FH-Dozent Ing. Mag. Horst Greifeneder
Allgemein beeideter und gerichtlich zertifizierter Sachverständiger, Fachgebiet Informationstechnik;
Lehrbeauftragter an der FH Salzburg, Master-Studiengang Informationstechnik & System-Management;
Computerforensik-Spezialist

Forensische Datenauswertung von Prefetch-Dateien zum Nachweis eines verdächtigen Programmeinsatzes

1. Einleitung

Der Nachweis des Einsatzes eines verdächtigen Programmes stellt häufig eine zentrale Fragestellung bei einer computerforensischen Untersuchung dar. Schnelle Antworten kann ein Blick in das Programmverzeichnis oder die Registry des Computersystems liefern. Wurden jedoch Programmeinträge am sichergestellten Computersystem gezielt gelöscht, lassen sich gegebenenfalls Antworten über die forensische Auswertung vorhandener Prefetch-Dateien finden.

Der Fokus des Artikels liegt in der Erörterung der Aussagekraft von Prefetch-Dateien im Zuge einer computerforensischen Datenauswertung. Zum besseren Verständnis des Ermittlungsansatzes werden die technischen Grundlagen des Prefetching sowie einzelne Analysemethoden der Prefetch-Dateien näher beschrieben.

2. Prefetching-Grundlagen

Prefetching ist eine von Microsoft-Betriebssystemen seit Windows XP genutzte Cache-Technik, um den Einsatz von Anwendungen zu beschleunigen.

2.1. Prefetching unter Windows

Beim Prefetching sammelt und speichert das Betriebssystem ausgewählte Informationen zu den beim Booten oder Anwendungsstart benötigten Programmmodulen wie Dynamic Link Libaries, Steuerungsdateien oder Gerätetreiber.

Bei Windows-Client-Betriebssystemen werden die gesammelten Daten in Dateien mit der Dateiendung *.pf im Ordner C:\Windows\Prefetch gespeichert. Über das genaue Dateiformat der Prefetch-Dateien und den verwendeten Algorithmus bei der Verarbeitung der Daten schweigt sich Microsoft aus.[1] Vermutlich handelt es sich aber bei den gespeicherten Daten um Informationen über den Speicherort der beim Programmstart benötigten Module.

Wird eine ausführbare Datei gelöscht oder deinstalliert, verbleibt die Prefetch-Datei in der Regel am System erhalten.

2.2. Konfiguration von Prefetching

Standardmäßig haben Windows XP, Vista und Windows 7 sowohl Boot- als auch Applikations-Prefetching aktiviert. Bei SSD-Laufwerken ist das Prefetching standardmäßig deaktiviert.

Die Konfiguration des Prefetching kann über nachfolgenden Registry-Schlüssel ermittelt werden:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\Prefetch Parameters**Enable-Prefetcher**

Voreingestellt ist im Schlüssel „Enable-Prefetcher“ der Wert „3“, welcher sowohl den Systemstart als auch Anwendungen beschleunigen soll. Mit dem Wert „0“ für den Schlüssel lässt sich der Prefetcher deaktivieren. Bei „1“ werden nur Anwendungen, bei „2“ nur Systemdateien des Bootvorgangs protokolliert.

