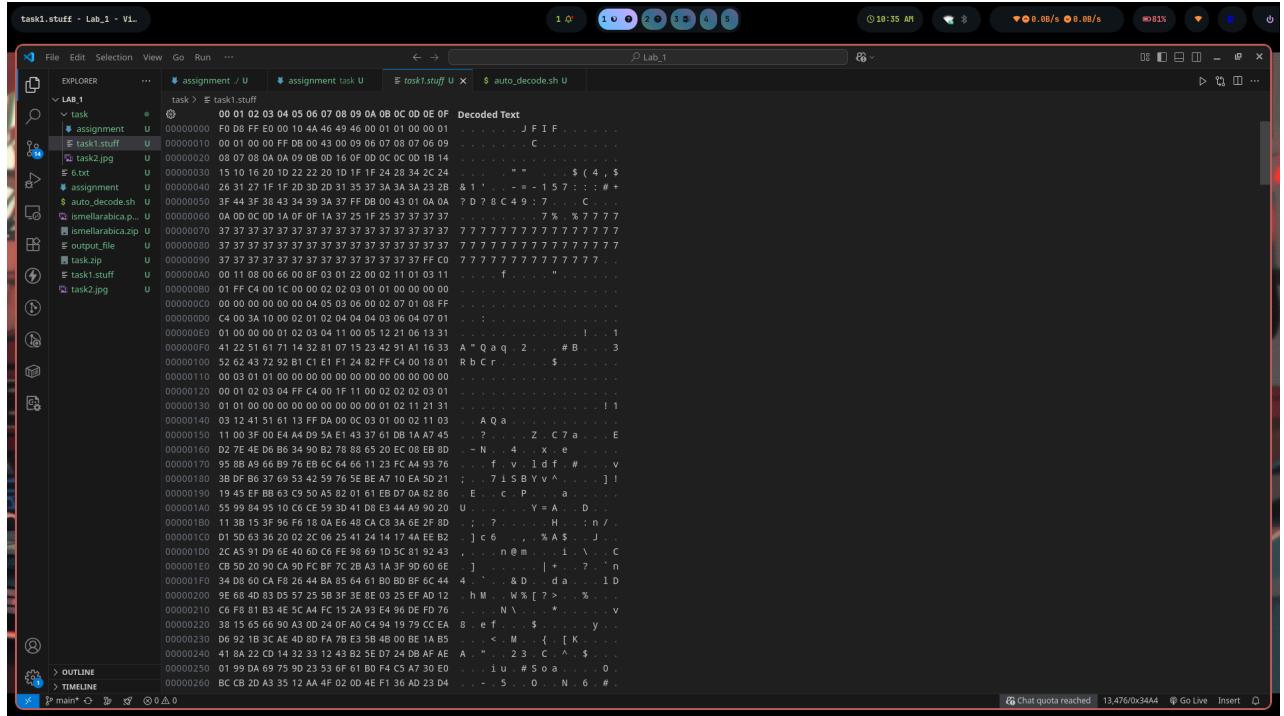


Digital Forensics Lab Report – Practical 1

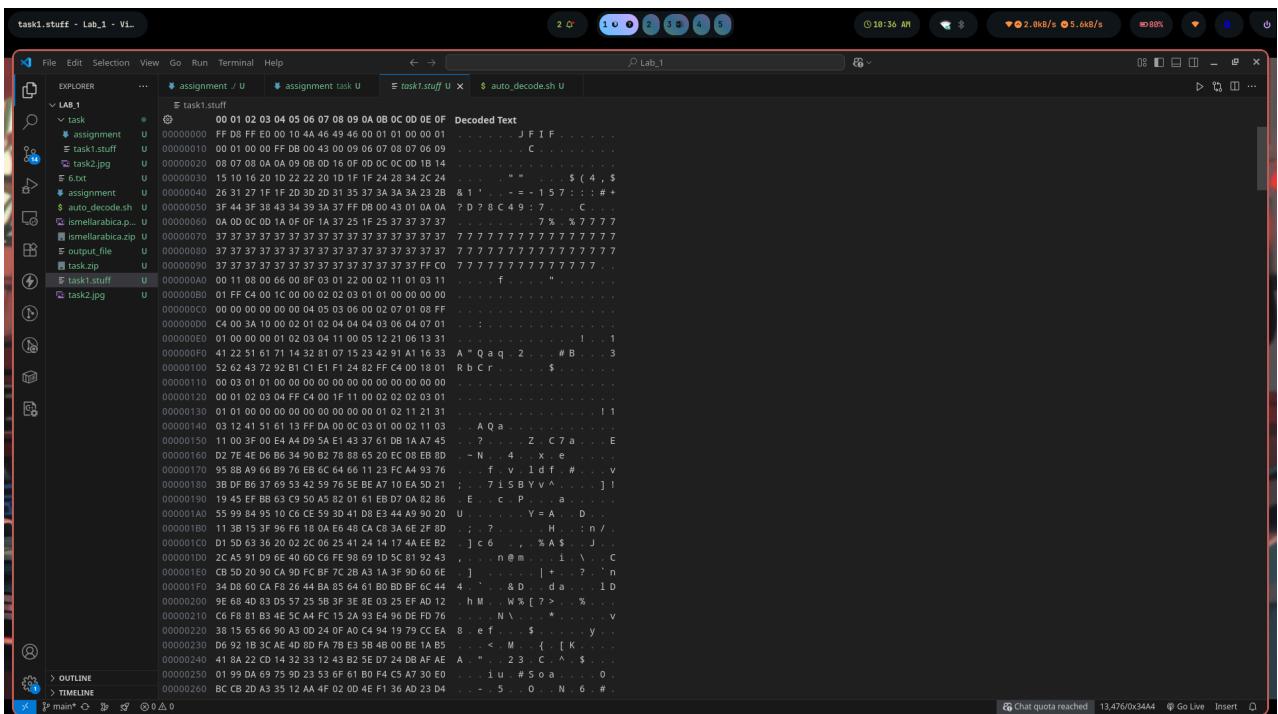
Using Hex Editors to Uncover Forensic Evidence

Task 1: Identifying and Recovering a File with Hidden Format

1. The given .stuff file was opened using a hex editor.



2. The first byte was observed to be incorrectly set to F0, which is not a valid header for known file formats. It was manually corrected to FF, resulting in a valid JPEG header (FF D8).

