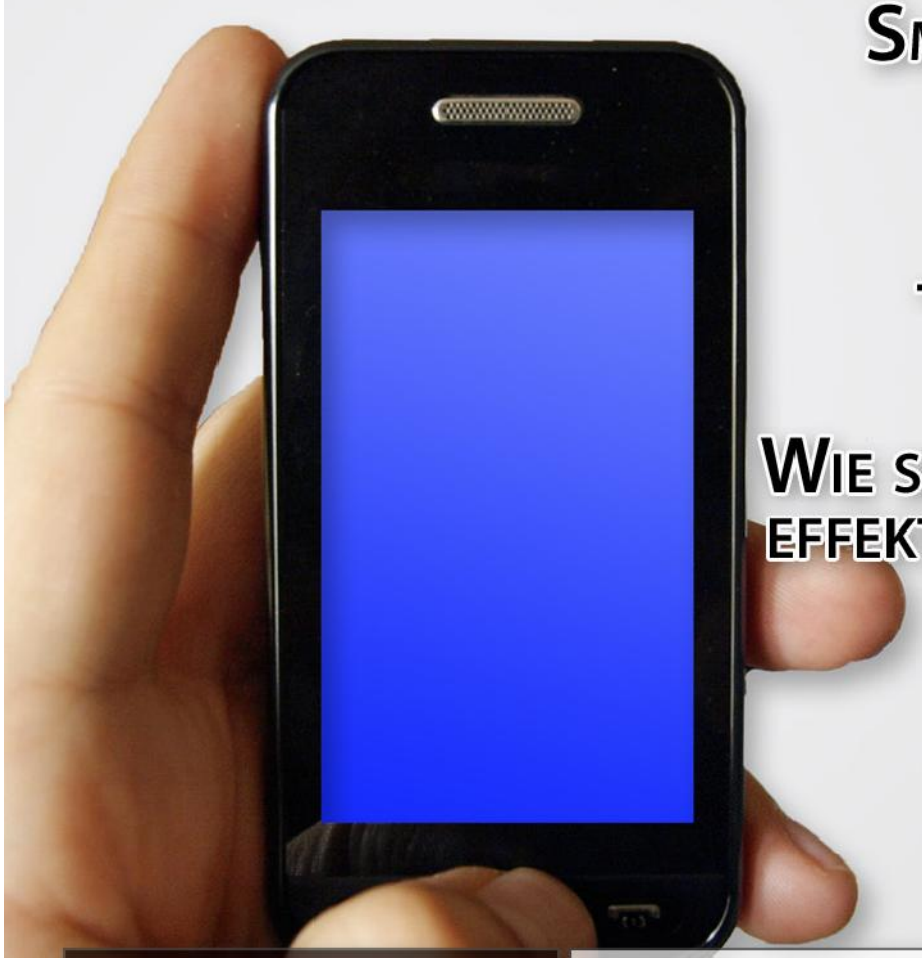
Hakin9

HARD CORE IT SECURITY MAGAZINE

Hakin9 Ausgabe 1/2012 Januar Monats-Online-Magazin

FIRMWARE VON SSDS



SMARTPHONE-FORENSIK

ONLINE-BEZAHLUNG – BEQUEM UND SICHER

WIE SICH ONLINE-HÄNDLER EFFEKTIV SCHÜTZEN KÖNNEN

DATENSICHERHEIT

PLUS **SSL-ZERTIFIKATE**

LIEBE HAKIN9 LESER!

das Hauptthema der Januar Ausgabe ist Firmware von SSDs.

Eine SSD ist ein Massenspeichergerät, genau wie eine Festplatte. SSD kommt ohne mechanische und bewegliche Teile aus - daher der Name „Solid State Drive“. In unserem neuen Artikel von Manuel Rundt erfahren Sie, welche speziellen Herausforderungen bei einer forensischen Sicherung aus IT-Forensischer Sicht von SSDs bestehen.

