to OWASP Downloads Funding Governance Initiatives Mailing Lists Membership Merchandise Presentations Press Projects Video Reference Activities Attacks Code Snippets Controls Glossary How To... Java Project .NET Project Principles Technologies Threat Agents Vulnerabilities Tools What links here Related changes Special pages Printable version Permanent link Page information

Modo estándar

Sitios +

Contexts

- Sitios
 - http://192.168.21.12
 - http://192.168.21.13
 - https://192.168.21.13

Bienvenido al OWASP Zed Attack Proxy (ZAP)

ZAP es una herramienta para pruebas de penetración, de fácil uso y con múltiples componentes, para encontrar vulnerabilidades en aplicaciones web.

Ten en cuenta que sólo debes atacar aplicaciones para las cuales se ha sido previamente autorizado.

Para probar una aplicación rápidamente, introduzca la URL y presione 'Atacar'.

URL a atacar: http://

Progreso: No iniciado

Para un análisis más en profundidad de la prueba se debe explorar la aplicación mediante pruebas de regresión automatizadas navegando a través ZAP como proxy.



Historia Buscar Alertas Salida +

Alertas (7)

- X-Frame-Options Header Not Set (142)
- Cookie Without Secure Flag (8)
- Incomplete or No Cache-control and Pragma HTTP Header Set (59)
- Password Autocomplete in Browser (8)
- Private IP Disclosure (16)
- Web Browser XSS Protection Not Enabled (142)
- X-Content-Type-Options Header Missing (142)

X-Frame-Options Header Not Set

URL: http://192.168.21.13/

Riesgo: Medium

Confianza: Medium

Parámetro:

Ataque:

Evidencia:

CWE ID: 16

WASC ID: 15

Origen: Desconocido

Descripción:

X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.

Otra info:

At "High" threshold this scanner will not alert on client or server error responses.

Solución:

Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web

Pentesting WEB:



- **Burp Suite** <https://portswigger.net/burp/> es una plataforma integrada para realizar pruebas de seguridad de aplicaciones web interceptando y modificando peticiones web.



El

addon

Foxy

Proxy

<https://addons.mozilla.org/en-US/firefox/addon/foxyproxy-standard/> para Firefox
(también está disponible para Chrome) nos facilitará gestionar las conexiones derivadas.

Pentesting WEB:

- **Nikto** <https://cirt.net/nikto2> escáner de vulnerabilidades al servidor de aplicaciones web <https://github.com/sullo/nikto>
- **W3af** (Web Application Attack and Audit Framework) <http://w3af.org/> es el ataque a la aplicación web y marco de auditoría, para identificar y explotar inyecciones SQL <https://github.com/andresriancho/w3af>
- **Commix** <http://www.commixproject.com/> es una herramienta automatizada de inyección y explotación de comandos del sistema operativo todo en uno. <https://gbhackers.com/commix-automated-all-in-one-os-command-injection-and-exploitation-tool/>

Pentesting WEB:

- **SQLMap** <http://sqlmap.org/> es una herramienta de toma de control de la base de datos e inyección SQL automática.
<https://gbhackers.com/sqlmap-detecting-exploiting-sql-injection/>
- **NoSQLMap** <https://github.com/codingo/NoSQLMap> es una herramienta automatizada para auditar ataques de inyección y explotación de aplicaciones web NoSQL.
- **SQLNinja** <http://sqlninja.sourceforge.net/> es una herramienta de inyección y adquisición de SQL Server. <https://kali-linux.net/article/sqlninja/>

Pentesting WEB:

- **Infection Monkey** <http://www.guardicore.com/infectionmonkey/> es una herramienta semiautomática para pruebas de intrusión, simulando un atacante humano <https://github.com/guardicore/monkey>
- **Arachni** <http://www.arachni-scanner.com/> es un framework de escáner de seguridad para aplicaciones web disponible para Linux, Mac OS y Windows.
- **TIDoS** <https://github.com/theInfectedDrake/TIDoS-Framework> es un framework ofensivo basado en Python de pruebas de penetración para webapp.

Colección de recursos interesantes <https://github.com/infoslack/awesome-web-hacking>

OLD MAN YELLS AT CLOUD



Older Abraham Lincoln
in a cave under a falling bridge

I said give me a pencil
we're old and we're stiff
just had a heart attack
and it's just KATHY
d'oh! d'oh! [sic] I did
so I'm gonna write a
widely known poem
about it
it's about
me
I'm the mother
I'm the mother
I'm the mother

ORACLE CLOUD

Engineered For Heroes

www.oracle.com/Ironman3



TM & © 2013 MARVEL. www.marvel.com

MARVEL

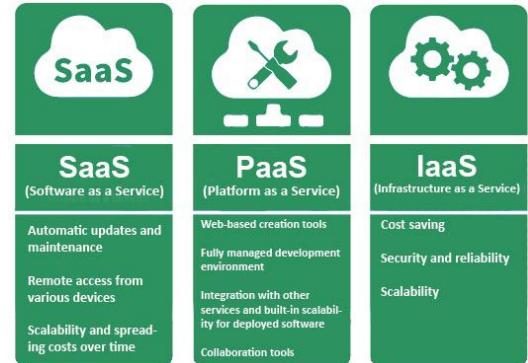
MARVEL
IRON MAN 3

ORACLE®

CLOUD:

Amenazas a la seguridad de la Nube:

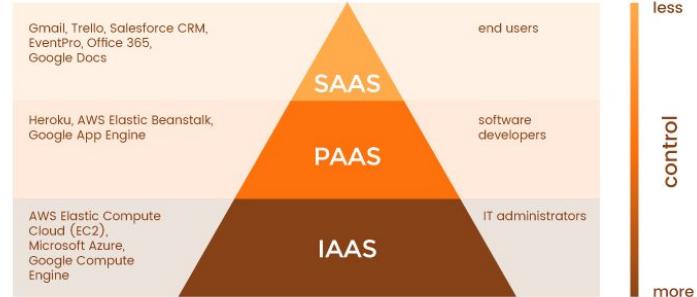
- Fugas de información (error humano, fallo en la configuración, ataque).
- Información sensible (salud, finanzas, propiedad intelectual y secreto comercial).
- Impacto: incumplimiento legal y multas, imagen pública y coste de recuperación.
- Control de acceso deficiente.
- Contraseñas débiles, repetidas ó fáciles de adivinar.
- API ó interfaces poco seguras.
- Vulnerabilidades del sistema.
- Secuestro o robo de cuenta (phishing, keylogger, ataque de hombre en el medio).
- trabajadores malintencionados.
- Amenazas Persistentes Avanzadas (APT) ataques sofisticados que perduran en el tiempo.
- Pérdida de datos, destrucción y borrado.
- Uso abusivo y actividad delictiva (IP o rango compartido), reputación, blacklist, etc. (Vecindario IP y SEO).
- Ataques de Denegación de servicio.
- Uso compartido de recursos (Procesador, RAM y almacenamiento).



