1092

Bell Laboratories

subject: TCMP - A Program for Comparing Program Text After a System Crash

date: April 27, 1976

from: T. M. Raleigh
MF-76-8234-029

MEMORANDUM FOR FILE

When a UNIX system crashes with no console message to indicate the nature of the problem, it is useful to determine whether parts of the operating system have been destroyed as a first step in determining whether hardware is at fault. Tcmp is a program which compares the original text (instructions) of a program with the text of that program in a system crash dump. It can be used to compare the text of the operating system or any user program with the memory image in the crash dump.

In order to compare the text of the operating system, Tcmp knows about the two virtual address space formats for the operating system. One virtual address space format is for versions of UNIX that have Instruction and Data space memory maps while the other is for versions of UNIX that have an Instruction space map only (11/40 processors do not have D space maps and therefore must use this version). The virtual and physical address space for I space only versions of UNIX is laid out as shown in Figure 1. As can be seen from the diagram, the text is in low memory and is followed by the data and bss (uninitialized data) areas. The physical and virtual address space for I and D space systems is shown in Figure 2. Here, it should be noted that the data and bss areas precede the text of the operating system in physical memory. (It should also be noted that because of the granularity of the hardware memory maps on PDP-11's, the text and data must begin at the nearest memory block boundary - 64 bytes per memory block.)

When comparing the operating system text with the image in a crash dump, the user must indicate whether the crash dump is from an I space only system ("-I" option) or an I and D space system. An I and D space format is assumed as a default. The file "/unix" is assumed to contain the object from which the system was loaded, however, a "-s" option allows the name of an alternate object file to be specified.

For comparing the text of a user program with its corresponding image in a system crash dump, the location of

the program in the crash dump and the path name of the user program must be supplied. These can be determined from the Dead command [1]. The Dead command prints a memory and swap map from the crash dump and will give to the best of its ability the names of the programs that were in memory when the system crashed [1]. The memory map lists the addresses in memory blocks and is sorted by increasing location. A sample listing from the use of the Dead command is attached. Reentrant processes have their reentrant and nonreentrant parts managed separately and the Dead command indicates the reentrant text for the command by appending a 'T' to the address. The addresses supplied by the Dead command are those needed by Tcmp to find the text of the program in the crash file. In the case of reentrant processes, the address of the reentrant text ("T" subscripted address) is used as a parameter to Tcmp. With the names and locations of processes in memory supplied by the Dead command, a crash file can be examined systematically to see if the operating system or a user's programs were destroyed.

Tcmp normally prints a summary of the differences between the text and the crash dump. The result of the comparison is to print the absolute address of the first location that differs, followed by a count of the number of succeeding locations that do not match. The "-v" option prints additionally the start address in vitual address terms and the "-t" option causes the start address to be interpreted symbolically from the namelist.

If the contents of the modified locations are desired, there are several options similar to those of the Od command which will print the differences in several formats. In all cases, the modified locations and their original contents are printed on adjacent lines. (The line containing the modified locations begins with a "*".) The following options for printing the contents of locations are available,

-a - as PDP-11 instructions
-o - octal
-d - in decimal
-c - ASCII characters

It should be remembered when using Tcmp that some nonreentrant programs are self modifying and will show differences. The operating system is not reentrant, however, the text is not self modifying so that Tcmp should list no differences.

The value of Tcmp lies in its use to see if any contiguous area of memory has been modified or if a pattern of locations throughout memory have been modified. This situation could be the result of a faulty DMA device on a system or less likely as the result of bad system software. In cases where a UNIX system does not crash gracefully, the

Dead command should be run on a crash file so that a summary of the status of the system when it crashed can be kept and Tcmp should be run at least to compare the operating system text with that in the crash file.

Tcmp can also be used on a running system to insure that the system has not been corrupted. The command

```
Tcmp /dev/mem
```

should produce no differences while the system is running.

Several examples of Tcmp printouts are attached. A comparison of the operating system text with the crash dump produced the listing shown in the attachment. Finally, the init program was compared for differences between its original object and the contents of the crash dump. The crash dump used for these examples is from a system on which many locations through the entire range of physical memory were modified and a DMA device (DQ11 synchronous line interface) was found to be the cause of the problem.

