



Thuraya Monitoring System

Thuraya Monitoring System

1- The Thuraya Personal Satellite Communications System

The Thuraya network has been in operation since early 2001, and is currently based on the Thuraya-2 geostationary satellite in an inclined orbit at a longitude of approximately 44° East. The Thuraya system provides telecommunications coverage to Europe, North, Central and some parts of Southern Africa, the Middle East, West and Central Asia, and the Asian Subcontinent, including more than 110 countries. Using a reduced capacity Thuraya-1 satellite at 98° East, provides some areas of the Far-East. In January 2007 the Thuraya-3 satellite was launched into the current location of the Thuraya-1 satellite, this new satellite has extended the coverage area of the Thuraya network to areas of Central and Eastern Russia and the Far East, including the eastern and south-eastern areas of mainland Asia, Japan, Taiwan, Malaysia, Indonesia, Brunei, the Philippines and Papua New Guinea.



Figure 1 – Map Showing Current Commercial Coverage from the Thuraya-2 Satellite

Since its introduction, the Thuraya system has proven to be extremely popular and exceeded the 150,000 subscriber barrier by the mid-2003, and it is estimated to currently have in the region of 340,000 subscribers. Thuraya forecast that they will ultimately achieve 1.75 million subscribers. One of its main appeals is to people living or traveling in the remote areas of Africa, the Middle East and Asia, where terrestrial infrastructure is not in place. The Thuraya network is designed to support 13,750 simultaneous telephone calls, and in some countries typical call levels are known to exceed 2,000 calls per hour.

2- The Strategic Thuraya Monitoring System

2.1- Principles of the Strategic Thuraya Monitoring System Operation

The strategic Thuraya Monitoring System (TMS) offered by TRL is designed to passively intercept downlinks from the Thuraya satellite at C-Band and L-Band.

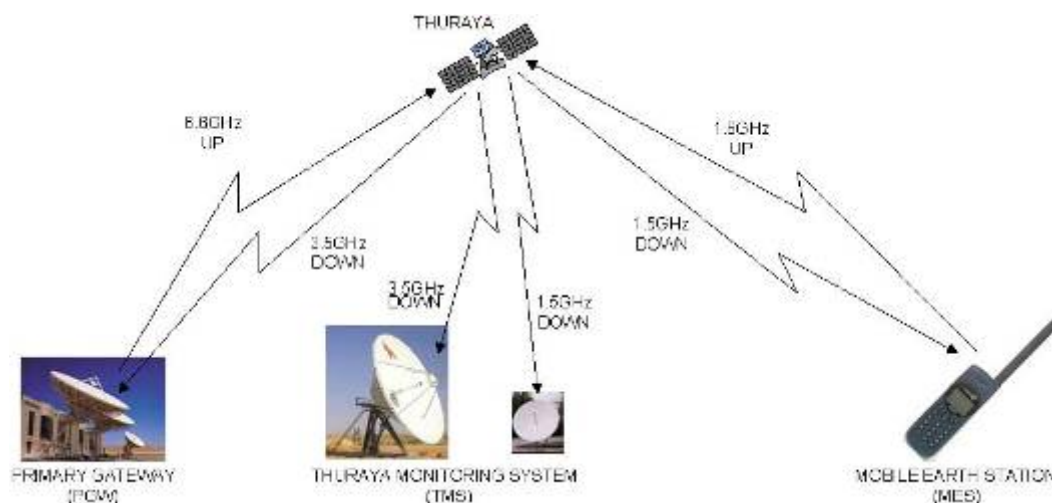


Figure 2 – Principle of TMS Operation

An L-Band antenna receives transmissions from the network to the Thuraya handset (MES), and a C-band antenna receives transmissions from the Thuraya handset to the network via the satellite.

The new system is designed to provide full duplex call interception and recording for all calls passing through a cluster of seven spotbeams centered on the geographical location of the installed system. It may be possible to perform duplex call intercept on other nearby spotbeams, but this cannot be guaranteed due to frequency reuse implemented on the Thuraya network at L-Band.

Additionally, with the inclusion of the optional Transportable Remote L-Band Monitoring System, all calls passing through an additional cluster of seven spotbeams centered on the geographical position of the remote system, may be intercepted and recorded.

In addition to the call intercept, the strategic TMS has the capability to monitor call activity for all spotbeams transmitted by the Thuraya satellite, by receiving the C-band signaling information. The proposed system has the capacity to monitor 25 such spotbeams.

Where the system is able to perform C- and L-Band monitoring of a given spotbeam, the following data is recorded by the system for every call:

- Date and time of the call
- A 4 or 5 digit subset of the IMSI of the MES
- The GPS position of the MES
- The telephone number dialed by the MES (in Mobile Originated calls only)
- The TMSI of the MES
- The Ciphering Key Sequence Number
- The RAND
- The SRES
- The Encryption Algorithm implement on the call

* See "Recoverable File Types" below

- The system also produces a computer file of the call that was recorded; this file is available for offline analysis

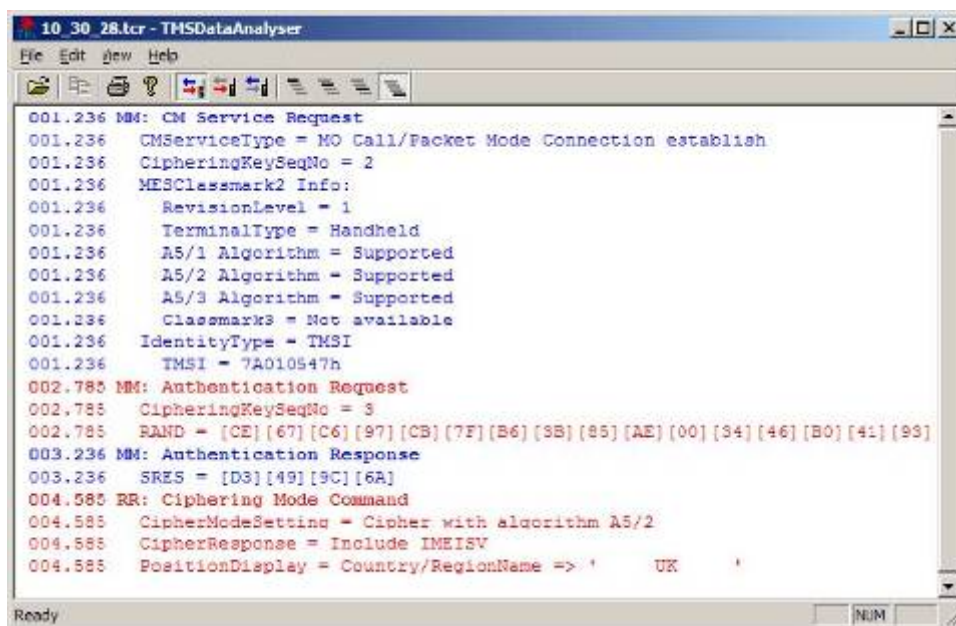
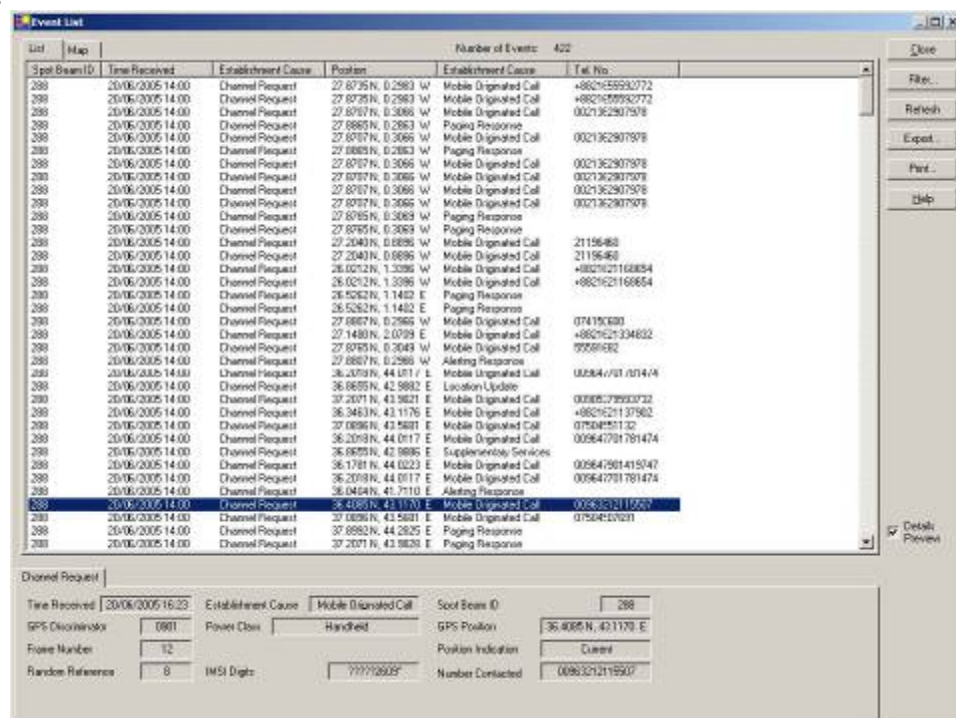


