

# Struttura file csv

Prime due righe:

- macrodroid: indica se è stata usata l'applicazione macrodroid per automatizzare l'applicazione che vogliamo monitorare
- fakeclient: indica se è stato utilizzato il finto client java che simula il dispositivo android connesso al web server

La terza riga è usata per i titoli delle colonne del file csv

Le altre righe sono composte dalle seguenti colonne:

- id: numero istruzione incrementale. Indice che parte da 1.
- Pid: identificativo del processo che sta eseguendo questa syscall
- Spid: identificativo del thread che sta eseguendo questa syscall
- Name: nome della syscall attuale
- Finished: indica se la syscall è terminata oppure se è ancora in esecuzione (valori true e false)
- StartTimestamp: timestamp di inizio syscall
- FinishTimestamp: timestamp di fine syscall
- ReturnValue: valore restituito dalla syscall
- Timestamp: timestamp nella quale viene aggiunto un redflag. Compreso tra StartTimestamp e FinishTimestamp
- DebugApp: red flag se sono installate applicazioni con debuggable flag attivato nel manifest file
- DeveloperOptions: red flag se le impostazioni sviluppatori sono attive nel device che stiamo monitorando
- ChargingType: red flag se il tipo di ricarica è usb
- PtracerStarted: red flag se non è partita automaticamente la libreria c++ e di conseguenza non riusciamo a monitorare i dati a basso livello
- StationaryDevice: red flag se il dispositivo è stato più volte stazionario a lungo
- SensorAlert: red flag se il dispositivo ha assunto più volte posizioni non valida (schermo sotto sopra)
- DebuggerFound: red flag se è stato trovato un debugger gdb o jdwp connesso al dispositivo
- InstructionMuchTime: red flag se ci sono molte istruzioni con una durata più lunga rispetto ai dati raccolti durante la fase di training
- SubsequenceFound: red flag se sono state trovate sottosequenze simili rispetto all'ultima esecuzione e di conseguenza cercare di identificare incremental execution path attacks
- SequenceNotSecure: red flag se sono state trovate molte sequenze syscallA->syscallB che non sono state mappate durante la fase di training

Qui di seguito si può osservare un esempio di file csv.

PS. Alla fine del file si può trovare una spiegazione con un esempio molto semplice.

```
macrodroid=False
fakeclient=False
Id,Pid,Spid,Name,Finished,StartTimestamp,FinishTimestamp,ReturnValue,Timestamp,DebugApp,DeveloperOptions,ChargingType,PtracerStarted,StationaryDevice,SensorAlert,DebuggerFound,InstructionMuchTime,SubsequenceFound,SequenceNotSecure
1,15053,15053,clock_gettime,True,1688223785117321,1688223785125602,0,1688223785117321,no,no,no,no,no,no,no,no,no,no,no
2,15053,15053,clock_gettime,True,1688223785125884,1688223785126759,0,1688223785125884,no,no,no,no,no,no,no,no,no,no,no
3,15053,15053,futex,True,1688223785127213,1688223785128340,1,1688223785127213,no,no,no,no,no,no,no,no,no,no,no
4,15053,15053,futex,True,1688223785128619,1688223785129172,1,1688223785128619,no,no,no,no,no,no,no,no,no,no,no
5,15053,15053,clock_gettime,True,1688223785130434,1688223785131443,0,1688223785130434,no,no,no,no,no,no,no,no,no,no,no
6,15053,15053,clock_gettime,True,1688223785131759,1688223785132644,0,1688223785131759,no,no,no,no,no,no,no,no,no,no,no
7,15053,15053,clock_gettime,True,1688223785133832,1688223785135393,0,1688223785133832,no,no,no,no,no,no,no,no,no,no,no
8,15053,15053,clock_gettime,True,1688223785135594,1688223785137549,0,1688223785135594,no,no,no,no,no,no,no,no,no,no,no
9,15053,15053,clock_gettime,True,1688223785144993,1688223785146084,0,1688223785144993,no,no,no,no,no,no,no,no,no,no,no
