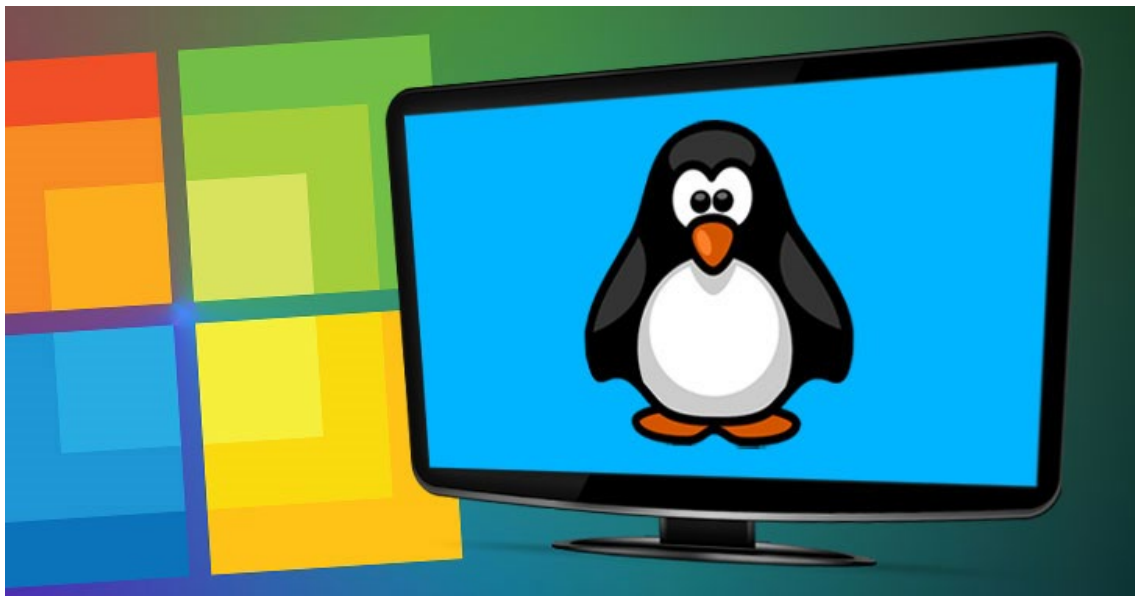


# **TOMA DE EVIDENCIAS EN SISTEMAS LINUX**



**Alfonso Rodríguez Rodríguez**

**Análisis forense  
Ciberseguridad**

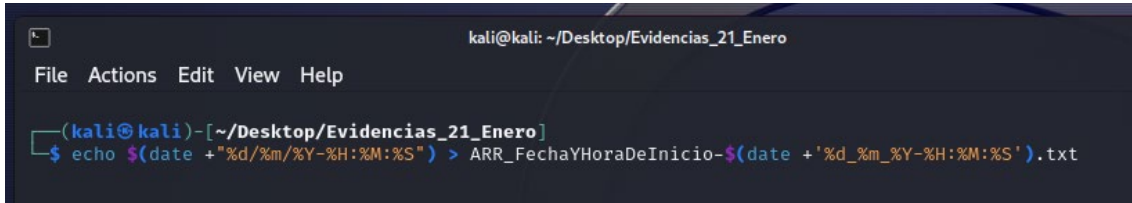
## Contenido

1. Información volátil.....	3
1.1. Hora y fecha del sistema.....	3
1.2. Volcado de memoria.....	3
1.3. Procesos en ejecución. ....	3
1.4. Servicios en ejecución.....	4
1.5. Usuarios que han iniciado sesión y listado de cuentas de usuario. ....	4
1.6. Información de red: estado, conexiones activas, puertos UDP y TCP abiertos.....	4
1.6.1. Estado de la red.....	4
1.6.2. Conexiones establecidas.....	5
1.6.3. Ficheros transferidos recientemente.....	5
1.6.4. Conexiones activas o puertos abiertos. ....	5
1.6.5. Contenido de la caché de DNS.....	6
1.6.6. ARP caché.....	6
1.6.7. Tráfico de red.....	6
1.7. Dispositivos USB conectados. ....	6
1.8. Listado de redes WiFi a las que se ha conectado el equipo. ....	7
1.9. Configuración del cortafuegos de Linux. ....	7
1.10. Programas que se ejecutan al iniciar el sistema operativo. ....	7
1.11. Ficheros abiertos recientemente.....	7
1.12. Software instalado. ....	8
1.13. Contraseñas.....	8
1.14. Información cacheada de los navegadores (direcciones, historiales de descarga...) .....	8
1.15. Árbol de directorios y ficheros.....	8
1.16. Histórico del intérprete de comandos.....	9
1.17. Capturas de pantalla.....	9
1.18. Información del portapapeles.....	9
1.19. Historial de Internet.....	9
1.20. Última búsqueda. ....	10
1.21. Cookies.....	10
1.22. Volúmenes cifrados.....	10
1.23. Unidades mapeadas. ....	10
1.24. Carpetas compartidas.....	11

2.	Información no volátil. ....	11
2.1.	Volcado de disco. ....	11
2.2.	Información del sistema. ....	11
2.3.	Tareas programadas. ....	12
