Spurensuche in der Windows-Registry

Goldmine

Alexander Geschonneck, Alexander Sigel

In der Registry, dem Herzen eines Windows-Systems, finden sich nicht nur Systemeinstellungen, sondern auch Gebrauchsspuren und häufig die Zeitpunkte der Änderungen – mit geeigneten Werkzeugen und Methoden angezapft eine unschätzbare Quelle für computerforensische Analysen.

Die Windows-Registry dient als umfassende, vom Konfigurationsmanager im Kernel verwaltete Datenbank des Windows-Systems und aller Systemdienste und -prozesse. Sie speichert vielfältige Steuerungsinformationen zu Systemeigenschaften (Hard- und Software inklusive Anwendungen und Benutzeroberfläche) sowie über Nutzeraktivitäten. Diesen Informationsreichtum unterschätzen Windows-Anwender oft.

Man unterscheidet Systembereiche („Kernel-Land“) von Einträgen, die sich je einem Nutzer zuordnen lassen („User-Land“). Die Einträge sind als Werte unter Schlüsseln mit diversen Namen abgelegt. Da sie mit Zeitstempeln versehen sind, können Ermittler die Registry auch wie ein Logbuch als Abfolge von Ereignissen interpretieren und anderen Datenspuren des Systems gegenüberstellen – eine Goldmine zum Analysieren eines Windows-Systems, um einen eventuellen Missbrauch feststellen zu können.

Aus der Registry lassen sich Hinweise auf das Wissen eines Verdächtigen gewinnen, auf Informationsabflüsse, Manipulationen des Systems, installierte Software, Kennungen und Kennwörter der Anwender oder darauf, was ein Nutzer zuletzt getan hat (most recently used, MRU). Zudem kann ein Anwender dort Informationen verstecken.

Die genauen Auswertungsmöglichkeiten hängen von der Windows-Version und den Nutzereinstellungen zur Datensparsamkeit ab. Zu den typischen Ergebnissen zählen die folgenden:

– Vom Nutzer angelegte, genutzte oder gespeicherte Dateien und Dateiverknüpfungen,
– Laufwerksbuchstaben, unter denen Verzeichnisse (auch mobiler Medien) mit dem System verbunden waren,
– von der Kommandozeile aus gestartete Programme,
– Einstellungen der Netzwerkkarten und Netze, mit denen der Rechner zuletzt verbunden war: Bei Laptops gibt die Liste der jemals verbundenen WLANs Hinweise auf ein Bewegungsprofil.
– Suchanfragen der Anwender im lokalen System sowie bei Internet-Suchmaschinen,
– Website-Besuche und dortige Formulareingaben,
– Geräte, insbesondere mobile Medien (etwa USB-Sticks oder Digitalkameras), die mit dem Rechner verbunden waren, inklusive Zeitpunkten und Seriennummern. Leider haben etliche USB-Geräte keine Seriennummer, sodass Windows jeweils dynamisch eine Proforma-Nummer vergibt, mit der sich ein Gerät aber nicht identifizieren lässt. Die Liste der angeschlossenen Geräte kann als Plan zur Sicherstellung von Asservaten bei der Hausdurchsuchung dienen, soweit die Geräte eindeutige Seriennummern aufweisen.
– Schadsoftware oder Anti-Forensik-Software, die installiert ist oder war, und Informationen darüber, wann sie lief.

Oftmals lassen sich aus früheren Registry-Kopien und ihren Verfallsformen noch Datenspuren rekonstruieren, die der Nutzer anderswo bereits gelöscht hat.

Anforderungen an Forensik-Tools

Übliche Registry-Editoren (wie *regedit* und verbesserte Nachbauten) reichen für die foren-

Bei Laptops gibt die Liste der jemals genutzten WLANs Hinweise auf ein Bewegungsprofil (erstellt mit RegRipper, Abb. 1).

```
NIC: Intel(R) PRO/Wireless 3945ABG Network Connection
  Static#0000 SSID : Schloss Lehen [Fri Mar  5 21:05:04 2010]
  Static#0001 SSID : link@sheraton_Pelikan [Fri Mar  5 21:05:06 2010]
  Static#0002 SSID : mshome [Thu Jan  1 00:00:00 1970]
  Static#0003 SSID : Etage 300 [Fri Mar  5 21:05:08 2010]
  Static#0004 SSID : RWLAN-6A7C17 [Fri Mar  5 21:05:10 2010]
  Static#0005 SSID : NETGEAR [Mon Nov 10 08:37:14 2008]
  Static#0006 SSID : HotelAir [Fri Mar  5 21:05:12 2010]
  Static#0007 SSID : IBMVISITOR [Fri Mar  5 21:05:14 2010]
  Static#0008 SSID : Orange [Fri Mar  5 21:05:16 2010]
  Static#0009 SSID : Gaestehaus [Fri Mar  5 21:05:18 2010]
```

