الفصل الثالث
في التحيل الجنائي التقني لمكونات الموبايل

أولاً: العلوم الجنائية الافتراضية

ثانياً: الفحص أو التحليل الآلي الجنائي التقني للموبايل:

أولاً: معني التحليل الجنائي:

أ. إظهار الموجود:

1. من رسائل 2. من مكالمات 3. من صور

ب – لإظهار أو استعادة أو استرداد المحذوف:

1. استعادة أو أظهار أو استرداد الرسائل المحذوفة.
2. استعادة أو إظهار أو استرداد المكالمات المحذوفة.
3. استعادة أو إظهار أو استرداد الصور المحذوفة.

ج - فك كلمات السر والشفرات.

تحليل الرقم المسلسل للجهاز.

تحليل رقم البطاقة (بطاقة المشترك).

ثانياً: عملية التحليل الجنائي الآلي التقني للموبايل:

1– أدوات وطرق التحليل بالكمبيوتر:

أ. أدوات التوصيل بين الجهاز والكمبيوتر الـــ **USB**

ب. أدوات وبرامج التحليل.

- **Personal Digital Assistants (PDA)**
- **Pocket PC**
- **Palm OS**
- **EnCase**
- الـــ **XACT**
- الـــ **EnCase Neutreno**
- الـــ **Doctor Pro**

أخري

2- طرق تحليل أرقام الموبايل على الإنترنت:

ثالثا: الفحص اليدوي للجهاز:

أ – للإستفادة منه في مسرح الجريمة.

ب - مضاهاة رسائل وتحليلها

أولاً: العلوم الجنائية الافتراضية

العلوم الجنائية التي تفسر الدليل المحتوي في أجهزة الكمبيوتر والأوساط الرقمية تُعرف بالعلوم الجنائية الإفتراضية. **Cyber Forensics** هذا المجال يتعلق باظهار المعلومات واسترداد وفك شفرات المعلومات المخبأة أو المخفية في الموبايل موضوع الفحص أو القضية أو الكمبيوتر كذلك **Data Hidden on a Suspected Computer and Mobile Phones phones** وغيرها من الأجهزة الكفية[28] ويتم نقل المعلومات من شريحة الموبايل إلي الكمبيوتر عن طريق جهاز يُعرف بال **Flasher Box**[29].

ثانياً: الفحص أو التحليل الآلي الجنائي التقني للموبايل

يظن المجرم انه قد ارتكب جريمته باستعمال الهاتف الجوال أو أى جريمة أخرى كان الهاتف فيها طرفا - أنه بعيداً عن التتبع والتعرف عليه وخاصة استغلاله شريحة غير مسجلة باسمه ولكن التكنولوجيا التى أوجدت الجهاز الصغير القادر على ارتكاب الجرائم الكبيرة يمكن وبكل سهولة الحصول على بياناته وتوجد خاصية تُعرف بخاصية التتبع والتى من خلالها يمكن معرفة أماكن تنقل حامل الهاتف الجوال لإثبات تواجده فترة ارتكاب الجريمة وذلك عبر الأقمار الصناعية.من خلال شبكات سيأتي ذكرها للإتصال الدولي.

العصابة سقطت بعد تحويل الرصيد!

اسيوط- محمد منير

ألقت مباحث اسيوط القبض على عصابة للسرقة بالاكراه مكونة من سبعة اشخاص قامت باحد هؤلاء على صاحب مزرعة دواجن وانتزاع منه على ٤٦ الف جنيه علاوة على هاتفه المحمول تحت تهديد بندقية آلية.. استغلت المباحث الاموال المسروقة وتمكنت من تحديد شخصيات الجناة بعدما اكتشف قيام احدهم بتحويل رصيد من هاتف المجني عليه الى هيفونه الخاص وقع الحادث بقرية بني عدلا التابعة لمركز القوصية حيث تلقى اللواء محسن مراد مدير امن اسيوط اخطارا بلاغ بالواقعه كشفت مناقشة العديد ابراهيم صابر مدير البحث الجنائي المجني عليه ان الجناة كانوا يرصدون تحركاته وعلموا بوجود ايراد بيع دورة الدواجن معه بحامت الشبهات حول طالب مقيم بجوار المزرعة وبتتبع من موقف رصد تحركات صاحبها وتأكدت التحريات بعدما تبين انه تم تحويل رصيد من الهاتف المسروق الى هاتف الطالب فتم القبض عليه حيث اعترف على باقي شركائه من العاملين.

