

التحليل الجنائي الرقمي

أمن المعلومات الرقمية والتحليل الجنائي للأدلة الرقمية



**METROPOLITAN
POLICE**

TOTAL POLICING

NEW
SCOTLAND
YARD

الأهداف

- ما هو الكمبيوتر؟
- أين الدليل؟
- ما هي أسباب أهمية التحليل الجنائي الرقمي؟
- ضبط الأدلة
- التشفير
- الملفات المخفية وحافظة الملفات
- أساليب الحصول الحي المباشر على المعلومات المخزنة إلكترونياً
- الحصول على معلومات باستخدام برنامج Dead Box
- صور الأدلة، المعالجة والتحليل الجنائي والنتائج
- أدوات التحليل الرقمي الجنائي – كيف تعمل
- هيكل الملفات، البيانات الوصفية (ميتاداتا)، بيانات إكسيف
- العلامات المرجعية (بوك مارك) والتقارير
- تكاليف المختبرات



**METROPOLITAN
POLICE**

TOTAL POLICING

NEW
SCOTLAND
YARD

ما هو الكمبيوتر؟

كمبيوتر محمول
(لاب توب)



كمبيوتر مكتبي
(دسك توب)



تايلت



هواتف



التخزين



**METROPOLITAN
POLICE**

TOTAL POLICING

**NEW
SCOTLAND
YARD**

أين الدليل؟



الممتلكات
العقارية



الإنترنت ووسائل
التواصل



الأشخاص



الشبكات
المؤسسية



الشركات



الصلاحيات
والولايات القضائية
الدولية



**METROPOLITAN
POLICE**

TOTAL POLICING

**NEW
SCOTLAND
YARD**

ما هي أسباب أهمية التحليل الجنائي الرقمي؟

ما الذي يمكننا استرجاعه؟



وورد

إكسل



باور بوينت

بي دي إف



البريد الإلكتروني



الإنترنت

الصور



بيانات الموقع

الوقت والتاريخ



المتصلون والمتصل بهم



محتوى غير قانوني



تقويم (رزمة)

الشركاء

والمتعاونون



METROPOLITAN
POLICE

TOTAL POLICING

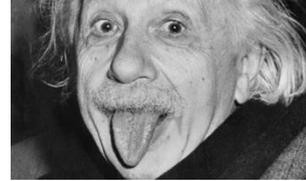
NEW
SCOTLAND
YARD

ضبط الأدلة

تشغيل الجهاز؟



الاستعانة بخبير!



إطفاء الجهاز؟



ضعها في الكيس!



METROPOLITAN
POLICE

TOTAL POLICING

NEW
SCOTLAND
YARD

التشفير

- التشفير قد يحول دون استرجاع البيانات
- يلزم توفر الأساليب المتخصصة والتدريب
- يلزم توفر البرامج والتطبيقات المتخصصة والمكونات المادية للكمبيوتر
- إذا كان الكمبيوتر في حالة تشغيل، استعن بخبير
- أين كلمة السر؟
- هذا هو سبب أهمية الحصول الحي المباشر على المعلومات والبيانات المخزنة إلكترونياً!



METROPOLITAN
POLICE

TOTAL POLICING

NEW
SCOTLAND
YARD

عرض توضيحي
Keyspace

الملفات المخفية وحافطة الملفات

- من الصعب العثور على الملفات المخفية
- يلزم استخدام برامج وتطبيقات متخصصة
- إذا كان الكمبيوتر في حالة التشغيل، استعن بخبير
- ما البرنامج التطبيقي الجاري استخدامه؟
- هذا هو سبب أهمية الحصول الحي المباشر على المعلومات والبيانات المخزنة إلكترونياً!



