Window Mobile Forensics

Guida pratica per acquisizione ed analisi dei device windows mobile.

Autore	Data	Versione
Evgueni Tchijevski	04-08-2009	0.2

1. Indice

2. Introduzione

Quasi sicuramente un analista forense, una volta nella vita si sarà trovato di fronte all'analisi di un cellulare.
Ad oggi l'argomento mobile forensic non è diffuso quanto l'analisi forense classica, e quindi si fanno fatica a trovare informazioni metodologie e procedure per eseguire una analisi completa su di un telefono. In oltre gli strumenti per questo tipo di analisi spesso sono closed source e dal valore di qualche k euro.
Quello che andrò a presentare è la mia esperienza sull'acquisizione ed analisi dei telefoni Windows Mobile.
Come prima cosa, vi anticipo che l'acquisizione è stata fatta dumpando la memoria interna del telefono, quindi non i soliti tool che recuperano i file logici recuperabili con tool di gestione del telefonino.
Il dump della memoria è stato eseguito con una suite di strumenti (XDA Utils) opensource sviluppata da dei volenterosi ragazzi, allo scopo di poter cambiare le ROM del proprio telefono. Gli strumenti vanno benissimo però anche per scopi che a noi interessando di più.
Ad oggi non esiste una soluzione che non comporti una alterazione al telefono (che sia sw o hw), la procedura descritta in questo documento purtroppo non è esente da questo problema. Infatti l'accesso diretto alla memoria richiede l'installazione di una dll all'interno del telefono.

3. Requisiti

- ActiveSync (da usare con Windows XP)
  http://www.microsoft.com/downloads/details.aspx?displaylang=it&FamilyID=9E641C34-6F7F-404D-A04B-DC09F8141141
- Windows mobile device Center (da usare con Windows Vista)
  http://www.microsoft.com/downloads/details.aspx?FamilyId=46F72DF1-E46A-4A5F-A791-09F07AAA1914&displaylang=it
- Virtual PC
  http://www.microsoft.com/downloads/details.aspx?displaylang=it&FamilyID=04d26402-3199-48a3-afa2-2dc0b40a73b6

Dipendentemente da quello che volete emulare:

- Windows Mobile 5
  http://www.microsoft.com/downloads/details.aspx?FamilyID=c62d54a5-183a-4a1e-a7e2-cc500ed1f19a&DisplayLang=en
- Windows mobile 6
  http://www.microsoft.com/downloads/details.aspx?FamilyID=38c46aa8-1dd7-426f-a913-4f370a65a582&DisplayLang=en
- Windows Mobile 6.1
  http://www.microsoft.com/downloads/details.aspx?familyid=1A7A6B52-F89E-4354-84CE-5D19C204498A&displaylang=en
- Windows Mobile 6.5
  http://www.microsoft.com/downloads/details.aspx?FamilyID=20686a1d-97a8-4f80-bc6a-ae010e085a6e&displayLang=en#Instructions

I tool di emulazione non sono strettamente necessari, ma in fase di analisi possono dare una mano.

Infine i tools di acquisizione e analisi.

- XDA Utils (http://nah6.com/~itsme/itsutilsbin-20090515.zip) per info:
  http://www.xs4all.nl/~itsme/projects/xda/tools.html
- DBExplorer (costo 19,95$) - http://www.phatware.com/index.php?q=product/details/dbexplorer

Analisi registro WindowsMobile.

- MakeHV (http://forum.xda-developers.com/showpost.php?p=898198&postcount=229)

4. Acquisizione

Il telefono va collegato al pc tramite cavo USB e richiede la sincronizzazione attraverso ActiveSync.
Dopo aver scompattato l'archivio delle XDA Utils si esegue il seguente comando:

```
C:\Users\install\Desktop\Log1\windump>pdocread.exe -l
Copying C:\Users\install\Desktop\Log1\windump\itsutils.dll to WCE:\windows\itsutils.dll
 61.40M (0x3d66800) DSK2:
|           2.62M (0x29fc00) Part00
|           2.75M (0x2c0000) Part01
|          56.00M (0x3800000) Part02
|           2.00T (0x1ffff986800)
 55.13M (0x3720000) DSK3:
|          55.12M (0x371fc00) Part00
STRG handles:
handle#0 476cb89a  55.12M (0x371fc00)
handle#1 4769f35e   2.00T (0x1ffff986800)
handle#2 4769f3c2  56.00M (0x3800000)
handle#3 876cb82e   2.75M (0x2c0000)
handle#4 276cb876   2.62M (0x29fc00)
disk 476cb89a
0 partitions, 0 binary partitions
customerid=00000000 uniqueid= 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 disk 4769f35e
0 partitions, 0 binary partitions
customerid=00000000 uniqueid= 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 disk 4769f3c2
0 partitions, 0 binary partitions
customerid=00000000 uniqueid= 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 disk 876cb82e
0 partitions, 0 binary partitions
customerid=00000000 uniqueid= 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 disk 276cb876
0 partitions, 0 binary partitions
customerid=00000000 uniqueid= 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

come si vede, viene caricato nella directory \Windows del telefono il file itsutils.dll:
Copying C:\Users\install\Desktop\Log1\windump\itsutils.dll to WCE:\windows\itsutils.dll
Quello che si vede dall'output del comando è la struttura delle memoria del telefono, i dati che ci interessano sono:

```
handle#0 476cb89a  55.12M (0x371fc00)
handle#1 4769f35e   2.00T (0x1ffff986800)
handle#2 4769f3c2  56.00M (0x3800000)
handle#3 876cb82e   2.75M (0x2c0000)
handle#4 276cb876   2.62M (0x29fc00)
```

queste sono le varie "partizioni" del telefono. Nel mio caso la prima (handle#0) contiene il firmware del telefono la ROM, e la terza (handle#2) la memoria utilizzata dal telefono per le applicazioni e storage dei dati (quella che ci interessa).
Notare tra parentesi e la dimensione della partizione in formato esadecimale.

Prossimo passo è il check sulla dimensione della partizione:

```
C:\Users\install\Desktop\Log1\windump>pdocread.exe -w -h #2 -t

real nr of sectors: 114688  -  56.00Mbyte, 0x3800000
```

le opzioni del comando:

-w	legge il contenuto del disco attraverso le api di windows (necessario con i telefoni nuovi)
-h	specifica il numero della partizione (in questo caso handle#2)
-t	stampa in output la dimensione della partizione

Il prossimo comando serve per eseguire il dump vero e proprio della memoria:

```
C:\Users\install\Desktop\Log1\windump>pdocread.exe -w -h #2 0x0 0x3800000 dump_2.raw

CopyTFFSToFile(0x0, 0x3800000, dump_2.raw)
```

le opzioni del comando:

-w	legge il contenuto del disco attraverso le api di windows (necessario con i telefoni nuovi)
-h	specifica il numero della partizione (in questo caso handle#2)
0x0 – 0x38000000	rispettivamente offset e lunghezza della partizione
dump_2.raw	nome file dell'immagine

A questo punto ci troviamo una bella immagine raw del cellulare, analizzabile con qualsiasi tool di analisi forense.

5. Analisi

Utilizziamo i tool forniti da sleuthkit per analizzare l'immagine.
Ad esempio scopriamo con il comando fsstat che la partizione che abbiamo in precedenza acquisito è FAT32.

```
soundwave@mrblack:~/lavoro/forense$ fsstat dump_2.raw
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: FAT32

OEM Name: MSWIN4.1
Volume ID: 0x7e80002
Volume Label (Boot Sector):
Volume Label (Root Directory): TFAT
File System Type Label: TFAT32
Next Free Sector (FS Info): 268437249
Free Sector Count (FS Info): 4294967295

Sectors before file system: 0

File System Layout (in sectors)
Total Range: 0 - 112893
* Reserved: 0 - 31
** Boot Sector: 0
** FS Info Sector: 1
** Backup Boot Sector: 0
* FAT 0: 32 - 913
* FAT 1: 914 - 1795
* Data Area: 1796 - 112893
** Cluster Area: 1796 - 112893
*** Root Directory: 1796 - 26096

METADATA INFORMATION
--------------------------------------------
Range: 2 - 1777570
Root Directory: 2

CONTENT INFORMATION
--------------------------------------------
Sector Size: 512
Cluster Size: 512
Total Cluster Range: 2 - 111099
…[snip]…
```

A questo punto l'indagine prosegue come per un normale hard-disk,
ad esempio andiamo ad elencare i file che sono stati cancellati.

