Weiterführende Informationen zum Artikel in der iX 1/2011

Spurensuche in der Windows-Registry: Goldmine

Alexander Geschonneck und Alexander Sigel, KPMG, Risk & Compliance, Forensic Technology

Inhalt

Dieses Dokument ergänzt den in der iX erschienenen Artikel um einige Details, die aus Platzgründen nicht abgedruckt werden konnten.

1. Welche Informationen kann man grundsätzlich mittels Registry-Analyse herausfinden? (Beispiele)

Für Forensiker sind beispielsweise folgende Informationen nützlich:

- Welche Details über das System und Windows gibt es? Welche davon sind zur Identifikation nützlich (z.B. Name der registrierten Person, MAC-Adresse)?
- Welche Kennungen gibt es (technische und für Nutzer) und wann waren diese zuletzt verwendet?
- Welche Programme sind installiert? Wann wurde diese installiert bzw. deinstalliert? Von welcher Quelle wurden Programme installiert?
- Welche Anwendungen wurden wann zuletzt genutzt?
- Welche spezielle Software lässt sich nachweisen (z.B. Anti-Forensik-Software, Software zur Elimination von Beweisen, Brenn-Programme, Malware)? Wann hat Malware etwas Verdächtiges installiert?
- Welche Hardware gibt es im System?
- Welche Gerätetreiber sind installiert?
- Welche Dienste sind installiert?
- Welche Partitionen gibt es und welche Signaturen haben diese? Gibt es alte Partitionen?
- Welche Dateisysteme sind installiert?
- Auf welche Dateien wurde zuletzt zugegriffen? Welche Dateien wurden gespeichert? Welche Verknüpfungen auf Dateien wurden gesetzt?
- Welche Shares gibt es?
- Welche Kommandos wurden vom Kommando-Prompt aus aufgerufen?
- Welche Geräte, insbesondere mobilen Medien (z.B. USB-Sticks, Digitalkameras) waren wann mit dem Rechner verbunden, und welche Seriennummern haben diese?
- Welche Verzeichnisse waren wann mit dem System verbunden (auch solche auf angeschlossenen mobilen Medien)? Unter welchen Laufwerksbuchstaben?
- Welche Nutzernamen und Kennwörter wurden für Windows, Programme, e-Mail und Internet verwendet?
- Welche Websites wurden wann besucht?
- Welche Werte wurden in Formulare von Webseiten eingegeben?
- Wonach wurde im lokalen System sowie bei Internet-Suchmaschinen gesucht?
- Mit welchen Einstellungen der Netzwerkkarten war der Rechner zuletzt mit welchen Netzwerken (inkl. WLANs) verbunden?
- Welche Ports wurden benutzt?
- Gibt es Artefakte, die auf einen Informationsabfluss über USB-Laufwerke oder das Brennen von CD-ROMs hindeuten? Von welchem Nutzerkonto aus wurde ein USB-Stick genutzt?
- Welche Artefakte haben Peer-to-Peer-Programme erzeugt?
- Zeitstempel-Analyse: Wie ergänzen welche Zeitstempel andere Zeitstempel-Analysen?
  - Für welche Zeitzonen wurde der Rechner konfiguriert?
  - Wurden Zeitstempel in anderen Bereichen manipuliert?
  - Gibt es auffällige Zeitstempel, die älter sind als das Erstellungsdatum des letzten Dateisystems oder neuer als das letzte Herunterfahren des Systems?
  - Gibt es Inkonsistenzen zwischen Zeitstempeln untereinander oder in Bezug auf externe Zeitgeber?

