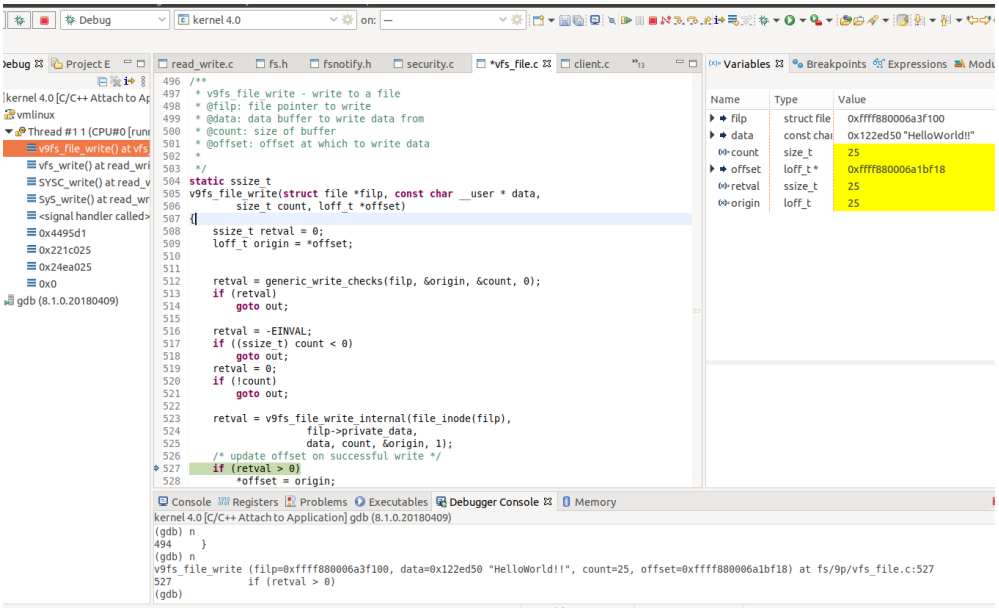
作業系統

407510046 經濟三 黃郁雯

甲.

```
/mnt/sharedFolder/hw09 # mount
rootfs on / type rootfs (rw,size=115272k,nr_inodes=28818)
proc on /proc type proc (rw,relatime)
tmpfs on /tmp type tmpfs (rw,relatime)
sysfs on /sys type sysfs (rw,relatime)
tmpfs on /dev type tmpfs (rw,relatime)
debugfs on /sys/kernel/debug type debugfs (rw,relatime)
sharedFolder on /mnt/sharedFolder type 9p (rw,sync,dirsync,relatime,trans=virtio
,version=9p2000.L,nobootwait)
devpts on /dev/pts type devpts (rw,relatime,mode=600)
/mnt/sharedFolder/hw09 # ls
makefile            write_w_newline     write_w_newline.c
/mnt/sharedFolder/hw09 # ./write_w_newline
```



乙.

fdget_pos：透過__to_fd 回傳 struct fd 物件,取得 unsigned long, return __to_fd(__fdget_pos(fd))

