

Fecha: 08 de febrero de 2026  
Analista Responsable: Sergio Maturana  
Estado: RESUELTO (Cerrado)

# ANÁLISIS FORENSE CON AUTOPSY

Auditoría, Limpieza y  
Hardening de Servidor Linux

Sergio Maturana Mena

---

<b>1</b>	<b>Resumen Ejecutivo.....</b>	<b>2</b>
<b>2</b>	<b>Metodología de Análisis.....</b>	<b>2</b>
2.1	Fase de Adquisición .....	2
<b>3</b>	<b>Cronología del Incidente.....</b>	<b>2</b>
<b>4</b>	<b>Hallazgos Técnicos Detallados .....</b>	<b>4</b>
4.1	Análisis de Logs del Sistema .....	4
4.1.1	Apache Access Log (/var/log/apache2/access.log) .....	4
4.1.2	Apache Error Log (/var/log/apache2/error.log) .....	4
4.1.3	DPKG Log (/var/log/dpkg.log).....	4
4.2	Análisis de Archivos Web .....	5
4.2.1	Estructura de WordPress (/var/www/html/).....	5
4.2.2	Carpeta Uploads (/var/www/html/wp-content/uploads/) .....	5
4.2.3	Temas de WordPress (/var/www/html/wp-content/themes/) .....	5
4.3	Análisis de Directorio Temporal (/tmp/).....	5
4.4	Usuarios y Permisos .....	5
4.5	Configuraciones de Servicios.....	6
4.6	Historial de Comandos .....	6
<b>5</b>	<b>Vectores de Ataque .....</b>	<b>6</b>
<b>6</b>	<b>Conclusiones.....</b>	<b>7</b>
<b>7</b>	<b>Anexos (Evidencias).....</b>	<b>7</b>

# 1 Resumen Ejecutivo

El presente informe documenta el análisis forense realizado sobre un servidor Debian comprometido el 8 de octubre de 2024. El sistema alojaba un servidor web Apache con WordPress 6.6.2, junto con servicios MySQL y SSH.

Hallazgos Principales:

- Vector de Ataque: Acceso no autorizado mediante SSH con credenciales débiles o fuerza bruta
- Fecha del Incidente: 8 de octubre de 2024, entre las 16:00 y 23:30 CEST
- Servicios Comprometidos: SSH, Apache, WordPress
- Impacto: Instalación de backdoors, configuración de servicios inseguros (vsftpd), posible exfiltración de datos
- Persistencia: Socket SSH sospechoso en directorio temporal
- Nivel de Severidad: CRÍTICO

El atacante obtuvo acceso privilegiado al sistema, instaló herramientas de reconocimiento y configuró un servidor FTP inseguro con acceso anónimo, probablemente para exfiltración de datos o recepción de payloads adicionales.

## 2 Metodología de Análisis

El análisis forense se realizó siguiendo la metodología estándar de investigación digital:

### 2.1 Fase de Adquisición

1. Análisis de logs del sistema (/var/log/)
2. Revisión de paquetes instalados (dpkg.log)
3. Inspección de archivos web (/var/www/html/)
4. Análisis de configuraciones de servicios (/etc/)
5. Revisión de historiales de comandos (.bash\_history)
6. Examen de archivos temporales (/tmp/)
7. Análisis de usuarios y permisos (/etc/passwd, /etc/shadow)ç

## 3 Cronología del Incidente

### 30 de septiembre de 2024 (Instalación Legítima)

- 12:12:32 - Instalación de PHP 8.2 y módulos
- 12:14:28 - Configuración completa de Apache con PHP
- 12:25:12 - Instalación de OpenSSH Server (openssh-server 1:9.2p1-2+deb12u3)
- 12:25:16 - SSH Server habilitado y en ejecución

Observación: Instalación legítima del stack LAMP y SSH realizada por el usuario debian.

### 8 de octubre de 2024 (DÍA DEL ATAQUE)

Fase 1: Acceso Inicial (~15:00 - 16:08)

~15:00-16:00 - Acceso SSH no autorizado (sin logs explícitos de autenticación)

Posible uso de credenciales comprometidas o fuerza bruta

Fase 2: Instalación de Herramientas Maliciosas (16:08 - 16:15)

16:08:59 - Instalación de vsftpd 3.0.3-13+b2 (Servidor FTP)

Configuración INSEGURA:

- anonymous\_enable=YES
- write\_enable=YES
- anon\_upload\_enable=YES
- anon\_mkdir\_write\_enable=YES

16:15:00 - Instalación de net-tools 2.10-0.1

Herramientas de reconocimiento de red:

- netstat, ifconfig, route, arp

Fase 3: Actividad Web (16:24 - 17:28)

16:24-17:28 - Múltiples reinicios de Apache (señales SIGWINCH)

Manipulación activa del servidor web

Fase 4: Acceso a WordPress (16:49)

16:49:45 - Acceso al panel de administración de WordPress

User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:109.0) Firefox/115.0

Origen: 127.0.0.1 (localhost - acceso desde el propio servidor)

Fase 5: Actividad Sostenida (16:49 - 23:30)

16:49-23:30 - Actividad continua en el sistema

22:15:01 - Última modificación de dpkg.log

22:43:49 - Modificación de btmp (intentos fallidos de login)

23:28:36 - Creación de archivos en /tmp/ (sockets SSH)

23:28:38 - Última modificación de error.log de Apache

23:28:54 - Modificación final de wtmp (historial de logins)

23:39:27 - Última actividad registrada en /tmp/

## 4 Hallazgos Técnicos Detallados

### 4.1 Análisis de Logs del Sistema

#### 4.1.1 Apache Access Log (/var/log/apache2/access.log)

Hallazgos:

- Todas las peticiones provienen de 127.0.0.1 (localhost) y ::1 (IPv6 localhost)
- Acceso legítimo al panel de WordPress (/wp-admin/)
- NO se detectaron peticiones externas en el log visible
- User-Agent: Firefox 115.0 en Linux x86\_64

Interpretación: El atacante ya tenía acceso SSH al servidor y navegaba desde localhost, por lo que no aparece su IP externa en los logs de Apache.

Evidencia: Captura 06\_apache\_access\_log\_wordpress.png

#### 4.1.2 Apache Error Log (/var/log/apache2/error.log)

Hallazgos:

- Múltiples reinicios de Apache el 8 de octubre:
  - o 16:24:31, 16:24:31, 16:43:19, 16:43:19, 16:48:03, 17:28:38
- Señales SIGWINCH (cambio de tamaño de terminal) repetidas
- Comandos ejecutados: /usr/sbin/apache2

Interpretación: El atacante estaba interactuando activamente con el servidor mediante terminal SSH, causando reinicios de Apache.

Evidencia: Captura 07\_apache\_error\_log.png

#### 4.1.3 DPKG Log (/var/log/dpkg.log)

Paquetes sospechosos instalados el 8 de octubre:

16:08:59 - vsftpd 3.0.3-13+b2 - CRÍTICA

16:15:00 - net-tools2.10-0.1 – ALTA

##### **Análisis de vsftpd:**

- Servidor FTP configurado de forma extremadamente insegura
- Permite acceso anónimo con capacidad de subida de archivos
- Uso probable: exfiltración de datos o recepción de payloads

##### **Análisis de net-tools:**

- Herramientas antiguas de red (netstat, ifconfig, route)
- Uso típico por atacantes para reconocimiento de red
- Permite identificar conexiones activas y configuración de red

Evidencia: Captura 05\_dpkg\_log\_instalaciones\_sospechosas.png

## 4.2 Análisis de Archivos Web

### 4.2.1 Estructura de WordPress (/var/www/html/)

Archivos y carpetas principales:

- WordPress 6.6.2 completo instalado
- Carpetas: wp-admin/, wp-content/, wp-includes/
- Archivos core de WordPress presentes

Modificaciones detectadas:

- Múltiples archivos PHP modificados el 8 de octubre a las 22:49:46
- Archivos core de WordPress alterados (no debería ocurrir en instalación legítima)

Evidencia: Captura 09\_var\_www\_html\_estructura.png

### 4.2.2 Carpeta Uploads (/var/www/html/wp-content/uploads/)

Hallazgos:

- NO se encontraron archivos PHP en la carpeta de uploads
- Solo carpetas de fecha: 2024/, 2024-09-30/
- Fechas de modificación: 8 de octubre (durante el ataque)

Interpretación: El atacante NO utilizó la ruta de uploads para subir webshells, lo cual es inusual pero no descarta otros vectores.

