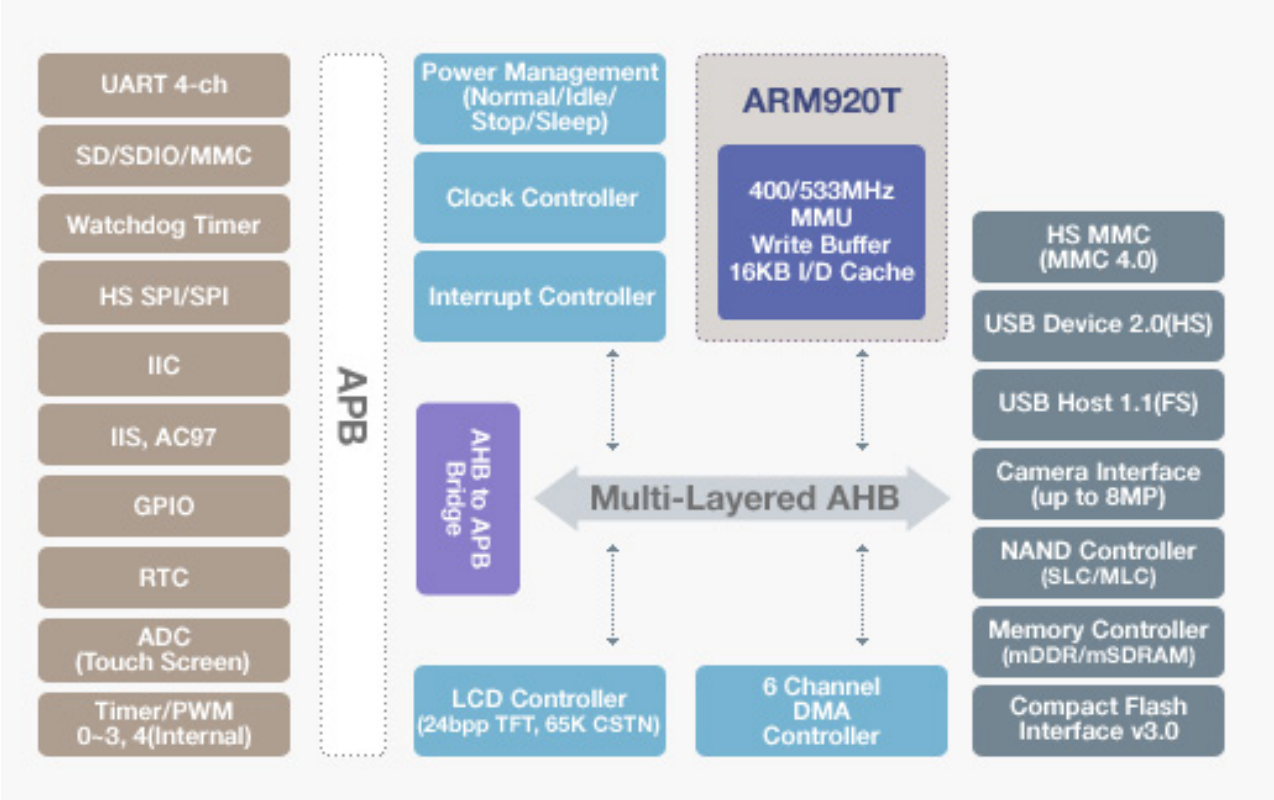
SPERIMENTAZIONE
DI UN METODO DI ANALISI FORENSE
DEL DISPOSITIVO DI NAVIGAZIONE SATELLITARE
TOMTOM

Clara Maria Colombini

INTRODUZIONE

I primi navigatori satellitari nascono a scopi militari sui sottomarini statunitensi Polaris, allo scopo di rilevare la loro posizione. Col passare degli anni, la tecnologia di rilevazione satellitare si è evoluta e diffusa al punto da essere presente su gran parte degli autoveicoli in circolazione.
TomTom, dispositivo di navigazione satellitare nato per l'utenza automobilistica, si avvale del collegamento al sistema satellitare globale di navigazione (GNSS) NAVSTAR Global Positioning System (GPS) (USA), consistente di 32 satelliti in orbita MEO su sei differenti piani orbitali.

Il dispositivo Tomtom si avvale al suo interno di un computer con processore ARM creato da Samsung, che gestisce, attraverso un sistema Linux, il funzionamento del software che, a seconda del dispositivo, può trovarsi sia su una scheda SD che nella memoria interna. Un 'boot loader' nel computer ricerca nel contenuto della memoria interna o nella scheda SD il software e i dati della mappa in uso. Esso poi trasferisce il software alla memoria RAM interna da 64 MB e avvia il software. L'hardware avvia il GPS e l'applicazione di navigazione. L'applicazione di navigazione quindi legge tutte le impostazioni installate, come la voce preferita e l'ultimo percorso prescelto.



Architettura interna di Tomtom

Il modulo GPS integrato assicura che il segnale del satellite si traduca in coordinate che individuino la posizione esatta sulla mappa. Dopo l'avvio, il modulo GPS calcola la posizione in base ai segnali del satellite più vicino, che elabora la posizione calcolando la distanza da almeno quattro diversi satelliti, che inviano informazioni quali la loro identità, altitudine, posizione in relazione agli altri satelliti, ecc.

Sui modelli più recenti è inoltre presente la modalità RDS-TMC ("Radio Data System-Traffic Message Channel") (sistema per trasmissioni via radio-Canale per i messaggi di traffico). E' un servizio che comunica informazioni sul traffico in tempo reale al dispositivo di navigazione attraverso un apposito ricevitore. Il service provider codifica il messaggio e lo invia ai trasmettitori radio FM, che lo trasmettono come un segnale RDS (Radio Data System) all'interno delle normali trasmissioni radio FM. Il decoder TMC all'interno di TomTom decodifica il messaggio e lo comunica come messaggio visivo o vocale.

