Dell™ Digitale Forensiklösung

Lösungshandbuch

Anmerkungen, Vorsichtshinweise und Warnungen

ANMERKUNG: Eine ANMERKUNG macht auf wichtige Informationen aufmerksam, mit denen Sie den Computer besser einsetzen können.

VORSICHT: Durch VORSICHT werden Sie auf Gefahrenquellen hingewiesen, die Hardwareschäden oder Datenverlust zur Folge haben können, wenn die Anweisungen nicht befolgt werden.

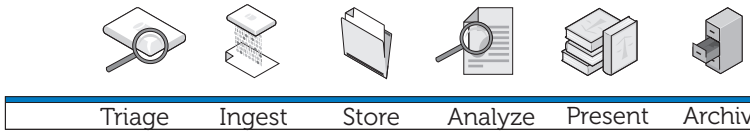
WARNUNG: Mit WARNUNG wird auf eine potenziell gefährliche Situation hingewiesen, die zu Sachschäden, Verletzungen oder zum Tod führen kann.

2011 - 07 **Rev. A00**

Inhalt

1

Einführung



In den letzten Jahren ließ sich weltweit ein exponentielles Wachstum hinsichtlich der Anzahl, Schnelligkeit, Vielfältigkeit und Raffinesse der Cybertätigkeit von Kriminellen und Terrorgruppen beobachten. Heutzutage weisen die meisten Straftaten eine digitale Komponente auf. Nicht wenige bezeichnen dies als *digitalen Tsunami*. Dieses Wachstum wurde durch die dramatischen Fortschritte in Bereich elektronischer Hardware vorangetrieben. Die zunehmende Vielfalt elektronischer Endgeräte und deren immer größer werdende Speicherkapazität bieten Kriminellen und Terroristen ungeahnte Möglichkeiten, wenn es darum geht, schädigende oder gefährliche Informationen zu verbergen.

Es ist nicht ungewöhnlich, dass PCs und Laptops über Festplatten mit Hunderten GB an Speicher verfügen. Die neuesten Festplatten bieten zum Teil 1-4 TB. Ein Terabyte entspricht dem Inhalt von bis zu 200 DVDs, also einer riesigen Speichermenge und damit einem Problem, das sich in Zukunft noch verschärfen wird.

Ob PCs oder Laptops, Mobiltelefone oder USB-Sticks und sogar Spielekonsolen – in der digitalen Kriminaltechnik stoßen Analytiker beim Klonen, Erfassen, Indizieren, Analysieren und Speichern einer wachsenden Menge verdächtiger Daten an ihre Grenzen, während gleichzeitig die digitale Kontrollkette gewahrt werden muss und der Schutz der Bürger nicht zu vernachlässigen ist.

Tabelle 1-1. Wie groß ist ein Zettabyte?

Kilobyte (KB)	1.000 Byte	2 KB	eine maschinengeschriebene Seite
Megabyte (MB)	1.000.000 Byte	5 MB	das vollständige Werk Shakespeares
Gigabyte (GB)	1.000.000.000 Byte	20 GB	eine umfangreiche Sammlung der Werke von Beethoven
Terabyte (TB)	1.000.000.000.000 Byte	10 TB	eine akademische Forschungsbibliothek
Petabyte (PB)	1.000.000.000.000.000 Byte	20 PB	jährliche Produktion von Festplattenlaufwerken
Exabyte (EB)	1.000.000.000.000.000.000 Byte	5 EB	alle jemals von der menschlichen Rasse gesprochenen Wörter
Zettabyte (ZB)	1.000.000.000.000.000.000.000 Byte	2 ZB	erwartete Menge weltweit erstellter Daten im Jahr 2010*

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

Wenn unter Verdacht stehende Kriminelle angeklagt und Computer sowie andere digitale Quellen beschlagnahmt wurden, stehen die Experten der digitalen Kriminaltechnik unter enormem Druck, potenzielles Beweismaterial in kürzester Zeit und in Umgebungen, die für die Anforderungen zur Beweissicherung nicht unbedingt ideal geeignet sind, zu verarbeiten und zu analysieren. Wenn ganze Organisationen krimineller oder terroristischer Aktivitäten verdächtigt werden, erhöht sich die Anzahl der zu analysierenden Geräte u. U. dramatisch.

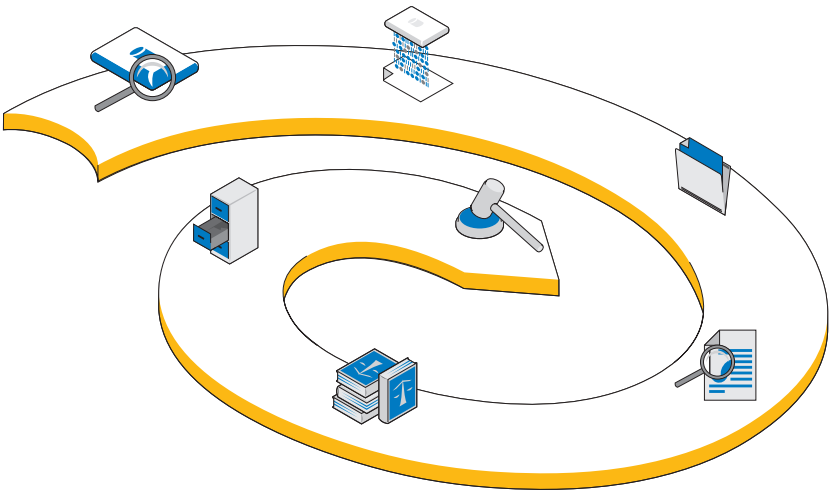
Die digitale Forensik stellt Mittel zur Verfügung, um von Computern oder anderen Digitalgeräten (Mobiletelefonen, Spielekonsolen, Flash-Laufwerken, GPS-Geräten usw.) abgerufene Daten zu erfassen und diese Daten auf eine Weise wissenschaftlich zu untersuchen und zu analysieren, dass die gewonnenen Informationen auch vor Gericht verwendet werden können. Die digitale Kriminaltechniklösung von Dell umfasst die erste echte End-to-End-Organisationslösung, mit der Strafverfolgungsbehörden, Sicherheitsstellen in Unternehmen und Verwaltung sowie E-Discovery-Organisationen die Hardware und Software sowie den Service und Support für die Sammlung, Sichtung, Erfassung und Image-Erstellung, Speicherung, Analyse, Berichterstellung und Archivierung von digitalem Beweismaterial erhalten.

Dank Dells skalierbarer und günstiger Enterprise-Server- und -Speicherhardware sowie – abhängig von den Anforderungen Ihrer Softwareumgebung – Oracle-Datenbanksystemen als Backend, der Verbindung von extrastabilen Dell-Laptops und der SPEKTOR-Software während Außeneinsätzen und durch den Komplettservice und -Support von Dell können Ermittler Daten schnell und einfach digital-kriminaltechnisch sichten und erfassen – mit einer ununterbrochene Kontrollkette, angefangen vom Tatort über das Rechenzentrum bis in den Gerichtssaal.

Digitaler forensischer Lebenszyklus nach Dell

Die digitale Kriminaltechniklösung von Dell unterstützt forensische Ermittler während der sechs Phasen im forensischen Lebenszyklus: Sichtung, Erfassung, Speicherung, Analyse, Präsentation und Archivierung.

Abbildung 1-1. Digitaler forensischer Lebenszyklus nach Dell



Sichtung

Der Sichtungsprozess gibt der digitalen Kriminaltechnik die Gelegenheit, sich einen schnellen Überblick über den Inhalt der Zielgeräte zu verschaffen, um zu bestimmen, ob ein Gerät zur Analyse und Vorbereitung auf eine Präsentation vor Gericht ins Labor verbracht werden soll.

Erfassung

Die Erfassung ist die Phase der digitalen Kriminaltechnik, in der ein Image der Zieldaten (es sei denn, die Daten wurden im Außeneinsatz während der Sichtungsphase erstellt) und eine exakte Kopie des verdächtigen Speichergeräts erstellt werden, und zwar so, dass die Integrität des Duplikats sichergestellt ist. Hierzu werden die Hashes der ursprünglichen und duplizierten Datenlaufwerke verglichen.

Gemäß bestehender Praxis wird ein *Image* der verdächtige Daten in der digitalen Kriminaltechniklösung von Dell erstellt. Statt der Daten-Image-Erstellung auf einer Workstation werden die Daten jedoch in einem zentralen Beweismaterial-Repository erfasst. Durch die sofortige Erfassung der Daten im Rechenzentrum stehen die Daten mehreren Analytikern zur Verfügung, werden der Übertragungsaufwand zwischen einzelnen Geräten minimiert und die Produktivität und Effizienz deutlich erhöht. Eine Erfassung ist jedoch auch während des Außeneinsatzes möglich, sofern die Kapazität des Zielspeichers entsprechend klein ist. Die digitale Kriminaltechniklösung von Dell bietet über ein optionales SPEKTOR Imager-Moduls die Möglichkeit zur Vor-Ort-Erfassung.

Speicherung

Die digitale Kriminaltechniklösung von Dell umfasst verschiedenste, für die jeweiligen Kundenanforderungen geeignete Speicher- und Netzwerkzugriffsoptionen. High-Speed-Speicherung und -Abruf im gesamten Organisationsnetzwerk ermöglichen eine Mehrfachbenutzer-Konfiguration, die die Effizienz und Produktivität erhöhen. Analytiker sind nicht länger gezwungen, ihr eigenen Computerressourcen für Beweisanalysen aufzuwenden, da alle diese Vorgänge auf einem hierzu vorgesehenen Server durchgeführt werden.

Analyse

Dank der parallelen Verarbeitungsfunktionen der digitalen Kriminaltechniklösung von Dell kann der Analytiker Daten auf Hochleistungsservern, anstatt auf weitaus weniger leistungsstarken Einzel-PCs indizieren und sichten. Darüber hinaus ist es möglich, mithilfe der Back-End-Konfigurationen der Lösung mehrere Analytikersitzungen gleichzeitig auf einer oder mehreren Workstations auszuführen. Diese Funktion trägt u. a. zum Schutz des Systems und der Integrität von Beweismaterial sowie zum Erhalt der Kontrollkette bei.

Außerdem entfällt ein Neuaufsetzen der Workstations, sollte bösartiger Code versehentlich ausgeführt werden oder die Arbeit an einem neuen Fall beginnen. In einer digitalen Forensik-Umgebung lässt sich der Begriff *Kontrollkette* wie folgt definieren: als Erhalt der Beweismaterial-Integrität von der Erfassung über die Vorstellung der Ergebnisse bis zur möglichen Präsentation vor Gericht.

Präsentation

Mithilfe der digitalen Kriminaltechniklösung von Dell sind zur Beweismaterialbewertung verantwortliche Teams und Ermittler in der Lage, auf potenzielles Beweismaterial eines Falles sicher und in Echtzeit zuzugreifen. Auf diese Weise lässt sich vermeiden, Beweismaterial auf DVD freigeben zu müssen oder Sachverständige anreisen zu lassen, damit sie im Labor auf Daten zugreifen können.

Archivierung

Die Dell-Lösung bietet eine formalisierte Sicherungs-, Wiederherstellungs- und Archivierungsinfrastruktur, um die Zusammenarbeit zwischen Behörden und Sicherheitsabteilungen, auch grenzüberschreitend, zu optimieren, den Verwaltungsaufwand zu reduzieren, Konsistenz zwischen Laboren zu gewährleisten und Risiken für den Erhalt der digitalen Kontrollkette zu minimieren.

Außerdem umfasst das Design der digitalen Kriminaltechniklösung von Dell eine optionale Suchkomponente zum Aufspüren von Übereinstimmungen zwischen erfassten Datensätzen.

Dell-Lösung: Abhilfe für Branchenprobleme

Durch Verwendung der digitalen Kriminaltechniklösung von Dell ist es für Ermittler deutlich einfacher, digitales Beweismaterial vom Tatort in den Gerichtssaal zu schaffen, und zwar durch:

- sich auf dem neuesten Stand der Technik befindliche Netzwerke im Rechenzentrum, die die Erfassung, Analyse und gemeinsame Nutzung digitaler Daten beschleunigen
- Informationssicherheit durch eine weitere Automatisierung des digitalen forensischen Prozesses, dadurch Verringerung des Fehlerrisikos und der Gefahr von Datenveränderungen

- zusätzliche Sicherheit in puncto Datenintegrität, derzeit durch die Verwendung von Hash-Protokollen mit dem höchsten Sicherheitsstandard, und demnächst durch Implementierung einer Audit-Funktion zur automatisierten Aufzeichnung der Kontrollkette

ANMERKUNG: Alle in diesem Dokument beschriebenen Schlussfolgerungen bzw. Empfehlungen, die ggf. rechtsberatend wirken oder erscheinen, sollten durch einen Rechtsbeistand gründlichen geprüft werden. Setzen Sie sich mit dem in Ihrer Region zuständigen Gericht, der Staatsanwaltschaft und den kriminaltechnischen Laboren vor Ort hinsichtlich ihrer bevorzugte(n) Methode(n) bei der Sammlung digitalen Beweismaterials in Verbindung.

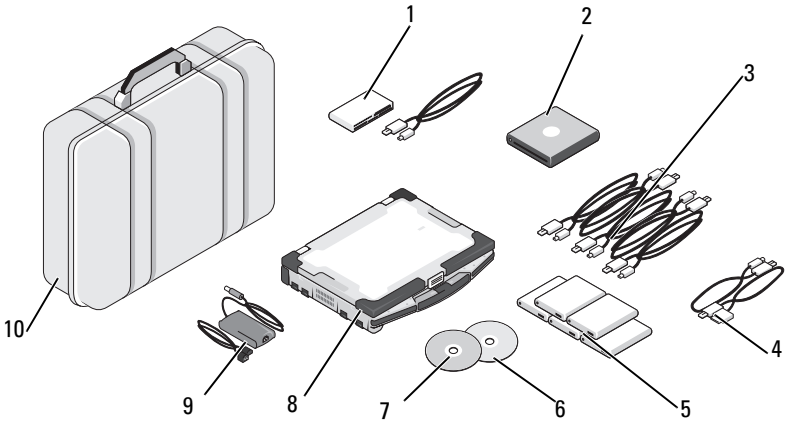
- eine End-to-End-Lösung, die die Komplexität bei Planung, Implementierung und Verwaltung digitaler forensischer Prozesse auf Organisationsebene beträchtlich vereinfacht
- eine günstige und flexible, modulare und skalierbare „Pay-as-you-go"-Lösung

Lösungskomponenten

Im Außeneinsatz

Die Mobilkomponenten der Lösung passen in einen Hartschalenkoffer, der sich im Handgepäckfach eines Flugzeugs verstauen lässt. Der Schutzkoffer bietet Platz für sämtliche Werkzeuge und Software, die zur Vor-Ort-Sichtung verdächtiger Speichergeräte erforderlich sind, und enthält einen extrastabilen Dell E6400 XFR-Laptop mit vorinstallierter SPEKTOR-Forensik-Software, forensische Tableau-Schreibblockern mit Zubehör, eine optionale Anzahl externer USB-Laufwerke, die für den Einsatz mit SPEKTOR-Software als Triage-Image-*Collectors* lizenziert sind, ein 50:1-Kartenleser sowie die in Abbildung 1-2 aufgeführten Adapter und Kabel.

Abbildung 1-2. Digitale Kriminaltechniklösung von Dell: Mobilkomponenten



1	50:1-Kartenleser	6	Image-Wiederherstellungsdatenträger
2	USB-DVD-ROM	7	Startfähiger SPEKTOR-Datenträger
3	Collector-USB-Kabel	8	Extrastabiler Dell-Laptop
4	Telefonkabel für SPEKTOR PI (optional)	9	Stromversorgung für den extrastabilen Dell-Laptop
5	Externe Festplatten-Collectors (5)	10	Schutzkoffer

Im Rechenzentrum

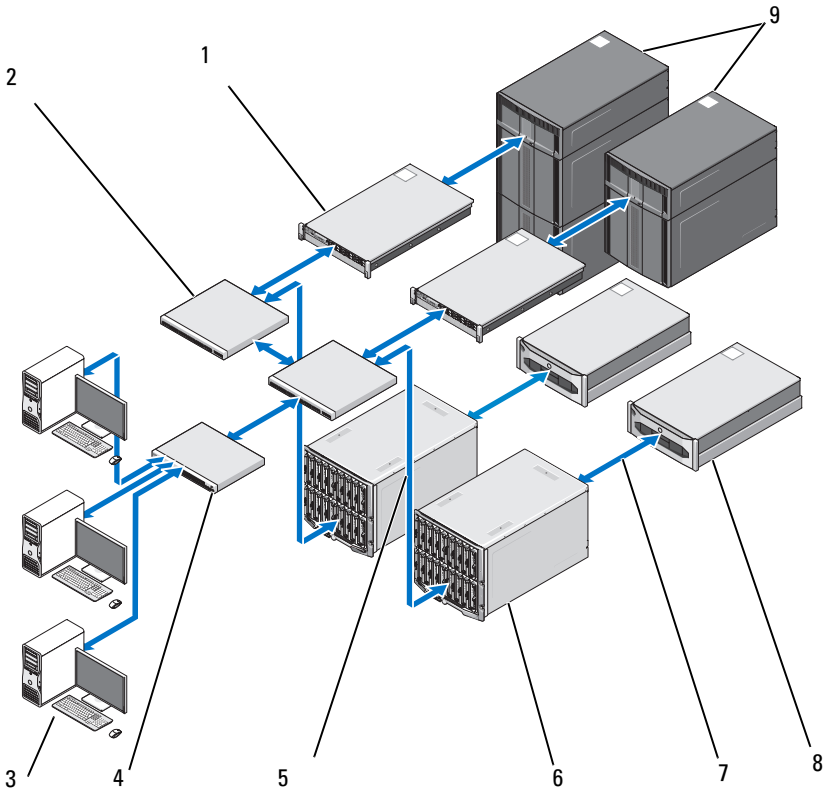
Im Rechenzentrum umfasst die digitale Kriminaltechniklösung von Dell eine individuell angepasste Konfiguration folgender Komponenten:

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

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

Die Dell PowerEdge Rack- und Blade-Server können in verschiedensten Rollen fungieren: als Dateiserver, Beweismaterialserver, Archivserver, Datenbankserver, EnCase- und FTK-Lizenzserver, Sicherungsserver oder Domänencontroller. Sie bieten Unterstützung für Microsoft Active Directory sowie sämtliche Sicherheits- und Forensik-Software der digitalen Kriminaltechniklösung von Dell.

Abbildung 1-3. Digitale Kriminaltechniklösung von Dell: Rechenzentrum



1	PowerEdge R410-Server oder R610-Server (optional)	6	Dell PowerEdge M1000E und M610 Blade-Server
2	Dell PowerConnect-Switch	7	10-GB-Datenstrom
3	Dell Precision- oder OptiPlex-Workstation	8	Dell EqualLogic-Speichersysteme der Serie PS4000 oder PS6000
4	Dell PowerConnect-Switch	9	Dell PowerVault ML-Speicher
5	1-GB-Datenstrom		

Über dieses Dokument

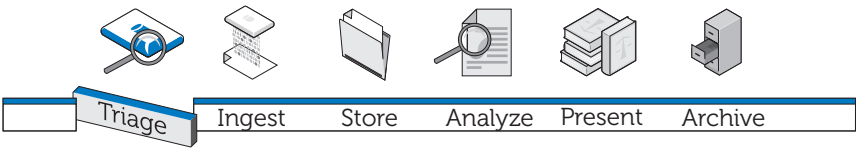
Dieses Dokument beschreibt jede Phase des digitalen forensischen Prozesses in einem eigenen Kapitel, mit zusätzlichen Kapiteln zur Fehlerbehebung und der von der Lösung unterstützten Hardware sowie Software. Jedes der Kapitel beginnt mit einer Erläuterung bewährter Verfahren und spezifischer Probleme, auf die Sie ggf. beim Implementieren und Verwalten der Lösung stoßen. Im Anschluss daran werden Ihnen die verschiedenen Werkzeuge und Komponenten der jeweiligen Phase Schritt für die Schritt vorgestellt.

Relevante Dokumentation und Ressourcen

Über **support.dell.com/manuals** können Sie auf zusätzliche Informationen zugreifen.

2

Sichtung



Was bedeutet Sichtung?

Die Sichtung (Englisch: „Triage“) ermöglicht im Bereich der digitalen Kriminaltechnik, die auf verdächtigen Geräten befindlichen Daten zu durchsuchen und zu entscheiden, bei welchen Geräten sich tatsächlich Beweismaterial finden lässt und sich eine Beschlagnahme zur lokalen Image-Erstellung (falls die Daten nicht zu umfassend sind) oder spätere Image-Erstellung im Rechenzentrum lohnt. Dank dieser Vorschaufunktion und einer Beschlagnahme von nur ausgewählten Zielgeräten werden Ermittler in die Lage versetzt, Beweise zeitnah zu präsentieren, da es zu weniger Verzögerungen kommt. Durch eine Sichtung lässt sich die Menge der im forensischen Labor zur Image-Erstellung vorgesehenen Speichergeräte reduzieren. So werden nicht nur weniger Ressourcen belegt und eine zusätzliche Belastung einer bereits übervollen Warteschlange verhindert, vielmehr werden auch die Betriebskosten drastisch gesenkt.

Die Vorteile der Triage-Lösung von Dell

Mobil

Die digitale Kriminaltechniklösung von Dell kann vom Ermittler direkt am Tatort eingesetzt werden. Im Rahmen eingehender Tests wurden alle Komponenten auf eine einwandfreie Zusammenarbeit geprüft. Sie decken zudem eine Vielzahl der im Außeneinsatz möglicherweise anzutreffenden Ports und Anschlüssen von Zielgeräten ab.

Schnell

Vorhandene forensische Triage-Lösungen können nicht nur langsam sein, ihnen entgehen u. U. sogar Daten, da Vorgänge wie Stichwortsuche oder Hash-Abgleich während der Datenerfassung durchgeführt werden. Die digitale Kriminaltechniklösung von Dell überwindet dieses Problem, indem zur Analyse der gesammelten Daten die Rechenleistung des extrastabilen Dell-Laptops und nicht die des Ziel-PCs genutzt wird. Unter bestimmten Umständen ist es sogar möglich, auf die Image-Erstellung und Indizierung im forensischen Labor komplett zu verzichten.

Benutzerfreundlich

Die Sichtungskomponenten der Lösung können direkt und ohne vorherige Anpassungen eingesetzt werden. Die vorinstallierte Software verfügt über eine intuitive Touchscreen-Oberfläche, und es ist möglich, benutzerdefinierte, wiederverwendbare Erfassungsprofile für unterschiedliche Szenarien für den standardmäßigen Gebrauch zu erstellen.

