Windows-8-Forensik: Ein erster Überblick

Neue Spurenlage

Alexander Sigel, Markus Loyen, Martin Wundram

Bei jedem neuen Betriebssystem stellt sich für Forensikexperten wieder die Frage, welche Datenspuren neu sind und welche sich geändert haben. Erste Untersuchungen zeigen die spezifischen Besonderheiten von Windows 8.

Jede neue Betriebssystemversion aus Redmond weist im Rahmen IT-forensischer Untersuchungen ihre Eigenheiten auf, die zu berücksichtigen sind und die die Experten vor neue Herausforderungen stellen. Erfahrungsgemäß dauert es nach der Veröffentlichung einer Windows-Version geraume Zeit, bis sämtliche Neuerungen in ihrer Bedeutung von der weltweiten Gemeinschaft der Forensiker zuverlässig untersucht, verstanden und die Erkenntnisse in Auswertungswerkzeuge eingeflossen sind – zumal diese hier in der Regel nicht wie bei Linux auf Spezifikationen oder Quellcode zurückgreifen kann. Vereinzelt kann dies mehrere Jahre dauern. Trotzdem gibt es bereits jetzt erste zu untersuchende Windows-8-Fälle. Was weiß man also schon? Welche Auswirkungen wird dies voraussichtlich auf die IT-forensische Analyse haben?

Als Orientierungsgrundlage dient zunächst im Schnelldurchlauf ein kurzer Rückblick darauf, welche wichtigen Artefakte IT-Forensiker typischerweise unter Windows 7 untersuchen. Grob unterscheidet man hier die Bereiche Hauptspeicher, Dateisystem/Verschlüsselung, Betriebssystem mit zugehörigen Anwendungen und weitere spezifische Anwendungen, die nicht mit dem Betriebssystem mitgeliefert, sondern installiert oder portabel genutzt werden. Die Spuren teilt man in direkte und indirekte Hinweise.

Beim Hauptspeicher steht nicht nur der eigentliche RAM-Dump im Fokus, wichtig sind auch hauptspeicherähnliche Artefakte wie Crash- oder Prozessdumps, *Hiberfil.sys* und die Windows-Auslagerungsdatei. Bei den Dateisystemen sind NTFS und exFAT aufgrund ihrer Metadaten im MFT (Master File Table) relevant. Link-Dateien (LNK) verweisen auf Dateien und enthalten oft wichtige Metadaten. Zehntausende Ereignisse notiert das Event Log und Datenmüll liegt im Papierkorb. Prefetch-/Superfetch-Dateien sowie zugehörige Datenbanken enthalten zur Optimierung von Ladevorgängen Angaben zu Aufrufen von Programmen und hierzu geladene Dateien.

Die Aufgabenverwaltung (Scheduled Tasks) weiß, was automatisiert ablaufen soll oder abgelaufen ist. Sprunglisten (Jumplists) geben Auskunft über Häufigkeit und Zeitpunkte von Datei- oder Programmnutzungen. Die Registry als zentrale Registrierungsdatenbank enthält zahlreiche bedeutsame Einstellungen und Angaben, darunter zuletzt benutzte Dateien (MRU), zum Beispiel auch nutzerbezogen unter dem *UserAssist*-Schlüssel. Ein indirekter Nachweis von Aktionen auf einem Windows-System gelingt ge-

legentlich etwa über Downloads oder protokollierte Aktivitäten von Virenscanner oder Firewall.

Schattenkopien (VSCs) erlauben die Wiederherstellung früherer Systemzustände – häufig selbst dann, wenn Verdächtige Daten zum Teil schon gelöscht haben. Die Zahl der Anwendungs-Artefakte ist unüberschaubar. Bei den Datenbanken ragen Extensible-Storage-Engine-Datenbanken (ESE-DB) und SQLite heraus. Da auch Nicht-Windows-Geräte Daten auf Windows-Systemen sichern oder sich mit ihnen synchronisieren, befinden sich dort immer öfter Sicherungen von iPhones und Android-Mobilgeräten, die ihrerseits beispielsweise SQLite-Datenbanken ablegen.

Windows 8: Ein „aufgebohrtes" Windows 7?

Win 8 führt eine Vielzahl von Neuerungen und Änderungen ein, die IT-forensische Auswertungen aufwendiger machen. Wichtiger denn je ist es folglich, klare Erkenntnisziele zu setzen. Zum Glück können IT-Forensiker auf ihrem bisherigen Erfahrungswissen aufbauen, denn Windows 8 ist keine vollständige Neuentwicklung, sondern eine Weiterentwicklung von Windows 7. Wenn man so will, ist es ein „aufgebohrtes" Windows 7: Die Versionsnummerierung wurde lediglich in der Minor Number hochgezählt (von 6.1.7601 für Windows 7 auf 6.2.9200 für Windows 8). Der Sprung ist also viel geringer als von XP zu Vista.

Dementsprechend sind praktisch alle von Windows 7 gewohnten Artefakte noch da, allerdings zum Teil mit neuen Features. Auch viele Binärformate sind unverändert, etwa Eventlogs, Link-Dateien, OLE-Container (Object Linking and Embedding) oder die schon genannten ESE-Datenbanken. Viele Neuerungen betreffen wichtige Pfade und Einstellungen sowie etliche Artefakte, insbesondere die Registry. Grund dafür sind die zahlreichen Änderungen an der Oberfläche und die Verbesserung der Systemleistung, die für den Endanwender am augenscheinlichsten sind. Dies zieht natürlich Änderungen am Backend nach sich, auch wenn dieses sich weniger ändert als die Oberfläche. Solche Neuerungen führen zu einer geänderten Spurenlage.

