التحليل الجنائي الرقمي

أمن المعلومات الرقمية والتحليل الجنائي للأدلة الرقمية

METROPOLITAN POLICE

TOTAL POLICING

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 إلكترونيا
- 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

ما هو الكمبيوتر؟

كمبيوتر مكتبي
(دسك توب)

كمبيوتر محمول
(لاب توب)

تابلت

هواتف

التخزين

أين الدليل؟

الإنترنت ووسائل التواصل

الشبكات المؤسسية

الصلاحيات والولايات القضائية الدولية

الممتلكات العقارية

الأشخاص

الشركات

ما هي أسباب أهمية التحليل الجنائي الرقمي؟

ما الذي يمكننا استرجاعه؟

البريد الإلكتروني

الإنترنت

المُتصلون والمُتّصَل بهم

تقويم (رزنامة)

ووورد

إكسل

باور بوينت

بي دي إف

بيانات الموقع

الوقت والتاريخ

محتوى غير قانوني

الشركاء والمتعاونون

الصور

METROPOLITAN POLICE

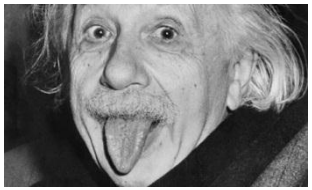
TOTAL POLICING

NEW SCOTLAND YARD

ضبط الأدلة

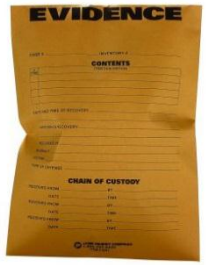
تشغيل الجهاز؟

الاستعانة بخبير!



إطفاء الجهاز؟

ضعها في الكيس!



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 إلكترونيا!

