Heiko Rittelmeier

Wer ist Miriam?

Ein ganz normaler PC unter der Lupe

Um ein Gefühl für die Brisanz des Themas zu bekommen, haben wir den Forensiker Heiko R. beauftragt, einen ganz normal genutzten PC forensisch zu untersuchen. Er schildert, wie viele Informationen er über die Besitzerin herausgefunden hat – mit minimalem Aufwand.

Für den Test bekomme ich ein Image von ungefähr 320 GByte. Es enthält zwei interessante Partitionen, vermutlich eine für das Betriebssystem und eine für die Daten. Mein Mittel der Wahl ist in diesem Fall Autopsy unter DEFT Linux: Ich erstelle einen neuen Case und importiere das Image. Ein erster Blick auf die erste Partition lässt mich vermuten, dass es sich bei dem Computer um einen Rechner mit Windows XP handelt. Der nächste Blick gilt dem Ordner „Dokumente und Einstellungen“: Dort gibt es einen Ordner „miriam“ (Name geändert).

Das nächste Ziel ist der Desktop-Ordner; auf den ersten Blick sticht mir eine Datei „adressen_firma.xls“ ins Auge, die anscheinend gelöscht wurde. Die Wiederherstellung kostet einen Klick. Es handelt sich um eine Excel-Tabelle mit Kontaktdaten von Kollegen, teilweise inklusive privater Nummern und Adressen.

Auch Miriam findet sich darin – mit vollem Namen, Geburtsdatum und Privatadresse. Die Dame ist wohl verheiratet, denn es gibt eine zweite Mailadresse von web.de mit anderem Nachnamen. Ihre Aufgabe in der Firma kenne ich jetzt auch – eine ideale Grundlage für gezieltes Phishing.

„Miriam ist verheiratet.“

Ein Dokument namens „Anamnesebogen.pdf“ weckt mein Interesse. Es handelt sich um ein leeres Formblatt, das aus dem Internet heruntergeladen wurde. Darauf deutet jedenfalls ein Alternate Data Stream „Zone Identifier“ hin. Der Inhalt „ZoneId=3“ zeigt, dass die Datei aus dem Internet stammt. Zwei gelöschte Dokumente „Eheurkunde.(xxx)“ lassen sich spontan nicht wiederherstellen, das würde mit anderen Werkzeugen möglicherweise trotzdem funktionieren.

Zumindest zeigt mir die eingescannte Teilnahmebescheinigung einer Fortbildungsveranstaltung, dass ihr Mann „Mark“ heißt (auch hier: Name geändert) und mit Gebäudeplanung zu tun hat. Der Rest der Dateien auf dem Desktop interessiert mich gerade nicht (vorwiegend Kochrezepte).

Ihre privaten Mails liest Miriam anscheinend mit Thunderbird, größere Datendateien sind erkennbar. An der Stelle höre ich auf, ich bin schließlich kein Stalker. Ich finde zumindest keinen Hinweis darauf, dass ich die E-Mails nicht lesen kann. Auch das (vermutlich gespeicherte) Passwort des Mail-Accounts werde ich nicht versuchen auszulesen. Nach diesem ersten Überblick wende ich mich der zweiten Partition zu.

Die Benutzerin scheint Sinn für Ordnung zu haben, alles ist fein säuberlich thematisch in Unterordner eingruppiert.

„… singt im Chor.“

In der nächsten Ebene ist wieder ein Verzeichnis „miriam“ enthalten, darunter eines, das mich besonders interessiert: „BERUF“. Darin finde ich – schön sortiert – Unterlagen zu allen bisherigen und dem aktuellen Arbeitgeber.

Dabei Bewerbungen, Arbeitsverträge, Tabellen mit den gezahlten Gehältern. Der Scan einer Bescheinigung zum Mutterschutz deutet darauf hin, dass die Familie um (mindestens) ein Mitglied gewachsen ist. Ich finde einen Ex-Arbeitgeber aus der Finanzbranche, dazu eine Versicherung und Hinweise auf ein Auslandsstudium.

