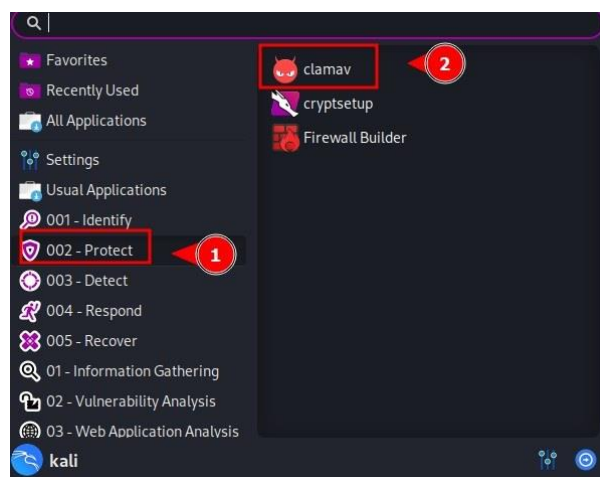


# ANTIVIRUS CLAMAV

## ¿Qué es ClamAV?

**ClamAV** es un software **antivirus de código abierto**, ampliamente utilizado para detectar troyanos, virus, malware y otras amenazas en sistemas Unix-like, incluyendo Linux, BSD y macOS. Se puede encontrar por **defecto** en **Kali Linux Purple**.



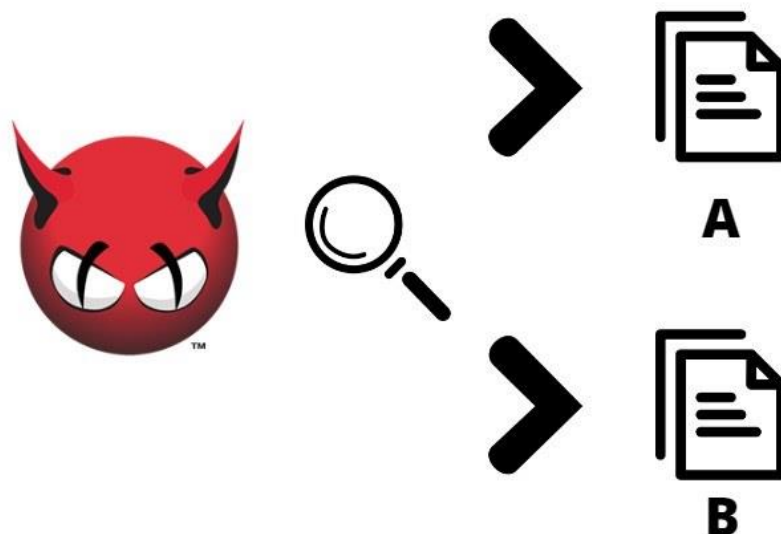
## El funcionamiento básico de un antivirus

Un antivirus como ClamAV (como la mayoría de antivirus) opera siguiendo estos pasos generales:

**1. Definición de firmas:** Los antivirus utilizan **bases de datos de firmas**, que son patrones únicos asociados a **cada tipo de malware**. Estas firmas se actualizan constantemente para incluir nuevas amenazas. En el caso de **ClamAV** se realiza mediante el comando **freshclam**

```
(kali㉿kali)-[~]  
$ sudo freshclam  
[sudo] password for kali:  
Thu Sep 19 12:36:06 2024 → ClamAV update process started at Thu Sep 19  
12:36:06 2024  
Thu Sep 19 12:36:06 2024 → daily database available for download (remote  
version: 27403)  
Time: 10.2s, ETA: 0.0s [=====] 61.18MiB/61.1  
Thu Sep 19 12:36:17 2024 → Testing database: '/var/lib/clamav/tmp.aef3  
bce82/clamav-601529ba8b593847ffd8b082a6a43faf.tmp-daily.cvd' ...  
Thu Sep 19 12:36:23 2024 → Database test passed.  
Thu Sep 19 12:36:23 2024 → daily.cvd updated (version: 27402, sigs: 20  
6917, f-level: 90, builder: raynman)  
Thu Sep 19 12:36:23 2024 → Received an older daily CVD than was advert  
sed. We'll retry so the incremental update will ensure we're up-to-date  
Thu Sep 19 12:36:23 2024 → daily database available for update (local  
ersion: 27402, remote version: 27403)  
Current database is 1 version behind.  
Downloading database patch # 27403 ...
```

