Bit Bucket x'32'

Tom Conley, pinncons@rochester.rr.com
Ed Jaffe, edjaffe@phoenixsoftware.com
Mary Anne Matyaz, maryanne4psu@gmail.com
Sam Knutson, Samuel.Knutson@compuware.com
Skip Robinson, Jo.skip.robinson@sce.com

SHARE 125
Session 17229
Orlando, FL
14 Aug 2015

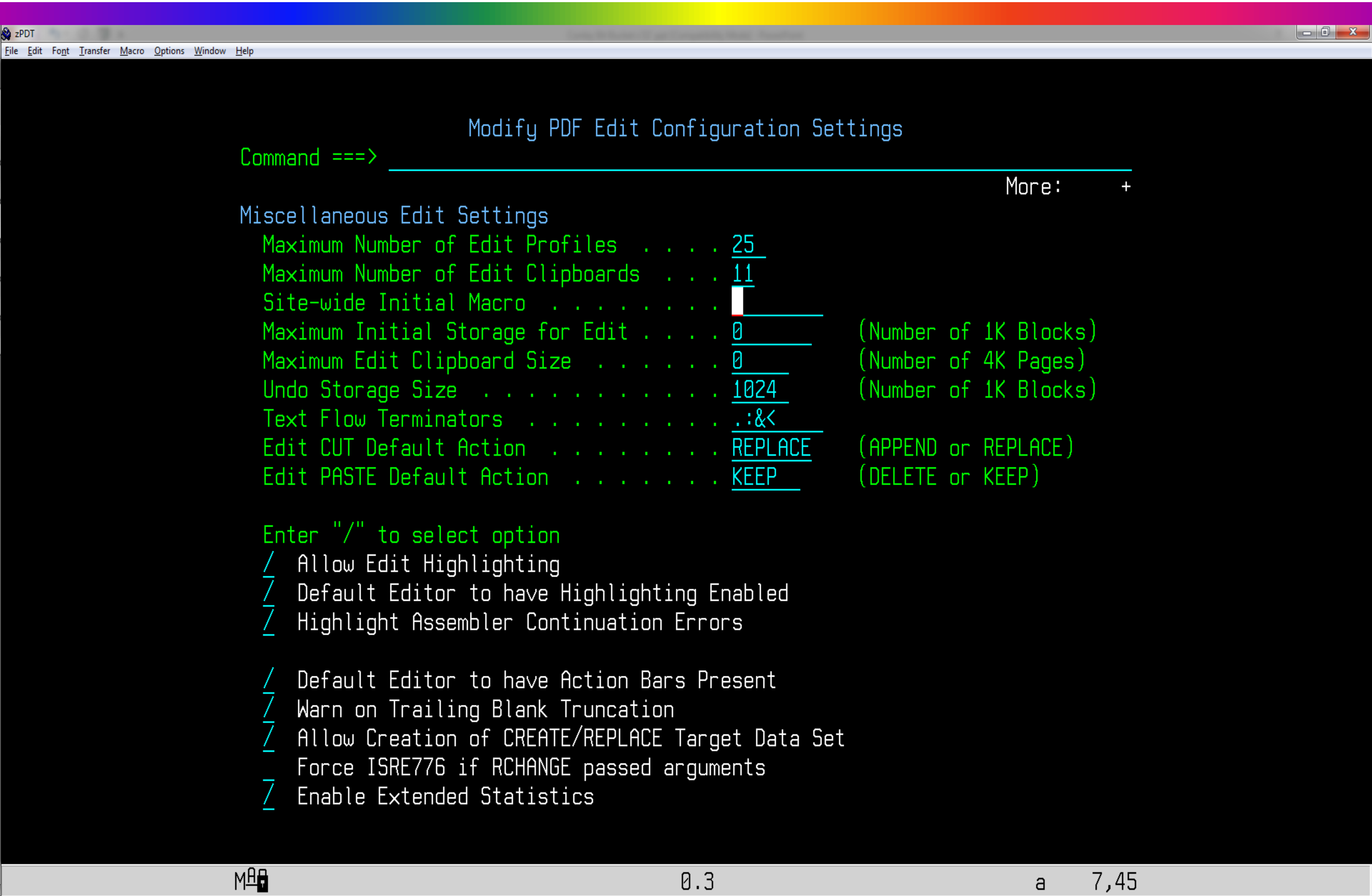
UNDO That Voodoo That You UNDO So Well

(Tom Conley)

UNDO Past a Save?

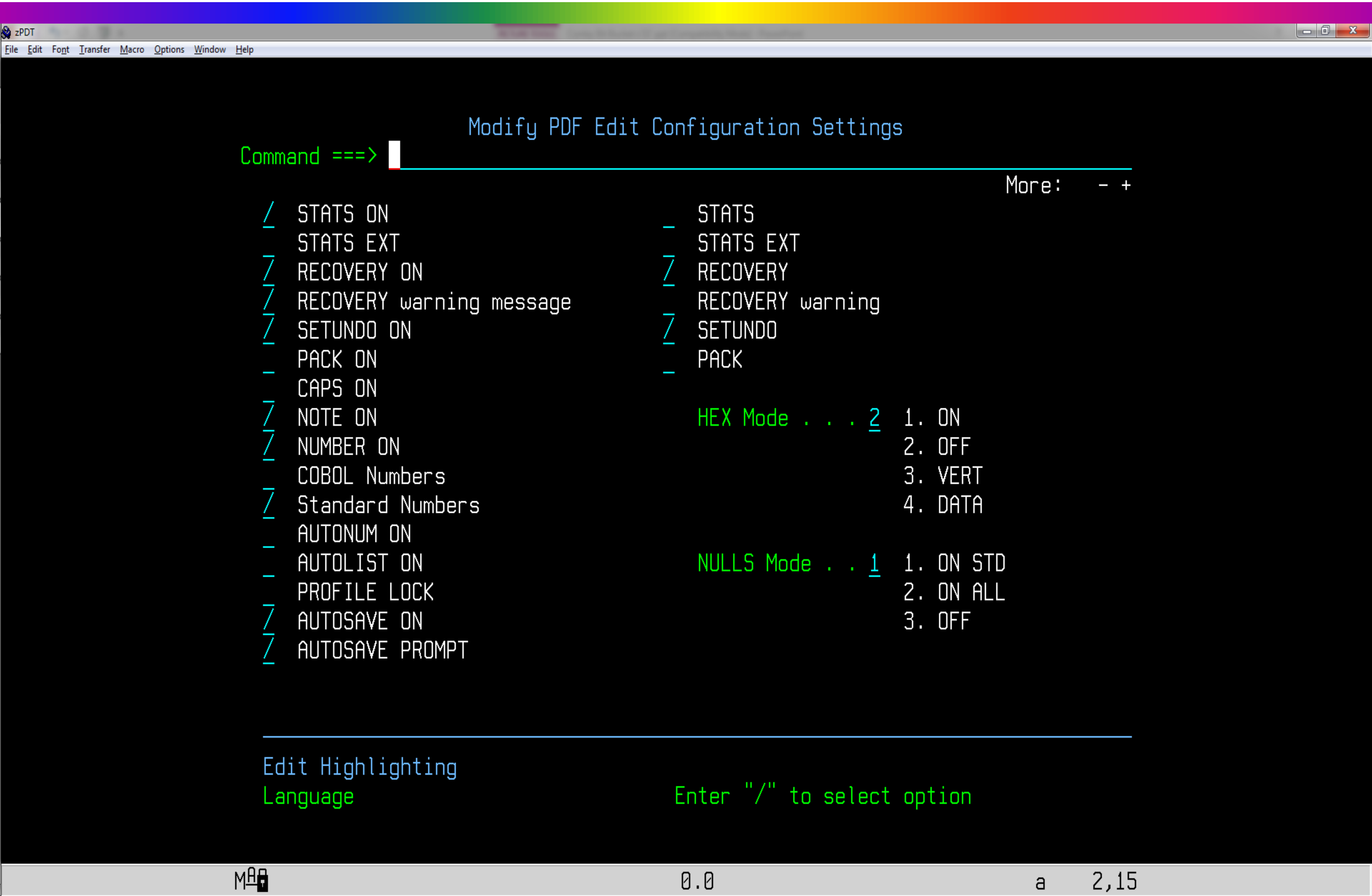
- I got a question about UNDO past a SAVE in ISPF EDIT
- User wanted to go back to an UNDO level before SAVE
- I didn't think it was possible, but I was not exactly right
- SETUNDO KEEP has been around since z/OS V1R9
- It keeps the UNDO buffers even after SAVE
- Allows a user to go back prior to SAVE
- To enable SETUNDO KEEP, run ISPCCONF
- In Editor Settings, set Undo Storage Size to non-zero
- Check SETUNDO on and check FORCE SETUNDO

UNDO Past a Save?



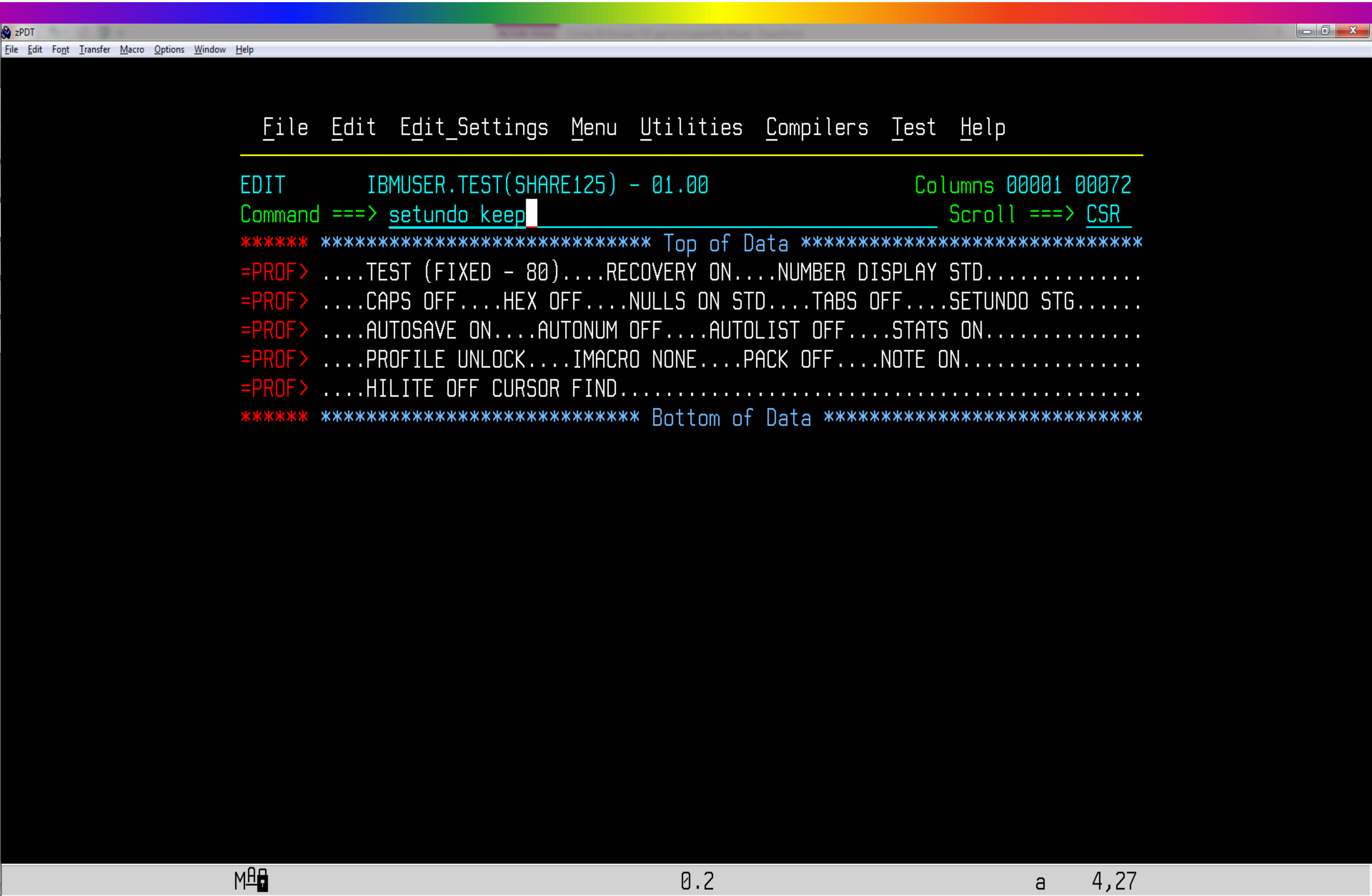
```
                   Modify PDF Edit Configuration Settings
Command ===> ________________________________________________________________
                                                              More:     +
Miscellaneous Edit Settings
  Maximum Number of Edit Profiles . . . . 25
  Maximum Number of Edit Clipboards . . . 11
  Site-wide Initial Macro . . . . . . . .
  Maximum Initial Storage for Edit . . . . 0          (Number of 1K Blocks)
  Maximum Edit Clipboard Size  . . . . . . 0          (Number of 4K Pages)
  Undo Storage Size  . . . . . . . . . . . 1024       (Number of 1K Blocks)
  Text Flow Terminators  . . . . . . . . . .:&<
  Edit CUT Default Action  . . . . . . . . REPLACE    (APPEND or REPLACE)
  Edit PASTE Default Action  . . . . . . . KEEP       (DELETE or KEEP)

  Enter "/" to select option
  /  Allow Edit Highlighting
  /  Default Editor to have Highlighting Enabled
  /  Highlight Assembler Continuation Errors

  /  Default Editor to have Action Bars Present
  /  Warn on Trailing Blank Truncation
  /  Allow Creation of CREATE/REPLACE Target Data Set
     Force ISRE776 if RCHANGE passed arguments
  /  Enable Extended Statistics

MA                          0.3                          a     7,45
```

UNDO Past a Save?



```
                    Modify PDF Edit Configuration Settings
Command ===>
                                                                More:    - +
  / STATS ON                           _ STATS
  _ STATS EXT                          _ STATS EXT
  / RECOVERY ON                        / RECOVERY
  / RECOVERY warning message           _ RECOVERY warning
  / SETUNDO ON                         / SETUNDO
  _ PACK ON                            _ PACK
  _ CAPS ON
  / NOTE ON                              HEX Mode . . . 2  1. ON
  / NUMBER ON                                              2. OFF
  _ COBOL Numbers                                          3. VERT
  / Standard Numbers                                       4. DATA
  _ AUTONUM ON
  _ AUTOLIST ON                          NULLS Mode . . 1  1. ON STD
  _ PROFILE LOCK                                           2. ON ALL
  / AUTOSAVE ON                                            3. OFF
  / AUTOSAVE PROMPT

  Edit Highlighting
  Language                           Enter "/" to select option

MA                                 0.0                          a     2,15
```

