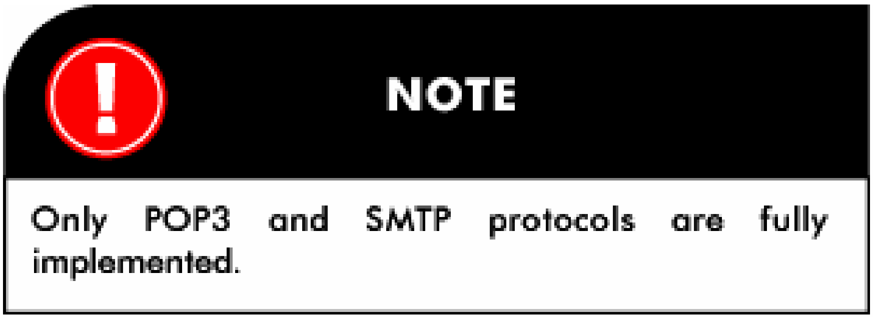
elaman
GERMAN SECURITY SOLUTIONS

EMUN
Email Monitoring System

GOVERNMENTAL SECURITY SOLUTIONS

INTRODUCTION
This document describes the different parts of the Email Monitoring System – what they are used for, how to configure them properly, technical specifications and how to complete different tasks using the Email Monitoring System.

SUBJECT
This document gives a detailed description of the Email Monitoring System.
The Email Monitoring System works for POP3 and SMTP, and can also be
used to monitor html pages.



NOTE

Only POP3 and SMTP protocols are fully implemented.

AUDIENCE
This manual is for all users of the Email Monitoring System.

READER SKILLS
To gain full benefit of this document, it is recommended that the user has knowledge in the following fields:

Entry-level computer skills – including the ability of operating a mouse

Basic knowledge of how to operate Windows NT It is preferable to have knowledge of different internet protocols.

HOW TO SET UP THE EMAIL MONITORING SYSTEM

This section will describe how to set up the Email Monitoring System - Connecting hardware and installing software.

SETTING UP HARDWARE

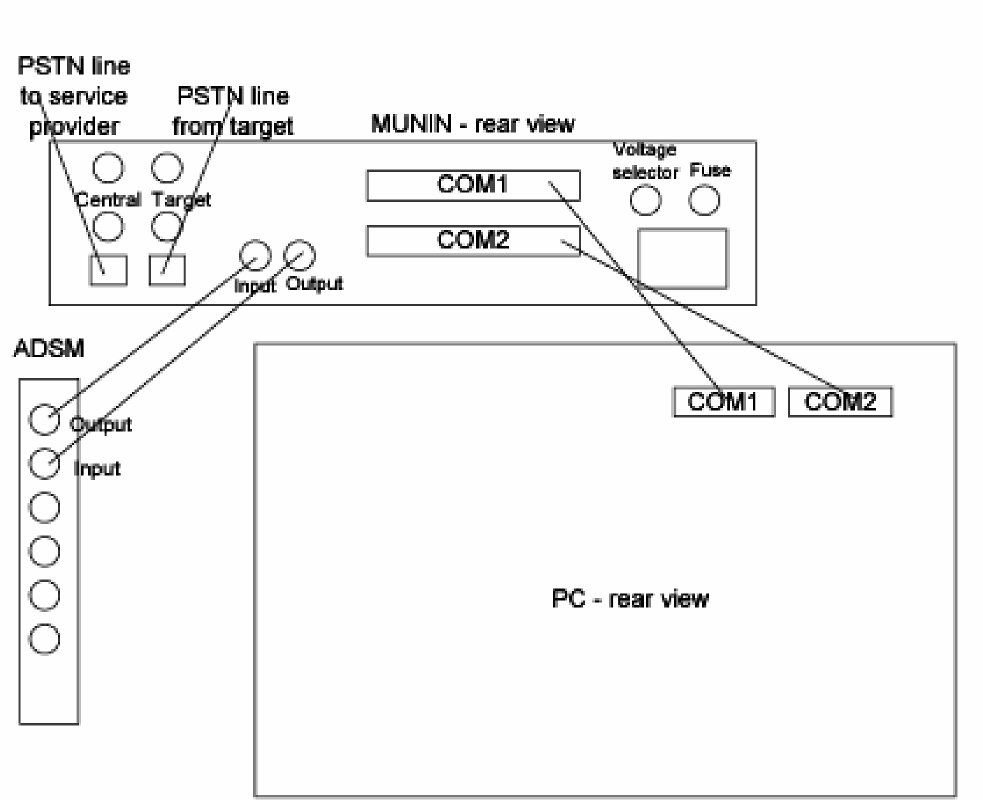


Figure – connecting the Email Monitoring System.