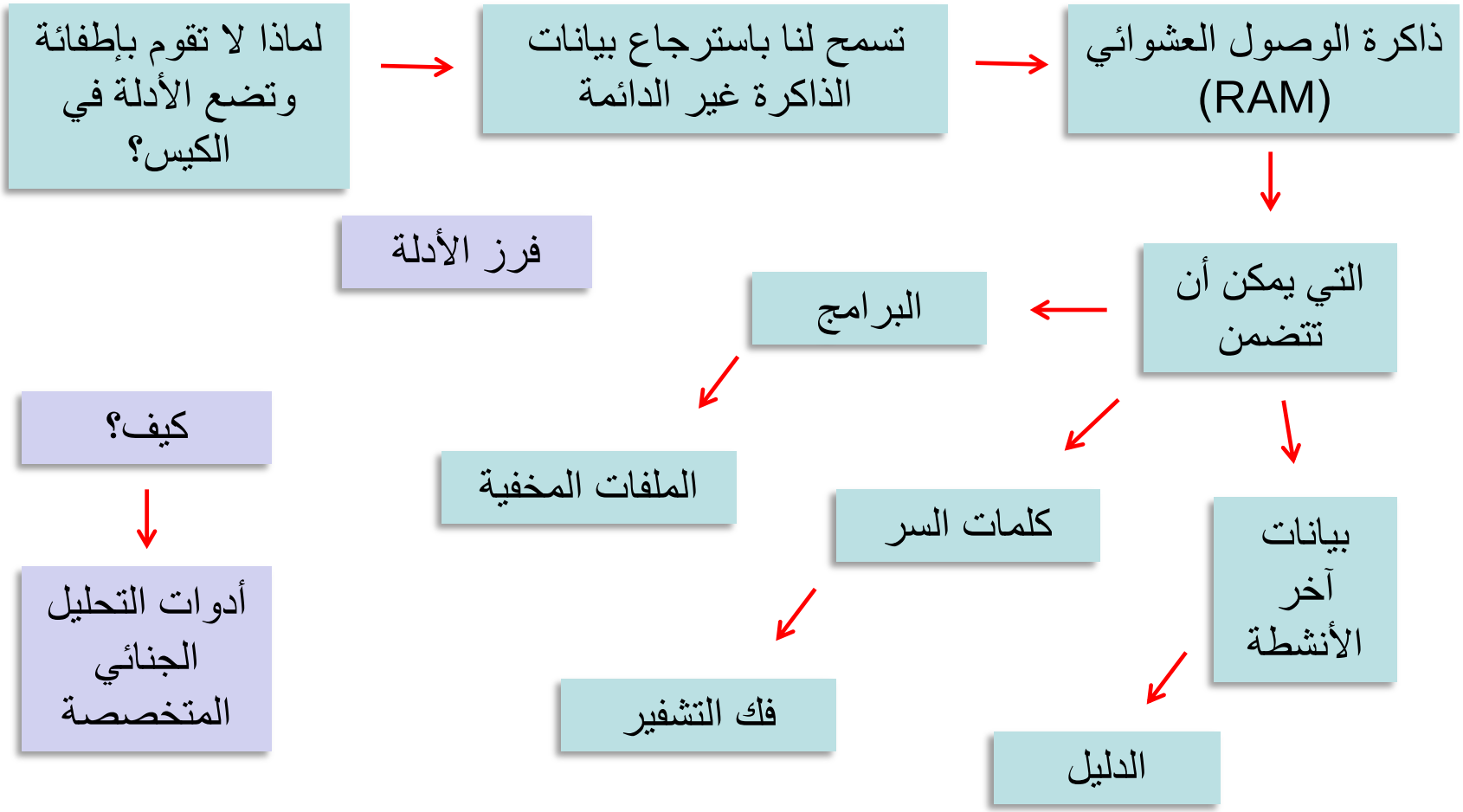
عرض توضيحي
Keyspace

الملفات المخفية وحافظة 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 إلكترونيا!

عرض توضيحي عن الصورة المخفية

الحصول الحي المباشر على البيانات والمعلومات



الحصول الحي المباشر على البيانات والمعلومات

أدوات التحليل الجنائي المتخصصة

EnCase® Portable

F-Response

RAPTOR 2.0
by Forward Discovery

FTK

IEF TRIAGE
INTERNET EVIDENCE FINDER

عرض توضيحي لبرنامج EnCase Portable

الحصول على بيانات الصندوق الميت

خلق صورة رقمية للتحليل

ماذا نفعل به؟

ضعها في الكيس!

في حالة إطفاء؟

كيف؟

إزالة المكونات الصلبة (هارد درايف)

