PROCEDIMIENTO 2: RECOPILACIÓN DE DATOS VOLÁTILES

La información volátil son datos que se borran cuando el sistema se desconecta del suministro eléctrico. Entre estos datos cabe citar los siguientes:

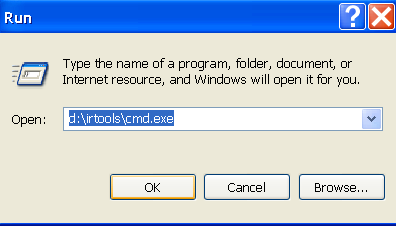
* Hora y fecha del sistema
* El nombre del usuario conectado al sistema en ese momento
* Los puertos y servicios abiertos en el sistema en ese momento
* Los procesos que se están ejecutando en el sistema en ese momento
* Los archivos abiertos en el sistema en ese momento
* Los sistemas conectados al sistema en ese momento o anteriormente
* Las horas de creación, modificación y acceso de todos los archivos

Antes de comenzar a recopilar datos, es necesario que conozca los conceptos siguientes y la forma en que se relacionan con el proceso de recopilación:

* Cómo preparar el sistema operativo Windows para la recopilación de datos
* Los comandos utilizados para la recopilación de datos
* Las utilidades empleadas para la recopilación de datos

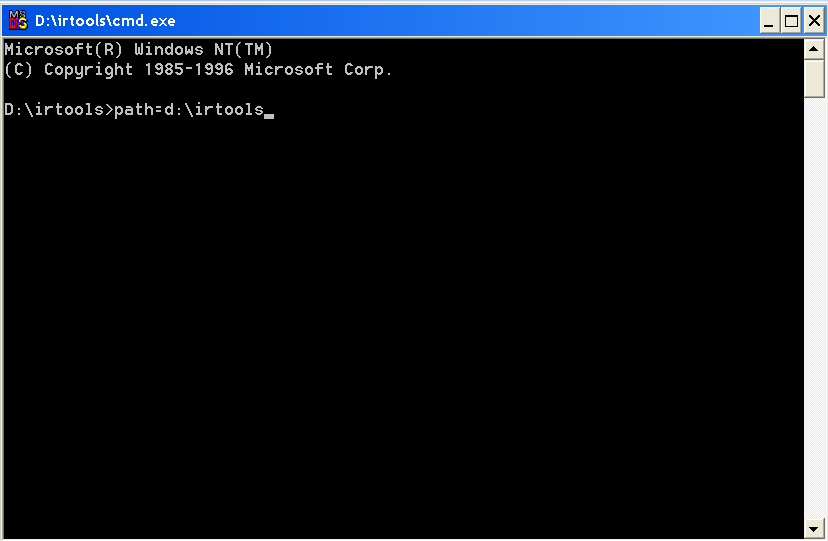
Antes de la recopilación de datos volátiles y durante ésta, documente cada acción que realice.





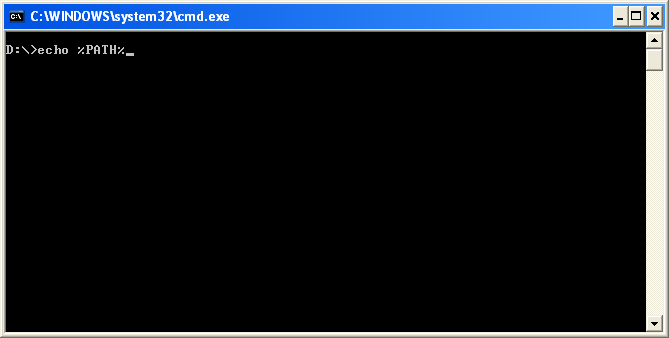
|  |  |
| --- | --- |
| **Paso** | **Acción** |
| 1. | Continúe el registro de la documentación y documente cada paso que realice. |
| 2. | Inserte el disquete forense en la unidad correspondiente. |
| 3. | Inserte el CD-ROM de comandos y herramientas forenses en la unidad de CD- ROM. |
| 4. | Abra una ventana de comandos siguiendo los pasos a continuación:   * Haga clic en el botón **Start** (Iniciar). * Haga clic en **Run** (Ejecutar). * En el cuadro **Open:** (Abrir), teclee **d:\irtools\cmd.exe**. * Haga clic en **OK** (Aceptar).   **NOTA**: este comando abre un shell de comandos y lo ejecuta desde las herramientas forenses limpias de respuesta a incidentes. Recuerde: NO se usan los comandos de la máquina vulnerada porque los archivos binarios del sistema de dicha máquina podrían contener un troyano o podrían mostrar datos incompatibles con la configuración del sistema real. |





