Subject: : AmigaOS4
Topic: : GDB
Re: GDB
Author: : kas1e
Date: : 2021/3/23 20:04:11
URL:

@billyfish
Quote:

> Roman, can you remember when we did we have breakpoints working? If we did, then that will give me a base to compare to.

As far as I can tell, we never have a working breakpoint in our version, we only now reach the point when we start to make it works.

I downloaded now your latest commit at this moment, and rebuild it all from scratch, and tested it on x5000 firstly - still crashes.

Results from serial:

```
 <amigaos_init>
</amigaos_init>
<_initialize_amigaos_nat>
<init_amigaos_ops>
Shell Process: Using v6.3 breakpoint code
Shell Process: Using deprecated mem transfer code
</init_amigaos_ops>
</_initialize_amigaos_nat>
<amigaos_can_run>
</amigaos_can_run>
<amigaos_can_run>
</amigaos_can_run>
<amigaos_create_inferior>
Shell Process: Creating inferior process: exec_file = /Work/aa/test, args = , env = 0x610A87C0, from_tty = 1
<AllocateDebugInfo>
</AllocateDebugInfo>
<Ux2DOS>
</Ux2DOS>
```

Shell Process: Getting elf handle for seglist 0x1882CF41
Shell Process: Process created: 0x60E84360
Shell Process: Task: 0x60E84360
Shell Process: Suspending Task
Shell Process: Adding debug hook from 0x60E84360
Shell Process: Added debug hook for 0x60E84360
Shell Process: amigaos target_pushed_count 0
Shell Process: pushing amigaos target
Shell Process: add_thread 1630521616 inf 0x610A8738
</amigaos_create_inferior>
<amigaos_terminal_ours>
Shell Process: terminal_ours is a STUB
</amigaos_terminal_ours>
<amigaos_fetch_registers>
Shell Process: inferior_ptid=0x612FC868
Shell Process: regno = 64 (pc)
Shell Process: context = 0x5FBCCFC8, sp = 0, pc = 0, lr = 0
</amigaos_fetch_registers>
<amigaos_has_execution>
</amigaos_has_execution>
<amigaos_has_registers>
</amigaos_has_registers>
<amigaos_has_stack>
</amigaos_has_stack>
<amigaos_has_memory>
</amigaos_has_memory>
<amigaos_has_registers>
</amigaos_has_registers>
<amigaos_has_stack>
</amigaos_has_stack>
<amigaos_has_memory>
</amigaos_has_memory>
<amigaos_deprecated_xfer_memory>
Shell Process: amigaos_xfer_memory(memaddr = 0x010004D4, myaddr = 0x612FC2F8, len = 4, write = 0,
attrib = 0x00000000, target = 0x5FBB7A4C)
kernel 54.34 (5.2.2021) AmigaOne X5000 release
Machine model: 9 (AmigaOne X5000/20)
Dump of context at 0xEFD673E0
Trap type: DSI exception
DSISR: 00000000 DAR: 010004D4
No matching page found
Machine State (raw): 0x0002F030
Machine State (verbose): [Critical Ints on] [ExtInt on] [User] [IAT on] [DAT on]
Instruction pointer: in module kernel+0x00041A70 (0x01841A70)
Crashed process: gdb_751 (0x67648DB0)
DSI verbose error description: Access to address 0x010004D4 not allowed by page protection in user state (
protection violation)
Access was a load operation
Exception Syndrome Register: 0x00000000
 0: 01A65794 612FC120 00000002 612FC2F8 010004D4 00000004 00000004 00000004
 8: 010004D0 00000001 612FC2F4 01A65764 00000794 5FBBDEC8 5FBB0000 00000001

16: 00000000 61489860 5FBB0000 5FBB0000 610A8738 01846030 5FBB7A4C 00000000
24: 612FC2F8 00000004 0224A968 00000000 5E845074 010004D4 5E843750 612FC2F8
CR: 37555935 XER: A000007E CTR: 00000001 LR: 01841BD4

Disassembly of crash site:
 01841A60: 3943FFFC subi r10,r3,4
 01841A64: 5529F0BE rlwinm r9,r9,30,2,31
 01841A68: 39290001 addi r9,r9,1
 01841A6C: 7D2903A6 mtctr r9
>01841A70: 85280004 lwzu r9,4(r8)
 01841A74: 952A0004 stwu r9,4(r10)
 01841A78: 4200FFF8 bdnz+ 0x1841A70
 01841A7C: 54A507BE rlwinm r5,r5,0,30,31
 01841A80: 7C843A14 add r4,r4,r7
 01841A84: 2F850000 cmpwi cr7,r5,0
msr: 0x0002B032
TLB1 (64 entries):
 * [51]: size=7 tid = 0 TS = 1 epn=0xFE000000 rpn=0x0000000F_FE000000 WIMG=0x5 XXWWRR=0xF
protected
 * [52]: size=6 tid = 0 TS = 1 epn=0x01000000 rpn=0x00000000_01000000 WIMG=0x0 XXWWRR=0x5
protected
 * [53]: size=6 tid = 0 TS = 1 epn=0x01400000 rpn=0x00000000_01400000 WIMG=0x0 XXWWRR=0x5
protected
 * [54]: size=6 tid = 0 TS = 1 epn=0x01800000 rpn=0x00000000_01800000 WIMG=0x0 XXWWRR=0x33
protected
 * [55]: size=6 tid = 0 TS = 1 epn=0x01C00000 rpn=0x00000000_01C00000 WIMG=0x0 XXWWRR=0x33
protected
 * [56]: size=6 tid = 0 TS = 1 epn=0x02000000 rpn=0x00000000_02000000 WIMG=0x0 XXWWRR=0xF
protected
 * [57]: size=4 tid = 0 TS = 1 epn=0x02400000 rpn=0x00000000_02400000 WIMG=0x0 XXWWRR=0xF
protected
 * [58]: size=3 tid = 0 TS = 1 epn=0x02440000 rpn=0x00000000_02440000 WIMG=0x0 XXWWRR=0xF
protected
 * [59]: size=3 tid = 0 TS = 1 epn=0x02450000 rpn=0x00000000_02450000 WIMG=0x0 XXWWRR=0xF
protected
 * [60]: size=3 tid = 0 TS = 1 epn=0x02460000 rpn=0x00000000_02460000 WIMG=0x0 XXWWRR=0xF
protected
 * [61]: size=7 tid = 0 TS = 0 epn=0xFE000000 rpn=0x0000000F_FE000000 WIMG=0x5 XXWWRR=0xF
protected
 * [62]: size=A tid = 0 TS = 0 epn=0x00000000 rpn=0x00000000_00000000 WIMG=0x0 XXWWRR=0x3F
protected
 * [63]: size=A tid = 0 TS = 0 epn=0x40000000 rpn=0x00000000_40000000 WIMG=0x0 XXWWRR=0x3F
protected
HAL_MaxTLB = 50, HAL_NextTLB = 0
MMUCFG = 0x064809C4
mas0 = 0x103F0000
mas1 = 0xC0000A00
mas2 = 0x40000000
mas3 = 0x4000003F
mas4 = 0x00000100
mas5 = 0x00000000