2.4.	Variables de entorno. ....	12
2.5.	Logs del sistema. ....	12
2.6.	Papelera de reciclaje.....	13
2.7.	Ficheros hosts.....	13

## 1. Información volátil

### 1.1. Hora y fecha del sistema.

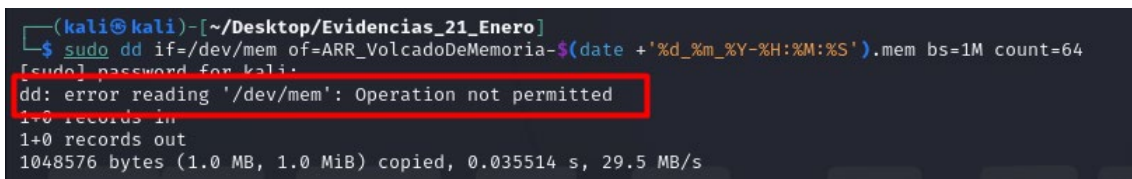


```
kali@kali: ~/Desktop/Evidencias_21_Enero
File Actions Edit View Help

(kali@kali)~[~/Desktop/Evidencias_21_Enero]
$ echo $(date +"%d/%m/%Y-%H:%M:%S") > ARR_FechaYHoraDeInicio-$(date +"%d_%m_%Y-%H:%M:%S').txt
```


Este comando utiliza el comando **date** para obtener la fecha y hora del sistema y luego, redirige la salida hacia un archivo llamado con el formato deseado.

### 1.2. Volcado de memoria.



```
(kali@kali)~[~/Desktop/Evidencias_21_Enero]
$ sudo dd if=/dev/mem of=ARR_VolcadoDeMemoria-$(date +"%d_%m_%Y-%H:%M:%S').mem bs=1M count=64
[sudo] password for kali:
dd: error reading '/dev/mem': Operation not permitted
1+0 records in
1+0 records out
1048576 bytes (1.0 MB, 1.0 MiB) copied, 0.035514 s, 29.5 MB/s
```

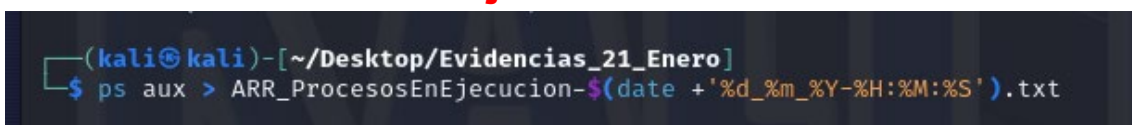
El error "**dd: error reading '/dev/mem': Operation not permitted**" indica que no tienes los permisos necesarios para acceder al archivo `/dev/mem`. El acceso a `/dev/mem` está restringido en sistemas modernos por razones de seguridad.



```
(kali@kali)~[~/Desktop/Evidencias_21_Enero]
$ sudo dd if=/proc/kcore of=ARR_VolcadoDeMemoria-$(date +"%d_%m_%Y-%H:%M:%S').mem bs=1M count=64
64+0 records in
64+0 records out
67108864 bytes (67 MB, 64 MiB) copied, 0.154709 s, 434 MB/s
```

En lugar de usar `/dev/mem`, podrías **utilizar /proc/kcore** para realizar un volcado de memoria. Este comando intentará realizar un volcado de 64 MB (puedes cambiar este valor en el `count`) de la memoria del sistema a un archivo con el formato deseado.