|  |  |
| --- | --- |
| 5. | Para comprobar que sus comandos se ejecuten desde el CD-ROM de comandos y herramientas forenses, teclee el comando siguiente:  **PATH=d:\irtools**  Presione la tecla **Enter** (Entrar).  **NOTA**: cambiamos la ubicación desde donde la máquina vulnerada ejecuta los archivos binarios. Hay una ruta de acceso predeterminada dentro del sistema de archivos, y esta ruta suele incluir la unidad C:\. Recuerde: deseamos asegurarnos de que todos los comandos ejecutados durante los procedimientos de respuesta a incidentes se ejecuten desde el CD-ROM de comandos y herramientas forenses. Por lo tanto, debemos cambiar nuestra ruta de acceso predeterminada a la unidad D:\, o la letra de unidad asignada a la unidad de CD-ROM que esté utilizando. |





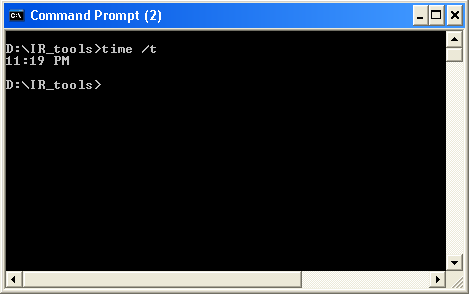
|  |  |
| --- | --- |
| 6. | Para comprobar que se haya definido la ruta de acceso, cuando vea el aviso D:\ teclee lo siguiente:  **echo %PATH%**  Presione la tecla **Enter** (Entrar).  **NOTA**: usted debe definir la RUTA DE ACCESO cada vez que abra una nueva ventana de comando. Si por algún motivo cierra el shell de comandos actual, compruebe siempre que la ruta de acceso se defina de nuevo. Cuando cambiamos la instrucción de la ruta, el cambio es válido sólo para ese shell de comandos. Este comando se ejecuta para asegurar que hayamos cambiado correctamente la ruta de acceso a la unidad D:\. Si su ruta de acceso no dice D:\, repita el paso 6. |



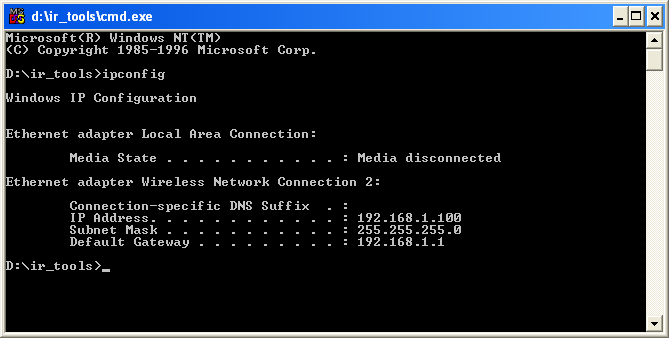
|  |  |
| --- | --- |
| 7. | El comando de fecha se usa para que aparezca la fecha actual del sistema.  La opción /t le permite mostrar la fecha sin configurarla en el sistema con sólo presionar **Enter** (Entrar) al final del comando. Con esto aparecerá la fecha actual del sistema en cuestión.  Para ver la fecha, teclee: **date /t**    Para enviar los resultados al disquete de almacenamiento forense, teclee lo siguiente:  **date /t > a:\startdate.txt**  **NOTA**: el motivo por el cual capturamos la fecha del sistema es para asegurarnos de tener configuradas la fecha y hora correctas en la máquina vulnerada o del agresor. Esto nos ayuda a correlacionar mejor los archivos de registro, y revela si se ha cambiado la fecha del sistema para ocultar pruebas o proporcionar una coartada al sospechoso. |

