Seguridad en Internet Multimedia Subsystem (IMS)

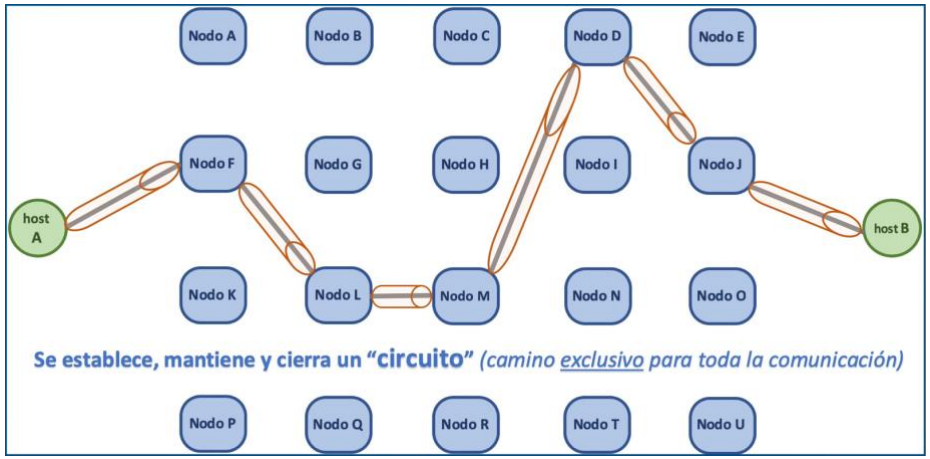
y

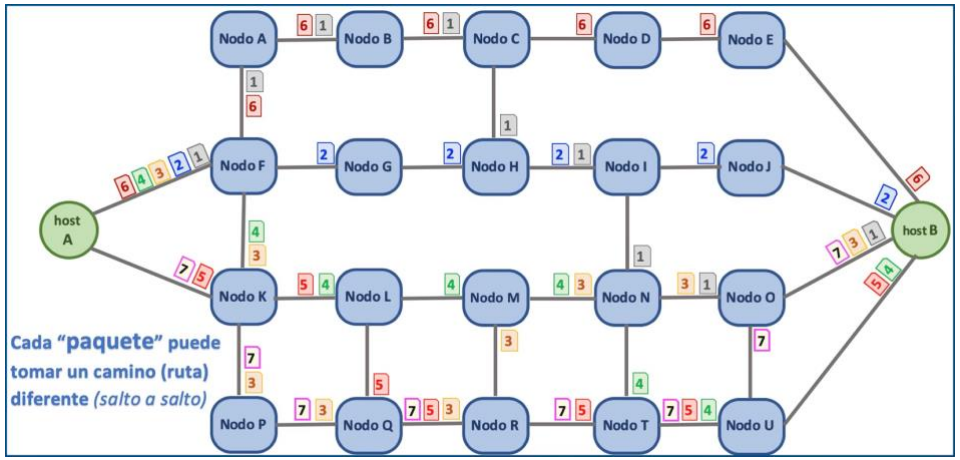
Session Initiation Protocol (SIP)

Alejandro Corletti Estrada

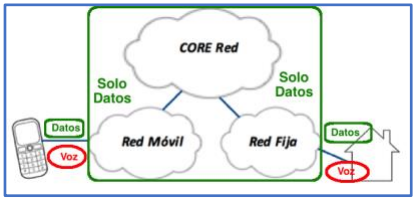
acorletti@darFe.es

Las redes de voz están orientadas originalmente a la conexión y al establecimiento de circuitos. Pero desde hace muchos años, se encuentran dos tipos de redes: Redes de conmutación de circuitos y redes de conmutación de paquetes.





Las redes de datos, están orientadas a la flexibilidad de sus rutas y a la entrega de paquetes. Hoy en día todas las operadoras de telefonía tienen su core como red de datos.



Al implantar definitivamente la "paquetización de voz" desde el acceso mismo (*terminal móvil o teléfono fijo*), es decir con **VoLTE** (*Voz sobre LTE*) en la red móvil y para los accesos por medio de **fibra óptica** en la red fija, estas conversaciones ingresan a la red ya como paquetes. La actual red de 5G es pura de conmutación de paquetes.

Una red de paquetes no tiene ninguna razón para mantener un flujo constante en ambos sentidos. Esto sí se viene realizando para las redes de voz convencionales desde hace más de 30 años con el sistema de señalización 7 (**SS7**).

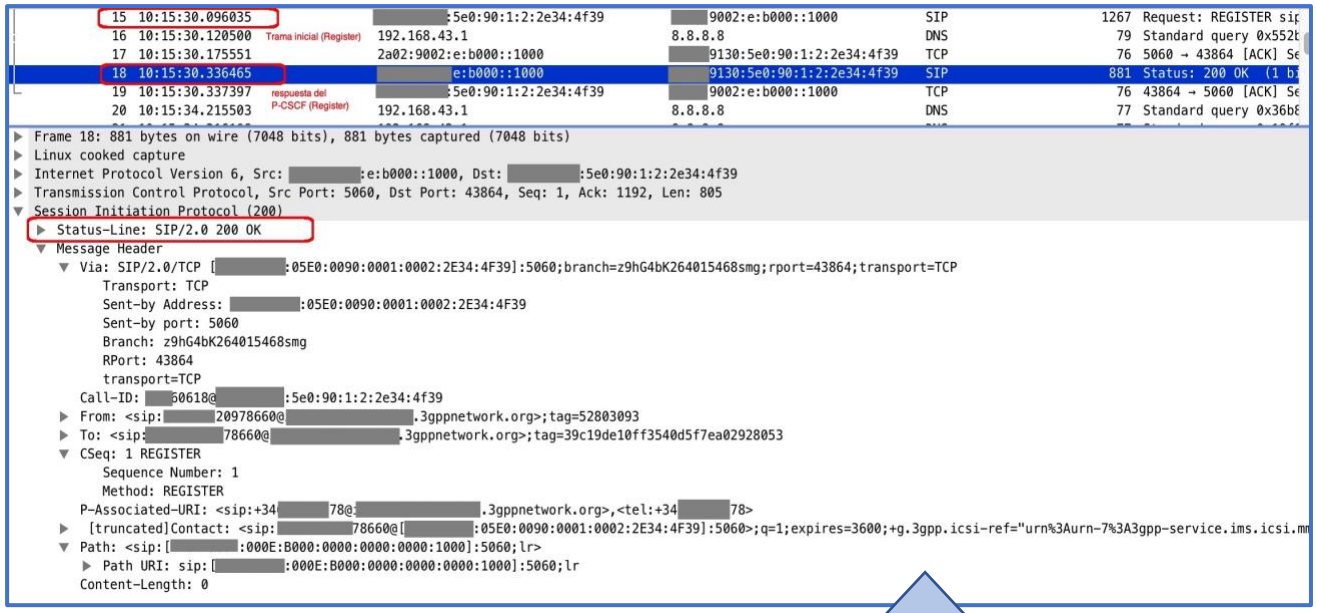
Este SS7 ya no se puede implementar en redes de paquetes, para las mismas su reemplazo es el protocolo Session Initiation Protocol IP (**SIP**).

Para resumir estos conceptos introductorios, cuando ingresamos por **VoLTE** o por fibra nuestra voz paquetizada, a la par de estos paquetes que contienen voz, también se generan paquetes SIP que son los responsables de "señalizar" estas conversaciones. El diálogo **SIP** fundamentalmente se realiza contra esta Infraestructura que se llama IMS.

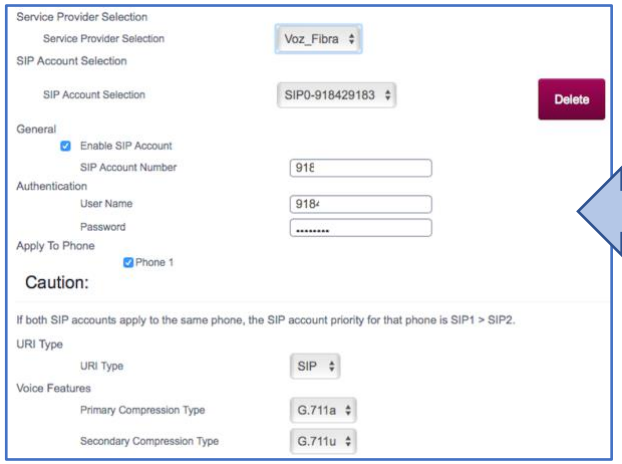
Ahora bien, con los avances tecnológicos, hoy en día no solo nos importa la voz, sino varios tipos de diálogos más, que los englobamos en la categoría de "**multimedia**".

IMS está diseñado para gestionar todo este tipo de "diálogos multimedia" en las sesiones de un usuario a otro(s) usuario(s), o de un usuario a un servicio.

Lo interesante de todo esto es que ahora, si logro ser "**root**" de mi teléfono móvil o del router de fibra óptica de mi casa, ya estoy siendo parte de esta comunicación directa hacia la infraestructura IMS...



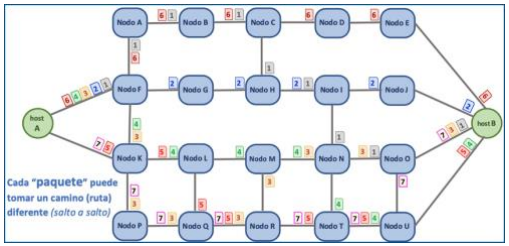
¿y la operadora lo tendrá bien o mal configurado/bastionado?..... de esto hablaremos en esta charla.



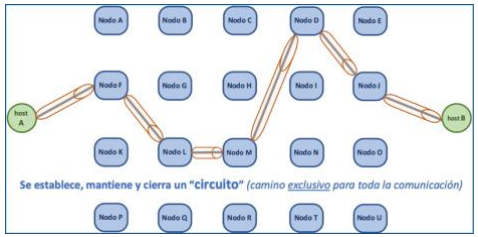
Desarrollo

1. Por qué hoy hablamos de IMS.

En la actualidad, como hemos dicho toda operadora de voz y datos, en realidad está obligada a mantener estos dos tipos de redes:



Red de conmutación de circuitos (**PSTN**: Public Switched Telephone Network).



Red de conmutación de paquetes (**PSDN**: Packet Switched Data Network).

Los "datos" hoy superan ampliamente al tráfico de voz, por lo que día a día las operadoras necesitan invertir más y más en redes de paquetes de alta velocidad con altas exigencias de calidad de servicio, y a su vez mantener "viva" la PSTN, sobre la cual no se desea invertir mucho más, por no tener sentido pues disminuye día a día.

La historia de la transmisión de voz por medio de las redes de telecomunicaciones en sus más de cien años, se basó SIEMPRE en mantener el sincronismo, este fue el pilar que la sustentó sin duda. Se montaban enormes infraestructuras para poder hacer viajar la voz, como si fuera el metro circular de Madrid (*la línea gris*), pasando vagones cada "n" mili o microsegundos, a los cuales subían o bajaban sus pasajeros (voz) en cada estación, SIEMPRE, cada "n" intervalos de tiempo. En lo personal, siempre se me representó esta como la mejor analogía.

Las redes de paquetes, nacen como un "desorden organizado" de envío y recepción de datos por medio de rutas que pueden variar según un amplio juego de opciones, de envíos y recepción, que no tienen por qué estar en orden, de "delay" variables, de paquetes cuyo tamaño

no es fijo, de conexiones punto / multipunto, etc… Es decir, un verdadero CAOS, y concretamente así lo veíamos todos lo que veníamos del mundo de la telefonía…. ¡¡¡ Esto no va andar!!!..... pero como el chiste → **¡Andó!** (o anduvo, si somos muy castellanos y poco graciosos).

Estas redes de paquetes, aumentaron tanto y tanto su velocidad en pocos años, que hoy en día un sencillo paquete que transfiera una voz digitalizada, puede ser enviado a 10.000 km de distancia, si falla volverlo a enviar, y se produce un error, tomar otra ruta, enviarlo nuevamente, cien, mil o diez mil veces y todo esto sin superar los 400 milisegundos de demora que suele ser el umbral en el cual una conversación de voz comienza a degradarse.

Hay un hecho muy significativo y es que el ancho de banda de las redes actuales de paquetes de las operadoras telefónicas permiten garantizar determinados patrones clave.

GSMA estandarizó un parámetro fundamental denominado "Identificador de clase de QoS" (**QCI**) que especifica el nivel de latencia y pérdida aceptable para diferentes tipos de tráfico, como se muestra en la siguiente figura:

QCI	Tipo de portador	Prioridad	Retardo de paquetes	Pérdida de paquetes	Ejemplo
1	GBR	2	100 mseg	10^{-2}	Llamada VoIP
2		4	150 ms	10^{-3}	Llamada de video
3		3	50 mseg		Juegos en línea (en tiempo real)
4		5	300 ms	10^{-6}	Transmisión de video por secuencias
5	No GBR	1	100 mseg		Señalización IMS
6		6	300 ms		Video, servicios basados en TCP, por ejemplo: correo electrónico, "chat", ftp, etc.
7		7	100 mseg	10-3	Voz, video, juegos interactivos
8		8	300 ms	10^{-6}	Video, servicios basados en TCP, por ejemplo: correo electrónico,
9		9			"chat", ftp, etc.

Tabla 1: QCI

GBR (Guarranty Bit Rate) como su nombre lo indica implica que la red debe garantizar una tasa "constante" de entrega de bits, y por el contrario **No GBR** no debe hacerlo, pero en ambos casos se debe cumplir un "retardo de paquetes" (delay) y una tasa de pérdida de los mismos inferior a lo que para cada línea se expone en la tabla. Si prestamos atención a eta tabla, podemos notar que, en el caso de nuestro especial interés (paquetes de voz), el retardo que debe cumplir cualquier tipo de comunicación de voz es muy inferior a los 400 ms que acabo de mencionar.

Las actuales redes de telecomunicaciones en las grandes operadoras están en capacidad de ofrecer estos valores sobradamente, con lo que ya no es necesario seguir invirtiendo en dos redes paralelas (PSTN y PSDN) pues con una sola de ellas será suficiente en pocos años.

Para que podamos ofrecer TODOS los servicios actuales de telecomunicaciones a través de la PSDN es **imprescindible** contar con una robusta infraestructura de **IMS**.

NOTA: Todos estos conceptos están desarrollados en detalle en los puntos 1.5. **Voz sobre IP y VoLTE**, 1.6 **NGN** (Next Generation Network) y 1.7. **IMS** (IP Multimedia Subsystem) de mi libro "**Seguridad en Redes**" (*que puede descargarse gratuitamente en: www.darFe.es*), por lo que no continuaremos ampliándolo en este texto.

Lo que sí deseo remarcar es que las características principales de los servicios IP multimedia que IMS hace posible son las siguientes:

- La comunicación orientada a sesión de un usuario a otro(s) usuario(s), o de un usuario a un servicio.
- La comunicación en tiempo real o diferido.
- Las sesiones IP multimedia compuestas por flujos y contenidos multimedia diversos, con un nivel adecuado de Calidad de Servicio para vídeo, audio y sonido, texto, imagen, datos de aplicación, etc.
- La identificación de usuarios, servicios y nodos mediante URIs (Universal Resource Identifier), que aumenta la usabilidad de los servicios de cara a los abonados. Éstos ya no tienen que manejar números de teléfono imposibles de recordar, sino nombres al estilo de servicios Internet, como el correo electrónico.

2. Convergencia Fija móvil y el modelo de capas IMS.

El tema clave de este punto se encuentra en el **protocolo SIP**. El día que logre apagarse definitivamente **SS7** (Sistema de Señalización 7) del que hablamos en el último Webinar, el mundo se señalizará por SIP, con todas las ventajas que esta familia está demostrando (integrar audio, video, multiconferencia, servicios de valor agregado, mensajes, mail, web, etc.).