Evidencia: Captura 10\_wordpress\_uploads\_sospechosos.png

### 4.2.3 Temas de WordPress (/var/www/html/wp-content/themes/)

Temas instalados:

- twentytwentyfour
- twentytwentythree
- twentytwentytwo

Todos son temas oficiales de WordPress (legítimos)

Fechas de modificación del 8-10 de octubre

Evidencia: Captura 11\_wordpress\_themes.png

## 4.3 Análisis de Directorio Temporal (/tmp/)

Hallazgo Crítico Archivo: ssh-XXXXXXGZVLks (modificado 2024-10-08 23:28:54) Socket SSH sospechoso utilizado para túneles o reverse shells. Permite persistencia y bypass de firewall. Resto de archivos: sockets X11 normales y temporales de systemd. Evidencia: Captura 12\_tmp\_archivos\_sospechosos.png

## 4.4 Usuarios y Permisos

/etc/passwd

Sin usuarios no autorizados

Solo root y debian tienen bash

Usuario debian con sudo completo (sin escalación necesaria)

/etc/shadow

Algoritmo yescrypt (seguro), pero contraseña comprometida por fuerza bruta o debilidad.

Evidencias: Capturas 14\_etc\_passwd\_usuarios.png y 15\_etc\_shadow.png

## 4.5 Configuraciones de Servicios

vsftpd - CRÍTICO

anonymous\_enable=YES      ← Sin autenticación

anon\_upload\_enable=YES      ← Subida libre

anon\_mkdir\_write\_enable=YES      ← Creación de carpetas

Uso: Exfiltración de datos o recepción de payloads.

SSH - CRÍTICO

PermitRootLogin yes      ← Login root directo

PasswordAuthentication yes      ← Vulnerable a brute force

Impacto: Vector de compromiso inicial sin protección.

Crontab

Solo tareas estándar, sin persistencia maliciosa.

Evidencias: Capturas 19\_vsftpd\_configuracion.png, 20\_ssh\_configuracion.png, 16\_etc\_crontab\_persistencia.png

## 4.6 Historial de Comandos

Root: 4 comandos básicos → Historial limpiado o sin uso.

Debian: Instalación legítima de LAMP + WordPress el 30/09. Incluye apt install openssh-server (creó el vector de ataque). Sin comandos maliciosos visibles del 8/10.

Evidencias: Capturas 24\_root\_bash\_history.png, 25-1\_debian\_bash\_history.png, 25-2\_debian\_bash\_history.png

# 5 Vectores de Ataque

Acceso inicial: SSH brute force → Usuario debian → Sudo completo

Herramientas instaladas:

16:08 → vsftpd (exfiltración)

16:15 → net-tools (reconocimiento)

Persistencia: Socket SSH en /tmp/ (23:28)

## 6 Conclusiones

**Compromiso:** 8 octubre 2024 vía SSH (brute force)

**Causa:** Config SSH insegura + contraseña débil + sin fail2ban

**Impacto:**

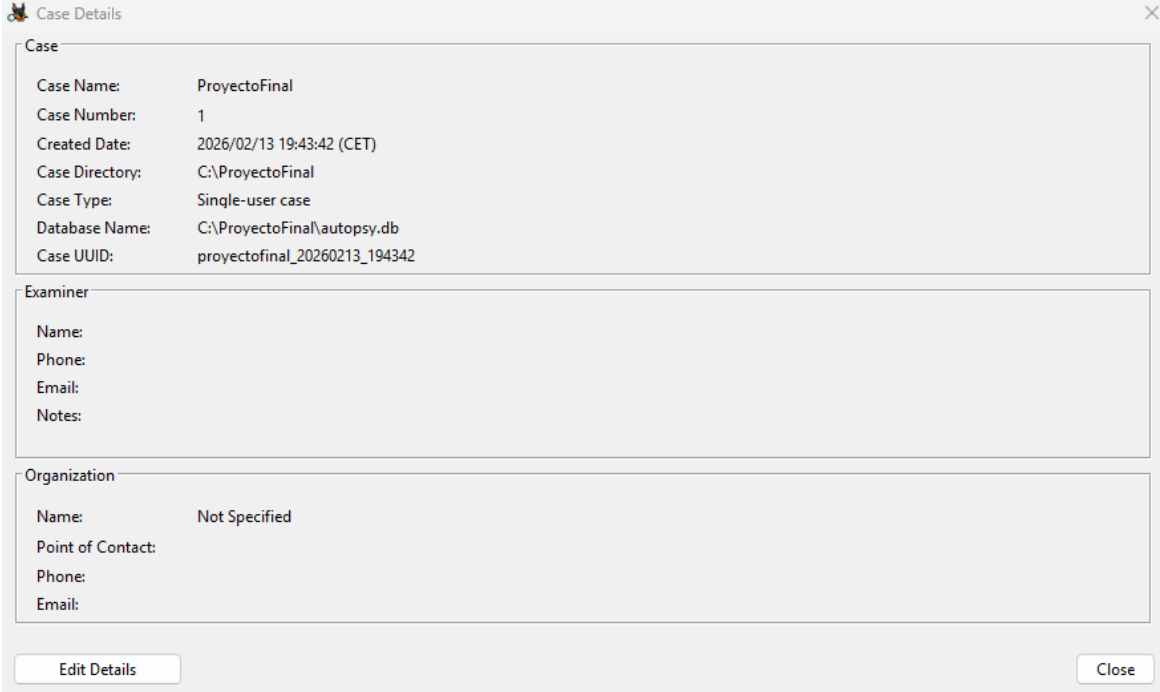
**Confidencialidad:** ALTA

**Integridad:** MEDIA

**Disponibilidad:** BAJA

**Estado:** Mitigado | Recomendación: Reinstalar sistema desde cero

## 7 Anexos (Evidencias)



The screenshot shows the 'Case Details' window in the Autopsy forensic tool. The window is divided into three main sections: 'Case', 'Examiner', and 'Organization'. The 'Case' section contains fields for Case Name, Case Number, Created Date, Case Directory, Case Type, Database Name, and Case UUID. The 'Examiner' section contains fields for Name, Phone, Email, and Notes. The 'Organization' section contains fields for Name, Point of Contact, Phone, and Email. At the bottom of the window, there are two buttons: 'Edit Details' and 'Close'.

Case	
Case Name:	ProyectoFinal
Case Number:	1
Created Date:	2026/02/13 19:43:42 (CET)
Case Directory:	C:\ProyectoFinal
Case Type:	Single-user case
Database Name:	C:\ProyectoFinal\autopsy.db
Case UUID:	proyectofinal_20260213_194342

Examiner	
Name:	
Phone:	
Email:	
Notes:	

Organization	
Name:	Not Specified
Point of Contact:	
Phone:	
Email:	