ماذا لو لم تستطع الإزالة

الصورة باستخدام برامج وتطبيقات التحليل الجنائي

الصورة باستخدام أدوات تسجيل وخلق صور للتحليل الجنائي

قد يكون لدى الكمبيوتر طريقة خاصة لتحميل/إعادة تحميل نظام التشغيل

RAPTOR 2.0

EnCase Portable

الحصول على بيانات الصندوق الميت

أدوات تسجيل وإعداد صور الأدلة للتحليل الجنائي

- تتيح وجود جسر بين الوسائط

- تتيح خاصية حماية الكتابة للحفاظ على الأدلة

عرض توضيحي للحصول على بيانات بطاقة الذاكرة

صورة بيانات وأدلة التحليل الجنائي

ما هي صورة بيانات وأدلة التحليل الجنائي؟

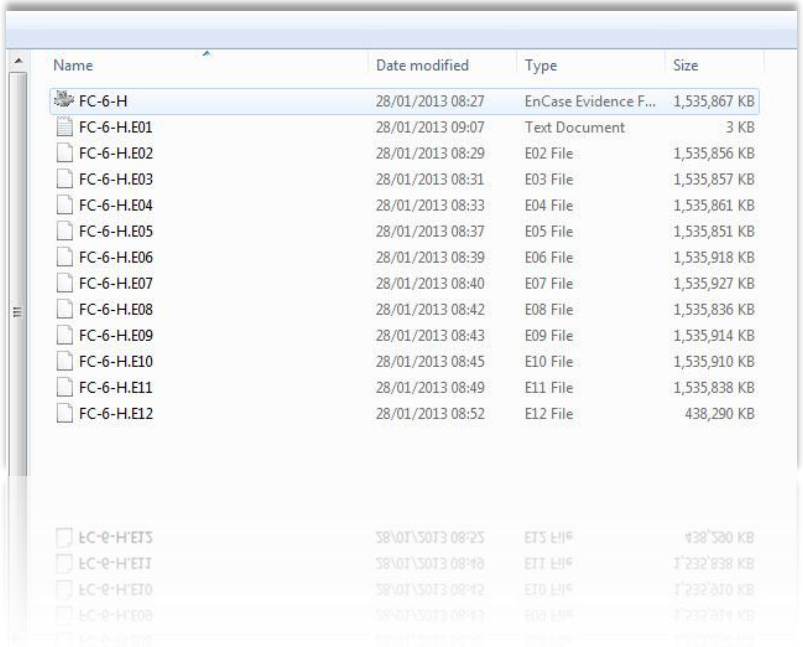
