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

Event type [hex]	Categoly	Mnemonic	Descripti	on of events	where to hook	filename	data recorded as "log_arg1"	data recorded as "log_arg2"	Idata recorded as "log_arg3"	Idata recorded as "log_arg4"	remarks
Eron ypo [no.]	outogoly	Witemonie	Becompa			liionamo	address of the task struct	address of the task struct	prev process state (value after	prev_process count(value before	from log arg3 log arg4 can determain
01		PROCESS_CONTEXTSWIT	CI Process context switching		schedule()	./kernel/sched.c			prev. process state (value alter	prev. process count (value before	non log_arg5, log_arg4, can determain
	Process					-	of "prev"	of "next"	Switch	Switch)	why processes were switched
02	management	PROCESS_WAKEUP WAKEUP			try_to_wake_up()		value of "p" in the function	synchronous			
03	managomon	PROCESS_SIGSEND	sending signal		send_sig_info()	./kernel/signal.c	value of "sig" in the function	value of "t" in the function	pointer to into (into)		
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		INT HARDWARE ENTRY	hardware	entrance	do_IRQ()	./arch/i386/kernel/irg.c	value of "irq" in the function	interrupt status (status)	pointer to register stack		
12	.	INT TASKI ETHI ENTRY		entrance	tasklet hi action()	/kernel/softira c	value of "t->func" in the function				
14	Interrupts	INT TASKLET ENTRY	software	entrance	tasklet_action()	, nome, contrate	value of "t->func" in the function				
16	-		contrato	ontranco	hb action()		value of "pr" in the function	address of action (bb. base)			
10		II_BH_ENIRY	1	entrance	Dn_action()	·		address of action (bit_base)			
		EXCEPTION_ENTRY	de								
			int3								
			overflow		error_code						
			bounds	-							
			involid on	-							
	Exceptions		lilvaliu_op	_							
			double_fault								
			coprocessor_segment_overrun	entrance		./arch/i386/kernel/entry.S	handler address (edi)	1			
			invalid_TSS								
			segment not present					error code (esi)			
			stack segment						exception occurred address (eip)		
20											
20			alignment_check								
			coprocessor_error								
			simd_coprocessor_error								
			debua								
			general protection								
			pege foult	-							
			page_lault	_							
1		1	machine_check	4	1					1	1
1		1	sprious_interrupt_bug			J				1	1
1		1	device_not_available		device_not_available		the number of this success?			1	1
I			nmi	7	nmi	1	the number of this exception			1	
1	-		device not available	1	device not available	1			1	1	1
04			nmi		nmi				+	4	1
21		EAGEPTION_EAT	inili			4	the number of this exception			4	1
L			exceptions other than above two		error_code	L	handler address (edi)				<u> </u>
20		SVSCALL ENTRY									recording arguments of system calls is
30		STSCALL_ENTRY	entrance		beginning of system call()	./arch/i386/kernel/entrv.S	the number of this system call			1	optional feature
31	۲_	SYSCALL FYIT	exit		ending of system call()	/arch/i386/kernel/entry S	the number of this system call	errno			
31	System calls	STOCALL_EATT			shang of system_can()	, a.orwiodo, kernewentry.o	and number of this system call	00	+		recording arguments of system calls is
32	1	SYSCALL SYSENTER	augustas is struction of		heating of everything of the	(arab/i206/i	the number of this sustain "				antional feature
	4		sysenter instruction entrance		peginning or sysenter_entry()	/arcn/i386/kernel/entry.S	the number of this system call				opuonai reature
33		SYSCALL_SYSEXIT	sysexit instruction exit		ending of sysenter_entry()	./arch/i386/kernel/entry.S	the number of this system call	errno			
50		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)				
50			Swap III	ovit	do_swap_page()		pointer to page ollopeted (now, page)				
52	_		mem_uo_nopage	exit	uu_liu_paye()	./mm/memory.c	pointer to page anocated (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 det zeronade	exit	get zeroed page()	/mm/page_alloc_c	pointer to page (address)	type of page (ofp_mask)	call address		
57	Memory		mom_got_zotopago	entrance	free_page()	/mm/page_allee.e	pointer to (addr)	the number of page (order)	call address		
	Management		mem_meepage	entrance	liee_pages()	./mm/page_alloc.c					
58	Junio	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		
5h		MEM CACHE ALLOC	mem cache alloc	exit	kmem_cache_alloc()	/mm/slab.c	cachep	flags	ohip	call address	
50	1		mem malloc	exit	kmalloc()	/mm/slab.c	cachen	flags	obin	call address	1
30	_					./mm/siab.c	cachep	liays		Call address	
50		MEM_CACHE_FREE	mem_cache_free	entrance	kmem_cache_free()	./mm/slab.c	cacnep	qlqo	call address		
5e		MEM_FREE	mem_free	entrance	kfree()	./mm/slab.c	objp	call address			
60		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	Networking		receiving packets	entrance	netif rx()	/net/core/dev.c	skh				
02	Networking		interrupt on receiving peakets	ontronoo	not ry action()	/net/core/dov.o	5105 b				
63	_										within an equal of an exit of eventeers call
64		NET_SOCKETIF	socket() entrance	entrance	sys_socketcall	./net/socket.c	call	args			exit is recorded as exit of system call.
