UECE – SISTEMAS OPERACIONAIS
PROJETO DE PROGRAMAÇÃO
NOME:GUSTAVO DOS SANTOS SOARES
MATRÍCULA: 1357347

Item A

Aplicações escolhidas:
- cp (copiar)
- mv (mover)

Arquivos de strace gerados com Ids e chamadas:

log_syscall_cp.txt

```
[00007fc3f98c6fb7] execve
[00007fe0bcd24639] brk
[00007fe0bcd2540a] access
[00007fe0bcd25357] open
[00007fe0bcd252e2] fstat
[00007fe0bcd2550a] mmap
[00007fe0bcd254b7] close
[00007fe0bcd25357] open
[00007fe0bcd25377] read
[00007fe0bcd252e2] fstat
[00007fe0bcd2550a] mmap
[00007fe0bcd2550a] mmap
[00007fe0bcd255a7] mprotect
[00007fe0bcd2550a] mmap
[00007fe0bcd254b7] close
[00007fe0bcd25357] open
[00007fe0bcd25377] read
[00007fe0bcd252e2] fstat
[00007fe0bcd2550a] mmap
[00007fe0bcd255a7] mprotect
[00007fe0bcd2550a] mmap
[00007fe0bcd254b7] close
[00007fe0bcd25357] open
[00007fe0bcd25377] read
[00007fe0bcd252e2] fstat
[00007fe0bcd2550a] mmap
[00007fe0bcd255a7] mprotect
[00007fe0bcd2550a] mmap
[00007fe0bcd2550a] mmap
[00007fe0bcd254b7] close
[00007fe0bcd2550a] mmap
[00007fe0bcd0cc55] arch_prctl
[00007fe0bcd255a7] mprotect
```

```
[00007fe0bcd255a7] mprotect
[00007fe0bcd255a7] mprotect
[00007fe0bcd255a7] mprotect
[00007fe0bcd255a7] mprotect
[00007fe0bcd25587] munmap
[00007fe0bc63d799] brk
[00007fe0bc63d799] brk
[00007fe0bc5833c3] open
[00007fe0bc6374e2] fstat
[00007fe0bc64123a] mmap
[00007fe0bc583487] close
[00007fe0bc614997] geteuid
[00007fe0bc5cd4ea] open
[00007fe0bc6374e2] fstat
[00007fe0bc5ccf4c] read
[00007fe0bc5ccf4c] read
[00007fe0bc5cbb0b] close
[00007fe0bc586dc1] open
[00007fe0bc586dc1] open
[00007fe0bc586dc1] open
[00007fe0bc586dc1] open
[00007fe0bc637bf0] write
[00007fe0bc637bf0] write
[00007fe0bc637bf0] write
[00007fe0bc637bf0] write
[00007fe0bc637c4d] lseek
[00007fe0bc5cbb0b] close
[00007fe0bc5cbb0b] close
[00007fe0bc5cbb0b] close
[00007fe0bc613f88] exit_group
```

log_syscall_mv.txt

```
[00007fd52863efb7] execve
[00007f61d2c39639] brk
[00007f61d2c3a40a] access
[00007f61d2c3a357] open
[00007f61d2c3a2e2] fstat
[00007f61d2c3a50a] mmap
[00007f61d2c3a4b7] close
[00007f61d2c3a357] open
[00007f61d2c3a377] read
[00007f61d2c3a2e2] fstat
[00007f61d2c3a50a] mmap
[00007f61d2c3a50a] mmap
[00007f61d2c3a5a7] mprotect
[00007f61d2c3a50a] mmap
[00007f61d2c3a4b7] close
```