CLOUD:

Implementación de mejoras a la seguridad Cloud:

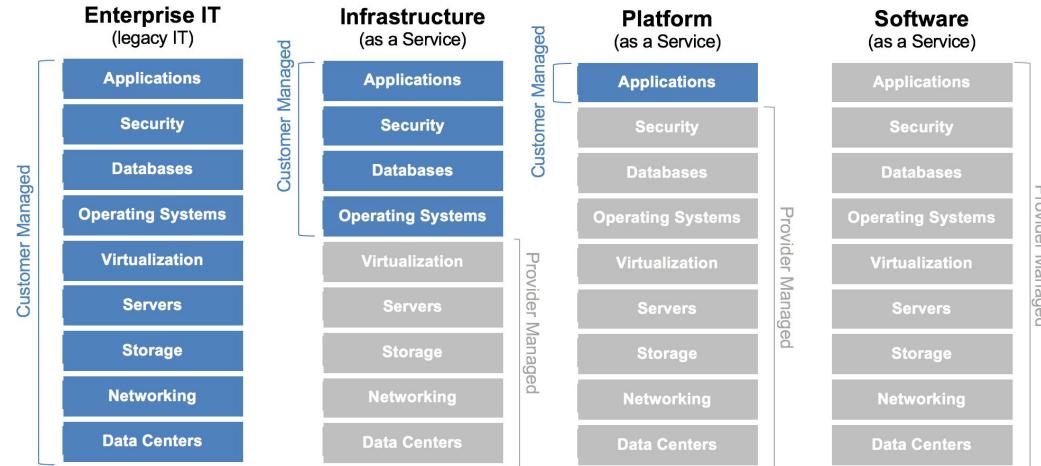
- Cifrado seguro.
- Mejora del control de accesos, ej. autenticación en dos pasos.
- Parcheo, escaneo de vulnerabilidad y auditoría.
- Formación al usuario final.
- Segregación completa de accesos y privilegios.
- Monitorización, seguimiento y auditoría.
- Backup y restore.
- Aislamiento de recursos críticos y detección de intrusiones. (HIDS basados en hosts, NIDS basados en red).



CLOUD:

IaaS: Infraestructura como servicio.

- <https://aws.amazon.com/s3/>
- <https://aws.amazon.com/es/ec2>
- <https://cloud.google.com/compute/>

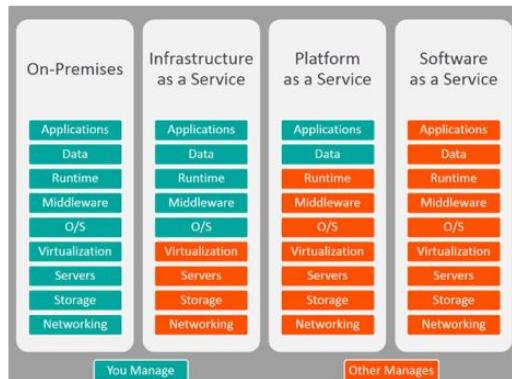


PaaS: Plataforma de Cliente y acceso a la Aplicación.

- Google App Engine <https://cloud.google.com/appengine/docs/>
- Microsoft Azure <https://azure.microsoft.com/es-es/overview/azure-stack/>

SaaS: Tan sólo el cliente.

- Dropbox <https://www.dropbox.com>
- Box <https://www.box.com>
- G Suite [https://gsuite.google.com/](https://gsuite.google.com)
- Office 365 <https://www.office.com/>



	AWS	Microsoft Azure	Google	IBM
Compute	EC2	Virtual Machines	Compute Engine App Engine	Bare Metal Servers Virtual Servers Power8
Storage	S3 EBS EFS Glacier	Blob Storage Queue Storage File Storage Disk Storage	Cloud Storage Persistent Disk	Object Storage Block Storage File Storage Mass Storage Servers
Backup and Disaster Recovery		Backup Site Recovery		Backup
Database and Data warehouse	Aurora RDS DynamoDB Redshift	Data Lake Store SQL Database DocumentDB Table Storage SQL Data Warehouse	Cloud SQL Cloud Bigtable Cloud Spanner Cloud Datastore	Data Services Big Data Hosting MongoDB Hosting Riak Hosting
In-Memory Technology	ElastiCache	Redis Cache		
Containers	Container Registry Container Service	Container Registry Container Service	Container Engine Container Registry Container Builder	Containers
Serverless/FaaS	Lambda	Functions	Cloud Functions	OpenWhisk
Analytics	Athena EMR Kinesis	HDIInsight Stream Analytics	BigQuery Cloud Dataflow Cloud Dataproc Cloud Datalab	Analytics Services Cloudera Hosting
Artificial Intelligence	Lex Polly Rekognition Machine Learning	Machine Learning Cognitive Services Bot Service Data Lake Analytics	Cloud Machine Learning Engine Cloud Natural Language API Cloud Speech API Cloud Translation API Cloud Vision API	Watson
Internet of Things	IoT Platform Greengrass	IoT Hub Event Hubs		Internet of Things

	Storage	Price per Month	Desktop App	Simultaneous Editing	Web Editor	Mobile Options
 OneDrive	15 GB 100 GB 200 GB 1 TB (Biz)	Free \$1.99 \$3.99 \$2.50/User				All
 Dropbox	2 GB 100 GB 200 GB 500 GB Unlimited	Free \$10.99 \$21.99 \$54.99 \$17/User				Android & iOS
 Google Drive	15 GB 100 GB 1 TB 10 TB 20 TB 30 TB	Free \$1.99 \$9.99 \$99.99 \$199.99 \$299.99				Android & iOS

10 Free Cloud Storage Services Comparison Chart



SkyDrive



box



bitcasa



cloud
drive
amazon

ADrive

	Google Drive	SkyDrive	SpiderOak	box	SugarSync	bitcasa	mozy	Dropbox	cloud drive amazon	ADrive
Free storage	5 GB	7 GB	2 GB	5 GB	5 GB	unlimited (beta)	2 GB	2 GB	5 GB	50 GB
Sync	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗
Platforms	Windows Mac	Windows Mac	Windows Mac Linux Ubuntu	free web only	Windows Mac	Windows Mac	Windows Mac	Windows Mac Linux Ubuntu	Windows Mac	Linux paid user only
Paid storage 100 GB / month	\$ 4.99	\$ 19.99	\$ 9.99	\$ 19.99 50 GB	\$ 14.99	free while in beta	\$ 9.99 115 GB	\$ 19.99	\$ 8.33 billed annually	\$ 13.95
Encryption local server side	✗ ✓	✗ ✓	✓ ✓	✗ ✓	✗ ✓	✗ ✓	✓ ✓	✗ ✓	✗ ✓	✗ paid only

Platform-specific app availability

ars technica

	Windows	OS X	Linux	Android	iOS	Windows Phone	Web
 Microsoft SkyDrive				Third-party clients			
 Drive							
 iCloud							
 Dropbox							
 SugarSync							
 box							
 SPIDERoAK							



Nuestras gamas de servidores

Hosting

Configuraciones asequibles y polivalentes para alojar sitios web o tiendas online.

Procesadores Xeon-D de hasta 8 cores

[Descubrir la gama](#)

Desde:
54,99 € + IVA (66,54 € IVA incl.)

[Ver los precios](#)

Infraestructura

Red privada vRack incluida y potentes procesadores para construir infraestructuras de múltiples niveles.