صورة تبين أهمية وجود الموبايل في مسرح الجريمة المنشورة في جريدة الأخبار المصرية

أولاً: معني التحليل الجنائي التقني:

أ) **لإظهار الموجودات**: يتم استخدام وسائل وأدوات التحليل لجهاز الموبايل **Mobile Device Analysis** ومنها البسيطه لإظهار الموجود خلال التعامل ومالم يكن محذوفا احيانا لعرض جنائي واحيانا يحتاج لها المستعمل للجهاز بغرض عمل نسخة من سجل الهاتف او عندما يغير الشريحه أو الجهاز وماهو موجود على الشريحة او الذاكرة وربما بالذاكرة الداخلية للجهاز يكون كلآتي:

1. رسائل 2. صور 3. سجل هاتف

ب) **لإظهار أو استعادة أو استرداد المحذوف**: لقد امكن وبفضل جهود العلماء الأكادميين والمهندسين التقنيين من ايجاد أدوات تحليل لمكونات الموبايل لأظهار ما يكون قد حذف من :

1. رسائل 2. مكالمات 3. صور 4. إيميلات

ويتضمن الكشف عن المستور التواريخ والساعة التي أُجريت فيها المكالمة أو التي أُستقبلت فيها والوقت الذي أرسلت فيه الرسالة والذي استقبلت فيه الأخري. وهو ماله أهمية كبيرة في التتابع الزمني للجريمة.

والتحليل لإستعادة المحذوفات يتطلب :

1. تحليل البطاقة SIM Card لإستعادة أو أظهار أو استرداد الرسائل المحذوفة.
2. تحليل البطاقة SIM لإستعادة أو إظهار أو استرداد المكالمات المحذوفة.
3. تحليل البطاقة Memory Card لإستعادة أو إظهار أو استرداد الصور المحذوفة.

ج) **فك كلمات السر والشفرات**: كثيرا ما يواجه خبير الفحص الفني التقني لجرائم الموبايل وجود ارقام سرية لقفل الجهاز او الرسائل او المكالمات او الصوت او الملفات ولذا يتوجب معرفتة وجاهزيتة لفك الرموز والتي قد توفرها شركات التصنيع أو تتوفر لأغراض اخري وهنا تُثار عملية الإختراق لشرعية الجهاز وما هو الذي يجب الاطلاع عليه ومالايجب اثباتة لأنه كماهو التفتيش في النواحي القانونية والتي يحظر قانون الإجراءات الجنائية القيام به إلا وفق الاجراءات وإلا كان التفتيش باطلاً لبطلان الاجراءات.

ثانياً: عملية التحليل الجنائي الآلي التقني للموبايل:

1- أدوات وطرق التحليل بالكمبيوير:

أ) أدوات التوصيل بين الجهاز والكمبيوتر الـــ USB.

ب) أدوات وبرامج التحليل.

2- طرق تحليل أرقام الموبايل على الإنترنت:

1- أدوات وطرق التحليل بالكمبيوير

أ) أدوات التوصيل بين جهاز الموبايل والكمبيوتر الـــ USB: والـــ USB تعني Universal Serial Busوهي وصلة Cable بين الموبايل والكمبيوتر حيث يوصل أحد طرفيها في جهاز ا الموبايل والآخر في جهاز الكمبيوتر وذلك لنقل المعلومات من الموبايل إلي الكمبيوتر حيث يتم استعراضها على الشاشة ،أي يمكن قراءتها وتخزينا وطبعها.

إلي الكمبيوتر إلي الموبايل

وصلة الـــ USB بين الموبايل والكمبيوتر والمسماة بالـــ Cable لها طرفان

2- قارئات المعلومات:

(أ)

(ب)

(ج)

(أ، ب، ج) ثلاثة أشكال من القارئات أ، ب لقراءة بطاقة المشترك SIM وج لقراءة للذاكرة

نوع من وصلات الـــ USB لقراءة الذاكرات المختلفة الحجم

ب) أدوات وبرامج التحليل: الحصول على الرسائل النصـــية المحذوفـــة والمعلومـــات الأخري المخزنة على بطاقة المعلومات SIMالممحوة مثل الرسائل القصيرة SMS علـــى بطاقة المشترك ـــ أداة واسترداد ملفات الشريحة يعيد معلومات الموبايل المزالة أو التالفة أو التي محيت بصورة عارضة من الذاكرة.

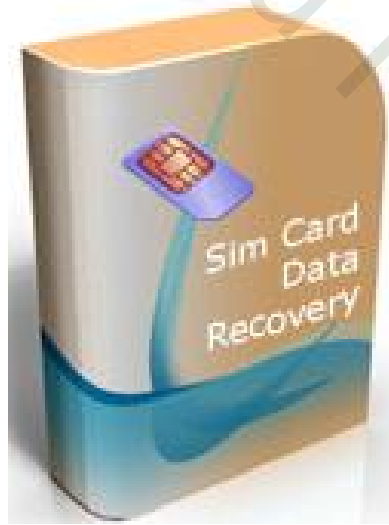
أداة إظهار بيانات بطاقة المشترك لا تؤثر على البيانات:

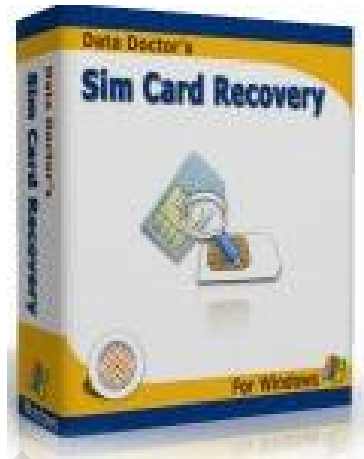
برمجيات استعادة بيانات كل الرسائل النصية المحذوفة وأرقام الهاتف المفقودة من بطاقة موبايلك. وتسمح بعرض المعلومات بما في ذلك حذف أرقام الاتصال والرسائل النصية (الرسائل القصيرة). وتسمح للمستخدم لاعداد تقرير مفصل لعرض تاريخ ووقت إرسال الرسائل نصية.

