

SECURINETS



Club de la sécurité informatique
INSAT

Dans le cadre de

SECURIDAY 2010

Et sous le thème de

Computer Forensics Investigation



VOUS PRÉSENTE L'ATELIER :

Equipement Mobile

Chef Atelier : Nadia Jouini (RT4)

- Aymen Frikha (RT3)
- Jguirim Hajer (RT5)
- Dahi nouha (RT5)

SECURINETS



Club de la sécurité informatique
INSAT

Presentation de l'atelier :

Au cours de cet atelier on va traiter le thème « computer forensics et investigation » coté équipement mobile.

Donc on va récupérer les données, analyser les équipements mobiles du victime tels que l'ipod et Smartphone, analyser la carte SIM, le carnet d'adresse, les photos, les mails, à fin de voir tout indice ayant un lien avec la crime.

I. Les équipements Mobiles :

✓ **Installation, Configuration lancement des logiciels utilisés :**

• **Collecte d'information en utilisant MOBILEEDIT**

MOBILEEDIT est un logiciel qui permet de contrôler le téléphone à partir de votre PC. Il permet aussi la création et la sauvegarde de texte et de numéro, l'envoi de SMS ou des MMS, la sauvegarde de toutes vos données.

Fonctionnalités:

- Analysez les téléphones via Bluetooth, IrDA ou câble de connexion
- Analysez l'annuaire téléphonique, les derniers numéros, appels manqués, la réception d'appels, des SMS, des messages multimédia, des photos, des fichiers, le numéro de téléphone, agenda, notes, tâches et plus
- Direct SIM analyseur par les lecteurs SIM
- Lire les messages supprimés de la carte SIM
- Produire et imprimer des rapports prêts à l'audience
- Assurer la sécurité et infalsifiable l'aide de hachage MD5 des données récupérées.
- etc

SECURINETS



Club de la sécurité informatique
INSAT

- **Collecte d'information a partir d'une carte Sim en utilisant GSM SIM UTILITY**

Le **SIM GSM** est un package, qui permet aux utilisateurs de sauvegarder leurs données SIM sur leur PC.

La sauvegarde des données est cryptée par un algorithme DES (Data Encryption Standard).

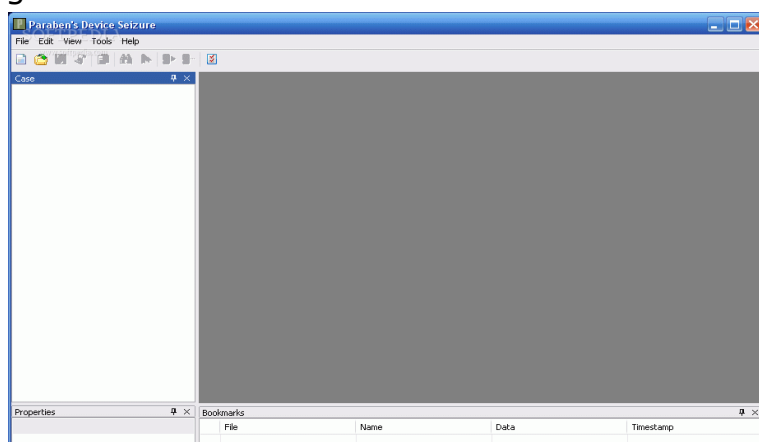
Le crackage est proche de 100% pour l'algorithme COMP128 V1 et plus rapide que tout autre produit actuellement sur le marché.