Ab Windows Vista lassen sich Netzwerk-Verbindungen detailliert auswerten (erstellt mit RegRipper, Abb. 2).

```
Interface {2BF31E67-CA93-4025-8CB6-334947AA22D5}
Name: Wireless Network Connection
Control\Network key LastWrite time Mon Aug  7 20:43:08 2006 (UTC)
Services\Tcpip key LastWrite time Thu Oct 19 17:17:38 2006 (UTC)
      DhcpDomain     = chvlva.adelphia.net
      DhcpIPAddress  = 192.168.1.8
      DhcpSubnetMask = 255.255.255.0
      DhcpNameServer = 192.168.0.1
      DhcpServer     = 192.168.1.1

Interface {1417AF83-197F-4A7B-B921-C02538ADA33A}
Name: Local Area Connection
Control\Network key LastWrite time Tue Jun 28 21:46:51 2005 (UTC)
Services\Tcpip key LastWrite time Mon Sep 19 20:55:17 2005 (UTC)
      IPAddress      = 192.168.1.28
      SubnetMask     = 255.255.255.0
      DefaultGateway = 192.168.1.1
```

sische Analyse nicht aus. Ermittler benötigen insbesondere Funktionen in folgenden Bereichen:

– Auswertung aller Informationen verschiedener Windows-Systeme, nicht nur des laufenden,
– Auswertung sowohl der volatilen als auch der statischen Inhalte,
– Vergleich der Zustände zu unterschiedlichen Zeitpunkten, inklusive Sicherungskopien,
– Analyse und grafische Darstellung von Ereignisabfolgen anhand der Zeitstempel,
– Wiederherstellung gelöschter Registry-Dateien und -Einträge,
– Finden von Einträgen im „Schlupfspeicher“ (slack space) und robuste Anzeige auch unvollständig erhaltener Informationen,
– Definition von Signaturen und Extraktions-Schablonen für forensisch relevante Einträge,
– Korrelation von Informationen aus verschiedenen Einträgen, etwa in Tabellenform,
– übersichtliche Dokumentation in nachvollziehbaren, flexibel anpassbaren forensischen Berichten,
– Unterstützung bei der Interpretation binärer und codierter Werte,
– ausgefeilte Suchfunktionen über Einträge in verschiedenen Bereichen, Codierungen und Formaten,
– Zugriff auf geschützte Bereiche und Entschlüsselung verschlüsselter Bereiche, soweit möglich und rechtlich zulässig.

Das Folgende bezieht sich auf die entsprechenden Funktionen der frei verfügbaren Werkzeuge RegRipper und Volatility sowie in den kommerziellen, integrierten Forensik-Werkzeugen ProDiscover Forensics, X-Ways Forensics, EnCase Forensic und Forensic Toolkit (FTK).

Grundsätzlich ähneln die Arbeitsweisen all dieser Werkzeuge einander, wobei sie unterschiedliche Schwerpunkte setzen. Trotz einiger Veränderungen haben sich die Struktur sowie die wesentlichen Inhalte der Registry in Vista und Windows 7 nicht geändert. Neu sind insbesondere transaktionsbasierte Registry-Änderungen (TxR) sowie virtuelle Registries (Umleitung von Schreibzugriffen).

Verschiedene Windows-Versionen halten die Registry-Daten auf unterschiedliche Weise im Hauptspeicher. Noch nicht alle Werkzeuge erfassen Registry-Einträge unter Vista und Win7 vollständig. Für eine umfassende Auswertung und den Vergleich der damit erzielten Ergebnisse benötigt man daher mehrere. Es kommt nicht darauf an, ob eines von einem bekannten Hersteller einer Forensic Suite stammt, sondern ob es das tut, was man genau benötigt, und ob man versteht, was es tut. Eine forensische Analyse setzt voraus, dass man wichtige Konzepte versteht, weiß, welche Möglichkeiten und Grenzen es gibt und wie man Erweiterungen und fallspezifische Anpassungen vornehmen kann. Nur die

iX-TRACT

- Windows nutzt eine Registrierungsdatenbank (Registry) als zentralen Speicher für vielerlei Systeminformationen.
- IT-Forensiker finden Anwendungs- und Benutzerinformationen nicht nur in den Registry-Dateien selbst, sondern in deren temporären Kopien anderswo auf der Platte oder im RAM.
- Zum Filtern, Vorsortieren und übersichtlichen Darstellen der Informationsfülle stehen Ermittlern diverse freie und kommerzielle Werkzeuge zur Verfügung.

Analysefunktion eines Werkzeugs aufrufen zu können, reicht nicht aus.

Grundlagen und Vorgehensweise

Die Registry ist in mehrere logische Bereiche (Hives) aufgeteilt. Informationen liegen teils statisch in physischen Dateien vor, teils nur im Hauptspeicher (etwa im Hardware-Hive), sind also flüchtig (volatil). Die genaue Aufteilung und der Ablageort unterscheiden sich je nach Betriebssystem-Version und Einstellung. Systeminformationen finden sich in der Windows-NT-Familie ohne Dateierweiterung unter *%WINDIR%\System32\Config*. Windows erstellt automatisch Sicherungskopien der Dateien, ein Nutzer kann sie zudem manuell anlegen. Sie können Informationen über ältere Stände oder inzwischen wieder gelöschte Schlüssel enthalten. Möglicherweise gibt es auch insgesamt gelöschte ältere Hives.