Bei Beweisbeschlüssen und dem Sicherstellen haben Forensiker es bei Windows-Geräten nicht mehr nur mit klassischen x86-Prozessoren und Desktops, Laptops oder Servern zu tun, sondern zunehmend mit ARM-Prozessoren in mobilen Endgeräten (Tablets, Mobiltelefonen oder einfach Geräte mit Touchscreen). Somit müssen die Experten mit einem noch größeren Gerätezoo zurechtkommen.

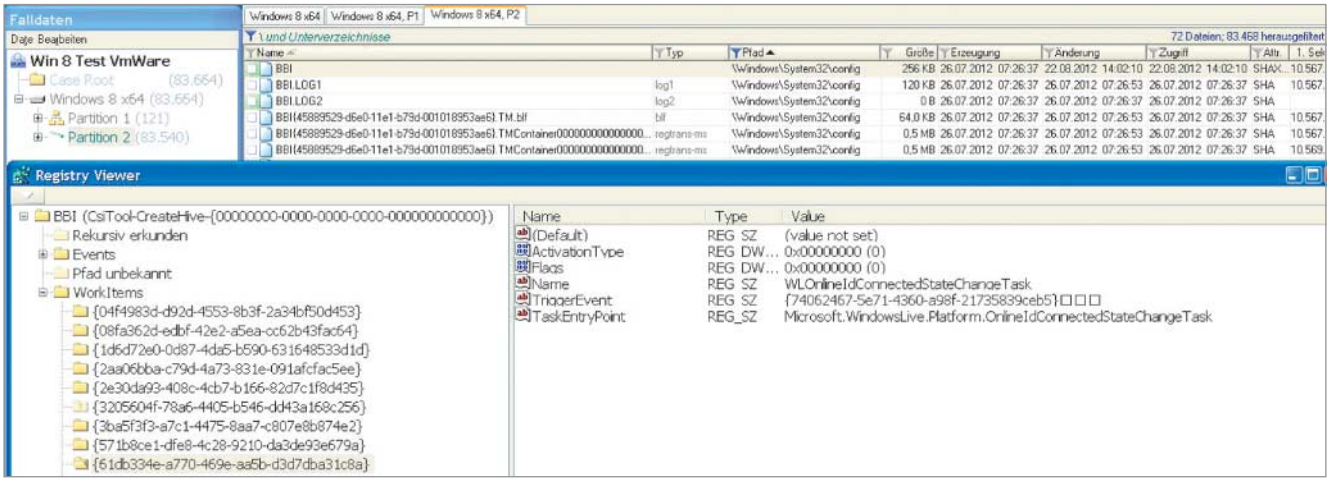
Windows-8-Telefone sind erstaunlich leistungsfähig. Windows Phone 8, das mobile Pendant zu stationären Windows-8-Rechnern, basiert erstmals nicht mehr auf CE, sondern auf Win 8 RT. Da dieses nun einen Großteil der Codebasis von Windows 8 enthält (wesentliche Änderungen wurden für neue Hardwarekomponenten wie den ARM-Prozessor und die Touch-Optimierung vorgenommen), können Forensikexperten die in Win-8-Telefonen enthaltenen Artefakte (Metro-Apps, Dateiexplorer, mobiles Office, IE10 et cetera) weitgehend wie auf Win-8-Systemen auswerten. Zudem stehen ab sofort USB-Sticks stärker im Fokus, da sie wegen der neuen Funktion „Windows To Go" vollwertige Windows-8-Systeme beherbergen können.

„TGFKAM" und die nervenden Kacheln

Am auffallendsten bei Windows 8 ist die neue Benutzeroberfläche Metro in Form von Kacheln mit den zugehörigen Apps. Metro, von den Autoren scherzhaft als TGFKAM – „The GUI Formerly Known

iX-TRACT

- Jedes neue Betriebssystem erfordert gründliche Untersuchungen, welche neuen und geänderten Funktionen an welchen Orten Spuren hinterlassen.
- Handelt es sich technisch gesehen um ein Minor Release, wie im Fall von Windows 8, haben Forensiker das Glück, dass zahlreiche Datenspuren, Fundorte und Methoden dieselben geblieben sind.
- Problematisch ist, dass sowohl die Erforschung des neuen Betriebssystems sowie die Anpassung der Werkzeuge auch dann oft noch nicht abgeschlossen sind, wenn es schon die ersten Anwendungsfälle gibt.



Neues Hive für das Browser-Based Interface (BBI): Auswertung mit dem Werkzeug X-Ways Forensics (Abb. 1)

As Metro" – bezeichnet (siehe Kasten im Artikel „Acht geben" Seite 42), wird aufgrund der aktuellen Namensdebatte zukünftig nur noch im Backend so heißen. Doch die Oberfläche bietet ein weiteres Universum mit einer Vielzahl von Einstellungsmöglichkeiten, Artefakten und Nutzungsspuren. Dieses gilt es ab jetzt parallel zum traditionellen Desktop zu untersuchen.

