The SOURCE III

6809 Disassembler & Assembly Language Source Generator

COCO III 128/512K SYSTEM

CER-COMP LTD.
5566 Ricochet Ave.
Las Vegas, Nevada 89110
(702) 452-0632

The "SOURCE III" manual index

SOURCE III - Disassembler & Source Code Generator

Introduction

The SOURCE is a machine language program which enables the user to examine and/or disassemble un-protected machine language programs on disk or in ROM space. It will allow the user to take a machine language program or subroutine and create an assembly language source file to a disk or printer. This can be extremely helpful for learning how machine language programs work as well as enable the user to modify or relocate machine language programs for which the assembler source is not readily available. The source code files generated by the SOURCE are standard motorola format ASCII files. Which can be loaded, edited or examined by most text editors, word processors and even by a Basic program.

The SOURCE can also be used to generate your own disassembly listing of the Basic Roms in the Color Computer. You could print out the complete listing and use the comments that have been published in several of the magazines to make a complete commented source listing of the Roms. You could also disassemble some of the subroutines, such as the RS-232 drivers, to learn how the RS-232 port works or to modify the routines to use in your own programs.

The entire program is menu driven, with mostly single key commands for quick easy, operation. For most commands, additional prompts are displayed to instruct the user as to what type of information is expected. In many cases, if you wish to abort the command or return to the main menu, all you have to do is press the <ENTER> key. For the most part, the main menu and command prompts will supply you with enough information to run the program without any difficulty. But we advise that you should read thru the manual at least briefly, before using the program. The manual is not very lengthy or complex, because the program is self prompting and fairly easy to use. The manual is only really needed for initial startup and occasional reference.

SOURCE III - Disassembler & Source Code Generator

STARTUP PROCEDURES

The SOURCE is a 6809 machine language program written for use on a Disk Extended Basic Color Computer with at least 32K of RAM. To execute the program, place the original disk in your drive and enter LOADM "SOURCE3"<enter>. This will cause the program to be loaded into memory and automatically executed. The program will then initialize itself and come up with the main program menu displayed. You are now ready to begin examining or disassembling a program. Be sure to remove the original disk from your disk drive as it is no longer needed at this point.

If an error should occur while trying to load the program, check the disk directory to make sure you are using the correct file name as listed in the disk directory. Also, make sure you are using the Original disk and not a backup copy, as it is only used to restore the original disk as described in the backup procedures.

Backup Procedures

As soon as you receive this program you should immediately make a backup copy using the "BACKUP" command. This is for your protection. Should the original disk fail for some reason, use the "Backup Disk" you created to restore the original disk. Put the backup disk in a safe place. Do not write on the original disk as this might destroy the contents of it or possibly any other disk in an active disk drive. The only way the original disk should be written on is with a "BACKUP" command using the backup disk you created from the original.

If you are unable to restore the Original disk due to physical damage etc., return the Original disk only, to Cer-Comp with a check or M.O. in the amount of $2.50. We will replace the disk and ship it back to you within one working day.

SOURCE III - Disassembler & Source Code Generator

Main MENU Commands

Main Menu Display

After the program has been successfully loaded and executed, you will see the main menu appear on the screen. This menu will also appear after the completion of specific commands or functions. This display also contains some status information, which can be very useful. On the bottom left side you will see the BEGIN, END and EXECUTION addresses of the current Binary program displayed. On the bottom right side you will see the Byte Mode status, Printer On/Off status & Baud Rate, and the Video display On/off status. These will be explained in more detail later in the manual.

The upper portion of the display contains the program name and copyright message and the Single Key Command list. The center portion of the screen contains a list of Commands, with the first character of each command word highlighted (reverse video). These highlighted characters are the Single Key Commands. To execute any of the commands displayed, just press the key that corresponds to the highlighted character in the command word. For example to change the Video Display mode you just press the "V" key. The command will be executed and the display will be updated to reflect the change. If you press the "R" key (Rate for Printer command), you will be prompted to enter the baud rate desired. If you press the "D" Directory command you will be prompted to enter the drive number that you want the directory for, and so on.