10,15053,15053,clock_gettime,True,1688223785146198,1688223785146843,0,1688223785146198,no,no,no,no,no,no,no,no,no,no,no
11,15053,15053,rt_sigprocmask,True,1688223785148484,1688223785149127,0,1688223785148484,no,no,no,no,no,no,no,no,no,no,no
```

12,15053,15053,rt\_sigprocmask,True,1688223785149368,1688223785149901,0,1688223785149368,no,no,no,no,no,no,no,no,no  
13,15053,15053,rt\_sigprocmask,True,1688223785150112,1688223785150628,0,1688223785150112,no,no,no,no,no,no,no,no,no  
14,15053,15053,rt\_sigprocmask,True,1688223785150840,1688223785151354,0,1688223785150840,no,no,no,no,no,no,no,no,no  
15,15053,15053,rt\_sigprocmask,True,1688223785152394,1688223785163326,0,1688223785152394,no,no,no,no,no,no,no,no,no  
16,15053,15053,rt\_sigprocmask,True,1688223785163505,1688223785164404,0,1688223785163505,no,no,no,no,no,no,no,no,no  
17,15053,15053,rt\_sigprocmask,True,1688223785164687,1688223785165669,0,1688223785164687,no,no,no,no,no,no,no,no,no  
18,15053,15053,rt\_sigprocmask,True,1688223785165952,1688223785166541,0,1688223785165952,no,no,no,no,no,no,no,no,no  
19,15184,15184,clock\_gettime,True,1688223962591291,1688223962591986,0,1688223962591291,no,no,no,no,no,no,no,no,no  
20,15184,15184,ioctl,True,1688223962592124,1688223962607227,0,1688223962592124,no,no,no,no,no,no,no,no,no  
21,15184,15184,clock\_gettime,True,1688223962607306,1688223962607587,0,1688223962607306,no,no,no,no,no,no,no,no,no  
22,15184,15184,ioctl,True,1688223962608214,1688223962610766,0,1688223962608214,no,no,no,no,no,no,no,no,no  
23,15184,15184,ioctl,True,1688223962610959,1688223962612047,0,1688223962610959,no,no,no,no,no,no,no,no,no  
24,15184,15184,futex,True,1688223962612161,1688223962614645,1,1688223962612161,no,no,no,no,no,no,no,no,no  
25,15184,15184,ioctl,True,1688223962617123,1688223962619465,0,1688223962617123,no,no,no,no,no,no,no,no,no  
26,15184,15184,ioctl,True,1688223962619618,1688223962620138,0,1688223962619618,no,no,no,no,no,no,no,no,no  
27,15184,15184,getuid,True,1688223962620221,1688223962620512,10333,1688223962620221,no,no,no,no,no,no,no,no,no  
28,15184,15184,prctl,True,1688223962620557,1688223962621533,1,1688223962620557,no,no,no,no,no,no,no,no,no  
29,15184,15184,mprotect,True,1688223962621750,1688223962622554,0,1688223962621750,no,no,no,no,no,no,no,no,no  
30,15184,15184,mprotect,True,1688223962622663,1688223962623481,0,1688223962622663,no,no,no,no,no,no,no,no,no  
31,15184,15184,mprotect,True,1688223962623545,1688223962624459,0,1688223962623545,no,no,no,no,no,no,no,no,no  
32,15184,15184,mprotect,True,1688223962624571,1688223962626667,0,1688223962624571,no,no,no,no,no,no,no,no,no  
33,15184,15184,mmap,True,1688223962626769,1688223962627897,503664656384,1688223962626769,no,no,no,no,no,no,no,no,no  
34,15184,15184,prctl,True,1688223962627985,1688223962628899,0,1688223962627985,no,no,no,no,no,no,no,no,no  
35,15184,15184,openat,True,1688223962629091,1688223962629677,18446744073709551614,1688223962629091,no,no,no,no,no,no,no,no,no  
36,15184,15184,openat,True,1688223962631506,1688223962638599,18446744073709551614,1688223962631506,no,no,no,no,no,no,no,no,no  
37,15184,15184,mprotect,True,1688223962638774,1688223962639553,0,1688223962638774,no,no,no,no,no,no,no,no,no  
38,15184,15184,mprotect,True,1688223962639618,1688223962641794,0,1688223962639618,no,no,no,no,no,no,no,no,no  
39,15184,15184,mprotect,True,1688223962642253,1688223962642938,0,1688223962642253,no,no,no,no,no,no,no,no,no  
40,15184,15184,mprotect,True,1688223962643050,1688223962643774,0,1688223962643050,no,no,no,no,no,no,no,no,no  
