Dell™ Digital Forensics

# Guide de la solution

# Remarques, précautions et avertissements

**REMARQUE :** Une REMARQUE indique des informations importantes qui facilitent l'utilisation de l'ordinateur.

**PRÉCAUTION : Une PRÉCAUTION indique un endommagement potentiel du matériel ou une perte de données potentielle si les instructions ne sont pas respectées.**

**AVERTISSEMENT : Un AVERTISSEMENT indique un endommagement potentiel d'un bien, une blessure potentielle ou un risque mortel.**

---

**Les informations de ce document peuvent être modifiées sans préavis.**
**© 2011 Dell Inc. Tous droits réservés.**

Toute reproduction de ce contenu est strictement interdite sans autorisation préalable de Dell Inc.

Marques commerciales citées dans ce texte : Dell™, le logo DELL™, PowerEdge™, EqualLogic™ et PowerConnect™ sont des marques commerciales de Dell Inc. Oracle® est une marque d'Oracle Corporation et/ou de ses filiales. Citrix® est une marque de Citrix Systems, Inc. aux Etats-Unis et/ou dans d'autres pays.

Les autres marques et noms commerciaux utilisés dans ce document font référence à des entités propriétaires des marques et des noms de leurs produits. Dell Inc. ne revendique aucun intérêt concernant ces marques et noms.

**2011 - 07** **Rév. A00**

# Table des matières

# 1

# Présentation


Ces dernières années ont vu une augmentation exponentielle de l'activité numérique par les criminels et les groupes terroristes du monde entier tant du point de vue du volume, de la rapidité et de la variété que de la sophistication. Actuellement, la plupart des crimes ont une composante numérique. Pour certains, il s'agit d'un véritable *tsunami numérique*. Cette croissance s'explique par les avancées remarquables qui touchent les matériels électroniques. La diversité croissante des appareils électroniques grand public et leur capacité de mémoire et de stockage croissante donnent aux criminels et aux terroristes une multitude de possibilités pour masquer des informations malveillantes.

Les PC et les ordinateurs portables disposant de disques durs de plusieurs centaines de gigaoctets ne sont pas rares. Les derniers disques durs offrent une capacité de 1 à 4 téraoctets. Sachez qu'un téraoctet permet de stocker le contenu de deux cents DVD ; une énorme capacité de stockage qui représente un problème grandissant.

Qu'il s'agisse de PC ou d'ordinateurs portables, de téléphones mobiles ou de clés USB et même de consoles de jeux, les professionnels de l'investigation numérique sont amenés à cloner, incorporer, indexer, analyser et stocker des volumes croissants de données suspectes tout en préservant la chaîne de conservation et en continuant de protéger les citoyens.

**Table 1-1. Quelle est la taille d'un zettaoctet ?**

| | | | |
|---|---|---|---|
| Kilo-octets (Ko) | 1 000 octets | 2 Ko | Une page dactylographiée |
| Megaoctet (Mo) | 1 000 000 octets | 5 Mo | L'oeuvre complète de Shakespeare |
| Gigaoctet (Go) | 1 000 000 000 octets | 20 Go | Une bonne partie de l'oeuvre de Beethoven |
| Téraoctet (To) | 1 000 000 000 000 octets | 10 To | Une bibliothèque de recherche d'université |
| Pétaoctets (Po) | 1 000 000 000 000 000 octets | 20 Po | Production annuelle de disque dur |
| Exaoctets (Eo) | 1 000 000 000 000 000 000 octets | 5 Eo | Tous les mots prononcés par les être humains |
| Zettaoctets (Zo) | 1 000 000 000 000 000 000 000 octets | 2 Zo | Données qui ont été créées au niveau mondial en 2010* |

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

Lorsque des criminels sont accusés et des ordinateurs et d'autres ressources numériques saisis, les professionnels de l'investigation numérique sont soumis à d'énormes pressions sur une brève période et dans des environnements qui ne sont pas propices à l'établissement aisé de la preuve. Lorsque des organisations entières sont suspectées d'activités criminelles ou terroristes, le nombre d'appareils à analyser peut augmenter de manière exponentielle.

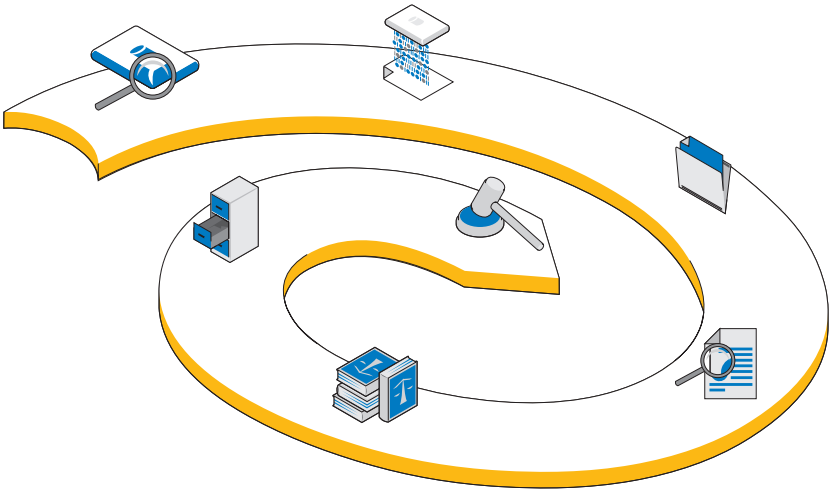
L'investigation numérique permet d'acquérir les données extraire des ordinateurs et d'autres appareils numériques (téléphones mobiles, consoles de jeux, unités flash, GPS, etc.) et d'analyse et de vérifier scientifiquement ces données pour les utiliser devant un tribunal. La solution Dell Digital Forensics comprend la première vraie solution de niveau entreprise de bout en bout destinée aux organismes chargés de l'application de la loi, aux agences de sécurité d'entreprise et publiques et aux organisations d'e-discovery, qui fournit tout le matériel, le logiciel, le service et le support nécessaire pour collecter, trier, incorporer, créer des images, stocker, analyser, générer des rapports et archiver les preuves numériques.

En utilisant le serveur d'entreprise évolutif et économique et le matériel de stockage de Dell et, selon la configuration de votre environnement logiciel, des systèmes de base de données Oracle sur le back-end, une combinaison d'ordinateurs portables dédiés Dell, le logiciel SPEKTOR sur le terrain et le support de Dell, les enquêteurs peuvent effectuer rapidement et aisément des opérations de collecte et de triage des données d'investigation numérique, en maintenant la chaîne de conservation du site au centre de données et au tribunal.

# Le cycle de vie Dell Digital Forensics

La solution Dell Digital Forensics soutient l'enquêteur informatique pendant les six phases du cycle de vie de l'investigation : Triage, Incorporation, Stockage, Analyse, Présentation et Archivage.

**Figure 1-1. Le cycle de vie Dell Digital Forensics**



### *Triage*

Le triage permet à l'enquêteur informatique de visualiser rapidement le contenu des périphériques cible pour déterminer si le périphérique doit être envoyé au laboratoire pour être analysé et préparer un dossier en vue d'un procès.

### *Incorporation*

Il s'agit de l'étape du processus d'investigation informatique au cours de laquelle l'image des données cible est créée (si elle n'a pas été créée sur le site pendant le triage) et une copie exacte du périphérique de stockage suspect est générée de sorte que l'intégrité de la copie peut être garantie en comparant les hachages du périphérique de données d'origine et de la copie du périphérique.

Conformément aux pratiques existantes, l'*image* des données suspectes est créée dans la solution Dell Digital Forensics. Au lieu de créer l'image des données sur un seul poste de travail, l'image est incorporée dans un référentiel de preuves central. En incorporant immédiatement les données au centre de données, les données sont accessibles à plusieurs analystes, peuvent être transférées d'un périphérique vers un autre en un minimum de temps et la productivité et l'efficacité augmentent considérablement. Toutefois, l'incorporation a lieu sur site si la capacité de stockage cible est insuffisante. La solution Dell Digital Forensics permet l'incorporation sur site en utilisant un module SPEKTOR Imager en option.

### *Stockage*

La solution Dell Digital Forensics fournit un large éventail d'options de stockage et d'accès réseau pour répondre aux besoins de chaque client. Le stockage et l'extraction haut débit dans un environnement réseau d'entreprise permet d'utiliser une configuration multiutilisateur qui accroît la productivité et l'efficacité. Les analystes n'ont plus à allouer leurs ressources informatiques à l'analyse des preuves, car tout se passe sur le serveur dédié.

### *Analyse*

Le traitement parallèle fournit par la solution Dell Digital Forensics permet à l'analyste d'indexer et de trier les données sur des serveurs haute performance plutôt que sur des PC beaucoup moins puissants. En outre, il est possible d'exécuter simultanément plusieurs sessions d'analyse sur un ou plusieurs postes de travail en utilisant les configurations qui incluent la solution. Cela permet de protéger le système et l'intégrité des preuves, de réinstaller les postes de travail si du code malveillant est exécuté par accident, de préserver la chaîne de conservation et de ne pas avoir à régénérer les postes de travail des analystes lors du passage d'une affaire à une autre. Dans l'environnement Digital Forensics, la *chaîne de conservation* vise à maintenir l'intégrité des données numériques de la collecte et la communication des conclusions jusqu'à la présentation des preuves au tribunal.

### *Présentation*

En utilisant solution Dell Digital Forensics, les équipes de visualisation et les enquêteurs peuvent accéder à des preuves potentielles en toute sécurité en temps réel, ce qui évite de transférer les preuves sur des DVD ou aux experts de se rendre au laboratoire pour accéder aux fichiers.

### *Archivage*

La solution Dell fournit une infrastructure de sauvegarde, de récupération et d'archivage formalisée pour optimiser la coopération entre les agences et les divisions de sécurité et même les pays, éliminer la charge administrative, garantir la cohérence entre les laboratoires et réduire les risques au niveau de la chaîne de conservation des données numériques.

De plus, la solution Digital Forensics de Dell contient un compostant de recherche en option qui permet d'établir des corrélations entre les ensembles de données incorporés.

## La solution Dell élimine les problèmes du secteur

La solution Dell Digital Forensics facilite considérablement l'apport des preuves numériques de la scène du crime au tribunal pour les professionnels de l'investigation en fournissant :

- des communications réseau de centre de données de pointe qui accélèrent l'incorporation, l'analyse et le partage des informations numériques
- une garantie sur les informations en automatisant davantage l'investigation des données numériques en réduisant les risques d'erreurs et de compromission des données
- une garantie d'intégrité étendue des données en utilisant les protocoles de hachage les plus sûrs et bientôt par la mise en oeuvre d'une fonction d'audit qui permettra d'automatiser les enregistrements de la chaîne de conservation

**REMARQUE :** Toute conclusion ou recommandation dans ce document qui peut ressembler à un conseil juridique doit être analysé par un conseiller juridique. Contactez la juridiction locale, le tribunal local et le laboratoire d'investigation informatique local pour connaître les méthodes de collecte des preuves numériques à appliquer.

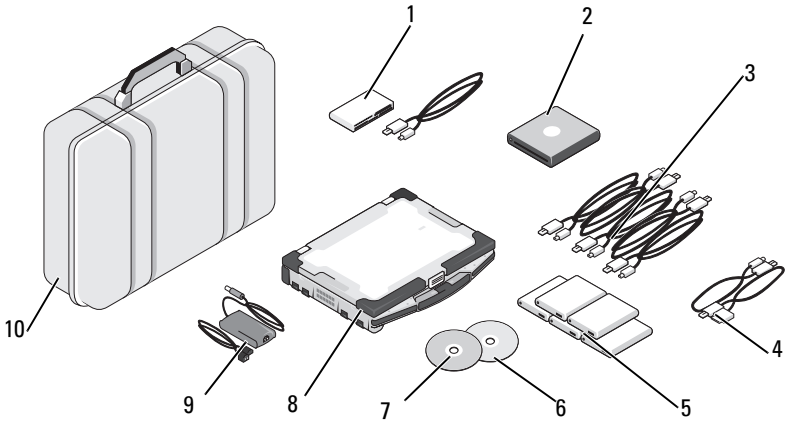
- une solution de bout en bout qui réduit sensiblement la complexité de la planification, de la mise en oeuvre et de la gestion d'une procédure d'investigation numérique d'entreprise
- une solution souple, économique, modulaire, évolutive, durable et sur mesure

# Composants de la solution

## Sur site

La partie mobile de la solution entre dans une malette robuste qui entre dans le rack d'un avion. La malette contient tous les outils et les logiciels nécessaires au triage sur site des périphériques de stockage suspects, ainsi qu'un ordinateur portable renforcé Dell E6400 XFR doté du logiciel d'investigation SPEKTOR préinstallé, des bloqueurs d'écriture d'investigation Tableau avec des accessoires, des unités de disques externes USB en qui peuvent fonctionner sous licence avec le logiciel SPEKTOR comme *collecteurs* d'image de triage, un lecteur de cartes 50:1 et les adaptateurs et les câbles répertoriés dans la Figure 1-2.

**Figure 1-2. Solution Dell Digital Forensics : Composant mobiles**




| | | | |
|---|---|---|---|
| 1 | Lecteur de cartes 50:1 | 6 | Disque de restauration d'image |
| 2 | ROM USB DVD | 7 | Disque de démarrage SPEKTOR |
| 3 | Câbles USB de collecteur | 8 | Ordinateur portable renforcé Dell |
| 4 | Options de câbles téléphoniques pour SPEKTOR PI (en option) | 9 | Alimentation électrique pour ordinateur portable renforcé |
| 5 | Collecteurs pour disque dur externe (5) | 10 | Affaire Pelican |

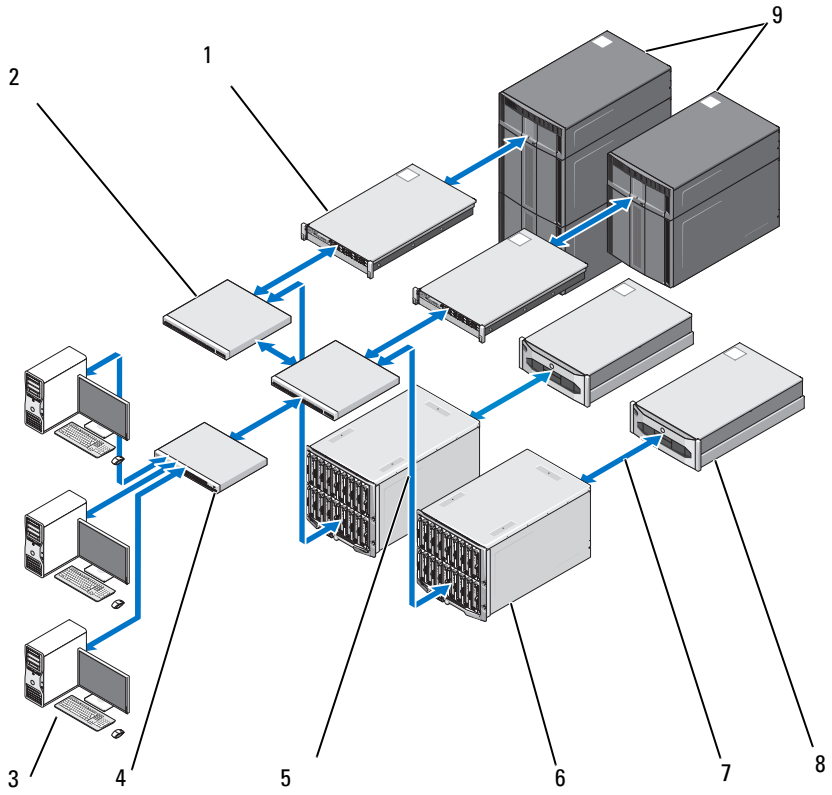
### Dans le centre de données

Dans le centre de données, la solution Dell Digital Forensics inclut une configuration personnalisée constituée des composants suivants :

- Serveurs en rack Dell PowerEdge R410, R610 et R710
- Serveurs Dell PowerEdge M610 et M710 Blade
- Dell EqualLogic 4000\6000 Series SAN
- Windows Server 2008 R2
- Citrix XenApp 6.0
- AccessData FTK 1.8, AccessData FTK 3, AccessData Lab
- Guidance En e 6.15
- NTP Software On-Demand Data Management (ODDM)
- Symantec Enterprise Vault
- Symantec Backup Exec 2010
- Commutateurs Dell PowerConnect
- Commutateurs Extreme Networks

Les serveurs en rack et lames Dell PowerEdge peuvent remplir différents rôles : serveur de fichiers, serveur de preuves, serveur d'archives, serveur de base de données, serveur de licences En e et FTK, serveur de sauvegarde ou contrôleur de domaine. Ils sont compatibles avec Microsoft Active Directory et tous les logiciels de sécurité et d'investigation informatique de la solution Dell Digital Forensics.

**Figure 1-3. Solution Dell Digital Forensics : Centre de données**




| | | | |
|---|---|---|---|
| 1 | Serveur PowerEdge R410 ou R610 (en option) | 6 | Serveurs Dell PowerEdge M1000E et M610 Blade |
| 2 | Commutateur Dell PowerConnect | 7 | Flux de données 10 Go |
| 3 | Poste de travail Dell Precision ou OptiPlex | 8 | Systèmes de stockage Dell EqualLogic PS4000 ou PS6000 Series |
| 4 | Commutateur Dell PowerConnect | 9 | Sockage Dell PowerVault ML |
| 5 | Flux de données 1 Go | | |

## A propos de ce document

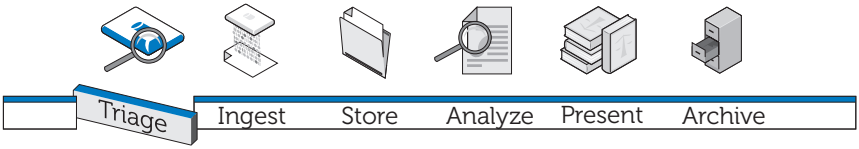
Ce document couvre chaque étape de l'investigation informatique dans un chapitre distinct et contient des chapitres sur la résolution des problèmes et les matériels et les logiciels pris en charge par la solution. Chacun des chapitres de la procédure commence par une discussion sur les meilleures pratiques et les problèmes que vous pouvez rencontrer lors de la mise en oeuvre et de la gestion de la solution et se termine avec la description des outils et des composants correspondant à l'étape de la solution.

## Documentation et ressources associées

Vous pouvez accéder à des informations complémentaires sur le site **support.dell.com/manuals**.

# 2

# Triage




## Qu'est-ce que le triage ?

Le triage permet à la personne chargée de l'investigation informatique de parcourir les données contenues dans des périphériques suspects et de prendre des décisions relatives aux périphériques qui nécessitent à l'évidence d'être saisis pour créer une image immédiatement sur site (si les données représentent un petit volume) ou plus tard dans le centre de données. La possibilité de prévisualiser et de saisir certains périphériques uniquement peut permettre aux enquêteurs de respecter le délai de présentation des preuves en accélérant sensiblement le processus. Le triage permet de réduire le nombre de périphériques de stockage qui doivent faire l'objet d'investigation en évitant d'encombrer davantage une file d'attente déjà saturée et en diminuant considérablement les coûts.

## Avantage de la solution de triage de Dell

### *Mobilité*

La solution Digital Forensics de Dell peut se trouver sur la scène du crime avec l'enquêteur ; tous les composants ont été soigneusement prétestés pour fonctionner ensemble et ils couvrent un large éventail de ports et de connecteurs de périphérique cible qui peuvent exister.

