Digital Forensics Hands-on #3

This project consists of two parts.

Part #1: Windows registry analysis

You are provided with a forensically collected copy of a Windows 10 registry named "**Win10Reg.7z**".

Your task is to use any tool or technique discussed in class to find the following information:

- How many users and groups are associated with this system according to the Security Accounts Manager?
- What are the names of the users associated with this registry?
- When did the user aubie last log in to the system?
- What applications are automatically started when the user logs into the system and when was the last time the autostart was run?
- What was the private IP address associated with the system?
- What are the most recently executed commands from the Windows Run command window?

You need to provide detailed report including the commands you ran along with annotated screenshots of the output. You need to discuss and justify your answers.

Part #2: Network Forensics

An FTP server was employed to store and share sensitive employee data within your organization. An authorized employee was assigned to log in and download a file containing employee details. Unfortunately, this file was later leaked, leading to suspicious activity being detected on the FTP server. Multiple unauthorized login attempts were recorded from various IP addresses, with these users trying to download or upload files to the server.

You are give a captured traffic from the server name **FTPPackets.pcap** and tasked to perform forensic analysis of the incident, identify the employees involved, and recover all relevant details and files related to these unauthorized activities.

Authorized Login and Download

- Identify the authorized employee who logged in initially and provide their ftp_username.
- Provide login timestamp, MAC and IP address of the user, and the name of file downloaded (employee details file).
- Recover the file and provide the file's size (in bytes), SHA-256 hash, and MD5 hash of the file.

Step 2: Detect Unauthorized Access

- Analyze the server logs for all subsequent logins and identify:
    - All the users who logged in (by username).
    - The IP addresses they used.
    - The timestamps (actual times in DD-MM-YYYY HH:MM:SS format) of their login activities.

Step 3: Analyze Uploaded and Downloaded Files

- For each login, determine:
    - Whether the files were downloaded or uploaded.
    - Each file's name, size and hash value to confirm if files were modified.
    - Recover all the files that were downloaded and uploaded.

Provide a summary of your findings in a table format with the following columns:

Username	**IP Address**	**MAC address**	**Login Time (DD-MM-YYYY HH:MM:SS)**	**Action (Download/Upload)**	**File name + extension**	**File size (bytes)**	**File hash**

You need to provide detailed report including annotated screenshots supporting your findings.

You need to provide a copy of all received files that were part of the activities on the server.

Final report and submission

- Submit your final report in PDF format for both parts into one report with all the required details and justification. Note that a single-page report will not adequately show your work so be prepared to have an in-depth analysis and description of the methods you used to work on this project.
- The actual recovered files.

Grading Rubric

Activity	**%**	**Points**
Windows Registry Analysis	30%	60
Accounts Overview - Users & Groups ▪ Count of all users and groups clearly stated (8 points) ▪ Names of all users listed and supported by evidence and explanation (8 points)		16
Last logon for "Aubie" ▪ Correct timestamp identified with evidence (8 points) ▪ Methodology and tool output shown (4 points)		12
Autostart Entries & Last Run Time ▪ Applications started at runtime clearly listed with evidence (8 points)		12

▪ Correct timestamp of last autostart time with evidence (4 points)		
Private IP Address ▪ Correct private IP addresses shown (5 points) ▪ Evidence included with answer (5 points)		10
Windows "Run" MRU Entries ▪ Most recently executed commands listed (5 points) ▪ Evidence provided with answer (5 points)		10
Network Forensics	70%	140
Authorized Login & Initial Download ▪ Identify Authorized Employee (10 points) ▪ Login timestamp, MAC, IP, and downloaded file name (15 points) ▪ Recovered file attached, with correct file size and SHA-256/MD5 hash (15 points)		40
Unauthorized Access Enumeration ▪ List ALL logins with usernames, IPs, and timestamps		30
File Activity & Integrity per logon ▪ Correctly identify actions (upload/download) and filenames (10 points) ▪ Provide file size (bytes) and SHA-256 hash, and analyze files (10 points)		20
Recovery of ALL transferred files		30
Timeline Table included		20

Some Global Deductions:

(-20) More than one report submitted (You should submit 1 report for this entire assignment)

(-10) Report is not in PDF format

(-10) Report is submitted within a zip file.

(-30) No annotated screenshots. PER section.

(-20) Missing Table in Executive Summary with Questions Asked and Answers

Example of Table in Executive Summary:

How many users and groups are associated with this system according to the Security Accounts Manager?	ANSWER GOES HERE (No explanation needed for the table)
…	….