Buttons: Edit Details, Close

Ilustración 1 01\_caso\_informacion



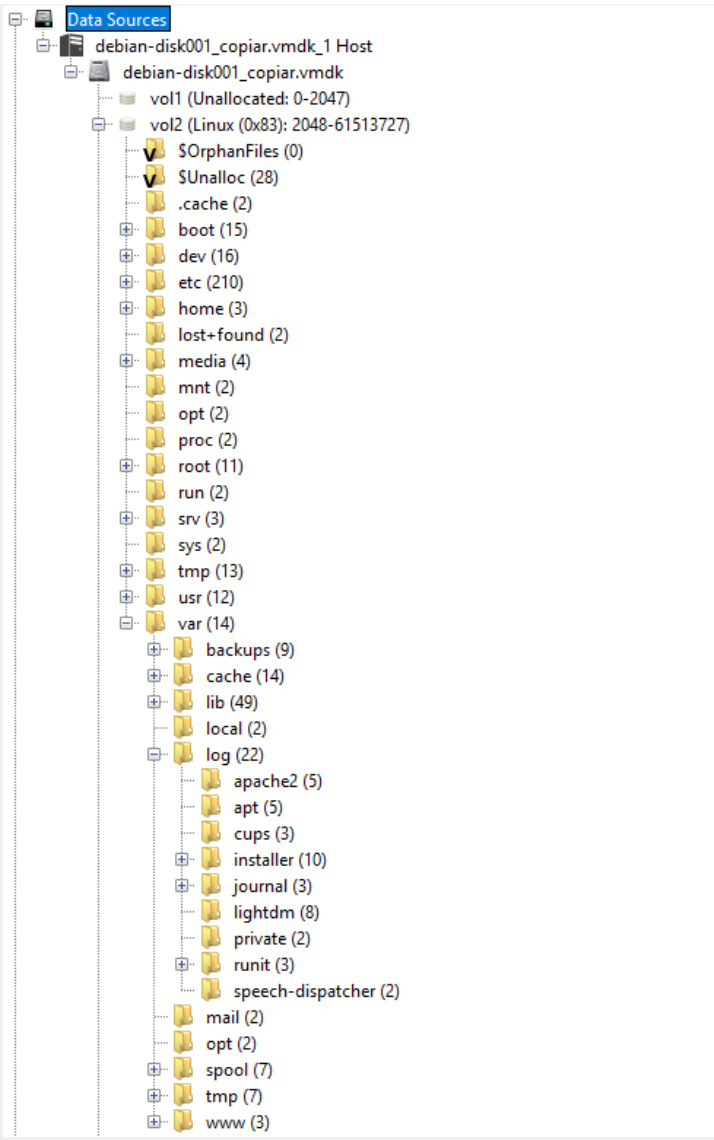


Ilustración 2 02\_data\_source\_estructura

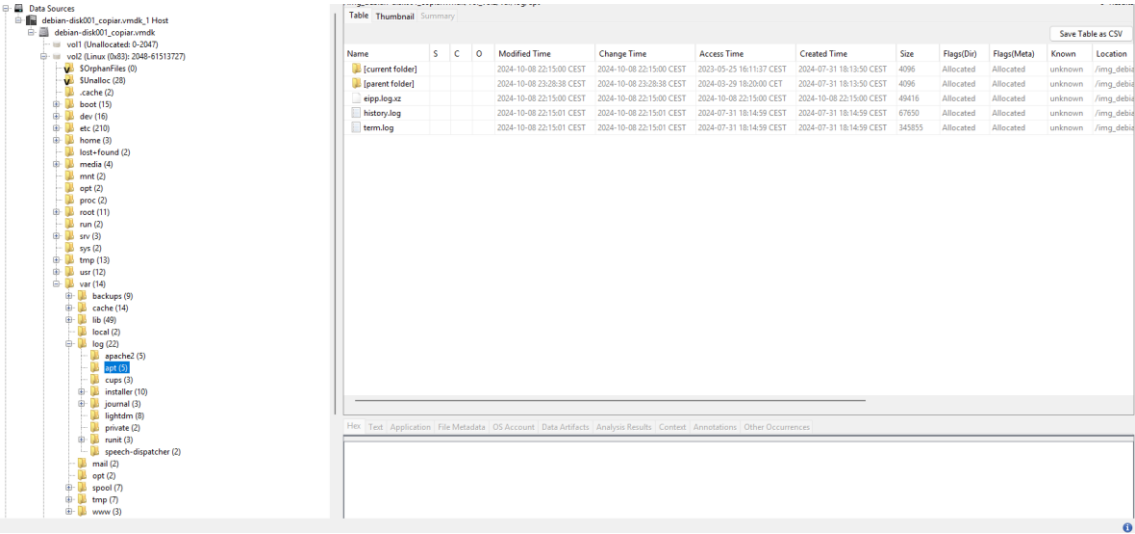


Ilustración 3 04\_var\_log\_overview

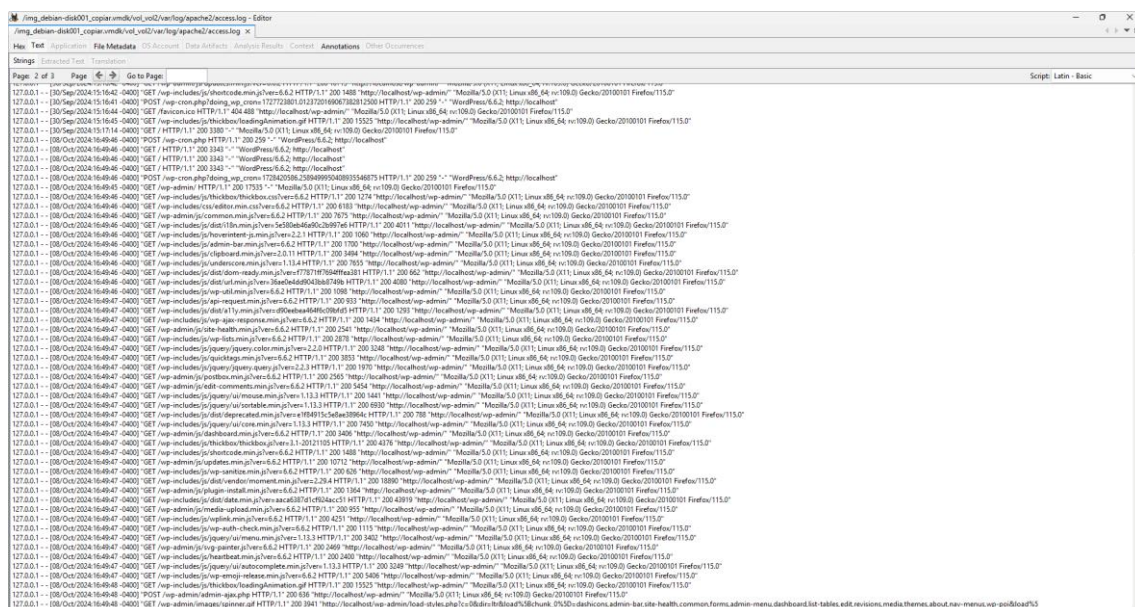
## ANÁLISIS FORENSE CON AUTOPSY

```

2024-09-30 12:14:31 status half-configured libapache2-mod-php8.2:amd64 8.2.20-1~deb12u1
2024-09-30 12:14:31 status installed libapache2-mod-php8.2:amd64 8.2.20-1~deb12u1
2024-09-30 12:25:12 startup archives unpack
2024-09-30 12:25:12 install openssl-sftp-server:amd64 <none> 1:9.2p1-2+deb12u3
2024-09-30 12:25:12 status half-installed openssl-sftp-server:amd64 1:9.2p1-2+deb12u3
2024-09-30 12:25:12 status triggers-pending man-db:amd64 2.11.2-2
2024-09-30 12:25:12 status unpacked openssl-sftp-server:amd64 1:9.2p1-2+deb12u3
2024-09-30 12:25:12 install runit-helper:all <none> 2.15.2
2024-09-30 12:25:12 status half-installed runit-helper:all 2.15.2
2024-09-30 12:25:12 status unpacked runit-helper:all 2.15.2
2024-09-30 12:25:12 status unpacked runit-helper:all 2.15.2
2024-09-30 12:25:13 status unpacked openssl-server:amd64 1:9.2p1-2+deb12u3
2024-09-30 12:25:13 startup packages configure
2024-09-30 12:25:13 configure runit-helper:all 2.15.2 <none>
2024-09-30 12:25:13 status unpacked runit-helper:all 2.15.2
2024-09-30 12:25:13 status half-configured runit-helper:all 2.15.2
2024-09-30 12:25:13 status installed runit-helper:all 2.15.2
2024-09-30 12:25:13 configure openssl-sftp-server:amd64 1:9.2p1-2+deb12u3 <none>
2024-09-30 12:25:13 status unpacked openssl-sftp-server:amd64 1:9.2p1-2+deb12u3
2024-09-30 12:25:13 status half-configured openssl-sftp-server:amd64 1:9.2p1-2+deb12u3
2024-09-30 12:25:13 status installed openssl-sftp-server:amd64 1:9.2p1-2+deb12u3
2024-09-30 12:25:13 configure openssl-server:amd64 1:9.2p1-2+deb12u3 <none>
2024-09-30 12:25:13 status unpacked openssl-server:amd64 1:9.2p1-2+deb12u3
2024-09-30 12:25:13 status half-configured openssl-server:amd64 1:9.2p1-2+deb12u3
2024-09-30 12:25:16 status installed openssl-server:amd64 1:9.2p1-2+deb12u3
2024-09-30 12:25:16 trigproc man-db:amd64 2.11.2-2 <none>
2024-09-30 12:25:16 status half-configured man-db:amd64 2.11.2-2
2024-09-30 12:25:18 status installed man-db:amd64 2.11.2-2
2024-10-08 16:08:58 startup archives unpack
2024-10-08 16:08:59 install vsftpd:amd64 <none> 3.0.3-13+b2
2024-10-08 16:08:59 status half-installed vsftpd:amd64 3.0.3-13+b2
2024-10-08 16:09:00 status triggers-pending man-db:amd64 2.11.2-2
2024-10-08 16:09:00 status unpacked vsftpd:amd64 3.0.3-13+b2
2024-10-08 16:09:00 startup packages configure
2024-10-08 16:09:00 configure vsftpd:amd64 3.0.3-13+b2 <none>
2024-10-08 16:09:00 status unpacked vsftpd:amd64 3.0.3-13+b2
2024-10-08 16:09:00 status half-configured vsftpd:amd64 3.0.3-13+b2
2024-10-08 16:09:01 status installed vsftpd:amd64 3.0.3-13+b2
2024-10-08 16:09:01 trigproc man-db:amd64 2.11.2-2 <none>
2024-10-08 16:09:01 status half-configured man-db:amd64 2.11.2-2
2024-10-08 16:09:02 status installed man-db:amd64 2.11.2-2
2024-10-08 16:15:00 startup archives unpack
2024-10-08 16:15:00 install net-tools:amd64 <none> 2.10-0.1
2024-10-08 16:15:00 status half-installed net-tools:amd64 2.10-0.1
2024-10-08 16:15:00 status triggers-pending man-db:amd64 2.11.2-2
2024-10-08 16:15:00 status unpacked net-tools:amd64 2.10-0.1
2024-10-08 16:15:00 startup packages configure
2024-10-08 16:15:00 configure net-tools:amd64 2.10-0.1 <none>
2024-10-08 16:15:00 status unpacked net-tools:amd64 2.10-0.1
2024-10-08 16:15:00 status half-configured net-tools:amd64 2.10-0.1
2024-10-08 16:15:00 status installed net-tools:amd64 2.10-0.1
2024-10-08 16:15:00 trigproc man-db:amd64 2.11.2-2 <none>
2024-10-08 16:15:00 status half-configured man-db:amd64 2.11.2-2
2024-10-08 16:15:01 status installed man-db:amd64 2.11.2-2

