Dell™ Digital Forensics

Guia da Solução

Notas, Avisos e Advertências

NOTA: uma NOTA indica informações importantes que ajudam a usar melhor o computador.

AVISO: um AVISO indica um potencial de danos ao hardware ou de perda de dados caso as instruções não sejam seguidas.

ADVERTÊNCIA: uma ADVERTÊNCIA indica possibilidade de danos à propriedade ou risco de lesões corporais ou morte.

2011 - 07 **Rev. A00**

Sumário

1

Introdução

Nos últimos anos, tem havido um aumento exponencial do volume, velocidade, variedade e sofisticação da atividade digital realizada por criminosos e grupos terroristas ao redor do mundo. Hoje, a maioria dos crimes tem um componente digital. Alguns já usaram o termo *tsunami digital*. Esse crescimento foi aumentado pelos imensos avanços do hardware eletrônico. A diversidade crescente dos dispositivos eletrônicos disponíveis ao consumidor e sua memória e capacidade de armazenamento cada vez maiores oferecem aos criminosos e terroristas inúmeras oportunidades de ocultar informações prejudiciais.

Não é raro PCs e laptops virem com discos rígidos com centenas de Gigabytes de armazenamento. Os discos rígidos mais recentes incluem opções para um ou quatro Terabytes. Considere que um único Terabyte pode armazenar o conteúdo de duzentos DVDs: uma vasta quantidade de armazenamento que representa um problema que continuará a crescer.

Desde PCs até laptops, celulares a pen drives e até consoles de jogos, os profissionais forenses digitais estão sendo desafiados até o limite para clonar, ingerir, indexar, analisar e armazenar quantidades cada vez maiores de dados suspeitos, ao mesmo tempo em que preservam a cadeia de custódia digital e continuam a proteger os cidadãos.

Tabela 1-1. Qual é o tamanho de um Zettabyte?

Kilobyte (KB)	1.000 bytes	2 KB	uma página digitada
Megabyte (MB)	1.000.000 bytes	5 MB	as obras completas de Shakespeare
Gigabyte (GB)	1.000.000.000 bytes	20 GB	uma boa coletânea das obras de Beethoven
Terabyte (TB)	1.000.000.000.000 bytes	10 TB	uma biblioteca de pesquisa acadêmica
Petabyte (PB)	1.000.000.000.000.000 bytes	20 PB	produção anual de discos rígidos
Exabyte (EB)	1.000.000.000.000.000.000 bytes	5 EB	todas as palavras já ditas por seres humanos
Zettabyte (ZB)	1.000.000.000.000.000.000.000 bytes	2 ZB	quantidade de dados criada globalmente durante o ano de 2010*

* Roger E. Bohn, et. al., How Much Information? 2009, Global Information Industry Center, University of California, San Diego (Janeiro de 2010).

Quando criminosos suspeitos são acusados e computadores e outros ativos digitais são confiscados, os profissionais forenses digitais ficam sob enorme pressão para processar e analisar evidências potenciais em um período muito curto de tempo e em ambientes longe do ideal para assegurar os requisitos necessários a evidências. Quando organizações inteiras são suspeitas de atividades criminosas ou terroristas, o número de dispositivos a serem analisados pode aumentar drasticamente.

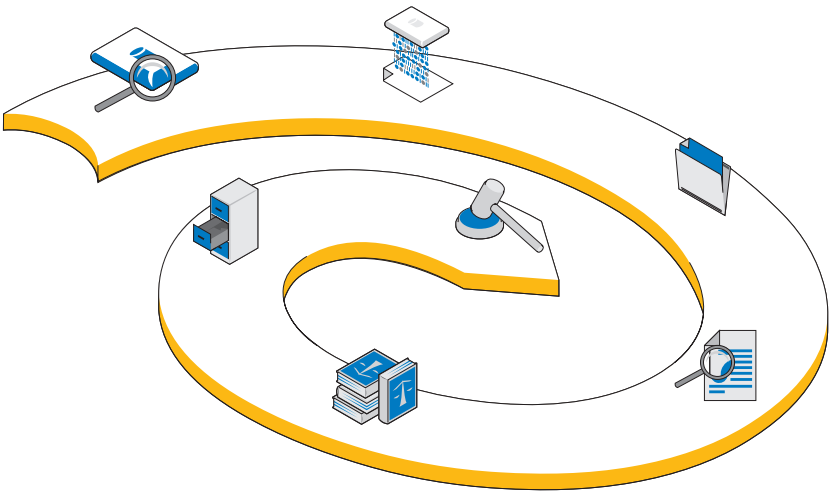
O Digital Forensics proporciona um meio de adquirir dados recuperados de computadores e de outros dispositivos digitais (celulares, consoles de jogos, unidades flash, GPSs, etc.), bem como o exame e análise científica desses dados de maneira a garantir que as informações possam ser usadas em tribunal. A solução Dell Digital Forensics representa a primeira verdadeira solução de ponta a ponta de nível empresarial para órgãos de segurança corporativa e governamental de imposição da lei, proporcionando todo o hardware, software, suporte e serviço necessário para coletar, triar, ingerir ou criar imagem, armazenar, analisar, elaborar relatórios e arquivar evidências digitais.

Usando o hardware escalável e acessível para servidor empresarial e armazenamento da Dell e – dependendo de seu ambiente de software – sistemas de banco de dados Oracle no back-end, uma combinação de laptops reforçados da Dell e software SPEKTOR em campo e o serviço e suporte completos da Dell, os investigadores podem conduzir, com rapidez e simplicidade, a triagem e coleta de dados forenses digitais, assegurando a cadeia de custódia desde o campo até o data center, e no tribunal.

Ciclo de vida do Dell Digital Forensics

A solução Dell Digital Forensics presta suporte ao investigador forense durante os seis estágios do ciclo de vida forense: Triagem, Ingestão, Armazenamento, Análise, Apresentação e Arquivamento.

Figura 1-1. Ciclo de vida do Dell Digital Forensics



Triagem

O processo de triagem oferece ao investigador forense digital a oportunidade de visualizar rapidamente o conteúdo de dispositivos de destino a fim de determinar se o dispositivo deve ou não ser removido para o laboratório para aprofundamento da análise e preparação para apresentação em tribunal.

 *Ingestão*

A Ingestão é o estágio do processo forense digital em que se cria uma imagem dos dados de destino (a menos que a imagem tenha sido criada em campo, como parte do estágio de Triagem) e uma cópia exata do dispositivo de armazenamento suspeito é criada, de modo que a integridade da duplicata possa ser assegurada pela comparação dos hashes das unidades de dados original e duplicada.

De acordo com as práticas existentes, a *imagem* dos dados suspeitos é criada na solução Dell Digital Forensics. No entanto, em vez de criar a imagem dos dados em uma única estação de trabalho, os dados da imagem são ingeridos em um repositório central de evidências. Por terem sido imediatamente ingeridos no data center, os dados ficam disponíveis para várias análises, a transferência de um dispositivo para outro é minimizada e a produtividade e eficiência são consideravelmente aumentadas. No entanto, a ingestão pode acontecer em campo se a capacidade de armazenamento de destino for pequena o suficiente. A solução Dell Digital Forensics proporciona a ingestão na localidade por meio do uso do módulo opcional SPEKTOR Imager.

 *Armazenamento*

A solução Dell Digital Forensics proporciona uma grande variedade de opções possíveis de armazenamento e acesso pela rede a fim de atender às necessidades de cada cliente. O armazenamento e a recuperação em alta velocidade no ambiente de rede de nível empresarial possibilita uma configuração multiusuário que aumenta a eficiência e a produtividade. Os analistas não precisarão mais alocar seus ativos individuais de computação para concluir a análise da evidência, visto que tudo isso acontecerá no servidor dedicado a essa finalidade.

 *Análise*

A capacidade de processamento paralelo oferecida pela solução Dell Digital Forensics permite ao analista indexar e triar dados em servidores de alto desempenho em vez de se valer de PCs individuais muito menos poderosos. Além disso, várias sessões de analistas podem ser executadas simultaneamente em uma única ou em várias estações de trabalho usando as configurações de back-end de que a Solução se compõe. Essa capacidade ajuda a proteger tanto o sistema quanto a integridade das evidências, ajuda a evitar a necessidade de refazer a estação de trabalho caso algum código mal-intencionado seja executado por engano, ajuda a preservar a cadeia de custódia e elimina a necessidade de refazer da estação de trabalho ao passar de um caso para outro. No ambiente do Digital Forensics, a *Cadeia de custódia* pode ser definida como a manutenção da integridade dos dados digitais como evidência, desde o momento de sua coleta, durante o tempo em que os achados são relatados e até que sejam apresentados em tribunal.

Apresentação

Usando a solução Dell Digital Forensics, as equipes e os investigadores que cuidam da visualização podem acessar evidências potenciais do caso com segurança e em tempo real, o que atenua a necessidade de liberar evidências em DVDs ou de solicitar o deslocamento de especialistas até o laboratório para fins de acesso aos arquivos.

Arquivamento

A Solução da Dell oferece uma infraestrutura formalizada de backup, recuperação e arquivamento para ajudar a otimizar a cooperação entre os órgãos e as divisões de segurança e até entre fronteiras, liberar a sobrecarga administrativa, proporcionar consistência entre os laboratórios e minimizar os riscos para a cadeia de custódia digital.

Além disso, o projeto da solução Dell Digital Forensics inclui um componente de pesquisa opcional que permite a correlação das informações entre conjuntos de dados ingeridos.

A Solução da Dell facilita os pontos problemáticos do setor

O uso da solução Dell Digital Forensics pode tornar o processo de trazer evidências digitais da cena do crime para o tribunal infinitamente mais simples para os profissionais investigadores por fornecer:

- Rede de data center de última geração, que acelera a ingestão, a análise e o compartilhamento das informações digitais
- Garantia da informação, pela maior automação do processo forense digital, o que reduz o risco de erro e de comprometimento dos dados
- Garantia adicional da integridade dos dados, atualmente pelo uso dos protocolos de hash mais seguros, e em breve pela implementação de um recurso de auditoria que ajudará a automatizar os registros da cadeia de custódia

NOTA: quaisquer conclusões ou recomendações neste documento que possam se assemelhar a orientações legais devem ser examinadas por meio de um aconselhamento jurídico. Verifique sempre junto à jurisdição local, ao promotor público local e ao laboratório forense local com relação a seus métodos preferenciais de coleta de evidência digital.

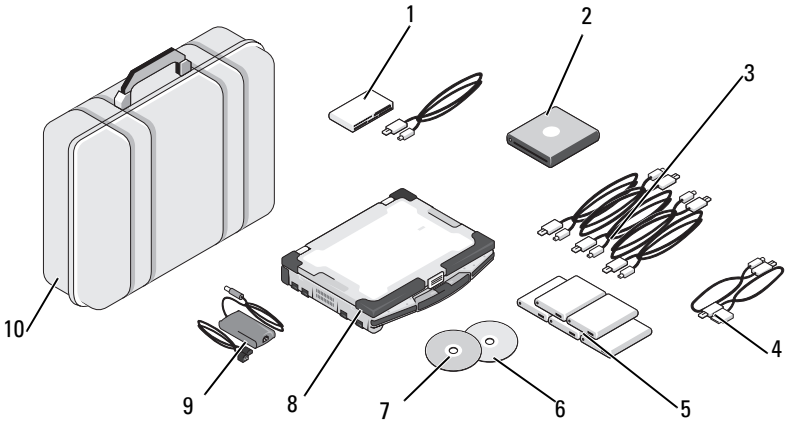
- Uma solução de ponta a ponta que reduz significativamente a complexidade do planejamento, da implementação e do gerenciamento de um processo forense digital de nível empresarial
- Uma solução acessível e flexível, modular, escalável e expansível pela qual você paga à medida que utiliza

Componentes da Solução

Em campo

A parte móvel da solução cabe em um estojo rígido projetado para caber no compartimento de bagagens acima das poltronas de um avião. O estojo reforçado comporta todas as ferramentas e softwares necessários para triagem no local de dispositivos de armazenamento suspeitos, além de incluir um Laptop reforçado Dell E6400 XFR com software forense SPEKTOR pré-instalado, Bloqueadores de gravação forenses da Tableau com acessórios, um número opcional de discos rígidos USB externos licenciados para o trabalho com o software SPEKTOR como *coletores* de imagens de triagem, um leitor de cartão 50:1 e os adaptadores e cabos relacionados na Figura 1-2.

Figura 1-2. Solução Dell Digital Forensics: componentes móveis



1	Leitor de cartão 50:1	6	Disco de restauração de imagem
2	USB DVD ROM	7	Disco de inicialização do SPEKTOR
3	Cabos USB do Coletor	8	Laptop reforçado da Dell
4	Cabos telefônicos opcionais para SPEKTOR PI (opcional)	9	Fonte de alimentação do laptop reforçado da Dell
5	Coletores do disco rígido externo (5)	10	Estojo Pelican

No data center

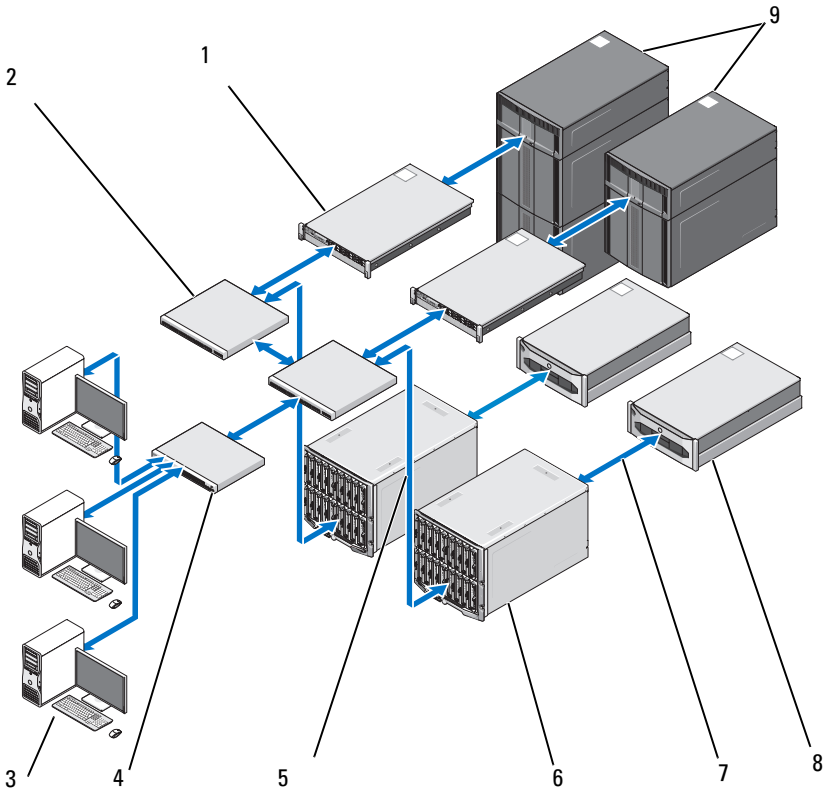
No data center, a solução Dell Digital Forensics inclui uma configuração personalizada que consiste nos seguintes componentes:

- Servidores de rack Dell PowerEdge R410, R610 e R710
- Servidores blade Dell PowerEdge M610 e M710
- SAN Dell EqualLogic séries 4000\6000
- Windows Server 2008 R2
- Citrix XenApp 6.0
- AccessData FTK 1.8, AccessData FTK 3, AccessData Lab
- Guidance EnCase 6.15

- NTP Software On-Demand Data Management (ODDM)
- Symantec Enterprise Vault
- Symantec Backup Exec 2010
- Switches Dell PowerConnect
- Switches Extreme Networks

Os servidores blade e de rack Dell PowerEdge podem desempenhar diversos papéis: servidor de arquivos, servidor de evidências, servidor de arquivamento, servidor de banco de dados, servidores de licenças do EnCase e do FTK, servidor de backup ou controlador de domínio. Eles oferecem suporte ao Microsoft Active Directory e a todo o software forense e de segurança que compõem a solução Dell Digital Forensics.

Figura 1-3. Solução Dell Digital Forensics: data center



1	Servidor PowerEdge R410 ou servidor R610 (opcional)	6	Servidores blade Dell PowerEdge M1000E e M610
2	Switch Dell PowerConnect	7	Fluxo de dados de 10 GB
3	Estação de trabalho Dell Precision ou OptiPlex	8	Sistemas de armazenamento Dell EqualLogic série PS4000 ou PS6000
4	Switch Dell PowerConnect	9	Armazenamento Dell PowerVault classe ML
5	Fluxo de dados de 1 GB		

Sobre este documento

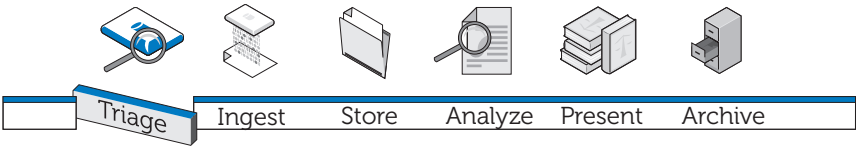
Este documento abrange cada estágio do processo forense digital em seu próprio capítulo, com capítulos adicionais sobre solução de problemas e hardware e software compatíveis com a Solução. Cada um dos capítulos sobre o processo começa com uma discussão das melhores práticas e dos problemas específicos que você pode encontrar ao implementar e gerenciar a Solução e, em seguida, passa para instruções passo a passo sobre as várias ferramentas e componentes relevantes a esse estágio da Solução.

Documentação e recursos relacionados

Você pode acessar informações adicionais em **support.dell.com/manuals**.

2

Triagem



O que é Triagem?

A Triagem permite ao investigador forense digital navegar pelos dados contidos em dispositivos suspeitos e tomar decisões quanto a quais dispositivos realmente constituem evidência e são dignos de confisco para criação imediata de imagem no local (se os dados representarem um pequeno volume) ou para criação posterior da imagem no data center. Essa capacidade de prever e confiscar somente dispositivos de destino selecionados pode reduzir substancialmente os atrasos que afetam a capacidade dos investigadores de apresentar evidência em tempo hábil. A Triagem pode reduzir o acúmulo de dispositivos de armazenamento aguardando a criação de imagem no laboratório forense, usar menos recursos, evitar acréscimos a uma fila de ingestão já sobrecarregada e reduzir drasticamente os custos operacionais.

Vantagem da solução de triagem da Dell

Móvel

A solução Dell Digital Forensics pode estar na cena do crime com o investigador. Todos os componentes foram cuidadosamente pré-testados para funcionarem juntos e abrangem uma ampla variedade de portas e conectores de dispositivos de destino que possam ser encontrados em campo.

Rápida

As soluções de triagem forense existentes podem ser lentas e até podem deixar passar dados por executarem tarefas, como pesquisas de palavras-chave ou correspondência de hash durante a coleta de dados. A solução Dell Digital Forensics supera esse obstáculo usando o poder computacional do laptop reforçado da Dell em vez do PC de destino para executar a análise dos dados coletados. Em alguns casos, é possível contornar completamente os processos de criação de imagem e indexação no laboratório forense.

Fácil de usar

Os componentes de Triagem da Solução já estão prontos para usar diretamente do estojo rígido. O software pré-instalado oferece uma interface intuitiva com tela sensível ao toque. Perfis de coleta reutilizáveis definidos pelo usuário para diferentes cenários podem ser criados para implantação padrão.