mas6 = 0x00000001
mas7 = 0x00000000
mas8 = 0x00000000

Kernel command line: serial munge debuglevel=1

Registers pointing to code:
r0 : native kernel module newlib.library.kmod+0x00008fb4
r9 : module Work:aa/test at 0x00000001 (section 0 @ 0xFFFFFFDC)
r11: native kernel module newlib.library.kmod+0x00008f84
r13: gdb_751:symbuf()+0x3d5c (section 16 @ 0x753C)
r14: module gdb_751 at 0x5FBB0000 (section 3 @ 0xFFFFFFDC)
r15: module Work:aa/test at 0x00000001 (section 0 @ 0xFFFFFFDC)
r18: module gdb_751 at 0x5FBB0000 (section 3 @ 0xFFFFFFDC)
r19: module gdb_751 at 0x5FBB0000 (section 3 @ 0xFFFFFFDC)
r21: native kernel module kernel+0x00046030
r22: gdb_751:amigaos_ops()+0x0 (section 16 @ 0x10C0)
r26: native kernel module kernel+0x00a4a968
r28: module gdb_751 at 0x5E845074 (section 1 @ 0x5050)
r30: gdb_751:__PRETTY_FUNCTION__.26864()+0x0 (section 3 @ 0x374C)
ip : native kernel module kernel+0x00041a70
lr : native kernel module kernel+0x00041bd4
ctr: module Work:aa/test at 0x00000001 (section 0 @ 0xFFFFFFDC)

Stack trace:
(0x612FC120) native kernel module kernel+0x00041a70
(0x612FC130) native kernel module kernel+0x00041bd4
(0x612FC140) gdb_751:amigaos_deprecated_xfer_memory()+0x2c4 (section 1 @ 0x27964)
(0x612FC190) gdb_751:default_xfer_partial()+0x128 (section 1 @ 0x13B9BC)
(0x612FC1C0) gdb_751:memory_xfer_partial_1()+0x1a8 (section 1 @ 0x13D3AC)
(0x612FC240) gdb_751:target_xfer_partial()+0x230 (section 1 @ 0x13DAEC)
(0x612FC290) gdb_751:target_read()+0xc8 (section 1 @ 0x13CDE4)
(0x612FC2E0) gdb_751:target_read_memory()+0x44 (section 1 @ 0x13CF2C)
(0x612FC2F0) gdb_751:rs6000_skip_main_prologue()+0x30 (section 1 @ 0x2CF0)
(0x612FC320) gdb_751:skip_prologue_sal()+0x418 (section 1 @ 0xDF5B8)
(0x612FC3A0) gdb_751:convert_linespec_to_sals()+0xa58 (section 1 @ 0xEF9FC)
(0x612FC480) gdb_751:parse_linespec()+0x314 (section 1 @ 0xF1D54)
(0x612FC5F0) gdb_751:decode_line_full()+0x140 (section 1 @ 0xF27D8)
(0x612FC6D0) gdb_751:decode_linespec_default.isra.49()+0x50 (section 1 @ 0x99530)
(0x612FC700) gdb_751:addr_string_to_sals()+0x9c (section 1 @ 0xA6608)
(0x612FC830) gdb_751:breakpoint_re_set_default()+0x40 (section 1 @ 0xA9598)
(0x612FC880) gdb_751:breakpoint_re_set_one()+0x58 (section 1 @ 0x9508C)
(0x612FC890) gdb_751:catch_errors()+0x74 (section 1 @ 0x112A5C)
(0x612FC8F0) gdb_751:breakpoint_re_set()+0xbc (section 1 @ 0xA9750)
(0x612FC930) gdb_751:post_create_inferior()+0xec (section 1 @ 0xF8610)
(0x612FC980) gdb_751:run_command_1()+0x194 (section 1 @ 0xF8DC4)
(0x612FC9E0) gdb_751:execute_command()+0x278 (section 1 @ 0x1D9A08)
(0x612FCA20) gdb_751:command_handler()+0x84 (section 1 @ 0x11BA64)
(0x612FCA40) gdb_751:command_line_handler()+0x464 (section 1 @ 0x11C118)
(0x612FCA90) gdb_751:rl_callback_read_char()+0x1a8 (section 1 @ 0x227868)
(0x612FCAD0) gdb_751:rl_callback_read_char_wrapper()+0x10 (section 1 @ 0x11BAE0)