### 1.3. Procesos en ejecución.



```
(kali@kali)~[~/Desktop/Evidencias_21_Enero]
$ ps aux > ARR_ProcesosEnEjecucion-$(date +"%d_%m_%Y-%H:%M:%S').txt
```

Este comando utiliza **ps aux** para listar los procesos en ejecución y luego redirige la salida hacia un archivo con el nombre que incluye la fecha y hora de la ejecución del comando.

## 1.4. Servicios en ejecución.

```
(kali@kali)-[~/Desktop/Evidencias_21_Enero]
$ service --status-all > ARR_ServiciosEnEjecucion-$(date +%d_%m_%Y-%H:%M:%S').txt
```

Este comando utiliza el comando **service --status-all** para obtener el estado de todos los servicios en ejecución y luego redirige la salida hacia un archivo con el nombre que incluye la fecha y hora de la ejecución del comando.

## 1.5. Usuarios que han iniciado sesión y listado de cuentas de usuario.

```
(kali@kali)-[~/Desktop/Evidencias_21_Enero]
$ who > ARR_UsuariosEnSesion-$(date +%d_%m_%Y-%H:%M:%S').txt
```

Este comando utiliza el comando **who** para mostrar información sobre los usuarios que han iniciado sesión en el sistema. La salida se redirige (>) a un archivo de texto con un nombre que incluye la fecha y hora actual en el formato especificado.

```
kali@kali: ~/Desktop/Evidencias_21_Enero
File Actions Edit View Help
(kali@kali)-[~/Desktop/Evidencias_21_Enero]
$ cat /etc/passwd > ARR_CuentasDeUsuario-$(date +%d_%m_%Y-%H:%M:%S').txt
```

Este comando utiliza **cat** para mostrar el contenido del archivo **/etc/passwd**, que contiene información sobre las cuentas de usuario en el sistema, luego, redirige ese contenido a un nuevo archivo de texto.

## 1.6. Información de red: estado, conexiones activas, puertos UDP y TCP abiertos.

### 1.6.1. Estado de la red.

```
(kali@kali)-[~/Desktop/Evidencias_21_Enero]
$ ip link > ARR_EstadoRed-$(date +%d_%m_%Y-%H:%M:%S').txt
```

Este comando utiliza el comando **ip link** para mostrar información sobre las interfaces de red del sistema. La salida se redirige a un archivo de texto con un nombre que incluye la fecha y hora actual en el formato especificado.

### 1.6.2. Conexiones establecidas.

```
(kali@kali)-[~/Desktop/Evidencias_21_Enero]
$ sudo netstat -tupn > ARR_ConexionesEstablecidas-$(date +%d_%m_%Y-%H:%M:%S').txt
```

Este comando utiliza el comando **netstat** para mostrar información sobre las conexiones de red, tanto TCP como UDP, y los programas que las utilizan. La salida se redirige a un archivo de texto con un nombre que incluye la fecha y hora actual en el formato especificado.

### 1.6.3. Ficheros transferidos recientemente.

```
(kali@kali)-[~/Desktop/Evidencias_21_Enero]
$ sudo apt update && sudo apt upgrade
```

Los comandos **sudo apt update** y **sudo apt upgrade** se utiliza en sistemas basados en Debian, como Ubuntu o Kali Linux, para **actualizar el índice de paquetes del sistema** y luego realizar la **actualización de los paquetes instalados**.

```
(kali@kali)-[~/Desktop/Evidencias_21_Enero]
$ sudo apt install iftop
```

```
(kali@kali)-[~/Desktop/Evidencias_21_Enero]
$ sudo iftop > ARR_FicherosTransferidos-$(date +%d_%m_%Y-%H:%M:%S').txt

interface: eth0
IP address is: 10.0.2.15
MAC address is: 08:00:27:21:b1:d0
```

Este comando utiliza el comando **iftop** para mostrar información en tiempo real sobre el tráfico de red y las transferencias de archivos. La salida se redirige a un archivo de texto con un nombre que incluye la fecha y hora actual en el formato especificado.