برمجيات استعادة بيانات بطاقة المشترك صنعت لتسترد بأمان جميع ما حذف من رسائل نصية من شريحة الموبايل. بمساعدة يو إس بي قارئ بطاقة سيم فالأداة بفحص بطاقة المشترك وتسترد المعلومات المحذزفة بسرعة وبنجاح. من الناحية التطبيقية فهي مفيدة جدا لضباط التحقيق للحصول على الأدلة من البطاقات واسترداد الرسائل النصية المحذوفة وأرقام الاتصال المخزنة.

مميزات البرمجيات :

- استعادة بيانات بطاقة المشترك هي للقراءة فقط وغير مدمرة للمساعدة في استعادة البيانات.
- بفعالة لتستعيد البيانات التي حذفت بطريق الخطأ.
- تسترد الرسائل النصية القصيرة المحذوفة وأرقام الاتصال المحفوظة فيذاكرة بطاقة موبايلك.





SIM Cardالمشترك أداة (برنامج) تحليل بطاقة

شكل آخر من ادوات التحليل

ملحوظة:

موضح التقرير الخاص باداة التحليل Pro Data Doctor بالفصل السابع وعن طرق تحليل بطاقات SIM للأجهزة الكفية والموبايل واستعادة البيانات المحذوفة Data Recovery .

تحليل جرائم الكمبيوتر للأجهزة الكفية في مجال والموبايل وتحليل بطاقات SIM card وهذا المجال اشتهر في الآوانه الأخيرة بشكل كبير ويعتبر مجال مهم في تحليل جرائم الكمبيوتر وينقسم هذا الموضوع إلى ثلاثة أجزاء وهي:

1. **تحليل بطاقات GSM SIM card** : وهو عبارة عن تحليل شامل ومفصل لأرشيف بطاقات الموبايل مثل الاتصالات والأرقام والوقت لمعرفة الرسائل المرسلة والمستقبلة وإعادة الرسائل التي تم حذفها , ومعرفة الأرقام المخزنة التي تم الاتصال بها أو 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 والأوقات التي يستخدم بها الموبايل للوصول إلى دليل معين ومن اشهر البرامج المستخدمه في هذا المجال برنامج SIMConوهو عملي وهذا مثال لإستخراج بعض المعلومات المحذوفة لرسائل SMS وتوجد برامج ابسط مثلData Doctor Recovery - Sim Card .
2. **تحليل الذاكرة**: اغلب الاجهزة الالكترونية تحتوي ذاكرة لتخزين الملفات والبيانات مثل ذاكرة الموبايل وذاكرة الكاميرا الرقمية يتم حل اغلب الغاز الجرائم الالكترونية بتحليل هذه الذواكر 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 recovery software أو تستخدم اجهزة هارد وير Hardware خاصة للتحليل مثل Disklabs Memory Card Recovery ويمكن مشاهدة مثال بالفيديو على الموقع هنا[30]:

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

مايبحث عنه الفاحص في المجال الجنائي للموبايل الأتي:

1-_ Calendar Entries
2_ Call History (Inbound and Outbound)
3_ Contacts/Phonebook
4_ Email
5_ Internet History
6_ Instant Messaging (IM) chat
7_ Multimedia Messages (MMS)
8_ Pictures
9_ Short Message Service (SMS) or Text Messages
10_ Telecommunication Settings
11_ Videos
12- Voice Mail

تتوقف عملية التحليل الجنائي على :

_ Analysis tool أداة التحليل

_ Proprietary file systems أنظمة الملفات

_ Vendor installed files and configuration of the device الملفات الممستخدمة

_ Technical skill of the examiner مهارة الفاحص

أنواع المعلومات التي توجد كدليل رقمي على الـــــ SIM:

1_ Last Number Dialed (LDN) الرقم الأخير

2_ Phonebook/Contacts (ADN) سجل التليفون والأتصالات

3_ Text Messages (SMS), including deleted text messages الرسائل القصـــيرة مشـــتملة الرسائل التي حذفت

4_ Location information (LOCI) from position of last usage بيانـــات الموضـــع الـــذي استخدم فيه الموبايل آخر مرة

5- Service Related Information خدمات متصلة بالمعلومات

أنواع المعلومات التي توجد كدليل رقمي على الـــــ Memory Cards:

1_ Pictures الصور

2_ Movies

3_ Audio Files الملفات الصوتية

4_ Documents المستندات

Network Service Provider (NSP) فوائد مزود الخدمة

يمد بالمعلومات عن information:

1_ Subscriber Information معلومات عن المشترك

2_ Call Data Records - related to phone calls and text Messages. المعلومات المسجلة المتعلقة بمكالمات الموبايلو الرسائل النصية

3_ Subscriber Location - this relates to geo location of the physical device, in an effort to track the subscriber. موضع المشترك من خلال حركة الجهاز املاحقم وتتبع المشترك

4_ BlackBerry Messaging التراسل عن طريق البلاك بري

هناك عدة اوامر للتراسل عبرجهاز البلاك بري وهي:

1) PIN to PIN
2) SMS
3) MMS (Multimedia Messaging Service)
4) Email

عمليات فحص أجهزة البلاك بري Examination of BB devices :

لا تختلف عن خطوات فحص الكمبيوتر وتتطلب من الفاحص عمل ملـف an IPD file.