70		SYSV_IPC_SEMOP	IPC functions	entrance	sys_semop()		semid	tsops	nsops		
71		SYSV_IPC_SEMGET SYSV_IPC_SEMCTL SYSV_IPC_MSGSEND SYSV_IPC_MSGSEND SYSV_IPC_MSGGET SYSV_IPC_MSGCTL SYSV_IPC_SHMAT			sys_semget()	./ipc/sem.c	key	nsems	semflg		
72					svs semctl()		semid	semnum	cmd	argument for the function	
73					sys_msgsend()		msaid	msan	msgs7	msafla	
73					sys_msgrou()	-	megid/megflg	mean	megez	moglig	
/4	Suel/IDO					./ipc/msg.c	kov	maafla	110902	mogup	
/5	SYSV IPC				sys_IIIsgget()	-		mogliy	h		
76			_		sys_msgcti()		msqia	cind	bul		1
77					sys_shmat()	1	snmid	snmaddr	snmtig	raddr	
78		SYSV_IPC_SHMDT			sys_shmdt()	/inc/chm c	shmaddr				
79		SYSV_IPC_SHMGET			sys_shmget()	.//pc/sillii.c	key	size	shmflg		
7a					sys_shmctl()	1	shmid	cmd	buf		1
80			1	lock	in lock()	1	address where it was called	lock		1	inline
00	-			try lock (avit)	opin_trylook()	4	addroso whore it was called	look	roturn voluo		inling
01	-		Spiniock		spin_trylock()	10Ck() lock() ck() /lock() /lock() /include/asm-i386/spinlock.h	address where it was talled	look			
82	_	LK_SPINUNLOCK			spin_uniock()		auuress where it was called		+	 	
83	Locks	LK_WRLOCK		WITE IOCK	Write_IOCK()		address where it was called	rwiock			Inline
84	20010	LK_WRTRYLOCK		write try lock (exit)	write_trylock()		address where it was called	rwiock	return value	L	Inline
85		LK WRUNLOCK	read/write lock	write unlock	write_unlock()		address where it was called	rwlock			define
86	1			read lock re	read lock()	1	address where it was called	rwlock		T	inline
87	-			read unlock	read_unlock()		address where it was called	rwlock			define
-01	+		rup timor list	- sad drilool	rup timor list/	+	function address/fn)	argument for the function (date)	+		
au	-	TIMER_RUN TIMER_ADD				4	runction address(III)	argument for the function(data)	for the set of the set		
a1	Timer		add to timer list		auu_timer()	4	pointer to timer list (timer)	unexpirea term (timer->expires)	iunction address (timer->function)	argument for the function (timer-	1
a2	Fimer	TIMER_MOD	modify timer list		mod_timer()	./kernel/timer.c	pointer to timer list (timer)	unexpired term (timer->expires)	runction 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 synch	ronous	del timer sync()	1	pointer to timer list (timer)	unexpired term (timer->expires)	function address (timer->function)	argument for the function (timer-	
64 60	1	OORS ROEAUUT	oops in page foult headler	just before the consideration	do page fault()	/arch/i386/mm/fault a	address where it was accessed	address where excention occurred	excention error code	Sector and random (union-	1
00	Oops	OURS_FORAULI	oops in page lauit nandler	just before the case aparetics	nmi wotobdog tick/	/arch/i200/mm/tautt.C	address where it was accessed	address where exception occurred			
D1	Others	OUPS_NMIWDUG oops in nmi watchdog timer		just before the oops operation	ULT() or between OLTT() and	./arch/i386/kernel/nmi.c	audress where it was running				
۵n		O_PORTIN O_PORTOUT O_PANIC			OUI() or betweenOUI1() and					1	L
90			io commands port output port input	OUT2()/include/asr tail ofIN()/kernel/pani /kernel/print 	./include/asm-i386/io.h	port address/byte width	value to output	address where it was called	1	inline	
91					/kernel/panic.c /kernel/printk.c	port address/byte width	value to input	address where it was called		inline	
02			point input printk Progress of LKST initialization process kernel dump event LKST switches the masksets LKST stifts the huffers			address of argument	address where it was called	, , duild			
32						address of argument	address where it was called	+	1	1	
93	+	O_PRINTK LKST_INIT LKST_KERNEL_DUMP LKST_MSET_XCHG					audiess where it was called			+	
f00	4				./ariver/ikst/lkst.c	Initialization status					
f01					./driver/lkst/lkst.c				I	I his event is embeded in LKST. User	
101						dump state old maskset ID	dump device		1	can't handle it.	