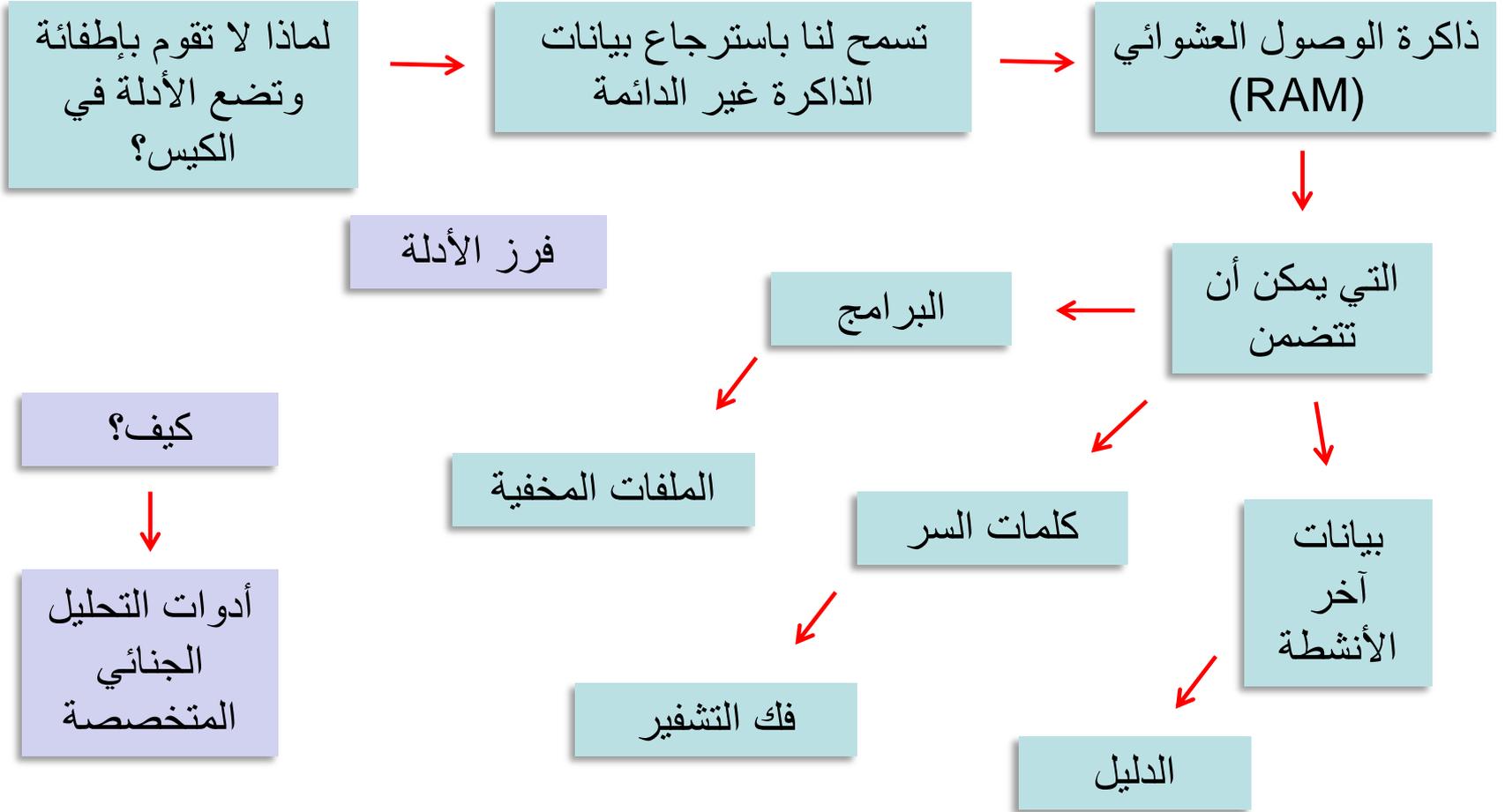
METROPOLITAN
POLICE

TOTAL POLICING

NEW
SCOTLAND
YARD

عرض توضيحي عن الصورة المخفية

الحصول الحي المباشر على البيانات والمعلومات



METROPOLITAN
POLICE

TOTAL POLICING

NEW
SCOTLAND
YARD

الحصول الحي المباشر على البيانات والمعلومات

أدوات التحليل الجنائي المتخصصة



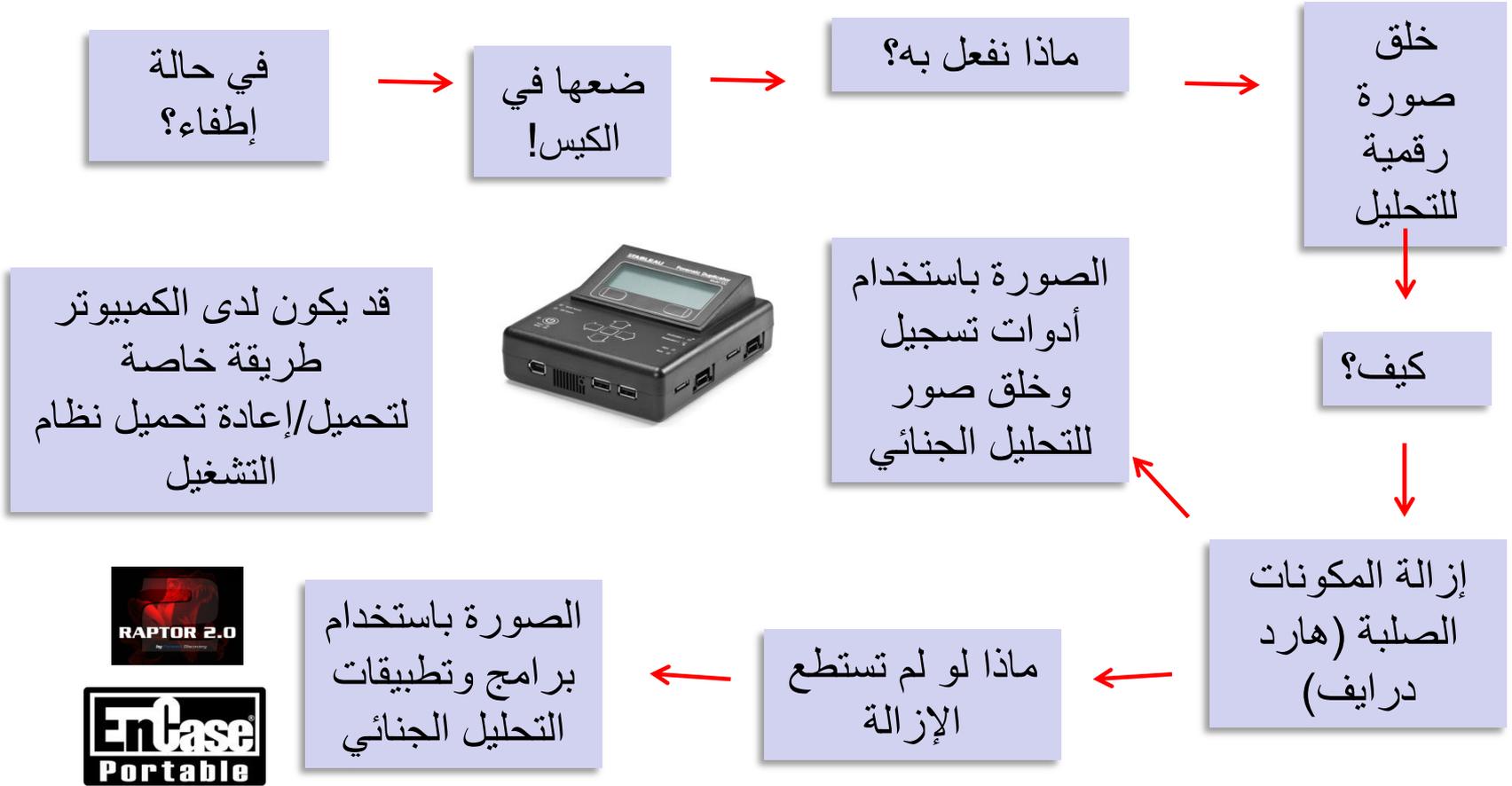
**METROPOLITAN
POLICE**

TOTAL POLICING

**NEW
SCOTLAND
YARD**

عرض توضيحي لبرنامج
EnCase Portable

الحصول على بيانات الصندوق الميت



METROPOLITAN
POLICE

TOTAL POLICING

NEW
SCOTLAND
YARD

الحصول على بيانات الصندوق الميت

أدوات تسجيل وإعداد صور الأدلة للتحليل الجنائي

- تتيح وجود جسر بين الوسائط



- تتيح خاصية حماية الكتابة للحفاظ على الأدلة



**METROPOLITAN
POLICE**

TOTAL POLICING

**NEW
SCOTLAND
YARD**

عرض توضيحي للحصول على بيانات بطاقة الذاكرة

صورة بيانات وأدلة التحليل الجنائي

ما هي صورة بيانات
وأدلة التحليل الجنائي؟

وعاء البيانات المحمية

رقم تعريف فريد
(Hash)

تتكون من:

- اسم الملف
- ملف نصي
- معلومات الحالة
- ملاحظات
- مجموعات البيانات
- Hash

| Name | Date modified | Type | Size |
|------------|------------------|----------------------|--------------|
| FC-6-H | 28/01/2013 08:27 | EnCase Evidence F... | 1,535,867 KB |
| FC-6-H.E01 | 28/01/2013 09:07 | Text Document | 3 KB |
| FC-6-H.E02 | 28/01/2013 08:29 | E02 File | 1,535,856 KB |
| FC-6-H.E03 | 28/01/2013 08:31 | E03 File | 1,535,857 KB |
| FC-6-H.E04 | 28/01/2013 08:33 | E04 File | 1,535,861 KB |
