Output A:

Read event log entries

16995 read(3<pipe:[96930]>, <unfinished ...>

16995 read(3</lib/x86\_64-linux-gnu/libc-2.23.so>, "\177ELF\2\1\1\3\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0P\t\2\0\0\0\0\0"..., 832) = 832

16995 read(0</dev/tty1>, "Can I get a shell?\n", 400) = 19

16931 read(0</dev/tty1>, "\7", 1) = 1

16931 read(0</dev/tty1>, "w", 1) = 1

16931 read(0</dev/tty1>, "h", 1) = 1

16931 read(0</dev/tty1>, "o", 1) = 1

16931 read(0</dev/tty1>, "a", 1) = 1

16931 read(0</dev/tty1>, "m", 1) = 1

16931 read(0</dev/tty1>, "i", 1) = 1

16931 read(0</dev/tty1>, "\r", 1) = 1

16997 read(3<pipe:[96968]>, <unfinished ...>

16997 read(3</lib/x86\_64-linux-gnu/libc-2.23.so>, "\177ELF\2\1\1\3\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0P\t\2\0\0\0\0\0"..., 832) = 832

16997 read(3</etc/nsswitch.conf>, "# /etc/nsswitch.conf\n#\n# Example"..., 4096) = 497

16997 read(3</etc/nsswitch.conf>, "", 4096) = 0

16997 read(3</lib/x86\_64-linux-gnu/libnss\_compat-2.23.so>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\320\22\0\0\0\0\0\0"..., 832) = 832

16997 read(3</lib/x86\_64-linux-gnu/libnsl-2.23.so>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\360?\0\0\0\0\0\0"..., 832) = 832

16997 read(3</lib/x86\_64-linux-gnu/libnss\_nis-2.23.so>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\260 \0\0\0\0\0\0"..., 832) = 832

16997 read(3</lib/x86\_64-linux-gnu/libnss\_files-2.23.so>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\260!\0\0\0\0\0\0"..., 832) = 832

16931 read(0</dev/tty1>, "i", 1) = 1

16931 read(0</dev/tty1>, "d", 1) = 1

16931 read(0</dev/tty1>, "\r", 1) = 1

16999 read(3<pipe:[97005]>, <unfinished ...>

16999 read(3</lib/x86\_64-linux-gnu/libselinux.so.1>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\260Z\0\0\0\0\0\0"..., 832) = 832

16999 read(3</lib/x86\_64-linux-gnu/libc-2.23.so>, "\177ELF\2\1\1\3\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0P\t\2\0\0\0\0\0"..., 832) = 832

16999 read(3</lib/x86\_64-linux-gnu/libpcre.so.3.13.2>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0000\25\0\0\0\0\0\0"..., 832) = 832

16999 read(3</lib/x86\_64-linux-gnu/libdl-2.23.so>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\240\r\0\0\0\0\0\0"..., 832) = 832

16999 read(3</lib/x86\_64-linux-gnu/libpthread-2.23.so>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\260`\0\0\0\0\0\0"..., 832) = 832

16999 read(3</proc/filesystems>, "nodev\tsysfs\nnodev\trootfs\nnodev\tr"..., 1024) = 362

16999 read(3</proc/filesystems>, "", 1024) = 0

16999 read(3</etc/locale.alias>, "# Locale name alias data base.\n#"..., 4096) = 2995

16999 read(3</etc/locale.alias>, "", 4096) = 0

16999 read(3</etc/nsswitch.conf>, "# /etc/nsswitch.conf\n#\n# Example"..., 4096) = 497

16999 read(3</etc/nsswitch.conf>, "", 4096) = 0

16999 read(3</lib/x86\_64-linux-gnu/libnss\_compat-2.23.so>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\320\22\0\0\0\0\0\0"..., 832) = 832

16999 read(3</lib/x86\_64-linux-gnu/libnsl-2.23.so>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\360?\0\0\0\0\0\0"..., 832) = 832

16999 read(3</lib/x86\_64-linux-gnu/libnss\_nis-2.23.so>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\260 \0\0\0\0\0\0"..., 832) = 832

16999 read(3</lib/x86\_64-linux-gnu/libnss\_files-2.23.so>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\260!\0\0\0\0\0\0"..., 832) = 832

