Università degli Studi di Salerno
Facoltà di Scienze MM.FF.NN.

GPS Forensic, un caso di studio: TomTom

Armando Faggiano
armando.faggiano@gmail.com

Ermanno Travaglino
ermanno.travaglino@gmail.com

Indice

La storia

GPS (Global Positioning System) è un sistema di posizionamento su base satellitare gestito dagli USA.

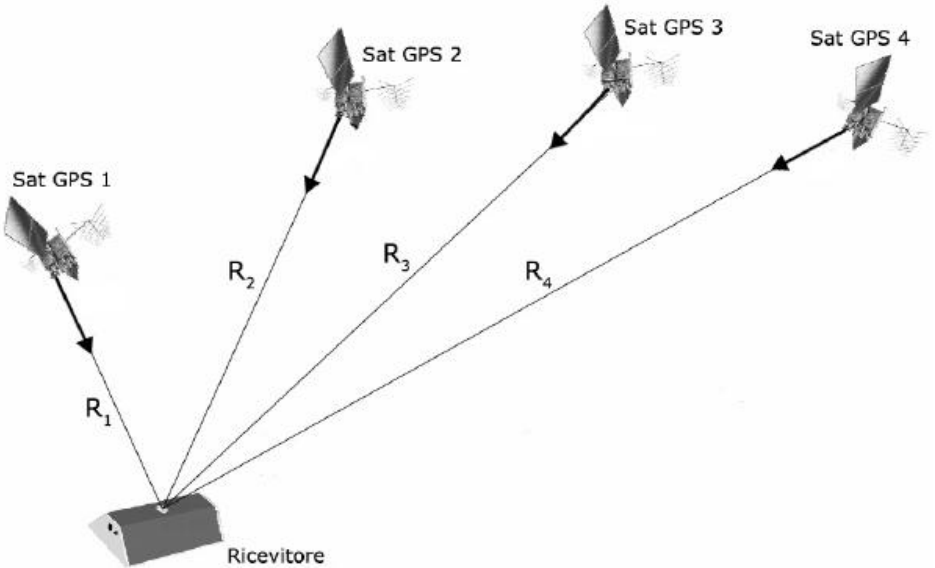
Anno 1991: USA aprono al mondo il servizio con il nome **SPS (Standard Positioning System)** per uso civile.

Anno 2003: Prende forma il progetto **Galileo** nell'UE.

Determinazione coordinate GPS

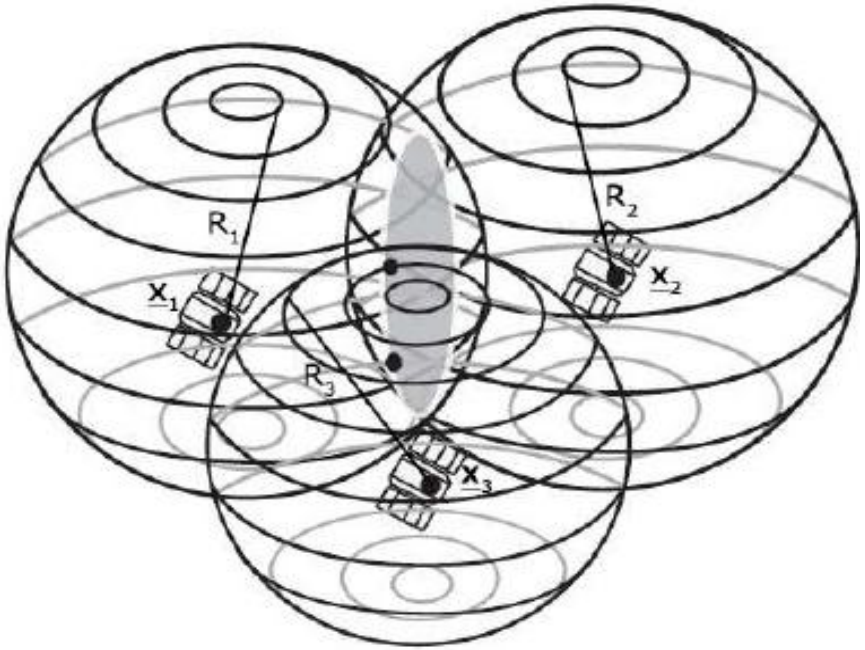
Informazioni presenti nei messaggi:

- Tempo di trasmissione
- Effemèridi (precise informazioni orbitali relative al satellite)
- Almanacco (salute del sistema e orbite di tutti i satelliti)



Determinazione coordinate GPS

Per ogni satellite individuato, il ricevitore traccia una sfera di raggio R con centro la posizione del satellite stesso. Si calcolano le intersezioni delle sfere e si ottiene la posizione del dispositivo.



Determinazione coordinate GPS

Un ricevitore GPS, utilizzando i messaggi ricevuti da un minimo di 3 satelliti, è in grado di determinare i tempi d'invio e poi le posizioni dei satelliti.

x, y e z rappresentano le componenti della posizione e t il tempo d'invio. Il messaggio generato dal satellite in un istante t_i arriva al ricevitore in un istante t_r, il tempo di propagazione è dato da $\Delta t = t_r - t_i$. Assumendo che il messaggio viaggi alla velocità della luce c, la pseudo-distanza è data da $\Delta t\ c$.

Gli orologi di satellite e ricevitore non è detto che siano sincronizzati, quindi con b rappresentiamo l'errore dell'orologio del ricevitore.

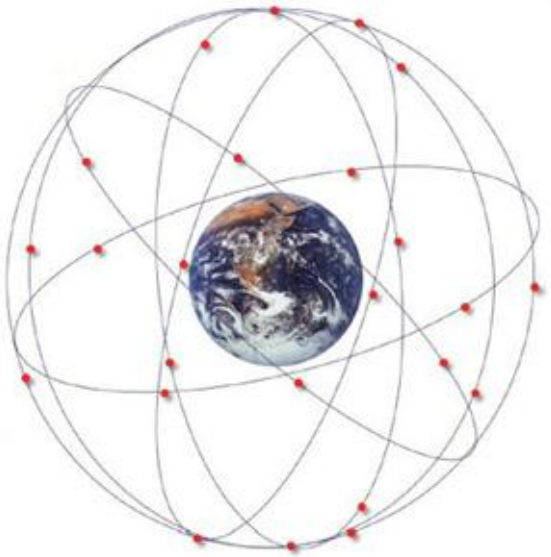
Le equazioni delle superfici delle sfere sono date da:

$$(x - x_i)^2 + (y - y_i)^2 + (z - z_i)^2 = ([t_r - t_i + b]c)^2$$

Struttura del sistema

Consiste in 32 satelliti in orbita MEO (Medium Earth Orbit)

- Disposti su 6 piani orbitali;
- Inclinati di 55° rispetto al piano equatoriale e di 60° tra di loro;
- Da ogni punto della terra sono visibili almeno 5 satelliti.



Indice

L’azienda: TomTom International BV

E’ una società olandese, nata nel 1991, che produce sistemi di navigazione satellitare per automobili, motoveicoli e smartphone.

- Dispositivi di navigazione con ricevitori GPS che utilizzano principalmente mappe digitali Tele Atlas (Whereis per l’Australia e GeoSmart per la Nuova Zelanda);
- Applicazioni per iPhone, iPad e WindowsMobile (ormai fuori produzione).

