Journaling Forensics 101

Steven Wolk
Chief Technology Officer
PC Richard & Son
SWolk@PCRichard.com

Today's Agenda

- Review of journaling concepts
- Tuning your journaling environment for forensics
- The old-fashioned, manual approach to dumping journal receivers
- The DMPJRN and CVTJRNDTA commands
- Practical example (time permitting…)

Disclaimer

- **ALL SOFTWARE IS PROVIDED "AS IS" WITHOUT ANY WARRANTY OF ANY NATURE WHATSOEVER. THE PROVIDER OF THIS SOFTWARE HEREBY DISCLAIMS ALL WARRANTIES, REPRESENTATIONS, AND CONDITIONS, STATUATORY OR OTHERWISE, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO WARRANTY OF TITLE AND THE IMPLIED WARRANTY OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE PROVIDER SHALL NOT BE LIABLE FOR ANY DAMAGES ARISING FROM OR AS A RESULT OF YOUR USE OF THIS SOFTWARE. USE IT AS YOUR OWN RISK.**

Disclaimer

- **This product is meant for educational purposes only. Any resemblance to real persons, living or dead is purely coincidental. Void where prohibited. Some assembly required. Batteries not included. Contents may settle during shipment. Use only as directed. No other warranty expressed or implied. Objects in the mirror are closer than they appear. Baby tested, mother approved. Melts in your mouth, not in your hand. Past performance does not guarantee future results. Do not use while operating a motor vehicle or heavy equipment. Postage will be paid by addressee. Subject to approval. This is not an offer to sell securities. Apply only to affected area. May be too intense for some viewers. For recreational use only. All models over 18 years of age. If condition persists, consult your physician. No user-serviceable parts inside. Freshest if eaten before date on carton. Subject to change without notice. Times approximate. Simulated picture. No postage necessary if mailed in the United States. Breaking seal constitutes acceptance of agreement. For off-road use only. As seen on TV. One size fits all. Many suitcases look alike. Contains a substantial amount of non-tobacco ingredients. Colors may, in time, fade. Slippery when wet. For office use only. Not affiliated with the American Red Cross. Drop in any mailbox. Edited for television. Keep cool; process promptly. Post office will not deliver without postage. List was current at time of printing. Not responsible for direct, indirect, incidental or consequential damages resulting from any defect, error or failure to perform. At participating locations only. Penalty for private use. Substantial penalty for early withdrawal. Do not write below this line. Falling rocks. Lost ticket pays maximum rate. Your cancelled check is your receipt. Avoid contact with skin. Sanitized for your protection. Be sure each item is properly endorsed. Sign here without admitting guilt. Slightly higher west of the Mississippi. Employees and their families are not eligible. Beware of dog. Contestants have been briefed on some questions before the show. Limited time offer, call now to ensure prompt delivery. You must be present to win. No passes accepted for this engagement. No purchase necessary. Shading within a garment may occur. Use only in well-ventilated area. Keep away from fire or flame. Replace with same type. Check here if tax deductible. Some equipment shown is optional. Price does not include taxes. No Canadian coins. Not recommended for children. Prerecorded for this time zone. Reproduction strictly prohibited. No solicitors. No alcohol, dogs, or horses. Restaurant package, not for resale. List at least two alternate dates. First pull up, then pull down. Call toll free before digging. Driver does not carry cash. Some of the trademarks mentioned in this product appear for identification purposes only. Record additional transactions on back of previous stub. Decision of judges is final.**

Obligatory Brag Slide

- PC Richard & Son
  - Founded in 1909 as a hardware store in Bensonhurst, Brooklyn.
  - Began transition to appliances by selling the first electric iron, and later the first washing machines.
  - Currently own and operate 66 retail showrooms throughout NY, NJ, CT, & PA.
  - Family owned and operated – 5th Generation
- Steve Wolk
  - Joined PCR in 1986
  - Became company's first CTO in 2000.

