eman ta zabal zazu
Universidad del País Vasco
Euskal Herriko Unibertsitatea
BILBOKO INGENIARITZA ESKOLA
ESCUELA DE INGENIERÍA DE BILBAO

GRADO EN INGENIERÍA EN TECNOLOGÍA INDUSTRIAL

TRABAJO FIN DE GRADO

IMPLEMENTACIÓN DE UNA ARQUITECTURA DE COMUNICACIONES SEGURAS PARA SISTEMAS EMBEBIDOS INDUSTRIALES

Alumno: Martínez Gómez, Iñigo

Director: Lázaro Arrotegui, Jesús

Curso: 2.018 – 2.019

Fecha: Bilbao, 8 de julio de 2.019

Universidad del País Vasco
Euskal Herriko Unibertsitatea

BILBOKO INGENIARITZA ESKOLA
ESCUELA DE INGENIERÍA DE BILBAO

Índice general

Índice de figuras

Índice de cuadros

1. Introducción

Título: Implementación De Una Arquitectura De Comunicaciones Seguras Para Sistemas Embebidos Industriales.

Resumen: El objetivo de este proyecto es probar distintas configuraciones de comunicación entre ordenadores. El proyecto está enfocado al análisis de la norma de seguridad IEEE 802.1AE y su aplicación en el sistema operativo Linux. Esta norma permite realizar una comunicación segura entre dos o más ordenadores. Asimismo, en este proyecto se estudian otras tecnologías relacionadas con la aplicación de ésta.

Palabras clave: Seguridad informática, comunicaciones, criptografía.

Izenburua: Komunikazio Seguruen Arkitekturaren Implementazioa Sistema Embebitu Industrialetarako.

Laburpena: Proiektu honen helburua, ordenagailuen arteko komunikazio ezarpen ezberdinak frogatzea da. I.E.E.E. 802.1AE segurtasun arauaren analisisan eta Linux sistema eragilerako erabileran kokatzen da proiektu hau. Beste teknologietako erabilera ikertuko da.

Hitz gakoak: Seguritate informatikoa, komunikazioa, kriptografia.

Título: Secure Comunication Architecture Implementation For Embedded Industrial Systems.

Abstract: The purpose of this proyect is to test diferent computer comunications betwen computers. The project is focused on the analysis of the security standard I.E.E.E. 802.1AE and its aplication on Linux operating system. This standard allows a secure comunication betwen computers. Other technologies related with this one will be studied as well.

Keywords: Computer security, comunications, cryptography.

Cuadro 1.1.: Tabla de acrónimos

Acrónimo	**Significado**
APERT	Applied Electronics Research Team
MV	Máquina Virtual
SO	Sistema Operativo
IP	Internet Protocol
NIST	National Institute For Standard and Technology
AES	Advanced Encription Standard
IEEE	Institute of Electrical and Electronics Engineers

2. Memoria

2.1. Contexto

Establecer una comunicación entre dos partes que no pueda ser interpretada por un tercero ha sido una ambición constante a lo largo del tiempo. Los sistemas de cifrado modernos recurren a algoritmos matemáticos implementados sobre plataformas digitales frente a los sistemas electromecánicos empleados durante la segunda mitad del siglo XX y los métodos manuales que, a su vez, precedieron a estos.

La norma empleada para cifrar las comunicaciones de este proyecto se denomina AES. Fue publicada el 26 de noviembre de 2001 por el instituto NIST tras ser aprobada por el Ministerio De Comercio estadounidense. Dicha norma emplea el Algoritmo De Rijndael, particularizado para paquetes de 128 bits y los protege empleando claves de 128, 192 o 256 bits. (Notar que en este proyecto se emplean claves de longitud 256 bits.)

El presente proyecto se sitúa dentro del área de la telemática y desarrolla temas relacionados con sistemas operativos y electrónica digital.

2.2. Objetivos y alcance del trabajo

El objetivo que marca el desarrollo de este proyecto es conseguir una comunicación segura entre dos ordenadores. Para conseguirlo se deben cumplir los siguientes hitos: (Ver Figura 2.1)

- **Creación de una tarjeta de red virtual MACSec:** Que es aquella a través de la cual circulan las comunicaciones cifradas.
- **Creación de una subred en la que se den las comunicaciones:** Mediante el gestor de máquinas virtuales, lo que requiere familiarizarse con su funcionamiento.

Asimismo, se cumplen otros objetivos secundarios que pueden resultar de igual interés.

- **Familiarizarse con los gestores de máquinas virtuales:** Estos programas permiten administrar diversos sistemas operativos dentro de un mismo ordenador huésped.

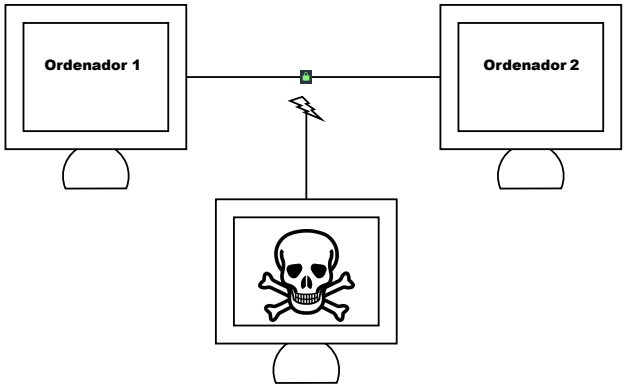


Figura 2.1.: Infografía del propósito de este TFG

- **Conocer el manejo del sistema operativo LNUX, distribución Debian:** Frente a otras opciones, se ha optado por este sistema para la realización de las comunicaciones, lo que requerirá familiarizarse con su utilización.

- **Redactar textos mediante LaTeX:** LaTeX es un sistema de redacción de documentos técnicos y científicos. Dicho sistema permite redactar sin ocuparse del formato del texto.

2.3. Beneficios que aporta el trabajo

Este proyecto consigue establecer una comunicación segura entre dos partes. Asimismo, prueba que dicha comunicación no es accesible por una tercera parte que tenga acceso a la red que une a las dos primeras. La tecnología empleada para ello es de interés actual.

El conocimiento adquirido en este proyecto tiene aplicaciones sobre las necesidades de comunicación actuales en la industria. No solo es necesario una red de comunicaciones que permita transmitir datos de una manera fiable, si no que, dicha transmisión de datos debe garantizar la seguridad de la conexión. El proyecto se desarrolla entorno a la norma de comunicación MacSec, realizando un ejemplo de aplicación en el sistema operativo Debian. Con esta demostración, se pretende dar a conocer dicha norma y mostrar su eficacia.

2.4. Descripción de requerimientos y/o Análisis del estado del arte

Existen diversas normas que permiten establecer un vínculo cifrado. A continuación, se mencionan dos de ellas:

- **IpSec:** Es un protocolo de comunicación segura que encripta los paquetes de información enviados sobre la red IPv4.[...] Este sistema de protección incluye mecanismos para establecer una mutua autentificación entre los agentes al principio de una sesión y el negociado de claves criptográficas para ser usadas durante la sesión.

  Proporciona seguridad a nivel *Layer 3* (Ver Figura 2.2). *IPsec está implementado por un conjunto de protocolos criptográficos para asegurar el flujo de paquetes, garantizar la autenticación mutua y establecer parámetros criptográficos.* [2]

- **Media Access Control Security (MACsec):** Es una norma de IEEE que proporciona una comunicación segura para todo el tráfico en vínculos de Internet. Permite seguridad punto a punto en nodos conectados directamente y es capaz de identificar y prevenir la mayoría de amenazas, por ejemplo, un ataque *man-in-the-middle* [10]. (Ver Figura 2.3)

  Proporciona seguridad a nivel *Layer 2. MACsec es un mecanismo que provee comunicaciones seguras, y dado que opera en la capa de enlace de datos (L2 del modelo OSI), provee confidencialidad e integridad, evitando que la información pueda ser monitoreada o alterada. MACsec provee cifrado simétrico entre los endpoint y los switches (downlink) o incluso en las interconexiones entre los distintos switches de una red local (uplink). [5]*

2.5. Selección/Descripción de la solución propuesta

A fin de simplificar las operaciones que requiere este proyecto, se ha optado por recurrir a un gestor de máquinas virtuales. Esto permite ejecutar varios sistemas operativos en un mismo ordenador a través de la virtualización del hardware.

El gestor por el que se ha optado es *VirtualBox* dada su gratuidad (el programa puede descargarse con fines educativos); su facilidad de uso y el hecho de que permite distintos tipos de conexiones de red entre varias máquinas virtuales (Ver Apartado Configuración de Red). Asimismo, existen otras alternativas a este *software*, entre otras, *VMWare*. A diferencia del primero, la configuración de redes en este resulta más laboriosa, ya que no dispone de un asistente tan intuitivo como *VirtualBox*.

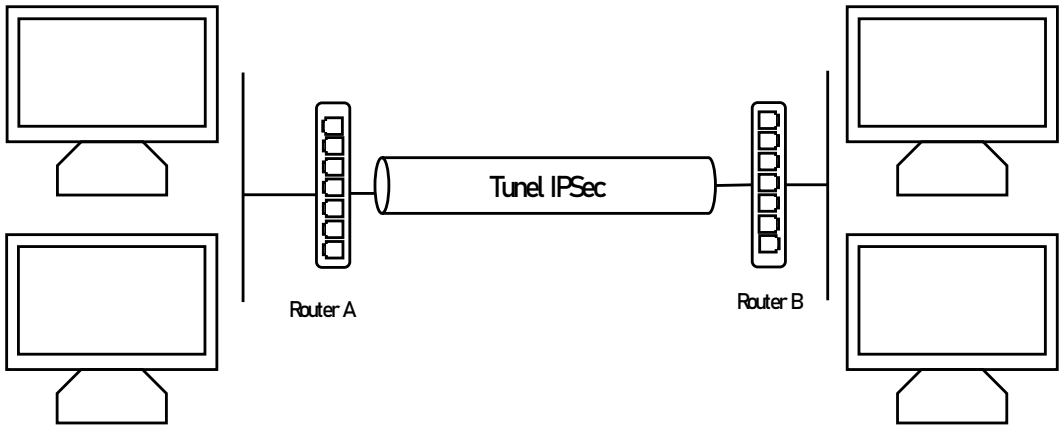


Figura 2.2.: Funcionamiento Protocolo IPSec

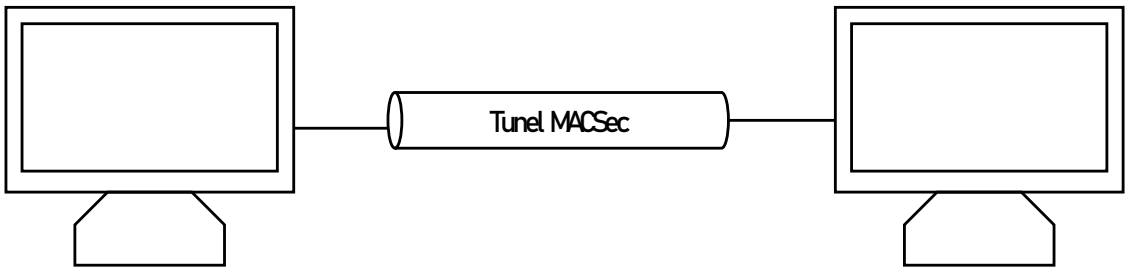


Figura 2.3.: Funcionamiento Protocolo MACSec

El sistema operativo sobre el que se realizaran las pruebas es Linux, en la distribución *Debian*. Dado que posee una versión para ordenadores de escritorio y otra para dispositivos *RaspberryPI* (Ver Apéndice A) es idónea para las pruebas que se desean realizar. Puede optarse por otras distribuciones de Linux para este fin, por ejemplo, Ubuntu. No obstante, no suele ser común entre el resto de distros encontrar compilaciones para el dispositivo RaspberryPI, lo que puede complicar futuros pasos en el proyecto.