```
soundwave@mrblack:~/lavoro/forense$ fls -d -r -p  cell_dump1.raw
r/r * 535462:   Windows/System/ConfigMgr/ConfigManagerTransactionRollback.xml
r/r * 535465:   Windows/System/ConfigMgr/FileOperation.rbk
r/r * 535467:   Windows/System/ConfigMgr/67C9154F-E516
r/r * 535470:   Windows/System/ConfigMgr/FileOperation.rbk
r/r * 388944:   Windows/System/ConfigMgrCertEnroll.rbk
r/r * 250820:   Windows/StartUp/coldinit.lnk
r/r * 250822:   Windows/StartUp/welcome.lnk
r/r * 250826:   Windows/StartUp/HP iPAQ QuickStart Tour.lnk
r/r * 541827:   Windows/Profiles/guest/Temporary Internet Files/Content.IE5/01234567/_TP-JS~1.HTM
r/r * 96209:    Windows/Profiles/guest/Temporary Internet Files/Content.IE5/3HCNMJ6P/_APS~1.GOO
r/r * 477375:   Windows/Profiles/guest/Cookies/guest@mail[1].txt
....[snip].....
```

Oppure usare il framework di analisi preferito (vedi sotto Autopsy).

Purtroppo la memoria del telefono è quella che è, la probabilità che venga trovato qualcosa di cancellato ed integro è molto bassa.
Nel mio caso sono riuscito a trovare alcune immagini (carving) e sms cancellati (ricerca di stringhe).

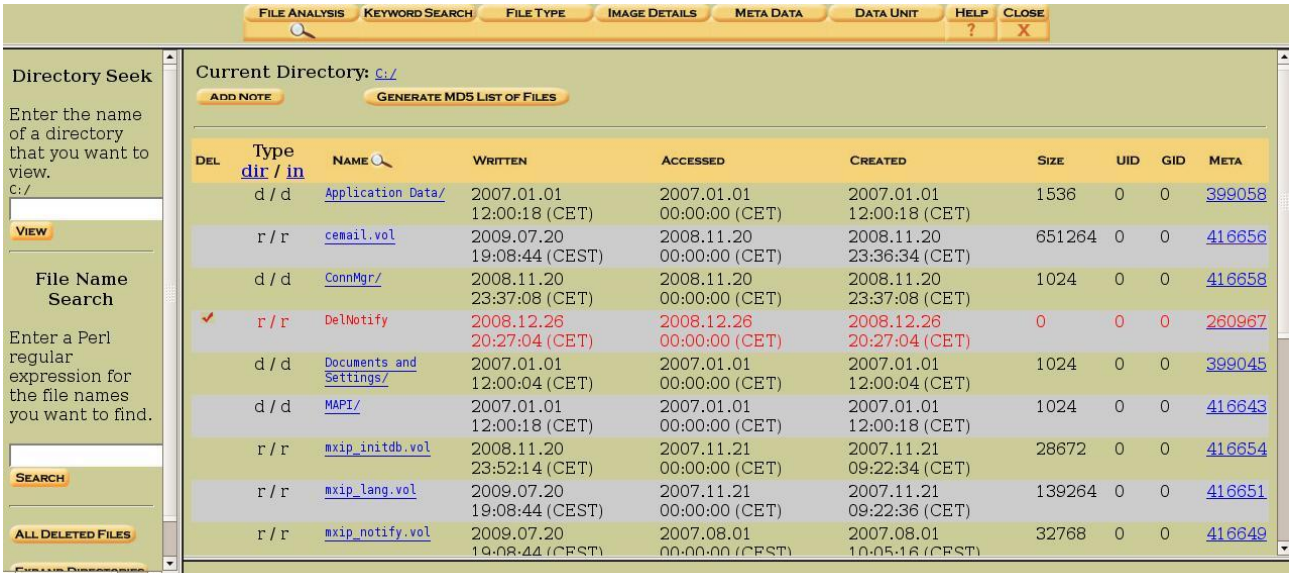

Figura 1 – Analisi in Autopsy

SMS

Una delle cose più importanti da analizzare all'interno di un telefono, ovviamente sono i text messages (SMS, MMS ed e-mail). Windows Mobile memorizza gli SMS inviati, ricevuti, cancellati (cestino) all'interno di un database interno. Struttura e dati del database sono contenuti all'interno di un file memorizzato nella root del filesystem. Il file si chiama **cemail.vol,** ed è in formato CEDB (proprietario Microsoft). Per poter leggere questo database è necessaria l'applicazione DBExplorer.

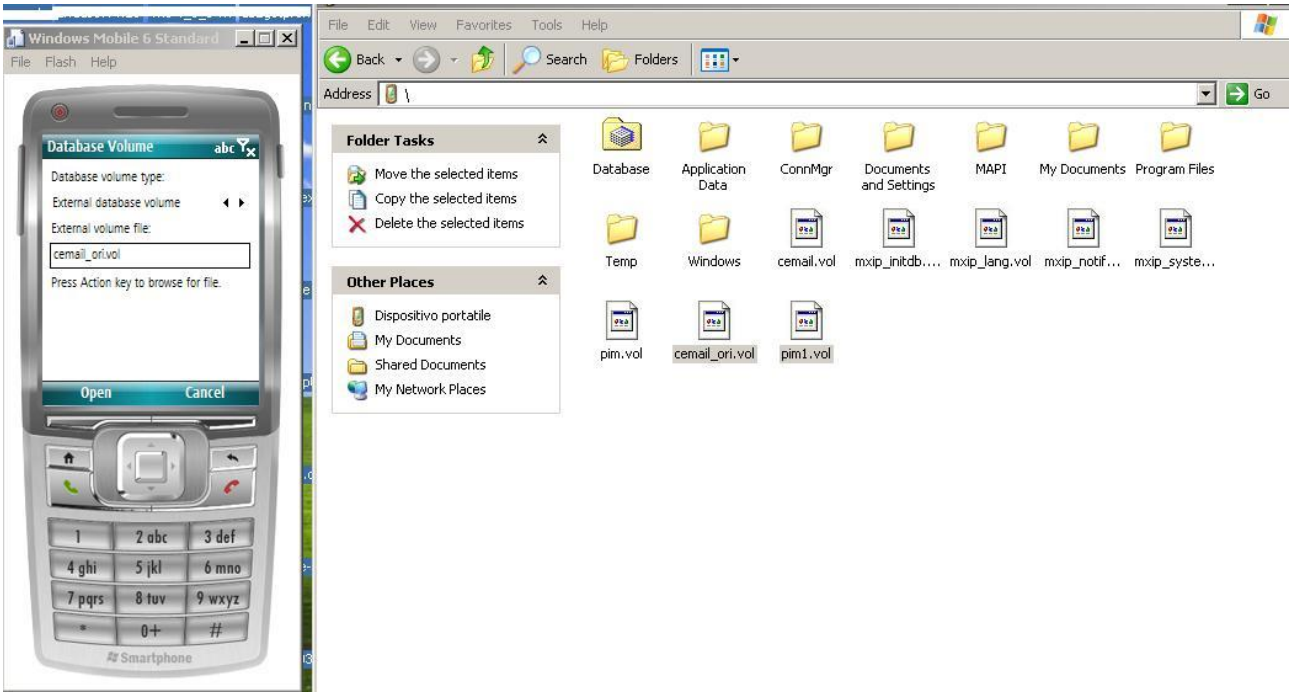

Figura 2 - Emulazione Windows Mobile per estrazione DB

A questo punto entra in gioco l'emulatore di windows mobile (di solito destinato agli sviluppatori). L'emulatore ci permette di eseguire operazioni sui file del telefono analizzato senza dover utilizzare il telefono. L'installazione di tutto l'ambiente virtuale richiede pochi minuti (http://www.megalab.it/2776/).

Ultimata l'installazione dell'emulatore, si può procedere con l'installazione dell'applicazione DBExplorer e con l'analisi dei file esportati. Una volta sincronizzato il telefono con ActiveSync, si va a caricare il file cemail.vol all'interno del telefono emulato. Purtroppo non è possibile copiare semplicemente il file, sostituendo il file già presente. Però è possibile rinominare il file da analizzare con altro nome. Nel caso in esame il file è stato chiamato "cemail_ori.vol" e poi semplicemente copiato all'interno della root del telefono.
Per fare l'estrazione dei messaggi si può procedere in due modi:

- Aprire il file cemail_ori.vol direttamente dal programma DBExplorer e fare l'esportazione in formato CSV.
- Aprire il file cemail_ori.vol con DBExplorer ed eseguire le estrazioni con la suite XDA Utils.

Di seguito i comandi per l'estrazione dei messaggi.
Dump dei vari database caricati in memoria con le relative tabelle.