### *Rapide*

Les solutions de triage de l'investigation informatique peuvent être lentes et peuvent même ne pas tenir compte de données, car elles exécutent des tâches de recherche de mot de passe ou de correspondance de hachage pendant la collecte des données. La solution Digital Forensics de Dell élimine ces obstacles en utilisant la puissance de traitement de l'ordinateur portable éprouvé de Dell et non pas le PC cible pour analyser les données collectées. Dans certains cas, vous pouvez ne pas créer d'image ni indexer les données dans le laboratoire d'investigation informatique.

### *Simplicité d'utilisation de solution*

Les composants de triage de la solution sont prêts à l'emploi. Le logiciel préinstallé dispose d'une interface graphique tactile intuitive. Vous pouvez créer des profils réutilisables de collecte pour différents scénarios pour un déploiement standard.

### *Processus d'investigation acceptable*

Le logiciel de triage applique un processus d'analyse efficace et acceptable d'un point de vue investigation pour que chaque preuve potentielle puisse être capturée, vérifiées et stockée sans compromis.

### *Souplesse*

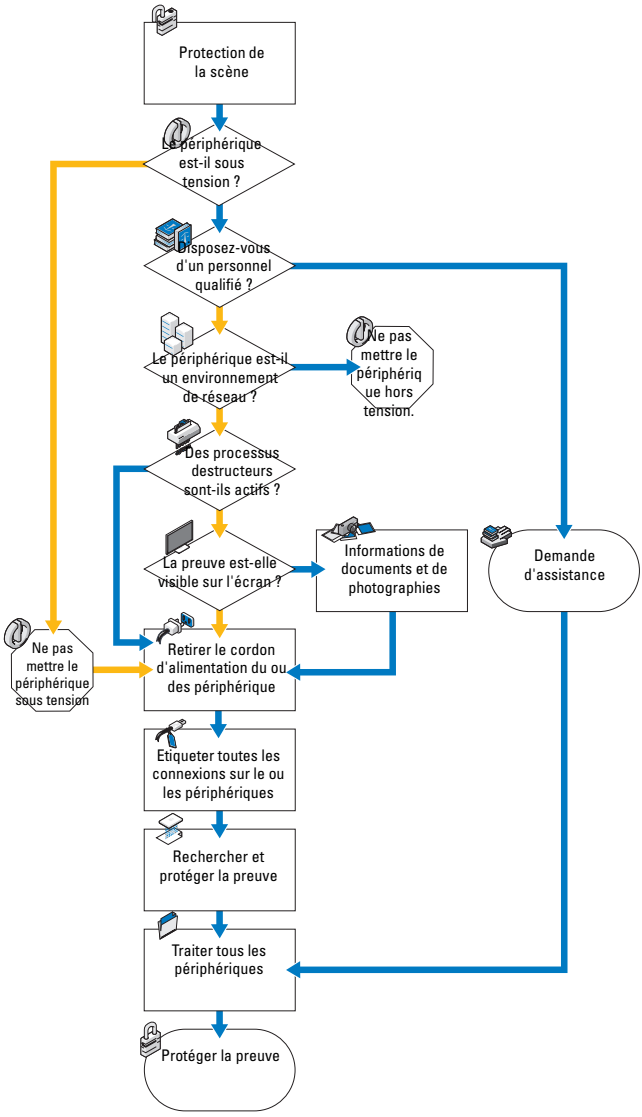
Les composants de triage peuvent être utilisés pour examiner la plupart des périphériques et plates-formes de stockage numériques, notamment les périphériques fonctionnant sous les systèmes d'exploitation Windows et Mac OS X d'Apple, ainsi qu'un large éventail de types de périphériques de stockage numériques, tels que les lecteurs MP3, les disques durs externes, les cartes mémoire, les téléphones mobiles et satellites, les unités GPS, les iPads et les iPhones et les unités flash. En outre, vous pouvez exporter vers d'autres programmes les résultats du triage en utilisant la solution Digital Forensics de Dell.

### *Puissance*

L'ordinateur portable éprouvé de Dell contrôle l'ensemble du processus, de l'analyse automatique des données ciblées à la fourniture des résultats détaillés dans un format de rapport clair en quelques minutes. Avec la solution Dell, l'enquêteur est à même d'exécuter plusieurs analyses de triage en parallèle avec une seule clé de licence.

# Collecte des preuves avec l'investigation informatique numérique

**Figure 2-1. Flux de collecte des données**



# Acquisition standard et acquisition dynamique

La solution Digital Forensics de Dell permet d'exécuter deux types d'acquisition : standard et dynamique. Au cours de la procédure d'acquisition standard, l'ordinateur portable éprouvé de Dell utilise le disque de démarrage SPEKTOR pour capture les données de triage sur un périphérique de stockage hors tension. En revanche, la procédure d'acquisition dynamique capture les données de triage depuis un périphérique de stockage sous tension pour obtenir les preuves qui ne pourraient pas être obtenues autrement.

Auparavant, les normes du secteur imposaient à l'enquêteur de débrancher l'appareil numérique et de le saisir pour l'emmener au laboratoire. Il s'en suivait une perte potentielle de preuve dans les données volatiles stockées : données stockées dans le presse-papiers, fichiers ouverts, contenu de la mémoire RAM, mots de passe en mémoire cache, etc. En outre, les données chiffrées peuvent être perdues si l'ordinateur est mis hors tension avant la création de l'image du disque. D'autre part, sachant que la plupart des ordinateurs protègent le BIOS et le disque dur par des mots de passe définis par l'utilisateur, la mise hors tension d'un système dont le BIOS est protégé par un mot de passe peut empêcher d'accéder à l'ensemble du contenu du périphérique.

Les meilleures pratiques du secteur recommandent à un enquêteur de suivre les instructions ci-dessous pour traiter un périphérique de stockage de données suspect :

- Si le périphérique est sous tension, maintenez-le sous tension dans la mesure du possible jusqu'à ce qu'une investigation soit exécutée.
- Si le périphérique est hors tension, laissez-le hors tension.

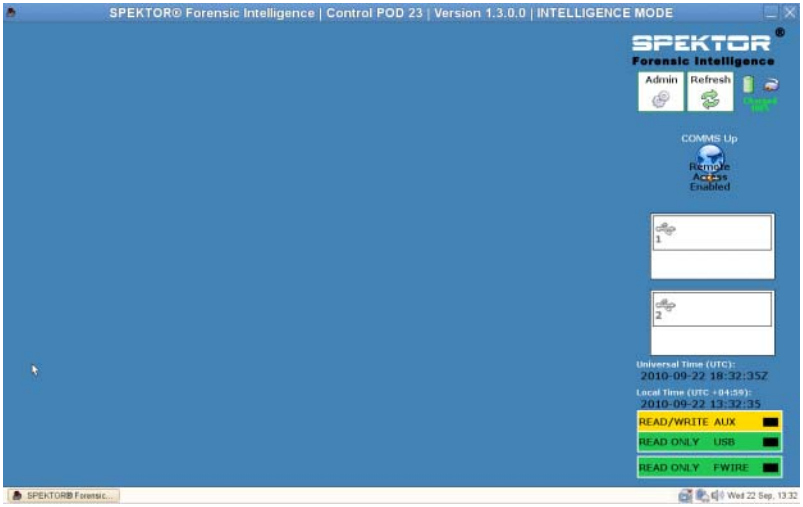
Ces instructions visent à permettre à l'enquêteur de conserver tels quels les périphériques de stockage sur le site et d'apporter le moins de modifications possibles au périphérique et à son contenu.

# Exécution du triage en utilisant la solution Digital Forensics de Dell

### Mettre sous tension l'ordinateur portable renforcée Dell

1. Appuyez sur le bouton d'alimentation pour ouvrir une session sur l'ordinateur. L'ordinateur charge automatiquement le logiciel SPEKTOR.
2. Tapez ou cliquez sur **Accept EULA**. L'écran d'**accueil** s'affiche.

**Figure 2-2. Ecran d'accueil**




## Graver un CD pour les procédures d'acquisition standard

1 Dans l'écran d'**accueil**, tapez ou cliquez sur **Admin**. Tapez ou cliquez sur **Burn Boot CD**.

**Figure 2-3. Bouton Burn Boot CD dans l'écran d'accueil**


2 Suivez les instructions qui s'affichent et cliquez sur **Finish**.

## Enregistrer un collecteur ou un disque de stockage

**REMARQUE :** Les collecteurs doivent avoir une licence et être configurés par SPEKTOR pour pouvoir être utilisés avec la solution Dell Digital Forensics. Contactez l'administrateur système si vous avez besoin de collecteurs ou de licences supplémentaires.

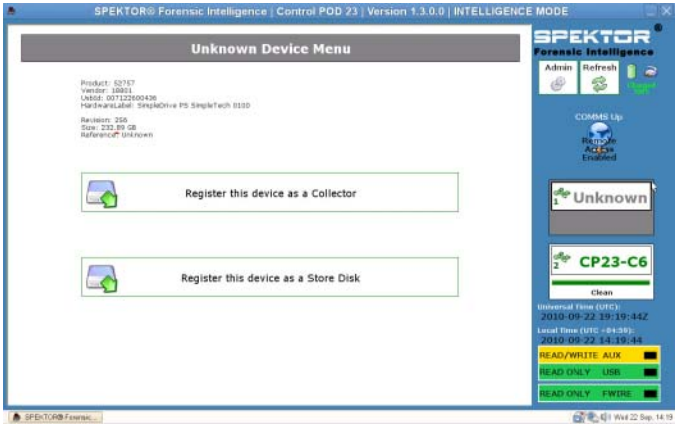
1 Connectez un nouveau collecteur ou disque de stockage à l'un des ports USB sur le côté gauche de l'ordinateur portable renforcée Dell. Le périphérique apparaît comme périphérique non reconnu.

**Figure 2-4. Indicateur d'état Inconnu de collecteur ou de disque de stockage**


2 Tapez ou cliquez sur l'icône d'**indicateur d'état** du collecteur ou du disque de stockage que vous avez connecté. L'icône du périphérique qui a été enregistrée devient verte (pour un collecteur) ou orange (pour un disque de stockage).

3 Le menu **Unknown Device** (Périphérique inconnu) s'affiche.

**Figure 2-5. Menu Unknown Device**




4 Tapez ou cliquez sur **Register this device as a Collector** ou **Register this device as a Store Disk**.

5 Tapez ou cliquez sur **Oui**.

L'indicateur d'état indique le numéro du nouveau collecteur ou disque de stockage et son état devient **Dirty**.

**Figure 2-6. Icônes de collecteur et de disque de stockage sales**


**REMARQUE :** Les collecteurs et les disques de stockage, qu'ils viennent d'être enregistrés ou qu'ils aient été déjà utilisés pour d'autres collectes de données, doivent être nettoyés pour pouvoir être déployés de nouveau par rapport à une cible.

6 *Pour un disque de stockage uniquement*, entrez le numéro de série du disque.

## Nettoyer un collecteur ou un disque de stockage

**REMARQUE :** L'opération prend environ deux heures pour un volume de collecteur de 100 Go.

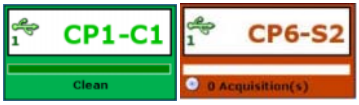
1 Sélectionnez l'**indicateur d'état** du collecteur à nettoyer.

2 Dans le **Collector Menu** tapez ou cliquez sur **Clean Collector**.

3 Tapez ou cliquez sur **Yes** pour confirmer la sélection. Le nettoyage démarre et l'**indicateur d'état** indique l'avancement de l'opération.

A la fin du nettoyage, le logiciel exécute un programme de vérification pour confirmer que le collecteur ne contient que des zéro.

**Figure 2-7. Indicateurs Registered, Clean Collector and Store Disk Status**




**REMARQUE :** Si le nettoyage échoue, l'indicateur d'état indique que le collecteur est sale. Dans ce cas, vous devez relancer le nettoyage. S'il échoue de nouveau, essayez un autre collecteur ou disque de stockage.

## Configurer un profil de collecteur

**REMARQUE :** Par défaut, les paramètres de configuration du logiciel de triage ne permettent de ne collecter aucun fichier. Définissez un sous-groupe de tous les fichiers sur le périphérique cible pour réduire la durée de la collecte et pour ne pas dépasser la capacité du collecteur.

La configuration d'un collecteur permet de déterminer une série de types de fichiers ou de fichiers créés entre des dates données entre lesquelles le collecteur collecte les données d'un périphérique de stockage suspect pour les trier. Plus vous limitez les paramètres de collecte, plus la durée de la collecte des données à vérifier est rapide.

Dell recommande de créer des profils de configuration standard que vous ou votre agent rencontrez fréquemment. Exemple de profils de configuration standard :

- Photo and Vidéos capture les types de fichiers ***.jpg**, ***.png**, ***.swf**, ***.vob** et ***.wmv** qui sont associés aux photographiques, vidéos et autres types de supports visuels.
- Documents collecte les types de fichiers ***.pdf**, ***.doc**, ***.docx**, ***.txt**.
- Audio_Files collecte les fichiers ***.mp3**, ***.mp4**, ***.wav** et d'autres fichiers audio.

#### Configuration d'un collecteur pour l'acquisition

**REMARQUE :** Pour les différences existant entre l'acquisition standard et l'acquisition dynamique, voir « Acquisition standard et acquisition dynamique », page 20.

**REMARQUE :** Lorsqu'un collecteur est configuré pour l'acquisition standard ou dynamique, vous devez le nettoyer pour pouvoir le reconfigurer pour l'utiliser dans l'autre type d'acquisition.

1 Dans le **Collector Menu** tapez ou cliquez sur **Clean Collector**.

**Figure 2-8. Menu Collector**


2 Si vous avez déjà créé un profil de configuration que vous voulez utiliser, sélectionnez le profil et tapez ou cliquez sur **Configure using selected profile** pour lancer la configuration du collecteur. Sinon, tapez ou cliquez sur **New** pour créer un profil.

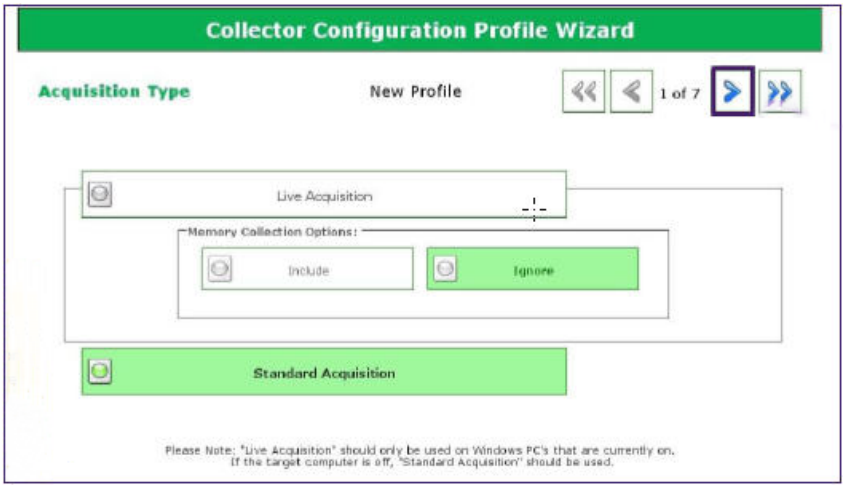
**REMARQUE :** Figure 2-9 montre l'écran **Selected Profile** lorsque vous utilisez le logiciel pour la première fois avant de définir ou d'enregistrer des profils. Lorsque vous commencez à créer des profils de configuration, les profils apparaissent dans cet écran pour les utiliser.

**REMARQUE :** Pour passer d'un écran de configuration de collecteur à un autre, tapez ou cliquez les boutons fléchés gauche et droit situés dans la partie supérieure et sur l'un des côtés de l'écran.

**Figure 2-9. Sélectionner un profil**


**3** Déterminez le type d'acquisition à exécuter, l'acquisition dynamique ou standard (voir « Acquisition standard et acquisition dynamique », page 20 pour plus d'informations sur les différences entre ces deux types d'acquisitions), puis tapez ou cliquez sur **Live Acquisition** ou **Standard Acquisition**.

**Figure 2-10. Etape 1 de la configuration de profil : Type d'acquisition**



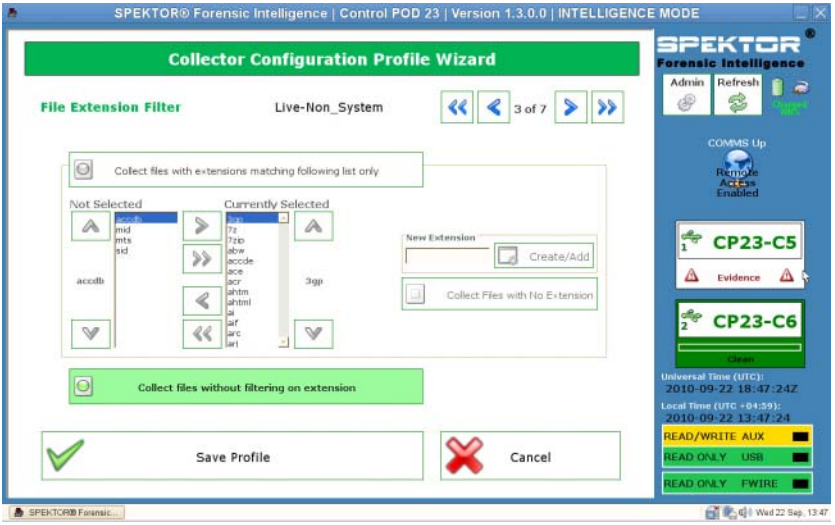

4 Définissez les paramètres d'horodatage du nouveau profil. Plus vous êtes spécifique, plus le traitement des fichiers capturés est rapide.

**Figure 2-11. Etape 2 de configuration de profil : Paramètres d'horodatage des fichiers**

5 Cliquez sur la flèche Droite dans l'angle supérieur droit de l'écran.

6 Dans l'écran **File Extension Filter** sélectionnez les types de fichiers à collecter. Utilisez la flèche Droite pour transférer les types de fichiers sélectionnés et leurs extension de la zone de liste **Not Selected** vers la zone de liste **Currently Selected**.

**Figure 2-12. Etape 3 de la configuration de profil : Filtre d'extensions de fichier**



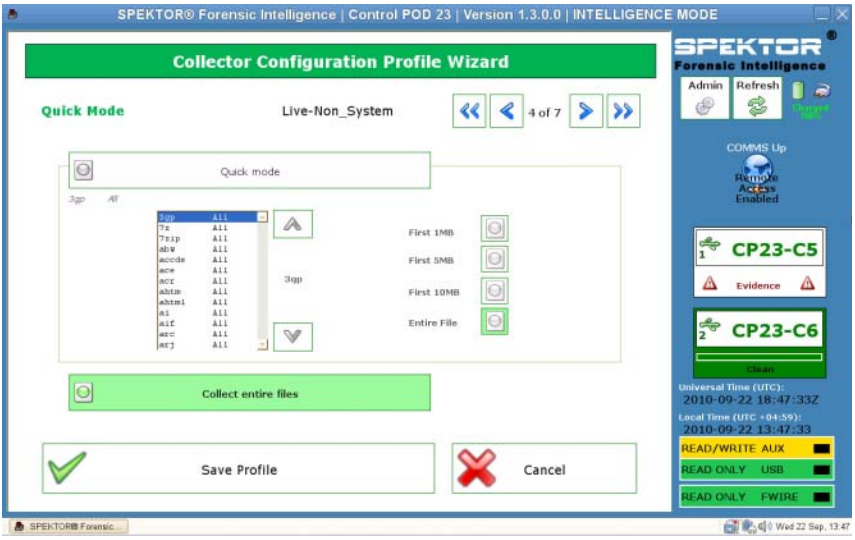

7 Cliquez sur la flèche Droite dans l'angle supérieur droit de l'écran après avoir sélectionné les types de fichiers et les extensions.

