Computer-Forensik mit Open-Source-Tools

[05.04.2004 15:35]

Artikel aus c't 7/2004, S.200

Holger Morgenstern

Digitale Autopsie

Computer-Forensik mit Open-Source-Tools

Nach einem Sicherheitsvorfall gilt es, Beweismittel zu sichern. Dabei kommt es nicht nur darauf an, Spuren zu entdecken - man muss sie auch gerichtsverwertbar sicherstellen. Bei beiden Aufgaben leisten Open-Source-Tools unschätzbare Dienste.

Wie reagiert man am besten auf einen Sicherheitsvorfall im Computerbereich? Diese Frage stellen sich in letzter Zeit immer mehr Firmen, Organisationen und auch Privatpersonen. Ist auch nur im Entferntesten damit zu rechnen, dass der Vorfall in einem Rechtsstreit oder in einer Strafverfolgung eine Rolle spielen könnte, muss besonders überlegt gehandelt werden, um die Beweislage nicht zu verschlechtern. Leider werden dabei oft aus Unwissenheit, in guter Absicht oder auch in Panik viele Fehler gemacht, die eventuelle Spuren der kriminellen Aktionen unwiederbringlich vernichten oder ihre Verwendung in einem Gerichtsprozess verhindern.

Mit dieser Art der Beweismittelsicherung beschäftigt sich die so genannte Computer-Forensik. Analog zu anderen Bereichen der Kriminalistik gilt es auch hier, möglichst viele relevante Beweise zu sammeln, zu analysieren, zu rekonstruieren und diese dann neutral, nachvollziehbar und gerichtstauglich darzustellen.

Keine Hexerei

Viele sehen in der Computer-Forensik eine moderne Form der schwarzen Magie, die vermeintlich vernichtete Daten wieder rekonstruiert oder entschlüsselt. Informationen, von denen man gar nicht wusste, dass sie existieren, kommen plötzlich zum Vorschein und selbst gebrauchte Kopierer geben geheime Dokumente preis. Doch so erstaunlich manche Ergebnisse auch aussehen mögen - auch der beste Forensiker kann keine Daten herbeizaubern, die physikalisch nicht mehr vorhanden sind. Und noch eine kleine Warnung vorweg: Computer-Forensik erfordert einiges an Systemkenntnis und man sollte schon ganz genau wissen, was man tut. Ein paar vertauschte Parameter und schon werden einige der hier vorgestellten Werkzeuge schnell zu Anti-Forensik-Tools. Nicht zuletzt müssen bei einer Analyse natürlich immer auch Datenschutzaspekte und Persönlichkeitsrechte berücksichtigt werden.

Neben den Geheimdiensten und Strafverfolgungsbehörden, die normalerweise ihre eigene Forensik betreiben, haben vor allem Datenrettungsunternehmen die Computer-Forensik für sich entdeckt und lassen sich dabei nicht so gerne in die Karten schauen. Auf dem internationalen Markt gibt es einige renommierte kommerzielle Hard- und/oder Softwarepakete wie Encase, SafeBack oder SMART, die oft auch im Bereich der Strafverfolgung zum Einsatz kommen.

Daneben existieren aber auch eine Vielzahl von Open-Source-Tools, die sich entweder im Computer-Forensik-Bereich einsetzen lassen oder sogar speziell dafür entwickelt wurden. Gerade was die Verwendung im Gerichtsumfeld anbetrifft, haben Open-Source-Anwendungen klare Vorteile. Beweisketten müssen in rechtsstaatlichen Verfahren neutral und jederzeit von Dritten überprüfbar dargestellt werden. Beim Einsatz von Tools mit offen zugänglichem Quellcode ist dies auf jeder Ebene möglich, bei Closed-Source-Anwendungen kann man dagegen nur auf den guten Ruf des Herstellers vertrauen oder Black-Box-Tests durchführen, was aber kaum die letzte Sicherheit geben dürfte. Offene Quellcodes bieten Forensikern zudem einen nicht zu unterschätzenden Lerneffekt und erleichtern eine schnelle Reaktion auf neue Anforderungen durch individuelle, vom Experten selbst durchführbare Anpassungen der Werkzeuge.