### 1.6.4. Conexiones activas o puertos abiertos.

```
(kali@kali)-[~/Desktop/Evidencias_21_Enero]
$ ss -tunlp > ARR_ConexionesPuertosAbiertos-$(date +%d_%m_%Y-%H:%M:%S').txt
```

Este comando utiliza el comando **ss** para mostrar información sobre las conexiones de red, tanto TCP como UDP, y los programas que las utilizan. La salida se redirige a un archivo de texto con un nombre que incluye la fecha y hora actual en el formato especificado.

### 1.6.5. Contenido de la caché de DNS.

```
(kali㉿kali)-[~/Desktop/Evidencias_21_Enero]
$ cat /etc/resolv.conf > ARR_ContenidoCachedDNS-$(date +%d_%m_%Y-%H:%M:%S').txt
```

Este comando muestra el contenido del archivo `/etc/resolv.conf`, que contiene la configuración de resolución de nombres de dominio (DNS) del sistema. La salida se redirige a un archivo de texto con un nombre que incluye la fecha y hora actual en el formato especificado.

### 1.6.6. ARP caché.

```
(kali㉿kali)-[~/Desktop/Evidencias_21_Enero]
$ arp -a > ARR_ARPCache-$(date +%d_%m_%Y-%H:%M:%S').txt
```

Este comando **muestra la tabla ARP** (Address Resolution Protocol) que mapea direcciones IP a direcciones MAC en el sistema. La salida se redirige a un archivo de texto con un nombre que incluye la fecha y hora actual en el formato especificado.

### 1.6.7. Tráfico de red.

```
(kali㉿kali)-[~/Desktop/Evidencias_21_Enero]
$ sudo tcpdump -i any -w ARR_TraficoRed-$(date +%d_%m_%Y-%H:%M:%S').pcap

tcpdump: data link type LINUX_SLL2
tcpdump: listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes
^C16 packets captured
16 packets received by filter
0 packets dropped by kernel
```

El comando `tcpdump` se utiliza para capturar y mostrar el tráfico de red en tiempo real. La salida se redirige a un archivo de texto con un nombre que incluye la fecha y hora actual en el formato especificado.

## 1.7. Dispositivos USB conectados.

```
(kali㉿kali)-[~/Desktop/Evidencias_21_Enero]
$ lsusb > ARR_DispositivosUSB-$(date +%d_%m_%Y-%H:%M:%S').txt
```

Este comando utiliza `lsusb` para listar los dispositivos USB conectados al sistema. La salida se redirige a un archivo de texto con un nombre que incluye la fecha y hora actual en el formato especificado.



## 1.8. Listado de redes WiFi a las que se ha conectado el equipo.

```
(kali@kali)-[~/Desktop/Evidencias_21_Enero]
$ cat /etc/NetworkManager/system-connections/* > ARR_ListadoRedesWifi-$(date +%d_%m_%Y-%H:%M:%S').txt
cat: '/etc/NetworkManager/system-connections/*': No such file or directory
```

Este comando muestra la configuración de las conexiones de red inalámbrica almacenadas en **NetworkManager**. La salida se redirige a un archivo de texto con un nombre que incluye la fecha y hora actual en el formato especificado.

En este ordenador no hay posibilidad de ver redes Wifi debido a que **solo tiene tarjeta de red Ethernet**.

## 1.9. Configuración del cortafuegos de Linux.

```
(kali@kali)-[~/Desktop/Evidencias_21_Enero]
$ sudo iptables -L > ARR_ConfiguracionCortafuegos-$(date +%d_%m_%Y-%H:%M:%S').txt
```

Este comando utiliza **iptables** para mostrar la configuración actual del cortafuegos en Linux. La salida se redirige a un archivo de texto con un nombre que incluye la fecha y hora actual en el formato especificado.