As you can see from this brief explanation, most commands are fairly easy to use. Some commands require a little more knowledge of what you want to do, such as the Memory range and Auxilary File commands. It is best not to experiment with these commands until you understand what they are for and how they are used.

```
::::::::::::::::::::::::::::::::::::::::::::
: 'THE SOURCE III'  CODE GENERATOR V3.0    :
:     COPYRIGHT (C) 1987 BY CER-COMP       :
:        single key command menu           :
: Source disassemble      Memory range     :
: Input file setup        Kill disk file   :
: Printer output on/off   Video options    :
: Offset value            Xecution add     :
: Const fcb,fdb,fcc       Directory        :
: Hex/ascii dump          Rate (prn)       :
: List tables             Quit             :
: Fast disassemble        New              :
:                                          :
: START=$0000          BYTE MODE = MULT.   :
:   END=$0000          PRN.  off   9600    :
:  EXEC=$0000          VIDEO on            :
:Offset=$0000          COMMAND > _         :
::::::::::::::::::::::::::::::::::::::::::::
```

SOURCE III - Disassembler & Source Code Generator

Main MENU Commands

Single Key Commands

Input file setup - "I"

The Input file setup is most likely one of the first commands that will be used when examining or disassembling a binary file. After the "I" command is entered, you will be prompted for the name of the binary input file. The name is to be entered just like any normal file name, including the extension and drive number. If you decide you don't want to setup a binary input file, or hit the command key by mistake, just hit the <ENTER> key only and you will be returned to the main menu.

If you enter a file that cannot be found, or any other error occurs, you will be notified and returned to the main menu.

If all goes well, and the file is a normal LOADM format machine language program, the SOURCE will proceed to map out the program and display the beginning & ending addresses of each segment of the program. When done, the program execution address will be displayed and you will be prompted to return to the main menu. When you return to the main menu, you will notice that the Start, End, and Execution addresses for the program are now displayed on the main screen.

Once the Binary file is mapped out, you have several possible options. If this is a new program you are working on, it is necessary to identify all areas of the program according to their use, data, constants, variables and text. This is necessary so that the source code generated will represent the binary program as closely as possible to the way it was originally written. It is probably best to use the Hex/ascii dump command to locate any constant data and text areas in the program. You could also use the Fast disassembly command to get a quick look at the code generated to see if it produces FCB's in areas not designated as such. This is a good indication that those areas are not normal instructions, but should be FCC, FCB or FDB's. When located, use the Constant bytes command to classify the type of area and the address range it encompasses. This process may take several attempts before the code generated correctly represents the original assembler code. There are several commands in the SOURCE to help you with this task.

SOURCE III - Disassembler & Source Code Generator

Main MENU Commands

Hex/ascii dump - "H"

The Hex/Ascii dump command can be very helpful in locating areas of a binary program that are not instructions, but constant data or text. When using this command in conjunction with the video display, it will generate a four digit hex address on the left side of the screen followed by 8 bytes of hex data. The line immediatly following, will display the ASCII equivalent characters underneath the hex data byte. This is probably the fastest method available for locating FCC text areas in a program.

When working on a new program, it can be very helpful to make a dump of the program on the printer. When used in conjunction with the printer, the dump format will differ slightly from the video display. It will display the 4 digit hex address followed by 16 bytes of hex data, and then by the 16 ASCII equivalent characters off to the right side of the page. This format is much more compact and handier when working on larger programs. It is also easier to spot constant text areas when using this format.

In order to obtain a Hex/Ascii dump on the printer, just use the "P" command to enable output to the printer. When the main display status shows the printer as being on, just press the "H" key to start the printer dump. If you would like to suppress the video display, use the "V" command to disable its output before the "H" command.

When using the Hex/Ascii dump command you can pause the display or printout by pressing the "Break" key, or using the Shift "@" key (the same as Basic). If you want to abort the dump and return to the main menu before the command completes, you can terminate it by pressing the "." key. You will then be prompted to hit the enter key to return to the main menu.