Tcmp with no crash dump file argument is a convenient means of finding out where in physical memory the operating system is loaded.

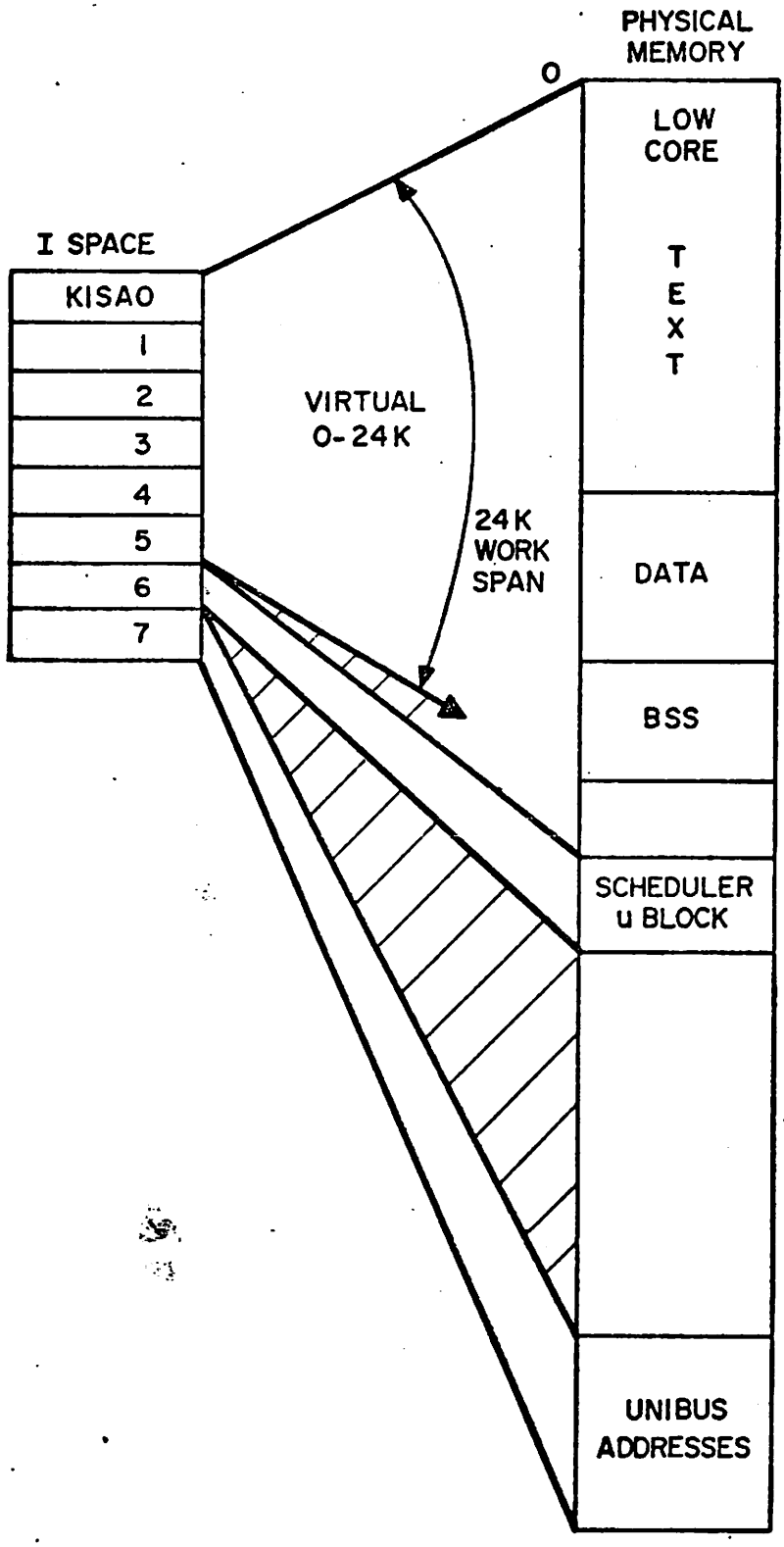
T M Raleigh

T.M.Raleigh

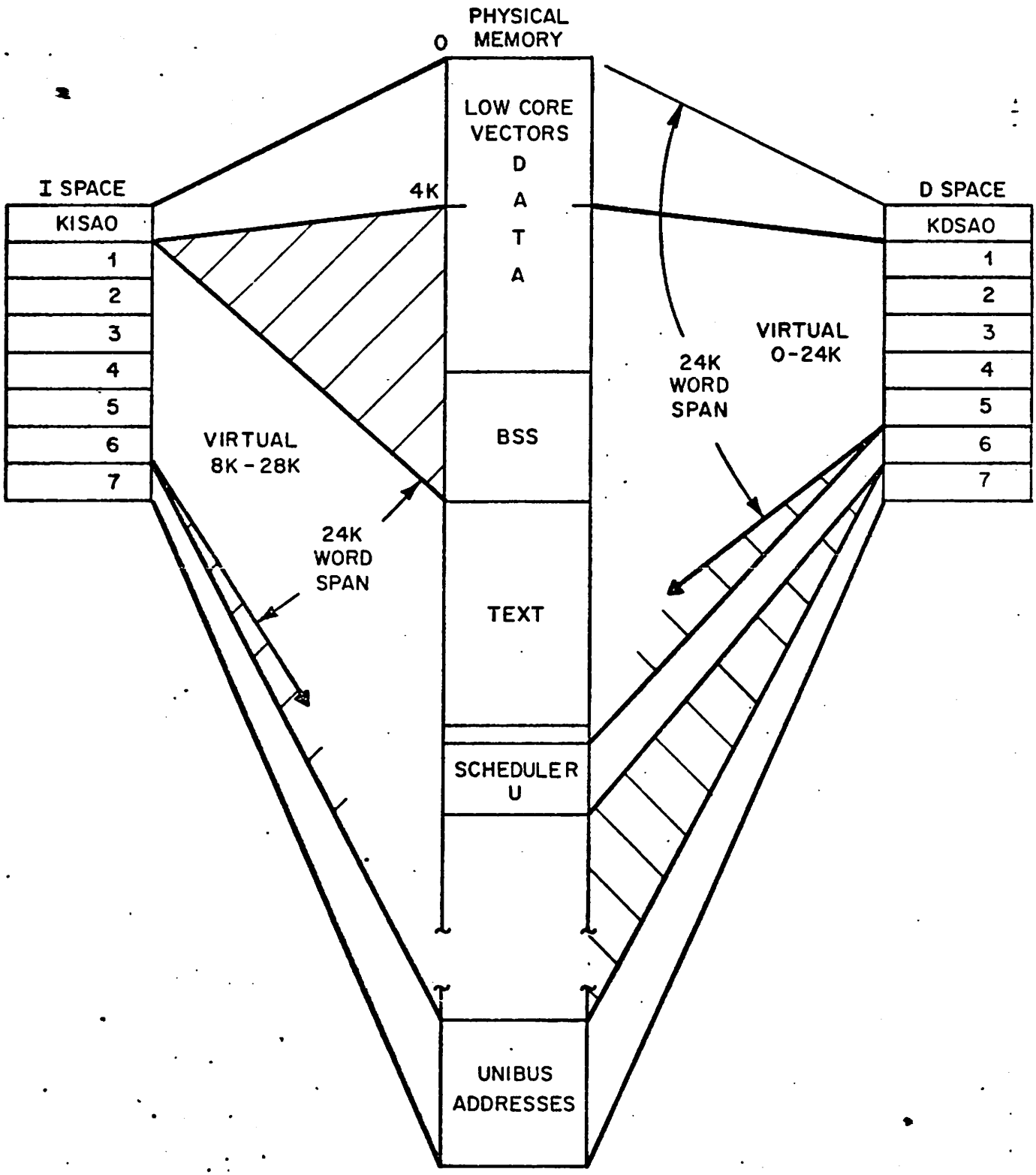
Copy to
G.L. Baldwin
Department 8234
D. Cochran
J. Carran
N. Chaffee
D. Dejager
M. Pilla
P. Kennedy
J. Malik
A. Gross
D. Jackowski
R. Farbanish
S. Arnold
D.M. Ritchie

REFERENCES

[1] Raleigh, T. M., "Dead - A Program for Analyzing UNIX System Crash", MF-76-8234-030, April 30, 1976.



