تقرير التحليل الجنائي الرقمي إنشاء صورة قرص وفحصها

اعداد الطالب: محمد حيدر مرشد ناصر المعمري

1. الملخص التنفيذي

يوثق هذا التقرير ما تعرضه لقطات الشاشة: وحدة التخزين TESTING (Z:) بنظام NTFS، ونافذة تصغير حجم، واختيار Z:\ - TESTING [NTFS] كمصدر Logical Drive في FTK Imager. تُظهر الصور اختيار E01، وحفظ الصورة في D:\mohammedTesting باسم Test_Drive، ونتيجة تحقق للملف test.E01 بعدد 4,192,256 قطاعاً؛ كما تعرض تطابق MD5 وSHA1 ونتيجة Match وعدم وجود كتل تالفة. وفي Autopsy تظهر القضية Forensic_Lab_1 ومصدر البيانات Host Test_Drive.E01_1 و19 نتيجة في File System. يقتصر التقرير على المعلومات الظاهرة في الصور، ولا يفترض خطوات أو نتائج غير موثقة فيها.

2. المقدمة

يعرض هذا التقرير تسلسل العمل كما يظهر في لقطات الشاشة: تحديد وحدة TESTING (Z:) بنظام NTFS كمصدر Logical Drive في FTK Imager، اختيار صيغة E01 وإعداد الوجهة، ثم عرض نتيجة التحقق. وتعرض الصور بعد ذلك إنشاء قضية في Autopsy، اختيار Disk Image or VM File وإضافة المصدر من D:\mohammedTesting، ثم عرض قائمة Data Sources ونتائج File System.

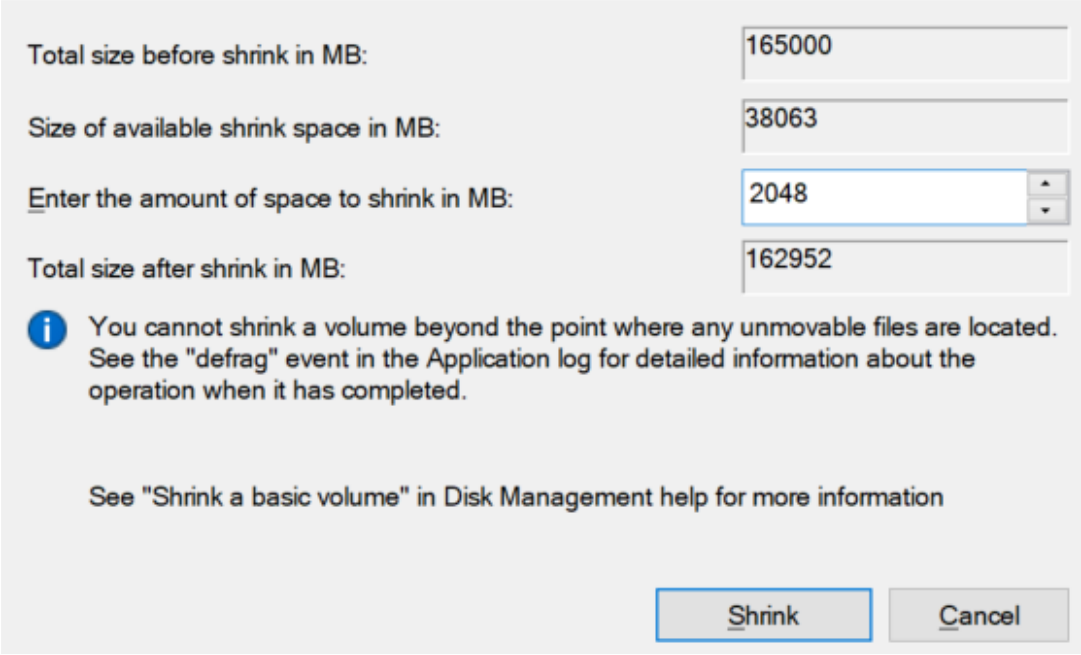
3. بيئة العمل

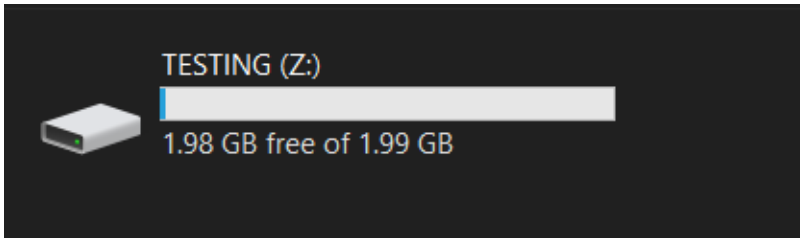
العنصر	القيمة
نظام التشغيل	Windows
أداة الاستحواذ	FTK Imager
أداة التحليل	Autopsy
القرص المصدر	`Z:\\ - TESTING [NTFS]`
مسار الحفظ	D:\mohammedTesting
المنطقة الزمنية	Asia/Riyadh (GMT+3:00)

4. المرحلة الأولى: الاستحواذ على القرص (Disk Imaging)

4.1 نافذة تصغير وحدة التخزين (Shrink Volume)

تُظهر نافذة إدارة الأقراص القيم التالية: الحجم قبل التصغير 165000 MB، والمساحة المتاحة للتصغير 38063 MB، والكمية المُدخلة للتصغير 2048 MB، والحجم بعد التصغير 162952 MB. كما يظهر تحذير Windows بشأن الملفات غير القابلة للنقل. اللقطة تعرض النافذة وخياري Shrink وCancel، ولا تثبت وحدها أن زر Shrink ضُغط أو أن العملية اكتملت.





4.2 الملفات الظاهرة على وحدة TESTING (Z:)

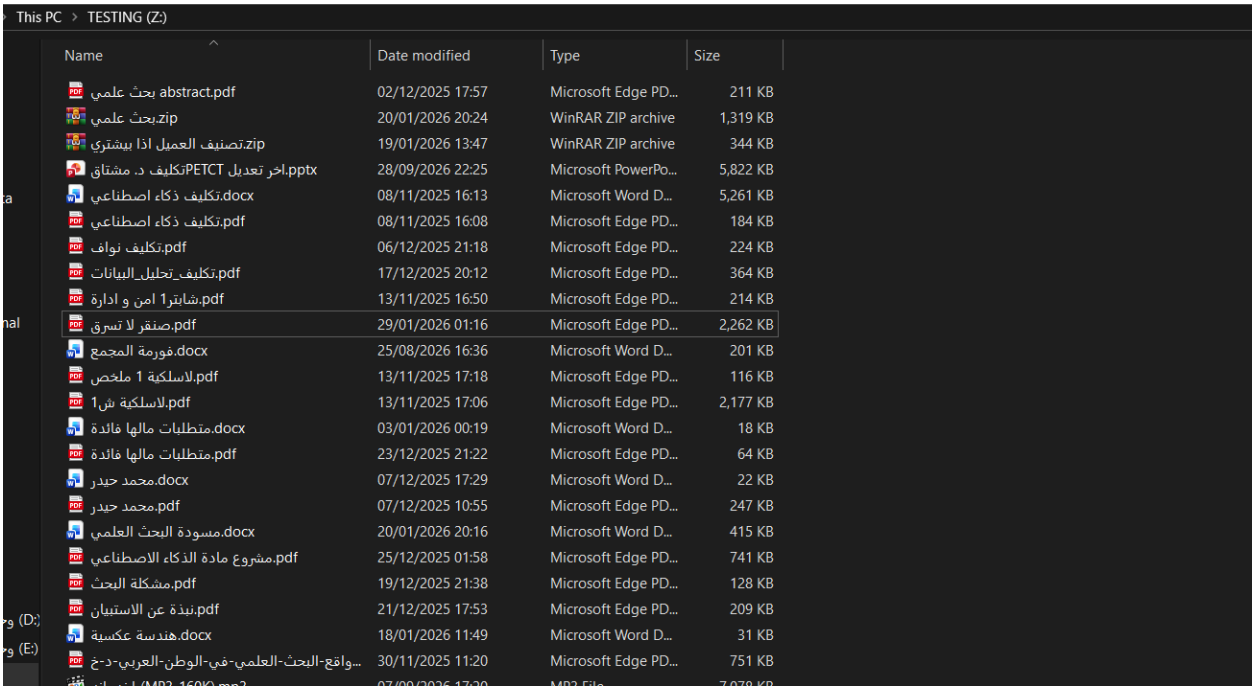
ما تظهره اللقطات:

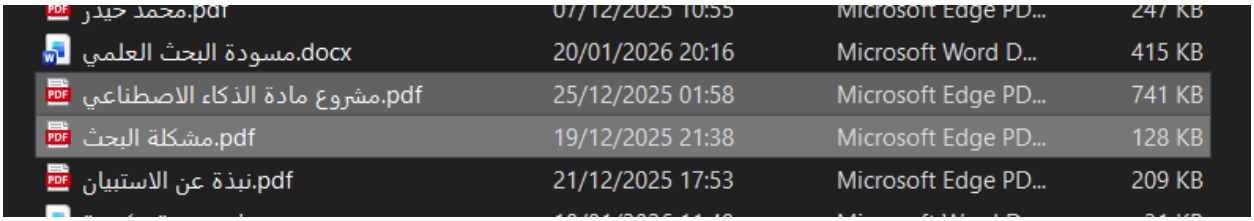
تُظهر لقطة مستكشف الملفات الوحدة باسم TESTING (Z:) وبمساحة 1.99 GB، منها 1.98 GB متاحة.
تظهر في قائمة الملفات عناصر بصيغ PDF وZIP وPPTX وDOCX، كما يظهر جزء من صف ملف MP3 أسفل اللقطة.
اللقطات لا توثق نسخ الملفات أو تحديد ملفات للحذف أو إفراغ سلة المحذوفات.

التحليل:

المحتوى المرئي في اللقطات يثبت وجود ملفات متعددة على TESTING (Z:)، ومن الأنواع المقروءة بوضوح PDF وZIP وPPTX وDOCX. لا يمكن تحديد العدد الكامل للملفات أو تأكيد إجراء حذفٍ أو إفراغ سلة المحذوفات من لقطات مستكشف الملفات وحدها.

تُستخدم هذه اللقطات هنا لتوثيق أسماء الملفات وأنواعها الظاهرة على الوحدة، لا لإثبات كيفية إنشاء الملفات أو حذفها. أما نتائج Autopsy الظاهرة لاحقاً فتُسرد كما تظهر في نافذة File System، دون نسبها إلى طريقة استعادة محددة.



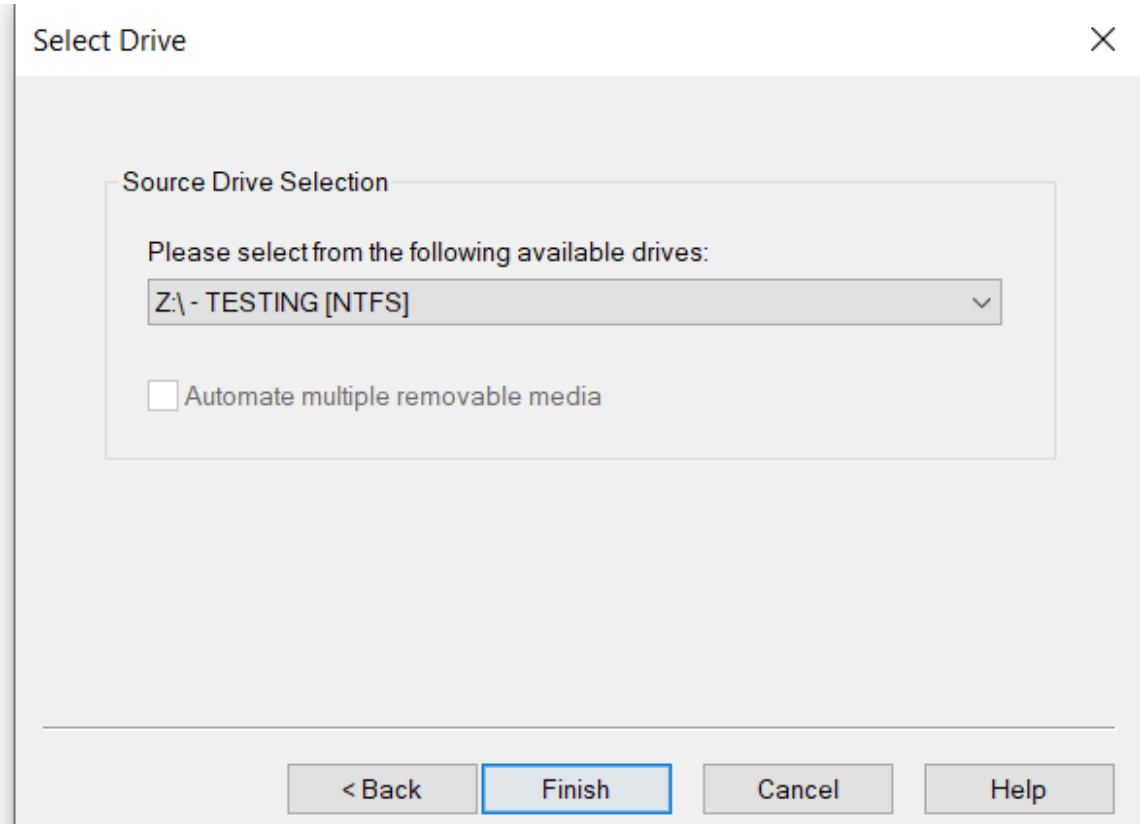


4.3 تحديد المصدر وإعداد صورة القرص (FTK Imager)

ما تظهره لقطات FTK Imager:

تُظهر اللقطات واجهات FTK Imager المستخدمة في هذا الإجراء، بما فيها اختيار مصدر Logical Drive، وتحديد صيغة الصورة، وحقول بيانات الدليل والوجهة والتحقق. يقتصر الشرح على عناصر الواجهة والقيم المقروءة في الصور.

تعرض الصور اختيار المصدر **Logical Drive** والوحدة `Z:\\ - TESTING [NTFS]`، ثم اختيار صيغة الصورة **E01**.



الخطوات:

1. في Select Source اختير **Logical Drive**، ثم ظهرت الوحدة `Z:\\ - TESTING [NTFS]` في قائمة المصدر.
2. في Select Image Type اختيرت صيغة **E01**.
3. في Evidence Item Information تظهر القيم: `3` Case Number، وEvidence Number `MohammedCase`، و`testing` Unique Description، و`mohammed` Examiner، مع ترك Notes

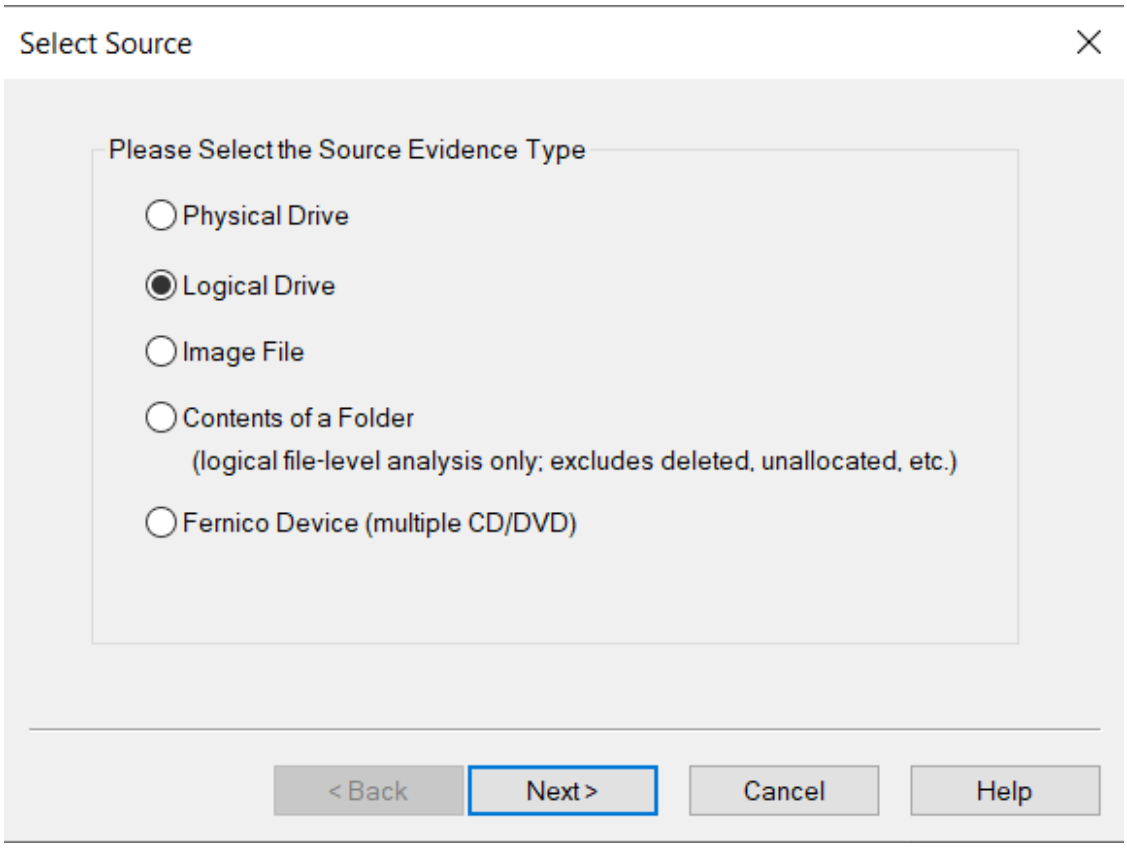
فارغاً.