**REMARQUE :** Laissez Quick Mode (Mode rapide) désactivé, sauf indication contraire.

8 Dans l'écran **Quick Mode**, sélectionnez le nombre de mégaoctets (**1 Mo**, **5 Mo**, **10 Mo**, ou **Entire File** de la première partie des fichiers à capturer. En collectant uniquement la première partie de fichiers très volumineux (fichiers multimédia, généralement), vous pouvez vérifier un nombre suffisant de fichiers pour déterminer le sujet tout en réduisant le temps de traitement nécessaire.

**REMARQUE :** Si vous n'avez pas sélectionné d'extensions de fichier à l'étape 6, aucun fichier n'est collecté et aucun type de fichier ne s'affiche pour la sélection dans cet écran. Revenez à l'étape 6 et sélectionnez les types de fichiers à activer pour l'étape 8.

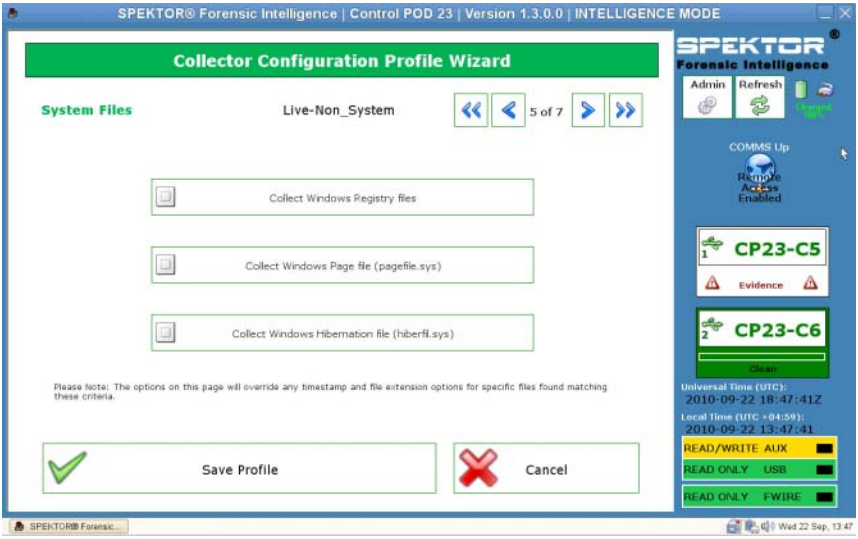
**Figure 2-13. Etape 4 de la configuration de profil : Quick Mode**




9 Cliquez sur la flèche Droite dans l'angle supérieur droit de l'écran.

10 Tapez ou cliquez sur le bouton approprié pour sélectionner les fichiers système à inclure dans la collecte.

**Figure 2-14. Etape 5 de la configuration de profil : fichiers système**




**11** Cliquez sur la flèche Droite dans l'angle supérieur droit de l'écran.

**12** Dans l'écran **Deleted File Filter**, indiquez si vous voulez inclure les fichiers actifs et supprimés, uniquement les fichiers actifs ou uniquement les fichiers supprimés dans la collecte. Si vous ne sélectionnez pas ces options, aucun fichier n'est collecté.

**Figure 2-15. Etape 6 de la configuration de profil : Filtre d'extensions de fichier**


**REMARQUE :** Seuls les fichiers supprimés qui n'ont pas été remplacés sur le périphérique cible sont collectés. Les fichiers supprimés et remplacés sont endommagés ou inextractibles.

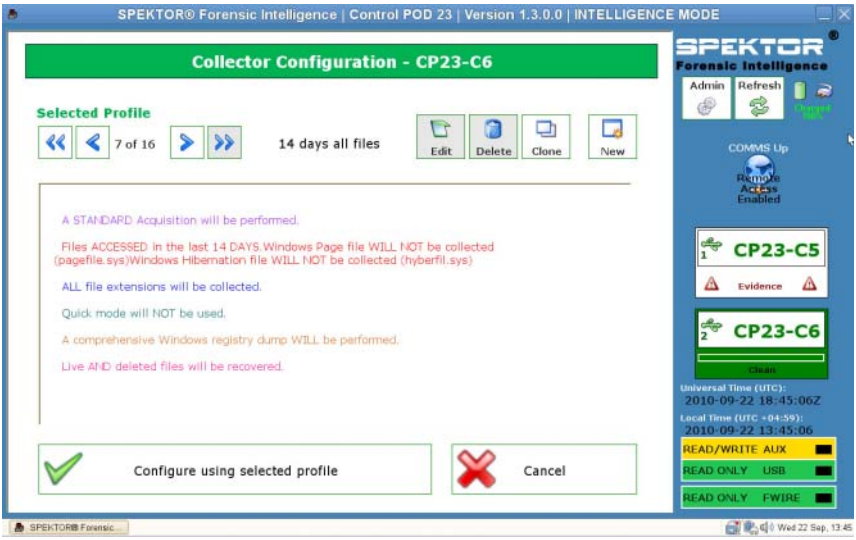
**13** Cliquez sur la flèche Droite dans l'angle supérieur droit de l'écran.

**14** Dans l'écran **Profile Name**, entrez le nom du profil, puis tapez ou cliquez sur **Save Profile**.

**Figure 2-16. Etape 7 de la configuration de profil : Nom du profil**

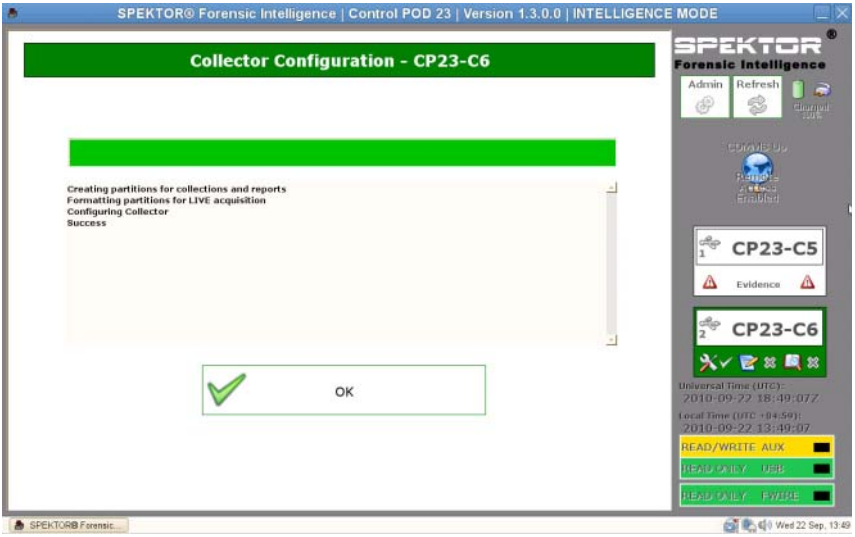

**15** Cliquez sur la flèche Droite dans l'angle supérieur droit de l'écran. Le nouveau profil apparaît dans l'écran **Selected Profile**. L'écran **Collector Configuration** affiche le nom du profil (**14 days all files** (14 jours tous les fichiers, en l'occurrence) et les informations du profil dans la partie principale de l'écran.

**Figure 2-17. Profil sélectionné après la création du profil**




**16** Tapez ou cliquez sur **Configure using selected profile** pour lancer la configuration du collecteur.

**Figure 2-18. Profil sélectionné après la création du profil**




17 Tapez ou cliquez sur **OK** pour configurer le collecteur. L'opération prend une ou deux minutes uniquement.

Une fois le collecteur configuré, vous pouvez le déployer par rapport à un ordinateur cible ou un périphérique de stockage cible. Voir « Déployer les outils de triage », page 34.

18 Cliquez sur la flèche Droite dans l'angle supérieur droit de l'écran.

## Déployer les outils de triage

**REMARQUE :** Pour les différences existant entre l'acquisition dynamique et l'acquisition standard, voir « Acquisition standard et acquisition dynamique », page 20.

**REMARQUE :** Bien que vous puissiez utiliser un collecteur pour plusieurs affaires, il est vivement recommandé que chaque collecteur contienne uniquement les données d'une seule affaire, même si les données de plusieurs périphériques de stockage de l'affaire peuvent être stockés dans le collecteur.

**Déployer un collecteur pour l'acquisition standard par rapport à un ordinateur cible**

**AVERTISSEMENT : Vous devez modifier la séquence de démarrage du système dans le BIOS du système de l'ordinateur cible pour pouvoir exécuter une acquisition standard. Si l'ordinateur cible est configuré pour démarrer depuis son disque dur et non pas le lecteur optique avec le disque de démarrage SPEKTOR, le contenu du disque de l'ordinateur cible sera altéré. Vérifiez que vous savez accéder au BIOS du système de l'ordinateur cible avant de mettre l'ordinateur cible sous tension.**

**AVERTISSEMENT : Avant de mettre l'ordinateur cible sous tension, veillez à placer le disque de démarrage SPEKTOR dans le lecteur optique depuis lequel l'ordinateur doit démarrer. Si vous démarrez l'ordinateur sans le disque de démarrage, vous altérez le contenu de l'unité de l'ordinateur.**

**REMARQUE :** Vous devez disposer d'un disque de démarrage SPEKTOR pour pouvoir déployer l'acquisition standard acquisition par rapport à un ordinateur cible. Voir « Graver un CD pour les procédures d'acquisition standard », page 21 pour plus d'informations sur la création d'un disque de démarrage.

1. Sur l'ordinateur portable renforcé Dell, tapez ou cliquez sur **Deploy Collector.**
2. Sélectionnez **Target Computer.**
3. Cliquez sur **OK** et débranchez le collecteur de l'ordinateur portable renforcé Dell.
4. Connectez le collecteur à un port USB sur l'ordinateur cible.

**REMARQUE :** Dell recommande de toujours utiliser le lecteur optique interne de l'ordinateur cible avec le disque de démarrage. Si ce n'est pas possible, utilisez un lecteur optique externe avec un connecteur USB.

5. Placez le disque de démarrage SPEKTOR dans le lecteur optique.
6. Accédez au BIO du système de l'ordinateur cible et changez l'ordre de démarrage pour que l'ordinateur démarre depuis le lecteur optique.

   Le disque de démarrage SPEKTOR se charge et l'interface du disque de démarrage s'affiche.
7. Entrez les informations demandée en appuyant sur <Entrée> ou les touches fléchées pour passer d'un champ à l'autre, puis accédez au champ **COLLECT** et appuyez sur <Entrée> pour lancer la collecte des données.

**PRÉCAUTION : Ne retirez pas le disque de démarrage SPEKTOR du lecteur optique tant que l'ordinateur cible ne s'est pas arrêté complètement.**

8. A la fin de la collecte, appuyez sur <Entrée> pour arrêter l'ordinateur.

9 Retirez le disque de démarrage SPEKTOR du lecteur optique, débranchez le collecteur du port USB de l'ordinateur cible et branchez-le dans un port USB de l'ordinateur portable renforcé Dell.

### Déployer un collecteur pour l'acquisition standard par rapport à un ordinateur cible

1 Connectez le périphérique de stockage cible au port USB en lecture seul ou au port Firewire de l'ordinateur portable renforcé Dell.

2 Tapez ou cliquez sur **Deploy Collector**.

3 Tapez ou cliquez sur **Target Storage Device**, entrez les informations demandées, puis tapez ou cliquez sur **Collect from Device**.

4 A la fin de la collecte, débranchez le périphérique de stockage cible du port USB et tapez ou cliquez sur **OK**.

### Déployer un collecteur pour l'acquisition dynamique

**REMARQUE :** Veillez à conserver des notes précises et détaillées au cours de cette procédure comme meilleures pratiques de chaîne de conservation.

**REMARQUE :** Vous n'avez pas besoin du disque démarrage SPEKTOR pour exécuter un déploiement d'acquisition dynamique.

1 Cliquez sur **Deploy Collector→ Target Computer**.

2 Sur le périphérique cible, accédez à **Poste de travail** (**Ordinateur** sur les ordinateurs qui fonctionnent sous Windows Vista ou Windows 7).

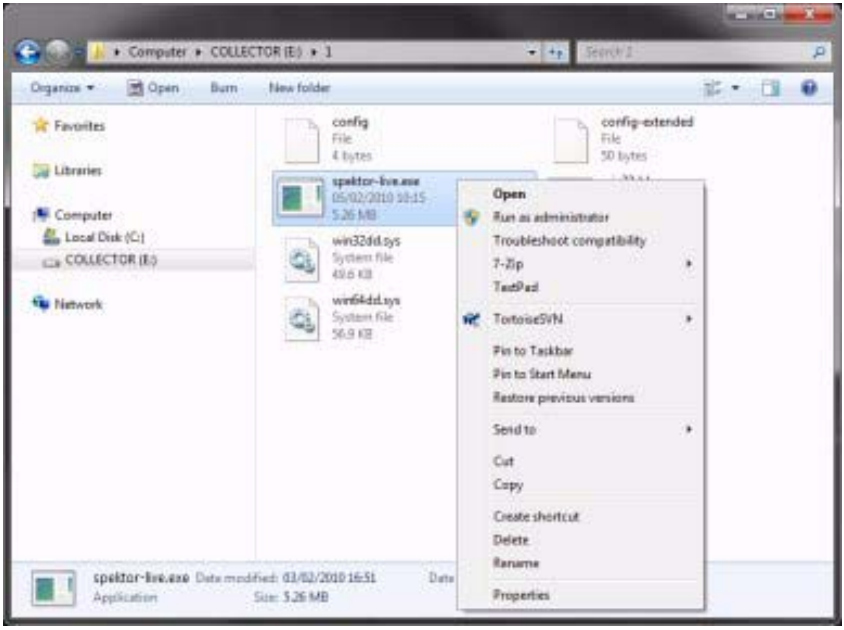
3 Cliquez deux fois sur l'icône **Collector** qui apparaît pour afficher le contenu du collecteur.

**Figure 2-19. Icône Collector**


4 Cliquez sur le dossier portant le numéro le plus élevé. Un seul dossier apparaît s'il s'agit du premier déploiement depuis le nettoyage du collecteur.

5 Cliquez avec le bouton droit de la souris sur **spektor-live.exe**, puis sélectionnez **Exécuter comme administrateur** dans la zone de liste déroulante. Si un message demande votre autorisation pour exécuter l'application comme administrateur, cliquez sur **Continue** (Continuer).

**Figure 2-20. Exécuter comme administrateur**




6 Entrez les informations demandées dans l'écran **SPEKTOR Live Collection**, puis cliquez sur **Run**.

7 Cliquez sur **Close** lorsqu'un message vous le demande.

8 Déconnectez le collecteur du périphérique cible et stockez-le dans un endroit sûr pour le placer plus tard dans le centre de données.

## Vérification des fichiers collectés après le triage

1 Dans le **Collector Menu**, cliquez sur **Reporting**. Cette option indexe les données collectées et crée un groupe de rapports automatiquement.

2 Dans l'écran **Collector Collections**, sélectionnez un **rapport principal**, puis cliquez sur **Generate Selected Reports**.

**Figure 2-21. Générer des rapports**

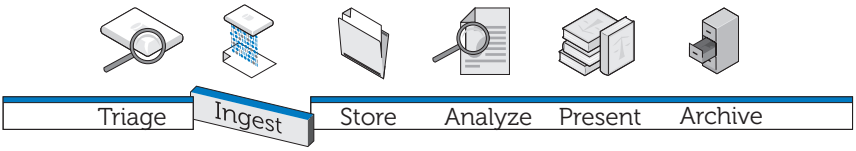

3 Cliquez sur **OK** à la fin de la génération des rapports pour revenir au menu **Reporting**.

**REMARQUE :** Voir le *manuel d'utilisation* SPEKTOR pour plus d'informations sur la création et l'exportation de rapports en utilisant des critères. Voir *« Documentation et ressources associées », page 15*.

4 Cliquez sur **View Collection Report** pour consulter les rapports, puis cliquez sur l'une des cinq catégories de rapports **Images**, **Documents**, **Multimedia**, **Other** ou **System** pour afficher des rapports.

# 3

# Incorporation




La phase d'incorporation de la solution Dell Digital consiste à créer une image du périphérique de stockage cible (si cela n'a pas été fait lors du triage), puis à transférer l'image vers un emplacement central accessible pour y être analysée Pour transférer les applications d'investigation informatique vers le centre de données tout en continuant de préserver l'environnement de l'ordinateur, Dell, en partenariat avec Citrix, a créé des progiciels distincts pour les principales applications d'investigation pour les transférer de manière transparente vers le centre de données, en créant un environnement utilisateur plus disponible et plus rapide.

Dans le cadre de la solution Digital Forensics, Dell a certifié les applications d'investigation informatique suivantes :

- SPEKTOR
- EnCase 6
- FTK 1.8
- Version standard FTK 3
- FTK 3 Lab

Vous pouvez utiliser n'importe quelle combinaison de ces applications pour y accéder simultanément depuis un seul périphérique utilisateur.

## EnCase 6 de centre de données

Dans l'exemple de solution suivant, l'application EnCase 6 est hébergée sur un ou plusieurs périphériques de serveur Dell dans le centre de données pour fournir des sessions EnCase 6 multi-utilisateurs.

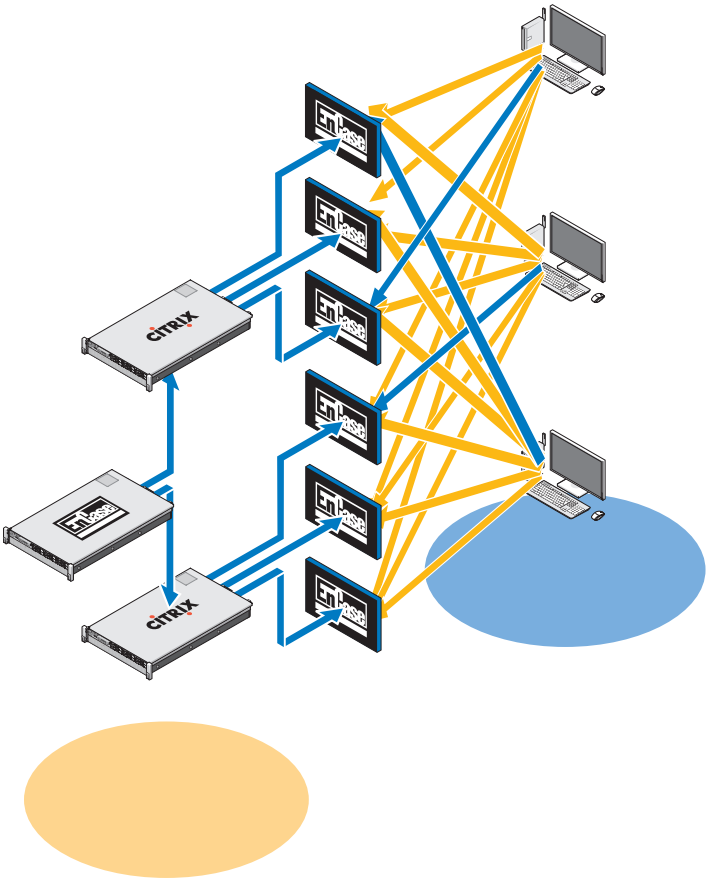
### Solution à un seul serveur

Dans la solution EnCase 6 à un seul serveur, plusieurs clients peuvent se connecter à un serveur. Tous les clients pointent vers ce serveur et ne peuvent pas se connecter à un autre serveur EnCase 6. En cas de défaillance du serveur, toutes les connexions client sont perdues.