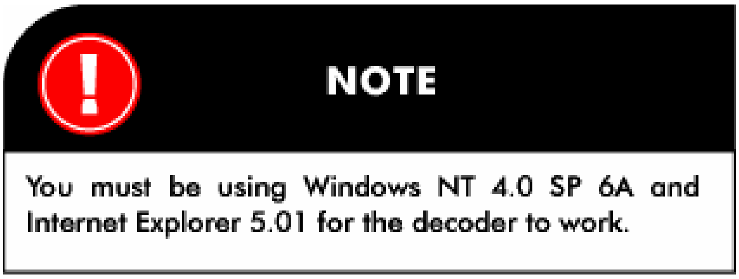
When you are setting up the Email Monitoring System, it is fairly important that it is connected like shown above. It will not harm the system if you connect the COM-ports or Input/Output ports reverse – the system just will not work.

The ADSM card must be installed in a free ISA slot. The card ID must be set to 0 (all dip-switches in off position). For the ADSM card and drivers to work you must also adjust some settings in the BIOS. In the PNP area you must reserve IRQ 10 for the ISA and you must also reserve a memory area (for instance D0000 and 8K ahead).

The phone lines must NOT be simple drop lines from the service provider (SP) but must be the physical line going from the target to the SP’s central otherwise it is impossible to distinguish between forward and reverse channels.

INSTALLING SOFTWARE

In order to install the Email Monitoring System software on your PC you need to run the setup program from included the disk. Please follow the instructions below in order to set it up correctly:



NOTE

You must be using Windows NT 4.0 SP 6A and Internet Explorer 5.01 for the decoder to work.

1. Go to the Start menu and select Run.

2. Select Browse, and find the Setup.exe program on the appropriate drive.

3. Follow the instructions on the screen. Now the Email Monitoring System software will be installed. This includes the Email Monitoring System Intercept Viewer, DAD decoder and ADSM device driver. Please reboot the system on completion for the changes to take effect.

4. Upon reboot, the system is basically ready to use. You should start the DAD decoder before the Email Monitoring System Intercept Viewer.

EMAIL MONITORING SYSTEM HARDWARE CONFIGURATION

WHICH HARDWARE TO USE

An Email Monitoring System consists of following:

1 Email Monitoring System Interface box
1 Email Monitoring System PC
1 PSTN line (from target to PSTN network)
2 serial modem cables
2 5-wire Lemo cables
2 standard power cords – 110/220V

HARDWARE SET UP

For the Email Monitoring System to work correctly, it is fairly important that the hardware is connected correctly. Below is a drawing that shows how to connect the Email Monitoring System correctly.

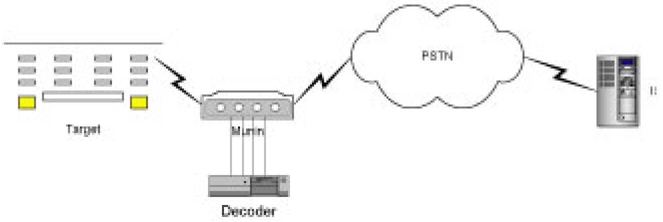


Figure – Typical Email Monitoring Setup

The figure above shows a typical Email Monitoring System set-up. In this scenario, the PSTN line between the target and the PSTN network has been cut and connected through the Email Monitoring System box. From there the signal runs back and forth from the Decoder, which will monitor whether it is modem communication or not.

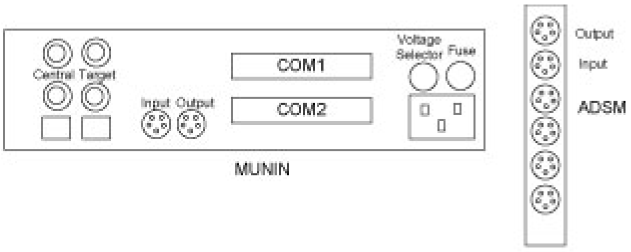


Figure – Connectors in the Email Monitoring System

As shown in the figure above, the Email Monitoring System Interface must be connected to the Email Monitoring System PC with the two serial modem cables and the two 5 wire Lemo cables.