Die physischen Speicherorte der Sicherungskopien sind wiederum von der Windows-Version abhängig (z. B. Wiederherstellungspunkte oder Volume-Schattenkopien, Volume Snapshot Service – VSS). Man muss wissen, welche Hives wo gesichert sind und wie man unterschiedliche Versionen miteinander vergleicht, etwa mit *regmultidiff.pl* aus dem Perl-Modul Parse::Win32Registry. Für XP-Wiederherstellungspunkte leistet dies etwa *RipXP* aus der RegRipper-Sammlung.

Sollen Informationen über die Registry am „lebenden System“ (Live- oder Online-

Forensik-Werkzeuge für die Registry-Analyse im Überblick

Parse::Win32Registry: Entwickler können über die Win32-API auf die Registry zugreifen, unter Perl etwa mit Win32::TieRegistry. Das Verwenden der Windows-API hat jedoch aus forensischer Sicht einige Nachteile; in manchen Fällen sind direkte Systemzugriffe zu bevorzugen. Die Windows-API rückt nicht immer alle Informationen ungefiltert heraus. Dann sind Ermittler mit einem Werkzeug, das auf einer tieferen Ebene ansetzt, besser bedient. Das objektorientierte Perl-Modul Parse::Win32Registry von James MacFarlane kommt ohne Rückgriff auf die API aus und enthält außerdem einige nützliche Kommandozeilen-Werkzeuge sowie einen auf Gtk2-perl-basierenden Registry-Viewer.

RegRipper: Harlan Carvey, Spezialist für Computerforensik und Incident Response, hat durch seine Bücher [1] und insbesondere mit seinem frei verfügbaren Werkzeug RegRipper die Forensik der Windows Registry erheblich vorangebracht. Er gilt daher als „König der Registry-Analyse“. Anfang 2011 wird sein Buch „Windows Registry Forensics“ erscheinen.

Im Unterschied zu üblichen Registry-Viewern handelt es sich bei dem in Perl geschriebenen RegRipper um ein Werkzeug zum Extrahieren, Korrelieren und Anzeigen spezifischer forensisch relevanter Informationen in Form übersichtlicher Berichte. RegRipper basiert auf Parse::Win32Registry und lässt sich flexibel über spezifische Plug-ins erweitern (derzeit sind 72 enthalten). Dritte haben weitere Plug-ins sowie einen Plug-in-Generator veröffentlicht. Regscan zeigt Basisinformationen über jeden Dienst. So kann Malware dadurch auffallen, dass in den Registry-Einträgen *svchost* erscheint:

```
regscan | find "svchost.exe -k netsvcs"
```

Regslack findet Registry-Einträge im Schlupfspeicher. RegRipper 2.02 hat eine einfache, aber ausreichende grafische Oberfläche; Rip und RipXP sind kommandozeilenorientiert. RipXP berücksichtigt Registry-Informationen aus XP-Wiederherstellungspunkten. Um etwa alle Einträge für UserAssist Active Desktop zu bekommen, ruft man das Plug-in *userassist* mit einer passenden Hive-Datei unter Angabe des Restore-Verzeichnisses auf:

```
ripxp -r <hive_datei, hier ntuser.dat> -d <restore_Verzeichnis> ↵
                                    -p <Plugin_Modul, z.B. userassist>
```

Das Werkzeug ist flexibel und mit Perl-Kenntnissen leicht zu erweitern. Zusammen mit den Perl-basierten ProScripts in ProDiscover Forensics hat RegRipper ein großes Potenzial für tiefgehende Untersuchungen und eine weitgehende Automatisierung in umfangreichen Fällen.

Das **Volatility Framework** (in Python) ist unverzichtbar zum Analysieren von Hauptspeicherinhalten. Spezifische Registry-Analysen sind mit Plug-ins möglich, etwa mit den frei verfügbaren VolReg und VolRip von Brendan Dolan-Gavitt. VolReg implementiert Besonderheiten der Hauptspeicher-Analyse von Registries (nur Windows XP), VolRip (nur unter Linux) ist eine Hülle, mit der sich RegRipper direkt unter Python nutzen lässt. Mit HiveScan findet man den Rohversatz der Hives im Hauptspeicher, mit HiveList zeigt man für den ersten Hive die Adressen und Pfade/Namen der Hives an. Nun kann man mit PrintKey Details zu Schlüsseln ausgeben, oder mit einer der vier Dump-Funktionen Informationen ausgeben: HashDump für lokale Kennwort-Hashes, CacheDump für zwischengespeicherte Anmeldeinformationen von Windows-Domänen, LSADump für den über die Local Security Authority (LSA) geschützten Speicher, der Kennwörter enthalten kann, sowie HiveDump, das alle Informationen über Schlüssel und Werte als CSV-Datei ausgibt.