Aceitável do ponto de vista forense

O software de Triagem impõe um processo eficiente e aceitável do ponto de vista forense, garantindo que qualquer evidência potencial seja capturada, examinada e armazenada sem comprometimento.

Flexível

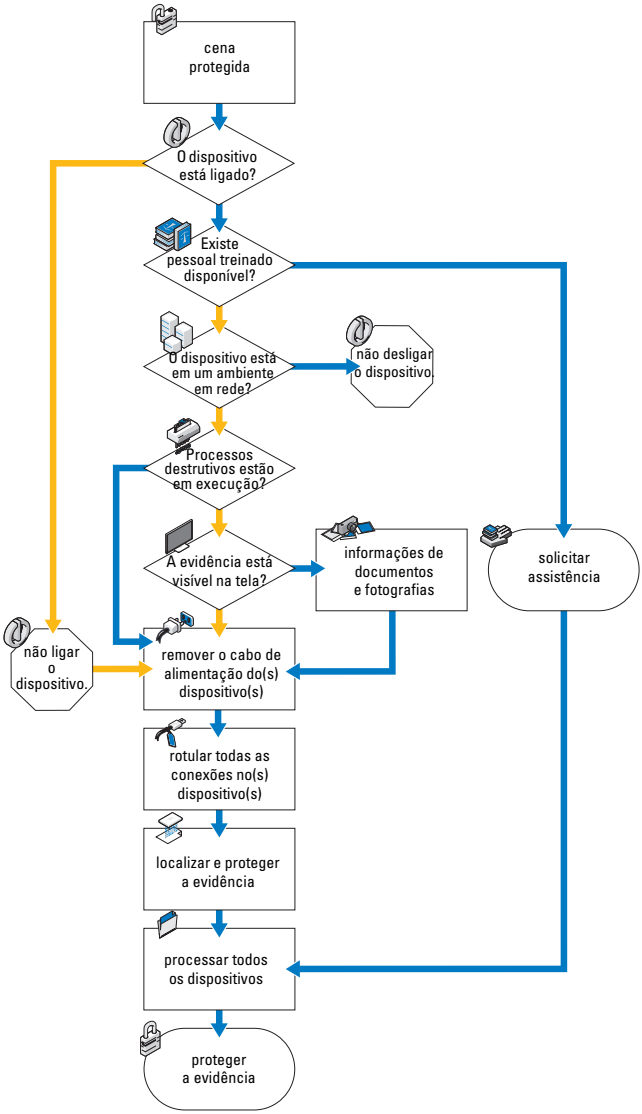
Os componentes de Triagem podem ser usados para examinar os dispositivos de armazenamento digital e as plataformas mais comuns, inclusive dispositivos que executam sistemas operacionais tanto Windows quanto Apple Mac OS X, bem como uma grande variedade de tipos de dispositivos de armazenamento digital, como MP3 players, discos rígidos externos, cartões de memória, telefones celulares e via satélite, unidades de GPS, iPads e iPhones e unidades flash. Além disso, os resultados da triagem feita com a solução Dell Digital Forensics podem ser exportados para outros programas.

Poderosa

O laptop reforçado da Dell controla todo o processo, desde a execução de uma análise automatizada dos dados de destino até o fornecimento de resultados detalhados em um formato de relatório fácil de usar, pronto em questão de minutos da captura dos dados. Usando a Solução da Dell, o investigador poderá executar várias varreduras de triagem em paralelo com uma única chave de licença.

Como coletar evidência forense digital

Figura 2-1. Fluxo de trabalho da coleta



Aquisição padrão x Aquisição ao vivo

A solução Dell Digital Forensics oferece dois tipos de aquisição: Standard (Padrão) e Live (Ao vivo). Durante um procedimento de aquisição padrão, o laptop reforçado da Dell usa o disco de inicialização do SPEKTOR para capturar dados de triagem de um dispositivo de armazenamento de destino já desativado. Um procedimento de triagem de aquisição ao vivo, por outro lado, se destina a capturar dados de triagem de um dispositivo de armazenamento de destino ainda ativado, o que permite a obtenção de evidência que não estaria disponível de outra forma.

Anteriormente, os padrões do setor exigiam que o investigador desconectasse e confiscasse um dispositivo digital para transporte e exame no laboratório. Essa prática significava a perda de evidência potencialmente valiosa na forma de dados voláteis armazenados: quaisquer dados armazenados na área de transferência, arquivos abertos no momento, o conteúdo da RAM, senhas armazenadas em cache, etc. E ainda, dados criptografados podiam ser perdidos se o computador fosse desligado antes da criação da imagem do disco. Além disso, muitos computadores têm senhas de BIOS e de disco rígido determinadas pelo usuário, e remover a energia de um sistema ativo com senha de BIOS pode causar a perda do acesso a todo o conteúdo do dispositivo.

As melhores práticas do setor exigem que o investigador aborde um dispositivo de armazenamento de dados suspeito com as seguintes orientações em mente:

- Se o dispositivo estiver ligado, mantenha-o ligado sempre que possível até que uma investigação completa possa ser executada.
- Se o dispositivo estiver desligado, deixe-o desligado.

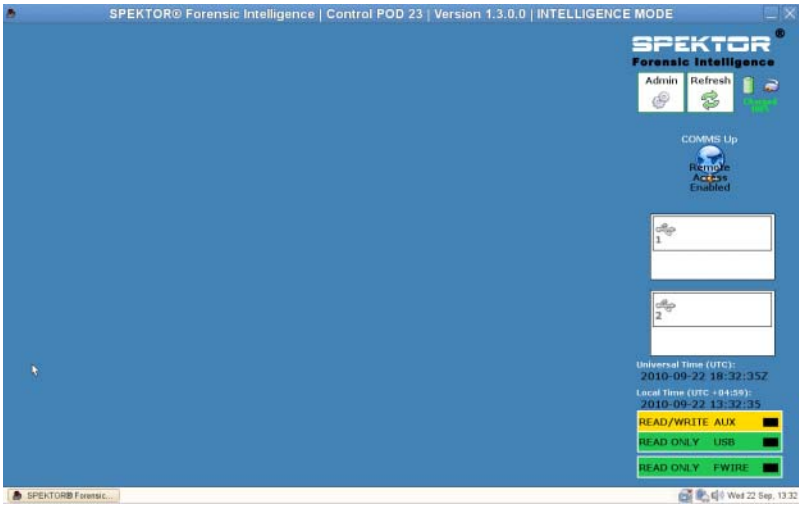
O motivo para essas orientações é que o investigador precisa tomar cuidado para preservar o dispositivo de armazenamento nas condições em que o encontrou na cena, introduzindo tão poucas alterações quanto possível ao dispositivo e seu conteúdo.

Como executar a Triagem usando a solução Dell Digital Forensics

Ligar seu laptop reforçado da Dell

1. Pressione o botão liga/desliga para fazer login no laptop reforçado da Dell. O laptop carrega automaticamente o software SPEKTOR.
2. Toque ou clique em **Accept EULA**. A tela **Home** (Início) é aberta.

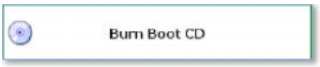
Figura 2-2. Tela Home (Início)



Gravar um CD de inicialização para procedimentos de Aquisição padrão

1 Na tela **Home** (Início), toque ou clique em **Admin**. Em seguida, toque ou clique em **Burn Boot CD**.

Figura 2-3. Botão Burn Boot CD (Gravar CD de inicialização) na tela Home (Início)



2 Siga as instruções na tela e, em seguida, clique em **Finish**.

Registrar um Coletor ou Disco de armazenamento

NOTA: Coletores precisam ser licenciados e configurados pela SPEKTOR para poderem ser usados com a solução Dell Digital Forensics. Entre em contato com o administrador de seu sistema se precisar de Coletores ou licenças adicionais.

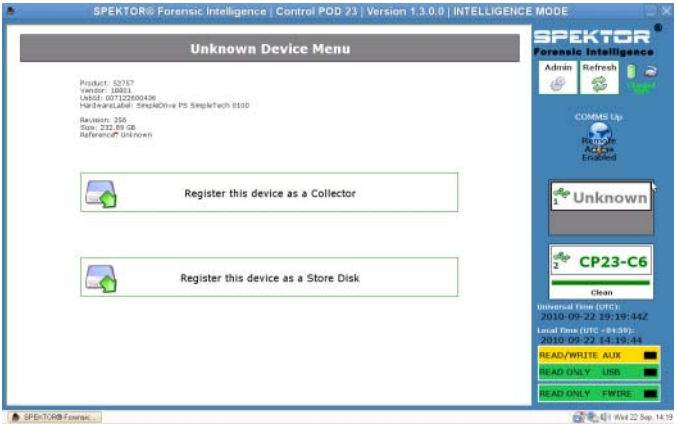
1 Conecte um novo Coletor ou disco de armazenamento a uma das portas USB do lado esquerdo do laptop reforçado da Dell. O dispositivo é exibido na tela como dispositivo não reconhecido.

Figura 2-4. Indicador de Coletor ou Disco de armazenamento desconhecido

2 Toque ou clique no ícone **Status Indicator** (Indicador de status) correspondente ao Coletor ou disco de armazenamento conectado ao laptop reforçado da Dell. O ícone do dispositivo que foi registrado ficará verde (no caso de um Coletor) ou laranja (para um disco de armazenamento).

3 O **Unknown Device Menu** será exibido.

Figura 2-5. Unknown Device Menu (Menu de dispositivo desconhecido)



4 Toque ou clique em **Register this device as a Collector** ou **Register this device as a Store Disk**.

5 Toque ou clique em **Yes**.

O indicador de status mostrará o número do novo Coletor ou disco de armazenamento e seu status mudará para **Dirty**.

Figura 2-6. Ícones de Coletor e disco de armazenamento sujos

NOTA: os Coletores e discos de armazenamento, independentemente de terem sido recém-registrados ou usados previamente em outras coletas de dados, precisam ser limpos para que possam ser usados no destino.

6 *Somente no caso de um disco de armazenamento*, insira o número de série do disco de armazenamento.

Limpar um Coletor ou Disco de armazenamento

NOTA: reservar aproximadamente duas horas para cada 100 GB de volume do Coletor.

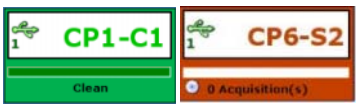
1 Selecione o **Status Indicator** (Indicador de status) que representa o Coletor a ser limpo.

2 No **Collector Menu**, toque ou clique em **Clean Collector**.

3 Toque ou clique em **Yes** (Sim) para confirmar sua seleção. A limpeza começa e o **Status Indicator** (Indicador de status) confirma o progresso da limpeza.

Quando a limpeza for concluída, o software executará um programa de verificação para confirmar que os únicos caracteres na unidade do Coletor sejam zeros.

Figura 2-7. Indicadores de status de Coletor e disco de armazenamento registrado e limpo



NOTA: se o processo de limpeza não tiver sido bem-sucedido, o indicador de status indicará que o Coletor permanece sujo. Será preciso reiniciar o processo de limpeza. Se a limpeza for malsucedida uma segunda vez, experimente usar outro Coletor ou disco de armazenamento.

Configurar um perfil de Coletor

NOTA: por padrão, as definições da configuração do software de triagem são definidas para não coletar arquivos. Especifique um subconjunto restrito de todos os arquivos no dispositivo de destino para reduzir o tempo de coleta e evitar exceder a capacidade do Coletor.

Configurar um Coletor permite ao usuário determinar uma série de tipos de arquivo específicos ou arquivos criados entre um conjunto de datas específico que o Coletor extrairá do dispositivo de armazenamento suspeito para triagem. Quanto mais você puder restringir os parâmetros de coleta, mais rapidamente os dados de destino podem ser adquiridos para exame.

A Dell recomenda estabelecer um conjunto de perfis de configuração padrão encontrados repetidamente por você ou por sua entidade. Estes são exemplos de perfis de configuração padrão:

- Photos and Videos (Fotos e vídeos) para capturar tipos de arquivo como ***.jpg**, ***.png**, ***.swf**, ***.vob** e ***.wmv**, que são associados a fotografias, vídeos e outros tipos de mídia visual
- Documents (Documentos) para coletar especificamente todos os arquivos dos tipos ***.pdf**, ***.doc**, ***.docx**, ***.txt**.
- Audio_Files (Arquivos de áudio) para reunir ***.mp3**, ***.mp4**, ***.wav** e outros arquivos de áudio.

Como configurar um Coletor para aquisição

NOTA: para obter uma explicação das diferenças entre a aquisição padrão e ao vivo, consulte "Aquisição padrão x Aquisição ao vivo" na página 20.

NOTA: quando um Coletor está configurado para aquisição padrão ou ao vivo, precisa ser limpo para poder ser reconfigurado para uso no outro tipo de aquisição.

1 No **Collector Menu**, toque ou clique em **Configure Collector**.

Figura 2-8. Collector Menu (Menu do Coletor)

2 Se você tiver criado previamente um perfil de configuração que deseje usar, selecione o perfil e toque ou clique em **Configure using selected profile** para iniciar a configuração do Coletor. Caso contrário, toque ou clique em **New** para criar um novo perfil.

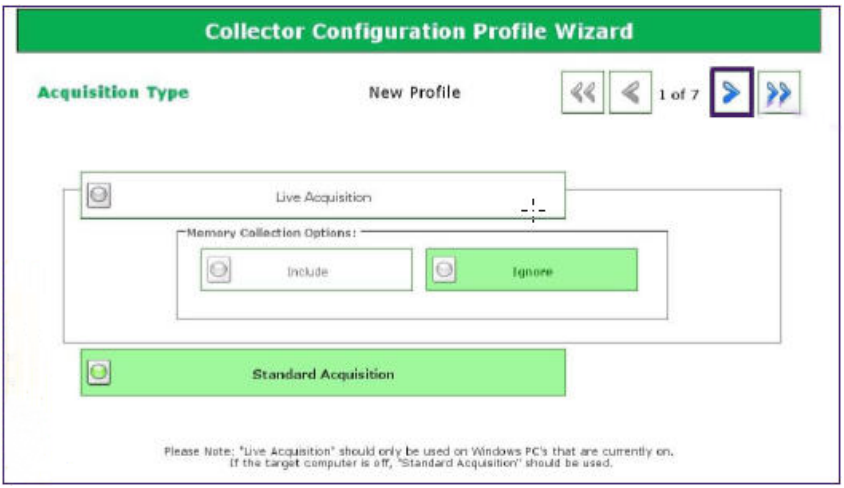
NOTA: a Figura 2-9 mostra a tela **Selecionado Profile** (Perfil selecionado) na primeira vez que o software é usado, antes que quaisquer perfis tenham sido definidos e salvos. Quando você começar a criar perfis de configuração, eles serão exibidos neste tela para seu uso.

NOTA: a navegação de uma tela Collector Configuration (Configuração do Coletor) para outra é feita tocando-se ou clicando-se nos botões de seta para a esquerda ou direita na parte superior e lateral da tela.

Figura 2-9. Selecionar perfil

3 Determine o tipo de aquisição que deseja executar, Ao vivo ou Padrão (consulte "Aquisição padrão x Aquisição ao vivo" na página 20 para obter mais informações sobre a diferença entre os tipos de aquisição Ao vivo e Padrão) e, em seguida, toque ou clique em **Live Acquisition** ou em **Standard Acquisition**.

Figura 2-10. Etapa 1 da Configuração de perfil: Tipo de aquisição



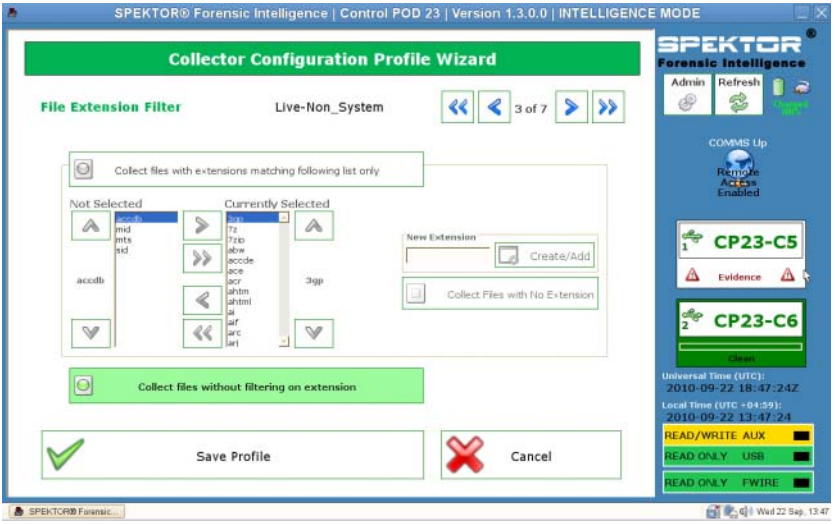
4 Determine as configurações de carimbo de data e hora para seu novo perfil. Quanto mais específico você puder ser, menos tempo levará para processar os arquivos capturados.

Figura 2-11. Etapa 2 da Configuração de perfil: Configurações de carimbo de data e hora dos arquivos

5 Clique na seta para a direita no canto superior direito da tela.

6 Na tela **File Extension Filter**, selecione os tipos de arquivo que deseja coletar. Use a seta para a direita para mover os tipos de arquivo selecionados e as extensões a eles associados da caixa de listagem **Not Selected** para **Currently Selected**.

Figura 2-12. Etapa 3 da Configuração de perfil: Filtro de extensão de arquivo



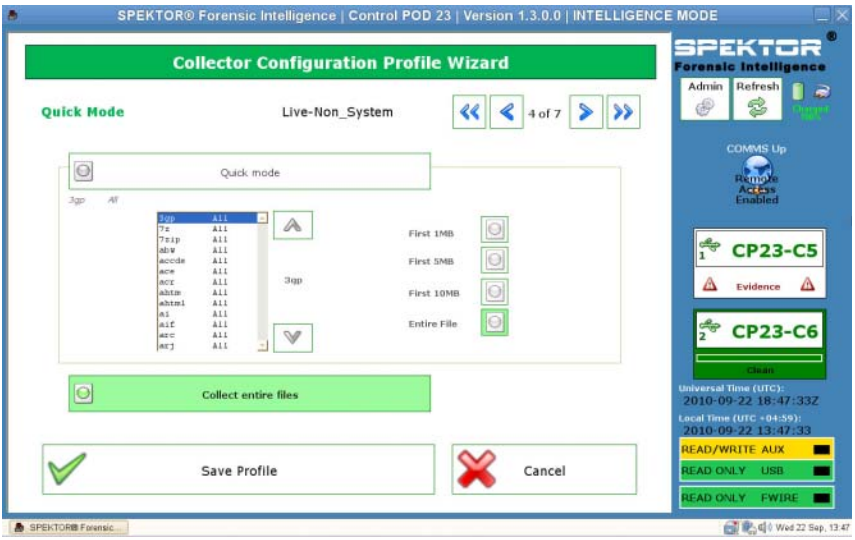
7 Clique na seta para a direita no canto superior direito da tela quanto tiver terminado de selecionar os tipos de arquivos e as extensões.

NOTA: a menos que seja especificamente necessário, sugere-se deixar o Quick Mode (Modo rápido) desligado.