أدوات المساعدات في تحليل الموبايل:

أدوات المساعدات الرقمية للمعلومات هي PDA's:

a) Palm Pilots (Palm OS),
b) Pocket PC's (Windows CE, Windows Mobile),
c) BlackBerry's (RIM OS) that contain no radio (cellular) capability.
d) Others (Linux, Newton).
e) EnCase

دورات لتعليم استخلاص المعلومات جنائيا من الـ EnCase tool [31]:

- Students will learn the history of EnCase Neutrino
- Students will be given an overview of mobile phone networks
- Students will learn how to identify mobile phones
- Students will learn how to work with various service providers
- Students will learn proper seizure techniques
- Students will be given a detailed understanding of all componets that make up EnCase Neutrino
- Students will acquire data from mobile phones
- Students will acquire and examine SIM cards
- Students will examine the data that they have acquired
- Students will learn how to create logical evidence files with EnCase Neutrino
- Students will receive an overview of mobile phone data storage
- Students will learn how to use conditiona in EnCase Neutrino
-Students will learn how to report their findings EnCase NeutrinoMobile Phone Forensics

Day 1 في اليوم الأول يتم تعليم

- The history of EnCase Neutrino
- Overview of the GSM network
- Identifying and differentiating cell phones models
- Liaising with mobile phone service providers
- A detailed review of the components of EnCase Neutrino
- Acquiring data from mobile phones
- Working with and examining SIM(Subscriber Identify Module) cards
- Creating logical evidence files

Day 2 في اليوم الثاني يتم تعليم

- EnCase Neutrino mobile phone acquisition device components
- Mobile device data acquisition
- Examination of mobile phone data
- Overview of legal concernsTM

الـــ Pocket PC

برنامج التحليل الجنائي الـــ Pocket PC يعطي أفضـــل الحلـــول لإســـتخلاص كـــل المعلومات من الموبايل المرتبطة بالحاسب الآلي (الكمبيوتر) لأجهزة الـــ PDA والـــــ Smart Phones والمعلومات تشمل :

1-Windows registry records.
2- database records.
3- files information (video files).
4- saved text messages.
5- personal contact numbers.

وهي أداة زكية لفحص معظم أجهزة الموبايل وتشمل:

Sony Ericsson, LG, Nokia, Motorola, Blackberry, Samsung and many more.

ومميزات البرنامج هي:

1. استخلاص المعلومات المفصلة للتليفونات الذكية (الموباليلات الذكيـــة) وأجهـــزة ال **PDA**.
2. استعراض سجلات الـــ **windows** وسجلات قاعدة المعلومات وأرقام الإتصال للـــــ **multimedia cell phone**

ملحوظة: موضح جانب من التقرير الخاص بالـــ**Pocket PC** بالفصل السابع

ب) طرق تحليل ومحللات أرقام الموبايل على الإنترنت: تحليل أرقام الموبايل Mobile Number Analyzer[32]:

هنا مصادر مفيدة لتحليل أدلة الموبايل وهي متاحة عبر الإنترنت بالمجان ويمكن لمـــن يتصدي لتحليل جرائم الموبايل استخدامها

وفيما يلي المواقع الخاصة بالتحليل:

1. تحليل ارقام الاتصال Phone Dialing Number Analysis عاي الموقع.

https://www.numberingplans.com//?page=analysis&sub=phonenr

2. تحليل **رقم المشترك** International Mobile Subscriber Identity (IMSI) Analysis

علي الموقع

https://www.numberingplans.com//?page=analysis&sub=imsinr

3- تحليل الرقم الدولي المسلسل للموبايلInternational Mobile Equipment Identity (IMEI) Analysis

علي الموقع

https://www.numberingplans.com//?page=analysis&sub=imeinr

4- تحليل الرقم المسلسل لشريحة الموبايل SIM Serial Number (SIM Card number) Analysis

علي الموقع

https://www numberingplans.com

أدوات تحليل الأرق Number analysis tools **تشمل أدوات التحليل الجنائي لجرائم الموبايل الآتي:**

» Phone number analysis
» IMSI number analysis
» IMEI number analysis
» SIM number analysis
» ISPC number analysis

تحليل أرقام الموبايل Analysis of telephone numbers:

فيما يلي الطريقة التي يتم بها تحليل مكونات الموبايل عبر برامج محملة على الإنترنت:

أدخل رقم الموبايل Enter telephone number below

analyse

Example: ***+49-209-8765432***

تحليل الرقم المسلسل للجهاز. Structure of an IMEI Number IMEI تركيب الرقم:

الرقم المسلسل **IMEI** يتكون من 15 -17 رقماً فإذا كان 15 رقماً يبحث في الـ 14 رقم ويكون الرقم 15 هو الحكم.