Kriminaltechnisch zulässig

Triage-Software setzt einen effizienten und kriminaltechnisch zulässigen Prozess durch, so dass potenzielles Beweismaterial ohne Wenn und Aber gesammelt, geprüft und gespeichert wird.

Flexibel

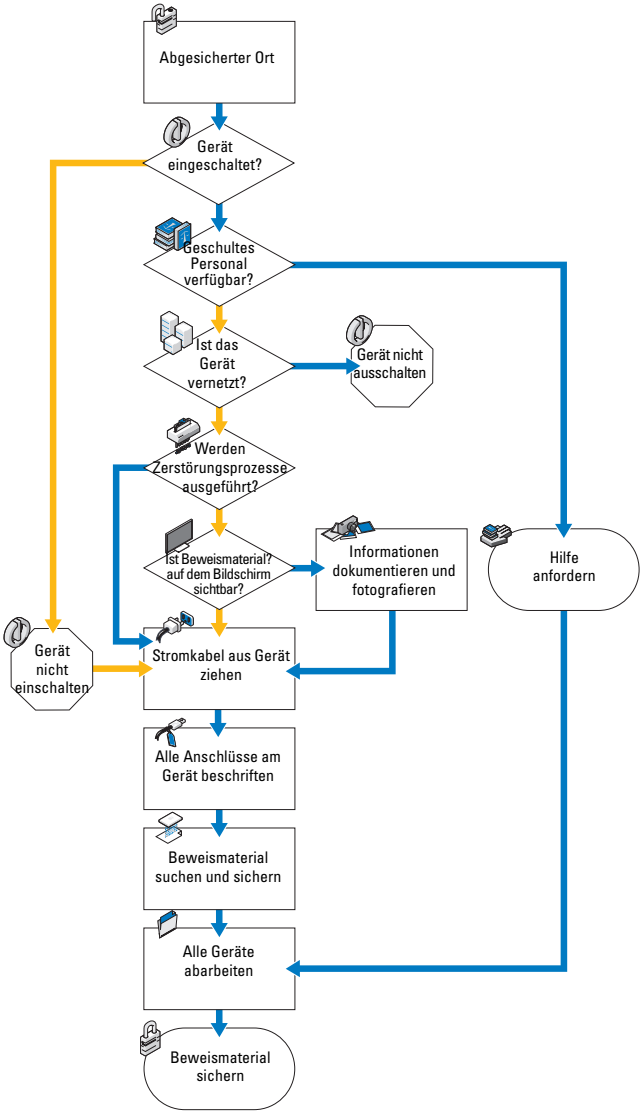
Die Sichtungskomponenten sind zur Untersuchung der gängigsten Plattformen, darunter Geräte mit Windows- und Apples Mac OS X-Betriebssystemen, sowie verschiedensten Typen digitaler Speichergeräte, etwa MP3-Player, externe Festplatten, Speicherkarten, Mobil- und Satellitentelefone, GPS-Geräte, iPads und iPhones sowie Flashlaufwerke, geeignet. Darüber hinaus lassen sich die Sichtungsergebnisse mithilfe der digitalen Kriminaltechniklösung von Dell in andere Programme exportieren.

Leistungsstark

Der extrastabile Dell-Laptop steuert den vollständigen Prozess, von der automatisierten Analyse der Zieldaten bis hin zur Ausgabe detaillierter Ergebnisse in einem benutzerfreundlichen Berichtsformat nur Minuten nach der Datenerfassung. Durch die Dell-Lösung wird der Ermittler in die Lage versetzt, mit nur einem Lizenzschlüssel mehrere Sichtungsvorgänge gleichzeitig auszuführen.

Sammlung von digitalem forensischen Beweismaterial

Abbildung 2-1. Ablaufdiagramm der Beweissammlung



Standard- und Live-Erfassung

Die digitale Kriminaltechniklösung von Dell bietet zwei Arten der Erfassung: Standard und Live. Während einer Standarderfassung nutzt der extrastabile Dell-Laptop den startfähigen SPEKTOR-Datenträger, um die Sichtungsdaten von einem bereits ausgeschalteten Zielspeichergerät zu erfassen. Bei einer Live-Erfassung als Sichtungsverfahren sollen wiederum Sichtungsdaten von einem noch eingeschalteten Zielspeichergerät erfasst und damit sonst nicht verfügbares Beweismaterial sichergestellt werden.

Früher musste der Ermittler laut Industriestandards das Zielgerät ausstecken und ein digitales Gerät zum Transport und zur Untersuchung im Labor verwenden. Diese Praxis bedeutete den Verlust potenziell wertvollen Beweismaterials in Form gespeicherter flüchtiger Daten. Beispiele hierzu: in der Zwischenablage gespeicherte Daten, aktuell geöffnete Dateien, RAM-Inhalt, zwischengespeicherte Kennwörter usw. Außerdem gehen verschlüsselte Daten u. U. verloren, wenn der Computer vor der Image-Erstellung der Festplatte heruntergefahren wird. Darüber hinaus verfügen viele Computer über benutzerdefinierte BIOS- und Festplattenkennwörter. Wenn ein Live-System mit einem BIOS-Kennwort von der Stromversorgung getrennt wird, geht damit u. U. der Zugriff auf sämtliche Daten des Geräts verloren.

Gemäß den sich in der Branche bewährten Verfahren haben Ermittler beim ersten Umgang mit einem verdächtigen Datenspeichergerät folgende Leitlinien zu berücksichtigen:

- Ein eingeschaltetes Gerät ist so lange eingeschaltet zu lassen, bis eine gründliche Untersuchung durchgeführt werden kann.
- Ein ausgeschaltetes Gerät ist ausgeschaltet zu lassen.

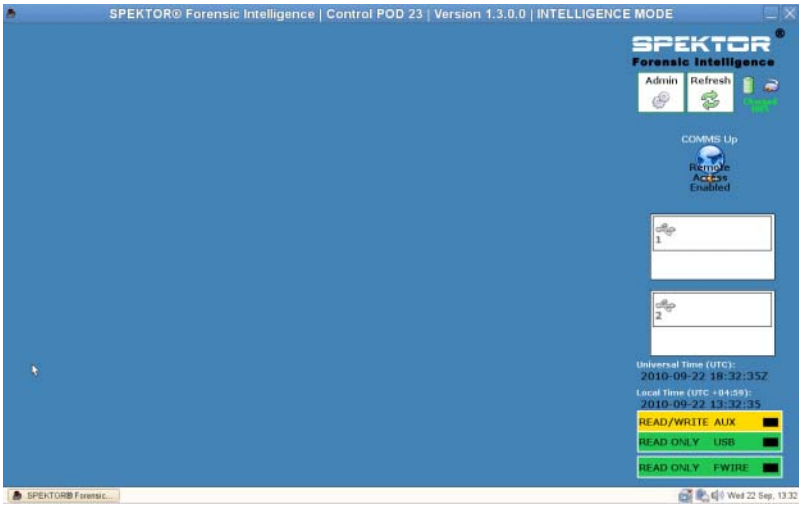
Der Hintergrund für diese Leitlinien: Der Ermittler muss vorsichtig agieren, damit das Speichergerät in dem am jeweiligen Ort gefundenen Zustand erhalten wird und Gerät und Inhalt möglichst unverändert bleiben.

Sichten mit der digitalen Kriminaltechniklösung von Dell

Einschalten des extrastabilen Dell-Laptops

1. Drücken Sie die Einschalttaste, um sich beim extrastabilen Dell-Laptop anzumelden. Der Laptop lädt automatisch die SPEKTOR-Software.
2. Tippen oder klicken Sie auf **Accept EULA**. Der **Startbildschirm** wird geöffnet.

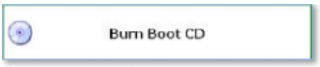
Abbildung 2-2. Startbildschirm



Brennen einer startfähigen CD für standardmäßige Erfassungsverfahren

1 Tippen oder klicken Sie auf dem **Startbildschirm** auf **Admin**. Tippen oder klicken Sie anschließend auf **Burn Boot CD**.

Abbildung 2-3. Option „Burn Boot CD" auf dem Startbildschirm



2 Folgen Sie den Anweisungen auf dem Bildschirm und klicken Sie dann auf **Finish**.

Registrieren eines Collector oder Speicherdatenträgers

ANMERKUNG: Vor einem Einsatz mit der digitalen Kriminaltechniklösung von Dell muss ein Collector zunächst von SPEKTOR lizenziert und konfiguriert werden. Wenden Sie sich an Ihren Systemadministrator, wenn Sie weitere Collectors oder Lizenzen benötigen.

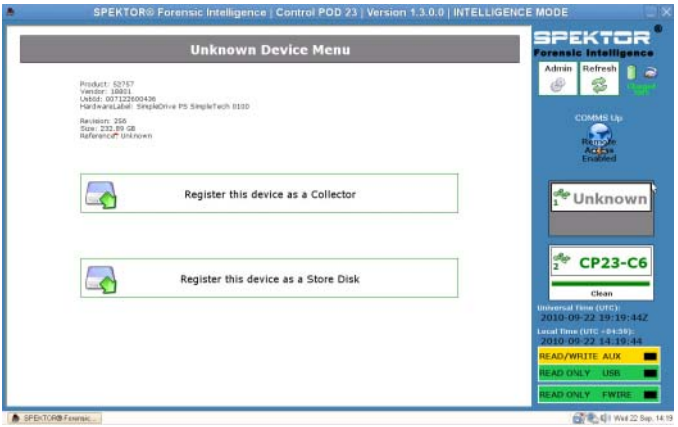
1 Stecken Sie einen neuen Collector bzw. Speicherdatenträger in einen der USB-Anschlüsse auf der linken Seite des extrastabilen Dell-Laptops. Das Gerät wird auf dem Bildschirm als unbekanntes Gerät gemeldet.

Abbildung 2-4. Anzeige für unbekannten Collector bzw. Speicherdatenträger

2 Tippen oder klicken Sie auf das **Statusanzeige**-Symbol, das dem an den extrastabilen Dell-Laptop angeschlossenen Collector bzw. Speicherdatenträger entspricht. Das Symbol für das registrierte Gerät wird bei einem Collector grün, bei einem Speicherdatenträger orange.

3 Der Bildschirm **Unknown Device Menu** wird angezeigt.

Abbildung 2-5. Unknown Device Menu



4 Tippen oder klicken Sie auf **Register this device as a Collector** oder **Register this device as a Store Disk**.

5 Tippen oder klicken Sie auf **Yes**.

In der Statusanzeige wird die Nummer des neuen Collector bzw. Speicherdatenträgers angezeigt, und der Status ändert sich zu **Dirty**.

Abbildung 2-6. Unbereinigt-Symbole für Collector und Speicherdatenträger

ANMERKUNG: Collectors und Speicherdatenträger, ob neu registriert oder bereits bei anderen Datenerfassungen verwendet, müssen bereinigt werden, bevor Sie auf ein Ziel angewendet werden können.

6 *Nur für Speicherdatenträger*: Geben Sie die Seriennummer des Speicherdatenträgers ein.

Bereinigen eines Collector oder Speicherdatenträgers

ANMERKUNG: Planen Sie ca. zwei Stunden pro 100 GB Collector-Umfang ein.

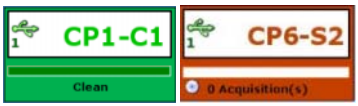
1 Wählen Sie die **Statusanzeige** für den zu bereinigen Collector aus.

2 Tippen oder klicken Sie im **Collector Menu** auf **Clean Collector**.

3 Tippen oder klicken Sie auf **Yes**, um Ihre Auswahl zu bestätigen. Daraufhin wird der Bereinigungsvorgang gestartet, und über die **Statusanzeige** wird der Reinigungsfortschritt angezeigt.

Nach Abschluss der Bereinigung führt die Software ein Prüfprogramm aus, um sicherzustellen, dass die Null das einzig verbliebene Zeichen auf dem Collector-Laufwerk ist.

Abbildung 2-7. Statusanzeige für registrierte, bereinigte Collectors und Speicherdatenträger



ANMERKUNG: War der Bereinigungsvorgang nicht erfolgreich, gibt die Statusanzeige an, dass der Collector nach wie vor in unbereinigtem Zustand vorliegt. In diesem Fall müssen Sie den Bereinigungsvorgang neu starten. Schlägt die Bereinigung ein zweites Mal fehl, wiederholen Sie den Vorgang mit einem anderen Collector oder Speicherdatenträger.

Konfigurieren eines Collector-Profils

ANMERKUNG: Standardmäßig sind die Konfigurationseinstellungen in der Triage-Software so eingestellt, dass keine Dateien gesammelt werden. Geben Sie einen eingeschränkten Teilsatz aller Dateien auf dem Zielgerät an, um die zur Erfassung benötigte Zeit zu reduzieren und eine Überschreitung der Collector-Kapazität zu vermeiden.

Durch Konfiguration eines Collector kann der Benutzer eine Reihe bestimmter Dateitypen oder in einem bestimmten Datumsbereich erstellte Dateien festlegen. Anhand dieser Kriterien zieht der Collector dann zwecks Sichtung Daten von dem verdächtigen Speichergerät. Je genauer die Sammelparameter definiert sind, desto schneller lassen sich die Zieldaten für eine Prüfung erfassen.

Dell empfiehlt die Erstellung verschiedener standardmäßiger Konfigurationsprofile zur wiederholten Verwendung durch den Benutzer oder die Behörde. Hier einige Beispiele für solche standardmäßigen Konfigurationsprofile:

- Mit dem Profil „Fotos und Videos“ ließen sich z. B. mit Fotos, Videos und anderen visuellen Medien verknüpfte Dateitypen wie ***.jpg**, ***.png**, ***.swf**, ***.vob** und ***.wmv** erfassen.
- Mit dem Profil „Dokumente“ ließen sich insbesondere alle Dokumente mit Dateitypen wie ***.pdf**, ***.doc**, ***.docx** und ***.txt** erfassen.
- Mit dem Profil „Audiodateien“ ließen sich ***.mp3**, ***.mp4**, ***.wav** und andere Audiodateien erfassen.

Konfigurieren eines Collector zur Erfassung

ANMERKUNG: Eine Erläuterung zu den Unterschieden zwischen einer Standard- und Live-Erfassung finden Sie unter „Standard- und Live-Erfassung“ auf Seite 20.

ANMERKUNG: Wenn ein Collector für eine Standard- oder Live-Erfassung konfiguriert werden soll, muss dieser zunächst bereinigt werden. Erst dann kann der Collector zur Verwendung für die andere Erfassungsform konfiguriert werden.

1 Tippen oder klicken Sie im **Collector Menu** auf **Configure Collector**.

Abbildung 2-8. Collector Menu

2 Wenn Sie ein zuvor erstelltes Konfigurationsprofil verwenden möchten, wählen Sie das Profil aus und tippen oder klicken Sie auf **Configure using selected profile**, um mit der Konfiguration des Collector zu beginnen. Tippen oder klicken Sie andernfalls auf **New**, um ein neues Profil zu erstellen.

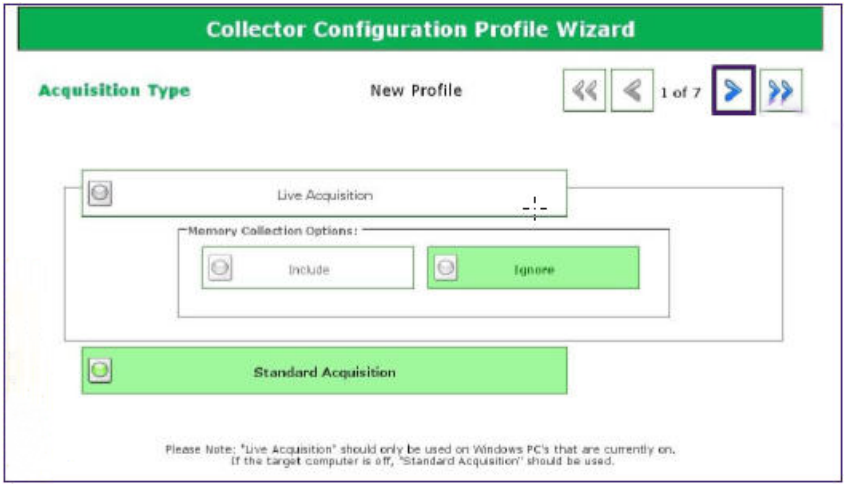
ANMERKUNG: Abbildung 2-9 zeigt den Bildschirm **Selected Profile** bei der ersten Softwareverwendung, also vor der Erstellung und Speicherung von Profilen. Wenn Konfigurationsprofile erstellt wurden, werden diese in diesem Bildschirm zu Ihrer Verwendung angezeigt.

ANMERKUNG: Um zwischen den einzelnen Bildschirmen zur Collector-Konfiguration zu wechseln, tippen oder klicken Sie auf oben auf die auf einer Seite des Bildschirms befindlichen Links- und Rechtspfeile.

Abbildung 2-9. Bildschirm „Selected Profile“

3 Legen Sie fest, welche Art von Erfassung durchgeführt werden soll: Live oder Standard. (Weitere Informationen zu den Unterschieden einer Live- und Standarderfassung finden Sie unter „Standard- und Live-Erfassung“ auf Seite 20.) Tippen oder klicken Sie dann auf **Live Acquisition** oder **Standard Acquisition**.

Abbildung 2-10. Schritt 1 der Profilkonfiguration: Fenster „Acquisition Type“



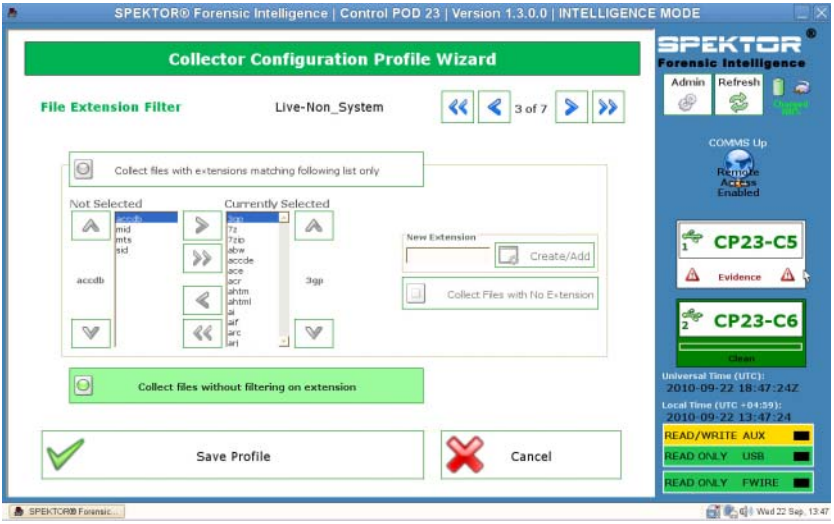
4 Legen Sie die Zeitmarken-Einstellungen für Ihr neues Profil fest. Je genauer Ihre Angabe, desto schneller werden die gesammelten Daten verarbeitet.

Abbildung 2-11. Schritt 2 der Profilkonfiguration: Zeitmarken-Einstellungen für Dateien

5 Klicken Sie oben rechts auf dem Bildschirm auf den Rechtspfeil.

6 Wählen Sie im Bildschirm **File Extension Filter** die zu sammelnden Dateitypen aus. Verschieben Sie mithilfe des Rechtspfeils die ausgewählten Dateitypen und ihre entsprechenden Erweiterungen vom Listenfeld **Not Selected** in das Listenfeld **Currently Selected**.

Abbildung 2-12. Schritt 3 der Profilkonfiguration: Fenster „File Extension Filter“



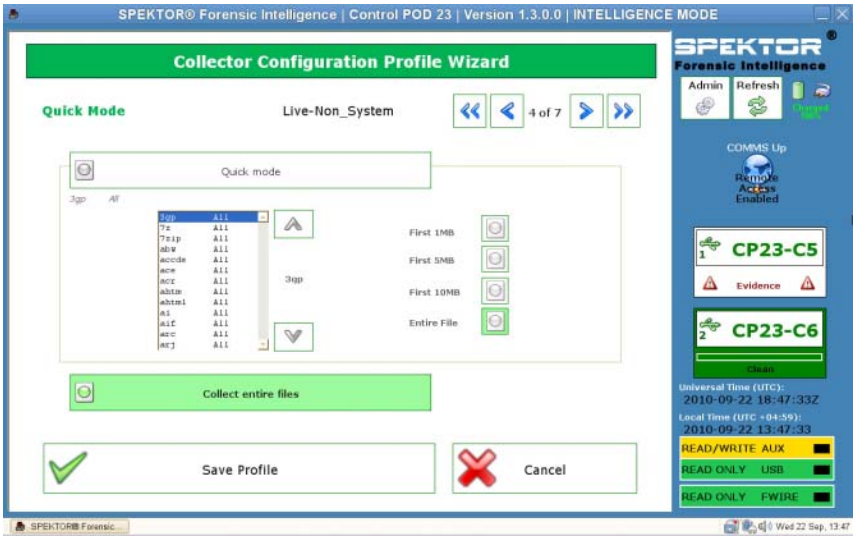
7 Klicken Sie nach Auswahl der gewünschten Dateitypen und Erweiterungen oben rechts auf dem Bildschirm auf den Rechtspfeil.

ANMERKUNG: Sofern nicht erforderlich, wird empfohlen, von einer Aktivierung des Schnellmodus (Quick Mode) abzusehen.

8 Wählen Sie im Bildschirm **Quick Mode** die Megabyte-Menge (**1 MB**, **5 MB**, **10 MB**, oder **Entire File**) des ersten Teils der zu erfassenden Daten. Wenn nur der erste Teil sehr großer Dateien (gewöhnlich Multimedia-Dateien) gesammelt werden, sind Sie in der Lage, genügend Dateien zu überprüfen, um die Thematik bei minimierter Verarbeitungszeit zu bestimmen.

ANMERKUNG: Wenn Sie in Schritt 6 keine Dateierweiterungen ausgewählt haben, werden keine Dateien gesammelt und keine Dateitypen zur Auswahl auf diesem Bildschirm angezeigt. Kehren Sie zu Schritt 6 zurück und wählen Sie die erforderlichen Dateitypen zur Aktivierung in Schritt 8 aus.

