



iSecurity Capture

User Guide
Version 5.01

www.razlee.com

Contents

Contents	2
About this Manual	5
Chapter 1: Introducing Capture	9
Taking User Activity Tracking Seriously	9
Limitations of IBM i (OS/400) Auditing	10
Limitations of IBM i (OS/400) Screen-Copy	10
The Capture Solution	11
Principal Features	11
How Capture Works	12
Integration with iSecurity	15
Chapter 2: Getting Started	16
Overview	16
Starting Capture for the First Time	17
Configuring Capture	17
Defining General Definitions	19
Defining Capture Retention	21
Setting Highlight Color	23
Auto-Save Definition	24
Defining Business Item Support	25
Email Definitions	27
Activating Capture	29
Local Activation	29
Global Activation	30
Capture All Rule	34
Practical Tutorials for Working with Capture	35
Tutorial 1: Defining Your First Capture Rule	35
Tutorial 2: Viewing Your First Captured Screens	36
Tutorial 3: Start Capture Screen	40
Chapter 3: Capture Rules	41

Overview of Capture Rules	41
Strategic Approach	41
Working with Time Groups	45
Defining Rules for Automatic Capture Sessions	47
Manually Initiating Capture Sessions	49
Starting a Capture Session from Capture	49
Starting a Capture Session from the Command Line	51
Using Action to Trigger a Capture Session	52
Chapter 4: Auditing User Activity	54
Reviewing Captured Screens	54
Selecting Screen Capture Sessions for Audit	55
Navigating Through a Capture Session	58
Using the Capture Menu	60
Free Text Search	61
Printing and Mailing Captured Screens	64
Printing/Mailing Jobs from a Captured Session	64
Chapter 5: Capture Business Items	67
Reporting	69
Display Captured Frames	69
Process Captured Screen	74
Check and Auto Repair Changes	74
Extract Business Items	75
Remove Extractions	75
DSPF Defined in the System	77
Work with DSPF Records	77
Work with Records Displayed Together	80
Business Items Definition	82
Collect DSPF Fields	82
Identify Business Items	84
Prepare Business Items Processing	89
Environments	90

Work with Environments	90
Apply New Environment Names	93
Chapter 6: Maintenance Menu	94
Journal Files	95
Add Journal	95
Remove Journal	96
Display Journal	97
Uninstall	98

About this Manual

This user guide is intended for system administrators and security administrators responsible for the implementation and management of security on IBM i systems. However, any user with basic knowledge of IBM i operations will be able to make full use of this product after reading this book.

Raz-Lee takes customer satisfaction seriously. Our products are designed for ease of use by personnel at all skill levels, especially those with minimal IBM i experience. The documentation package includes a variety of materials to get you familiar with this software quickly and effectively.

This user guide, together with the iSecurity Installation Guide, is the only printed documentation necessary for understanding this product. It is available in HTML form as well as in user-friendly PDF format, which may be displayed or printed using Adobe Acrobat Reader version 6.0 or higher. If you do not have Acrobat Reader, you can download it from the Adobe website: <http://www.adobe.com/>. You can also read and print pages from the manual using any modern web browser.

This manual contains concise explanations of the various product features as well as step-by-step instructions for using and configuring the product.

Raz-Lee's iSecurity is an integrated, state-of-the-art security solution for all System i servers, providing cutting-edge tools for managing all aspects of network access, data, and audit security. Its individual components work together transparently, providing comprehensive "out-of-the-box" security. To learn more about the iSecurity Suite, visit our website at <http://www.razlee.com/>.

Intended Audience

The Capture User Guide document was developed for users, system administrators and security administrators responsible for the implementation and management of security on IBM® AS/400 systems. However, any user with a basic knowledge of System i operations is able to make full use of this document following study of this User Guide.

NOTE: Deviations from IBM® standards are employed in certain circumstances in order to enhance clarity or when standard IBM® terminology conflicts with generally accepted industry conventions.

This document may also serve for new versions' upgrade approval by management.

Native IBM i (OS/400) User Interface

Capture is designed to be a user-friendly product for auditors, managers, security personnel and system administrators. The user interface follows standard IBM i CUA conventions. All product features are available via the menus, so you are never required to memorize arcane commands.

Many features are also accessible via the command line, for the convenience of experienced users.

Conventions Used in the Document

Menu options, field names, and function key names are written in **Courier New Bold**.

Links (internal or external) are emphasized with underline and blue color as follows: "About this Manual" on the previous page.

Commands and system messages of IBM i® (OS/400®), are written in ***Bold Italic***.

Key combinations are in Bold and separated by a dash, for example: **Enter, Shift-Tab**.

Emphasis is written in **Bold**.

A sequence of operations entered via the keyboard is marked as

COMMAND > 81 > 32

meaning: Syslog definitions activated by typing ***COMMAND*** and selecting option: **81** then option: **32**.

Menus

Product menus allow easy access to all features with a minimum of keystrokes. Menu option numbering and terminology is consistent throughout this product and with other Raz-Lee products. To select a menu option, simply type the option number and press **Enter**. The command line is

available from nearly all product menus. If the command line does not appear (and your user profile allows use of the command line), press **F10** to display it.

Data Entry Screens

Data entry screens include many convenient features such as:

- Pop-up selection windows
- Convenient option prompts
- Easy-to-read descriptions and explanatory text for all parameters and options
- Search and filtering with generic text support

The following describes the different data entry screens.

- To enter data in a field, type the desired text and then press Enter or Field Exit
- To move from one field to another without changing the contents press Tab
- To view options for a data field together with an explanation, press F4
- To accept the data displayed on the screen and continue, press Enter

The following function keys may appear on data entry screens.

- **F1: Help** Display context-sensitive help
- **F3: Exit** End the current task and return to the screen or menu from which the task was initiated
- **F4: Prompt** Display a list of valid options for the current field or command. For certain data items, a pop-up selection window appears
- **F6: Add New** Create a new record or data item
- **F8: Print** Print the current report or data item
- **F9: Retrieve** Retrieve the previously-entered command
- **F12: Cancel** Return to the previous screen or menu without updating

Legal Notice

This document is provided by Raz-Lee Security for information purposes only and is not a legal binding document.

While Raz-Lee is doing its best to coordinate between this document and Raz-Lee's products, changes might occur. In case a change has been encountered, please inform Raz-Lee. Raz-Lee keeps its right to modify the software or the document as per its sole discretion Usage of this document, and all information (including product information) provided within, are subject to the following terms and conditions, and all

applicable laws. If you do not agree with these terms, please do not access or use the remainder of this document.

This document contains highly confidential information, which is proprietary to Raz-Lee Security Ltd. and/or its affiliates (hereafter, "Raz-Lee"). No part of this document's contents may be used, copied, disclosed or conveyed to any third party in any manner whatsoever without prior written permission from Raz-Lee. The information included in this document is intended for your knowledge and for negotiation purposes only. Raz-Lee makes no implicit representations or warranties with respect to such information. The information included in this document is subject to change without notice. Any decision to rely on the information contained herein shall be at your sole responsibility, and Raz-Lee will not accept any liability for your decision to use any information or for any damages resulting therefrom. Certain laws do not allow limitations on implied warranties or the exclusion or limitation of certain damages. If these laws apply to you, some or all of the above disclaimers, exclusions, or limitations may not apply to you.

All registered or unregistered trademarks, product names, logos and other service marks mentioned within this document are the property of Raz-Lee or their respective owners. Nothing contained herein shall be construed as conferring by implication, estoppels, or otherwise any license or right, either express or implied, under any patent or trademark of Raz-Lee or any third party. No use of any trademark may be made without the prior written authorization of Raz-Lee. This document and all of its contents are protected intellectual property of Raz-Lee. Any copying, reprinting, reuse, reproduction, adaptation, distribution or translation without the prior written permission of Raz-Lee is prohibited.

Please check your End User License Agreement (EULA) for terms and Conditions.

2020 © Copyright Raz-Lee Security Inc. All rights reserved.

Contacts

Raz-Lee Security Inc. www.razlee.com

Marketing: marketing@razlee.com 1-888-RAZLEE-4 (1-888-7295334)

Support: support@razlee.com 1-888-RAZLEE-2 (1-888-7295332)

Chapter 1: Introducing Capture

Taking User Activity Tracking Seriously

In today's increasingly complex business environment, an effective audit trail is a key component of any organizational IT security program. In certain environments, such as banking and health care, regulations are now in effect that require organizations to maintain detailed transaction activity records and to retain these records for an extended period.

Simply creating a security policy and purchasing some security software tools is not enough. Management should ensure that security policies and procedures are properly implemented and enforced. In addition, managers must be able to evaluate and test the effectiveness of these policies on a continuing basis.

Outside auditing firms, as well as internal audit departments, routinely perform extensive reviews of data systems. Such audit programs typically involve:

- Transaction testing, including accuracy review
- Verification that transactions are initiated and approved only by authorized personnel
- Ensuring prompt detection and correction of errors with appropriate traceability
- Ensuring adequacy of the audit trail
- Implementing and testing the adequacy of IT security policy

Additionally, IT departments and technical support personnel need to monitor user activity in order to troubleshoot error conditions, track performance bottlenecks, and ensure compliance with organizational policies. This often requires detailed knowledge of not only what users are doing, but also, how they are doing it. Computer logs and audit reports, more often than not, do not provide enough forensic evidence for these purposes.

Auditors, managers and even many system administrators are less likely to be familiar with the complex, arcane nature of the IBM i (OS/400) operating

system and its tools in today's IT environment. They need intuitive and user-friendly tools that provide solutions quickly and efficiently.

NOTE: This product works for Interactive jobs (INT).

Limitations of IBM i (OS/400) Auditing

The IBM i operating system, through its journaling facility, creates highly detailed logs of system activities. It is capable of tracking a wide variety of events and retains an extensive volume of data in its journal database. Unfortunately, IBM i provides only minimal, user hostile tools that allow operators to access and manage this data. Analysis and baseline tools are also sorely lacking.

The following is a list of several important limitations of IBM i auditing:

- IBM i journals alone do not provide a visual audit trail of activities that constitute a security breach or are contributing factors to errors. Likewise, the journals do not effectively track data entry errors or routine activities that violate organizational policies.
- The journals provide a primitive, unformatted data display of the journal log with minimal data filtering.
- IBM i lacks a query facility capable of easily extracting data buried in the journal database.
- IBM i provides no audit reports. You must manually export journal data to a file and then use Query, DFU or a third party query tool, such as FileScope, in order to create reports.
- Journal management is a difficult task. Unnecessary data in the security audit journal can adversely affect system performance and waste valuable disk space.

Limitations of IBM i (OS/400) Screen-Copy

As part of the native IBM i operating system which supports and runs the IBM AS/400 (also known as System i or System i) computers, IBM provides functionality for copying screen images of user sessions. This functionality includes capturing on-screen contents and saving the captured images as disk files.

The IBM i operating system includes a function called STRCPYSCN (Start Copy Screen) which enables copying Telnet session screen(s) onto a disk file. This function facilitates inspecting session activity at a later time.

The STRCPYSCN system function operates as follows:

- A monitor decides to start the STRCPYSCN function for a designated user session.
- The user session receives a message which “breaks into” its regular activity announcing that the screen is about to be copied and requesting confirmation from the user.
- When the user confirms this request, all session activity is recorded to a file.

The above described activities transpire without any further intervention to the session being monitored.

The Capture Solution

Capture is a unique solution that complements journals and reports with a visual audit trail of user activity. This powerful data security product shows exactly what users are doing and when they are doing it. Capture helps organizations comply with the strict security regulations that apply to many industries such as banking, insurance, health care, and defense. Capture also provides invaluable traceability capabilities to technical support departments by tracking user activities that result in application or system errors.

Principal Features

- Providing the possibility to display (that is, to replay) captured user session screens and to search contents or patterns in the captured screens. Such searching enables locating screen images in accordance with auditor’s or regulator’s requests.
- A monitor which decides to activate the STRCPYSCN system functionality for designated TELNET sessions. The decisions of this monitor are based on sets of rules which relate, for example, to the time of day, the user of the TELNET session, the IP address of the TELNET session, the device of the TELNET session, and so on.

- Nullifying the system requirement regarding confirmation by users whose screen images are to be recorded. The importance of this feature is in order to actually “capture” possibly illicit behavior without the user being aware that the incriminating session is being recorded.
- Before activating the system function, the user session attributes are modified so that the message will be issued will not “break” into the session but rather will be handled by an automatic feature of this method without the knowledge of the user.
- At the time the STRCPYSCN system function is activated, the message which is sent to the TELNET session as a result of this activation does not “break” into nor interfere with the on-going session activity. Rather the message is responded to automatically.
- A method which generates a warning when the user whose screen images are to be recorded actually initiates the session. It is at this point that Capture enables the possibility of copying screens.
- Managing all accumulated user session information to provide advanced capabilities for managing these saved session files.
- Facilitates retrieval of captured screens with an easy-to-use process and free text search capability.
- If, after inspection, the monitor realizes that the user session screens are not being copied to a disk file, the monitor will once again initiate the STRCPYSCN function.
- Preserves job logs and CL Command logs for subsequent review, changes the job attributes to *LOGCLPGM(*YES)* .
- Uses a simple rule definition process suitable for both IT professionals and non-technical users
- Archives captured screens offline to meet data retention requirements without consuming excessive disk resources

How Capture Works

Capture works silently and invisibly in the background without adversely affecting system performance. User may not even be aware that it is working.

Screen Captures

Screen captures occur only when needed. It is not practical to track all users all the time, especially in a large organization, as this would affect system performance and it would be impossible to review such a large volume of data effectively.

Capture automatically triggers screen capturing according to predefined rules covering a variety of circumstances using variable criteria such as:

- Incoming IP address including subnet mask
- Day and time
- Job (Session or Terminal ID)
- User profile
- Subsystem

You can also manually initiate a screen capture session at any time, for example to track a suspicious user or error condition. Action can also trigger a manual capture session based on its rules.

Backup

Once a day, the previous day's recorded user screen sessions are transferred to a library named SMCPyymmdd. This library contains the log file and the data file for all the sessions which were "captured" during that day; these user screen sessions can be displayed using option **42. Display Restored Log** or printed/displayed using option **46. Display RestoredData**.

Information that is older than the specified retention definition (as defined using option **81. System Configuration** then option **2. Capture Retention**) can be backed up. If a backup program was defined on this screen, the backup program will run automatically before the captured data is deleted.

When the information is copied to a separate backup library, the library's name is updated in the online log; this online log is kept for an unlimited amount of time.

When an auditor or system administrator wishes to access a library, Capture first looks for the requested information in the product library, **SMZCDTA** (**SMZ4DTA** in previous releases). If the information is not found in this library,

Capture will look for it in the backup library pointed to by the entry in the log.

When historical (backed up) information is requested, a message will be sent to the system operator, requesting to load the backup library where the old information is stored.

Options **42. Display Restored Log** and **46. Display Restored Data** may be useful in this situation.

Retrieving Captured Screens

You can retrieve captured screens by means of an intuitive process and easy-to-use tools for locating the captured data screens and logs. Screens are arranged according to individual capture 'sessions'. Within each session, you can scroll through the screens sequentially or you can use the moveable **Capture Menu** to move directly to a particular screen or search for screens containing a specific text string.

The **Capture Menu** also provides commands for displaying the job log and the Audit log entries related to that particular screen and capture session. You can even access the *DSPJOB* command and print the screen directly from the **Capture Menu**.



Integration with iSecurity

Capture is an integral part of the iSecurity suite and, as such, is designed to work together with other components in order to provide a comprehensive security auditing solution.