| FC-6-H.E05 | 28/01/2013 08:37 | E05 File | 1,535,851 KB |
| FC-6-H.E06 | 28/01/2013 08:39 | E06 File | 1,535,918 KB |
| FC-6-H.E07 | 28/01/2013 08:40 | E07 File | 1,535,927 KB |
| FC-6-H.E08 | 28/01/2013 08:42 | E08 File | 1,535,836 KB |
| FC-6-H.E09 | 28/01/2013 08:43 | E09 File | 1,535,914 KB |
| FC-6-H.E10 | 28/01/2013 08:45 | E10 File | 1,535,910 KB |
| FC-6-H.E11 | 28/01/2013 08:49 | E11 File | 1,535,838 KB |
| FC-6-H.E12 | 28/01/2013 08:52 | E12 File | 438,290 KB |

Hash
مهم لإظهار
الاستمرارية

أنواع ملفات الصور
.EO1 .E01. L01
.Lx01 .Ex01 .AD1



METROPOLITAN
POLICE

TOTAL POLICING

NEW
SCOTLAND
YARD

معالجة التحليل والنتائج

أدوات التحليل الجنائي

فاحص
EnCase

The screenshot displays the EnCase forensic software interface. The main window shows a file system tree on the left and a detailed table of entries in the center. The table has columns for Name, Tag, File Ext, Logical Size, Category, Signature Analysis, File Type, Protected, Protection complexity, Last Accessed, and File Created. The entries include folders like 'Op Birkhill', 'C', 'EFI', 'APPLE', 'EXTENSIONS', 'Firmware.scap', 'FIRMWARE', 'MBA41_0077_B0F_LOCKED.scap', 'EFI', 'Volume Boot', 'Primary FAT', 'Secondary FAT', 'Unallocated Clusters', and 'Customer', as well as files like '1 Customer', 'Macintosh HD', and 'Recovery HD'. The bottom panel shows the 'Fields' tab with a list of attributes and their values for the selected entry.