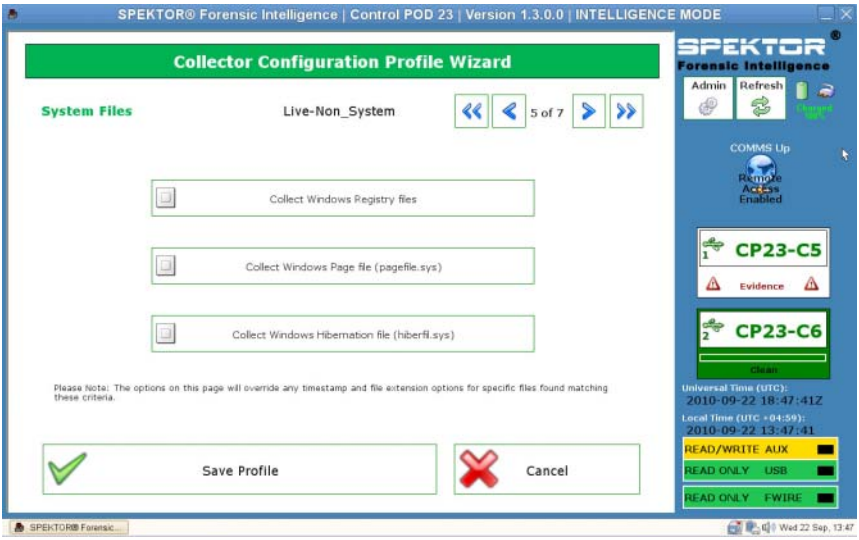
Abbildung 2-13. Schritt 4 der Profilkonfiguration: Fenster „Quick Mode“



9 Klicken Sie oben rechts auf dem Bildschirm auf den Rechtspfeil.

10 Tippen oder klicken Sie auf die entsprechende Schaltfläche, um die in Ihre Sammlung einzuschließenden Systemdateien auszuwählen.

Abbildung 2-14. Schritt 5 der Profilkonfiguration: Fenster „System Files“



11 Klicken Sie oben rechts auf dem Bildschirm auf den Rechtspfeil.

12 Legen Sie im Bildschirm **Deleted File Filter** fest, ob Live- und gelöschte Dateien, ausschließlich Live-Dateien oder ausschließlich gelöschte Dateien in Ihrer Sammlung eingeschlossen werden sollen. Wird keine dieser Optionen ausgewählt, werden keine Dateien gesammelt.

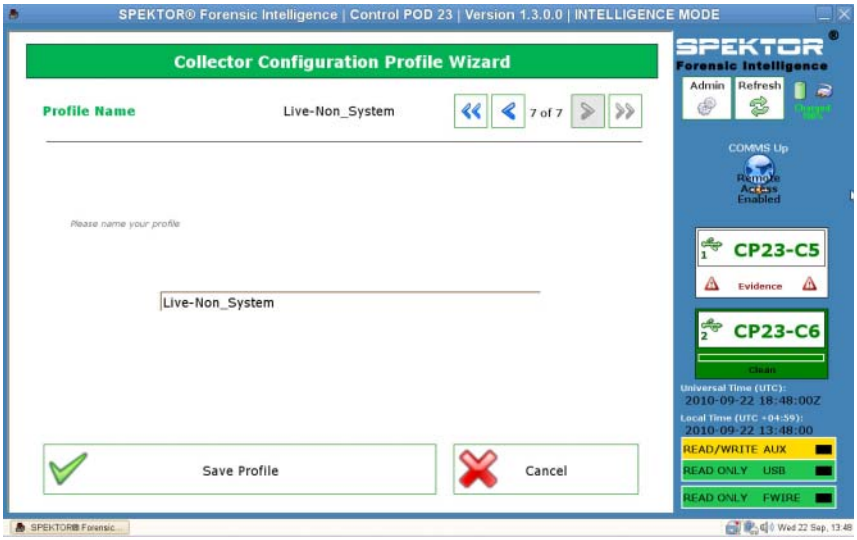
Abbildung 2-15. Schritt 6 der Profilkonfiguration: Fenster „Deleted File Filter“

ANMERKUNG: Nur gelöschte Dateien, die auf dem Zielgerät nicht bereits überschrieben wurden, können wahrscheinlich erfolgreich gesammelt werden; gelöschte Dateien, die überschrieben wurden, sind entweder beschädigt oder nicht abrufbar.

13 Klicken Sie oben rechts auf dem Bildschirm auf den Rechtspfeil.

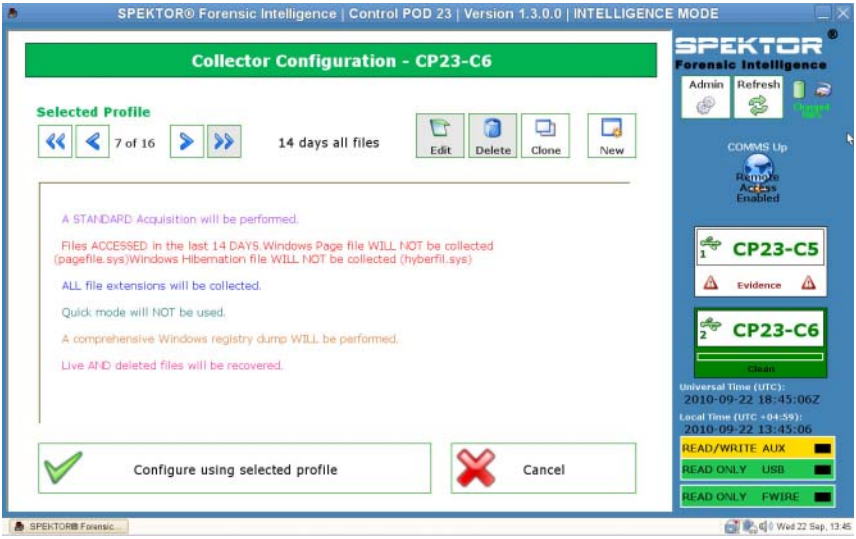
14 Geben Sie im Bildschirm **Profile Name** einen Namen für Ihr neues Profil ein. Tippen oder klicken Sie anschließend auf **Save Profile**.

Abbildung 2-16. Schritt 7 der Profilkonfiguration: Fenster „Profile Name“



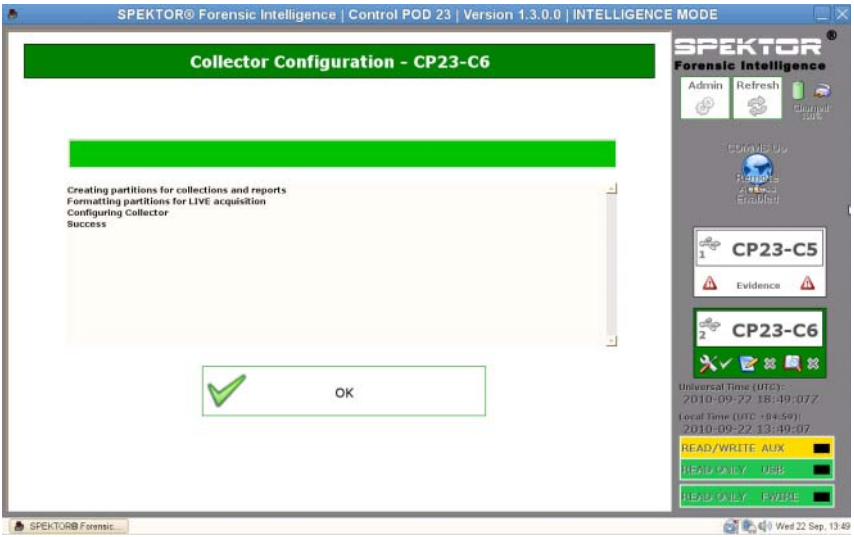
15 Klicken Sie oben rechts auf dem Bildschirm auf den Rechtspfeil. Ihr neues Profil wird im Bildschirm **Selected Profile** angezeigt. Im Bildschirm **Collector Configuration** wird der Titel des Profils angezeigt (in diesem Fall **14 days all files**). Dabei werden die Profildetails im Hauptbereich des Fensters aufgeführt.

Abbildung 2-17. Ausgewähltes Profil nach der Profilerstellung



16 Tippen oder klicken Sie auf **Configure using selected profile**, um die Konfiguration des Collector zu starten.

Abbildung 2-18. Ausgewähltes Profil nach der Profilerstellung



17 Tippen oder klicken Sie auf **OK**, um mit der Collector-Konfiguration zu beginnen. Dieser Vorgang dauert nur ein bis zwei Minuten.

Nach Abschluss der Collector-Konfiguration kann der Collector auf einem Zielcomputer oder ein Zielspeichergerät angewendet werden. Siehe „Anwenden von Sichtungswerkzeugen“ auf Seite 34.

18 Klicken Sie oben rechts auf dem Bildschirm auf den Rechtspfeil.

Anwenden von Sichtungswerkzeugen

ANMERKUNG: Weitere Informationen zu den Unterschieden einer Live- und Standarderfassung finden Sie unter „Standard- und Live-Erfassung“ auf Seite 20.

ANMERKUNG: Obwohl es möglich ist, einen Collector für mehrere Fälle einzusetzen, sollte gemäß bewährten Verfahren jeder Collector nur die Daten eines einzelnen Falles enthalten. Dabei ist es jedoch zulässig, dass Daten von mehreren Speichergeräten eines einzelnen Falles auf dem Collector gespeichert werden.

Anwenden eines Collector zur Standarderfassung auf einem Zielcomputer

WARNUNG: Vor einer Standarderfassung müssen Sie die Systemstartreihenfolge über das System-BIOS des Zielcomputers ändern. Wenn der Zielcomputer so eingerichtet ist, dass er von seiner Festplatte und nicht über das optische Laufwerk mit startfähigem SPEKTOR-Datenträger gestartet wird, wird der Laufwerkinhalt des Zielcomputers verändert. Stellen Sie vor dem Einschalten des Zielcomputers sicher, dass Sie wissen, wie Sie auf das System-BIOS des Zielcomputers zugreifen.

WARNUNG: Stellen Sie vor dem Einschalten des Zielcomputers sicher, dass sich der startfähige SPEKTOR-Datenträger in dem optischen Laufwerk befindet, über das der Zielcomputer laut Einstellung startet. Wenn der Zielcomputer ohne diesen startfähigen Datenträger gestartet wird, wird der Laufwerkinhalt des Zielcomputers verändert.

ANMERKUNG: Sie müssen über einen startfähigen SPEKTOR-Datenträger verfügen, um eine Standarderfassung auf einem Zielcomputer durchzuführen. Weitere Informationen zum Erstellen eines bootfähigen Datenträgers finden Sie unter „Brennen einer startfähigen CD für standardmäßige Erfassungsverfahren“ auf Seite 21.

1. Tippen oder klicken Sie auf dem extrastabilen Dell-Laptop auf die Option **Deploy Collector.**
2. Wählen Sie **Target Computer** aus.
3. Klicken Sie auf **OK**. Trennen Sie dann den Collector von dem extrastabilen Dell-Laptop.
4. Schließen Sie den Collector über einen verfügbaren USB-Anschluss an den Zielcomputer an.

ANMERKUNG: Dell empfiehlt, stets das interne optische Laufwerk des Zielcomputers mit dem startfähigen Datenträger zu verwenden. Sollte dies nicht möglich sein, nutzen Sie ein externes optisches Laufwerk mit einem USB-Anschluss.

5. Legen Sie den startfähigen SPEKTOR-Datenträger in das optische Laufwerk.
6. Greifen Sie auf das System-BIOS-Programm des Zielcomputers zu und ändern Sie die Startreihenfolge, damit der Zielcomputer über das optische Laufwerk gestartet wird.

   Der startfähige SPEKTOR-Datenträger wird geladen, und die Startlaufwerk-Schnittstelle wird angezeigt.
7. Geben Sie die auf dem Bildschirm angeforderten Informationen ein. (Um zwischen den Feldern zu wechseln, drücken Sie die <Eingabetaste> oder Pfeiltasten.) Gehen Sie dann zum Feld **COLLECT** und drücken Sie die <Eingabetaste>, um mit der Datenerfassung zu beginnen.

VORSICHT: Entfernen Sie den startfähigen SPEKTOR-Datenträger erst aus dem optischen Laufwerk, nachdem der Zielcomputer vollständig heruntergefahren wurde.

8 Drücken Sie nach Abschluss der Datenerfassung die <Eingabetaste>, um den Zielcomputer herunterzufahren.

9 Entfernen Sie den startfähigen SPEKTOR-Datenträger aus dem optischen Laufwerk, trennen Sie den Collector vom USB-Anschluss des Zielcomputer und schließen Sie ihn an einen verfügbaren USB-Anschluss des extrastabilen Dell-Laptops an.

Anwenden eines Collector zur Standarderfassung auf einem Zielspeichergerät

1 Schließen Sie das Zielspeichergerät entweder an den schreibgeschützten USB-Anschluss oder den Firewire-Anschluss des extrastabilen Dell-Laptops an.

2 Tippen oder klicken Sie auf **Deploy Collector**.

3 Tippen oder klicken Sie auf **Target Storage Device** und geben Sie die erforderlichen Informationen ein. Tippen oder klicken Sie anschließend auf **Collect from Device**.

4 Trennen Sie nach Abschluss der Erfassung das Zielspeichergerät vom USB-Anschluss und tippen oder klicken Sie auf **OK**.

Anwenden eines Collector zur Live-Erfassung

ANMERKUNG: Achten Sie darauf, während dieses Vorgangs und im Rahmen bewährter Kontrollkettenverfahren genaue und detaillierte Notizen anzufertigen.

ANMERKUNG: Für eine Live-Erfassung ist kein startfähiger SPEKTOR-Datenträger erforderlich.

1 Klicken Sie auf **Deploy Collector→ Target Computer**.

2 Navigieren Sie auf dem Zielcomputer zu **Arbeitsplatz** (oder **Computer** auf Computern mit Windows Vista oder Windows 7).

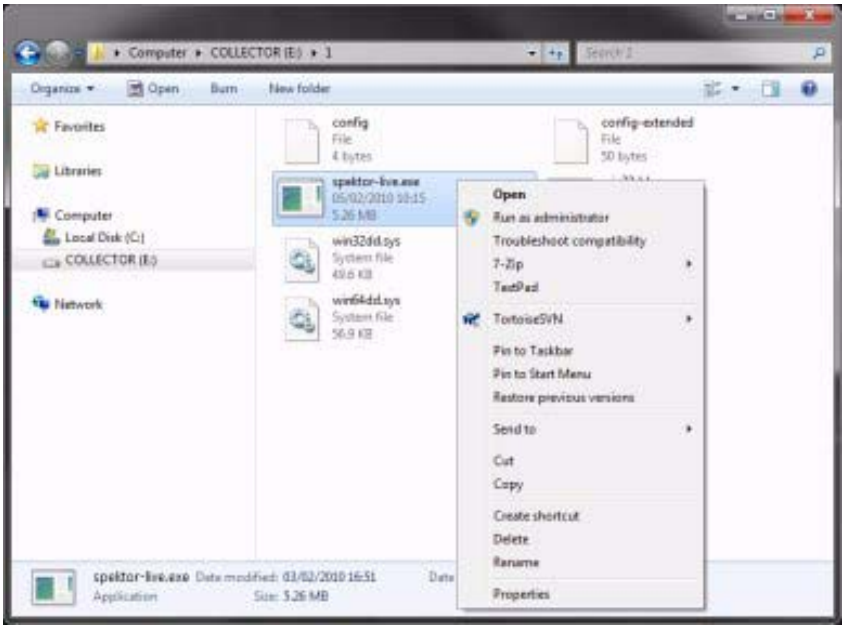
3 Doppelklicken Sie auf das **Collector**-Symbol, wenn es zum Anzeigen des Collector-Inhalts dargestellt wird.

Abbildung 2-19. Collector-Symbol

4 Klicken Sie auf den Ordner mit der höchsten Anzahl. Bei der ersten Anwendung seit der Collector-Bereinigung wird nur ein Ordner angezeigt.

5 Klicken Sie mit der rechten Maustaste **spektor-live.exe** und wählen Sie im Dropdown-Feld die **Option Run as administrator** aus. Wenn Sie über eine Meldung aufgefordert werden, eine Berechtigungen zum Ausführen der Anwendung als Administrator zu erteilen, klicken Sie auf den Befehl zum **Fortfahren**.

Abbildung 2-20. Run as Administrator



6 Geben Sie die angeforderten Informationen auf dem Bildschirm **SPEKTOR Live Collection** (Spektor-Live-Erfassung) ein und klicken Sie dann auf **Run**.

7 Klicken Sie, wenn Sie dazu aufgefordert werden, auf **Close**.

8 Trennen Sie den Collector vom Zielgerät und bewahren Sie ihn zur späteren Erfassung im Rechenzentrum sicher auf.

Überprüfen von gesammelten Dateien nach der Sichtung

1 Klicken Sie im **Collector Menu** auf **Reporting**. Diese Option indiziert die gesammelten Daten und erstellt automatisch verschiedene Berichte.

2 Wählen Sie im Bildschirm **Collector Collections** einen Hauptbericht unter **Main Report**. Klicken Sie dann auf **Generate Selected Reports**.

Abbildung 2-21. Berichte generieren

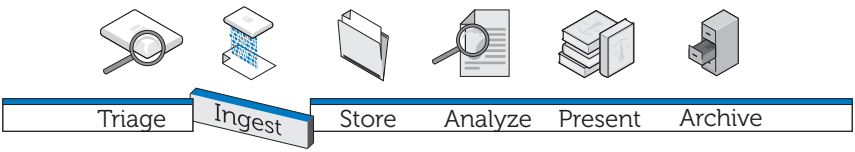
3 Klicken Sie nach der Berichtgenerierung auf **OK**, um zum Menü **Reporting** zurückzukehren.

ANMERKUNG: Weitere Informationen zum Erstellen und Exportieren anhand spezifischer Kriterien finden Sie im SPEKTOR-*Benutzerhandbuch*. Siehe „Relevante Dokumentation und Ressourcen“ auf Seite 16.

4 Klicken Sie auf **View Collection Report**, um Ihre Berichte anzuzeigen. Klicken Sie dann zum Anzeigen bestimmter Berichte auf eine von fünf Berichtskategorien: **Images**, **Documents**, **Multimedia**, **Other** oder **System**.

3

Erfassung



Die Phase „Erfassung“ der digitalen Kriminaltechniklösung von Dell umfasst die Image-Erstellung des Zielspeichergeräts (falls noch nicht während der Sichtung geschehen) und anschließende Übertragung des Image an einen zentralen Speicherort für einen möglichen Zugriff zu Analysezwecken. Um die forensischen Anwendungen ins Rechenzentrum zu verlagern und dennoch die gewohnte Benutzererfahrung zu erhalten, hat Dell in Zusammenarbeit mit Citrix verschiedene Softwarepakete für gängige forensische Anwendungen entwickelt, um diese nahtlos in das Rechenzentrum zu integrieren und eine Benutzererfahrung zu ermöglichen, die sich durch höhere Verfügbarkeit, mehr Geschwindigkeit und einen größeren Funktionsumfang auszeichnet.

Die folgenden forensischen Anwendungen sind für die digitalen Kriminaltechniklösung von Dell zertifiziert:

- SPEKTOR
- EnCase 6
- FTK 1.8
- FTK 3 (eigenständige Version)
- FTK 3 Lab

Alle diese forensischen Anwendungen können in beliebiger Kombination von einem Benutzergerät aus gleichzeitig verwendet werden.

Für den Einsatz im Rechenzentren geeignet: EnCase 6

Im folgenden Lösungsbeispiel wird die EnCase 6-Anwendung im Rechenzentrum auf einem Dell-Servergerät gehostet. Hierdurch werden EnCase 6-Sitzungen mit mehreren Benutzern möglich.

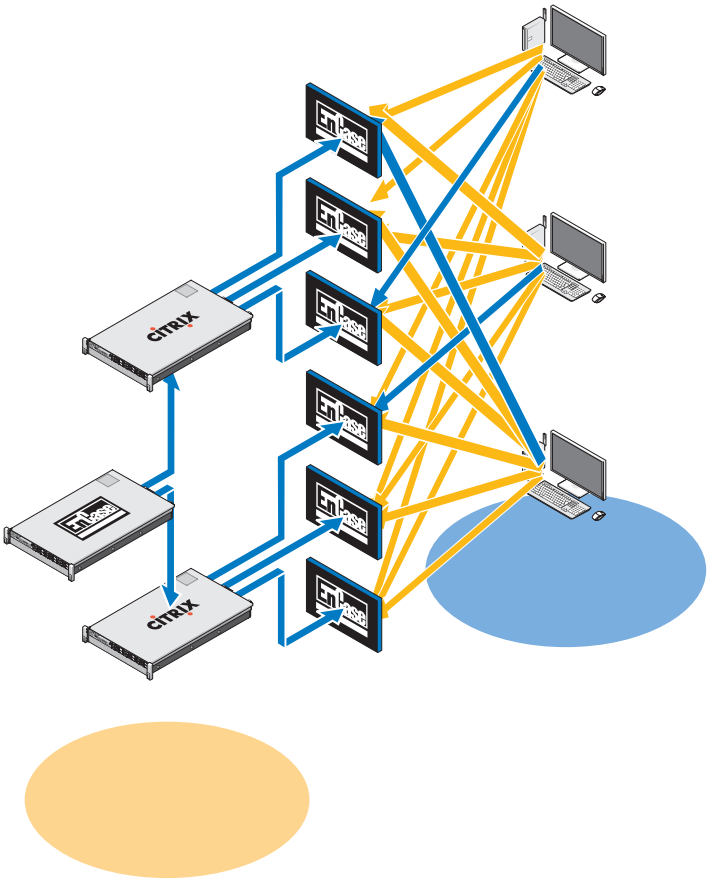
Einzelserverlösung

Im Falle der EnCase 6-Einzelserverlösung können sich mehrere Clients mit einem Server verbinden. Alle Clients verweisen auf diesen Server und können sich nicht mit einem anderen EnCase 6-Server verbinden. Bei einem Serverausfall gehen sämtliche Clientverbindungen verloren.

Multiserverlösung (hohe Verfügbarkeit)

Im Falle der Multiserverlösung stellt ein Benutzer eine Verbindung zur EnCase 6-Anwendung in der Citrix-Farm her und wird dann nahtlos zu dem EnCase 6-Server mit der derzeit niedrigsten Auslastung weitergeleitet. Falls der Benutzer mehrere EnCase 6-Instanzen ausführt, kann jede Instanziierung von einem anderen Server erstellt werden. Das Benutzererlebnis bleibt dabei erhalten. Denn der Benutzer bemerkt gar nicht, wie mehrere Instanzen erstellt werden. Alle Sitzungen erwecken den Anschein, als würden sie von demselben Server mit dem gleichen Erscheinungsbild ausgeführt.

