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

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 privilegado 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:
  - 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 CríticoArchivo: 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 forcé

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)

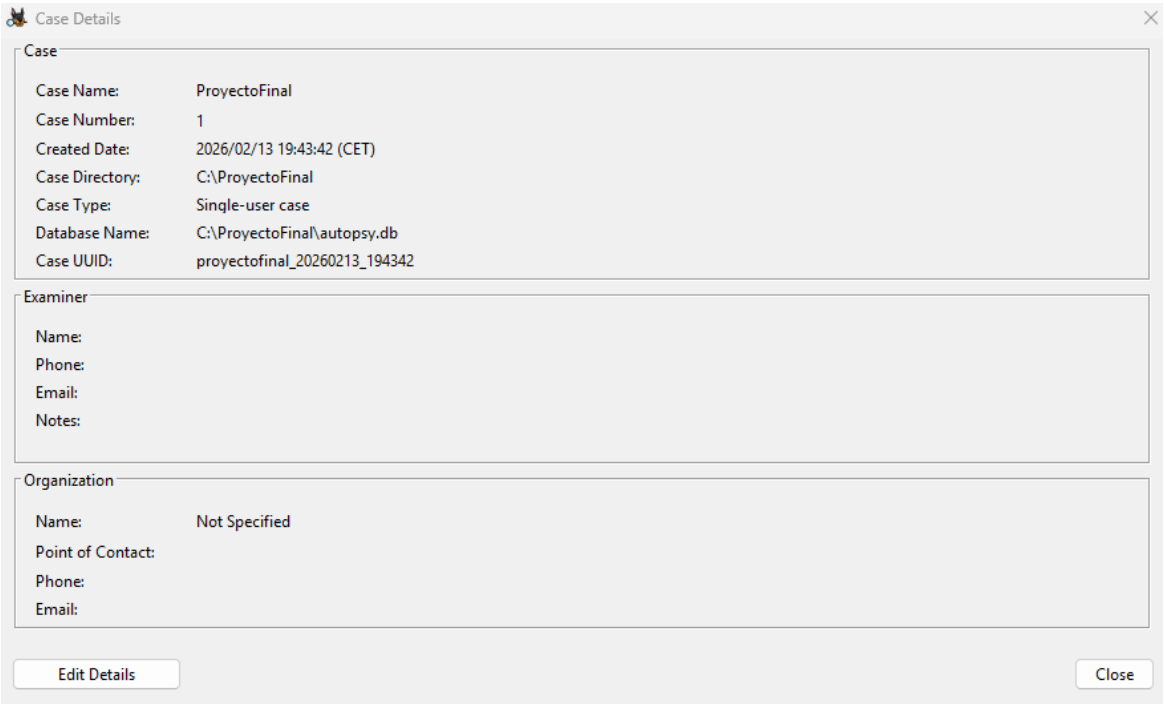

Ilustración 1 01_caso_informacion

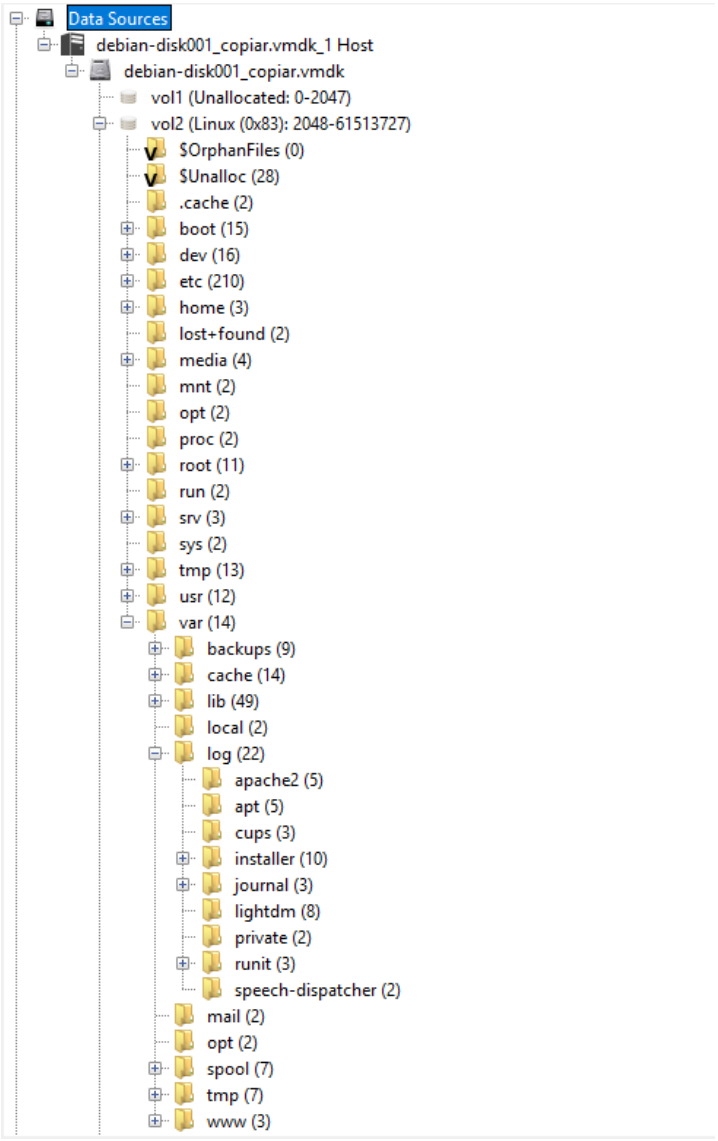

Ilustración 2 02_data_source_estructura

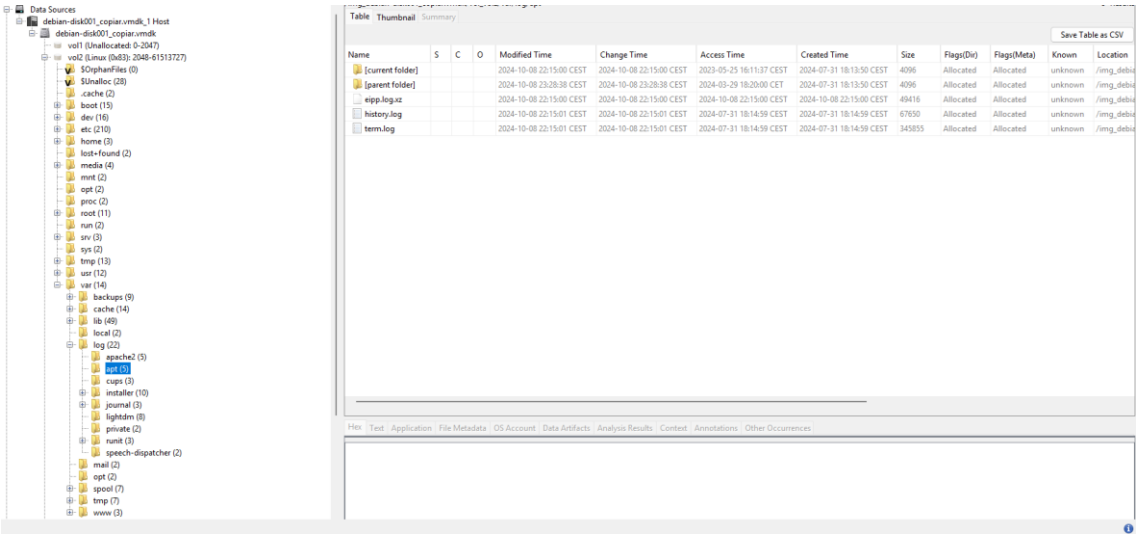

Ilustración 3 04_var_log_overview

```
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 openssh-sftp-server:amd64 <none> 1:9.2p1-2+deb12u3