La arquitectura de IMS es independiente de la red de acceso, pero para ofrecer la totalidad de los servicios que posee IMS, es necesario garantizar los valores que expusimos en la tabla del punto anterior de extremo a extremo (e2e). Por esta razón es que en estos días la voz sobre IP a nivel operadora de servicios de voz y datos, sólo se ofrece a través de "**VoLTE**" para los acceso móviles y a través de acometidas

con **fibra óptica** para los accesos de la red fija. También encontraremos servicios a través de accesos fijos de empresas o "WiFi" para teléfonos móviles en zonas de gran afluencia (aeropuertos, terminales, centros comerciales), cabe aclarar que este último siempre y cuando tengamos "VoLTE" en nuestro teléfono y operadora y en vez de conectarme a través de la antena 4G, lo haga por medio de WiFi.

Cada una de estas tecnologías, accede a la infraestructura de IMS por caminos diferentes, los cuáles los desarrollaremos más adelante, pero lo que sí es importante destacar es que los caminos diferentes son los de "señalización", es decir los paquetes "SIP", luego los paquetes de voz (en general **RTP**: Real Time Protocol), seguirán la ruta que esta señalización, junto a los diferentes nodos de la arquitectura IMS le indiquen como cualquier otro paquete IP de datos.

La arquitectura de referencia del modelo de capas la podemos graficar como se presenta en la imagen de la derecha.

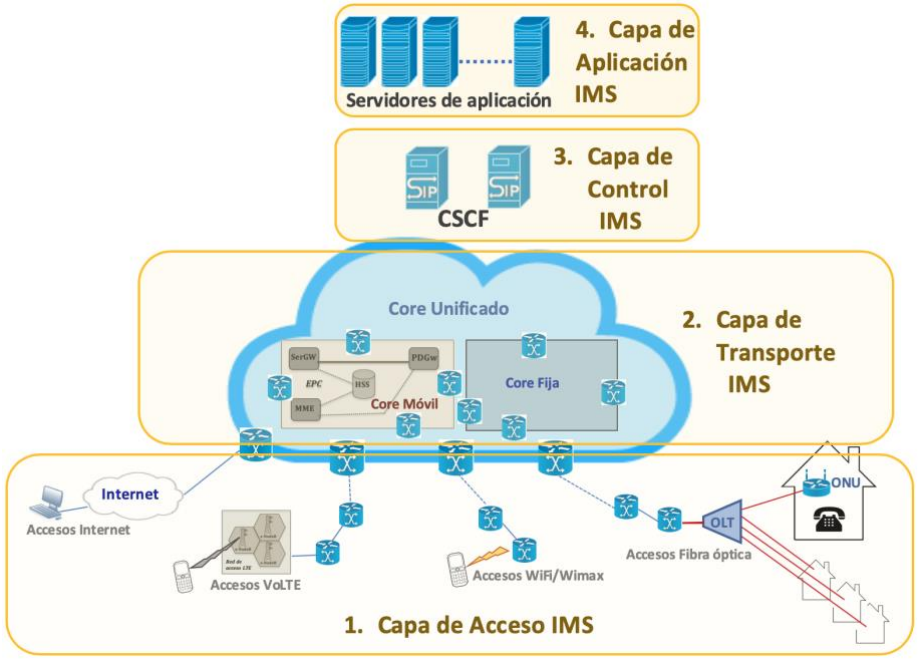


Imagen 1. Modelo de capas de IMS

Analicemos la imagen.

1) Capa de Acceso IMS.

Como hemos presentado, este tipo de accesos a IMS, en la actualidad las diferentes operadoras de telecomuncaciones, lo ofrecen bajo estas cuatro tecnologías (*Fibra óptica, VoLTE, WiFi/Wimax*) y hemos querido considerar aquí también Internet como una última posibilidad, pues también es cierto que es una vía de accesos que abre grandes posibilidades hacia IMS.

En la imagen, se ha intentado poner de manifiesto, que si bien cualquiera de estas redes de acceso (*en virtud del nivel, tecnología, área, etc.*), en diferentes gráficos o mapas se resaltan los dispositivos que la componen (*antenas, e-nodoB, DSLAM, BRAS, OLT, ONT, etc.*), por tratarse de redes que son exclusivamente de paquetes. En realidad, la mayoría de estos dispositivos/nombres/funciones, lo que hacen es puramente "**enruta**r", por eso hemos hecho hincapié en resaltar la presencia de una cadena de routers de acceso que van sumando tráfico hasta el Core de la red. En la jerga de teleco, estos niveles suelen diferenciarse como: Acceso, Transporte y Agregación.

2) Capa de transporte IMS.

La capa de transporte, en realidad es la que en el modelo TCP/IP desempeña la capa 3 (*Red*), es la responsable de enrutar el tráfico.

Las actuales operadoras telefónicas, pueden tener tres casuísticas:

a. Core Fija
b. Core móvil
c. Core unificado (fija, móvil y hasta unificado también voz y datos).

Esta capa es la responsable de transmitir los paquetes de señalización y de media, en ambos sentidos y de extremo a extremo.

3) Capa de control IMS.

Este es el verdadero "Cerebro" de la arquitectura IMS.

Como se aprecia en la imagen, lo componen básicamente los **CSCF** (Call Session Control Function o Función de Control de Sesión de Llamada) es el elemento principal dentro de la red IMS. Es la pieza clave para la señalización a través del protocolo **SIP** para establecer, modificar y terminar una sesión multimedia. Podemos pensarlo concretamente como un "Servidor SIP". Este elemento lógico desempeña tres funciones principales que pueden encontrarse en un mismo dispositivo o en hardware diferente, esta son:

- **P-CSCF**: (Proxy - Call Session Control Function) Función de control de sesión de llamada Proxy. Es el primer punto de entrada a la red IMS y actúa como entrada y salida de la misma. Toda petición iniciada desde un terminal IMS, se inicia aquí. Como veremos más adelante, es quién gestiona las peticiones SIP Registrer Request, almacenando toda la información de registro de ese "User Equipment (UE)". Es probable que por razones de distribución de carga, encontremos más de uno en cada Operadora de telecomunicaciones.
- **I-CSCF**: (Interrogating - Call Session Control Function) Función de control de sesión de llamada. Este es el punto de contacto entre la red de la Operadora. Su principal tarea es asignar a cada usuario su correspondiente S-CSCF. Y mantener la comunicación con el **HSS** (Home Subscriber Server) empleando con este protocolo DIAMETER. En general este dispositivo es quien genera los **CDR** (Call Data Records) para la tarificación.

- **S-CSCF**: (Serving - Call Session Control Function) Función de control de sesión de servidor. Es el responsable del control y mantenimiento de las sesiones de cada UE a través del protocolo SIP, también mantiene comunicación con el HSS por medio del protocolo DIAMTER para consultas del perfil de usuario.

A su vez el CSCF ofrece otras funcionalidades que también se llevan a cabo desde el mismo dispositivo, estas son:

- Servicio de Emergencia, E-CSCF (Emergency CSCF), permite encaminar peticiones SIP relacionadas con llamadas o servicios de emergencia.
- Función de Control de Pasarela de Salida, **BGCF** (Break-out Gateway Control Function): Este nodo es el responsable de seleccionar las pasarelas adecuadas cuando la comunicación está relacionada con redes de conmutación de circuitos (CS: Circuit Switching o PSTN). Por lo general este dispositivo, enruta las peticiones hacia los **MGCF** (Media Gateway Control Function).
- Función de Control de Entradas, BCF (Break-in Control Function), este es el dispositivo inverso al anterior, y actúa cuando un usuario de una red no IMS desea emplear los servicios de esta arquitectura.

Veremos más adelante el detalle de ciertos elementos de seguridad que por ahora podemos presentarlos como sigue.

SBC (Serial o Session Border Controller) También llamado **SBG** (Gateway): es el encargado de la correlación de toda la señalización y los flujos de media (como audio y vídeo) que pasa por los extremos de la red, proporcionando un conjunto completo de funciones que son necesarias para acceder e interconectar el dominio IMS con otras redes IP multimedia. Este nodo proporciona acceso con seguridad, protección del ancho de banda, calidad del servicio, nivel de servicios acordados y otras funciones críticas para las transmisiones en tiempo real de audio o vídeo.

Podríamos pensarlo “casi” como un Firewall de toda esta arquitectura.

El SBC se debería localizar en **ambos** extremos de la red, el punto de infraestructura donde una sesión pasa de una red a otra. Dentro del nodo podemos diferenciar dos partes que lo componen:

- **SGC**, Session Gateway Controller, que se encarga del plano de señalización.
- **MG**, Media Gateway (o Media Proxy), que soporta el tráfico de datos.

- **A-SGC**: cuando la funcionalidad SBG se implementa entre la red IMS core y la red de acceso. Sólo permite el tráfico de señalización hacia y desde los usuarios que están registrados en la red central IMS (en el HSS). La excepción se produciría con llamadas de emergencia de usuarios no registrados que pueden ser aceptadas si así se configura en el nodo.
- **N-SGC**: funcionalidad implementada entre la red IMS core y una red (Network) externa.
- **MP** (Media Proxy): protege los nodos centrales de la red IMS de los posibles ataques y bloquea el tráfico malicioso. Dispone de alarmas están para hacer que el operador sea consciente de posibles intentos de ataque.

  Para asegurarse de que las interfaces Ethernet no se utilice excesivamente, el MP realiza un seguimiento del ancho de banda reservado para el flujo de datos. Una parte del ancho de banda está siempre reservado para llamadas de emergencia.

  Las acciones más destacables del nodo sobre la red son:

  - La protección del perímetro de la red central IMS: filtrado, protección contra sobrecarga, y la limitación de velocidad para bloquear las inundaciones de tráfico IP y proporcionar protección contra la denegación de servicio (DoS).
  - Registro y alertas de ataques de red y los eventos relacionados con la seguridad
  - Validación de mensajes SIP / H3.23: Control de sintaxis de mensajes. Además, A-SBG sólo acepta mensajes desde los agentes de usuario registrados o mensajes de llamadas de emergencia.
  - Ocultación de identidad: no hay información sobre las direcciones IP utilizadas en el núcleo de red IMS o por los usuarios de la red de acceso y la red externa.
  - Permite al operador configurar el SBG funcionalidades que implementan RTCP (Real Time Control Protocol).
  - Media anchoring: actualización de direcciones y puertos en el SDP (Session Description Protocol: *parte de la familia SIP*) para que los flujos pasen a través de SBG.
  - Asegurar la QoS: control sobre el ancho de banda disponible en cada momento.
  - Permite tráfico SIP/UDP o SIP/TCP
  - Soporta centralitas IP-PBX tanto SIP como H.323 y reconoce el tráfico que va desde/hacia la IP-PBX y aplica un tratamiento especial en los mensajes. Puede modificar las cabeceras de los mensajes para direccionarlos correctamente.

- Acepta llamadas de emergencia incluso de usuarios ajenos a la red y prioriza las mismas tanto en el plano de señalización como en el de control.
- Adapta la señalización entre SIP y H.323 (N-SBG)
- Un SBG puede configurarse al mismo tiempo como A-SBG y N-SBG

Como acabamos de ver este nodo es un **elemento clave** para la seguridad de nuestra Operadora.

AS (Application Servers)

Los AS proporcionan la lógica de los servicios que lleve implementados IMS. Generalmente dentro de la red existen múltiples AS, donde cada uno suele implementar un servicio. Los AS pueden localizarse en la 'Home Network' o en redes externas, si se trata de un servicio que por ejemplo proporciona un proveedor que haya solicitado el operador de red. Todos se caracterizan por implementar Interfaz SIP hacia el S-CSCF, conocido como **ISC** (IMS Service Control). Además, estos nodos pueden implementar protocolos como HTTP o WAP necesarios para este tipo de aplicaciones.

Existen diferentes tipos de AS:

- **SIP-AS**: Este AS es el primero que se estableció en la red IMS, es capaz de comunicarse con el nodo HSS (basado en DIAMETER) de manera opcional si es necesario para la lógica que implementa obtener datos de este nodo. Este nodo se comunica directamente con el S-CSCF asignado al usuario de esta sesión para mantener el control SIP de la misma.
- **OSA-SCS**: (Open Service Access – Service Capability Server) con este AS se permite obtener un interfaz de comunicación hacia el entorno de aplicación OSA desde la red IMS. Se conoce como Servidor de Mediación, ya que permite acceder a servicios de otra tecnología. Todos los servicios que se desarrollan hoy en día utilizan los servidores SIP, pero para las funcionalidades ya existentes en esta plataforma (OSA) se permite el acceso a través de estos AS.
- **IM-SSF**: (IP Multimedia – Service Switching Function). Se trata de un servidor de mediación, que puede actuar como servidor de aplicación SIP que a la vez es capaz de comunicarse mediante el protocolo CAMEL (Customized Application for mobile-Network for Enhanced Logic) para utilizar los servicios de las redes GSM.

El grupo 3GPP describe en su especificación técnica **TS 23.228** los nodos P-CSCF, ICSCF, S-CFCS, E-CSCF y el BGC.

4) Capa de aplicación IMS.

Esta capa está conformada por los servidores de Aplicación de Media que son los responsables de integrar la totalidad de los servicios, funcionalidades y conversiones de protocolos.

Dentro de este modelo de capas, es importante considerar que existen dos flujos diferentes:

- **Flujo de señalización.**
- **Flujo de media** (voz o datos).

En la imagen de la derecha podemos ver la diferencia entre ellos, en este ejemplo con una comunicación entre dos teléfonos móviles VoLTE (uno accede mediante 4G y otro por medio de WiFi/Wimax).

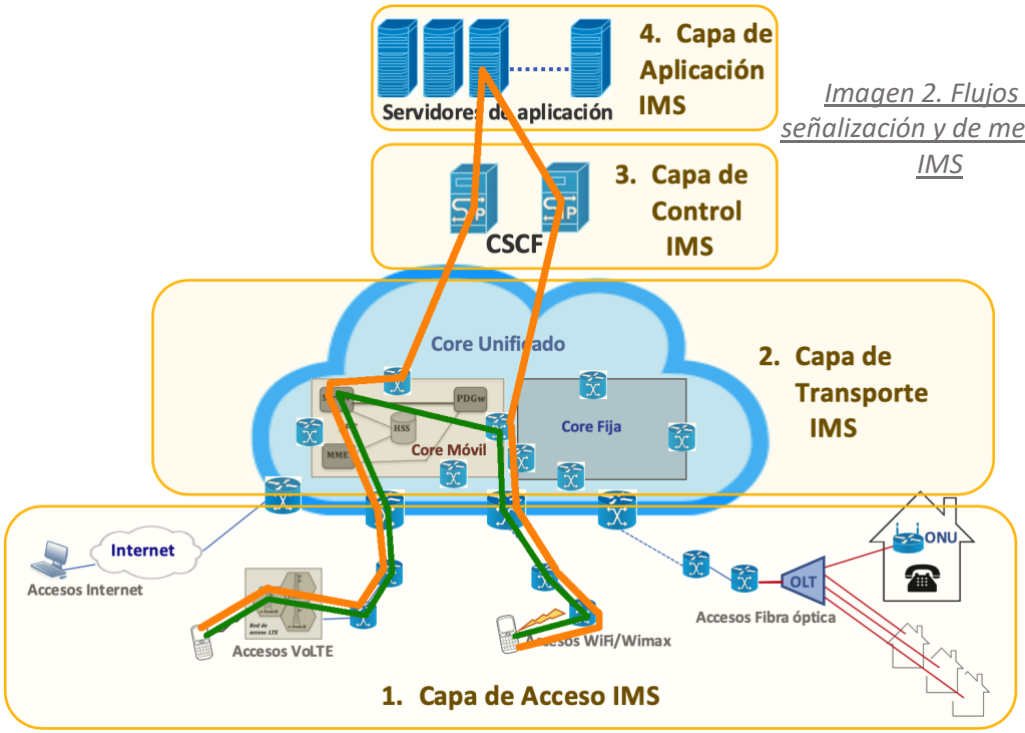


Imagen 2. Flujos de señalización y de media en IMS

Flujo de media (*voz o datos*).