Desde 16 GB hasta 512 GB de RAM

[Descubrir la gama](#)

Desde:
64,99 € + IVA (78,64 € IVA incl.)

[Ver los precios](#)

Enterprise

Servidores para alojar aplicaciones web o consolidar entornos virtuales.

Procesadores de 4 a 28 cores por servidor

[Descubrir la gama](#)

Desde:
49,99 € + IVA (60,49 € IVA incl.)

[Ver los precios](#)

Almacenamiento

Servidores para archivado, backup o almacenamiento distribuido.

Red privada vRack, hasta 216 TB de espacio en disco

[Descubrir la gama](#)

Desde:
79,99 € + IVA (96,79 € IVA incl.)

[Ver los precios](#)

Servidores Alta Gama

Las configuraciones más potentes y totalmente personalizables, especialmente diseñadas para entornos críticos o intensivos.

Hasta 36 cores por CPU y 1 TB de RAM

[Descubrir la gama](#)

Desde:
86,99 € + IVA (105,26 € IVA incl.)

[Ver los precios](#)

GAME

Protección anti-DDoS GAME incluida para alojar y proteger sus partidas de juego online.

Hasta 5 GHz en modo «turbo»

[Descubrir la gama](#)

Desde:
54,99 € + IVA (66,54 € IVA incl.)

[Ver los precios](#)

Servidores Privados Virtuales (VPS) OVH

Rendimiento, seguridad y disponibilidad para todos los usos

Nuestras tres gamas: VPS SSD, VPS Cloud y VPS Cloud RAM

VPS SSD

SLA del 99,95%
VPS potente y accesible

Suscripción anual desde:
2,99 €
/mes + IVA (3,62 € IVA incl.)*

Seleccionar

VPS Cloud

SLA 99,99 %
VPS con disponibilidad garantizada

Suscripción anual desde:
7,99 €
/mes + IVA (9,67 € IVA incl.)*

Seleccionar

VPS Cloud RAM

SLA 99,99 %
VPS con mucha RAM

Suscripción anual desde:
7,99 €
/mes + IVA (9,67 € IVA incl.)*

Seleccionar

*Esta oferta promocional permite disfrutar de un descuento de 1,00 €/mes en el precio (IVA no incl.) de su VPS SSD2, VPS SSD3, VPS CLOUD 1, VPS CLOUD 2, VPS CLOUD 3, VPS CLOUD RAM 1, VPS CLOUD RAM 2 y VPS CLOUD RAM 3 (gama VPS SSD Discover no incluida), al contratar durante al menos doce (12) meses un VPS de OVH. Aplicable a pedidos realizados entre el 27/05/2018 a las 15:00 y el 31/12/2018 a las 15:00 (hora de Madrid). En caso de litigio, dará fe la hora del registro del pedido por OVH. Renovación del VPS al precio indicado en la fecha de renovación en www.ovh.es. Contratación sujeta a la aceptación previa de las condiciones contractuales de OVH.

Digital Forensics



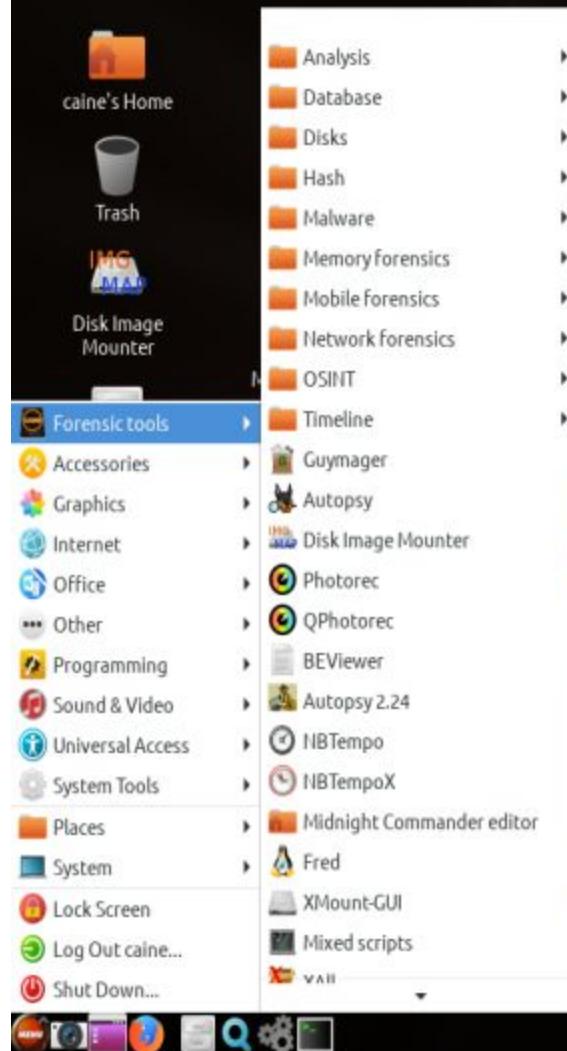


mount_points

log2timeline-
cheatsheet.pdfMemory Forensics
Cheat Sheet .pdfwindows-to-unix-
cheatsheet.pdfnetwork-forensics-
cheatsheet.pdfBrochure_
SANSDFIR.pdfSIFT-Cheat-Sheet.
pdfPoster_Fall_2013_
Evidence_Of.pdfPoster_2014_Find_
Evil.pdf

```
sansforensics@siftworkstation: ~
sansforensics@siftworkstation:~$ 
```





Auditoría Forense:

El borrado de huellas es la última de las fases en un ataque. La auditoría forense digital permite investigar la trazabilidad y recuperar las evidencias.

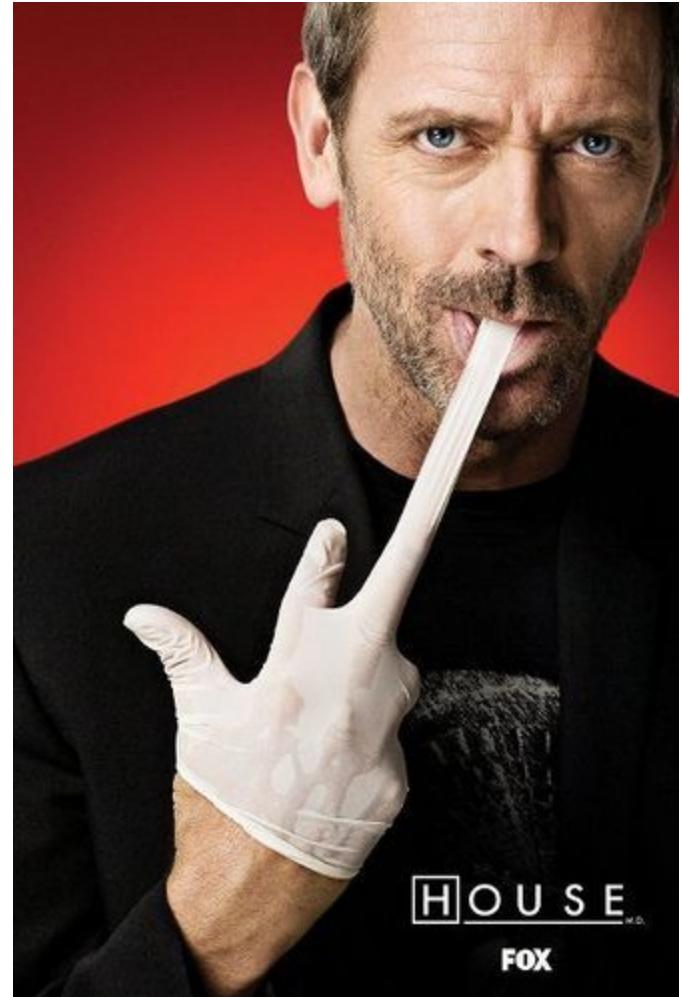
http://www.forensicswiki.org/wiki/Main_Page

