HARVESTER
User Manual

Version 6.0
All Editions

Revision 6.0
June 2018

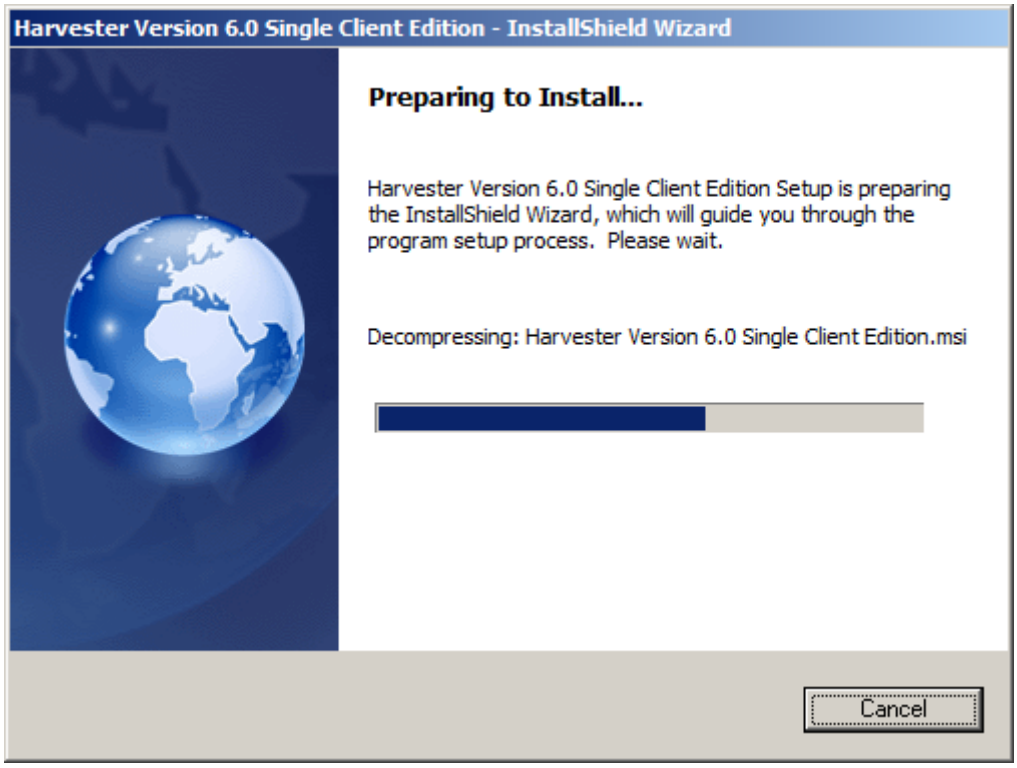
Table of Contents

1. Setup

signals intelligence (SIGINT): 1. *A category of intelligence comprising, either individually or in combination, all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted. [JP 1-02]* **2.** *Intelligence derived from communications, electronics, and foreign instrumentation signals. [JP 1-02]*

1.1 Installation

To install the HARVESTER software, run the downloaded file *harvester_xxx_setup.exe* file and follow the onscreen installation instructions. The installation will create a *SIGINT Systems/Harvester* folder within the *Program Files* directory into which will be placed the HARVESTER application and it's associated files.



Once installation is successfully completed, HARVESTER will run in demo mode until a registration is purchased. Demo mode provides full functional with stored frequency limit of a maximum of 25 frequencies across the radio spectrum.

1.2 Setting up the Database

Unlike previous versions of HARVESTER that used Microsoft SQL Server, the application is now build on Oracle's MySQL database platform which allows the application to be quickly and easily deployed as well as offering a flexible choice of operating system for the database server for Standard and Professional versions.

As HARVESTER is essentially a professional platform, setting up the database requires a little more work, though the benefits of speed, data handling capacity and robustness will soon outweigh any effort spent installing the database. A detailed installation guide is included in Appendix A – Setting up the MySQL database.

NOTE These scripts must be run before you try to run the client otherwise there will be no database for the client to connect to. These SQL scripts are used to create the database, and once created should not be re-run as this may cause the database and its tables to be dropped resulting in a complete loss of all data.

The Harvester login screen

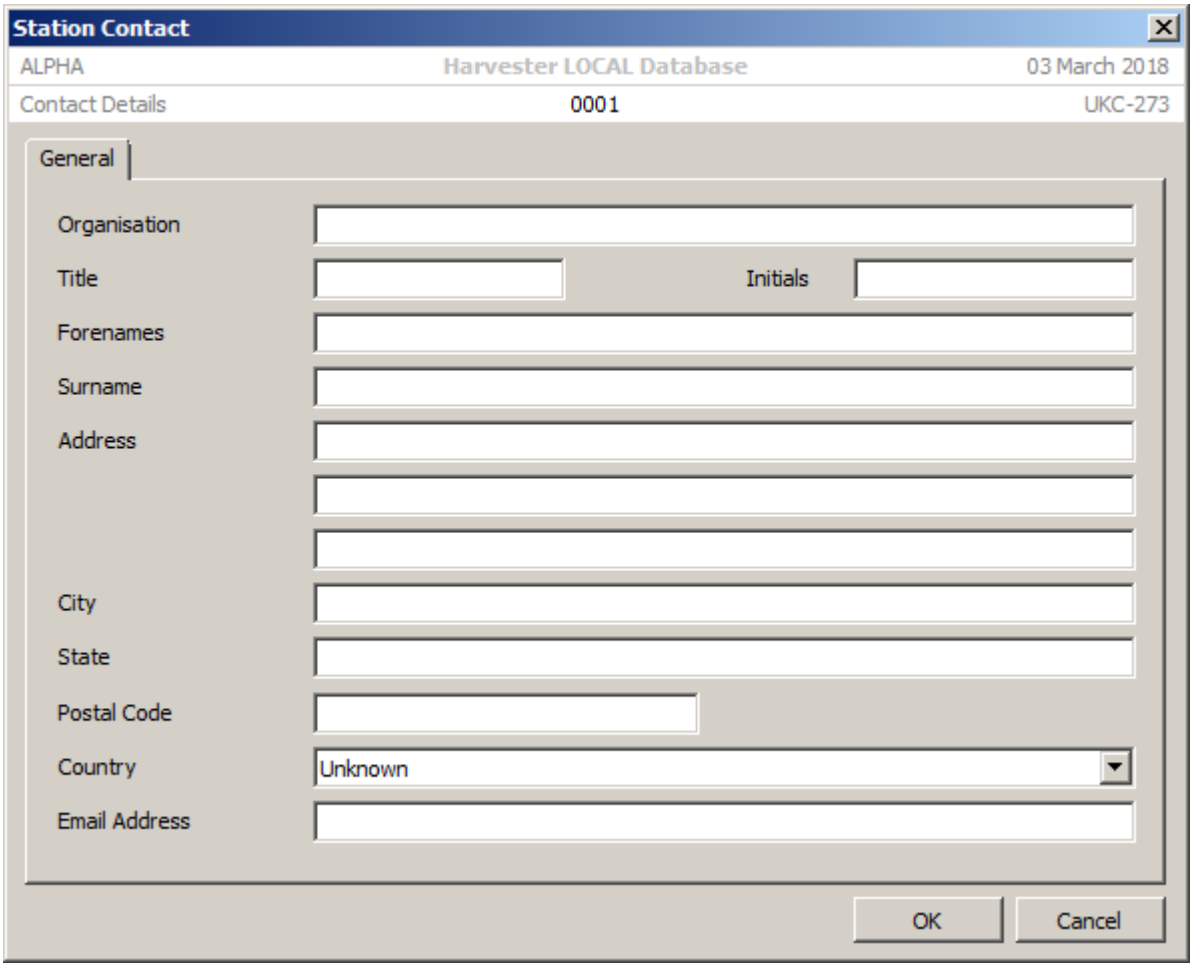
1.3 Setting up the Application

When you run HARVESTER for the first time, it is important that you take a little time to set up the application with your specific user and location details. This is done in the **Station Manager** screen which provides an opportunity for each user to enter details about themselves to aid in the correlation of logs that may subsequently be submitted for inclusion in future updates.

NOTE None of the user data entered here will ever be passed on to third parties. This is purely for reference and to aid in the process of correlating and analysing any logs that you may submit.

To open the **Station Manager** screen, select the **Station Manager** option from the Tools menu on the main Harvester screen.

Once opened, the **Station Manager** provides a number of options. Station contact details including your name, organisation or company name, address and email address can be entered in the **Station Contact** option in the **Tools** menu. Once this page is setup, it will not need to be edited again. Note that this page must be completed before you try to generate your registration file.



TIP At this point, it is a good idea to ensure that your computer clock is set to the correct local date and time since log accuracy depends on your computer clock being correct. HARVESTER will take care of time zone differences and convert all log dates and times to UTC.

1.3.1 Setting up the Station

The main purpose of the **Station Manager** is to set up, manage and keep track of your station in terms of Intercept Locations, Receivers, Antennas and the actual Intercept Positions within the station.

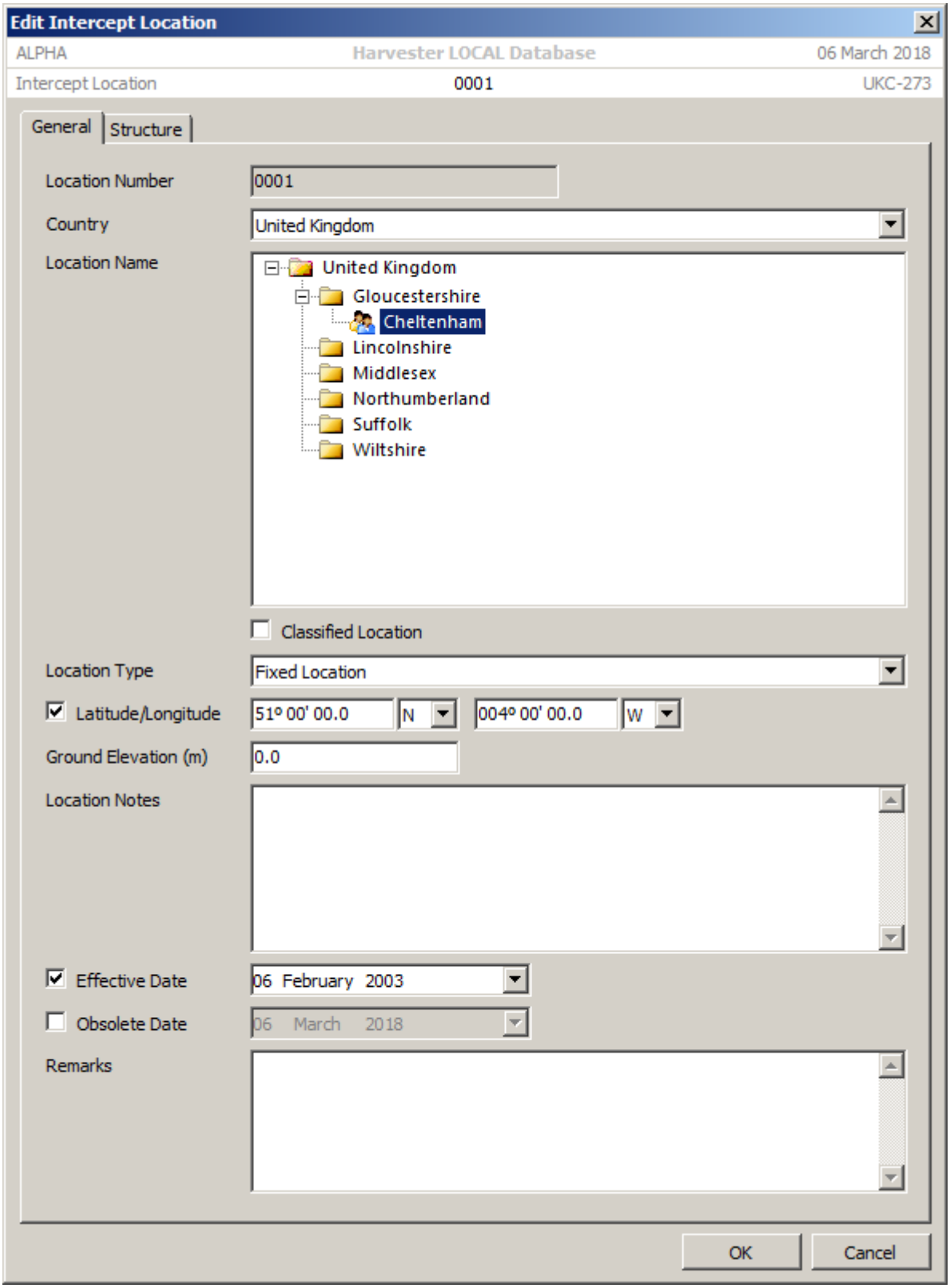
1.3.1.1 Intercept Location

An Intercept Location is defined as the location where you perform any type of signals collection. This may be your permanent, fixed location but may also be a mobile or temporary collection site.

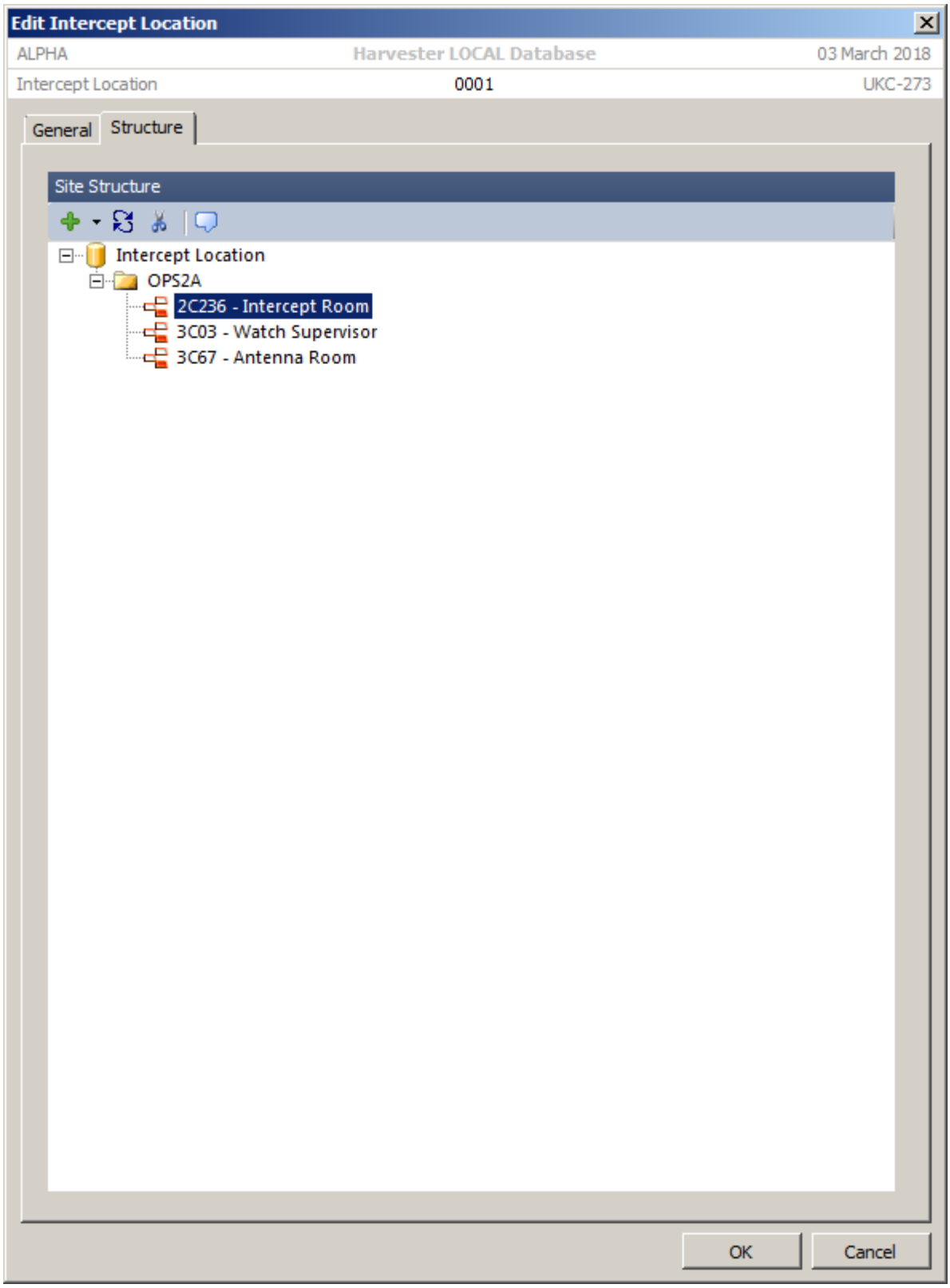
Highlight the **Intercept Locations** option in the navigation menu and click the Add icon to create a new location. This will open the **Add New Intercept Location** screen.

TIP The data that drives the Location Name treeview in Intercept Locations is managed by the Geolocation screen (See chapter 6). If you cannot find your location or want to add a new location, right-click on the treeview to bring up the menu and select the Geolocation option. Once you have entered your location in Geolocation, close it then right-click on the treeview again and select Refresh.

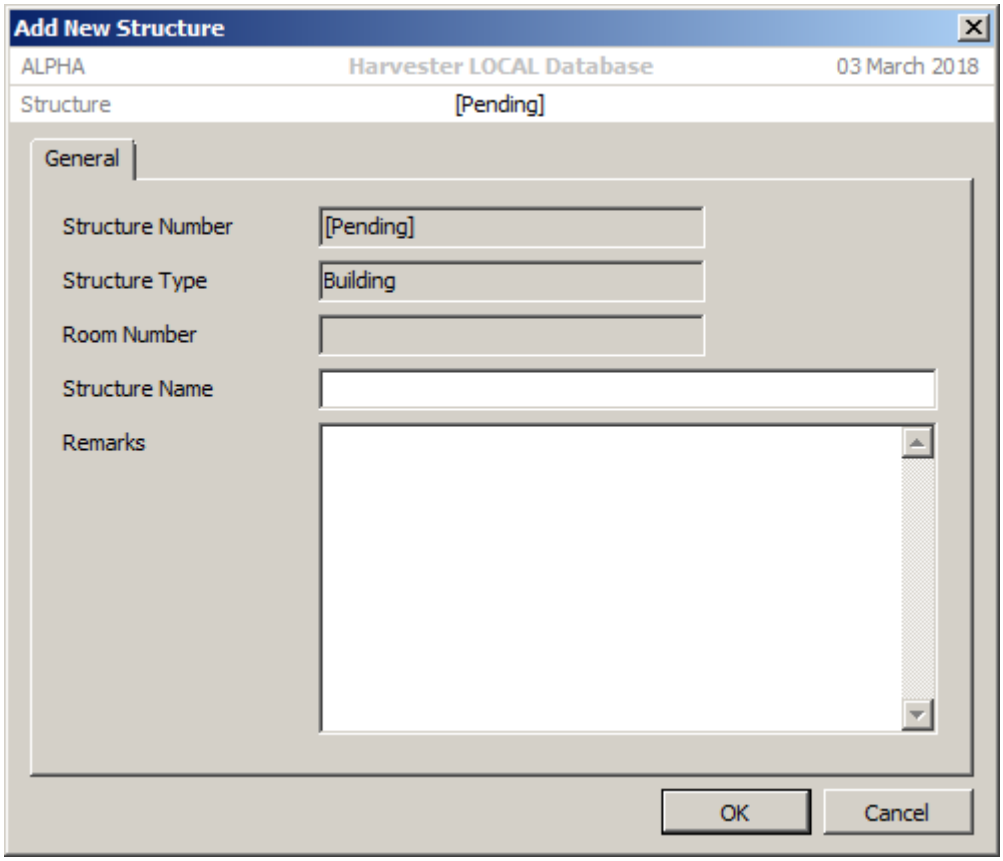
Enter all the relevant details of the location and press OK. If you intend to perform Direction Finding and enter DF or LOB logs from this location, make sure that you enter the location's latitude and longitude. Any Intercept Positions attached to this location will automatically inherit these coordinates which are essential when correlating Line of Bearing logs.



Details of individual buildings and rooms within the **Intercept Location** can be added on the **Structure** tab. This will allow you to build up a detailed picture of the location of assets. Intercept Positions can also be attached to individual rooms to aid station management.



To add a new building or room, select the appropriate parent node and click the Add icon and select either **Add New Building** or **Add New Room**. This will open the **Add New Structure** screen where details of the new building or room can entered.



1.3.1.2 Intercept Positions

An **Intercept Position** is essentially defined as a receiver with its associated antenna, and any other devices that are used to record and/or demodulate the signals intercepted. Each **Intercept Location** can have multiple **Intercept Positions**, each reflecting a different of receiver and antenna configuration.

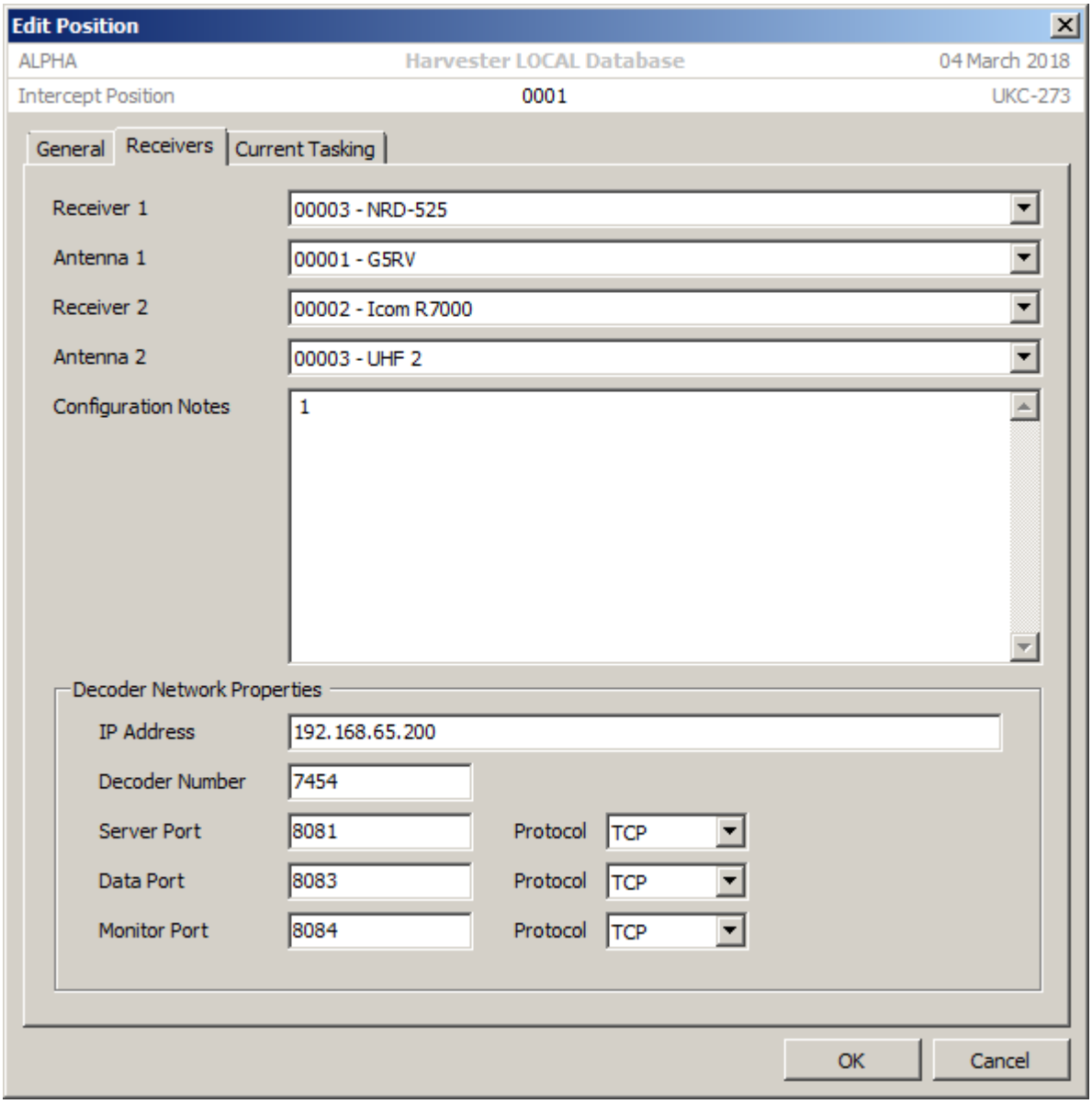
Intercept Positions are automatically added whenever a new Harvester client is run for the first time. These records are originally created as skeleton records but can be amended with specific details such as the Position Notation, Position Type and its associated **Intercept Location** and room within the site. The IP Address and hostname of the position along with its telephone number can also be entered as well as the network configuration of any associated decoder software, the dates when the position was valid and any notes you wish to record about the position. Each **Intercept Position** requires to be identified by the Intercept Position Notation. This is an 32-character free text field. Traditionally these have made some reference to the nature and scope of the position, such as POCORO 3.

To edit an Intercept Position, either double-click the location in the displayed. This will open the **Edit Intercept Position** screen where any amendments can be made.

Note that unlike previous versions of HARVESTER, you do not need to set default locations and positions. This is automaticsally set by the intercept location that an intercept position is attached to when the client logs in.

The **Receivers** tab provides an opportunity to define and record individual receivers and antennas used by each intercept position as well as any notes on the configuration of the position. Receivers and Antennas are defined in the appropriate sections (See below).

For multi-mode intercept positions that use digital demodulators as part of their collection, decoder properties can be stored in the **Decoder Network Properties** section.



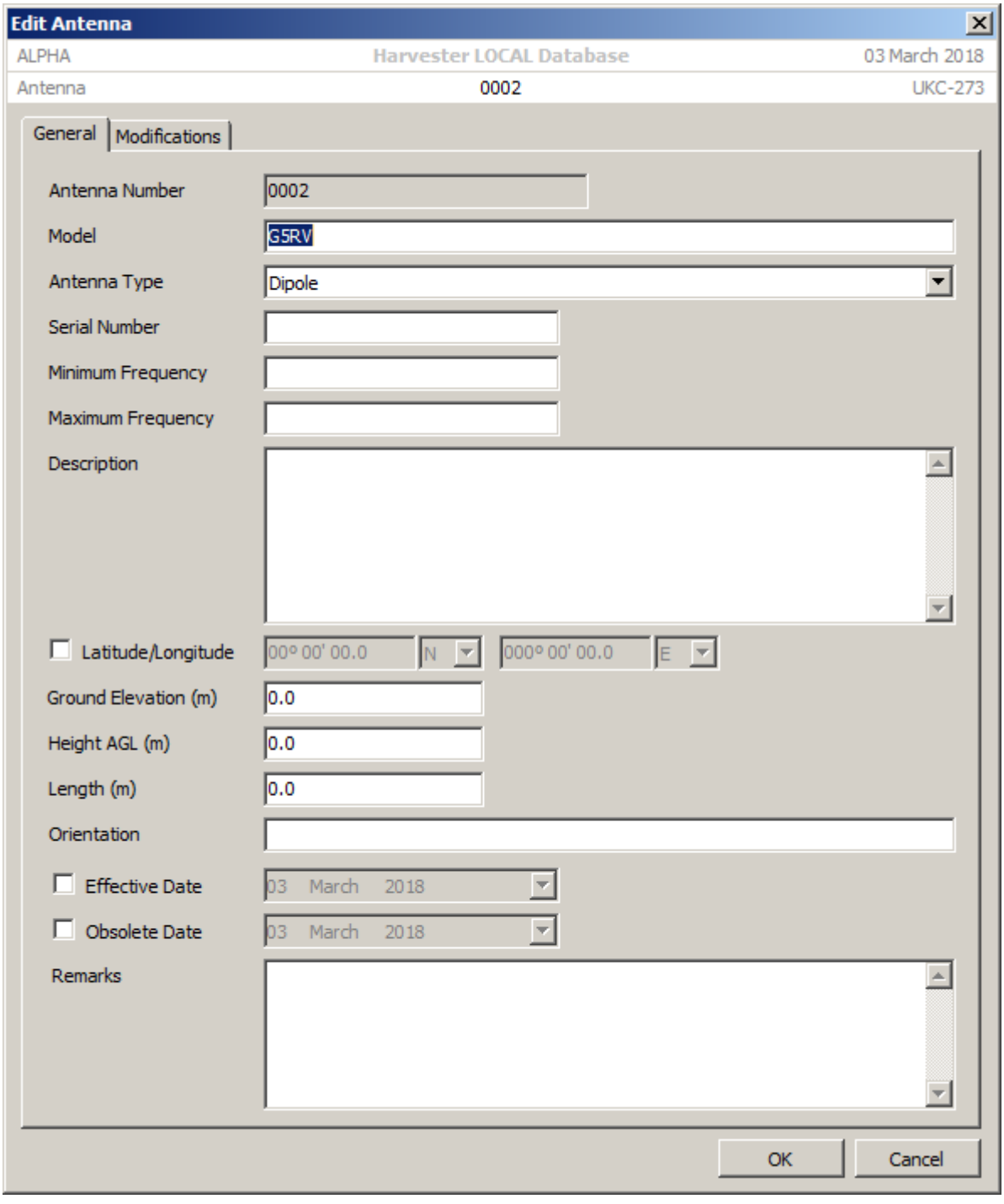
The **Current Tasking** tab, currently read only, provides details of the local Signal Collection and TEXTA blocks used but the application. Currently both set to the default value of 000, these values could be used to reflect specifc collection projects within a sttaion whereby individual intercept positions focus of collection of specifically defined targets.

1.3.1.3 Antennas and Receivers

Within each station, the Antennas and Receivers screens in the **Station Manager** provide a method of maintaining a detailed inventory of intercept and collection equipment. This includes a defintion of the type of equipment, its serial number, the range of frequencies that it can operate over, and in the case of antennas, the specific latitude and longitude that can be used in the analysis of DF Line of Bearing logs.

The screens also provide a method of recording any repairs or modifications carried out. This is particularly useful for recording the progress of programmes of receiver upgrades and modifications.

To Add and new **Antenna** or **Receiver**, select the appropriate option in the Navigation Menu and click on the Add icon in the toolbar. This will open the appropriate screen where details of the specific antenna or receiver can be entered.



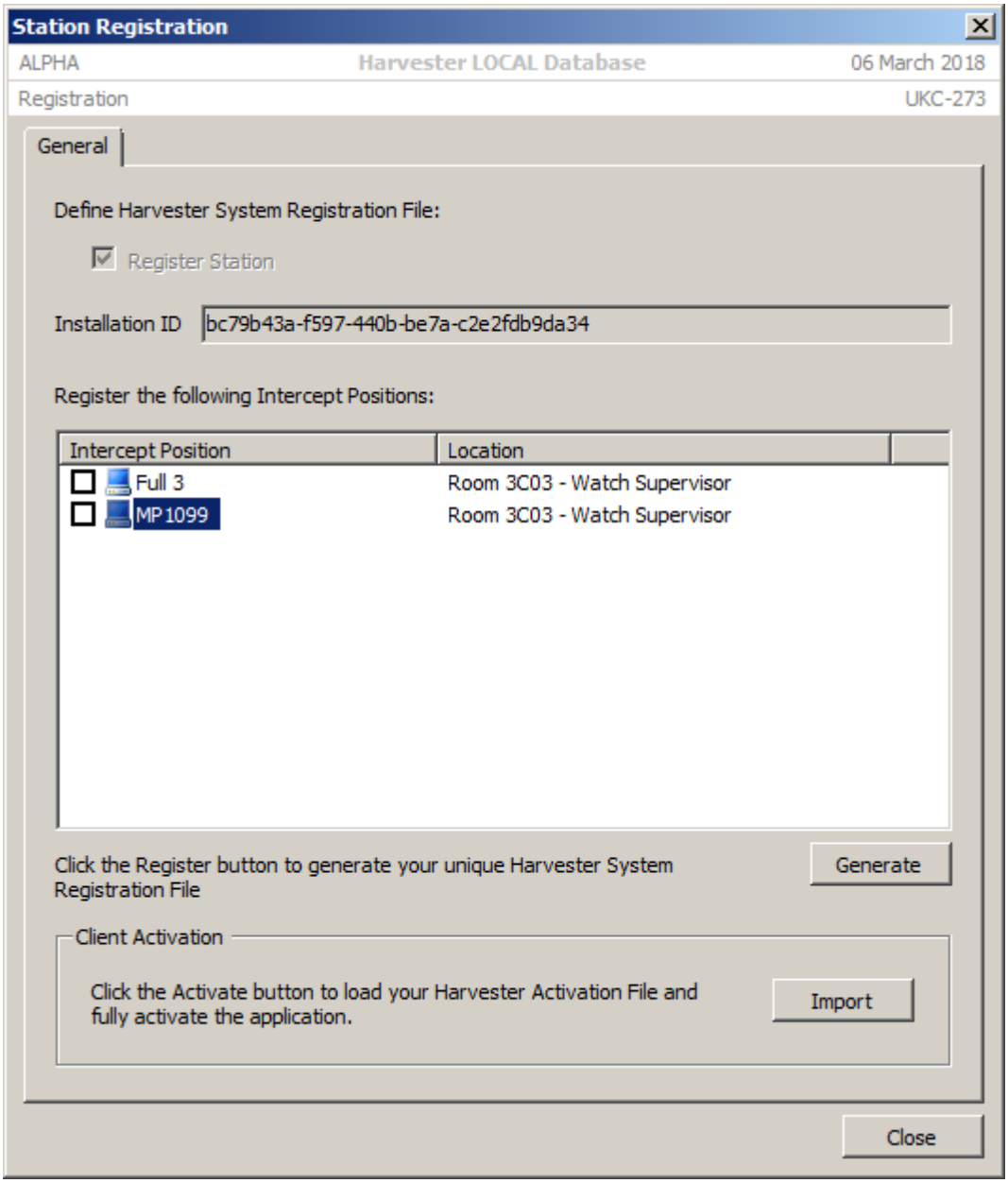
1.4 Registration

To use the full functionality of HARVESTER, each intercept position must be registered. To register your software, an activation file, obtained from SIGINT Systems, must be loaded into the

system. This will be sent to you when you purchase a HARVESTER licence and send your registration file to SIGINT Systems.

To purchase a HARVESTER registration, please visit the web page:

http://www.sigintsystems.co.uk/register.html



1.4.1 HARVESTER Registration Process

The Harvester registration is a simple four-step process:

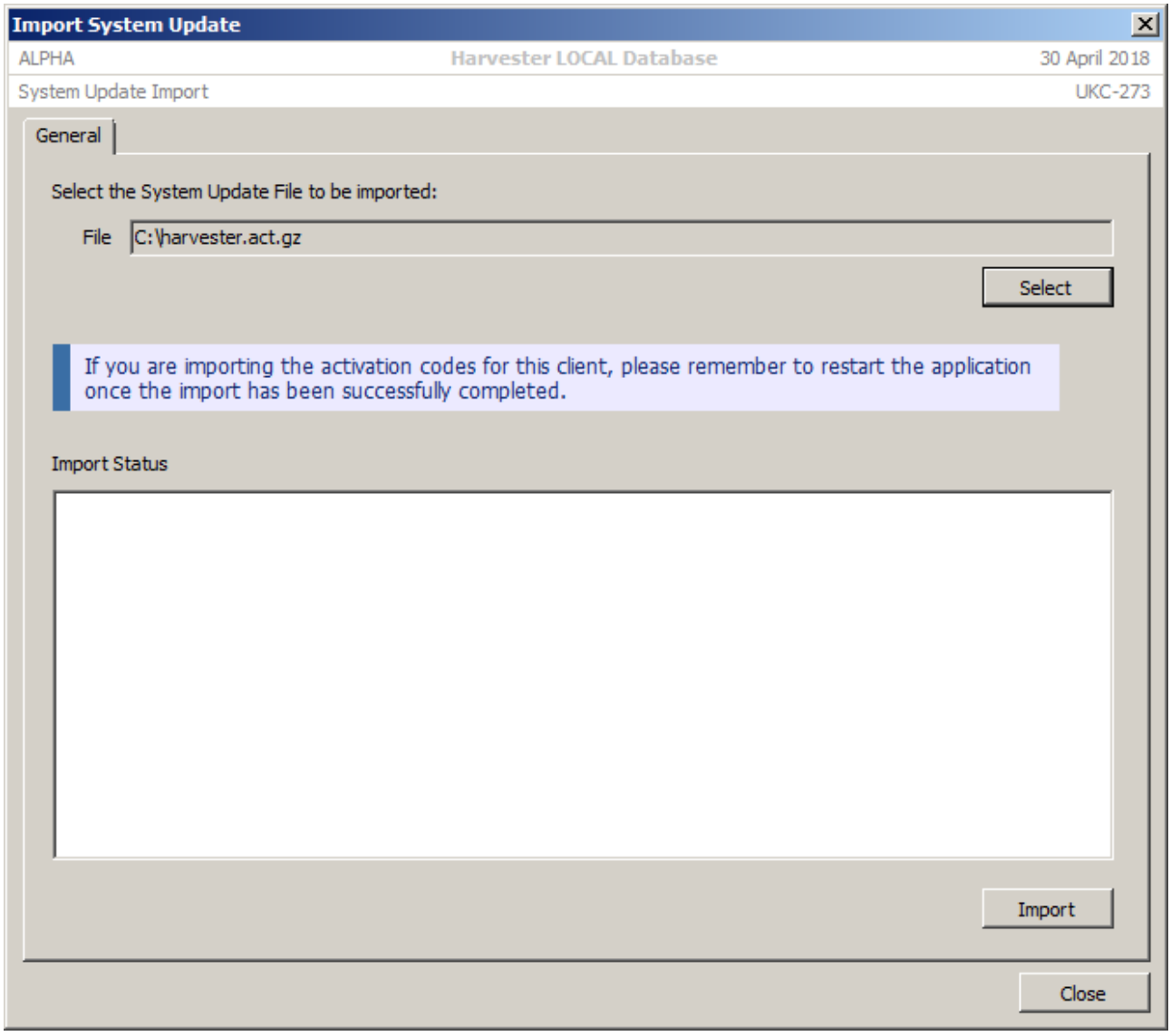
- Generate your Station Registration File, including the individual intercept positions that you want to activate, select the **Station Registration** option from the **Tools** menu in **Station Manager**. Select all the Intercept Positions that you want to activate then click the **Generate** button. This will create your Registration file, called *harvester_yyyymmddhhMMss.hrf.gz*, that will be saved in the **exports** folder. Don't worry if you can already registered an Intercept Position. Re-

registering an already registered Intercept Position will not affect the performance or registration status of the application.

- Email your Registration File to register@sigintsystems.co.uk as an attachment.

- Go to the Registration page on the SIGINT Systems web site and add the appropriate HARVESTER licences for your installation into your basket then proceed to the checkout. If you are not already have a PayPal user, signing-up for an account will only take a few minutes. Before making a payment, please ensure that you include your Installation ID in the Additional Information text box. We require this to match your payment with the Registration File you send us. For simplicity, the Installation ID can be copied from the top of this same screen.

- Once we have received both your Registration File and payment, we will send you your unique Activation File for your specific HARVESTER installation. To load the file into HARVESTER and fully activate the software, return to the **Station Registration** screen click the **Import** button.



Use the file screen to locate the file we have sent you, called *harvester.act.gz*, and then click **OK**. On screen messages will tell you the progress of the import and

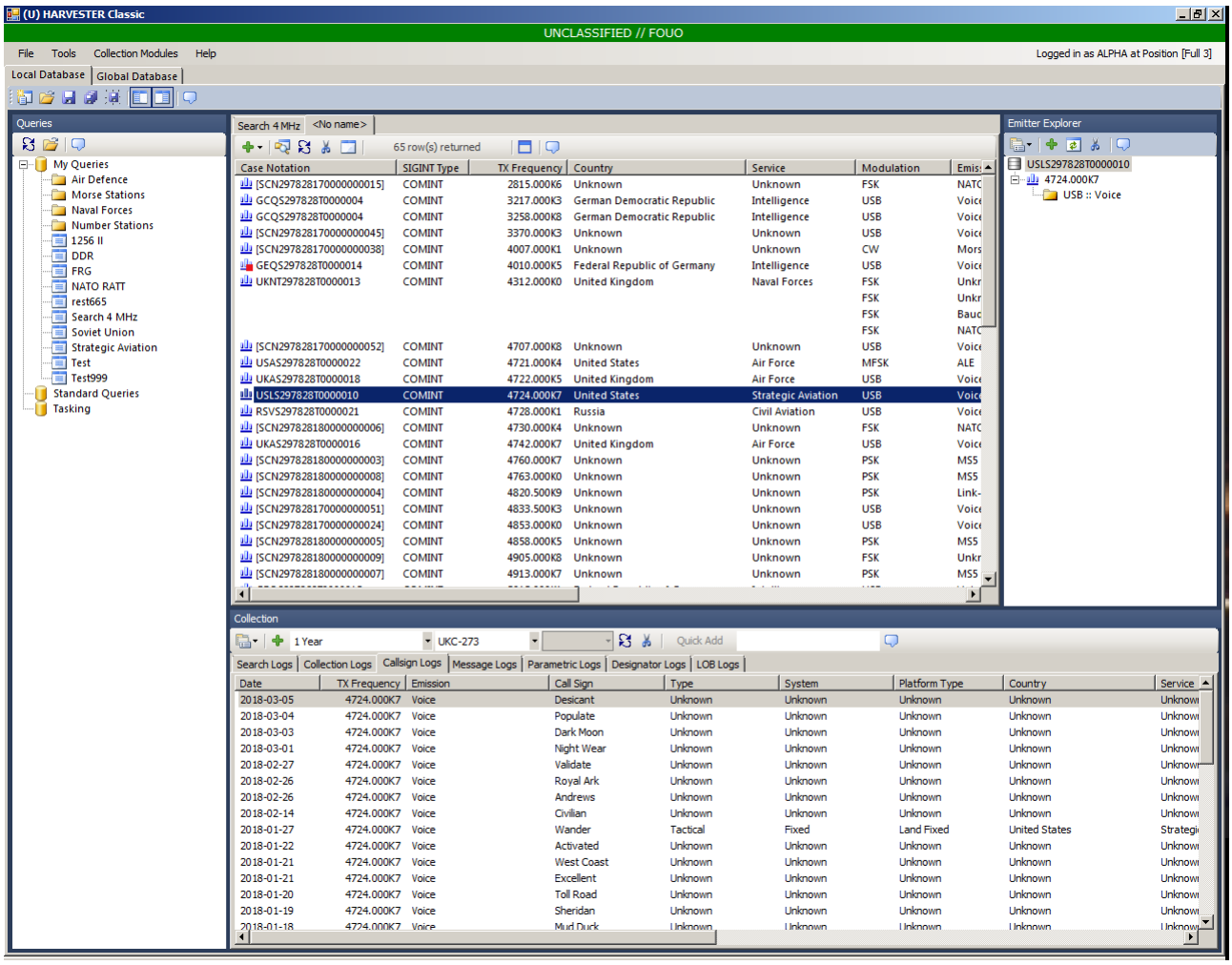
when the software is fully registered. Please remember to close down and restart your client when it is initially registered.

DON'T PANIC If you experience any problems with this process, please contact the Help Desk. We have tried to ensure that this process is as simple and problem-free as possible but things can sometimes go wrong. If they do go wrong, please contact us and we will help you resolve any issues.

2. Emitters

signals intelligence (SIGINT): 1. *A category of intelligence comprising, either individually or in combination, all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted. [JP 1-02]* **2.** *Intelligence derived from communications, electronics, and foreign instrumentation signals. [JP 1-02]*

In almost every commercially available frequency database, and certainly in earlier versions of HARVESTER, each emission is treated as a unique and individual frequency. It's a perfectly acceptable method of recording frequencies but it can give rise to some unusual situations. For example in the case of a station transmitting in both Voice and CW on the same frequency. Because Voice is logged on one record and CW is logged against the other, there was no easy way to link both emissions and their associated logs to the same station. That was changed in the last version of HARVESTER with the software moving away from the idea of frequencies in favour of the more versatile notion of emitters and the accompanying hierarchical benefits of adopting a case notation system (See Chapter 4 – TEXTA System).



Users of previous versions of HARVESTER will notice a marked difference in the appearance and functionality of the main screen, and this demonstrates a fundamental change in the way data is both processed by the software and held in the database. So how

do these changes affect what HARVESTER does and what changes will the user have to make to take advantage these new benefits? At the most fundamental level, these changes make HARVESTER a far more agile application, able to adapt to any number of signal structures and configurations, making it capable of handling intercepts using a more formalised object orientated methodology.

From a user point of view, there is only a slight shift in thinking, and that is probably true of new as well as seasoned users. HARVESTER is not just a list of frequencies. It is principally a frontline intelligence-gathering tool that can be used to collect the information required to build detailed profiles of communications targets. In many other frequency databases you will see two or more different emissions from the same station on the same frequency being logged as two or more separate frequencies, or in even more extreme cases, several transmissions from the same station using the same emission on the same frequency being logged as several frequencies! HARVESTER consolidates intercepts making it easier to spot trends and process gathered information into useful intelligence.

Let's look at an example. Take the second 4020 kHz entry. The emitter has a frequency value of 4020.000 kHz and to it are attached three different emission types, Soviet50 (or Bee), Morse and Baudot. To each of these emissions are attached more properties, such as Baud Speed, Centre Frequency, FSK Shift, Words per Minute, and so on. (See Appendix B for a guide to logging intercepts.)

4018.000K3	PSK	MS5 Fire		Russia
4019.000K4	FSK	81-81	41.0000/500.00//1087	Unknown
	CW	Morse	//18.00/1334	Unknown
4020.000K6	FSK	Soviet 50	50.0000/200.00//2200	Russia
4020.000K6	FSK	Soviet 50	50.0000/500.00//2200	Russia
	CW	Morse		Russia
	FSK	Baudot	50.0000/500.00//2200	Russia
4021.000K7	CW	Morse	//30.00/1000	Unknown
4023.000K9	PSK	MS5 Fire		Russia
	USB	Voice		Russia
4025.000K1	FSK	Soviet 50	50.0000/200.00//1087	Russia
4026.000K2	CW	Morse	//29.00/800	Unknown
4026.000K2	LSB	Voice		Russia

With HARVESTER, the emphasis is on intelligence correlation beginning at the point of interception. The key to this is being able to identify a frequency and being able to confirm that the signal you are intercepting relates to the frequency in the database. To achieve this, a number of key parametrics are made available to aid re-identification. When you intercept a frequency, think of it as an object to which can be attached a number of properties, such as frequency, emissions and channels. It's a very subtle change thinking of the frequency as a transmitter or transmitting entity rather than just a frequency.

2.1 The Harvester Screen

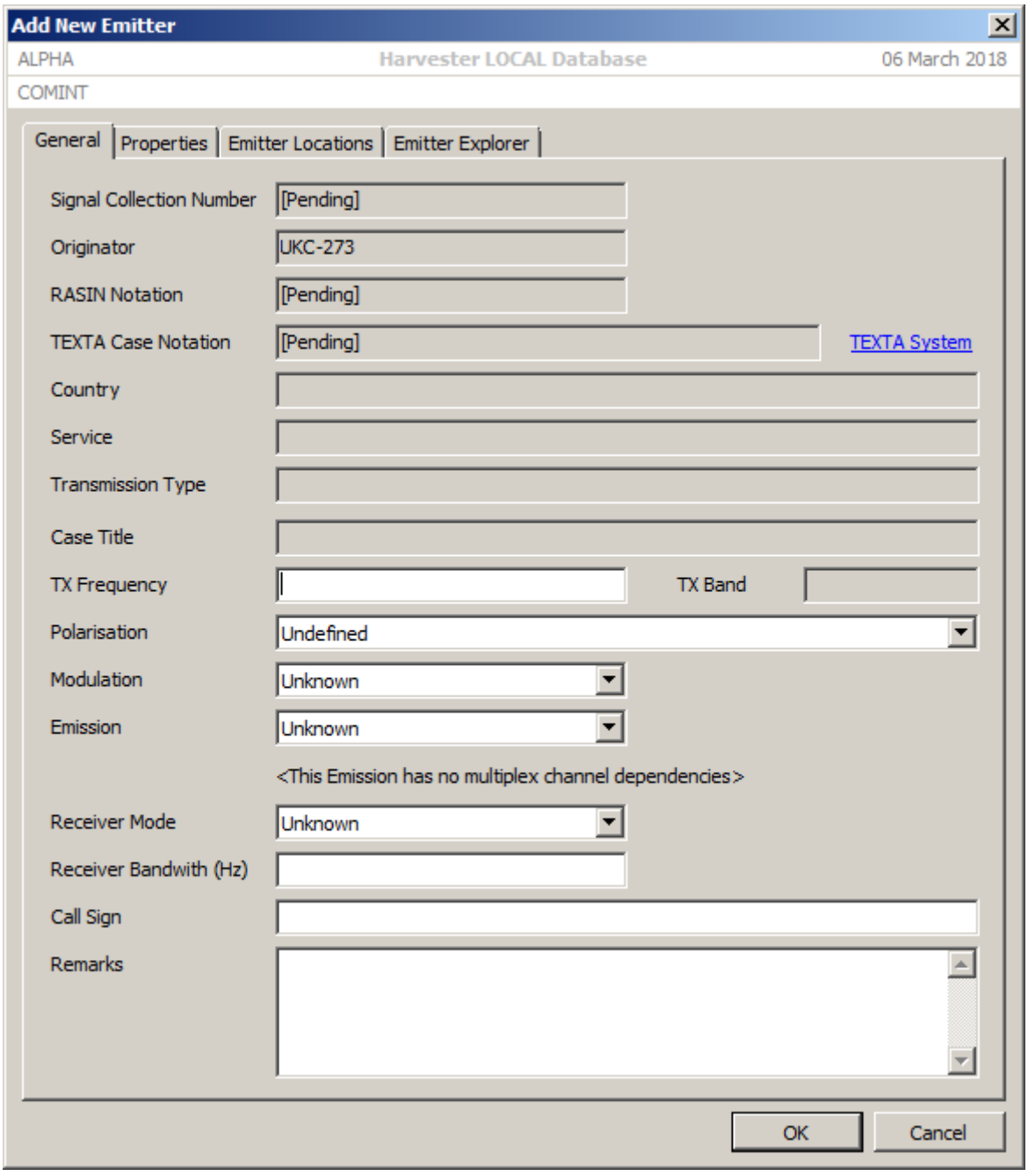
All logs and intelligence can be entered and accessed from the main HARVESTER screen. It comprises an unlimited number of frequency search tabs in which any portion of the RF spectrum can be displayed. From this screen there is also access to a number of collection and intelligence tools, such as TEXTA, TEXTA Case Files, search, collection, callsign, message, parametric, designator and LOB logs. This screen also provides access to a number of collection project screens: **GSM Mapper**, **Pager Networks**, **Antenna Mapper, Trunked Networks** and **Open Source Collection**, as

well as links to the **TEXTA System** (see Chapter 4) and **Target Entities/Order of Battle** (see Chapter 6).

