Subject: : AmigaOS4
Topic: : GDB
Re: GDB
Author: : kas1e
Date: : 2021/2/26 4:07:39
URL:

@All

So, while we think if it better or not to attach/close the file via hooks inside of exec.c as it was done in our old gdb 6.3a, I made it the same, together with enabling debug output and with enabling debug gdb/target.c in both, our old gdb 6.3a and new 7.5.1 to compare what we should have and what we have. So, there results:

GDB 6.3.a

That our current SDK version, and when we run this gdb over test binary, doing a list, then set a breakpoint and type "run", that what we have in the console with enabled debug in a target.c:

```
 3/0.Work:aa> gdb_6_3a_clib2 test_dwarf2
GNU gdb 6.3 (AmigaOS build 20050719)
Copyright 2004 Free Software Foundation, Inc.
GDB is free software, covered by the GNU General Public License, and you are
welcome to change it and/or distribute copies of it under certain conditions.
Type "show copying" to see the conditions.
There is absolutely no warranty for GDB.  Type "show warranty" for details.
This GDB was configured as "ppc-amigaos"...
(gdb) list
list
target_xfer_memory (0x7fd4944c, xxx, 4, read, xxx) = 0
1    #include <stdio.h>
2    int main()
3    {
4    printf("asdfn");
5    }
(gdb) break 1
break 1
Breakpoint 1 at 0x7fd4944c: file test.c, line 1.
(gdb) r
r
Starting program: Work:aa/test_dwarf2
target_xfer_memory (0x7fd4944c, xxx, 4, read, xxx) = 4, bytes = 94 21 ff f0
target_xfer_memory (0x7fd4944c, xxx, 4, write, xxx) = 4, bytes = 7d 82 10 08
target_insert_breakpoint (0x7fd4944c, xxx) = 0
```

```
target_fetch_registers (pc) = 00000000 0x0 0
target_terminal_inferior ()
target_resume (-1, continue, 0)
target_wait (-1, status) = 1653873664,   status->kind = stopped, signal = SIGBUS
target_fetch_registers (pc) = 023aecf0 0x23aecf0 37416176
target_terminal_ours_for_output ()

Program received signal SIGBUS, Bus error.
target_xfer_memory (0x7fd4944c, xxx, 4, write, xxx) = 4, bytes = 94 21 ff f0
target_remove_breakpoint (0x7fd4944c, xxx) = 0
target_terminal_ours ()
target_fetch_registers (r1) = 02249f90 0x2249f90 35954576
0x023aecf0 in ?? ()
target_create_inferior (Work:aa/test_dwarf2, , xxx, 1)
(gdb)
```

That Sigbus error with 0x023aecf0 in ?? () there mean not a deal for us (that x5000 issue we had to deal with).

GDB 7.5.1

Now, that what we have when we doing the same (enable debug in gdb/target.c, add attaching a file via a hook in exec.c, etc). There is the console output:

```
 10/0.Work:aa> gdb_751 test
GNU gdb (GDB) 7.5.1
Copyright (C) 2012 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "ppc-amigaos".
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>...
Reading symbols from /Work/aa/test...done.
(gdb) list
list
target_memory_map ()
target_get_section_table ()
exec:target_xfer_partial (2, (null), 0x62662488, 0x0, 0x10004d4, 4) = 4, bytes = 3d 20 01 00
target_get_section_table ()
exec:target_xfer_partial (2, (null), 0x62662558, 0x0, 0x10004d4, 4) = 4, bytes = 3d 20 01 00
1    #include <stdio.h>
2    int main()
3    {
4    printf("asdfn");
5    }
(gdb) break 1
break 1
```

```
target_get_section_table ()
exec:target_xfer_partial (2, (null), 0x62662458, 0x0, 0x10004d4, 4) = 4, bytes = 3d 20 01 00
target_get_section_table ()
exec:target_xfer_partial (2, (null), 0x626626d0, 0x0, 0x10004d4, 4) = 4, bytes =
 3d 20 01 00
Breakpoint 1 at 0x10004d4: file test.c, line 1.
(gdb) r
r
Starting program: /Work/aa/test
[New process 1755977616]
target_thread_architecture (process 1755977616) = 0x61eb0018 [powerpc:common]
target_terminal_ours ()
../../gdb/target.c:3242: internal-error: Can't determine the current address space of thread process 1755977616

A problem internal to GDB has been detected,
further debugging may prove unreliable.
Quit this debugging session? (y or n) [answered Y; input not from terminal]
../../gdb/target.c:3242: internal-error: Can't determine the current address space of thread process 1755977616

A problem internal to GDB has been detected,
further debugging may prove unreliable.
Create a core file of GDB? (y or n) [answered Y; input not from terminal]
***Command 'gdb_751' returned with unfreed signals 80000000!

10/1.Work:aa>
```

See, output and calling function pretty differently. I do check both GDB sources, and for example, target_memory_map() and target_get_section_table() are new things not present in the old gdb, so that expected that they are called. But next, we fail in target_thread_architecture() with "Can't determine the current address space of thread process 1755977616"

The same happens if I test the new version on pegasos2 too, so it's not x5000 related.

