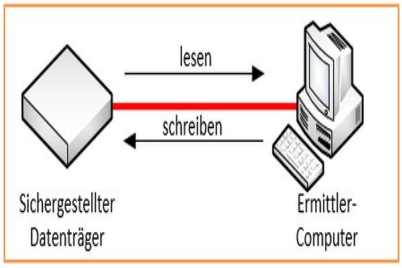
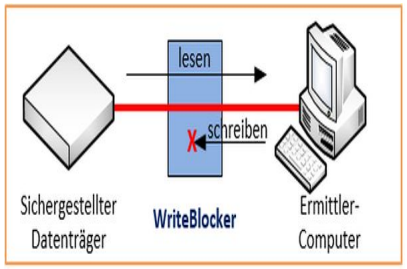
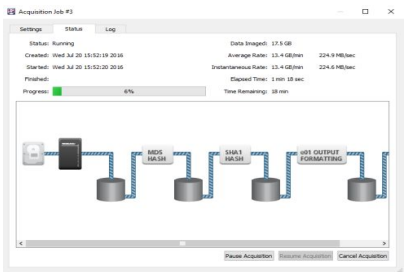
Im Einsatz – im Thema.
POLIZEI PRAXIS

HERAUSFORDERUNGEN DER DIGITALEN BEWEISMITTELAUFNAHME UND ANALYSE FLEXIBEL BEGEGNEN







Seit vielen Jahren werden die klassischen Ermittlungstätigkeiten der Polizei und anderer Ermittlungsbehörden im zunehmenden Maße ergänzt durch die Analyse digitaler Daten – die IT-Forensik. Während für die Auswertung der gewonnenen Daten inzwischen eine Reihe von leistungsfähigen Computerprogrammen zur Verfügung stehen, die dem Ermittler die Arbeit zwar nicht abnehmen, ihn aber bei der Verarbeitung der teils immensen Datenmengen

extrem unterstützen, gilt es zu Beginn dieses Ermittlungsprozesses diese Daten zunächst einmal zu sichern. Hierbei ist die lückenlose Dokumentation und ein Nachweis über die Integrität der Daten (die Unverfälschtheit) unerlässlich, sollen diese in einem späteren Stadium vor einem Gericht Bestand haben.

Der schnelle Innovationszyklus in der IT stellt dabei die Ermittler laufend vor neue Herausforderungen. Eine Vielzahl von unterschiedlichen Datenträgern beherbergen eine stetig größer werdende Fülle an Informationen und nicht zuletzt spielt der Fakor Zeit eine entscheidende Rolle. Erscheint es als nicht sinnvoll oder schlicht nicht umsetzbar, die Datenträger in ein IT-forensisches Labor zu verbringen, ist es notwendig, diese Datensicherung vor Ort durchzuführen.

Ein bewährtes Werkzeug hierzu ist der Trecorder der Firma mh SERVICE GmbH aus Karlsruhe.

Die mobile forensische Hochleistungs-Workstation ist speziell darauf ausgelegt, am Einsatzort möglichst schnell die Arbeit aufnehmen zu können. Nach dem Verbinden mit einer Steckdose und dem Einschalten kann die Arbeit sofort beginnen.

In seiner Ausführung ist der TreCorder sehr robust und widerstandsfähig gegen mechanische Einflüsse gestaltet. Das stabile Alu-Gehäuse verzeiht so manchen Stoß. Der eingebaute 17 Zoll Monitor wird durch die Tastatur geschützt, die zur Bedienung einfach heruntergeklappt wird. Während auf der linken Seite Zugang zu allen Standard-Schnittstellen des Computers besteht, befinden sich auf der rechten Seite alle, für die forensische Arbeit notwendigen schreibgeschützten Schnittstellen und Zugänge.

Bei der Entwicklung des TreCorders wurde auf mehrere Eigenschaften Wert gelegt:

· Leistung: Im TreCorder werden ausschließlich Hochleistungs Server-Komponenten (Mainboard, CPU, RAM, etc.) verbaut. Diese sind zum einen erheblich leistungsfähiger als vergleichbare sogenannte mobile Komponenten (wie z.B. in Laptops verbaut), zum Anderen erhelblich wartungsfreundlicher.

