The Sleuth Kit

(TSK)

Du hast ein Festplattenabbild.

Du hast ein Festplattenabbild.

Was jetzt?

Erstmal das Offensichtliche

Erstmal schauen, womit wir es überhaupt zu tun haben.

Erstmal das Offensichtliche

Erstmal schauen, womit wir es überhaupt zu tun haben.

`file` geht eigentlich immer.

Erstmal das Offensichtliche

Erstmal schauen, womit wir es überhaupt zu tun haben.

`file` geht eigentlich immer.

Und dann noch die Klassiker:

Erstmal das Offensichtliche

Erstmal schauen, womit wir es überhaupt zu tun haben.

`file` geht eigentlich immer.

Und dann noch die Klassiker:

```
stat
```

```
ls
```

```
cat
```

mm-Befehle

`mm` steht scheinbar für **media management**. Okay.

mm-Befehle

`mm` steht scheinbar für **media management**. Okay.

Diese Befehle sind für **Festplattenabbilder** (Disk Images) gedacht, also 1:1 Kopien eines Speichermediums.

Aufbau eines Disk Images

Auf einem Disk Image liegt normalerweise eine **Partitionstabelle**:

Aufbau eines Disk Images

Auf einem Disk Image liegt normalerweise eine **Partitionstabelle**:

- **MBR** (legacy)

Aufbau eines Disk Images

Auf einem Disk Image liegt normalerweise eine **Partitionstabelle**:

- **MBR** (legacy)
- **GPT**

Aufbau eines Disk Images

Auf einem Disk Image liegt normalerweise eine **Partitionstabelle**:

- **MBR** (legacy)
- **GPT**

Diese teilt die Festplatte in große zusammenhängende Blöcke (Partitionen) ein.

Aufbau eines Disk Images

Auf einem Disk Image liegt normalerweise eine **Partitionstabelle**:

- **MBR** (legacy)
- **GPT**

Diese teilt die Festplatte in große zusammenhängende Blöcke (Partitionen) ein.

Und in den Partitionen stecken dann die **Dateisysteme**.

Aber!

Aber!

Man kann ein Dateisystem auch direkt
auf die gesamte Platte schreiben.

Ganz ohne Partitionstabelle.

Die mm-Befehle

`mmstat` zeigt Infos über den Disk-Typ

Die mm-Befehle

`mmstat` zeigt Infos über den Disk-Typ *(naja...)*

`mmls`

Die mm-Befehle

`mmstat` zeigt Infos über den Disk-Typ *(naja...)*

`mmls` zeigt die **Partitionsliste**

`mmcat`

Die mm-Befehle

`mmstat` zeigt Infos über den Disk-Typ *(naja...)*

`mmls` zeigt die **Partitionsliste**

`mmcat` gibt den rohen Inhalt einer Partition aus

„mmls Beispiel“

Und jetzt rein
ins Dateisystem.

Und jetzt rein ins Dateisystem.

Die `fs`-Befehle

Infos über das Dateisystem

Du willst wissen, was für ein Dateisystem auf der Partition ist?

Infos über das Dateisystem

Du willst wissen, was für ein Dateisystem auf der Partition ist?

```
fsstat -o <offset> disk.img
```

Infos über das Dateisystem

Du willst wissen, was für ein Dateisystem auf der Partition ist?

```
fsstat -o <offset> disk.img
```

Gibt dir: Dateisystemtyp, Blockgröße, Anzahl Inodes, ...

Dateien auflisten

Du willst wissen, welche Dateien auf der Partition sind?

Dateien auflisten

Du willst wissen, welche Dateien auf der Partition sind?

`fls` (mit `-r`)

Datei-Inhalt lesen

Du willst den Inhalt einer Datei?

Datei-Inhalt lesen

Du willst den Inhalt einer Datei?

```
icat
```

Datei-Inhalt lesen

Du willst den Inhalt einer Datei?

```
icat
```

Wofür steht das `i`?

Datei-Inhalt lesen

Du willst den Inhalt einer Datei?

```
icat
```

Wofür steht das `i`?

Inode!

Datei-Inhalt lesen

Du willst den Inhalt einer Datei?

```
icat
```

Wofür steht das `i`?

Inode!

Alternativ: `fcat` mit dem Dateipfad statt der Inode-Nummer

Inodes

Jede Datei hat eine **Inode** (eindeutige ID) im Dateisystem.