41,15184,15184,munmap,True,1688223962643852,1688223962644502,0,1688223962643852,no,no,no,no,no,no,no,no,no  
42,15184,15184,ioctl,True,1688223962645066,1688223962645986,0,1688223962645066,no,no,no,no,no,no,no,no,no  
43,15184,15184,clock\_gettime,True,1688223962646255,1688223962676306,0,1688223962646255,no,no,no,no,no,no,no,no,no  
44,15184,15184,clock\_gettime,True,1688223962676483,1688223962677645,0,1688223962676483,no,no,no,no,no,no,no,no,no  
45,15184,15184,clock\_gettime,True,1688223962678330,1688223962681306,0,1688223962678330,no,no,no,no,no,no,no,no,no  
46,15184,15184,ioctl,True,1688223962681426,1688223962683116,0,1688223962681426,no,no,no,no,no,no,no,no,no  
47,15184,15184,clock\_gettime,True,1688223962683280,1688223962684277,0,1688223962683280,no,no,no,no,no,no,no,no,no  
48,15184,15184,ioctl,True,1688223962684404,1688223962685848,0,1688223962684404,no,no,no,no,no,no,no,no,no  
49,15184,15184,mprotect,True,1688223962686121,1688223962687728,0,1688223962686121,no,no,no,no,no,no,no,no,no  
50,15184,15184,mprotect,True,1688223962687830,1688223962688613,0,1688223962687830,no,no,no,no,no,no,no,no,no  
51,15184,15184,clock\_gettime,True,1688223962688835,1688223962689752,0,1688223962688835,no,no,no,no,no,no,no,no,no  
52,15184,15184,ioctl,True,1688223962689852,1688223962691145,0,1688223962689852,no,no,no,no,no,no,no,no,no  
53,15184,15184,clock\_gettime,True,1688223962691328,1688223962698462,0,1688223962691328,no,no,no,no,no,no,no,no,no  
54,15184,15184,ioctl,True,1688223962698593,1688223962699037,0,1688223962698593,no,no,no,no,no,no,no,no,no  
55,15184,15184,write,True,1688223962699663,1688223962701724,8,1688223962699663,no,no,no,no,no,no,no,no,no  
56,15184,15184,ioctl,True,1688223962702857,1688223962705818,0,1688223962702857,no,no,no,no,no,no,no,no,no  
57,15184,15184,clock\_gettime,True,1688223962708920,1688223962712427,0,1688223962708920,no,no,no,no,no,no,no,no,no  
58,15184,15184,ioctl,True,1688223962712551,1688223962714134,0,1688223962712551,no,no,no,no,no,no,no,no,no  
59,15184,15184,clock\_gettime,True,1688223962714263,1688223962715178,0,1688223962714263,no,no,no,no,no,no,no,no,no  
60,15184,15184,ioctl,True,1688223962715387,1688223962716233,0,1688223962715387,no,no,no,no,no,no,no,no,no  
61,15184,15184,write,True,1688223962718043,1688223962720588,8,1688223962718043,no,no,no,no,no,no,no,no,no  
62,15184,15184,write,True,1688223962720811,1688223962721818,8,1688223962720811,no,no,no,no,no,no,no,no,no  
63,15184,15184,getuid,True,1688223962722264,1688223962723061,10333,1688223962722264,no,no,no,no,no,no,no,no,no  
64,15184,15184,getuid,True,1688223962723296,1688223962723952,10333,1688223962723296,no,no,no,no,no,no,no,no,no  
65,15184,15184,getuid,True,1688223962724158,1688223962726000,10333,1688223962724158,no,no,no,no,no,no,no,no,no  
66,15184,15184,getuid,True,1688223962726198,1688223962726888,10333,1688223962726198,no,no,no,no,no,no,no,no,no  
67,15184,15184,gettextofday,True,1688223962727019,1688223962727695,0,1688223962727019,no,no,no,no,no,no,no,no,no  
68,15184,15184,futex,True,1688223962729663,1688223962738872,0,1688223962729663,no,no,no,no,no,no,no,no,no  
69,15184,15184,futex,True,1688223962739071,1688223962739988,0,1688223962739071,no,no,no,no,no,no,no,no,no  
70,15184,15184,futex,True,1688223962740174,1688223962740848,0,1688223962740174,no,no,no,no,no,no,no,no,no  
71,15184,15184,futex,True,1688223962740909,1688223962741605,0,1688223962740909,no,no,no,no,no,no,no,no,no  
72,15184,15184,futex,True,1688223962741721,1688223962742420,0,1688223962741721,no,no,no,no,no,no,no,no,no  
