**Capture the Flag (CTF)**

Challenge on Cloud Forensics • Challenge 1

**Index**

**Assumptions/Needs** 3

**Objective** 3

**Problem** 3

**Question 1** 4

**Question 2** 5

**Question 3** 7

**Objective**

The basis of this challenge will be that the user will be viewing timestamps using **FTK Imager** and **debugfs**. The user will also transfer files using **“pscp”** and use debugfs to see file timestamps on an Ubuntu Linux Machine.

**Problem**

This CTF challenge is replicating a scenario in which a malicious attacker has remotely modified private and publicly stored files on the user’s machine.

**Assumptions/Needs**

* Hyper-V and/or VirtualBox software for virtual machines
* Microsoft OneDrive free account (https://onedrive.live.com/about/en-us/)
* Windows and Ubuntu Linux machine
* FTK Imager software (<http://marketing.accessdata.com/ftkimager3.4.2>) and debugfs enabled in Linux.

**Question 1**

Was the modify-time unchanged? Or was it updated? Please upload a screenshot.

**Question 2**

Was the **entry-modify** time unchanged? Or was it updated? Please upload a screenshot.

**Question 3**

What are the new timestamps for the newly transferred file? Did they remain unchanged or stay the same. Please upload a screenshot.