



Who and what changed your IMS Data and when did it happen....Big Questions, do you have the answers?

Webcast

Problem Investigator - Version 1.2

Program number 5655-K50



Highlights

IBM IMS Problem Investigator provides IMS administrators, system programmers and auditors with enhanced problem determination services.

Advanced features include:

- Support for IMS log, CQS log and IMS Connect event data
- Powerful dialog with a specialized log file viewer:
 - ▶ Full record formatting according to the mapping DSECTs
 - ▶ Zoom to get more field-level and diagnostic help information
 - ▶ Navigation aids to locate exact points in time
 - ▶ Tracking to trace the lifecycle of transactions through the log
 - ▶ Filters that allow you to see required log events only
 - ▶ Forms that allow you to format records to show required information only
 - ▶ User and vendor log records supported in the same way as IMS log records
 - ▶ Merge data from for sysplex, MSC, Connect etc. to get end-to-end picture
- Batch utility with identical features to the dialog



Problem 1: User reports a transaction failure

A user reports that his transaction produced incorrect results.

The only information available is user id, transaction code and the approximate time of the problem.

The IMS system uses MSC to process transactions remotely, but the same techniques can be applied equally for shared queues or other cross-system type analysis: To diagnose, we will go through the following steps:

1. Locate the start of the transaction in the front-end log file
2. Review the transaction input message details
3. Zoom to get additional information
4. Track the front-end transaction
5. Track until we arrive at the response
6. Review the transaction response
7. Locate the start of the transaction in the back-end log file
8. Use a Filter to select the required back-end transaction
9. Review the back-end transaction
10. Track until we locate the database updates
11. Assess the database update, notify application programmer and user!



1.1 Locate start of front-end transaction

```

BROWSE      IMS1. FE. OLP01                      Record 00006423 More: < >
Command ==> FIND 'USERID=JIM'                    Scrol I ==> CSR
Forwards / Backwards . . HH.MM.SS.THMIJU       Time of Day . . 10.35.01.260569
Code Descripti on                               Date 2005-08-09 Tuesday      Time (-7)
-----
/ 01  IMS Message                               10.35.01.260569
   UTC=10.35.01.260564 TranCode=ORDER Userid=JIM LTerm=LTERM01
   Terminal =TERM01 OrgUOWID=IMS5/BD6FADE29B4DF6A3
-----
- 35  Enqueue or Re-Enqueue a Message           10.35.01.260585
   UTC=10.35.01.260564 LTerm=TERM01 OrgUOWID=IMS5/BD6FADE29B4DF6A3
-----
- 31  GU from the Message Queue                 10.35.01.260641
   UTC=10.35.01.260639 LTerm=TERM01 OrgUOWID=IMS5/BD6FADE29B4DF6A3
-----
- 66  Standard 3600                             10.35.01.260657
-----
- 4002 Checkpoint - Message Queue records       10.35.01.261149
-----
- 4002 Checkpoint - Message Queue records       10.35.01.262979
-----
- 03  IMS Message                               10.35.01.263461
   UTC=10.35.01.236147 TranCode=GMMTRN01 Userid=CI CP5S02 LTerm=LC080015
   Terminal =LC080015 OrgUOWID=IMS5/BD6FADE294CD7B84
-----
- 31  GU from the Message Queue                 10.35.01.263473
   UTC=10.35.01.263466 TranCode=GMMTRN01 Userid=CI CP5S02 LTerm=LC080015
   Terminal =LC080015 Region=00A9 OrgUOWID=IMS5/BD6FADE294CD7B84
   RecToken=IMS5/08624909
-----
    
```