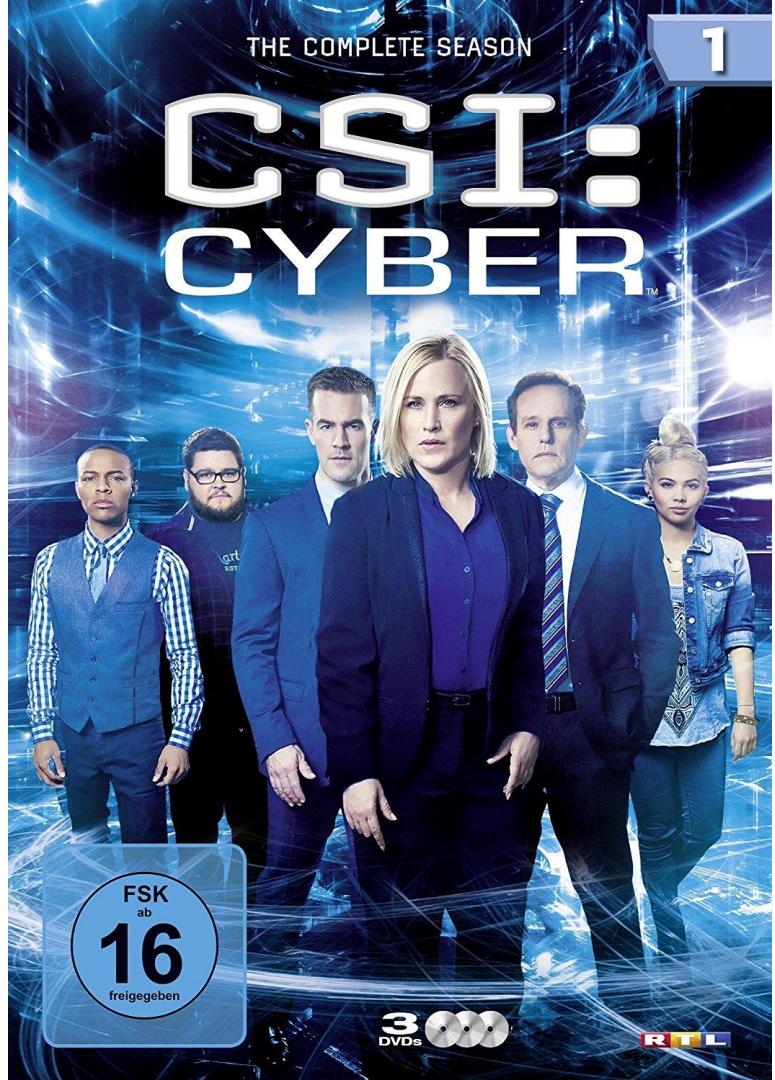
- **SANS SIFT** (SANS Investigative Forensic Toolkit)
<https://digital-forensics.sans.org/community/downloads> es una imagen ova e iso de estación de trabajo para forense digital basada en ubuntu.
<https://digital-forensics.sans.org/community/cheat-sheets>
- **Caine** <https://www.caine-live.net/> es una imagen iso de distribución Linux basada en Ubuntu con herramientas pre-instaladas para informática forense. Otra opción basada en Ubuntu es Dreft <http://www.deftlinux.net/>

Auditoría Forense:

El borrado de evidencias y ocultación de huellas:

- Borrado de logs:
 - Se debe tener acceso total.
 - Borrado fino: sólo borrar las líneas reveladoras del ataque.
- Ocultación de ficheros creados:
 - Directorios TEMP, SYSTEM32, etc.





Autopsy® is a digital forensics platform and graphical interface to [The Sleuth Kit®](#) and other digital forensics tools. It is used by law enforcement, military, and corporate examiners to investigate what happened on a computer. You can even use it to recover photos from your camera's memory card.

[Download Now](#)

[Training](#) and [Commercial Support](#) are available from Basis Technology.

Easy to Use

Autopsy was designed to be intuitive out of the box. Installation is easy and wizards guide you through every step. All results are found in a single tree. See the [intuitive](#) page for more details.

Extensible

Autopsy was designed to be an end-to-end platform with modules that come with it out of the box and others that are available from [third-parties](#). Some of the modules provide:

- [Timeline Analysis](#) - Advanced graphical event viewing interface (video tutorial included).
- Hash Filtering - Flag known bad files and ignore known good.
- [Keyword Search](#) - Indexed keyword search to find files that mention relevant terms.
- [Web Artifacts](#) - Extract history, bookmarks, and cookies from Firefox, Chrome, and IE.
- Data Carving - Recover deleted files from unallocated space using [PhotoRec](#)
- Multimedia - Extract EXIF from pictures and watch videos.
- Indicators of Compromise - Scan a computer using [STIX](#).

See the [Features](#) page for more details. Developers should refer to the [module development page](#) for details on building modules.

Fast

Everyone wants results yesterday. Autopsy runs background tasks in parallel using multiple cores and provides results to you as soon as they are found. It may take hours to fully search the drive, but you will know in minutes if your keywords were found in the user's home folder. See the [fast results](#) page for more details.

[Home](#)[About The Project](#)[Research Alliance](#)[Challenges](#)[Presentations](#)[Whitepapers](#)[Tools](#)[Our Book](#)[Funding/Donations](#)[Mirrors](#)[Search](#)

Scan of the Month

Scan 24

This month's challenge is a little different. Sponsored by the folks from [Digital Forensic Research WorkShop](#), they have created a fictional situation, where your job is to analyze forensic evidence. All submissions are due no later than 23:00 EST, Friday, 25 October. Results will be released Friday, 01 November.

Skill Level: *Intermediate*

The Challenge:

The folks from [Digital Forensic Research WorkShop](#) have created a unique challenge for you. Your mission is to analyze a recovered floppy and answer the questions below. What makes this challenge unique, you will need to read [the police report](#) before continuing your challenge. Just like an investigation in the real world, you will have some background information and some evidence, but its up to you and your technical skills to dig up the answers. Below is the dd image of the recovered floppy. This is the image that will provide you the answers, providing you can 'extract' the data.

Download:

[image.zip](#) MD5 = b676147f63923e1f428131d59b1d6a72 (image.zip)

Make sure you check the MD5 checksum of your download *before* you unzip it.

Questions

You can find all the criteria for judging and rules at the [SotM main page](#).