- **Installation de Device Seizure :**

Avec Windows Mobile vous aurez besoin de charger le gestionnaire pour appareil Windows Mobile pour acquérir l'appareil. Avant de commencer l'acquisition, Assurez-vous que l'appareil est sous tension et correctement connecté à votre système d'acquisition



Puis on va utiliser le logiciel **device seizure** :



SECURINETS

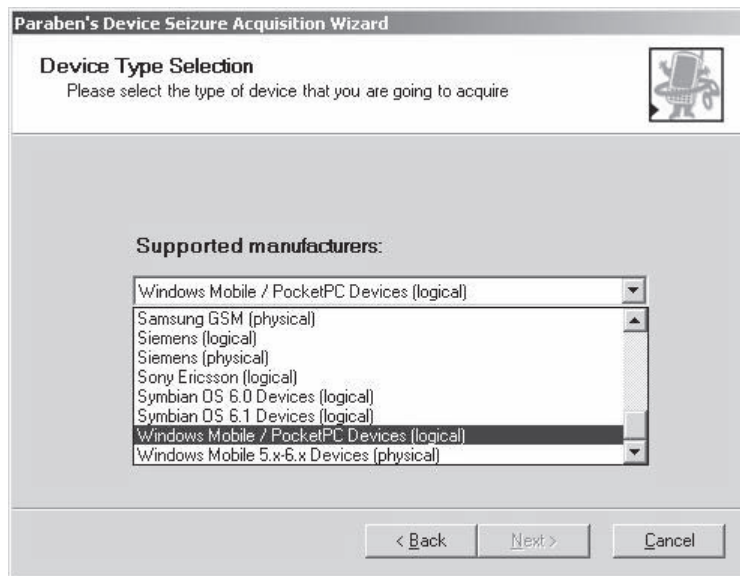


Club de la sécurité informatique
INSAT

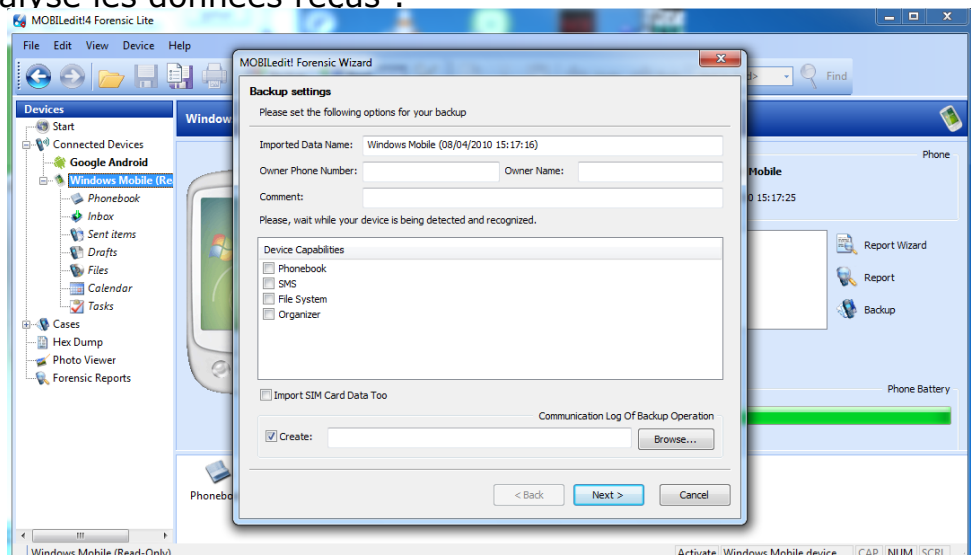
L'assistant de device seizure vous guide durant tout le processus :



Dans la liste déroulante liste de sélection, sélectionnez le modèle et le type de l'appareil mobile. Cliquez ensuite sur l'acquisition, physique ou logique, puis cliquez sur Suivant.