El PC huésped en el que se realizan las pruebas es un computador de escritorio con un procesador *Intel Core i5* con soporte nativo para la virtualización de hardware. Dicho dispositivo cuenta con potencia suficiente para ejecutar varias máquinas virtuales simultaneamente.

3. Metodología seguida en el desarrollo del trabajo

3.1. Descripción de tareas, fases, equipos o procedimientos

El proyecto se desarrolla sobre dos sistemas operativos distintos: *Linux*, que es el sistema operativo que realiza las comunicaciones, y *Windows* 7, que es el sistema operativo que hospeda todo el *software* de virtualización. Asimismo, se requieren distintos programas informáticos para realizar y estudiar las comunicaciones en el desarrollo del proyecto. A saber:

- ***Oracle VM VirtualBox***: *VirtualBox* es una potente herramienta de virtualización para procesadores AMD64/Intel64 enfocada para el uso empresarial y doméstico. Se puede obtener de manera gratuita como *Open Source Software* bajo la los términos de la licencia *GNU General Public License*. Será el programa encargado de hospedar las máquinas virtuales.
- ***WhireShark:*** *Wireshark* es un analizador de paquetes de red. Este programa trata de capturar los paquetes de red y mostrar su información de la manera más detallada posible. Se puede considerar un programa de estos como una herramienta para analizar qué ocurre dentro de un cable de red.
- **Terminal:** El Terminal de Linux es una herramienta propia del núcleo del sistema operativo. Ofrece un camino para mostrar información recibida del núcleo e introducir entradas de texto del usuario.

3.1.1. Instalación de Debian en VirtualBox

Las instalación del sistema operativo comienza descargando una imagen del disco de instalación[1]. De entre todas las posibles opciones de descarga, en este proyecto, se opta por la versión para arquitecturas i386. Esta decisión, se toma basándose en que la versión de la distribución escogida debe ser compatible con la familia del procesador del ordenador que hospeda las máquinas virtuales, en este caso i386. Dicho archivo tiene la extensión *.iso*.

[1]La imagen puede descargarse de la página web *www.debian.org*.

Una vez descargada esta imagen, se puede comenzar la instalación del sistema operativo en una máquina virtual en *VirtualBox*. Para ello, partimos de la ventana primera del gestor de máquinas virtuales. [Figura 3.1]

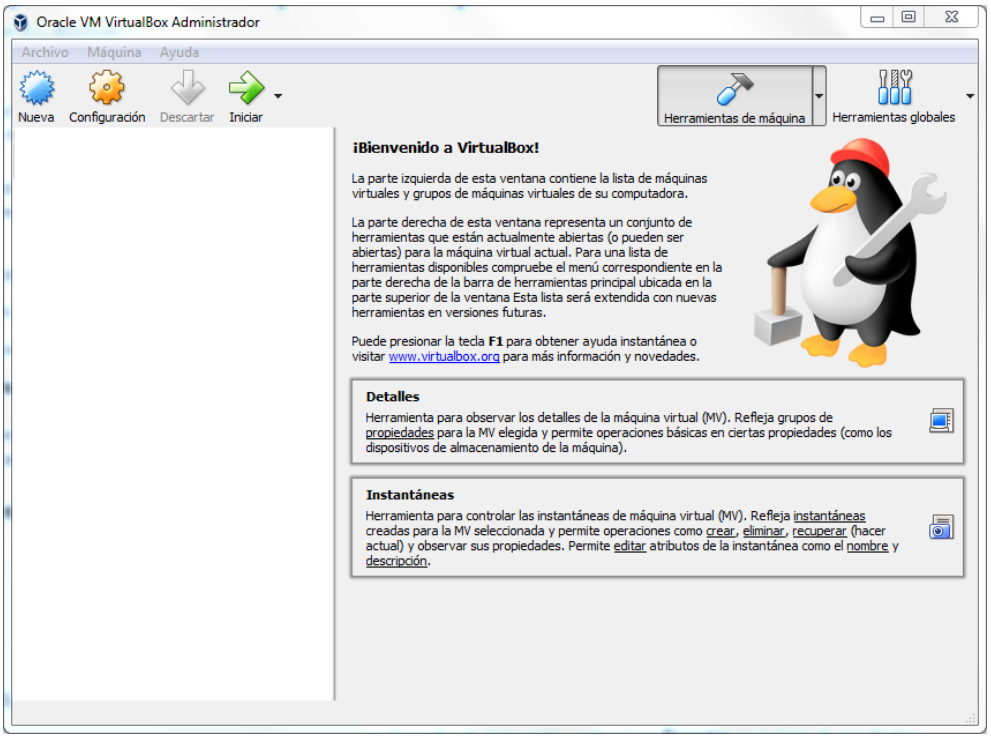


Figura 3.1.: Ventana de trabajo de *VirtualBox*

Una vez en esta venta de trabajo, la opción **Nueva** permite crear una nueva máquina virtual. A continuación se enumeran las opciones indicadas para la creación de la máquina virtual: [Figura 3.2]

- **Nombre:** Debian (Posteriormente se enumerarán las máquinas virtuales)
- **Tipo:** Linux
- **Versión:** Debian (32-bit)
- **Tamaño de memoria:** 2048 MB
- **Disco duro:** Crear disco duro ahora. En la ventana que aparece a continuación, se eligen las opciones por defecto que crearán un archivo con extensión *.vdi* que contendrá la imagen del disco duro de nuestro sistema

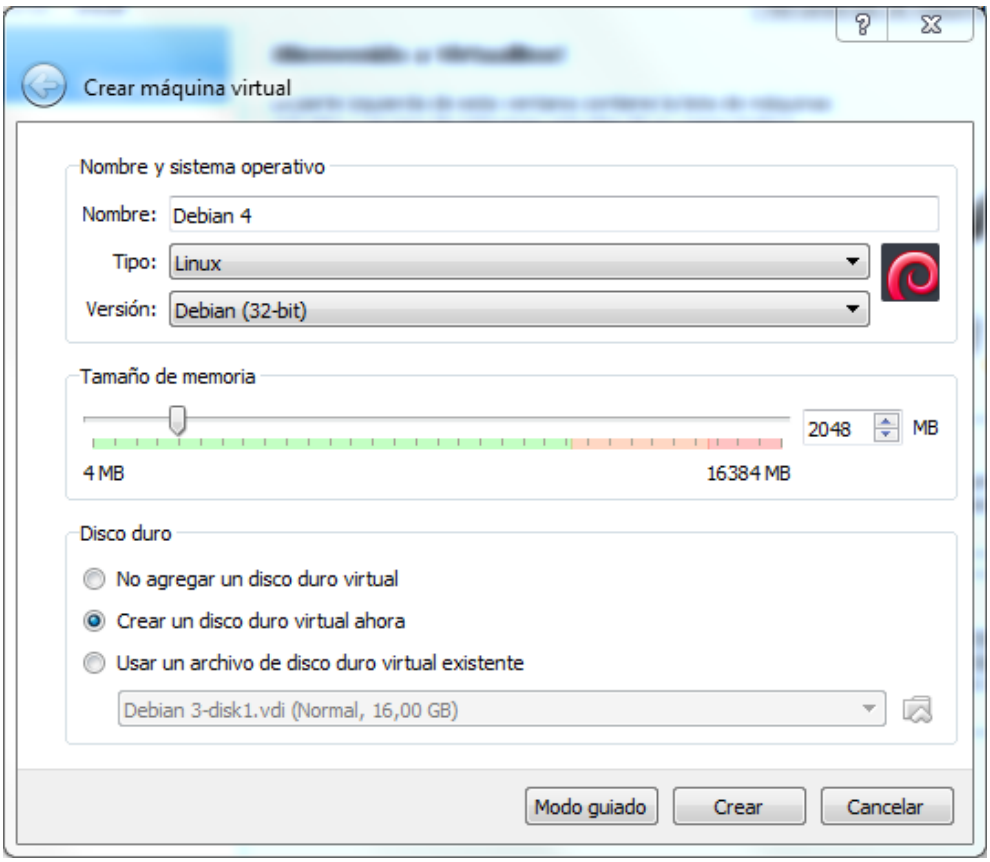


Figura 3.2.: Ventana de creación de máquina virtual

Los pasos mencionados hasta ahora crean una máquina virtual vacía sobre la que debe instalarse *Debian*. Para ello, se selecciona la máquina Debian (que ahora figura en la venta principal de *VirtualBox*) y se hace clic en la opción **Configuración**. En la ventana que surge, dentro de la sección *Almacenamiento*, se indica la unidad virtual que contiene el disco de instalación [Figura 3.3].

Se procede con los pasos de instalación del sistema operativo *Debian* y se concluye con una imagen de disco duro virtual que contiene el S.O. *Debian* [Figura 3.4]. Notar que en el proceso de instalación, se requiere una contraseña para la cuenta de superusuario, que es la que más *privilegios* otorga dentro del sistema operativo.

Por último, se procede a replicar esta máquina virtual dos veces en *VirtualBox*. Para ello, se hace clic derecho del ratón sobre la máquina virtual y se selecciona la opción *clonar*. Los parámetros requeridos en el asistente *Clonar Máquina Virtual* son los siguientes:

- **Nuevo nombre de máquina:** Las máquinas virtuales clonadas se denominan *Debian 2* y *Debian 3*. En esta misma ventana se marca la opción **Reinicializar la dirección MAC de todas las tarjetas de red**.

