**Capture the Flag (CTF)**

Challenge on Cloud Forensics • Instructor • 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)?

**Description**

The participant will create a .txt file on both filesystems and then create a copy of this file inside of the same directory. They will use FTK Imager and debugfs to observe and record baseline timestamps of the original file, then after creating a copy, they will observe and record the newly created file’s timestamps and then provide their conclusion to complete the challenge.

**Evidence**

The participant will submit a minimum of 4 screenshots. 2 screenshots (1 for each set of baseline timestamps per filesystem) and 2 screenshots (1 for each set of timestamps for the file copy).

**Analysis**

After successfully recording the timestamps, it will be clear to the participant what the correct answer to this challenge will be.

**Expected Answer**

On Windows NTFS and Ubuntu, after a file is copied the timestamps of the original file DO NOT change. In Windows NTFS the newly created file has the same timestamps as the original. In Ubuntu the newly created file has NONE of the same timestamps as the original.

**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)?

**Description**

The participant will create a .txt file on both filesystems and then upload the file to a public cloud service (Google Drive). They will then use FTK Imager and debugfs to observe and record ALL file timestamps on both filesystems and then provide their conclusion to complete the challenge.

**Evidence**

The participant will submit a minimum of 2 screenshots of their recorded timestamps for the original file on both filesystems. These screenshots should reflect their answer to the question.

**Analysis**

After recording the timestamps, the participant will see that nearly all of the timestamps of the original file (post-upload) will remain unchanged.

**Expected Answer:**

When a file is uploaded to the public cloud from a Windows machine ALL timestamps of the original file remain the same EXCEPT for modify time in $STANDARD\_INFORMATION inside of the $MFT. For Linux, ALL timestamps of the original file remain the same EXCEPT for create time (cr-time) in which there is no change.

**Question 3**

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

**Description**

The participant will create a .txt file on both filesystems and then compress the file (.zip and .7z on Windows and .tar on Linux). They will then use FTK Imager and debugfs to observe and record the file timestamps on both filesystems for the original file and then provide their conclusion to complete the challenge.

**Evidence**

The participant will submit a minimum of 2 screenshots of their recorded timestamps for the original file on both filesystems.

**Analysis**

After recording the timestamps, the participant will see on Windows that they are all completely new and represent the newly created compressed file. On Linux, the participant will see that only c-time and cr-time were modified.

**Expected Answer:**

When a file is compressed using both compression algorithms on Windows, ALL timestamps are changed. When a file is compressed on Linux, only the change time (c-time) and the create time (cr-time) of the original file will be changed.