Dell™ Digital Forensics

Guía de soluciones

Notas, precauciones y avisos

NOTA: Una NOTA proporciona información importante que lo ayuda a utilizar su equipo de la mejor manera posible.

PRECAUCIÓN: Un mensaje de PRECAUCIÓN indica la posibilidad de daños en el hardware o la pérdida de datos si no se siguen las instrucciones.

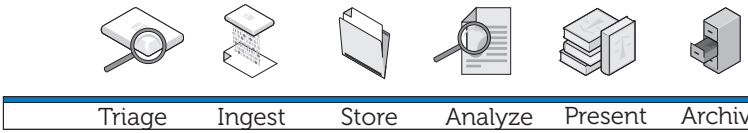
AVISO: Un mensaje de AVISO indica el riesgo de daños materiales, lesiones o incluso la muerte.

2011 - 07 **Rev. A00**

Contenido

1

Introducción



En los últimos años ha habido un aumento exponencial en el volumen, velocidad, variedad y sofisticación de la actividad digital por parte de grupos criminales y terroristas en todo el mundo. Hoy en día muchos delitos tienen un componente digital. Algunos lo han llamado *tsunami digital*. Este crecimiento ha sido magnificado por los espectaculares avances en el hardware electrónico. La amplia diversidad de dispositivos electrónicos para el consumo y su cada vez mayor capacidad de memoria y almacenamiento ofrecen a los delincuentes y terroristas una gran oportunidad para ocultar la información dañina.

No es infrecuente que los PC y los portátiles dispongan de discos duros que se miden en cientos de gigabytes de capacidad de almacenamiento. Los últimos discos duros incluyen opciones para uno o cuatro terabytes. Piénsese que un solo terabyte puede almacenar el contenido de doscientos discos DVD: una enorme cantidad de almacenamiento que representa un problema que seguirá creciendo.

Desde equipos de escritorio hasta portátiles, desde teléfonos móviles hasta las unidades extraíbles e incluso las consolas de juegos, los profesionales de la informática forense digital están siendo presionados hasta el límite para clonar, examinar, indexar, analizar y guardar crecientes cantidades de datos sospechosos al tiempo que se mantiene la cadena de custodia digital y se continúa protegiendo a los ciudadanos.

Tabla 1-1. ¿Cuánto representa un zetabyte?

Kilobyte (KB)	1.000 bytes	2 KB	una página tecleada
Megabyte (MB)	1.000.000 bytes	5 MB	la obra completa de Shakespeare
Gigabyte (GB)	1.000.000.000 bytes	20 GB	una buena colección de las obras de Beethoven
Terabyte (TB)	1.000.000.000.000 bytes	10 TB	una biblioteca de investigación académica
Petabyte (PB)	1.000.000.000.000.000 bytes	20 PB	producción de discos duros anualmente
Exabyte (EB)	1.000.000.000.000.000.000 bytes	5 EB	todas las palabras habladas por el hombre
Zetabyte (ZB)	1.000.000.000.000.000.000.000 bytes	2 ZB	datos que se espera se creen globalmente durante 2010*

* Roger E. Bohn, et. al., ¿cuánta información? 2009, Global Information Industry Center, Universidad de California, San Diego (Enero, 2010).

Cuando existen sospechas sobre algún delincuente y se incautan ordenadores y otros activos digitales, los profesionales de la informática forense reciben una enorme presión para procesar y analizar la evidencia potencial en un período de tiempo muy breve en entornos muy poco adecuados para garantizar los requisitos evidenciales. Cuando organizaciones enteras son sospechosas de actividades ilegales o terroristas, el número de dispositivos a analizar puede aumentar de un modo espectacular.

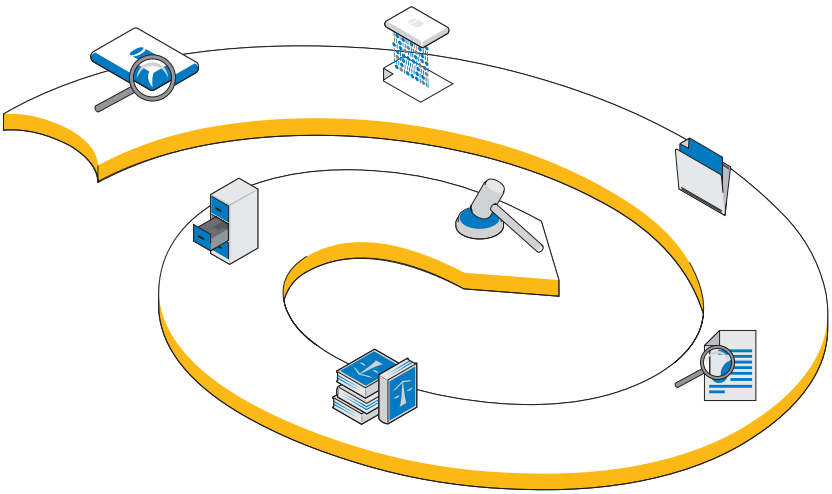
Digital Forensics ofrece un medio para adquirir datos recuperados de ordenadores u otros dispositivos digitales (teléfonos móviles, consolas de juegos, unidades flash, GPS, etc.), así como el examen y análisis científico de dichos datos de manera que se asegure que la información pueda usarse en los tribunales. La solución Digital Forensics de Dell constituye la primera solución integral verdaderamente a nivel de empresa para organismos de seguridad corporativos y gubernamentales encargados de hacer cumplir la ley, así como organizaciones de descubrimiento electrónico (e-discovery), facilitando todo el hardware, software y servicio y soporte técnico necesario para la recogida, triaje, investigación o reproducción de imágenes, almacenamiento, análisis, informes y obtención de la evidencia digital de archivos.

Usando el hardware de servidor y almacenamiento ampliable y asequible de Dell y —dependiendo de los requisitos de su entorno de software— los sistemas de bases de datos de Oracle en el servidor, una combinación de portátiles reforzados de Dell y el software SPEKTOR en el trabajo de campo, así como el servicio y soporte completos de Dell, el personal de investigación puede realizar el triaje y la recogida de datos para el trabajo forense digital de forma rápida y sencilla, asegurando la cadena de custodia desde el lugar de trabajo hasta el centro de datos y los tribunales.

Ciclo de vida de Digital Forensics de Dell

La solución Digital Forensics de Dell sirve de ayuda al investigador forense a lo largo de las seis etapas del ciclo de vida forense: triaje, examen, almacenamiento, análisis, presentación y archivado.

Ilustración 1-1. Ciclo de vida de Digital Forensics de Dell



Triaje

El proceso de triaje ofrece al investigador forense digital la oportunidad de ver rápidamente los contenidos de los dispositivos objetivo con el fin de determinar si deben llevarse al laboratorio para un posterior análisis y preparación para su presentación en los tribunales.

Examen

El examen es la etapa del proceso forense digital en la que se reproducen los datos objetivo (a menos que se hayan reproducido en el lugar de trabajo como parte de la etapa de triaje). Se crea una copia exacta del dispositivo de almacenamiento sospechoso de forma que se pueda garantizar la integridad del duplicado comparando valores hash de las unidades de datos del original y del duplicado.

En consonancia con las prácticas existentes, los datos sospechosos se *reproducen* en la solución Digital Forensics de Dell. No obstante, en lugar de reproducir datos en una única estación de trabajo, los datos reproducidos se examinan en un repositorio de evidencias central. Examinando los datos inmediatamente en el centro de datos, los datos están disponibles para múltiples analistas, se minimiza la transferencia de un dispositivo a otro y se mejora espectacularmente la productividad y la eficiencia. No obstante, si la capacidad de almacenamiento objetivo es suficientemente pequeña, el examen puede llevarse a cabo en el lugar de trabajo. La solución Digital Forensics de Dell permite el examen sobre la marcha en el emplazamiento gracias al uso de un módulo SPEKTOR Imager opcional.

Almacenamiento

La solución Digital Forensics de Dell proporciona una amplia gama de posibles opciones de almacenamiento y acceso de red para adaptarse al cliente de forma individualizada. El almacenamiento y la recuperación de alta velocidad en un entorno de red a nivel de empresa permiten una configuración multiusuario que aumenta la eficiencia y la productividad. Los analistas ya no tendrán que asignar sus activos informáticos individuales para completar el análisis de la evidencia puesto que todo esto tendrá lugar en el servidor dedicado a dicho fin.

Analizar

La capacidad de procesamiento en paralelo que ofrece la solución Digital Forensics de Dell permite al analista indexar y realizar un triaje de los datos en servidores de alto rendimiento en lugar de en ordenadores individuales con mucha menos potencia. De forma adicional, se pueden ejecutar varias sesiones de analistas a la vez en una única o en varias estaciones de trabajo usando las configuraciones de servidor de las que dispone la solución. Esta capacidad sirve de ayuda para proteger tanto el sistema como la integridad de la evidencia, para ayudar a prevenir la necesidad de regeneraciones de la estación de trabajo

si se ejecutan por error códigos maliciosos y para ayudar también a mantener la cadena de custodia, obviando la necesidad de regeneraciones de la estación de trabajo del analista cuando se pasa de un caso a otro. En el entorno de Digital Forensics, *cadena de custodia* puede definirse como el mantenimiento de la integridad de los datos digitales como evidencia desde el momento en que se recogen, mientras se informa de los hallazgos y hasta el momento en que se presenta en los tribunales.

Presentación

Con la solución Digital Forensics de Dell, los equipos de visualización y los investigadores pueden acceder a la evidencial potencial del caso de un modo seguro y en tiempo real, por lo que se reduce la necesidad de trasladar la evidencia a discos DVD o de requerir que algún experto tenga que desplazarse al laboratorio con el fin de acceder a los archivos.

Archivado

La solución de Dell ofrece una infraestructura formalizada de copias de seguridad, recuperaciones y archivado que ayudan a optimizar la cooperación entre los organismos y los departamentos de seguridad e incluso a través de las fronteras, liberando la sobrecarga administrativa, proporcionando coherencia entre los laboratorios y minimizando los riesgos de la cadena de custodia digital.

De forma adicional, la guía de la solución Digital Forensics de Dell incluye un componente de búsqueda opcional que permite la correlación de información entre los conjuntos de datos examinados.

La solución de Dell simplifica los puntos difíciles del sector

La solución Digital Forensics de Dell puede hacer que el proceso de llevar la evidencia digital de la escena del delito a los tribunales sea infinitamente más sencillo para los profesionales de la investigación ofreciendo:

- Una vanguardista red de centros de datos que acelera el examen, análisis y uso compartido de la información digital.
- Seguridad de la información automatizando más el proceso forense digital, disminuyendo así el riesgo de errores y el compromiso de los datos.

- Seguridad adicional de la integridad de los datos actualmente a través del uso de los protocolos hash más seguros y pronto a través de la aplicación de una prestación de auditoría que ayudará a automatizar los registros de la cadena de custodia.

NOTA: Cualquier conclusión o recomendación de este documento que pueda parecer un consejo de tipo legal deberá someterse a un completo asesoramiento jurídico. Consulte siempre con su jurisdicción local, la fiscalía y el laboratorio forense local todo lo relacionado con sus métodos preferidos de recogida de la evidencia digital.

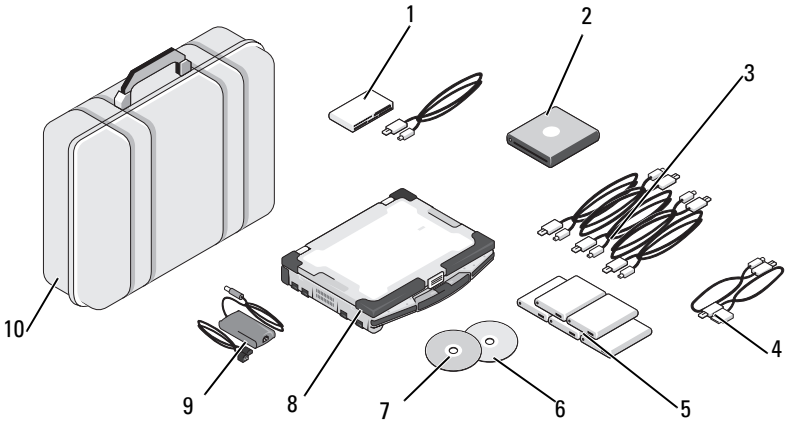
- Una solución integral que reduce considerablemente la complejidad de la planificación, aplicación y gestión del proceso forense digital a nivel de empresa.
- Una solución asequible y flexible que es modular y escalable y que se puede ampliar y pagar conforme se precise.

Componentes de la solución

En el terreno

La parte móvil de la solución entra en un maletín diseñado para caber en el portaequipajes del avión. El maletín reforzado lleva todas las herramientas y software que se necesitan para el triaje en el sitio de dispositivos de almacenamiento sospechosos e incluye un portátil reforzado Dell E6400 XFR con el software de informática forense SPEKTOR preinstalado, Tableau Forensics Write-Blockers con accesorios, un número opcional de discos duros USB externos con licencia para trabajar con el software SPEKTOR como *colectores* de imágenes de triaje, un lector de tarjetas 50:1 y los adaptadores y cables que se muestran en la Ilustración 1-2.

Ilustración 1-2. Solución Digital Forensics de Dell: componentes móviles



1	Lector de tarjetas 50:1	6	Disco de restauración de imágenes
2	ROM DVD USB	7	Disco de inicio SPEKTOR
3	Cables USB de colectores	8	Portátil reforzado de Dell
4	Opción de cables de teléfono para SPEKTOR PI (opcional)	9	Fuente de alimentación del portátil reforzado Dell
5	Colectores externos de disco duro (5)	10	Maletín Pelican

En el centro de datos

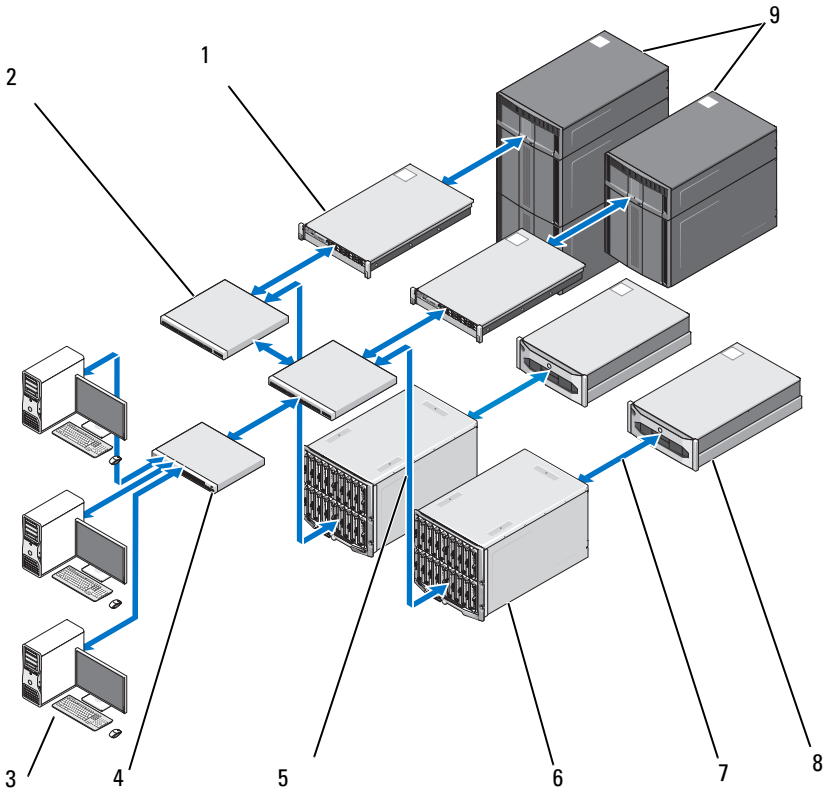
En el centro de datos, la solución Digital Forensics de Dell incluye una configuración personalizada compuesta por los siguientes componentes:

- Rack Servers Dell PowerEdge R410, R610 y R710
- Blade Servers Dell PowerEdge M610 y M710
- Dell EqualLogic serie 4000\6000 SAN
- Windows Server 2008 R2
- Citrix XenApp 6.0
- AccessData FTK 1.8, AccessData FTK 3, AccessData Lab
- Guía EnCase 6.15

- Software NTP On-Demand Data Management (ODDM)
- Symantec Enterprise Vault
- Symantec Backup Exec 2010
- Conmutadores Dell PowerConnect
- Conmutadores de redes extremas

Dell PowerEdge Rack y Blade Servers pueden realizar varias funciones: servidor de archivos, servidor de evidencias, servidor de archivado, servidor de bases de datos, servidores de licencias de EnCase y FTK, servidor de copias de seguridad o controlador de dominios. Son compatibles con Microsoft Active Directory y con todo el software de seguridad e informática forense que componen la solución Digital Forensics de Dell.

Ilustración 1-3. Solución Digital Forensics de Dell: centro de datos



1	Servidor PowerEdge R410 o servidor R610 (opcional)	6	Dell PowerEdge M1000E y M610 Blade Servers
2	Conmutadores Dell PowerConnect	7	Transmisión de datos de 10 GB
3	Estación de trabajo Dell Precision u OptiPlex	8	Sistemas de almacenamiento Dell EqualLogic series PS4000 o PS6000
4	Conmutadores Dell PowerConnect	9	Almacenamiento de clase Dell PowerVault ML
5	Transmisión de datos de 1 GB		

Acerca de este documento

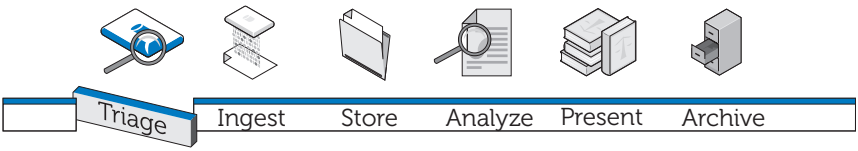
Este documento cubre cada una de las etapas del proceso de informática forense digital de su propio capítulo con capítulos adicionales sobre la solución de problemas, hardware y software compatible con la solución. Cada uno de los capítulos del proceso empieza con una exposición de las buenas prácticas y problemas específicos que se pueden encontrar al aplicar y gestionar la solución, pasando después a un examen de las diferentes herramientas y componentes relativas a dicha etapa de la solución.

Documentación relacionada y recursos

Puede acceder a información adicional en la página **support.dell.com/manuals.**

2

Triaje



¿Qué es el triaje?

El triaje permite a los investigadores de informática forense examinar los datos que contienen dispositivos sospechosos y tomar decisiones en relación con los que realmente presentan evidencias y es necesario incautar para la creación de imágenes sobre la marcha (si los datos representan un pequeño volumen) o para una posterior investigación en el centro de datos. La posibilidad de previsualizar e incautar solamente algunos dispositivos seleccionados puede reducir considerablemente los retrasos que afectan a la capacidad de los investigadores para presentar evidencias de un modo puntual. El triaje puede reducir la acumulación de dispositivos de almacenamiento a la espera de una investigación en el laboratorio de informática forense, empleando menos recursos, evitando agregarlos a una cola de examen ya sobrecargada y reduciendo espectacularmente los costes de funcionamiento.

Ventajas de la solución de triaje de Dell

Movilidad

El investigador puede llevar consigo la solución Digital Forensic de Dell al lugar del delito. Todos los componentes han sido previamente probados en profundidad, cubriendo una amplia gama de puertos y conectores de dispositivos que es previsible encontrar en el lugar de trabajo.