### Solution multiserveur (haut disponibilité)

Dans la solution multiserveur, l'utilisateur se connecte à l'application EnCase 6 de la batterie Citrix et il est dirigé de manière transparente vers le serveur EnCase 6 ayant la charge de travail la plus faible. Si l'utilisateur exécute plusieurs instanciations du logiciel EnCase 6, chaque instanciation peut être créée par un serveur différent. L'environnement utilisateur est préservé, car l'utilisateur ne sait pas du tout comment les instances sont créées et toutes les sessions semblent s'exécuter sur le même serveur avec la même interface.

**Figure 3-1. Schéma Client/Serveur EnCase 6 de centre de données**




En cas de défaillance d'un serveur, l'utilisateur doit cliquer de nouveau sur l'icône de l'application EnCase sur le bureau et le système dirige la connexion utilisateur vers le serveur disponible suivant qui héberge EnCase 6. Chaque serveur EnCase peut prendre en charge *x* sessions utilisateur, où *x* = *(nombre de coeurs x 2)*. Chaque session utilisateur nécessite 3 Go de RAM sur le serveur.

# FTK 1.8 de centre de données

Dans la solution FTK 1.8 de centre de données, l'application FTK 1.8 est hébergée sur un ou plusieurs périphériques de serveur Dell dans le centre de données pour fournir des sessions FTK 1.8 multi-utilisateurs (une session utilisateur unique par serveur).

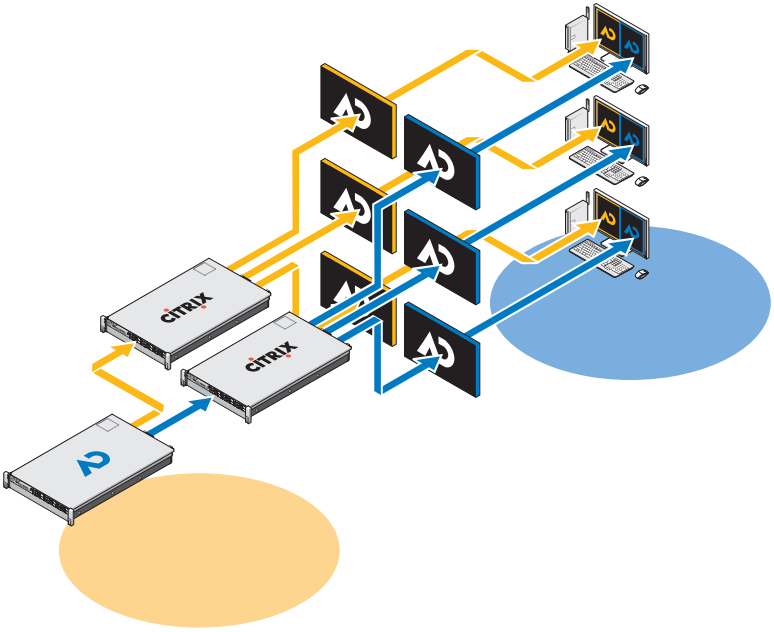
### Session FTK 1.8 par ordinateur de bureau

Dans la solution FTK 1.8 monoserveur, plusieurs clients peuvent se connecter à un seul serveur. Tous les clients pointent vers ce serveur et ne peuvent pas se connecter à un autre serveur FTK 1.8. En cas de défaillance du serveur, toutes les connexions client sont perdues. L'utilisateur peut exécuter une seule session FTK 1.8 par compte utilisateur Windows.

### Plusieurs sessions FTK 1.8 par ordinateur de bureau

Dan la solution FTK 1.8 multiserveur, l'utilisateur se connecte aux serveurs FTK 1.8 en utilisant plusieurs icônes de bureau, FTK Server1, FTK Server2, etc. Chaque liaison est associée à un serveur donné. La Figure 3-2montre la bordure colorée de la session de serveur FTK 1.8 active sur le serveur exécutant la session FTK 1.8 (serveur 1 = bleu, serveur2 = rouge). Deux sessions de l'application FTK 1.8 ne peuvent pas s'exécuter depuis le même serveur en utilisant le même compte utilisateur. L'environnement utilisateur de l'application serveur FTK 1.8 est identique sur tous les clients.

**Figure 3-2. Schéma multiclient et multiserveur FTK 1.8**




En cas de défaillance d'un serveur, l'utilisateur perd l'accès à la session de serveur correspondante FTK 1.8. Dans ce cas, il doit utiliser les autres serveurs FTK. Toutes les informations d'affaire et de preuve (en supposant que l'utilisateur dispose de privilèges NAS) sont disponibles depuis toutes les sessions serveur FTK 1.8 via le NAS/SAN partagé.

Chaque serveur FTK 1.8 peut prendre en charge *x* sessions utilisateur, où *x* = *(nombre de coeurs x 2)*. Chaque session utilisateur nécessite 3 GO de RAM de serveur et 1 000 E/S par seconde pour le disque du centre de données.

## FTK 3 de centre de données

Dans la solution FTK 3 de centre de données, l'application est hébergée sur un ou plusieurs périphériques de serveur Dell dans le centre de données pour fournir une seule session d'application FTK 3 par serveur.

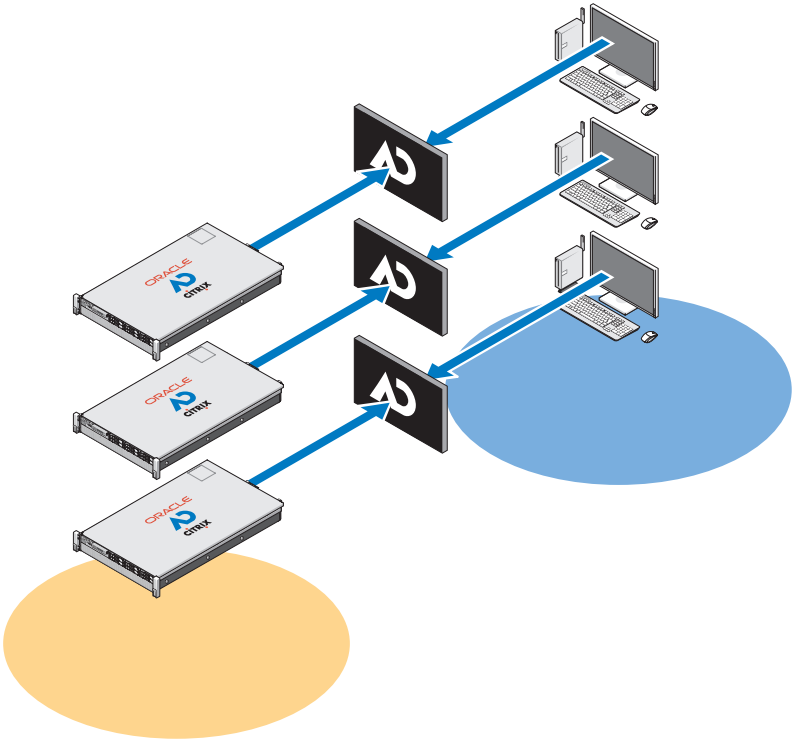
### Solution monoserveur FTK 3

Dans la solution FTK 3 monoserveur, un seul client FTK 3 peut se connecter à un seul serveur. Tous les clients pointent vers ce serveur et ne peuvent pas se connecter à un autre serveur FTK 3. En cas de défaillance du serveur, toutes les connexions client sont perdues. Le serveur FTK 3 exécute également la base de données Oracle intégrée FTK, car cette version de la base de données ne prend pas en charge la collaboration entre les autres bases de données Oracle FTK ou d'autres utilisateurs FTK.

### Solution multiserveur (pas de haute disponibilité)

Dans la solution multiserveur, chaque client se connecte à son serveur de base FTK 3 et ne peut pas se connecter à aucun autre serveur FTK 3. Lorsqu'une session FTK 3 est active sur un serveur, le serveur n'est plus disponible pour accepter de nouvelles sessions client FTK 3 ; le programme de configuration de l'infrastructure d'investigation informatique Dell empêche un serveur d'exécuter plusieurs sessions de l'application FTK 3 simultanément. En autorisant une seule session active par serveur, l'application FTK 3 à unités d'exécution multiples alloue toutes les ressources serveur au traitement d'une affaire pour améliorer les performances.

**Figure 3-3. Schéma Client/Serveur FTK 3 de centre de données**




Avec l'édition FTK standard, chaque serveur doit exécuter une version locale de la base de données Oracle intégrée FTK (une version de la base de données Oracle par utilisateur simultané). Cette version de l'application FTK et de la base de données Oracle ne permet pas la collaboration entre les utilisateurs FTK et les autres bases de données Oracle FTK.

Chaque base de données dispose d'un agent de sauvegarde Oracle sur le serveur et la base de données est sauvegardée lors des sauvegardes normales (voir « Archivage », page 87 pour plus d'informations).

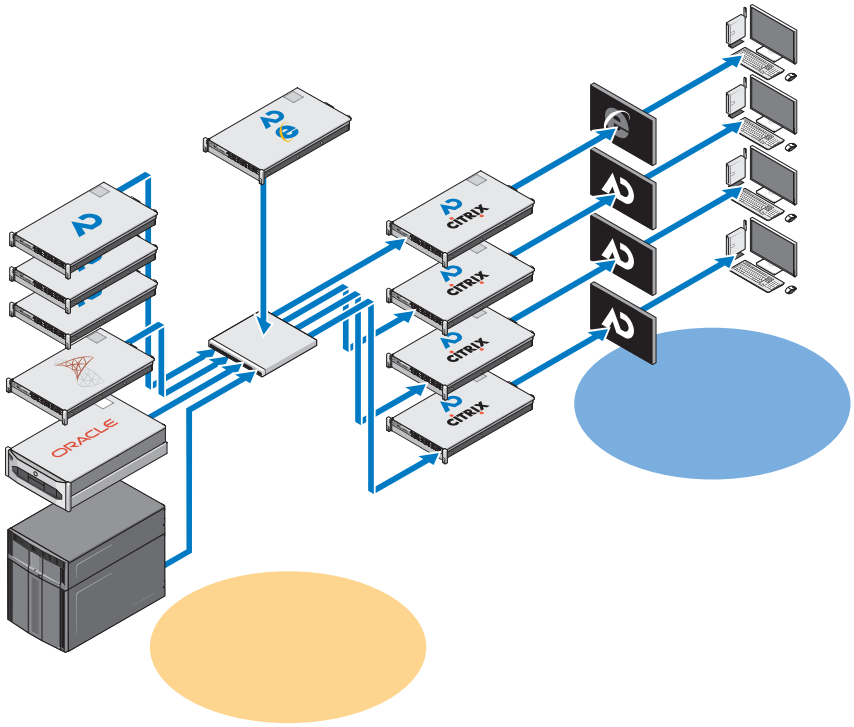
En cas de défaillance d'un serveur, l'utilisateur doit se connecter manuellement à un autre serveur FTK 3 disponible (si n+1 FTK 3 serveurs sont disponibles). Toutefois, en cas de défaillance simultanée de la base de données Oracle, aucun accès n'est disponible aux affaires préexistantes déjà traitées, car elles sont liées spécifiquement à la base de données Oracle FTK 3 d'origine de l'utilisateur.

Chaque serveur FTK 3 peut prendre en charge une seule session utilisateur simultanée. Chaque session utilisateur nécessite 64 Go de RAM de serveur (48 Go pour Oracle et 16 Go pour FTK) et plus de 1 000 E/S par seconde pour le magasin de fichiers et plus 600 E/S par seconde pour la base de données (configuration minimale).

## FTK 3 Lab Edition

Dans la configuration FTK 3 Lab Edition, l'utilisateur se connecte à un serveur qui héberge AccessData Lab et la base de données centralisée des affaires. Plusieurs utilisateurs peuvent se connecter simultanément à la même affaire et exécuter différentes analyses au même moment. Le traitement est géré en utilisant le modèle de traitement distribué.

**Figure 3-4. Schéma Client/Serveur FTK 3 Lab Edition**




Le stockage des affaires est optimisé en combinant du matériel SAS et SATA et l'ensemble du centre de données d'investigation informatique peut être géré centralement par un gestionnaire d'administration.

## Plusieurs applications d'investigation informatique sur seul ordinateur de bureau

Dans la solution multifournisseur ou multiapplication, toutes les solutions d'application individuelle décrites précédemment sont combinées pour permettre à l'enquêteur informatique d'accéder à toutes les applications d'investigation informatique (EnCase 6, FTK 1.8 et FTK 3 ou FTK 3 Lab edition) depuis un seul ordinateur de bureau. Toutes les applications peuvent être fournies en mode haute disponibilité pour que, en cas de défaillance, l'utilisateur puisse toujours accéder à l'application et dans le cas de FTK 1.8, en utilisant l'une des autres icônes FTK 1.8 sur l'ordinateur de bureau.

# Recommandations de configuration réseau

**Table 3-1. Structure d'adresse IP recommandée**

| Adresse IP | Fonction serveur | Nom du serveur |
|---|---|---|
| 192.168.1.1 | Contrôleur de domaine 1 | DF-DC1 |
| 192.168.1,2 | Contrôleur de domaine 2 | DF-DC2 |
| 192.168.1.3 | Serveur de preuve | DF-Evidence |
| 192.168.1.4 | Serveur d'espace de travail | DF-Workspace |
| 192.168.1.5 | FTK Oracle Server | DF-FTK |
| 10.1.0.0/24 | Plage d'adresses IP statiques 1 Go | |
| 10.1.1.0/24 | Plage d'adresses IP statiques 10 Go | |
| 10.1.2.0/24 | Plage DHCP 1 Go, clients | |
| 10.1.0.250-254 | Commutateur(s) 1 Go | |
| 10.1.1.250-254 | Commutateur(s) 10 Go | |
| 10.1.0.200 | Serveur DNS | |

**Table 3-2. Conventions d'appellation recommandées pour les serveurs de la solution**

| Nom | Abréviation |
|---|---|
| Nom de domaine | DF (Digital Forensics) |
| Contrôleur de domaine 1 | DF-DC1 |
| Contrôleur de domaine 2 | DF-DC2 |
| Stockage de preuve | DF-Evidence |
| Espace de travail | DF-Workspace |
| Oracle | DF-Oracle |
| SQL | DF-SQL |
| FTK-Lab | FTK-Lab |
| FTK-Standalone | FTK |
| Gestionnaire(s) de traitement distribué | DF-DPM, DF-DPM1, DF-DPM2 |
| Moteur(s) de traitement distribué | DF-DPE, DF-DPE1, DF-DPE2 |

**Table 3-3. Conventions d'appellation recommandées pour l'association de cartes réseau**

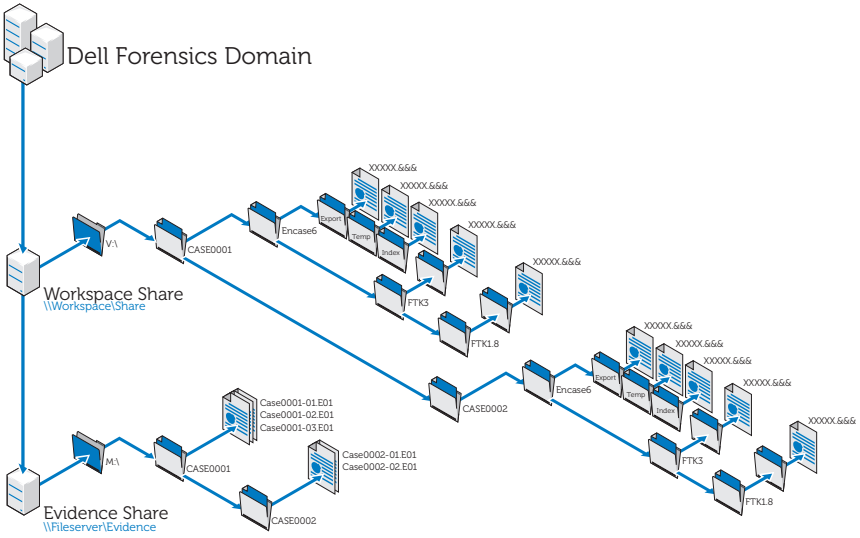
| | | |
|---|---|---|
| Association de cartes réseau 1 | Réseau public | Pour les serveurs interconnectés |
| Association de cartes réseau 2 | iSCSI | Pour les serveurs connectés à des périphériques de stockage EqualLogic |

**Table 3-4. Structure d'association de lettres d'unité**

| Nom d'appel | Unité | Local ou SAN | RAID | Notes |
|---|---|---|---|---|
| Unité locale | C: | Local | RAID1 (2 disques 15 k SAS) | |
| | D: | Local | | |
| CD-ROM | E: | | | |
| | F: | | | |
| | G: | | | |
| SQL | H: | SAN | RAID0+1 | Ne doivent pas être des disques SATA |
| Oracle | I: | SAN | RAID0+1 | Ne doivent pas être des disques SATA |
| Unité EV Vault | J: | SAN | RAID50 | |
| Sauvegarde sur disque | K: | SAN | RAID50 | |
| Secours | L: | SAN | RAID50 | |
| Preuve 1 | M: | SAN | RAID50 | |
| Preuve 2 | N: | SAN | RAID50 | |
| Preuve 3 | O: | SAN | RAID50 | |
| Preuve 4 | P: | SAN | RAID50 | |
| Preuve 5 | Q: | SAN | RAID50 | |
| Preuve 6 | R: | SAN | RAID50 | |
| Preuve 7 | S: | SAN | RAID50 | |

| Nom d'appel | Unité | Local ou SAN | RAID | Notes |
|---|---|---|---|---|
| Preuve 8 | T: | SAN | RAID50 | |
| Preuve 9 | U: | SAN | RAID50 | |
| Espace de travail 1 | V: | SAN | RAID50 | |
| Espace de travail 2 | W: | SAN | RAID50 | |
| Espace de travail 3 | X: | SAN | RAID50 | |
| Espace de travail 4 | Y: | SAN | RAID50 | |
| Espace de travail 5 | Z: | SAN | RAID50 | |

**Figure 3-5. Structure de fichier recommandée**



# Exécution de l'incorporation en utilisant la solution Dell Digital Forensics

## Incorporation en utilisant SPEKTOR

### Enregistrer et nettoyer un périphérique USB externe comme disque de stockage

1. Connectez le périphérique USB externe non enregistré à un port Collector sur l'ordinateur portable renforcé.
2. Cliquez ou tapez sur l'cône de périphérique lorsqu'elle apparaît, puis sur **Register the Device as a Store Disk→ Yes**. Entrez les informations demandées.
3. Dans le menu contextuel accessible en cliquant avec le bouton droit de la souris, sélectionnez le périphérique enregistré, puis tapez ou cliquez sur **Clean/Reformat→ Clean.**
4. Cliquez sur **OK** à la fin de l'opération.

### Déployer le disque de stockage

1. Connectez le disque de magasin à l'ordinateur renforcé, puis tapez ou cliquez sur le disque pour afficher le **Store Disk Menu**.
2. Dans le **Store Disk Menu**, tapez ou cliquez sur **Deploy**.

   *Si vous effectuez le déploiement par rapport à un ordinateur cible :*

   a. Tapez ou cliquez sur **Target Computer**.

   b. Retirez le disque de stockage de l'ordinateur portable renforcé et connectez-le à un port USB sur l'ordinateur cible.

   c. Suivez les mêmes instructions de déploiement que celles utilisées pour capturer une image de triage dans « Déployer les outils de triage », page 34.

   d. Lorsque le CD de démarrage est chargé, l'assistant **SPEKTOR Imaging** (Image SPECKTOR) vous aide à exécuter le reste du processus de création d'image. Les instructions détaillées se trouvent dans le *manuel d'utilisation de SPEKTOR*. Voir « Documentation et ressources associées », page 15 pour plus d'informations

   e. Arrêtez l'ordinateur cible, débranchez le disque de stockage et replacez-le dans le centre de données pour le stockage.