وعاء البيانات المحمية

رقم تعريف فريد (Hash)

Hash
مهم لإظهار الاستمرارية

تتكون من:

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



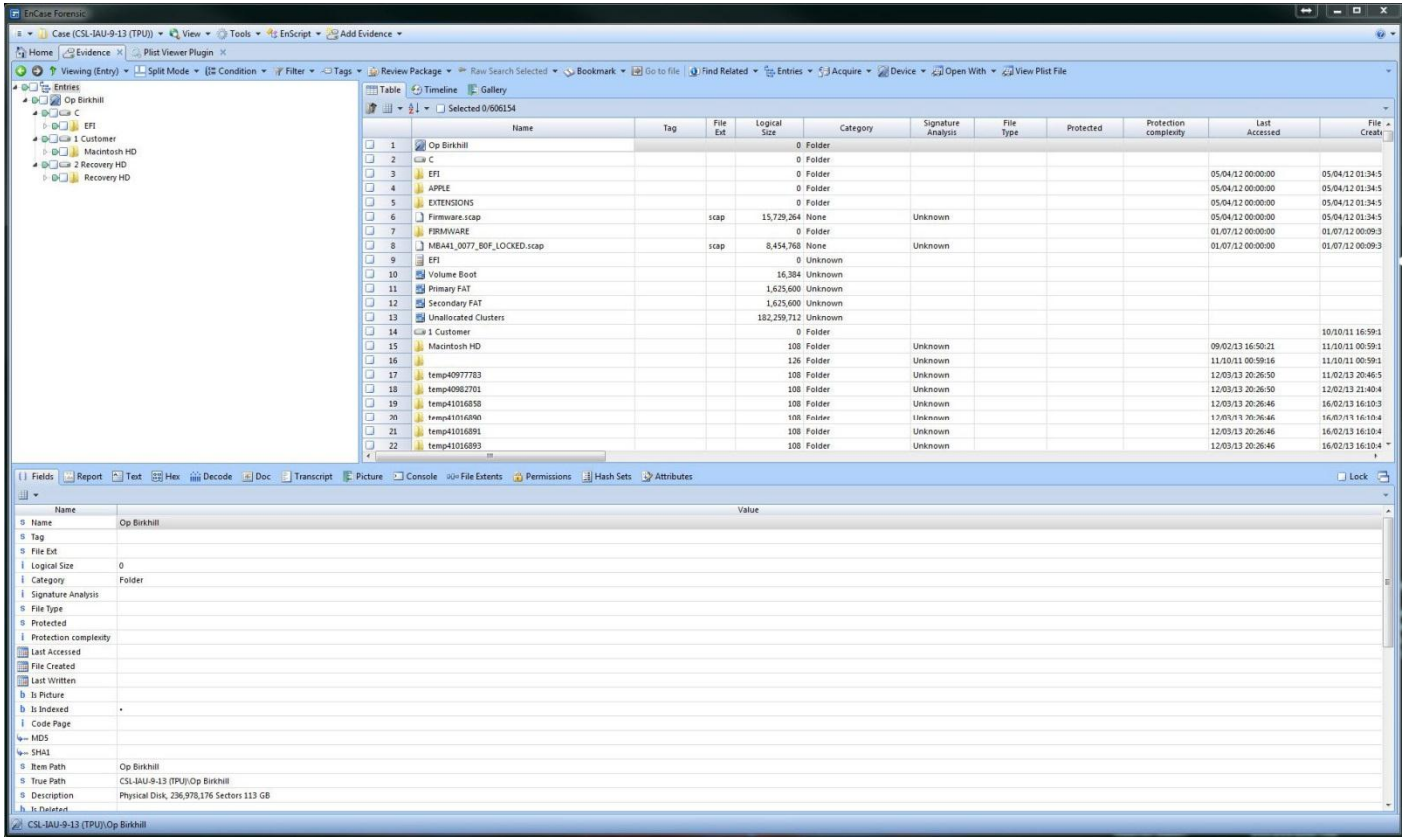
Name	Date modified	Type	Size
FC-6-H	28/01/2013 08:27	EnCase Evidence F...	1,535,867 KB
FC-6-H.E01	28/01/2013 09:07	Text Document	3 KB
FC-6-H.E02	28/01/2013 08:29	E02 File	1,535,856 KB
FC-6-H.E03	28/01/2013 08:31	E03 File	1,535,857 KB
FC-6-H.E04	28/01/2013 08:33	E04 File	1,535,861 KB
FC-6-H.E05	28/01/2013 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