73,15184,15184,futex,True,1688223962742500,1688223962743087,0,1688223962742500,no,no,no,no,no,no,no,no,no  
74,15184,15184,futex,True,1688223962743164,1688223962743790,0,1688223962743164,no,no,no,no,no,no,no,no,no  
75,15184,15184,futex,True,1688223962743876,1688223962745647,0,1688223962743876,no,no,no,no,no,no,no,no,no  
76,15184,15184,futex,True,1688223962746008,1688223962747968,0,1688223962746008,no,no,no,no,no,no,no,no,no  
77,15184,15184,futex,True,1688223962748082,1688223962748971,0,1688223962748082,no,no,no,no,no,no,no,no,no  
78,15184,15184,futex,True,1688223962749789,1688223962752663,0,1688223962749789,no,no,no,no,no,no,no,no,no  
79,15184,15184,futex,True,1688223962752790,1688223962753902,0,1688223962752790,no,no,no,no,no,no,no,no,no  
80,15184,15184,futex,True,1688223962754038,1688223962754916,0,1688223962754038,no,no,no,no,no,no,no,no,no  
81,15184,15184,futex,True,1688223962755003,1688223962756415,0,1688223962755003,no,no,no,no,no,no,no,no,no  
82,15184,15184,futex,True,1688223962756556,1688223962757933,0,1688223962756556,no,no,no,no,no,no,no,no,no  
83,15184,15184,futex,True,1688223962758030,1688223962758664,0,1688223962758030,no,no,no,no,no,no,no,no,no  
84,15184,15184,futex,True,1688223962758737,1688223962759439,0,1688223962758737,no,no,no,no,no,no,no,no,no  
85,15184,15184,futex,True,1688223962759522,1688223962760251,0,1688223962759522,no,no,no,no,no,no,no,no,no  
86,15184,15184,futex,True,1688223962760322,1688223962761700,0,1688223962760322,no,no,no,no,no,no,no,no,no  
87,15184,15184,futex,True,1688223962761784,1688223962762435,0,1688223962761784,no,no,no,no,no,no,no,no,no  
88,15184,15184,futex,True,1688223962762518,1688223962763141,0,1688223962762518,no,no,no,no,no,no,no,no,no  
89,15184,15184,futex,True,1688223962763223,1688223962763848,1,1688223962763223,no,no,no,no,no,no,no,no,no  
90,15184,15184,futex,True,1688223962763928,1688223962764569,1,1688223962763928,no,no,no,no,no,no,no,no,no  
91,15184,15184,clock\_gettime,True,168822396277754,1688223962778573,0,168822396277754,no,no,no,no,no,no,no,no,no  
92,15184,15184,clock\_gettime,True,1688223962778921,1688223962779556,0,1688223962778921,no,no,no,no,no,no,no,no,no  
93,15184,15184,clock\_gettime,True,1688223962779771,1688223962780359,0,1688223962779771,no,no,no,no,no,no,no,no,no  
94,15184,15184,clock\_gettime,True,1688223962780557,1688223962781114,0,1688223962780557,no,no,no,no,no,no,no,no,no  
95,15184,15184,clock\_gettime,True,1688223962782038,1688223962782763,0,1688223962782038,no,no,no,no,no,no,no,no,no  
96,15184,15184,clock\_gettime,True,1688223962782978,1688223962783579,0,1688223962782978,no,no,no,no,no,no,no,no,no  
97,15184,15184,ioctl,True,1688223962783789,1688223962785011,0,1688223962783789,no,no,no,no,no,no,no,no,no  
98,15184,15184,clock\_gettime,True,1688223962785807,1688223962786526,0,1688223962785807,no,no,no,no,no,no,no,no,no  
99,15184,15184,ioctl,True,1688223962786737,1688223962787404,0,1688223962786737,no,no,no,no,no,no,no,no,no  
100,15184,15184,clock\_gettime,True,1688223962787986,1688223962788736,0,1688223962787986,no,no,no,no,no,no,no,no,no  
101,15184,15184,clock\_gettime,True,1688223962788819,1688223962789466,0,1688223962788819,no,no,no,no,no,no,no,no,no  
102,15184,15184,clock\_gettime,True,1688223962789696,1688223962790332,0,1688223962789696,no,no,no,no,no,no,no,no,no  
103,15184,15184,clock\_gettime,True,1688223962790423,1688223962791011,0,1688223962790423,no,no,no,no,no,no,no,no,no  
104,15184,15184,clock\_gettime,True,1688223962791199,1688223962791838,0,1688223962791199,no,no,no,no,no,no,no,no,no  
105,15184,15184,clock\_gettime,True,1688223962791968,1688223962795261,0,1688223962791968,no,no,no,no,no,no,no,no,no  