Derzeit eignet sich das Volatility Framework leider nur für Windows XP. Man darf auf Erweiterungen gespannt sein.

ProDiscover Forensics kann Registry-Dateien in einem Viewer anzeigen. Es ist mit Skripten in der Perl-basierten Sprache ProScript beliebig automatisierbar. Die API steht in Form des Moduls *ProScript.pm* zur Verfügung. Carvey beschreibt dies und stellt passende Skripte bereit. Die Perl-Automatisierung lässt sich gut mit RegRipper koppeln.

Forensic Toolkit (FTK) und **Registry Viewer (RV):** Die forensische Analyse-Plattform FTK3 ist im Funktionsumfang vergleichbar mit EnCase oder X-Ways (siehe unten). Der Registry-Viewer läuft autonom oder integriert in FTK3. Mittels grafischer Konfiguration lässt sich die Suche auf interessant erscheinende Schlüssel eingrenzen. Flexible Schablonen für zusammenfassende Berichte, von AccessData veröffentlicht, erlauben übersichtliche Ausgaben. In Kombination mit dem Password Recovery Toolkit (PRTK) lassen sich bestimme Daten entschlüsseln. Für auf diese Weise nicht ermittelbare Kennwörter kann man eine Wortliste aus dem Registry-Viewer exportieren – für einen Brute-Force-Lexikon-Angriff mittels PRTK.

Bei X-Ways konfiguriert man Schablonen textbasiert, bei FTK in der grafischen Oberfläche. Das ermöglicht aussagekräftige Berichte, jedoch keine komplexeren Auswertungen, insbesondere Korrelationen verschiedener Schlüssel.

Mit **EnCase Forensic** mountet der Ermittler Hive-Dateien zum Anzeigen, was je nach Hive-Größe eine Weile dauern kann. Das Werkzeug stellt die Ergebnisse der Suche nach gelöschten Schlüsseln und Einträgen im Schlupfspeicher grafisch und übersichtlich dar. EnCase kann ROT-13-transformierte Werte im Klartext anzeigen, bietet aber für komplexere Fälle keine Unterstützung. Den mit Microsofts Encrypting File System (EFS) geschützten Speicherbereich einer Registry kann allerdings die EnCase Decryption Suite (EDS) automatisiert entschlüsseln und analysieren. Um einen interessierenden Eintrag in einen Bericht aufzunehmen, kann man unterschiedliche Lesezeichen setzen. Eine Automatisierung von Registry-Auswertungen erlaubt EnScript auf eingeschränkte Weise. Zum Analysieren von Haupt-

Forensik) oder von einem forensischen Image (post mortem) ausgehend untersucht werden? Sind neben statischen Informationen auch volatile erforderlich? Sind nur aktuelle Informationen relevant oder auch alle Sicherungskopien sowie alle gelöschten Hives und in Hives gelöschte Schlüssel? Welche Fragestellungen ein Ermittler auch immer bearbeitet – auf einen blinden Fleck sei hingewiesen: Ein Angreifer kann unter Umgehung des Konfigurationsmanagers Einträge im Hauptspeicher verändern und wieder zurückzusetzen, ohne dass Windows sie physisch schreibt.

Wenn etwa jemand Berechtigungen temporär erweitert und nutzt, zeigt dies möglicherweise kein Image. Da Hives ständig in Benutzung sind, lassen sie sich nicht im laufenden System kopieren oder durchsuchen. In der Live-Forensik hängt man daher die Registry schreibgeschützt wie ein Dateisystem ein (z. B. mit SmartMount oder – unter Linux – *ntreg*) oder nutzt ein Forensik-Werkzeug wie F-Response Enterprise Edition, gefolgt von einer forensischen Registy-Analyse (etwa mit RegRipper). Kann man von einer Linux-CD booten, empfiehlt sich F.I.R.E, das automatisch alle gefundenen Registry-Dateien ins Data-Verzeichnis kopiert. Für eine umfassende Analyse müssen – wie im Folgenden angenommen – vom betreffenden Windows-System sowohl ein Image des Datenträgers mit statischen Informationen als auch ein Hauptspeicherabbild mit den volatilen Informationen vorliegen.

speicher-Images lässt sich zum Beispiel der HBGary Responder integrieren.

Das Mounten macht einen separaten Registry-Viewer überflüssig, allerdings auch die Anzeige langsamer. EnCase fällt mehrfach durch längere Ladezeiten und hohe Latenzzeiten auf. Die Menüführung ist durch die vielen Bereiche gewöhnungsbedürftig. Der Filter auf Hives ist im Vergleich zu X-Ways etwas umständlich zu bedienen. Zwar ist eine Registry-Analyse grundsätzlich möglich, jedoch im Detail etwas mühsam. Es fehlen insbesondere vordefinierte Schablonen für Berichte über forensisch interessante Einträge sowie Funktionen zur fortgeschrittenen inhaltlichen Analyse, wie in RegRipper mit Plug-ins umgesetzt. RegRipper eignet sich als externer Viewer für EnCase. Engagierte Anwender haben EnScript-Skripte veröffentlicht, die das Analysieren der Registry und von Hauptspeicherinhalten erleichtern. Für spezielle Analysen empfiehlt es sich, Registry-Informationen aus EnCase zu exportieren und mit anderen Werkzeugen weiter zu untersuchen.

