Windows Registry Forensics

اسم الطالب: محمد حيدر مرشد ناصر المعمري

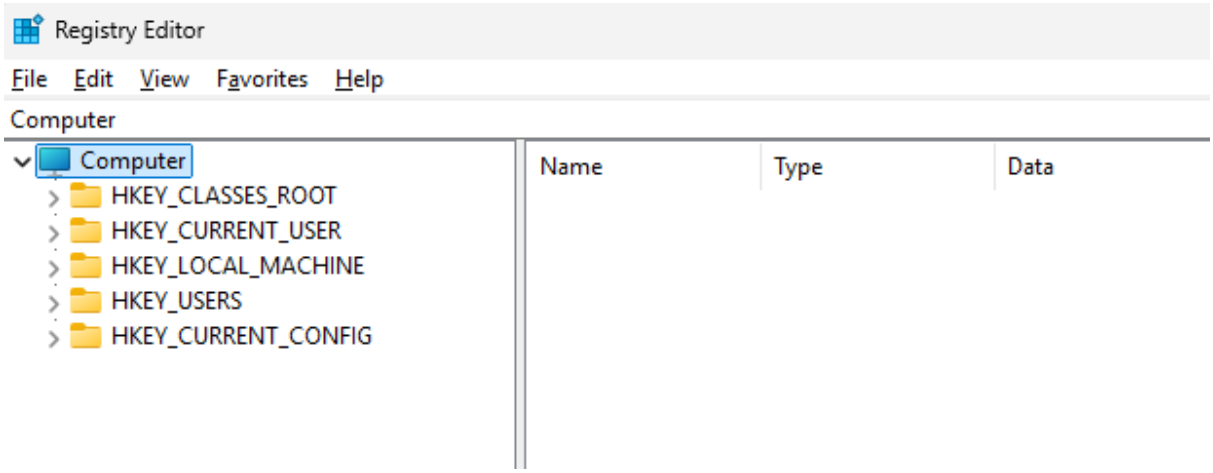
الملخص التنفيذي

يعرض هذا التقرير مساراً تمهيدياً لتحليل سجل Windows باستخدام Registry Editor وFTK Imager وRegistry Explorer. يبدأ بفهم البنية العامة للسجل، ثم اختيار وسيط تخزين وتجهيز ملفات الخلايا، وبعدها مراجعة آثار مثل الحسابات المحلية، التشغيل التلقائي، المستندات الحديثة، البرامج المثبتة، والشبكات والأجهزة الطرفية.

النطاق والمنهجية

- **النطاق:** الصور العشرون المضمنة، بترتيبها الحالي، وما تعرضه من سجل Windows وأدوات جمع الأدلة وتحليل الخلايا.
- **المنهج:** وصف الشاشة، تحديد الأثر الجنائي المحتمل، ثم توضيح حدود الاستنتاج. الخلايا الأساسية مثل `SAM` و`SECURITY` و`SOFTWARE` و`SYSTEM` و`NTUSER.DAT` هي ملفات سجل منفصلة مرتبطة بمجموعات مختلفة من إعدادات النظام والمستخدمين. [1]
- **حدود التقرير:** لم تُقدَّم هنا صورة قرص موثقة أو ملفات الخلايا الأصلية أو سجلات التجزئة؛ لذا لا يمكن تأكيد صحة الأوقات، اكتمال الجمع، أو صحة أي استنتاج يتعلق بحادثة بعينها.

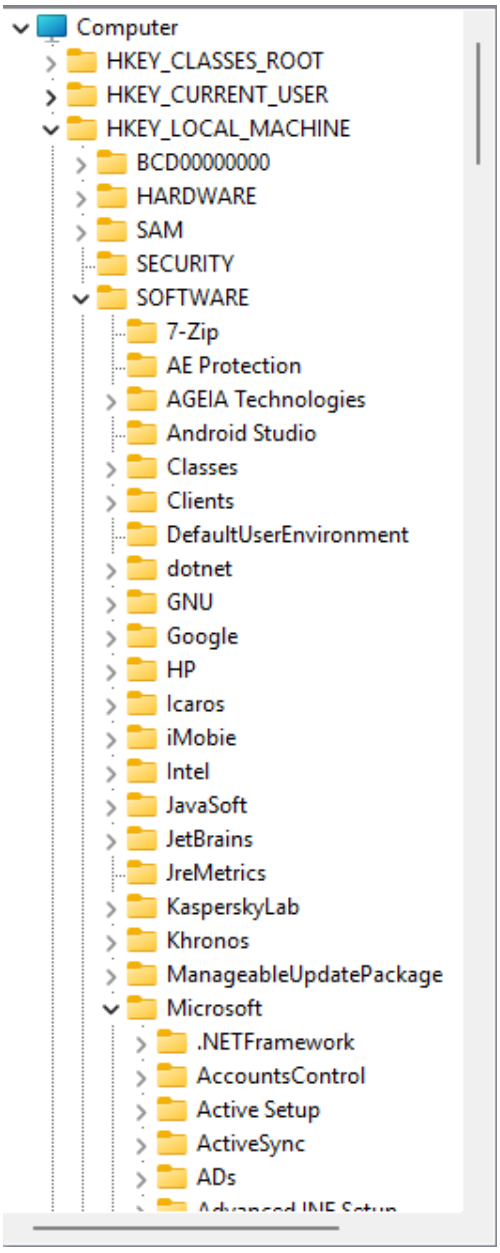
01 — المفاتيح الجذرية في Registry Editor



تعرض الشاشة الجذرية لمحرر السجل، ومنها تبدأ المسارات المنطقية مثل `HKEY_LOCAL_MACHINE` و`HKEY_CURRENT_USER` و`HKEY_USERS`. تمثل هذه الجذور نقاط وصول إلى إعدادات الجهاز أو المستخدم، وليست ملفات مستقلة بحد ذاتها في كل الحالات.

الأهمية: تساعد هذه النظرة على التمييز بين آثار النظام العامة وآثار ملف مستخدم بعينه قبل اختيار الخلية أو المفتاح المراد فحصه. في الفحص الجنائي، ينبغي توثيق المسار كاملاً وعدم الاكتفاء باسم الجذر.

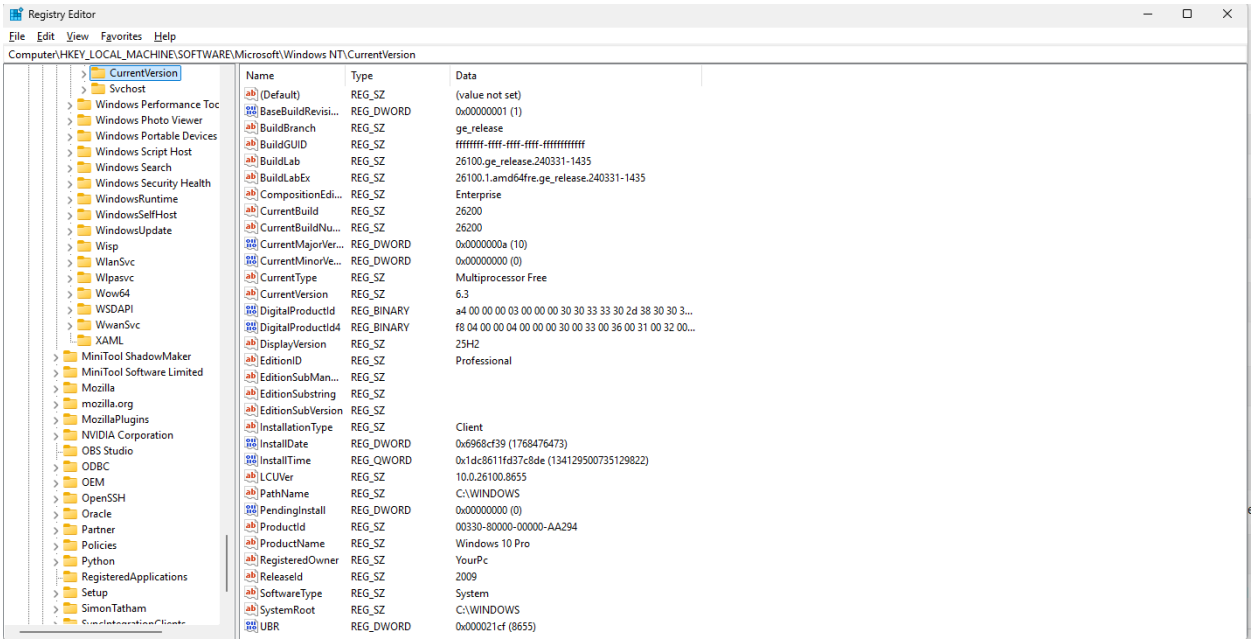
02 — توسيع `HKEY_LOCAL_MACHINE`



تُظهر اللقطة فروعاً تحت `HKEY_LOCAL_MACHINE`، منها `SAM` و`SECURITY` و`SOFTWARE`، إضافةً إلى فروع أخرى كـ`SYSTEM`. ترتبط هذه الخلايا بأنواع مختلفة من بيانات الجهاز: معلومات الحسابات المحلية، إعدادات الأمان، إعدادات البرامج، وإعدادات النظام والخدمات.