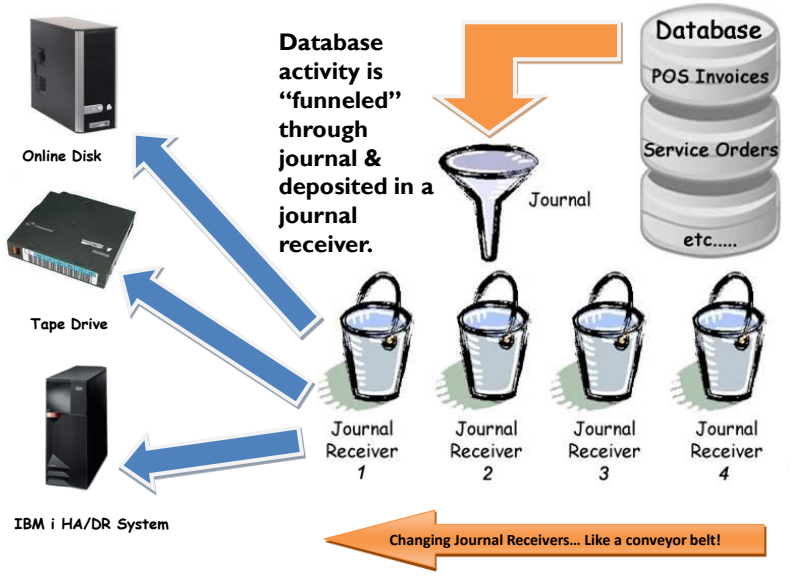
Most IBM i shops journal their DB files.

- Does yours?
- Why you should:
  - Enables use of Commitment Control
  - Recovery – APYJRNCHG, RMVJRNCHG
  - Replication to HA/DR system
  - Forensics

Objects involved in Journaling

- Journal
  - Attributes governing the what, where, when and how of journaling
  - Pointers to objects being journaled
  - Pointers to Journal Receivers
  - The Journal records the who, what, where, and when of what was done – along with what it looked like both before and after!
- Journal Receiver
  - Containers for the storage of journal entries, recording the journaled activity

Brief Review of Journaling Concepts



Optimal Journal Forensic Settings

- CRTJRN MINENTDTA(*NONE)
  - MINENTDTA (Minimize Entry Specific Data) is great in that it saves space in your journal receivers by only recording the changed bytes. However, by not recording the entire record, it makes forensics very difficult.
- STRJRNPF IMAGES(*BOTH)
  - This also takes more space in your journal receivers, but it's very useful to see both the before and after image when examining a changed record.

Journal Forensics…What's in it for me?

- You have bad data – what program did it?
- What else did that program do at that time?
- Replay events and transactions to understand a chain of events
- And of course … Find the bad guy

Dumping a Journal

- Step 1 – Gather Information
  - The file whose journal entries you need to dump
  - The journal used for this file – DSPFD
  - The journal receivers needed based on date/time range – WRKJRNA F15 to see the attach/detach date/time for each receiver.

Dumping a Journal

- Step 2 - DSPJRN to *OUTFILE
  - DSPJRN JRN(MYJRNLIB/MYJOURNAL)
    FILE((MYDBLIB/MYDBFILE MYMEMBER))
    RCVRNG(MYJRNLIB/STR_RCVR MYJRNLIB/END_RCVR)
    OUTPUT(*OUTFILE)
    OUTFILE(QTEMP/TMPJRNOUT)
    ENTDTALEN(*CALC)
  - This gives you an output file containing all the journal activity fields from record format QJORDJE along with a single field containing your database data. The length of this field is determined automatically by the ENTDTALEN(*CALC). This is known as the Entry Specific Data.

What does the Journal tell me?

Description	Field	Type	Length	Dec
Length of entry	JOENTL	S	5	0
Sequence number	JOSEQN	S	10	0
Journal Code	JOCODE	A	1	
Entry Type	JOENTT	A	2	
Date of entry	JODATE	A	6	
Time of entry	JOTIME	S	6	0
Name of Job	JOJOB	A	10	
Name of User	JOUSER	A	10	
Number of Job	JONBR	S	6	0
Name of Program	JOPGM	A	10	
Name of Object	JOOBJ	A	10	
Objects Library	JOLIB	A	10	
Name of Member	JOMBR	A	10	
Count or relative record	JOCTRR	S	10	0
Flag: 1 or 0	JOFLAG	A	1	
Commit cycle identifier	JOCCID	S	10	0
Incomplete Data: 1 or 0	JOINCDAT	A	1	
Minimized Esd: 0, 1, or 2	JOMINESD	A	1	
Not used	JORES	A	6	
Entry Specific Data	JOESD	A	Varies	

What does the Journal tell me?