4. في Select Image Destination تظهر الوجهة `D:\\mohammedTesting` والاسم `Test_Drive` وحجم الجزء `MB 1500` ومستوى الضغط `6`، وخيار Use AD Encryption غير محدد.
5. تعرض نافذة Drive/Image Verify Results اسم الملف `test.E01` وعدد القطاعات `4192256`.
6. تعرض النافذة نتيجة `Match` لكل من MD5 وSHA1.
7. تعرض النافذة عبارة `No bad blocks found in image`.
8. اسم الوجهة الأساسي واسم ملف التحقق مختلفان في اللقطتين (`Test_Drive` و`test.E01`)؛ يورد التقرير كلاً منهما كما يظهر دون افتراض سبب الاختلاف.

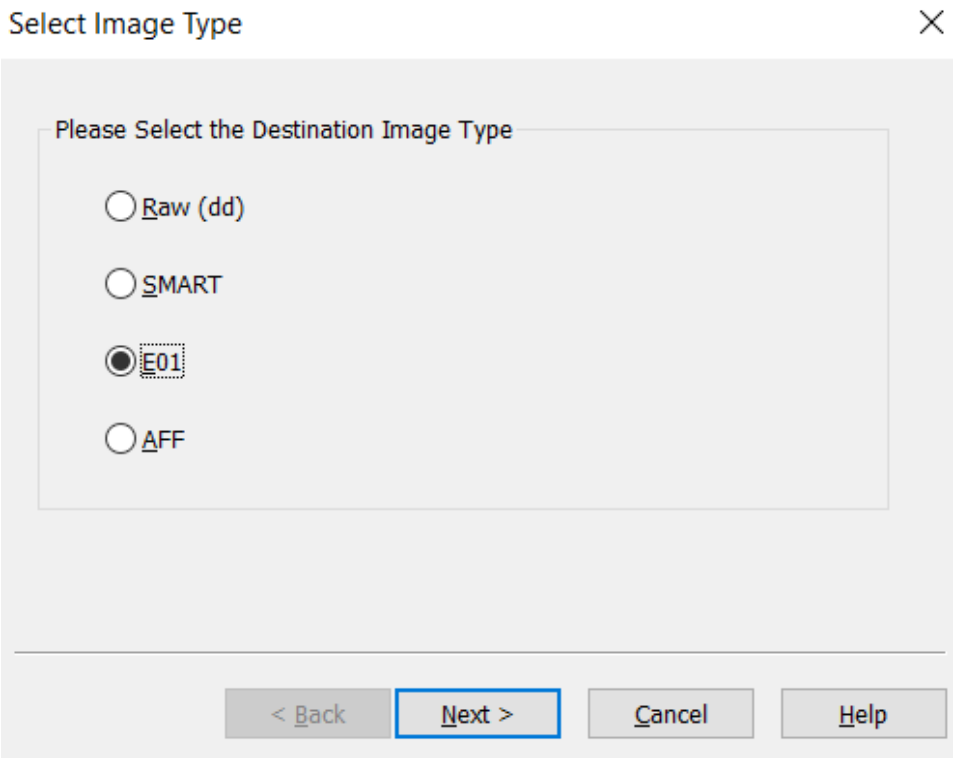
التحليل:

تُظهر لقطات الإعداد أن المصدر المحدد هو `Z:\\ - TESTING [NTFS]`، وأن الوجهة هي `D:\\mohammedTesting` والاسم الأساسي للصورة `Test_Drive`. وتعرض نافذة النتائج اسم `test.E01`، لذا أُبقي الاسمان كما يظهران في لقطتي الإعداد والتحقق دون افتراض سبب اختلافهما.

خيارات الصورة في FTK Imager:



الخيار	الوصف	الاستخدام الأمثل
Physical Drive	يصوّر القرص الصلب بأكمله (جميع الأقسام، قطاعات الإقلاع، والمساحة غير المخصصة)	التحقيقات الشاملة للنظام
Logical Drive	يصوّر قسماً/وحدة تخزين واحدة (مثل A:, C:, D:)	عندما تقتصر الأدلة على قسم واحد
Image File	يعالج صورة جنائية موجودة (E01, RAW)	التحقق أو التحويل أو النسخ المتماثل
Contents of a Folder	ينسخ الملفات والمجلدات المرئية فقط	**غير موصى به** — لا يلتقط الملفات المحذوفة
Fernico Device	خيار متخصص لنسخ الأقراص الضوئية (CD/DVD)	العمل مع أقراص CD/DVD متعددة



صيغ الصور:

الصيغة	الوصف	المزايا	العيوب
Raw (dd)	نسخة بتاً بت	بسيطة، توافق عالمي	لا ضغط، لا تحقق مدمج، لا بيانات وصفية
SMART	صيغة قديمة خاصة	تدعم الضغط وبعض البيانات الوصفية	قديمة، دعم محدود
E01 (EnCase)	المعيار الصناعي	ضغط، تحقق MD5/SHA-1، بيانات وصفية، تقسيم	مدعومة تجارياً
AFF	صيغة مفتوحة المصدر	ضغط، بيانات وصفية، توقيعات رقمية	دعم أقل من E01

الصورة: نافذة معلومات عنصر الدليل (Evidence Item Information) في FTK Imager

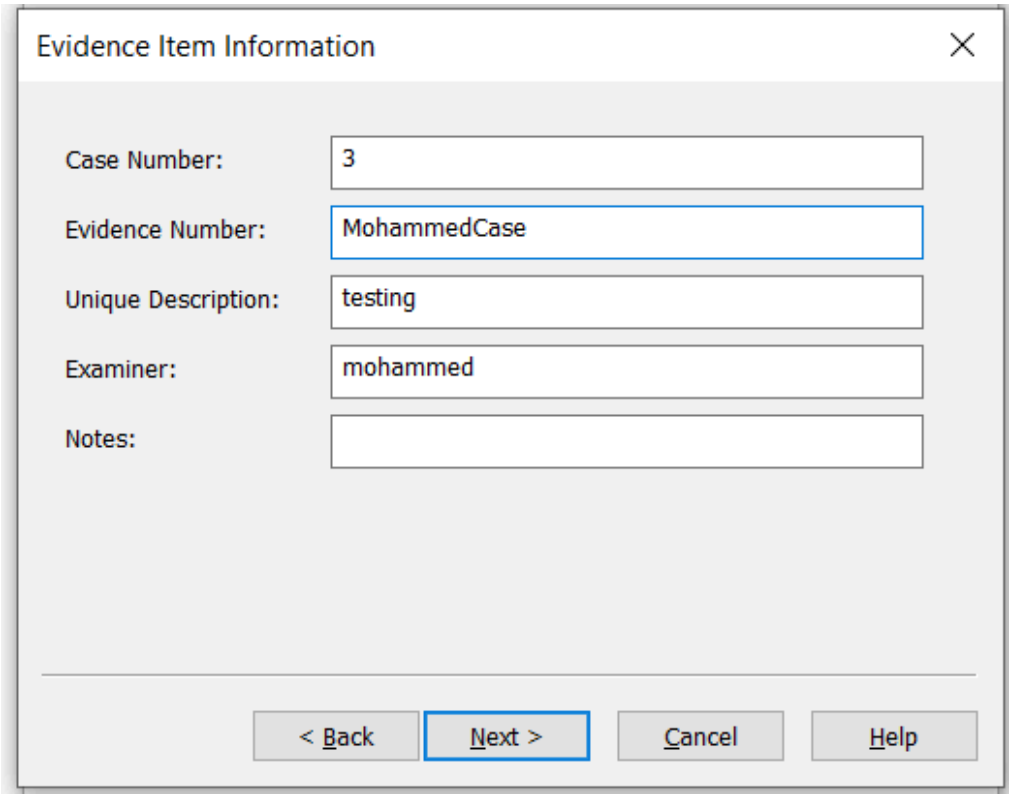
تُظهر اللقطة نافذة Evidence Item Information بعد اختيار E01، وتتضمن حقول Case Number وEvidence Number وUnique Description وExaminer وNotes. تسرد اللقطات التالية القيم الظاهرة في هذه الحقول دون افتراض ما لم تعرضه الصورة.