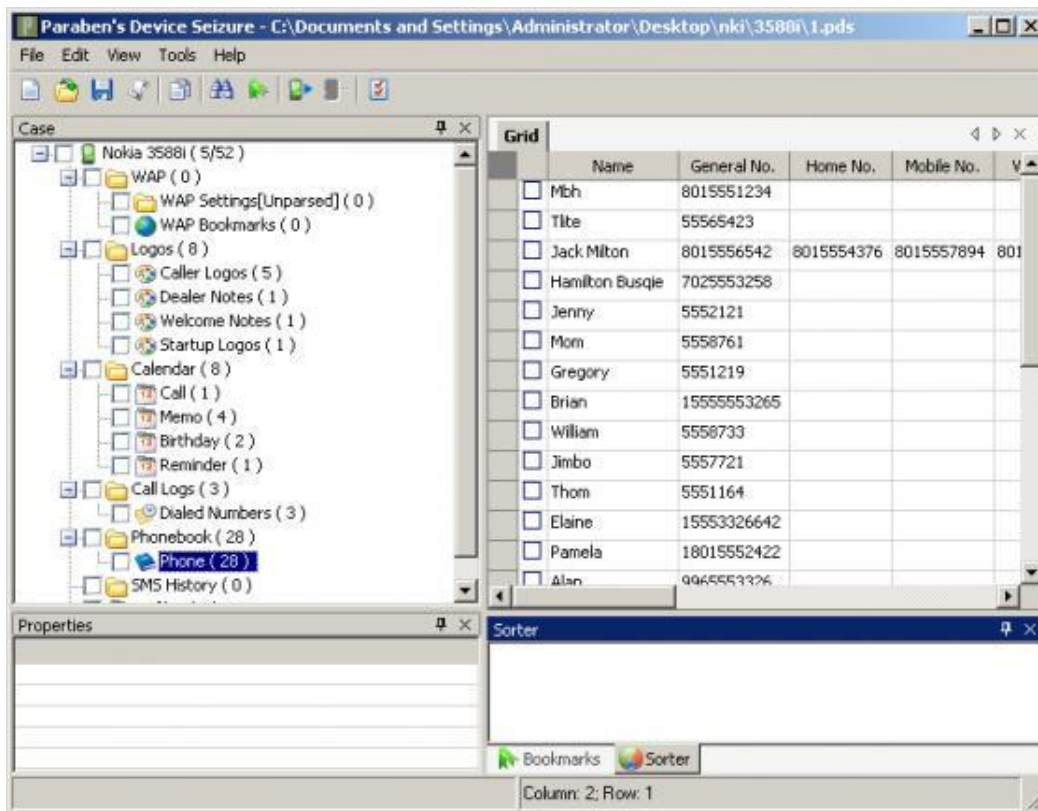
Maintenant on analyse les données recus :



SECURINETS



Club de la sécurité informatique
INSAT



- **Utilisation de Mobicedit :**

Pour utiliser ce logiciel, il faut utiliser le logiciel de synchronisation pour les téléphones dotés de Windows mobile

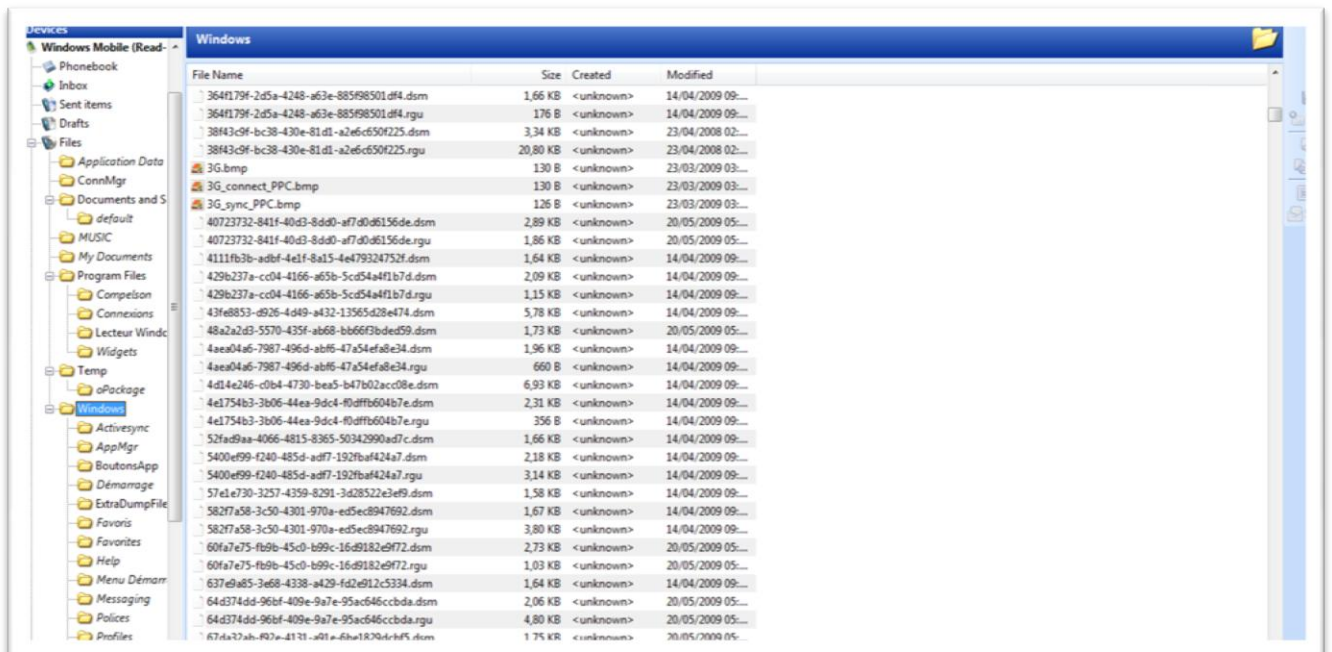
Puis à l'aide de **Mobicedit** on peut extraire les données du notre équipement mobile :

