**P5 - Digital Forensics Challenge – Animal Trafficking**

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.**

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*

You may start with the above description then complete the analysis guides below.

**Questions for analysis**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Product ID** | **Animal Type** | **Nickname** | **Date kidnapped** | **Price** | **Location (give more info than country)** |
| Product\_E1 |  |  |  |  | Address:  Detail: what is the nearest road? |
| Product\_P1 |  |  |  |  | Address:  Detail: what evidence is there that the kidnappers are dangerous? |
| Product\_R1 |  |  |  |  | Address:  Detail: What does the street sign mean? |
| Product\_D1. |  |  |  |  | Address:  Detail: what body of water is nearby? |
| Dig deeper - what was the most expensive product and why? | | | | |  |

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

|  |  |  |
| --- | --- | --- |
| **Username** | **Real Name** | **Role in the Gang** |
|  |  |  |

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

|  |  |
| --- | --- |
| What is the URL of the website? | What is the IP address? |

Identify detailed data found from alleged buyer's browsing data

|  |  |
| --- | --- |
| Name: | Cell Phone #: |
| Email address: | Company: |
| MailingAddress: | Title: |
| Credit Card #: |