

تم تحميل الملف من موقع
البوصلة التقنية
www.boosla.com

احذر خطر سرقة الملفات والصور من الموبايل

جرائم الكمبيوتر و التجسس الإلكتروني الدولي والشخصي للمعلومات (دراسه أولى لـ JAAS)
جميع اجزاء الموضوع تجدها في الموقع <http://www.JAAScois.com>



تحليل أنظمة الأجهزة الكفية وإستعادة البيانات المحذوفة Data Recovery
تحليل بطاقات SIM للأجهزة الكفية وإستعادة البيانات المحذوفة Data Recovery
سندخل اليوم في مجال تحليل جرائم الكمبيوتر للأجهزة الكفية والموبايل
وتحليل بطاقات SIM card ، هذا المجال اشتهر في الاوانه الاخيرة بشكل
كبير ويعتبر مجال مهم في تحليل جرائم الكمبيوتر
وينقسم هذا الموضوع الى ثلاثة اجزاء وهي

١ - تحليل بطاقات GSM SIM card

وهو عبارة عن تحليل شامل ومفصل لأرشفة بطاقات الموبايل مثل
الاتصالات والارقام والوقت لمعرفة الرسائل المرسله والمستقبله وإعادة
الرسائل التي تم حذفها ، ومعرفة الارقام المخزنة
التي تم الاتصال بها او تلقي مكالمات منها واعاده الارقام التي تم حذفها ،
وتحليل اكواد البطاقة PIN and PUK والتلاعب بها وترميز الشبكات

هذا القسم يعتبر حل شامل لكشف اغلب الجرائم مثل جرائم التهديد وتعقب
الاتصالات وحتى تحليل كامل لشخصية صاحب الموبايل الجهات التي
يتعامل معها والارقام التي يتصل بها والرسائل التي
يحذفها باستمرار والاقوات التي يستخدم بها الموبايل للوصول الى دليل معبر

من اشهر البرامج المستخدمة في هذا المجال برنامج SIMCon وهو عملي
وهذا مثال لإستخراج بعض المعلومات المحذوفة لرسائل SMS

Item	Value	File
<input type="checkbox"/> Short Message 1	(in) Any chance to see you Today?	EF_SMS
<input type="checkbox"/> Short Message 2	(out) w8 10 sec	EF_SMS
<input type="checkbox"/> Short Message 3	(out) hello darling, i will be late today. loads of work...	EF_SMS
<input type="checkbox"/> Short Message 4	(in) Ok	EF_SMS
<input type="checkbox"/> Short Message 5	(in) Not AGAIN! See you tonight	EF_SMS
<input type="checkbox"/> Short Message 6		EF_SMS
<input type="checkbox"/> Short Message 7	(del) Hi again sweetie. That bitch still believes me. Your pl...	EF_SMS
<input type="checkbox"/> Short Message 8	(del) Hi again sweetie. That bitch still believes me. Your pl...	EF_SMS
<input type="checkbox"/> Short Message 9	(in) Ok see you later sexy.	EF_SMS
<input type="checkbox"/> Short Message 10		EF_SMS
<input type="checkbox"/> Short Message 11		EF_SMS
<input type="checkbox"/> Short Message 12		EF_SMS