```

*Ilustración 4 05\_dpkg\_log\_instalaciones\_sospechosas*



*Ilustración 5 06\_apache\_access\_log\_wordpress*

# Sergio Maturana Mena

## ANÁLISIS FORENSE CON AUTOPSY

[Mon Sep 30 10:44:30.112562 2024] [mpm\_event:notice] [pid 35916:tid 35916] AH00489: Apache/2.4.62 (Debian) configured -- resuming normal operations  
[Mon Sep 30 10:44:30.112739 2024] [core:notice] [pid 35916:tid 35916] AH00094: Command line: '/usr/sbin/apache2'  
[Mon Sep 30 12:05:46.470124 2024] [mpm\_event:notice] [pid 35916:tid 35916] AH00492: caught SIGWINCH, shutting down gracefully  
[Mon Sep 30 12:05:46.807956 2024] [mpm\_event:notice] [pid 39748:tid 39748] AH00489: Apache/2.4.62 (Debian) configured -- resuming normal operations  
[Mon Sep 30 12:05:46.808161 2024] [core:notice] [pid 39748:tid 39748] AH00094: Command line: '/usr/sbin/apache2'  
[Mon Sep 30 12:14:27.686258 2024] [mpm\_event:notice] [pid 39748:tid 39748] AH00492: caught SIGWINCH, shutting down gracefully  
[Mon Sep 30 12:14:27.823038 2024] [mpm\_prefork:notice] [pid 50136:tid 50136] AH00163: Apache/2.4.62 (Debian) configured -- resuming normal operations  
[Mon Sep 30 12:14:27.823236 2024] [core:notice] [pid 50136:tid 50136] AH00094: Command line: '/usr/sbin/apache2'  
[Mon Sep 30 12:14:28.431284 2024] [mpm\_prefork:notice] [pid 50136:tid 50136] AH00170: caught SIGWINCH, shutting down gracefully  
[Mon Sep 30 12:14:29.230486 2024] [mpm\_prefork:notice] [pid 50176:tid 50176] AH00163: Apache/2.4.62 (Debian) configured -- resuming normal operations  
[Mon Sep 30 12:14:29.230579 2024] [core:notice] [pid 50176:tid 50176] AH00094: Command line: '/usr/sbin/apache2'  
[Mon Sep 30 12:19:00.906952 2024] [mpm\_prefork:notice] [pid 50176:tid 50176] AH00170: caught SIGWINCH, shutting down gracefully  
[Mon Sep 30 12:14:27.823236 2024] [mpm\_prefork:notice] [pid 50616:tid 50616] AH00163: Apache/2.4.62 (Debian) configured -- resuming normal operations  
[Mon Sep 30 12:19:01.320537 2024] [core:notice] [pid 50616:tid 50616] AH00094: Command line: '/usr/sbin/apache2'  
[Mon Sep 30 12:19:01.320607 2024] [core:notice] [pid 50616:tid 50616] AH00094: Command line: '/usr/sbin/apache2'  
[Mon Sep 30 12:27:50.914090 2024] [mpm\_prefork:notice] [pid 50616:tid 50616] AH00170: caught SIGWINCH, shutting down gracefully  
[Mon Sep 30 15:09:52.566780 2024] [mpm\_prefork:notice] [pid 608:tid 608] AH00163: Apache/2.4.62 (Debian) configured -- resuming normal operations  
[Mon Sep 30 15:09:52.570869 2024] [core:notice] [pid 608:tid 608] AH00094: Command line: '/usr/sbin/apache2'  
[Mon Sep 30 15:30:52.284974 2024] [mpm\_prefork:notice] [pid 608:tid 608] AH00170: caught SIGWINCH, shutting down gracefully  
[Mon Sep 30 15:30:52.519696 2024] [mpm\_prefork:notice] [pid 3044:tid 3044] AH00163: Apache/2.4.62 (Debian) configured -- resuming normal operations  
[Mon Sep 30 15:30:52.519824 2024] [core:notice] [pid 3044:tid 3044] AH00094: Command line: '/usr/sbin/apache2'  
[Mon Sep 30 15:32:42.452825 2024] [mpm\_prefork:notice] [pid 3044:tid 3044] AH00170: caught SIGWINCH, shutting down gracefully  
[Mon Sep 30 15:32:42.577995 2024] [mpm\_prefork:notice] [pid 3188:tid 3188] AH00163: Apache/2.4.62 (Debian) configured -- resuming normal operations  
[Mon Sep 30 15:32:42.578042 2024] [core:notice] [pid 3188:tid 3188] AH00094: Command line: '/usr/sbin/apache2'  
[Tue Oct 08 16:24:31.046216 2024] [mpm\_prefork:notice] [pid 3188:tid 3188] AH00170: caught SIGWINCH, shutting down gracefully  
[Tue Oct 08 16:24:31.238481 2024] [mpm\_prefork:notice] [pid 5990:tid 5990] AH00163: Apache/2.4.62 (Debian) configured -- resuming normal operations  
[Tue Oct 08 16:24:31.238544 2024] [core:notice] [pid 5990:tid 5990] AH00094: Command line: '/usr/sbin/apache2'  
[Tue Oct 08 16:43:19.045745 2024] [mpm\_prefork:notice] [pid 620:tid 620] AH00163: Apache/2.4.62 (Debian) configured -- resuming normal operations  
[Tue Oct 08 16:43:19.046757 2024] [core:notice] [pid 620:tid 620] AH00094: Command line: '/usr/sbin/apache2'  
[Tue Oct 08 16:48:03.446108 2024] [mpm\_prefork:notice] [pid 622:tid 622] AH00163: Apache/2.4.62 (Debian) configured -- resuming normal operations  
[Tue Oct 08 16:48:03.446734 2024] [core:notice] [pid 622:tid 622] AH00094: Command line: '/usr/sbin/apache2'  
[Tue Oct 08 17:28:38.662828 2024] [mpm\_prefork:notice] [pid 648:tid 648] AH00163: Apache/2.4.62 (Debian) configured -- resuming normal operations  
[Tue Oct 08 17:28:38.663646 2024] [core:notice] [pid 648:tid 648] AH00094: Command line: '/usr/sbin/apache2'

