Assignment 4: RAM

Digital Forensics

Assignment 4: RAM

At last - the final assignment! Somehow you can’t hide your excitement that this semester is soon ending …

Your first task is to demonstrate your overall forensic capabilities and acquire a RAM dump of an operating system of your choosing!

Assignment 4: RAM

You can choose your target and acquisition method freely:

- on Windows you could use e.g. WinPMem
- on Linux you could use e.g. LiME
- you may also use a virtual machine
- If you have an ARM-based Mac, please use e.g. a Raspberry Pi or your favourite cloud provider …

Please note: include a very specific and unique artefact that makes your skills verifyable, such as a specific running process or a specific open network connection!

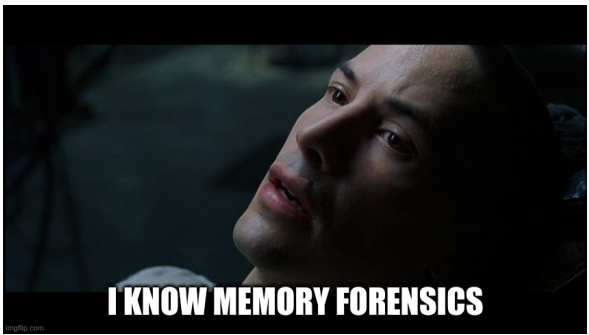
Assignment 4: RAM

Your second task is to analyze the just acquired RAM dump using volatility:

- list all the running processes
- list all the network connections
- make sure to not *list*, but *scan* too & discuss the differences
- verify that you also find your previously included unique artefact

Assignment 4: RAM

You tweeted/tooted that you now know memory forensics.
Then things got weird …



Assignment 4: RAM

Someone sent you a RAM dump to challenge your skills:

- download the RAM dump from here
- SHA-256 of physmem.raw:
  fee4a87527509ed8a67c51a2b3-
  e21a74ae52739e0d69020312180339cfd79e3b
- and answer the questions on the next slide

Assignment 4: RAM

Questions:

- What information can you extract about the operating system?
- What happened at the time of the RAM dump:
  - e.g., date, time, ...
  - running processes, network connections, ...
  - are all the browsers the same?
- what is the user SID?
- can you find/crack the user password (and get a hint who sent you the RAM dump)?

Assignment 4: RAM

Recommended tools:

- Volatility 3 2.5.0

Target group: medium management!

- Report has to be comprehensible and pleasant.

Assignment 4: RAM

Deadline: Jan 17th 2024, 23:55

- solve alone!
- submission:
  - report as pdf, including answers to all questions
  - if you have written code upload a ZIP file including the report.
- Submit in TUWEL prior to the deadline

Maximum points: 12

- 10 for questions, 2 for report form