Figure 3 – Information Available from an Intercepted Call before Encryption is Started

Where the system is only able to perform C-band monitoring of a given spotbeam, the following data is recorded by the system for every call:

- Date and time of call
- A 4 or 5 digit subset of the IMSI of the MES
- The GPS position of the MES
- The telephone number dialed by the MES (in Mobile Originated calls only)

For C-Band only monitoring, the call cannot be intercepted, and therefore no recording file is generated.



* See "Recoverable File Types" below

Figure 4 – Information Received from C-Band Monitoring

2.2- Decryption

TRL has now identified, tested and verified the functionality of a Thuraya Cryptanalysis and Decryption device provided by a third-party company. This company is a proven supplier of passive GSM monitoring systems including A5/2 cryptanalysis and decryption. The Thuraya cryptanalysis and decryption unit is their complete solution, developed as a result of determining the Thuraya encryption algorithm and developing their existing GSM cryptanalysis product to process the Thuraya traffic.

This solution when connected to the Strategic Thuraya Monitoring System provides the capability for the play-back of audio voice calls and the display of the SMS, fax and data sessions.

2.2.1- Additional Functionality Available with a Cryptanalysis Solution

With the Thuraya cryptanalysis and decryption solution integrated with the strategic TMS, the following additional information becomes available from calls intercepted in a full duplex C and L-band monitoring system:

- **Human Comprehensible Call Content.** This would include live and archived stereo audio playback of voice calls, and presentation of decoded SMS and fax. Additionally, a range of commercial data protocols would also be supported for decoding data transmitted over the Thuraya network.
- **MES IMEI.** The IMEI of the MES would be recorded, significantly enhancing the ability to identify and track particular Thuraya terminals.
- **Calling Line Identity Presentation (CLIP).** The telephone number of call originator would be available on some calls. In particular, the telephone number of the land-line in fixed originated calls, and the telephone number of both parties in a Thuraya terminal to terminal call would become available.

Cryptographic and Cryptanalysis technology is subject to export control by the governments of many Western countries, including the United Kingdom. Upon development of a GMR-1 cryptanalysis solution, any European or North American developer would be obliged to apply to their respective governments for permission to export the solution.

2.3- A Typical Strategic Thuraya Monitoring System

A typical TMS system would include:

- Full duplex interception of Thuraya calls for terminals located within the same spotbeam as the monitoring system, and up to 6 spotbeams immediately adjacent to that central spotbeam
- Antenna system, including a 9.3m C-Band antenna and demodulator subsystem for monitoring of up to 1088 simultaneous calls in the area covered by the main installation – including GPS co-ordinates of mobile terminals
- Analysis subsystem, complete with 6 server computers and 8 analysis workstations complete with TMS analysis software
- Full Operator, Administrator and Maintainer training programs, held both at TRL and at the customer's site if required
- Comprehensive operation and support documentation
- Full warranty for the first year
- The option of a Remote L-Band Unit, to extend the interception coverage of the monitoring system, to another group of up to 7 spotbeams anywhere within the Thuraya coverage
- C-band Only monitoring of Terminal activity in any Thuraya spotbeam on the satellite. Up to 35 spotbeams can be monitored in the default configuration. This monitoring provides

* See "Recoverable File Types" below

the GPS position and the dialed telephone numbers for all Thuraya phones operating in the spotbeams of interest

The proposed strategic Thuraya Monitoring System comprises 3 subsystems, each are described below:

2.3.1- RF/IF Subsystem

The RF/IF subsystem receives the downlink signals from the Thuraya satellite that are intended for the MES and the PGW. It includes the following components:

Outdoor Equipment

- 9.3m Diameter C-Band Earth Station Antenna
- Flat Plate L-Band Antenna

Low Noise Amplifiers are included with all antennas, as well as Inter-Facility Cabling between the Antennas and the Customer Supplied Equipment Room. The 9.3m C-Band Antenna is fully motorized.



Figure 5 – Typical C-Band Antenna

- Satellite Tracking Antenna Controller
- Satellite Beacon Tracking Receiver
- 4 C-Band Synthesized Tuneable Downconverters
- 1 L-Band Synthesis Tuneable Downconverter
- RF/IF Signal Distribution
- 10 MHz GPS Corrected Station Frequency Reference
- Uninterruptible Power Supply

The above indoor equipment is supplied installed in a 19" rack cabinet.

2.3.2- Demodulator Subsystem

The demodulator subsystem receives the satellite signals from the RF/IF subsystem at IF, and demodulates them. It includes the following:

- Demodulator Cards. A sufficient number of demodulator cards will be supplied in order to perform dual C- and L-band monitoring and call intercept of all traffic on up to seven spotbeams surrounding the monitoring station, as well as C-band only monitoring for at

* See "Recoverable File Types" below

least 10 other spotbeams. If the optional Remote L-Band Monitoring System is also ordered, then the strategic system will be fitted with additional demodulator cards to provide C-band monitoring and call intercept for the spotbeams monitored by the remote system. The demodulator cards are fitted in to card racks, each housing 12 cards.

- Ethernet Switch
- Uninterruptible Power Supply

All components of the Demodulator Subsystem are supplied installed in a 19" rack cabinet.