__to_fd：return {(structfile*)(v&~3),v&3}

file_pos_read(f.file)：如果 fd f 有符合 file 結構體，取得當前檔案位置 pos

vfs_write：參數 buf，為指向用戶空間的內存地址

loff_t *pos=>pos 表示從何處開始寫入，其值需要初始化

EX: loff_t pos = fp->f_pos

__vfs_write：內部包含了 file_start_write 和 file_end_write，利用 file->f_op->write 寫入檔案

v9fs_file_write：將資料寫入 fs/9p/位置

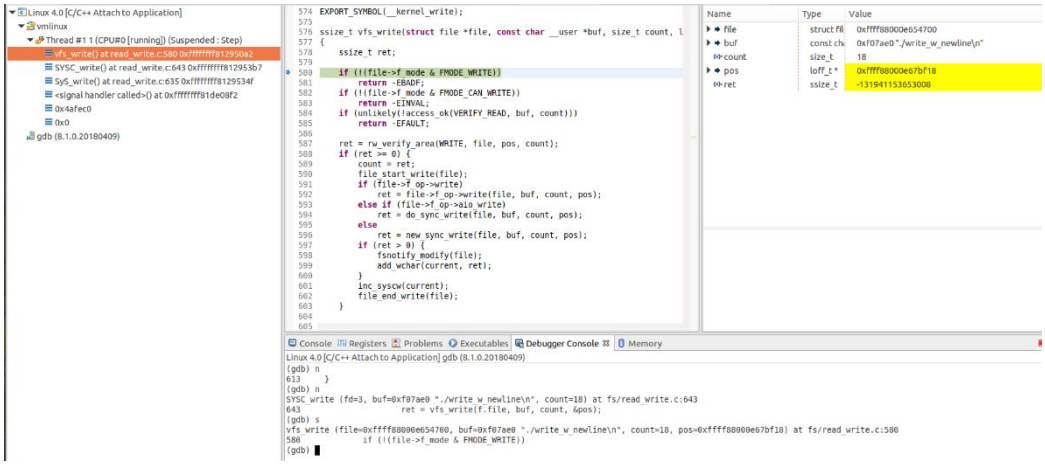
*file_inode：打開檔案

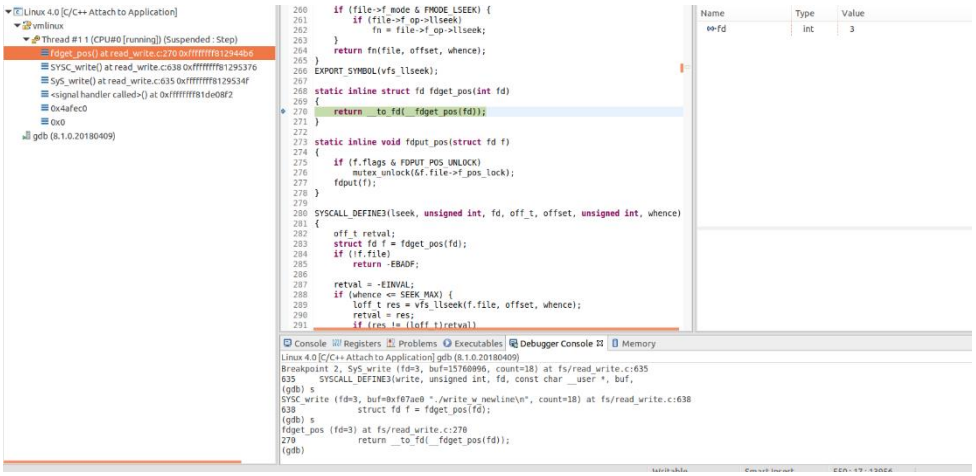
new_sync_write：初始化 kiocb,並調用 call_write_iter

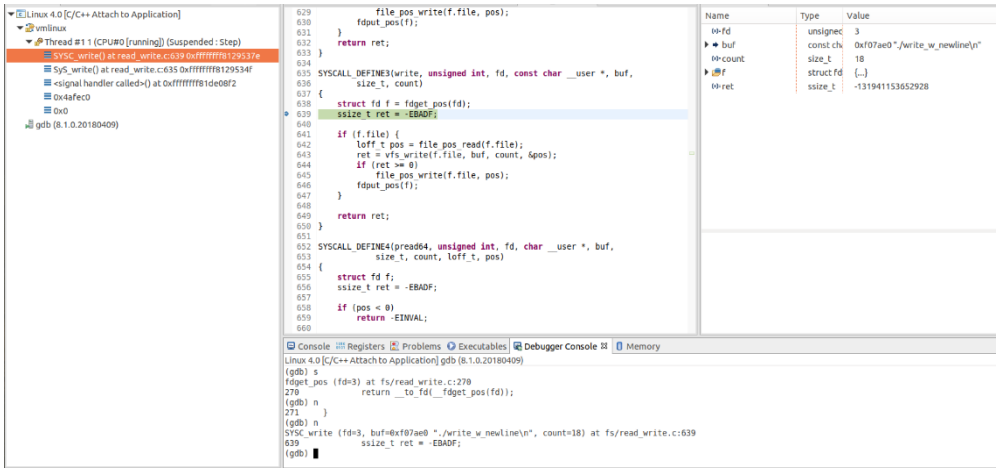
__always_inline：inline 是行內函式，是指將此 function 的內容整合至呼叫此函式位置