```
C:\Documents and Settings\Administrator\Desktop\itsutilsbin-20090515>pdblist.exe -D
volume {00000000-0000-0000-0000-000000000000} \Documents and Settings\default.vol
volume {46b88b00-2fb6-5a7f-a5e3-0ff71d0c22a3} \ReplStorVol
oid30000001: dbase F00010017 T00000000  113  10780 ... 'ReplStor'
   ORDERING: 00650013:00000001
volume {fb012800-e760-e396-12e8-11da0bee51ed} \mxip_notify.vol
oid3100000e: dbase F00000017 T00000000    4    860 ... 'DB_notify_queue'
   ORDERING: 00010040:00000000
oid30000001: dbase F00020017 T00000000    9    960 ... 'DB_notify_events'
   ORDERING: 0001001f:00000000
volume {7bb3d500-eb62-1fa7-b947-42ebb1fe2536} \mxip_lang.vol
oid300001ac: dbase F00020017 T00000000  105  19708 ... '\MetabaseOptions'
   ORDERING: 00000013:00000000
oid30000046: dbase F00020017 T00000000  366  30132 ... '\MetabaseLabels'
   ORDERING: 00000013:00000000
oid30000001: dbase F00020017 T00000000   67   4376 ... '\FileNameLang'
   ORDERING: 0001001f:00000002
volume {9ca9a900-ecea-16bd-bd6e-7ae850801dab} \cemail.vol
oid33000029: dbase F00000017 T00000000    0    356 ... 'pmailVolumes'
oid3b000017: dbase F00000017 T00000000    1    412 ... 'pmailNamedProps'
   ORDERING: 8300001f:00000000 83010013:00000000
oid30000009: dbase F00000017 T00000000   11    964 ... 'pmailMsgClasses'
   ORDERING: 8300001f:00000000 83010013:00000000
oid30000007: dbase F00000017 T00000000    0    356 ... 'pmailOldTables'
oid30000003: dbase F00000017 T00000000    0    356 ... 'pmailMsgs'
   ORDERING: 800c001f:00000000 0e090013:00000000 00150040:00000000
oid30000001: dbase F00000017 T00000000   14   1732 ... 'pmailFolders'
   ORDERING: 0e090013:00000000
volume {274fa500-db95-9d70-0a66-1afb5c6e8446} \mxip_system.vol
oid30000001: dbase F00020017 T00000000  906 117376 ... '\ConfigMetabase'
   ORDERING: 0952001f:00000002 0f520013:00000001