f08					/driver/lkst/lkst.c		new maskset ID	pointer to old maskset	poniter to new maskset	Recorded 2 times: before/after	
f10		IKST BLIEF SHIFT			lkst evhandlernrim buffer shift inling/	ing_init/driver/ikst/ikst.c	old buffer ID	new buffer ID	pointer to old buffer	pointer to new buffer	Recorded 2 times: before/after
110	LKST	LKS1_BUFF_SHIF1				er_sniit_iniine()./ariver/ikst/ikst.c					Leed for automatically shifting buffer
f11	internal event	LIKOT DUEE OVELOW								1	used for automatically shifting puller.
		LKSI_BUFF_OVFLOW	overrun occurred in the current	butter.	IKst_evhandlerprim_entry_next()	./inlude/linux/lkst_private.h	pointer to the buffer				IT 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
f1h	7	LKST SYNC PGID	Synchronization with PGID		svs *pgid(), svs setsid()	/kernel/sys.c	PID	PGRP	pointer to the process table	session leader flag	for compensation of dropped log data
f1.c	-		Synchronization with TID		svs gettid()	/kernel/timer c_svs c	TID(pid)		pointer to the process table	i i i i i i i i i i i i i i i i i i i	for compensation of dropped log data
			Synomication with HD		oyo_gottio()	anonovanier.e, sys.e	(inclinia)		Pointer to the process table		ior compensation or uropped tog uata

Copyright (C) Hitachi, Ltd., 2002-2003. All rights reserved.

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

						Copyright (C) Hitachi, Ltd., 200'						
Event type [he	x] Categoly	Mnemonic	Descriptio	on 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"	from log arg3 log arg4 can determain	
01	Process	PROCESS_CONTEXTSWITCH	Process context switching		schedule()	./kernel/sched.c	of "prev"	of "next"	switch)	switch)	why processes were switched	
02	management	PROCESS_WAKEUP WAKEUP			try_to_wake_up()		value of "p" in the function	synchronous				
03	management	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)			
10		INT HARDWARE ENTRY	hardware	entrance	do IRQ()	/arch/ia64/kernel/irg.c	value of "irg" in the function	interrupt status (status)	pointer to register stack			
12		INT_TASKLETHI_ENTRY		entrance	tasklet_hi_action()	./kernel/softirq.c	value of "t->func" in the function					
14	menupto	INT_TASKLET_ENTRY	software	entrance	tasklet_action()	_	value of "t->func" in the function	address of action (bb. base)				
16		INT BH ENTRY	vhot miss	entrance	pn_action()			address of action (bh_base)				
20		EXCEPT_PGFLT_ENTRY	itlb_miss	entrance		./arch/ia64/mm/fault.c						
			dtlb_miss				fault address(ifa)	isr	ipsr	iip		
21		EXCEPT POFLT EXIT	alt_itlb_miss	exit								
21			nested dtlb miss									
22		EXCEPT_ILLOP_ENTRY	general exception	entrance	ia64 illegal op fault()		ec		ipsr	iip		
23		EXCEPT_ILLOP_EXIT	gonoraoncopiion	exit	ido i_inogai_op_raan()	-			ipoi	"P		
24		EXCEPT_BADBRK_ENTRY	-break_instruction	exit	ia64_bad_break()		break number(iim)		ipsr	iip		
26			general_exception		—ia64_fault()	./arch/ia64/kernel/traps.c						
			disabled_fp_reg instruction_key_miss ata_key_miss nat_consumption debug_vector unsupported_data_reference fo_fout	entrance			fault vector number					
								isr				
	Exceptions	EXCEPT_FAULT_ENTRY										
			fp trap						ipsr	iip		
			lower_privilege_transfer_trap taken_branch_trap	exit								
27		EXCEPT_FAULT_EXIT	single_step_trap									
			ia32_intercept ia32_interrupt									
20		EXCEPT LINALION ENTRY										
20		EXCEPT UNALIGN EXIT	unaligned_access	exit	ia64_handle_unaligned()	./arch/ia64/kernel/unaligned.c	ifa		ipsr	iip		
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	
31	cycle.in duild	SYSCALL_EXIT	exit	evit	ending of system_call()		system call function address	errno			optional feature	
50		MEM SWAPOUT	swap out	exit	do swap page()	./mm/vmscan.c	pointer to page swapped out (page)				1	
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		
57	Memory Management	MEM_GET_ZEROFAGE	mem_get_zeropage	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			
50		MEM_CACHE_ALLOC	mem_cache_alloc	exit	kmalloc()	./mm/slab.c	cachep	flags	objp	call address		