1. Who is Joe Jacob's supplier of marijuana and what is the address listed for the supplier?
2. What crucial data is available within the coverpage.jpg file and why is this data crucial?
3. What (if any) other high schools besides Smith Hill does Joe Jacobs frequent?
4. For each file, what processes were taken by the suspect to mask them from others?
5. What processes did you (the investigator) use to successfully examine the entire contents of each file?

Bonus Question:

6. What Microsoft program was used to create the Cover Page file. What is your proof (Proof is the key to getting this question right, not just making a guess).

Open A Case Autopsy Help

localhost:9999/autopsy?mod=0&view=3&x=56&y=9

Search

Open A Case

Select the case to open or create a new one

CASE GALLERY Host GALLERY HOST MANAGER

Name Description

mb0010a Análisis forense de un Disquete [details](#)

OK NEW CASE MAIN MENU
HELP

Name	Description	Details
mb0010a	Análisis forense de un Disquete	details

- <http://old.honeynet.org/scans/scan24/>
- <http://old.honeynet.org/scans/scan24/image.zip>

MD5 = b676147f63923e1f428131d59b1d6a72 (image.zip)

Select a volume to analyze or add a new image file.

CASE GALLERY

HOST GALLERY

HOST MANAGER



mount

C:/

name

image-0-0

fs type

fat12

[details](#)

[ANALYZE](#)

[ADD IMAGE FILE](#)

[CLOSE HOST](#)

[HELP](#)

[FILE ACTIVITY TIME LINES](#)

[IMAGE INTEGRITY](#)

[HASH DATABASES](#)

[VIEW NOTES](#)

[EVENT SEQUENCER](#)

Current Directory: C:/

[ADD NOTE](#)

[GENERATE MD5 LIST OF FILES](#)

DEL	Type dir / in	Name 	Written	Accessed	Created	Size	UID	GID	Meta
	v / v	\$FAT1	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	4608	0	0	45780
	v / v	\$FAT2	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	4608	0	0	45781
	v / v	\$MBR	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	512	0	0	45779
	d / d	\$OrphanFiles/	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0	0	0	45782
	r / r	cover_page.jpgc	2002-09-11 08:30:52 (EDT)	2002-09-11 00:00:00 (EDT)	2002-09-11 08:50:27 (EDT)	15585	0	0	8
✓	r / r	Jimmy Jungle.doc	2002-04-15 14:42:30 (EDT)	2002-09-11 00:00:00 (EDT)	2002-09-11 08:49:49 (EDT)	20480	0	0	5
	r / r	Scheduled_Visits.exe	2002-05-24 08:20:32 (EDT)	2002-09-11 00:00:00 (EDT)	2002-09-11 08:50:38 (EDT)	1000	0	0	11

ASCII ([display - report](#)) * Hex ([display - report](#)) * ASCII Strings ([display - report](#)) * [Export](#) * [Add Note](#)

File Type: Composite Document File V2 Document, Little Endian, Os: Windows, Version 5.1, Code page: 1252, Title: Jimmy Jungle, Author: 0000, Template: Normal, Last Saved By: 0000t, Revision Number: 9, Name of Creating Application: Microsoft Word 10.0. Total Editing Time: 18:00. Create Time/Date: Mon Apr 15 21:30:00 2002. Last Saved Time/Date: Mon Apr 15 22:42:00 2002. Number of Pages: 1. Number of

Contents Of File: C:/Jimmy Jungle.doc

626 Jungle Ave Apt 2
Jungle, NY 11111

Jimmy:

Dude, your pot must be the best ! it made the cover of High Times Magazine! Thanks for sending me the Cover Page. What do you put in your soil when you plant the marijuana seeds? At least I know your growing it and not some guy in Columbia.

These kids, they tell me marijuana isn't addictive, but they don't stop buying from me. Man, I'm sure glad you told me about targeting the high school students. You must have some experience. It's like a guaranteed paycheck. Their parents give t

I emailed you the schedule that I am using. I think it helps me cover myself and not be predictive. Tell me what you think. To open it, use the same password that you sent me before with that file. Talk to you later.

Thanks,

Joe

r / r [Scheduled Visits.exe](#) 2002-05-24 08:20:32 (EDT) 2002-09-11 00:00:00 (EDT) 2002-09-11 08:50:38 (EDT) 1000 0 0 [11](#)

ASCII ([display - report](#)) * Hex ([display - report](#)) * ASCII Strings ([display - report](#)) * [Export](#) * [Add Note](#)
File Type: gzip ERROR: Exec `gzip' failed, No such file or directory (Zip archive data, at least v2.0 to extract)

Contents Of File: C:/Scheduled Visits.exe

PK0000Z0,0U`0000B00000Scheduled Visits.xls@1*0I■0p00100H0<K0uq0Q00*60\$0~uF00NV0000`6T0.#00R0■0#-4HT0b0^0?0Rr00f
J_007x05kUM0000a_00SA#0;0QK■00
00I000;020VS
0t8n00220[3m
0.7H00
00000B0000gvmq[A0UU0000100000i00[0dz0e00xT00030wx\af0000N0020]000G08zq080<00Z^0s+000B>n00W003180'0 N[!00z0U0000f0~I0000Z0wE700Vv
0r00P60000d0U
0007%00XJ_00080■0BKRE w
a0■b0g00000020X0000?00Z0Jw{0m'L0sC6g(0yGU-0000j0T0ü?0nRUF00000H000I-00@000I+00&00åQg0420.+bN0c0X0W00G{>Yt0p?00 0;u0j00_0000p0\05"s}U70yW0.0|t;00B05C0:0C0 0TH0Xbq000b0>00\$PÜ+bg^0l00000
0000F00#e0Aqs0q0D00000..00

File Type (Recovered):

Composite Document File V2 Document, Little Endian, Os: Windows, Version 5.1, Code page: 1252, Title: Jimmy Jungle, Author: 0000, Template: Normal, Last Saved By: 0000t, Revision Number: 9, Name of Creating Application: Microsoft Word 10.0, Total Editing Time: 18:00, Create Time/Date: Mon Apr 15 21:30:00 2002, Last Saved Time/Date: Mon Apr 15 22:42:00 2002, Number of Pages: 1, Number of Words: 138, Number of Characters: 787, Security: 0

MD5 of recovered content:

b775eb6a4ccc319759d9aaae1e340acc -

SHA-1 of recovered content:

8bb25919c1c5762f05f528fc9c5c0edf74f36a39 -

Details:

Directory Entry: 5

Not Allocated

File Attributes: File, Archive

Size: 20480

Name: _IMMYJ~1.DOC

Directory Entry Times:

Written: 2002-04-15 14:42:30 (EDT)

Accessed: 2002-09-11 00:00:00 (EDT)

Created: 2002-09-11 08:49:49 (EDT)

Sectors:

[33](#) [34](#) [35](#) [36](#) [37](#) [38](#) [39](#) [40](#)

[41](#) [42](#) [43](#) [44](#) [45](#) [46](#) [47](#) [48](#)

[49](#) [50](#) [51](#) [52](#) [53](#) [54](#) [55](#) [56](#)

[57](#) [58](#) [59](#) [60](#) [61](#) [62](#) [63](#) [64](#)

[65](#) [66](#) [67](#) [68](#) [69](#) [70](#) [71](#) [72](#)