*Si vous effectuez le déploiement par rapport à un périphérique de stockage cible locament :*

**a** Tapez ou cliquez sur **Target Storage Device**.

**b** Connectez le périphérique de stockage cible au port USB en lecture seule ou FireWire sur le côté droit de l'ordinateur portable renforcé.

**c** Sélectionnez le périphérique ou la partition pour laquelle vous voulez créer une image, puis cliquez sur la flèche dans l'angle supérieur droit.

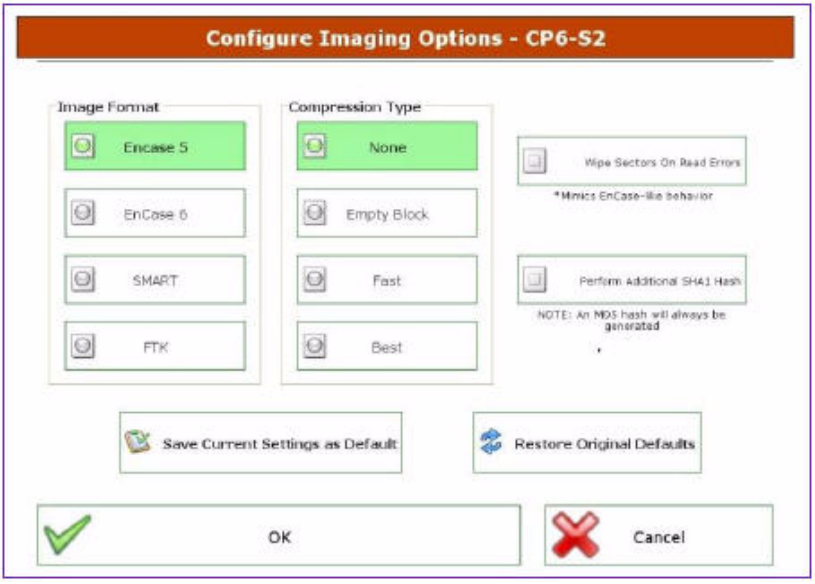
**d** Entrez les informations d'affaire demandées, puis tapez ou cliquez sur **Image Now**.

**e** Si nécessaire, tapez ou cliquez sur **Configure Imaging Options** pour changer le **format d'image** ou le **type de compression** ou pour **nettoyer les secteurs en cas d'erreurs de lecture** ou **exécuter un hachage SHA1 supplémentaire**.

**REMARQUE :** Un hachage MDS est toujours généré au cours du traitement d'une image.

**REMARQUE :** Voir le *manuel d'utilisation SPEKTOR* pour plus d'informations sur chacune de ces options d'image. Voir « Documentation et ressources associées », page 15.

**Figure 3-6. Définir les options d'image**




**f** Tapez ou cliquez sur **Image Now**→ **Yes** pour créer une image.

**g** A la fin de l'opération, tapez ou cliquez sur **OK**.

**h** Débranchez le périphérique de stockage cible et le disque de stockage de l'ordinateur portable renforcé, puis remplacez le disque de stockage dans le centre de données pour le stockage et l'analyse.

**REMARQUE :** Le transfert d'une image peut durer longtemps ; 6 heures pour un disque dur de 60 Go standard n'est pas inhabituel.

### Incorporation en utilisant EnCase

Dans la solution Dell Digital Forensics, l'obtention d'une licence EnCase est réalisée en utilisant un système d'affectation de licence réseau. Généralement, une instance de EnCase SAFE est installée sur l'un des serveurs du centre de données et une clé (dongle) contenant plusieurs licences utilisateur est connectée au serveur. Les clients EnCase sont configurés pour rechercher une licence sur ce serveur et aucune clé n'est nécessaire. Voir le *Guide d'installation et de configuration de Dell Digital Forensics* pour plus d'informations. Voir « Documentation et ressources associées », page 15. En outre, contactez l'administrateur des systèmes réseau pour plus d'informations sur l'installation de la solution de votre agence.

1. Connectez le périphérique de stockage cible au poste de travail d'incorporation approprié dans le centre de données.
   a. Si vous créez l'image d'un périphérique SATA, voir « Connexion du bloqueur Tableau à un disque dur SATA », page 56 pour plus d'informations.
   b. Si vous créez l'image d'un périphérique IDE, voir « Connexion du bloqueur Tableau à un disque dur IDE », page 57 pour plus d'informations.
2. Créez une affaire.

**REMARQUE :** Les instructions suivantes portent sur le réseau et la structure de dossier décrite comme meilleure pratique proposée par Dell pour sa solution Digital Forensics Solution. Voir Figure 3-5pour plus d'informations.

   a. Cliquez sur **New**, puis entrez les informations demandées.
   b. Sur **l'unité W:** (zone de travail), créez les dossiers en utilisant la structure suivante :
      - `W:\[CaseName]\EnCase6\Export`
      - `W:\[CaseName]\EnCase6\Temp`
      - `W:\[CaseName]\EnCase6\Index`
   c. Cliquez sur **Finish.**
   d. Cliquez sur **Yes** pour chaque demande de création d'un dossier.
   e. Dans l'écran **EnCase Acquisition**, cliquez sur l'option de menu **Add Device**.
   f. Cochez la case **Sessions**.

g Dans le volet de droitre, sélectionnez l'affaire.

h Cliquez sur **Add Evidence Files**, puis accédez au référentiel E01 (en utilisant la configuration de meilleure pratique décrite dans Figure 3-5, ce référentiel doit être stocké sur l'unité **X:**\).

i Cliquez sur **Next**→ **Next**→ **Finish**. Une icône de chronomètre apparaît dans la partie inférieure droite de l'écran EnCase **Acquisition** et EnCase va vérifier le fichier E01. La vérification peut durer un certain temps en fonction de la taille du fichier.

3 Dans le logiciel EnCase, ajoutez le périphérique de stockage cible en utilisant l'assistant **Add Device**.

4 Obtenez le contenu du périphérique.

a Depuis le logiciel EnCase, cliquez sur **Cases**→ **Entries**→ **Home**, puis cliquez avec le bouton droit de la souris sur le périphérique dont vous voulez obtenir le contenu.

b Sélectionnez **Acquire** dans le menu déroulant.

c Dans la boîte de dialogue **After Acquisition**, sélectionnez le type du **fichier de la nouvelle image** :

- **N'ajoutez pas** les options qui excluent la nouvelle image acquise de l'affaire ouverte.
- **Add to Case** ajoute la nouvelle image acquise dans le fichier d'affaire associé au périphérique sur lequel l'image a été prise.
- **Replace a source device** ajoute la nouvelle image acquise à l'affaire et supprime le périphérique prévisualisé où a été exécuté l'acquisition.

d Cliquez sur **Finish**. A la fin de la création d'image, la boîte de dialogue **Acquisition Results** s'affiche.

### Utilisation des bloqueurs d'écriture de Tableau

**PRÉCAUTION : Ne retirez pas un disque dur un point d'investigation informatique sous tension.**

**PRÉCAUTION : N'utilisez pas de rallonge USB avec un pont d'investigation informatique.**

***Connexion du bloqueur Tableau à un disque dur SATA***

1. Placez le **DC IN B** du pont T35es Forensic SATA/IDE sur la position **B On**.
2. Connectez la source d'alimentation TP2 ou TP3 sur le côté gauche du pont SATA T35es en utilisant le connecteur Mini-DIN à 5 broches.
3. Connectez le cordon d'alimentation à la source d'alimentation TP2 et au connecteur électrique.
4. Mettez sous tension le pont pour vérifier que le voyant de bloc blanc s'allume. Mettez sous tension le pont avant de connecter le périphérique de stockage cible.
5. Connectez le connecteur Molex femelle du câble d'alimentation TC5-8 SATA à l'emplacement **DC OUT** situé sur le côté droit du pont T35es SATA/IDE.
6. Connectez le connecteur d'alimentation SATA du câble d'alimentation TC5-8 SATA au connecteur d'alimentation SATA du disque dur cible.

**PRÉCAUTION : L'utilisation de connexions électriques Molex et SATA lors de la connexion d'un périphérique de stockage cible surcharge le périphérique cible.**

7. Connectez le câble d'interface TC3-8 SATA au pont T35es SATA/IDE.
8. Connectez l'autre extrémité du câble d'interface TC3-8 SATA au périphérique de stockage cible.
9. Connectez l'une des extrémités du câble de données (USB 2,0, deux connexions Fire Wire 800 ou FireWire 400 4 broches Orion) à l'un des ports sur le côté gauche du pont T35es SATA/IDE.
10. Connectez l'autre extrémité du câble de données à un port de l'ordinateur portable renforcé Dell ou du poste de travail Dell OptiPlex.
11. Placez le commutateur sur la partie supérieure du pont T35es SATA/IDE sur la position **A ON**. L'ordinateur portable renforcé Dell ou le poste de travail Dell OptiPlex doit maintenant enregistrer la présence du périphérique de stockage cible.

***Connexion du bloqueur Tableau à un disque dur IDE***

1. Placez le **DC IN B** du pont T35es Forensic SATA/IDE sur la position **B On**.
2. Connectez la source d'alimentation TP2 ou TP3 sur le côté gauche du pont SATA/IDE T35es en utilisant le connecteur Mini-DIN à 5 broches.

**REMARQUE :** Le connecteur DIN à 7 broches sur l'alimentation électrique TP3 ne fonctionnera pas avec les ponts Tableau. Vous devez utiliser le câble adaptateur TCA-P7-P5 7 DIN 7 broches-DIN 5 broches pour connecter l'alimentation électrique TP3 aux ponts Tableau.

3. Connectez le cordon d'alimentation à la source d'alimentation TP2 et au connecteur électrique.
4. Mettez sous tension le pont pour vérifier que le voyant de **bloc blanc** est **allumé**, puis mettez le pont **hors tension** avant de connectez le disque dur cible.
5. Connectez le connecteur Molex femelle du câble d'alimentation TC2-8 SATA à l'emplacement DC OUT situé sur le côté droit du pont T35es SATA/IDE.
6. Connectez l'autre connecteur Molex femelle du câble d'alimentation TC2-8 Molex au connecteur Molex du disque dur suspect.
7. Connectez l'extrémité bleue du câble d'interface TC6-8 IDE (pour aligner la broche 1) au pont T35es SATA/IDE.
8. Connectez l'autre extrémité du câble d'interface TC6-8 IDE au périphérique de stockage cible.
9. Connectez l'une des extrémités du câble de données (USB 2,0, deux connexions Fire Wire 800 ou FireWire 400 4 broches Orion) à l'un des ports sur le côté gauche du pont T35es SATA/IDE.
10. Connectez l'autre extrémité du câble de données à un port de l'ordinateur portable renforcé Dell ou du poste de travail Dell OptiPlex.
11. Placez le commutateur sur la partie supérieure du pont T35es SATA/IDE sur la position **A ON**. L'ordinateur portable renforcé Dell ou le poste de travail Dell OptiPlex doit maintenant enregistrer la présence du périphérique de stockage cible.

## Incorporer en utilisant FTK 1.8 et 3.0 de centre de données

Dans la solution Dell Digital Forensics, l'obtention d'une licence FTK est réalisée en utilisant un système d'affectation de licence réseau. Généralement, le serveur de licences réseau FTK est installé sur l'un des serveurs du centre de données et une clé (dongle) FTK contenant plusieurs licences utilisateur est connectée au serveur. Les clients FTK sont configurés pour rechercher une licence sur ce serveur et aucune clé n'est nécessaire. Voir le *Guide d'installation et de configuration de Dell Digital Forensics* pour plus d'informations. Voir « Documentation et ressources associées », page 15. En outre, contactez l'administrateur des systèmes réseau pour plus d'informations sur l'installation de la solution de votre agence.

### Créer une image du périphérique de stockage cible

1. Dans l'application AccessData FTK Imager, cliquez sur **File→ Create Disk Image. . .**
2. Dans la fenêtre contextuelle **Select Source** (Sélectionner une source), sélectionnez le type de preuve pour laquelle vous voulez créer une image : Physical Drive (Unité physique), Logical Drive (Unité logique), Image File (Fichier image), Contents of a Folder (Contenu d'un dossier) ou Fernico Device (Unité Fernico), puis cliquez sur **Next**.

**REMARQUE :** L'exemple suivant utilise l'option **Imaging a Physical Drive** pour montrer la procédure de création d'une image. Les autres options de fichier sont converties dans le *guide d'utilisation FTK*. Voir « Documentation et ressources associées », page 15.

3. Dans la zone déroulante, sélectionnez l'unité physique pour laquelle vous voulez créer une image dans les unités disponibles et cliquez sur **Finish**.
4. Dans la fenêtre contextuelle **Create Image** (Créer une image, cliquez sur **Add. . .** et sélectionnez le type d'image à créer (Raw, SMART, E01, or AFF). Cliquez sur **Next**.
5. Entrez les informations demandées dans la fenêtre **Evidence Item Information** (numéro d'affaire, numéro de preuve, description unique et remarques). Cliquez sur **Next**.
6. Dans la fenêtre **Select Image Destination**, accédez à la zone de stockage allouée aux images de preuve (voir Figure 3-5pour le fichiers recommandé de Dell et la nomenclature de serveur), entrez le nom de fichier de l'image et cliquez sur→

7 Cliquez sur **Start**. La fenêtre **Creating Image. . .** s'affiche et affiche la barre d'avancement de l'opération.

**REMARQUE :** La création d'une image peut prendre plusieurs heures en fonction du volume de données ajouté.

8 Si vous avez décidé précédemment d'afficher le résumé du résultat de l'image, la fenêtre **Drive/Image Verify Results** s'affiche à la fin de la création de l'image. Vérifiez le résultat et cliquez sur **Close**.

9 Cliquez de nouveau sur **Close** pour fermer la fenêtre **Creating Image . . .**

### Créer une affaire

1 Cliquez sur **File→ New Case.** Entrez les informations suivantes : le **nom de l'enquêteur**, le **numéro de l'affaire**, le **nom de l'affaire**, le **chemin de l'affaire** et le **dossier de l'affaire**.

2 Dans la fenêtre **Forensic Examiner Information** entrez l'**agence/la société** et le **nom,** l'**adresse**, le **numéro de téléphone**, le **fax**, l'**adresse électronique** et les **commentaires** de l'analyseur. Cliquez sur **Next**.

3 Dans la fenêtre **Case Log Options** sélectionnez les options à modifier :

- Case and evidence events (Evénements d'affaire et de preuve)
- Error messages (Messages d'erreur)
- Bookmarking events (Evénement de signet)
- Data Carving events (Evénement de reconstruction de fichiers)
- Data carving/Internet searches (Evénement de reconstruction de fichiers/Recherches Internet)
- Autres événements

4 Dans la fenêtre **Processes to Perform**, sélectionnez les processus à exécuter. Vous pouvez sélectionner les **processus** suivants :

- 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 Cliquez sur **Next**.

6 Dans la fenêtre **Refine Case** incluez ou excluez différents types de données de l'affaire. Les options prédéfinies incluent cinq conditions communes :

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

7 Cliquez sur **Next**.

8 Dans la fenêtre **Refine Index**, incluez ou excluez différents types de données de l'indexaction.

9 Cliquez sur **Next**.

#### Ajouter une preuve

1 Cliquez sur **Add Evidence**. La fenêtre contextuelle **Add Evidence to Case** s'affiche.

2 Sélectionnez le type de preuve à ajouter à l'affaire : **Acquired Image of Drive**, **Local Drive**, **Contents of a Folder** ou **Individual File** en sélectionnez le bouton radio. Cliquez sur **Continue**.

3 Accédez à l'image, à l'unité, au dossier ou au fichier, sélectionnez le fichier et cliquez sur **Open**.

*Si vous avez sélectionné* **Aquired Image of Drive** comme type de preuve, une fenêtre contextuelle **Evidence Information** s'affiche. Entrez les informations demandées et cliquez sur **OK**.

*Si vous avez sélectionné* **Local Drive** comme type de preuve,

**a** la fenêtre **Select Local Drive** s'affiche. Sélectionnez l'unité locale à ajouter et **Logical Analysis** ou **Physical Analysis**. Cliquez sur **OK**.

**b** Dans la fenêtre **Evidence Information**, entrez les informations demandées et cliquez sur **OK**.

*Si vous avez sélectionné* **Cntents of a Folder ou Individual File**, sélectionnez le dossier ou le fichier à ajouter à l'affaire et cliquez sur **Open.**

**4** Cliquez sur **Next**.

**5** Dans la fenêtre **New Case Setup is Now Complete**, vérifiez vos sélections. Cliquez sur **Finish.**

## Incorporation en utilisant FTK 3 Lab Edition

### Créer une image du périphérique de stockage cible

Voir « Créer une image du périphérique de stockage cible », page 58.

### Créer une affaire

**1** Cliquez sur **Case→ New**. La fenêtre **New Case Options** s'affiche.

**2** Entrez le nom de l'affaire et les informations de référence ou descriptives demandées par votre agence.

**3** Accédez au répertoire du dossier de l'affaire et sélectionnez le gestionnaire de traitement dans la zone de liste déroulante.

**REMARQUE :** Si vous ne savez pas ou se trouvent ce répertoire et le gestionnaire, contactez l'administrateur système.

**4** Cliquez sur **Detailed Options** pour afficher les données à inclure dans l'affaire. Voir le *guide d'utilisation d'AccessData FTK 3* pour plus d'informations sur la limitation des données des affaires. Voir « Documentation et ressources associées », page 15.

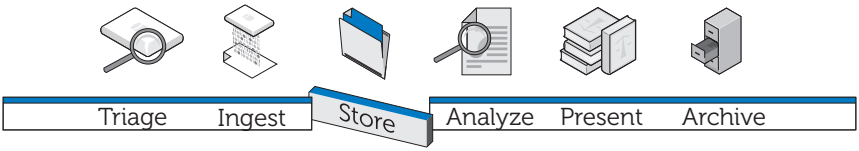
**5** Cliquez sur **OK**. La fenêtre **Manage Evidence** s'ouvre.

**Ajouter une preuve à une affaire**

1. Dans la fenêtre **Manage Evidence**, cliquez sur **Add**. Cliquez sur le bouton radio à côté du type de preuve à ajouter : **Acquired Image(s)**, **All Images in Directory**, **Contents of a Directory**, **Individual File(s)**, **Physical Drive** ou **Logical Drive**. Cliquez sur **OK**.
2. Accédez au répertoire **Evidence** et sélectionnez le fichier de preuve. Cliquez sur **Open**.
3. Choisissez un fuseau horaire (obligatoire).
4. Cliquez sur **OK**. La fenêtre **Data Processing Status** s'affiche.
5. Lorsque l'**état du processus** devient **Finished**, cliquez sur **Close**. La preuve apparaît dans l'affaire dans l'interface du logiciel.

# 4

# Stockage




La méthode classique en matière de stockage des preuves numériques commence par les recherches qu'effectuent indépendamment les enquêteurs sur des postes de travail individuels dans une configuration multisilos. Le fichier de preuve est stocké plus ou moins de manière sécurisée sur le poste de travail ou transféré chaque jour d'un serveur de stockage vers le poste de travail, le transfert en continu de fichiers très volumineux augmentant la charge du réseau. La structure ne tire pas partie de la vitesse du traitement réparti, des économies d'échelle et des économies de coût substantielles qu'offre un traitement parallèle au niveau de l'entreprise et une architecture de stockage multiniveau. En outre, dans cette configuration, il est difficile, au mieux, de partager des données ou de collaborer avec les équipes internes et externes pour sauvegarder régulièrement et de manière fiable les données et surtout garantir l'intégrité et la sécurité des fichiers.