| Name | Tag | File Ext | Logical Size | Category | Signature Analysis | File Type | Protected | Protection complexity | Last Accessed | File Created |
|----------------------------|-----|----------|--------------|----------|--------------------|-----------|-----------|-----------------------|-------------------|------------------|
| Op Birkhill | | | 0 | Folder | | | | | | |
| C | | | 0 | Folder | | | | | 05/04/12 00:00:00 | 05/04/12 01:34:5 |
| EFI | | | 0 | Folder | | | | | 05/04/12 00:00:00 | 05/04/12 01:34:5 |
| APPLE | | | 0 | Folder | | | | | 05/04/12 00:00:00 | 05/04/12 01:34:5 |
| EXTENSIONS | | | 0 | Folder | | | | | 05/04/12 00:00:00 | 05/04/12 01:34:5 |
| Firmware.scap | | scap | 15,729,264 | None | Unknown | | | | 05/04/12 00:00:00 | 05/04/12 01:34:5 |
| FIRMWARE | | | 0 | Folder | | | | | 01/07/12 00:00:00 | 01/07/12 00:09:3 |
| MBA41_0077_B0F_LOCKED.scap | | scap | 8,454,768 | None | Unknown | | | | 01/07/12 00:00:00 | 01/07/12 00:09:3 |
| EFI | | | 0 | Unknown | | | | | | |
| Volume Boot | | | 16,384 | Unknown | | | | | | |
| Primary FAT | | | 1,625,600 | Unknown | | | | | | |
| Secondary FAT | | | 1,625,600 | Unknown | | | | | | |
| Unallocated Clusters | | | 182,299,712 | Unknown | | | | | | |
| 1 Customer | | | 0 | Folder | | | | | | 10/10/11 16:59:1 |
| Macintosh HD | | | 108 | Folder | Unknown | | | | 09/02/13 16:50:21 | 11/10/11 00:59:1 |
| temp40977783 | | | 126 | Folder | Unknown | | | | 11/10/11 00:59:16 | 11/10/11 00:59:1 |
| temp40982701 | | | 108 | Folder | Unknown | | | | 12/03/13 20:26:50 | 11/02/13 20:46:5 |
| temp41016858 | | | 108 | Folder | Unknown | | | | 12/03/13 20:26:50 | 12/02/13 21:40:4 |
| temp41016890 | | | 108 | Folder | Unknown | | | | 12/03/13 20:26:46 | 16/02/13 16:10:3 |
| temp41016891 | | | 108 | Folder | Unknown | | | | 12/03/13 20:26:46 | 16/02/13 16:10:4 |
| temp41016893 | | | 108 | Folder | Unknown | | | | 12/03/13 20:26:46 | 16/02/13 16:10:4 |



METROPOLITAN
POLICE

TOTAL POLICING

NEW
SCOTLAND
YARD

معالجة التحليل والنتائج

أدوات التحليل الجنائي

مجموعة
أدوات
التحليل
الجنائي
(FTK)

The screenshot displays the AccessData Forensic Toolkit (FTK) interface. The top section shows a grid of thumbnails representing various files and folders. Below this, the 'Evidence Items' pane shows a tree view of the current case. The main area displays a 'File Content' view with a hex dump and a 'File List' table.