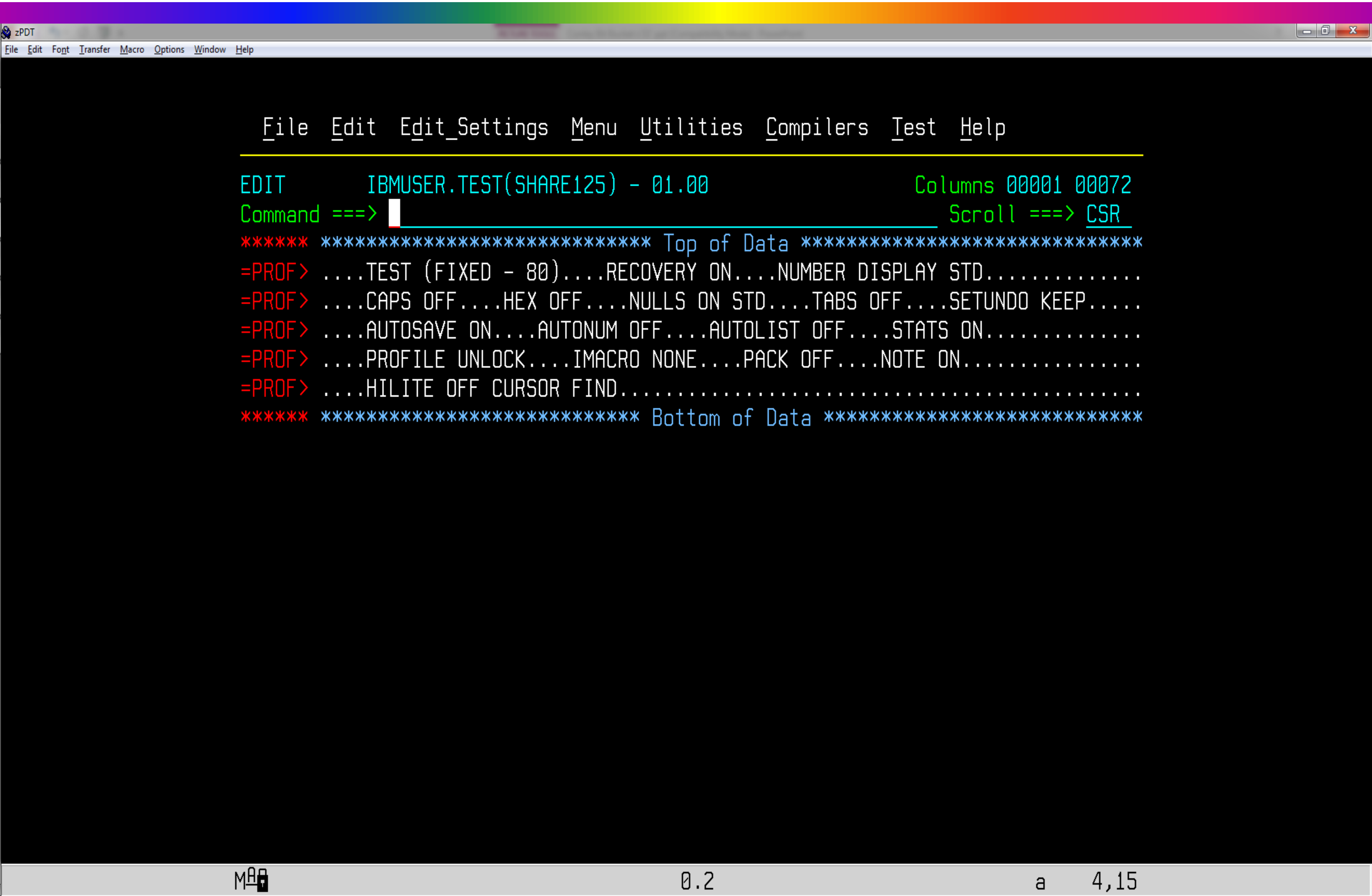
UNDO Past a Save?



```
   File  Edit  Edit_Settings  Menu  Utilities  Compilers  Test  Help
 ───────────────────────────────────────────────────────────────────────────────
EDIT       IBMUSER.TEST(SHARE125) - 01.00                  Columns 00001 00072
Command ===> setundo keep                                     Scroll ===> CSR
****** ***************************** Top of Data ******************************
=PROF> ....TEST (FIXED - 80)....RECOVERY ON....NUMBER DISPLAY STD..............
=PROF> ....CAPS OFF....HEX OFF....NULLS ON STD....TABS OFF....SETUNDO STG......
=PROF> ....AUTOSAVE ON....AUTONUM OFF....AUTOLIST OFF....STATS ON..............
=PROF> ....PROFILE UNLOCK....IMACRO NONE....PACK OFF....NOTE ON................
=PROF> ....HILITE OFF CURSOR FIND..............................................
****** **************************** Bottom of Data ****************************
```

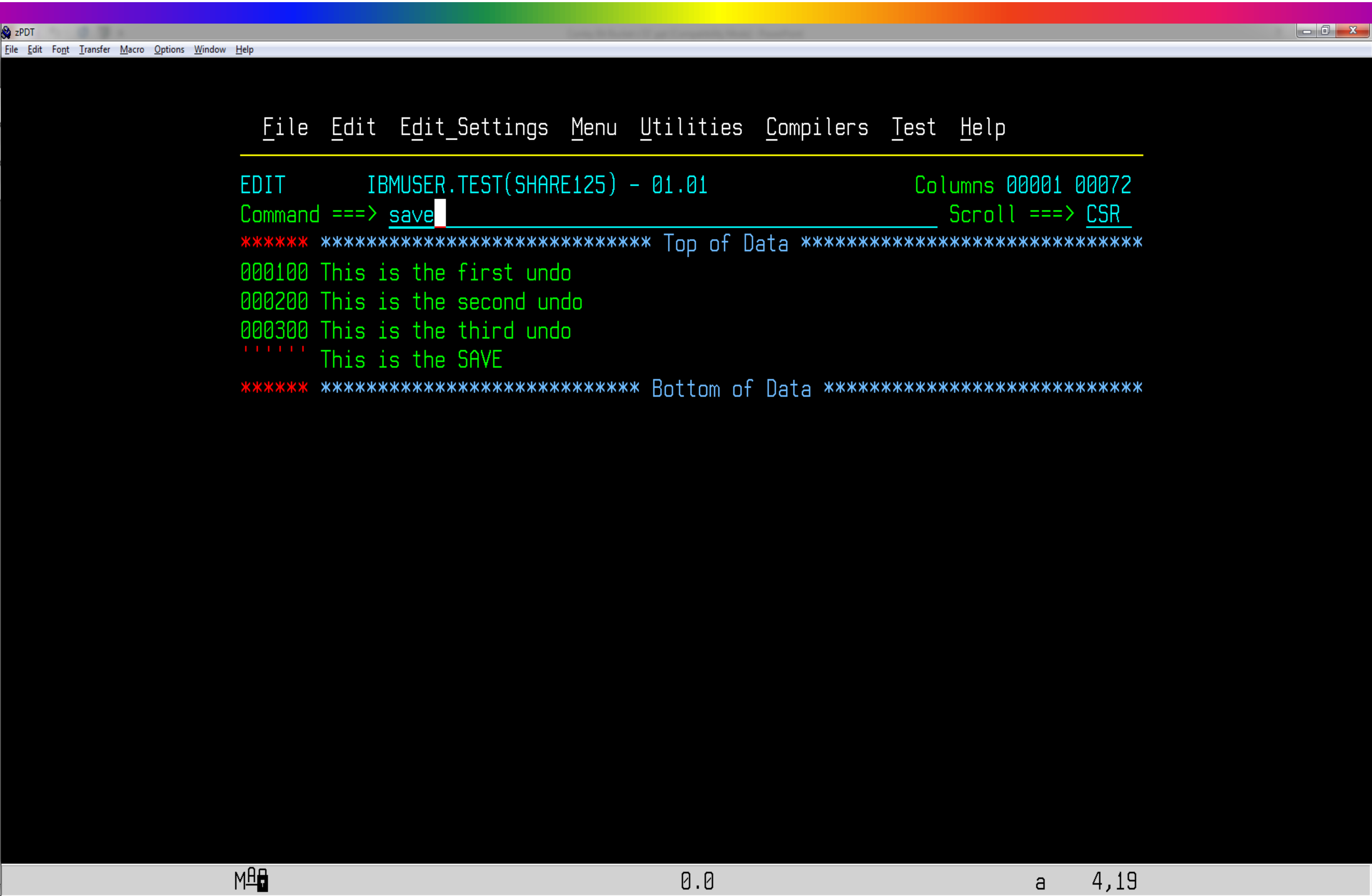
```
MA                           0.2                          a     4,27
```

UNDO Past a Save?



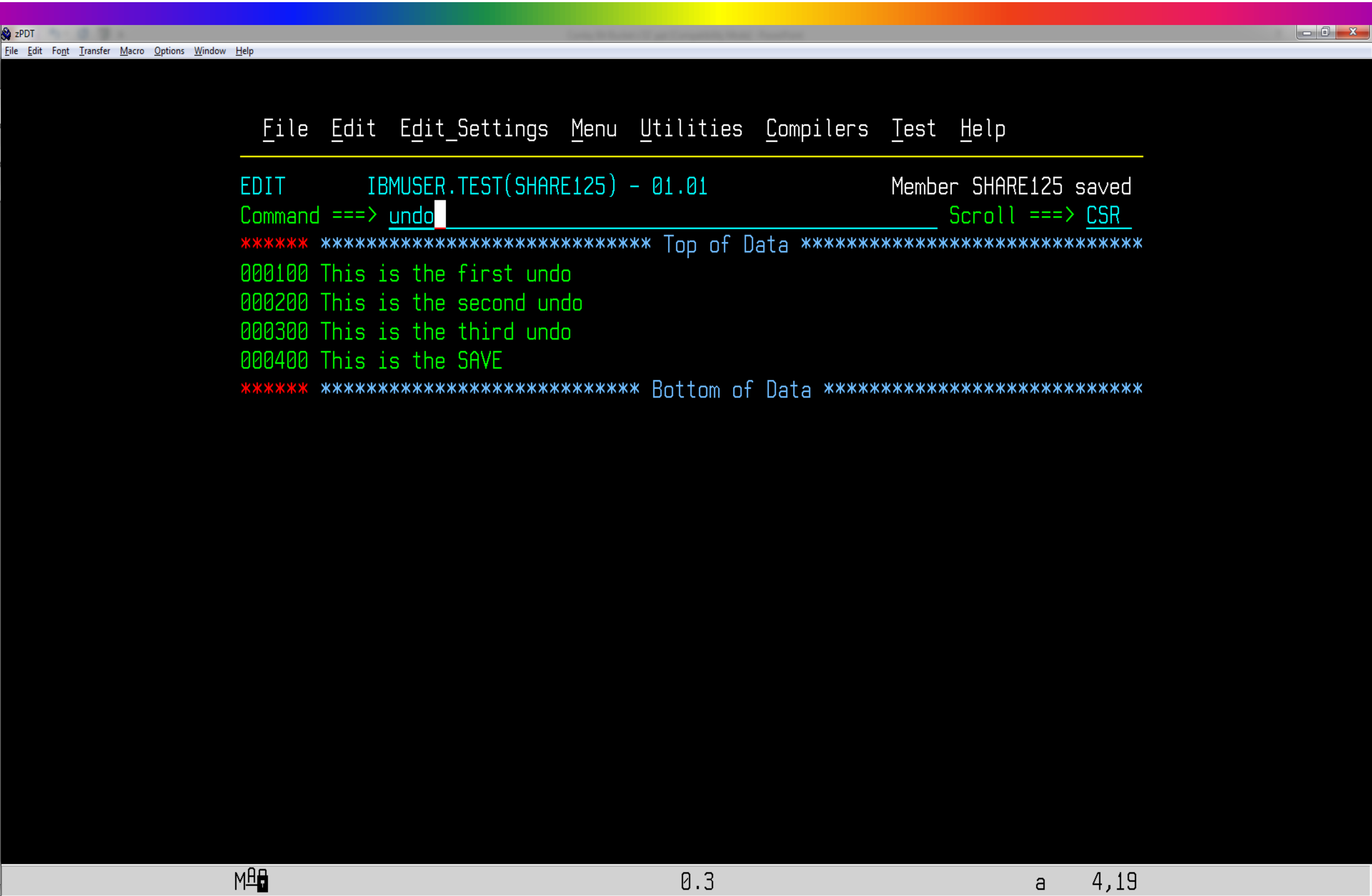
```
  File  Edit  Edit_Settings  Menu  Utilities  Compilers  Test  Help
EDIT       IBMUSER.TEST(SHARE125) - 01.00                  Columns 00001 00072
Command ===>                                                  Scroll ===> CSR
****** ***************************** Top of Data ******************************
=PROF> ....TEST (FIXED - 80)....RECOVERY ON....NUMBER DISPLAY STD.............
=PROF> ....CAPS OFF....HEX OFF....NULLS ON STD....TABS OFF....SETUNDO KEEP.....
=PROF> ....AUTOSAVE ON....AUTONUM OFF....AUTOLIST OFF....STATS ON.............
=PROF> ....PROFILE UNLOCK....IMACRO NONE....PACK OFF....NOTE ON...............
=PROF> ....HILITE OFF CURSOR FIND.............................................
****** **************************** Bottom of Data ****************************
```

UNDO Past a Save?



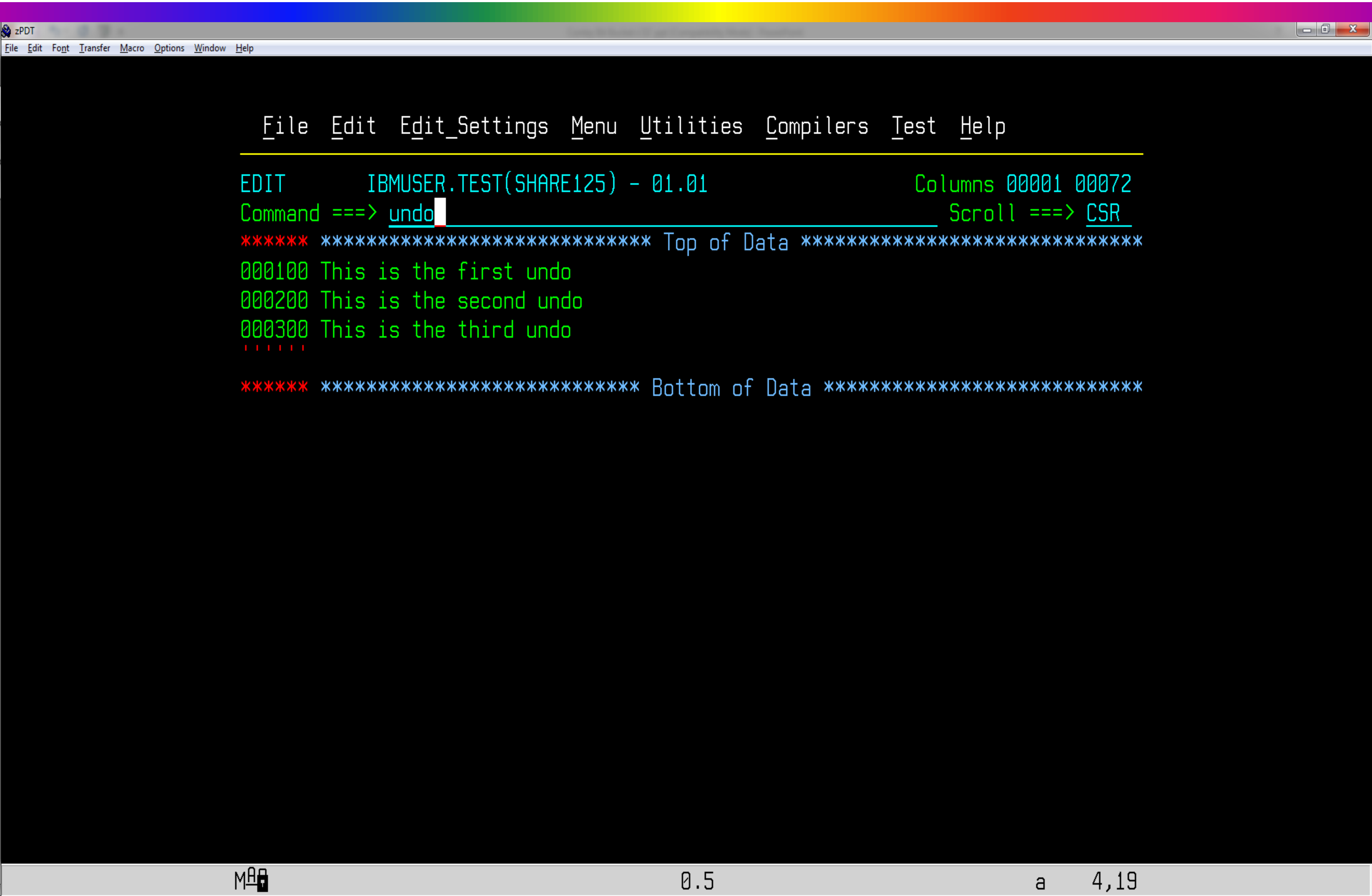
```
 File  Edit  Edit_Settings  Menu  Utilities  Compilers  Test  Help
───────────────────────────────────────────────────────────────────────────────
EDIT       IBMUSER.TEST(SHARE125) - 01.01                 Columns 00001 00072
Command ===> save                                            Scroll ===> CSR
****** ***************************** Top of Data ******************************
000100 This is the first undo
000200 This is the second undo
000300 This is the third undo
''''''' This is the SAVE
****** **************************** Bottom of Data ****************************
```

UNDO Past a Save?