I see that in old amigaos-nat we have implemented "amigaos_xfer_memory", which is then used. Through see what we have at end of amigaos-nat:

Quote:

```
/* FIXME use to_xfer_partial instead of deprecated_xfer_memory */
/**/amigaos_ops.deprecated_xfer_memory = amigaos_xfer_memory;
```

So it was already deprecated in 6.3a, and probably now (and in our in 7.5.1 too) "amigaos_xfer_partial()" is should be used instead.

At the moment i tried to just add into amigaos-nat that:

```
 static LONGEST
amigaos_xfer_partial (struct target_ops *ops, enum target_object object,
              const char *annex, gdb_byte *readbuf,
              const gdb_byte *writebuf,
              ULONGEST offset, LONGEST len)
{

   dprintf("we in ?n");

  switch (object)
    {
    case TARGET_OBJECT_MEMORY:
      dprintf("TARGET_OBJECT_MEMORYn");
      return -1;
      //amigaos_xfer_memory (offset, len, readbuf, writebuf);

    default:
      return -1;
    }

}
```

And add this:

Quote:

```
        amigaos_ops.to_xfer_partial = amigaos_xfer_partial;
```

But this one never called, instead still pure exec:target_xfer_partial is called still.

EDIT:

I then build exactly the same 7.5.1 version of GDB on my linux/x64 , enabled debug in gdb/target.c, and that how it looks like there:

```
 kas1e@kas1e-laptop:~/work/gdb-7.5.1/gdb-build/gdb$ ./gdb test
GNU gdb (GDB) 7.5.1
Copyright (C) 2012 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-unknown-linux-gnu".
```

```
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>...
Reading symbols from /home/kas1e/work/gdb-7.5.1/gdb-build/gdb/test...done.
(gdb) list
target_memory_map ()
target_get_section_table ()
exec:target_xfer_partial (2, (null), 0x7fff9fd1f280, 0x0, 0x63a, 18) = 18, bytes =
 55 48 89 e5 48 8d 3d 9f 00 00 00 e8 c6 fe ff ff ...
target_get_section_table ()
exec:target_xfer_partial (2, (null), 0x7fff9fd1f240, 0x0, 0x63a, 1) = 1, bytes =
 55
target_get_section_table ()
exec:target_xfer_partial (2, (null), 0x7fff9fd1f280, 0x0, 0x63b, 3) = 3, bytes =
 48 89 e5
target_get_section_table ()
exec:target_xfer_partial (2, (null), 0x7fff9fd1f3a0, 0x0, 0x63a, 18) = 18, bytes =
 55 48 89 e5 48 8d 3d 9f 00 00 00 e8 c6 fe ff ff ...
target_get_section_table ()
exec:target_xfer_partial (2, (null), 0x7fff9fd1f360, 0x0, 0x63a, 1) = 1, bytes =
 55
target_get_section_table ()
exec:target_xfer_partial (2, (null), 0x7fff9fd1f3a0, 0x0, 0x63b, 3) = 3, bytes =
 48 89 e5
1    #include <stdio.h>
2    int main()
3    {
4    printf("asdfasdfn");
5    }
(gdb) break 1
target_get_section_table ()
exec:target_xfer_partial (2, (null), 0x7fff9fd1f280, 0x0, 0x63a, 18) = 18, bytes =
 55 48 89 e5 48 8d 3d 9f 00 00 00 e8 c6 fe ff ff ...
target_get_section_table ()
exec:target_xfer_partial (2, (null), 0x7fff9fd1f240, 0x0, 0x63a, 1) = 1, bytes =
 55
target_get_section_table ()
exec:target_xfer_partial (2, (null), 0x7fff9fd1f280, 0x0, 0x63b, 3) = 3, bytes =
 48 89 e5
target_get_section_table ()
exec:target_xfer_partial (2, (null), 0x7fff9fd1f950, 0x0, 0x63e, 1) = 1, bytes =
 48
Breakpoint 1 at 0x63e: file test.c, line 1.
(gdb) r
Starting program: /home/kas1e/work/gdb-7.5.1/gdb-build/gdb/test
target_wait (17726, status) = 17726,   status->kind = stopped, signal = SIGTRAP
target_terminal_init ()
target_terminal_inferior ()
target_resume (17726, continue, 0)
target_wait (17726, status) = 17726,   status->kind = stopped, signal = SIGTRAP
target_post_startup_inferior (17726)
target_create_inferior (/home/kas1e/work/gdb-7.5.1/gdb-build/gdb/test, , xxx, 1)
```

```
target_terminal_ours ()
child:target_xfer_partial (10, target.xml, 0x5652742ee400, 0x0, 0x0, 4095) = -1
target_thread_architecture (process 17726) = 0x5652742ef420 [i386:x86-64]
target_thread_address_space (process 17726) = 1
target_fetch_registers (rip) = 9040ddf7ff7f0000 0x7ffff7dd4090 140737351860368
child:target_xfer_partial (6, (null), 0x5652742f9880, 0x0, 0x0, 4096) = 320, bytes =
 21 00 00 00 00 00 00 00 00 a0 ff f7 ff 7f 00 00 ...
child:target_xfer_partial (6, (null), 0x5652742f99c0, 0x0, 0x140, 3776) = 0
target_memory_map ()
child:target_xfer_partial (2, (null), 0x5652742fa890, 0x0, 0x555555554040, 504) = 504, bytes =
 06 00 00 00 04 00 00 00 40 00 00 00 00 00 00 00 ...
child:target_xfer_partial (2, (null), 0x7fff9fd1ef10, 0x0, 0x55555555463a, 18) = 6, bytes =
 55 48 89 e5 48 8d
child:target_xfer_partial (2, (null), 0x7fff9fd1ef16, 0x0, 0x555555554640, 12) = 8, bytes =
3d 9f 00 00 00 e8 c6 fe