Ilustración 6 07\_apache\_error\_log

Listing													
/img_debian-disk001_copiar.vmdk/vol_vol2/var/www/html													
23 Results													
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	
[current folder]				2024-10-08 22:49:46 CEST	2024-10-08 22:49:46 CEST	2024-10-08 22:17:59 CEST	2024-09-30 16:44:18 CEST	4096	Allocated	Allocated	unknown	/img_debian-disk001_copiar.vmdk/vol_vol2/var/www/html	
[parent folder]				2024-09-30 16:44:18 CEST	2024-09-30 16:44:18 CEST	2024-09-30 16:44:10 CEST	2024-09-30 16:44:18 CEST	4096	Allocated	Allocated	unknown	/img_debian-disk001_copiar.vmdk/vol_vol2/var/www/html	
wp-admin				2024-09-10 17:23:18 CEST	2024-10-08 22:18:00 CEST	2024-10-08 22:18:00 CEST	2024-09-30 17:56:22 CEST	4096	Allocated	Allocated	unknown	/img_debian-disk001_copiar.vmdk/vol_vol2/var/www/html/wp-admin	
wp-content				2024-10-08 22:49:46 CEST	2024-10-08 22:49:46 CEST	2024-10-08 22:18:00 CEST	2024-09-30 17:56:21 CEST	4096	Allocated	Allocated	unknown	/img_debian-disk001_copiar.vmdk/vol_vol2/var/www/html/wp-content	
wp-includes				2024-09-10 17:23:20 CEST	2024-10-08 22:17:59 CEST	2024-10-08 22:17:59 CEST	2024-09-30 17:56:21 CEST	12288	Allocated	Allocated	unknown	/img_debian-disk001_copiar.vmdk/vol_vol2/var/www/html/wp-includes	
htaccess				2024-09-30 18:23:12 CEST	2024-10-08 22:18:00 CEST	2024-10-08 22:49:45 CEST	2024-09-30 18:23:12 CEST	523	Allocated	Allocated	unknown	/img_debian-disk001_copiar.vmdk/vol_vol2/var/www/html/htaccess	
index.html				2024-09-30 16:44:22 CEST	2024-10-08 22:18:00 CEST	2024-10-08 22:49:46 CEST	2024-09-30 16:44:22 CEST	10701	Allocated	Allocated	unknown	/img_debian-disk001_copiar.vmdk/vol_vol2/var/www/html/index.html	
index.php				2020-02-06 07:33:11 CET	2024-10-08 22:18:00 CEST	2024-09-30 18:23:12 CEST	2024-09-30 17:56:21 CEST	405	Allocated	Allocated	unknown	/img_debian-disk001_copiar.vmdk/vol_vol2/var/www/html/index.php	
license.txt				2024-01-01 01:00:19 CET	2024-10-08 22:17:59 CEST	2024-09-30 17:55:16 CEST	2024-09-30 17:56:21 CEST	19915	Allocated	Allocated	unknown	/img_debian-disk001_copiar.vmdk/vol_vol2/var/www/html/license.txt	
readme.html				2024-06-18 13:59:14 CEST	2024-10-08 22:18:00 CEST	2024-09-30 17:55:16 CEST	2024-09-30 17:56:21 CEST	7409	Allocated	Allocated	unknown	/img_debian-disk001_copiar.vmdk/vol_vol2/var/www/html/readme.html	
wp-activate.php				2024-02-13 15:19:09 CET	2024-10-08 22:18:00 CEST	2024-09-30 17:55:18 CEST	2024-09-30 17:56:22 CEST	7387	Allocated	Allocated	unknown	/img_debian-disk001_copiar.vmdk/vol_vol2/var/www/html/wp-activate.php	
wp-blog-header.php				2020-02-06 07:33:11 CET	2024-10-08 22:18:00 CEST	2024-09-30 18:23:12 CEST	2024-09-30 17:56:21 CEST	351	Allocated	Allocated	unknown	/img_debian-disk001_copiar.vmdk/vol_vol2/var/www/html/wp-blog-header.php	
wp-comments-post.php				2023-06-14 16:11:16 CEST	2024-10-08 22:18:00 CEST	2024-09-30 17:55:19 CEST	2024-09-30 17:56:22 CEST	2323	Allocated	Allocated	unknown	/img_debian-disk001_copiar.vmdk/vol_vol2/var/www/html/wp-comments-post.php	
wp-config.php				2024-09-30 18:02:41 CEST	2024-10-08 22:20:04 CEST	2024-10-08 22:49:45 CEST	2024-09-30 17:56:21 CEST	3017	Allocated	Allocated	unknown	/img_debian-disk001_copiar.vmdk/vol_vol2/var/www/html/wp-config.php	
wp-cron.php				2023-05-30 20:48:19 CEST	2024-10-08 22:18:00 CEST	2024-10-08 22:49:46 CEST	2024-09-30 17:56:21 CEST	5638	Allocated	Allocated	unknown	/img_debian-disk001_copiar.vmdk/vol_vol2/var/www/html/wp-cron.php	
wp-links-opml.php				2022-11-26 22:01:17 CET	2024-10-08 22:18:00 CEST	2024-09-30 17:55:17 CEST	2024-09-30 17:56:21 CEST	2502	Allocated	Allocated	unknown	/img_debian-disk001_copiar.vmdk/vol_vol2/var/www/html/wp-links-opml.php	
wp-load.php				2024-03-11 11:05:15 CET	2024-10-08 22:18:00 CEST	2024-10-08 22:49:45 CEST	2024-09-30 17:56:21 CEST	3937	Allocated	Allocated	unknown	/img_debian-disk001_copiar.vmdk/vol_vol2/var/www/html/wp-load.php	
wp-login.php				2024-05-28 13:13:12 CEST	2024-10-08 22:18:00 CEST	2024-10-08 18:23:27 CEST	2024-09-30 17:56:21 CEST	51238	Allocated	Allocated	unknown	/img_debian-disk001_copiar.vmdk/vol_vol2/var/www/html/wp-login.php	
wp-mail.php				2023-09-16 08:50:23 CEST	2024-10-08 22:18:00 CEST	2024-09-30 17:55:17 CEST	2024-09-30 17:56:21 CEST	8525	Allocated	Allocated	unknown	/img_debian-disk001_copiar.vmdk/vol_vol2/var/www/html/wp-mail.php	
wp-settings.php				2024-07-09 17:43:14 CEST	2024-10-08 22:18:00 CEST	2024-10-08 22:49:45 CEST	2024-09-30 17:56:21 CEST	28774	Allocated	Allocated	unknown	/img_debian-disk001_copiar.vmdk/vol_vol2/var/www/html/wp-settings.php	
wp-signup.php				2023-06-19 20:27:27 CEST	2024-10-08 22:18:00 CEST	2024-09-30 17:55:16 CEST	2024-09-30 17:56:21 CEST	34385	Allocated	Allocated	unknown	/img_debian-disk001_copiar.vmdk/vol_vol2/var/www/html/wp-signup.php	
wp-trackback.php				2023-06-22 16:36:26 CEST	2024-10-08 22:18:00 CEST	2024-09-30 17:55:19 CEST	2024-09-30 17:56:22 CEST	4885	Allocated	Allocated	unknown	/img_debian-disk001_copiar.vmdk/vol_vol2/var/www/html/wp-trackback.php	
xmlrpc.php				2024-03-02 14:49:06 CET	2024-10-08 22:17:59 CEST	2024-09-30 17:55:16 CEST	2024-09-30 17:56:21 CEST	3246	Allocated	Allocated	unknown	/img_debian-disk001_copiar.vmdk/vol_vol2/var/www/html/xmlrpc.php	

Ilustración 7 09\_var\_www\_html\_estructura

Listing													
/img_debian-disk001_copiar.vmdk/vol_vol2/var/www/html/wp-content/uploads													
3 Results													
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	
[current folder]				2024-09-30 18:23:13 CEST	2024-10-08 22:18:00 CEST	2024-10-08 22:18:00 CEST	2024-09-30 18:23:13 CEST	4096	Allocated	Allocated	unknown	/img_debian-disk001_copiar.vmdk/vol_vol2/var/www/html/wp-content/uploads	
[parent folder]				2024-10-08 22:49:46 CEST	2024-10-08 22:49:46 CEST	2024-10-08 22:18:00 CEST	2024-09-30 17:56:21 CEST	4096	Allocated	Allocated	unknown	/img_debian-disk001_copiar.vmdk/vol_vol2/var/www/html/wp-content/uploads	
2024				2024-10-08 22:49:46 CEST	2024-10-08 22:49:46 CEST	2024-10-08 22:18:00 CEST	2024-09-30 18:23:13 CEST	4096	Allocated	Allocated	unknown	/img_debian-disk001_copiar.vmdk/vol_vol2/var/www/html/wp-content/uploads/2024	

Ilustración 8 10\_wordpress\_uploads\_sospechosos

Listing													
/img_debian-disk001_copiar.vmdk/vol_vol2/var/www/html/wp-content/themes													
6 Results													
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	
index.php				2014-06-05 17:59:14 CEST	2024-10-08 22:18:00 CEST	2024-09-30 17:55:17 CEST	2024-09-30 17:56:21 CEST	28	Allocated	Allocated	unknown	/img_debian-disk001_copiar.vmdk/vol_vol2/var/www/html/wp-content/themes/index.php	
twentytwentyfour				2024-09-10 17:23:19 CEST	2024-10-08 22:18:00 CEST	2024-10-08 22:18:00 CEST	2024-09-30 17:56:21 CEST	4096	Allocated	Allocated	unknown	/img_debian-disk001_copiar.vmdk/vol_vol2/var/www/html/wp-content/themes/twentytwentyfour	
twentytwentythree				2024-09-10 17:23:19 CEST	2024-10-08 22:18:00 CEST	2024-10-08 22:18:00 CEST	2024-09-30 17:56:21 CEST	4096	Allocated	Allocated	unknown	/img_debian-disk001_copiar.vmdk/vol_vol2/var/www/html/wp-content/themes/twentytwentythree	
twentytwentytwo				2024-09-10 17:23:19 CEST	2024-10-08 22:18:00 CEST	2024-10-08 22:18:00 CEST	2024-09-30 17:56:21 CEST	4096	Allocated	Allocated	unknown	/img_debian-disk001_copiar.vmdk/vol_vol2/var/www/html/wp-content/themes/twentytwentytwo	
[current folder]				2024-09-10 17:23:21 CEST	2024-10-08 22:49:46 CEST	2024-09-30 17:55:16 CEST	2024-09-30 17:56:21 CEST	4096	Allocated	Allocated	unknown	/img_debian-disk001_copiar.vmdk/vol_vol2/var/www/html/wp-content/themes	
[parent folder]				2024-10-08 22:49:46 CEST	2024-10-08 22:49:46 CEST	2024-10-08 22:18:00 CEST	2024-09-30 17:56:21 CEST	4096	Allocated	Allocated	unknown	/img_debian-disk001_copiar.vmdk/vol_vol2/var/www/html/wp-content/themes	