رسائل SMS

حاله الرسائل محذوفة

Number : deleted

g plan : international

4790002100 : رقم مركز الرسائل

SMS-SUBMIT

no RP

TP-SRR) : status report not requested

(R) : 213

ber : international

lan : E.164 ISDN

-DA) : 4741428707

-PID) : mobile-mobile

ng : GSM

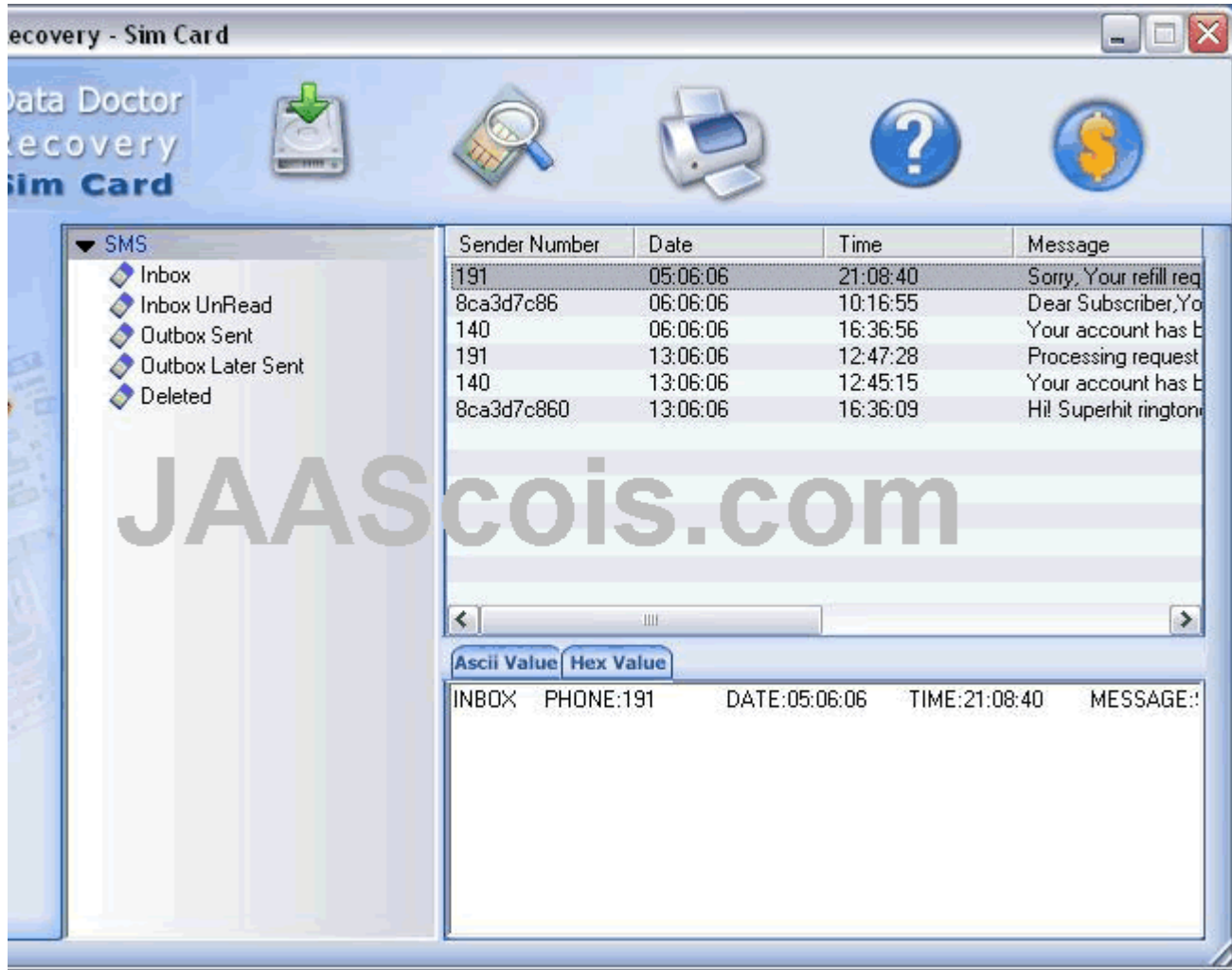
s : Immediate display

s : 63 weeks

Hi again sweetie. That bitch still believes me. Your place at 5?