Constant bytes - "C"

The Constant bytes command is used when you want to classify a range of addresses as either FCB (form constant bytes), FDB (form double bytes), FCC (form constant characters) or Skip (skip over data). After you enter the single key command "C", you will be prompted to enter either a "B" for FCB range, "C" for FCC range, "D" for FDB range or "S" for skip range. If you enter any key other than one of these three you will automatically be returned to the main menu. If you enter one of the three requested keys, the program will display the function you selected FCB, FCC, FDB or SKIP and request the starting address. When entering the addresses, the program assumes that all addresses are entered in hex notation. It will accept up to 4 numbers for the address, if a space or enter key is pressed, it will assume that is being entered to terminate the number. If any key is entered other than 0-9 and A-F, an error will be displayed and you will be prompted again for an entry. If the begin address is larger than the end address or both addresses are zero, the entry will be ignored and control returned back to the main menu.

If your entry was valid, you will be prompted again for another range of address to be classified. The process will continue until you enter an illegal classification key (B,C,D), or you enter a range of 0 for the addresses. You can exit back to the main menu at the prompt, by simply pressing the <ENTER> key. The following is an example of a sample session using this command.

```
COMMAND > C
ENTER FCB, FCC, FDB, SKIP (B,C,D,S) - C
FCC BEGIN - 100<SPACE BAR>
FCC END - 1FF<SPACE BAR>
ENTER FCB, FCC, FDB (B,C,D) - B
FCB BEGIN - 1000 <automatic entry after 4 digits>
FCB END - 102F
ENTER FCB, FCC, FDB (B,C,D) - <enter> exit to main menu
```

Video options - "V"

This command will cause an additional single key command table to appear that tells you the current printer & video status and allows you to do several things.

```
::::::::::::::::::::::::::::::::::::::::::::::::
:   Video Display & Printer option menu        :
:                                              :
: V - Video Display on/off  - ON               :
: B - Baud rate for printer - 9600             :
: P - Printer output on/off - OFF              :
: W - Screen display - 6 = 40col/225res        :
: C - Video display colors  - 0/63             :
: L - Load screen & printer Setup              :
: S - Save screen & printer Setup              :
:                                              :
: OPTION CHARACTER OR <ENTER>  ?_              :
:                                              :
::::::::::::::::::::::::::::::::::::::::::::::::
```

The Video and Printer ON/OFF commands work the same as the "Printer ON/OFF" command. The Baud rate command "B" allows you to select a printer baud rate the same as the main menu command "Rate".

The Width command "W" allows you to select a desired display format for the program. When selected it will prompt you to select a display width value between 1 and 8. The values from 1-4 select a display width of 32, 40, 64 or 80 columns in 192 Resolution. The values of 5-8 select the same display widths of 32, 40, 64 or 80 columns in 225 Resolution. The default setup on the original disk is 40 columns in 225 Resolution. If you change the width the menu will display the new display mode selected, but will remain in the current display mode until you return to the Main Menu display. Some of the displays for commands like "Directory" and "Constant range Edit" will use a special display mode, but most others will use the selected format.

The Color command "C" allows you to select the desired foreground and background colors for the display. When you enter the "C" command, you will get a message to use the Left, Right, Up and Down arrow keys to change the foreground and background colors. As you change the colors the menu will display the current values selected for colors and the screen colors will change accordingly. When you have the color combination you like best, press the "Break" key to return to the command prompt.

The last two commands allow you to Save and Load the Screen & Printer configuration. If you Save a configuration setup, it will be written to a file called "SOURCE.SET". This file is used at program startup time to automatically configure the program display & printer baud rate to your selected configuration. You can change the automatic or current configuration at anytime you like. The Load command will only look for the file "SOURCE.SET" to load a configuration, you can not specify a file name. This would only be used if you wanted to re-load a configuration from another disk or to restore the configuration to the original startup configuration from the "SOURCE.SET" file.

SOURCE III - Disassembler & Source Code Generator

Main MENU Commands

Printer On/Off - "P"

The Printer command is a simple flip-flop commands that toggle the state of the printer output. Each time the command is executed the condition is flipped to the opposite state and the main display is automatically updated. If you were to enter a "P" at the command prompt after the initial program startup, you would see the printer output status go from an "OFF" to and "ON" condition after pressing the key the first time. If you press it again, the status would flip back to the "OFF" condition and so on.