Effective security auditing requires several tools to provide a high level of traceability. The **Audit** tools add powerful query and reporting functionality to the IBM i operating system. These logs and reports, together with the visual audit trail provided by **Capture** together provide complete documentation of what is going on in your System i environment.

The visual audit trail also compliments the active security components, Firewall and Screen by showing specifically what a user did to trigger a given event. For example, if a particular user program repeatedly executes SQL commands that are rejected by Firewall, the captured screens can show when and how the user ran that program. This, in turn, helps to determine if indeed a security problem exists or perhaps that the Firewall rule needs to be modified.

Most importantly, Action rules can automatically trigger a capture session whenever a suspicious event occurs. This means that, even if a session is not being recorded, an event such as an attempt to access confidential data or an unusual error condition will turn on the Capture camera without the user's knowledge.

NOTE: While Capture is active, transfer to a secondary job (System Request 1) is not available.

You cannot start a copy to a job that has an active secondary job.

Chapter 2: Getting Started

Overview

This chapter guides you through the steps necessary to begin using Capture for the first time. Also covered in this chapter are the basic procedures for configuring the product for day-to-day use.

The following is an overview of the initial Capture process.

- Starting Capture for the First Time
- Configuring Capture
- Defining General Definitions
- Defining Capture Retention
- Using Capture for the First Time
- Practical Tutorials for Working with Capture

Starting Capture for the First Time

In order to use this product, the user must have ***SECOFR** special authority. An additional product password may also be required to access certain functions. The default password is **QSECOFR**. We recommend that you change this password as soon as possible, using the procedure described below.

1. To start Capture, type the **STRCPT** command at any command line. The main menu appears.

```
AUCMENU                                Capture                                iSecurity
                                       System:  S520

Select one of the following:

Capture
  1. Capture Rules
  3. Start Capture Screen
  4. End Capture Screen
  6. Start Capture User

Control
  11. Activation

Definitions
  21. Time Groups

Selection or command
===> █

Capture Screen Activity
  41. Display Current Log
  42. Display Restored Log
  45. Display Current Data
  46. Display Restored Data

Business Items Identification
  61. Business Items Menu

Maintenance
  81. System Configuration
  82. Maintenance Menu
  89. Base Support

F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel
F13=Information Assistant  F16=AS/400 main menu
```

2. Continue to the following procedures.

Configuring Capture

Capture is ready-to-run right out of the box. You should, however, review the default configuration parameters that control important features before using the product for the first time.

There is no “typical” or “optimal” configuration for a security product such as Capture. Each installation or application has different operational criteria

and security needs. The auditing requirements for a large manufacturing environment are quite different from those for a bank, a software developer or a service organization.

To work with product configuration, select **81. System Configuration** from the main menu.

The **System Configuration** menu appears.

```
CAPARMR                iSecurity/Capture System Configuration    27/04/14 14:24:43

Select one of the following:

Capture
 1. General Definitions
 2. Capture Retention
 3. Set Highlight Color

 7. Business Items Support

13. E-Mail Definitions

                                General
Selection ==> █                91. Language Support
                                99. Copyright Notice

Release ID . . . . . 03.24 13-10-14    440E466 520 7459
Authorization code . . . . . C01404762713          1 S520

F3=Exit    F22=Enter Authorization Code
```

NOTE: After you modify any of the parameters accessible from this menu, the message **“Modify data, or press Enter”** appears upon return to the menu.

You must press **Enter** again in order to save your changes and leave this menu. If you press **F3**, you will lose any changes that you have made.

Defining General Definitions

You can choose to warn users that Capture is monitoring user activity on their workstation by selecting the **Display Warning Message** option. Warning messages appear each time a user signs on for a session. You can define the time to wait at sign on, so as to enable Capture to start before interactive jobs start and also how often to check Capture rules.

1. Select **1. General Definitions** from the **System Configuration** menu. The **Capture General Definitions** screen appears.

```
Capture General Definitions                2/04/14 13:36:37

Type options, press Enter.

Display warning message . . . . . 1      0=No message
                                         1=Yes:"Session might be recorded"
                                         2=Yes:"Session will be recorded"

Capture can be configured to warn users that their session activity
may be recorded. The message is displayed at signon, for several seconds.
To modify these messages, compile *DSPF SMZC/CASOURCE AUCSGNFM into SMZCDTA.

Maximum seconds to wait at sign on.  15  0=*NOWAIT
A batch job has to start to enable capture. This parameter ensures that all
interactive screens will be captured, including the first ones.

Minutes between checks . . . . . 998  999=Check once only
                                         998=Never check

This parameter controls a periodic check of Capture rules. In any case, the
rules are checked for each job when it starts.

F3=Exit  F12=Cancel
```

The body of the screen contains these fields:

Display warning message

Capture can be configured to warn users that their session activity may be recorded. The message is displayed at signon, for several seconds. To modify these messages, compile ***DSPF SMZC/CASOURCE AUCSGNFM** into SMZCDTA. Possible Values include:

- **0**: No message
- **1** =Yes: "Session might be recorded"
- **2** =Yes: "Session will be recorded"

Maximum seconds to wait at sign on

The number of seconds that the batch that starts capture has to wait when starting. This parameter ensures that all interactive screens will be captured, including the first ones. Enter a value from **1-999**, or **0** for ***NOWAIT**.

Minutes between checks

All rules are checked when they start. This parameter controls how frequently, in minutes, they are checked afterward. Possible values are:

- The time in minutes
- **999**: Check once only
- **998**: Never check

2. Enter your required parameters and press **Enter** to continue.

Defining Capture Retention

You can define the length of time that captured screens are retained on-line and also specify a backup routine to store archived captures off-line automatically after the designated retention period has expired. In order to ensure compliance with data retention requirements in certain industries, it is highly recommended that you store archived captures on external media, such as tape or optical media.

Captured Data Retention Period

1. Select **2. Capture Retention** from the **System Configuration** menu. The **Capture Retention** screen appears.

```

Capture Retention

Type options, press Enter.

Capture retention period (days) . 0          Days, 99=*NOMAX
Backup program for Captured data. *NONE      Name, *STD, *NONE
Backup program library . . . .

You may specify a backup program to run automatically before deleting
captured data. This program runs prior to automatic deletion of data
whenever the retention period expires.

The *STD program is SMZC/CASOURCE AUCPTBKP.

F3=Exit  F12=Cancel

```

The screen contains the following fields:

Capture retention period (days)

The number of days that captured information is retained. Set it to **0** for ***NOMAX**.

Backup program for Captured data

The program that backs up the captured data. Possible values are:

- A program that your organization provides
- ***STD**: The default backup program provided with Capture, SMZC/CASOURCE AUCPTBKP
- ***NONE**

Backup program library

The name of the library that contains the backup program.

2. Enter your required parameters and press **Enter** to continue.

Setting Highlight Color

You can specify a specific color to highlight key words specified in a free-text search of captured screens. All instances of the key words will appear in this color on the captured screen.

1. Select **3. Set Highlight Color** from the **System Configuration** menu. The **Capture Retention** screen appears.



2. Select the desired color and press **Enter** to continue.

Auto-Save Definition

You can define a period of time in days after which all Capture files will automatically be saved.

Defining Business Item Support

You can define the Business Item Support parameters, such as if Business Items Support is enabled, for how long to retain Business Items, automatic backups of Business Items, and so on.

1. Select **7. Business Items Support** from the **System Configuration** menu. The **Business Items Support** screen appears.

```
Business Items Support                27/04/14 14:37:50

Type options, press Enter.

Enable Business Items support . .  Y                Y=Yes, N=No
Include last user program & stmt.  N                Y=Yes, N=No
Analyze run environment by *LIBL.  Y                Y=Yes, U=User-pgm, N=No
If Y, temporary env. names are given automatically per *LIBL. These can be
renamed later. If U user program is called. See SMZC/CASOURCE CAENVR.

Business Items retention period .  30                Days, 9999=*NOMAX
Backup program for BizItems data.  *NONE                Name, *STD, *NONE
Backup program library . . . .    _____

You can specify a backup program to run automatically before deleting
captured data. This program runs prior to automatic deletion of data
whenever the retention period expires.

The *STD program is SMZC/CASOURCE CPTBZBKP.

F3=Exit  F12=Cancel
```

The body of the screen contains these fields:

Enable Business Items support

- **Y:** Yes
- **N:** No

Include last user program & stmt

- **Y:** Yes
- **N:** No

Analyze run environment by *LIBL

- **Y**: Yes. Temporary environment names are allocated automatically for the *LIBL and can be renamed later. See [Environments](#) for more information.
- **U**: User-written program, such as **SMZC/CASOURCE** **CPTBZBKP**.
- **N**: No

Bizitems retention period (days)

The number of days that captured information is retained. Set it to **9999** for ***NOMAX**.

Backup program for Bizitems data

The program that backs up the Bizitems data. Possible values are:

- A program that your organization provides
- ***STD**: The default backup program provided with Capture, **SMZC/CASOURCE AUCPTBKP**
- ***NONE**

Backup program library

The name of the library that contains the backup program.

2. Enter your required parameters and press **Enter** to continue.

To work with Business Items, see "Chapter 5: Capture Business Items" on page 67.

Email Definitions

Before Capture can send e-mail messages, your System i must be properly configured to send e-mail and at least one e-mail user must be defined in the Directory Entries table (*WRKDIRE*). This procedure can be quite complex and is beyond the scope of this manual.

Refer to the appropriate IBM documentation for more details on these procedures.

To configure Capture to send e-mail messages, perform the following steps:

1. Select **13** from the **iSecurity/Base System Configuration** menu. The **E-MailDefinitions** screen appears.

```

                                     E-mail Definitions                26/01/14 15:00:29

Type options, press Enter.

E-mail Method . . . . . 1          1=Advanced, 2=Native, 3=Secured, 9=None
Advanced or Secured mode is recommended for simplicity and performance.

Advanced/Secured E-mail Support
Mail (SMTP) server name . . *LOCALHOST
                               _____
                               Mail server, *LOCALHOST
Use the Mail Server as defined for outgoing mail in MS Outlook.
Reply to mail address . . . DONOT@REPLY.COM
                               _____
If Secured, E-mail user . . _____
Password . . . . . _____

Native E-mail
E-mail User ID and Address. _____ User Profile. _____
Users must be defined as E-mail users prior to using this screen.
The required parameters may be found by using the WRKDIRE command.
This option does not support attached files.

F3=Exit  F12=Cancel
```

Email Method

How Capture sends email. Possible values include:

- **1**: Advanced
- **2**: Native
- **3**: Secured
- **9**: None

For simplicity and performance, we recommend **1** or **3**.

If set to **2**, users must be defined as Email users before using this screen. You can find the required parameters for this by using the *WRKDIRE* command. The option does not support attached files.

Mail (SMTP) server name

The name of the SMTP server, or ***LOCALHOST**.

Reply to mail address

The email address to receive replies.

If secured, Email user and password

If you chose **Email Method 1** or **3**, enter the email user that will be used to send the emails, and the password of that user.

Email user ID and address

If you chose **Email Method 2**, enter the user ID and address that will be used to send the emails.

User Profile

If you chose **Email Method 2**, the user profile that will be used to send the emails.

2. Enter the required parameters and press **Enter** .

Activating Capture

You must activate the Capture monitor in order to enable the automatic capture features. It is strongly recommended that you configure Capture to activate automatically each time an IPL occurs on your IBM i.

To work with activation, select **11. Activation** from the main menu. You should perform each of the following activities prior to using Capture for the first time.

```
AUCCTL                               Activation                               Capture
                                     System:  S520

Select one of the following:

Activation
  1. Activate Capture Now
  2. De-activate Capture Now

  5. Work With Active Monitor Jobs

Global Activation
  11. Enable Capture
  12. Disable Capture
  13. Activate at IPL
  14. Do Not Activate at IPL

  19. Add Capture All rule (if no rule)

Selection or command
===> █

-----
F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel
F13=Information Assistant  F16=AS/400 main menu
```

Local Activation

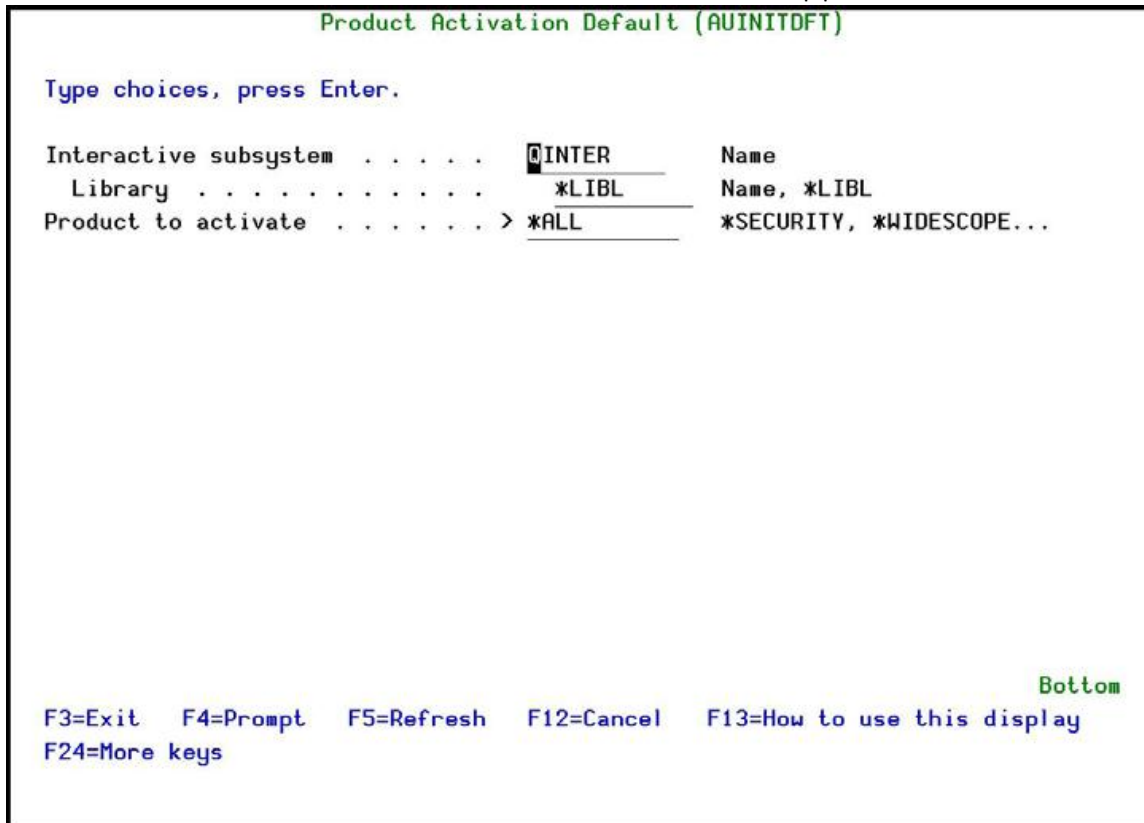
- To activate the Capture monitor, select **1. Activate Capture Now** from the **Activation** menu.
- To de-activate the Capture monitor, select **2. De-activate Capture Now** from the **Activation** menu.

Global Activation

Manual Activation

To enable Capture :

1. Select **11. Enable Capture** from the **Activation** menu. The **Product Activation Default** screen appears.



The body of the screen contains these fields:

Interactive subsystem

The name of the subsystem for which you want to enable Capture . The default value is **QINTER**.

Library

The name of the library of the subsystem for which you want to enable Capture. The default value is **LIBL**.

