Spezielle Bereiche des Datenträgers analysieren

Es gibt an vielen Stellen eines Betriebssystems Fundorte für Gebrauchsspuren oder Hinweise auf Auffälligkeiten. Diese Stellen sollten grundsätzlich aufgesucht und analysiert werden. Hierzu sollten alle Datenträgerbereiche in die Suche einbezogen werden. Im weiteren Verlauf dieses Kapitels werden Datenträgerbereiche vorgestellt, die nur mit Spezialwerkzeugen gelesen werden können. Dies betrifft besonders die scheinbaren Speicherbereiche, wie beispielsweise den File Slack, die Master File Table, den Alternate Data Stream, die Volume-Shadow-Kopien, die NTFS- und Registry-Transaktionslogs – einfach alles.

Viele der in diesem Kapitel genannten Analyseschritte lassen sich automatisieren oder sind in integrierten Forensik-Werkzeugen bereits als automatisierte Tasks enthalten. Häufig lassen sich diese Tätigkeiten auch über Skripte anstoßen und sollten als Erstes gestartet werden, wenn man als Ermittler noch keine genauen Vorstellungen von den zu erwartenden Ergebnissen hat. Die Auswertung dieser automatisierten Tasks kann dann oft die ersten Hinweise geben.

5.2 Analyse des File Slack

Der File Slack kann für den Ermittlungsverlauf wesentliche Informationen enthalten. Dies liegt in der Besonderheit einiger Dateisysteme begründet, die im Folgenden näher beschrieben werden. Wenn eine Datei erstellt wird, hängt ihre Größe vom Dateiinhalt ab. Aus Gründen der Effektivität wird diese Datei auf Datenträgern in sogenannten Datenblöcken gespeichert.

Sektoren

Diese Blöcke haben eine feste Länge und werden Sektoren genannt. Sektoren sind die kleinste Speichereinheit auf einem Datenträger. Diese Sektoren werden erstellt, wenn der Datenträger Low-Level-formatiert wird (durch den Hersteller oder über eine BIOS-Funktion).

Cluster

Alle Microsoft-Betriebssysteme speichern Daten in festen Blocklängen, die Cluster genannt werden. Cluster bilden sich unter Windows also aus Gruppen von Sektoren. Cluster werden bei der Formatierung des Datenträgers durch das Betriebssystem erstellt – die sogenannte High-Level-Formatierung. Wird also eine Datei auf einem Datenträger gespeichert, stimmt in den meisten Fällen der Inhalt der Dateien nicht exakt mit der Größe der Cluster überein. Der freie Platz innerhalb eines Clusters vom Ende der Datei bis zum Ende des letzten zugewiesenen Clusters wird als File Slack bezeichnet. Wenn die Datei geschrieben wird, füllt das Betriebssystem den File Slack mit zufälligen Daten auf.

Cluster-Größen variieren abhängig vom verwendeten Betriebssystem. Sie können sowohl aus einem als auch aus bis zu 128 Sektoren bestehen. Bei einigen älteren Windows-Systemen hängt dies z.B. von der Größe der logischen Partitionen ab. Größere Cluster haben größere File-Slack-Bereiche zur Folge, was aus Anwendersicht bei diesen Systemen Platzverschwendung bedeutet. Diese Designschwäche in einigen Dateisystemen hat für die forensische Ermittlung jedoch einen ernormen Nutzen, da gerade in diesen File Slacks wesentliche interessante Informationen und Datenspuren zu finden sind, die einem normalen Anwender in der Regel verborgen bleiben.

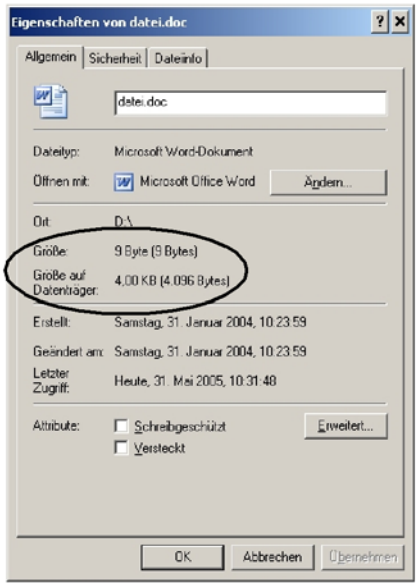

Abb. 5–1
Die Dateieigenschaften zeigen, dass diese 9 Byte große Datei 4 KB auf der Platte belegt: Der File Slack ist in diesem Fall also 4087 Byte groß.

