TICOM

TECHNICAL INTELLIGENCE COMMUNICATIONS

Issue #2, March 2005
http://www.iirg.net/~ticom/zine/ - email: ticom@iirg.net

This issue brought to you with help from Magic Hat #9

CONTENTS:

Frequency Counter Logging to a PC

Back when the first decent handheld frequency counters came out that were suitable for SIGINT operations, they lacked the features of current models. I used one of the Radio Shack counters with some success despite the lack of capture and hold features. Of course, it was much easier to use as a passenger in a vehicle than as a driver. Optoelectronics then came out with their "Scout" model that was specifically designed for this sort of thing. It also had a $450 price tag. Many hardcore SIGINT hackers went and bought one to have fun with. Among the nice things about the Scout was that it had a 400 frequency memory, the capability to download frequency hits to a PC, and the ability to reaction tune an Icom or AOR receiver to the frequency it detected. The price tag however, kept it out of the range of most hobbyists. Optoelectronics still makes different models of the Scout, and they are still as expensive as they were ten years ago.

Other companies have started making frequency counters that feature the capability to automatically tune receivers to the frequency they detect. One such company is Aceco, whose products are also sold under other names. I came across one of their "RF Finders", the FC3002, at a local electronics shop for about half the price of the Optoelectronics Scout. It too was capable of automatically tuning an Icom or AOR receiver, and it does an admirable job with my Icom R-10. The feature it didn't have was memory storage of frequency hits. I figured that since it had a serial port and I had enough old laptops

lying around, there would be no problems with automatic frequency hit logging. I should also note that Optoelectronics at one time made a stripped-down version of the Scout that was basicly intended for reaction-tuning receivers, and also lacked the memory storage of its big brother. You might come across one at a hamfest somewhere, and the information in this article also applies to that unit.

These frequency counters have a sub-mini speaker jack that is a TTL serial port. The frequency data can be sent out in either Icom's CI-V, or AORs command format; depending on what brand of receiver you are using with it. Of the two, the AOR format is the one that is the easiest for a person to read without software translation. The Aceco FC3002 has a switch on the front labeled "COM". Simply switch it to the "AOR" setting, and you'll be set. You will then need a TTL/Serial converter. For this article I used an Optoelectronics Optolynx. You may want to build your own if you are on a budget. TTL/Serial converters are a simple enough project, and on the next page is an example of an inexpensively-built one found on the net.. You will also need a PC of some sort running a terminal program at 9600 baud 8N1. The old Compaq in the picture was what I had handy, but I could have dug out a TRS-80 Model 100 and used that if so inclined. The equipment list when I was done looked like this:

- Aceco FC3002 Frequency Counter
- Optoelectronics Optolynx
- 24" patch cord, 1/8" miniature speaker plugs on each end
- sub-mini to 1/8" sepaker plug adapter (the jack on the counter is a sub-mini)
- 9-pin "D" Serial Cable
- Old Compaq laptop running terminal software (Telix); 9600 baud, 8N1