2.2 Adding a New COMINT Emitter

To add a new COMINT frequency, click the **Add** button on the toolbar and select **Add New COMINT Emitter**. Additionally, you can press the **F5** function key to open the **Add New Emitter** screen, however this automatically assumes that the emitter you wish to add is a COMINT emitter.

The key to building and maintaining the accuracy of the database is to gather as much intelligence as possible from an intercept, and that begins with the frequency intercept. The **Add New Emitter** screen allows for the entering of a wide variety of technical and circuit parameters as well as date, time and the location of the report so as to provide the fullest description of the intercept.



General

➢ **Signal Collection Number**. Note that each emitter is automatically assigned a Signal Collection Number (SCN). This number is unique to each intercept station and emitter

➢ **Originator**. This is the SIGAD or identification of the intercept station that initially logged this emitter.

➢ **RASIN Notation**. This is a reference notation that identifies an emitter and is globally unique.

➢ **TEXTA Case Notation**. Case Notation (CN) provides a powerful tool to grouping and cataloguing similar nets and circuits under the same heading. It is a system of classifying the function, purpose and ownership of a circuit as well as providing a common reference against which logs, reports, analysis and assessments can be made.

If no Case Notation is set, the emitter will be identified by the **Signal Collection Number**. To set a Case Notation, click the **TEXTA System** link. This will open the **Case Notation Selector** and after browsing the various Case Notations, the appropriate CN can be set. Once a CN is set against a, County and Service details can be amended in the **TEXTA Manager**. To clear the Case Notation, go back to the **Case Notation Selector** screen and click the **Clear** button.

➢ **TX Frequency**. All frequencies should be entered in frequency-units notation. In the example above, the frequency of 4470 kHz is entered as 4470K. This could also have been entered as 4.47M. A checksum will be automatically added to each frequency, thus 4470K will become 4470.000K5. This notation is used throughout HARVESTER.

➢ **Polarisation**. Polarisation is a property of that specifically describes an attribute of the transmitting antenna and is generally used in reference to VHF to EHF antennas. A number of broadband signals can be packed close together in a limited bandwidth without each channel causing interference to adjacent channels by having a diametrically opposing polarisation. This is used extensively on satellite communications systems where bandwidth is limited.

Circular	Linear
Circular, Left	Mixed
Circular, Right	Other
Dual	Rotating
Elliptical	Slant, Left
Horizontal	Slant, Right
Horizontal or Vertical selectable	Vertical

➢ **Modulation.** This describes the modulation of the intercepted signal.

8PSK	CW	DSB
AM	DBPSK	FEK
BPSK	DPSK	FM
COFDM	DQPSK	FQPSK-B

FSK	MSK	PSK
FSK OOK	NFSK	QAM 16
ISB	OOK	QAM 64
LSB	OQPSK	QPSK
MFSK	PCM	

➢ **Emission**. This describes the coding system used to modulate the intercepted signal. The current list contains 185 commonly heard COMINT modes intercepted across the entire RF spectrum. If the intercepted signal uses an emission that is not present in the list, please contact the Help Desk to have it added in the next data update.

802.11	CIS-14	G-TOR
81-29	CIS-14	Global Wireless Dataplex
81-81	CIS-27	GMDSS/DSC
ACARS	CIS-75	GOLAY
ALE	CIS-FSK	GSM
Algerian 4 Tone	Clover 2000	HARCO
Algerian 8 Tone	Clover II	HC-ARQ
ALIS	CODAN 16	Hellscreiber
ALIS-2	CODAN 81	Hellscreiber Feld
ANDVT	CODAN 8580	Hellscreiber PSK 105
ANUM-13	CODAN CHIRP	Hellscreiber PSK 245
APOC	CODAN SELCAL	HNG-FEC
APOR-VFT	Coquelet 13	HYPERFIX
ARCOTEL-ALE	Coquelet 8	INMARSAT A
ARINC HF Datalink	Coquelet 80	INMARSAT B
ARQ-E	Coquelet 82	INMARSAT C
ARQ-E3	Crowd 36	INMARSAT C TDM
ARQ-M2-242	CTCSS	INMARSAT C TDMA
ARQ-M2-342	Czech Diplo	INMARSAT M
ARQ-M4-242	DECCA	IRA-ARQ
ARQ-M4-342	DME	Japanese Mil 8-Tone
ARQ-N	DPRK-FSK	Link-11
ARQ6-70	DPRK-PSK	Link-11B
ARQ6-90	DRM	Link-16
ARQ6-98	DTMF	Link-4C
ASCII	DUP-ARQ	MEROD
ASCII-ARQ Czech	DUP-ARQ-2	MFSK-16
ASCII-ARQ Russian	DUP-FEC-2	MFSK-34
ASCII-Bulgarian	DVB	MFSK-8
ASCII-Slovak	EAS	MIL-STD-188-110A
AUTOSPEC	ECHOTEL-EAS	MOBITEX
Baudot	EDACS	Morse
BR6028	EEA	Moruz
BULG-ASCII	EIA	MS5 Fire
Bulgarian 8 Tone	ERMES	MT63
CIS 6-Tone Mazielka	EURO	NATEL
CIS-11	FAX	NATO RATT
CIS-11	FEC-A	NATO STANAG 4285
CIS-12	FLEX	NATO STANAG 4529

NATO STANAG 5066	PRC 32-Tone	Spread
NEXTEL	PRC 39-Tone	SSTV
NTSC	PRC 4+4	Super POCSAG
NUM13	PRC 8-Tone	SWED-ARQ
PACTOR	PSK31	Swedish Diplo
PACTOR 2	PSK63F	System3000
PACTOR 3	RAC-ARQ	Tadiran Data
PACTOR 4	REFLEX	Taiwanese FSK
PACTOR 5	ROU-FEC	TETRA
PACTOR 6	RS-ALIS	THROB
PACTOR 7	RS-ALIS 2	TOR-G
PACTOR II	RS-ARQ	TT2300B
PACTOR III	SECAM	Turkish 25-Tone
PAL	SI-ARQ	Twinplex
Piccolo	SI-FEC	Unknown
Piccolo 12	Singaporean FSK	VDEW
POCSAG	SITOR-A	VFT R39
POL-ARQ	SITOR-B	Voice
PRC 16-Tone	SKYFAX	Voice Cipher
PRC 19-Tone	Soviet 50	YUG Diplo

Additionally, there are a number of currently unknown emissions, which have been added to the list to enable logging and will be renamed once they are positively identified. These include:

UNID-RS-4FSK
UNID-RS-FSK-72
UNID-RS-FSK-162
UNID-XX-MFSK-12

The format of these unidentified emissions take the form of the UNID label followed by the Country Code, the Modulation type and a code which refers to some feature of the emission.

➢ **Receiver Mode and Bandwidth.** This is used to record the receiver modulation mode and audio bandwidth setting to aid intercept operators with further intercepts.

➢ **Callsign.** This is the fixed call sign used by the circuit's Net Control Station (NCS) or the fixed call sign used by the emitter, for example a merchant shipping shore station such as LZW, allocated to Varna Radio in Bulgaria. There is no history held against this call sign so call signs allocated randomly or on a rota system should not be stored here. These should instead be stored in the Call Sign log of the Intercept Operator's Log.

Properties

➢ **Signal Environment**. Defines whether an emitter exists in a terrestrial or satellitle environment.

➢ **Emitter**. Describes properties of the emitter:

Emitter Support FDM Multiplex. Describes whether or not the emitter supports a frequency division multiplexing baseband. If so, the bandwidth of the baseband is recorded in **FDM Bandwidth**.

First and Last Heard. Defines the first and last date that an emitter is recorded in intercept logs. These dates ar eautomatically updated when new logs are added.

TX Frequency Accuracy. Possibly of more use with historic, pre-digital receivers but can be used to describe the accuracy of the logged TX frequency. Possible values are:

- **Averaged**
- **Confirmed**
- **Estimated**
- **Measured**
- **Varying**

Emitter Obsolete Date. Defines the date that a particular emission is no longer operational.

Transponder. Used to record the channel name or transponder name that carries the logged circuit.

Emitter Part of Trunked Network. Used to flag whether or not the emitter is part of a trunked radio network. Detailed logging of trunked radio networks can be using the Trunked Networks Collection module.

- **Emission**. Describes properties of the emission:

RASIN Emission Number. This is a sequential number that refers to each emission attached to an emitter. The Radio Signal Notation prefix for the emitter can be found on the General tab.

Circuit Type. Described the main use of the circuit.

- **Broadcast**. This is a one-way flow of communications from sender to receiver with no return path.
- **Downlink**. This describes the downlink signal from a satellite or airborne platform.
- **Net**. This is a circuit of two or more stations communicating on single or multiple frequencies.
- **Point-to-Point Link**. This is a dedicated communications link between two sites or nodes.

- **Relay**. A Relay or Repeater acts to increase the path length of a signal by either boosting the signal at strategic points along the path or by routing the signal around obstacles that would otherwise prevent communications.

Uplink. This describes the uplink signal from the ground to a satellite or airborne platform

Signal Exchange Type. Describes the main type of signal exchnage behaviour operating on the circuit.

- **Broadcast**. This is a one-way flow of communications from sender to receiver with no return path.

- **Full Duplex**. This describes a system or channel that support simultaneous two-way communications. A classic example would be a land-line telephone.

- **Half Duplex**. This describes a system that support two-way communications using two operating frequencies or channels, but not simultaneously. An HF ship-to-shore radio telephone service is classic example.

Simplex. Similar to Half Duplex, except communications are carried out on a single operating frequency.

Frequency Use. Defines whether the frequency is used by the net control station or by out stations. This is particularly relevant with circuits that operate duplex frequency plans.

- **Control Station**. This is a one-way flow of communications from sender to receiver with no return path.

- **Out Station**. This describes a system or channel that support simultaneous two-way communications

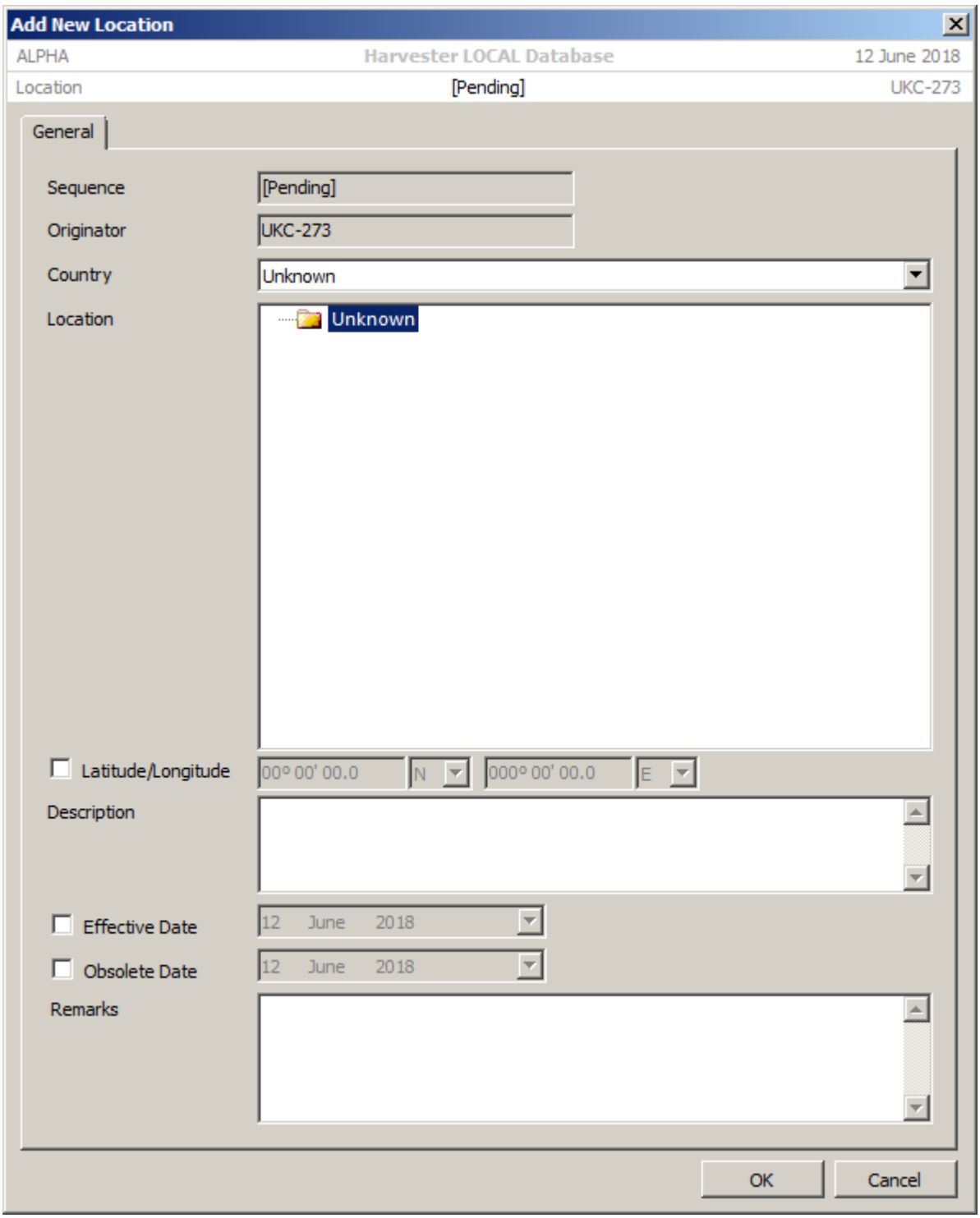
First and Last Heard. Defines the first and last date that an emission is recorded in intercept logs. These dates ar eautomatically updated when new logs are added.

Emission Obsolete Date. Defines the date that a particular emission is no longer operational.

Emitter Locations

When the location of individual emitters are identified through direction finding or by other means, it can be entered in the **Emitter Locations** tab on this Emitter screen. This tab supports multiple locations as might be seen in circuits which connect multiple station however we suggest that you only log fixed station locations. Mobile platform locations can be recorded against individual platforms in the Target Entities module.

Click the **Add** button to open the **Add New Location** screen.

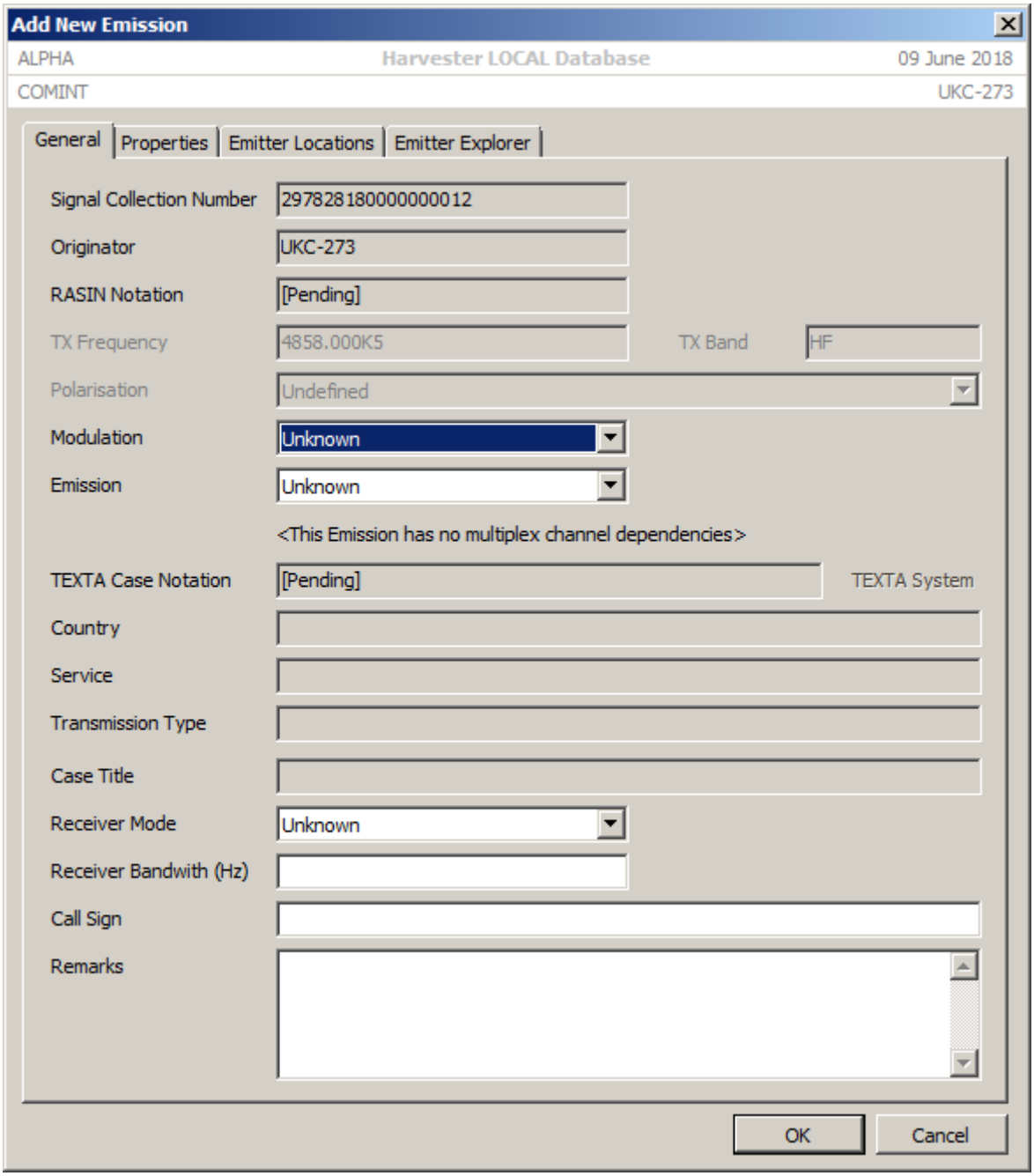


Emitter Explorer

The Emitter Explorer provides a useful overview of the emitter, the emissions attached to it and any multiplex channels supported by the emissions.

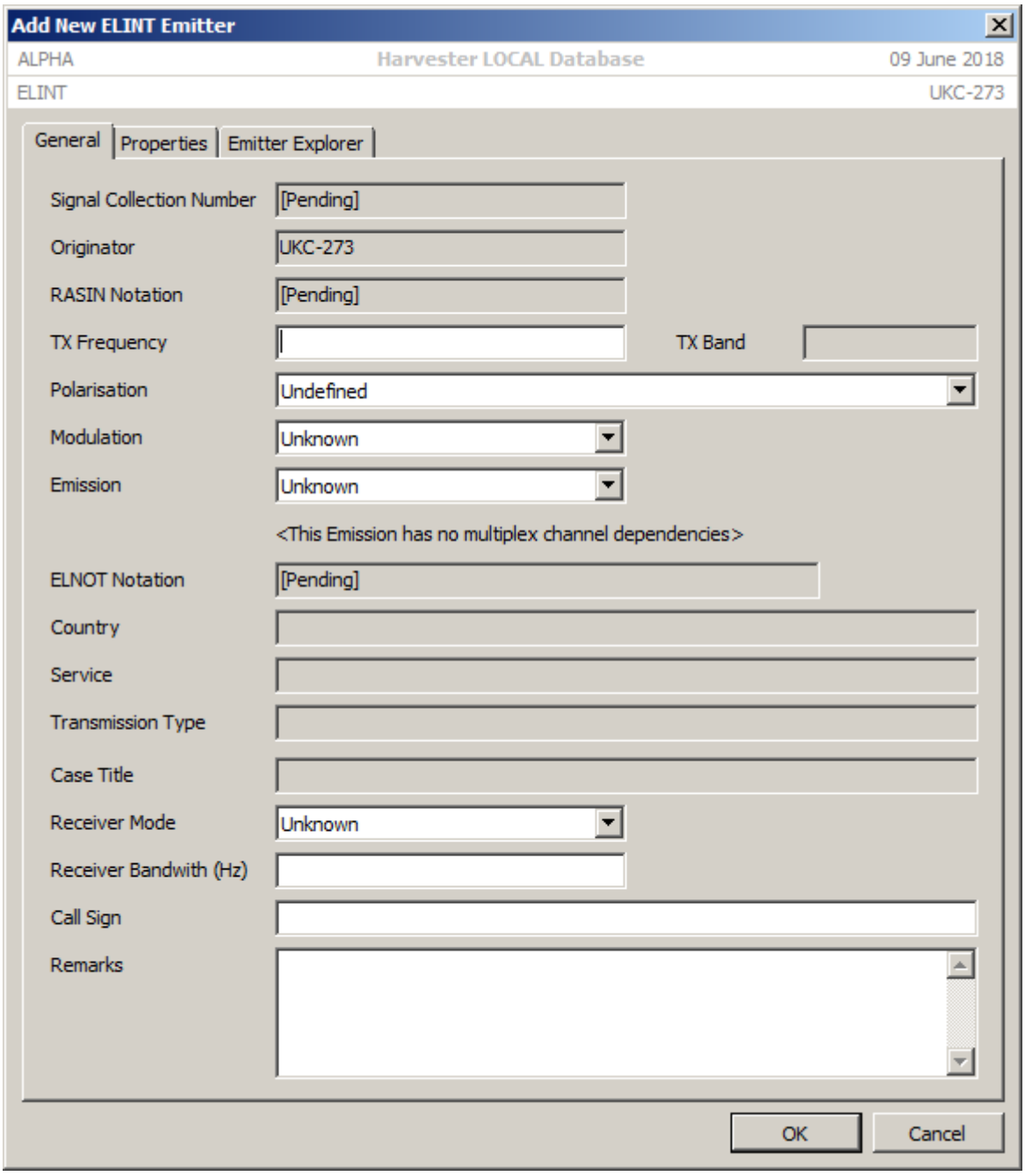
2.3 Adding a New COMINT Emission

To add a new COMINT emission, select the appropriate COMINT emitter then click the **Add** button on the toolbar and select **Add New Emission**. This will open the **Add New Emission** screen. Note that emitter specific fields such TX frequency, polarisation and the emitter details on the **Properties** tab with be populated but read only. These details can only be edited by selecting the primary emission attached to the emitter.



2.4 Adding a New ELINT Emitter

To add a new ELINT emitter, click the **Add** button on the toolbar and select **Add New ELINT Emitter** to open the **Add New ELINT Emitter** screen.



➢ **Emission**. This describes the coding system used to modulate the intercepted signal. The current list contains 10 commonly heard ELINT modes intercepted across the entire RF spectrum. If the intercepted signal uses an emission that is not present in the list, please contact the Help Desk to have it added in the next data update.

Chirpsounder	DME
DECCA	EPIRB

ILS Glideslope
ILS Localiser
Long-range Ocean Radar
NDB
OTHR System
TACAN
VOR

2.5 Frequency Tab Shortcut Menu

Each HARVESTER frequency tab has a shortcut menu that provides eleven options:

➢ **Add New**. Adds a new record.

- COMINT Emitter
- COMINT Emission

➢ **Delete**. This deletes the selected emitter or emission.

➢ **Quick Log**. This provides a quick method of creating one of seven pre-defined Search Logs:

- Broadcast
- Traffic
- Chatter
- Net
- Radio Check
- Idle
- Nil Heard

➢ **Sort by Case Notation**. Applies or removed frequency list sorting by Case Notation.

➢ **Open Search in New Tab**. Opens a new frequency tab using the current search query.

➢ **Open Case Notation in New Tab**. Opens a new frequency tab with a query based on the case notation of the selected emitter.

➢ **Open Country/Service in New Tab**. Opens a new frequency tab with a query based on the country and service of the selected emitter.

➢ **Open Country in New Tab**. Opens a new frequency tab with a query based on the country of the selected emitter.

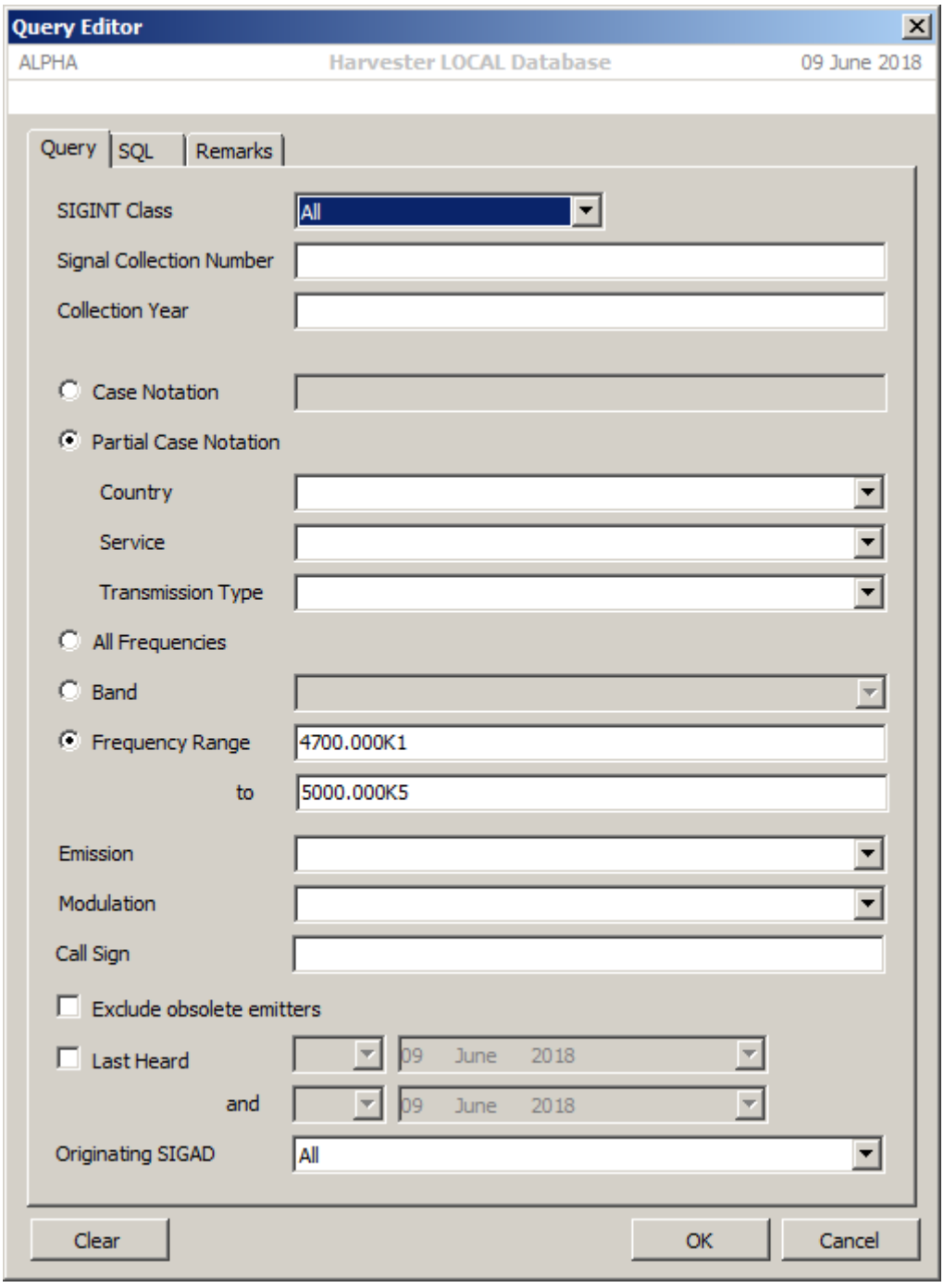
➢ **Open Service in New Tab**. Opens a new frequency tab with a query based on the service of the selected emitter.

➢ **Open Emission in New Tab**. Opens a new frequency tab with a query based on the emission of the selected emitter.

- **Refresh**. Refreshes the current frequency search.

2.6 Queries

One of the key features of any logging application is it's ability to search the existing frequency list to focus on specific regions of the spectrum, countries, users and emissions. This is done in HARVESTER by using the **Query Editor** which can be accessed on each frequency tab by clicking the **Query Editor** icon.



Using the Query Editor, searches can be built up from simple frequency range searches, to whole bands, specifying TEXTA case notations, counries, services, modulations and

emissions. Clicking OK will run the query and display the results in the currently selected frequency tab.

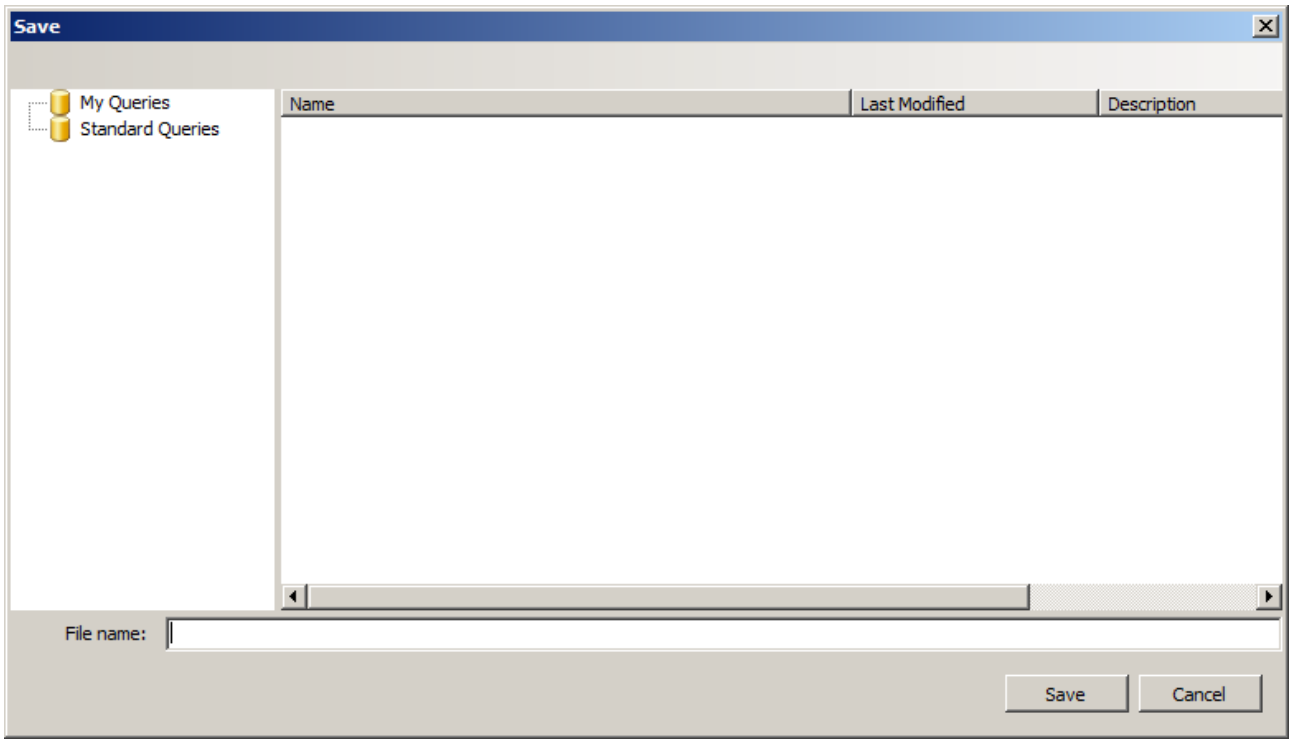
To save a query, click the Save button on the database tab toolbar. This will take you to the Save Query screen. The screen shows the two default query folders, My Queries and Standard Queries.

- **My Queries**. As the name suggests, the My Queries folder is specific to each intercept operator and is only accessible to that operator. Should the operator log into a different intercept positions, all their saved queries will still be available to them

- **Standard Queries**. Standard Queries offers a common shared area where queies commonly used by all operators can be saved. Any query saved in this folder will be accessible to all operators.

- **Tasking**. Though not displayed on the Save screen, there is a third folder which appears in the Queries panel on the main HARVESTER screen. This is designed specifically for operator tasking queries. These queries would be created for specific tasking requirements.

The My Queries and Standard Queries folders function like any normal hierarchical folder structure and operators can add new folders into which queries can be saved. To add a new folder, right-click on an exisiting folder and select the **New Folder** option.



Opening saved queries is done by navigating to the appropriate query in the **Queries** panel on the main HARVESTER screen and either double-clicking the query, right-clicking on it and selecting the **Open** option or clicking the **Open** icon in the toolbar.

2.7 Properties Panel

At the right hand side of the main HARVESTER screen is the **Properties** panel. This consists of four information tab that provide quick access to information about the selected emitter. The four tabs are:

- **Emitter Explorer**. The Emitter Explorer provides a useful overview of the emitter, the emissions attached to it and any multiplex channels supported by the emissions.

- **Calendar**. The Calendar provides a graphical representation of intercepts by time of day against the days of the week. It can be filtered to look at intercepts during the current day right up to all intercepts in the last year.

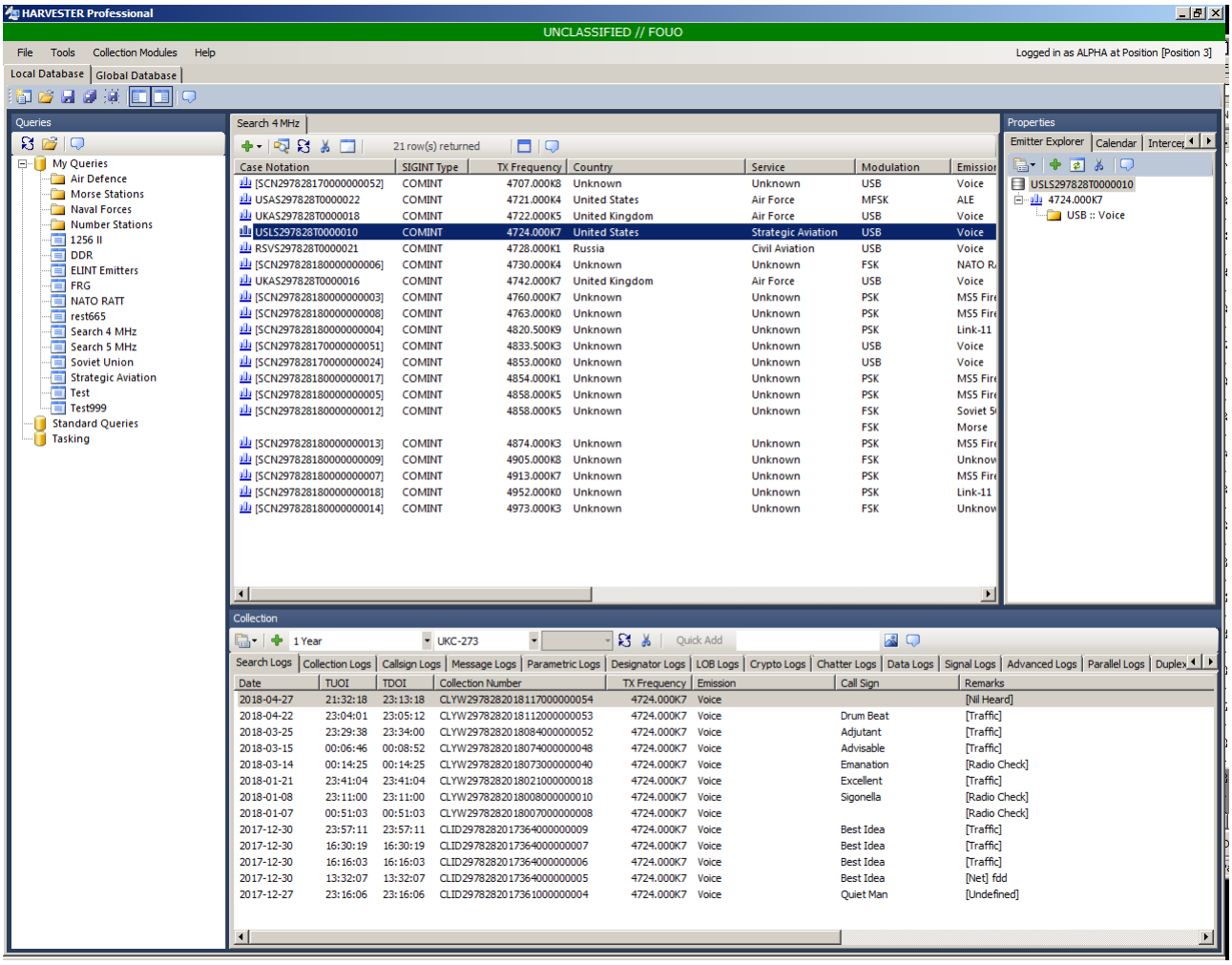
- **Intercept Dates**. This is very similar to Calendar but provides intercept days in a tabular form, including day name and the day of the year.

- **Emitter Locations**. This provides a list of the locations that have been added to the emitter on the Emitter screen.

3. Collection

signals intelligence (SIGINT): 1. *A category of intelligence comprising, either individually or in combination, all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted. [JP 1-02]* **2.** *Intelligence derived from communications, electronics, and foreign instrumentation signals. [JP 1-02]*

Once a frequency, emitter or channel has been logged in a search tab in the main **HARVESTER** screen, the business of intelligence collection can begin in earnest. Collection is an integral part of the Intelligence Cycle, forming the vital link between Planning and Processing. It is a key function in the development of any intelligence strategy and provides the raw material upon which intelligence assessments are based and confirmed. Collection is therefore an important part of the HARVESTER system that has been designed to aid in the gathering of any and all available intelligence from intercepted signals.

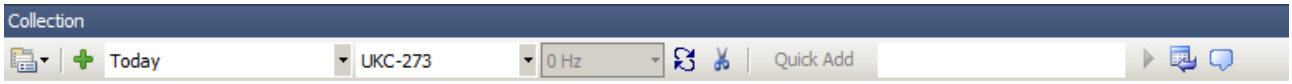


The main functions of intelligence collection are carried out within the **Collection**, which is located at the bottom of the main Harvester screen. This tool provides a family of generic intercept log forms covering most, if not all, intercept scenarios such as search logs, sustained collection logs, parametric logs, call sign lists, activity reports, Line of

Bearing (LOB) logs, chatter logs, data logs and message texts. Logs can be entered from both current real-time and historic intercepts.

NOTE All logs that span a period of time now use a Time Up of Intercept (TUOI) and Time Down Of Intercept (TDOI). These intercepts can only be logged against the specific Date of Intercept (DOI) and cannot extend past midnight UTC. Logs that continue after 23:59:59Z will end at 23:59:59Z on the initial Date of Intercept (DOI), then should be recommenced at 00:00:00Z on the following UTC day.

3.1 The Collection Toolbar



The logical flow of the screen begins with the **Toolbar**. It is used with all tabs and is made up of nine key items:

- **Group/Ungroup Case Notation**. Used to filter the types of logs that appear in each tab. They can be limited to the selected Emitter or the Case Notation attached to the emitter.

- **Add**. This button adds a new log screen for the selected collection tab.

- **Date Filter**. Allows the filtering of logs by 16 pre-defined date ranges.

- **SIGAD**. Allows filtering of logs by collector.

- **Bandwidth**. Allows filtering of audio files by bandwith. Not currently in use.

- **Refresh**. Refreshes the currectly selected tab.

- **Delete**. Deletes logs that have been incorrected added. User scan only delete their own station logs.

- **Callsign Quick Add**. This provides a quick method of added a callsign log. Simply enter the callsign and hit enter and the callsign will be logged against the selected emitter with today's date.

- **Play Audio Intercept**. Plays the selected audio intercept file in the Audio Files tab..

- **Import Logs**. This provides a method of importing certain log types from an external pre-formatted file.

- **Feedback**. User feedback is always important and this icon appears all through HARVESTER. It provides access to the Feedback screen where user suggestions, error reports and data requests can be logged.

3.2 Collection Tabs

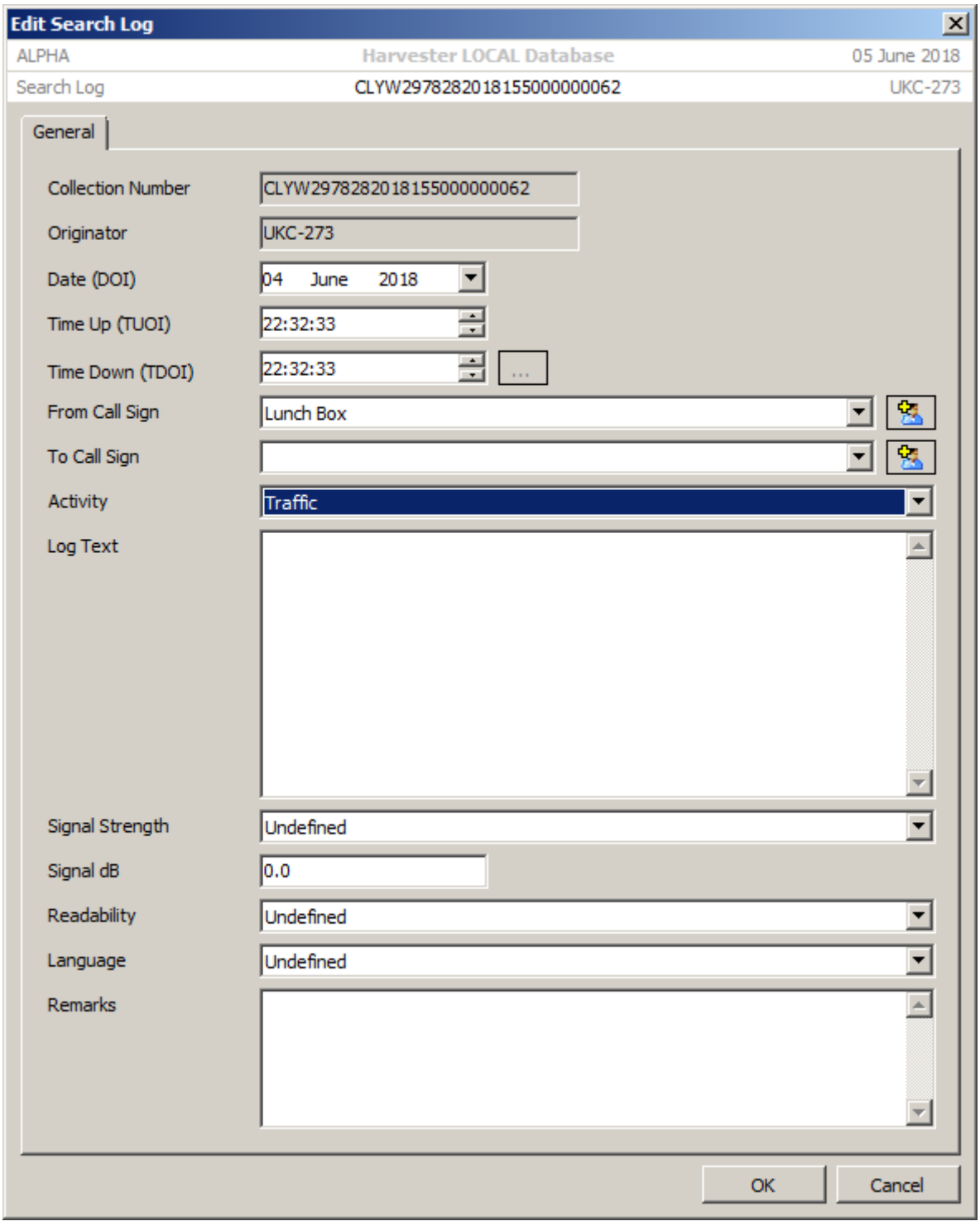
The **Collection** panel contains the majority of the most commonly used intercept logs within HARVESTER. Clicking on the appropriate button on the toolbar create the corresponding log. The log options are:

- **Search Logs**. Search logs are probably the most commonly used logs as they apply to most of the more common intercepted activities, such as logging a broadcast, a marker, a test, traffic, an idle or a net as well as a nil heard log.
- **Sustained Collection Logs**. Sustained Collection logs are best for targetted and tasked collection of circuits over extended periods of time. As their name suggests, these logs are intended to capture 24 hours worth of traffic, day after day.
- **Callsign Logs**. Callsign logs not only allow the logging of received callsign but can also be a useful guide to station activity, callsign trends and analysis.
- **Message Logs**. Message logs allows the logging of individual plain or cipher text messages along with sender details, distribution lists, internals and externals, routing indicators and handling instructions.
- **Parametrics Logs**. Provides a method of logging emitter and emission parameters.
- **Audio File**. This provides a method of storing audio intercept files against emitters.
- **Designator Logs**. A useful tool for logging the use of designators and channel identifiers heard on circuits that may refer to the intercepted circuit or another channel.
- **LOB Logs**. LOB or Line Of Bearing logs are key in the determination of transmitter locations. A set of accurate LOB logs obtained from several different locations provides data for the triangulation of the transmitter, leading to identifying it's position, and with it, revealing significant intelligence on it's purpose and it's user.
- **Crypto Logs**. Provides a useful method of logging encrypted system preambles, initialization vectors and system parameters.
- **Chatter Logs**. A chatter log provides a method of logging in real-time what is said by stations on the circuit.
- **Data Logs**. A data log provides a method of recording the internal data structure of an emission such as character bit length.
- **Signal Logs**. A signal log provides a method of describing a physical signal profile.
- **Parallel Frequency Logs**. Logs a list of frequencies on which a particular intercept is simultaneously heard. These logs are useful in schedule re-construction where frequency selection and grouping are fundamental parts of the station's schedule.
- **Duplex Frequency Logs**. Logs the duplex working frequency identified in a particular intercept.
- **ELINT Radar Parametrics**. ELINT Radar Parametrics logs the physical parameters associated with an intercepted radar signal.

NOTE The Collection Logs, LOB Logs, Audio Files, Chatter Logs, Crypto Logs, Data Logs, Signal Logs and ELINT Radar Parametrcis tabs are not available in the Lite Version.

3.2.1 General Search Logs

To open the **General Search Log** window, select the emitter and **Search Logs** tab then click the **Add** button on the toolbar. This will open the report form and pre-populate key fields with relevant information as Log Originator, Date of Intercept, Time Up and Time Down of Intercept. The Collection Number will appear as Pending until the log is saved, when a unique number will be generated.



➢ **Intercept Date.** Note that all Logs are logged according to the UTC day. For intercepts that continue past midnight UTC, they are logged to end at 23:59:59 on the first day and resume at 00:00:00 on the next day. Intercept Date is automatically set to the current date when the log is created, or if used in the Intercept Log screen, to the currently selected report date.

➢ **Time Up of Intercept (TUOI) and Time Down of Intercept (TDOI).** Both TUOI and TDOI are automatically set to the current time when the log is created. TDOI can be re-adjusted to the current time by clicking the **Set to Current Time** button.

➢ **Call Sign To and Call Sign From.** Whenever possible, every effort should be made to identify and report the call signs used by both sending and receiving stations on a circuit. Where call signs have already been added, the appropriate call sign relating to an intercept can be selected from the dropdown boxes.

To add a new Call Sign, click the Add New Call Sign button to the right of each Call Sign dropdown. This will change the dropdown to a text box to allow the new Call Sign to be entered. Hit the return key to accept the new Call Sign and this will automatically add the call sign to the Call Sign page and both Call Sign To and Call Sign From dropdowns.

➢ **Activities**. Activities are divided into seven generic categories, which can be used to broadly cover more or less every intercept event.

- **Broadcast**. A typical voice, video, fax or internet transmission. This includes commercial broadcasters, and broadcast feeders.
- **Chatter**. A conversation between two or more parties. This could be voice, Morse, teletype or any other two-way emission. Radio telephones
- **Idle**. Non-specific idle condition that includes Alpha, Beta and Reversals.
- **Marker**. A non-specific marker, such as CW, ARQ, Voice or some other form of transmission that is used to mark the channel. A short repeating transmission, often containing the station call sign, used to mark a circuit as being in use in between messages or traffic. Propagation beacons
- **Net**. A radio circuit supporting the operation of two or more stations, call signs or net participants.
- **Nil Heard**. It is just as important to log when a frequency is not active as when it is active, as non-activity might well provide crucial intelligence when attempting to reconstruct transmission schedules
- **Radio Check**. A radio check between two or more stations.
- **Test**. Any form of test transmission used by stations to test signal propagation and connectivity. These can take many forms of a teletype, video or voice test tape. These include a variety of test tapes designed to test every character on a telex system, such as THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG, VOYEZ LE BRICK GEANT QUE J'EXAMINE PRES DU GRAND WHARF and DAVID EXIGE PLAZO FIJO EMBARQUE URGENTE TRUCHAS NEW YORK 1234567890. REGLAGE.

- **Traffic**. General description for any transmission that carries some form of information. This includes a variety Voice and teletype transmission format used by some countries to send coded messages, including 4, 3/2 and 5 digit and letter groups.

➢ **Signal Strength**. This is a subjective assessment of the strength of the intercepted signal at the receiving site and will depend on atmospheric conditions and the receiving antenna as much as the effective radiated power of the transmitter. The options are:

- Very Strong
- Strong
- Good
- Fair
- Weak

➢ **Readability**. This is an operator's assessment of the ease with which a signal can be understood at the intercept location. The descriptions are broadly in line with the SINPO, RST or SIO codes with a few refinements and provide a reliability factor to the accuracy of the intercepted messages, chatter or text.

- Very Good
- Good
- Fair
- Poor
- Unreadable

➢ **Language**. Wherever possible, it is critical that the language used in an intercept be identified and logged. The **Language** field describes the predominant language used in a broadcast. The system currently contains the xx world languages, 97 of which are currently supported by linguists at the National Security Agency.