مع العام **2004** هذا الرقم قسم إلي **AA-BBBBBB-CCCCCC-D** والرقمان الأولان للتقرير ويدلان على مجموعة **The GSMA group** والمسمي **Type Allocation Code (or TAC)** والمجموعة التالية هي ستة أرقام الباقية من ال **TAC** لكن الأرقام **CCCCCC** هي ارقام تتابع الموديل والأخيرة **The Lu the GSMA group** والتي **The Type Allocation Code (or TAC hn Check digit,** والرقم الأخير هو لتعريف الرقم من خلال صيغة الجمع **Use of IMEI.Checksum Formula .**

كل الحكومات على مستوي العالم تجمع على تقديم الشكر لفائدة الرقم IMEI في حالة سرقة الجهاز من خلال مركز الرقم المسلسل بشركة الإتصال.

ويمكن اختبارما إذا كان الرقم IMEI أصلي أم تم تغييره عن طريق اختبار المجموع للأرقام Check Digit Computation كالآتي:

الرقم الأخير يمكن اختباره من خلال الـ check digit باستخدام اللوغاريتمات Algorithm وهو دالة في جميع ارقام الـ IMEI الأخري وهو لا ينقل إلي الشبكات والغرض من هذا الإجراء من باب الحراسة الأمنية. وال Check Digit يختصر إلي CD ودائما ال CDينقل إلي الشبكات على أنه صفر(0).

الإختبار يتم في ثلاث خطوات هي:

1. Starting from the right, double a digit every two digits (e.g., 7 → 14).
2. Sum the digits (e.g., 14 → 1 + 4).
3. Check if the sum is divisible by 10.

One can calculate the IMEI by choosing the check digit that would give a sum divisible by 10. For the example IMEI 49015420323751?,

IMEI	4	9	0	1	5	4	2	0	3	2	3	7	5	1	?
Double every other	4	18	0	2	5	8	2	0	3	4	3	14	5	2	?
Sum digits	4 + (1 + 8) + 0 + 2 + 5 + 8 + 2 + 0 + 3 + 4 + 3 + (1 + 4) + 5 + 2 + ? = 52 + ?														

To make the sum divisible by 10, we set ? = 8, so the IMEI is 490154203237518.

المرجع **http://en.wikipedia.org/wiki/IMEI**

ويمكن **تحليل الرقم خلال برنامج الإنترنت فورياً لمعرفة الرقم الصحيح كالآتي:**

Analysis of IMEI numbers تحليل الرقم المسلسل

All mobile phones are assigned a unique 15 digit IMEI code upon production. Below you can check all known information regarding manufacturer, model type, and country of approval of a handset.

Tip! The IMEI can be displayed on most mobile handsets by dialling *#06#. Otherwise check the compliance plate under the battery.
Top of Form
Enter IMEI number below

analyse

Example: ***350077-52-323751-3***

Analysis of SIM card number تحليل رقم بطاقة المشترك

لكل بطاقة من بطاقات شريحة المشترك في تليفون أو هاتف الموبايل رقم فريد وحيد. ويمكن إدخال رقم البطاقة في الخان التالية للتأكد من صلاحيتها ، وكذلك معرفة المزيد عن شبكة االموبايل التي اصدرت الشريحة

All mobile phone SIM cards have each been assigned a unique SIM card number. Below you can enter a SIM card number to check its validity as well as find out more about the mobile network that issued the chip.

Enter SIM card number below

8920022040816213961 analyse

Example: 8923440000000000003

وعندما وضعنا للبرنامج رقماً أحد اللأرقام به خطأ كانت النتيجة التالية:

ملاحظة:

من فضلك اختبر رقم بطاقة الـ SIM لأن الرقم الذي أدخلته لا يوجد لأي موبايل على أي شبكة على مستوي العالم

Bottom of Form
Note: Please check the SIM card number. The entered number was never issued by any mobile network worldwide.

وهذا الرقم يُعرف بالرقم الخاص ببطاقة المشترك أو أي شخص يحمل البطاقة للتعامل بها في الجهاز (International Mobile Subscriber Identity) IMSI

ويتكون هذا الرقم من 18 إلي 20 رقم وقد تكون في خمسة أو ستة أسطر بيانها كالتالي:

1. أول رقمين هما مفتاح دولي لكل الدول لانظمة الشبكات للإتصال وهما 89
2. الرقم الخاص بالدولة **Mobile Country Code MCC** .
3. الرقم الكودي للشبكة Mobile Network Code MNC .