[00007f61d2c3a357] open
[00007f61d2c3a377] read
[00007f61d2c3a2e2] fstat
[00007f61d2c3a50a] mmap
[00007f61d2c3a5a7] mprotect
[00007f61d2c3a50a] mmap
[00007f61d2c3a4b7] close
[00007f61d2c3a357] open
[00007f61d2c3a377] read
[00007f61d2c3a2e2] fstat
[00007f61d2c3a50a] mmap
[00007f61d2c3a5a7] mprotect
[00007f61d2c3a50a] mmap
[00007f61d2c3a50a] mmap
[00007f61d2c3a4b7] close
[00007f61d2c3a50a] mmap
[00007f61d2c21c55] arch_prctl
[00007f61d2c3a5a7] mprotect
[00007f61d2c3a5a7] mprotect
[00007f61d2c3a5a7] mprotect
[00007f61d2c3a5a7] mprotect
[00007f61d2c3a5a7] mprotect
[00007f61d2c3a587] munmap
[00007f61d2552799] brk
[00007f61d2552799] brk
[00007f61d24983c3] open
[00007f61d254c4e2] fstat
[00007f61d255623a] mmap
[00007f61d2498487] close
[00007f61d2529997] geteuid
[00007f61d2551f4a] ioctl
[00007f61d24e24ea] open
[00007f61d254c4e2] fstat
[00007f61d24e1f4c] read
[00007f61d24e1f4c] read
[00007f61d24e0b0b] close
[00007f61d249bdc1] open
[00007f61d249bdc1] open
[00007f61d249bdc1] open
[00007f61d249bdc1] open
[00007f61d254cbf0] write
[00007f61d254cbf0] write
[00007f61d254cbf0] write
[00007f61d254cbf0] write
[00007f61d254cc4d] lseek
[00007f61d24e0b0b] close
[00007f61d24e0b0b] close
[00007f61d24e0b0b] close

[00007f61d2528f88] exit_group

OBS: como as aplicações cp e mv são muito parecidas, a maioria das chamadas que elas fazem ao sistema coicidem.

Os logs são gerados pelo seguinte algoritmo:

_create_log_file

```
def _create_log_file(file="log_cp.txt",arq="teste_cp.txt"):
    with open(file,"r") as file1:
        with open(arq,"w") as arq1:
           for line in file1:
                result = line.split("(")[0]
                if result[1] != "+":
                   arq1.write(result+"\n")

_create_log_file(file="log_cp.txt",arq="teste_cp.txt")
```

Descrição: o código a seguir recebe o id e o nome de cada chamada que a aplicação faz ao sistema a partir dos straces

(I)

Criação dos N-grams

n_gram_cp

execve, brk, access, open, fstat, mmap, close, open, read, fstat
brk, access, open, fstat, mmap, close, open, read, fstat, mmap
access, open, fstat, mmap, close, open, read, fstat, mmap, mmap
open, fstat, mmap, close, open, read, fstat, mmap, mmap, mprotect
fstat, mmap, close, open, read, fstat, mmap, mmap, mprotect, mmap
mmap, close, open, read, fstat, mmap, mmap, mprotect, mmap, close
close, open, read, fstat, mmap, mmap, mprotect, mmap, close, open
open, read, fstat, mmap, mmap, mprotect, mmap, close, open, read
read, fstat, mmap, mmap, mprotect, mmap, close, open, read, fstat
fstat, mmap, mmap, mprotect, mmap, close, open, read, fstat, mmap
mmap, mmap, mprotect, mmap, close, open, read, fstat, mmap, mprotect
mmap, mprotect, mmap, close, open, read, fstat, mmap, mprotect, mmap
mprotect, mmap, close, open, read, fstat, mmap, mprotect, mmap, close
mmap, close, open, read, fstat, mmap, mprotect, mmap, close, open
close, open, read, fstat, mmap, mprotect, mmap, close, open, read
open, read, fstat, mmap, mprotect, mmap, close, open, read, fstat