Afrikaans	Dutch	Iraqi
Albanian	Egyptian	Italian
Algerian	English	Japanese
Amharic	Estonian	Jordanian
Arabic	Farsi	Kazakh
Armenian	Finnish	Kirghiz
Azerbaijani	Flemish	Korean
Basque	French	Kurdish
Belarussian	Georgian	Kuwaiti
Bengali	German	Lao
Berber	Greek	Latvian
Bulgarian	Haitian Creole	Levantine
Burmese	Hebrew	Libyan
Cambodian	Hindi	Lingala
Chinese	Hungarian	Lithuanian
Czech	Icelandic	Macedonian
Danish	Ilacano	Malaysian
Dari	Indonesian	Moldovan

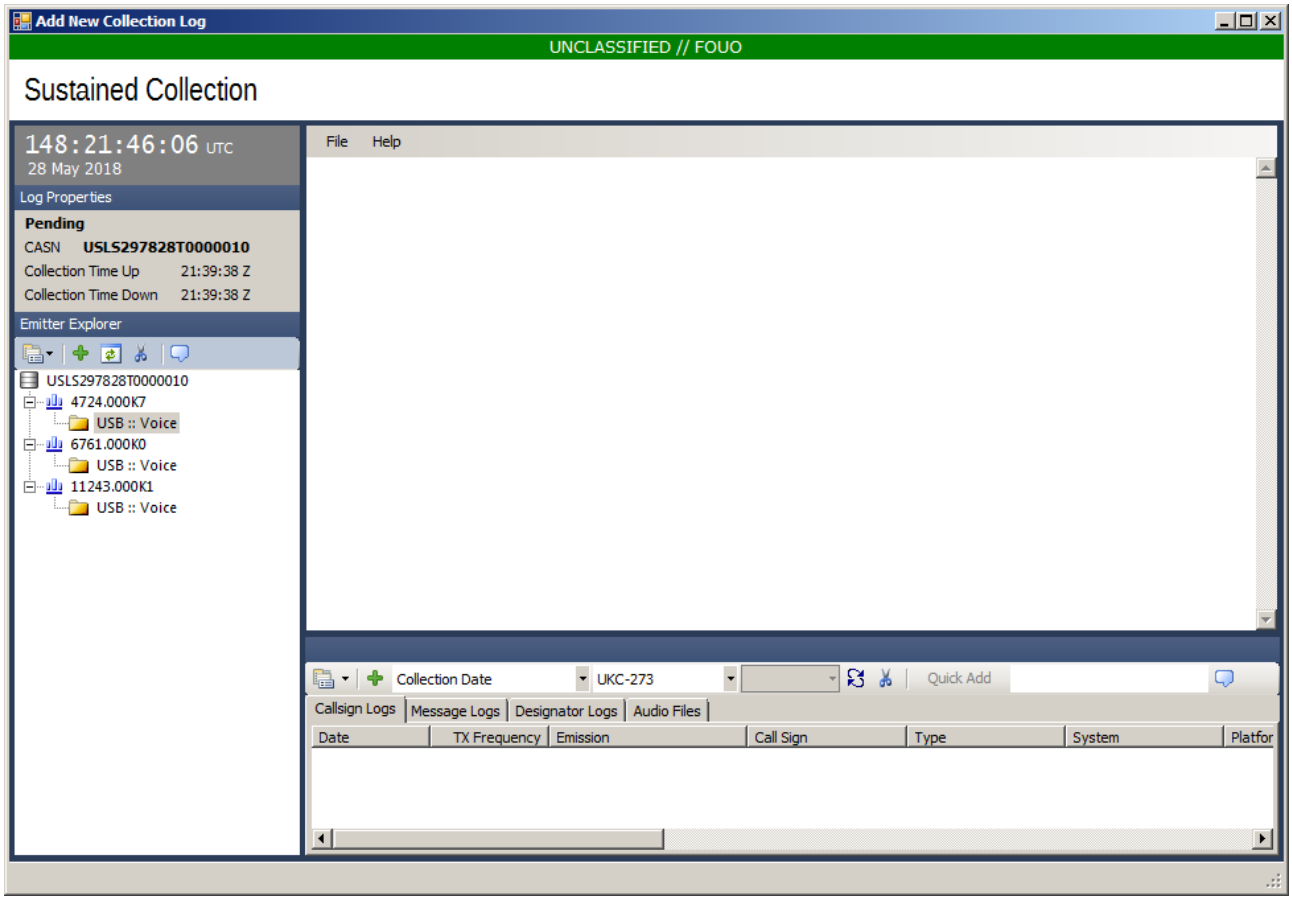
Mongolian	Serbo-Croatian	Thai
Moroccan	Sinhalese	Tibetan
Nepali	Slovak	Tigrinya
Norwegian	Slovene	Turkish
Papiamento	Slovenian	Turkmen
Pashto	Somali	Tunisian
Polish	Sotho	Ukrainian
Portuguese	Spanish	Urdu
Punjabi	Sudanese	Uzbek
Pushto	Swahili	Vietnamese
Quechua	Swedish	Visayan-Cebuano
Romanian	Syrian	Xhosa
Russian	Tajik	Yemeni
Saudi	Tamil	

- **Remarks.** An additional free-text area for operator notes and observations.

3.2.2 Collection Logs

Collection Logs focusses on sustained collection against a specific circuit or Case Notation. It supports a complete 24 hour cycle of collection with the ability to log callsigns, messages, designators and audio intercept logs. As this is primarily a collection screen, emission parametric, data and signal logs are not included.

To open the **Collection Log** window, select the emitter and **Collection Logs** tab then click the **Add** button on the toolbar. This will open the report form and pre-populate key fields with relevant information such as Date of Intercept, Time Up and Time Down of Intercept. The Collection Number will appear as Pending until the log is saved, when a unique number will be generated.



The top left panel of the screen provides a live clock displaying the day of the year, hours, minutes and seconds in UTC, as well as the calendar date. Below is the log properties panel which includes the automatically generated Collection Number, the Case Notation and the collection times of the log. These are amended automatically then the lag is saved. Below thatis the standard Emitter Explorer panel.

The log panel has a menu of tools that can be accessed by right-clicking th emouse anywhere on the text box. The options are:

➢ **Insert Frequency.** Inserts the currectly selected frequency into the text box, for example:

[4724.000K7]

➢ **Insert Frequency Details.** Inserts the currectly selected frequency and emission into the text box, for example:

[4724.000K7/Voice]

➢ **Insert Timestamp.** Inserts the current UTC time into the text box, for example:

[22:06:10]

➢ **Insert Operator Comment.** Inserts an empty set of double-brackets into the text box into which operators can add comments.

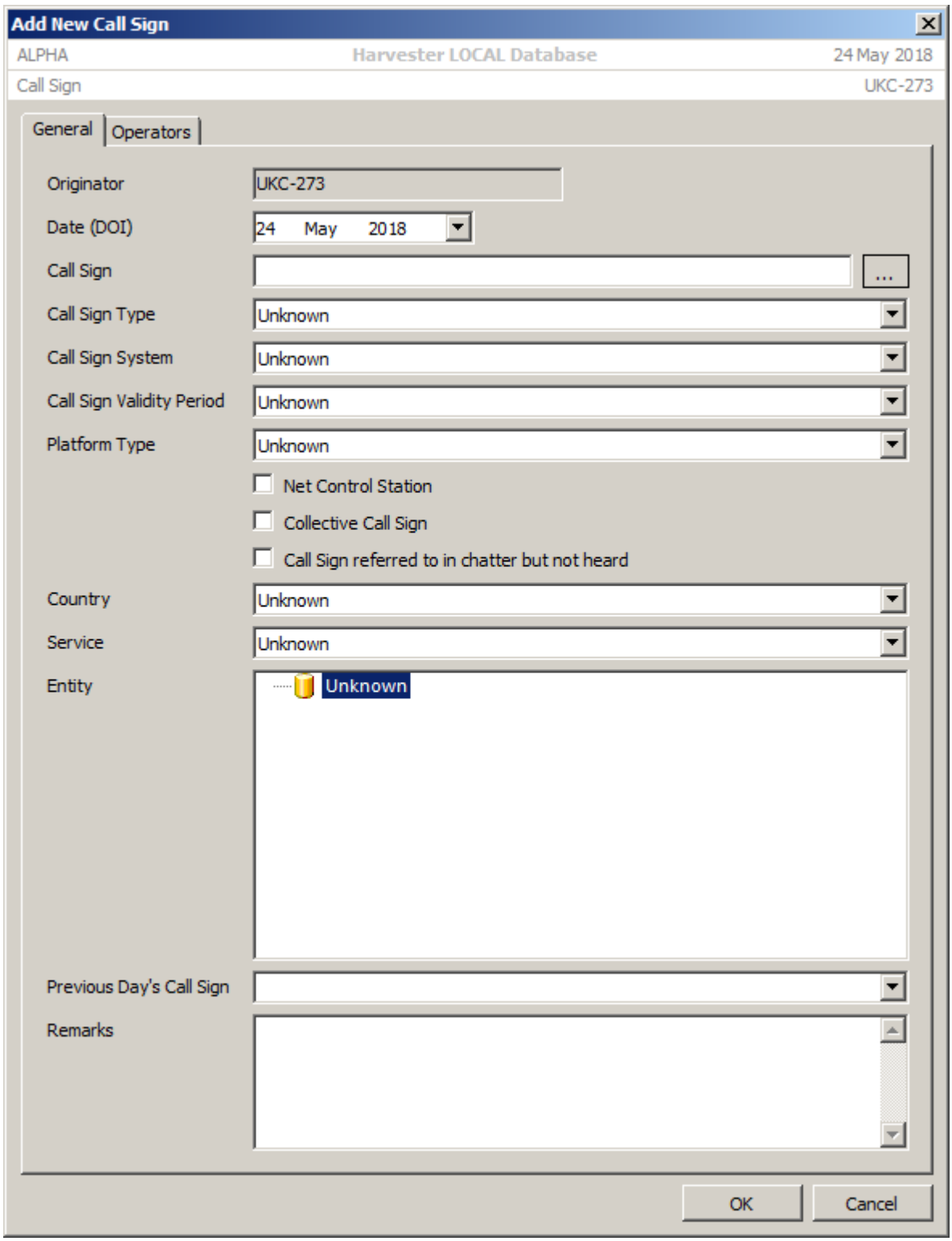
➢ **Log as New Callsign.** This allows the operator to select a portion of text from the collection log and log it as a callsign.

➢ **Log as New Message.** This allows the operator to select a portion of text from the collection log and log it as a message.

3.2.3 Callsign Logs

Call Signs provide far more than just a method of identifying a user. They can be used to track user activity over any number of networks and circuits, they can reveal the interactions of users operating on different circuits, and very often, their analysis can actually reveal the command structure of the network. Call Signs are therefore an important clue in the analysis of any communications system.

Call Signs can be added in the **Add New Call Sign** screen. To open the **Add New Call Sign** screen, select the emitter and **Callsign Logs** tab then click the **Add** button in the toolbar. The current UTC date and time are automatically set on screen. To add an historic call sign intercept, both date and time can be amended.

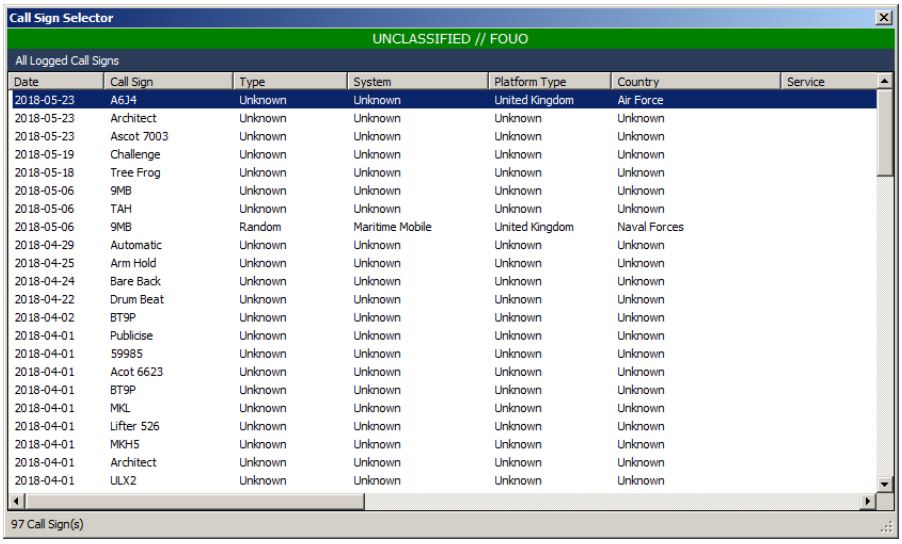


➢ **Date of Intercept**. This is automatically set when the screen opens and reflects the 24-hour UTC period during which the call sign was active. It should be noted that countries not conforming to the standard UTC day, such as former Soviet Republics, might well use call signs which remain current after midnight UTC. In such a case, the call sign will require to be logged on both days.

➢ **Call Sign**. The intercepted call sign should be entered in the **Call Sign** text box. Beside this box is a function button that allows various database searches to be performed on the entered call sign. There are twelve search options available:

- **Call Signs Logged Today.** Provides a list of all call signs logged on all frequencies during the current UTC day.
- **Previous Day's Call Signs.** Provides a list of all call signs logged on all frequencies during the previous UTC day.
- **Call Sign Matches (Partial).** Provides a list of all call signs logged on any frequencies that match the entered call sign. The list will include exact and partial matches.
- **Call Sign Matches (Exact).** Provides a list of all call signs logged on any frequencies that match exactly the entered call sign. The list will include only exact matches.
- **Country Call Signs**. Provides a list of all the call signs that have been logged to **County** defined **Call Sign Entity.**
- **Service Call Signs.** Provides a list of all the call signs that have been logged to **Service** defined **Call Sign Entity.**
- **Country/Service Call Signs.** Provides a list of all the call signs that have been logged to **County** and **Service** defined **Call Sign Entity.**
- **User Call Signs.** Provides a list of all call signs used by the owner of the selected frequency.
- **All Call Signs Previously Logged on this Circuit.** Provides a list of all the call signs previously logged on the selected frequency.
- **All Call Signs Previously Logged on this Case Notation.** Provides a list of all call signs logged on the selected Case Notation. This option is only available when the cal sign is being added to a circuit that has a defined Case Notation.
- **All Call Signs.** Provides a list of all call signs logged on all frequencies.

These searches can be used to confirm if the call sign has been used elsewhere or simply to confirm spelling. Once you have found the call sign that best matches your current intercept, double-click the entry to load all details into the **Add New Call Sign** screen.



➢ **Call Sign Type**. This defines the specific call sign class to which the intercepted call sign belongs, and includes:

ACARS Address	Maritime Mobile Selcal
Aircraft Registration	Maritime Selective Call Number
ALE	Pager Address
Fixed Service Maritime Selcal	Routing Designator
Fixed Service Selcal	Tactical
Flight Number	Unknown
ICAO24 Mode-S Address	Voice Call Sign
ITU	

➢ **Call Sign System**. This defines the behaviour of the call sign, whether it is **Random** as is the case with most **Tactical** call signs, **Rota** as is the case with **Flight Number** call signs, or **Semi-Permanent**, **Static, Temporary** or **Unknown**.

➢ **Call Sign Validity Period**. This defines the length of time that the call sign is valid. Values range from 3 hours to permanent as well as a Mission/Flight option.

➢ **Platform Type**. This described the call sign platform where known. The actual national and physical identity of the platform can be described in the **Platform** box but where this information is not available, **Platform Type** represents an intuitive or best guess.

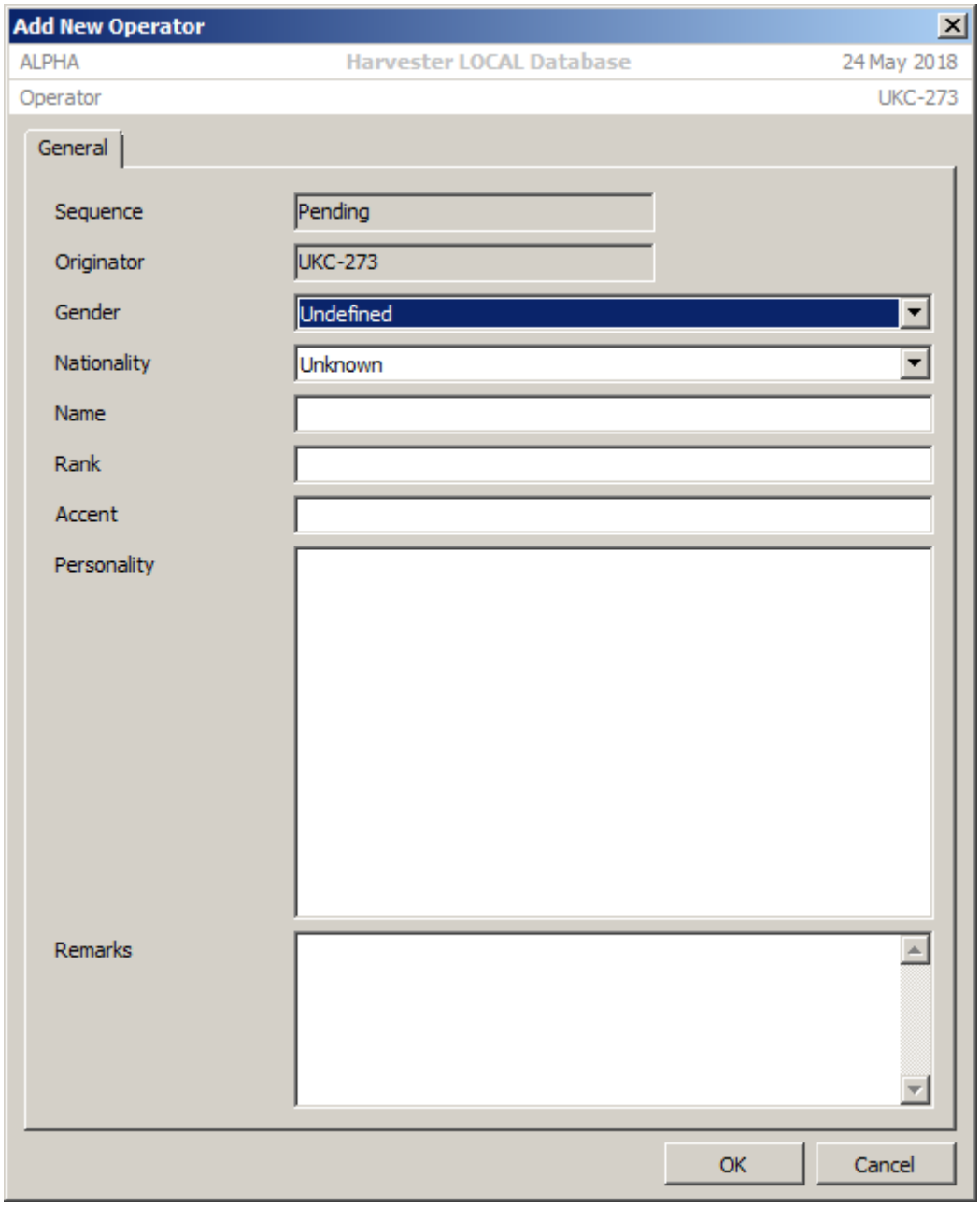
➢ **Net Control Station and Collective Call Sign**. These tick boxes are used to denote whether a particular call sign is assigned to the Net Control Station or whether the used as a collective call sign to call all members of a net. Both details can provide valuable clues in analysing network behaviour and structure.

➢ **Call Sign Entity**. **Call Sign Entity** deals with the physical identity of the call sign, which country is belongs to, which service is using it, and ultimately what echelon and platform which the service. Very often this information will remain unidentified. Once **Country** and **Service** have been selected, the **Organisation** box will be populated with all **Organisation** attached to that **Country** and **Service**. Selecting **Organisation** automatically populates the **Echelon/Function** and **Platform** lists. This is driven from the **Target Entities** module.

➢ **Previous Day's Call Sign**. This box is used to track the daily changes in tactical call signs. This option is particularly useful during large-scale exercises when operators' shifts span the daily midnight change of call sign. By matching voices, unit call signs can be tracked for the duration of the exercise.

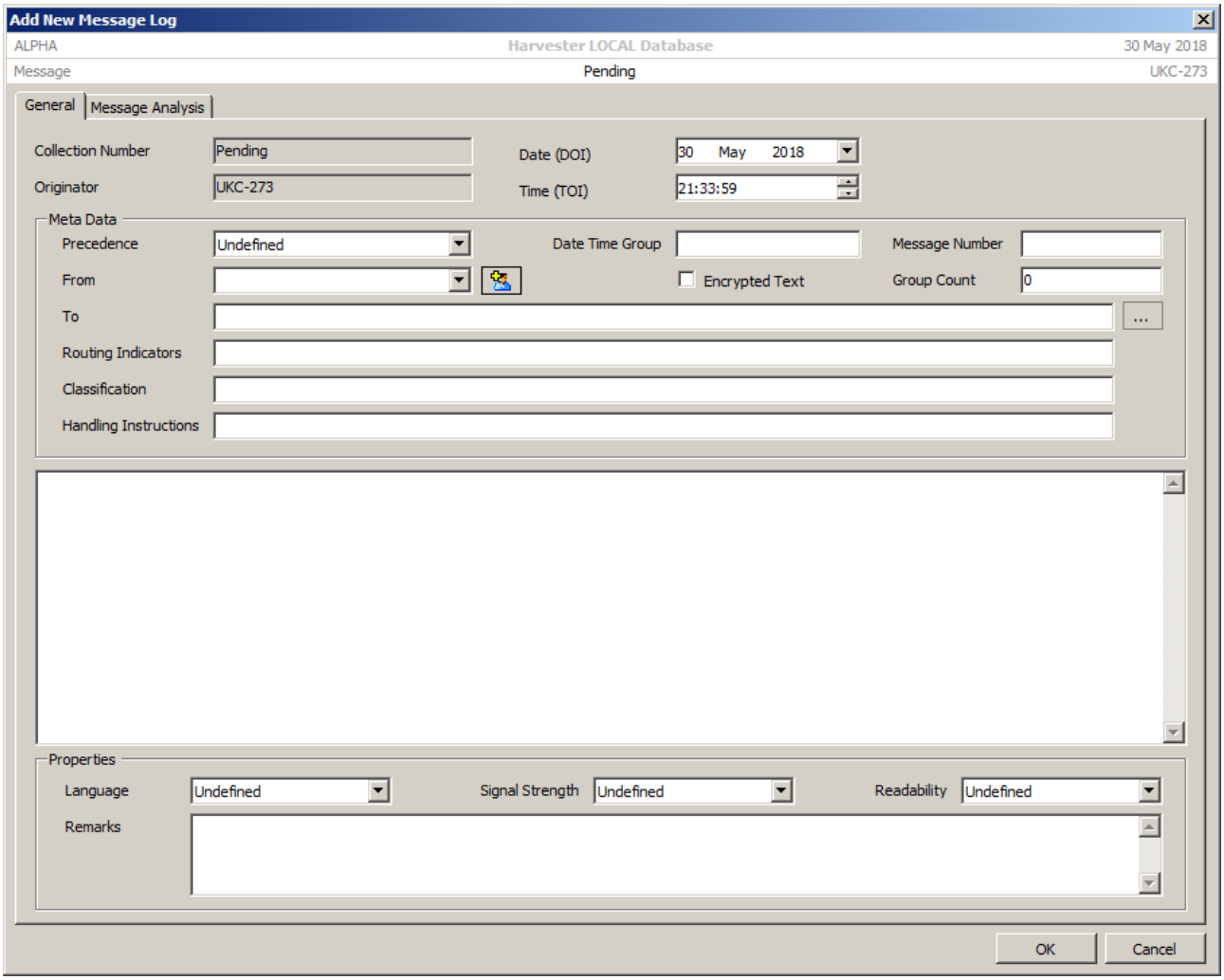
The Operators Tab

The Operator tab allows detailed descriptions of the operators at each call sign to be kept. Details such as **Gender**, **Nationality**, **Accent** and, where known, **Name** can all be used to build up a picture of call sign.



3.2.4 Message Logs

To open the **Message Log** window, select the emitter and **Message Logs** tab then click the **Add** button in the toolbar.. This will open the report form and pre-populate key fields with relevant information as Log Originator, Date of Intercept, Time Up and Time Down of Intercept. The Collection Number will appear as Pending until the log is saved, when a unique number will be generated.



➢ **Date and Time of Intercept**. Both DOI and TOI are automatically set to the current date and time when the log is created. These can be adjusted if the log being entered is historic.

➢ **Precedence**. This is used to record the level of urgency of the message. There are four levels of precedence in order of decreasing importance:

- **Flash**. The message must be delivered to recipients within 10 minutes.
- **Priority**. The message must be delivered to recipients within 30 minutes.
- **Immediate**. The message must be delivered to recipients within 3 hours.
- **Routine**. The message must be delivered to recipients within 6 hours.

➢ **Date Time Group**. When a message is prepared, it is a time stamp in the form of a date and time group. This is most commonly composed of the day of the month and the time is hour and minutes, such as 230728 meaning the 23rd day of the month at 0728. Frequently this group is suffixed by the time zone code and occasionally the month and year. Date Time Groups are usually expressed in UTC, or Zulu, though there are notable exceptions, such as the as former Eastern Bloc countries and the CIS .

➢ **Message Number**. All messages are uniquely identified by a message or serial number. This number very often represents a count of the number of messages send on a

particular network on a particular day. The serial number could equally have been selected from a pool of available message numbers.

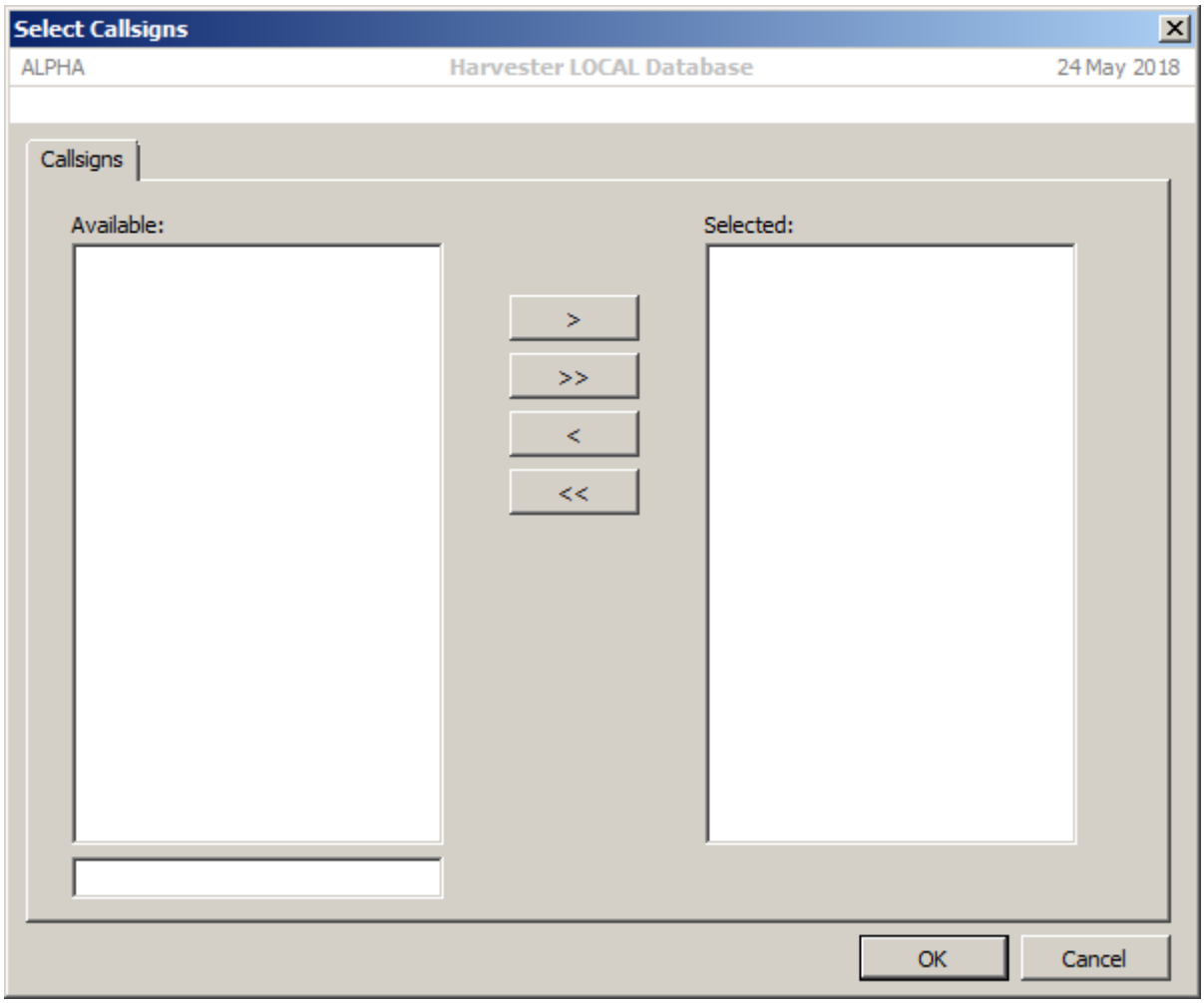
➢ **Group Count**. A count of the number of groups, or words, in a message. This number excludes any date or time groups, and any recipient addressee groups.

➢ **Encrypted Text**. This checkbox is used to indicate that the message text is encrypted, either on-line or off-line. The functions as filter during later analysis.

➢ **From and To**. It is essential in the analysis of traffic and messages that both the sender and the recipient or recipients are logged. To achieve this, call sign fields are provided for both sender (**From**) and recipients (**To**). The sender call sign can be selected from the dropdown list, or this if it is a new call sign, can be added by clicking the **Add New Call Sign** button.

Recipient call signs are handled in a slightly different to take into account the fact that a message may have more than one recipient. To all a recipient call sign, click the ellipsis (…) to the left of the **To** box to open the **Message Recipients** window.

Simply click the add or remove buttons to move **Available Call Signs** over to the list of **Message Recipients**. To add a new call sign, enter the call sign in the text box beneath the **Available Call Signs** list and hit Return. Click **OK** to close the window and an alphabetically ordered list of message recipient call signs will be displayed in the **To** box.



➢ **Routing Indicators**. Routing Indictors are handled in exactly the same way as message recipients.

➢ **Classification**. Occasionally, messages will carry some form of security classification. In most cases, this will be Unclassified or UNCLAS, however higher classifications have been observed.

➢ **Handling Instructions**. Handling instructions provide recipients with instructions on how the message is to handled, and distributed, upon receipt.

➢ **Message Text.** This free-text area provides ample storage for the message text.

The Analysis Tab

Additional information that will be useful to both traffic analysts and cryptanalysts, such as message discriminant, message internals and externals and group count, which can all be logged to aid later analysis.

➢ **First and Last 5 Groups**. In Traffic Analysis (TA), Message Externals and Internals

➢ **Message Externals and Internals**. In Traffic Analysis (TA), Message Externals and Internals provide a valuable insight into the way messages are constructed and what procedures are used to format, handle and transmit them. Message Externals focus on the information sent immediately before and after a message while Message Internals focus on the actual message contents, be that plaintext or cipher text.

3.2.5 Parametric Logs

To open the **Parametric Log** window, select the emitter and **Parametric Logs** tab then click the **Add** button in the toolbar.. This will open the report form and pre-populate key fields with relevant information as Log Originator, Date of Intercept, Time Up and Time Down of Intercept. The Collection Number will appear as Pending until the log is saved, when a unique number will be generated.

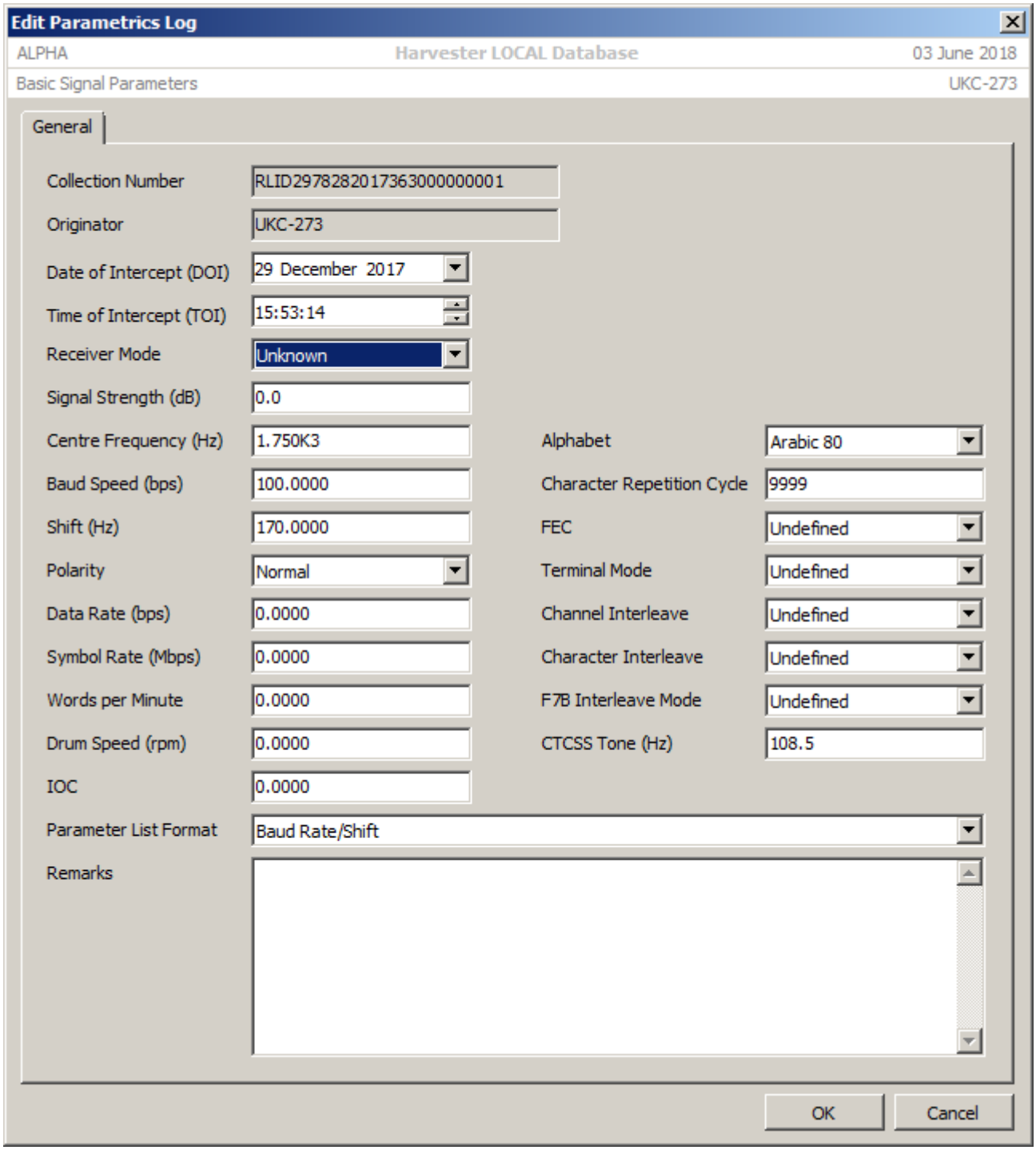
➢ **Date and Time of Intercept**. Both DOI and TOI are automatically set to the current date and time when the log is created. These can be adjusted if the log being entered is historic.

➢ **Receiver Mode**. When measuring signal parametrics, their values can be influenced by the mode of the receiver. Therefore it is essential that a note be made of the receiver mode so that the measurements can be reproduced.

➢ **Centre Frequency**. This is the centre frequency of the intercepted signal.

➢ **Baud Speed**. The telegraphic speed of a signal. Signal speeds can also be measured as Data Rate or Symbol Rate. Morse signals are measured in Words per Minute and Fax signals as Drum Speed.

➢ **Shift**. This is the measure of the separation bewteen the tones of a signal.



➢ **Parameter List Format**. This is used to define the way parameters are displayed against an emission. There are 4 options: Baud Rate/Shift, Words Per Minute, Drum Speed/IOC or Baud Rate/Data Rate/Interleave.

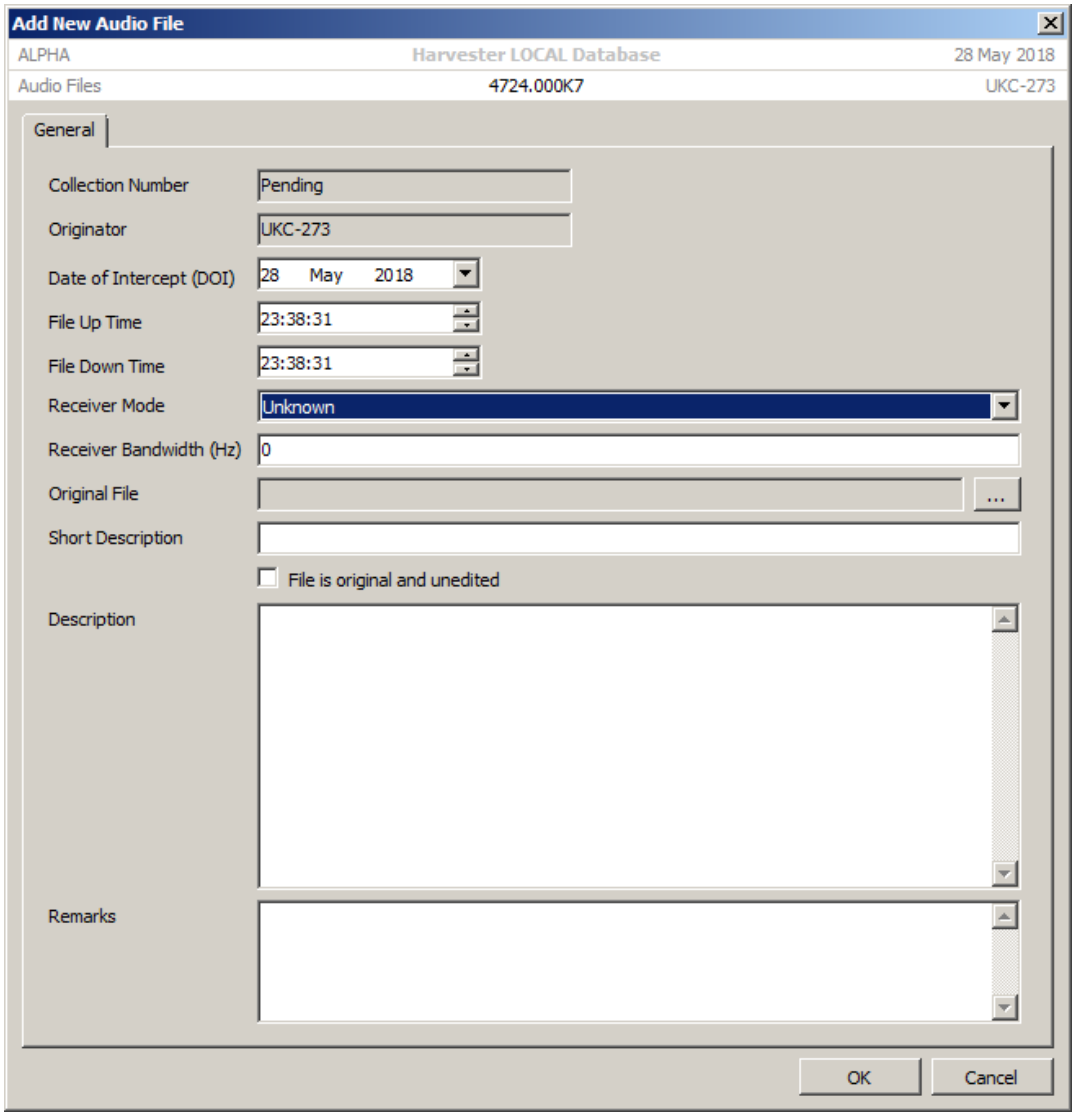
3.2.6 Audio Logs

Audio Intercept recordings have repeatedly proved to be a valuable addition to any intercept session. Whether a piece of information has been missed during collection the

live intercept or a sequence of events has to be confirmed, having an audio record is almost essential. In the days of reel to reel recording, intercept operators were required to avoid recording extended periods of silence between communications exchanges but with today's relatively inexpensive digital storage and file compression technology, operators can afford to record entire intercept sessions.

NOTE If recording intercept sessions is not already part of your intercept procedures, considerintroducing introducing it to your collection activities.

To open the **Audio Intercept Log** window, select the emitter and **Audio Logs** tab then click the **Add** button in the toolbar.. This will open the report form and pre-populate key fields with relevant information as Log Originator, Date of Intercept, Time Up and Time Down of Intercept. The Collection Number will appear as Pending until the log is saved, when a unique number will be generated.



➢ **Date and Time of File**. Both DOI and TOI are automatically set to the current date and time when the log is created. These can be adjusted if the log being entered is historic. The Up and Down times reflect the entire duration of the audio intercept though that actual file length may be if the file has been edited post-intercept.

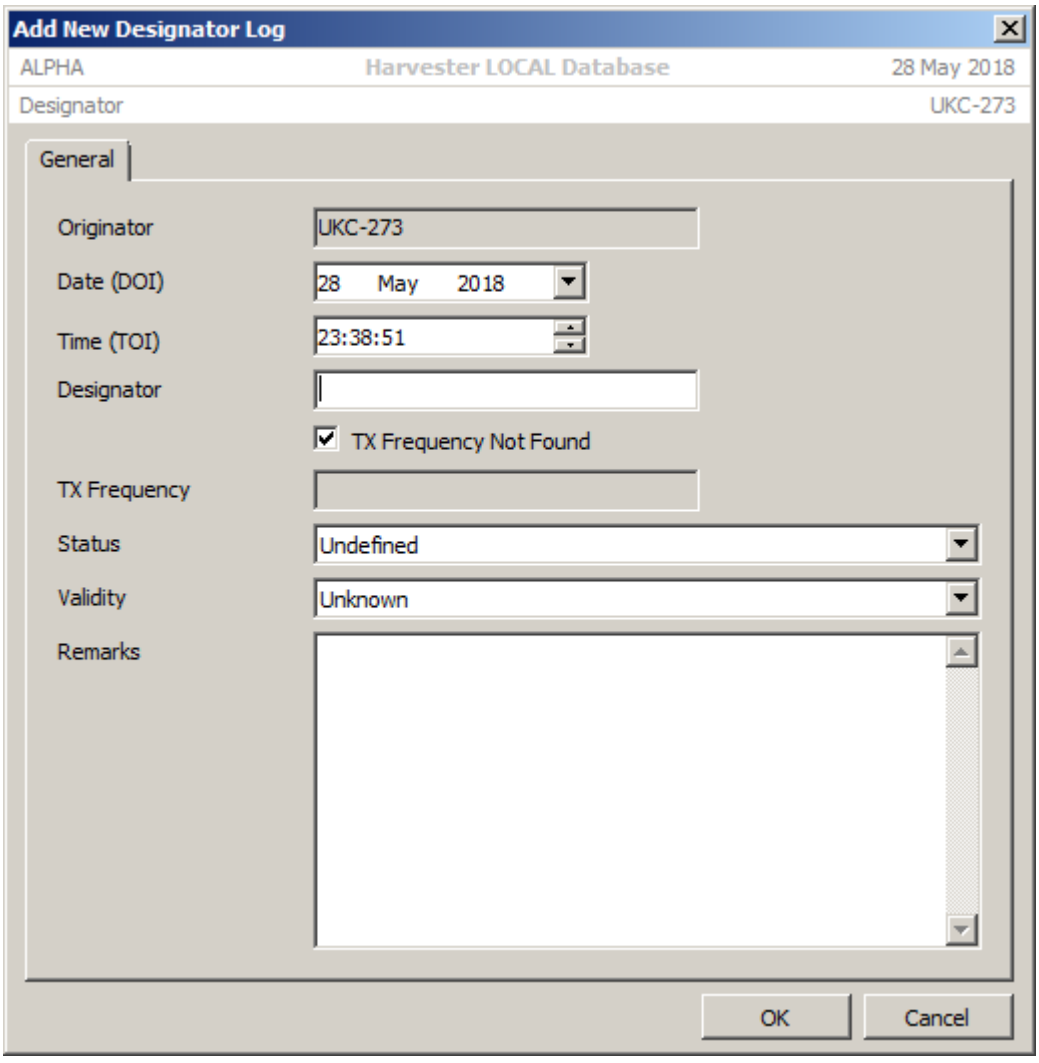
➢ **Receiver Mode and Bandwidth**. Both DOI and TOI are automatically set to the current date and time when the log is created. These can be adjusted if the log being entered is historic.

➢ **Original File**. Click the elipsis button to select the audio file to import. The Original File will always display the original location and filename of the file.

➢ **File is original and unedited**. Click this option to indicate that the audio file is raw, unedited and as it was recorded of the air with the length of the recording reflecting the duration of the intercept.

3.2.7 Designator Logs

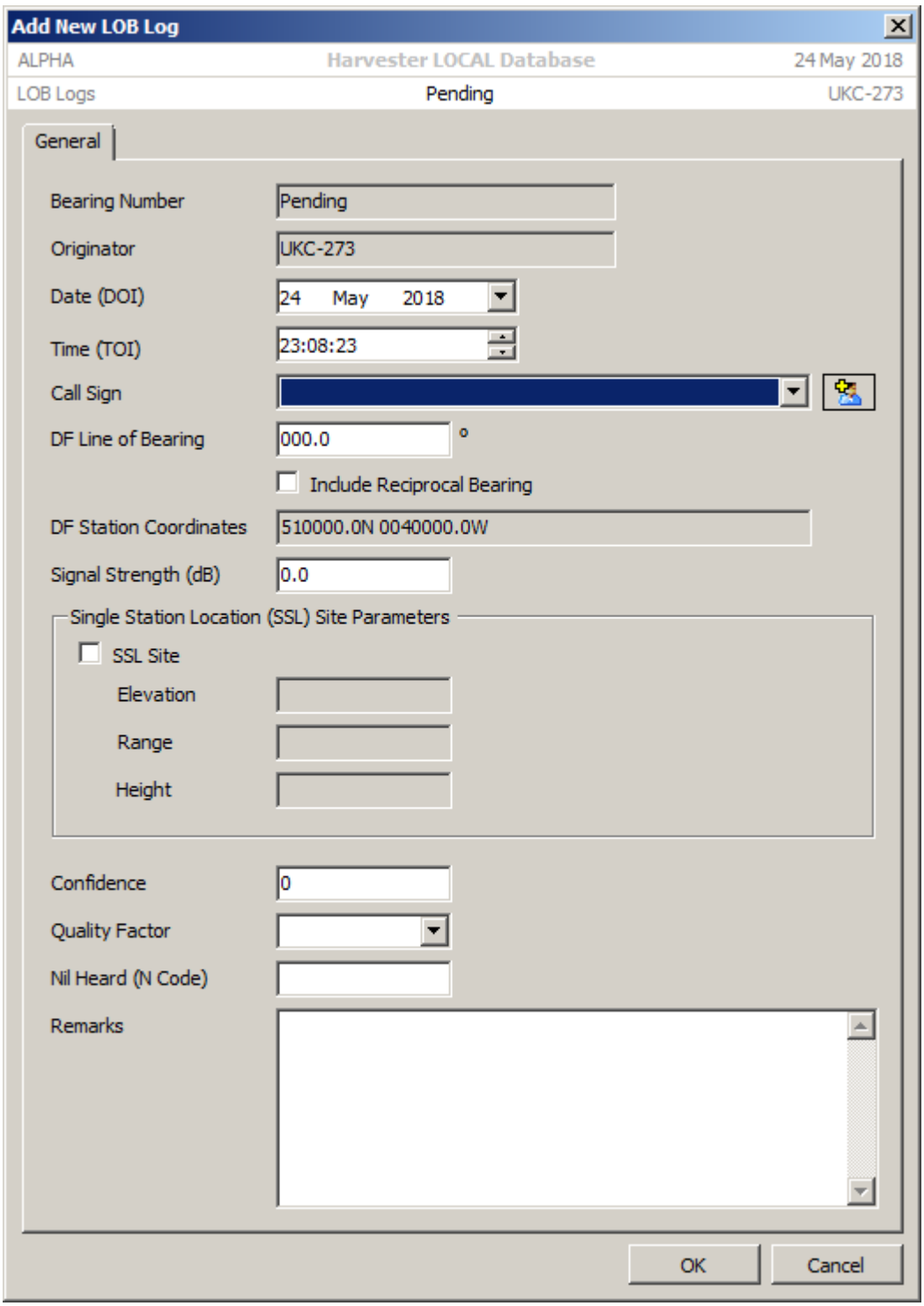
To open the **Designator Log** window, select the emitter and **Designator Logs** tab then click the **Add** button in the toolbar.. This will open the report form and pre-populate key fields with relevant information as Log Originator, Date of Intercept, Time Up and Time Down of Intercept. The Collection Number will appear as Pending until the log is saved, when a unique number will be generated.



3.2.8 LOB Logs

One of the primary methods of identifying the source of an intercepted signal is by Direction Finding, or DFing. This can be carried out by a number of directional antennas giving a bearing to the location of the signal's origin. By obtaining a number of lines of bearing from several different sites and plotting these lines on a Great Circle map, the natural the point of intersection of these Lines Of Bearing (LOB) reveal the approximate location of the transmitter.

To open the **LOB Log** window, click the **Add** button on the toolbar. This will open the report form and pre-populate key fields with relevant information as Log Originator, Date of Intercept, Time Up, Time Down of Intercept and the DF site's Latitude and Longitude. The Collection Number will appear as Pending until the log is saved, when a unique number will be generated.



➢ **Date and Time of Bearing**. Both date and date are automatically set to the current date and time when the log is created. These can be adjusted if the log being entered is historic.

➢ **Call Sign**. This provides a list of the call signs noted as active on the selected frequency. Select the **Call Sign** of the station for which the LOB has been obtained, or if the **Call Sign** is no already in the list, click the **Add New Call Sign** button and enter the new call sign, hitting the return key when finished.

➢ **Bearing Number**. This is a running count of the number of bearings taken on a specific frequency in any 24-hour period. This number provides a useful reference when plotting bearings. The number is automatically generated by the system.

➢ **DF Line Of Bearing**. The **DF Line Of Bearing** of the signal represents the bearing of the transmitter site from the receiver site and can be entered to an accuracy of 0.1º.

➢ **Single Station Location (SSL) Sites**. Both date and date are automatically set to the current date and time when the log is created. These can be adjusted if the log being entered is historic.