Dr. Tux

Schon ein ganz normales Linux hat Werkzeuge an Bord, die Imaging, Authentifizierung, Löschen und Durchsuchen von diversen Speichermedien erlauben. Die Eigenschaft von Linux, alles einschließlich Hardware als Datei zu behandeln, bietet im forensischen Umfeld ad hoc sehr weit reichende Kontroll- und Einsatzmöglichkeiten. Das reicht von Zugriffsbeschränkungen, der Replikation über Plattformgrenzen hinweg bis hin zu der Art, wie das Betriebssystem mit den betreffenden Medien interagiert. Der letzte Aspekt ist besonders wichtig, da in der Computer-Forensik wie in der übrigen Kriminologie als oberstes Gebot gilt, dass Beweise nicht verändert werden dürfen. Normalerweise sind zum Beispiel bei der Untersuchung von Festplatten spezielle Hard- oder Software-Write-Blocker nötig - unter Linux reicht ein einfaches Mounten im Read-only-Modus.

Linux unterstützt schon von Haus aus eine sehr große Zahl von Dateisystemen. Der Einsatz von Loopback Devices, das Um- und Weiterleiten von Standard Input und Output sowie die Möglichkeit, Prozesse und Kommandos zu überwachen und zu protokollieren, sind weitere Pluspunkte.

Da die nach einem Sicherheitsvorfall zu untersuchenden Systeme sowie deren Betriebssysteme in der Regel nicht mehr vertrauenswürdig sind - Systemkomponenten könnten ausgetauscht oder manipuliert worden sein -, sollten diese nicht für eine forensische Untersuchung benutzt werden. Linux kann auch in diesem Bereich glänzen, da es relativ einfach möglich ist, bootfähige Medien mit integrierten, statisch gelinkten Tool-Sets zu erstellen. Das Knoppix auf der Heft-CD in c't 4/04 ist ein idealer Ausgangspunkt zur Sicherung von Beweismitteln, da man damit den Festplatteninhalt kopieren kann, ohne das betroffene System zu verändern.

Spurenvernichtung

Forensik-Experten sind sich einig, dass die meisten Fehler passieren, kurz nachdem ein Sicherheitsvorfall bemerkt wurde. Sei es, dass Administratoren versuchen, das System möglichst schnell wieder zum Laufen zu bringen und dazu neu booten, Updates installieren oder ein Standard-Image aufspielen, oder dass Privatpersonen in Panik und aus Scham ihre vermeintlichen Internetspuren löschen, nachdem sie die Dialer-Gebühren auf der Telefonrechnung bemerkt haben. Außerdem sollte man immer bedenken, dass ausnahmslos alle Aktionen, die man mit Bordmitteln am betroffenen System durchführt, potenzielle Beweise vernichten beziehungsweise ihren Einsatz in einem Gerichtsprozess verhindern können.

Als erste Aktion sollte daher in jedem Fall ein forensisch korrektes Abbild aller betroffenen Daten erstellt und authentifiziert werden, ohne dabei die Originaldaten zu verändern. Muss oder kann man ein „live-system“ untersuchen, sollten die Daten möglichst in der Reihenfolge ihrer Halbwertszeit gesichert werden, also die flüchtigsten zuerst. Die konkrete Vorgehensweise dabei ist von Fall zu Fall verschieden und auch unter Experten umstritten. In der überwiegenden Anzahl der Fälle wurden die betroffenen Systeme jedoch bereits abgeschaltet und die Ermittlungen konzentrieren sich auf die permanenten Datenträger. Das Folgende bezieht sich deshalb auf die Forensik eines „toten“ Systems.

Ein forensisch korrektes Image ist eine exakte Kopie eines Datenmediums. Seine Erstellung sollte unabhängig von dessen logischer Organisation und dem verwendeten Dateisystem sowie eventuellen Fehler auf dieser Ebene sein.

Physikalische Fehler müssen robust und nachvollziehbar behandelt werden. Seine Authentizität sowie die Unverändertheit des Originalmediums sollten möglichst sicher nachgewiesen werden können.