## Efficacité

La solution Dell Digital Forensics peut s'adapter à de nombreuses configurations informatiques différentes. Plus la configuration est proche d'une véritable conception d'entreprise, constituée de postes de travail, de serveurs de traitement dédiés capables de répartir le traitement, d'une infrastructure réseau basée sur les communications parallèles et non série et d'un stockage, plus la configuration est efficace. Le trafic réseau est moins élevé et plus rapide, car ce sont les processeurs répartis qui effectuent la plus grande partie du travail ; le réseau se limite à transférer les résultats de ce travail et non pas les fichiers de preuve eux-mêmes.

Lorsque les fichiers sont gérés sur le serveur et non pas sur le poste de travail, l'analyste est libre d'utiliser le poste de travail pour lancer et contrôler *plusieurs* travaux au lieu d'être limité à tenter de traiter un seul travail. En outre, les analyses peuvent être exécutées encore plus rapidement, car plusieurs analystes et spécialistes conseil, tels que des experts en langues étrangères, peuvent travailler sur le même fichier ***.E01** simultanément depuis des postes de travail différents.

Le travail peut être trié en fonction des difficultés et affecté à des analystes ayant des niveaux de compétences différents ; un analyste non expérimenté peut être chargé des longues tâches d'extraction des fichiers graphiques d'un fichier ***.E01** alors que l'analyste expérimenté peut effectuer des analyses et des vérifications plus complexes sur ces fichiers.

## Evolutivité

Sur le back end, les composants du centre de données de la solution sont modulaires et évolutifs. Comme le centre de données gère la charge de travail, il n'est pas nécessaire que les postes de travail disposent de mémoire et d'une puissance de traitement. En fait, vous pouvez utiliser des terminaux légers pour accéder aux fichiers de preuve nécessaires et même au logiciel analytique stocké dans le centre de données.

## Sécurité

La tendance croissante d'agréger les informations rend les systèmes de stockage des données plus vulnérables. Mais, l'accès au stockage des preuves doit être le point le plus contrôlé d'un système d'investigation numérique. Les meilleures pratiques impliquent de mettre en oeuvre une stratégie à trois niveaux :

- Contrôle strict de l'accès physique au matériel où résident les données de preuve
- Couche de contrôle administratif qui inclut l'utilisation de groupes de stratégies
- Sécurité des ordinateurs, telle que règles de création de mots de passe sécurisés

A cette fin, lors de la détermination du volume et de la structure qui répondent à vos besoins (voir « Incorporation », page 39), la sécurité constitue la principale priorité d'une agence en terme de stockage.

### Couche d'accès physique

Les fichiers du serveur de preuves pour l'investigation numérique doivent être plus protégés que les autres fichiers de l'entreprise, y compris ceux des Ressources Humaines.

Voici quelques suggestions :

- Placez les serveurs d'analyse et le stockage des données dans un emplacement dédié du laboratoire d'analyse. Ainsi, tous les serveurs, entrepôts de données, câblages physiques, commutateurs et routeurs sont protégés physiquement par les mêmes mesures de sécurité qui limitent l'accès au laboratoire.
- Utilisez des protocoles de contrôle des entrées, tels que des lectures d'empreintes digitales ou des caractéristiques de la rétine ou des cartes d'accès à puces.
- Routez tout le trafic d'analyse via des commutateurs réseau dédiés et connectés physiquement à des serveurs et des postes de travail d'analyse.

### Couche de surveillance administrative et Active Directory

Votre solution de configuration fonctionnera sur un système d'exploitation Windows. Par conséquent, le reste de ce chapitre porte sur Windows et ses fonctions de sécurité Groupe et utilisateur Active Directory. Active Directory repose sur la sécurité de groupe et ses fonctions associées. Un groupe est un ensemble d'utilisateurs ou d'ordinateurs dans un domaine. Les deux types de groupes de base sont les *groupes de distribution* (utilisés pour la distribution du courrier électronique) et les *groupes de sécurité*. La création de groupes de sécurité permet de créer et d'appliquer des règles de sécurité, notamment :

- Accès aux ressources partagées et niveau de l'accès
- Droits d'utilisateur, y compris exigences de mot de passe
- Règles de verrouillage de compte
- Règles de limitation de logiciel
- Distribution des correctifs de sécurité aux ordinateurs portables, aux ordinateurs de bureau et aux serveurs

Par exemple, vous pouvez créer un groupe contenant les postes de travail et un second groupe contenant les utilisateurs administratifs. Vous pouvez utiliser des objets de stratégie de groupe pour limiter l'accès à ces postes de travail et aux membres du groupe d'utilisateurs administratifs. (Voir « Application de stratégies de sécurité en utilisant des objets de stratégie de groupe », page 70 pour plus d'informations sur l'utilisation des objets de stratégie de group.)

### Couche de sécurité des ordinateurs et Active Directory

Active Directory fournit également Kerneros, un protocole de sécurité d'authentification réseau qui permet aux noeuds qui communiquent sur des réseaux non sécurisés pour prouver leur identité à un autre noeud d'une manière sécurisée. Voir « Comptes utilisateur Active Directory », page 72 pour plus d'informations sur l'utilisation des comptes utilisateur et « Support Active Directory pour les stratégies de mot de passe sécurisé », page 71 pour plus d'informations sur la création de mots de passe.

#### Informations complémentaires sur la sécurité et l'investigation numérique

SP 800-41 Rév. 1 Sept. 2009 Guidelines on Firewalls and Firewall Policy

SP 800-46 Rév. 1 Jun. 2009 Guide to Enterprise Telework and Remote Access Security

SP 800-55 Rév. 1 Jul 2008 Performance Measurement Guide for Information Security

## Stockage multiniveau

La solution Digital Forensics de Dell utilise des stratégies de stockage multiniveau pour faire face à l'augmentation croissante du volume de données tout en contrôlant les coûts. Vous pouvez personnaliser une combinaison d'unités SATA et SAS de différentes capacités et ayant des niveaux de performances différents pour qu'elles correspondent aux profils de données et vous pouvez réévaluer cette combinaison régulièrement pour maintenir un niveau de fonctionnement optimal dans le temps. Généralement, les données stratégiques, telles que les données des affaires en cours d'analyse, sont stockées sur des unités chères haute performance, alors que les données moins urgentes, telles que les fichiers des affaires en début d'appel ou fermés sont placés sur des unités économiques de grande capacité.

**Figure 4-1. Stockage multiniveau pour l'archivage et l'extraction**

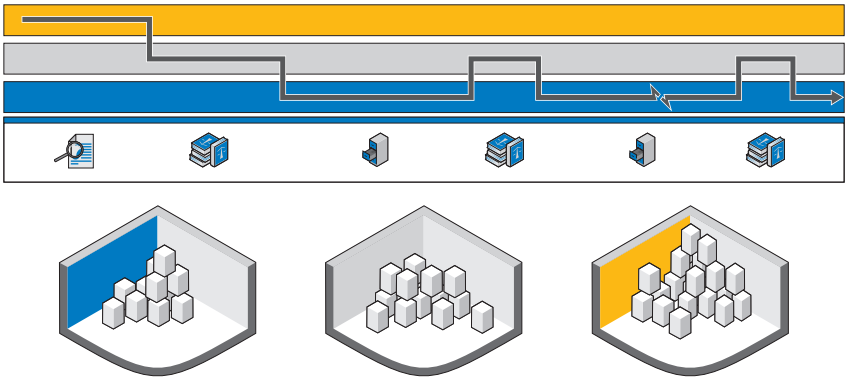


Figure 4-1 montre le chemin suggéré pour le stockage des preuves numériques entre la collecte des preuves et le stockage à long terme des preuves sur bande et la suppression finale.

## Correspondance entre l'archivage des preuves et l'extraction et la vie de l'affaire

*Saisie de la preuve (Analyse)* – Lors de la saisie du périphérique, un laboratoire High Tech anticrime cherchera normalement à extraire la preuve du périphérique et à lancer l'analyse dès que possible. Plus la recherche et l'indexation d'un fichier de preuve par un analyste est rapide, plus il est possible de prendre rapidement une décision quant aux suites à donner à l'affaire.

*Identification de la preuve (Présentation)* – Lorsqu'une preuve a été potentiellement trouvée au cours de l'analyse, différents groupes de compétences peuvent être maintenant nécessaires (langue, dessins techniques, comptabilité, etc.). La preuve doit être maintenant catégorisée par les équipes d'analyse. La partie « lourde » du traitement est maintenant terminée. La preuve peut donc résider dans un emplacement de stockage à long terme plus économique.

*Attente du procès (Archivage)* – Lorsque toutes les preuves ont été rassemblées et que le dossier est en cours, il est généralement inutile de continuer de stocker en ligne les données et les images des preuves de l'affaire qui sont accessibles instantanément. Généralement, le laboratoire peut répondre aux *demandes d'extraction de périodes*, ce qui peut être effectué de manière proactive si un événement connu d'envoi justifie la nécessité des données de l'affaire. Cette approche réduit le coût du stockage dans le laboratoire d'investigation, car il n'est pas nécessaire de conserver toutes les données dans le laboratoire ; qu'elle que soit la pertinence actuelle, elles peuvent être transférées de manière transparente vers un emplacement de stockage plus lent.

*Procès (Présentation)* – Si le dossier fait l'objet d'un procès, le laboratoire d'investigation informatique voudra pouvoir accéder rapidement à la preuve et aux données de l'affaire pour répondre aux questions des juges.

*Garde à vue (Archive)* – En cas de mise en garde à vue, la législation de la plupart des pays impose à la police ou au Ministère de la Justice de conserver la preuve et les fichiers de l'affaire pendant une période minimale ou le temps de la garde à vue et pendant un délai d'appel raisonnable ou 99 ans. Cette disposition vise à placer les données sur un support de stockage à long terme économique qui protège l'intégrité et la confidentialité des données.

*Appel (Présentation)* – En cas d'appel, les données de l'affaire et la preuve peuvent être extraites pour une nouvelle analyse. Cette extraction doit intervenir à un moment bien défini, mais les données sont rarement demandées immédiatement.

*Suppression* – Dans la plupart des pays, les organismes publics ne sont pas autorisés à conserver les données indéfiniment après un certain délai. Un processus simple doit permettre de supprimer les données. Ce processus peut être nécessaire également lorsqu'une non-culpabilité est reconnue et que les données doivent être également détruites.

# Configuration de la sécurité du stockage en utilisant la solution Dell Digital Forensics Solution et Active Directory

## Création et remplissage de groupes dans Active Directory

Vous créez des groupes via les services de domaine Active Directory Domain (Windows Server 2008).

### Création d'un groupe (Windows Server 2008)

1. Cliquez sur **Démarrer→ Outils d'administration→ Active Directory Administrative Center**.
2. Dans le volet de navigation, cliquez avec le bouton droit de la souris sur le noeud auquel vous voulez ajouter un groupe, puis cliquez sur **Nouveau**. Cliquez sur **Groupe**.
3. Entrez le nom du nouveau groupe.
4. Sélectionnez l'option appropriée dans **Etendue du groupe**.
5. Sélectionnez le **type du groupe**.
6. Sélectionnez **Protéger contre la suppression accidentelle**.
7. Modifiez les sections **Géré par**, **Membre de** et **Membres**, puis cliquez sur **OK**.

### Ajout de membre à un groupe (Windows Server 2008)

1. Cliquez sur **Démarrer→ Outils d'administration→ Active Directory Administrative Center**.
2. Dans le volet de navigation, cliquez sur le dossier du groupe.
3. Cliquez avec le bouton droit de la souris, puis sur **Propriétés**.
4. Sélectionnez **Ajouter** dans l'onglet **Membres**.
5. Entrez le nom de l'utilisateur, de l'ordinateur ou du groupe que vous ajoutez, puis cliquez sur **OK**.

## Application de stratégies de sécurité en utilisant des objets de stratégie de groupe

Après avoir créé un groupe, vous pouvez appliquer collectivement des paramètres de sécurité et d'autres attributs aux membres du groupe en créant et en configurant un objet de stratégie de groupe. Ainsi, vous pouvez gérer aisément la sécurité des utilisateurs et des ressources lorsque votre organisation d'investigation numérique évolue.

## Création et modification des objets de stratégie de groupe

### Création d'un GPO (Windows Server 2008)

Dans Windows Server 2008, les objets de stratégie de groupe sont gérés en utilisant la console de gestion des stratégies de groupe (GPMC).

1. Pour ouvrir la console, cliquez sur **Démarrer→ Outils d'administration→ Stratégie de groupe**.
2. Accédez à la forêt et au domaine dans lesquels vous allez créer le nouvel objet, puis cliquez sur **Objets de stratégie de groupe**.
3. Cliquez sur **Nouveau**.
4. Entrez le nom de l'objet de stratégie de groupe, puis cliquez sur **OK**.

## Modification d'un GPO (Windows Server 2008)

Dans Windows Server 2008, les objets de stratégie de groupe sont gérés en utilisant la console GPMC.

1. Pour ouvrir la console, cliquez sur **Démarrer→ Outils d'administration→ Stratégie de groupe**.
2. Accédez à la forêt et au domaine de l'objet de stratégie de groupe, puis cliquez sur **Objets de stratégie de groupe**.
3. Cliquez avec le bouton droit de la souris sur l'objet de stratégie de groupe.
4. Modifiez les paramètres de manière appropriée et enregistrez-les.

## Support Active Directory pour les stratégies de mot de passe sécurisé

Active Directory prend en charge diverses stratégies d'authentification, notamment les cartes à puce, les mots de passe renforcés et des paramètres de verrouillage de compte.

Les mots de passe et les autres stratégies d'authentification sont créés en utilisant des objets de stratégie de groupes. Voir « Application de stratégies de sécurité en utilisant des objets de stratégie de groupe », page 70 pour plus d'informations sur la création et la modification d'un objet de stratégie de groupe.

### Paramètres de mot de passe renforcé suggérés

Les valeurs suivantes sont suggérées lors de la définition des paramètres de mot de passe :

- Appliquer l'historique des mots de passe - Nombre de mots de passe uniques qui peuvent être utilisés avant qu'un mot de passe puisse être réutilisé. Entrez la valeur 24.
- Age maximal du mot de passe - Les mots de passe doivent être changés tous les *x* jours. Entrez la valeur 90.
- Durée de vie minimale du mot de passe - Nombre de jours d'utilisation d'un mot de passe pour pouvoir le changer. Entrez la valeur 1 ou 2.
- Longueur minimale du mot de passe - Utilisez 8 ou 12 caractères.
- Le mot de passe doit respecter des exigences de complexité - **Activé**. Les stratégies suivantes sont appliquées :
  - Les mots de passe doivent contenir au moins 6 caractères.
  - Les mots de passe doivent contenir des caractères d'au moins trois des quatre catégories suivantes :
    - Majuscules
    - Minuscules
    - Chiffres (0 à 9)
    - Symboles
  - Les mots de passe doivent contenir au moins trois caractères consécutifs du nom du compte ou de l'utilisateur

#### Stratégies de mot de passe affinées

Dans Windows Server 2008, les services de domaine Active Directory prennent en charge les objets PSO (Password Setting Objects) qui s'appliquent à des groupes de sécurité globaux ou des utilisateurs dans un domaine. Un objet PSO peut définir une longueur de mot de passe en caractères, la complexité d'un mot de passe, l'âge minimum et l'âge maximum d'un mot de passe et d'autres attributs.

Par conséquent, vous pouvez créer plusieurs objets PSO qui correspondent à la structure organisationnelle de l'investigation numérique. Par exemple, vous pouvez utiliser des objets PSO pour mettre en oeuvre des mots de passe plus longs qui expirent mensuellement pour les utilisateurs administratifs et des mots de passe plus courts qui expirent tous les trois mois pour les analystes.

## Comptes utilisateur Active Directory

#### Création de comptes utilisateur pour les analyses de l'investigation informatique

1. Ouvrez **Utilisateurs et ordinateurs Active Directory** :
   a. Cliquez sur **Démarrer→ Panneau de configuration**
   b. Cliquez deux fois sur **Outils d'administration**, puis cliquez deux fois sur **Utilisateurs et ordinateurs Active Directory**.
2. Dans l'arborescence de la console, cliquez avec le bouton droit de la souris sur le dossier auquel vous voulez ajouter un compte utilisateur.

   **Où ?**

   **Utilisateurs et ordinateurs Active Directory**/*noeud de domaine*/*dossier*
3. Pointez sur **Nouveau**, puis cliquez sur **Utilisateur**.
4. Dans **Prénom**, tapez le prénom de l'utilisateur.
5. Dans **Initiales**, tapez les initiales de l'utilisateur.
6. Dans **Nom**, tapez le nom de l'utilisateur.
7. Modifiez le **nom complet** pour ajouter des initiales ou inverser l'ordre du prénom et du nom.

8 Dans **Nom d'ouverture de session de l'utilisateur**, tapez le nom d'ouverture de session de l'utilisateur, cliquez sur le suffixe UPN dans la zone déroulante et sur **Suivant**.

Si l'utilisateur utilisera un nom différent pour se connecter à des ordinateurs exécutant Windows 95, Windows 98 ou Windows NT, vous pouvez remplacer le nom d'ouverture de session de l'utilisateur dans **Nom d'ouverture de session de l'utilisateur (avant Windows 2000)** par un nom différent.

9 Dans **Mot de passe** et **Confirmer le mot de passe**, tapez le mot de passe de l'utilisateur et sélectionnez les options de mot de passe appropriées.

**REMARQUE :** Pour pouvoir exécuter cette procédure, vous devez être membre du groupe Opérateurs de compte, Administrateurs de domaine ou Administrateurs de l'entreprise dans Directory ou vous devez avoir délégué le droit approprié. Comme bonne pratique de sécurité, utilisez *Exécuter en tant que* pour exécuter cette procédure. Pour plus d'informations, voir *Groupes locaux par défaut*, *Groupes par défaut* et *Utilisation de Exécuter en tant que*.

#### Créer un compte de gestionnaire de service FTK

**REMARQUE :** Au cours de l'installation de FTK, le système demande le nom du compte utilisateur que vous envisagez d'utiliser pour gérer la fonction de traitement réparti. Ne pas utiliser.

Si vous utilisez la fonction de traitement réparti de FTK comme l'un des outils d'investigation numérique, vous devez créer un compte de gestionnaire de service FTK dans Active Directory pour gérer la mise à jour automatique des mots de passe. Au cours de l'installation de FTK, le système demande le nom de l'utilisateur qui sera utilisé pour contrôler et gérer la fonction de traitement réparti. Ce compte doit être créé comme service dans Active Directory et il doit disposer des privilèges d'administrateur (mais il ne doit pas être le compte Administrateur) pour établir une liaison continue entre FTK et le serveur de preuves nécessaire à la fonction de traitement réparti.

1 Dans Active Directory, ouvrez **Outils d'administration**, puis cliquez sur **Utilisateurs et ordinateurs Active Directory**.

2 Dans l'arborescence de la console, cliquez deux fois sur le noeud du domaine.

3 Dans le volet **Détails**, cliquez avec le bouton droit de la souris sur l'unité d'organisation à laquelle vous voulez ajouter le compte de service. Sélectionnez **Nouveau**, puis cliquez sur **Utilisateur**.

4 Dans **Nom**, tapez `FTKServMgr` pour le compte de service ; n'entrez pas le **nom**.

5 Modifiez le **nom complet** de manière appropriée.

6 Dans **Nom d'ouverture de session de l'utilisateur**, tapez `FTKServMgr`. Le compte de service se connectera avec le nom que vous avez entré. Dans la liste déroulante, cliquez sur le **suffixe UPN** qui doit être ajouté au nom d'ouverture de session du compte de service (après le symbole @). Cliquez sur **Suivant**.