RAM Slack

Der File Slack kann beispielsweise Fragmente des Hauptspeichers enthalten. Dies kann vorkommen, da DOS und einige Windows-Systeme (z.B. bei FAT) in 512 Byte große Blöcke schreiben. Sind nicht mehr genug Daten in der Datei enthalten, um den letzten Sektor dieser Datei vollends zu füllen, fügt Windows dem Rest dieses Sektors wahllos Daten aus dem Memory Buffer des Betriebssystems hinzu. Diese zufällig ausgewählten Daten werden auch als RAM Slack bezeichnet, da die Daten direkt aus dem RAM des Systems stammen. Dieser RAM Slack kann demzufolge Informationsfragmente enthalten, die seit dem letzten Boot des Computers entstanden sein können, z.B. während der Bearbeitung eines Dokuments oder des Besuchs einer Webseite. In Extremfällen können dies auch sensible Informationen sein, die nur während der Bearbeitung im RAM unverschlüsselt vorliegen, z.B. Pass-

wörter. Wenn der Computer mehrere Tage nicht heruntergefahren wurde, können die Daten, die im File Slack gefunden werden, auch aus verschiedenen Arbeitssitzungen stammen.

Drive Slack

RAM Slack lässt sich nur im letzten Sektor einer Datei finden. Werden zusätzliche Sektoren benötigt, um die Blockgröße des letzten Clusters für eine Datei zu erreichen, wird ein weiterer Slack gebildet. Dieser wird Drive Slack genannt und in den übrigen Sektoren gespeichert, die vom Betriebssystem benötigt werden, um den letzten Cluster einer Datei zu erstellen. Anders als der RAM Slack, der Bestandteile des Hauptspeichers enthält, werden beim Drive Slack Auffülldaten verwendet, die sich vorher bereits auf der Festplatte befunden haben. Diese Daten enthalten Fragmente von gelöschten Dateien oder Informationen aus unallozierten Bereichen des Datenträgers.

Der File Slack wird zu dem Zeitpunkt erzeugt, wenn die Datei auf den Datenträger geschrieben wird. Wird eine Datei unter Windows gelöscht, bleiben die Datenfragmente, die sich innerhalb des RAM oder File Slack befanden, in dem Cluster erhalten, der zuvor dem Ende der gelöschten Datei zugeordnet war. Die Cluster, die dieser Datei zugewiesen waren, werden vom Betriebssystem wieder freigegeben und bis zum nächsten Überschreiben mit Daten einer neuen Datei als unallozierter Bereich auf dem Datenträger erhalten.

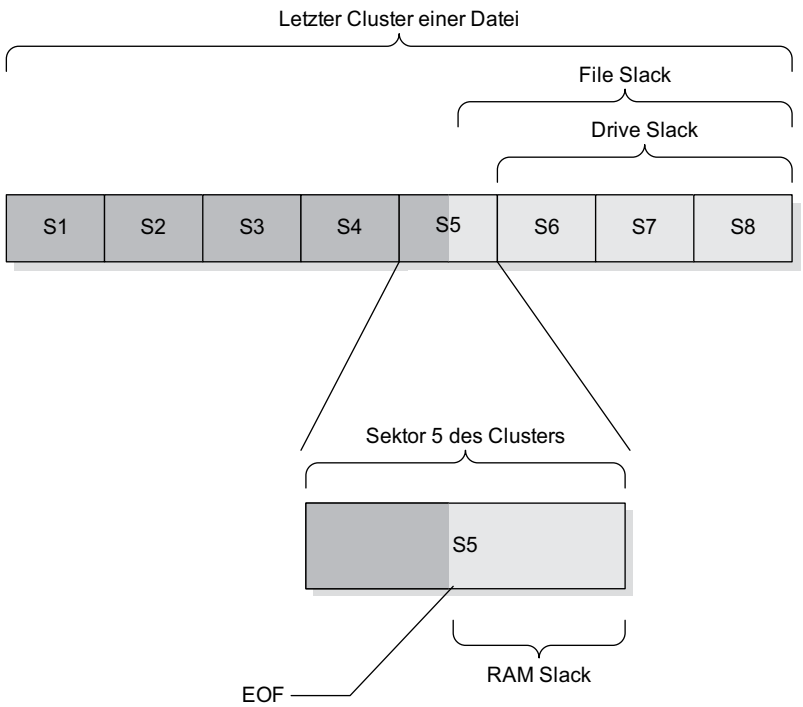

Abb. 5–2
File Slack = RAM Slack + Drive Slack

Master File Table

Die Master File Table (MFT) stellt das Herz der NTFS-Dateistruktur dar. Es handelt sich hierbei um eine spezielle Systemdatei, die eigentlich eine Art Datenbank ist, die die Informationen aller Dateien und Verzeichnisse des Laufwerks enthält. Wie jede andere Datenbank stellt die MFT eine Sammlung von Records dar. Für jede Datei und jedes Verzeichnis des NTFS-Laufwerks existiert mindestens ein Record. Jeder Record ist 1.024 Byte lang und enthält Informationen – auch Attribute genannt –, die dem Betriebssystem mitteilen, wie mit der zugehörigen Datei oder dem Verzeichnis umzugehen ist. Aus forensischer Sicht ist interessant, dass manchmal zusätzlich zu den Attributen auch Fragmente der zugehörigen Datei in der MFT abgelegt sind. In der MFT findet sich ebenfalls ein Zeitstempel, der das Datum der letzten Änderung der Attribute enthält.