البيانات المُدخلة في هذه القضية:

الحقل	القيمة
Case Number	`3`
Evidence Number	`MohammedCase`
Unique Description	`testing`
Examiner	`mohammed`
Notes	(فارغ)

شرح الحقول:

- **Case Number:** رقم القضية الرسمي.
- **Evidence Number:** رقم أو اسم فريد لعنصر الدليل.
- **Unique Description:** وصف موجز لمحتوى الدليل.
- **Examiner:** اسم المحقق الذي أخذ الصورة.
- **Notes:** ملاحظات إضافية (اختياري).



الصورة: نافذة تحديد وجهة الصورة (Select Image Destination) في FTK Imager

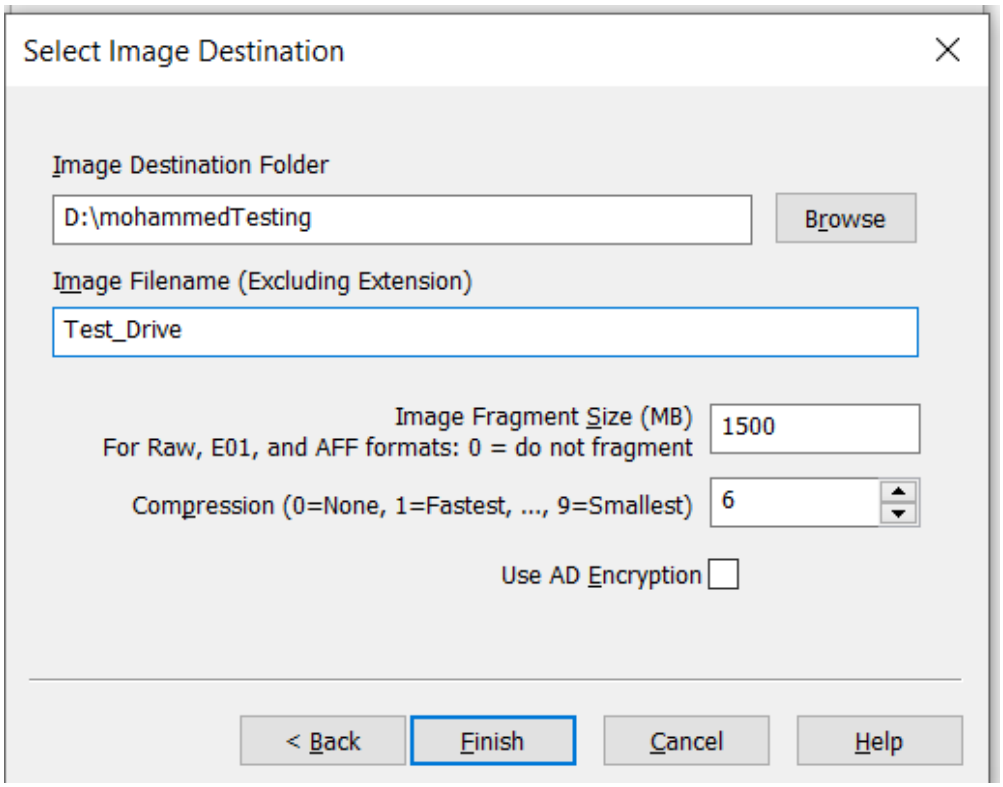
هذه النافذة تظهر بعد إدخال بيانات القضية في الخطوة السابقة، وتُستخدم لتحديد مكان حفظ الصورة وإعداداتها قبل بدء عملية أخذ الصورة الجنائية.

الإعدادات المُدخلة في هذه القضية:

الحقل	القيمة
Image Destination Folder	`D:\mohammedTesting`
Image Filename	`Test_Drive`
Image Fragment Size (MB)	`1500`
Compression	`6`
Use AD Encryption	غير مفعّل

شرح الحقول:

- **Image Destination Folder:** المسار الظاهر هو `D:\\mohammedTesting`. لا توضح اللقطة ما إذا كان D: وZ: قرصين ماديين منفصلين.
- **Image Filename:** الاسم الظاهر في الحقل هو `Test_Drive`.
- **Image Fragment Size:** القيمة الظاهرة هي `1500` `MB`.
- **Compression:** تعرض الواجهة المقياس من 0 إلى 9 مع توضيح None/Fastest/Smallest، والقيمة الظاهرة `6`.
- **Use AD Encryption:** مربع الاختيار غير محدد في اللقطة.



الصورة: نافذة نتائج التحقق من الصورة (Drive/Image Verify Results) في FTK Imager

تعرض اللقطة نافذة Drive/Image Verify Results وقيم التحقق الظاهرة أدناه.

النتائج المعروضة:

العنصر	القيمة
Name	`test.E01`
Sector count	`4192256`
MD5 Hash	
Computed hash	`3b122c90a186796211fe2fde62c5306d`
Stored verification hash	`3b122c90a186796211fe2fde62c5306d`
Report Hash	`3b122c90a186796211fe2fde62c5306d`
Verify result	**Match**
SHA1 Hash	
Computed hash	`5527d887d96f1426dbca5531a82814606eaeb07e`
Stored verification hash	`5527d887d96f1426dbca5531a82814606eaeb07e`

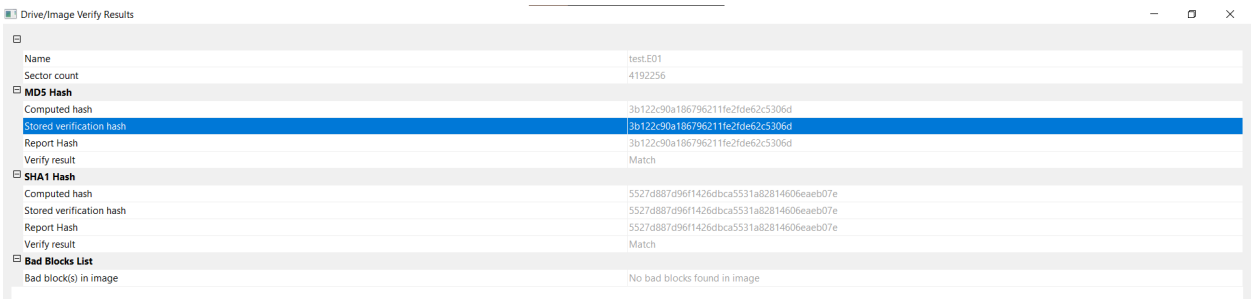
العنصر	القيمة
Report Hash	`5527d887d96f1426dbca5531a82814606eaeb07e`
Verify result	**Match**
Bad Blocks List	
Bad block(s) in image	`No bad blocks found in image`

شرح الحقول:

- **Name:** اسم ملف الصورة `test.E01`.
- **Sector count:** عدد القطاعات التي تم تصويرها (4,192,256 قطاع).
- **Computed hash:** القيمة التي تعرضها النافذة ضمن هذا الحقل.
- **Stored verification hash:** القيمة التي تعرضها النافذة ضمن هذا الحقل.
- **Report Hash:** القيمة التي تعرضها النافذة ضمن هذا الحقل.
- **Verify result:** تعرض النافذة النتيجة `Match` لكل من MD5 وSHA1.
- **Bad Blocks:** تعرض النافذة `No bad blocks found in image`.

