CONTACT

Examining a seized computer and answering the investigators

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



The context

A lawyer from French-speaking Switzerland entrusts us with the analysis of a laptop seized by the police in a criminal case with an international dimension. We receive a copy of its disk, made by the authorities, and we work exclusively on this copy, in read-only mode.

A first analysis covers the documents, the email, the browsing history and the accounts used on the machine. The report is delivered, the copy is returned and our working data is destroyed, as the assignment provides. The case then comes back several times.

The questions from a London investigation firm

A London investigation firm working on the case puts forward that this computer was used to connect to an organisation's server. Its investigators put their questions to us through our client. The prosecutor is pressing, so we have to answer quickly and precisely: is this device really the one that appears in the connection logs?

To answer, we need the hardware address of its network card. But the analysis tool used the first time does not extract it. The copy of the disk is found at the lawyer's office, on an external drive, and we reopen the case.

The questions asked

The investigators are not asking "what is on this disk?", but specific points, each of which could link the computer to the connections observed, or not:

- the identifier that an organisation's Microsoft directory assigns to a device when it registers there;

- the hardware address of each network card, current and past;
- the name of the machine, and any changes to it;
- the history of the Wi-Fi networks it has connected to;
- the use of random addresses, which allows a device to hide its true address on a network.

The tools

The first analysis was carried out with Autopsy, a free forensic tool: files, email, browsing, accounts, USB and Bluetooth devices, forms filled in, downloads. It does not report network cards, hence the second pass.

For this, the disk image, in EnCase format in seventeen segments, is mounted read-only with Arsenal Image Mounter. The registry databases are read with Eric Zimmerman's Registry Explorer, the trade's reference tool, then queried by script (python-registry, python-evtx) so that each value can be found and verified by a third party.

The depth of the search

We do not stop at the first place where Windows stores a piece of information. Thirteen sources are examined, each with its exact location in the image:

- the SYSTEM and SOFTWARE hives, which describe the hardware, network cards and registration with directories;
- the user profile (NTUSER.DAT), which keeps the trace of organisation accounts linked to the machine;
- the saved Wi-Fi profiles;
- the files left behind by the Windows installation;
- four event logs: system, setup, logon and security.

The cross-checks

An isolated value proves little. We therefore cross-check the sources against one another: the same machine name, the same network card and the same setting for random addresses must be found from one source to another, or else we have to explain why.

We then cross-check what the computer contains with what the London firm noted on the server side. The prefix of a hardware address designates the card's manufacturer. That of the seized computer does not match that of the two devices seen in the connection logs. Finally, the device identifier sought is also looked for in the SOFTWARE hive, which the firm's report stated it had not consulted.

Three technical details

- **Network cards** are read in the SYSTEM hive, under ControlSet001\Control\Class\{4D36E972-E325-11CE-BFC1-080
one subkey per installed adapter, with its driver, its model and, where applicable, the address set by the user.
- **Registration in an organisation's directory** leaves a trace in the user profile, under the WorkplaceJoin entries of NTUSER.DAT. We found two organisation accounts there, with the device name declared, but not the identifier sought.
- **The first three bytes of a MAC address** (the OUI) are assigned by the IEEE to a manufacturer. That of the seized computer designates a consumer Wi-Fi chip. Those of the two devices seen on the server point to cards fitted in the professional range of the same computer maker.

What the analysis establishes

None of the identifiers sought appears in the thirteen sources examined. The computer has only one network card, and random addresses are disabled in all the sources: no other address under which it might have presented itself appears. The difference in card manufacturer from the devices seen on the server had not been noted in the firm's report.

We write what the traces allow us to assert, and nothing more: "does not appear in any source examined" is not "never connected".

The deliverables

- A full report in two parts: the approach and the findings, with the source of each finding.
- A condensed reply in English for the London firm.
- A plain-language reading of the firm's report, for the lawyer and the prosecutor, with a box for each technical concept.

The names, identifiers and content of the case stay off this page. We present the approach, never the documents.

Digital forensics · All projects