IT-Forensik war das beliebteste Thema in unserer Umfrage und wir finden diesen Artikel für hochinteressant.

Zu weiteren Highlights der aktuellen Ausgabe gehören: Smartphone-Forensik, Online-Bezahlung, Datensicherheit und SSL-Zertifikate. Sie können auch erfahren, wie sich Online-Händler effektiv schützen können.

Wir bedanken uns für Ihr Vertrauen in unsere Arbeit und wünschen Ihnen und Ihrer Familie einen guten Start ins neue Jahr!

Nehmen Sie bitte auch an unserer Umfrage teil, damit können wir interessantere Artikel für Sie vorbereiten. Umfrage finden Sie unter *http://hakin9.eu/*

Falls Sie Interesse an einer Kooperation hätten oder Themenvorschläge, wenden Sie sich bitte an unsere Redaktion.

Viel Spaß mit der Lektüre!
Karolina Sokołowska

hakin9

Firmware von SSDs
– IT-forensische Herausforderungen

Manuel Rundt

Mit der zunehmenden Verbreitung von Solid State Disks (SSDs) wird auch die IT-forensische Community vor neue Herausforderungen gestellt: zum Einen verhalten sich SSDs gänzlich anders, als traditionelle Festplatten. Zum Anderen kann die Firmware von SSDs auch ohne jegliche äußere Einflüsse autonom die auf der SSD enthaltenen Daten ändern.

IN DIESEM ARTIKEL ERFAHREN SIE...

- welche speziellen Herausforderungen bei einer forensischen Sicherung aus IT-Forensischer Sicht von SSDs bestehen und welche autonomen Prozesse durch die Firmware von SSDs gesteuert werden.

WAS SIE VORHER WISSEN SOLLTEN...

- wie eine forensische Sicherungen digitaler Beweismittel abläuft und welche spezielle forensische Hardware benutzt wird.

Solid State Disks erfreuen sich aufgrund ihrer Schnelligkeit und mit sinkenden Preisen immer größerer Beliebtheit. So haben moderne SSDs üblicherweise Datendurchsätze von mehr als 500 MB/Sekunde, während traditionelle Festplatten selten über 130 MB/Sekunde hinauskommen. Ein weiterer großer Vorteil von SSDs sind schnelle Zugriffszeiten im Mikrosekunden-Bereich während traditionelle Festplatten in der Regel um die 8 - 12 Millisekunden brauchen. Eigentlich müssten sich auch IT-Forensiker aufgrund der höheren Geschwindigkeit freuen, weil die benötigte Zeit zur Sicherung digitaler Beweismittel damit deutlich sinkt, gäbe es nicht neue, spezielle Herausforderungen, die die forensische Sicherung von SSDs schwieriger machen.

Die Funktionsweise von traditionellen Festplatten

Traditionelle Festplatten organisieren die auf ihnen enthaltenen Daten in elektromagnetischer Form auf rotierenden Magnetscheiben. Dabei werden die Daten normalerweise in Einheiten von 512 Bytes in einem sogenannten Sektor organisiert, die von einem Schreib- und Lesekopf auf die rotierenden Magnetscheiben, sogenannte „Platter“, geschrieben werden. Moderne Festplatten bieten heute auch anderen Sektorengrößen bis zu 4 KB, also 4096 Bytes, an [1].

Je Magnetscheibe („Platter“) gibt es zwei Lese- und Schreibköpfe, je einen für die Ober- und Unterseite. Moderne Festplatten enthalten zwischen einer und bis zu fünf Magnetscheiben. Die Daten werden dabei auf jeder Magnetscheibe in Spuren („Tracks“) organisiert [2].