It can be handy to disable or enable the video and printer output, depending on what you are doing. When doing a Source disassemble, you can leave both the video and printer output off and it will allow the program to run all that much faster. When doing a disassemble with the video off, the current address of the disassembly will be displayed on the screen to the right side of the "Begin Pass 2" message.

Rate for printer - "R"

The Rate for printer command allows you to select a baud rate other than the standard 600 baud default rate. When you enter the "R" command, you will be prompted to enter the desired baud rate. There are 6 possible rates that can be entered: 300, 600, 1200, 2400, 4800, 9600. If a value is entered other than one of these six, an error message will be displayed and you will be prompted to return to the main menu. If you enter one of the legal baud rates, the command will automatically return to the main menu and the new baud rate will be displayed next to the printer status in the lower right corner or the screen.

```
COMMAND >  R
RATE FOR PRINTER - 9600 <automatic end at 4 digits>
```

List tables - "L"

The List command will display the name of the current binary input file and it's memory map if any. If an input file has not been defined, it will show the Begin and End addresses that were entered by the Memory range command. Following that, it will begin to display the map entries for the Constant data areas (FCB, FCC, FDB). Each entry will display what type of entry it is and the begin and end addresses of the area. If there are more than 10 entries in the map, it will scroll the screen up and continue displaying all the entries in the table. If this happens, you can pause the display by pressing the "Break" or Shift "@" key, it will continue by pressing any other key.

Once all entries have been displayed, you will be prompted to either return to the main menu by pressing the <enter> key or if you want to edit the Constant data table entries, to press the "E" key. Below is a sample display of the List tables command.

```
COMMAND > L
```

the screen clears & the following is displayed

```
::::::::::::::::::::::::::::::::::::::
: BINARY FILE = TEST.BIN:1           :
: DISK FILE MAP                      :
: 2700 - 2937                        :
:                                    :
:    FCB & FDB MODE = MULTI.   :
:    FCB, FCC & FDB AREA MAP         :
: FCB 2739 - 275F                    :
: FCC 2833 - 284F                    :
: FDB 2890 - 28FF                    :
: HIT e TO EDIT OR enter FOR MENU    :
:                                    :
:                                    :
::::::::::::::::::::::::::::::::::::::
```

Editing the Constant Area entries

If you elect to Edit the Constant data entries by pressing the "E" key, the screen will clear and a short option menu will be displayed at the top of the screen followed by the first table entry's type (FCB, FCC, FDB) and the begin and end addresses. To the left of the entry, you will see a number that tells you which entry number you are currently working on.

The program will now wait for you to enter one of the command keys that are highlighted on the display, any key entries other than the ones specified will be ignored. If you enter an "E" command, you will exit from the table edit function back to the main menu. You can use the up and down arrow keys to scan backward (up arrow) or forward (dn arrow) thru the table. Each time the entry number, classification, begin and end addresses displays will be updated. If you decide to change one of the entries, you must select the classification (B,C,D). If you want to keep the same classification, make sure you enter the same class type as displayed, otherwise the entered class type will be applied. If you want to delete the entry, it is suggested that you enter the address "FFFF" for both the begin and end address. If you decide that you didn't want to change the entry after selecting it, just press the <enter> key at the address prompt, and the entry will remain unchanged. Once an entry has been modified, the next entry in the map will be displayed. This process will continue until the end of the map table is reached, where you will again be prompted to return to the main menu or enter an "E" to edit the table. The following is a sample editing display.

```
HIT e TO EDIT OR enter FOR MENU  E
```

the screen clears and the following is displayed

```
::::::::::::::::::::::::::::::::::::::
:    fcb, fcc, fdb area map edit     :
:                                    :
:   UP & DOWN arrow = PREV/NEXT      :
:   B=fcb, C=fcc, D=fdb, X=end       :
:                                    :
:                                    :
:  0     FCB 2739 - 275F  C          :
:  FCC BEGIN - 2739                   :
:  FCC END - 274F                     :
:                                    :
::::::::::::::::::::::::::::::::::::::
```

The example shows the Edit mode being selected. When the first entry appears, it is changed from a FCB area to a FCC area and the address range is changed from 2739-275F to 2739-274F. The next entry would then have been displayed for editing.