Klassische Anwendungen erscheinen im TaskManager unter ihrem Namen, und ihre Ausführung hält das Betriebssystem (unter anderem) in der Jumplist fest. Sie legen ihre Anwendungsdaten unter *AppData* ab, zum Beispiel unter Roaming. Anders verhalten sich „Apps". Ihre Nutzeroberfläche kann mit XAML oder HTML+CSS erstellt werden, was bedeutet, dass jede App Metainformationen über ihren Autor und Ablageort kennt. Auch verwaltet jede App ihre eigenen Internet-Artefakte, etwa Zugriffe auf Webseiten.

Neue Anwendungen, neue Spuren

Metro-Apps treten im TaskManager lediglich als *WWAHost.exe* auf (der Eltern-Prozess ist *SVCHost*) und legen ihre Daten auch unter den Anwendungsdaten (*\Program Files\Applications*) ab. Apps werden automatisch angehalten, wenn sie nicht im Vordergrund sind. Klassische installierte Programme findet man im Verzeichnis *C:\Programme* und in der Installationsliste der Registry. Die Funktion „Measured Boot" erzeugt zur Absicherung des Bootvorgangs Maßzahlen einer gesicherten Umgebung. Diese „Fingerabdrücke" können Forensiker verwenden, um Anwendungen zu identifizieren.

Im TaskManager gibt es unter anderem einen neuen Reiter für den Benutzungsverlauf der Apps. Auch Gruppenrichtlinien und sogenannte Kontrakte (die die Zusammenarbeit von Funktionen oder Applikationen gewährleisten sollen) für Apps in der Registry können zum Nachweis der Installation oder Verwendung von Software dienen. Die Kontrakte finden sich unter *HKCU\registered-applications*, eine Liste der Kontrakte unter *SOFTWARE\Classes\Extensions\ContractId*. Da man Apps über den in Windows integrierten AppStore beziehen kann, gibt es neue Registry-Einträge für alle Anwendungen, die daher stammen. Der Store enthält übrigens auch Angaben zu klassischen Win32-Anwendungen, allerdings können sie nur angezeigt und nicht über den Store bezogen werden. Auch beim AppLocker finden sich Spuren von Anwendungen, denn dieser regelt, welche ein Benutzer starten darf.

Wichtige Artefakte unter *AppData* sind beispielsweise Daten von Metro-Apps sowie deren Einstellungen, Web-Cache, Cookies und Verlaufshistorie, mit IE 10 besuchte Webseiten sowie die nutzerdefinierten Favoriten, mit Windows Journal Notes erstellte Notizen und Desktop-Verknüpfungen.

Bei knappem RAM lagert das Betriebssystem die am wenigsten benutzten Apps auf die Festplatte aus. Über dieses Auslagern kann man Nachweise und Datenspuren erhalten. Besonders interessant sind die Apps für Kommunikation (E-Mail, Chat-Client, Facebook, Twitter et cetera) sowie die Interaktion mit sozialen Netzwerken über das als Win-8-App vorhandene Socialite. Denn diese enthalten Hinweise auf Beziehungen zu weiteren Personen sowie auf ausgetauschte Inhalte. Die Daten sind unter *AppData\Local\Packages\microsoft.windowscommunicationsapps** abgelegt.

Im neuen Betriebssystem gibt es zwei Varianten des Webbrowsers Internet Explorer. Für Forensiker bedeutet das: Beide müssen nun jeweils immer einzeln überprüft werden. Standardmäßig öffnet sich beim Anklicken eines Links vom Desktop der Vollclient. Der Benutzer kann jedoch einstellen, dass die Browser-Metro-App standardmäßig genutzt wird.

Der doppelte Browser

Der Vollclient des IE 10 ist mit vielen neuen Features ausgestattet. Die temporären Internet-Dateien finden sich weiterhin unter *\Users\<Username>\AppData\Local\Microsoft\Windows\Temporary Internet Files*. Im Unterschied zu Windows 7 legt Windows 8 TIF-Dateien nun im Unterordner *Low* ab. Werden unter Windows 7 Cookies noch unter den temporären Windows-Dateien und unter *AppData\Roaming\Microsoft\Windows\Cookies* gespeichert, so erscheinen sie unter Windows 8 nun unterhalb von *Low*.

Seit dem IE 9 sind Cookie-Dateien aus Sicherheitsgründen auch nicht mehr nach dem Namensschema Nutzer@TLD benannt, sondern zufällig. Man kann den Dateinamen daher nicht mehr ansehen, zu welchen Webseiten die Cookies gehören. Im IE 10 haben sich zudem die *Index.dat*-Dateien samt ihrer internen Struktur geändert. Die Verlaufshistorie ist nun nicht mehr unterhalb von *History* in der *Index.dat* enthalten, sondern steht jetzt in einer ESE-DB mit Namen *WebCacheV<nn>.dat* (nn ist eine zweistellige Zahl, beispielsweise 24).

Neben der Vollversion gibt es den sogenannten immersiven IE, die abgespeckte App-Version (nur HTML5, keine Add-

ons). Dessen Spuren finden sich unter *InternetExplorer\Recovery\Immersive*. Microsoft nennt Apps immersiv, weil eine App auf andere zugreifen kann und alles nahtlos integriert, das heißt einem Betriebssystem ähnlich wird.

