1. **Task 0**
2. Enter the [discord server](https://discord.com/invite/MJW5YUUwQj) and follow the prompts on the welcome screen
3. Go to the bot-commands channel and enter **!task0**
4. Enter the bot response into the challenge
5. **Task 1**
   1. Download the **.pcap** and the text file
   2. Use the ip.addr== filter to check all subnets in the text file
   3. For the four subnets that produce a response, **save the following**
      1. Subnet
      2. **Timestamps** – try to note the ones with HTTP/1.0 200 responses in the **.pcap**
      3. Source IP
      4. Destination IP (will be the same for all 4, this is the LP)
   4. Enter the 4 source IP addresses into the challenge
6. **Task 2**
7. Task 2 gives you a subnet, compare it to the list of subnets you saved from T1.
8. **Note the timestamp** of that subnet – this is the time zone for the company.
9. Now open **proxy.log** and look at the time zone at the top of the document.
10. Calculate the time difference for the HTTP/1.0 200 response connected to the company subnet’s IP address.
11. Go to the **logins.json** file, CTRL+F and enter the newly calculated timestamp. There should only be one occurrence found.
12. Note the **LOGONID** from that single occurrence. This will be in **integer** format, and you can provide it in **base 10 or base 16**.
13. Enter the Logon ID into the challenge.
14. **Task 3**
15. First, remember that single HTTP/1.0 200 request we found in the **.pcap**? Right click it and **export as raw data** – this should **not have a file extension**, but it should be done on **Windows**.
16. Now, use Notepad, Mousepad, or an email viewer to see the background contents of each email file for a **cipher**.
17. **Save the Message ID** of the email that you suspect – include the **<arrows>** in the result.
18. This cipher is **done the same way twice**, so once you decode it, copy the answer, and decode it the same way a second time.
19. Once you have decoded the cipher, you will have a **PowerShell script**, save it to a **text file**.
20. Open PowerShell and cd:/ to the location of the raw data you exported in step 1.
21. Enter the PowerShell script in one line at a time
22. After the **$result** line is entered, type **echo $result** and **copy the resulting code to a text file**
23. Look at the last line of the **$result**. Enter it into the challenge along with the **<Message ID>**
24. **Task 4**
25. To view the **.DAT** file, install **Windows Registry Recovery**. For the **artifacts**, you can use **Autopsy Digital Forensics**
26. First, open the output of the **$result** from Task 3 and review it to get an idea of what the malware is doing.
27. Open the **.DAT** file in **WRR** and view as raw data to navigate via a file system
28. You’ll find a path to login **sessions**. **Pay attention to the Hostnames**.
29. **Task 5 Part 3**
30. I’m so pissed off. It’s **/USR/BIN/MALICIOUSFILEGOESHERE**.
31. Happy file hunting ya filthy animals
32. **Task 6**
33. **apt-get install libc6-dbg gdb valgrind**