Der nächste Ordner, dem ich mich zuwende, heißt „SCANS“. Ein Fahrzeugschein verrät mir, wann „Mark“ (der Ehemann) Geburtstag hat. Der Scan der Eheurkunde vervollständigt meinen Überblick über die Familie: geheiratet wurde 2009 in Bremen, Mark kommt aus dem hohen Norden, Miriam eher nicht.

Im Verzeichnis „Outlook“ finde ich mehrere PST-Dateien. Die Größe lässt vermuten, dass da einiges Interessantes drinstecken könnte. Ich lasse auch hier die Finger davon. Eine Datei „Kontakte Verlobung.csv“ liefert mir trotzdem einen Einblick in Miriams Bekanntenkreis.

Außerdem scheint sie in einem Chor zu singen (Stimme „Alt“). Von den restlichen Chormitgliedern kenne ich jetzt auch die Stimmlage, Geburtstage, die privaten Telefonnummern und von vielen auch die Handynummer.

Interessant ist auch das Verzeichnis „WISO Sparbuch“: Es enthält die Steuererklärung eines Jahres (gemeinsame Veranlagung, ein Kind). Ob die Dateien der verschiedenen erkennbaren „WISO“-Versionen passwortgesichert sind, werde ich nicht testen. Zielloses Stöbern in den Dokumenten (teils gelöscht, teilweise nicht) zeigt mir, dass Miriam im Gemeinderat ihrer methodistischen Kirchengemeinde aktiv ist.

Ich beschließe, mich dem Verzeichnis „Bilder“ nur sehr oberflächlich zu widmen. Ich befürchte, dass auch dort viel Privates zu finden sein wird. Ein Bild „Miriam5.jpg“ zeigt eine hübsche Frau mit halblangen blonden Haaren. Auf einem anderen Bild ist sie zwar braunhaarig, auf der Mehrzahl der Bilder aber blond. Ich beschließe, dass mich das gelöschte Bild „Miriam in Badewanne.jpg“ nicht interessiert. Zu Testzwecken lasse ich PhotoRec über die freien Bereiche nach gelöschten Bilddateien suchen. Neben etlichen fehlerhaften Dateien zeigt die Vorschau auch noch deutlich mehr Fotos aus dem privaten Umfeld: Urlaubsfotos, Bewerbungsfotos, Bilder von privaten Feiern und Familienfesten. Portraits von allen möglichen Leuten. Bilder vom bunt bemalten Babybauch, Bilder nach der Geburt, beim Babyschwimmen, beim Stillen. Ein Bild oben ohne am Strand. Nichts, was irgendwie verwerflich wäre. Aber auch nichts, was einen Fremden wie mich irgendetwas angeht.

„… verdient jetzt mehr.“

Ich habe mich jetzt nicht einmal eine Stunde mit dem Image des Datenträgers befasst und fühle mich nicht mehr wohl mit dem, was ich schon jetzt weiß. Ich beschließe deshalb, den Fall an dieser Stelle zu schließen und das Image zu wipen.

Auch für mich als Forensiker war das ein spannendes Experiment, denn üblicherweise interessiere ich mich nicht für die Person, die einen Computer besessen hat. Es war erstaunlich, wie schnell ich mir dabei ein relativ gutes Bild von der Persönlichkeit des Computernutzers verschaffen konnte. Ein Krimineller, der bewusst noch tiefer einsteigt, fände problemlos Anknüpfungspunkte für weitere Aktionen: Phishing bei Arbeitskollegen oder Bekannten, Informationen über Konten und vorhandenes Vermögen, etc. Grund genug, seinen Computer nicht aus der Hand zu geben und dafür zu sorgen, dass auch dann nichts passieren kann, wenn das Gerät doch mal verloren geht. (ju) c't