SOURCE III - Disassembler & Source Code Generator

Main MENU Commands

Auxiliary File - "A"

The Auxiliary file command is used to load or save the constant data area map to/from disk. When the "A" command key is first pressed, the screen will clear and you will be prompted for the name of the Alternate Input file. If you hit just the <enter> key, the prompt will change to ask for an output file name. If you hit just the <enter> key again, the command will then proceed to display a list of tables the same as the "L" command.

If you enter an Output file name at the second prompt, the contents of the current Constant data area map will be save out to disk, under that name. This will save the work you've already done mapping out a program, all you have to do is give it a name at the output file prompt. Then when you want to pickup where you left off, select the "A" command and enter the name of the file you saved when prompted for the input file. If an error occurs during the disk i/o, an appropriate error message will be displayed and control returned to the main menu. When a file map is loaded from disk successfully, the command will automatically display a list of tables, the same as the "L" command.

Byte mode FCB/FDB - "B"

The Byte mode command is available for use with assemblers that do not support the use of multiple FCB and FDB in the source file, such as the Radio Shack EDTASM editor assembler. Most other assemblers including our own will support the use of multiple FCBs and FDBs. Each time the command key is entered, the mode switches between single (sgl.) & multiple (multi). When in the single mode, only one entry will be generated during disassembly, so that those assemblers will not have a problem assembling the generated source files. When in multiple mode, the disassembler will generate eight entries maximum on each FCB or FDB entry. This can save a substantial amount of space in both the listing an source files if your assembler will support it.

Directory display - "D"

The Directory command allows you to display the contents of a disk directory on the video display or printer if enabled. The Directory command will prompt you for the number of the disk drive to get the directory from, if just the <enter> key is pressed the directory from the current default drive will be displayed. If a drive number is entered, it will automatically become the default drive number, and then the directory will be displayed. If an error occurs, an appropriate error message will be displayed and control will return to the main menu.

Kill file - "K"

The Kill file command is similar to the normal Basic kill command. When specifying the file to be killed, the drive will automatically default to the last directory drive, and the file extension will default to .DAT if not specified. When the Kill command is executed, the screen is cleared and you are prompted to enter the name of the file to be killed. If just the <enter> key is pressed, the command is aborted and control returned to the main menu. If a file name is entered the program will attempt to locate the file on the specified drive and remove it. If an error is encountered an appropriate error message will be displayed and control returned back to the main menu.

Quit command - "Q"
New command - "N"

The Quit command is used when you are finished using the SOURCE and want to return to Basic. When the "Q" command is entered you will be prompted to make sure you want to quit the program, if you enter any key other than a "Y" the command will be aborted.

The New command is used when you want to disreguard all current information and start on a new file or program. When the "N" command is entered you will be prompted to make sure you want to restart the program, if you enter any key other than a "Y" the command will be aborted.

SOURCE III - Disassembler & Source Code Generator

Main MENU Commands

Memory range - "M"

The Memory range command is used when you want to disassemble some part of the ROM address space ($8000 - $FEFF). When the "M" command key is pressed, you will be prompted for the beginning and ending addresses. If you enter an invalid address range or enter just the <enter> key for the addresses, the command will be ignored. After both addresses have been entered you will be returned to the main menu and the begin and end addresses will be displayed in the status area.

Offset value - "O"

The Offset value is used when you have a program that you want to disassemble to a new location or one that requires an offset load to work correctly. The value specified is added to every reference address found during disassembly. Beware of lookup tables that use Double Byte references for executable sub-routines & modules.

Execution address - "X"

The Execution address may be specified separately or changed by the use of the "X" command. When the "X" command key is pressed, you will be prompted to enter the execution address for the program. If the <enter> key only is pressed, the command will be ignored. If an error is encountered while entering the address, an error message will be displayed and you will be re-prompted for the address.