Product to activate

The products for which you are activating Capture. Possible values include:

- ***SECURITY:** Enable Capture for all Raz-Lee security products.
- ***WIDESCOPe:** Enable Capture for all Raz-Lee security products.
- ***ALL:** Enable Capture for the entire subsystem.
- ***NONE:** This parameter should only be *NONE when you are disabling Capture .

2. Enter the required parameters and press **Enter** . Capture is enabled.

To disable Capture :

1. Select **12. Disable Capture** from the **Activation** menu. The **Product Activation Default** screen appears, as shown for Activating Capture.
2. Set the **Product to Activate** field to ***NONE**.
3. Press **Enter**. Capture is disabled.

Automatic Activation

- To activate Capture automatically each time an IPL occurs, select **13. Activate at IPL** from the **Activation** menu.
- To cancel automatic activation, select **14. Do Not Activate at IPL** from the **Activation** menu.

Verifying that the Capture Monitor is Active

Select **5. Work With Active Monitor Jobs** from the **Activation** menu to view the Capture monitor subsystem. The **Work with Subsystem Jobs** screen appears. It should display several lines similar to those on the screenshot below.

```
Work with Subsystem Jobs S720
Subsystem . . . . . : ZCAPTURE
Type options, press Enter.
  2=Change  3=Hold  4=End  5=Work with  6=Release  7=Display message
  8=Work with spooled files  13=Disconnect

Opt Job User Type -----Status----- Function
| AUCAP#MON SECURITY2P AUTO ACTIVE DLY-60
| AUCAP#SR1 SECURITY2P AUTO ACTIVE PGM-AUCRUNR
| AUCAP#SR2 SECURITY2P AUTO ACTIVE PGM-AUCRUNR
| AUCAP#SR3 SECURITY2P AUTO ACTIVE PGM-AUCRUNR
| AUCAP#SR4 SECURITY2P AUTO ACTIVE PGM-AUCRUNR

Parameters or command
===>
F3=Exit F4=Prompt F5=Refresh F9=Retrieve F11=Display schedule data
F12=Cancel F17=Top F18=Bottom

Bottom
```

Figure 5: Work with Subsystem Jobs

Capture All Rule

If you have not set any capture rules, you can set a general rule to capture all activity.

1. Select **19. Add Capture All rule (if no rule)** from the **Activation** menu. The rule is created.

Practical Tutorials for Working with Capture

Tutorial 1: Defining Your First Capture Rule

You must define Capture rules in order to begin capturing user screens automatically. In a new installation there are no default rules, therefore, screen captures will not occur until you define some rules. The following steps will guide you through the process of defining your first Capture rule. This example will capture all screen activity for the security officer (*QSECOFR*). The purpose of this exercise is simply to introduce you to the rule definition process. A detailed explanation of the various options can be found in [Rules](#).

1. Select **1. Capture Rules** from the main menu. The **Work with Capture Rules** screen appears.
2. Press **F6** to add a new rule. The **Add Rule** screen appears.
3. Type '**10**' in the **Sequence** field to cause this rule to be executed first.
4. Type a meaningful, descriptive text in the **Description** field.
5. Type '***ALL**' in the **IP Address** field. This indicates that the rule applies to all incoming addresses.
6. Type '**0.0.0.0**' in the **Subnet Mask** field. The subnet mask is required even though the rule applies to all IP addresses.
7. Type a user profile, a group or a special authority in the **User*, Special Auth, LMTCPB** field. This causes the rule to apply only to this user profile.
8. Type a '**Y**' in the **Copy screen** and **Log CL program commands** fields. This changes the job attributes to *LOGCLPGM(*YES)* and causes Screen to save screens, the job log and the CL command log for this user.
9. Press **Enter** to save the rule.
10. Press **F3** to exit the **Work with Capture Rules** screen.
11. Sign on to your IBM i system as the *QSECOFR* and perform some routine tasks. Capture will record your activity for later review.

Tutorial 2: Viewing Your First Captured Screens

When Capture has been activated and rules created, the system begins saving screen captures and logs immediately according to the rule parameters. You can view captured screens at any time after a capture session begins.

In this exercise, you will view several of the screens captured by the rule that you defined in the previous tutorial.

1. Select **41. Display Current Log** from the main menu. The **Display CapturedData** screen appears. This screen allows you to filter and display only those capture sessions that you wish to work with.

```
Display Captured Data (DSPCPTLOG)
Type choices, press Enter.
Display last n minutes . . . . . *BYTIME      Number, *BYTIME
Starting date and time:
  Starting date . . . . . *CURRENT          Date, *CURRENT, *YESTERDAY...
  Starting time . . . . . 000000           Time
Ending date and time:
  Ending date . . . . . *CURRENT          Date, *CURRENT, *YESTERDAY...
  Ending time . . . . . 235959           Time
User . . . . . _____             Name, generic*
Screen . . . . . _____            Name, generic*
IP generic* address . . . . . _____
String included in description _____
Data library . . . . . > *CURRENT      Name, *CURRENT, *PRV
Bottom
F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys
```

2. Press **Enter** to display the capture sessions for the current day. The **Work withCaptures** screen appears allowing you to select a specific capture session to view.

```

Work with Captures
iSecurity
Position to . . .
Type options, press Enter.
  1=Select  5=Display job  6=print  7=Search  8=Display job log
Estimated
Opt User   Terminal  Frames  IP Address  Capture Start  Capture End
█ ELVIO    QPADEV000L  25  192.168.1.8  2/10/08 12:52  2/10/08 14:06
- ELVIO    QPADEV000P  351 192.168.1.8  16/10/08 15:36 16/10/08 16:18
- ELVIO    QPADEV0005  235 192.168.1.9  10/10/08 16:28 10/10/08 16:51
- ELVIO    QPADEV0010  314 192.168.1.8  2/10/08 12:14  2/10/08 13:21
- ELVIO    QPADEV0010  13  192.168.1.8  2/10/08 13:23  2/10/08 13:27
- ELVIO    QPADEV0010  432 192.168.1.8  2/10/08 13:29  2/10/08 14:05
- FERNANDO QPADEV000C  152 1.1.1.177    20/10/08 12:07 20/10/08 14:27
- FERNANDO QPADEV000G  184 1.1.1.177    20/10/08 11:50 20/10/08 14:12
- JAVA1    QPADEV0008  40  1.1.1.164    2/10/08 14:57  2/10/08 15:02
- JAVA1    QPADEV0008  151 1.1.1.164    12/10/08 10:39 12/10/08 16:13
- JAVA1    QPADEV0008  16  1.1.1.164    15/10/08 9:42  15/10/08 9:58
- JAVA1    QPADEV0008  109 1.1.1.164    16/10/08 9:24  16/10/08 13:25
- JAVA1    QPADEV0008  10  1.1.1.164    19/10/08 11:04 19/10/08 16:11
Bottom
F3=Exit  F5=Refresh  F7=Subset  F11=Alt view  F12=Cancel  F13=Repeat

```

3. Type **1** to the left of the line showing the user.
4. The **Replay** screen now appears showing the first screen captured in the session. A floating **Capture** menu appears by default on all **Replay** screens. Press **F12** to hide the **Capture** menu. Press **F12** again and the **Capture** menu re-appears.

```

MAIN                               OS/400 Main Menu                               System:  S720

Select one of the following:

1. User tasks
2. Office tasks
3. General system tasks
4. Files, libraries, and folders
5. Programming
6. Communications
7. Define or change the system
8. Problem handling
9. Display a menu
10. Information Assistant options
11. Client Access/400 tasks

F5=DSPJOB   F6=Audit log   Capture   F8=DSPJOBLOG   F9=Print
Control. █ T, B, Frame#   91195/JAVA1/QPADEV0008   Frame: 1
Find . . .   Replay. 11:04 19/10/08
F3=Exit   F12=Un/Hide   F14=Colors   F16=Find   Enter=Move to cursor   Page Dn/Up
===> shwfc smz4dta/AUUSROP

-----
F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel   F13=Information Assistant
F23=Set initial menu
(C) COPYRIGHT IBM CORP. 1980, 2002.

```

5. Press **Page Down** and **Page Up** to scroll through the captured screens for this session. In this example, the user *QSECOFR* creates a new user profile.
6. Click at the top of the screen and press **Enter** . The **Capture** menu moves to the top, revealing the data hidden underneath.

```

MAIN                               OS/400 Main Menu
F5=DSPJOB   F6=Audit log   Capture   F8=DSPJOBLOG   F9=Print
Control.    _____ T, B, Frame#   91195/JAVA1/QPADEV0008   Frame:    1
Find . . . . .                               Replay: 11:04 19/10/08
F3=Exit   F12=Un/Hide   F14=Colors   F16=Find   Enter=Move to cursor   Page Dn/Up
  2. Office tasks
  3. General system tasks
  4. Files, libraries, and folders
  5. Programming
  6. Communications
  7. Define or change the system
  8. Problem handling
  9. Display a menu
 10. Information Assistant options
 11. Client Access/400 tasks

 90. Sign off

Selection or command
===> shwfc smz4dta/AUUSROP

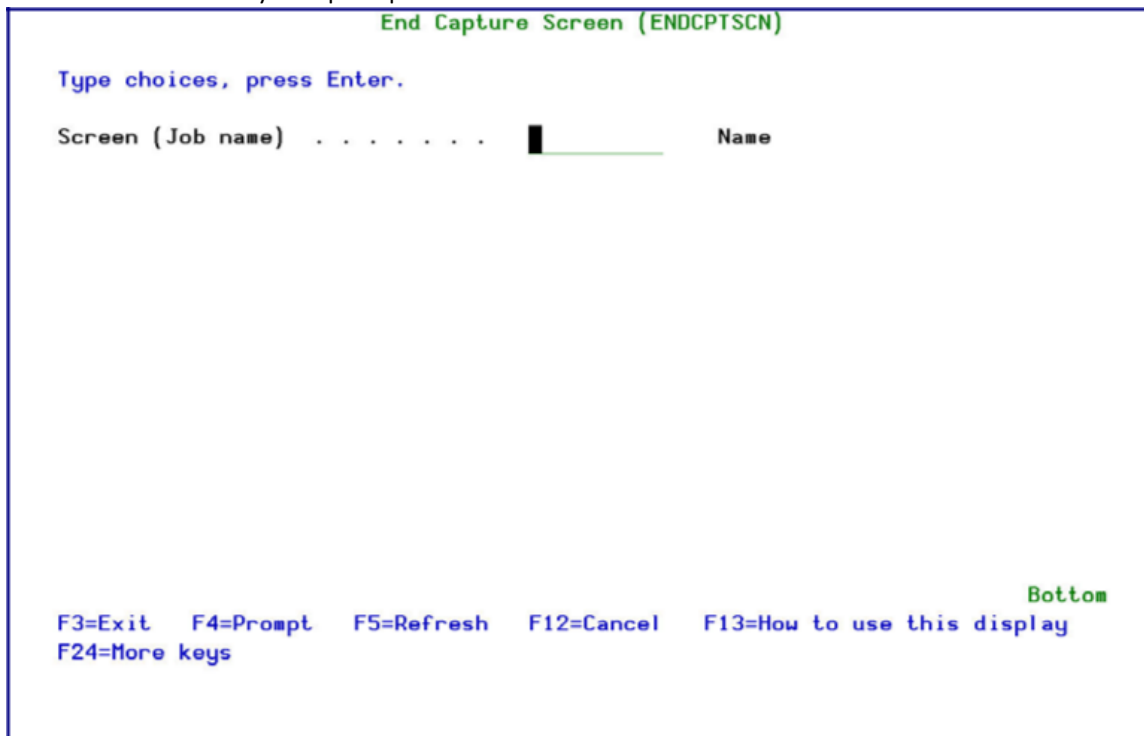
-----
F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel   F13=Information Assistant
F23=Set initial menu
(C) COPYRIGHT IBM CORP. 1980, 2002.

```

7. Type ' **B** ' in the **Control** field inside the **Capture** menu. The last screen captured in this session appears. Type ' **2** ' in the **Control** field. The second screen is displayed. You get the picture.
8. Press **F3** to exit the capture session. Press **F3** again to return to the main menu.

Tutorial 3: Start Capture Screen

1. Select **3. Start Capture Screen** off the main menu. The **Start Capture** screen appears. This screen allows you to immediately start capture sessions according to the screen (session/terminal) or the job name.
2. In order to end this action, Select **4. End Capture Screen** off the main menu and insert the screen or job name that you wish to immediately stop capture.



Chapter 3: Capture Rules

Capture uses rules to initiate capture sessions automatically according to one or more **Trigger criteria** covering different situations. Additionally, you can also use Action rules to trigger capture sessions based on events detected by other iSecurity components, such as Audit and Firewall .

Overview of Capture Rules

Strategic Approach

An effective audit trail is composed of data from several sources. Capture is most effective when used to supplement evidence collected from other security auditing tools (such as Audit) and network security tools (such as Firewall). Logs and reports generated by these tools provide an extensive written audit trail for virtually all security and system events. It is not necessary to have a visual audit trail for every event detected by these tools. However, a visual audit trail is highly appropriate for certain specific events and situations

Capture is provides you with tools that allow you to capture only those sessions where a visual audit trail is appropriate. You can define rules that trigger automatic captures according to a variety of conditions, such as time, user profile, IP address, and so on. Capturing all sessions at all times is **not recommended** because it may consume excessive system resources and contribute to performance degradation, especially in large organizations.

You should define capture rules to create a visual audit trail only when appropriate according to your security policies, regulatory environment, and operational requirements. The following paragraphs present a few examples of situational strategies.

Transaction Auditing in High Volume Environments

In environments with high transaction volumes, such as banking, retail, e-business, distribution, and so on, it is unrealistic to capture a lot of screen activity. In such cases, it would be more appropriate to capture a small sample of transactions for review. For example, you could define rules to

capture input activity by various users for limited time periods on a rotating basis. Should subsequent review uncover a high error rate or suspicious activity, you should create rules to capture a larger sample for these users.

Alternatively, you may wish to capture all or most activity of a particularly sensitive nature such as users responsible for offshore bank transfers, workstations dedicated to classified data or activity occurring outside of normal working hours.

Security Breaches and Suspicious Activity

Suspicious activity may be uncovered by auditing captured screen samples or by other security tools. In such cases, it is appropriate to create a visual audit trail for the particular user, workstation or IP address involved. Captured screens and command logs can supply crucial forensic evidence for legal proceedings or disciplinary action.

You can also use Action rules to initiate a capture session automatically upon detection of a suspected security breach or other suspicious activity.

Error Tracking and Debugging

Technical support departments can use Capture to provide visual evidence of specific user activities occurring immediately prior to error conditions. When a user reports an error condition, technical support personnel can initiate a manual screen capture prior to asking the user to replicate the condition. Programmers can initiate capture sessions by defining rules for specific users or test workstations while debugging new programs or features. They can also use Firewall rules to trigger a capture session automatically whenever a specific program or command is executed.

Trigger Criteria

Capture rules consist of **Trigger criteria** that, when true, initiate capture sessions automatically. A rule may contain several criteria, all of which must be true in order to trigger a capture session. Trigger criteria allow you to initiate capture sessions only when specifically required. Below are brief explanations of the various trigger criteria.

IP Address

You can initiate a capture session for a connection originating from a specific IP addresses or for a range of IP addresses with the subnet mask.

Additionally, you can use the Boolean **Not** field value to specify trigger criteria for all IP addresses **except** those specified in the rule.

For example, if you wish to capture all sessions that originate outside your local area network, use the IP address and subnet mask to define the range of valid addresses in your LAN and then select the Boolean **Not** field value.