Um Daten aus einem beliebigen Sektor zu lesen oder in diesen zu schreiben, wird die Adresse des Sektors auf die entsprechende Magnetscheibe, die Spur und den Sektor innerhalb dieser Spur umgewandelt, der zuständige Lesekopf auf die entsprechende Spur bewegt und die Daten dann ausgelesen bzw. mit dem Schreibkopf geschrieben. Sofern bereits Daten in dem Sektor vorhanden waren, werden diese beim Schreiben einfach überschrieben.

Die Adressierung und das Auslesen bzw. Schreiben der Daten erfolgt dabei durch den Controller der Festplatte. Dieser führt auch eine Liste mit defekten Sektoren und leitet Zugriffe auf diese transparent für den Benutzer und das Betriebssystem auf speziell reservierte Sektoren um. Welche Sektoren frei sind oder nicht, weiß der Controller dabei nicht. Diese Aufgabe übernimmt das Betriebssystem, das seine Daten in einem Dateisystem organisiert. Dabei werden in der Regel mehrere Sektoren zu einem sogenannten Cluster zusammengefasst. Bekannte Dateisysteme sind z.B. FAT32 oder das heute bei Windows übliche NTFS. Unter dem Betriebssystem Linux sind dies beispielsweise EXT2/EXT3/EXT4 und ReiserFS oder unter MacOS das Dateisystem HFS+. Auf die Arbeitsweise und Funktionen der

Dateisysteme soll hier zur Vereinfachung nicht eingegangen werden.

Da es bei traditionellen Festplatten nicht notwendig ist, vorhandene Daten vor dem Überschreiben zu löschen, sind die meisten Dateisysteme faul und markieren die Sektoren von gelöschten Dateien einfach als frei, ohne dabei die Daten auf der Festplatte zu überschreiben. Dank dieses Umstandes können IT-Forensiker daher in der Regel auch einen Großteil der gelöschten Dateien wieder rekonstruieren und auswerten, selbst wenn die Festplatte beispielsweise neu formatiert wurde.

Die Funktionsweise von Solid State Disks

Solid State Disks organisieren die auf ihnen enthaltenen Daten in transistorbasierten Speicherzellen, überwiegend sogenannte NAND-Transistorzellen, wie sie beispielsweise auch bei USB-Sticks Anwendung finden. Die Daten werden dabei üblicherweise in Blöcken von 512 KB organisiert, die in sogenannte Seiten („Pages“) von 4KB unterteilt sind [3].

Es gibt somit keine rotierenden Teile oder magnetische Scheiben, daher auch der Begriff „Solid State“. Die Daten werden in Transistorzellen gespeichert, indem in den Zellen elektrische Spannung gespeichert wird. Die Transistorzellen können dabei ihren Zustand auch ohne die Zufuhr von Strom für mehrere Jahre halten. Die Transistorzellen können dabei in etwa 10 Mikrosekunden ausgelesen werden, was ungefähr 1.000 Mal schneller ist, als bei traditionellen Festplatten mit Magnetscheiben. Das Schreiben von Daten ist dabei in der Regel mit etwa 100 Mikrosekunden deutlich langsamer als das Lesen, aber immer noch etwa 100 Mal schneller als bei traditionellen Festplatten [4].

Um Daten aus einem beliebigen Sektor zu lesen, wird die Adresse des Sektors auf die entsprechende Speicherzelle, den Block und die Seite umgewandelt und elektrisch ausgelesen. Die Adressierung und das Auslesen bzw. Schreiben der Daten erfolgt dabei durch den Controller der SSD. Dieser führt ebenfalls eine Liste über defekte Sektoren und leitet Zugriffe auf diese transparent für den Benutzer und das Betriebssystem auf andere Sektoren um.

Um Daten in einen beliebigen Sektor zu schreiben müssen jedoch zunächst die zuvor gespeicherten Daten gelöscht werden, bevor neue Daten geschrieben werden können. Das Löschen der vorhandenen Daten dauert dabei im Vergleich zum Lesen und Schreiben recht lange, nämlich etwa 10 Millisekunden, also etwa 100 Mal langsamer als der eigentliche Schreibvorgang und in etwa so lange wie bei einer traditionellen Festplatte [5].

