CONTACT

Einen beschlagnahmten Computer begutachten und den Ermittlern antworten

Un ordinateur saisi dans une procédure pénale internationale : treize sources analysées et une réponse point par point aux questions d'un cabinet d'enquête londonien.

Version du 27 novembre 2026 — Imprimé le 27 novembre 2026



Der Kontext

Ein Anwalt aus der Westschweiz vertraut uns die Analyse eines Laptops an, den die Polizei in einem Strafverfahren mit internationaler Dimension beschlagnahmt hat. Wir erhalten eine von den Behörden angefertigte Kopie seiner Festplatte und arbeiten ausschliesslich an dieser Kopie, schreibgeschützt.

Eine erste Analyse betrifft die Dokumente, die E-Mails, den Browserverlauf und die auf der Maschine verwendeten Konten. Der Bericht wird abgeliefert, die Kopie zurückgegeben, und unsere Arbeitsdaten werden vernichtet, wie es das Mandat vorsieht. Das Dossier kommt anschliessend mehrmals wieder.

Die Fragen einer Londoner Ermittlungsfirma

Eine Londoner Ermittlungsfirma, die an dem Fall arbeitet, bringt vor, dieser Computer habe dazu gedient, sich am Server einer Organisation anzumelden. Ihre Ermittler stellen uns ihre Fragen über unseren Auftraggeber. Die Staatsanwaltschaft drängt, man muss schnell und genau antworten: Ist dieses Gerät tatsächlich dasjenige, das in den Verbindungsprotokollen erscheint?

Um darauf zu antworten, braucht es die Hardware-Adresse seiner Netzwerkkarte. Das bei der ersten Analyse eingesetzte Analysewerkzeug extrahiert sie aber nicht. Die Kopie der Festplatte wird beim Anwalt auf einem externen Datenträger wiedergefunden, und wir öffnen das Dossier erneut.

Die gestellten Fragen

Die Ermittler fragen nicht «Was befindet sich auf dieser Festplatte?», sondern nach genauen Punkten, von denen

jeder den Computer mit den beobachteten Verbindungen verknüpfen kann oder nicht:

- die Kennung, die das Microsoft-Verzeichnis einer Organisation einem Gerät zuweist, wenn es sich dort registriert;
- die Hardware-Adresse jeder Netzwerkkarte, aktuell und früher;
- der Name der Maschine und seine allfälligen Änderungen;
- der Verlauf der WLAN-Netzwerke, mit denen sie verbunden war;
- die Verwendung zufälliger Adressen, mit denen ein Gerät seine tatsächliche Adresse in einem Netzwerk verbergen kann.

Die Werkzeuge

Die erste Analyse wurde mit Autopsy durchgeführt, einem freien Forensik-Werkzeug: Dateien, E-Mail, Browsernutzung, Konten, USB- und Bluetooth-Geräte, ausgefüllte Formulare, Downloads. Es gibt die Netzwerkkarten nicht wieder, daher die erneute Bearbeitung.

Dafür wird das Festplattenabbild im EnCase-Format in siebzehn Segmenten mit Arsenal Image Mounter schreibgeschützt eingebunden. Die Registry-Datenbanken werden mit Registry Explorer von Eric Zimmerman gelesen, dem Referenzwerkzeug des Fachs, und anschliessend per Skript abgefragt (python-registry, python-evtx), damit jeder Wert von Dritten wiedergefunden und überprüft werden kann.

Die Tiefe der Untersuchung

Wir bleiben nicht an der ersten Stelle stehen, an der Windows eine Information ablegt. Dreizehn Quellen werden untersucht, jede mit ihrem genauen Ort im Abbild:

- die Hives SYSTEM und SOFTWARE, die Hardware, Netzwerkkarten und die Registrierung in Verzeichnissen beschreiben;
- das Benutzerprofil (NTUSER.DAT), das die mit der Maschine verknüpften Organisationskonten festhält;
- die gespeicherten WLAN-Profile;
- die bei der Installation von Windows zurückgebliebenen Dateien;
- vier Ereignisprotokolle: System, Installation, Anmeldung und Sicherheit.

Die Abgleiche

Ein einzelner Wert beweist wenig. Wir gleichen die Quellen daher untereinander ab: Derselbe Maschinenname, dieselbe Netzwerkkarte und dieselbe Einstellung für zufällige Adressen müssen sich von einer Quelle zur anderen wiederfinden, sonst muss erklärt werden, warum.

Anschliessend gleichen wir ab, was der Computer enthält, mit dem, was die Londoner Firma auf der Serverseite festgestellt hat. Das Präfix einer Hardware-Adresse bezeichnet den Hersteller der Karte. Das des beschlagnahmten Computers stimmt nicht mit dem der beiden in den Verbindungsprotokollen gesehenen Geräte überein. Schliesslich wird die gesuchte Gerätekennung auch im Hive SOFTWARE gesucht, den der Bericht der Firma nach eigener Angabe nicht eingesehen hatte.

Drei technische Details

- **Die Netzwerkkarten** werden im Hive SYSTEM unter ControlSet001\Control\Class\{4D36E972-E325-11CE-BFC1-080 gelesen: ein Unterschlüssel pro installiertem Adapter, mit seinem Treiber, seinem Modell und gegebenenfalls der vom Benutzer festgelegten Adresse.
- **Die Registrierung im Verzeichnis einer Organisation** hinterlässt eine Spur im Benutzerprofil, unter den Einträgen WorkplaceJoin von NTUSER.DAT. Wir haben dort zwei Organisationskonten gefunden, mit dem angegebenen Gerätenamen, aber ohne die gesuchte Kennung.
- **Die ersten drei Bytes einer MAC-Adresse** (die OUI) werden von der IEEE einem Hersteller zugewiesen. Die des beschlagnahmten Computers bezeichnet einen handelsüblichen WLAN-Chip. Die der beiden auf dem Server gesehenen Geräte verweisen auf Karten aus der Profi-Baureihe desselben Computerherstellers.

Was die Analyse belegt

Keine der gesuchten Kennungen erscheint in den dreizehn untersuchten Quellen. Der Computer hat nur eine einzige Netzwerkkarte, und die zufälligen Adressen sind in allen Quellen deaktiviert: Es erscheint keine andere Adresse, unter der er sich hätte melden können. Der Unterschied beim Kartenhersteller gegenüber den auf dem

Server gesehenen Geräten war im Bericht der Firma nicht festgestellt worden.

Wir schreiben, was die Spuren zu behaupten erlauben, und nicht mehr: «Erscheint in keiner untersuchten Quelle» heisst nicht «hat sich nie angemeldet».

Die Lieferungen

- Ein vollständiger Bericht in zwei Teilen: das Vorgehen und die Feststellungen, mit der Quelle jeder Feststellung.
- Eine verdichtete Antwort auf Englisch für die Londoner Firma.
- Eine Darstellung des Berichts der Firma in einfacher Sprache, für den Anwalt und die Staatsanwaltschaft, mit einem Kasten zu jedem technischen Begriff.

Die Namen, die Kennungen und der Inhalt des Dossiers bleiben ausserhalb dieser Seite. Wir stellen das Vorgehen vor, nie die Unterlagen.

Digitale Forensik · Alle Referenzen