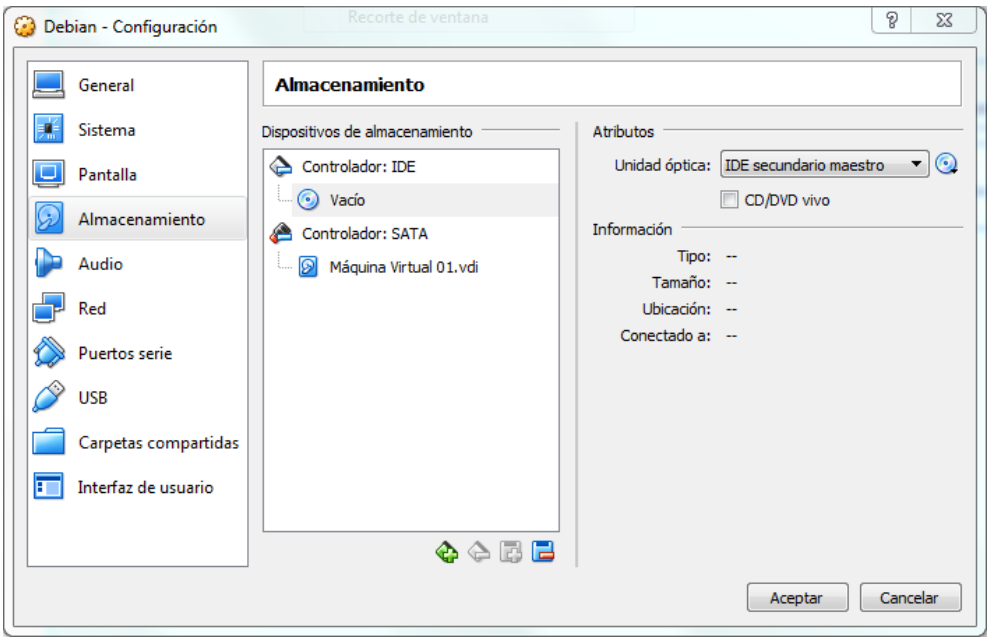


Figura 3.3.: Ventana en la que se indica la imagen para la unidad de disco virtual

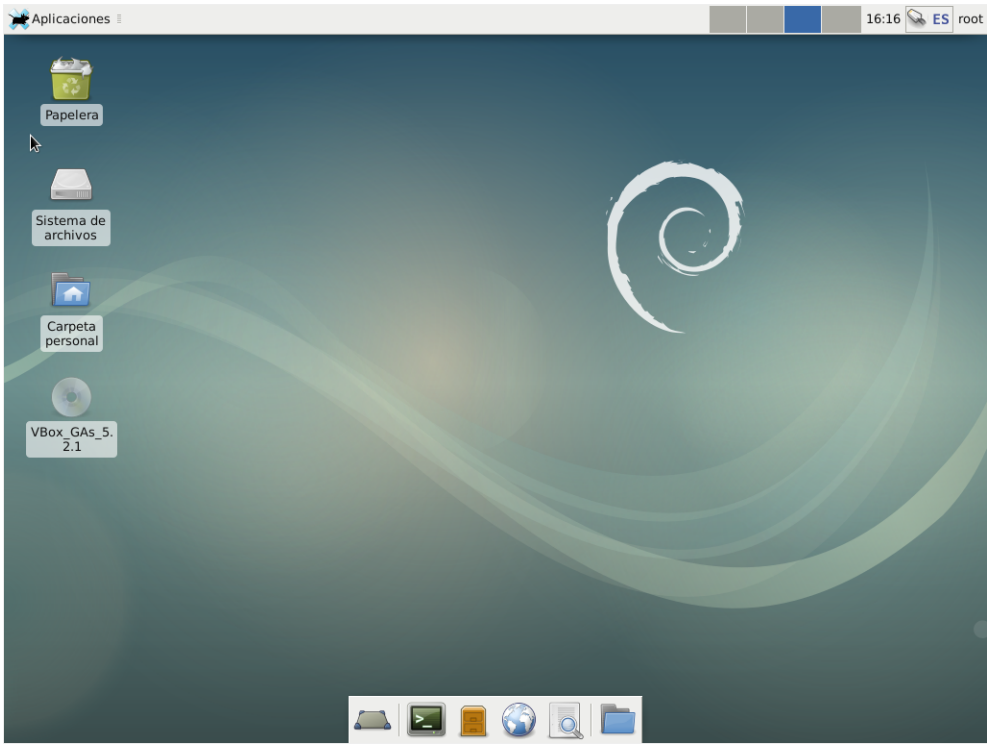


Figura 3.4.: Escritorio de *Debian* una vez concluida la instalación del sistema

- **Tipo de clonación:** En esta ventana se indica la opción *Clonación completa*. Esta acción separa los archivos de una máquina virtual respecto de las otras.

Cuadro 3.1.: Tipos de conexión que permite *VirtualBox* [8]

	VM ↔ Host	VM1 ↔ VM2	VM → Internet	VM ← Internet
Host-only	+	+	-	-
Internal	-	+	-	-
Bridged	+	+	+	+
NAT	-	-	+	Port forwarding
NAT Network	-	+	+	Port forwarding

Con este paso, se concluye con la creación de las máquinas virtuales.

3.1.2. Configuración de los parámetros de red en VirtualBox

El gestor de maquinas virtuales permite varios tipos de conexión de red para las máquinas virtuales. A la hora de escoger el tipo de conexión, se tiene en cuenta los requisitos de la red en la que trabaja el ordenador. Puesto que el actual proyecto se desarrolla en un ordenador conectado a la red de la universidad, algunas de las conexiones que indica la tabla 3.1 no funcionan correctamente.

De entre todas las posibles, se escoge la conexión *Host-only*, o en español, sólo-anfitrión. Este tipo de conexión, se indica dentro de la ventana de **configuración** de la MV. En la sección **red**, se elige este tipo de conexión.

3.1.3. PING entre dos máquinas virtuales

"Ping es una utilidad diagnóstica en redes de computadoras que comprueba el estado de la comunicación del host local con uno o varios equipos remotos de una red IP por medio del envío de paquetes ICMP de solicitud (ICMP Echo Request) y de respuesta (ICMP Echo Reply). Mediante esta utilidad puede diagnosticarse el estado, velocidad y calidad de una red determinada." [6]

Mediante esta utilidad, se comienza realizando una conexión no segura entre dos máquinas virtuales. Para ello, se inician dos de las tres máquinas virtuales y se introducen las credenciales hasta llegar al escritorio de trabajo. Una vez en él, se clica en él icono **Emulador de terminal**.

El siguiente paso requiere conocer la dirección IP de cada máquina virtual. Para ello, introducimos el comando **ifconfig**. Este comando muestra las tarjetas de red de las que dispone el sistema. La que resulta de interés en este caso es **enp0s3**.[Figura 3.5]

```
root@MV01:~# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.102  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::a00:27ff:fec4:835b  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:c4:83:5b  txqueuelen 1000  (Ethernet)
        RX packets 759  bytes 59690 (58.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 39  bytes 6093 (5.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 10408  bytes 842880 (823.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 10408  bytes 842880 (823.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figura 3.5.: Tarjetas de red conectadas a la máquina *Debian*. En la captura se puede ver la dirección IP local asignada a dicha tarjeta, así como la máscara de red

Conocida la dirección IP de las dos máquinas virtuales, se procede ahora a hacer PING de la una a la otra. Para ello, se escribe `ping 192.168.5.16` . Una vez hecho esto, la primera máquina virtual envía paquetes que son recibidos por la segunda. La prueba de que esta conexión es correcta es ver en el terminal de *Debian* lo correspondiente a la Figura 3.6.

En el mensaje retornado por la máquina, se puede observar un número asociado a cada mensaje *EcoPing* enviado (icmp_seq=número del páquete), el *time to leave* y la latencia medida en ms.