16999 read(3</proc/sys/kernel/ngroups\_max>, "65536\n", 31) = 6

16999 read(3</proc/sys/kernel/ngroups\_max>, "65536\n", 31) = 6

16931 read(0</dev/tty1>, "u", 1) = 1

16931 read(0</dev/tty1>, "n", 1) = 1

16931 read(0</dev/tty1>, "a", 1) = 1

16931 read(0</dev/tty1>, "m", 1) = 1

16931 read(0</dev/tty1>, "e", 1) = 1

16931 read(0</dev/tty1>, "\r", 1) = 1

17001 read(3<pipe:[97022]>, <unfinished ...>

17001 read(3</lib/x86\_64-linux-gnu/libc-2.23.so>, "\177ELF\2\1\1\3\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0P\t\2\0\0\0\0\0"..., 832) = 832

16931 read(0</dev/tty1>, <detached ...>

Total number of read events: 49

Output B:

Read event log entries

16931 read(0</dev/tty1>, "\r", 1) = 1

16955 read(5<pipe:[96376]>, <unfinished ...>

16956 read(3</lib/x86\_64-linux-gnu/libc-2.23.so>, <unfinished ...>

16956 read(0<pipe:[96374]>, <unfinished ...>

16957 read(3</lib/x86\_64-linux-gnu/libc-2.23.so>, "\177ELF\2\1\1\3\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0P\t\2\0\0\0\0\0"..., 832) = 832

16957 read(3</home/user/test/in.txt>, "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"..., 131072) = 112

16957 read(3</home/user/test/in.txt>, "", 131072) = 0

16956 read(3</lib/x86\_64-linux-gnu/libc-2.23.so>, "\177ELF\2\1\1\3\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0P\t\2\0\0\0\0\0"..., 832) = 832

16956 read(0<pipe:[96374]>, <unfinished ...>

16958 read(3</lib/x86\_64-linux-gnu/libc-2.23.so>, "\177ELF\2\1\1\3\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0P\t\2\0\0\0\0\0"..., 832) = 832

16958 read(0</dev/tty1>, <unfinished ...>

16958 read(0</dev/tty1>, <unfinished ...>

16959 read(3</lib/x86\_64-linux-gnu/libselinux.so.1>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\260Z\0\0\0\0\0\0"..., 832) = 832

16959 read(3</lib/x86\_64-linux-gnu/libc-2.23.so>, "\177ELF\2\1\1\3\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0P\t\2\0\0\0\0\0"..., 832) = 832

16959 read(3</lib/x86\_64-linux-gnu/libpcre.so.3.13.2>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0000\25\0\0\0\0\0\0"..., 832) = 832

16959 read(3</lib/x86\_64-linux-gnu/libdl-2.23.so>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\240\r\0\0\0\0\0\0"..., 832) = 832

16959 read(3</lib/x86\_64-linux-gnu/libpthread-2.23.so>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\260`\0\0\0\0\0\0"..., 832) = 832

16959 read(3</proc/filesystems>, "nodev\tsysfs\nnodev\trootfs\nnodev\tr"..., 1024) = 362

16959 read(3</proc/filesystems>, "", 1024) = 0

16956 read(0<pipe:[96374]>, <unfinished ...>

16958 read(0</dev/tty1>, <unfinished ...>

16960 read(3</lib/x86\_64-linux-gnu/libc-2.23.so>, "\177ELF\2\1\1\3\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0P\t\2\0\0\0\0\0"..., 832) = 832

16956 read(0<pipe:[96374]>, <unfinished ...>

16958 read(0</dev/tty1>, <unfinished ...>

16961 read(3</lib/x86\_64-linux-gnu/libselinux.so.1>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\260Z\0\0\0\0\0\0"..., 832) = 832

16961 read(3</lib/x86\_64-linux-gnu/libc-2.23.so>, "\177ELF\2\1\1\3\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0P\t\2\0\0\0\0\0"..., 832) = 832

16961 read(3</lib/x86\_64-linux-gnu/libpcre.so.3.13.2>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0000\25\0\0\0\0\0\0"..., 832) = 832

16961 read(3</lib/x86\_64-linux-gnu/libdl-2.23.so>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\240\r\0\0\0\0\0\0"..., 832) = 832

16961 read(3</lib/x86\_64-linux-gnu/libpthread-2.23.so>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\260`\0\0\0\0\0\0"..., 832) = 832

16961 read(3</proc/filesystems>, "nodev\tsysfs\nnodev\trootfs\nnodev\tr"..., 1024) = 362

16961 read(3</proc/filesystems>, "", 1024) = 0

16956 read(0<pipe:[96374]>, <unfinished ...>

16958 read(0</dev/tty1>, <unfinished ...>

16962 read(3</lib/x86\_64-linux-gnu/libc-2.23.so>, "\177ELF\2\1\1\3\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0P\t\2\0\0\0\0\0"..., 832) = 832