المدة ونص الرسالة

وتوجد برامج ايسط مثل Sim Card Data Doctor Recovery



٢ - تحليل الذاكرة للأجهزة الالكترونية

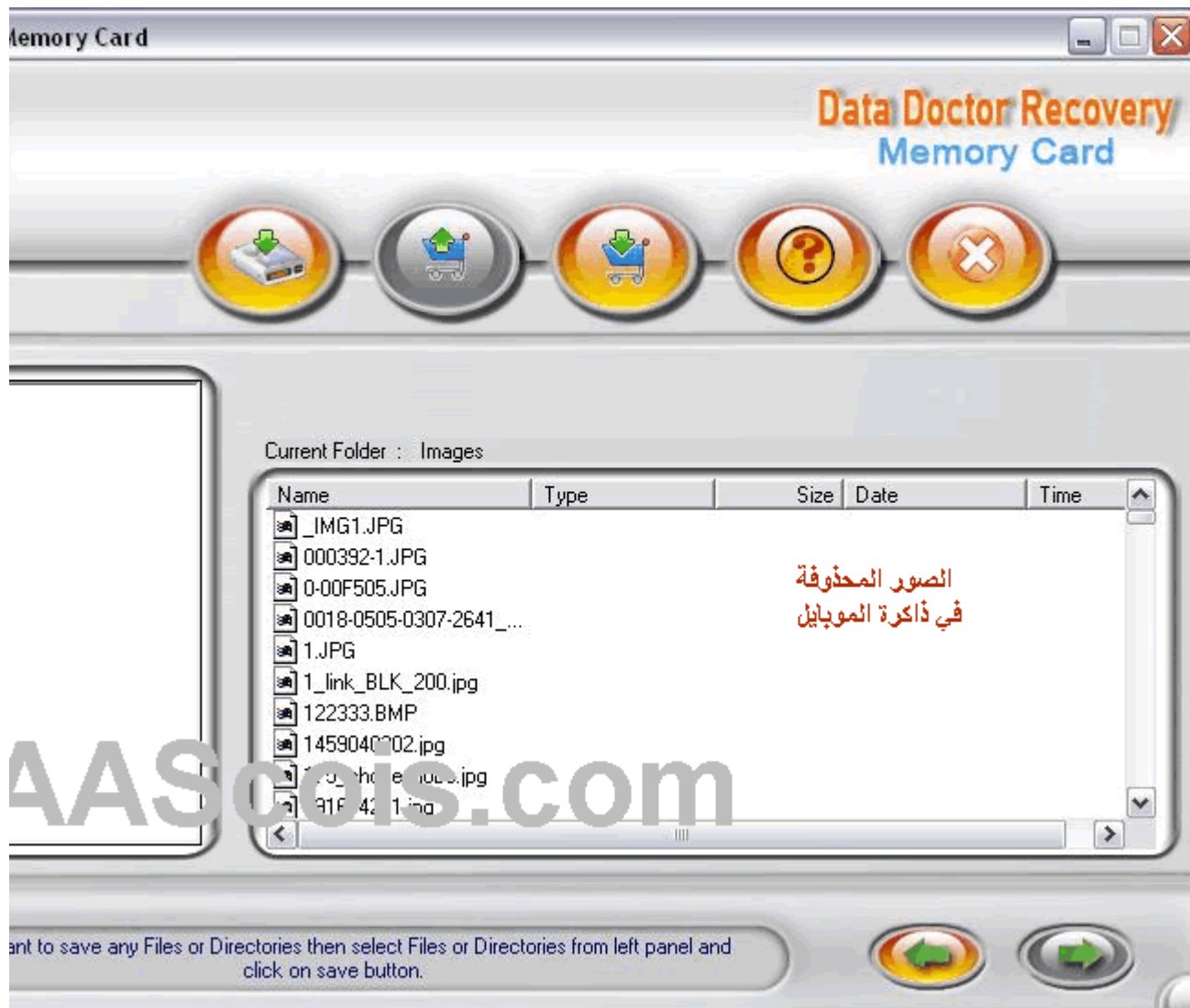
اغلب الاجهزة الالكترونية تحتوي ذاكرة لتخزين الملفات والبيانات مثل ذاكرة الموبايل وذاكرة الكمبيوتر الرقمية وذاكرة اجهزة الموسيقى وغيرها، يتم حل اغلب الغاز الجرائم الالكترونية بتحليل هذه الذاكر لمعرفة الملفات التي استخدمت والصور التي تم التقاطها ومشاهد الفيديو التي صورت حتى بعد حذفها او عمل فورمات للذاكرة وتستخدم برامج تحليل كثيرة في مثل هذا المجال منها

Memory card data recovery software
Digital camera data recovery software
Pen drive data recovery software
iPod data recovery software
Removable media data recovery software
Digital pictures recovery software
Zune music recovery software

او تستخدم اجهزة هاردوير خاصة للتحليل مثل Disklabs Memory Card Recovery ويمكنك مشاهدة مثال بالفيديو هنا

<http://www.mobilephoneforensics.com/mobile-phone-forensics.wmv>

او باستخدام احد البرامج المتخصصة + وصله USB تستطيع استرجاع وتحليل كافة البيانات في الذاكرة



وتوجد برامج متخصصة لتحليل أنظمة الاجهزة الكفية مثل أنظمة WinCE و Palm OS و Pocket PC ومثال على ذلك برنامج pdaseizure