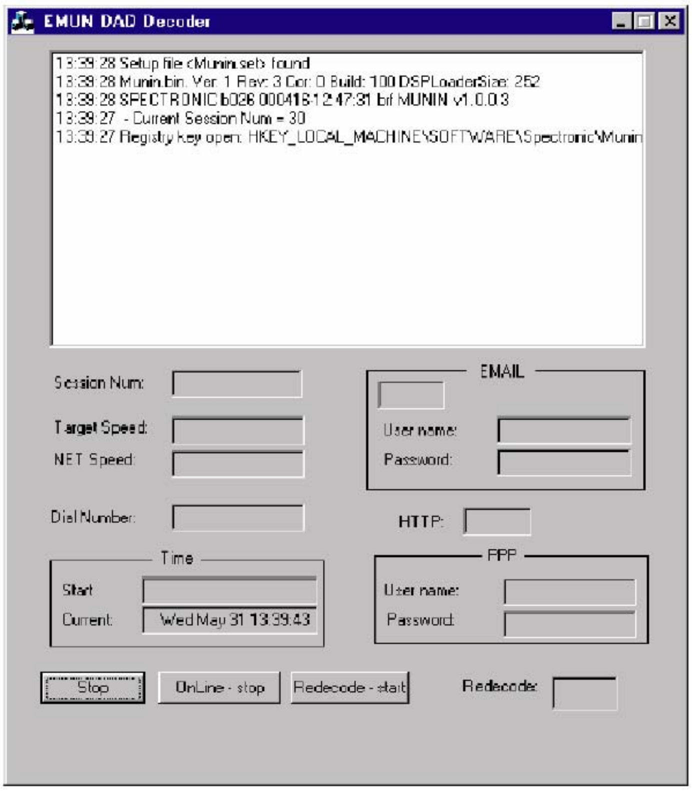
The serial cables must go from COM1 to COM1 and from COM2 to COM2. The Lemo cables must go from Input to Output and Output to Input.

The PSTN line from the target must be plugged into the target hole and the PSTN network line must be plugged in the Central. For the PSTN connection can be used RJ11 modular plug, banana plug or simply two wires.

THE EMAIL MONITORING SYSTEM DAD DECODER

THE EMAIL MONITORING SYSTEM DAD DECODER

The DAD decoder is an advanced protocol decoder created for decoding the PPP communications captured by the Email Monitoring System.



```
13:39:28 Setup file <Munin.set> found
13:39:28 Munin.bin. Ver: 1 Rev: 3 Cor: 0 Build: 100 DSPLoaderSize: 252
13:39:28 SPECTRONIC b026 000416 12:47:31 brf MUNIN v1.0.0.3
13:39:27  - Current Session Num = 30
13:39:27 Registry key open: HKEY_LOCAL_MACHINE\SOFTWARE\Spectronic\Munin
```

Current: Wed May 31 13:39:43

Figure – the DAD decoder

As you can see from the screen dump above, it is not meant to be a program with a lot of features, and besides decoding data, it is also a tool you can use to see statistics for a given session and re-decode already captured
sessions.

Basically, all you can do with it is to see statistics for a current session, start and stop the decoder and re-decode previous sessions (re-decoding and online decoding cannot be running in the same time).

The on-line decoder is running live. However, decoding speed depends on your PC.

COMPLETING TASKS

ON-LINE DECODING

By default, the DAD decoder is on on-line mode when it is started. However, if there is a button that reads OnLine start you can click that one to start the on-line decoder. This requires that the re-decoder is not running (there should be a button saying Redecode start).

