Lab1: Assignment + Tool

William Fan, Danielle Santos Almeida, Jose Marvin Garcia

Montgomery College

NWIT 246 - Attacker Tools and Techniques

Prof. Vargas

9/6/25

With the rapid increase in cyberattacks, organizations are under constant pressure to strengthen their defense measures. Traditional security tools such as firewalls and antivirus software are no longer sufficient at the corporate level, leading to the rise of strategies such as Active Cyber Defense (ACD) and Offensive Cyber Strategies (OCS). This report examines two real-world legal cases. United *States v. Aaron Swartz* and *United States v. Dreyer* illustrate the challenges these strategies raise in relation to unauthorized access, privacy, and jurisdictional limits. Both cases highlight the difficulty of balancing the effectiveness of cyber defense tools with compliance to existing laws. In addition, the report provides guidance on the use of Wireshark, a widely used network protocol analyzer, to demonstrate its role in cybersecurity investigations.

1. Legal Case: United States vs. Aaron Swartz

The first case, related to active cyber defense, is *United States vs. Aaron Swartz*.

1.1 Summary

Aaron Swartz was an activist and programmer who accessed millions of academic journal articles from JSTOR through MIT's network without permission. Between 2010 and 2011, Swartz accessed 4.8 million JSTOR academic articles. He used an MIT closed network that allowed him to bypass network controls and wrote a Python script to download the articles. Although JSTOR did not press charges against him, the U.S. government decided to prosecute Swartz under the Computer Fraud and Abuse Act (CFAA). The United States charged him with wire fraud and unauthorized access, which carried potential prison time and fines. The laws cited

in this case included the Computer Fraud and Abuse Act (18 U.S.C. § 1030) and the Wire Fraud statute (18 U.S.C. § 1343).

1.2 Relationship to Active Cyber Defense and Offensive Cyber Strategies

Active Cyber Defense (ACD) involves defensive actions to detect, analyze, and respond to cyber threats. In this case, MIT and JSTOR used network monitoring and security controls to identify Swartz's unusual download activity. Their systems detected the unauthorized access through alerts, log analysis, and network forensics. This demonstrates the importance of strong monitoring and detection measures to prevent potential data breaches. Offensive Cyber Strategies (OCS), by contrast, involve actions aimed at exploiting or disrupting systems. The government viewed Swartz's actions as resembling an offensive operation because he bypassed security controls, automated large-scale downloads, and used MIT's network without authorization. While Swartz did not intend to damage JSTOR's systems, the techniques he used are similar to those seen in offensive cyber tactics, which led to his prosecution under U.S. law.

1.3 Challenges

The case of United States v. Swartz highlights the difficulty of distinguishing between legitimate research, activism, or civil disobedience and unlawful offensive cyber operations. Active monitoring by MIT and JSTOR successfully detected the activity, but it also shows how aggressive monitoring and strict laws such as the CFAA can raise questions of overreach. The challenge is how to maintain strong defenses through monitoring and forensic tools while

ensuring that enforcement does not blur the line between legitimate use of systems and criminal activity.

2. Legal Case: United States vs Dreyer

2.1 Summary:

An NCIS agent named Steve Logan used government-issued loopback software called RoundUp, which scans public p2p file sharing networks for suspicious activity. Such activities include uploading and downloading of child pornography. During broad scanning encompassing the entire state of Washington, agent Logan detected suspicious activity from a device belonging to Michael Dreyer, a civilian. Agent Logan turned the evidence over to civilian law enforcement, which led to Michael Dreyer's arrest and prosecution.

