**Digital Forensics Lab-Tasks**



**Prepared By: Ms.Memoona Sadaf**

**Instructor: Ms.Memoona Sadaf**

**Lab/Teaching Assistant: Muhammad Ahmad Ali Qureshi**

**Air University Islamabad**

**Lab Task 07**

**Total Marks: 10 CLO-03**

**Download the Memory Image File form the following link and answer following questions.**

<https://drive.google.com/file/d/11XJF1onelpieHwD0NJnyPTsJ5aurlnxx/view>

**Tasks**

**1.What is the first suggested profile to use on this memory image?**

Use Command: *python vol.py -f "../Exercise 6 (1)..raw" imageinfo*

**2.What folder was copied and contained within the system’s clipboard?**

Use Command: *python vol.py -f "../Exercise 6 (1)..raw" --profile=Win7SP1x64 clipboard*

**3.What directories were explored from the command prompt?**

Use Command: *python vol.py -f “../Exercise 6 (1)..raw" --profile=Win7SP1x64 consoles*

**4.Was TrueCrypt running at the time of memory acquisition?**

Use Command: *python vol.py -f "../Exercise 6 (1)..raw" --profile=Win7SP1x64 pslist | grep -i truecrypt*

*Or*

Use Command: *python vol.py -f "../Exercise 6 (1)..raw" --profile=Win7SP1x64 psscan | grep -i truecrypt*

**5.If so, what was the process ID?**

Use Command: *Look in the output from the previous commands (pslist or psscan)*

**6.How many times had TrueCrypt been executed?**

Use Command: *python vol.py -f "../Exercise 6 (1)..raw" --profile=Win7SP1x64 psscan | grep -i truecrypt*

**7.What was the parent process associated with notepad.exe?**

Use Command for Parent PID: *python vol.py -f "../Exercise 6 (1)..raw" --profile=Win7SP1x64 pslist | grep -i notepad*

Use Command to find that PID in pslist *: python vol.py -f "../Exercise 6 (1)..raw" --profile=Win7SP1x64 pslist*

**8.How many dll files are associated with Notepad.exe?**

Use Command: *python vol.py -f "../Exercise 6 (1)..raw" --profile=Win7SP1x64 dlllist -p <PID> | grep 'Base' | wc -l*

**9.What is the Local IP address and Foreign IP address associated with the first ESTABLISHED chrome.exe connection?**

Use Command: *python vol.py -f "../Exercise 6 (1)..raw" --profile=Win7SP1x64 netscan | grep -i chrome*

**Note:** Provide a proper report with Screenshots and Marks will based on the Viva XD.