Event type [hex] Categoly		Mnemonic	Descriptio	n of events	where to hook	filename	data recorded as "log_arg1"	data recorded as "log arg2"	data recorded as "log_arg3"	data recorded as "log_arg4"	remarks
							ı ————		prev. process state (value after switch)		
01		PROCESS_CONTEXTSWITCH	Process context switching		schedule()	./kernel/sched.c					from log_arg3, can determain why
	Process management				1		address of the task_struct of "prev"	address of the task_struct of "next"	prev. process count (value before switch)		processes were switched
02		PROCESS WAKEUP	WAKELIP		try to wake up()		value of "p" in the function	synchronous	SWILCIT)		
03					send_sig_info()	./kernel/signal.c	value of "sig" in the function	value of "t" in the function	pointer to info (info)		
04		PROCESS_LTHREADGEN	creating a kernel thread		kernel_thread()	./arch/i386/kemel/process.c	value of "fn" in the function	pointer to argument of kernel thread	flag		
10		INT_HARDWARE_ENTRY	hardware	entrance	do_IRQ()	./arch/i386/kernel/irq.c	value of "irq" in the function	interrupt status (status)			
12	Interrupts	INT_TASKLETHI_ENTRY		entrance	tasklet_hi_action()	./kernel/softirq.c	value of "t->func" in the function				
14		INT TASKLET ENTRY	software	entrance	tasklet action()	1	value of "t->func" in the function				
16		INT_BH_ENTRY		entrance	bh action()		value of "nr" in the function	address of action (bh_base)			
			de								
			int3 overflow								
			bounds								
			invalid_op								
			double fault				handler address (edi) the number of this exception	error code (esi)			
			coprocessor segment overrun		error_code				exception occurred address (eip)		
			invalid_TSS	error_code entrance							
		EXCEPTION_ENTRY	segment not present								
20			stack_segment								
			alignment check			/arch/i386/kernel/entry S					
	Exceptions		coprocessor error			Jacon звокетеленну.5					
			simd_coprocessor_error debug		device not available						
			general protection	oug lie d							
			page fault								
1	1		machine check								
			sprious interrupt bug								
1			device not available								
	4		nmi		nmi						
21		EVOCUTION EVIT	device_not_available		device_not_available		handler address			4	
21		EXCEPTION_EXIT	nmi	exit	nmi	4	the number of this exception			_	
-	1		exceptions other than above two		error_code		handler address (edi)				recording arguments of system calls is
30	System calls	SYSCALL_ENTRY	entrance		beginning of system call()	/arch/i386/kernel/entry.S	the number of this system call				optional feature
31	1	SYSCALL_EXIT	exit		ending of system_call()	/arch/i386/kernel/entry.S	the number of this system call	ermo			
40		FS_DEVRW	device IO	creation of request for device	II_rw_block()	./drivers/block/ll_rw_blk.c	buffer (bh)	READ/WRITE (rw)	num of blocks to transfer (nr)		
41	Filesystems	FS_DEVEND	I	completion of request for device	end_buffer_io_sync()	./fs/buffer.c	buffer (bh)	uptodate			
42		FS_BUFBUSY		buffer busy wait	wait_on_buffer()	./fs/buffer.c	buffer (bh)				
50		MEM_SWAPOUT	swap out	exit	try_to_swap_out()	./mm/vmscan.c	pointer to page swapped out (page)				
51 52		MEM_SWAPIN	swap in	exit	do_swap_page()	./mm/memory.c	pointer to page swapped in (page)				
		MEM_DO_NOPAGE MEM_DO_WPPAGE	mem_do_nopage	exit	do_no_page()	./mm/memory.c	pointer to page allocated (new_page)				
53 54		MEM_DO_WPPAGE MEM_WAIT_PAGE	mem_do_wppage mem_wait_page		do_wp_page() wait on page()	./mm/memory.c /mm/filemap.c	pointer to page (new page)				
55		MEM_WAIT_FAGE	mem_get_freepage	entrance exit	get_free_page()	./mm/page_alloc.c	pointer to page (page) pointer to page (paddr)	type of page (gfp_mask)	the number of page (order)	call address	
56	Memory Management	MEM GET ZEROPAGE	mem_get_zeropage	exit	get_zeroed_page()	./mm/page_alloc.c	pointer to page (address)	type of page (gfp_mask)	call address	Can address	
