**Lab 9: Investigating and Responding to Security Incidents**

**By**

**Natnael Kebede**



**University of Dallas**

**2020**

This Paper Submitted in Partial Fulfillment of the Requirements for

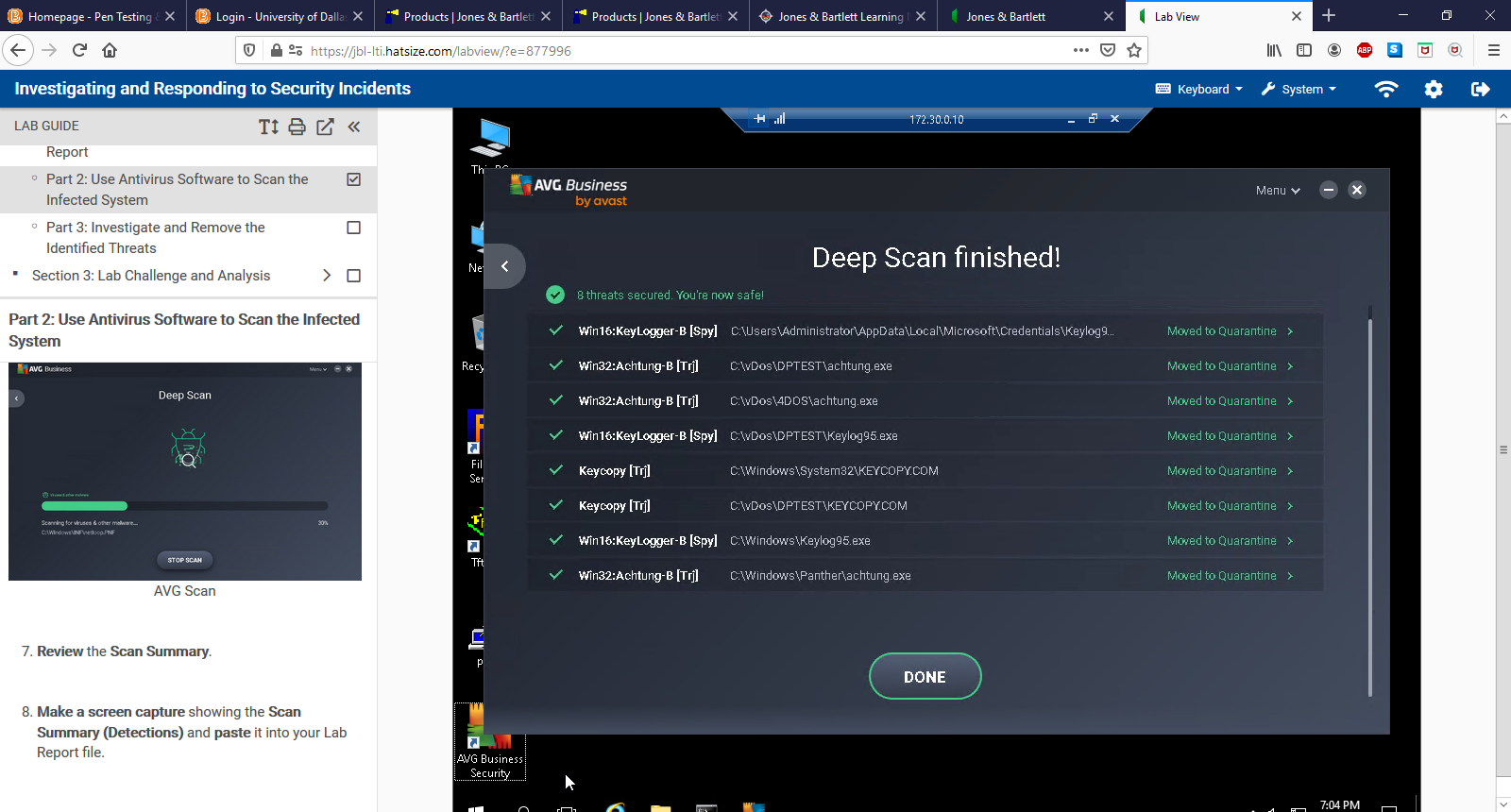
CYBS 7359 – Penetration Testing and Vulnerability Assessment