End address - "E"

The End address command is not displayed on the main menu since it is not used very often. When the "E" command is entered, you will be prompted to enter the end address for the program. If the <enter> key only is pressed, the command will be ignored. If an error is encountered while entering the address, an error message will be displayed and you will be re-prompted for the address.

SOURCE III - Disassembler & Source Code Generator

Main MENU Commands

Fast disassembly - "F"

The Fast disassembly command is used to do a simple one pass disassembly for the input program. No labels will be generated during a Fast disassembly, it is used mainly to help locate constant data areas in a program, and for testing of the areas that are mapped in the constant data area table. It is equivalent to the output of most Basic disassembler programs. If the printer is on, it will output to the printer. Once the "F" command is entered, the program disassembly will begin immediatly. To pause the display or printer press the "Break" or Shift "@" key, to continue press any key. To stop the output and return to the main menu, press the "." key.

SOURCE III - Disassembler & Source Code Generator

Main MENU Commands

Source disassembly - "S"

The Source disassembly command is the main reason for using the SOURCE. It is a two pass disassembler, that builds a table of all the label references used in the binary program. When the first pass is completed, all the label references are sorted into an assending sequence before the second pass is actually begun. During the second pass, the SOURCE will automatically generate labels in the required locations of the program. These labels have the form of "L"+hex address of the label. This means that all labels referenced in the program will start with the letter "L" followed by a 2 or 4 digit hex address. For example if the binary program makes reference to memory location $1000, the SOURCE will generate an equate label that looks like "L1000 EQU $1000" in the beginning of the listing. All program instructions would then reference address $1000 by using the label "L1000" such as "LDX #L1000" or "FDB L1000". This way, the source file generated by the SOURCE can be fed back into an assembler program, and the assembler will produce code that corresponds to the same memory addresses.

When the Source disassembly command key "S" is pressed, the screen will clear and you will be prompted for the name to be assigned to the output file. If only the <enter> key is pressed, no output file will be generated. This can be helpful for doing trial disassemblies of long complex programs to make sure that all areas of the program are classified correctly so the source file generated, is as close to the original source as possible. If a file name is entered at the prompt the extension will default to .DAT if not specified, and the output drive will default to the last directory drive if not specified.

During the first pass, the SOURCE will display the current disassembly address on the screen, to the right of the "Begin pass 1" message. That way you have some idea the the program is actually working and not just fooling around. When the first pass is completed, the "Begin pass 2" message will be displayed, followed by a message stating that "xxxxx" label references are being sorted. This could take anywhere from 1 second up to about a minute if there are over 1000 label references to be sorted. Once the sorting is finished, the SOURCE will begin to create a disk assembly source file if the output file name was entered, other wise the source output will only be displayed on the screen or output to the printer. If the video display is disabled, the current disassembly address will be displayed on the screen, to the right of the "Begin pass 2" message, the same as during the first pass. Once the second pass is started and an output file has been opened, the "." key will not stop the disassembly.

SOURCE III - Disassembler & Source Code Generator

The "SOURCE" Disk file descriptions

The original disk provided contains several files that are not mentioned in the documentation. The files are demonstration program files to show you a little bit about the program. A list of the file names and a brief description follows.

```
SOURCE3 .BIN - This is the "SOURCE" program  (LOADM)
DEMOPROG.DAT - Original assembler source of DEMOPROG.BIN
DEMOPROG.BIN - Machine Language demonstration program.
DEMOPROG.MAP - The "SOURCE" map of DEMOPROG.BIN" FCC's & FCB's
DEMOPROG.SRC - Source code of DEMOPROG.BIN created by the SOURCE.
DEMOPROG.RSD - Same as DEMOPROG.SRC created for R.S.  EDTASM
LISTFILE.BAS - Basic program to list ASCII files on screen.
SOURCE  .SET - Setup file for Video width, colors, baud rate etc.
```

SOURCE3.BIN is the "SOURCE" binary program file, this is the file you LOADM to startup the "SOURCE". See the manual for more information.