## 1.10. Programas que se ejecutan al iniciar el sistema operativo.

```
kali@kali: ~/Desktop/Evidencias_21_Enero
File Actions Edit View Help
$ ls /etc/init.d > ARR_ProgramasInicioSistema-$(date +%d_%m_%Y-%H:%M:%S').txt
```

Este comando lista los programas que se ejecutan al iniciar el sistema operativo desde el directorio **/etc/init.d**. La salida se redirige a un archivo de texto con un nombre que incluye la fecha y hora actual en el formato especificado.

## 1.11. Ficheros abiertos recientemente.

```
(kali@kali)-[~/Desktop/Evidencias_21_Enero]
$ sudo find / -type f -atime -1 > ARR_FicherosAbiertosRecientemente-$(date +%d_%m_%Y-%H:%M:%S').txt
```

Este comando utiliza **find** para buscar y listar los archivos que han sido accedidos en las últimas 24 horas. La salida se redirige a un archivo de texto con un nombre que incluye la fecha y hora actual en el formato especificado.



## 1.12. Software instalado.

```
(kali@kali)-[~/Desktop/Evidencias_21_Enero]
$ dpkg -l > ARR_SoftwareInstalado-$(date +%d_%m_%Y-%H:%M:%S').txt
```

Este comando utiliza **dpkg** para listar todo el software instalado en el sistema. La salida se redirige a un archivo de texto con un nombre que incluye la fecha y hora actual en el formato especificado.

## 1.13. Contraseñas.

```
kali@kali: ~/Desktop/Evidencias_21_Enero
File Actions Edit View Help
(kali@kali)-[~/Desktop/Evidencias_21_Enero]
$ cat /etc/passwd > ARR_Contraseñas-$(date +%d_%m_%Y-%H:%M:%S').txt
```

Este comando muestra el contenido del archivo **/etc/passwd**, que contiene información sobre las cuentas de usuario, incluyendo la información de las contraseñas (aunque cifradas). La salida se redirige a un archivo de texto con un nombre que incluye la fecha y hora actual en el formato especificado.

## 1.14. Información cacheada de los navegadores (direcciones, historiales de descarga...)

```
kali@kali: ~/Desktop/Evidencias_21_Enero
File Actions Edit View Help
(kali@kali)-[~/Desktop/Evidencias_21_Enero]
$ sqlite3 $(find ~/.mozilla/firefox -name "places.sqlite") "SELECT url FROM moz_places;" > ARR_InformacionCacheNavegadores-$(date +%d_%m_%Y-%H:%M:%S').txt
```

Este comando busca la **base de datos places.sqlite** utilizada por **Firefox** y ejecuta una consulta SQL para obtener las URLs del historial de navegación.

## 1.15. Árbol de directorios y ficheros.

```
(kali@kali)-[~/Desktop/Evidencias_21_Enero]
$ tree > ARR_ArbolDirectoriosFicheros-$(date +%d_%m_%Y-%H:%M:%S').txt
```

Este comando utiliza **tree** para mostrar la estructura de directorios y archivos a partir del directorio actual. La salida se redirige a un archivo de texto con un nombre que incluye la fecha y hora actual en el formato especificado.

## 1.16. Histórico del intérprete de comandos.

```
(kali@kali)-[~/Desktop/Evidencias_21_Enero]
$ history > ARR_HistoricoComandos-$(date +%d_%m_%Y-%H:%M:%S').txt
```

El comando **history** se utiliza para mostrar una lista de comandos previamente ejecutados en la terminal. La salida se redirige a un archivo de texto con un nombre que incluye la fecha y hora actual en el formato especificado.

## 1.17. Capturas de pantalla.

```
(kali@kali)-[~/Desktop/Evidencias_21_Enero]
$ ls -ltu ~/Pictures | grep -i ".png|.jpg" > ARR_CapturasPantalla-$(date +%d_%m_%Y-%H:%M:%S').txt
```

Este comando **lista las capturas de pantalla en el directorio ~/Pictures**, ordenadas por la fecha de última modificación. La salida se redirige a un archivo de texto con un nombre que incluye la fecha y hora actual en el formato especificado.