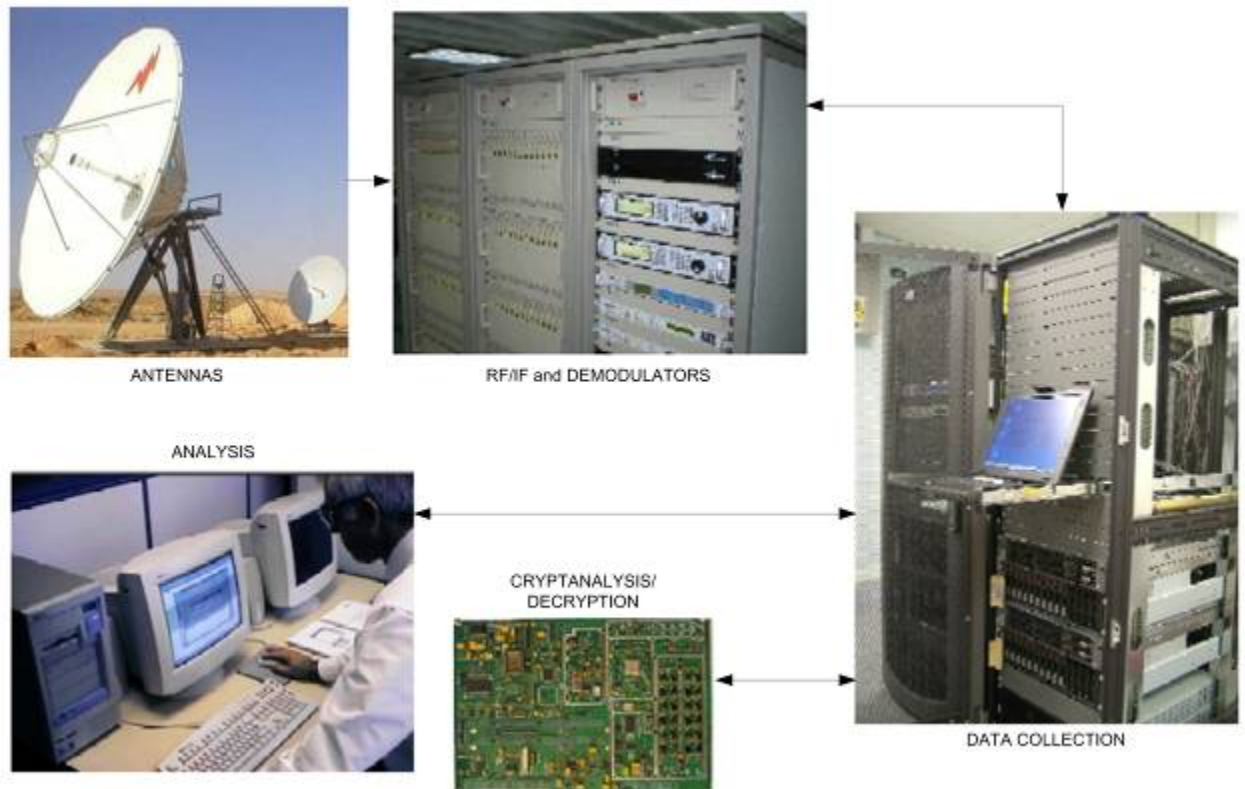


Figure 6 – Typical TMS Equipment

2.3.3- Analysis Subsystem

The analysis subsystem configures the demodulator subsystem according to the User's operational requirements. It receives the satellite signals from the Demodulator subsystem via an Ethernet network, and stores them in the server computers. The analysis software performs decoding and de-multiplexing of the received signals and interprets them providing the User with information about the traffic on the Thuraya network as described in Section X2.1X. The software includes a geographical mapping interface based on the ESRI standard ArcGIS software, and displays the positions of the MESs making calls on the Thuraya network, as well as information related to the available spotbeams on a map.

* See "Recoverable File Types" below

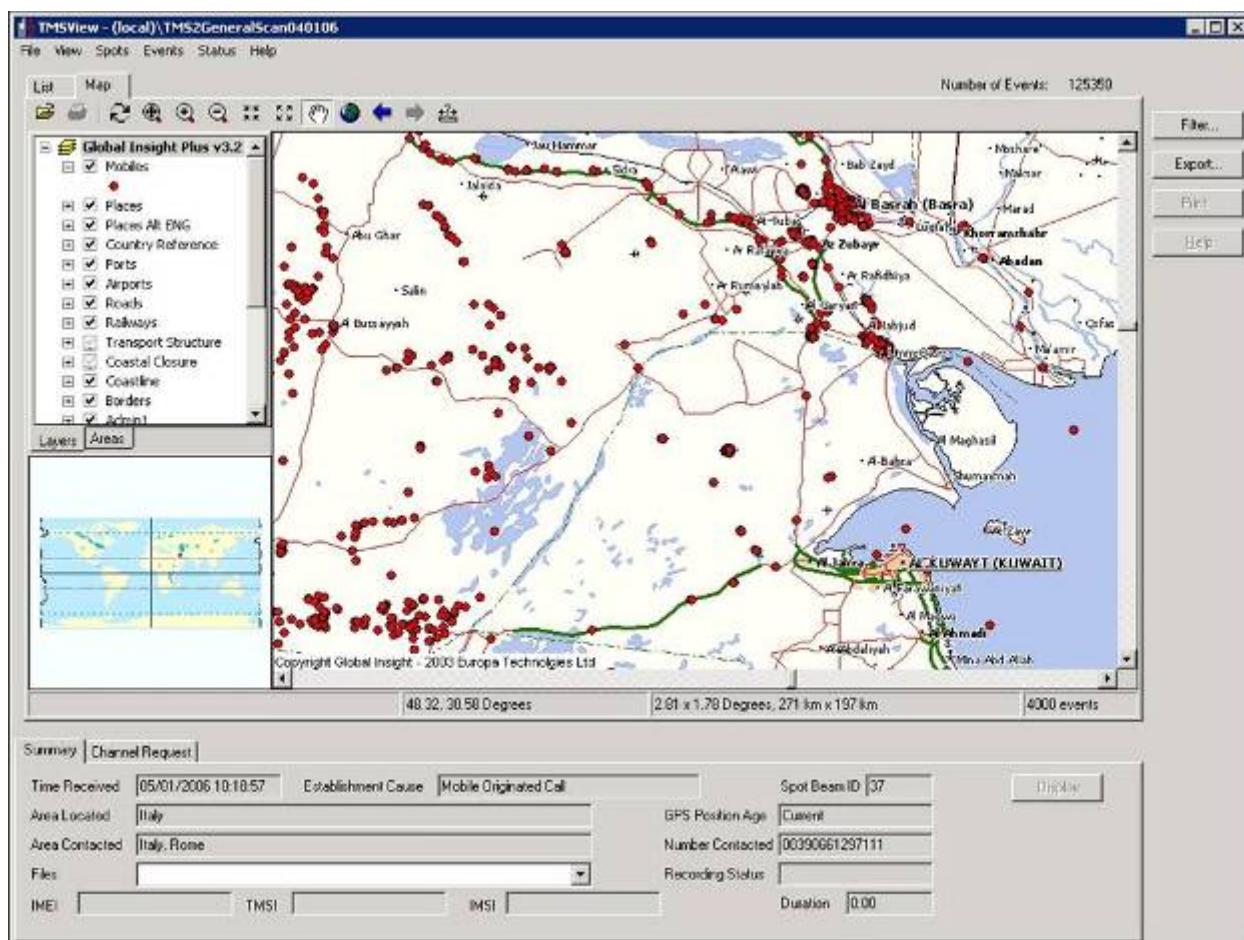


Figure 7 – Sample Map Generated from C-band Monitoring Data

The Analysis Subsystem includes the following components:

19" Rack Mounted

- Server Computers
- Keyboard, Video, Mouse (KVM) Drawer
- KVM Switch
- Ethernet Switch
- Uninterruptible Power Supply

Free Standing

- Workstation Computers with 19" LCD TFT Flat Screen Monitors
- Uninterruptible Power Supply Units

It is assumed that suitable buildings, civil works and electrical power is to be provided by the customer, and therefore is not included within the scope of this proposal.

Training is provided in the administration, operation and maintenance of the system both at TRL facilities, and at the customer site upon completion of the system installation.

The strategic TMS is supplied with a full spares pack to reduce potential system downtime in the event of a component failure.

The TMS has a modular design allowing all aspects to be scaled to meet customer requirements.

* See "Recoverable File Types" below

Remote L-Band Thuraya Monitoring Expansion

A Remote L-Band Thuraya Monitoring System (TMS) expands upon the amount of spotbeams that a strategic TMS can provide full duplex call intercept for.



Figure 8 – Map of the Thuraya Spotbeam Structure

The strategic TMS can provide full duplex monitoring for a cluster of up to seven spotbeams centered on its geographical location. The addition of a Remote L-Band TMS can extend this coverage to another cluster of up to seven spotbeams anywhere within the coverage area of the Thuraya satellite.