2. Welche Wurzelschlüssel sind welchen Hives zugeordnet?

Es gibt folgende sieben Wurzelschlüssel, von denen zwei nicht als physische Datei abgelegt werden:

a) Wurzelschlüssel, die physischen Dateien entsprechen:

Wurzelschlüssel	Abkürzung	Funktion
HKEY_CLASSES_ROOT = HKLM\Software\Classes	HKCR	Registrierte Anwendungen. Zuweisungen zu Dateierweiterungen und die OLE-Datenbank. Ab Windows 2000 sind sowohl Nutzer- als auch System-basierte Informationen enthalten, mit Vorrang der Nutzer-basierten
HKEY_CURRENT_USER = HKU\<SID>	HKCU	Spezifische Einstellungen des gegenwärtig angemeldeten Nutzers (Benutzerinformationen, Präferenzen und Einstellungen)
HKEY_LOCAL_MACHINE	HKLM	Spezifische Einstellungen des lokalen Rechners (Software, Hardware, Sicherheitseinstellungen, etc.)
HKEY_USERS	HKU	Unterschlüssel für jedes aktiv geladene Nutzerprofil (Standardprofil und gegenwärtig angemeldeter Nutzer)
HKEY_PERFOMANCE_ DATA	-	Zur Laufzeit vom Kernel oder bestimmten Programmen bereitgestellte Informationen über die Systemleistung (wird nicht von RegEdit angezeigt!)

b) Wurzelschlüssel, die keinen physischen Dateien entsprechen, volatil (HARDWARE-Hives):

Wurzelschlüssel	Abkürzung	Funktion
HKEY_CURRENT_CONFIG = HKLM\System\Current ControlSet\Hardware Profiles\Current	HKCC	Hardware-Informationen. Werden bei jedem Booten neu erzeugt und daher nicht physisch in eine Registry-Datei geschrieben.
HKEY_DYN_DATA *(nur Win95, Win98 und Win ME)*		Hardware-Geräte und Statistiken über die Netzwerkleistung

3. Wo sind Registry-Dateien unter verschiedenen Windows-Betriebssystemen abgelegt?

Legende:

- %WINDIR% = %SystemRoot = <Laufwerksbuchstabe:>\Windows
- %UserProfile = <Laufwerksbuchstabe:>\Windows\Profiles\<Benutzername>\ (Win 3.1), <Laufwerksbuchstabe:>\WinNT\Profiles\<Benutzername> (Windows NT) bzw. <Laufwerksbuchstabe:>\Dokumente und Einstellungen\<Benutzername>\ (Windows 2000, 2003 und XP)
  <Laufwerksbuchstabe:>\Users\<Benutzername> (Vista)
  bzw. englischsprachige Äquivalente

<table>
<tr><th>Betriebs-system-Familie</th><th>Schlüssel</th><th>Ablageort</th></tr>
<tr><td rowspan="2">Windows 3.11</td><td>System</td><td>%WINDIR\Reg.dat and system.dat</td></tr>
<tr><td>Nutzer</td><td>%UserProfile%\user.dat</td></tr>
<tr><td rowspan="2">Windows 95-Familie (95, 98, 98SE und ME)</td><td>System</td><td>%WINDIR%\system.dat
<u>Windows ME:</u>
aufgeteilt in: %WINDIR%\system.dat und classes.dat

Geschützter Speicherbereich für alle Nutzer, alle installierten Programme, ihre Einstellungen und zugehörige Nutzerkennungen und Kennwörter, Systemeinstellungen</td></tr>
<tr><td>Nutzer</td><td>%WINDIR%\user.dat (falls Nutzertrennung nicht aktiviert, sonst im Nutzerprofil-Verzeichnis %WINDIR%\ Profile\ <username>)

zuletzt benutzte Dateien (MRU)</td></tr>
<tr><td>Windows-NT-Familie (NT, 2000, 2003 und XP)</td><td>System</td><td>%WINDIR%\System32\Config\ (jeweils ohne Dateierweiterung)

<table>
<tr><th>Registry-Pfad</th><th>Datei-Pfad</th><th>Beschreibung</th></tr>
<tr><td>HKLM\System</td><td>system</td><td>Systemeinstellungen</td></tr>
<tr><td>HKLM\SAM</td><td>SAM</td><td>Informationen über den Security Accounts Manager Service: Verwaltung von Benutzerkonten und Sicherheitseinstellungen</td></tr>
<tr><td>HKLM\Security</td><td>SECURITY</td><td>Sicherheitseinstellungen</td></tr>
<tr><td>HKLM\Software</td><td>software</td><td>Alle installierten Programme, ihre Einstellungen und zugehörige Nutzerkennungen und Kennwörter</td></tr>
<tr><td>HKLM</td><td>Userdiff</td><td>Informationen über zugehörige Unterschlüssel für jeden registrierten Nutzer</td></tr>
</table>