Flujo de señalización.

3. Focalicemos el problema.

El objetivo de este texto, como su título indica, es tratar el tema de la seguridad en IMS, por lo que presentemos en primer lugar cuáles son los potenciales problemas de seguridad.

Tipos de ataques conocidos sobre IMS.

- Visibilidad/Segmentación de red: Este primer paso es un clásico, y se trata de obtener IPs, puertos, SSOO, nombres, aplicaciones, etc. de las diferentes rutas que siguen nuestros paquetes.
- Ataques SIP INVITE: el atacante trata de llamar (paquete INVITE) sin estar registrado previamente.
- Ataques SIP REGISTER: Obtención de información de usuarios y políticas de seguridad de la arquitectura.
- Ataques SIP BYE: Para forzar la desconexión de usuarios.
- Ataques de envenenamiento de caché ARP.
- Ataques MitM (Ataques del hombre del medio): Este tipo de ataques puede ser lanzado, cuando los protocolos SIP y/o RTP viajan en texto plano.
- Escucha/intercepción/redirección de RTP: Operar sobre los paquetes de voz.
- Fuzzing de protocolos: El objetivo de estos patrones de ataque es obtener mensajes de error, respuestas anómalas, o fallos en la pila de protocolos.
- DoS/DDoS/SIP flood : Negación de servicio.
- Escaneos sobre SIP: Obtención de información sobre el plano de control y/o el de aplicación, por medio del protocolo SIP.
- SPIT – spam over IP telephone (SPIT): Envío de llamadas dirigidas y no deseados a teléfonos IP
- Obtención de información sobre los servidores de aplicación (cuentas usuario por defecto, instalaciones por defecto, errores de parcheado o actualización, XSS, SQL injection, etc.).
- SPAM Messaging (SPIM): Envío de mensajes no deseados a teléfonos IP.
- Fraude en el mal uso de SIP, RTP y/o Servidores de aplicación: Se busca evitar el pago de llamadas o revender las mismas.

Formalmente podemos tener en cuenta la **RFC 3261 - SIP: Session Initiation Protocol.**

En el punto: 26 “Security Considerations: Threat Model and Security Usage Recommendations”, nos deja claro diferentes tipos de ataques:

26.1.1 Registration Hijacking

The SIP registration mechanism allows a user agent to identify itself to a registrar as a device at which a user (designated by an address of record) is located. A registrar assesses the identity asserted in the From header field of a REGISTER message to determine whether this request can modify the contact addresses associated with the address-of-record in the To header field. While these two fields are frequently the same, there are many valid deployments in which a third-party may register contacts on a user's behalf.

The From header field of a SIP request, however, can be modified arbitrarily by the owner of a UA, and this opens the door to malicious registrations. An attacker that successfully impersonates a party authorized to change contacts associated with an address-of-record could, for example, de-register all existing contacts for a URI and then register their own device as the appropriate contact address, thereby directing all requests for the affected user to the attacker's device.

This threat belongs to a family of threats that rely on the absence of cryptographic assurance of a request's originator. Any SIP UAS that represents a valuable service (a gateway that interworks SIP requests with traditional telephone calls, for example) might want to control access to its resources by authenticating requests that it receives. Even end-user UAs, for example SIP phones, have an interest in ascertaining the identities of originators of requests.

This threat demonstrates the need for security services that enable SIP entities to authenticate the originators of requests.

El resto de este punto 26.1.x describe diferentes tipos de ataques:

26.1.2 Impersonating a Server

26.1.3 Tampering with Message Bodies

26.1.4 Tearing Down Sessions

26.1.5 Denial of Service and Amplification

Luego describe los mecanismos de seguridad en el punto 26.2 “Security Mechanisms”

26.2 Security Mechanisms

From the threats described above, we gather that the fundamental security services required for the SIP protocol are: preserving the confidentiality and integrity of messaging, preventing replay attacks or message spoofing, providing for the authentication and privacy of the participants in a session, and preventing denial-of-service attacks. Bodies within SIP messages separately require the security services of confidentiality, integrity, and authentication.

Full encryption of messages provides the best means to preserve the confidentiality of signaling - it can also guarantee that messages are not modified by any malicious intermediaries. However, SIP requests and responses cannot be naively encrypted end-to-end in their entirety because message fields such as the Request-URI, Route, and Via need to be visible to proxies in most network architectures so that SIP requests are routed correctly. Note that proxy servers need to modify some features of messages as well (such as adding Via header field values) in order for SIP to function. Proxy servers must therefore be trusted, to some degree, by SIP UAs. To this purpose, low-layer security mechanisms for SIP are recommended, which encrypt the entire SIP requests or responses on the wire on a hop-by-hop basis, and that allow endpoints to verify the identity of proxy servers to whom they send requests.

4. Seguridad en el acceso.

Nos detendremos en particular al principio de este punto, pues dentro del lenguaje de los fabricantes de elementos de seguridad para la infraestructura de IMS, veremos el empleo de varios nombres o dispositivos, y cada uno de ellos en general lo usa a su modo. Para comenzar a abordar el tema de la seguridad de forma adecuada, haremos como siempre nos gusta hacer, es decir analizar qué es lo que dicen los estándares.

El documento con el que debemos comenzar sin lugar a dudas es:

3GPP TS 23.228 V16.0.0 (2019-03) **3rd Generation Partnership Project**; **Technical Specification Group Services and System Aspect**s**; IP Multimedia Subsystem** (IMS); Stage 2 (Release 16)

En su punto 4.14 Nos presenta los conceptos sobre "**Border Control**", hace referencia que, sobre la base de las preferencias del operador, esta función puede ser aplicada entre:

- Dos redes IM CN. (IM Core Network).
- Entre un IM CN y otra red multimedia SIP.

Esas funciones son provistas por el **IBCF** (Interconnection Border Control Function) y desde el punto de vista de la seguridad incluyen:

- Proveer configuraciones de red "ocultando" numeración, capacidades, etc. de la red.
- Monitorización de señalización SIP basada en políticas del operador.
- Selección de apropiadas interconexiones de señalización.
- Indicar cómo tratar una solicitud SIP entrante.
- Etc.

Cuando un IBCF es instalado en una red, este actúa como punto de entrada y salida de la misma. Hasta se hace referencia a que tanto I-CSCF e IBCF puede estar ubicados como un mismo dispositivo físico.

En el Anexo I de este estándar, se presenta en detalle este elemento.

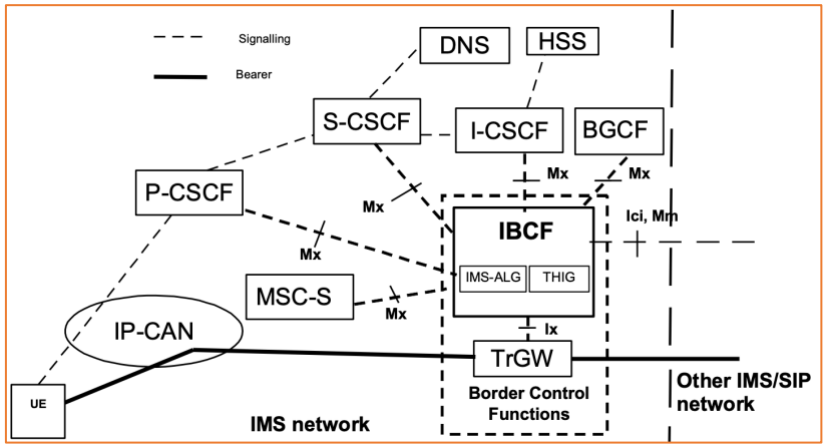
Si analizamos este anexo:

Annex I (Normative): Border Control Functions

Describe la colección de funciones que pueden ser ejecutadas por el IBCF

La figura **I.1** de este anexo lo presenta como sigue:

Figure I.1: Border Control Functions



En la imagen anterior, podemos ver con claridad el rol que desempeña el IBCF dentro del flujo de señalización y también debemos prestar atención al "**TrGW**" (Transition Gateway) que será el responsable del control del flujo de datos.

Sin seguir adelante con mucho más detalle sobre este dispositivo, solo presentaremos finalmente el flujo de ejemplo que propone con un cliente:

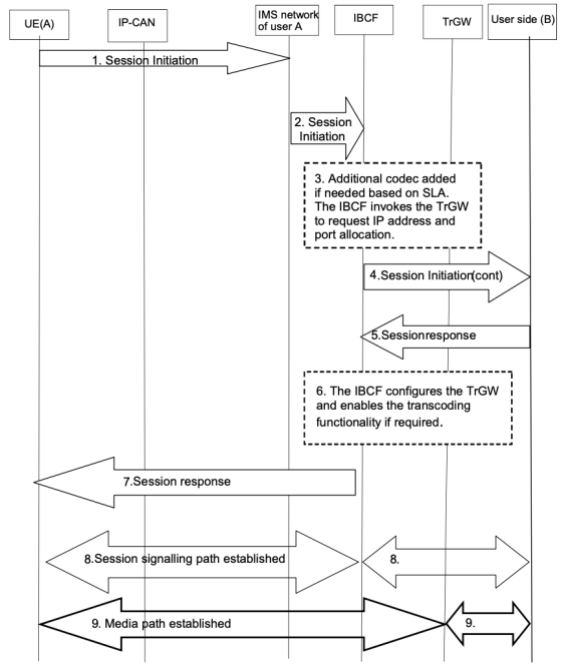


Figure I.4: Proactive transcoding invocation

La intención de la imagen de la derecha, es que podamos apreciar como el IBCF "corta" al flujo SIP entre el cliente y el Core de red del operador, lo cual para nosotros es el detalle a destacar en este texto.

El único documento que conocemos que regula y menciona el concepto de **SBC** (Session Border Controller) es la **RFC - 5853**: **Requirements from Session Initiation Protocol** (SIP) - **Session Border Control** (SBC) **Deployments** de fecha abril de 2010. En la figura 1 de esta RFC, lo presenta de esta forma.

```
                  +-----------------+
                  |       SBC       |
   [signaling]    |  +-----------+  |
<------------|->| signaling |<-|---------->
      outer       |  +-----------+  |   inner
      network     |        |        |   network
                  |  +-----------+  |
<------------|->|   media   |<-|---------->
      [media]     |  +-----------+  |
                  +-----------------+
```

Figure 1: SBC Architecture

Si analizamos la imagen anterior, podemos ver que en definitiva, está desempeñando el mismo rol que el BCF presentado en el párrafo anterior.

El último aspecto a destacar de esta RFC es la idea de "Cripografía" que presenta. En la imagen 14 de la misma, deja claro que el canal de "media" debería viajar "**Encripted**" fuera del Core de la red del operador.

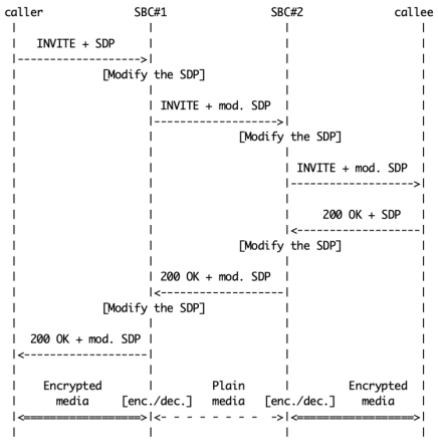


Figure 14: Media Encryption Example

Siguiendo con este concepto de seguridad en "media", la norma: ETSI **TS 133 328** V15.0.0 (2018-07), Universal Mobile Telecommunications System (UMTS); LTE; **IP Multimedia Subsystem (IMS) media plane security** (Release 15)

En sus puntos: 6 Security mechanisms, 6.1 Media security mechanisms, 6.1.1 Media security mechanisms for real-time traffic.

Deja claro que la protección de "**Integridad y Confidencialidad**" del tráfico RTP (Real Time Protool) y RTCP (RT Control Protocol) será habilitada empleando **SRTP** (Secure Real-Time Transport Protocol) y **SRCTP** (ídem).

ETSI y 3GPP especifican el empleo de la familia **IPsec ESP** en modo "túnel" en **TS 33.210** (interconnect and core) y **ESP** (Encapsulation Security Payload) en modo "transporte" en **TS 33.203** (access). Como en este texto, tal cual indicamos al principio, nos interesa evaluar las debilidades que se pueden explotar desde un móvil o un acceso de fibra óptica, detengámonos en la segunda de esta normas.

ETSI TS 133 203 V15.1.0 (2018-09) **Digital cellular telecommunications system** (Phase 2+) (GSM); **Universal Mobile Telecommunications System** (UMTS); **LTE; 3G security; Access security for IP-based services** (3GPP TS 33.203 version 15.1.0 Release 15).

1. Scope

The scope for this technical specification is to specify the security features and mechanisms for secure access to the IM subsystem (IMS) for the 3G mobile telecommunication system.

5.1.3 Confidentiality protection

Possibility for IMS specific confidentiality protection shall be provided to SIP signalling messages between the UE and the P-CSCF. Operators shall take care that the deployed confidentiality protection solution and roaming agreements fulfils the confidentiality requirements presented in the local privacy legislation. The following mechanisms are provided at SIP layer:

1. The UE shall always offer encryption algorithms for P-CSCF to be used for the session, as specified in clause 7.
2. The P-CSCF shall decide whether the IMS specific encryption mechanism is used. If used, the UE and the P-CSCF shall agree on security associations, which include the encryption key that shall be used for the confidentiality protection. The mechanism is based on IMS AKA and specified in clause 6.1.

Confidentiality between CSCFs, and between CSCFs and the HSS shall rely on mechanisms specified by Network Domain Security in TS 33.210 [5].

5.1.4 Integrity protection

Integrity protection shall be applied between the UE and the P-CSCF for protecting the SIP signalling, as specified in clause 6.3. The following mechanisms are provided.

Resumen de los conceptos de seguridad importantes de este punto:

a. En el acceso, la operadora debe instalar un dispositivo (IBGF, SBC) que “oculte” la red core del exterior.
b. Estos dispositivos deberían finalizar las conexiones SIP de acceso (y reenviarlas hacia el Core).
c. Estos dispositivos deben también “aislar” el core de la operadora, respecto a otras operadoras.
d. La operadora debería implantar las medidas de “confidencialidad” e “Integridad” en los accesos para el protocolo SIP (Señalización) por medio de protocolo IPSec en modo transporte.
e. La operadora debería implantar medidas de “confidencialidad” e “Integridad” en los accesos para el protocolo RTP y RCTP, por medio de SRTP y SCRTP.

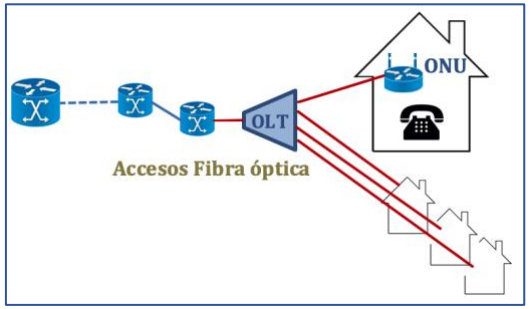
No se ha desarrollado el tema de autenticación, ni el control de acceso, pues esta función se sustenta en la creación de contextos móviles y la validación del router de fibra óptica, que son tecnologías maduras y que serían motivo de otro documento adicional por su complejidad.

