

Reflexión Act 4.3

Los grafos son un tipo de estructura de dato en los que se pueden llegar a encontrar adyacencias o vinculaciones entre dos datos a través de un arco o conexión. Éstos suelen ser utilizados en las aplicaciones como Google Maps o Waze para representar las calles y las conexiones entre éstas.

La situación problema que se está abordando en la clase es sobre los ataques cibernéticos y el poder identificar cuando este tipo de situaciones se dan. Entonces, durante la entrega 4.3 utilizamos los grafos para poder almacenar información que posiblemente pueda servirnos para identificar si se está llevando a cabo un ataque cibernético.

En una situación real, ya contando con los logs como es el caso de esta evidencia, es posible almacenar la información sobre qué computadoras tuvieron alguna conexión con otra utilizando para esto la IP. Al momento de guardar las conexiones que se llevaron a cabo, también es importante guardar la información como la hora, fecha y el motivo por el cual se presentó un error al intentar acceder a una determinada computadora. Ya teniendo las conexiones y la información, utilizando el método Max Heap, como se realizó en esta entrega, es posible obtener las computadoras que hayan tenido un mayor número de vinculaciones fallidas para así analizar detenidamente cada IP y así poder identificar si realmente se trata de un ataque cibernético.