- **Elevation**
- **Range**
- **Height**

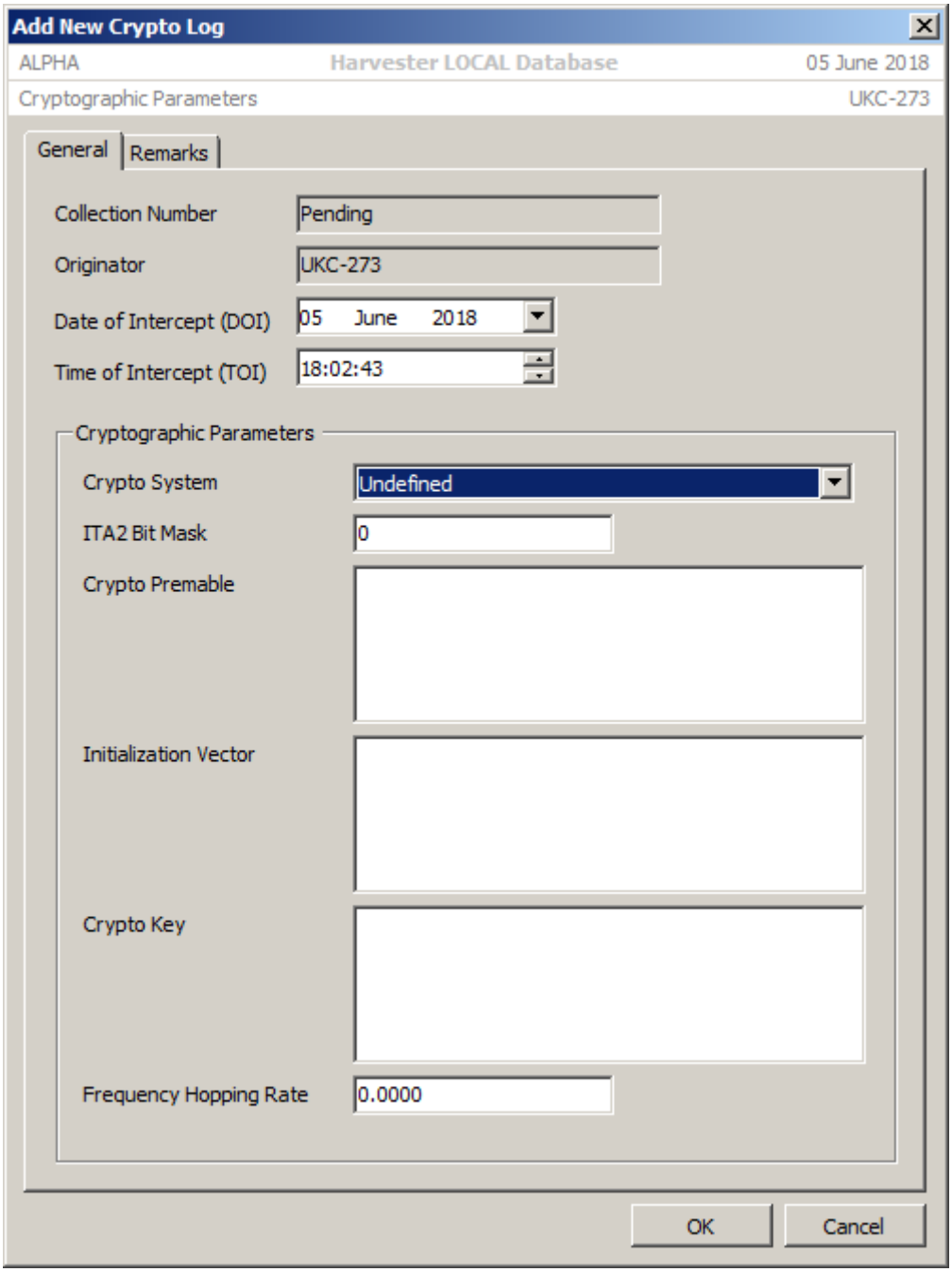
➢ **Confidence**. This is an objective assessment made by the intercept operator of the overall quality of the LOB, taking into account atmospheric conditions, the strength of the signal and the effectiveness of the DF antenna

➢ **Quality Factor**. This is an objective assessment made by the intercept operator of the overall quality of the LOB, taking into account atmospheric conditions, the strength of the signal and the effectiveness of the DF antenna.

➢ **Nil Heard**. This option provides a method for logging failed LOB attempt when a LOB fix has been requested on a signal, but the signal is inaudible at the intercept location.

3.2.9 Crypto Logs

To open the **Crypto Log** window, select the emitter and **Crypto Logs** tab then click the **Add** button in the toolbar.. This will open the report form and pre-populate key fields with relevant information as Log Originator, Date of Intercept, Time Up and Time Down of Intercept. The Collection Number will appear as Pending until the log is saved, when a unique number will be generated.



➢ **Crypto System**. This is used to description the generic type of encryption used by the intercepted signal.

➢ **ITA2 Bit Mask**. This is one of the simplest ways to obfiscate an online system by performing a fixed XOR operation on the character's bits.

➢ **Crypto Preamble**. This is a fixed binary preamble that is used to signal the start of an ecrypted message. These preambles are used by encryption devices to synchronise the device to the incoming binary stream.

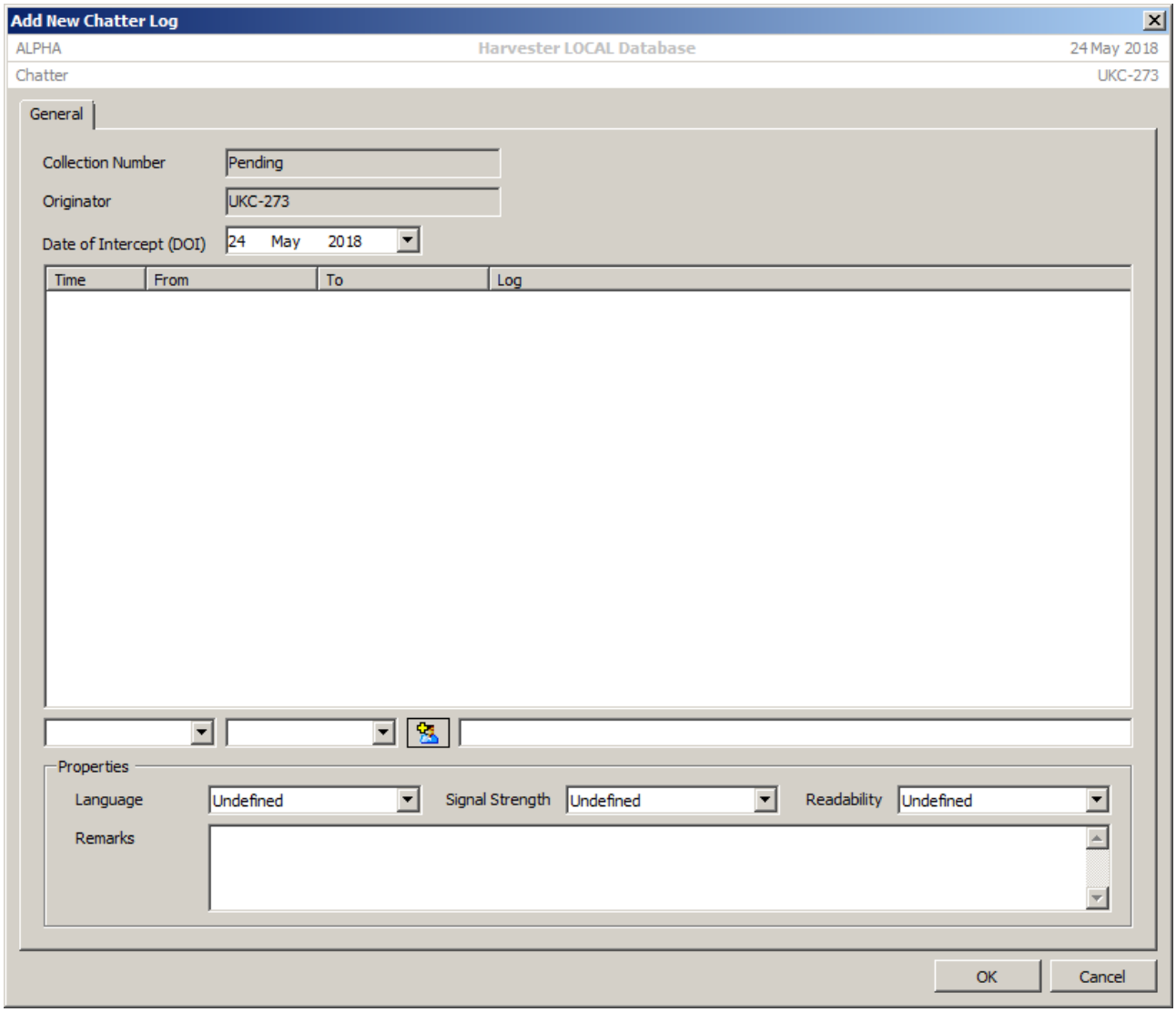
➢ **Initialization Vector**. Often referred to as message keys, these are used by online encryption systems to part key settings to the receiving station and are usually transmitted immediately before the encrypted part of the message. These should not be confused with cryptographic key settings, which are never transmitted with the message.

➢ **Crypto Key**. This is the cryptographic key setting, the key the enabled encryption and decryption of a symmetric crypto system. These are generally unknown but keys for the simpler hand ciphers may be recovered by cryptanalysis.

➢ **Frequency Hopping Rate**. Some crypto radio modules use frequency hopping to obfiscate a signal rather than encrypt a transmission. This refres to the number of frequency hops per second.

3.2.10 Chatter Logs

To open the **Chatter Log** window, click the **Add** button on the toolbar. This will open the report form and pre-populate key fields with relevant information as Log Originator, Date of Intercept, Time Up and Time Down of Intercept. The Collection Number will appear as Pending until the log is saved, when a unique number will be generated.



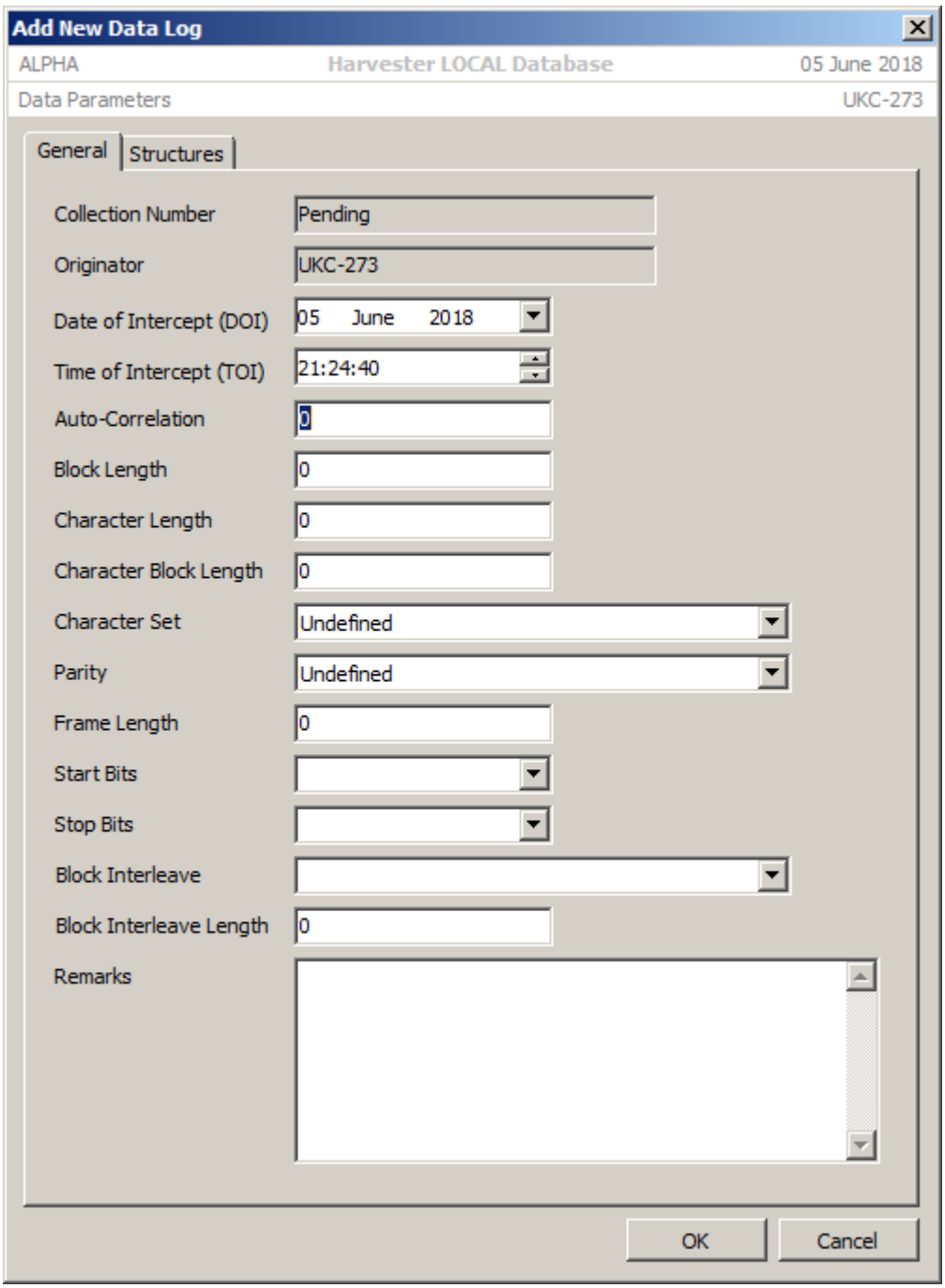
➢ **Date and Time of Intercept**. Both DOI and TOI are automatically set to the current date and time when the log is created. This report is configured to run in real-time mode, therefore historic chatter logs cannot be entered.

➢ **Chatter Log Sheet**. The Chatter Log Sheet consists of two dropdown **From** and **To** and a Chatter text box.

The first dropdown represents the sender with the second representing the recipient. If the required call sign does not appear in the list, click the **Add New Call Sign** button to a new call sign. This is cause a textbox to appear over both **From** and **To** dropdowns.

3.2.11 Data Logs

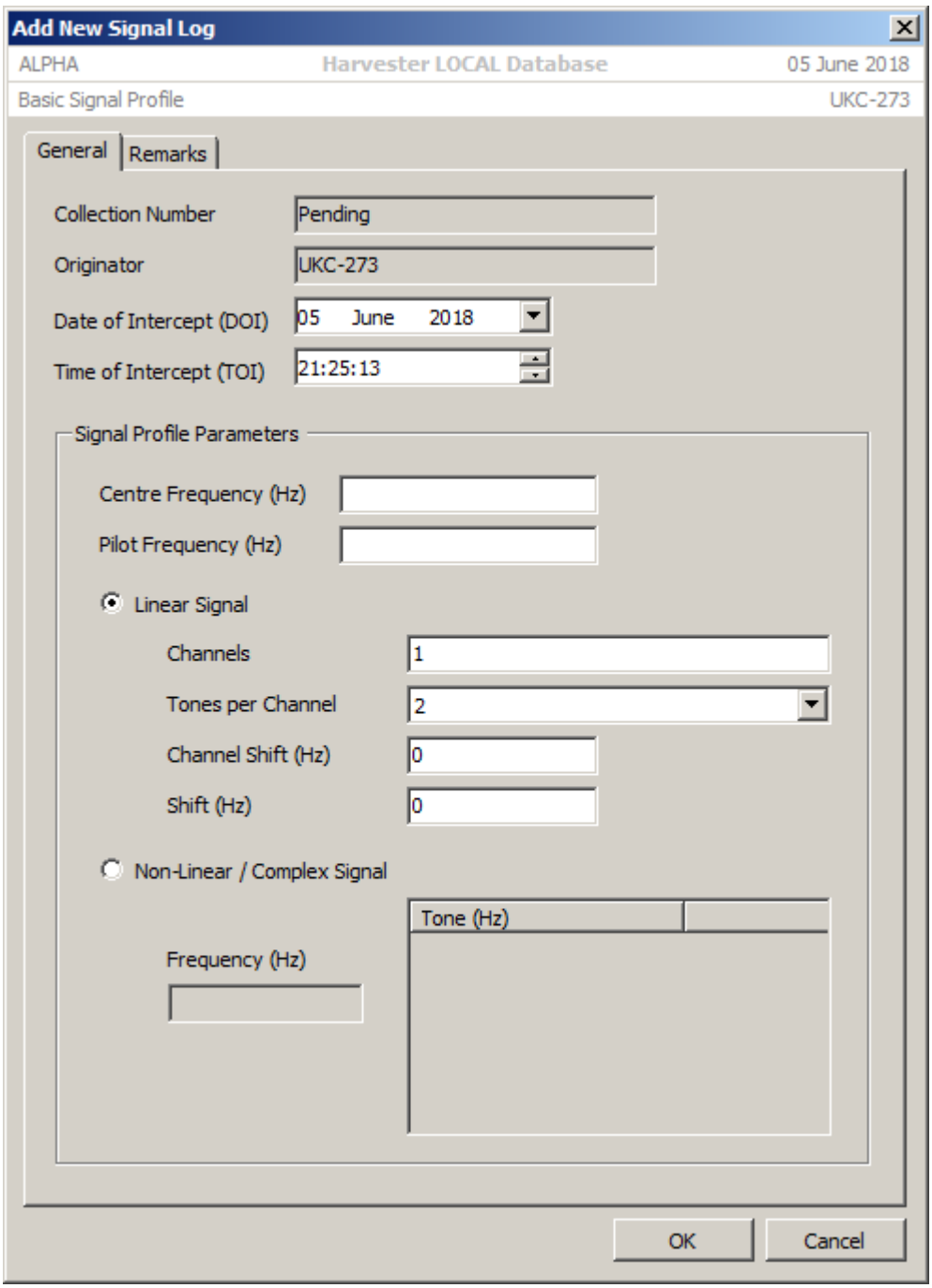
To open the **Data Log** window, select the emitter and **Data Logs** tab then click the **Add** button in the toolbar. This will open the report form and pre-populate key fields with relevant information as Log Originator, Date of Intercept, Time Up and Time Down of Intercept. The Collection Number will appear as Pending until the log is saved, when a unique number will be generated.



The **Data Log** screen is used to record the workings on an unknown telegraphic system. It can also be used to record the normal of anomolous behaviour of known systems.

3.2.12 Signal Logs

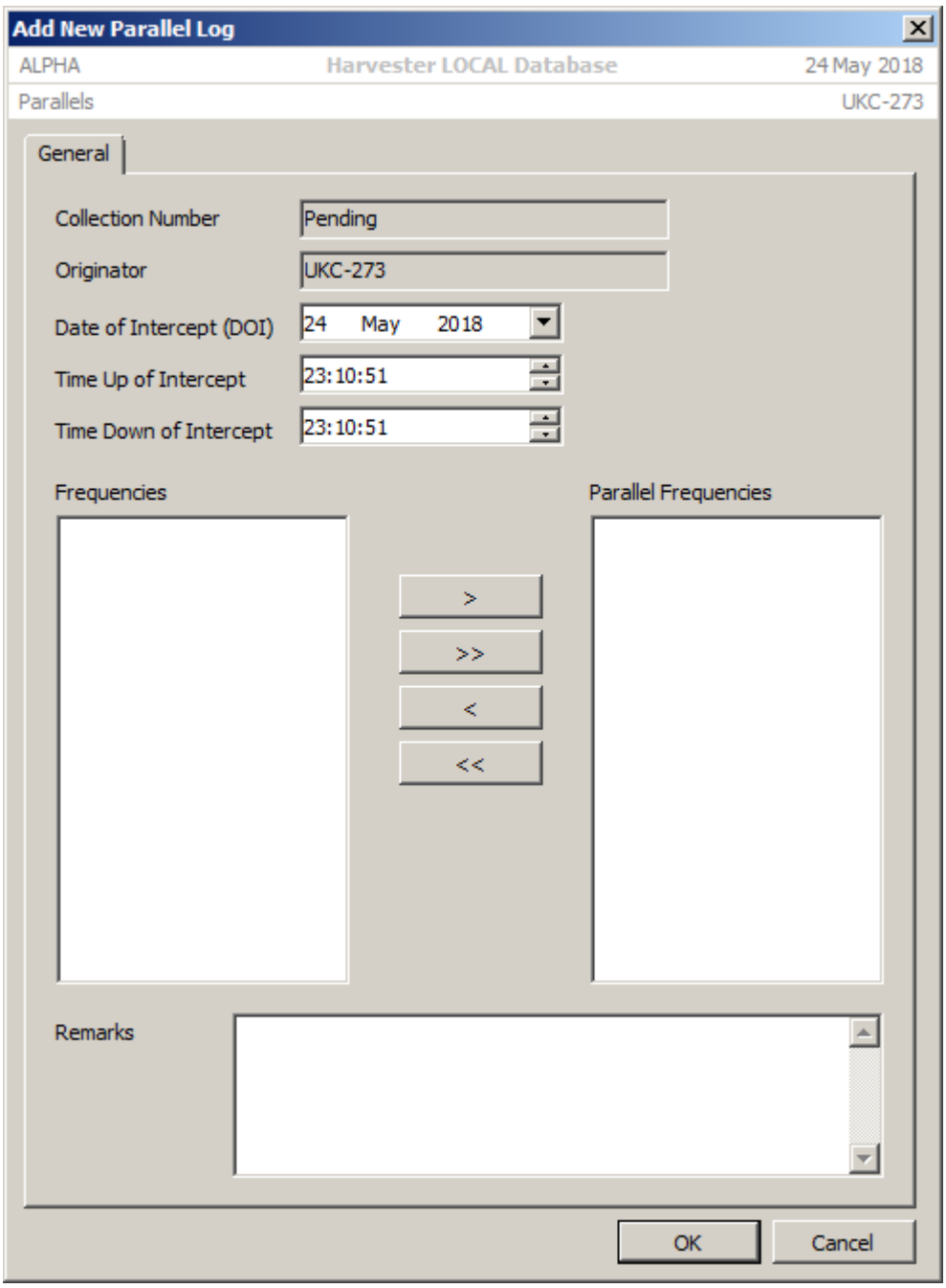
To open the **Signal Log** window, select the emitter and **Signal Logs** tab then click the **Add** button in the toolbar. This will open the report form and pre-populate key fields with relevant information as Log Originator, Date of Intercept, Time Up and Time Down of Intercept. The Collection Number will appear as Pending until the log is saved, when a unique number will be generated.



The first sight of a new system is it's audio spectum. The **Signal Log** screen provides a simple method of recording the physical structure of that audio spectrum.

3.2.13 Parallel Logs

Parallel Frequency Logs are an invaluable intelligence resource when attempting to reconstruct transmission schedules, determine transmitter utilisation schedules and plan further interception. To add a **Parallel Frequency Log**, click the **Add** button on the toolbar. This will open the report form and pre-populate key fields with relevant information as Log Originator, Date of Intercept, Time Up and Time Down of Intercept. The Collection Number will appear as Pending until the log is saved, when a unique number will be generated.

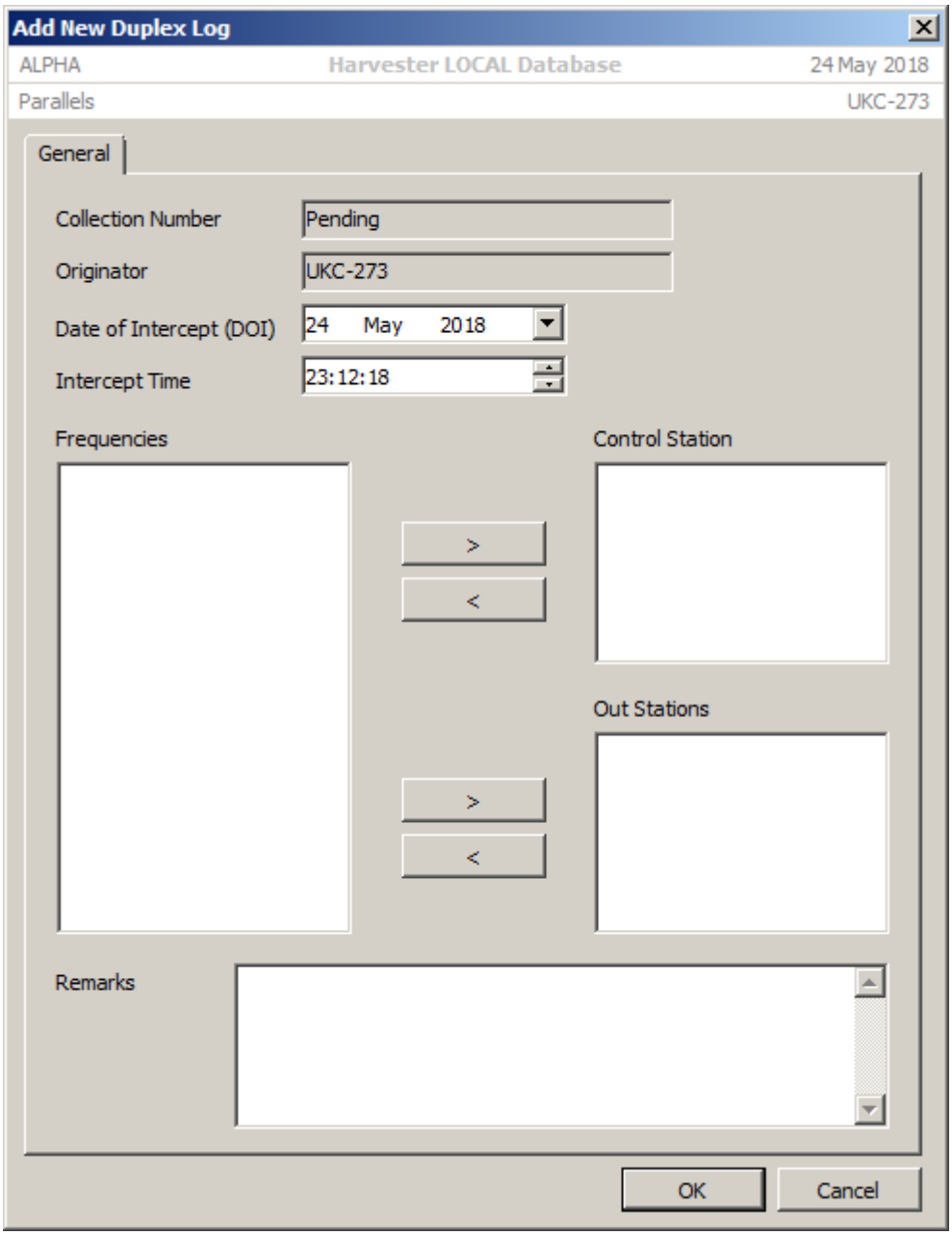


➢ **Date, Time Up and Time Down of Intercept**. Date of Intercept (TOI), Time Up (TUOI) and Time Down (TDOI) are automatically set to the current date and time when the log is created. These can be adjusted as required if the log being entered is historic, and can be updated by clicking the **Set Current Time** button.

➢ **Parallel Frequency Details**. When this form opens, the **Available Frequencies** list is automatically populated with all the currently known frequencies on which the selected emitter is known to transmit. By clicked the appropriate **Add** or **Remove** buttons or double-clicking an entry, frequencies can be moved to and from the **Parallel Frequencies** list.

3.2.14 Duplex Logs

Duplex Frequency Logs are an invaluable intelligence resource when attempting to reconstruct transmission schedules, determine transmitter utilisation schedules and plan further interception. To add a **Duplex Frequency Log**, click the **Add** button on the toolbar. This will open the report form and pre-populate key fields with relevant information as Log Originator, Date of Intercept, Time Up and Time Down of Intercept. The Collection Number will appear as Pending until the log is saved, when a unique number will be generated.



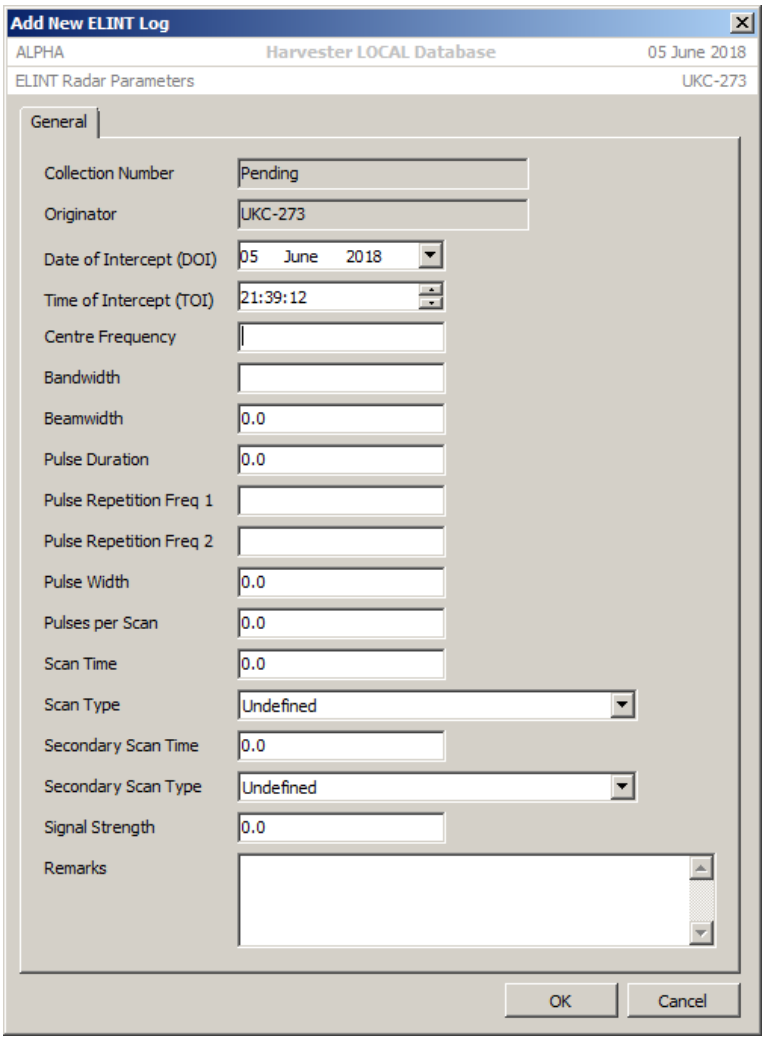
➢ **Date, Time Up and Time Down of Intercept**. Date of Intercept (TOI), Time Up (TUOI) and Time Down (TDOI) are automatically set to the current date and time when the log is created. These can be adjusted as required if the log being entered is historic, and can be updated by clicking the **Set Current Time** button.

➢ **Duplex Frequency Details**. When this form opens, the **Available Frequencies** list is automatically populated with all the currently known frequencies on which the selected emitter is known to transmit. By clicked the appropriate **Add** or **Remove** buttons or

double-clicking an entry, frequencies can be moved to and from the **Duplex Frequencies** list.

3.2.15 ELINT Radar Parametrics

To open the **ELINT Radar Parametric Log** window, select the emitter and **ELINT Radar Parametric Logs** tab then click the **Add** button in the toolbar. This will open the report form and pre-populate key fields with relevant information as Log Originator, Date of Intercept, Time Up and Time Down of Intercept. The Collection Number will appear as Pending until the log is saved, when a unique number will be generated.



4. TEXTA System

signals intelligence (SIGINT): 1. *A category of intelligence comprising, either individually or in combination, all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted. [JP 1-02]* **2.** *Intelligence derived from communications, electronics, and foreign instrumentation signals. [JP 1-02]*

The TEXTA System, which uses Case Notations to reference to individual communications circuits, was touched on very briefly in previous versions of HARVESTER but it is not until now that the full power of this system has been incorporated as an integral part of the application. So what exactly is the TEXTA System, why is it so important and how does it help in logging intercepted signals?

At its most basic level, the TEXTA (*Technical Extract of Traffic Analysis*) System is nothing more than a filing system, but it is a filing system with a difference. It provides the who, the what, the where and the how of a communications network. Originally devised and created in the 1950's as a method of cataloguing the plethora of COMINT networks being intercepted by the then newly formed UKUSA alliance countries of the United States, the United Kingdom, Canada, Australia and New Zealand, TEXTA quickly became the backbone of COMINT collection and reporting for over half a century and is a key component in the successful collation and production of intelligence.

From these humble beginnings, TEXTA has had to continuously evolve to accommodate the ever-increasing variety of signals and circuits, new emissions, multiplexing schemes, satellite communications and an explosion in the number of organisations relying on some form of radio communications to carry out their daily business. Despite outgrowing its original design, the system continues to provide the basic functions that are key to both collectors and analysts.

One of the first mentions of TEXTA Case Notations in the public domain appeared in the European Parliament's Scientific and Technological Options Assessments, Intelligence Capabilities 2000, which stated:

> *At an early stage, if it is not inherent in the selection of the message or conversation, each intercepted signal or channel will be described in standard "case notation". Case notation first identifies the countries whose communications have been intercepted, usually by two letters. A third letter designates the general class of communications: C for commercial carrier intercepts, D for diplomatic messages, P for police channels, etc. A fourth letter designates the type of communications system (such as S for multi-channel). Numbers then designate particular links or networks. Thus for example, during the 1980s NSA intercepted and processed traffic designated as "FRD" (French diplomatic) from Chicksands, England, while the British COMINT agency GCHQ deciphered "ITD" (Italian diplomatic) messages at its Cheltenham headquarters.*

Within HARVESTER, the TEXTA system of Case Notations serve the exact same purpose as its does for the organisation that created it, though the case notation used here differs slightly in structure from that used by the Intelligence Community.

4.1 Case Notation Fields

The construction of a Case Notation follows a very specific format. All case notations begin with a four letter group identifying the Country, Service and Transmission Mode,

then go on to define, a serial number, amplify function and describe the operating area or identify link ends depending on the type of case notation in use.

➢ **Country**. Country is defined by a two-letter code as defined in Defense Intelligence Agency Publication Manual DIAM-65-18 "*Geopolitical Data Elements and Related Features*" and FIPS PUB 10-4 "*Countries, Dependencies, Areas of Special Sovereignty and Their Principal Administrative Divisions*." Where the Country cannot be determined or is unknown, the code XX is used.

➢ **Service**. Service broadly describes the general class or purpose of the circuit. These descriptions reflect the nature of targeting COMINT collection, highlighting the areas from where the most valuable and useful intelligence can be obtained.

A	Air Force	N	Naval Forces
B	Naval Aviation	O	
C	Commercial	P	Police Forces
D	Diplomatic	Q	Intelligence
E	Economic	R	Internal Security Forces
F	Research and Development	S	Merchant Shipping
G	Strategic Weapons	T	Research
H		U	
I	Forces Out Of Country	V	Civil Aviation
J	Military Transport Aviation	W	
K		X	Unknown
L	Strategic Aviation	Y	
M	Ground Forces	Z	Air Defence Force

➢ **Transmission Mode**. Like the Service indicator, Transmission Mode provides a broad general description of the type, or types, of communications used on a circuit.

A	Machine Morse	N	
B	Manual Morse	O	
C	Multi-Channel	P	
D	Generic Data	Q	
E		R	
F		S	Speech
G		T	Teleprinter
H		U	Teleprinter/Morse
I		V	
J		W	
K		X	Unknown
L		Y	Voice/Morse
M		Z	

NOTE The definitions of Service and Transmission Mode codes that have been left blank are currently not know. If anyone can fill in the gaps, we would be more than happy to include them in the software.

In the original UKUSA TEXTA system, the remainder of the Case Notation of composed of a Network serial number and the circuit number within that network. The famous example of this type of case notation is GCPB00101, a manual Morse circuit used by the East German Police

circuit in Berlin in the 1950s. It was this first circuit within the first East German Police Network listed.

Communications have come a long way since the 1950s when numbers of circuits could be measured in the thousands. Today, following the communications revolution of the 1980s and 1990s, the world has become a more complicated signals environment. It is true that the long haul communications that once filled commerical COMSATs have long since migrated onto optical fibre cables and the analaogue signals that were once so easily accessible have been digitised beyond the amateur's reach.

However, with all that in mind, the modern signals environment cannot be described in such simple terms as those of the 1950s. Recent documents released into the public domain have provided a rare glimpse at the next-generation TEXTA system that provides Case Notations at the project level for every current and future communications target. Combining the simplicity of the first-generation system with the scope of the system that has recently been released, we have developed a flexible hybrid system that will meet all current, future and historic needs.

4.2 Types of Case Notation

In this new hybrid TEXTA system, there are two basic types of Case Notation:

- **Temporary or Developmental**. As the name suggests, these temporary case notations are assigned to newly intercepted circuits, usually by the intercepting station where available intercepts have not yet provided sufficient intelligence to determine the exact nature of the circuit or match it was an already known circuit. As these case notations are incrementally developed, they are assigned a Country, Service and Transmission Mode, the 6-digit serial number of intercepting station, the single letter 'T' indicating that it is a temporary notation and a 7-digit serial number. This means that each station can create 10 million of it's own temporary case notation, more than enough for most signal environments.

A typical temporary case notation would take the form ITNS297828T0000015, and this would decode to:

Field Name	CN	Decode
Country	IT	Italy
Service	N	Naval Forces
Transmission Mode	S	Speech
Station Number	291220	
Temporary	T	
Serial Number	0000015	15

- **Permanent**. Permanent Case Notations are the product of extensive monitoring, development and analysis of the procedures of a circuit. They are assigned when and only when the identity and purpose of the circuit is positively identified. Permanent Case Notations are allocated centrally so do not include the number of the originating station.

Typically, a Permanent case notation would take the form RSNA17000251, and this would decode to:

Field Name	CN	Decode
Country	RS	Russia
Service	N	Navy
Transmission Mode	A	Machine Morse
Year	17	2017

Serial Number 000251 251

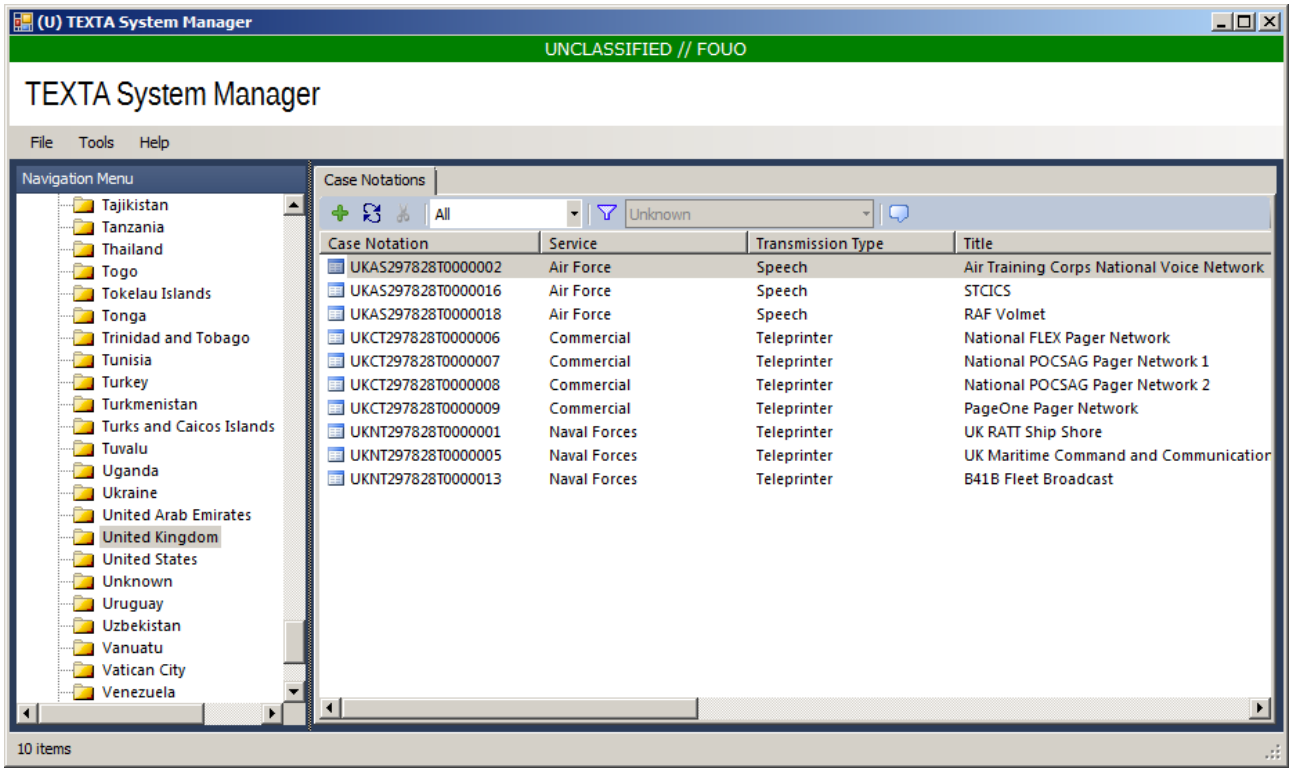
The most commonly created case notation will be the temporary or developmental case notation. This is the default type that is created at the station level for any new circuit that is intercepted. Initially defined as unknown, it is the analyst's job to firstly identify the country of origin then the service. If gathered information against the new case notation matches an existing case notation then that information should be transferred to the existing case and the new case notation obsoleted.

Once the purpose and operating procedures of the case notation are fully documented, stations can ask for their Temporary Case Notations to be reassigned as Permanent Case Notations.

NOTE This might sound all very complicated but HARVESTER takes care of everything! All you have to do is request a new Temporary Case Notation and HARVESTER will generate it for you while it keeps track of all the letters and serial numbers so that you can concentrate on intercepting and collecting signals.

4.3 TEXTA System Manager

Case Notations can be managed and maintained in the TEXTA System Manager, which can be accessed from the Tools menu on the main screen.



4.3.1 Adding a New Case Notation

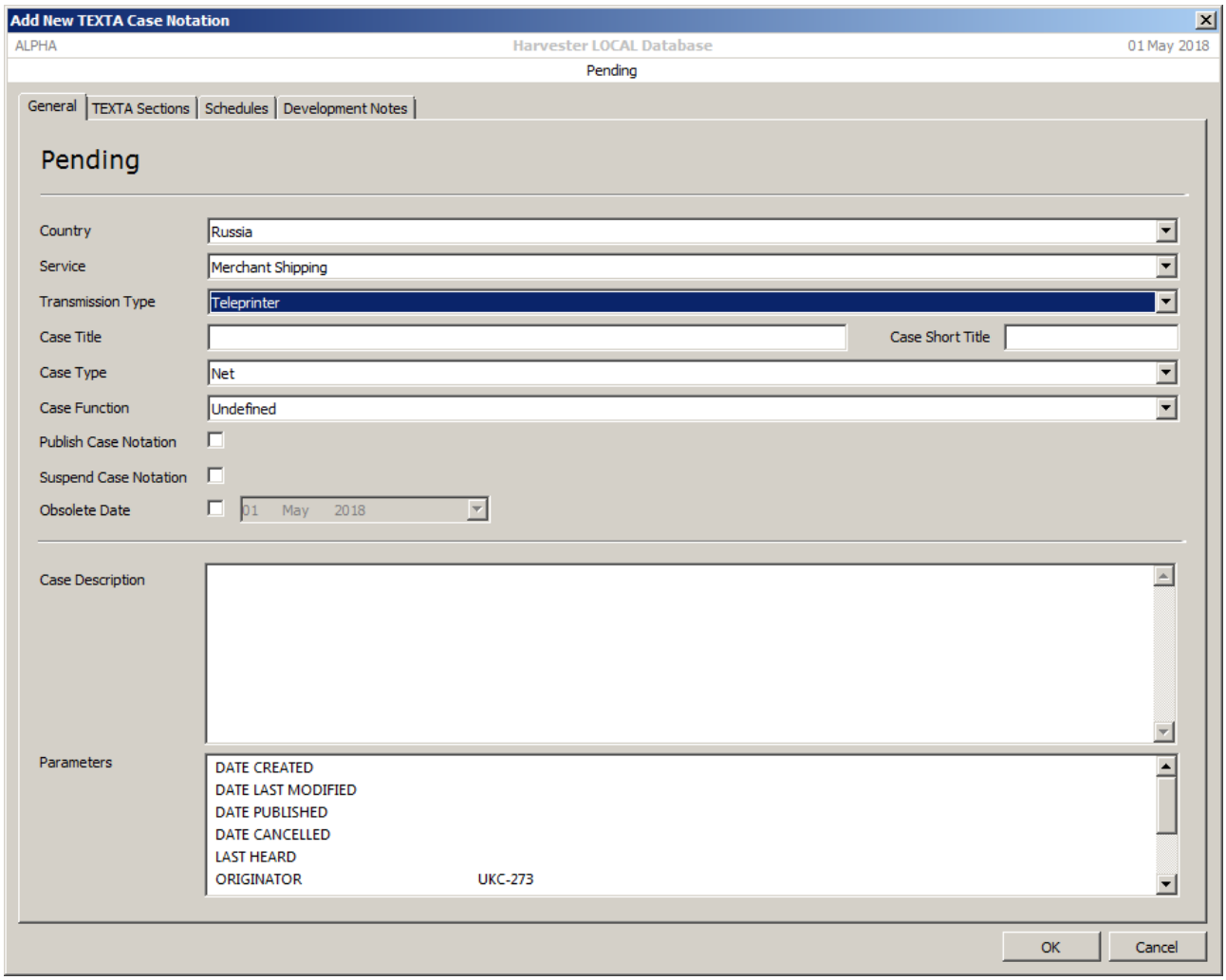
To add a new Case Notation, select the country from the navigation menu then click the **Add** button on the toolbar. This will open the **Add New TEXTA Case Notation** screen. This screen has four tabs:

- **General**. This first tab is used to define the Country, Service and Transmission Mode of the circuit as well as setting details such as title of the Case Notation, what

type of circuit it is (Broadcast, Net or Point to Point) and a general description of the circuit. To ensure that the Case Notation appears in the TEXTA Case Files, check the **Publish Case Notation** option.

To accommodate the use of alternative case notation systems within HARVESTER, the Case Short Title can be defined for each record. This will be particularly useful for users of the ENIGMA 2000 Control List.

➢ **TEXTA Sections**. Here is where the real details of the circuit can be entered. There are fourteen pre-defined sections covering callsigns, frequencies, operator habits and procedures, types of traffic, operator chat, Q and Z codes, entities and locations and a history of the Case Notation. These are the sections that will be used to positively identify unknown circuits so it is essential that these sections contain clear and concise information to help identify a circuit.



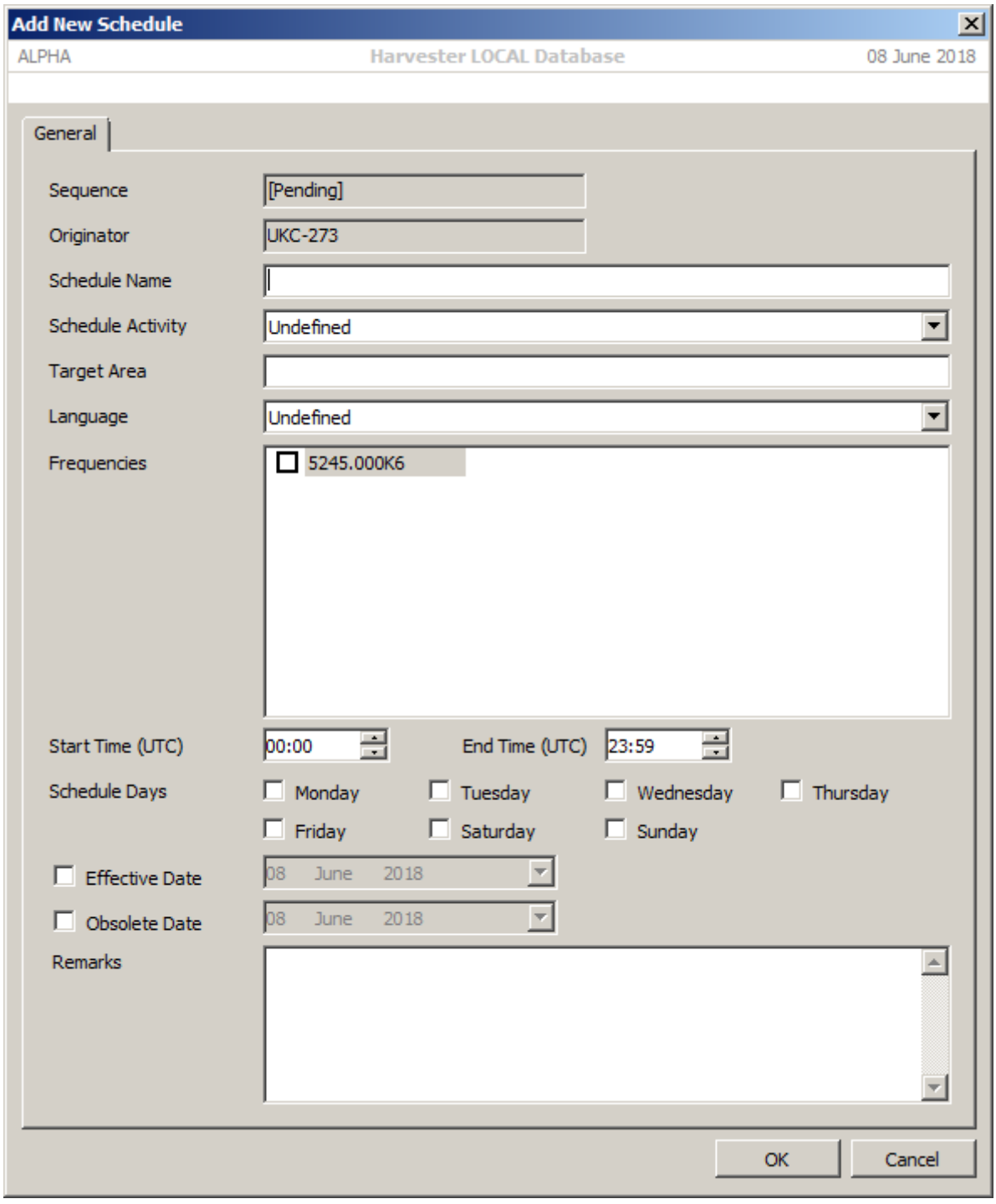
➢ **Schedules**. This is an additional tab to allow actual circuit schedules to be recorded against the Case Notation. These can be current or historic.

➢ **Development Notes**. This is an additional tab to allow actual circuit schedules to be maintained against the Case Notation.

4.3.2 Adding a New Schedule

Schedules play an important part is all communications networks, whether it be the times of an international broadcaster's transmissions or the times of a foreign embassy sending traffic back to headquarters. Many schedules are regular events and that is particularly true of international broadcasters however many users operate obscure and often apparently pseudo-random schedules. The key to cracking any schedule lies in being able to compare numerous intercepts to determine any patterns.

Once schedules have been determined or obtained directly from the broadcaster, they can be entered in the **Schedule** tab. To add a new Channel, select the **Schedule** tab then select the appropriate Entity from the organisational hierarchy. Click the **Add Property** button on the toolbar to open the **Add New Schedule** window.



Each **Schedule** can be defined in terms of the **Schedule Times**; the start and end times, and days of the week on which the transmission activity occurs. Actual details of the schedule can be expanded in the **Schedule Description**. Here the period of validity of the schedule can be defined, although with the **Schedule Activity** described the type of transmission that is broadcast. Generic activities can be selected from the dropdown list.

Schedules may often be referred to by a specific **Service Name**, such as the North American Service, the Surface Fleet Broadcast, or the Russian Service. Details can be entered in the **Service Name** box, along with the **Target Area** if known, and the **Language**.

Schedule Frequencies can be selected from a list of all available frequencies. The list of available frequencies is taken from all the frequencies in the system that are attached to the selected Case Notation.

4.4 Allocating Case Notations

When a new circuit or network is discovered, it should be assigned a Case Notation as soon as possible. Review existing TEXTA material including TEXTA Case Files and intercepts to find a suitable match. Identify the country, service and mode of transmission and additional transmitter characteristics, and use these details to search the TEXTA database to identify the correct case notation. If no match exists, a new case notation should be created.