106,15184,15184,clock\_gettime,True,1688223962792780,1688223962793352,0,1688223962792780,no,no,no,no,no,no,no,no,no  
107,15184,15184,clock\_gettime,True,1688223962793541,1688223962794069,0,1688223962793541,no,no,no,no,no,no,no,no,no  
108,15184,15184,write,True,1688223962794520,1688223962796070,8,1688223962794520,no,no,no,no,no,no,no,no,no  
109,15184,15184,clock\_gettime,True,1688223962796212,1688223962796986,0,1688223962796212,no,no,no,no,no,no,no,no,no  
110,15184,15184,clock\_gettime,True,1688223962799363,1688223962800484,0,1688223962799363,no,no,no,no,no,no,no,no,no  
111,15184,15184,clock\_gettime,True,1688223962800553,1688223962801197,0,1688223962800553,no,no,no,no,no,no,no,no,no  
112,15184,15184,clock\_gettime,True,1688223962801397,1688223962802124,0,1688223962801397,no,no,no,no,no,no,no,no,no  
113,15184,15184,clock\_gettime,True,1688223962803087,1688223962803847,0,1688223962803087,no,no,no,no,no,no,no,no,no  
114,15184,15184,prctl,True,1688223962807488,1688223962808350,1,1688223962807488,no,no,no,no,no,no,no,no,no  
115,15184,15184,mprotect,True,1688223962808517,1688223962809113,0,1688223962808517,no,no,no,no,no,no,no,no,no  
116,15184,15184,mprotect,True,1688223962809210,1688223962809885,0,1688223962809210,no,no,no,no,no,no,no,no,no  
117,15184,15184,mprotect,True,1688223962809961,1688223962810676,0,1688223962809961,no,no,no,no,no,no,no,no,no  
118,15184,15184,mprotect,True,1688223962810767,1688223962811993,0,1688223962810767,no,no,no,no,no,no,no,no,no  
119,15184,15184,mmap,True,1688223962812087,1688223962812857,503664656384,1688223962812087,no,no,no,no,no,no,no,no,no

120,15184,15184,prctl,True,1688223962812898,1688223962813497,0,1688223962812898,no,no,no,no,no,no,no,no  
121,15184,15184,openat,True,1688223962813583,1688223962814216,105,1688223962813583,no,no,no,no,no,no,no,no  
122,15184,15184,readlinkat,True,1688223962814285,1688223962815014,37,1688223962814285,no,no,no,no,no,no,no,no  
123,15184,15184,fstat,True,1688223962815081,1688223962816228,0,1688223962815081,no,no,no,no,no,no,no,no  
124,15184,15184,mmap,True,1688223962816860,1688223962817641,506235072512,1688223962816860,no,no,no,no,no,no,no,no  
125,15184,15184,prctl,True,1688223962817684,1688223962818287,0,1688223962817684,no,no,no,no,no,no,no,no  
126,15184,15184,munmap,True,1688223962818766,1688223962819434,0,1688223962818766,no,no,no,no,no,no,no,no  
127,15184,15184,close,True,1688223962819517,1688223962820091,0,1688223962819517,no,no,no,no,no,no,no,no  
128,15184,15184,mprotect,True,1688223962820166,1688223962821092,0,1688223962820166,no,no,no,no,no,no,no,no  
129,15184,15184,mprotect,True,1688223962821175,1688223962821917,0,1688223962821175,no,no,no,no,no,no,no,no  
130,15184,15184,mprotect,True,1688223962822037,1688223962822847,0,1688223962822037,no,no,no,no,no,no,no,no  
131,15184,15184,mprotect,True,1688223962822920,1688223962823625,0,1688223962822920,no,no,no,no,no,no,no,no  
132,15184,15184,munmap,True,1688223962823695,1688223962824363,0,1688223962823695,no,no,no,no,no,no,no,no  
133,15184,15184,prctl,True,1688223962824438,1688223962825295,1,1688223962824438,no,no,no,no,no,no,no,no  
134,15184,15184,clock\_gettime,True,1688223962834628,1688223962835567,0,1688223962834628,no,no,no,no,no,no,no,no  
135,15184,15184,write,True,1688223962835666,1688223962836388,8,1688223962835666,no,no,no,no,no,no,no,no  
136,15184,15184,futex,True,1688223962836429,1688223962837683,18446744073709551605,1688223962836429,no,no,no,no,no,no,no,no  
137,15184,15184,write,True,1688223962837777,1688223962838299,8,1688223962837777,no,no,no,no,no,no,no,no  