Die Registry-Pfade HKLM\Hardware und HKLM\System\Clone sind volatil, daher existiert hierfür kein Dateipfad</td></tr>
</table>

<table>
<tr><th>Betriebs-system-Familie</th><th>Schlüssel</th><th>Ablageort</th></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td>Nutzer</td><td>
<table>
<tr><th>Registry-Pfad</th><th>Datei-Pfad</th><th>Beschreibung</th></tr>
<tr><td>HKU\<User SID></td><td>• %UserProfile%\NTuser.dat sowie
• %UserProfile%\Local Settings\Application Data\Microsoft\Windows\ Usrclass.dat</td><td>Nutzer-spezifische Einstellungen</td></tr>
<tr><td>HKU\.Default</td><td>Default</td><td>Standard-System-einstellungen</td></tr>
</table>
Geschützter Speicherbereich für diesen Nutzer, zuletzt benutzte Dateien (MRU), Nutzerpräferenzen

Neben den Nutzern gibt es Einträge für die Systemkennungen:
• Default User (S-1-5-18)
• LocalService (S-1-5-19, für zentrale Dienste, die nicht im Konto des lokalen Systems laufen müssen) und
• NetworkService (S-1-5-20, für zentrale Netzwerk-Dienste)
</td></tr>
<tr><td rowspan="2">Windows Vista (ähnlich wie NT-Familie, aber …)</td><td>System</td><td>%WINDIR%\System32\Config

<table>
<tr><th>Registry-Pfad</th><th>Datei-Pfad</th><th>Beschreibung</th></tr>
<tr><td>HKLM\Components</td><td>COMPONENTS</td><td>Systemeinstellungen</td></tr>
<tr><td>HKLM\BCD00000000</td><td>BCD</td><td>EFS-Bootwerte</td></tr>
<tr><td>HKLM\BCD</td><td><Laufwerks-buchstabe:>\ Boot\BCD</td><td>Boot Configuration Data</td></tr>
<tr><td>HKLM\BCD</td><td>BCD-Template</td><td>Boot Configuration Data</td></tr>
<tr><td>HKLM\BCD</td><td>%WINDIR%\ Windows\winsxs \x86_microsoft-windows-b..(langer Pfad)\BCD-Template</td><td>Boot Configuration Data</td></tr>
</table>
HKLM\Schema ist volatil
</td></tr>
<tr><td>Nutzer</td><td>%UserProfile%\AppData\Local\Microsoft\Windows\Usrclass.dat

<table>
<tr><th>Registry-Pfad</th><th>Datei-Pfad</th><th>Beschreibung</th></tr>
<tr><td>HKU\<User SID></td><td>system</td><td>Nutzer-spezifische Einstellungen</td></tr>
</table>
</td></tr>
<tr><td>Windows 7 (vergleichbar mit Windows Vista)</td><td>System</td><td>
<table>
<tr><th>Registry-Pfad</th><th>Datei-Pfad</th><th>Beschreibung</th></tr>
<tr><td>HKLM\BCD</td><td>%WINDIR%Boot\, z.B. DVD\PCAT</td><td>Boot Configuration Data</td></tr>
</table>
Unter %WINDIR%\System32\config\systemprofile existiert auch eine Datei
</td></tr>
</table>

Betriebs-system-Familie	**Schlüssel**	**Ablageort**
		ntuser.dat
	Nutzer	Die Profile für die Servicekennungen LocalService und NetworkService befinden sich nun unter %WINDIR%\\ServiceProfiles\

Die grundlegende Struktur sowie die wesentlichen Inhalte der Registry haben sich in Vista und Windows 7 nicht geändert.