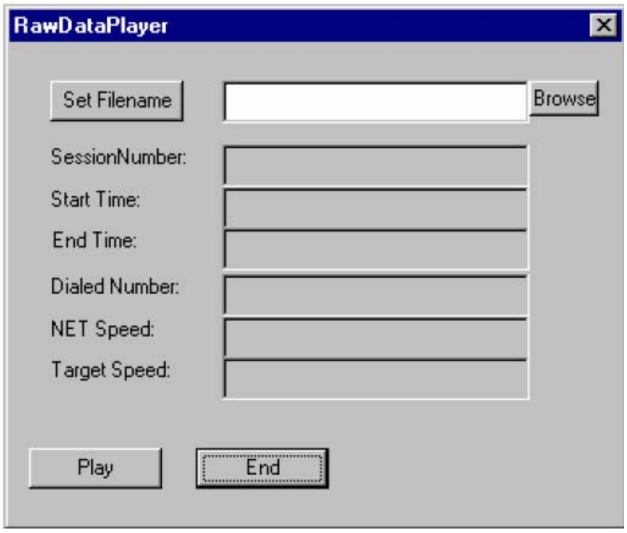
STOPPING ON-LINE DECODING
To stop the on-line decoder, all you need to do is to click the OnLine stop button. This button only appears if the on-line decoder is running.

RE-DECODING A SESSION
To re-decode a session you must first stop the on-line decoder, if it is running.

To start the re-decoder you click the Redecoder Start button. A new window will now pop up.

First you must browse for the file you want to re-decode. Raw-data files are usually located in the Destination\Rawdatalog folder.

When you have found the file, click select filename.



Upon returning to the previous window and seeing the file name there, click the Set Filename button. If it is a correct file, information on the given session will be shown in the appropriate fields.

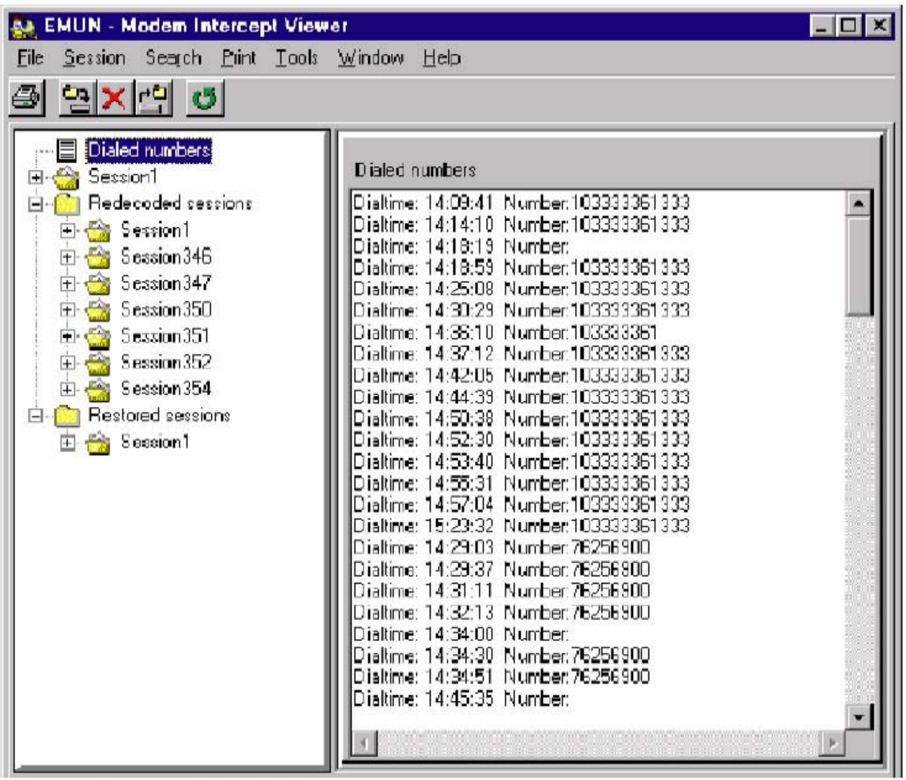
Finally press play to start running the re-decoder. It will work just like when running the on-line decoder, meaning that you can also use the on-line viewer to see the actual result of the decoding.

When the session is done, it will be placed in the Redecoded Sessions folder in the viewer. To return to the main window again, you simply click the End button.

THE EMAIL MONITORING SYSTEM INTERCEPT VIEWER

THE EMAIL MONITORING SYSTEM INTERCEPT VIEWER.

The Email Monitoring System Intercept Viewer is designed with Windows Explorer's navigation mechanisms in mind. This is done to make it easier for the general user to adapt to it. See figure 1 for a picture of the main screen.



