**Capture the Flag (CTF)**

Challenge on Cloud Forensics • Challenge 2

**Index**

**Assumptions/Needs** 4

**Objective** 4

**Problem** 4

**Question 1** 5

**Question 2** 7

**Question 3** 9

**Objective**

The basis of this challenge will be that the user will be viewing timestamps using FTK Imager and debugfs in Windows and Ubuntu Linux environments over the public cloud software OneDrive.

**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**

What timestamps were missing after a file was uploaded to OneDrive? Which timestamp times stayed the same (did not change from the baseline)? Please upload a screenshot.

**Question 2**

Which timestamp times stayed the same (did not change from the baseline)? 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.