|  |  |
| --- | --- |
| 8. | El comando de hora indica la hora actual del sistema.  La opción /t le permite mostrar la hora sin configurarla en el sistema. Para ver la hora, teclee **time /t**.  Para enviar los resultados al disquete de almacenamiento forense, teclee lo siguiente:  **time /t > a:\starttime.txt**  **NOTA:** de nuevo, esto le ayudará, como investigador o administrador del sistema, a establecer una mejor escala de tiempo. Si el reloj del sistema no está configurado con la hora exacta, documente la configuración y establezca una correlación con la hora real. Es posible que la fecha y la hora del sistema hayan sido cambiadas para encubrir o proporcionar una coartada al sospechoso que cometió los delitos. |



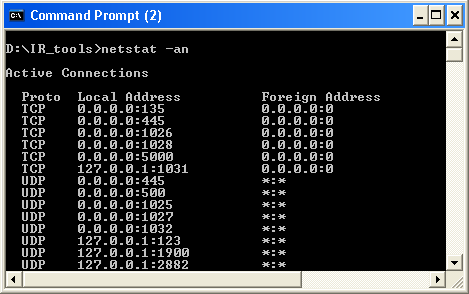






|  |  |
| --- | --- |
| 9. | El paso siguiente es capturar el protocolo de Internet (IP, *Internet Protocol*) actual asignado al sistema vulnerado que usted está investigando. En este paso, usaremos el comando **IPCONFIG.exe**.  Al aparecer el símbolo del sistema, teclee lo siguiente:  **ipconfig** y presione la tecla **Enter** (Entrar).  Para enviar los resultados del comando a la unidad del disquete, teclee lo siguiente:  **ipconfig > a:\ipconfig.txt**  El comando **ipconfig.exe** proporciona la dirección exacta de la máquina en la red, y muestra la forma en que se desglosa el segmento de la red. La dirección de IP sólo puede asignarse por un período breve y se considera un dato volátil porque puede perderse si el investigador desconecta el suministro eléctrico. Las direcciones de IP que se asignan sólo por poco tiempo se conocen como ***DHCP***. Las demás direcciones que no cambian se denominan direcciones de IP ***ESTÁTICAS***. Las direcciones de IP de una máquina son como un domicilio particular. Una sección de la dirección de IP es la red o la calle, y la otra mitad de la dirección de IP es el número de host o el número de la casa. |