Abbildung 3-1. Schematische Client- und Serverdarstellung für rechenzentrumsfähige EnCase 6-Anwendung



Bei einem Serverausfall muss der Benutzer erneut auf das EnCase-Anwendungssymbol auf dem Desktop klicken. Das System leitet die Benutzerverbindung daraufhin an den nächsten verfügbaren EnCase 6-Hostserver um. Jeder EnCase-Server kann *x* Benutzersitzungen unterstützen (*x* steht dabei für *die Anzahl der Kerne x 2*). Jede Benutzersitzung erfordert 3 GB Server-RAM.

Für den Einsatz im Rechenzentren geeignet: FTK 1.8

Bei der für den Einsatz im Rechenzentrum geeigneten Lösung FTK 1.8 wird die FTK 1.8-Anwendung im Rechenzentrum auf einem Dell-Servergerät gehostet. Hierdurch werden FTK 1.8-Sitzungen mit mehreren Benutzern möglich (eine eindeutige Benutzersitzung pro Server).

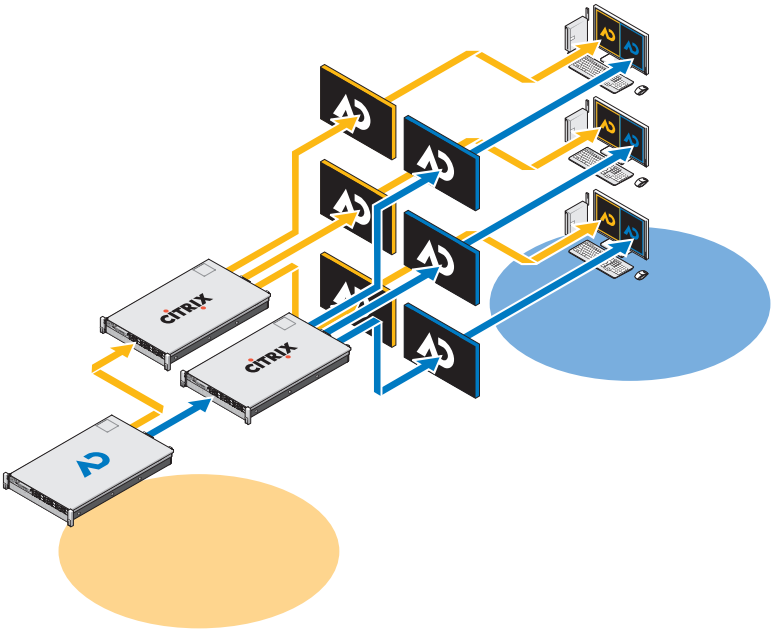
Eine FTK 1.8-Sitzung pro Desktop

Bei der FTK 1.8-Einzelserverlösung können sich mehrere Clients mit einem einzelnen Server verbinden. Alle Clients verweisen auf diesen Server und können sich nicht mit einem anderen FTK 1.8-Server verbinden. Bei einem Serverausfall gehen sämtliche Clientverbindungen verloren. Der Benutzer kann nur FTK 1.8-Sitzung pro Windows-Benutzerkonto ausführen.

Mehrere FTK 1.8-Sitzungen pro Desktop

Bei der FTK 1.8-Multiserverlösung stellt der Benutzer eine Verbindung zu den FTK 1.8-Servern her, indem er mehrere Desktopsymbole (FTK Server1, FTK Server2 usw.) verwendet. Jede Verknüpfung gilt für einen bestimmten Server. Zu Illustrationszwecken wird in Abbildung 3-2 die Grenze zwischen der aktiven FTK 1.8-Serversitzung und dem Server, der die FTK 1.8-Sitzung ausführt, farbcodiert dargestellt (Server1 = blau, Server2 = rot). Zwei Sitzungen der 1.8-Anwendung können nicht von demselben Server mit demselben Benutzerkonto ausgeführt werden. Die Benutzererfahrung bei der serverbasierten FTK 1.8-Anwendung ist auf allen Clients gleich.

Abbildung 3-2. Schematische Client- und Serverdarstellung für FTK 1.8-Multiserverlösung



Bei einem Serverausfall verliert der Benutzer den Zugriff auf die entsprechende FTK 1.8-Serversitzung. In diesem Fall muss der Benutzer die Funktion mithilfe der anderen FTK-Server weiterverwenden. Sämtliche Fall- und Beweisdaten (NAS-Zugriffsrechte des Benutzers vorausgesetzt) sind von allen FTK 1.8-Serversitzungen über das freigegebene NAS/SAN verfügbar.

Jeder FTK 1.8-Server kann *x* Benutzersitzungen unterstützen (*x* steht dabei für *die Anzahl der Kerne x 2*). Jede Benutzersitzung erfordert 3 GB Server-RAM und 1000 E/A pro Sekunde Festplattenleistung des Rechenzentrums.

Für den Einsatz im Rechenzentren geeignet: FTK 3

Bei der für den Einsatz im Rechenzentrum geeigneten Lösung FTK 3 wird die Anwendung im Rechenzentrum auf einem Dell-Servergerät gehostet. Hierdurch wird eine FTK 3-Anwendungsitzung pro Server möglich.

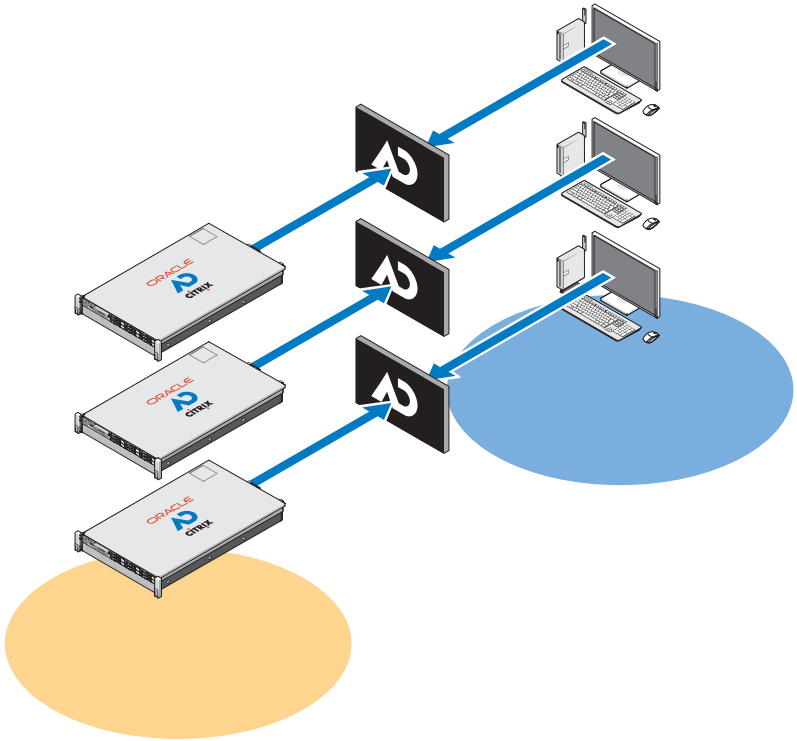
FTK 3-Einzelserverlösung

Bei der FTK 3-Einzelserverlösung kann sich ein FTK 3-Client mit einem einzelnen Server verbinden. Der Client verweist auf diesen Server und kann sich nicht mit einem anderen FTK 3-Server verbinden. Bei einem Serverausfall geht die Clientverbindung verloren. Der FTK 3-Server führt ebenfalls die lokale in FTK eingebettete Oracle-Datenbank aus, da diese Datenbankversion die Zusammenarbeit zwischen anderen FTK-Oracle-Datenbanken oder anderen FTK-Benutzern nicht unterstützt.

Multiserverlösung (keine hohe Verfügbarkeit)

Bei der Multiserverlösung verbindet sich jeder Client mit seinem ursprünglichen FTK 3-Server und kann keine Verbindung zu anderen FTK 3-Servern herstellen. Wenn auf einem Server eine FTK 3-Sitzung ausgeführt wird, ist er zur Annahme weiterer neuer FTK 3-Clientsitzungen nicht mehr verfügbar: Aufgrund des Software-Setup im Forensik-Framework von Dell können Server nicht mehr als eine Sitzung der FTK 3-Anwendung gleichzeitig ausführen. Indem pro Server nur eine Sitzung ausgeführt werden darf, ist die FTK 3-Multithreaded-Anwendung in der Lage, alle verfügbaren Serverressourcen auf die Verarbeitung eines Falles zu verwenden und somit die Leistung zu steigern.

Abbildung 3-3. Schematische Client- und Serverdarstellung für rechenzentrumsfähige FTK 3-Anwendung



Bei Verwendung der FTK Standard-Edition muss jeder Server eine lokal Version der FTK-eingebetteten Oracle-Datenbank ausführen (eine Oracle-Datenbankversion pro gleichzeitiger Benutzersitzung). Diese Version der FTK-Anwendung und Oracle-Datenbank unterstützt nicht die Zusammenarbeit zwischen anderen FTK-Benutzern oder anderen FTK-Oracle-Datenbanken.

Jede Oracle-Datenbank verfügt über einen Oracle-Backup-Agenten auf dem Server, und die Datenbank wird im Rahmen des normalen Backup-Verfahrens gesichert (weitere Informationen unter „Archivierung“ auf Seite 89).

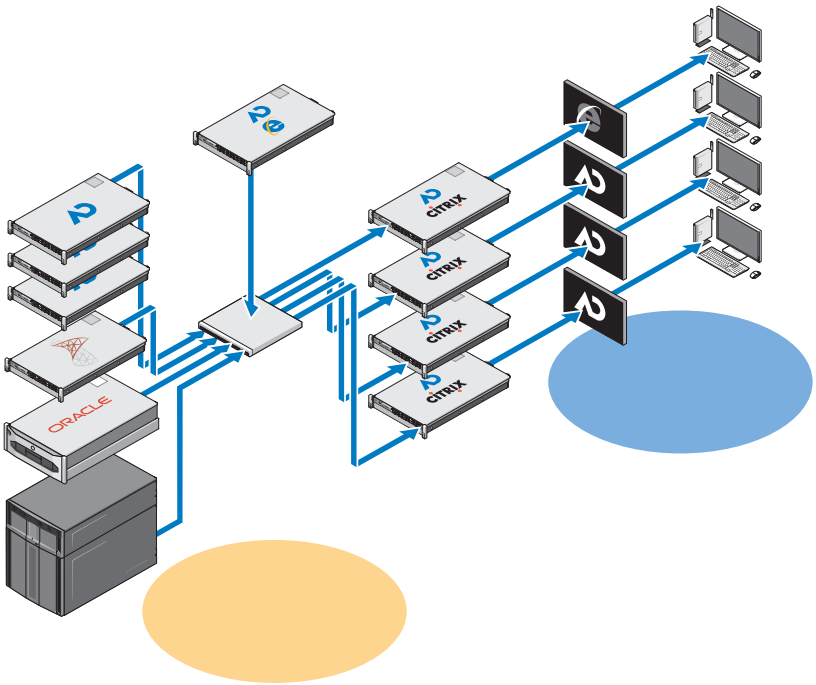
Bei einem Serverausfall muss sich der Benutzer manuell mit einem anderen verfügbaren FTK 3-Server verbinden (sofern mehr als ein FTK 3-Server verfügbar ist). Sollte die Oracle-Datenbank ebenfalls ausfallen, gibt es keinen Zugriff auf bereits verarbeitete, existierende Fälle, da diese mit der ursprünglichen lokalen FTK 3-Oracle-Datenbank für diesen Benutzer verknüpft sind.

Jeder FTK 3-Server kann eine gleichzeitige Benutzersitzung unterstützen. Jede Benutzersitzung erfordert 64 GB Server-RAM (48 GB für Oracle und 16 GB für FTK) und 1000+ E/A pro Sekunde für den Dateispeicher sowie 600+ E/A pro Sekunde für die Datenbank (Minimalkonfiguration).

FTK 3 Lab Edition

Bei der FTK 3 Lab Edition-Konfiguration stellt der Benutzer eine Verbindung zu einem AccessData Lab-Hostserver und der zentralen Falldatenbank her. Mehrere Benutzer können gleichzeitig auf denselben Fall zugreifen und dabei auch unterschiedliche Analysen durchführen. Die Verarbeitung wird über ein verteiltes Verarbeitungsmodell abgewickelt.

Abbildung 3-4. Schematische Client- und Serverdarstellung für FTK 3 Lab Edition



Die Fallspeicherung wird über eine Mischung von SAS- und SATA-Hardware optimiert, und das komplette forensische Rechenzentrum kann zentral von einem Admin-Manager verwaltet werden.

Mehrere forensische Anwendungen auf einem Desktop

In der Lösung mit mehreren Anwendungen verschiedener Anbieter werden alle zuvor beschriebenen Einzelanwendungen zusammengeführt, damit forensische Analytiker über einen Desktop Zugriff auf alle forensischen Anwendungen (EnCase 6, FTK 1.8 und FTK 3 oder FTK 3 Lab Edition) erhalten. Alle Anwendungen können in einem Hochverfügbarkeitsmodus bereitgestellt werden, so dass der Benutzer bei einem Ausfall nach wie vor auf eine bestimmte Anwendung zugreifen kann; im Fall von FTK 1.8 erhält der Benutzer durch Verwendung eines der FTK 1.8-Symbole auf dem Desktop Zugriff.

Empfohlene Netzwerkkonfigurationen

Tabelle 3-1. Empfohlene IP-Adressstruktur

IP-Adresse	Serverfunktion	Servername
192.168.1.1	Domänencontroller 1	DF-DC1
192.168.1.2	Domänencontroller 2	DF-DC2
192.168.1.3	Beweismaterialserver	DF-Beweismaterial
192.168.1.4	Arbeitsbereichsserver	DF-Arbeitsbereich
192.168.1.5	FTK-Oracle-Server	DF-FTK
10.1.0.0/24	1 GB statischer IP-Adressbereich	
10.1.1.0/24	10 GB statischer IP-Adressbereich	
10.1.2.0/24	1 GB DHCP-Bereich, Clients	
10.1.0.250-254	1-GB-Switch(es)	
10.1.1.250-254	10-GB-Switch(es)	
10.1.0.200	DNS-Server	

Tabelle 3-2. Empfohlene Namenskonventionen für Lösungsserver

Name	Abkürzung
Domänenname	DF (digitale Forensik)
Domänencontroller 1	DF-DC1
Domänencontroller 2	DF-DC2
Beweismaterialspeicher	DF-Beweismaterial
Arbeitsbereich	DF-Arbeitsbereich
Oracle	DF-Oracle
SQL	DF-SQL
FTK-Lab	FTK-Lab
FTK-Standalone	FTK
Manager verteilte Verarbeitung	DF-DPM, DF-DPM1, DF-DPM2
Engine(s) verteilte Verarbeitung	DF-DPE, DF-DPE1, DF-DPE2

Tabelle 3-3. Empfohlene Namenskonventionen für NIC-Teaming

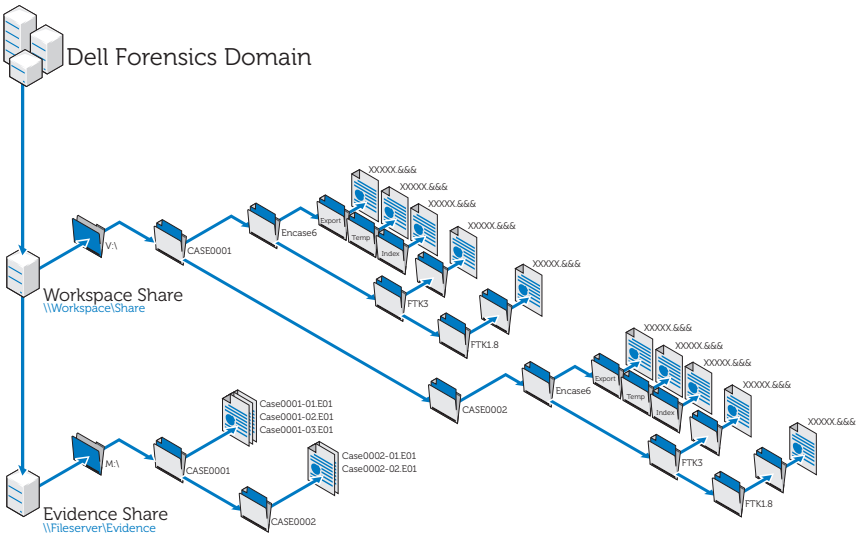
NIC-Team 1	Öffentliches Netzwerk	Für untereinander verbundene Server
NIC-Team 2	iSCSI	Für an EqualLogic-Speichergeräte angeschlossene Server

Tabelle 3-4. Empfohlene Zuordnungsstruktur für Laufwerksbuchstaben

Bezeichnung	Laufwerk	Lokal oder SAN	RAID	Anmerkungen
Lokales Laufwerk	C:	Lokal	RAID1 (2 x SAS-Festplatten mit 15.000 U/min)	
	D:	Lokal		
CD-ROM	E:			
	F:			
	G:			
SQL	H:	SAN	RAID0+1	Auf SATA-Festplatten nicht zulässig
Oracle	I:	SAN	RAID0+1	Auf SATA-Festplatten nicht zulässig
EV Vault-Laufwerk	J:	SAN	RAID50	
Backup auf Festplatte	K:	SAN	RAID50	
Spare	L:	SAN	RAID50	
Beweis 1	M:	SAN	RAID50	
Beweis 2	N:	SAN	RAID50	
Beweis 3	O:	SAN	RAID50	
Beweis 4	P:	SAN	RAID50	
Beweis 5	Q:	SAN	RAID50	
Beweis 6	R:	SAN	RAID50	
Beweis 7	S:	SAN	RAID50	

Bezeichnung	Laufwerk	Lokal oder SAN	RAID	Anmerkungen
Beweis 8	T:	SAN	RAID50	
Beweis 9	U:	SAN	RAID50	
Arbeitsbereich 1	V:	SAN	RAID50	
Arbeitsbereich 2	W:	SAN	RAID50	
Arbeitsbereich 3	X:	SAN	RAID50	
Arbeitsbereich 4	Y:	SAN	RAID50	
Arbeitsbereich 5	Z:	SAN	RAID50	

Abbildung 3-5. Empfohlene Dateistruktur



Erfassen mit der digitalen Kriminaltechniklösung von Dell

Erfassen mit SPEKTOR

Registrieren und Bereinigen eines externen USB-Geräts als Speicherdatenträger

1. Schließen Sie ein nicht registriertes extern USB-Geräts an einen Collector-Anschluss des extrastabilen Laptops an.
2. Klicken oder tippen Sie auf das Gerätesymbol, wenn es angezeigt wird. Klicken oder tippen Sie dann auf **Register the Device as a Store Disk→ Yes**. Geben Sie anschließend die angeforderten Informationen ein.
3. Wählen Sie im Menü auf der rechten Seite das registrierte Gerät aus. Tippen oder klicken Sie anschließend auf **Clean/Reformat→ Clean**.
4. Klicken Sie nach Abschluss des Vorgangs auf **OK**.

Anwenden des Speicherdatenträgers

1. Verbinden Sie den Speicherdatenträger mit dem extrastabilen Laptop. Tippen oder klicken Sie anschließend auf das Speicherdatenträger, um das Menü **Store Disk Menu** anzuzeigen.
2. Tippen oder klicken Sie im Menü **Store Disk Menu** auf **Deploy**.

   Beim Anwenden auf einen Zielcomputer:

   a. Tippen oder klicken Sie auf **Target Computer**.

   b. Trennen Sie den Speicherdatenträger vom extrastabilen Laptop und verbinden Sie ihn über einen freien USB-Anschluss mit dem Zielcomputer.

   c. Befolgen Sie die gleichen Bereitstellungsanweisungen wie beim Erfassen eines Sichtungs-Image (siehe „Anwenden von Sichtungswerkzeugen“ auf Seite 34).

   d. Sobald die startfähige CD geladen ist, führt Sie der **SPEKTOR Imaging Wizard** durch den restlichen Imaging-Prozess. Schrittweise Anweisungen finden sie im *SPEKTOR-Benutzerhandbuch*. Weitere Informationen finden Sie unter „Relevante Dokumentation und Ressourcen“ auf Seite 16.

e Fahren Sie den Zielcomputer herunter, trennen Sie den Speicherdatenträger und führen Sie den Speicherdatenträger anschließend wieder dem Rechenzentrum zu Speicherzwecken zu.

Beim Anwenden auf ein lokales Zielspeichergerät:

a Tippen oder klicken Sie auf **Target Storage Device**.

b Schließen Sie das Zielspeichergerät entweder an den schreibgeschützten USB-Anschluss oder den Firewire-Anschluss auf der rechten Seite des extrastabilen Dell-Laptops an.

c Wählen Sie das Laufwerk bzw. die Partitionen für die Image-Erstellung aus und klicken Sie dann auf den Rechtspfeil oben rechts auf dem Bildschirm.

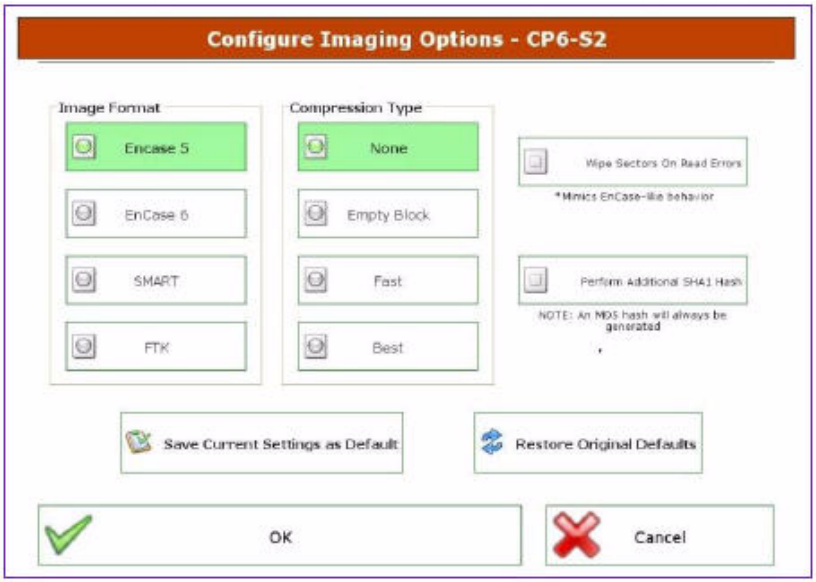
d Geben Sie die angeforderten Falldaten ein. Tippen oder klicken Sie anschließend auf **Image Now**.

e Tippen oder klicken Sie ggf. auf **Configure Imaging Options**, um die Einstellungen für **Image Format**, **Compression Type**, **Wipe Sectors on Read Errors** oder **Perform Additional SHA1 Hash** zu ändern.