(0x612FCAE0) gdb_751:process_event()+0xb8 (section 1 @ 0x11A3C0)
(0x612FCB00) gdb_751:gdb_do_one_event()+0x3a4 (section 1 @ 0x11A84C)
(0x612FCB40) gdb_751:start_event_loop()+0x40 (section 1 @ 0x11AA1C)
(0x612FCB80) gdb_751:captured_command_loop()+0x1c (section 1 @ 0x1141E4)
(0x612FCB90) gdb_751:catch_errors()+0x74 (section 1 @ 0x112A5C)
(0x612FCBF0) gdb_751:captured_main()+0xcb4 (section 1 @ 0x115204)
(0x612FCC80) gdb_751:catch_errors()+0x74 (section 1 @ 0x112A5C)
(0x612FCCE0) gdb_751:gdb_main()+0x34 (section 1 @ 0x1153B8)
(0x612FCCF0) gdb_751:main()+0x30 (section 1 @ 0x478)
(0x612FCD10) native kernel module newlib.library.kmod+0x00002614
(0x612FCD60) native kernel module newlib.library.kmod+0x00003340
(0x612FCF10) native kernel module newlib.library.kmod+0x00003864
(0x612FCF40) gdb_751:_start()+0x1e0 (section 1 @ 0x1DC)
(0x612FCF90) native kernel module dos.library.kmod+0x0002a490
(0x612FCFC0) native kernel module kernel+0x0005c6c8
(0x612FCFD0) native kernel module kernel+0x0005c740

Disassembly of crash site:
```
 01841A60: 3943FFFC   subi          r10,r3,4
 01841A64: 5529F0BE   rlwinm         r9,r9,30,2,31
 01841A68: 39290001   addi          r9,r9,1
 01841A6C: 7D2903A6   mtctr         r9
>01841A70: 85280004   lwzu          r9,4(r8)
 01841A74: 952A0004   stwu          r9,4(r10)
 01841A78: 4200FFF8   bdnz+         0x1841A70
 01841A7C: 54A507BE   rlwinm         r5,r5,0,30,31
 01841A80: 7C843A14   add           r4,r4,r7
 01841A84: 2F850000   cmpwi         cr7,r5,0
```
Stack pointer (0x612FC120) is inside bounds
Redzone is OK (4)

68k register dump
DATA: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
ADDR: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
Page information:
Page not found

Ready Tasks
```
                WinFrame 19 Process (pri   5, sigrec 0x00800000, sigwait 0xFF800000, masked 0x00800000)
        IDF1/FastFileSystem 53.2  (pri   5, sigrec 0x20000000, sigwait 0xA8000100, masked 0x20000000)
        IDF0/FastFileSystem 53.2  (pri   5, sigrec 0x20000000, sigwait 0xA8000100, masked 0x20000000)
                  compose.task (pri   1, sigrec 0x00000020, sigwait 0x00000021, masked 0x00000020)
                   Workbench (pri   1, sigrec 0x80000100, sigwait 0x80000000, masked 0x80000000)
             ScreenBlanker Library. (pri   1, sigrec 0x08000100, sigwait 0xE8001000, masked 0x08000000)
                  dopus_clock (pri   1, sigrec 0x40000000, sigwait 0xC0000000, masked 0x40000000)
                    AmiDock (pri   0, sigrec 0x00300100, sigwait 0x00000100, masked 0x00000100)
           NotificationServer (pri   0, sigrec 0x08000000, sigwait 0xF8001000, masked 0x08000000)
             TCP/IP Control (pri   0, sigrec 0x40000100, sigwait 0xF8009080, masked 0x40000000)
              ELF Collector (pri   0, sigrec 0x00000100, sigwait 0x00000100, masked 0x00000100)
                hub.usbfd (pri   0, sigrec 0x10000000, sigwait 0x30000000, masked 0x10000000)
                hub.usbfd (pri   0, sigrec 0x10000000, sigwait 0x30000000, masked 0x10000000)
```

CPUDock_idleTask (pri -127, sigrec 0x00000000, sigwait 0x40000000, masked 0x00000000)
idle.task (pri -128, sigrec 0x00000000, sigwait 0x00000000, masked 0x00000000)

