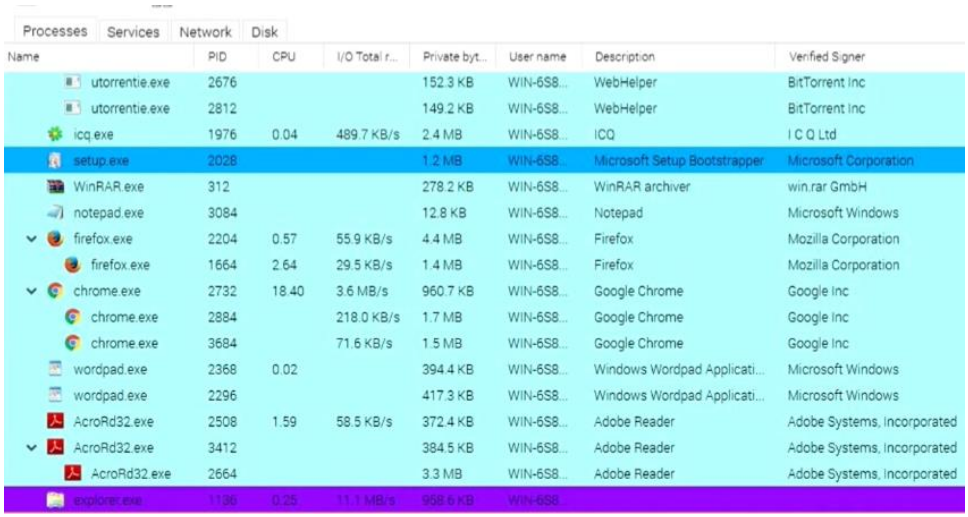
Curso de triage informático

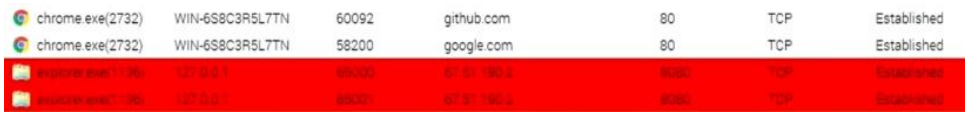
El triage informático se define como un proceso para analizar y priorizar las respuestas ante incidentes de seguridad informática, en base a la gravedad de su condición; escogiendo, separando y analizando evidencias, de una forma rápida, para identificar, contener y erradicar el daño, e iniciar la pertinente investigación y análisis forense del Sistema.

En este curso he aprendido a analizar los procesos activos en nuestro ordenador aplicando la heurística para detectar posibles casos de malware.

En izquierda se puede ver como la ejecución de Chrome tiene una descripción y una firma fiables mientras que el de la derecha no tiene ninguno de los dos. Además el proceso de la derecha se está ejecutando en TEMP lo cual no es común, todo esto nos hace sospechar que se pueda tratar de un proceso malicioso.



Viendo los procesos activos podemos ver como el proceso explorer.exe resaltado en morado a establecido una conexión y no tiene una descripción ni una firma por lo cual debemos analizar ese proceso más detenidamente.



Analizando más detenidamente vemos que ha establecido una conexión a una dirección ip y no a un dominio como lo han hecho los procesos de Chrome. Esto nos indica que se trata de un proceso malicioso.

Además, en este curso se enseña como de detectar posibles emails falsos viendo si el dominio de la dirección de email no coincide con el de la empresa, si hay faltas de ortografía o de

concordancia, si el correo solicita información personal, si el asunto del correo es de máxima alerta. También suelen contener archivos adjuntos. Viendo todo esto podremos hacernos una idea de si un correo puede ser malicioso.