Appendix: List of events which Linux Kernel State Tracer records on IA32

Event type [hex]	Categoly	Mnemonic	Description 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
01	Process management	PROCESS_CONTEXTSWITCH	Process context switching		schedule()	./kernel/sched.c	address of the task_struct of "prev"	address of the task_struct of "next"	prev. process state (value after switch)	prev. process count (value before switch)	from log_arg3, log_arg4, can determain why processes were switched
02		PROCESS_WAKEUP	WAKEUP		try_to_wake_up()	./kernel/signal.c	value of "p" in the function	synchronous			
03		PROCESS_SIGSEND	sending signal		send_sig_info()		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/kernel/process.c	value of "fn" in the function	pointer to argument of kernel thread (arg)	flag		
10	Interrupts	INT_HARDWARE_ENTRY	hardware	entrance	do_IRQ()	./arch/i386/kernel/irq.c	value of "irq" in the function	interrupt status (status)	pointer to register stack		
12		INT_TASKLETHI_ENTRY	software	entrance	tasklet_hi_action()	./kernel/softirq.c	value of "t->func" in the function				
14		INT_TASKLET_ENTRY		entrance	tasklet_action()		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)			
20	Exceptions	EXCEPTION_ENTRY	de	entrance	error_code	./arch/i386/kernel/entry.S	handler address (edi)	error code (esi)	exception occurred address (eip)		
			int3								
			overflow								
			bounds								
			invalid_op								
			double_fault								
			coprocessor_segment_overrun								
			invalid_TSS								
			segment_not_present								
			stack_segment								
			alignment_check								
			coprocessor_error								
			simd_coprocessor_error								
			debug								
			general_protection								
			page_fault								
			machine_check								
			sprious_interrupt_bug								
			device_not_available		device_not_available		the number of this exception				
			nmi		nmi						
21		EXCEPTION_EXIT	device_not_available	exit	device_not_available		handler address				
			nmi		nmi		the number of this exception				
			exceptions other than above two		error_code		handler address (edi)				
30	System calls	SYSCALL_ENTRY	entrance		beginning of system_call()	./arch/i386/kernel/entry.S	the number of this system call				recording arguments of system calls is optional feature
31		SYSCALL_EXIT	exit		ending of system_call()	./arch/i386/kernel/entry.S	the number of this system call	errno			
32		SYSCALL_SYSENTER	sysenter instruction entrance		beginning of sysenter_entry()	./arch/i386/kernel/entry.S	the number of this system call				recording arguments of system calls is optional feature
33		SYSCALL_SYSEXIT	sysexit instruction exit		ending of sysenter_entry()	./arch/i386/kernel/entry.S	the number of this system call	errno			
50	Memory Management	MEM_SWAPOUT	swap out	exit	try_to_swap_out()	./mm/vmscan.c	pointer to page swapped out (page)				
51		MEM_SWAPIN	swap in	exit	do_swap_page()	./mm/memory.c	pointer to page swapped in (page)				
52		MEM_DO_NOPAGE	mem_do_nopage	exit	do_no_page()	./mm/memory.c	pointer to page allocated (new_page)				
53		MEM_DO_WPPAGE	mem_do_wppage		do_wp_page()	./mm/memory.c	pointer to page (new page)				
54		MEM_WAIT_PAGE	mem_wait_page	entrance	__wait_on_page()	./mm/filemap.c	pointer to page (page)				
55		MEM_GET_FREEPAGE	mem_get_freepage	exit	__get_free_page()	./mm/page_alloc.c	pointer to page (paddr)	type of page (gfp_mask)	the number of page (order)	call address	
56		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		
57		MEM_FREEPAGE	mem_freepage	entrance	free_pages()	./mm/page_alloc.c	pointer to (addr)	the number of page (order)	call address		
58		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_cache_free	entrance	kmem_cache_free()	./mm/slab.c	cachep	objp	call address		