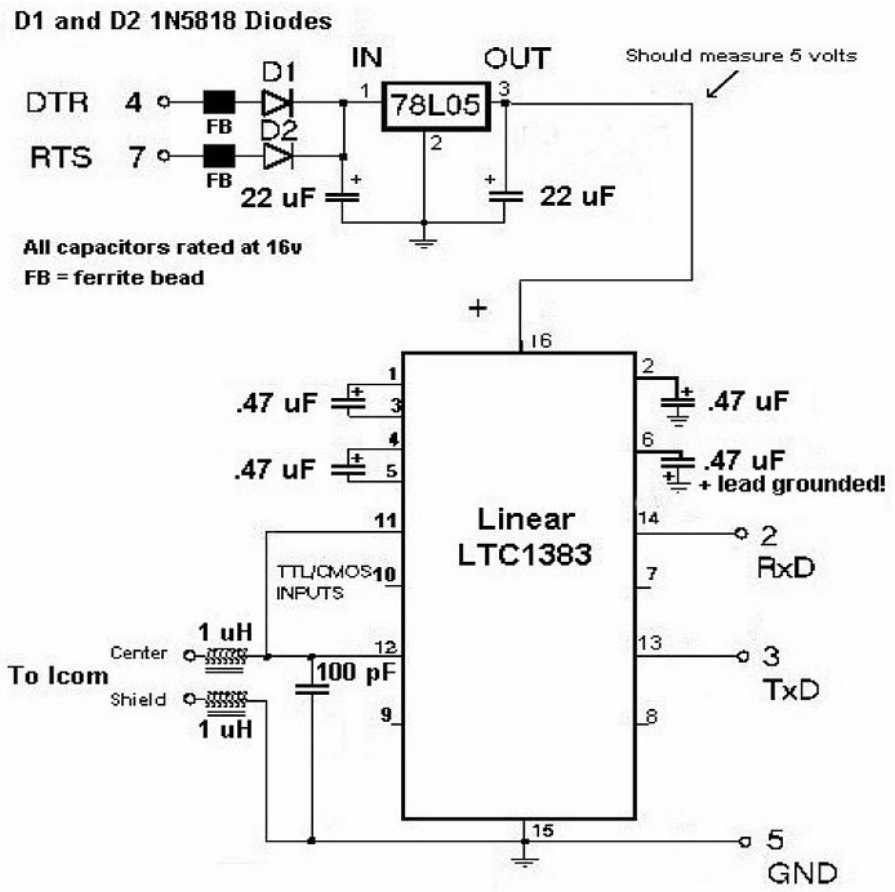
After equipment assembly, simply turn everyting on, set the frequency counter to reaction tune mode (On the Aceco, push the "FUNCTION" button until "HOLD" on the display starts flashing.), boot up the PC, and load the terminal software. At this point, you will want to test it with a transmitter to make sure it's working. Key up, and you should see the frequency of your transmitter displayed on the screen in the format of M0000000 where the 0000000 is the frequency. From there you can simply activate an ASCII text download on your terminal software, and all your frequency hits will be logged to disk.

5. WORD Document Changes Due to Divestiture

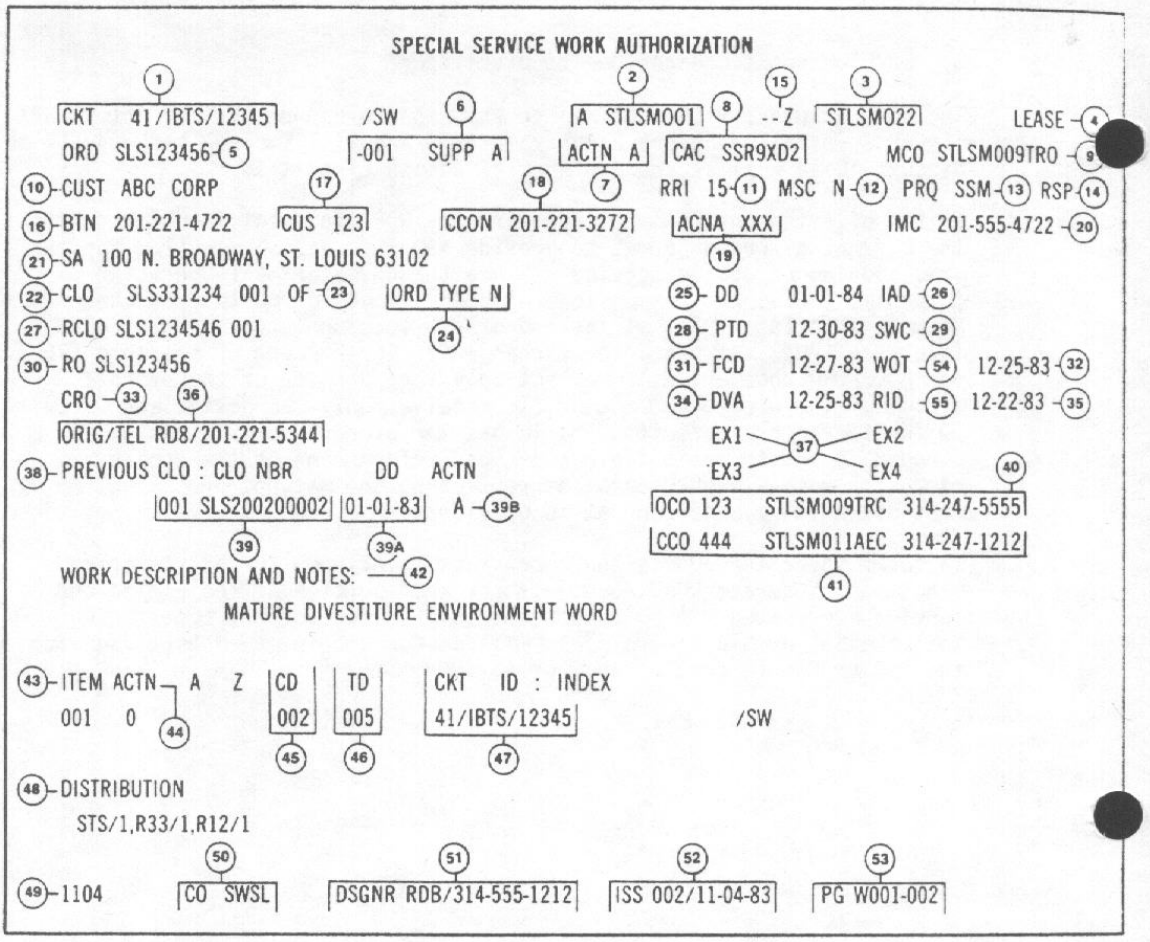
The WORD document will continue to show end-to-end design for inter-LATA circuits installed before January 1, 1984 and will include the overall IC Circuit ID as well as the BOC special access Circuit ID.