[continua]…
```

```
volume {4c471600-b1cc-4ebc-d9ca-f96086433141} \cemail_ori.vol
oid38000162: dbase F00000017 T00000000    2    644 ... 'fldr31000030'
   ORDERING: 0e060040:00000000 0c1a001f:00000002 0037001f:00000002 001a0013:00000000
oid39000151: dbase F00000017 T00000000    0    356 ... 'fldr31000031'
   ORDERING: 0e060040:00000000 0c1a001f:00000002 0037001f:00000002 001a0013:00000000
oid330000ec: dbase F00000017 T00000000    0    356 ... 'pmailAttachs'
   ORDERING: 81000013:00000000
oid3c0000e4: dbase F00000017 T00000000    0    356 ... 'fldr31000028'
   ORDERING: 0e060040:00000000 0c1a001f:00000002 0037001f:00000002 001a0013:00000000
oid310000de: dbase F00000017 T00000000    0    356 ... 'fldr32000023'
   ORDERING: 0e060040:00000000 0c1a001f:00000002 0037001f:00000002 001a0013:00000000
oid320000d9: dbase F00000017 T00000000  335  68288 ... 'fldr31000026'
   ORDERING: 0e060040:00000000 0c1a001f:00000002 0037001f:00000002 001a0013:00000000
oid310000c9: dbase F00000017 T00000000    2    656 ... 'fldr3100002e'
   ORDERING: 0e060040:00000000 0c1a001f:00000002 0037001f:00000002 001a0013:00000000
oid310000c4: dbase F00000017 T00000000    0    356 ... 'fldr3200002c'
   ORDERING: 0e060040:00000000 0c1a001f:00000002 0037001f:00000002 001a0013:00000000
oid320000bf: dbase F00000017 T00000000    0    356 ... 'fldr3100002d'
   ORDERING: 0e060040:00000000 0c1a001f:00000002 0037001f:00000002 001a0013:00000000
oid310000ac: dbase F00000017 T00000000   50  18280 ... 'fldr31000027'
   ORDERING: 0e060040:00000000 0c1a001f:00000002 0037001f:00000002 001a0013:00000000
oid320000a7: dbase F00000017 T00000000    0    356 ... 'fldr31000025'
   ORDERING: 0e060040:00000000 0c1a001f:00000002 0037001f:00000002 001a0013:00000000
oid3d000032: dbase F00000017 T00000000  437 142136 ... 'fldr31000024'
   ORDERING: 0e060040:00000000 0c1a001f:00000002 0037001f:00000002 001a0013:00000000
oid33000029: dbase F00000017 T00000000    0    356 ... 'pmailVolumes'
oid3b000017: dbase F00000017 T00000000   53   3768 ... 'pmailNamedProps'
   ORDERING: 8300001f:00000000 83010013:00000000
oid30000009: dbase F00000017 T00000000   14   1124 ... 'pmailMsgClasses'
   ORDERING: 8300001f:00000000 83010013:00000000
oid30000007: dbase F00000017 T00000000    0    356 ... 'pmailOldTables'
oid30000003: dbase F00000017 T00000000  826 136536 ... 'pmailMsgs'
   ORDERING: 800c001f:00000000 0e090013:00000000 00150040:00000000
oid30000001: dbase F00000017 T00000000   21   2980 ... 'pmailFolders'
   ORDERING: 0e090013:00000000
```

Dump di una particolare tabella (non serve specificare il database), in questo caso abbiamo il contenuto della tabella dei messaggi inviati.

```
C:\Documents and Settings\Administrator\Desktop\itsutilsbin-20090515>pdblist -d fldr31000026
3d00074c (  676 10    442)
        8005 T13 L003d F0000 UI4 939525962
        8011 T13 L0037 F0000 UI4 146
        001a T13 L0e17 F0000 UI4 822083599
        003d T1f L0e06 F0000 STR [00156360]( 0) ''
        0037 T1f L0e07 F0000 STR [00156364](35) 'Quando hai ferie?dove vai?con chi? '
        0e17 T13 L8001 F0000 UI4 262144
        0e06 T40 L3008 F0000 FT  2009-07-19 16:27:56.000
        0e07 T13 L3008 F0000 UI4 33
        8001 T13 L0074 F0000 UI4 1023412044
        3008 T40 L0020 F0000 FT  2009-07-19 16:27:56.000

…[snip]…
```

MMS

Come illustrato nel precedente paragrafo, tutti i text messages sono contenuti all'interno del database cemail.vol. Gli MMS sono particolari messaggi che non contengono unicamente testo, ma possono contenere anche oggetti multimediali. Il formato che è stato scelto per questo tipo di messaggi, per mantenere un minimo di interoperabilità tra i diversi dispositivi mobili, è il formato SMIL.
Memorizzare gli oggetti multimediali che compongono gli MMS all'interno di un database, probabilmente non è molto conveniente, quindi questi oggetti sono memorizzati sotto forma di file *.dat (binari) all'interno della directory "/My Documents/UAContents/" . I file sono codificati secondo lo standard dettato da Open Mobile Alliance (www.openmobilealliance.org) e si possono decifrare utilizzando un semplice parser scritto in perl (http://search.cpan.org/dist/MMS-Parser/).