ويتكون من 10 أرقام. ويتلوها أرقام مع حرف كلتالي:

الأكواد الخاصة بشبكات الإتصال:

Analysis of ISPC numbers

فيما يلي الأكواد المستخدمة:

international telecommunication networks to indentify eachother and interconnect, signalling points codes are used. Below you can find out more about specific ISPC codes:

Top of Form

Enter ISPC number below

analyse

Example: 5-018-4 or *00000110100111*

محللات أخري للموبايل:

الموبايل[33] :مفتش جهاز المفتش:

Mobile Phone Inspector Utility 2.0.1.5

يفتش عن كل شيئ في الجهاز حتي عن ارقامة وتحليلاتها وليس فقط عن الرسائل والمكالمات والصور وبذلك فهو يعطي تقريراً متكاملاً عن جهاز الموبايل ومكوناته واتصالاته ورسائلة وصوره. هذا البرنامج مناسب للموبايلات المصنعة من الشركات

Nokia, Haier, Motorola, Sony Ericsson, LG, Samsung, Spice, i-mate

ويعمل مع:

windows 98, 2000, 2003, ME, NT, XP and windows Vista.

ويُستخدم برنامج مثل برنامج Mobiledit Forensic لدعم أنواع متعـــددة من الموبايلات وتحليلها.وموضح جانب من التقارير بالفصل السابع.

برنامج يقوم بقراءة الرسائل بشكل مسموع(34):

TWT SMS Reader v 1.32.943

يقوم هذا البرنامج بقراءة الرسائل القصيرة بشكل مسموع

صورة للبرنامج

برامج XACT [35] :

هي برامج لاستعادة المواد المحذوفة من الموبايل:

هذه البرامج تُمكن الخبراء المختصين في التحقيق في جرائم الموبايل على استرجاع المعلومات المحذوفة من جميع أنواع أجهزة الموبايل المضبوطة في الجرائم أو الموجودة في مسرح الجريمة كأدلة مادية من دون التأثير على المعلومات ويتم إعداد التقارىر لاستخدامها في المجالات القانونية والتحقيق والاستخبارات وبرنامج إكس آكت الجدىد يساعد في التحقىق بشكل سريع وهو مفيد بدرجة كبيرة في العمل الجنائي لاستعادة بيانات الشريحة SIM والرسائل القصيرة المحذوفة التي تمت عن طريقها وذلك لتفرىغها بشكل فعال وسريع . كما تسمح برمجىات أكس آكت للخبراء في الأدلة الجنائىة بالمزىد من التعمق وذلك من خلال جمع البىانات من أجهزة الموبايل المغلقة.

يُمكن برنامج إكس آكت الجدىدالخبراء من:

1. تفريغ ذاكرة أجهزة الموبايل وبطاقات الذاكرة بشكل آمن.
2. فك الشفرة الآلي.

وبرامج إكس آكت تُعتبر حل كامل وتشتمل على الأجهزة، البرامج، والكابلات -كل الأدوات المطلوبة للحصول على المعلومات من الهواتف وبطاقات الذاكرة .ومن المزايا الرئيسية لبرامج إكس آكت قدرتها على الوصول إلى المحتوى المحمي والمحذوف والذي قد يشكل عنصراً حاسماً في تحقيقات الشرطة.

ليس البرامج مثل برامج اكس آكت: فإن التحليل الجنائي لجرائم الموبايل هو عبارة عن مضيعة للوقت ومحفوف بالمخاطرلأن اعتماد المسئولين عن إنفاذ القانون والخبراء على أدوات غير جنائية فنية لتفريغ وفك شفرة المعلومات يدوياً، وهي عملية قد تستغرق أياماً أو حتى أسابيع.

وتتضمن هذه الإجراءات مستوي عالي من المخاطر ينتج من تعريض جودة المعلومات ومن ثم اهتزاز موقفها القانوني في المحكمة واضعاف درجة الثقة أو الموثوقية في الدليل عن هذا الطريق. تعرِض الأساليب الحالية، في وقد تؤدي الطرق اليدوية إلي إفساد الهاتف وتدمير الأدلة في هذه العملية .- ولكن برنامجXACT الفعال الشامل الحلول لكل مشاكل الموبايل الجنائية - يوفر الحماية للبيانات التي يقوم الخبراء بتفريغها وفك شفرتها. ستدعم النسخة

الأولى من برامج إكس آكت بيانات هكس دمب Hex-dumps لأجهزة الموبايل المستخدمة بشكل شائع كما أنها ستدعم فك شفرة بعض منها، في حين تغطي النسخ التالية مزيد من منتجات أجهزة الموبايل.

المواصفات التكنولوجية:

1. في الذاكرة المادية Hex-dumps (ذاكرة بيانات هكس دمب): فهي تسمح بالوصول إلى المحتوى المحذوف والمحمي لجميع الأجهزة المتضمنة وتدعم الذاكرة الداخلية والوسائط القابلة للإزالة والقيم المشوشة لصورة الذاكرة.
2. فك شفرة الذاكرة الآلي لمحتويات الذاكرة: إعادة بناء هياكل البيانات المنطقية وإعادة بناء البيانات المحذوفة واحضار البيانات الأصلية وعرض البيانات في تطبيق تقليدي لبرامج إكس آر واي. ونظام فحص أجهزة الموبايل يشتمل على حقيبة انتقال مع برنامج استعادة معلومات المواد المحذوفة حيث يتم تحليل هذه المعلومات واستخدامها كأدلة جنائية.