2024-09-30 12:25:12 status half-installed openssh-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 openssh-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 install openssh-server:amd64 <none> 1:9.2p1-2+deb12u3
2024-09-30 12:25:12 status half-installed openssh-server:amd64 1:9.2p1-2+deb12u3
2024-09-30 12:25:13 status unpacked openssh-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 openssh-sftp-server:amd64 1:9.2p1-2+deb12u3 <none>
2024-09-30 12:25:13 status unpacked openssh-sftp-server:amd64 1:9.2p1-2+deb12u3
2024-09-30 12:25:13 status half-configured openssh-sftp-server:amd64 1:9.2p1-2+deb12u3
2024-09-30 12:25:13 status installed openssh-sftp-server:amd64 1:9.2p1-2+deb12u3
2024-09-30 12:25:13 configure openssh-server:amd64 1:9.2p1-2+deb12u3 <none>
2024-09-30 12:25:13 status unpacked openssh-server:amd64 1:9.2p1-2+deb12u3
2024-09-30 12:25:13 status half-configured openssh-server:amd64 1:9.2p1-2+deb12u3
2024-09-30 12:25:16 status installed openssh-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

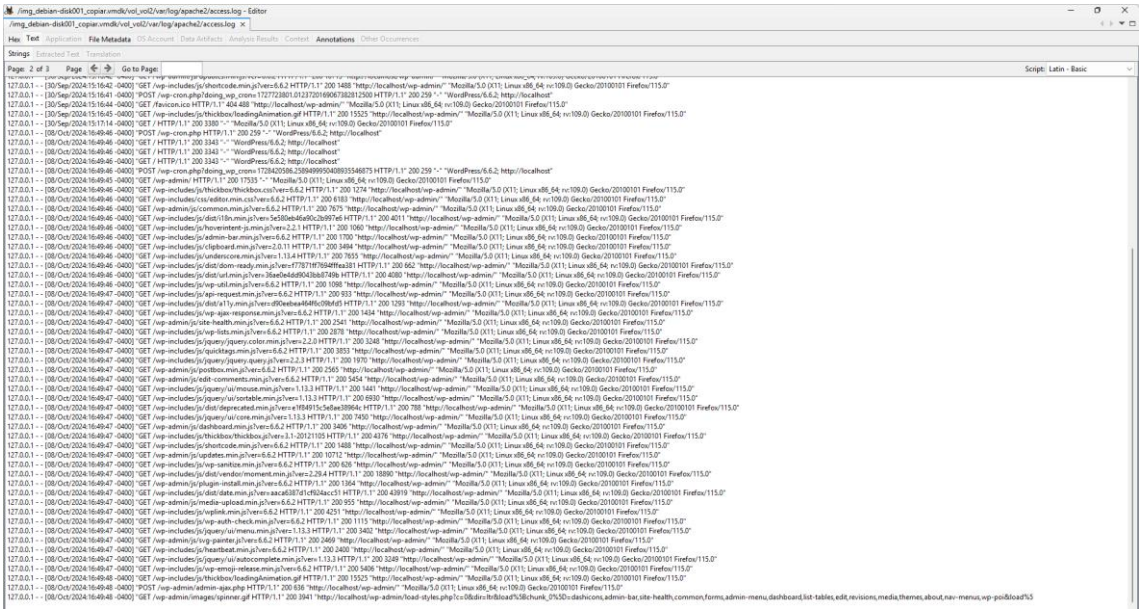

Ilustración 5 06_apache_access_log_wordpress

```
[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 12:19:01.320537 2024] [mpm_prefork:notice] [pid 50616:tid 50616] AH00163: Apache/2.4.62 (Debian) configured -- resuming normal operations
[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