Rapidez

Las actuales soluciones de triaje de la informática forense pueden resultar lentas y es posible que incluso pierdan datos debido a que realizan tareas como la búsqueda de palabras clave o la coincidencia de hash durante la recogida de

los datos. La solución Digital Forensics de Dell resuelve este obstáculo usando la potencia informática de los equipos portátiles reforzados de Dell en lugar de los PC para realizar el análisis de los datos recogidos. En algunos casos, se podrán omitir a la vez los procesos de creación de imágenes e indexación en el laboratorio de informática forense.

Facilidad de uso

Los componentes de triaje de la solución están listos para poder usarse con toda facilidad. El software preinstalado ofrece una intuitiva interfaz de pantalla táctil. Para una implementación estándar, se pueden crear perfiles de colecciones reutilizables definidos por el usuario con los diferentes escenarios.

Informática forense aceptable

El software de triaje ejecuta un proceso forense informático aceptable, asegurando que se capte, revise y almacene sin compromiso cualquier evidencia potencial.

Flexibilidad

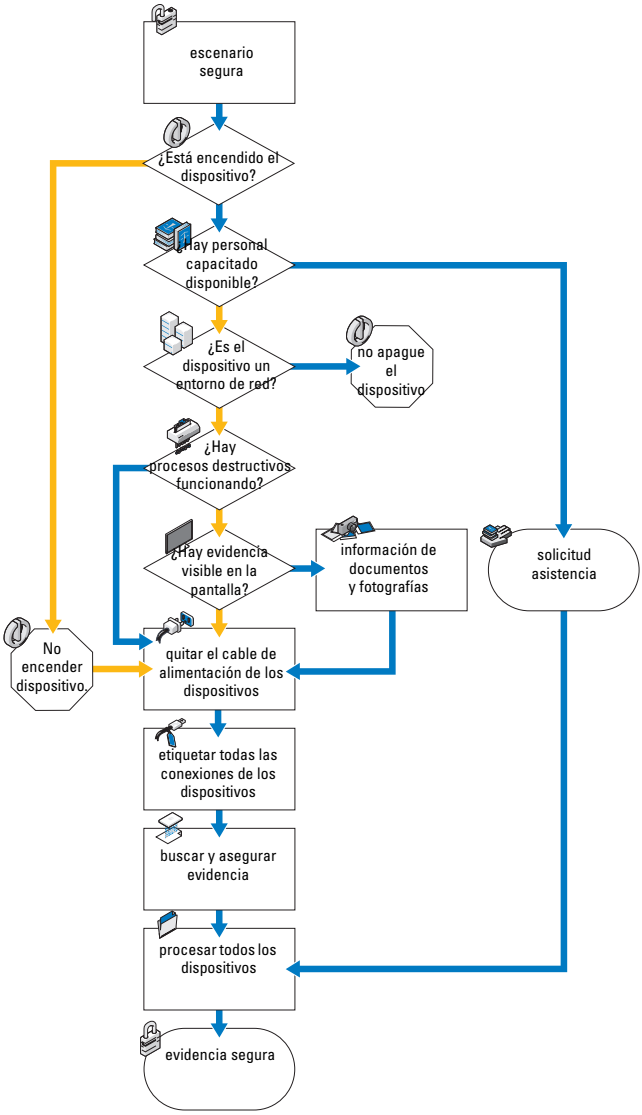
Los componentes de triaje pueden usarse para examinar los dispositivos y plataformas digitales de almacenamiento más comunes, incluyendo dispositivos que funcionen con los sistemas operativos tanto Windows como Mac OS X de Apple, así como con un amplio abanico de tipos de dispositivos de almacenamiento digital, como reproductores de MP3, discos duros externos, tarjetas de memoria, teléfonos móviles y por satélite, unidades de GPS, iPads e iPhones y unidades flash. Además, los resultados del triaje usando la solución Digital Forensics de Dell son exportables a otros programas.

Potencia

El portátil reforzado de Dell controla todo el proceso, desde la realización de un análisis automatizado de los datos seleccionados hasta la presentación de los resultados en un sencillo formato de informe unos minutos después de la captura de los datos. Empleando la solución de Dell, el investigador podrá ejecutar varias exploraciones de triaje en paralelo con una única clave de licencia.

Recogida de evidencias de Digital Forensics

Ilustración 2-1. Flujo de trabajo de la recogida



Adquisición estándar o en vivo

La solución Digital Forensics de Dell ofrece dos tipos de adquisición: estándar y en vivo. Durante los procedimientos de adquisición estándar, el portátil reforzado de Dell utiliza el disco de inicio SPEKTOR para capturar datos de triaje de dispositivos de almacenamiento seleccionados que ya están apagados. Por otra parte, los procedimientos de triaje por adquisición en vivo dirigen la captura de datos de triaje desde un dispositivo de almacenamiento seleccionado que todavía está encendido, obteniendo evidencias que de otro modo no estarían disponibles.

Anteriormente, las normas del sector requerían que el investigador desenchufara e incautara el dispositivo para llevarlo al laboratorio con el fin de poder examinarlo. Esta práctica implica la pérdida de una evidencia potencialmente valiosa en forma de datos volátiles guardados: cualquier dato guardado en el portapapeles, archivos abiertos, contenidos de la RAM, contraseñas registradas, etc. Además, se pueden perder datos cifrados si se apaga el ordenador antes de generar la imagen del disco. Aparte de esto, muchos ordenadores tienen contraseña de la BIOS y el disco duro que determina el propio usuario. Desconectar la alimentación de los sistemas encendidos con contraseña de la BIOS puede provocar la pérdida del acceso a todo el contenido del dispositivo.

Las buenas prácticas requieren que el investigador trate los dispositivos de almacenamiento de datos sospechosos con las siguientes directrices en mente:

- Si el dispositivo está encendido, manténgalo así mientras sea posible hasta que se pueda realizar una investigación completa.
- Si el dispositivo está apagado, déjelo como está.

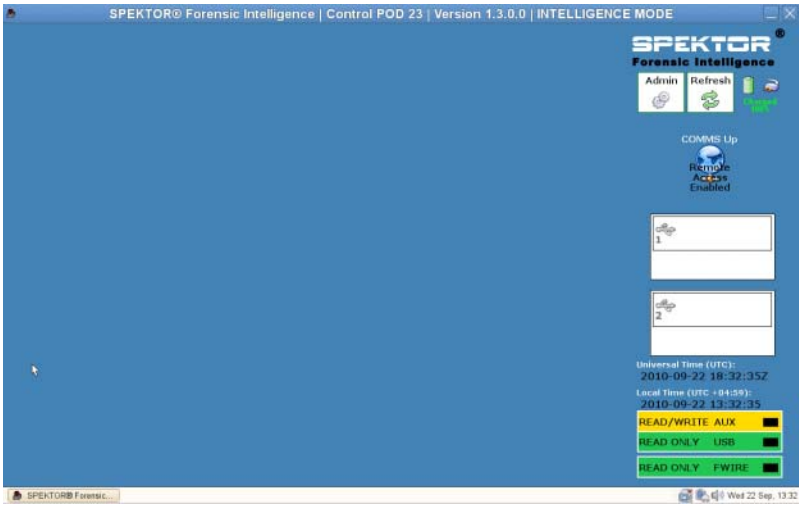
La razón de estas directrices es que el investigador deber tener cuidado de conservar el dispositivo de almacenamiento como lo encuentre y realizar el menor número de cambios posible tanto en el dispositivo como en lo que contiene.

Cómo realizar el triaje usando la solución Digital Forensics de Dell

Encienda el portátil reforzado de Dell

1. Pulse el botón de encendido para iniciar el portátil reforzado de Dell. El portátil carga automáticamente el software SPEKTOR.
2. Toque o haga clic en **Accept EULA**. Se abrirá la pantalla **Home**.

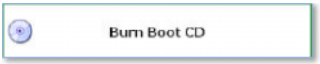
Ilustración 2-2. Pantalla Home



Grabación de un CD de inicio para los procedimientos de adquisición estándar

1 En la pantalla **Home**, toque o haga clic en **Admin**. Después toque o haga clic en **Burn Boot CD**.

Ilustración 2-3. Grabación de CD de inicio en la pantalla Home



2 Siga las instrucciones que aparecen en la pantalla y haga clic en **Finish**.

Registro de colectores o discos de almacenamiento

NOTA: Los colectores deben estar autorizados y configurados por SPEKTOR antes de poder usarse con la solución Digital Forensics de Dell. Póngase en contacto con su administrador de sistema si necesita colectores o licencias adicionales.

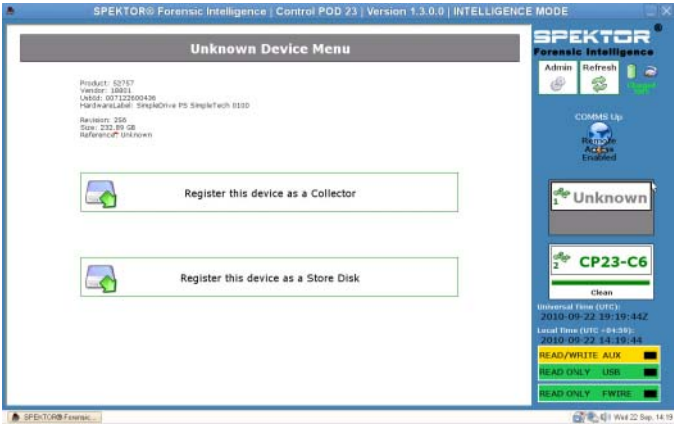
1 Enchufe un nuevo colector o disco de almacenamiento a uno de los puertos USB de la izquierda del portátil reforzado Dell. El dispositivo aparece en la pantalla como dispositivo sin reconocer.

Ilustración 2-4. Indicador de estado de colector o disco de almacenamiento desconocido

2 Toque o haga clic en el icono **Status Indicator** que corresponde con el colector o disco de almacenamiento que ha enchufado en el portátil reforzado Dell. El icono del dispositivo que ha sido registrado se pondrá en verde (para los colectores) o en naranja (para los discos de almacenamiento).

3 Se mostrará **Unknown Device Menu**.

Ilustración 2-5. Menú de dispositivo desconocido



4 Toque o haga clic en **Register this device as a Collector** o **Register this device as a Store Disk**.

5 Toque o haga clic en **Yes**.

El indicador de estado mostrará el número del nuevo colector o disco de almacenamiento y su estado cambiará a **Dirty**.

Ilustración 2-6. Iconos de colector o disco de almacenamiento sucios

NOTA: Los colectores y los discos de almacenamiento, bien se hayan registrado recientemente o hayan sido usados previamente en otras recogidas de datos, deberán estar limpios antes de poder implementarse en un destino.

6 *Con los discos de almacenamiento solamente*, introduzca el número de serie del disco.

Limpieza de colectores o discos de almacenamiento

NOTA: Espere aproximadamente dos horas por 100 GB de volumen de colector.

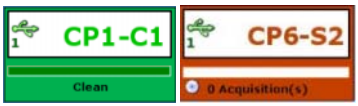
1 Seleccione el **indicador de estado** que represente el colector que desee limpiar.

2 En el **menú de colector** toque o haga clic en **Clean Collector**.

3 Toque o haga clic en **Yes** para confirmar la selección. Comenzará la limpieza y el **indicador de estado** confirmará el progreso de ésta.

Cuando se haya completado la limpieza, el software ejecutará un programa de verificación para confirmar que solo son ceros los caracteres de la unidad del colector.

Ilustración 2-7. Indicadores de estado de Registado y Colector y disco de almacenamiento limpios



NOTA: Si el proceso de limpieza no ha sido correcto, el indicador de estado indicará que el colector permanece sucio. Será necesario volver a iniciar el proceso de limpieza. Si la limpieza no ha sido correcta por segunda vez, pruebe otro colector o disco de almacenamiento.

Configuración de un perfil de colector

NOTA: De forma predeterminada, los parámetros de configuración del software de triaje están ajustados para no recoger archivos. Especifique un subconjunto restringido de todos los archivos del dispositivo de destino para disminuir el tiempo de recogida y evitar exceder la capacidad del colector.

Configurar un colector permite al usuario determinar una serie de tipos de archivos o archivos específicos creados entre un grupo específico de fechas que el colector recogerá del dispositivo de almacenamiento sospecho para el triaje. Cuanto más se puedan restringir los parámetros de recogida, más rápidamente se podrán obtener los datos objetivo para su revisión.

Dell recomienda establecer un conjunto de perfiles de configuración estándar que usted o la agencia puedan encontrar repetidamente. A continuación se indican algunos ejemplos de dichos perfiles de configuración estándar:

- Las fotos y vídeos capturarían tipos de archivos como ***.jpg**, ***.png**, ***.swf**, ***.vob** y ***.wmv**, que están asociados con fotografías, vídeos y otros tipos de soportes visuales.
- Los documentos recogerían específicamente tipos de archivos como todos los ***.pdf**, ***.doc**, ***.docx**, ***.txt**.
- Los archivos de audio se reunirían en archivos como ***.mp3**, ***.mp4**, ***.wav** y otros tipos de archivos de audio.

Configuración de un colector para la adquisición

NOTA: Para ver una explicación sobre las diferencias entre adquisiciones estándar y en vivo, consulte "Adquisición estándar o en vivo" en la página 20.

NOTA: Cuando un colector esté configurado para adquisición estándar o en vivo, será necesario limpiarlo antes de que se pueda volver a configurar para su uso en otro tipo de adquisición.

1 En el **menú de colector**, toque y haga clic en **Configure Collector**.

Ilustración 2-8. Menú de colector

2 Si ha creado previamente un perfil de configuración que desee usar, selecciónelo y toque o haga clic en **Configure using selected profile** para iniciar la configuración del colector; en caso contrario, toque o haga clic en **New** para crear un nuevo perfil.

NOTA: La Ilustración 2-9 muestra la pantalla **Selected Profile** en el primer uso del software antes de que se haya definido y guardado ningún perfil. Cuando haya empezado a crear perfiles de configuración, aparecerán en esta pantalla para su uso.

NOTA: Pasar de una de las pantallas de configuración de colector a la siguiente se realiza tocando o haciendo clic en los botones de las flechas izquierda y derecha situadas en la parte superior y a un lado de la pantalla.

Ilustración 2-9. Seleccionar perfil

3 Determine el tipo de adquisición que desee realizar, en vivo o estándar (consulte "Adquisición estándar o en vivo" en la página 20 para ver información sobre la diferencia entre los tipos de adquisición en vivo o estándar). A continuación, toque o haga clic en **Live Acquisition** o en **Standard Acquisition**.

Ilustración 2-10. Paso de configuración de perfil 1: tipo de adquisición

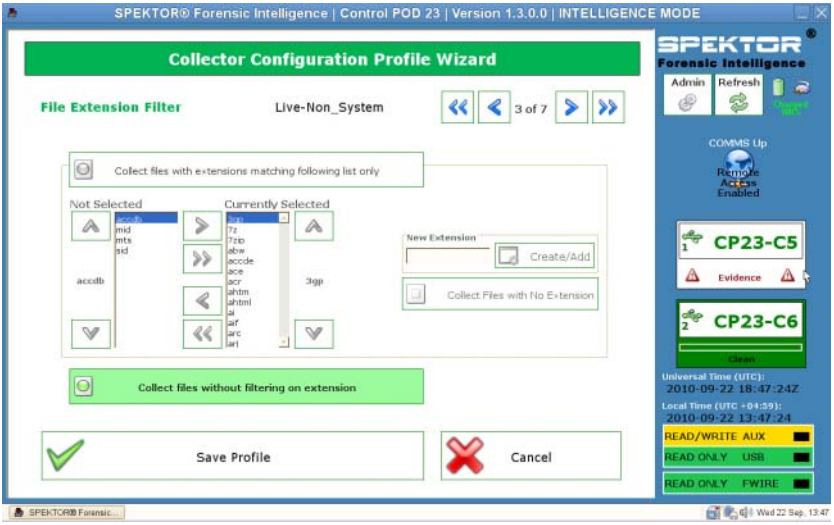
4 Determine la configuración de marca de hora del nuevo perfil. Cuanto más específico sea, menos tiempo tardará el proceso de los archivos capturados.

Ilustración 2-11. Paso de configuración de perfil 2: configuración de la marca de hora de los archivos

5 Haga clic en la flecha a la derecha de la esquina superior derecha de la pantalla.

6 En la pantalla **File Extension Filter**, seleccione los tipos de archivo que desee recoger. Utilice la flecha a la derecha para mover los tipos de archivos seleccionados y las extensiones asociadas de **Not Selected** al recuadro de lista **Currently Selected**.

Ilustración 2-12. Paso de configuración de perfil 3: filtro de extensión de archivos



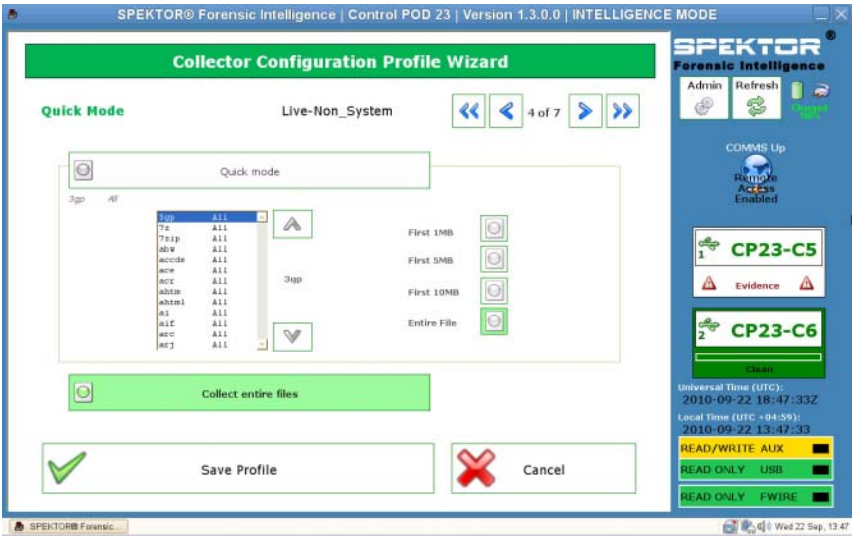
7 Haga clic en la flecha a la derecha de la esquina superior derecha de la pantalla cuando haya terminado de seleccionar tipos de archivo y extensiones.

NOTA: A menos que específicamente se requiera, se recomienda salir del Quick Mode.

8 En la pantalla **Quick Mode**, seleccione el número de megabytes (**1 MB**, **5 MB**, **10 MB** o **Entire File**) de la primera parte de archivos que desee capturar. Recogiendo solo la primera parte de archivos muy grandes (normalmente archivos multimedia), podrá revisar lo suficiente de los archivos para determinar su contenido, al tiempo que se minimiza la cantidad de tiempo de procesamiento requerida.

NOTA: Si no seleccionó las extensiones de archivo en el paso 6, no se recogerán archivos ni se mostrarán tipos de archivo para la selección en esta pantalla. Vuelva al paso 6 y seleccione los tipos de archivo requeridos para activar en el paso 8.