UNIX KERNEL VIRTUAL ADDRESS SPACE
(I SPACE ONLY) 11/40



UNIX KERNEL VIRTUAL ADDRESS SPACE
(I & D SPACE) 11/45, 11/70

NAME

tcmp – text comparison for crash dump

SYNOPSIS

tcmp [**–Iusvtabcdho**] crashfile [offset][.][**m**] [file]

DESCRIPTION

When a unix system crashes with no console message, it is sometimes fruitful to determine whether any parts of the operating system have been destroyed. *Tcmp* is a program for comparing the text (instructions) of a program or the operating system with the text that appears in a crash dump. The differences can be printed in summary form or the contents of the modified and original locations can be printed. There are a number of options which allow the differences to be printed in ascii, octal, etc. and options which allow the address of the differences to be printed in absolute, virtual or symbolic terms. If the values of the differencces are not explictily requested by using one of the format options, only a summary of the differences is printed.

There are several options which select whether a user program or the operating system is to be compared. The default is to compare the text in the file /unix with the crashfile and to assume that the system is in an I and D space format. The options are,

I indicates that an I space only operating system (all 11/40's) is to be compared.

s This option allows the specification of a file other than /unix for the comparison. No offset argument needed when comparing the operating system text with the crashfile.

u indicates that a user program is to be compared. The address (offset) of the user program must be specified and the file name of the user program must be given (see below).

The following options select the type of address to be printed. The default is to print the absolute address. The addresss options are,

v indicates that the virtual address of the start address is to be printed.

t indicates that a symbolic address is to be constructed from the namelist for the start address.

If only the above options are used, a summary of the differences is printed. The summary consists of the absolute address of the first difference followed by a byte count of the number of locations starting at that address which differ. If the **v** and/or **t** options are used, then the start address is repeated and interpreted in virtual and/or symbolic terms. In all cases, when a summary is requested, the absolute memory address and the byte counted are printed.

If any of the following options are used, the contents of the modified locations are printed. The differences are printed as two line pairs. The first line prints what the location should contain and the second prints the contents of the location from the crashfile. (An asterisk is printed at the beginning of each line containing modified data.) The meaning of the format argument options are:

a interprets words as PDP-11 instructions and dis-assembles the operation code. Unknown operation codes print as ???.

b interprets bytes in octal.

c interprets bytes in ascii. Unknown ascii characters are printed as \?.

d interprets words in decimal.

h interprets words in hex.

o interprets words in octal.

The *crashfile* argument specifies a file which contains a system crash dump.

The *offset* argument is used when comparing a user program with the crash file and specifies the offset in the crash file where the text is to be found. This offset can be found by using the **-m** option of the dead(VIII) command which produces a sorted memory map for the crash file.

For nonreentrant programs, the offset is simply the address given by the dead(VIII) command. For reentrant programs, the -m option of the dead(VIII) command indicates where the text is located by appending a T as a subscript to the memory address.

The *offset* is normally interpreted as octal bytes. If '.' is appended, the offset is interpreted in decimal. If an **m** is appended, the offset is interpreted in memory blocks (64 bytes). The address printed by the dead command is in memory blocks.

The *file* argument specifies where the object for the operating system resides when a file other than "/unix" contains the object (s option) or the pathname of a file containing the object for a user program when a user program's text is being compared (u option). *Tcmp* complains if the file specified does not have a namelist and the t option has been selected.

As part of every invokation, *tcmp* gives the absolute and virtual address range for the program being compared.

The command

```
tcmp /dev/mem
```

should produce no differences while the system is running.