## 1.18. Información del portapapeles.

```
(kali@kali)-[~/Desktop/Evidencias_21_Enero]
$ sudo apt install xclip
```

```
(kali@kali)-[~/Desktop/Evidencias_21_Enero]
$ xclip -selection clipboard -o > ARR_InformacionPortapapeles-$(date +%d_%m_%Y-%H:%M:%S').txt
```

Este comando utiliza la **selección del portapapeles (clipboard)** y, si STRING no está disponible, intentará con el formato PRIMARY.

## 1.19. Historial de Internet.

```
(kali@kali)-[~/Desktop/Evidencias_21_Enero]
$ sqlite3 $(find ~/.mozilla/firefox -name "places.sqlite" -print -quit 2>/dev/null || echo "/dev/null") "SELECT url FROM moz_places;" | grep -i -E 'http|https' > ARR_HistorialInternet-$(date +%d_%m_%Y-%H:%M:%S').txt
```

Este comando utiliza directamente la salida de sqlite3 y la pasa a grep para **filtrar las URLs que contienen "http" o "https"**. La salida se redirige a un archivo de texto.

## 1.20. Última búsqueda.

```
(kali@kali)-[~/Desktop/Evidencias_21_Enero]
$ sqlite3 $(find ~/.mozilla/firefox -name "places.sqlite" -print -quit 2>/dev/null || echo "/dev/null") "SELECT moz_places.url
FROM moz_historyvisits JOIN moz_places ON moz_historyvisits.place_id = moz_places.id ORDER BY moz_historyvisits.visit_date DESC L
IMIT 1;" > ARR_UltimaPaginaVisitada-$(date +%d_%m_%Y-%H:%M:%S').txt
```

El comando completo usa **sqlite3** para realizar una **consulta SQL** en la base de datos del historial de Firefox y extraer la URL de la última visita. La salida de este comando será la URL de la última página web visitada según el historial de Firefox. La salida se redirige a un archivo de texto.

## 1.21. Cookies.

```
(kali@kali)-[~/Desktop/Evidencias_21_Enero]
$ sqlite3 $(find ~/.mozilla/firefox -name "cookies.sqlite" -print -quit 2>/dev/null || echo "/dev/null") "SELECT * FROM moz_coo
okies;" > ARR_Cookies-$(date +%d_%m_%Y-%H:%M:%S').txt
```

Este comando selecciona todas las columnas de la tabla **moz\_cookies** en la base de datos **cookies.sqlite** y redirige la salida a un archivo de texto.

## 1.22. Volúmenes cifrados.

```
kali@kali: ~/Desktop/Evidencias_21_Enero
File Actions Edit View Help
(kali@kali)-[~/Desktop/Evidencias_21_Enero]
$ sudo cryptsetup luksDump /dev/sda > ARR_InformacionVolúmenesCifrados-$(date +%d_%m_%Y-%H:%M:%S').txt
[sudo] password for kali:
Device /dev/sda is not a valid LUKS device.
```

El comando **cryptsetup** se utiliza para configurar y gestionar dispositivos cifrados utilizando el sistema de cifrado LUKS (Linux Unified Key Setup). En mi caso, estoy utilizando **cryptsetup** para obtener información sobre un volumen cifrado pero no hay volúmenes cifrados en este sistema.

## 1.23. Unidades mapeadas.

```
(kali@kali)-[~/Desktop/Evidencias_21_Enero]
$ mount > ARR_UnidadesMapeadas-$(date +%d_%m_%Y-%H:%M:%S').txt
```

Este comando utiliza el comando **mount** para mostrar las unidades actualmente montadas en el sistema y redirige la salida a un archivo de texto.

## 1.24. Carpetas compartidas.

```
(kali@kali)-[~/Desktop/Evidencias_21_Enero]
$ showmount -e > ARR_CarpetasCompartidas-$(date +%d_%m_%Y-%H:%M:%S').txt
cInt_create: RPC: Unable to receive
```

Este comando utiliza **showmount** para listar las carpetas compartidas en tu sistema y redirige la salida a un archivo de texto pero este sistema no tiene carpetas compartidas.