ANMERKUNG: Ein MDS-Hash wird immer während der Image-Erstellung generiert.

ANMERKUNG: Weitere Informationen zu den einzelnen Imaging-Optionen finden Sie im *SPEKTOR-Benutzerhandbuch*. Siehe „Relevante Dokumentation und Ressourcen“ auf Seite 16.

Abbildung 3-6. Konfigurieren von Imaging-Optionen



f Tippen oder klicken Sie auf **Image Now**→ **Yes**, um mit dem Image-Vorgang zu beginnen.

g Tippen oder klicken Sie nach Abschluss des Imaging-Vorgangs auf **OK**.

h Trennen Sie das Zielspeichergerät und den Speicherdatenträger vom extrastabilen Laptop. Führen Sie dann den Speicherdatenträger wieder dem Rechenzentrum zwecks Speicher und Analyse zu.

ANMERKUNG: Die Image-Übertragung kann sehr lange dauern (sechs Stunden zur Übertragung einer typischen 60-GB-Festplatte ist nicht ungewöhnlich).

Erfassen mit EnCase

Bei der digitalen Kriminaltechniklösung von Dell wird die Lizenzierung für EnCase über ein Netzwerklizenzierungssystem durchgeführt. Normalerweise wird eine Instanz von EnCase SAFE auf einen der Server im Rechenzentrum installiert, und ein Dongle mit mehreren Benutzerlizenzen wird an diesen Server angeschlossen. EnCase-Clients sind so konfiguriert, dass sie auf diesem Server nach der Lizenzierung suchen, so dass keine lokalen Dongle erforderlich sind. Weitere Informationen finden Sie im *Handbuch zur Installation und Konfiguration der digitalen Kriminaltechniklösung von Dell*. Siehe „Relevante Dokumentation und Ressourcen“ auf Seite 16. Von Ihrem Netzwerksystemadministrator erhalten Sie ebenfalls Informationen zu der bei Ihrer Behörde installierten Lösung.

1. Stellen Sie eine Verbindung zwischen dem Zielspeichergerät und der entsprechenden zur Erfassung vorgesehenen Workstation im Rechenzentrum her.
   a. Im Falle einer Image-Erstellung für ein SATA-Laufwerk finden Sie unter „Anschließen des Tableau-Schreibblockers an eine SATA-Festplatte“ auf Seite 56 weitere Informationen.
   b. Im Falle einer Image-Erstellung für ein IDE-Laufwerk finden Sie unter „Anschließen des Tableau-Schreibblockers an eine IDE-Festplatte“ auf Seite 57 weitere Informationen.
2. Legen Sie einen neuen Fall an.

ANMERKUNG: Die folgenden Anweisungen beziehen sich auf die Netzwerk- und Ordnerstruktur, die Dell für seine digitale Kriminaltechniklösung als bewährte Vorgehensweise empfiehlt. Abbildung 3-5 liefert weitere Informationen hierzu.

   a. Klicken Sie auf **New** und geben Sie anschließend die angeforderten Informationen ein.
   b. Erstellen Sie auf Laufwerk **W:** (dem Arbeitsbereich) Ordner gemäß der folgenden Struktur:
      - `W:\[Fallbezeichnung]\EnCase6\Export`
      - `W:\[Fallbezeichnung]\EnCase6\Temp`
      - `W:\[Fallbezeichnung]\EnCase6\Index`
   c. Klicken Sie auf **Finish**.
   d. Klicken Sie auf **Yes** bei jeder Anforderung zum Erstellen eines Ordners.

e Klicken Sie im Bildschirm **EnCase Acquisition** auf die Menüoption **Add Device**.

f Vergewissern Sie sich, dass das Kontrollkästchen **Sessions** aktiviert ist.

g Wählen Sie im rechten Fensterbereich Ihren Fall aus.

h Klicken Sie auf **Add Evidence Files**. Navigieren Sie dann zum E01-Repository (gemäß der in Abbildung 3-5 beschriebenen bewährten Konfiguration sollte dieses Repository auf Laufwerk **X:** abgelegt sein).

i Klicken Sie auf **Next**→ **Next**→ **Finish**. Ein Stoppuhr-Symbol wird unten rechts auf dem EnCase-Bildschirm **Acquisition** angezeigt, und EnCase überprüft die E01-Datei. Je nach Dateigröße kann diese Prüfung eine gewisse Zeit in Anspruch nehmen.

3 Fügen Sie innerhalb der EnCase-Software mithilfe des Assistenten **Add Device** das Zielspeichergerät hinzu.

4 Führen Sie eine Erfassung für den Geräteinhalt durch.

a Klicken Sie innerhalb der EnCase-Software auf **Cases**→ **Entries**→ **Home**. Klicken Sie dann mit der rechten Maustaste auf das zu erfassende Gerät.

b Wählen Sie aus dem Dropdown-Menü die Option **Acquire** aus.

c Wählen Sie im Dialogfeld **After Acquisition** unter **New Image File** den gewünschten Typ aus:

- **Aktivieren Sie keine** Optionen, die das neu erfasste Image des aktuell offenen Falls ausschließen.
- Mit **Add to Case** wird das neu erfasste Image der Falldatei hinzugefügt, die mit dem Gerät, auf dem das Image erstellt wurde, verknüpft ist.
- Mit **Replace a source device** wird das neu erfasste Image dem Fall hinzugefügt und das in einer Vorschau angezeigte Gerät, auf dem die Erfassung durchgeführt wurde, entfernt.

d Klicken Sie auf **Finish**. Im Abschluss an den Imaging-Vorgang wird das das Dialogfeld **Acquisition Results** angezeigt.

Arbeiten mit Tableau-Schreibblockern

VORSICHT: Eine Festplatte darf bei eingeschaltetem Strom nicht von einer Forensik-Bridge getrennt werden.

VORSICHT: Verwenden Sie keine USB-Kabelverlängerer bei Forensik-Bridges.

Anschließen des Tableau-Schreibblockers an eine SATA-Festplatte

1. Vergewissern Sie sich, dass **DC IN B** bei der T35es Forensic SATA/IDE-Bridge auf **B On** eingestellt ist.
2. Schließen Sie die TP2- bzw. TP3-Stromquelle mithilfe des 5-poligen Mini-DIN-Steckers an die linke Seite der T35es SATA-Bridge an.
3. Schließen Sie das Stromkabel an die TP2-Stromquelle und eine Steckdose an.
4. Schalten Sie den Strom ein, um zu überprüfen, ob die LED des Schreibblockers leuchtet. Schalten Sie anschließend den Strom für die Bridge aus, bevor Sie eine Verbindung zum Zielspeichergerät herstellen.
5. Schließen Sie den Molex-Steckverbinder (Buchse) des TC5-8 SATA-Stromkabels an den **DC OUT**-Anschluss auf der rechten Seite der T35es SATA/IDE-Bridge an.
6. Verbinden Sie den SATA-Netzanschluss des TC5-8 SATA-Stromkabels mit dem SATA-Netzanschluss der Zielfestplatte.

VORSICHT: Wenn beide Molex- und SATA-Stromversorgungsanschlüsse für den Anschluss an das Zielspeichergerät verwendet werden, führt dies zu einer Überlastung des Zielgeräts.

7. Verbinden Sie das TC3-8 SATA-Signalkabel mit der T35es SATA/IDE-Bridge.
8. Verbinden Sie das andere Ende des TC3-8 SATA-Signalkabels mit dem Zielspeichergerät.
9. Stecken Sie ein Ende des Datenkabels (USB 2.0, zwei FireWire 800-Verbindungen oder Orion 4-Pin FireWire 400) in einen Anschluss auf der linken Seiten der T35es SATA/IDE-Bridge.
10. Stecken Sie das andere Ende des Datenkabels in einen Anschluss des extrastabilen Dell-Laptop bzw. der Dell OptiPlex-Workstation.
11. Stellen Sie den Schalter oben an der T35es SATA/IDE-Bridge auf **A ON**. Der extrastabile Dell-Laptop bzw. die Dell OptiPlex-Workstation sollte nun das Vorhandensein des Zielspeichergeräts registrieren.

Anschließen des Tableau-Schreibblockers an eine IDE-Festplatte

1. Vergewissern Sie sich, dass **DC IN B** bei der T35es Forensic SATA/IDE-Bridge auf **B On** eingestellt ist.
2. Schließen Sie die TP2- bzw. TP3-Stromquelle mithilfe des 5-poligen Mini-DIN-Steckers an die linke Seite der T35es SATA/IDE-Bridge an.

ANMERKUNG: Der 7-polige DIN-Stecker der TP3-Stromversorgung funktioniert nicht bei Tableau-Bridges. Sie müssen das enthaltene 7- bis 5-polige DIN TCA-P7-P5-Adapterkabel verwenden, um die TP3-Stromversorgung an die Tableau-Bridges anzuschließen.

3. Schließen Sie das Stromkabel an die TP2-Stromquelle und eine Steckdose an.
4. Schalten Sie den Strom ein, um zu überprüfen, ob die LED des **Schreibblockers leuchtet**. Schalten Sie anschließend den Strom für die Bridge **aus**, bevor Sie eine Verbindung zur Zielfestplatte herstellen.
5. Schließen Sie den Molex-Steckverbinder (Buchse) des TC2-8 Molex-Stromkabels an den DC OUT-Anschluss auf der rechten Seite der T35es SATA/IDE-Bridge an.
6. Schließen Sie den anderen Molex-Steckverbinder des TC2-8 Molex-Stromkabels an den Molex-Stecker der verdächtigen Festplatte an.
7. Schließen Sie das blaue Ende des TC6-8 IDE-Signalkabels (zur Ausrichtung an Pin 1) an die T35es SATA/IDE-Bridge an.
8. Verbinden Sie das schwarze Ende des TC6-8 IDE-Signalkabels mit dem Zielspeichergerät.
9. Stecken Sie ein Ende des Datenkabels (USB 2.0, zwei FireWire 800-Verbindungen- Orion 4-Pin FireWire 400-Verbindung) in einen Anschluss auf der linken Seiten der T35es SATA-Bridge.
10. Stecken Sie das andere Ende des Datenkabels in einen Anschluss des extrastabilen Dell-Laptop bzw. der Dell OptiPlex-Workstation.
11. Stellen Sie den Schalter oben an der T35es SATA/IDE-Bridge auf **A On**. Der extrastabile Dell-Laptop bzw. die Dell OptiPlex-Workstation sollte nun ein Vorhandensein des Zielspeichergeräts erkennen.

Erfassen mit rechenzentrumsfähiger FTK 1.8- und 3.0-Anwendung

Bei der digitalen Kriminaltechniklösung von Dell wird die Lizenzierung für FTK über ein Netzwerklizenzierungssystem durchgeführt. Normalerweise ist der FTK-Netzwerklizenzierungsserver auf einen der Server im Rechenzentrum installiert, und ein FTK-Dongle mit mehreren Benutzerlizenzen wird an diesen Server angeschlossen. Die FTK-Clients sind so konfiguriert, dass sie auf diesem Server nach der Lizenzierung suchen, so dass keine lokalen Dongle erforderlich sind. Weitere Informationen finden Sie im *Handbuch zur Installation und Konfiguration der digitalen Kriminaltechniklösung von Dell*. Siehe „Relevante Dokumentation und Ressourcen“ auf Seite 16. Von Ihrem Netzwerksystemadministrator erhalten Sie ebenfalls Informationen zu der bei Ihrer Behörde installierten Lösung.

Erstellen eines Image auf dem Zielspeichergerät

1. Klicken Sie in der Anwendung AccessData FTK Imager auf **File→ Create Disk Image . . .**
2. Wählen Sie im Popup-Menü **Select Source** den Typ Beweismaterial, für den ein Image erstellt werden soll. Zur Auswahl stehen: „Physical Drive“, „Logical Drive“, „Image File“, „Contents of a Folder“ und „Fernico Device“. Klicken Sie dann auf **Next**.

ANMERKUNG: Im Folgenden wird die Option **Imaging a Physical Drive** zur Veranschaulichung des Image-Erstellprozesses verwendet. Die anderen Dateioptionen werden im *FTK-Benutzerhandbuch* behandelt. Siehe „Relevante Dokumentation und Ressourcen“ auf Seite 16.

3. Wählen Sie über das Dropdown-Feld aus den verfügbaren Laufwerken das physikalische Laufwerk aus, für das Sie ein Image erstellen möchten. Klicken Sie dann auf **Finish**.
4. Klicken Sie im Popup-Fenster **Create Image** auf **Add . . .**und wählen Sie den zu erstellenden Image-Typ („Raw“, „SMART“, „E01“ oder „AFF“) aus. Klicken Sie anschließend auf **Next**.
5. Geben Sie die angeforderten Informationen in das Fenster **Evidence Item Information** ein („Case Number“, „Evidence Number“, „Unique Description“, „Examiner“ und „Notes“). Klicken Sie anschließend auf **Next**.

6 Navigieren Sie im Fenster **Select Image Destination** zu dem den Beweis-Images zugeordneten Speicherbereich (siehe Abbildung 3-5 für Dells empfohlene Datei- und Servernomenklatur), geben Sie den Image-Dateinamen ein und klicken Sie dann auf →.

7 Klicken Sie auf **Start.** Die Popup-Meldung **Creating Image . . .** wird mit einem Vorgang-Statusbalken angezeigt.

ANMERKUNG: Der Image-Erstellprozess kann abhängig vom Umfang der hinzugefügten Daten Stunden dauern.

8 Wenn Sie sich zuvor zur Anzeige einer Zusammenfassung der Image-Ergebnisse entschieden haben, wird nach Abschluss der Image-Erstellung das Fenster **Drive/Image Verify Results** angezeigt. Überprüfen Sie die Ergebnisse und klicken Sie dann auf **Close**.

9 Klicken Sie erneut auf **Close**, um die Popup-Meldung **Creating Image . . .** zu schließen.

Anlegen eines neuen Falles

1 Klicken Sie auf **File→ New Case**. Machen Sie in folgenden Rubriken Ihre Angaben: **Investigator Name**, **Case Number**, **Case Name**, **Case Path** und **Case Folder**.

2 Machen Sie im Fenster **Forensic Examiner Information** Angaben unter Folgendem: **Agency/Company**, **Examiner's Name**, **Address**, **Phone**, **Fax**, **E-Mail** und **Comments**. Klicken Sie anschließend auf **Next**.

3 Wählen Sie im Fenster **Case Log Options** die zu ändernden Optionssätze aus:

- Case and evidence events
- Error messages
- Bookmarking events
- Searching events
- Data carving/Internet searches
- Other events

4 Wählen Sie im Fenster **Processes to Perform** die durchzuführenden Prozesse aus. Wählen Sie unter **Processes** aus folgenden Optionen aus:

- 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 Klicken Sie auf **Next**.

6 Schließen Sie über das Fenster **Refine Case** unterschiedliche Datentypen von Ihrem Fall aus bzw. schließen Sie sie darin ein. Zu den vorkonfigurierten Optionen gehören fünf allgemeine Anforderungen:

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

7 Klicken Sie auf **Next**.

8 Schließen Sie über das Fenster **Refine Index** unterschiedliche Datentypen in den Indizierungsvorgang aus bzw. schließen Sie sie darin ein.

9 Klicken Sie auf **Next**.

Hinzufügen von Beweismaterial

1. Klicken Sie auf **Add Evidence**. Das Popup-Fenster **Add Evidence to Case** wird angezeigt.
2. Wählen Sie durch Aktivierung der jeweiligen Optionsschaltfläche (**Acquired Image of Drive**, **Local Drive**, **Contents of a Folder** oder **Individual File**) den Typ Beweismaterial aus, der Ihrem Fall hinzugefügt werden soll. Klicken Sie dann auf **Continue**.
3. Navigieren Sie zu dem Image, Laufwerk, Ordner oder der Datei. Wählen Sie dann die Datei aus und klicken Sie auf **Open**.

   Wenn Sie **Acquired Image of Drive** als Beweismaterialtyp ausgewählt haben, wird ein Popup-Fenster **Evidence Information** angezeigt. Geben Sie die angeforderten Informationen ein und klicken Sie auf **OK**.

   Bei Auswahl von **Local Drive** als Beweismaterialtyp:

   a. Das Popup-Fenster **Select Local Drive** wird angezeigt. Wählen Sie das hinzuzufügende lokale Laufwerk und dann entweder **Logical Analysis** oder **Physical Analysis** aus. Klicken Sie auf **OK**.

   b. Geben Sie in das Fenster **Evidence Information** die angeforderten Informationen ein und klicken Sie dann auf **OK**.

   Wenn Sie **Contents of a Folder oder Individual File** ausgewählt haben, wählen Sie Ordner und Datei aus, die Ihrem Fall hinzugefügt werden sollen. Klicken Sie dann auf **Open**.
4. Klicken Sie auf **Next**.
5. Überprüfen Sie im Fenster **New Case Setup is Now Complete** Ihre Auswahl. Klicken Sie dann auf **Finish**.

Erfassen mit FTK 3 Lab Edition

Erstellen eines Image auf dem Zielspeichergerät

Siehe „Erstellen eines Image auf dem Zielspeichergerät“ auf Seite 58.

Anlegen eines neuen Falles

1. Klicken Sie auf **Case→ New**. Das Fenster **New Case Options** wird angezeigt.
2. Geben Sie den Fallnamen sowie Referenzen oder beschreibende Informationen ein, die für Ihre Behörde erforderlich sind.
3. Navigieren Sie zu „Case Folder Directory“ und wählen Sie aus dem Dropdown-Feld die Option „Processing Manager“ aus.

ANMERKUNG: Wenn Sie den Case Folder Directory- und Processing Manager-Pfad nicht kennen, wenden Sie sich an Ihren Systemadministrator.

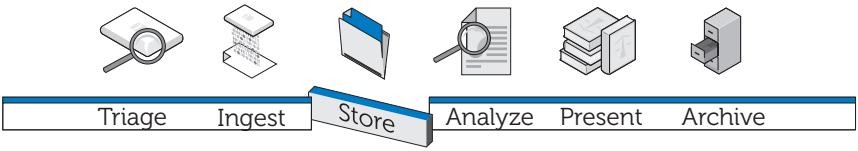
4. Klicken Sie auf **Detailed Options**, um die Auswahl der in Ihren Fall einzuschließenden Daten zu verfeinern. Weitere Informationen zum Einschränken von Falldaten finden Sie im *AccessData FTK 3-Benutzerhandbuch*. Siehe „Relevante Dokumentation und Ressourcen“ auf Seite 16.
5. Klicken Sie auf **OK**. Das Fenster **Manage Evidence** wird geöffnet.

Hinzufügen von Beweismaterial zu einem Fall

1. Klicken Sie im Fenster **Manage Evidence** auf **Add**. Klicken Sie dann auf die Optionsschaltfläche neben dem Typ hinzuzufügenden Beweismaterials. Zur Auswahl stehen die Optionen: **Acquired Image(s)**, **All Images in Directory**, **Contents of a Directory**, **Individual File(s)**, **Physical Drive** oder **Logical Drive**. Klicken Sie dann auf **OK**.
2. Navigieren Sie zum Verzeichnis **Evidence** und wählen Sie Ihre Beweisdatei aus. Klicken Sie dann auf **Open**.
3. Wählen Sie eine Zeitzone aus (erforderlich).
4. Klicken Sie auf **OK**. Das Fenster **Data Processing Status** wird geöffnet.
5. Wenn unter **Process State** der Status zu **Finished** wechselt, klicken Sie auf **Close**. Das Beweismaterial wird nun innerhalb des Benutzeroberfläche der Software im entsprechenden Fall angezeigt.

4

Speicherung



Bei der herkömmlichen Speicherung digitalen Beweismaterials arbeiten Ermittler unabhängig voneinander auf einzelnen Workstations innerhalb einer Multi-Silo-Konfiguration. Die Beweisdatei wird, mehr oder weniger unsicher, auf der Workstation gespeichert oder täglich von einem Speicherserver auf die Workstation übertragen, so dass das Netzwerk durch ständige Übertragungen sehr großer Dateien belastet wird. Eine derartige Struktur bietet nicht die schnelle verteilte Verarbeitung, Größeneffekte und beträchtlichen Kosteneinsparungen einer Organisationsarchitektur mit paralleler Verarbeitung und Tiered Storage. Darüber hinaus ist es bei einer solchen Konfiguration zumindest schwierig, Daten effizient freizugeben oder mit internen und externen Teams zusammenzuarbeiten, regelmäßige und zuverlässige Datensicherungen zu gewährleisten, Dateiänderungen zu überprüfen und, besonders wichtig, für Integrität und Sicherheit der Dateien zu sorgen.

Effizienz

Die digitale Kriminaltechniklösung von Dell Konfiguration kann für verschiedenste IT-Konfigurationen angepasst werden. Je mehr eine Konfiguration einem echten Organisationsdesign entspricht, also aus Workstations, dedizierten, für eine verteilte Verarbeitung geeigneten Verarbeitungsservern, einer auf paralleler statt serieller Kommunikation basierenden Netzwerkinfrastruktur sowie Speicher besteht, desto größer ist die Effizienz. Der Datenverkehr im Netzwerk ist weniger umfangreich und verläuft schneller, da verteilte Prozessoren den Großteil der Arbeit erledigen – das Netzwerk überträgt lediglich das Ergebnis dieser Arbeit und nicht die eigentlichen Beweisdaten.

Wenn Beweisdateien auf dem Server statt auf der Workstation gespeichert werden, kann der Analytiker die Workstation zum Initiieren und Überwachen *mehrerer* Aufgaben einsetzen und ist so nicht auf die Verarbeitung einer einzelnen Aufgabe beschränkt. Außerdem lassen sich Analysen noch schneller abschließen, da mehrere Analytiker und Sachverständige, etwa Fremdsprachenspezialisten, auf verschiedenen Workstations gleichzeitig an derselben *.E01-Datei arbeiten können.

Aufgaben lassen sich entsprechend ihrer Schwierigkeit auswählen und Analytikern mit unterschiedlichem Erfahrungsgrad zuweisen. So können etwa Analytiker mit weniger Erfahrung die zeitintensive Aufgabe übernehmen, Grafikdateien aus einer *.E01-Datei zu extrahieren, während erfahrene Analytiker ihre Arbeitszeit eher für die komplexere Überprüfung und Analyse dieser Grafikdateien aufwenden sollten.