```
root@MV01:~# ping 192.168.56.102
PING 192.168.56.102 (192.168.56.102): 56 data bytes
64 bytes from 192.168.56.102: icmp_seq=0 ttl=64 time=1,802 ms
64 bytes from 192.168.56.102: icmp_seq=1 ttl=64 time=0,925 ms
64 bytes from 192.168.56.102: icmp_seq=2 ttl=64 time=0,921 ms
64 bytes from 192.168.56.102: icmp_seq=3 ttl=64 time=0,900 ms
64 bytes from 192.168.56.102: icmp_seq=4 ttl=64 time=0,932 ms
64 bytes from 192.168.56.102: icmp_seq=5 ttl=64 time=0,917 ms
64 bytes from 192.168.56.102: icmp_seq=6 ttl=64 time=0,960 ms
^C--- 192.168.56.102 ping statistics ---
7 packets transmitted, 7 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0,900/1,051/1,802/0,307 ms
```

Figura 3.6.: Terminal de *Debian* cuando el PING es correcto

3.1.4. Utilización de MACSec en Debian

"MACsec es una norma perteneciente a la IEEE que proporciona una comunicación segura para todo el tráfico de internet. Garantiza seguridad punto a punto en vínculos de internet mediante nodos conectados directamente y es capaz de identificar y prevenir la mayoría de las amenazas informáticas, incluyendo negación del servicio, intrusión,

man-in-the-middle[...]" [4]

La norma de comunicación segura, viene incluida por defecto en el núcleo de la distribución de *Debian* empleada. Se utiliza de la siguiente manera:

Máquina virtual 1: Se introducen los siguientes comandos:

1. `sudo ifconfig enp0s3 0.0.0.0`: Este comando asigna la dirección IP 0.0.0.0 a la tarjeta de red enp0s3
2. $ `sudo modprobe macsec`: Este comando carga el módulo de MACsec
3. $ `sudo ip link add link enp0s3 macsec0 type macsec`: Este comando carga sobre la tarjeta de red enp0s3 la tarjeta de red virtual macsec0.
4. $ `sudo ip macsec add macsec0 tx sa 0 pn 1 on key 01 1111111111111111 1111111111111111`: Este comando crea la tarjeta de red virtual `macsec0` sobre la tarjeta de red real. Asimismo, se indica la clave criptográfica con la que se envían los mensajes.
5. $ `sudo ip macsec add mascec0 rx address 08:00:27:f2:1d:8c port 1`: En este comando se debe indicar la dirección MAC del receptor de los mensajes.
6. $ `sudo ip macsec add mascec0 rx address 08:00:27:f2:1d:8c port 1 sa 0 pn 100 on key 02 22222222222222222222222222222222`: En este comando se indica la clave criptográfica de los mensajes recibidos.
7. $ `sudo ip link set dev macsec0 up`
8. $ `sudo ifconfig macsec0 1.1.1.1/24`: Este comando asigna la dirección IP 1.1.1.1 y la máscara de subred 255.255.255.0 a la tarjeta macsec0.

Máquina virtual 2: Se introducen los siguientes comandos:

1. $ `sudo modprobe macsec` Este comando carga el módulo de MACsec.
2. $ `sudo ip link add link enp0s3 macsec0 type macsec`: Este comando carga sobre la tarjeta de red enp0s3 la tarjeta de red virtual macsec0.
3. $ `sudo ip macsec add macsec0 tx sa 0 pn 100 on key 02 222222222222222 222222222222222`: Este comando crea la tarjeta de red virtual `macsec0` sobre la tarjeta de red real. A diferencia de la MV 01, esta máquina virtual envía los mensajes con la clave criptográfica 02.
4. $ `sudo ip macsec add mascec0 rx address 08:00:27:f2:1d:8c port 1`: En este comando se debe indicar la dirección MAC del receptor de los mensajes.

5. $ `sudo ip macsec add mascec0 rx address 08:00:27:f2:1d:8c port 1 sa 0 pn 100 on key 01 11111111111111111111111111111111`: En este comando se indica la clave criptográfica de los mensajes recibidos. A diferencia de la MV 01, aquí los mensajes se reciben con la clave criptográfica 01.
6. $ `sudo ip link set dev macsec0 up`
7. $ `sudo ifconfig macsec0 1.1.1.2/24`: Este comando asigna la dirección IP 1.1.1.2 y la máscara de subred 255.255.255.0 a la tarjeta macsec0.

En este punto, a nivel lógico y dentro de cada máquina virtual existen dos tarjetas de red. A saber, enp0s3 y macsec0. Cada una está conectada a una subred distinta, lo que implica que el tráfico que dirijamos de la MV 01 a la MV 02 a través de la dirección IP 1.1.1.2 se realizará a través de la tarjeta de red macsec0 y se encriptará su contenido. Sin embargo, si la dirección IP de destino es la dirección IP de la tarjeta de red enp0s3 de la MV 02[2], el tráfico se dirigirá a través de esta tarjeta y no se protegerá.

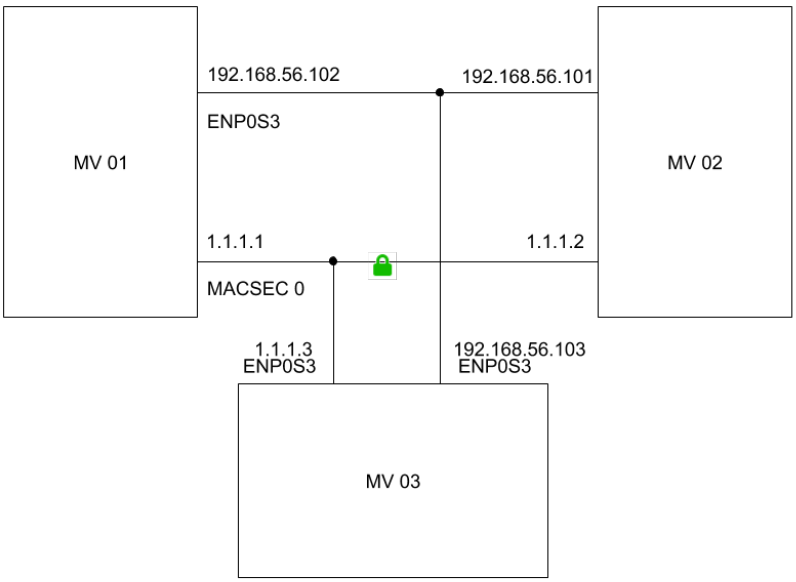


Figura 3.7.: Esquema de las conexiones de red de la máquina virtual

3.1.5. Prueba de seguridad

El siguiente paso de este proyecto, es realizar una prueba que verifique que la comunicación entre las dos máquinas virtuales es segura. Para ello se recurre al programa

[2]Un ejemplo de IP local de esta tarjeta de red es 192.168.56.102

informático *Wireshark*.

"[...] Wireshark permite ver lo que ocurre en una red a nivel microscópico y es, de facto, norma entre empresas comerciales y no lucrativas, agencias e instituciones educativas. El desarrollo de Whireshark se sustenta en la contribución de expertos en redes de todo el mundo, siendo la continuación del proyecto empezado por Geral Combs en 1998." [1]

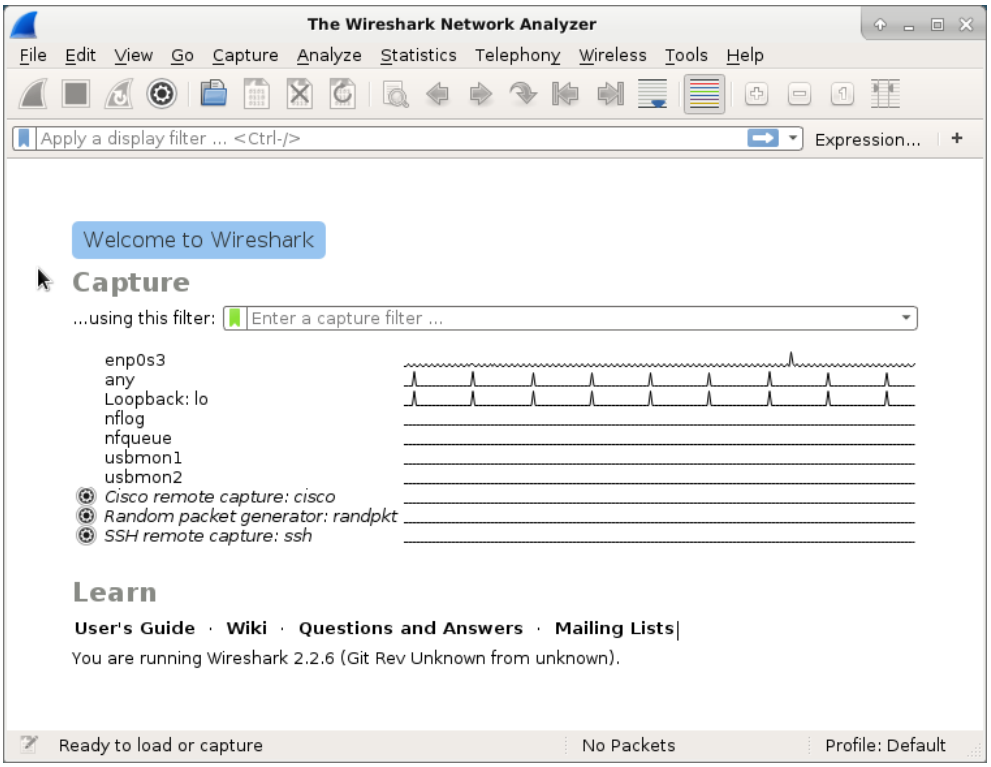


Figura 3.8.: Entorno de trabajo de *Wireshark*

Habiendo realizado la configuración indicada, se procede a probar los dos tipos de conexiones, segura y no segura entre máquinas virtuales. Se comienza iniciando el programa *Wireshark* en la tercera máquina virtual (MV 03) y se continua con los pasos que se describen a continuación.[Figura 3.8]

- **Conexión no segura:** Esta prueba es sencilla de realizar. Por defecto las tarjetas de red se enp0s3 de las tres máquinas virtuales se encuentran dentro de la misma subred, lo que implica que introduciendo el comando `$ ping` en MV 01 seguido de la dirección IP local de la MV 02, comienza a transmitirse información de la máquina virtual primera a la segunda.

En la tercera máquina virtual, se inicia el programa *Wireshark* y en su ventana principal, se indica la tarjeta de red con la que se quiere capturar el tráfico (en este caso enp0s3), haciendo doble clic sobre ella, se pueden ver todos los paquetes que circulan a través de la red. Se va a estudiar un paquete `Echo (ping) request`. [Figura 3.9]

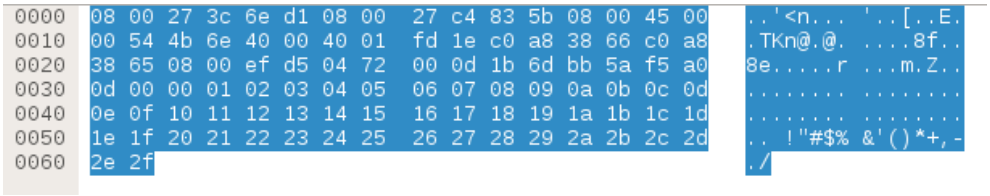


Figura 3.9.: Mensaje `Echo (ping) request` sin encriptar

Datos a destacar de este paquete son:

Los 6 primeros pares de dígitos: Indican la dirección MAC del receptor del mensaje.

Los pares de dígitos del 7 al 12: Indican la dirección MAC del emisor del mensaje.

Los 42 últimos pares de dígitos: Son una sucesión de números desde 00 hasta 2f en hexadecimal.

- **Conexión segura:** Sobre las tarjetas de red macsec0 conforme a lo indicado en el Apartado 3.1.4 ("Utilización de *MACsec* en *Debian*") en sendas máquinas virtuales, este paso del proyecto requiere cambiar la subred en la que se encuentra la tarjeta de red enp0s3. Para ello, se introduce en MV 03 el comando `ifconfig enp0s3 1.1.1.3/24`, lo que hace que la tarjeta que capta las comunicaciones entre MV 01 y MV 02 se encuentre ahora en la subred en la que las comunicaciones se transmiten de forma segura.

Ahora se pueden realizar los mismos pasos realizados en el punto de conexión no segura. Lo que se ve en esta ocasión en la ventana de trabajo es lo mostrado en la Figura 3.10.

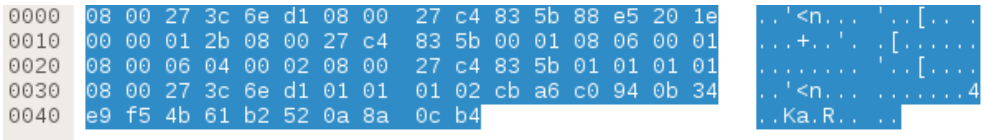


Figura 3.10.: Mensaje `Ping` encriptado

Datos a destacar de este paquete son:

Los 6 primeros pares de dígitos: Indican la dirección MAC del receptor del mensaje.

Los pares de dígitos del 7 al 12: Indican la dirección MAC del emisor del mensaje.

Los pares de dígitos del 15 al : Indican que el mensaje ha sido cifrado con la norma de seguridad 802.1AE.

Los pares de dígitos del 13 al 58: Son el mismo mensaje que en el caso anterior (la sucesión de dígitos 00 01 02...) pero en esta ocasión su contenido no es visible.

3.1.6. Prueba de velocidad: Latencia y ancho de banda

"En redes informáticas de datos la latencia es la suma de retardos temporales dentro de una red. Un retardo es producido por la demora en la propagación y transmisión de paquetes dentro de la red."

"[...] se conoce como ancho de banda a la cantidad de datos que pueden enviarse y recibirse en el marco de una comunicación. Dicho ancho de banda suele expresarse en bits por segundo o en múltiplos de esta unidad."

Por último se procede a realizar la medida de los parámetros de latencia y ancho de banda de la conexión entre las máquinas virtuales. Dicha medida se realizará en las dos situaciones de comunicación logradas: la conexión segura y la conexión no segura.

3.1.6.1. Latencia