Dreyer aimed to suppress the evidence from RoundUp, arguing that military personnel are prohibited from engaging in civilian investigation under Posse Comitatus Act (PCA) (Ryan, Paragraph 1). As the Ninth Circuit explained, "Agent Logan's surveillance of all computers in Washington was therefore prohibited by the PCA"(United States v. Dreyer, Page 32). However, while the court acknowledged the violation, it declined to apply the exclusionary rule which maintained the defendant's conviction. He was sentenced to 18 years in prison and likely to be released in 2028. Laws violated in this case were:

1. Uniform Code of Military Justice (UCMJ)
2. Posse Comitatus Act (PCA) | 18 u.s.c. § 1385
3. Possession of Child Pornography | 18 U.S.C. § 2252(a)(4)(B)

2.2 Relationship to Active Cyber Defense and Offensive Cyber Strategies:

This case is closely related to the concept of Active Cyber Defense, because the scanning tool used by Agent Logan functioned as an active scanner that targeted both military and civilian systems. This highlights the risk of overreach in active cyber defense activities. In this case, although the appeal from the defendant was denied, a civilian was detected conducting illegal activity through the use of a military-grade, cutting edge tool. Dreyer, who might otherwise have remained under the radar, was detected only because that tool had been deployed.

For Offensive Cyber Strategies, stricter caution must be taken to prevent jurisdictional overreach, since such actions could undermine the legitimacy of civilian law enforcement. As Lawfare notes, "the Ninth Circuit concluded that suppression of the evidence was not warranted, despite 'troubling violations' of the PCA" (Ryan, P2). Going forward, NCIS must clearly draw the line between conducting lawful, routine scanning of military systems and avoid engaging in unlawful offensive cyber operations that intrude into civilian domains.

2.3 Challenges:

In the case of United States v. Dreyer, the challenge was how to conduct lawful routing scanning without mistakenly targeting civilian systems. The RoundUp tool is definitely designed as a means of active cyber defense, but its use in this instance demonstrated overreach. The key challenge is that ACD must stay within authorized systems, and OCS should only be carried out by personnel with clear government approval and legal authority. The Dreyer case highlights why the Posse Comitatus Act (PCA) strictly limits military involvement in civilian law enforcement. Even if tools like RoundUp are effective, scanning across civilian systems undermines legal boundaries and risks delegitimizing prosecutions. Future use of Active Cyber

Defense must be minimized to authorized domains, with clear legal authority and oversight to avoid sacrificing legality for effectiveness.

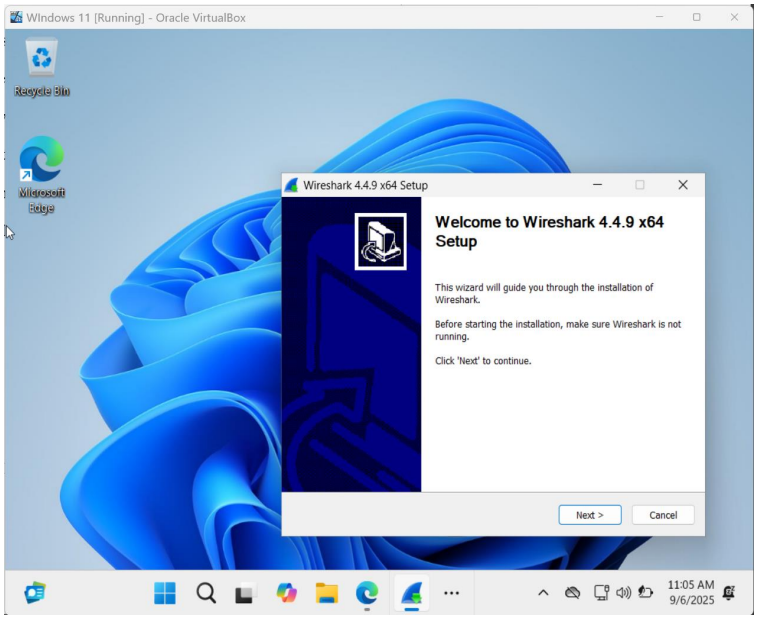
3. Tool: Wireshark

We chose Wireshark because it is a network protocol analyzer that captures traffic. It is useful in legal and forensic investigations. In LC1: United States V. Aaron Swartz, wireshark could have been used to show how abnormal traffic patterns of Swartz's abnormal amount of downloads. In LC2: United States V. Dreyer, Wireshark can be comparable to NCIS's RoundUp tool. It shows how scanning can reveal illegal file sharing, if monitor mode is enabled in wireshark. In conclusion, Wireshark is helpful for evidence and risky if being misused beyond appropriate boundaries.

