Digital Forensics Workshop (CSE3156)

Assignment on Volatility

Computer Science Department, SOA University

Dr. Rourab Paul

Download Sample Files

- Sample Memory Dump Files
- The above link has many sample files. You can select 'Malware - R2D2 (pw: infected)' for your first investigation.
- Before downloading any memory dump files of infected RAM, it is required to verify the hash. Hash assures that source file is not altered. Altered memory dump file may infect your device
- Please check the sha1sum of the file: which must be

  $ sha1sum 0zapftis.vmem

  It should be :

  e4d4f4d1c304919ed51e17593a56d24b37c5acd9 0zapftis.vmem

  Detail Report of 0zapftis.vmem

Extract Sample Files

List inside the rar Remember that the password to view or extract the contents is infected.

unrar l 0zapftis.rar.

Now, we can extract the 0zaoftis.vmem file by typing in

unrar e -r 0zapftis.rar

Extract specific column from a given filename in python


```
def extract_pids_from_file(filename, column_no):
    pids = []
    try:
        with open(filename, 'r') as file:
            for line in file:
                columns = line.split()  # Split the line by whitespace (spaces/tabs)
                if len(columns) >= 1:  # Ensure there are at least 1 columns
                    pid = columns[column_no]  # The 0th column is the PID (index 0)
                    pids.append(pid)
    except FileNotFoundError:
        print(f"Error: The file {filename} was not found.")
    except Exception as e:
        print(f"An error occurred: {e}")
    return pids
```