X-Ways Forensics kann das Carving als besondere Stärke für sich verbuchen, wenngleich es Hive-Einträge nicht gesondert unterstützt. Mit geeigneten Schablonen kann X-Ways Forensics in einfachen Fällen auch Teile von Registry-Informationen aus Hauptspeicherabbildern extrahieren. Ohne Nachbearbeitung mit anderen Werkzeugen geht es jedoch nicht. Der Registry-Viewer zeigt bis zu 32 erkannte Registry-Dateien an. X-Ways Forensics kann übersichtliche Berichte über potenziell relevante Einträge im HTML-Format erstellen, die sich auf einfache Weise in andere Dokumente übernehmen und zum Beispiel mit einer Tabellenkalkulation sortieren und filtern lassen.

Welche Informationen in die Berichte einfließen, legen Schablonen in der Konfigurationsdatei *RegReport.txt* fest. Dabei sind Platzhalter erlaubt. Jeder Bericht enthält eine Auflistung von Detailangaben für die konfigurierten Schlüssel sowie folgende Übersichten, die auf 12 Schlüsseln basieren und für Ermittler besonders relevant sind: angeschlossene Geräte mit Seriennummer (nach Carvey), Partitionen mit Disk-Signaturen, installierte Treiber, Dateisysteme und Dienste.

Da X-Ways Forensics als interaktives Werkzeug konzipiert ist, helfen Daten-Dolmetscher und Hex-Editor beim Interpretieren binärer Registry-Einträge. Es orientiert sich bei der Registry-Analyse ausdrücklich an der Arbeit von Carvey und besticht durch das hohe Tempo. Signaturen und Carving-Schablonen sind flexibel definierbar. Das Ausfiltern relevanter Registry-Dateien aus einem Image ist bei X-Ways gegenüber EnCase intuitiver. Bezüglich der Wiederherstellung gelöschter Schlüssel und dem Durchsuchen des Schlupfspeichers sind X-Ways und EnCase in etwa gleichwertig. Die Berichtsvorlage enthält eine umfassende Auswahl forensisch interessanter Schlüssel, die Einstellungen sind gut anpassbar. Die Tabellen am Ende des Berichts sind besonders übersichtlich und hilfreich.

Gelöschte Dateien wiederherstellen

Aus dem Datenträger-Image lassen sich gelöschte Registry-Dateien in ihren unterschiedlichen Verfallsformen ganz oder teilweise wiederherstellen. Ältere Stände von Registry-Dateien könnten sich unter anderem in einer inzwischen gelöschten Partition oder im Schlupfspeicher befinden. Hier kommt auch das Durchsuchen der ganzen Platte nach Dateikennungen (Carving, in diesem Fall die Überprüfung auf den Dateityp „Registry“) zum Einsatz. Unterschiedliche Registry-Informationen hält Windows ständig an verschiedenen Stellen im Hauptspeicher.

Dank der Auslagerungsdateien *pagefile.sys* und *hiberfil.sys* finden sich manche Registry-Einträge aus dem Hauptspeicher in einem Datenträger-Image wieder. Die Datenstruktur von Registry-Einträgen im Hauptspeicher unterscheidet sich allerdings von derjenigen der Hives und hängt zudem von der Windows-Version ab. Zum Carving von Registry-Informatio-