57		MEM FREEPAGE	mem_freepage	entrance	free_pages()	./mm/page_alloc.c	pointer to (addr)	the number of page (order)	call address		
58	Management	MEM VMALLOC	mem vmalloc	exit	vmalloc()	./mm/vmalloc.h	address (addr)	size	call address		
59		MEM_VFREE	mem_vfree	entrance	vfree()	./mm/vmalloc.c	address (addr)				
5a		MEM_CACHE_CREATE	mem_cache_create	exit	kmem cache create()	./mm/slab.c	name	size	cachep		
5b		MEM_CACHE_ALLOC	mem_cache_alloc	exit	kmem_cache_alloc()	./mm/slab.c	cachep	flags	objp	call address	
5c		MEM_MALLOC	mem malloc	exit	kmalloc()	./mm/slab.c	cachep	flags	objp	call address	
5d		MEM_CACHE_FREE MEM FREE	mem cache free	entrance	kmem cache free()	./mm/slab.c ./mm/slab.c	cachep	objp	call address		
5e 60		NET PKTSEND	mem_free	entrance entrance	kfree() dev gueue xmit()	./mm/siab.c ./net/core/dev.c	objp skh	call address			
61	-		sending packets interrupt on sending packets			/net/core/dev.c	h h				
62		NET PKTRECV	receiving packets	entrance	netif rx()	/net/core/dev.c	skh				
63		NET PKTRECVI	interrupt on receiving packets	entrance	net rx action()	/net/core/dev.c	h				
64		NET_SOCKETIF	socket()	entrance	sys socketcall	./net/socket.c	call	args			exit is recorded as exit of system call.
70	SysV IPC	SYSV_IPC	IPC functions	entrance	sys ipc()	./arch/i386/kernel/sys i386.c	call/first	second/third	*ptr	1	
80	1	LK_SPINLOCK LK_SPINTRYLOCK	anin look	lock	spin_lock()	/include/asm-i386/spinlock.h	address where it was called	lock		+	inline
81 82	-	LK_SPINTRYLOCK LK_SPINUNLOCK	spin lock	try lock (exit) unlock	spin_trylock() spin_unlock()		address where it was called address where it was called	lock lock	return value	+	inline
82	-	LK_SPINUNLOCK LK_WRLOCK		uniock write lock	write lock()		address where it was called address where it was called	rwlock		+	inline
84		LK WRTRYLOCK	+	write lock write try lock (exit)	write_lock()		address where it was called	rwlock	return value	+	inline
85		LK WRUNLOCK	read/write lock	write unlock	write unlock()		address where it was called	rwlock	Total Talue	1	define
86		LK_RDLOCK	Ť	read lock	read_lock()		address where it was called	rwlock			inline
87		LK_RDUNLOCK	<u> </u>	read unlock	read unlock()		address where it was called	rwlock			define
a0	4		run timer list		run_timer_list()		function address(fn)	argument for the function(data)			
a1		TIMER_ADD	add to timer list				pointer to timer list (timer)		for the state of t	argument for the function (timer-	
-	1				add_timer()	./kernel/timer.c	pointer to timer list (timer)	unexpired term (timer->expires)	function address (timer->function)	>data)	
a2	Timer	TIMER_MOD	modify timer list		mod timer()		pointer to timer list (timer)	unexpired term (timer->expires)	function address (timer->function)	argument for the function (timer- >data)	
	1	THES. DEL	delete from timer list		mod umdit)		personal to union not furnory	and to the funds and proof		argument for the function (timer-	
a3		TIMER_DEL	delete from timer list	aerete nom timer list			pointer to timer list (timer)	unexpired term (timer->expires)	function address (timer->function)	>data)	1
					del timer()					argument for the function (timer-	
24		TIMED DEL SVNC	dalata from timer list with complete	inoue			pointer to timer list (timer)	unexpired term (timer->expires)	function address (timer->function)	I to a	1
a4		TIMER_DEL_SYNC	delete from timer list with synchro	nous	del timer sync()		pointer to timer list (timer)	unoxpired term (unter 20xpires)	idirction address (timer->idirction)	>data)	
a4 90					OUT() or betweenOUT1() and					>data)	
90	0	O_PORTIN	delete from timer list with synchrolio commands	port output	OUT() or betweenOUT1() and OUT2()	./include/asm-i386/io.h	port address/byte width	value to output	address where it was called	>oata)	inline