Eine weitere Eigenschaft der SSDs ist, dass die Speicherzellen nicht beliebig oft geschrieben werden können, weil diese nach einer gewissen Anzahl an Schreibzyklen kaputt gehen. Bei frühen SSDs waren dies etwa 10.000 Zyklen. Moderne SSDs halten heute meistens mehr als 100.000 Zyklen aus.

Industrielle SSDs schaffen sogar noch deutlich mehr, etwa 1 Mio. Zugriffe [3]. Um dieser Abnutzung („Wear“) einzelner Speicherzellen zu begegnen, führt der Controller der SSDs darüber Buch, welche Speicherzellen wie oft geschrieben werden und leitet Datenblöcke von Dateien, die häufig geschrieben werden wie z.B. Logdateien, daher bei jeden erneuten Schreiben auf andere Speicherzellen um, um die vorhandenen Speicherzellen gleichmäßig zu nutzen („Wear Levelling“). Diese Umleitung erfolgt dabei transparent für Benutzer und Betriebssystem durch den sogenannten Flash Translation Layer („FTL“) im Controller [6].

Diese Technik führt zu einem weiteren interessanten Nebeneffekt, nämlich dem, dass ein sicheres Löschen von Dateien nicht mehr mit absoluter Gewissheit durchgeführt werden kann, da die Daten aus dem Überschreiben der Datei durch den Flash Translation Layer mit einiger Sicherheit in einer anderen Zelle gespeichert werden, als die ursprüngliche Datei und diese somit physisch nicht überschrieben wird [7].

Da das Schreiben von Daten in Zellen, die noch einen Inhalt haben, sehr langsam ist, wurde eine weitere Optimierung in die Controller integriert, nämlich die, dass die Controller zum Löschen freigegebene Blöcke oder Blöcke, die überschrieben werden sollen, autonom im Betrieb löschen, während die neuen Daten durch den Flash Translation Layer in andere Speicherzellen umgeleitet werden. Dieser Prozess wird dabei als „Garbage Collection“ (auf Deutsch „Müllsammlung“) bezeichnet. Dieser Prozess wird vom Controller der SSD vollautonom vorgenommen und startet meist nach einer gewissen Zeit nachdem die SSD Stromzufuhr erhält – in verschiedenen Experimenten australischer IT-Forensiker mit einer SSD startete dieser Prozess meist nach etwa 180 Sekunden nach Start der SSD [5]. Die Garbage Collection-Prozesse sind dabei von Hersteller zu Hersteller verschieden und die verwendeten Algorithmen gehören zu den Betriebsgeheimnissen und sind daher bisher nicht veröffentlicht.

Der Garbage Collection-Prozess kann von außen nicht abgeschaltet oder aufgehalten werden. Selbst der Betrieb der SSD an einem externen Write-Blocker schaltete bei den Experimenten der australischen IT-Forensiker diesen Prozess nicht ab. Jedoch kann aber dank eines Schalters für die externe Stromversorgung die Zeitspanne zwischen Einschalten der SSD und dem Start der Sicherung der digitalen Beweismittel verkürzt werden und so ein kurzer

Literatur

[1] Western Digital, Advanced Format Technology, z.B. in der Baureihe WD20EARS *http://www.wdc.com/wdproducts/library/WhitePapers/DEU/2579-771430.pdf*
[2] Wikipedia *http://de.wikipedia.org/wiki/Cylinder_Head_Sector*
[3] Wikipedia, Solid State Drives *http://de.wikipedia.org/wiki/Solid-State-Drive*
[4] Tomshardware.de - Zugriffszeiten SSDs *http://www.tomshardware.de/6gb-s-ssd-hdd,testberichte-240539-6.html*
[5] „Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery?", Graeme B. Bell, Richard Boddington in Journal of Digital Forensics, Security and Law, Vol. 5(3)
[6] Wikipedia, Flash Translation Layer *http://en.wikipedia.org/wiki/Flash_Translation_Layer*
[7] winfuture.de - Sichere Daten-Löschung von SSDs ist ein Problem *http://winfuture.de/news,61528.html*
[8] Sicherung digitaler Beweismittel, Manuel Rundt, Martin Wundram, Alexander Sigel in Hakin9, Ausgabe 12/2011

Vorsprung vor dem Start eines Garbage Collectors gewonnen werden [5].