| Name | Label | Item # | Ext | Path | Category | P-Size | L-Size | MCS | SHA1 | SHA256 | Created | Accessed | Modified |
|--------------------------|-------|--------|-----|---|----------|----------|----------|-----|------|--------|-------------------|---|---|
| 606305a-723-40e-9... | | 9227 | dat | RAID.E01:Read Drive on Mac 3 [NTFS]/[root]/[RECYCLE.BIN]/S-1-5-21-185993338-3563470148-180034955-1000/98P6... | JPEG | 21.45 MB | 21.45 MB | | | | 10/05/2013 12:... | 10/05/2013 12:... | 09/05/2013 03:43:02 (2013-05-09 02:43:02 UTC) |
| 606c53af-679f-43c5-a3... | | 43397 | dat | RAID.E01:Read Drive on Mac 3 [NTFS]/[root]/FTK Case Folder/CSL_JAU_5_13/thumbnails/606c53af-679f-43c5-a3e5-46a... | JPEG | 1180 KB | 1176 KB | | | | 24/05/2013 10:... | 24/05/2013 10:... | 10/04/2013 15:41:43 (2013-04-10 14:41:43 UTC) |
| 61234a6e-4b3b-4140-9... | | 19301 | dat | RAID.E01:Read Drive on Mac 3 [NTFS]/[root]/[RECYCLE.BIN]/S-1-5-21-185993338-3563470148-180034955-1000/98P7... | JPEG | 9640 KB | 9639 KB | | | | 11/03/2013 15:... | 11/03/2013 15:... | 14/05/2013 21:36:05 (2013-04-19 21:36:05 UTC) |
| 61691914-5261-4032-b... | | 42903 | dat | RAID.E01:Read Drive on Mac 3 [NTFS]/[root]/[RECYCLE.BIN]/S-1-5-21-185993338-3563470148-180034955-1000/98P7... | JPEG | 44.20 KB | 43.69 KB | | | | 10/05/2013 10:... | 10/05/2013 10:... | 10/05/2013 10:04:43 (2013-05-09 09:04:43 UTC) |
| 62198275-482-41c9-b... | | 43398 | dat | RAID.E01:Read Drive on Mac 3 [NTFS]/[root]/FTK Case Folder/CSL_JAU_5_13/thumbnails/62198275-482-41c9-b8d7-455... | JPEG | 528.0 KB | 524.5 KB | | | | 24/05/2013 10:... | 24/05/2013 10:... | 10/05/2013 15:41:33 (2013-04-10 14:41:33 UTC) |
| 631a8581-1e2e-49e6-b... | | 42904 | dat | RAID.E01:Read Drive on Mac 3 [NTFS]/[root]/[RECYCLE.BIN]/S-1-5-21-185993338-3563470148-180034955-1000/98P7... | JPEG | 52.00 KB | 48.76 KB | | | | 10/05/2013 10:... | 10/05/2013 10:... | 10/05/2013 10:04:53 (2013-05-09 09:04:53 UTC) |
| 666f959f-3a8e-46b6-a... | | 9228 | dat | RAID.E01:Read Drive on Mac 3 [NTFS]/[root]/[RECYCLE.BIN]/S-1-5-21-185993338-3563470148-180034955-1000/98P6... | JPEG | 24.79 MB | 24.78 MB | | | | 10/05/2013 12:... | 10/05/2013 12:... | 09/05/2013 03:43:03 (2013-05-09 02:43:03 UTC) |
| 671b14c-708e-8ed3-a... | | 43399 | dat | RAID.E01:Read Drive on Mac 3 [NTFS]/[root]/FTK Case Folder/CSL_JAU_5_13/thumbnails/671b14c-708e-8ed3-a56a-85e... | JPEG | 604.0 KB | 603.9 KB | | | | 24/05/2013 10:... | 24/05/2013 10:... | 10/04/2013 15:41:23 (2013-04-10 14:41:23 UTC) |
| 679888b-1233-43b7-9... | | 43400 | dat | RAID.E01:Read Drive on Mac 3 [NTFS]/[root]/FTK Case Folder/CSL_JAU_5_13/thumbnails/679888b-1233-43b7-9d14-090... | JPEG | 580.0 KB | 579.8 KB | | | | 24/05/2013 10:... | 24/05/2013 10:... | 10/04/2013 15:41:41 (2013-04-10 14:41:41 UTC) |
| 6918f4e-5e67-4074-9... | | 690 | dat | RAID.E01:Read Drive on Mac 3 [NTFS]/[root]/[RECYCLE.BIN]/S-1-5-21-185993338-3563470148-180034955-1000/98P4... | JPEG | 528.0 KB | 524.5 KB | | | | 10/05/2013 09:... | 22/02/2013 17:13:32 (2013-02-22 17:13:32 UTC) | |
| 69d533e-1345-438b-9... | | 9229 | dat | RAID.E01:Read Drive on Mac 3 [NTFS]/[root]/[RECYCLE.BIN]/S-1-5-21-185993338-3563470148-180034955-1000/98P6... | JPEG | 24.55 MB | 24.55 MB | | | | 10/05/2013 12:... | 10/05/2013 12:... | 09/05/2013 03:44:44 (2013-05-09 02:44:44 UTC) |
| 6c8e91e4-1414-4d9f-9... | | 9230 | dat | RAID.E01:Read Drive on Mac 3 [NTFS]/[root]/[RECYCLE.BIN]/S-1-5-21-185993338-3563470148-180034955-1000/98P6... | JPEG | 20.79 MB | 20.79 MB | | | | 10/05/2013 12:... | 10/05/2013 12:... | 09/05/2013 00:09:51 (2013-05-09 00:09:51 UTC) |
| 7015668f-4764-4061-9... | | 9231 | dat | RAID.E01:Read Drive on Mac 3 [NTFS]/[root]/[RECYCLE.BIN]/S-1-5-21-185993338-3563470148-180034955-1000/98P6... | JPEG | 8440 KB | 8436 KB | | | | 10/05/2013 12:... | 10/05/2013 12:... | 09/05/2013 02:44:45 (2013-05-09 02:44:45 UTC) |
| 70b8e0d-4e46-46e2-9... | | 9232 | dat | RAID.E01:Read Drive on Mac 3 [NTFS]/[root]/[RECYCLE.BIN]/S-1-5-21-185993338-3563470148-180034955-1000/98P6... | JPEG | 26.29 MB | 26.29 MB | | | | 10/05/2013 12:... | 10/05/2013 12:... | 09/05/2013 00:09:26 (2013-05-09 00:09:26 UTC) |



METROPOLITAN
POLICE

TOTAL POLICING

NEW
SCOTLAND
YARD

معالجة التحليل والنتائج

أدوات التحليل الجنائي

أداة العثور
على الأدلة
من الانترنت
(IEF)

The screenshot displays the IEF Report Viewer interface. On the left, a sidebar lists 'Recovered Artifacts' categorized by type and count:

- Cloud: 25 (Google Docs)
- Email: 30 (Gmail Fragments, Gmail Webmail, Hotmail Webmail)
- Media: 36796 (Pictures, Videos, Web Video Fragments)
- Social Networking: 2 (Facebook Chat), 5 (Facebook Pages), 31 (Facebook Pictures), 6 (Facebook Status Updates/Wall Po...)
- Web Related: 72703 (Browser Activity, Chrome Archived Web History, Chrome Autofill, Chrome Cache Records, Chrome Carved Web History, Chrome Cookies, Chrome Downloads, Chrome Favicons, Chrome History Index, Chrome Logins, Chrome Top Sites, Chrome Web History, Firefox Bookmarks, Firefox Cache Records, Firefox Carved FormHistory, Firefox Cookies, Firefox Downloads, Firefox Favicons, Firefox FormHistory, Firefox Input History, Firefox SessionStore Artifacts, Firefox Web History)

The main window shows a table of browser activity with columns: #, Page Title, URL, Created Date/Time, Domain, Cache Table, Cache RowID, and Source. The table contains 2780 rows of data, with the first few rows showing 'Flextag' entries from 'ja2.wiles.com'.