8 Na tela **Quick Mode**, selecione o número de megabytes (**1 MB**, **5 MB**, **10 MB** ou **Entire File**) da primeira parte dos arquivos que você deseja capturar. Coletando apenas a primeira parte de arquivos muito grandes (geralmente arquivos multimídia), você poderá examinar uma parte suficiente dos arquivos para determinar o assunto, ao mesmo tempo em que minimiza o tempo de processamento necessário.

NOTA: se você não tiver selecionado as extensões de arquivo na etapa 6, nenhum arquivo será coletado e nenhum tipo de arquivo seja exibido na tela para seleção. Volte à etapa 6 e selecione os tipos de arquivo necessários a serem ativados na etapa 8.

Figura 2-13. Etapa 4 da Configuração de perfil: Quick Mode (Modo rápido)



9 Clique na seta para a direita no canto superior direito da tela.

10 Toque ou clique no botão apropriado para selecionar os arquivos de sistema que você deseja incluir na coleta.

Figura 2-14. Etapa 5 da Configuração de perfil: Arquivos de sistema

11 Clique na seta para a direita no canto superior direito da tela.

12 Na tela **Deleted File Filter**, determine se deseja ou não incluir arquivos ao vivo e excluídos, somente arquivos ao vivo ou somente arquivos excluídos na coleta. Se você não selecionar nenhuma dessas opções, não coletará nenhum arquivo.

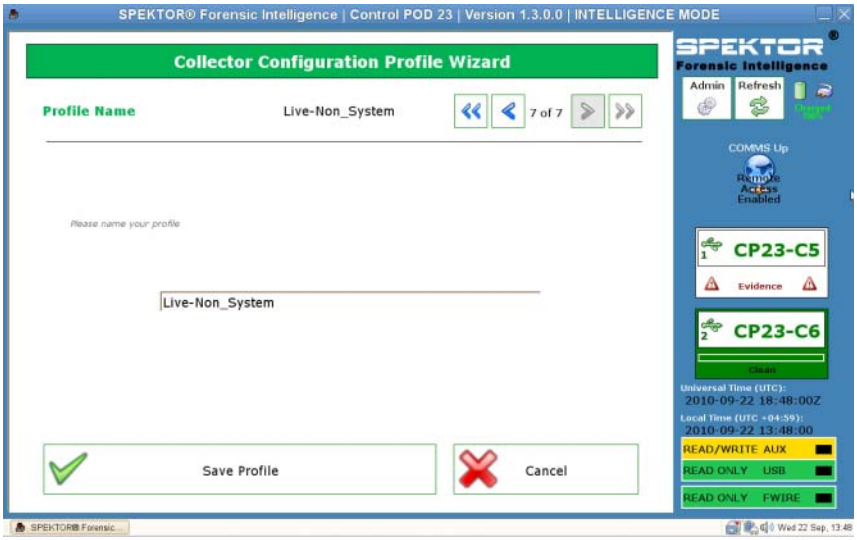
Figura 2-15. Etapa 6 da Configuração de perfil: Filtro de arquivos excluídos

NOTA: provavelmente, somente os arquivos excluídos que ainda não tiverem sido sobregravados no dispositivo de destino serão coletados com êxito. Arquivos que foram excluídos e sobregravados estarão corrompidos ou não poderão ser recuperados.

13 Clique na seta para a direita no canto superior direito da tela.

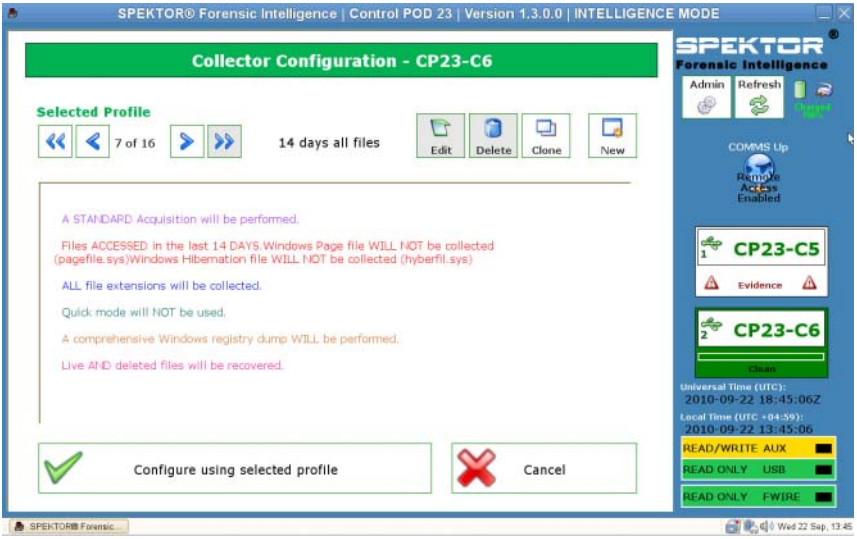
14 Na tela **Profile Name**, insira um nome para o novo perfil e, em seguida, toque ou clique em **Save Profile**.

Figura 2-16. Etapa 7 da Configuração de perfil: Nome do perfil



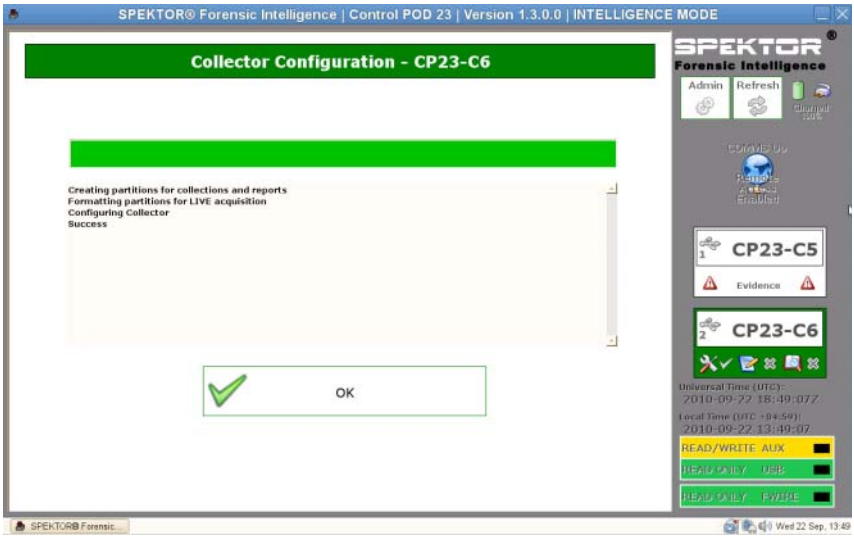
15 Clique na seta para a direita no canto superior direito da tela. Seu novo perfil será exibido na tela **Selected Profile**. A tela **Collector Configuration** exibirá o título do perfil (neste caso, **14 days all files**) e relacionará os detalhes do perfil na parte principal da janela.

Figura 2-17. Perfil selecionado após a criação do perfil



16 Toque ou clique em **Configure using selected profile** para iniciar a configuração do Coletor.

Figura 2-18. Perfil selecionado após a criação do perfil



17 Toque ou clique em **OK** para iniciar a configuração do Coletor. Esse processo levará apenas um ou dois minutos.

Quando a configuração do Coletor for concluída, o Coletor estará pronto para ser implantado em um computador ou dispositivo de armazenamento de destino. Consulte "Implantar ferramentas de Triagem" na página 33.

18 Clique na seta para a direita no canto superior direito da tela.

Implantar ferramentas de Triagem

NOTA: para obter informações sobre as diferenças entre aquisição ao vivo e padrão, consulte "Aquisição padrão x Aquisição ao vivo" na página 20.

NOTA: ainda que seja possível usar um Coletor para vários casos, as melhores práticas recomendam veementemente que cada Coletor contenha somente os dados pertinentes a um único caso, embora os dados de vários dispositivos de armazenamento desse único caso possam ser armazenados no Coletor.

Implantar um Coletor para aquisição padrão em um computador de destino

ADVERTÊNCIA: é preciso alterar a ordem de inicialização do sistema no BIOS do sistema do computador de destino antes de tentar uma aquisição padrão. Se o computador de destino estiver definido para inicialização a partir do disco rígido em vez da unidade ótica com o disco de inicialização do SPEKTOR inserido, o conteúdo da unidade do computador de destino será alterado. Assegure-se de saber como acessar o BIOS do sistema do computador de destino antes de ligar o computador de destino.

ADVERTÊNCIA: antes de ligar o computador de destino, assegure-se de ter inserido o disco de inicialização do SPEKTOR na unidade ótica na qual o computador de destino está definido para ser inicializado. Inicializar o computador de destino sem o disco de inicialização no lugar resultará na alteração do conteúdo da unidade do computador de destino.

NOTA: você precisa ter um disco de inicialização do SPEKTOR para fazer uma implementação de aquisição padrão em um computador de destino. Consulte "Gravar um CD de inicialização para procedimentos de Aquisição padrão" na página 21 para obter mais informações sobre como criar um disco de inicialização.

1. No laptop reforçado da Dell, toque ou clique em **Deploy Collector**.
2. Selecione **Target Computer**.
3. Clique em **OK** e, em seguida, desconecte o Coletor do laptop reforçado da Dell.
4. Conecte o Coletor em uma porta USB disponível no computador de destino.

NOTA: a Dell recomenda usar sempre a unidade ótica interna do computador de destino com o disco de inicialização. Se isso não for possível, use uma unidade ótica externa com um conector USB.

5. Coloque o disco de inicialização do SPEKTOR na unidade ótica.
6. Acesse o programa de BIOS do sistema do computador de destino e altere a ordem de inicialização, de modo que o computador de destino seja inicializado a partir da unidade ótica.

   O disco de inicialização do SPEKTOR será carregado e a interface da unidade de inicialização será exibida.
7. Insira as informações solicitadas na tela, pressionando <Enter> ou as teclas de setas para mover-se entre os campos e, em seguida, mova-se para o campo **COLLECT** e pressione <Enter> para iniciar a coleta de dados.

AVISO: não remova o disco de inicialização do SPEKTOR da unidade ótica até que o computador de destino tenha sido completamente desligado.

8 Quando o processo de coleta for concluído, pressione <Enter> para desligar o computador de destino.

9 Remova o disco de inicialização do SPEKTOR da unidade ótica, desconecte o Coletor da porta USB do computador de destino e conecte-o em uma porta USB disponível no laptop reforçado da Dell.

Implantar um Coletor para aquisição padrão em um dispositivo de armazenamento de destino

1 Conecte o dispositivo de armazenamento de destino na porta USB somente leitura ou na porta firewire do laptop reforçado da Dell.

2 Toque ou clique em **Deploy Collector**.

3 Toque ou clique em **Target Storage Device**, insira as informações necessárias e, em seguida, toque ou clique em **Collect from Device**.

4 Quando a coleta for concluída, desconecte o dispositivo de armazenamento de destino da porta USB e toque ou clique em **OK**.

Implantar um Coletor para aquisição ao vivo

NOTA: assegure-se de fazer anotações precisas e detalhadas durante este procedimento como parte das melhores práticas de cadeia de custódia.

NOTA: você não precisa do disco de inicialização do SPEKTOR para fazer uma implantação da aquisição ao vivo.

1 Clique em **Deploy Collector→ Target Computer**.

2 No dispositivo de destino, navegue até **My Computer** (Meu computador) (ou **Computer** em computadores com o Windows Vista ou o Windows 7).

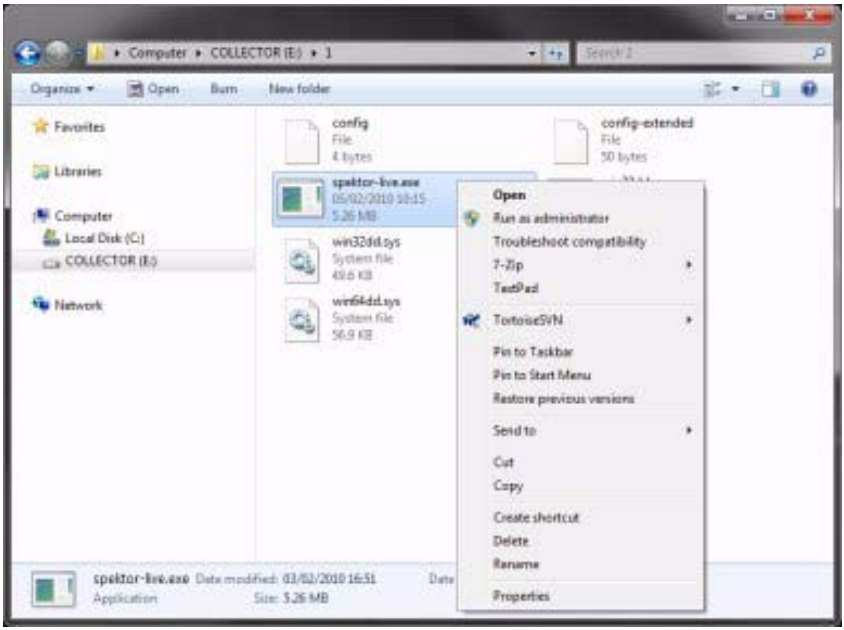
3 Clique duas vezes no ícone **Collector** que for exibido para exibir o conteúdo do Coletor.

Figura 2-19. Ícone do Coletor

4 Clique na pasta cujo nome tenha o número mais alto. Somente uma pasta será exibida se esta for sua primeira implantação desde a limpeza do Coletor.

5 Clique com o botão direito do mouse em **spektor-live.exe** e, em seguida, selecione **Run as administrator** na caixa suspensa. Se uma mensagem for exibida solicitando permissão para que o aplicativo seja executado como administrador, clique em **Continue** (Continuar).

Figura 2-20. Executar como administrador



6 Insira as informações solicitadas na tela **SPEKTOR Live Collection** e, em seguida, clique em **Run**.

7 Quando solicitado, clique em **Close**.

8 Desconecte o Coletor do dispositivo de destino e guarde-o com segurança para posterior ingestão no data center.

Como examinar arquivos coletados após a Triagem

1 No **Collector Menu**, clique em **Reporting**. Esta opção indexa os dados coletados e cria um conjunto de relatórios automaticamente.

2 Na tela **Collector Collections**, selecione um **Main Report** e clique em **Generate Selected Reports**.

Figura 2-21. Gerar relatórios

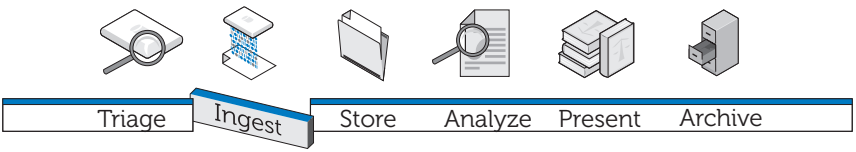
3 Clique em **OK** quanto o processo de geração de relatórios for concluído para retornar ao menu **Reporting**.

NOTA: consulte o *Manual do usuário do* SPEKTOR para obter mais informações sobre a criação e a exportação de relatórios usando critérios específicos. Consulte "Documentação e recursos relacionados" na página 16.

4 Clique em **View Collection Report** para examinar seus relatórios e, em seguida, clique em uma das cinco categorias de relatórios, **Images**, **Documents**, **Multimedia**, **Other** ou **System** para exibir relatórios específicos.

3

Ingestão



O estágio de Ingestão da solução Dell Digital Forensics consiste na criação de uma imagem do dispositivo de armazenamento de destino (caso isso ainda não tenha sido feito durante o estágio de Triagem) e, em seguida, na transferência da imagem para um local centralizado onde possa ser acessada para análise. Para mover os aplicativos forenses para o data center e ainda preservar a experiência padrão do usuário, a Dell, em parceria com a Citrix, criou vários pacotes de software distintos para os principais aplicativos forenses a fim de movê-los fluidamente para o data center, criando uma experiência mais disponível, rápida e capaz para o usuário.

Como parte da solução Digital Forensics, a Dell certificou os seguintes aplicativos forenses:

- SPEKTOR
- EnCase 6
- FTK 1.8
- FTK 3 versão independente
- FTK 3 Lab

Qualquer um desses aplicativos forenses pode ser usado em qualquer combinação para proporcionar acesso simultâneo a partir de um único dispositivo de usuário.

EnCase 6 habilitado para data center

No exemplo de solução a seguir, o aplicativo EnCase 6 é hospedado em um ou mais dispositivos de servidor Dell no data center, proporcionando sessões multiusuário do EnCase 6.

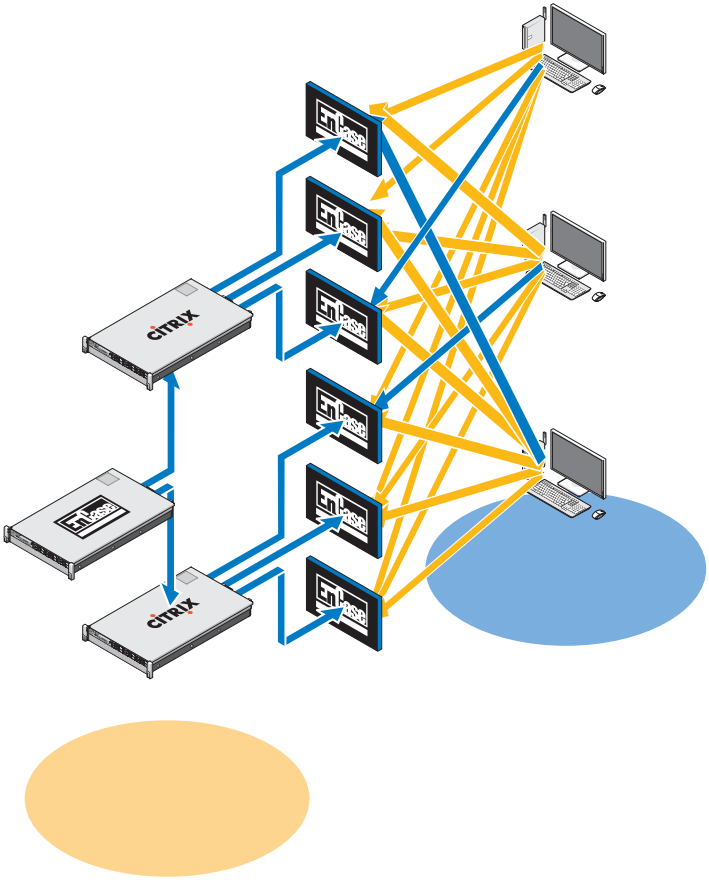
Solução com um único servidor

Na solução com um único servidor EnCase 6, vários clientes podem se conectar a um servidor. Todos os clientes são direcionados a esse servidor e não podem se conectar a nenhum outro servidor EnCase 6. No caso de falha de um servidor, todas as conexões de clientes serão perdidas.

Solução multisservidor (alta disponibilidade)

Na solução multisservidor, um usuário se conectará ao aplicativo EnCase 6 na farm do Citrix e será direcionado fluidamente para o servidor EnCase 6 que estiver trabalhando com a carga mais leve no momento. Caso o usuário esteja executando várias instanciações do software EnCase 6, cada instanciação pode ser criada por um servidor diferente. A experiência do usuário seria preservada, pois este ficaria totalmente alheio à maneira como várias instâncias são criadas, e todas as sessões pareceriam estar em execução no mesmo servidor e com a mesma aparência.