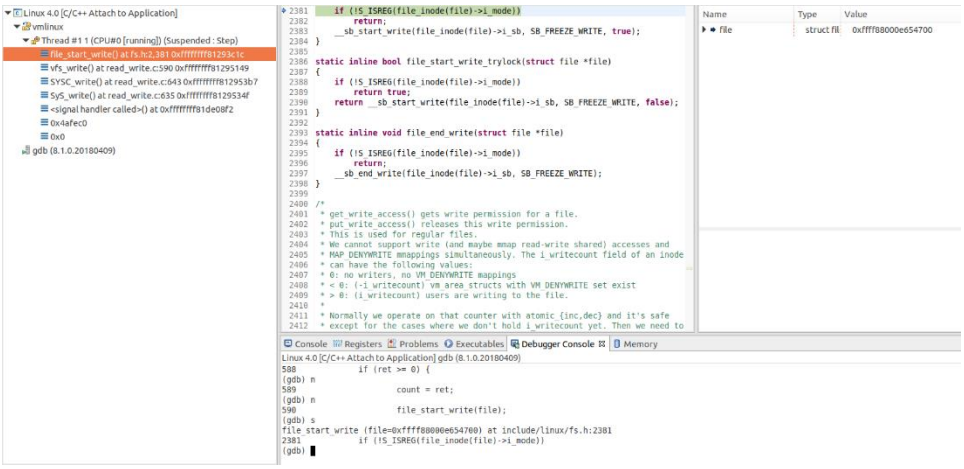
file_end_write：停止檔案書寫

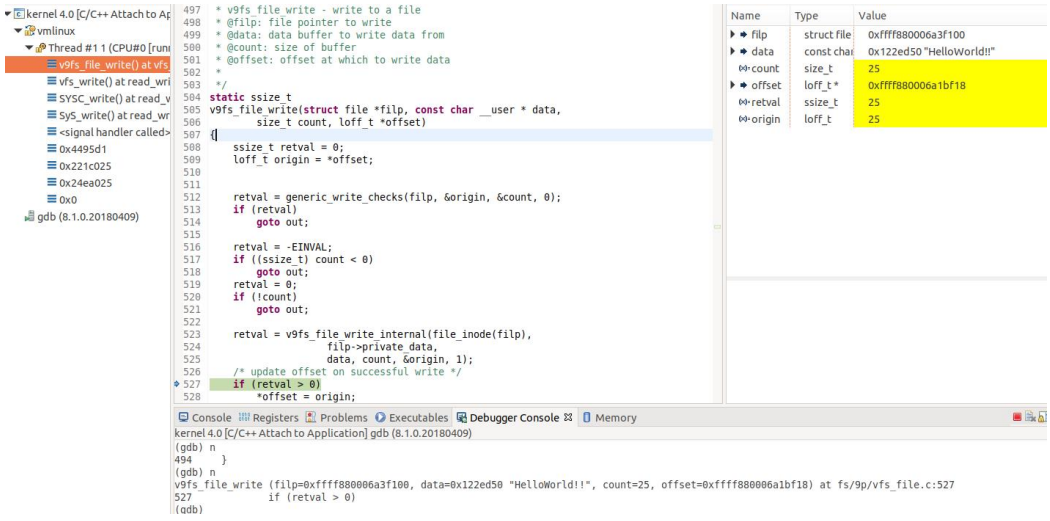
丙.