Ab Vista neu sind Transaktionale Registries (Registry Transaction Logging (TxR) sowie Registry-Virtualisierung.
Wenn Vista keinen Schreibzugriff auf die Registry hat, z.B. weil ein Nutzer eine virtuelle Maschine ausführt, schreibt Vista in ein Log im Nutzerprofil. Registry-Operationen mit potenziell globaler Auswirkung können unter Nutzerinformationen geschrieben werden.

Beispiel:
Nicht berechtigter Schreibversuch auf HKLM\Software\App wird umgeleitet auf HKU\<SID>_Classes\VirtualStore\Machine\Software\.
Wenn der Nutzer sich einloggt, wird folgende Datei auf diesen Schlüssel gemappt: %UserProfile%\AppData\Local\Microsoft\Windows\usrclass.dat

4. Wo und für welche Registry-Dateien legen verschiedene Windows-Betriebssysteme Sicherungskopien an?

Betriebs-system-Familie	Schlüssel	Sicherungsanlass/-form	Sicherungskopie(n)
Windows95	System	Bei jedem Reboot, der nicht im SafeMode erfolgt	%WINDIR%\System.da0
	Nutzer		%WINDIR%\User.da0
Windows 98, 98SE und ME	System	Täglich, unter Nutzung von ScanregW.exe, als Cabinet-Dateien, bis zu fünf Generationen	%WINDIR%\Sysbckup\RB000.cab bis RB0005.cab
	Nutzer		
Windows 95, 98, 98SE und ME	System	Bei Installation von Windows	<Laufwerksbuchstabe:>\System.1st Windows ME: <Laufwerksbuchstabe:>\System.1st und Classes.1st
Windows 2000, 2003 und XP	Nutzer	Bei Installation von Windows	%WINDIR%\System32\Config*.sav sowie unter %WINDIR%\repair\ Sicherungskopie
Windows2000			*.ALT Backup-Kopie, die es nur bei Windows 2000 gibt
Windows XP		Bei jeder Erstellung eines Wiederherstellungs-Punktes (Restore-Point)	Im System Restore Information-Ordner auf demselben Laufwerk, auf dem Windows installiert ist, üblicherweise <Laufwerksbuchstabe:>\System Volume Information\{GUID}\
Windows Vista und Windows 7	System		Hives in den Volume Shadow-Kopien %WINDIR%\System32\config\ RegBack wird angelegt für alle sechs System-relevanten Hives: • SYSTEM • SECURITY • SAM • COMPONENTS • SOFTWARE • DEFAULT

Legende:
.log ist das Transaktions-Log der Änderungen in einem Hive.
1 .log1: tatsächliches Log der Änderungen
.log und .log2: Werden beim Windows7-Setup erzeugt und bleiben unverändert

5. Welche Registry-Schlüssel/-Werte sind aus IT-forensischer Sicht besonders interessant? (Beispiele)

Harlan Carvey hat eine Liste mit nützlichen Schlüsseln veröffentlicht und als Plugins in RegRipper umgesetzt. Beispiele für solche Schlüssel finden sich u.a. bei AccessData, bei Lih Wern Wong oder bei Derrick J. Farmer. Die im Lieferumfang von X-Ways Forensics enthaltene Datei "Reg Report.txt" mit knapp 300 Schlüsseln eignet sich ebenfalls gut als Vorlage für eigene Sammlungen solcher Schlüssel.

Funktion	**Schlüssel**
Auto-Vervollständigung des Windows Explorers	\HKCU\Software\Microsoft\InternetExplorer\IntelliForms \HKCU\Software\Microsoft\InternetExplorer\IE Data
Im lokalen System ausgeführte Suchen	HKCU\SOFTWARE\Microsoft\ Search Assistant\ACMru\nnnn 5001 5603: Suchbegriffe bei Suche nach Ordnern und Dateinamen 5604: Suchbegriffe bei Suche in Dateien 5647
Geschützter Speicherbereich	HKCU\Software\Microsoft\Protected Storage System Provider\
Zuletzt benutzte Dateien (MRU)	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ ComDlg32\OpenSaveMRU HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ ComDlg32\LastVisitedMRU HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ RecentDocs
Zuletzt im DOS-Prompt ausgeführte Programme	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ RunMRU
Gegenwärtig installierte Software (soweit über Systemsteuerung > Software sichtbar). Es gibt weitere installierte Software	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
Angeschlossene Geräte	HKLM\SYSTEM\MountedDevices
Informationen über mittels mount verbundener Geräte, z.B. USB-Sticks	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ MountPoints2\CPC\Volume\ HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ Map Network Drive MRU HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ MountPoints2