Parallelwelten: Windows To Go und Virtualisierung

Aus Datenschutzgründen ist es durchaus zu begrüßen, dass das portable Windows To Go (offiziell nur in der Enterprise-Version verfügbar), das man zum Beispiel von einem USB-Stick starten kann, keine Spuren mehr auf dem Wirt hinterlässt – vorausgesetzt, die Standardeinstellung, die Platten des Wirtssystems offline zu setzen, ist nicht verändert. Für den Forensiker bedeutet das allerdings, dass auch für ihn keine verwertbaren Spuren verbleiben, sollte das portable Betriebssystem für kriminelle Machenschaften benutzt worden sein.

Da sich die Virtualisierung stark weiterentwickelt hat, wurde auch die Auswertung virtueller Festplatten und virtualisierter Maschinen wichtiger. Für die x64-Editionen Professional und Enterprise ist ab sofort die Virtualisierungstechnik Hyper-V des Windows Server 2012 verfügbar. Umgekehrt ist damit der für Windows 7 optional frei verfügbare XP-Mode, der auf VirtualPC basierte, in Windows 8 nicht mehr möglich, weil das nun Hyper-V übernimmt.

Für virtuelle Festplatten gibt es zusätzlich zum bisherigen VHD das leistungsfähigere Format VHDx. Es unterstützt bis zu 16 TByte große virtuelle Festplatten, bei der dynamischen Variante wird zudem nicht der gesamte Speicherplatz alloziert. Nach einer Datenlöschung in einer VHDx kann man diese durch Schrumpfen (shrinking) verkleinern und so gegebenenfalls Beweismittel vernichten. Das geht zum Beispiel mit PowerShell in Hyper-V. Die Werkzeuge *disk2vhd* und *vhdtool* unterstützen bislang nur VHD, die Konvertierung zwischen den Formaten gelingt jedoch neuerdings mit Windows-8-Bordmitteln (Hyper-V/PowerShell), selbst wenn dieser Prozess eine ganze Weile dauern kann.

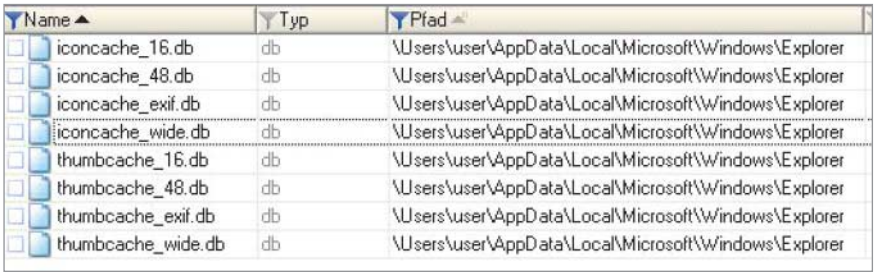
Aufgrund der effizienteren Hauptspeicherverwaltung kann man annehmen, dass es weniger wiederherstellbare Spuren im RAM und ähnliche Artefakte gibt. Den traditionellen Desktop lädt das Betriebssystem nur, wenn der Benutzer ihn benötigt und explizit anfordert. Das reduziert den Speicherbedarf des Kernels und damit die Spurenlage. Windows-Schnellboot („clean slate“) etwa schließt Nutzersitzungen vor dem Herunterfahren. Damit sollte die *hiberfil.sys* auch nur noch circa 10 – 15 % ihrer bisherigen Größe haben. Es gibt nun zwei Swapfiles (*pagefile.sys*, *swapfile.sys*). Da Windows 8 Hauptspeicherseiten dedupliziert, wird es die Aufgabe der Analysewerkzeuge sein, die damit eingeführten Referenzierungen oder Zeiger auf das gleiche Hauptspeicherobjekt zu erkennen und aufzulösen – was es noch schwieriger macht, Inhalte logisch wieder zusammenzusetzen.

Das renovierte Dateisystem NTFS 3.1 kann nun im laufenden Betrieb auch die Systempartition scannen und reparieren. Es gibt keine festen Durchläufe mit langer Laufzeit mehr, außerdem muss das Dateisystem dazu nicht mehr ausgehängt werden. Die Entwickler haben die Verwaltung von Plattenplatz (Trim, Unmap) verbessert, insbesondere für SSDs. Es kann also sein, dass Plattenplatz früher freigegeben und überschrieben wird, was die Wiederherstellbarkeit von Dateien erschweren dürfte.

Die neuen File-Systeme

Für Partitionen von Windows-Servern (noch nicht für Windows 8 verfügbar) führte Microsoft das neue, robustere Dateisystem ReFS (Resilient File System, teilweise ähnlich NTFS) ein. Für die Server-Variante soll es in voller Implementierung, auch für die Bootpartition, nachgereicht werden. Seit Version 16.5 unterstützt die Forensiksoftware X-Ways Forensics bereits die Erkennung von ReFS, noch nicht aber dessen Interpretation und Auswertung. Die Systemaufgabe „Schrubben“ (scrubbing), eingeführt zum Schutz gegen latente Plattenfehler, vergleicht proaktiv Prüfsummen und kann Daten verändern. Schlechte Kopien kann man auf diese Art mit Informationen aus guten reparieren.