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

معالجة التحليل والنتائج

أدوات التحليل الجنائي

فاحص
EnCase



METROPOLITAN POLICE

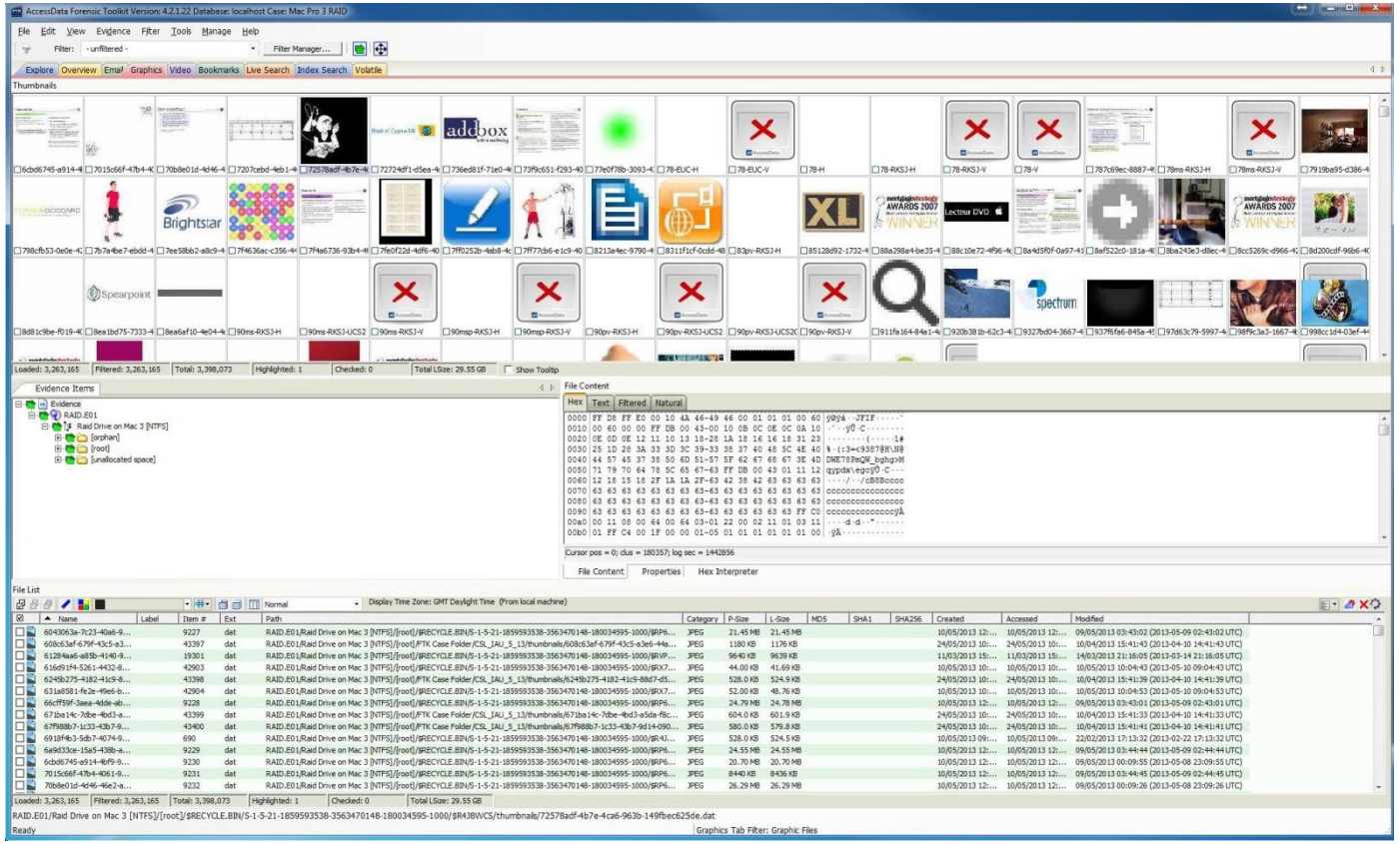
TOTAL POLICING

NEW SCOTLAND YARD

معالجة التحليل والنتائج

أدوات التحليل الجنائي

مجموعة أدوات التحليل الجنائي (FTK)