Das wichtigste Hilfsmittel für eine forensische Analyse ist somit eine ausreichend große Festplatte, die eine Datei der Größe der zu sichernden Festplatte aufnehmen kann. Diese kann man als zusätzliche Platte in das zu untersuchende System einbauen, um darauf das Image abzulegen und später auf einem anderen Computer zu untersuchen; Profis arbeiten mit externen Festplatten, die sie via SCSI, USB oder FireWire an das zu untersuchende System anschließen. Wer etwas mehr Zeit investiert, kann das Image auch übers Netz direkt auf dem Arbeitsplatzrechner erstellen.

Die üblichen Imaging-Tools eignen sich in der Regel nicht für das Erstellen eines forensisch korrekten Abbilds. Da sie in erster Linie auf Performance und Platzersparnis optimiert sind, lassen sie normalerweise freie Sektoren weg, verändern eventuell das Originalmedium und können nicht mit Fehlern in der Dateisystemstruktur umgehen. Das ist aber nötig, wenn ein Virus oder ein Angreifer als letzte Aktion zum Beispiel die Partitionstabelle gelöscht hat.

Das unscheinbare Systemtool dd, das zu jeder Linux-Distribution gehört, erfüllt dagegen alle oben genannten Anforderungen. Im Computer Forensic Tool Testing Programm der US Regierung [1] ist dd das einzige Imaging-Werkzeug, das ohne Einschränkung alle Tests bestanden hat. Selbst so renommierte kommerzielle Pakete wie Encase oder SafeBack wiesen in diesem Test Anomalien auf.

Das normale dd kümmert sich um die reine Erstellung des Abbilds. Dabei spielt es nahezu keine Rolle, um was für ein Medium es sich konkret handelt. Solange Linux es unterstützt, kann man davon mit dd ein Abbild erstellen. Das gilt insbesondere für alle Arten von Festplatten, optischen Laufwerken, Floppy-Disks, USB-Sticks, Speicherkarten und sogar für den Hauptspeicher.

Für die Authentifizierung eignen sich weit verbreitete Linux-Tools wie md5sum, md5deep oder sha1sum. Ein typischer Ablauf für das Erstellen eines forensisch korrekten Abbilds könnte zum Beispiel so aussehen:

```
md5sum /dev/hda > hash.txt
dd if=/dev/hda of=/mnt/sda1/cases/4711.dd
md5sum /dev/hda >> hash.txt
md5sum /mnt/sda1/cases/4711.dd >> hash.txt
```

Dabei ist /dev/hda die zu sichernde IDE-Platte, deren Abbild in einem Verzeichnis der ersten Partition einer externen SCSI/USB-Platte landet, die unter Knoppix auf /mnt/sda1 gemountet wurde. /dev/hda ist dabei nicht in das System eingebunden.

Falls keine physikalischen Fehler aufgetreten sind, stimmen die drei mit md5sum generierten Hash-Werte überein und weisen damit nach, dass die Dateien erstens korrekt kopiert und zweitens nicht verändert wurden. Mit dem Tool netcat kann man die erstellten Images auch sehr einfach über ein Netzwerk transportieren.

Dazu öffnet man auf dem Zielrechner einen Mini-Server, der alle ankommenden Daten in eine Datei schreibt:

```
nc -l -p 4711 > 4711.dd
```

und beschickt diesen dann mit den ausgelesenen Daten:

```
dd if=/dev/hda | nc <Ziel-Host> 4711
```