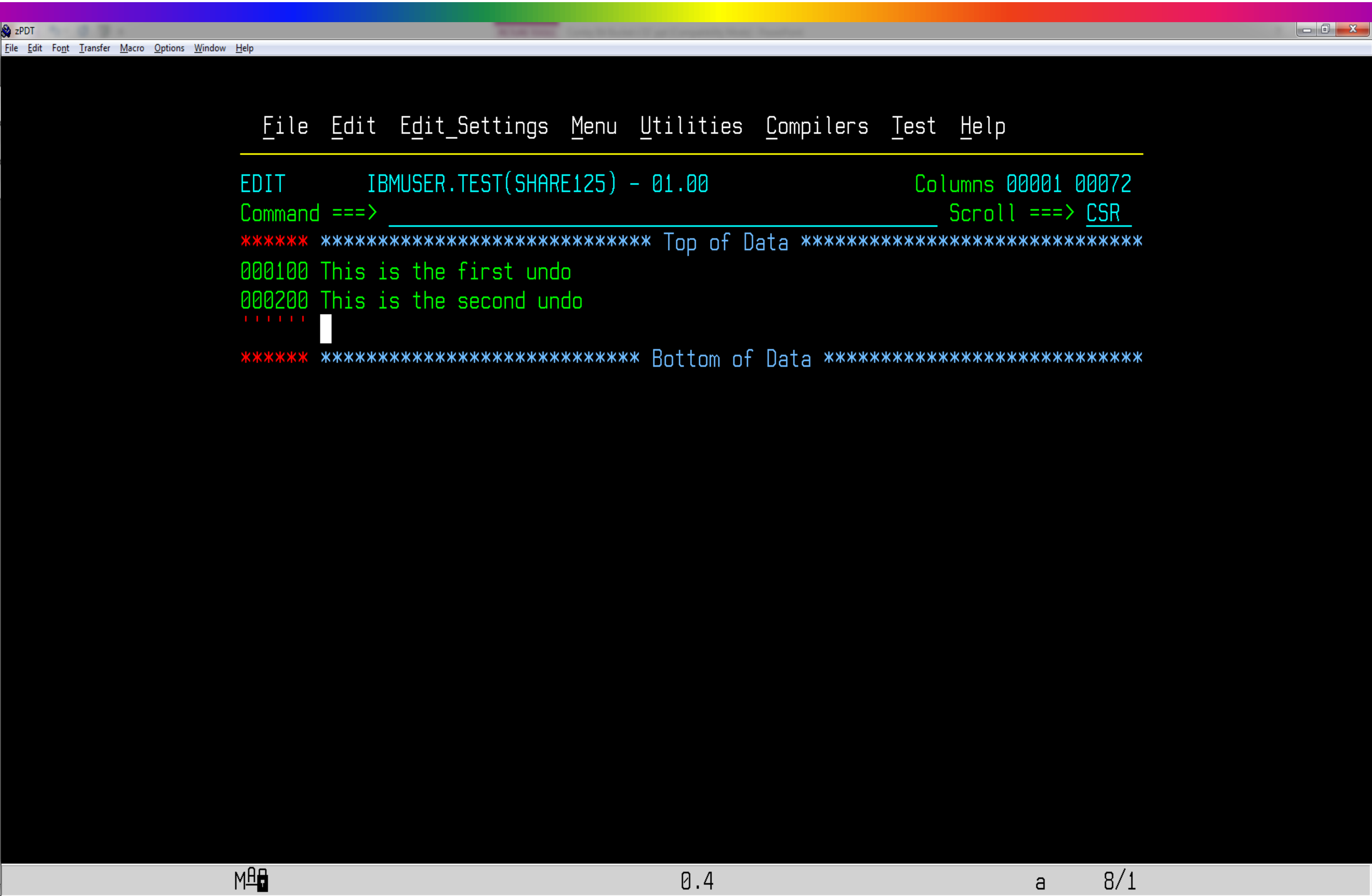
```
 File  Edit  Edit_Settings  Menu  Utilities  Compilers  Test  Help

EDIT       IBMUSER.TEST(SHARE125) - 01.01              Member SHARE125 saved
Command ===> undo                                              Scroll ===> CSR
****** ***************************** Top of Data ******************************
000100 This is the first undo
000200 This is the second undo
000300 This is the third undo
000400 This is the SAVE
****** **************************** Bottom of Data ****************************
```

UNDO Past a Save?



```
  File  Edit  Edit_Settings  Menu  Utilities  Compilers  Test  Help
 ───────────────────────────────────────────────────────────────────────────────
EDIT       IBMUSER.TEST(SHARE125) - 01.01                  Columns 00001 00072
Command ===> undo                                             Scroll ===> CSR
****** ***************************** Top of Data ******************************
000100 This is the first undo
000200 This is the second undo
000300 This is the third undo
''''''
****** **************************** Bottom of Data ****************************
```

UNDO Past a Save?



```
  File  Edit  Edit_Settings  Menu  Utilities  Compilers  Test  Help
EDIT       IBMUSER.TEST(SHARE125) - 01.00                Columns 00001 00072
Command ===>                                                Scroll ===> CSR
****** ***************************** Top of Data ******************************
000100 This is the first undo
000200 This is the second undo
''''''
****** **************************** Bottom of Data ****************************
```

My Back Page Datasets

(Tom Conley)

Page Datasets - ROTs

- Question keeps coming up on IBM-Main
- Is it OK if my page datasets are above 30%?
- NO, NO, a thousand times NO!!!
- There is a perception that the 30% threshold is “old” ROT
- Nothing could be further from the truth
- Above 30%, block paging algorithm is significantly inhibited
- So stop already with the “It’s OK above 30%”
- If you don’t believe me, believe Cheryl Watson
- If you have a page dataset above 30%, fix it
- Review page dataset allocations for addition or resizing
- Recommend 2-3X real memory on LPAR
- Allocate all page datasets with the same size
- Prevents smaller page datasets from hitting 30%
- ASM ignores page dataset size when allocating pages

Are You Free Tonight?

(Ed Jaffe)

New Function APAR OA46291

- John Shebey tangentially mentioned this new function APAR in the MVS Core Technologies Project Opening
- Its implementation caused the high half of R15 to be non-zero after a successful COND=YES STORAGE OBTAIN call under z/OS 2.1.
- THIS IS PERFECTLY LEGAL and yet many software products had failures as a result because they were looking at all 64 bits of R15 rather than just the low half.
    - This happened to us. A programmer erroneously did LTGR 15,15 after a conditional STORAGE OBTAIN. We corrected the problem by changing it to LTGFR 15,15
- The PTF (UA90976) was marked PE and new APAR OA48273 was opened to clear the high half of R15.
- This will give you some time to take a good hard look at new function APAR OA46291

New Function APAR OA46291

- Intended to reduce the number of IPTE instructions issued on z13 hardware.
- This instruction invalidates the virtual to real association when a page of storage is released.
- Because it must signal every processor in the configuration, IPTE can run slow on z13 with lots of CPUs
- Now when a page of storage is released by FREEMAIN or STORAGE RELEASE, it might not actually be freed in the traditional sense i.e., the storage will continue to be backed by real frames even while “free.”
- This design change has some interesting side effects.
  - Reference to the “freed” page will not cause abend0C4
  - TPROT will no longer generate CC=3 for the “freed” page
  - Configuring storage offline while storage constrained might fail if many freemained frames exist.

New Function APAR OA46291

- Specify FREEMAINEDFRAMES(NO) in DIAGxx to disable the feature system-wide.
- You also have FREEMAINEDFRAMES(YES) with EXCLUDEJOBLIST(job1,job2...job8) to specify up to eight job name masks (with wildcard characters) describing the jobs that should not get this treatment.
- New callable services IARBRVER and IARBRVEA have been added to allow you to verify primary and ALET-qualified virtual storage addresses respectively.
  - You pass the address to be tested in R1
  - You get back a return code in R15
    - 00 = write access and not backed by a freemained frame
    - 01 = read access and not backed by a freemained frame
    - 02 = no access and not backed by a freemained frame
    - 04 = page can't be translated or is backed by freemained frame
- This PDF contains the full list of documentation updates for this new function http://publibz.boulder.ibm.com/zoslib/pdf/OA46291.pdf

Forewarned is Forearmed

(Ed Jaffe)

SHARE Requirements for NJE Over TCP/IP

- SSJES3032647
  - August 2002
  - 3.9 score
- SSJES2038885
  - March 2003
  - 3.6 score
- At that time, VSE POWER and VM RSCS already had the support for several releases.
- JES NJE over TCP/IP delivered in 2006 and 2007
- Quickly became the de Facto connection for NJE
- Very few pure SNA/NJE sites left
  - Some use Enterprise Extender and similar technologies

Recommended JES Security APARs

- Affects customers using NJE over TCP/IP
  - 2015/07/23 OA48306 Security APAR (JES Common)
  - 2015/07/24 OA48307 Security APAR (JES2)
  - 2015/07/24 OA48349 Security APAR (JES3)
- New configuration option for NETSERVs
  - `NETSERV SECURE=REQUIRED|OPTIONAL`
- Can limit NETSERV to allow only AT-TLS connections
- JES3 default is OPTIONAL
- JES2 defines an additional option USE_SOCKET as its default, which derives NETSERV setting from SOCKET setting (SECURE=YES|NO).
- Affects both inbound and outbound NJE connections

Restart Information for JES2

```
RESTART:
  *****************************************************************
  * FUNCTION AFFECTED: JES2/JES3                        (OA48306) *
  *                      Networking                               *
  *                        TCP/IP NJE                             *
  *****************************************************************
  * DESCRIPTION      : RESTART                                    *
  *****************************************************************
  * TIMING           : Post-APPLY                                 *
  *****************************************************************
  To activate the code without an IPL do the following:
  1. Apply the fix
  2. Stop all active NETSRV (NETSERV) address spaces
  3. If the NETSRV (NETSERV) code is in the link list
     concatenation, then issue a MODIFY LLA,REFRESH
     and wait for it to complete (CSV210I message)
  4. Restart all NETSRV (NETSERV) address spaces that
     were previously stopped in step 2


IPL:
  *****************************************************************
  * FUNCTION AFFECTED: 5752SC1BH                        (OA48307) *
  *                      JES2                                     *
  *****************************************************************
  * DESCRIPTION      : IPL with CLPA                              *
  *****************************************************************
  * TIMING           : Post-APPLY                                 *
  *****************************************************************

  In order for this PTF to be fully effective, an IPL with CLPA
  is required.
```

Restart Information for JES3

```
RESTART:
  ****************************************************************
  * FUNCTION AFFECTED: JES2/JES3                       (OA48306) *
  *                      Networking                              *
  *                        TCP/IP NJE                            *
  ****************************************************************
  * DESCRIPTION      : RESTART                                   *
  ****************************************************************
  * TIMING           : Post-APPLY                                *
  ****************************************************************
  To activate the code without an IPL do the following:
  1. Apply the fix
  2. Stop all active NETSRV (NETSERV) address spaces
  3. If the NETSRV (NETSERV) code is in the link list
     concatenation, then issue a MODIFY LLA,REFRESH
     and wait for it to complete (CSV210I message)
  4. Restart all NETSRV (NETSERV) address spaces that
     were previously stopped in step 2


RESTART:
  ****************************************************************
  * FUNCTION AFFECTED: JES3                            (OA48349) *
  ****************************************************************
  * DESCRIPTION      : RESTART                                   *
  ****************************************************************
  * TIMING           : Post-APPLY                                *
  ****************************************************************
  Installation On (Global,Netserv)
               Order (Any)
  Activation   Order (Any)
               Type/JES3 restart (Hot,Netserv)
               Type/IPL (None)
               CLPA (No)
  (See Apar II07968 for definitions)
```

z/OS Network Job Entry Security Best Practices

- Published August 3rd, 2015
- http://public.dhe.ibm.com/common/ssi/ecm/zs/en/zsw03287usen/ZSW03287USEN.PDF
- Abstract:
  - Most installations have moved from BSC and SNA for NJE to TCP/IP, however the impact of this switch on security may have been overlooked. SNA and BSC are essentially a closed network whereas TCP/IP is an open network. The impact of this openness on concepts such as NJE node authentication and securing trusted nodes (nodes that can submit jobs without passwords) may not have been considered.
  - This document talks about best practices for helping secure an NJE network and managing the risk of trusted nodes, particularly when NJE is implemented over a TCP/IP network.

General JES Security Best Practices

- NJE networks should be secure
  - Consider who can access your NJE connection
  - Could some windows computer on your network access your mainframe?
  - If so, it there a password and AT-TLS profile?
- What about your data sets on SPOOL?
  - JESSPOOL class protects data sets on SPOOL
  - Analogous to DATASET class
  - If JESSPOOL is not active, your data sets on SPOOL are not protected

TPG APARs

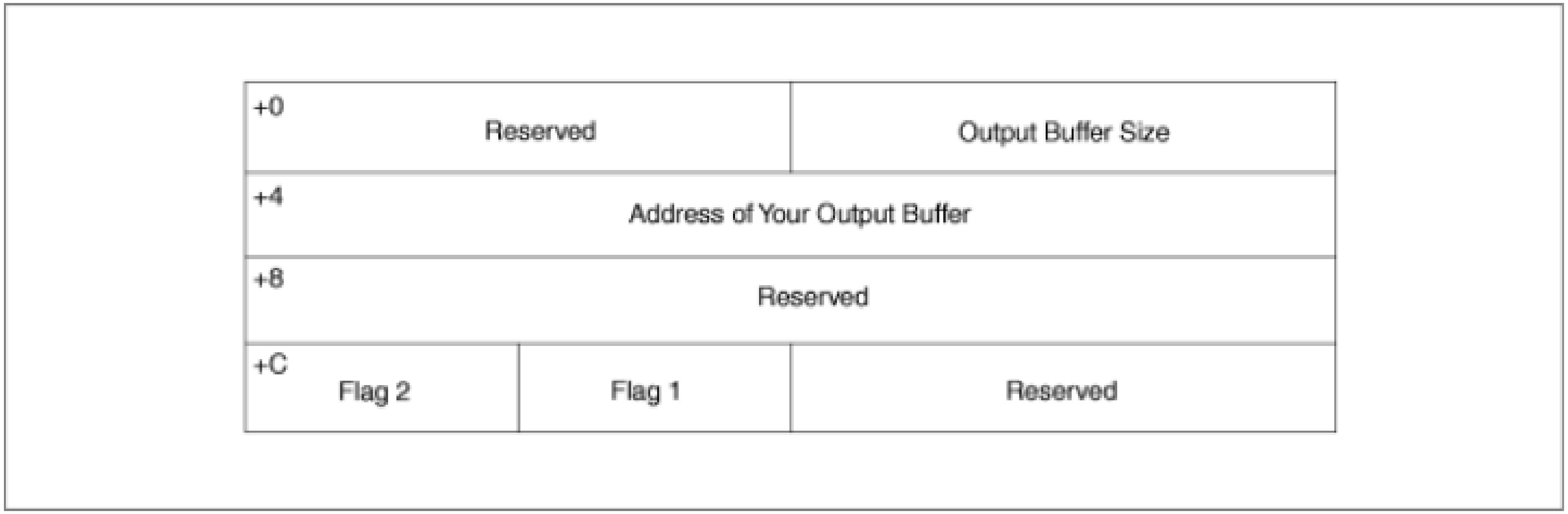
- TPG is the TSO/E fullscreen PUTGET service
- After OA46359 our products started receiving abend0C4 inside IKTVTPUT as it attempted to write on top of the TPG service parameter list in storage
- We assumed writing to the TPG parm list was something new and did research in an effort to understand how to avoid it.

```
ASID(X'007B') ADDRESS(DB9210.) KEY(00)
00DB9210 | 1744                | XR       R4,R4
00DB9212 | 9640 D018           | OI       X'18'(R13),X'40'
00DB9216 | BF47 5069           | ICM      R4,X'7',X'69'(R5)
00DB921A | 1711                | XR       R1,R1
00DB921C | 4310 401C           | IC       R1,X'1C'(,R4)
00DB9220 | 1700                | XR       R0,R0
00DB9222 | 41E0 600C           | LA       R14,X'C'(,R6)
00DB9226 | 41F0 D018           | LA       R15,X'18'(,R13)
00DB922A | E50F E000 F000 | MVCDK    X'0'(R14),X'0'(R15)
```

Relevant TPG Interface Descriptions

For TPG with the parameter list, register 0 is supplied with the output buffer number. It also sets the indicator of the output buffer number that is present in register 0 of the parameter list. The output buffer number is 0 through 65535. When it reaches 65535, it is reset to zero.