التحليل الجنائي:

- تُظهر حقول MD5 الثلاث القيمة نفسها، ونتيجة التحقق المعروضة هي `Match`.
- تُظهر حقول SHA1 الثلاث القيمة نفسها، ونتيجة التحقق المعروضة هي `Match`.
- تُظهر القائمة `No bad blocks found in image`.
- تُظهر النافذة نتيجة التحقق `Match`؛ ولا تحدد اللقطة وحدها القبول القانوني للدليل.
-



الصورة : نافذة معلومات القضية الجديدة (New Case Information) في Autopsy

هذه النافذة تظهر عند إنشاء قضية جديدة في Autopsy، وتُستخدم لتحديد اسم القضية ونوعها ومكان حفظ بياناتها.

الإعدادات المُدخلة:

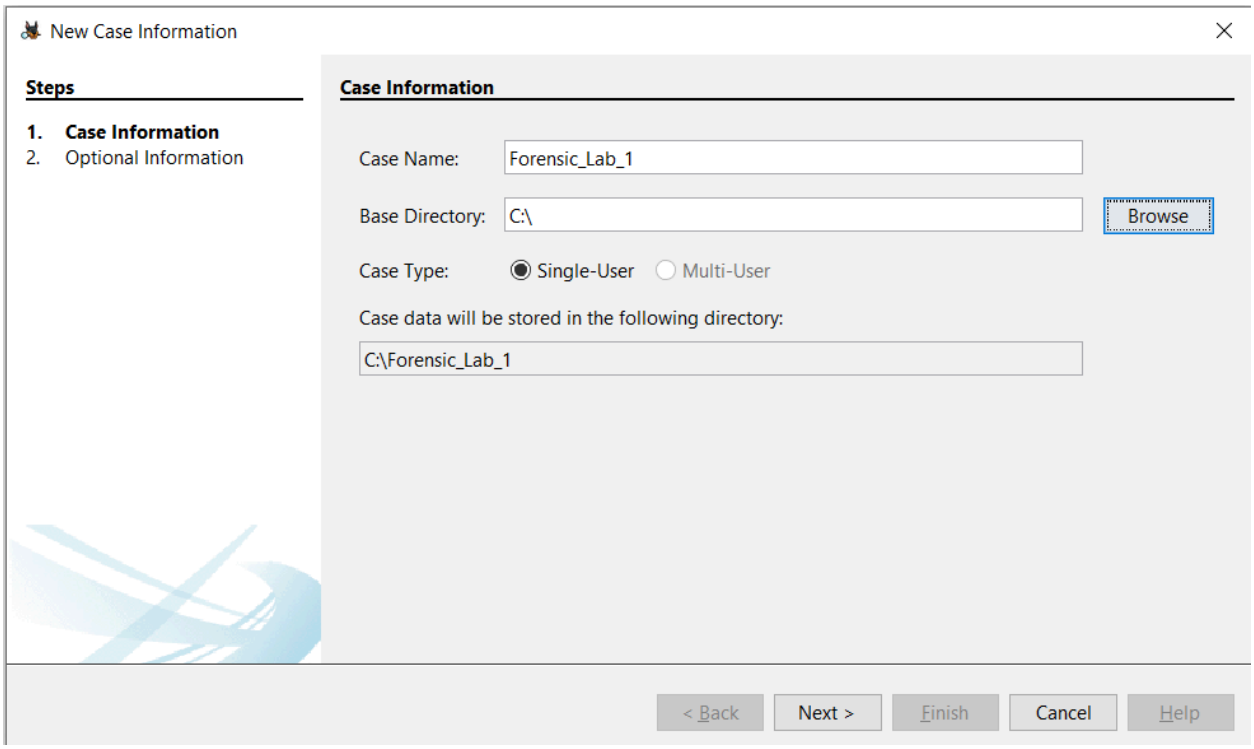
الحقل	القيمة
Case Name	`Forensic_Lab_1`
Base Directory	`C:\`
Case Type	**Single-User**
Case data directory	`C:\Forensic_Lab_1`

شرح الحقول:

- **Case Name:** اسم القضية `Forensic_Lab_1`.
- **Base Directory:** المجلد الأساسي لحفظ بيانات القضية على القرص `C:`.
- **Case Type:** نوع القضية، وتم اختيار **Single-User** (محقق واحد).
- **Case data directory:** المسار الكامل الذي ستُخزَّن فيه بيانات القضية.

التحليل الجنائي:

تُظهر اللقطة اختيار Case Type: Single-User، و`C` Base Directory`\\:`، ومجلد بيانات القضية `C:\\Forensic_Lab_1`. ولا تعرض الصورة إعدادات قاعدة البيانات أو خادماً مركزياً.



الصورة : نافذة إضافة مصدر بيانات (Add Data Source) - تحديد المضيف في Autopsy

هذه النافذة تظهر بعد إنشاء القضية، عند البدء في إضافة مصدر بيانات (صورة القرص). الخطوة الأولى هي تحديد **المضيف (Host)** الذي سيرتبط به مصدر البيانات.

الخيارات المتاحة:

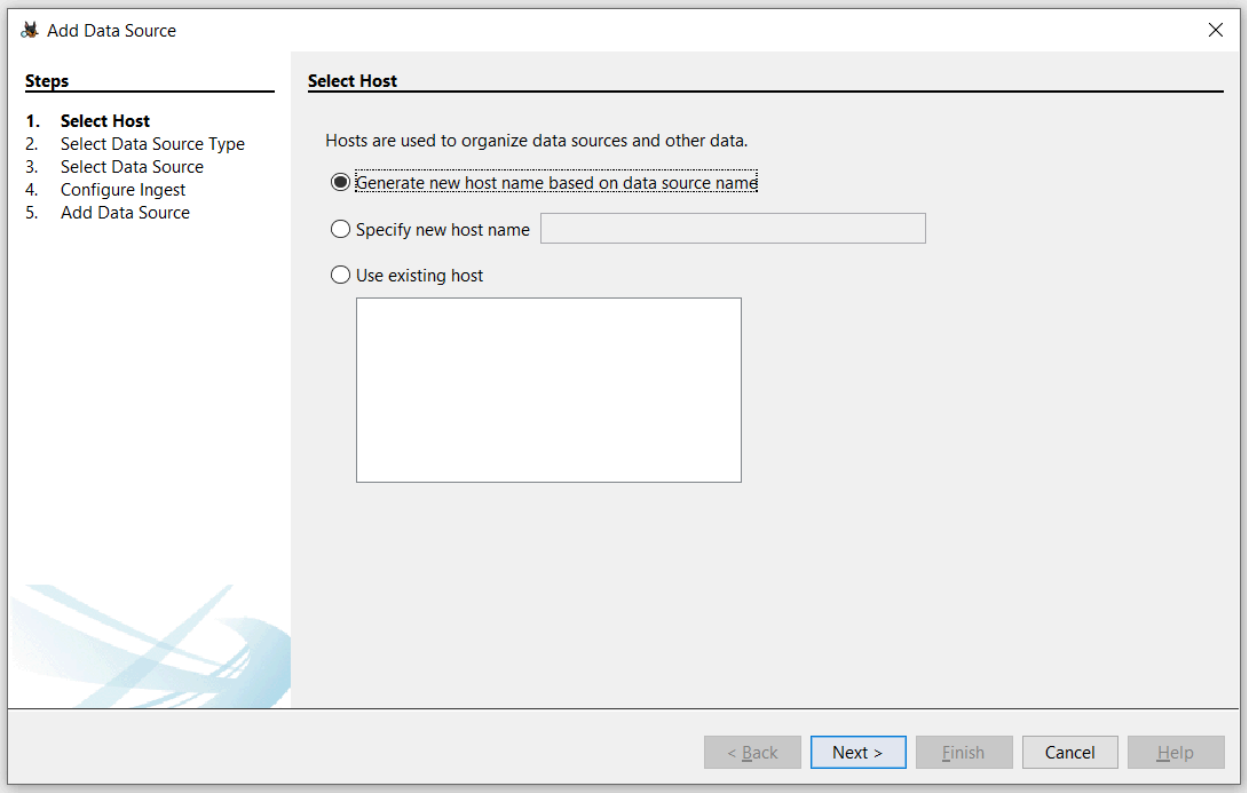
الخيار	الحالة
Generate new host name based on data source name	✅ محدد
Specify new host name	غير محدد
Use existing host	غير محدد

شرح الخيارات:

- **Generate new host name based on data source name:** إنشاء اسم مضيف تلقائياً بناءً على اسم مصدر البيانات.
- **Specify new host name:** إدخال اسم مضيف مخصص يدوياً.
- **Use existing host:** استخدام مضيف موجود مسبقاً في القضية.