La funzione Bluetooth, nei modelli che la contemplano, consente a TomTom di comunicare con altri dispositivi elettronici come il telefono cellulare, fungendo da vivavoce, o ricevendo le informazioni inviate al telefono cellulare tramite una connessione wireless GPRS (General Packet Radio Service) o UMTS (Universal Mobile Telecommunications System).

Il presente lavoro verte sulla ricerca di una procedura di analisi forense sui dispositivi di navigazione satellitare TOMTOM, sui quali è possibile rinvenire dati estremamente utili ai fini investigativi. Infatti, le informazioni sugli indirizzi memorizzati, gli itinerari costruiti, il punto "base", i punti di interesse personalizzati, ecc., permettono di ricostruire gli spostamenti, gli itinerari preferiti, le mete di viaggio più frequenti dell'utilizzatore del dispositivo.

Il punto centrale della sperimentazione è stata la ricerca di una procedura di realizzazione dell'immagine forense della memoria interna che sia "ripetibile", e cioè che consenta di ottenere, dal medesimo dispositivo, una identica immagine forense, a distanza di tempo, per eventuali analisi successive o di controparte.

DISPOSITIVI ANALIZZATI

Nello specifico, sono stati sottoposti ad analisi i seguenti modelli:

1. Tomtom One con sola memoria interna da 1 GB – modello 2006;
2. Tomtom One con sola memoria interna da 2 GB – modello 2008;
3. Tomtom One con sola memoria esterna SD Card – modello 2006;
4. Tomtom One XL Italia con memoria interna da 512 MB + SD Card – modello 2008;
5. Tomtom Go 730 con memoria interna da 1 GB + SD Card – modello 2008.

CREAZIONE DELL'IMMAGINE FORENSE

Si premette che, nella fase di sperimentazione che riguarda la connessione al PC, non è stata presa in considerazione la procedura di realizzazione dell'immagine forense della scheda di memoria SD Card, in quanto, essendo essa estraibile dal dispositivo, può essere trattata come una qualunque memoria di massa secondo le regole della Computer Forensics.

Per "immagine forense" si intende qui il risultato di una particolare procedura di copia, detta "bit a bit", che va a leggere la superficie fisica del supporto di memoria, leggendo un bit dopo l'altro, e ne produce un "clone", cioè una copia esattamente identica, su un supporto di destinazione, il cui contenuto verrà sottoposto ad analisi. Quando possibile, infatti, l'analisi forense non viene effettuata sul dispositivo originale, ma su un suo"clone", o immagine forense (la cosiddetta "bistream image"[1]), allo scopo di preservare l'integrità del reperto originale per eventuali analisi future.

Per ognuno dei 4 modelli presi in esame sono state realizzate tre immagini forensi (una per ogni PC), per i seguenti scopi:

1. non avendo a disposizione una immagine "originale" cioè "sicuramente non alterata" di partenza con cui confrontare le immagini realizzate con questa sperimentazione, situazione ottenibile solo in modo invasivo, si è scelto di utilizzare come punto di partenza la prima

[1] La "bit stream image", realizzata con appositi tool forensi, a differenza della mera copia, consente di operare su un supporto di memoria digitale identico all'originale, sia in maniera logica che fisica, quindi anche su eventuali parti presumibilmente vuote dello stesso, che potrebbero contenere file o frammenti di file cancellati non sempre visibili con i normali strumenti.

immagine realizzata, verificando sulle altre due eventuali modifiche verificatesi durante i test;

2. si è scelto di utilizzare tre PC differenti per simulare il più possibile situazioni ambientali differenti (es.: una controperizia, un'analisi in tempi successivi ecc.).

Allo scopo di offrire una panoramica sufficientemente ampia, si è proceduto alla realizzazione dell'immagine forense su:

- Personal Computer con sistema operativo Windows;
- Personal Computer con sistema operativo Linux.

PROCEDURA IN AMBIENTE WINDOWS

La procedura di realizzazione delle tre immagini forensi è stata eseguita su tre Personal Computer differenti:

1. PC workstation con sistema operativo Microsoft Windows XP PRO SP3;
2. PC notebook con sistema operativo Microsoft Windows Vista Home Edition;
3. Eee PC con sistema operativo Microsoft Windows XP Home Edition.

Software utilizzato:
Accessdata FTK Imager 2.55 (software a distribuzione gratuita).

Si precisa che non è stato possibile utilizzare il dispositivo hardware di blocco in scrittura a disposizione (Tableau T8) in quanto in tale modalità di connessione (TomTom ➔ T8 ➔ PC) il Personal Computer non riconosce il dispositivo.

PREPARAZIONE DEL PC

Per prima cosa si è verificato che sul PC non fosse presente il software TOMTOMHOME, utilità di collegamento per l'aggiornamento dati di Tomtom, e che nei file di registro non fosse presente alcuna chiave o voce di registro di precedenti installazioni di TomTom:

- file di registro SOFTWARE;
- file di registro SYSTEM, in cui nella sottochiave CONTROL SET …..\ENUM\USBSTOR non devono essere presenti voci relative a installazioni precedenti di driver USB di Tomtom.

Questa verifica si è resa necessaria in quanto Tomtom, non appena collegato al PC, tenta di aggiornare i propri dati ricercando sul PC il software e le chiavi di registro segnalate, con la conseguenza di alterare i file al suo interno.