The Remote L-band TMS should be connected to the strategic TMS via an 'always on' connection, such as a Leased Line, WAN, or satellite link (e.g. VSAT). In this way the Remote L-band TMS acts in a similar way to the L-band part of the strategic TMS. Information is passed across the remote link to ensure that the interceptions of two monitoring systems are synchronized. TRL recommend the use of a VSAT link for remote areas, and can offer this as part of a 'turnkey' solution if required.

The Remote L-band TMS comprises the following components:

Outdoor Equipment

- Flat Plate L-Band Antenna and Associated RF Cables

Rack Mount Indoor Equipment

- L-band Downconverter
- 12 Demodulator Cards are supplied as standard, in most cases this will enable L-band monitoring and call intercept of all traffic on the seven spotbeams surrounding the remote monitoring station. The demodulator cards are fitted into card racks, each housing 12 cards
- Server computer
- Uninterruptible Power Supply
- Ethernet Switch

* See "Recoverable File Types" below

- A full spares pack is also included

4- The Semi-Strategic Thuraya Monitoring System

The Semi-Strategic TMS operates in the same way as the Strategic Thuraya monitoring system, except that it is designed to work with a trailer-mounted 4.6m C-band antenna. Because of the reduced size of the antenna, it is not capable of intercepting the call content, instead it is used to monitor Thuraya activity in any spotbeam, providing the operator with the GPS positions of Thuraya terminals active within the spotbeams of interest, and the telephone numbers being dialed by these terminals.

The Semi-Strategic TMS comprises the following components:

- 4.6m Trailer Mounted C-Band Antenna
- Satellite Tracking Antenna Controller
- Satellite Beacon Tracking Receiver
- 4 C-Band Synthesised Tuneable Downconverters
- RF/IF Signal Distribution
- 10 MHz GPS Corrected Station Frequency Reference
- Demodulator Cards. A sufficient number of demodulator cards will be supplied in order to perform C-band only monitoring for up to 12 spotbeams
- Ethernet Switch
- Server Computer loaded with TMS Server software
- Keyboard, Video, Mouse (KVM) Drawer
- Uninterruptible Power Supply
- Laptop computer loaded with TMS Client software

A full spares pack is also included.



Figure 9 – Typical Semi-Strategic TMS Antenna

* See "Recoverable File Types" below

5- The Tactical Thuraya Monitoring System

The tactical Thuraya Monitoring System operates in the same way as the strategic system, except that it only receives L-Band signals. In order for it to be able to intercept both side of a duplex call, as well as receiving the L-Band satellite downlink to the Thuraya terminal, it also receives the L-band uplink from the target terminal via radio line-of-sight.

The tactical system will intercept all of the same information available from a strategic system, but only for terminals with its radio line-of-sight. The range of the system can vary from up to 10 km in clear terrain and from an advantageous monitoring point, to as little as a few hundred meters in dense urban areas or inside buildings.

The tactical TMS comprises the following components:

- Flat Plate L-Band Satellite Downlink Antenna
- Flat Plate L-Band Target Downlink Antenna
- RF Cables
- Tactical TMS Chassis fitted with 6 Demodulator Cards, Ethernet Switch Card, IF/FRU Card, and a Dual Downconverter card
- Laptop Computer

A full spares pack is also included.






Figure 10 – Tactical Thuraya Monitoring System

* See "Recoverable File Types" below

Thuraya Monitoring System Identities and information captured

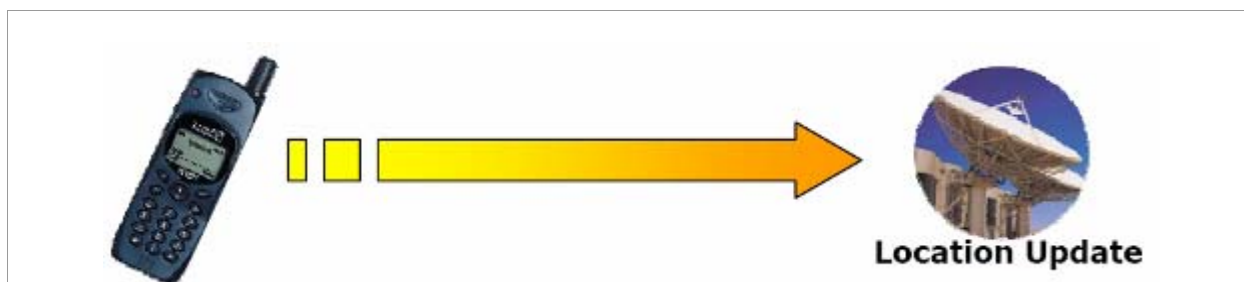
In the following scenarios, the Thuraya terminal marked "1" is always assumed to be in the coverage area of the Thuraya Monitoring System (L&C Band):

	
Thuraya Makes Call to Landline	
Thuraya MES1 information captured: Date and time call made GPS Location TMSI IMEI	Landline Phone Information captured: Number
Call content captured: Duplex - Voice, SMS, Data*	
	
Thuraya Makes Call to GSM Phone	
Thuraya MES1 information captured: Date and time call made GPS Location TMSI IMEI	GSM Phone Information captured: Number
Call content captured: Duplex - Voice, SMS, Data*	
	
Thuraya 1 Makes Call to Thuraya 2 in Area covered by TMS (L&C Band)	
Thuraya MES1 information captured: Date and time call made GPS Location Number (ISDN) – if not blocked TMSI IMEI	Thuraya MES2 Information captured: Date and time call received GPS Location Number (ISDN) TMSI IMEI
Call content captured: Duplex - Voice, SMS, Data*	

* See "Recoverable File Types" below

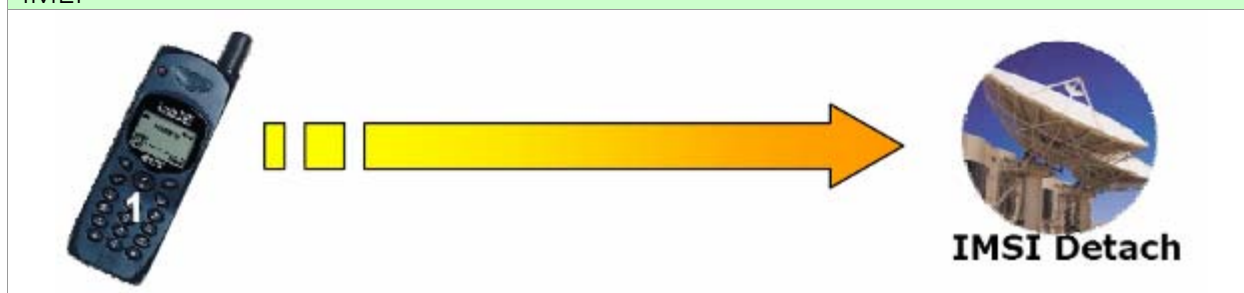
Thuraya 1 Makes Call to Thuraya 2 in Area not covered by TMS	
Thuraya MES 1 information captured: Date and time call made GPS Location TMSI IMEI	Thuraya MES 2 Information captured: Date And Time (if C Band coverage) GPS Location (if C Band coverage) But it is not possible to 'pair' this event with the call made from MES1
Call content captured: Duplex - Voice, SMS, Data*	
GSM Phone Makes Call to Thuraya	
GSM Phone information captured: Number (if not blocked)	Thuraya MES1 Information captured: Date and time call received GPS Location TMSI IMEI
Call content captured: Duplex - Voice, SMS, Data*	
Landline Phone Makes Call to Thuraya	
Landline Phone information captured: Number (if not blocked)	Thuraya MES1 Information captured: Date and time call received GPS Location TMSI IMEI
Call content captured: Duplex - Voice, SMS, Data*	

* See "Recoverable File Types" below



Thuraya Switches on

Thuraya MES1 Information captured:
Date and time call received
GPS Location
TMSI
IMEI



Thuraya Switches Off

Thuraya MES1 Information captured:
Date and time
GPS Location
TMSI
IMEI

Recoverable File Types

Typical file types which will be recovered and viewable from e-mail attachments or file transfers (FTP) are as follows:-