138,15184,15184,futex,True,1688223962838340,1688223962857342,0,1688223962838340,no,no,no,no,no,no,no,no  
139,15184,15184,clock\_gettime,True,1688223962857659,1688223962859113,0,1688223962857659,no,no,no,no,no,no,no,no  
140,15184,15184,clock\_gettime,True,1688223962859306,1688223962860009,0,1688223962859306,no,no,no,no,no,no,no,no  
141,15184,15184,clock\_gettime,True,1688223962860160,1688223962860719,0,1688223962860160,no,no,no,no,no,no,no,no  
142,15184,15184,read,True,1688223962860812,1688223962861647,48,1688223962860812,no,no,no,no,no,no,no,no  
143,15184,15184,futex,True,1688223962862355,1688223962863039,18446744073709551605,1688223962862355,no,no,no,no,no,no,no,no  
144,15184,15184,clock\_gettime,True,1688223962863120,1688223962863784,0,1688223962863120,no,no,no,no,no,no,no,no  
145,15184,15184,getuid,True,1688223962863850,1688223962865844,10333,1688223962863850,no,no,no,no,no,no,no,no  
146,15184,15184,writev,True,1688223962865941,1688223962868207,275,1688223962865941,no,no,no,no,no,no,no,no  
147,15184,15184,futex,True,1688223962868345,1688223962868962,1,1688223962868345,no,no,no,no,no,no,no,no  
148,15184,15184,getuid,True,1688223962869102,1688223962869696,10333,1688223962869102,no,no,no,no,no,no,no,no  
149,15184,15184,epoll\_wait,True,1688223962869795,1688223962870332,1,1688223962869795,no,no,no,no,no,no,no,no  
150,15184,15184,read,True,1688223962870391,1688223962870920,8,1688223962870391,no,no,no,no,no,no,no,no  
151,15184,15184,clock\_gettime,True,1688223962870984,1688223962871533,0,1688223962870984,no,no,no,no,no,no,no,no  
152,15184,15184,clock\_gettime,True,1688223962871671,1688223962872275,0,1688223962871671,no,no,no,no,no,no,no,no  
153,15184,15184,gettextofday,True,1688223962872351,1688223962873326,0,1688223962872351,no,no,no,no,no,no,no,no  
154,15184,15184,read,True,1688223962873418,1688223962873968,48,1688223962873418,no,no,no,no,no,no,no,no  
155,15184,15184,ioctl,True,1688223962874364,1688223962876001,0,1688223962874364,no,no,no,no,no,no,no,no  
156,15184,15184,clock\_gettime,True,1688223962876343,1688223962881004,0,1688223962876343,no,no,no,no,no,no,no,no  
156,15184,15184,clock\_gettime,True,1688223962876343,1688223962881004,0,1688223962876343,no,no,no,no,no,no,no,no  
157,15184,15184,read,True,1688223962881138,1688223962890929,48,1688223962881138,alert,alert,no,no,no,no,no,no,alert  
157,15184,15184,read,True,1688223962881138,1688223962890929,48,1688223962885857,alert,alert,no,no,no,no,no,no,alert  
158,15184,15184,getuid,True,1688223962891106,1688223962892531,10333,1688223962891106,alert,alert,no,no,no,no,no,no,alert  
159,15184,15184,epoll\_wait,True,1688223962892677,1688223962893528,0,1688223962892677,alert,alert,no,no,no,no,no,no,alert  
160,15184,15184,clock\_gettime,True,1688223962893662,1688223962894860,0,1688223962893662,alert,alert,no,no,no,no,no,no,alert  
161,15184,15184,clock\_gettime,True,1688223962895075,1688223962896580,0,1688223962895075,alert,alert,no,no,no,no,no,no,alert  
162,15184,15184,gettextofday,True,1688223962896667,1688223962897255,0,1688223962896667,alert,alert,no,no,no,no,no,no,alert  
163,15184,15184,read,True,1688223962897342,1688223962900158,48,1688223962897342,alert,alert,no,no,no,no,no,no,alert  
164,15184,15184,clock\_gettime,True,1688223962901337,1688223962902153,0,1688223962901337,alert,alert,no,no,no,no,no,no,alert  
165,15184,15184,clock\_gettime,True,1688223962902395,1688223962903901,0,1688223962902395,alert,alert,no,no,no,no,no,no,alert  
166,15184,15184,clock\_gettime,True,1688223962904265,1688223962906914,0,1688223962904265,alert,alert,no,no,no,no,no,no,alert  
