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

Die forensische Datensicherung nicht flüchtiger Speichermedien

1. Einleitung

Die zunehmende Verbreitung und allgegenwärtige Nutzung von Informationstechnologie hat zu vermehrten cyberkriminellen Handlungen auf oder mit Computersystemen geführt. Bei der Aufarbeitung rechtlich relevanter Vorfälle spielt die gerichtsfeste Beweissicherung der gespeicherten Daten eine zentrale Rolle. Der überwiegende Teil der beweisrelevanten Daten ist in der Regel auf physischen, nicht flüchtigen Speichermedien wie elektromagnetischen Festplatten gespeichert.

Der Beitrag richtet sich an informationstechnisch versierte Leser mit grundlegendem Interesse an forensischer Datensicherung. Nachfolgend werden die Grundlagen elektromagnetischer Festplatten, Methoden und Dateiformate zur forensischen Datensicherung beschrieben und es wird auf mögliche Fallstricke bei der digitalen Beweismittelsicherung verwiesen.

2. Grundlagen elektromagnetischer Festplatten

2.1. Allgemeines

Die elektromagnetische Festplatte (Harddisk) zählt zu den am häufigsten verwendeten Speichermedien der Informationstechnik. In der Regel sind fast alle in der Praxis verwendeten Rechnertypen mit mindestens einer Harddisk ausgestattet. Aktuelle Festplatten verfügen über bis zu 4 Terabyte Speicherkapazität und speichern Daten über mehrere Jahre.

Das Speichern der Daten erfolgt durch gezielte Magnetisierung kleinster Segmente auf ferromagnetisch beschichteten Scheiben. Die Scheiben sind in konzentrischen Kreisen (Spuren) organisiert, welche wiederum in mehrere Sektoren (Blöcke) unterteilt sind. Die Sektoren sind meist für eine Speicherkapazität von 512 Byte eingerichtet. Zur Adressierung der Speicherbereiche werden mehrere Sektoren zu einem Cluster zusammengefasst.

2.2. Partitions und Dateisysteme

Aus Sicht des Betriebssystems können Festplatten durch Partitionierung in mehrere logische Bereiche unterteilt werden. Man kann sich Partitions als virtuelle Laufwerke vorstellen, die durch das Betriebssystem als eigene Speichermedien dargestellt werden.

Zu beachten ist, dass durch entsprechende Partitionierung des Speichermediums freie Speicherplätze zwischen den Partitions angelegt werden können, die über den Dateimanager des Betriebssystems, zB Windows Explorer, nicht abrufbar sind und als etwaiges Datenversteck dienen können.

Dateisysteme wiederum dienen zur Verwaltung, Verarbeitung und Speicherung der Daten innerhalb einer Partition. Ein Dateisystem bildet somit einen Namensraum. Alle Dateien (oder dateiähnlichen Objekte) sind so über eine eindeutige Adresse (Dateiname inklusive Pfad oder URI) – innerhalb des Dateisystems – aufrufbar. Der Name einer Datei und weitere Informationen, die den gespeicherten Daten zugeordnet sind, werden als Metadaten bezeichnet.[1]

Gängige Dateisysteme führen ein Verzeichnis mit den belegten (allokierten) und unbenutzten (nicht allokierten) Sektoren auf dem Datenträger. Für jede Datei werden neben dem Namen unter anderen die Dateigröße, verschiedene Zeitdaten und die belegten Speicheradressen verwaltet.

Für unterschiedliche Betriebssysteme gibt es spezielle Dateisysteme wie NTFS und FAT32 bei Microsoft Windows sowie Extended Filesystem (ext3, ext4) bei Linux-basierten Systemen.

3. Methoden zur forensischen Datensicherung

Die forensische Datensicherung erfolgt mit dem obersten Ziel, die Integrität der digitalen Beweismittel zu bewahren. Insbesondere dürfen bei der forensischen Datensicherung keine auf der Festplatte befindlichen Daten verändert, gelöscht oder übersehen werden.