PDA Seizure - C:\Program Files\Paraben Corporation\PDA Seizure\Jornada.PDA

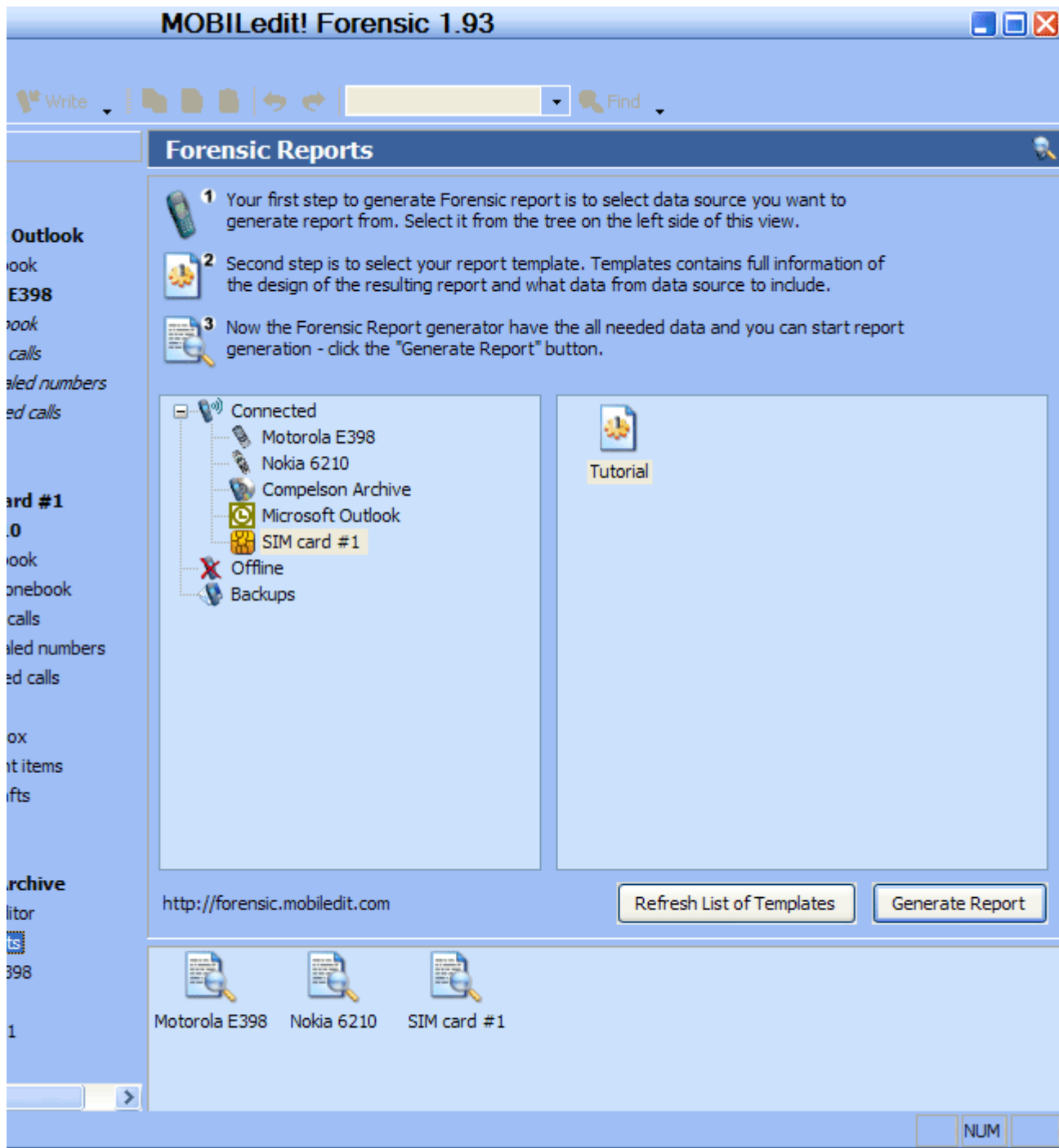
File Edit Tools View Help

Files Search Graphics Bookmarks

File Path	File Name	Type	Create Date	Modify Date	Attributes	Size	Status	L...	MD5 Hash
	Registry					3,966	Registry		3050A80D...
	MemImage					3,680	MemoryImage		F2C44410f
{Program Files}\Win default.	.lnk	.lnk	2000/01/01 20	2000/01/01 20:A		23	Acquired	RAM	6BD33A627
{My Documents}\Welcome To W.	.wma		2000/01/01 20	2000/01/01 20:A		24	Acquired	RAM	818AA698x
{My Documents}\Te Vehicle Mileage.	.pvt		2000/01/01 20	2000/01/01 20:HRA		7,498	Acquired	RAM	9C918BEFE
{My Documents}\Te To Do.	.psw		2000/01/01 20	2000/01/01 20:HRA		2,616	Acquired	RAM	0F7982DEE
{My Documents}\Te Phone Memo.	.psw		2000/01/01 20	2000/01/01 20:HRA		2,008	Acquired	RAM	9443F21C4
{My Documents}\Te Memo.	.psw		2000/01/01 20	2000/01/01 20:HRA		2,112	Acquired	RAM	523694AF6
{My Documents}\Te Meeting Notes	.psw		2000/01/01 20	2000/01/01 20:HRA		1,908	Acquired	RAM	40FB8E424
{My Documents}\Te Blank Documer	.psw		2000/01/01 20	2000/01/01 20:HRA		0	Acquired	RAM	
{My Documents}\Te To Do.	.pwi	.pwi	2000/01/01 20	2000/01/01 20:HRA		3,096	Acquired	RAM	B25EAC50:
{My Documents}\Te Phone Memo.	.pwi		2000/01/01 20	2000/01/01 20:HRA		2,008	Acquired	RAM	7F2CCAB0f
{My Documents}\Te Memo.	.pwi		2000/01/01 20	2000/01/01 20:HRA		2,112	Acquired	RAM	CAC4C826
{My Documents}\Te Meeting Notes	.pwi		2000/01/01 20	2000/01/01 20:HRA		1,592	Acquired	RAM	B876D7DEr
