TODO

1. Prepare evidence USB stick
   a. Download raw image, unzip and verify it’s signature
      ~~https://jan.skalny.sk/fiit/forensics/disk.img.zip~~ (from AIS or slack)
      password: `infected`
      hash: `b5d0de0ac00ae3e35c0b39a16c3b730162d193d120b9908b9de7b05eecaa0a5c`
      hash: `c350a294b5c29acea1371542f873c0ced74ceebc8dd2083808bd9aa68c3ae6c3`
   b. What hash algo was used?
   c. Flash image file to you USB stick using `dd` command
2. Using SIFT workstation, perform USB stick analysis
3. Acquire EWF image(s), document process and results
4. Analyze and verify EWF images using `ewfinfo` and `ewfverify`
5. Mount EWF image and inspect it’s content
6. Analyze partition table and it’s contents. Identify partitions, file systems, sizes...
7. Using mount, analyze contents of first partition
8. Compute hashes of all files, document sizes, timestamps, etc.
9. …
10. Bonus: Found anything suspicious on the disk?