Die steigende Nutzung mobiler Geräte und Datenablage in der Cloud sowie ein erhöhtes Sicherheitsbewusstsein bei den Anwendern lässt den Bedarf an zuverlässiger Verschlüsselung steigen. Da BitLocker Bestandteil verschiedener Windows-Editionen, darunter der Professional-Version, ist, wird die Verbreitung dieser Verschlüsselung vermutlich steigen. Bei BitLocker gibt es einige kleinere Änderungen. Zum Beispiel heißt der Klartextschlüssel zur Wiederherstellung jetzt *Bitlocker-Wiederherstellungsschlüssel-<Identifier>.txt*, wobei der Identifier (Key Protector ID, also das numerische Kennwort, das die Zuordnung zu einem



Name	Typ	Pfad
iconcache_16.db	db	\Users\user\AppData\Local\Microsoft\Windows\Explorer
iconcache_48.db	db	\Users\user\AppData\Local\Microsoft\Windows\Explorer
iconcache_exif.db	db	\Users\user\AppData\Local\Microsoft\Windows\Explorer
iconcache_wide.db	db	\Users\user\AppData\Local\Microsoft\Windows\Explorer
thumbcache_16.db	db	\Users\user\AppData\Local\Microsoft\Windows\Explorer
thumbcache_48.db	db	\Users\user\AppData\Local\Microsoft\Windows\Explorer
thumbcache_exif.db	db	\Users\user\AppData\Local\Microsoft\Windows\Explorer
thumbcache_wide.db	db	\Users\user\AppData\Local\Microsoft\Windows\Explorer

Weitere Auflösungen für Thumbcache- und Iconcache-Bilddateien unter Windows 8 (Abb. 2)

Volume ermöglicht) das Format nx8-nx4-nx4-nx4-nx12 hat (fünf durch Bindestrich getrennte alphanumerische Bereiche, 8, 3 × 4 und 1 × 12 Stellen lang). Damit enthält der Dateiname nur den Identifier, in der Datei selbst steht nochmals der Identifier sowie die eigentlich interessierende Ziffernfolge des Wiederherstellungsschlüssels.

Auch lässt sich der Wiederherstellungsschlüssel (Recovery Key) jetzt nicht mehr nur auf einem USB-Gerät speichern (bei der Sicherstellung digitale USB-Diktiergeräte nicht vergessen!), sondern auch im Windows SkyDrive. Damit ist demnächst sogar verstärkt zu rechnen, denn dieser Ablageort gehört zur Standardeinstellung für Stand-alone-Rechner, die sich nicht in einer Domäne befinden („Save to SkyDrive – Recommended“).

Die versteckte Startpartition ist nun 350 statt 100 MByte groß. Solche Dateien, die das Betriebssystem dort ablegt, kann man bei Untersuchungen per Hash als bekannte unverdächtige Dateien identifizieren und ausschließen. Neben dem Win-8-Bootloader und der Routine für die Entschlüsselung für die BitLocker-verschlüsselten Festplatten legt Windows 8 nun zusätzlich noch ein 180 MByte großes Verzeichnis namens *recovery* an, das für die Nutzung der neuen Recovery-Funktionen erforderlich ist.

Der Verschlüsselung auf der Spur

Die Signatur für die Dateisystem-Vollverschlüsselung ist die gleiche wie bei Win 7 (EB 58) und im Header des verschlüsselten Datenträgers ist weiterhin die Bezeichnung „FVE-FS“ (2D 46 56 45 2D 46 53 2D) enthalten. Es kann sich lohnen, die Gruppenrichtlinien für BitLocker aus der Registry auszulesen, weil man dann weiß, wann Festplatten zwangsverschlüsselt werden. Das Eventlog zeichnet BitLocker-Ereignisse in verschiedenen Kanälen auf, zum Beispiel Zeitstempel, Ver- und Entschlüsselung, Einbinden und Aushängen, Benutzung von Verschlüsselung durch Laufwerke, Erzeugen von Schlüsseln.

Da die Authentifizierung erstmals zusätzlich über Microsoft-Konten (ehemals Windows Live ID) und bildhafte Kennwörter mit Gesten möglich ist, sind auch solche Kennwortarten bei der Registry-Auswertung zu beachten. Bei erstmaliger Verwendung einer Live ID geht zudem eine Bestätigungsmail von Microsoft beim E-Mail-Postfach des Live-ID-Nutzers ein.

Alles gut registriert

Die Registry hat trotz Apps keineswegs ausgedient, vielmehr wird sie weiterhin intensiv genutzt – gerade auch von Apps, die somit nicht vollständig isoliert sind. Bei der Registry bleibt die Grundstruktur der aus Windows 7 bekannten Hives (Schlüsselsammlungen) und deren Binärformat gleich, es kommen jedoch Hives und insbesondere Schlüssel für neue Features hinzu. Neue Hives sind ELAM (Early Launch Anti-Malware), BBI (Browser-Based Interface) und SETTINGS.DAT (für Nutzerprofile) (Abb. 1).