Dialed numbers

```
Dialtime: 14:09:41  Number:103333361333
Dialtime: 14:14:10  Number:103333361333
Dialtime: 14:18:19  Number:
Dialtime: 14:18:59  Number:103333361333
Dialtime: 14:25:08  Number:103333361333
Dialtime: 14:30:29  Number:103333361333
Dialtime: 14:36:10  Number:103333361
Dialtime: 14:37:12  Number:103333381333
Dialtime: 14:42:05  Number:103333361333
Dialtime: 14:44:39  Number:103333361333
Dialtime: 14:50:38  Number:103333361333
Dialtime: 14:52:30  Number:103333361333
Dialtime: 14:53:40  Number:103333361333
Dialtime: 14:55:31  Number:103333361333
Dialtime: 14:57:04  Number:103333361333
Dialtime: 15:23:32  Number:103333361333
Dialtime: 14:29:03  Number:76256900
Dialtime: 14:29:37  Number:76256900
Dialtime: 14:31:11  Number:76256900
Dialtime: 14:32:13  Number:76256900
Dialtime: 14:34:00  Number:
Dialtime: 14:34:30  Number:76256900
Dialtime: 14:34:51  Number:76256900
Dialtime: 14:45:35  Number:
```

Figure1: Email Monitoring System main screen

To the left, you have the browser window, which is used to display which items are available for the user to look at. There is a folder for each session intercepted. Under this folder logs, e-mails and web pages are stored – future added protocols would also be added here.

There is also a "Redecoded Sessions" folder and a "Restored sessions" folder. These are used to store re-decoded and restored sessions respectively.

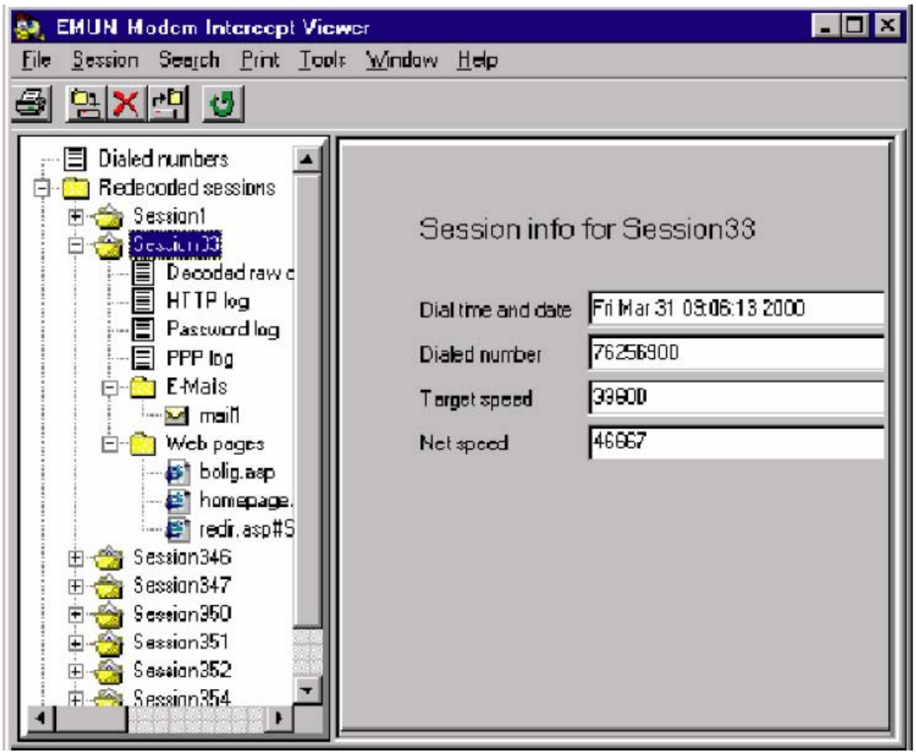
A session is defined by the duration of a remote connection.

To the right, you have the data window. That is where you see the content of the selected item – in this case, a list of dialled numbers.

On the top there is the menu and below that a toolbar, which can be enabled/disabled.

On the bottom, there is a status bar showing where the database is located and status of last command. Here you can also resize the window (Windows standard).

In Figure 2, below, there is an example of a session with data in it. There is a web page, some logs and an email with attachments – the attachments cannot be seen before the e-mail is opened.