SEE ALSO

od (I), pstat (VIII), dead (VIII)

BUGS

The '-t' option is slow.
Crashfiles produced on I space only systems have locations 04-034 modified by the system dump routine.

```
%dead -m sysdump

Time of day Thu Feb  5 03:40:02 1976


                Memory Map
maxmem 2000
    ADDR     RANGE      PID       NAME
       0      0561              Unix Data
     0561      0722              Unix Text
    01503       020        0    Scheduler
    01523      0772      279    /rp4/exsys/tgmon
    02515       045        4    /etc/updat
    02562       017              Free
    02601      0434      280    /rp4/exsys/dscrmon
    03235      0433      282    /rp4/exsys/prmon
    03670      0166      285    /rp4/crt/ctrl/prets
    04056      0110        1    /etc/init
    04166       076      308    testexec
    04264       020              Free
    04304      0151     5301    pgs
    04455        04              Free
    04461      0510      271    /rp4/exsys/dpp
    05171     01431      277    /rp4/exsys/xsys
    06622      0356      275    /rp4/exsys/xpoll
    07200      0266      278    /rp4/exsys/xpb
    07466      0112              Free

                Swap Map
number of swap blocks 3554

    ADDR     RANGE      PID       NAME
     024       023              Free
     047        06     2720
     055        06     2863
     063        06     2859
     071        06     2866
     077        06     2869
    0105       020     2502
    0125       013              Free
    0140       046      272
    0206      0123              Free
    0331       011       16
    0342       050      274
    0412      0212              Free
    0624       022      276
    0646       020      283
    0666      0124              Free
   01012       051      266
   01063     02515              Free
```

```
% tcmp sysdump
sysdumpunix:
I and D      Virtual              Absolute
Data      0000000-0056014      0000000-0056100
Text      0020000-0112104      0056100-0150300
    Absolute
0056176-000002
0056376-000002
0056576-000002
0056776-000002
0057176-000002
0057376-000002
0057576-000002
0057776-000002
0060176-000002
0060376-000002
0060576-000002
0060776-000002
0061176-000002
0061376-000002
0061576-000002
0061776-000002
0062176-000002
0062376-000002
0062576-000002
0062776-000002
0063176-000002
0063376-000002
0063576-000002
0063776-000002
0064176-000002
0064376-000002
0064576-000002
0064776-000002
0065176-000002
0065376-000002
0065576-000002
0065776-000002
0066176-000002
0066376-000002
0066576-000002
0066776-000002
0067176-000002
0067376-000002
0067576-000002
0067776-000002
0070176-000002
0070376-000002
0070576-000002
0070776-000002
0071176-000002
0071376-000002
0071576-000002
0071776-000002
0072176-000002
```

```
%tcmp -vt sysdump
sysdumpunix:
I and D      Virtual              Absolute
Data      0000000-0056014     0000000-0056100
Text      0020000-0112104     0056100-0150300
    Absolute          Virtual     Symbolic
0056176-000002         020076         call+070
0056376-000002         020276         getc
0056576-000002         020476         putc+046
0056776-000002         020676       fubyte+010
0057176-000002         021076       suword+044
0057376-000002         021276         aretu
0057576-000002         021476      clearse+034
0057776-000002         021676          csv+014
0060176-000002         022076         main+0160
0060376-000002         022276         main+0360
0060576-000002         022476        sureg+010
0060776-000002         022676      estabur+074
0061176-000002         023076      estabur+0274
0061376-000002         023276        iinit+06
0061576-000002         023476        alloc+02
0061776-000002         023676        alloc+0202
0062176-000002         024076         free+046
0062376-000002         024276         free+0246
0062576-000002         024476       ialloc+022
0062776-000002         024676       ialloc+0222
0063176-000002         025076       ialloc+0422
0063376-000002         025276       ialloc+0622
0063576-000002         025476       update+036
0063776-000002         025676       update+0236
0064176-000002         026076         iget+0156
0064376-000002         026276         iget+0356
0064576-000002         026476         iput+0126
0064776-000002         026676       iupdat+0176
0065176-000002         027076       itrunc+0120
0065376-000002         027276      maknode+060
0065576-000002         027476       printf+054
0065776-000002         027676       printn+042
0066176-000002         030076        panic+022
0066376-000002         030276        readi+0152
0066576-000002         030476        readi+0352
0066776-000002         030676       writei+066
0067176-000002         031076       writei+0266
0067376-000002         031276       writei+0466
0067576-000002         031476       iomove+0106
0067776-000002         031676        sleep+050
0070176-000002         032076       setrun+04
0070376-000002         032276        sched+0126
0070576-000002         032476        sched+0326
0070776-000002         032676        sched+0526
0071176-000002         033076        swtch+050
0071376-000002         033276      newproc+010
0071576-000002         033476      newproc+0210
0071776-000002         033676      newproc+0410
0072176-000002         034076       expand+0162
```

```
%tcmp -ta sysdump
sysdumpunix:
I and D      Virtual              Absolute
Data     0000000-0056014     0000000-0056100
Text     0020000-0112104     0056100-0150300
     call+070          bisb
*    call+070          halt
     getc              mov
*    getc              halt
     putc+046          rti
*    putc+046          halt
   fubyte+010          jsr
*  fubyte+010          halt
   suword+044          bit
*  suword+044          halt
    aretu              spl
*   aretu              halt
  clearse+034          mov
* clearse+034          halt
      csv+014          jmp
*     csv+014          halt
     main+0160         mov
*    main+0160         halt
     main+0360         jsr
*    main+0360         halt
    sureg+010          mov
*   sureg+010          halt
  estabur+074          ???
* estabur+074          halt
  estabur+0274         ash
* estabur+0274         halt
    iinit+06           wait
*   iinit+06           halt
    alloc+02           ???
*   alloc+02           halt
    alloc+0202         mov
*   alloc+0202         halt
     free+046          tstb
*    free+046          halt
     free+0246         iot
*    free+0246         halt
  ialloc+022           br
* ialloc+022           halt
  ialloc+0222          br
* ialloc+0222          halt
  ialloc+0422          ???
* ialloc+0422          halt
  ialloc+0622          ???
* ialloc+0622          halt
  update+036           ???
* update+036           halt
  update+0236          blo
* update+0236          halt
    iget+0156          ???
*   iget+0156          halt
    iget+0356          ???
*   iget+0356          halt
```