child:target_xfer_partial (2, (null), 0x7fff9fd1ef1e, 0x0, 0x555555554648, 4) = 4, bytes = ff ff ...
child:target_xfer_partial (2, (null), 0x7fff9fd1eed0, 0x0, 0x55555555463a, 1) = 1, bytes =
 55
child:target_xfer_partial (2, (null), 0x7fff9fd1ef10, 0x0, 0x55555555463b, 3) = 3, bytes =
 48 89 e5
child:target_xfer_partial (2, (null), 0x7fff9fd1fa10, 0x0, 0x555555554040, 56) = 56, bytes =
 06 00 00 00 04 00 00 00 40 00 00 00 00 00 00 00 ...
child:target_xfer_partial (2, (null), 0x7fff9fd1fa10, 0x0, 0x555555554078, 56) = 56, bytes =
 03 00 00 00 04 00 00 00 38 02 00 00 00 00 00 00 ...
child:target_xfer_partial (2, (null), 0x7fff9fd1fa10, 0x0, 0x5555555540b0, 56) = 56, bytes =
 01 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 ...
child:target_xfer_partial (2, (null), 0x7fff9fd1fa10, 0x0, 0x5555555540e8, 56) = 56, bytes =
 01 00 00 00 06 00 00 00 b8 0d 00 00 00 00 00 00 ...
child:target_xfer_partial (2, (null), 0x7fff9fd1fa10, 0x0, 0x555555554120, 56) = 56, bytes =
 02 00 00 00 06 00 00 00 c8 0d 00 00 00 00 00 00 ...
child:target_xfer_partial (2, (null), 0x5652742faa90, 0x0, 0x555555754dc8, 496) = 496, bytes =
 01 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 ...
child:target_xfer_partial (2, (null), 0x7fff9fd1faa0, 0x0, 0x555555754e90, 8) = 8, bytes =
 00 00 00 00 00 00 00 00
child:target_xfer_partial (2, (null), 0x7fff9fd1fa10, 0x0, 0x555555554040, 56) = 56, bytes =
 06 00 00 00 04 00 00 00 40 00 00 00 00 00 00 00 ...
child:target_xfer_partial (2, (null), 0x7fff9fd1fa10, 0x0, 0x555555554078, 56) = 56, bytes =
 03 00 00 00 04 00 00 00 38 02 00 00 00 00 00 00 ...
child:target_xfer_partial (2, (null), 0x7fff9fd1fa10, 0x0, 0x5555555540b0, 56) = 56, bytes =
 01 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 ...
child:target_xfer_partial (2, (null), 0x7fff9fd1fa10, 0x0, 0x5555555540e8, 56) = 56, bytes =
 01 00 00 00 06 00 00 00 b8 0d 00 00 00 00 00 00 ...
child:target_xfer_partial (2, (null), 0x7fff9fd1fa10, 0x0, 0x555555554120, 56) = 56, bytes =
 02 00 00 00 06 00 00 00 c8 0d 00 00 00 00 00 00 ...
child:target_xfer_partial (2, (null), 0x5652742faa90, 0x0, 0x555555754dc8, 496) = 496, bytes =
 01 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 ...
child:target_xfer_partial (2, (null), 0x7fff9fd1faa0, 0x0, 0x555555754e90, 8) = 8, bytes =
 00 00 00 00 00 00 00 00
child:target_xfer_partial (2, (null), 0x7fff9fd1eff0, 0x0, 0x55555555463a, 18) = 6, bytes =
 55 48 89 e5 48 8d
child:target_xfer_partial (2, (null), 0x7fff9fd1eff6, 0x0, 0x555555554640, 12) = 8, bytes = 3d 9f 00 00 00 e8 c6 fe
```

```
child:target_xfer_partial (2, (null), 0x7fff9fd1effe, 0x0, 0x555555554648, 4) = 4, bytes = ff ff ...
child:target_xfer_partial (2, (null), 0x7fff9fd1efb0, 0x0, 0x55555555463a, 1) = 1, bytes =
 55
child:target_xfer_partial (2, (null), 0x7fff9fd1eff0, 0x0, 0x55555555463b, 3) = 3, bytes =
 48 89 e5
target_close (0)
child:target_xfer_partial (2, (null), 0x7fff9fd1f0c0, 0x0, 0x55555555463a, 18) = 6, bytes =
 55 48 89 e5 48 8d
child:target_xfer_partial (2, (null), 0x7fff9fd1f0c6, 0x0, 0x555555554640, 12) = 8, bytes =
3d 9f 00 00 00 e8 c6 fe
child:target_xfer_partial (2, (null), 0x7fff9fd1f0ce, 0x0, 0x555555554648, 4) = 4, bytes = ff ff ...
child:target_xfer_partial (2, (null), 0x7fff9fd1f080, 0x0, 0x55555555463a, 1) = 1, bytes =
 55
child:target_xfer_partial (2, (null), 0x7fff9fd1f0c0, 0x0, 0x55555555463b, 3) = 3, bytes =
 48 89 e5
target_can_run () = 1
child:target_xfer_partial (2, (null), 0x7fff9fd1fab0, 0x0, 0x7ffff7ffa000, 64) = 64, bytes =
 7f 45 4c 46 02 01 01 00 00 00 00 00 00 00 00 00 ...
child:target_xfer_partial (2, (null), 0x5652742ede50, 0x0, 0x7ffff7ffa040, 224) = 224, bytes =
 01 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 ...
child:target_xfer_partial (2, (null), 0x5652742fb330, 0x0, 0x7ffff7ffa000, 5408) = 5408, bytes =
 7f 45 4c 46 02 01 01 00 00 00 00 00 00 00 00 00 ...
child:target_xfer_partial (2, (null), 0x7fff9fd1ef00, 0x0, 0x55555555463a, 18) = 6, bytes =
 55 48 89 e5 48 8d
child:target_xfer_partial (2, (null), 0x7fff9fd1ef06, 0x0, 0x555555554640, 12) = 8, bytes =
3d 9f 00 00 00 e8 c6 fe
child:target_xfer_partial (2, (null), 0x7fff9fd1ef0e, 0x0, 0x555555554648, 4) = 4, bytes = ff ff ...
child:target_xfer_partial (2, (null), 0x7fff9fd1eec0, 0x0, 0x55555555463a, 1) = 1, bytes =
 55
child:target_xfer_partial (2, (null), 0x7fff9fd1ef00, 0x0, 0x55555555463b, 3) = 3, bytes =
 48 89 e5
target_thread_address_space (process 17726) = 1
target_thread_address_space (process 17726) = 1
target_prepare_to_store ()