Non potendo usufruire di dispositivi hardware di blocco in scrittura, sono state poi configurate le porte USB in sola lettura creando una apposita voce di registro che ha permesso di disabilitare a comando l'opzione di scrittura sulle periferiche connesse al PC attraverso le porte USB.

Il PC è stato scollegato da Internet, per evitare incidentali tentativi di aggiornamento del dispositivo.

Per quanto riguarda la memorizzazione delle immagini forensi ottenute, su ognuno dei tre PC utilizzati è stata creata una nuova partizione di 50 GB, sottoposta a wiping[2] e formattata in Fat32.

CONNESSIONE DEL DISPOSITIVO AL PC

Materiale utilizzato: cavo di collegamento Mini USB per Tomtom.
Ambiente: l'analisi è stata eseguita in un locale chiuso, in modo da non permettere in alcun modo al dispositivo Tomtom di connettersi al satellite.

Il punto più delicato dell'intera sperimentazione è stato quello di trovare un metodo di connessione del dispositivo al Personal Computer che permetta al sistema operativo di "vedere" la memoria interna di Tomtom senza andare però a modificare in alcun modo i dati in essa contenuti, compresi i rispettivi "metadati", cioè quegli altri dati che li descrivono (es.: data di creazione, data di modifica, data di accesso, dimensione ecc.).

La procedura di connessione varia a seconda del modello: ognuno di loro infatti si comporta in modo diverso seguendo due tipi di comportamento a seconda che posseggano o meno la porta (slot) per SD Card.
Si precisa che per il modello con la sola SD Card si è proceduto all'analisi diretta della stessa secondo le regole della Computer Forensics.

Poiché il dispositivo Tomtom deve essere collegato alla porta USB del computer e acceso, allo scopo di rilevare eventuali modifiche ai dati in esso contenuti al momento dell'installazione dei driver, durante tutta la procedura di connessione si è effettuato il monitoraggio dei flussi delle comunicazioni via USB tra Tomtom e PC. L'analisi è stata realizzata tramite uno specifico tool, SysNucleus USB Trace v. 2.0.

[2] Procedura di cancellazione attraverso la quale i file vengono eliminati definitivamente dal supporto di memoria scrivendo ripetutamente al loro posto informazioni nulle fino al eliminarne qualsiasi traccia.

MODELLI SENZA PORTA PER SD CARD

MODELLI SOTTOPOSTI A TEST:
Tomtom One con sola memoria interna da 1 GB – modello 2006;
Tomtom One con sola memoria interna da 2 GB – modello 2008.

CONNESSIONE

Si accende il PC e si avvia il sistema operativo.
Si fa partire il monitoraggio del flusso di dati via USB sulla porta di collegamento scelta per la connessione.
Si collega il dispositivo spento al PC tramite il cavo apposito. Si accende il dispositivo Tomtom.
Sullo schermo del dispositivo appare la schermata qui sotto illustrata:

Si seleziona “SI”. Sullo schermo successivo appare l’immagine qui sotto riportata che indica che la connessione è stata avviata.

Quando la connessione è stata stabilita, appare la schermata qui sotto riportata.

Il computer avvisa che è stato trovato un nuovo dispositivo USB, ne installa i driver ed assegna alla nuova periferica collegata una lettera di unità disco.
La procedura è stata la medesima per i tre differenti PC utilizzati.
L'analisi dei dati prodotti dal monitoraggio dei flussi delle comunicazioni via USB tra Tomtom e PC, effettuato durante l'operazione di connessione ed installazione dei driver di ogni dispositivo, ha permesso di evidenziare che non vengono effettuate modifiche ai dati contenuti nel dispositivo.

CREAZIONE DELL'IMMAGINE

La creazione dell'immagine forense sui tre differenti PC a disposizione, viene effettuata utilizzando il software FTK Imager di Accessdata v. 2.55, che calcola gli Hash[3] MD5 e Sha1 sia dell'originale[4] che dell'immagine creata e ne verifica l'identicità.
Viene scelta come origine l'unità fisica della nuova periferica UBS collegata e si sceglie come tipo immagine il formato dd (non elaborato).
Unità di destinazione la partizione creata ad hoc su PC.

La procedura è la medesima per i tre PC utilizzati.

[3] Per "hash " va inteso l'hash calcolato su un flusso di dati che si determina dopo che due sistemi intelligenti (con CPU) hanno aderito su un protocollo di comunicazione.
[4] Per "originale" va inteso non l'originale contenuto di dati del dispositivo, ma l'originale del flusso di dati che dal dispositivo esce quando connesso ad un sistema Windows.

RISULTATO

La verifica dei file di Hash MD5 e SHA1[5], che risultano identici, conferma che le tre immagini realizzate per ognuno dei 4 dispositivi sono esattamente uguali e che non è avvenuta alcuna modifica dei dati nel flusso che il Tomtom genera quando collegato ad uno dei sistemi Windows.
L'operazione di confronto è stata effettuata attraverso il tool MD5summer v. 1.2.0.11.

In ogni caso, come si è potuto rilevare, operazione indispensabile è sempre e comunque l'accensione del dispositivo, in quanto si è voluto effettuare una procedura "non invasiva" di analisi, e cioè che non comporti l'apertura dello stesso e/o l'estrazione della memoria interna.

[5] Gli algoritmi di Hash costituiscono una sorta di "impronta", che contraddistingue in maniera univoca la traccia informatica oggetto dell'analisi forense, al fine di ottemperare alle esigenze di integrità del dato. Tale "marchio digitale" è creato con un'operazione cosiddetta di hashing a senso unico, (es MD5 e SHA1), che generano un'impronta che costituisce un riferimento certo alla traccia originale, ma non ne consente la ricostruzione. Tali algoritmo sono utilizzati a livello internazionale e garantiscono un buon livello di sicurezza.