Day and Time (Time Groups)

You can initiate a capture session automatically at specific times and on specific days by using predefined sets of day and time combinations called **Time Groups**. After it is defined, a given Time Group may be used in any number of rules. If you change the definition of a Time Group, the change is incorporated automatically into all rules using that group. Additionally, you can use the **Boolean Not** field value to specify trigger criteria for activity occurring outside the times specified in the rule.

For example, if you wish to capture activity for specific users working on the night shift, define a Time Group covering the days and working hours for the night shift and then specify this Time Group as a trigger criterion in your rules.

Terminal Session or Job

You can initiate a capture session for a specific terminal session by specifying the terminal name for that session. This is useful when tracking suspicious activity at a specific workstation.

You can also use the generic indicator ' * ' at the end of a text string to apply a trigger criteria to all terminal sessions beginning with the specified text string. For example, type ' *QPADEV** ' to start a capture session for sessions beginning with ' *QPADEV* '.

User Profile

You can initiate a capture session for a specific user. This is useful when tracking activity by specific users irrespective of the workstation or session name.

You can also use the generic indicator ‘ * ’ at the end of a text string to apply a trigger criteria to activity for all user profiles beginning with the specified text string. For example, type ‘ J* ’ to start a capture session for users beginning with the letter ‘ J ’.

Subsystem

You can initiate a capture session for jobs initiated under a particular subsystem. For example, if all of your payroll management applications run under a specific subsystem, you can capture all sessions using the payroll system with a single rule.

End Capture Session

You can specify a fixed time and date for the capture session to end. By default, a capture session ends only when the terminal session ends. This trigger criterion overrides the default.

Working with Time Groups

Time groups allow you to apply pre-defined sets of time-based criteria to capture rules without having to define complex criteria for each rule.

Time group filters can be:

- Inclusive – **Include all activities occurring during time group periods**
- Exclusive – **Include all activities not occurring during time group periods**

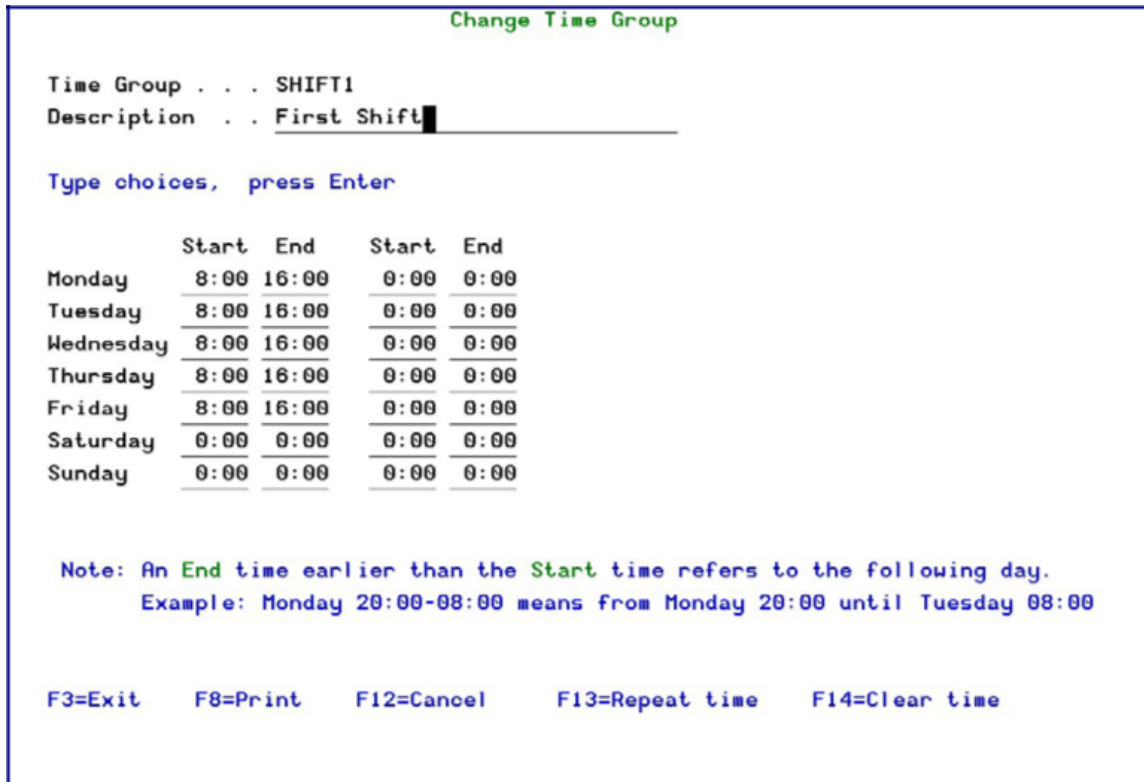
For example, you may define rules to track the activities of certain employees during normal working hours and others during nights and weekends. You can accomplish all of this with just one time group using the following guidelines.

1. Create a time group that defines normal working hours for each day of the week.
2. Use an inclusive time group filter (activities occurring during the time group periods) for each rule covering activity during normal working hours.
3. Use an exclusive time group filter (activities **not** occurring during the time group periods) for each rule covering activity outside of normal working hours.

Defining Time Groups

To define a Time Group, perform the following steps:

1. Select **21. Time Groups** from the Main menu. The **Define Time Groups** screen appears.
2. Select an existing time group to modify or press **F6** to create a new time group.
3. Enter the starting and ending times for each day of the week. Press **Enter** when finished.



The body of the screen includes these fields:

Description

A text description of the time group

Start and End

The starting and ending times for each group on that day, in 24-hour notation.

NOTE : If the ending time is less than the starting time, the period is considered to roll forward to the next day. For example, the period **20:00 – 08:00** extends from 20:00 until 08:00 the next morning.

The screen uses these function keys, in addition to the usual ones:

F13 (Shift-F1)

Copy starting and ending times from the cursor line to all subsequent days.

F14 (Shift-F2)

Erase the starting and ending times for the cursor line and all lines below it.

Defining Rules for Automatic Capture Sessions

This section describes the procedures and data entry screens for defining rules that initiate capture sessions automatically.

To create or modify a rule:

1. Select **1. Capture Rules** from the **Main** menu. The Work with Capture Rules screen appears.
2. Press **F6**. The **Add Rule** screen appears. Leave a field blank if there are no trigger criteria for that item.

```

Add Rule

Type choices, press Enter.

Sequence . . . . . █ 10.0-999.9
Description . . . . . _____

Selection criteria      N=Not  Value      Only specified fields are checked.
IP Address . . . . . - _____ N=Not within
  Subnet mask . . . . . - _____
Time group . . . . . - _____ N=Not within
Job (Terminal Id) . . . . . _____ Generic*
User*, Special Auth, LMTCPB _____
Enter generic* user profile, group profile, special authority (e.g. *ALLOBJ
*SECADM) or *SPCAUT for any special authority, limit capabilities. Use F4
Subsystem . . . . . _____ Generic*
Rule is valid until date _____ time _____

Process
Capture (copy screen) . . . Y Y, N, Blank = *SAME
Log CL program commands . . - Y, N, Blank = *SAME

F3=Exit  F4=Prompt          F12=Cancel
  
```

The body of the screen includes these fields:

Sequence

The sequence number for this rule. Rules are processed in sequential order according to this value.

Description

A text description of this rule.

IP Address

An IP address in decimal notation. Type '**N**' in the the Not field to apply this rule to all IP addresses other than that which is specified.

- ***ALL**: All IP addresses
- ***LCL**: All local 5250 (Twinax) terminal connections

Subnet mask

Subnet mask specifying IP address ranges. Press **F4** for help.

Time group

Time group that contains the times during which this rule will be applied. Press **F4** to select from list. Type '**N**' in the Not field to apply this rule to any time outside of that specified in the group.

Job (Terminal ID)

Terminal session name (This is also the job name.)

User*, Special Auth, LMTCPB

IBM i (OS/400) user profile or profile group

Subsystem

Subsystem in which the job is running

Rule is valid until ...

Date and time when the capture session is to end. If Blank, the rule is valid until the end of the terminal session.

Copy screen

Y: Capture and retain user screens

Keep CL commands

Y: Changes the job attributes to *LOGCLPGM(*YES)* .

3. Enter your trigger criteria and press **Enter** .

Manually Initiating Capture Sessions

You can initiate a capture session either from the main menu or from any command line. This option is useful if you discover a security breach or suspicious activity. Technical support personnel may also wish to initiate a capture session manually while troubleshooting error conditions or debugging applications.

Manual capture sessions may be started for any active job. You must know the job name (terminal session name) in order to perform this action. Use the *STRCPTSCN* command to obtain the job name.

Starting a Capture Session from Capture

To manually start a capture session:

1. Select **3. Start Capture Screen** from the main menu. The **Capture Screen** command screen appears.

```
Start Capture Screen (STRCPTSCN)

Type choices, press Enter.

Screen (Job name) . . . . . ██████████ Name, *
Valid for jobs starting within *BYTIME Minutes
Valid for jobs starting until:
  Date . . . . . *IMMED Date, *IMMED, *CURRENT
  Time . . . . . 235959 Time
Text . . . . . 'Requested by STRCPTSCN'

-----

F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys
Parameter SCREEN required.

Bottom
```

The body of the screen includes these fields:

Screen (Job name)

Terminal session name (this is also the job name)

Valid for jobs starting within

Enter the number of minutes

Valid for jobs starting until

Enter the date and time after which this capture session will end.

Press **F4** for options.

Text

Description of this capture session

2. Enter parameters as described in the following table. Enter your trigger criteria and press **Enter** .

Starting a Capture Session from the Command Line

To start a capture session from outside Capture :

1. Enter the ***STRCPTSCN*** command from any command line. The **Cap-
ture Screen** command screen appears.
2. Enter parameters as described in "Starting a Capture Session from Capture" on page 49

NOTE: In case the command *STRCPTSCN* is used for the same screen it is running in, no initial *GRINIT* is required.

Using Action to Trigger a Capture Session

You can use an Action command script to initiate a capture session automatically upon detection of a particular event, such as suspicious activity or an error condition. This powerful feature allows you to capture user activity silently and invisibly whenever these conditions are detected by Audit real time auditing or if a violation of Firewall rules occurs.

Real time auditing must be active at in order to take advantage of this feature. Additionally, if you are using a Firewall rule, you must configure the IBM i (OS/400) server to allow Action to react. Refer to the documentation for these products for further details.

To use Action to trigger a Capture Session:

1. Define a real time auditing rule, as described in the Audit manual.
2. Define your rule until the **Edit Action Script** screen appears.

```

                                Edit Action Script

Action . . WARN000001   User profile changed !

Type choices, press Enter.
Note: Add quotes where needed. e.g. CALL PGM PARM('&PARM01' '&PARM02').
Order Label      Command, GOTO label (unconditional)
-----
1.00             STRCPTSCN
-----
                On error, go to label . .
-----
2.00             On error, go to label . .
-----
                On error, go to label . .
-----
3.00             On error, go to label . .
-----
                On error, go to label . .
-----
4.00             On error, go to label . .
-----
                On error, go to label . .
-----
More...
F3=Exit  F4=Prompt  F7=Replacement variables  F8=Replacement job  F12=Cancel
F14=SYSLOG
Modify data, or press Enter to confirm.

```

3. Enter the **STRCPTSCN** command to capture a device or the **STRCPTUSR** command to capture a user profile on the first line.
4. Press **F4** to add parameters. The Start Capture Screen appears.
5. Press **F10** to view all parameters.
6. Enter the required parameters and press **Enter** .

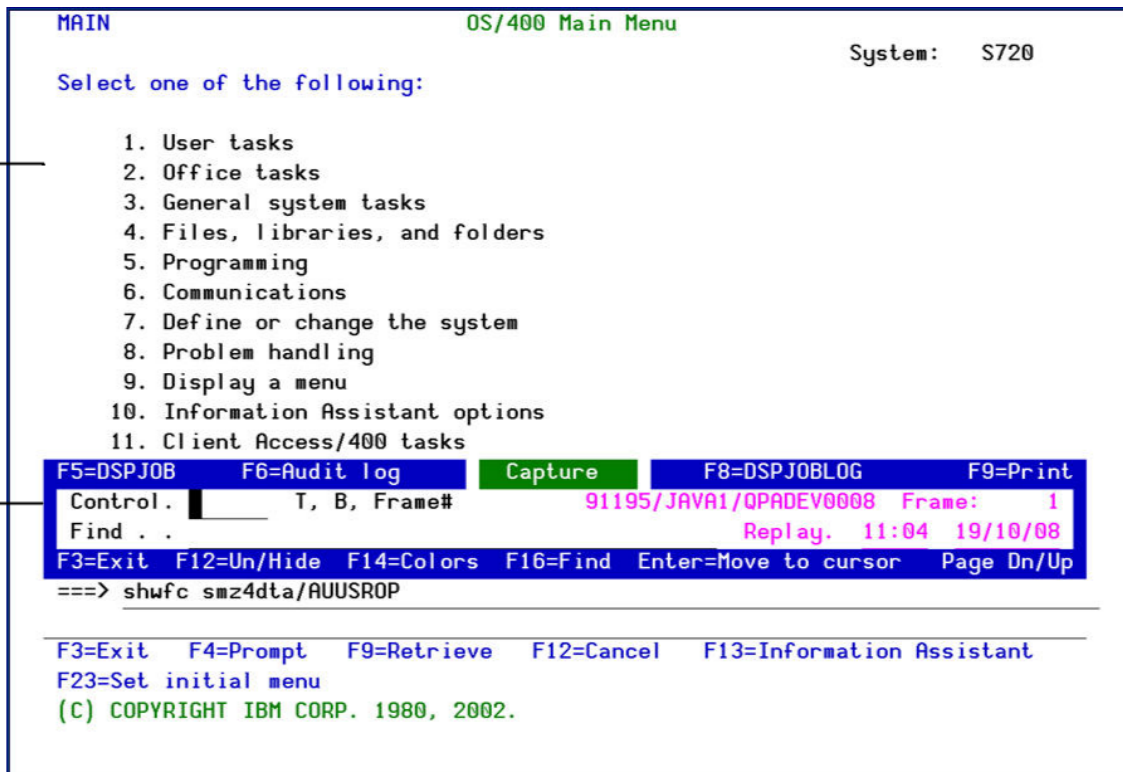
7. Press **F7** and select variables from the list. This inserts a **replacement variable** in the command script representing session (job) name.
8. Press **Enter** twice to complete the process.

Your capture session will begin automatically whenever the conditions defined in your rule are fulfilled.

Chapter 4: Auditing User Activity

Reviewing Captured Screens

You can replay captured screens by means of an intuitive process and easy-to-use tools for locating the captured data screens and logs. Captured screens are arranged as **frames** in individual capture sessions. Within each session, you can scroll through the frames sequentially or you can use the floating **Capture Menu** to move directly to a particular screen or search for screens containing a specific text string.