التحليل الجنائي:

الخيار المحدد في اللقطة هو **Generate new host name based on data source name**.
وتظهر لقطة Data Sources لاحقاً الاسم `Test_Drive.E01_1 Host`؛ لذا نذكر الاسم كما يظهر دون إضافة تفسير غير ظاهر في الواجهة.



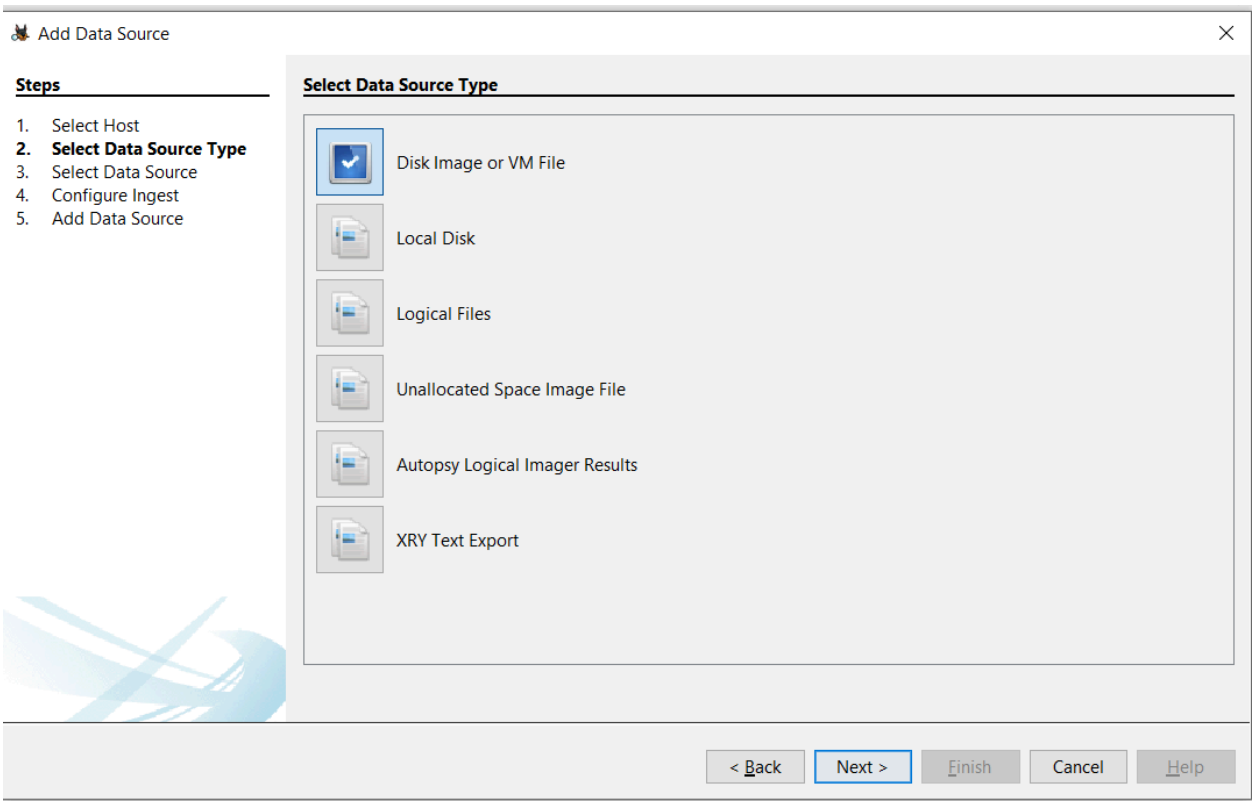
الصورة : نافذة إضافة مصدر بيانات (Add Data Source) - تحديد نوع مصدر البيانات في Autopsy

هذه النافذة تظهر بعد تحديد المضيف، وتُستخدم لاختيار نوع مصدر البيانات الذي سيتم تحليله.

التحليل الجنائي:

تُظهر اللقطة أن **Disk Image or VM File** هو الخيار المحدد من بين أنواع مصادر البيانات المعروضة.

الخطوة التالية: الضغط على **Next** للانتقال إلى تحديد مسار مصدر البيانات.



الصورة : نافذة إضافة مصدر بيانات (Add Data Source) - تحديد مصدر البيانات في Autopsy

هذه النافذة تظهر بعد اختيار نوع مصدر البيانات، وتُستخدم لتحديد مسار الصورة وإعداداتها.

الإعدادات المُدخلة:

الحقل	القيمة
Path	`D:\mohammedTesting`
Ignore orphan files in FAT file systems	غير مفعّل
Time zone	`(GMT+3:00) Asia/Riyadh`
Sector size	`Auto Detect`
MD5	(فارغ)
SHA-1	(فارغ)
SHA-256	(فارغ)

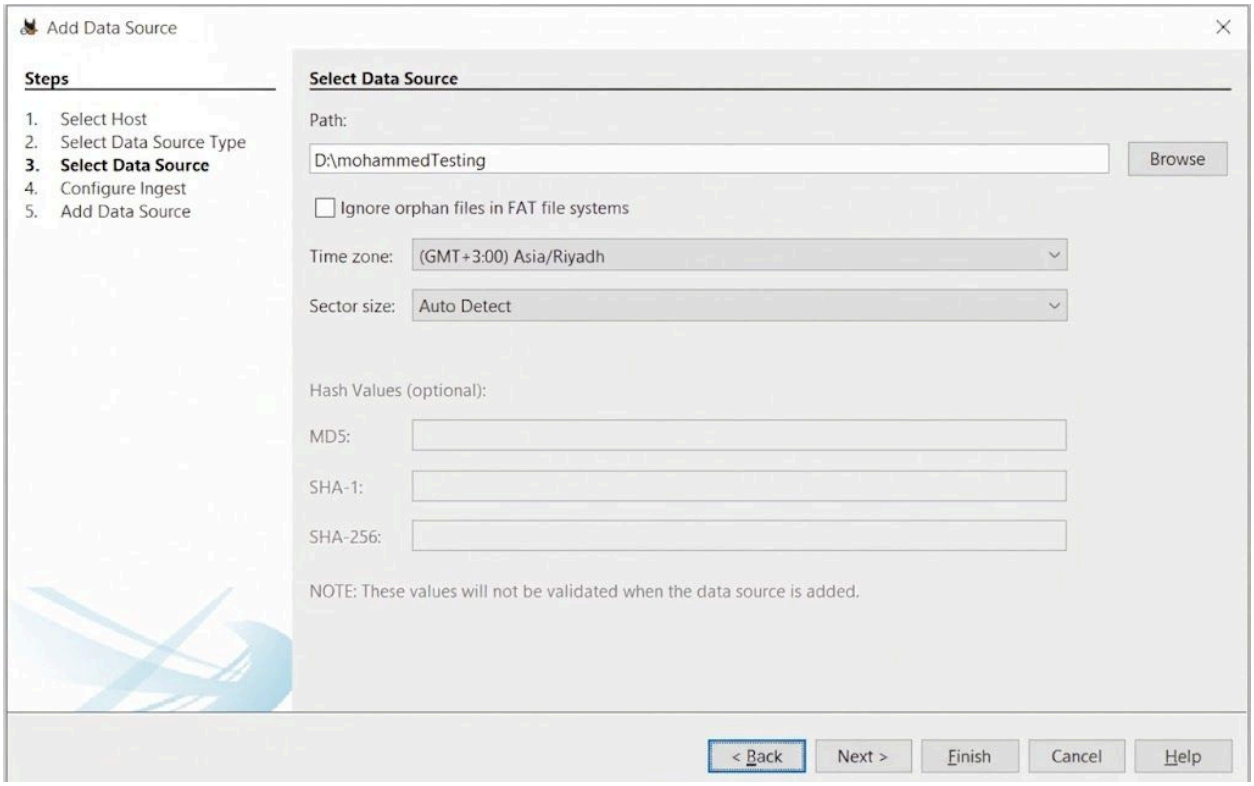
شرح الحقول:

- **Path:** مسار صورة القرص `D:\mohammedTesting`.

- **Ignore orphan files in FAT file systems:** مربع الاختيار غير محدد.
- **Time zone:** القيمة الظاهرة هي `(GMT+3:00) Asia/Riyadh`.
- **Sector size:** حجم القطاع، تلقائي (`Auto Detect`).
- **Hash Values (optional):** حقول MD5 وSHA-1 وSHA-256؛ ظاهرة وفارغة في اللقطة. وتظهر ملاحظة بأن القيم لن تُتحقق عند إضافة مصدر البيانات.