MODELLI CON MEMORIA INTERNA + PORTA PER SD CARD

MODELLI SOTTOPOSTI A TEST

Tomtom One XL Italia con memoria interna da 512 MB + SD Card – modello 2008.

Tomtom Go 730 con memoria interna da 1 GB + SD Card – modello 2008.

Materiale aggiuntivo utilizzato: scheda di memoria di tipo SD Card sottoposta a wiping [2] .

CONNESSIONE

Nel caso in cui il dispositivo Tomtom sia fornito, oltre che della memoria interna, anche di slot per scheda di memoria SD Card, si rende necessaria un'operazione preliminare alla connessione vera e propria per la realizzazione dell'immagine forense, poiché questo tipo di dispositivi offre due modalità di connessione a PC:

- senza SD card inserita nello slot: il dispositivo si pone in modalità "aggiornamento" andando a ricercare sul PC il software Tomtom Home, attraverso il quale si connette ad Internet per aggiornare i propri dati. Non trovandolo, tenta di installarlo (nel software presente sui dispositivi è compresa una versione compatta di TomTom Home autoinstallante). Il PC lo riconosce come dispositivo di navigazione e installa i driver per l'aggiornamento dati. In questa modalità alcuni file presenti sul dispositivo vengono automaticamente aggiornati e quindi alterati. Ciò viene confermato dall'analisi dei dati prodotti dal monitoraggio dei flussi delle comunicazioni via USB tra Tomtom e PC, effettuato tramite il tool SysNucleus USB Trace v. 2.0, durante l'operazione di connessione di ogni dispositivo di questo tipo nella modalità qui descritta.

- con SD Card inserita: il dispositivo si pone in modalità "periferica USB"e come tale viene riconosciuto dal PC, che installa i soli driver di connessione USB. Non viene tentata alcuna comunicazione volta all'aggiornamento dei dati di Tomtom e non viene ricercato il software Tomtom Home sul PC. Quindi non viene effettuata alcuna modifica di file all'interno del dispositivo, ma esso rende visibile alla macchina il contenuto della sola SD Card, cui viene

assegnata una lettera di unità disco esterno. L'analisi dei dati prodotti dal monitoraggio dei flussi delle comunicazioni via USB tra Tomtom e PC, effettuato tramite il tool SysNucleus USB Trace v. 2.0, durante l'operazione di connessione ed installazione dei driver di ogni dispositivo, conferma che non vengono effettuate modifiche ai dati contenuti nel dispositivo.

Ala luce delle informazioni così ottenute, si è proceduto alla connessione nel modo qui di seguito riportato, che si è rivelato ottimale per la rilevazione da parte del PC del contenuto della memoria interna.

Dopo aver eliminato dai PC utilizzati ogni traccia dei driver di Tomtom precedentemente installati, si collega il dispositivo spento al PC tramite il cavo mini-usb.

Si inserisce nel dispositivo la SD Card "forense"creata (vedi sopra: materiale aggiuntivo utilizzato).

Si accende quindi il dispositivo.

L'immagine qui sotto riportata mostra la schermata di TomTom in via di connessione.

La schermata di Tomtom mostra che il dispositivo è in fase di connessione: si è posto in modalità periferica Usb ed il PC visualizza il contenuto della sola SD Card, cui il sistema operativo assegna una lettera di unità disco esterno.

Un volta installati i driver di connessione USB, si spegne il dispositivo, si rimuove la SD Card e si riaccende il dispositivo.
La schermata di Tomtom mostra di nuovo la schermata di connessione.

Il computer non necessita di riconoscere di nuovo la periferica, in quanto possiede già i relativi driver, e visualizza il contenuto della memoria interna all'interno dell'unità disco esterno precedentemente assegnata alla SD Card. L'analisi dei dati prodotti dal monitoraggio dei flussi delle comunicazioni via USB tra Tomtom e PC, effettuato tramite il tool SysNucleus USB Trace v. 2.0, durante l'operazione di connessione ed installazione dei driver di ogni dispositivo, conferma che non vengono effettuate modifiche ai dati contenuti nel dispositivo.

CREAZIONE DELL'IMMAGINE

A questo punto si procede con la creazione dell' immagine forense sui tre differenti PC a disposizione, utilizzando il software FTK Imager di Accessdata v. 2.55.
Viene scelta come origine l'unità fisica della nuova periferica USB collegata e si sceglie come tipo immagine il formato dd (non elaborato).
Unità di destinazione la partizione creata ad hoc su PC.
La procedura è la medesima per i tre differenti PC.

RISULTATO

La verifica dei file di Hash MD5 e SHA1[6], che risultano identici, conferma che le tre immagini realizzate per ognuno dei 4 dispositivi sono esattamente uguali e che non è avvenuta alcuna modifica dei dati nel flusso che il Tomtom genera quando collegato ad uno dei sistemi Windows.
L'operazione di confronto è stata effettuata attraverso il tool MD5summer v. 1.2.0.11.

In ogni caso, come si è potuto rilevare, operazione indispensabile è sempre e comunque l'accensione del dispositivo, in quanto si è voluto effettuare una procedura "non invasiva" di analisi, e cioè che non comporti l'apertura dello stesso e/o l'estrazione della memoria interna.