Waiting Tasks
EHCI Controller Task Unit 1 (pri 15, sigrec 0x00000000, sigwait 0xBE009000, masked 0x00000000)
EHCI Controller Task Unit 0 (pri 15, sigrec 0x00000000, sigwait 0xBE009000, masked 0x00000000)
USB stack (pri 18, sigrec 0x00000000, sigwait 0xF800D000, masked 0x00000000)
rx_pm (pri 100, sigrec 0x00000000, sigwait 0x80000001, masked 0x00000000)
CON/con-handler 53.82 (pri 5, sigrec 0x00000000, sigwait 0xB0000100, masked 0x00000000)
rx_gc (pri 100, sigrec 0x00000000, sigwait 0x80000001, masked 0x00000000)
appdir envarc manager (pri -50, sigrec 0x00000000, sigwait 0x00000100, masked 0x00000000)
hid.usbfd (pri 10, sigrec 0x00000100, sigwait 0xE0000000, masked 0x00000000)
HID Keyboard (pri 10, sigrec 0x00000000, sigwait 0x90001000, masked 0x00000000)
p50x0sata.device Port 0 (pri 12, sigrec 0x10000000, sigwait 0xC0007000, masked 0x00000000)
ICD1/CDFileSystem 53.8 (pri 10, sigrec 0x00000000, sigwait 0x00000100, masked 0x00000000)
ICD0/CDFileSystem 53.8 (pri 10, sigrec 0x00000000, sigwait 0x00000100, masked 0x00000000)
DH2/SmartFilesystem 1.293 (pri 11, sigrec 0x00000000, sigwait 0x00000100,
masked 0x00000000)
DH3/SmartFilesystem 1.293 (pri 11, sigrec 0x00000000, sigwait 0x00000100,
masked 0x00000000)
serial.device (pri 1, sigrec 0x00000000, sigwait 0x7E000000, masked 0x00000000)
dos_signal_server (pri -5, sigrec 0x00000000, sigwait 0x0000F000, masked 0x00000000)
X-Dock (pri 0, sigrec 0x00000100, sigwait 0xFE001000, masked 0x00000000)
hid.usbfd (pri 10, sigrec 0x00000100, sigwait 0xE0000000, masked 0x00000000)
HID Mouse (pri 10, sigrec 0x00000000, sigwait 0x80001000, masked 0x00000000)
New Process (pri 0, sigrec 0x00000000, sigwait 0x00000010, masked 0x00000000)
P50x0 Ethernet (pri 20, sigrec 0x00000000, sigwait 0x00001000, masked 0x00000000)
Background CLI (pri 0, sigrec 0x00000100, sigwait 0x10001080, masked 0x00000000)
New Process (pri 0, sigrec 0x00000000, sigwait 0x00000010, masked 0x00000000)
dos_filedir_notify (pri 5, sigrec 0x80000000, sigwait 0x40001000, masked 0x00000000)
New Process (pri 0, sigrec 0x00000000, sigwait 0x00000010, masked 0x00000000)
TCP/IP Superserver (pri 0, sigrec 0x00000100, sigwait 0xD0000080, masked 0x00000000)
TCP/IP Configuration (pri 0, sigrec 0x00000100, sigwait 0xF8003000, masked 0x00000000)
ClickToFront (pri 21, sigrec 0x00000100, sigwait 0xE000D000, masked 0x00000000)
DirectoryOpus (pri 0, sigrec 0x00000000, sigwait 0x5C009000, masked 0x00000000)
DH3/SmartFilesystem 1.293 (pri 10, sigrec 0x00000000, sigwait 0xE0000100,
masked 0x00000000)
DH2/SmartFilesystem 1.293 (pri 10, sigrec 0x00000000, sigwait 0xE0000100,
masked 0x00000000)
? IPrefs ? (pri 0, sigrec 0x00000000, sigwait 0x0000F000, masked 0x00000000)
ContextMenus (pri 0, sigrec 0x04000000, sigwait 0xE0001000, masked 0x00000000)
RexxMaster (pri 4, sigrec 0x00000100, sigwait 0xC0000000, masked 0x00000000)
DefIcons (pri 0, sigrec 0x00000100, sigwait 0x80009000, masked 0x00000000)
ContextMenus Command Dispatcher (pri 1, sigrec 0x00000000, sigwait 0x80001000,
masked 0x00000000)
URL/launch-handler 53.39 (pri 5, sigrec 0x00000100, sigwait 0x80000000, masked 0x00000000)
TEXTCLIP/textclip-handler 53.4 (pri 3, sigrec 0x00000100, sigwait 0x80000000, masked 0x00000000
)
RANDOM/Random-Handler 52.1 (pri 5, sigrec 0x00000000, sigwait 0x00000100,
masked 0x00000000)
Mounter Task (pri -1, sigrec 0x00000000, sigwait 0xB0001000, masked 0x00000000)