Name	Größe	Typ	Geändert am	Erstellt am
WUAUCLT.EXE-399A8E72.pf	63 KB	PF-Datei	5.6.2012 16:57	22.4.2012 23:26
NTOSBOOT-B00DFAAD.pf	986 KB	PF-Datei	5.6.2012 16:57	22.4.2012 23:26
CMD.EXE-087B4001.pf	16 KB	PF-Datei	5.6.2012 16:54	22.4.2012 23:26
VER.CLSID.EXE-3667BD89.pf	17 KB	PF-Datei	5.6.2012 16:52	22.4.2012 23:26
MSIEXEC.EXE-2F8A8CAE.pf	147 KB	PF-Datei	5.6.2012 16:52	22.4.2012 23:26
LOGON.SCR-151EFAEA.pf	8 KB	PF-Datei	30.5.2012 18:03	22.5.2012 17:45
MPSIGSTUB.EXE-1D30D19B.pf	25 KB	PF-Datei	30.5.2012 17:50	22.5.2012 17:07
AM_DELTA.EXE-2F7A6F0C.pf	22 KB	PF-Datei	30.5.2012 17:49	22.5.2012 17:07
WMIPRVSE.EXE-28F301A9.pf	48 KB	PF-Datei	30.5.2012 17:49	22.4.2012 23:26
MPCMDRUN.EXE-122AF334.pf	36 KB	PF-Datei	30.5.2012 17:49	22.5.2012 17:07
FLASHPLAYERUPDATESERVICE.EXE-34BC5027.pf	27 KB	PF-Datei	30.5.2012 17:48	22.5.2012 17:12
DFRGNTFS.EXE-269967DF.pf	41 KB	PF-Datei	29.5.2012 18:24	22.5.2012 17:51
DEFRAG.EXE-273F131E.pf	17 KB	PF-Datei	29.5.2012 18:24	22.5.2012 17:51
Layout	411 KB	Konfigurationseinst…	29.5.2012 18:24	17.5.2012 17:43
MSOHTMED.EXE-14B8D6FE.pf	9 KB	PF-Datei	29.5.2012 18:08	22.5.2012 17:03
OSE.EXE-313A091F.pf	6 KB	PF-Datei	29.5.2012 18:04	22.5.2012 17:03
FIREFOX.EXE-1D57670A.pf	57 KB	PF-Datei	29.5.2012 18:02	22.5.2012 16:58
SPUPDSVC.EXE-21B36524.pf	10 KB	PF-Datei	29.5.2012 17:59	22.4.2012 23:32
WMIADAP.EXE-2DF425B2.pf	31 KB	PF-Datei	25.5.2012 08:58	22.4.2012 23:26
REGSVR32.EXE-25EEFE2F.pf	32 KB	PF-Datei	25.5.2012 08:52	22.4.2012 23:26
RUNDLL32.EXE-451FC2C0.pf	15 KB	PF-Datei	25.5.2012 08:50	22.4.2012 23:38
UPDATE.EXE-156E0976.pf	81 KB	PF-Datei	25.5.2012 08:42	25.5.2012 08:42
UPDATE.EXE-2C15253E.pf	81 KB	PF-Datei	25.5.2012 08:42	25.5.2012 08:42
UPDATE.EXE-20EBC2E4.pf	50 KB	PF-Datei	25.5.2012 08:42	25.5.2012 08:42
UPDATE.EXE-2A5F3612.pf	63 KB	PF-Datei	25.5.2012 08:42	25.5.2012 08:42
PLUGIN-CONTAINER.EXE-170C935C.pf	74 KB	PF-Datei	25.5.2012 08:42	22.5.2012 17:13
UPDATE.EXE-023D4CB8.pf	81 KB	PF-Datei	25.5.2012 08:42	25.5.2012 08:42
UPDATE.EXE-2B6890C3.pf	81 KB	PF-Datei	25.5.2012 08:42	25.5.2012 08:42

Abbildung 1: Datei-Listing des Prefetch-Ordners unter Windows XP (Ausschnitt)

Generelle Voraussetzung für das Funktionieren von Prefetching ist, dass der Taskplaner nicht deaktiviert worden ist.

2.3. Dateien im Prefetch-Ordner

Die im Prefetch-Verzeichnis befindlichen Dateien können in drei Kategorien – Bootvorgang, Anwendung und Host-Anwendungen – unterteilt werden.

Für den Bootvorgang existiert genau eine Prefetch-Datei mit dem Namen NTOSBOOT-B00DFAAD. Die Datei hat immer den gleichen Namen und beinhaltet Informationen zum Bootvorgang des Systems. Aufgezeichnet werden Systemvorgänge innerhalb der ersten 2 Minuten des Bootvorgangs bzw 60 Sekunden nach dem Start aller Win32-Dienste.

Prefetch-Dateien für Anwendungen sind für die computerforensische Analyse am interessantesten. Die Namenskonvention für anwendungsbezogene Prefetch-Dateien verwendet den Namen der ausgeführten Datei, deren Dateiendung sowie einen 32-Bit-Hashwert (zB FIREFOX.EXE-1D57670A.pf), welcher den jeweiligen Speicherort der ausgeführten Anwendung repräsentiert.[2] Aufgezeichnet werden die ersten 10 Sekunden nach einem Programmstart.