Figura 3-1. Esquema de cliente/servidor EnCase 6 habilitado para data center



No caso de falha de um servidor, o usuário precisaria clicar novamente no ícone do aplicativo EnCase na área de trabalho, e o sistema redirecionaria a conexão do usuário para o próximo servidor disponível que esteja hospedando o EnCase 6. Cada servidor EnCase pode oferecer suporte a *x* sessões de usuário, onde *x* = *(número de núcleos x 2)*. Cada sessão de usuário requer 3 GB de RAM de servidor.

FTK 1.8 habilitado para data center

Na solução FTK 1.8 habilitada para data center, o aplicativo FTK 1.8 é hospedado em um ou mais dispositivos de servidor da Dell no data center, proporcionando sessões multiusuário do FTK 1.8 (uma única sessão de usuário por servidor).

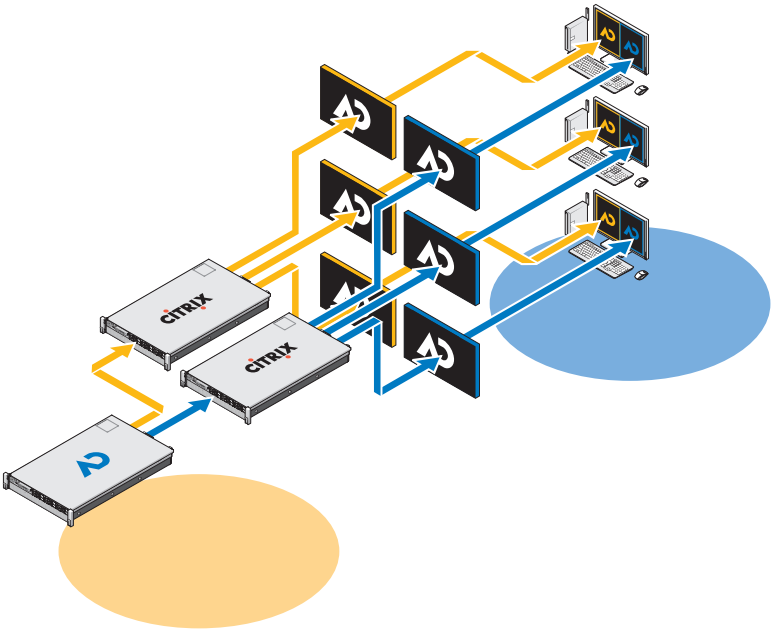
Sessão única do FTK 1.8 por desktop

Na solução do FTK 1.8 com um único servidor, vários clientes podem se conectar a um único servidor. Todos os clientes são direcionados a esse servidor e não podem se conectar a nenhum outro servidor FTK 1.8. No caso de falha de um servidor, todas as conexões de clientes serão perdidas. O usuário pode executar somente uma sessão do FTK 1.8 em cada conta de usuário do Windows.

Várias sessões do FTK 1.8 por desktop

Na solução multisservidor FTK 1.8, um usuário se conectará aos servidores FTK 1.8 usando vários ícones da área de trabalho FTK Server1, FTK Server2, etc. Cada link está associado a um servidor específico. Para fins de ilustração, a Figura 3-2 mostra a borda da sessão do servidor FTK 1.8 em execução com código de cores para o servidor que executa a sessão do FTK 1.8 (servidor1 = azul, servidor2 = vermelho). Não é possível executar duas sessões do aplicativo FTK 1.8 no mesmo servidor usando a mesma conta de usuário. A experiência do usuário do aplicativo FTK 1.8 baseado em servidor é a mesma em todos os clientes.

Figura 3-2. Esquema com vários clientes e servidores FTK 1.8



No caso de falha de um servidor, o usuário perderia o acesso à sessão de servidor correspondente do FTK 1.8. Nesse caso, o usuário precisaria continuar funcionando usando os outros servidores FTK. Todas as informações de casos e evidências ficam disponíveis em todas as sessões de servidor do FTK 1.8 por meio do NAS/SAN compartilhado (supondo-se que o usuário tenha privilégios de acesso ao NAS).

Cada servidor FTK 1.8 pode oferecer suporte a *x* sessões de usuário, onde *x* = *(número de núcleos x 2)*. Cada sessão de usuário requer 3 GB de RAM de servidor e 1000 E/S por segundo de desempenho de disco do data center.

FTK 3 habilitado para data center

Na solução FTK 3 habilitada para data center, o aplicativo é hospedado em um ou mais dispositivos de servidor da Dell no data center, proporcionando uma única sessão do aplicativo FTK 3 por servidor.

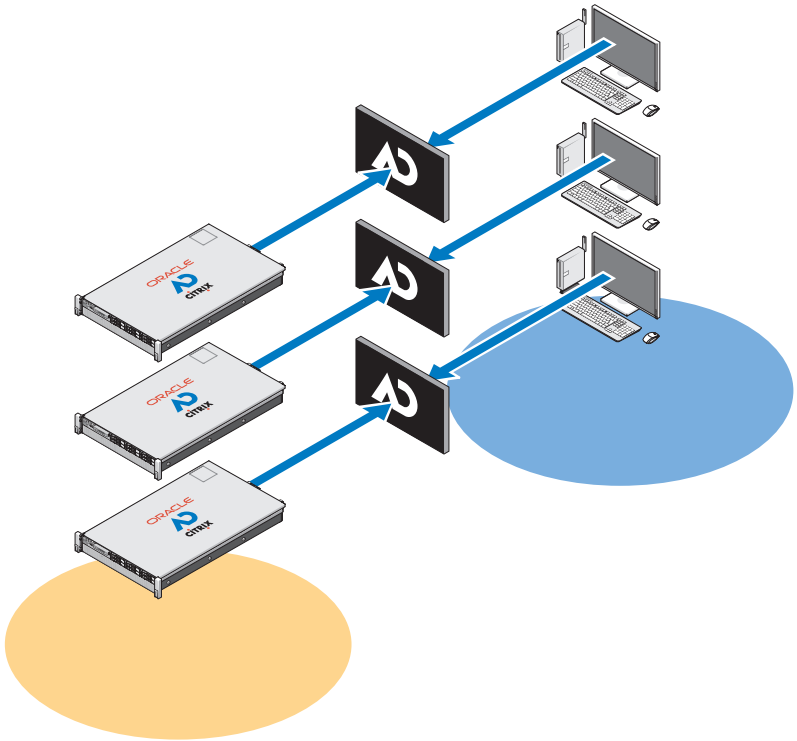
Solução de um único servidor FTK 3

Na solução de um único servidor FTK 3, um único cliente FTK 3 pode se conectar a um único servidor. O cliente é direcionado a esse servidor e não pode se conectar a nenhum outro servidor FTK 3. No caso de falha de um servidor, a conexão do cliente será perdida. O servidor FTK 3 também estará executando o banco de dados Oracle incorporado ao FTK local, porque esta versão do banco de dados não oferece suporte à colaboração entre outros bancos de dados Oracle do FTK ou outros usuários do FTK.

Solução multisservidor (sem alta disponibilidade)

Na solução multisservidor, cada cliente se conectará ao seu próprio servidor FTK 3, não podendo se conectar a nenhum outro servidor FTK 3. Quando um servidor tem uma sessão do FTK 3 em execução, não fica mais disponível para aceitar nenhuma nova sessão de cliente do FTK 3: a configuração do software na estrutura forense da Dell faz com que seja impossível para um servidor executar mais de uma sessão do aplicativo FTK 3 simultaneamente. Ao permitir que apenas uma sessão seja executada por servidor, o aplicativo FTK 3 com vários threads pode devotar todos os recursos de servidor disponíveis ao processamento de um caso, o que aumenta o desempenho.

Figura 3-3. Esquema de cliente e servidor FTK 3 habilitado para data center



Usando o FTK Standard Edition, cada servidor precisa executar uma versão local do banco de dados Oracle incorporado ao FTK (uma versão do banco de dados Oracle por usuário simultâneo). Essa versão do aplicativo FTK e do banco de dados Oracle não oferece suporte à colaboração entre outros usuários do FTK nem outros bancos de dados Oracle do FTK.

Cada banco de dados Oracle tem um agente de backup Oracle no servidor, e o backup do banco de dados é feito como parte do regime normal de backup (consulte "Arquivamento" na página 87 para obter mais informações).

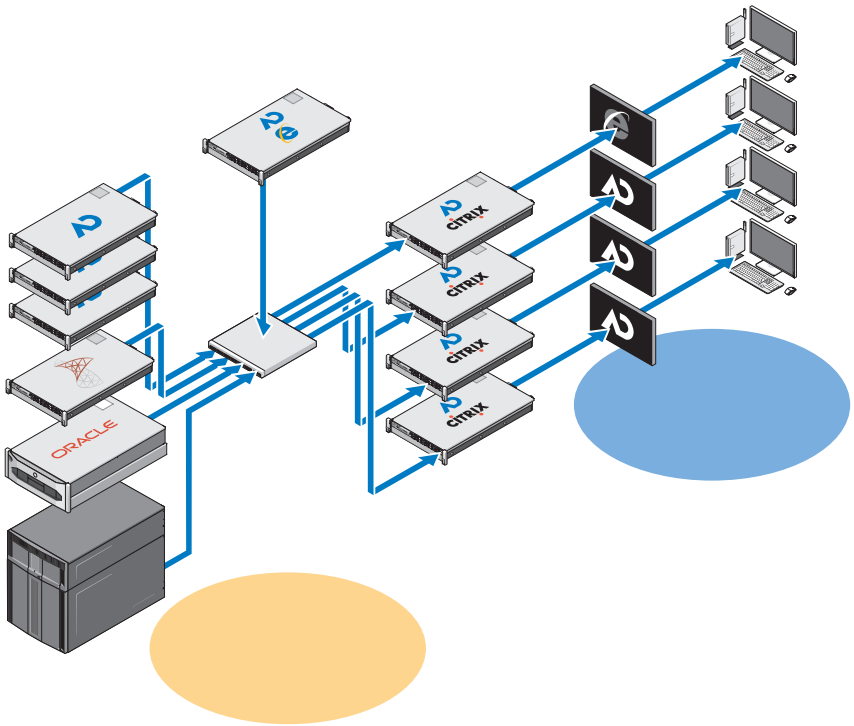
No caso de uma falha do servidor, o usuário precisará se conectar manualmente a outro servidor FTK 3 disponível (se houver n+1 servidores FTK 3 disponíveis). No entanto, caso o banco de dados Oracle também tenha falhado, não haverá acesso disponível a casos pré-existentes já processados, visto que estes estarão vinculados especificamente ao banco de dados Oracle do FTK 3 local original desse usuário.

Cada servidor FTK 3 pode oferecer suporte a uma sessão de usuário de cada vez. Cada sessão de usuário requer 64 GB de RAM de servidor (48 GB para o Oracle e 16 GB para o FTK), e 1000+ E/S por segundo para o armazenamento de arquivos, além de 600+ E/S por segundo para o banco de dados (configuração mínima).

FTK 3 Lab Edition

Na configuração do FTK 3 Lab Edition, o usuário se conectará a um servidor que hospeda o AccessData Lab e o banco de dados de caso centralizado. Vários usuários podem acessar o mesmo caso e executar diferentes análises ao mesmo tempo. O processamento é manipulado por meio de um modelo de processamento distribuído.

Figura 3-4. Esquema de cliente e servidor do FTK 3 Lab Edition



O armazenamento de casos é otimizado com um mix de hardware SAS e SATA, e todo o data center forense pode ser gerenciado centralmente por um gerente administrativo.

Vários aplicativos forenses fornecidos a uma área de trabalho

Na solução com vários fornecedores e aplicativos, todas as soluções de aplicativos individuais descritas anteriormente são combinadas para fornecer ao analista forense acesso a todos os aplicativos forenses (EnCase 6, FTK 1.8 e FTK 3, ou FTK 3 Lab Edition) a partir de uma única área de trabalho, em um único painel. Todos os aplicativos podem ser entregues em um modo de alta disponibilidade para que, no caso de uma falha, o usuário ainda tenha acesso ao aplicativo específico. E no caso do FTK 1.8, o usuário tem acesso usando um dos outros ícones do FTK 1.8 na área de trabalho.

Recomendações sobre a configuração da rede

Tabela 3-1. Estrutura de endereços IP recomendada

Endereço IP	Função do servidor	Nome do servidor
192.168.1.1	Controlador de domínio 1	DF-DC1
192.168.1.2	Controlador de domínio 2	DF-DC2
192.168.1.3	Servidor de evidência	DF-Evidência
192.168.1.4	Servidor de espaço de trabalho	DF-Espaço de trabalho
192.168.1.5	Servidor Oracle FTK	DF-FTK
10.1.0.0/24	Intervalo de endereços IP estáticos de 1 GB	
10.1.1.0/24	Intervalo de endereços IP estáticos de 10 GB	
10.1.2.0/24	Intervalo de DHCP de 1 GB, clientes	
10.1.0.250-254	Switch(es) de 1 GB	
10.1.1.250-254	Switch(es) de 10 GB	
10.1.0.200	servidor DNS	

Tabela 3-2. Convenções de nomenclatura recomendadas para servidores da solução

Nome	Abreviação
Nome de domínio	DF (Digital Forensics)
Controlador de domínio 1	DF-DC1
Controlador de domínio 2	DF-DC2
Armazenamento de evidência	DF-Evidência
Espaço de trabalho	DF-Espaço de trabalho
Oracle	DF-Oracle
SQL	DF-SQL
FTK-Lab	FTK-Lab
FTK-Independente	FTK
Gerenciador(es) de processamento distribuído	DF-DPM, DF-DPM1, DF-DPM2
Mecanismo(s) de processamento distribuído	DF-DPE, DF-DPE1, DF-DPE2

Tabela 3-3. Convenções de nomenclatura recomendadas para equipe de NIC

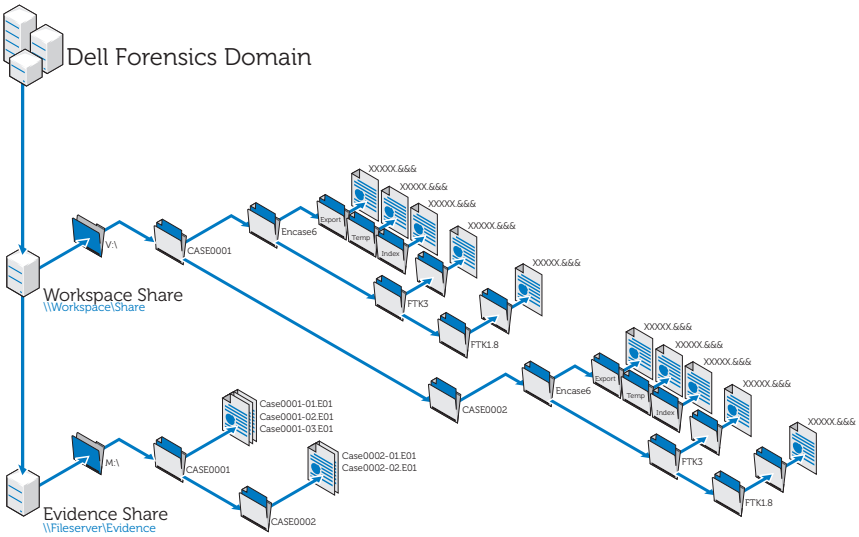
Equipe de NIC 1	Rede pública	Para servidores conectados uns aos outros
Equipe de NIC 2	iSCSI	Para servidores conectados a dispositivos de armazenamento EqualLogic

Tabela 3-4. Estrutura de mapeamento de letras de unidades recomendada

Nome de chamada	Unidade	Local ou SAN	RAID	Notas
Unidade local	C:	Local	RAID1 (2 discos SAS de 15.000 rpm)	
	D:	Local		
CD-ROM	E:			
	F:			
	G:			
SQL	H:	SAN	RAID0+1	Não pode ser em discos SATA
Oracle	I:	SAN	RAID0+1	Não pode ser em discos SATA
Unidade de cofre EV	J:	SAN	RAID50	
Backup em disco	K:	SAN	RAID50	
Sobressalente	L:	SAN	RAID50	
Evidência 1	M:	SAN	RAID50	
Evidência 2	N:	SAN	RAID50	
Evidência 3	O:	SAN	RAID50	
Evidência 4	P:	SAN	RAID50	
Evidência 5	Q:	SAN	RAID50	
Evidência 6	R:	SAN	RAID50	
Evidência 7	S:	SAN	RAID50	

Nome de chamada	Unidade	Local ou SAN	RAID	Notas
Evidência 8	T:	SAN	RAID50	
Evidência 9	U:	SAN	RAID50	
Espaço de trabalho 1	V:	SAN	RAID50	
Espaço de trabalho 2	W:	SAN	RAID50	
Espaço de trabalho 3	X:	SAN	RAID50	
Espaço de trabalho 4	Y:	SAN	RAID50	
Espaço de trabalho 5	Z:	SAN	RAID50	

Figura 3-5. Estrutura de arquivos recomendada



Como executar a Ingestão usando a solução Dell Digital Forensics

Ingestão usando o SPEKTOR

Registrar e limpar um dispositivo USB externo como disco de armazenamento

1. Conecte o dispositivo USB externo não registrado na porta do Coletor no laptop reforçado.
2. Clique ou toque no ícone do dispositivo quando for exibido e, em seguida, clique ou toque em **Register the Device as a Store Disk→ Yes**. Em seguida, insira as informações solicitadas.
3. No menu à direita, selecione o dispositivo registrado e, em seguida, toque ou clique em **Clean/Reformat→ Clean**.
4. Clique em **OK** quando o processo for concluído.

Implantar o disco de armazenamento

1. Conecte o disco de armazenamento no laptop reforçado e, em seguida, toque ou clique no dispositivo de disco de armazenamento para exibir o menu **Store Disk Menu**.
2. No **Store Disk Menu**, toque ou clique em **Deploy**.

   Se estiver implantando em um computador de destino:

   a. Toque ou clique em **Target Computer**.

   b. Remova o disco de armazenamento do laptop reforçado e conecte-o em uma porta USB sobressalente no computador de destino.

   c. Siga as mesmas instruções de implantação usadas para capturar uma imagem de triagem em "Implantar ferramentas de Triagem" na página 33.

   d. Quando o CD de inicialização for carregado, o **SPEKTOR Imaging Wizard** o orientará pelo restante do processo de criação de imagem. Instruções passo a passo podem ser encontradas no *Manual do usuário do SPEKTOR*. Consulte "Documentação e recursos relacionados" na página 16 para obter mais informações.

   e. Desligue o computador de destino, desconecte o disco de armazenamento e, em seguida, retorne o disco de armazenamento ao data center para armazenamento.

Se estiver implantando localmente em um dispositivo de armazenamento de destino:

a Toque ou clique em **Target armazenamento Device** (Dispositivo de armazenamento de destino).

b Conecte o dispositivo de armazenamento de destino na porta USB somente leitura ou na porta FireWire do lado direito do laptop reforçado.

c Selecione a unidade ou as partições cuja imagem deseja criar e, em seguida, clique na seta para a direita no canto superior direito da tela.