- | | |
|--------------------------------|---|
| Text files | Text, Rich text, Postscript, PDF |
| Web Pages | Text, HTML |
| Sound Files | Basic audio, x-aiff, wav |
| Pictures | Image files, gif, jpeg, pjjpeg, tiff, x-png, x-bitmap bmp, x-jg, x-emf, x-wmf |
| Video clips | Avi, mpeg |
| Programs/applications | Base64, x-msdownload, octet-stream |
| Compressed files | x-compressed, x-zip-compressed, x-gzip-compressed |
| Application files, for Example | Microsoft Word documents
Microsoft Excel spreadsheets
Microsoft PowerPoint presentations
Word perfect documents
Lotus Notes documents |

* See "Recoverable File Types" below

Protocols Supported

Underlying Protocols

The following Data Layer protocols are supported:

- SLIP
- PPP
- Synchronous
- PPP (Bit Stuffed Flag Frames)
- X Modem, Y MODEM

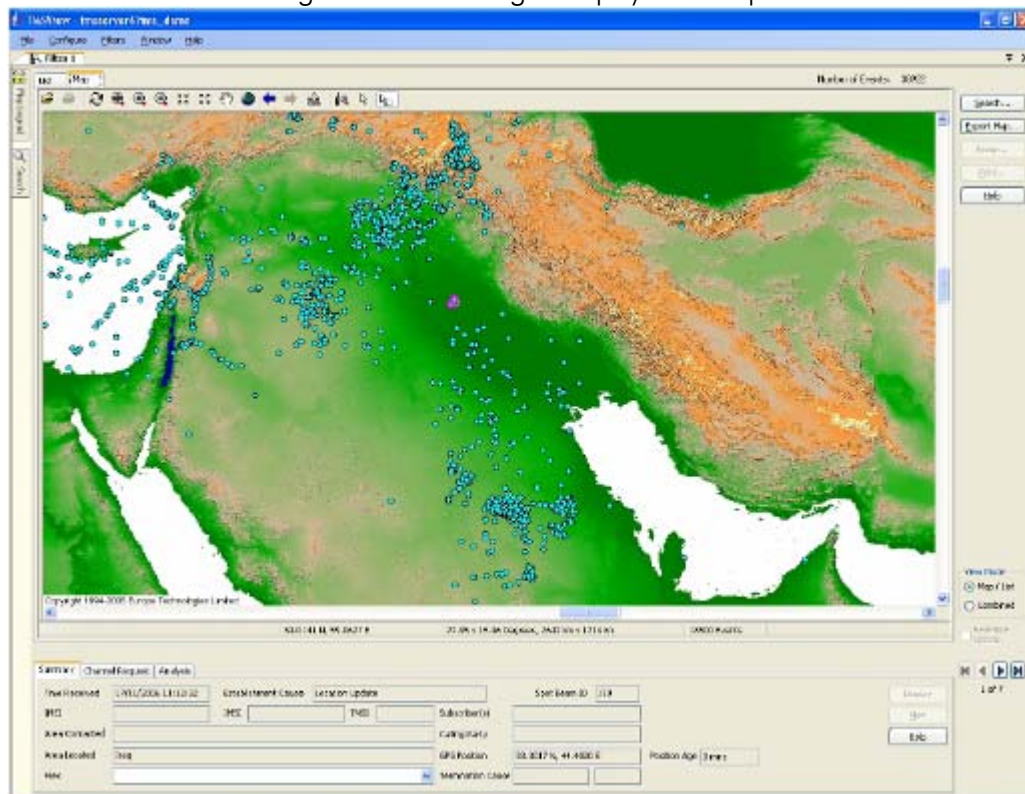
TCP/IP Protocols

- HTTP (WWW)
- FTP (File Transfer)
- POP3 (e-mail)
- SMTP (e-mail)

Modem Protocols (File Transfer)

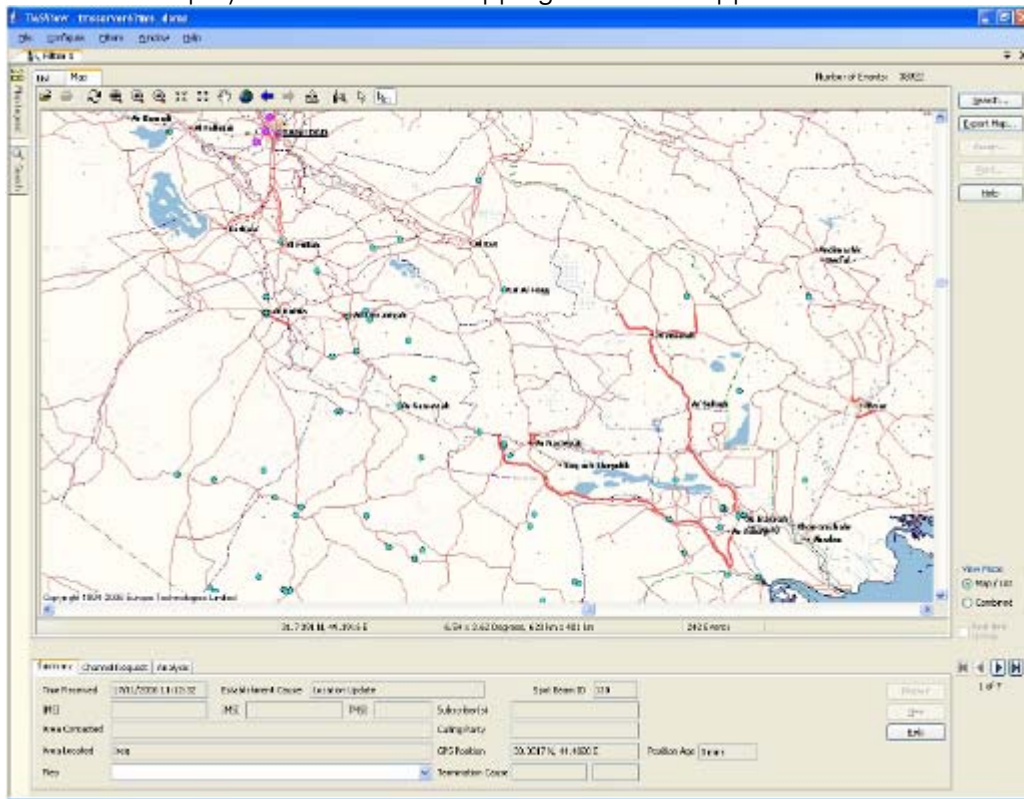
- XMODEM,
- XMODEM-1K
- XMODEM-CRC
- YMODEM
- YMODEM-1K
- YMODEM-CRC