Ein paar Beispiele für Erweiterungen bisheriger Hives:
– SYSTEM kennt neue ortsbasierte Dienste (Location Based Services), Sensoren und zugehörige Geräte. Die Informationen könnten möglicherweise das Erstellen von Bewegungsprofilen ermöglichen. Statt herkömmlichem BIOS unterstützt der Bootloader nun automatisch UEFI (Unified Extensible Firmware Interface). Windows 8 beschränkt mit dem Secure-Boot-Mechanismus das Booten auf vorher signierte Bootloader. *UEFISecureBootEnabled* im *CurrentControlSet* unter *SecureBoot\State* enthält die Information, ob SecureBoot aktiviert ist. Das kann bei der Beurteilung helfen, ob das System von anderen Medien gebootet werden kann oder in der Vergangenheit wurde.
– SAM speichert in *Domains\Account\Users\Internet User Name* das Microsoft-Konto und in *Domains\Account\Users\UserTile* das zugehörige Nutzersymbolbild.
– SOFTWARE merkt sich, welche Metro-Apps auf dem System installiert sind (*Microsoft\Windows\CurrentVersion\AppX\AppxAllUserStore\Applications*). Auch ist festgehalten, welche Metro-Apps ein Nutzer installiert hat (derselbe Pfad plus *\%SID%*). Der nahtlos integrierte Webbrowser legt ebenfalls Einstellungen ab. Die Anbindung an die Cloud erfordert neue Angaben, beispielsweise zu Synchronisierungseinstellungen. Es gibt zusätzliche Funktionen bei Datei-Backup und der Systemwiederherstellung.
– In NTUSER verfügt *TypedURLs*, der Verlauf besuchter Webseiten, nun auch über einen Zeitstempel *FileTime* (*Software\Microsoft\Microsoft\Internet Explorer\TypedURLsTime*). Um ihn auszulesen, existiert ein angepasstes RegRipper-Plug-in.

Einzelne Artefakte aus verschiedenen Quellen

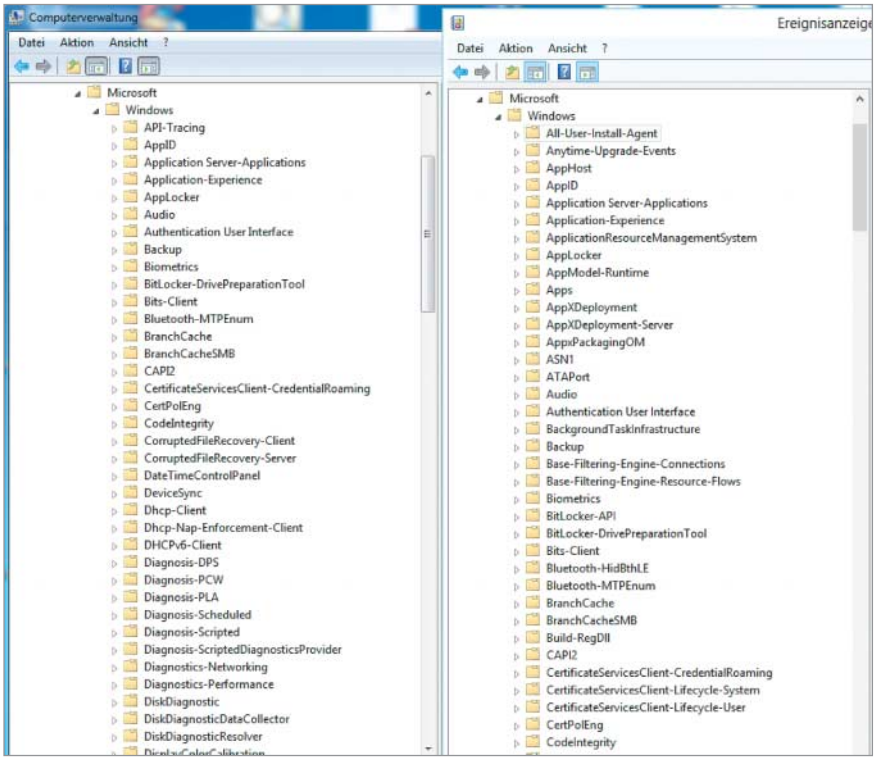
Trotz PowerShell 3.0 gibt es die DOS-Kommandozeile noch. Für beide Varianten lassen sich aus den zugehörigen Artefakten Informationen wiederherstellen.

Beim Dateiexplorer haben die Entwickler einige Kopiervorgänge verbessert. So erzeugt die Kopieranzeige beim Kopieren von Bilddateien Vorschaubilder, bei Textdateien erscheint die Vorschau nur bei Dateinamenskonflikten. Für andere Dateitypen gibt es – aus Sicht der Forensiker leider – nur Standard-Icons. Zur Unterstützung weiterer Auflösungen (Dateinamen: 16, 48, exif, wide) und Geräte erzeugt Windows 8 für Thumbcache (für Bilder) und Iconcache (für Icons) zusätzliche kleine Bildchen (Abb. 2). Die Forensiksoftware Thumbcache Viewer kann nun auch Win8-Artefakte anzeigen.

Wie unter Windows 7 heißt der Papierkorb weiterhin *Recycle.bin* und wie gehabt befinden sich darin eine *Desktop.ini* sowie Verzeichnisse, geordnet nach SID. Auch die paarweise mit gleichem zufälligen Namen auftretenden Dateien *$R* (Inhalt) und *$I* (Metainfo) gibt es unter Windows 8 weiterhin. Zudem sind die Speicherverwaltungsfeatures Prefetch/Superfetch gleich geblieben.