## 2. Información no volátil.

### 2.1. Volcado de disco.

```
(kali@kali)-[~/Desktop/Evidencias_21_Enero]
$ sudo dd if=/dev/sda of=ARR_VolcadoDeDisco-$(date +%d_%m_%Y-%H:%M:%S').img bs=4M status=progress
696254464 bytes (696 MB, 664 MiB) copied, 12 s, 57.6 MB/s
```

Este comando utiliza **dd** para copiar todo el contenido del disco (if=/dev/sda) y guardar la salida en un archivo .img. El parámetro bs=4M establece el tamaño de bloque para la copia. Lo he parado a los 15GB debido a que el disco de la maquina virtual es de 80 y tardaría y pesaría mucho la copia.

### 2.2. Información del sistema.

```
(kali@kali)-[~/Desktop/Evidencias_21_Enero]
$ {
  uname -a
  lsb_release -a
  hostnamectl
  lscpu
} > ARR_InformacionDelSistema-$(date +%d_%m_%Y-%H:%M:%S').txt
```

Para obtener información del sistema en Linux, puedes utilizar el comando **uname** para detalles del kernel, y comandos como **lsb\_release**, **hostnamectl**, y **lscpu** para detalles específicos del sistema operativo. Este comando ejecuta múltiples comandos y redirige la salida a un archivo.

### 2.3. Tareas programadas.

```
(kali@kali)-[~/Desktop/Evidencias_21_Enero]
$ {
  cat /etc/cron.d/*
  cat /etc/cron.daily/*
} > ARR_TareasProgramadas-$(date +%d_%m_%Y-%H:%M:%S').txt
```

Para obtener información sobre las tareas programadas a nivel de sistema, podrías **revisar los directorios /etc/cron.d/ y /etc/cron.daily/**. Este comando concatena el contenido de los archivos en esos directorios y lo guarda en un archivo de texto.

### 2.4. Variables de entorno.

```
(kali@kali)-[~/Desktop/Evidencias_21_Enero]
$ env > ARR_VariabesDeEntorno-$(date +%d_%m_%Y-%H:%M:%S').txt
```

El comando **env** se utiliza para mostrar el entorno actual o ejecutar un comando en un entorno modificado.

### 2.5. Logs del sistema.

**Journalctl** te permitirá ver los registros del sistema gestionados por **systemd**.

Algunos de estos comandos pueden requerir privilegios de superusuario (root) para acceder a los archivos de registro.

```
(kali@kali)-[~/Desktop/Evidencias_21_Enero]
$ journalctl --system > ARR_LogsSistema-$(date +%d_%m_%Y-%H:%M:%S').txt
```

La opción **--system** de **journalctl** se utiliza para mostrar los registros del sistema.

```
(kali@kali)-[~/Desktop/Evidencias_21_Enero]
$ journalctl --user > ARR_LogsUsuario-$(date +%d_%m_%Y-%H:%M:%S').txt
```

La opción **--user** de **journalctl** se utiliza para mostrar los registros del usuario.

## 2.6. Papelera de reciclaje.

```
(kali@kali)-[~/Desktop/Evidencias_21_Enero]
$ tar -zcvf ARR_Papelera-$(date +%d_%m_%Y-%H-%M-%S').tar.gz ~/.local/share/Trash/
```

El comando **crea un archivo comprimido** (con extensión .tar.gz) de la **papelera** del usuario, La opción -z indica que el archivo debe ser comprimido usando gzip, y las opciones -cvf especifican la creación del archivo de forma verbose.

## 2.7. Ficheros hosts.

```
kali@kali: ~/Desktop/Evidencias_21_Enero
File Actions Edit View Help
(kali@kali)-[~/Desktop/Evidencias_21_Enero]
$ cat /etc/hosts > ARR_FicheroHosts-$(date +%d_%m_%Y-%H:%M:%S').txt
```

Este comando utiliza **cat** para mostrar el contenido del archivo **/etc/hosts** en la terminal y luego redirige ese contenido a un nuevo archivo de texto con el nombre que incluye la fecha y hora actual. No se necesitan privilegios de superusuario para leer el archivo /etc/hosts.