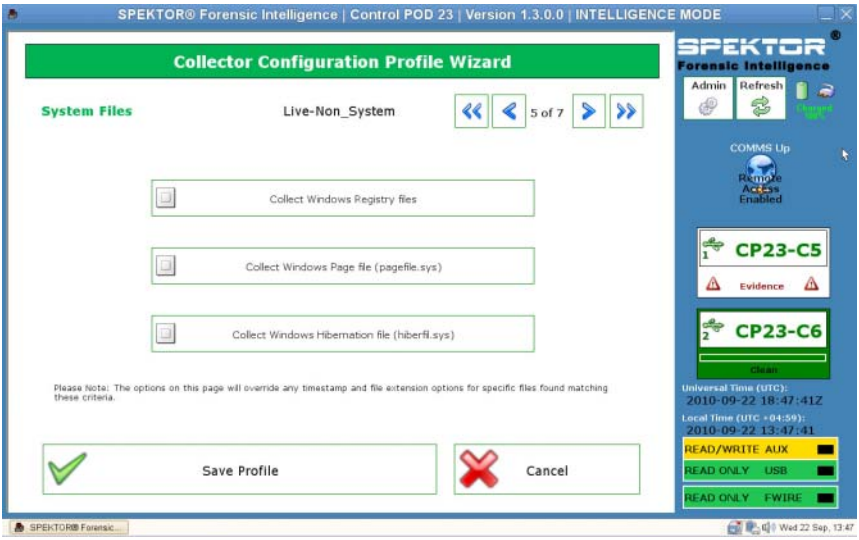
Ilustración 2-13. Paso de configuración de perfil 4: modo rápido



9 Haga clic en la flecha a la derecha de la esquina superior derecha de la pantalla.

10 Toque o haga clic en el botón adecuado para seleccionar cualquier archivo de sistema que desee incluir en la recogida.

Ilustración 2-14. Paso de configuración de perfil 5: archivos de sistema



11 Haga clic en la flecha a la derecha de la esquina superior derecha de la pantalla.

12 En la pantalla **Deleted File Filter**, determine si en la recogida desea incluir o no archivos en vivo y eliminados, solo archivos en vivo o solo archivos eliminados. Si no selecciona ninguna de estas opciones, no recogerá ningún archivo.

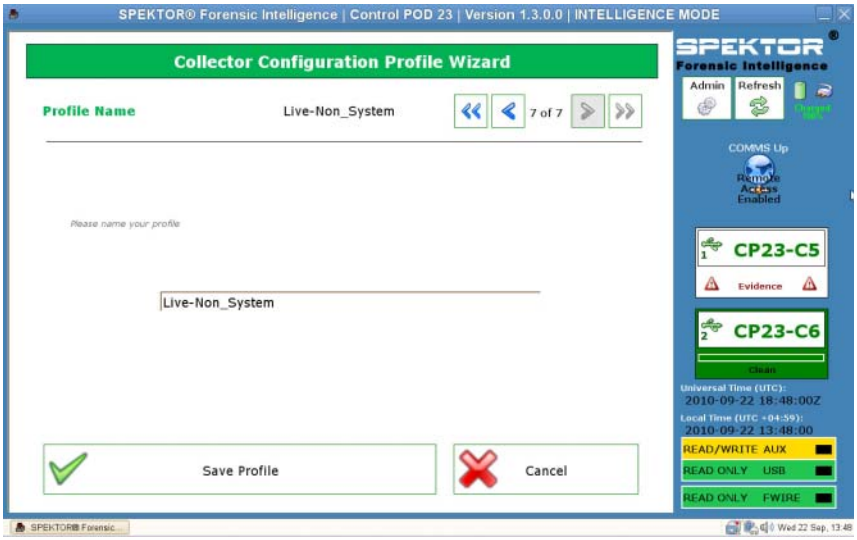
Ilustración 2-15. Paso de configuración de perfil 6: filtro de archivos eliminados

NOTA: Es probable que solo se recojan correctamente archivos eliminados que no se hayan sobrescrito ya en el dispositivo de destino; los archivos que hayan sido eliminados y después sobrescrito estarán dañados o no se podrán recuperar.

13 Haga clic en la flecha a la derecha de la esquina superior derecha de la pantalla.

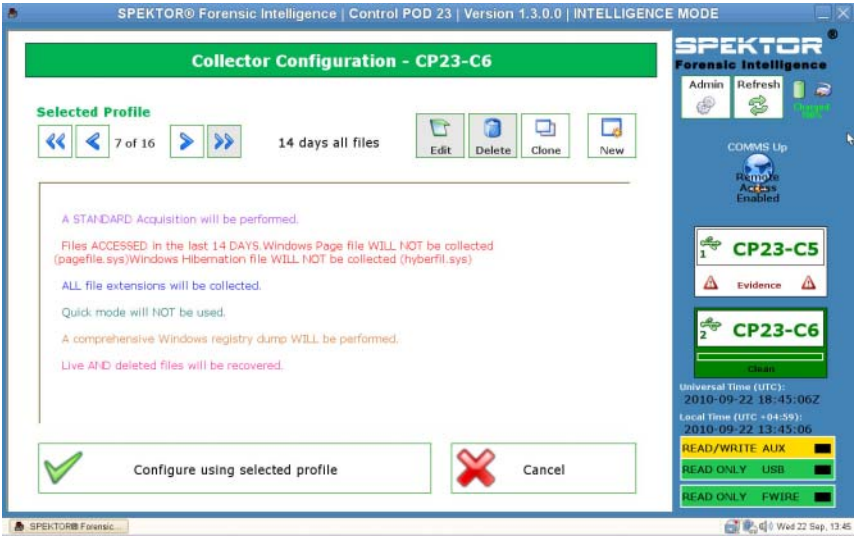
14 En la pantalla **Profile Name**, introduzca un nombre para el nuevo perfil y toque o haga clic en **Save Profile**.

Ilustración 2-16. Paso de configuración de perfil 7: nombre de perfil



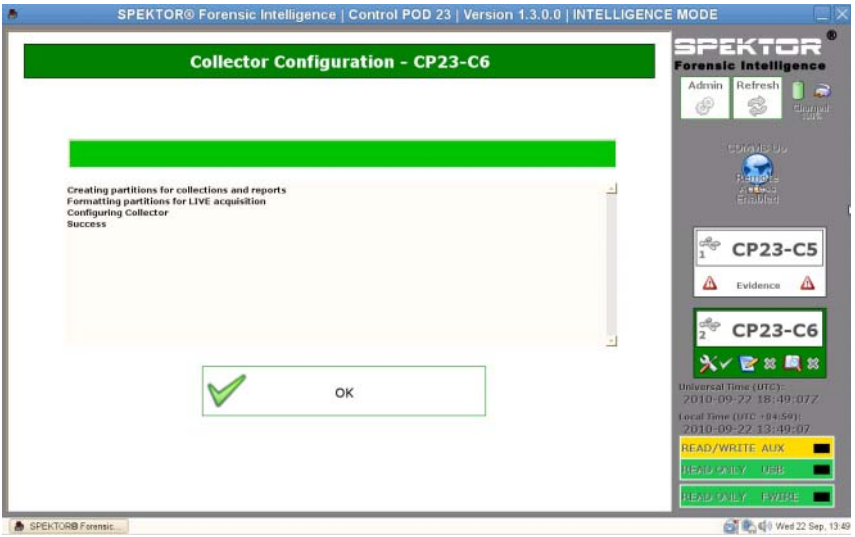
15 Haga clic en la flecha a la derecha de la esquina superior derecha de la pantalla. El nuevo perfil aparece en la pantalla **Selected Profile**. La pantalla **Collector Configuration** mostrará el título del perfil (en este caso, **14 days all files**) y mostrará los datos del perfil en la parte principal de la ventana.

Ilustración 2-17. Perfil seleccionado después de la creación de perfiles



16 Toque o haga clic en **Configure using selected profile** para iniciar la configuración del colector.

Ilustración 2-18. Perfil seleccionado después de la creación de perfiles



17 Toque o haga clic en **OK** para iniciar la configuración del colector. Este proceso tardará solamente uno o dos minutos.

Cuando se haya completado la configuración del colector, éste estará listo para implementarse en el ordenador o dispositivo de almacenamiento de destino. Consulte "Implementación de las herramientas de triaje" en la página 34.

18 Haga clic en la flecha a la derecha de la esquina superior derecha de la pantalla.

Implementación de las herramientas de triaje

NOTA: Para ver las diferencias entre la adquisición en vivo y la estándar, consulte "Adquisición estándar o en vivo" en la página 20.

NOTA: Aunque se puede usar un colector para varios casos, las buenas prácticas recomiendan encarecidamente que cada colector contenga solo los datos que pertenezcan a un único caso, aunque se puedan guardar en el colector datos de varios dispositivos de almacenamiento de ese caso único.

Implementación de un colector para la adquisición estándar frente a un ordenador de destino

AVISO: Antes de intentar una adquisición estándar será necesario cambiar el orden de inicio del sistema desde dentro del BIOS del ordenador de destino. Si el ordenador de destino está configurado para iniciarse desde la unidad de disco duro en lugar de la unidad óptica con el disco de inicio SPEKTOR introducido, los contenidos de la unidad del ordenador de destino se verán alterados. Antes de encender el ordenador de destino, asegúrese de que sabe cómo acceder al BIOS.

AVISO: Antes de encender el ordenador de destino, asegúrese de que ha colocado el disco de inicio SPEKTOR en la unidad óptica del ordenador de destino que está configurado para el inicio. Si no se inicia el ordenador de destino sin el disco de inicio colocado se producirán alteraciones en los contenidos de la unidad del ordenador.

NOTA: Deberá tener un disco de inicio SPEKTOR para conseguir la implementación de una adquisición estándar en el ordenador de destino. Consulte "Grabación de un CD de inicio para los procedimientos de adquisición estándar" en la página 21 para ver información sobre la creación de un disco de inicio.

1. En el portátil reforzado de Dell, toque o haga clic en **Deploy Collector**.
2. Seleccione **Target Computer**.
3. Haga clic en **OK** y desenchufe el colector del portátil reforzado de Dell.
4. Enchufe el colector en un puerto disponible del ordenador de destino.

NOTA: Dell recomienda usar siempre la unidad óptica interna del ordenador de destino con el disco de inicio. Si no es posible, utilice una unidad externa con un conector USB.

5. Coloque el disco de inicio SPEKTOR en la unidad óptica.
6. Acceda al programa BIOS del ordenador de destino y cambie el orden de inicio para que se inicie desde la unidad óptica.

   Se cargará el disco de inicio SPEKTOR mostrándose la interfaz de la unidad de inicio.
7. Introduzca la información solicitada en la pantalla, pulsando <Intro> o las teclas de flechas para moverse entre los campos, vaya al campo **COLLECT** y pulse <Intro> para empezar la recogida de datos.

PRECAUCIÓN: No retire el disco de inicio SPEKTOR de la unidad óptica hasta que se haya apagado por completo el ordenador de destino.

8 Cuando se haya completado el proceso de recogida, pulse <Intro> para apagar el ordenador de destino.

9 Quite el disco de inicio SPEKTOR de la unidad óptica, desenchufe el colector del puerto USB del ordenador de destino y enchúfelo en un puerto USB disponible del portátil reforzado de Dell.

Implementación de un colector para la adquisición estándar frente a un dispositivo de almacenamiento de destino

1 Enchufe el dispositivo de almacenamiento en el puerto USB de solo lectura o en el puerto Firewire del portátil reforzado de Dell.

2 Toque o haga clic en **Deploy Collector**.

3 Toque o haga clic en **Target Storage Device**, introduzca la información requerida y toque o haga clic en **Collect from Device**.

4 Cuando se haya completado la recogida, desenchufe el dispositivo de almacenamiento de destino del puerto USB y toque o haga clic en **OK**.

Implementación de un colector para la adquisición en vivo

NOTA: Durante este procedimiento asegúrese de realizar notas precisas y detalladas como parte de las buenas prácticas de la cadena de custodia.

NOTA: No se necesita el disco de inicio SPEKTOR para la implementación de la adquisición en vivo.

1 Haga clic en **Deploy Collector→ Target Computer**.

2 En el ordenador de destino vaya a **Mi PC** (o **Equipo** en los equipos que funcionen con Windows Vista o Windows 7).

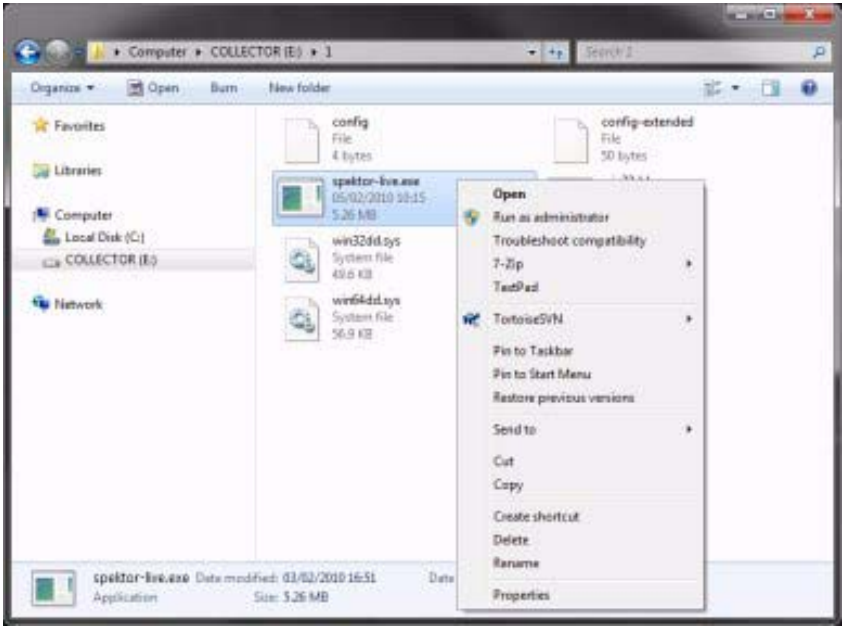
3 Haga doble clic en el icono **Collector** cuando aparezca para ver los contenidos en el colector.

Ilustración 2-19. Icono Collector

4 Haga clic en la carpeta que tenga el nombre con el número más alto. Si ésta es la primera implementación desde la limpieza de este colector, aparecerá solo una carpeta.

5 Haga clic en **spektor-live.exe** y seleccione **Ejecutar como administrador** en el recuadro desplegable. Si aparece un mensaje pidiéndole permiso para ejecutar la aplicación como administrador, haga clic en **Continuar**.

Ilustración 2-20. Ejecutar como administrador



6 Introduzca la información solicitada en la pantalla **SPEKTOR Live Collection** y haga clic en **Run**.

7 Cuando se le solicite, haga clic en **Close**.

8 Desconecte el colector del dispositivo de destino y guárdelo en un sitio seguro para una posterior investigación en el centro de datos.

Revisión de los archivos recogidos después del triaje

1 En **Menu Collector** haga clic en **Reporting**. Esta opción indexa los datos recogidos y crea un conjunto de informes automáticamente.

2 En la pantalla **Collector Collections**, seleccione un **Main Report** y haga clic en **Generate Selected Reports**.

Ilustración 2-21. Generar informes

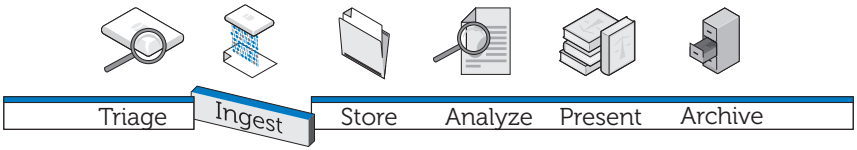
3 Haga clic en **OK** cuando se haya completado el proceso de generación del informe para volver al menú **Reporting**.

NOTA: Consulte el manual del usuario de SPEKTOR para ver más información sobre la creación y exportación de informes usando criterios específicos. Consulte "Documentación relacionada y recursos" en la página 16.

4 Haga clic en **View Collection Report** para ver los informes y haga clic en las cinco categorías de informe, **Images**, **Documents**, **Multimedia**, **Other** o **System** para ver informes específicos.

3

Examen



La etapa de examen consta de la creación de una imagen del dispositivo de almacenamiento de destino (si todavía no se ha hecho durante la etapa de triaje), transfiriendo después dicha imagen a una ubicación centralizada desde la que se pueda acceder para el análisis. Para mover las aplicaciones forenses al centro de datos conservando aún la experiencia del usuario estándar, Dell, en asociación con Citrix, ha creado varios paquetes distintos de software para que las principales aplicaciones forenses se puedan mover sin problemas al centro de datos, creando una experiencia de usuario más disponible, más rápida y capaz.

Como parte de la solución Digital Forensics, actualmente Dell ha certificado las siguientes aplicaciones forenses:

- SPEKTOR
- EnCase 6
- FTK 1.8
- FTK 3 versión independiente
- FTK 3 Lab

Se puede usar cualquiera de estas aplicaciones forenses en cualquier combinación para el acceso simultáneo desde un único dispositivo de usuario.

EnCase 6 con centro de datos activado

En el siguiente ejemplo de solución, la aplicación EnCase 6 está alojada en un dispositivo o dispositivos servidores de Dell del centro de datos, proporcionando sesiones multiusuario de EnCase 6.

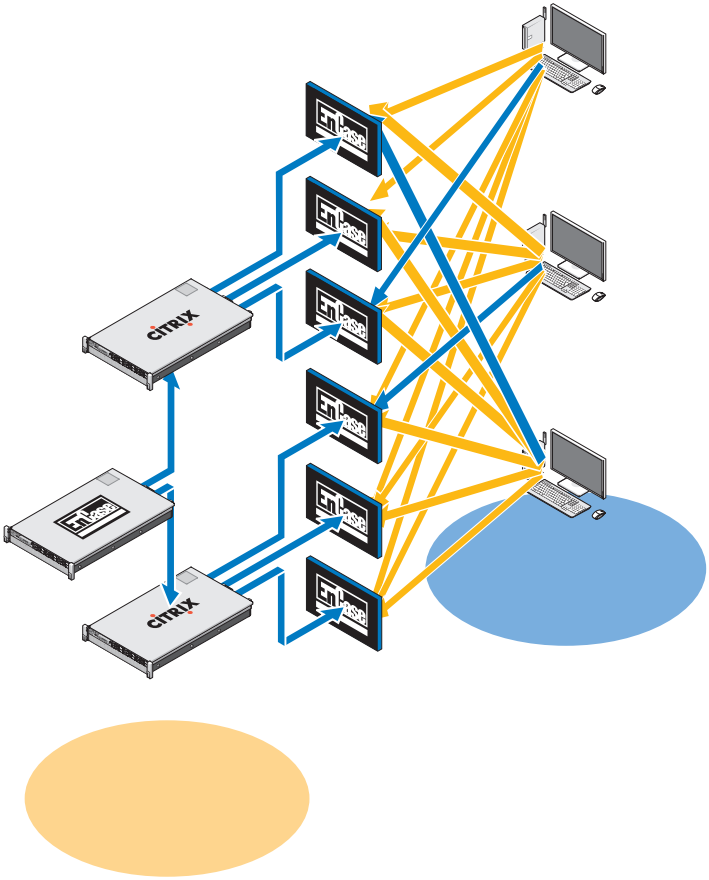
Solución de servidor único

En la solución de servidor único EnCase 6 se pueden conectar varios clientes a un servidor. Todos los clientes apuntan a este servidor y no se pueden conectar a otro servidor de EnCase 6. En el caso de que se produzca un fallo del servidor, se perderán todas las conexiones de cliente.

Solución multiservidor (alta disponibilidad)

En la solución multiservidor, los usuarios se conectarán a la aplicación EnCase 6 del conjunto de servidores de Citrix y se dirigirán sin problemas al servidor de EnCase 6 que esté trabajando con la carga más ligera. En el caso de que el usuario esté funcionando en varias instancias del software EnCase 6, cada instancia podrá ser creada por un servidor diferente. Se conservaría la experiencia del usuario debido a que éste no tendría ninguna constancia de la forma en que se crean varias instancias, pareciendo que todas las secciones funcionan desde el mismo servidor con la misma apariencia y la misma sensación.