5e		MEM_FREE	mem_free	entrance	kfree()	./mm/slab.c	objp	call address			
60	Networking	NET_PKTSEND	sending packets	entrance	dev_queue_xmit()	./net/core/dev.c	skb				
61		NET_PKTSENDI	interrupt on sending packets	entrance	net_tx_action()	./net/core/dev.c	h				
62		NET_PKTRECV	receiving packets	entrance	netif_rx()	./net/core/dev.c	skb				
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_SEMOP	IPC functions	entrance	sys_semop()	./ipc/sem.c	semid	tsops	nsops		
71		SYSV_IPC_SEMGET			sys_semget()		key	nsems	semflg		
72		SYSV_IPC_SEMCTL			sys_semctl()		semid	semnum	cmd	argument for the function	
73		SYSV_IPC_MSGSEND			sys_msgsend()	./ipc/msg.c	msqid	msgp	msgsz	msgflg	
74		SYSV_IPC_MSGRCV			sys_msgrcv()		msqid/msgflg	msgp	msgsz	msgtyp	
75		SYSV_IPC_MSGGET			sys_msgget()		key	msgflg			
76		SYSV_IPC_MSGCTL			sys_msgctl()		msqid	cmd	buf		
77		SYSV_IPC_SHMAT			sys_shmat()	./ipc/shm.c	shmid	shmaddr	shmflg	raddr	
78		SYSV_IPC_SHMDT			sys_shmdt()		shmaddr				
79		SYSV_IPC_SHMGET			sys_shmget()		key	size	shmflg		
7a		SYSV_IPC_SHMCTL			sys_shmctl()		shmid	cmd	buf		
80	Locks	LK_SPINLOCK	spin lock	lock	spin_lock()	./include/asm-i386/spinlock.h	address where it was called	lock			inline
81		LK_SPINTRYLOCK		try lock (exit)	spin_trylock()		address where it was called	lock	return value		inline
82		LK_SPINUNLOCK		unlock	spin_unlock()		address where it was called	lock			inline
83		LK_WRLOCK	read/write lock	write lock	write_lock()		address where it was called	rwlock			inline
84		LK_WRTRYLOCK		write try lock (exit)	write_trylock()		address where it was called	rwlock	return value		inline
85		LK_WRUNLOCK		write unlock	write_unlock()		address where it was called	rwlock			define
86		LK_RDLOCK		read lock	read_lock()		address where it was called	rwlock			inline
87		LK_RDUNLOCK		read unlock	read_unlock()		address where it was called	rwlock			define
a0	Timer	TIMER_RUN	run timer list		run_timer_list()	./kernel/timer.c	function address(fn)	argument for the function(data)			
a1		TIMER_ADD	add to timer list		add_timer()		pointer to timer list (timer)	unexpired term (timer->expires)	function address (timer->function)	argument for the function (timer-	
a2		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-	
a3		TIMER_DEL	delete from timer list		del_timer()		pointer to timer list (timer)	unexpired term (timer->expires)	function address (timer->function)	argument for the function (timer-	
a4		TIMER_DEL_SYNC	delete from timer list with synchronous		del_timer_sync()		pointer to timer list (timer)	unexpired term (timer->expires)	function address (timer->function)	argument for the function (timer-	
b0	Oops	OOPS_PGFAULT	oops in page fault handler	just before the oops operation	do_page_fault()	./arch/i386/mm/fault.c	address where it was accessed	address where exception occurred	exception error code		
b1		OOPS_NMIWDOG	oops in nmi watchdog timer	just before the oops operation	nmi_watchdog_tick()	./arch/i386/kernel/nmi.c	address where it was running				
90	Others	O_PORTIN	io commands	port output	__OUT() or between __OUT1() and __OUT2()	./include/asm-i386/io.h	port address/byte width	value to output	address where it was called		inline
91		O_PORTOUT		port input	tail of __IN()		port address/byte width	value to input	address where it was called		inline
92		O_PANIC	panic			./kernel/panic.c	address of argument	address where it was called			
93		O_PRINTK	printk			./kernel/printk.c	address of argument	address where it was called			
f00	LKST internal event	LKST_INIT	Progress of LKST initialization process		lkst_init_stage[0-1]()	./driver/lkst/lkst.c	initialization status				
f01		LKST_KERNEL_DUMP	kernel dump event		lkst_dump_notify_handler()	./driver/lkst/lkst.c	dump state	dump device			This event is embeded in LKST. User can't handle it.