· Mobilität: Die gesamte Technik befindet sich in einem Gehäuse. Das Gerät muss lediglich mit einem Stromkabel mit dem Stromnetz verbunden werden und ist sofort einsatzbereit. Zum Transport dient ein mitgelieferter Trolley mit Rollen, in dem alles sicher verstaut und transportiert werden kann.

· Flexibilität: Mit dem TreCorder können neben dem Anfertigen forensischer Abbilder von Datenträgern (sog. Images) gleichzeitig auch schon forensische Untersuchungen vor Ort durchgeführt werden; aufgrund seiner Konzeption durchaus gleichzeitig mit dem Image-Prozess. Standardmäßig wird der TreCorder als Dual-Boot-System konfiguriert. D.h. neben dem Betriebssystem Windows® von Microsoft® kann das Gerät auch unter Linux gestartet werden, was dem IT-Forensiker eine Vielzahl von Möglichkeiten eröffnet.

· Forensik: Für den Einsatz in der IT-Forensik entwickelt verfügt der TreCorder über drei durch das US-Amerikanische National Institute of Standard and Technology (NIST) zertifizierte Schreibschutzadabter (Writeblocker). Durch diese Zertifizierung ist der TreCorder anerkannt als Werkzeug für eine technisch rechtssichere Beweismittelaufnahme. Für die Analyse und Auswertung des Datenmaterials können alle gängigen IT-forensischen Programme eigesetzt werden.

· Ökologie und Ökonomie: Um mit der technischen Entwicklung mithalten zu können, ist es erforderlich, von Zeit zu Zeit die Ermittlungswerkzeuge nachzurüsten. Daher wurde bei der Entwicklung des TreCorders auf ein nachhaltiges Konzept geachtet. Zum einen durch Langlebigkeit, Ausbaufähigkeit aber auch die Möglichkeit kostengünstig das einmal angeschaffte Gerät auf die jeweils aktuelle Komponentenversion aufgerüstet werden.

Der TreCorder wurde speziell dafür konzipiert, Sicherheits- und Strafverfolgungsbehörden, die unter Zeitdruck stehen, das forenisch korrekte Anfertigen von nahezu allen digitalen Datenträgern Abbilder (Images) zu ermöglichen. Hierzu können gleichzeitig bis zu drei Datenträger (z.B. Festplatten, USB-Sticks, SSDs, etc.) mit maximaler Geschwindigkeit in ein forensisches Image, d.h. ein 1:1 Abbild des Datenträgers, überführt werden. Maximale Geschwindigkeit bedeutet, dass die Steuerelektronik des sichergestellten Datenträgers die maximal mögliche Datenmenge liefert. Eine weitere Steigerung ist physikalisch nicht mehr möglich.

Die so erstellten Datenträger-Images werden auf jeweils einer eigenen Zielfestplatte abgelegt. Diese befinden sich in von außen werkzeuglos zugänglichen Wechselrahmen. Verfügt diese über keinen Speicherplatz mehr oder wird ein weiterer Datenträger zur Sicherung angeschlossen, kann die Zielfestplatte im laufenden Betrieb entfernt und durch eine weitere ersetzt werden. Durch dieses sog. Hot-Swap-Verfahren entfällt das zeitraubende Herunter- und wieder Hochfahren des Rechners.

Zum essentiellen Kern des TreCorders gehören die drei Writeblocker der Firma Tableau. Writeblocker sind eine absolut notwendige Komponente wenn es darum geht, digitale Datenträger so zu sichern, dass diese Daten als Beweismittel vor Gericht Bestand haben. Hier kommt der oben erwähnte Nachweis für die Integrität der Daten zum Tragen. Um als Beweismittel anerkannt zu werden, muss belegt werden können, dass die gesicherten Daten eine 100%ig identische Kopie der sichergestellten Daten (bzw. Datenträger) darstellen.
Der Nachweis dieser Übereinstimmung erfolgt über sogenannte Hash-Werte, die beim Anfertigen des Daten-Images erstellt werden. Hash-Werte sind Prüfsummen über den gesamten Datenbestand. Mithilfe eines mathematischen Algorithmusses wird ein digitaler Fingerabdruck erstellt. Dieser digitale Fingerabdruck des angefertigten Daten-Image muss eindeutig identisch sein, mit dem der Quelldaten. Nur dann kann zweifelsfrei belegt werden, dass die zu Ermittlungszwecken verwendeten Daten absolut identisch mit den vorgefundenen Daten sind. Dieses Verifizierungsverfahren zur Integritätsprüfung von digitalen Daten ist inzwischen weltweit anerkannter Standard.