Ilustración 3-1. Cliente de EnCase 6 con centro de datos activado/Server Schematic



En el caso de que se produzca un fallo del servidor, el usuario tendría que hacer clic de nuevo en el icono del escritorio de la aplicación EnCase y el sistema redirigirá la conexión del usuario al siguiente alojamiento de servidor disponible de EnCase 6. Cada servidor EnCase puede admitir *x* sesiones de usuario, en donde *x* = *(número de núcleos x 2)*. Cada sesión de usuario requiere 3 GB de RAM del servidor.

FTK 1.8 con centro de datos activado

En la solución FTK 1.8 con centro de datos activado, la aplicación FTK 1.8 está alojada en un dispositivo o dispositivos de servidor de Dell del centro de datos, proporcionando sesiones de FTK 1.8 multiusuario (una única sesión de usuario por servidor).

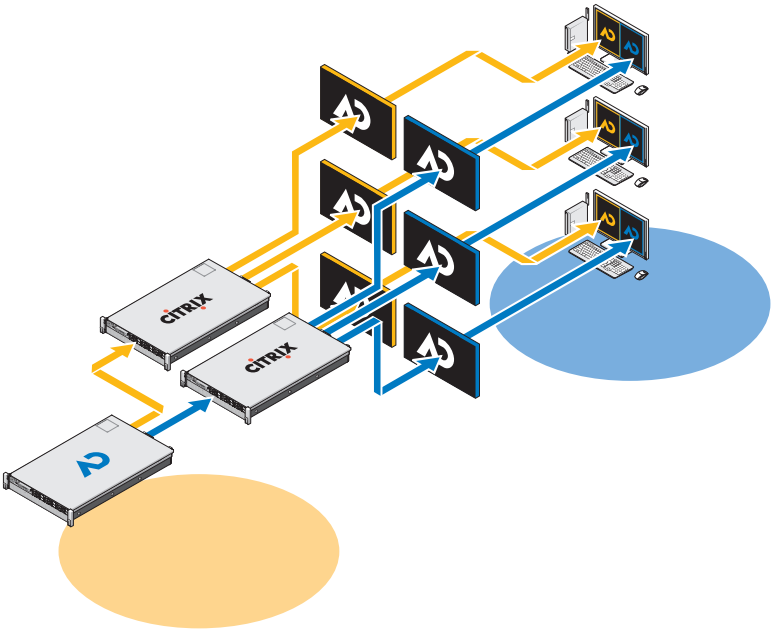
Sesión de FTK 1.8 única por escritorio

En la solución FTK 1.8 de servidor único, se pueden conectar varios clientes a un único servidor. Todos los clientes apuntan a este servidor y no se pueden conectar a otro servidor FTK 1.8. En el caso de que se produzca un fallo del servidor, se perderán todas las conexiones de cliente. El usuario puede ejecutar solamente una sesión de FTK 1.8 por cada cuenta de usuario de Windows.

Varias sesiones de FTK 1.8 por escritorio

En la solución FTK 1.8 multiservidor, los usuarios se conectarán a los servidores FTK 1.8 empleando varios iconos de escritorio FTK Server1, FTK Server2, etc. Cada vínculo está asociado con un servidor específico. A efectos ilustrativos, la Ilustración 3-2 muestra el borde de la sesión de servidor FTK 1.8 funcionando con una codificación de colores para el servidor que ejecuta la sesión de FTK 1.8 (servidor1 = azul, servidor2 = rojo). No se pueden ejecutar dos sesiones de la aplicación FTK 1.8 desde el mismo servidor usando la misma cuenta de usuario. La experiencia de usuario de la aplicación FTK 1.8 basada en servidor es la misma en todos los clientes.

Ilustración 3-2. Multiple FTK 1.8 Client y Server Schematic



Si se produjera un fallo del servidor, el usuario perdería el acceso a la correspondiente sesión del servidor de FTK 1.8. En este caso, para funcionar el usuario tendría que continuar usando los otros servidores FTK. Toda la información del caso y de la evidencia (asumiendo que el usuario tenga privilegios de acceso NAS) se encuentra disponible desde todas las sesiones de servidor de FTK 1.8 a través del NAS/SAN compartido.

Cada servidor FTK 1.8 puede admitir *x* sesiones de usuario, en donde *x* = *(número de núcleos x 2)*. Cada sesión de usuario requiere 3 GB de RAM del servidor y 1000 E/S por segundo de rendimiento de disco del centro de datos.

FTK 3 con centro de datos activado

En la solución FTK 3 con centro de datos activado, la aplicación está alojada en un dispositivo o dispositivos de servidor Dell del centro de datos, proporcionando una única sesión de la aplicación FTK 3 por servidor.

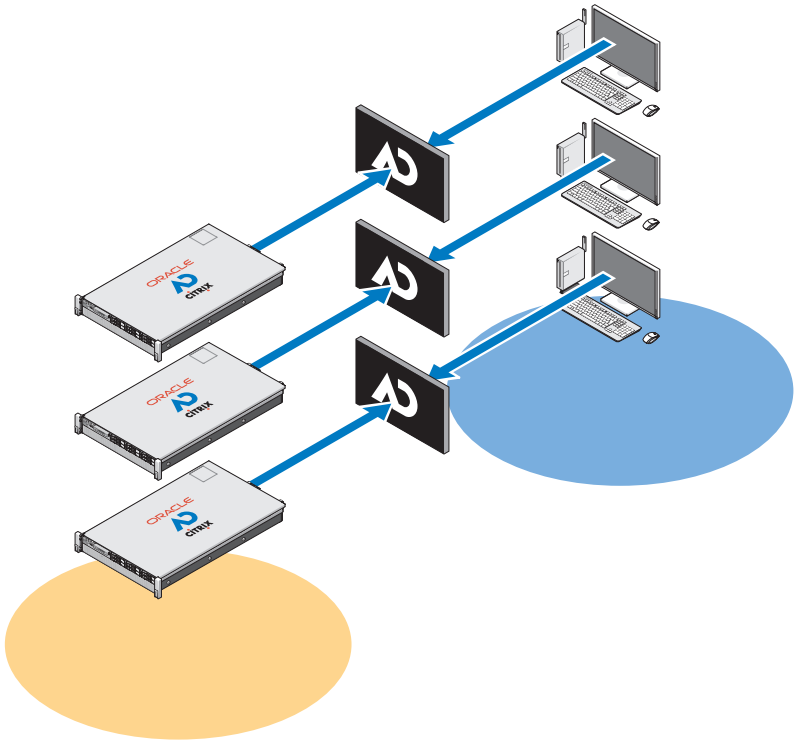
Solución de servidor FTK 3 único

En la solución de servidor FTK 3 único, se puede conectar un solo cliente FTK 3 a un único servidor. El cliente apunta a este servidor y no se puede conectar a otro servidor FTK 3. En el caso de que se produzca un fallo del servidor, se perderá la conexión de cliente. El servidor FTK 3 también ejecutará la base de datos Oracle integrada en el FTK local debido a que esta versión de la base de datos no permite la colaboración entre otras bases de datos Oracle de FTK u otros usuarios FTK.

Solución multiservidor (sin alta disponibilidad)

En la solución de multiservidor, cada cliente se conectará a su propio servidor FTK 3 y no se podrá conectar a ningún otro servidor FTK 3. Cuando un servidor tiene funcionando una sesión de FTK 3, ya no está disponible para aceptar ninguna nueva sesión de cliente de FTK 3: la configuración del software del marco de trabajo forense de Dell hace que los servidores no puedan ejecutar más de una sesión de la aplicación FTK 3 simultáneamente. Permitiendo que se ejecute solo una sesión por servidor, la aplicación FTK 3 multiproceso puede dedicar todos los recursos de servidor disponibles al procesamiento de un caso, mejorando así el rendimiento.

Ilustración 3-3. Cliente de FTK 3 con centro de datos activado y Server Schematic



Usando la edición FTK Standard, cada servidor debe ejecutar una versión local de la base de datos Oracle integrada de FTK (una versión de base de datos Oracle por usuario a la vez). Esta versión de la aplicación FTK y de la base de datos Oracle no permite la colaboración entre otros usuarios de FTK u otras bases de datos Oracle de FTK.

Cada base de datos Oracle tiene un agente de copia de seguridad Oracle en el servidor. De la base de datos se hace copia de seguridad como parte del régimen normal de copias de seguridad (consulte "Archivado" en la página 89 para ver más información).

En el caso de que se produzca un fallo en el servidor, el usuario tendría que conectarse manualmente a otro servidor FTK 3 disponible (si hay disponibles n+1 servidores FTK 3). No obstante, en el caso de que también falle la base

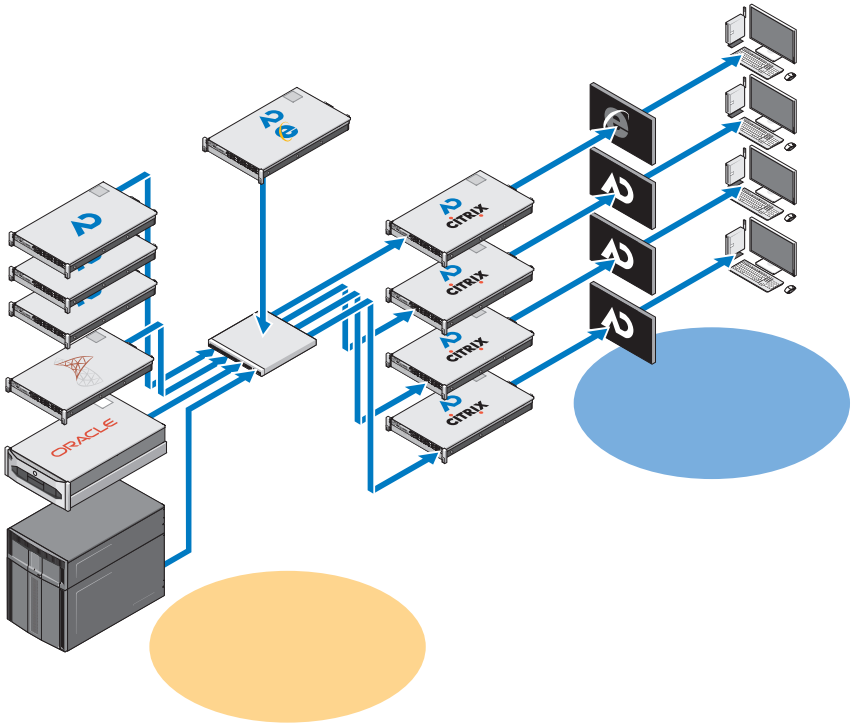
de datos Oracle, no habrá ningún acceso disponible a los casos preexistentes que ya estén procesados puesto que estarán vinculados específicamente a la base de datos Oracle del FTK 3 local original de dicho usuario.

Cada servidor FTK 3 puede admitir una sesión de usuario a la vez. Cada sesión de usuario requiere 64 GB de RAM del servidor (48 GB para Oracle y 16 GB para FTK) y 1000+ E/S por segundo para el almacenamiento de archivos más 600+ E/S por segundo para la base de datos (configuración mínima).

FTK 3 Lab Edition

En la configuración de FTK 3 Lab Edition, el usuario se conectará a un alojamiento de servidor AccessData Lab y la base de datos centralizada del caso. Pueden acceder varios usuarios a la vez al mismo caso y ejecutar diferentes análisis también al mismo tiempo. El procesamiento se realiza usando un modelo de procesamiento distribuido.

Ilustración 3-4. FTK 3 Lab Edition Client y Server Schematic



El almacenamiento de casos se optimiza usando una mezcla de hardware SAS y SATA. Se puede gestionar centralizadamente todo el centro de datos forense mediante un gestor de administración.

Varias aplicaciones forenses situadas en un escritorio

En la solución multiproveedor y multiaplicación se combinan todas las soluciones de aplicaciones individuales previamente descritas para ofrecer al analista forense el acceso a todas las aplicaciones forenses (EnCase 6, FTK 1.8 y FTK 3 o FTK 3 Lab Edition) desde un único escritorio y un único panel de cristal. Todas las aplicaciones se pueden ofrecer en un modo de alta disponibilidad de manera que incluso en el caso de que se produzca un fallo, el usuario todavía tenga acceso a la aplicación específica; y en el caso del FTK 1.8, el usuario tiene acceso utilizando uno de los otros iconos del FTK 1.8 del escritorio.

Recomendaciones para la configuración de la red

Tabla 3-1. Estructura de direcciones IP recomendada

Dirección IP	Función de servidor	Nombre de servidor
192.168.1.1	Controlador de dominio 1	DF-DC1
192.168.1.2	Controlador de dominio 2	DF-DC2
192.168.1.3	Servidor de evidencias	DF-Evidence
192.168.1.4	Servidor de espacios de trabajo	DF-Workspace
192.168.1.5	Servidor de Oracle FTK	DF-FTK
10.1.0.0/24	Rango de direcciones IP estáticas de 1 GB	
10.1.1.0/24	Rango de direcciones IP estáticas de 10 GB	
10.1.2.0/24	Rango de DHCP de 1 GB, clientes	
10.1.0.250-254	Conmutador(es) de 1 GB	
10.1.1.250-254	Conmutador(es) de 10 GB	
10.1.0.200	Servidor DNS	

Tabla 3-2. Convenciones de nombres recomendadas para los servidores de la solución

Nombre	Abreviatura
Nombre de dominio	DF (Digital Forensics)
Controlador de dominio 1	DF-DC1
Controlador de dominio 2	DF-DC2
Almacenamiento de evidencias	DF-Evidence
Espacio de trabajo	DF-Workspace
Oracle	DF-Oracle
SQL	DF-SQL
FTK-Lab	FTK-Lab
FTK-Independiente	FTK
Administrador(es) de procesamiento distribuido	DF-DPM, DF-DPM1, DF-DPM2
Motor(es) de procesamiento distribuido	DF-DPE, DF-DPE1, DF-DPE2

Tabla 3-3. Convenciones de nombres recomendadas para equipos NIC

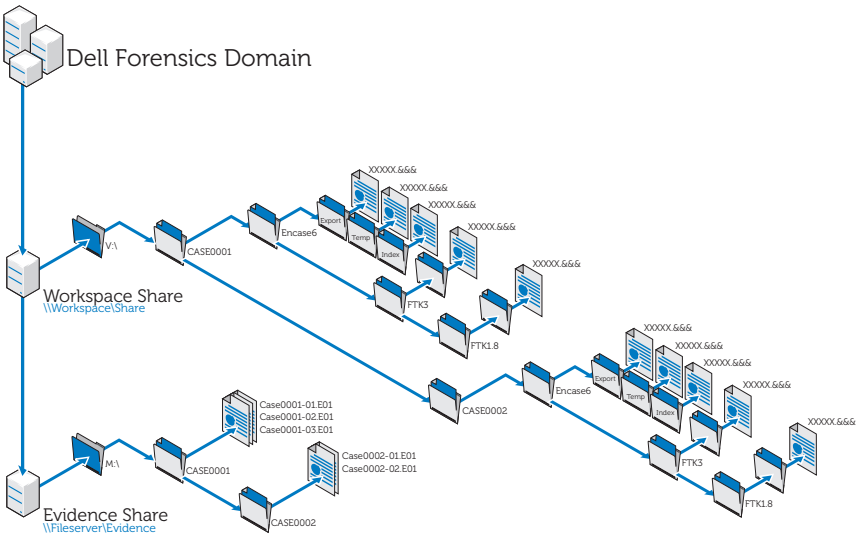
Equipo NIC 1	Red pública	Para servidores conectados entre sí
Equipo NIC 2	iSCSI	Para servidores conectados a dispositivos de almacenamiento EqualLogic

Tabla 3-4. Estructura recomendada de asignación de letras de las unidades

Nombre de la llamada	Unidad	Local o SAN	RAID	Notas
Unidad local	C:	Local	RAID1 (discos 2xSAS 15 K)	
	D:	Local		
CD-ROM	E:			
	F:			
	G			
SQL	H	SAN	RAID0+1	No debe estar en discos SATA
Oracle	I:	SAN	RAID0+1	No debe estar en discos SATA
Unidad EV Vault	J:	SAN	RAID50	
Copia de seguridad en disco	K:	SAN	RAID50	
Sustitución	L:	SAN	RAID50	
Evidencia 1	M:	SAN	RAID50	
Evidencia 2	N:	SAN	RAID50	
Evidencia 3	O:	SAN	RAID50	
Evidencia 4	P:	SAN	RAID50	
Evidencia 5	Q:	SAN	RAID50	
Evidencia 6	R:	SAN	RAID50	
Evidencia 7	S:	SAN	RAID50	

Nombre de la llamada	Unidad	Local o SAN	RAID	Notas
Evidencia 8	T:	SAN	RAID50	
Evidencia 9	U:	SAN	RAID50	
Espacio de trabajo 1	V:	SAN	RAID50	
Espacio de trabajo 2	W:	SAN	RAID50	
Espacio de trabajo 3	X:	SAN	RAID50	
Espacio de trabajo 4	Y:	SAN	RAID50	
Espacio de trabajo 5	Z:	SAN	RAID50	

Ilustración 3-5. Estructura de archivos recomendada



Cómo realizar el examen usando la solución Digital Forensics de Dell

Examen usando SPEKTOR

Registro y limpieza de un dispositivo USB externo como disco de almacenamiento

1. Enchufe el dispositivo USB externo sin registrar en un puerto colector del portátil reforzado.
2. Haga clic o toque el icono del dispositivo cuando aparezca; a continuación toque o haga clic en **Register the Device as a Store Disk→ Yes**. Después introduzca la información solicitada.
3. En el menú de la derecha, seleccione el dispositivo registrado; a continuación toque o haga clic en **Clean/Reformat→ Clean**.
4. Haga clic en **OK** cuando se termine el proceso.

Implementación del disco de almacenamiento

1. Conecte el disco de almacenamiento al portátil reforzado; a continuación toque o haga clic en el dispositivo del disco de almacenamiento para mostrar el **Store Disk Menu**.
2. En este **Store Disk Menu**, toque o haga clic en **Deploy**.

   Si va a realizar la implementación en un ordenador de destino:

   a. Toque o haga clic en **Target Computer**.

   b. Quite el disco de almacenamiento del portátil reforzado y conéctelo en un puerto USB del ordenador de destino.

   c. Siga las mismas instrucciones de implementación que en la captura de imágenes de triaje en "Implementación de las herramientas de triaje" en la página 34.

   d. Cuando se cargue el CD de inicio, el **Asistente de PEKTOR Imaging** le llevará a través del recordatorio del proceso de generación de imagen. Se pueden encontrar instrucciones paso a paso en el *Manual del usuario de SPEKTOR*. Para obtener más información, consulte "Documentación relacionada y recursos" en la página 16.

   e. Apague el ordenador de destino, desconecte el disco de almacenamiento y devuelva el disco al centro de datos para su almacenamiento.

Si va a realizar la implementación en un dispositivo de almacenamiento de destino localmente:

a Toque o haga clic en **Target Storage Device**.

b Enchufe el dispositivo de almacenamiento en el puerto USB de solo lectura o en el puerto FireWire de la parte derecha del portátil reforzado.

c Seleccione la unidad o las particiones que desee reproducir y haga clic en la flecha a la derecha situada en la esquina superior derecha de la pantalla.