Mounter GUI (pri 0, sigrec 0x00000000, sigwait 0x80007000, masked 0x00000000)
Mounter Companion Process (pri -1, sigrec 0x00000000, sigwait 0x80003000,
masked 0x00000000)
Workbench DosList Notify (pri 1, sigrec 0x00000100, sigwait 0x00003000, masked 0x00000000)
ramlib.support (pri -2, sigrec 0x00000000, sigwait 0x80005000, masked 0x00000000)
ramlib (pri 1, sigrec 0x00000000, sigwait 0x80001000, masked 0x00000000)
dopus_arbiter (pri 0, sigrec 0x00000000, sigwait 0x00000100, masked 0x00000000)
dopus_hotkeez (pri 1, sigrec 0x00000000, sigwait 0xC0000000, masked 0x00000000)
CON/con-handler 53.82 (pri 5, sigrec 0x00000000, sigwait 0xA0000100, masked 0x00000000)
FKey (pri 0, sigrec 0x00000000, sigwait 0xC000D000, masked 0x00000000)
MUI imagespace screen notify (pri 1, sigrec 0x00000100, sigwait 0xC0001000,
masked 0x00000000)
TextEditor.mcc clipboard server (pri 1, sigrec 0x00000100, sigwait 0x80000000, masked 0x00000000
)
New Process (pri 0, sigrec 0x00000000, sigwait 0x80000010, masked 0x00000000)
KeymapSwitcher.docky (pri 0, sigrec 0x00000000, sigwait 0x80001000, masked 0x00000000)
select.gadget prefs (pri 0, sigrec 0x00000100, sigwait 0x80001000, masked 0x00000000)
AsyncWB (pri 0, sigrec 0x00000100, sigwait 0xC0001000, masked 0x00000000)
texteditor.gadget Clipboard Server (pri 1, sigrec 0x00000100, sigwait 0x80000000,
masked 0x00000000)
RAWBInfo (pri 0, sigrec 0x00000100, sigwait 0x80001000, masked 0x00000000)
CON/con-handler 53.82 (pri 5, sigrec 0x00000000, sigwait 0xA0000100, masked 0x00000000)
CON/con-handler 53.82 (pri 5, sigrec 0x00000000, sigwait 0xA0000100, masked 0x00000000)
CON/con-handler 53.82 (pri 5, sigrec 0x00000000, sigwait 0xA0000100, masked 0x00000000)
CON/con-handler 53.82 (pri 5, sigrec 0x00000000, sigwait 0xA0000100, masked 0x00000000)
CON/con-handler 53.82 (pri 5, sigrec 0x00000000, sigwait 0xA0000100, masked 0x00000000)
application.library messageserver (pri 0, sigrec 0x00000000, sigwait 0xC0000000,
masked 0x00000000)
New Process (pri 0, sigrec 0x80000000, sigwait 0x00000010, masked 0x00000000)
Workbench Clipboard Server (pri 1, sigrec 0x00000100, sigwait 0x80000000, masked 0x00000000
)
New Process (pri 0, sigrec 0x00000000, sigwait 0x00000010, masked 0x00000000)
New Process (pri 0, sigrec 0x00000000, sigwait 0x00000010, masked 0x00000000)
New Process (pri 0, sigrec 0x00000000, sigwait 0x00000010, masked 0x00000000)
New Process (pri 0, sigrec 0x00000000, sigwait 0x00000010, masked 0x00000000)
New Process (pri 0, sigrec 0x00000000, sigwait 0x00000010, masked 0x00000000)
New Process (pri 0, sigrec 0x00000000, sigwait 0x00000010, masked 0x00000000)
New Process (pri 0, sigrec 0x00000000, sigwait 0x00000010, masked 0x00000000)
New Process (pri 0, sigrec 0x00000000, sigwait 0x00000010, masked 0x00000000)
New Process (pri 0, sigrec 0x00000000, sigwait 0x00000010, masked 0x00000000)
New Process (pri 0, sigrec 0x00000000, sigwait 0x00000010, masked 0x00000000)
New Process (pri 0, sigrec 0x00000000, sigwait 0x00000010, masked 0x00000000)
New Process (pri 0, sigrec 0x00000000, sigwait 0x00000010, masked 0x00000000)
New Process (pri 0, sigrec 0x00000000, sigwait 0x00000010, masked 0x00000000)
New Process (pri 0, sigrec 0x00000000, sigwait 0x00000010, masked 0x00000000)
TCP/IP Log (pri 0, sigrec 0x00000000, sigwait 0x80003000, masked 0x00000000)
hid.usbfd (pri 10, sigrec 0x00000100, sigwait 0xE0000000, masked 0x00000000)
HID Consumer (pri 10, sigrec 0x00000000, sigwait 0x80001000, masked 0x00000000)
ConClip (pri 0, sigrec 0x00000000, sigwait 0x80000000, masked 0x00000000)
HID Consumer (pri 10, sigrec 0x00000000, sigwait 0x80001000, masked 0x00000000)
diskimage.device unit 1 (pri 4, sigrec 0x00000100, sigwait 0xC0000000, masked 0x00000000)

diskimage.device unit 0 (pri 4, sigrec 0x00000100, sigwait 0xC0000000, masked 0x00000000)
diskimage.device unit 5 (pri 4, sigrec 0x00000100, sigwait 0xC0000000, masked 0x00000000)
diskimage.device unit 4 (pri 4, sigrec 0x00000100, sigwait 0xC0000000, masked 0x00000000)
HID Consumer (pri 10, sigrec 0x00000000, sigwait 0x80001000, masked 0x00000000)
HID Keyboard (pri 10, sigrec 0x00000000, sigwait 0x90001000, masked 0x00000000)
hid.usbfd (pri 10, sigrec 0x00000100, sigwait 0xE0000000, masked 0x00000000)
hid.usbfd (pri 10, sigrec 0x00000100, sigwait 0xE0000000, masked 0x00000000)
AUDIO/AHI-Handler 6.2 (pri 5, sigrec 0x00000000, sigwait 0x00000100, masked 0x00000000)
USB stack Process (pri 0, sigrec 0x00000000, sigwait 0x80001000, masked 0x00000000)
APPDIR/appdir-handler 54.18 (pri 5, sigrec 0x00000100, sigwait 0x80000000, masked 0x00000000
)
MassStorage Notifier (pri 0, sigrec 0x00000000, sigwait 0x80001000, masked 0x00000000)
DST watcher (pri 0, sigrec 0x00000000, sigwait 0xC0000000, masked 0x00000000)
NotifyA Server (pri 1, sigrec 0x00000000, sigwait 0xE8001000, masked 0x00000000)
string.gadget server (pri 1, sigrec 0x00000100, sigwait 0x40000000, masked 0x00000000)
datatypes.library (pri 1, sigrec 0x00000000, sigwait 0x80001000, masked 0x00000000)
RAM/ram-handler 54.24 (pri 10, sigrec 0x00000100, sigwait 0x80000000, masked 0x00000000)
ENV/env-handler 54.18 (pri 5, sigrec 0x00000100, sigwait 0x80000000, masked 0x00000000)
CON/con-handler 53.82 (pri 5, sigrec 0x00000000, sigwait 0xA0000100, masked 0x00000000)
RAW/con-handler 53.82 (pri 5, sigrec 0x00000000, sigwait 0xA0000100, masked 0x00000000)
CON/con-handler 53.82 (pri 5, sigrec 0x00000000, sigwait 0xA0000100, masked 0x00000000)
SFS DosList handler (pri 19, sigrec 0x00000000, sigwait 0x80000000, masked 0x00000000)
dos_nbmd_process (pri 5, sigrec 0x00000000, sigwait 0x00001100, masked 0x00000000)
dos_lock_handler (pri 5, sigrec 0x00000000, sigwait 0x00001100, masked 0x00000000)
hub.usbfd (pri 0, sigrec 0x00000000, sigwait 0x30000000, masked 0x00000000)
hub.usbfd (pri 0, sigrec 0x00000000, sigwait 0x30000000, masked 0x00000000)
p50x0sata.device Port 1 (pri 12, sigrec 0x00000000, sigwait 0xC0007000, masked 0x00000000)
DMA2 Channel 4 Handler (pri 0, sigrec 0x00000000, sigwait 0x80001000, masked 0x00000000)
DMA1 Channel 4 Handler (pri 0, sigrec 0x00000000, sigwait 0x80001000, masked 0x00000000)
DMA2 Channel 3 Handler (pri 0, sigrec 0x00000000, sigwait 0x80001000, masked 0x00000000)
DMA1 Channel 3 Handler (pri 0, sigrec 0x00000000, sigwait 0x80001000, masked 0x00000000)
DMA2 Channel 2 Handler (pri 0, sigrec 0x00000000, sigwait 0x80001000, masked 0x00000000)
DMA1 Channel 2 Handler (pri 0, sigrec 0x00000000, sigwait 0x80001000, masked 0x00000000)
DMA2 Channel 1 Handler (pri 0, sigrec 0x00000000, sigwait 0x80001000, masked 0x00000000)
DMA1 Channel 1 Handler (pri 0, sigrec 0x00000000, sigwait 0x80001000, masked 0x00000000)
Exec Command and Control (pri 30, sigrec 0x00000000, sigwait 0x80000000,
masked 0x00000000)