Dispositivo analizzato

TOMTOM START ITALIA

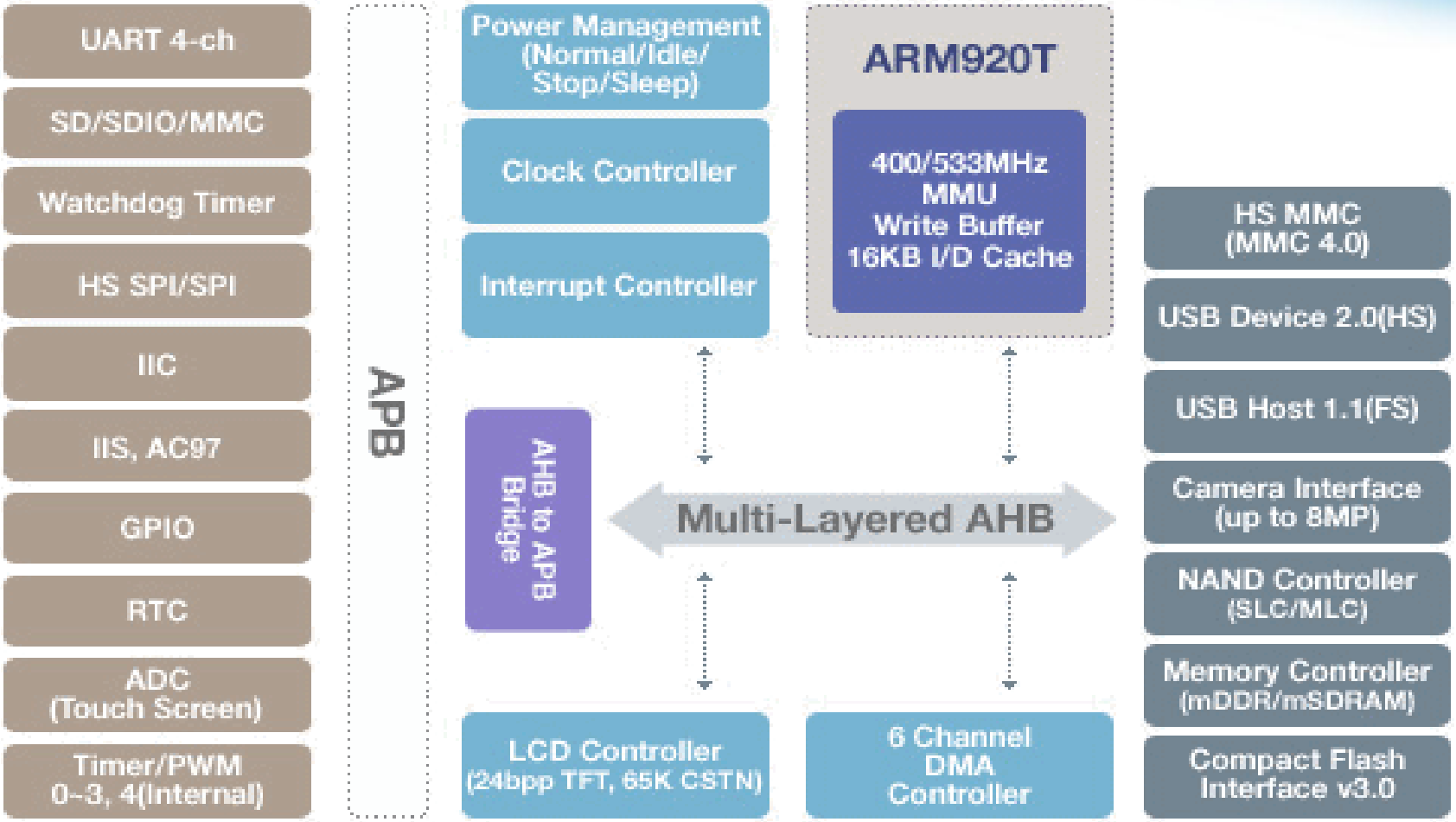
Possiede una memoria centrale e non necessita di una scheda SD esterna.

Funzionalità

Oltre alla costruzione del percorso, il dispositivo TomTom permette di:

- Memorizzare indirizzi e contatti;
- Itinerari costruiti;
- Memorizzare l'Home location;
- Memorizzare punti di interesse.

Architettura generica dispositivo TomTom

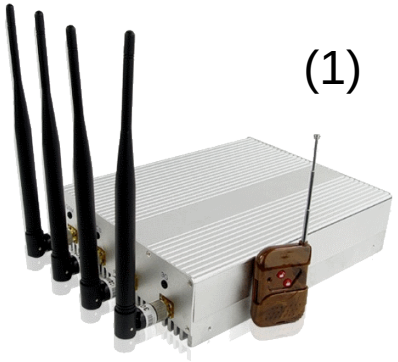


Indice

Best practices per la copia forense

- Best practices [Mattia Epifani]:
  - Isolamento del dispositivo
    - Jammer (1)
    - Gabbia di Faraday (2)
  - Sincronizzazione della macchina (che acquisirà i dati) con un server NTP noto
  - Accesso alla memoria del dispositivo TomTom in sola lettura
  - Verifica conformità della copia effettuata

(1)



(2)

Software utilizzati per la copia forense

- Distribuzione CAINE 2.0 (kernel 2.6.32-24)
  - Ideata da Giancarlo Giustini, Centro di Ricerca Interdipartimentale per la Sicurezza (CRIS) dell'Università di Modena e Reggio Emilia.
  - Basata su Ubuntu 10.04 LTS
  - Tool AIR

Procedimento per effettuare una copia forense

1) Connessione del dispositivo
2) Montaggio del file system INTERNAL
3) Copia forense con il tool *AIR*
4) Eject file system INTERNAL
5) Disconnessione del dispositivo dal PC

La conseguenza del quarto passo è la partenza del dispositivo in modalità utente...

File alterati durante la modalità utente

Connettendo nuovamente il dispositivo, i file alterati risulteranno:

- *CurrentMap.dat*: contiene la mappa in uso corrente.
- *ttgo.bif*: contiene le informazioni relative al dispositivo tra cui modello, numero di serie, lingua, mappa corrente, base corrente, voce ecc..
- */itn/temporary.iti*: contiene gli itinerari non memorizzati con un nome file (itinerari di default).
- *settings.dat*: contiene il nome ed il mac address del telefono (Bluetooth) eventualmente collegato, la configurazione del provider telefonico, i dati del telefono e dell'utente se immessi (solo per modelli TomTom GO).
- *UserPatch.dat*: contiene le eventuali modifiche effettuate dall'utente su determinati punti stradali condivise tra i vari dispositivi.

Per i primi due file viene modificato soltanto il timestamp, mentre per gli altri tre file viene modificato anche il contenuto.

Procedimento per una copia forense ripetibile

1) Connessione del dispositivo
2) Montaggio del file system INTERNAL
3) Copia forense con il tool *AIR*
4) **Unmount del file system INTERNAL**
5) **Spegnimento del dispositivo**
6) **Disconnessione del dispositivo dal PC**

Video dimostrativo

Copia forense della memoria flash

Dispositivo */dev/mmcblk1*

Contenuto della memoria flash

Lo scopo di alcuni file sulla partizione NGFFS (Next Generation Flash File System, è un driver del file system per kernel Linux) è noto.

- "*bootver*" memorizza la versione del bootloader del dispositivo.
- "*cal*" memorizza i dati di calibrazione del touch screen.
- "*id*" memorizza l'id del dispositivo o il numero di serie.
- "*mac*" memorizza l'indirizzo mac del bluetooth.
- "*imei*" si pensa contenga l'International Mobile Equipment Identity (IMEI) di un dispositivo con funzionalità GSM (non verificato).
- "*btcal*" contenga i dati di calibrazione del bluetooth.

Indice

BusyBox

Presente di default in ver. 1.00

E’ stata inserita la BusyBox 1.92

- compilata per il processore ARM926 presente nel dispositivo.
- contiene comandi per l’analisi forense (dd).