In der Regel steht für die forensische Datensicherung ein Computersystem im stromlosen Zustand (*post mortem*) zur Verfügung. Das System enthält eine oder mehrere Festplatten, deren gesamte Datenmenge für gerichtliche Beweismittelzwecke zu sichern ist.

Stand der Technik bei der forensischen Beweismittelsicherung ist das Imaging der Festplatte. Beim Imaging wird ein exaktes Duplikat der zu sichernden Festplatte erzeugt. Der Prozess erfolgt auf Sektorenebene und kopiert Bit für Bit den Inhalt aller allokierten und nicht allokierten Sektoren auf ein Sicherungsmedium.

Der grundsätzliche Ablauf einer forensischen Datensicherung erfolgt in einer vordefinierten Reihenfolge:[2]

- Hashwert-Berechnung der zu sichernden Festplatte;
- Imageerstellung durch bitweise Sicherung der Daten in den allokierten und nicht allokierten Sektoren der Festplatten;
- Hashwert-Berechnung des Images;
- Feststellung der Integrität durch Vergleich der beiden Hashwerte.

Nach dem Integritäts-Check sollte die Originalfestplatte zum Schutz vor nachträglichen Veränderungen an einem sicheren Ort verwahrt werden.

3.1. Methoden zur Sicherung von Festplattendaten

Zur Sicherung der Beweismitteldaten werden in der Regel forensische Tools wie das Linux-Programm dcfldd sowie herstellereigene Programme wie LinEn oder FTK Imager eingesetzt.

Das Tool dcfldd ist eine für computerforensische Zwecke erweiterte Version des Linux-Programms dd.[3] LinEn und FTK Imager sind Programme führender Hersteller von Forensik-Softwarepaketen.

Zur Sicherung der Festplattendaten unterscheidet man verschiedene Methoden wie Imaging mittels Datensicherungssystems, Imaging im Originalsystem und Imaging über das Netzwerk.

3.2. Imaging mittels Datensicherungssystems

Zur Sicherung der Festplatte wird diese aus dem Originalsystem ausgebaut und über entsprechende Schnittstellenadapter an ein Datensicherungssystem angeschlossen. Um beim Imaging eine versehentliche Änderung der Daten ausschließen zu können, sollte die zu sichernde Festplatte über einen Hardware-Writeblocker an das Datensicherungssystem angeschlossen werden. Dieses Gerät verhindert mögliche Modifikationen der Originaldaten physisch, sodass die Integrität der Daten sichergestellt ist.

3.3. Imaging im Originalsystem

Bei dieser Vorgehensweise wird an das Originalsystem über USB, Firewire oder eSATA eine externe Festplatte angeschlossen. Das Originalsystem wird dann mit einer Live-CD vom CD-Laufwerk gestartet. Die Live-CD bootet ein eigenes Betriebssystem, meist auf Linux-Basis. Spezialisierte Live-CD-Distributionen wie Helix haben eine große Auswahl an nützlichen Forensik-Werkzeugen an Bord.[4]

Bei der Sicherung im Originalsystem ist unbedingt darauf zu achten, dass keinerlei Modifikationen der Beweismitteldaten erfolgen. In der Regel wird beim Starten über die Live-CD die im Gerät befindliche Festplatte nicht in das System eingebunden und somit ein ungewollter Zugriff auf die Harddisk verhindert.

Diese Vorgehensweise wird häufig eingesetzt, wenn das Originalsystem über spezielle Hardware verfügt, die zum Anschließen des verwendeten Datenträgers nötig ist. Es kann sich dabei zB um einen Raid Controller handeln, über den mehrere Festplatten zusammengeschlossen sind. Voraussetzung für diese Sicherungsart ist die Unterstützung der Hardware durch die verwendete Linux-Distribution.