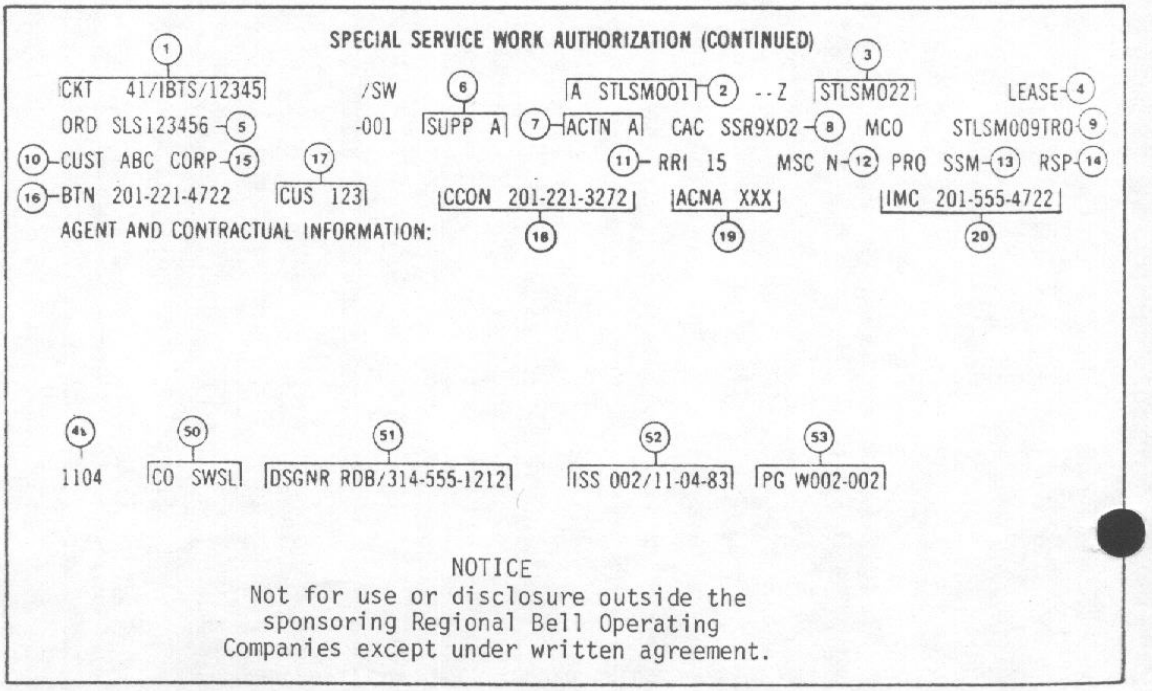
In the divested environment, however, the WORD document is changed from the current standard format to provide new information required for the provisioning of access service. Since the divested Bell Operating Companies (BOCs) are responsible only for access circuits from the Network Interface (NI), at the end user's location, to the Point of Interface (POI), at the Inter-exchange Carrier's Point of Presence (POP), the BOC WORD document will reflect only that portion of the overall circuit. Therefore, the SSC or STC receives only the design and Circuit ID for the access circuit. The IC has the overall service design and Circuit ID and is responsible for cross-referencing to the access circuit. A sample WORD document reflecting the mature, or post-divestiture, environment is provided.