Attached devices by serial number

Drive	Last access	Prev. access	Name	Serial
	07.12.2006 13:16:15		DiskST94019A_____3.05____	5&67f6dd6&0&0.0.0
	07.12.2006 13:16:19		CdRomTOSHIBA_DVD-ROM_SD-C2612_____1F27____	
	02.01.2008 10:58:25		Disk&Ven_ST325062&Prod_0A&Rev_3.AA	000ECC110005213D&0
	02.01.2008 13:43:05		Disk&Ven_ST325062&Prod_0A&Rev_0811	6&3897a41b&0
	19.02.2008 13:37:44	19.02.2008 13:37:30	Disk&Ven_USB_2.0&Prod_SAC7001-P0709&Rev_0.00	6&2e451a79&0&_&0
	22.02.2008 11:52:40	22.02.2008 11:52:35	Disk&Ven_Verbatim&Prod_STORE_N_GO&Rev_PMAP	077714170736&0
	08.04.2008 16:12:28		Disk&Ven_USB&Prod_DISK_2.0&Rev_0828	814S5BM8MPWP9QSJ&0
	23.04.2008 15:11:36		Disk&Ven_WD&Prod_4000AAK_External&Rev_1.06	57434153383130303735323 1&0
	22.05.2008 09:47:06		Disk&Ven_WD&Prod_10EACS_External&Rev_1.65	57442D574341534A31353733393539&0
	17.06.2008 10:24:59		Disk&Ven_Ext_Hard&Prod__Disk&Rev_	000ECC20003501DC&0
	31.07.2008 13:27:52	31.07.2008 13:27:46	Disk&Ven_Sony&Prod_DSC&Rev_1.00	D340D074816B&0
	06.08.2008 10:00:32	06.08.2008 10:00:24	Disk&Ven_&Prod_USB_DISK_2.0&Rev_PMAP	0771164E0081&0
	28.08.2008 12:03:30	28.08.2008 12:03:23	Disk&Ven_Kingston&Prod_DataTraveler_2.0&Rev_1.00	0010000000000000000414&0
	02.09.2008 19:32:37		Disk&Ven_Freecom&Prod_FM-10_Pro&Rev_3000	00000000000000000644&0
	18.09.2008 16:24:51	18.09.2008 16:24:38	Disk&Ven_Lexar&Prod_JD_FireFly&Rev_1100	AA04016900000635&0
	07.10.2008 18:43:36		Disk&Ven_SAMSUNG&Prod_HD502IJ&Rev_	SAMSUNG_HDS13TJDWQ442677_____&0
	30.10.2008 09:52:11	30.10.2008 09:51:30	Disk&Ven_USB_2.0&Prod_Flash_Disk&Rev_2.00	2405296068 7D&0
	05.11.2008 11:47:42		Disk&Ven_Kingston&Prod_DataTraveler2.0&Rev_1.00	080401160617 1&0
	28.11.2008 09:05:10	28.11.2008 09:05:00	Disk&Ven_PNY&Prod_USB_2.0_FD&Rev_PMAP	6E730C000B5A&0
	05.12.2008 10:20:42	05.12.2008 10:20:22	Disk&Ven_Generic&Prod_USB_SD_Reader&Rev_1.00	058F118111B&0
	05.12.2008 10:20:43	05.12.2008 10:20:22	Disk&Ven_Generic&Prod_USB_MS_Reader&Rev_1.03	058F118111B&1

Die Liste der angeschlossenen Geräte mit Seriennummer kann als Grundlage zum Sicherstellen von Asservaten bei der Hausdurchsuchung dienen (erstellt mit X-Ways Forensics, Abb. 3).

nen sind komplexere Strategien als einfache Signatursuchen erforderlich, die genauere Kenntnis über die Binärstruktur von Registries sowie über die Hauptspeicher-Organisation voraussetzen. Mit Ausnahme des VolReg-Plug-ins für Volatility (nur Windows XP) unterstützen Werkzeuge dies jedoch noch nicht ausreichend.

Ob die Daten respektive -Fragmente der Struktur einer Registry-Datei entsprechen, zeigt zum Beispiel das Perl-Modul Parse::Win32Registry. Auch Hive-Dateien weisen einen Schlupfspeicher auf. Zum Wiederherstellen gelöschter Registry-Schlüssel aus Registry-Dateien und zum Extrahieren von Inhalten aus dem nicht allozierten Bereich eignet sich *Regslack.pl* aus der RegRipper-Sammlung. Bei EnCase funktioniert dies über „Search Entry Slack“ beim Mounten einer Hive-Datei.

Der Ermittler muss genau wissen, welche forensisch relevanten Informationen unter welchen Pfaden liegen, wie sie zu interpretieren sind und zusammenhängen. Die Schlüssel weichen zwischen den Windows-Versionen leicht voneinander ab. Für viele Systeminformationen und Anwendungsprogramme gibt es keine offizielle Dokumentation, jedoch Zusammenstellungen von Forensikern, die sich gut als Vorlage für eigene Anpassungen eignen.

Wer weitere relevante Schlüssel ermitteln möchte, kann etwa in einer virtuellen Maschine Werkzeuge wie RegMon, Regshot, InCtrl5 oder UnDOReg verwenden, um herauszufinden, welche Registry-Veränderungen bestimmte kontrollierte Interaktionen mit dem System hervorrufen. Zur Arbeitserleichterung definiert man Schablonen, die vielversprechende Einträge extrahieren und automatisch in Berichte eintragen. In X-Ways pflegt man dazu eine textbasierte Konfigurationsdatei, im Registry-Viewer von FTK konfiguriert man häufig verwendete Schlüssel mittels grafischer Oberfläche.

FTK enthält vordefinierte Schablonen für Berichte über Registry-Einträge (Registry Summary Reports, RSR), die sich nach Bedarf anpassen lassen. Zusammenfassende Berichte erlauben, Einträge in nutzerdefinierte Abschnitte zu gliedern, mit Überschriften zu versehen und genau anzugeben, welche Teile eines Eintrags nötig sind. Die Korrelation zusammengehöriger Einträge realisiert RegRipper über Plug-ins, von denen sich mehrere unter einer Option zusammenfassen lassen.