الأهمية: توجيه التحليل إلى الخلية المناسبة يختصر البحث، لكنه لا يثبت بحد ذاته وجود حساب أو برنامج مشبوه. تُقرأ المفاتيح ضمن سياق النظام وإصداره ووقت جمع البيانات.

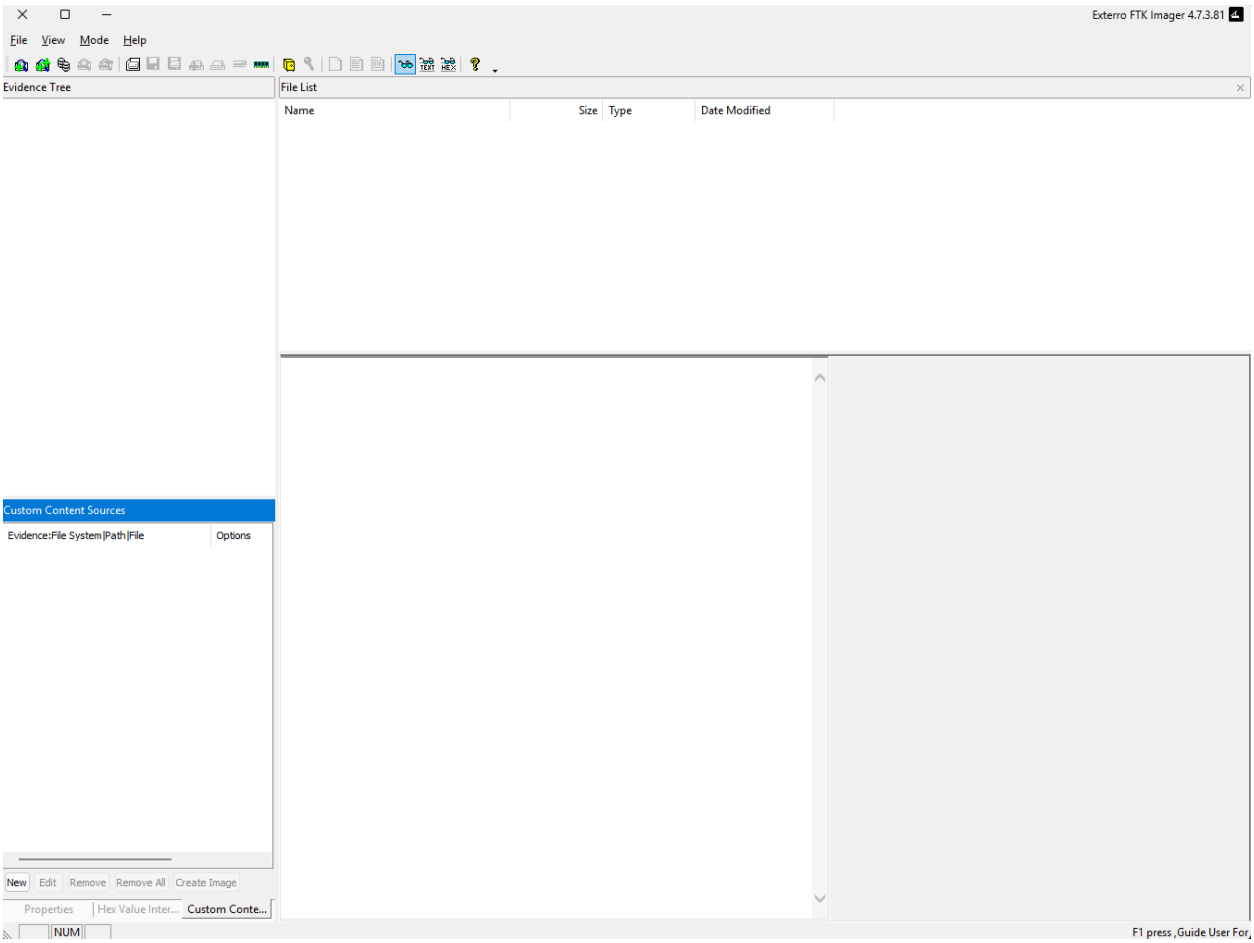
03 — معلومات إصدار Windows عبر `CurrentVersion`



تعرض اللقطة قيماً ضمن مسار `CurrentVersion`، مثل اسم المنتج وإصدار Windows ورقم البناء. يظهر في وصف الصورة نظام Windows 10 Pro؛ ويُستحسن عند إعداد سجل الأدلة تدوين أسماء القيم وبياناتها كما ظهرت، لا الاكتفاء بملخص نصي.

الأهمية: تساعد معلومات الإصدار على وضع بقية الآثار في سياقها، لأن مواضع بعض المفاتيح وسلوكها قد تختلف بين الإصدارات. عند تحليل نسخة غير متصلة، ينبغي تمييز بيانات الخلية المستخرجة عن بيانات النظام الذي يجري عليه التحليل.

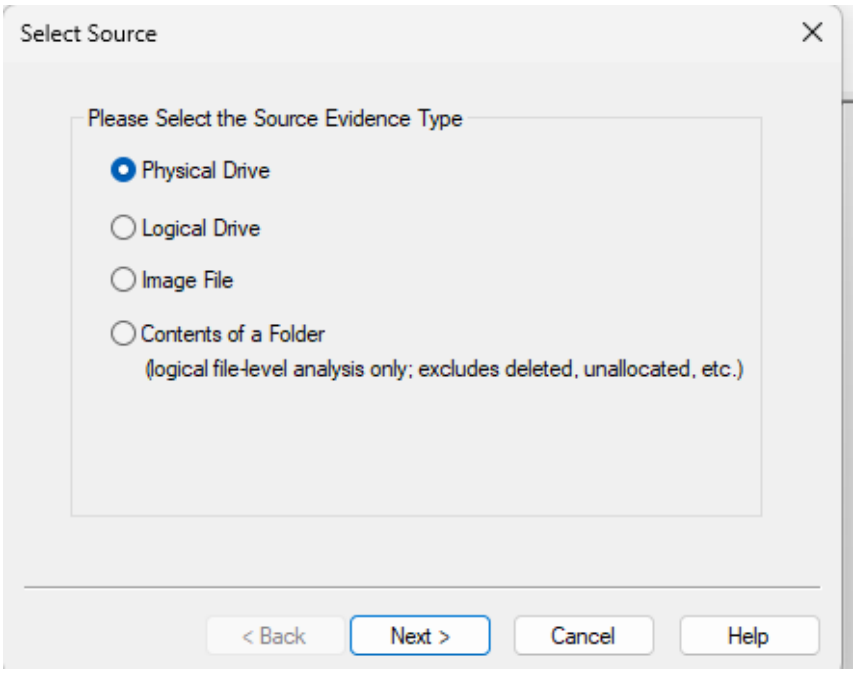
04 — واجهة FTK Imager قبل إضافة مصدر



هذه لقطة لواجهة FTK Imager في حالة البداية. تُستخدم الأداة لمعاينة الأدلة وجمعها وإنشاء صور جنائية؛ وتذكر الشركة أن الأداة تدعم تصوير الأقراص والتحقق بالتجزئة، لكن هذه الشاشة وحدها لا تثبت بدء التصوير أو اكتماله. [2]

نقطة توثيق: سجّل إصدار الأداة، اسم المحقق، وقت بدء العملية، ومعرّف الدليل قبل الانتقال إلى اختيار المصدر.

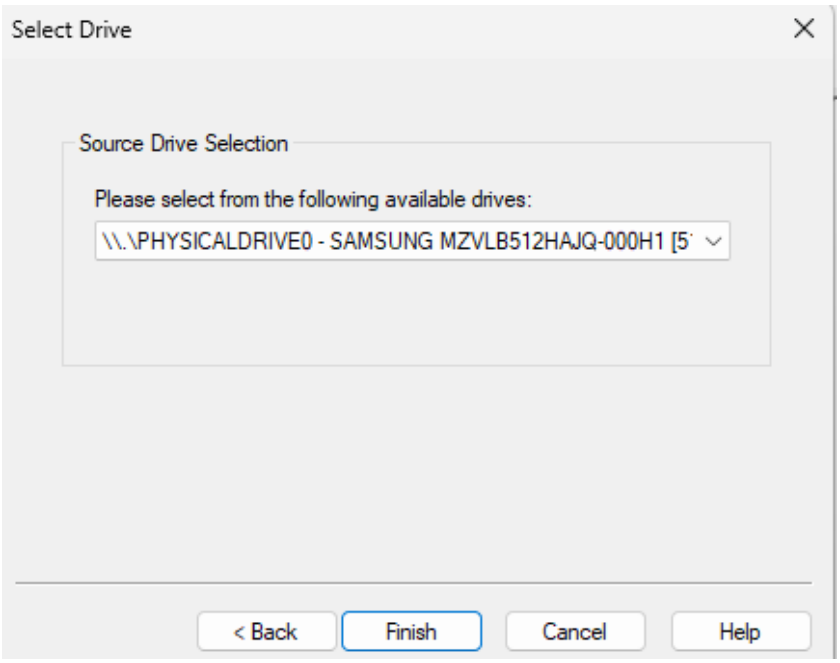
05 — اختيار نوع مصدر الأدلة



تعرض النافذة خيارات مصادر الأدلة، وقد اختير **Physical Drive**. يعني ذلك توجيه الأداة إلى قرص فعلي بدلاً من ملف صورة موجود مسبقاً؛ ولا يعني أن عملية الاستحواذ قد بدأت أو أنها شملت كل القطاعات بالفعل.

