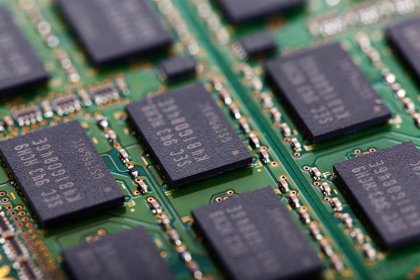
**Análisis de Memoria Volátil de un Sistema Windows**



Daniel Escaño Hernández CET Ciberseguridad

# **1. Índice:**

[**1. Índice:**](#_lmwzrhyaxgtw) **1**

[**2. Cuestiones**](#_g59i8ewd3ed3) **2**

[**2.1 ¿Cuál es el perfil de la memoria proporcionada?**](#_5d38uxjyswtl) **2**

[**2.2 ¿Qué identificador de proceso tiene notepad.exe?**](#_yg73ik5isboe) **2**

[**2.3 ¿Cuál es el identificador del proceso padre de DumpIt.exe?**](#_cjt9fahybett) **2**

[**2.4 ¿Cuáles son los procesos hijos del proceso explorer.exe?**](#_qcjam1cgh9md) **2**

[**2.5 ¿Qué IP tiene la máquina en el momento en el que la memoria RAM fue adquirida?**](#_303mfgyxsrzp) **3**

[**2.6 ¿A qué dirección IP, en su puerto 443, se accedió desde el navegador chrome en el equipo?¿Qué uso se da a ese puerto?¿A qué organización pertenece esa dirección IP?**](#_xt2gq1x0ijo0) **3**

[**2.7 ¿A qué organización pertenece la otra IP accedida desde ese mismo navegador?**](#_na46f1raeiw6) **4**

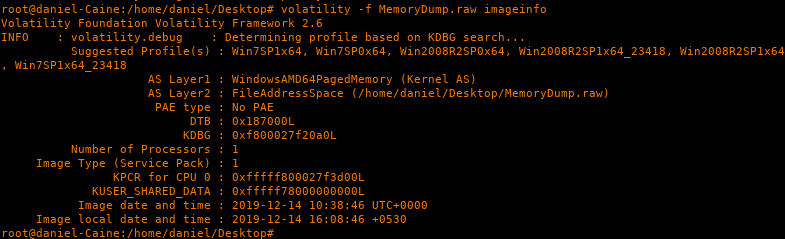
[**2.8 ¿Qué proceso que reside en la memoria está asociado a la librería WINBRAND.dll?**](#_b6n127hcbhey) **5**

[**2.9 Como hemos visto, residía en memoria un proceso relacionado con la terminal. ¿Podrías decirnos qué fue lo primero registrado que se escribió en ella?**](#_4s68mnb4sy0w) **5**

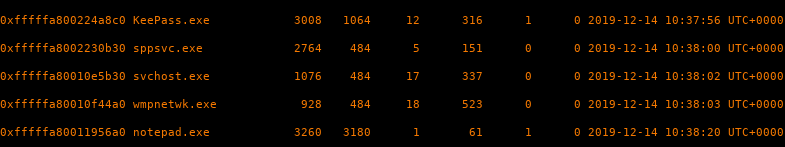
[**2.10 ¿Podrías decir en qué directorio se almacenó la imagen adquirida?**](#_8tsh75dwmhj4) **5**

# **2. Cuestiones**

### **2.1 ¿Cuál es el perfil de la memoria proporcionada?**



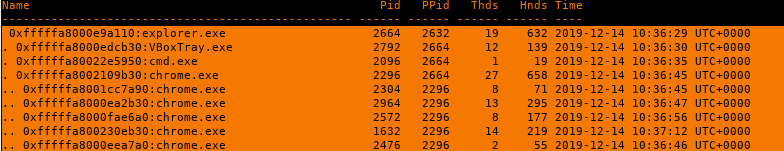
### **2.2 ¿Qué identificador de proceso tiene notepad.exe?**



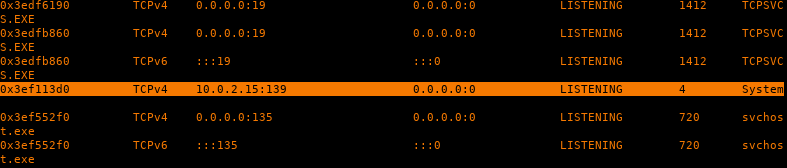
### **2.3 ¿Cuál es el identificador del proceso padre de DumpIt.exe?**



### **2.4 ¿Cuáles son los procesos hijos del proceso explorer.exe?**

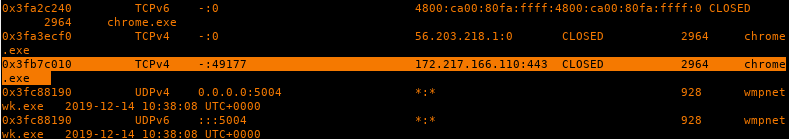


### **2.5 ¿Qué IP tiene la máquina en el momento en el que la memoria RAM fue adquirida?**



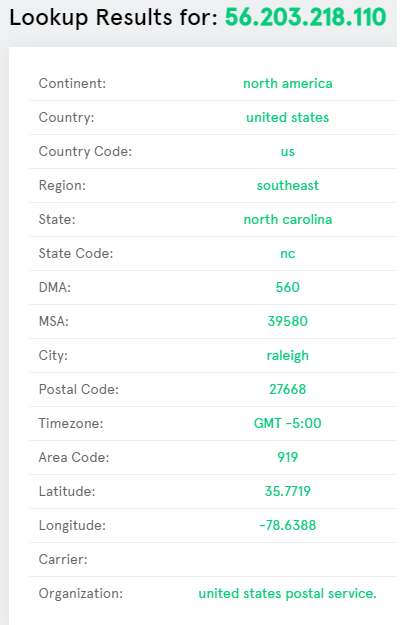
### **2.6 ¿A qué dirección IP, en su puerto 443, se accedió desde el navegador chrome en el equipo?¿Qué uso se da a ese puerto?¿A qué organización pertenece esa dirección IP?**

El puerto 443, normalmente es utilizado para el protocolo HTTPS.





### **2.7 ¿A qué organización pertenece la otra IP accedida desde ese mismo navegador?**

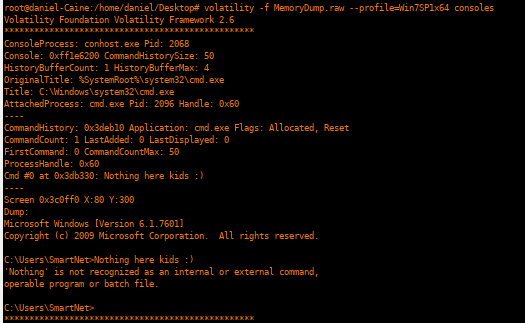


### **2.8 ¿Qué proceso que reside en la memoria está asociado a la librería WINBRAND.dll?**

(Utilice, para mayor comodidad, el comando “Select-String” (junto con el parámetro -context) en Windows, o “grep” en Linux, para filtrar el resultado obtenido al listar las librerías asociadas a procesos)



### **2.9 Como hemos visto, residía en memoria un proceso relacionado con la terminal. ¿Podrías decirnos qué fue lo primero registrado que se escribió en ella?**



### **2.10 ¿Podrías decir en qué directorio se almacenó la imagen adquirida?**

Si atendemos a la salida que ofrece la terminal, podemos ver que también se muestra información de la salida del programa usado para realizar la adquisición de memoria. Atendiendo a esa información,