2. Find the start of the transaction
3. Note the start of the transaction

1. Navigate directly to the time of the problem

4. Verify the user id, transaction code and terminal

5. Note the Tracking UOW ID



1.2 Review the Transaction Input Message

```

BROWSE      IMS1. FE. OLP01                      Record 00006423 Line 00000000
Command ===> _____ Scroll I ===> PAGE

Form      ===> MSC01  + _ Use Form in Filter      Format ===> FORM

***** Top of data *****
+0004 Code... 01      IMS Message
+0386 STCK... BD6FADE29B519843      LSN... 000000BF79F1027
      Date... 2005-08-09 Tuesday      Time... 10.35.01.260569

+0004 MSGLCODE... 01      MSGFLAGS... C4      MSGDFLG2... 82
+0014 MSGUOW... Unit of Work (UOW) - Tracking
+0014 MSGORGI D... 'IMS1 '      MSGORGTK... BD6FADE29B4DF6A3
+0024 MSGPROI D... 'IMS1 '      MSGPROTK... BD6FADE29B4DF6A3

+0040 MSGSSEGM... Message Prefix System Segment; Item ID = 81
+0048 MSGLNODE 'LTERM01 '      MSGI DSTN... 'LTERM01 '
+0068 MSGODSTN... 'REMOTE2 '

+00BE MSGMSE... Message System Extension; Item ID = 8A
+00C2 MSGUTC... Coordinated Universal Time (UTC)
+00C2 MSGUDATE... 2005221F      MSGUTIME... 173501260564
+00CC MSGUZONE... 028D

+00D6 MSGMSCE MSC Extension System Segment; Item ID = 8B
+00E6 MSGMSFL5... 01      MSGMSFL6... 00      MSGMSFL7... 00
+00E9 MSGMSFL6... 00      MSGDSSI D... 0161      MSGRSI D... 05FB

+013E MSGMSC... TMR System Segment; Item ID = 8C
+014E MSGMSONM... 'REMOTE2 '      MSGMSI NM... 'LTERM01 '

+01D2 MSGXSTXT... Message Text
+0000 D6E2C9D4 F0C4E6F0 40C3C4C3 F1F3F8F1      *ORDER      CUSTOME*
+0010 F9404040 40404040 40D5C2D2 E2F4D2C6      *R IS WIDGETS INC*
    
```

1. Use special MSC Form to show only relevant information

2. Message destination is a remote system

3. Verify the transaction input message text



1.3 Zoom to get additional information

```

BROWSE      IMS1. FE. OLP01                               Line 00000000
Command ==> _____ Scroll ==> PAGE
***** Top of data *****
+00E6  MSGMSFL5... 01  MS flags -- Byte five

  Off  MSG5DTLU... 80  Associated Dest (MSGMNONM) is a TIB LUName
  Off  MSG5DQLU... 40  Associated Dest (MSGMSONM) is a QAB LUName
  Off  MSG5PRA... 20  User Program Route Exit
                        (DFSCMPRO or DFSMSCEO Routed message)
  Off  MSG5SMSN... 04  Source (MSGIDSTN) is a MSName. Used to be MSG5MSC
  Off  MSG5DRMT... 02  Destination (MSGODSTN) is a Remote Transaction
  On   MSG5DMSN... 01  Destination (MSGODSTN) is a MSName
***** End of data *****

```

We can “zoom” to every field in every record to find out more information.

In this case we can see that the input transaction message destination is a remote MSC system.

PI recognizes and formats all field types including:

Character, Hexadecimal, Dump, Integer counters, Flag bytes broken down into their bit settings (above), UTC timestamps, STCK timestamps (below) and elapsed times.

```

BROWSE      IMS1. FE. OLP01                               Line 00000000
Command ==> _____ Scroll ==> PAGE
***** Top of data *****
+002C  MSGPROTK... BA93F6015645A3C0

      Time (LOCAL)... 2004-01-05 18.00.03.865690 Monday

      Processing Token (STCK value)
***** End of data *****

```

1.4 Track the front-end transaction

```

BROWSE      IMS1. FE. 0LP01                      Record 00006423 More: < >
Command ==> . FESTART                          1. Establish a label so we can return to later  Scroll ==> CSR_
Forwards / Backwards . . HH.MM.SS.IHMIJU      Time of Day . . 10.35.01.260569

Code Descripti on                               Date 2005-08-09 Tuesday      Time (-7)
-----
TF 01  IMS Message                               10.35.01.260569
      UTC=10.35.01.260564 TranCode=ORDER Userid=JIM LTerm=LTERM01
      Terminal =TERM01 OrgUOWI D=IMS5/BD6FADE29B4DF6A3
-----
35  Enqueue or Re-Enqueue a Message              10.35.01.260585
      UTC=10.35.01.260564 LTerm=TERM01 OrgUOWI D=IMS5/BD6FADE29B4DF6A3
-----
31  GU from the Message Queue                    10.35.01.260641
      UTC=10.35.01.260639 LTerm=TERM01 OrgUOWI D=IMS5/BD6FADE29B4DF6A3
-----

```

2. Start tracking forwards from the start of the transaction.

Function Key 6 (F6) takes us to the next record associated with the transaction so you can follow its life-cycle.