الأهمية: الاختيار الصحيح للمصدر شرط لتفادي جمع الجهاز الخطأ. يُفضّل استخدام مانع كتابة مناسب، وتوثيق رقم القرص وسعته وطرازه ورقمه التسلسلي قبل المتابعة.

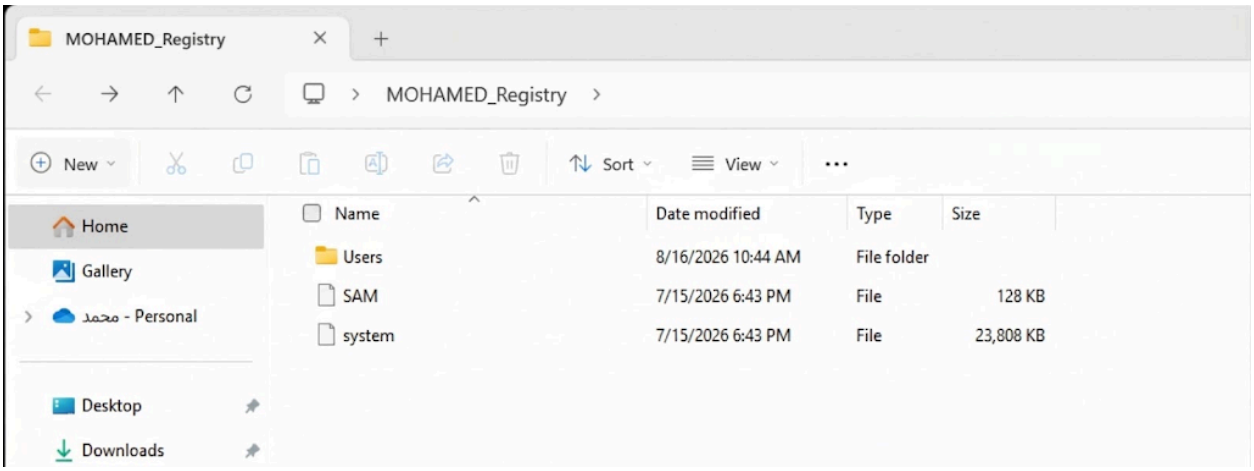
06 — تحديد القرص الفعلي (SAMSUNG)



تُظهر الشاشة اختيار قرص مادي من نوع SAMSUNG. اسم الشركة المصنّعة وحده لا يكفي للتعرّف إلى الدليل؛ ينبغي مطابقة الطراز والسعة والرقم التسلسلي ومعرّف القرص مع سجل الحيازة.

تنبيه: لا تُعدّ لقطة تحديد القرص دليلاً على أن نسخة جنائية قد أُنشئت أو تم التحقق منها. يجب حفظ سجل عملية الجمع ونتائج التجزئة، والعمل لاحقاً على نسخة موثقة لا على الأصل. [2]

07 — مجلد عمل أولي لملفات السجل

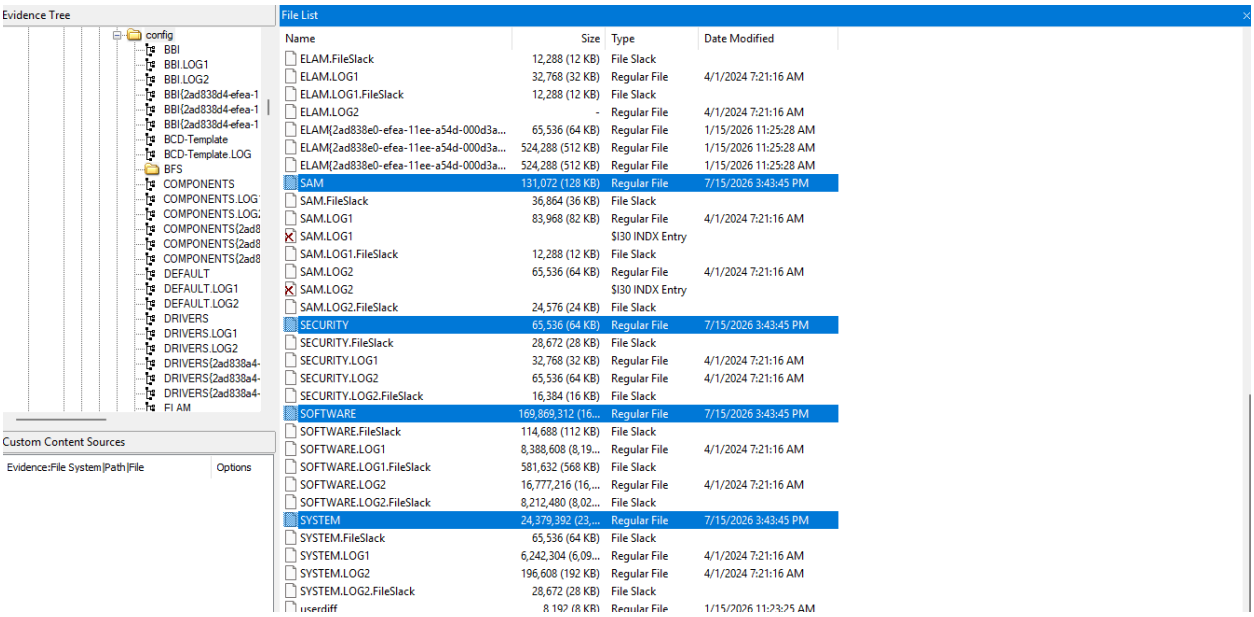


تُظهر نافذة الملفات مجلداً باسم `MOHAMED_Registry` يحتوي على مجلد `Users` وملفي `SAM` و`system`. تبدو هذه لقطة لمجلد عمل أو مرحلة تجهيز أولية، ولا تُظهر بمفردها اكتمال جمع كل

الخلايا.

الأهمية: تنظيم الملفات في مجلد مستقل يساعد على فصل مخرجات التحليل عن النظام المصدر. ينبغي تسجيل مصدر كل ملف ومساره وحجمه وقيمة التجزئة، مع تجنب إعادة تسمية الأدلة بطريقة تفقدها صلتها بالمصدر.

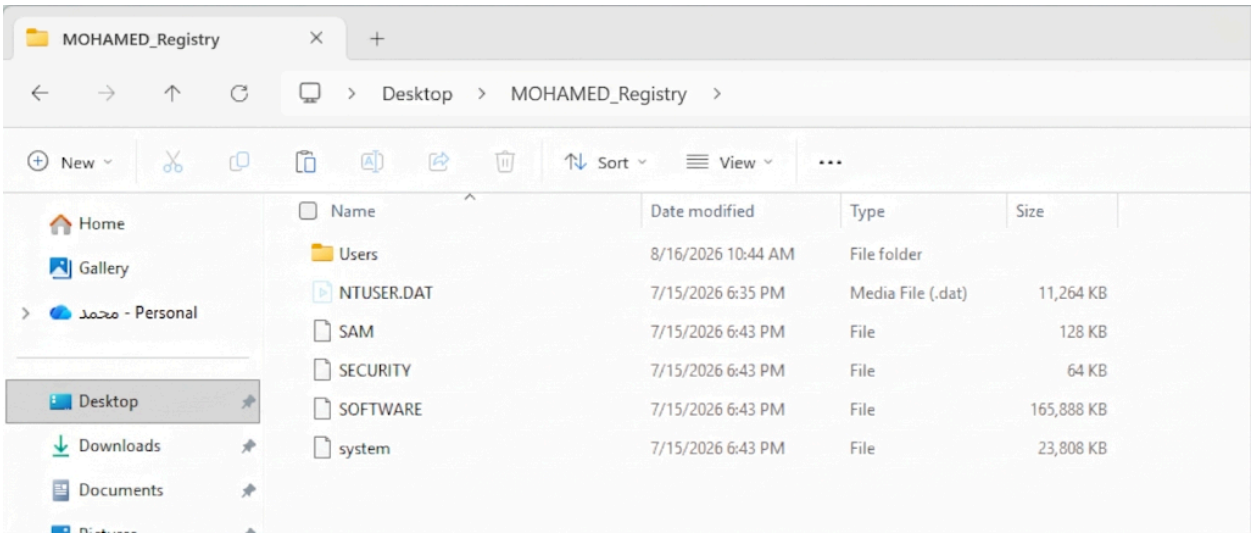
08 — استعراض مجلد `config` في FTK Imager



تُظهر اللقطة محتويات مجلد `config` داخل مصدر الأدلة، مع ملفات السجل الأساسية مثل `SAM` و`SECURITY` و`SOFTWARE` و`SYSTEM`. يُستخدم هذا الاستعراض لتحديد الملفات التي ستُصدَّر للتحليل، مع الحفاظ على نسبتها إلى المصدر الأصلي.