7 Dans **Mot de passe** et **Confirmer le mot de passe**, tapez un mot de passe pour le compte de service.

8 Sélectionnez les options de mot de passe appropriées, puis cliquez sur **Suivant**.

9 Cliquez sur **Terminer** pour terminer la création du compte de service.

### Créer un compte utilisateur non administratif

1 Ouvrez une session sur un ordinateur Windows Vista avec un compte utilisateur administratif.

2 Ouvrez le menu **Démarrer**. Cliquez avec le bouton droit de la souris sur **Ordinateur**, puis cliquez sur **Gérer**.

3 Cliquez sur la flèche en regard de **Utilisateur et groupes locaux.**

4 Cliquez avec le bouton droit de la souris sur **Utilisateurs**, cliquez sur **Nouvel utilisateur**.

5 Tapez le nom de l'utilisateur pour lequel vous créez un compte. Par exemple, si vous voulez appeler l'utilisateur **utilisateurweb1**, tapez `utilisateurweb1` dans la zone **Nom d'utilisateur** et dans la zone **Nom complet**.

6 Tapez un mot de passe à mémoriser dans les zones **Mot de passe** et **Confirmer le mot de passe**.

**REMARQUE :** Les mots de passe sont sensibles à la casse. Le mot de passe que vous tapez dans les zones **Mot de passe** et **Confirmer le mot de passe** doivent correspondre pour pouvoir ajouter le compte utilisateur.

7 Désélectionnez la case **L'utilisateur doit changer le mot de passe à la prochaine ouverture de session**.

8 Cochez les cases **Le mot de passe n'expire jamais** et **L'utilisateur ne peut pas changer le mot de passe**.

9 Cliquez sur **Créer** et sur **Fermer**.

10 Cliquez sur **Fichier** et sur **Quitter**.

## Configuration de la sécurité des fichiers d'affaire et de preuve individuels

1 Dans **Windows Explorer**, accédez au fichier pour lequel vous voulez définir des autorisations. Cliquez avec le bouton droit de la souris sur le fichier, puis sélectionnez **Propriétés**.

2 Cliquez sur l'onglet **Sécurité**.

3 Désélectionnez la case **Tout le monde**, si nécessaire.

4 Ajoutez uniquement les utilisateurs qui devront accéder au fichier, comme défini par la stratégie de votre espace de travail.

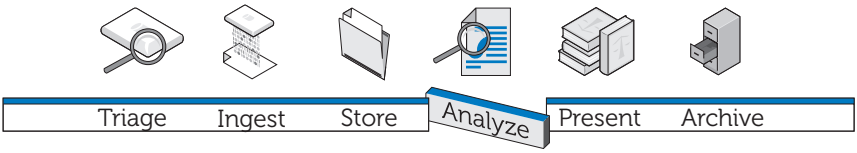
   a Cliquez sur **Ajouter**.

   b Dans la zone **Entrer les noms d'objet à sélectionner**, entrez les noms des utilisateurs appropriés. Cliquez sur **OK**.

   c Modifiez les **autorisations** de chaque utilisateur, comme défini par la stratégie de votre espace de travail.

# 5

# Analyse




L'analyste doit pouvoir exécuter différents types d'investigation sur les données de preuve, notamment, des analyses de signature, de hachage et d'indexation étendue et des recherches de mots de passe. Toutes ces analyses nécessitent une puissance de traitement considérable, car les fichiers de preuve d'une affaire peuvent atteindre le téraoctet et le traitement de ces fichiers peut prendre des dizaines d'heures, voir de jours, en utilisant les architectures de centre de données qui existent généralement actuellement. Les enquêteurs qui tentent ce type d'analyse sur un poste de travail doivent tenir compte de ce fait lors de la planification du traitement d'une affaire, car l'analyse et l'indexation d'un cas peuvent utiliser toutes les ressources matérielles de l'enquêteur. La solution Digital Forensics de Dell offre des avantages de traitement distribués significatifs et cela peut tout changer. Nous allons aborder le traitement réparti dans quelques instants, mais examinons préalablement quelques types d'analyses qu'exécute généralement l'enquêteur informatique.

## Types d'analyses

### Analyse de hachage

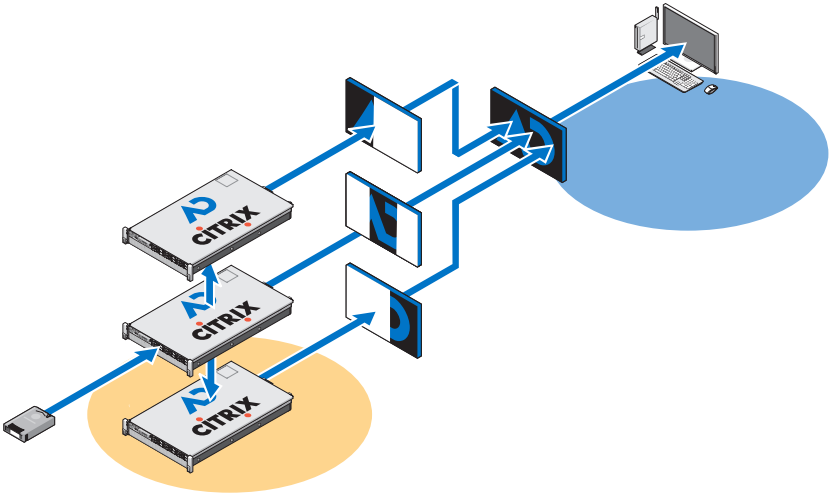
Une fonction de hachage utilise des algorithmes cryptographiques pour créer une empreinte numérique des données. Le hachage peut être utilisé pour comparer un hachage des données d'origine à l'un des hachages des données d'investigation informatique analysées, ce que peuvent accepter les juges comme preuve que les deux groupes de données sont identiques. L'analyse de hachage compare les valeurs de hachage d'un fichier d'affaire à des valeurs de hachage stockées connues.

### Analyse de signature de fichier

Chaque fichier a un type de fichier généralement indiqué par l'extension à trois ou quatre lettres du nom du fichier. Par exemple, un fichier texte peut porter l'extension ***.txt** et un fichier image peut avoir l'extension ***.jpg**. Il est fréquent que ces extensions de fichier soient été remplacées par quelque chose d'apparemment inoffensif. Un fichier image, par exemple, peut être renommé avec une extension de fichier texte pour masquer un contenu pornographique.

Toutefois, chaque fichier dispose également d'un en-tête qui contient un code de type de fichier différent de l'extension, mais qui indique uniquement un type de fichier spécifique. Par exemple, un fichier ***.bmp** a le code d'en-tête de type de fichier ***.bm8**. Lorsque ce code et l'extension de fichier diffèrent, l'enquêteur informatique doit analyser les données de manière plus approfondie.

**Figure 5-1. Traitement réparti**




## Qu'est-ce que le traitement réparti ?

*Le traitement réparti* fait référence à l'utilisation de plusieurs processeurs, chacun disposant de sa propre ressource de mémoire, qui sont appliqués individuellement à une partie différente d'une tâche de calcul et qui utilisent un système d'envoi de messages pour communiquer entre eux dans le groupe.

Le traitement réparti n'est pas identique au *traitement parallèle* qui fait référence à l'utilisation de plusieurs processeurs qui partagent une seule ressource de mémoire.

Tenez compte des points suivants, qui vous donneront une idée générale des avantages de la solution Dell de l'utilisation d'une installation de traitement réparti. L'utilisation du traitement réparti pour exécuter une analyse de cinq fichiers de 200 Go peut ne prendre que 3,5 heures alors que celle d'un seul fichier de 200 Go sur un poste de travail autonome peut nécessiter environ 7 à 8 heures.

Le transfert du traitement des données de preuve du poste de travail de l'analyste vers le serveur ne signifie pas la fin de l'opération. La solution Dell permet d'exécuter un logiciel d'analyse, tel que FTK ou EnCase sur le serveur en transformant le poste de travail en interface intégrée pouvant exécuter plusieurs instances de différents progiciels d'investigation informatique sous des systèmes d'exploitation utilisés simultanément sans affecter les performances des clients.

# Utilisation du traitement réparti dans FTK 3.1

Le traitement réparti permet d'appliquer les ressources supplémentaires de trois ordinateurs supplémentaires simultanément au traitement des affaires. Après avoir installé et configuré le moteur de traitement réparti, vous pouvez réduire la durée de traitement des affaires de manière exponentielle.

**REMARQUE :** L'utilisation du traitement réparti, en général, ne réduit pas la durée du traitement si le nombre d'objets à traiter n'excède pas 1 000 fois le nombre de processeurs dans le système. Par exemple, sur un système à huit coeurs, les machines supplémentaires à moteur de traitement réparti ne réduisent pas la durée du traitement si la preuve ne contient pas plus de 8 000 éléments.

**REMARQUE :** Pour des informations sur l'installation et la configuration du module de traitement réparti dans le cadre de la solution, voir la section appropriée du *guide d'utilisation FTK*.

1. Veillez à ce que le dossier de l'affaire soit partagé avant d'ajouter et de traiter la preuve. Si vous suivez les conventions recommandées de Dell d'appellation des fichiers, le dossier de l'affaire doit se trouver sur l'unité **W:/** du poste de travail. Si vous ne savez pas où se trouve le dossier de l'affaire, contactez l'administrateur système.

2 Entrez le chemin du dossier de l'affaire dans la boîte de dialogue **Create New Case** dans le format UNC :

`(\\[computername_or_IP_address]\[pathname]\[filename])`

3 Cliquez sur **Detailed Options** et sélectionnez les options comme vous le faites habituellement.

4 Cliquez sur **OK** pour revenir à la boîte de dialogue **New Case Options** et cochez l'option **Open the case**. Cliquez sur **OK** pour créer une affaire et l'ouvrir.

5 Cliquez sur **Add** après avoir ouvert l'affaire et l'ouverture automatique de la boîte de dialogue **Manage Evidence**. Sélectionnez le fichier de preuve et cliquez sur **Open**.

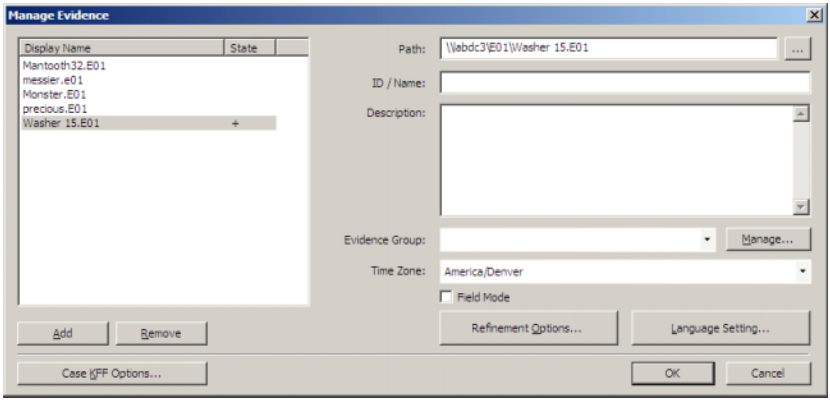
6 Le chemin de la preuve est désigné par la lettre d'unité par défaut. Changez le chemin pour utiliser le format UNC en remplaçant la lettre d'unité par le nom de la machine ou l'adresse IP de la machine où se trouve le fichier de preuve en respectant la syntaxe suivante :

`\\[computername_or_IP_address]\[pathname]\[filename]`

7 Laissez le chemin restant tel quel.

8 Le chemin UNC de la preuve est indiqué dans l'illustration suivante :

**Figure 5-2. Boîte de dialogue Manage Evidence (Gérer la preuve)**




9 Cliquez sur **OK**.

### Vérification de l'installation

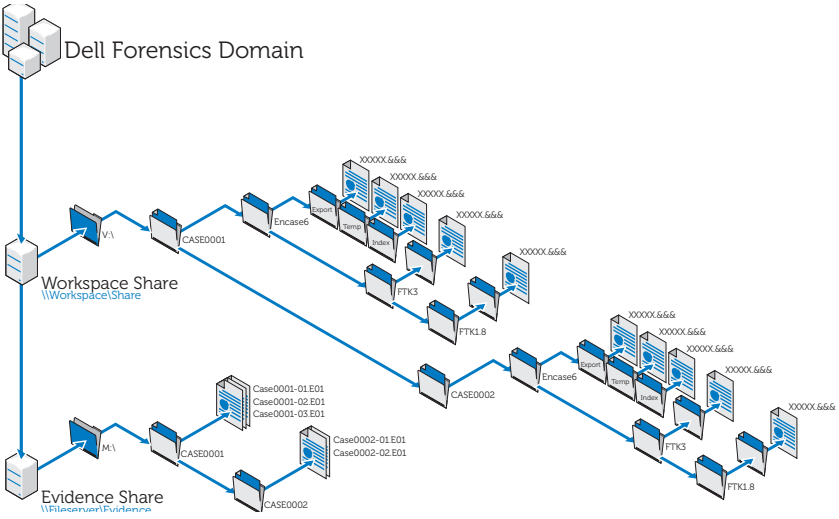
Une fois l'installation effectuée, ouvrez le **gestionnaire de tâches** sur l'ordinateur distant et maintenez-le ouvert lorsque vous ajoutez la preuve et commencez le traitement. Ces étapes permettent de surveiller l'activité de **ProcessingEngine.exe** dans l'onglet **Processes** (Processus).

Le moteur de traitement réparti ne s'active pas tant que l'affaire ne dépasse pas 30 000 éléments environ. Lorsqu'il s'active, le pourcentage UC et l'utilisation de la mémoire augmente pour **ProcessingEngine.exe** dans le **gestionnaire des tâches**.

## Recherche de fichiers sur le réseau

La meilleure pratique impose de stocker séparément les fichiers de preuve et de travail sur le réseau. Dell recommande de définir jusqu'à deux unités de partage en créant les fichiers et les sous-fichiers d'affaire à partir de cet emplacement, comme indiqué dans la Figure 5-3.

**Figure 5-3. Structure de fichiers recommandées par Dell**



# Analyse en utilisant FTK

## Ouvrir une affaire existante

### Utilisation du menu File (Fichier)

1. Dans FTK, sélectionnez **File** et sélectionnez **Open Case**.
2. Sélectionnez l'affaire à ouvrir et cliquez dessus pour lancer l'affaire.

**REMARQUE :** Tous les fichiers d'affaire s'appellent **case.ftk**. Le fichier **case.ftk** de chaque affaire est stocké dans le dossier d'affaire correspondant.

### Depuis la ligne de commande

Sur la ligne de commande, tapez :

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

## Traitement de la preuve d'affaire

FTK traite la preuve lorsqu'une affaire est créée ou que la preuve est ajoutée ensuite à l'affaire. Pour les instructions de création d'une affaire, voir « Créer une affaire », page 61 ou le *guide d'utilisation de FTK*. Pour les instructions d'ajout de preuves à une affaire existante, voir « Ajouter une preuve à une affaire », page 62 ou le *guide d'utilisation de FTK*. Voir « Documentation et ressources associées », page 15 pour plus d'informations.

# Analyse en utilisant EnCase

## Ouvrir une affaire existante

1. Dans le menu File (Fichier), sélectionnez **File→ Open**.
2. Accédez à l'affaire et cliquez sur **Open**.

### Créer un travail d'analyse

1. Cliquez sur l'onglet **Analysis Jobs** dans la boîte de dialogue **Source Processor**.
2. Cliquez sur **New**. La boîte de dialogue **Create Analysis Job/Job Name** s'affiche.

   Le nom par défaut est Job__[yyyy_mm_dd__hh_mm_ss], par exemple : Job___2009_06_24__03_42_42_PM.

   Un nom de travail ne peut pas commencer et se terminer par un espace ni par les caractères \ / : * ? " < > |
3. Entrez un nom de travail et cliquez sur **Next**. La boîte de dialogue **Create Analysis Job/Module Name** (Créer un travail d'analyse/Nom de travail) s'affiche.

   Cette boîte de dialogue contient les dossiers de module dans le volet de gauche et les modules individuels dans ces dossiers dans le volet de droite.

   Si un module est inclus dans un travail d'analyse et qu'il n'existe aucune donnée pour le module lorsque le travail est exécuté par rapport à une collecte, le module est ignoré. Cette fonction permet de créer des travaux d'analyse génériques pour divers ensembles de données collectées.
4. Cochez la case du module.

   Vous pouvez sélectionner plusieurs modules.

   Les modules d'analyse n'ont pas de paramètres définissables par l'utilisateur.

   Pour sélectionner tous les modules dans un groupe, cochez le nom de dossier du groupe dans le volet de gauche.
5. Cliquez sur **Finish**.

**REMARQUE :** Les travaux d'analyse peuvent répertorier les modules disponibles qui ne le sont pas dans les travaux de collecte. Ces modules sont identifiés comme des modules existants. Par conséquent, vous pouvez analyser les données collectées dans les versions précédentes du processeur source en utilisant des modules qui n'existent plus.

### Exécuter un travail d'analyse

1. Dans l'onglet **Collected Data**, sélectionnez la preuve à analyser en sélectionnant préalablement le nom du travail dans le volet de gauche. Sélectionnez les fichiers de preuve dans le tableau sur la droite.
2. Cliquez sur **Run Analysis**. La boîte de dialogue **Select Analysis to Run**.
3. Sélectionnez le travail d'analyse, puis cliquez sur **Run**. Le processeur source exécute l'analyse sur la preuve sélectionnée. A la fin de l'analyse, le navigateur de données s'affiche.

### Exécution d'une analyse de signature

1. Cliquez **Search**.
2. Cochez la case **Verify file signatures** (Vérifier la signature des fichiers) dans la zone **Additional Options** (Options supplémentaires) dans la partie droite, puis cliquez sur **Start**. L'analyse des signatures s'exécute en arrière-plan. A la fin de l'opération, une boîte de fin de recherche s'affiche. Elle contient l'état, les heures et les données de fichiers de la recherche.

Vous pouvez également visualiser ces données dans la console.

### Affichage des résultats de l'analyse des signatures

1. Cliquez sur **Set-Include** dans le volet **Tree** pour afficher tous les fichiers de l'affaire.

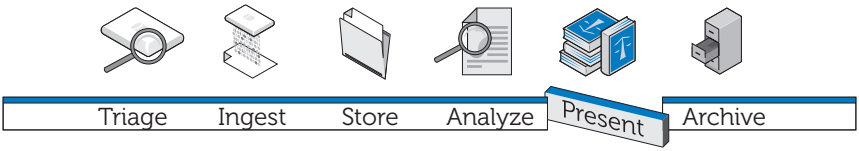
   A ce stade, **Set Include** sélectionne tout le contenu du fichier de preuve.
2. Organisez les colonnes dans le volet **Table** pour que les colonnes **Name**, **File Ext** et **Signature** soient côte à côte.
3. Triez les colonnes avec **Signature** au premier niveau, **File Ext,** au deuxième et **Name**, au troisième.

   Faites défiler vers le haut ou vers le bas pour afficher toutes les signatures.
4. Cliquez sur **Set-Include** dans la section **Entries** dans le volet **Tree**.

   La liste des fichiers d'affaire avec leurs signatures de fichier associées et d'autres données s'affichent dans le volet **Table**.
5. Triez les données de manière appropriée.

# 6

# Présentation




Créer un rapport sur les résultats de l'analyse fait partie intégrante de la solution Dell Digital Forensics. Cette opération s'effectue via le logiciel d'investigation que vous utilisez dans la solution.