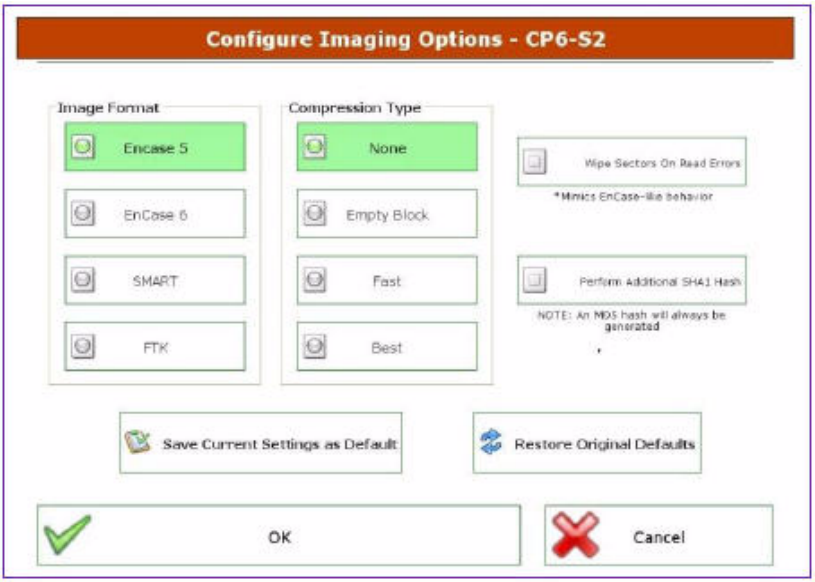
d Introduzca la información del caso solicitada y toque o haga clic en **Image Now**.

e Si es necesario, toque o haga clic en **Configure Imaging Options** para cambiar el formato de imagen (**Image Format**) o el tipo de compresión (**Compression Type**) o para borrar sectores de errores de lectura (**Wipe Sectors on Read Errors**) o realizar hash SHA1 adicionales (**Perform Additional SHA1 Hash**).

NOTA: Los hash MDS se generarán siempre durante el proceso de generación de imágenes.

NOTA: Consulte el *Manual del usuario de SPEKTOR* para ver más información sobre cada una de estas opciones de generación de imágenes. Consulte "Documentación relacionada y recursos" en la página 16.

Ilustración 3-6. Opciones de configurar reproducción de imágenes



f Toque o haga clic en **Image Now→ Yes** para iniciar el proceso de generación de imágenes.

g Cuando se complete el proceso de creación de imágenes, toque o haga clic en **OK**.

h Desconecte el dispositivo de almacenamiento de destino y el disco de almacenamiento del portátil reforzado; después devuelva el disco al centro de datos para su almacenamiento y análisis.

NOTA: La transferencia de una imagen puede tardar mucho tiempo; no es infrecuente seis horas para una transferencia de disco duro de 60 GB.

Examen usando EnCase

En la solución Digital Forensics de Dell, la concesión de licencias de EnCase se realiza usando un sistema de concesión de licencias de red. Normalmente hay instalada una instancia de EnCase SAFE en uno de los servidores del centro de datos y una mochila que contiene varias licencias de usuario conectada a dicho servidor. Los clientes de EnCase están configurados para buscar las licencias en ese servidor, no siendo necesarias otras mochilas locales. Consulte

la *Guía de instalación y configuración de Digital Forensics de Dell* para obtener más información. Consulte "Documentación relacionada y recursos" en la página 16. Consulte también su administrador de sistemas de red para ver información específica sobre la instalación de la solución de su organismo.

1. Conecte el dispositivo de almacenamiento de destino a la estación de trabajo de examen adecuada del centro de datos.
   a. Si va a reproducir la imagen de una unidad SATA, consulte "Conexión del Tableau Write-Blocker a un disco duro SATA" en la página 55 para ver más información.
   b. Si va a reproducir la imagen de una unidad IDE, consulte "Conexión del Tableau Write-Blocker a un disco duro IDE" en la página 56 para ver más información.
2. Cree un nuevo caso.

NOTA: Las siguientes instrucciones se refieren a la estructura de red y de carpetas reseñadas como buenas prácticas recomendadas por Dell para su solución Digital Forensics; consulte Ilustración 3-5 para obtener más información.

   a. Haga clic en **New** e introduzca la información solicitada.
   b. En la **unidad W:** (área de trabajo), cree carpetas usando la siguiente estructura:
      - `W:\[Nombredelcaso]\EnCase6\Exportar`
      - `W:\[Nombredelcaso]\EnCase6\Temp`
      - `W:\[Nombredelcaso]\EnCase6\Índice`
   c. Haga clic en **Finish.**
   d. Haga clic en **Yes** con cada solicitud de crear la carpeta.
   e. En la pantalla **EnCase Acquisition**, haga clic en la opción del menú **Add Device**.
   f. Asegúrese de que está marcada la casilla de verificación **Sessions**.
   g. Seleccione su caso en el panel de la derecha.
   h. Haga clic en **Add Evidence Files**; a continuación vaya al repositorio E01 (usando la configuración de buenas prácticas reseñada en la Ilustración 3-5, este repositorio debería estar guardado en la unidad **X:**).
   i. Haga clic en **Next→ Next→ Finish**. En la parte inferior derecha de la pantalla de adquisición de EnCase (**Acquisition**) aparecerá un icono de un cronómetro y EnCase verificará el archivo E01. Dependiendo del tamaño del archivo, la verificación llevará algún tiempo.

3 En el software EnCase, añada el dispositivo de almacenamiento de destino usando el asistente **Add Device**.

4 Adquiera el contenido del dispositivo.

a En el software EnCase, haga clic en **Cases**→ **Entries**→ **Home**; a continuación haga clic con el botón derecho en el dispositivo que desee adquirir.

b Seleccione **Acquire** en el menú desplegable.

c En el cuadro de diálogo **After Acquisition**, seleccione el tipo adecuado de nuevo archivo de imagen (**New Image File**):

- **Do not add** las opciones que excluyen la imagen recientemente adquirida del caso que esté abierto.
- **Add to Case** añade la imagen recientemente adquirida en el archivo del caso asociado con el dispositivo en el que se tomó la imagen.
- **Replace a source device** añade la imagen recientemente adquirida al caso y elimina el dispositivo previsualizado en donde se realizó la adquisición.

d Haga clic en **Finish**. Cuando se completa el proceso de creación de imagen se muestra el cuadro de diálogo **Acquisition Results**.

Trabajo con Tableau Write-Blockers

PRECAUCIÓN: No extraiga un disco duro de un puente forense mientras esté encendido.

PRECAUCIÓN: No utilice alargadores de cables USB con ningún puente forense.

Conexión del Tableau Write-Blocker a un disco duro SATA

1 Asegúrese de que **DC IN B** del puente T35es Forensic SATA/IDE está en la posición **B On**.

2 Conecte la fuente de alimentación TP2 o TP3 a la parte izquierda del puente SATA T35es usando el conector Mini-DIN de 5 patas.

3 Conecte el cable de alimentación a la fuente de alimentación TP2 y también a una toma eléctrica.

4 Encienda la alimentación para verificar que el LED del bloque de escritura está encendido; después apague la alimentación del puente antes de conectar el dispositivo de almacenamiento de destino.

5 Conecte el conector hembra Molex del cable de alimentación TC5-8 SATA-Style en la posición **DC OUT** situada en la parte derecha del puente T35es SATA/IDE.

6 Conecte el conector de la alimentación SATA del cable de alimentación TC5-8 SATA-Style al conector de alimentación SATA de la unidad de disco duro de destino.

PRECAUCIÓN: Usando las dos conexiones de alimentación Molex y SATA al conectarse a un dispositivo de almacenamiento de destino sobrecargará el dispositivo de destino.

7 Conecte el cable de señal TC3-8 SATA al puente T35es SATA/IDE.

8 Conecte el otro extremo del cable de señal TC3-8 SATA al dispositivo de almacenamiento de destino.

9 Enchufe un extremo del cable de datos (USB 2.0, dos conexiones Fire Wire 800 o FireWire 400 de 4 patas Orion) a uno de los puertos de la parte izquierda del puente T35es SATA/IDE.

10 Enchufe el otro extremo del cable de datos a un puerto del portátil reforzado de Dell o a la estación de trabajo Dell OptiPlex.

11 Coloque el conmutador de la parte superior del puente T35es SATA/IDE en la posición **A ON**. El portátil reforzado de Dell o la estación de trabajo Dell OptiPlex deberá registrar ahora la presencia del dispositivo de almacenamiento de destino.

Conexión del Tableau Write-Blocker a un disco duro IDE

1 Asegúrese de que **DC IN B** del puente T35es Forensic SATA/IDE está en la posición **B On**.

2 Conecte la fuente de alimentación TP2 o TP3 a la parte izquierda del puente SATA/IDE T35es a través del conector Mini-DIN de 5 patas.

NOTA: El enchufe DIN de 7 patas de la fuente de alimentación TP3 no funcionará con los puentes Tableau. Deberá usar el cable adaptador TCA-P7-P5 de DIN de 7 patas a DIN de 5 patas que se incluye para conectar la fuente de alimentación TP3 a los puentes Tableau.

3. Conecte el cable de alimentación a la fuente de alimentación TP2 y también a una toma eléctrica.
4. Encienda la alimentación para verificar que el LED del **bloque de escritura** está **ENCENDIDO**; después **APAGUE** la alimentación del puente antes de conectar la unidad de disco duro de destino.
5. Conecte un conector hembra Molex del cable de alimentación TC2-8 Molex-style en la posición DC OUT situada en la parte derecha del puente T35es SATA/IDE.
6. Conecte el otro conector Molex hembra del cable de alimentación TC2-8 Molex-style al conector Molex de la unidad de disco duro sospechosa.
7. Conecte el extremo azul del cable de señal TC6-8 IDE (de forma que se alinee con la pata 1) al puente T35es SATA/IDE.
8. Conecte el extremo negro del cable de señal TC6-8 IDE al dispositivo de almacenamiento de destino.
9. Enchufe un extremo del cable de datos (USB 2.0, dos conexiones FireWire 800, conexión FireWire 400 de 4 patas Orion) a uno de los puertos de la parte izquierda del puente T35es SATA/IDE.
10. Enchufe el otro extremo del cable de datos a un puerto del portátil reforzado de Dell o a la estación de trabajo Dell OptiPlex.
11. Coloque el conmutador de la parte superior del puente T35es SATA/IDE en la posición **A On**. El portátil reforzado de Dell o la estación de trabajo Dell OptiPlex deberá reconocer la presencia del dispositivo de almacenamiento de destino.

Examen usando FTK 1.8 y 3.0 con centro de datos activado

En la solución Digital Forensics de Dell, la concesión de licencias de FTK se realiza usando un sistema de concesión de licencias de red. Normalmente el servidor de concesión de licencias de red de FTK está instalado en uno de los servidores de centro de datos. Asimismo dicho servidor tiene conectada una mochila de FTK que contiene varias licencias de usuario. Los clientes de FTK están configurados para buscar las licencias en ese servidor, no siendo necesarias otras mochilas locales. Consulte la *Guía de instalación y configuración de Digital Forensics de Dell* para obtener más información. Consulte el apartado "Documentación relacionada y recursos" en la página 16. Consulte también su administrador de sistemas de red para ver información específica sobre la instalación de la solución de su organismo.

Creación de una imagen del dispositivo de almacenamiento de destino

1. En la aplicación AccessData FTK Imager, haga clic en **File**→ **Create Disk Image. . .**
2. En la ventana emergente **Select Source**, seleccione el tipo de evidencia que desee reproducir en imagen: Physical Drive, Logical Drive, Image File, Contents of a Folder o Fernico Device y haga clic en **Next**.

NOTA: A continuación se usa la opción **Imaging a Physical Drive** para demostrar el proceso de creación de imagen. Loas otras opciones de archivo se encuentran en la *Guía del usuario de FTK*. Consulte "Documentación relacionada y recursos" en la página 16.

3. Usando el recuadro desplegable, seleccione la unidad física que desee reproducir en imagen desde las unidades disponibles y haga clic en **Finish**.
4. En el menú desplegable **Create Image**, haga clic en **Add. . .** y seleccione el tipo de imagen que desee crear (Raw, SMART, E01 o AFF). A continuación, haga clic en **Next**.
5. Introduzca la información solicitada en la ventana **Evidence Item Information** (Case Number, Evidence Number, Unique Description, Examiner y Notes). A continuación, haga clic en **Next**.
6. En la ventana **Select Image Destination**, examine el área de almacenamiento asignada para las imágenes de evidencias (consulte la Ilustración 3-5 para ver la nomenclatura de archivos y servidores recomendada por Dell), introduzca un nombre de archivo de imagen y, a continuación, haga clic en →
7. Haga clic en **Start**. Aparece la ventana emergente **Creating Image. . .** que proporciona una barra de progreso de la operación.

NOTA: El proceso de creación de imágenes puede tardar horas dependiendo del volumen de datos que se agreguen.

8. Si se optó antes por ver un resumen de los resultados de la imagen, aparecerá la ventana **Drive/Image Verify Results** cuando se complete el proceso de creación de imagen. Revise los resultados y haga clic en **Close**.
9. Haga clic de nuevo en **Close** para cerrar la ventana **Creating Image. . .**.

Crear un caso

1. Haga clic en **File**→ **New Case**. Introduzca los siguientes datos: **Investigator Name**, **Case Number**, **Case Name**, **Case Path** y **Case Folder**.

2. En la ventana **Forensic Examiner Information**, introduzca los siguientes datos: **Agency/Company**, **Examiner's Name**, **Address**, **Phone**, **Fax**, **E-Mail** y **Comments**. A continuación, haga clic en **Next**.
3. En la ventana **Case Log Options**, seleccione el conjunto de opciones que desee cambiar:
   - Eventos del caso y la evidencia
   - Mensajes de error
   - Eventos de marcadores
   - Eventos de búsquedas
   - Recuperación de datos/Búsquedas de Internet
   - Otros eventos
4. En la ventana **Processes to Perform**, seleccione los procesos que desee llevar a cabo. Seleccione los **Procesos** de las siguientes opciones:
   - Hash MD5
   - Hash SHA1
   - Búsqueda KFF
   - Prueba de entropía
   - Índice de texto lleno
   - Miniaturas de almacenamiento
   - Descifrar archivos EFS
   - Base de datos de listas de archivos
   - Listas de archivos HTML
   - Recuperación de datos
   - Informes de registro
5. Haga clic en **Next**.
6. En la ventana **Refine Case** incluya o excluya los diferentes tipos de datos del caso. Las opciones previamente configuradas incluyen cinco requisitos comunes:
   - Incluir todos los elementos
   - Configuración óptima
   - Énfasis en el correo electrónico

- Énfasis en el texto
- Énfasis en los gráficos

7 Haga clic en **Next**.

8 En la ventana **Refine Index**, incluya y excluya los diferentes tipos de datos del proceso de indexación.

9 Haga clic en **Next**.

Agregar evidencia

1 Haga clic en **Add Evidence**. Aparecerá la ventana emergente **Add Evidence to Case**.

2 Seleccione el tipo de evidencia para agregar al caso: **Acquired Image of Drive**, **Local Drive**, **Contents of a Folder** o **Individual File** seleccionando el botón circular. A continuación haga clic en **Continue**.

3 Vaya a la imagen, unidad, carpeta o archivo; seleccione el archivo y haga clic en **Open**.

Si seleccionó **Acquired Image of Drive** como tipo de evidencia, se mostrará una ventana emergente de información de la evidencia (**Evidence Information**). Introduzca la información solicitada y haga clic en **OK**.

Si seleccionó **Local Drive** como tipo de evidencia,

a Aparecerá la ventana emergente **Select Local Drive**. Seleccione la unidad local que desee agregar; a continuación seleccione **Logical Analysis** o **Physical Analysis**. Haga clic en **OK**.

b En la ventana **Evidence Information**, introduzca la información requerida y haga clic en **OK**.

Si seleccionó **Contents of a Folder or Individual File**, seleccione la carpeta o el archivo que desee agregar a su caso y haga clic en **Open**.

4 Haga clic en **Next**.

5 En la ventana **New Case Setup is Now Complete**, revise las selecciones que haya hecho. Después haga clic en **Finish**.

Examen usando FTK 3 Lab Edition

Creación de una imagen del dispositivo de almacenamiento de destino

Consulte "Creación de una imagen del dispositivo de almacenamiento de destino" en la página 58.

Crear un caso

1. Haga clic en **Case**→ **New**. Aparecerá la ventana **New Case Options**.
2. Introduzca el nombre de su caso y cualquier información de referencia o descripción que requiera su organismo.
3. Examine el directorio de carpetas del caso y seleccione el administrador de procesamiento del recuadro desplegable.

NOTA: Si no sabe donde están el directorio de carpetas del caso y el administrador de procesamiento, consulte con el administrador de los sistemas.

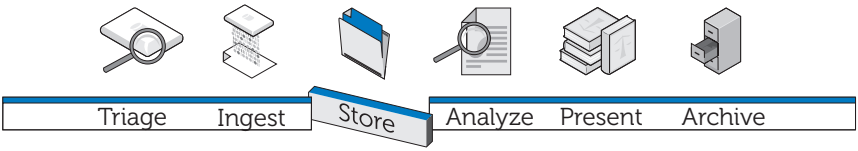
4. Haga clic en **Detailed Options** para restringir los datos que desee incluir en el caso. Consulte la *Guía del usuario de AccessData FTK 3* para ver información sobre cómo restringir datos del caso. Consulte "Documentación relacionada y recursos" en la página 16.
5. Haga clic en **OK**. Se abrirá la ventana **Manage Evidence** (Administrar evidencia).

Agregar evidencia a un caso

1. En la ventana **Manage Evidence**, haga clic en **Add**. A continuación haga clic en el botón de selección al lado del tipo de evidencia que desee agregar: **Acquired Image(s)**, **All Images in Directory**, **Contents of a Directory**, **Individual File(s)**, **Physical Drive** o **Logical Drive**. A continuación, haga clic en **OK**.
2. Vaya al directorio **Evidence** y seleccione el archivo de evidencia. A continuación haga clic en **Open**.
3. Elija una zona horaria (obligatorio).
4. Haga clic en **OK**. Se abrirá la ventana **Data Processing Status**.
5. Cuando el estado de procesamiento (**Process State**) cambie a **Finished**, haga clic en **Close**. Ahora la evidencia aparecerá en el caso dentro de la interfaz del software.

4

Almacenamiento



El planteamiento tradicional del almacenamiento de evidencias digitales empieza con investigadores que trabajan de forma independiente en estaciones de trabajo individuales con una configuración de varios silos. El archivo de la evidencia se guarda, de un modo más o menos seguro, en la estación de trabajo o se transfiere diariamente de un servidor de almacenamiento a la estación de trabajo, sobrecargando la red con la transferencia continuada de archivos muy grandes. La estructura no se puede beneficiar de la velocidad del procesamiento distribuido, las economías de escala y los sustanciales ahorros que puede ofrecer el procesamiento paralelo a nivel de empresa y la arquitectura de almacenamiento escalonado. Además, con esta configuración, es difícil compartir eficazmente datos o colaborar con equipos internos o externos para asegurar unas copias de seguridad de los datos de las evidencias regular y fiable, auditar los cambios en los archivos y, lo más importante, asegurar la integridad y seguridad de los datos.

Eficiencia

La solución Digital Forensics de Dell puede adaptarse a muchas configuraciones de TI diferentes. Cuanto más cercana esté la configuración a un diseño a nivel de empresa de las estaciones de trabajo, con servidores de procesamiento dedicados para el procesamiento distribuido, una infraestructura de red con una comunicación y almacenamiento en paralelo en lugar de en serie, mayor será la amortización en términos de eficiencia. El tráfico de red es menor y más rápido debido a que los procesadores distribuidos hacen el grueso del trabajo. La red solo transfiere los resultados del trabajo, en lugar de los archivos materiales de la evidencia.