Analisi forense

- MapSettings.cfg
- ttgo.bif
- settings.dat
- \contacts\:
  - called.txt
  - callers.txt
  - contacts.txt
  - inbox.txt
  - outbox.txt

Non presenti su TomTom Start

MapSettings.cfg

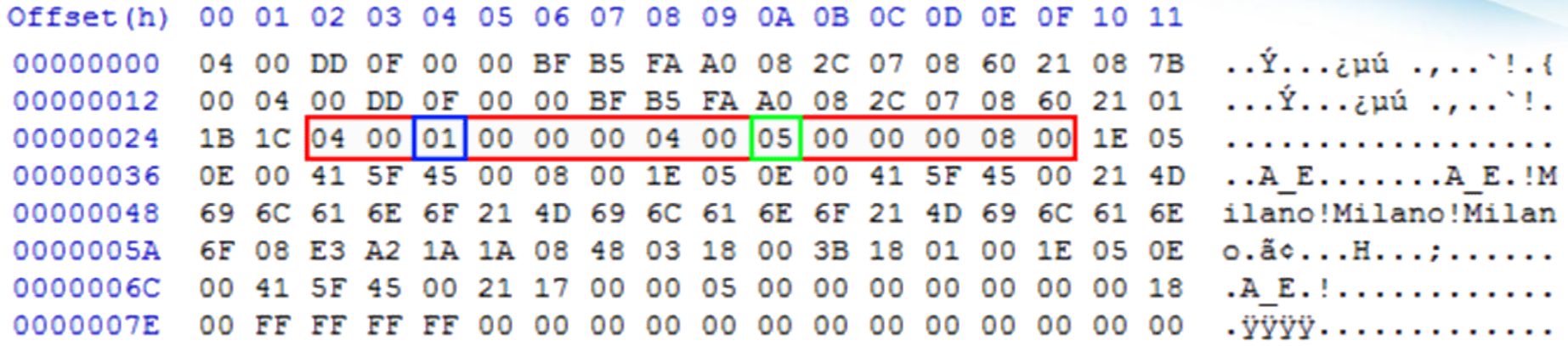
Contenuto del file:

- Indirizzi inseriti (preferiti);
- Indirizzi parzialmente inseriti;
- Punti di interesse (POI).

Indice

Struttura del record

- Record di lunghezza variabile



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	
00000000	04	00	DD	0F	00	00	BF	B5	FA	A0	08	2C	07	08	60	21	08	7B	..Ý...¿µú .,..`!.{
00000012	00	04	00	DD	0F	00	00	BF	B5	FA	A0	08	2C	07	08	60	21	01	...Ý...¿µú .,..`!.
00000024	1B	1C	04	00	01	00	00	00	04	00	05	00	00	00	08	00	1E	05	.....
00000036	0E	00	41	5F	45	00	08	00	1E	05	0E	00	41	5F	45	00	21	4D	..A_E.....A_E.!M
00000048	69	6C	61	6E	6F	21	4D	69	6C	61	6E	6F	21	4D	69	6C	61	6E	ilano!Milano!Milan
0000005A	6F	08	E3	A2	1A	1A	08	48	03	18	00	3B	18	01	00	1E	05	0E	o.ã¢...H...;.....
0000006C	00	41	5F	45	00	21	17	00	00	05	00	00	00	00	00	00	00	18	.A_E.!.....
0000007E	00	FF	FF	FF	FF	00	00	00	00	00	00	00	00	00	00	00	00	00	.ÿÿÿÿ.....

Valori del byte XX (precisione della location)

Byte XX	Precisione
01	Centro città
02	Incrocio specifico
03	Numero civico o edificio
04	Ovunque su una strada

Valori del byte YY (tipo della location)

Byte YY	Tipo del record
01	Inserito tramite mappa o codice postale
03	Preferito
04	Home location
05	Inserito tramite l'indirizzo
06	Inserito tramite POI
07	Inizio dell'ultima rotta calcolata

Primo e secondo set di coordinate

```
00000030  00 00 08 00 0D 8B 16 00 E6 1B 3E 00 08 00 04 8B 16 00 EB 1B 3E 00 25 50  .....‹..æ.>....‹..ë.>.%P
00000048  65 6C 6C 65 7A 7A 61 6E 6F 26 56 69 61 20 46 69 6C 61 6E 64 61 35 56 69  ellezzano&Via Filanda5Vi
00000060  61 20 46 69 6C 61 6E 64 61 20 33 33 2C 20 50 65 6C 6C 65 7A 7A 61 6E 6F  a Filanda 33, Pellezzano
00000078  08 F7 BA 0A 21 00 00 C0 1B 08 48 03 18 00 7A AD 2C 00 FF 8A 16 00 22 1C  .÷°.!..À..H...z.,.ÿŠ..".
```

Longitudine espressa in formato Little-endian — `0D 8B 16`

Convertita in formato Big-endian — `16 8B 0D`

Convertita da esadecimale in decimale e divisa per 100.000 — 14,77389

Per la Latitudine viene effettuato lo stesso procedimento, ottenendo 40,70374

Indice

Label per l’indirizzo

Segue le coordinate ed è costituita da tre parti:

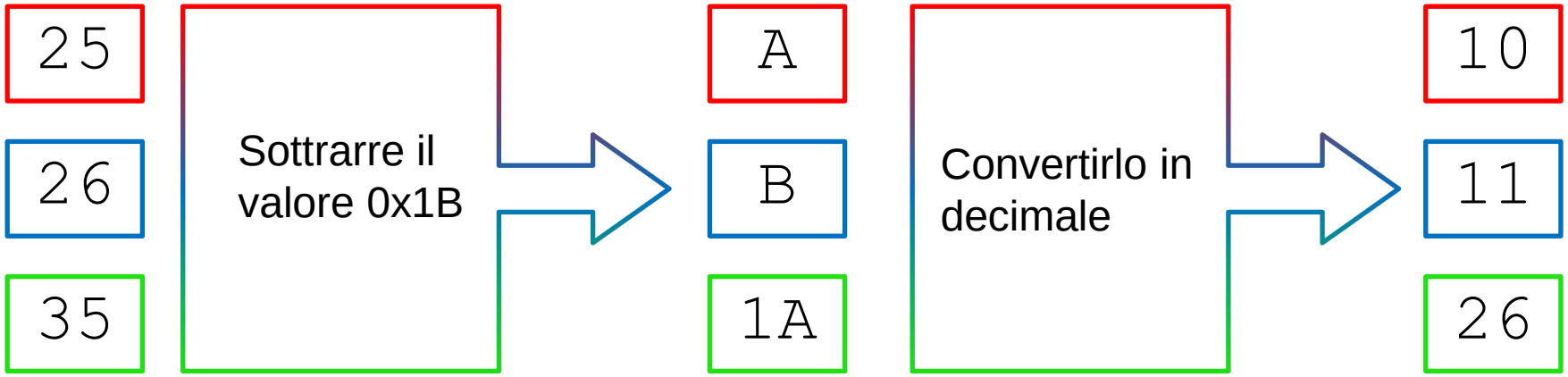
- Le prime due parti contengono l’inizio del percorso calcolato
- La terza parte contiene il nome del POI

```
16 00 EB 1B 3E 00 25 50 65 6C 6C 65 7A 7A 61 6E  ..ë.>.%Pellezzan
6F 26 56 69 61 20 46 69 6C 61 6E 64 61 35 56 69  o&Via Filanda5Vi
61 20 46 69 6C 61 6E 64 61 20 33 33 2C 20 50 65  a Filanda 33, Pe
6C 6C 65 7A 7A 61 6E 6F 08 F7 BA 0A 21 00 00 C0  llezzano.÷º.!..À
```

Label per l'indirizzo

Determinazione lunghezza campi

```
16 00 EB 1B 3E 00 25 50 65 6C 6C 65 7A 7A 61 6E   ..ë.>.%Pellezzan
6F 26 56 69 61 20 46 69 6C 61 6E 64 61 35 56 69   o&Via Filanda5Vi
61 20 46 69 6C 61 6E 64 61 20 33 33 2C 20 50 65   a Filanda 33, Pe
6C 6C 65 7A 7A 61 6E 6F 08 F7 BA 0A 21 00 00 C0   llezzano.÷º.!..À
```



Indice

Ultima posizione GPS rilevata

L’idea di base è stata quella di compiere più rilevazioni di posizioni GPS vicine fra loro (coordinate indicate dal display del dispositivo). Tale procedimento è formato dai seguenti passi:

- Reset del dispositivo TomTom (per avere il dispositivo con le impostazioni di fabbrica).
- Posizionamento fisico del dispositivo TomTom in un punto di coordinate noto.
- Rilevamento dei dati GPS presenti sull’interfaccia grafica del dispositivo TomTom e salvataggio del file *MapSettings.cfg* su un PC.
- Ripetizione dei passi precedenti.

