Capture The Flag

NAME: RALPH RODRIGUEZ

TEAM NAME: OMEGA RED

Introduction

- The CTF Problem
- Introduction to the Problem
- Working Toward a Solution
- Arriving at The Solution
- Strategies, Pitfalls, Lessons Learned
- Workplace Relevance
- Summary
- Demo

CTF The Problem :

CHALLENGE 6: USE THE CAPTURE FILE PROVIDED TO DETERMINE DARTH VADER'S PASSWORD.

- Passwords are often misplaced or forgotten — even by high-profile users.
  This challenge simulates a realistic scenario where recovering a lost password is critical.
- We explore a fast and effective recovery method using forensic tools.
  By analyzing network traffic from a capture file, we extract key data in just minutes.

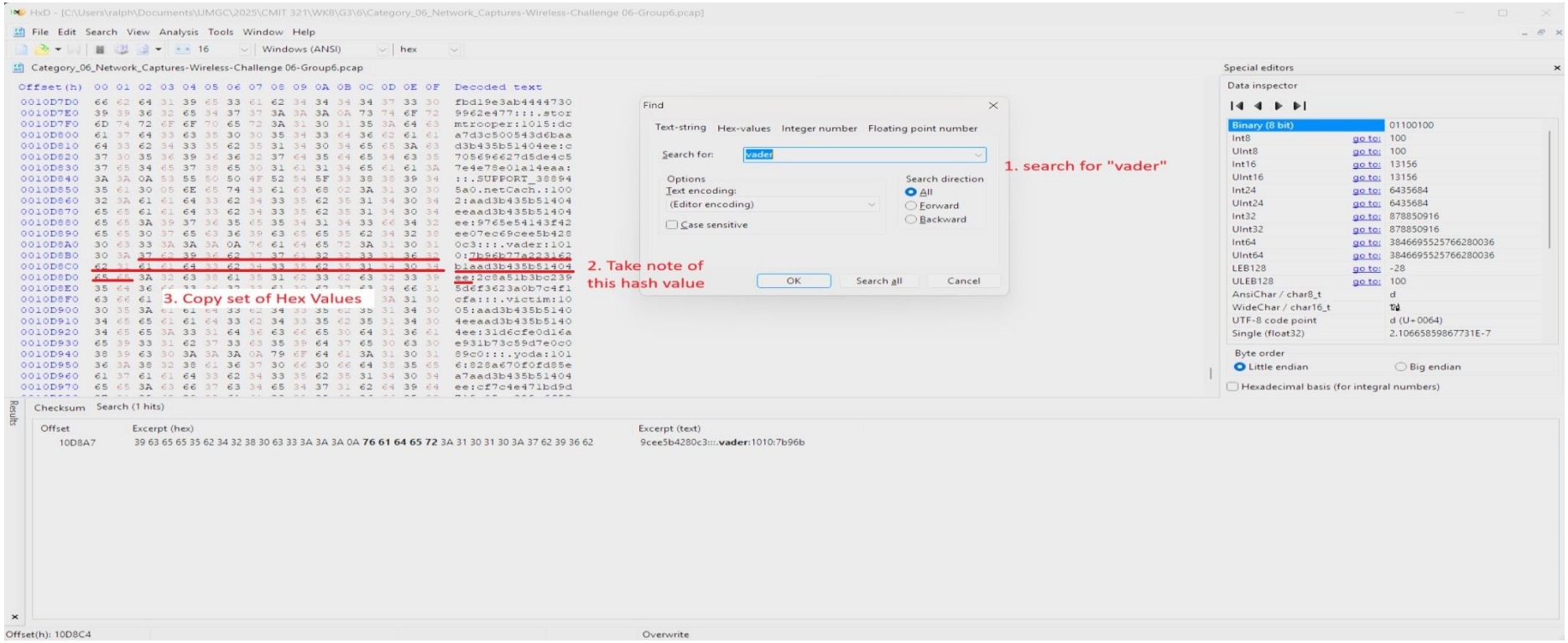
CTF The Problem :

CHALLENGE 6: USE THE CAPTURE FILE PROVIDED TO DETERMINE DARTH VADER'S PASSWORD.

