Network and Internet Forensics

Birmingham City University

Computer Forensics

Contents

[Part A – Technical Supporting Discussion 2](#_Toc120013781)

[a. Monitoring Network Traffic 2](#_Toc120013782)

[b. Recovering Digital Evidence 2](#_Toc120013783)

[Part B – Network Traffic Analysis 2](#_Toc120013784)

[1. Management Summary 2](#_Toc120013785)

[2. Technical Analysis 2](#_Toc120013786)

[3. Contemporaneous Notes 2](#_Toc120013787)

# Part A – Technical Supporting Discussion

# Monitoring Network Traffic

# Recovering Digital Evidence

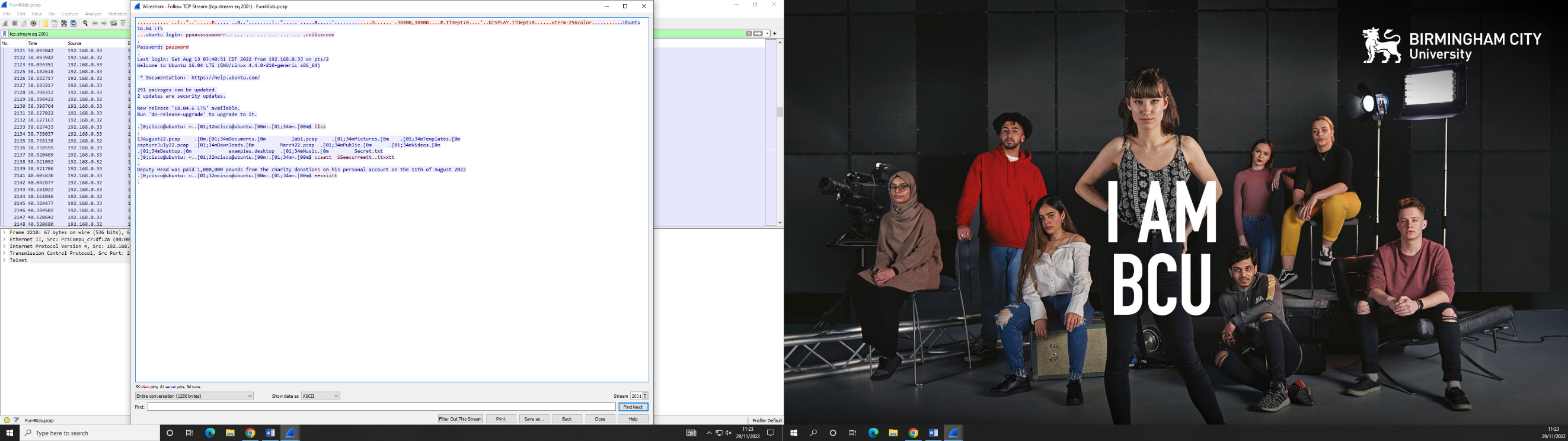
# Part B – Network Traffic Analysis

# Management Summary

Fun4Kids is a UK event agency that specialises in managing and organizing events for kids. In July 2022, there was and fundraising event to raise money for disadvantaged children in West Midlands. Employees started to notice that the process of the handling and recording of the donations hadn’t been transparent so they were suspecting that there have been deductions in the money donated to the charity. John was the main suspect as he was acting suspicious. Peter decided to remotely check John’s computer for evidence.

On Saturday 13th August, Peter found a text file with an interesting note in John’s computer. This note stated ‘Deputy Head was paid 1,000,000 pounds from the charity donations on his personal account on the 11th of August 2022’. Upon finding this note, Peter hands the evidence to the IT Department Manager, Victor. However, Peter does breach a piece of vital legislation during this investigation. That legislation is The Computer Misuse Act (1990) by breaching John’s account without permission.

# Technical Analysis

When investigating the incident, I found the note which stated ‘‘Deputy Head was paid 1,000,000 pounds from the charity donations on his personal account on the 11th of August 2022’. This was done by using Wireshark. When on Wireshark, I needed to scroll through the all of the data and see if there was anything that stood out as suspicious. When getting to the Telnet data, I decided to ‘Follow TCP Stream’. This groups all of the Telnet data together, making it easy to see everything. The image below shows this:

Peter goes into the terminal and starts off by typing the command ‘ls’. This command is a command to list computer files and directories. When analysing the Telnet packet, it was found that Peter set Echo to ‘Will Echo’. This is when anything that Peter types into the terminal is always repeated back twice. The last login is shown. The last login was Saturday August 13th at 03:40:51, which also shows him logging onto Ubuntu. This helps with the investigation a lot as it clearly shows when Peter started the investigation.

**Talk about the command CAT and what it does**

Peter’s IP address that was used during this investigation was 192.168.0.33 and the MAC address was 08:00:27:e7:3d:0b. John’s IP address that was used was 192.168.0.32 and the MAC address was 08:00:27:c7:df:2a. The Operating System used was Ubuntu 16.04 LTS (GNU/Linux 4.4.0-210-generic x86\_64).

# Contemporaneous Notes

July 2022 – This is when the fundraising event took place, when employees witnessed the process of handling and recording the donations wasn’t transparent and there were suspicions of deductions in the money donated to the charity.

11th August 2022 – This is when the Deputy head was paid £1,000,000 from the charity donations on his personal account. This was displayed within the text file on John’s computer.

Saturday 13th August – This is when Peter decided to investigate the suspicions of John being the person doing this. When the office was closed, Peter remotely checked John’s computer for evidence, to back the suspicion.