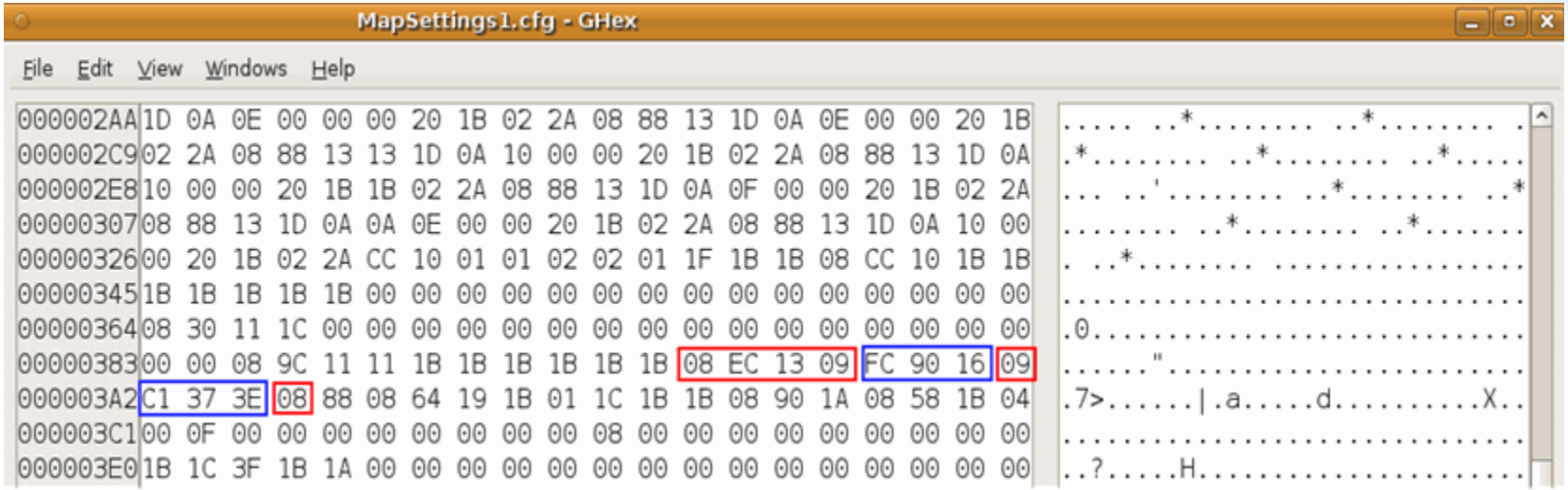
Ultima posizione GPS rilevata

Analizzando i diversi file MapSettings.cfg salvati, utilizzando il comando compare, è emerso:

cmp -l /…/MapSettings1.cfg /…/MapSettings2.cfg

Offset (byte)	MapSettings1 (valore)	MapSettings2 (valore)
927	374	35
928	220	221
931	301	315