Zeitstempel-Analyse

Jeder Schlüssel trägt einen Zeitstempel, wann dieser zuletzt geschrieben wurde (LastWrite, entspricht Last Modification Time). Obwohl dies nicht einer vollständigen „MAC time“ (Modification, Access, Change respektive Creation) entspricht, erlaubt dieser Wert dennoch die Interpretation einer Registry als Logfile. So kann man auch klären, ob ein Anwender Zeitstempel in anderen Bereichen manipuliert hat. Seit Vista sind viele Zeitstempel nicht mehr gepflegt, daher kommt Zeitstempeln in der Registry, soweit noch vorhanden, eine größere Bedeutung zu. Das Datumsformat von Zeitstempeln ist nicht einheitlich, so kommen das 32-Bit-Unix-Format, das 64-Bit-Windows-Format sowie ein 128-Bit-Format vor. Zudem kann es je nach Eintrag weitere Zeitstempel geben.

Als Beispiel kann X-Ways dienen, das den Zeitstempel in der Statuszeile anzeigt. Der Registry-Viewer von FTK decodiert Einträge wie FILETIME-Objekte im SAM-Hive automatisch. X-Ways und EnCase zeigen Zeitleisten grafisch an. RegRipper zeigt mit dem Plug-in ACMru und der Option -t Zeitstempel an, *regtimeline.pl* aus dem Perl-Modul Parse::Win32Registry gibt für NT-Registries Schlüssel und Werte in zeitlicher Reihenfolge aus.

Ein Eintrag hat einen Namen, einen Datentyp und einen Wert (data). Der Wert muss einem von elf Datentypen entsprechen. Ein Datentyp legt die Länge und das Format der Daten fest. So stehen im Datentyp REG_BINARY Binärdaten im Hexformat. Daten in der Registry liegen in un-

```
### Deleted Key  ###

$$
$PROTO.HIV\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\
{2490fb13-f08b-11d8-958e-806d6172696f}\Shell\AutoRun\command
Offset: 0x8e578 [Mon Sep 26 23:34:10 2005]
Number of values: 1
Offset: 0x8e5e0 -->REG_SZ; Default; D:\ShellExe.exe PDServer.exe

Recovered 4 keys and 9 values: #0 keys from allocated space.

Rejected 35 keys and 0 values.

### Unallocated Space ###

Offset 0x68020 - 0x69128:
08 11 00 00 14 00 00 00 05 00 00 00 01 00 01 00 ................
04 00 00 00 14 00 00 00 43 00 3a 00 5c 00 57 00 ........C.:.\.W.
49 00 4e 00 44 00 4f 00 57 00 53 00 5c 00 45 00 I.N.D.O.W.S.\.E.
78 00 70 00 6c 00 6f 00 72 00 65 00 72 00 2e 00 x.p.l.o.r.e.r...
45 00 58 00 45 00 00 00 00 00 00 00 00 00 00 00 E.X.E...........
```

Gelöschte Schlüssel, hier rekonstruiert mittels RegSlack, können sich als für Ermittler besonders interessant erweisen (Abb. 4).

Ausgewählte Werkzeuge für die Registry-Forensik

Produkt	Hersteller	Webseite	Lizenz und Preis
Kommerzielle Forensik-Werkzeuge			
EnCase Forensic 6.18	Guidance Software, Inc.	www.guidancesoftware.com	Dongle, Einzelplatzlizenz Standard Edition, inkl. 1 Jahr Wartung: EUR 2340
EnCase Decryption Suite (EDS) 6.18	Guidance Software, Inc.	www.guidancesoftware.com	Dongle, Zusatzprodukt zu EnCase Forensic, inkl. 1 Jahr Wartung: 355 EUR, enthalten in der EnCase Forensic DeLuxe-Edition (VFS, PDE, EDS): 3480 EUR
HBGary Responder 2.0.0.0899	HBGary, Inc.	www.hbgary.com	auf Anfrage
Forensic Toolkit (FTK) 3.2	AccessData Corp.	www.accessdata.com	auf Anfrage
Password Recovery Toolkit (PRTK) 6.5.1	AccessData Corp.	www.accessdata.com	Zusatzprodukt zu FTK, Preis auf Anfrage
Registry Viewer 1.6.3	AccessData Corp.	www.accessdata.com	Zusatzprodukt zu FTK, Preis auf Anfrage
ProDiscover Forensics 6.7.0.9	Technology Pathways, LLC	www.techpathways.com	auf Anfrage
X-Ways Forensics 15.8-SR3	X-Ways Software Technology AG	www.x-ways.net	Dongle, Einzelplatzlizenz, inkl. 1 Jahr Softwarewartung: EUR 799,90
Kostenlose Werkzeuge			
Cain & Abel Protected Storage Password Manager 4.9.36	Massimiliano Montoro	www.oxid.it/ca_um/	Freeware
Registry Ripper 2.02 (RegRipper 20080909 mit regscan, regslack und ripxp)	Harlan Carvey	www.regripper.net	Freeware
Parse::Win32Registry 0.60	James Macfarlane	http://search.cpan.org/~jmacfarla/Parse-Win32Registry/	Freeware
Volatility Framework1.3 Beta	Volatile Systems LLC	https://www.volatilesystems.com/default/volatility	Freeware, GPL
Volatility Plug-ins VolReg 0.6, VolRip 0.1	Brendan Dolan-Gavitt	www.cc.gatech.edu/~brendan/volatility/	Freeware, GPL
Win32::TieRegistry 0.26	Adam Kennedy	http://search.cpan.org/~adamk/Win32-TieRegistry-0.26/	Freeware