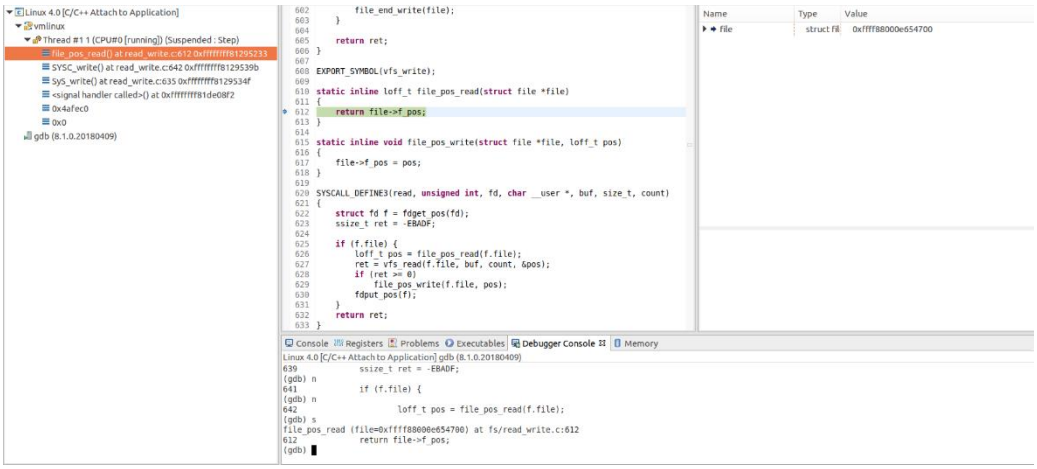


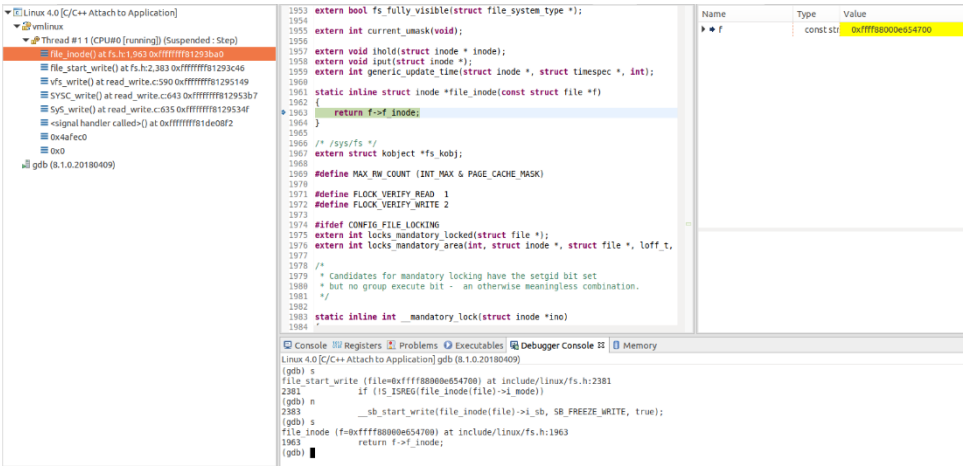


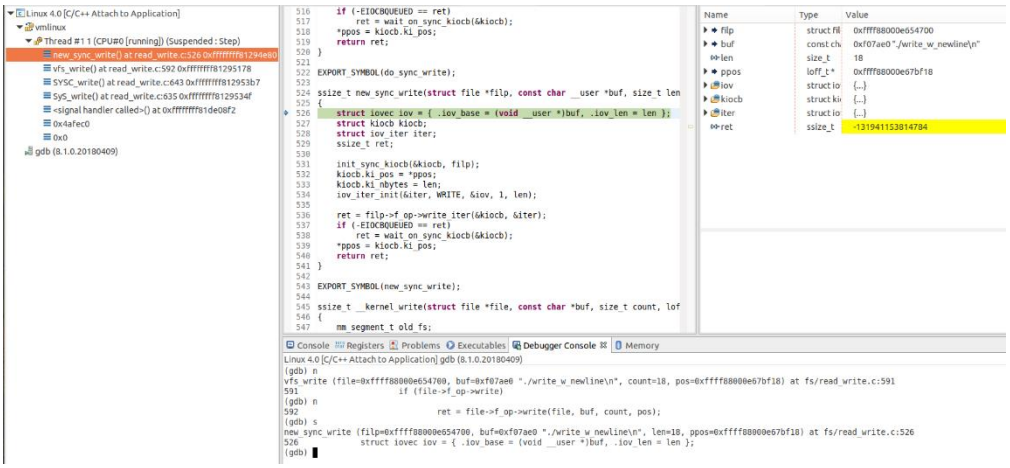


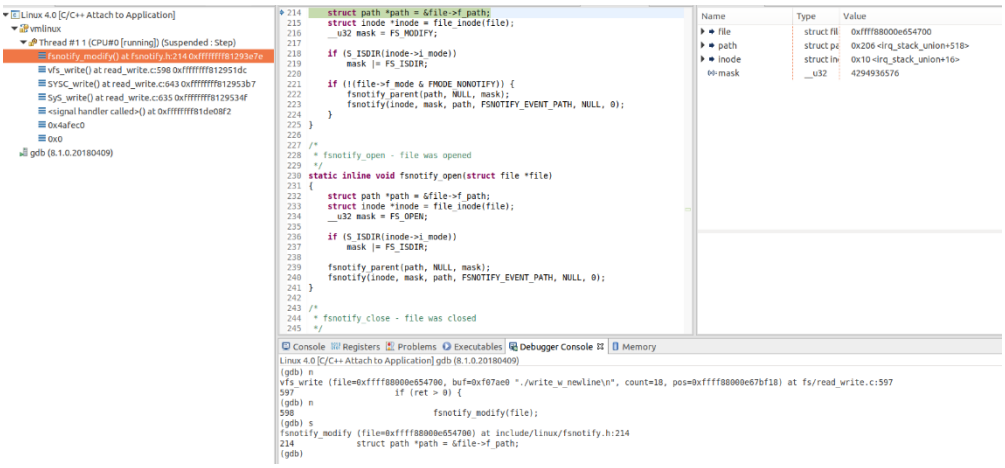

Linux 4.0 [C/C++ Attach to Application]
vmlinux
Thread #1 1 (CPU#0 [running]) (Suspended : Step)
file_start_write() at fs.h:2381 0xffffffff81223c1c
vfs_write() at read_write.c:590 0xffffffff81295149
SYSC_write() at read_write.c:643 0xffffffff8129537b7
SyS_write() at read_write.c:635 0xffffffff8129534f
<signal handler called>() at 0xffffffff81de08f2
0x4afec0
0x0
gdb (8.1.0.20180409)
Name
Type
Value
file
struct fil
0xffff88000e654700
Console
Registers
Problems
Executables
Debugger Console
Memory
Linux 4.0 [C/C++ Attach to Application] gdb (8.1.0.20180409)
508 if (ret >= 0) {
(gdb) n
589 count = ret;
(gdb) n
590 file_start_write(file);
(gdb) s
file_start_write (file=0xffff88000e654700) at include/linux/fs.h:2381
2381 if (!S_ISREG(file_inode(file)->i_mode))
(gdb)