Herausforderungen für IT-Forensiker

Diese vollautonomen Prozesse stellen die IT-Forensik vor mehrere schwierige Aufgaben: zum Einen wird es in der Regel nicht mehr so einfach möglich sein, gelöschte Dateien zu rekonstruieren, weil diese bereits durch den Garbage Collector im laufenden Betrieb gelöscht worden sein können. Zum Anderen bedeutet die vollautonome Änderung der gespeicherten Daten durch den Controller der SSD selbst auch, dass ein einmal erstelltes Abbild der SSD wahrscheinlich nicht mehr verifiziert werden kann, da sich in diesem Fall zwar nicht das forensische Abbild der SSD ändert, dafür aber das Originalmedium. Somit hätte das Abbild einer SSD vor Gericht den Makel, dass ein Nachweis über die Unversehrtheit der Daten bzw. der Nachweis, dass keine Manipulationen stattgefunden haben, nicht mehr geführt werden kann. Somit könnte lediglich nachgewiesen werden, dass keine nachträglichen Manipulationen an dem zu einem bestimmten Zeitpunkt erstellten Abbild stattgefunden haben, wenn die Prüfsumme („Hash") nachweislich zum Zeitpunkt der Erstellung von einer externen Institution mit einem Zeitstempel signiert wird. Hier gibt es verschiedene Anbieter, die teilweise kostenlos, meistens aber gegen Geld einen solchen Service übernehmen.

Da sich die Hersteller von SSDs wahrscheinlich nicht dazu überreden lassen werden, für die IT-Forensiker einen Befehl zur Abschaltung der autonom arbeitenden Garbage Collection einzubauen, wird eines der wichtigsten IT-forensischen Hauptgebiete zur Gewinnung von digitalen Beweisen, nämlich die Suche nach Beweismitteln in den gelöschten Datenbereichen einer Festplatte, zukünftig wohl nur eingeschränkt zur Verfügung stehen. Dies betrifft in gleichem Maße auch die komplette Branche der Datenrettungsunternehmen, die die Daten einer versehentlich gelöschten oder formatierten SSD ebenfalls nicht mehr werden rekonstruieren können, sofern die SSD seit dem Vorgang der Löschung noch für einige Zeit in Betrieb war.

Bisher hat die IT-forensische Community auch noch keine Lösungen für diese Herausforderungen gefunden. Eventuell muss sich die IT-Forensik im Fall von SSDs, wie auch bei der Sicherung von volatilen Daten – wie beispielsweise dem Hauptspeicher – von ihrem obersten Gebot verabschieden, durch das Sichern der digitalen Beweismittel keine Veränderung an den zu untersuchenden Daten zu verursachen [8]. Eventuell müssen hier auch Gerichtsentscheidungen abgewartet werden, die eine Zulässigkeit von digitalen Beweismitteln klären, deren Manipulationsfreiheit und Unversehrtheit nicht mehr oder nur eingeschränkt nachgewiesen werden kann.

MANUEL RUNDT

Manuel Rundt, Dipl.-Kfm. ist Geschäftsführer der IT Compliance Systeme GmbH. Er beschäftigt sich bereits seit mehr als 9 Jahren mit dem Thema Wirtschaftskriminalität insbesondere IT Forensik und Incident Response.
manuel.rundt@compliance-systeme.de