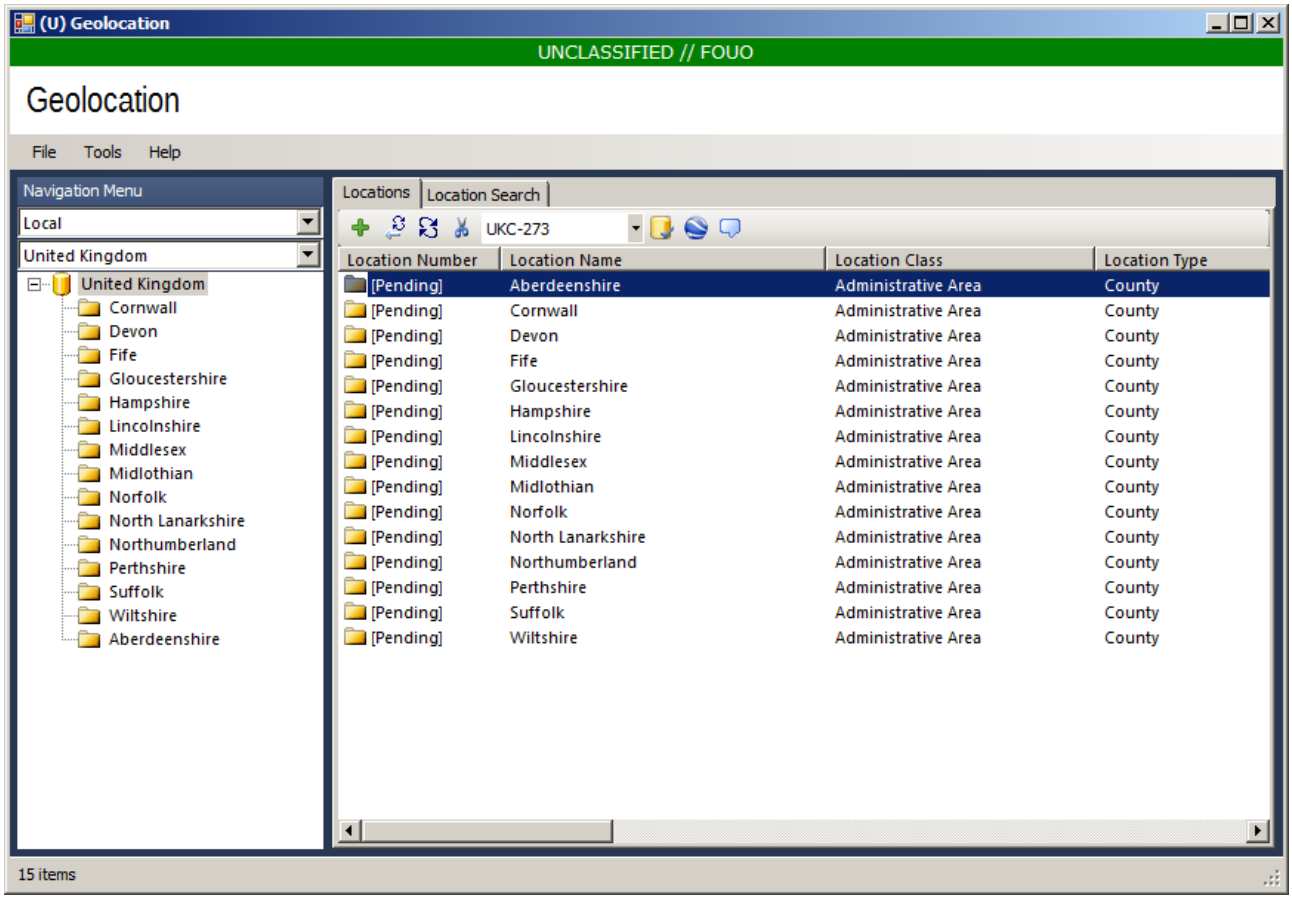
4.5 ELINT Notations (ELNOT)

Electronic Intelligence (ELINT) has it’s own Case Notation system called ELINT Notation or ELNOT.

5. Geolocation

signals intelligence (SIGINT): 1. *A category of intelligence comprising, either individually or in combination, all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted. [JP 1-02]* **2.** *Intelligence derived from communications, electronics, and foreign instrumentation signals. [JP 1-02]*

The concept of geolocation is a feature new to HARVESTER 6 and addresses the need for a coordinated approach of the geographic location of emitters, platforms and other location-centric entities. While simple in design, this functionality provides a powerful tool to unify often disparate and unrelated location details under a single heading.



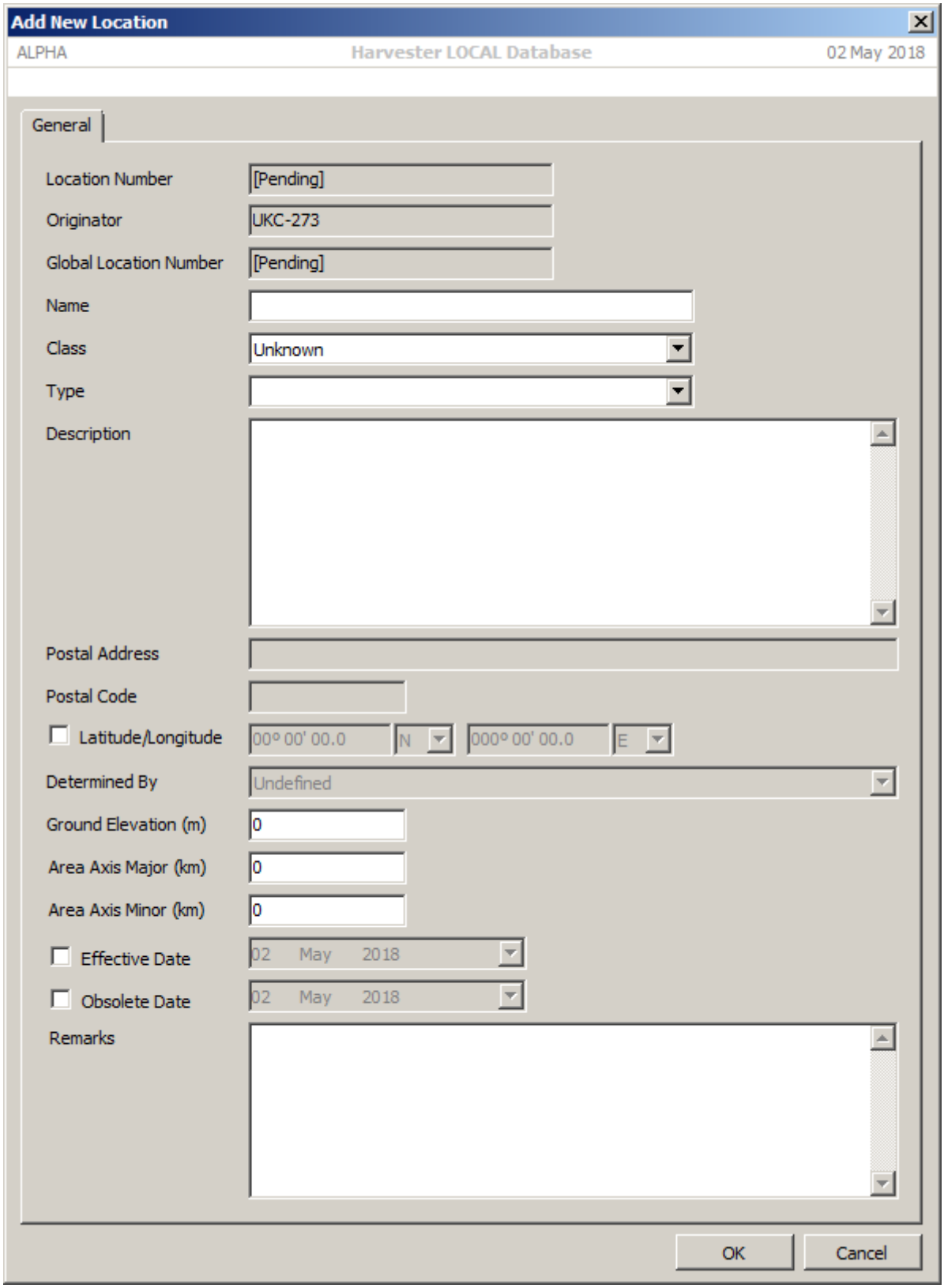
Geolocation is build on a hierarchical model which begins with the country and gradually increases in gradularity by breaking the that country down into administrative areas such as states, regions or counties. These areas can then be further divided into poulation areas such as cities, towns and villages.

Alongside population areas, installations can also be added. These are sites with both strategic and signals interests, such as civilian and military airfields, harbours, hospitals, railway stations and government buildings.

It is important to understand that the Geolocation screen is at the heart of all geolocation related intelligence within HARVESTER and that all modules that use location will derive that information from this csreen. It is therefore essential that this information is kept up-to-date, is accurate and reflects the geolocation collection strategies of each station.

5.1 Adding a New Location

To add a new location, select the appropriate parent location from the geolocation hierarchy then click the **Add** button in the toolbar. This will open the **Add New Location** screen.



Enter the name of the location then select the most appropriate class of location from the Class dropdown. There are four types of location class:

- **Administrative Area**. There are generally the geoplitical regions, states and counties that a country is divided up into and provide the coarsest location description of a country.

- **Population Area**. These are the cities, towns and villages of a country.

- **Geographical Feature**. These are the hills, mountain ranges, lakes, rivers and even small islands than make up a country.

- **Installation**. Along with population areas, these are of the greatest strategic and signals interest. They represent the military and industrial heart of a country, reflect transport and communications infrastructures and are likely to provide the richest signals environments.

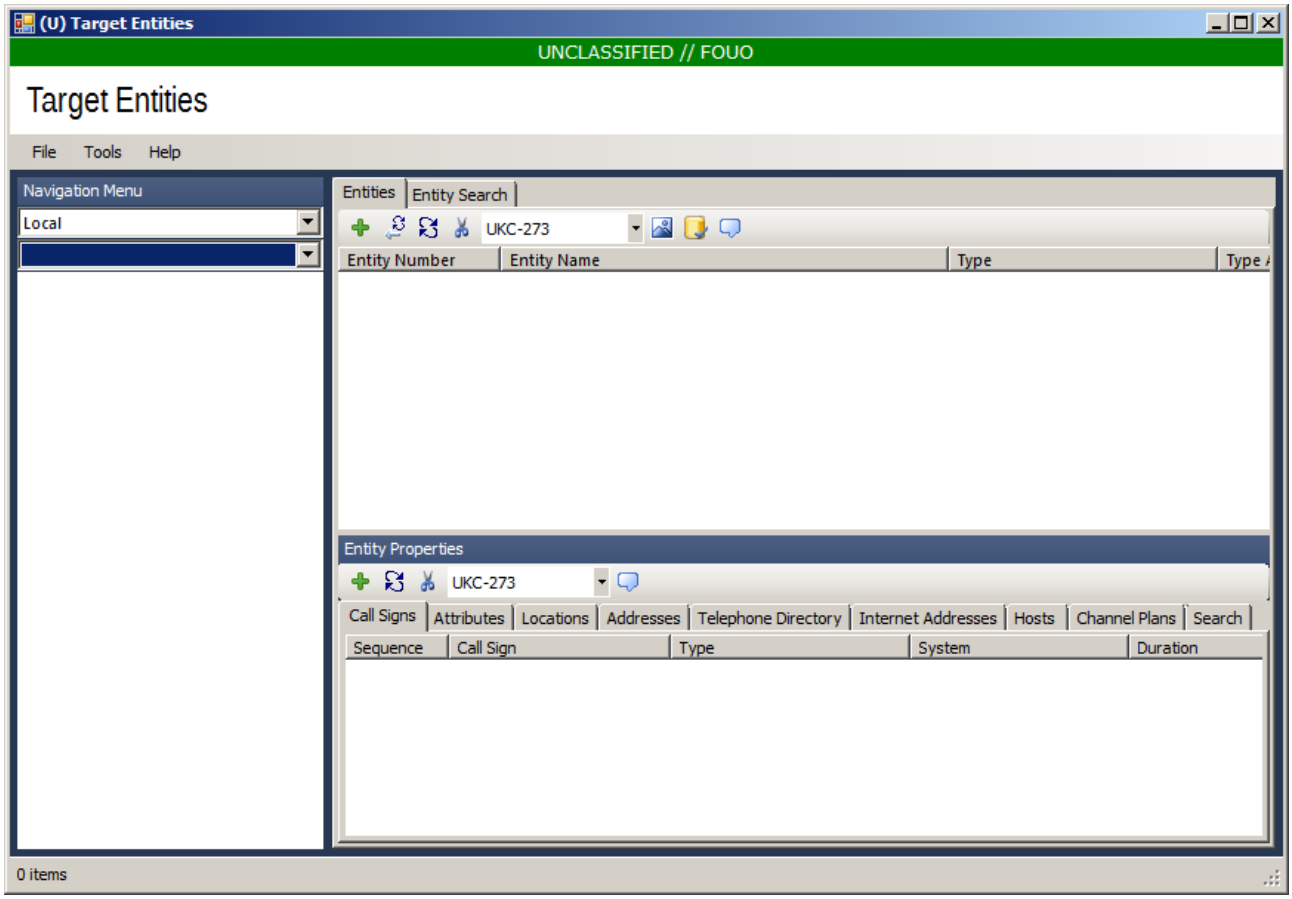
Class location can be further amplified with the Type dropdown and additional information can be added in the descriptions box.

NOTE The Class Amplifier description in HARVESTER are an evolving concept so there may be descriptions you require that are not currently available. Please use the user feedback screen that is available on each screen to suggest further descriptions that should be added. Alternatively, please contact us with your suggestions and requirements.

6. Target Entities

signals intelligence (SIGINT): 1. *A category of intelligence comprising, either individually or in combination, all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted. [JP 1-02]* **2.** *Intelligence derived from communications, electronics, and foreign instrumentation signals. [JP 1-02]*

Successfully correlating the many pieces of collected information to form an accurate overall picture of any communications system depends largely on the ability to attribute individual communications, messages and chatter to their respective official organisations and users. In many cases, such as broadcasting stations, this is a straightforward matter, however large, secretive and more complex organisations, such as military forces, often exist as a collection of many branches and departments. Attributing collected information to this type of user to the correct department depends on stored information being able to mimic the organisation's own hierarchy. By allowing the creation of multiple tiers and branches of organisational structure within each organisation, the **Target Entities** screen provides all the tools necessary to accurately reconstruct the corporate, political or echelon hierarchy of any organisation.



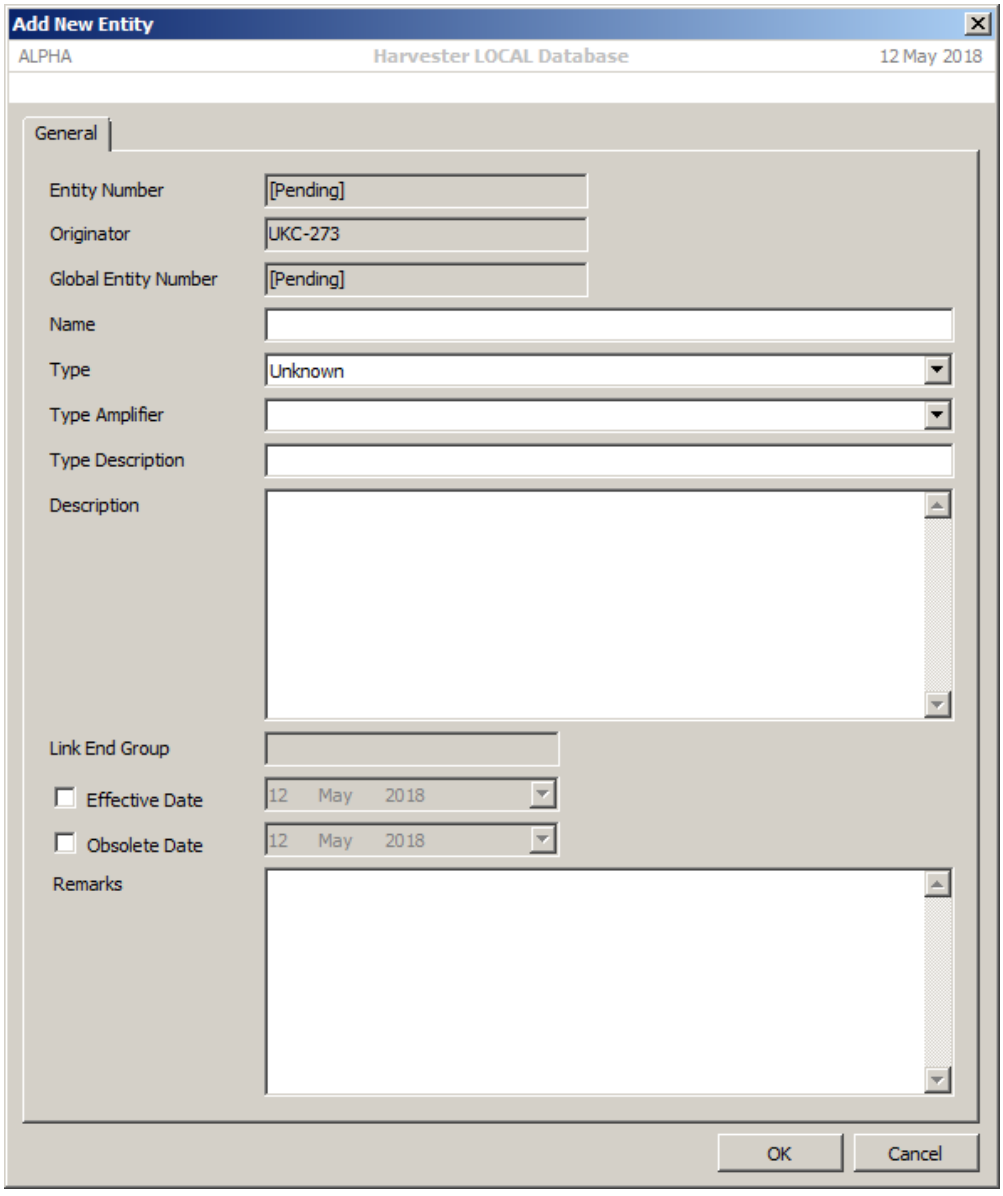
6.1 Organisations, Functions, Echelons and Elements

Target Entities, or **Order of Battle,** defines the hierarchical chain of command of any communications system, and in almost all cases, is an accurate reflection of the command structure of the target. Each target, or Organisation is built up of various Functions or

Echelons, to which can be attached various Elements. This combination of Echelons and Elements is used to build up a picture of each target, a picture that can be added to and developed with additional information derived from intercepts and open sources. In previous versions of HARVESTER, different entity types were treated seperately, now they all treated as variations of a single entity. There are five possible entity types: Organisation, Echelon, Function, Platform and Personality.

6.2 Adding a New Entity

To add a new entity, select the appropriate country from the dropdown list of countries and click on the **Add** icon on the main toolbar to open the **Add New Entity** screen.



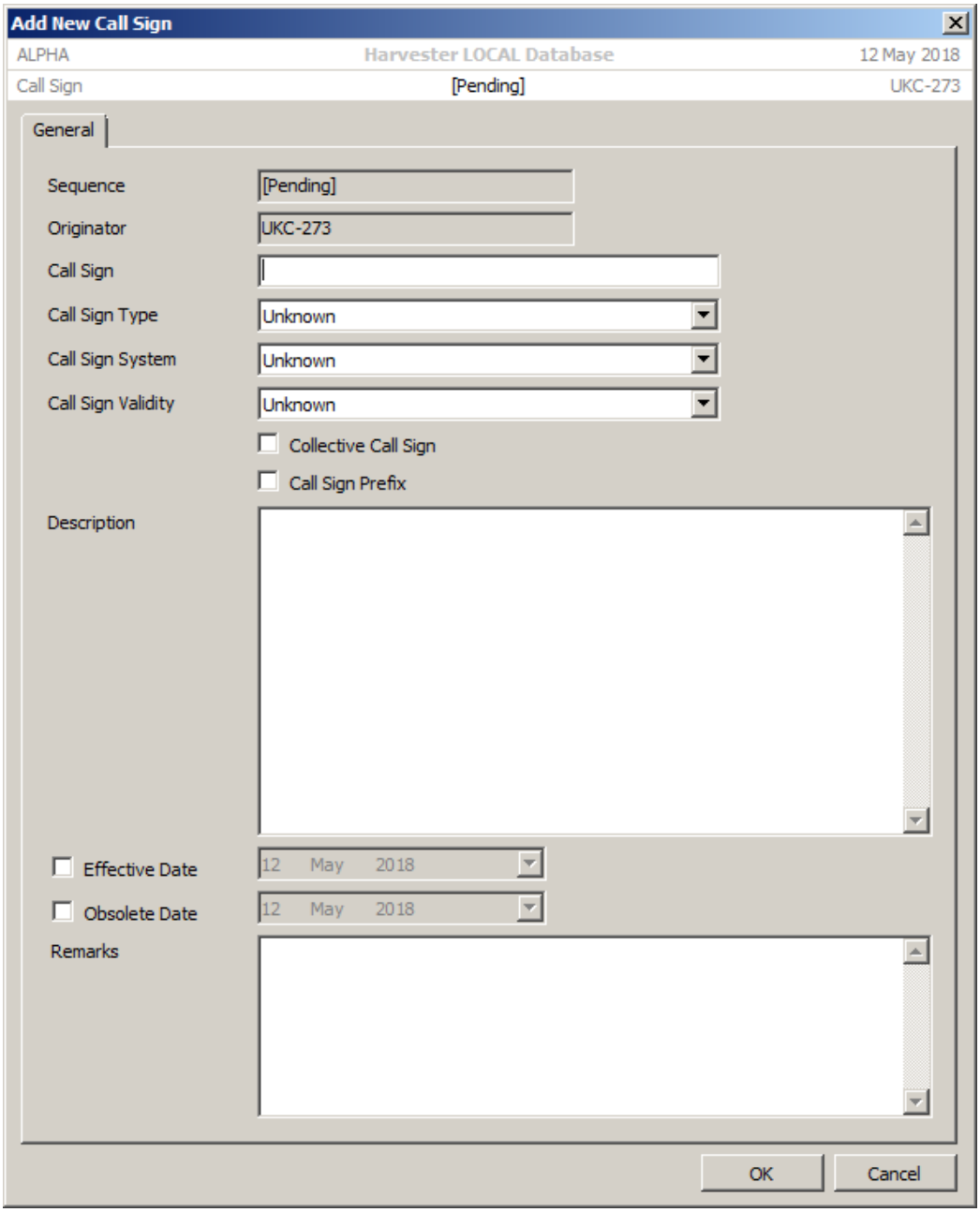
Enter the official name of the **Entity**. This can either be in English, or in the native language of the **Entity**, though English may be the most appropriate choice. Next enter the type of the Entity. This can be further expanded by the Type Amplifier and a free text Type Description, a short description of the Entity's generalised role or purpose.

6.3 Entity Properties

Within the EOB hierarchy, organisations, echelons and elements make up the structure profile of each target country. Each entity within that structure can be further enhanced with the addition of identifiers, addresses, channel plans, schedules and movements gathered from intercepts, open sources and observations.

6.3.1 Adding an Call Sign

An **Call Sign** is defined as any fixed, temporary or random call sign that can be used to identify an EOB entity. Many organisations have a number of unique static call sign types while other, such as military forces, will use random call signs to make identification of an entity more difficult.



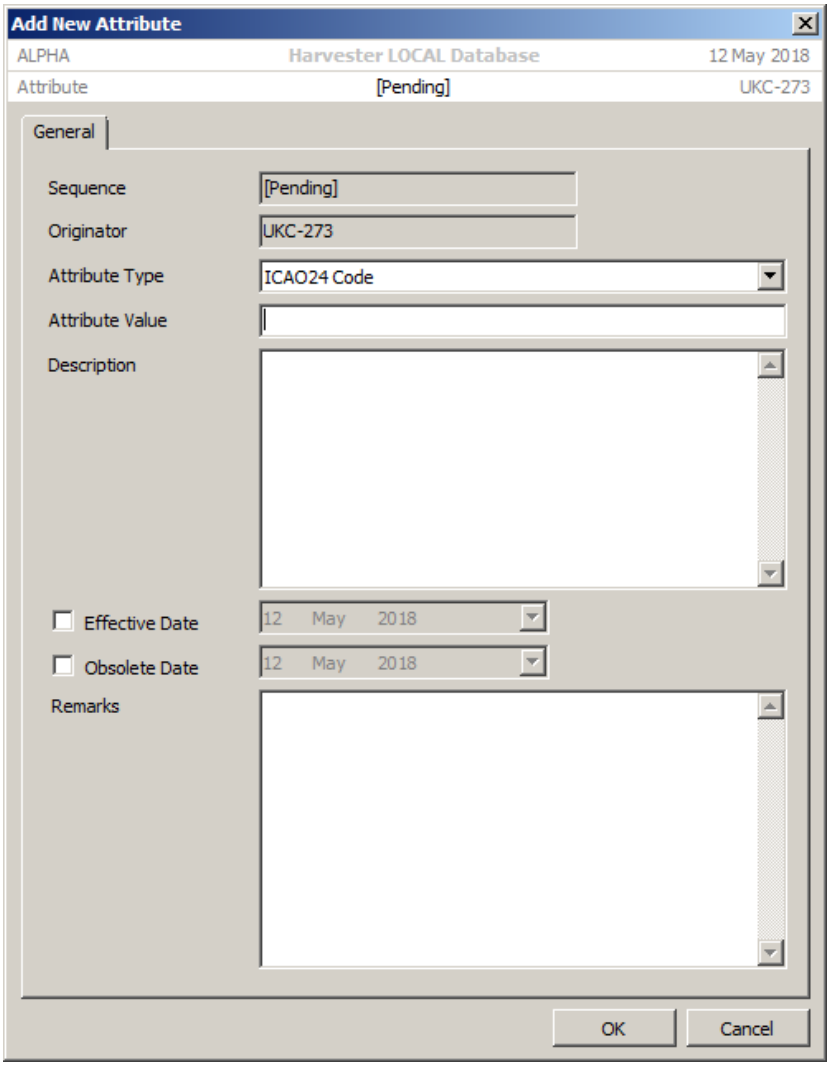
Select Entity from the organisational list then select the **Call Signs** tab. Click the **Add** button on the toolbar to open the **Add Call Sign** window. First select the Identifier type from the dropdown list. There are currently 11 options:

ACARS Address	ICAO24 Mode-S Address
Aircraft Registration	ITU Call Sign
ALE	Pager Address
Fixed Service Maritime Selcal	Tactical Call Sign
Fixed Service Selcal	Voice Call Sign
Flight Number	

Type the Call Sign into the Call Sign box and add any additional information in the form of a short description and remarks. Click the **OK** button to add the identifier, which will be automatically displayed in the **Call Signs** tab.

6.3.2 Adding an Attribute

An **Attribute** is defined as any static code or designator that can be used to identify an entity. Many organisations have a number of unique static identifiers associated with them. Airlines, for example, are identified by a unique three-letter code allocated by the ICAO. They are also identified by a two-letter code allocated by IATA, which appears on flight tickets, airport arrivals and departures screens and baggage tags.



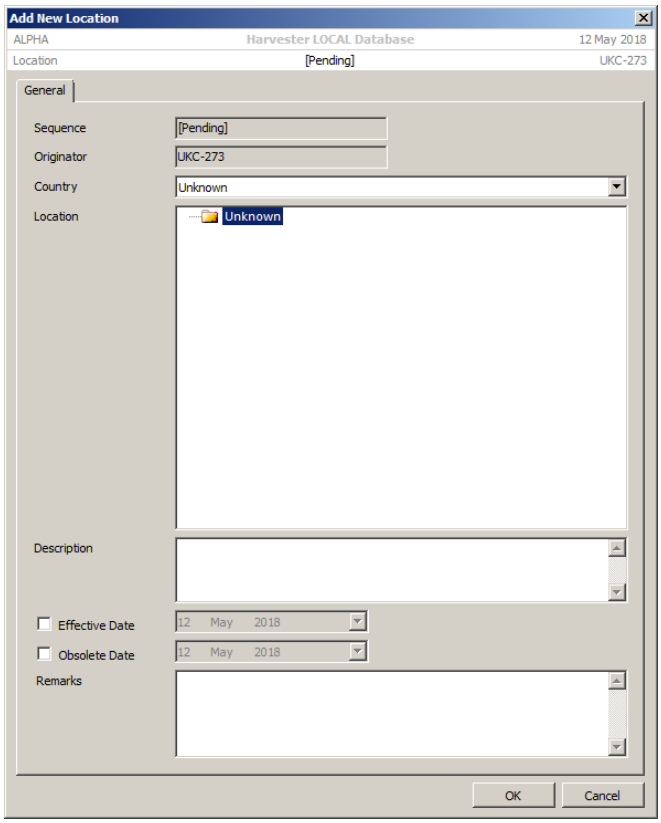
Select the **Attribute** tab, and then select the Entity from the organisational hierarchy. Click the **Add** button on the toolbar to open the **Add New Attribute** window. First select the Identifier type from the dropdown list. There are currently 25 options:

ACARS Address
Aeronautical ANNEX-10 Selcal
Aircraft Registration
ALE
Commercial Call Sign Prefix
DSN Prefix
Fixed Service Maritime Selcal
Fixed Service Selcal
Flight Number
Hull Number
IATA 2-Letter Airline Code
IATA 3-Letter Airfield Code
ICAO 3-Letter Airline Code
ICAO 4-Letter Airfield Code
ICAO24 Mode-S Address
IMO Number
ITU Call Sign
Maritime Mobile Selcal
Maritime Selective Call Number
MMSI Number
Pager Address
Routing Designator
Tactical Call Sign
Talkgroup
WMO Observing Station Index

Type the Attrubute into the Attrubute box and add any additional information in the form of a short description and remarks. Click the **OK** button to add the identifier, which will be automatically displayed in the **Attributes** tab.

6.3.3 Adding A Location

The **Locations** tab allows platform observations to be entered and recorded. This is a particularly useful facility for logging the movements of aircraft and ships, and can prove of great value in call sign analysis when the identities of tactical call signs are established by confirmed sightings.

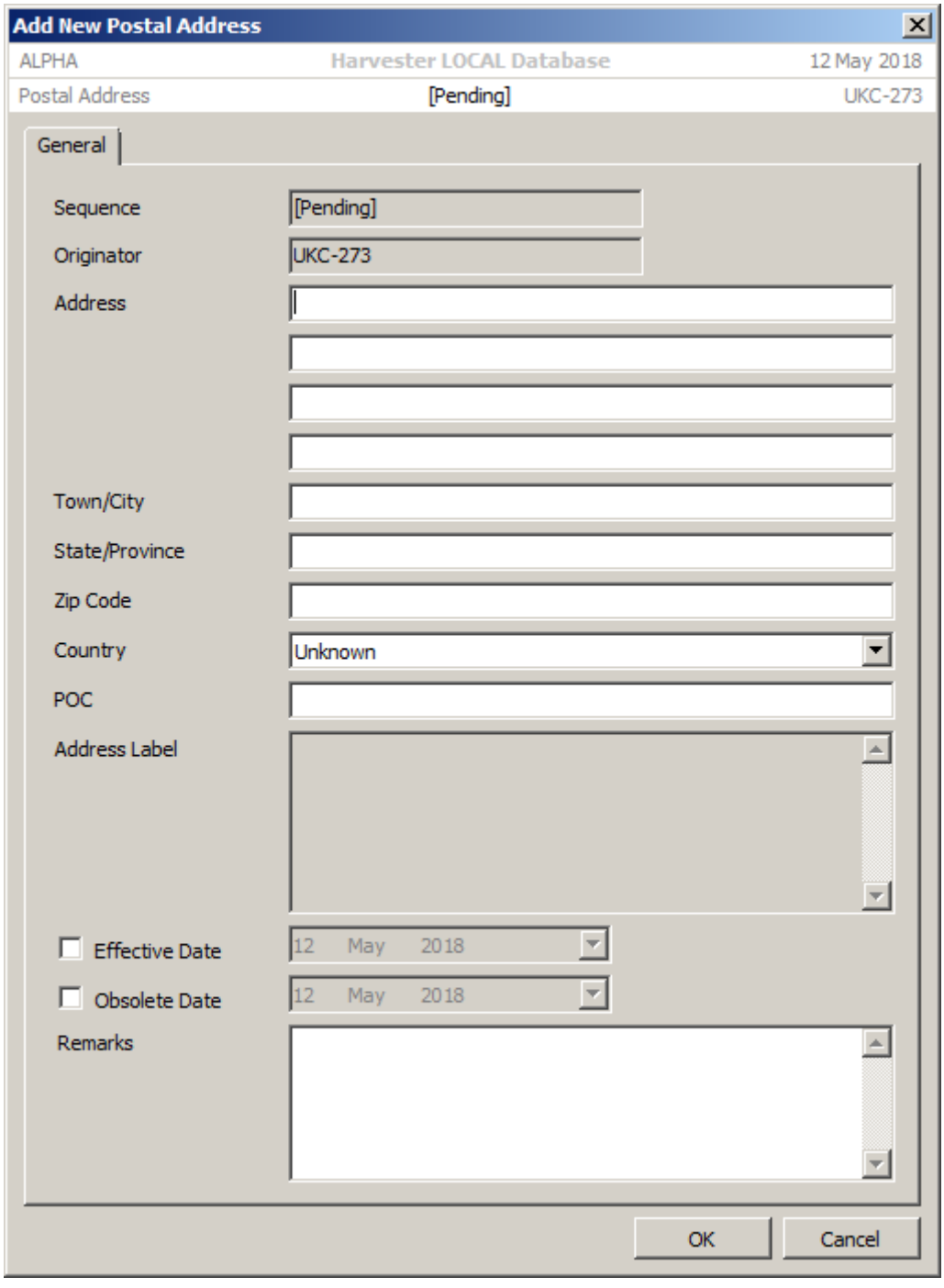


To add a new **Locations**, select the **Locations** tab then select the Entity from the organisational hierarchy. Click the **Add** button on the toolbar to open the **Add New Locations** window.

Select the country then select the location from the location hierarchy. Additionl information can be added in the location Description and Remarks boxes along witj the effective and obsolete dates of the location if known.

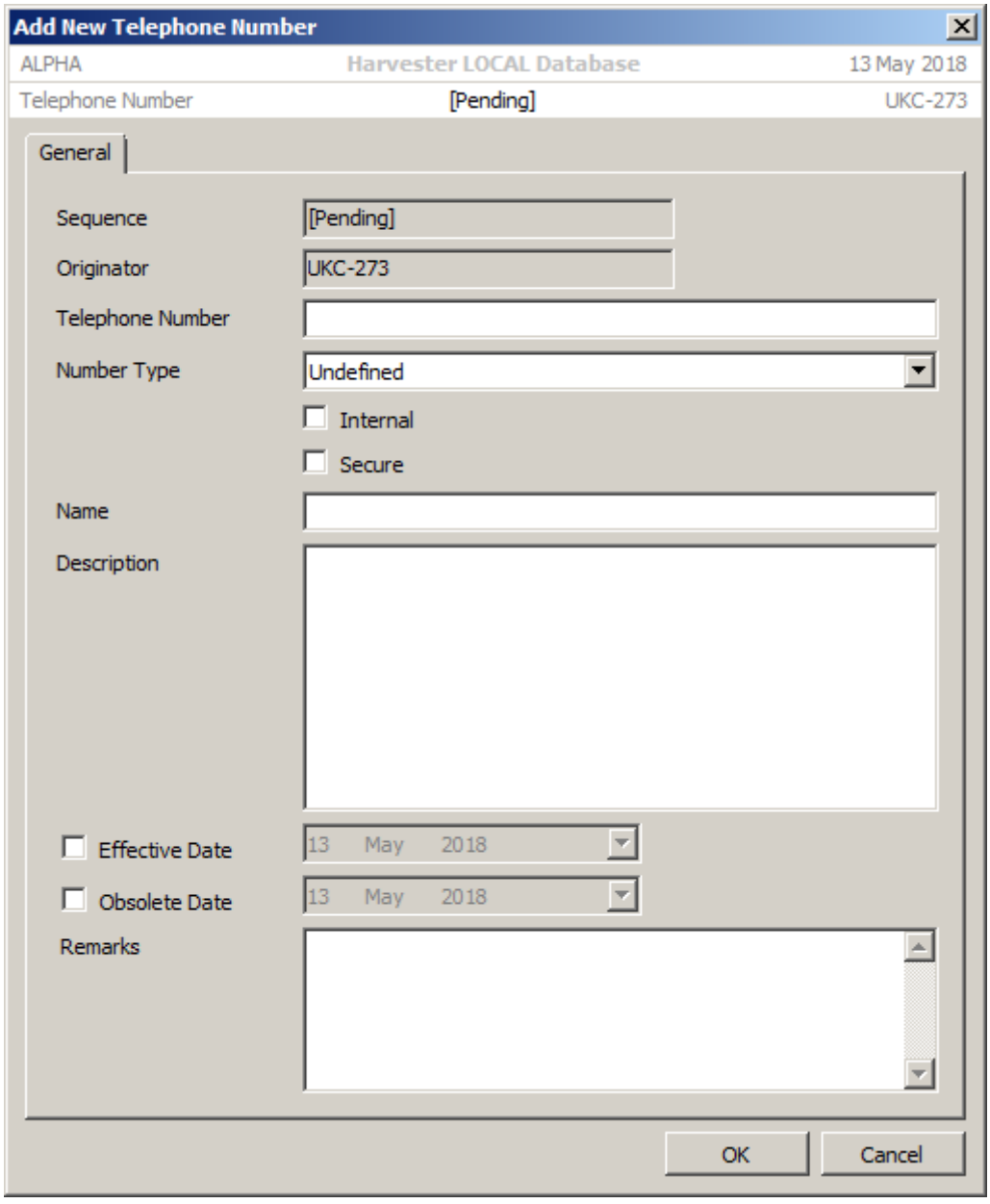
6.3.4 Adding an Address

In this age fast electronic communications, physical postage addresses remain an important piece of information for entities. To add a new Address, select the Address tab then select the Entity from the organisational hierarchy. Click the Add button on the toolbar to open the **Add New Postal Address** window



6.3.5 Adding a Telephone Number

An entity's telephone directory can often provide a valuable insight into the internal structures of an organisation and its staff. To add a new **Telephone Number**, select the Telephone Number tab then select the Entity from the organisational hierarchy. Click the Add button on the toolbar to open the **Add New Telephone Number** window.



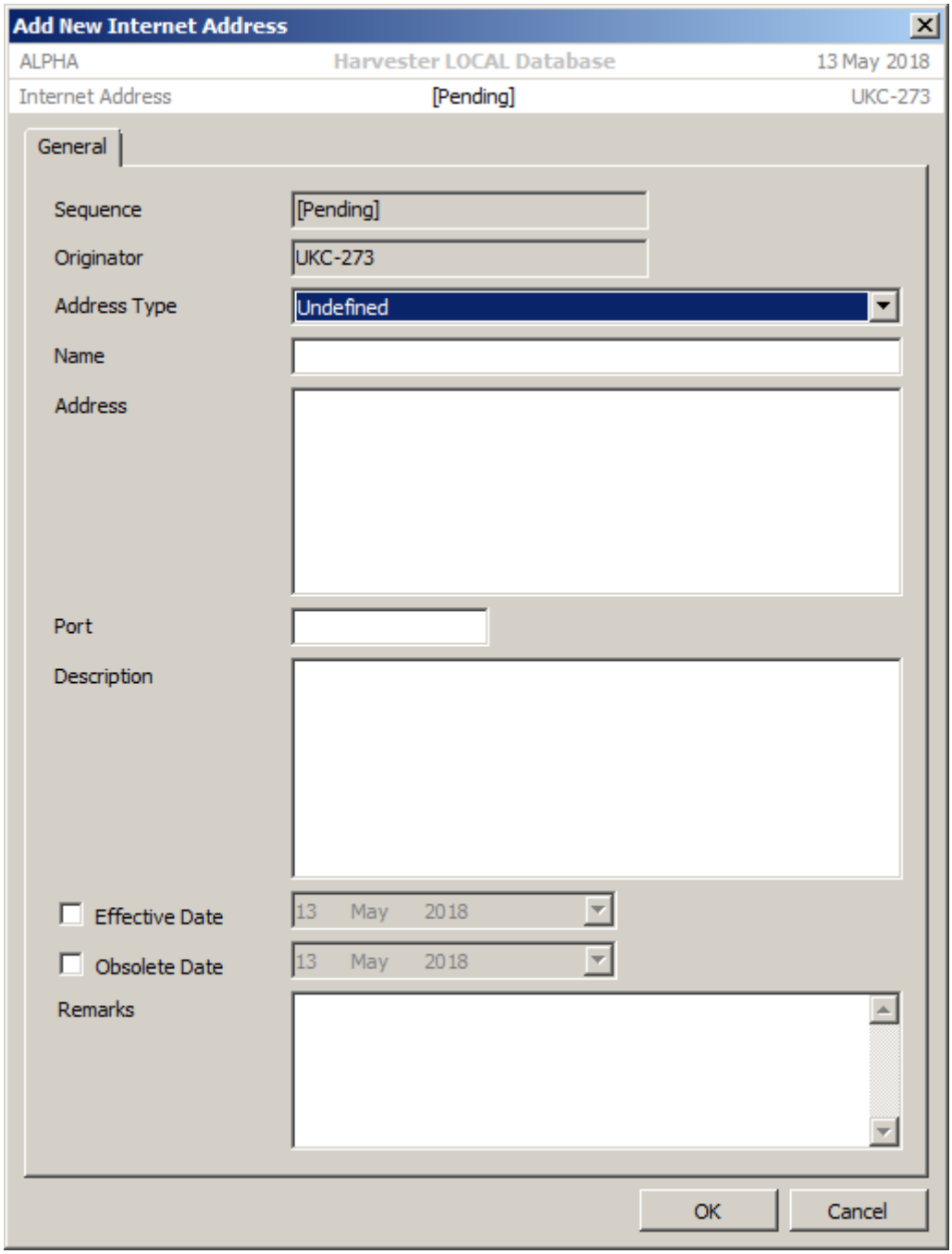
There are currently 14 telephone number types to choose from:

DSN Fax Number
DSN Prefix
DSN Voice Number
Fax Number
Globestar Number
INMARSAT Number
Iridium Number
Landline Telephone Number
Mobile Number
Pager Number
PSTN Number
Telex Number
Thuraya Number
Undefined
Voice Number

6.3.6 Adding an Internet Address

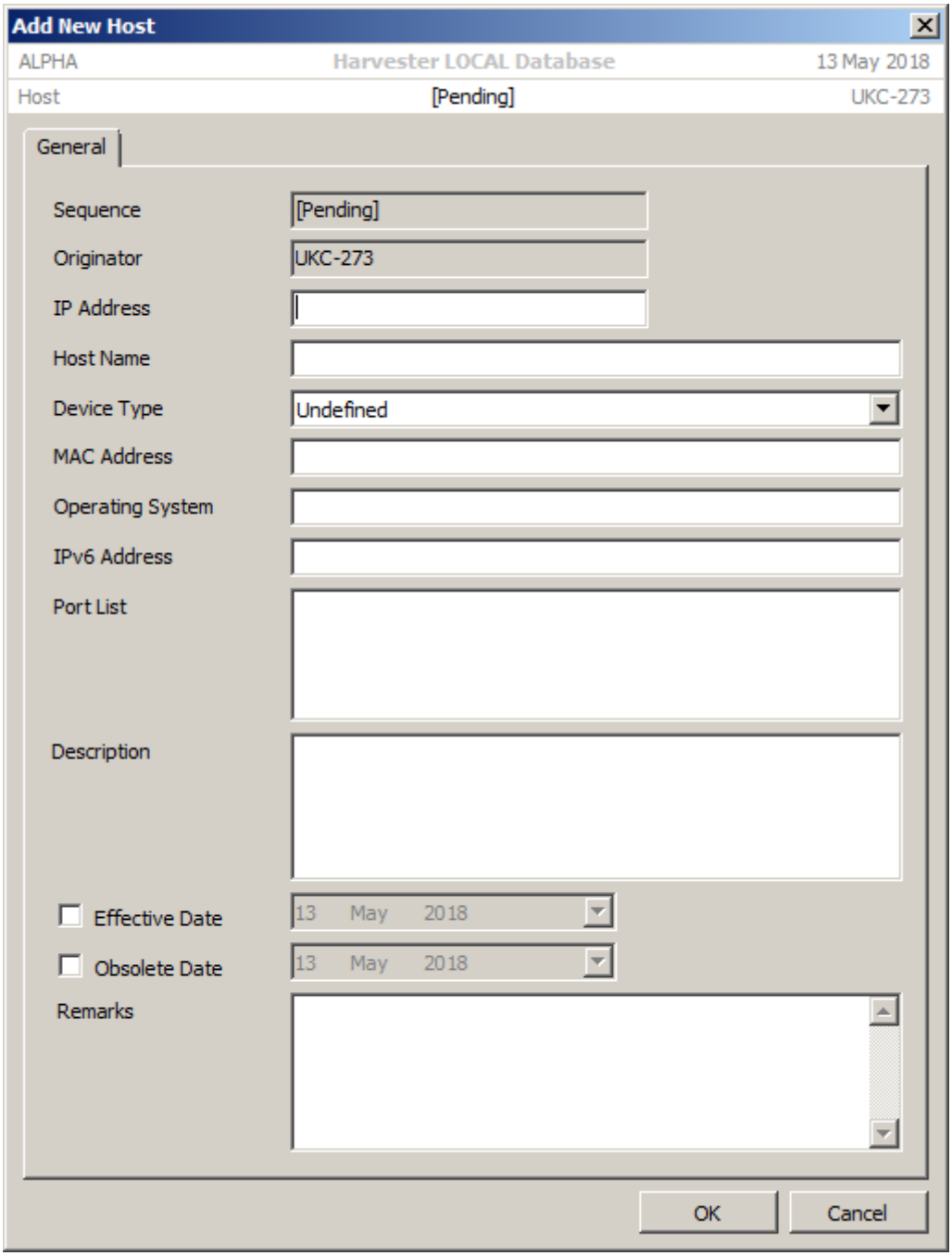
Just as important as postal address are the email addresses and URLs of numerous services. Each address adds an additional layer of information about the entity, making it easier to identify in communications, and assisting in the development of the organisational profile.

To add a new Internet address, select the **Internet Addresses** tab then select the Entity from the organisational hierarchy. Click the **Add** button on the toolbar to open the **Add New Internet Address** window.



6.3.7 Adding a Host

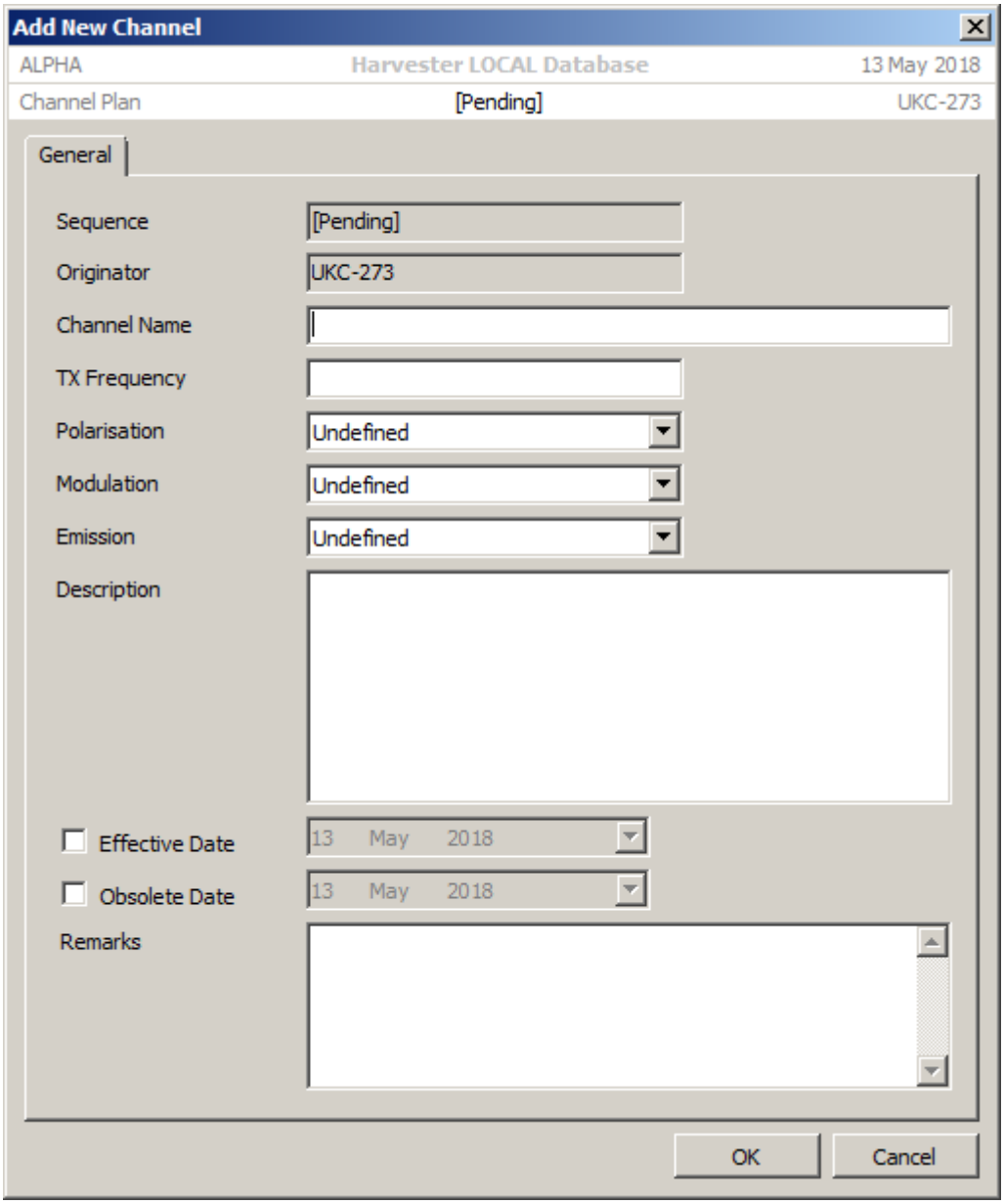
Developing on internet addresses are the servers, workstations and network devices attached to the internet. To add a new host, select the Host tab then select the Entity from the organisational hierarchy. Click the Add button on the toolbar to open the Add New Host window.



6.3.7 Adding a Channel Plan

Although an organisation may be licensed to use any number of frequencies, most if not all organisations refer to these frequencies not in terms of their kilohertz or megahertz values but by some easily conveyed indicator. It may be in plain language or encrypted, static or periodically changing, logical or completely meaningless but will nonetheless convey a specific frequency to echelons and elements that require to know. Channel indicators or designators, as they are often called, are used by a wide range of

organisations to both protect frequency information and make referencing to operating frequencies much simpler.



To add a new Channel, select the **Channel Plan** tab then select the Entity from the organisational hierarchy. Click the **Add** button on the toolbar to open the **Add New Channel** window.

