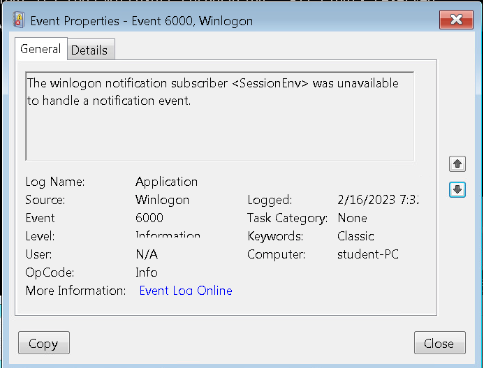
Lab 13: Log Analysis

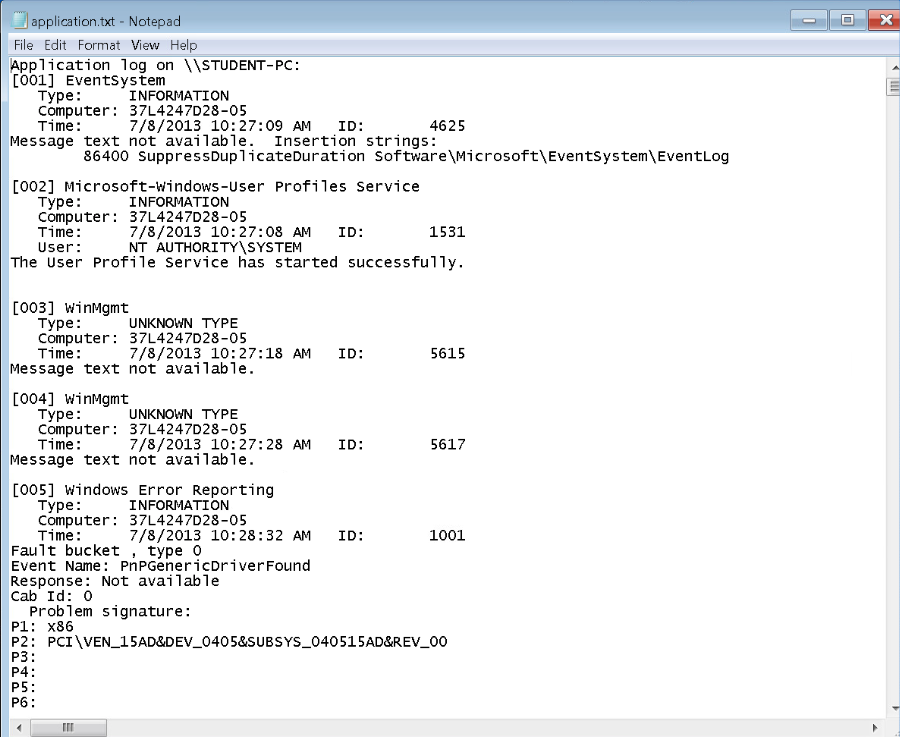
Lab 13 report Name: Kevin Ubilla

This Lab is required for Unit 4. It is worth 15 points. The Challenge Flags are worth 2.5 Extra Credit points.

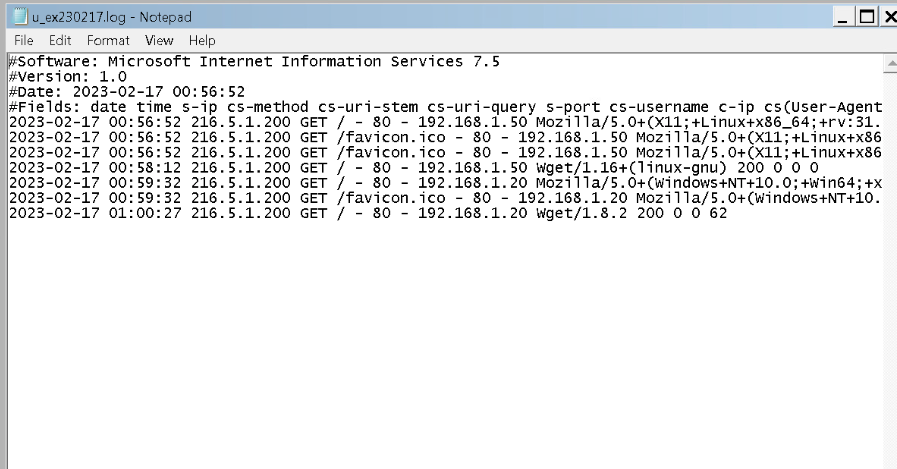
1. **Examining Windows Event Logs, IIS Logs, and Scheduled Tasks, Step 10.** You have drilled down to read specific events in the log. Please find a specific event, preferably one from the security log, and capture it in detail to paste below.

**→**  **←**

1. **Examining Windows Event Logs, IIS Logs, and Scheduled Tasks, Step 23.** You have now dumped the application log and can view it using Notepad. Please capture a portion of what you see when you type **C:\>notepad application.txt**, including the Notepad header, and paste it here.

**→  ←**

1. **Examining Windows IIS Logs, Step 25.** Now that you have opened the IIS log of the IP addresses that have connected, please capture the specific entry, with the surrounding entries as well, that shows the connection from the Kali Linux machine and paste it below.

**→ ←**

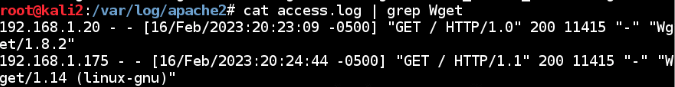
1. **Examining Windows IIS Logs, General.** Please say, in your own words, just where we can find the IIS log files in a Windows 10 machine.

**→** This is a Win7 machine, but on a Win10 we will most likely find the IIS log files in the LogFiles folder. This will likely be located on the main system drive in a directory resembling “C:\inetpub\logs\LogFiles”**. ←**

1. **Examining Linux Log Files, Step 3.** You are using Nmap to see if there are any ports open at IP address **127.0.0.1.** Why are you doing this for this particular address?

**→**We use this particular address because it is the localhost. Essentially, we are checking for open ports on that machine. **←**

1. **Examining Linux Log Files, Step 21.** You are looking at the auth log of the Kali machine web accesses, specifically searching for instances of where a “**wget**” occurred. Please capture the results of this search and paste them below.

**→  ←**

1. **Examining Linux Log Files, Step 39.** You are looking at the Apache log of the Kali machine searching for **forensicuser**. Please capture the result of your search and paste it below.

**→ Text

Description automatically generated ←**

**If you encountered any issues, either positive or negative, with this Lab, please let me know by commenting here. (This IS an experiment, after all.) I am tuning this according to what you say.**

**→ ←**