TODO

- Analyze disk image from the workstation of possible ransomware author
- Help your CSIRT team (and victims) by identifying the encryption keys and algorithms used by ransomware
- Gather evidence about suspect + Log + Chain of custody
  - Extra bonus points
  - Hint: `apt-get install sqlite3`
- Remember - You are now part of law enforcement, so behave accordingly! You can consult with your "supervisor" via organisations slack. :P

fca5051aad2da02d642e59b0bcb247a3fe8a75a9e6412cf8b3441d52737ba42c lab4.zip