Session info for Session33

Dial time and date: Fri Mar 31 09:06:13 2000

Dialed number: 76256900

Target speed: 33600

Net speed: 46667

Figure 2: An example of a Case

Currently a session is selected and its information is shown in the data window. For emails and web pages a source page will also be shown (you have the opportunity to choose between two tab pages).

The Menus
In the Email Monitoring System Intercept Viewer there are different menus, which you can use to control the program’s behaviour. See figure 3 below to get a view of the menus.
In the File menu, all you can do is to shutdown the application.
The Session menu is used to session handling. This includes Backup, Delete,
Restore and Re-decoding. Three of the items are also located on the toolbar described below.

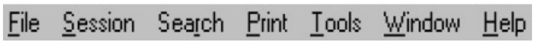


Figure 3: The menus

The toolbar
Just below the menus the toolbar is located. See Figure 4 below to get a view of the toolbar. Anything that you can control from the toolbar, you can also control from the menus.

The first button, from the right, is the print button. It is equal to the Print->Print Current (CTRL+P) menu. It will print the current selected item.

The second button is the backup button. It is equal to the Session->Backup menu. It will make a backup of the current selected session. If no session is selected, it will show an error message.

The third button is the delete button. It is equal to the Session->Delete menu. It will delete the selected session. If no session is selected, it will show an error message.

The fourth button is the restore button. It is equal to the Session->Restore menu. It will ask for a file and afterwards try to decompress and restore that file into the system.

The fifth button is the online viewer button. It is equal to the Tools->Online Viewer menu. It will put the viewer into on-line mode. It will disable some of the menus and the entire tool buttons but itself.

The sixth button is the refresh button. It is equal to the Window->Refresh (F5)
menu. It will reload the system database in order to show new items.

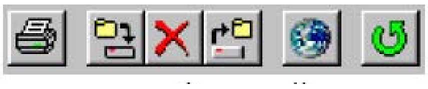


Figure 4: The toolbar

COMPLETING TASKS

SYSTEM SETUP

Set the database path

To set the database path, you need to select the Tools->Settings menu. Here you have the possibility to browse for the database - clicking the button opens a browser.

You only need to use this feature if your database is located in a place different from the default or if you need to use another database.

Set the virtual drive letter

The virtual driver letter is used when you are viewing web pages; this is to ensure that the pages are displayed better. This is, like the database path, set by selecting the Tools->Settings menu. Here you can enter a virtual drive letter: A – Z, where Z is the default drive letter.

In general you should make sure the drive letter you are selecting is not already in use since it may have an undesirable effect on the system.

E-MAIL HANDLING
All events except for "Viewing an e-mail" described in this section assume that you have already selected an e-mail.

Viewing an e-mail

To view an e-mail you must select a session. Within the session there is an Email folder. If there is a + sign next to the E-mail folder it will contain emails, otherwise it will be empty.

When you have opened the E-mail folder, simply click on the e-mail you want to view and it will be opened in the right site pane.

You can also right-click the e-mail and select Open – the e-mail will then be opened with Outlook Express. This is very handy in relation to HTML mails and mails with Chinese text for instance.

Viewing a raw e-mail

To view a raw e-mail you simply click the Raw E-Mail page when you are viewing the e-mail. The raw e-mail is the data that is sent through the mail servers.

Opening an attachment

In order to open an attachment you can do either one of two things.

1. You can double click the attachment or right click and select Open.
2. You can right click the attachment and select Open With

If you select the first option, the viewer will try to open the file with its default association. If no association has been made for the given file type nothing will happen, otherwise the default application will open the file.

If you select the second option, the viewer will ask you which program should be used to open the given file. Browse for the program you want to use to open the file type and click ok.

Saving an attachment

If you want to save an attachment, you can right click the given attachment and select Save. Then you will be asked where you want to save the file. You can also click Save to A-Drive and the file will be saved on the A-drive. When you have selected a folder and a name, click Save and the file will be copied to that location.

WEB-PAGE HANDLING

Viewing a web-page

To view a web page you simply open the session in which the page is located. In here, you open the Web pages folder – now you can click the page you want to see, and it will be displayed in the right site pane.

Viewing the source code for a web-page

To view the source code for a web page you can do either one of following:
1. Right click the web page and select View Source
2. Click on the Source page.

LOG-FILE HANDLING

Viewing a log file

To view a log file, you do it the same way, as with web pages – you do not need to open a subfolder, but only the given session. There is also a Dialled numbers log in the root of the browser window. It contains a list of all the numbers that have been dialled.