7. GSM Mapper

signals intelligence (SIGINT): 1. *A category of intelligence comprising, either individually or in combination, all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted. [JP 1-02]* **2.** *Intelligence derived from communications, electronics, and foreign instrumentation signals. [JP 1-02]*

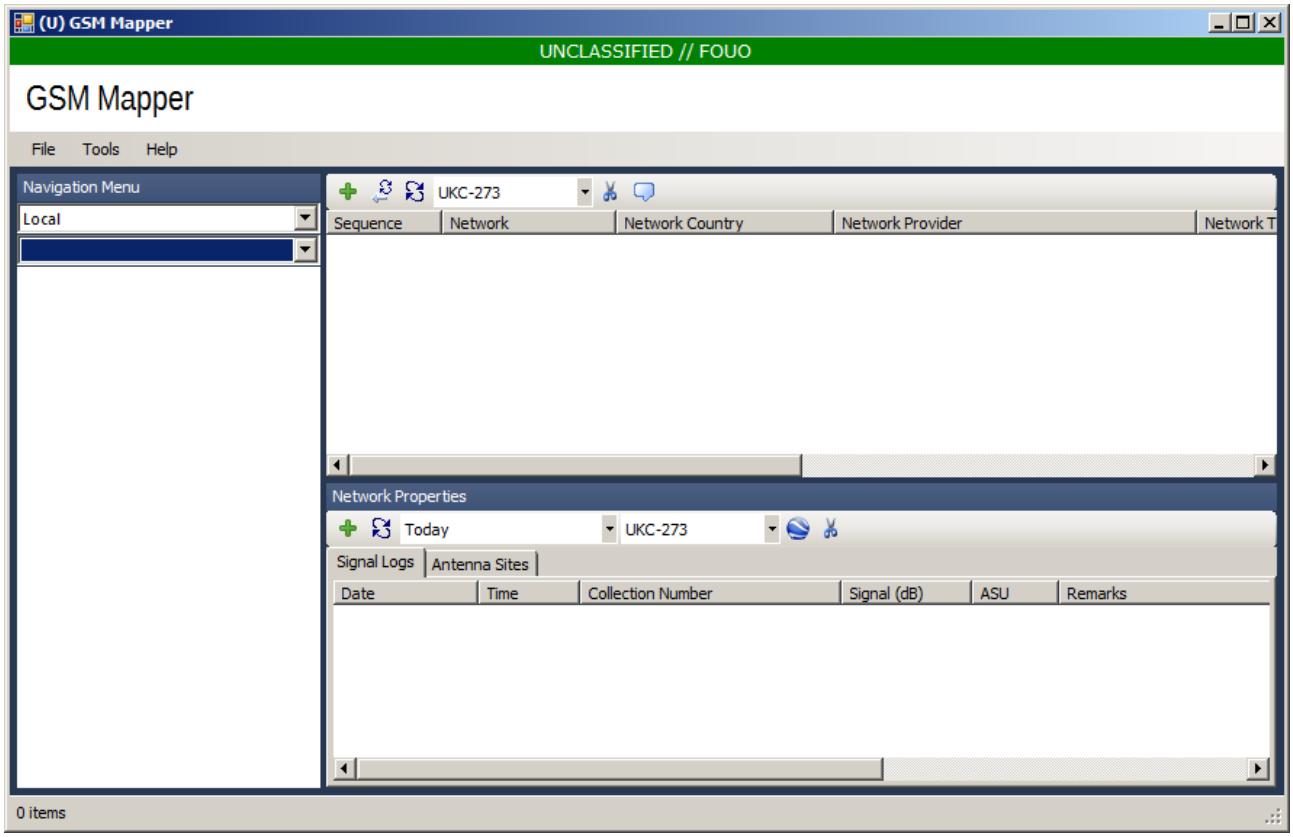
This functionality is not available in the HARVESTER Lite Version

This is a new feature in HARVESTER 6 to meet requirements for mapping GSM mobile telephone networks. Mobile telephones have been in use for well over 40 years using a variety of transmission protocols and technologies from early analogue signals to the encrypted digital systems that are used today by an estimated 7 billion users worldwide. This number continues to grow each year.

Although encryption has effectively taken voice and data collection out of the reach of non-governmental intercept operators, the structure of these networks can still provide a wealth of information on the distribution of service providers, their tower instrastructure and the signal coverage of individual nodes and cells.

Behind all mobile telephone networks are the trunk networks that route signals to and for towers. These are often carried by fibre but many towers still relay on a co-located microwave antenna. Mapping the location and azimuth of these antennas can provide a detailed map of a network.

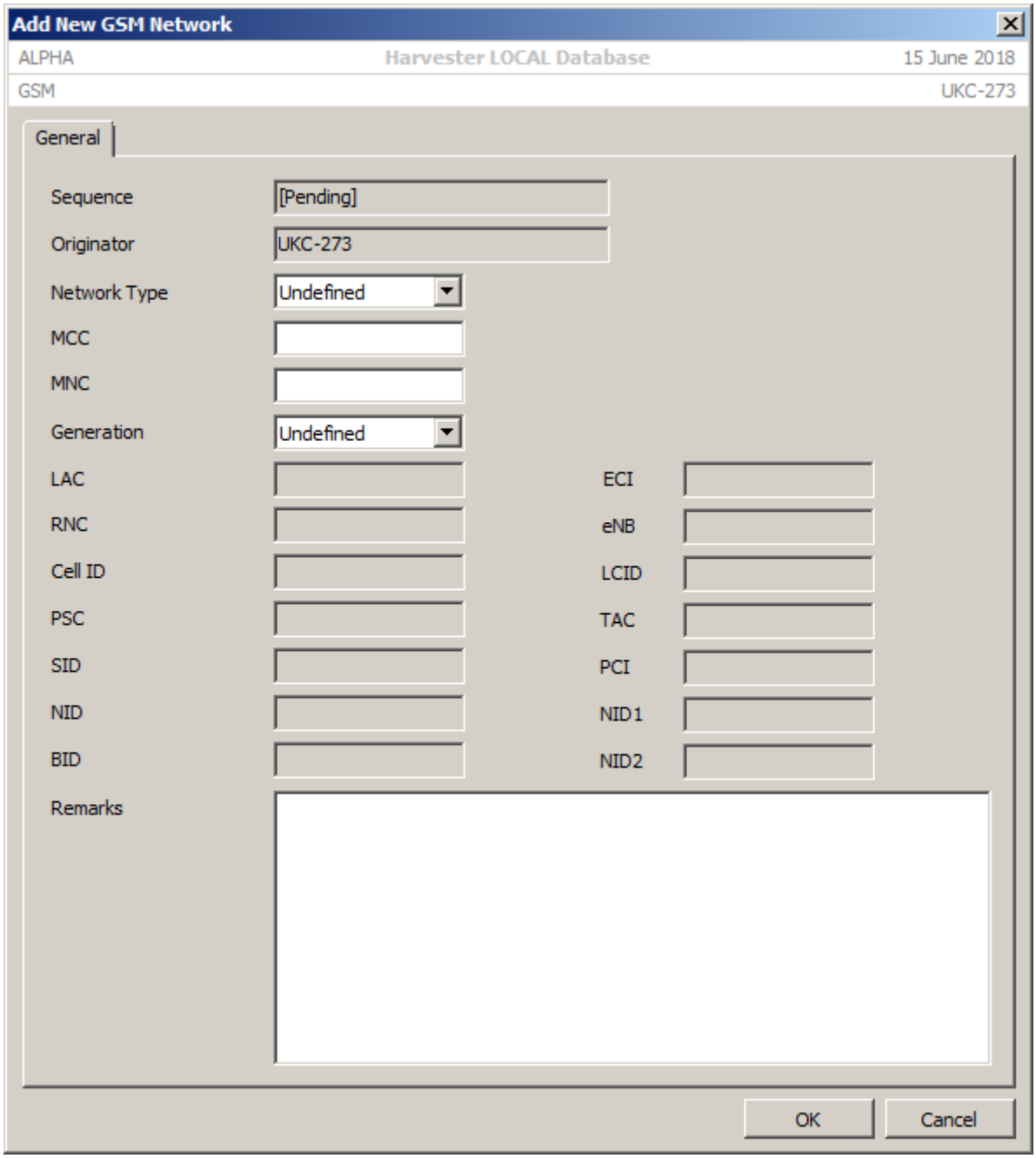
The GSM Mapper module can be accessed from the Collection Modules menu on the main HARVESTER screen.



The screen is organised by country and location information is maintained by the **Geolocation** module (See Chapter 5). Simply select the country you are interested in from the Country dropdown list, then select and expand the appropriate location to begin to add new networks.

7.1 Adding a New GSM Network

To add a new GSM network, navigate to and select the appropriate location in the navigation menu then click on the **Add** icon. This will open the **Add New GSM Network** screen.



Each network is given a sequence number and this will be allocated when the network is saved for the first time.

➢ **Network Type**. This is the network protocol used:

- **CDMA**. Code Division Multiple Access
- **EDGE**. Extended Data Rates for GSM Evolution.
- **EVDO**. Evolution Data Optimised.
- **GSM**. Global System form Mobile communications
- **HSPA**. High Speed Packet Access
- **HSPA+**. Evolved High Speed Packet Access or 4G
- **LTE**. Long Term Evolution.
- **WCDMA**. Wideband Code Division Multiple Access

➢ **MCC**. This is the Mobile Country Code which uniquely identifies the country in which the service is being provided.

➢ **MNC**. This is the Mobile Network Code which uniquely identifies the service provider with the country in which the service is being provided.

➢ **Generation**. This defines the technology generation of the network.

➢ **System Settings**. Each GSM network type use a different set of parameters to define and operate their network. As the Network Type is selected from the dropdown, the relevant parameter fields will be enabled for editing. The available parameters are:

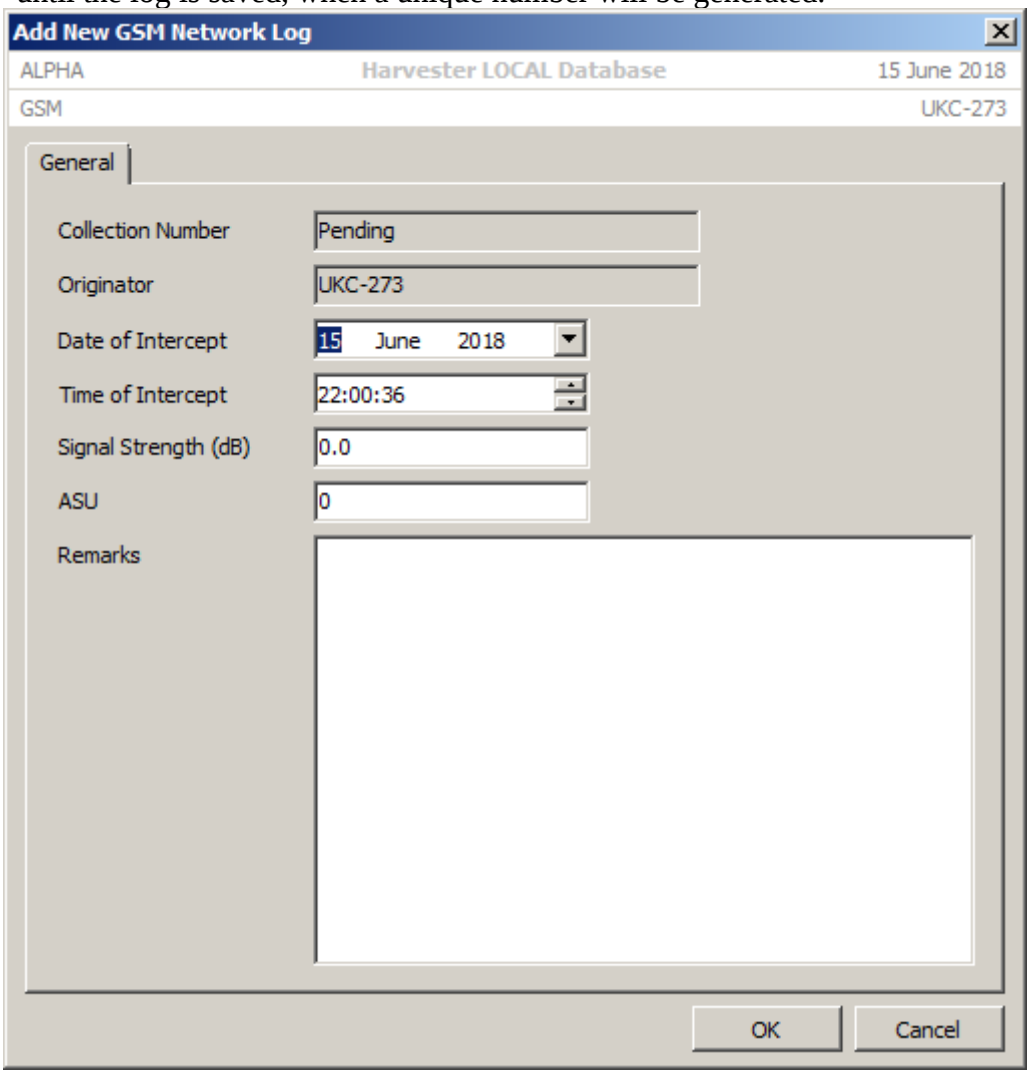
- **LAC**. Location Area Code.
- **RNC**. Rdio Network Controller.
- **Cell ID**, The GSM Cell ID identifies each cell node within each LAC.
- **PSC**. Local Network Cell ID.
- **SID**. The 15-bit System ID.
- **NID**. Network ID.
- **BID**. Base Station ID.
- **ECI**. The E-UTRAN Cell ID.
- **ENB**. The eNodeB ID.
- **LCID**. The UTRAN Cell ID which is the contcatenation of the 12-bit RNC and the 16-bit Cell ID.
- **TAC**. The 16-bit Tracking Area Code.
- **PCI**. The Physical Cell ID.
- **NID1**. Network ID 1.
- **NID2**. Network ID 2.

7.2 Adding a New Log

To add a new log, select the **Signal Logs** tab then select the appropriate network from the availble list. Click on the **Add** button in the toolbar to open the **Add New GSM Network Log** screen.

The **GSM Network Log** screen is primarily designed to record the signal strength of individual networks and signals at different intercept locations. The screen will open the report form and pre-populate key fields with relevant information as Log Originator,

Date of Intercept and Time of Intercept. The Collection Number will appear as Pending until the log is saved, when a unique number will be generated.



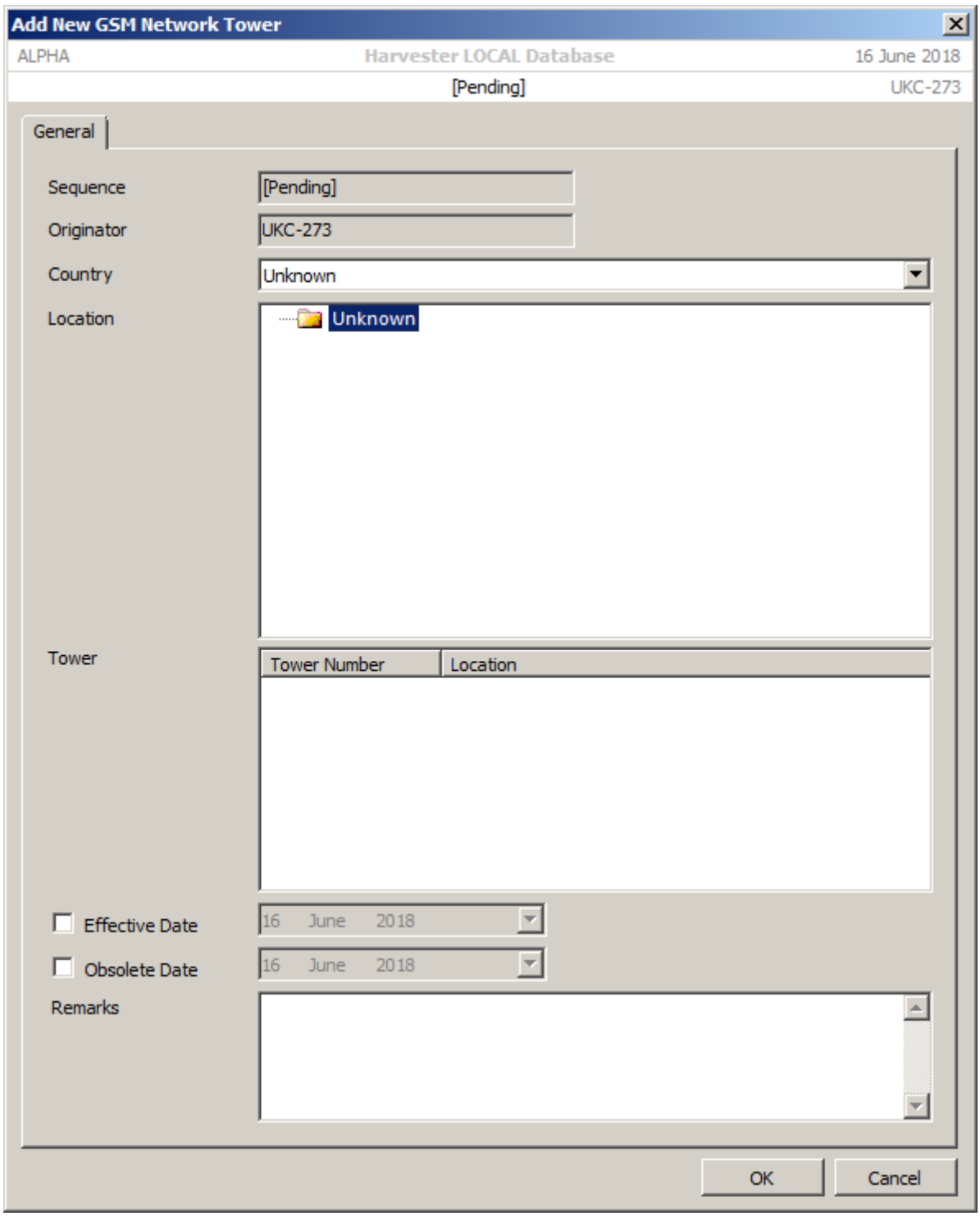
Signal strength can be entered in dB units or in ASU, which can be reed directly from mobile telephone signal monitoring applications, such as Mobile Tower Cell ID or Network Signal Info apps.

7.3 Adding a New Tower

To add a new GSM network tower, make sure you have the **Antenna Sites** tab selected then select the appropriate GSM network from the list then click on the **Add** button in the toolbar to open the **Add New GSM Network Tower** screen.

Select the country from the Country dropdown list. This will automatically load all available loactions in the **Location** box. The location information that appear in the Location box is maintained by the **Geolocation** module (See Chapter 5). Simply select the country you are interested in from the Country dropdown list, then select and expand the appropriate location to find the location you are interested in.

Once a location has been selected, a list of antenna sites associated with that site will appear in the **Tower** box. The tower information that appear in the **Tower** box is maintained by the **Antenna Mapper** module (See Chapter 9).

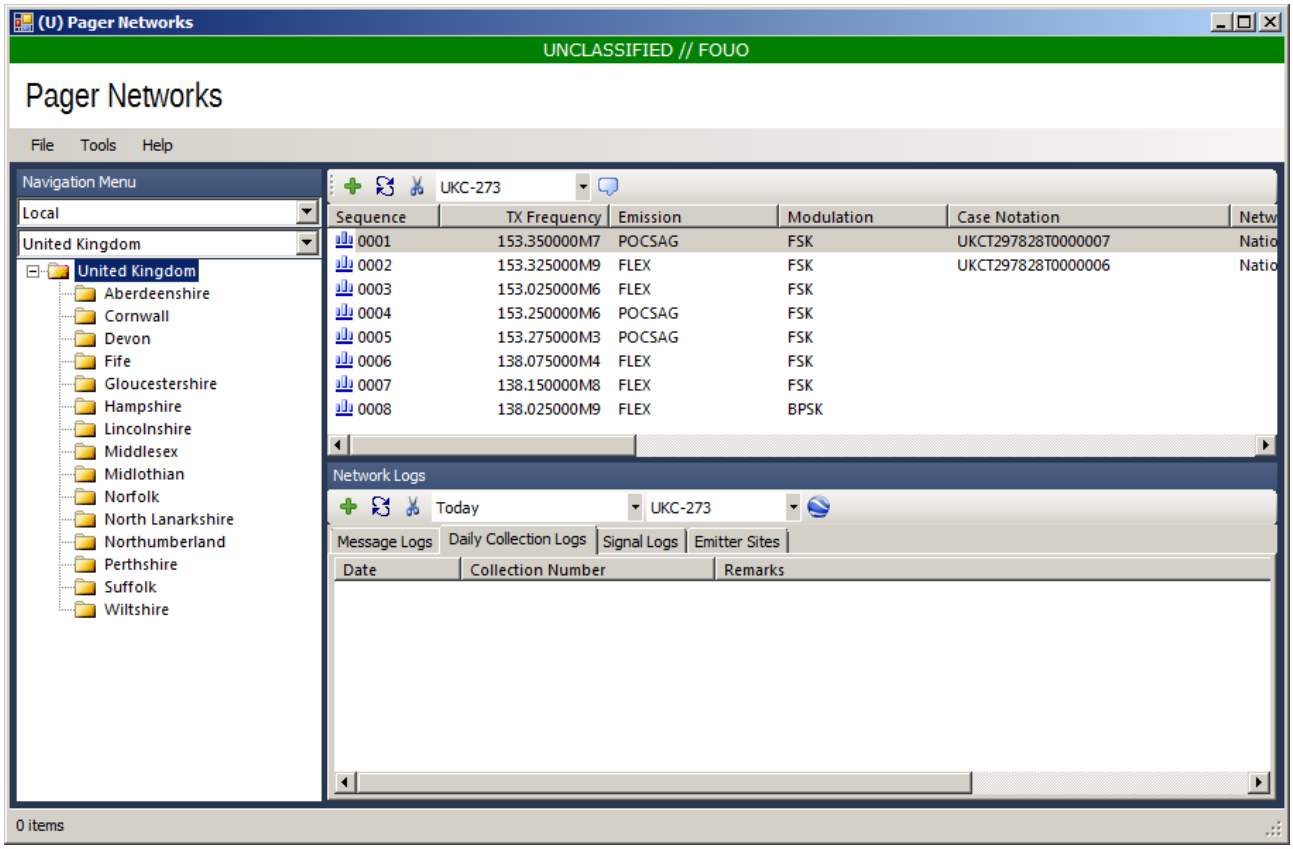

Add New GSM Network Tower
ALPHA
Harvester LOCAL Database
16 June 2018
[Pending]
UKC-273
General
Sequence
[Pending]
Originator
UKC-273
Country
Unknown
Location
Unknown
Tower
Tower Number
Location
Effective Date
16 June 2018
Obsolete Date
16 June 2018
Remarks
OK
Cancel

8. Pager Networks

signals intelligence (SIGINT): 1. *A category of intelligence comprising, either individually or in combination, all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted. [JP 1-02]* **2.** *Intelligence derived from communications, electronics, and foreign instrumentation signals. [JP 1-02]*

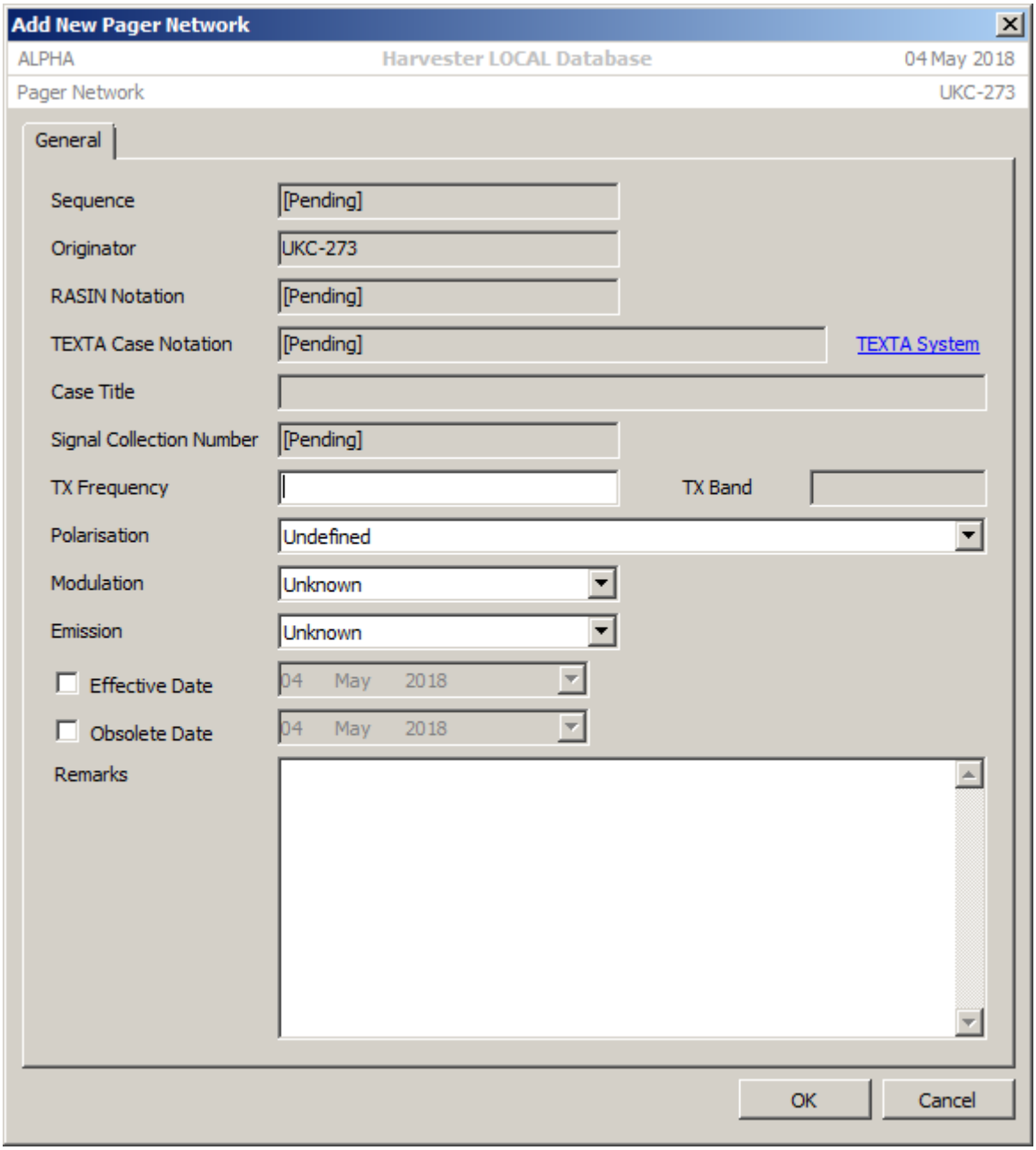
This functionality is not available in the HARVESTER Lite Version

This is new feature in HARVESTER 6 to meet requirements for the collection of national, regional and local area Pager networks. Pagers first appeared in the 1950s and over the years, have become smaller in size, have increased in functionality, and surprisingly, as analogue technology, have survived well into the digital age. To open the Pager Network screen, click Pager Networks in the Collection Modules menu.



8.1 Adding a New Network

To add a new pager network, navigate to the appropriate location then click on the **Add** icon. For nationwide pager networks, ensure that the top level country node is selected. For regional or local networks, select the area or installation where the network is operational.



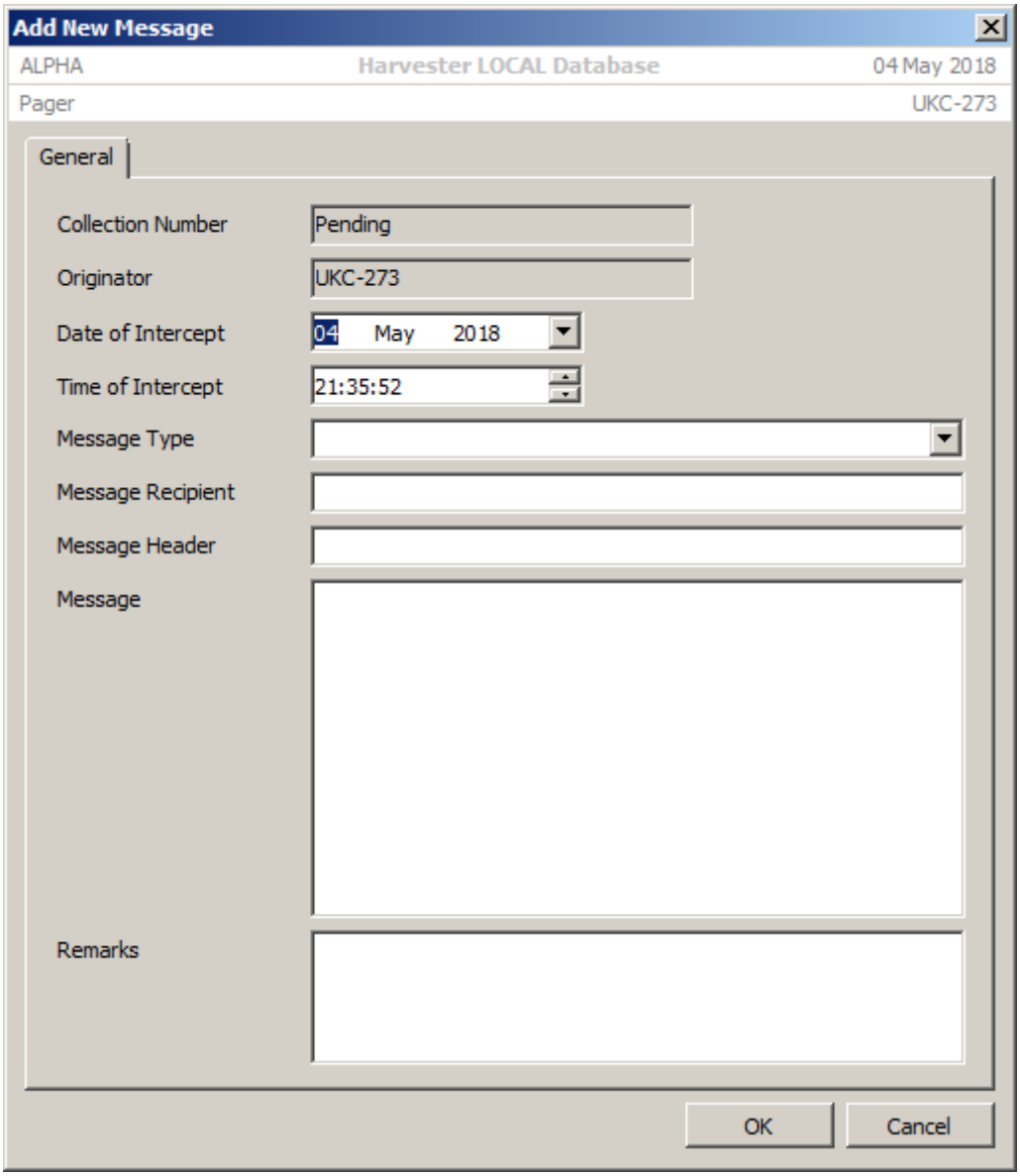
Enter the frequency, emitter polarisation if known, and the modulation and emission of the network. At this stage, you may also wish to define the network's TEXTA Case Notation. Click the TEXTA System link to open the **Case Notation Selection** screen. Once all the details of the network have been entered, click the **OK** button to save the record. The record will automatically be added to the network list along with an auto-generated sequence number.

8.2 Adding a New Message Log

To add a new message log, ensure that the appropriate pager network and Message Logs tab are selected then click on the **Add New** icon in the Networks Logs section of th escreen. This will open the **Add New Message** screen.

This screen is designed to log individual messages along with details of the message type and the message recipient. Note the each message will be given a unique Collection

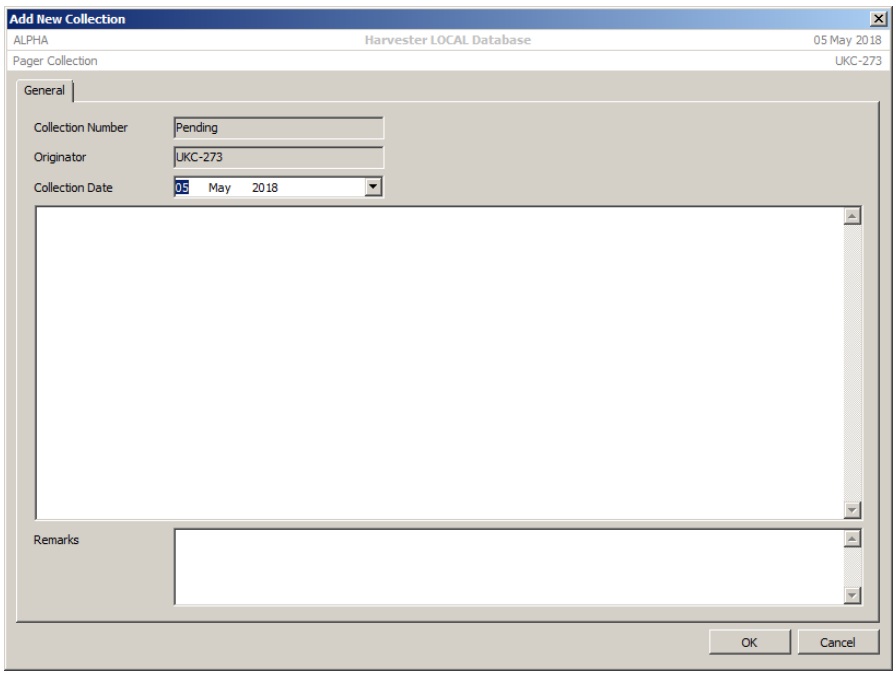
Number. This is unique to every installation and uniquely identifies the message and collecting station.



8.3 Adding a New Daily Collection Log

To add an entire log of messages collected over a period of time, the Daily Collection Log is ideal for this purpose. It provides the facility to record bulk collection logs for a selected network to be anaylsed at a later date.

To add a new Daily Collection Log, ensure that the appropriate pager network and Daily Collection Logs tab are selected then click on the **Add New** icon in the Networks Logs section of the screen. This will open the **Daily Collection Log** screen. Paste the logs into the log box and click the **OK** button to save the log.

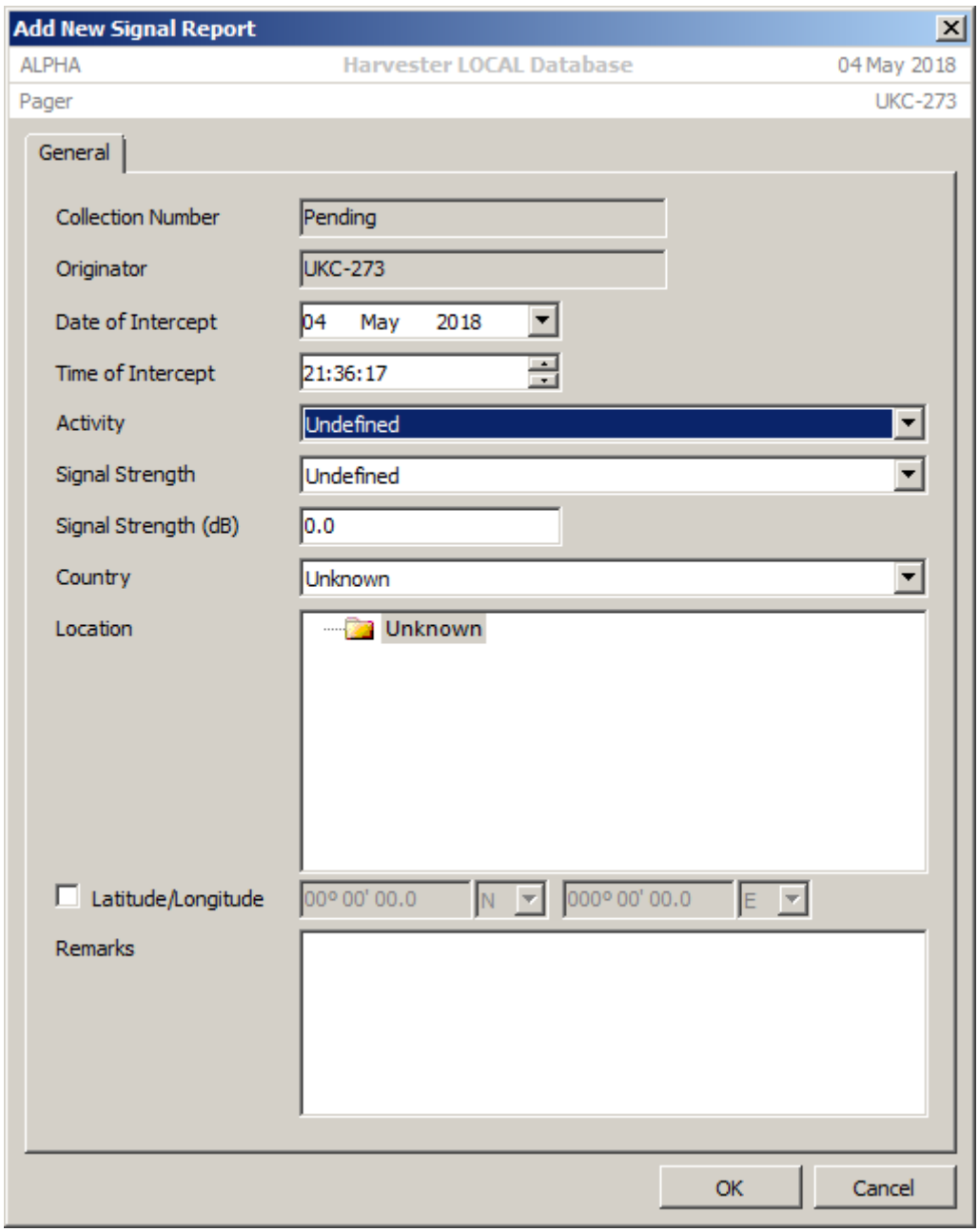


8.4 Adding a New Signal Log

As well as logging actual networks and messages, it is often useful to log signal strengths of networks, especially in the context of developing reports on signals collection environments. Regular logging of received signal strengths can be used to build up a picture of exactly which stations have the best collection opportunities for individual networks. It also provides a useful log of local signal strengths.

To add a new Signal Log, select the appropriate pager network from the list of networks. Make sure the Signal Log tab is selected in the Network Logs panel then click the **Add New** icon in the toolbar. This will open the **Add New Signal Log** screen. As well as logging Date and Time, network activity can also be logged. This is particularly useful to logging events such as network tests and general system failures when the network is unavailable. Signal strength can be logged as both a listener's impression as well as a more specific dB reading.

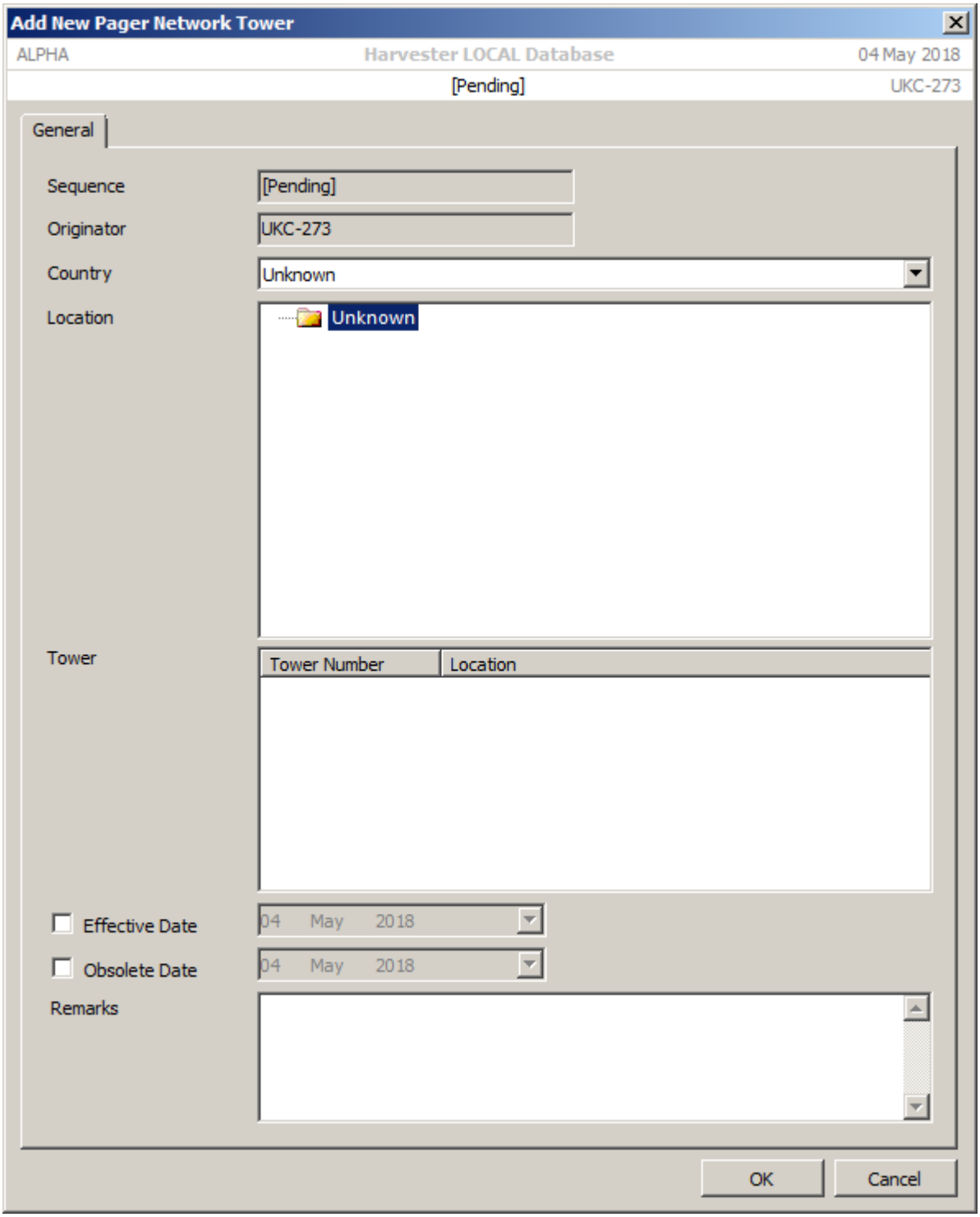
Not only does the screen allow signal logging at the local station, it also provides the facility to produce signal strength maps by storing the location where the log was mode. Generally, this can be left blank as it will be the local station's location but should logs be made during mobile collection, the location as well as latitude and longitude can be recorded.



8.5 Adding a New Emitter Site

Often the final stage of network analysis is the determining of transmitter and emitter sites. Pager networks offer a unique challenge in that as well as opertaing at a very local or regional level, like GSM networks. They can also operate at a national level, often meaning the emitters can number in the tens of thousands. The will also be supported by a further network that routes traffic to these emitters.

To add a new emitter location, select the appropriate pager network from the list of networks. Make sure the Emitter Sites tab is selected in the Network Logs panel then click the **Add New** icon in the toolbar. This will open the **Add New Pager Network Tower** screen. When the emitter location has been determined, first select he country. This will populate the current available locations (defined in Geolocation). Selecting a locationm will produce a list of known antenna sites at the location (defined in Antenna Sites). Simply select the appriopriate antenna site or tower and click **OK**.


Add New Pager Network Tower
ALPHA
Harvester LOCAL Database
04 May 2018
[Pending]
UKC-273
General
Sequence
[Pending]
Originator
UKC-273
Country
Unknown
Location
Unknown
Tower
Tower Number
Location
Effective Date
04 May 2018
Obsolete Date
04 May 2018
Remarks
OK
Cancel

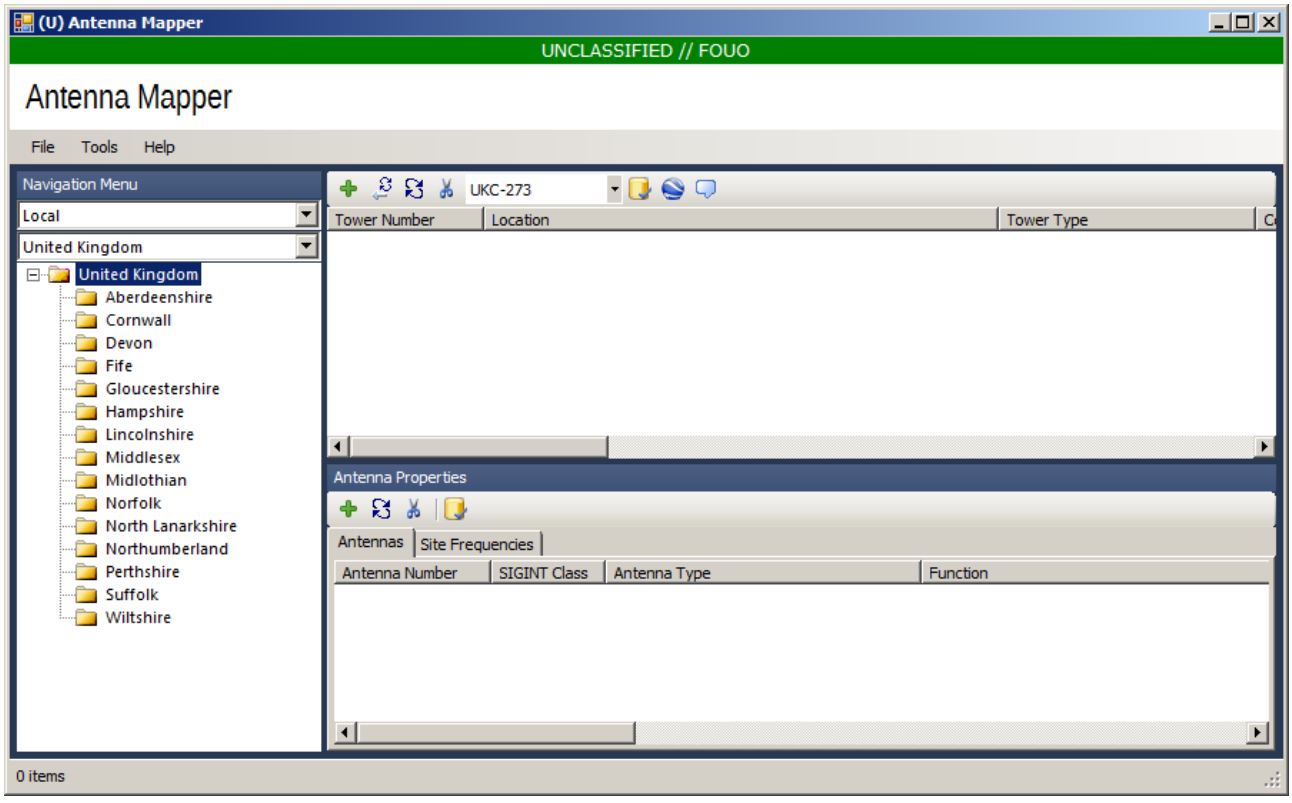
9. Antenna Mapper

signals intelligence (SIGINT): 1. *A category of intelligence comprising, either individually or in combination, all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted. [JP 1-02]* **2.** *Intelligence derived from communications, electronics, and foreign instrumentation signals. [JP 1-02]*

This functionality is not available in the HARVESTER Lite Version

One of the key elements to understanding and successfully analysing any communications network is the ability to identify the location of the transmitter used to transmit a specific frequency of interest. Not only can this information be used to confirm the country of origin of a signal but often also the user and purpose of the transmission. Knowing the location of the transmitter site will also help in estimating the likelihood of reception, something that is particularly useful with line-of-sight frequencies above 30 MHz.

To facilitate the gathering of such information, the Antenna Sites screen provides the user with the tools to log and graphically analyse transmitter sites, their relative positions, the antennas associated with these sites and the communications links between individual sites.



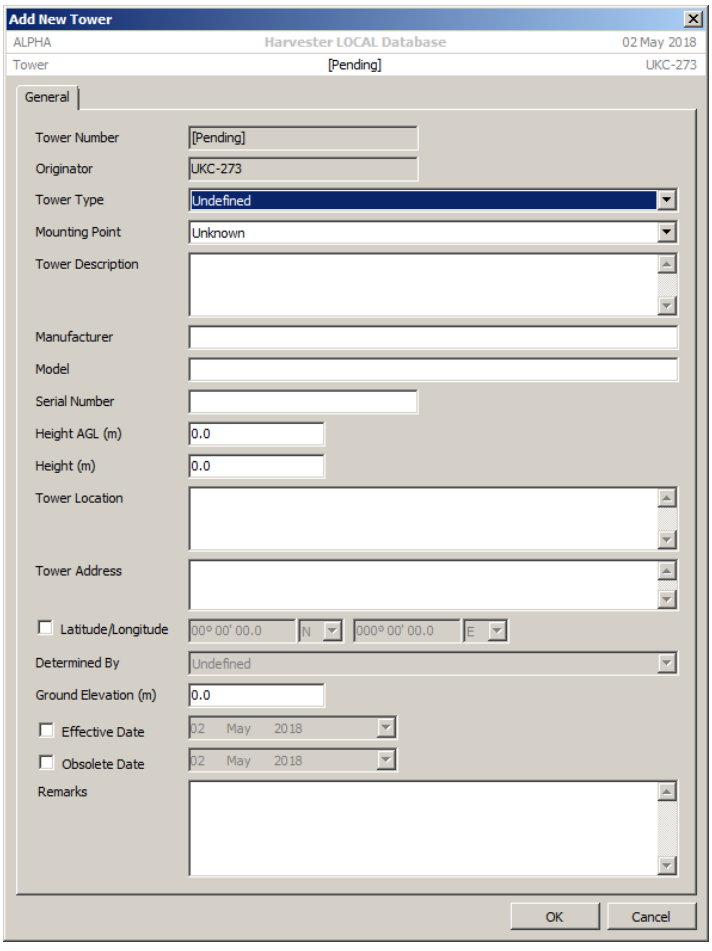
A brief look at any communications site will reveal the presence of any number of antennas of varying size, design and construction. Many will provide omni-directional coverage where the signal can be received over a wide area of countryside or simultaneously at a number of disparate fixed and mobile locations while others will be positioned on very precise bearings to link into a similar line-of-sight antenna at some distant location.

The purpose of the site can often be determined from type of antennas. A multiple vertical element array is indicative of a mobile telephone node, which will very often have an associated

dish through which traffic flows. Tracing the path of the dish will reveal where the node connects into the main network backbone. In some circumstances, nodes may be fed by fibre so there will be no obvious link into the network. Dish antennas can also be used to carry other types of data signals such as telemetry and broadcast links. These signals may be fed into another site antennas for general broadcast or may be further relayed by a co-located dish.

Much of this activity occurs on frequencies in the UHF/SHF range. Directional antennas generally operate above 1 GHz while omni-directional sites operate between 30 MHz and 1 GHz. There is however a sizeable number of sites used to broadcast on frequencies below 30 MHz. By the nature of these signals, antennas are much larger and often take the form of longwire or curtain antennas tens or even hundreds of metres in length and height. Plotting these sites and connecting the various directional antennas can quickly build up a detailed plan of any country's communications network.