أمثلة على المعلومات التي يمكن أن يقوم جهاز إكس آر واي بتنزيلها:

1. دليل الهاتف.
2. الأسماء.
3. الأرقام .
4. البريد الإلكتروني.
5. نصوص الرسائل التي المرسلة التي تم إرسالها أو التي لم ترسل أو التي تمت أرشفتها.
6. المكالمات - التي تم طلبها أو التي لم يتم الرد عليها أو التي تم استلامها.
7. الصور المستقبلة والصور المخزنة والصور التي تم التقاطها.
8. معلومات التقويم.
9. قائمة المهام.
10. الملفات السمعية.
11. التعرف الدولي على أجهزة الموبايل ونظام إدارة هذه الأجهزة.
12. التعرف تلقائيا على نوعية جهاز الموبايل الذي قمت بتوصيله بوحدة الاتصال.
13. ويشار الي انه تم تطوير هذا النظام بالتشاور مع سلطات والشرطة والمختبر القومي للعلوم الجنائى وبمعلومات مقدمة من الشرطة البريطانية.

التطبيق العملي للاتصال:

تتصل الوحدة بالحاسب الآلي عن طريق منفذ USB (يو اس بي) حيث يتم تصميم هذه الوحدة لتكون مرنة وقوية ومحمولة لتناسب كل من العمل الميداني والعمل المكتب.

وحدة يو إس بي:

تجعل من السهل التوصيل بكل أنواع أجهزة الموبايل ومع الجهاز جهاز إكس آر واي مع شاشة تطبيقية. ويمكن استخدام كوابل الشركة التي قامت بتصنيع االجهاز أو كوابل ميكرو مناسبة.

تقنية البلوتوث والأشعة فوق الحمراء:

البلوتوث الذي يعد خاصية في العديد من الموديلات الأكثر حداثة من أجهزة الموبايل ويتم توريد جهاز خاص للربط البيني مع تقنية البلوتوث وما زالت الأشعة فوق الحمراء شائعة جدا كخاصية لأجهزة الموبايل.وجهاز إكس آر واي يقوم بالربط البيني بين الإجهزة والأشعة فوق الحمراء.

تقرير كامل باللغة العربية:

يقوم جهاز إكس واي آر بإعداد تقرير بكل المعلومات التي تم تنزيلها . والتقرير جاهز أيضا للمعلومات الإدارية مثل الرقم الذي يشير الي الحالة واسم من قام بتشغيل الجهاز والمعلومات الأخرى المفيدة للتحقيق. ويقوم جهاز اكس واي آر تلقائيا بتدوين وقت وتاريخ القيام بالفحص.

والرسائل النصية:

يتم إعداد قائمة بعرض واضح:

1- لكل المكالمات الواردة والصادرة والمكالمات التي لم يتم الرد عليها المخزنة على الموبايل.
2- وتتضمن أيضا أي اسم مع رقم الهاتف.
3- وتتضمن كذلك الرسائل النصية التي تم قراءتها أو إرسالها أو التي لم ترسل أو التي تم أرشفتها.
4- ويتم تحديد المعلومات بموقع تخزينها على جهاز الموبايل - أو بطاقة التعريف الأمنية الخاصة به إس آي إم SIM.

بيانات الاتصال:

تتضمن القائم:

1. كل البيانات الخاصة بالاتصالات في جهاز الموبايل كالاسم ورقم الهـــاتف أو رقما أجهاز الموبايل.
2. ورسائل البريد الالكتروني الخ.
3. يتم تحدد كل هذه المعلومات السابقة في 1 ،2 بموقعها على جهاز الموبايل أو بطاقة التعريف الأمنية الخاصة به.

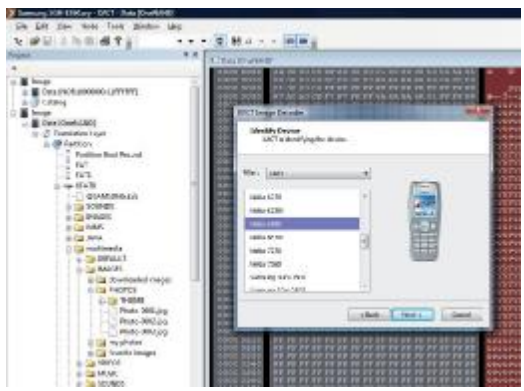
الصور والأصوات:

ويتضمن التقرير:

1. كل الصور المخزنة على جهاز الموبايل.
2. وتقدم خاصية المشاهدة المسبقة على الجهاز بتكبير الصور لإلقاء نظرة أولى عليها.
3. كل الملفات الصوتية والسمعية المخزنة على جهاز الموبايل ويمكن تشغيل هذه الملفات بشكل مباشر.

التطوير المستمر للنظام:

تقوم الشركة المصنعة للجهاز بتطويره بشكل مســـتمر ليواكـــب الخصـــائص الجديدة في أجهزة الموبايل والموديلات الجديدة من هذه الموبايلات في الســـوق التجاريوربطها بقاعدة البيانات الدولية.