SESSION HANDLING

Deleting a session

To delete a session you simply select the given session and press the button ☒ and click yes on the dialog.

Backup a session

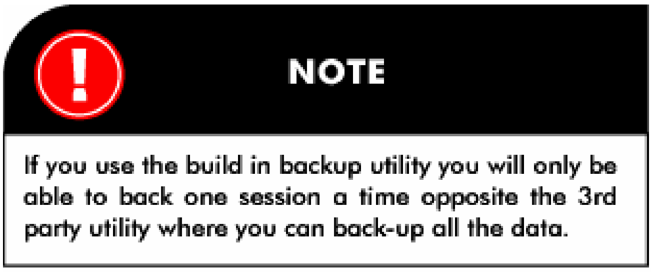
In the Email Monitoring System Intercept Viewer, you have two possibilities to backup and restore a session.

1. The build in backup tool
2. A 3rd party backup tool like MS Backup

If you wish to not use the build in tool, you need to locate the database files.
This can be done from the Tool->Settings menu and then find a folder with the name of the session you want to backup.

If you wish to use the build in tool, you first have to select the session you want to backup. Then you will have to start the backup by clicking the Session->Backup menu or by clicking the button.

The program will ask you where you want to save the session. For example, you can choose to save it on a floppy disk or in a different folder on the hard-drive. When you have selected the correct folder, simply click save and the backup will start.



NOTE

If you use the build in backup utility you will only be able to back one session a time opposite the 3rd party utility where you can back-up all the data.

Restore a session

In order to restore a session you will have to use the same tool as when you made the backup.
If you used the build in tool to make the backup, you must click the button to restore the session again.
You will be asked where the file to restore is located.

When the restore has been completed, the session will be located within Restored Sessions.

SEARCHING FOR INFORMATION

It is possible to search for any kind of information in the database as long as it is text based. When the viewer finds the string you are searching for, it will mark the text and show it in the data window. This cannot be done with actual web pages though – only the source-code of the given page. The following section will describe how to search for information in the Email Monitoring System Intercept Viewer.

The search is activated in one of two ways:

1. Press Ctrl+F , click the 🔍 icon or select the Search->Find menu to start a new search.
2. Press F3 to continue a previous search. If there is none, a new search will be started.

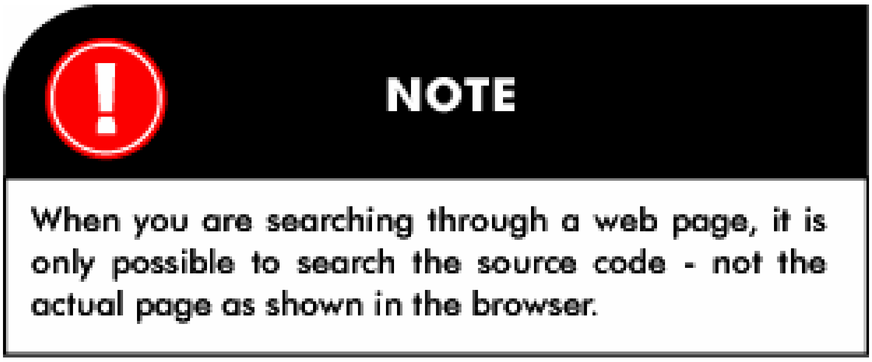
Searching a session

If a session is a selected and you start searching, the entire session will be searched for the text. When the first text is found it is marked and shown in the data window. To continue searching you can either press Find next or you can close the dialog and press F3.

When the end is reached a message will show. If you start the search again by pressing F3 the search will start from the beginning of the session.

Searching e-mail, web and log

Searching through an e-mail, web page or log is no different from searching a session. The only difference is the scope in which the search is performed.



NOTE

When you are searching through a web page, it is only possible to search the source code - not the actual page as shown in the browser.

PRINTER HANDLING

Printing information
To print any intercepted information, you simply select the given item and either click the 🖨 icon or the select the Print-Print Current menu item. If you just 🖨 click icon, the item will be printed directly. If you go through the
menu you will see a print dialog. However, for HTTP a print dialog will show in both cases.

Configuring the printer

To configure the printer, you select the Print->Printer-Setup menu. You now have the possibility to set up the printer as in other programs.