read, fstat, mmap, mprotect, mmap, close, open, read, fstat, mmap
fstat, mmap, mprotect, mmap, close, open, read, fstat, mmap, mprotect
mmap, mprotect, mmap, close, open, read, fstat, mmap, mprotect, mmap
mprotect, mmap, close, open, read, fstat, mmap, mprotect, mmap, mmap
mmap, close, open, read, fstat, mmap, mprotect, mmap, mmap, close
close, open, read, fstat, mmap, mprotect, mmap, mmap, close, mmap
open, read, fstat, mmap, mprotect, mmap, mmap, close, mmap, arch_prctl
read, fstat, mmap, mprotect, mmap, mmap, close, mmap, arch_prctl, mprotect
fstat, mmap, mprotect, mmap, mmap, close, mmap, arch_prctl, mprotect, mprotect
mmap, mprotect, mmap, mmap, close, mmap, arch_prctl, mprotect, mprotect, mprotect
mprotect, mmap, mmap, close, mmap, arch_prctl, mprotect, mprotect, mprotect, mprotect
mmap, mmap, close, mmap, arch_prctl, mprotect, mprotect, mprotect, mprotect, mprotect
mmap, close, mmap, arch_prctl, mprotect, mprotect, mprotect, mprotect, mprotect, munmap
close, mmap, arch_prctl, mprotect, mprotect, mprotect, mprotect, mprotect, munmap, brk
mmap, arch_prctl, mprotect, mprotect, mprotect, mprotect, mprotect, munmap, brk, brk
arch_prctl, mprotect, mprotect, mprotect, mprotect, mprotect, munmap, brk, brk, open
mprotect, mprotect, mprotect, mprotect, mprotect, munmap, brk, brk, open, fstat
mprotect, mprotect, mprotect, mprotect, munmap, brk, brk, open, fstat, mmap
mprotect, mprotect, mprotect, munmap, brk, brk, open, fstat, mmap, close
mprotect, mprotect, munmap, brk, brk, open, fstat, mmap, close, geteuid
mprotect, munmap, brk, brk, open, fstat, mmap, close, geteuid, open
munmap, brk, brk, open, fstat, mmap, close, geteuid, open, fstat
brk, brk, open, fstat, mmap, close, geteuid, open, fstat, read
brk, open, fstat, mmap, close, geteuid, open, fstat, read, read
open, fstat, mmap, close, geteuid, open, fstat, read, read, close
fstat, mmap, close, geteuid, open, fstat, read, read, close, open
mmap, close, geteuid, open, fstat, read, read, close, open, open
close, geteuid, open, fstat, read, read, close, open, open, open
geteuid, open, fstat, read, read, close, open, open, open, open
open, fstat, read, read, close, open, open, open, open, write
fstat, read, read, close, open, open, open, open, write, write
read, read, close, open, open, open, open, write, write, write
read, close, open, open, open, open, write, write, write, write
close, open, open, open, open, write, write, write, write, lseek
open, open, open, open, write, write, write, write, lseek, close
open, open, open, write, write, write, write, lseek, close, close
open, open, write, write, write, write, lseek, close, close, close
open, write, write, write, write, lseek, close, close, close, exit_group

n_gram_mv
execve, brk, access, open, fstat, mmap, close, open, read, fstat
brk, access, open, fstat, mmap, close, open, read, fstat, mmap
access, open, fstat, mmap, close, open, read, fstat, mmap, mmap
open, fstat, mmap, close, open, read, fstat, mmap, mmap, mprotect
fstat, mmap, close, open, read, fstat, mmap, mmap, mprotect, mmap

mmap, close, open, read, fstat, mmap, mmap, mprotect, mmap, close
close, open, read, fstat, mmap, mmap, mprotect, mmap, close, open
open, read, fstat, mmap, mmap, mprotect, mmap, close, open, read
read, fstat, mmap, mmap, mprotect, mmap, close, open, read, fstat
fstat, mmap, mmap, mprotect, mmap, close, open, read, fstat, mmap
mmap, mmap, mprotect, mmap, close, open, read, fstat, mmap, mprotect
mmap, mprotect, mmap, close, open, read, fstat, mmap, mprotect, mmap
mprotect, mmap, close, open, read, fstat, mmap, mprotect, mmap, close
mmap, close, open, read, fstat, mmap, mprotect, mmap, close, open
close, open, read, fstat, mmap, mprotect, mmap, close, open, read
open, read, fstat, mmap, mprotect, mmap, close, open, read, fstat
read, fstat, mmap, mprotect, mmap, close, open, read, fstat, mmap
fstat, mmap, mprotect, mmap, close, open, read, fstat, mmap, mprotect
mmap, mprotect, mmap, close, open, read, fstat, mmap, mprotect, mmap
mprotect, mmap, close, open, read, fstat, mmap, mprotect, mmap, mmap
mmap, close, open, read, fstat, mmap, mprotect, mmap, mmap, close
close, open, read, fstat, mmap, mprotect, mmap, mmap, close, mmap
open, read, fstat, mmap, mprotect, mmap, mmap, close, mmap, arch_prctl
read, fstat, mmap, mprotect, mmap, mmap, close, mmap, arch_prctl, mprotect
fstat, mmap, mprotect, mmap, mmap, close, mmap, arch_prctl, mprotect, mprotect
mmap, mprotect, mmap, mmap, close, mmap, arch_prctl, mprotect, mprotect, mprotect
mprotect, mmap, mmap, close, mmap, arch_prctl, mprotect, mprotect, mprotect, mprotect
mmap, mmap, close, mmap, arch_prctl, mprotect, mprotect, mprotect, mprotect, mprotect
mmap, close, mmap, arch_prctl, mprotect, mprotect, mprotect, mprotect, mprotect, munmap
close, mmap, arch_prctl, mprotect, mprotect, mprotect, mprotect, mprotect, munmap, brk
mmap, arch_prctl, mprotect, mprotect, mprotect, mprotect, mprotect, munmap, brk, brk
arch_prctl, mprotect, mprotect, mprotect, mprotect, mprotect, munmap, brk, brk, open
mprotect, mprotect, mprotect, mprotect, mprotect, munmap, brk, brk, open, fstat
mprotect, mprotect, mprotect, mprotect, munmap, brk, brk, open, fstat, mmap
mprotect, mprotect, mprotect, munmap, brk, brk, open, fstat, mmap, close
mprotect, mprotect, munmap, brk, brk, open, fstat, mmap, close, geteuid
mprotect, munmap, brk, brk, open, fstat, mmap, close, geteuid, ioctl
munmap, brk, brk, open, fstat, mmap, close, geteuid, ioctl, open
brk, brk, open, fstat, mmap, close, geteuid, ioctl, open, fstat
brk, open, fstat, mmap, close, geteuid, ioctl, open, fstat, read
open, fstat, mmap, close, geteuid, ioctl, open, fstat, read, read
fstat, mmap, close, geteuid, ioctl, open, fstat, read, read, close
mmap, close, geteuid, ioctl, open, fstat, read, read, close, open
close, geteuid, ioctl, open, fstat, read, read, close, open, open
geteuid, ioctl, open, fstat, read, read, close, open, open, open
ioctl, open, fstat, read, read, close, open, open, open, open
open, fstat, read, read, close, open, open, open, open, write
fstat, read, read, close, open, open, open, open, write, write
read, read, close, open, open, open, open, write, write, write
read, close, open, open, open, open, write, write, write, write
close, open, open, open, open, write, write, write, write, lseek
open, open, open, open, write, write, write, write, lseek, close
open, open, open, write, write, write, write, lseek, close, close