```
soundwave@mrblack:~/lavoro/forense/mmsparser/MMS-Parser/eg$ ./message-structure.pl –s 56359.dat
Message is of type M-Send-Req
Headers:
  'transaction_id_head' => 'ABC',
  'to_head' => {
    'text' => '+3934801234567/TYPE=PLMN',
    'TYPE' => 'PLMN',
    'address' => '+3934801234567'
  },
  'MMS_version_head' => '1.0',
  'message_type_head' => 'm_retrieve_conf',
  'content_type_head' => {
    'parameters' => {},
    'text' => 35,
    'media_type' => 35
  },
  'from_head' => 'insert-address'
Message has 2 parts:
1) text/plain
   | This is a sample text message.
   |
   | Let the World live in Peace!!!

2) image/jpeg
   * saving part data into erice-352.jpg
```

Registro chiamate, rubrica, appuntamenti

Oltre agli SMS ed email può essere molto utile avere l'elenco dei contatti, delle chiamate effettuate e ricevute e degli appuntamenti memorizzati nell'agenda del dispositivo. Come per gli SMS questi dati si trovano all'interno di un database. Il database è contenuto all'interno del file pim.vol. In questo caso la struttura del database è EDB (diversa dal CEDB utilizzata per gli SMS). Anche in questo caso viene in aiuto l'applicazione DBExplorer. In questo caso essendo la struttura del database EDB, non è possibile utilizzare i tool XDA, ma si deve per forza fare l'estrazione CSV attraverso le opzione di DBExplorer.

Data - Ora Inzio	Data – Ora Fine	Code	Numero Tel	Nome Rubrica	?	Progressivo
19/07/2009 20.56.15	19/07/2009 20.56.51	2054	+39340XXXXXX	Mario	0	2188
19/07/2009 20.42.19	19/07/2009 20.42.19	2053	+39340XXXXXX	Mario	0	2187
19/07/2009 19.30.54	19/07/2009 19.33.16	2054	+39340XXXXXX	Mario	0	2186
19/07/2009 19.14.02	19/07/2009 19.15.58	2054	+39347XXXXXX	Matteo	0	2185
19/07/2009 19.09.36	19/07/2009 19.12.25	2054	+39347XXXXXX	Matteo	0	2184
19/07/2009 17.18.23	19/07/2009 17.18.23	2053	+39329XXXXXX	Enzo	0	2183
19/07/2009 13.01.28	19/07/2009 13.01.28	2053	+39329XXXXXX	Enzo	0	2182
19/07/2009 10.42.57	19/07/2009 10.42.57	2053	+39329XXXXXX	Enzo	0	2181

I dati sono composto dai seguenti campi:

Data – Ora Inizio	Inizio della chiamata
Data – Ora Fine	Fine della chiamata
Code	Codice identificativo chiamata ingresso/uscita/risposta/persa (vedi tabella successiva)
Numero tel	Numero telefono interlocutore
Nome Rubrica	Contatto come registrato in rubrica (se non registrato il campo rimane vuoto)
?	Da identificare

Progressivo	Numero progressivo delle chiamate

Nella seguente tabella vengono illustrati i possibili codici (Code) presenti nel registro chiamate.

Code	Ingresso/Uscita	Andata a buon fine	Presente in rubrica
4	Ingresso	No	No
5	Uscita	No	No
6	Ingresso	Si	No
7	Uscita	Si	No
2052	Ingresso	No	Si
2053	Uscita	No	Si
2054	Ingresso	Si	Si
2055	Uscita	Si	Si

Registri

Come ogni sistema operativo Microsoft, anche Windows Mobile conserva le configurazioni delle applicazioni dell'utente e lo stato attuale del sistema nei file di registro. I file binari che contengono queste informazioni sono i seguenti:

Path	File	Contenuto
/Documents and Settings/	Default.hv	Registro di sistema
/Documents and Settings/	System.hv	Registro di sistema
/Documents and Settings/default/	Default.hv	Registro user

Purtroppo la struttura dei registri non è uguale a quella dei sistemi windows tradizionali, quindi non è possibile utilizzare RegRipper (a meno di non scrivere qualche plugin).
Si può sopperire a questa mancanza trasformando i file binari in file plaintext, ed andare a spulciare manualmente quello che ci interessa. La conversione è possibile attraverso il tool Make HV.
Di seguito trovate la sintassi per questo tool.

```
C:\Documents and Settings\Administrator\Desktop\forensic_tmp\make_hv_111>set _FLATRELEASEDIR=.