METROPOLITAN POLICE

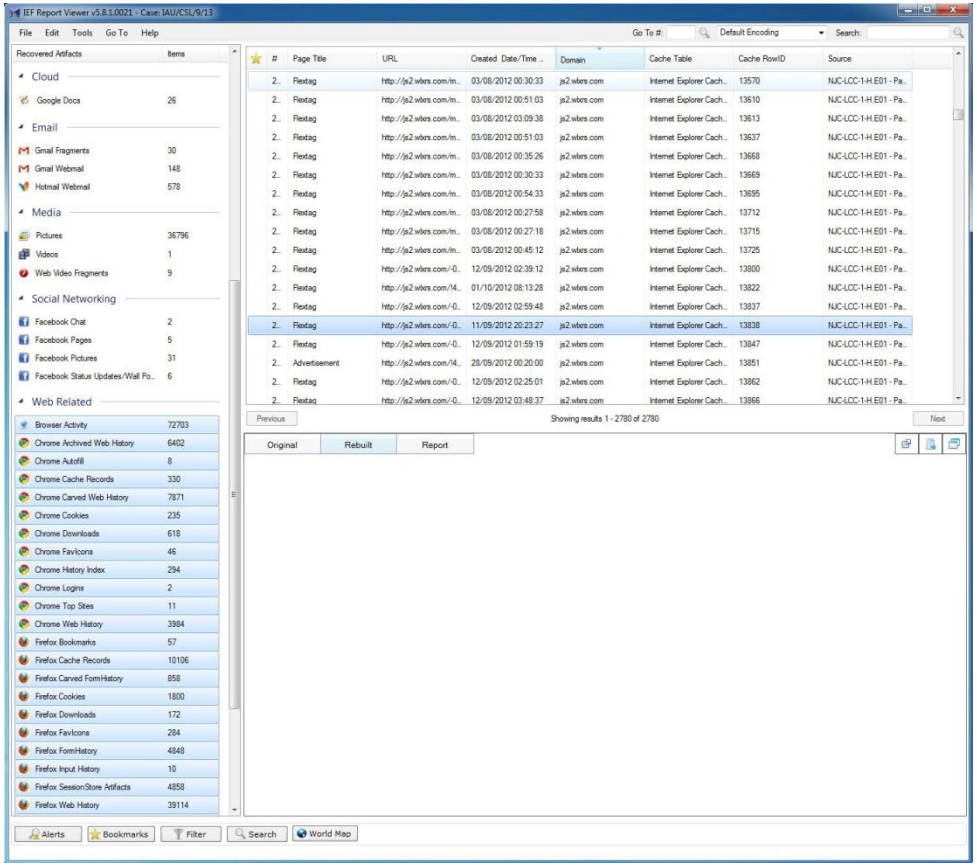
TOTAL POLICING

NEW SCOTLAND YARD

معالجة التحليل والنتائج

أدوات التحليل الجنائي

أداة العثور على الأدلة من الانترنت (IEF)



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
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
000060	00	02	00	00	00	06	00	00-00	B2	01	32	00	02	00	00
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
000090	00	04	00	00	00	01	00	00-02	52	00	00	03	1C	41	70
0000a0	70	6C	65	00	69	50	68	6F-6E	65	20	35	00	00	00	00
0000b0	00	48	00	00	00	01	00	00-00	48	00	00	00	01	36	2E
0000c0	31	2E	33	00	32	30	31	33-3A	30	35	3A	33	30	20	31
0000d0	32	3A	34	30	3A	32	31	00-00	18	82	9A	00	05	00	00
0000e0	00	01	00	00	01	F2	82	9D-00	05	00	00	00	01	00	00