Description

Length of entry
Sequence number
Journal Code
Entry Type
Date of entry
Time of entry
Name of Job
Name of User
Number of Job
Name of Program
Name of Object
Objects Library
Name of Member
Count or relative record
Flag: 1 or 0
Commit cycle identifier
Incomplete Data: 1 or 0
Minimized Esd: 0, 1, or 2
Not used
Entry Specific Data

Journal Codes

A	System accounting entry
B	Integrated file system operation
C	Commitment control operation
D	Database file operation
E	Data area operation
F	Database file member operation
I	Internal operation
J	Journal or journal receiver operation
L	License management
M	Network management data
P	Performance tuning entry
Q	Data queue operation
R	**Record level operation** ★★★★
S	SNADS, network alerts, or MSF
T	Audit trail entry
U	User generated
Y	Library operation

What does the Journal tell me?

Description
Length of entry
Sequence number
Journal Code
Entry Type
Date of entry
Time of entry
Name of Job
Name of User
Number of Job
Name of Program
Name of Object
Objects Library
Name of Member
Count or relative record
Flag: 1 or 0
Commit cycle identifier
Incomplete Data: 1 or 0
Minimized Esd: 0, 1, or 2
Not used
Entry Specific Data

Entry types for journal code R

BR	Before-image of record updated for rollback
DL	Record deleted from physical file member
DR	Record deleted for rollback
IL	Increment record limit
PT	Record added to physical file member
PX	Record added directly to physical file member
UB	Before-image of record updated in physical file member
UP	After-image of record updated in physical file member
UR	After-image of record updated for rollback

- To view list of entry types for other journal codes:
  - DSPJRN
  - Position cursor on "Type" column
  - Press Help

What does the Journal tell me?

Description
Length of entry
Sequence number
Journal Code
Entry Type
Date of entry
Time of entry
Name of Job
Name of User
Number of Job
Name of Program
Name of Object
Objects Library
Name of Member
Count or relative record
Flag: 1 or 0
Commit cycle identifier
Incomplete Data: 1 or 0
Minimized Esd: 0, 1, or 2
Not used
Entry Specific Data

- YOUR DATA!
- Hex representation of your record format though.
- The ESD must be broken apart into discrete fields to be really useful.
- Can be a pain to do this.

Why do we need to break down the ESD into discrete fields?

```
            Entry specific data
Column      *...+....1....+....2....+....3....+....4....+....5
00001      'A ¬        TK  VHB655X                    ¬È     '
00051      '      r¤   å±   ø           ¤                ¬   '
00101      '          Y       Â¬   "       '
```

Ugly… Isn't It? Of course, we could always F11 for hex view…

```
            Entry specific data
Column      * . . . + . . . . 1 . . . . + . . . . 2 . . . . +
00001      'C1055F1214010F001F001FE3D2001FE5C8C2F6F5F5E7404040'
00026      '40404040404040404040404040404040404040285F740F080F00'
00051      '00172F000001999F000000478F000001700F000F0000000F00'
00076      '000F009F001F020F012F000F000F000F000F00000F055F0000'
00101      '0F00000F00000F404040E840000F000F4008625F4001037F07'
00126      '380F00000F'
```

Not much better…

Dumping a Journal

- Step 3 – Break ESD into discrete fields
  - Use DDS or SQL to create a new PF containing the journal activity fields and your database fields.
- Step 4 – Map the data
  - CPYF FMTOPT(*NOCHK).
  - This maps the ESD to your discrete database fields.

But this all is a lot of effort, and we don't always have the time… so we create tools!