open, open, write, write, write, write, lseek, close, close, close open, write, write, write, write, lseek, close, close, close, exit_group

Gerados pelo seguinte algoritmo:

_create_gram

```
def _create_gram(n, file="log_syscall_mv_without_id.txt", arq="n_gram_mv.txt"):
    with open(file, "r") as file1, open(arq, "w") as arq1:
        data = [x[:-1] for x in file1]
        for i in range(len(data) - n + 1):
            arq1.write(str(data[i:i+n])[1:-1].replace("\'","") + "\n")

_create_gram(10, file="log_syscall_mv_without_id.txt", arq="n_gram_mv.txt")
```

Descrição: este código recebe o log com as chamadas de cada aplicação e escreve um arquivo de retorno com a paginação de tamanho 10 até a ultima chamada feita pela aplicação

OBS: para a criação dos n-grams também foram gerados arquivos de log sem o id de cada chamada, usando o seguinte código:

_create_log_without_ip

```
def _create_log_without_id(file="teste_mv.txt",arq="teste_mv_without_id.txt"):
    with open(file) as file1, open(arq, "w") as arq1:
        for line in file1:
            result = line.split("] ")[1]
            if result[1] != "+":
                arq1.write(result)

_create_log_without_id(file="teste_mv.txt", arq="teste_mv_without_id.txt")
```

Descrição: este código recebe o log gerado anteriormente contendo o ide e nome das chamadas e extrai somente o nome, para facilitar as demais operações.

(II)

Comparação dos arquivos saudável e infectado

Retorno da comparação
Infection: 20.0%

_compare

```
def _compare(healthy="n_gram_cp.txt", infected="n_gram_mv.txt"):
    with open(healthy, "r") as arq_healthy, open(infected, "r") as arq_infected:
        arq1 = [z[:-1] for z in arq_healthy]
        arq2 = [y[:-1] for y in arq_infected]
        inter = set(arq1).intersection(arq2)
        list = [x[:-1] for x in inter]


        print("Elements file1: "+str(arq1)+"\n")
        print("Elements file2: "+str(arq2)+"\n")
        print("Infection: "+str(100-(len(list) / len(arq2))*100) + "%")


_compare(healthy="n_gram_cp.txt", infected="n_gram_mv.txt")
```

Descrição: este código recebe o gram das aplicações cp e mv e faz a comparação para ver qual chamada de sistema não está presente no arquivo saudavel, essa chamada é tida como infectada, retornando taxa de infecção presente no arquivo.