Funktion	Schlüssel
Bezeichnung und Seriennummer von USB-Speichergeräten, soweit diese eine Seriennummer haben (ggf. nur Pseudo-Seriennummer, die keine Rückverfolgung erlaubt)	HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR
Mögliche Hinweise auf Malware beim Systemstart bzw. bei Ausführung von cmd.exe	HKLM\ SOFTWARE \Microsoft\Windows\CurrentVersion\Run, RunOne, RunOnceEx, RunServices, RunServicesOnce HKLM\SOFTWARE\Microsoft\Command Processor HKCU\Software\Microsoft\Command Processor
Netzwerkadapter, zuletzt aufgerufene IP-Adresse	HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\GUID HKLM\SOFTWARE\Microsoft\WZCSVC\Parameters\Interfaces\GUID
Zugriffe auf Systemobjekte, wie z.B. Programme, Shortcuts oder Steuerungselemente (ROT-13-chiffriert)	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist (leichte Veränderungen der Struktur unter Windows 7)
Zuletzt im Internet Explorer eingegebene URLs	HKCU\Software\Microsoft\Internet Explorer\TypedURLs

6. Mit welchen IT-forensischen Gegenmaßnahmen (Anti-Forensik) muss man bei der Registry-Analyse rechnen?

Anti-forensische Techniken in der Computer-Forensik sind Gegenmaßnahmen (counterforensics), mit denen jemand versucht, eine IT-forensische Analyse zu behindern, sodass eine Aufklärung von Sachverhalten erschwert oder unmöglich gemacht wird.

Eine gängige Einteilung unterscheidet das Verbergen von Daten, das Löschen von Artefakten, die Verschleierung von Spuren sowie Angriffe gegen Prozesse und Werkzeuge von IT-Forensikern.

Vgl. hierzu auch:
- Alexander Geschonneck:„Anti-Forensik-Methoden im Überblick", in: iX 8/2007, S. 104ff.
- <http://en.wikipedia.org/wiki/Anti-computer_forensics>
- <http://www.forensicswiki.org/wiki/Anti-forensic_techniques>
- < http://www.anti-forensics.com/>

Anti-Forensiker möchten etwa wissen:
- Vermeiden: Wie kann ich mich gegen diese Datenüberwachung durch das Betriebssystem weitmöglichst schützen?
- Manipulieren: Wie kann ich Forensiker bei der Analyse der Registry in die Irre führen oder ihre Ergebnisse angreifbar machen?
- Verbergen: Wie kann ich die Registry nutzen, um geheime Informationen vor dem Zugriff durch Dritte zu verstecken.

Vermeiden von Datenspuren

Es ist nicht leicht, der Registry abzugewöhnen, bestimmte Informationen nicht mehr zu verzeichnen. Denn dazu muss man an vielen Stellen Einträge in der Registry ändern, die nicht offiziell dokumentiert sind. Zudem besteht die Gefahr, dass man damit benötigte Systemfunktionalitäten ausschaltet oder etwas durcheinanderbringt. Möglicherweise hilft auch der Einsatz eines Registry Cleaners (z.B. bei System Mechanic, www.iolo.com, enthalten).