Figure 2. Parameter List Expansion for the List Form of TPG



+0	Reserved		Output Buffer Size
+4	Address of Your Output Buffer		
+8	Reserved		
+C	Flag 2	Flag 1	Reserved

For Figure 2, the possible settings of Flag1 are shown in Table 1. Flag2 is X'01' for the NOEDIT option and X'02' for the TPG macro.

The value of Flag2 in the parameter list upon return from TPUT SVC is X'40'. This indicates that register 0 is supplied with the output buffer number.

APAR OA46359 Can't be Viewed

- Experience indicates this usually implies a security APAR rather than a bug in IBMLink
- I have absolutely no knowledge whatsoever of what the exposure was and don't want anyone to tell me.
  - Not knowing for sure gives me the freedom to "speculate"
- My "educated" guess is that TPG was turning on the x'40' bit in flag 2 while running in key zero (or similar) and that created an exposure.
- Furthermore, the APAR attempted to correct that problem by ensuring the TPG parameter list was always in the TCBPKF key.
- Not a workable solution for privileged code
  - Good citizens are using PSW key 0-7 storage
  - Forcing privileged code to place the TPG parm list in normal user key storage introduces a *new* exposure.
  - It would have been much better to use the key of caller instead of TCBPKF

APAR OA44798 is NOT a Secret

- The folks at IBM's z Systems Center for Secure Engineering agreed with my assessment of the *new* exposure as well as my suggested solution.
- I let the people handling my SR know this and a short while later APAR OA47798 was opened.

```
PROBLEM SUMMARY:
  ****************************************************************
  * USERS AFFECTED:                                              *
  * All TSO users.                                               *
  ****************************************************************
  * PROBLEM DESCRIPTION:                                         *
  * ABEND0C4 in IKTVTPUT.                                        *
  ****************************************************************
  * RECOMMENDATION:                                              *
  * Apply the provided PTF.                                      *
  ****************************************************************
  This problem may be described as follows:
     1. Application task was running in key 8.
         But the program changed the psw key to 1.
         It issued TPG to send the data to the terminal.
     2. IKTVTPUT received control to process the TPG.
         It tried to update the user storage using key 8
         from TCB. But user program was running in
         key 1 and its storage was also in key 1. This
         caused the abend0c4 in iktvtput.

  PROBLEM CONCLUSION:
  IKTVTPUT has been changed to use the user key
  from the RB to access the user storage.
```

TPG Final Recommendation

- It's probably a good idea to update TPG on your systems (apply OA46359) to mitigate the original exposure whatever it was – whether it be my "educated" guess or something else entirely.
- Apply OA47798 to avoid disruptions caused by the original solution.

Who Moved my Datacenter?

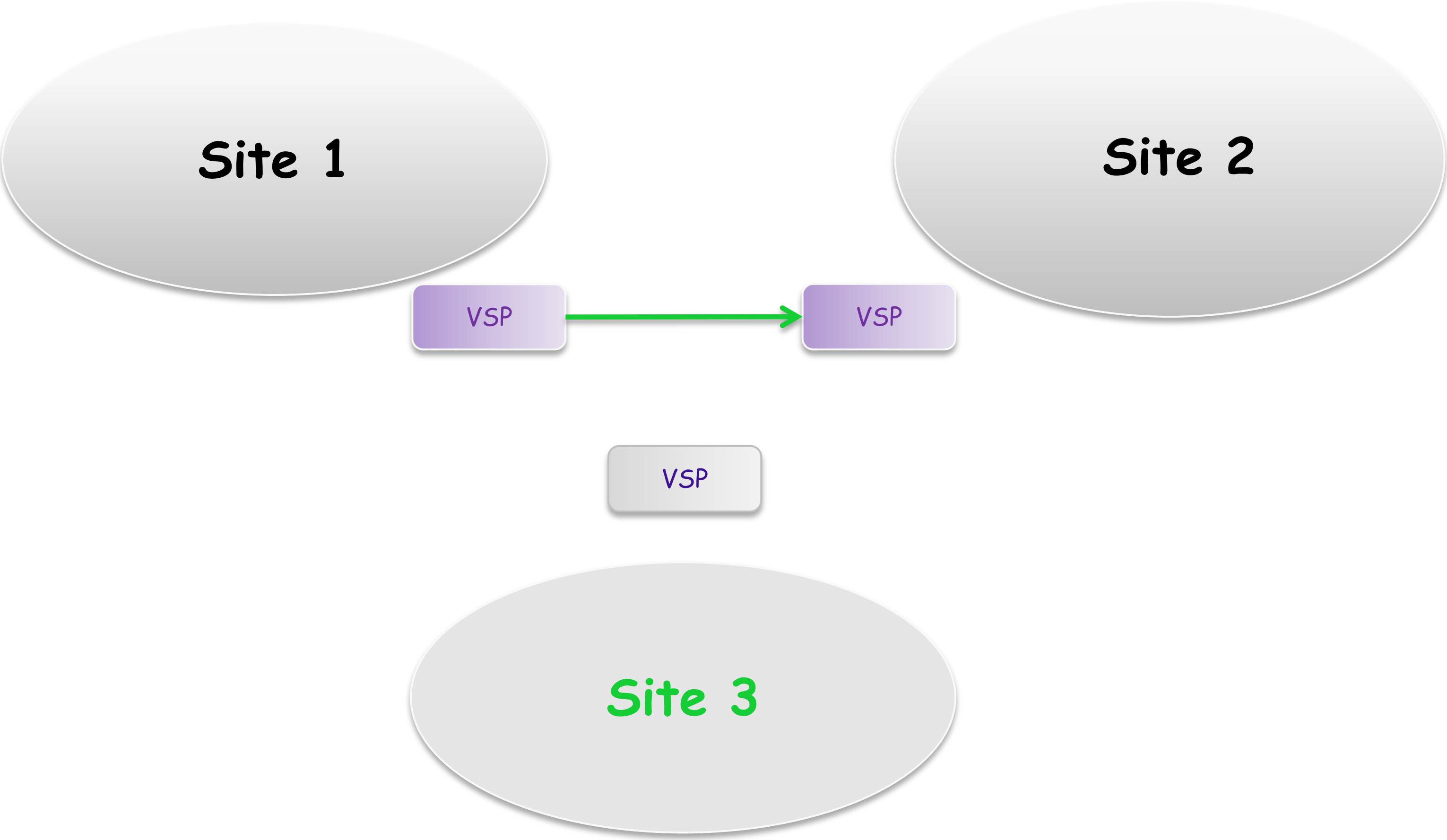
(Mary Anne Matyaz)

The Hardware

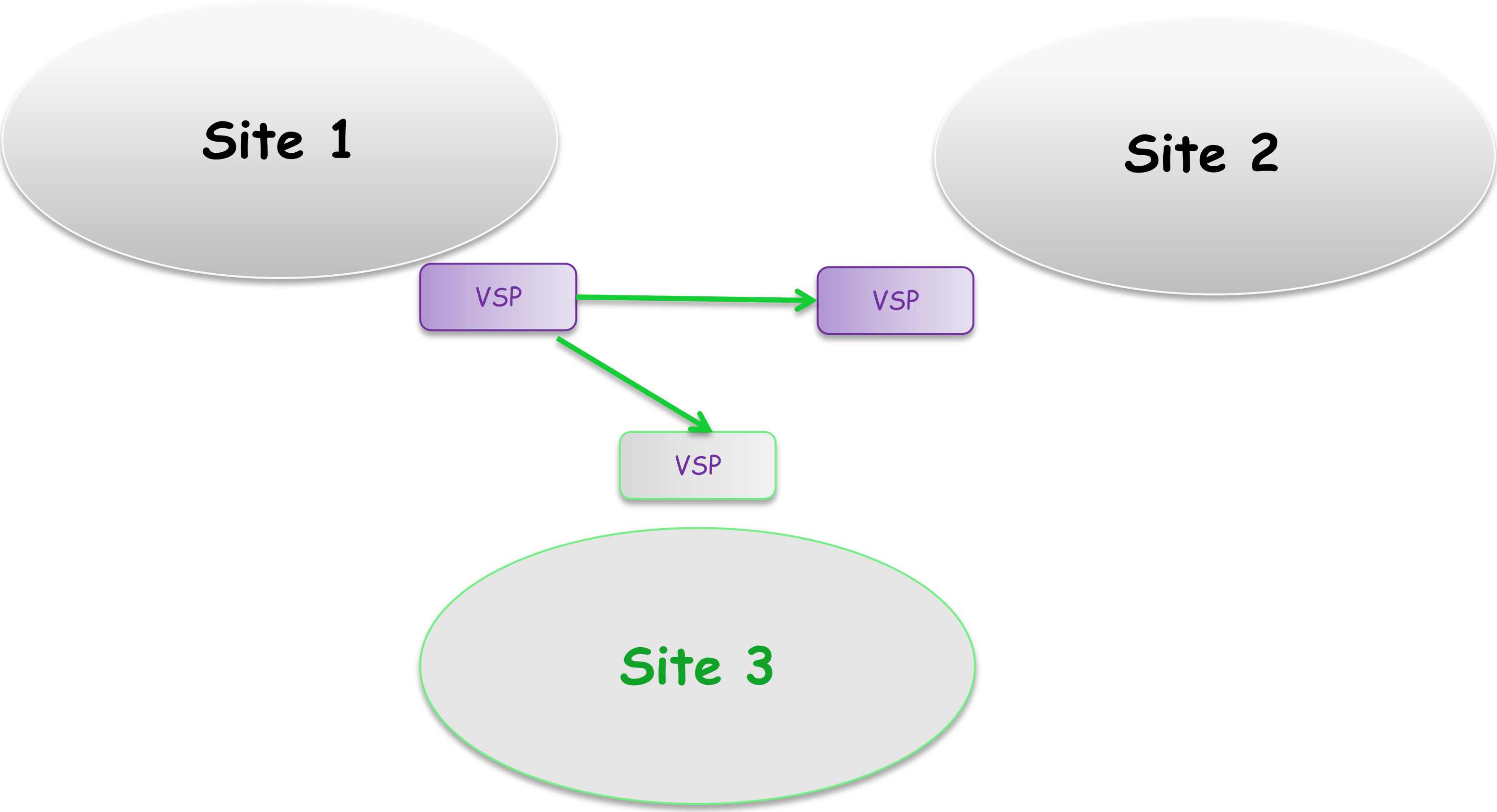
- Two z10's at Site 1
- One z196 at Site 2
- One EC12 at Site 3

- Site 2 LPARs are migrating to Site 3, then Site 2 will be shut down
- Site 1 is D/R for Site 2, and will be D/R for Site 3
- Site 2 is D/R for Site 1; Site 3 will take over this responsibility
- Hitach VSP DASD at all three sites
- IBM 7720 VTL at all three sites

The Vision



The Vision



Trust Your Highly-paid Consultant

- MGR: “How long will the outage be?”
- Me: “Six Hours.”
- MGR: “What do you base that on?”
- Me: “25 years of experience.”
- MGR: “I think it’ll be two.”
- Me: “Ok.”

- How long was it?

- Should you be a hero or a loser?

The Cutover

- Timeline planning indicated 6 hours. Commit time 9:30AM
- Outage ended up being…. 5.5 Hours, Available at 8:50
- Steps:
  - Verify LOADxx and CONSOLxx settings
    - *SQA, OSA Changes*
  - Shutdown test apps and lpars in Site 2
  - Shutdown prod apps and lpars in Site 2
  - Quiesce replication from Site 1→ Site 2 and Site 2→3
  - Bring up a one pack system at Site 2 to run the split job
  - Build HUR environment, specify PAIR CREATE, COPY=NONE
  - IPL Production lpars
  - IPL the test lpars

The Cutover - Continued

- Network time
  - Remove Natting
  - Begin advertising new routes
- IPL Production
  - Why not test?
- Initial verification focused on network:
  - Check for the absence of natting
  - NJE Connectivity (Several different sites)
  - EE Pipes
  - CA ENF
  - Connect Direct

The Cutover - Continued

- Turn system over to application owners for testing
- Make Go/NoGo decision prior to FDR backups
  - (We flash, then backup from the flashed copies)
- Continue to observe and fight fires

- There weren't any. Really.

Hindsight

- How long will the outage be?
- TESTing plans are essential and a huge time saver
  - Jobs and before/after output in a separate PDS
- Before/After displays (TSO DISP NETSTAT CONN) or run an IKJEFT01 with a bunch of displays
  - I use TSO DISP a lot!
- Lots of copies of before/after syslogs
- On the bridge call and webex, we found that webex is blocked from midnight to 6AM. (??)

What We Learned

- Increased our number of generations for syslog
- Better IPL and Shutdown doc
  - Moved operations which involved all new operators
- Run batch jobs with output of commands (netstat,iplinfo)
  - I use TSO DISP a lot!
- Better doc for recovering consoles etc. after network 'hiccups'.
- 30 days of tapes

DISP

BONUS!

- I guess you could call this shareware, but the only place I could find it was on the IBMMain listserv. You add DISP in front of any command and it puts the output of the command in a dataset for you to peruse. Great for netstat and help commands, and any command with large output where you may want to scroll forward and backward.

  TSO DISP NETSTAT CONN

  http://newsgroups.derkeiler.com/Archive/Comp/bit.listserv.ibm-main/2006-05/msg01735.html

- Mark Zelden's at http://mzelden.com/mvsfiles/tsob.txt

  Or Lionel Dyck's variation at http://www.tsotimes.com/quicktips/su95qt1.html

- and yet another version at http://www.jmit.com/os390/systools/rexx/FULL.txt

Immense but not Indefinite Integrity

(Sam Knutson)

IBM's Statement of Integrity

- IBM z/OS System Integrity Statement was first issued in 1973, IBM's MVS™ System Integrity Statement, and subsequent statements for OS/390® and z/OS, has stood for over three decades as a symbol of IBM's confidence in and commitment to the z/OS operating system.
- It has recently changed to highlight which releases IBM will fix and some that they won't
- http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=ZSL03361USEN&attachment=ZSL03361USEN.PDF
- Or Google ZSL03361USEN
- Integrity discussed in Bit Bucket x'2C' in San Francisco and many times before and after in great SHARE presentations