f08		LKST_MSET_XCHG	LKST switches the masksets		lkst_evhandlerprim_maskset_xchg_inli	./driver/lkst/lkst.c	old maskset ID	new maskset ID	pointer to old maskset	poniter to new maskset	Recorded 2 times; before/after
f10		LKST_BUFF_SHIFT	LKST shifts the buffers		lkst_evhandlerprim_buffer_shift_inline()	./driver/lkst/lkst.c	old buffer ID	new buffer ID	pointer to old buffer	pointer to new buffer	Recorded 2 times; before/after
f11		LKST_BUFF_OVFLOW	overrun occurred in the current buffer.		lkst_evhandlerprim_entry_next()	./inlude/linux/lkst_private.h	pointer to the buffer				Used for automatically shifting buffer. If masked, LKST stops it.
f19		LKST_SYNC_UID	Synchronization with UID		sys_*uid(), set_user()	./kernel/timer.c, sys.c	UID		pointer to the process table		for compensation of dropped log data
f1a		LKST_SYNC_GID	Synchronization with GID		sys_*gid()	./kernel/timer.c, sys.c	GID		pointer to the process table		for compensation of dropped log data
f1b		LKST_SYNC_PGID	Synchronization with PGID		sys_*pgid(), sys_setsid()	./kernel/sys.c	PID	PGRP	pointer to the process table	session leader flag	for compensation of dropped log data
f1c		LKST_SYNC_TID	Synchronization with TID		sys_gettid()	./kernel/timer.c, sys.c	TID(pid)		pointer to the process table		for compensation of dropped log data

Appendix: List of events which Linux Kernel State Tracer records on IA64

Event type [hex]	Categoly	Mnemonic	Description 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
01	Process management	PROCESS_CONTEXTSWITCH	Process context switching		schedule()	./kernel/sched.c	address of the task_struct of "prev"	address of the task_struct of "next"	prev. process state (value after switch)	prev. process count (value before switch)	from log_arg3, log_arg4, can determain why processes were switched
02		PROCESS_WAKEUP	WAKEUP		try_to_wake_up()		value of "p" in the function	synchronous			
03		PROCESS_SIGSEND	sending signal		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/ia64/kernel/process.c	value of "fn" in the function	pointer to argument of kernel thread (arg)	flag		
10	Interrupts	INT_HARDWARE_ENTRY	hardware	entrance	do_IRQ()	./arch/ia64/kernel/irq.c	value of "irq" in the function	interrupt status (status)	pointer to register stack		
12		INT_TASKLETHI_ENTRY	software	entrance	tasklet_hi_action()	./kernel/softirq.c	value of "t->func" in the function				
14		INT_TASKLET_ENTRY		entrance	tasklet_action()		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)			
20	Exceptions	EXCEPT_PGFLT_ENTRY	vhpt_miss itlb_miss dtlb_miss	entrance	ia64_do_page_fault()	./arch/ia64/mm/fault.c	fault address(ifa)	isr	ipsr	iip	
21		EXCEPT_PGFLT_EXIT	alt_itlb_miss alt_dtlb_miss nested_dtlb_miss	exit							
22		EXCEPT_ILLOP_ENTRY	general_exception	entrance	ia64_illegal_op_fault()	./arch/ia64/kernel/traps.c	ec		ipsr	iip	
23		EXCEPT_ILLOP_EXIT		exit							
24		EXCEPT_BADBRK_ENTRY	break_instruction	entrance	ia64_bad_break()		break number(iim)		ipsr	iip	
25		EXCEPT_BADBRK_EXIT		exit							
26		EXCEPT_FAULT_ENTRY	general_exception disabled_fp_reg instruction_key_miss data_key_miss nat_consumption debug_vector unsupported_data_reference fp_fault	entrance	ia64_fault()		fault vector number	isr	ipsr	iip	
