Datenextraktion von 9-Spur-Bändern

PROF. DR. BRUCE NIKKEL

Berner Fachhochschule

Im Jahr 1964 wurde der legendäre IBM System/360 Grossrechner vorgestellt. Dieser nutzte die 12,7 mm (½ Zoll) breite 9-Spur-Magnetbandtechnologie, die sich später zum Industriestandard entwickeln sollte. Gängige Bandspulengrössen waren 7, 8, 5 und 10,5 Zoll Durchmesser, jeweils mit unterschiedlichen Bandlängen (die längste 1,1 km). Die Bänder waren durch eine Kunststoffhülle oder eine Schutzkappe geschützt, die vor der Verwendung (manuell oder automatisch) entfernt werden musste. Auf der Unter-/Rückseite des Bandes befanden sich eine eindeutige Kennung und abnehmbare Schreibfreigaberinge (ohne diese waren die Bänder nur lesbar). Die Bänder hatten ausserdem eine runde Vertiefung an der Vorder-/Oberseite, durch die man das im Laufwerk eingelegte Band manuell aufwickeln konnte.

Der 9-Spur-Lesekopf konnte ein 8-Bit-Byte und ein Paritätsbit lesen und schreiben. Die Aufzeichnungsdichte wurde in Zeichen oder Bytes pro Zoll (cpi bzw. bpi) gemessen, und das Codierungsverfahren wurde im Laufe der Zeit verbessert: NRZI (Non-Return-to-Zero Inverted) für 800 bpi, PE (Phase Encoding) für 1600 bpi und GCR (Group Coded Recording) für 6250 bpi. Die Bänder besassen reflektierende Markierungen, die den Bandanfang (BOT) und das Bandende (EOT) anzeigten. Diese Markierungen wurden mit Lichtsensoren im Laufwerk festgestellt.

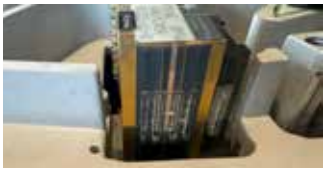
Die Daten auf dem Band wurden in Blöcken oder Datensätzen gespeichert, die durch Blöcke oder Datensätze mit Zwischenräumen (typischerweise 8 bis 15 mm) getrennt waren. Die Kodierung, die Länge und die Blockgrösse bestimmten die Gesamtspeicherkapazität des Bandes, die üblicherweise zwischen 40 MB und 160 MB lag. Mehrere aufeinanderfolgende Bandblöcke bilden eine Banddatei. Es können mehrere Banddateien vorhanden sein, die durch Dateimarkierungen getrennt und in sequenzieller Reihenfolge auf einem Band gespeichert sind. Eine vollständige Datenwiederherstellung umfasst die Suche nach mehreren Banddateien und deren Extraktion.

Die Datenrettung von einem unbeschädigten Band erfordert ein Bandlaufwerk, ein Hostsystem und die entsprechende Software. Die Verwendung älterer Bandlaufwerke wie der IBM 2400 oder 3400 ist zwar möglich, setzt aber ein funktionierendes Laufwerk und Hostsystem mit dem Originalbetriebssystem und der zugehörigen Software so-

Verschiedene Bandgrössen

Schutzhülle

Schreibfreigaberinge



9-Spur-Bandkopf

Lichtsensoren

Reflektierender Marker

wie entsprechende Bedienungskenntnisse voraus. Neuere SCSI-basierte Bandlaufwerke können weiterhin alte 9-Spur-Bänder lesen und ermöglichen die Datenextraktion mit modernen Linux-Systemen, Open-Source-Tools und grundlegenden Shell-Kenntnissen.