Eventually we will arrive at the output response from the back-end MSC system.

1.5 Track until we arrive at the response

```

BROWSE      IMS1.FE.OLP01                      Record 00007126 More: < >
Command ==> _____ Scroll ==> CSR
Forwards / Backwards . . . HH.MM.SS.THMIJU   Time of Day . . . 10.35.01.260569
Code Description                      Date 2005-08-09 Tuesday   Time (-7)
/-----
TF 01    IMS Message                      10.35.01.260569
        UTC=10.35.01.260564 TranCode=ORDER Userid=JIM LTerm=LTERM01
        Terminal =TERM01  OrgUOWID=IMS5/BD6FADE29B4DF6A3
-----
. . . Skipped log records

S 01    IMS Message                      10.35.01.385960
        UTC=10.35.01.260564 TranCode=ORDER Userid=JIM LTerm=LTERM01
        Terminal =TERM01  OrgUOWID=IMS5/BD6FADE29B4DF6A3
-----
    
```

1. Input and Output messages "connected" by tracking UOW ID

S

2. Select the transaction response record to verify the results of the transaction



1.6 Review the Transaction Response

BROWSE IMS1.FE.OLP01 Record 00007126 Line 00000000

Command ==> _____ Scroll ==> PAGE

Form ==> MSC01 + _ Use Form in Filter Format ==> FORM

***** Top of data *****

```

+0004 Code... 01      IMS Message
+0386 STCK... BD6FADE2B9EE8047      LSN... 000000BF79F12E6
      Date... 2005-08-09 Tuesday      Time... 10.35.01.385960

+0004 MSGLCODE... 01      MSGFLAGS... C4      MSGDFLG2... 82
+0014 MSGUOW.... Unit of Work (UOW) - Tracking
+0014 MSGORGI D... 'IMS1'      MSGORGTK... BD6FADE29B4DF6A3
+0024 MSGPROI D... 'IMS1'      MSGPROTK... BD6FADE29B4DF6A3

+0040 MSGSSEGM... Message Prefix System Segment; Item ID = 81
+0048 MSGI NODE... 'LTERM01'      MSGI DSTN... 'LTERM01'
+0068 MSGODSTN... 'REMOTE2'

+00BE MSGMSE.... Message System Extension; Item ID = 8A
+00C2 MSGUTC.... Coordinated Universal Time (UTC)
+00C2 MSGU DATE... 2005221F      MSGUTI ME... 173501260564
+00CC MSGUZONE... 028D

+00D6 MSGMSCE... MSC Extension System Segment; Item ID = 8B
+00E6 MSGMSFL5... 04      MSGMSFL6... 00      MSGMSFL7... 00
+00E9 MSGMSFL8... 0A0      MSGDSSI D... 05FB      MSGSRSI D... 05FB

+013E MSGMSC.... TMR System Segment; Item ID = 8C
+014E MSGMSONM... 'REMOTE2'      MSGMSI NM... 'LTERM01'

```

```

+01D2 MSGXSTXT... Message Text
      +0000 D6E2C9D4 F0C4E6F0 40C3C4C3 F1F3F8F1      *ORDER FOR WIDGET*
      +0010 F9404040 40404040 40D5C2D2 E2F4D2C6      *S INC REJECTED! *