Search for File Name

File Type:

gzip ERROR: Exec `gzip' failed, No such file or directory (Zip archive data, at least v2.0 to extract)

MD5 of content:

082a5cc64deea22a3a580ffbb5a6fa66 -

SHA-1 of content:

c8e7f25380d63c9034d9f27faab29de1f09240b5 -

Details:

Directory Entry: 11

Allocated

File Attributes: File, Archive

Size: 1000

Name: SCHEDU~1.[EXE](#)

Directory Entry Times:

Written: 2002-05-24 08:20:32 (EDT)

Accessed: 2002-09-11 00:00:00 (EDT)

Created: 2002-09-11 08:50:38 (EDT)

Sectors:

[104](#) [105](#)

Auditoría Forense:

- **Autopsy** <https://www.sleuthkit.org/autopsy/> es una plataforma forense digital e interfaz gráfica para The Sleuth Kit y otras herramientas forenses digitales, disponible para Linux, Mac OS y Windows.
- **Cuckoo Sandbox** <https://cuckoosandbox.org/> es para el análisis forense de malware en Linux, Mac OS y Windows. <https://github.com/cuckoosandbox>
- **Rekall** <http://www.rekall-forensic.com/> y **Volatility** <https://www.volatilityfoundation.org/> (ambos escritos en Python) para análisis forense de memoria volátil.

Auditoría Forense:

Colección de herramientas <https://gbhackers.com/computer-forensics-tools/> e interesantes recursos de forense <https://github.com/Cugu/awesome-forensics>

Colección de recursos interesantes <https://github.com/rshipp/awesome-malware-analysis> para el análisis de malware.

El análisis forense digital de USB <https://gbhackers.com/usb-forensics/> incluye la preservación, colección, validación, identificación, análisis, interpretación, documentación y presentación de las evidencias.

Auditoría Forense... ANÁLISIS FORENSE DE RED

Colección de herramientas interesantes para la trazabilidad de las redes

<https://github.com/caesar0301/awesome-pcaptools>

- **Dshell** <https://github.com/USArmyResearchLab/Dshell> es un marco de análisis forense de red.
- **Passivedns** <https://github.com/gamelinux/passivedns> es un detector de red que registra todas las respuestas del servidor DNS para usar en una configuración pasiva de DNS.



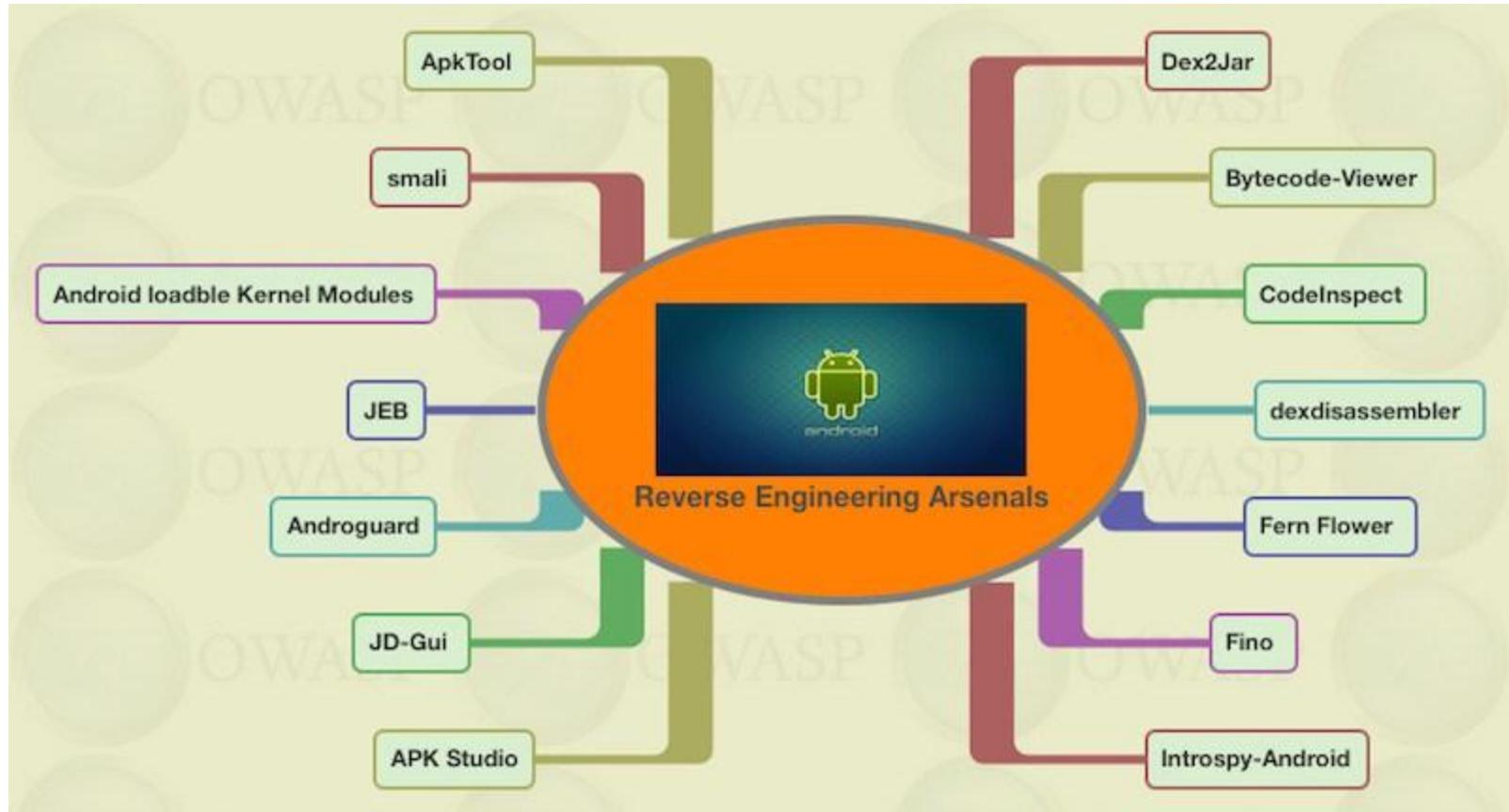
Auditoría... SMARTPHONE



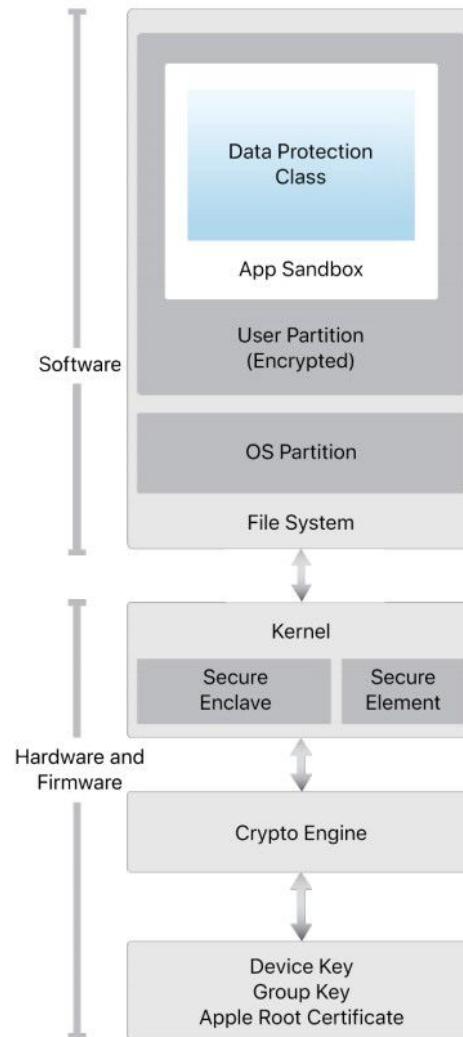
Wiki de seguridad móvil <https://mobilesecuritywiki.com/> y otros recursos
<https://github.com/secmobi/wiki.secmobi.com>