In cases where the BOC is under contract to ATTCOMM for provisioning functions, separate WORD documents for each portion of the end-to-end service are issued. A WORD document is provided for the access circuit that the SSC or STC controls, as well as for the inter-exchange service the SSC or STC is controlling for ATTCOMM.



CI-V to RS-232 Converter
from http://www.qsl.net/kd6uu/icomci.html





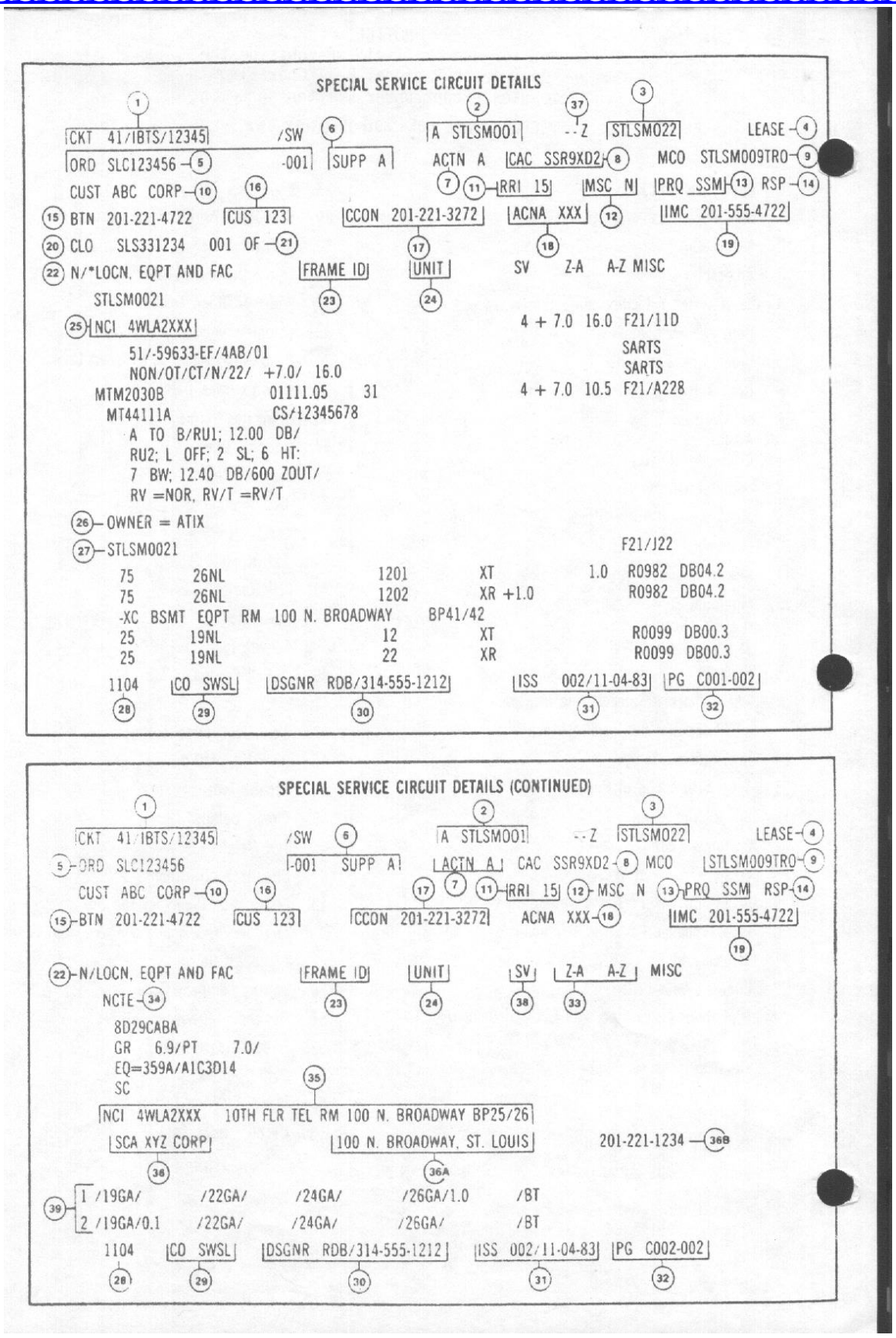
NOTICE
Not for use or disclosure outside the sponsoring Regional Bell Operating Companies except under written agreement.