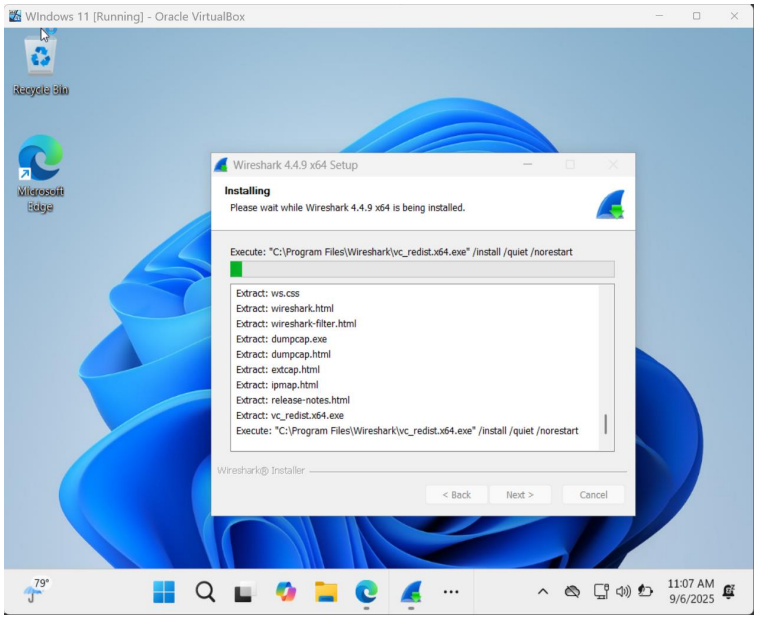
3.1 Installation:

The installation was done on a Windows 11 VM.

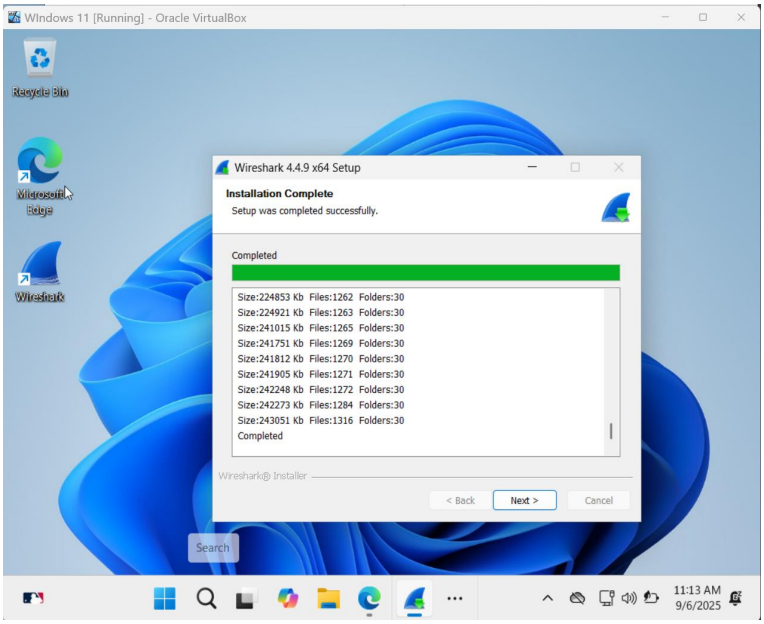
3.1.1 Initiating Wireshark Setup Wizard:



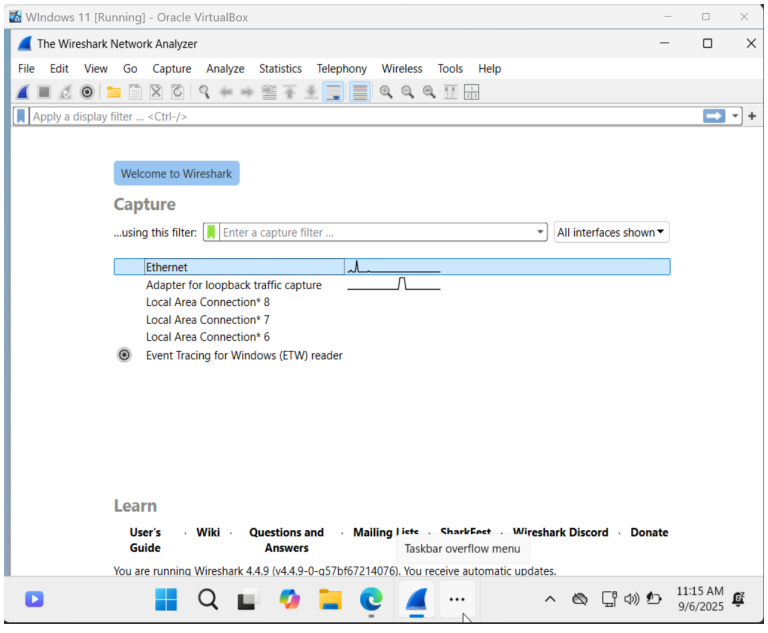
3.1.2 After following the configuration steps, the installation started:



3.1.3 Installation completed:



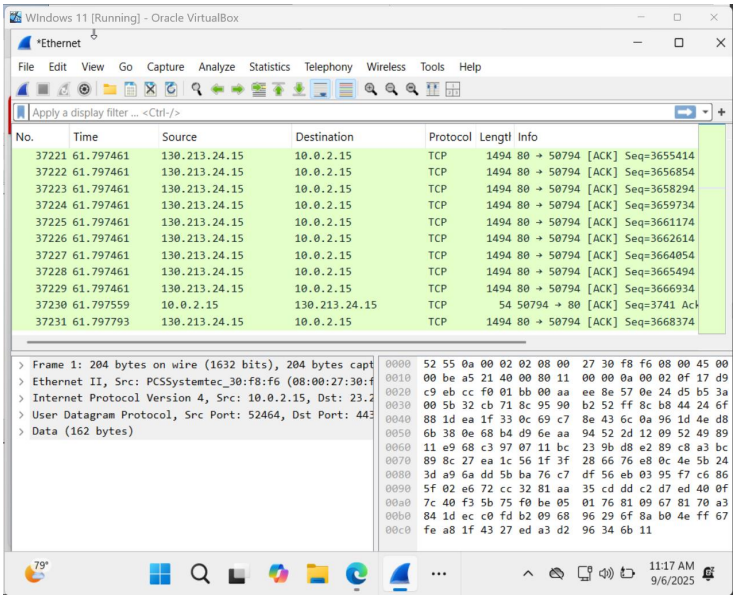
3.2 Wireshark interface:



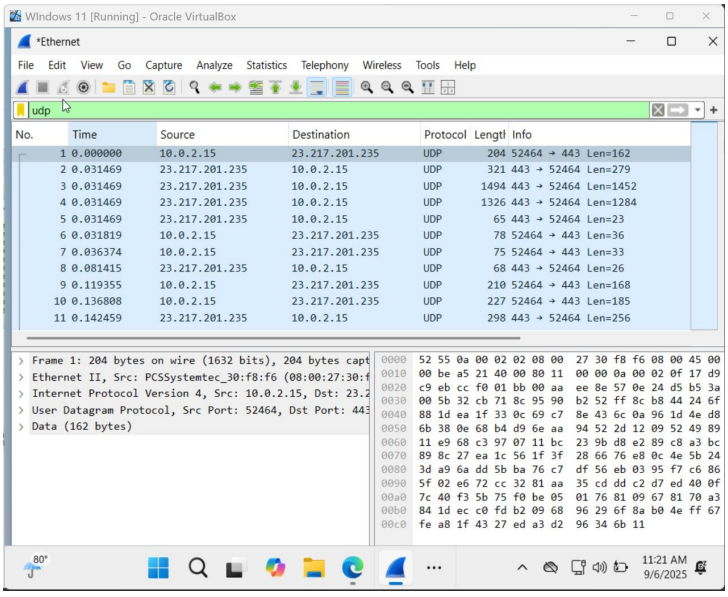
3.2.1 This screenshot shows Wireshark capturing live traffic on the Ethernet interface.