DEMOPROG.DAT is the original assembler source file used to create the binary program DEMOPROG.BIN. It was included so you could compare an original listing to the one generated by the "SOURCE".

DEMOPORG.BIN is the program that was generated from the source file DEMOPROG.DAT, by an assembler. It is a standard LOADM machine language program, the same as any other normal machine language program.

DEMOPROG.MAP is a file that was created by the "SOURCE" to save the mapping information used to generate the files DEMOPROG.SCR and DEMOPROG.RSD.

DEMPROGR.SRC & DEMOPROG.RSD are two source files that were generated with the "SOURCE". The first one .SRC was generated using the standard Motorola format for assembly language source programs (multiple FCB's, FDB's and no line numbers). This format is compatible with just about all assemblers, except for the R.S. EDTASM editor/assembler. The second file was generated in a format for the R.S. EDTASM program. It includes line numbers and single entry FCB and FDB directives. Either format can be used with the CER-COMP EDT/ASM III assembler.

LISTFILE.BAS is a short Basic program that was provided so you could see the files that were generated by the "SOURCE" as well as the original assembler source file DEMOPROG.DAT. It might be helpful to see what the original assembler source file looks like and to compare it to the Disassembled Source files generated by the "SOURCE".

SOURCE.SET - This is the automatic configuration setup file used at program startup to setup the display format, colors and printer.

SOURCE III - Disassembler & Source Code Generator

A Short Tutorial on using the SOURCE

The "SOURCE" is a Disk based Disassembler and Source code generator. It allows you to disassemble and generate assembler compatible source files from a binary program file on disk. Most other disassemblers have to have a program loaded into memory before being able to disassemble the program. This requires that the user know the begin, end and execute address of the program to be disassembled and to offset load the program so it does not interfere with the disassembler. Well the "SOURCE" makes disassembling disk files easy, since it works directly with the program from disk. It does not require you to know any more about a program on disk other than its file name. The following is a short tutorial on how to use the "SOURCE".

Load the "SOURCE" from the original disk by entering LOADM"SOURCE"<enter>. Once the program is loaded, it will automatically execute and the MENU screen will appear. All of the Single Key commands are highlighted on the screen, to use on of the commands all you have to do is press the key for that command.

To start with, press the "I" key to setup an Input file, the screen will clear and you will be prompted to enter the name of the file to be disassembled. Enter the following: DEMOPROG:0<enter>, if the original disk is still in drive 0 it will proceed to check out the file name entered. If it is a standard format binary program file, the program will proceed to map out the file and display its memory address and execution address. If it is not a normal program file the program will tell you so and prompt to return to the main menu. Once the file has been setup and no errors have occured you will be prompted to return to the main menu.

At this point you have several options, you can do a Fast disassembly, Hex/Ascii dump or do a Source disassembly. Since this is you first time working with this input program, it would be best to use the Hex/Ascii dump to examine the file and find the areas that contain Ascii data (text) and map those out first. Press the "H" key to start a dump, if you have a printer, it would be much easier to examine the dump if it was output to the printer. To enable the printer output, just press the "P" key. You will see the screen get updated and it will now show that the printer is ON. Now if you press the "H" key the dump will go to the printer as well as the screen. If you are just using the screen, you can press the "Break" or Shift "@" key to pause the display. If you press the "." key it will cause the dump to end immediatly. On the dump you will see a four digit hex address on the left followed by 8 bytes of data from the program (16 on the printer) and the Ascii equivalent data is displayed underneath each character (to the right side on the printer output). You will notice that some of the characters show "."'s, these characters do not have printable Ascii equivalents. If you look

carefully on the dump, you will notice that the word "ENTER" is displayed starting at location 3039, this is the beginning of a text area in the program. It extends up thru 3068. This is a "FCC" form constant character text area of the program. To map it out for the program, you would press the "C" key at the command prompt for "Constant data". You will then be prompted to enter what type of data it is "FCB, FCC or FDB (B,C,D)", press the "C" key again to signify you are specifying "FCC" data. You will then be prompted to enter the begin address of the FCC area, enter 3039. After the fourth digit is entered, it will automatically prompt you for the end address, enter 3069. You will now be prompted to see if you want to enter any more areas, if not just press "Enter". Since we were looking carefully we noticed that there were 3 bytes of data 0D, 0A and 04 which followed the text, this is a FCB form constant byte area. Enter a "B" at the constant data prompt, you will then be prompted to enter the begin address of the "FCB" area, the same as you did for the FCC. Enter 3069 and then 306B, when prompted for more constant areas, press "Enter".