% nroff tcmp.5

```
%tcmp -tu sysdump 4056m /etc/init
init:
I only      Virtual              Absolute
Text      0000000-0003300      0407600-0413100
Data      0003300-0004200      0413100-0414000

    Absolute      Symbolic
0407600-000002          +01
0407700-000004       main+052
0407742-000002       main+0114
0407750-000002       main+0122
0410000-000002       main+0152
0410100-000004       main+0252
0410142-000002       main+0314
0410150-000002       main+0322
0410200-000002       main+0352
0410300-000004       main+0452
0410342-000002       main+0514
0410350-000002       main+0522
0410400-000002       main+0552
0410500-000004       main+0652
0410542-000002       main+0714
0410550-000002       main+0722
0410600-000002       main+0752
0410700-000004       term+014
0410742-000002      rline+06
0410750-000002      rline+014
0411000-000002      rline+044
0411100-000004      dfork+04
0411142-000002      dfork+046
0411150-000002      dfork+054
0411200-000002      dfork+0104
0411300-000004       rmut+040
0411342-000002       rmut+0102
0411350-000002       rmut+0110
0411400-000002       rmut+0140
0411500-000004       rmut+0240
0411542-000002      chmod+036
0411550-000002      chown+04
0411600-000002      chown+034
0411700-000004        dup+010
0411742-000002        dup+052
0411750-000002       fork
0412000-000002       kill
0412100-000004       read+04
0412142-000002       seek+04
0412150-000002       seek+012
0412200-000002       seek+042
0412300-000004     signal+076
0412342-000002     signal+0140
0412350-000002     signal+0146
0412400-000002       time+016
0412500-000004      write+030
0412550-000002      nargs+012
0412600-000002      nargs+042
0412700-000004      nargs+0142
0412742-000002      reset+012
0412750-000002      reset+020
0413000-000002        csv

DONE
```