[6] Gli algoritmi di **Hash** costituiscono una sorta di "impronta", che contraddistingue in maniera univoca la traccia informatica oggetto dell'analisi forense, al fine di ottemperare alle esigenze di integrità del dato. Tale "marchio digitale" è creato con un'operazione cosiddetta di hashing a senso unico, (es MD5 e SHA1), che generano un'impronta che costituisce un riferimento certo alla traccia originale, ma non ne consente la ricostruzione. Tali algoritmo sono utilizzati a livello internazionale e garantiscono un buon livello di sicurezza

PROCEDURA IN AMBIENTE LINUX

La procedura è stata eseguita anche qui su tre Personal Computer differenti:

1. PC workstation con sistema operativo Linux Fedora v. 10;
2. PC notebook con sistema operativo Linux Helix v. 1.9 in modalità live[7] da CD;
3. Eee PC con sistema operativo Linux NBCaine v. 0.5. in modalità live da penna USB.

CONNESSIONE

In ambiente Linux non si è resa necessaria alcuna particolare procedura di connessione diversificata per i differenti modelli del dispositivo.
Si collega il dispositivo spento al PC attraverso il cavo mini-usb e quindi si accende.
Il sistema operativo Linux riconosce il dispositivo come periferica di memoria USB.
Non è necessario "montare"[8] il dispositivo TomTom che rimane quindi configurato in sola lettura.
Si monta e si configura invece in lettura-scrittura il supporto di destinazione delle immagini.

CREAZIONE DELL'IMMAGINE

Si procede quindi alla creazione delle immagini forensi in formato "dd", utilizzando i software qui riportati:

1. Linux Fedora v. 10: procedura a riga di comando tramite console[9];
2. CD Helix Live 3: ADEPTO 2.0;
3. USB NBCaine: AIR 1.2.8.

[7] La modalità **live** permette l'utilizzazione di un sistema operativo caricato in memoria direttamente da un CD o da una penna USB, senza quidi la necessità di coinvolgere il /gli hard disk presenti nella macchina.
[8] L'operazione di **mount** consente di inizializzare una periferica a blocchi al fine di ottenere un accesso in modalità lettura/scrittura.
[9] La modalità a **console** si contrappone alla modalità grafica nella quale la scelta del comando da impartire è agevolato da un'interfaccia grafica con pulsanti e finestre. In modalità console, ogni comando impartito, va scritto senza nessuna intermediazione.

PROCEDURA A RIGA DI COMANDO

Si verifica con il comando *mount*[8] che nessuno dei due dischi (sia quello di origine, cioè la memoria interna di Tomtom, che la partizione da noi scelta per la memorizzazione dell'immagine) sia stato automaticamente montato, e si procede di conseguenza al montaggio in scrittura della partizione destinata a contenere l'immagine forense, mentre non si esegue il *mount* del disco originale in quanto si va a leggere direttamente dal dispositivo con il comando di copia.

 # mount -o rw /dev/hdb4 /media/hdb4

Prima di procedere alla copia, si effettua un *wiping* del supporto di destinazione, in modo da cancellare qualsiasi dato precedentemente memorizzato. L'operazione si può completare con il seguente comando:

 # wipe /media/hdb4

Si effettua l'*hash* dell'originale con l'uso del comando *DD* specificando solo l'input file e mandando l'output di questo comando in *pipe*[10] ad un *md5sum* (esecuzione del'hash MD5*).*

 # dd if=/dev/hda1 | md5sum

Si procede quindi alla creazione dell'immagine: il tool scelto per la copia è *DD*, usato nella sua forma più semplice. La sintassi del comando richiede di specificare un *input file* ed un *output file*.

 # dd if=/dev/sdb1 of=/media/hdb4/tomtom01.img

A operazione conclusa, il comando restituisce il numero di record letti e scritti, con qualche statistica circa i byte copiati, il tempo totale dell'operazione e il transfert rate medio del processo.

Si effettua infine l'hash dell'immagine creata con l'uso del comando *DD* specificando solo l'input file e mandando l'output di questo comando in *pipe*[11] ad un *md5sum.*

 # dd if=/media/hdb4/tomtom01.img | md5sum

[10] La **pipe** in UNIX è un meccanismo che consente di controllare il flusso di informazioni. In altri termini, la pipe è un sistema che consente di utilizzare il flusso di informazioni in uscita da un comando, come input per un altro comando.

PROCEDURA TRAMITE IL TOOL AIR

L'utilizzo di tool a riga di comando comporta inevitabilmente dei vantaggi e degli svantaggi; il vantaggio principale è che si ha il completo controllo di ogni singola istruzione impartita, specificando in prima persona quali devono essere le opzioni ed i relativi parametri per ogni strumento; d'altra parte, la complessità dei comandi stessi ed il diverso numero di opzioni, possono indurre più facilmente in errore.