90	Others	O_PORTIN O_PORTOUT	io commands		OUT() or betweenOUT1() and		port address/byte width port address/byte width	value to output value to input		>oata)	inline inline
90 91 92	Others	O_PORTIN O_PORTOUT O_PANIC	io commands panic	port output	OUT() or betweenOUT1() and OUT2()	./kemel/panic.c	port address/byte width port address/byte width address of argument	value to output value to input address where it was called	address where it was called	>oata)	inline inline
90	Others	O_PORTIN O_PORTOUT	io commands panic printk	port output port input	OUT() or betweenOUT1() and OUT2()		port address/byte width port address/byte width	value to output value to input	address where it was called	>oata)	inline inline
90 91 92 93		O_PORTOUT O_PORTOUT O_PANIC O_PRINTK LKST_INIT	io commands panic printk Progress of LKST initialization pr	port output port input	_OUT() or betweenOUT1() and OUT2() tail ofIN() lkst init stage(0-1)()	./kernel/panic.c ./kernel/printk.c ./driver/lkst/lkst.c	port address/byte width port address/byte width address of arqument address of argument initialization status	value to output value to input address where it was called address where it was called	address where it was called address where it was called		inline
90 91 92 93 f00		O_PORTIN O_PORTOUT O_PANIC O_PRINTK LKST INIT LKST MSET XCHG	io commands panic printk Progress of LKST initialization pr LKST switches the maskeds	port output port input	_OUT() or between _OUT1() and _OUT2() tail of _IN() lkst init stage[0-1]() lkst evhandlerprim maskset xchg inlin	./kernel/panic.c ./kernel/printk.c	port address/byte width port address/byte width address of argument address of argument	value to output value to input address where it was called	address where it was called	poniter to new maskset pointer to new buffer	inline inline Recorded 2 times; before/after Recorded 2 times; before/after
90 91 92 93 f00 f08 f10		O_PORTIN O_PORTOUT O_PANIC O_PRINTK LKST_INIT LKST_MSET_XCHG LKST_BUFF_SHIFT	io commands panic printk Progress of LKST initialization pr LKST switches the masksets LKST shifts the buffers	port output port input	_OUT() or between _OUT1() and OUT2() tail of _IN() lkst init stage[0-11() lkst evhandlerprim maskset xchq inlin lkst evhandlerprim buffer shift inline()	/kernel/panic.c /kernel/printk.c /driver/lkst/lkst.c /driver/lkst/lkst.c /driver/lkst/lkst.c	port address/byte width port address/byte width address of argument address of argument initialization status old maskset ID old buffer ID	value to output value to input address where it was called address where it was called new maskset ID	address where it was called address where it was called pointer to old maskset	poniter to new maskset	inline Recorded 2 times; before/after Recorded 2 times; before/after Used for automatically shifting buffer.
90 91 92 93 100 108 110	LKST	O_PORTIN O_PORTOUT O_PAINIC O_PRINTK LKST_INIT LKST_MSET_XCHG LKST_BUFF_SHIFT LKST_BUFF_OVFLOW	io commands panic printk Progress of LKST initialization pr LKST switches the maskeds	port output port input	_OUT() or between _OUT1() and OUT2() tail of _IN() lkst init stage[0-11() lkst evhandlerprim maskset xchq inlin lkst evhandlerprim buffer shift inline()	/kernel/panic.c /kernel/printk.c /driver/lkst/lkst.c /driver/lkst/lkst.c	port address/byte width port address/byte width address of argument address of argument initialization status old maskset ID	value to output value to input address where it was called address where it was called new maskset ID	address where it was called address where it was called address where it was called pointer to old maskset pointer to old buffer	poniter to new maskset	Inline Recorded 2 times; before/after Recorded 2 times; before/after Used for automatically shifting buffer. It masked, LKST stops it.