C:\Documents and Settings\Administrator\Desktop\forensic_tmp\make_hv_111>rgucomp.exe -nologo -o
user.hv>reg.txt
```

il risultato che se ne ottiene è il seguente:

```
…[SNIP]….
 [HKEY_CURRENT_USER\System\State]
  "Profile"="Vibrazione"

[HKEY_CURRENT_USER\System\State\Shell]
  "Active Application"="Profili_"
  "Start
MRU"=hex:0A,00,00,00,70,00,00,00,FF,FF,FF,FF,FF,FF,FF,FF,5C,00,57,00,69,00,6E,00,64,00,6F,00,77,0
0,73,00,5C,00,53,00,74,00,61,00,72,00,74,00,20,00,4D,00,65,00,6E,00,75,00,5C,00,41,00,63,00,63,00
,65,00,73,00,73,00,6F,00,72,00,69,00,65,00,73,00,5C,00,54,00,61,00,73,00,6B,00,20,00,4D,00,61,00,
6E,00,61,00,67,00,65,00,72,00,2E,00,6C,00,6E,00,6B,00,00,00,00,00,5C,00,00,00,FF,FF,FF,FF,FF,FF,F
F,FF,5C,00,57,00,69,00,6E,00,64,00,6F,00,77,00,73,00,5C,00,53,00,74,00,61,00,72,00,74,00,20,00,4D
,00,65,00,6E,00,75,00,5C,00,46,00,69,00,6C,00,65,00,20,00,45,00,78,00,70,00,6C,00,6F,00,72,00,65,
00,72,00,2E,00,6C,00,6E,00,6B,00,00,00,00,00,00,00,50,00,00,00,FF,FF,FF,FF,FF,FF,FF,FF,5C,00,57,0
0,69,00,6E,00,64,00,6F,00,77,00,73,00,5C,00,53,00,74,00,61,00,72,00,74,00,20,00,4D,00,65,00,6E,00
,75,00,5C,00,53,00,65,00,74,00,74,00,69,00,6E,00,67,00,73,00,2E,00,6C,00,6E,00,6B,00,00,00,00,00,
54,00,00,00,FF,FF,FF,FF,FF,FF,FF,FF,5C,00,57,00,69,00,6E,00,64,00,6F,00,77,00,73,00,5C,00,53,00,7
4,00,61,00,72,00,74,00,20,00,4D,00,65,00,6E,00,75,00,5C,00,4D,00,65,00,73,00,73,00,61,00,67,00,69
,00,6E,00,67,00,2E,00,6C,00,6E,00,6B,00,00,00,00,00,00,00,64,00,00,00,FF,FF,FF,FF,FF,FF,FF,FF,5C,
00,57,00,69,00,6E,00,64,00,6F,00,77,00,73,00,5C,00,53,00,74,00,61,00,72,00,74,00,20,00,4D,00,65,0
0,6E,00,75,00,5C,00,49,00,6E,00,74,00,65,00,72,00,6E,00,65,00,74,00,20,00,45,00,78,00,70,00,6C,00
,6F,00,72,00,65,00,72,00,2E,00,6C,00,6E,00,6B,00,00,00,00,00,00,00,50,00,00,00,FF,FF,FF,FF,FF,FF,
FF,FF,5C,00,57,00,69,00,6E,00,64,00,6F,00,77,00,73,00,5C,00,53,00,74,00,61,00,72,00,74,00,20,00,4
D,00,65,00,6E,00,75,00,5C,00,43,00,61,00,6C,00,65,00,6E,00,64,00,61,00,72,00,2E,00,6C,00,6E,00,6B
,00,00,00,00,00,60,00,00,00,FF,FF,FF,FF,FF,FF,FF,FF,5C,00,57,00,69,00,6E,00,64,00,6F,00,77,00,73,
00,5C,00,53,00,74,00,61,00,72,00,74,00,20,00,4D,00,65,00,6E,00,75,00,5C,00,56,00,6F,00,69,00,63,0
0,65,00,20,00,43,00,6F,00,6D,00,6D,00,61,00,6E,00,64,00,65,00,72,00,2E,00,6C,00,6E,00,6B,00,00,00
,00,00,00,00,4C,00,00,00,FF,FF,FF,FF,FF,FF,FF,FF,5C,00,57,00,69,00,6E,00,64,00,6F,00,77,00,73,00,
5C,00,53,00,74,00,61,00,72,00,74,00,20,00,4D,00,65,00,6E,00,75,00,5C,00,54,00,61,00,73,00,6B,00,7
3,00,2E,00,6C,00,6E,00,6B,00,00,00,00,00,00,00,4C,00,00,00,FF,FF,FF,FF,FF,FF,FF,FF,5C,00,57,00,69
,00,6E,00,64,00,6F,00,77,00,73,00,5C,00,53,00,74,00,61,00,72,00,74,00,20,00,4D,00,65,00,6E,00,75,
00,5C,00,43,00,61,00,6D,00,65,00,72,00,61,00,2E,00,6C,00,6E,00,6B,00,00,00,00,00,6C,00,00,00,FF,F
F,FF,FF,FF,FF,FF,FF,5C,00,57,00,69,00,6E,00,64,00,6F,00,77,00,73,00,5C,00,53,00,74,00,61,00,72,00
,74,00,20,00,4D,00,65,00,6E,00,75,00,5C,00,41,00,63,00,63,00,65,00,73,00,73,00,6F,00,72,00,69,00,
65,00,73,00,5C,00,43,00,61,00,6C,00,63,00,75,00,6C,00,61,00,74,00,6F,00,72,00,2E,00,6C,00,6E,00,6
B,00,00,00,00,00
  "Most Recent
Event"=hex:00,00,00,00,00,00,00,00,43,00,6F,00,6C,00,6C,00,65,00,67,00,61,00,6D,00,65,00,6E,00,74
,00,69,00,00,00,5C,00,57,00,69,00,6E,00,64,00,6F,00,77,00,73,00,5C,00,48,00,50,00,53,00,68,00,6F,
00,72,00,74,00,63,00,75,00,74,00,73,00,2E,00,65,00,78,00,65,00,00,00,00,00