Bei Prefetch-Dateien für Host-Anwendungen (z.B. DLLHOST.EXE-4B6CB38A.pf) erfolgt die Dateibenennung über eine leicht modifizierte Hashwert-Berechnung. Dieses Verfahren ermöglicht die Existenz mehrerer DLLHOST-Dateien gleichen Ursprungs im Prefetch-Verzeichnis und Rückschlüsse auf die Anwendung, welche den Windows-Prozess aktivierte.

Aus computerforensischer Sicht überaus interessant ist die Datei Layout.ini. Die Textdatei beinhaltet eine Auflistung der beim System- bzw Programmstart aufgerufenen Dateien und Verzeichnisse. Die Layout.ini wird benutzt, um die Dateien beim Defragmentieren optimiert für schnelleres Lesen auf der Festplatte anzuordnen, und wird periodisch erneuert.

3. Forensische Datenauswertung

Die Prefetch-Analyse eröffnet dem Sachverständigen verschiedene Ermittlungsansätze, welche detaillierte Auskunft über die Existenz und den Einsatz von Anwendungen geben.

3.1. Liste der verwendeten Programme

Die Auflistung der im Prefetch-Ordner befindlichen Dateien im Windows Explorer weist auf die am System verwendeten Programme hin. Der Prefetch-Ordner enthält bis zu 128 Prefetch-Dateien. Der Einsatz eines ohne Installation lauffähigen oder deinstallierten Programmes ist über dessen Eintrag in der Layout.ini nachweisbar.

3.2. Zeitpunkt der Programmnutzung

Der Zeitpunkt der erst- und letztmaligen Programmnutzung lässt sich über die für das jeweilige Programm im Dateisystem gespeicherten Erstell- und Änderungszeiten erfassen. Dabei sind die unterschiedlichen Zeitstempel-Algorithmen der unterschiedlichen Windows-Versionen zu berücksichtigen. Ferner ist zu beachten, dass Windows 7 und Vista standardmäßig die Einträge für das Änderungsdatum nicht aktualisieren.

3.3. Rückschlüsse auf Benutzer

Dateien im Prefetch-Ordner beziehen sich immer auf die gesamte Systemnutzung. Sind auf einem Computer mehrere Benutzerkonten aktiv, kann eine verdächtige Programmnutzung über eine vorhandene Prefetch-Datei nicht direkt einen bestimmten Benutzer zugeordnet werden. Eine Bestimmung individueller Benutzeraktivitäten wäre eventuell über benutzerspezifische Einträge in der Layout.ini-Datei oder durch die Auswertung von Event-Log-Dateien oder Registry-Einträgen durchführbar. Im Sicherheitslog finden sich beispielsweise die Loginzeiten und Namen der eingeloggten Benutzerkonten. In der Registry liefert eine Untersuchung der UserAssist-Einträge entsprechende Hinweise auf vom Benutzer genutzte Programme.[3]

3.4. Häufigkeit der Programmnutzung

Die Häufigkeit der Nutzung eines Programmes lässt sich anhand des Wertes von Count ermitteln. Der Wert von Count einzelner Prefetch-Dateien ist über den Windows Explorer nicht ersichtlich. Es existieren jedoch kostenfreie Tools wie Windows File Analyzer oder WinPrefetchView, welche eine rasche Auswertung der Dateien ermöglichen.

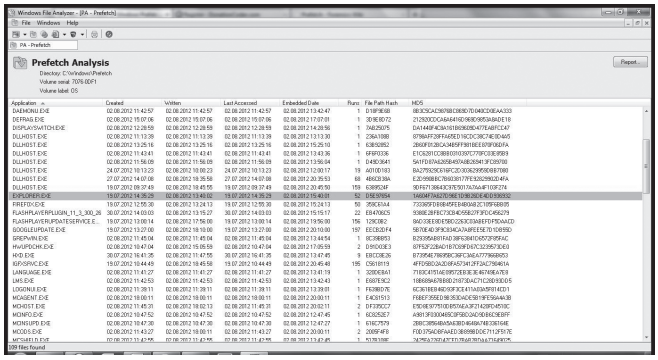

Abbildung 2: Screenshot: Auswertung Prefetch-Verzeichnis, Tool Windows File Analyzer[4]

