

Megamon

Megamon is a sophisticated disassembly/monitor which will work on the complete range of Amstrad machines. Among its many features are an intelligent move memory facility, control over the lower Rom state, machine code trace, read or write object code to tape or disc, full memory dump to the printer, and a disassembly that will even understand all of the 102 undocumented Z-80 instructions. All of the controls are accessed through single key-presses so Megamon is easy to understand and simple to use.

Listing 1 is the short loader program for Megamon. Type this in and save it as the first thing on your tape as "MEGLoader". Listing 2 is the standard two-located program which points to the hex code from DATA statements. When all the bytes have been successfully entered then the loader program will prompt you to hit any key which ready to save the code. Entry your tape is positioned after the megamon Basic loader.

To run the program typed the tape and type the "MEGLoader". When the program has loaded the first screen will appear and you will be asked for an address at which to load Megamon. This can be any address from 4000H up to 9000H. Obviously the monitor will not work if loaded underneath the lower Rom.

Once the address has been entered the object code the Megamon is loaded and you will be presented with Megamon's Front Panel screen display:

Laurie Smart's monitor takes you places you've no right to see in your Amstrad.

Z80 Register — The top right of the screen shows the Z80 register AL,BC,DE,HL,IX,IXH together with the stack pointer (SP) and the program counter (PC). The register contents are shown (at starting these are always zero) and then the contents of the memory location addressed by that register; there is also the register name P, T, which points to AF on start-up. It's not all to be done so shortly.

Lower Rom State — Below the register display the state of the lower rom is shown, either Enabled or Disabled.

Memory Display — The memory display occupies the bottom of the screen and its purpose is to display the bytes around the memory pointer, indicated by *. The bytes can be displayed either in hex or in ascii.

PC Instruction — The instruction at the Program Counter is constantly displayed above and to the left of the Memory Display.

List Display — The left of the screen shows the Memory Display is taken up by the List Display. At start-up this display will be blank, but if you are eager to see it in action then for the moment press I, followed by a full-stop. You will see the 14 instructions from address zero disassembled for your perusal.

Unfortunately, space does not permit a detailed discussion of the undocumented instructions, needless to say their use is becoming much more frequent in many of today's top games. Disassembler that can cope with them are rare and the format for displaying them varies. For example, look at the instruction ADD A,0.

This means "Add A to the low-byte of IX, the "L" tagged on to indicate the low-byte. Alternatively, you can use ADD A,0xH.

This means "Add A to the high byte of IX, a add A to I. Megamon would display the two instructions above as follows:

The lower in capitals indicates which byte of the register pair is being operated upon. The same applies to all undocumented instructions that use the IX register pair.

There now follows a list of the Megamon keys and a full explanation of their usage.

The First Cursor Arrow — The four corner keys about the function pad are used to move the Memory Pointer "*" within the Memory Display in the appropriate direction, enabling you to step up or down through the memory, or steps of one or eight bytes at a time.

The Full Stop Key — Pressing the full stop will advance the Register Cursor "*" onto the next register pair in the Register Display.

I — Asterisk in Action — Pressing this key will produce the prompt



"Are you Sure?". It is impossible to this point "Y" if you wish to leave Megamon and return to Basic. Any other key press will return you back to Megamon itself. When Megamon returns to Basic it retains the Rom to whatever they were at starting.

C — Clear List Window — The List Window can be cleared at any time by pressing the "C" key.

D — Display Memory — This allows you to change the address around which the Memory Display works. You will be asked for a new address for the Memory Pointer — this must be entered as a hex number (omitted by a \$) or a decimal. If, instead of a hex number, you

Listing 1.

```

100 ROMK 1
101 LOADK 0,1,1,PRINT"LAU: Press any key"
102 LOADK 14,0,PRINT"PROGRAM"
103 LOADK 0,1,0,PRINT"LOAD ADDRESS IN CHEEKST"
104 PRINTK 0-1
105 FLOUREST"LOADK 1,0-1,PRINT"Please wait... Loading DATA
106 ROM 0,1,0,LOAD"PROGRAM"DATA"
107 GOTO 10
    
```

Listing 2.

```

100 ROM 0000,0000,LOADK 0000
101 ADDR0-17999,179-1999,HEXSTR 0000-1
102 ADDR0-17999,179-1999,HEXSTR 0000-1
103 FOR A=0 TO 17999 STEP 1000
104 IF A=0 THEN PRINT"
105 FOR B=0 TO 160 STEP 10
106 PRINT A+1 TO A+B,HEXSTR 0000-1
107 NEXT B
108 NEXT A
109 END
    
```

```

1000 PRINT "DATA CORRECT"CHR$(10);PRINT "TIME AND PRESS
1010 A KEY"
1020 GOTO "PROGRAM END"CHR$(10);GOTO 1120
1100 END
1110 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1120 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1130 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1140 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1150 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1160 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1170 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1180 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1190 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1200 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1210 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1220 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1230 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1240 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1250 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1260 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1270 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1280 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1290 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1300 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1310 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1320 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1330 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1340 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1350 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1360 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1370 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1380 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1390 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1400 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1410 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1420 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1430 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1440 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1450 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1460 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1470 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1480 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1490 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1500 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1510 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1520 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1530 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1540 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1550 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1560 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1570 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1580 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1590 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1600 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1610 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1620 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1630 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1640 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1650 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1660 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1670 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1680 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1690 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1700 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1710 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1720 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1730 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1740 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1750 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1760 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1770 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1780 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1790 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1800 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1810 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1820 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1830 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1840 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1850 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1860 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1870 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1880 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1890 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1900 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1910 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1920 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1930 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1940 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1950 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1960 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1970 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1980 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
1990 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
2000 DATA 0000,0000,0000,0000,0000,0000,0000,0000,0000,0000
    
```

press the full stop key then the Memory Pointer will be set to whatever address the Program Counter currently holds.