Suspended Tasks
/Work/aa/test (pri 0, sigrec 0x00000000, sigwait 0x00000000, masked 0x00000000)

Results from the console:

```
 2/0.Work:aa> gdb_751 -q test
_initialize_amigaos_nat
[New inferior 0]
Reading symbols from /Work/aa/test...done.
(gdb) break 1
break 1
```

target_memory_map ()
target_get_section_table ()
target_get_section_table () for exec
exec:target_xfer_partial (2, (null), 0x612fc038, 0x0, 0x10004d4, 4) = 4, bytes = 3d 20 01 00
target_get_section_table ()
target_get_section_table () for exec
exec:target_xfer_partial (2, (null), 0x612fc108, 0x0, 0x10004d4, 4) = 4, bytes = 3d 20 01 00
target_get_section_table ()
target_get_section_table () for exec
exec:target_xfer_partial (2, (null), 0x612fc458, 0x0, 0x10004d4, 4) = 4, bytes = 3d 20 01 00
target_get_section_table ()
target_get_section_table () for exec
exec:target_xfer_partial (2, (null), 0x612fc6d0, 0x0, 0x10004d4, 4) = 4, bytes =
 3d 20 01 00
Breakpoint 1 at 0x10004d4: file test.c, line 1.
(gdb) r
r
t: PowerPC PPCBug monitor on port 0
 t: PowerPC PPCBug monitor on port 1
 t: DINK32 monitor
 t: Debug an Amiga process
 amigaos_can_run returning 1
t: Remote serial target in gdb-specific protocol
 t: Extended remote serial target in gdb-specific protocol
 t: Local trace dump file
 t: Local core dump file
 t: Local exec file
 t: Process record and replay target
 t: Process record and replay target
 Starting program: /Work/aa/test
t: PowerPC PPCBug monitor on port 0
 t: PowerPC PPCBug monitor on port 1
 t: DINK32 monitor
 t: Debug an Amiga process
 amigaos_can_run returning 1
t: Remote serial target in gdb-specific protocol
 t: Extended remote serial target in gdb-specific protocol
 t: Local trace dump file
 t: Local core dump file
 t: Local exec file
 t: Process record and replay target
 t: Process record and replay target
 [New process 1625834336]
target_create_inferior (/Work/aa/test, , xxx, 1)
target_terminal_ours ()
target_get_section_table ()
target_get_section_table () for exec
subtask:target_xfer_partial (10, target.xml, 0x5f0f4fc8, 0x0, 0x0, 4095) = -1
target_thread_architecture (process 1625834336) = 0x5e98a010 [powerpc:common]
ptid_equal (null_ptid, ptid (1625834336, 0,0)
pid 1625834336 for ptid (1625834336, 0,0)

get_thread_arch_regcache (process 1625834336) = 0x610a86c8
ptid_equal (null_ptid, ptid (1625834336, 0,0)
pid 1625834336 for ptid (1625834336, 0,0)
get_thread_arch_regcache (process 1625834336) = 0x610a86c8
target_fetch_registers (pc) = 00000000 0x0 0
target_get_section_table ()
target_get_section_table () for exec
subtask:target_xfer_partial (11, (null), 0x5f0f5420, 0x0, 0x0, 4095) = -1
target_memory_map ()
<<<< CRASH >>>>

Then tried it on pegasos2. There I didn't have a crash, but after I set breakpoint and hit "run", it then didn't stop on a breakpoint and didn't give me the ability to type things in the terminal (i.e. it didn't finish the executing now as well)

Results from serial:

<amigaos_init>
</amigaos_init>
<_initialize_amigaos_nat>
<init_amigaos_ops>
Shell Process: Using v6.3 breakpoint code
Shell Process: Using deprecated mem transfer code
</init_amigaos_ops>
</_initialize_amigaos_nat>
<amigaos_can_run>
</amigaos_can_run>
<amigaos_can_run>
</amigaos_can_run>
<amigaos_create_inferior>
Shell Process: Creating inferior process: exec_file = /RAM Disk/test, args = , env = 0x64E5A2F8, from_tty = 1
<AllocateDebugInfo>
</AllocateDebugInfo>
<Ux2DOS>
</Ux2DOS>
Shell Process: Getting elf handle for seglist 0x194D38D1
Shell Process: Process created: 0x62039020
Shell Process: Task: 0x62039020
Shell Process: Suspending Task
Shell Process: Adding debug hook from 0x62039020
Shell Process: Added debug hook for 0x62039020
Shell Process: amigaos target_pushed_count 0
Shell Process: pushing amigaos target
Shell Process: add_thread 1700079888 inf 0x64E5A280
</amigaos_create_inferior>
<amigaos_terminal_ours>
Shell Process: terminal_ours is a STUB
</amigaos_terminal_ours>