MapSettings1.cfg



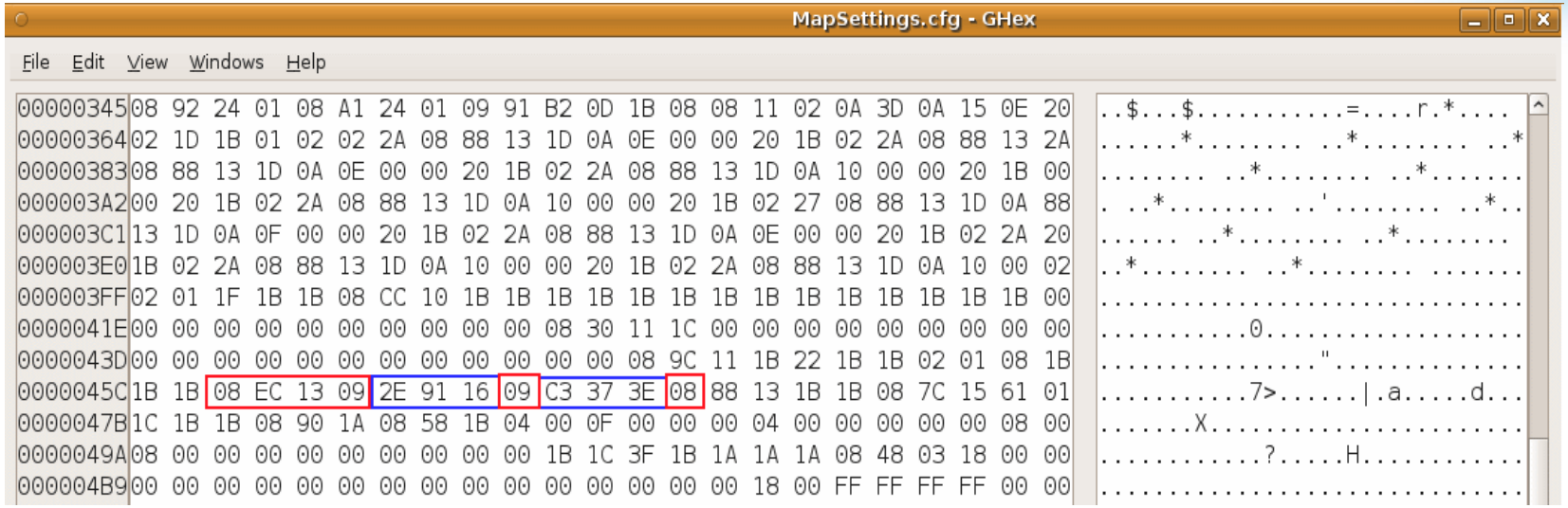
Little-endian Big-endian

Da Hex a Dec e divisione per 100.000

Longitudine `FC 90 16` `16 90 FC` → 14,78908

Latitudine `C1 37 3E` `3E 37 C1` → 40,77505

MapSettings2.cfg



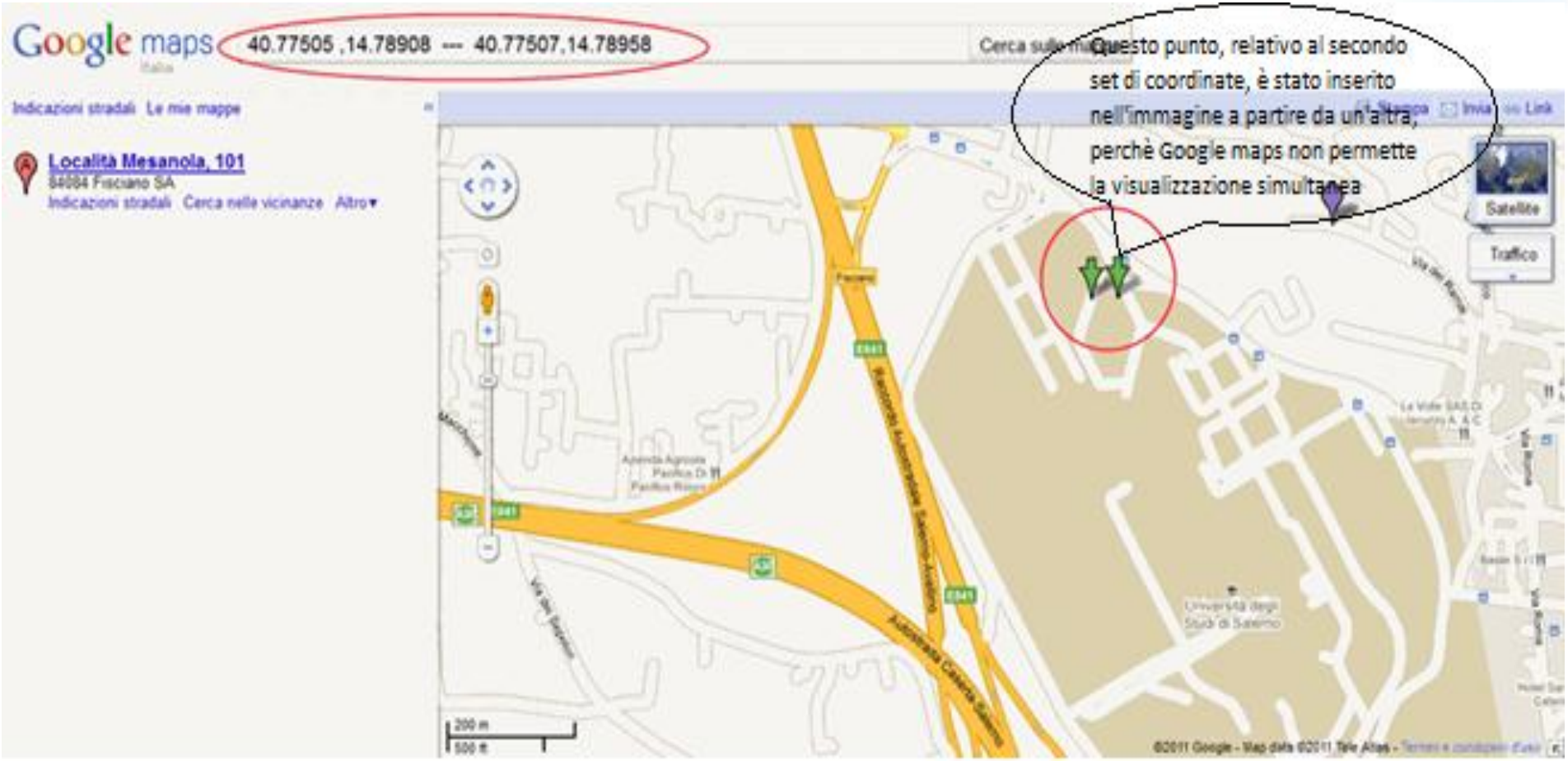
Little-endian Big-endian

Da Hex a Dec e divisione per 100.000

Longitudine `2E 91 16` `16 91 2E` → 14,78958

Latitudine `C3 37 3E` `3E 37 C3` → 40,77507

Ultima posizione GPS rilevata



Indice

Viaggi effettuati

Quando viene effettuato un viaggio il dispositivo TomTom salva i dati in un file di log.

Programma dichiarato per la "Raccolta statistiche di utilizzo anonime"

Qualora, all’avvio del dispostivo, si accetti tale condizione nella directory */mnt/sdcard/statdata/* apparirà il file Allowtrip.dat e nel file Triplog-aaaa-mm-gg.dat verranno salvati i file relativi ai viaggi effettuati, altrimenti sarà presente il file Disallowtrip.dat.

Precisazioni file Triplog

File utilizzati per il servizio IQ Routes (presentato nel Marzo del 2008 ad Hannover) che calcola la velocità media reale su oltre dieci miliardi di Km analizzati.

27 Aprile 2011: acquisto delle informazioni dalla polizia olandese (fonte "Algemeen Dagblad").

Analisi Triplog

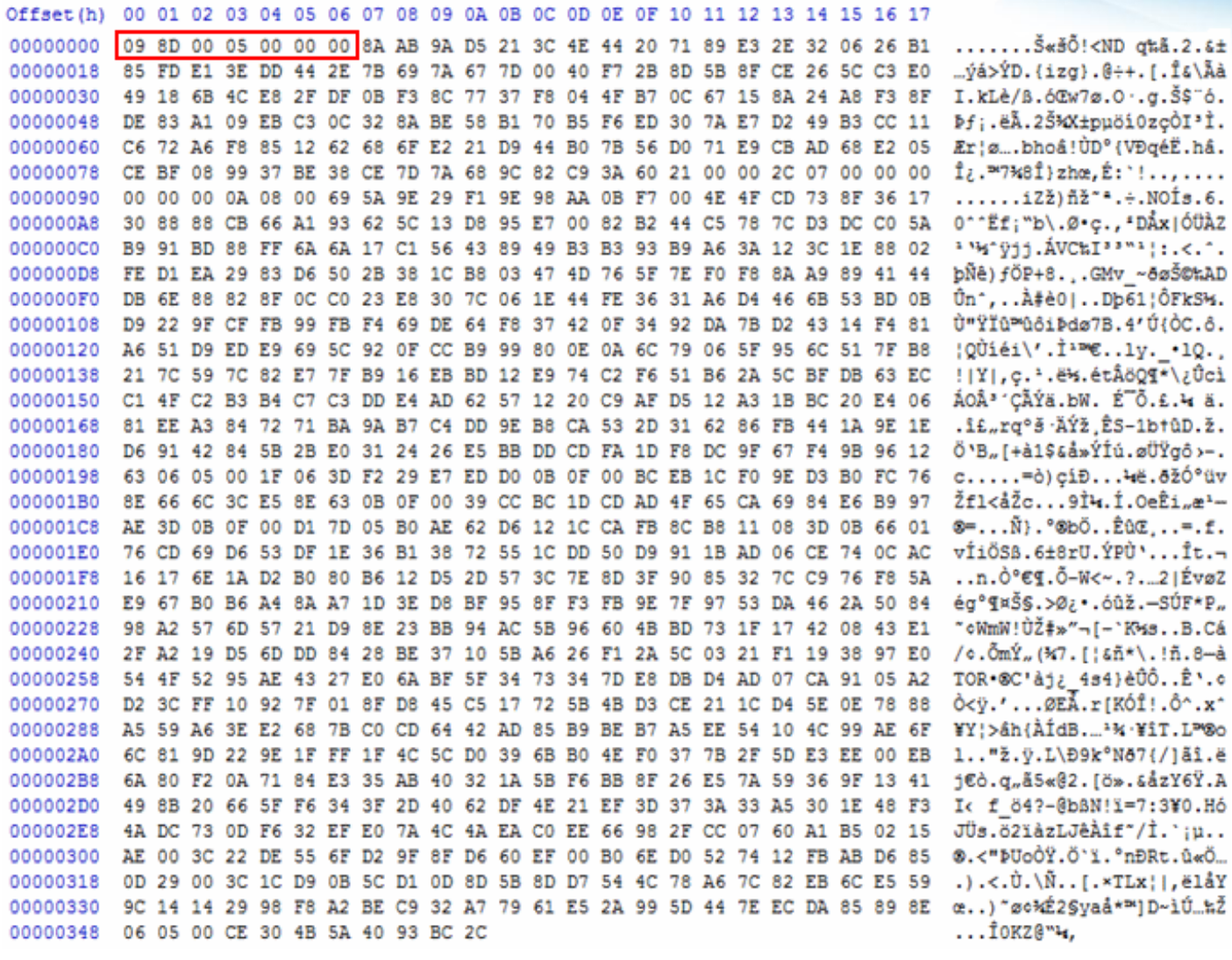
I file di log vengono salvati nella memoria interna (directory /mnt/statdata/Triplog-aaaa-mm-gg.dat).

Nel caso si effettuino piu viaggi verranno sovrascritti.

L'operazione di scrittura del file *Triplog* viene eseguita durante il viaggio.

Fin dall'inizio della sperimentazione questo file è parso di natura crittografica (non compressa).