- Et après on analyse les données

SECURINETS



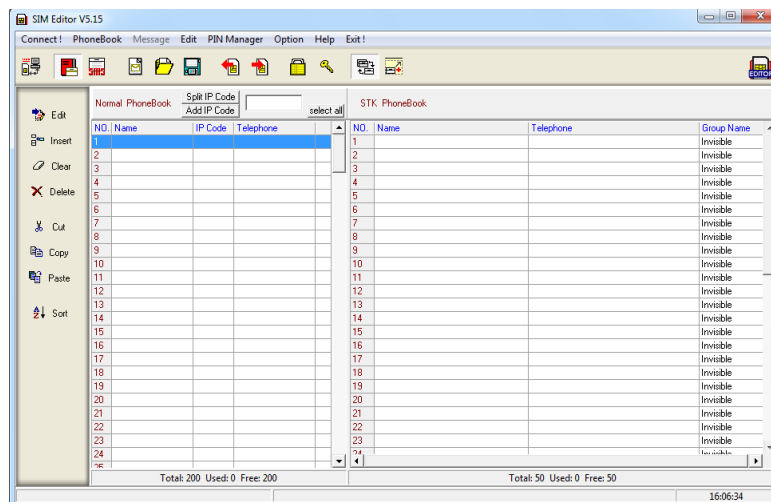
Club de la sécurité informatique
INSAT



Utilisation de GSM SIM Utility

Avant tout on doit avoir un lecteur carte sim qu'on doit le connecter au pc et installer son driver

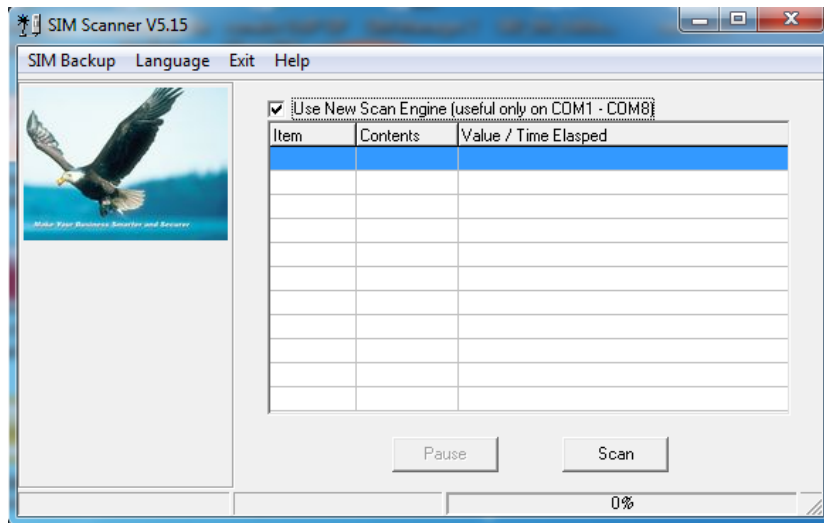
Puis on commence l'acquisition des données.