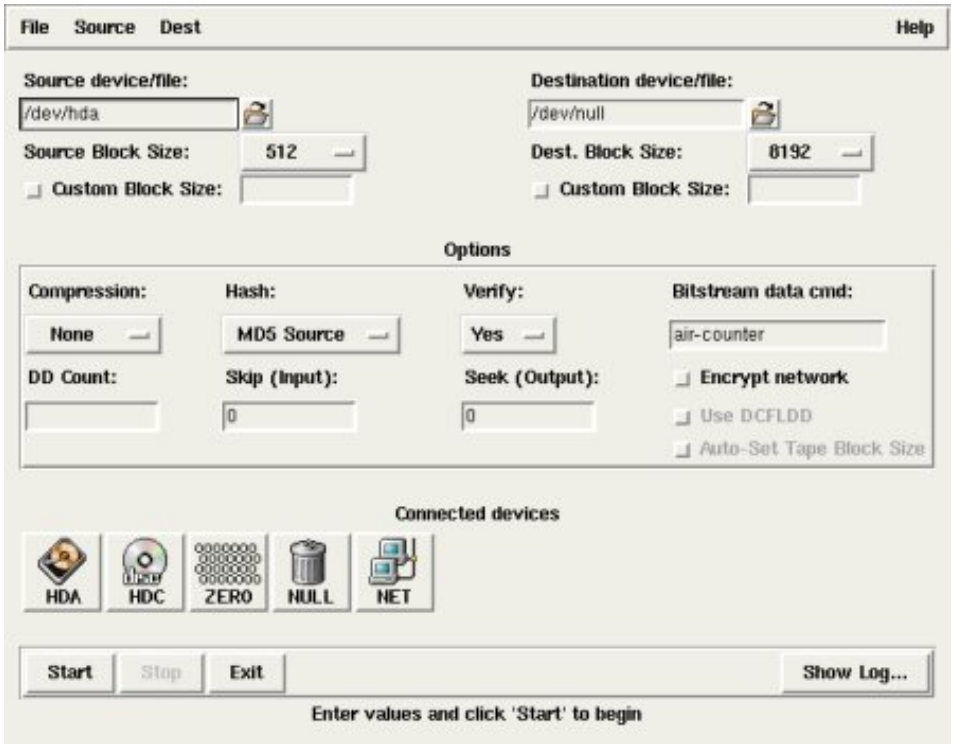
Natürlich ist auch hier ein Vergleich der MD5-Hashes vorzunehmen. Wenn es nur um den konkreten Datenbestand auf einem Dateisystem - einem Laufwerk im Windows-Jargon - geht, kann man auch statt ganzer Platten einzelne Partitionen sichern und dd statt aus hda aus hdaX (X=1, 2, ...) lesen lassen. Das vereinfacht die spätere Auswertung, kommt aber nur in Frage, wenn die Partitionstabellen unversehrt sind. Man „verliert“ dabei außerdem alle Informationen, die außerhalb der Dateisysteme beispielsweise im Master Boot Record abgelegt sind. Profis arbeiten deshalb

grundsätzlich mit Images kompletter Platten.

Die vom Computer Forensic Lab des US-Verteidigungsministeriums erweiterte dd-Version dcfldd bietet eine integrierte MD5-Hash-Berechnung. Bei der Bearbeitung von defekten Datenträgern kann dd_rescue weiterhelfen. Allerdings sind „auffällige“ Datenträger oft besser in einem Datenrettungslabor aufgehoben, bevor zu viel Material abgetragen wird. (Alle Tools finden Sie über den Soft-Link am Ende des Artikels.)

Mehr Komfort

Das Open-Source-Projekt AIR-Imager (automated image and restore) bemüht sich um ein wenig mehr Komfort beim Einsatz dieser Tools und entwickelt dafür eine grafische Benutzeroberfläche zur Steuerung von dd & Co. Sie bietet eine komfortable Auswahl von Quell- und Ziellaufwerken, den Einsatz von Kompression, Netzwerktransfer, automatische Authentifizierung sowie das Löschen von Devices an. AIR-Imager kann wahlweise das normale dd oder auch dcfldd verwenden.



[1]
Die TK-Oberfläche von AirImager vereinfacht den Einsatz von Tools wie dd, md5sum und netcat.

Das noch in einem frühen Entwicklungsstadium befindliche Projekt ODESSA (Open Digital Evidence Search and Seizure Architecture) bindet in den Prozess der Image-Erstellung erste Analysefunktionen ein. Dabei setzt es auf eine Client/Server-Struktur auf, die ein forensisches Arbeiten innerhalb eines LAN ermöglicht. Über eine Plug-in-Schnittstelle bindet es unter anderem Module zur Hash-Berechnung, String-Suche oder auch zur Extraktion von Dateien anhand von Header- und Footer-Signaturen ein.

