CFRS 772: Forensic Artifact Extraction
Homework Project 5

Homework

Edit the setupapi_parser.**v2**.py code from the text book to parse the Windows setupapi.app.log file (example on BlackBoard). Output a list of the commands that were run (just the part after "CMD:", not the dates or any other info). Optional: output a de-duplicated list of commands.

On BlackBoard, submit (1) a PDF file with your output against the provided file, and (2) your Python code (the modified setupapi_parser.v2.py code); name your program hw5_yourname.py.