SECURINETS



Club de la sécurité informatique
INSAT



✓ Environnement logiciel

1- Gsm Sim Utility

http://download.cnet.com/GSM-SIM-Utility/3000-18508_4-10396246.html

2- Mobiledit

<http://www.softpedia.com/get/Internet/Telephony-SMS-GSM/MOBILedit-Forensic.shtml>

3- Device seizure

<http://www.clubic.com/telecharger-fiche181742-device-seizure.html>

SECURINETS



Club de la sécurité informatique
INSAT

II. L'équipement Smartphone :

Durant cette partie, on a utilisé l'émulateur **Smartphone Android :**

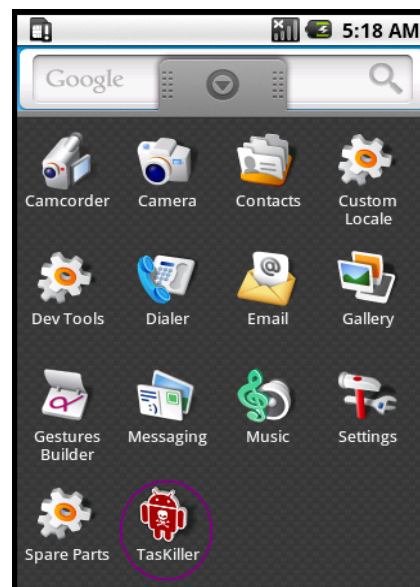


• L'étape de collecte et acquisition des données :

Installation de Taskiller :

Taskiller est un gestionnaire de tâches pour les Smartphones. Il permet d'afficher tous les processus lancés sur votre équipement .Il permet aussi de tuer les processus et les applications sélectionnées avec la possibilité d'« **autoKill** », c'est-à-dire de tuer automatiquement les taches au démarrage de votre équipement .

En l'installant sur l'**Emulateur Android**, **Taskiller** nous affiche les différentes versions disponibles (2.7, 2.6.2) et les caractéristiques de chacune.

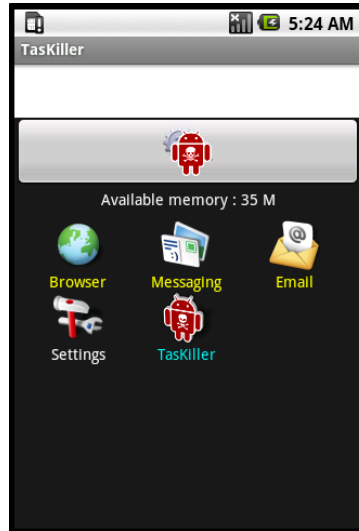


SECURINETS

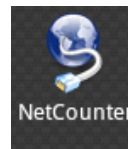


Club de la sécurité informatique
INSAT

Voilà une imprime écran de l'exécution de **Taskiller**, qui affiche bien les taches et les applications lancés sur le **Smartphone**.



- ⇒ Cette application est utile durant **la phase d'acquisitions des données**. Elle nous permet de voir tous les processus en cours d'exécution sur notre équipement, donc de découvrir les applications malveillantes qui sont en cours d'exécution sur notre équipement.

