**Capture the Flag (CTF)**

Challenge on Cloud Forensics • Challenge 3

**Index**

**Assumptions/Needs** 4

**Objective** 4

**Problem** 4

**Question 1** 5

**Question 2** 6

**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 be conducting more advanced file operations than in previous challenges.

**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**

* VirtualBox software for virtual machines
* Windows and Ubuntu Linux machine
* FTK Imager software (http://marketing.accessdata.com/ftkimager3.4.2), debugfs enabled in Linux, and pcsp enabled in Windows.
* Free Google Drive account

**Question 1**

When a file is copied in Windows NTFS and Ubuntu, are the timestamps of the original file changed? Which (if any) of the newly created file’s timestamps have the same values as the original file (on both systems)?

**Question 2**

When a file is uploaded to a public cloud (Use Google Drive) from Windows and Linux, what timestamps of the ORIGINAL file are changed (Check ALL timestamps)?

**Question 3**

After compressing a file in Windows (.zip or .7z) and Linux (.tar), what timestamps of the ORIGINAL file are changed?