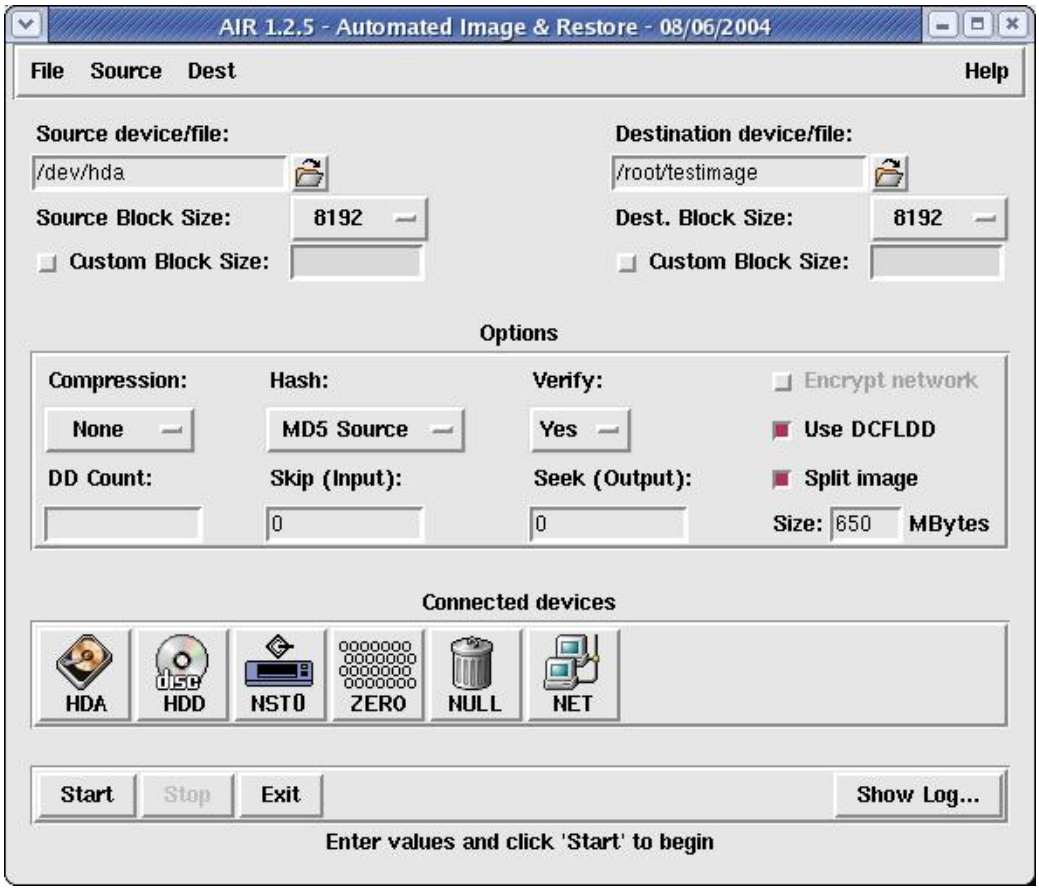
Le distribuzioni Helix e Caine però, vengono incontro a queste difficoltà, offrendo una serie di tool ad interfaccia grafica che consentono all'operatore di sfruttare l'usabilità delle interfacce a finestre.

Si mostra qui di seguito la procedura di creazione del'immagine forense attraverso il tool grafico Air, acronimo di Automated Image & Restore, compresa nella distribuzione Caine.

Si procede nel selezionare il device (dispositivo) sorgente sulla parte sinistra della maschera, mentre sulla destra si sceglie il device di destinazione.
Si sceglie quindi di non effettuare alcuna compressione del'immagine creata.
Si seleziona il tipo di hash da utilizzare per verificare l'identità tra quanto letto e la copia effettuata.
Si utilizza DCFLDD[12] al posto di DD.
Si è scelto di non dividere l'immagine in diversi file e di non cifrare il file con una chiave.
Si è infine specificata l'opzione *noerror* al parametro *conv*, che fa proseguire l'operazione di creazione del'immagine anche in caso di errori in fase di lettura.

Prima di premere sul pulsante start e dare inizio al processo di copia, si è aperta la finestra di stato, cliccando sul bottone *show status windows*, che mostra l'andamento del'operazione.

[12] DCFLDD consente di effettuare alcune operazioni più ed ha soprattutto il vantaggio del calcolo dell'hash simultaneamente alla creazione della copia eliminando il passaggio aggiuntivo richiesto con l'utilizzo di DD.



Finestra grafica del tool AIR

RISULTATO

La verifica dei file di Hash, che risultano identici, conferma che le tre immagini realizzate per ognuno dei 4 dispositivi sono esattamente uguali e che non è avvenuta alcuna modifica dei dati nel flusso che il Tomtom genera quando collegato ad un sistema.

In ogni caso, come si è potuto rilevare, operazione indispensabile è sempre e comunque l'accensione del dispositivo, in quanto si è voluto effettuare una procedura "non invasiva" di analisi, e cioè che non comporti l'apertura dello stesso e/o l'estrazione della memoria interna.

ANALISI

I supporti di memoria contenuti nei dispositivi TomTom (sia la memoria interna che le SD card) si comportano esattamente come qualsiasi altro supporto di memoria digitale in cui è possibile memorizzare, occultare e cancellare file di qualsiasi tipo.
La creazione dell'immagine forense "bit a bit" della memoria di Tomtom ha permesso di effettuare l'analisi del suo intero contenuto, consentendo quindi anche il carving[13] di dati cancellati o frammentati, con l'utilizzo di appositi software forensi.

Per effettuare l'analisi è stato utilizzato il tool AccessData FTK 2.2 in ambiente Windows, in grado di visualizzare il contenuto di tutti i file presenti, compresi i relativi metadati, e di recuperare i file cancellati o frammentati.

Ai fini però di un'indagine rivolta alla ricerca di dati sulla navigazione satellitare operata con il dispositivo, vengono qui di seguito elencati solo i file relativi.

TTGO.BIF	Contiene le informazioni relative al dispositivo, tra cui: modello, numero di serie, lingua, mappa corrente, base corrente, voce. Qui di seguito un esempio del contenuto del file da cui si evincono le informazioni. [TomTomGo] DeviceName=TomTom ONE XL DeviceVersionHW=ONE XL DeviceSerialNumber=L26497J00167 DeviceUniqueID=AK8AG AADSW RamDiskVersion=20080529 BootLoaderVersion=53026 LinuxVersion=190943 ApplicationVersionVersionNumber=8010 ApplicationVersion=9369 UserLanguage=Italiano UserName=L26497J00167 LastConnectionTime=Never GPSFirmwareVersion= BuiltInColorScheme0=Belgica BuiltInColorScheme1=Brittanica BuiltInColorScheme2=America BuiltInColorScheme3=Germanica

[13] Per data **carving** si intende la tecnica di recupero di file cancellati o deallocati.