File triplog



```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17
00000000   09 8D 00 05 00 00 00 8A AB 9A D5 21 3C 4E 44 20 71 89 E3 2E 32 06 26 B1
00000018   85 FD E1 3E DD 44 2E 7B 69 7A 67 7D 00 40 F7 2B 8D 5B 8F CE 26 5C C3 E0
00000030   49 18 6B 4C E8 2F DF 0B F3 8C 77 37 F8 04 4F B7 0C 67 15 8A 24 A8 F3 8F
00000048   DE 83 A1 09 EB C3 0C 32 8A BE 58 B1 70 B5 F6 ED 30 7A E7 D2 49 B3 CC 11
00000060   C6 72 A6 F8 85 12 62 68 6F E2 21 D9 44 B0 7B 56 D0 71 E9 CB AD 68 E2 05
00000078   CE BF 08 99 37 BE 38 CE 7D 7A 68 9C 82 C9 3A 60 21 00 00 2C 07 00 00 00
00000090   00 00 00 0A 08 00 69 5A 9E 29 F1 9E 98 AA 0B F7 00 4E 4F CD 73 8F 36 17
000000A8   30 88 88 CB 66 A1 93 62 5C 13 D8 95 E7 00 82 B2 44 C5 78 7C D3 DC C0 5A
000000C0   B9 91 BD 88 FF 6A 6A 17 C1 56 43 89 49 B3 B3 93 B9 A6 3A 12 3C 1E 88 02
000000D8   FE D1 EA 29 83 D6 50 2B 38 1C B8 03 47 4D 76 5F 7E F0 F8 8A A9 89 41 44
000000F0   DB 6E 88 82 8F 0C C0 23 E8 30 7C 06 1E 44 FE 36 31 A6 D4 46 6B 53 BD 0B
00000108   D9 22 9F CF FB 99 FB F4 69 DE 64 F8 37 42 0F 34 92 DA 7B D2 43 14 F4 81
00000120   A6 51 D9 ED E9 69 5C 92 0F CC B9 99 80 0E 0A 6C 79 06 5F 95 6C 51 7F B8
00000138   21 7C 59 7C 82 E7 7F B9 16 EB BD 12 E9 74 C2 F6 51 B6 2A 5C BF DB 63 EC
00000150   C1 4F C2 B3 B4 C7 C3 DD E4 AD 62 57 12 20 C9 AF D5 12 A3 1B BC 20 E4 06
00000168   81 EE A3 84 72 71 BA 9A B7 C4 DD 9E B8 CA 53 2D 31 62 86 FB 44 1A 9E 1E
00000180   D6 91 42 84 5B 2B E0 31 24 26 E5 BB DD CD FA 1D F8 DC 9F 67 F4 9B 96 12
00000198   63 06 05 00 1F 06 3D F2 29 E7 ED D0 0B 0F 00 BC EB 1C F0 9E D3 B0 FC 76
000001B0   8E 66 6C 3C E5 8E 63 0B 0F 00 39 CC BC 1D CD AD 4F 65 CA 69 84 E6 B9 97
000001C8   AE 3D 0B 0F 00 D1 7D 05 B0 AE 62 D6 12 1C CA FB 8C B8 11 08 3D 0B 66 01
000001E0   76 CD 69 D6 53 DF 1E 36 B1 38 72 55 1C DD 50 D9 91 1B AD 06 CE 74 0C AC
000001F8   16 17 6E 1A D2 B0 80 B6 12 D5 2D 57 3C 7E 8D 3F 90 85 32 7C C9 76 F8 5A
00000210   E9 67 B0 B6 A4 8A A7 1D 3E D8 BF 95 8F F3 FB 9E 7F 97 53 DA 46 2A 50 84
00000228   98 A2 57 6D 57 21 D9 8E 23 BB 94 AC 5B 96 60 4B BD 73 1F 17 42 08 43 E1
00000240   2F A2 19 D5 6D DD 84 28 BE 37 10 5B A6 26 F1 2A 5C 03 21 F1 19 38 97 E0
00000258   54 4F 52 95 AE 43 27 E0 6A BF 5F 34 73 34 7D E8 DB D4 AD 07 CA 91 05 A2
00000270   D2 3C FF 10 92 7F 01 8F D8 45 C5 17 72 5B 4B D3 CE 21 1C D4 5E 0E 78 88
00000288   A5 59 A6 3E E2 68 7B C0 CD 64 42 AD 85 B9 BE B7 A5 EE 54 10 4C 99 AE 6F
000002A0   6C 81 9D 22 9E 1F FF 1F 4C 5C D0 39 6B B0 4E F0 37 7B 2F 5D E3 EE 00 EB
000002B8   6A 80 F2 0A 71 84 E3 35 AB 40 32 1A 5B F6 BB 8F 26 E5 7A 59 36 9F 13 41
000002D0   49 8B 20 66 5F F6 34 3F 2D 40 62 DF 4E 21 EF 3D 37 3A 33 A5 30 1E 48 F3
000002E8   4A DC 73 0D F6 32 EF E0 7A 4C 4A EA C0 EE 66 98 2F CC 07 60 A1 B5 02 15
00000300   AE 00 3C 22 DE 55 6F D2 9F 8F D6 60 EF 00 B0 6E D0 52 74 12 FB AB D6 85
00000318   0D 29 00 3C 1C D9 0B 5C D1 0D 8D 5B 8D D7 54 4C 78 A6 7C 82 EB 6C E5 59
00000330   9C 14 14 29 98 F8 A2 BE C9 32 A7 79 61 E5 2A 99 5D 44 7E EC DA 85 89 8E
00000348   06 05 00 CE 30 4B 5A 40 93 BC 2C
```

Analizzando il file con un editor esadecimale è emersa una sola parte comune.

Principale fonte di software

Si è deciso di effettuare l'hacking del dispositivo per provare diversi tipologie di attacco.

Si è fatto riferimento alla comunità OpenTom (www.opentom.org) che fornisce:

- Software aggiuntivi/alternativi
  - TTconsole
- Bootloader

Hacking del dispositivo

Una volta scaricato il software da OpenTom e inserito nel dispositivo, si va in Impostazioni Avanzate dove apparirà quest'icona. Una volta cliccato…

Hacking del dispositivo

La tastiera è risultata scomoda da utilizzare, così si è cercato il file da modificare per inserire i comandi lanciando direttamente Text Console

Ttconsole-wrapper

Tale file si trova in /bin

```
options="--keyboardlayout_it --bigfont" # --bigkeys"
 # usually you want this on Systems with Navcore 8.xxx and 9.xxx

dodog=yes
#first do some settings like the PWD, HOME and PATH
cd /mnt/sdcard

export PATH=$PATH:/mnt/sdcard/bin
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/mnt/sdcard/lib
export HOME=/mnt/sdcard/
export TERMINFO=/mnt/sdcard/lib/terminfo
export TERMCAP=/mnt/sdcard/lib/termcap

if [ "$dodog" = "yes" ]
then
kill -STOP `pidof ttn`
dogfeed &
fi

# now start the console application
TTconsole  $options
```