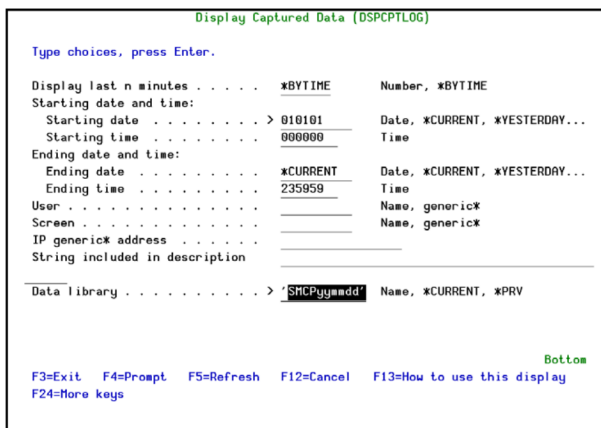
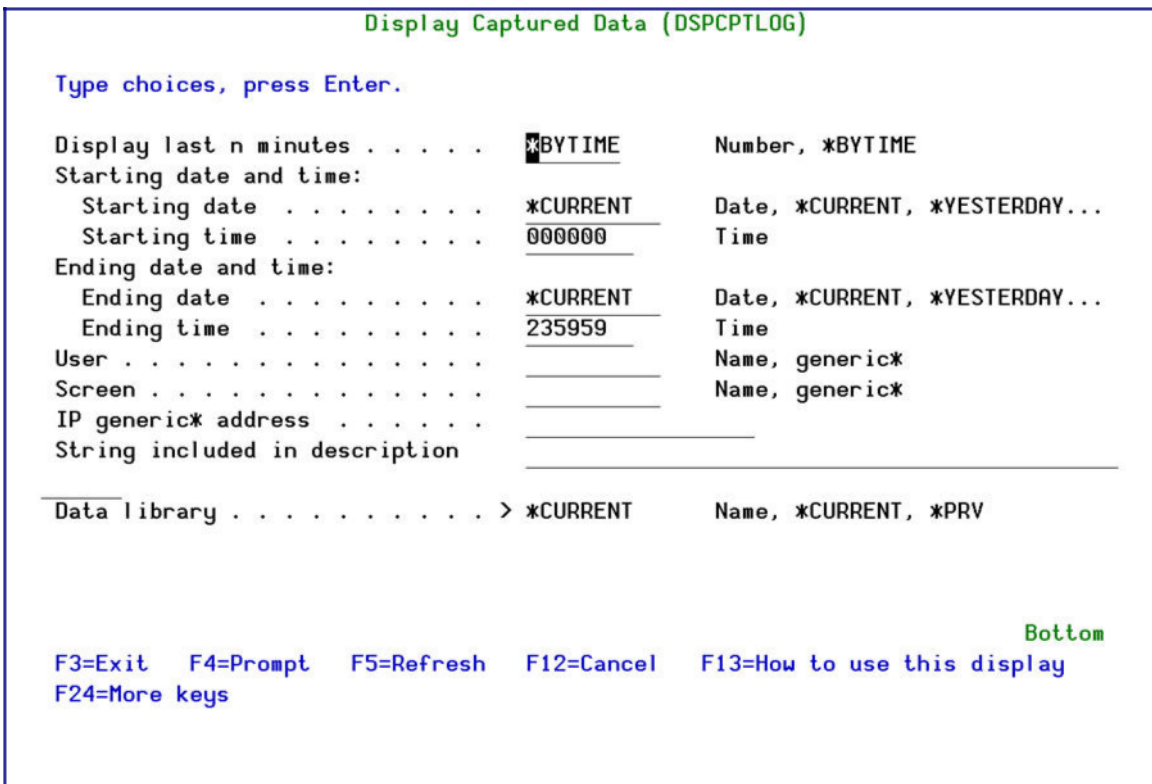
While reviewing the replay of captured screens, you can also use the Capture menu to display the job log, the Display Job menu and the Audit history log that relates to the current capture session.

The sections that follow describe the procedure and options for reviewing and auditing user activity as displayed on captured screens.

Selecting Screen Capture Sessions for Audit

You can work with screen capture sessions from either current data or restored data.

1. From the **Capture** main menu, select either **41. Display Current Log** or **42. Display Restored Log**. The **Display Captured Data** command screen appears. This screen allows you to select and display only those capture sessions that you wish to work with.



The body of the screen contains these fields:

Display Last n Minutes

Select only those records occurring within the previous number of minutes as specified by the user. To use the values from the next field, enter ***BYTIME**.

Starting Date & Time / Ending Date & Time

Select only those records occurring within the range specified by the starting and ending date/time combination.

Enter an appropriate specific date or time or use these values:

- ***CURRENT**: Today (Current Date)
- ***YESTERDAY**: Previous date
- ***WEEKSTR/*PRVWEEKS**: Current week/Previous week
- ***MONTHSTR/*PRVMONTH**: Current month/Previous month
- ***YEARSTR/ *PRVYEARS**: Current year/ Previous year
- ***SUN - *SAT**: Day of week

User

IBM i (OS/400) user profile or profile group

Screen

Terminal session name (This is also the job name)

IP Generic Address

IP address in decimal notation. Leave blank for all IP addresses.

String included in description

Text contained in Capture session descriptions. Only sessions containing this text string in the description field will be displayed.

Data library

For restored data only: Enter the name of the library to which the data was backed up. The name of the library is **SMCPyymmdd**, where **yymmdd** is the date of the backup.

2. Press **Enter** to display the capture sessions for the selected date and time. The **Work with Captures** screen appears which allows you to select a specific capture session to view. Each line represents a single capture session.


```

Work with Capture
iSecurity
Position to . . .
Type options, press Enter.
1=Select 5=Display job 6=Print 7=Search 8=Print Command 9=Mail as HTML
Estimated
Opt User Terminal Frames IP Address Capture Start Capture End
  AU QPADEV000L 9 1.1.1.154 11/02/14 10:40 11/02/14 10:41
  TEVG3 EVG3 0 1.1.1.193 11/02/14 12:10
Bottom
F3=Exit F5=Refresh F7=Subset F11=Alt view F12=Cancel F13=Repeat

```

Enter these values into the Opt field for each session:

- **1**: Replay screens in the selected capture session
- **5**: Display the IBM i (OS/400) Display Job (*DSPJOB*) menu for the selected capture session (Active jobs only)
- **6**: Print selected frames in the selected capture session
- **7**: Perform a free text search on the selected capture session. Type the search string in the pop-up window that appears and then press **Enter** to jump to the first screen containing the search string.
- **8**: Print the selected Capture session
- **9**: Mails the selected capture session as an HTML email

You can use these function keys in addition to the usual ones:

- **F7**: Refine selection parameters to display a smaller subset of the capture sessions
- **F11**: Toggle the screen display to show different capture session parameters
- **F13 (Shift+F1)**: Repeat the option entered on the current line for all subsequent lines. For example, if you type ' 1 ' to select the fifth line, you can press **F13** to select all lines that follow.

Navigating Through a Capture Session

When you select a capture session, the **Replay** screen appears showing the first frame (captured screen). The floating **Capture** menu appears by default on all **Replay** screens. Press **F12** to hide the **Capture** menu. Press **F12** again and the **Capture** menu re-appears.

```
MAIN                                OS/400 Main Menu                                System:  S720

Select one of the following:

1. User tasks
2. Office tasks
3. General system tasks
4. Files, libraries, and folders
5. Programming
6. Communications
7. Define or change the system
8. Problem handling
9. Display a menu
10. Information Assistant options
11. Client Access/400 tasks

F5=DSPJOB   F6=Audit log   Capture   F8=DSPJOBLOG   F9=Print
Control.   T, B, Frame#   91195/JAVAI/QPADEV0008   Frame: 1
Find . . .   Replay. 11:04 19/10/08
F3=Exit   F12=Un/Hide   F14=Colors   F16=Find   Enter=Move to cursor   Page Dn/Up
===> shwfc smz4dta/AUUSR0P

F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel   F13=Information Assistant
F23=Set initial menu
(C) COPYRIGHT IBM CORP. 1980, 2002.
```

- To scroll through the captured screens one screen at a time, use the **Page Down** and **Page Up** keys.
- To move the **Capture** menu and show the text below, simply move the cursor to another line on the screen and press **Enter**. The **Capture** menu moves to the cursor location.

```

MAIN                                OS/400 Main Menu
F5=DSPJOB  F6=Audit log  Capture  F8=DSPJOBLOG  F9=Print
Control.  T, B, Frame#  91195/JAVR1/QPDEV0008  Frame:  1
Find . . . . .  Replay.  11:04  19/10/08
F3=Exit  F12=Un/Hide  F14=Colors  F16=Find  Enter=Move to cursor  Page On/Up

  2. Office tasks
  3. General system tasks
  4. Files, libraries, and folders
  5. Programming
  6. Communications
  7. Define or change the system
  8. Problem handling
  9. Display a menu
 10. Information Assistant options
 11. Client Access/400 tasks

 90. Sign off

Selection or command
==> shufc smz4dta/AUUSROP

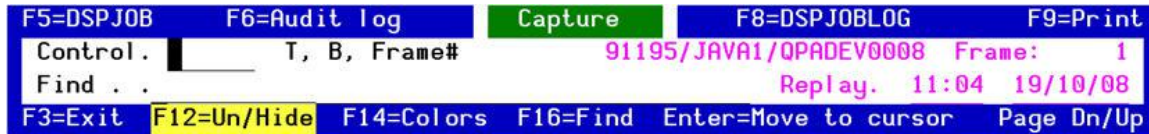
F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel  F13=Information Assistant
F23=Set initial menu
(C) COPYRIGHT IBM CORP. 1980, 2002.

```

- To hide or re-display the **Capture** menu, Press **F12** .
- To move to the last frame in the capture session, type '**B**' (Bottom) in the **Control** field inside the **Capture** menu. To move to the first frame, type '**T**'. To move to a specific frame, type the frame number.

Using the Capture Menu

The floating Capture menu serves as a convenient control panel for navigating through frames and for displaying job and audit history logs associated with the current capture session. The following table describes the features available from this menu.



The menu contains these fields:

Control

Move to a specific frame in the capture session

- **T** = First frame (Top)
- **B** = Last frame (Bottom)
- Frame Number = Move to the designated frame

Replay

Shows the capture time, date and frame number for the current frame

Find

Type a text string here to search for frames containing that string

You can use these function keys from the menu:

- **F3**: Exit the current capture session
- **F5**: Show the Display Job screen associated with the current capture session
- **F6**: Display the audit history log associated with the current capture session
- **F8**: Display the job log associated with the current capture session
- **F9**: Print one or more frames from the current capture session
- **F12**: Hide or un-hide the Capture menu
- **F16 (Shift+F4)**: Change the color used to highlight the search text string in frames
- **Enter**: Move the Capture menu to the cursor position
- **PgUp/PgDn**: Scroll forward or backward through frames

Free Text Search

Capture lets you search for screens within a capture session that contain a specific text string. This powerful feature allows you to locate specific screens quickly and easily within a capture session containing hundreds of screens. For example, you can use the free text search to locate screens containing:

- Specific data items, such as customer numbers or transaction codes
- Occurrences of error messages
- Use of certain commands, applications or parameters
- Programming keywords
- User profiles names

The free text search feature is available from both the **Work with Captures** list screen and from the **Capture** menu on replay screens. The basic procedure is the same with both methods.

Searching from the Work with Captures List Screen

1. Type '7' in the option field on any capture session line in the list and press **Enter**.
2. Type the search string in the pop-up window and press **Enter** again.

The screenshot shows the 'Work with Captures' screen with a search window open. The search window contains the text 'Please enter the argument to search: Find . .'. Below the search window, a list of capture sessions is displayed, filtered to show only sessions for user 'JAVA1'. The list includes columns for 'Opt', 'User', 'Terminal', 'Estimated Frames', 'IP Address', 'Capture Start', and 'Capture End'. The search results show several sessions for 'JAVA1' with various terminal IDs and IP addresses.

Opt	User	Terminal	Estimated Frames	IP Address	Capture Start	Capture End
7	ELVIO	QPADEV000L	25	192.168.1.8	2/10/08 12:52	2/10/08 14:06
-	ELVIO	QPADEV000P	351	192.168.1.8	16/10/08 15:36	16/10/08 16:18
-	ELVIO	QPADEV0005	235	192.168.1.9	10/10/08 16:28	10/10/08 16:5
-	FERNANDO	QPADEV000G	184	1.1.1.177	20/10/08 11:50	20/10/08 14:12
-	JAVA1	QPADEV0008	40	1.1.1.164	2/10/08 14:57	2/10/08 15:02
-	JAVA1	QPADEV0008	151	1.1.1.164	12/10/08 10:39	12/10/08 16:13
-	JAVA1	QPADEV0008	16	1.1.1.164	15/10/08 9:42	15/10/08 9:58
-	JAVA1	QPADEV0008	109	1.1.1.164	16/10/08 9:24	16/10/08 13:25
-	JAVA1	QPADEV0008	10	1.1.1.164	19/10/08 11:04	19/10/08 16:11

4. The first replay screen containing the desired text string appears. The text string appears highlighted in the color specified in system configuration (Default = **Red**). You can change this color by pressing **F14**.
5. To search for additional occurrences of the text string, press **F16**.

Searching Using the Capture Menu

1. Type the search string in the **Find** field in the **Capture** menu and press **Enter**.

```

Browse/Copy Options

Type choices, press Enter.

Selection . . . . . 1          1=Member
                                   2=Spool file
                                   3=Output queue
Copy all records . . . . . N    Y=Yes, N=No
Browse/copy member . . . . . grchkor  Name, F4 for list
  File . . . . . QRPGRSRC      Name, F4 for list
  Library . . . . . gs         Name, *CURLIB, *LIBL

Browse/copy spool file . . . . . KOREA  Name, F4 for list
  Job . . . . . KOREA         Name
  Use . . . . . FERNANDO     Name, F4 for list

F5=DSPJOB   F6=Audit log   Capture   F8=DSPJOBLOG   F9=Print
Control. █ T, B, Frame#   91228/FERNANDO/QPADEV000C   Frame: 9
Find . . job               Replay, 12:08 20/10/08
F3=Exit   F12=Un/Hide   F14=Colors   F16=Find   Enter=Move to cursor   Page Dn/Up
Library . . . . . *LIBL   Name, *CURLIB, *LIBL

F3=Exit      F4=Prompt      F5=Refresh      F12=Cancel
F13=Change session defaults   F14=Find/Change options
  
```

2. The first replay screen containing the desired text string appears. The text string appears highlighted in the color specified in system configuration (Default = Red). You can change this color by pressing **F14**.
3. To search for additional occurrences of the text string, press **F16**.

Printing and Mailing Captured Screens

While reviewing the replay of captured screens, you can also use the Capture menu to print/mail the job log, the Display Job menu and the Audit history log that relates to a specific job within a capture session.

Printing/Mailing Jobs from a Captured Session

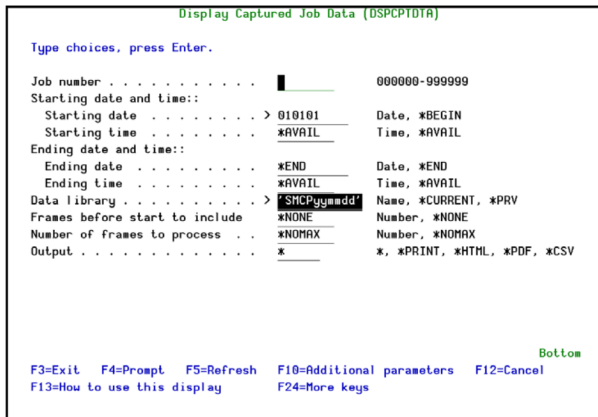
1. From the **Capture** main menu, select either **45. Display Current Data** or **46. Display Restored Data**. The **Display Captured Job Data** command screen appears. This screen allows you to select the job that you wish to work with.

```
Display Captured Job Data (DSPCPTDTA)

Type choices, press Enter.

Job number . . . . . █ 000000-999999
Starting date and time::
  Starting date . . . . . *BEGIN Date, *BEGIN
  Starting time . . . . . *AVAIL Time, *AVAIL
Ending date and time::
  Ending date . . . . . *END Date, *END
  Ending time . . . . . *AVAIL Time, *AVAIL
Data library . . . . . > *CURRENT Name, *CURRENT, *PRV
Frames before start to include *NONE Number, *NONE
Number of frames to process . . *NOMAX Number, *NOMAX
Output . . . . . * *, *PRINT, *HTML, *PDF, *CSV

Bottom
F3=Exit F4=Prompt F5=Refresh F10=Additional parameters F12=Cancel
F13=How to use this display F24=More keys
```

The screen contains these fields:

Job number

000000 - 999999

Starting Date & Time / Ending Date & Time

Select only those records occurring within the range specified by the starting and ending date/time combination.