Habiendo comprendido este conjunto de medidas de seguridad que las operadoras deberían considerar, seguiremos adelante analizando de forma práctica si es cierto que las adoptan.

5. Análisis de seguridad IMS desde un acceso fijo y desde uno móvil.

Esta última parte del texto se presenta desde los dos puntos principales de acceso que podemos tener a nuestro alcance: fijo y móvil.

a. Acceso fijo (Fibra óptica).



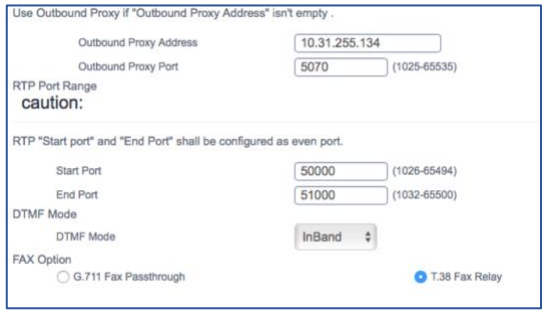
Recordemos que un acceso por medio de fibra óptica, puede ser tanto domiciliario, como empresarial. Las actuales tecnologías de acometida de fibra óptica, en general emplean la tecnología **GPON** (Giga Passive Optical Network) y en estos casos, suelen denominarse: **FTTH** (Fiber To The Home) o para empresas **FTTB** (Fiber To the Building). La lógica es la misma: Se llega con un hilo de fibra hasta la **OLT** (Optical Line Terminator), y desde la OLT, se bifurcan "n" cantidad de nuevos hilos que llegan hasta el destino final ONT (Oplical Network Terminal) del hogar o empresa. La mejor analogía es pensar en la OLT como una especia de "prisma" que divide la luz que le llega por un hilo hacia los "n" salientes, que en la actualidad, esta tecnología permite acometer en el orden de 32, 64 y hasta 128 nuevos hilos de Fibra cuyos destinos finales serán ese mismo número de ONTs.

Entender este primer concepto es importante, pues en definitiva hasta la OLT desde nuestros hogares, llegamos por medio de un nivel físico (fibra óptica), un nivel de enlace (Ethernet), uno de red (IP) y uno de transporte (TCP y/o UDP).

La OLT, dependiendo del fabricante y el operador, valida a ese router de cliente, por diferentes tipos de parámetros, en general suele ser por direccionamiento MAC, por un número de código del fabricante y/o OLT o por un secreto compartido.

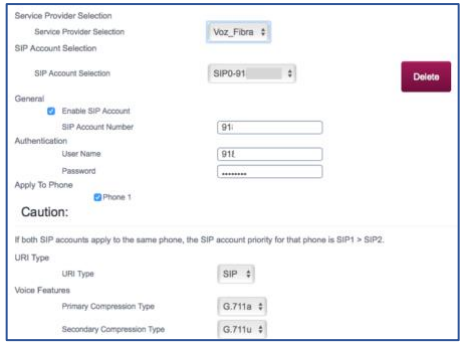
El primer aspecto a considerar para poder avanzar sobre la red del operador, es sin lugar a dudas poder lograr acceso al router cliente (el que tengo en casa) y de ser posible escalar privilegios (root) sobre el mismo. Solo de este forma, podré "operar" sobre la interfaz o interfaces de salida del mismo. También podríamos plantearnos instalar un "splitter" de fibra óptica… si es que contamos con más de 10.000 euros para comprarlo, o también con un switch de fibra, que otra alternativa (costosa también). En resumen lo más accesible, es pegarse unas horas en Internet y encontrar la forma de escalar privilegios en mi router, cosa que suele lograrse con altas tasas de éxito… aunque, por supuesto, aquí no daremos más consejos al respecto.

NOTA: en ninguna de las imágenes que se presentan en este texto, se ha dejado información pública sobre el operador de la red.



Al acceder al router, comenzamos a recolectar información sobre la red del operador, podemos identificar su esquema de direccionamiento, los puertos que emplea.

Se puede identificar el empleo y configuraciones de SIP y RTP. Un dato importante es la identificación de interfaces y tablas de rutas, pues con ello sabemos por donde capturar y dirigir el tráfico.



IPv4 Routing Table :

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
0.0.0.0	0.0.0.0	0.0.0.0	U	0	6	ppp0.1
1.1.1.0	0.0.0.0	255.255.255.0	U	0		br0
10.28.64.0	0.0.0.0	255.255.192.0	U	0	3	veip0.2
10.31.218.107	10.28.64.1	255.255.255.255	UGH	0	3	veip0.2
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0
192.168.116.141	10.28.64.1	255.255.255.255	UGH	0	3	veip0.2
192.168.144.1	0.0.0.0	255.255.255.255	UH	0	6	ppp0.1
192.168.249.0	0.0.0.0	255.255.255.252	U	0		br0

En el caso de lograr escalar privilegios y ser "root" de ese router, podremos también editar y modificar las tablas del firewall interno que posee.

Tal vez lo más importante de toda esta información es que nos abre las puertas para comenzar nuestro avance sobre la red del operador y nos presenta los caminos a seguir.

Sobre la información recolectada, es necesario profundizar un poco más para poder analizar qué otros dispositivos son alcanzables desde mi accesos, en particular lo que menos debería ser visible son los rangos de direccionamiento privado, pues los mismos nos indican que son direcciones que el operador emplea "internamente".

veip0.2 3 IPoE 10.28.77.184
ppp0.1 6 PPPoE 8x.xxx.xxx.xxx

En QoS classification se ve:
NGNpublic 1 Local 8x.xxx.xxx.0/22 UDP
ACS 2 Local 8x.xxx.xxx.xxx/26

11	☑	SSH_22_Range1	ppp0.1	Protocol: TCP Src IP: 8 Src Mask: 255.255.255.128 Dst Port: 22	Action: Permit	☐	Edit
12	☑	SSH_22_Range2	ppp0.1	Protocol: TCP Src IP: 172.20.25.1 Src Mask: 255.255.255.0 Dst Port: 22	Action: Permit	☐	Edit
13	☑	SSH_22_Range3	ppp0.1	Protocol: TCP Src IP: 172.20.45.1 Src Mask: 255.255.255.0 Dst Port: 22	Action: Permit	☐	Edit
14	☑	SSH_22_Range4	ppp0.1	Protocol: TCP Src IP: 19 Src Mask: 255.255.255.240 Dst Port: 22	Action: Permit	☐	Edit
15	☑	Telnet_23	br0	Protocol: TCP or UDP Dst IP: 192.168.1.1 Dst Mask: 255.255.255.255 Dst Port: 23	Action: Drop	☐	Edit

Si se lanza un "**traceroute**" sobre cada una de las interfaces, se podrá evaluar el camino que siguen cada una de ellas.

```
# traceroute to 8x.xxx.xxx.xxx (8x.xxx.xxx.xxx), 64 hops max, 52 byte packets
 1  192.168.1.1 (192.168.1.1)  6.255 ms  1.782 ms  2.264 ms
 2  192.168.144.1 (192.168.144.1)  5.792 ms  5.910 ms  6.779 ms
 3  9x……................  8.971 ms
    1x……................  6.768 ms
 4  2xx…..7.272 ms  16.520 ms  6.142 ms

……
```

Cuando se detectan rangos privados (Ej: 192.168.144.1) se debe seguir avanzando en profundidad sobre los mismos, por ejemplo:

 # nmap -n -sT --open 192.168.144.0/24

Siguiendo estos pasos, en principio se obtiene un buen "fingerprinting" de esa arquitectura de red del operador.

Para comenzar a evaluar la arquitectura IMS, es necesario primero saber qué tipo de medidas de seguridad está implantando el operador. Veamos una captura de tráfico.

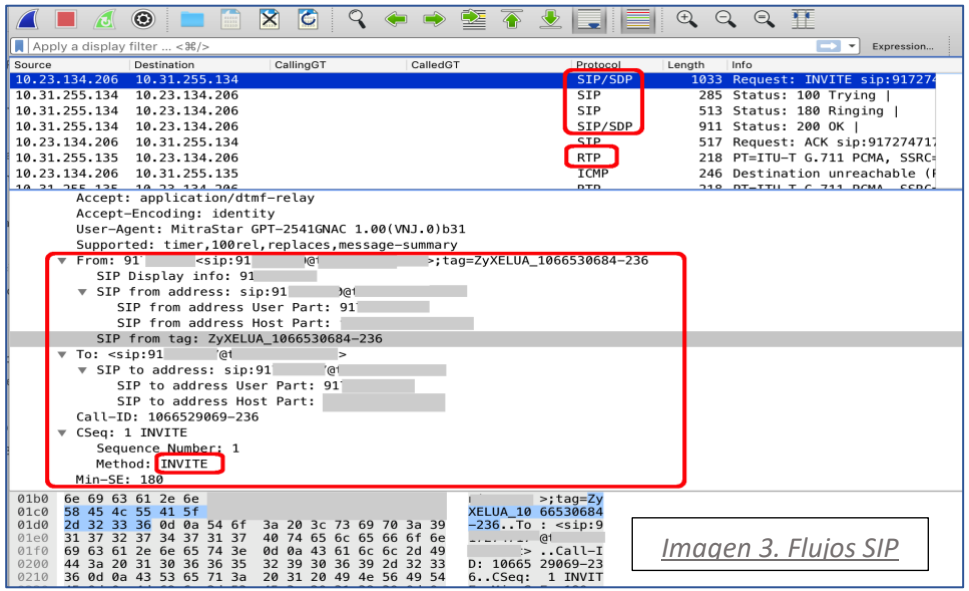


Imagen 3. Flujos SIP

En la imagen de la izquierda, queda claro que el operador en cuestión está empleando protocolo SIP (en texto plano) y también RTP.

Un detalle adicional, es que la OLT que mencionamos al principio, básicamente a nivel de enlace, opera como un "Switch", es decir que si se logra realizar algún tipo de "envenenamiento cache" podremos realizar escuchas y hasta ataques del hombre del medio sobre el tráfico de voz de cualquiera de los vecinos (32, 64 0 128) que estén conectados por ese último segmento de fibra óptica a la misma.

A continuación se presenta una captura de este tipo de tráfico RTP.

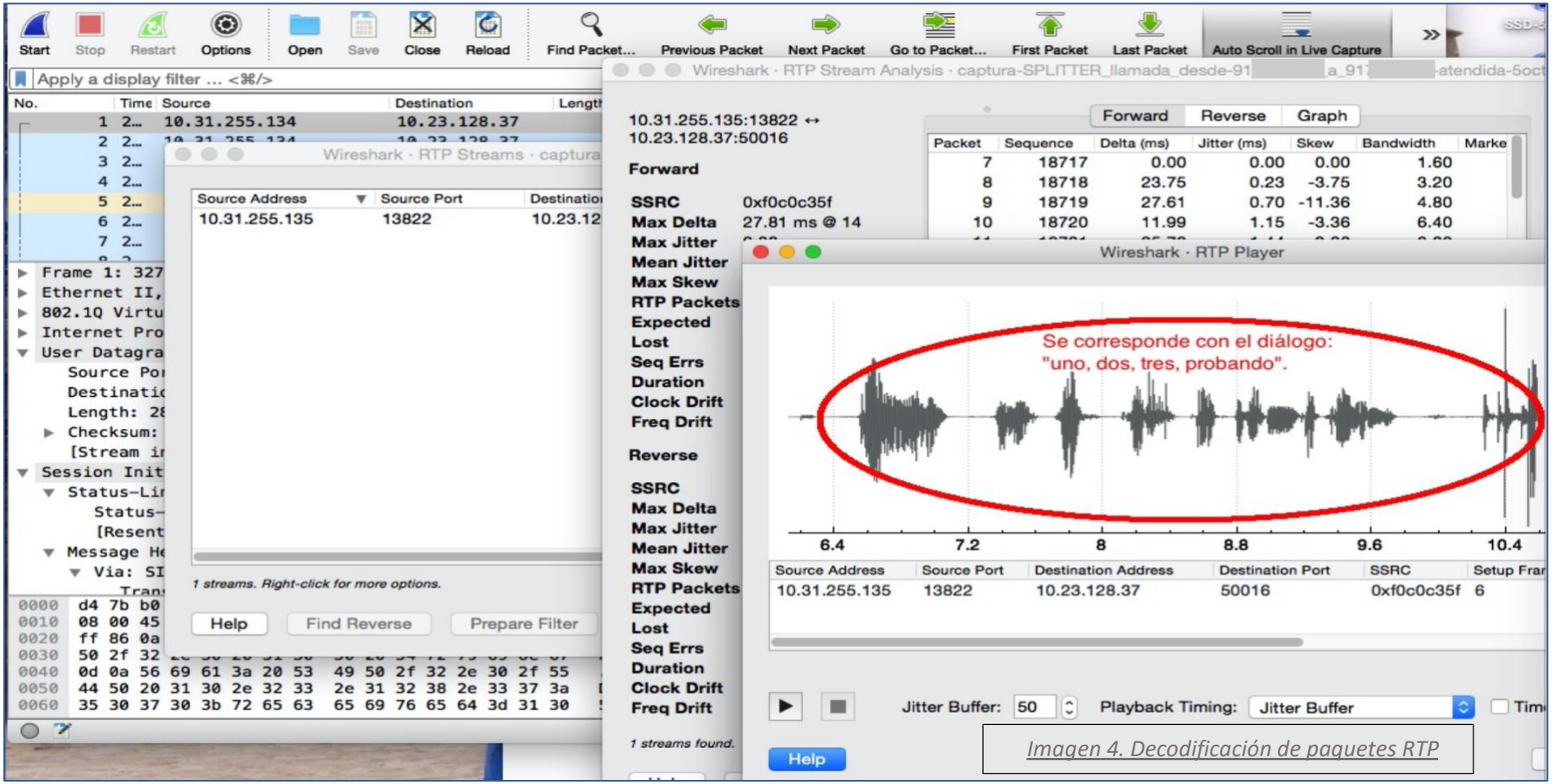


Imagen 4. Decodificación de paquetes RTP

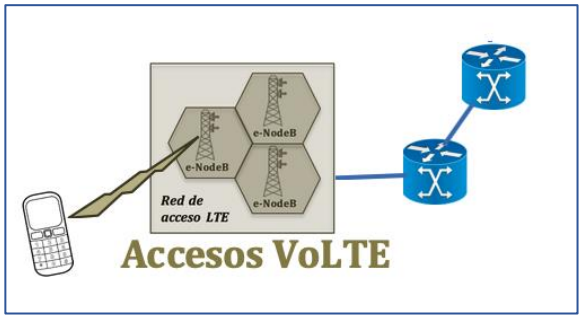
Todo lo que acabamos de presentar es un caso real, sobre un acceso a la red de voz paquetizada de una operadora por medio de un enlace FTTH. Esta actividad es posible, en virtud que en este caso, la operadora:

- Instala en domicilio del cliente un router que no se encuentra debidamente bastionado.
- No oculta los dispositivos de su propia red.
- No emplea medidas de seguridad en su OLT.
- No emplea "confidencialidad" en SIP ni RTP.
- No emplea protocolo IPSec para el acceso.