<amigaos_fetch_registers>
Shell Process: inferior_ptid=0x65552868
Shell Process: regno = 64 (pc)
Shell Process: context = 0x6556FFC8, sp = 0, pc = 0, lr = 0
</amigaos_fetch_registers>
<amigaos_has_execution>
</amigaos_has_execution>
<amigaos_has_registers>
</amigaos_has_registers>
<amigaos_has_stack>
</amigaos_has_stack>
<amigaos_has_memory>
</amigaos_has_memory>
<amigaos_has_registers>
</amigaos_has_registers>
<amigaos_has_stack>
</amigaos_has_stack>
<amigaos_has_memory>
</amigaos_has_memory>
<amigaos_deprecated_xfer_memory>
Shell Process: amigaos_xfer_memory(memaddr = 0x010004D4, myaddr = 0x655522F8, len = 4, write = 0,
attrib = 0x00000000, target = 0x6555AA4C)
</amigaos_deprecated_xfer_memory>
<amigaos_has_registers>
</amigaos_has_registers>
<amigaos_has_stack>
</amigaos_has_stack>
<amigaos_has_memory>
</amigaos_has_memory>
<amigaos_has_registers>
</amigaos_has_registers>
<amigaos_has_stack>
</amigaos_has_stack>
<amigaos_has_memory>
</amigaos_has_memory>
<amigaos_has_registers>
</amigaos_has_registers>
<amigaos_has_stack>
</amigaos_has_stack>
<amigaos_has_memory>
</amigaos_has_memory>
<amigaos_memory_insert_breakpoint>
Shell Process: Trying to set breakpoint at 0x010004D4 (host_addr=0x010004D4, code_elf_addr=0xABADCAFE
, code_size=0xABADCAFE)
<DebugPrintBuffers>
Shell Process: pre-read
Shell Process: src [0] 0x010004D4 = 0, dest [0] 0x64E153B0 = 0
</DebugPrintBuffers>
<amigaos_deprecated_xfer_memory>
Shell Process: amigaos_xfer_memory(memaddr = 0x010004D4, myaddr = 0x64E153B0, len = 4, write = 0,
attrib = 0x00000000, target = 0x6555AA4C)

</amigaos_deprecated_xfer_memory>
Shell Process: Saved at addr 0x010004D4 the instruction 0x64E153B0
<DebugPrintBuffers>
Shell Process: post-read
Shell Process: src [0] 0x010004D4 = 0, dest [0] 0x64E153B0 = 0
</DebugPrintBuffers>
Shell Process: Setting breakpoint at addr=0x010004D4 bp=0x65553018
<DebugPrintBuffers>
Shell Process: pre-write
Shell Process: src [0] 0x65553018 = 7D821008, dest [0] 0x010004D4 = 0
</DebugPrintBuffers>
<amigaos_deprecated_xfer_memory>
Shell Process: amigaos_xfer_memory(memaddr = 0x010004D4, myaddr = 0x64E15520, len = 4, write = 1,
attrib = 0x00000000, target = 0x6555AA4C)
Shell Process: Writing 0x7D821008 to 0x010004D4 (was 0x00000000)
Shell Process: Now is 0x7D821008
</amigaos_deprecated_xfer_memory>
<DebugPrintBuffers>
Shell Process: post-write
Shell Process: src [0] 0x65553018 = 7D821008, dest [0] 0x010004D4 = 7D821008
</DebugPrintBuffers>
</amigaos_memory_insert_breakpoint>
<amigaos_has_registers>
</amigaos_has_registers>
<amigaos_has_stack>
</amigaos_has_stack>
<amigaos_has_memory>
</amigaos_has_memory>
<amigaos_can_run>
</amigaos_can_run>
<amigaos_resume>
Shell Process: amigaos_resume: restarting 0x62039020
</amigaos_resume>
<amigaos_debug_callback>
/RAM Disk/test: amigaos_debug_callback task_p 0x62039020 (process=0x62039020)
/RAM Disk/test: Received DBHMT_OPENLIB (process=0x62039020)
/RAM Disk/test: amigaos_debug_callback returning 0
</amigaos_debug_callback>
<amigaos_debug_callback>
/RAM Disk/test: amigaos_debug_callback task_p 0x62039020 (process=0x62039020)
/RAM Disk/test: Received DBHMT_OPENLIB (process=0x62039020)
/RAM Disk/test: amigaos_debug_callback returning 0
</amigaos_debug_callback>
<amigaos_can_run>
</amigaos_can_run>
<amigaos_debug_callback>
/RAM Disk/test: amigaos_debug_callback task_p 0x62039020 (process=0x62039020)
/RAM Disk/test: Received DBHMT_CLOSELIB (process=0x62039020)
/RAM Disk/test: amigaos_debug_callback returning 0
<amigaos_wait>
Shell Process: wait ptid = 0x62039020 (FFFFFFFF), status = 0x65552878, kind 0

<is_process_alive>
Shell Process: is_process_alive for 0x62039020 is returning 1
</amigaos_debug_callback>
<amigaos_debug_callback>
/RAM Disk/test: amigaos_debug_callback task_p 0x62039020 (process=0x62039020)
</is_process_alive>
/RAM Disk/test: Received DBHMT_CLOSELIB (process=0x62039020)
Shell Process: Waiting for message (process=0x62039020)
/RAM Disk/test: amigaos_debug_callback returning 0
</amigaos_debug_callback>
<amigaos_debug_callback>
reaper.task: amigaos_debug_callback task_p 0x62039020 (process=0x62039020)
reaper.task: Recieved DBHMT_REMTASK (process=0x62039020)
reaper.task: amigaos_debug_callback returning 0
</amigaos_debug_callback>