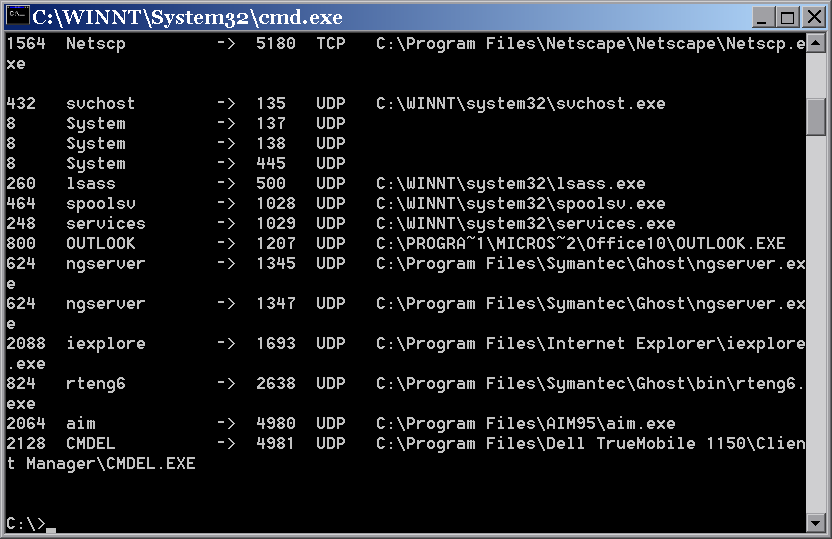




|  |  |
| --- | --- |
| 10. | El comando **netstat command** se utiliza para mostrar el estado de la red y los servicios que se están ejecutando en el sistema.  **-a** Con la visualización predeterminada, esto muestra el estado de todos los sockets; normalmente no se muestran los sockets que usan los procesos del servidor.  **-n** Esto muestra la dirección de IP de la red real del sistema y sólo los puertos locales que tienen conexiones TCP establecidas.  Para ver los datos netstat, teclee el comando siguiente:  **netstat –an**  Para enviar los resultados al disquete de almacenamiento forense, teclee lo siguiente:  **netstat -an > a:\netstat.txt**  **NOTA:** este es un dato muy importante que los investigadores deben capturar durante los procedimientos de respuesta a incidentes. El comando netstat muestra todas las conexiones y puertos abiertos actuales de la máquina. Si un agresor está en la máquina en tiempo real, usted verá una conexión activa junto con la dirección de IP del agresor. Este puede ser el dato de prueba que resuelva su investigación. Si usted se limita a desconectar la máquina sin obtener esta información, puede perderla permanentemente.  Protocolo Dirección local Dirección extranjera  **TCP 192.168.1.100:31337 64.1.23.45:32789**  En el ejemplo indicado arriba, hay una conexión con la máquina de la víctima (192.168.1.100) en el puerto 31337 (bo2k) desde la máquina del agresor 64.1.23.45. |

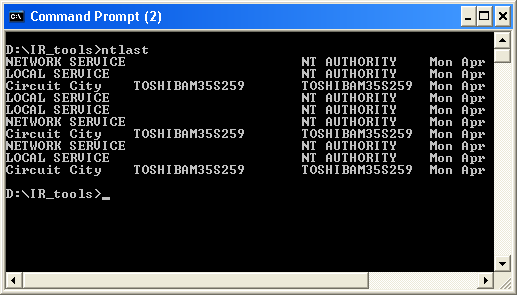
|  |  |
| --- | --- |
| 11. | La herramienta Fport se usa para asignar puertos abiertos a los procesos que se están ejecutando en este momento.  El comando fport proporciona la siguiente información:   * Número de identificación del proceso (PID, *Process Identification*) * Nombre del proceso * Protocolo que se utiliza * Puerto al que está enlazado el programa * Ruta de acceso absoluta al programa enlazado con ese puerto Para ver los datos de Fport, teclee el comando siguiente:   **fport**  Para enviar los resultados al disquete de almacenamiento forense, teclee lo siguiente:  **fport > a:\fport.txt**  **NOTA:** este es otro dato crucial que los investigadores y los administradores del sistema deben capturar. El comando fport asigna el archivo binario que abre los puertos. Este comando trabaja paralelamente al comando netstat.  Aquí podemos ver el puerto, el servicio y la ruta de acceso completa al archivo binario que inició el proceso de escucha del servicio. Por lo tanto, si ve un puerto sospechoso, ahora puede dirigirse directamente al archivo binario y examinarlo para detectar alguna actividad sospechosa. Esto da muy buen resultado con los archivos troyanos y binarios. |





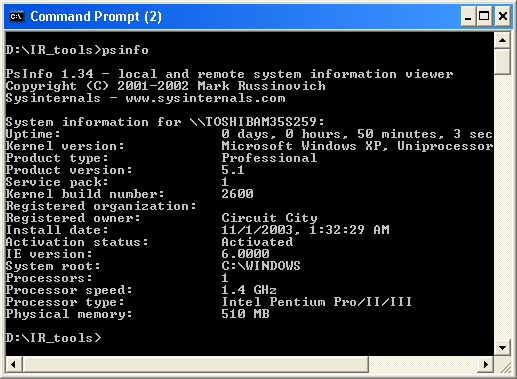
|  |  |
| --- | --- |
| 12. | El comando ntlast se usa para recuperar los últimos usuarios que se conectaron a la computadora víctima. ***Se debe activar la auditoría para recuperar esta información*.**  Para ver los datos ntlast, teclee el comando siguiente:  **ntlast**  Para enviar los resultados al disquete de almacenamiento forense, teclee lo siguiente:  **ntlast > a:\ntlast.txt**  **NOTA**: este comando le ayuda a determinar quién se ha conectado a la máquina durante un cierto período. El comando sólo funciona si se han activado los registros de auditoría del sistema (Sistema, Seguridad y Aplicación). Esta información le ayuda a determinar si se han usado cuentas válidas para comprometer la seguridad el sistema. |