مُحددات الملفات

رأس الصفحة

ذيل الصفحة

أدوات التحليل الجنائي – كيف تعمل

فحص جدول الملف الرئيسي

تسجيل جميع الفايلات المخزنة على درايف

الحجم

اسم الملف

نوع الملف

المكان

تم إنشاؤه

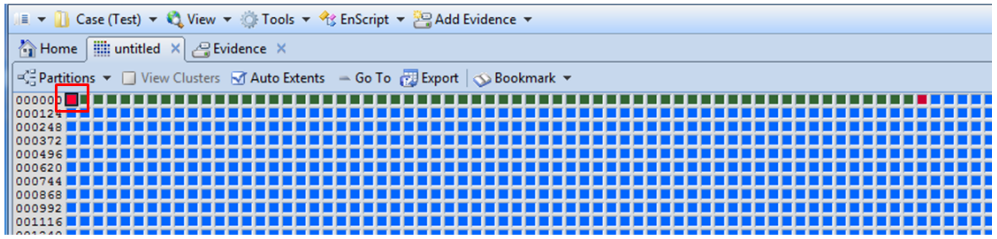
تم الدخول عليه

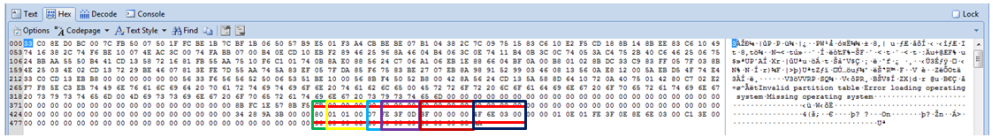
تم تعديله

تم حذفه

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

عرض توضيحي لبطاقة ذاكرة مجموعة أدوات
التحليل الجنائي FTK Memory Card

البيانات الوصفية (ميتاداتا) وبيانات إكسيف

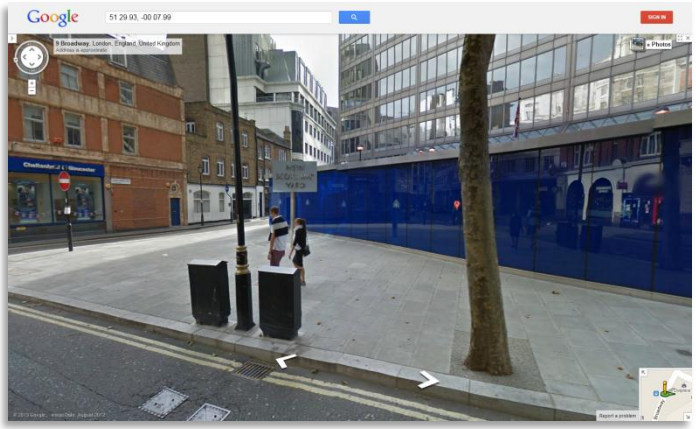
المعلومات داخل ملف صورة

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 وطرازها ونوعها

تحديد المواقع الجغرافية



تواريخ

أوقات

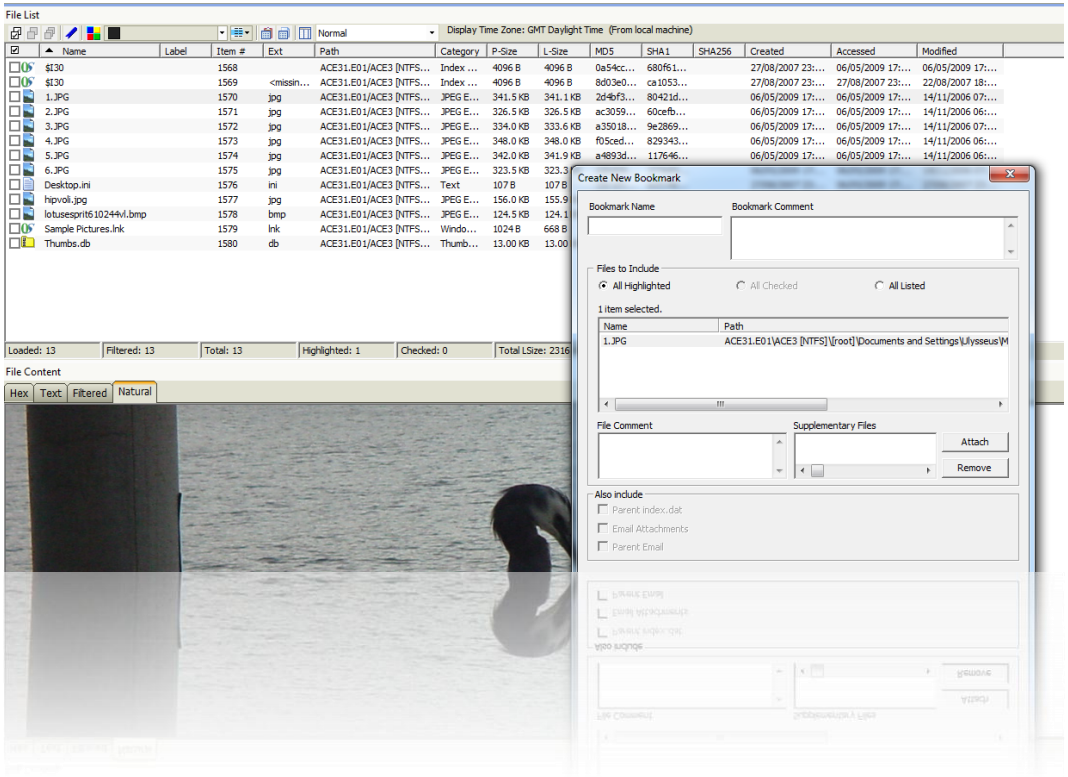
المؤلف

عرض توضيحي لبيانات إكسيف

معالجة التحليل والنتائج

العلامات المرجعية (بوك مارك) والتقارير

- تظليل الملفات
- إضافة تعليقات
- إرفاق ملفات
- النقل إلى التقارير



تكاليف المختبرات

- المقاولون والمتعاقدون

مقابل

- الموظفون
- الأجهزة والمعدات
- التدريب

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 إلكترونيا
- 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