Mock Semifinals 2025 Web-Based Challenge
Challenge 3: Core Dump Forensics

Description
The attached files are core dumps obtained with the “gcore” command on an Ubuntu 24.04 system. These files contain the memory of a process that was intentionally crashed. This memory is frozen in its state, so we can examine what the program was doing when it crashed. Some useful tools to analyze the coredump are “file” and “gdb”.

Coredump Information: All the coredumps were taken on the same computer. Provide the UID of the user running the programs, the name of the user, the platform (architecture) of the machine running the programs, and the current working directory (without trailing slash) that was used when running all four programs (all four programs were run in the same directory).

File 1: The file “core.773” contains the first core dump. Include the PID of the program, the full filepath to the binary that was run, the address at which program execution stopped (in decimal format), and the value in the `rsi` register at the time of the program crash (in decimal format).

File 2: The file “core.989” contains the second core dump. Include the PID of the program, the full filepath to the binary that was run, the address at which program execution stopped (in decimal format), and the number of seconds the program would have run for, if it was not stopped early.

File 3: The file “core.1093” contains the third core dump. Include the PID of the program, the full filepath to the binary that was run, the address at which program execution stopped (in decimal format), and the memory value (as a decimal 64-bit integer, which was stored in memory as little-endian), located at the memory address 0x55ee05d85d30.

File 4: The file “core.1240” contains the third core dump. Include the PID of the program, the full filepath to the binary that was run, the address at which program execution stopped (in decimal format), and the user that tried to log into this machine while the program was running

(continued on next page)

Submission Instructions

You must submit your answer as a .csv file, in the following format:

- ☐ The first line of the submission should contain your team number.
- ☐ The second line should contain the requested coredump information.
- ☐ The third line should contain the information about File 1.
- ☐ The fourth line should contain the information about File 2.
- ☐ The fifth line should contain the information about File 3.
- ☐ The sixth line should contain the information about File 4.

In each line, separate your answers with a comma, with no space in between each answer. Refer to the below example for formatting help. The first line should have 4 pieces of information. The last four lines should have 4 pieces of information each.

Each field is weighted equally in scoring. You will get points for each ciphertext you get correct. You will get 10 tries to submit before you will not be able to submit anymore.

Example Submission

```
16-2250
1001,ctf,aarch64,/home/ctf
332,/usr/bin/cat,139718791150964,139715627925898
122,/usr/bin/bash,139719468146609,442
543,/usr/bin/sh,139719243812941,3439848561820441660
1233,/usr/bin/kill,139719270150645,priyam
```