Wird eine Prefetch-Datei gelöscht, erfolgt beim erneuten Start der Anwendung in der Regel ein Reset des Zählers auf „0“. Interessant in diesem Zusammenhang ist die Beobachtung, dass unter Windows 7 manche Prefetch-Dateien (zB MS Office-Dateien) als Count-Wert immer „1“ aufweisen.

3.5. E-Mail-Nutzung

Wird am System als E-Mail-Client Microsoft Outlook verwendet, dann sind bei einer Analyse der Prefetch-Datei von Outlook die zuletzt abgerufenen E-Mail-Konten und deren Speicherorte als Einträge ersichtlich. Besonders komfortabel ist diese Analyse mit dem Tool WinPrefetch-View zu bewerkstelligen.

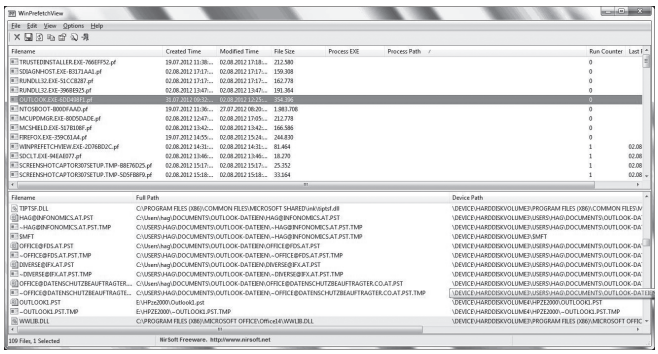

Abbildung 3: Screenshot: Zugriff auf Outlook-Konten, Tool WinPrefetchView[5]

3.6. Rekonstruktion gelöschter Prefetch-Dateien

Wurde eine Prefetch-Datei gelöscht, besteht – sofern die Daten nicht bereits überschrieben wurden – die Möglichkeit, die Datei über File Carving[6] ganz oder teilweise wiederherzustellen und in einem Hex-Editor zu analysieren.

Soweit bekannt, bestehen Prefetch-Dateien aus zwei Teilen. Im – forensisch besonders interessanten – ersten Teil werden Metadaten wie Programmname, Zeitstempel und die Häufigkeit der Programmausführung (Run Count) in codierter Form gespeichert. Der zweite Teil beinhaltet ein textbasiertes Verzeichnis der Dateien, auf die beim Programmstart zugegriffen wurde, sowie deren Speicheradresse.

Prefetch-Datei verfügen über einen charakteristischen Header in ASCII „....SCCA“ bzw n hexadezimal Darstellung „0x11 00 00 00 53 43 43 41“ (XP) bzw „0x17 00 00 00 53 43 43 41“ /Vista/7). Eine Prefetch-Datei beinhaltet keine spezielle Zeichenkombination, welche das Ende der Datei kennzeichnet.