**2. Análisis de archivos:** Cuando un archivo es escaneado, el antivirus compara su contenido con las firmas conocidas. Si encuentra una coincidencia, se considera que el archivo está infectado. En este caso se procede a analizar dos archivos, un archivo ejecutable de windows descargado desde una página web y el segundo sacado de un repositorio de github.



Para analizar los archivos se utiliza el comando **clamscan -i -r --max-scansize=4000M --max-filesize=4000M /home/kali/archivo1**

```
(kali@kali)-[~]
$ clamscan -i -r --max-scansize=4000M --max-filesize=4000M /home/kali/Desktop/a 10.8.9_x86.exe

----- SCAN SUMMARY -----
Known viruses: 8698761
Engine version: 1.0.1
Scanned directories: 0
Scanned files: 1
Infected files: 0
Data scanned: 131.34 MB
Data read: 123.33 MB (ratio 1.06:1)
Time: 41.767 sec (0 m 41 s)
Start Date: 2024:09:19 12:51:52
End Date: 2024:09:19 12:52:33

(kali@kali)-[~]
$
```

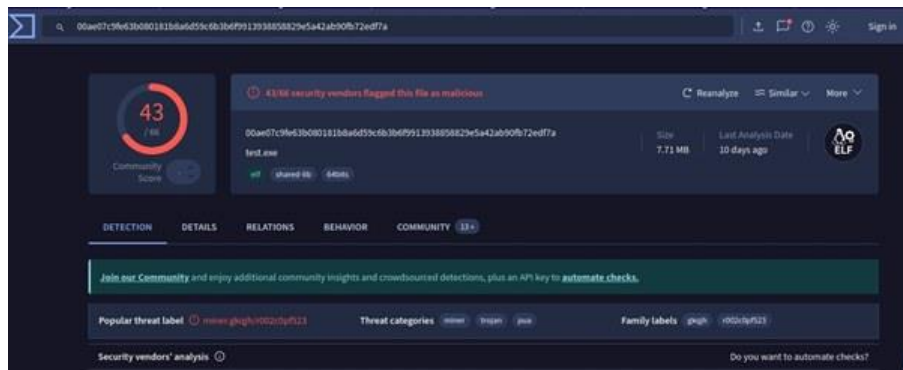
Usamos el mismo comando para el segundo archivo `clamscan -i -r --max-scansize=4000M --max-filesize=4000M /home/kali/archivo2`

```
(kali@kali)-[~]
$ clamscan -i -r --max-scansize=4000M --max-filesize=4000M /home/kali/Desktop/00ae07c9fe63b080181b8a6d59c6b3b6f9913938858829e5a42ab90fb72edf7a
/home/kali/Desktop/00ae07c9fe63b080181b8a6d59c6b3b6f9913938858829e5a42ab90fb72edf7a: Multios.Coinminer.Miner-6781728-2 FOUND

----- SCAN SUMMARY -----
Known viruses: 8698761
Engine version: 1.0.1
Scanned directories: 0
Scanned files: 1
Infected files: 1
Data scanned: 8.20 MB
Data read: 7.71 MB (ratio 1.06:1)
Time: 15.020 sec (0 m 15 s)
Start Date: 2024:09:19 13:02:43
End Date: 2024:09:19 13:02:58
```

