# Information about Forensics Projects

## Project # 1

## Computer Forensics Essentials

Project - Part A (Live Acquisition of Volatile Data (Memory Dump) & Analysis)

1. Explain Volatile Data and provide order of volatility from most to least volatile.
2. Capture the RAM of your own Live Running System using any available forensic tool preferably command line.
3. While capturing try to have network connections, open browsing pages like google classroom or open social media accounts so that you can have maximum data.
4. Analyze the captured image of RAM using any open-source tool e.g. Bulk Extractor
5. Explain each step in detail with screenshots.

Project - Part B: Dead Acquisition of Non-Volatile Data

#### Situations:

#### i. where you can remove the hard drive,

#### ii. where you're not allowed to remove the hard drive

1. What are the necessary steps that must be followed before creating forensic images of source devices?
2. Create forensic images of any source device e.g. disk/USB/SD cards etc. with title of your name using FTK or any other validated forensic tool (Situation-i).
3. Explain how you can create live bootable USB using Paladin ISO file and state the main features of using Paladin (Situation-ii).
4. Create forensic image of any source device of disk/USB/SD cards etc. with title of your name using the prepared live bootable Paladin forensic tool (situation-i).
5. Explain each step in detail with screenshots for both situations.

Project - Part C: Analysis of Dead Acquisition of a Disk Forensic Image.

#### Fictional Mass Shooting Case Scenario

1. Analyze the provided forensic image of a disk drive of a laptop.
2. Use FTK/Autopsy for extracting the windows registry hives and use Reg Ripper for ripping and analyzing the hives.
3. You can also use autopsy for the analysis.
4. Find out the artifacts associated/linked to the crime activities that were planned.
5. Explain each artifact with associated hives in detail (time & date) with screenshots.
6. Write down your findings of analysis in the form of a report (report sample was provided in previous class lectures).
7. Attach the evidence copies if available/found.

## Project # 2

## Operating System Forensics

### Project: Data Recovery (Manual Method Through Header and Footer)

1. Take any USB or other low storage device as convenient, format it, copy and paste two .jpg and .png files on it, and then delete them.
2. Create dd Image of USB using Linux command line instructions in your VM (instruction file is attached)
3. Each student should create a dd image of his/her own name as an image file name. (e.g. Ali.dd)
4. Give details of each step and calculations.
5. Prepare your data recovered in written file.

## Project # 3

## Advance Forensics

### Case Forensic Project: Report Submission for Active Directory Forensics-Case Study

1. The report must be based on the timeline of a real incident and artifacts from the pre-extracted NTDS.DIT files of the Active Directory.

### Project: Create Artifacts and Set Log files for Cloud Storage Services i.e. Google Drive

1. Look for the following artifacts and record them in the form of a written document along with screenshots.
2. Artifacts created during the installation process
3. Information present in the database files
4. Artifacts created when a file is uploaded or downloaded
5. Artifacts left when a file is shared
6. Artifacts left after using anti-forensics tool
7. Logs recorded and their accuracy
8. Artifacts left behind after the uninstallation process
9. Other sources of information

## Project # 4

## Mobile Forensics

### Project: Perform Logical Data Acquisition from Android Devices using Android Debug Bridge (ADB) OR iOS Devices using Finder/iTunes

1. Mentioned device model/version
2. Document each step with written demonstration and screenshots
3. After acquiring data/backup file, I used methods or tools to extract data from these files.
4. Similar screenshots or assignment files will be marked as zero.