Digital Forensics Exercises

Maximilian Heim

December 10, 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`

3 Exercise 2.1: Forensic backup

Exercise description Erstellen Sie ein mit dem Tool dd [Howto] ein 50MB großes virtuelles Laufwerk und formatieren Sie diese mit FAT. Verwenden Sie hierfür das Tool mkfs [Howto]. Binden Sie das Laufwerk ein und kopieren Sie anschließend verschiedene, beliebige Dateien auf die Partition. Erstellen Sie eine forensische Kopie der Partition - verwenden Sie hierfür das Programm dcfldd [Website][Howto]. Beachten Sie dabei, dass das Laufwerk nicht eingebunden sein darf. Der MD5-Hash-Wert der Kopie soll dabei in eine Datei geschrieben werden. Beschreiben Sie Ihr Vorgehen und die verwendeten Befehle. Wie sieht der Befehl aus, wenn Sie das Image in 10 MB große Dateien aufsplitten?

Backup partition as image The following command dumps the partition into an image file and saves the hash into a file

```
dcfldd if=imagetest.img of=imagedump.img hashlog=imagedumphash.md5 hash=md5
```

Backup partition splitted This command additionally splits the contents into 10 MB files

```
dcfldd if=imagetest.img split=10000000 of=imagedump.img hashlog=imagedumphash.md5 hash=
```

4 Exercise 2.2: Hash validation

Exercise Validieren Sie den Hash-Wert aus Übung 2.1, indem Sie einen Hashwert des virtuellen Laufwerkes mit dem Programm md5sum erzeugen. Führen Sie anschließend einen automatisierten Vergleich der beiden Hash-Werte durch. Beschreiben Sie Ihr Vorgehen und die verwendeten Befehle.

Generation of hash md5sum imagetest.img ¿ original.md5

Comparison of hashes cmp -n 32 –ignore-initial 0:14 original.md5 imagedumphash.md5

References