NOTICE
Not for use or disclosure outside the sponsoring Regional Bell Operating Companies except under written agreement.

SPECIAL SERVICE WORK AUTHORIZATION - WA

*1. Circuit Identification
(In Common Language)
**2. A Location
**3. Z Location
4. Lease (when a facility equipment is leased from another company)
5. Order Type & Number
6. Item & Item Supplement Indicator
7. Activity Type
A-Add
D-Disconnect, etc.
8. Circuit Access Code
9. Maintenance Control Office
10. Customer
11. Rebate Required Interval in Hours
12. Minimum Service Charge
-Y (If applicable)
-N (If not applicable)
13. Protection Required
- SSM (Special Safeguarding Measures)
- SSP (Special Service Protection)
14. Restoration Priority
15. Type & Direction of Pulsing
16. Bill to Number
17. Customer Code
18. Customer Contact Tel. No.
19. Access Customer's Name Abbreviation
20. Inter-Exchange Carrier's Maintenance Tel. No.
21. Service Address
22. Circuit Layout Order
23. # of Items (associated with CLO - if more than 1)
24. Order Type
- N (New)
- C (Change) etc.
25. Due Date
26. Inventory Availability Date
27. Related Circuit Layout Order
28. Plant Test Date
29. Scheduled Work Completion
30. Related Order
31. Frame Continuity Date
32. Wired & Office Tested
33. Complete with Related Order
34. Designed, Verified & Assigned Date
35. Records Issue Date
36. Originator (Name & Tel. No.)
37. Optional Due
38. Previous Circuit (Layout)
-CLO Number
-Due Date
-Activity Type
39. CLO Number
39A. Due Date
39B Activity Type
40. Overall Control Office
41. Circuit Control Office
42. Work Description & Notes
43. Item No. of Order
44. Activity Type
45. Circuit Details
46. Test Details
47. Circuit Identification
48. Distribution (Specifies the No. of copies and locations where word is sent)
49. Broadcast Date
50. Issuing Company Code
51. Designer & Designer Tel. No.
52. Issue & Issue Date
53. Page Number
54. Wired & Office Tested
55. Records Issue Date

*1 REFER TO BSP 795-402-100
**2. AND 3. REFER TO BSP 682-400-100 TABLE A & B


SPECIAL SERVICE CIRCUIT DETAILS
CKT 41/IBTS/12345
/SW
A STLSM001
--Z
STLSM022
LEASE
ORD SLC123456
-001
SUPP A
ACTN A
CAC SSR9XD2
MCO STLSM009TRO
CUST ABC CORP
RRI 15
MSC N
PRQ SSM
RSP
BTN 201-221-4722
CUS 123
CCON 201-221-3272
ACNA XXX
IMC 201-555-4722
CLO SLS331234 001 OF
N/*LOCN, EQPT AND FAC
FRAME ID
UNIT
SV Z-A A-Z MISC
STLSM0021
NCI 4WLA2XXX
4 + 7.0 16.0 F21/11D
51/-59633-EF/4AB/01
SARTS
NON/OT/CT/N/22/ +7.0/ 16.0
SARTS
MTM2030B 01111.05 31
4 + 7.0 10.5 F21/A228
MT44111A CS/12345678
A TO B/RU1; 12.00 DB/
RU2; L OFF; 2 SL; 6 HT:
7 BW; 12.40 DB/600 ZOUT/
RV =NOR, RV/T =RV/T
OWNER = ATIX
STLSM0021
F21/J22
75 26NL 1201 XT 1.0 R0982 DB04.2
75 26NL 1202 XR +1.0 R0982 DB04.2
-XC BSMT EQPT RM 100 N. BROADWAY BP41/42
25 19NL 12 XT R0099 DB00.3
25 19NL 22 XR R0099 DB00.3
1104
CO SWSL
DSGNR RDB/314-555-1212
ISS 002/11-04-83
PG C001-002