الوصلات Cables التي اعدت لجميع أنواع الموبايلات لجميع الشركات المنتجة

رابعاً: الفحص اليدوي لجهاز الموبايل:

أ) للإستفادة منه في مسرح الجريمة.

ب) لمضاهاة الرسائل وتحليلها.

أ) للإستفادة منه في مسرح الجريمة:

يُستفاد من الموبايل في مسرح الجريمة في كثير من الجرائم: فقد يتم سرقته– حيث انتشرت سرقة الموبايل في السنوات الأخيرة في بريطانيا بشكل لافت للنظر[23]، وقد يُفقد ، وقد يوجد في مسرح الجريمة. فقد يحتاج البحث للإستعراف علي هوية الضحية من معلومات الهاتف المعثورعليه في مسرح الجريمة، وقد تُفيد معلوماته وتدل على كيفية ارتكاب الجريمة أو على الجاني أو الجناة أو على الشركاء ومسرح الجريمة قد يكون هو جيب الجانى.

ويمكن إتباع الخطوات السريعة ا في الفحص اليدوي للجهاز والتي تتضمن إيجاد الرقم المسلسل واسم الجهاز وآخر اتصال ورقم الشريحة أو الخط حسب ما يتوفر من إمكانات الجهاز أو شركة الاتصالات في كل بلد.

الفحص اليدوى للجهاز يتم من خلال كشف أسرار الجهاز التى قد تكون معروفة لنوع واحد من الأجهزة أو حسب شركة الاتصال الخاصة التابع لها شريحة الجهاز.

من المعلومات اليدوية السريعة للبحث عن هوية صاحب الجهاز مايلى:

الحصول على الرقم المسلسل للجهاز وهو الذى سبق الحديث عنه والمعروف بـ IMEI ويتم إيجاده بطريقتين:

- قراءته على الملصق الداخلى ببطن الجهاز أعلى أو أسفل العلامة C€0168 أو C€0434 او أي رقم آخروذلك إذا كان هناك مشكلة في الشريحة أو في الاتصال أو التشفير.
- الضغط على نجمة ثم مربع (شباك) ثم صفر ثم رقم 6 ثم مربع (شباك) فقط فيظهر الرقم بطريقة سريعة على شاشة العرض[28].
- ويمكن كتابته باللغة الانجليزية كالآتي:

(*#06#) أو (star hash zero six hash).

وهذا الرقم يمكن للشخص العادى تسجيله بعيداً عن الجهاز بالطبع للإبلاغ عنه عند الفقد فيمكن للشركة إبطال خاصيته فلا يستفاد منه وتصبح السرقة عديمة الفائدة وتقل حوادثها. وعن طريقه يمكن متابعة السارق بالأقمار الصناعية والقبض عليه.

- خاصية لشركة فوادفون في مصر فإن الحصول على رقم الخط بشريحة الجهاز يكون بالضغط على نجمة ثمانية سبعة ثمانية مربع (شباك) ثم ضغط اتصال ويمكن كتابته باللغة الانجليزية كالآتي:

(*878#) أو (star eight seven eight hash)

ثم الضغط على اتصال.

وكذلك للحصول على آخر رقم اتصل بالجهاز حتي ولو كان الجهاز مغلقاً فإنه يكون بالضغط على نجمة واحد خمسة صفر شباك تم اتصال ويظهر معها وقت الاتصال وتاريخه.

ويكون باللغة الإنجليزية كالآتي:

(#150*) أو (star one five zero hash). ثم الضغط على اتصال.

- للحصول على بيانات خاصة بصنع الجهاز وتاريخ الصنع واسم الجهاز ورقمه فانه يمكن الضغط على الأزرار(#0000#*) دون الضغط على رز اتصال.
- للحصول على معلومات الجهاز من رقم مسلسل والعمليات التى تمت به يمكن الضغط على #92702689#* مباشرة تظهر هذه المعلومات على الشاشة[28].

ب) لمضاهاة الرسائل وتحليلها:

الطرق ارسال الرسائل القصيرة ترسل الرسائل القصيرة بثلاث طرق هي:

1- من جهاز إلي جهاز
2- من الموقع الي جهاز
3- من ايميل الي إيميل الشبكة

يمكن مضاهاة رسائل الموبايل للتعرف على:

1. شخص كاتب الرسالة من خلال اسلوبه:
2. من التهميز
3. وضع النقاط أو اهمالها.
   - الاسلوب الذي يبدا به الرسالة.
   - الاسلوب الذي تنتهي به الرسالة.
   - الحالة النفسية للكاتب
   - دلالة الكلمات التي كتبها.
4. جنسية الكاتب.

قام عدد من الباحثين النفسيين في محاولة التعرف على مرسل رسائل من خلال استخدام الاختصارات من الموبايل لمعاونة البوليس ما اذا كان شخصاً معيناً ارسل الرسالة من خلال دراسة رسائل عديدة بلغت اكثر من 1500 رسالة[36].