Retracted

## Retracted – Notes

### **Task 1: Introduction**

* **Scenario:** A mother reports her PC behavior changed suddenly—files became inaccessible, ransomware wallpaper appeared, and then everything reverted to normal except for a Bitcoin note.
* **Goal:** Use **Windows Event Logs (Sysmon)** to investigate what happened, identify the malware, track its actions, and understand how it was reversed.

### **Task 2: The Message**

1. **Path of the ransom note:** C:\Users\Sophie\Desktop\SOPHIE.txt
2. **Program used to create the file:** notepad.exe (found via Sysmon Event ID 1 process creation logs).
3. **Time of creation (UTC):** 2024-01-08 14:25:30

### **Task 3: Something Wrong**

1. **Installer filename:** antivirus.exe (found in Download history and Sysmon process logs).
2. **Download location:** C:\Users\Sophie\download
3. **File extension added by installer:** .dmp (Sysmon Event ID 11 for file creation shows files encrypted with .dmp extension).
4. **Installer network contact IP:** 10.10.8.111 (found via Sysmon Event ID 3 for network connection from antivirus.exe).

### **Task 4: Back to Normal**

1. **RDP login source IP:** 10.11.27.46 (Sysmon Event ID 3 filtering for RDP connection events in 2024).
2. **When decryptor was run:** 2024-01-08 14:24:18 UTC (decryptor.exe execution logged via Sysmon Event ID 1).

### **Task 5: Doesn’t Make Sense**

Order of events (chronologically labeled 1–7):

1. Sophie downloaded and ran the malware.
2. The malware encrypted files and displayed a ransomware note.
3. Sophie ran to get help after seeing the ransom note.
4. An intruder logged in via RDP and explored the machine.
5. The intruder downloaded a decryptor and decrypted all files.
6. Before leaving, the intruder left a message saying “check your Bitcoin.”
7. You arrived to investigate and found the system restored.

### **Task 6: Conclusion**

* **Wrap-up question:** Did the intruder retract the attack out of remorse?
* **Answer:** "Yeah, possibly." A change of heart seems plausible given the aftermath.

### **Sysmon Event IDs Used**

Here's the key Sysmon Event IDs referenced in this room:

arduino

CopyEdit

1 Process creation

3 Network connection

11 File creation

These were essential for tracking file generation, communications, and executable activity.[Medium](https://happycamper84.medium.com/retracted-tryhackme-walkthrough-cdbd460ab52b?utm_source=chatgpt.com)

**Summary:**  
You efficiently reconstructed a ransomware event timeline—from its execution and encryption, through intruder intervention and file decryption—by using Sysmon logs and the Event Viewer.