SPECIAL SERVICE CIRCUIT DETAILS (CONTINUED)
CKT 41/IBTS/12345
/SW
A STLSM001
--Z
STLSM022
LEASE
ORD SLC123456
-001
SUPP A
ACTN A
CAC SSR9XD2
MCO
STLSM009TRO
CUST ABC CORP
RRI 15
MSC N
PRQ SSM
RSP
BTN 201-221-4722
CUS 123
CCON 201-221-3272
ACNA XXX
IMC 201-555-4722
N/LOCN, EQPT AND FAC
FRAME ID
UNIT
SV
Z-A A-Z
MISC
NCTE
8D29CABA
GR 6.9/PT 7.0/
EQ=359A/A1C3D14
SC
NCI 4WLA2XXX 10TH FLR TEL RM 100 N. BROADWAY BP25/26
SCA XYZ CORP
100 N. BROADWAY, ST. LOUIS
201-221-1234
1 /19GA/ /22GA/ /24GA/ /26GA/1.0 /BT
2 /19GA/0.1 /22GA/ /24GA/ /26GA/ /BT
1104
CO SWSL
DSGNR RDB/314-555-1212
ISS 002/11-04-83
PG C002-002

SPECIAL SERVICE CIRCUIT DETAILS (CD)

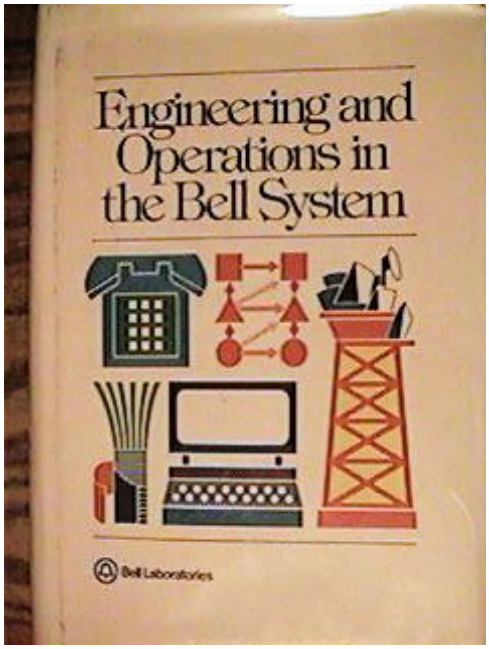
1. Circuit Identification
2. A Office Location
3. Z Office Location
4. Lease
5. Order Type & Number
6. Supplement Indicator
7. Activity Type
8. Circuit Access Code
9. Maintenance Control Office
10. Customer
11. Rebate Required Interval
12. Minimum Service Charge
13. Protection Required
14. Restoration Priority
15. Bill to Number
16. Customer Code
17. Customer Contact Tel. No.
18. Access Customer's Name Abbreviation
19. Inter-Exchange Carrier's Maintenance Tel. No.
20. Circuit Layout Order
21. # of Items (associated with CLO)
22. Locations, Equipment & Facilities
23. Frame Identification
24. UNIT (contains the number of the unit assigned for each hard-wired component)
25. Network Channel Interface Code
26. Owner (of FAC/EQPT, when leased from a company other than the BOC)
27. CLLI
28. Broadcast Date
29. Issuing Company Code
30. Designer & Designers Telephone Number
31. Issue & Issue Date
32. Page Number
33. Transmission Levels from Z-A and A-Z
34. Network Channel Terminating Equipment
35. Network Channel Interface Code and Point of Presence (POP)
36. Station Customer's Name

36A Station Customer's Address

36B Station Customer's Contact Tel. No.

37. Type & Direction of Pulsing
38. Signal & Voice Path
39. Local Cable Makeup.

One of the Reasons Why Real Hackers Check Out Used Bookstores:



I was searching one of my regular used bookstore haunts a few days ago, and found this little gem in the "technical" section next to two copies of the DuPont Blasters Handbook (the definitive guide for the practical applications of high explosives). I already had a copy of the Blasters Handbook (also purchased at a used bookstore), so I bought this instead. This is the third Bell System publication that I have acquired at a used bookstore, and the latest of I can't recall how many decent technical publications.

The morals of this story are as follows:

- There are good reference materials out there that you won't find on the fucking Internet.
- Turn off the damn computer once and a while.
- Go outside and explore the real world.
- Go learn something.