EXECUTION FLOW

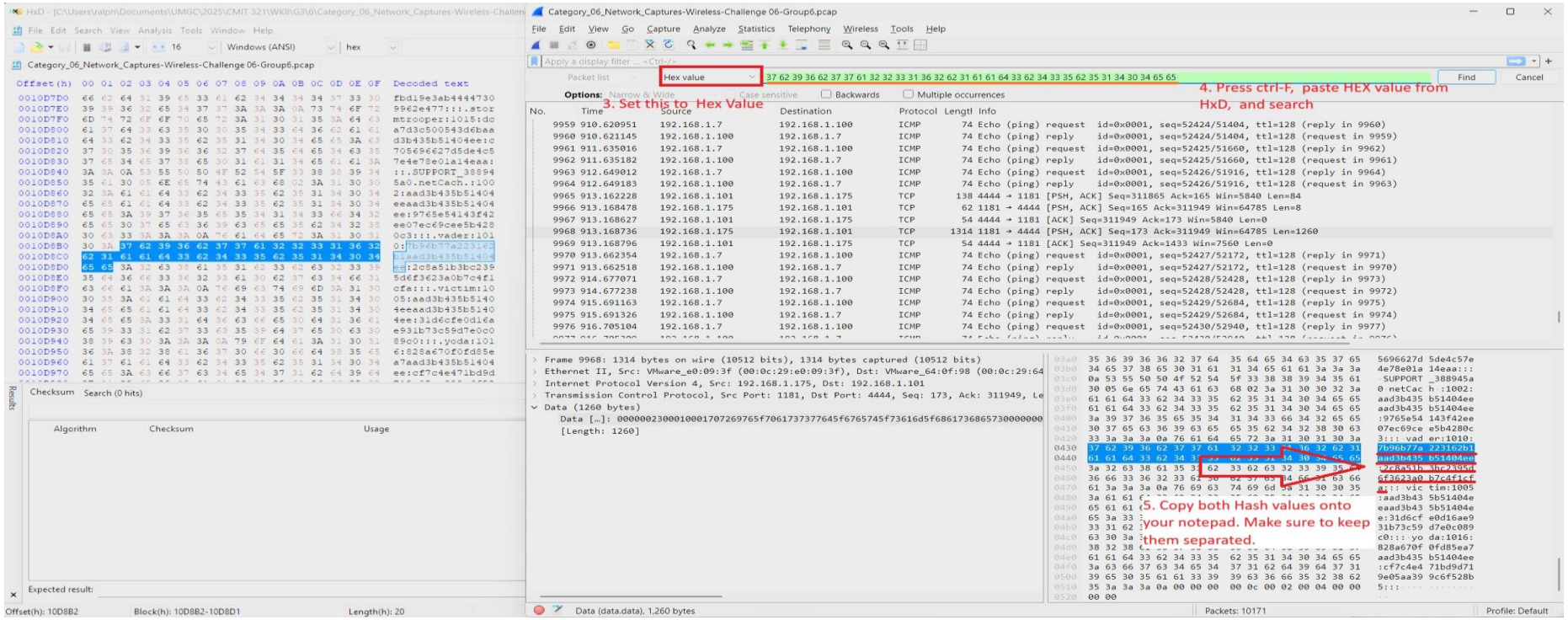
- PACKET ANALYSIS
- HASH EXTRACTION
- PASSWORD RECOVERY

Introduction to the Problem



- With a Hex editor open the PCAP file and search for "Vader'
- Take note of the HASH value and copy the HEX values