167,15184,15184,clock\_gettime,True,1688223962907009,1688223962921210,0,1688223962907009,alert,alert,no,no,no,no,no,no,alert  
168,15184,15184,clock\_gettime,True,1688223962921716,1688223962922463,0,1688223962921716,alert,alert,no,no,no,no,no,no,alert  
169,15184,15184,clock\_gettime,True,1688223962922549,1688223962923137,0,1688223962922549,alert,alert,no,no,no,no,no,no,alert  
170,15184,15184,clock\_gettime,True,1688223962923326,1688223962923941,0,1688223962923326,alert,alert,no,no,no,no,no,no,alert  
171,15184,15184,clock\_gettime,True,1688223962924015,1688223962924564,0,1688223962924015,alert,alert,no,no,no,no,no,no,alert  
172,15184,15184,clock\_gettime,True,1688223962924697,1688223962925626,0,1688223962924697,alert,alert,no,no,no,no,no,no,alert  
173,15184,15184,clock\_gettime,True,1688223962925697,1688223962926308,0,1688223962925697,alert,alert,no,no,no,no,no,no,alert  
174,15184,15184,clock\_gettime,True,1688223962926468,1688223962927060,0,1688223962926468,alert,alert,no,no,no,no,no,no,alert  
175,15184,15184,clock\_gettime,True,1688223962927323,1688223962927870,0,1688223962927323,alert,alert,no,no,no,no,no,no,alert  
176,15184,15184,clock\_gettime,True,1688223962928167,1688223962928801,0,1688223962928167,alert,alert,no,no,no,no,no,no,alert  
177,15184,15184,clock\_gettime,True,1688223962928874,1688223962929430,0,1688223962928874,alert,alert,no,no,no,no,no,no,alert  
178,15184,15184,clock\_gettime,True,1688223962929625,1688223962930191,0,1688223962929625,alert,alert,no,no,no,no,no,no,alert  
179,15184,15184,clock\_gettime,True,1688223962930263,1688223962930826,0,1688223962930263,alert,alert,no,no,no,no,no,no,alert  
180,15184,15184,clock\_gettime,True,1688223962930973,1688223962931533,0,1688223962930973,alert,alert,no,no,no,no,no,no,alert  
181,15184,15184,clock\_gettime,True,1688223962931604,1688223962932142,0,1688223962931604,alert,alert,no,no,no,no,no,no,alert  
182,15184,15184,clock\_gettime,True,1688223962932332,1688223962932952,0,1688223962932332,alert,alert,no,no,no,no,no,no,alert  
183,15184,15184,clock\_gettime,True,1688223962933035,1688223962933583,0,1688223962933035,alert,alert,no,no,no,no,no,no,alert  
184,15184,15184,clock\_gettime,True,1688223962933737,1688223962934333,0,1688223962933737,alert,alert,no,no,no,no,no,no,alert  
185,15184,15184,clock\_gettime,True,1688223962934399,1688223962936053,0,1688223962934399,alert,alert,no,no,no,no,no,no,alert  
186,15184,15184,clock\_gettime,True,1688223962936695,1688223962937702,0,1688223962936695,alert,alert,no,no,no,no,no,no,alert  
187,15184,15184,clock\_gettime,True,1688223962937787,1688223962938404,0,1688223962937787,alert,alert,no,no,no,no,no,no,alert  
188,15184,15184,clock\_gettime,True,1688223962938570,1688223962939181,0,1688223962938570,alert,alert,no,no,no,no,no,no,alert  
189,15184,15184,clock\_gettime,True,1688223962939250,1688223962939856,0,1688223962939250,alert,alert,no,no,no,no,no,no,alert  
190,15184,15184,clock\_gettime,True,1688223962940306,1688223962941024,0,1688223962940306,alert,alert,no,no,no,no,no,no,alert  
191,15184,15184,clock\_gettime,True,1688223962941177,1688223962941785,0,1688223962941177,alert,alert,no,no,no,no,no,no,alert  
192,15184,15184,clock\_gettime,True,1688223962942015,1688223962942632,0,1688223962942015,alert,alert,no,no,no,no,no,no,alert  
193,15184,15184,clock\_gettime,True,1688223962942709,1688223962943346,0,1688223962942709,alert,alert,no,no,no,no,no,no,alert  
194,15184,15184,clock\_gettime,True,1688223962943504,1688223962944454,0,1688223962943504,alert,alert,no,no,no,no,no,no,alert  