OWASP Mobile Security Project
https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Top_10_Mobile_Risks analiza los principales riesgos. Además de la guía para las pruebas de seguridad móvil https://www.owasp.org/index.php/OWASP_Mobile_Security_Testing_Guide se proponen herramientas para la ingeniería inversa en Android e iOS https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=M-Tools



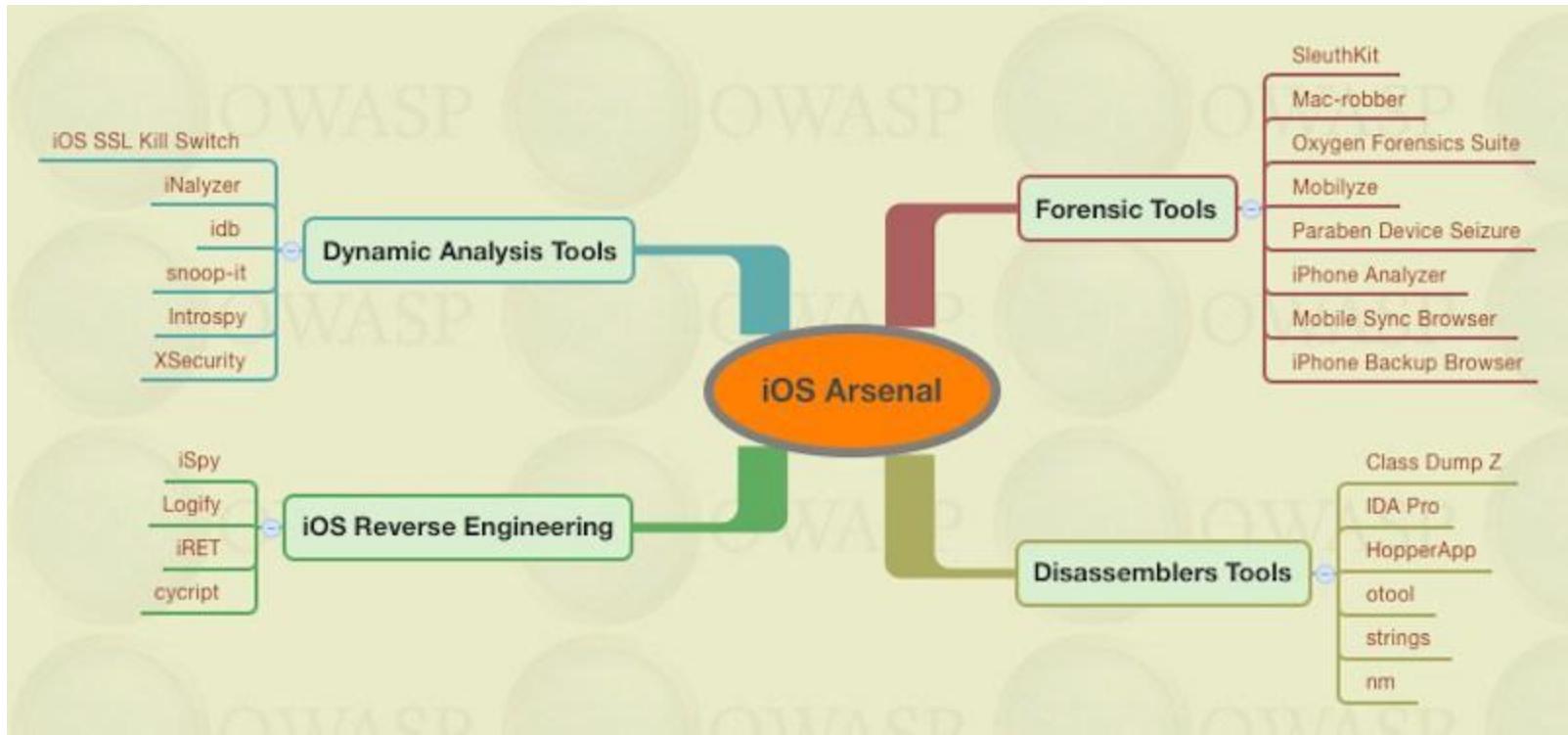


iOS



Jailbreak en iOS:





Understand and improve mobile signal.

Get better signal, find free WiFi and see which operator is best in your location.



The trusted global standard for mobile experience.

Providing real-world, competitive insights from over **20 million** users of the OpenSignal app

[See Business Solutions](#)



Test de Velocidad

Pon a prueba la velocidad **REAL** de tu conexión



Velocidad **REAL** de Movistar



40 ms
Latencia

85,30 Mbps
Bajada

36,28 Mbps
Subida

REALIZAR OTRA PRUEBA

COMPARTIR

Estadísticas de Redes



Aquí se muestran los resultados promedio que los usuarios de OpenSignal han medido en esta área.

Operador	Bajada (Mbps)	Subida (Mbps)
----------	---------------	---------------

orange	Orange	12.92	5.92
--------	--------	-------	------

Vodafone	15.62	7.83
----------	-------	------

Estadísticas de Redes



Aquí se muestran los resultados promedio que los usuarios de OpenSignal han medido en esta área.

Latencia (ms)	Señal
---------------	-------

orange	63	
--------	----	--

Vodafone	56	
----------	----	--

Estadísticas

Tiempo por tipo de r..▼

Última hora▼

TE HAS CONECTADO

100% DEL TIEMPO

basado en **28** mediciones



ESTADÍSTICAS DE SEÑAL



4G (100%)

3G (0%)

2G (0%)

Sin señal (0%)

Estadísticas

Tiempo por tipo de r..▼

Hoy ▾

TE HAS CONECTADO

98% DEL TIEMPO

basado en **43** mediciones



ESTADÍSTICAS DE SEÑAL



4G (0%)

3G (86%)

2G (11,6%)

Sin señal (2,3%)



Termux

Termux is an Android terminal emulator and Linux environment app that works directly with no rooting or setup required. A minimal base system is installed automatically - additional packages are available using the APT package manager.



[Read the wiki to learn more](#)

Secure. Access remote servers using the ssh client from OpenSSH. Termux combines standard packages with accurate terminal emulation in a beautiful open source solution.

Feature packed. Take your pick between Bash, fish or Zsh and nano, Emacs or Vim. Grep through your SMS inbox. Access API endpoints with curl and use rsync to store backups of your contact list on a remote server.