نقطة جنائية: عند نسخ خلايا السجل، لا تُهمل ملفات السجلّات المرافقة (مثل ملفات `LOG.`) إذا كانت موجودة ومطلوبة للتحليل؛ إذ قد تساعد في فهم التغييرات غير المكتوبة بعد إلى ملف الخلية. [1]

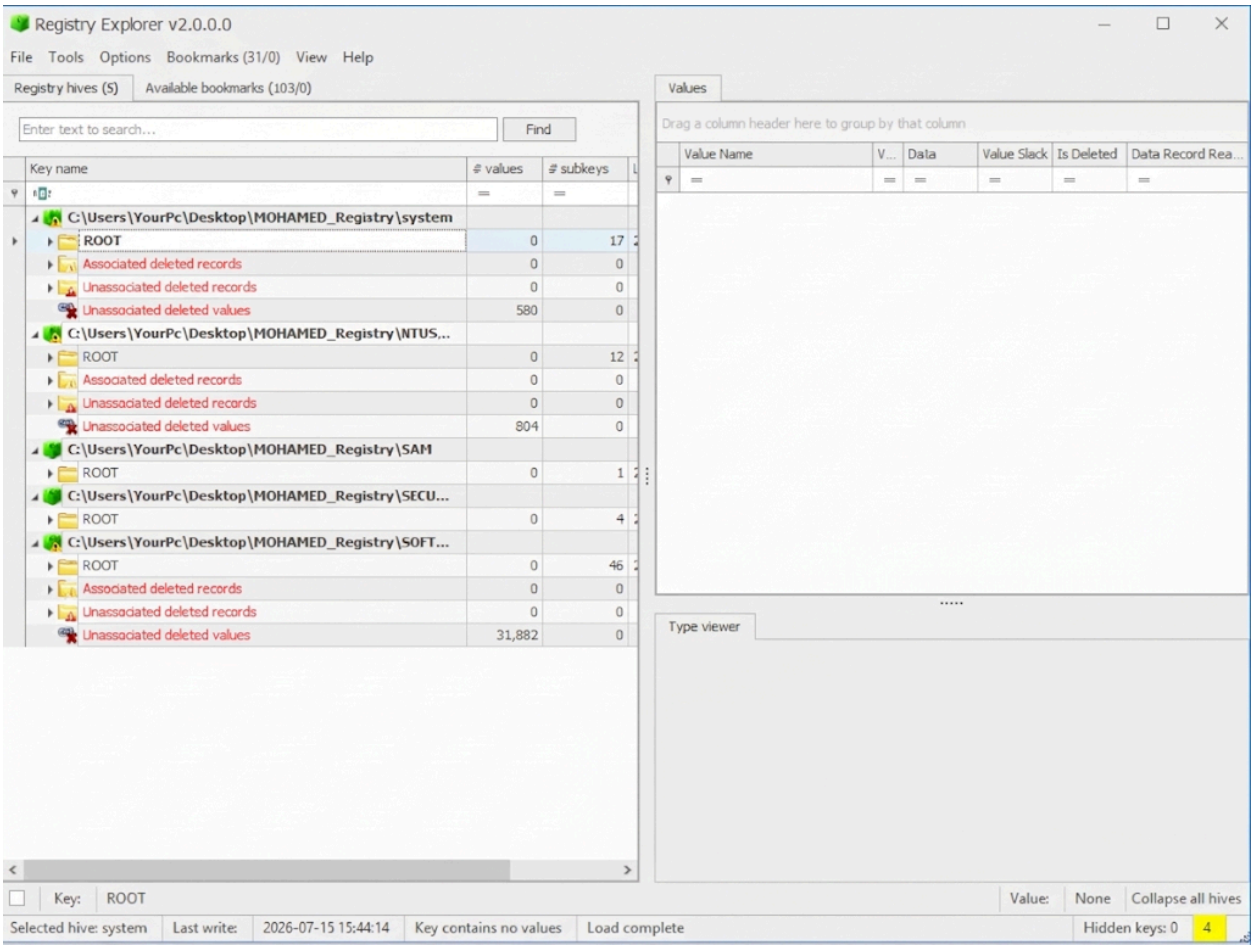
09 — مجموعة الخلايا المستخرجة وملف المستخدم



يعرض المجلد ملفات `NTUSER.DAT` و`SAM` و`SECURITY` و`SOFTWARE` و`system` إلى جانب مجلد `Users`. وجود `NTUSER.DAT` مهم لأنه يخص إعدادات ملف مستخدم، بينما الخلايا الأخرى تمثل نطاقات أوسع من بيانات Windows.

الأهمية: هذه المجموعة تمهّد لتحليل متعدد الخلايا وربط إعدادات النظام بآثار المستخدم. وجود الملفات في المجلد لا يثبت وحده اكتمالها أو سلامتها؛ لذلك تُقارن أحجامها وبصماتها وسجل استخراجها مع المصدر.

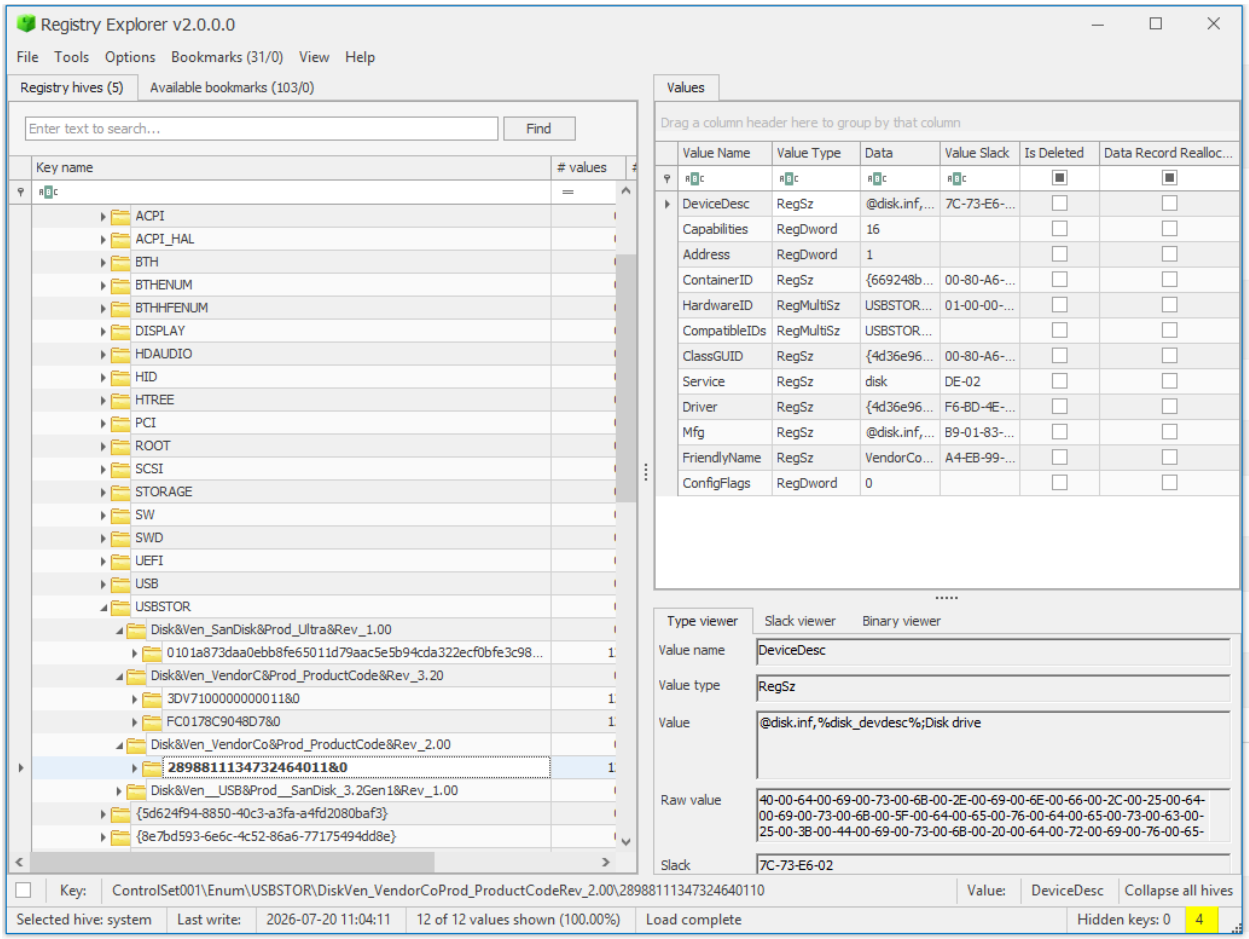
10 — تحميل الخلايا ومراجعة السجلات المحذوفة



تعرض Registry Explorer خمس خلايا محمّلة، وتظهر مجموعات للسجلات المحذوفة المرتبطة وغير المرتبطة. تعرض الواجهة أعداداً للسجلات المسترجعة في بعض الخلايا؛ وهي ناتج تحليل للأداة وليست حكماً بأن تلك السجلات ضارة أو مرتبطة بالحادثة.