|  |  |
| --- | --- |
| 13. | El comando psinfo enumera información del sistema acerca de la computadora. Para ver los datos psinfo, teclee el comando siguiente:  **psinfo**  Para enviar los resultados al disquete de almacenamiento forense, teclee lo |





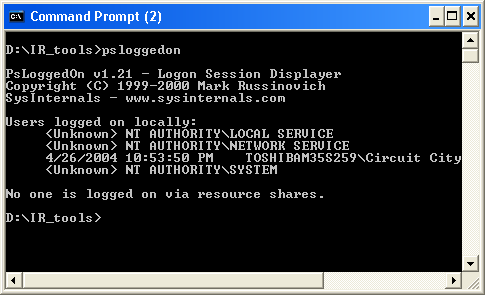


|  |  |
| --- | --- |
|  | siguiente:  **psinfo > a:\psinfo.txt**  **NOTA**: el comando psinfo proporciona mucha información acerca del sistema. Como puede ver del ejemplo anterior, proporciona fechas, horas, directorios raíz del sistema, fecha de instalación, versiones de Internet Explorer y más. Es una forma rápida y fácil de recabar gran cantidad de información acerca del sistema. Toda esta información puede ser útil para determinar el tipo de ataques a los que puede ser vulnerable la computadora de la víctima y la clase de información que pueda ser residual del tipo de ataque. |



|  |  |
| --- | --- |
| 14. | El comando pslist se usa para recuperar información acerca de los procesos que se están ejecutando actualmente en la computadora de la víctima.  Para ver los datos de pslist, teclee:  **pslist**    Para enviar los resultados al disquete de almacenamiento forense, teclee lo siguiente:  **pslist > a:\pslist.txt**  **NOTA:** el comando pslist le ayuda, como investigador, a establecer los procesos en ejecución y sus PID (números de identificación de proceso) asociados. En su calidad de investigador o administrador del sistema, debe conocer el tiempo que se ha ejecutado un proceso y la medida de la velocidad utilizada de la unidad central de procesamiento (CPU, *Central Processing Unit*). Por ejemplo, si se está ejecutando un servicio troyano, es conveniente  saber cuánto tiempo ha estado ejecutándose ese proceso para que usted determine el intervalo de tiempo en que puede haber sucedido el ataque. |