Customizable. Install what you want through the APT package management system known from Debian and Ubuntu GNU/Linux. Why not start with installing Git and syncing your dotfiles?

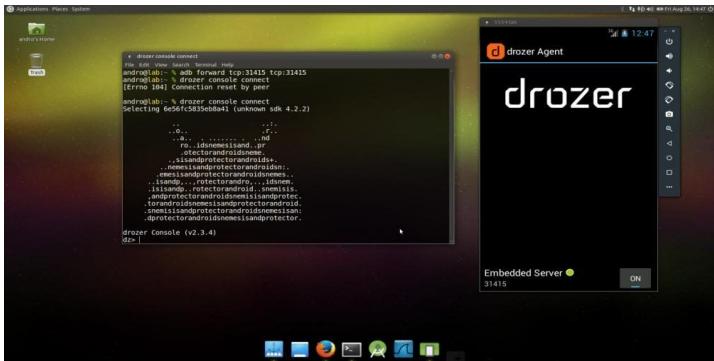
Explorable. Have you ever sat on a bus and wondered exactly which arguments tar accepts? Packages available in Termux are the same as those on Mac and Linux - install man pages on your phone and read them in one session while experimenting with them in another.

With batteries included. Can you imagine a more powerful yet elegant pocket calculator than a readline-powered Python console? Up-to-date versions of Perl, Python, Ruby and Node.js are all available.

Ready to scale up. Connect a Bluetooth keyboard and hook up your device to an external display if you need to - Termux supports keyboard shortcuts and has full mouse support.



Auditoría... LABORATORIOS DE SMARTPHONE:



- **Androl4b** <https://github.com/sh4hin/Androl4b> es una máquina virtual basada en Ubuntu Mate empleada como framework para la ingeniería inversa y análisis forense (y de malware) en aplicaciones Android. El usuario y contraseña son ambos: **andro** y el pin para el emulador: 1234
- **Santoku** <https://santoku-linux.com/> es otra distribución basada en Lubuntu orientada al forense de smartphone.

Auditoría... LABORATORIOS DE ENTRENAMIENTOS PARA SMARTPHONE:

- **DIVA** (Damn Insecure and vulnerable App for Android) <https://github.com/payatu/diva-android> es un laboratorio intencionalmente diseñado inseguro para el entrenamiento en seguridad Android.
- **DVIA** (Damn Vulnerable iOS Application) <http://damn vulnerabileiosapp.com/> es un laboratorio de testeo y prueba de vulnerabilidades en iOS con asistencia de la ayuda y tutoriales <https://github.com/prateek147/DVIA-v2>

Auditoría... SMARTPHONE

Colección de herramientas y recursos interesantes para Android

<https://github.com/ashishb/android-security-awesome>

<https://github.com/sundaysec/Android-Exploits> y OSX e iOS

<https://github.com/ashishb/osx-and-ios-security-awesome>



- Apkpure <https://apkpure.com/es/> es un repositorio de aplicaciones desde donde podemos descargar también versiones anteriores de fuentes oficiales para el estudio de vectores de ataque.

Auditoría... SMARTPHONE



- **Apktool** <https://ibotpeaches.github.io/Apktool/> es una aplicación Java empleada para el reversing de código de aplicaciones móviles, <https://github.com/iBotPeaches/Apktool> permitiendo desensamblar y volver a compilar en APK o JAR.
- **JD-Gui** <http://jd.benow.ca/> es un decompilador de código Java.

• python

Please update from master branch or check for new releases.

System check identified no issues (0 silenced).

April 02, 2018 - 10:31:08

Django version 1.11.3, using settings 'MobSF.settings'

Starting development server at http://127.0.0.1:8000/

Quit the server with CONTROL-C.

[02/Apr/2018 10:33:34] "GET / HTTP/1.1" 200 7692

[02/Apr/2018 10:33:35] "GET /static/css/bootstrap.min.css HTTP/1.1"

[02/Apr/2018 10:33:35] "GET /static/js/jquery.min.js HTTP/1.1" 200 9

[02/Apr/2018 10:33:35] "GET /static/css/dropzone.css HTTP/1.1" 200 1

[02/Apr/2018 10:33:35] "GET /static/css/cover.css HTTP/1.1" 200 2850

[02/Apr/2018 10:33:35] "GET /static/js/ie-emulation-modes-warning.js

00 2132

[02/Apr/2018 10:33:35] "GET /static/js/dropzone.js HTTP/1.1" 200 644

[02/Apr/2018 10:33:35] "GET /static/js/bootstrap.min.js HTTP/1.1" 200

[02/Apr/2018 10:33:35] "GET /static/js/viewport-bug-workaround.

200 694

[02/Apr/2018 10:33:35] "GET /static/img/MobSF_Logo_small.png HTTP/1.

[02/Apr/2018 10:33:35] "GET /static/favicon.ico HTTP/1.1" 200 370070

[02/Apr/2018 10:33:35] "GET /static/fonts/glyphicons-halflings-regu

l.1" 200 25320

]



Emulator



SocialDrive_v4.2.5
apkpure.com.apk



LinkedIn_v4.1.156
apkpure.com.apk



CyRSocial
Conductores y Red
Social_v1.1.17_ap...



Lookout Security
Antivirus_v10.21.1-
71c0cca_apkpure...

• Mobile Security Framework - Mozilla Firefox

1. Documentation · MobsF · Mobile Security Framework

127.0.0.1:8000 | C | Q mobsf

MOBSF

Drag files here or click Upload & Analyze

Upload & Analyze

Search MD5

Recent Scans | About

© 2018 Mobile Security Framework - MobSF v0.9.5.2 Beta. All Rights Reserved

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Refresh Firefox... x

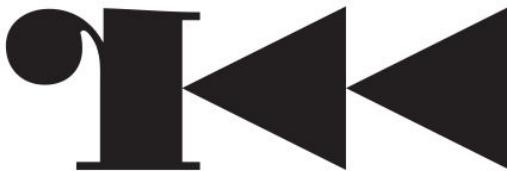
Icons: File, Folder, Home, Stop, Refresh, Back, Forward, Search, Help, Address Bar, Tab, Window Control Buttons.

Auditoría... SMARTPHONE



- **MobSF** (Mobile Security Framework)
<https://github.com/MobSF/Mobile-Security-Framework-MobSF> es una imagen Docker escrita en Python empleada como marco de análisis automatizado de aplicaciones (Android, iOS y Windows) para generar informes.
- **DroidBox** <https://github.com/pjilantz/droidbox> ofrece además análisis dinámico
<https://hackmag.com/uncategorized/droidbox-for-dynamic-malware-analysis/>
- **Appmon** <https://dpnishant.github.io/appmon/> es un framework automatizado para la monitorización y manipulación de llamadas a API (interfaz de programación de aplicaciones) en Android e iOS.

Auditoría... SMARTPHONE



- **Radare2** <https://www.radare.org/> es un framework portable de reversing que permite desensamblar y decompilar código. <https://github.com/radare/radare2>
- **Androguard** <https://github.com/androguard/androguard/> es otra utilidad de reversing para analizar aplicaciones Android. <https://androguard.readthedocs.io/en/latest/index.html>