كيفية التعامل: سجّل الخلية والمسار والقيمة وتفاصيل الاسترجاع، ثم تحقّق من السياق والبيانات الخام وأي أثر داعم. يوضح دليل Registry Explorer أن الأداة تستطيع استعادة مفاتيح وقيم محذوفة وعرض السجلات التي تعذّر ربطها بمفاتيح نشطة؛ ولذلك يجب وصفها كعناصر مسترجعة تحتاج إلى تحقق، لا كوقائع مؤكدة منفردة. [3]

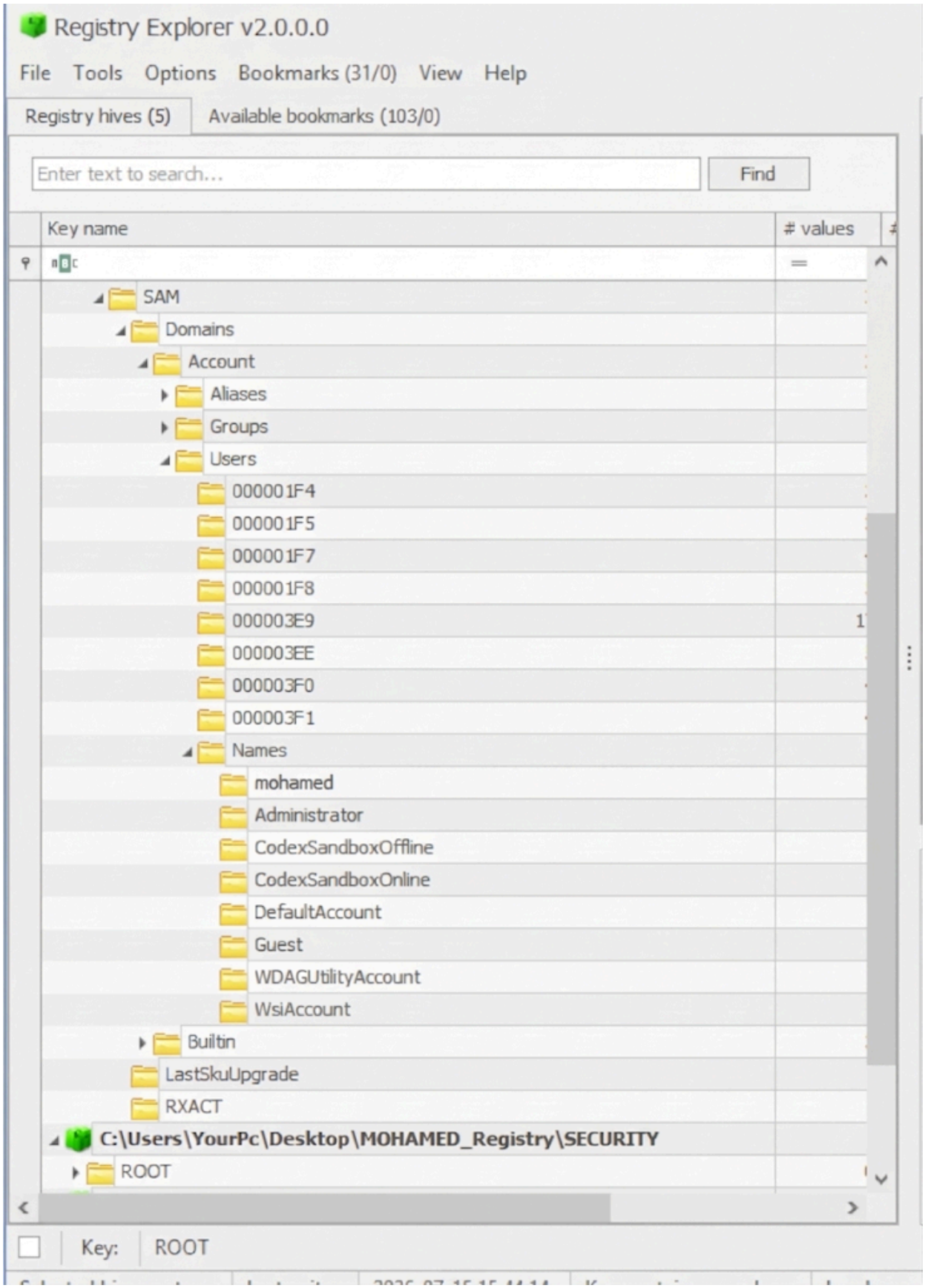
11 — أثر وسيط USB في `USBSTOR`



تُظهر اللقطة فحص مسار `USBSTOR` في خلية `SYSTEM` وبيانات مرتبطة بوسيط تخزين SanDisk. قد تساعد هذه الآثار في تحديد أن Windows تعرّف على جهاز تخزين، وقد تتضمن معرّف الجهاز أو الطراز بحسب القيم المتاحة.

حدود الاستنتاج: وجود أثر للجهاز لا يثبت وحده نقل ملفات أو نسخ بيانات. اربط معرّفات الجهاز وأوقاته بسجلات النظام، وآثار الملفات، وأي سجلات أخرى ذات صلة قبل استنتاج الاستخدام.

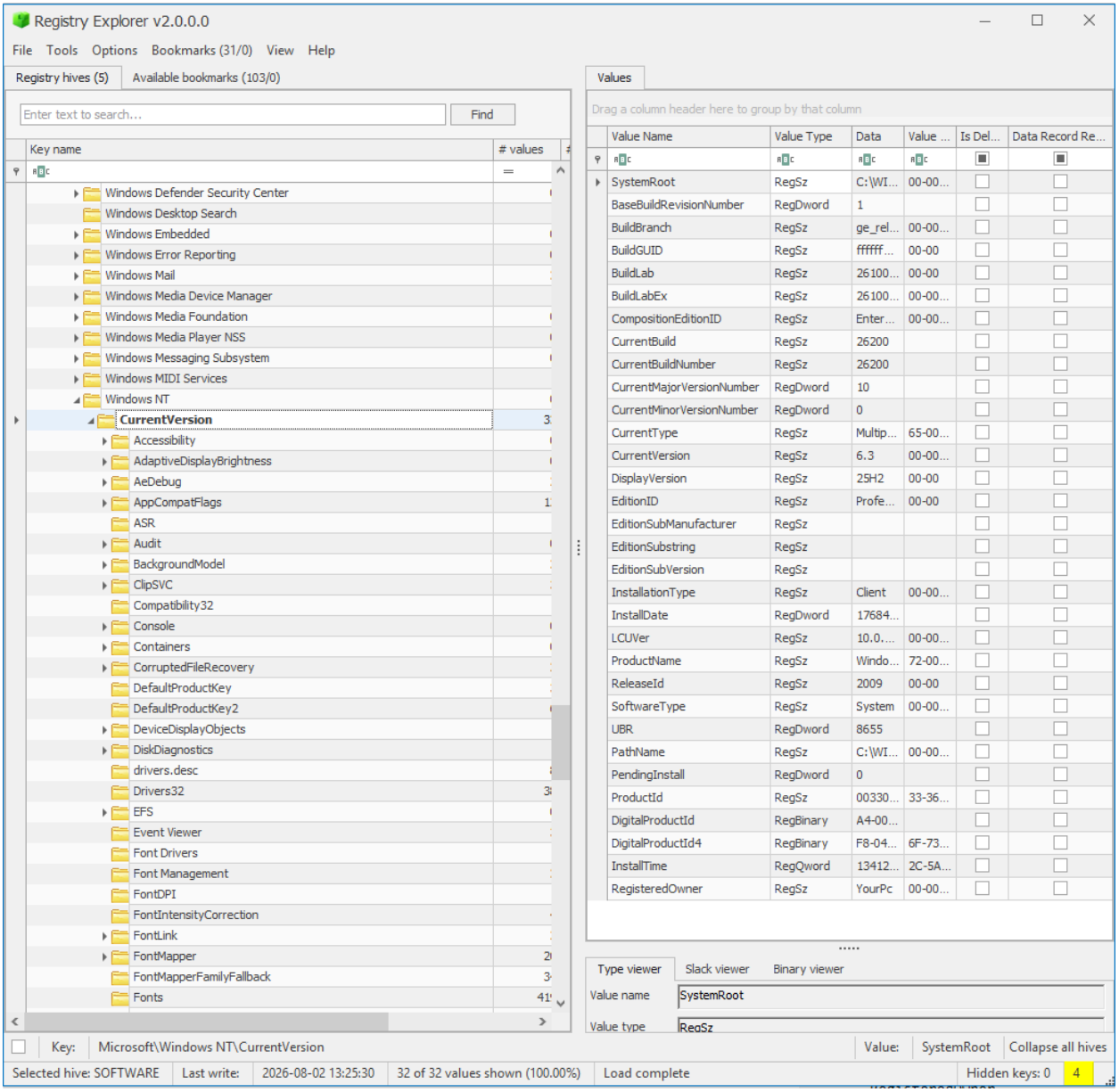
12 — حسابات المستخدمين في خلية `SAM`


Registry Explorer v2.0.0.0
File Tools Options Bookmarks (31/0) View Help
Registry hives (5) Available bookmarks (103/0)
Enter text to search...
Find
Key name
values
SAM
Domains
Account
Aliases
Groups
Users
000001F4
000001F5
000001F7
000001F8
000003E9
000003EE
000003F0
000003F1
Names
mohamed
Administrator
CodexSandboxOffline
CodexSandboxOnline
DefaultAccount
Guest
WDAGUtilityAccount
WsiAccount
Builtin
LastSkuUpgrade
RXACT
C:\Users\YourPc\Desktop\MOHAMED_Registry\SECURITY
ROOT
Key: ROOT

تعرض الشاشة بنية `SAM\Domains\Account\Users\Names` وأسماء حسابات محلية، ومنها `mohamed` و`Administrator` و`Guest` وحسابات نظام أخرى. تظهر أيضاً مفاتيح فرعية ذات معرّفات رقمية؛ ويمكن تحليلها مع أسماء الحسابات وRIDs لتكوين صورة أدق عن الحسابات المسجلة.