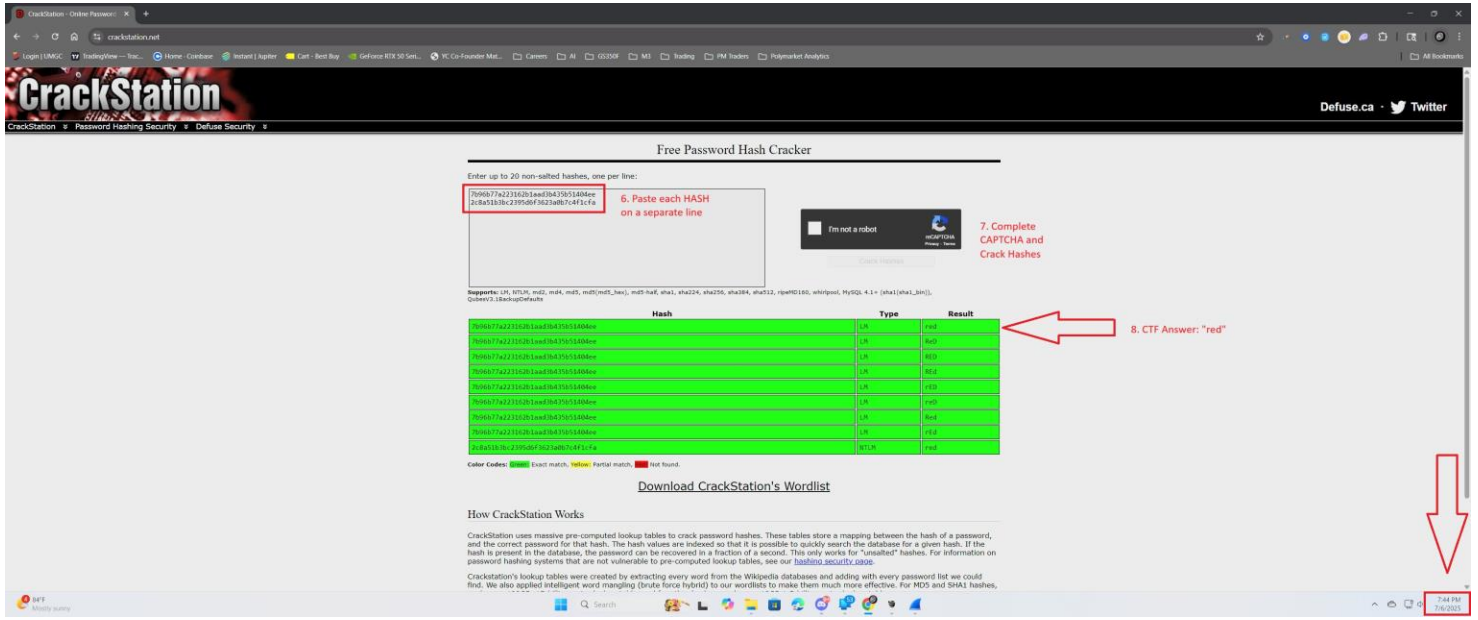
Working Toward A Solution



- Open the same file with WireShark & search for the same HEX value
- Verify the same HASH value from the left (HxD) are the same as with the ones on the right (WireShark)
- Copy the 2 HASH values from Wireshark

Arriving at the Solution

- Open a web browser and visit crackstation.net
- *Paste each HASH value on a separate line, complete the CAPTCHA, and click "Crack Hashes"*
- *Navigate to the results column and the answer: "red"*



Strategies, Pitfalls, Lessons Learned

- **Faster Strategy:**
  The hash can be copied directly from the hex editor (HxD) and submitted to CrackStation without needing Wireshark — saving time.
- **Common Pitfall:**
  Since the file is a `.pcap`, it's natural to open it in Wireshark first. However, searching for `"vader"` in Wireshark doesn't return useful results — HxD is more effective in this case.
- **Lesson Learned:**
  It's important to understand the strengths and limitations of both Wireshark and HxD. Choosing the right tool for the task makes a big difference in solving CTF challenges efficiently.

Workplace Relevance

- **Real-World Packet Analysis:**
  Skills in analyzing .pcap files using tools like Wireshark and hex editors are directly applicable in incident response and threat hunting.
- **Hash Recognition and Cracking:**
  Understanding how to identify and crack password hashes helps with password auditing, penetration testing, and verifying credential leaks.
- **CTF Practice = Hands-On Readiness:**
  Capture the Flag (CTF) challenges simulate real cybersecurity problems, building muscle memory for tasks like data extraction, protocol analysis, and threat detection.

Summary

In these challenges, I successfully extracted and cracked a password from a `.pcap` file using a combination of HxD (hex editor) and online tools. Although Wireshark is a go-to tool for packet analysis, this scenario highlighted the importance of choosing the right tool for the task. HxD provided a more direct path to the solution. I learned that understanding how to navigate raw data, identify hashes, and use external resources like CrackStation can significantly speed up problem-solving. This hands-on exercise not only strengthened my technical skills but also deepened my understanding of packet-level data analysis, which is highly relevant in cybersecurity roles such as threat analysis, digital forensics, and penetration testing.