3.4. Imaging über das Netzwerk

Bei der Sicherung über das Netzwerk wird das Originalsystem ebenfalls von einer Linux-Live-CD gebootet. Mit dem Programm netcat wird eine TCP/IP-Verbindung zum Zielcomputer hergestellt. Über die Netzwerkverbindung werden die beispielsweise mit dem Tool dd gesicherten Daten direkt auf dem Zielcomputer übertragen und dort als Image gespeichert. Auf dem Zielcomputer wird dazu das Programm netcat gestartet und für einen bestimmten Port konfiguriert. Das Programm lauscht auf diesem Port und schreibt alle ankommenden Daten in eine Datei.[5]

3.5. Integritätsnachweis der Sicherungskopie

Die Echtheit des Image wird durch die Erstellung von Prüfsummen (Hashes) der Originaldaten und des Duplikats sichergestellt. Als Hashverfahren kommen SHA-1 oder MD5 zum Einsatz. Sind die ermittelten Prüfsummen für die beiden Datenmengen identisch, stimmen die gesicherten Daten hundertprozentig mit dem Original überein.

4. Dateiformate zur digitalen Beweismittelsicherung

Für die digitale Beweismittelsicherung kommen mehrere Dateiformate in Frage. Sie unterscheiden sich im Wesentlichen durch Art und Weise der Datenspeicherung, die verwendeten Methoden zur Integritätssicherung und die Verwendung von fallspezifischen Metadaten.

4.1. Raw Image (dd, ddclfd)

Eine Raw-Image-Datei ist eine bitweise Kopie der Originaldaten ohne Hinzufügungen und Löschungen. Die Dateien beinhalten keine Metadaten und werden mittels Linux-Programmen wie dd oder ddclfd erstellt. Raw-Image-Dateien können in der Regel in jedes marktgängige Forensik-Programm zur weiteren Analyse importiert werden.

Der Nachteil eines Raw Images liegt darin, dass es nicht komprimiert werden kann und keine zusätzlichen Informationen in der Datei gespeichert werden können. Das Erstellen der Prüfsummen sowie die Integritätsprüfung müssen manuell durchgeführt werden.[6]

4.2. Electronic Witness Format (EWF)

Das Expert Witness Compression Format (EWF) ist das grundlegende Dateiformate für spezialisierte Forensik-Anwendungen wie Encase, Forensic Tool Kit oder das X-Ways Forensics.[7]

Das Dateiformat dient zur komprimierten Speicherung von Daten, auf die auch ohne vollständige Dekomprimierung zugegriffen werden kann. Dabei werden jeweils nur ein-

zelne Datenblöcke in der Größe von 32 Kilobyte komprimiert und im Image des Datenträgers gespeichert. Bei der Analyse der Daten kann gezielt und schnell auf bestimmte Datenbereiche zugegriffen werden, ohne das ganze Image dekomprimieren zu müssen. Zusätzlich kann ein Image auf mehrere Dateien (Segmente) aufgeteilt werden.

In seiner Modifikation des EWF-Dateiformats, dem herstellereigenen Evidence File Format (E01), hat Encase für eine erhöhte Integritätssicherung gesorgt, indem beim erzeugten Image Hashwerte für jeden 32K-Block und den gesamten gespeicherten Datenbestand erzeugt werden. Somit erkennt das Programm jedwede Veränderung des ursprünglichen Datenbestands sofort und zeigt dem Benutzer eine entsprechende Warnmeldung an.

Praktisches Software-Tool zur Erstellung von Images im Evidence File Format ist LinEn, welches vom Hersteller kostenfrei unter Linux zur Verfügung gestellt wird und unter anderem in der Forensik-Software Helix3Pro enthalten ist.

4.3. Advanced Forensics Format (AFF)

Ähnlich wie beim EWF-Dateiformat handelt es sich auch beim Advanced Forensics Format (AFF) um eine komprimierte Speicherung der Beweismitteldaten. AFF ist ein freies Dateiformat und unterstützt zusätzlich den LZMA-Algorithmus, der zwar langsamer ist, als die beim EWF verwendete Zlib-Komprimierung, aber dafür deutlich bessere Komprimierungsraten erzielt.

Datensicherungen im AFF können unter anderem mit den Programmen Aimage, Guymager oder FTK Imager erstellt werden.