Enter an appropriate specific date or time or use these values:

- ***CURRENT**: Today (Current Date)
- ***YESTERDAY**: Previous date
- ***WEEKSTR/*PRVWEEKS**: Current week/Previous week
- ***MONTHSTR/*PRVMONTH**: Current month/Previous month
- ***YEARSTR/ *PRVYEARS**: Current year/ Previous year
- ***SUN - *SAT**: Day of week

Data library

For restored data only: Enter the name of the library to which the data was backed up. The name of the library is **SMCPyymmdd**, where **yymmdd** is the date of the backup.

Frames before start to include

The number of frames before the start to include. To include none, enter ***NONE**.

Number of frames to process

The number of frames to process. To process all frames, enter ***NOMAX**.

Output

The destination for the output.

- *
- *PRINT
- *HTML
- *PDF
- *CSV

Keep as IFS file

- *NO
- *YES

Directory

Mail to

Mail text

Delete if attached

- *NO
- *YES

Compress and send together

- *NO
- *YES

Chapter 5: Capture Business Items

Business Items are the unique keys that access your data, such as a social security number, an insurance policy number, a bank account number. Use the Business Items menu to capture information relating to these important pieces of data.

Business Items provides all screen-related activities for specific business items and allows you to do the following:

- Extract business-items
- Isolate business items, even if programmers change their placement, as business item position is obtained directly from display file objects
- Detect related “environment” aspects such as the bank whose screen data is being viewed, whether the screen is from a test or production environment, and so on.
- Log all screens and pertinent information such as the job name, current user, name of display file and record format, name of the program which sent the screen and the line number within the program, library list, and so on.
- Send captured screens via HTML email to relevant people, aids in documenting the application, admissible in court, enables search and playback of captured screens Capture Business Items uses files CAFF and CABI, both of which are located in library SMZCDTA. The files are connected by the common fields of Job Name and Job Number. It is the responsibility of your organization to manage these files and to ensure that they do not fill up.

To use Capture Business Items, use the following workflow:

- Enable Business Items, as described in [Auto-Save Definition](#)
- [You can define a period of time in days after which all Capture files will automatically be saved.](#)
- [Defining Business Items Support](#) on page [21](#).
- Define Business Items, as described in [Business Items Definition](#) on page [67](#).

- If you set **Analyze run environment by *LIBL** to **Y** when you enabled Business Items, define the Business Items environments, as described in [Environments](#) on page 71.
- Define where Business Items appear in Display Files, as described in [Extract BusinessItems](#) on page 61.
- On a regular basis, check if any changes have been made in the Display Files, as described in [Check and Auto Repair Changes](#) on page 60.

To access the Business Items Handling menu, select **61. Business Items Menu** from the main menu. The **Business Items Handling** menu appears.

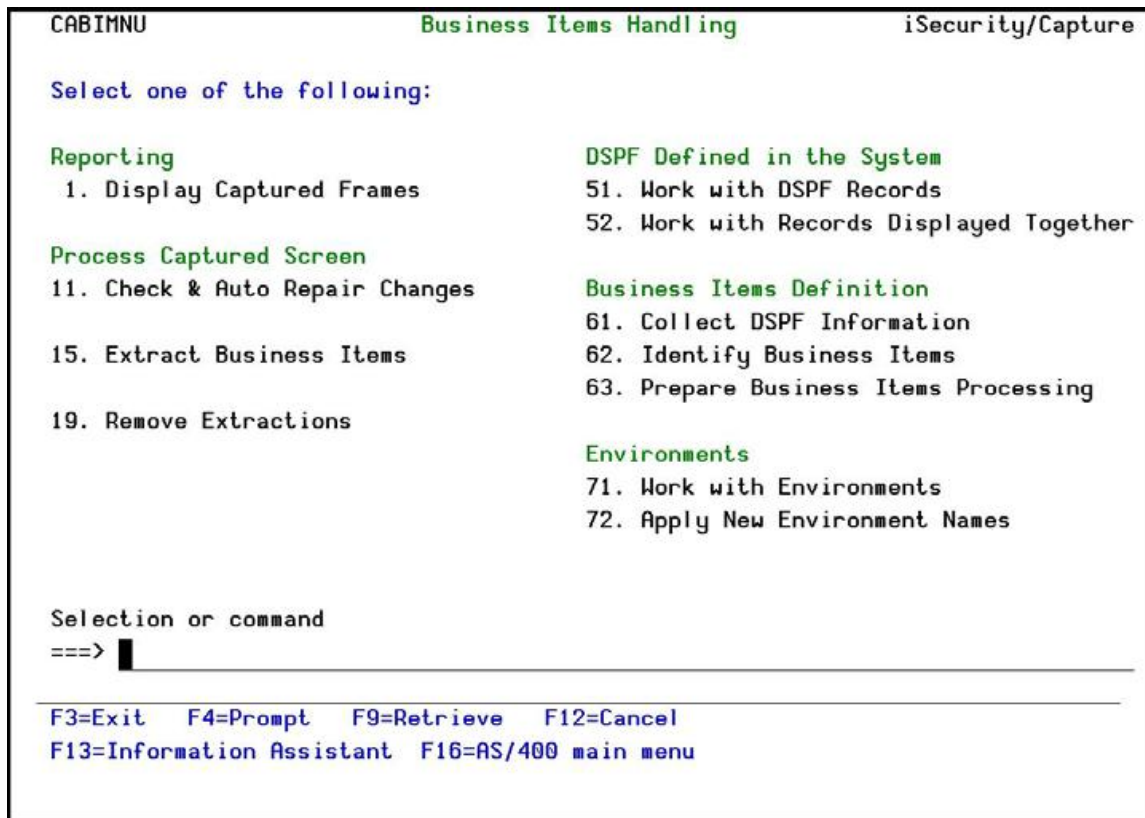


Figure 28: Business Items Handling

Reporting

Display Captured Frames

Displaying the captured frames allows you to see a step by step replay of the actions that were performed on the selected Business Items.

To display captured frames:

1. Select **1. Display Captured Frames** from the **Business Items Handling** menu. The **Display Capture Frames** screen appears.

```
Display Capture Frames (DSPCPTFRM)

Type choices, press Enter.

Display last minutes . . . . . *BYTIME      Number, *BYTIME
Starting date and time:
  Starting date . . . . . *CURRENT      Date, *CURRENT, *YESTERDAY...
  Starting time . . . . . 000000          Time
Ending date and time:
  Ending date . . . . . *CURRENT      Date, *CURRENT, *YESTERDAY...
  Ending time . . . . . 235959          Time
Analyze business data:
  Business item . . . . . *ALL          Name, *ALL
  Test . . . . .                    EQ, NE, GT, GE, LT, LE...
  Value . . . . .                    _____

+ for more values
User profile . . . . . *ALL          Name, generic*, *ALL
Environment . . . . . *ALL          Name, generic*, *ALL
Display file . . . . . *ALL          Name, generic*, *ALL

More...

F3=Exit  F4=Prompt  F5=Refresh  F10=Additional parameters  F12=Cancel
F13=How to use this display  F24=More keys
```

The screen includes these fields:

Display Last n Minutes

Select only those records occurring within the previous number of minutes as specified by the user To use the values from the next field, enter ***BYTIME**.

Starting Date & Time / Ending Date & Time

Select only those records occurring within the range specified by the starting and ending date/time combination.

Enter an appropriate specific date or time or use these values:

- ***CURRENT**: Today (Current Date)
- ***YESTERDAY**: Previous date
- ***WEEKSTR/*PRVWEEKS**: Current week/Previous week
- ***MONTHSTR/*PRVMONTH**: Current month/Previous month
- ***YEARSTR/*PRVYEARS**: Current year/ Previous year
- ***SUN - *SAT**: Day of week

Analyze business data

Business item

The name of one of your defined business items or ***ALL**

Test

If you enter a Business Item, you can filter further by testing it for specific values. You can use the following for testing:

- **EQ**: Equals the value in the **Value** field
- **NE**: Not Equal to the value in the **Value** field
- **GT**: Greater Than the value in the **Value** field
- **GE**: Greater Than or Equal to the value in the **Value** field
- **LT**: Less Than the value in the **Value** field
- **LE**: Less Than or Equal to the value in the **Value** field
- **LIKE**: Contains the value in the **Value** field
- **NLIKE**: Does not contain the value in the **Value** field
- **LIST**: Is in the List in the **Value** field
- **NLIST**: Is not in the List in the **Value** field

Value

The value to which the Business Item is compared

User Profile

Selects a subset of records by user profile. This can be a username, a Generic* name, or ***ALL**.

Environment

Selects a subset of records by environment. This can be a name, a Generic* name, or ***ALL**.

Display File

Selects a subset of records by display file. This can be a name, a Generic* name, or ***ALL**.

Program Name

Filter by the name of the program that created the record.

Library

The Library that contains the program

Job Name

User

Filter records by IBM i (OS/400) job name user.

Number

Filter records by IBM i (OS/400) job number.

Filter by time group

Relationship

- ***IN**: Include all records in time group
- ***OUT**: Include all records not in time group
- ***NONE**: Do not use time group, even if included in query definition
- ***QRY**: Use time group as specified in query definition

Time group

The name of the time group. Enter ***SELECT** to select the time group at run time.

Filter using query rules

The name of an existing query to use. Leave it at ***NONE** if not using an existing query.

Number of records to process

The maximum number of records to process. Set it to ***NOMAX** to process all the records.

Output

- *****
- ***PRINT**

- ***PRINT1 - PRINT9**
- ***OUTFILE**

Outfile format

- ***BYLINE**
- ***FRAME**

File to receive output

Name

The name of the field to receive output

Library

The library containing the file, or ***LIBL**

Output member options

Member to receive output

The name of the member, or ***FIRST**

Replace or add records

- ***REPLACE**
- ***ADD**

2. Enter your required parameters and press **Enter** . The **Work with Capture** screen appears with the appropriate entries.


```
Work with Capture

Type options, press Enter.
  1=Select  5=Display header

Opt User      Job      Date-time      Display      Function      Frame
█  FS      QPADEV0012  2014-04-23-15.10.16  QDUODSPF  P  INLPGM      0002
-  FS      QPADEV0012  2014-04-23-15.07.26  QDUODSPF  P  INLPGM      0001
-

F3=Exit  F5=Refresh  F12=Cancel  F17=Top

Bottom
```

3. Select option **1** to open the captured frames of a session or option **5** to see header information.

Process Captured Screen

Check and Auto Repair Changes

Once a day you should check that your Business Items are up to date.

To perform the daily check:

1. Select **11. Check & Auto Repair Changes** from the **Business Items Handling** menu. The **Is user intervention required?** screen appears.

```
CABIMNU                               Business Items Handling                               iSecurity/Capture
Se .....
: █                                     Is user intervention required?                               :
Re :                                                                              :
1 : There are 69 record formats of DSPFs that were changed.                               :
:                                                                              : r
Pr : There are 27 new Environments that were detected.                               :
11 :                                                                              :
: If any of the above numbers is not zero, you should take care of                               :
15 : the situation before extracting the information.                               :
:                                                                              :
: Press Enter to continue.                               :
:                                                                              :
:                                                                              :
:                                                                              :
.....

Selection or command
==> 11

-----
F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel
F13=Information Assistant  F16=AS/400 main menu
```

2. If the screen reports that either DSPFs or environments were changed, run the processes described in [Business Items Definition](#) on page [67](#).

Extract Business Items

Run an automatic procedure to extract all Business Items appearances in display files.

To extract the Business Items, select **15. Extract Business Items** from the **Business Items Handling** menu. If found, the Business Items are extracted. A message shows the result of the process.

Remove Extractions

You can remove some of the extracted Business Items from the repository.

To remove the extracted Business Items:

1. Select **19. Remove Extractions** from the **Business Items Handling** menu. The **Remove BI Extractions** screen is displayed.

```
Remove BI Extractions (RMVBIEXT)

Type choices, press Enter.

Starting date and time:
  Starting date . . . . .
  Starting time . . . . . 000000      Date, *CURRENT, *YESTERDAY...
                                         Time
Ending date and time:
  Ending date . . . . . *CURRENT    Date, *CURRENT, *YESTERDAY...
  Ending time . . . . . 235959      Time
Display file . . . . . *ALL         Name, generic*, *ALL
Library . . . . . *ALL             Name, generic*, *ALL
Record . . . . . *ALL              Name, generic*, *ALL

                                         Bottom
F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys
```

Starting Date & Time / Ending Date & Time

Remove only those Business items records for which the event occurred within the range specified by the starting and ending date/time combination.

Enter an appropriate specific date or time or use these values:

- ***CURRENT**: Today (Current Date)
- ***YESTERDAY**: Previous date
- ***WEEKSTR/ *PRVWEEKS**: Current week/Previous week
- ***MONTHSTR/ *PRVMONTH**: Current month/Previous month
- ***YEARSTR/ *PRVYEARS**: Current year/ Previous year
- ***SUN - *SAT**: Day of week

Display file

Selects a subset of records by display file. This can be a specific file name, a Generic* name, or ***ALL**.

Library

Selects a subset of records by library. This can be a specific name, a Generic* name, or ***ALL**.

Record

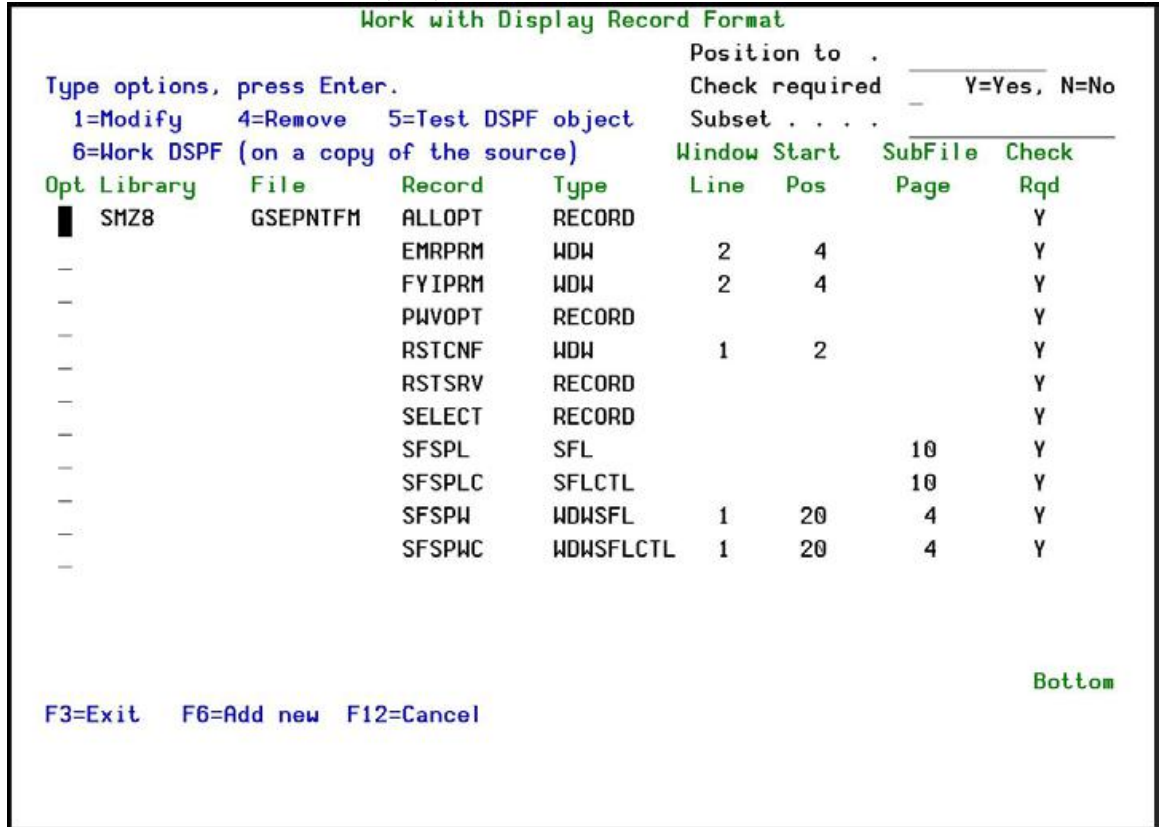
Selects a subset of records by record. This can be a specific name, a Generic* name, or ***ALL**.