	BuiltInColorScheme4=Australia BuiltInColorScheme5=Deuteranopia BuiltInColorScheme6=Greys BuiltInColorScheme7=Antarctica BuiltInColorScheme8=Africa BuiltInColorScheme9=Astra CurrentColorSchemeBuiltIn=1 CurrentVoiceInfo=Roberto CurrentMap=Italia CurrentMapVersion=710.1571 CurrentHomeLocation=45.53052,9.03387,Via Francesco Daverio 11, Milano Traffic=N CurrentFuelpricesType= CurrentFuelpricesTypeString= CurrentFuelpricesLastFullUpdate= ValueRatio=BpHDxKhXmBZzHUCpsA== Features=PlusDownloadDynamic,PlusDownloadGeneral,PlusDownloadMap,PlusDownloadPOI,PlusDownloadScheme,PlusDownloadUpgrade,PlusDownloadVoice,PlusDownloadRingTone,PlusMessageNotification,PlusPushChannel,PlusTraffic,PlusWeather,PlusEphemeris,PlusBuddies,PlusMobileSafetyCameras,PlusRoadConditions,PlusFixedSafetyCameras,PlusFuelPrices,HDTraffic,PlusOnlineCamera,PlusTripReporting,HomeBackup,PhotoJPGViewer,PhotoBMPViewer,Newyork,Newyork1Dot6,Itinerary,Caymann,Durham,PhoneFeatures,CarSymbol,RDSTMC,Prague,Bluetooth,SDSlot,InternalFlash SupportedPatchTypes=1F NrSupportedErrorTypes=132 UserPatchDatVersion=102 CompressedPatchVersion=150 MapServerPatchDatVersion=104 DeletedPoiDatVersion=200 ServerLineIndexDatVersion=102 ServerNameIndexDatVersion=102 MapShareSupportedProviders=203 CharacterSet=Latin-1
CURRENTLOCATION.DAT	Contiene l'ultima posizione del dispositivo.
CURRENTMAP.DAT	Contiene la mappa in uso corrente.
GPRSETTINGS.DAT	Contiene la configurazione GPRS (se presente)
SETTINGS.DAT	Contiene il nome e il MAC Address del telefono eventualmente collegato, la configurazione wireless, i dati del provider, i dati del telefono e dell'utente, se immessi (solo modelli GO)
GPRS.CONF	Contiene il PIN GPRS (se immesso) (solo modelli GO)
MAPSETTINGS.CFG	I file con l'estensione "CFG", come "mapsettings.cfg" o "nome_mappa.cfg" sono contenuti nelle cartelle delle rispettive mappe e contengono tutte le informazioni sui Preferiti, sugli itinerari seguiti, sugli indirizzi immessi, i punti di interesse memorizzati .
\CONTACTS\ CALLED.TXT	Contiene i i numeri telefonici chiamati dal telefono collegato a TomTom (solo modelli GO)

\CONTACTS\ CALLERS.TXT	Contiene i i numeri telefonici che hanno chiamato il telefono collegato a TomTom (solo modelli GO)
\CONTACTS\ CONTACTS.TXT	Contiene i numeri della rubrica telefonica del telefono collegato a Tomtom (solo modelli GO)
\CONTACTS\ INBOX.TXT	Contiene i testi dei messaggi ricevuti dal telefono collegato a TomTom (solo modelli GO)
\CONTACTS\ OUTBOX.TXT	Contiene i testi dei messaggi rinviati dal telefono collegato a TomTom (solo modelli GO)
NOMEFILE.ITI	Contiene gli itinerari memorizzati
TEMPORARY.ITI	Contiene gli itinerari non memorizzati con un nomefile

Si rendo noto infine che, a secondo del modello, alcuni file possono essere presenti o non presenti sul dispositivo.

Si riporta qui di seguito una tabella riassuntiva dei diversi file presenti sui differenti modelli.

	RECENT DESTINATION	BIF FILE	SETTING FILE	CALLED FILE	CALLS FILE	INBOX FILE	OUTBOX FILE
TOMTOM ONE REGIONAL	SI	SI	NO	NO	NO	NO	NO
TOMTOM ONE EUROPE	SI	SI	NO	NO	NO	NO	NO
TOMTOM GO 510	SI	SI	SI	SI	SI	SI	SI
TOMTOM GO 710/720/730/750/790	SI	SI	SI	SI	SI	SI	SI
TOMTOM GO 910//920/930	SI	SI	SI	SI	SI	SI	SI
TOMTOM NAVIGATOR 6	SI	SI	NO	NO	NO	NO	NO