MFT Slack

Ein weiterer interessanter Fakt ist, dass man bei diesen Daten keinen File Slack findet, da sie ja nicht in einem Cluster gespeichert werden, sondern innerhalb der MFT. Wenn die Daten allerdings kleiner als die 1.024 Byte eines Record sind, kann der überschüssige Bereich Fragmente von alten Dateien enthalten. Dieser Bereich wird MFT Slack genannt. Es ist wichtig zu wissen, dass dieser Bereich zusätzlich zum allgemein bekannten File Slack existiert und bei einer Analyse mit ausgewertet werden sollte.

Bedeutung für die Computer-Forensik

Aus Sicht der Computer-Forensik ist es wichtig, die Bedeutung des File Slack für die Ermittlung richtig einzuschätzen. Da der File Slack möglicherweise zufällige Hauptspeicherinhalte des Computers enthält, ist es durchaus denkbar, darin möglicherweise Login-Daten mit Passwörtern oder andere im Zusammenhang mit der Computeranwendung stehende sensible Informationen zu finden. Häufig finden sich im File Slack Informationen über die gerade im Hauptspeicher aktiven Programme und deren geöffnete Dateien oder auch gerade betrachtete Webseiten. Der File Slack kann weiterhin dahin gehend analysiert werden, herauszufinden, wofür der Computer in der vergangenen Zeit möglicherweise verwendet wurde. Diese Informationen könnten das fehlende Mosaiksteinchen in einer Ermittlung liefern.

Größe des File Slack

Es spricht für die Bedeutung dieser Analyse, dass bei einer gut gefüllten, größeren Festplatte mit ca. 80 GB der File Slack oft mehrere Hundert Megabyte Daten enthalten kann. Fragmente von vermeintlich gelöschten Textdokumenten oder E-Mails lassen sich dort finden. Es sollte außerdem noch erwähnt werden, dass sich der File Slack nicht nur auf Festplatten, sondern auch auf Disketten, Zip Drives oder anderen externen Datenträgern finden lässt.

Das immer noch häufig unter Linux verwendete Dateisystem ext2 speichert Daten in Blöcken und bildet auch Slack-Bereiche, wenn die

gespeicherten Dateien weniger als 1, 2 oder 4 KB der Dateisystem-Blöcke verwenden. Hier können ebenso wie unter Windows Datenfragmente gefunden werden, allerdings wird dazu übergegangen, echte Zufallswerte zum Auffüllen zu verwenden.

Im File Slack lassen sich vom Angreifer gelöscht geglaubte Informationen finden. Hierzu gehören Hauptspeicherinhalte oder bereits vorher auf dem System gelöschte Datenfragmente.

5.3 Timeline-Analysen

Zeitliche Zusammenhänge im Betriebssystem darstellen

Timeline-Analysen sind oft der erste Ansatzpunkt, um Vorgänge auf einem kompromittierten System nachzuvollziehen. Bei der Timeline-Analyse werden Zeitstempel ausgewertet, die sowohl im Dateisystem zu finden sind als auch durch diverse Artefakte des Betriebssystems oder Anwendungen erstellt werden. Der Ermittler möchte als Ergebnis der Timeline-Analyse wissen, zu welchem Zeitpunkt welches Ereignis auf dem System stattgefunden hat und welche Benutzerkennung dieses Ereignis ausgelöst hat. Die Ergebnisse der Timeline-Analysen können sehr gut für die Plausibilisierung von Angaben verwendet werden. Die große Anzahl von auswertbaren Zeitstempeln eines kompromittierten Systems hat einen hohen Beweiswert, da diese automatisch erstellt werden und deren vollständige Manipulation für den durchschnittlichen Täter oft recht komplex ist.

Es gibt unterschiedliche Fundorte für Zeitstempel, die in diesem Kapitel näher erläutert werden sollen. Zum einen finden sich im Dateisystem selbst ausführliche Zeitstempelinformationen, zum anderen enthalten die einzelnen im Dateisystem gespeicherten Dateien unterschiedliche Metadaten, z.B. aus Office-Dokumenten, die Rückschlüsse auf zeitliche Zusammenhänge geben. Die dritte Quelle sind Zeitstempel, die sich aus Anwendungen ermitteln lassen. Alle diese Zeitstempel müssen in Zusammenhang gebracht werden. Dabei ist es besonders wichtig zu wissen, in welchem Format und in welcher Zeitzone[3] die einzelnen Zeitstempel tatsächlich geschrieben werden, damit man nachher auch wirklich etwas damit anfangen kann. Gerade einige Office-Dateiformate speichern nicht durchgängige Zeitstempel in der korrekten Zeitzone ab. Unter Windows sollte unbedingt der entsprechende Registry Key ausgelesen werden, unter Unix/Linux und Mac OS die entsprechenden Konfigurationsparameter.

3. Ein Zeitzonenkonverter findet sich unter *http://www.timeanddate.com/worldclock/converter.html*.