Digital Forensics Exercises

Maximilian Heim

December 8, 2023

Contents

1 Exercise 1.1

1.1 Useful links

Time for Truth: Forensic Analysis of NTFS Timestamps - `https://eprints.cs.univie.ac.at/7091/`

1.2 a) Which timestamps do Linux and Windows provide?

Linux

1. atime - Acess time
2. mtime - Modification time
3. ctime - Creation time

Windows `https://eprints.cs.univie.ac.at/7091/1/3465481.3470016.pdf`

1. Modified - Modification time
2. Accessed - Access time
3. Changed - Change of file metadata via the MFT entry
4. Birth - Creation of file va the MFT entry

2 Exercise 1.3: Read only

Exercise description Ein USB-Stick und ein virtuelles Laufwerk sollen beim Anschließen an einen Rechner nicht vollständig gemountet werden, sondern im „nur-lesen“ Modus eingebunden werden. Beschreiben Sie die notwendigen Konfigurationen und erstellen Sie jeweils ein Script um den Vorgang zu automatisieren.

2.1 a)

To mount a block device read in read only mode `mount -o ro <drive> /mnt` may be used

2.2 b)

First automount has to be disabled via `mountvol.exe /N`. After that the media can be connected to the system. The next step is to enable the read only flag for the volume via `attributes volume set readonly`. Then the volume may be mounted. `https://superuser.com/questions/213005/how-to-mount-an-ntfs-partition-read-only-i`

References