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000   17 00 00 00 53 43 43 41 11 00 00 00 50 1B 02 00   ....SCCA....P...
00000010   46 00 49 00 52 00 45 00 46 00 4F 00 58 00 2E 00   F.I.R.E.F.O.X...
00000020   45 00 58 00 45 00 00 00 00 00 00 00 00 00 00 00   E.X.E...........
00000030   47 00 00 00 00 80 FA FF FF 00 00 00 00 00 00 00   G...€úÿÿ........
00000040   00 00 00 00 00 00 00 00 00 00 6E 9D 0E 03 A4 61 9C 35   ........n...¤aœ5
00000050   00 00 00 00 F0 00 00 00 62 00 00 00 30 0D 00 00   ....ð...b...0...
00000060   47 26 00 00 84 D8 01 00 66 35 00 00 F0 0D 02 00   G&..„Ø..f5..ð...
00000070   01 00 00 00 60 0D 00 00 16 00 00 00 01 00 00 00   ....`...........
00000080   4E 11 71 86 A4 B6 CD 01 00 8C 86 47 00 00 00 00   N.q†¤¶Í..Œ†G....
00000090   00 8C 86 47 00 00 00 00 00 [54] 00 00 00 06 00 00 00   .Œ†G....T.......
```

Abbildung 4: Screenshot: Header der Prefetch-Datei für Firefox.exe in Win 7 (Ausschnitt)

Wird per File Carving eine gelöschte Prefetch-Datei identifiziert, ist in der Regel eine Aussage über die ursprüngliche Anwendung (Offset 0x10: Name der ausgeführten Datei) möglich. Im Normalfall sind noch weitere Metadaten wie Run Count (Offset 0x90 (XP), 0x98 (Vista/7): Anzahl der Dateiaufrufe) und letzter Ausführungszeitpunkt (Offset 0x78 (XP), 0x80 (Vista/7): Zeitstempel des letzten Aufrufs) der Prefetch-Datei rekonstruierbar.

Können mehrere gelöschte Prefetch-Dateien einer ausgeführten Datei wiederhergestellt werden, sind über die Run-Count-Werte Aussagen hinsichtlich der unterschiedlichen Ausführungszeitpunkte möglich.[7]

4. Fazit

Prefetch-Dateien stellen in Hinblick auf Fragen zur Existenz und Nutzung von Programmen auf einem Windows-System eine wertvolle Beweismittelquelle für den Computerforensiker dar.

Durch computerforensische Auswertung der Dateien im Prefetch-Ordner lassen sich gegebenenfalls wichtige Rückschlüsse auf genutzte Programme, DLL-Dateien, Steuerungsdateien, Gerätetreiber, den Zeitpunkt und die Häufigkeit der Programmnutzung sowie einzelne Benutzeraktivitäten ziehen. Der Umstand, dass sich gegebenenfalls auch Aussagen zu deinstallierten bzw ohne Installation lauffähigen Anwendungen treffen lassen, macht eine Analyse der Layout.ini-Datei besonders interessant.

Bei der Arbeit mit Prefetch-Dateien darf dennoch nicht übersehen werden, dass sich die Daten auf das gesamte System beziehen und deshalb Rückschlüsse auf einzelne Benutzeraktivitäten nur eingeschränkt möglich sind.

Anmerkungen:

1 Windows Prefetch File Format, Forensics Wiki, online abrufbar unter http://www.forensicswiki.org/wiki/Windows_Prefetch_File_Format (2. 8. 2012).

2 *Russinovich/Solomon*, Windows XP: Kernel Improvements Create a More Robust, Powerful, and Scalable OS, MSDN Magazine 12/2001, online abrufbar unter http://msdn.microsoft.com/en-us/magazine/cc302206.aspx (26. 7. 2012).

3 Bei einer Live-Analyse erfolgt der Zugang zum UserAssist-Key am einfachsten mit dem Registrierungseditor unter HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist. Bei einer *Post-mortem*-Analyse finden sich die Einträge in der Datei NTUSER.DAT im benutzerspezifischen Verzeichnis.

4 MiTec, Windows File Analyzer, online abrufbar unter http://www.mitec.cz/wfa.html (22. 10. 2012).

5 Nirosft, WinPrefetchView v1.12, online abrufbar unter http://www.nirsoft.net/utils/trans/winprefetchview_german.zip (22. 10. 2012).

6 Beim File Carving sucht die Software nach typischen Byte-Sequenzen, beispielsweise nach dem Anfang oder dem Ende von Dateien (Header und Footer) oder bestimmten Datenmustern spezieller Dateitypen. Werden ausreichend viele Fragmente einer gelöschten Datei identifiziert, so kann oftmals auf die gelöschte Datei geschlossen werden. Oftmals lässt sich diese teilweise oder sogar vollständig wiederherstellen (Quelle: Fraunhofer-Institut für Sichere Informationstechnologie).

7 *Kuhlee/Völzow*, Computer-Forensik Hacks (2012).

Korrespondenz:
Ing. Mag. Horst Greifeneder
Schenkelbachweg 32, 4600 Wels
Tel.: 07242 / 77715
Fax: 07242 / 77716
E-Mail: office@fds.at