Forensische Analyse

Nachdem forensische Kopien aller betroffenen Datenträger erstellt wurden, sollten man die Originale sicher verwahren. Weitere Analysen erfolgen nur noch auf den Kopien. Damit ist sichergestellt, dass ein unabhängiger Dritter später die gefundenen Ergebnisse wirklich sauber nachvollziehen und überprüfen kann. Des Weiteren empfiehlt es sich, die Images zur Untersuchung immer nur im Read-only-Modus zu mounten - schon um versehentliche Änderungen zu vermeiden.

Auch auf dem Gebiet der Analyse bietet Linux von Haus aus viele Werkzeuge und Mechanismen zum Durchsuchen der Daten. Im praktischen Einsatz erweist sich das Loopback Device als besonders nützlich. Damit ist es möglich, ein forensisches dd-Image read only zu mounten:

```
mount -o loop,ro hda1.dd /mnt/test1
```

Danach kann man für die weitere Untersuchung damit arbeiten, als wäre der physische Datenträger im System vorhanden. Handelt es sich bei dem Image um das Abbild einer ganzen Platte, muss man Partitionen mit passenden Offsets mounten oder via dd extrahieren [2]. Mehr Komfort bietet hier das von NASA-Mitarbeitern erweiterte Enhanced Loopback Device, das die Partitionsinformationen in einem Imagefile automatisch interpretiert.

Bei der Analyse setzen auch Experten gern System-Tools wie grep, strings, find, file oder hexedit ein. Da die Größen der zu untersuchenden Speichermedien jedoch sehr schnell ansteigen und auch der beste Forensiker keine 200-GByte-Festplatte mit einem Hexeditor in akzeptabler Zeit untersuchen kann, sind aber auch spezielle Werkzeuge gefragt, die Teile der Analyse automatisieren und die Handarbeiten auf ein vertretbares Maß reduzieren.

Spürhunde am Werk

Für die Postmortem-Analyse eines Unix-Systems nach einem Sicherheitsvorfall gibt es im Open-Source-Bereich seit 1999 eine von Dan Farmer und Wietse Venema entwickelte sehr umfangreiche Werkzeugkollektion mit dem bezeichnenden Namen The Coroner's Toolkit (TCT, Werkzeugkasten des Leichenbeschauers). Darin sind unter anderem Analyse-Tools wie grave-robber oder mactime enthalten, die Informationen über im Dateisystem enthaltene Zugriffsdaten auch von gelöschten Dateien preisgeben. unrm und lazarus stellen gelöschte Dateien wieder her. Dabei ist TCT plattformspezifisch - Analyse- und Untersuchungsplattform müssen gleich sein.

Eine Weiterentwicklung des TCT, die diesen Nachteil behebt, stammt von Brian Carrier. Das Sleuth Kit, bis vor kurzem unter dem Namen TASK bekannt, läuft unter verschiedenen Unix-Versionen inklusive Linux. Es analysiert DOS-, BSD- und MAC-Partitionen sowie Sun-Slices, kann zurzeit allerdings nur die Dateisysteme NTFS, FAT, FFS, ext2fs sowie ext3fs lesen.

Die Kommandozeilenwerkzeuge des Sleuth Kit benötigen keine Betriebssystemfunktionen für die Analyse der Images. Statt sie zu mounten, greifen sie auf eine eigene Infrastruktur zur Interpretation von Daten und Metadaten zurück. Sie spüren auch Daten auf, die zwischen Partitionen versteckt wurden, und unterstützen alle Attribute von NTFS-Dateien wie zum Beispiel alternative Dateiströme.

Im Bereich der Computer-Forensik bestehen relevante Informationen nicht nur aus Dateiinhalten. In einigen Fällen ergeben sich wertvolle Beweise aus den im Dateisystem enthaltenen Zugriffsmustern, den so genannten Media-Access- kurz MAC-Times. Das Sleuth Kit bietet hier sehr gute Werkzeuge, um eine Timeline der Aktivitäten unter Berücksichtigung der ursprünglichen Zeitzone sowie von eventuellen Zeitversätzen (Skews) zu erstellen. Dazu kann es auch andere zeitbasierte Ereignisprotokolle, beispielsweise Log-Dateien von Proxy-Servern, Firewalls et cetera, importieren und in die Timeline einbeziehen.