2. Enter your required parameters and press **Enter** . The appropriate extracted Business Items are removed from the system.

DSPF Defined in the System

Work with DSPF Records

1. Select **51. Work with DSPF Records** from the **Business Items Handling** menu. The **Work with Display Record Format** screen appears.



2. Type **1** next to a format to modify it or press **F6** to add a new format. The **Add RecordFormat Relations** screen appears. Values are pre-populated according to the position of the cursor in the **Work with Display Record Format** screen.

```

Add Record Format Relations

Type choices, press Enter.

Display file . . . . . GSEPNTFM      Name
Library . . . . . SMZ8

Record . . . . . ALLOPT      Name
Type . . . . .                SFL, SFLCTL, RECORD, WDWSFL,
                               WDWSFLCTL, WINDOW

For Window:
Current      Previous
Actual start line . . . 0          0
Actual start position . 0          0

For SFLCTL:
Subfile page . . . . . 0
Check required . . . . . Y

F3=Exit   F4=Prompt   F12=Cancel

```

The body of the screen includes these fields:

Display file

Selects a subset of records by display file. This can be a specific file name, a Generic* name, or ***ALL**.

Library

Selects a subset of records by library. This can be a specific name, a Generic* name, or ***ALL**.

Record

Selects a subset of records by record. This can be a specific name, a Generic* name, or ***ALL**.

Type

- SFL
- SFLCTL
- RECORD
- WDWSFL

- WDWSFLCTL
- WINDOW

For Window:

Actual start line

The start line of the window

Actual start position

The starting position of the window

For SFLCTL

Subfile page

The subfile page of the SFLCTL

Check required

If set to Y, this record will be shown as requiring intervention in the **Is user intervention required?** screen, as shown in "Check and Auto Repair Changes" on page 74.

3. Enter your selection parameters and press **Enter** . The **Work with Display RecordFormat** screen re-appears.
4. Press **Enter** . The **Auto Update DSPF Record and Fields** screen appears.
5. Press **Enter** . Changes to DSPFs are automatically corrected in the Repository.

For DSPFs that have been modified, changes such as the position of fields on the screen or changes to the SFLPAG (Subfile page) are automatically corrected. Other changes, such as the renaming of Records or Fields, require user intervention.

Work with Records Displayed Together

1. Select **52. Work with Records Displayed Together** from the **Business ItemsHandling** menu. The **Work with Display Record Format Relations** screen appears.

```

Work with Display Record Format Relations

Type options, press Enter.                Position to . _____
1=Modify  4=Remove  5=Test DSPF object  Subset . . . _____
6=Work DSPF (on a copy of the source)    Auto
Opt Library  File      Record      Record      Added
┌ SMZ0      ODACTJFM  ALLOPT      SFLSPL
├           CHGCHDFM  SFSPPLC
├ SMZ1      CHGDFNFM  ADDP
├           SFCHSC
├ SMZ8      GSEPNTFM  ALLOPT      Y
├           EMRPRM      Y
├           FYIPRM      Y
├           SFSPPL      SFSPPLC
├           SFSPW      SFSPWC
├           SFSPWC      Y
└

F3=Exit  F6=Add new  F12=Cancel

Bottom
  
```

2. Type **1** next to a format to modify it or press **F6** to add a new format. The **Add RecordFormat Relations** screen appears. Values are pre-populated according to the position of the cursor in the **Work with Display Record Format** screen.

Add Record Format Relations

Type choices, press Enter.

Display file	<u>COACTJFM</u>	Name
Library	<u>SMZO</u>	
Record	_____	Name
Additional record	_____	Name

F3=Exit F4=Prompt F12=Cancel

3. Enter your selection parameters and press **Enter** .

Business Items Definition

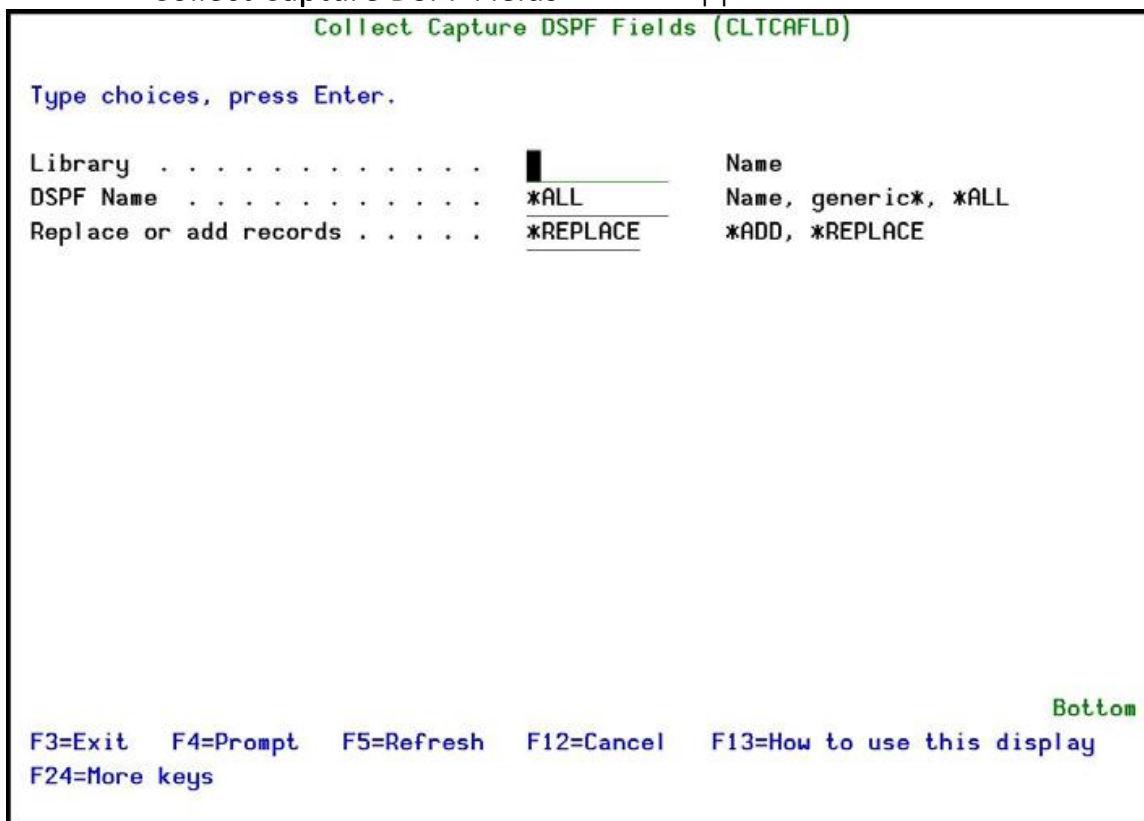
To work with Business Items in Capture , you must first define them to Capture . You do this by first collecting fields from all display files in the systems that you want to capture and then within that collection of fields, you identify the relevant Business Items.

Collect DSPF Fields

You must run this option once for every library for which you want to collect display fields. After you have run the option for every library, run the process described in [Identify BusinessItems](#) on page 68.

To collect display file fields from a library:

1. Select **61. Collect DSPF Fields** from the **Business Items Handling** menu.
The **Collect Capture DSPF Fields** screen appears.



The body of the screen includes these fields:

Library

The name of the library for which you want to collect display fields

DSPF Name

The name of the Display File. This can be a specific name, a Generic* name, or ***ALL**

Replace or add records

- ***ADD**: Add the records to the file.
- ***REPLACE**: Replace the records in the file.

For the first library for which you collect fields, use either ***ADD** or ***REPLACE**. For all consequent libraries, use ***ADD**.

Note that if you work with QTEMP, you must finish the process by running [Identify Business Items](#) before signing off from the session. If you sign off, then all information is lost and you must repeat the collection process again. Also, if you work with QTEMP, you must run the [Identify Business Items](#) option from the same workstation.

2. Enter your required parameters and press **Enter** . The fields that match the parameter requirements are collected.

Identify Business Items

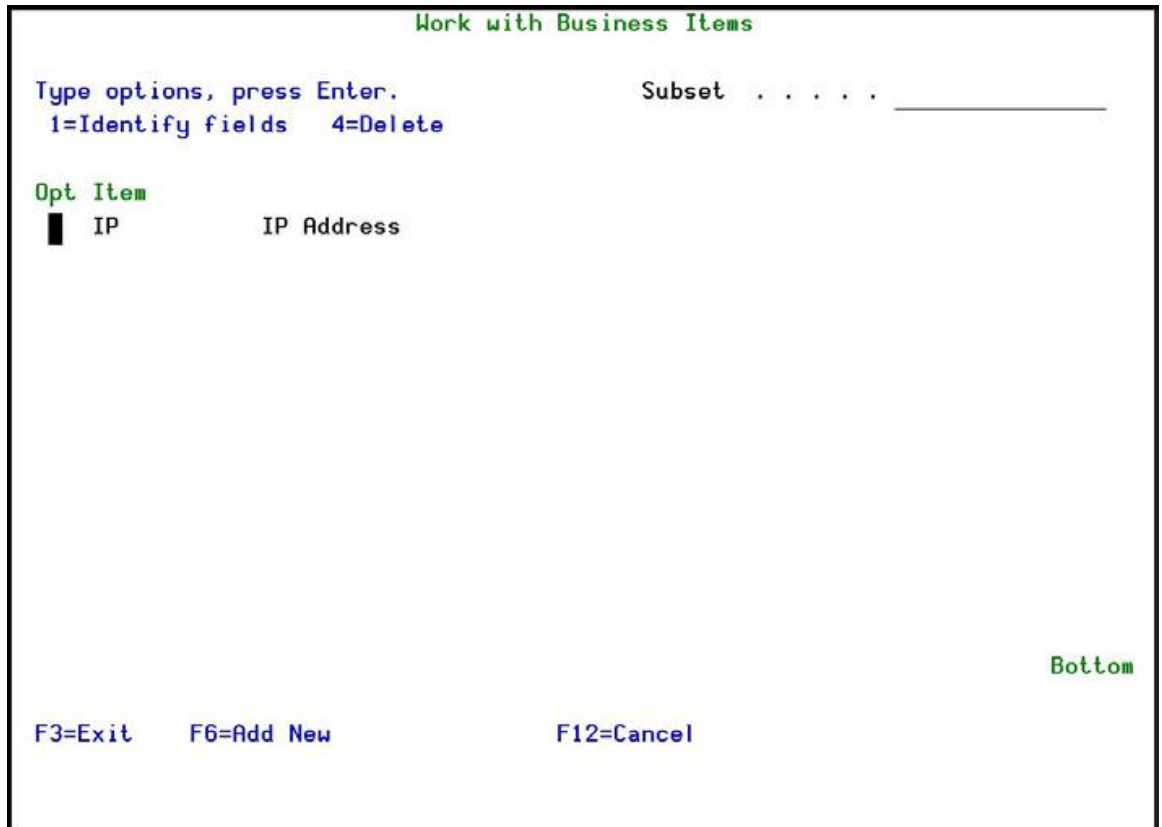
Before you identify the Business Items in the display files, you must first prepare the information by running the process described in "Collect DSPF Fields" on page 82

To collect display file fields from a library:

1. Select **62. Identify Business Items** from the **Business Items Handling** menu. The **Select Capture DSPF Fields** screen appears.



2. Enter the **Work Library** you used in the [Collect DSPF Fields](#) process and press **Enter** . The **Work with Business Items** screen appears.



3. Press **F6** to add new Business Items. The **Add Business Item** screen appears. Use this screen to filter for Business Items you want to track.

Add Business Item

Business item name	<input type="text"/>	Name	
Text	<input type="text"/>		
Type	A	A=Alpha, N=Numeric	
Length0		
Keep empty values in extracted BI	N	Y= Yes, N=No	

Include fields which either of the following is true for them:

Field name contains

or

Field text contains

or

Referencing field in file

library

or in file

library

F3=Exit F12=Cancel

Parameter or Option

The body of the screen contains these fields:

Business item name

Type a name for the Business Item

Text

Type a meaningful description for the Business Item

Type

The type of field to search for:

- **A** : Alphanumeric
- **N** : Numeric

Length

Enter the field length to search for. For a numeric field, include the number of decimal places.

Keep empty values in extracted BI

You can choose whether you want to extract a Business Item whose value is empty.

- **Y** : Yes
- **N** : No

Define fields which either of the following is true for them

Field name contains

Filters for field name.

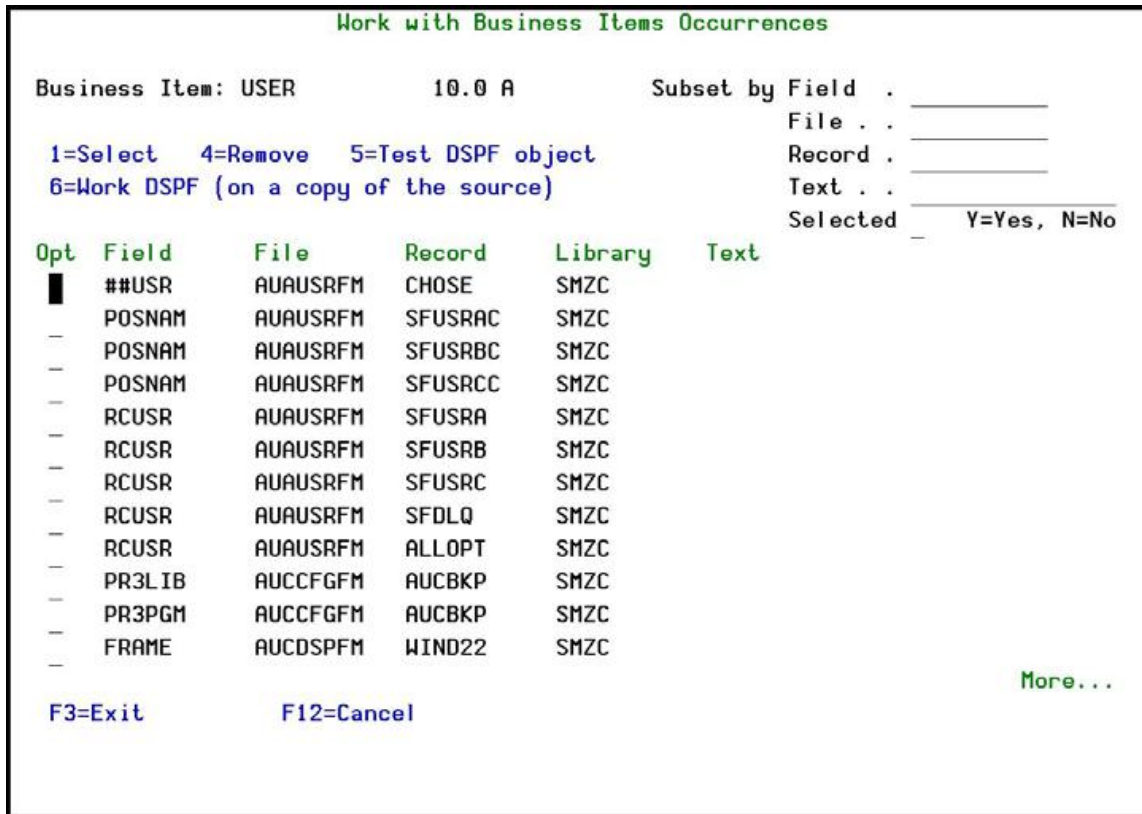
Field text contains

Filters for field text

Referencing field

Filters for referencing fields. Enter the field name, the file name and the library.