16956 read(0<pipe:[96374]>, <unfinished ...>

16958 read(0</dev/tty1>, <unfinished ...>

16963 read(3</lib/x86\_64-linux-gnu/libselinux.so.1>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\260Z\0\0\0\0\0\0"..., 832) = 832

16963 read(3</lib/x86\_64-linux-gnu/libc-2.23.so>, "\177ELF\2\1\1\3\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0P\t\2\0\0\0\0\0"..., 832) = 832

16963 read(3</lib/x86\_64-linux-gnu/libpcre.so.3.13.2>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0000\25\0\0\0\0\0\0"..., 832) = 832

16963 read(3</lib/x86\_64-linux-gnu/libdl-2.23.so>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\240\r\0\0\0\0\0\0"..., 832) = 832

16963 read(3</lib/x86\_64-linux-gnu/libpthread-2.23.so>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\260`\0\0\0\0\0\0"..., 832) = 832

16963 read(3</proc/filesystems>, "nodev\tsysfs\nnodev\trootfs\nnodev\tr"..., 1024) = 362

16963 read(3</proc/filesystems>, "", 1024) = 0

16956 read(0<pipe:[96374]>, <unfinished ...>

16931 read(0</dev/tty1>, "\33", 1) = 1

16931 read(0</dev/tty1>, "\t", 1) = 1

16931 read(0</dev/tty1>, <detached ...>

Total number of read events: 47

Output C

Read from keyboard event log entries

16995 read(0</dev/tty1>, "Can I get a shell?\n", 400) = 19

16931 read(0</dev/tty1>, "\7", 1) = 1

16931 read(0</dev/tty1>, "w", 1) = 1

16931 read(0</dev/tty1>, "h", 1) = 1

16931 read(0</dev/tty1>, "o", 1) = 1

16931 read(0</dev/tty1>, "a", 1) = 1

16931 read(0</dev/tty1>, "m", 1) = 1

16931 read(0</dev/tty1>, "i", 1) = 1

16931 read(0</dev/tty1>, "\r", 1) = 1

16931 read(0</dev/tty1>, "i", 1) = 1

16931 read(0</dev/tty1>, "d", 1) = 1

16931 read(0</dev/tty1>, "\r", 1) = 1

16931 read(0</dev/tty1>, "u", 1) = 1

16931 read(0</dev/tty1>, "n", 1) = 1

16931 read(0</dev/tty1>, "a", 1) = 1

16931 read(0</dev/tty1>, "m", 1) = 1

16931 read(0</dev/tty1>, "e", 1) = 1

16931 read(0</dev/tty1>, "\r", 1) = 1

16931 read(0</dev/tty1>, <detached ...>

Total number of read from keyboard log entries in Log A: 19

Output D

Read from keyboard event log entries

16931 read(0</dev/tty1>, "\r", 1) = 1

16958 read(0</dev/tty1>, <unfinished ...>

16958 read(0</dev/tty1>, <unfinished ...>

16958 read(0</dev/tty1>, <unfinished ...>

16958 read(0</dev/tty1>, <unfinished ...>

16958 read(0</dev/tty1>, <unfinished ...>

16958 read(0</dev/tty1>, <unfinished ...>

16931 read(0</dev/tty1>, "\33", 1) = 1

16931 read(0</dev/tty1>, "\t", 1) = 1

16931 read(0</dev/tty1>, <detached ...>

Total number of read from keyboard log entries in Log B: 10

Output E

Read from file events

16995 read(3</lib/x86\_64-linux-gnu/libc-2.23.so>, "\177ELF\2\1\1\3\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0P\t\2\0\0\0\0\0"..., 832) = 832

16997 read(3</lib/x86\_64-linux-gnu/libc-2.23.so>, "\177ELF\2\1\1\3\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0P\t\2\0\0\0\0\0"..., 832) = 832

16997 read(3</etc/nsswitch.conf>, "# /etc/nsswitch.conf\n#\n# Example"..., 4096) = 497

16997 read(3</etc/nsswitch.conf>, "", 4096) = 0

16997 read(3</lib/x86\_64-linux-gnu/libnss\_compat-2.23.so>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\320\22\0\0\0\0\0\0"..., 832) = 832

16997 read(3</lib/x86\_64-linux-gnu/libnsl-2.23.so>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\360?\0\0\0\0\0\0"..., 832) = 832