Die heute untersuchten Medien enthalten oft sehr große Datenmengen. Schon allein die verwendeten Betriebssysteme bringen jede Menge eigene Dateien mit. So enthält beispielsweise eine Windows-2000-Installation allein knapp 6000 Bilddateien. Für eine effiziente Analyse derartiger Medien kann es deshalb sehr wichtig sein, bekannte Dateien sicher herauszufiltern und nur den Rest weiter zu betrachten oder aber - zum Beispiel bei der Suche nach Raubkopien - diese positiv zu identifizieren.

Die US-Regierung betreibt dazu eine umfangreiche Datenbank, in der die jeweiligen Hash-Werte einer Vielzahl von bekannten Dateien hinterlegt sind. Diese Datenbank ist frei zugänglich und die Sleuth-Kit-Werkzeuge können sie in die

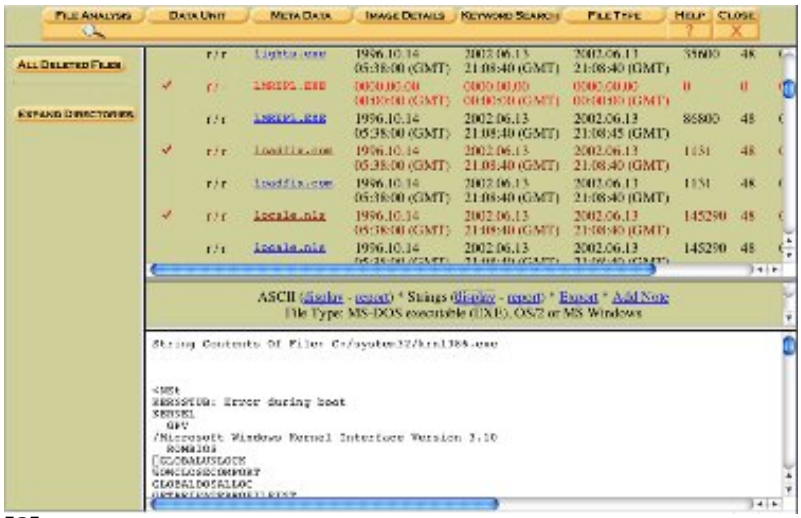
Untersuchung miteinbeziehen. [3]

Zeit für eine Autopsie

Ebenfalls von Brian Carrie stammt der Forensic Browser Autopsy, der die Sleuth-Kit-Werkzeuge unter einer grafischen Benutzeroberfläche zusammenfasst. Autopsy stellt nach dem Start einen gesicherten HTML-Server bereit, durch den es auch übers Netz zu bedienen ist.

Ein Vorteil dieser Architektur liegt darin, dass sich mehrere Ermittler von unterschiedlichen Orten beteiligen können. Um die forensische Korrektheit dennoch zu gewährleisten, integriert Autopsy ein umfangreiches Host- und Case-Management und protokolliert zusätzlich alle durchgeführten Aktionen getrennt nach Ermittlern, Medium und Fall.

Des Weiteren kann es umfangreiche Datei-, Inhalts- und Dateityp-Analysen durchführen. Da-zu stellt Autopsy eine Art Dateimanager-Interface bereit und präsentiert dort auch Details zu gelöschten und versteckten Dateien sowie zu internen Dateisystemstrukturen.



[2]
Dateianalyse und Suchfunktionen gehören zu einem leistungsfähigen Toolkit wie Autopsy.

In die von Autopsy aus dem Dateisystem extrahierte Aktivitäts-Timeline kann man auch weitere zeitbasierte Ereignisse einarbeiten und kommentieren, was für eine verständliche, gerichtstaugliche Darstellung der Ergebnisse nützlich ist. Neben der Zusammenarbeit mit der Hash-Datenbank bekannter Dateien der US-Regierung kann der Benutzer auch eigene Hash-Daten integrieren und als gut oder böse deklarieren. Eine Anwendung dafür wäre zum Beispiel ein Hash-Set von einer Installation eines sauberen Vergleichssystems.