50 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		NET_PKTSEND	sending packets	entrance	dev_queue_xmit()	./net/core/dev.c	skb					
61	Networking		receiving packets	entrance	net_tx_action()	/net/core/dev.c	n					
63	Networking	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_SEMOP	IPC functions		sys_semop()	Jipc/sem.c Jipc/msg.c Jipc/shm.c	semid	tsops	nsops			
71	_	SYSV_IPC_SEMGET		entrance	sys_semget()		key	nsems	cmd	argument for the function		
73		SYSV IPC MSGSEND			sys_msgsend()		msqid	msgp	msgsz	msgflg		
74		SYSV_IPC_MSGRCV			sys_msgrcv()		msqid/msgflg	msgp	msgsz	msgtyp		
75	SysV IPC	SYSV_IPC_MSGGET			sys_msgget()		key	msgflg	h f			
76		SYSV_IPC_MSGCTL			sys_hmat()		shmid	shmaddr	shmfla	raddr		
78		SYSV IPC SHMDT			sys_shmdt()		shmaddr	Shinada	Shiring			
79		SYSV_IPC_SHMGET			sys_shmget()		key	size	shmflg			
7a					sys_snmcti()		snmid address where it was called	lock	bui	l	inline	
80			spin lock	try lock (exit)	spin_lock()	-	address where it was called	lock	return value		inline	
82	Locks		SPINUNLOCK	unlock	spin_unlock()		address where it was called	lock			inline	
83		LK_WRLOCK		write lock	write_lock()	./include/asm-ia64/spinlock.b	address where it was called	rwlock			inline	
84	_		read/write lock	write try lock (exit) write uplock	write_trylock() (IA32 only		address where it was called	rwiock	return value		inine define	
86		LK RDLOCK		read lock	read_lock()		address where it was called	rwlock			inline	
87		LK RDUNLOCK	7	read unlock	read_unlock()		address where it was called	rwlock			define	
a0		TIMER_RUN	run timer list		run_timer_list()	4	tunction address(fn)	argument for the function(data)	function address (Arran function)	orgument for the first the first	+	
a1	Timer	TIMER_ADD	aud to timer list		mod timer()	/kernel/timer.c	pointer to timer list (timer)	unexpired term (timer->expires)	function address (timer->function)	argument for the function (timer-	1	
a3	T IIIIGI	TIMER DEL	delete from timer list		del timer()	./Kernel/umer.c	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 synchro	nous	del_timer_sync()		pointer to timer list (timer)	unexpired term (timer->expires)	function address (timer->function)	argument for the function (timer-		
90 91			PORTIN io commands port input PORTOUT panic port input		ia64_inb()	-	port address/byte width	value to input value to output				
		O DODTU:			ia64_inI()	/include/asm-ia64/io.h			address where it was called			
		O_PORTIN		port input	ia64_insb()						inline	
					ia64_insw()							
					ia64_insl()							
	Others				ia64_outw()						inline	
					ia64_oul()		port addross/buts width					
		0_FORTOUT			ia64_outsb()		port address/byte width		address where it was called			
					ia64_outsw()							
02		O PANIC			iao4_outsi()		address of argument	address where it was called				
93		O_PRINTK	printk		printk()	./kernel/printk.c	address of argument	address where it was called			1	
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_INIT	Progress of LKST initialization pro	DCess	Ikst_init_stage[0-1]()	/driver/lkst/lkst.c	initialization status	now moskoot ID	pointer to old mooliset	popitor to pour marker t	Beenried 2 times: hefere /star	
108 f10		LKST_WOET_XCHG	LNST shifts the buffers		IKSL_evnandierprim_maskset_xchg_inlin	/driver/lkst/lkst.c	old buffer ID	new huffer ID	pointer to old maskset	pointer to new maskset	Recorded 2 times; before/after	
	LIVET		KST_BUFF_SHIFT LKST shifts the buffers KST_BUFF_OVFLOW overrun occurred in the current buffer.			a creating indention in the company of the company					Used for automatically shifting buffer.	
t11	LKS1	LKST_BUFF_OVFLOW			lkst_evhandlerprim_entry_next() ./inlude/linux/lkst	./inlude/linux/lkst_private.h	pointer to the buffer				If masked, LKST stops it.	
f19	internal event	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	
<u>f1a</u>		LKST_STNC_GID	Synchronization with GID		sys_gla() sys_snaid() 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	