Neben den eigentlichen Nutzdaten (Dokumente, Bilder, Programme, etc.) befinden sich auf jedem Datenträger auch eine Reihe von Systemdaten, die das Betriebssystem dort ablegt. Wird nun ein Datenträger an einen Computer angeschlossen, finden sofort Schreibvorgänge des Betriebssystems statt. Diese verändern zwar noch nicht unbedingt und unmittelbar die Nutzdaten, aber auch schon veränderte Systemdaten führen dazu, dass die Integrität der Daten nicht mehr zweifelsfrei belegt werden kann, was unter Umständen dazu führt, dass das Beweismittel juristisch nicht mehr verwertbar ist.

An dieser Stelle kommt nun der bereits oben erwähnte Writeblocker zum Einsatz. Dieser erlaubt dem Computer des Ermittlers nur noch lesende Zugriffe auf den sichergestellten Datenträger und unterbindet alle schreibenden. Somit wird garantiert, dass die gesicherten Daten absolut identisch mit den sichergestellten Quelldaten sind.

Wird nach dem Anschluss eines Datenträgers an den Writeblocker der Sicherungsprozess gestartet, wird der bereits erwähnte Hash-Wert von der Imaging-Software automatisch erstellt und in einer speziellen Log-Datei gemeinsam mit dem Daten-Image abgelegt (Abbildung am Beispiel des Imaging-Programs der Firma Tableau). Je nach Einstellung und Erforderniss werden sogar gleichzeitig zwei unterschiedliche Prüfsummen (hier ‚MD5' und SHA1') erstellt, welche in Kombination den Nachweis der Integrität der Daten sogar noch verstärken.
Im Zunehmenden Maße sind Ermittler auch damit konfrontiert, dass Daten nicht mehr auf einem einzelnen Datenträger vorliegen. Immer häufiger finden Ermittler sehr große Datenmengen auf großen Speichereinheiten (Storage-Center, Server, NAS-Laufwerke, aber auch Cloud-Speicher) vor. Hier ist es in aller Regel wenig sinnvoll und meißt praktisch gar nicht durchführbar, die Datenträger einzeln zu sichern. Gerade bei großen Verbundlaufwerken, sog. RAID-Systemen, liegen die Daten verteilt auf mehreren Datenträgern. Die Rekonstruktion eines solchen RAID-Systems aus Einzellaufwerken ist technisch nur sehr schwer möglich.

In diesen Fällen findet dann meist eine sog. Live-Sicherung statt. Im laufenden Betrieb werden alle Daten des RAID-Systems über Netzwerk oder spezielle Zugänge gesichert. Da hier die zu sichernden Datenmengen in aller Regel nicht auf eine Zielfestplatte passen, wird der Ermittler durch die Hot-Swap-Fähigkeit enorm entlastet. Das System fordert den Ermittler zu gegebener Zeit dazu auf, eine weitere leere Festpatte in den Wechselrahmen einzulegen, damit die Datensicherung fortgesetzt werden kann.

Fazit:

Vor der eigentlichen Analyse der Daten steht die Sicherung derselben. Um die steigende Flut von Daten gerichtsverwertbar und schnell sichern zu können, benötigen die Ermittler vor Ort geeignete Werkzeuge. Mit dem TreCorder steht ihnen ein hochflexibles, leistungsstarkes und mobiles Gerät zur Verfügung um den Herausforderungen der digitalen Beweismittaufnahme angemessen begegnen zu können.

Text: Bernd Hiltel
Grafik/Bilder: mh SERVICE GmbH

Alle Artikel dieser Kategorie