target_store_registers (orig_rax) = ffffffffffffffff 0xffffffffffffffff -1
child:target_xfer_partial (2, (null), 0x7fff9fd1fb70, 0x0, 0x55555555463e, 1) = 1, bytes =
 48
child:target_xfer_partial (3, (null), 0x0, 0x565272cbd4a0, 0x55555555463e, 1) = 1, bytes =
 cc
target_insert_breakpoint (0x000055555555463e, xxx) = 0
child:target_xfer_partial (2, (null), 0x7fff9fd1fb70, 0x0, 0x7ffff7de3f60, 1) = 1, bytes =
 f3
child:target_xfer_partial (3, (null), 0x0, 0x565272cbd4a0, 0x7ffff7de3f60, 1) = 1, bytes =
 cc
target_insert_breakpoint (0x00007ffff7de3f60, xxx) = 0
target_thread_address_space (process 17726) = 1
target_thread_address_space (process 17726) = 1
target_terminal_inferior ()
target_pass_signals (151, {
SIGALRM SIGURG SIGCHLD SIGIO SIGVTALRM SIGPROF SIGWINCH SIGPOLL SIGWAITING SIGLWP SI
GPRIO SIGCANCEL })
```

```
target_resume (17726, continue, 0)
target_wait (-1, status) = 17726,   status->kind = stopped, signal = SIGTRAP
target_thread_architecture (process 17726) = 0x5652742ef420 [i386:x86-64]
target_thread_address_space (process 17726) = 1
target_fetch_registers (rip) = 613fdef7ff7f0000 0x7ffff7de3f61 140737351925601
target_prepare_to_store ()
target_store_registers (rip) = 603fdef7ff7f0000 0x7ffff7de3f60 140737351925600
target_thread_address_space (process 17726) = 1
target_thread_address_space (process 17726) = 1
target_thread_address_space (process 17726) = 1
target_stopped_by_watchpoint () = 0
target_thread_address_space (process 17726) = 1
target_thread_address_space (process 17726) = 1
target_terminal_ours_for_output ()
child:target_xfer_partial (2, (null), 0x7fff9fd1f410, 0x0, 0x555555554040, 56) = 56, bytes =
 06 00 00 00 04 00 00 00 40 00 00 00 00 00 00 00 ...
child:target_xfer_partial (2, (null), 0x7fff9fd1f410, 0x0, 0x555555554078, 56) = 56, bytes =
 03 00 00 00 04 00 00 00 38 02 00 00 00 00 00 00 ...
child:target_xfer_partial (2, (null), 0x7fff9fd1f410, 0x0, 0x5555555540b0, 56) = 56, bytes =
 01 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 ...
child:target_xfer_partial (2, (null), 0x7fff9fd1f410, 0x0, 0x5555555540e8, 56) = 56, bytes =
 01 00 00 00 06 00 00 00 b8 0d 00 00 00 00 00 00 ...
child:target_xfer_partial (2, (null), 0x7fff9fd1f410, 0x0, 0x555555554120, 56) = 56, bytes =
 02 00 00 00 06 00 00 00 c8 0d 00 00 00 00 00 00 ...
child:target_xfer_partial (2, (null), 0x5652742faa90, 0x0, 0x555555754dc8, 496) = 496, bytes =
 01 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 ...
child:target_xfer_partial (2, (null), 0x7fff9fd1f4a0, 0x0, 0x555555754e90, 8) = 8, bytes =
 40 e1 ff f7 ff 7f 00 00
child:target_xfer_partial (2, (null), 0x7fff9fd1f490, 0x0, 0x7ffff7ffe148, 8) = 8, bytes =
 70 e1 ff f7 ff 7f 00 00
child:target_xfer_partial (2, (null), 0x5652742fb070, 0x0, 0x7ffff7ffe170, 40) = 40, bytes =
 00 40 55 55 55 55 00 00 00 e7 ff f7 ff 7f 00 00 ...
child:target_xfer_partial (2, (null), 0x5652742fadd0, 0x0, 0x7ffff7ffd9f0, 40) = 40, bytes =
 00 30 dd f7 ff 7f 00 00 38 42 55 55 55 55 00 00 ...
child:target_xfer_partial (2, (null), 0x7fff9fd1f454, 0x0, 0x555555554238, 4) = 4, bytes = 2f 6c 69 62
child:target_xfer_partial (2, (null), 0x7fff9fd1f454, 0x0, 0x55555555423c, 4) = 4, bytes = 36 34 2f 6c
child:target_xfer_partial (2, (null), 0x7fff9fd1f454, 0x0, 0x555555554240, 4) = 4, bytes = 64 2d 6c 69
child:target_xfer_partial (2, (null), 0x7fff9fd1f454, 0x0, 0x555555554244, 4) = 4, bytes = 6e 75 78 2d
child:target_xfer_partial (2, (null), 0x7fff9fd1f454, 0x0, 0x555555554248, 4) = 4, bytes = 78 38 36 2d
child:target_xfer_partial (2, (null), 0x7fff9fd1f454, 0x0, 0x55555555424c, 4) = 4, bytes = 36 34 2e 73
child:target_xfer_partial (2, (null), 0x7fff9fd1f454, 0x0, 0x555555554250, 4) = 4, bytes = 6f 2e 32 00
child:target_xfer_partial (2, (null), 0x5652742f28e0, 0x0, 0x7ffff7ffe710, 40) = 40, bytes =
 00 a0 ff f7 ff 7f 00 00 b0 eb ff f7 ff 7f 00 00 ...
child:target_xfer_partial (2, (null), 0x7fff9fd1f454, 0x0, 0x7ffff7ffebb0, 4) = 4, bytes = 6c 69 6e 75
child:target_xfer_partial (2, (null), 0x7fff9fd1f454, 0x0, 0x7ffff7ffebb4, 4) = 4, bytes = 78 2d 76 64
child:target_xfer_partial (2, (null), 0x7fff9fd1f454, 0x0, 0x7ffff7ffebb8, 4) = 4, bytes = 73 6f 2e 73
child:target_xfer_partial (2, (null), 0x7fff9fd1f454, 0x0, 0x7ffff7ffebbc, 4) = 4, bytes = 6f 2e 31 00
child:target_xfer_partial (2, (null), 0x7fff9fd1f4e0, 0x0, 0x7ffff7ffe140, 4) = 4, bytes =
 01 00 00 00
target_terminal_ours ()
warning: Could not load shared library symbols for linux-vdso.so.1.
```