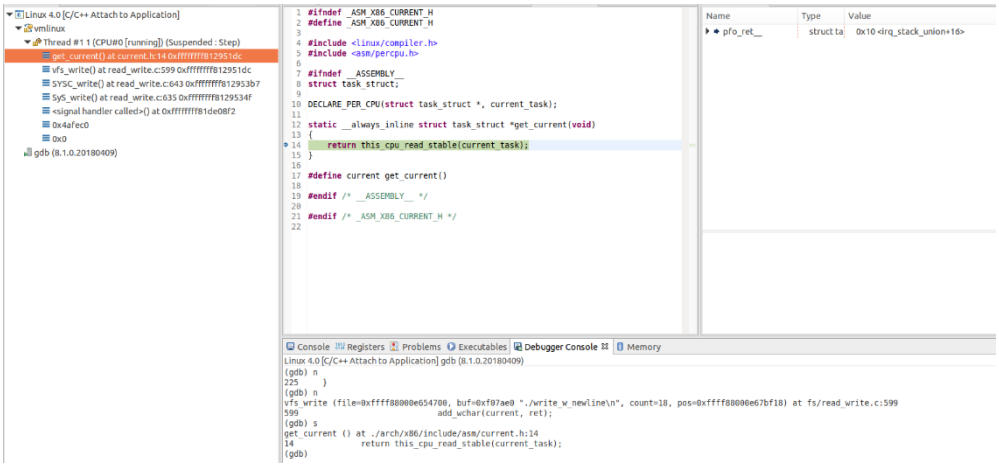

kernel 4.0 [C/C++ Attach to Ap
vmlinux
Thread #1 1 (CPU#0 [runn
v9fs_file_write() at vfs
vfs_write() at read_wri
SYSC_write() at read_v
SyS_write() at read_wr
<signal handler called>
0x4495d1
0x221c025
0x24ea025
0x0
gdb (8.1.0.20180409)
Name
Type
Value
filp
struct file
0xffff880006a3f100
data
const char
0x122ed50 "HelloWorld!!"
count
size_t
25
offset
loff_t *
0xffff880006a1bf18
retval
ssize_t
25
origin
loff_t
25
Console
Registers
Problems
Executables
Debugger Console
Memory
kernel 4.0 [C/C++ Attach to Application] gdb (8.1.0.20180409)
(gdb) n
494 }
(gdb) n
v9fs_file_write (filp=0xffff880006a3f100, data=0x122ed50 "HelloWorld!!", count=25, offset=0xffff880006a1bf18) at fs/9p/vfs_file.c:527
527 if (retval > 0)
(gdb)

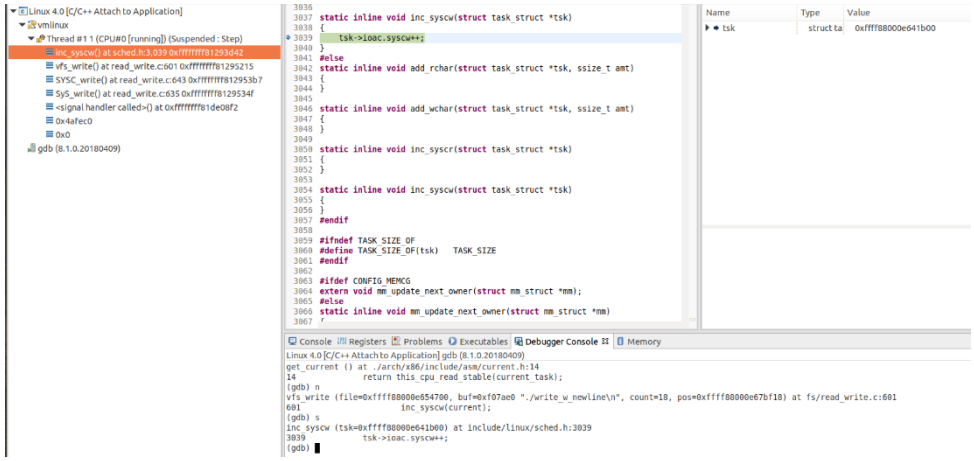

Linux 4.0 [C/C++ Attach to Application]
vmlinux
Thread #1 1 (CPU#0 [running]) (Suspended : Step)
file_pos_read() at read_write.c:612 0xffffffff81295233
SYSC_write() at read_write.c:642 0xffffffff8129539b
SyS_write() at read_write.c:635 0xffffffff8129534f
<signal handler called>() at 0xffffffff81de08f2
0x4afec0
0x0
gdb (8.1.0.20180409)
Name
Type
Value
file
struct fil
0xffff88000e654700
Console
Registers
Problems
Executables
Debugger Console
Memory
Linux 4.0 [C/C++ Attach to Application] gdb (8.1.0.20180409)
639 ssize_t ret = -EBADF;
(gdb) n
641 if (f.file) {
(gdb) n
642 loff_t pos = file_pos_read(f.file);
(gdb) s
file_pos_read (file=0xffff88000e654700) at fs/read_write.c:612
612 return file->f_pos;
(gdb)