27		EXCEPT_FAULT_EXIT	fp_trap lower_privilege_transfer_trap taken_branch_trap single_step_trap ia32_exception ia32_intercept ia32_interrupt	exit							
28		EXCEPT_UNALIGN_ENTRY	unaligned_access	entrance	ia64_handle_unaligned()	./arch/ia64/kernel/unaligned.c	ifa		ipsr	iip	
29		EXCEPT_UNALIGN_EXIT		exit							
30	System calls	SYSCALL_ENTRY	entrance		beginning of system_call()	./arch/ia64/kernel/ivt.S	system call function address	the number of this system call			recording arguments of system calls is optional feature
31		SYSCALL_EXIT	exit		ending of system_call()		system call function address	errno			
50	Memory Management	MEM_SWAPOUT	swap out	exit	try_to_swap_out()	./mm/vmscan.c	pointer to page swapped out (page)				
51		MEM_SWAPIN	swap in	exit	do_swap_page()	./mm/memory.c	pointer to page swapped in (page)				
52		MEM_DO_NOPAGE	mem_do_nopage	exit	do_no_page()	./mm/memory.c	pointer to page allocated (new_page)				
53		MEM_DO_WPPAGE	mem_do_wppage		do_wp_page()	./mm/memory.c	pointer to page (new page)				
54		MEM_WAIT_PAGE	mem_wait_page	entrance	__wait_on_page()	./mm/filemap.c	pointer to page (page)				
55		MEM_GET_FREEPAGE	mem_get_freepage	exit	__get_free_page()	./mm/page_alloc.c	pointer to page (paddr)	type of page (gfp_mask)	the number of page (order)	call address	
56		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		
57		MEM_FREEPAGE	mem_freepage	entrance	free_pages()	./mm/page_alloc.c	pointer to (addr)	the number of page (order)	call address		
58		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_cache_free	entrance	kmem_cache_free()	./mm/slab.c	cachep	objp	call address		
5e		MEM_FREE	mem_free	entrance	kfree()	./mm/slab.c	objp	call address			
60	Networking	NET_PKTSEND	sending packets	entrance	dev_queue_xmit()	./net/core/dev.c	skb				
61		NET_PKTSENDI	interrupt on sending packets	entrance	net_tx_action()	./net/core/dev.c	h				
62		NET_PKTRECV	receiving packets	entrance	netif_rx()	./net/core/dev.c	skb				
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_SEMOP	IPC functions	entrance	sys_semop()	./ipc/sem.c	semid	tsops	nsops		
71		SYSV_IPC_SEMGET			sys_semget()		key	nsems	semflg		
72		SYSV_IPC_SEMCTL			sys_semctl()		semid	semnum	cmd	argument for the function	
73		SYSV_IPC_MSGSEND			sys_msgsend()	./ipc/msg.c	msqid	msgp	msgsz	msgflg	
74		SYSV_IPC_MSGRCV			sys_msgrcv()		msqid/msgflg	msgp	msgsz	msgtyp	
75		SYSV_IPC_MSGGET			sys_msgget()		key	msgflg			
76		SYSV_IPC_MSGCTL			sys_msgctl()		msqid	cmd	buf		
77		SYSV_IPC_SHMAT			sys_shmat()	./ipc/shm.c	shmid	shmaddr	shmflg	raddr	
78		SYSV_IPC_SHMDT			sys_shmdt()		shmaddr				
79		SYSV_IPC_SHMGET			sys_shmget()		key	size	shmflg		
7a		SYSV_IPC_SHMCTL			sys_shmctl()		shmid	cmd	buf		
80	Locks	LK_SPINLOCK	spin lock	lock	spin_lock()	./include/asm-ia64/spinlock.h	address where it was called	lock			inline
81		LK_SPINTRYLOCK		try lock (exit)	spin_trylock()		address where it was called	lock	return value		inline
82		LK_SPINUNLOCK		unlock	spin_unlock()		address where it was called	lock			inline
83		LK_WRLOCK	read/write lock	write lock	write_lock()		address where it was called	rwlock			inline
84		LK_WRTRYLOCK		write try lock (exit)	write_trylock() (IA32 only		address where it was called	rwlock	return value		inline
85		LK_WRUNLOCK		write unlock	write_unlock()		address where it was called	rwlock			define