90 91 92 93 100 108 110 111	LKST internal event	O_PORTIN O_PORTIOUT O_PANIC O_PRINTK LUST INIT LUST INSET XCHG LUST BUFF SHIFT LUST_BUFF OVFLOW LUST_SYNC_UID	io commands panic printk Progress of LKST initialization pr LKST switches the masksets LKST shifts the buffers overrun occurred in the current the synchronization with UID	port output port input ccess	_OUT() or between _OUT() and OUT2() tail of _IN() lkst init stage(0-11() lkst ovhandlerprim maskset xchq inlin lkst ovhandlerprim buffer shift inline() lkst evhandlerprim pertyr next() sys 'tuld(), set user()	./kernel/panic.c //kernel/printk.c //driver/lkst/lkst.c //driver/lkst/lkst.c //driver/lkst/lkst.c //infuel/finux/lkst private.h //kernel/timer.c, sys.c	port address/byte width port address/byte width address of argument address of argument address of argument initialization status old maskest ID old buffer IID pointer to the buffer UID	value to output value to input address where it was called address where it was called new maskset ID	address where it was called address where it was called address where it was called pointer to old maskset pointer to old buffer pointer to the process table	poniter to new maskset	Inline Recorded 2 times; before/after Recorded 2 times; before/after Used for automatically shifting buffer. If masked, LKST stops it. for compensation of dropped log data
90 91 92 93 600 608 610 611 611	LKST internal event	O_PORTIN O_PORTOUT O_PANIC O_PRINTK UKST_INIT UKST_BUFF_SHIFT UKST_BUFF_OVFLOW UKST_SYNC_UID UKST_SYNC_UID UKST_SYNC_GID	io commands panic printk Prooress of LKST initialization pr LKST switches the masksets LKST shifts the buffers overrun occurred in the current t Synchronization with GID synchronization with GID	port output port input ccess	_OUT() or between _OUT() and OUT2() tail of _IN() list exhanclerorim maskset xchq inini list exhanclerorim buffer shft inline() list exhanclerorim buffer shft inline() list exhanclerorim entry next() sys _Ud(), set user() sys _Ud().	/kernel/panic.c /kernel/printk.c /driver/ikst/lkst.c /driver/ikst/lkst.c /driver/ikst/lkst.c /driver/ikst/lkst.c /inlude/linux/lkst, private.h /kernel/timer.c, sys.c	port address/byte width port address/byte width address of argument address of argument address of argument initialization status old maskest ID old buffer ID pointer to the buffer	value to output value to input address where it was called address where it was called new maskset ID new buffer ID	address where it was called address where it was called address where it was called pointer to old maskset pointer to old buffer pointer to the process table pointer to the process table	poniter to new maskset pointer to new buffer	Inline Recorded 2 times; before/after Recorded 2 times; before/after Used for automatically shifting buffer. If masked, LKST stops it. for compensation of dropped log data for compensation of dropped log data
90 91 92 93 100 108 110 111	LKST internal event	O_PORTIN O_PORTIOUT O_PANIC O_PRINTK LUST INIT LUST INSET XCHG LUST BUFF SHIFT LUST_BUFF OVFLOW LUST_SYNC_UID	io commands panic printk Progress of LKST initialization pr LKST switches the masksets LKST shifts the buffers overrun occurred in the current the synchronization with UID	port output port input ccess	_OUT() or between _OUT() and OUT2() lat of _IN() lkst init stage(0-11) lkst evhandlerprim maskset xcho inlin lkst evhandlerprim buffer shift inline() lkst evhandlerprim buffer shift inline() lkst evhandlerprim entry next() sys _uid(), set user() sys _uid(), set user() sys _pid(), sys setsid()	./kernel/panic.c //kernel/printk.c //driver/lkst/lkst.c //driver/lkst/lkst.c //driver/lkst/lkst.c //infuel/finux/lkst private.h //kernel/timer.c, sys.c	port address/byte width port address/byte width address of argument address of argument address of argument initialization status old maskest ID old buffer IID pointer to the buffer UID	value to output value to input address where it was called address where it was called new maskset ID	address where it was called address where it was called address where it was called pointer to old maskset pointer to old buffer pointer to the process table	poniter to new maskset	Inline Recorded 2 times; before/after Recorded 2 times; before/after Used for automatically shifting buffer. If masked, LKST stops it. for compensation of dropped log data