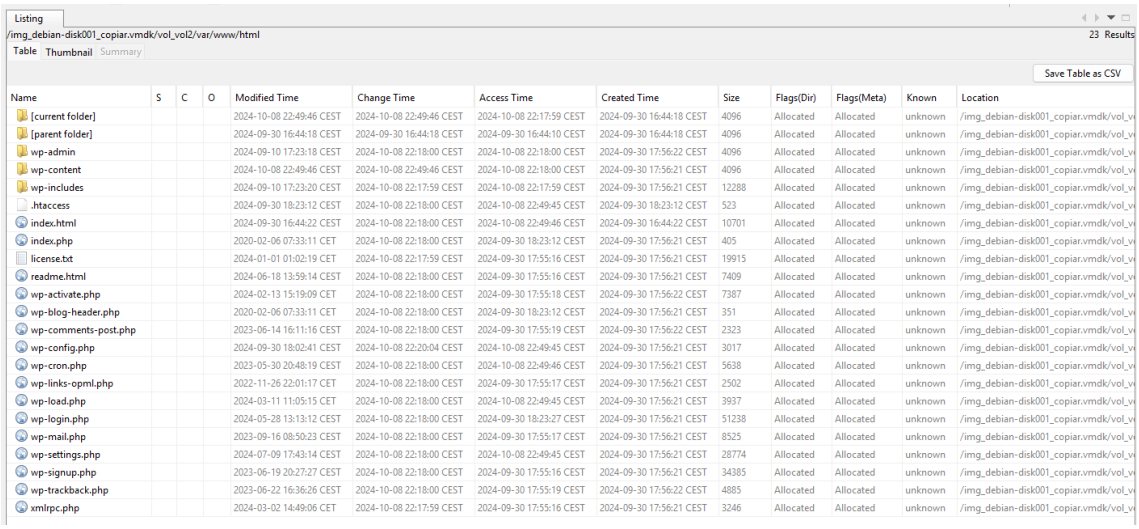

Ilustración 7 09_var_www_html_estructura

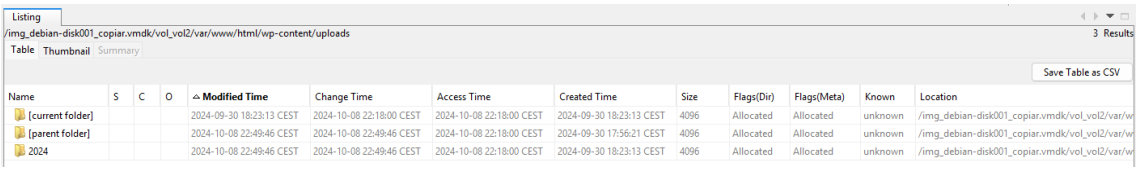

Ilustración 8 10_wordpress_uploads_sospechosos

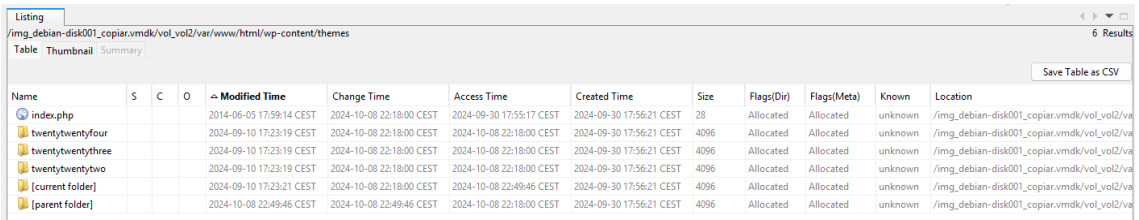