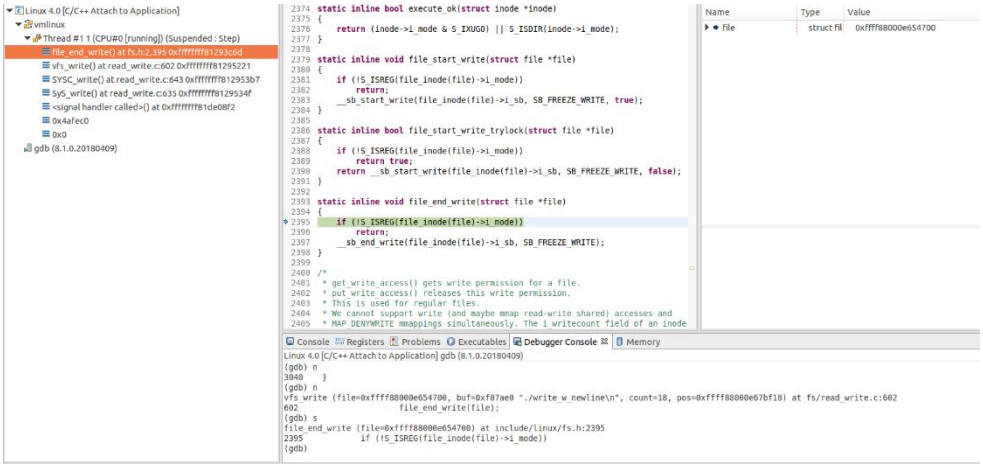

Linux 4.0 [C/C++ Attach to Application]
vmlinux
Thread #1 1 (CPU#0 [running]) (Suspended : Step)
file_inode() at fs.h:1,963 0xffffffff81293ba0
file_start_write() at fs.h:2,383 0xffffffff81293c46
vfs_write() at read_write.c:590 0xffffffff81295149
SYSC_write() at read_write.c:643 0xffffffff812953b7
SyS_write() at read_write.c:635 0xffffffff8129534f
<signal handler called>() at 0xffffffff81de08f2
0x4afec0
0x0
gdb (8.1.0.20180409)
extern bool fs_fully_visible(struct file_system_type *);
extern int current_umask(void);
extern void ihold(struct inode * inode);
extern void iput(struct inode *);
extern int generic_update_time(struct inode *, struct timespec *, int);
static inline struct inode *file_inode(const struct file *f)
{
return f->f_inode;
}
/* /sys/fs */
extern struct kobject *fs_kobj;
#define MAX_RW_COUNT (INT_MAX & PAGE_CACHE_MASK)
#define FLOCK_VERIFY_READ 1
#define FLOCK_VERIFY_WRITE 2
#ifdef CONFIG_FILE_LOCKING
extern int locks_mandatory_locked(struct file *);
extern int locks_mandatory_area(int, struct inode *, struct file *, loff_t,
/*
* Candidates for mandatory locking have the setgid bit set
* but no group execute bit - an otherwise meaningless combination.
*/
static inline int __mandatory_lock(struct inode *ino)
Name
Type
Value
f
const str
0xffff88000e654700
Console
Registers
Problems
Executables
Debugger Console
Memory
Linux 4.0 [C/C++ Attach to Application] gdb (8.1.0.20180409)
(gdb) s
file_start_write (file=0xffff88000e654700) at include/linux/fs.h:2381
2381 if (!S_ISREG(file_inode(file)->i_mode))
(gdb) n
2383 __sb_start_write(file_inode(file)->i_sb, SB_FREEZE_WRITE, true);
(gdb) s
file_inode (f=0xffff88000e654700) at include/linux/fs.h:1963
1963 return f->f_inode;
(gdb)