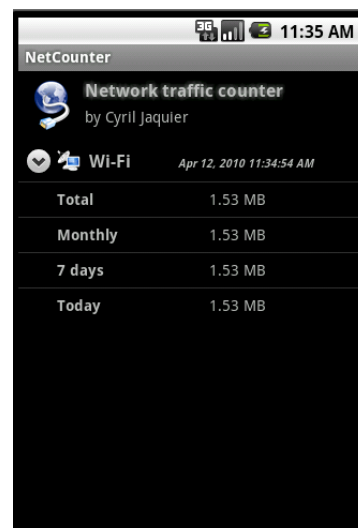
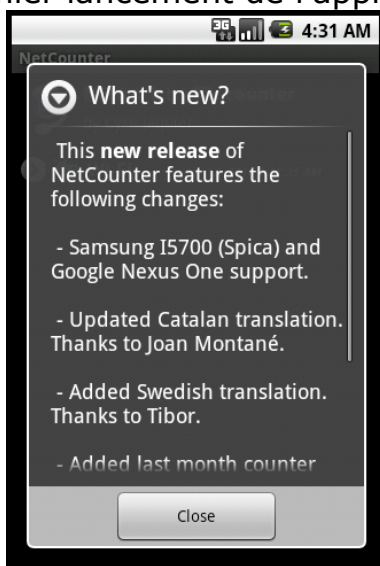


Installation de NetCounter:

NetCounter est un compteur de trafic réseau, trafic **3G ou wifi**. Il montre votre utilisation de données. Vous pouvez définir des compteurs (mensuel, les 7 derniers jours, aujourd'hui etc ..)

Donc il permet de surveiller le trafic réseaux envoyé et reçu par votre Smartphone

Au premier lancement de l'application on a cette fenêtre :

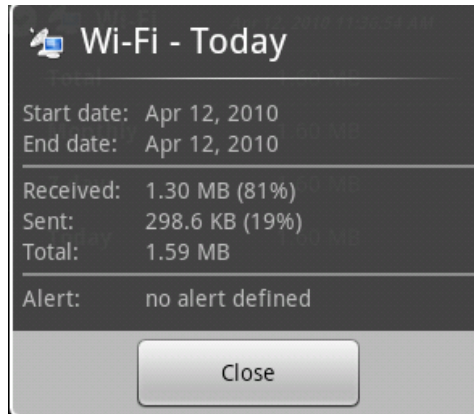


SECURINETS



Club de la sécurité informatique
INSAT

Par exemple on peut choisir de voir la quantité de trafic échangé aux cours de cette journée on trouve :



- ✓ Supposant le cas où on n'a pas utilisé le Wi-Fi et le 3G durant la journée, et j'ai trouvé que 80 % des trafics sont envoyés par mon **iPhone**. Je peux conclure de ce que mon Smartphone est endommagé, et qu'il y a un code malicieux entraînant de s'exécuter et entraînant d'envoyer des données au pirate => c'est pourquoi cette application est trop utile.

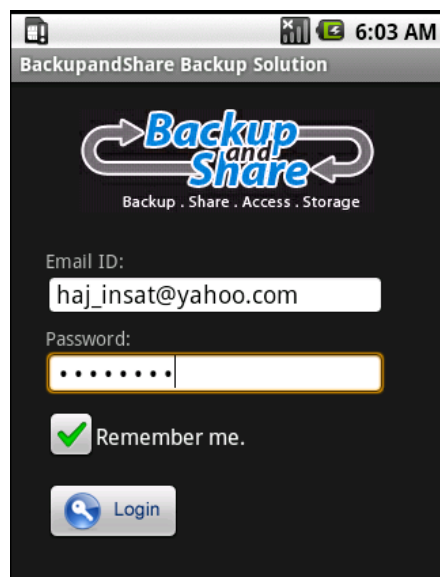
• L'étape de Récupération des données (Recovery):

Pour se faire, on a installé l'application **BackupandShare**, qui permet de récupérer et restaurer tous les contacts, fichiers musicaux, photos et vidéos sauvegardés sur votre téléphone. Il permet aussi la restauration des données sur votre iPhone, avec un simple click

Après l'installation de cette application on trouve cette icône dans le menu :



Le lancement de l'application :



SECURINETS



Club de la sécurité informatique
INSAT

• L'étape d'analyse des données :

Installation d'antivirus :

Cette application permet de protéger votre **Smartphone**

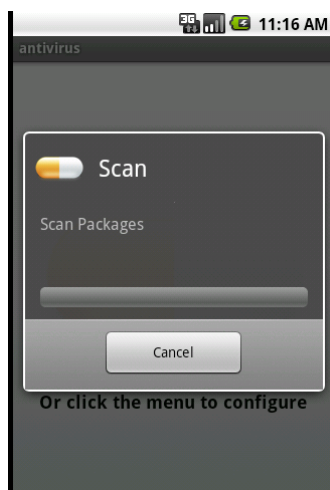
Contre les virus, les logiciels malveillants et les exploits,
avec un analyse en temps réel.