Copia logica root

options="--keyboardlayout_it --bigfont" # --bigkeys"

usually you want this on Systems with Navcore 8.xxx and 9.xxx

…

Ls -l -R /

…

cp -R / /mnt/sdcard/copia

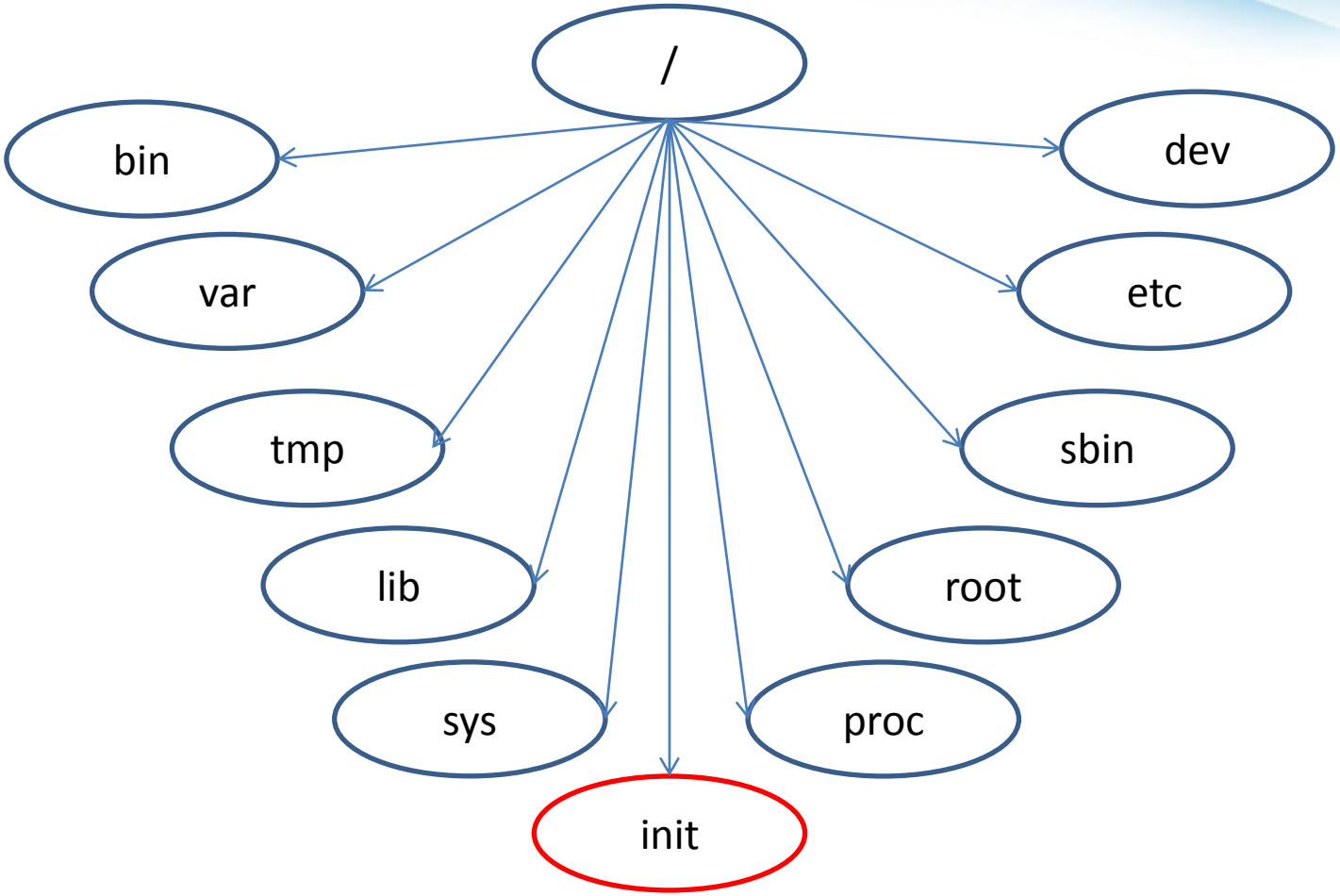
now start the console application

TTconsole $options

Contenuto root

Directory

- bin
- dev
- etc
- lib
- proc
- root
- sbin
- sys
- tmp
- var



File

- init

Componenti file /init

1) Configurazione delle path

2) Dichiarazione ed implementazione delle funzioni

3) Start-up

4) Main-loop

File /init - Configurazione path

Il dispositivo andrà a cercare le path da allocare, tra cui la sdmount, le applicazioni, i tools e il log file della console.

Porzione di codice

```
…
devbase="/dev"
sdmnt="/mnt/sdcard"
mvmnt="/mnt/movinand"
carlinkapp="carlinkd"
carlinkdir="/bin"
ttnapp="ttn"
ttntooldir="ttntools"
ttntool="ttntool.sh"
ttndir="/bin“
…
```

File /init - Funzioni

mount_sys()	Monta il sistema
mount_flash()	Monta la memoria flash
check_gps_receiver()	Verifica il tipo di ricevitore GPS
start_gps()	Avvia il firmware del GPS
start_ttn()	Avvia i servizi principali del dispositivo
start_shell()	Avvia la shell
start_navigator()	Invoca tutte le funzioni per la navigazione

File /init - Start up e main loop

3) Start-up

- Viene mostrata la versione
- Monta il sistema
- Inizializzazione i file di log

4) Main-loop

- Monta la memoria interna SD
- Avvia la modalità navigazione
- Unmount allo spegnimento

Sostituzione pipe

Vengono create due pipe:

/var/run/gpspipe

- presente all'avvio del dispositivo
- alto tasso di aggiornamento

/var/run/gpsfeed

- presente dopo l'avvio di *navcore*
- fornisce l'output in ritardo

E' stata esaminata la pipe /var/run/gpspipe…

Contenuto pipe /var/run/gpsfeed

options="--keyboardlayout_it --bigfont" # --bigkeys"

usually you want this on Systems with Navcore 8.xxx and 9.xxx

…

cat * /var/run/gpsfeed >> /mnt/sdcard/nmea/log_gpsfeed.txt*

now start the console application

TTconsole $options

Dati ricevuti dai satelliti GPS

Frammento del contenuto del file log_gpsfeed.txt
(le informazioni sono espresse in formato NMEA 0183)

[.....]
$GPRMC,152826.00,A,4046.471896,N,01447.361011,E,000.0,000.0,080711,,,E*5E
$GPGGA,152827.00,4046.479684,N,01447.359100,E,1,06,3.0,290.4,M,42.0,M,,*65
$PGLOR,STA,152827.00,0.443,0.000,-359,1,30,1,PWR,D*26
$PGLOR,SAT,25,047,1F,29,037,17,12,044,1F,39,034,3,31,042,1F,09,022,17,27,027,17,02,046,13*64
$PGLOR,SIO,TxERR,1,RxERR,0,TxCNT,244,RxCNT,1772,DTMS,926,DTIN,2,DTOUT,166*76
$GPGSV,3,1,11,25,71,348,47,29,64,241,37,12,52,075,44,39,41,164,34*71
$GPGSV,3,2,11,31,27,315,42,09,19,154,22,27,09,152,27,02,01,000,46*71
$GPGSV,3,3,11,33,33,221,,40,21,119,,04,05,034,*40
$GPGSA,A,3,09,12,25,27,29,31,,,,,,,2.3,1.6,1.7*33
$PGLOR,FIX,1.0*3°
[.....]

Campo GPRMC

$GPRMC,152826.00,A,4046.471896,N,01447.361011,E,010.3,000.0,080711,,,E*5E

152826.00	Orario 15:28:26 UTC
A	Stato A=active or V=Void.
4046.471896,N	Latitudine 40 gradi, 46 primi, 28 secondi, N
01447.361011,E	Longitudine 14 gradi, 47 primi, 21 secondi, E
010.3	Velocità espressa in nodi
000.0	Angolo espresso in gradi
080711	data – 8 Luglio 2011
‘ ’E	Variazione magnetica Est/Ovest
*5E	Checksum CRC32

Calcolo del CRC32

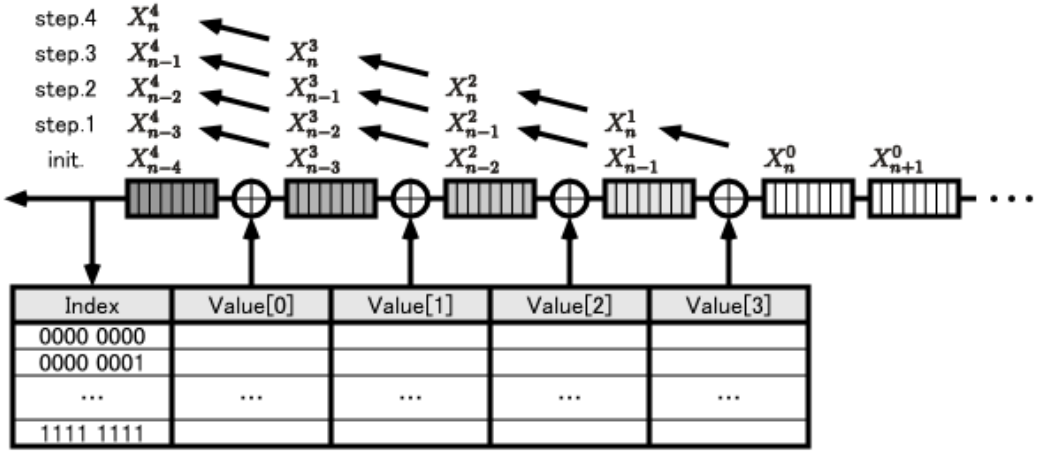
$PGLOR,FIX,1.0 * 3E <-- CRC32

Interpretazione esadecimale della riga.