التحليل الجنائي:

تُظهر نافذة Select Data Source المنطقة الزمنية `Asia/Riyadh (GMT+3:00)`.
تظهر حقول MD5 وSHA-1 وSHA-256 فارغة، وتذكر النافذة أنها لن تُتحقق عند إضافة مصدر البيانات.



الصورة : نافذة تكوين وحدات الاستيعاب (Configure Ingest) في Autopsy

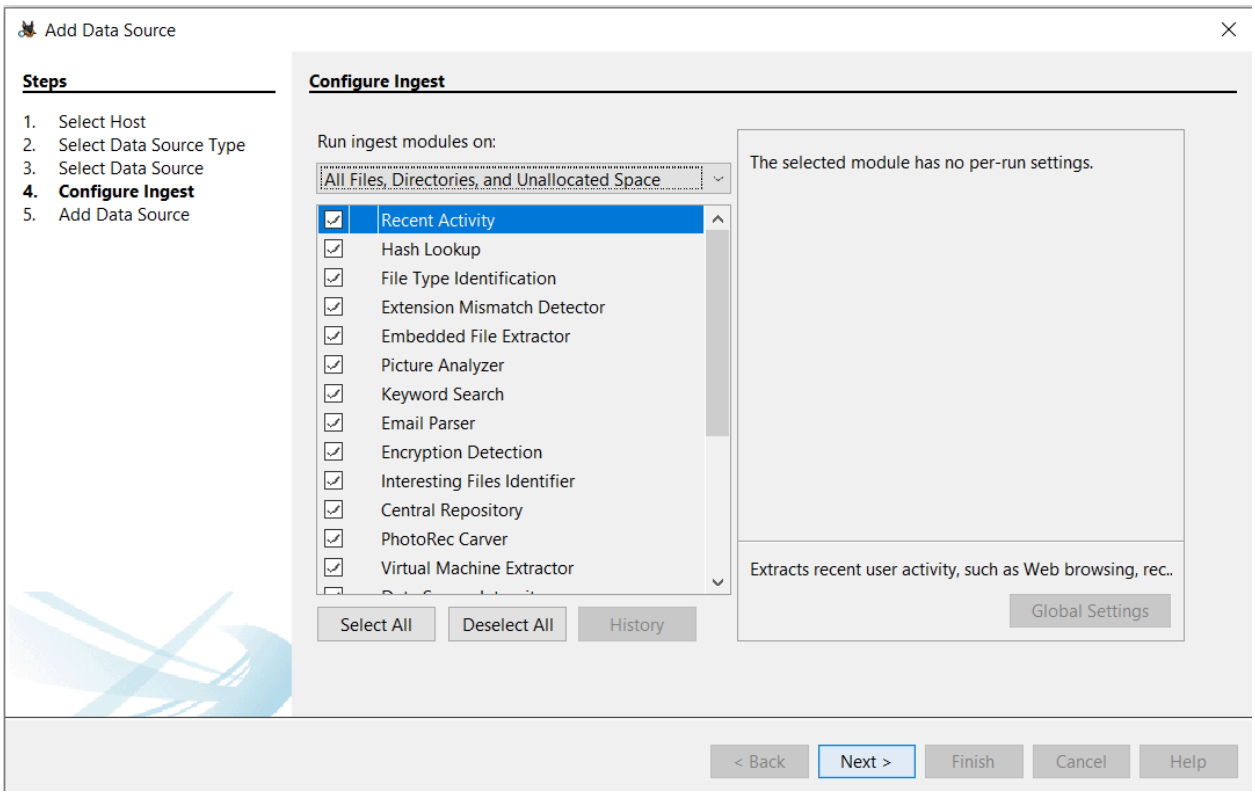
هذه النافذة تظهر بعد تحديد مصدر البيانات، وتُستخدم لاختيار وحدات التحليل الآلي التي ستعمل على الصورة الجنائية.

الوحدات المُفعّلة:

الوحدة	الوظيفة
Recent Activity	استخراج النشاط الأخير (تصفح، تنزيلات)
Hash Lookup	البحث عن قيم التجزئة في قواعد البيانات
File Type Identification	تحديد أنواع الملفات
Extension Mismatch Detector	كشف عدم تطابق الامتدادات
Embedded File Extractor	استخراج الملفات المدمجة
Picture Analyzer	تحليل الصور
Keyword Search	البحث بالكلمات المفتاحية
Email Parser	تحليل البريد الإلكتروني
Encryption Detection	كشف التشفير
Interesting Files Identifier	تحديد الملفات المهمة
Central Repository	المستودع المركزي
PhotoRec Carver	استعادة الملفات المحذوفة
Virtual Machine Extractor	استخراج بيانات الأجهزة الافتراضية

التحليل الجنائي:

تُظهر اللقطة أن النطاق المحدد هو **All Files, Directories, and Unallocated Space**، وأن مربعات الوحدات الظاهرة محددة، ومنها **Keyword Search** و**PhotoRec Carver**. هذه اللقطة توثق إعداد الاختيار فقط، ولا تعرض نتائج تشغيل الوحدات.



الصورة : نافذة عرض مصادر البيانات (Data Sources) في Autopsy

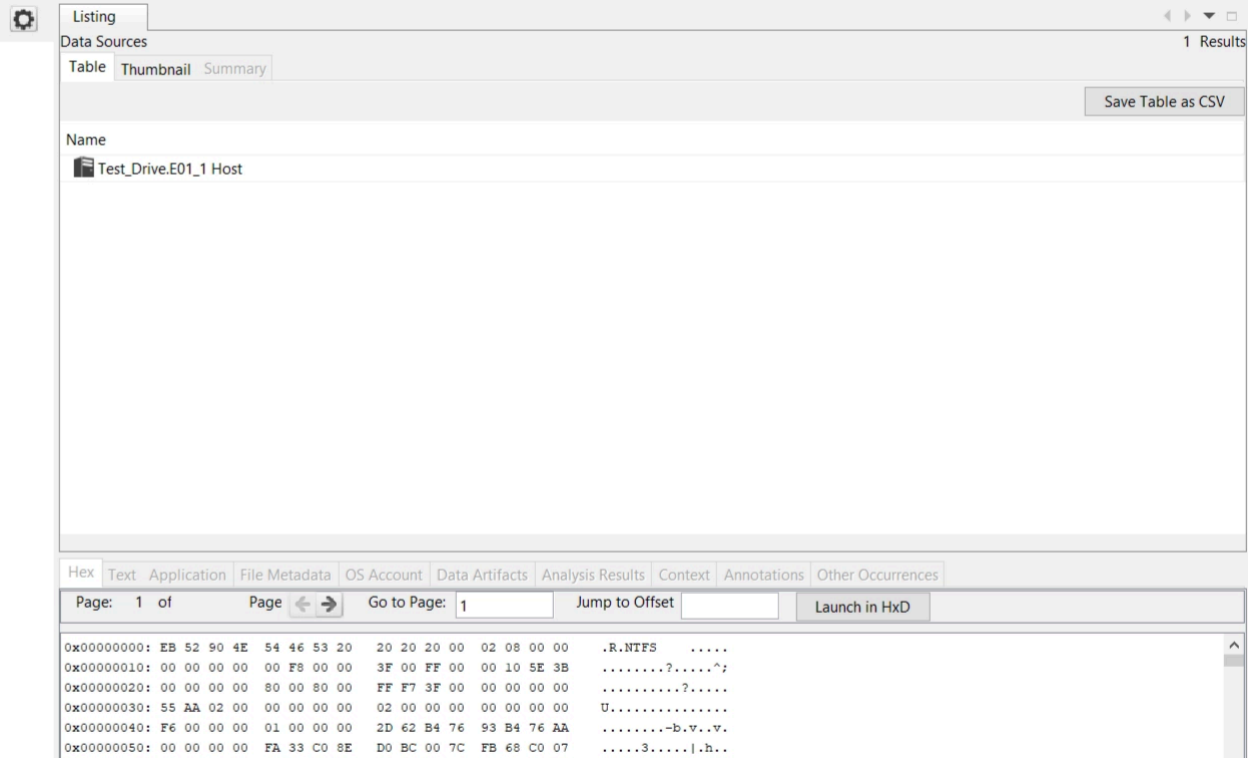
هذه النافذة تظهر بعد انتهاء إضافة مصدر البيانات، وتعرض قائمة المصادر المضافة مع عرض Hex للمحتوى.