In diesem Artikel verwende ich ein DEC TSZ07 Tischbandlaufwerk aus den frühen 1990er-Jahren zum Lesen von 9-Spur-Bändern. Das Laufwerk verfügt über eine Frontladeklappe, in die das Band eingelegt wird. Zum Einfädeln des Bandes wird ein Luftstrom verwendet, der das flatternde Bandende durch die Tonköpfe und Sensoren zur Aufwickelrolle führt, wo es sicher aufgewickelt wird. Luftstrom- und Druckkammern wurden auch in frühen IBM-Laufwerken zur Regulierung der Bandgeschwindig-

Tischgerät DEC TSZ07

Frontbedienfeld und Anzeigetafel

Interne Bandkammer

Adaptec 2944 SCSI-Karte

Rückseite des TSZ07

keit und -spannung eingesetzt, dies wird beim TSZ07 jedoch nicht verwendet. Das Laufwerk kann über die Frontplatte konfiguriert und bedient werden, die auch über ein LED-Display und Kontrollleuchten verfügt.

Der PC und die SCSI-Karte müssen nicht besonders schnell oder leistungsstark sein, um 9-Spur-Bänder zu lesen. Ich verwendete eine aktuelle Version von Debian Linux auf einem PC mit älterem Mainboard, 8 GB RAM und parallelen PCI-Steckplätzen. Die SCSI-Karte ist eine Adaptec AHA-2944UW mit einem Adapter auf SCSI-2. Die Wahl der richtigen SCSI-Schnittstelle ist wichtig. Dieses Laufwerk verwendet eine differentielle SCSI-Schnittstelle mit höheren Signalspannungen, die nicht mit gängigen SCSI-Karten für Consumer-PCs kompatibel ist.

Die Software, die für generische SCSI-Bandlaufwerke verwendet wird, kann auch für SCSI-basierte 9-Spur-Bandlaufwerke verwendet werden. Der Linux-Kernel verwendet die Zeichengeräte /dev/st0 und /dev/nst0, um auf ein einzelnes angeschlossenes Bandlaufwerk zuzugreifen. Für die Datenwiederherstellung ist das nicht automatisch rückspulbare Gerät /dev/nst0 praktischer.

Die benötigten Werkzeuge stammen aus der UNIX-Welt und umfassen typischerweise dd, mt und tar. Der Befehl mt steuert das Laufwerk und sendet SCSI-Befehle zum Zurückspulen, Auswerfen, Vor- und Zurückspulen des Bandes, Abrufen von Statusinformationen und vielem mehr. Es gibt zwei gängige Versionen: mt-gnu und mt-st (mt-st bietet mehr Low-Level-Funktionen). Der Befehl dd liest sequenzielle Datenblöcke vom Band und speichert sie im lokalen Dateisystem des PCs. Die Konvertierung von der IBM-EBCDIC-Kodierung kann mit dd während der Datenextraktion vom Band oder als zweiter Schritt für bereits extrahierte Daten erfolgen. Sind die auf dem Band gespeicherten Dateien als tar (Tape Archive) bekannt, kann der übliche tar-Befehl verwendet werden. Die Parameter und die Verwendung dieser Werkzeuge sind in den Handbuchseiten dokumentiert.

Nachdem die Banddateien vom Band extrahiert (und gegebenenfalls von EBCDIC konvertiert) wurden, muss das Format bzw. die Struktur der Daten ermittelt werden. Die ursprüngliche Software, mit der die Banddateien geschrieben wurden, kann dieses Format dokumentiert haben. Falls die Banddatei unbekannt ist, kann es erforderlich sein, deren Inhalt durch Reverse Engineering zu rekonstruieren. Ziel ist es, die Daten der Banddatei in ein modernes, verwendbares Format wie Text oder CSV zu konvertieren. Sobald dies erreicht ist, war die Datenextraktion erfolgreich.

Referenzen

The original English version of this article:
https://digitalforensics.ch/enter/

TSZ07 Tape Drive Technical Manual:
https://bitsavers.org/pdf/dec/magtape/tsz07/

ANSI standard:
https://nvlpubs.nist.gov/nistpubs/Legacy/FIPS/fipspub50.pdf

EMCA standard:
https://ecma-international.org/publications-and-standards/standards/ecma-62/

mt-st manpage: https://www.unix.com/man_page/debian/1/mt-st

mt-gnu manpage: https://www.unix.com/man_page/linux/1/mt-gnu/

dd manpage: https://www.unix.com/man_page/linux/1/dd/

tar manpage: https://www.unix.com/man_page/linux/1/tar