Ilustración 9 11\_wordpress\_themes

Sergio Maturana Mena

## ANÁLISIS FORENSE CON AUTOPSY

Listing										
/img_debian-disk001_copiar.vmdk/vol_vol2/tmp										
Table Thumbnail Summary										
13 Results										
Save Table as CSV										
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
[parent folder]				2024-09-30 16:35:23 CEST	2024-09-30 16:35:23 CEST	2024-09-30 16:35:24 CEST	2024-07-31 18:13:37 CEST	4096	Allocated	Allocated
font-unix				2024-10-08 23:28:36 CEST	2024-10-08 23:28:36 CEST	2024-10-08 23:28:36 CEST	2024-10-08 23:28:36 CEST	4096	Allocated	Allocated
XIM-unix				2024-10-08 23:28:36 CEST	2024-10-08 23:28:36 CEST	2024-10-08 23:28:36 CEST	2024-10-08 23:28:36 CEST	4096	Allocated	Allocated
systemd-private-af0a79f76920440c8e08594d654744				2024-10-08 23:28:37 CEST	2024-10-08 23:28:37 CEST	2024-10-08 23:28:37 CEST	2024-10-08 23:28:37 CEST	4096	Allocated	Allocated
systemd-private-af0a79f76920440c8e08594d654744				2024-10-08 23:28:37 CEST	2024-10-08 23:28:37 CEST	2024-10-08 23:28:37 CEST	2024-10-08 23:28:37 CEST	4096	Allocated	Allocated
systemd-private-af0a79f76920440c8e08594d654744				2024-10-08 23:28:37 CEST	2024-10-08 23:28:37 CEST	2024-10-08 23:28:37 CEST	2024-10-08 23:28:37 CEST	4096	Allocated	Allocated
systemd-private-af0a79f76920440c8e08594d654744				2024-10-08 23:28:37 CEST	2024-10-08 23:28:37 CEST	2024-10-08 23:28:37 CEST	2024-10-08 23:28:37 CEST	4096	Allocated	Allocated
X11-unix				2024-10-08 23:28:38 CEST	2024-10-08 23:28:38 CEST	2024-10-08 23:28:38 CEST	2024-10-08 23:28:38 CEST	4096	Allocated	Allocated
X0-lock				2024-10-08 23:28:38 CEST	2024-10-08 23:28:38 CEST	2024-10-08 23:28:38 CEST	2024-10-08 23:28:38 CEST	11	Allocated	Allocated
JCE-unix				2024-10-08 23:28:54 CEST	2024-10-08 23:28:54 CEST	2024-10-08 23:28:54 CEST	2024-10-08 23:28:54 CEST	4096	Allocated	Allocated
ssh-X0000XGZYLks				2024-10-08 23:28:54 CEST	2024-10-08 23:28:54 CEST	2024-10-08 23:28:54 CEST	2024-10-08 23:28:54 CEST	4096	Allocated	Allocated
systemd-private-af0a79f76920440c8e08594d654744				2024-10-08 23:28:56 CEST	2024-10-08 23:28:56 CEST	2024-10-08 23:28:56 CEST	2024-10-08 23:28:56 CEST	4096	Allocated	Allocated
[current folder]				2024-10-08 23:39:27 CEST	2024-10-08 23:39:27 CEST	2024-10-08 23:39:28 CEST	2024-07-31 18:13:51 CEST	4096	Allocated	Allocated

Ilustración 10 12\_tmp\_archivos\_sospechosos

/img\_debian-disk001\_copiar.vmdk/vol\_vol2/etc/passwd - Editor

/img\_debian-disk001\_copiar.vmdk/vol\_vol2/etc/passwd x

HexTextApplicationFile MetadataOS AccountData ArtifactsAnalysis ResultsContextAnnotationsOther Occurrences

StringsExtracted TextTranslation

Page: 1 of - PageMatches on page: - of - Match100%Reset

root:x:0:0:root:/root:/bin/bash  
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin  
bin:x:2:2:bin:/bin:/usr/sbin/nologin  
sys:x:3:3:sys:/dev:/usr/sbin/nologin  
sync:x:4:65534:sync:/bin:/bin/sync  
games:x:5:60:games:/usr/games:/usr/sbin/nologin  
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin  
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin  
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin  
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin  
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin  
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin  
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin  
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin  
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin  
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin  
\_apt:x:42:65534:/:nonexistent:/usr/sbin/nologin  
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin  
systemd-network:x:998:998:systemd Network Management:/:usr/sbin/nologin  
systemd-timesync:x:997:997:systemd Time Synchronization:/:usr/sbin/nologin  
messagebus:x:100:107:/:nonexistent:/usr/sbin/nologin  
avahi-autoipd:x:101:110:Avahi autoip daemon,,:/var/lib/avahi-autoipd:/usr/sbin/nologin  
usbmux:x:102:46:usbmux daemon,,:/var/lib/usbmux:/usr/sbin/nologin  
dnsmasq:x:103:65534:dnsmasq,,:/var/lib/misc:/usr/sbin/nologin  
avahi:x:104:112:Avahi mDNS daemon,,:/run/avahi-daemon:/usr/sbin/nologin  
speech-dispatcher:x:105:29:Speech Dispatcher,,:/run/speech-dispatcher:/bin/false  
pulse:x:106:114:PulseAudio daemon,,:/run/pulse:/usr/sbin/nologin  
saned:x:107:117:/:/var/lib/saned:/usr/sbin/nologin  
lightdm:x:108:118:Light Display Manager:/var/lib/lightdm:/bin/false  
polkitd:x:996:996:polkit:/nonexistent:/usr/sbin/nologin  
rtkit:x:109:119:RealtimeKit,,:/proc:/usr/sbin/nologin  
colord:x:110:120:colord colour management daemon,,:/var/lib/colord:/usr/sbin/nologin  
debian:x:1000:1000:4geeks,,:/home/debian:/bin/bash  
mysql:x:111:121:MySQL Server,,:/nonexistent:/bin/false  
sshd:x:112:65534:/:run/ssh:/usr/sbin/nologin  
ftp:x:113:122:ftp daemon,,:/srv/ftp:/usr/sbin/nologin