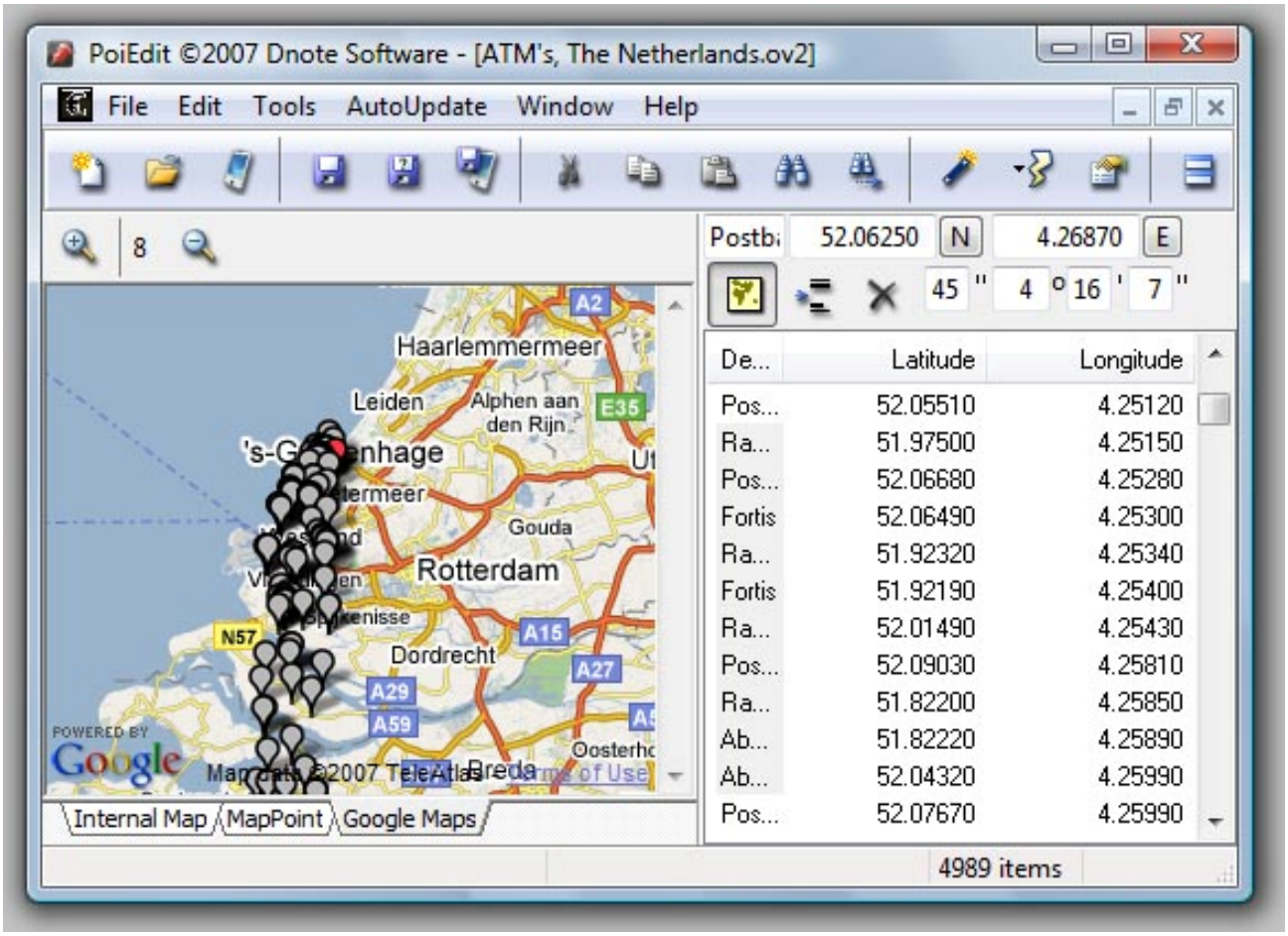
SOFTWARE DI ANALISI SPECIFICI PER TOMTOM

Esistono sul mercato diversi software commerciali che eseguono un'analisi mirata del contenuto dei soli file di navigazione contenuti all'interno di TomTom.

POIedit, tool gratuito per il S.O. Windows, è in grado di leggere il contenuto dei file DAT.

Assai interessante la sua funzione di individuazione e visualizzazione, sulle mappe fornitegli da GoogleMap (necessita di collegamento ad Internet per la visualizzazione), dell'esatta posizione degli indirizzi contenuti nel file "mapsettings.cfg".

La figura sottostante fornisce un esempio di localizzazione su mappa geografica degli indirizzi contenuti nel file "mapsettings.cfg".



BIBLIOGRAFIA

1. C.M. Colombini, Y. Corio, *La corretta gestione di un incidente informatico e alcune ipotesi di linee guida per le operazioni di forensics. La Dead Analysis*. White Paper, Corso di Perfezionamento in Computer Forensics e Investigazioni Digitali, AA 2007/2008.

2. B. Nutter , *Pinpointing TomTom location records: A forensic analysis.* 2008 Elsevier Ltd.

3. Peter Hannay, *A Methodology for the forensic acquisition of the TomTom One satellite navigation System – A research in progress*, Edith Cowan University, 2007.

4. A.K. Theiss, DD.CC. Yen, C.Y. Ku, *Global positioning systems: an analysis of applications, current development and future implementations*. Computer Standards & Interfaces, 2005.
5. SEC.AU, Edith Cowan University

6. ACPO (2003*). Good Practice Guide for Computer based Electronic Evidence 3.0*. Retrieved 16 Oct, 2007.

7. P. Hannay, *A Methodology for the Forensic Acquisition of the TomTom One Satellite Navigation System–A Research in Progress.* Paper presented at the 5th Australian Digital Forensics Conference, 2007.

8. A. K. Theiss, D. C. Yen, & Ku, *Global Positioning Systems: an analysis of applications.* 2005.

9. http://www.marcomattiucci.it.

10. http://ww.tomtom.com

11. http://www.GPSforensics.org

12. http://www.forensicswiki.org/wiki/GPS

13. http://www.symbian.com

14. http://www.samsung.com/global/business/semiconductor/productInfo.do?fmly_id=229&partnum=S3C2443

15. http://www.maerco.it/index.php/2007/01/03/open-tom-tomtom-opensource/

16. http://www.opentom.org/Main_Page

Un ringraziamento particolare al Magg. Marco Mattiucci, Comandante dell'RTI – Reparto Tecnologie Informatiche - RACIS Roma – Arma dei Carabinieri.