To open the **Antenna Mapper** screen, select the **Antenna Mapper** option in the **Collection Modules** menu. The screen is organised by country and location information is maintained by the **Geolocation** screen. Simply select the country you are interested in from the Country dropdown list, then select and expand the appropriate location to begin to add new antenna. Unlike previous versions of HARVESTER, we have moved away from the concept of antenna sites and focussed on the antennas themselves. All antennas have some form of mounting point, be it a tower, a wall, a roof or the ground.



9.1 Adding a New Tower

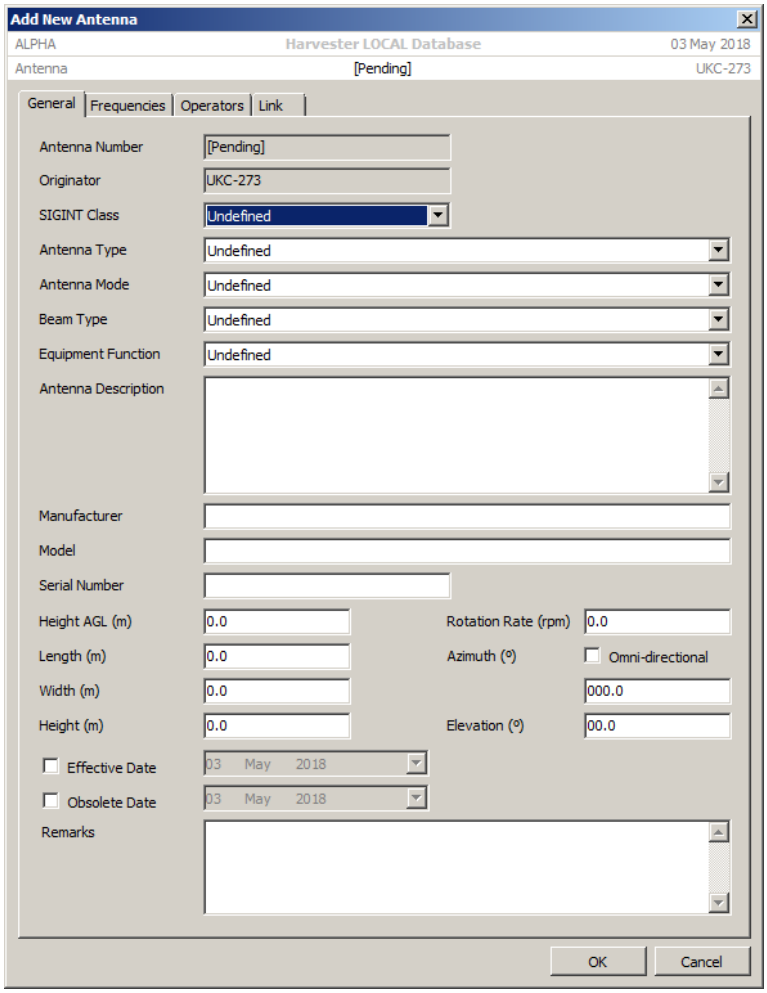
To add a new antenna tower, select the appropriate location then click on the **Add** icon on the main toolbar to bring up the **Add New Tower** screen.

A detailed description of the tower, its make and type as well as manufacturer's details and model number can be entered here along with its physical dimensions. An accurate description of the tower's location and physical appearance can also be entered. To enable accurate plotting of these sites on maps, site latitude and longitude can also be entered. The latitude and longitude of the site can be determined from maps or by obtaining a GPS fix. Most commercial, geopolitical and military maps carry an additional form of grid system, such as WGS84 or UTM, to aid in the identification of locations. Any such grid coordinates can be entered in the **Grid** field but these are not used in site plotting.

Ground elevation, or height above mean sea level (AMSL), is another key feature that aids in the determination of signal reception with line-of-sight frequencies above 30 MHz. Signals transmitted from a site at sea level will be received over a smaller area that a signal beamed from a hill top. This information is readily obtainable from any survey map, or indeed by measuring the site elevation with a GPS.

9.2 Adding a New Antenna

To add a new antenna to an existing tower, select the appropriate tower then click the **Add** button in the **Antenna Properties** section to open the **Add New Antenna** window. On this screen, details and specifications of the antenna, such Type, Mode, as the number of elements in the antenna, its length, width and height, can be added in order that it can be readily identified. Additionally, the azimuth and elevation of directional antennas can also be entered.



Three further tabs allow additional details to be added:

- **Frequencies.** Operating frequencies of individual antennas can be recorded on this tab. The frequency list is derived from the list of site frequencies, and frequencies confirmed as being used by a specific antenna can simply be ticked.

- **Operators.** On this tab, known users of that antenna can be added. Even in the absence of operating frequencies that could be used to confirm the purpose or users of the antenna, corporate markings on antennas can provide useful information as to the nature of the antenna and its users.

- **Links.** This tab allows two directional antenna links to be represented the communications link between both sites. To define a directional link, click the **Add** button to open the **Add New Link** screen.

  On the **Antenna Link** screen, select the country and location where the link station is located. A list of available towers and antennas will be displayed. Select the desired tower, then from the antenna list, select the antenna that is to be linked, then click the **OK** button.

9.3 Adding a New Site Frequency

When a tower supports a single antenna, determining which frequencies that antenna uses is relatively straightforward. When multiple antennas operate from the same tower or co-located with other near-by towers, finding out which antenna radiates which frequency is a little more difficult. To overcome this issue, at least in the initail stages of analysing an antenna tower, operating frequencies can be logged at the tower level.

To add a new frequency, select the Site Frequencies tab and click the **Add** button in the toolbar. This will open the **Add New Frequency** screen. On this csreen you can enter the Frequency, its SIGINT class, modulation and emission as well as its function, and if possible, it can be linked to a known TEXTA circuit.

NOTE Mapping antennas might sound like a strange way of monitoring communications but each antenna represents an individual emitter. If its operating frequencies are known that it provides confirmation of the emitter's location, if not, then it represents an emitter that is yet to be discovered and another a potential source of communications to be exploited.

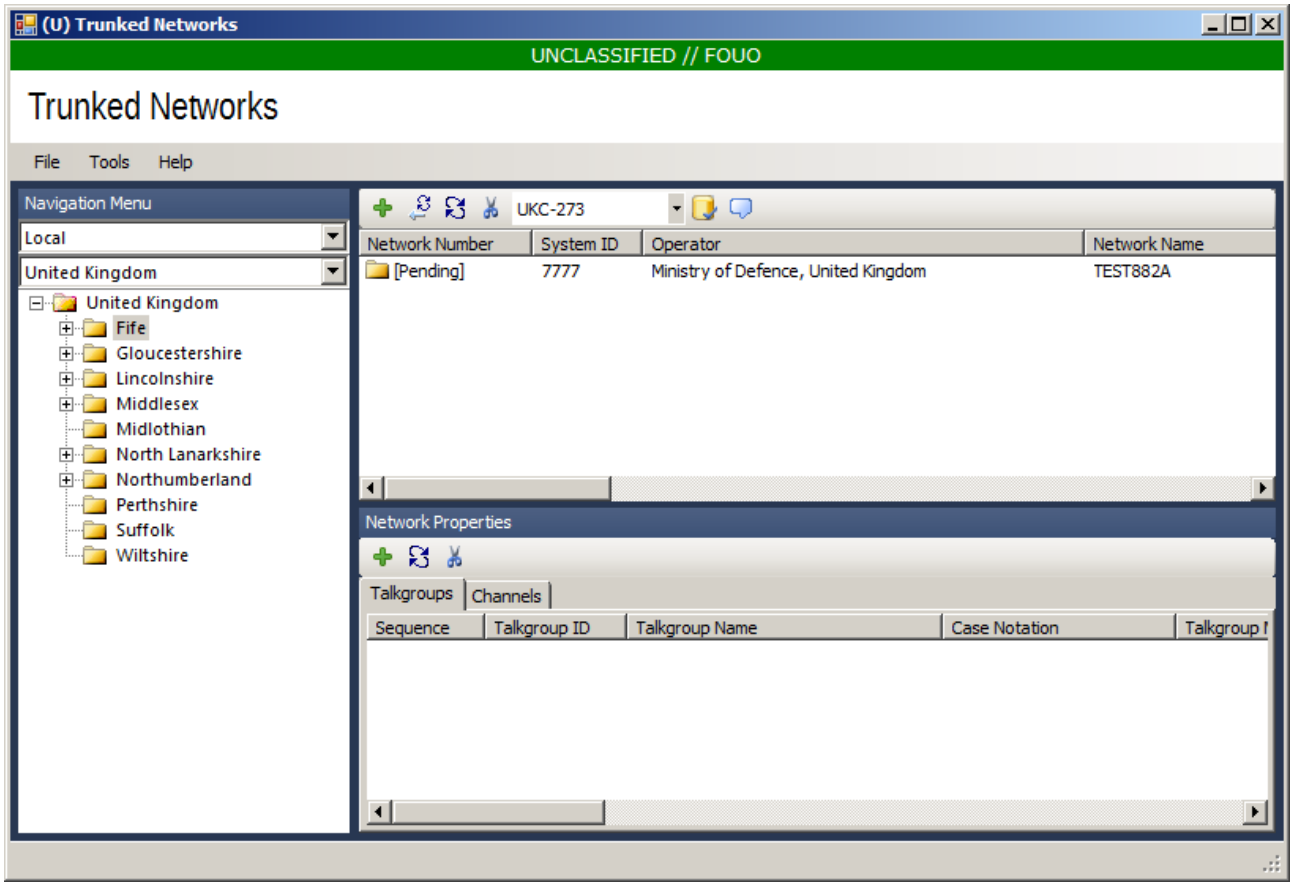
10. Trunked Networks

signals intelligence (SIGINT): 1. *A category of intelligence comprising, either individually or in combination, all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted. [JP 1-02]* **2.** *Intelligence derived from communications, electronics, and foreign instrumentation signals. [JP 1-02]*

This functionality is not available in the HARVESTER Lite Version

As the number of radio users continues to rise in an ever-diminishing bandwidth, the reliance on trunked radio networks for efficient use of the radio spectrum continues to increase. It is therefore essential that HARVESTER can handle trunked radio logs just like another other transmission. The **Trunked Networks** screen was a new addition in Version 3 and continues to provide additional intercept flexibility to operators who require to accurately log these signals.

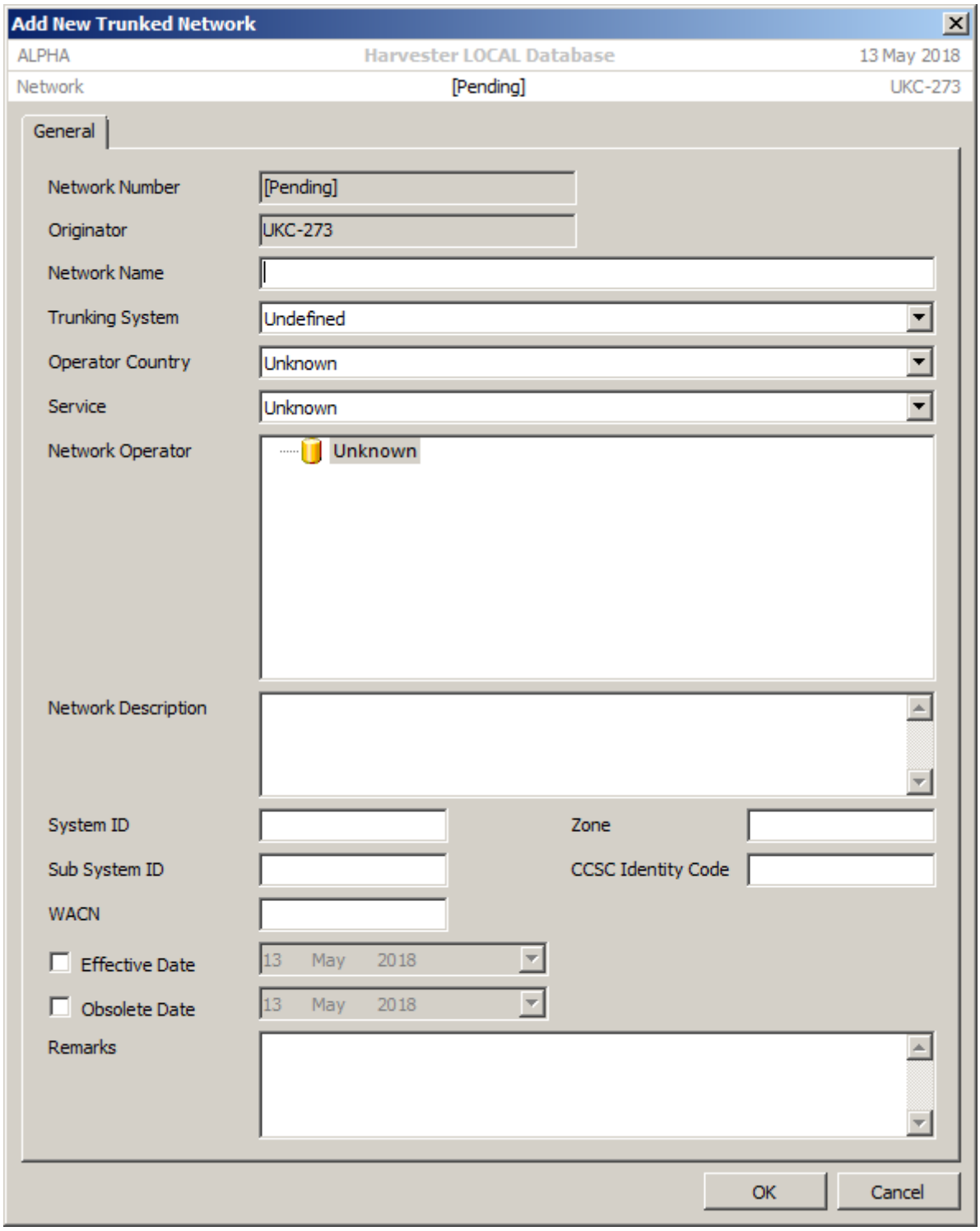
Trunked networks were once the preserve of large corporate and government users but a reduction in the cost of accessing this technology has provided even small scale organisations with trunked radio capacity.



The **Trunked Networks** screen can be accessed from the main screen by clicking the **Trunked Networks** option in the **Collection Modules** menu.

10.1 Adding a New Network

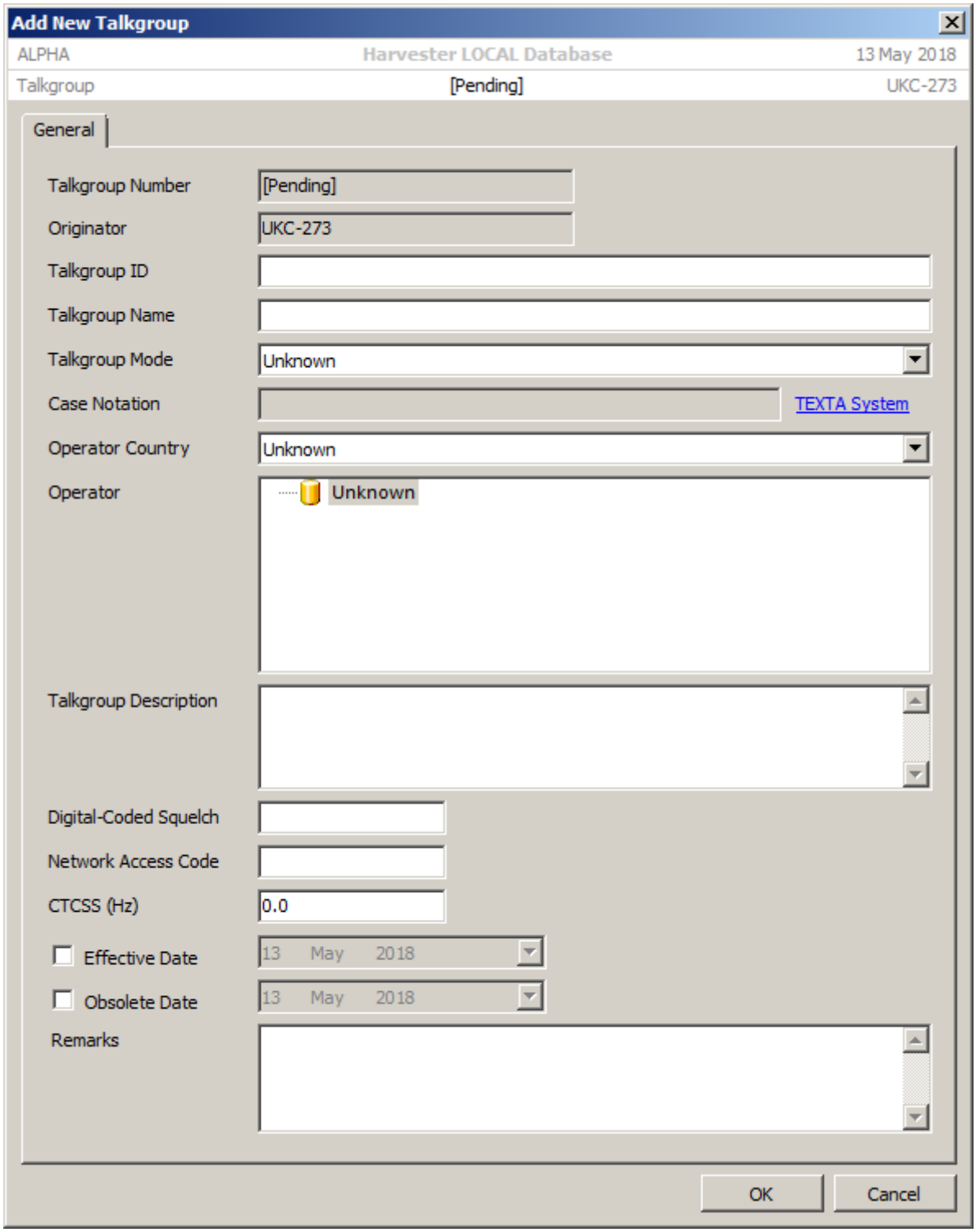
To add a new Network, select the appropriate country and location from the geolocation hierarchy then click the **Add** button in the toolbar. This opens the **Add New Trunked Network** screen.



Enter the network name, type of trunking system protocol, details of the network operator or provider and their location, a description of the network and any network parameters that are know. In the case of digital networks, details may require a little more analysis to determine the parameters.

10.2 Adding a New Talkgroup

Once a **Trunked Network** has been defined, **Talkgroups** can be added to the network. To add a new Talkgroup to a network, select the appropriate **Trunked Network** from the Network list then click the **Add** button on the toolbar. This will open the **Add New Talkgroup** screen.

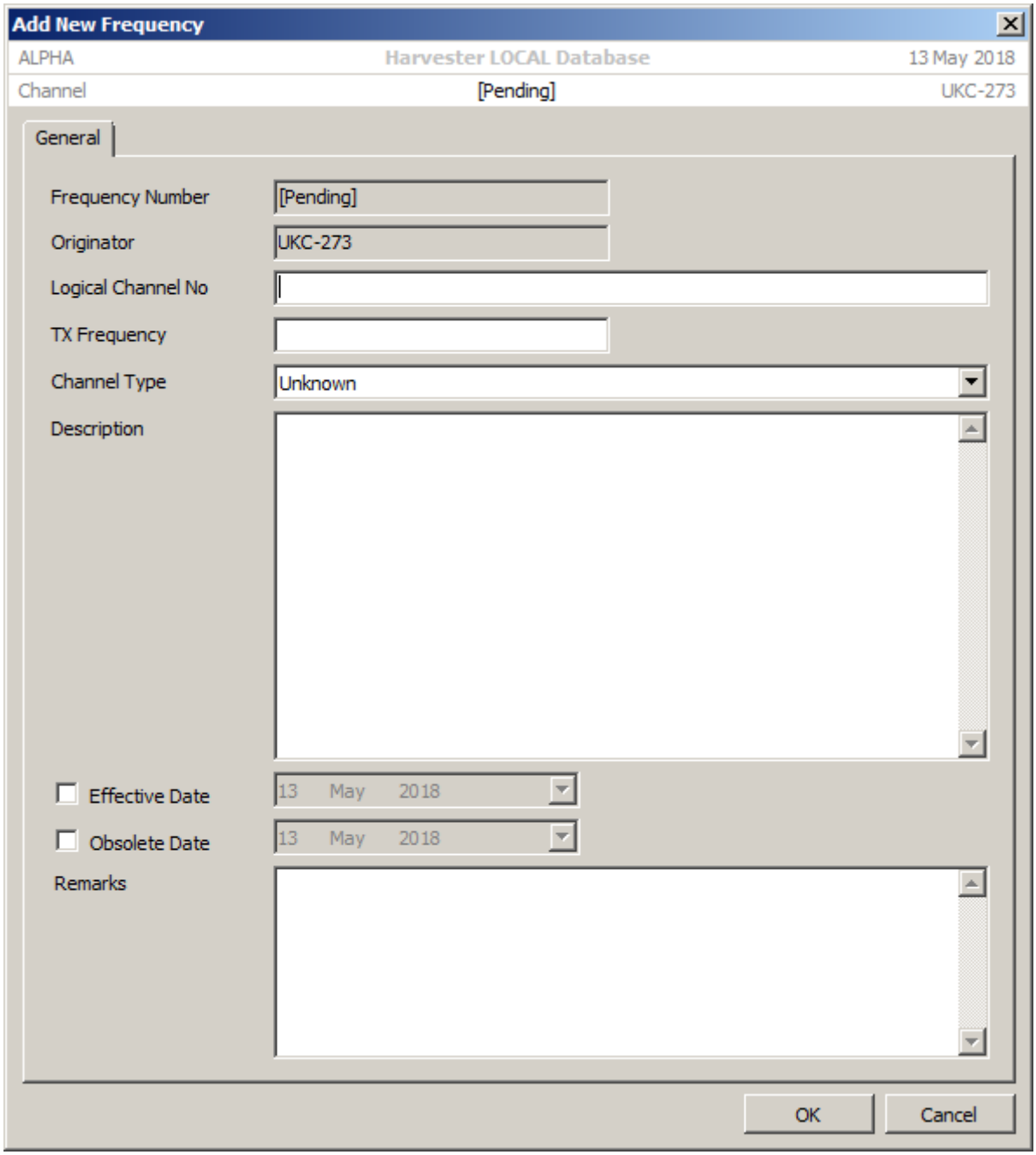


➢ **Talkgroup ID**. Each **Talkgroup** within a **Trunked Network** is identified by a numerical group. This Talkgroup code would also be used when programming radios to access the Talkgroup.

➢ **Talkgroup Name**. To made the Talkgroup identity more user-friendly most Talkgroups will also be referred to by a Talkgroup Name.

10.3 Adding a New Channel

To add a new Frequency, select the appropriate **Trunked Network** from the Network list then click the **Add** button on the toolbar. This will open the **Add New Frequency** screen.



Enter the channel's logical name within the network, its frequency's and the type of channel.

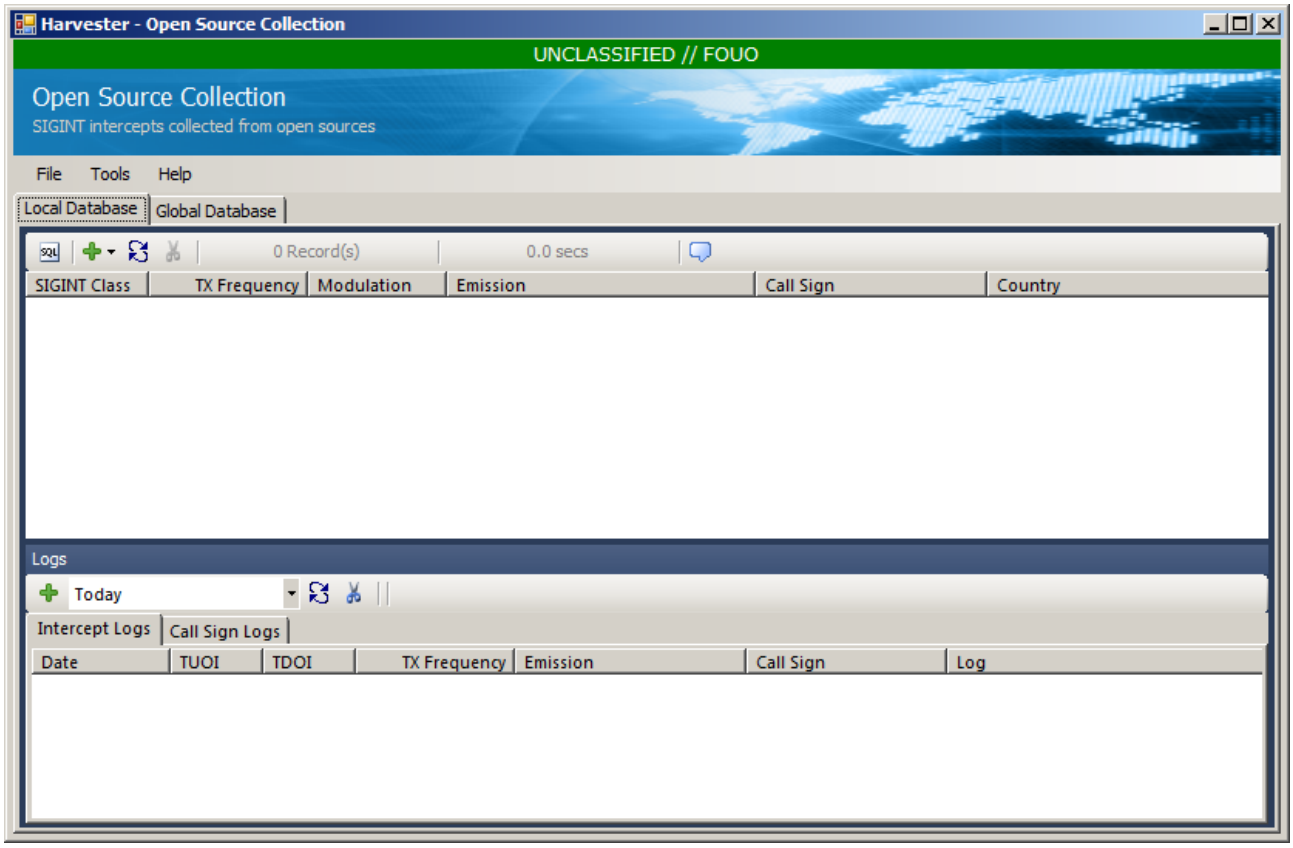
11. Open Source

signals intelligence (SIGINT): 1. *A category of intelligence comprising, either individually or in combination, all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted. [JP 1-02]* **2.** *Intelligence derived from communications, electronics, and foreign instrumentation signals. [JP 1-02]*

This functionality is not available in the HARVESTER Lite Version

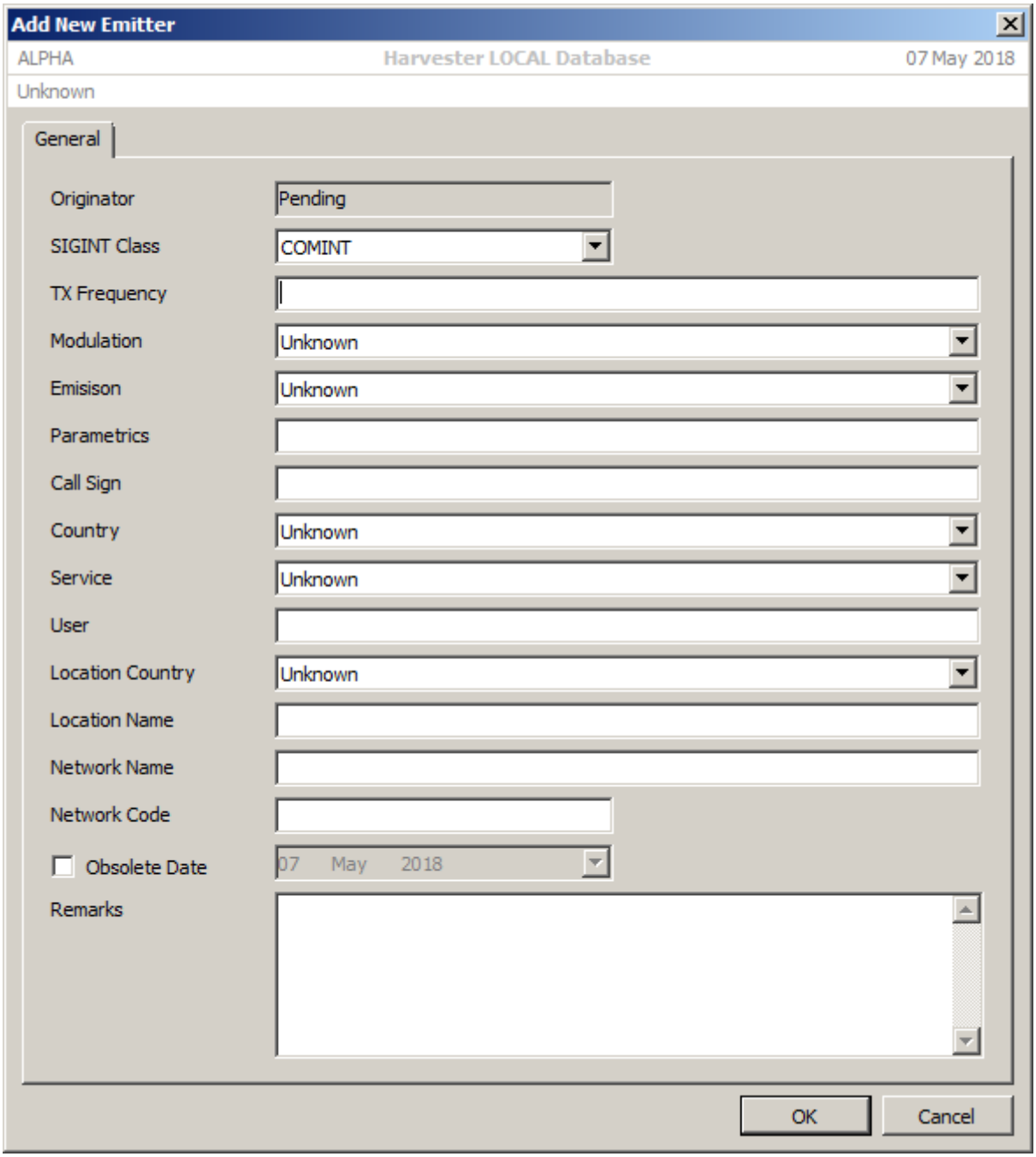
Open Source Collection is a new feature in HARVESTER 6 and is intended to tap into the extensive logging undertaken by many online radio groups and publications as well as a wealth of historic logs that appear in old radio magazines. In terms of analysis of radio systems and networks, any and all logs are an absolute goldmine of information. Often seemingly insignificant logs, partial messages and callsigns are recorded only to suddenly prove to be the missing part of network analysis or the vital clue that finally adds context to an analysis problem. Of course, not all open source logs will prove to be so valuable but they are nonetheless an incredibly rich resource that cannot afford to be ignored.

As the accuracy and provenance of Open Source logs cannot always be guaranteed, this self-contained module is provided for recording them, completely isolated from the main HARVESTER logs but easily accessible to enter and search. The Open Source Collection module can be accessed by clicking the Open Source Collection open in the Collection Modules menu on the main HARVESTER screen.



11.1 Adding a New Frequency

To add a new Frequency to the Open Source Collection module could not be easier. Click the **Add** button in the toolbar and from the dropdown menu, select **Add New Emitter**. This will open the **Add New Emitter** screen.

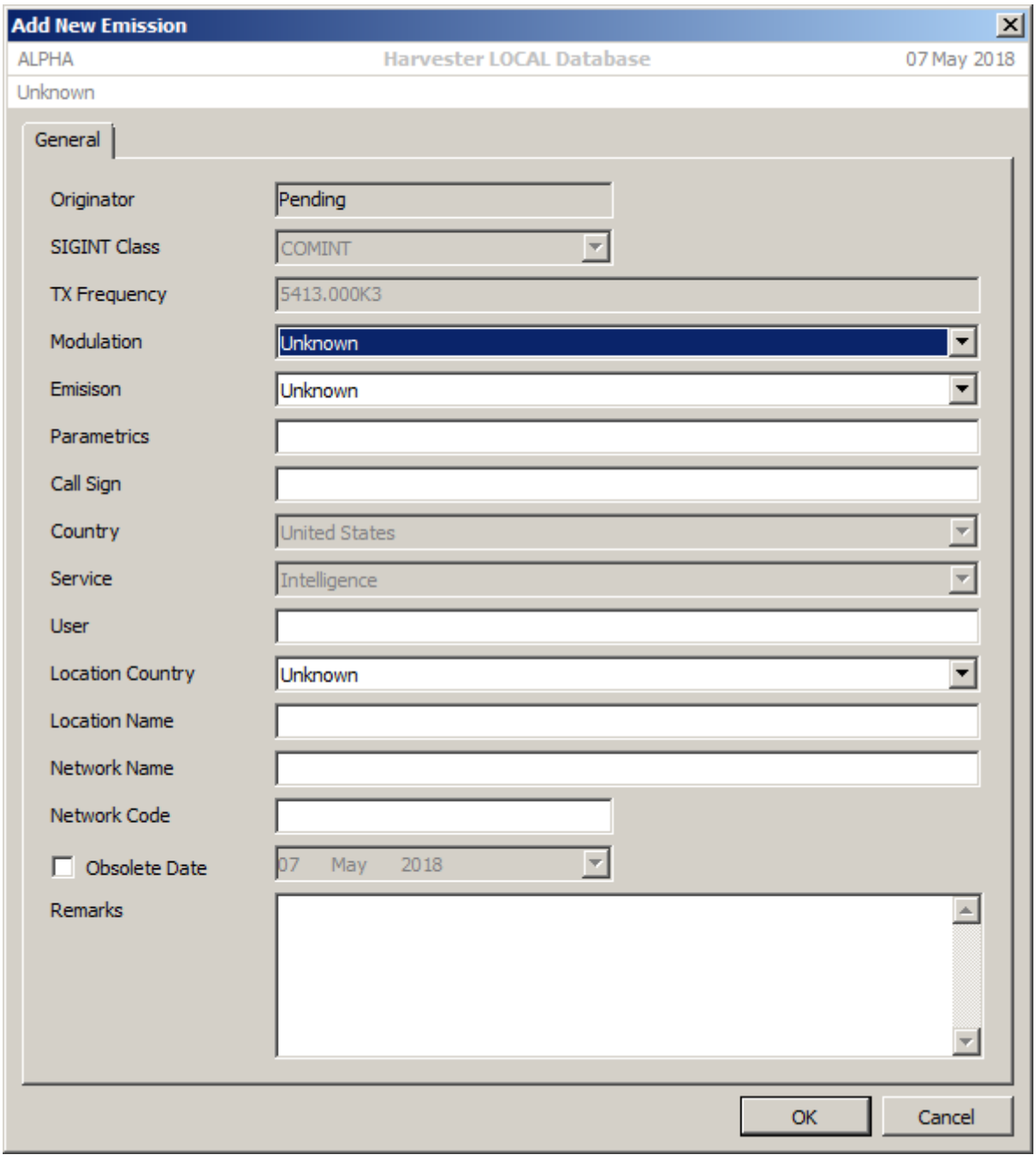


Both COMINT and ELINT emitters can be added along with frequency, modulation, emission and various other details. This information is typically derived from the basic log with more specific net activities being logged as an Intercept Log. The emitter record provides an opportunity to store information that makes it unique from other emitters on the same frequency. Remember that just because two similar emissions occur on the same frequency doesnot confirm that they are from the same user or indeed as operating in the same network. Details such as Country, Service and User can aid in the unique identification of the nework, and subsequently future logs recorded against the correct emitter.

NOTE At the emitter level, both Network Name and Network Code can be entered. While the former can be accepted name of the network, the latter can be used as an alias, such as the Enigma 2000 code.

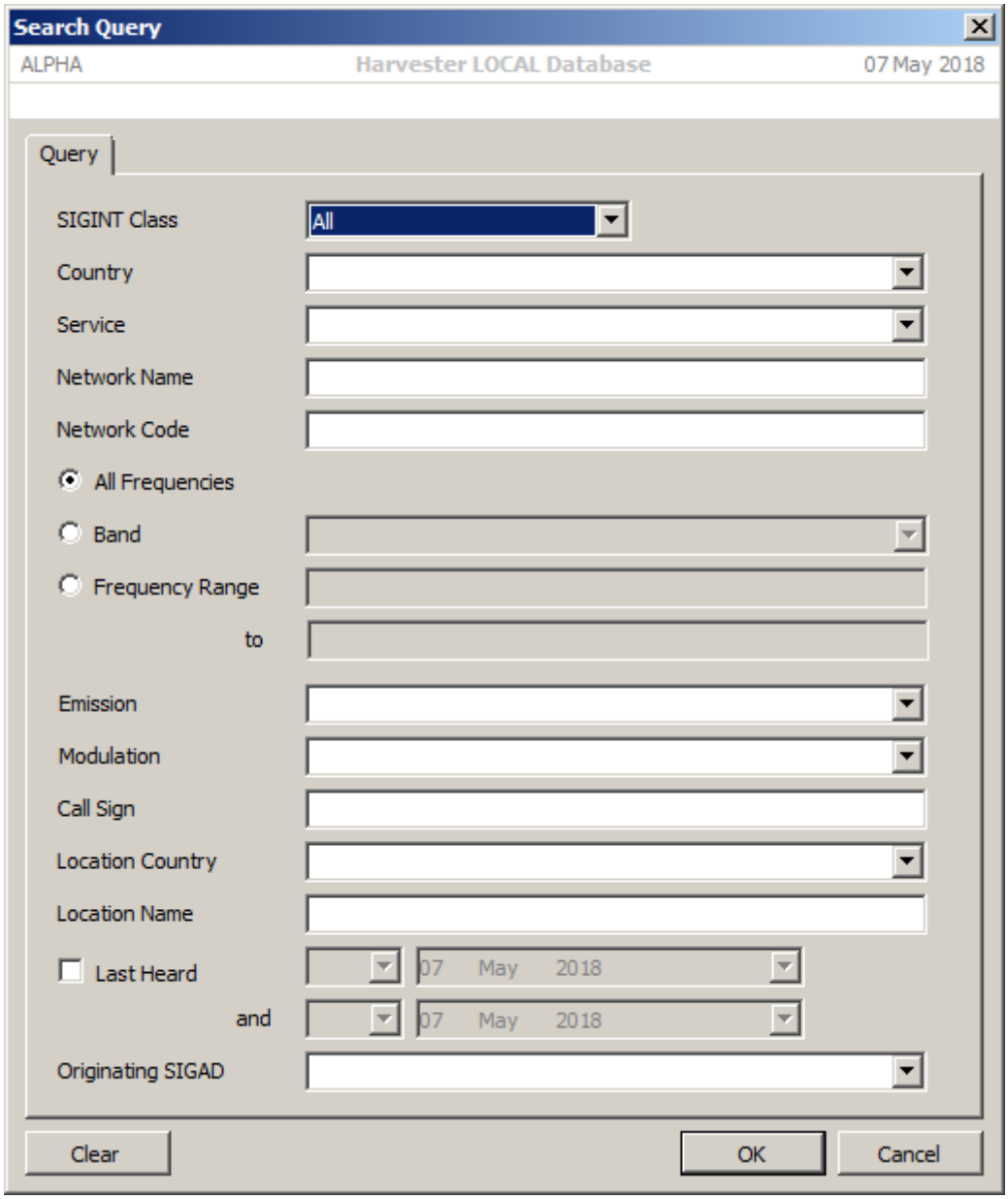
To add a new emission to an existing emitter, select the appropriate emitter from the displayed frequency list then click the **Add** button in the toolbar and from the dropdown menu, select **Add New Emission**. This will open the **Add New Emission** screen, which is similar to the **Add New Emitter** screen but has a number of emitter specific fields disabled. These parameters, such as the SIGINT class and emitter frequency are fixed for all emissions originating from that emitter.

NOTE You can only add an emission to an existing emitter. Emissions cannot be added without a supporting emitter. If you observe multiple emissions on the same frequency, take great care when attaching them to an emitter. The same frequency does not always mean the same emitter or network!



11.2 Search Queries

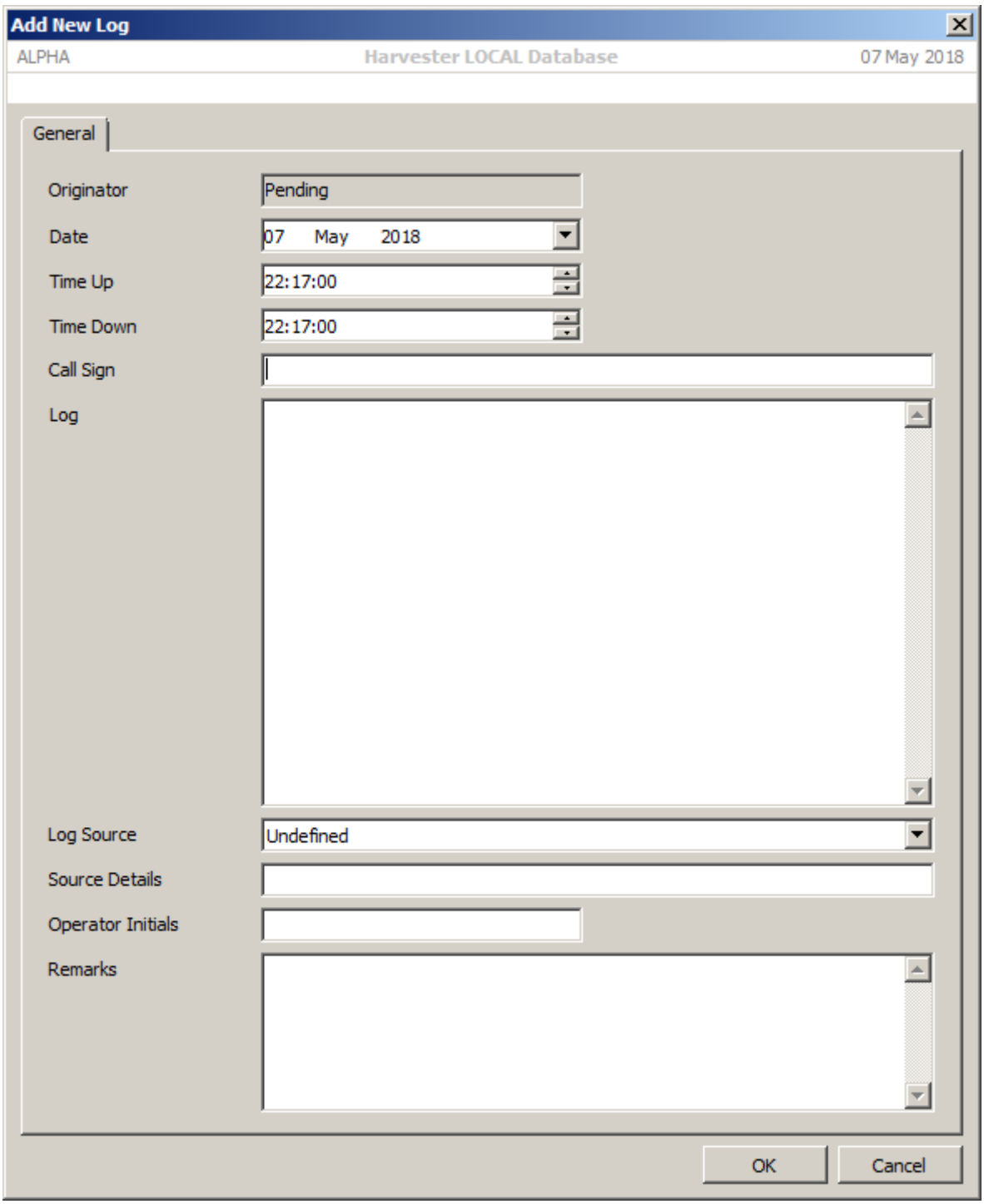
Searching for specific frequencies, frequency bands, emissions, users, countries, servcies and locations can be carried out using the Search Query Editor screen. This screen allows the user to build up complex queries based on a number of parameters and returns the results in the frequency list panel.



11.3 Adding an Intercept Log

Open source intercept logs can be logged against emitters and emissions through the **Add New Log** screen. To open the **Add New Log** screen, select the appropriate emission from the frequency list, ensure that the Intercept Logs tab is selected then click the **Add** button in the toolbar in the **Logs** panel.

Logs comprise of the Intercept date, Intercept Up and Down times, the Callsign on the net control station and the intercept log itself. It is suggeted that logs are added verbatum unless obvious corrections are required, in which case an opearator comment should be added in double brackets.

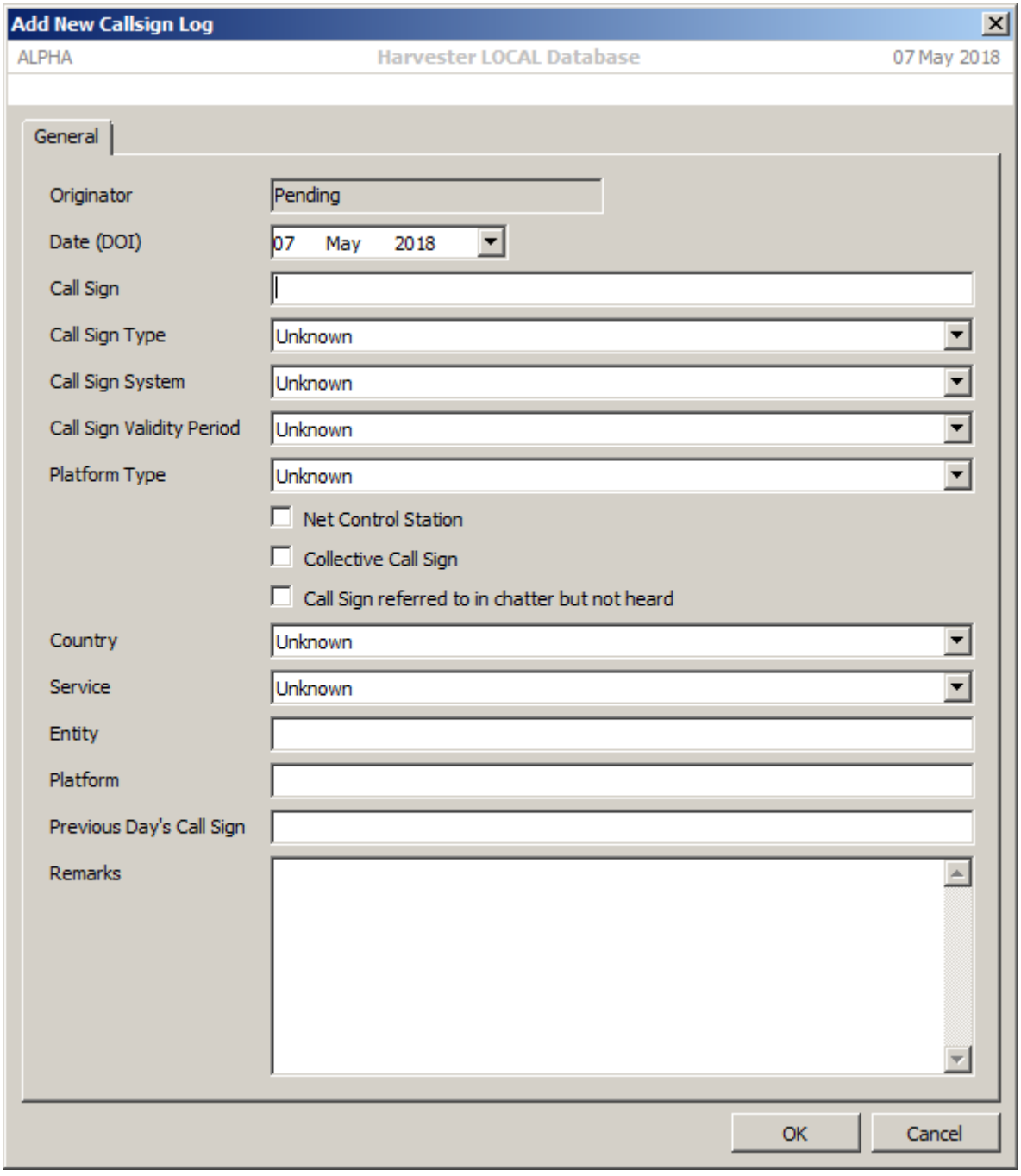


It is also important to annotate the source of the log, such as a monitoring website, an email group such as UDXF (or the older WUN for historical logs) or monitoring magazines such as Monitoring Times. Add as much details as possible, including the URL, if necessary, page numbers, etc. Additional information can be added in the Remarks text.

11.4 Adding a Callsign Log

As well as recording intercept logs, an accurate list of callsigns that operate on a given network is of immense value to analysts. The **Callsign Log** screen provides a facility to record all the callsigns mentioned in each intercept log. To open the **Add Callsign Log**

screen, select the appropriate emission from the frequency list, ensure that the **Call Sign Logs** tab is selected then click the **Add** button in the toolbar in the **Logs** panel.



Enter as much information as possible that can be derived from intercept log as this will not only be usueful for future reference but will also provide a record of which callsigns were operational on a given network on a given day. Take care to ensure than callsigns mentioned in logs actually make sense to be included in the selected network. If you are in doubt, make a note in the Remarks box.

NOTE Although you may have added the net control station callsign to the emitter or emission, it is always worth including that callsign in the callsign logs as a record of when it was operational, and in the case of random or semi-permanent callsigns, when a particular callsign was valid and in use.

12. Importing Log Files

signals intelligence (SIGINT): 1. *A category of intelligence comprising, either individually or in combination, all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted. [JP 1-02]* **2.** *Intelligence derived from communications, electronics, and foreign instrumentation signals. [JP 1-02]*

This functionality is not available in the HARVESTER Lite Version

Harvester now has the functionality to enable the loading of records and logs from external files. The logs are required to be preformatted into a data scheme that the application can both recognise and validate and ultimately import, though this is a fairly simple task for logs that are stored in a database or spreadsheet. To ensure that data integrity is maintained within the Harvester system, logs can only be imported into a single emitter/emission combination at a time. This means that data will require some formatting and filtering before it can be successfully imported. This will ensure that all logs are stored against the correct emission and prevent spurious duplication of emitter records.

Currently, this function can import Intercept Logs, Call Sign Logs and LOB Logs. Each log type requires a different data file format, the details of which are given below.