الأهمية: يفيد الحصر في ملاحظة الحسابات غير المتوقعة أو الحسابات التي تستحق مراجعة إضافية. لكن وجود اسم حساب في الخلية لا يثبت أنه استُخدم خلال فترة الحادث، كما أن بعض الحسابات الظاهرة قد تكون حسابات Windows مدمجة أو حسابات خدمة.

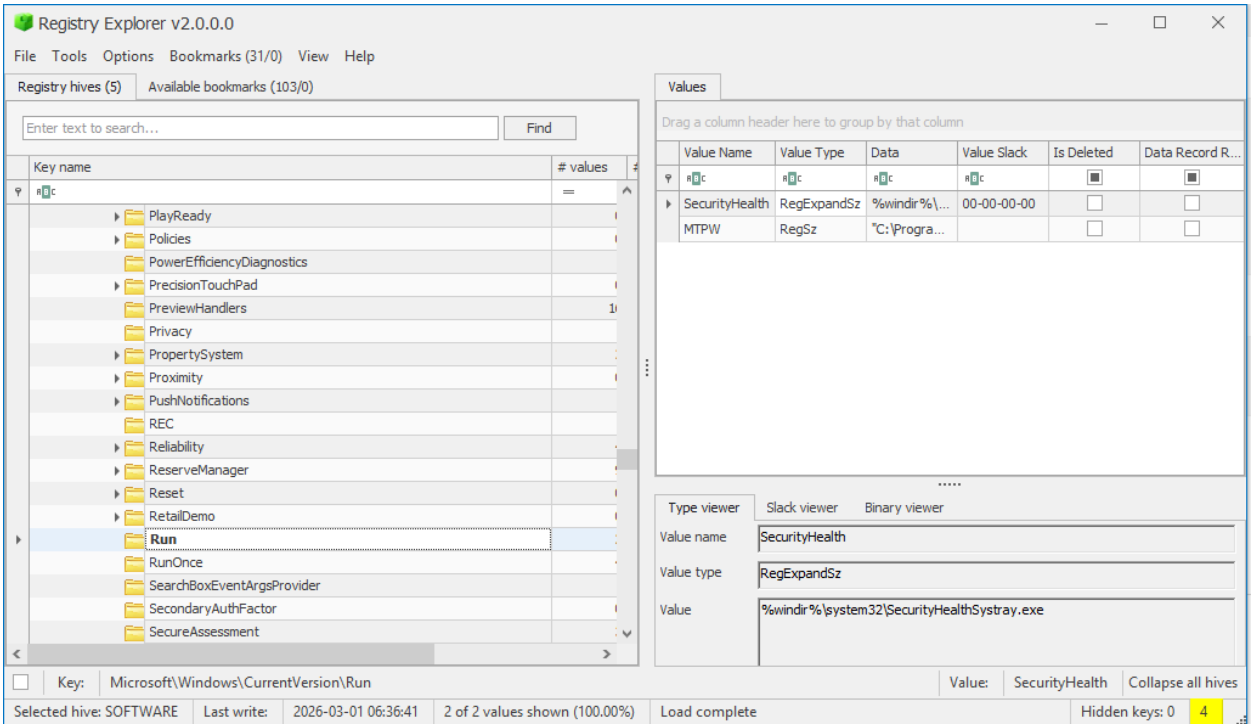
13 — التحقق من إصدار النظام في الخلية المستخرجة



تعرض Registry Explorer قيماً من `SOFTWARE\Microsoft\Windows NT\CurrentVersion`، مثل اسم المنتج والبناء ومسار النظام وتاريخ التثبيت بحسب القيم الظاهرة. تكرار فحص معلومات الإصدار في الخلية المستخرجة يساعد على تأكيد سياق الدليل ومقارنته بما ظهر في Registry Editor.

نقطة توثيق: سجّل المسار الدقيق وأسماء القيم ونصوصها كما تظهر، وميّز بين تاريخ تثبيت النظام ووقت آخر كتابة للمفتاح؛ فهما ليسا بالضرورة التاريخ نفسه.

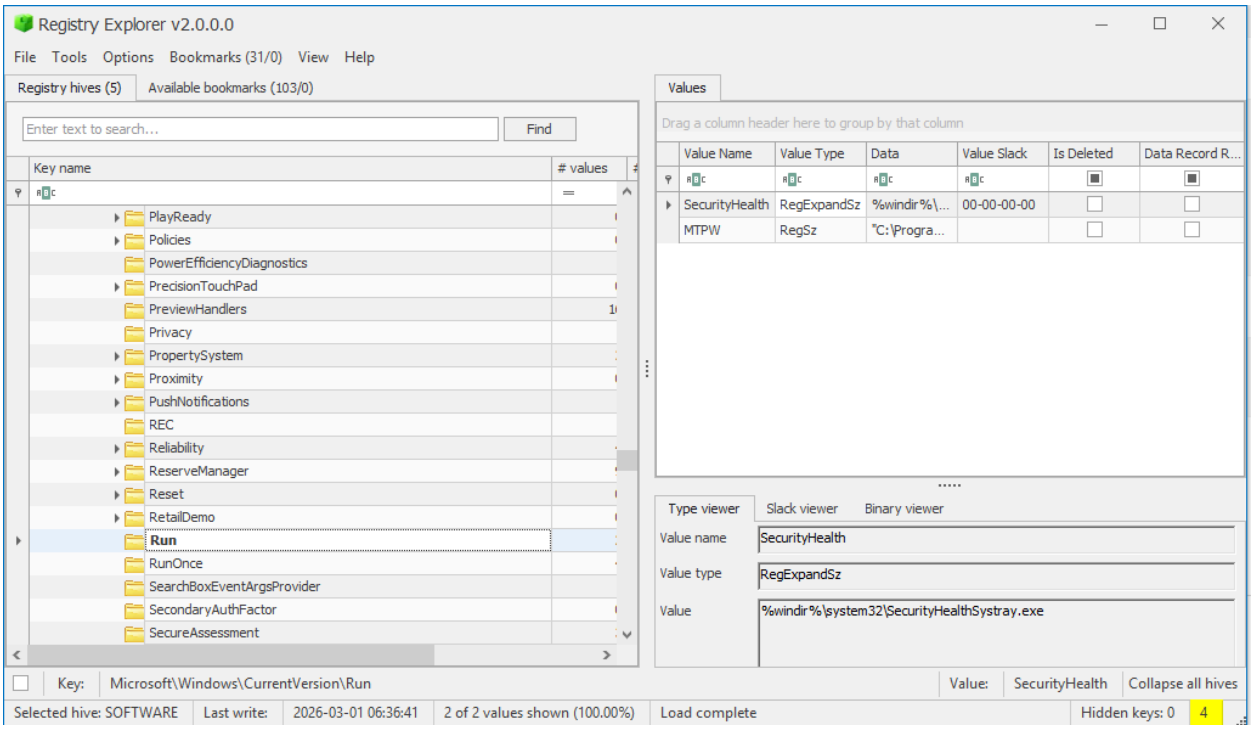
14 — عناصر التشغيل التلقائي في `Run`



تتناول الصورة مسار `Run` في خلية `SOFTWARE`، وهو من المواضع التي تُراجع لفهم البرامج المسجلة للتشغيل عند تسجيل الدخول. تشرح Microsoft أن مفاتيح `Run` يمكن إعدادها على مستوى الجهاز أو المستخدم، وأن البرنامج المسجل فيها يُشغَّل عند تسجيل الدخول وفق سلوك Windows. [4]

ما ينبغي فحصه: اسم القيمة، سطر الأوامر كاملاً، مسار الملف، الناشر والتوقيع الرقمي، نطاق المفتاح (الجهاز أو المستخدم)، وملاءمة البرنامج لبيئة الجهاز. وجود قيمة تشغيل تلقائي ليس دليلاً منفرداً على البرمجية الخبيثة.