Ilustración 9 11_wordpress_themes

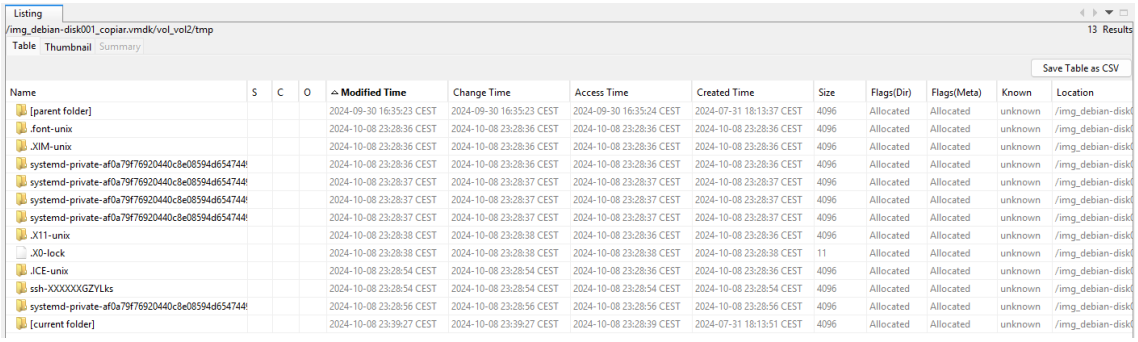

Ilustración 10 12_tmp_archivos_sospechosos

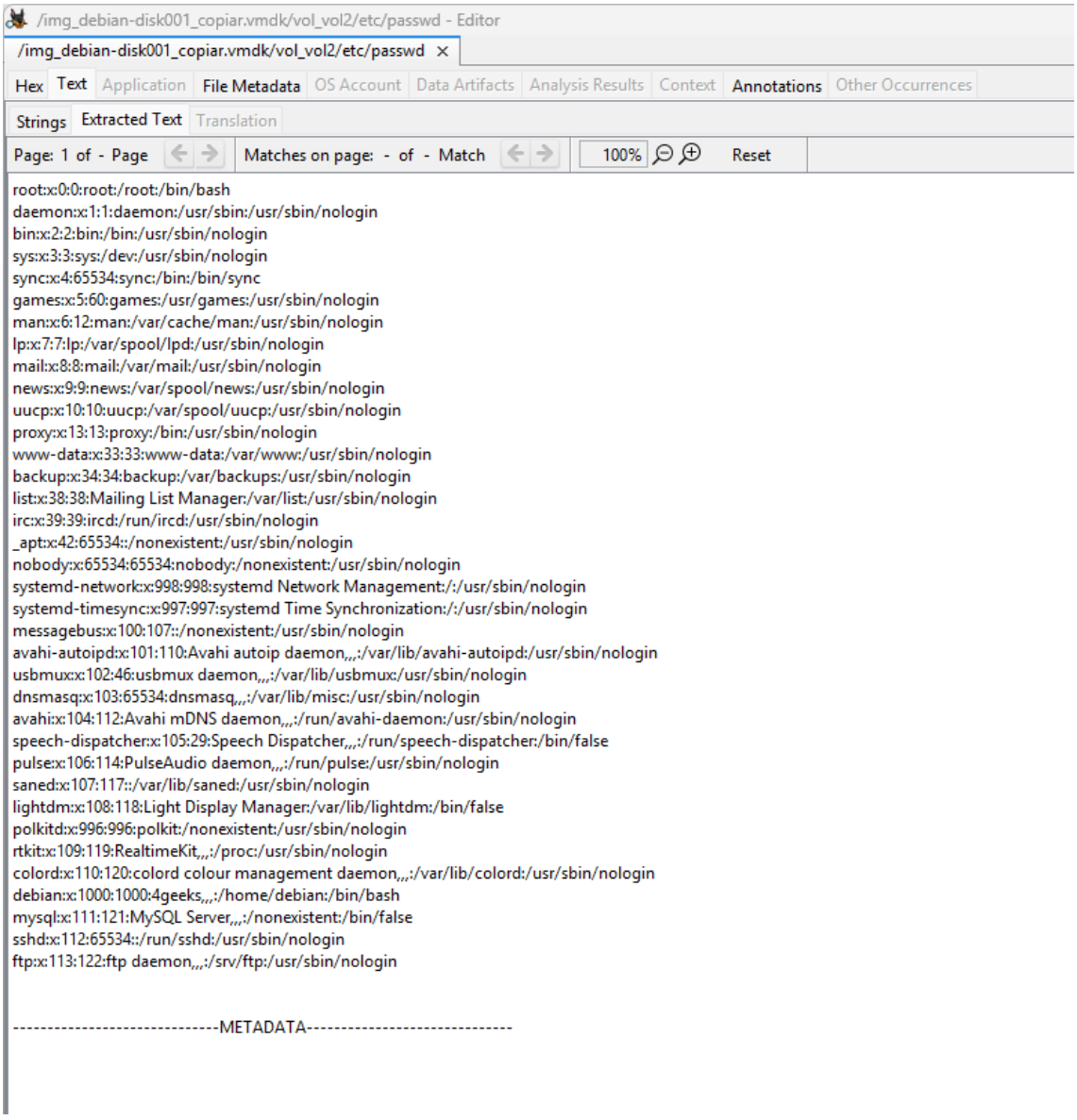

Ilustración 11 14_etc_passwd_usuarios