4. Enter your selection parameters and press **Enter** . The **Work with Business Items Occurrences** screen appears, showing all fields that meet the selection parameters.



5. Use option **1** to select all the fields you want to include and press **Enter**. The fields you want to track for this Business Item are chosen.

Prepare Business Items Processing

You should finally run a process to check if any changes have been made to the Display Files that contain the Business Items.

To prepare Business Items processing:

1. Select **63. Prepare Business Items Processing** from the **Business ItemsHandling** menu. The **Prepare Business Items Processing** screen appears.

```
CABIMNU                                Business Items Handling                                iSecurity/Capture

Se .....
: █                                     Prepare Business Items Processing      :
Re :
1 : This option checks and coordinates the system after selection      :
: of Business Items.                                                    :
Pr :
11 :
:
15 :
16 :
:
19 : Press Enter to continue, F3 to Cancel.                               :
:
: .....

Selection or command
===> 63

-----
F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel
F13=Information Assistant  F16=AS/400 main menu
```

Figure 42: Prepare Business Items Processing

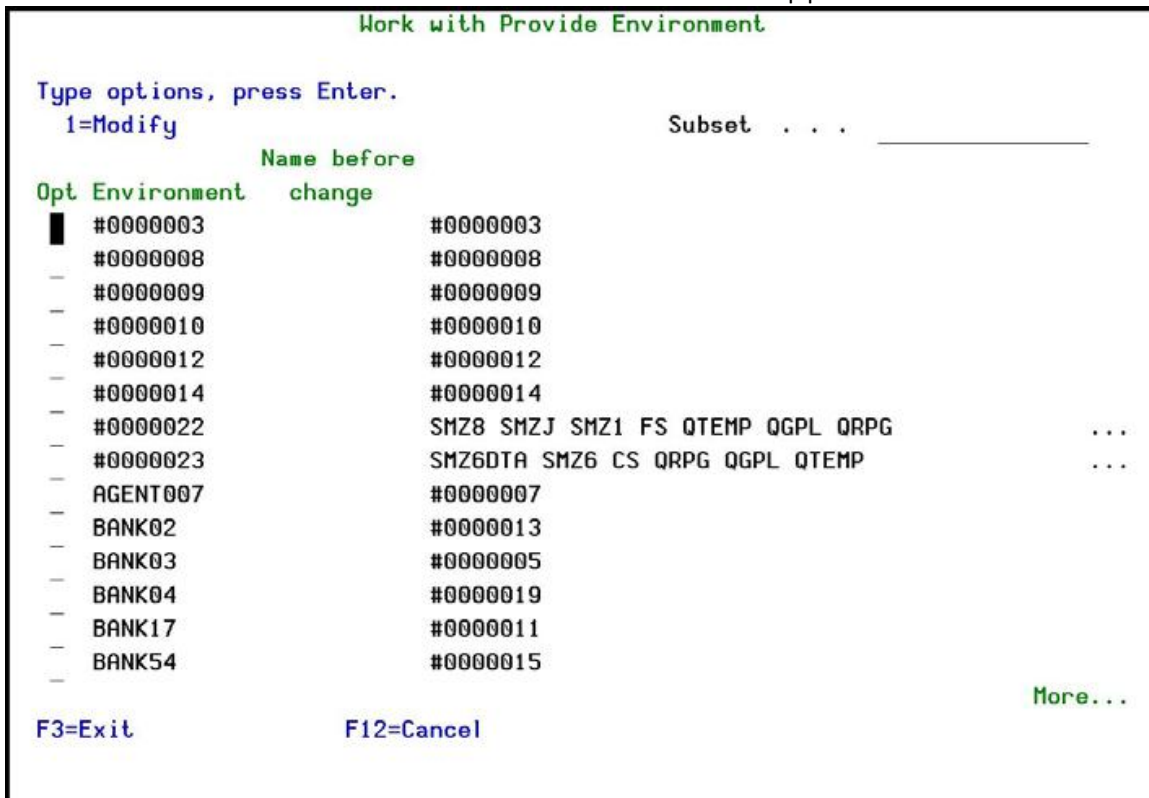
2. Press **Enter** . The display files are checked and a message showing the result of the checks appears.
3. If the message indicates that changes were detected, you must re-run the processes described in *Extract Business Item* , on page [61](#).

Environments

If, when you configured Business Items Support, you answered **Y** for the **Analyze runenvironment by *LIBL**, then temporary environment names are allocated automatically by Library List (See "Auto-Save Definition" on page 24 for more details). You should change these names to a meaningful name.

Work with Environments

1. Select **71. Work with Environments** from the **Business Items Handling** menu. The **Work with Provide Environment** screen appears.



2. Type **1** by the Environment you want to change. The **Modify Provide Environment** screen appears.

```

Modify Provide Environment

Type choices, press Enter.

Environment . . . BANK02
Description . . . #0000013
Name before change BANK02
Library list . . . QGPL      QTEMP      SMZ4DTA    SMZ4      SMZ0DTA
                  SMZO

F3=Exit          F12=Cancel

```

3. Update either the Environment field, or the Description field, or both fields, and press **Enter** twice. The **Work with Provide Environment** screen appears.
4. Press **F3** to exit the **Work with Provide Environment** screen. The **Set Permanent Environment Names** screen appears. This screen allows you to apply your changes to the Captures Screen Repository.

Apply New Environment Names

If you have multiple changes to Environment Names, you can apply all the changes at the same time.

1. Select **72. Apply New Environment Names** from the **Business Items Handling** menu. The **Set Permanent Environment Names** screen appears.

```
CABIMNU                               Business Items Handling           iSecurity/Capture

Se .....
:                                     Set Permanent Environment Names      :
Re :
1 : New names have been assigned to automatically selected Environments.  :
: These names must be applied to the Captures Screen Repository.          : r
Pr :
11 : Apply new names . . . . .           Y=Yes, N=No                       :
:                                                                           :
15 :                               :
: F3=Exit  F12=Cancel              :
:                               :
:                               :
: .....                          :
:                               72. Apply New Environment Names           :

Selection or command
===> 72

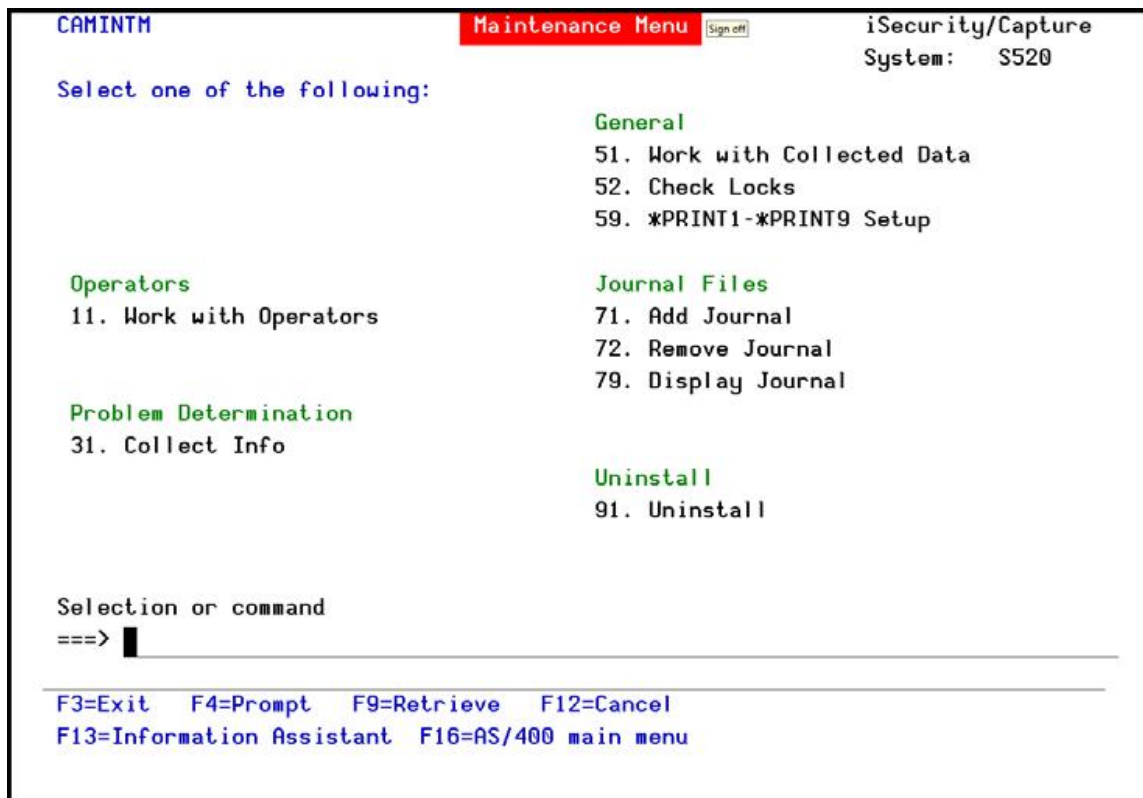
-----
F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel
F13=Information Assistant  F16=AS/400 main menu
```

2. Press **Enter** to apply your changes.

5

Chapter 6: Maintenance Menu

The **Maintenance Menu** enables you set and display global definitions for **Capture** . To access the **Maintenance Menu** , select **82. Maintenance Menu** from the main menu. The **Maintenance Menu** appears.



Journal Files

Add Journal

1. Select **71. Add Journal** from the **System Maintenance** menu. The **CreateJournal - Confirmation** screen appears.

```
CAMINTM                               Maintenance Menu                               iSecurity/Capture
.....                               .....                               .....
Select : █                            Create Journal - Confirmation           : S520
:                                       :                                       :
:   You are about to start journaling the product files.           :
:   The journal receivers will be created in library                :
:   SMZCJRND . If this library does not exist, it will              :
:   be automatically created.                                       :
Operat :                               :                                       :
11. Wo :   If you wish to create the library in a specific ASP,     :
:   you should press F3=Exit, create this library, and             :
:   run again this option.                                         :
Proble :                               :                                       :
31. Co :   Run this program again after future release upgrades.   :
:                                       :                                       :
:   Press Enter to start journaling, F3 to Exit.                   :
:                                       :                                       :
:   F3=Exit                                                         :
Selecti :                               :                                       :
==> 71 :.....                               :.....                               :
-----                               -----                               -----
F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel
F13=Information Assistant  F16=AS/400 main menu
```

2. Press **Enter** to confirm. The process of journaling the product files begins. The journal receivers will be created in library **SMZCJRND** . If this library does not exist, it will be automatically created.

NOTE: If you wish to create the library in a different ASP, press F3=Exit, create the library and run this option again.

NOTE: You must re-run this option after every release upgrade.

Remove Journal

1. Select **72. Remove Journal** from the **System Maintenance** menu. The **EndJournal - Confirmation** screen appears.

```
CAMINTM                               Maintenance Menu                               iSecurity/Capture
                                         System: S520
Select .....
: █                               End Journal - Confirmation           :
:                               :                                       :
:   You are about to end journaling the product files.             :
:   The journaling will stop in library SMZCJRND                   :
:                               :                                       :
Operat : Press Enter to end journaling.                             :
11. Wo :                                                               :
:   F3=Exit                                                         :
:                               :                                       :
Proble :.....
31. Collect Info
                               Uninstall
                               91. Uninstall

Selection or command
===> 72

-----
F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel
F13=Information Assistant  F16=AS/400 main menu
```

2. Press **Enter** to confirm.

Display Journal

1. Select **79. Display Journal** from the **System Maintenance** menu. The **DisplayJournal Entries** screen appears.

```
Display Journal Entries

Journal . . . . . : SMZC          Library . . . . . : SMZCDTA
Largest sequence number on this screen . . . . . : 0000000000000000012
Type options, press Enter.
  5=Display entire entry

Opt  Sequence  Code  Type  Object      Library      Job          Time
  █          1    J    PR
  -          2    D    JF  AUCAJOB1   SMZCDTA     QPADEV000B  10:54:18
  -          3    F    JM  AUCAJOB1   SMZCDTA     QPADEV000B  10:54:18
  -          4    D    JF  AUCHDR     SMZCDTA     QPADEV000B  10:54:18
  -          5    F    JM  AUCHDR     SMZCDTA     QPADEV000B  10:54:18
  -          6    D    JF  AUCRTG     SMZCDTA     QPADEV000B  10:54:18
  -          7    F    JM  AUCRTG     SMZCDTA     QPADEV000B  10:54:18
  -          8    D    JF  AUPRUD     SMZCDTA     QPADEV000B  10:54:18
  -          9    F    JM  AUPRUD     SMZCDTA     QPADEV000B  10:54:18
  -         10    D    JF  AUSYSID    SMZCDTA     QPADEV000B  10:54:18
  -         11    F    JM  AUSYSID    SMZCDTA     QPADEV000B  10:54:18
  -         12    D    JF  AUTIMEP    SMZCDTA     QPADEV000B  10:54:18
                                          More...

F3=Exit  F12=Cancel
```

2. To display a specific entry, type **5** by that entry and press **Enter** . The **DisplayJournal Entry** screen appears.

```

Display Journal Entry
Object . . . . . : AUCAJOB1      Library . . . . . : SMZCDBA
Member . . . . . :
Incomplete data . . : No          Minimized entry data : No
Sequence . . . . . : 2
Code . . . . . : D - Database file operation
Type . . . . . : JF - Start journaling for file

Entry specific data
Column *...+...1...+...2...+...3...+...4...+...5
00001 '10'

Bottom

Press Enter to continue.

F3=Exit  F6=Display only entry specific data
F10=Display only entry details  F12=Cancel  F24=More keys

```

Uninstall

Choose **98. Uninstall Product** from the **Maintenance** Menu, and follow the directions on the screen.

Uninstall CAPTURE

You are about to uninstall this product.

All program files, data and definitions will be deleted.

You are advised to print this screen for further reference.

Before proceeding, ensure that:

- o The product has been entirely de-activated
- o No user or batch job is working or intends to work with this product

To run uninstall procedure you should do the following:

- o Exit from the current session
- o Open a new session using QSECOFR or equivalent user profile
- o Enter: CALL SMZC/CARMVPRD

Once the uninstall is completed, enter: DLTLIB SMZC

Backups of previous releases might exist under the name QGPL/P_SMZ*

F3=Exit

