UNIVERSAL DISASSEMBLER v2.3

...author: René LeBlanc

The **Universal Disassembler** offers a unique combination of features to analyze TI-99/4A object code, whether it be in Console ROM, Command Modules, Expansion RAM or on Disk.

In particular, the Diskette analysis features set it apart from any other disassembler package available.

The START screen provides a summary of the major commands available.

> *NOTE: Pause most output with any key.*

> *NOTE: Exit during output with CLEAR (<fctn+4>).*

To **DIS**assemble from memory, enter the low and high addresses in HEX that cover the range to be disassembled. Remember the following ranges:

Hex Range	Description
`0000 – 1FFF`	CONSOLE ROM
`2000 – 3FFF`	LOW EXPANSION MEMORY
`4000 – 5FFF`	DSR ROM—*[The proper CRU points must be set to map different DSRs into here.]*
`6000 – 7FFF`	Command Module Port—*[Note that command module GROM cannot be disassembled normally. If you get all zeros out, it is GROM.]*
`8000 – 9FFF`	Memory Mapped Devices
`A000 – FFFF`	High Expansion Memory

Due to the size of the **Universal Disassembler** and the non-relocatable nature of its **TI Forth** base, it is not practical to try to load another program in along with it (except in the Mini-Memory Module).

The real power of the **Universal Disassembler** lies in its ability to disassemble directly from disk.

The **Universal Disassembler** supports Disk analysis with a number of utilities. **DIR** (a directory function) lets you quickly check the files on the disk in question.

FIL (a file analysis function) locates the beginning and ending sectors of each fragment of a file on the disk.

SSS (Sector String Search) lets you enter any ASCII string up to 80 characters, and will search the disk over the range of sectors specified. If found, the sector # and offset within the sector is displayed. **SHS** (Sector Hex string Search) lets you enter any HEX string with a length from 2 – 80, and will search the disk over the range of sectors specified. **SHS** cannot locate HEX strings beginning in the low-order (right-hand) nibble of a byte.

DMP (a dump utility) lets you dump any sectors to the screen with both HEX and ASCII representations of the information. This is useful to help you determine which of the three object code formats is used, or if the file is 9900 object code at all.

When using the **DIS** function to disassemble from disk, object files may be in any of three formats:

1. Tagged Object (uncompressed)—can be recognized because all fields are in ASCII.

2. Tagged Object (compressed)—has a pattern of ASCII tag fields with intermediate hex data.

3. Untagged Object (saved program)—is all hex data with no regular patterns of ASCII tags.

 Other text or BASIC files exist for which disassembly is meaningless.

The disassembler output has the form:

`AAAA DDDD TT O... S...,D...`

where:

> **AAAA** is the real or virtual address of the instruction or data. You can provide a Relocation Base address to match particular load addresses.

> **DDDD** is the contents of address **AAAA**.

> **TT** is an ASCII Text interpretation of **DDDD** to help you see if **DDDD** might be text data.

> **O...** is the Operation Code.

> **S...** is the Source operand.

> **D...** is the Destination operand.

A screen dump is available at most times, simply by pressing *<fctn+0>* ('fctn' key and '0' key at the same time).

CONFIG (a configuration control utility) is provided, which lets you tailor the program to your system's printer interface and disk configuration. It also lets you set up the screen display colors to your preferred selection.

.CONFIG (print configuration command) will display the current parameters so you can see what you are starting with.

SAVE-CONFIG (save configuration command) will make any changes permanent.

The alternate output commands enable you to define the file descriptor to be used when using screen dumps or operating in the **PRINTER** mode. After selecting one of the commands, you may then type the remainder of the file descriptor selected. Enter will give you what you see. **TO_OTHER** expects you to enter the entire file description for the alternate output device. **TO_DSK** is not yet supported.

To support disassembly from memory, several memory-oriented utilities are provided.

The **SET_DSR** utility lets you switch the memory mapping of **>4000 – >5FFF** to any of the DSR ROMs that are equipped in your system. Then you can **DUMP** or **DIS** (disassemble) from that range.

DUMP lets you dump from any non-VDP addresses.

VDUMP lets you dump from VDP RAM.

REDIRECTION OF OUTPUT TO PRINTER

Type **PRINTER** to direct subsequent non-interactive output to the printer.

Type **SCREEN** to direct all output to the monitor screen.

A **PRNTMODE** command is provided to send various control commands to your printer. This is set up for EPSON/GEMINI printers. This routine is loaded from source on Screen #51. It can be edited with **TI Forth** to support other printers.

In addition to all these utilities, all the power of the underlying FORTH language has been retained. You can interactively perform calculations or other operations in support of your disk and memory analysis.

Following are a few available FORTH commands that could be useful while interacting with the disassembler:

Command	Description
VLIST	Look at FORTH vocabulary
PAGE	Clear screen
PFF	Printer form feed
PLF	Printer line feed
n PLIST	List Block n to printer
n LIST	List Block n
DECIMAL	Change base to decimal
HEX	Change base to hexadecimal
1,2,...	Put any # on the stack
.	Print the top stack number
.S	Print stack contents
SP!	Clear parameter stack
FREE	Check free memory
COLD	Perform cold start
BYE	Exit to main screen

Operational Comments

Due to the fact that TMS9900 instructions may be from 1 to 3 words long, a 3-word disassembly buffer is used when disassembling from disk. This results in a minor side-effect that Assembler Commands, such as **AORG** and **RORG**, may appear out of sequence by a word or two. The address control is compensated so that the address at the left of each instruction or data field is properly scaled, except for the odd case where it can temporarily show as a negative value.

Note that activating the various DSRs prevents access to disk or printer. It is not possible to use the **PRINTER** option when DSRs are activated. Also, selection of **HELP** or other commands that use disk or printer will automatically disable any DSRs that were previously set. This is necessary to avoid system lock-up due to DSR access conflicts. (Sorry!)

> *NOTE: The Screen Dump cannot be used to dump these* **HELP** *screens. Use the* **PRINTER** *mode to list these.*

If you wish to print a screen with DSR memory information on it, follow the following sequence:

1. **DSRSOFF** (disable DSR)

2. **HCPY-ON** (re-enable interrupt)

3. <fctn+0>

This procedure allows printing DSR memory on a screen-by-screen basis. It is not very convenient, but it is better than nothing (ideas for practical alternatives are welcomed). The author keeps a list of all contributing owners of the **Universal Disassembler**. Contributing owners will be notified of significantly improved versions of the **Universal Disassembler**. At any time, contributing owners may send the author a diskette with mailer and postage, and the author will return the latest version to you at no charge.

The author welcomes your comments or questions. He tries to be responsive.