{My Documents}\Te Blank Note.	.pwi		2000/01/01 20	2000/01/01 20:HRA		0	Acquired	RAM	
{Windows}\Home M HP game butt.	.lnk		2000/01/01 20	2000/01/01 20:A		18	Acquired	RAM	72E4BACB:
{Windows}\Home M HP backup.	.lnk		2000/01/01 20	2000/01/01 20:A		20	Acquired	RAM	8DA836DA
{Windows}\Home M Regional Settir	.lnk		2000/01/01 20	2000/01/01 20:A		28	Acquired	RAM	E0723177E
{Windows}\Home M Network.	.lnk		2000/01/01 20	2000/01/01 20:A		28	Acquired	RAM	AD4F5D1A
{Windows}\Home M Clock.	.lnk		2000/01/01 20	2000/01/01 20:A		28	Acquired	RAM	2FA61C98x
{Windows}\Home M Modem.	.lnk		2000/01/01 20	2000/01/01 20:A		28	Acquired	RAM	AC946E0E7
{Windows}\Home M PC.	.lnk		2000/01/01 20	2000/01/01 20:A		28	Acquired	RAM	C02FC610:
{Windows}\Home M Today.	.lnk		2000/01/01 20	2000/01/01 20:A		28	Acquired	RAM	6A65E55E:
{Windows}\Home M Buttons.	.lnk		2000/01/01 20	2000/01/01 20:A		28	Acquired	RAM	7CCAC988

634 Files NUM

وبرنامج Mobiledit Forensic لدعم انواع متعددة من الموبايلات وتحليلها



ملاحظة:

وبعد ان شاهدت طريقة استعادة الملفات المحذوفة والرسائل اي كانت ، انصحك بعدم حفظ اي معلومات شخصية او صور او فيديو خاص في ذاكرة الموبايل واذا كنت مصر انصحك بعدم بيع الذاكرة مع الموبايل او الموبايل بشكل عام لانه يكشف اسرارك ببساطة ؟

٣- والنوع الثالث هو باستخدام برامج تحليل الانظمة الالكترونية وناقشنا هذا الموضوع بتفصيل في الصفحة التاليه

<http://www.jascois.com/research/36601029>

وبالتوفيق للجميع ،،، ترقبوا بقيه الاجزاء
لموضوع

جرائم الكمبيوتر و التجسس الإلكتروني الدولي والشخصي للمعلومات (دراسه أولى لـ JAAS)
<http://www.jascois.com>