Al final de este texto veremos herramientas concretas que se pueden emplear para operar con protocolo SIP y RTP y que aplican a cualquier tipo de accesos. Estas herramientas son las que permiten realizar todo tipo de ataques sobre infraestructuras IMS, tanto en el acceso como en el Core, cuando la operadora ofrece este tipo de debilidades.

b. Acceso móvil (VoLTE).

Como hemos presentado al principio, básicamente el acceso a una red VoLTE, responde al esquema de la imagen de la derecha.



El **UE** (User Equipement) se conecta a través de un **e-nodeB** a la red y desde el mismo está en contacto directamente con el Core de 4G que se llama **EPC** (Evolved Packet Core), no es motivo de este texto entrar en detalles sobre el mismo. A partir de este EPC el acceso a IMS es similar al que acabamos de ver para la red fija.

En este caso, lo primero que se debe hacer para analizar la arquitectura IMS, es poder "**rootear**" un teléfono móvil, para poder operar sobre el mismo como si fuera un ordenador portátil, o mejor aún, una vez "rooteado" instalar en el móvil un servidor SSH y conectarse al mismo desde un ordenador portátil para poder operar de forma más amigable. Veamos brevemente estos pasos.

Estas líneas **no** son un manual para rootear teléfonos móviles, sencillamente es transmitir brevemente nuestra experiencia. Una herramienta sencilla para poder "rootear un teléfono móvil con Android, es "**ODIN**".

Los pasos están bien explicados en nuestro video:
Hacking móvil (https://youtu.be/ZKlqqdbQl9o)

Por supuesto tomemos primero todas las medidas para poder hacer un "roll back" (volver atrás si algo falla) y sólo agregar que aconsejamos como punto de partida, actualizar la versión de Android a exactamente la misma que nos indica Odin para nuestro dispositivo antes de comenzar con el proceso.

La segunda herramienta que recomendamos es "**Termux**" que se trata de una interfaz por línea de comandos que ya trae muchos comandos iguales o similares a cualquier Linux. Si deseamos conectarnos desde un portátil, un buen software es el mismo demonio "**sshd**" que ya viene instalado en Termux (y se lanza con "sshd") y recomendamos también los clásicos: openssh, nmap, tcpdump, wget, coreutils, vim, etc…

Como se puede apreciar en la imagen de este lateral, una vez instalado y ejecutado "Termux" tenemos una interfaz de línea de comandos en la que es posible escalar a "root".

A partir de ahora, los pasos a seguir son similares a los que planteamos anteriormente, con la salvedad que las redes 4G cuando emplean VoLTE, crean dos "contextos" y por lo tanto tendrá al menos dos interfaces con direccionamiento IP. A continuación presentamos un ejemplo real de las mismas:

#Ifconfig

```
rmnet2  176.87.226.22/30
rmnet1  xxxx:xxxx:xxxx:0:1:2:5a52:df09
rmnet0  10.91.79.121/30
wlan0   192.168.43.1/24
```

En una de las conexiones de prueba de esta arquitectura VoLTE, se capturó tráfico seguro, es decir el caso en que la operadora hace uso del protocolo IPSec, tal cual se aprecia en la imagen que sigue.

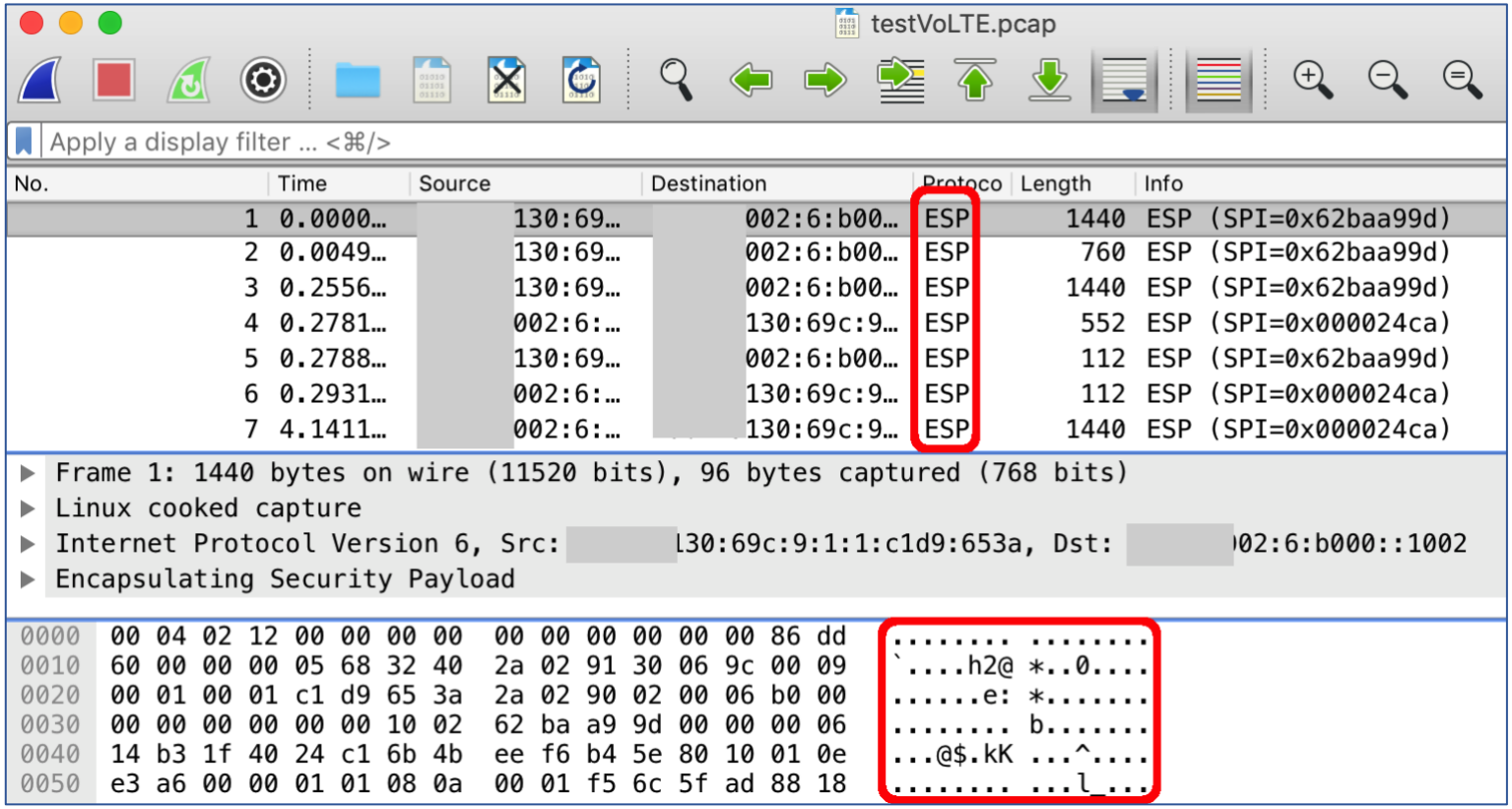


Imagen 5. Tráfico ESP (IPSec)

Como podemos ver, en todas las tramas, se está empleando **ESP** (Encapsulation Security Payload), con lo cual, resulta imposible desencriptar la misma o modificar cualquier bit, pues, tal cual se indicó, en este caso la operadora tuvo en cuenta "Confidencialidad" e "Integridad" por medio del empleo de **IPSec**.

Hemos querido presentar la imagen anterior, justamente para que podamos comparar la diferencia de una red IMS bastionada de una que no lo está.

6. Empleo de herramientas.

Aprovechamiento del protocolo SIP

A continuación presentamos algunos flujos de los ataques que se han mencionado sobre SIP:

Corte de llamadas

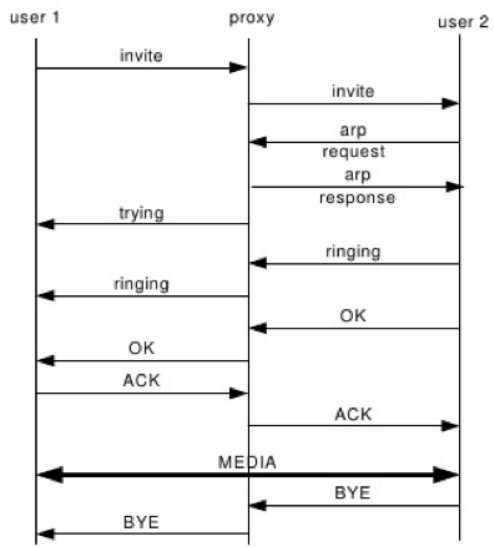


Figure 2. Normal session termination

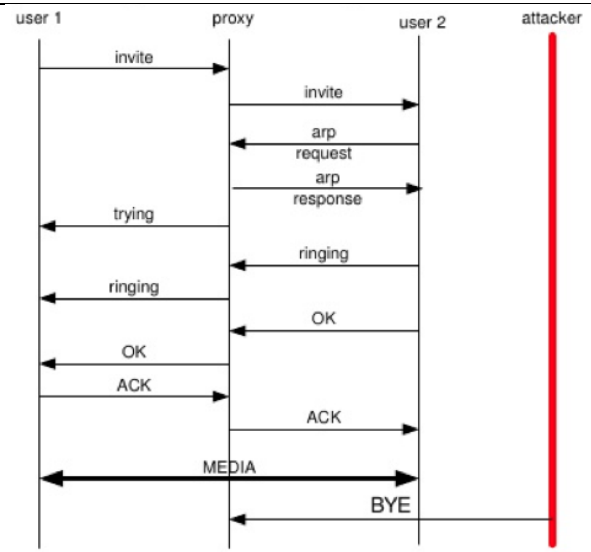


Figure 3. BYE attack

Cancelación de llamadas

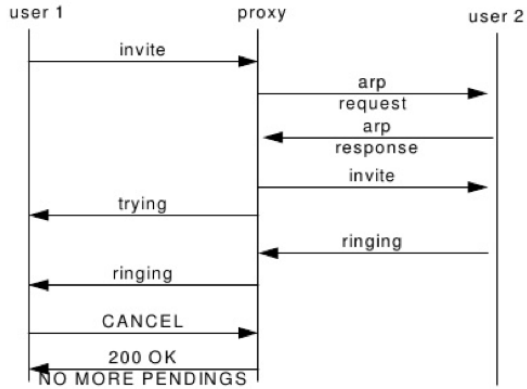


Figure 4. CANCEL request

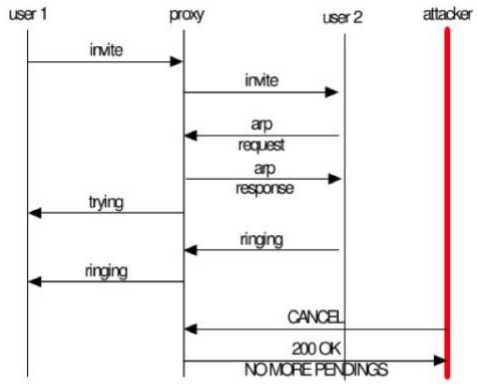


Figure 5. CANCEL attack

Re -invite

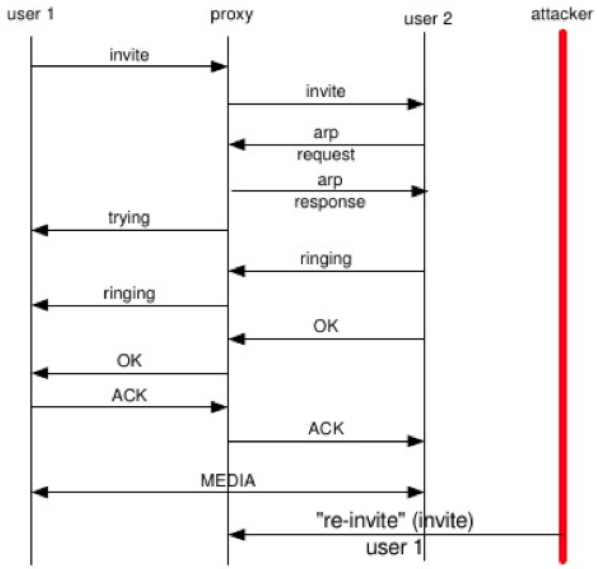


Figure 6. "Re-INVITE" Attack

Update

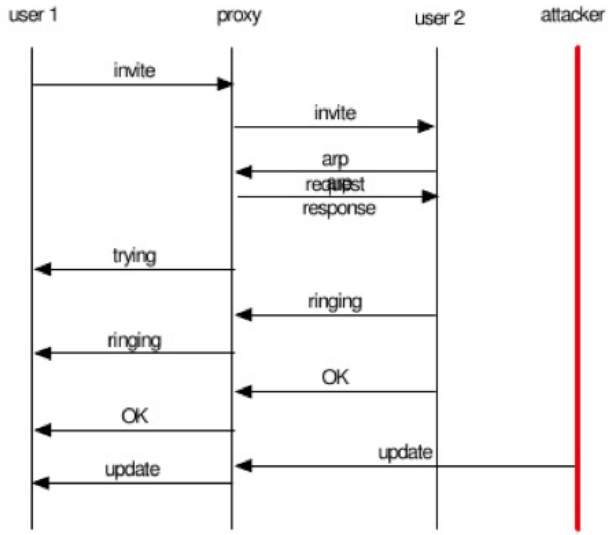


Figure 7. UPDATE attack

Vamos a analizar el tráfico desde una central de una operadora de telefonía Internacional:

(Se presentan únicamente las imágenes, pero durante el trabajo real se analizó todo el flujo con "Wireshark" de esta captura real de varias comunicaciones internacionales por medio de una infraestructura IMS).

Filter: (ip.addr eq 10.15.24.244 and ip.addr eq 10.15 | Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
552	17:00:30.329004	10.15.24.244	10.15.4.16	SIP	592	Request: PRACK sip:10.15.4.16:5060 |
798	17:00:30.339974	10.15.24.244	10.15.4.16	SIP/SDP	1125	Request: INVITE sip:201010452223062571@10.15.4.16 | , with session description
1147	17:00:30.355609	10.15.24.244	10.15.4.16	SIP/SDP	1124	Request: INVITE sip:201010455558567932@10.15.4.16 | , with session description
1200	17:00:30.358145	10.15.24.244	10.15.4.16	SIP	592	Request: BYE sip:10.15.4.16:5060 |
1753	17:00:30.384702	10.15.24.244	10.15.4.16	SIP	611	Request: BYE sip:10.15.4.16:5060 |
1754	17:00:30.384805	10.15.24.244	10.15.4.16	SIP	895	Request: ACK sip:201010453171085346@172.25.0.36 |
2249	17:00:30.406317	10.15.24.244	10.15.4.16	SIP	589	Request: PRACK sip:10.15.4.16:5060 |
2468	17:00:30.416428	10.15.24.244	10.15.4.16	SIP/SDP	890	Status: 183 Session Progress | , with session description
3528	17:00:30.463006	10.15.24.244	10.15.4.16	SIP/SDP	1016	Request: INVITE sip:00505219631143500@10.15.4.16 | , with session description
3692	17:00:30.469851	10.15.24.244	10.15.4.16	SIP	894	Request: ACK sip:201010457731194755@172.25.0.36 |
3793	17:00:30.474663	10.15.24.244	10.15.4.16	SIP/SDP	979	Request: INVITE sip:00245216441575476@10.15.4.16;user=phone | , with session de
3885	17:00:30.478546	10.15.24.244	10.15.4.16	SIP	592	Request: PRACK sip:10.15.4.16:5060 |
4049	17:00:30.486539	10.15.24.244	10.15.4.16	SIP/SDP	1125	Request: INVITE sip:201010459993254682@10.15.4.16 | , with session description
4758	17:00:30.517827	10.15.24.244	10.15.4.16	SIP/SDP	1124	Request: INVITE sip:201010446672022517@10.15.4.16 | , with session description
5403	17:00:30.546624	10.15.24.244	10.15.4.16	SIP	542	Request: CANCEL sip:00505216142475683@10.15.4.16 |
5847	17:00:30.567439	10.15.24.244	10.15.4.16	SIP	592	Request: PRACK sip:10.15.4.16:5060 |
5879	17:00:30.569135	10.15.24.244	10.15.4.16	SIP	592	Request: PRACK sip:10.15.4.16:5060 |
5939	17:00:30.571747	10.15.24.244	10.15.4.16	SIP	569	Request: ACK sip:00505216142475683@200.36.178.10 |
5973	17:00:30.572816	10.15.24.244	10.15.4.16	SIP/SDP	912	Request: INVITE sip:00505218711833339@10.15.4.16 | , with session description
6225	17:00:30.584893	10.15.24.244	10.15.4.16	SIP	620	Request: ACK sip:00245217331226715@200.36.178.10;user=phone |
6408	17:00:30.592167	10.15.24.244	10.15.4.16	SIP	592	Request: PRACK sip:10.15.4.16:5060 |
6521	17:00:30.597713	10.15.24.244	10.15.4.16	SIP	556	Request: ACK sip:10.15.4.16:5060 |

- Frame 552: 592 bytes on wire (4736 bits), 592 bytes captured (4736 bits)
- Ethernet II, Src: 4c:00:82:e7:ee:00 (4c:00:82:e7:ee:00), Dst: 00:17:e0:39:95:c0 (00:17:e0:39:95:c0)
- Internet Protocol Version 4, Src: 10.15.24.244 (10.15.24.244), Dst: 10.15.4.16 (10.15.4.16)
- User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
- Session Initiation Protocol (PRACK)
  - Request-Line: PRACK sip:10.15.4.16:5060 SIP/2.0
    - Method: PRACK

Imagen 6. Tráfico (Wireshark)

De este tráfico real, seleccionamos (exportamos) sólo una trama “INVITE”.