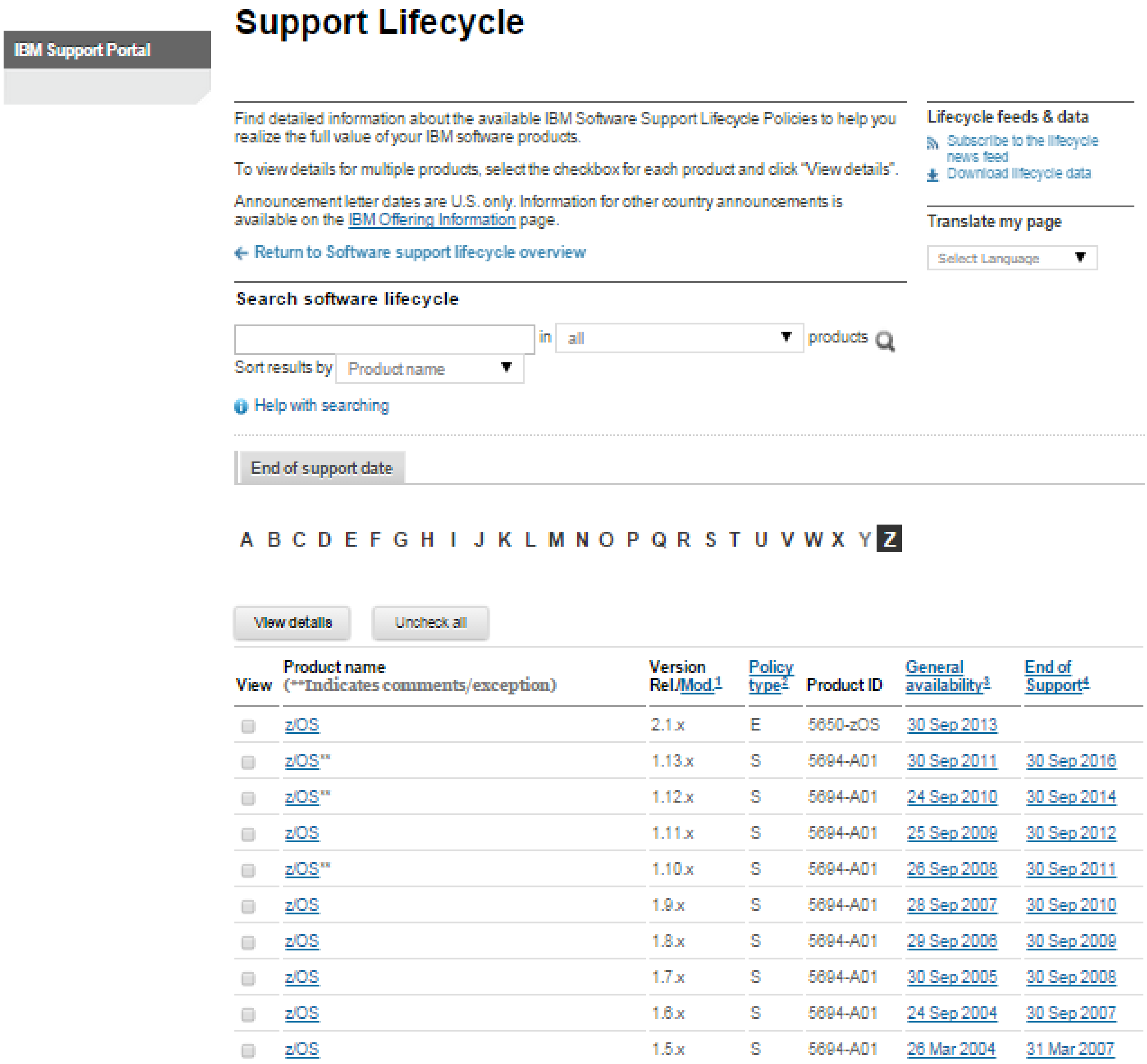
IBM's Statement of Integrity

IBM's commitment includes design and development practices intended to prevent unauthorized application programs, subsystems, and users from bypassing z/OS security – that is, to prevent them from gaining access, circumventing, disabling, altering, or obtaining control of key z/OS system processes and resources unless allowed by the installation. Specifically, z/OS "System Integrity" is defined as the inability of any program not authorized by a mechanism under the installation's control to circumvent or disable store or fetch protection, access a resource protected by the z/OS Security Server (RACF®), or obtain control in an authorized state; that is, in supervisor state, with a protection key less than eight (8), or Authorized Program Facility (APF) authorized. In the event that an IBM System Integrity problem is reported to IBM, IBM will always take action to resolve it in the specified operating environment for releases that have not reached their announced End of Support (1) dates.

IBM's Statement of Integrity

- Notes:
- 1. End of Support dates are the last dates on which IBM will deliver standard support services for a given version or release of a product. Information about end of support dates is available at http://www.ibm.com/software/support/lifecycle/index_z.html
- 2. IBM reserves the right to change, modify or withdraw its offerings, policies and practices at any time. All products and support obligations are subject to the terms of the applicable license and services agreements.

IBM Support Lifecycle



Support Lifecycle

Find detailed information about the available IBM Software Support Lifecycle Policies to help you realize the full value of your IBM software products.

To view details for multiple products, select the checkbox for each product and click "View details".

Announcement letter dates are U.S. only. Information for other country announcements is available on the IBM Offering Information page.

← Return to Software support lifecycle overview

Lifecycle feeds & data

Subscribe to the lifecycle news feed

Download lifecycle data

Translate my page

Select Language ▼

Search software lifecycle

in all ▼ products

Sort results by Product name ▼

Help with searching

End of support date

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

View	Product name (**Indicates comments/exception)	Version Rel./Mod.[1]	Policy type[2]	Product ID	General availability[3]	End of Support[4]
□	z/OS	2.1.x	E	5650-zOS	30 Sep 2013	
□	z/OS**	1.13.x	S	5694-A01	30 Sep 2011	30 Sep 2016
□	z/OS**	1.12.x	S	5694-A01	24 Sep 2010	30 Sep 2014
□	z/OS	1.11.x	S	5694-A01	25 Sep 2009	30 Sep 2012
□	z/OS**	1.10.x	S	5694-A01	26 Sep 2008	30 Sep 2011
□	z/OS	1.9.x	S	5694-A01	28 Sep 2007	30 Sep 2010
□	z/OS	1.8.x	S	5694-A01	29 Sep 2006	30 Sep 2009
□	z/OS	1.7.x	S	5694-A01	30 Sep 2005	30 Sep 2008
□	z/OS	1.6.x	S	5694-A01	24 Sep 2004	30 Sep 2007
□	z/OS	1.5.x	S	5694-A01	26 Mar 2004	31 Mar 2007

IBM z Systems Security Portal

- Integrity APARs are not new as evidenced by the age of the Statement of Integrity
- IBM provides a means with the Security Portal for you as a customer to stay informed
- The Security Portal also provide you the CVSS (v2) score for a defect
- Common Vulnerability Scoring System (CVSS) provides an open framework for communicating the characteristics and impacts of IT vulnerabilities.
- To obtain access to the z Systems Security Portal, you need to register and provide the customer name, your name and Resource Link ID
- http://www-03.ibm.com/systems/z/solutions/security_subintegrity.html

Insurgency Soldier of Fortan soldiers on

(Sam Knutson)

Phil Young sightings

- Blog http://mainframed767.tumblr.com/
- Spoke at DEFCON 23 in Las Vegas this week with and released some new open source tools for mainframe security research free video & proceedings here https://media.defcon.org/ all things start here https://defcon.org/
- Materials released from the DEF CON 23 talk include Exploits and Shellcode, Network tools https://github.com/zedsec390/defcon23
- Network Tools include
  - NMAP Upgrades and enhancements for TN3270 and more!
  - iNJEctor NJE JES2 command injector for z/OS
  - SET'n'3270. Script and library for tricking 3270 users (fake TN3270 server)

Phil Young sightings

- Slides for Security necromancy - Further adventures in mainframe hacking http://www.slideshare.net/bigendiansmalls/security-necromancy-publish
- Very thoughtful blog White Hats, Black Hats. A Hacker Community is Emerging Around the Mainframe. What You Need to Know… by MIKE ROGERS on AUGUST 11, 2015
  - https://www.attachmate.com/blogs/legacymodernization/white-hats-black-hats-a-hacker-community-is-emerging-around-the-mainframe-what-you-need-to-know/

MF-PEN

- Phil Young has spoken and SHARE and other conferences about mainframe security creating a new level of awareness
- Recently a mailing list has been established for those seriously or less seriously interested in Mainframe Security Penetration Testing
- MF-PEN topics include All things Mainframe security, penetration testing and general hackery.
- Subscribe here https://lists.bitrot.info/mailman/listinfo/mf-pen
- Ironically the site has a certificate issue which makes accessing it to subscribe considered an unsafe activity by most modern browsers ☹

What the *$#@*???

(Skip Robinson)

Sysplex Failure Mgmt Policy and AUTOIPL

- We have run with SFM Policy for years
- A few weeks ago, a system hung up during shutdown
- Even before Ops could react..
    - System was fenced out of sysplex by another member
    - 'Hands free' standalone was taken
    - System was reIPLed as before
- All this took only a few minutes with no intervention
- Message from another member at 01:11:25
- IXC446I SYSTEM X1 IS IN MONITOR-DETECTED STOP STATUS
- BUT IS SENDING XCF SIGNALS. SFM WILL TAKE SSUM ACTION
- 07/26/2015 01:14:25 IF SYSTEM REMAINS IN THIS STATE.
- SAD title: "AUTOIPL WAIT STATE CODE 001040A2"

Enable Status Detect in Sysplex Couple DS

- Status Detect allows sysplex to take action if another member fails to provide timely status

```
DEFINEDS SYSPLEX(plex-name)
        DSN(sysplex-couple-DSN) VOLSER(volser)
        MAXSYSTEM(n)
        CATALOG
    DATA TYPE(SYSPLEX)
         ITEM NAME(GROUP) NUMBER(150)
         ITEM NAME(MEMBER) NUMBER(120)
         ITEM NAME(GRS) NUMBER(1)
         ITEM NAME(SSTATDET) NUMBER(1)
```

SFM Policy

- SYSTEM
- NAME(*) [this includes failing system]
- WEIGHT(10)
- SSUMLIMIT(180)
- MEMSTALLTIME(240)
- CFSTRHANGTIME(900) /* PER R12 HEALTHCHK */

- Policy removes (fences) an unresponsive system after 3 minutes
- 'Stalled' means not updating couple data set
- Even if still communicating via sysplex links

Support in SYS1.PARMLIB(DIAGxx)

- Edit following line into SYS1.PARMLIB(DIAGxx):
- AUTOIPL SADMP(uuuu,SMSYSC) MVS(LAST)
- uuuu is the SAD IPL volume you have prepared
- I.e. the volume you would IPL from for manual SAD
- 'SMSYSC' allows SAD to proceed with no intervention
  - Do not prompt operator for SAD title, instead use generic title
  - Overwrite any existing dump on the SAD device(s)
  - Write all messages to HMC Operating System Messages
- After SAD, IPLs automatically from last used sysres
- Operators may be unaware of failure/reIPL!
- YOU may be unaware!!!
- Action performed by hardware, so no console message
- If you suspect auto IPL occurred, browse SAD dataset
- "AUTOIPL WAIT STATE CODE 001040A2" date/time

How Green is My Screen?

(Skip Robinson)

Why I Love Vista tn3270 (c)

- I have used Vista tn3270 exclusively since the 1990s
- One day my then-colleague Tom Brennan asked me to 'try out' an emulator he had written
- Since that day I have not used any other emulator in my work
- Here are some of the reasons why

- It's the only emulator written by an experienced mainframe sysprog
- Tom learned MVS first, then C++ and Windows application programming
- He knew what mainframe users need from the get-go

Why I Love Vista tn3270 (c)

- Vista contains time/labor saving usability features
- Several variations of copy/paste
- Macro creation, editing, execution
- Some are supported by key shortcuts, others selectable from drop down menus
- Many functions are context sensitive for JCL

- Easy to install and configure
- Lightweight, initializes quickly
- Installs in its own directory structure

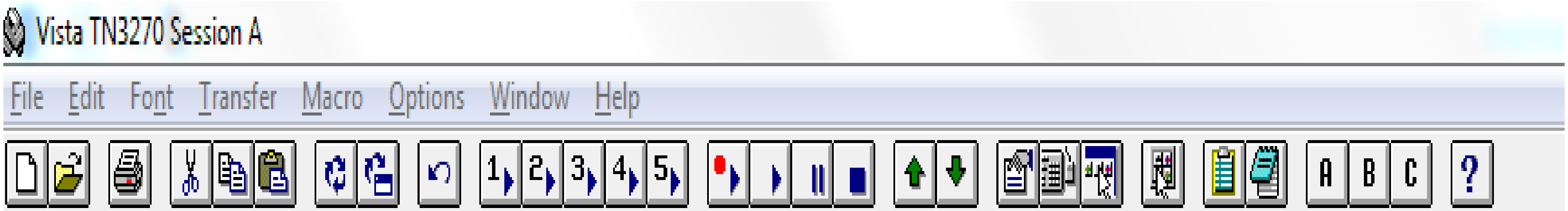
Some down sides to Vista tn3270

- Windows only, no Linux version

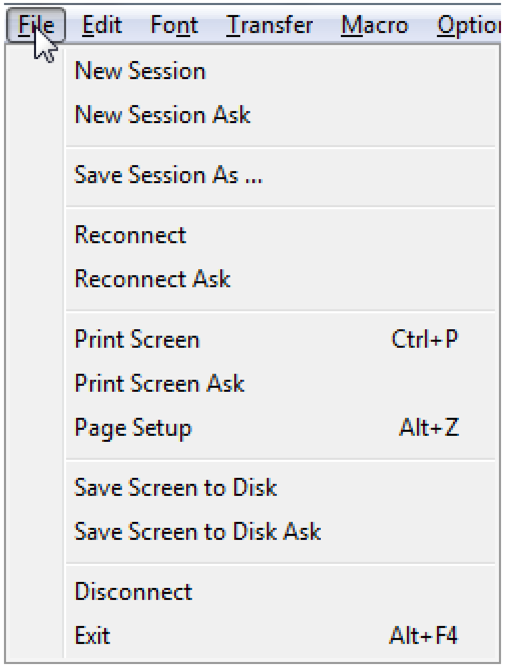
- Does not perform certain 'fancy' graphics
- I personally have never missed those
- Nowadays there are better platforms than 3270 for fancy graphics

- Tom Brennan Software is a one-man ISV
- Could be an issue for a large shop
- No vendor has provided better service over the years
- I have used Vista for all my mainframe work since the 90s with no pushback
- This is not a fiscal problem but an issue of corporate policy

