**Capture the Flag (CTF)**

Challenge on Cloud Forensics • Instructor • 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**

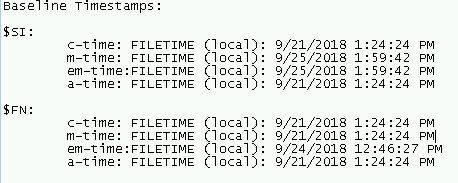
What timestamps were missing after a file was uploaded to OneDrive? Which timestamp times stayed the same (did not change from the baseline)? Please upload a screenshot.

**Description**

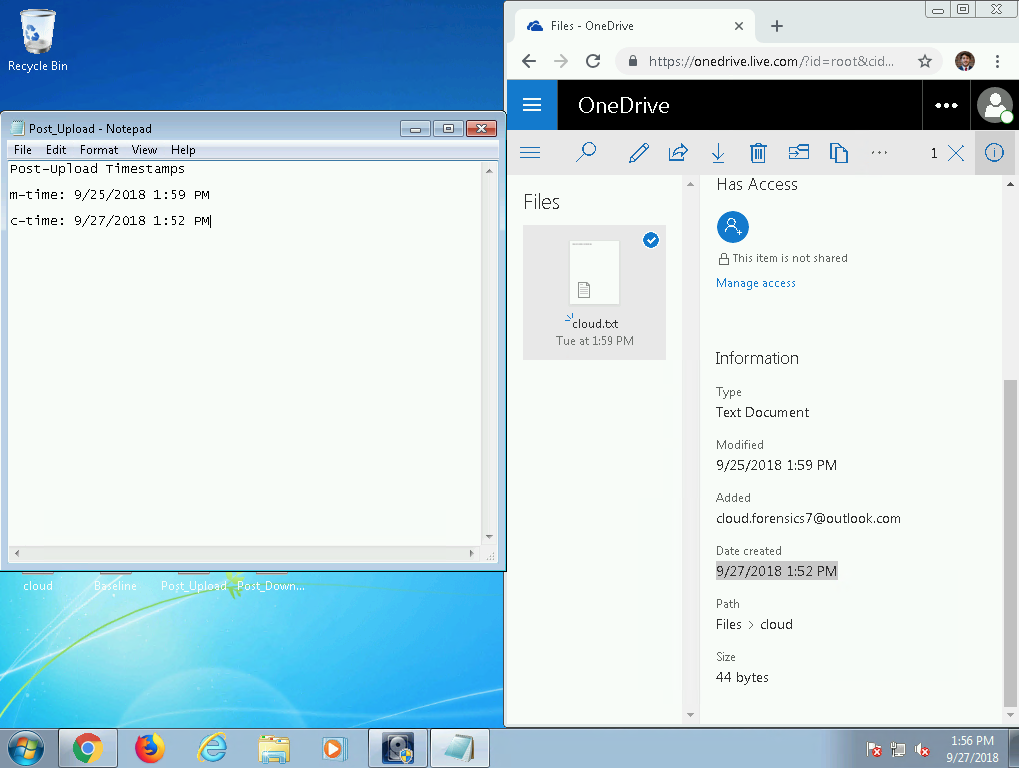
The first stage will have the user collect baseline timestamps for a file in Windows using FTK, then they will upload the file to the public cloud software OneDrive. After this, the user will compare the timestamps to see any changes/anomalies.

**Evidence**

This is an example of pre-upload baseline timestamps for a file.



The participant should provide a screenshot similar to this to complete the challenge. Here it can be seen that indeed there are only two timestamps (no a-time or em-time) and that the **modify-time** in OneDrive did not change from the baseline Windows $SI timestamp for m-time.



**Analysis**

The participant will show that when a file is uploaded to OneDrive, OneDrive keeps the same modify time for the file according to the file’s metadata.

**Expected Answer**

The participant should answer the question/challenge by stating that a-time and em-time were missing from OneDrive (i.e. there were only 2 timestamps available) and that the m-time did NOT change. The participant should upload a screenshot of the times.

**Question 2**

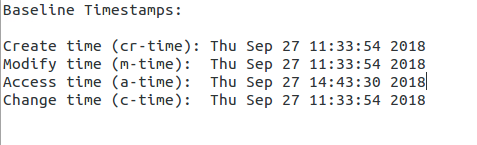
Which timestamp times stayed the same (did not change from the baseline)? Please upload a screenshot.

**Description**

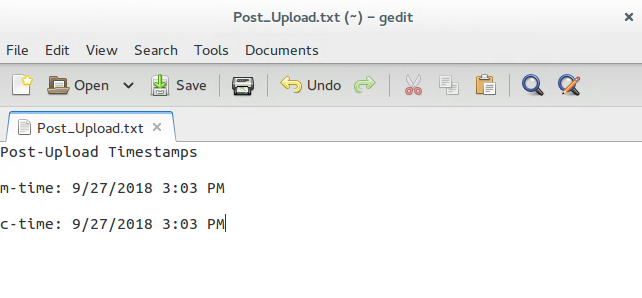
The second stage will have the user collect baseline timestamps for a file in the Linux machine using debugfs, then they will upload the file to the public cloud software OneDrive. After this, the user will compare the timestamps to see any changes/anomalies.