1. Screen shot showing call locations against physical map

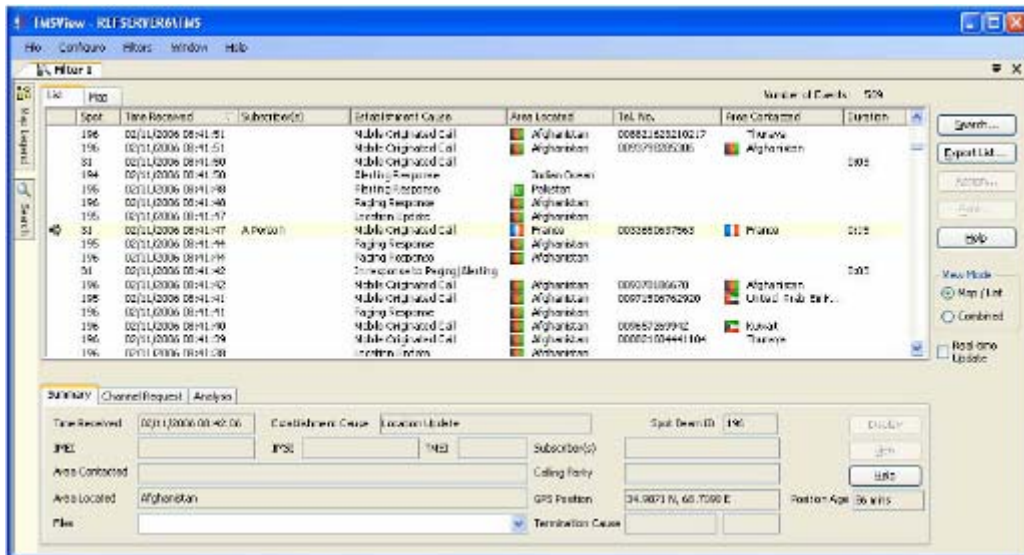


* See "Recoverable File Types" below

2. Mobiles displayed on standard mapping software supplied with TMS

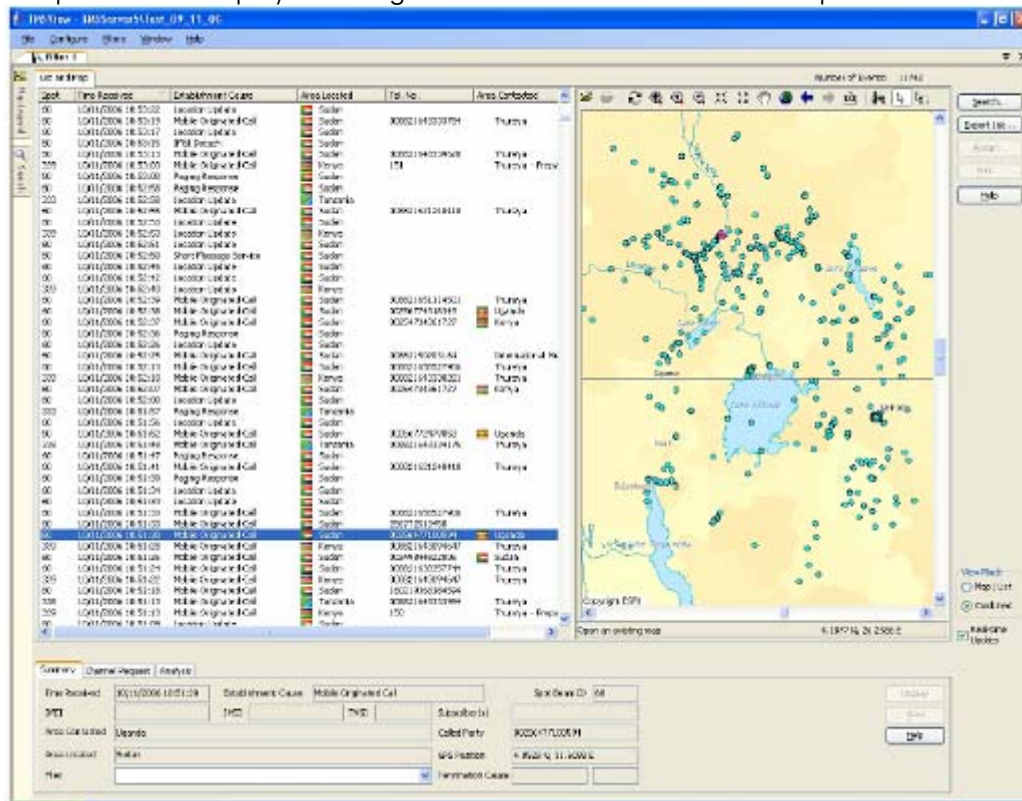


3. List View

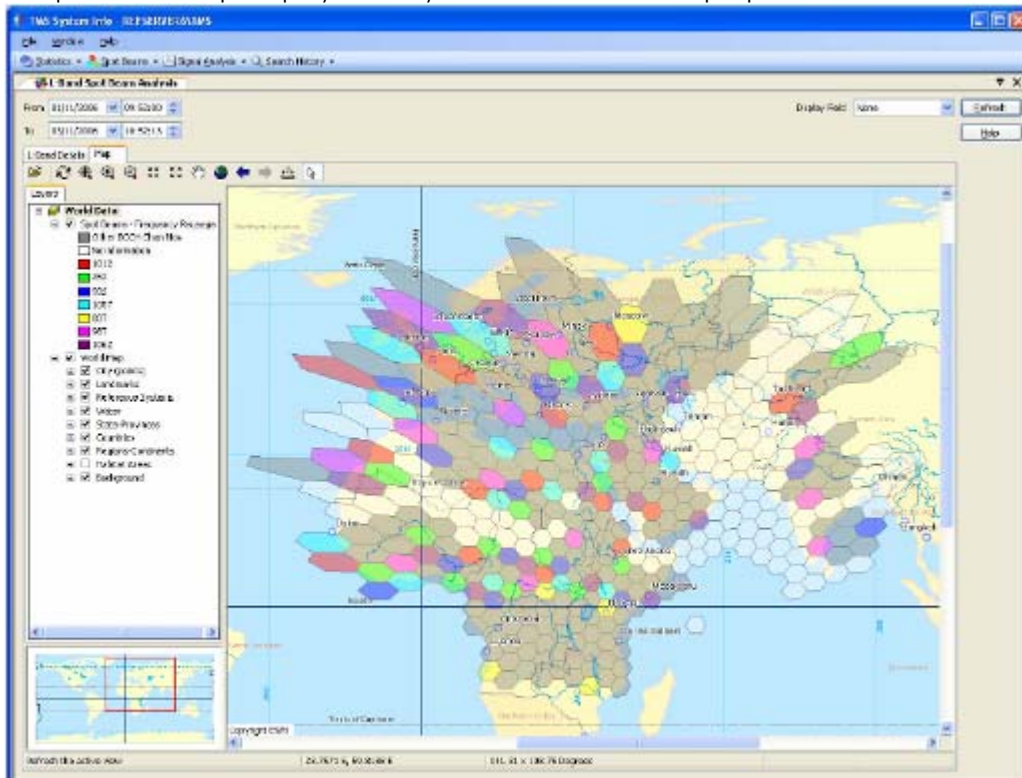


* See "Recoverable File Types" below

4. Split screen display showing new list view and associate map view

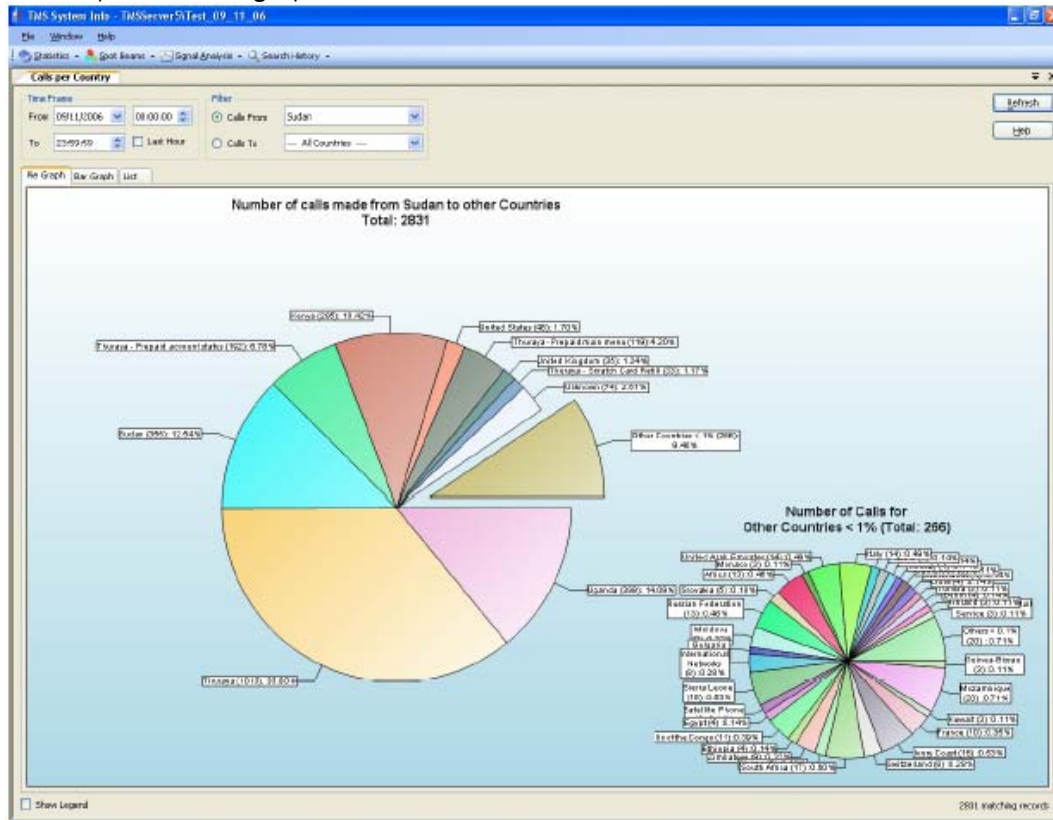


5. Spotbeam map display – for system administration purpose