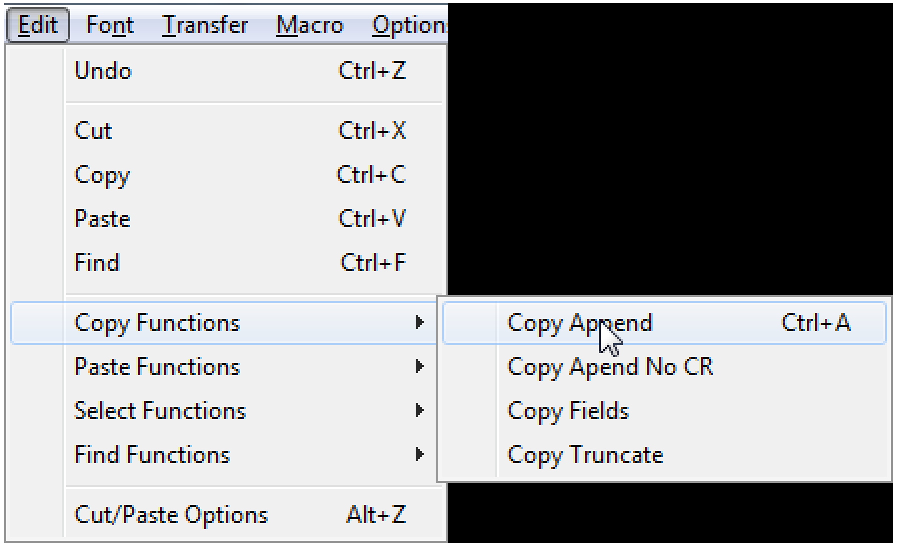
Vista tn3270 customizable tool bar



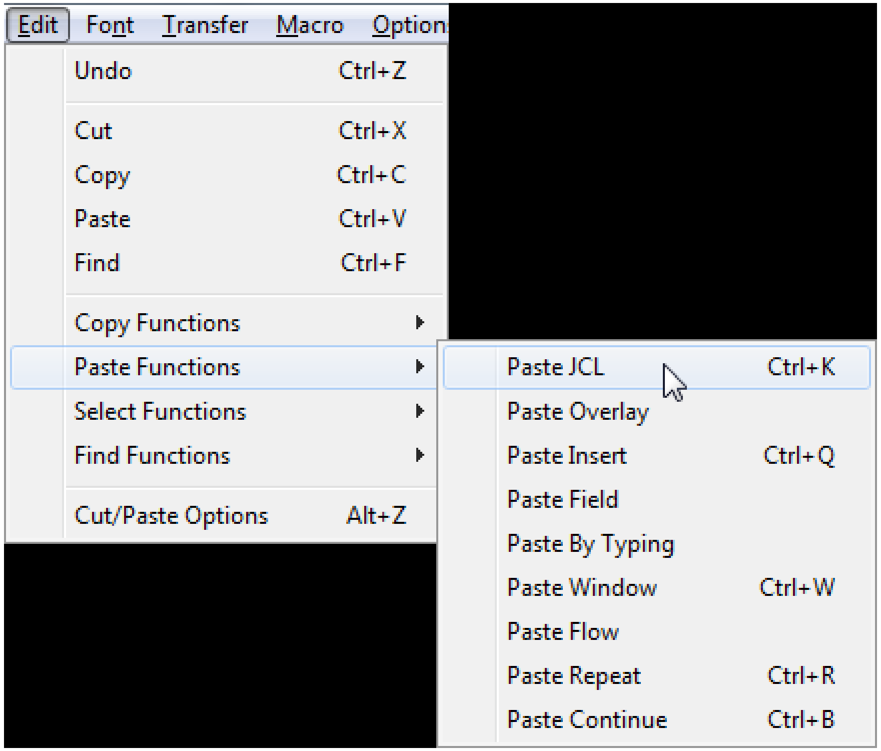
'File' drop down menu



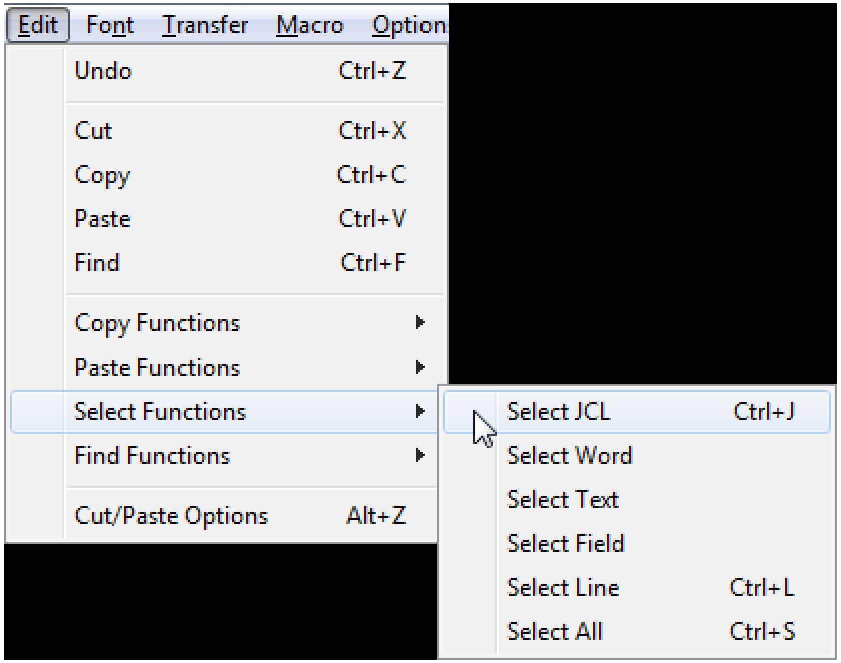
'Edit Copy Functions' drop down menu



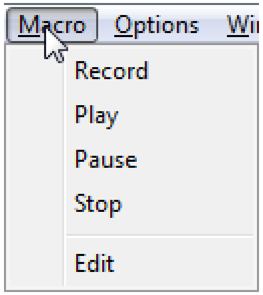
'Edit Paste Functions' drop down menu



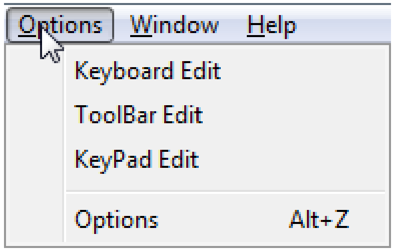
'Edit Select Functions' drop down menu



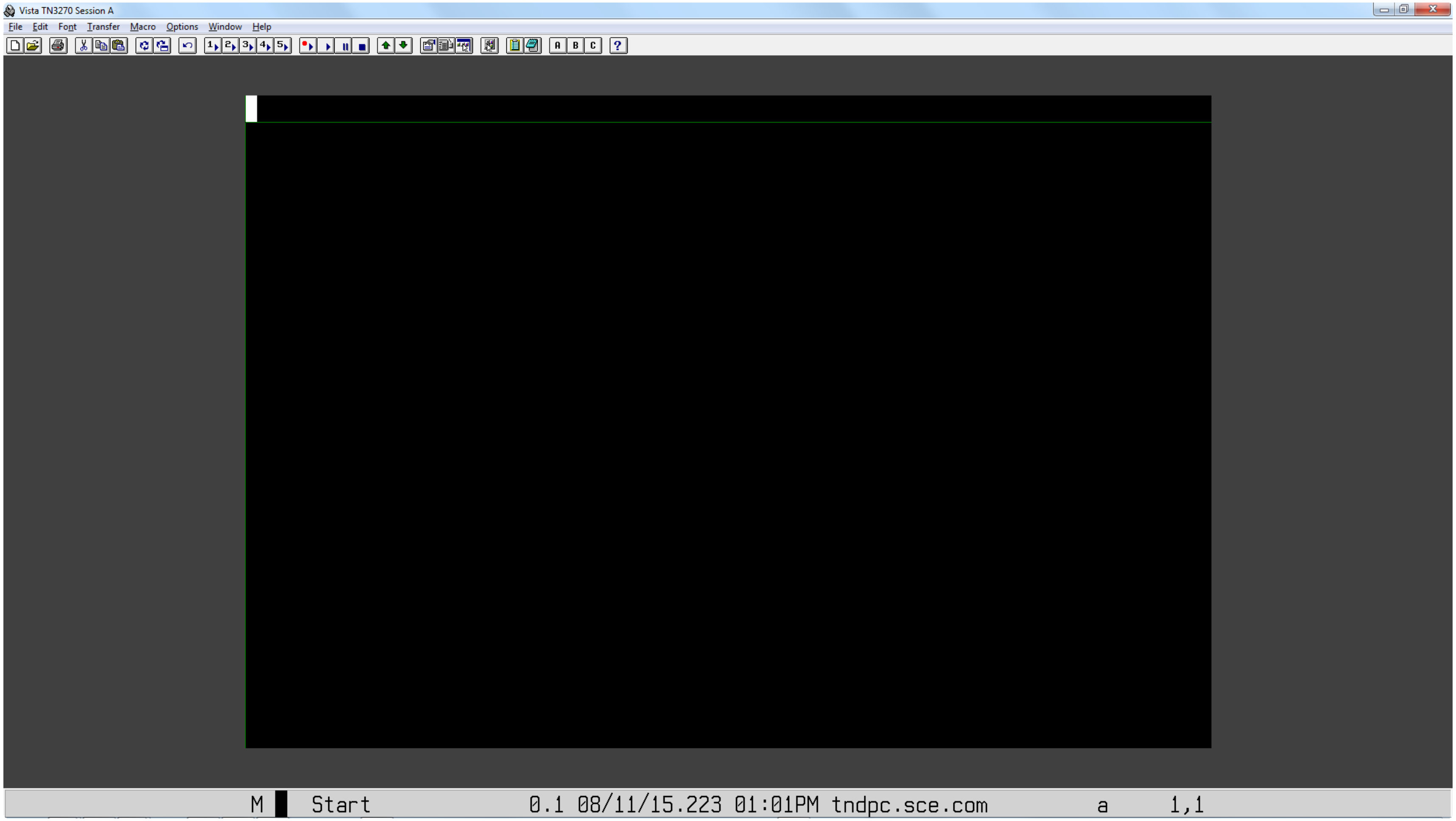
'Macro' drop down menu



'Options' drop down menu



Macro for logging on to TPX: initial screen

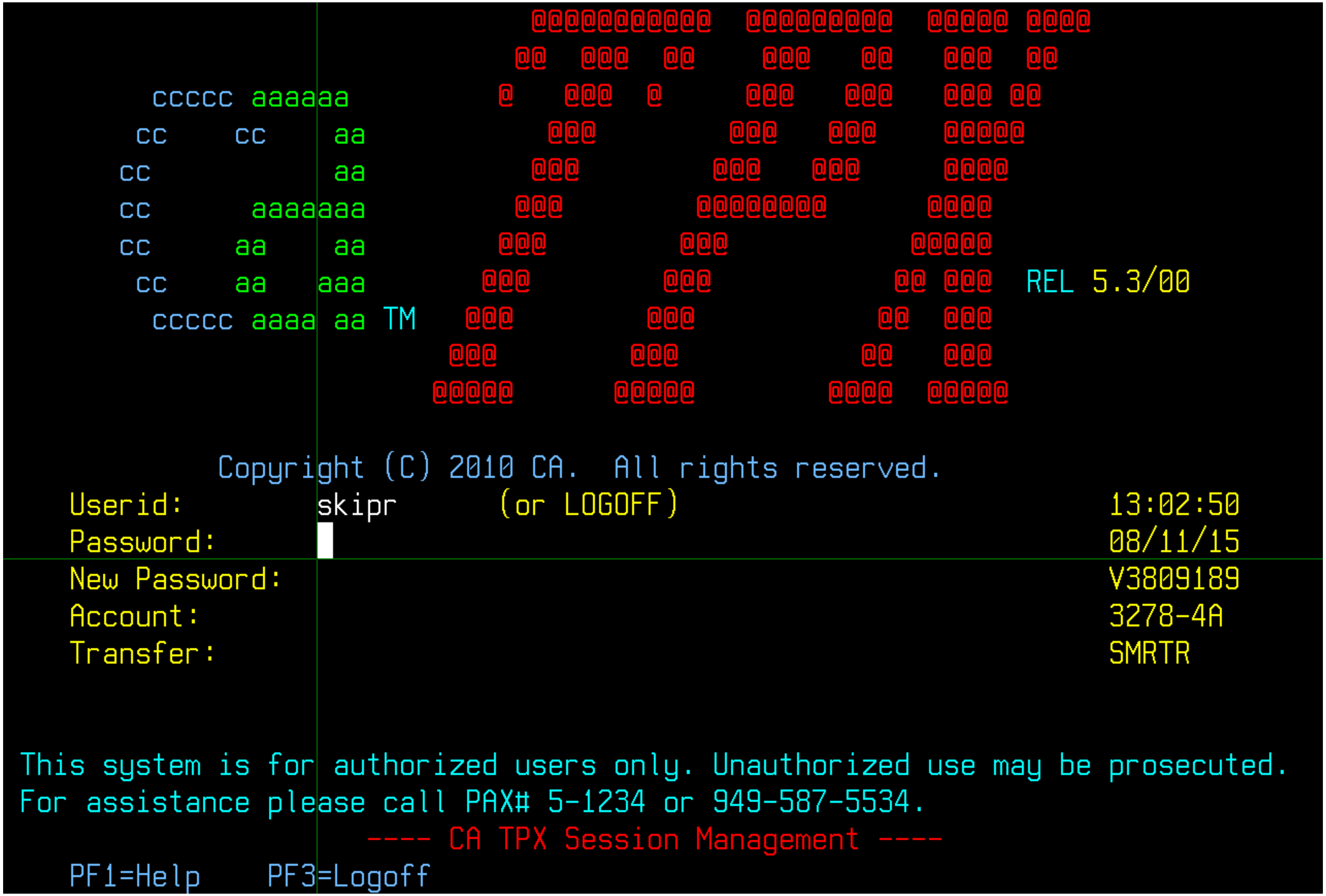


```
M █  Start           0.1 08/11/15.223 01:01PM tndpc.sce.com          a      1,1
```

“Startup Macro” (recorded from keystrokes)

```
***********************************************
* Vista macro generated on 01/22/98 15:47:34
***********************************************
Wait(20,Status="Unlocked")
Type("tpx pcmod4")
Key("Enter")
Wait(20,Status="Unlocked" & CursorPos = "14,20")
Type(“skipr")
Key("NewLine")
```

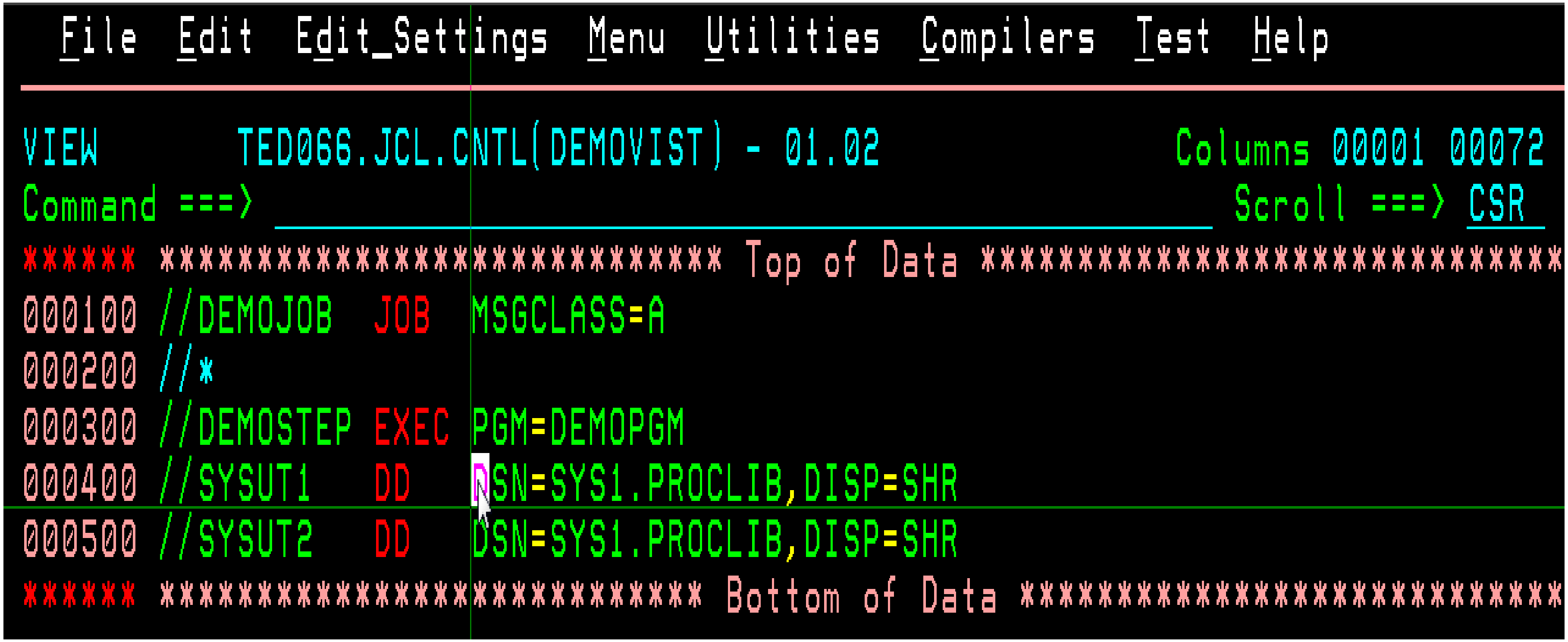
Login to TPX: screen after initial macro



```
                                @@@@@@@@@@@  @@@@@@@@@  @@@@@ @@@@
                               @@  @@@  @@    @@@   @@   @@@  @@
         ccccc aaaaaa         @   @@@  @     @@@   @@@   @@@ @@
        cc    cc    aa           @@@        @@@   @@@    @@@@@
       cc           aa          @@@        @@@   @@@     @@@@
       cc      aaaaaaa         @@@        @@@@@@@@      @@@@
       cc     aa    aa        @@@        @@@           @@@@@
        cc    aa   aaa       @@@        @@@           @@ @@@  REL 5.3/00
         ccccc aaaa aa TM   @@@        @@@           @@  @@@
                           @@@        @@@           @@   @@@
                          @@@@@      @@@@@        @@@@  @@@@@

             Copyright (C) 2010 CA.  All rights reserved.
    Userid:        skipr      (or LOGOFF)                          13:02:50
    Password:                                                      08/11/15
    New Password:                                                  V3809189
    Account:                                                       3278-4A
    Transfer:                                                      SMRTR


 This system is for authorized users only. Unauthorized use may be prosecuted.
 For assistance please call PAX# 5-1234 or 949-587-5534.
                      ---- CA TPX Session Management ----
    PF1=Help    PF3=Logoff
```