No time to dump journals the old fashioned way…

DMPJRN to the rescue…

The DMPJRN Command

```
                        Dump Journal Data (DMPJRN)

Type choices, press Enter.

Journal  . . . . . . . . . . . . JRN          _________
  Library  . . . . . . . . . . .               *LIBL
Range of journal receivers:      RCVRNG
  Starting journal receiver  . .              _________
    Library  . . . . . . . . . .               *LIBL
  Ending journal receiver  . . .              _________
    Library  . . . . . . . . . .               *LIBL
Journaled file:                  FILE

                                              _________
    Library  . . . . . . . . . .               *LIBL
  Member . . . . . . . . . . . .              *ALL
Converted Output file  . . . . . CVTOUTF      _________
  Library  . . . . . . . . . . .               *LIBL
Replace or add records . . . . . OUTOPT       *REPLACE
```

How does DMPJRN work?

- Reconstructs the DSPJRN command based on the DMPJRN parameters specified
- Passes the command to QCMDEXC
- Uses the CVTJRNDTA command to process the DMPJRN temporary output file

Tell me more about CVTJRNDTA!

```
                    Convert Journal Data (CVTJRNDTA)

Type choices, press Enter.

DSPJRN Output file . . . . . . . DSPJRNOUTF
  Library  . . . . . . . . . . .                  *LIBL
Converted Output file  . . . . . CVTOUTF
  Library  . . . . . . . . . . .                  *LIBL
Replace or add records . . . . . OUTOPT           *NONE
```

What CVTJRNDTA does…

- Creates the output file using an SQL join between the DSPJRN temporary output file and the original journaled PF.
- sqlcmd='create table ' + %trim(outlib) + '/' + %trim(outfil) +
  ' as (select joentl, joseqn, jocode, joentt, jodate, +
  jotime, jojob, jouser, jonbr, jopgm, joobj, jolib, +
  jombr, joctrr, joflag, joccid, joincdat, jominesd, +
  jores, ' + %trim(JrnFil) + '.* from ' +
  %trim(dsplib) + '/' + %trim(dspfil) + ', ' +
  %trim(jrnlib) + '/' + %trim(jrnfil) +
  ') with no data';

What CVTJRNDTA does…

- This new file contains the best of both worlds – the journal audit fields and your discrete database fields.
- Copies the data from the DSPJRN temporary output file to the newly created PF.

Duty calls…

- We use the DMPJRN command to check the security access file:

```
DMPJRN  JRN(WHITEHOUSE/JOURNAL)
        RCVRNG(*CURCHAIN)
        FILE(WHITEHOUSE/SECURITY)
        CVTOUTF(WHITEHOUSE/AUDIT)
```

- We view the results:

```
Select * from AUDIT
```

Surprising results

Jrn Seq #	Ent Type	Date	Time	Job	User	Job#	Program	Object	User	Clearance
13	UB	082412	221809	DEV1	JLYNCH	479286	SEC_CTRL	SECURITY	John Lynch	Minimal
14	UP	082412	221809	DEV1	JLYNCH	479286	SEC_CTRL	SECURITY	John Lynch	Presidential
15	BR	082412	221812	DEV1	JLYNCH	479286	SEC_CTRL	SECURITY	John Lynch	Presidential
16	UR	082412	221812	DEV1	JLYNCH	479286	SEC_CTRL	SECURITY	John Lynch	Minimal
19	UB	082412	221926	DEV1	JLYNCH	479286	QDZTD00001	SECURITY	John Lynch	Minimal
20	UP	082412	221926	DEV1	JLYNCH	479286	QDZTD00001	SECURITY	John Lynch	Presidential

- JLYNCH tried to raise his clearance from Minimal to Presidential using program SEC_CTRL – but this program had safeguards and, using commitment control, issued a rollback.
- The nefarious JLYNCH then used the ultimate weapon… DFU… and raised his clearance to Presidential.

The tools are free!

- Download the zip file containing a save file and instructions from the LISUG web site.
- Open the zip file and follow the instructions in the ReadMe.txt.
- For V5R3M0 and later only.

Thank you!

- Any questions?
- Please send any feedback on the DMPJRN & CVJRNDTA commands to:

Steve Wolk
SWolk@PCRichard.com