The address is displayed, along with its contents. You can either enter a new hex number for this location or press the > to exit the memory change. When a new number is entered the memory pointer is advanced to the next location and your options are the same again. At any time during the input of a number you can press the Esc key to abort and leave the Memory Pointer unchanged.

E — Register Lower Show State Press the "E" key and the Lower Box will be toggled between Enabled and Disabled.

F — Find Memory: The prompt "FID" appears and the number entered here will be the start address for the program to use. You are then asked for the address at which the program will end its fill, and finally the hex to fill the memory with. For example, if you enter 8000 in response to "Find F", 8000 in response to "to F", and FF in response to "With F", the memory between 8000 hex and 8000 hex will be filled with FF (255 decimal).

G — Go To: This allows you to locate the object code currently under examination with the use of "breakpoints", i.e. places at which the object code is stopped in its tracks and control returned to the monitor for you to examine the registers etc.

The address which you enter in response to "Go?" will be the address at which the monitor starts execution of the object code. As usual with all prompts, if you press the Esc key then the

operation will be aborted. You can then add for an address — "to F" — at which control will be returned to Megasoft i.e. the address at which you wish your breakpoint to be inserted.

When you have entered this address Megasoft will go off and execute the code. When the breakpoint has been reached, assuming that the code has not caused a fatal crash, a small line will be displayed on the screen and this means that Megasoft is waiting for you to press any key before updating all of its displays.

W — Search For String: The prompt "Search For S" is displayed. You can now enter a sequence of up to 255 hexes which will form the string which Megasoft will search for. Each number should be entered by pressing Return and by pressing Return on its own you will terminate the string.

At this stage, assuming the string can be found, Megasoft will update the Memory Display and the Memory Pointer > will be pointing to the second byte of the input string. Also see the explanation of the next instruction, "C".

A — Find Next Occurrence: Pressing the "W" key will tell Megasoft to find the next occurrence of a string you have searched for using H.

J — Toggle Between Ascii and Hex: By pressing the "J" key you can toggle the Memory Display Memory so that it shows either Hex or the Ascii equivalent.

L — Exit: You can enter a new address from which the disassembler will list its H instructions. However, there are two other alternatives to entering

a new address. If you press the full stop key in response to List then the disassembler will begin from the address currently held in the Program Counter.

Alternatively you can press Return in response to the prompt and the disassembler will continue from where it left off.

M — Move a Block of Memory: The prompt move S will be displayed and the address you enter will be the start of the memory block you wish to move. The prompt "find," asks you for the end address of the memory block and the prompt "to S" asks you for the destination address for this block. The routine is "intelligent" so that if your destination address lies within the limits of the block you wish to move Megasoft takes this into account and performs the move correctly.

O — Append Object Code: This reads a block of object code from its form on tape or disc, depending on which system it is on. You are prompted to enter a filename and then an address at which the code will be loaded. Needless to say, you should take care not to overwrite Megasoft.

P — Printer Disassembly: With this option you can produce a disassembly of any length to your printer, you could even list the Assembled Rom. Then first address you enter in response to "Print," is the start address for the disassembly, and the second address is the end. Assuming the printer is connected a disassembly will now appear on the printer which can be aborted at any time by pressing the Esc key.

X — Change Register: By

pressing the "R" key you can change the value of the register pair currently pointed to by the register cursor >. The register pair will take on the value you enter at the keyboard.

S — Single Step Megasoft: will execute the SINGLE instruction at the Program Counter when you press the "S" key, allowing you to examine the effects of the code upon the registers and memory. This function will also single-step through a Call instruction.

T — Trace: If you press the "T" key Megasoft will execute the instruction at the Program Counter in the same way as the "S" function above, except that using "T" allows you to monitor a Call instruction automatically.

U — Write Object Code: This writes a block of code to tape or disc under a given filename. You are prompted to enter the filename and then the first and last (inclusive) addresses of the block you wish to write.

Z — Register Alternative Register: Pressing the "Z" key will toggle the Register Display between AF,BC,DE,HL,IX and the alternate registers registers APT,BC,DE,IX. You are prompted to enter the values in the alternate register set unchanged as these are in constant use by the firmware (for further details see the Advanced Firmware Specifications — Soft 158, Appendix XI).

If the sight of all these hex types is enough to put you off then copies of Megasoft, mounted on quality blank tapes, are available at a cost of £2.50 each, including postage. From Laurie Simons, 20 Astorian Street, Burley, Leeds LS3.

```
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
1100 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
2200 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
3300 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
4400 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
5500 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
6600 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
7700 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
8800 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
9900 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
A000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
B000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
C000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
D000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
E000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
F000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000

```

```
1100 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
2200 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
3300 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
4400 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
5500 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
6600 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
7700 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
8800 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
9900 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
A000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
B000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
C000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
D000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
E000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
F000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000

```

Continued on next page