Der TaskManager zeigt im Reiter *App History* von Apps verwendete Ressourcen im Zeitverlauf an sowie unter anderem die „Kachel-Updates“. Diesen Verlauf kann man auch manuell löschen.

Eine besondere Herausforderung ist es für Forensiker, einen Sachverhalt durch



Windows 8 (rechts) hat nicht nur zahlreiche neue Features gegenüber Windows 7 (links), sondern auch mehr protokollierte Informationen über sie und die anderen Funktionen. Da freut sich der Forensiker (Abb. 3).

indirekte Spuren nachzuweisen. Zu diesen zählt neben einer Firewall auch ein Virenscanner. Unter günstigen Voraussetzungen sollte es möglich sein, über Quarantäne, Logfiles oder Hashwerte zu zeigen, dass eine bestimmte Datei oder Anwendung existiert hat, selbst wenn deren andere Hinterlassenschaften unwiederbringlich gelöscht sind.

Beweise durch die Hintertür

In Windows 8 sind gleich zwei dieser indirekten Spurengeber integriert: Der Virenscanner „Windows Defender", der nun mehr Funktionen als sein Vorgänger hat und Updates ohne zeitliche Beschränkungen erhält. Außerdem der Filter „SmartScreen". Er kümmert sich um die Malware-Erkennung, indem er mit großer Sammelleidenschaft Hashwerte nach Hause funkt. Immerhin ist das im Vorfeld in die Kritik geratene Feature abstellbar. Nach Protesten hat Microsoft die *https*-Version aktualisiert, damit sind die Infos mittlerweile nicht mehr so leicht Dritten zugänglich.

Wenig überraschend: Die neuen Features müssen auch im Eventlog ihren Niederschlag finden. Es sind viele Logfile-Kanäle und einige neue Ereignisse hinzugekommen, was die Spurenlage verbessert (Abb. 3). Die Metro-Apps werden umfangreich protokolliert (etwa *AppID*, *AppModel-Runtime* et cetera), aber auch das Logging von BitLocker, Mobile Broadband Experience, Smartcards oder TPM haben die Entwickler erweitert.

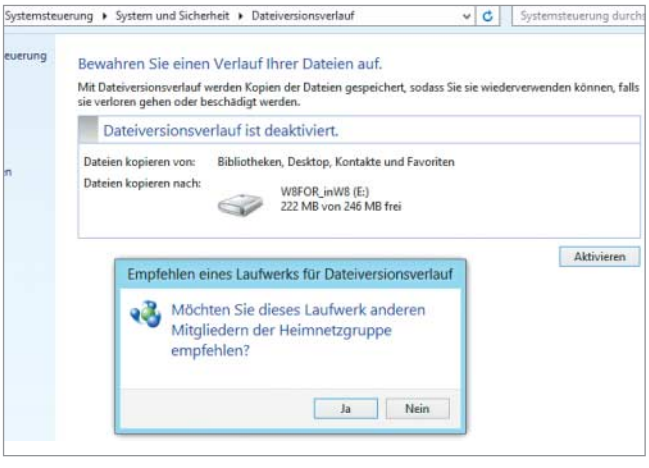
Viele Microsoft-Anwendungen verwenden als Datenbank statt dem leicht auszuwertenden SQLite die proprietäre ESE-DB (Extensible Storage Engine Database File). Deren Format ist nur teilweise bekannt und es gibt nur wenige Werkzeuge, zum Beispiel den EseDBViewer. Auch die eifrig indexierende Windows Search, ebenfalls in Windows 8 erweitert, nutzt eine solche EDB im Artefakt *Windows.edb*. Die wichtigste Änderung ist, dass *SystemIndex_0A*, unter Windows 7 die Haupttabelle, ersetzt wurde durch *SystemIndex_PropertyStore*. Zudem können neue Felder Forensikern weitere Hinweise geben. Joachim B. Metz, Autor der Bibliothek *libesedb*, hat sie in [1] beschrieben. Das Werkzeug Windows Search Index Analyzer (WSia) soll in seiner nächsten Version die Auswertung der Windows 8 Search unterstützen.

Mit Druckern Neuland betreten

Mit Windows 8 hat Microsoft eine neue Druckertreiberarchitektur eingeführt, das deutlich weniger ressourcenfressende „Print Class Driver Framework". Sofern möglich, ist das Zwischenformat nun die von Microsoft entwickelte XML Paper Specification (XPS). Drucken lässt sich auch aus den Metro-Apps heraus, die das ebenfalls auf XML beruhende Grafikformat Direct2D verwenden. XML lässt sich leichter auswerten als Binärformate, enthält aber auch möglicherweise weniger für Forensiker interessanten Datenmüll.

Durch Wegfall alter Treiber, geringeren Hauptspeicherverbrauch und geänderte Installation gibt es einerseits weniger Spuren, andererseits kommen einige neue Artefakte hinzu. Am auffälligsten zeigt sich dies bei einem Blick in den Gerätemanager: Dieser zeigt Drucker neuerdings als Druckerwarteschlangen an. Die Praxis muss zeigen, ob es schwieriger wird, Drucker zu identifizieren, und ob zusätzlich vorhandene Lokationsdaten unterwegs eingebundener Drucker Bewegungsprofile anreichern können.