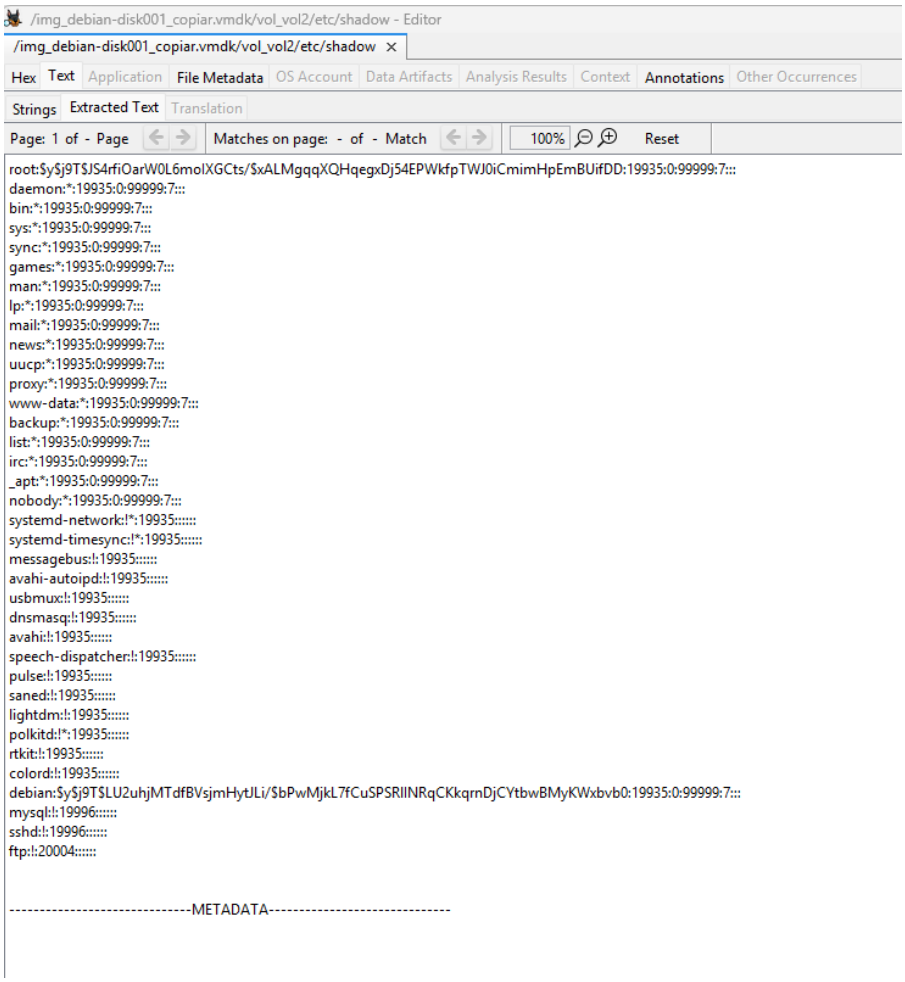

Ilustración 12 15_etc_shadow

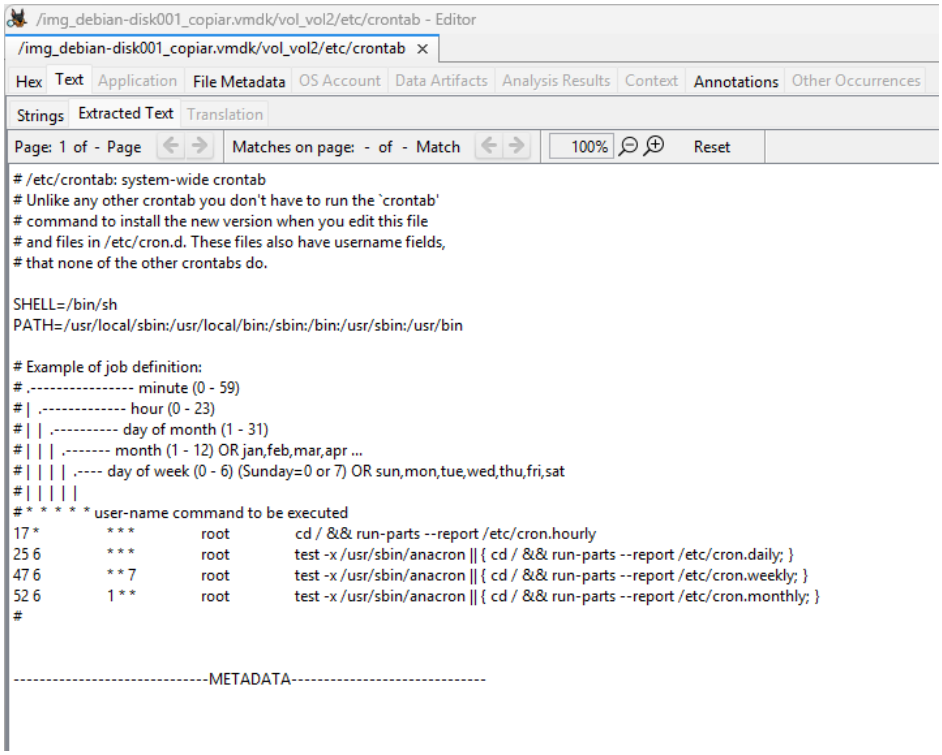

Ilustración 13 16_etc_crontab_persistencia

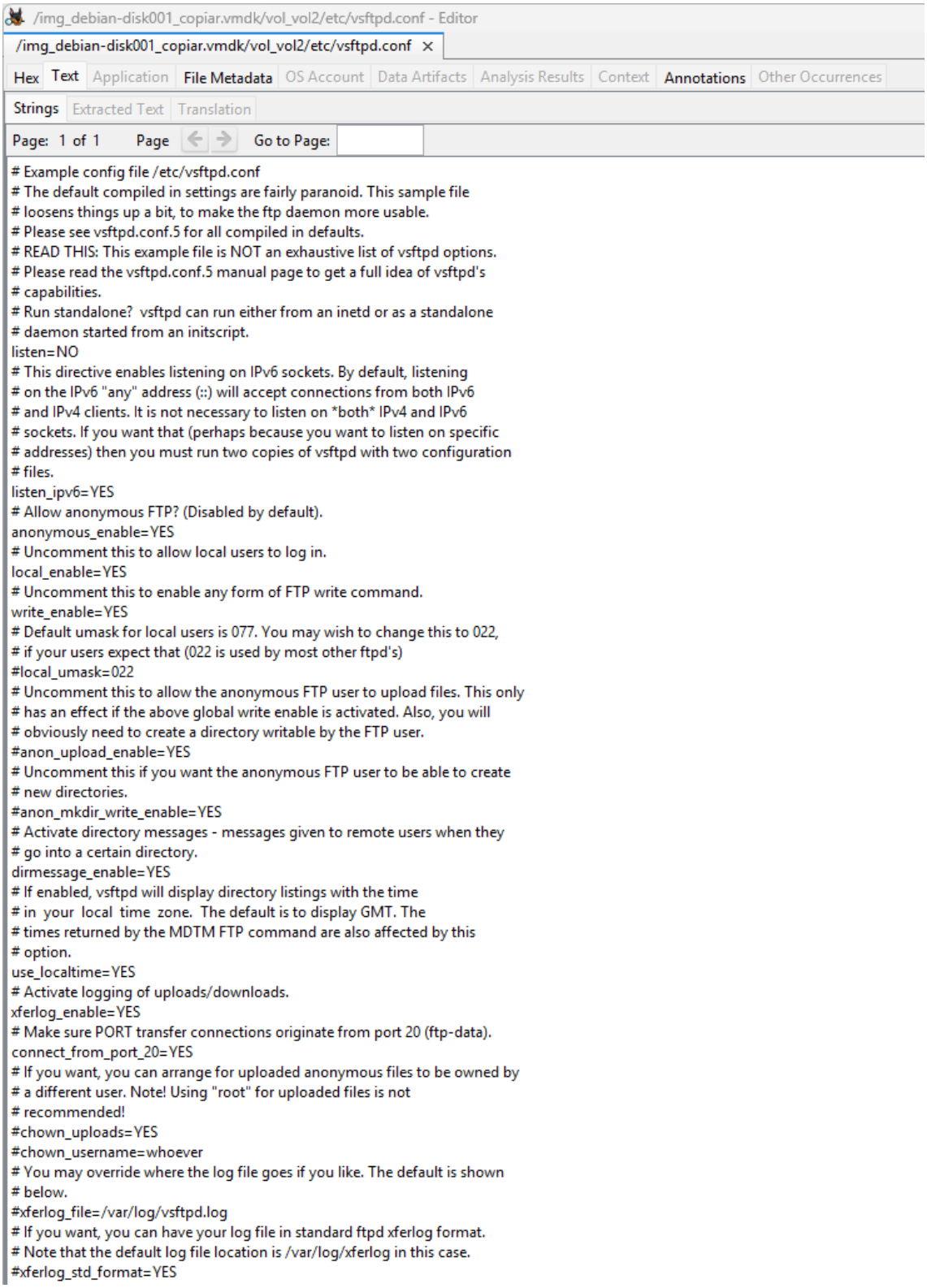

Ilustración 14 19_vsftpd_configuracion

Ilustración 15 20_ssh_configuracion

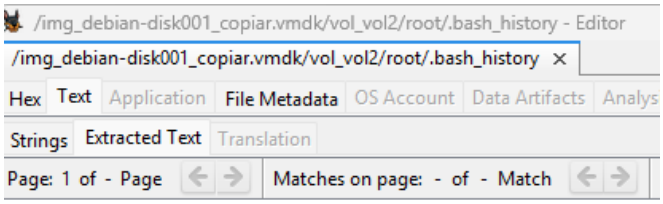

Ilustración 16 24_root_bash_history

Ilustración 17 25-1_debian_bash_history

Ilustración 18 25-2_debian_bash_history