```

1. Verify the output response indicates failure

1.7 Back-end log file – where do we start?

```

BROWSE      IMS2. BE. OLP02      Record 00000001 More: < >
Command ==> FILTER           Scroll ==> CSR
Forwards / Backwards . . HH.MM.SS.THMIJU   Time of Day . . 10.35.01.260569
Code Description                               Date 2005-08-09 Tuesday   Time (-7)
-----
/ -----
___ 5600 External Subsystem - ESAF                10.35.00.002431
___ 03  IMS Message                               10.35.00.003283
___ 35  Enqueue or Re-Enqueue a Message          10.35.00.003293
___ 03  IMS Message                               10.35.00.003488
___ 35  Enqueue or Re-Enqueue a Message          10.35.00.003503
___ 37  Transfer Message from Temp to Perm Dest at SYNCPOINT 10.35.00.003509
___ 37  Transfer Message from Temp to Perm Dest at SYNCPOINT 10.35.00.003520
___ 31  GU from the Message Queue                10.35.00.003986
___ FA  Unknown Code: FAF10074F7F0F500F8F1F0F0F3F3F0F0C9D7E2F3 10.35.00.004023
___ 5600 External Subsystem - ESAF                10.35.00.004481
___ 5612 External Subsystem - End of Phase 2 Syncpoint (DBCTL) 10.35.00.004483
___ 5607 External Subsystem - Start of a Unit-of-Recovery     10.35.00.004483
___ 36  Dequeue/Save/Delete a Message on a Permanent Dest    10.35.00.004602

```

1. Log files contain records not applicable to our current investigation, so we need a way of removing unnecessary records.

2. Use a Filter to specify record selection criteria. Only records that match the criteria will be displayed.

1.8 Use a Filter to select the required transaction

```

EDIT                                     Filter                               Row 1 of 2 More: < >
Command ===> _____ Scroll I ===> PAGE

Filter . . . . . MSCPROB1 +
Description : . . . MSC Problem #1          _ Activate Tracking

/ Log Code + Exc Description
S ALL Global Criteria for all Log Record Codes
  Conditions . . . Yes Form . . . _____ +
-----
***** Bottom of data *****
    
```

- 1. Select all log records...
- 2. With our transaction tracking UOW ID

```

Command ===> _____ Condi ti ons                               Row 1 to 1 of 1
                                                                    Scroll I ===> PAGE

Code: ALL Global Criteria for all Log Record Codes

/ Field Name + Oper Value +
ORGUOWI D EQ */BD6FADE258AE1364
-----
***** Bottom of data *****
    
```

- Filter Features:**
- Select field name from the Prompt List
 - Useful common fields, no hex offsets required
 - Set common criteria for all record types

CODE	Log record Code	LSN	Log sequence number
TRANCODE	Transaction Code	PROGRAM	Program (PSB) name
USERID	User ID	LTERM	Logical Terminal
TERMI NAL	VTAM Termi nal	DATABASE	Database name
RBA	VSAM RBA or OSAM RBN	REGI ON	PST (Regi on) ID
LMSI D	IMS System ID		
ORGUOWI D	Org Tracking UOW ID	RECTOKEN	Recovery Token



1.9 Back-end transaction that performed the work

```

BROWSE      IMS2. BE. OLP02                      Record 00005511 More: < >
Command ==>                                     Scroll ==> CSR
Forwards / Backwards . . HH.MM.SS.THMIJU   Time of Day . . 10.35.01.260569
Code Descripti on                               Date 2005-08-09 Tuesday   Time (-7)
/
01  IMS Message                                10.35.01.181212
35  Enqueue or Re-Enqueue a Message            10.35.01.181219
31  GU from the Message Queue                  10.35.01.181718
03  IMS Message                                10.35.01.237407
35  Enqueue or Re-Enqueue a Message            10.35.01.237415
37  Transfer Message from Temp to Perm Dest at SYNCPPOINT 10.35.01.237437
33  Free Message                               10.35.01.237450
31  GU from the Message Queue                  10.35.01.237505
36  Dequeue/Save/Delete a Message on a Permanent Dest 10.35.01.279644
33  Free Message                               10.35.01.279651
***** Bottom of Data *****
    
```

