**Digital Forensics Challenge - Save the Animals**

**Scenario:**

The Toy Story Police Department (TSPD) is investigating a series of kidnappings. Baby stuffed animals are being kidnapped from their homes and sold on the international stuffed slave market. Sheriff Woody raided the office of the suspected ringleader. The Toy Story Incident Response (TSIR) team was able to perform data acquisition on found devices and computers. The suspect claims he is innocent and that any evidence found was planted on his computer. TSPD has also captured a laptop from one of the alleged stuffed animal buyers. **Your job is to analyze the acquired data and answer the questions in the attached document so that Sheriff Woody can bust this evil stuffed slave market.**

This is an Inventory list of Product IDs of recently sold kidnapped stuffed animals

* + Product\_E1
  + Product\_P1
  + Product\_D1
  + Product\_R1

Additional Evidence:

1. Hard Drive from suspect's computer = *FlashEvidence.001*
2. Packet Capture from activity on suspect's computer = *Evidence\_Pcap.pcapng*
3. Registry from suspect's computer = *SAM hive*
4. Browser file from alleged buyer's laptop = *j3uv3vkf.default*

NOTE: You may need to find some information on the Internet but all evidence files needed are included in the Lab downloads folder. This is NOT a web exploitation exercise so please do not waste your time probing deep into website code.

**Digital Forensics Challenge - Save the Animals**

Tips - SKIP this page if you do not want any direction on solving the challenge

#1 The challenge questions are in no specific order - you can start with any of the evidence and any question. However, some answers will not be reachable until other evidence is found. It's a process!

#2 The goal of the challenge is to provide practice in the following digital forensics techniques - included are some suggested tools to help with each technique. These are only suggestions, there are many other forensics tools that you may prefer to use.

* Analyze file metadata --- Possible tools: exiftool, Jeffrey's Exif viewer website
* Extracting information and files from a packet capture --- Possible tools: Wireshark, NetworkMiner
* Retrieving deleted files --- Possible tools: The Sleuth Kit, Autopsy, FTK Imager
* File carving fragmented files --- Possible tools: foremost, scalpel
* Retrieving info from Browser files (Firefox) === Possible tools: Firefox SQLite Manager Addon, SQLiteExpertPersonal, Nirsoft Browser tools. Note that if the browser had been Internet Explorer or Chrome, a different set of tools might be needed.
* Extract info about a Windows computer from a Registry File --- RegRipper, Access Data Registry Viewer

#3 The challenge can be performed using Windows or Linux tools. For more practice, try doing each technique with a tool from each Operating System. \*\*\* The SIFT Workstation 3.0 is an simple way to access lots of Linux forensic tools. It can be downloaded as a Virtual Machine from [https://digital-forensics.sans.org/blog/2014/03/23/sans-sift-3-0-virtual-machine-released#](https://digital-forensics.sans.org/blog/2014/03/23/sans-sift-3-0-virtual-machine-released%23)

**Digital Forensics Challenge - Save the Animals**

**Questions for analysis**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Product ID** | **Animal Type** | **Nickname** | **Date kidnapped** | **Price** | **Location (give more info than country)** |
| Product\_E1 | Elephant | Dumbo | 2014:04:14 19:09:58 | $3000 | Address: Takaka Hill, New Zealand  Detail: what is the nearest road?  West Road |
| Product\_P1 | Penguin | Wheezy | 2014:07:02 06:34:56 | $2000 | Address: Kruger Park, South Africa  Detail: what evidence is there that the kidnappers are dangerous?  Kidnapper is armed with a rifle |
| Product\_R1 | Reindeer | Rudolph | 2015:07:07 19:36:02 | $11000 | Address: Øvre Holmegate 26-22, 4006 Stavanger, Norway  Detail: What does the street sign mean?  Pedestrian zone |
| Product\_D1. | Dog | Spot | 2015-07-03, 17:22 | $100 | Address: Cannes, France  Detail: what body of water is nearby?  Bay of Cannes |
| Dig deeper - what was the most expensive product and why? | | | | | Reindeer. Cost is high due to increased armed security at this location |

**Questions for analysis**

Identify all the usernames on the Suspect's computer and find matching data where possible

|  |  |  |
| --- | --- | --- |
| **Username** | **Real Name** | **Role in the Gang** |
| Skywalker  Darth  ObiWan  Wookie | Spider Baby  Emperor Zurg  Stinky Pete  Jack Chew | Evil Leader  Henchman #1  Henchman #2 |

Investigators believe the Gang has an online website to find clients.

|  |  |
| --- | --- |
| What is the URL of the website?  http://globalstuffed.weebly.com/ | What is the IP address?  199.34.228.53 |

Identify detailed data found from alleged buyer's browsing data

|  |  |
| --- | --- |
| Name: Keyser | Cell Phone #: 212-555-1212 |
| Email address: ksoze@creepy.com | Company: Kobayashi, Inc |
| MailingAddress: | Title: Storyteller |
| Credit Card #: Amex 4824-954076-33132 code 1432 exp 03/17 |