| # | Page Title | URL | Created Date/Time | Domain | Cache Table | Cache RowID | Source |
|----|---------------|-----------------------------|---------------------|---------------|---------------------------|-------------|-------------------------|
| 2. | Flextag | http://ja2.wiles.com/in... | 03/08/2012 00:30:33 | ja2.wiles.com | Internet Explorer Cach... | 13570 | NUC-LCC-1H-ED01 - Pa... |
| 2. | Flextag | http://ja2.wiles.com/in... | 03/08/2012 00:51:03 | ja2.wiles.com | Internet Explorer Cach... | 13610 | NUC-LCC-1H-ED01 - Pa... |
| 2. | Flextag | http://ja2.wiles.com/in... | 03/08/2012 03:09:38 | ja2.wiles.com | Internet Explorer Cach... | 13613 | NUC-LCC-1H-ED01 - Pa... |
| 2. | Flextag | http://ja2.wiles.com/in... | 03/08/2012 00:51:03 | ja2.wiles.com | Internet Explorer Cach... | 13637 | NUC-LCC-1H-ED01 - Pa... |
| 2. | Flextag | http://ja2.wiles.com/in... | 03/08/2012 00:36:26 | ja2.wiles.com | Internet Explorer Cach... | 13668 | NUC-LCC-1H-ED01 - Pa... |
| 2. | Flextag | http://ja2.wiles.com/in... | 03/08/2012 00:30:33 | ja2.wiles.com | Internet Explorer Cach... | 13669 | NUC-LCC-1H-ED01 - Pa... |
| 2. | Flextag | http://ja2.wiles.com/in... | 03/08/2012 00:54:33 | ja2.wiles.com | Internet Explorer Cach... | 13695 | NUC-LCC-1H-ED01 - Pa... |
| 2. | Flextag | http://ja2.wiles.com/in... | 03/08/2012 00:27:58 | ja2.wiles.com | Internet Explorer Cach... | 13712 | NUC-LCC-1H-ED01 - Pa... |
| 2. | Flextag | http://ja2.wiles.com/in... | 03/08/2012 00:27:18 | ja2.wiles.com | Internet Explorer Cach... | 13715 | NUC-LCC-1H-ED01 - Pa... |
| 2. | Flextag | http://ja2.wiles.com/in... | 03/08/2012 00:40:12 | ja2.wiles.com | Internet Explorer Cach... | 13725 | NUC-LCC-1H-ED01 - Pa... |
| 2. | Flextag | http://ja2.wiles.com/-/0... | 12/09/2012 02:39:12 | ja2.wiles.com | Internet Explorer Cach... | 13800 | NUC-LCC-1H-ED01 - Pa... |
| 2. | Flextag | http://ja2.wiles.com/14... | 01/10/2012 08:13:28 | ja2.wiles.com | Internet Explorer Cach... | 13822 | NUC-LCC-1H-ED01 - Pa... |
| 2. | Flextag | http://ja2.wiles.com/-/0... | 12/09/2012 02:59:48 | ja2.wiles.com | Internet Explorer Cach... | 13837 | NUC-LCC-1H-ED01 - Pa... |
| 2. | Flextag | http://ja2.wiles.com/-/0... | 11/09/2012 20:23:27 | ja2.wiles.com | Internet Explorer Cach... | 13838 | NUC-LCC-1H-ED01 - Pa... |
| 2. | Flextag | http://ja2.wiles.com/-/0... | 12/09/2012 01:59:19 | ja2.wiles.com | Internet Explorer Cach... | 13847 | NUC-LCC-1H-ED01 - Pa... |
| 2. | Advertisement | http://ja2.wiles.com/14... | 28/09/2012 00:20:00 | ja2.wiles.com | Internet Explorer Cach... | 13851 | NUC-LCC-1H-ED01 - Pa... |
| 2. | Flextag | http://ja2.wiles.com/-/0... | 12/09/2012 02:25:01 | ja2.wiles.com | Internet Explorer Cach... | 13862 | NUC-LCC-1H-ED01 - Pa... |
| 2. | Flextag | http://ja2.wiles.com/-/0... | 12/09/2012 03:48:37 | ja2.wiles.com | Internet Explorer Cach... | 13866 | NUC-LCC-1H-ED01 - Pa... |