1. Our Filter has reduced the display to show only back-end transaction records only

```

BROWSE      IMS2. BE. OLP02                      Record 00005511 More: < >
Command ==>                                     Scroll ==> CSR
Forwards / Backwards . . HH.MM.SS.THMIJU   Time of Day . . 10.35.01.260569
Code Descripti on                               Date 2005-08-09 Tuesday   LSN
/
TF 01  IMS Message                                10.35.01.181212
      UTC=12.35.00.987641 TranCode=ORDER Userid=JIM LTerm=LTERM01
      Terminal =TERM01 OrgUOWID=IPW3/BD6FADE258AE1364
-----
- 35  Enqueue or Re-Enqueue a Message            10.35.01.181219
      UTC=13.35.01.181217 TranCode=ORDER OrgUOWID=IPW3/BD6FADE258AE1364
-----
- 31  GU from the Message Queue                  10.35.01.181718
      UTC=13.35.01.181715 TranCode=ORDER Region=0126
      OrgUOWID=IPW3/BD6FADE258AE1364 RecToken=IMS2/057D29AE
-----
    
```

Tracking uses the Recovery Token to "find" recoverable events for example database updates



1.10 Track until we find database updates

```

BROWSE      IMS2. BE. OLP02                               Record 00005511 More: < >
Command ==> _____ Scroll I ==> CSR
Forwards / Backwards . . . HH.MM.SS.THMIJU   Time of Day . . . 10.35.01.260569
Code Description                               Date 2005-08-09 Tuesday   LSN
-----
TF 01  IMS Message                               10.35.01.181212
      UTC=12.35.00.987641 TranCode=ORDER Userid=JIM LTerm=LTERM01
      Terminal =TERM01 OrgUOWID=IPW3/BD6FADE258AE1364
-----
31  GU from the Message Queue                   10.35.01.181718
      UTC=13.35.01.181715 TranCode=ORDER Region=0126
      OrgUOWID=IPW3/BD6FADE258AE1364 RecToken=IMS2/057D29AE
-----
. . . Skipped log records
-----
S 50  Database Update                             10.35.01.227489
      UTC=13.34.46.059700 Program=ORDER Userid=JIM Database=ORDERDB
      RBA=1D74E000 Region=0126 RecToken=IPS3/057D29AE
-----
    
```

1. Start tracking forwards

Transaction events "connected" by Recovery Token

2. Select the database update to review the changes

3. Notice the database that was updated



1.11 Review database update, problem found!

```

BROWSE      IMS2. BE. OLP02                      Record 00006040 Line 00000000
Command    ===>
Form       ===> COMP50 + Use Form in Filter      Scroll ===> PAGE
Format    ===> FORM
***** Top of data *****
+0004 Code... 50 Database Update
+0B22 STCK... BD6FADE2A10BF582 LSN... 000000014605B7EC
      Date... 2005-08-09 Tuesday Time... 10.35.01.284031

+0006 DLOGPSTN... 0126
+0008 DLOGRTKN... Recovery Token
+0008 DLOIMSID... 'IPS3' DLOOASN... 057D29AE DLOCOMN... 00000001
+002A DLOGDBOR... 40 DLOGDSOR... 88
+002C DPGMNAME... 'PORDER' DDBDNAME... 'ORDERDB' DDSID... 01
+003E DLOGSLVL... 03 DLOGCALL... 40 DLOGRBA... 13060000
+0044 DLOGBLKO... 0000

+007A DLOGID... RACF Userid Section
+007A DLOGUSER... 'JIM'

+008A DLOGCDAT... Expanded UNDO Data (Compressed if Expand fails)
      +0000 01000000 00000A67 0000004B C1C4D4D5 *ACCOUNT=OK
      +0010 C2D2C3C9 F3C940D5 C2D2C30F 00001050 *+$1000

+00AA DLOGCDAT... Expanded REDO Data (Compressed if Expand fails)
      +0000 01000000 00000A67 0000004B C1C4D4D5 *ACCOUNT=ERROR
      +0010 C2D2C3C9 F3C940D5 C2D2C30F 00001050 *-$2000
    
```

Log data can be compressed, so PI automatically expands it

Database record before,
all is OK

Database record after,
Application data error

We now have all the information to help resolve the problem



Problem 2: IMS Connect Transactions ABEND

Helpdesk has reported that TCPIP-based internet transactions are failing.

IMS transactions are ABENDING and users are receiving error messages indicating that their requests have failed.