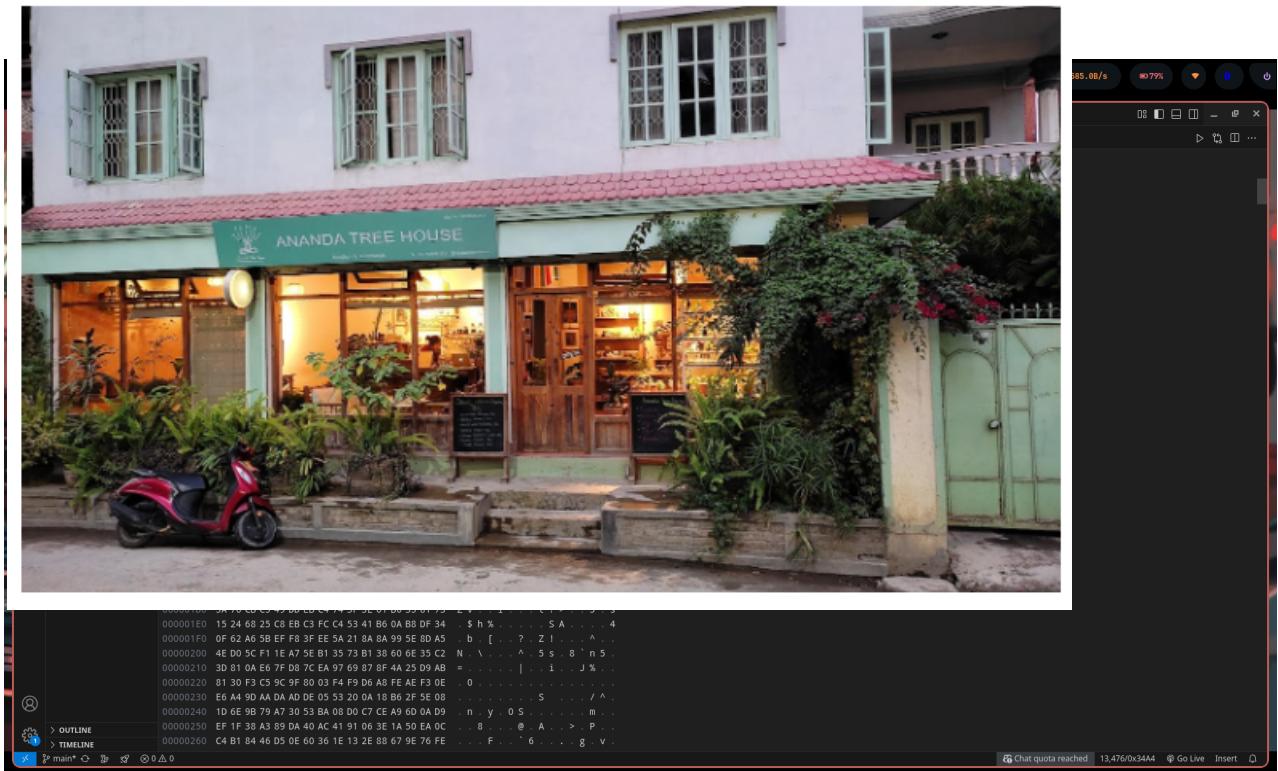


3. After saving the change, the file was opened in an image viewer and successfully rendered, confirming it as a valid JPEG image.



Task 2: Extracting and Decoding Hidden Data

1. The second file was opened in a hex editor to inspect any hidden or appended data.
2. Upon examining the hex content, a URL was discovered embedded within the file.
<https://drive.google.com/file/d/1wEc1XWktXkoLUloysMxVgoJitc1w6E5P/view>



3. The linked image was downloaded and its extension changed to .zip. After extracting, a .txt file containing an encoded string was found.

Vm0wd2VFNUdiRmRpUm1oVF ltdHdUMVp0TVc5V1JteFZVMjA1VjFadGVEQmFWVll3VmpB
eFdHVkljRmhoTweweFZtdFZlRll4WkhGUmJVWlhWbXhzTTFaclVrZFpWMUpIVm01V2FsSnR
hRzlVVm1oRFqRlpI RmRzV214U2JIQjVWR3hhWVdGV1NuTlhemxYWWxoU00xVXhXbXRXT
VhCSIk wZDRVMDFFUIRCV2Fra3hVekpLUjFOdVRsaGlSMmhXVm10V1MxUkdjRlpYYlhScVl
rZFNlbFl5Y3pGV01WcEhWMnBhVjJFeVVUQldha1poVTBaS2NWZHNaR2xoZWxab1YxZDBZ
Vlp0VWhoalJtaHNvakJhVkZadGRIZGxiRnBJWIvkR2FGSXhXbnBXTW5SdlZqRktSbGRzYUZka
GExcG9WV3HZDFKdFNrZFRiV3hUVmxoQ2RsWnRNWGRVTWtsNVZteGthbEpXV2xSWmE
xVXhWa1pzY2xkcmRHeFdiRlkxV1ROd1YxWnJNvmRqUldoWFRXNW9hRlp xUmtwbGJGWjF
WMjFHVTFKV2NGUlhiRnBoVXpKU1YxVnVUbFZpVjJod1ZXeG9RMWRHV25KWGHJUmF
WbXN4TkZWc2FHOVdiVXB5VGx ab1YyRXhXbWhXVlZwelkyeGFWVkpzWkdsU2JHOTNWMV
JPZDFZeFdYZE5WbHBxVW0xU1dGbHNhRU5XUmxwMFpVZE dVMkpWTlVwVmJYaFhWR3h
hZFZGclZsZG!SMUV3VlZSR1lWWnJNvlpXYXpWVFVrVkZOUT09

4. The encoded string was identified as Base64 and was decoded iteratively using a script. Each decoded output was examined until a meaningful result was obtained.

5. The final decoded content revealed location coordinates, possibly hinting at a real-world location or next clue in the forensic investigation.