Linux 4.0 [C/C++ Attach to Application]
vmlinux
Thread #1 1 (CPU#0 [running]) (Suspended : Step)
new_sync_write() at read_write.c:526 0xffffffff81294e80
vfs_write() at read_write.c:592 0xffffffff81295178
SYSC_write() at read_write.c:643 0xffffffff812953b7
SyS_write() at read_write.c:635 0xffffffff8129534f
<signal handler called>() at 0xffffffff81de08f2
0x4afec0
0x0
gdb (8.1.0.20180409)
if (-EIOCBQUEUED == ret)
ret = wait_on_sync_kiocb(&kiocb);
*ppos = kiocb.ki_pos;
return ret;
}
EXPORT_SYMBOL(do_sync_write);
ssize_t new_sync_write(struct file *filp, const char __user *buf, size_t len
{
struct iovec iov = { .iov_base = (void __user *)buf, .iov_len = len };
struct kiocb kiocb;
struct iov_iter iter;
ssize_t ret;
init_sync_kiocb(&kiocb, filp);
kiocb.ki_pos = *ppos;
kiocb.ki_nbytes = len;
iov_iter_init(&iter, WRITE, &iov, 1, len);
ret = filp->f_op->write_iter(&kiocb, &iter);
if (-EIOCBQUEUED == ret)
ret = wait_on_sync_kiocb(&kiocb);
*ppos = kiocb.ki_pos;
return ret;
}
EXPORT_SYMBOL(new_sync_write);
ssize_t __kernel_write(struct file *file, const char *buf, size_t count, lof
{
mm_segment_t old_fs;
Name
Type
Value
filp
struct fil
0xffff88000e654700
buf
const ch
0xf07ae0 "./write_w_newline\n"
len
size_t
18
ppos
loff_t *
0xffff88000e67bf18
iov
struct io
{...}
kiocb
struct ki
{...}
iter
struct io
{...}
ret
ssize_t
-131941153814784
Console
Registers
Problems
Executables
Debugger Console
Memory
Linux 4.0 [C/C++ Attach to Application] gdb (8.1.0.20180409)
(gdb) n
vfs_write (file=0xffff88000e654700, buf=0xf07ae0 "./write_w_newline\n", count=18, pos=0xffff88000e67bf18) at fs/read_write.c:591
591 if (file->f_op->write)
(gdb) n
592 ret = file->f_op->write(file, buf, count, pos);
(gdb) s
new_sync_write (filp=0xffff88000e654700, buf=0xf07ae0 "./write_w_newline\n", len=18, ppos=0xffff88000e67bf18) at fs/read_write.c:526
526 struct iovec iov = { .iov_base = (void __user *)buf, .iov_len = len };
(gdb)


Linux 4.0 [C/C++ Attach to Application]
vmlinux
Thread #1 1 (CPU#0 [running]) (Suspended : Step)
fsnotify_modify() at fsnotify.h:214 0xffffffff81293e7e
vfs_write() at read_write.c:598 0xffffffff812951dc
SYSC_write() at read_write.c:643 0xffffffff812953b7
SyS_write() at read_write.c:635 0xffffffff8129534f
<signal handler called>() at 0xffffffff81de08f2
0x4afec0
0x0
gdb (8.1.0.20180409)
struct path *path = &file->f_path;
struct inode *inode = file_inode(file);
__u32 mask = FS_MODIFY;
if (S_ISDIR(inode->i_mode))
mask |= FS_ISDIR;
if (!(file->f_mode & FMODE_NONOTIFY)) {
fsnotify_parent(path, NULL, mask);
fsnotify(inode, mask, path, FSNOTIFY_EVENT_PATH, NULL, 0);
}
}
/*
* fsnotify_open - file was opened
*/
static inline void fsnotify_open(struct file *file)
{
struct path *path = &file->f_path;
struct inode *inode = file_inode(file);
__u32 mask = FS_OPEN;
if (S_ISDIR(inode->i_mode))
mask |= FS_ISDIR;
fsnotify_parent(path, NULL, mask);
fsnotify(inode, mask, path, FSNOTIFY_EVENT_PATH, NULL, 0);
}
/*
* fsnotify_close - file was closed
*/
Name
Type
Value
file
struct fil
0xffff88000e654700
path
struct pa
0x206 <irq_stack_union+518>
inode
struct in
0x10 <irq_stack_union+16>
mask
__u32
4294936576
Console
Registers
Problems
Executables
Debugger Console
Memory
Linux 4.0 [C/C++ Attach to Application] gdb (8.1.0.20180409)
(gdb) n
vfs_write (file=0xffff88000e654700, buf=0xf07ae0 "./write_w_newline\n", count=18, pos=0xffff88000e67bf18) at fs/read_write.c:597
597 if (ret > 0) {
(gdb) n
598 fsnotify_modify(file);
(gdb) s
fsnotify_modify (file=0xffff88000e654700) at include/linux/fsnotify.h:214
214 struct path *path = &file->f_path;
(gdb)







丁.

目前追蹤到現在，還是沒有找到。