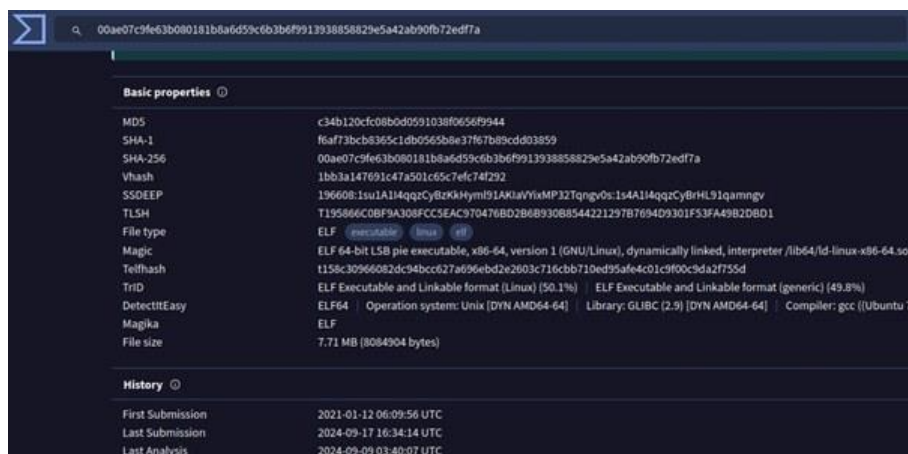
Como podemos ver, el **primer archivo no es detectado como amenaza**, pero lo recomendable es pasarlo una **segunda vez o probar otro antivirus para evitar falsos negativos**. El segundo archivo tiene **Malware (Coinminers)** que se utiliza para obtener criptomonedas )

Lo recomendable siempre es consultar en las máximas bases de datos por si la firma o hash ya está **registrada**. Esta última característica se puede ver en la herramienta **Virustotal** que **consulta en diferentes bases de datos** de antivirus.



3. **Heurística:** Además de las firmas, muchos antivirus utilizan técnicas heurísticas para **detectar malware desconocido**. Estas técnicas se basan en el análisis del comportamiento de los archivos y pueden identificar patrones sospechosos que no se corresponden con ninguna firma conocida.

4.



¿Por qué ClamAV es una buena herramienta en el análisis forense?

- **Detección temprana:** ClamAV puede ayudar a identificar infecciones en sistemas comprometidos, lo que es fundamental para contener una amenaza y evitar una mayor propagación.
- **Análisis de malware:** Al analizar archivos infectados, ClamAV puede proporcionar información valiosa sobre el tipo de malware, su función y su origen.
- **Verificación de la integridad:** ClamAV se puede utilizar para verificar la integridad de archivos y sistemas, asegurando que no hayan sido modificados por malware.
- **Integración con otros sistemas:** ClamAV se integra fácilmente con otros sistemas y herramientas de análisis forense, lo que facilita la creación de flujos de trabajo automatizados.

- **Gratuito y de código abierto:** Esto permite a cualquier persona **acceder a su código fuente** y personalizarlo según sus necesidades.
- **Alta velocidad de escaneo:** ClamAV es conocido por su eficiencia, lo que lo hace ideal para escanear grandes cantidades de datos.
- **Modularidad:** ClamAV se puede configurar para **adaptarse a diferentes entornos** y necesidades.

### Usos de ClamAV en el análisis forense:

- **Investigación de incidentes:** Identificar malware en sistemas comprometidos y determinar el alcance de una infección.
- **Análisis de malware:** Desensamblar y **analizar muestras de malware** para comprender su funcionamiento.
- **Verificación de la integridad de la evidencia:** Asegurar que las evidencias digitales no hayan sido alteradas.
- **Creación de entornos de análisis seguros:** Escanear imágenes de disco y memorias USB para identificar posibles amenazas antes de analizarlas en un entorno aislado.

ClamAV es una herramienta invaluable para cualquier profesional de la ciberseguridad. Su capacidad para **detectar malware, su facilidad de uso y su integración** con otras herramientas lo convierten en un componente esencial de cualquier arsenal de análisis forense.