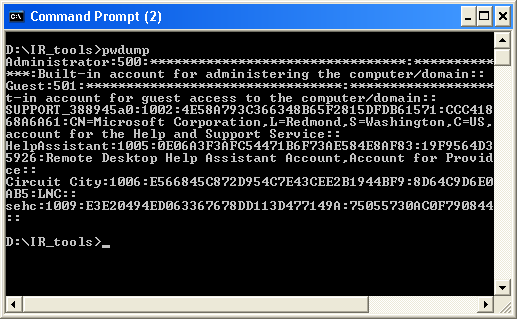




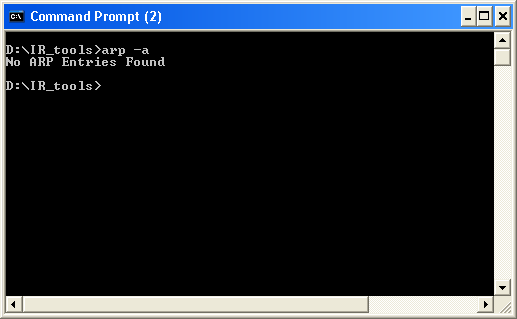
|  |  |
| --- | --- |
| 15. | El comando psloggedon se usa para determinar quién está conectado al sistema en ese momento.  Para ver los datos de psloggedon, teclee el comando siguiente:  **psloggedon**  Para enviar los resultados al disquete de almacenamiento forense, teclee lo siguiente:  **psloggedon > a:\psloggedon.txt**  **NOTA:** otro dato clave es el nombre del usuario conectado en ese momento al sistema en cuestión. En este caso, es posible que vea varios inicios de sesión o sólo un inicio de sesión a la vez. Se deben verificar estos inicios de sesión con el administrador del sistema para comprobar que cuenten con el debido acceso a la computadora. Es posible que vea al agresor conectado al sistema utilizando una cuenta válida de usuario. Tal vez el usuario ya no trabaje para la empresa o esté ausente el día en cuestión. Revise cada una de las cuentas de usuario con inicio de sesión, verifique que el acceso sea válido y documente cada inicio de sesión. |

|  |  |
| --- | --- |
| 16. | El comando pwdump se usa para enumerar los usuarios y sus respectivas contraseñas con función hash.  Para ver los datos de pwdump, teclee el comando siguiente:  **pwdump**  Para enviar los resultados al disquete de almacenamiento forense, teclee lo siguiente:  **pwdump > a:\pwdump.txt**  **NOTA:** puede ser necesario capturar las contraseñas del sistema de computadora vulnerado o del sospechoso. En este caso, tal vez tenga que obtener un nombre de usuario y un código de acceso válidos para entrar al sistema. El comando pwdump le permite volcar las cuentas de usuarios y las contraseñas codificadas a un archivo, y luego ejecutar una herramienta, como L0phtcrack, para descifrar las contraseñas codificadas. Así, podrá conectarse con una cuenta de usuario y un código de acceso válidos. |



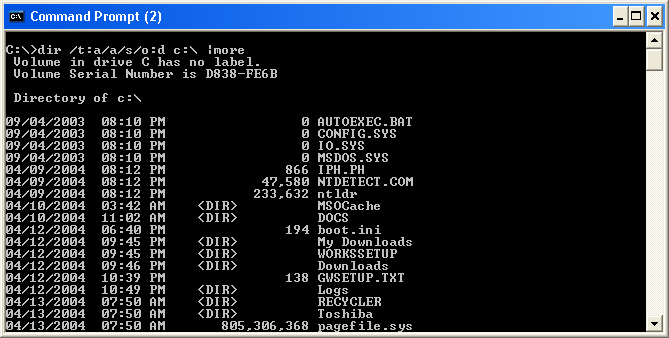






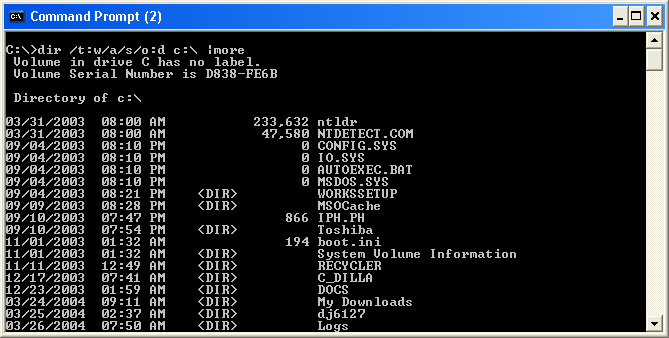
|  |  |
| --- | --- |
| 17. | El comando arp se usa para mostrar las direcciones MAC de los sistemas que están en comunicación con la computadora.  Para ver los datos de arp, teclee el comando siguiente:  **arp** –**a**  Para enviar los resultados al disquete de almacenamiento forense, teclee lo siguiente:  **arp -a > a:\arp.txt**  **NOTA:** otro factor de la investigación es ampliar el alcance del registro que usted realiza en el lugar de la computadora vulnerada. Es posible que el usuario local o el sistema de computadoras se encuentren dentro de la misma infraestructura del mismo edificio físico. El comando arp le proporcionará las direcciones MAC de las últimas computadoras que se comunicaron con el sistema. |