METROPOLITAN
POLICE

TOTAL POLICING

NEW
SCOTLAND
YARD

أدوات التحليل الجنائي - كيف تعمل

فحص هياكل الملفات

جميع أنواع الملفات هيكل بيانات رسمي



المعلومات داخل
الملف

| Hex | Text | Filtered | Natural |
|--------|---|----------|------------------|
| 000000 | FF D8 FF E1 2F FE 45 78-69 66 00 00 4D 4D 00 2A | | y0yá/pExif- MM.* |
| 000010 | 00 00 00 08 00 0B 01 0F-00 02 00 00 00 06 00 00 | | |
| 000020 | 00 92 01 10 00 02 00 00-00 09 00 00 00 98 01 12 | | |
| 000030 | 00 03 00 00 00 01 00 01-00 00 01 1A 00 05 00 00 | | |
| 000040 | 00 01 00 00 00 A2 01 1B-00 05 00 00 00 01 00 00 | | |
| 000050 | 00 AA 01 28 00 03 00 00-00 01 00 02 00 00 01 31 | | ..- (.....-1 |
| 000060 | 00 02 00 00 00 06 00 00-00 B2 01 32 00 02 00 00 | |*-2 |
| 000070 | 00 14 00 00 00 B8 02 13-00 03 00 00 00 01 00 01 | | |
| 000080 | 00 00 87 69 00 04 00 00-00 01 00 00 00 CC 88 25 | | ...i.....i-§ |
| 000090 | 00 04 00 00 00 01 00 00-02 52 00 00 03 1C 41 70 | |R....Ap |
| 0000a0 | 70 6C 65 00 69 50 68 6F-6E 65 20 35 00 00 00 00 | | ple-iPhone 5.... |
| 0000b0 | 00 48 00 00 00 01 00 00-00 48 00 00 00 01 36 2E | | ..H.....H....6. |
| 0000c0 | 31 2E 33 00 32 30 31 33-3A 30 35 3A 33 30 20 31 | | 1.3-2013:05:30 1 |
| 0000d0 | 32 3A 34 30 3A 32 31 00-00 18 82 9A 00 05 00 00 | | 2:40:21..... |
| 0000e0 | 00 01 00 00 01 F2 82 9D-00 05 00 00 00 01 00 00 | |ò..... |

مُحددات الملفات

رأس الصفحة

ذيل الصفحة



METROPOLITAN
POLICE

TOTAL POLICING

NEW
SCOTLAND
YARD

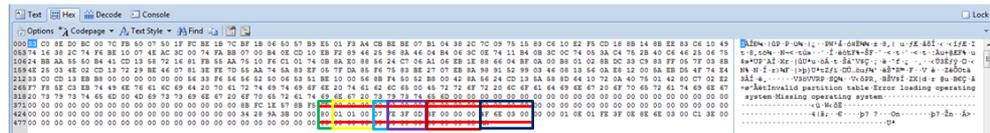
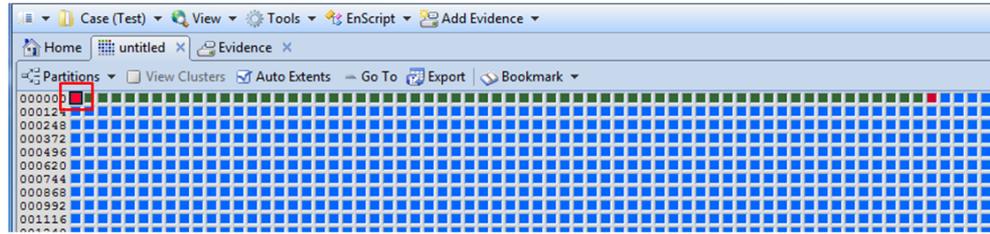
أدوات التحليل الجنائي – كيف تعمل

فحص جدول الملف الرئيسي

تسجيل جميع الفايلات المخزنة على درايڤ

Windows XP Operating System

Master Boot Record (MBR) Sector 0



Partition 1 Offset 446 - 16 Bytes Bootable flag Starting CHS address

Partition Type Ending CHS address Starting LBA sector offset Partition sector count

الحجم

اسم الملف

نوع الملف

المكان

تم إنشاؤه

تم الدخول عليه

تم تعديله

تم حذفه



METROPOLITAN
POLICE

TOTAL POLICING

NEW
SCOTLAND
YARD

عرض توضيحي لبطاقة ذاكرة مجموعة أدوات
FTK Memory Card التحليل الجنائي

البيانات الوصفية (ميتاداتا) وبيانات إكسيف

المعلومات داخل ملف صورة

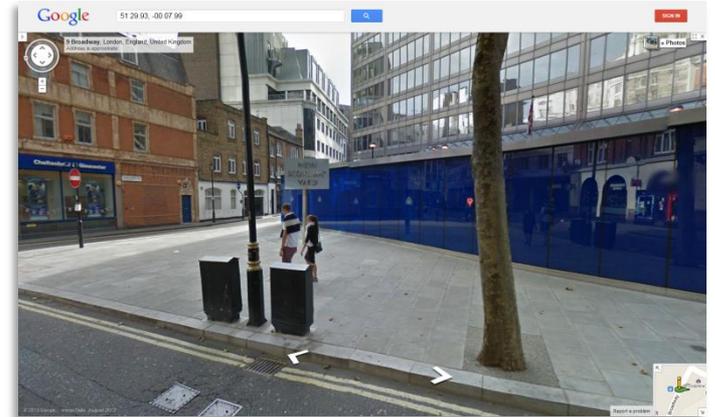
ماذا نحصل عليه؟

| | |
|---------------------------------|--------------------|
| Exif.GPSInfo.GPSLatitudeRef | N |
| Exif.GPSInfo.Latitude | 51/1 2993/100 0/1 |
| Exif.GPSInfo.LongitudeRef | W |
| Exif.GPSInfo.Longitude | 0/1 799/100 0/1 |
| Exif.GPSInfo.AltitudeRef | 0 |
| Exif.GPSInfo.Altitude | 67199/1326 |
| Exif.GPSInfo.GPSTimeStamp | 11/1 40/1 2131/100 |
| Exif.GPSInfo.GPSImgDirectionRef | T |
| Exif.GPSInfo.GPSImgDirection | 36305/289 |