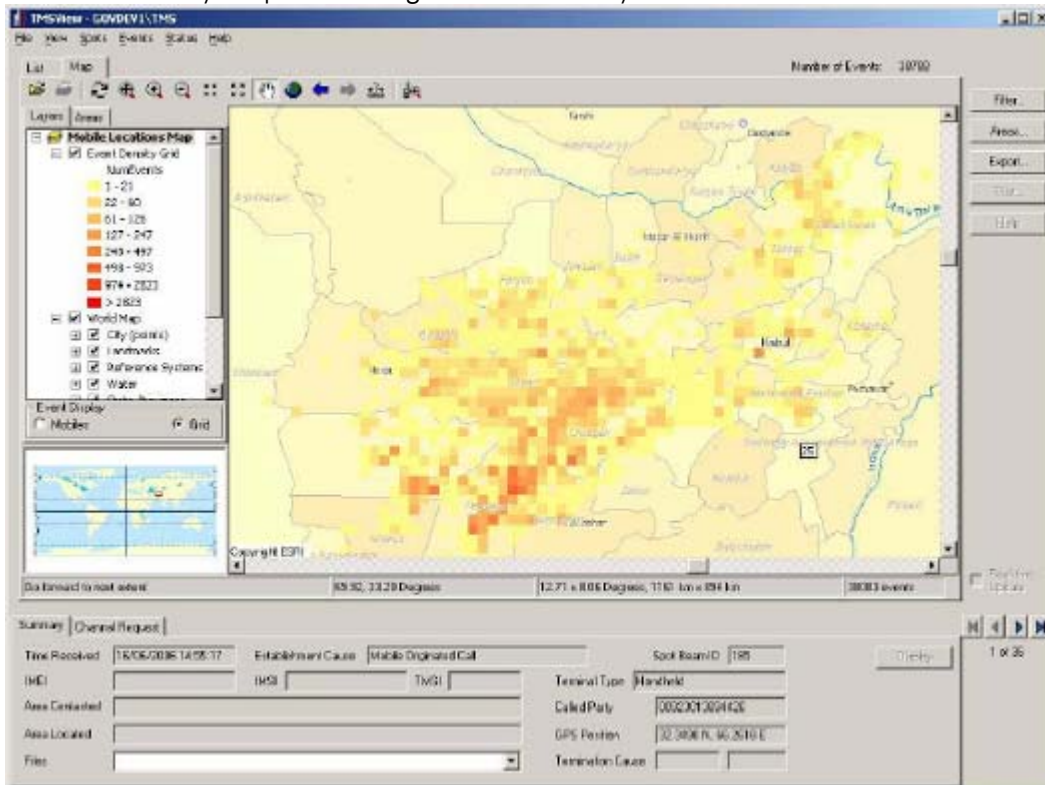


* See "Recoverable File Types" below

6. Analysis of calls graph - user definable

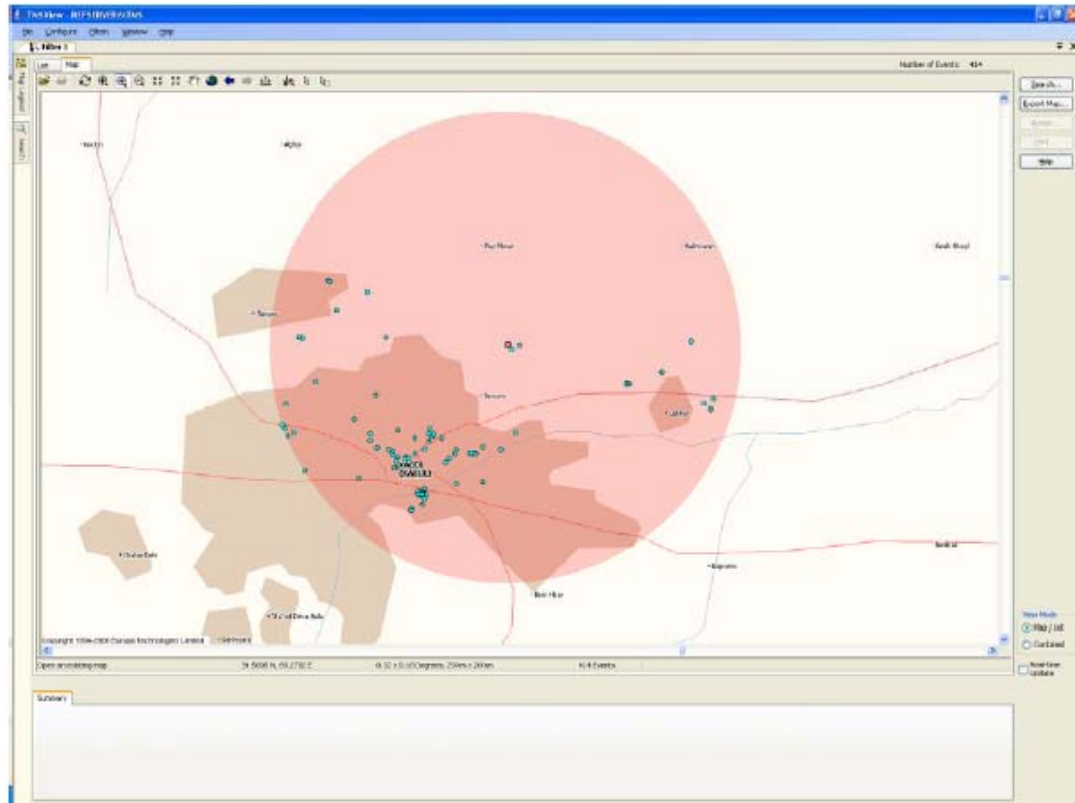


7. Event density map – showing areas of activity rather than individual calls.

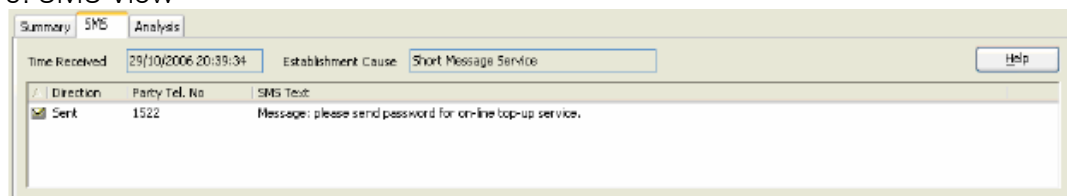


* See "Recoverable File Types" below

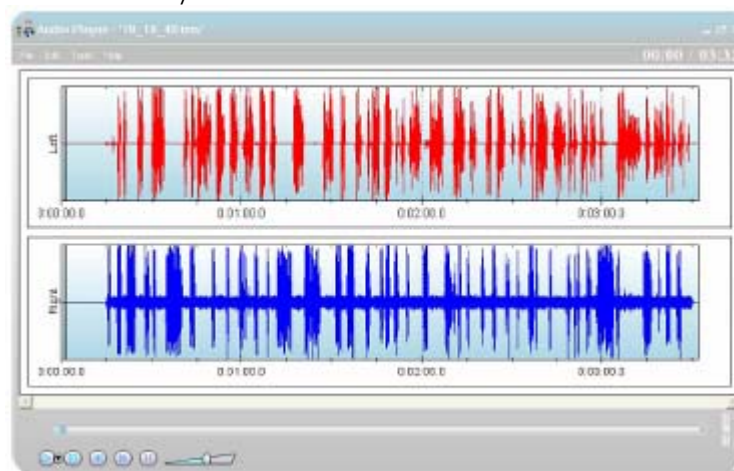
8. Geo-location map screen – to set up geo-fence area to filter calls from a particular site of Interest