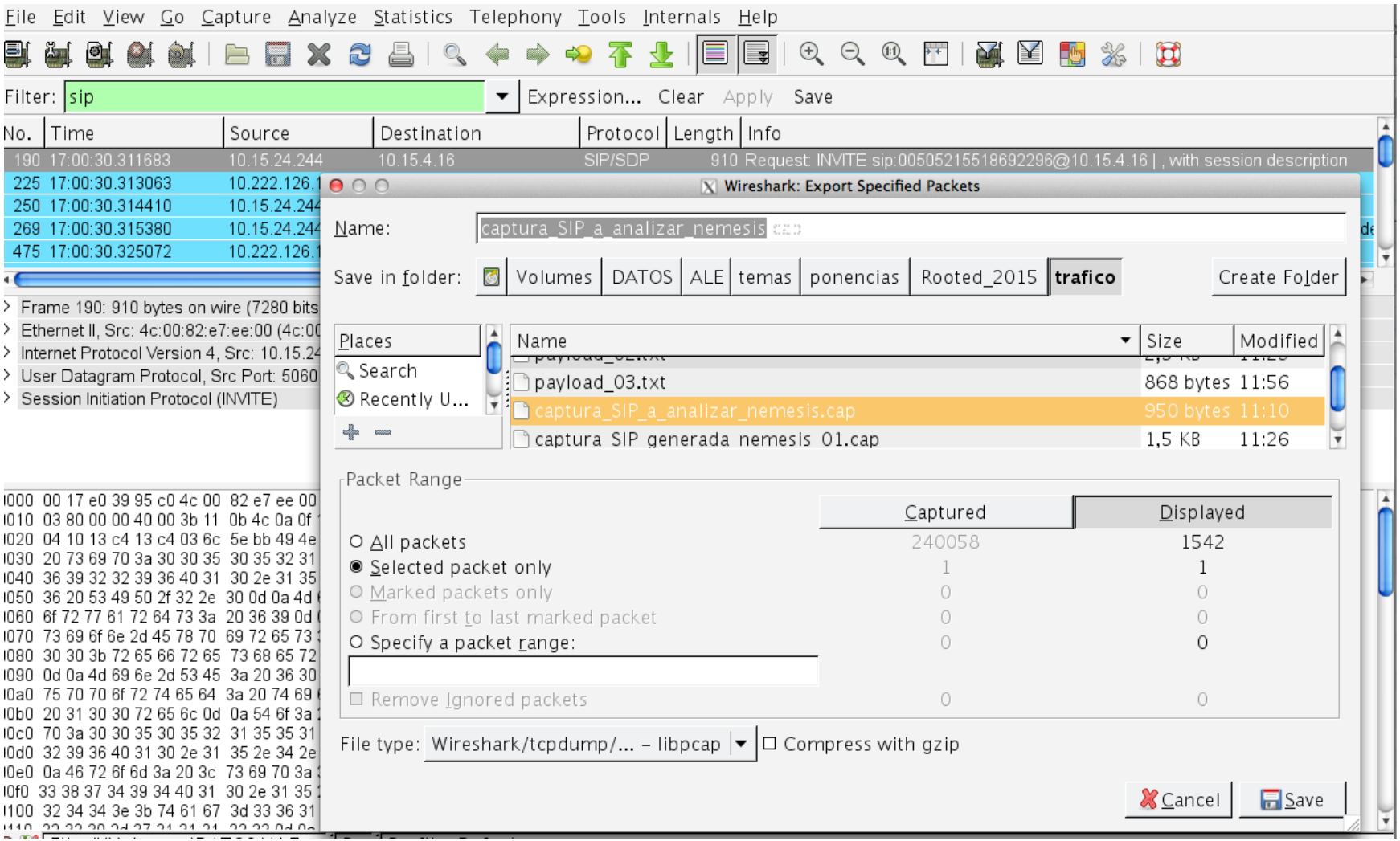


Imagen 7. (Wireshark)

Para un mejor análisis y trabajo con las misma, desde Wireshark también la “Imprimimos” en formato texto, y nos queda como se presenta a continuación (*Algún dato de numeración telefónica ha sido modificada par ocultar datos reales*):

```
No.  Time          Source          Destination     Protocol Length Info
   1 17:00:30.311683 10.15.24.244    10.15.4.16      SIP/SDP  910    Request: INVITE sip:00605215518692396@10.15.4.16 | , with session description

Frame 1: 910 bytes on wire (7280 bits), 910 bytes captured (7280 bits)
  WTAP_ENCAP: 1
  Arrival Time: Jul 25, 2014 17:00:30.311683000 CEST
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1406300430.311683000 seconds
  [Time delta from previous captured frame: 0.000000000 seconds]
  [Time delta from previous displayed frame: 0.000000000 seconds]
  [Time since reference or first frame: 0.000000000 seconds]
  Frame Number: 1
  Frame Length: 910 bytes (7280 bits)
  Capture Length: 910 bytes (7280 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ip:udp:sip:sdp]
  [Coloring Rule Name: UDP]
  [Coloring Rule String: udp]
Ethernet II, Src: 4c:00:82:e7:ee:00 (4c:00:82:e7:ee:00), Dst: 00:17:e0:39:95:c0 (00:17:e0:39:95:c0)
  Destination: 00:17:e0:39:95:c0 (00:17:e0:39:95:c0)
    Address: 00:17:e0:39:95:c0 (00:17:e0:39:95:c0)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: 4c:00:82:e7:ee:00 (4c:00:82:e7:ee:00)
    Address: 4c:00:82:e7:ee:00 (4c:00:82:e7:ee:00)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Type: IP (0x0800)
Internet Protocol Version 4, Src: 10.15.24.244 (10.15.24.244), Dst: 10.15.4.16 (10.15.4.16)
  Version: 4
  Header length: 20 bytes
```

```
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
      0000 00.. = Differentiated Services Codepoint: Default (0x00)
      .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
    Total Length: 896
    Identification: 0x0000 (0)
    Flags: 0x02 (Don't Fragment)
      0... .... = Reserved bit: Not set
      .1.. .... = Don't fragment: Set
      ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 59
    Protocol: UDP (17)
    Header checksum: 0x0b4c [correct]
      [Good: True]
      [Bad: False]
    Source: 10.15.24.244 (10.15.24.244)
    Destination: 10.15.4.16 (10.15.4.16)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
    Source port: 5060 (5060)
    Destination port: 5060 (5060)
    Length: 876
    Checksum: 0x5ebb [validation disabled]
      [Good Checksum: False]
      [Bad Checksum: False]
  Session Initiation Protocol (INVITE)
    Request-Line: INVITE sip: 00605215518692396@10.15.4.16 SIP/2.0
      Method: INVITE
      Request-URI: sip: 00605215518692396@10.15.4.16
        Request-URI User Part: 00605215518692396
        Request-URI Host Part: 10.15.4.16
      [Resent Packet: False]
    Message Header
      Max-Forwards: 69
      Session-Expires: 3600;refresher=uac
```

```
    Min-SE: 600
    Supported: timer, 100rel
    To: <sip: 00605215518692396@10.15.4.16>
      SIP to address: sip: 00605215518692396@10.15.4.16
        SIP to address User Part: 00605215518692396
        SIP to address Host Part: 10.15.4.16
    From: <sip:3466387494@10.15.24.244>;tag=3615289230-711133
      SIP from address: sip:3466387494@10.15.24.244
        SIP from address User Part: 3466387494
        SIP from address Host Part: 10.15.24.244
      SIP from tag: 3615289230-711133
    Call-ID: 753261-3615289230-711129@MTY-BMSW-01D.datos.temm
    CSeq: 1 INVITE
      Sequence Number: 1
      Method: INVITE
    Allow: CANCEL, ACK, INVITE, BYE, OPTIONS, REGISTER, NOTIFY, INFO, REFER, SUBSCRIBE, PRACK, UPDATE, MESSAGE, PUBLISH
    Via: SIP/2.0/UDP 10.15.24.244:5060;branch=z9hG4bK9b39c13355d40025c8ae6fb918f289b8
      Transport: UDP
      Sent-by Address: 10.15.24.244
      Sent-by port: 5060
      Branch: z9hG4bK9b39c13355d40025c8ae6fb918f289b8
    Contact: <sip:3466387494@10.15.24.244:5060>
      Contact URI: sip:3466387494@10.15.24.244:5060
        Contact URI User Part: 3466387494
        Contact URI Host Part: 10.15.24.244
        Contact URI Host Port: 5060
    Content-Type: application/sdp
    Accept: application/sdp
    Content-Length: 227
  Message Body
    Session Description Protocol
      Session Description Protocol Version (v): 0
      Owner/Creator, Session Id (o): MTY-BMSW-01D 188 1 IN IP4 10.15.24.244
        Owner Username: MTY-BMSW-01D
        Session ID: 188
        Session Version: 1
```

```
    Owner Network Type: IN
    Owner Address Type: IP4
    Owner Address: 10.15.24.244
Session Name (s): sip call
Connection Information (c): IN IP4 10.15.24.245
    Connection Network Type: IN
    Connection Address Type: IP4
    Connection Address: 10.15.24.245
Time Description, active time (t): 0 0
    Session Start Time: 0
    Session Stop Time: 0
Media Description, name and address (m): audio 23766 RTP/AVP 18 101
    Media Type: audio
    Media Port: 23766
    Media Protocol: RTP/AVP
    Media Format: ITU-T G.729
    Media Format: DynamicRTP-Type-101
Media Attribute (a): rtpmap:18 G729/8000
    Media Attribute Fieldname: rtpmap
    Media Format: 18
    MIME Type: G729
    Sample Rate: 8000
Media Attribute (a): fmtp:18 annexb=no
    Media Attribute Fieldname: fmtp
    Media Format: 18 [G729]
    Media format specific parameters: annexb=no
Media Attribute (a): rtpmap:101 telephone-event/8000
    Media Attribute Fieldname: rtpmap
    Media Format: 101
    MIME Type: telephone-event
    Sample Rate: 8000
Media Attribute (a): fmtp:101 0-15
    Media Attribute Fieldname: fmtp
    Media Format: 101 [telephone-event]
    Media format specific parameters: 0-15
Media Attribute (a): ptime:20
```

```
        Media Attribute Fieldname: ptime
        Media Attribute Value: 20

0000  00 17 e0 39 95 c0 4c 00 82 e7 ee 00 08 00 45 00   ...9..L.......E.
0010  03 80 00 00 40 00 3b 11 0b 4c 0a 0f 18 f4 0a 0f   ....@.;..L......
0020  04 10 13 c4 13 c4 03 6c 5e bb 49 4e 56 49 54 45   .......l^.INVITE
0030  20 73 69 70 3a 30 30 35 30 35 32 31 35 35 31 38    sip:00605215518
0040  36 39 32 32 39 36 40 31 30 2e 31 35 2e 34 2e 31   692396@10.15.4.1
0050  36 20 53 49 50 2f 32 2e 30 0d 0a 4d 61 78 2d 46   6 SIP/2.0..Max-F
0060  6f 72 77 61 72 64 73 3a 20 36 39 0d 0a 53 65 73   orwards: 69..Ses
0070  73 69 6f 6e 2d 45 78 70 69 72 65 73 3a 20 33 36   sion-Expires: 36
0080  30 30 3b 72 65 66 72 65 73 68 65 72 3d 75 61 63   00;refresher=uac
0090  0d 0a 4d 69 6e 2d 53 45 3a 20 36 30 30 0d 0a 53   ..Min-SE: 600..S
00a0  75 70 70 6f 72 74 65 64 3a 20 74 69 6d 65 72 2c   upported: timer,
00b0  20 31 30 30 72 65 6c 0d 0a 54 6f 3a 20 3c 73 69    100rel..To: <si
00c0  70 3a 30 30 35 30 35 32 31 35 35 31 38 36 39 32   p:00605215518692
00d0  32 39 36 40 31 30 2e 31 35 2e 34 2e 31 36 3e 0d   396@10.15.4.16>.
00e0  0a 46 72 6f 6d 3a 20 3c 73 69 70 3a 33 34 37 37   .From: <sip:3466
00f0  33 38 37 34 39 34 40 31 30 2e 31 35 2e 32 34 2e   387494@10.15.24.
0100  32 34 34 3e 3b 74 61 67 3d 33 36 31 35 32 38 39   244>;tag=3615289
0110  32 33 30 2d 37 31 31 31 33 33 0d 0a 43 61 6c 6c   230-711133..Call
0120  2d 49 44 3a 20 37 35 33 32 36 31 2d 33 36 31 35   -ID: 753261-3615
0130  32 38 39 32 33 30 2d 37 31 31 31 32 39 40 4d 54   289230-711129@MT
0140  59 2d 42 4d 53 57 2d 30 31 44 2e 64 61 74 6f 73   Y-BMSW-01D.datos
0150  2e 74 65 6d 6d 0d 0a 43 53 65 71 3a 20 31 20 49   .temm..CSeq: 1 I
0160  4e 56 49 54 45 0d 0a 41 6c 6c 6f 77 3a 20 43 41   NVITE..Allow: CA
0170  4e 43 45 4c 2c 20 41 43 4b 2c 20 49 4e 56 49 54   NCEL, ACK, INVIT
0180  45 2c 20 42 59 45 2c 20 4f 50 54 49 4f 4e 53 2c   E, BYE, OPTIONS,
0190  20 52 45 47 49 53 54 45 52 2c 20 4e 4f 54 49 46    REGISTER, NOTIF
01a0  59 2c 20 49 4e 46 4f 2c 20 52 45 46 45 52 2c 20   Y, INFO, REFER,
01b0  53 55 42 53 43 52 49 42 45 2c 20 50 52 41 43 4b   SUBSCRIBE, PRACK
01c0  2c 20 55 50 44 41 54 45 2c 20 4d 45 53 53 41 47   , UPDATE, MESSAG
01d0  45 2c 20 50 55 42 4c 49 53 48 0d 0a 56 69 61 3a   E, PUBLISH..Via:
01e0  20 53 49 50 2f 32 2e 30 2f 55 44 50 20 31 30 2e    SIP/2.0/UDP 10.
01f0  31 35 2e 32 34 2e 32 34 34 3a 35 30 36 30 3b 62   15.24.244:5060;b
0200  72 61 6e 63 68 3d 7a 39 68 47 34 62 4b 39 62 33   ranch=z9hG4bK9b3
```

```
0210  39 63 31 33 33 35 35 64 34 30 30 32 35 63 38 61   9c13355d40025c8a
0220  65 36 66 62 39 31 38 66 32 38 39 62 38 0d 0a 43   e6fb918f289b8..C
0230  6f 6e 74 61 63 74 3a 20 3c 73 69 70 3a 33 34 37   ontact: <sip:347
0240  37 33 38 37 34 39 34 40 31 30 2e 31 35 2e 32 34   7289494@10.15.24
0250  2e 32 34 34 3a 35 30 36 30 3e 0d 0a 43 6f 6e 74   .244:5060>..Cont
0260  65 6e 74 2d 54 79 70 65 3a 20 61 70 70 6c 69 63   ent-Type: applic
0270  61 74 69 6f 6e 2f 73 64 70 0d 0a 41 63 63 65 70   ation/sdp..Accep
0280  74 3a 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 73   t: application/s
0290  64 70 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67   dp..Content-Leng
02a0  74 68 3a 20 32 32 37 0d 0a 0d 0a 76 3d 30 0d 0a   th: 227....v=0..
02b0  6f 3d 4d 54 59 2d 42 4d 53 57 2d 30 31 44 20 31   o=MTY-BMSW-01D 1
02c0  38 38 20 31 20 49 4e 20 49 50 34 20 31 30 2e 31   88 1 IN IP4 10.1
02d0  35 2e 32 34 2e 32 34 34 0d 0a 73 3d 73 69 70 20   5.24.244..s=sip
02e0  63 61 6c 6c 0d 0a 63 3d 49 4e 20 49 50 34 20 31   call..c=IN IP4 1
02f0  30 2e 31 35 2e 32 34 2e 32 34 35 0d 0a 74 3d 30   0.15.24.245..t=0
0300  20 30 0d 0a 6d 3d 61 75 64 69 6f 20 32 33 37 36    0..m=audio 2376
0310  36 20 52 54 50 2f 41 56 50 20 31 38 20 31 30 31   6 RTP/AVP 18 101
0320  0d 0a 61 3d 72 74 70 6d 61 70 3a 31 38 20 47 37   ..a=rtpmap:18 G7
0330  32 39 2f 38 30 30 30 0d 0a 61 3d 66 6d 74 70 3a   29/8000..a=fmtp:
0340  31 38 20 61 6e 6e 65 78 62 3d 6e 6f 0d 0a 61 3d   18 annexb=no..a=
0350  72 74 70 6d 61 70 3a 31 30 31 20 74 65 6c 65 70   rtpmap:101 telep
0360  68 6f 6e 65 2d 65 76 65 6e 74 2f 38 30 30 30 0d   hone-event/8000.
0370  0a 61 3d 66 6d 74 70 3a 31 30 31 20 30 2d 31 35   .a=fmtp:101 0-15
0380  0d 0a 61 3d 70 74 69 6d 65 3a 32 30 0d 0a         ..a=ptime:20..
```