## Création de rapports en utilisant la solution Dell Digital Forensics

### Créer et exporter des rapports en utilisant EnCase 6

1. Sélectionnez les éléments pour lesquels vous voulez créer un rapport, qu'ils s'agissent de fichiers, de signets, de résultats de recherche ou autres.
2. Sélectionnez le type de rapport à utiliser en utilisant les onglets du panneau **Tree**.
3. Dans l'onglet **Table** dans le panneau **Table**, activez les éléments que vous voulez placer dans le rapport.
4. Dans l'onglet **Table**, accédez à l'onglet **Report**.
5. Modifiez le rapport de manière appropriée.
6. Exportez le rapport dans un format lisible en dehors de EnCase.
   a. Cliquez avec le bouton droit de la souris dans le rapport et cliquez sur **Export** dans le menu déroulant. La boîte de dialogue **Export Report** s'affiche.
   b. Cliquez sur le bouton radio approprié pour sélectionner le format de sortie à utiliser (TEXT, RTF ou HTML).

c Entrez le chemin de sortie ou accédez-y.

d Si nécessaire, sélectionnez **Burn to Disc** pour activer la zone **Destination Folder**, puis cliquez avec le bouton droit de la souris sur **Archive Files** pour créer un dossier et enregistrer un fichier **.iso** sur disque.

e Cliquez sur **OK**

## Rapports en utilisant FTK

1 Cliquez sur **File**→ **Report** pour lancer l'**assistant Report**.

2 Entrez les informations de cas de base demandées par l'assistant.

3 Sélectionnez les propriétés des signets.

4 Déterminez si vous voulez afficher des graphiques de cas dans le rapport et le mode d'affichage.

5 Détermine si vous voulez inclure dans le rapport une section qui répertorie les chemins et les propriétés des fichiers dans les catégories sélectionnées.

6 Ajoutez les sections **Registry Viewer**, si nécessaire.

### Afficher le rapport en dehors de FTK

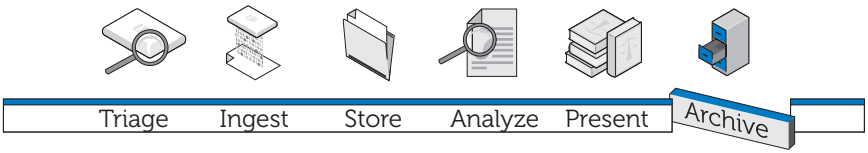
1 Accédez au fichier du rapport.

2 Cliquez sur le fichier, puis :

- cliquez sur **index.htm** pour ouvrir un document HTML dans un navigateur Web.
- cliquez sur [*report*]**.pdf** pour ouvrir le rapport dans un visualiseur PDF.

7

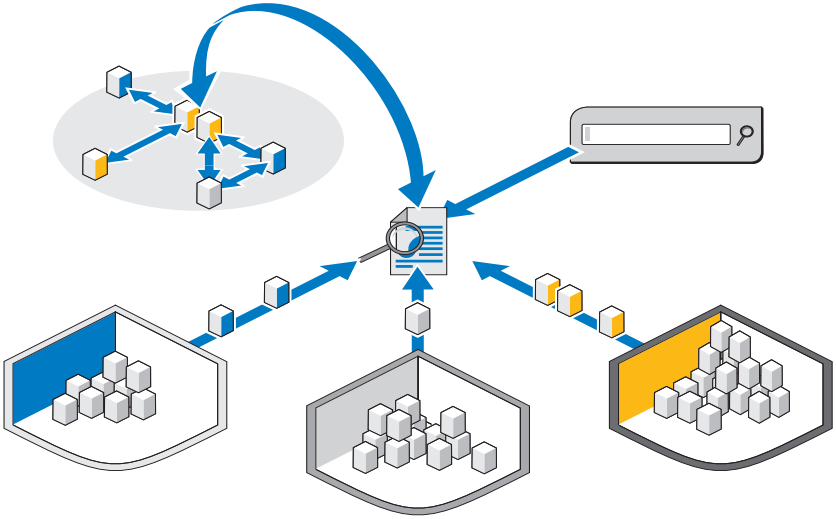
# Archivage




Aucune solution d'investigation informatique digne de ce nom ne peut se passer d'un composant d'archivage et d'extraction évolutif, sûr et complet. La solution Dell Digital Forensics vous offre bien plus. Dans l'infrastructure de la solution Dell, nous nous sommes efforcés de créer une interface simple qui fonctionne avec toutes les applications d'investigation informatique pour contrôler le cycle de vie des fichiers de preuve et d'affaire. Comme il est difficile de savoir quand des données peuvent être nécessaires ou de déterminer la durée d'une enquête, nous avons créé une solution souple qui demande à l'enquêteur de déterminer les fichiers qu'il rappellera et archivera. Cette solution utilise une méthode de stockage multiniveau adaptée à vos besoins : une combinaison de matériels SATA et SAS et l'archivage géré par l'utilisateur utilisant le logiciel d'archivage à la demande de NTP.

La solution Dell est constituée de composants modulaires qui fournissent un environnement évolutif qui peut être étendu pour répondre aux besoins croissants de traitement et de stockage. L'infrastructure formalisée de sauvegarde, de récupération et d'archivage (BURA) optimise la coopération entre les agences, les organismes concernés et les pays. Elle élimine la charge administrative en automatisant la plupart des tâches de sauvegarde, garantir la cohérence entre les laboratoires des agences et réduit les risques associés à la chaîne de conservation des données numériques.

**Figure 7-1. Fonctions de recherche multimédia et multi-affaires de la solution Dell**



Un composant de recherche très puissant en option permet de corréler les informations entre les ensembles de données incorporés. Ce composant permet d'effectuer des recherches Internet dans l'ensemble du magasin d'affaires dans le contenu actif et en ligne et dans les données archivées des affaires précédentes.

## Solution client d'archivage en un clic

Avec les outils d'archivage et d'extraction de la solution Dell Digital Forensics, un analyste peut archiver ou rappeler des fichiers individuels et des structures entières de répertoires en cliquant simplement avec le bouton droit de la souris. Des commandes contextuelles supplémentaires ont été ajoutées au logiciel d'archivage à la demande NTP pour que l'utilisateur puisse sélectionner et archiver ou sélectionner et restaurer simplement les données. Lorsqu'un fichier est sélectionné pour être archivé, une fenêtre supplémentaire s'affiche pour demander à l'utilisateur de confirmer l'action. Une fois l'action confirmée, la solution exécute une procédure en arrière-plan pour transférer le fichier vers une unité de bande ou un périphérique de stockage quasi en ligne. Ce processus s'exécute d'une manière entièrement transparente en arrière-plan sans affecter les performances du poste de travail de l'utilisateur.

A la fin de la procédure en arrière-plan, l'icône affectée au fichier devient grise pour indiquer clairement à l'utilisateur que le fichier a été archivé. Toutefois, le dossier et la structure de fichiers sont toujours visibles pour que l'utilisateur puisse retrouver aisément le fichier à des fins de restauration. Pour restaurer un fichier, l'utilisateur navigue simplement dans la structure des dossiers d'origine, recherche le dossier ou le fichier à restaurer, clique avec le bouton droit de la souris sur le fichier ou le dossier et sélectionnez l'option de restauration.

Dell recommande de placer tous les fichiers de preuve et d'affaire sur un périphérique NAS central évolutif permettant d'utiliser un point de stockage central extensible facilitant la collaboration entre les analystes. Cette recommandation permet aussi de disposer d'un seul point d'audit pour la chaîne de conservation. Lorsqu'un fichier est sélectionné pour être archivé, il est transféré vers la fenêtre de traitement disponible suivante du stockage principal vers l'option secondaire (bande ou périphérique quasi en ligne).

La vitesse d'archivage et de rappel varie considérablement en fonction du trafic vers et depuis le stockage NAS central, les fichiers à archiver et le type de support de l'option de stockage secondaire. Par exemple, SATA quasi en ligne est plus rapide que les bandes. Tous les fichiers peuvent être chiffrés sur bande pour renforcer la sécurité lorsqu'ils restent archivés longtemps dans la solution, ce qui peut nécessiter d'autres licences.

# Recommandations de sauvegarde Dell

### Sauvegardes fichiers de preuve et d'affaire

Un laboratoire utilise trois types de fichiers principaux :

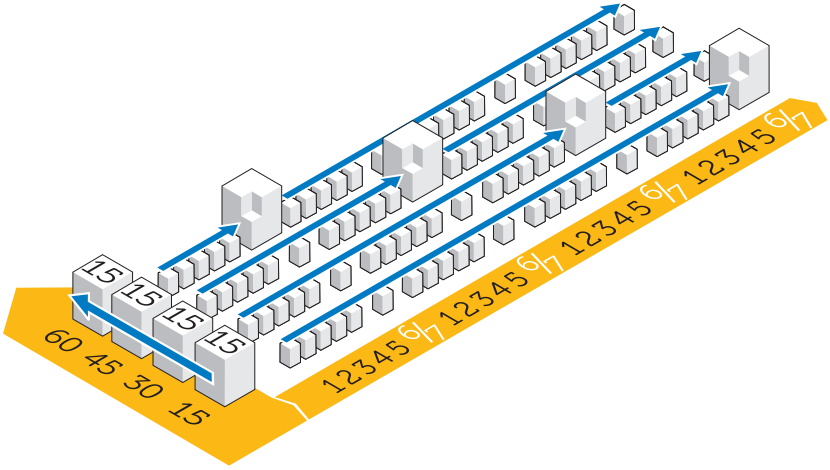
- Fichiers images : il s'agit des images sûres d'investigation du périphérique incriminé. Une fois incorporés, ils ne changent jamais et ils ne doivent être sauvegardés qu'une seule fois (extensions possibles : **E01**, **DD**, etc.). Les fichiers de preuve sont généralement moins nombreux, mais plus volumineux.
- Fichiers d'affaire : il s'agit des fichiers de données et des index résultant des analyses ; il peut être nécessaire de les exporter de l'application d'investigation. Les fichiers changent fréquemment si l'affaire est active et ils peuvent contenir plusieurs types d'extension, ce qui implique qu'ils doivent être sauvegardés tous les jours. Les fichiers d'affaire sont généralement nombreux, mais de petite taille.

- Base de données : ce type de fichier est utilisé uniquement dans FTK 3 (actuellement), mais il contient tous les liens entre les fichiers d'affaire et les fichiers de preuve, ainsi que tous les signets et notes d'investigation. Les fichiers de base de données doivent être sauvegardés tous les jours.

Figure 7-2 montre la meilleure pratique suggérée de sauvegarde d'un laboratoire d'investigation des données numériques. Comme les laboratoires d'investigation utilisent généralement un stockage de plus de 50 To, l'exécution d'une sauvegarde complète dans une fenêtre de sauvegarde de fin de semaine standard peut ne pas pouvoir être possible. Pour que les données puissent être restaurées en cas de sinistre avec le point de récupération minimum, la sauvegarde est divisée en sections égales et elle est exécutée sur un mois.

Ce processus nécessite de limiter la taille maximale des sauvegardes complètes à 15 To. Chaque LUN accepte les mises à jour incrémentielles pour le reste du cycle de la sauvegarde jusqu'à la prochaine sauvegarde complète.

**Figure 7-2. Plan de sauvegarde - Meilleure pratique**



### Hors hôte et réseau

Compte tenu de la taille des données à transférer sur bande pour la restauration en cas de sinistre dans les laboratoires d'investigation, le stockage dans des LUN est divisé en LUN de 15 To. Cela facilite la gestion et la sauvegarde et réduit les risques associés au cluster du système de fichiers en cas d'incident.

Deux types de sauvegarde peuvent être exécutés : réseau ou hors hôte.

- Dans une configuration de sauvegarde sur réseau, toutes les données de sauvegarde sont transmises sur le réseau au serveur de sauvegarde en utilisant un agent de sauvegarde qui réside sur le serveur.
- Dans une solution de sauvegarde hors hôte, certains des serveurs disposant des fichiers magasins de fichiers les plus grands ne sauvegardent pas leurs données sur le réseau. A la place, le module de stockage crée un instantané de la LUN et monte cette copie directement sur le serveur de sauvegarde. Ce processus accélère la sauvegarde, car aucun fichier de sauvegarde n'est envoyé sur le réseau normal pour provoquer des problèmes d'encombrement supplémentaires.

Dans la plupart des laboratoires d'investigation actuels, les sauvegardes sont créées sur des réseaux de 10 Go.

L'illustration suivante montre les agents nécessaires pour chaque serveur pour la sauvegarde :

**Figure 7-3. Agents de sauvegarde**

| 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 & Orade | 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 Agent Open File

AD Active Directory

OA Agent Oracle (agent de base de données générique nécessaire sur Backup Exec de Symantec)

SA Agent Oracle (agent de base de données générique nécessaire sur Backup Exec de Symantec)

NBU Net Backup Server

BE Backup Exec Server

EV Licence de sauvegarde Symantec Enterprise Vault

MI Sauvegarde complète mensuelle, incrémentielle quotidienne

SS Etat système relevé une fois par mois

**REMARQUE :** Alors que la quantité augmente au fil du temps, une solution de sauvegarde hors hôte peut être nécessaire.

# Archivage en utilisant la solution Dell Digital Forensics

## Archivage à la demande

Les logiciels NTP ODDM et NTP Right-Click Data Movement (RCDM) fonctionnent avec Enterprise Vault pour réduire la nécessité d'analyser l'ensemble du système de fichiers, comme dans le cas d'un archivage classique, en mettant en oeuvre l'*archivage à la demande*. Les coûts de stockage sont réduits et la qualité de l'archivage augmente.

Selon l'étape du cycle de vie des données, comme décrit dans « Correspondance entre l'archivage des preuves et l'extraction et la vie de l'affaire », page 67, l'analyste peut décider d'archiver les données à long terme ou de conserver les données pour y accéder et les traiter immédiatement.

En outre, le logiciel NTP ODDM peut être utilisé pour archiver automatiquement les données qui doivent être stockées à des fins judiciaires.

## Configuration nécessaire

Le logiciel NTP ODDM nécessite Microsoft IIS, Microsoft .NET Framework, SQL et Enterprise Vault. Les logiciels NTP ODDM et Enterprise Vault doivent être installés sur le même serveur. Les installations plus grandes peuvent gérer la base de données SQL sur un serveur dédié.

## Installation

Pour les instructions d'installation détaillées, pour les logiciels NTP ODDM et RCDM, voir le *Guide d'installation et de configuration de Dell Digital Forensics*. Voir « Documentation et ressources associées », page 15 pour plus d'informations.

## Archivage en utilisant le logiciel NTP ODDM

### Archivage géré par l'utilisateur

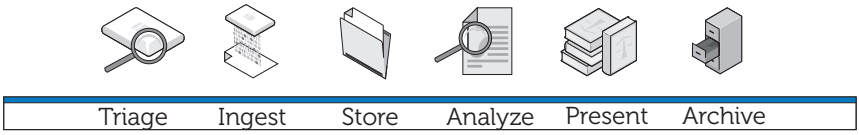
1. Lorsque l'analyste stocke des fichiers de données, le logiciel NTP QFS indique à l'utilisateur que les fichiers doivent être archivés.
2. L'analyste sélectionne les fichiers à archiver en utilisant le logiciel NTP Storage Investigator et cliquez sur **Archive**. Toutefois, si le module complémentaire NTP RCDM est installé, il clique avec le bouton droite de la souris sur les fichiers.

   Une fois les fichiers sélectionnés, le logiciel NTP Storage Investigator le signale au logiciel NTP ODDM qui active Enterprise Vault.

   La demande d'archivage est ajoutée à la file d'attente d'archivage.

# 8

# Dépannage




## Conseils généraux de dépannage

- Vérifiez que tous les clients et serveurs se voient mutuellement, qu'ils peuvent s'envoyer une commande Ping en fonction du nom NetBIOS et de l'adresse IP.
- Vérifiez que les pare-feu ne bloquent pas le trafic.
- Redémarrez les serveurs et les clients pour vérifier que toutes les modifications d'installation et de configuration ont été reconnues par les systèmes.

## Problèmes logiciels d'investigation

### EnCase: EnCase démarre en mode Acquisition

Ce problème indique que EnCase n'a pas de licence.

1. Dans EnCase sélectionnez **Tools→ Options** et définissez le **chemin de clé utilisateur**, le **chemin de clé serveur** et l'**adresse serveur** sont définis (ces champs doivent désignent les emplacements des clés de licence).
2. Vérifiez le pare-feu sur le client et le serveur de licences EnCase pour déterminer si le port 4445 est ouvert.
3. Vérifiez que le client peut envoyer une commande Ping au serveur de licences EnCase.

### FTK Lab : le navigateur lancé par le client n'affiche pas l'interface utilisateur

1. Vérifiez que le client dispose de MS Silverlight.
2. Vérifiez sur les services Oracle sont démarrés sur le serveur de la base de données Oracle.

### FTK 1.8 : message de version d'évaluation avec limite à 5 000 objets

Si vous recevez ce message, cela implique que FTK n'a pas de licence. Vérifiez que le serveur de licences réseau fonctionne et qu'il dispose des licences FTK 1.8 :

1. Ouvrez une fenêtre de navigateur sur le serveur qui héberge le service de licence réseau et entrez **http://localhost:5555** dans la barre d'adresse.
2. Vérifiez que les licences sont en place. Si tel n'est pas le cas, vous devez les installer.

### FTK 1.8 : un message d'accès impossible au fichier temporaire apparaît lors du lancement

Autorisez l'utilisateur à lancer l'application (ou sa session Citrix) pour avoir accès au disque dur du serveur OU exécuter l'application comme administrateur.

## Problèmes Citrix

### Citrix : les applications ne démarrent pas

1. Vérifiez que tous les services (notamment MFCOM et IMA) ont démarré sur les serveurs qui hébergent XenApp.
2. Vérifiez que le client peut voir et envoyer une commande Ping aux serveurs XenApp.
3. Vérifiez le pare-feu sur les clients et les serveurs XenApp pour déterminer si les ports XenApp sont ouverts.
4. Vérifiez le serveur de licences Citrix pour déterminer que le service de licence réseau dispose d'une licence qu'il peut émettre. Le service de licences Citrix est généralement installé sur l'un des serveurs Citrix XenApp accessible via **Démarrer→ Programmes→ Citrix→ Management Consoles→ Citrix Licensing**.

5 Ouvrez la **Console de gestion Citrix** (**Démarrer→ Programmes→ Citrix→ Management Consoles→ Citrix Delivery services console**). Exécutez une découverte pour vérifier que tous les serveurs XenApp sont présents dans la batterie.

6 Vérifiez que l'application a été publiée sur un serveur XenApp valide (inclus dans la batterie).

7 Consultez la **console Citrix Delivery Services** pour vérifier que l'utilisateur qui lance l'application se trouve dans un groupe autorisé à lancer l'application.

8 Pour les applications en continu, vérifiez que le contrôle de compte d'utilisateur est désactivé sur le serveur.

### Sessions Citrix gelées ou bloquées

Lorsque les utilisateurs ne se déconnectent pas de leurs sessions Citrix correctement, les sessions orphelines ralentissent et peuvent amener le serveur à se geler ou se bloquer. Par conséquent, il est très important que les utilisateurs respectent les meilleures pratiques pour fermer chaque session formellement et correctement (**Démarrer→ Logoff→ Ok**) et qu'ils ne se limitent pas à cliquer sur la croix (*x*) dans l'angle supérieur droit de la fenêtre de session.

Toutefois, ce problème peut continuer d'apparaître. Vous pouvez le résoudre des deux manières suivantes :

1 Déconnectez manuellement l'utilisateur.

   a Ouvrez une session comme administrateur Citrix.

   b Vérifiez la liste des sessions ouvertes et fermez manuellement chaque session.

2 Redémarrez le serveur.

# Index

## T