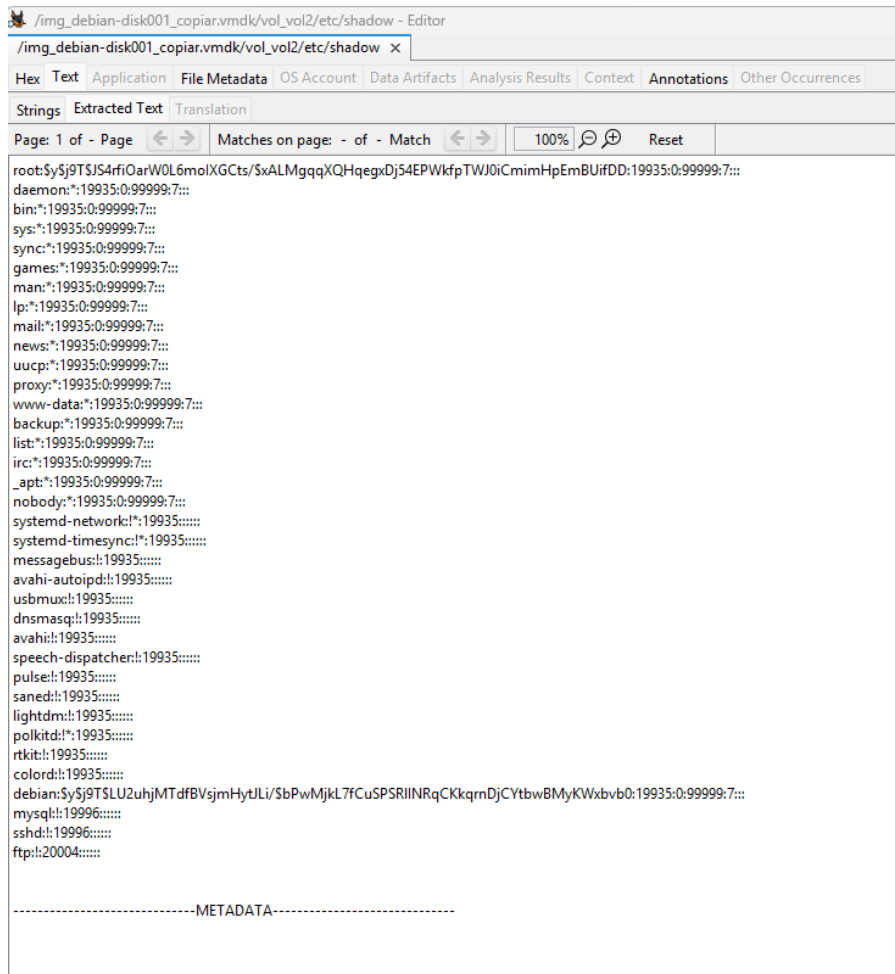
-----METADATA-----

Ilustración 11 14\_etc\_passwd\_usuarios



## Sergio Maturana Mena

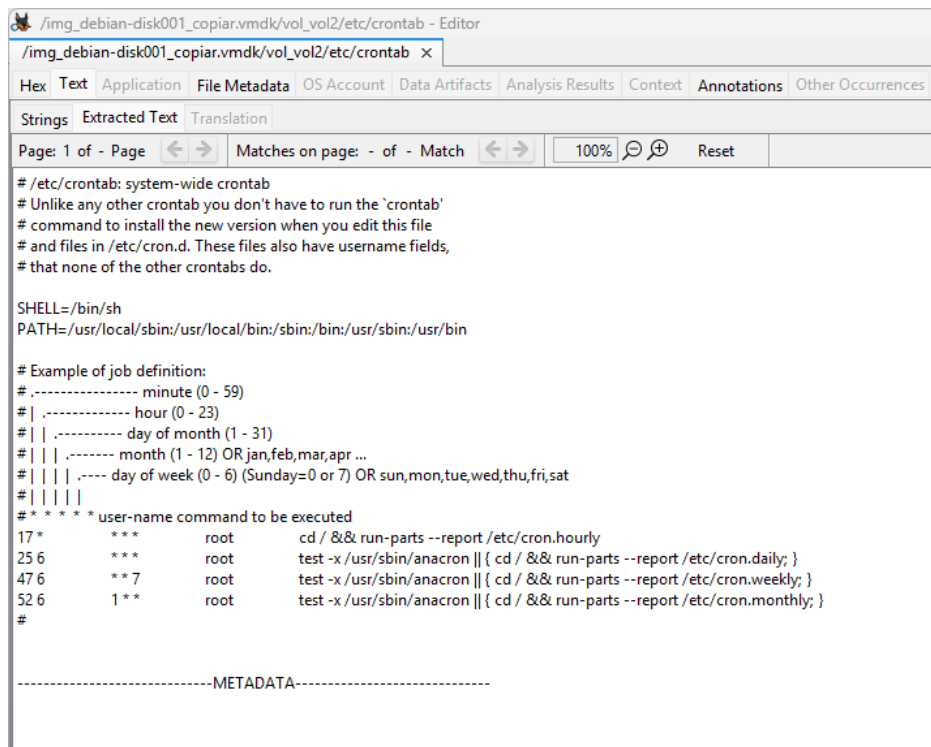
### ANÁLISIS FORENSE CON AUTOPSY



```
root:$y$9T$JS4rfiOarW0L6molXGCts/$xALMgqqXQHqegxDj54EPWkfpTWJ0iCmimHpEmBUIfDD:19935:0:99999:7:::
daemon:*:19935:0:99999:7:::
bin:*:19935:0:99999:7:::
sys:*:19935:0:99999:7:::
sync:*:19935:0:99999:7:::
games:*:19935:0:99999:7:::
man:*:19935:0:99999:7:::
lp:*:19935:0:99999:7:::
mail:*:19935:0:99999:7:::
news:*:19935:0:99999:7:::
uucp:*:19935:0:99999:7:::
proxy:*:19935:0:99999:7:::
www-data:*:19935:0:99999:7:::
backup:*:19935:0:99999:7:::
list:*:19935:0:99999:7:::
irc:*:19935:0:99999:7:::
_apt:*:19935:0:99999:7:::
nobody:*:19935:0:99999:7:::
systemd-network:*:19935:::
systemd-timesync:*:19935:::
messagebus:*:19935:::
avahi-autoipd:*:19935:::
usbmux:*:19935:::
dnsmasq:*:19935:::
avahi:*:19935:::
speech-dispatcher:*:19935:::
pulse:*:19935:::
saned:*:19935:::
lightdm:*:19935:::
polkitd:*:19935:::
rtkit:*:19935:::
colord:*:19935:::
debian:$y$9T$LU2uhjMTdfBVsjmHytLi/$bPwMjkl7FcCuSPSRlINRqCKkqrmDjCYtbwBMyKWxbvb0:19935:0:99999:7:::
mysql:*:19996:::
sshd:*:19996:::
ftp:*:20004:::
```

-----METADATA-----

Ilustración 12 15\_etc\_shadow



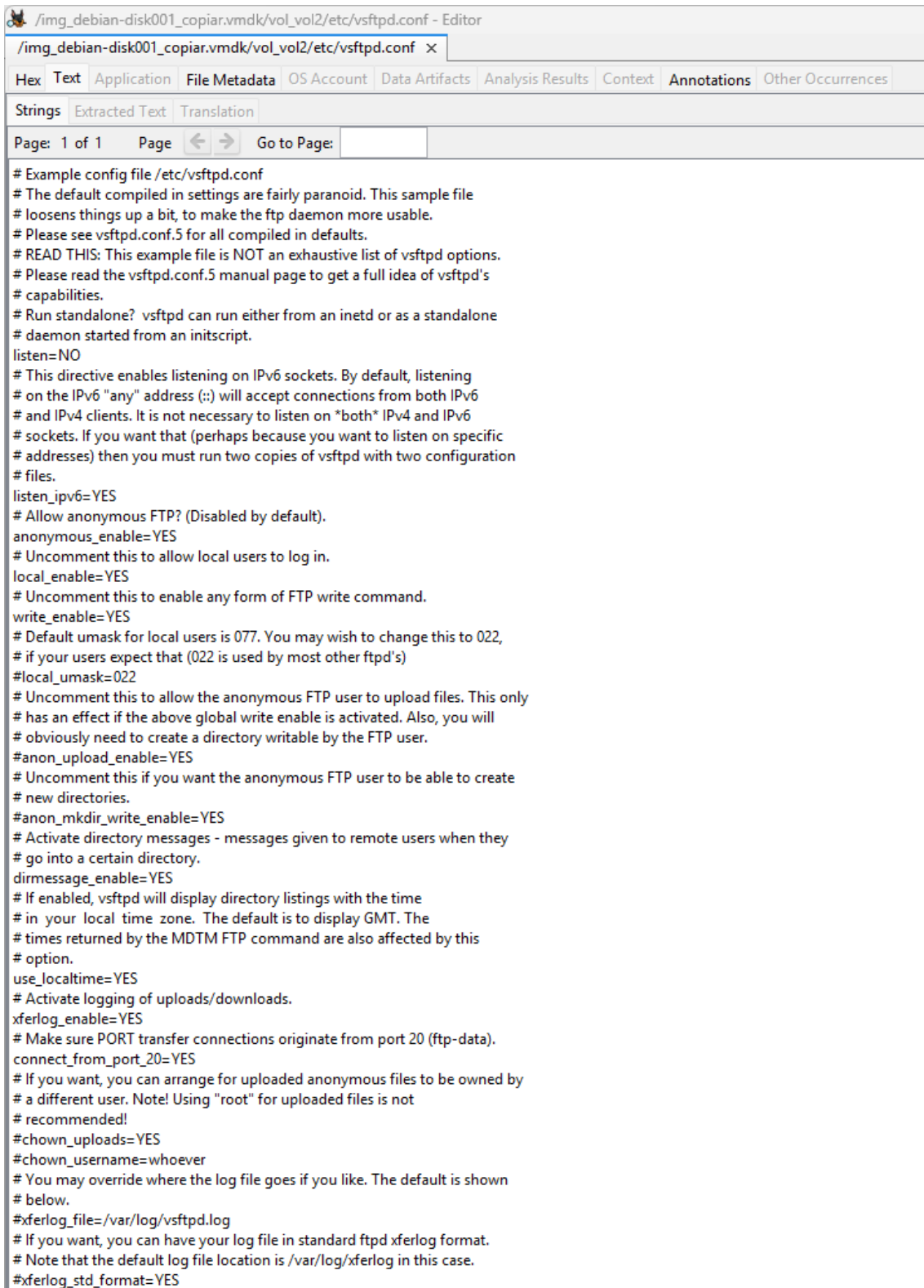
```
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .----- minute (0 - 59)
# | .----- hour (0 - 23)
# | | .----- day of month (1 - 31)
# | | | .----- month (1 - 12) OR jan,feb,mar,apr ...
# | | | | .----- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# | | | |
# * * * * * user-name command to be executed
17 * * * * root cd / && run-parts --report /etc/cron.hourly
25 6 * * * root test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.daily; }
47 6 * * 7 root test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.weekly; }
52 6 1 * * root test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.monthly; }
#
```