Do you need "set solib-search-path" or "set sysroot"?
target_terminal_inferior ()
target_thread_address_space (process 17726) = 1
target_thread_address_space (process 17726) = 1
child:target_xfer_partial (3, (null), 0x0, 0x5652742b0ad4, 0x55555555463e, 1) = 1, bytes = 48
target_remove_breakpoint (0x000055555555463e, xxx) = 0
child:target_xfer_partial (3, (null), 0x0, 0x5652742fb294, 0x7ffff7de3f60, 1) = 1, bytes = f3
target_remove_breakpoint (0x00007ffff7de3f60, xxx) = 0
target_thread_address_space (process 17726) = 1
target_terminal_inferior ()
target_pass_signals (0, { })
target_resume (17726, step, 0)
target_wait (-1, status) = 17726,   status->kind = stopped, signal = SIGTRAP
target_thread_architecture (process 17726) = 0x5652742ef420 [i386:x86-64]
target_thread_address_space (process 17726) = 1
target_fetch_registers (rip) = 126eddf7ff7f0000 0x7ffff7dd6e12 140737351872018
target_thread_address_space (process 17726) = 1
target_thread_address_space (process 17726) = 1
target_thread_address_space (process 17726) = 1
target_stopped_by_watchpoint () = 0
target_thread_address_space (process 17726) = 1
target_thread_address_space (process 17726) = 1
target_thread_address_space (process 17726) = 1
child:target_xfer_partial (2, (null), 0x7fff9fd1f5d0, 0x0, 0x55555555463e, 1) = 1, bytes =
 48
child:target_xfer_partial (3, (null), 0x0, 0x565272cbd4a0, 0x55555555463e, 1) = 1, bytes =
 cc
target_insert_breakpoint (0x000055555555463e, xxx) = 0
child:target_xfer_partial (2, (null), 0x7fff9fd1f5d0, 0x0, 0x7ffff7de3f60, 1) = 1, bytes =
 f3
child:target_xfer_partial (3, (null), 0x0, 0x565272cbd4a0, 0x7ffff7de3f60, 1) = 1, bytes =
 cc
target_insert_breakpoint (0x00007ffff7de3f60, xxx) = 0
target_thread_address_space (process 17726) = 1
target_terminal_inferior ()
target_pass_signals (151, {
SIGALRM SIGURG SIGCHLD SIGIO SIGVTALRM SIGPROF SIGWINCH SIGPOLL SIGWAITING SIGLWP SI
GPRIO SIGCANCEL })
target_resume (17726, continue, 0)
target_wait (-1, status) = 17726,   status->kind = stopped, signal = SIGTRAP
target_thread_architecture (process 17726) = 0x5652742ef420 [i386:x86-64]
target_thread_address_space (process 17726) = 1
target_fetch_registers (rip) = 613fdef7ff7f0000 0x7ffff7de3f61 140737351925601
target_prepare_to_store ()
target_store_registers (rip) = 603fdef7ff7f0000 0x7ffff7de3f60 140737351925600
target_thread_address_space (process 17726) = 1
target_thread_address_space (process 17726) = 1
target_thread_address_space (process 17726) = 1
target_stopped_by_watchpoint () = 0
target_thread_address_space (process 17726) = 1
target_thread_address_space (process 17726) = 1