Vista 'editing' a JCL file

Right-click to capture keyword and value

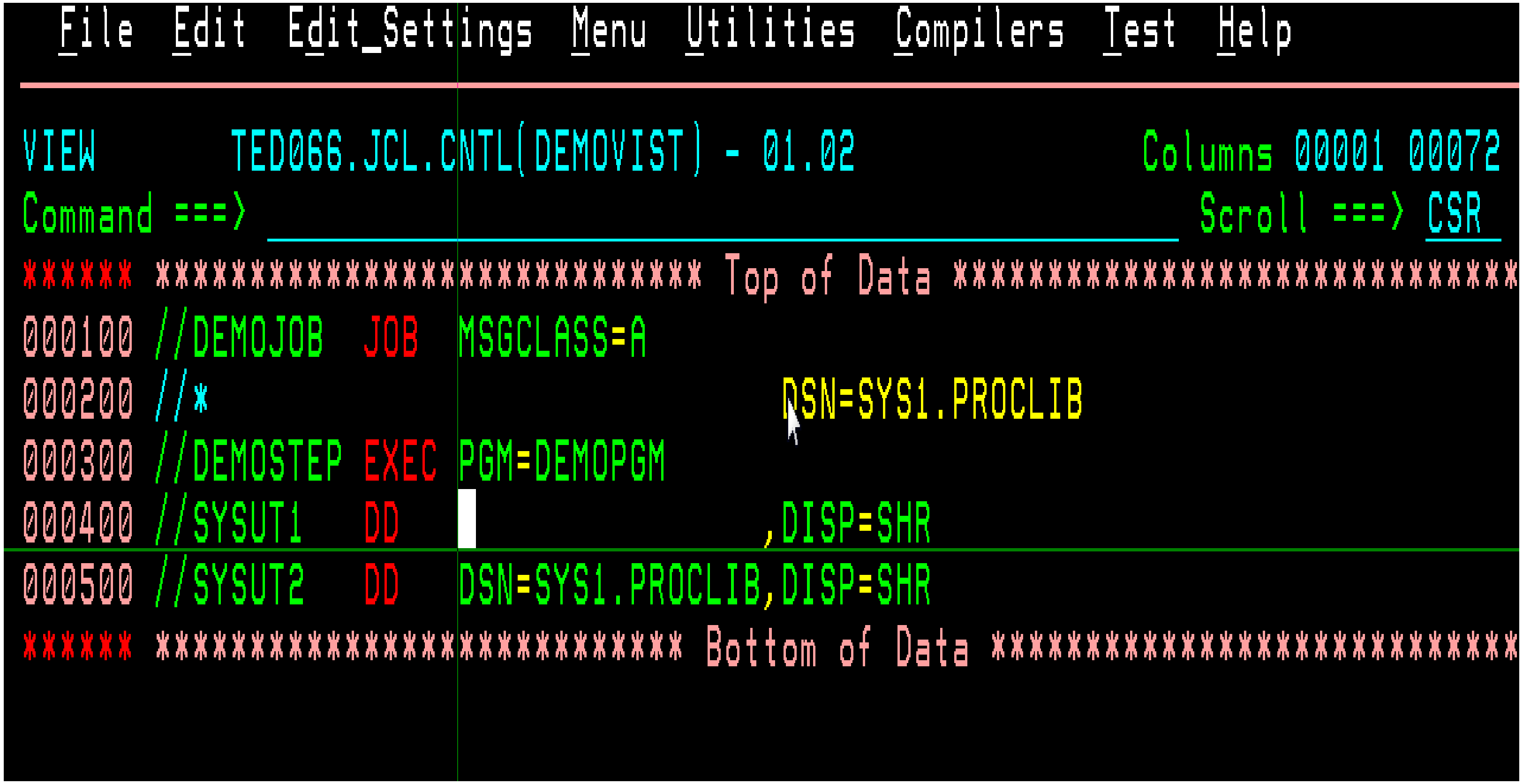


File Edit Edit_Settings Menu Utilities Compilers Test Help

```
VIEW       TED066.JCL.CNTL(DEMOVIST) - 01.02             Columns 00001 00072
Command ===>                                                 Scroll ===> CSR
****** **************************** Top of Data ****************************
000100 //DEMOJOB  JOB  MSGCLASS=A
000200 //*
000300 //DEMOSTEP EXEC PGM=DEMOPGM
000400 //SYSUT1   DD   DSN=SYS1.PROCLIB,DISP=SHR
000500 //SYSUT2   DD   DSN=SYS1.PROCLIB,DISP=SHR
****** *************************** Bottom of Data ***************************
```

Vista ‘editing’ a JCL file

Right-click on DSN to select it, then left-click to drag it out of line

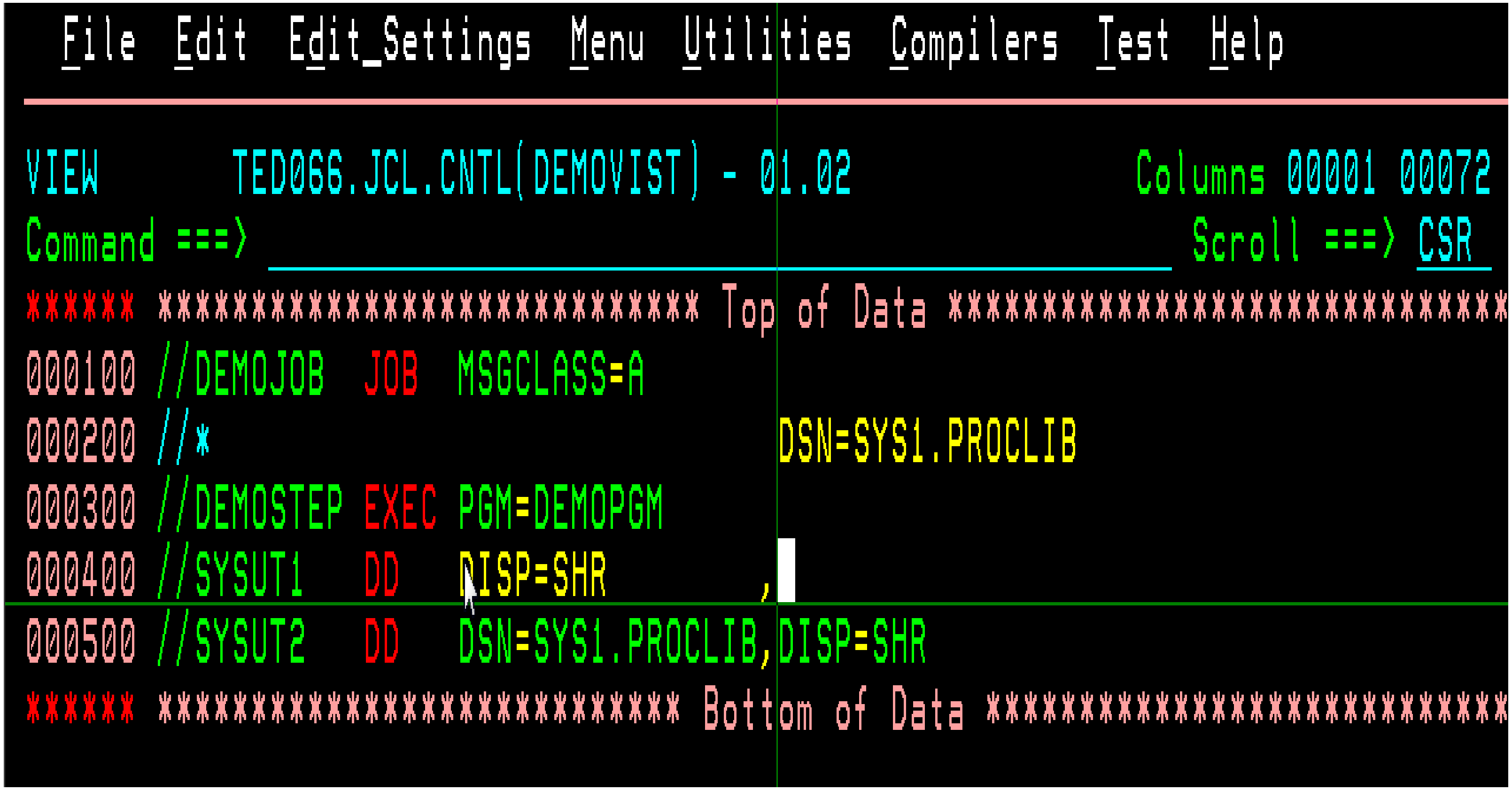


File Edit Edit_Settings Menu Utilities Compilers Test Help

```
VIEW       TED066.JCL.CNTL(DEMOVIST) - 01.02                Columns 00001 00072
Command ===>                                                    Scroll ===> CSR
****** ***************************** Top of Data ******************************
000100 //DEMOJOB  JOB  MSGCLASS=A
000200 //*                              DSN=SYS1.PROCLIB
000300 //DEMOSTEP EXEC PGM=DEMOPGM
000400 //SYSUT1   DD                   ,DISP=SHR
000500 //SYSUT2   DD   DSN=SYS1.PROCLIB,DISP=SHR
****** **************************** Bottom of Data ****************************
```

Vista ‘editing’ a JCL file

Right-click on DISP to select it, then left-click to drag it to the left

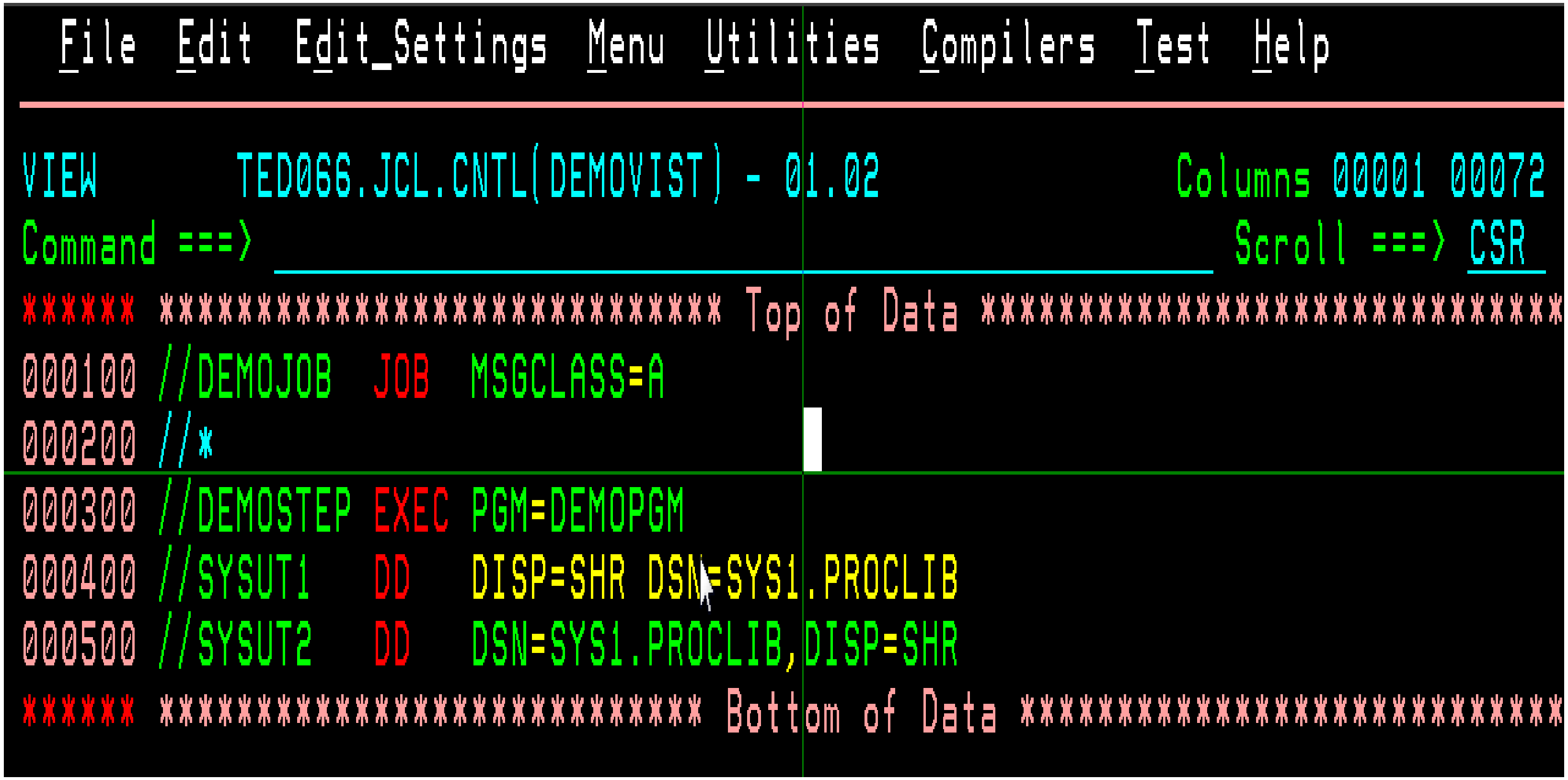


File Edit Edit_Settings Menu Utilities Compilers Test Help

```
VIEW       TED066.JCL.CNTL(DEMOVIST) - 01.02               Columns 00001 00072
Command ===>                                                  Scroll ===> CSR
****** ***************************** Top of Data ******************************
000100 //DEMOJOB  JOB  MSGCLASS=A
000200 //*                                  DSN=SYS1.PROCLIB
000300 //DEMOSTEP EXEC PGM=DEMOPGM
000400 //SYSUT1   DD   DISP=SHR           ,
000500 //SYSUT2   DD   DSN=SYS1.PROCLIB,DISP=SHR
****** **************************** Bottom of Data ****************************
```

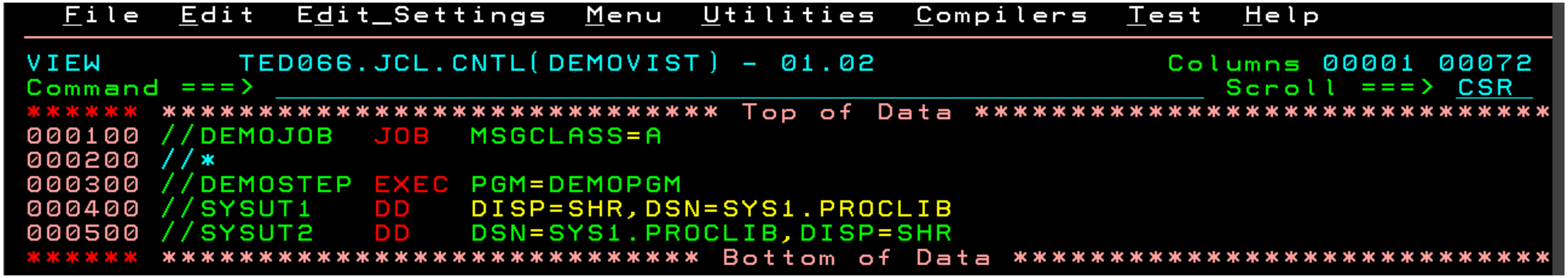
Vista 'editing' a JCL file

Right-click on DSN, then drag back in line



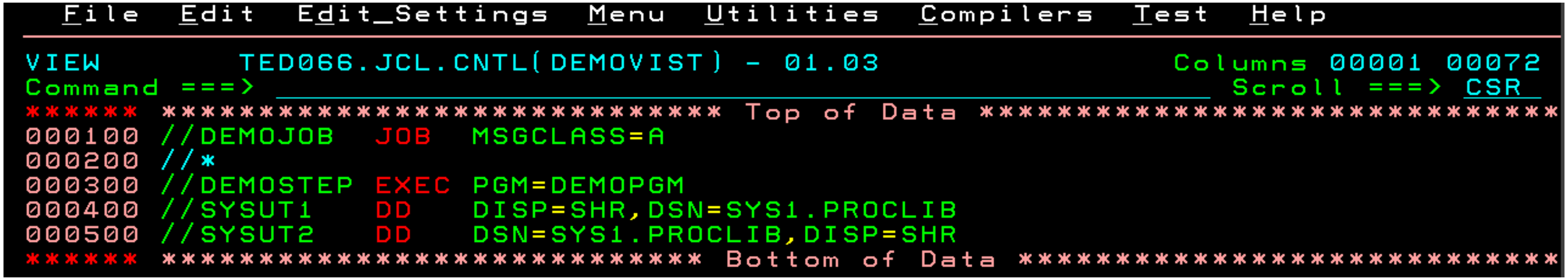
```
VIEW       TED066.JCL.CNTL(DEMOVIST) - 01.02             Columns 00001 00072
Command ===>                                                  Scroll ===> CSR
****** ***************************** Top of Data ******************************
000100 //DEMOJOB  JOB  MSGCLASS=A
000200 //*
000300 //DEMOSTEP EXEC PGM=DEMOPGM
000400 //SYSUT1   DD   DISP=SHR DSN=SYS1.PROCLIB
000500 //SYSUT2   DD   DSN=SYS1.PROCLIB,DISP=SHR
****** **************************** Bottom of Data ****************************
```