-----METADATA-----

Ilustración 13 16\_etc\_crontab\_persistencia



```
# Example config file /etc/vsftpd.conf
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
# Run standalone? vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=NO
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on "both" IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=YES
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=YES
# Uncomment this to allow local users to log in.
local_enable=YES
# Uncomment this to enable any form of FTP write command.
write_enable=YES
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
#local_umask=022
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the FTP user.
#anon_upload_enable=YES
# Uncomment this if you want the anonymous FTP user to be able to create
# new directories.
#anon_mkdir_write_enable=YES
# Activate directory messages - messages given to remote users when they
# go into a certain directory.
dirmessage_enable=YES
# If enabled, vsftpd will display directory listings with the time
# in your local time zone. The default is to display GMT. The
# times returned by the MDTM FTP command are also affected by this
# option.
use_localtime=YES
# Activate logging of uploads/downloads.
xferlog_enable=YES
# Make sure PORT transfer connections originate from port 20 (ftp-data).
connect_from_port_20=YES
# If you want, you can arrange for uploaded anonymous files to be owned by
# a different user. Note! Using "root" for uploaded files is not
# recommended!
#chown_uploads=YES
#chown_username=whoever
# You may override where the log file goes if you like. The default is shown
# below.
#xferlog_file=/var/log/vsftpd.log
# If you want, you can have your log file in standard ftpd xferlog format.
# Note that the default log file location is /var/log/xferlog in this case.
#xferlog_std_format=YES
```

*Ilustración 14 19\_vsftpd\_configuracion*

Sergio Maturana Mena  
ANÁLISIS FORENSE CON AUTOPSY



The screenshot shows the Autopsy forensic tool interface. The top bar indicates the file path: `/img_debian-disk001_copiar.vmdk/vol_vol2/etc/ssh/sshd_config`. Below the toolbar, the 'Text' tab is selected, displaying the contents of the `sshd_config` file. The interface includes a search bar at the top with 'Matches on page: - of - Match' and a 'Reset' button. The file content is displayed in a monospaced font, showing various configuration options and their default values, such as `Port 22`, `AddressFamily any`, `ListenAddress 0.0.0.0`, and `HostKey` paths. The configuration is commented out with `#` symbols.

```
# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/bin:/usr/games

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2

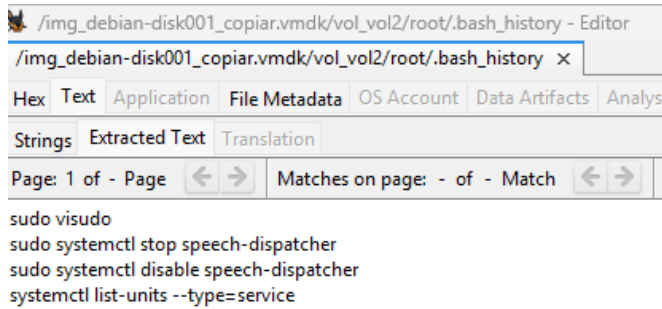
#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication yes
```

*Ilustración 15 20\_ssh\_configuracion*



/img\_debian-disk001\_copiar.vmdk/vol\_vol2/root/.bash\_history - Editor

/img\_debian-disk001\_copiar.vmdk/vol\_vol2/root/.bash\_history x

Hex Text Application File Metadata OS Account Data Artifacts Analysis

Strings Extracted Text Translation

Page: 1 of - Page < > Matches on page: - of - Match < >

```
sudo visudo
sudo systemctl stop speech-dispatcher
sudo systemctl disable speech-dispatcher
systemctl list-units --type=service
```

-----METADATA-----

Ilustración 16 24\_root\_bash\_history



/img\_debian-disk001\_copiar.vmdk/vol\_vol2/home/debian/.bash\_history - Editor

/img\_debian-disk001\_copiar.vmdk/vol\_vol2/home/debian/.bash\_history x

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Strings Extracted Text Translation

Page: 1 of - Page < > Matches on page: - of - Match < > 100% ⌕ ⊕ Reset

```
sudo systemctl stop speech-dispatcher
sudo usermood -aG root debian
pwd
sudo usermood -aG sudo debian
whoami
sudo visudo
su
sudo rmod speakup
sudo rmmmod speakup
sudo rmmmod speakup_soft
sudo apt-get remove speakup
sudo apt-get remove speakup_soft
sudo ls /etc
sudo ls /etc/modprobe.d/
sudo nano /etc/modprobe.d/blacklist-speakup.conf
sudo nano /etc/default/grub
sudo update-grub
sudo reboot
dpkg -l | grep -i speech
sudo apt-get remove speech
dpkg -l | grep -i voice
dpkg -l | grep -i espeak
sudo apt-get remove espeak
sudo apt-get remove espeakup
sudo apt-get remove libespeak
sudo nano /etc/modprobe.d/blacklist-speakup.conf
dpkg -l | grep -i festival
dpkg -l | grep -i espeakup
sudo apt-get remove espeakup
sudo systemctl disable espeakup
sv-inst
sudo systemd-sysv-install disable espeakup
sudo /lib/systemd/systemd-sysv-install disable espeakup
sudo service espeakup stop
sudo systemctl status espeakup
sudo apt-get install git
git --version
pwd
ls
sudo apt update && sudo apt upgrade -y
sudo apt install apache2 -y
sudo systemctl enable apache2
sudo systemctl start apache2
sudo systemctl status apache2
sudo apt install mysql-server php php-mysqli -y
sudo apt install mariadb-server -y
sudo systemctl start maria-db
sudo apt install mariadb-server
sudo systemctl start mariadb-server
sudo systemctl start mariadb
sudo systemctl enable mariadb
sudo mysql_secure_installation
sudo mysql -u root -p
cd /tmp
curl -O https://wordpress.org/latest.tar.gz
sudo apt install curl
```

Ilustración 17 25-1\_debian\_bash\_history



Sergio Maturana Mena  
ANÁLISIS FORENSE CON AUTOPSY



The screenshot shows the Autopsy interface with the file `/img_debian-disk001_copiar.vmdk/vol_vol2/home/debian/.bash_history` open in the Editor. The interface includes a top menu bar with tabs like Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences. Below the menu is a toolbar with buttons for Strings, Extracted Text, and Translation. The main area displays the content of the `.bash_history` file, which contains a series of terminal commands. At the bottom of the file content, there is a line indicating the start of the metadata section: `-----METADATA-----`.

```
/img_debian-disk001_copiar.vmdk/vol_vol2/home/debian/.bash_history
sudo apt-get remove nbspeakup
sudo nano /etc/modprobe.d/blacklist-speakup.conf
dpkg -l | grep -i festival
dpkg -l | grep -i espeakup
sudo apt-get remove espeakup
sudo systemctl disable espeakup
sv-inst
sudo systemd-sysv-install disable espeakup
sudo /lib/systemd/systemd-sysv-install disable espeakup
sudo service espeakup stop
sudo systemctl status espeakup
sudo apt-get install git
git --version
pwd
ls
sudo apt update && sudo apt upgrade -y
sudo apt install apache2 -y
sudo systemctl enable apache2
sudo systemctl start apache2
sudo systemctl status apache2
sudo apt install mysql-server php php-mysqli -y
sudo apt install mariadb-server -y
sudo systemctl start maria-db
sudo apt install mariadb-server
sudo systemctl start mariadb-server
sudo systemctl start mariadb
sudo systemctl enable mariadb
sudo mysql_secure_installation
sudo mysql -u root -p
cd /tmp
curl -O https://wordpress.org/latest.tar.gz
sudo apt install curl
curl -O https://wordpress.org/latest.tar.gz
tar xzvf latest.tar.gz
sudo cp -a /tmp/wordpress/. /var/www/html/
sudo chown -R www-data:www-data /var/www/html/
sudo chmod -R 755 /var/www/html/
cd /var/www/html/
sudo mv wp-config-sample.php wp-config.php
sudo nano wp-config.php
ip a
sudo systemctl restart apache2
sudo systemctl status apache2
sudo apt install php libapache2-mod-php php-mysqli php-gd php-xml php-mbstring php-curl -y
cd ..
sudo nano /etc/apache2/sites-available/000-default.conf
sudo systemctl restart apache2
sudo nano /var/www/html/info.php
ls /var/www/html
sudo apt install openssh-server -y
sudo systemctl start ssh
sudo systemctl enable ssh
sudo systemctl status ssh
sudo systemctl start apache2

-----METADATA-----
```

Ilustración 18 25-2\_debian\_bash\_history