NOTE *This function is only available when the application is fully registered and can only be used in the Local Database.*

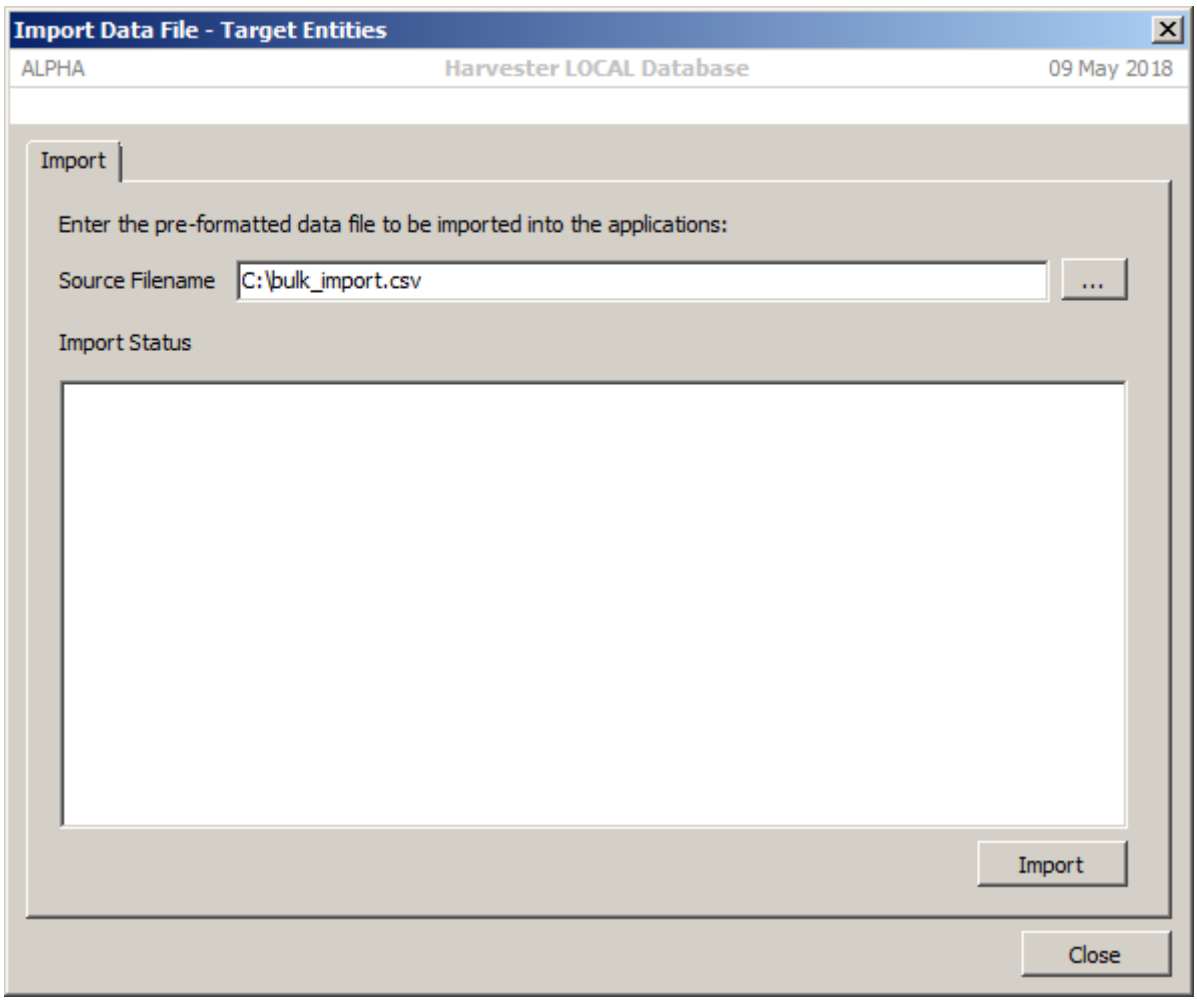
12.1 Importing Logs

Select the emitter and specific emission into which you wish to import the logs in the target frequencies list, then firstly select the emitter and emission you wish to add the logs to. Next, in the Collection panel, select the tab where you wish to add the logs, either Search Logs, Callsign Logs or LOB Logs, then finally click the Import Data File icon on the toolbar to open the **Import Data File** screen.

When the **Import Data File** screen opens, it will already know what type of record file you are trying to load, based on the tab you have selected. Select the source file that contains the appropriately preformatted records, then click the **Import** button to begin the import process. The first step in this process is data validation. This validation is dependant of the Log Type selected. Should the validation process encounter any problems, an error report will be displayed in the Import Status box, itemising the line number of the log and the errors detected. This provides the user with an opportunity to correct any errors before resubmitting the import file for validation and processing.

Once validation has been successfully completed, the process of importing that data begins, the conclusion of which is signalled by an “Import Completed” along with a count of the number of intercept logs imported.

In the case of entering historic records where an emitter and emission record does not already exist, create the emitter record with any available historic parametric information then import the historic intercept, call sign and LOB logs.



12.2 Import File Formats

Import files should be comma-delimited files, typically with the csv file extension. The internal format of each file varies according to the type of logs it contains and will be composed of a combination of string and numeric values. String values should be enclosed in double quotation marks.

12.2.1 Call Sign Logs

Call Sign Log import records consist of seven fields:

Field	Data Type	Remarks
Callsign_Date	Integer	In the format yyyymmdd
Callsign	String	
Callsign_Type	Integer	
Callsign_System	Integer	
Callsign_Country	Integer	
Callsign_Service	Integer	
Platform_Type	Integer	
Remarls	String	

A typical line in a call sign log report would be of the form:

```
20080526,"9MB",3,3,218,14,6,"Net Control Station"
```

NOTE *If you are importing Intercept Logs or LOB Logs that contain Call Sign information, it is useful to import the Call Sign Logs first as this will import far more information about the Call Signs than the Intercept or LOB Log import can manage.*

- **Callsign_Type.** This describes the general type of the call sign.

Index	Description
0	Unknown
1	ITU
2	Voice Call Sign
3	Tactical
4	ACARS Address
5	Aircraft Registration
6	ALE
7	Fixed Service Maritime Selcal
8	Fixed Service Selcal
9	Flight Number
10	ICAO24 Mode-S Address
11	Pager Address

- **Callsign_System.** This describes the general behaviour of the call sign and it's frequency of change.

Index	Description
0	Unknown
1	Fixed
2	Rota
3	Random
4	Semi-Permanent
5	Temporary

- **Callsign_Country** This describes the country with which the call sign is associated.

Index	Description
0	Unknown
1	Afghanistan
2	Albania
3	Algeria
4	American Samoa
5	Andorra
6	Angola
7	Anguilia
8	Antarctica
9	Antigua and Barbuda
10	Argentina
11	Armenia

12	Aruba
13	Australia
14	Austria
15	Azerbaijan
16	Bahamas
17	Bahrain
18	Bangladesh
19	Barbados
20	Belgium
21	Belize
22	Benin
23	Bermuda
24	Bhutan
25	Bolivia
26	Bosnia-Herzegovina
27	Botswana
28	Bouvet Island
29	Brazil
30	British Indian Ocean Territory
31	British Virgin Islands
32	Brunei
33	Bulgaria
34	Burkina Faso
35	Burma
36	Burundi
37	Byelarus
38	Cambodia
39	Cameroon
40	Canada
41	Cape Verde
42	Cayman Islands
43	Central African Republic
44	Chad
45	Chile
46	China (Peoples Republic)
47	Cocos (Keeling) Islands
48	Colombia
49	Comoro Islands
50	Congo
51	Cook Islands
52	Costa Rica
53	Croatia
54	Cuba
55	Cyprus
56	Czech Republic
57	Denmark
58	Djibouti
59	Dominica
60	Dominican Republic
61	Ecuador
62	Egypt
63	El Salvador

64	Equatorial Guinea
65	Eritrea
66	Estonia
67	Ethiopia
68	Falkland/Malvinas Islands
69	Faroe Islands
70	Fiji
71	Finland
72	France
73	French Guiana
74	French Polynesia
75	Gabon
76	Gambia, The
77	Gaza Strip
78	Georgia
79	Germany
80	Ghana
81	Gibraltar
82	Greece
83	Greenland
84	Grenada
85	Guadeloupe
86	Guam
87	Guatemala
88	Guinea-Bissau
89	Guinea-Bisseau
90	Guyana
91	Haiti
92	Heard and McDonald Islands
93	Honduras
94	Hungary
95	Iceland
96	India
97	Indonesia
98	Iran
99	Iraq
100	Iraq-Saudi Arabia Neutral Zone
101	Ireland
102	Israel
103	Italy
104	Ivory Coast
105	Jamaica
106	Japan
107	Johnston Atoll
108	Jordan
109	Juan De Nova Island
110	Kazakhstan
111	Kenya
112	Korea, Democratic Peoples Republic
113	Korea, Republic of
114	Kuwait
115	Kyrgyzstan

116	Laos
117	Latvia
118	Lebanon
119	Lesotho
120	Liberia
121	Libya
122	Liechtenstein
123	Lithuania
124	Luxembourg
125	Macau
126	Macedonia
127	Madagascar
128	Malawi
129	Malaysia
130	Maldives
131	Mali
132	Malta
133	Martinique
134	Mauritania
135	Mauritius
136	Mexico
137	Midway Islands
138	Moldova
139	Monaco
140	Mongolia
141	Montserrat
142	Morocco
143	Mozambique
144	Nambia
145	Nauru
146	Nepal
147	Netherland Antilles
148	Netherlands
149	New Caledonia
150	New Hebrides
151	New Zealand
152	Nicaragua
153	Niger
154	Nigeria
155	Niue
156	Norfolk Island
157	Norway
158	Oman
159	Pakistan
160	Palestine Authority
161	Panama
162	Papua New Guinea
163	Paracel Islands
164	Paraguay
165	Persian Gulf
166	Peru
167	Philippines

168	Pitcairn Islands
169	Poland
170	Portugal
171	Puerto Rico
172	Qatar
173	Reunion
174	Romania
175	Russia
176	Rwanda
177	San Marino
178	Sao Tome and Principe
179	Saudi Arabia
180	Senegal
181	Seychelles
182	Sierra Leone
183	Singapore
184	Slovak Republic
185	Slovenia
186	Solomon Islands
187	Somalia
188	South Africa
189	Spain
190	Sri Lanka
191	St. Helena
192	St. Kitts/Nevis
193	St. Lucia
194	St. Pierre and Miquelon
195	St. Vincent & the Grenadine Islands
196	Sudan
197	Surinam
198	Swaziland
199	Sweden
200	Switzerland
201	Syria
202	Taiwan
203	Tajikistan
204	Tanzania
205	Thailand
206	Togo
207	Tokelau Islands
208	Tonga
209	Trinidad and Tobago
210	Tunisia
211	Turkey
212	Turkmenistan
213	Turks and Caicos Islands
214	Tuvalu
215	Uganda
216	Ukraine
217	United Arab Emirates
218	United Kingdom
219	United States

220	Uruguay
221	Uzbekistan
222	Vanuatu
223	Vatican City
224	Venezuela
225	Vietnam
226	Virgin Islands (U.S.)
227	Wake Island
228	Wallis and Futuna
229	Western Samoa
230	Yemen
231	Serbia
232	Zaire
233	Zambia
234	Zimbabwe
237	German Democratic Republic
238	Soviet Union
239	North Vietnam
240	South Vietnam
241	Czechoslovakia
242	Federal Republic of Germany
243	South Sudan
244	North Sudan
245	Christmas Island

- **Callsign_Service.** This describes the service with which the call sign is associated.

Index	Description
1	Air Force
2	Naval Aviation
3	Commercial
4	Diplomatic
5	Economic
6	Research and Development
7	Strategic Weapons
8	*(Currently Undefined)*
9	Forces Out of Country
10	Military Transport Aviation
11	*(Currently Undefined)*
12	Strategic Aviation
13	Ground Forces
14	Naval Forces
15	*(Currently Undefined)*
16	Police Forces
17	Intelligence
18	Internal Security Forces
19	Merchant Shipping
20	Research
21	*(Currently Undefined)*
22	Civil Aviation
23	*(Currently Undefined)*

24	Unknown
25	*(Currently Undefined)*
26	Air Defence Forces

NOTE *Some Service types are currently undefined and these values should not be used to describe a call sign in the import file.*

- **Platform_Type.** This describes the platform type with which the call sign is associated.

Index	Description
0	Unknown
1	Satellite
2	Aeronautical Mobile
3	Land Fixed
4	Land Mobile
5	Maritime Fixed
6	Maritime Mobile

12.2.2 Intercept Logs

Intercept Log import records consist of nine fields:

Field	Data Type	Remarks
Log Date	Integer	In the format yyyymmdd
TUOI	String	In the format hh:mm:ss
TDOI	String	In the format hh:mm:ss
Callsign	String	
Activity	Integer	
Language	Integer	
Signal Strength	Integer	
Readability	Integer	
Log Text	String	

A typical Intercept Log report would be of the form:

```
20080526,"07:30:00","07:53:00","TAH",31,2,3,3,"Link"
```

- **Activity.** This describes the type of activity being reported.

Index	Description
0	Undefined
1	Nil Heard
2	Net
3	Traffic
4	Idle
5	Test
6	Marker
7	Chatter
8	Broadcast

- **Language.** This describes the language identified in the intercept.

Index	Description
1	Afrikaans
2	Albanian
3	Algerian
4	Amharic
5	Arabic
6	Armenian
7	Azerbaijani
8	Basque
9	Belarussian
10	Bengali
11	Berber
12	Bulgarian
13	Burmese
14	Cambodian
15	Chinese
16	Czech
17	Danish
18	Dari
19	Dutch
20	Egyptian
21	English
22	Estonian
23	Farsi
24	Finnish
25	Flemish
26	French
27	Georgian
28	German
29	Greek
30	Haitian Creole
31	Hebrew
32	Hindi
33	Hungarian
34	Icelandic
35	Ilacano
36	Indonesian
37	Iraqi
38	Italian
39	Japanese
40	Jordanian
41	Kazakh
42	Kirghiz
43	Korean
44	Kurdish
45	Kuwaiti
46	Lao
47	Latvian

48	Levantine
49	Libyan
50	Lingala
51	Lithuanian
52	Macedonian
53	Malaysian
54	Moldovan
55	Mongolian
56	Moroccan
57	Nepali
58	Norwegian
59	Papiamento
60	Pashto
61	Polish
62	Portuguese
63	Punjabi
64	Pushto
65	Quechua
66	Romanian
67	Russian
68	Saudi
69	Serbo-Croatian
70	Sinhalese
71	Slovak
72	Slovene
73	Slovenian
74	Somali
75	Sotho
76	Spanish
77	Sudanese
78	Swahili
79	Swedish
80	Syrian
81	Tajik
82	Tamil
83	Thai
84	Tibetan
85	Tigrinya
86	Turkish
87	Turkmen
88	Tunisian
89	Ukrainian
90	Urdu
91	Uzbek
92	Vietnamese
93	Visayan-Cebuano
94	Xhosa
95	Yemeni
96	Yoruba
97	Zulu
98	Unknown
98	Baluchi

99	Brahui
100	Hausa
101	Mirpuri
102	Potohari
103	Shona
104	Sorani

- **Signal Strength**

Index	Description
0	Undefined
1	Weak
2	Fair
3	Good
4	Strong
5	Very Strong

- **Readability**

Index	Description
0	Undefined
1	Unreadible
2	Poor
3	Fair
4	Good
5	Very Good

12.2.3 LOB Logs

LOB Log import records consist of five fields:

Field	Data Type	Remarks
Date	Integer	In the format yyyymmdd
Time	String	In the format hh:mm:ss
Callsign	String	
Bearing	Numeric	
Remarks	String	

A typical LOB Log report would be of the form:

```
20080809,”13:32:00”,”GBHS”,294.5,”Ship stationary”
```

12.3 Geolocation and Target Entities

New to HARVESTER 6 is the ability to load lists of locations and entities making it much easier for users to build detailed location and entity hierarchies within the system. This cuts out the need to manually create records saving both time and effort. Geolocation and Entity record work slightly differently than collection logs in that they work within a defined hierarchy.Lists can only be added one level at a time to each parent.

12.3.1 Geolocation

Geolocation import records consist of three fields:

Field	Data Type	Remarks
Geolocation Name	String	
Location Type	Integer	
Type Amplifier	Integer	

➢ **Location Type.** This describes the general type of the location.

Index	Description
0	Unknown
1	Administrative Area
2	Population Area
3	Geographical Feature
4	Installation

➢ **Location Type Amplifier.** This amplifies the location type. Note that this is directly related to Type.

Type	Index	Description
1	1	Region
1	2	State
1	3	County
1	4	Province
2	1	City
2	2	Town
2	3	Village
3	1	Hill
3	2	Mountain
3	2	Fixed Location
3	3	Island
3	4	River
3	5	Canal
3	6	Lake
4	1	Airfield, Civilian
4	2	Airfield, Military
4	3	Radar Station, Civilian
4	4	Radar Station, Military
4	5	Harbour, Civilian
4	6	Antenna Site
4	7	Railway Station
4	8	Embassy
4	9	Police Station
4	10	Fire Station
4	11	Hospital
4	12	Power Station, Gas Fired
4	13	Power Station, Coal Fired
4	14	Power Station, Nuclear

4	15	Power Station, Hydro Electric
4	16	Industrial Complex
4	17	Railway Junction
4	18	Railway Yard
4	19	Railway Signal Box
4	20	Barracks
4	21	Office Building
4	22	Supermarket
4	23	Harbour, Military

A typical Geolocation record would be of the form:

```
"London",2,1
```

12.3.2 Target Entities

Target Entity import records consist of three fields:

Field	Data Type	Remarks
Entity Name	String	
Type	Integer	
Type Amplifier	Integer	

- **Type.** This describes the type of activity being reported.

Index	Description
0	Unknown
1	Organisation
2	Echelon
3	Function
4	Platform

- **Type Amplifier.** This describes the type of activity being reported.

Type	Index	Description
1	1	Government
1	2	Military, Army
1	3	Emergency Services
1	4	Military, Navy
1	5	Military, Air Force
1	6	Law Enforcement
1	7	Civil Air Transport
1	8	Intelligence
1	9	Diplomatic
1	10	Telecommunications
1	11	Broadcaster
1	12	Merchant Shipping
2	1	Battalion
2	2	Squadron
4	1	Satellite

4	2	Aeronautical Mobile
4	3	Land Fixed
4	4	Land Mobile
4	5	Maritime Fixed
4	6	Maritime Mobile
5	1	Naval Vessel, Submarine
5	2	Aircraft, Passenger
5	3	Aircraft, Cargo

A typical Target Entity record would be of the form:

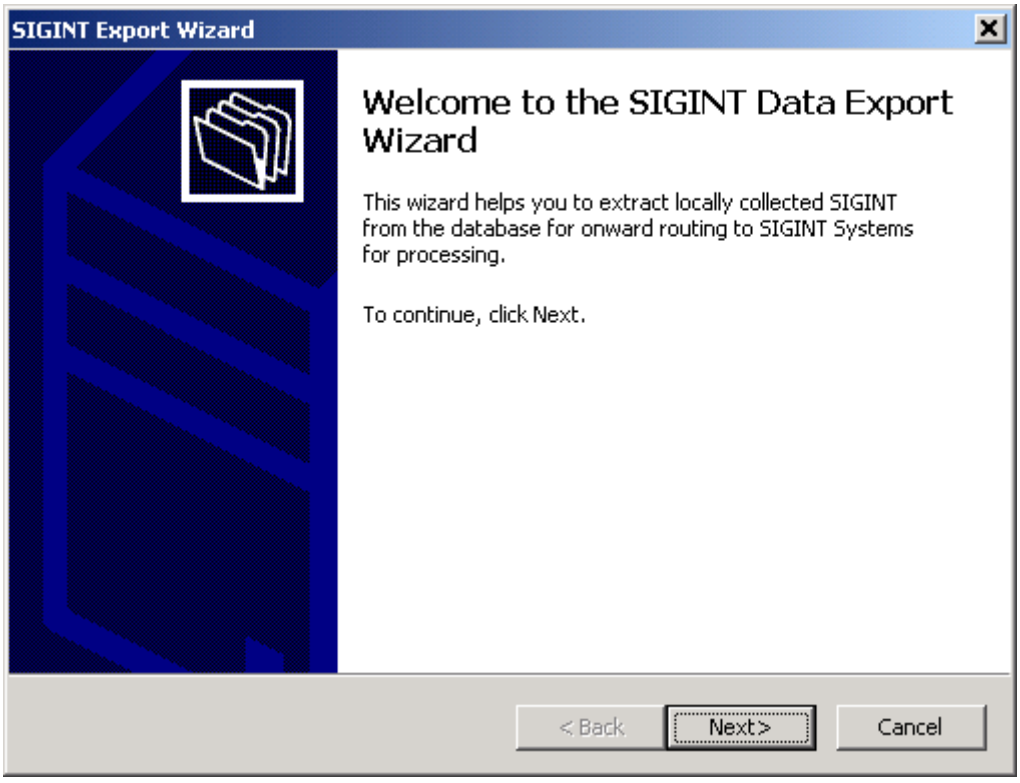
```
“HMS Ark Royal”,4,6
```

13. Data Exports

signals intelligence (SIGINT): 1. *A category of intelligence comprising, either individually or in combination, all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted. [JP 1-02]* **2.** *Intelligence derived from communications, electronics, and foreign instrumentation signals. [JP 1-02]*

One of the new features of HARVESTER is the ability to export, and import, intercepts and supporting associated intelligence. Imports are handled by a separate standalone application called GATEWAY which can be downloaded from the website.

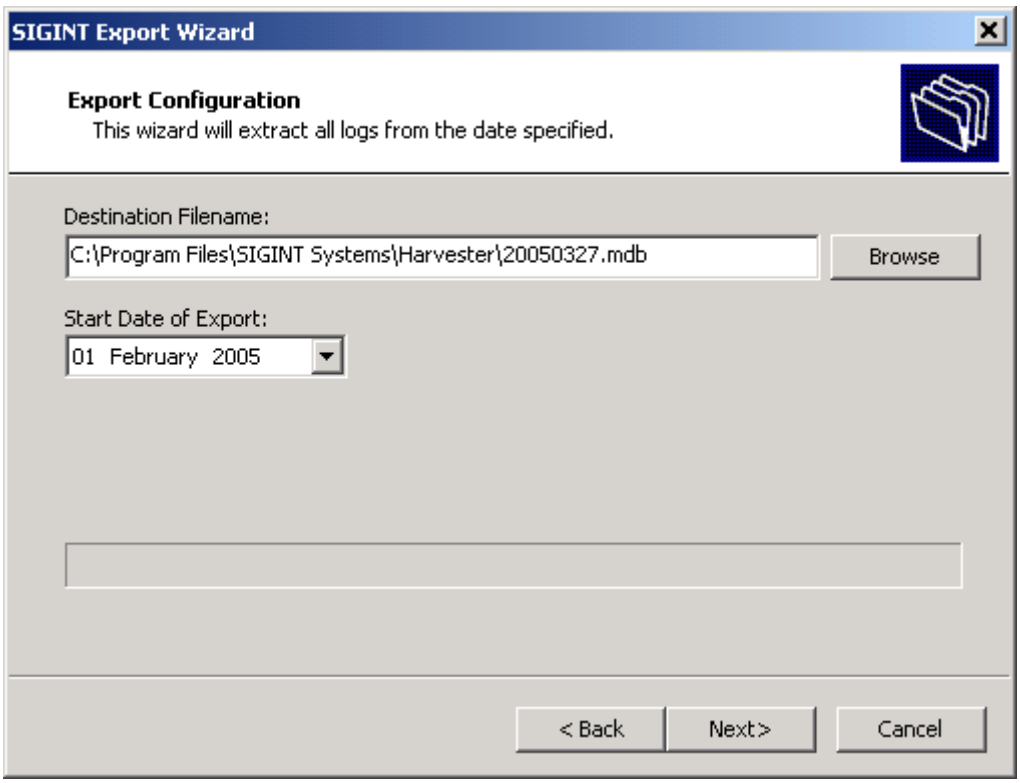
To open the **SIGINT Export Wizard**, select the **SIGINT Updates** option from the **File** menu, and then select **Export**.



Click **Next** to open the next window and continue with the SIGINT data export.

In the next window, two simple selections must be made. First, the **Destination Filename** of the export file and where it is going to be saved. The default location is the **Harvester** installation directory but the export can be saved anywhere on your hard disk, provided there is enough save to store the file. The export filename defaults to the current date in year-month-day format.

Next, select the **Start Date of Export**. This is the earliest date from which data will be extracted. The wizard automatically defaults to the first day of the current month and this is usually adequate to capture all of the most recent intercepts. If you are submitted regular exports, it is a good idea to set this date to the same date at the previous extract was created thus avoiding any gaps in the logs.

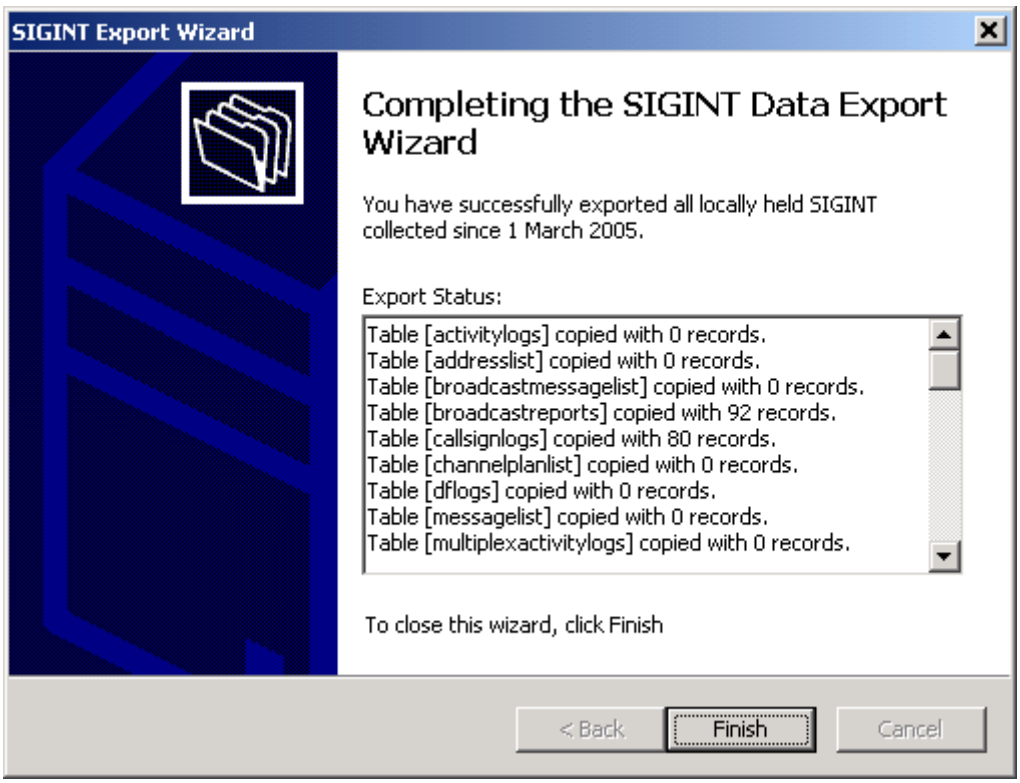


Once you have made these selections, click the **Next** button and the wizard will begin to build the extract. Progress will be displayed by the progress bar as it moves across the screen and by a caption above the progress bar which displays which table is being processed.

When the wizard has completed the extract, the **Completing the SIGINT Data Export Wizard** window will appear. This window contains a status report that lists all the tables that were used to build the extract and the number of records extracted from each table. Click **Finish** to close the wizard.

Depending on the number of logs being extracted and the length of time that the extract covers, the wizard will normally take a minute or so to complete the process. File size also depends on the number of logs being extracted and the length of time that the extract covers but is normally between 2 and 3 MB. To save space and time sending the file by email, the file is automatically compressed. This will reduce the file size considerable, often to less than 20% of the original file.

Once the extract has been zipped, it should be attached to a blank email and sent to **nsoc@sigintsystems.co.uk**. Once we receive the extract, it will be compared and combined with all the other logs received for the same period and processed to create an update file that will be made available to GATEWAY users to import into their local HARVESTER database. Each update will include a wealth of new and updated intelligence that will keep your database up-to-date with the very latest information, and enable your monitoring to benefit from the logs and intercepts of our users.


SIGINT Export Wizard
Completing the SIGINT Data Export Wizard
You have successfully exported all locally held SIGINT collected since 1 March 2005.
Export Status:
Table [activitylogs] copied with 0 records.
Table [addresslist] copied with 0 records.
Table [broadcastmessagelist] copied with 0 records.
Table [broadcastreports] copied with 92 records.
Table [callsignlogs] copied with 80 records.
Table [channelplanlist] copied with 0 records.
Table [dflogs] copied with 0 records.
Table [messagelist] copied with 0 records.
Table [multiplexactivitylogs] copied with 0 records.
To close this wizard, click Finish
< Back
Finish
Cancel

Appendix A. Setting up the MySQL Database

signals intelligence (SIGINT): 1. *A category of intelligence comprising, either individually or in combination, all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted. [JP 1-02]* **2.** *Intelligence derived from communications, electronics, and foreign instrumentation signals. [JP 1-02]*

Before running HARVESTER 6 for the first time, you must setup the HARVESTER database. Depending on the version of the software you are using, this could be on your local machine (Lite or Single Client) or on a remote database server (Standard or Professional). The first step is to install Oracle's MySQL server.

A.1 Install MySQL Server

Download MySQL Community server Version 5.7 from the MySQL website:

https://dev.mysql.com/downloads/mysql/

Install MySQL Server on a PC or server according to the version of HARVESTER you are using. If you are using the HARVESTER Professional, you may consider installing the Enterprise Edition of MySQL Server.

A.2 Install MySQL Workbench

Download and install MySQL Workbench from the MySQL website:

https://dev.mysql.com/downloads/workbench/

There are other free MySQL tools, such as Dell's Toad for MySQL which can also be used if you prefer.

A.3 Run the Database Creation Script

Open MySQL Workbench and connect to the database instance you created in step 1. In the File menu, select Open SQL Script. Navigate to the location:

C:\Program Files\SIGINT Systems\Harvester\resources\setup\database

Select the file *create_db.sql* and click open. This script will create the new HARVESTER database, create all the tables and view. Once the file is open, click the Execute button on the toolbar to begin the progress.

Next, open the file *populate_db.sql* and click the Execute button. This will insert static data values into the database The jobs should take no more than a few minutes to run and once completed, you are now ready to run HARVESTER for the first time.

Now run the Harvester Client!

Appendix B. A Guide to Logging Emitters and Emissions

signals intelligence (SIGINT): 1. *A category of intelligence comprising, either individually or in combination, all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted. [JP 1-02]* **2.** *Intelligence derived from communications, electronics, and foreign instrumentation signals. [JP 1-02]*

A system is only as good as the information that is entered. That may sound like common sense, but it is a fundamental fact that is so often overlooked. HARVESTER is no exception to this rule and you will only get out of the system what you put in to it. The underlying data structures in HARVESTER Version 6 may have been completely redesigned to ensure a higher degree of data integrity but data accuracy is still the responsibility of the user, and the accurate logging of intercepted signals is at the heart of all intelligence gathering by SIGINT.

A prime factor in the design of HARVESTER is the consolidation of intelligence at the point of collection. It is therefore incumbent on the user to do as much as possible to ensure that intercepts are entered with a degree of care and professionalism. The introduction of the Case Notation system and its functionality helps to pull related information together, grouping related frequencies, procedures and information under a single heading. This should be used wherever possible to confirm the exact identities of signals, and to ensure that intercepts are logged against the correct circuits and emitters.

B.1 When you intercept a Signal

There are a variety of well-established steps that operators should carry out when intercepting a signal. These form the essential skills-set that ensure accurate logging of all intercepts. Below are key skills that every HARVESTER user should be aware of, not only to ensure accuracy of data, but also to enhance your abilities to log and identify signals.

B.1.1 Before you even start!

Date and Time

Ensure that your PC is set to the correct date and time and that your time zone is set. Don’t worry about setting your PC to UTC, HARVESTER will do that for you, but setting the correct local time is essential. PC clocks are far from perfect, and do over time, gradually drift off the correct time. Most PCs can now automatically synchronise their clocks from Network Time Protocol (NTP) servers on the web, such as NIST (http://tf.nist.gov) in the US.

Centre Frequency

Determine the centre frequency of your receiver. This is particularly important when receiving OOK or FSK signals and enabled you to accurately establish the correct transmitter frequency. FSK signals can in theory be received using almost any mode. Most will allow the signal to be demodulated, but only when the receiver is switched to the RTTY, do you stand any chance of accurately establishing the exact transmitter frequency and the polarity of the signal.

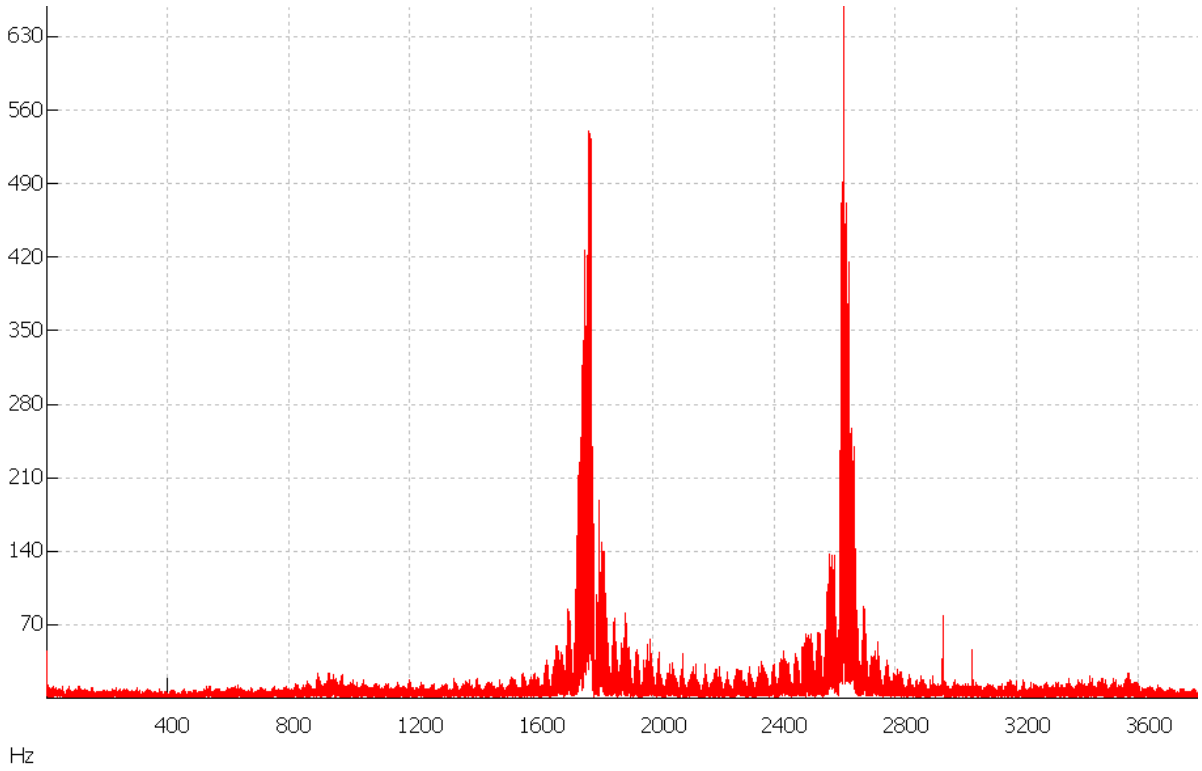
There are various methods of establishing the centre frequency of your receiver, however this method is both quick and accurate, and readily demonstrates exactly how an operator establishes the transmitter frequency of a live signal. For this method, you will require a software demodulator. TrueTTY by DXSoft (http://www.dxsoft.com) is an excellent and free option, however there are many other more specialised applications, such as Hoka's Code300.

After you have installed the software and starting it, connect the audio output of your receiver to the audio input of your PC. The audio trace in the software will instantly display the audio spectrum of the input signal. Switch your receiver to the RTTY mode and set it to one of the following frequencies:

Frequency	Shift	Service
4280.00 kHz	850 Hz	75 Baud Royal Netherlands Navy
4583.00 kHz	450 Hz	50 Baud Deutche Seewetterdienst
4732.00 kHz	850 Hz	75 Baud NATO RATT
7646.00 kHz	450 Hz	50 Baud Deutche Seewetterdienst
10100.80 kHz	450 Hz	50 Baud Deutche Seewetterdienst
11039.00 kHz	450 Hz	50 Baud Deutche Seewetterdienst
14467.30 kHz	450 Hz	50 Baud Deutche Seewetterdienst

These transmitters are all European based but provide 24 hr continuous service, which should be audible in many parts of the world.

What you should now see on screen is something that looks like this:



This is the audio spectrum of 4732.00 kHz, showing an FSK signal with a shift of 850 Hz. Note that the FSK tones are positioned at 1775 and 2625 Hz, exactly half the shift below and half the shift above the centre frequency of 2200 Hz. So the centre frequency for this particular receiver is 2200 Hz. In the RTTY mode,

most receivers have a centre frequency of around 2200 Hz. For most Icom receivers, the centre frequency is 2150 Hz.

Now when you intercept an FSK signal, tune the receiver until the FSK tones exactly straddle the centre frequency, then read off the correct transmitter frequency from the receiver.

B.1.2 Interception

- Ensure that your receiver is switched to the correct receiving mode to receive the modulation of the intercepted emission. This will ensure that you obtain the correct transmitter frequency.

- Determine the exact frequency of the transmission. This can easily be done by ear with SSB signals, and with practice, also with FSK signals, however on the more complex signals, a software spectrum analyser is essential. This is where selecting the correct receiver mode and knowing your centre frequency is essential. Different receiver modes have different centre frequencies, therefore selecting the wrong mode may allow you to demodulate the signal but it will result in an incorrect polarity and transmitter frequency, making identification much more difficult.

- Once the correct transmitter frequency has been established, check the database for likely matches. If there is a likely candidate, check past intercepts and parametrics to ensure that it is the same circuit you are intercepting. There may be two or more almost identical transmissions on the same frequency and none may be related to each other, or to the one you have intercepted. A classic example of this is shown below.

4018.000K3	PSK	MS5 Fire		Russia
4019.000K4	FSK	81-81	41.0000/500.00//1087	Unknown
└	CW	Morse	//18.00/1334	Unknown
4020.000K6	FSK	Soviet 50	50.0000/200.00//2200	Russia
4020.000K6	FSK	Soviet 50	50.0000/500.00//2200	Russia
├	CW	Morse		Russia
└	FSK	Baudot	50.0000/500.00//2200	Russia
4021.000K7	CW	Morse	//30.00/1000	Unknown
4023.000K9	PSK	MS5 Fire		Russia
└	USB	Voice		Russia
4025.000K1	FSK	Soviet 50	50.0000/200.00//1087	Russia
4026.000K2	CW	Morse	//29.00/800	Unknown
4026.000K2	LSB	Voice		Russia

There are two known Soviet50 emitters on 4020 kHz but intercepting a Soviet50 signal on this frequency should not automatically be assumed to be from one of the existing senders. Great care much be taken in identifying an intercept as time spend getting it correct at the point of interception will pay dividends later when logs are being analysed for patterns, schedules and other information of intelligence value. Review historic intercepts, Local Case Files, and if available, TEXTA, to positively confirm that what you are intercepting matches the circuit already logged in the database.

- If you cannot find a match, or have any doubts that the new intercept matches anything currently logged, always err on the side of caution and create a new emitter log. After all, if your new log turns out to be a part of a circuit that has already been logged, the new intercept can always be merged with the establish

log. It’s a lot more difficult trying to extract or split a log from the wrong emitter!

Appendix C. Quick Start Guide

signals intelligence (SIGINT): 1. *A category of intelligence comprising, either individually or in combination, all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted. [JP 1-02]* **2.** *Intelligence derived from communications, electronics, and foreign instrumentation signals. [JP 1-02]*

Installing HARVESTER Version 6 is now a slightly more involved process, as the application also requires the installation of a relational database server. Below is a list of the key steps in the setting up process for both a standalone PC, if all you require is a single HARVESTER client, or the server and numerous HARVESTER clients should you require a complete network.

C.1 Quick Start Installation

1. Download MySQL Community server from the MySQL website:

   https://dev.mysql.com/downloads/mysql/

   If you intend to use only one HARVESTER client, this should be installed on your local PC. However, if you intend to run several clients, this should be installed on a central server or PC that will always be available.

2. Install Harvester Version 6 on all client PCs, and the server if required.

3. Install the MySQL Connector Client on all client PCs. This can also be downloaded from the MySQL website:

   https://dev.mysql.com/downloads/connectors/odbc/

4. In a MySQL tool such as Workbench, open and run the create_db.sql in the \resources\ folder of your Harvester Version 6 installation . This script creates the database and is needs to be run only once on the PC or server on the MySQL server is installed. If you need to move this file onto the server, be sure to copy both create_db.bat and create_db.sql.

   MySQL Workbench can be dowloaded at

   https://dev.mysql.com/downloads/workbench/

5. Run the Harvester Version 6 client. Enter the username, password amd server name in the login screen. (*Note* Lite and Single Client Editions are both set to localhost)

6. Fill in user details on the Setup screen, add intercept locations and positions and begin logging!

END-USER LICENSE AGREEMENT

IMPORTANT—READ CAREFULLY: This End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and SIGINT Systems for the software that accompanies this EULA, which includes computer software and may include associated media, online or electronic documentation, and Internet-based services ("Software"). An amendment or addendum to this EULA may accompany the Software. YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA BY INSTALLING, COPYING, OR OTHERWISE USING THE SOFTWARE. IF YOU DO NOT AGREE, DO NOT INSTALL, COPY, OR USE THE SOFTWARE; YOU MAY RETURN IT TO YOUR PLACE OF PURCHASE (IF APPLICABLE) FOR A FULL REFUND.

SIGINT SYSTEMS SOFTWARE LICENSE

1. GRANTS OF LICENSE. SIGINT Systems grants you the rights described in this EULA provided that you comply with all terms and conditions of this EULA.

1.1 General License Grant. SIGINT Systems grants to you as an individual, a personal, nonexclusive license to use the Software for the purposes of designing, developing, testing, and demonstrating your software product(s), provided that you are the only individual using the Software.

If you are an entity, SIGINT Systems grants to you a personal, nonexclusive license to use the Software, and to make and use copies of the Software, provided that for each individual using the Software within your organization, you have acquired a separate and valid license for each such individual.

1.2 Documentation. You may make and use an unlimited number of copies of any documentation, provided that such copies shall be used only for personal purposes and are not to be republished or distributed (either in hard copy or electronic form) beyond your premises.

1.3 Storage/Network Use. You may also store or install a copy of the Software on a storage device, such as a network server, used only to install or run the Software on computers used by licensed end users in accordance with Section 1.1. A single license for the Software may not be shared or used concurrently by multiple end users.

2. RESERVATION OF RIGHTS AND OWNERSHIP. SIGINT Systems reserves all rights not expressly granted to you in this EULA. The Software is protected by copyright and other intellectual property laws and treaties. SIGINT Systems own the title, copyright, and other intellectual property rights in the Software. The Software is licensed, not sold.

3. LIMITATIONS ON REVERSE ENGINEERING, DECOMPILATION, AND DISASSEMBLY. You may not reverse engineer, decompile, or disassemble the Software, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation.

4. NO RENTAL/COMMERCIAL HOSTING. You may not rent, lease, lend or provide commercial hosting services with the Software.

5. CONSENT TO USE OF DATA. You agree that SIGINT Systems may collect and use technical information and intelligence gathered as part of the product support services provided to you, if any, related to the Software. SIGINT Systems may use this information solely to improve our products or to provide customized services or technologies to you and will not disclose this information in a form that personally identifies you.

6. ADDITIONAL SOFTWARE/SERVICES. This EULA applies to updates, supplements, add-on components, or Internet-based services components, of the Software that SIGINT Systems may provide to you or make available to you after the date you obtain your initial copy of the Software, unless we provide other terms along with the update, supplement, add-on component, or Internet-based services component. SIGINT Systems reserves the right to discontinue any Internet-based services provided to you or made available to you through the use of the Software.

7. UPGRADES/DOWNGRADES

7.1 Upgrades. To use a version of the Software identified as an upgrade, you must first be licensed for the software identified by SIGINT Systems as eligible for the upgrade. After upgrading, you may no longer use the software that formed the basis for your upgrade eligibility.

7.2 Downgrades. Instead of installing and using the Software, you may install and use copies of an earlier version of the Software, provided that you completely remove such earlier version and install the current version of the Software within a reasonable time. Your use of such earlier version shall be governed by this EULA, and your rights to use such earlier version shall terminate when you install the Software.

8. NOT FOR RESALE SOFTWARE. Software identified as "Not For Resale" or "NFR," may not be sold or otherwise transferred for value, or used for any purpose other than demonstration, test or evaluation.

9. SOFTWARE TRANSFER. The initial user of the Software may make a one-time permanent transfer of this EULA and Software to another end user, provided the initial user retains no copies of the Software. This transfer must include all of the Software (including all component parts, the media and printed materials, any upgrades. The transfer may not be an indirect transfer, such as a consignment. Prior to the transfer, the end user receiving the Software must agree to all the EULA terms.

10. TERMINATION. Without prejudice to any other rights, SIGINT Systems may terminate this EULA if you fail to comply with the terms and conditions of this EULA. In such event, you must destroy all copies of the Software and all of its component parts.

11. DISCLAIMER OF WARRANTIES. SIGINT SYSTEMS PROVIDE THE SOFTWARE AND SUPPORT SERVICES (IF ANY) AS IS AND WITH ALL FAULTS, AND HEREBY DISCLAIM ALL OTHER WARRANTIES AND CONDITIONS, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY (IF ANY) IMPLIED WARRANTIES, DUTIES OR CONDITIONS OF MERCHANTABILITY, OF FITNESS FOR A PARTICULAR PURPOSE, OF RELIABILITY OR AVAILABILITY, OF ACCURACY OR COMPLETENESS OF RESPONSES, OF RESULTS, OF WORKMANLIKE EFFORT, OF LACK OF VIRUSES, AND OF LACK OF NEGLIGENCE, ALL WITH REGARD TO THE SOFTWARE, AND THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT OR OTHER SERVICES, INFORMATION, SOFTWARE, AND RELATED CONTENT THROUGH THE SOFTWARE OR OTHERWISE ARISING OUT OF THE USE OF THE SOFTWARE. ALSO, THERE IS NO WARRANTY OR CONDITION OF TITLE, QUIET ENJOYMENT, QUIET POSSESSION, CORRESPONDENCE TO DESCRIPTION OR NON-INFRINGEMENT WITH REGARD TO THE SOFTWARE.
12. EXCLUSION OF INCIDENTAL, CONSEQUENTIAL AND CERTAIN OTHER DAMAGES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL SIGINT SYSTEMS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, PUNITIVE, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS OR CONFIDENTIAL OR OTHER INFORMATION, FOR BUSINESS INTERRUPTION, FOR PERSONAL INJURY, FOR LOSS OF PRIVACY, FOR FAILURE TO MEET ANY DUTY INCLUDING OF GOOD FAITH OR OF REASONABLE CARE, FOR NEGLIGENCE, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SOFTWARE, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT OR OTHER SERVICES, INFORMATION, SOFTWARE, AND RELATED CONTENT THROUGH THE SOFTWARE OR OTHERWISE ARISING OUT OF THE USE OF THE SOFTWARE, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS EULA, EVEN IN THE EVENT OF THE FAULT, TORT (INCLUDING NEGLIGENCE), MISREPRESENTATION, STRICT LIABILITY, BREACH OF CONTRACT OR BREACH OF WARRANTY OF SIGINT SYSTEMS OR ANY SUPPLIER, AND EVEN IF SIGINT SYSTEMS OR ANY SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
13. LIMITATION OF LIABILITY AND REMEDIES. NOTWITHSTANDING ANY DAMAGES THAT YOU MIGHT INCUR FOR ANY REASON WHATSOEVER (INCLUDING, WITHOUT LIMITATION, ALL DAMAGES REFERENCED HEREIN AND ALL DIRECT OR GENERAL DAMAGES IN CONTRACT OR ANYTHING ELSE), THE ENTIRE LIABILITY OF SIGINT SYSTEMS AND ANY OF ITS SUPPLIERS UNDER ANY PROVISION OF THIS EULA AND YOUR EXCLUSIVE REMEDY HEREUNDER (EXCEPT FOR ANY REMEDY OF REPAIR OR REPLACEMENT ELECTED BY SIGINT SYSTEMS WITH RESPECT TO ANY BREACH OF THE LIMITED WARRANTY) SHALL BE LIMITED TO THE GREATER OF THE ACTUAL DAMAGES YOU INCUR IN REASONABLE RELIANCE ON THE SOFTWARE UP TO THE AMOUNT ACTUALLY PAID BY YOU FOR THE SOFTWARE OR US$5.00. THE FOREGOING LIMITATIONS, EXCLUSIONS AND DISCLAIMERS (INCLUDING SECTIONS 11, AND 12) SHALL APPLY TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, EVEN IF ANY REMEDY FAILS ITS ESSENTIAL PURPOSE.

The guarantee - The Software is designed and offered as a general-purpose software, not for any user's particular purpose. You accept that no Software is error free and you are strongly advised to back-up your files regularly. Provided that you have a valid license, SIGINT Systems guarantees that a) for a period of 90 days from the date of receipt of your license to use the Software or the shortest period permitted by applicable law it will perform substantially in accordance with the written materials that accompany the Software; and b) any support services provided by SIGINT Systems shall be substantially as described in applicable written materials provided to you by SIGINT Systems and SIGINT Systems support engineers will use reasonable efforts, care and skill to solve any problem issues. In the event that the Software fails to comply with this guarantee, SIGINT Systems will either (a) repair or replace the Software or (b) return the price you paid. This guarantee is void if failure of the Software results from accident, abuse or misapplication. Any replacement Software will be guaranteed for the remainder of the original guarantee period or 30 days, whichever period is longer. You agree that the above guarantee is your sole guarantee in relation to the Software and any support services.

Exclusion of All Other Terms - To the maximum extent permitted by applicable law and subject to the guarantee above, SIGINT Systems disclaims all warranties, conditions and other terms, either express or implied (whether by statute, common law, collaterally or otherwise) including but not limited to implied warranties of satisfactory quality and fitness for particular purpose with respect to the Software and the written materials that accompany the Software. Any implied warranties that cannot be excluded are limited to 90 days or to the shortest period permitted by applicable law, whichever is greater.

Limitation of Liability - To the maximum extent permitted by applicable law and except as provided in the SIGINT Systems Guarantee, SIGINT Systems and its suppliers shall not be liable for any damages whatsoever (including without limitation, damages for loss of business profits, business interruption, loss of business information or other pecuniary loss) arising out of the use or inability to use the Software, even if SIGINT Systems has been advised of the possibility of such damages. In any case SIGINT Systems' entire liability under any provision of this Agreement shall

be limited to the amount actually paid by you for the Software. These limitations do not apply to any liabilities that cannot be excluded or limited by applicable laws.

Should you have any questions concerning this EULA, or if you desire to contact SIGINT Systems for any reason, please visit SIGINT Systems on the World Wide Web at http://www.sigintsystems.co.uk