**Evidence**

This is an example of collected baseline timestamps for a file in the Ubuntu Linux machine.



The user/participant should then upload the file to a OneDrive account and notice and collect the modify and create times for the uploaded file.



After this is done, the participant should conclude that unlike in the Windows machine, the modify time for the uploaded file changes and is updated in the Linux machine.

**Analysis**

The participant will show that when a file is uploaded to OneDrive on Ubuntu Linux, OneDrive updates the modify time for the file to the time the file was uploaded.

**Expected Answer:**

The participant should answer the question/challenge by stating that both the OneDrive modify and create times changed and were updated with new times.

**Question 3**

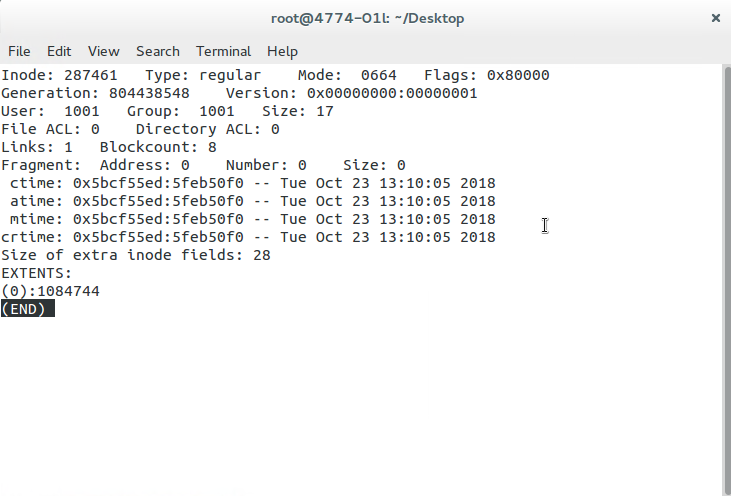
What are the new timestamps for the newly transferred file? Did they remain unchanged or stay the same. Please upload a screenshot.

**Description**

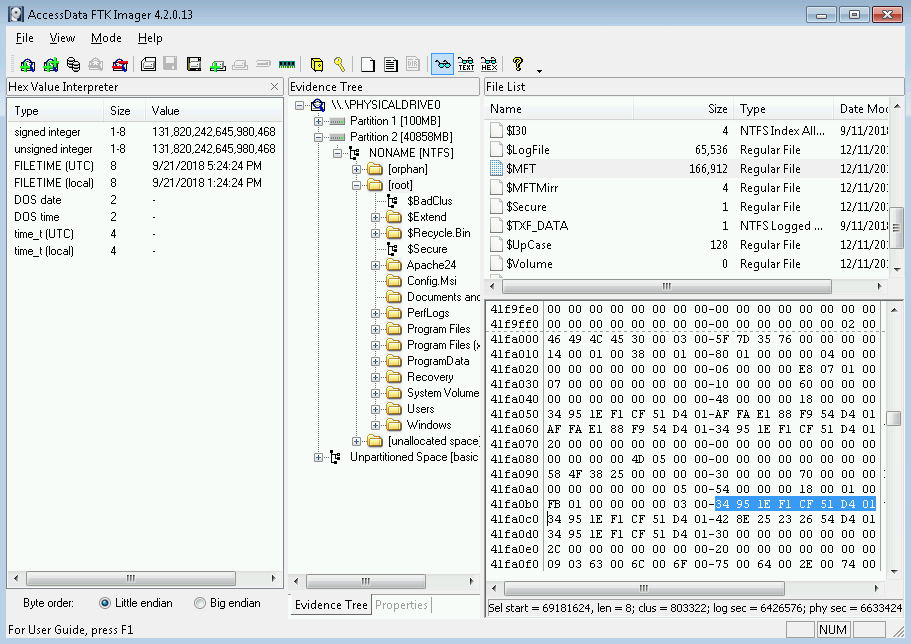
The last stage will be the user downloading the file back to their machine on both Windows and Linux. They will then use FTK and debugfs to find the file’s timestamps and identify any patterns in the timestamps.

**Evidence**

The user will use debugfs to find/view the timestamps of the newly downloaded file from OneDrive. Here is an example screenshot showing the timestamps.



The user will then use FTK to find the timestamps for the downloaded file from OneDrive. Here is an example screenshot of the Windows $SI timestamps.



The participant/user needs to have found the timestamps for the file in both filesystems to complete the challenge.

**Analysis**

Having found all timestamps and provided screenshots for submission of the challenge, the user should be able to conclude and answer the question (that the timestamps in both filesystems were completely updated).