Results from the console:

```
 4.RAM Disk:> gdb_751_commit_45 -q test
_initialize_amigaos_nat
[New inferior 0]
Reading symbols from /RAM Disk/test...done.
(gdb) break 1
break 1
target_memory_map ()
target_get_section_table ()
target_get_section_table () for exec
exec:target_xfer_partial (2, (null), 0x65552038, 0x0, 0x10004d4, 4) = 4, bytes = 3d 20 01 00
target_get_section_table ()
target_get_section_table () for exec
exec:target_xfer_partial (2, (null), 0x65552108, 0x0, 0x10004d4, 4) = 4, bytes = 3d 20 01 00
target_get_section_table ()
target_get_section_table () for exec
exec:target_xfer_partial (2, (null), 0x65552458, 0x0, 0x10004d4, 4) = 4, bytes = 3d 20 01 00
target_get_section_table ()
target_get_section_table () for exec
exec:target_xfer_partial (2, (null), 0x655526d0, 0x0, 0x10004d4, 4) = 4, bytes =
 3d 20 01 00
Breakpoint 1 at 0x10004d4: file test.c, line 1.
(gdb) r
r
t: PowerPC PPCBug monitor on port 0
 t: PowerPC PPCBug monitor on port 1
 t: DINK32 monitor
 t: Debug an Amiga process
 amigaos_can_run returning 1
t: Remote serial target in gdb-specific protocol
 t: Extended remote serial target in gdb-specific protocol
 t: Local trace dump file
```

t: Local core dump file
t: Local exec file
t: Process record and replay target
t: Process record and replay target
Starting program: /RAM Disk/test
t: PowerPC PPCBug monitor on port 0
t: PowerPC PPCBug monitor on port 1
t: DINK32 monitor
t: Debug an Amiga process
amigaos_can_run returning 1
t: Remote serial target in gdb-specific protocol
t: Extended remote serial target in gdb-specific protocol
t: Local trace dump file
t: Local core dump file
t: Local exec file
t: Process record and replay target
t: Process record and replay target
[New process 1644400672]
target_create_inferior (/RAM Disk/test, , xxx, 1)
target_terminal_ours ()
target_get_section_table ()
target_get_section_table () for exec
subtask:target_xfer_partial (10, target.xml, 0x64e14fc8, 0x0, 0x0, 4095) = -1
target_thread_architecture (process 1644400672) = 0x64e31010 [powerpc:common]
ptid_equal (null_ptid, ptid (1644400672, 0,0)
pid 1644400672 for ptid (1644400672, 0,0)
get_thread_arch_regcache (process 1644400672) = 0x64e59ee0
ptid_equal (null_ptid, ptid (1644400672, 0,0)
pid 1644400672 for ptid (1644400672, 0,0)
get_thread_arch_regcache (process 1644400672) = 0x64e59ee0
target_fetch_registers (pc) = 00000000 0x0 0
target_get_section_table ()
target_get_section_table () for exec
subtask:target_xfer_partial (11, (null), 0x64e14fc8, 0x0, 0x0, 4095) = -1
target_memory_map ()
subtask:target_xfer_partial (2, (null), 0x655522f8, 0x0, 0x10004d4, 4) = 4, bytes = 00 00 00 00
ptid_equal (null_ptid, ptid (1644400672, 0,0)
pid 1644400672 for ptid (1644400672, 0,0)
get_thread_arch_regcache (process 1644400672) = 0x64e59ee0
ptid_equal (null_ptid, ptid (1644400672, 0,0)
pid 1644400672 for ptid (1644400672, 0,0)
get_thread_arch_regcache (process 1644400672) = 0x64e59ee0
subtask:target_xfer_partial (2, (null), 0x64e153b0, 0x0, 0x10004d4, 4) = 4, bytes =
00 00 00 00
subtask:target_xfer_partial (2, (null), 0x0, 0x65553018, 0x10004d4, 4) = 4, bytes = 7d 82 10 08
target_insert_breakpoint (0x010004d4, xxx) = 0
ptid_equal (null_ptid, ptid (1644400672, 0,0)
pid 1644400672 for ptid (1644400672, 0,0)
get_thread_arch_regcache (process 1644400672) = 0x64e59ee0
ptid_equal (null_ptid, ptid (1644400672, 0,0)
pid 1644400672 for ptid (1644400672, 0,0)

get_thread_arch_regcache (process 1644400672) = 0x64e59ee0
t: PowerPC PPCBug monitor on port 0
t: PowerPC PPCBug monitor on port 1
t: DINK32 monitor
t: Debug an Amiga process
amigaos_can_run returning 1
t: Remote serial target in gdb-specific protocol
t: Extended remote serial target in gdb-specific protocol
t: Local trace dump file
t: Local core dump file
t: Local exec file
t: Process record and replay target
t: Process record and replay target
target_terminal_inferior ()
target_resume (-1, continue, 0)
t: PowerPC PPCBug monitor on port 0
t: PowerPC PPCBug monitor on port 1
t: DINK32 monitor
t: Debug an Amiga process
amigaos_can_run returning 1
t: Remote serial target in gdb-specific protocol
t: Extended remote serial target in gdb-specific protocol
t: Local trace dump file
asdfasdf
t: Local core dump file
t: Local exec file
t: Process record and replay target
t: Process record and replay target

As far as I can see when comparing serial logs from x5000 and pegasos2, x5000 do not like the "amigaos_xfer_memory()" function. It can be that it has an issue, just a crash didn't happen on other than x5000 machines by some luck (maybe that issue indirectly can have impact on non-working breakpoint code?)