Lo que nos interesa para poder trabajar son las direcciones IP, sus Flags, puertos UDP y payload:

```
Src: 10.15.24.244 (10.15.24.244)

Dst: 10.15.4.16 (10.15.4.16)

   Flags: 0x02 (Don't Fragment)
      0... .... = Reserved bit: Not set
      .1.. .... = Don't fragment: Set
      ..0. .... = More fragments: Not set
User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
   Source port: 5060 (5060)
```

Destination port: 5060 (5060)

Del “Payload”, lo que necesitamos para poder generar tráfico con “**nemesis**” es la parte de la derecha de la presentación formato “.cap” como se presenta en la imagen que sigue:

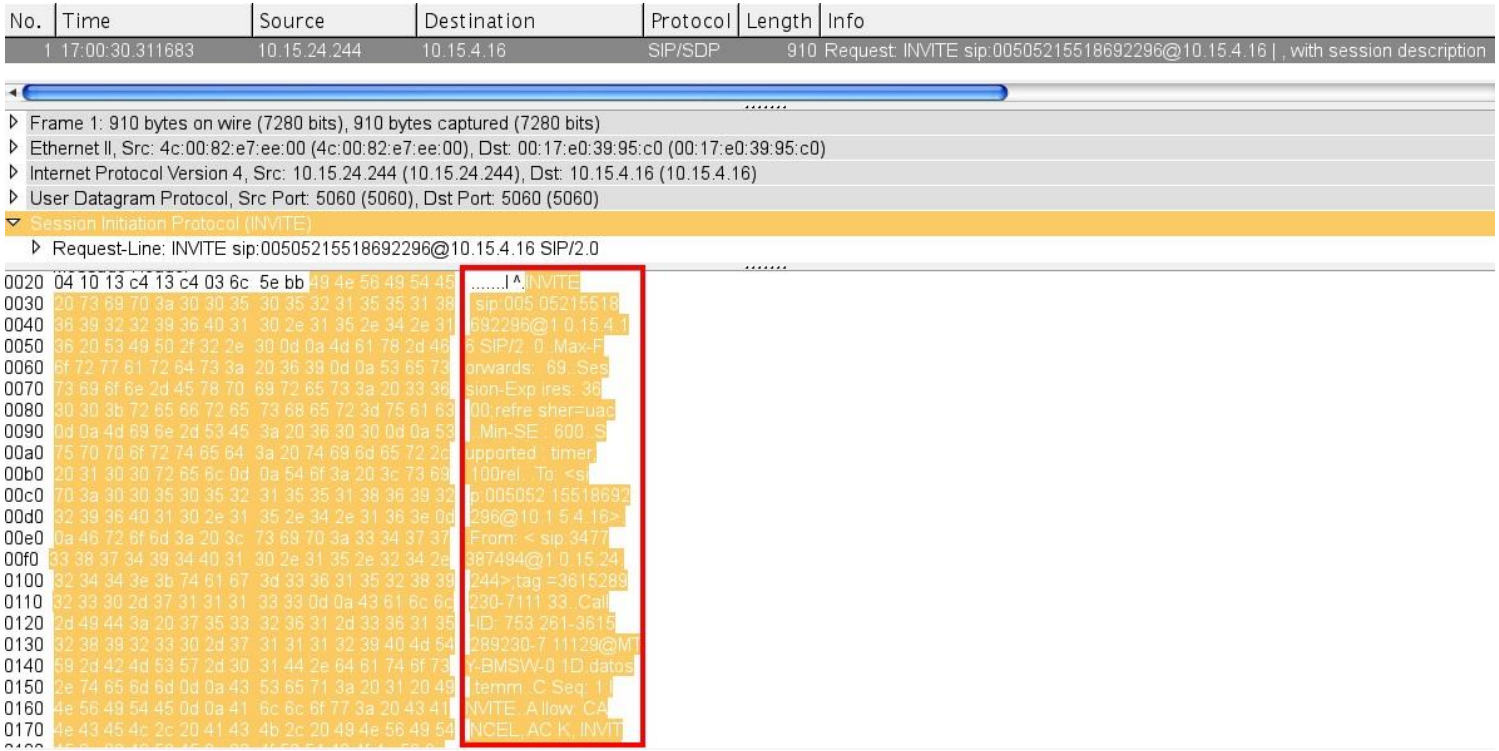


Imagen 8. (Wireshark campo payload)

Lo cual al tener la trama completa en formato de texto, deberemos filtrar sólo ese contenido, el cual nos queda como se presenta a continuación:

INVITE sip:00505215518692296@10.15.4.16 SIP/2.0..Max-Forwards: 69..Session-Expires: 3600;refresher=uac..Min-SE: 600..Supported: timer, 100rel..To: <sip:00505215518692296@10.15.4.16>..From:

<sip:3477387494@10.15.24.244>;tag=3615289230-711133..Call-ID: 753261-3615289230-711129@MTY-BMSW-01D.datos.temm..CSeq: 1 INVITE..Allow: CANCEL, ACK, INVITE, BYE, OPTIONS,REGISTER, NOTIFY, INFO, REFER, SUBSCRIBE, PRACK, UPDATE, MESSAGE, PUBLISH..Via: SIP/2.0/UDP 10.15.24.244:5060;branch=z9hG4bK9b39c13355d40025c8ae6fb918f289b8..Contact: <sip:3477387494@10.15.24.244:5060>..Content-Type: application/sdp..Accept: application/sdp..Content-Length: 227....v=0..o=MTY-BMSW-01D 188 1 IN IP4 10.15.24.244..s=sip call..c=IN IP4 10.15.24.245..t=0 0..m=audio 23766 RTP/AVP 18 101..a=rtpmap:18 G729/8000..a=fmtp: 18 annexb=no..a=rtpmap:101 telephone-event/8000..a=fmtp:101 0-15..a=ptime:20..

Este archivo de texto, lo podemos guardar con cualquier nombre, en nuestro caso lo llamaremos “payload_03.txt” y nos servirá para poder comenzar a trabajar con el software “**nemesis**” en la generación de tráfico.

Para poder generar una trama exactamente igual (desde el nivel 3, considerando su control de errores) el comando que debemos ejecutar es:

```
sh-3.2# nemesis udp -v -d en0 -D
10.15.4.16 -y 5060 -FD -S
10.15.24.144 -x 5060 -P
payload_03.txt
```

A continuación se presenta la captura con Wireshark de esta trama, en la cual podemos ver que es exactamente igual a la capturada en el tráfico real:

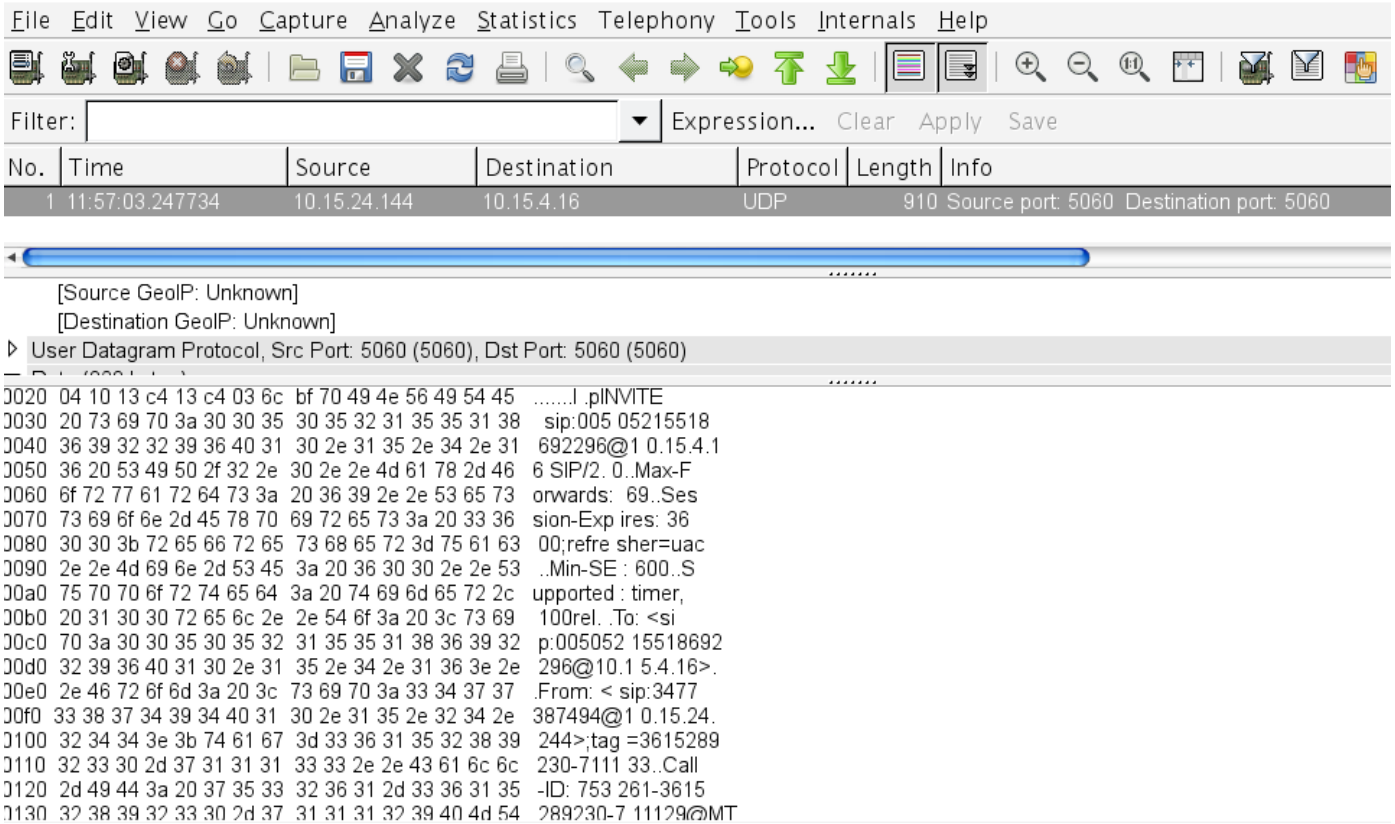


Imagen 9. (Captura de trama generada con la herramienta “nemesis”)

No.	Time	Source	Destination	Protocol	Length	Info
1	17:00:30.311683	10.15.24.244	10.15.4.16	SIP/SDP	910	Request: INVITE sip:00505215518692296@10.1

Frame 1: 910 bytes on wire (7280 bits), 910 bytes captured (7280 bits)
Ethernet II, Src: 4c:00:82:e7:ee:00 (4c:00:82:e7:ee:00), Dst: 00:17:e0:39:95:c0 (00:17:e0:39:95:c0)
Internet Protocol Version 4, Src: 10.15.24.244 (10.15.24.244), Dst: 10.15.4.16 (10.15.4.16)
User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)

```
0020  04 10 13 c4 13 c4 03 6c  5e bb 49 4e 56 49 54 45   ......l^INVITE
0030  20 73 69 70 3a 30 30 35  30 35 32 31 35 35 31 38   sip:005 05215518
0040  36 39 32 32 39 36 40 31  30 2e 31 35 2e 34 2e 31   692296@1 0.15.4.1
0050  36 20 53 49 50 2f 32 2e  30 0d 0a 4d 61 78 2d 46   6 SIP/2. 0..Max-F
0060  6f 72 77 61 72 64 73 3a  20 36 39 0d 0a 53 65 73   orwards:  69..Ses
0070  73 69 6f 6e 2d 45 78 70  69 72 65 73 3a 20 33 36   sion-Exp ires: 36
0080  30 30 3b 72 65 66 72 65  73 68 65 72 3d 75 61 63   00;refre sher=uac
0090  0d 0a 4d 69 6e 2d 53 45  3a 20 36 30 30 0d 0a 53   ..Min-SE : 600..S
00a0  75 70 70 6f 72 74 65 64  3a 20 74 69 6d 65 72 2c   upported : timer,
00b0  20 31 30 30 72 65 6c 0d  0a 54 6f 3a 20 3c 73 69   100rel. .To: <si
00c0  70 3a 30 30 35 30 35 32  31 35 35 31 38 36 39 32   p:005052 15518692
00d0  32 39 36 40 31 30 2e 31  35 2e 34 2e 31 36 3e 0d   296@10.1 5.4.16>.
00e0  0a 46 72 6f 6d 3a 20 3c  73 69 70 3a 33 34 37 37   .From: < sip:3477
00f0  33 38 37 34 39 34 40 31  30 2e 31 35 2e 32 34 2e   387494@1 0.15.24.
0100  32 34 34 3e 3b 74 61 67  3d 33 36 31 35 32 38 39   244>;tag =3615289
0110  32 33 30 2d 37 31 31 31  33 33 0d 0a 43 61 6c 6c   230-7111 33..Call
0120  2d 49 44 3a 20 37 35 33  32 36 31 2d 33 36 31 35   -ID: 753 261-3615
0130  32 38 39 32 33 30 2d 37  31 31 31 32 39 40 4d 54   289230-7 11129@MT
```

Imagen 10. (Captura de tráfico real)

A partir de ahora, todo el trabajo que se puede realizar es por medio de este “Payload” con el cual cambiando cualquiera de los parámetros del encabezado SIP, podemos generar el tipo de trama que deseemos.

