# CY5210 Case Study 2 Scenario

**Background**

***Capital Computing*** is a distributor of computer related products for corporate, small business, and educational clients. The company is currently working on several new products that the production and marketing departments expect to bring in a significant amount of market share, when the products are released at the start of the 2019 fiscal year (September 2018). If the product designs, memos, components and involved expenses of these products are leaked or shared with external entities, the company could lose a significant advantage over competitors. The company could lose millions of dollars in potential revenue if their proprietary information was exposed. Capital Computing marks all company products by identifying the sensitivity of the data and classifying the filename or entering headers and footers labeling the data accordingly (Sensitive, Proprietary, or For Official Use Only – FOUO).

# Incident

Ethan Thomas has worked at Capital Computing for almost ten years as a Senior Consultant working on some of the companies most profitable projects. The majority of the projects and products produced by Capital Computing are high risk, high gain. This means that although not all projects are completed through production, those that are create a significant amount of market share for the company.

Ethan Thomas reported that his primary Windows system was running slow and had several anti-virus alerts identifying various versions of adware and malware installed. This system has been wiped and re- imaged by the Service Desk department. Mr. Thomas was given a new updated Windows 10 system for use on the corporate network while his infected system was analyzed by the Cyber Investigations Team on 27 March 2018.

Mr. Thomas’s supervisor, Daniel Smith reported to the Human Resources department that other employees had informed him that Ethan was drafting his notice and had planned to work for a potential competitor, ***Next Generation Computing***. The companies Cyber Investigations Team is also responsible for identifying insider threat cases and investigating potential data exposure.

# Scope

A remote acquisition of Mr. Thomas’s new Windows 10 system was performed with AccessData Enterprise on 3 April 2018. The Director of Cybersecurity has asked for a full forensic report on any potential data loss, exposure, or company proprietary data that may have been leaked by Mr. Thomas. The potential timeframes, methods, and tools used to exfiltrate this data should also be reported with the appropriate filenames and data types. Make sure you identify the artifacts proving knowledge of, access to, and removal of any proprietary data as well as any attempts to cover up any evidence.