16997 read(3</lib/x86\_64-linux-gnu/libnss\_nis-2.23.so>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\260 \0\0\0\0\0\0"..., 832) = 832

16997 read(3</lib/x86\_64-linux-gnu/libnss\_files-2.23.so>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\260!\0\0\0\0\0\0"..., 832) = 832

16999 read(3</lib/x86\_64-linux-gnu/libselinux.so.1>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\260Z\0\0\0\0\0\0"..., 832) = 832

16999 read(3</lib/x86\_64-linux-gnu/libc-2.23.so>, "\177ELF\2\1\1\3\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0P\t\2\0\0\0\0\0"..., 832) = 832

16999 read(3</lib/x86\_64-linux-gnu/libpcre.so.3.13.2>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0000\25\0\0\0\0\0\0"..., 832) = 832

16999 read(3</lib/x86\_64-linux-gnu/libdl-2.23.so>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\240\r\0\0\0\0\0\0"..., 832) = 832

16999 read(3</lib/x86\_64-linux-gnu/libpthread-2.23.so>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\260`\0\0\0\0\0\0"..., 832) = 832

16999 read(3</proc/filesystems>, "nodev\tsysfs\nnodev\trootfs\nnodev\tr"..., 1024) = 362

16999 read(3</proc/filesystems>, "", 1024) = 0

16999 read(3</etc/locale.alias>, "# Locale name alias data base.\n#"..., 4096) = 2995

16999 read(3</etc/locale.alias>, "", 4096) = 0

16999 read(3</etc/nsswitch.conf>, "# /etc/nsswitch.conf\n#\n# Example"..., 4096) = 497

16999 read(3</etc/nsswitch.conf>, "", 4096) = 0

16999 read(3</lib/x86\_64-linux-gnu/libnss\_compat-2.23.so>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\320\22\0\0\0\0\0\0"..., 832) = 832

16999 read(3</lib/x86\_64-linux-gnu/libnsl-2.23.so>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\360?\0\0\0\0\0\0"..., 832) = 832

16999 read(3</lib/x86\_64-linux-gnu/libnss\_nis-2.23.so>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\260 \0\0\0\0\0\0"..., 832) = 832

16999 read(3</lib/x86\_64-linux-gnu/libnss\_files-2.23.so>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\260!\0\0\0\0\0\0"..., 832) = 832

16999 read(3</proc/sys/kernel/ngroups\_max>, "65536\n", 31) = 6

16999 read(3</proc/sys/kernel/ngroups\_max>, "65536\n", 31) = 6

17001 read(3</lib/x86\_64-linux-gnu/libc-2.23.so>, "\177ELF\2\1\1\3\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0P\t\2\0\0\0\0\0"..., 832) = 832

Total number of read from file events in Log A: 26

Output F

Read from file events

16956 read(3</lib/x86\_64-linux-gnu/libc-2.23.so>, <unfinished ...>

16957 read(3</lib/x86\_64-linux-gnu/libc-2.23.so>, "\177ELF\2\1\1\3\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0P\t\2\0\0\0\0\0"..., 832) = 832

16957 read(3</home/user/test/in.txt>, "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"..., 131072) = 112

16957 read(3</home/user/test/in.txt>, "", 131072) = 0

16956 read(3</lib/x86\_64-linux-gnu/libc-2.23.so>, "\177ELF\2\1\1\3\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0P\t\2\0\0\0\0\0"..., 832) = 832

16958 read(3</lib/x86\_64-linux-gnu/libc-2.23.so>, "\177ELF\2\1\1\3\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0P\t\2\0\0\0\0\0"..., 832) = 832

16959 read(3</lib/x86\_64-linux-gnu/libselinux.so.1>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\260Z\0\0\0\0\0\0"..., 832) = 832

16959 read(3</lib/x86\_64-linux-gnu/libc-2.23.so>, "\177ELF\2\1\1\3\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0P\t\2\0\0\0\0\0"..., 832) = 832

16959 read(3</lib/x86\_64-linux-gnu/libpcre.so.3.13.2>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0000\25\0\0\0\0\0\0"..., 832) = 832

16959 read(3</lib/x86\_64-linux-gnu/libdl-2.23.so>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\240\r\0\0\0\0\0\0"..., 832) = 832

16959 read(3</lib/x86\_64-linux-gnu/libpthread-2.23.so>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\260`\0\0\0\0\0\0"..., 832) = 832

16959 read(3</proc/filesystems>, "nodev\tsysfs\nnodev\trootfs\nnodev\tr"..., 1024) = 362