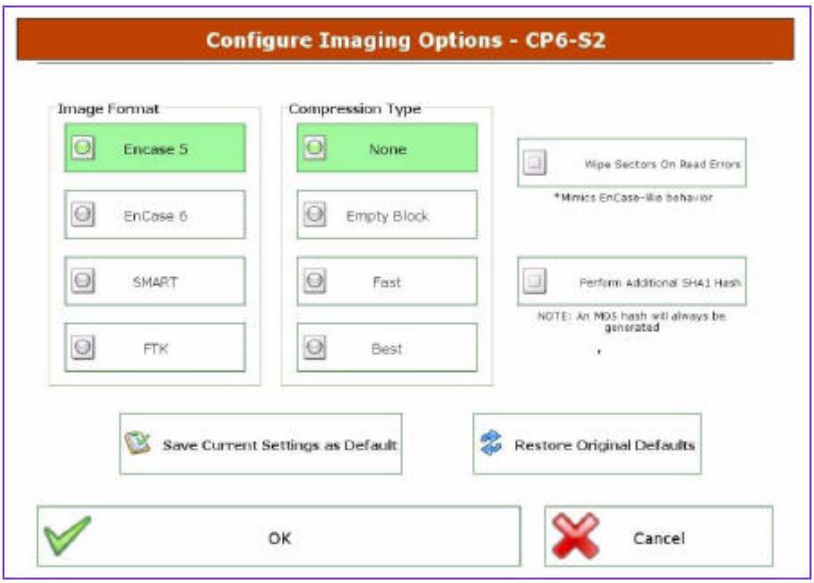
d Insira as informações do caso solicitadas e, em seguida, toque ou clique em **Image Now**.

e Se necessário, toque ou clique em **Configure Imaging Options** para alterar o **Image Format** ou o **Compression Type** ou para **Wipe Sectors on Read Errors** ou **Perform Additional SHA1 Hash**.

NOTA: um hash MDS será sempre gerado durante o processo de criação de imagem.

NOTA: consulte o *Manual de usuário do SPEKTOR* para obter mais informações sobre cada uma dessas opções da criação de imagem. Consulte "Documentação e recursos relacionados" na página 16.

Figura 3-6. Configurar opções de criação de imagem



f Toque ou clique em **Image Now→ Yes** para iniciar o processo de criação de imagem.

g Quando o processo de criação de imagem for concluído, toque ou clique em **OK**.

h Desconecte o dispositivo de armazenamento de destino e o disco de armazenamento do laptop reforçado e, em seguida, retorne o disco de armazenamento para o data center para armazenamento e análise.

NOTA: transferir uma imagem pode demorar muito tempo. Seis horas para a transferência de uma disco rígido típico de 60 GB é o comum.

Ingestão usando o EnCase

Na solução Dell Digital Forensics, o licenciamento do EnCase é feito com o uso de um sistema de licenciamento pela rede. Normalmente, uma instância do EnCase SAFE é instalada em um dos servidores de data center e um dongle que contém várias licenças de usuário é conectado a esse servidor. Os clientes do EnCase são configurados para acessar esse servidor para o licenciamento, sem a necessidade de dongles locais. Consulte o *Dell Digital Forensics Installation and Configuration Guide* (Guia de Instalação e Configuração do Dell Digital Forensics) para obter mais informações. Consulte "Documentação e recursos relacionados" na página 16. Além disso, consulte o administrador de seu sistema de rede para obter informações específicas à instalação da solução na sua entidade.

1 Acople o dispositivo de armazenamento de destino na estação de trabalho de ingestão apropriada no data center.

   a Se estiver criando a imagem de uma unidade SATA, consulte "Como conectar o Bloqueador de gravação da Tableau a um disco rígido SATA" na página 55 para obter mais informações.

   b Se estiver criando a imagem de uma unidade IDE, consulte "Como conectar o Bloqueador de gravação da Tableau a um disco rígido IDE" na página 56 para obter mais informações.

2 Crie um novo caso.

NOTA: as instruções a seguir se referem à estrutura de rede e de pastas descrita como melhor prática sugerida pela Dell para a solução Digital Forensics. Consulte Figura 3-5 para obter mais informações.

a Clique em **New** e, em seguida, insira as informações solicitadas.

b Na **unidade W:** (área de trabalho), crie pastas usando a seguinte estrutura:

- `W:\[NomedoCaso]\EnCase6\Export`
- `W:\[NomedoCaso]\EnCase6\Temp`
- `W:\[NomedoCaso]\EnCase6\Index`

c Clique em **Finish**.

d Clique em **Yes** para cada solicitação para criar a pasta.

e Na tela **EnCase Acquisition**, clique em na opção de menu **Add Device**.

f Assegure-se de que a caixa de seleção **Sessions** esteja marcada.

g No painel da direita, selecione seu caso.

h Clique em **Add Evidence Files** e navegue até o repositório E01 (de acordo com a configuração de melhor prática descrita na Figura 3-5, esse repositório deve estar armazenado na unidade **X:**).

i Clique em **Next→ Next→ Finish**. Um ícone de cronômetro é exibido na parte inferior direita da tela **Acquisition** do EnCase e o EnCase verifica o arquivo E01. Dependendo do tamanho do arquivo, a verificação pode levar algum tempo.

3 No software EnCase, adicionar o dispositivo de armazenamento de destino usando o assistente **Add Device**.

4 Adquira o conteúdo de seu dispositivo.

a No software EnCase, clique em **Cases→ Entries→ Home** e, em seguida, clique com o botão direito do mouse no dispositivo que deseja adquirir.

b Selecione **Acquire** no menu suspenso.

c Na caixa de diálogo **After Acquisition**, selecione o tipo apropriado de **New Image File**:

- **Não adicione** as opções que excluem a imagem recém-adquirida do caso aberto no momento.
- **Add to Case** adiciona a imagem recém-adquirida ao arquivo de caso associado ao dispositivo de onde a imagem foi tirada.
- **Replace a source device** adiciona a imagem recém-adquirida ao caso e remove o dispositivo visualizado em que a aquisição foi feita.

d Clique em **Finish**. Quando o processo de criação de imagem for concluído, a caixa de diálogo **Acquisition Results** será exibida.

Como trabalhar com os Bloqueadores de gravação da Tableau

AVISO: não remova um disco rígido de uma ponte forense enquanto a eletricidade estiver ligada.

AVISO: não use extensores de cabo USB com uma ponte forense.

Como conectar o Bloqueador de gravação da Tableau a um disco rígido SATA

1. Assegure-se de que a entrada **DC IN B** da ponte T35es Forensic SATA/IDE esteja na posição **B On**.
2. Conecte a fonte de alimentação TP2 ou TP3 ao lado esquerdo da ponte T35es SATA usando o conector Mini-DIN de 5 pinos.
3. Conecte o cabo de energia à fonte de alimentação TP2 e à tomada elétrica.
4. Ligue a energia para verificar se o LED de bloqueio de gravação está aceso e, em seguida, desligue a energia da ponte antes de conectar o dispositivo de armazenamento de destino.
5. Conecte o conector Molex fêmea do cabo de alimentação TC5-8 estilo SATA à posição **DC OUT** localizada do lado direito da ponte T35es SATA/IDE.
6. Conecte o conector de energia SATA do cabo de alimentação TC5-8 estilo SATA ao conector de alimentação SATA do disco rígido de destino.

AVISO: usar conexões de energia tanto Molex quanto SATA ao conectar-se a um dispositivo de armazenamento de destino sobrecarregará o dispositivo de destino.

7. Conecte o cabo de sinal TC3-8 SATA à ponte T35es SATA/IDE.
8. Conecte a outra extremidade do Cabo de sinal TC3-8 SATA ao dispositivo de armazenamento de destino.
9. Conecte uma extremidade do cabo de dados (USB 2.0, duas conexões FireWire 800 ou Orion FireWire 400 de 4 pinos) a uma das portas do lado esquerdo da ponte T35es SATA/IDE.
10. Conecte a outra extremidade do cabo de dados a uma porta no laptop reforçado da Dell ou na estação de trabalho Dell OptiPlex.
11. Acione o interruptor na parte superior da ponte T35es SATA/IDE para a posição **A ON**. Agora o laptop reforçado da Dell ou a estação de trabalho Dell OptiPlex deve registrar a presença do dispositivo de armazenamento de destino.

Como conectar o Bloqueador de gravação da Tableau a um disco rígido IDE

1. Assegure-se de que a entrada **DC IN B** da ponte T35es Forensic SATA/IDE esteja na posição **B On**.
2. Conecte a fonte de alimentação TP2 ou TP3 ao lado esquerdo da ponte T35es SATA/IDE usando o conector Mini-DIN de 5 pinos.

NOTA: o plugue DIN de 7 pinos na fonte de alimentação TP3 não funciona com as pontes da Tableau. É preciso usar o cabo com adaptador DIN de 7 pinos para DIN TCA-P7-P5 de 5 pinos para conectar a fonte de alimentação TP3 às pontes da Tableau.

3. Conecte o cabo de energia à fonte de alimentação TP2 e à tomada elétrica.
4. Ligue a energia para verificar se o LED de **bloqueio de gravação** fica **ACESO** e, em seguida, **DESLIGUE** a energia da ponte antes de conectar o disco rígido de destino.
5. Conecte um conector Molex fêmea do cabo de alimentação TC2-8 estilo Molex à posição DC OUT localizada do lado direito da ponte T35es SATA/IDE.
6. Conecte o outro conector Molex fêmea do cabo de alimentação TC2-8 estilo Molex ao conector Molex do disco rígido suspeito.
7. Conecte a extremidade azul do cabo de sinal TC6-8 IDE (alinhando o pino 1) à ponte T35es SATA/IDE.
8. Conecte a extremidade preta do Cabo de sinal TC6-8 IDE ao dispositivo de armazenamento de destino.
9. Conecte uma extremidade do cabo de dados (USB 2.0, duas conexões FireWire 800 ou Orion FireWire 400 de 4 pinos) a uma das portas do lado esquerdo da ponte T35es SATA.
10. Conecte a outra extremidade do cabo de dados a uma porta no laptop reforçado da Dell ou na estação de trabalho Dell OptiPlex.
11. Acione o interruptor na parte superior da ponte T35es SATA/IDE para a posição **A ON**. Agora o laptop reforçado da Dell ou a estação de trabalho Dell OptiPlex deve reconhecer a presença do dispositivo de armazenamento de destino.

Ingerir usando o FTK 1.8 e 3.0 habilitados para data center

Na solução Dell Digital Forensics, o licenciamento do FTK é feito com o uso de um sistema de licenciamento pela rede. Normalmente, o Servidor de licenciamento pela rede do FTK é instalado em um dos servidores do data center e um dongle do FTK que contém várias licenças de usuário é conectado nesse servidor. Os clientes do FTK são configurados para acessar esse servidor para o licenciamento, sem a necessidade de dongles locais. Consulte o *Dell Digital Forensics Installation and Configuration Guide* (Guia de Instalação e Configuração do Dell Digital Forensics) para obter mais informações. Consulte "Documentação e recursos relacionados" na página 16. Além disso, consulte o administrador de seu sistema de rede para obter informações específicas à instalação da solução na sua entidade.

Criar uma imagem do dispositivo de armazenamento de destino

1. No aplicativo AccessData FTK Imager, clique em **File→ Create Disk Image . . .** (Arquivo - Criar imagem de disco...)
2. Na janela pop-up **Select Source**, selecione o tipo de evidência cuja imagem deseja criar: Physical Drive (Unidade física), Logical Drive (Unidade lógica), Image File (Arquivo de imagem), Contents of a Folder (Conteúdo de uma pasta) ou Fernico Device (Dispositivos Fernico) e clique em **Next**.

NOTA: o exemplo a seguir usa a opção **Imaging a Physical Drive** (Criação de imagem de uma unidade física) para demonstrar o processo de criação de imagem. As outras opções de arquivo são abordadas no *Manual do usuário do FTK*. Consulte "Documentação e recursos relacionados" na página 16.

3. Usando a caixa suspensa, selecione entre as unidades a unidade física cuja imagem deseja criar e, em seguida, clique em **Finish**.
4. Na janela pop-up **Create Image**, clique em **Add . . .** (Adicionar)e selecione o tipo de imagem que deseja criar (Raw, SMART, E01 ou AFF). Em seguida, clique em **Next**.
5. Insira as informações solicitadas na janela **Evidence Item Information** (Case Number, Evidence Number, Unique Description, Examiner e Notes). Em seguida, clique em **Next**.
6. Na janela **Select Image Destination**, navegue até a área de armazenamento alocada para imagens de evidência (consulte a Figura 3-5 para informar-se sobre a nomenclatura de arquivos e servidores recomendada pela Dell), insira um nome de arquivo para a imagem e, em seguida, clique em→

7 Clique em **Start**. A janela pop-up **Creating Image . . .** (Criando imagem) é exibida com uma barra de progresso da operação.

NOTA: o processo de criação de imagem pode levar horas, dependendo do volume de dados que está sendo adicionado.

8 Se você tiver optado anteriormente por exibir um resumo dos resultados de imagem, a janela **Drive/Image Verify Results** será exibida quando o processo de criação de imagem for concluído. Examine os resultados e, em seguida, clique em **Close**.

9 Clique em **Close** novamente para fechar a janela **Creating Image . . .** (Criação de imagem).

Criar um caso

1 Clique em **File**→ **New Case**. Insira o seguinte: **Investigator Name**, **Case Number**, **Case Name**, **Case Path** e **Case Folder**.

2 Na janela **Forensic Examiner Information**, insira as seguintes informações: **Agency/Company**, **Examiner's Name**, **Address**, **Phone**, **Fax**, **E-Mail** e **Comments**. Em seguida, clique em **Next**.

3 Na janela **Case Log Options**, selecione o conjunto de opções que deseja alterar:

- Eventos de casos e evidências
- Mensagens de erro
- Marcação de eventos
- Pesquisa de eventos
- Escavação de dados/pesquisas na Internet
- Outros eventos

4 Na janela **Processes to Perform**, selecione os processos que deseja conduzir. Selecione os **Processos** nas seguintes opções:

- MD5 Hash
- SHA1 Hash
- KFF Lookup
- Entropy Test
- Full Text Index

- Store Thumbnails
- Decrypt EFS Files
- File Listing Database
- HTML File Listing
- Data Carve
- Registry Reports

5 Clique em **Next**.

6 Na janela **Refine Case**, inclua ou exclua do caso os diferentes tipos de dados. As opções pré-configuradas incluem cinco requisitos comuns:

- Include All Items
- Optimal Settings
- Email Emphasis
- Text Emphasis
- Graphics Emphasis

7 Clique em **Next.**

8 Na janela **Refine Index**, inclua ou exclua do processo de indexação os diferentes tipos de dados.

9 Clique em **Next**.

Adicionar evidência

1 Clique em **Add Evidence**. A janela pop-up **Add Evidence to Case** é exibida.

2 Selecione o tipo de evidência a ser adicionado ao caso: **Acquired Image of Drive**, **Local Drive**, **Contents of a Folder** ou **Individual File** selecionando o botão de opção. Em seguida, clique em **Continue**.

3 Navegue até a imagem, unidade, pasta ou arquivo, selecione o arquivo e clique em **Open**.

Se tiver selecionado **Acquired Image of Drive** como tipo de evidência, uma janela pop-up **Evidence Information** será exibida. Insira as informações solicitadas e clique em **OK**.

Se tiver selecionado **Local Drive** como tipo de evidência,

a A janela pop-up **Select Local Drive** será exibida. Selecione a unidade local a ser adicionada e, em seguida, selecione **Logical Analysis** ou **Physical Analysis**. Clique em **OK**.

b Na janela **Evidence Information**, insira as informações solicitadas e, em seguida, clique em **OK**.

Se tiver selecionado **Contents of a Folder or Individual File** selecione a pasta ou o arquivo que deseja adicionar ao caso e, em seguida, clique em **Open**.

4 Clique em **Next**.

5 Na janela **New Case Setup is Now Complete**, examine suas seleções. Em seguida, clique em **Finish**.

Ingerir usando o FTK 3 Lab Edition

Criar uma imagem do dispositivo de armazenamento de destino

Consulte "Criar uma imagem do dispositivo de armazenamento de destino" na página 57.

Criar um caso

1 Clique em **Case→ New**. A janela **New Case Options** é exibida.

2 Insira o nome do caso e quaisquer informações de referência ou descrição necessárias em sua entidade.

3 Navegue até seu Case Folder Directory (Diretório de pastas de casos) e selecione seu Processing Manager (Gerenciador de processamento) na caixa suspensa.

NOTA: se não souber onde seu Case Folder Directory (Diretório de pastas de casos) e Processing Manager (Gerenciador de processamento) estão, consulte o administrador do sistema.

4 Clique em **Detailed Options** para restringir os dados que você deseja incluir em seu caso. Consulte o *Manual do usuário do AccessData FTK* 3 para obter mais informações sobre como restringir os dados do caso. Consulte "Documentação e recursos relacionados" na página 16.

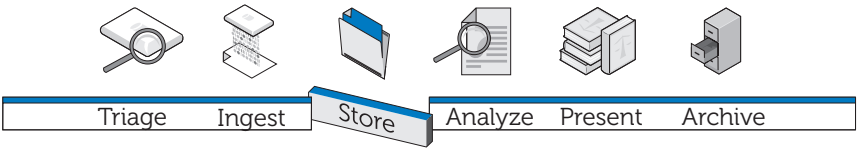
5 Clique em **OK**. A janela **Manage Evidence** é aberta.

Adicionar evidência a um caso

1. Na janela **Manage Evidence**, clique em **Add**. Em seguida, clique no botão de opção ao lado do tipo de evidência que você deseja adicionar: **Acquired Image(s)**, **All Images in Directory**, **Contents of a Directory**, **Individual File(s)**, **Physical Drive** ou **Logical Drive**. Em seguida, clique em **OK**.
2. Navegue até o diretório **Evidence** e selecione seu arquivo de evidência. Em seguida, clique em **Open**.
3. Escolha um fuso horário (obrigatório).
4. Clique em **OK**. A janela **Data Processing Status** é aberta.
5. Quando o **Process State** for alterado para **Finished**, clique em **Close**. Agora a evidência é exibida no caso, na interface do software.

4

Armazenamento



A abordagem tradicional ao armazenamento de evidências digitais começa com o trabalho independente dos investigadores em estações de trabalho individuais em uma configuração com vários silos. O arquivo de evidência é armazenado, com maior ou menor proteção, na estação de trabalho ou transferido diariamente de um servidor de armazenamento para a estação de trabalho, sobrecarregando a rede com a transferência contínua de arquivos muito grandes. A estrutura deixa de aproveitar a velocidade do processamento distribuído, as economias de escala e a economia substancial de custos que um processamento paralelo de nível empresarial e uma arquitetura de armazenamento em camadas podem oferecer. Além disso, com essa configuração, fica no mínimo difícil de compartilhar os dados ou colaborar com equipes internas e externas de modo eficiente, a fim de garantir os backups regulares dos dados de evidências, auditorar as alterações aos arquivos e, o mais importante, garantir a integridade e a segurança dos arquivos.

Eficiência

A solução Dell Digital Forensics pode se adaptar a muitas configurações diferentes de TI. Quanto mais próximo a configuração estiver de um verdadeiro design de nível empresarial – composta por estações de trabalho, servidores de processamento dedicados capazes de executar o processamento distribuído, uma infraestrutura de rede baseada na comunicação paralela em vez de serial e armazenamento – mais compensadora será em termos de energia. O tráfego da rede é menos intenso e mais rápido porque os processadores distribuídos fazem a maior parte do trabalho – a rede só transfere os resultados do trabalho em vez dos arquivos de evidências propriamente ditos.