Spring 2020

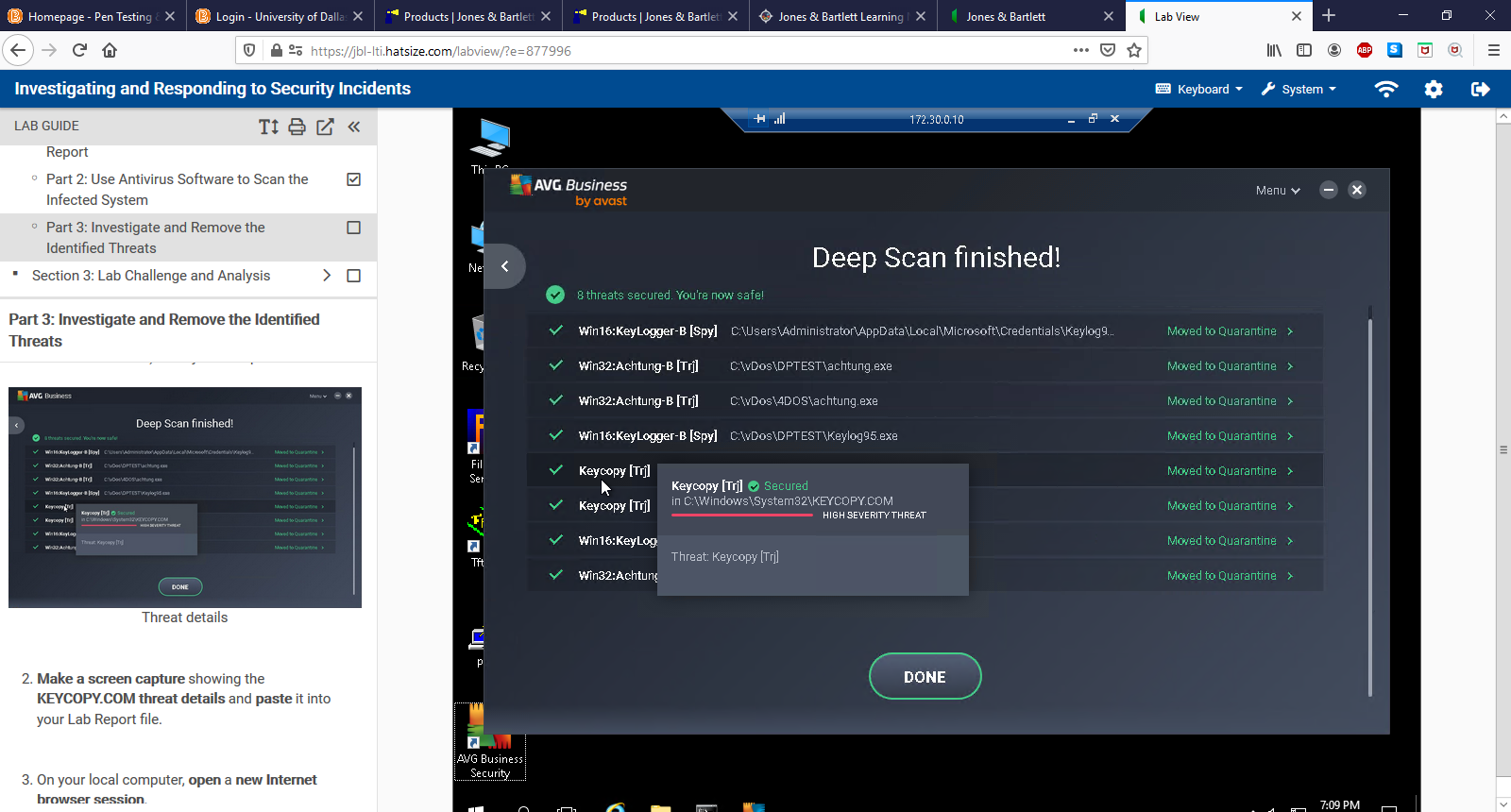
Presented to Dr. Renita Murimi

**Section 2**

1. Make a screen capture showing the Scan Summary (Detections) and paste it into your Lab Report file.



1. Make a screen capture showing the KEYCOPY.COM threat details and paste it into your Lab Report file.



1. In your Lab Report file, document any information you discover about eradicating this threat.

**KEYCOPY.COM - Keylogger**

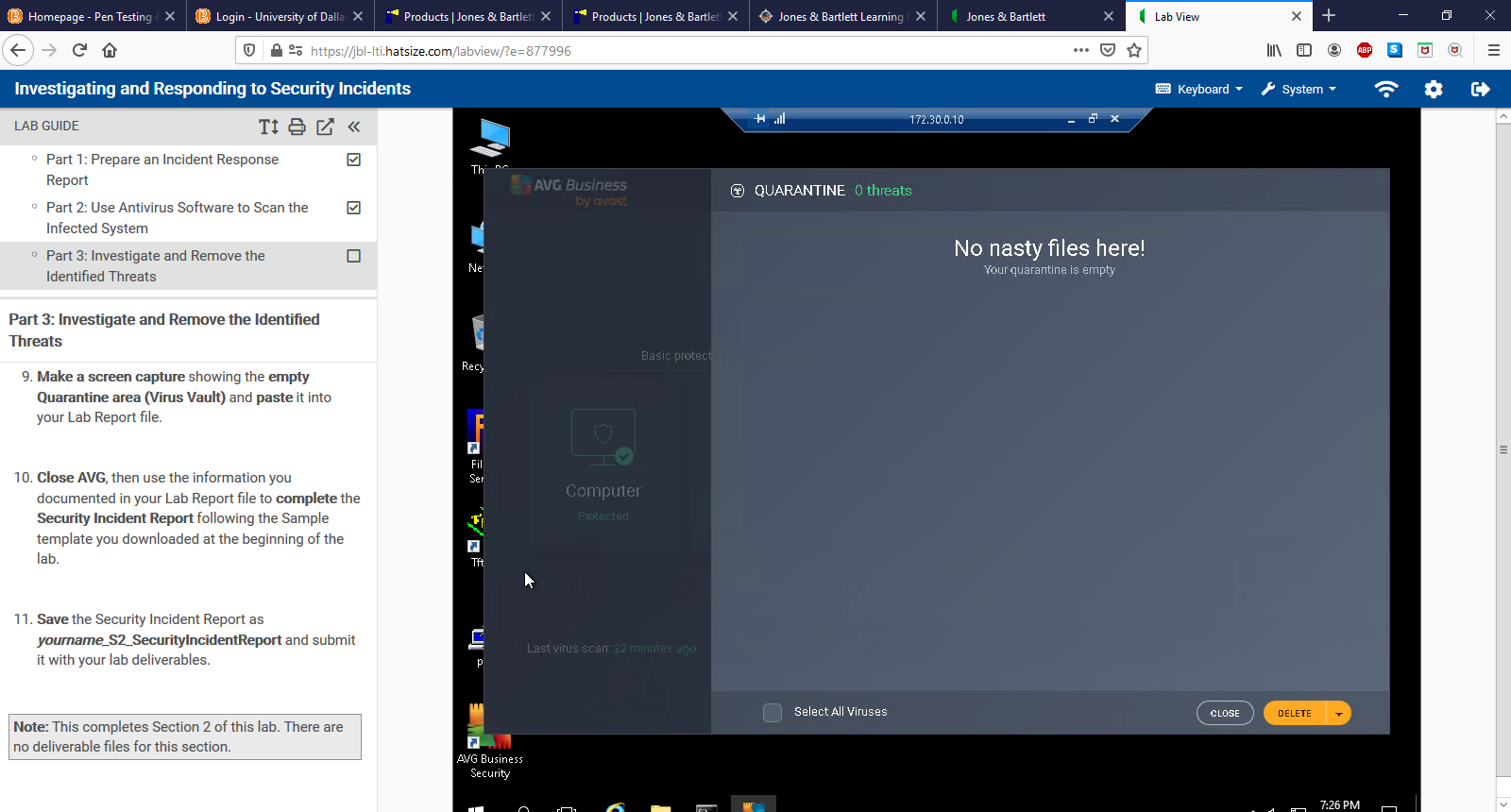
Keycopy is a highly severe threat that tracks all the keystrokes a user types in his or her computer. Keycopy is generally present at the hidden location in the system hard drive and may slow down the victim’s system performance and leads to abrupt shutdown of the computer. In terms of capability, keycopy can change the default homepage of the user and redirects entire searches to a malicious website. Even worse, it may lock the victim’s computer and demand money to recover the problem.

Keycopy is known to be able to corrupt most operating system versions including Windows XP, Vista, Windows 7, and Windows 8.

Eradication

* Obtain the most recent virus definitions for an Antivirus software such as AVG Antivirus software
* Start the Antivirus and Ran a full system scan to make sure it’s scans all files for the malware among others
* When the scan is complete, the Antivirus will display any detected threats, their severity, and the actions taken to contain them. Review the threat details to find any that are associated with KEYCOPY.COM file. It is usually located in C:\Windows\System32\KEYCOPY.COM
* Remove the threat completely by manually selecting it from the quarantine area of the antivirus software. This will delete the malicious software from the victim’s computer.

1. Make a screen capture showing the empty Quarantine area (Virus Vault) and paste it into your Lab Report file.



1. Other Deliverables
   * Natnael\_S2\_SecurityIncidentReport