Cuando los archivos de evidencias se mantienen en el mismo servidor en lugar de en la estación de trabajo, el analista es libre de usar la estación para iniciar y supervisar *varios* trabajos y no está limitado a procesar un único trabajo. Además, los análisis se pueden completar incluso más rápidamente debido a que pueden trabajar al mismo tiempo varios analistas y especialistas consultores, como expertos en idiomas, en el mismo archivo ***.E01** simultáneamente desde diferentes estaciones de trabajo.

Se puede hacer un triaje del trabajo de acuerdo con la dificultad y asignarse a analistas con diferentes niveles de experiencia; un analista con poca experiencia puede encargarse de las tareas que consumen más tiempo de extraer archivos gráficos de un archivo ***.E01**, mientras que los más experimentados pueden emplear su tiempo en realizar revisiones y análisis más complicados de dichos archivos gráficos.

Escalabilidad

En el servidor, los componentes del centro de datos de la solución son modulares y están diseñados teniendo en cuenta la escalabilidad. Como la carga de trabajo se trata en el centro de datos, las estaciones de trabajo no tienen que cargarse con memoria o potencia informática. De hecho, se pueden usar terminales muy baratas, de muy poco peso, para acceder a los archivos de evidencias requeridos e incluso al software analítico guardado en el centro de datos.

Seguridad

La creciente tendencia a la acumulación de información hace que los sistemas de almacenamiento de datos sean cada vez más vulnerables. Al mismo tiempo, el acceso al almacenamiento de las evidencias debería ser el área más rigurosamente controlada de los sistemas forenses digitales. Una buena práctica exige la aplicación de una estrategia de tres grados:

- Acceso físico estrictamente regulado que limite el acceso al hardware en donde se encuentren los datos de la evidencia.
- Una capa de control administrativo que incluya el uso de directivas de grupo.
- Seguridad basada en el ordenador, como directivas de creación de contraseñas seguras.

A este respecto, cuando se plantea el problema de diseñar el volumen y la estructura adecuados a sus necesidades (consulte "Examen" en la página 39), la seguridad es una de las principales consideraciones de la organización en lo que se refiere al almacenamiento.

Capa de acceso físico

Los archivos del servidor de evidencias forenses digitales deberían alojarse con más seguridad que cualquier otro archivo de la organización, incluyendo los archivos de recursos humanos.

Considere las siguientes recomendaciones:

- Coloque los servidores de examen y el almacenamiento de datos dentro de un espacio dedicado del laboratorio de examen. De esta forma, todos los servidores, almacenes de datos, cableados físicos, conmutadores y enrutadores estarán físicamente protegidos por las mismas medidas de seguridad que restringen el acceso al laboratorio.
- Utilice los protocolos de control de entrada, como los escáner retinales o de huellas dactilares o los accesos mediante tarjeta inteligente.
- Dirija todo el tráfico de examen a través de conmutadores de red dedicados conectados físicamente solo a los servidores de examen y estaciones de trabajo.

Capa de control administrativo y Active Directory

La configuración de la solución funcionará en sistemas operativos de Windows, por lo que el resto de este capítulo trata de Windows y de sus funciones de seguridad de grupos y usuarios de Active Directory. Active Directory se basa en la seguridad de grupos y las funciones relacionadas. Un grupo es un conjunto de usuario u ordenadores dentro de un dominio. Los dos tipos básicos de grupos son *grupos de distribución* (usados para la distribución de correo electrónico) y *grupos de seguridad*. El establecimiento de grupos de seguridad permite crear y aplicar directivas relacionadas con la seguridad, incluyendo:

- Acceso a recursos compartidos y el nivel de dicho acceso.
- Derechos de usuario incluyendo los requisitos de contraseña.
- Directivas de bloqueo de cuentas.
- Directivas de restricción de software.
- Distribución de revisiones de seguridad a portátiles, ordenadores de escritorio y servidores.

Por ejemplo, se puede crear un grupo que contenga estaciones de trabajo administrativas y un segundo grupo que contenga usuarios administrativos. Después se podrán usar Objetos de directivas de grupos (GPO) para limitar el acceso a dichas estaciones de trabajo y miembros del grupo de usuarios administrativos. (Consulte "Aplicación de directivas de seguridad usando Objetos de directivas de grupo" en la página 70 para ver información sobre el trabajo con objetos de directivas de grupos.)

Capa de seguridad basada en el ordenador y Active Directory

Active Directory también proporciona Kerberos, un protocolo de seguridad de autenticación de red que permite a los nodos comunicarse entre sí por redes no seguras para probar su identidad de un modo seguro. Consulte "Cuentas de usuario de Active Directory" en la página 72 para ver información sobre el trabajo con cuentas de usuario y consulte también "Compatibilidad de Active Directory con las directivas de contraseña segura" en la página 71 para obtener información sobre la creación de contraseñas.

Información adicional sobre la seguridad y Digital Forensics

SP 800-41 Rev. 1 Sept. 2009 Pautas generales sobre servidores de seguridad y directivas de servidores de seguridad

SP 800-46 Rev. 1 Junio 2009 Guía para la seguridad en el teletrabajo de las empresas y el acceso remoto

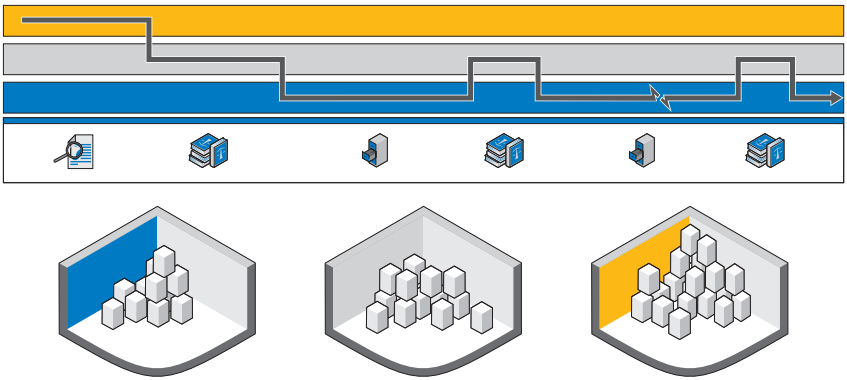
SP 800-55 Rev. 1 Julio 2008 Guía de medición del rendimiento para la seguridad de la información

Almacenamiento escalonado

La solución Digital Forensics de Dell utiliza estrategias de almacenamiento escalonado con el fin de asimilar el rápido crecimiento de los datos al tiempo que se controlan los costes. Se puede crear una combinación a la medida de unidades SATA y SAS con diferentes niveles de capacidad y rendimiento para adaptarse a los perfiles de datos. Esta combinación puede volver a valorarse periódicamente para mantener la optimización con el tiempo. Normalmente, los datos de carácter crítico, como los datos de los casos que se encuentran en

la etapa de análisis, se guardan en costosas unidades de alto rendimiento, mientras que los datos menos urgentes, como los archivos de los casos cuyo proceso acaba de solicitarse o los que ya están cerrados, se mueven a unidades de alta capacidad menos costosas.

Ilustración 4-1. Uso del almacenamiento escalonado para el archivado y la recuperación



LaIlustración 4-1 muestra la ruta de acceso para el almacenamiento de la evidencia digital desde el momento en que se recoge hasta su eventual almacenamiento a largo plazo en cinta o su eliminación final.

Adaptación del archivado y la recuperación a la vida del caso

Obtención de la evidencia (Analizar): cuando se toma el dispositivo digital por primera vez, los laboratorios contra el crimen de alta tecnología lo que quieren es sacar la evidencia potencial del dispositivo tan rápidamente como sea posible e iniciar el proceso de análisis. Cuanto más rápido pueda el analista buscar e indexar un archivo de evidencias, más rápidamente se podrá tomar la decisión de si continuar con el caso o no.

Identificación de la evidencia (Presentar): cuando se ha encontrado potencialmente una evidencia durante la etapa de análisis, se precisarán diferentes conocimientos (idiomas, planos técnicos, contabilidad, etc.). Ahora los equipos de visualización

tendrán que establecer la categoría de la evidencia. El proceso más pesado ha sido terminado, por lo que la evidencia podrá residir en un almacenamiento de largo plazo más lento y económico.

Espera por el juicio (Archivado): una vez reunida toda la evidencia potencial y con el caso en marcha, normalmente no hay necesidad de mantener los datos del mismo, así como las imágenes de la evidencia, en un almacenamiento en línea, desde donde se puede acceder de forma instantánea. En los casos normales, el laboratorio podrá tener que enfrentarse con un *tiempo de días para recuperar el caso*, lo que puede hacerse de forma proactiva si algún acontecimiento conocido previsto va a hacer necesarios los datos del caso. Este planteamiento reduce el coste de almacenamiento en los laboratorios forenses debido a que no es necesario conservar todos los datos en el laboratorio, independientemente de la importancia. Se pueden mover sin problemas a un almacenamiento más lento.

Juicio (Presentar): en el supuesto de que el caso se lleve a juicio, el laboratorio forense querrá tener un acceso rápido a la evidencia y los datos del caso con el fin de poder responder a cualquier pregunta durante la celebración del juicio.

Sentencia con pena privativa de libertad (Archivado): en el caso de que se produzca una condena de prisión, la mayoría de países requieren que la policía o el departamento de justicia conserven la evidencia y los archivos del caso durante un período mínimo o la duración de la sentencia de prisión más un plazo razonable de tiempo para apelaciones o 99 años. Aquí el objetivo es mantener los datos a largo plazo en un soporte de almacenamiento de bajo coste que proteja su integridad y confidencialidad.

Apelación (Presentar): en el caso de apelación, podría ser necesario recuperar los datos del caso y la evidencia para un posterior análisis o examen detallado. Esta recuperación tiene que suceder de un modo muy puntual, aunque muy raramente los datos se requieren de forma instantánea.

Eliminar: en la mayoría de países de todo el mundo, los organismos públicos no pueden conservar datos indefinidamente una vez que éstos han alcanzado su límite legal de retención. Es necesario disponer de un proceso sencillo para eliminar dichos datos. Este proceso también puede ser necesario en el caso de veredictos de inocencia, con lo que los datos deberán eliminarse igualmente.

Cómo configurar la seguridad del almacenamiento usando la solución Digital Forensics de Dell y Active Directory

Creación y ocupación de grupos en Active Directory

Los grupos se establecen a través de los servicios de dominios de Active Directory (Windows Server 2008).

Creación de un nuevo grupo (Windows Server 2008)

1. Haga clic en **Iniciar→ Herramientas administrativas→ Centro administrativo de Active Directory**.
2. En el panel de navegación haga clic con el botón derecho en el nodo que desee agregar un grupo nuevo y haga clic en **Nuevo**. A continuación haga clic en **Grupo**.
3. Introduzca el nombre del nuevo grupo.
4. Seleccione la opción adecuada en **Ámbito de grupo**.
5. Seleccione el **Tipo de grupo**.
6. Seleccione **Proteger contra eliminación accidental**.
7. Modifique las secciones **Administrado por**, **Miembro de** y **Miembros** y, a continuación, haga clic en **Aceptar**.

Añadir miembros a un grupo (Windows Server 2008)

1. Haga clic en **Iniciar→ Herramientas administrativas→ Centro administrativo de Active Directory**.
2. En el panel de navegación, haga clic en la carpeta en donde resida el grupo.
3. Haga clic con el botón derecho del ratón en el grupo y, a continuación, haga clic en **Propiedades**.
4. Seleccione **Agregar** en la ficha **Miembros**.
5. Introduzca el nombre del usuario, ordenador o grupo que desee agregar y haga clic en **Aceptar**.

Aplicación de directivas de seguridad usando Objetos de directivas de grupo

Una vez que se haya creado un grupo, podrá aplicar colectivamente la configuración de seguridad y otros atributos a los miembros de dicho grupo creando y configurando un Objeto de directiva de grupo (GPO). Esto facilita el mantenimiento de la seguridad de los usuarios y recursos conforme cambie su organización forense digital.

Creación y edición de GPO

Creación de un nuevo GPO (Windows Server 2008)

En Windows Server 2008, los GPO se administran usando la Consola de administración de directivas de grupo (GPMC).

1. Para abrir la GPMC, haga clic en **Iniciar→ Herramientas administrativas→ Administración de directivas de grupo**.
2. Vaya a al bosque y el dominio en el que desee crear el nuevo objeto y, a continuación, haga clic en **Objetos de directivas de grupo**.
3. Haga clic en **Nuevo**.
4. Introduzca el nombre del nuevo GPO y, a continuación, haga clic en **Aceptar**.

Edición de un nuevo GPO (Windows Server 2008)

En Windows Server 2008, los GPO se administran mediante la GPMC.

1. Para abrir la GPMC, haga clic en **Iniciar→ Herramientas administrativas→ Administración de directivas de grupo**.
2. Vaya al bosque y el dominio en donde resida el GPO y, a continuación, haga clic en **Objetos de directivas de grupo**.
3. Haga clic con el botón derecho en GPO.
4. Haga los cambios necesarios en la configuración y guárdelos.

Compatibilidad de Active Directory con las directivas de contraseña segura

Active Directory permite diferentes directivas de autenticación, incluyendo configuraciones de tarjetas inteligentes, contraseña segura y bloqueo de cuentas.

Las contraseñas y otras directivas de autenticación se crean usando Objetos de directivas de grupo (GPO). Consulte "Aplicación de directivas de seguridad usando Objetos de directivas de grupo" en la página 70 para ver información sobre la creación y edición de GPO.

Configuración recomendada de contraseña segura

Cuando se configuren parámetros de contraseñas, se recomiendan los siguientes valores:

- Forzar el historial de contraseñas: el número de contraseñas únicas que se deberán usar antes de que se pueda reutilizar una contraseña. Configurado para 24.
- Vigencia máxima de la contraseña: las contraseñas deben cambiarse cada *x* días. Configurado para 90.
- Vigencia mínima de la contraseña: el número de días que las contraseñas tienen que tener efecto antes de poder cambiarse. Configurado para 1 ó 2.
- Longitud mínima de la contraseña: ajustado para 8 ó 12 caracteres.
- Las contraseñas deben cumplir los requerimientos de complejidad: configurado para **Activado**. Se aplican las siguientes directivas:
  - Las contraseñas tienen que tener al menos 6 caracteres.
  - Las contraseñas tienen que incluir caracteres de al menos tres de estas cuatro categorías:
    - Caracteres en mayúsculas
    - Caracteres en minúsculas
    - Números (de 0 a 9)
    - Símbolos
  - Las contraseñas no deben contener tres o más caracteres consecutivos del nombre de la cuenta o el usuario.

Directivas de contraseñas granulares (Fine-Grained Password Policies)

En Windows Server 2008, los servicios de dominios de Active Directory permiten Objetos de configuración de contraseñas (PSO) que se aplican a grupos o usuarios de seguridad globales en particular dentro de un dominio. Un PSO puede especificar la extensión de las contraseñas en caracteres, la complejidad de éstas, la duración máxima y mínima y otros atributos.

Por tanto, se pueden crear varios PSO que correspondan a la estructura organizativa de sus instalaciones forenses digitales. Por ejemplo, se pueden usar PSO para implementar contraseñas más largas que caduquen mensualmente para usuarios administrativos y contraseñas más cortas que caduquen cada tres meses para los analistas.

Cuentas de usuario de Active Directory

Establecimiento de cuentas de usuario para analistas forenses

1. Abra **Usuarios y equipos de Active Directory**:
   a. Haga clic en **Iniciar→ Panel de control**
   b. Haga doble clic en **Herramientas administrativas** y, a continuación, haga doble clic en **Usuarios y equipos de Active Directory**.
2. En el árbol de la consola, haga clic con el botón derecho en la carpeta en la que desee agregar una cuenta de usuario.

   ¿Dónde?

   Usuarios y equipos de Active Directory/*dominio*/*nodo*/*carpeta*
3. Señale **Nuevo** y, a continuación, haga clic en **Usuario**.
4. En **Nombre**, escriba el nombre de pila del usuario.
5. En **Iniciales**, escriba las iniciales del usuario.
6. En **Apellido**, escriba el apellido del usuario.
7. Modifique **Nombre completo** para agregar iniciales o invertir el orden del nombre y el apellido.
8. En **Nombre de inicio de sesión de usuario**, escriba el nombre de inicio de sesión del usuario, haga clic en el sufijo UPN de la lista desplegable y, a continuación, haga clic en **Siguiente**.

Si el usuario utilizará un nombre diferente para iniciar sesión en equipos que funcionen con Windows 95, Windows 98 o Windows NT, podrá cambiar el nombre de inicio de sesión de usuario como aparece en **Nombre de inicio de sesión de usuario (antes de Windows 2000)** por un nombre diferente.

9 En **Contraseña** y en **Confirmar contraseña**, escriba la contraseña de usuario y después seleccione las opciones de contraseña adecuadas.

NOTA: Para realizar este procedimiento deberá ser miembro del grupo de Operadores de cuentas, el grupo Administradores de dominios o el grupo Administradores de organización en Active Directory; o bien deberá tener delegada la suficiente autoridad. Como buena práctica de seguridad, considere el uso de *Ejecutar como* para llevar a cabo este procedimiento. Para obtener más información, consulte *Grupos locales predeterminados*, *Grupos predeterminados* y *Uso de Ejecutar como*.

Establecimiento de una cuenta de administrador de servicios de FTK

NOTA: Durante el curso de la instalación de FTK, se le pedirá el nombre de la cuenta de usuario que tiene pensado utilizar para administrar la función de Procesamiento distribuido. No lo use.

Si utiliza la función de procesamiento distribuido de FTK como una de las herramientas forenses digitales, deberá crear una cuenta de Administrador de servicios de FTK en Active Directory para poder realizar la actualización automática de las contraseñas. Durante el proceso de instalación de FTK se le pedirá que facilite el nombre del usuario que se usará para supervisar y gestionar la función de procesamiento distribuido. Esta cuenta deberá crearse como un servicio en Active Directory y deberá tener derechos de administrador (pero no deberá ser la cuenta de Administrador) para facilitar el protocolo de enlace continuo entre FTK y el servidor de evidencias que precisa la función de procesamiento distribuido.

1 En Active Directory, abra **Herramientas administrativas** y, a continuación, haga clic en **Usuarios y equipos de Active Directory**.

2 En el árbol de la consola, haga doble clic en el nodo Dominio.

3 En el panel **Detalles**, haga clic con el botón derecho en la unidad organizativa en donde desee agregar la cuenta de servicio. Seleccione **Nuevo** y, a continuación, haga clic en **Usuario**.

4 En **Nombre**, escriba `FTKServMgr` para la cuenta de servicio; deje **Apellido** en blanco.

5 Modifique **Nombre completo** como desee.

6 En **Nombre de inicio de sesión de usuario**, escriba `FTKServMgr`. La cuenta de usuario iniciará sesión con el nombre que introduzca. En la lista desplegable, haga clic en el **sufijo UPN** que deba añadirse al nombre de inicio de sesión de la cuenta de servicio (seguido del símbolo @). Haga clic en **Siguiente**.