Quando os arquivos de evidências são mantidos no servidor em vez de ficarem na estação de trabalho, a análise fica livre para usar a estação de trabalho para iniciar e monitorar *vários* trabalhos em vez de ficar restrita ao tentar processar um único trabalho. Além disso, as análises podem ser concluídas ainda mais rapidamente porque vários analistas e especialistas em consultoria, como especialistas em línguas estrangeiras, podem trabalhar no mesmo arquivo *.E01 simultaneamente usando diferentes estações de trabalho.

O trabalho pode ser triado de acordo com a dificuldade e atribuído a analistas com diferentes níveis de experiência. Um analista júnior pode assumir a tarefa mais demorada de extrair arquivos gráficos de um arquivo *.E01, enquanto o analista sênior mais experiente pode investir melhor seu tempo fazendo exames e análises mais complicadas desses arquivos gráficos.

Escalabilidade

No back-end, os componentes do data center da solução são modulares e projetados com a escalabilidade em mente. Visto que o data center lida com a carga de trabalho, as estações de trabalho não precisam ser carregadas com memória ou poder de computação. Na verdade, terminais muito leves e baratos podem ser usados para acessar os arquivos de evidências necessários e até mesmo o software analítico armazenado no data center.

Segurança

A tendência crescente à agregação de informações torna nossos sistemas de armazenamento de dados cada vez mais vulneráveis. Ao mesmo tempo, o acesso ao armazenamento de evidências deve ser a área mais rigorosamente controlada do sistema forense digital. A melhor prática sugere a implementação de uma estratégia em três camadas:

- Acesso físico rigorosamente controlado ao hardware em que seus dados de evidência residem
- Uma camada de controle administrativo que inclui o uso de políticas de grupo
- Segurança baseada em computador, como políticas de criação de senhas

Para tanto, ao lidar com a questão de projetar o volume e a estrutura adequados às suas necessidades (consulte "Ingestão" na página 39), a segurança é a principal consideração de uma entidade quando o armazenamento está envolvido.

Camada de acesso físico

Seus arquivos de servidor de evidência forense digital devem ser abrigados mais seguramente do que quaisquer outros arquivos em sua organização, o que inclui arquivos de Recursos Humanos.

Considere as seguintes sugestões:

- Coloque os servidores de exame e de armazenamento de dados dentro de um espaço laboratorial dedicado. Dessa forma, todos os servidores, data warehouses, cabeamento físico, switches e roteadores ficarão fisicamente protegidos pelas mesmas medidas de segurança que restringem o acesso ao laboratório.
- Use protocolos de controle de entrada, como impressões digitais ou verificações de retina ou acesso com cartão inteligente.
- Direcione todo o tráfego do exame pelos switches de rede dedicados e conectados fisicamente somente aos servidores de exame e às estações de trabalho.

Camada de controle administrativo e Active Directory

Sua configuração da solução será executada em um sistema operacional Windows e, portanto, o restante deste capítulo aborda o Windows e seus recursos de segurança de grupo e usuário do Active Directory. O Active Directory se baseia na segurança de grupos e em seus recursos relacionados. Um grupo é um conjunto de usuários ou computadores em um domínio. Os dois tipos básicos de grupos são *grupos de distribuição* (usados para distribuição de email) e *grupos de segurança*. Estabelecer grupos de segurança permite criar e aplicar políticas relacionadas à segurança, inclusive:

- Acesso a recursos compartilhados e o nível desse acesso
- Direitos de usuários, inclusive requisitos de senhas
- Políticas de bloqueio de contas
- Políticas de restrição de software
- Distribuição de patches de segurança para notebooks, desktops e servidores

Por exemplo, você pode criar um grupo que contém estações de trabalho administrativas e um segundo grupo que contém usuários administrativos. Em seguida, pode usar os Objetos de diretiva de grupo (GPOs) para limitar o acesso a essas estações de trabalho aos membros do grupo de usuários administrativos. (Consulte "Como aplicar políticas de segurança usando Objetos de diretiva de grupo" na página 70 para obter informações sobre como trabalhar com objetos de diretiva de grupo.)

Camada de segurança baseada em computador e Active Directory

O Active Directory também oferece o Kerberos, um protocolo de autenticação de rede que permite que nós de comunicação em redes não protegidas comprovem sua identidade uns aos outros de maneira segura. Consulte "Contas de usuário do Active Directory" na página 72 para obter informações sobre como trabalhar com contas de usuário e consulte também "Suporte do Active Directory a políticas de senhas seguras" na página 70 para obter informações sobre a criação de senhas.

Informações adicionais sobre segurança e laboratório criminal digital

SP 800-41 Rev. 1º de set. de 2009 Guidelines on Firewalls and Firewall Policy (Orientações sobre firewalls e política de firewall)

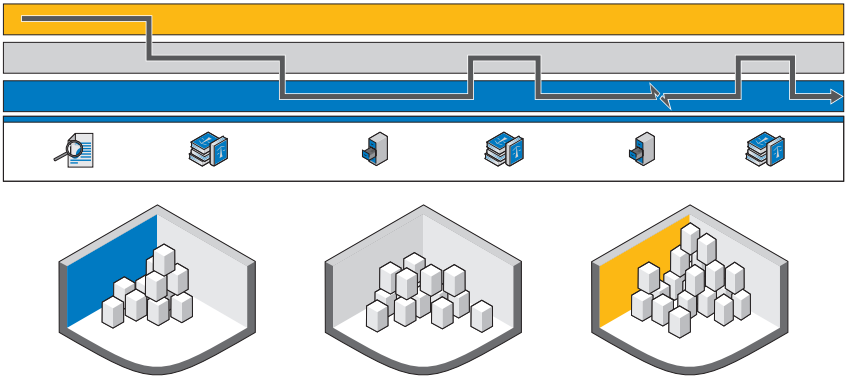
SP 800-46 Rev. 1º de jun. de 2009 Guide to Enterprise Telework and Remote Access Security (Guia de segurança de trabalho à distância e acesso remoto)

SP 800-55 Rev. 1º de jul. de 2008 Performance Measurement Guide for Information Security (Guia de medição de desempenho para segurança da Informação)

Armazenamento em camadas

A solução Dell Digital Forensics usa estratégias de armazenamento em camadas para acomodar o rápido crescimento dos dados, ao mesmo tempo em que controla os custos. Um mix de unidades SATA e SAS de várias capacidades e níveis de desempenho pode ser ajustado de modo a corresponder aos perfis de dados, e esse mix pode ser reavaliado periodicamente para que se mantenha o nível de otimização com o passar do tempo. Normalmente, dados críticos à missão, como dados de casos atualmente no estágio de análise, são armazenados em unidades de alto desempenho e alto custo, enquanto dados menos urgentes, como arquivos de casos arquivados ou cujos processos de apelação têm início, são movidos para unidades de menor custo e alta capacidade.

Figura 4-1. Uso do armazenamento em camadas para arquivamento e recuperação



A Figura 4-1 mostra o caminho sugerido para armazenamento de evidências digitais desde o momento em que a evidência é coletada até seu armazenamento em fita por períodos prolongados ou sua exclusão final.

Como fazer a correspondência do arquivamento e recuperação das evidências com o ciclo de vida do caso

Confisco da evidência (Análise) – Quando o dispositivo digital é confiscado, um laboratório criminal de alta tecnologia provavelmente desejará extrair a evidência potencial do dispositivo tão rapidamente quanto possível e dar início ao processo de análise. Quanto mais rápido um analista puder pesquisar e indexar um arquivo de evidência, mais rapidamente uma decisão poderá ser tomada quanto a levar ou não o caso adiante.

Identificação da evidência (Apresentação) – Quando a evidência foi potencialmente encontrada durante o estágio de análise, diferentes conjuntos de habilidades podem ser necessários (idiomas, desenhos técnicos, contabilidade, etc.). Agora a evidência precisa ser categorizada pelas equipes que a examinam. O processamento intenso já terminou e a evidência pode residir em um armazenamento mais econômico, de longo prazo.

Espera do julgamento (Arquivamento) – Depois que todas as evidências potenciais tiverem sido reunidas e o aso estiver em andamento, normalmente não existe necessidade de manter os dados do caso e as imagens da evidência no armazenamento online, onde possa ser acessado instantaneamente. Em casos normais, o laboratório conseguirá estar atento à necessidade de *recuperação do caso*, o que pode ser feito proativamente se um evento de encaminhamento conhecido criar a necessidade dos dados do caso. Essa abordagem reduz o custo de armazenamento no laboratório forense, porque nem todos os dados precisam ser mantidos no laboratório independentemente de sua relevância no momento, podendo ser movidos fluidamente para um armazenamento mais lento.

Julgamento (Apresentação) – Se o caso chegar a julgamento, o laboratório forense pode desejar contar com rápido acesso à evidência e aos dados do caso para responder a quaisquer questões no tribunal.

Sentença de custódia (Arquivamento) – No caso de uma sentença de custódia, a maioria dos países exige que a Polícia ou o ministério da justiça mantenha as evidências e os arquivos do caso por um período mínimo ou durante a vigência da sentença de custódia mais um período razoável para apelação ou por 99 anos. A meta é colocar os dados em uma mídia de armazenamento de baixo custo e de longo prazo que proteja a integridade e a confiabilidade dos dados.

Apelação (Apresentação) – Se houver apelação, talvez seja preciso que os dados do caso e as evidências sejam recuperados para análise ou escrutínio adicionais. Essa recuperação precisa acontecer em tempo hábil, mas os dados muito raramente são solicitados instantaneamente.

Exclusão – Na maioria dos países ao redor do globo, os órgãos do setor público não estão autorizados a manter os dados indefinidamente depois de atingido o limite legal de retenção. Um processo simples precisa estar disponível para exclusão desses dados. Esse processo também pode ser necessário caso o veredito de inocente seja retornado e os dados também precisem ser excluídos.

Como configurar a segurança do armazenamento usando a solução Dell Digital Forensics e o Active Directory

Como criar e preencher grupos no Active Directory

Grupos são estabelecidos pelos Serviços de domínio Active Directory (Windows Server 2008).

Como criar um novo grupo (Windows Server 2008)

1. Clique em **Start**→ **Administrative Tools**→ **Active Directory Administrative Center** (Iniciar - Ferramentas administrativas - Centro administrativo do Active Directory).
2. No painel de navegação, clique com o botão direito do mouse no nó ao qual deseja adicionar um novo grupo e clique em **New** (Novo). Em seguida, clique em **Group** (Grupo).
3. Insira o nome do novo grupo.
4. Selecione a opção apropriada em **Group Scope** (Escopo do grupo).
5. Selecione o **Group Type** (Tipo de grupo).
6. Selecione **Protect from accidental deletion** (Proteger contra exclusão acidental).
7. Modifique as seções **Managed By** (Gerenciado por), **Member Of** (Membro de) e **Members** (Membros) e, em seguida, clique em **OK**.

Como adicionar membros a um grupo (Windows Server 2008)

1. Clique em **Start**→ **Administrative Tools**→ **Active Directory Administrative Center** (Iniciar - Ferramentas administrativas - Centro administrativo do Active Directory).
2. No painel de navegação, clique na pasta em que o grupo reside.
3. Clique no grupo com o botão direito do mouse e, em seguida, clique em **Properties** (Propriedades).
4. Selecione **Add** (Adicionar) na guia **Members** (Membros).
5. Insira o nome do usuário, computador ou grupo que você deseja adicionar e clique em **OK**.

Como aplicar políticas de segurança usando Objetos de diretiva de grupo

Depois de criar um grupo, você pode aplicar coletivamente configurações de segurança e outros atributos aos membros de um grupo criando e configurando um Objeto de diretiva de grupo (GPO). Fazer isso facilita a manutenção dos usuários e recursos à medida que a organização forense digital evolui.

Como criar e editar GPOs

Como criar um novo GPO (Windows Server 2008)

No Windows Server 2008, os GPOs são gerenciados pelo uso do Console de gerenciamento de diretiva de grupo (GPMC).

1. Para abrir o GPMC, clique em **Start→ Administrative Tools→ Group Policy Management** (Iniciar - Ferramentas administrativas - Gerenciamento de diretiva de grupo).
2. Navegue até a floresta e o domínio em que deseja criar um novo objeto e, em seguida, clique em **Group Policy Objects** (Objetos de diretiva de grupo).
3. Clique em **New**.
4. Insira o nome do novo GPO e clique em **OK**.

Como editar um novo GPO (Windows Server 2008)

No Windows Server 2008, os GPOs são gerenciados por meio do uso do GPMC.

1. Para abrir o GPMC, clique em **Start→ Administrative Tools→ Group Policy Management** (Iniciar - Ferramentas administrativas - Gerenciamento de diretiva de grupo).
2. Navegue até a floresta e o domínio em que o GPO reside e, em seguida, clique em **Group Policy Objects** (Objetos de diretiva de grupo).
3. Clique com o botão direito do mouse no GPO.
4. Faça as alterações necessárias às configurações e salve-as.

Suporte do Active Directory a políticas de senhas seguras

O Active Directory oferece suporte a uma variedade de políticas de autenticação, inclusive cartões inteligentes, senhas de alta segurança e configurações de bloqueio de conta.

As senhas e as outras políticas de autenticação são criadas usando-se GPOs. Consulte "Como aplicar políticas de segurança usando Objetos de diretiva de grupo" na página 70 para obter informações sobre como criar e editar um GPO.

Configurações sugeridas de senhas de alta segurança

Os valores a seguir são sugeridos para a definição de configurações de senha:

- Enforce password history (Impor histórico de senhas) - O número de senhas diferentes que precisa ser usado antes que uma senha possa ser reutilizada. Definido como 24.
- Maximum password age (Idade máxima da senha) - As senhas precisam ser alteradas a cada *x* dias. Definido como 90.
- Minimum password age (Idade mínima da senha) - O número de dias que uma senha precisa ficar em vigor antes de poder ser alterada. Definido como 1 ou 2.
- Minimum password length (Comprimento mínimo da senha) - Definido como 8 ou 12 caracteres.
- Password must meet complexity requirements (Senha precisa atender aos requisitos de complexidade) - Definido como **Enabled** (Ativado). As seguintes políticas são aplicadas:
  - As senhas precisam ter pelo menos 6 caracteres
  - As senhas precisam incluir caracteres de pelo menos três destas quatro categorias:
    - Caracteres maiúsculos
    - Caracteres minúsculos
    - Numerais (0 a 9)
    - Símbolos
  - As senhas não podem conter três ou mais caracteres consecutivos do nome da conta ou do nome do usuário

Políticas detalhadas de senhas

No Windows Server 2008, os Serviços de domínio Active Directory oferecem suporte a Objetos de definição de senha (PSOs) que se aplicam a grupos ou usuários de segurança global específicos em um domínio. Um PSO pode especificar o comprimento da senha em caracteres, a complexidade da senha, a idade mínima e máxima da senha, entre outros atributos.

Consequentemente, você pode criar vários PSOs que correspondam à estrutura organizacional de suas instalações forenses digitais. Por exemplo, você pode usar PSOs para implementar senhas mais longas que expiram mensalmente para usuários administrativos e senhas mais curtas que expiram a cada três meses para analistas.

Contas de usuário do Active Directory

Como estabelecer contas de usuário para análise forense

1. Abra **Active Directory Users and Computers** (Usuários e computadores do Active Directory):
   a. Clique em **Start→ Control Panel** (Iniciar - Painel de controle)
   b. Clique duas vezes em **Administrative Tools** (Ferramentas administrativas) e, em seguida, clique duas vezes em **Active Directory Users and Computers** (Usuários e computadores do Active Directory).
2. Na árvore do console, clique com o botão direito do mouse na pasta em que deseja adicionar uma conta de usuário.

   Onde?

   Active Directory Users and Computers (Usuários e computadores do Active Directory)/*nó de domínio*/*pasta*
3. Aponte para **New** (Novo) e clique em **User** (Usuário).
4. Em **First name** (Prenome), digite o prenome do usuário.
5. Em **Initials** (Iniciais), digite as iniciais do usuário.
6. Em **Last name** (Sobrenome), digite o sobrenome do usuário.
7. Modifique **Full name** (Nome completo) para adicionar as iniciais ou inverter a ordem do prenome e do sobrenome.
8. Em **User logon name** (Nome de logon do usuário), digite o nome de logon do usuário, clique no sufixo UPN na lista suspensa e, em seguida, clique em **Next** (Avançar).

   Se o usuário pretender usar um nome diferente para fazer logon em computadores que executam o Windows 95, Windows 98 ou Windows NT, você poderá alterar o nome de logon do usuário exibido em **User logon name (pre-Windows 2000)** (Nome de logon do usuário [pré-Windows 2000]) para o nome diferente.
9. Em **Password** (Senha) e **Confirm password** (Confirmar senha), digite a senha do usuário e selecione as opções apropriadas para a senha.

NOTA: para executar este procedimento, você precisa ser membro do grupo Account Operators (Operadores de contas), Domain Admins (Admins do domínio) ou Enterprise Admins (Administradores de empresa) no Active Directory; ou a devida autoridade precisa lhe ter sido delegada. Como melhor prática de segurança, considere usar *Run as* (Executar como) para executar este procedimento. Para obter mais informações, consulte *Default local groups* (Grupos locais padrão), *Default groups* (Grupos padrão) e *Using Run as* (Como usar Executar como).

Estabelecer uma conta de gerenciador de serviço do FTK

NOTA: durante o curso da instalação do FTK, você será indagado sobre o nome da conta de usuário que planeja usar para gerenciar o recurso Distributed Processing (Processamento distribuído). Não o use.

Se você estiver usando o recurso de processamento distribuído do FTK como uma de suas ferramentas forenses, deverá criar uma conta de Gerenciador de serviço do FTK no Active Directory para lidar com a atualização automática das senhas. durante o processo de instalação do FTK, você será solicitado a fornecer o nome do usuário que será usado para monitorar e gerenciar a função de processamento distribuído. Essa conta precisa ser criada como um serviço no Active Directory, e precisa ter privilégios de administrador (mas não deve ser a conta Administrador) para fornecer o handshake contínuo entre o FTK e o servidor de evidências exigido pelo recurso de processamento distribuído.

1. No Active Directory, abra **Administrative Tools** (Ferramentas administrativas) e clique em **Active Directory Users and Computers** (Usuários e computadores do Active Directory).
2. Na árvore do console, clique duas vezes em no nó Domain (Domínio).
3. No painel **Details** (Detalhes), clique com o botão direito do mouse na unidade organizacional onde deseja adicionar a conta de serviço. Selecione **New** (Novo) e, em seguida, clique em **User** (Usuário).
4. Em **First name** (Prenome), digite `FTKServMgr` para a conta de serviço e deixe **Last name** (Sobrenome) em branco.
5. Modifique **Full name** (Nome completo) como desejar.
6. Em **User logon name** (Nome de logon do usuário), digite `FTKServMgr`. A conta de serviço fará logon com o nome que você tiver inserido. Na lista suspensa, clique em **UPN suffix** (Sufixo UPN), que precisa ser anexado ao nome de logon da conta de serviço (após o símbolo @). Clique em **Next** (Avançar).
7. Em **Password** (Senha) e em **Confirm password** (Confirmar senha), digite uma senha para a conta de serviço.
8. Selecione as opções apropriadas para a senha e, em seguida, clique em **Next** (Avançar).
9. Clique em **Finish** (Concluir) para terminar de criar a conta de serviço.