Once back at the main menu, press the "L" key, this will list the memory map of the program and show you the areas that have been entered as constant data areas. If you made a mistake entering the FCC or FCB areas, you could press the "E" key and edit the entry in error, see the manual for more details on editing. For now we will assume that everything was entered correctly, press "Enter" to return to the menu. Now you can do a Source disassembly to see what it looks like, press the "S" key. The screen will clear and you will be prompted to enter the name to be assigned for the output disk file, jsut press the "Enter" key (no output file will be generated). The "Begin of Pass 1" message will appear with some numbers displayed to the right of the message. This is a visual indication that the disassembler is working, it shows the address of each instruction as it is being disassembled. The address display appears with some address digits in reverse video, this is normal. The display was made this way because it is much faster than printing the address, which would slow down the program. When the first pass is done, it will display a second message indication the start of pass two and that the program labels are being sorted. For the demonstration program it will happen very quickly, you might not even see it unless you pause the display. If you pause the display or get a hard copy of the disassembly you will notice that the message "** BAD OP **" is displayed after the FCB at address 3038. This is the disassemblers way of telling you that this area of the program may not be mapped correctly. You can go back and add a constant data entry from 3038 to 3038 using the "C" command and the "B" FCB type. You could also go back to the map listing using the "L" command and edit the first FCC entry to start at 3038 and end at 3068. If a FCC mapped area contains data that is not a printable character, they will automatically be changed into

FCB statements.

If you were finished mapping the program and wanted to save the infromation entered you could press the "A" key for alternate file saving and loading. When you press the "A" key you will be prompted for the name of an INPUT file that was previously saved. We already have a file out there called DEMOPROG.MAP that was the map we used to create the DEMOPROG.SRC file. Enter DEMOPROG.MAP:0 at the input prompt to load the map, once loaded it will display the information map the same as the "L" command. If you want to save a map you created, press the "Enter" key at the input prompt, you will then be prompted for the name to be assigned to the output file for the current map. If you press "Enter" again, the command will be aborted.

If you load the file DEOPROG.MAP, you will notice that we mapped the FCC area starting at 3038 thru 3068 and the FCB area at 3069 thru 306B, the only difference is that the last 3 bytes would be mapped as individual FCB's instead of a single FCB with 3 entries (multiple FCB mode). This is a perfectly legimitate way to map text, since most text areas will have some non printable character used at the end of each text segment to signify the end of a line when printing etc. See the original source listing DEMOPROG>DAT for an example of how this is normally done in a program.

You may have noticed the "M" memory range command in the menu, this command is used for disassembling the memory resident ROMS. It allows you to specify any part or all of the ROM space in the computer. It will not allow you to enter any addresses below 8000 since the only program that can reside in low memory is the SOURCE itself.

The Directory and Kill commands are used for displaying a disk directory and Killing files on disk. If you would like to get a printout of the disk directory, enable the printer with the "P" command before using the "D" directory command. The Kill command is similar to the normal Basic Kill command, when prompted, specify the file name, extension, and drive where the file is to be deleted.

If you are going to use the "SOURCE" to work on more than one program in a single session, use the "N" new command. This will clear all the old information out of the program and start you off with a clean slate. When you are finished using the program and are ready to return to Basic, use the "Q" quit command. It will automatically prompt you to be sure you want to exit from the program, just enter a "Y" when prompted.

Well thats about it, I know it was short, but it should get you started using the SOURCE without too much trouble. For more

information on some of the commands discussed, refer to the manual. If you are new at disassembling don't be too suprised if it takes several passes at disassembling a program before it all looks right, this is normal. Even for an experienced disassembler user it takes several attempts before it comes out right. Happy Disassembling!!!