The Packet List panel displays TCP packets exchanged between the VM (10.0.2.15) and an

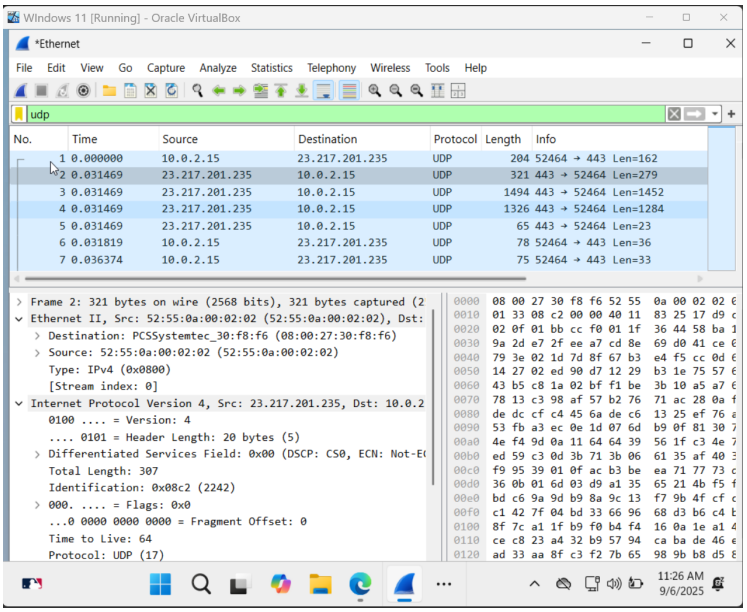
external server (130.213.24.15), confirming that Wireshark is successfully recording network activity in real time.



3.2.2 Here, a display filter (UDP) has been applied to the capture. Only UDP packets are displayed in the Packet List, demonstrating how Wireshark can focus on specific protocols or traffic types, making analysis more efficient.



3.2.3 The UDP packet is expanded in the Packet Details panel, showing its structure across the Ethernet II, IPv4, and UDP layers. The Packet Bytes panel below displays the raw data in both hexadecimal and ASCII formats.



This view highlights Wireshark's ability to break down traffic into protocol layers and allow detailed inspection of packet contents for analysis.

3.3 Conclusion

Wireshark demonstrates how network analysis tools can play a crucial role in legal cases. In *United States v. Swartz*, it could have revealed abnormal traffic from large-scale downloads, while in *United States v. Dreyer*, it mirrors the scanning power of RoundUp. These cases show that while Wireshark is valuable for uncovering misuse and supporting investigations, its application must remain within strict legal and ethical limits.

Works Cited

Liberatore, Marc, et al. *RoundUp Predictive Tool (RPT) Project: Final Report.* U.S. Department of Justice, awarded through Grant No. 2011-MC-CX-0001, Sept. 30, 2014, https://www.ojp.gov/pdffiles1/ojjdp/grants/248596.pdf.

National Institute of Standards and Technology. "Active Cyber Defense." *NIST Computer Security Resource Center Glossary*, https://csrc.nist.gov/glossary/term/active_cyber_defense.

Ryan, David. "*United States v. Dreyer*: Suppression of Evidence Not Needed to Deter Future Violations of the Posse Comitatus Act." *Lawfare*, 5 Nov. 2015, https://www.lawfaremedia.org/article/united-states-v-dreyer-suppression-evidence-not-needed-deter-future-violations-posse-comitatus-act.

United States Court of Appeals, Ninth Circuit. *United States v. Dreyer*, 804 F.3d 1266 (9th Cir. 2015) (en banc), filed Nov. 4, 2015. Ninth Circuit Court, https://cdn.ca9.uscourts.gov/datastore/opinions/2015/11/04/13-30077.pdf.

United States v. Aaron Swartz. U.S. District Court, District of Massachusetts, 2013. U.S. Department of Justice, https://www.justice.gov/archive/opa/pr/2013/January/13-crm-041.html.