[HKEY_CURRENT_USER\System\State\Messages\Syncing]

[HKEY_CURRENT_USER\System\State\Messages\vmail\VoIP\Unread]

[HKEY_CURRENT_USER\System\State\Messages\vmail\Line2\Unread]
  "Count"=dword:0

[HKEY_CURRENT_USER\System\State\Messages\vmail\Line1\Unread]
  "Count"=dword:0
…[SNIP]…
```

I registri che potrebbero rivelarsi utili e che si trovano all'interno degli hive sono i seguenti (la lista non è esaustiva)

Registro	**Descrizione**
HKLM\Software\Microsoft\WZCSVC\Parameters\Interfaces\	Reti a cui si è connesso il dispositivo
HKLM\Software\Microsoft\Shell\CumulativeCallTimers\Line_0	Statistiche globali sulle chiamate (tempo)
HKLM\Software\Microsoft\Bluetooth\device\	Dispositivi BT a cui si è connesso il dispositivo
HKLM\Comm\[nome-connessione]	Indirizzi IP del DHCP e DNS di connessioni effettuate.
HKLM\Comm\Tcpip\Parms	Parametri dell'ultima connessione
HKLM\Comm\Tcpip\Hosts\ppp_peer	Indirizzo ip assegnato durante l'ultima connessione.
HKLM\Comm\ConnMgr\Providers\[id interfaccia]\[nome rete]	Reti a cui il dispositivo ha tentato di connettersi
HKLM\Software\Microsoft\RIL	Informazioni riguardanti IMSI ICCID

HKLM\Software\HP\HPiPAQDataConnect	Contiene l'IMSI corrente e l'IMSI precedente (solo dispositivi HP?)

Formato IMSI

Il numero IMSI è l'identificativo univoco della schede SIM. Si tratta i un numero che viene associato ad ogni utenza mobile. Questo numero è inviato alla rete mobile per identificare la scheda SIM.

Il numero è formato da 15 digit suddiviso in:

- Mobile Country code (MCC)
- Mobile Network Code (MNC)
- Mobile Station Identification Number (MSIN)

Di seguito una tabella esemplificativa con degli MCC Europei:

MCC	**Country CODE**	**Country**
222	IT	Italy
232	AT	Austria
228	CH	Switzerland
262	DE	Germay
208	FR	France
214	ES	Spain
292	SM	San Marino (esatto, anche san marino ha un operatore mobile)

Di seguito una tabella con gli MNC degli operatori italiani

MNC	**Operatore**
01	TIM
02	Elsacom (satellitare)
10	Vodafone
30	RFI (Rete ferroviaria italiana)
88	Wind
99	Tre italia

Nella tabella non sono compresi gli operatori virtuali chiamati MVNO (es. MTV mobile, PosteMobile, etc), in italia non hanno un proprio MNC ma utilizzano quello dell'operatore a cui si appoggiano.

Prendiamo ad esempio il seguente numero IMSI: 222881234567890
Questo è suddiviso come segue:

222	Numero identificativo dell'Italia
88	Numero Identificativo dell'operatore Wind
1234567890	Identificativo SIM (MSIN) mobile station id num

Per evitare di doversi tenere a mente tutti i codici degli operatori è possibile utilizzare il tool IMSI lookup raggiungibile al seguente URL.

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

6. References

1. IMSI Search engine -https://www.numberingplans.com/?page=analysis&sub=imsinr
2. MIAT-WM5: Forensic acquisition for windows mobile pocketPC, Fabio Dellutri, Vittorio Ottaviani, Gianluigi Me - http://www.scs-europe.net/conf/ecms2008/ecms2008%20CD/hpcs2008%20pdf/hpcs08w1-5.pdf
3. XDA Developer forum- http://forum.xda-developers.com
4. XDA Utils - http://www.xs4all.nl/~itsme/projects/xda/tools.html
5. Registry converter tool - http://forum.xda-developers.com/showpost.php?p=898198&postcount=229
6. SMIL standards - http://www.w3.org/AudioVideo/
7. IMSI reference - http://en.wikipedia.org/wiki/IMSI
8. DBExplorer - http://www.phatware.com
9. CEDB format Database - http://msdn.microsoft.com/en-us/library/aa916035.aspx
10. EDB format Database - http://msdn.microsoft.com/en-us/library/aa914733.aspx
11. MMS binary Parser - http://search.cpan.org/dist/MMS-Parser/