Criar uma conta de usuário não administrativo

1. Faça logon com uma conta de usuário administrativo em um computador que esteja executando o Windows Vista.
2. Abra o menu **Start** (Iniciar). Clique com o botão direito do mouse em **Computer** e, em seguida, clique em **Manage** (Gerenciar).
3. Clique na seta ao lado de **Local Users and Groups** (Usuários e grupos locais).
4. Clique com o botão direito do mouse em **Users** (Usuários) e, em seguida, clique em **New User** (Novo usuário).
5. Digite o nome do usuário para o qual você está criando uma conta. Por exemplo, se quiser dar ao usuário o nome **webuser1**, digite `webuser1` no campo **Username** (Nome de usuário) e no campo **Full name** (Nome completo).
6. Digite uma senha de que vá se lembrar nos campos **Password** (Senha) e **Confirm Password** (Confirmar senha).

NOTA: as senhas fazem distinção entre maiúsculas e minúsculas. As senhas que você digitar nos campos **Password** (Senha) e **Confirm Password** (Confirmar senha) precisam coincidir para que você possa adicionar a conta de usuário.

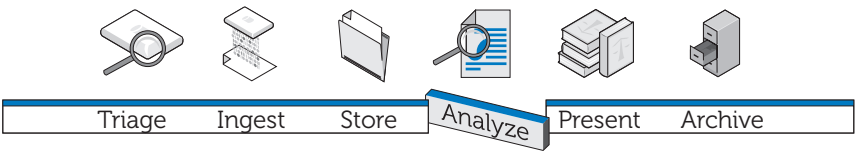
7. Desmarque a caixa de seleção **User must change password at next logon** (O usuário deve alterar a senha no próximo logon).
8. Marque as caixas de seleção **Password never expires** (A senha nunca expira) e **User cannot change password** (O usuário não pode alterar a senha).
9. Clique em **Create** (Criar) e, em seguida, clique em **Close** (Fechar).
10. Clique em **File** (Arquivo) e, então, clique em **Exit** (Sair).

Como configurar a segurança de casos individuais e arquivos de evidências

1. No **Windows Explorer**, navegue até o arquivo cujas permissões deseja definir. Clique com o botão direito do mouse no arquivo e, em seguida, selecione **Properties** (Propriedades).
2. Clique na guia **Security** (Segurança).
3. Desmarque a caixa de seleção ao lado de **Everyone** (Todos), se necessário.
4. Adicione somente os usuários que precisarão de acesso ao arquivo, conforme determinado pela política de seu local de trabalho.
   a. Clique em **Add** (Adicionar).
   b. No campo **Enter the object names to select** (Digite os nomes de objetos a serem selecionados), insira os nomes de usuário apropriados. Em seguida, clique em **OK**.
   c. Modifique as **Permissions** (Permissões) de cada usuário, conforme determinado pela política de seu local de trabalho.

5

Análise



Existem vários tipos diferentes de análise dos dados de evidências que o investigador precisa ser capaz de conduzir, inclusive análise de assinatura de arquivos e de hash, e extensa indexação e pesquisas de palavras-chave. Todas essas análises exigem uma capacidade de processamento considerável, visto que os arquivos de evidências de um único caso podem chegar a tamanhos na faixa de um terabyte e o processamento desses arquivos pode levar dezenas de horas – ou até mesmo dias – usando arquiteturas de data center comumente definidas hoje em dia. Os investigadores que tentam fazer essa análise em uma única estação de trabalho precisam levar essa questão em consideração ao programarem o processamento do caso, visto que a análise e a indexação de um único caso podem esgotar os ativos de hardware do investigador. A solução Dell Digital Forensics oferece as significativas vantagens do processamento distribuído, o que pode reverter completamente a situação. Abordaremos o processamento distribuído em breve, mas primeiro vamos examinar alguns dos tipos de análise tipicamente encontrados pelo investigador forense.

Tipos de análises

Análise de hash

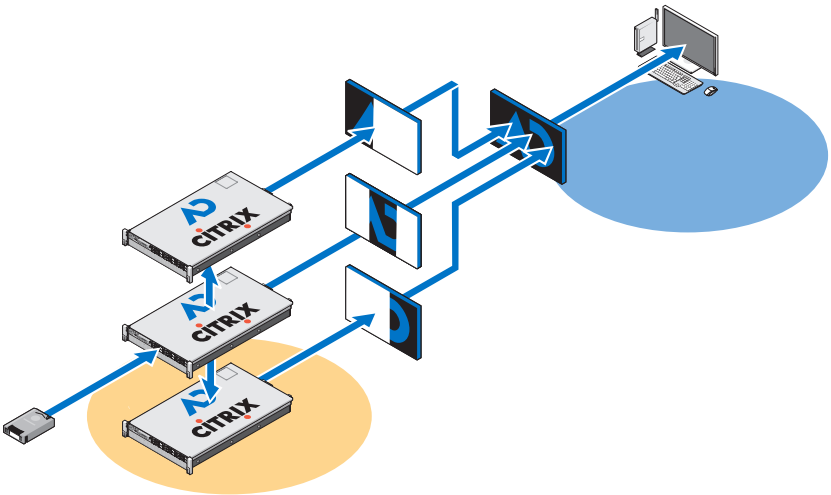
Uma função de hash usa algoritmos criptográficos para criar uma impressão digital dos dados. O hash pode ser usado para comparar um hash dos dados originais com o dos dados forenses analisados, o que pode ser aceito em tribunal como prova de que os dois grupos de dados são idênticos. A análise de hash compara os valores de hash do arquivo do caso com valores de hash conhecidos armazenados.

Análise de assinatura de arquivo

Cada arquivo tem um tipo, geralmente indicado pela extensão de três ou quatro letras do nome do arquivo. Por exemplo, um arquivo de texto pode ter a extensão ***.txt** e um arquivo de imagem pode ter a extensão ***.jpg**. Não é incomum que essas extensões de arquivo tenham sido alteradas para algo aparentemente inofensivo – um arquivo de imagem, por exemplo, pode ter sido renomeado com uma extensão de arquivo de texto na tentativa de mascarar seu conteúdo pornográfico.

No entanto, cada arquivo também possui um cabeçalho de arquivo, que inclui um código de tipo de arquivo diferente da extensão, mas indicativo somente de um tipo de arquivo específico. Por exemplo, um arquivo ***.bmp** terá o código de cabeçalho de tipo *.bm8. Quando o código do cabeçalho de tipo e a extensão do arquivo diferem, a análise forense precisa examinar os dados mais atentamente.

Figura 5-1. Processamento distribuído



O que é o Processamento distribuído?

O *Processamento distribuído* se refere ao uso de vários processadores, cada um com sua própria memória, individualmente aplicados a uma parte diferente de uma única tarefa computacional, que usam um sistema de passagem de mensagens para se comunicarem um com o outro no grupo. Processamento distribuído não é o mesmo que *processamento paralelo*, que se refere ao uso de vários processadores que compartilham um único ativo de memória.

Considere o seguinte, que lhe dará uma ideia aproximada das vantagens do uso de uma instalação com processamento distribuído pela Solução da Dell: a conclusão de uma análise de cinco arquivos de 200 GB pode levar apenas 3,5 horas, enquanto o processamento de um único arquivo de 200 GB em uma estação de trabalho independente pode levar cerca de 7-8 horas para ser concluído.

Mover o processamento dos dados de evidência da estação de trabalho do analista para o servidor não é tudo. A Solução da Dell também oferece a opção de executar o software analítico propriamente dito, como FTK ou EnCase, no servidor, o que permite que a estação de trabalho se torne uma interface integrada capaz de executar várias instâncias de diferentes pacotes de software forense em sistemas operacionais visualizados simultaneamente, sem degradação do desempenho do cliente.

Como usar o processamento distribuído no FTK 3.1

O Processamento distribuído permite aplicar os recursos adicionais de até três outros computadores de uma vez ao processamento dos casos. Depois que tiver instalado e configurado o Mecanismo de processamento distribuído, você poderá reduzir exponencialmente o tempo de processamento dos casos.

NOTA: como regra geral, usar o Processamento distribuído não reduz os tempos de processamento, a menos que o número de objetos a serem processados exceda 1.000 vezes o número de núcleos existentes no sistema. Por exemplo, em um sistema com oito núcleos, os mecanismos adicionais de processamento distribuído podem não reduzir o tempo de processamento, a menos que a evidência contenha mais de 8.000 itens.

NOTA: Para obter informações sobre a instalação e a configuração do módulo de Processamento distribuído como parte da Solução, consulte a seção apropriada do *Manual do usuário do FTK*.

1. Certifique-se de que a pasta do caso esteja compartilhada antes de tentar adicionar e processar a evidência. Se estiver seguindo as convenções de nomenclatura de arquivos da Dell, a pasta do caso deve estar localizada na unidade W:/ de seu espaço de trabalho. Se não tiver certeza quanto à localização da pasta do caso, entre em contato com o administrador do sistema.

2 Insira o caminho até a pasta do caso na caixa de diálogo **Create New Case** no formato UNC:

```
(\\[nomedocomputador_ou_endereço_IP]\[nomedocaminho]\[nomedoarquivo])
```

3 Clique em **Detailed Options** e selecione as opções que usaria normalmente.

4 Clique em **OK** para retornar à caixa de diálogo **New Case Options** e insira uma marca de verificação ao lado da opção **Open the case**. Clique em **OK** para criar o novo caso e abri-lo.

5 Clique em **Add** depois que o novo caso for aberto e a caixa de diálogo **Manage Evidence** será aberta automaticamente. Selecione o arquivo de evidência a ser adicionado e, em seguida, clique em **Open**.

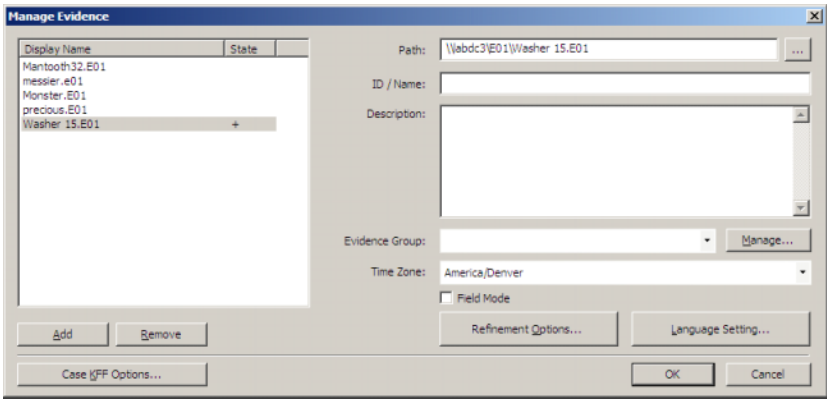
6 Por padrão, o caminho até a evidência é designado pela letra da unidade. Altere o caminho para o formato UNC alterando a letra da unidade para o nome ou endereço IP da máquina onde o arquivo de evidência está localizado, de acordo com a seguinte sintaxe:

```
\\[nomedocomputador_ou_endereço_IP]\[nomedocaminho]\[nomedoarquivo]
```

7 Deixe o restante do caminho como está.

8 O caminho UNC até a evidência é ilustrado na figura a seguir:

Figura 5-2. Caixa de diálogo Manage Evidence (Gerenciar evidência)



9 Clique em **OK**.

Como verificar a instalação

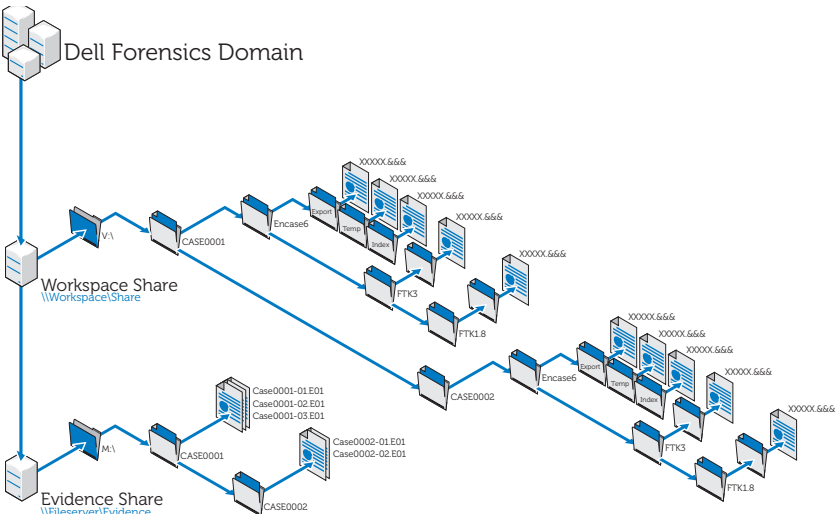
Quanto tiver concluído a instalação, abra o **Task Manager** no computador remoto e mantenha-o aberto enquanto adiciona a evidência e dá início ao processamento. Essas etapas permitirão que você observe a atividade de **ProcessingEngine.exe** na guia **Processes** (Processos).

O Mecanismo de processamento distribuído não é ativado até que um caso exceda aproximadamente 30.000 itens. Quando for ativado, você verá a porcentagem da CPU e a utilização da memória aumentarem para o **ProcessingEngine.exe** no **Task Manager**.

Como localizar arquivos na rede

As melhores práticas recomendam que os arquivos de evidência e de trabalho sejam armazenados separadamente na rede. A Dell recomenda configurar duas unidades de compartilhamento e, então, estabelecer arquivos e subarquivos de caso a partir de lá, conforme ilustrado na Figura 5-3.

Figura 5-3. Estrutura de arquivos recomendada pela Dell



Análise usando o FTK

Abrir um caso existente

Como usar o menu File (Arquivo)

1. No FTK, selecione **File** e, em seguida, selecione **Open Case**.
2. Realce o caso que deseja abrir e clique nele pra iniciar o caso.

NOTA: O nome de todos os arquivos de caso é **case.ftk**. O arquivo **case.ftk** de cada caso é armazenado na pasta do caso aplicável.

Na Linha de comando

Na linha de comando, digite:

```
caminho_para_o_arquivo_de_programa_do_ftk\ftk.exe
/OpenCase diretório_do_caso_de_destino
```

Como processar a evidência do caso

O FTK processa a evidência quando um caso é criado ou quando evidência é adicionada posteriormente ao caso. Para obter instruções sobre como criar um novo caso, consulte "Criar um caso" na página 60 ou consulte o *Manual do usuário do FTK*. Para obter instruções sobre como adicionar evidência a um caso existente, consulte "Adicionar evidência a um caso" na página 61 ou consulte o *Manual do usuário do FTK*. Consulte "Documentação e recursos relacionados" na página 16 para obter mais informações.

Análise com o uso do EnCase

Abrir um caso existente

1. No menu File (Arquivo), selecione **File→ Open**.
2. Navegue até o caso e clique em **Open**.

Criar um trabalho de análise

1. Clique na guia **Analysis Jobs** (Trabalhos de análise) na caixa de diálogo **Source Processor** (Processador de origem).
2. Clique em **New**. A caixa de diálogo **Create Analysis Job/Job Name** é exibida.

   O nome padrão do trabalho é Job__[aaaa_mm_dd__hh_mm_ss] como, por exemplo: Job___2009_06_24__03_42_42_PM.

   O nome de um trabalho não pode conter espaços no começo ou no fim nem qualquer dos seguintes caracteres: \ / : * ? " < > |
3. Insira o nome de um trabalho e clique em **Next**. A caixa de diálogo **Create Analysis Job/Module Selection** é exibida.

   Essa caixa de diálogo mostra as pastas de módulo no painel esquerdo e módulos individuais contidos nessas pastas do lado direito.

   Se um módulo estiver incluído em um trabalho de análise, mas não houver dados para esse módulo quando o trabalho for executado em uma coleção, esse módulo será ignorado. Esse recurso permite criar trabalhos de análise genéricos para uma variedade de conjuntos de dados coletados.
4. Insira uma marca na caixa de seleção do módulo.

   É possível selecionar mais de um módulo.

   Os módulos de análise não têm configurações que possam ser definidas pelo usuário.

   Para selecionar todos os módulos em um grupo, insira uma marca ao lado do nome da pasta do grupo no painel à esquerda.
5. Clique em **Finish**.

NOTA: os trabalhos de análise podem listar os módulos disponíveis não relacionados nos trabalhos de coleta. Esses módulos são identificados como módulos herdados, para que você possa analisar dados coletados em versões anteriores do Processador de origem usando módulos que não existem mais.

Executar como trabalho de análise

1. Na guia **Collected Data**, selecione a evidência que deseja analisar selecionando primeiro o nome do trabalho no painel da esquerda. Em seguida, selecione os arquivos de evidência propriamente ditos na tabela da direita.

2 Clique em **Run Analysis**. A caixa de diálogo **Select Analysis to Run** é aberta.

3 Selecione o trabalho de análise e, em seguida, clique em **Run**. O Processador de origem executa a análise na evidência selecionada. Quando a análise é concluída, o navegador de dados é exibido.

Como executar uma análise de assinatura

1 Clique em **Search**.

2 Marque a caixa **Verify file signatures** (Verificar assinaturas de arquivo) na área **Additional Options** (Opções adicionais) no canto inferior direito e, em seguida, clique em **Start**. A rotina de análise de assinatura é executada em segundo plano. Quando terminada, uma caixa de diálogo de conclusão de pesquisa é exibida. A caixa de diálogo apresenta o status da pesquisa, os tempos e os dados do arquivo.

Você pode exibir esses mesmos dados no console.

Como exibir os resultados da análise de assinatura

1 Clique em **Set-Include** no painel **Tree** para exibir todos os arquivos no caso.

Nesse nível, **Set Include** seleciona tudo no arquivo de evidência.

2 Organize as colunas no painel **Table**, de modo que as colunas **Name**, **File Ext** e **Signature** fiquem próximas umas às outras.

3 Classifique as colunas com **Signature** no primeiro nível, **File Ext** no segundo nível e **Name** no terceiro nível.

Role para cima ou para baixo para ver todas as assinaturas.

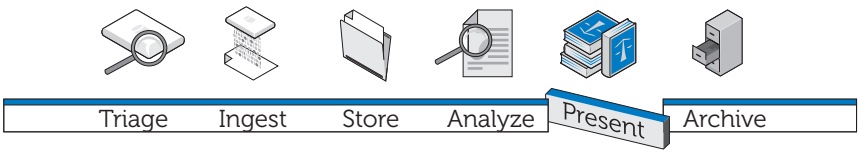
4 Clique em **Set-Include** na seleção **Entries** no painel **Tree**.

Uma lista de arquivos de caso, com suas assinaturas de arquivo associadas entre outros dados, é exibida no painel **Table**.

5 Classifique os dados, conforme desejado.

6

Apresentação



Elaborar relatórios dos resultados de sua análise é uma parte integral da solução Dell Digital Forensics, executada principalmente pelo software forense que você estiver usando como parte da Solução.