86		LK_RDLOCK		read lock	read_lock()		address where it was called	rwlock			inline
87		LK_RDUNLOCK		read unlock	read_unlock()		address where it was called	rwlock			define
a0	Timer	TIMER_RUN	run timer list		run_timer_list()	./kernel/timer.c	function address(fn)	argument for the function(data)			
a1		TIMER_ADD	add to timer list		add_timer()		pointer to timer list (timer)	unexpired term (timer->expires)	function address (timer->function)	argument for the function (timer-	
a2		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-	
a3		TIMER_DEL	delete from timer list		del_timer()		pointer to timer list (timer)	unexpired term (timer->expires)	function address (timer->function)	argument for the function (timer-	
a4		TIMER_DEL_SYNC	delete from timer list with synchronous		del_timer_sync()		pointer to timer list (timer)	unexpired term (timer->expires)	function address (timer->function)	argument for the function (timer-	

90	Others	O_PORTIN	io commands	port input	__ia64_inb()
					__ia64_inw()
					__ia64_inl()
					__ia64_insb()
					__ia64_insw()
					__ia64_insl()
						./include/asm-ia64/io.h	port address/byte width	value to input	address where it was called		inline

91		O_PORTOUT		port input	__ia64_outb()
					__ia64_outw()
					__ia64_oul()
					__ia64_outsb()
					__ia64_outsw()
					__ia64_outsl()
							port address/byte width	value to output	address where it was called		inline

92		O_PANIC	panic		panic()	./kernel/panic.c	address of argument	address where it was called			
93		O_PRINTK	printk		printk()	./kernel/printk.c	address of argument	address where it was called			
b0	**Oops**	OOPS_PGFAULT	oops in page fault handler	just before the oops operation	do_page_fault()	./arch/ia64/mm/fault.c	address where it was accessed	address where exception occurred	exception error code		
f00	LKST internal event	LKST_INIT	Progress of LKST initialization process		lkst_init_stage[0-1]()	./driver/lkst/lkst.c	initialization status				
f08		LKST_MSET_XCHG	LKST switches the masksets		lkst_evhandlerprim_maskset_xchg_inlin	./driver/lkst/lkst.c	old maskset ID	new maskset ID	pointer to old maskset	poniter to new maskset	Recorded 2 times; before/after
f10		LKST_BUFF_SHIFT	LKST shifts the buffers		lkst_evhandlerprim_buffer_shift_inline()	./driver/lkst/lkst.c	old buffer ID	new buffer ID	pointer to old buffer	pointer to new buffer	Recorded 2 times; before/after
f11		LKST_BUFF_OVFLOW	overrun occurred in the current buffer.		lkst_evhandlerprim_entry_next()	./inlude/linux/lkst_private.h	pointer to the buffer				Used for automatically shifting buffer. If masked, LKST stops it.
f19		LKST_SYNC_UID	Synchronization with UID		sys_*uid(), set_user()	./kernel/timer.c, sys.c	UID		pointer to the process table		for compensation of dropped log data
f1a		LKST_SYNC_GID	Synchronization with GID		sys_*gid()	./kernel/timer.c, sys.c	GID		pointer to the process table		for compensation of dropped log data
f1b		LKST_SYNC_PGID	Synchronization with PGID		sys_*pgid(), sys_setsid()	./kernel/sys.c	PID	PGRP	pointer to the process table	session leader flag	for compensation of dropped log data
f1c		LKST_SYNC_TID	Synchronization with TID		sys_gettid()	./kernel/timer.c, sys.c	TID(pid)		pointer to the process table		for compensation of dropped log data