Elle permet aussi d'analyser tous les données sur votre
Equipements (videos, sms) et les contacts et données
sur votre carte SIM .

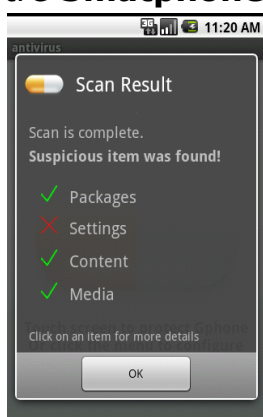
En plus vous pouvez filtrer les messages et les SMS
pour ne pas recevoir des Spam messages.



On lance l'analyse:



Après l'analyse, cette application nous affiche les éléments et les fichiers suspects, se trouvant dans notre **Smatphone** ou dans notre carte SIM



SECURINETS



Club de la sécurité informatique
INSAT

• Simulations :

Pour bien comprendre l'utilité de chaque application et chaque étape de forensics .On va programmer le virus « **Duh** » et on va le lancer sur notre Smartphone et puis on va essayer de suivre les traces de ce virus pour conclure en fin son existence sur l'équipement.

Le virus Duh :

C'est un virus ciblant les **Smartphones** et les **iPods**.

Il recherche les informations bancaires et les envoie sur un serveur en Lituanie.

Ce virus transforme le **Smartphones** en un automate, qui transfère toutes les données sensibles présentes sur le **Smartphone** vers les serveurs de pirates.



Simulation de ce virus :

On a simulé le fonctionnement de ce virus, en créant un processus

qui envoie périodiquement des données au serveur de pirate .Pour se faire on utilise eclipse (java)

```
Java - Virus Duh/src/attaque/virus/Main.java - Eclipse
File Edit Run Source Refactor Navigate Search Project Window Help
Package Explorer Hierarchy
bonjourAndroid
HelloAndroid
Virus Duh
  src
    attaque.virus
      Main.java
  gen [Generated Java Files]
  Android 2.1
  assets
  res
  AndroidManifest.xml
  default.properties
HelloAndroid.java Main.java
package attaque.virus;
import android.app.Activity;
public class Main extends Activity {
    /** Called when the activity is first created. */
    @Override
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.main);
    }
}
Problems Javadoc Declaration Console
Android
[2010-04-12 12:56:28 - HelloAndroid] Device API version is 7 (Android
[2010-04-12 12:56:28 - HelloAndroid] HOME is up on device 'emulator-
[2010-04-12 12:56:28 - HelloAndroid] Uploading HelloAndroid.apk onto
[2010-04-12 12:56:46 - HelloAndroid] Installing HelloAndroid.apk...
[2010-04-12 12:57:06 - HelloAndroid] Success!
[2010-04-12 12:57:08 - HelloAndroid] Starting activity Securinets.At
[2010-04-12 12:57:13 - HelloAndroid] ActivityManager: Starting: Inte
[2010-04-12 13:58:42 - Virus Duh] -----
[2010-04-12 13:58:42 - Virus Duh] Android Launch!
[2010-04-12 13:58:42 - Virus Duh] adb is running normally.
[2010-04-12 13:58:42 - Virus Duh] Performing attaque.virus.Main acti
[2010-04-12 13:58:42 - Virus Duh] Automatic Target Mode: using exist
```