HEX --> 24 50 47 4C 4F 52 2C 46 49 58 2C 31 2E 30 2A 33 45 (2A 33 45 --> * 3E)

XOR tra i valori che compongono la riga ad esclusione dei simboli $ e *.

XOR --> 50 xor 47 xor 4C xor 4F xor 52 xor 2C xor 46 xor 49 xor 58 xor 2C xor 31 xor 2E xor 30 = 3E !



Ricerca processo di scrittura

 # grep -lir "triplog" /*

Triplice obiettivo:

1) Ottenere il file in chiaro
2) Debuggare il software
3) Riferimenti alla chiave

Ottenuto riscontro nel file
/bin/ttn

Analisi file /bin/ttn

Provato disassemblaggio

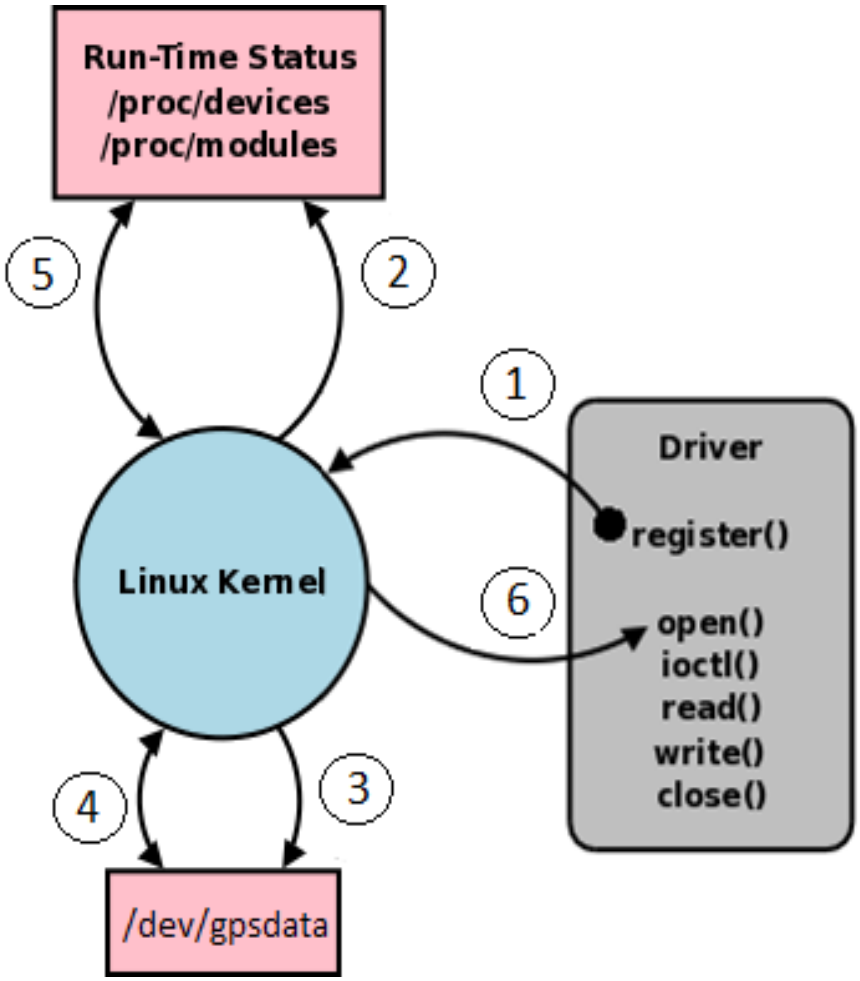
Contenuto */bin/ttn* con *Ghex*

triplog-%04d-%02d-%02d.dat → xxxxlog-%04d-%02d-%02d.dat

26CTripEncryptionBlowFishRSA....23CTripEncryptionBlowFish...23CTripEncryptionStrategy

13CTripRecorder.%02d:%02d:%02d..(?).%s,%s,%s,%s,%s,%s,%s,%s,%s,%s,%s,%s,%s,%s,%s,%s,%s

Analisi file system /proc



Questo diagramma mostra come avviene il riconoscimento (fasi 1-3) e l'iterazione di una periferica hardware (fasi 4-6) con il kernel.
Nelle prime 3 fasi viene mappato il dispositivo:
1. Viene caricato il modulo del kernel.
2. Vengono aggiornate le variabili runtime (/proc/devices, /proc/modules).
3. Viene creato il device file (/dev/gpsdata) con il tipo appropriato e gli vengono assegnati i riferimenti major e minor.
Nelle altre 3 fasi avviene l'iterazione:
4. Viene identificato il tipo di dispositivo e i riferimenti minor e major (ls -l /dev).
5. Vengono identificati i moduli associati al device file.
6. Il controllo viene trasferito alla funzione scelta nel driver.

Indice

1. Il sistema GPS
2. Il dispositivo TomTom
3. La copia forense
4. L'analisi delle informazioni
    1. Punti di interesse
    2. Label per l'indirizzo
    3. Ultima posizione GPS rilevata
    4. Triplog
5. Conclusioni e sviluppi futuri

Conclusioni

- ✓ **Reso la copia forense ripetibile**
- ✓ **Individuato l'ultima posizione GPS rilevata**
- x **File triplog**

Sviluppi futuri

- Analisi della memoria RAM del dispositivo (JTAG)
- Analisi di un dispositivo TomTom con Bluetooth
- Individuare i riferimenti (minor e major) nel kernel specifici del device */dev/gpsfeed* per condurre un attacco di tipo known-plain-text al file triplog.

Riferimenti

- GPS, Wikipedia (http://en.wikipedia.org/wiki/Global_Positioning_System).
- TomTom, Wikipedia (http://en.wikipedia.org/wiki/TomTom).
- Colombini Maria Clara - Experimental Testing of a Forensic Analysis Method on the TomTom GPS Navigation Device, April 2009 (http://www.iisfa.net/index.php?option=com_docman&task=doc_download&gid=19&Itemid=40).
- Mattia Epifani - Digital Evidence: dall'hard disk ai social network.
- OpenTom (http://www.opentom.org/Main_Page).
- Beverley Nutter - Pinpointing TomTom location records: A forensic analysis, Digital Investigation, Volume 5, Issues 1–2, September 2008, Pages 10-18, ISSN 1742-2876, 10.1016/j.diin.2008.06.003. (http://www.sciencedirect.com/science/article/pii/S1742287608000479).
- AD - TomTom tipt politie over verkeersmisbruik, 27 April 2011. (http://www.ad.nl/ad/nl/5597/Economie/article/detail/2426526/2011/04/27/TomTom-tipt-politie-over-verkeersmisbruik.dhtml).
- Van Eijk Onno & Roeloffs Mark - Forensic acquisition and analysis of the random access memory of tomtom GPS navigation systems, Digital Investigation 2010, Volume 6 (3-4), 179-188. (http:/www.sciencedirect.com/science/article/pii/S1742287610000137).

GRAZIE PER L’ATTENZIONE