Medir la latencia resulta bastante sencillo, únicamente se debe utilizar el comando `ping` en una de las dos máquinas virtuales indicando la dirección IP de la tarjeta de red destino. Recurriendo a esta herramienta se han obtenido los resultados mostrados en las Tablas 3.3a, 3.3b, 3.5a, 3.5b.

Cuadro 3.2.: Resultados de latencia en una comunicación no segura (ms)

(a) MV 01 a MV 02

1,300	0,858	0,766	0,705	0,763
0,785	0,791	0,771	0,775	0,786
0,770	0,826	0,746	0,765	0,914
0,756	0,561	0,787	0,827	0,760
0,764	0,850	0,769	0,757	0,744
0,778	0,752	0,761	0,786	0,779
0,750	0,763	0,764	0,750	0,765
0,777	0,854	0,825	0,755	0,747
0,764	0,743	0,794	0,254	0,848
0,427	0,790	0,762	0,769	0,760
0,701	0,844	0,751	0,745	0,760
0,757	0,765	0,750	0,771	0,725
0,785	0,827	0,762	0,753	0,744
0,746	0,704	0,740	0,750	0,741
0,734	0,763	0,722	0,739	0,752
0,490	0,720	0,771	0,798	0,789
0,928	0,753	0,765	0,730	0,715
0,820	0,743	0,762	0,815	0,763
0,836	0,742	0,753	0,766	0,738
0,776	0,710	0,741	0,732	0,749

(b) MV 02 a MV 01

0,804	0,365	0,751	0,734	0,757
0,827	0,740	0,739	0,784	0,757
0,671	0,755	0,772	0,735	0,747
0,851	0,764	0,771	0,744	0,654
0,755	0,857	0,761	0,755	0,744
0,810	0,757	0,767	0,765	0,751
0,828	0,889	0,762	0,763	0,747
0,840	0,866	0,735	0,752	0,755
0,929	0,743	0,760	0,719	0,757
0,846	0,842	0,757	0,500	0,821
0,745	1,394	0,728	0,747	0,753
0,855	0,757	0,785	0,751	0,744
0,759	0,763	0,735	0,802	0,748
0,749	0,759	0,738	0,752	0,764
0,766	1,400	0,821	0,770	0,728
0,744	0,814	0,826	0,750	0,732
0,731	0,734	0,761	0,758	0,755
0,781	0,483	0,749	0,782	0,762
0,815	0,681	0,757	0,736	0,736
0,725	0,745	0,759	0,754	0,770

Cuadro 3.4.: Resultados de latencia en una comunicación segura (ms)

(a) MV 01 a MV 02

0,645	0,851	0,875	0,873	0,871
0,581	0,858	0,854	0,861	0,896
0,895	0,832	0,891	0,852	0,875
0,503	1,016	0,857	0,854	0,875
0,918	0,856	0,854	0,862	0,831
0,719	0,842	0,893	0,886	0,877
0,954	0,846	0,880	0,901	0,866
0,841	0,865	0,843	0,846	0,844
0,631	0,855	0,864	0,850	0,869
0,964	0,857	0,801	0,866	0,860
0,890	0,844	0,910	0,868	0,836
0,441	0,891	0,906	0,860	0,871
0,875	0,867	0,857	0,769	0,856
0,902	0,798	0,867	0,863	0,903
0,968	0,920	0,874	0,796	0,867
0,806	0,831	0,866	0,863	0,847
0,934	0,882	0,889	0,864	0,863
0,881	0,892	0,857	0,879	0,864
0,943	0,855	0,876	0,805	0,889
0,807	0,851	0,932	0,849	0,865

(b) MV 02 a MV 01

0,894	0,892	0,893	0,924	0,876
0,859	0,991	0,996	0,872	0,937
0,934	0,913	0,908	0,951	0,892
0,875	0,866	0,919	0,854	0,924
0,656	0,886	0,914	0,905	0,782
1,071	0,914	0,994	0,916	0,814
0,876	0,899	0,959	0,830	0,902
0,943	0,803	0,813	0,893	0,896
0,855	0,767	0,861	0,735	0,886
0,857	1,019	0,897	0,983	0,779
0,905	0,901	0,890	0,902	0,870
0,877	0,971	0,895	0,940	0,967
0,846	0,864	0,891	0,891	0,909
0,921	1,062	0,900	0,847	0,914
0,853	0,891	0,867	0,964	0,881
0,873	0,909	0,849	0,829	0,898
0,850	0,862	0,853	0,889	0,846
0,871	0,936	0,891	0,891	0,877
0,883	0,976	0,902	0,973	0,894
0,766	0,972	0,862	0,788	0,797

Es importante destacar que previo a la realización de la prueba de conexión se debe configurar la tabla de rutado del núcleo del sistema, para garantizar que los paquetes que son enviados desde macsec0 llegen a macsec0 y los enviados desde enp0s3 lleguen a enp0s3 en la otra máquina virtual. Para ello, se introduce el comando `route add -net 1.1.1.2 dev macsec0` en el terminal del sistema operativo, donde:

`1.1.1.2` : Es la dirección que recibe los paquetes

`macsec0` : Es la tarjeta de red por la que deben de ir los paquetes.

"El núcleo del sistema lee la tabla de enrutamiento antes de reenviar paquetes a la red local. La tabla de enrutamiento enumera las direcciones IP de las redes que conoce el sistema, incluida la red local predeterminada del sistema. La tabla también enumera la dirección IP de un sistema de portal para cada red conocida. El portal es un sistema que puede recibir paquetes de salida y reenviarlos un salto más allá de la red local." [3]

3.1.6.2. Ancho de banda

En computación de redes y en biotecnologia, ancho de banda digital, ancho de banda de red o simplemente ancho de banda es la medida de datos y recursos de comunicación disponible o consumida1 expresados en bit/s o múltiplos de él como serían los Kbit/s,Mbit/s y Gigabit/s.[...] Ancho de banda puede referirse a la capacidad de ancho de banda o ancho de banda disponible en bit/s, lo cual típicamente significa el rango neto de bits o la máxima salida de una huella de comunicación lógico o físico en un sistema de comunicación digital.[...] Ancho de banda puede también referirse a ancho de banda consumido (consumo de ancho de banda), que corresponde al throughput o goodput conseguido; esto es, la tasa media de transferencia de datos exitosa a través de una vía de comunicación. [9]

Para poder medir el ancho de banda se recurre a un paquete llamado iperf. Dicho paquete se instala en MV 01 y MV 02, y se procede a los siguientes pasos:

- **1.** Se introduce el comando `iperf -s` en una de las dos máquinas virtuales. Esto hará que dicha máquina virtual actue de servidor.
- **2.** Se introduce el comando `iperf -c 192.168.1.56` en la segunda máquina virtual, donde `192.168.1.56` es la dirección IP de la tarjeta de red enp0s3 de la primera máquina virtual. Este comando devuelve el ancho de banda de la conexión no segura.
- **3.** Se introduce el comando `iperf -c 1.1.1.2` en la segunda máquina virtual, donde `1.1.1.2` es la dirección IP de la tarjeta de red enp0s3 de la primera máquina virtual. Este comando devuelve el ancho de banda de la conexión segura.

No Segura	Segura
$\overline{\chi}_{muestral}$ =0,766 ms/$\sigma^2_{muestral}$ =0,106 ms^2	$\overline{\chi}_{muestral}$ =0,871 ms/$\sigma^2_{muestral}$ =0,0741 ms^2

Cuadro 3.6.: Parámetros calculados

Estos comandos devuelven el siguiente texto:

Client connecting to 1.1.1.2, TCP port 5001
TCP window size: 43.8 KByte (default)

---

local 1.1.1.1 port 39434 connected with 1.1.1.2 port 5001
IDInterval Transfer Bandwidth
0.0-10.0 sec 1.10 GBytes 944 Mbits/sec
root@MV01: iperf -c 192.168.56.101

Client connecting to 192.168.56.101, TCP port 5001
TCP window size: 43.8 KByte (default)

---

local 192.168.56.102 port 33872 connected with 192.168.56.101 port 5001
IDInterval Transfer Bandwidth
0.0-10.0 sec 3.12 GBytes 2.68 Gbits/sec

3.2. Diagrama de Gantt/cronograma

Ver Figura 3.11.

3.3. Cálculos, algoritmos

En esta sección del documento se parte de los resultados experimentales de latencia mostrados en las Tablas 3.3a, 3.3b, 3.5a y 3.5b. Se recurren a las fórmulas estadísticas de media [Ecuación 3.1] y desviación típica [Ecuación 3.2] para calcular sus parámetros estadísticos.(Dichos parámetros se resumen en la Tabla 3.6)

$$\overline{\chi}_{muestral} = \sum_{i=0}^{n} \frac{\chi_i}{n} \tag{3.1}$$

$$\sigma^2_{muestral} = \frac{\sum_{i=0}^{n} (\chi_i - \overline{\chi})^2}{n} \tag{3.2}$$

El las figuras 3.13a y 3.13b se pueden observar los histogramas de los valores medidos. Asimismo se muestra la distribución normal asociada a estas medidas experimentales.

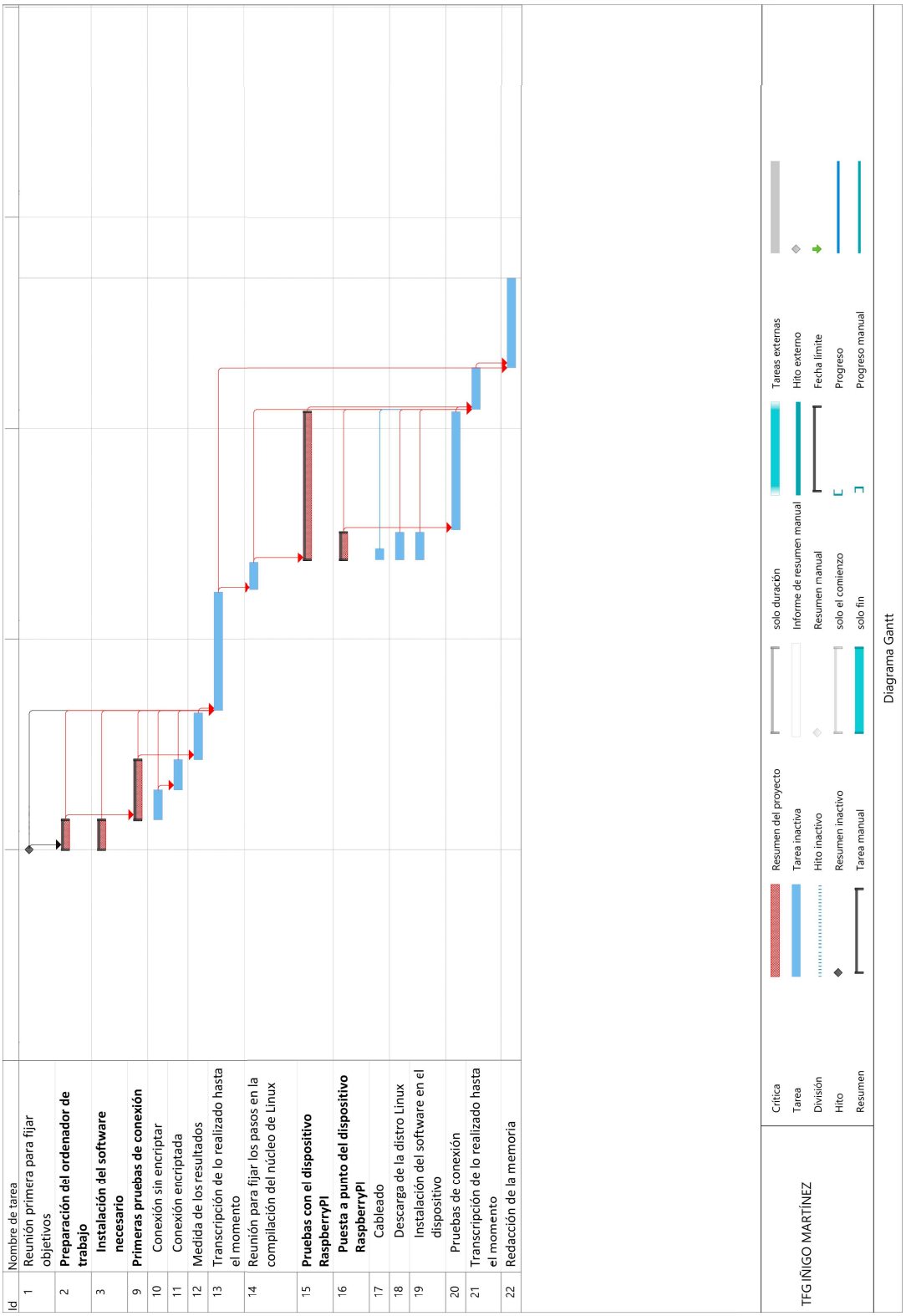


Figura 3.11.: Diagrama de Gantt realizado con MS Project

Para poderla graficar estos resultados, se recurre al programa informático *Microsoft Excel*. En dicho *software* se introducen las Ecuaciones 3.1 y 3.2 y se obtienen los parámetros media y varianza. Con dichos parámetros y las funciones integradas en el programa se puede trazar la curva de probabilidad asociada a la distribución normal resultado de estos exprerimentos.

3.4. Descripción de los resultados

Comparando las Figuras 3.9 y 3.10 se aprecia claramente la diferencia entre proteger mediante criptografía una comunicación o no hacerlo.

De las Figuras 3.13a, 3.13b se observa un claro aumento de la latencia en el caso de comunicación segura. No obstante, la distribución típica de los resultados se reduce al aplicar los mecanismos de encriptación, lo que puede resultar beneficioso en ciertas situaciones.

3.5. Extensión del proyecto

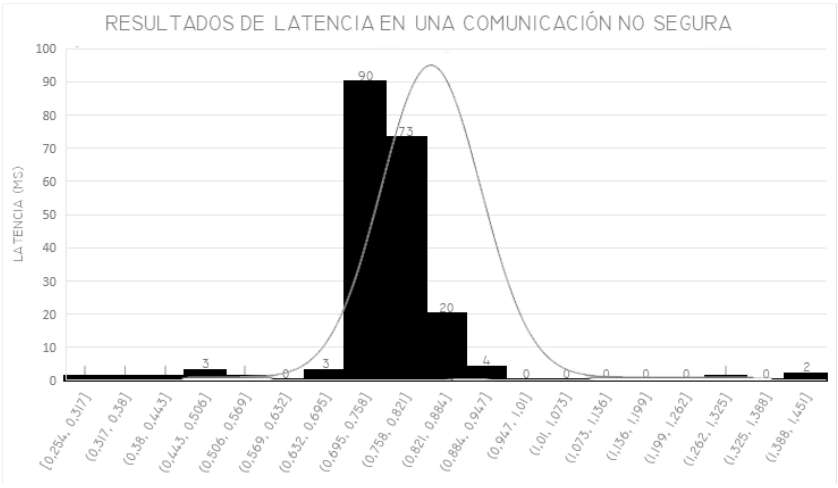
Una vez realizadas las pruebas en el programa *VirtualBox*, es posible extender el uso de las técnicas aquí vistas a otros dispositivos. Ejemplo de ello es el dispositivo *RaspberryPI* (Ver anexo A).