To diagnose, we will go through the following steps:

1. Use a Filter to look for application ABENDs in the IMS log file
2. Filtered log file shows ABENDs only
3. Track backwards to replay transaction in reverse
4. Identify the Connect Transaction Logon Token
5. Use IMS Connect Extensions to review the Connect events



2.1 Use a Filter to look for application ABENDs

- 1. Select type x'07' records
- 2. With the ABEND indicator set

```

EDIT                               Filter                               Row 1 of 2 More: < >
Command ==> _____ Scroll I ==> PAGE

Filter . . . . . ABEND2_ +
Description : : : ABEND Problem #2 _____ Activate Tracking

/ Log Code + Exc Description
S IMS 07      Application Terminate Accounting
Conditions . . Yes Form . . _____ +
-----
***** Bottom of data *****
    
```

```

                               Conditions                               Row 1 to 1 of 1
Command ==> _____ Scroll I ==> PAGE

Code: ALL Global Criteria for all Log Record Codes

/ Field Name + Oper Value +
DLRCMP      NE 0
-----
***** Bottom of data *****
    
```

3. Simple condition specification

- Filter Features:**
- Select field name from the Prompt list
 - Useful common fields, no hex offsets required
 - Set common criteria for all record types

DLRCMP	ABEND Flag Byte
DLRABEND	Application ABENDED
DLRBFALL	Dynamic backout failed
DLRCOMP	Completion Code in System format
DLRNJOB	Job name
. . .	



2.2 Filtered log file shows ABENDs only

Our Filter has caused only application ABENDs in the log file to be displayed allowing you to go directly to the record identifying the problem

```

BROWSE      TEAM23. IMS710. OTMA. LOG                      Record 00001678 More: < >
Command ===> _____ Scroll ===> CSR

Forwards / Backwards . . HH.MM.SS.THMIJU    Time of Day . . 10.35.01.260569

Code Descrip ti on                      Date 2004-01-05 Monday      Time (LOCAL)
/-----
- 07  Appl i cati on Termi nate Accounti ng      18. 16. 30. 744905
      UTC=18. 16. 30. 744900 TranCode=CEBTRAN5 Program=CEBPGM01 Regi on=0003
      RecToken=IMS0/00008F5E ABEND=U0119
-----
- 07  Appl i cati on Termi nate Accounti ng      18. 16. 30. 760665
      UTC=18. 16. 30. 760660 TranCode=CEBTRAN5 Program=CEBPGM01 Regi on=0004
      RecToken=IMS0/00008F5D ABEND=U0119
-----
TB 07  Appl i cati on Termi nate Accounti ng      18. 16. 31. 215192
      UTC=18. 16. 31. 215127 TranCode=CEBTRAN5 Program=CEBPGM01 Regi on=0002
      RecToken=IMS0/00008F5F ABEND=U0119
-----
***** Bottom of Data *****
  
```

1. Start tracking backwards to replay the transaction in reverse

2.4 Identify the Connect Transaction Logon Token

Records are formatted according to their DSECT mappings. In the case of the type x'01' record for a Connect transaction, this includes OTMA and Connect data

```

+0004 Code... 01      IMS Message
+03F6 STCK... BA93F9006D117F80      LSN... 0000000000ED1FE
      Date... 2004-01-05 Monday      Ti me... 18. 13. 28. 216855

+0000 MSGLRLL... 0406      MSGLRZZ... 0000      MSGLCODE... 01
+0005 MSGFLAGS... D1      MSGDFLG2... 81      MSGFPADL... 94
+0008 MSGMDRRN... 08001B22      MSGRDRRN... 08001B22      MSGPRFLL... 03B4
+0012 MSGCSW... 00      MSGDFLG3... 00
+0014 MSGUOW... Unit of Work (UOW) - Tracking
+0014 MSGORGI D... ' IMSO '      MSGORGTK... BA93F9006D0A1080
+0024 MSGPROI D... ' IMSO '      MSGPROTK... BA93F9006D0A1080

. . .
+0090 DFSYPRE... MVS APPC System Segment for OTMA; Item ID = 87
+0090 LUY_LENGTH... 024A      LUY_ZZ... 0000
+0092 LUY_MSG_PREFIX_TYPE... 87
+0095 LUY_CONVERSATION_TYPE... ' '
+0096 LUY_SYNC_LEVEL... ' C '
+0097 LUY_MSG_TYPE... 85      LUY_MSG_FLAG... 85
+0099 LUY_RACF_OPT... ' F '

. . .
+01DA HWSOMUSR... IMS Connect User Data
+01DA OMUSRLN... 0100      OMUSR_DESTI D... ' IMSO '
+01E6 OMUSR_ORI GI D... ' TRCBS003 '
+01EE OMUSR_PORTI D... 3382
+01F6 OMUSR_LTOKEN... BA93F9003069BE40
+01FE OMUSR_RETCODE... 00000000
+0202 OMUSR_RESCODE... 0000000000000000
+020A OMUSR_RTOKEN... 0B764AB8
+020E OMUSR_PASSTI CK... 0000000000000000
+0216 OMUSR_FLAG1... 00      OMUSR_FLAG2... 00
+0218 OMUSR_FLAG3... 20      OMUSR_TI MER... 00
+021A OMUSR_USTAT... 00000000