9. SMS View

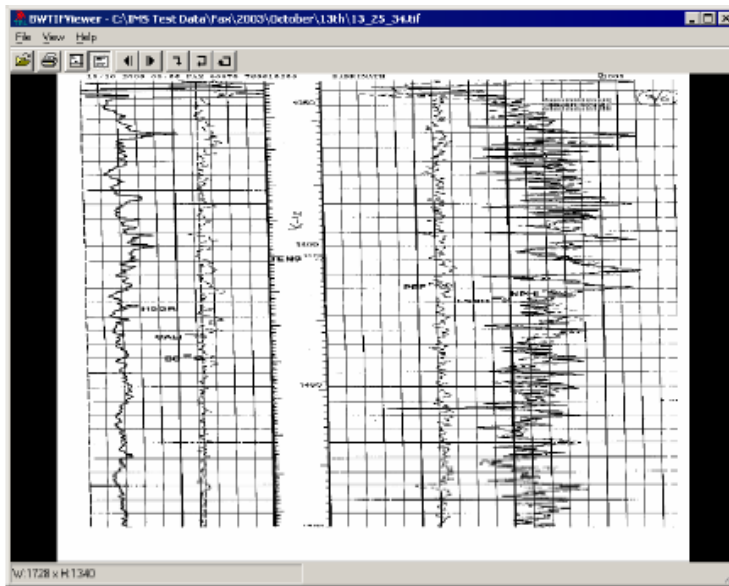


10. Audio Player

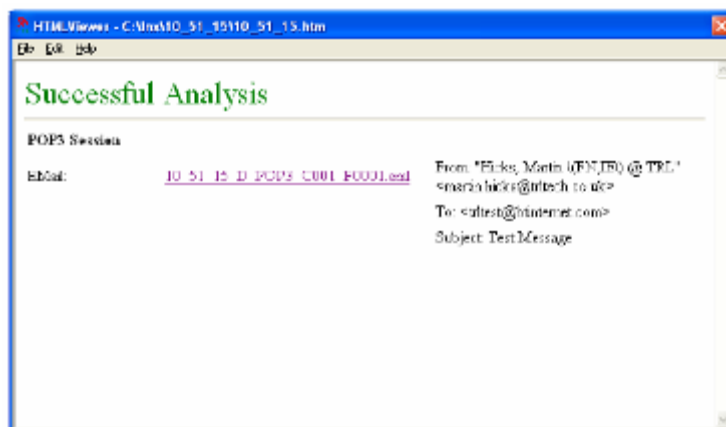


* See "Recoverable File Types" below

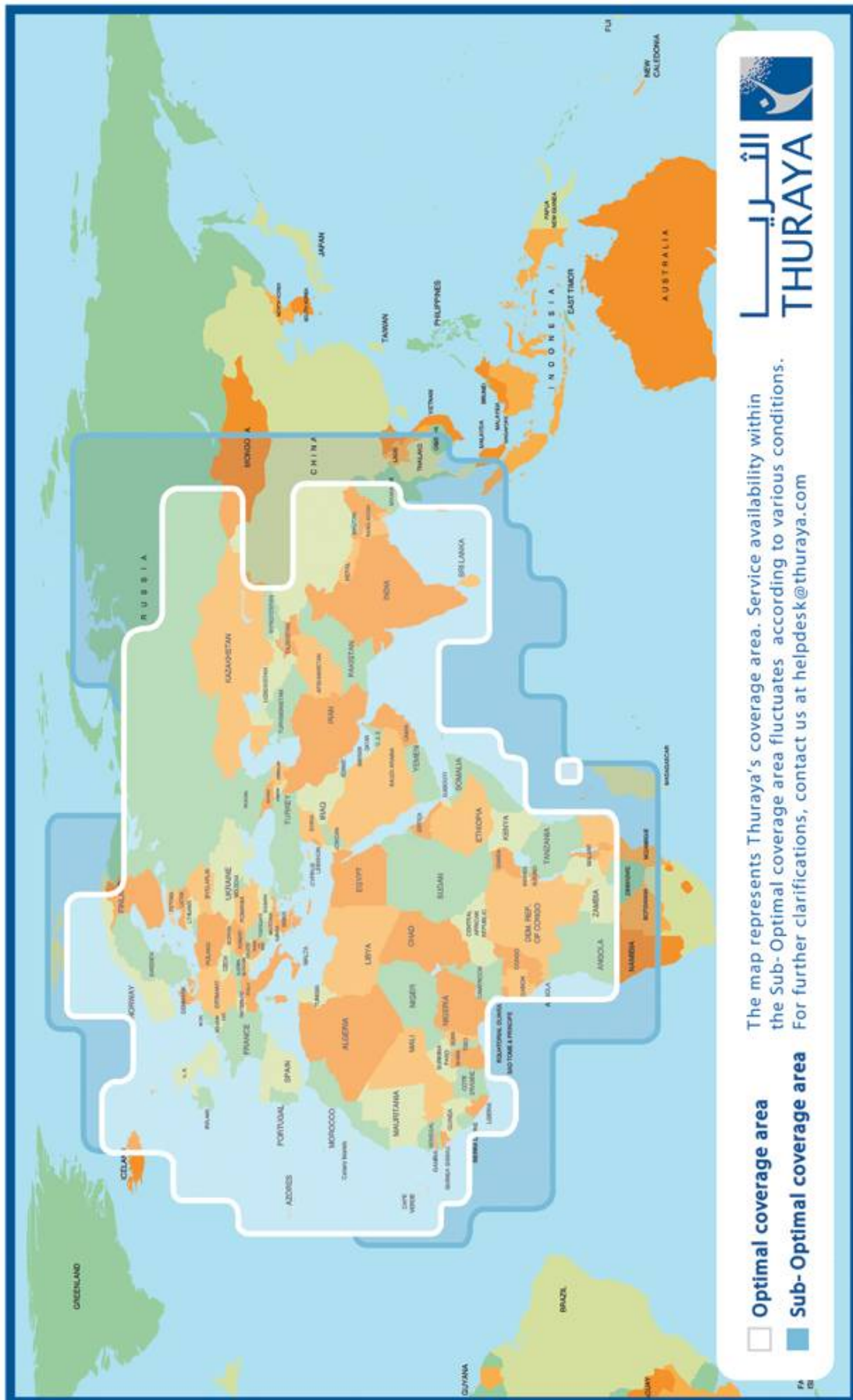
11. Fax View



12. Data View (POP3 example)



* See "Recoverable File Types" below



* See "Recoverable File Types" below

CONFIDENTIAL



If you would like further Information about ELAMAN,
or would like to discuss a specific requirement or project, please contact us at:

Elaman GmbH
German Security Solutions
Seitzstr. 23
80538 Munich
Germany

Tel: +49-89-24 20 91 80
Fax: +49-89-24 20 91 81
info@elaman.de
www.elaman.de