Eine eingebaute Suchfunktion durchsucht ein Dateisystem nach vorgegebenen Zeichenfolgen, die auch grep-like als reguläre Ausdrücke angegeben werden können. Eine vorher erstellte Indexdatei beschleunigt diesen Vorgang erheblich. Im Anschluss daran kann man die jeweiligen Fundstellen mittels ASCII oder Hexeditor näher untersuchen.

Finden mit Köpfchen

Eine besonders effiziente Suche nach bestimmten Datentypen wie Bilder oder Videos ermöglicht das Open-Source-Tool Foremost. Die Special Agents der US Air Force Kendall und Kornblum haben es dem DOS-Programm CarvThis des amerikanischen Defense Computer Forensic Labs nachempfunden. Neben dem Linux-Original gibt es mittlerweile auch eine Windows-Version.

Auch Foremost kann sowohl physische Datenträger als auch dd-Abbilder untersuchen. Eine Konfigurationsdatei spezifiziert dabei Header- und Footer-Signaturen der gesuchten Dateien sowie eine maximale Dateigröße. Foremost

extrahiert danach automatisch alle Dateien, die dem Suchmuster entsprechen. Allerdings funktioniert das nur dann korrekt, wenn die Dateien nicht fragmentiert sind. Ansonsten erhält man unter Umständen nur Fragmente der ursprünglichen Datei. Eine Log-Datei protokolliert dabei alle verwendeten Parameter, alle durchgeführten Aktionen und die Offsets aller Fundstellen.

Die hier vorgestellten Open-Source-Tools brauchen den Vergleich mit kommerziellen Produkten nicht zu scheuen. Darüber hinaus gibt es eine Vielzahl von Erweiterungen und eigenständigen Werkzeugen, die hier keinen Platz mehr gefunden haben. Dazu kommt die Erkenntnis, dass gerade in diesem sensiblen Bereich offene Standards, transparente Analysen und wirklich unabhängige Experten mehr als nur technische Vorteile bieten. (ju)

Holger Morgenstern arbeitet als öffentlich bestellter und vereidigter EDV-Sachverständiger auf dem Gebiet der Computer-Forensik.

Literatur

[1] **Computer Forensic Tool Testing[3]** Programm der US Regierung

[2] **Infos[4]** zum Mounten via Loopback

[3] **Hash-Werte bekannter Dateien[5]**

[4] Übersicht zu **Open-Souce-Forensik[6]**

Open Source Tools

- **dcfl-dd[7]**
- **Enhanced Loopback Device[8]**
- **ForeMost[9]**
- **Sleuth Kit[10]**
- **Odessa[11]**
- **AIR-Imager[12]**
- **Autospy[13]**
- **The Coroner's Toolkit[14]**
- **dd-rescue[15]**

Kommerzielle Tools

- **SMART[16]**
- **SafeBack[17]**
- **Encase[18]**

URL dieses Artikels:
http://www.heise.de/security/artikel/46297

Links in diesem Artikel:
[1] /bilder/46297/1/1
[2] /bilder/46297/2/1
[3] http://www.cftt.nist.gov
[4] http://www.trekweb.com/~jasonb/articles/linux_loopback.shtml
[5] http://www.nsrl.nist.gov
[6] http://www.computerforensik.net
[7] http://sourceforge.net/projects/biatchux
[8] ftp://ftp.hq.nasa.gov/pub/ig/ccd/enhanced_loopback/patches
[9] http://foremost.sourceforge.net/
[10] http://www.sleuthkit.org/

[11] http://odessa.sourceforge.net/
[12] http://air-imager.sourceforge.net/
[13] http://www.sleuthkit.org/autopsy/
[14] http://www.porcupine.org/forensics/tct.html
[15] http://www.garloff.de/kurt/linux/ddrescue/
[16] http://www.asrdata.com/tools/
[17] http://www.forensics-intl.com/safeback.html
[18] http://www.guidancesoftware.com/support/downloads.shtm