|  |  |
| --- | --- |
| 18a. | Para obtener una lista de directorios de todos los archivos en el sistema seleccionado como objetivo, tamaño de grabación y horas de modificación (m), acceso (a) y creación (c), use el comando dir con los conmutadores correspondientes.  **dir /t:a/a/s/o:d c:\** proporciona una lista de directorios recursivos de todas las horas de **acceso** en la unidad C:.  Teclee el comando siguiente:  **dir /t:a/a/s/o:d c:\**  Para enviar los resultados al disquete de almacenamiento forense, teclee lo siguiente:  **dir /t:a/a/s/o:d c:\ > a:\accesstime.txt**  **NOTA:** uno de los motivos de preocupación principales de las fuerzas del orden y de los profesionales de la seguridad es mantener el sistema en su formato original (sin cambiar) al llegar al lugar del delito, y recopilar los datos volátiles. La serie de comandos a continuación intenta capturar las horas MAC (de modificación, acceso y cambio). Estos intervalos de tiempo son esenciales para realizar una investigación. Permiten a los investigadores determinar los archivos que han sido tocados, cambiados o creados durante los intervalos de tiempo del presunto ataque. Por lo tanto, obtener estos intervalos de tiempo durante la recopilación de datos volátiles se ha vuelto muy importante. Si los investigadores o los profesionales de la seguridad cambian cualquier intervalo de tiempo al llevar a cabo sus capturas de datos volátiles, no se obtendrá el intervalo original. |



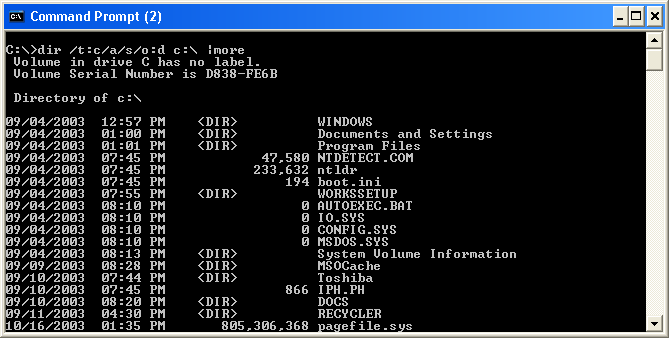


**NOTA SOBRE LOS DATOS**: al capturar estos intervalos de tiempo en el lugar del delito, usted SÍ cambiará los intervalos de tiempo de acceso de todas las carpetas del sistema que esté investigando.

|  |  |
| --- | --- |
| 18b. | **dir /t:w/a/s/o:d c:\** proporciona una lista de directorios recursivos de todas las horas de **modificación** en la unidad C:.  Teclee el comando siguiente:  **dir /t:w/a/s/o:d c:\**  Para enviar los resultados al disquete de almacenamiento forense, teclee el comando siguiente:  **dir /t:w/a/s/o:d c:\ > a:\modification.txt** |

|  |  |
| --- | --- |
| 18c. | **dir /t:c/a/s/o:d c:\** proporciona una lista de directorios recursivos de todas las horas de **creación** en la unidad C:.  Teclee el comando siguiente:  **dir /t:c/a/s/o:d c:\**  Para enviar los resultados al disquete de almacenamiento forense, teclee el comando siguiente:  **dir /t:c/a/s/o:d c:\ > a:\creation.txt** |







|  |  |
| --- | --- |
| 19. | Para obtener un hash md5sum de los datos volátiles almacenados en el disquete forense, teclee el comando siguiente:  **a:<ENTER>**  **md5sum a:\\*.txt > a:\md5sumvolatile.txt** |
| 20. | Para verificar que el hash md5sum se haya grabado en el disquete forense, teclee el comando siguiente:  **more a:\md5sumvolatile.txt** |
| 21. | Expulse el CD-ROM de comandos y herramientas forenses de las unidades respectivas, así como el disquete de almacenamiento forense. |
| 22. | Guarde el CD-ROM de comandos y herramientas forenses, y el disquete de almacenamiento forense en una bolsa o caja para pruebas. |
| 23. | Firme, feche y etiquete la bolsa o caja para pruebas. |