Este dispositivo es uno de tantos precursores del conocido como *Internet de las Cosas (IoT).La definición de IoT podría ser la agrupación e interconexión de dispositivos y objetos a través de una red (bien sea privada o Internet, la red de redes), dónde todos ellos podrían ser visibles e interaccionar.[...] Cualquier cosa que se pueda imaginar podría ser conectada a internet e interaccionar sin necesidad de la intervención humana, el objetivo por tanto es una interacción de máquina a máquina, o lo que se conoce como una interacción M2M (machine to machine) o dispositivos M2M* [7]. Por mencionar algunos usos de este dispositivo: estación meteorológica, cámara de seguridad, servidor de impresión, videoconsola,...

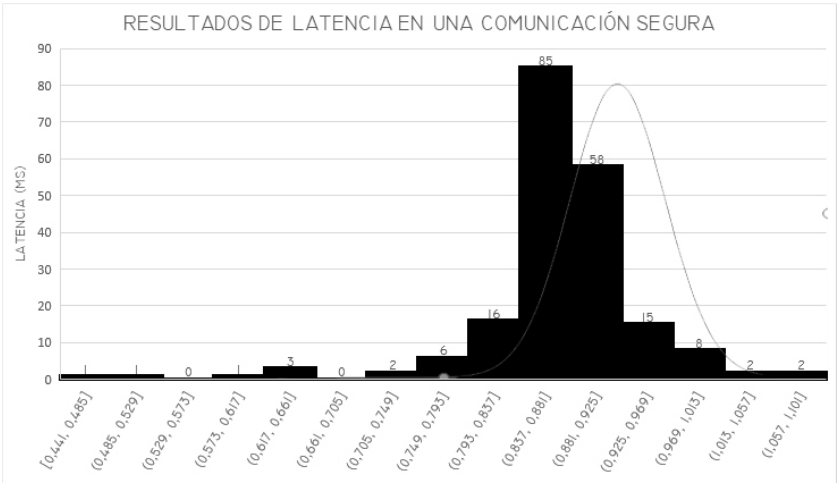
Debido a la elección de la distribución realizada (a saber *Raspbian* y *Debian*), es posible replicar el procedimiento de creación de una tarjeta de red MACSec en esta placa. No obstante, el usuario puede encontrarse ante la circunstancia de que el módulo *MACSec* no esté incluido por defecto en la compilación de Linux que ha descargado. Solucionarlo requerirá realizar una compilación del núcleo del sistema operativo. Este procedimiento, junto con un breve texto sobre la puesta a punto de *RaspberryPI* se puede encontrar en el Anexo A.

Asimismo, se debe tener en cuenta que de hacer las pruebas en la red de la EIB, no se

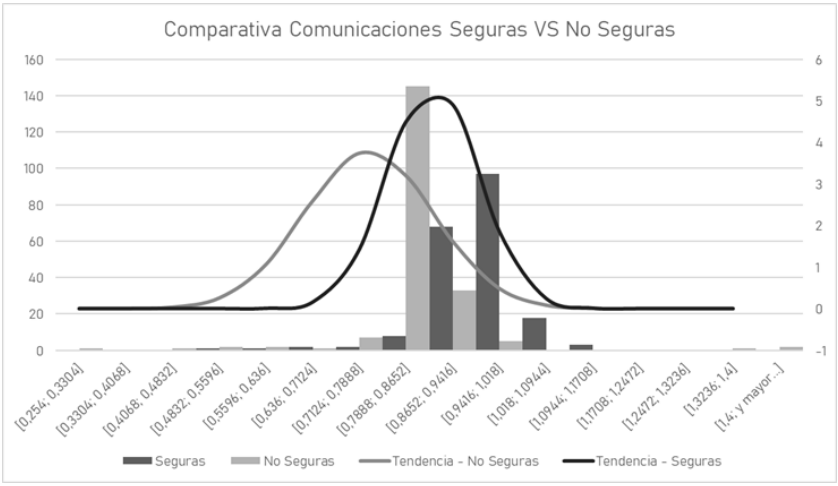
Figura 3.12.: Resultados de la medida



(a) Resultados de la medida de latencia en una comunicación no segura.



(b) Resultados de la medida de latencia en una comunicación segura.



(c) Comparativa entre los dos casos de comunicación.

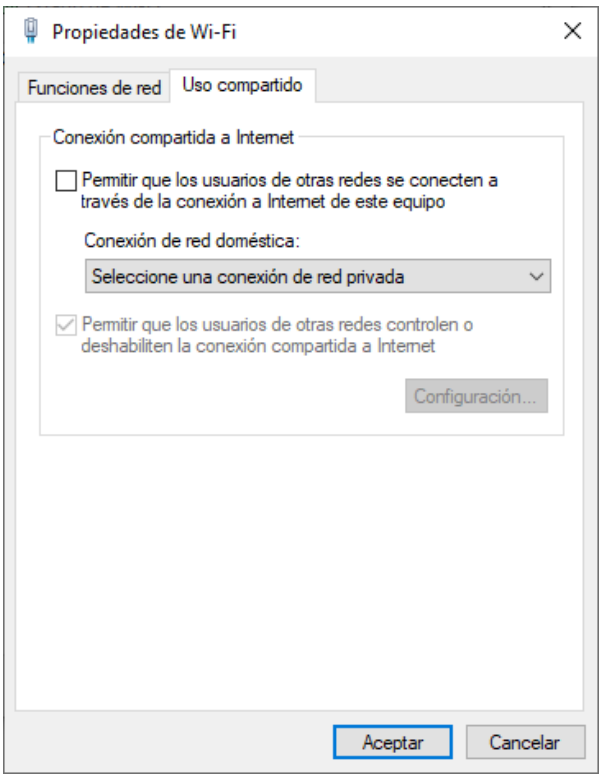


Figura 3.14.: Ventana *uso compartido de internet*

podrá conectar la placa mediante las clavijas RJ-45 dispuestas a tal fin. Esto es debido a que la universidad cuenta con un mecanismo de protección que impide que ordenadores no autorizados accedan a la red cableada. Las soluciones a este problema son varias:

- **Conseguir una dirección MAC válida:** Si se encuentra un ordenador en desuso que sí esté autorizado a acceder a Internet, se puede copiar la dirección MAC de su tarjeta de red a fin de usarla con la placa.
- **Usar la función "Compartir acceso a internet"de *Microsoft Windows*:** Siendo esta la opción elegida por el autor del presente documento, requiere dos puertos de red en el ordenador *host*. El primero de ellos se conecta a la red de la Escuela, teniendo acceso a Internet por ser un ordenador ya autorizado previamente. El segundo se conecta al dispositivo *RaspberryPI* y se habilita la opción *uso compartido de internet*. (Ver Figura 3.14)

Una vez seguidos los pasos aquí indicados, tanto la placa como el ordenador *host* estarán dentro de una misma subred, por lo que podrán realizarse los ensayos requeridos.

4. Conclusiones

4.1. Conclusiones relativas a la seguridad

De las pruebas realizadas se puede observar cómo el paquete que se envía primeramente sin encriptar puede ser fácilmente interpretado por cualquier persona con acceso a la subred sobre la que se envía el mensaje.([Figura 3.9]se observa una sencilla sucesión aritmética de cifras hexadecimales)

Sin embargo, una vez se recurre al protocolo de comunicaciones seguras *MACSec*, dicha sucesión queda protegida, no siendo posible acceder a la información del paquete sin la clave de cifrado.

4.2. Conclusiones relativas a la latencia y ancho de banda

En la Tabla 4.1 se resumen todos los resultados relacionados con la latencia y ancho de banda obtenidos en este proyecto.

De los resultados obtenidos se puede concluir lo siguiente:

- La conexión sin encriptar es claramente insegura y fácilmente accesible por cualquier intruso con acceso a la red en la que se realizan las comunicaciones.
- El protocolo *MACSec* proporciona una solución de seguridad a nivel *Layer 2*, impidiendo que la información enviada entre los dos dispositivos no pueda ser interpretada sin las claves de encriptación.
- La utilización del sistema *MACSec* requiere que antes de comenzar la configuración las dos partes conozcan las claves de encriptación que van a ser utilizadas. No hay opción (en esta solución) a generar claves sin haberlas pactado previamente.

Conexión	No Segura	Segura
Latencia	$\overline{\chi}_{muestral} = 0,766ms / \sigma^2_{muestral} = 0,106ms$	$\overline{\chi}_{muestral} = 0,871ms / \sigma^2_{muestral} = 0,0741ms$
A.d. banda	2,68 Gbits/sec	944 Mbits/sec

Cuadro 4.1.: Resultados obtenidos

- La aplicación de este mecanismo de seguridad aumenta la latencia en un 13,79 por 100, factor que debe tenerse en cuenta en sistemas que requieran un rápido envío de información. No obstante, el canal seguro ofrece una mayor certidumbre respecto a la latencia, lo que puede resultar beneficioso en situaciones en las que se esté dispuesto a sacrificar esta característica a cambio de tener valores más preponderantes a la media.
- El ancho de banda es 2,70 veces mayor en la conexión no segura que en la conexión segura, lo que resulta beneficioso en el envio de grandes cantidades de datos.

REFERENCIAS

[1] About wireshark. Tech. rep., Wireshark. Consultado 28/03/2018.

[2] Ipsec. *Wikipedia La Enciclopedia Libre*.

[3] Guía de administración del sistema: servicios ip. Tech. rep., Oracle, 2010. Consultado 16/04/2018.

[4] Understanding media access control security (macsec). Tech. rep., juniper, 2017.

[5] Macsec-solución para el cifrado de red. *Totalsec News* (2018).

[6] Cano, L. Commandes réseau sous windows et linux. *Pandora FMS* (2018). Consultado el 26/03/2018.

[7] Gracia, M. Iot - internet of things. *Deloitte*.

[8] Oracle Corporation. *Oracle VM VirtualBox® User Manual*, 2004.

[9] Quiñones-Angulo, F. X. Estudio de la red telefónica ip basada en elastix instalada en la comunidad salesiana maría auxiliadora. *Tesis para obtener el grado de Ingeniero en Sistemas y Computación* (2016).

[10] Seaman, M. Ieee standard for local and metropolitan area networks–media access control (mac) security.

A. Compilación del núcleo de Linux

El módulo *MACSec* viene instalado por defecto en las distribuciones *Debian* AMD64 e i386 que se utilizan en el presente documento. No obstante existen otras muchas distribuciones del SO *Linux* que no necesariamente incluyen de manera predeterminada esta característica.

La solución a este problema es realizar una compilación propia del núcleo de *LINUX* para poder incluir este módulo. Para realizar la demostración de los pasos a seguir en dicha tarea, se recurre al dispositivo *Raspberry Pi* y una distribución del SO llamada Raspbian.

"Raspberry Pi se refiere a una serie de pequeños dispositivos que constituyen un ordenador de una sola placa. Los desarrolla la Fundación Raspberry Pi en El Reino Unido con el fin de facilitar el aprendizaje de ciencias computacionales básicas en las escuelas. El modelo original resultó más popular de lo esperado, llegando a mercados que no habían sido previstos tales como la robótica." [Página web oficial de *Raspberry Pi*] (Ver Figura A.1)

Figura A.1.: Dispositivo Raspberry Pi

Para comenzar, se descarga una copia de la distribución *Raspbian* de la pagina web del dispositivo *Raspbery PI* (`https://www.raspberrypi.org/downloads/raspbian/`). Se presentan dos opciones para la descarga: la instalación mínima y la instalación con escritorio. Se opta por la instalación con escritorio, lo que hace que el proceso resulte mucho más sencillo.

Una vez descargada la imagen, esta se descomprime (recurriendo por ejemplo al programa *Winrar*) y se graba en una tarjeta de memoria *micro SD* a través del programa *Etcher*. El resultado será una tarjeta de memoria en la cual existen todos los archivos necesarios para ejecutar la distribución *Raspbian*.

A continuación, se introduce la tarjeta de memoria en la ranura dispuesta para ello en la placa *Raspberry Pi*. Asimismo, se realizan las conexiones necesarias para hacer funcionar el dispositivo, a saber:

- **Cable de red:** El cable con clavija RJ-45 proporciona acceso a internet.[1]
- **Cable micro USB:** Este proporciona corriente eléctrica al dispositivo. Se debe aplicar una tensión continua de 5V. Se conecta al puerto micro USB de la placa.
- **Teclado y ratón:** Serán los periféricos de entrada del dispositivo. Se conectan a cualquiera de los cuatro puertos USB de la placa.
- **Cable micro HDMI:** Cuyo segundo extremo se conecta al monitor en el que se desea visualizar el sistema operativo.
- **Ventilador:** Es recomendable emplear algún dispositivo activo o pasivo para refrigerar la CPU mientras se compila el núcleo del sistema.

Para comenzar se instalan los paquetes git y bc mediante el comando:

```
pi@raspberrypi: sudo apt-get install git bc
```

A continuación, se descarga el código del núcleo de *LINUX*:

```
pi@raspberrypi: git clone --depth=1 https://github.com/raspberrypi/linux
```

git: Usar el paquete git.

clone: Hacer una copia del directorio.

–depth=1: Descargar la última versión del núcleo.

[1] Los accesos por cable a internet de la UPV/EHU están protegidos y no permiten el acceso sin una dirección MAC en el dispositivo que haya sido validada. Para solucionar este problema se recurre a una segunda tarjeta de red en un ordenador con permisos de acceso a la red y la función *Permitir que los usuarios de otras redes se conecten a internet a través de este equipo* de *Windows 7*.

https://....: Es la URL del directorio.

Una vez hecho esto, se introduce:

```
pi@raspberrypi: cd linux
pi@raspberrypi:/linux KERNEL=kernel7
pi@raspberrypi:/linux make menuconfig
```

Lo que lleva a la ventana de configuración del núcleo de *LINUX*. Una vez en esta ventana, en la sección: `Device drivers/Network device suport`, se marca la opción `IEEE 802.1AE MAC-level encryption (MACsec).` Se guarda la configuración y se sale del menú de configuración del núcleo de LINUX.

Por último, se introducen los siguientes comandos:
make -j4 zImage modules dtbs
sudo make modules_install
sudo cp arch/arm/boot/dts/*.dtb /boot/
sudo cp arch/arm/boot/dts/overlays/*.dtb /boot/overlays/
sudo cp arch/arm/boot/dts/overlays/README /boot/overlays/
sudo cp arch/arm/boot/zImage /boot/ %KERNEL.img

Con estas acciones, el núcleo del sistema incluye ahora el módulo *MACSec* y por lo tanto, puede utilizarse el dispositivo *RaspberryPi* para cualquier prueba de seguridad conforme a lo visto en la memoria de este documento

B. Redacción de documentos en LaTeX

"LaTeXes un sistema de preparación de documentos para redacciones de alta calidad. Es utilizado principalmente en redacciones científico-técnicas de longitud media o larga, siendo posible utilizarlo en cualquier tipo de publicaciones.
LaTeXno es un procesador de textos. En cambio, permite al autor no preocuparse por la apariencia de sus documentos, si no, en redactar el contenido correcto."

La herramienta empleada para la redacción de este documento es el sistema de redacción de documentos LaTeX. Se ha optado por él ante el interés en emplearlo en futuros proyectos de mayor extensión. Aunque complicado al principio, es un recurso fácilmente accesible desde distintas plataformas y que proporciona múltiples recursos al redactor del documento. A continuación se muestran los pasos para redactar documentos en LaTeX.

B.1. Instalación de software necesario

Existen múltiples programas que permiten la redacción en el sistema (por ejemplo: Texmaker, Led, Kile, WinEdt...). Se ha optado por el programa *MikTeX* dada su facilidad de instalación y de uso. Para instalarlo, se accede a la página web `https://miktex.org/download` y se descarga una copia del instalador. Una vez descargada se realiza la instalación del *software* y se hace doble clic en su icono para empezar a trabajar con él.[Figura B.1]

Como alternativa a este programa, se muestra la página web *overleaf.com*. Dicha dirección permite la redacción de documentos con el sistema LaTeXmediante un navegador web y sin necesidad de ninguna instalación (la opción gratuita requiere únicamente registrarse con una dirección de correo electrónico válida). Asimismo, esta opción permite el almacenamiento de los archivos de la redacción *on-line*, sin necesidad de guardar ninguna copia por parte del usuario, lo que facilita la elaboración de documentos.[Figura B.2]

B.2. Redacción de documentos

En LaTeX, los textos no se redactan de la manera en la que un usuario de *suites* ofimáticas está acostumbrado. En este sistema, los documentos se redactan mediante

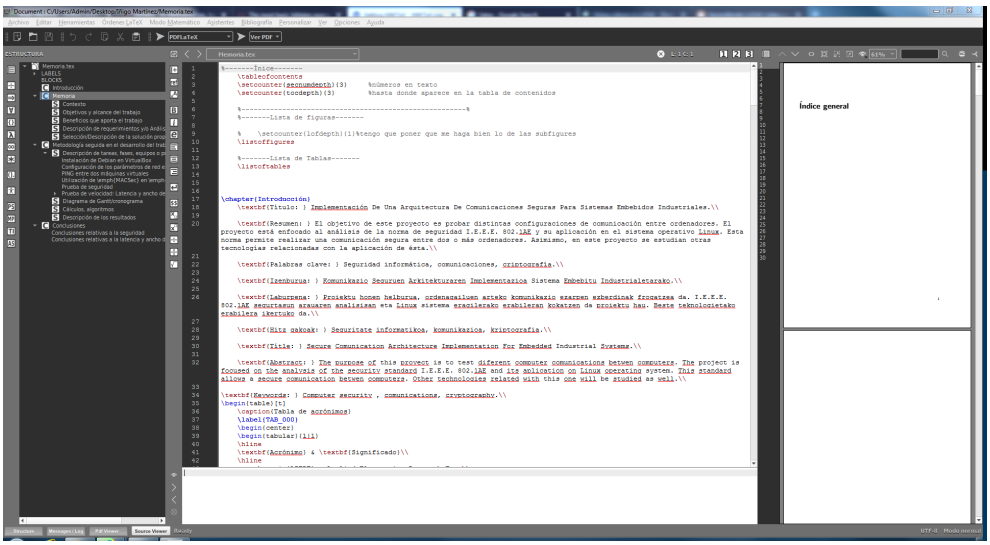


Figura B.1.: Ventana de trabajo de *MikTeX*

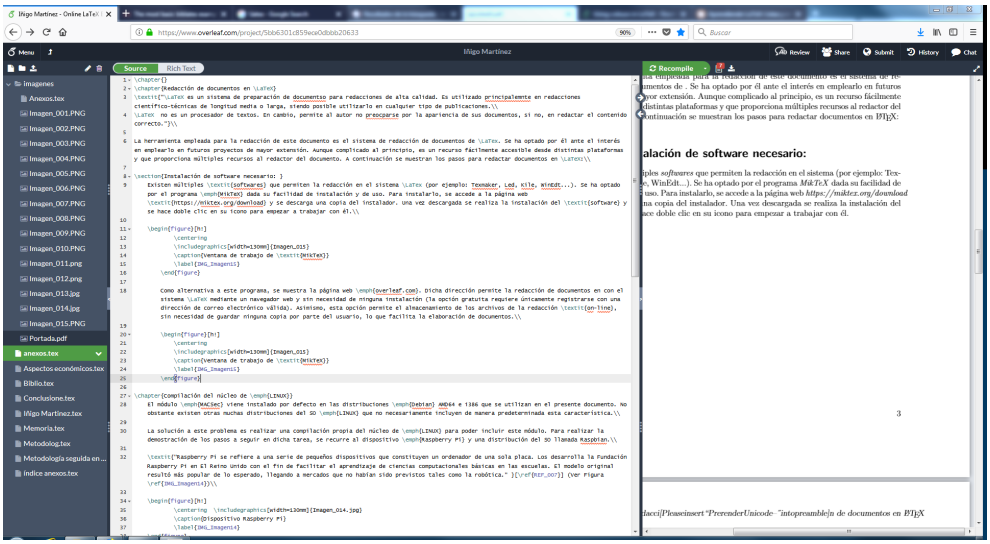


Figura B.2.: Ventana de trabajo de *overleaf.com*

clases de documentos, **paquetes** y **etiquetas**. La primera noción que el usuario de programas comunes (tales como *MS Word*) debe perder es la de pretender alcanzar un formato concreto en sus documentos. La inmensa mayoría de las opciones que en estos programas están al alcance del usuario común no lo están en LaTeX. La segunda idea a suprimir es que los documentos no se imprimen ni se guardan con formatos concretos, en cambio, se compilan.

Se comienzan los textos indicando la clase de documento que se va a redactar. La clase indica el tipo de documento que se va a redactar. Las clases más utilizadas son el *book*, *article* y *report*. En la primera línea del código del texto en LaTeXse incluye la clase a

utilizar precedida por las opciones de dicha clase:

```
\documentclass[opción1, opción2, etc.]{article}
```

Las opciones disponibles para cada clase se enumeran a continuación:

1. **Font size (10pt, 11pt, 12pt):** Con este parámetro se indica el tamaño de la fuente por defecto. En caso de no indicar nada, será de 10pt. Ejemplo de aplicación: `\documentclass[14pt]{article}`

2. **Paper size and format (a4paper, letterpaper, etc.):** En esta opción se indica el tipo de papel sobre el que se desea redactar el documento (a4paper, letterpaper, a5paper, b5paper, executivepaper, legalpaper...). Ejemplo de aplicación: `\documentclass[letterpaper]{article}`

3. **Draft mode (draft):** Esta opción permite que las compilaciones del documento no carguen las imágenes, en su lugar aparecerá cuadros en el documento. Con ello se agiliza la redacción del documento. Una vez se desee una edición definitiva, se elimina esta opción de la clase. Ejemplo de aplicación: `\documentclass[draft]{article}`

4. **Multiple columns (onecolumn, twocolumn):** Con este parámetro se indica si el texto debe aparecer en una o dos columnas. En caso de no indicar nada, será de una columna. Ejemplo de aplicación: `\documentclass[twocolumn]{article}`

5. **Formula-specific options (fleqn and leqno):** Esta opción indica la forma en la que debe aparecer las ecuaciones en el documento. En la Figura B.4e se muestra en la parte superior la configuración para ecuaciones por defecto, y en la inferior se aplican sendas opciones fleqn (alineación de las fórmulas izquierda en lugar de centrada) y leqno (índice de la ecuación a la izquierda en lugar de derecha). Ejemplo de aplicación: `\documentclass[fleqn,leqno]{article}`

6. **Landscape print mode (landscape):** Este parámetro cambia la orientación de la página sobre la que se está escribieno. No obstante, no cambia el tamaño del área sobre la que se redacta, por lo que se hace conveniente utilizar un paquete a tal fin. En la parte izquierda de la Figura B.4g se muestran los márgenes de la orientación horizontal por defecto, y en la derecha se ha utilizado el paquete geometry. Ejemplo de aplicación: `\documentclass[landscape]{article}`

7. **Single- and double-sided documents (oneside, twoside):** Esto indica si las páginas del documento deben ser todas iguales, o deben tener una simetría derecha-izquierda para que el documento pueda ser leido en forma de libro. Ejemplo de aplicación: `\documentclass[twoside]{article}`

8. **Titlepage behavior (notitlepage, titlepage):** Esta opción indica si cada página debe empezar con el título del capítulo en el que se encuentra. Por defecto *report* y *book* incluyen el título, mientras que *article* no. Ejemplo de aplicación: `\documentclass[titlepage]{article}`

9. **Chapter opening page (openright, openany):** Este parámetro permite que cada capítulo comience en cualquier página o comience exclusivamente en la página derecha.

Lo siguiente que debe incluirse en el código del documento LaTeXson los paquetes a utilizar. Estos son algunos de los paquetes utilizados en la redacción del presente documento:

- **babel:** Indicando para este paquete la opción spanish, permite tildar las vocales. En general, este paquete permite introducir caracteres própios de cada idioma.
- **inputenc:** Este paquete traduce la codificación en la que se escribe el código del documento al lenguaje interno de LaTeX.
- **graphicx:** Permite introducir imágenes en el documento.
- **appendix:** Aplica un formato distintivo a los índices de los títulos de los anexos.
- **listings:** Permite crear varios tipos de enumeraciones.
- **subcaption:** Con este paquete se crean las subtablas.
- **color:** Permite aplicar color al texto y crear cuadros de colores en los que aparezca texto.
- **biblatex:** Requiere un programa externo para su funcionamiento (JabRef), correctamente ejecutado crea de manera automática la bibliografía del documento.

Lo siguiente que debe escribirse en el código es: `\begin {document}`. Esto da comienzo al espacio en el que el texto se redacta el texto que compone el documento. La estructura del texto será la siguiente:

- `part`
- `chapter`
- `section`
- `subsection`
- `subsubsection`
- `paragraph`
- `subparagraph`

Una manera sencilla de redactar es comenzar utilizando únicamente `chapter` y `section`. Es el compilador el que asigna índices numéricos a cada capitulo y sección, por lo que el usuario puede comenzar a redactar libremente una vez ha indicado mediante las sentencias: `\chapter{capitulo de ejemplo}`, `\section{sección de ejemplo}` dónde se encuentra dentro del documento. A continuación se muestran sentencias útiles a emplear en la redacción del documento:

- Las siguientes sentencias introducen el índice del documento, el índice de tablas y el índice de imágenes:
  ```
  \tableofcontents
  \listoffigures
  \listoftables
  ```

- `\textbf{ }`: Pone el texto entre corchetes en negrita.
- `\ref{código de la referencia}`: Permite referenciar tablas o imágenes.
- Estas secuencias permiten incluir imágenes en el documento:
  ```
  \begin { figure }
  \centering
  \caption {Aquí se introduce el texto que acompaña a la imagen}
  \includegraphics[width=130mm]
  \label { Aquí se introduce el código para referenciar la imagen }
  \end { figure }
  ```

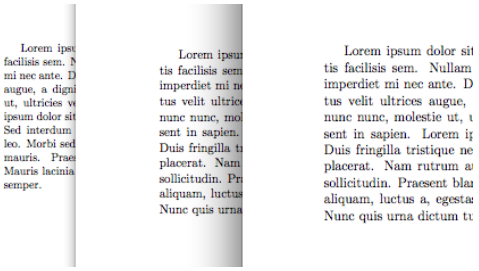
- Con el siguiente código se genera una tabla:
  ```
  \begin { table }
  \caption {Aquí se introduce el texto que acompaña a la imagen}
  \label { Aquí se introduce el código para referenciar la tabla }
  \begin { tabular } {|l|l|l|l| }
  ```

```
\hline% Introduce una línea horizontal
\multicolumn { 3 } {|l| }{ Texto de prueba }  0
\hline%Aquí se combinan las primeras 3 columnas para la 1ª fila de la
tabla.
1 & 2 & 3 & 4 \\\hline
5 & 6 & 7 & 8\\\hline
\end { tabular }
\end { table }
```

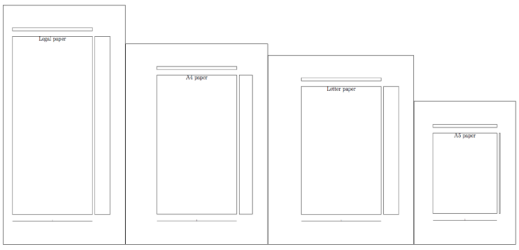
- El comando \printbibliography acompañado del paquete *biblatex* y gestionando las referencias con el programa *JabRef*, redacta de manera automática las referencias bibliográficas.

Lo último que debe introducirse en el documento es la sentencia \end { document }, lo que pone fin a la redacción del documento.

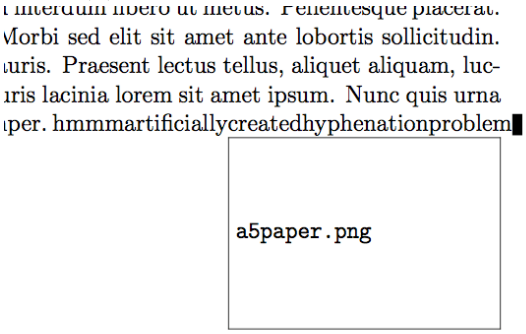
Figura B.3.: Opciones de cada clase



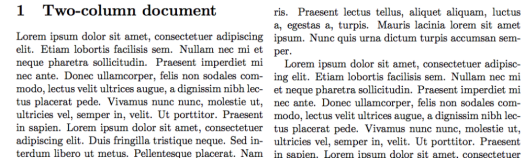
(a) Distintos tamaños de letra



(b) Distintos tipos de papel



(c) Imagen en el documento cuando figura la opción draft

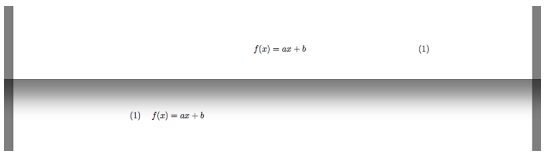


1 Two-column document

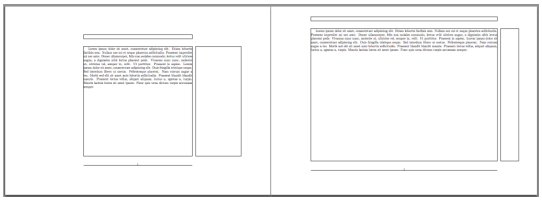
Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam

(d) Opción dos comulmnas indicada



(e) Distintas maneras de mostrar las ecuaciones



(f) Orientación horizontal de la página sin y con paquete para modificar los márgenes

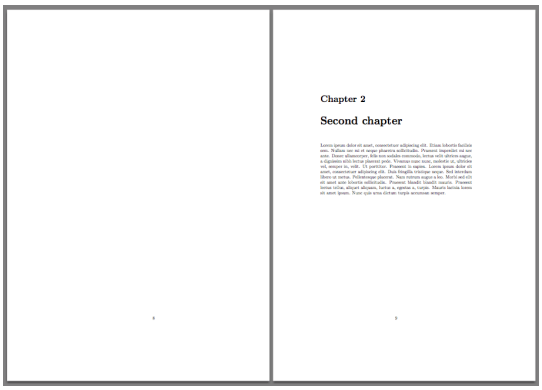
This is an article

February 7, 2013

Abstract

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

(g) Opción twoside indicada, las páginas son simétricas



Chapter 2

Second chapter

(h) Opción openright indicada