Inodes

Jede Datei hat eine **Inode** (eindeutige ID) im Dateisystem.

Die Inode speichert Metadaten: Größe, Berechtigungen, Zeitstempel...

Inodes

Jede Datei hat eine **Inode** (eindeutige ID) im Dateisystem.

Die Inode speichert Metadaten: Größe, Berechtigungen, Zeitstempel...

...und zeigt auf die eigentlichen Datenblöcke auf der Platte.

Inodes

Jede Datei hat eine **Inode** (eindeutige ID) im Dateisystem.

Die Inode speichert Metadaten: Größe, Berechtigungen, Zeitstempel...

...und zeigt auf die eigentlichen Datenblöcke auf der Platte.

Weitere nützliche Tools:

Inodes

Jede Datei hat eine **Inode** (eindeutige ID) im Dateisystem.

Die Inode speichert Metadaten: Größe, Berechtigungen, Zeitstempel...

...und zeigt auf die eigentlichen Datenblöcke auf der Platte.

Weitere nützliche Tools:

`istat` Details zu einer bestimmten Inode

`ils`

Inodes

Jede Datei hat eine **Inode** (eindeutige ID) im Dateisystem.

Die Inode speichert Metadaten: Größe, Berechtigungen, Zeitstempel...

...und zeigt auf die eigentlichen Datenblöcke auf der Platte.

Weitere nützliche Tools:

`istat` Details zu einer bestimmten Inode

`ils` alle Inodes auflisten

`ifind`

Inodes

Jede Datei hat eine **Inode** (eindeutige ID) im Dateisystem.

Die Inode speichert Metadaten: Größe, Berechtigungen, Zeitstempel...

...und zeigt auf die eigentlichen Datenblöcke auf der Platte.

Weitere nützliche Tools:

`istat` Details zu einer bestimmten Inode

`ils` alle Inodes auflisten

`ifind` welche Inode belegt eine Data-Unit?

`ffind`

Inodes

Jede Datei hat eine **Inode** (eindeutige ID) im Dateisystem.

Die Inode speichert Metadaten: Größe, Berechtigungen, Zeitstempel...

...und zeigt auf die eigentlichen Datenblöcke auf der Platte.

Weitere nützliche Tools:

`istat`	Details zu einer bestimmten Inode
`ils`	alle Inodes auflisten
`ifind`	welche Inode belegt eine Data-Unit?
`ffind`	welcher Dateiname gehört zu einer Inode?

„Okay, aber das ist doch alles nur für ext4… oder?“

„Okay, aber das ist doch alles nur für ext4… oder?“

Nope.

„Okay, aber das ist doch alles nur für ext4… oder?“

Nope.

TSK funktioniert für so ziemlich **jedes** Dateisystem.

„Okay, aber das ist doch alles nur für ext4… oder?“

Nope.

TSK funktioniert für so ziemlich **jedes** Dateisystem.

Inklusive **NTFS** (aka. Windows).

Geht das nicht auch einfacher?

Muss ich für jede Datei einzeln `icat` aufrufen?

Geht das nicht auch einfacher?

Muss ich für jede Datei einzeln `icat` aufrufen?

Oder `fls` mit `icat` zusammen scripten?

Geht das nicht auch einfacher?

Muss ich für jede Datei einzeln `icat` aufrufen?

Oder `fls` mit `icat` zusammen scripten?

`tsk_recover` macht das für dich!

Und wenn die Kommandozeile zu viel ist?

Dann gibt es noch **Autopsy**.

Und wenn die Kommandozeile zu viel ist?

Dann gibt es noch **Autopsy**.

Grafische Oberfläche, basiert intern auf TSK.

Und wenn die Kommandozeile zu viel ist?

Dann gibt es noch **Autopsy**.

Grafische Oberfläche, basiert intern auf TSK.

Kann noch ein bisschen mehr: Timeline-Analyse, Keyword-Suche, ...

Und wenn die Kommandozeile zu viel ist?

Dann gibt es noch **Autopsy**.

Grafische Oberfläche, basiert intern auf TSK.

Kann noch ein bisschen mehr: Timeline-Analyse, Keyword-Suche, …

Das auf Linux zum Laufen zu bringen ist allerdings… sagt Bescheid, wenn ihr es geschafft habt.