Skalierbarkeit

Die für das Rechenzentrum vorgesehenen Lösungskomponenten sind, auf Back-End-Seite, modular aufgebaut und sind per Design skalierbar. Da das Rechenzentrum die Rechenlast übernimmt, müssen Workstations nicht mit zusätzlicher Speicher- oder Rechenleistung ausgestattet werden. Tatsächlich können äußerst günstige, kompakte Terminals für den Zugriff auf erforderliche Beweisdateien und die im Rechenzentrum gespeicherte Analysesoftware verwendet werden.

Sicherheit

Aufgrund des stärker werdenden Trends, immer mehr Informationen und Daten anzusammeln, werden unser Datenspeichersysteme in zunehmenden Maß verwundbar. Gleichzeitig sollte der Zugriff auf gespeichertes Beweismaterial der am strengsten kontrollierte Bereich eines digital-kriminaltechnischen Systems sein. Dabei hat sich die Umsetzung einer dreistufigen Strategie bewährt:

- streng reglementierter physikalischer Zugriff, der den Zugriff auf die Hardware mit den Beweisdaten beschränkt
- eine administrative Kontrollschicht, die den Einsatz von Gruppenrichtlinien vorsieht
- computerbasierte Sicherheit, etwa Richtlinien zur Erstellung sicherer Kennwörter

Nachdem Umfang und Struktur an die jeweiligen Anforderungen angepasst wurden (siehe „Erfassung“ auf Seite 39), gilt daher das Hauptaugenmerk einer Behörde bei der Speicherfrage dem Thema Sicherheit.

Physikalische Zugriffsschicht

Die Dateien auf Ihrem Beweismaterialserver für digitale Forensik sollten sicherer als alle anderen Dateien in Ihrer Organisation, einschließlich Personalakten, aufbewahrt werden.

Beachten Sie die folgenden Vorschläge:

- Stellen Sie die Prüfserver und Datenspeicher in einem dedizierten Bereich des Prüflabors auf. Auf diese Weise sind alle Server, Data Warehouses, physikalischen Kabel, Switches und Router durch dieselben Sicherheitsvorkehrungen, die den Zutritt zum Labor beschränken, physikalisch geschützt.
- Setzen Sie Protokolle zur Zugangskontrolle (etwa Fingerabdruck- und Netzhautscanner) oder Smart Cards ein.
- Leiten Sie sämtlichen Datenverkehr über Netzwerk-Switches, die ausschließlich den Prüfservern und -Workstations vorbehalten und an diese physikalisch angeschlossen sind.

Administrative Kontrollschicht und Active Directory

Ihr Lösungskonfiguration wird auf einem Windows-Betriebssystem ausgeführt. Daher werden im weiteren Verlauf dieses Kapitels Windows, seine Active Directory-Gruppe und Benutzer-Sicherheitsfunktionen beschrieben. Active Directory baut auf Gruppensicherheit und den entsprechenden Funktionen auf. Bei einer Gruppe handelt es sich um Benutzer oder Computer einer Domäne. Die beiden grundlegenden Gruppentypen sind *Verteilergruppen* (zur E-Mail-Verteilung) und *Sicherheitsgruppen*. Die Einrichtung von Sicherheitsgruppen ermöglicht es, sicherheitsbezogene Richtlinien zu erstellen und anzuwenden, z. B.:

- Zugriff auf freigegebene Ressourcen und Ebene dieses Zugriffs
- Benutzerberechtigungen, einschließlich Kennwortanforderungen
- Richtlinien für Kontosperrungen
- Richtlinien für Softwareeinschränkung
- Verteilung von Sicherheitspatches auf Notebooks, Desktop-PCs und Servern

Sie können beispielsweise eine Gruppe mit administrativen Workstations und eine zweite Gruppe mit administrativen Benutzern erstellen. Anschließen können Sie die Gruppenrichtlinienobjekte dazu verwenden, den Zugriff auf diese Workstations und Mitglieder der administrativen Benutzergruppe zu beschränken. (Weitere Informationen zum Arbeiten mit Gruppenrichtlinienobjekte finden Sie unter „Anwenden von Sicherheitsrichtlinien mit Gruppenrichtlinienobjekten“ auf Seite 70.)

Computerbasierte Sicherheitsschicht und Active Directory

Active Directory enthält auch Kerberos, ein Sicherheitsprotokoll zur Netzwerkauthentifizierung, das Knoten die Kommunikation über nicht sichere Netzwerke erlaubt, damit sie auf sichere Weise einen gegenseitigen Nachweis für ihre Identität erbringen können. Unter „Active Directory-Benutzerkonten“ auf Seite 73 finden Sie weitere Informationen zum Arbeiten mit Benutzerkonten, unter „Active Directory-Unterstützung für Richtlinien zum Erstellen sicherer Kennwörter“ auf Seite 71 finden Sie weitere Informationen zum Erstellen von Kennwörtern.

Zusätzliche Informationen zum Thema Sicherheit und digitale Forensik

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

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

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

Tiered Storage

Die digitale Kriminaltechniklösung von Dell nutzt Tiered Storage-Strategien, um dem schnellen Datenwachstum bei gleichzeitiger Kostenkontrolle Herr zu werden. Eine Mischung von SATA- und SAS-Laufwerken mit unterschiedlich hohen Kapazitäten und Leistungsstufen können auf die Anforderungen von Datenprofilen angepasst werden. Dieser Mix kann dann regelmäßig einer erneuten Bewertung unterzogen werden, um auch weiterhin einen optimierten Betrieb sicherzustellen. Normalerweise werden wichtige Daten, etwa für Fälle in der Analysephase, auf leistungsstarken, hochpreisigen Laufwerken gespeichert, während weniger dringliche Daten, etwa Dateien für gerade begonnene Berufungsverfahren oder geschlossene Fälle, auf günstigere Laufwerke hoher Kapazität verschoben werden.

Abbildung 4-1. Tiered Storage für Archivierung und Abruf

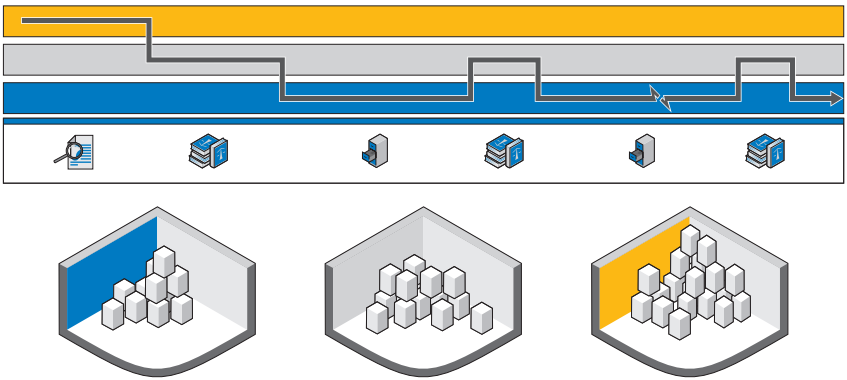


Abbildung 4-1 zeigt den empfohlenen Pfad für die Speicherung digitalen Beweismaterials, und zwar von der Beweissammlung bis zur langfristigen Speicherung auf Band oder endgültigen Löschung.

Archivierung und Abruf von Beweismaterial im Lebenszyklus eines Falles

Beschlagnahme von Beweismaterial (Analyse) – Wenn das digitale Gerät erstmalig beschlagnahmt wird, ist ein kriminaltechnisches High-Tech-Labor bestrebt, potenzielles Beweismaterial so schnell wie möglich vom jeweiligen Gerät zu ziehen und mit dem Analysevorgang zu beginnen. Je schneller ein Analytiker eine Beweisdatei durchsuchen und indizieren kann, desto schneller kann eine Entscheidung darüber getroffen werden, ob der Fall weiterverfolgt wird.

Identifizierung von Beweismaterial (Präsentation) – Wenn während der Analysephase potenzielles Beweismaterial gefunden wurde, sind anschließend möglicherweise verschiedene Fähigkeiten und Kenntnisse (im Bereich Sprachen, technische Zeichnungen, Rechnungsweisen usw.) gefragt. Das Beweismaterial muss nun von den für die Bewertung verantwortlichen Teams kategorisiert werden. Die heiße Verarbeitungsphase ist nun vorüber, so dass das Beweismaterial auf langsamerem, kosteneffizientem Speicher langfristig abgelegt werden kann.

Warten auf das Gerichtsverfahren (Archivierung) – Nachdem sämtliches potenzielles Beweismaterial gesammelt wurde und der Fall voranschreitet, besteht normalerweise kein Anlass, Images mit Falldaten und Beweismaterial im Online-Speicher zu belassen, wo sie sofort abrufbar sind. Unter normalen Umständen kann das Labor *Tage mit Fallabrufen* problemlos bewältigen. Dies kann beispielsweise proaktiv geschehen, wenn Falldaten für ein bekanntes zukünftiges Ereignis benötigt werden. Dieser Ansatz reduziert die Speicherkosten im forensischen Labor, da nicht alle Daten im Labor gespeichert werden müssen. Ungeachtet ihrer aktuellen Relevanz können sie nahtlos auf langsameren Speicher verschoben werden.

Gerichtsverfahren (Präsentation) – Kommt der Fall vor Gericht, ist das forensische Labor an einem schnellen Zugriff auf das Beweismaterial und die Falldaten interessiert, um während des Gerichtsverfahrens auf Fragen antworten zu können.

Freiheitsstrafe (Archivierung) – Wird eine Freiheitsstrafe verhängt, ist es in den meisten Ländern vorgeschrieben, dass Beweismaterial und Falldateien von Polizei oder den Justizbehörden für einen Mindestzeitraum, während der Haftzeit plus einer angemessenen Frist zur Einlegung einer Berufung oder 99 Jahre lang aufbewahren sind. Das Ziel lautet hier, die Daten auf einem langfristigen, günstigen Speichermedium abzulegen, das die Integrität und Vertraulichkeit der Daten schützt.

Berufung (Präsentation) – Im Falle einer Berufung müssen die Falldaten und das Beweismaterial ggf. zur weiteren Analyse oder genauen Untersuchung wieder abgerufen werden. Ein solcher Abruf muss zwar zeitnah erfolgen, allerdings werden die Daten nur äußerst selten sofort benötigt.

Löschung – In den meisten Ländern sind öffentliche Stellen nicht dazu berechtigt, Daten nach Ablauf der gesetzlich vorgeschriebenen Aufbewahrungsfristen auf unbestimmte Zeit zu archivieren. Es muss ein einfacher Prozess zum Löschen dieser Daten vorhanden sein. Dieser Prozess ist ggf. ebenfalls nach einem Freispruch erforderlich, der die Löschung der entsprechenden Daten nach sich zieht.

Einrichten von Speichersicherheit mit der digitalen Kriminaltechniklösung von Dell und Active Directory

Erstellen und Füllen von Gruppen in Active Directory

Gruppen werden durch Active Directory-Domänendienste (Windows Server 2008) festgelegt.

Erstellen einer neuen Gruppe (Windows Server 2008)

1. Klicken Sie auf **Start→ Verwaltung→ Active Directory-Verwaltungscenter**.
2. Klicken Sie im Fensterbereich für die Navigation mit der rechten Maustaste auf den Knoten, dem Sie eine neue Gruppe hinzufügen möchten. Klicken Sie auf **Neu**. Klicken Sie dann auf **Gruppe**.
3. Geben Sie den Namen der neuen Gruppe ein.
4. Wählen Sie die entsprechende Option unter **Gruppenbereich** aus.
5. Wählen Sie den **Gruppentyp** aus.
6. Wählen Sie **Vor zufälligem Löschen schützen** aus.
7. Ändern Sie die Abschnitte **Verwaltet von**, **Mitglied von** sowie **Mitglieder** und klicken Sie dann auf **OK**.

Hinzufügen von Mitgliedern zu einer Gruppe (Windows Server 2008)

1. Klicken Sie auf **Start→ Verwaltung→ Active Directory-Verwaltungscenter**.
2. Klicken Sie im Fensterbereich für die Navigation auf den Ordner mit der Gruppe.
3. klicken Sie mit der rechten Maustaste auf die Gruppe und klicken Sie dann auf **Eigenschaften**.
4. Wählen Sie auf der Registerkarte **Mitglieder** auf **Hinzufügen**.
5. Geben Sie den Namen des Benutzers, des Computers oder der Gruppe ein, der bzw. die hinzugefügt werden soll, und klicken Sie dann auf **OK**.

Anwenden von Sicherheitsrichtlinien mit Gruppenrichtlinienobjekten

Sobald eine Gruppe erstellt wurde, können Sie die Sicherheitseinstellungen und anderen Attribute zusammen auf die Mitglieder dieser Gruppe anwenden, indem Sie ein Gruppenrichtlinienobjekt erstellen und konfigurieren. Hierdurch wird die Sicherheit für Benutzer und Ressourcen bei Änderungen in Ihrem für die digitale Forensik zuständigen Organisationsbereich gewahrt.

Erstellen und Bearbeiten von Gruppenrichtlinienobjekten

Erstellen eines neuen Gruppenrichtlinienobjekts (Windows Server 2008)

In Windows Server 2008 werden Gruppenrichtlinienobjekte mithilfe der Gruppenrichtlinien-Verwaltungskonsole (GPMC, Group Policy Management Console) verwaltet.

1. Zum Öffnen der Gruppenrichtlinien-Verwaltungskonsole klicken Sie auf **Start→ Verwaltung→ Gruppenrichtlinienverwaltung**.
2. Navigieren Sie zu der Struktur und der Domäne, in der Sie das neue Objekt erstellen möchten. Klicken Sie dann auf **Gruppenrichtlinienobjekte**.
3. Klicken Sie auf **New**.
4. Geben Sie den Namen des neuen Gruppenrichtlinienobjekts ein und klicken Sie dann auf **OK**.

Bearbeiten eines neuen Gruppenrichtlinienobjekts (Windows Server 2008)

In Windows Server 2008 werden Gruppenrichtlinienobjekte mithilfe der Gruppenrichtlinien-Verwaltungskonsole verwaltet.

1. Zum Öffnen der Gruppenrichtlinien-Verwaltungskonsole klicken Sie auf **Start→ Verwaltung→ Gruppenrichtlinienverwaltung**.
2. Navigieren Sie zu der Struktur und der Domäne mit dem Gruppenrichtlinienobjekt und klicken Sie dann auf **Gruppenrichtlinienobjekte**.
3. klicken Sie mit der rechten Maustaste auf das Gruppenrichtlinienobjekt.
4. Ändern Sie die Einstellungen wie erforderlich und speichern Sie sie anschließend.

Active Directory-Unterstützung für Richtlinien zum Erstellen sicherer Kennwörter

Active Directory unterstützt verschiedene Authentifizierungsrichtlinien, darunter Smart Cards, sicheres Kennwort und Einstellungen für Kontosperrungen.

Kennwörter und andere Authentifizierungsrichtlinien werden mithilfe von Gruppenrichtlinienobjekten erstellt. Weitere Informationen zum Erstellen und Beareiten eines Gruppenrichtlinienobjekts finden Sie unter „Anwenden von Sicherheitsrichtlinien mit Gruppenrichtlinienobjekten“ auf Seite 70.

Empfohlene Einstellungen für sichere Kennwörter

Die folgenden Werte werden zum Konfigurieren von Kennworteinstellungen empfohlen:

- Kennwortchronik erzwingen – Die Anzahl eindeutiger Kennwörter, die verwendet werden muss, bevor ein Kennwort wiederverwendet werden darf. Stellen Sie diesen Wert auf 24 ein.
- Maximales Kennwortalter – Kennwörter müssen alle *x* Tage geändert werden. Stellen Sie diesen wert auf 90 ein.
- Minimales Kennwortalter – Die Anzahl der Tage, die ein Kennwort aktiv sein muss, bevor es geändert werden kann. Stellen Sie diesen Wert auf 1 oder 2 ein.

- Minimale Kennwortlänge – Stellen Sie diesen Wert auf 8 oder 12 Zeichen ein.
- Kennwort muss Komplexitätsvoraussetzungen entsprechen – Stellen Sie diesen Wert auf **Aktiviert** ein. Die folgenden Richtlinien werden angewendet:
  - Kennwörter müssen mindestens 6 Zeichen lang sein.
  - Kennwörter müssen Zeichen aus mindestens drei dieser vier Kategorien enthalten:
    - Großbuchstaben
    - Kleinbuchstaben
    - Ziffern (0-9)
    - Symbole
  - Kennwörter sind nicht zulässig, wenn sie drei oder mehr aufeinander folgende Zeichen des Konto- oder Benutzernamens aufweisen.

Abgestimmte Kennwortrichtlinien

In Windows Server 2008 werden Kennworteinstellungsobjekte (Password Setting Objects, PSOs) von den Active Directory-Domänendiensten unterstützt. Diese Objekte gelten für eine bestimmte globale Sicherheitsgruppen oder bestimmte Benutzer einer Domäne. Ein Kennworteinstellungsobjekt kann die Kennwortlänge (in Zeichen), die Kennwortkomplexität, das minimale und maximale Kennwortalter sowie andere Attribute festlegen.

Dementsprechend können Sie mehrere Kennworteinstellungsobjekte erstellen, die der Organisationsstruktur Ihrer Einrichtung für digitale Forensik entsprechen. Beispielsweise ist es möglich, mithilfe von Kennworteinstellungsobjekten längere Kennwörter mit monatlicher Ablauffrist für administrative Benutzer und kürzere Kennwörter mit quartalsmäßiger Ablauffrist für Analytiker zu implementieren.

Active Directory-Benutzerkonten

Einrichten von Benutzerkonten für forensische Analytiker

1. Öffnen Sie **Active Directory-Benutzer und -Computer**:
   a. Klicken Sie auf **Start→ Systemsteuerung**.
   b. Doppelklicken Sie auf **Verwaltung** und dann auf **Active Directory-Benutzer und -Computer**.
2. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf den Ordner, dem Sie ein Benutzerkonto hinzufügen möchten.

   Wo?

   Active Directory-Benutzer und -Computer/*Domänenknoten*/*Ordner*
3. Zeigen Sie auf **Neu** und klicken Sie dann auf **Benutzer**.
4. Geben Sie in das Feld **Vorname** den Vornamen des Benutzers ein.
5. Geben Sie in das Feld **Initialen** die Initialen des Benutzers ein.
6. Geben Sie in das Feld **Nachname** den Nachnamen des Benutzers ein.
7. Ändern Sie **Vollständiger Name**, um Initialen oder eine umgekehrte Reihenfolge von Vor- und Nachnamen hinzuzufügen.
8. Geben Sie unter **Benutzeranmeldename** den Benutzeranmeldenamen ein, klicken Sie auf das Benutzerprinzipalnamens-Suffix in der Dropdown-Liste und dann auf **Weiter**.

   Wenn der Benutzer einen anderen Namen zum Anmelden bei Computern mit Windows 95, Windows 98 oder Windows NT verwendet, können Sie den Benutzeranmeldenamen im Feld **Benutzeranmeldename (vor Windows 2000)** ändern.
9. Geben Sie in die Felder **Kennwort** und **Kennwort bestätigen** das Kennwort des Benutzers ein und wählen Sie dann die entsprechenden Kennwortoptionen aus.

ANMERKUNG: Um dieses Verfahren durchführen zu können, müssen Sie in Active Directory ein Mitglied der Gruppe „Konten-Operatoren", „Domänen-Admins" bzw. „Organisations-Admins" sein oder es muss Ihnen die entsprechende Berechtigung übertragen worden sein. Nach bewährter Sicherheitspraxis sollten Sie *Ausführen als* zur Durchführung dieses Verfahrens verwenden. Weitere Informationen hierzu finden Sie unter *Lokale Standardgruppen*, *Standardgruppen* sowie *Verwenden von „Ausführen als"*.

Einrichten eines FTK-Dienst-Manager-Kontos

ANMERKUNG: Während der FTK-Installation werden Sie aufgefordert, den Namen des Benutzerkontos einzugeben, das Sie zum Verwalten der Funktion für die verteilte Verarbeitung verwenden werden. Nicht verwenden.

Wenn Sie die Funktion für die verteilte Verarbeitung von FTK als eines Ihrer digitalen forensischen Tools verwenden, müssen Sie in Active Directory ein FTK-Dienst-Manager-Konto für die Handhabung automatischer Kennwortaktualisierungen erstellen. Während der FTK-Installation werden Sie aufgefordert, den Namen des Benutzers einzugeben, der die Funktion für die verteilte Verarbeitung überwachen und verwalten wird. Dieses Konto muss in Active Directory als ein Dienst erstellt werden und über Administratorrechte verfügen (es sollte aber kein Administratorkonto sein), damit zwischen FTK und dem Beweismaterialserver ein fortlaufender Handshake bereitgestellt wird, wie laut Funktion für die verteilte Verarbeitung erforderlich.

1. Öffnen Sie in Active Directory die **Verwaltung** und klicken Sie dann auf **Active Directory-Benutzer und -Computer**.
2. Doppelklicken Sie in der Konsolenstruktur auf den Domänenknoten.
3. Klicken Sie im Fensterbereich **Details** mit der rechten Maustaste auf die Organisationseinheit, in der Sie das Dienstkonto hinzufügen möchten. Wählen Sie **Neu** aus und klicken Sie dann auf **Benutzer**.
4. Geben Sie im Feld **Vorname** als Bezeichnung für das Dienstkonto `FTKServMgr` ein; lassen Sie das Feld **Nachname** leer.
5. Ändern Sie **Vollständiger Name** wie gewünscht.
6. Geben Sie in das Feld **Benutzeranmeldename** die Bezeichnung `FTKServMgr` ein. Das Dienstkonto meldet sich mit dem von Ihnen eingegebenen Namen an. Klicken Sie in der Dropdown-Liste auf das **Benutzerprinzipalnamens-Suffix**, der dem Anmeldenamen für das Dienstkonto angehängt werden muss (nach dem @-Symbol). Klicken Sie auf **Weiter**.
7. Geben Sie in die Felder **Kennwort** und **Kennwort bestätigen** das Kennwort für das Dienstkonto ein.
8. Wählen Sie die entsprechenden Kennwortoptionen und klicken Sie dann auf **Weiter**.
9. Klicken Sie auf **Fertig stellen**, um den Erstellvorgang des Dienstkontos abzuschließen.

Erstellen eines nicht administrativen Benutzerkontos

1. Melden Sie sich bei einem Windows Vista-Computer mit einem administrativen Benutzerkonto an.
2. Öffnen Sie das **Start** menü. Klicken Sie mit der rechten Maustaste auf **Computer** und klicken Sie dann auf **Verwalten**.
3. klicken Sie auf den Pfeil neben **Lokale Benutzer und Gruppen**.
4. Klicken Sie mit der rechten Maustaste auf **Benutzer** und klicken Sie dann auf **Neuer Benutzer**.
5. Geben Sie den Namen des Benutzers ein, für den Sie ein Konto erstellen. Wenn Sie den Benutzer beispielsweise **webbenutzer1** nennen möchten, geben Sie `webbenutzer1` in das Feld **Benutzername** und in das Feld **Vollständiger Name** ein.
6. Geben Sie in die Felder **Kennwort** und **Kennwort bestätigen** ein Kennwort ein, an das Sie sich erinnern können.