7 En **Contraseña** y en **Confirmar contraseña**, escriba una contraseña para la cuenta de servicio.

8 Seleccione las opciones de contraseña adecuadas y, a continuación, haga clic en **Siguiente**.

9 Haga clic en **Finalizar** para completar la creación de una cuenta de servicio.

Creación de una cuenta de usuario no administrativo

1 Inicie sesión en un equipo que funcione con Windows Vista usando una cuenta de usuario administrativo.

2 Abra el menú **Iniciar**. Haga clic con el botón derecho en **Equipo** y haga clic en **Administrar**.

3 Haga clic en la flecha al lado de **Usuarios y grupos locales.**

4 Haga clic con el botón derecho del ratón en **Usuarios** y, a continuación, haga clic en **Nuevo usuario**.

5 Escriba el nombre del usuario para el que vaya a crear una cuenta. Por ejemplo, si desea poner el nombre **usuarioweb1** al usuario, escriba `usuarioweb1` en el campo **Nombre de usuario** y también en el campo **Nombre completo**.

6 Escriba una contraseña que pueda recordar los campos **Contraseña** y **Confirmar contraseña**.

NOTA: Las contraseñas distinguen entre mayúsculas y minúsculas. La contraseña que escriba en los campos **Contraseña** y **Confirmar contraseña** deberán coincidir para poder agregar la cuenta de usuario.

7 Desmarque la casilla de verificación **El usuario debe cambiar la contraseña en el próximo inicio de sesión**.

8 Marque las casillas de verificación **La contraseña nunca caduca** y **El usuario no puede cambiar la contraseña**.

9 Haga clic en **Crear** y seleccione **Cerrar**.

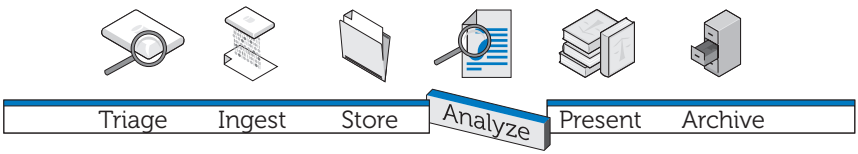
10 Haga clic en **Archivo** y seleccione **Salir**.

Configuración de la seguridad para archivos de casos individuales y evidencias

1. En el **Explorador de Windows**, vaya al archivo para el que se establecerán los permisos de archivo. Haga clic con el botón derecho del ratón en el archivo y, a continuación, seleccione **Propiedades**.
2. Haga clic en la ficha **Seguridad**.
3. Si es necesario, desmarque la casilla de verificación **Todos**.
4. Agregue solo los usuarios que necesitarán acceder al archivo como se determine en la directiva de su lugar de trabajo.
   a. Haga clic en **Agregar**.
   b. En el campo **Escriba los nombres de objeto que desea seleccionar**, introduzca los nombres de los correspondientes usuarios. A continuación, haga clic en **Aceptar**.
   c. Modifique los **Permisos** de cada usuario como determine la directiva de su lugar de trabajo.

5

Analizar



Hay varios tipos diferentes de análisis que el investigador necesita para poder tratar los datos de las evidencias, incluyendo la firma de los archivos y el análisis de hash, así como un amplio indexado y búsquedas de palabras clave. Todos estos análisis requieren una considerable potencia de procesamiento ya que los archivos de evidencias pueden llegar a tener tamaños cercanos al terabyte y el procesamiento de dichos archivos puede llevar horas — incluso días — usando las arquitecturas de los centros de datos normalmente colocados hoy en día. Los investigadores que intenten este análisis en una única estación de trabajo deben tener en cuenta este problema cuando programen el procesamiento de casos debido a que el análisis y el indexado de un único caso pueden emplear todos los activos de hardware del investigador. La solución Digital Forensics de Dell ofrece las importantes ventajas del procesamiento distribuido y que puede cambiar la imagen por completo. En breve veremos el procesamiento distribuido, pero primero examinemos algunos de los tipos de análisis que normalmente se encuentra el investigador de informática forense digital.

Tipos de análisis

Análisis de hash

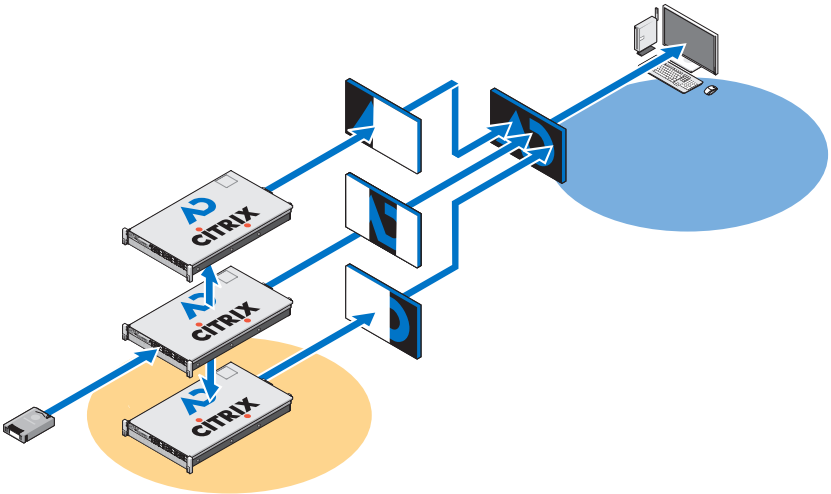
La función hash utiliza algoritmos criptográficos para crear una huella digital a partir de los datos. El hash puede usarse para comparar un hash de los datos originales con uno de los datos forenses analizados, que puede ser aceptado en los tribunales como prueba de que dos grupos de datos son idénticos. El análisis hash compara valores de hash de archivos de casos con valores de hash conocidos y guardados.

Análisis de firma del archivo

Cada archivo es de un tipo propio, que normalmente se indica mediante la extensión de tres o cuatro letras en el nombre. Por ejemplo, un archivo de texto puede tener una extensión ***.txt** y un archivo de imagen la extensión ***.jpg**. No es infrecuente que estas extensiones de archivos hayan sido cambiadas a algo aparentemente inocuo. Se puede cambiar un archivo de imagen, por ejemplo, con una extensión de archivo de texto en un intento de ocultar su contenido pornográfico.

Sin embargo, cada archivo también posee un encabezado que incluye un código de tipo de archivo diferente de la extensión, pero únicamente indicativo de un tipo de archivo específico. Por ejemplo, un archivo ***.bmp**, tendrá el código de encabezado de tipo de archivo ***.bm8**. Cuando el código del encabezado con el tipo de archivo y la extensión del archivo son diferentes, el analista forense digital deberá examinar con más detalle los datos.

Ilustración 5-1. Procesamiento distribuido



¿Qué es el procesamiento distribuido?

Procesamiento distribuido se refiere al uso de varios procesadores, cada uno con su propio activo de memoria, que se aplica individualmente a una parte diferente de una única tarea informática y que emplea un sistema de envío de mensajes para comunicarse entre sí dentro del grupo. El procesamiento distribuido no es lo mismo que el *procesamiento paralelo*, que se refiere al uso de varios procesadores que comparten un único activo de memoria.

Considere lo siguiente, que le dará una idea general de las ventajas de la solución de Dell usando una instalación de procesamiento distribuido. Con el uso del procesamiento distribuido, completar un análisis de cinco archivos de 200 GB puede llevar solamente 3,5 horas, mientras que procesar un único archivo de 200 GB en una estación de trabajo independiente puede tardar unas 7 u 8 horas.

Mover el procesamiento de datos de evidencias de la estación de trabajo del analista al servidor no es el final. La solución de Dell también ofrece la opción de ejecutar el mismo software de análisis, como FTK y EnCase en el servidor, permitiendo que la estación de trabajo se convierta en una interfaz integrada que puede ejecutar varias instancias diferentes de paquetes de software de informática forense en sistemas operativos vistos a la vez sin degradación alguna del rendimiento del cliente.

Uso del procesamiento distribuido en FTK 3.1

El procesamiento distribuido permite aplicar los recursos adicionales de hasta tres ordenadores adicionales en el momento de procesar los casos. Una vez que ha instalado y configurado el motor de procesamiento distribuido puede reducir exponencialmente el tiempo de procesamiento de los casos.

NOTA: Por regla general, el uso del procesamiento distribuido no reduce los tiempos de procesamiento a menos que el número de objetos a procesar supere 1.000 veces el número de núcleos que existen dentro del sistema. Por ejemplo, en los sistemas con ocho núcleos, los equipos de motores de procesamiento distribuido adicional no pueden bajar el tiempo de procesamiento a menos que la evidencia contenga más de 8.000 veces.

NOTA: Para obtener información sobre la instalación y configuración del módulo de procesamiento distribuido como parte de su solución, consulte la sección adecuada de la *Guía del usuario de FTK*.

1. Asegúrese de que se comparte la carpeta del caso antes de tratar de agregar y procesar la evidencia. Si sigue las convenciones de nombres de archivos recomendadas por Dell, la carpeta del caso debería encontrarse en la unidad de su espacio de trabajo, **W:/**. Si no está seguro de dónde se encuentra la carpeta del caso, póngase en contacto con el administrador de los sistemas.
2. Introduzca la ruta de acceso de la carpeta del caso en el cuadro de diálogo **Create New Case** en formato UNC:

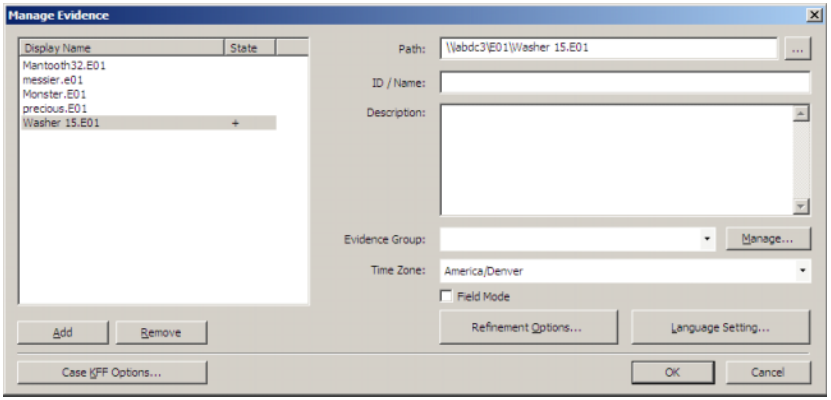
   ```
   (\\[nombre del ordenador_o_dirección _IP]\[nombre
   de la ruta de acceso]\[nombre del archivo])
   ```

3. Haga clic en **Detailed Options** y seleccione las opciones como lo haría normalmente.
4. Haga clic en **OK** para volver al cuadro de diálogo **New Case Options** y marque la casilla de verificación al lado de la opción **Open the case**. Haga clic en **OK** para crear el caso nuevo y abrirlo.
5. Haga clic en **Add** después de que se abra el nuevo caso y se abrirá automáticamente el cuadro de diálogo **Manage Evidence**. Seleccione el archivo de evidencia a agregar y haga clic en **Open**.
6. La ruta de acceso a la evidencia está designada de forma predeterminada mediante la letra de unidad. Cambie la ruta de acceso al formato UNC cambiando la letra de la unidad por el nombre del ordenador o la dirección IP en donde se encuentra el archivo de la evidencia conforme con la siguiente sintaxis.

   ```
   (\\[nombre del ordenador_o_dirección _IP]\[nombre
   de la ruta de acceso]\[nombre del archivo])
   ```

7. Deje el resto de la ruta de acceso como está.
8. En la siguiente figura se muestra la ruta de acceso UNC para la evidencia:

Ilustración 5-2. Recuadro de diálogo para administrar la evidencia



9 Haga clic en **OK**.

Comprobación de la instalación

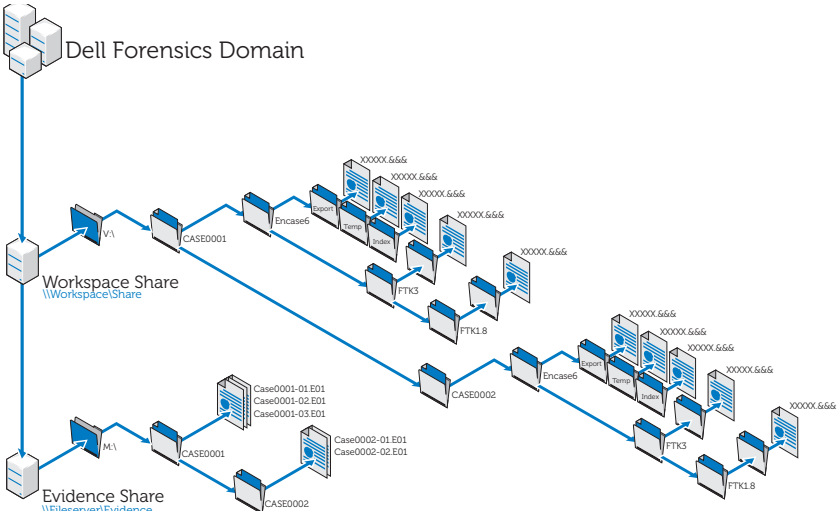
Cuando haya completado la instalación, abra el **Administrador de tareas** en el equipo remoto y manténgalo abierto mientras agrega la evidencia y empieza a procesarse. Estos pasos le permitirán ver la actividad de **ProcessingEngine.exe** en la ficha **Procesos**.

El motor de procesamiento distribuido no se activa hasta que un caso supere aproximadamente 30.000 elementos. Cuando se active verá aumentar el porcentaje de CPU y uso de memoria en el archivo **ProcessingEngine.exe** del **Administrador de tareas**.

Búsqueda de archivos en la red

Las buenas prácticas exigen que se guarde la evidencia y los archivos de trabajo por separado en la red. Dell recomienda configurar dos unidades compartidas y después establecer archivos y subarchivos del caso desde allí como se muestra en la Ilustración 5-3.

Ilustración 5-3. Estructura de archivos recomendada por Dell



Análisis usando FTK:

Abrir un caso existente

Uso del menú de archivos

1. Desde FTK, seleccione **File** y seleccione **Open Case**.
2. Seleccione el caso que desee abrir y haga clic sobre él para iniciarlo.

NOTA: Todos los archivos de casos tiene el nombre **case.ftk.** El archivo **case.ftk** de cada caso se guarda en la correspondiente carpeta de casos.

Desde la línea de comandos

En la línea de comandos, escriba:

```
path_to_ftk_program_file\ftk.exe /OpenCase
target_case_directory
```

Procesamiento de la evidencia del caso

FTK procesa la evidencia conforme se crean los casos o conforme se añada la evidencia más tarde al caso. Para ver instrucciones sobre la creación de un nuevo caso, consulte "Crear un caso" en la página 61 o la *Guía del usuario de FTK*. Para ver instrucciones sobre cómo añadir evidencia a un caso existente, consulte "Agregar evidencia a un caso" en la página 61 o la *Guía del usuario de FTK*. Para obtener más información, consulte "Documentación relacionada y recursos" en la página 16.

Análisis usando EnCase:

Abrir un caso existente

1. En el menú de archivos, seleccione **File→ Open**.
2. Busque el caso y haga clic en **Open**.

Crear un trabajo de análisis

1. Haga clic en la ficha **Analysis Jobs** en el diálogo principal **Source Processor**.
2. Haga clic en **New**. Aparecerá el diálogo **Create Analysis Job/Job Name**.

   El nombre de trabajo predeterminado es Trabajo__[aaaa_mm_dd__hh_mm_ss], por ejemplo: Trabajo___2009_06_24__03_42_42_PM.

   Los nombres de los trabajos no pueden contener espacios al principio o al final del nombre ni ninguno de los siguientes caracteres: \ / : * ? " < > |
3. Escriba un nombre de trabajo y haga clic en **Next**. Aparecerá el diálogo **Create Analysis Job/Module Selection**.

   El diálogo muestra carpetas de módulos en el panel izquierdo y los módulos únicos dentro de dichas carpetas en el panel de derecho.

   Si se incluye un módulo en el trabajo de análisis, pero no hay datos de dicho módulo cuando se ejecuta el trabajo en una recogida, el módulo quedará ignorado. Esta función permite crear trabajos de análisis genéricos para una variedad de conjuntos de datos recogidos.
4. Marque la casilla de verificación del módulo.

   Se puede seleccionar más de un módulo.

Los módulos de análisis no tienen parámetros configurables por el usuario.

Para seleccionar todos los módulos del grupo, coloque una marca al lado del nombre de la carpeta del grupo en el panel izquierdo.

5 Haga clic en **Finish**.

NOTA: Los trabajos de análisis pueden mostrar los módulos disponibles que no se encuentran en los trabajos de recogida. Estos módulos se identifican como módulos heredados, por lo que es posible analizar datos recogidos en anteriores versiones del procesador de origen usando módulos que ya no existen.

Ejecutar un trabajo de análisis

1 En la ficha **Collected Data**, seleccione la evidencia que desee analizar seleccionando primero el nombre de archivo en el panel izquierdo. A continuación, seleccione los archivos de evidencias reales en la tabla de la derecha.

2 Haga clic en **Run Analysis**. Se abrirá el diálogo **Select Analysis to Run**.

3 Seleccione el trabajo de análisis y haga clic en **Run**. El procesador de origen ejecuta el análisis sobre la evidencia seleccionada. Cuando se ha completado el análisis, se muestra el explorador de datos.

Realización de un análisis de firmas

1 Haga clic en **Search**.

2 Marque la casilla **Verify file signatures** en el área **Additional Options** y haga clic en **Start**. La rutina de análisis de firmas se ejecuta en segundo plano. Al terminar se muestra un diálogo completo de búsqueda. El diálogo presenta el estado de la búsqueda, tiempos y datos del archivo.

Estos mismos datos se pueden ver en la consola.

Ver resultados del análisis de firmas

1 Haga clic en **Set-Include** en el panel de **árbol** para mostrar todos los archivos del caso.

En este nivel, **Set Include** selecciona todo lo que hay en el archivo de evidencia.

2 Organice las columnas del panel de la **tabla** de forma que las columnas **Name**, **File Ext** y **Signature** estén juntas.

3 Clasifique las columnas con **Signature** en el primer nivel, **File Ext** en el segundo y **Name** en el tercero.

Desplácese hacia arriba o hacia abajo para ver todas las firmas.

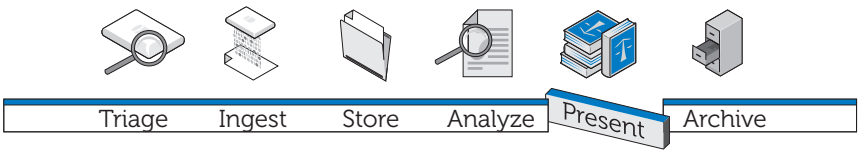
4 Haga clic en **Set-Include** en la selección **Entries** del panel de **árbol**.

En el panel de la **tabla** se muestra una lista de archivos de casos con sus firmas de archivos y otros datos asociados.

5 Clasifique los datos como desee.

6

Presentación



La comunicación de los resultados de los análisis forma parte integral de la solución Digital Forensics de Dell y se facilita principalmente a través del software forense que se usa como parte de la solución.

Cómo crear informes usando la solución Digital Forensics de Dell

Creación y exportación de informes usando EnCase 6

1. Seleccione los elementos sobre los que hacer el informe, bien sean archivos, marcadores, resultados de búsquedas u otros datos.
2. Seleccione el tipo de informe que desee empleando las fichas del panel **Tree**.
3. En la ficha **Table** del panel **Table**, active los elementos que desee mostrar en el informe.
4. En la ficha **Table**, cambie a la ficha **Report**.
5. Modifique el informe según sea necesario.
6. Exporte el informe a un formato que se pueda ver fuera de EnCase.
   a. Haga clic con el botón derecho en el informe y haga clic en **Export** en el menú desplegable. Se abre el diálogo **Export Report**.
   b. Haga clic en el botón de selección adecuado para seleccionar el formato de salida que desee usar (TEXT, RTF o HTML).
   c. Introduzca o vaya a la ruta de acceso de salida.

d Si lo desea, seleccione **Burn to Disc** para activar el cuadro **Destination Folder** y, a continuación, haga clic en **Archive Files** para crear una nueva carpeta y guardar un archivo **.iso** en disco.

e Haga clic en **OK**.