target_terminal_ours_for_output ()
child:target_xfer_partial (2, (null), 0x7fff9fd1f410, 0x0, 0x555555554040, 56) = 56, bytes =
06 00 00 00 04 00 00 00 40 00 00 00 00 00 00 00 ...
child:target_xfer_partial (2, (null), 0x7fff9fd1f410, 0x0, 0x555555554078, 56) = 56, bytes =
03 00 00 00 04 00 00 00 38 02 00 00 00 00 00 00 ...
child:target_xfer_partial (2, (null), 0x7fff9fd1f410, 0x0, 0x5555555540b0, 56) = 56, bytes =
01 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 ...
child:target_xfer_partial (2, (null), 0x7fff9fd1f410, 0x0, 0x5555555540e8, 56) = 56, bytes =
01 00 00 00 06 00 00 00 b8 0d 00 00 00 00 00 00 ...
child:target_xfer_partial (2, (null), 0x7fff9fd1f410, 0x0, 0x555555554120, 56) = 56, bytes =
02 00 00 00 06 00 00 00 c8 0d 00 00 00 00 00 00 ...
child:target_xfer_partial (2, (null), 0x5652742faa90, 0x0, 0x555555754dc8, 496) = 496, bytes =
01 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 ...
child:target_xfer_partial (2, (null), 0x7fff9fd1f4a0, 0x0, 0x555555754e90, 8) = 8, bytes =
40 e1 ff f7 ff 7f 00 00
child:target_xfer_partial (2, (null), 0x7fff9fd1f490, 0x0, 0x7ffff7ffe148, 8) = 8, bytes =
70 e1 ff f7 ff 7f 00 00
child:target_xfer_partial (2, (null), 0x5652742f7c50, 0x0, 0x7ffff7ffe170, 40) = 40, bytes =
00 40 55 55 55 55 00 00 00 e7 ff f7 ff 7f 00 00 ...
child:target_xfer_partial (2, (null), 0x5652742f28e0, 0x0, 0x7ffff7ffe710, 40) = 40, bytes =
00 a0 ff f7 ff 7f 00 00 b0 eb ff f7 ff 7f 00 00 ...
child:target_xfer_partial (2, (null), 0x7fff9fd1f454, 0x0, 0x7ffff7ffebb0, 4) = 4, bytes = 6c 69 6e 75
child:target_xfer_partial (2, (null), 0x7fff9fd1f454, 0x0, 0x7ffff7ffebb4, 4) = 4, bytes = 78 2d 76 64
child:target_xfer_partial (2, (null), 0x7fff9fd1f454, 0x0, 0x7ffff7ffebb8, 4) = 4, bytes = 73 6f 2e 73
child:target_xfer_partial (2, (null), 0x7fff9fd1f454, 0x0, 0x7ffff7ffebbc, 4) = 4, bytes = 6f 2e 31 00
child:target_xfer_partial (2, (null), 0x5652742f7c50, 0x0, 0x7ffff7fd5000, 40) = 40, bytes =
00 20 9e f7 ff 7f 00 00 d0 ed ff f7 ff 7f 00 00 ...
child:target_xfer_partial (2, (null), 0x7fff9fd1f454, 0x0, 0x7ffff7ffedd0, 4) = 4, bytes = 2f 6c 69 62
child:target_xfer_partial (2, (null), 0x7fff9fd1f454, 0x0, 0x7ffff7ffedd4, 4) = 4, bytes = 2f 78 38 36
child:target_xfer_partial (2, (null), 0x7fff9fd1f454, 0x0, 0x7ffff7ffedd8, 4) = 4, bytes = 5f 36 34 2d
child:target_xfer_partial (2, (null), 0x7fff9fd1f454, 0x0, 0x7ffff7ffeddc, 4) = 4, bytes = 6c 69 6e 75
child:target_xfer_partial (2, (null), 0x7fff9fd1f454, 0x0, 0x7ffff7ffede0, 4) = 4, bytes = 78 2d 67 6e
child:target_xfer_partial (2, (null), 0x7fff9fd1f454, 0x0, 0x7ffff7ffede4, 4) = 4, bytes = 75 2f 6c 69
child:target_xfer_partial (2, (null), 0x7fff9fd1f454, 0x0, 0x7ffff7ffede8, 4) = 4, bytes = 62 63 2e 73
child:target_xfer_partial (2, (null), 0x7fff9fd1f454, 0x0, 0x7ffff7ffedec, 4) = 4, bytes = 6f 2e 36 00
child:target_xfer_partial (2, (null), 0x5652742e7390, 0x0, 0x7ffff7ffd9f0, 40) = 40, bytes =
00 30 dd f7 ff 7f 00 00 38 42 55 55 55 55 00 00 ...
child:target_xfer_partial (2, (null), 0x7fff9fd1f454, 0x0, 0x555555554238, 4) = 4, bytes = 2f 6c 69 62
child:target_xfer_partial (2, (null), 0x7fff9fd1f454, 0x0, 0x55555555423c, 4) = 4, bytes = 36 34 2f 6c
child:target_xfer_partial (2, (null), 0x7fff9fd1f454, 0x0, 0x555555554240, 4) = 4, bytes = 64 2d 6c 69
child:target_xfer_partial (2, (null), 0x7fff9fd1f454, 0x0, 0x555555554244, 4) = 4, bytes = 6e 75 78 2d
child:target_xfer_partial (2, (null), 0x7fff9fd1f454, 0x0, 0x555555554248, 4) = 4, bytes = 78 38 36 2d
child:target_xfer_partial (2, (null), 0x7fff9fd1f454, 0x0, 0x55555555424c, 4) = 4, bytes = 36 34 2e 73
child:target_xfer_partial (2, (null), 0x7fff9fd1f454, 0x0, 0x555555554250, 4) = 4, bytes = 6f 2e 32 00
child:target_xfer_partial (2, (null), 0x7fff9fd1f4e0, 0x0, 0x7ffff7ffe140, 4) = 4, bytes =
01 00 00 00
child:target_xfer_partial (2, (null), 0x7fff9fd1e9f0, 0x0, 0x55555555463a, 18) = 6, bytes =
55 48 89 e5 48 8d
child:target_xfer_partial (2, (null), 0x7fff9fd1e9f6, 0x0, 0x555555554640, 12) = 8, bytes =
3d 9f 00 00 00 e8 c6 fe
child:target_xfer_partial (2, (null), 0x7fff9fd1e9fe, 0x0, 0x555555554648, 4) = 4, bytes = ff ff ...