An dieser Stelle sei jedoch verraten:
- Windows > Zuletzt geöffnete Dokumente > Einträge löschen löscht zuletzt genutzte Dokumente und eingegebene URLs aus dem Registry. „Internet Explorer-Verlauf löschen löscht die aufgerufenen URLs.
- Das Mitloggen von Daten im UserAssist-Schlüssel kann ausgeschaltet werden, indem man unter dem Settings-Schlüssel einen DWORD-Wert mit dem Namen NoLog und dem Wert 1 erzeugt.
- HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management, ClearPagefileAtShutdown = 1 sorgt dafür, dass beim Herunterfahren das Pagefile löscht.
- Vermeiden, dass Zeitstempel für Dateien gesetzt werden: HKLM\\SYSTEM\CurrentControlSet\Control\FileSystem\ NtfsDisableLastAccessUpdate auf 1 setzen: schaltet die Aktualisierung der Zeitstempel beim letzten Zugriff aus. Dies kann die forensische Analyse erheblich erschweren. (Ist ab Vista standardmäßig ausgeschaltet!)

Es ist allerdings zu beachten, dass auch Anwendungen Zeitstempel schreiben, sodass die Vermeidung von Zeitstempel auf Dateisystem-Ebene allein ggf. nicht ausreicht, den IT-Forensiker zu täuschen.

Irreführung von IT-Forensikern

Zeitstempel können gefälscht werden. Dabei ändern sich nicht einmal die Prüfsummen, die sich nur auf den Inhalt von Dateien beziehen.

Dies funktioniert beispielsweise mit dem Werkzeug timestomp aus dem Metasploit Anti-Forensic Investigation Arsenal (MAFIA).
<http://www.forensicswiki.org/wiki/Timestomp>
<http://www.metasploit.com/research/projects/antiforensics/>

Weitere Informationen finden sich auch in den Arbeiten von Adrian Crenshaw, der Webseiten zur Informationssicherheit unter www.irongeek.com betreibt, z.B. in seiner „Occult Computing Class
< http://www.irongeek.com/i.php?page=videos/anti-forensics-occult-computing>

Verbergen von Daten

Zum Verbergen von Daten sind grundsätzlich steganographische Werkzeuge geeignet. Typischerweise werden Daten in Bildern oder Video-Dateien untergebracht, dies geht aber in beliebigen Dateien, z.B. im Slackspace (vgl. Slacker <http://www.metasploit.com/data/antiforensics/slacker.exe>), in $MFT, in der Host Protected Area (HPA), in Zeitstempeln von Logfiles, oder in der Windows-Registry.

In der Windows-Registry sind potenziell interessant:

- reservierte, aber nicht genutzte Bereiche
- Bereiche für Zeitstempel, in denen in einem Zeitstempel-Format Daten abgelegt werden, die keine Zeitstempel sind.

Anti-Anti-Forensik

Unter Anti-Anti-Forensik versteht man Gegenmaßnahmen, die Anti-Forensik-Maßnahmen erschweren oder ausgleichen. Beispielsweise kann man gefälschte Zeitstempel möglicherweise durch Querreferenzierung zwischen Zeitstempeln (z.B. Logfiles des Dateisystems und von Virenscannern), auch in Bezug auf externe Zeitgeber, entlarven (z.B. Google Cookies).