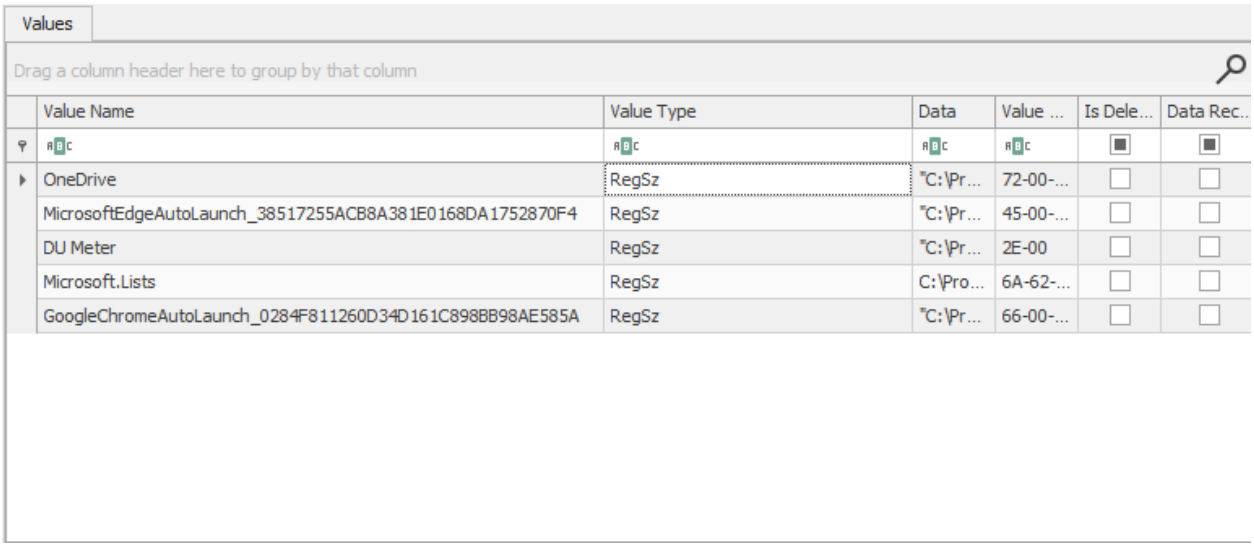
15 — عناصر التشغيل لمرة واحدة في `RunOnce`



تركز هذه اللقطة على `RunOnce`. بخلاف `Run`، يُستخدم هذا المفتاح عادةً لأمر يُنفَّذ مرة واحدة ثم تُزال قيمته؛ وتوضح Microsoft أن القيمة تُحذف افتراضياً قبل تشغيل الأمر، مع استثناءات مرتبطة ببادئات معينة. قد يكون المفتاح طبيعياً في عمليات التثبيت أو الإعداد، لذلك يلزم فحص الأمر وتاريخه وسياقه قبل تفسيره. [4]

قيمة التحقيق: إذا لم تعد القيمة موجودة، فقد تكون هناك آثار أخرى أو سجلات سابقة لازمة لإثبات وجودها؛ عدم ظهورها في لقطة حالية لا ينفي أنها كانت موجودة في وقت سابق.

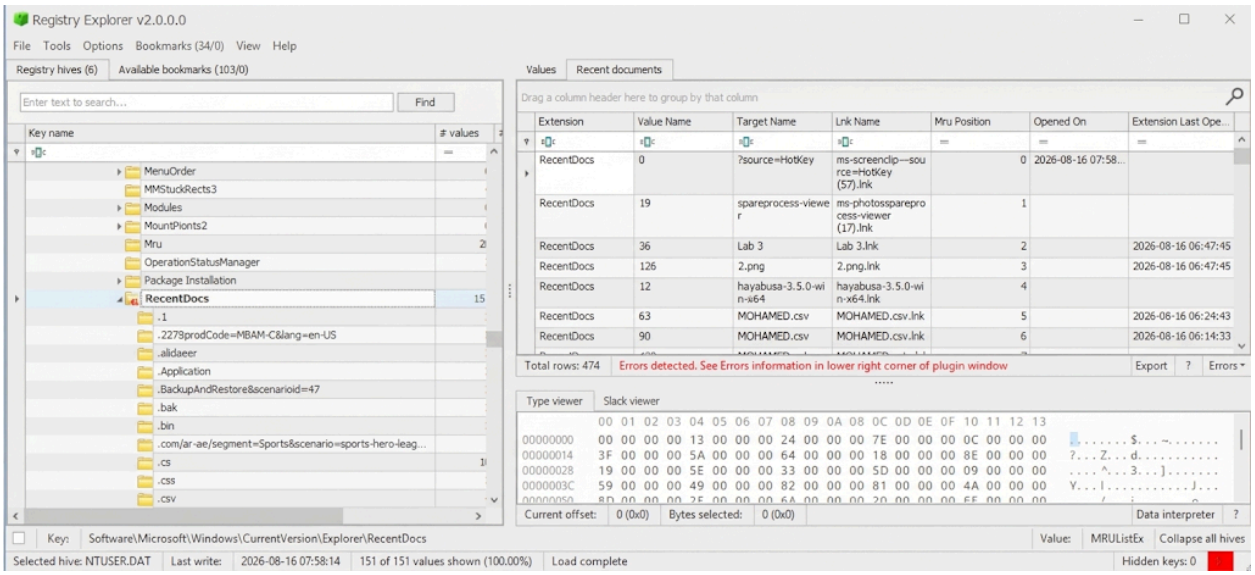
16 — مراجعة تطبيقات بدء التشغيل (AutoLaunch)



تُظهر الصورة قيماً مرتبطة بتشغيل تطبيقات مثل Edge وChrome وOneDrive. وجود تطبيقات معروفة لا يعفي من التحقق؛ فالمهم هو مسار التنفيذ، والوسائط الممرّرة إلى البرنامج، وهوية الملف الفعلية، ومصدر القيمة وتاريخها.

خطوات التحقق: قارن المسار بالمسارات المتوقعة، افحص التوقيع والتجزئة، وابحث عن أسماء ملفات أو معاملات غير مألوفة. لا تُصنّف التطبيق على أنه خبيث لمجرد أنه يعمل تلقائياً.

17 — المستندات الحديثة `RecentDocs`

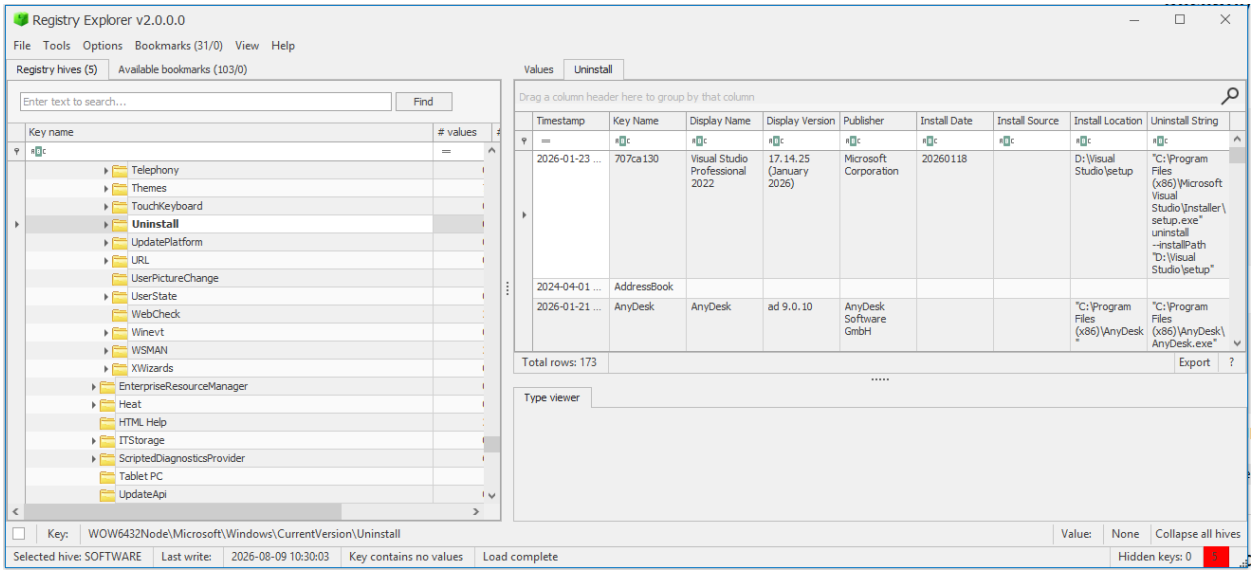


تعرض اللقطة مفتاح `RecentDocs` ضمن خلية `NTUSER.DAT` مع بيانات أسماء ملفات أو اختصارات وترتيب MRU وحقول زمنية ظاهرة في الواجهة. يمكن لهذه الآثار أن تساعد في بناء تصور عن

تفاعل ملف المستخدم مع أنواع من الملفات، مع ضرورة التمييز بين أثر قائمة حديثة وبين إثبات فتح محتوى الملف أو قراءته فعلياً.

التحليل الزمني: سجّل المنطقة الزمنية ومصدر الوقت، ثم قارن القيم مع آثار أخرى مثل ملفات الاختصار وسجلات النظام. قد تتأثر القوائم بالتنظيف أو سياسات الخصوصية أو استخدام تطبيقات مختلفة، فلا يُفترض أنها سجل كامل لكل الملفات.