Informes usando FTK

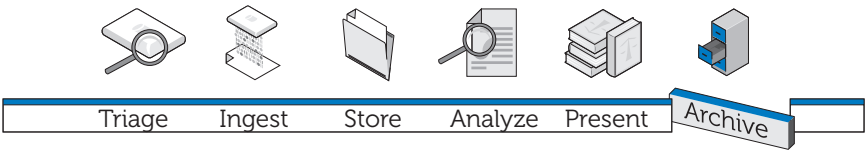
1. Haga clic en **File**→ **Report** para abrir el **Report Wizard**.
2. Introduzca la información básica del caso que solicita el asistente.
3. Seleccione las propiedades de los marcadores.
4. Determine si desea mostrar los gráficos del caso y cómo hacerlo en el informe.
5. Determine si desea o no incluir una sección en el informe que muestre las rutas de acceso de los archivos, así como las propiedades de éstos, en las categorías seleccionadas.
6. Si lo desea, añada las secciones **Registry Viewer**.

Ver el informe fuera de FTK

1. Busque el archivo del informe.
2. Haga clic en el archivo del informe y, a continuación:
   - Haga clic en **index.htm** para abrir un documento HTML en un navegador de Internet.
   - Haga clic en [*report*]**.pdf** para abrir un informe en un visualizador de PDF.

7

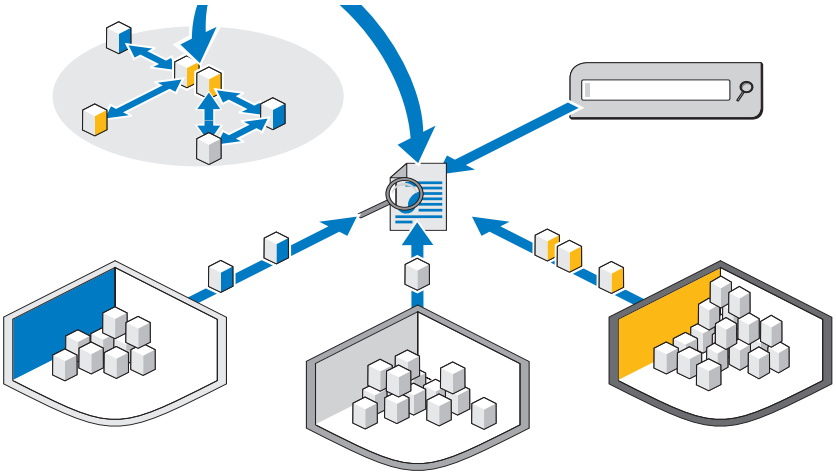
Archivado



Ninguna solución forense digital está completa sin un archivado y componente de recuperación escalable, seguro e integral. La solución Digital Forensics de Dell ofrece eso y más. En el marco de trabajo de la solución de Dell hemos tratado de crear una sencilla interfaz que funcione con todas las aplicaciones de informática forense para controlar el ciclo de vida de la evidencia y los archivos de los casos. Debido al hecho de que es difícil predecir cuando se pueden necesitar los datos en el futuro o cuanto puede durar una investigación, hemos creado una solución flexible que requiere que el analista forense determine los archivos que recuperará y archivará. Esta solución utiliza un planteamiento escalonado para el almacenamiento a la medida de sus necesidades — una mezcla de hardware SATA y SAS — y un archivado realizado por el usuario usando software de archivado bajo demanda de NTP.

La solución de Dell está formada por componentes modulares que proporcionan un entorno escalable que se puede ampliar para satisfacer las exigencias de crecimiento de los requisitos de procesamiento y almacenamiento. La infraestructura de copia de seguridad, recuperación y archivado (BURA) de la solución ayuda a optimizar la cooperación entre organismos y fuerzas y a través de las fronteras. Libera de cargas administrativas automatizando muchas de las tareas de copia de seguridad de los datos, proporciona coherencia entre los laboratorios de las organizaciones y minimiza el riesgo de la cadena de custodia digital.

Ilustración 7-1. Capacidades de búsqueda en soportes y casos cruzados de la solución de Dell



Un componente opcional de búsqueda muy potente permite la correlación de la información entre los conjuntos de datos examinados. Este componente ofrece la posibilidad de realizar búsquedas como las de Internet en todo el almacén de datos del caso tanto del contenido activo como del contenido en línea, así como del material archivado de casos anteriores.

Solución de archivado Client One-Click

Con las herramientas de archivado y recuperación de la solución Digital Forensics de Dell, el analista puede archivar o recuperar tanto archivos únicos como las estructuras completas de directorios con el botón derecho del ratón. Se han añadido otros comandos del botón derecho adicionales al software de archivado bajo demanda NTP para que el usuario solo tenga que seleccionar y archivar o seleccionar y restaurar datos. Cuando se selecciona un archivo para el archivado aparece una ventana pidiendo al usuario que confirme la acción. Una vez confirmada, la solución realizará un proceso en segundo plano para mover dicho archivo a un dispositivo de cinta o a un dispositivo de almacenamiento cerca de la línea. Este proceso tiene lugar sin problema en segundo plano y no perjudica el rendimiento de la estación de trabajo del usuario.

Cuando se ha completado el proceso en segundo plano, el icono atribuido a dicho archivo cambia a gris para indicar claramente al usuario que el archivo ha sido archivado, aunque la estructura de carpetas y archivos sigue visible para que el usuario pueda encontrar fácilmente el archivo de nuevo en el futuro con fines de restauración. Para restaurar un archivo, el usuario solo tiene que ir a la estructura de carpetas original, buscar la carpeta o el archivo que desee restaurar, hacer clic con el botón derecho en el archivo o carpeta y seleccionar la opción de restauración.

Dell recomienda colocar todos los archivos de la evidencia y el caso en un dispositivo NAS escalable central que permita un punto de almacenamiento ampliable central, lo que facilita la colaboración entre los analistas. Esta recomendación también permite que haya un único punto de auditoría a efectos de la cadena de custodia. Cuando se selecciona un archivo para el archivado, éste se mueve a la siguiente ventana de procesamiento del sistema disponible desde el almacenamiento principal a la opción secundaria (cinta o cerca de la línea).

Los tiempos de archivado y recuperación variarán considerablemente dependiendo del tráfico existente con el almacenamiento NAS centralizado, los archivos que se estén guardando y el tipo de soporte que comprenda la opción de almacenamiento secundario. Por ejemplo, el SATA cerca de la línea será mucho más rápido que la cinta. Se pueden cifrar todos los archivos en una cinta para disponer de una seguridad adicional cuando lleguen a la fase de archivado a largo plazo de la solución, lo que puede requerir licencias adicionales.

Recomendaciones de copia de seguridad de Dell

Copia de seguridad de los archivos de la evidencia y el caso

Los laboratorios forenses tienen tres tipos de archivos principales:

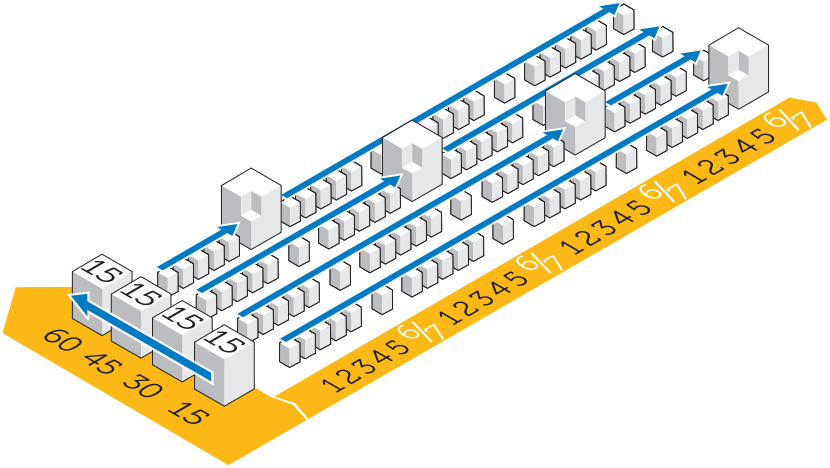
- Archivos de imagen: son las imágenes forensemente válidas del dispositivo sospechoso. Una vez examinados nunca cambian y solo es necesario hacer copia de seguridad de ellos una vez (posibles extensiones: **E01**, **DD**, etc.). Los archivos de evidencias tienden a encontrarse en menor cantidad, pero con un tamaño muy grande.

- Archivos del caso: son los archivos de datos y los índices que constituyen el resultado de los análisis; es posible que sea necesario exportarlos fuera de la aplicación forense. Los archivos cambian frecuentemente si el caso está activo y pueden contener muchos tipos de extensiones, siendo necesario hacer copia de seguridad de ellos de forma diaria. Los archivos del caso tienden a ser numerosos en cantidad, pero normalmente tienen un tamaño muy pequeño.
- Base de datos: este tipo de archivos se usa solamente en FTK 3 (por el momento), pero contienen todos los vínculos entre los archivos del caso y los archivos de la evidencia, así como todos los marcadores y notas de la investigación. Se debe hacer copia de seguridad de los tipos de archivo de bases de datos de forma diaria.

Ilustración 7-2 muestra la buena práctica recomendada para hacer copias de seguridad de un laboratorio forense digital. Debido al hecho de que muchos laboratorios forenses tienen más de 50 TB de almacenamiento, es posible que no se pueda realizar una copia de seguridad completa en una ventana de copia de seguridad semanal estándar. Para asegurar que se pueden restaurar los datos en el caso de un desastre con el punto de recuperación mínimo posible, la copia de seguridad se divide en secciones iguales y se ejecuta en el espacio de un mes.

Este proceso requiere que se restrinja el tamaño de las copias de seguridad completas a un máximo de 15 TB. Después cada LUN realiza actualizaciones incrementales durante el resto del ciclo de la copia de seguridad hasta que vuelva a corresponder una copia completa.

Ilustración 7-2. Buenas prácticas de los planes de copias de seguridad



Fuera del host o Red

Debido al tamaño de los datos que es necesario mover a cinta a efectos de recuperación ante desastres en la mayoría de laboratorios forenses, el almacenamiento de los LUN se divide en LUN de 15 TB. Este requisito permite una gestión y copia de seguridad más sencillas, reduciendo también los problemas de clúster del sistema de archivos que pueden aparecer con el tiempo en el caso de que se produzcan errores.

Se pueden realizar dos tipos de copia de seguridad, bien sea por la red o como copia de seguridad fuera del host.

- En una configuración por la red, los datos de la copia de seguridad se transmiten por la red al servidor de copia de seguridad usando un agente de copia que reside en el servidor.
- En una solución de copia de seguridad fuera del host, algunos de los servidores con los almacenamientos de archivos más grandes no hacen copia de seguridad de sus datos por la red. En lugar de ello, la matriz de almacenamiento toma una instantánea del LUN y después monta esta copia directamente en el servidor de copia de seguridad. Este proceso aumenta la velocidad global de la copia de seguridad puesto que no se transmiten archivos de la copia por la red normal que pueden crear problemas adicionales de contención de la red.

En muchos laboratorios forenses de la actualidad, las copias de seguridad se realizan por redes de 10 GB.

En la siguiente figura se muestran los agentes que se requieren por servidor para llevar a cabo las copias de seguridad:

Ilustración 7-3. Agentes de la copia de seguridad

Name	Qty	Type	Application	OF	AD	OA	SA	BE	NBU	EV	Cluster	MI	SS
	1	M610	SQL Server	X			X				No	X	X
	1	M610	NTP file auditor	X							No		X
	2	M610	Active Directory	X	X						No	X	X
	4	M610	Siloed Citrix	X							No		X
	7	M610	FTK & Oracle	X		X					No	X	X
	2	M910	File Server	X							Yes	X	X
	2	M610	Encase & FTK1.8	X							No		X
	1	M610	Enterprise Vault	X						20 Users	No		X
	2	R710	Backup Exec	X				X			No	X	X
	0	n/a	Web Server	X							No		X

OF Open File Agent

AD Active Directory

OA Oracle Agent (agente de bases de datos genérico requerido en Backup Exec de Symantec)

SA SQL Agent (agente de bases de datos genérico requerido en Backup Exec)

NBU Net Backup Server

BE Backup Exec Server

EV Licencia de copia de seguridad de Symantec Enterprise Vault

MI Copia de seguridad completa mensual, incremental diariamente

SS Estado del sistema tomado una vez al mes

NOTA: Puesto que la cantidad de datos crece con el tiempo, es posible que se requiera una solución de copia de seguridad fuera del host.

Cómo realizar el archivado usando la solución Digital Forensics de Dell

Archivado bajo demanda

NTP Software ODDM y NTP Software Right-Click Data Movement (RCDM) funcionan junto con Enterprise Vault para disminuir la necesidad de exploraciones de todo el sistema de archivos, como en el caso del archivado convencional, aplicando el *archivado bajo demanda*. Los costes de almacenamiento se reducen y se mejora la calidad del archivado.

Dependiendo de la etapa del ciclo de vida de los datos, como se describe en "Adaptación del archivado y la recuperación a la vida del caso" en la página 67, el analista puede elegir archivar datos en un almacenamiento a largo plazo o mantener los datos para un acceso y procesamiento inmediatos.

Además, se puede usar NTP Software ODDM para archivar datos automáticamente que se deben guardar con fines legales.

Requisitos

NTP Software ODDM requiere Microsoft IIS, Microsoft .NET Framework, SQL y Enterprise Vault. NTP Software ODDM y Enterprise Vault deben estar instalados en el mismo servidor. Las instalaciones más grandes pueden mantener la base de datos SQL en un servidor dedicado.

Instalación

Para ver instrucciones detalladas sobre la instalación de NTP Software ODDM y NTP Software RCDM, consulte la *Guía de instalación y configuración de Digital Forensics de Dell*. Para obtener más información, consulte "Documentación relacionada y recursos" en la página 16.

Archivado usando NTP Software ODDM

Archivado realizado por el usuario

1 Cuando el analista guarda archivos de datos, NTP Software QFS alerta al usuario de que es necesario archivar los archivos.

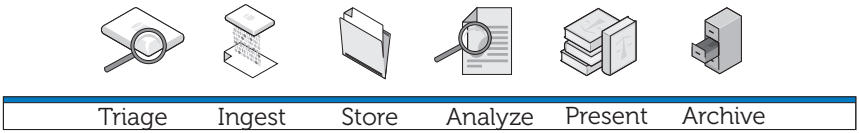
2 El analista selecciona los archivos a archivar usando el NTP Software Storage Investigator y después hace clic en **Archive**. Sin embargo, si está instalado el complemento NTP RCDM, hará clic con el botón derecho en los archivos.

Una vez seleccionados los archivos, el NTP Software Storage Investigator informa a NTP Software ODDM, que a su vez activa Enterprise Vault.

La solicitud de archivado se agrega a la cola de archivado.

8

Solución de problemas



Sugerencias generales para la solución de problemas

- Asegúrese de que todos los clientes y servidores pueden comunicarse, que pueden hacer ping tanto por el nombre de NetBIOS como por la dirección IP.
- Asegúrese de que los servidores de seguridad permiten el tráfico.
- Reinicie los servidores y clientes para asegurarse de que los sistemas han reconocido todos los cambios realizados en la instalación y la configuración.

Problemas específicos de software de Forensics

EnCase: EnCase se abre en el modo de adquisición

Este problema indica que EnCase no tiene licencia.

1. Dentro de EnCase seleccione **Tools→ Options** y asegúrese de que **User Key Path**, **Server Key Path** y **Server Address** están cubiertos (estos campos deben apuntar a las ubicaciones de las claves de la licencia).
2. Compruebe el servidor de seguridad del cliente y del servidor de la licencia de EnCase para asegurarse de que está abierto el puerto 4445.
3. Asegúrese de que el cliente puede hacer ping en el servidor de licencia de EnCase.

FTK Lab: el navegador iniciado por el cliente no puede mostrar la interfaz de usuario

1. Asegúrese de que el cliente tiene instalado MS Silverlight.
2. Asegúrese de que se han iniciado los servicios Oracle en el servidor que aloja la base de datos de Oracle.

FTK 1.8: mensaje de límite de 5000 objetos/versión de prueba

Si recibe este mensaje, FTK no tiene licencia. Asegúrese de que el servidor de la licencia de red está funcionando y que tiene las licencias de FTK 1.8:

1. Abra una ventana del navegador en el servidor que aloja el servicio de la licencia de red e introduzca **http://localhost:5555** en la barra de direcciones.
2. Observe si tiene las licencias. Si no las tiene, deberá instalarlas.

FTK 1.8: en el inicio aparece el error Cannot Access Temp File (No es posible acceder al archivo temporal)

Permita que el usuario abra la aplicación (o su sesión Citrix) para tener acceso al disco duro del servidor O BIEN ejecute la aplicación como administrador.

Problemas con Citrix

Citrix: las aplicaciones no se iniciarán

1. Asegúrese de que se han iniciado todos los servicios (en particular MFCOM y IMA) en los servidores que alojan XenApp.
2. Asegúrese de que el cliente puede ver y hacer ping en los servidores XenApp.
3. Compruebe el servidor de seguridad de los clientes y los servidores XenApp para asegurarse de que los puertos de XenApp están abiertos.
4. Compruebe el servidor de licencias de Citrix para asegurarse de que el servicio de concesión de licencias en red tiene una licencia que pueda conceder. Normalmente el servidor de concesión de licencias de Citrix está instalado en uno de los servidores Citrix XenApp, disponible a través de **Iniciar→ Programas→ Citrix→ Management Consoles→ Citrix Licensing**.

5 Abra la **consola de administración de Citrix** (**Iniciar→ Programas→ Citrix→ Management Consoles→ Citrix Delivery services console**). Después ejecute un descubrimiento para asegurarse de que todos los servidores XenApp se encuentran presentes en el conjunto de servidores.

6 Asegúrese de que la aplicación ha sido publicada en un servidor válido XenApp (que esté incluido en el conjunto de servidores).

7 Mire en la **Citrix Delivery Services Console** para asegurarse de que el usuario que inicia la aplicación está en un Grupo con permiso para abrir la aplicación.

8 Con las aplicaciones transmitidas, asegúrese de que el control de cuentas de usuarios (UAC) está desactivado en el servidor.

Sesiones de Citrix bloqueadas o con errores

Cuando los usuarios no cierran la sesión de Citrix correctamente, las sesiones huérfanas empiezan a ser más lentas y eventualmente pueden hacer que el servidor se bloquee o presente errores. Por tanto, es extremadamente importante que los usuarios sigan las buenas prácticas para cerrar las sesiones formal y correctamente (**Iniciar→ Cerrar sesión→ Aceptar**) y que no hagan simplemente clic en la *x* situada en la esquina superior derecha de la ventana de la sesión.

No obstante, todavía es posible encontrarse con este problema. He aquí dos formas de resolverlo:

1 Cierre manualmente la sesión del usuario.

   a Abra una sesión como administrador de Citrix.

   b Revise la lista de sesiones abiertas y cierre manualmente cada sesión.

2 Reinicie el servidor.

Índice

T