النتائج المعروضة:

الحقل	القيمة
Name	`Test_Drive.E01_1 Host`
Results	1

التحليل الجنائي:

تُظهر نافذة Data Sources نتيجة واحدة باسم `Test_Drive.E01_1 Host`، وتظهر لوحة Hex أسفلها. تعرض اللقطة كذلك نصاً يتضمن `NTFS` ضمن بيانات Hex.



الصورة : نافذة عرض نظام الملفات (File System) في Autopsy

تُظهر نافذة File System قائمة نتائج وعددها 19، وتظهر علامة X حمراء بجوار العناصر المدرجة.

النتائج المعروضة: 19 نتيجة

النتائج الظاهرة بعلامة X حمراء:

الاسم	الحجم (Bytes)	تاريخ التعديل
`$IP7ONUS.pdf`	70	2026-07-17
`$RK2ZNF4.pdf`	527506	2025-12-19
`$RP7ONUS.pdf`	153750	2025-12-07
`$RID5Y0F.pdf`	1168705	2026-01-26
`$REXCBPN.pdf`	249124	2025-12-10
`$REXCBPN.pdf.Zone.Identifier`	26	2025-12-10
`$RAE87T8.pdf`	772709	2026-01-22
`$RS1RMTM.pdf`	1271284	2025-11-14
`$ROW17O4.pdf`	2360829	2026-01-27

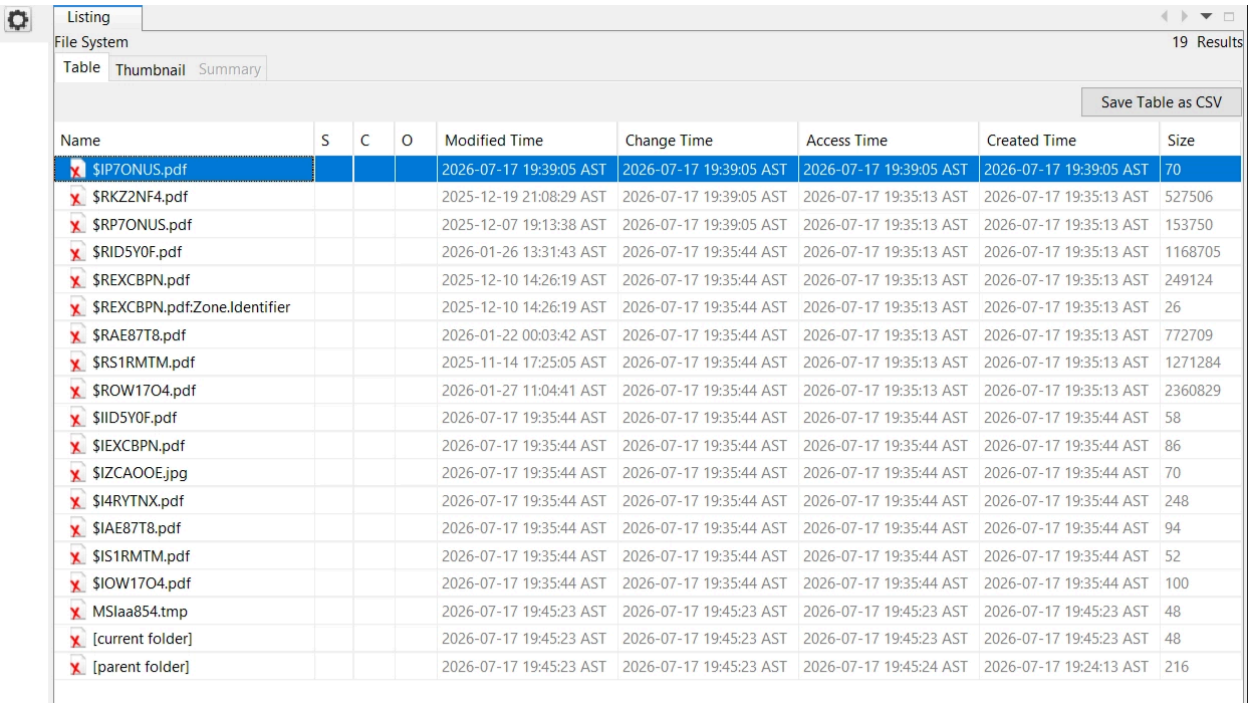
الاسم	الحجم (Bytes)	تاريخ التعديل
`$IID5Y0F.pdf`	58	2026-07-17
`$IEXCBPN.pdf`	86	2026-07-17
`$IZCAOOE.jpg`	70	2026-07-17
`$I4RYTNX.pdf`	248	2026-07-17
`$IAE87T8.pdf`	94	2026-07-17
`$IS1RMTM.pdf`	52	2026-07-17
`$IOW17O4.pdf`	100	2026-07-17
`MSlaa854.tmp`	48	2026-07-17
`[current folder]`	48	2026-07-17
`[parent folder]`	216	2026-07-17

تحليل أسماء الملفات المحذوفة:

- تظهر عدة أسماء تبدأ بـ `R$`، كما في الجدول أعلاه.
- تظهر عدة أسماء تبدأ بـ `I$`، كما في الجدول أعلاه.
- يظهر الاسم `MSlaa854.tmp` في القائمة.

التحليل الجنائي:

تُظهر نافذة File System عدد `Results 19`، مع الأسماء والأحجام والتواريخ المعروضة في الجدول. لا تكفي هذه اللقطة وحدها لإثبات أن النتائج استُعيدت بواسطة PhotoRec Carver أو أنها استُخرجت من المساحة غير المخصصة؛ لقطة Configure Ingest توثق تحديد الوحدة فقط.



الخاتمة

تُظهر صور FTK Imager اختيار وحدة TESTING (Z:) بنظام NTFS ومصدر Logical Drive، واختيار E01، وإعداد الوجهة `D:\\mohammedTesting` باسم `Test_Drive`. تعرض نافذة التحقق تطابق MD5 وSHA1 ونتيجة `Match`، مع عبارة `No bad blocks found in image`.

وفي لقطات Autopsy تظهر القضية `Forensic_Lab_1`، ومصدر البيانات `Test_Drive.E01_1 Host`، و19 نتيجة في نافذة File System. كما تظهر لقطات Configure Ingest وحدات محددة، ومنها PhotoRec Carver وKeyword Search، لكنها لا تعرض نتائج تشغيلهما.

يقتصر هذا التقرير على القيم والخيارات والنتائج الظاهرة في الصور؛ ولا تثبت الصور وحدها إجراء حذف محدد أو إفراغ سلة المحذوفات أو استعادة نتائج عبر وحدة بعينها.

ملاحظات توثيقية وفق الصور

1. وثّق وحدة المصدر كما تظهر في الصورة: `Z:\\ - TESTING [NTFS]`.
2. اذكر مسار الوجهة `D:\\mohammedTesting` والاسم `Test_Drive` كما يظهران في نافذة الوجهة.
3. احتفظ بقيم MD5 وSHA1 المعروضة ونتيجة `Match` كما تظهر في نافذة التحقق.
4. ميّز في الشرح بين وحدات Autopsy المحددة وبين نتائج تشغيلها؛ الصور تعرض الإعداد ولا تعرض مخرجات الوحدات.

5. أدرج بيانات الدليل الظاهرة: Case Number `3`، و`MohammedCase` Evidence Number، و`mohammed` Examiner، و`testing` Unique Description.
6. أدرج إعداد الوجهة الظاهر: حجم الجزء `MB 1500`، والضغط `6`، وUse AD Encryption غير محدد.
7. اذكر أن Autopsy يعرض المنطقة الزمنية `Asia/Riyadh (GMT+3:00)` وحجم القطاع `Auto` `Detect`.
8. اذكر قضية `Forensic_Lab_1` Autopsy والمسار `C:\\Forensic_Lab_1` كما يظهران في اللقطة.
9. سجّل أن نافذة File System تعرض `Results 19` والأسماء والأحجام والتواريخ الواردة في الجدول.
10. لا تنسب نتيجة استعادة إلى PhotoRec Carver أو حذفاً/إفراغاً لسلة المحذوفات ما لم تظهر صور توثق ذلك.