1. Nachweis des Besitzes von Nashornbildern: 11
2. Anzahl der identifizierten Nashornbildern: 11
3. Alle Zugangsdaten oder Credentials, die zu weiteren Systemen mit Nashornbildern gehören könnten:

*log1*
FTP: IP=137.30.122.253, USER=**gnome,** PASS=**gnome123**
IMAP: IP=137.30.120.39 , USER=**golden**, PASS=**kinky!tang**
TELNET: IP=137.30.122.253, USER=**ggnnoommee**, PASS=**gnome123**

FTP:
Request: STOR **rhino1.jpg**
Request: STOR **rhino3.jpg**
//Request: STOR contraband.zip (**rhino2.jpg**) (pw=monkey)

*log2*
HTTP:
http://www.cs.uno.edu/~gnome/**rhino4.jpg** *
http://www.cs.uno.edu/~gnome/**rhino5.gif** *

*log3*
HTTP:
http://groups.google.com/groups?q=**rhino.exe**&hl=en&lr=&ie=UTF-8&oe=UTF-8&sa=N&tab=wg
http://www.cs.uno.edu/~gnome/**rhino.exe** *
http://www.google.com/search?hl=en&ie=UTF-8&oe=UTF-8&q=**rhino.exe** *

*Wer gab dem Verdächtigen Zugriff?*
???
*Welche Art von Zugriffen hatte der Verdächtige?*
FTP-Server, IMAP-Server (E-Mail), TELNET, HTTP

*Wie lauten die Zugangsdaten des Verdächtigen?*
(rhino.log)
FTP: IP=137.30.122.253, USER=**gnome,** PASS=**gnome123**
IMAP: IP=137.30.120.39 , USER=**golden**, PASS=**kinky!tang**
*TELNET: IP=137.30.122.253, USER=**ggnnoommee**, PASS=**gnome123***

*Wie tauschte er sich mit Seinesgleichen aus?*
*???*

*Welche relevanten Dateien können aus den Netzwerk-Traces gewonnen werden?*
***rhino1.jpg***
***rhino2.jpg (entpackt und entschlüsselt von contraband.zip (**pw=monkey**))***
***rhino3.jpg***
***rhino4.jpg***
***rhino5.jpg***

*Was ist mit der Festplatte passiert?*
*Wurde in den Mississippi River versenkt.*

*Was geschah mit dem USB-Stick?*

*Wurde formatiert.*

*Welche relevanten Dateien können von dem USB-Stick gewonnen werden?*

*16 x *.jpg*
*1 x *.mp4*
*1 x *.doc*
*1 x *.txt*
*1 x *.jar*

*Wie kann der USB-Stick mit den Netzwerk-Traces in Verbindung gebracht werden?*

*Das Passwort von „contraband.zip“ stand versteckt in eine *.txt*