child:target_xfer_partial (2, (null), 0x7fff9fd1e9b0, 0x0, 0x55555555463a, 1) = 1, bytes =
55
child:target_xfer_partial (2, (null), 0x7fff9fd1e9f0, 0x0, 0x55555555463b, 3) = 3, bytes =
48 89 e5
target_terminal_inferior ()
target_thread_address_space (process 17726) = 1
target_thread_address_space (process 17726) = 1
target_thread_address_space (process 17726) = 1
child:target_xfer_partial (3, (null), 0x0, 0x5652742ee4a4, 0x55555555463e, 1) = 1, bytes = 48
target_remove_breakpoint (0x000055555555463e, xxx) = 0
child:target_xfer_partial (3, (null), 0x0, 0x5652742fb294, 0x7ffff7de3f60, 1) = 1, bytes = f3
target_remove_breakpoint (0x00007ffff7de3f60, xxx) = 0
target_thread_address_space (process 17726) = 1
target_terminal_inferior ()
target_pass_signals (0, { })
target_resume (17726, step, 0)
target_wait (-1, status) = 17726,   status->kind = stopped, signal = SIGTRAP
target_thread_architecture (process 17726) = 0x5652742ef420 [i386:x86-64]
target_thread_address_space (process 17726) = 1
target_fetch_registers (rip) = f174ddf7ff7f0000 0x7ffff7dd74f1 140737351873777
target_thread_address_space (process 17726) = 1
target_thread_address_space (process 17726) = 1
target_thread_address_space (process 17726) = 1
target_stopped_by_watchpoint () = 0
target_thread_address_space (process 17726) = 1
target_thread_address_space (process 17726) = 1
target_thread_address_space (process 17726) = 1
child:target_xfer_partial (2, (null), 0x7fff9fd1f5d0, 0x0, 0x55555555463e, 1) = 1, bytes =
48
child:target_xfer_partial (3, (null), 0x0, 0x565272cbd4a0, 0x55555555463e, 1) = 1, bytes =
cc
target_insert_breakpoint (0x000055555555463e, xxx) = 0
child:target_xfer_partial (2, (null), 0x7fff9fd1f5d0, 0x0, 0x7ffff7de3f60, 1) = 1, bytes =
f3
child:target_xfer_partial (3, (null), 0x0, 0x565272cbd4a0, 0x7ffff7de3f60, 1) = 1, bytes =
cc
target_insert_breakpoint (0x00007ffff7de3f60, xxx) = 0
target_thread_address_space (process 17726) = 1
target_terminal_inferior ()
target_pass_signals (151, {
SIGALRM SIGURG SIGCHLD SIGIO SIGVTALRM SIGPROF SIGWINCH SIGPOLL SIGWAITING SIGLWP SI
GPRIO SIGCANCEL })
target_resume (17726, continue, 0)
target_wait (-1, status) = 17726,   status->kind = stopped, signal = SIGTRAP
target_thread_architecture (process 17726) = 0x5652742ef420 [i386:x86-64]
target_thread_address_space (process 17726) = 1
target_fetch_registers (rip) = 3f46555555550000 0x55555555463f 93824992233023
target_prepare_to_store ()
target_store_registers (rip) = 3e46555555550000 0x55555555463e 93824992233022
target_thread_address_space (process 17726) = 1
target_thread_address_space (process 17726) = 1

```
target_thread_address_space (process 17726) = 1
target_stopped_by_watchpoint () = 0
target_thread_address_space (process 17726) = 1
target_thread_address_space (process 17726) = 1
child:target_xfer_partial (3, (null), 0x0, 0x5652742ee4a4, 0x55555555463e, 1) = 1, bytes = 48
target_remove_breakpoint (0x000055555555463e, xxx) = 0
child:target_xfer_partial (3, (null), 0x0, 0x5652742fb294, 0x7ffff7de3f60, 1) = 1, bytes = f3
target_remove_breakpoint (0x00007ffff7de3f60, xxx) = 0
target_terminal_ours ()
target_thread_address_space (process 17726) = 1

target_thread_address_space (process 17726) = 1
child:target_xfer_partial (2, (null), 0x7fff9fd1faf7, 0x0, 0x55555555463e, 1) = 1, bytes = 48
child:target_xfer_partial (2, (null), 0x7fff9fd1faf7, 0x0, 0x55555555463e, 1) = 1, bytes = 48
child:target_xfer_partial (3, (null), 0x565274335d5c, 0x0, 0x7fffffffde80, 64) = 64, bytes = 60 46 55 55 ...
child:target_xfer_partial (4, (null), 0x5652742f9820, 0x0, 0x7fffffffdea8, 8) = 8, bytes =
 f7 3b a0 f7 ff 7f 00 00
target_thread_address_space (process 17726) = 1
target_thread_address_space (process 17726) = 1
Breakpoint 1, main () at test.c:4
4    printf("asdfasdfn");
target_thread_address_space (process 17726) = 1
(gdb)
```