16959 read(3</proc/filesystems>, "", 1024) = 0

16960 read(3</lib/x86\_64-linux-gnu/libc-2.23.so>, "\177ELF\2\1\1\3\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0P\t\2\0\0\0\0\0"..., 832) = 832

16961 read(3</lib/x86\_64-linux-gnu/libselinux.so.1>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\260Z\0\0\0\0\0\0"..., 832) = 832

16961 read(3</lib/x86\_64-linux-gnu/libc-2.23.so>, "\177ELF\2\1\1\3\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0P\t\2\0\0\0\0\0"..., 832) = 832

16961 read(3</lib/x86\_64-linux-gnu/libpcre.so.3.13.2>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0000\25\0\0\0\0\0\0"..., 832) = 832

16961 read(3</lib/x86\_64-linux-gnu/libdl-2.23.so>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\240\r\0\0\0\0\0\0"..., 832) = 832

16961 read(3</lib/x86\_64-linux-gnu/libpthread-2.23.so>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\260`\0\0\0\0\0\0"..., 832) = 832

16961 read(3</proc/filesystems>, "nodev\tsysfs\nnodev\trootfs\nnodev\tr"..., 1024) = 362

16961 read(3</proc/filesystems>, "", 1024) = 0

16962 read(3</lib/x86\_64-linux-gnu/libc-2.23.so>, "\177ELF\2\1\1\3\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0P\t\2\0\0\0\0\0"..., 832) = 832

16963 read(3</lib/x86\_64-linux-gnu/libselinux.so.1>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\260Z\0\0\0\0\0\0"..., 832) = 832

16963 read(3</lib/x86\_64-linux-gnu/libc-2.23.so>, "\177ELF\2\1\1\3\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0P\t\2\0\0\0\0\0"..., 832) = 832

16963 read(3</lib/x86\_64-linux-gnu/libpcre.so.3.13.2>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0000\25\0\0\0\0\0\0"..., 832) = 832

16963 read(3</lib/x86\_64-linux-gnu/libdl-2.23.so>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\240\r\0\0\0\0\0\0"..., 832) = 832

16963 read(3</lib/x86\_64-linux-gnu/libpthread-2.23.so>, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\260`\0\0\0\0\0\0"..., 832) = 832

16963 read(3</proc/filesystems>, "nodev\tsysfs\nnodev\trootfs\nnodev\tr"..., 1024) = 362

16963 read(3</proc/filesystems>, "", 1024) = 0

Total number of read from file events in Log B: 29

Output G

File A:

File Count Timestamp

/lib/x86\_64-linux-gnu/libc-2.23.so 4 time 89; time 257; time 493; time 893;

/etc/nsswitch.conf 4 time 287; time 288; time 582; time 583;

/lib/x86\_64-linux-gnu/libnss\_compat-2.23.so 2 time 296; time 591;

/lib/x86\_64-linux-gnu/libnsl-2.23.so 2 time 304; time 599;

/lib/x86\_64-linux-gnu/libnss\_nis-2.23.so 2 time 320; time 615;

/lib/x86\_64-linux-gnu/libnss\_files-2.23.so 2 time 328; time 623;

/lib/x86\_64-linux-gnu/libselinux.so.1 1 time 483;

/lib/x86\_64-linux-gnu/libpcre.so.3.13.2 1 time 502;

/lib/x86\_64-linux-gnu/libdl-2.23.so 1 time 510;

/lib/x86\_64-linux-gnu/libpthread-2.23.so 1 time 519;

/proc/filesystems 2 time 549; time 550;

/etc/locale.alias 2 time 562; time 563;

/proc/sys/kernel/ngroups\_max 2 time 656; time 659;

File B:

File Count Timestamp

/lib/x86\_64-linux-gnu/libc-2.23.so 9 time 259; time 343; time 392; time 458;

time 522; time 626; time 684; time 780; time 838;

/home/user/test/in.txt 2 time 369; time 371;

/lib/x86\_64-linux-gnu/libselinux.so.1 3 time 512; time 674; time 828;

/lib/x86\_64-linux-gnu/libpcre.so.3.13.2 3 time 531; time 693; time 847;

/lib/x86\_64-linux-gnu/libdl-2.23.so 3 time 539; time 701; time 855;

/lib/x86\_64-linux-gnu/libpthread-2.23.so 3 time 548; time 710; time 864;

/proc/filesystems 6 time 578; time 579; time 740; time 741;

time 894; time 895;