ANMERKUNG: Bei Kennwörtern wird zwischen Groß- und Kleinschreibung unterschieden. Das Kennwort, das Sie in die Felder **Kennwort** und **Kennwort bestätigen** eingeben, muss übereinstimmen, damit das Benutzerkonto hinzugefügt werden kann.

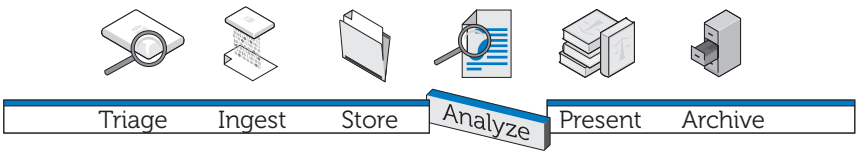
7. Deaktivieren Sie das Kontrollkästchen **Benutzer muss Kennwort bei der nächsten Anmeldung ändern**.
8. Aktivieren Sie die Kontrollkästchen **Kennwort läuft nie ab** und **Benutzer kann Kennwort nicht ändern**.
9. Klicken Sie auf **Erstellen** und dann auf **Schließen**.
10. Klicken Sie auf **Datei** und dann auf **Beenden**.

Einrichten von Sicherheitseinstellungen für Fall- und Beweisdateien

1. Navigieren Sie in **Windows Explorer**, zu der Datei, für Sie Sie Dateiberechtigungen festlegen möchten. Klicken Sie mit der rechten Maustaste auf die Datei und wählen Sie dann **Eigenschaften** aus.
2. Klicken Sie auf die Registerkarte **Sicherheit**.
3. Deaktivieren Sie ggf. das Kontrollkästchen neben **Jeder**.
4. Fügen Sie nur die Benutzer hinzu, die gemäß Ihrer Arbeitsplatzrichtlinie Zugriff auf die Datei benötigen.
   a. Klicken Sie auf **Hinzufügen**.
   b. Geben Sie in das Feld **Geben Sie die zu verwendenden Objektnamen ein** die Namen der entsprechenden Benutzer ein. Klicken Sie dann auf **OK**.
   c. Ändern Sie die **Berechtigungen** für jeden Benutzer gemäß Ihrer Arbeitsplatzrichtlinie.

5

Analyse



Ein Ermittler muss Beweismaterial in Form von Daten verschiedenen Typen der Analyse unterziehen können, darunter die Dateisignatur- und Hash-Analyse sowie eine umfangreiche Indizierung und Stichwortsuche. All diese Analysen bedürfen einer enormen Verarbeitungsleistung, da Beweisdateien für einen einzelnen Fall schon im Terabyte-Bereich liegen können, und die Verarbeitung dieser Dateien dauert mitunter dutzende Stunden – sogar Tage – bei den heutzutage häufig in Rechenzentren anzutreffenden Architekturen. Ermittler, die versuchen, diese Analyse auf einem einzelnen Workstation-Rechner durchzuführen, sollten den gerade genannten Aspekt bei der Zeitplanung für die Fallbearbeitung berücksichtigen, da die Analyse und Indizierung eines Falles bereits die vollständigen Hardwareressourcen des Ermittlers aufbrauchen kann. Die digitale Kriminaltechniklösung von Dell bietet deutliche, sich durch eine verteilte Verarbeitung ergebende Vorteile. Und hierdurch wandelt sich das Bild zum Teil vollständig. Wir beschäftigen uns gleich mit dem Thema der verteilten Verarbeitung. Untersuchen wir aber zunächst einige Analysetypen, die in der digitalen Kriminaltechnik typischerweise Anwendung finden.

Typen der Analyse

Hash-Analyse

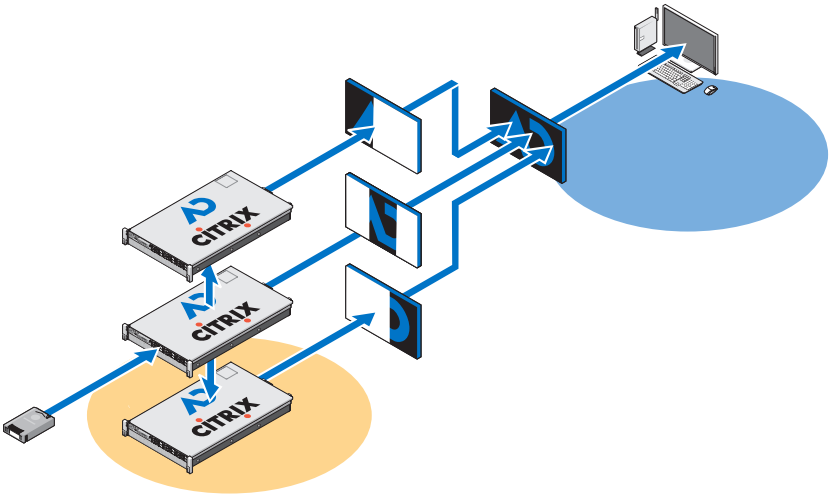
Eine Hash-Funktion nutzt kryptografische Algorithmen, um einen digitalen Fingerabdruck aus Daten zu erstellen. Das Hash kann verwendet werden, um ein Hash der Originaldaten mit einem der analysierten forensischen Daten zu vergleichen. Vor Gericht wird dies möglicherweise als Beweis zugelassen, dass es sich um zwei identische Datengruppen handelt. Bei der Hash-Analyse werden Hash-Werte der Falldatei mit denen bekannter, gespeicherter Hash-Werte verglichen.

Dateisignatur-Analyse

Jede Datei hat einen Dateityp. Dieser wird in der Regel durch die aus drei oder vier Buchstaben bestehenden Erweiterung angegeben. Eine Textdatei kann beispielsweise die Erweiterung ***.txt** aufweisen, eine Bilddatei womöglich die Erweiterung ***.jpg**. Nicht selten werden diese Dateierweiterungen zu etwas Unverfänglichem geändert – etwa wenn eine Bilddatei umbenannt und mit einer Textdateierweiterung versehen wurde, um ihren pornografischen Inhalt zu maskieren.

Jede Datei verfügt jedoch auch über einen Datei-Header mit einem Dateitypcode enthält, der sich von der Erweiterung unterscheidet und einzig einem spezifischen Dateityp vorbehalten ist. Eine ***.bmp**-Datei hat z. B. den Dateityp-Header-Code ***.bm8**. Wenn sich der Header-Code des Dateityps und die Dateierweiterung unterscheiden, muss der IT-Forensiker die Daten genauer untersuchen.

Abbildung 5-1. Verteilte Verarbeitung



Was ist die verteilte Verarbeitung?

Die *verteilte Verarbeitung* bezieht sich auf den Einsatz mehrerer Prozessoren mit jeweils eigenen Speicherressourcen, die individuell auf verschiedene Bereiche einer Computeraufgabe angewendet werden und die in der Gruppe ein Nachrichtenübertragungssystem zur gegenseitigen Kommunikation verwenden. Verteilte Verarbeitung und *parallele Verarbeitung* sind nicht das Gleiche. Die parallele Verarbeitung bezieht sich auf den Einsatz mehrerer Prozessoren, die gemeinsam dieselben Speicherressourcen verwenden.

Das folgende Beispiel liefert eine ungefähre Vorstellung der Vorteile, die sich durch eine Installation der Dell-Lösung zur verteilten Verarbeitung ergeben: Bei der verteilten Verarbeitung dauert die Analyse von fünf 200 GB großen Dateien nur 3,5 Stunden, während die Verarbeitung einer einzelnen 200 GB großen Datei auf einer eigenständigen Workstation ca. 7 bis 8 Stunden in Anspruch nehmen kann.

Mit der Auslagerung der Datenverarbeitung von Beweismaterial von der Workstation des Analytikers auf den Server ist das Ende der Fahnenstange noch nicht erreicht. Die Dell-Lösung ermöglicht außerdem die Ausführung der eigentlichen Analysesoftware auf dem Server, etwa FTK und EnCase. Hierdurch wird die Workstation zu einer integrierten Schnittstelle, die mehrere Instanzen verschiedener Forensik-Softwarepakete auf gleichzeitig angezeigten Betriebssystemen ausführen kann, ohne dass hierdurch die Clientleistung geschmälert wird.

Verwenden der verteilten Verarbeitung in FTK 3.1

Mithilfe der verteilten Verarbeitung lassen sich zur Fallbearbeitung zusätzliche Ressourcen auf bis zu drei zusätzliche Computer gleichzeitig anwenden. Nach der Installation und Konfiguration der Engine zur verteilten Verarbeitung ist eine exponentielle Reduzierung der zur Fallbearbeitung benötigten Zeit möglich.

ANMERKUNG: Als Faustformel gilt, dass sich mit der verteilten Verarbeitung die Verarbeitungsdauer nur dann reduziert, wenn die Anzahl der zu verarbeitenden Objekte die Anzahl der im System vorhandenen Kerne um das 1000-Fache übersteigt. Auf einem System mit acht Kernen sorgen die zusätzlichen Engine-Computer zur verteilten Verarbeitung beispielsweise erst dann zu einer kürzeren Verarbeitungszeit, wenn das Beweismaterial mehr als 8.000 Elemente umfasst.

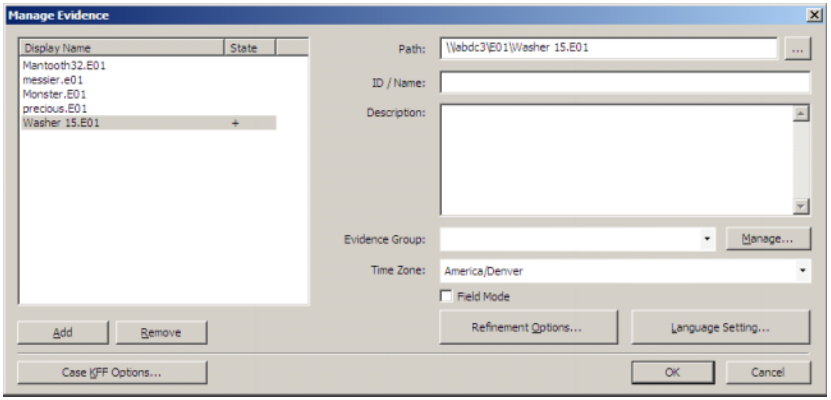
ANMERKUNG: Informationen zum Installieren und Konfigurieren des Moduls zur verteilten Verarbeitung als Teil der Lösung finden Sie im entsprechenden Abschnitt des *FTK-Benutzerhandbuchs*.

1. Vergewissern Sie sich, dass der Fallordner freigegeben ist, bevor Sie versuchen, Beweismaterial hinzuzufügen und zu verarbeiten. Wenn Sie den von Dell empfohlenen Konventionen zur Dateibenennung gefolgt sind, sollte sich der Fallordner auf dem Arbeitsbereichslaufwerk **W:/** befinden. Wenn Sie sich nicht sicher sind, wo der Fallordner abgelegt ist, wenden Sie sich an den Systemadministrator.
2. Geben Sie den Pfad zum Fallordner in das Dialogfeld **Create New Case** ein, und zwar im UNC-Format:

   `(\\[computername_oder_IP_adresse]\[pfadname]\[dateiname])`
3. Klicken Sie auf **Detailed Options** und wählen Sie wie gewohnt die gewünschten Optionen aus.
4. Klicken Sie auf **OK**, um zum Dialogfeld **New Case Options** zurückzukehren, und setzen Sie ein Häkchen neben der Option **Open the case**. Klicken Sie auf **OK**, um den neuen Fall anzulegen und ihn zu öffnen.
5. Klicken Sie auf **Add**, nachdem der neue Fall geöffnet wurde. Daraufhin wird das Dialogfeld **Manage Evidence** automatisch geöffnet. Wählen Sie die hinzuzufügende Beweisdatei aus und klicken Sie dann auf **Open**.
6. Der Pfad zum Beweismaterial ist standardmäßig durch den Laufwerksbuchstaben gekennzeichnet. Ändern Sie den Pfad in das UNC-Format, indem Sie den Laufwerksbuchstaben in den Rechnernamen bzw. die IP-Adresse, wo sich die Beweisdatei befindet, abändern. Halten Sie sich dabei an folgende Syntax:

   `\\[computername_oder_IP_adresse]\[padname]\[Dateiname]`
7. Lassen Sie den Rest des Pfads unverändert.
8. Der UNC-Pfad zum Beweismaterial wird in folgender Abbildung dargestellt:

Abbildung 5-2. Dialogfeld „Manage Evidence“



9 Klicken Sie auf **OK**.

Überprüfen der Installation

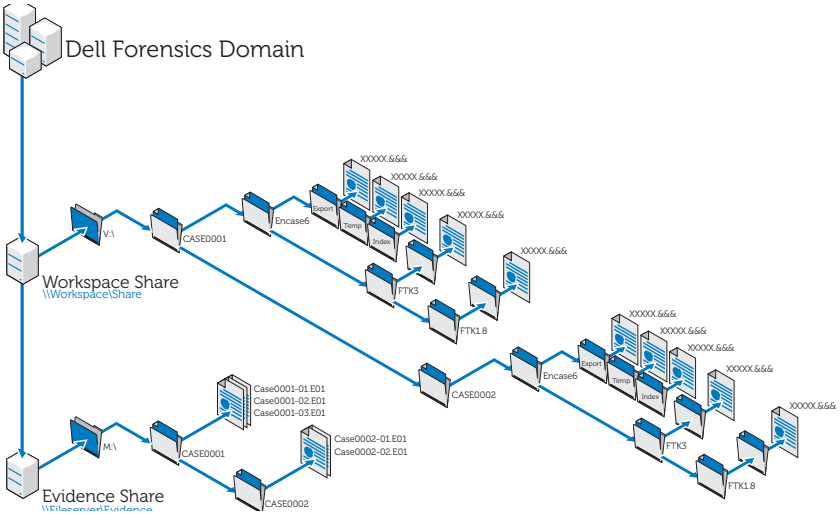
Öffnen Sie nach Abschluss der Installation den **Task-Manager** auf dem Remote-Computer und lassen Sie ihn geöffnet, während Sie Beweismaterial hinzufügen und mit der Verarbeitung beginnen. Diese Schritte ermöglichen Ihnen, die Aktivität von **ProcessingEngine.exe** auf der Registerkarte **Prozesse** zu überwachen.

Die Engine zur verteilten Verarbeitung wird bei einem Fall erst ab einer Menge von ca. 30.000 Elementen aktiviert. Im Falle einer Aktivierung können Sie beobachten, dass sich die CPU-Auslastung in Prozent und die Speicherbelegung für **ProcessingEngine.exe** im **Task-Manager** erhöhen.

Suchen nach Dateien im Netzwerk

Gemäß bewährten Verfahren müssen Beweismaterial und Arbeitsdateien im Netzwerk getrennt voneinander gespeichert werden. Dell empfiehlt die Einrichtung zweier freigegebener Laufwerke sowie die darauf basierende Erstellung von Falldateien und Unterdateien, siehe Abbildung 5-3.

Abbildung 5-3. Von Dell empfohlene Dateistruktur



Analysieren mit FTK

Öffnen eines bestehenden Falls

Über das Dateimenü

1. Wählen Sie in FTK das Menü **File** und dann den Befehl **Open Case**.
2. Markieren Sie den zu öffnenden Fall und klicken Sie darauf, um den Fall aufzurufen.

ANMERKUNG: Sämtliche Falldateien tragen die Bezeichnung **case.ftk**. Die **case.ftk**-Datei für jeden Fall ist im entsprechenden Fallordner gespeichert.

Über die Befehlszeile

Geben Sie Folgendes in die Befehlszeile ein:

```
pfad_zur_ftk_programmdatei\ftk.exe /OpenCase
fall_zielverzeichnis
```

Verarbeiten des Beweismaterials eines Falles

FTK verarbeitet Beweismaterial beim Anlegen eines Falles oder beim späteren Hinzufügen von Beweismaterial zu dem Fall. Anweisungen zum Anlegen eines neuen Falles finden Sie unter „Anlegen eines neuen Falles“ auf Seite 62 oder im *FTK-Benutzerhandbuch*. Anweisungen zum Hinzufügen von Beweismaterial zu einem bestehenden Fall finden Sie unter „Hinzufügen von Beweismaterial zu einem Fall“ auf Seite 62 oder im *FTK-Benutzerhandbuch*. Weitere Informationen finden Sie unter „Relevante Dokumentation und Ressourcen“ auf Seite 16.

Analysieren mit EnCase

Öffnen eines bestehenden Falls

1. Wählen Sie **File→ Open** aus.
2. Navigieren Sie zu dem Fall und klicken Sie auf **Open**.

Erstellen einer Analyseaufgabe

1. Klicken Sie im Hauptdialogfeld **Source Processor** auf die Registerkarte **Analysis Jobs**.
2. Klicken Sie auf **New**. Das Dialogfeld **Create Analysis Job/Job Name** wird angezeigt.

   Standardmäßig ist die Aufgabe wie folgt benannt: Job__[jjjj_mm_tt__hh_mm_ss], z. B. Job___2009_06_24__03_42_42_PM.

   Am Anfang und Ende eines Aufgabenamens dürfen weder Leerzeichen noch eines der folgenden Zeichen stehen: \ / : * ? " < > |
3. Geben Sie einen Aufgabenamen ein und klicken Sie auf **Next**. Das Dialogfeld **Create Analysis Job/Module Selection** wird angezeigt.

   Das Dialogfeld zeigt im linken Fensterbereich Modulordner, im rechten Fensterbereich einzelne Module innerhalb dieser Order an.

Wenn ein Modul Teil einer Analyseaufgabe ist, aber bei Ausführung der Aufgabe für die Sammlung keine Daten für das Modul vorhanden sind, wird das Modul ignoriert. Diese Funktion ermöglicht die Erstellung generischer Analyseaufgaben für verschiedene gesammelte Datensätze.

4 Aktivieren Sie das Kontrollkästchen für das Modul.

Es können mehr als ein Modul ausgewählt werden.

Analysemodule verfügen nicht über vom Benutzer konfigurierbare Einstellungen.

Zum Auswählen aller Module einer Gruppe setzen Sie im linken Fensterbereich ein Häkchen neben dem Ordnernamen dieser Gruppe.

5 Klicken Sie auf **Finish**.

ANMERKUNG: Analyseaufgaben enthalten u. U. eine Liste verfügbarer Module, die in Erfassungsaufgaben nicht vorhanden sind. Diese Module werden als Legacy-Module identifiziert, so dass Sie Daten, die in vorherigen Quellprozessor-Versionen mit nicht länger existierenden Modulen gesammelt wurden, analysieren können.

Ausführen einer Analyseaufgabe

1 Wählen Sie auf der Registerkarte **Collected Data** das zu analysierende Beweismaterial, indem Sie zunächst den Aufgabennamen im linken Fensterbereich auswählen. Wählen Sie dann auf der rechten Seite die eigentlichen Beweisdateien aus.

2 Klicken Sie auf **Run Analysis**. Das Dialogfeld **Select Analysis to Run** wird geöffnet.

3 Wählen Sie die Analyseaufgabe aus und klicken Sie dann auf **Run**. Der Quellprozessor führt die Analyse für das ausgewählte Beweismaterial aus. Nach Abschluss der Analyse wird der Datenbrowser angezeigt.

Durchführen einer Signaturanalyse

1 Klicken Sie auf **Search**.

2 Aktivieren Sie unten rechts im Bereich **Additional Options** das Kontrollkästchen **Verify file signatures**. Klicken Sie dann auf **Start**. Die Routine zur Signaturanalyse wird im Hintergrund ausgeführt. Bei Abschluss informiert ein Dialogfeld über den beendeten Suchvorgang. Im Dialogfeld werden der Suchstatus, Zeiten sowie Dateidaten angegeben.

Dieselben Daten können Sie in der Konsole anzeigen.

Anzeigen von Signaturanalyse-Ergebnissen

1. Klicken Sie im Fensterbereich **Tree** auf **Set Include**, um alle Dateien im Fall anzuzeigen.

   Auf dieser Ebene werden mit **Set Include** alle Objekte in der Beweisdatei ausgewählt.

2. Ordnen Sie die Spalten im Fensterbereich **Table** so an, dass die Spalten **Name**, **File Ext** und **Signature** nebeneinander erscheinen.
3. Sortieren Sie Spalten mit **Signature** auf der ersten Ebene, **File Ext** auf der zweiten Ebene und **Name** auf der dritten Ebene.

   Führen Sie einen Bildlauf nach oben oder unten durch, um sämtliche Signaturen anzuzeigen.

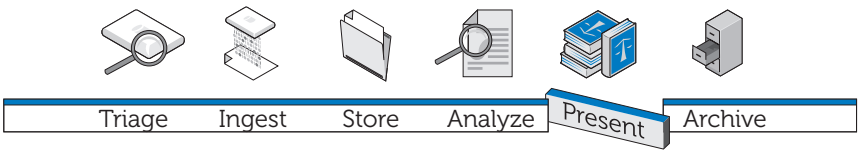
4. Klicken Sie im Fensterbereich **Tree** im Auswahlbereich **Entries** auf **Set Include**.

   Eine Liste mit Falldateien und zugehörigen Dateisignaturen sowie weiteren Daten wird im Fensterbereich **Table** angezeigt.

5. Sortieren Sie die Daten wie gewünscht.

6

Präsentation



Die Aufnahme Ihrer Analyseergebnisse in Berichte ist ein wesentlicher Bestandteil der digitalen Kriminaltechniklösung von Dell und wird hauptsächlich durch die im Rahmen dieser Lösung verwendete Forensik-Software abgewickelt.