As can be seen those "nulls" in the exec:target_xfer_partial at the begining are fine, and then on x86 we have:

Quote:

> target_thread_architecture (process 17726) = 0x5652742ef420 [i386:x86-64]
> target_thread_address_space (process 17726) = 1

So on our side we didn't reach "target_thread_address_space" and fail right after "target_thread_architecture".

And our failing part in gdb/target.c are:

```
 /* Determine the current address space of thread PTID.  */

struct address_space *
target_thread_address_space (ptid_t ptid)
{
  struct address_space *aspace;
  struct inferior *inf;
  struct target_ops *t;

  for (t = current_target.beneath; t != NULL; t = t->beneath)
```

```
  {
    if (t->to_thread_address_space != NULL)
  {
    aspace = t->to_thread_address_space (t, ptid);
    gdb_assert (aspace);

    if (targetdebug)
      fprintf_unfiltered (gdb_stdlog,
            "target_thread_address_space (%s) = %dn",
            target_pid_to_str (ptid),
            address_space_num (aspace));
    return aspace;
  }
  }

 /* Fall-back to the "main" address space of the inferior.  */
 inf = find_inferior_pid (ptid_get_pid (ptid));

 if (inf == NULL || inf->aspace == NULL)
   internal_error (__FILE__, __LINE__,
         _("Can't determine the current "
           "address space of thread %sn"),
         target_pid_to_str (ptid));

 return inf->aspace;
}
```

Added few printfs, and:

1). for first we never go inside of the for (t = current_target.beneath; t != NULL; t = t->beneath) loop.
2). when we "fallback", inf is NULL too.