```

The Connect Logon Token uniquely identifies the transaction to IMS Connect.

We can replay the transaction as it happened inside IMS Connect using IMS Connect Extensions.

2.5 Review the transaction events in IMS Connect

IMS Connect Extensions provides comprehensive instrumentation for events in IMS Connect:

1. TCP/IP and socket events
2. Message Exits
3. SAF security calls
4. OTMA activity
5. Exception events, eg. time-out
6. Confirm ACKs and NAKs
7. Connect events, eg. tmember and datastore resources started and stopped

```

BROWSE      TEAM23. IMS710. OTMA. LOG                      Record 00001826 More: < >
Command ===>                                         Scroll ===> CSR
Forwards / Backwards . . 00.00.01.000000      Time of Day . . 18.08.00.000000
Code Description                               Date Date 2004-01-05 Monday      Time (LOCAL)
-----
/ -----
___ A03C Prepare READ Socket                      18.13.14.337549
___ A049 READ Socket                              18.13.14.557421
___ A049 READ Socket                              18.13.14.557467
___ A03D Message Exit called for READ, XMIT, EXER 18.13.14.557484
___ A03E Message Exit returned from READ, XMIT, EXER 18.13.14.557543
      TranCode=DSPALLI  Userid=MTC  OrgUOWID=CEX/BBDA9BEEFF6DE940  IMSID=IMD4
-----
___ A041 Message sent to OTMA                      18.13.14.557777
___ A042 Message received from OTMA                18.16.14.563185
___ A042 Message received from OTMA                18.16.14.565327
      OrgUOWID=CEX/BBDA9BEEFF6DE940  RESP=NAK
-----
___ A03D Message Exit called for READ, XMIT, EXER 18.16.14.565440
___ A03E Message Exit returned from READ, XMIT, EXER 18.16.14.565473
___ A04A WRITE Socket                             18.16.14.565572
___ A00C Begin CLOSE Socket                       18.16.14.565599
___ A00D End CLOSE Socket                         18.16.14.566096
___ A048 Trigger Event                             18.16.14.566118
***** Bottom of Data *****

```

The abending IMS transaction identified previously in the log file can be found in the IMS Connect Log by correlating the Connect Logon Token.

Problem 3: Transaction and Database audit

The IMS log contains an audit trail of all transaction and database update activity.

IMS PI provides advantages for system auditors to help them identify unauthorized system activity:

1. Removes much of the mystery surrounding log records and their contents
2. Provides easy-to-use features to help identify potentially unauthorized activity
3. Extract log record information to an audit trail file for long-term retention



3.1 Filter to look for potential unauthorized activity

x'01' Transaction input messages
x'50' Database update

```

EDIT                                     Filter                               Row 1 of 2 More: < >
Command ===> _____ Scroll I ===> PAGE

Filter . . . . . AUDIT1 +
Description . . . . . Look for unauthorized activity _ _ Activate
Tracking

/ Log Code + Exc Description
-----
S IMS 01          IMS Message
                  Conditions . . Yes Form . . _____ +
-----
S IMS 50          Database Update
                  Conditions . . Yes Form . . _____ +
-----
    
```

x'01' Look for transactions with suspicious input options
x'50' Look for database updates with suspicious updates

```

                                     Conditions
Code: 01  IMS Message

/  Field Name      +          Oper  Value +
-  TRANCODE        +          EQ    P*
-  MSGXSTXT(*)     +          EQ    UNAUTHORI ZED
***** Bottom of data *****
    
```

```

                                     Conditions
Code: 50  Database Update

/  Field Name      +          Oper  Value +
-  DATABASE        +          EQ    D*
-  DLOGDDAT(*)     +          EQ    $1,000,000
***** Bottom of data *****
    
```