ONLINE VIEWING

To start the online viewer you either click the 🌐 icon or select the Tools- >Online viewer menu. After on-line mode is started, you will see a web page telling that you are in on-line mode. When the session stops, the viewer will automatically go off-line again. When you are in on-line mode the system will automatically show intercepted web sites but not e-mails.

RELOAD THE DATABASE

You can reload the database by clicking the ↻ icon or by selecting the Windows->Refresh menu. Reload is automatically done upon completing an on-line session.

APPENDIX A. TECHNICAL SPECIFICATIONS

EMAIL MONITORING SYSTEM LINE INTERFACE

MODEM INACTIVE

PSTN Line attenuation:	0 dB (relay coupled feed through)
DC load impedance:	> 10 M Ohm
AC load impedance:	> 30 k Ohm

MODEM ACTIVE

PSTN Line:	Split up
Line towards Central:	Terminated by means of an internal modem
Line towards Target:	Loop resistance drive capability: min. 2000 ohm Input impedance: 900 ohm (standard configuration) Network balance: 900 ohm (standard configuration) Loop current: 24 mA (standard configuration)
Line Protection:	VDR in parallel with solid state clamp
Modem protocol V.90/K56Flex:	Compatible
Connect speed:	NET: max. 56000 bps Target: max. 33600 bps

GENERAL

Voice and Fax transmissions:	Direct feed through (not monitored)
Line Voltage LED indicator:	Threshold level 4.7 VDC. Approximately 30 second turn-off delay.
Off Hook LED indicator:	Threshold level 9 mA
Mains power requirements:	
Voltage range:	115/230 VAC (–10%/+5 %)
Power consumption:	15W, maximum 20 W
Fuse:	500 mA Anti-surge (T)
Enclosure:	
Material:	Aluminium
Colour:	Grey with black front/back panel
Dimension HxWxD:	55 x 230.5 x 240 mm

PC REQUIREMENTS

Processor:	Pentium II 400MHz or better
RAM:	128 MB
Free Disk capacity:	2 GB
Slot for ADSM Card:	ISA Slot
Ports for Email Monitoring System Line Interface:	2 COM ports
Software installed	Windows NT 4.0 SP6A Internet Explorer 5

APPENDIX B. ENVIRONMENTAL SPECIFICATIONS

Temperature:	
Operating temperature range:	0 to 40 degrees centigrade
Storage temperature range:	-20 to 70 degrees centigrade
Humidity:	Maximum 90% humidity
Protection:	IP22

APPENDIX C. EXTERNAL INTERFACES

FRONT PANEL

Power Switch:	On / Off
LED Indicators for:	Power Line Voltage Off Hook Modem Active

BACK PANEL

Power input:	
Connector:	IEC Plug
Voltage Selector:	110 / 220 VAC
PC Interface:	
Serial interface:	RS-232
Connector:	D-Sub 25-pole, Standard modem cable
Interface to ADSM Card:	
Output:	
Connector:	5-pole Lemo
Pinning:	
Pin 1: Signal out	
Pin 2, 3, 4: Gnd	
Pin 5:	On-hook: Open Off-hook: Short to Gnd

Input:

Connector: 5-pole Lemo

Pinning:

Pin 4: Control Input

Open = Modem inactive

Short = Modem active

Pin 5: Gnd

PSTN Interface to Central and Target:

Connector: RJ11 in parallel with

Banana Jack 4mm with cross hole

INTERNAL

Module for set-up of the characteristics for the Target Line:

Parameters: Input impedance

Network balance

Max loop current

Connector: 10 pin SIL, 0.1" pitch

ADSM CARD

Input from Email Monitoring System Line Interface:

Connector: 5-pole Lemo

Pinning:

Pin 1: Signal in

Pin 2, 3, 4: Gnd

Pin 5: On-hook: Open

Off-hook: Short to Gnd

Output for Email Monitoring System Line Interface:

Connector: 5-pole Lemo

Pinning:

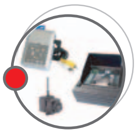
Pin 4: Control output

Open = Modem inactive

Short = Modem active

Pin 5: Gnd.

GOVERNMENTAL SECURITY SOLUTIONS



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

Elaman GmbH
German Security Solutions
Seitzstr. 23
80538 Munich
Germany

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