5. Fallstricke bei der digitalen Beweismittelsicherung

Bei der Beweismittelsicherung von Festplatten sind insbesondere verschiedene ATA-Features zur Speichergrößenmanipulation, ATA-Security-Features und die Verschlüsselung der Festplatte bzw einzelner Festplattenbereiche potenzielle Hindernisse, die es im Einzelfall nach Möglichkeit zu berücksichtigen bzw überwinden gilt.

5.1. ATA-Features zur Speichergrößenmanipulation

Das Schnittstellenprotokoll ATA (Advanced Technology Attachment) bietet unterschiedliche Möglichkeiten wie Host Protected Area (HPA) und Device Configuration Overlay (DCO) zur Manipulation der zugänglichen Festplattenbereiche.

HPA ist ein speziell reservierter Bereich auf der Festplatte zur Speicherung von Daten außerhalb des normalen Dateisystems. Dieser Bereich wird in Windows vor dem Dateisystem – somit auch vor Programmen zur Formatierung oder Partitionierung – versteckt und ist deshalb für dieses nicht sichtbar bzw nutzbar.

DCO ermöglicht Herstellern die willkürliche Festlegung von Speichergrößen für Festplatten. Genutzt wird diese Möglichkeit, um größere Festplatten „künstlich“ zu verkleinern. HPA und DCO können parallel auf einer entsprechend konfigurierten Festplatte existieren.

Forensisch ist nicht nur interessant, dass in den beiden genannten Bereichen größere Datenmengen versteckt werden können, sondern auch, dass HPA und DCO durch Imaging-Programme nicht immer korrekt identifiziert werden. Geben Hersteller von Imaging-Tools an, dass sie HPA finden und auch für eine spätere Analyse aufzeichnen können, so gibt es teilweise bei DCO keine genaueren Angaben.

Gerade bei einem konkreten Verdacht auf den Besitz von strafrechtlich relevanten Daten ist eine Untersuchung der Festplatte auf die Existenz von HPA- bzw DCO und gegebenenfalls darin versteckten Daten unbedingt erforderlich.

5.2. ATA-Passwort

Die meisten aktuell auf dem Markt verfügbaren Festplatten verfügen über einen 32 Byte langen Passwortschutz mit General- und Nutzerschlüssel. Sind General- und Nutzschlüssel unbekannt, kann nicht auf die Daten der Festplatte zugegriffen werden. Die Zugangssperre kann, wenn überhaupt, nur mit Hilfe des Festplatten-Herstellers beseitigt werden.

5.3. Verschlüsselung

Das größte Hindernis bei der physischen Auswertung von Festplatten bieten Verfahren, welche die gesamte Systemplatte verschlüsseln und vor dem Booten der Festplatte eine Zugriffskontrolle durchführen. Die besondere Tücke dieses Verfahrens liegt darin, dass bei einer *Post-mortem*-Untersuchung der sicher verschlüsselten Festplatte *de facto* keine Möglichkeit besteht, das Kennwort zu ermitteln, und somit eine forensische Auswertung der Daten unmöglich ist.[8]

Anmerkungen:

1 Seite „Dateisystem“ in Wikipedia – Die freie Enzyklopädie (Bearbeitungsstand: 20. 1. 2011, 15:54 UTC), http://de.wikipedia.org/w/index.php?title=Dateisystem&oldid=84165998 (abgerufen 27. 1. 2011, 12:44 UTC).

2 *Geschonneck*, Computer-Forensik[3] (2008).

3 Seite „dcfldd“, http://dcfldd.sourceforge.net/ (abgerufen 27. 1. 2011).

4 Seite „e-fense: Cyber Security & Computer Forensics Software“, http://www.e-fense.com/products.php (abgerufen 20. 1. 2011).

5 *Giacobbi*, The GNU Netcat project (2006), http://netcat.sourceforge.net/.

6 *Carrier*, File System Forensic Analysis (2005).

7 *Metz*, Expert Witness Compression Format specification, http://sourceforge.net/projects/libewf/files/documentation/EWF%20file%20format/Expert%20Witness%20Compression%20Format%20%28EWF%29.pdf/download (abgerufen 8. 2. 2011).

8 *TrueCrypt Foundation* (Hrsg), System Encryption, http://www.truecrypt.org/docs/?s=system-encryption.

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