7. Welche Literatur eignet sich zur Vertiefung?

AccessData: Registry Quick Find Chart
http://www.accessdata.com/media/en_us/print/papers/wp.Registry_Quick_Find_Chart.en_us.pdf
AccessData: Registry Summary Report (RSR) files
http://www.accessdata.com/rsr.html
AccessData: Windows Forensics — Registry. Forensic Toolkit, FTK Imager, Password. Recovery Toolkit and Registry Viewer. Advanced. Three-day
http://www.accessdata.com/downloads/course_syllabus/Microsoft_Windows_Registry.pdf
Andrew Aronoff (9. November 2009): [Von "Silent Runners" überprüfte Registry-Werte]
http://www.silentrunners.org/sr_launchpoints.html
Steve Bunting & William Wei (2006): EnCase Computer Forensics: The Official EnCe: EnCase Certified Examiner Study Guide, Kapitel 14 "Advanced EnCase", S. 417-425: "Registry". Wiley.
Harlan Carvey (2008): regref.xls
http://www.regripper.net/RegRipper/Documents/regref.xls
Harlan Carvey & Eoghan Casey (2009): Windows Forensic Analysis. DVD Toolkit. 2nd edition. Syngress (mit DVD)
Harlan Carvey (2011): Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry , Syngress. 248 Seiten, erscheint Januar 2011
Damon Cortesi (22. März 2005): Using shadow copies to steal the SAM
http://dcortesi.com/2005/03/22/using-shadow-copies-to-steal-the-sam/
Brendan Dolan-Gavitt (4. September 2007)
Challenges in Carving Registry Hives from Memory
http://moyix.blogspot.com/2007/09/challenges-in-carving-registry-hives.html
und weitere Einträge unter http://moyix.blogspot.com/search/label/hive
Brendan Dolan-Gavitt (2008): Forensic analysis of the Windows registry in memory, in: digital information 5(2008), 26-32
http://dfrws.org/2008/proceedings/p26-dolan-gavitt.pdf
http://dfrws.org/2008/proceedings/p26-dolan-gavitt_pres.pdf (Folien)
Brendan Dolan-Gavitt (2009): Registry Analysis and Memory Forensics: Together at Last. Vortrag SANS Forensics 2009.
http://www.slideshare.net/mooyix/sans-forensics-2009-memory-forensics-and-registry-analysis
Derrick J. Farmer (2008): A Windows Registry Quick-Reference for the Everyday Examiner
http://eptuners.com/forensics/contents/A_Forensic_Examination_of_the_Windows_Registry.pdf
Jason Koppe (7. Oktober 2008): RegRipper, regview, and Bluetooth Registry Settings.
http://nssadoc.blogspot.com/2008/10/regripper-regview-and-bluetooth.html
Richard McQuown ("ForensicZone") (28. Januar 2009): [Nutzung von VolReg für Passwort-Entschlüsselung]
http://forensiczone.blogspot.com/2009/01/using-volatility-1.html
Timothy D. Morgan (2008): Recovering deleted data from the Windows registry, in: digital investigation 5(2008), 33-41
http://www.dfrws.org/2008/proceedings/p33-morgan.pdf

Timothy D. Morgan (9. Juni 2009, Version 0.4): The Windows NT Registry File Format
http://www.sentinelchicken.com/data/TheWindowsNTRegistryFileFormat.pdf
In diesem Verzeichnis auch sein Beitrag „Recovering deleted data from the Windows registry", digital investigation 5(2008), 33-41, inklusive Folien.

Lance Mueller (17. Juli 2007): EnCase EnScript to quickly sort last written timestamps on registry keys
http://www.forensickb.com/2007/07/encase-enscript-to-quickly-sort-last.html

Peter Nordahl-Hagen: Offline NT Password & Registry Editor
http://pogostick.net/~pnh/ntpasswd/

Registry
http://msdn.microsoft.com/en-us/library/ms724871(VS.85).aspx

Mark Russinovich: Inside the Registry, ursprünglich erschienen in: Windows NT Magazine
http://technet.microsoft.com/en-us/library/cc750583.aspx

Zhenhua Tang, Hong Ding, Ming Xu, Jian Xu (2009): Carving the Windows Registry Files Based on the Internal Structure, in: Information Science and Engineering, International Conference on, 4788-4791.
http://www.computer.org/portal/web/csdl/doi/10.1109/ICISE.2009.379

Windows Registry
http://en.wikipedia.org/wiki/Windows_Registry

Windows Server 2003 Resource Kit Registry Reference
http://technet.microsoft.com/en-us/library/cc778196(WS.10).aspx
(aktualisiert am 28. März 2003)

Lih Wern Wong: Forensic Analysis of the Windows Registry
http://www.forensicfocus.com/downloads/forensic-analysis-windows-registry.pdf/
(bezieht sich auf Win XP SP2)

Yuandong Zhu, Pavel Gladyshev & Joshua James (2009): Using shellbag information to reconstruct user activities, in: digital investigation 6(2009), 69-77
http://www.dfrws.org/2009/proceedings/p69-zhu.pdf