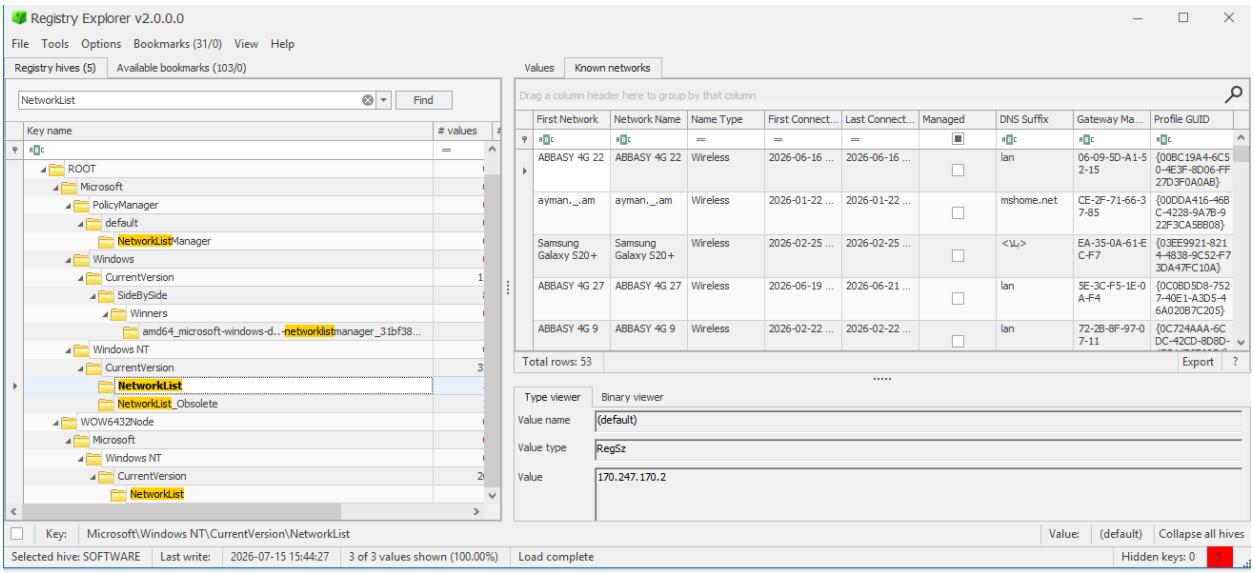
18 — البرامج المسجلة ضمن `Uninstall`



تستعرض الصورة بيانات البرامج المثبتة المسجلة في `Uninstall`، مثل الاسم والناشر وتاريخ التثبيت، وقد أشير في وصف الصورة إلى AnyDesk. هذه المعلومات مفيدة لإعداد قائمة بالبرامج التي تستحق التحقق، خصوصاً أدوات الوصول عن بُعد.

حدود الاستنتاج: تسجيل برنامج في قائمة الإزالة لا يثبت أنه شُغّل أو استُخدم للسيطرة على الجهاز. تحقق من النسخة ومسار التثبيت وحساب المستخدم وسجلات التشغيل، وقارنها بسياسة الاستخدام المشروعة.

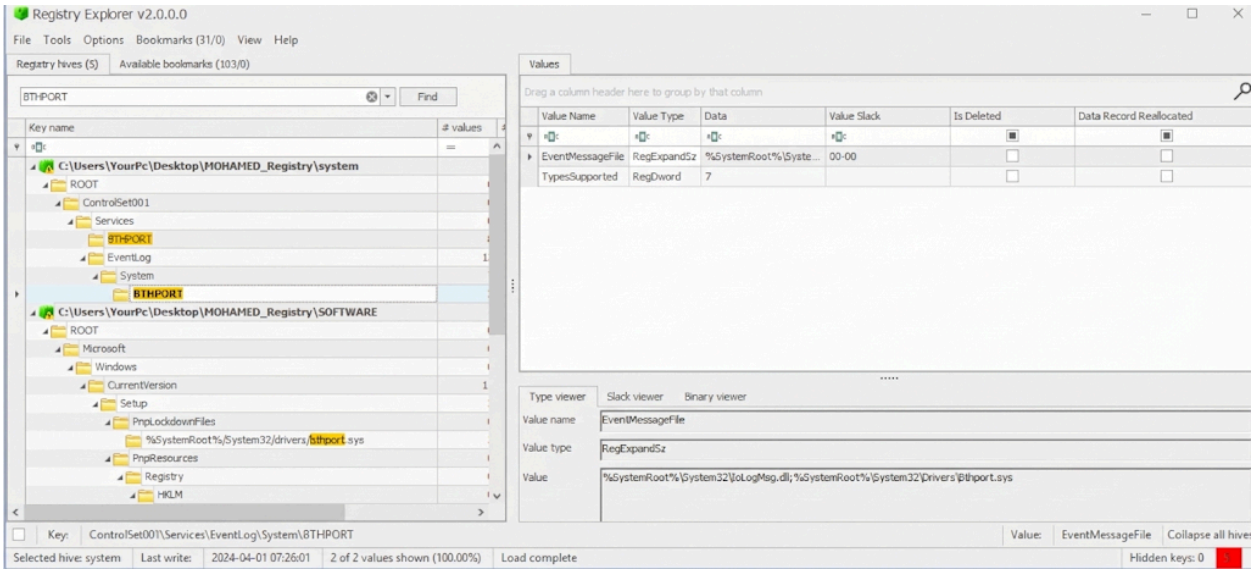
19 — الشبكات المعروفة في `NetworkList`



تعرض اللقطة سجلات شبكات معروفة في `NetworkList` وما يرتبط بها من أوقات أول أو آخر اتصال بحسب البيانات المتاحة. يمكن أن تساعد أسماء الشبكات ومعرّفات ملفاتها في ربط الجهاز بسياق شبكي أو زمني.

تنبيه تفسيري: اسم شبكة محفوظ لا يثبت موقع الجهاز الجغرافي ولا أن الاتصال وقع في لحظة الحادث. قارِن الأوقات مع سجلات WLAN وDHCP والجدار الناري، وراعِ اختلاف المنطقة الزمنية أو انحراف ساعة النظام.

20 — البحث عن `BTHPORT` وآثار Bluetooth



تُظهر نافذة Registry Explorer البحث عن `BTHPORT` في خلية `SYSTEM`، مع ظهور مسارات مرتبطة بخدمات Bluetooth ومصدر أحداث النظام، وقيم مثل `EventMessageFile` و`TypesSupported`. توضح النتيجة مواضع إعدادات أو مكونات مرتبطة بخدمة Bluetooth؛ ولا تكفي وحدها لإثبات اقتران جهاز بعينه أو نقل بيانات عبره.

للتوسّع: ابحث عن آثار الأجهزة المقترنة ومعرّفاتها في المسارات المناسبة، ثم اربطها بسجلات الأحداث وملفات المستخدم والأوقات ذات الصلة. يجب الفصل بين إعداد الخدمة العام وبين أثر اتصال محدد.

خلاصة النتائج وحدودها

توضح الصور مساراً تعليمياً من تحديد البنية العامة للسجل، إلى تجهيز ملفات الخلايا وتحميلها في Registry Explorer، ثم مراجعة آثار قد تفيد في التحقيق: الحسابات، أجهزة USB وBluetooth، التشغيل التلقائي، المستندات الحديثة، البرامج المثبتة، والشبكات المعروفة. أقوى قيمة لهذه الآثار تظهر عند ربطها ببعضها وبمصادر مستقلة، لا عند تفسير مفتاح منفرد بمعزل عن السياق.

لا تسمح الصور وحدها بالجزم بوقوع اختراق أو سرقة بيانات أو تشغيل برنامج ضار. يلزم فحص الدليل الأصلي أو نسخة جنائية موثقة، والتحقق من القيم وسياقها الزمني، ومضاهاة النتائج بآثار مستقلة.

قائمة تحقق للتوثيق المهني

- سجّل رقم القضية/الدليل، الجهة المستلمة، أسماء المحققين، أوقات الاستلام والجمع، والمنطقة الزمنية.
- وثّق طراز القرص وسعته ورقمه التسلسلي ومصدره، واستخدم مانع كتابة عند الاقتضاء.
- احتفظ بسجل الأداة وإصدارها وخيارات الجمع، وأرفق تقرير التصوير ونتائج SHA-256 قبل التحليل وبعده متى كانت متاحة. يدعم FTK Imager إنشاء صور جنائية وتقارير تحقق بالتجزئة.
- حلّل نسخة عمل، وحافظ على الأصل دون تعديل، واحتفظ بملفات السجلّات المصاحبة للخلايا عند الحاجة.
- لكل أثر، دوّن الخلية والمسار واسم القيمة ونوعها وبياناتها وتوقيتها ومصدر التوقيت، ثم أضف تفسيراً ودرجة ثقة وحدوداً واضحة.
- اربط آثار Registry بمصادر أخرى مثل سجلات الأحداث والملفات والاختصارات وسجلات الشبكة؛ لا تجعل قرينة منفردة نتيجة نهائية.