Erstellen von Berichten mit der digitalen Kriminaltechniklösung von Dell

Erstellen und Exportieren von Berichten mit EnCase 6

1. Wählen Sie die Elemente für die Berichtserstellung aus, ob Dateien, Lesezeichen, Suchtreffer oder andere Daten.
2. Wählen Sie den zu verwendenden Berichtstyp über die Registerkarten im Fensterbereich **Tree** aus.
3. Wählen Sie auf der Registerkarte **Table** des Fensterbereichs **Table** die Elemente aus, die im Bericht erscheinen sollen.
4. Wechseln Sie von der Registerkarte **Table** zur Registerkarte **Report**.
5. Bearbeiten Sie den Bericht nach Bedarf.
6. Exportieren Sie den Bericht in ein für die Anzeige außerhalb von EnCase geeignetes Format.
   a. Klicken Sie mit der rechten Maustaste auf den Bericht und wählen Sie im Dropdown-Menü den Befehl **Export** aus. Das Dialogfeld **Export Report** wird geöffnet.

b Klicken Sie auf die entsprechende Optionsschaltfläche, um das gewünschte Ausgabeformat (TEXT, RTF oder HTML) auszuwählen.

c Geben Sie den Ausgabepfad ein oder navigieren Sie dorthin.

d Wählen Sie, falls gewünscht, die Option **Burn to Disc** aus, um das Feld **Destination Folder** zu aktivieren. Klicken Sie dann mit der rechten Maustaste auf **Archive Files**, um einen neuen Ordner zu erstellen und eine **.iso**-Datei auf einem Datenträger zu speichern.

e Klicken Sie auf **OK**.

Erstellen von Berichten mit FTK

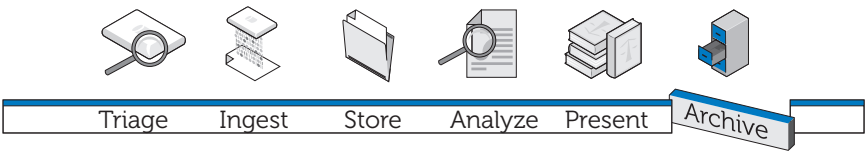
1. Klicken Sie auf **File**→ **Report**, um den **Report Wizard** zu starten.
2. Geben Sie die vom Assistenten angeforderten grundlegenden Falldaten ein.
3. Wählen Sie die Eigenschaften für Lesezeichen aus.
4. Legen Sie fest, ob und wie Fallgrafiken im Bericht präsentiert werden sollen.
5. Legen Sie fest, ob Ihr Bericht einen Abschnitt mit Dateipfaden und Dateieigenschaften von Dateien ausgewählter Kategorien enthalten soll.
6. Fügen Sie ggf. die Abschnitt **Registry Viewer** hinzu.

Anzeigen des Berichts außerhalb von FTK

1. Navigieren Sie zur der Berichtsdatei.
2. Klicken Sie auf die Berichtsdatei. Gehen Sie dann wie folgt vor:
   - Klicken Sie auf **index.htm**, um ein HTML-Dokument in einem Webbrowser zu öffnen.
   - Klicken Sie auf [*bericht*]**.pdf**, um den Bericht in einem PDF-Viewer zu öffnen.

7

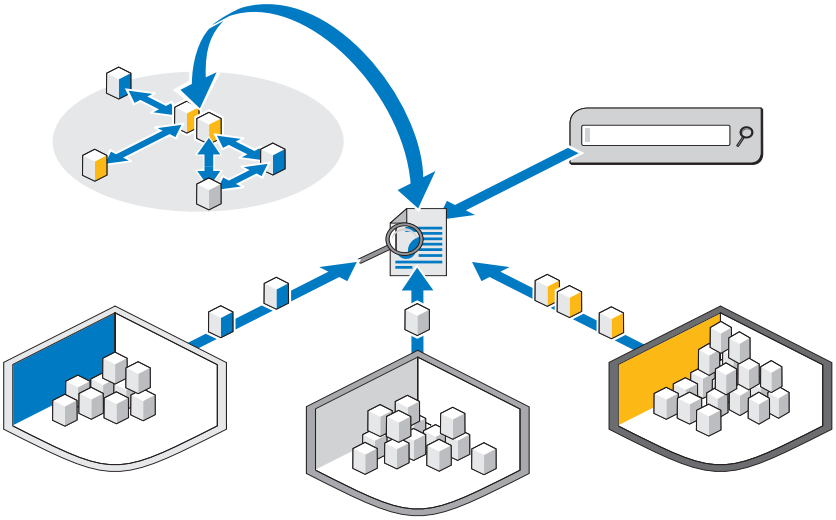
Archivierung



Ohne eine skalierbare, sichere und umfassende Archivierungs- und Abrufkomponente ist keine digitale Kriminaltechniklösung vollständig. In Ihrer digitale Kriminaltechniklösung von Dell bietet nicht nur diese Komponente, sondern noch vieles mehr. Beim Framework der Dell-Lösung wurde versucht, eine einfach Schnittstelle zu entwickeln, die mit allen forensischen Anwendungen funktioniert, um den Lebenszyklus von Beweismaterial und Falldateien steuern zu können. Da es schwierig ist, vorherzusagen, wann Daten in der Zukunft benötigt werden oder wie lange eine Ermittlung möglicherweise dauert, haben wir eine flexible Lösung entwickelt. Dabei muss jeder forensische Analytiker die Dateien bestimmen, die er abrufen und archivieren wird. Diese Lösung nutzt einen stufenbasierten Ansatz für einen auf Ihre Anforderungen zugeschnittenen Speicher – eine Mischung von SATA- und SAS-Hardware – sowie eine benutzergesteuerte Archivierung mit der On-Demand Archiving-Software von NTP.

Die Dell-Lösung besteht aus modularen Komponenten für eine skalierbare, erweiterbare Umgebung, um steigende Anforderungen in Hinblick auf Verarbeitung und Speicherung erfüllen zu können. Die formalisierte BURA-Infrastruktur der Lösung (Backup, Recovery, and Archiving; Sicherung, Wiederherstellung und Archivierung) trägt zu einer optimierten Zusammenarbeit zwischen Behörden und Einsatzkräften, auch grenzüberschreitend. Sie bedeutet eine Entlastung im Bereich der Administration durch eine größtenteils automatisiert ablaufende Datensicherung. Außerdem sorgt sie für Konsistenz zwischen ressortübergreifenden Laboren und minimiert Risiken für die digitale Kontrollkette.

Abbildung 7-1. Medien- und fallübergreifende Suchfunktionen der Dell-Lösung



Eine äußerst leistungsstarke optionale Suchkomponente ermöglicht die Korrelation von Informationen zwischen erfassten Datensätzen. Über diese Komponente lassen sich internetähnliche Suchvorgänge im kompletten Fall-Datenspeicher durchführen, sowohl nach aktiven und Online-Inhalten als auch nach archiviertem Material älterer Fälle.

Clientbasierte Ein-Klick-Archivierungslösung

Mit den Archivierungs- und Abrufwerkzeugen der digitalen Kriminaltechniklösung von Dell wird ein Analytiker in die Lage versetzt, einzelne Dateien und gesamte Verzeichnisstrukturen per Rechtsklick zu archivieren bzw. abzurufen. Der On-Demand Archiving-Software von NTP wurde um zusätzliche Kontextmenübefehle ergänzt, so dass der Benutzer nur noch Elemente auswählen und archivieren oder Daten auswählen und wiederherstellen muss. Wenn eine Datei zur Archivierung ausgewählt wurde, wird ein zusätzliches Fenster geöffnet, in dem der Benutzer zur Vorgangsbestätigung aufgefordert wird. Im Falle einer Bestätigung führt die Lösung einen Prozess im Hintergrund durch, um diese Datei entweder auf ein Bandgerät oder ein Nearline-Speichergerät zu verschieben. Dieser Prozess wird völlig nahtlos im Hintergrund abgewickelt, ohne dass die Leistung der Benutzer-Workstation im Mindesten geschmälert wird.

Nach Abschluss des Hintergrundprozesses wird das dieser Datei zugeordnete Dateisymbol grau und gibt so dem Benutzer eindeutig an, dass die Datei archiviert wurde. Ordner und Dateistruktur sind allerdings nach wie vor sichtbar, damit der Benutzer die Datei in Zukunft einfach wieder finden kann, wenn sie wiederhergestellt werden soll. Zum Wiederherstellen einer Datei muss der Benutzer lediglich durch die ursprüngliche Ordnerstruktur navigieren, nach dem wiederherzustellenden Ordner bzw. der wiederherzustellenden Datei suchen, mit der rechten Maustaste auf die Datei bzw. den Ordner klicken und dann die Wiederherstellungsoption auswählen.

Dell empfiehlt, sämtliches Beweismaterial und alle Falldateien auf einem zentralen skalierbaren NAS-Gerät mit einem zentralen, erweiterbaren Speicherpunkt zu platzieren, was die Zusammenarbeit zwischen Analytikern vereinfacht. Diese Empfehlung ermöglicht zudem die Einrichtung eines zentralen Prüfpunkt im Rahmen der Kontrollkette. Nachdem eine Datei zur Archivierung ausgewählt wurde, wird sie im nächsten verfügbaren Systemverarbeitungsfenster vom Primärspeicher auf ein sekundäres (Band- oder Nearline-)Speichergerät verschoben.

Archivierungs- und Abrufzeiten sind stark vom aktuellen Datenverkehr zum und vom zentralen NAS-Speicher, den aktuell archivierten Dateien und dem Medientyp der sekundären Speicheroption abhängig. Nearline-SATA-Hardware sorgt beispielsweise für wesentlich schnellere Abschlussraten als Bänder. Alle Dateien können auf Band zwecks zusätzlicher Sicherung verschlüsselt werden, wenn sie in die langfristige Archivierungsphase der Lösung übergehen. Hierzu ist ggf. eine zusätzliche Lizenzierung erforderlich.

Sicherungsempfehlungen von Dell

Erstellen einer Sicherungskopie von Beweismaterial und Falldateien

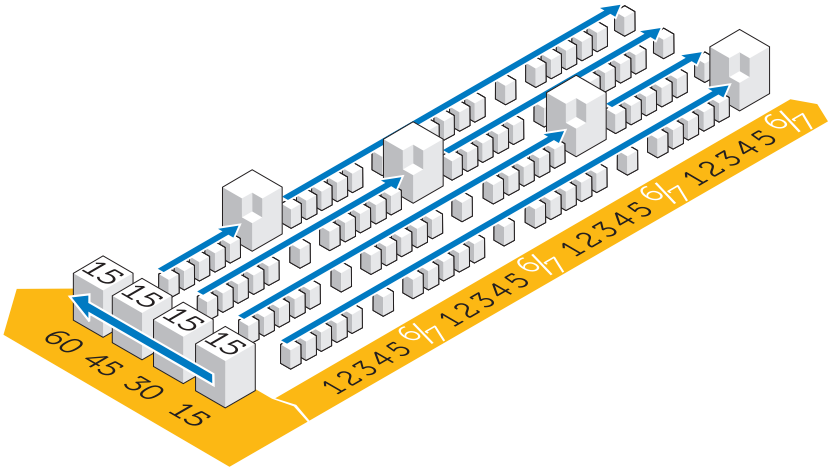
Ein forensisches Labor verfügt über drei Dateihaupttypen:

- Abbilddateien – Hierbei handelt es sich um forensisch einwandfreie Images des verdächtigen Geräts. Nach ihrer Erfassung werden sie keinesfalls geändert und müssen nur einmal gesichert werden (möglicher Erweiterungen: **E01**, **DD** usw.). Beweisdateien sind nicht häufig anzutreffen, sind dafür aber sehr umfangreich.
- Falldateien – Hierbei handelt es sich um Datendateien und Indizes der Analyseergebnisse; sie müssen ggf. aus der Forensik-Anwendung exportiert werden. Dateien offener Fälle sind häufigen Änderungen unterworfen und können mehrere Dateierweitungstypen enthalten, so dass tägliche Sicherungen erforderlich sind. Falldateien sind meist in großer Anzahl vorhanden, haben dafür aber in der Regel einen kleinen Umfang.
- Datenbank – Dieser Dateityp wird (derzeit) nur in FTK 3 verwendet, enthält jedoch sämtliche Verknüpfungen zwischen Fall- und Beweisdateien sowie alle Lesezeichen und Notizen der Ermittlung. Dateien des Typs Datenbank müssen täglich gesichert werden.

Abbildung 7-2 zeigt das empfohlene bewährte Verfahren zur Sicherung eines digitalen forensischen Labors. Da viele forensische Labore über 50 TB (und mehr) Speicher verfügen, ist eine vollständige Sicherung innerhalb eines standardmäßigen Sicherungszeitfensters am Wochenende ggf. nicht möglich. Um sicherzustellen, dass Daten bei Eintreten einer Notfallsituation mit minimalstem Wiederherstellungspunkt wiederhergestellt werden können, wird die Sicherung in gleichmäßige Abschnitte unterteilt und im Laufe eines Monats ausgeführt.

Aufgrund dieses Vorgangs ist es erforderlich, dass die Sicherungskopie einer vollständigen Sicherung maximal 15 TB groß ist. Jede LUN führt dann so lange inkrementelle Updates für den verbleibenden Sicherungszyklus durch, bis eine vollständige Sicherung erneut ansteht.

Abbildung 7-2. Sicherungsplan nach bewährtem Verfahren



Off-Host- und Netzwerksicherung

Aufgrund der Größe der Daten, die zur Notfall-Wiederherstellung in den meisten forensischen Laboren auf Band übertragen werden müssen, ist der LUN-Speicher in 15 TB große LUNs aufgeteilt. Dies ermöglicht nicht nur eine vereinfachte Verwaltung und Sicherung, sondern reduziert zudem die Failover-Zeit des Dateisystem-Clusters bei einem Ausfall.

Zwei Sicherungstypen können durchgeführt werden, entweder über das Netzwerk oder als Off-Host-Sicherung.

- Bei einer konfigurierten Netzwerksicherung werden alle Sicherungsdaten mit einem sich auf dem Server befindlichen Backup-Agenten über das Netzwerk auf den Sicherungsserver übertragen.
- Bei einer Off-Host-Sicherungslösung sichern manche Server mit größeren Dateien ihre Daten nicht über Netzwerk. Stattdessen erstellen die Speicher-Arrays einen Snapshot der LUN und mounten diese Kopie dann direkt auf den Sicherungsserver. Dieser Vorgang erhöht die Backup-Gesamtgeschwindigkeit, da keine Sicherungsdateien über das normale Netzwerk übertragen werden, was zu zusätzlichen Netzwerkkonflikten führen könnte.

Heutzutage werden in vielen forensischen Laboren Sicherungen über 10-GB-Netzwerke abgewickelt.

Die folgende Abbildung stellt die Agenten dar, die pro Server für eine vereinfachte Sicherung erforderlich sind:

Abbildung 7-3. Backup-Agenten

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

OF	Open File Agent
AD	Active Directory
OA	Oracle Agent (allgemeiner, für Symantec Backup Exec erforderlicher Datenbankagent)
SA	SQL Agent (allgemeiner, für Backup Exec erforderlicher Datenbankagent)
NBU	Net Backup Server
BE	Backup Exec Server
EV	Symantec Enterprise Vault-Backup-Lizenz
MI	Monatliche vollständige Sicherung, tägliche inkrementelle Sicherung
SS	Einmal im Monat ermittelter Systemzustand (System State)

ANMERKUNG: Da sich die Datenmenge im Laufe der Zeit erhöht, ist möglicherweise eine Off-Host-Sicherung erforderlich.

Archivieren mit der digitalen Kriminaltechniklösung von Dell

On-Demand-Archivierung

Dank NTP Software ODDM, NTP Software Right-Click Data Movement (RCDM) und Enterprise ist ein Scan des gesamten Dateisystems nicht mehr zwingend erforderlich – im Falle der konventionellen Archivierung gelingt dies durch Implementierung der sogenannten *On-Demand-Archivierung*. Die Speicherkosten werden auf diese Weise reduziert und die Archivierungsqualität verbessert.

Abhängig von der Phase des Datenlebenszyklus, siehe „Archivierung und Abruf von Beweismaterial im Lebenszyklus eines Falles“ auf Seite 68, kann der Analytiker zwischen der Archivierung der Daten im langfristigen Speicher und dem Erhalt der Daten zum direkten Zugriff und zur direkten Verarbeitung wählen.

Darüber hinaus können für juristische Zwecke aufzubewahrende Daten mithilfe von NTP Software ODDM automatisch archiviert werden.

Voraussetzungen

NTP Software ODDM erfordert Microsoft IIS, Microsoft .NET Framework, SQL und Enterprise Vault. NTP Software ODDM und Enterprise Vault müssen auf demselben Server installiert sein. Größere Installationen können die SQL-Datenbank auf einem dedizierten Server unterhalten.

Installation

Ausführliche Installationsanweisungen für NTP Software ODDM und NTP Software RCDM finden Sie im*Handbuch zur Installation und Konfiguration der digitalen Kriminaltechniklösung von Dell*. Weitere Informationen finden Sie unter „Relevante Dokumentation und Ressourcen“ auf Seite 16.

Archivieren mit NTP Software ODDM

Benutzergesteuerte Archivierung

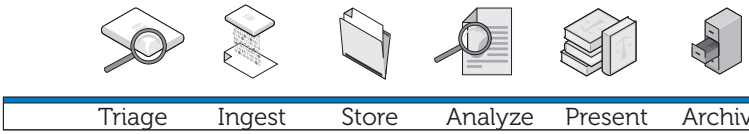
1. Wenn der Analytiker Datendateien speichert, weist NTP Software QFS den Benutzer darauf hin, dass die Dateien möglicherweise archiviert werden müssen.
2. Der Analytiker wählt mithilfe von NTP Software Storage Investigator die zu archivierenden Dateien aus und klickt dann auf **Archive**. Ist jedoch das NTP RCDM-Add-On installiert, klickt er mit der rechten Maustaste auf die Dateien.

   Nach Auswahl der Dateien informiert NTP Software Storage Investigator die Anwendung NTP Software ODDM, die wiederum Enterprise Vault aktiviert.

   Die Archivierungsanforderung wird der Archivierungswarteschlange hinzugefügt.

8

Fehlerbehebung



Allgemeine Tipps zur Fehlerbehebung

- Stellen Sie sicher, dass alle Clients und Server für einander sichtbar sind – ein Ping-Vorgang sollte problemlos möglich sein, ob mit dem NetBIOS-Namen oder mit der IP-Adresse.
- Stellen Sie sicher, dass Firewalls Datenverkehr zulassen.
- Starten Sie Server und Clients neu, um sicherzustellen, dass alle Installations- und Konfigurationsänderungen von den Systemen erkannt werden.

Spezifische Probleme der Forensik-Software

EnCase: EnCase startet im Erfassungsmodus

Diese Problem deutet darauf hin, dass EnCase über keine Lizenz verfügt.

1. Wählen Sie in EnCase den Menübefehl **Tools→ Options** und vergewissern Sie sich, dass die Felder **User Key Path**, **Server Key Path** und **Server Address** ausgefüllt sind (diese Felder sollten auf den Pfad mit den Lizenzschlüsseln verweisen).
2. Überprüfen Sie die Firewall auf dem Client und den EnCase-Lizenzserver, um sicherzustellen, dass der Port 4445 offen ist.
3. Stellen Sie sicher, dass der Client den EnCase-Lizenzserver anpingen kann.

FTK Lab: Vom Client gestarteter Browser kann Benutzeroberfläche nicht anzeigen

1. Stellen Sie sicher, dass auf dem Client MS Silverlight installiert ist.
2. Stellen Sie sicher, dass die Oracle-Dienste auf dem als Hostserver mit der Oracle-Datenbank gestartet wurden.

FTK 1.8: Meldung „5000 object limit\trial version"

Wenn Sie diese Meldung erhalten, verfügt FTK über keine Lizenz. Vergewissern Sie sich, dass der Netzwerklizenzserver einwandfrei funktioniert und über FTK 1.8-Lizenzen verfügt:

1. Öffnen Sie ein Browserfenster auf dem Hostserver des Netzwerklizenzservers und geben Sie **http://localhost:5555** in die Adressleiste ein.
2. Überprüfen Sie, ob Lizenzen vorhanden sind. Falls nicht, müssen Sie die Lizenzen installieren.

FTK 1.8: Fehler „Cannot Access Temp File" beim Start

Erlauben Sie dem Benutzer, die Anwendung (oder Citrix-Sitzung) zu starten, um Zugriff auf die Serverfestplatte zu erhalten, ODER führen Sie die Anwendung als Administrator aus.

Citrix-Probleme

Citrix: Anwendungen starten nicht

1. Stellen Sie sicher, dass alle Dienste (insbesondere MFCOM und IMA) auf den XenApp-Hostservern gestartet wurden.
2. Stellen Sie sicher, dass der Client die XenApp-Server sehen und anpingen kann.
3. Überprüfen Sie die Firewall auf den Clients und XenApp-Servern, um sicherzustellen, dass die XenApp-Ports offen sind.
4. Überprüfen Sie den Citrix-Lizenzserver, um sicherzustellen, dass der Netzwerklizenzierungsserver über eine auszugebende Lizenz verfügt. Der Citrix-Lizenzierungsserver ist normalerweise auf einem der Citrix XenApp-Server installiert. Der Zugriff erfolgt über **Start→ Programme→ Citrix→ Management Consoles→ Citrix Licensing**.

5 Öffnen Sie die **Citrix Management Console** (**Start→ Programme→ Citrix→ Management Consoles→ Citrix Delivery services console**). Führen Sie dann einen Erkennungsvorgang durch, um sicherzustellen, dass alle XenApp-Server in der Farm vorhanden sind.

6 Stellen Sie sicher, dass die Anwendung auf einem gültigen (in der Farm vorhandenen) XenApp-Server veröffentlicht wurde.

7 Rufen Sie die **Citrix Delivery Services Console** auf, um sicherzustellen, dass der die Anwendung startende Benutzer Mitglied einer Gruppe ist, die zum Starten der Anwendung berechtigt ist.

8 Stellen Sie im Falle gestreamter Anwendungen sicher, dass die Benutzerkontensteuerung auf dem Server deaktiviert ist.

Eingefrorene oder abgestürzte Citrix-Sitzungen

Wenn Benutzer sich nicht ordnungsgemäß von ihren Citrix-Sitzungen abmelden, wird die verwaiste Sitzung immer langsamer und kann letztendlich zu einem Einfrieren oder Abstürzen des Servers führen. Daher ist es äußerst wichtig, dass die Benutzer die bewährten Verfahren zum formellen und ordnungsgemäßen Abmelden jeder Sitzung befolgen (**Start→ Logoff→ OK**) und nicht einfach nur auf das Feld X oben rechts im Sitzungsfenster klicken.

Dennoch ist es möglich, dass dieses Problem auftritt. Es gibt zwei Wege, diesen Fehler zu beheben:

1 Melden Sie den Benutzer manuell ab.

   a Öffnen Sie eine Sitzung als Citrix-Administrator.

   b Überprüfen Sie die Liste offener Sitzungen und schließen Sie jede Sitzung manuell.

2 Starten Sie den Server neu.

Stichwortverzeichnis

S

T

V