Wenigstens die Forensik für USB-Sticks funktioniert unter dem neuen Betriebssystem glücklicherweise noch so wie für Windows 7 von Harlan Carvey beschrieben [2]. Die Logdatei *setupapi*.



Mit der neuen Backup-Funktion kann der Benutzer auch Daten für andere Mitglieder des Netzwerks freigeben. Die Formulierungen sind allerdings nicht selbsterklärend (Abb. 4).

dev.log im Windows-Verzeichnis der Systempartition verrät, wann ein Gerät das erste Mal angeschlossen war. Mittels Registry-Analyse, etwa RegRipper-Plugins, korreliert man dazu Angaben aus den drei Hives SYSTEM (*USBStore*, *DeviceClasses*, *MountedDevices*, *USB*), SOFTWARE (*Windows Portable Devices*, *EMDMgmt*) und NTUSER.dat (*MountPoints2*) untereinander und über die Volume Serial Number (VSN) mit LNK-Dateien und Sprunglisten.

Bei den Netzwerken ist besonders die Heimnetzwerk-Gruppe von Interesse. Sie dient der vereinfachten Freigabe von Dateien für vertrauenswürdige Mitmenschen, typischerweise zu Hause. Hierzu gibt es die Logdatei *C:\Windows\Logs\HomeGroup\homegrouplog.etl*. Erstaunlich, dass hier mit *.etl* ein altes Ereignislog-Format verwendet wird (das aktuelle ist *.evtx*). Weitere Einträge finden sich in den Eventlog-Quellen *HomeGroup**. Auch im Eventlog „Sicherheit" finden sich Einlog-Vorgänge zu *HomeGroup*, zum Beispiel EventID 4738. Log-Ereignisse finden sich allerdings (nur) bei dem Rechner, der die jeweilige Heimnetz-Gruppe erzeugt hat.

Nicht einfacher geworden: Sichern und Wiederherstellen

Bei der Datensicherung hat sich einiges geändert. Bei den für forensische Untersuchungen weiterhin sehr wichtigen Schattenkopien (Volume Shadow Copies, VSC) haben die Entwickler im Unterschied zu Windows 7 die GUI von der Nutzeroberfläche entfernt. Damit kann ein Nutzer diese Kopien nicht mehr direkt anfordern und auch „frühere Versionen" nicht mehr direkt über ein Kontextmenü aufrufen. Wer allerdings weiß, wie er es anstellen muss, kann weiterhin die API nutzen, um eine Schattenkopie zu erzwingen.

Standardmäßig sichern Schattenkopien auch weiterhin Nutzerdaten ohne Nutzerinteraktion, das heißt Daten unterhalb von *Users*. Das neue Backup-Feature „File History" (Dateiversionsverlauf) ersetzt das alte „Backup & Restore". Die Funktion schützt und sichert die Bibliotheken und Dateien des Benutzers (user space) auf dem Desktop. Man kann auf andere Medien sichern, als Ziel ist sogar eine virtuelle Festplatte (VHD) möglich.

Zu File History finden sich die Spuren in der Registry, im Event Log und in Dateien. Da der Nutzer die so gesicherten Daten auch für die Mitglieder der HomeGroup freigegeben kann (Ablageort den Mitgliedern „empfehlen", Abb. 4), können sich weitere Spuren auf anderen Rechnern befinden (zum Beispiel Registry-Schlüssel am gemeinsamen empfohlenen Ablageort). In Fällen von Datendiebstahl können Forensiker so möglicherweise weitere Rechner und mobile Datenträger finden. Mit „Refresh & Recovery" gelingt neben der Wiederherstellung von Daten auch das Löschen von Spuren. Man kann erkennen, wann diese Funktionen das letzte Mal ausgeführt wurden. Bei mit „Refresh" zurückgesetzten Systemen sind für IT-Forensiker die Artefakte *$SysReset*, *Windows.old* und *Lost Files* wertvoll, weil sie die meisten relevanten Spuren enthalten.

Mit dem neuen Windows 8 ist die Auswertung der Aktivitäten auf dem Rechner beziehungsweise der hinterlassenen Spuren wieder einmal komplexer geworden. Mit dem richtigen Know-how lässt sich aber oft noch vieles über Täter und Taten herausfinden. Gegenwärtig unterstützen die meisten IT-forensischen Werkzeuge Windows 8 noch nicht ausreichend. Ein späterer Artikel wird sich im Detail mit einzelnen Windows-8-Artefakten und der Windows-8-Unterstützung ausgewählter Auswertungswerkzeuge befassen. (ur)

Alexander Sigel

ist Geschäftsführer der DigiTrace GmbH in Köln und hält Schulungen zur IT-forensischen Auswertung von Windows 8.

Markus Loyen

ist Geschäftsführer der CORIFOR GmbH & Co. KG, Nidderau, und berät rund um IT-Forensik.

Martin Wundram

ist Geschäftsführer der TronicGuard GmbH und ö.b.u.v. Sachverständiger für Systeme und Anwendungen der Informationsverarbeitung.

Literatur

[1] Joachim B. Metz; Windows Search: Analysis of the Window Search Database; August 2012; https://libesedb.googlecode.com/files/Windows%20Search.pdf

[2] Harlan Carvey; HowTo: USB Thumb Drives; Februar 2012; windowsir.blogspot.de/2012/02/howto-usb-thumb-drives.html

Alle Links: www.ix.de/ix1211050