195,15184,15184,clock\_gettime,True,1688223962944540,1688223962945943,0,1688223962944540,alert,alert,no,no,no,no,no,no,alert  
196,15184,15184,clock\_gettime,True,1688223962946162,1688223962946879,0,1688223962946162,alert,alert,no,no,no,no,no,no,alert  
197,15184,15184,clock\_gettime,True,1688223962946953,1688223962947536,0,1688223962946953,alert,alert,no,no,no,no,no,no,alert  
198,15184,15184,clock\_gettime,True,1688223962947686,1688223962948314,0,1688223962947686,alert,alert,no,no,no,no,no,no,alert  
199,15184,15184,clock\_gettime,True,1688223962948359,1688223962948941,0,1688223962948359,alert,alert,no,no,no,no,no,no,alert  
200,15184,15184,clock\_gettime,True,1688223962949136,1688223962949739,0,1688223962949136,alert,alert,no,no,no,no,no,no,alert  
201,15184,15184,clock\_gettime,True,1688223962949796,1688223962950396,0,1688223962949796,alert,alert,no,no,no,no,no,no,alert  
202,15184,15184,clock\_gettime,True,1688223962950578,1688223962951190,0,1688223962950578,alert,alert,no,no,no,no,no,no,alert  
203,15184,15184,clock\_gettime,True,1688223962951235,1688223962951816,0,1688223962951235,alert,alert,no,no,no,no,no,no,alert  
204,15184,15184,clock\_gettime,True,1688223962951973,1688223962952718,0,1688223962951973,alert,alert,no,no,no,no,no,no,alert  
205,15184,15184,clock\_gettime,True,1688223962952780,1688223962953354,0,1688223962952780,alert,alert,no,no,no,no,no,no,alert  
206,15184,15184,clock\_gettime,True,1688223962953556,1688223962954142,0,1688223962953556,alert,alert,no,no,no,no,no,no,alert  
207,15184,15184,clock\_gettime,True,1688223962954201,1688223962954875,0,1688223962954201,alert,alert,no,no,no,no,no,no,alert  
208,15184,15184,clock\_gettime,True,1688223962955011,1688223962955776,0,1688223962955011,alert,alert,no,no,no,no,no,no,alert  
209,15184,15184,clock\_gettime,True,1688223962955820,1688223962956618,0,1688223962955820,alert,alert,no,no,no,no,no,no,alert  
210,15184,15184,clock\_gettime,True,1688223962956781,1688223962957442,0,1688223962956781,alert,alert,no,no,no,no,no,no,alert  
211,15184,15184,clock\_gettime,True,1688223962957487,1688223962958054,0,1688223962957487,alert,alert,no,no,no,no,no,no,alert  
212,15184,15184,clock\_gettime,True,1688223962958195,1688223962958840,0,1688223962958195,alert,alert,no,no,no,no,no,no,alert  
213,15184,15184,clock\_gettime,True,1688223962958901,1688223962959440,0,1688223962958901,alert,alert,no,no,no,no,no,no,alert  
214,15184,15184,clock\_gettime,True,1688223962959619,1688223962960230,0,1688223962959619,alert,alert,no,no,no,no,no,no,alert  
215,15184,15184,clock\_gettime,True,1688223962960278,1688223962960833,0,1688223962960278,alert,alert,no,no,no,no,no,no,alert

## Esempio di righe

```
156,15184,15184,clock_gettime,True,1688223962876343,1688223962881004,0,1688223962876343,no,no,no,no,no,no,no,no,no  
156,15184,15184,clock_gettime,True,1688223962876343,1688223962881004,0,1688223962878688,alert,alert,no,no,no,no,no,no,no
```

### Spiegazione:

- Possiamo osservare che la syscall numero 156 è l'istruzione `clock_gettime` ed inizia al timestamp 1688223962876343 e finisce al timestamp 1688223962881004.
- Possiamo osservare che dal timestamp 1688223962876343 al timestamp 1688223962878687 non c'è nessun red flag attivato. Infatti è stata aggiunta una seconda riga con la stessa syscall che indica che dal timestamp 1688223962878688 sono stati attivati i primi due red flag nello stesso momento.
- Di conseguenza una struttura a range di timestamp è utile per osservare i sotto timestamp per ciascuna syscall quando alcuni red flag vengono attivati.