Como criar relatórios usando a solução Dell Digital Forensics

Criar e exportar relatórios usando o EnCase 6

1. Selecione os itens sobre os quais elaborar o relatório, sejam eles arquivos, marcadores, resultados de pesquisas ou outros dados.
2. Selecione o tipo de relatório desejado usando as guias no painel **Tree**.
3. Na guia **Table** no painel **Table**, ative os itens que deseja mostrar no relatório.
4. Na guia **Table**, alterne para a guia **Report**.
5. Modifique o relatório, conforme necessário.
6. Exporte o relatório para um formato que pode ser exibido fora do EnCase.
   a. Clique com o botão direito do mouse no relatório e clique em **Exportar** no menu suspenso. A caixa de diálogo **Export Report** é aberta.
   b. Clique no botão de opção apropriado para selecionar o formato de saída que deseja usar (TEXT, RTF ou HTML).
   c. Insira o caminho de saída ou navegue até ele.

d Se desejado, selecione **Burn to Disc** para ativar a caixa **Destination Folder** e, em seguida, clique com o botão direito do mouse em **Archive Files** para criar uma nova pasta e salvar um arquivo **.iso** no disco.

e Clique em **OK**.

Relatórios usando o FTK

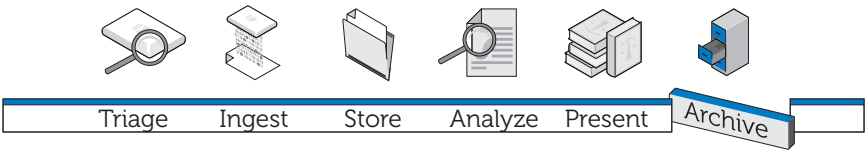
1. Clique em **File**→ **Report** para iniciar o **Report Wizard**.
2. Insira as informações básicas do caso solicitadas pelo assistente.
3. Selecione as propriedades dos marcadores.
4. Determine se e como deseja exibir os gráficos do caso em seu relatório.
5. Determine se deseja ou não incluir uma seção no relatório que lista os caminhos de arquivo e as propriedades dos arquivos nas categorias selecionadas.
6. Adicione as seções **Registry Viewer**, se desejar.

Exiba o relatório fora do FTK

1. Navegue até o arquivo do relatório.
2. Clique no arquivo do relatório e, em seguida:
   - Clique em **index.htm** para abrir um documento HTML em um navegador da Web.
   - Clique em [*report*]**.pdf** para abrir o relatório em um visualizador de PDF.

7

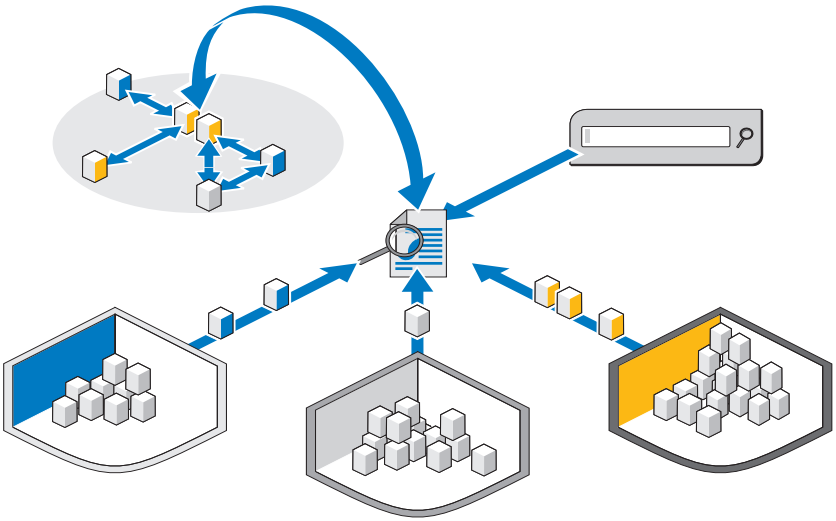
Arquivamento



Nenhuma solução forense digital estaria completa sem um componente escalável, seguro e abrangente de arquivamento e recuperação. Sua solução Dell Digital Forensics oferece isso e muito mais. Na estrutura da Solução da Dell, tentamos criar uma interface simples que funciona com todos os aplicativos forenses para controlar o ciclo dos arquivos de evidência e de casos. Devido ao fato de ser difícil prever quando os dados serão necessários no futuro ou quanto tempo uma investigação pode durar, criamos uma solução flexível que requer que o analista forense determine quais arquivos precisará recuperar ou arquivar. Esta solução usa uma abordagem em camadas para proporcionar armazenamento personalizado de acordo com suas necessidades – um mix de hardware SATA e SAS – e arquivamento determinado pelo usuário por meio de software NTP On-Demand Archiving.

A Solução da Dell consiste em componentes modulares que oferecem um ambiente escalável que pode ser expandido para atender às demandas crescentes dos requisitos de processamento e armazenamento. A infraestrutura formalizada de backup, recuperação e arquivamento (BURA) da Solução ajuda a otimizar a cooperação entre entidades e instituições e entre fronteiras. Ela libera sobrecargas administrativas por automatizar grande parte da tarefa de fazer backup dos dados, proporciona consistência entre os laboratórios de diferentes entidades e minimiza os riscos para a cadeia de custódia digital.

Figura 7-1. Recursos de pesquisa entre diferentes mídias e diferentes casos da Solução Dell



Um componente de pesquisa opcional muito poderoso permite a correlação de informações entre conjuntos de dados ingeridos. Esse componente oferece a capacidade de conduzir pesquisas semelhantes às da Internet em todo o armazenamento de dados do caso, tanto de conteúdo ativo e online quanto de material arquivado de casos anteriores.

Solução de arquivamento com um clique do cliente

Usando as ferramentas de arquivamento e recuperação da solução Dell Digital Forensics, um analista pode arquivar ou recuperar tanto arquivos individuais quanto estruturas de diretório inteiras com o clicar do botão direito do mouse. Comandos adicionais com o clique do botão direito do mouse foram adicionados ao software NTP On-Demand Archiving, de modo que basta que o usuário selecione e arquive ou selecione e restaure os dados. Quando um arquivo tiver sido selecionado para arquivamento, uma janela adicional será exibida solicitando ao usuário que confirme a ação. Após a confirmação, a solução executará um processo em segundo plano para mover o arquivo para um dispositivo de fita ou para um dispositivo de armazenamento mais acessível. Esse processo acontece com total fluidez em segundo plano, sem nenhuma degradação do desempenho da estação de trabalho do usuário.

Quando o processo em segundo plano tiver sido concluído, o ícone atribuído ao arquivo mudará para a cor cinza para identificar claramente ao usuário que o arquivo foi arquivado, mas a pasta e a estrutura de arquivos ainda ficarão visíveis, para que o usuário possa localizar o arquivo novamente no futuro com facilidade para fins de restauração. Para restaurar um arquivo, tudo que o usuário precisa fazer é navegar pela estrutura de pastas original, localizar a pasta ou arquivo que deseja restaurar, clicar com o botão direito do mouse no arquivo ou pasta e, em seguida, selecionar a opção de restauração.

A Dell recomenda que todos os arquivos de evidências e de casos fiquem localizados em um dispositivo NAS central escalável que permita um ponto de armazenamento centralizado e expansível, o que possibilita a fácil colaboração entre os analistas. Essa recomendação também possibilita um único ponto de auditoria para fins de cadeia de custódia. Quando um arquivo é selecionado para arquivamento, é movido para a próxima janela de processamento de sistema disponível do armazenamento principal para uma opção secundária (fita ou mais acessível).

Os tempos de arquivamento e de recuperação variam grandemente, dependendo do tráfego atual para o armazenamento NAS centralizado e a partir dele, dos arquivos que estão sendo arquivados e do tipo de mídia em que consiste a opção de armazenamento secundário. Por exemplo, SATA mais acessível apresentará taxas de conclusão muito mais rápidas do que a fita. Todos os arquivos podem ser criptografados na fita para reforço da segurança quando atingirem a fase de arquivamento de longo prazo da Solução, o que pode exigir um licenciamento adicional.

Recomendações de backup da Dell

Backup de arquivos de evidência e de casos

Um laboratório forense tem três tipos de arquivo principais:

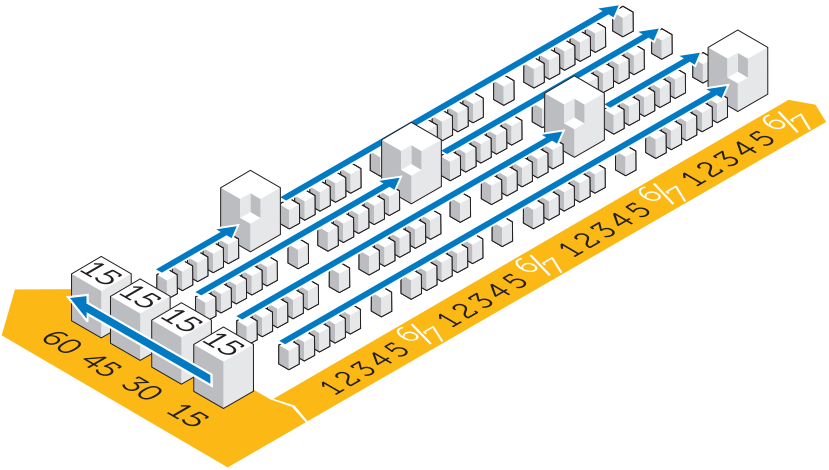
- Arquivos de imagens – As imagens criminalmente significativas do dispositivo suspeito. Uma vez ingeridas, elas nunca são alteradas e seu backup precisa ser feito apenas uma vez (possíveis extensões: **E01**, **DD**, etc.). Arquivos de evidência tendem a ser encontrados em baixa quantidade, mas com tamanho muito grande.
- Arquivos de caso – Trata-se dos arquivos de dados e indexes que resultam da análise. Podem precisar ser exportados do aplicativo forense. Os arquivos mudam frequentemente se o caso estiver ativo e podem conter vários tipos de extensão, o que exige que seu backup seja feito diariamente. Arquivos de caso tendem a ser numerosos, mas geralmente de tamanho muito pequeno.

- Banco de dados – Este tipo de arquivo é usado somente no FTK 3 (no momento), mas contém todos os vínculos entre os arquivos de caso e os arquivos de evidência, bem como todos os marcadores e notas da investigação. O backup dos tipos de arquivo de banco de dados precisa ser feito diariamente.

A Figura 7-2 mostra a melhor prática sugerida para o backup de um laboratório forense digital. Devido ao fato de que muitos laboratórios forenses têm mais de 50 TB de armazenamento, pode não ser possível fazer um backup completo em uma janela padrão de backup de um fim de semana. Para garantir que, no caso de um desastre, os dados possam ser restaurados com o mínimo ponto de recuperação possível, o backup é dividido em seções iguais e executado no período de um mês.

Esse processo requer que o tamanho máximo de qualquer backup completo se restrinja a 15 TB. Cada LUN cria atualizações incrementais para o resto do ciclo de backup, até que seja hora de fazer um backup completo novamente.

Figura 7-2. Melhor prática para plano de backup



Fora do host x Rede

Devido ao tamanho dos dados que precisam ser movidos para fita para fins de recuperação de desastres na maioria dos laboratórios forenses, o armazenamento dos LUNs é dividido em LUNs de 15 TB. Esse requisito facilita o gerenciamento e o backup, além de reduzir as falhas de cluster do sistema de arquivos com o tempo em caso de falha.

Dois tipos de backup podem ser executados: na rede ou como um backup fora do host.

- Em uma configuração na rede, todos os dados de backup são transmitidos pela rede para o servidor de backup por meio de um agente de backup que reside no servidor.
- Em uma solução de backup fora do host, alguns dos servidores com os maiores armazenamentos de arquivos não fazem o backup de seus dados pela rede. Em vez disso, a matriz de armazenamento cria um instantâneo do LUN e monta essa cópia diretamente no servidor de backup. Esse processo aumenta a velocidade do backup em geral, visto que nenhum arquivo de backup é transmitido pela rede normal causando problemas adicionais de competição pela rede.

Em muitos laboratórios forenses de hoje em dia, os backups são conduzidos em redes de 10 GB.

A figura a seguir mostra os agentes necessários por servidor para facilitar o backup:

Figura 7-3. Agentes de backup

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 Agente de arquivo aberto

AD Active Directory

OA Agente Oracle (agente genérico de banco de dados necessário em execução de backup da Symantec)

SA Agente SQL (agente genérico de banco de dados necessário na execução de backup)

NBU Servidor NetBackup

BE Servidor de execução de backup

EV Licença de backup do Symantec Enterprise Vault

MI Backup completo mensal, incrementos diários

SS Estado do sistema criado uma vez por mês

NOTA: conforme a quantidade dos dados aumenta com o tempo, uma solução de backup fora do host pode ser necessária.

Como arquivar usando a solução Dell Digital Forensics

Arquivamento sob demanda

O NTP Software ODDM e o NTP Software Right-Click Data Movement (RCDM) funcionam em conjunção com o Enterprise Vault para atenuar a necessidade de verificações de todo o sistema, como no caso do arquivamento convencional, por meio da implementação do *arquivamento sob demanda*. Os custos de armazenamento são reduzidos e a qualidade de arquivamento é aprimorada.

Dependendo do estágio no ciclo de vida dos dados, conforme descrito em "Como fazer a correspondência do arquivamento e recuperação das evidências com o ciclo de vida do caso" na página 67, o analista pode optar por arquivar os dados em armazenamento de mais longo prazo ou retê-los para acesso e processamento imediato.

Além disso, o NTP Software ODDM pode ser usado para arquivar automaticamente dados que precisam ser armazenados para fins legais.

Requisitos

O NTP Software ODDM requer o Microsoft IIS, o Microsoft .NET Framework, o SQL e o Enterprise Vault. O NTP Software ODDM e o Enterprise Vault precisam ser instalados no mesmo servidor. Instalações maiores podem manter o banco de dados SQL em um servidor dedicado.

Instalação

Para obter instruções detalhadas da instalação do NTP Software ODDM e do NTP Software RCDM, consulte o *Dell Digital Forensics Installation and Configuration Guide* (Manual de instalação e configuração do Dell Digital Forensics). Consulte "Documentação e recursos relacionados" na página 16 para obter mais informações.

Como arquivar usando o NTP Software ODDM

Arquivamento determinado pelo usuário

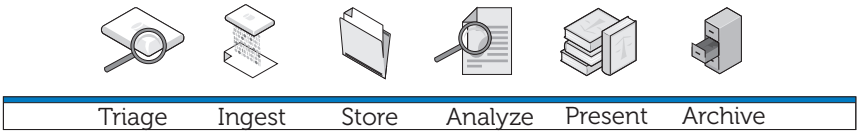
1. Quando o analista armazena arquivos de dados, o NTP Software QFS alerta o usuário quando à necessidade de arquivamento dos arquivos.
2. O analista seleciona os arquivos a serem arquivados usando o NTP Software Storage Investigator e, em seguida, clica em **Archive**. No entanto, se os suplementos do NTP RCDM estiverem instalados, ele poderá clicar com o botão direito nos arquivos.

   Quando os arquivos estiverem selecionados, o NTP Software Storage Investigator notificará o NTP Software ODDM que, por sua vez, ativará o Enterprise Vault.

   A solicitação de arquivamento será adicionada à fila de arquivamento.

8

Solução de problemas



Dicas gerais de solução de problemas

- Certifique-se de que todos os clientes e servidores estejam visíveis uns aos outros – que sejam capazes de executar ping uns dos outros, tanto pelo nome de NetBIOS quanto pelo endereço IP.
- Certifique-se de que os firewalls permitam o tráfego.
- Reinicie os servidores e clientes para se certificar de que todas as alterações à instalação e à configuração tenham sido reconhecidas pelos sistemas.

Questões específicas ao software forense

EnCase: o EnCase é iniciado no modo de Aquisição

Esse problema indica que o EnCase não está licenciado.

1. No EnCase, selecione **Tools**→ **Options** e assegure-se de que **User Key Path**, **Server Key Path** e **Server Address** estejam preenchidos (esses campos devem apontar para os locais das chaves de licença).
2. Verifique o firewall no cliente e o servidor de licença do EnCase para se assegurar de que a porta 4445 esteja aberta.
3. Certifique-se de que o cliente possa executar ping no servidor de licença do EnCase.

FTK Lab: navegador iniciado pelo cliente não pode exibir a interface de usuário

1. Certifique-se de que o cliente tenha o MS Silverlight instalado.
2. Assegure-se de que os serviços Oracle tenham sido iniciados no servidor que hospeda o banco de dados Oracle.

FTK 1.8: mensagem de limite de 5000 objetos\versão de avaliação

Se você receber esta mensagem, o FTK não tem uma licença. Assegure-se de que o servidor de licença de rede esteja funcionando e de que as licenças do FTK 1.8 estejam no lugar:

1. Abra uma janela do navegador no servidor que hospeda o serviço de licença de rede e insira **http://localhost:5555** na barra de endereço.
2. Observe se as licenças estão instaladas ou não. Se não estiverem será preciso instalar as licenças.

FTK 1.8: erro Cannot Access Temp File (Não é possível acessar arquivo temporário) exibido na inicialização

Permita que o usuário que está iniciando o aplicativo (ou sua sessão do Citrix) tenha acesso ao disco rígido do servidor OU execute o aplicativo como administrador.

Problemas como o Citrix

Citrix: os aplicativos não são iniciados

1. Certifique-se de que todos os serviços (especialmente MFCOM e IMA) tenham sido iniciados nos servidores que hospedam o XenApp.
2. Certifique-se de que o cliente possa ver e executar ping nos servidores XenApp.
3. Verifique o firewall nos clientes e nos servidores XenApp para se assegurar de que as portas do XenApp estejam abertas.
4. Verifique o servidor de licenças do Citrix para se certificar de que o serviço de licenciamento de rede tenha uma licença que possa emitir. Normalmente, o servidor de licenciamento do Citrix é instalado em um dos servidores Citrix XenApp, sendo acessível via **Start→ Programs→ Citrix→ Management Consoles→ Citrix Licensing**.

5 Abra o **Citrix Management Console** (**Start→ Programs→ Citrix→ Management Consoles→ Citrix Delivery services console**). Em seguida, execute uma detecção para garantir que todos os servidores XenApp estejam presentes na farm.

6 Assegure-se de que o aplicativo tenha sido publicado em um servidor XenApp válido (que esteja incluído na farm).

7 Olhe no **Citrix Delivery Services Console** para se certificar de que o usuário que está iniciando o aplicativo está em um Grupo autorizado a iniciar o aplicativo.

8 Para aplicativos em fluxo, certifique-se de que o User Account Control (UAC - Controle de conta de usuário) esteja desligado no servidor.

Sessões do Citrix congeladas ou travadas

Quando os usuários não fazem logoff corretamente de suas sessões do Citrix, as sessões órfãs começam a desacelerar o servidor, terminando por congelá-lo ou travá-lo. Portanto, é extremamente importante que os usuários sigam as melhores práticas de fazer logoff de maneira formal e apropriada de cada sessão (**Start→ Logoff→ Ok**) e não simplesmente cliquem no *x* no canto superior direito da janela da sessão.

Ainda assim, é possível que você se depare com esse problema, e estas são duas maneiras de solucioná-lo:

1 Faça logoff do usuário manualmente.

   a Abra uma sessão como Administrador do Citrix.

   b Examine a lista de sessões abertas e feche cada sessão manualmente.

2 Reinicie o servidor.

Índice remissivo

D

E

F

I

L

N

P

S

T