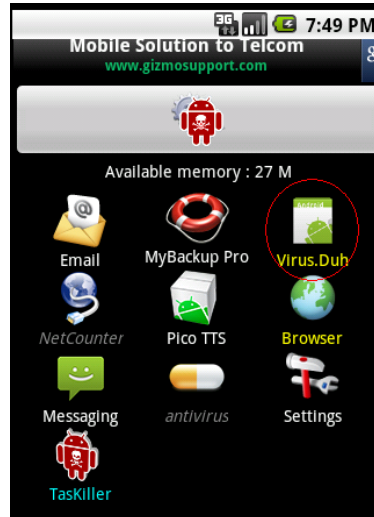
SECURINETS



Club de la sécurité informatique
INSAT

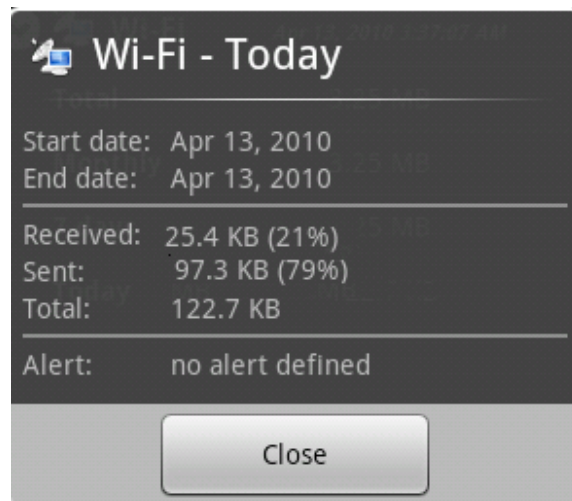
Détection avec Taskiller :

En lançant **Taskiller**, qui affiche la liste des processus en cours d'exécution, on trouve :



- ⇒ On remarque bien qu'il ya processus inconnus en cour d'exécution.
- ⇒ C'est un processus malveillant

Lancement de NetCounter :



On remarque bien qu'il ya 97,3 KB, presque 80 % des données sont envoyées par le **Smartphone**. Supposant les cas ou on n'a pas utilisé la connexion wifi et 3G de notre équipement durant la journée.

SECURINETS

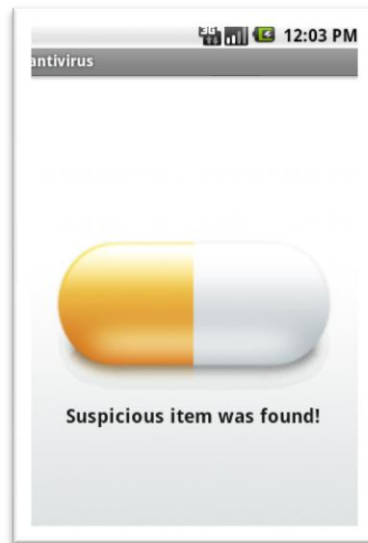


Club de la sécurité informatique
INSAT

- ⇒ On peut conclure facilement qu'il ya un programme malveillant, qui est entrain d'utiliser les connexions réseaux pour envoyer les données au pirate.

Détection avec l'antivirus :

On lance l'antivirus pour analyser les données sur notre équipement. On remarque bien détection d'une application malveillante.



Conclusion :

Les équipements mobiles deviennent de jour en jour un besoin vitale. Et chaque jour apparaissent des équipements de plus en plus développés (Smartphone, iPad) qui peuvent même remplacé l'ordinateur dans certaine fonctionnalités. En observant les employés d'une société on remarque bien que tous les employés ont des équipements mobile.ils peuvent à tous moments connecter leur équipements au réseau de l'entreprise, c'est qui représente bien un grand risque.

C'est pourquoi on doit faire attention à la coté sécurité des **Smartphones** et des équipements mobile. On doit faire attention et on doit s'intéresser à tout indice pouvant prouver l'existence d'un code malveillant. Par exemple la décharge rapide de la batterie, qui peut être due à l'importance des échanges de données, et peut être explique par la présence d'un code malveillant, un processus qui est entrain d'envoyer des données au pirates.

SECURINETS



Club de la sécurité informatique
INSAT