terschiedlichen Codierungen, ROT13-transformiert sowie verschlüsselt vor. Deswegen liefert das Suchen nach einer Zeichenkette, etwa unter *cygwin* mit

```
strings kopierte_hive_datei | 7
                        grep suchmuster
```

mit Sicherheit unvollständige Informationen. Jemand kann Daten in der Registry verbergen, etwa mithilfe von Schlüsseln, die Windows nicht verwendet, durch Ablegen von Daten im Datentyp REG_BINARY in anderen Codierungen oder mit anderen Datentypen, durch Aufteilung von Daten auf mehrere Schlüssel oder die Nutzung eigener Verschlüsselungen. Einige der Werkzeuge bieten ausgefeilte Suchfunktionen sowie Unterstützung bei der Interpretation von Daten an. So decodiert der Daten-Dolmetscher von X-Ways interaktiv binäre Einträge und zeigt den zugehörigen Datenblock synchronisiert an.

Aus Sicht des Forensikers können verschlüsselte Informationen besonders wertvoll sein. Die Registry enthält einen durch Verschlüsselung geschützten Speicherbereich (Protected Storage Area, im Schlüssel „Protected Storage System Provider“, PSSP). Zudem können Daten je nach Wert unterschiedlich codiert oder verschlüsselt sein. Im geschützten Bereich finden sich zum Beispiel Kennwörter und Zugangsdaten: Der Internet Explorer speichert Informationen beim Eingeben in Web-Formulare, um eine automatische Vervollständigung anbieten zu können.

Solche Informationen sind nützlich, wenn man nachweisen möchte, welches Wissen ein Täter gehabt haben kann. Zudem können Kennwörter enthalten sein. Da Nutzer Kennwörter häufig für unterschiedliche Anwendungen einsetzen, gelangt man so möglicherweise an weitere verschlüsselte Informationen. Zugangsdaten zu Windows-Systemen und Webseiten können sich in verschiedenen Caches befinden (SAM, WinINet API) und – wie auch für Outlook/Outlook Express sowie private Netze – wiederherstellbar sein.

Sofern nach rechtlicher Abwägung im Einzelfall zulässig, können Ermittler verschiedene Werkzeuge zum Extrahieren von Daten aus geschützten Bereichen und zur nachfolgenden Entschlüsselung einsetzen, darunter FTK mit dem Password Recovery Toolkit (PRTK) oder EnCase mit der EnCase Decryption Suite (EDS). Auf das Exportieren, etwa mittels

```
volatility hashdump -f Speicher-
Image.im > -y System-Hive-Versatz -s
SAM-Hive-Versatz
```

folgt das Entschlüsseln mit allgemeinen Passwort-Entschlüsselungs-Programmen wie John the Ripper und Ophcrack oder mit auf geschützte Registry-Bereiche spezialisierten Werkzeugen wie Protected Storage Password Manager aus dem Werkzeug Cain & Abel.

Fazit und Ausblick

Die forensische Analyse von Informationen aus Windows-Registries hat mit RegRipper und VolReg große Fortschritte gemacht. Dennoch gibt es noch viel zu tun. Dazu zählen: die Fortentwicklung von Extraktions- und Berichtsschablonen zur komplexen Korrelation verschiedener Registry-Einträge untereinander, wie mit Plug-ins bei RegRipper begonnen, weitere Funktionen zur Zeitstempel-Korrelation, vertieftes Verständnis von Einträgen und ihrer Bedeutung bei den veränderten und erweiterten Informationen in Vista, Windows 7 und neuen Anwendungen sowie der Ausbau und die verstärkte Nutzung von Methoden der Hauptspeicher-Forensik für volatile Registry-Inhalte. (un)

ALEXANDER GESCHONNECK

ist Partner im Bereich Forensic Technology bei KPMG.

ALEXANDER SIGEL

ist Assistant Manager im Bereich Forensic Technology bei KPMG.

Literatur

[1] Harlan Carvey, Eoghan Casey; Windows Forensic Analysis. DVD Toolkit. 2nd edition, 2009, Syngress; Kapitel 4: Registry Analysis

[2] Ergänzende Informationen zu diesem Artikel unter www.computer-forensik.org

Alle Links: www.ix.de/ix1101100