3.2 Unauthorized transaction request

The same ISPF dialog formatting and functions are available in batch reporting:

```
V1R2M0          IMS V9.1          IMS Problem Investigator - Log Report          Page 1

+0004  Code... 01      IMS Message
+0375  STCK... B9B146DF1E7FBD00      LSN.... 0000000000001693
      Date... 2003-07-09 Wednesday  Time... 10.53.10.038523

+0008  MSGMDRRN... 080000D0      MSGORGID... 'IMD3'      MSGORGTK...
B9B146DF18969740
+0060  MSGIDSTN... 'LOCAL01'      MSGODSTN... 'ORDER'      MSGRACUS... 'HACKER'
+0368  MSGXSTXT...
      +0000  D7C1D9E3 40C1D5F9 F6F0C3F1 F0      *ORDER IS UNAUTHORIZED *
```

Fields displayed limited to those specified in a purpose-built audit Form

3.3 Unauthorized database update

The same ISPF dialog formatting and functions are available in batch reporting:

```

+0004 Code... 50      Database Update
+00BA STCK... B96A36B719479900      LSN.... 00000000002D5CFA
      Date... 2003-05-13 Tuesday      Time... 17.22.50.258553

+007A DLOGID..... RACF Userid Section
+007A DLOGUSER... 'HACKER '
+0082 DLOGUNDO... Undo Data Section
+0082 DLOGDFLG... 80      DLOGDFUN... 40      DLOGDOFF... 04F6      DLOGDLEN... 0004
+0088 DLOGDDAT...
      +0000 C7D6D6C440C4C1E3C1      *GOOD DATA
+008C DLOGREDO... Redo Data Section
+008C DLOGDFLG... 80      DLOGDFUN... 40      DLOGDOFF... 04F6      DLOGDLEN... 0004
+0092 DLOGDDAT...
      +0000 C2C1C440C4C1E3C1      *BAD DATA
  
```

User "HACKER" has corrupted...

"good data"

with "bad data"

3.4 Unauthorized system access

```
+0004 Code... 10      Security Violation
+002C STCK... B96AB0ADDA8EF600      LSN.... 00000000002E3DB6
      Date... 2003-05-14 Wednesday  Time... 02.28.29.690095

+0000 SCDL..... 003C      SCDZZ..... 0000      SCRFLAG....
10
+0005 SCFLAG1.... 40      SCERROR.... +20
+0008 SCNODE..... 'TERM01  '  SCTRAN..... 'ORDER  '
+0018 SCDST..... Violation Timestamp (UTC)
+0018 SCDATE..... 2003134F      SCTIME..... 072829690078
+0022 SCOFFSET... 008C
+0024 SCPGM..... 1CCB585000182740
```

```
+0006 SCERROR.... +20
```

Type of error:

- 4 - User not defined
- 8 - Password not defined to user
- 12 - Password expired
- 20 - Group not defined to User

Zoom to find reason for Security Violation

Highlights

IBM IMS Problem Investigator provides IMS administrators, system programmers and auditors with enhanced problem determination services.

Advanced features include:

- Support for IMS log, CQS log and IMS Connect event data
- Powerful dialog with a specialized log file viewer:
 - ▶ Full record formatting according to the mapping DSECTs
 - ▶ Zoom to get more field-level and diagnostic help information
 - ▶ Navigation aids to locate exact points in time
 - ▶ Tracking to trace the lifecycle of transactions through the log
 - ▶ Filters that allow you to see required log events only
 - ▶ Forms that allow you to format records to show required information only
 - ▶ User and vendor log records supported in the same way as IMS log records
 - ▶ Merge data from for sysplex, MSC, Connect etc. to get end-to-end picture
- Batch utility with identical features to the dialog