Existen otro tipo de herramientas para esta actividad que figuran a continuación, pero se presentó en primer término “nemesis” pues por tratarse de línea de comandos, ofrece mucha mayor potencia en la generación de tráfico.

Existen muchas más, pero a continuación sólo se presentan solo algunas de ellas:

Una de ellas, específica para trafico SIP es "**SipScan**".

Imagen 11. (SipScan)

La otra que puede emplearse también es "**Packet Builder**".

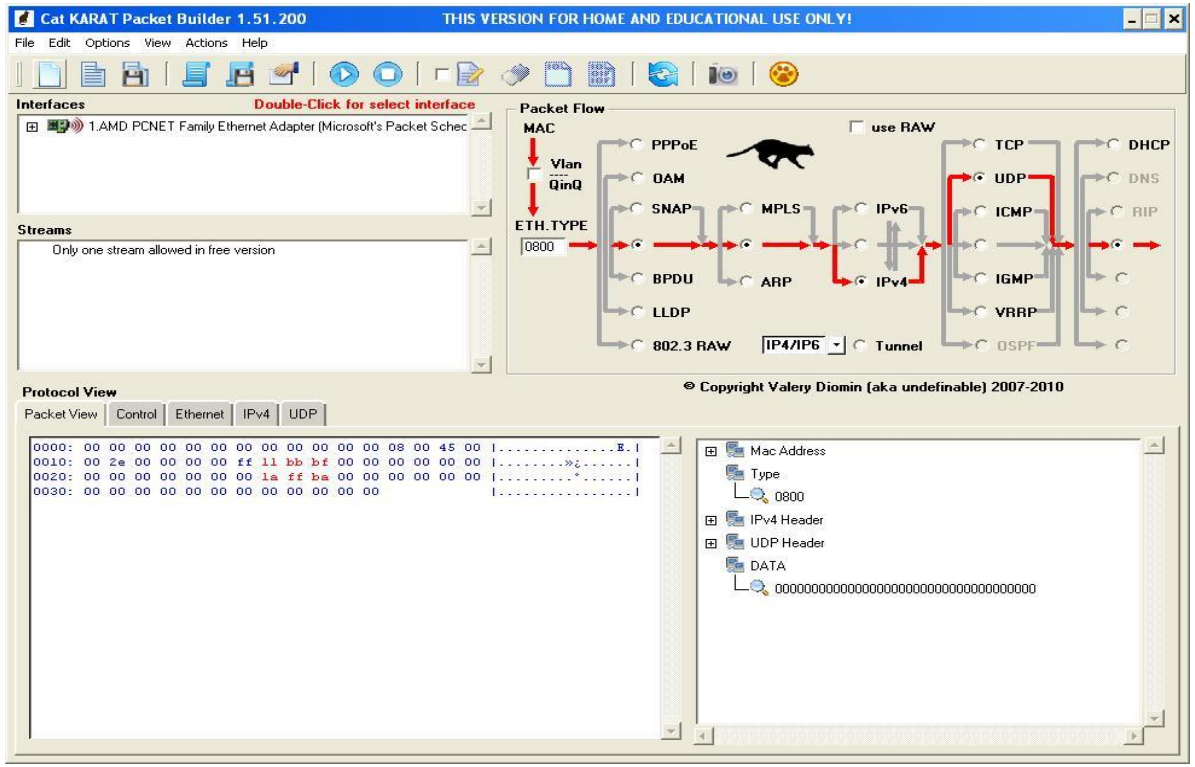


Imagen 12. (Packet Builder)

Otra que también recomendamos es “**SigPloit”.**

```
root@kali-2018:/var/tmp/sigploit/SigPloit-master# python sigploit.py

 _IMSI                  XXXXXX
0x1  GT   E       XXXX  X     X  GT       SGSN    E     --USIM--
PC        n      X    X X     X  PC      X    X   n        x0
 _IMEI    C      X      XXXXXX   x7      X    X   C        x2
     CI   r      X  gtp X        x6      X    X   r        x3
Kc  421   P      X    X X        x8      X    X   P        x8
 _HLR_    T       XXXX  X        Fraud    gGsN    T        x6

[-][-]          Signaling Exploitation Framework         [-][-]
[-][-]                  Version:BETA 1.1                 [-][-]
[-][-]          Author:Loay AbdelRazek(@sigploit)        [-][-]


Contributors:
        Rosalia D'Alessandro
        Ilario Dal Grande




    Module                      Description
   --------                  --------------------
  0) SS7                 2G/3G Voice and SMS attacks
  1) GTP                 3G/4G Data attacks
  2) Diameter            4G Data attacks
  3) SIP                 4G IMS attacks

   or quit to exit SigPloit

sig>
```

Imagen 13. (SigPloit)

Como lenguaje para crear todo tipo de protocolo y concatenarlos nivel a nivel, también recomendamos el empleo de "**Scapy**" escrito en Python.

Imagen 14. (Scapy)

SIPp

http://sipp.sourceforge.net

Es una herramienta open source para testear y generar tráfico SIP, permite generar parámetros INVITE; BYE; etc con muchas sencillez. Un detalle importante es que tiene soporte para IPv6 y SCTP que son protocolos difíciles de implementar de forma más manual.

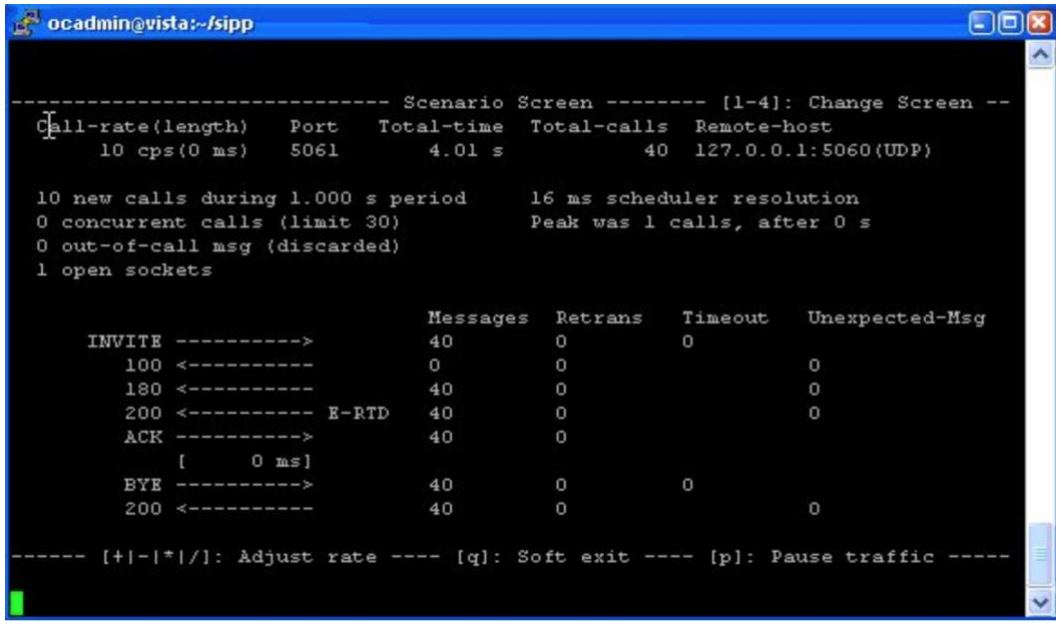


Imagen 15.

SIPVicious

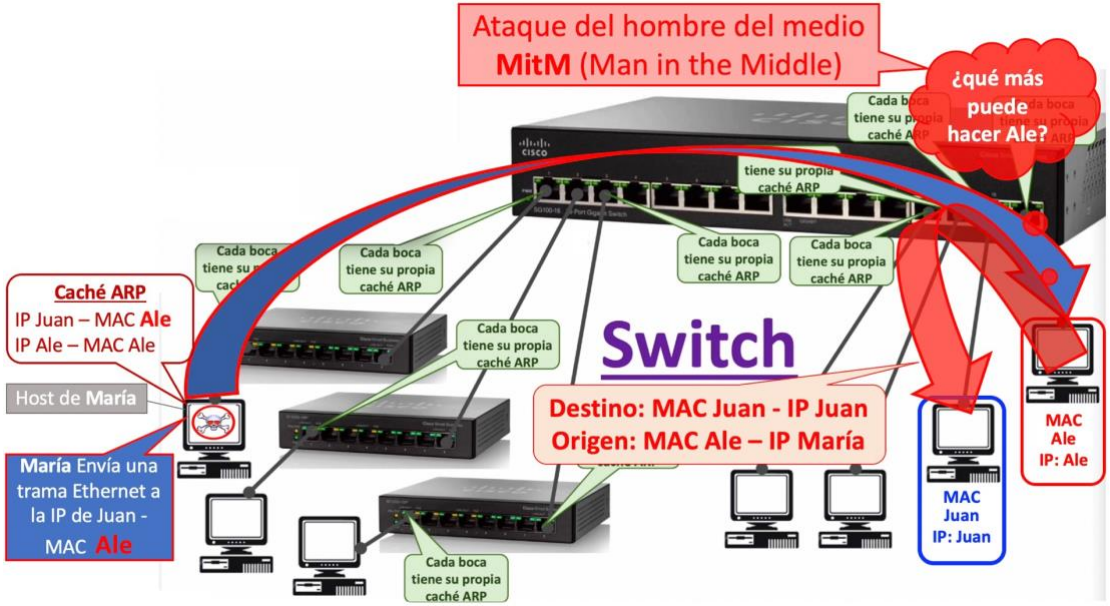
https://sipvicious.com/

Esta es una vieja suite de herramientas que tiene una versión gratuita y otra de pago que consta de lo siguiente:

- svmap
- svwar
- svcrack
- svreport
- svcrash

Puede descargarse desde github en: https://github.com/EnableSecurity/sipvicious

Entendamos de forma práctica de qué se trata todo esto.



El primer paso para la interceptación de una llamada de voz es el "envenenamiento de la caché ARP".

Con ello logramos que a nivel enlace, la dirección MAC que un host tiene asociada con una dirección IP sea falsa en su caché ARP.

Cuando ese host envíe información a esa dirección IP, lo hará colocando a nivel 2 (enlace) la dirección MAC FALSA.

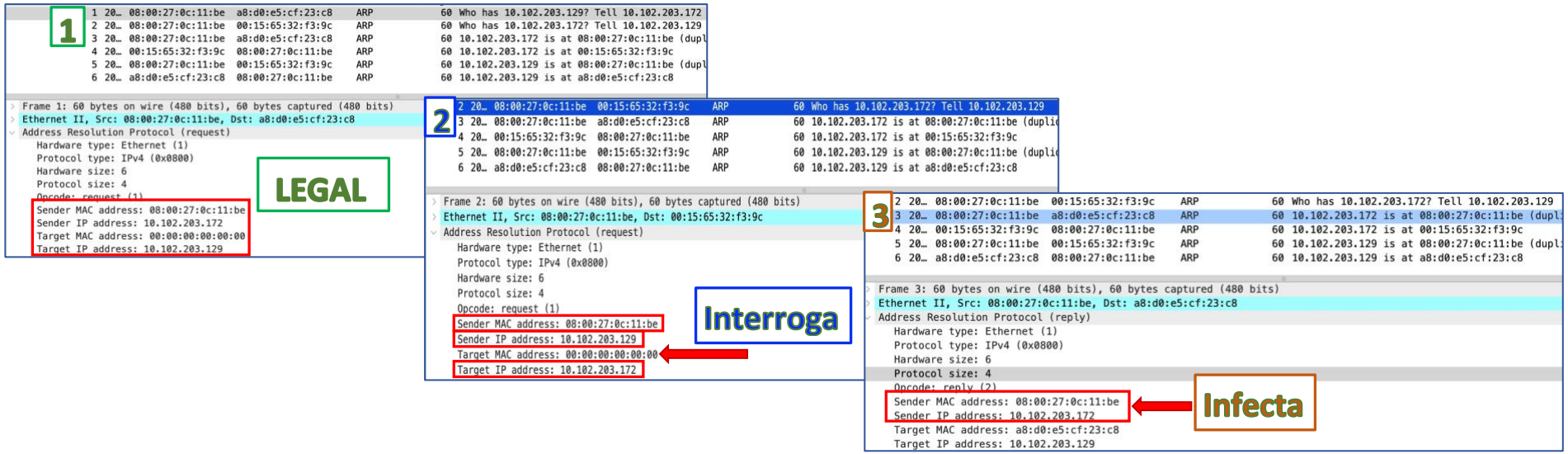
En concreto, todas las direcciones MAC descartarán esa información (incluida la verdadera) y solo procesará esa trama Ethernet la MAC falsa, que por supuesto es la del intruso.

Este intruso reenviará la información a la IP destino, pero ahora sí colocando su MAC verdadera, ante lo cual la IP destino cuando responda, lo hará colocando a nivel enlace la MAC desde la que recibió esa información, es decir la FALSA. El intruso cuando reciba esa información, le colocará la dirección MAC verdadera y la reenviará al origen verdadero, realizando un "Ataque del hombre del medio" (**MitM**). Si la información es tráfico SIP y/o RTP pasará por él toda la llamada telefónica, y si está en texto plano, podrá escucharla sin ningún tipo de problema.

Todo esto, está desarrollado con máximo detalle en los capítulos 17, 18 y 19 del libro "**Aprendiendo Ciberseguridad paso a paso (Volumen 1)**" que podéis descargar gratuitamente desde la Web: www.darFe.es

Igualmente como cierre de esta charla vamos a analizar un caso real de envenenamiento de caché ARP y inteceptación de VoIP en un entorno LAN.

Vamos a estudiar primero el envenenamiento de caché ARP, por medio de la captura de tráfico **secuencia-envenenamiento_ARP.cap**
Que se puede descargar de nuestra Web: www.darfe.es → "Descargas" → "Capturas de tráfico" → "Capturas de tráfico 2"



MAC: a8:d0:e5:cf:23:c8
IP: 10.102.203.194

MAC: 08:00:27:oc:11:be
IP: 10.102.203.129

MAC: 00:15:65:32:f2:9c
IP: 10.102.203.172

Vamos a estudiar ahora la captura de tráfico: **VoIP_02_SIP-SDP-RTP_solo.cap**
Que se puede descargar de nuestra Web: www.darfe.es → "Descargas" → "Capturas de tráfico" → "Capturas de tráfico 2"

Madrid, junio de 2025.