## Vorbereitung

Bereits vor dem Praktikum sollten Sie sich anhand der im Internet verfügbaren Informationen über folgende Anwendungen bzw. Werkzeuge und deren Einsatzmöglichkeiten informieren:

- testdisk – Test-, Info- und Recovery-Tool für Festplatten und Dateien
- photorec – Datei-Carver: Wiederherstellen von verlorenen Dateien
- wireshark – Package-Sniffer, beinhaltet aber auch ein – für uns interessantes – Network-Trace-Analyse-Tool
- stegdetect – Software zum Erkennen von Steganographie
- dd – Anwendung zum erstellen von Disk-Images oder lesen von beliebigen Bereichen einer Datei

Es wird der Umgang mit einer Konsole/Terminal vorausgesetzt. Bei Bedarf bitte auch dies nachschlagen. Sie sollten diese Werkzeuge auch auf ihrem eigenen Endgerät zum Laufen bringen können, dann geht das mit der Abnahme auch leichter und Sie können ggf. auch die aktuelleren Versionen nutzen. Vielleicht spendieren Sie sich auch eine eigene kleine VM, so dass diese Art Werkzeuge getrennt von Ihren Nutzdaten Verwendung finden.

## Aufgabe 1: Wo stecken sie denn?


> *News Flash:*
> ***Hamburg verabschiedet Gesetz gegen obszöne Bilder von Nashörnern**.*
> *Führende Meinungsforschungsinstitute haben herausgefunden, dass sich ein zunehmender Teil der Bevölkerung durch die Abbildung von Nashörnern erheblich gestört fühlt. Forscher konnten bisher keine eindeutigen Ursachen dafür ausmachen und warnen vor vorschnellen Entscheidungen.*
> *Hamburg hat nun als erstes Bundesland ein Verbot mit Androhung von harter Strafe gegen Bilder von Rhinozerossen erlassen. Die Rhino Search Group der HAW wird keine Mittel und Aufwände scheuen, um auch das letzte Bild zu finden – wie gut es auch versteckt sein mag!*

**Briefing**:

Wir wurden von dem Hamburger LKA um Mithilfe gebeten, weil sich auch dort herumgesprochen hat, dass Forensik auf dem Lernplan aufgetaucht ist. Bei einem besonders dreisten Fall eines Nashornbildersammlers sind die Ermittler durch Hinweise der NSA (Nashorn-Such-Allianz) bei einer globalen Analyse des hamburgischen Netzwerkverkehrs fündig geworden. Aufgrund des verbotenen Nashorntraffics wurde die IT des Verdächtigen sofort sichergestellt und gesichtet.

Leider fehlen die Festplatten und auch Laptops konnten nicht sichergestellt werden, nur ein einziger USB-Stick wurde im Besitz des Verdächtigen gefunden.

**Materialien**

Unsere Analyse muss allein auf Basis der übermittelten Daten – Mitschnitte des Netzwerkverkehrs und ein Image des gefundenen USB-Sticks – erfolgen.

| | |
|---|---|
| rhino.log | `c0d0093eb1664cd7b73f3a5225ae3f30` |
| rhino2.log | `cd21eaf4acfb50f71ffff857d7968341` |
| rhino3.log | `7e29f9d67346df25faaf18efcd95fc30` |
| usb.dd | `a7925aa1934ed0ba3433826ceedbf600` |

Im sichersten System der Welt, unserer eigenen Cloud, wurden die Daten abgelegt, unverschlüsselt, weil ja sicher!

`https://owncloud.informatik.haw-hamburg.de/index.php/s/uQpIuEwjVOR3RrT`

Das Passwort für den Zugang lautet: `its2016sose`

**Auftrag**

Unsere Aufgabe ist es, die übergebenen Daten auszuwerten und alle Hinweise, die zweckdienlich sind, zu dokumentieren. D.h. es ist **Ihre** Aufgabe, die Daten auseinander zu nehmen!

Besonders wichtig sind:

1. Nachweis des Besitzes von Nashornbildern
2. Anzahl der identifizierten Nashornbildern
3. Alle Zugangsdaten oder Credentials, die zu weiteren Systemen mit Nashornbildern gehören könnten

Stellen Sie so viele Nashornbilder wir möglich sicher, ein Ermittler glaubt, einer Äußerung des Verdächtigen entnehmen zu können, dass es insgesamt **11** sind!

Beantworten Sie, wenn möglich, folgende Fragen:

- Wer gab dem Verdächtigen Zugriff?
- Welche Art von Zugriffen hatte der Verdächtige?
- Wie lauten die Zugangsdaten des Verdächtigen?
- Wie tauschte er sich mit Seinesgleichen aus?
- Welche relevanten Dateien können aus den Netzwerk-Traces gewonnen werden?
- Was ist mit der Festplatte passiert?
- Was geschah mit dem USB-Stick?
- Welche relevanten Dateien können von dem USB-Stick gewonnen werden?
- Wie kann der USB-Stick mit den Netzwerk-Traces in Verbindung gebracht werden?