الكاميرا وطرزها ونوعها



تحديد المواقع
الجغرافية



تواريخ

أوقات

المؤلف



METROPOLITAN
POLICE

TOTAL POLICING

NEW
SCOTLAND
YARD

عرض توضيحي لبيانات إكسيف

معالجة التحليل والنتائج

العلامات المرجعية (بوك مارك) والتقارير

تظليل الملفات

إضافة تعليقات

إرفاق ملفات

النقل إلى التقارير

File List

| Name | Label | Item # | Ext | Path | Category | P-Size | L-Size | MD5 | SHA1 | SHA256 | Created | Accessed | Modified |
|------------------------|-------|--------|------|--------------------------|-----------|----------|----------|-----------|-----------|--------|-------------------|-------------------|-------------------|
| \$130 | | 1568 | | ACE31.E01\ACE3 [NTFS]... | Index ... | 4096 B | 4096 B | 0a54cc... | 680f61... | | 27/08/2007 23:... | 06/05/2009 17:... | 06/05/2009 17:... |
| \$130 | | 1569 | | ACE31.E01\ACE3 [NTFS]... | Index ... | 4096 B | 4096 B | 8603e0... | ca1053... | | 27/08/2007 23:... | 27/08/2007 23:... | 22/08/2007 18:... |
| 1.JPG | | 1570 | .jpg | ACE31.E01\ACE3 [NTFS]... | JPEG E... | 341.5 KB | 341.1 KB | 2d4bf3... | 80421d... | | 06/05/2009 17:... | 06/05/2009 17:... | 14/11/2006 07:... |
| 2.JPG | | 1571 | .jpg | ACE31.E01\ACE3 [NTFS]... | JPEG E... | 326.5 KB | 326.5 KB | ac3059... | 60cefb... | | 06/05/2009 17:... | 06/05/2009 17:... | 14/11/2006 06:... |
| 3.JPG | | 1572 | .jpg | ACE31.E01\ACE3 [NTFS]... | JPEG E... | 334.0 KB | 333.6 KB | a35018... | 9e2869... | | 06/05/2009 17:... | 06/05/2009 17:... | 14/11/2006 07:... |
| 4.JPG | | 1573 | .jpg | ACE31.E01\ACE3 [NTFS]... | JPEG E... | 348.0 KB | 348.0 KB | f05ced... | 829343... | | 06/05/2009 17:... | 06/05/2009 17:... | 14/11/2006 06:... |
| 5.JPG | | 1574 | .jpg | ACE31.E01\ACE3 [NTFS]... | JPEG E... | 342.0 KB | 341.9 KB | a4893d... | 117646... | | 06/05/2009 17:... | 06/05/2009 17:... | 14/11/2006 06:... |
| 6.JPG | | 1575 | .jpg | ACE31.E01\ACE3 [NTFS]... | JPEG E... | 323.5 KB | 323.3 KB | | | | | | |
| Desktop.ini | | 1576 | .ini | ACE31.E01\ACE3 [NTFS]... | Text | 107 B | 107 B | | | | | | |
| hipvok.jpg | | 1577 | .jpg | ACE31.E01\ACE3 [NTFS]... | JPEG E... | 156.0 KB | 155.9 KB | | | | | | |
| lotusesvri1610244v.bmp | | 1578 | .bmp | ACE31.E01\ACE3 [NTFS]... | JPEG E... | 124.5 KB | 124.1 KB | | | | | | |
| Sample Pictures.lnk | | 1579 | .lnk | ACE31.E01\ACE3 [NTFS]... | Windo... | 1024 B | 668 B | | | | | | |
| Thumbs.db | | 1580 | .db | ACE31.E01\ACE3 [NTFS]... | Thumb... | 13.00 KB | 13.00 KB | | | | | | |

Loaded: 13 | Filtered: 13 | Total: 13 | Highlighted: 1 | Checked: 0 | Total LSize: 2316

File Content

Hex | Text | Filtered | Natural

Create New Bookmark

Bookmark Name: []

Bookmark Comment: []

Files to Include

All Highlighted All Checked All Listed

1 item selected.

| Name | Path |
|-------|--|
| 1.JPG | ACE31.E01\ACE3 [NTFS] [root] Documents and Settings [Lysseus] M... |

File Comment: []

Supplementary Files: []

Also include

Parent index.dat

Email Attachments

Parent Email

NEW SCOTLAND YARD



METROPOLITAN
POLICE

TOTAL POLICING

تكاليف المختبرات

• الموظفون

• الأجهزة والمعدات

• التدريب

مقابل

• المقاولون
والمتعاقدون



**METROPOLITAN
POLICE**

TOTAL POLICING

NEW
SCOTLAND
YARD

ملخص

- ما هو الكمبيوتر؟
- أين الدليل؟
- ما هي أسباب أهمية التحليل الجنائي الرقمي؟
- ضبط الأدلة
- التشفير
- الملفات المخفية وحافظة الملفات
- أساليب الحصول الحي المباشر على المعلومات المخزنة إلكترونياً
- الحصول على معلومات باستخدام برنامج Dead Box
- صور الأدلة، المعالجة والتحليل الجنائي والنتائج
- أدوات التحليل الرقمي الجنائي – كيف تعمل
- هيكل الملفات، البيانات الوصفية (ميتاداتا)، بيانات إكسيف
- العلامات المرجعية (بوك مارك) والتقارير
- تكاليف المختبرات



**METROPOLITAN
POLICE**

TOTAL POLICING

NEW
SCOTLAND
YARD