Type in comma, still no <Enter>



```
   File   Edit   Edit_Settings   Menu   Utilities   Compilers   Test   Help
VIEW       TED066.JCL.CNTL(DEMOVIST) - 01.02               Columns 00001 00072
Command ===> ________________________________________________ Scroll ===> CSR
****** ***************************** Top of Data ******************************
000100 //DEMOJOB  JOB  MSGCLASS=A
000200 //*
000300 //DEMOSTEP EXEC PGM=DEMOPGM
000400 //SYSUT1   DD   DISP=SHR,DSN=SYS1.PROCLIB
000500 //SYSUT2   DD   DSN=SYS1.PROCLIB,DISP=SHR
****** **************************** Bottom of Data ****************************
```

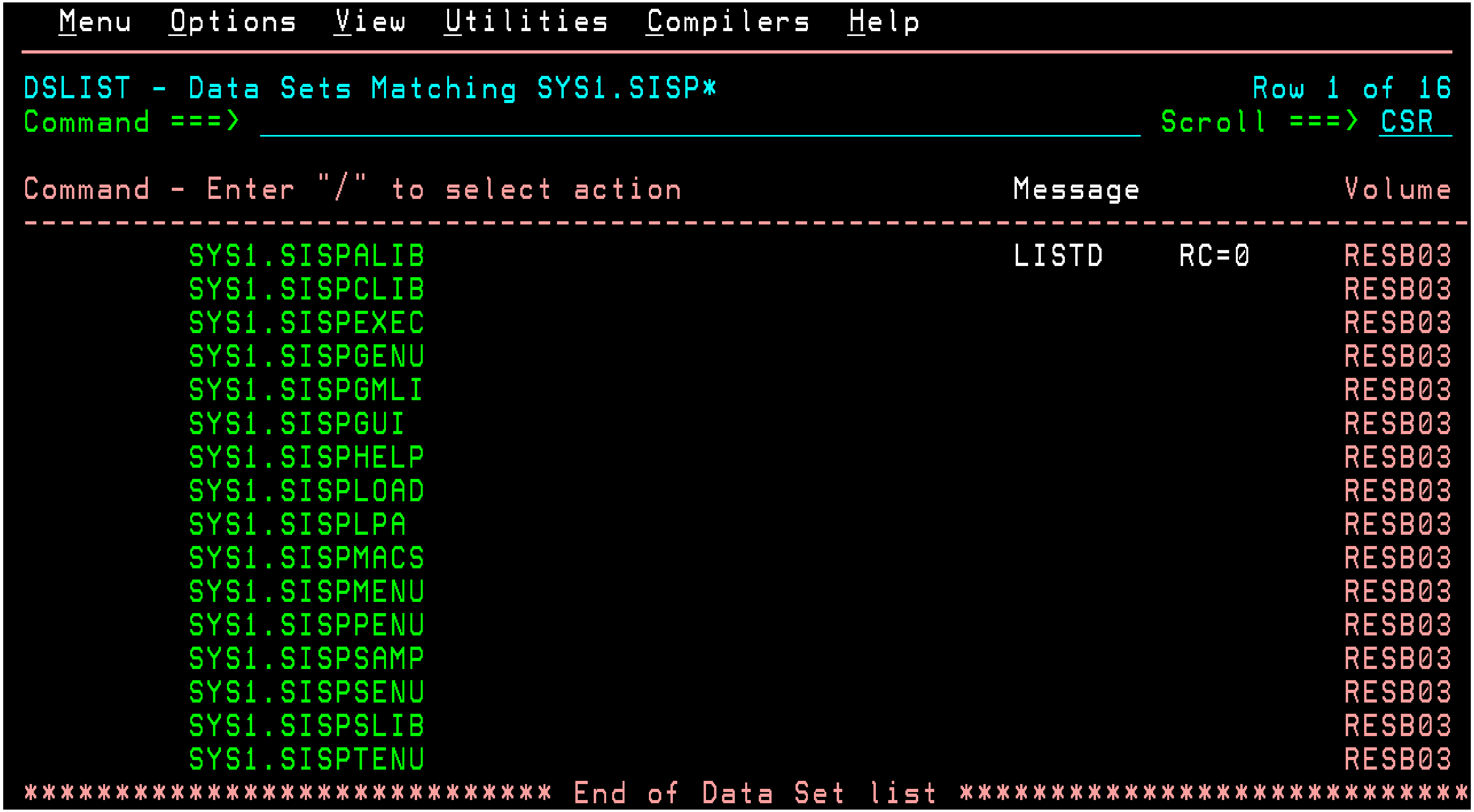
Finally hit <Enter> to harden change


File Edit Edit_Settings Menu Utilities Compilers Test Help

```
 VIEW       TED066.JCL.CNTL(DEMOVIST) - 01.03                Columns 00001 00072
 Command ===> ________________________________________________ Scroll ===> CSR
 ****** ***************************** Top of Data ******************************
 000100 //DEMOJOB  JOB   MSGCLASS=A
 000200 //*
 000300 //DEMOSTEP EXEC  PGM=DEMOPGM
 000400 //SYSUT1   DD    DISP=SHR,DSN=SYS1.PROCLIB
 000500 //SYSUT2   DD    DSN=SYS1.PROCLIB,DISP=SHR
 ****** **************************** Bottom of Data ****************************
```

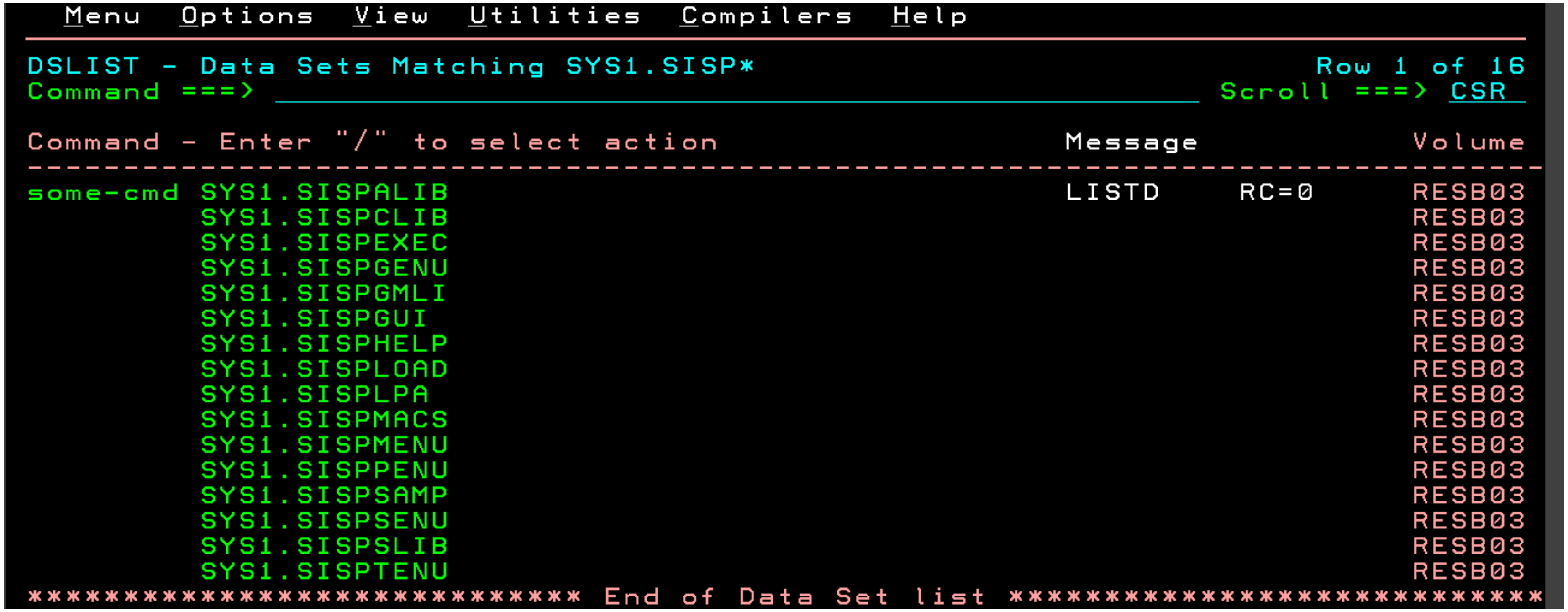
Using Paste Repeat to populate input fields

Start with a display containing command input



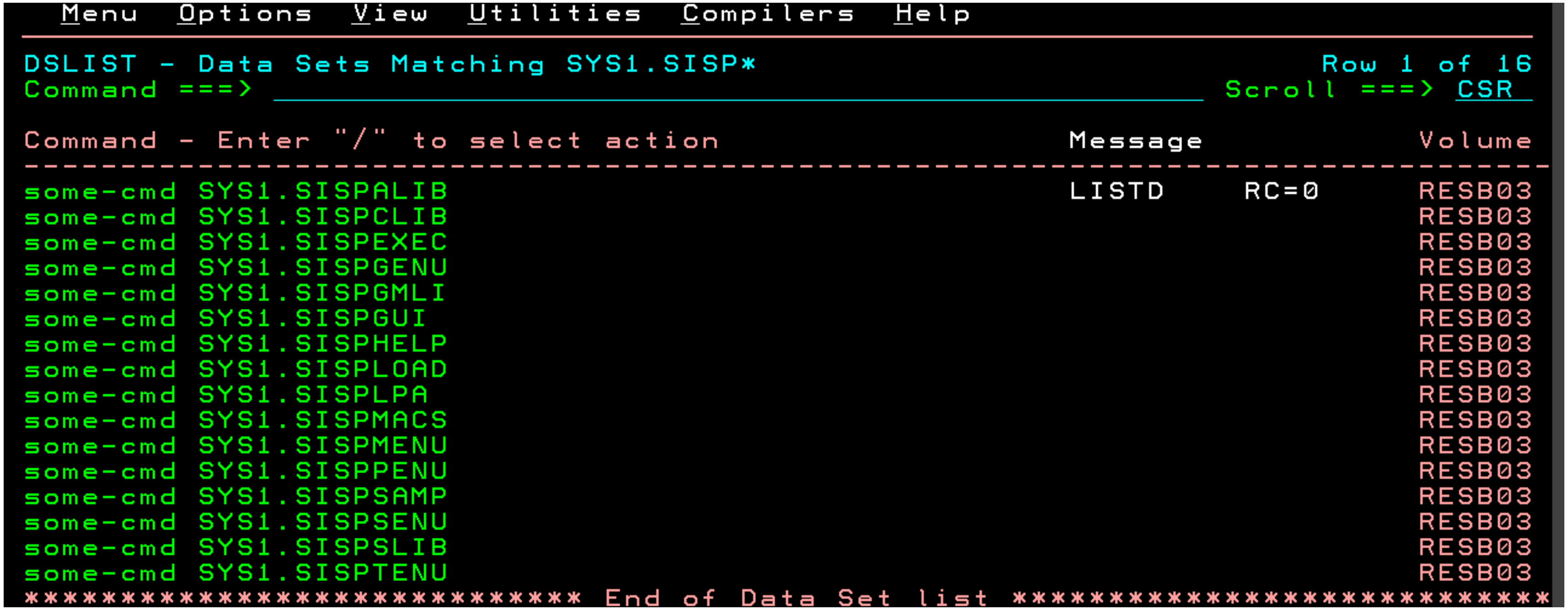
```
   Menu  Options  View  Utilities  Compilers  Help
 ------------------------------------------------------------------------------
 DSLIST - Data Sets Matching SYS1.SISP*                            Row 1 of 16
 Command ===> ________________________________________________ Scroll ===> CSR

 Command - Enter "/" to select action                  Message           Volume
 -------------------------------------------------------------------------------
          SYS1.SISPALIB                                LISTD    RC=0     RESB03
          SYS1.SISPCLIB                                                  RESB03
          SYS1.SISPEXEC                                                  RESB03
          SYS1.SISPGENU                                                  RESB03
          SYS1.SISPGMLI                                                  RESB03
          SYS1.SISPGUI                                                   RESB03
          SYS1.SISPHELP                                                  RESB03
          SYS1.SISPLOAD                                                  RESB03
          SYS1.SISPLPA                                                   RESB03
          SYS1.SISPMACS                                                  RESB03
          SYS1.SISPMENU                                                  RESB03
          SYS1.SISPPENU                                                  RESB03
          SYS1.SISPSAMP                                                  RESB03
          SYS1.SISPSENU                                                  RESB03
          SYS1.SISPSLIB                                                  RESB03
          SYS1.SISPTENU                                                  RESB03
 ***************************** End of Data Set list ****************************
```

Type command, double-right-click to copy it



```
   Menu  Options  View  Utilities  Compilers  Help
 ------------------------------------------------------------------------------
 DSLIST - Data Sets Matching SYS1.SISP*                            Row 1 of 16
 Command ===> ________________________________________________ Scroll ===> CSR

 Command - Enter "/" to select action                  Message           Volume
 -------------------------------------------------------------------------------
 some-cmd SYS1.SISPALIB                                 LISTD    RC=0     RESB03
          SYS1.SISPCLIB                                                   RESB03
          SYS1.SISPEXEC                                                   RESB03
          SYS1.SISPGENU                                                   RESB03
          SYS1.SISPGMLI                                                   RESB03
          SYS1.SISPGUI                                                    RESB03
          SYS1.SISPHELP                                                   RESB03
          SYS1.SISPLOAD                                                   RESB03
          SYS1.SISPLPA                                                    RESB03
          SYS1.SISPMACS                                                   RESB03
          SYS1.SISPMENU                                                   RESB03
          SYS1.SISPPENU                                                   RESB03
          SYS1.SISPSAMP                                                   RESB03
          SYS1.SISPSENU                                                   RESB03
          SYS1.SISPSLIB                                                   RESB03
          SYS1.SISPTENU                                                   RESB03
 ***************************** End of Data Set list ****************************
```

Cursor on 2nd line, then Ctrl+R (Paste Repeat)



```
   Menu  Options  View  Utilities  Compilers  Help
 ------------------------------------------------------------------------------
 DSLIST - Data Sets Matching SYS1.SISP*                            Row 1 of 16
 Command ===> ________________________________________________ Scroll ===> CSR

 Command - Enter "/" to select action                  Message           Volume
 -------------------------------------------------------------------------------
 some-cmd SYS1.SISPALIB                                LISTD     RC=0    RESB03
 some-cmd SYS1.SISPCLIB                                                  RESB03
 some-cmd SYS1.SISPEXEC                                                  RESB03
 some-cmd SYS1.SISPGENU                                                  RESB03
 some-cmd SYS1.SISPGMLI                                                  RESB03
 some-cmd SYS1.SISPGUI                                                   RESB03
 some-cmd SYS1.SISPHELP                                                  RESB03
 some-cmd SYS1.SISPLOAD                                                  RESB03
 some-cmd SYS1.SISPLPA                                                   RESB03
 some-cmd SYS1.SISPMACS                                                  RESB03
 some-cmd SYS1.SISPMENU                                                  RESB03
 some-cmd SYS1.SISPPENU                                                  RESB03
 some-cmd SYS1.SISPSAMP                                                  RESB03
 some-cmd SYS1.SISPSENU                                                  RESB03
 some-cmd SYS1.SISPSLIB                                                  RESB03
 some-cmd SYS1.SISPTENU                                                  RESB03
 ***************************** End of Data Set list ****************************
```

Acknowledgements Both Knowing and Unknowing

- Tom Brennan (Tom Brennan Software)
- Mark Brooks (IBM), mabrook@us.ibm.com
- David Jones (IBM), davidjon@us.ibm.com
- Jeff Magdall (IBM), magdall@us.ibm.com
- Chad Rikansurd (aka bigendiansmalls)
- Mike Rogers (Attachmate)
- Karl Schmitz (IBM), kdsch@us.ibm.com
- John Shebey (IBM), jshebey@us.ibm.com
- Stephen Warren (IBM), swarren@us.ibm.com
- Tom Wasik (IBM), wasik@us.ibm.com
- Phil Young (aka Soldier of Fortran)

See You in

San Antonio