**Adquisición de memoria volátil**



Daniel Escaño Hernández CET Ciberseguridad

# **1. Índice:**

[**1. Índice:**](#_lmwzrhyaxgtw) **2**

[**2. Windows 10**](#_g59i8ewd3ed3) **3**

[**2.1 FTK Image:**](#_5d38uxjyswtl) **3**

[**2.2 QuickHash:**](#_tftdadu8uekc) **4**

[**2.3 HxD:**](#_3egvsromnwpy) **5**

[**3. Linux**](#_78z7piud3t5h) **7**

[**3.1 LiME:**](#_3ady58149kfp) **7**

[**3.2 QuickHash (LiME):**](#_9jfwleup7qfm) **8**

[**3.3 Fmem:**](#_413gujf8w8wt) **10**

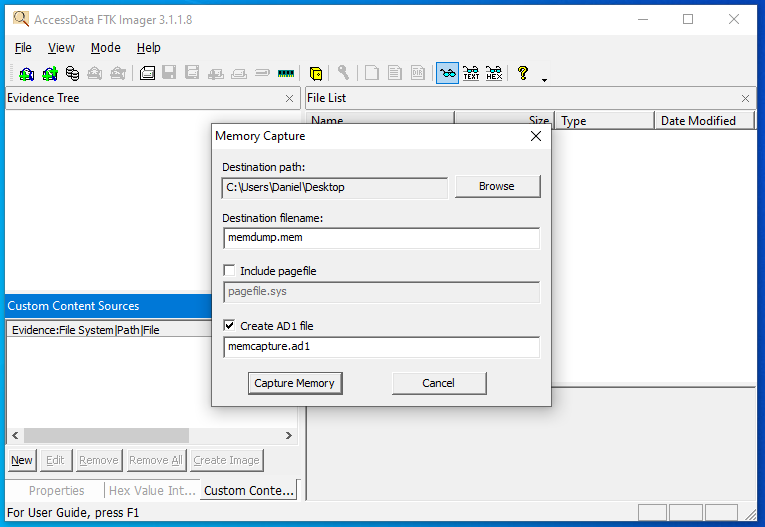
[**3.4 QuickHash (Fmem):**](#_9lnxlcfjibmi) **11**

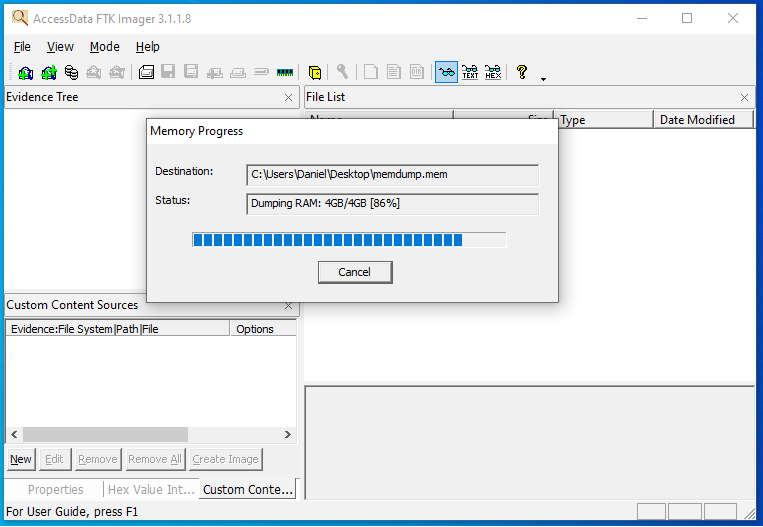
[**3.5 010 Editor:**](#_ela9b0d5ret0) **13**

# **2. Windows 10**

### **2.1 FTK Image:**

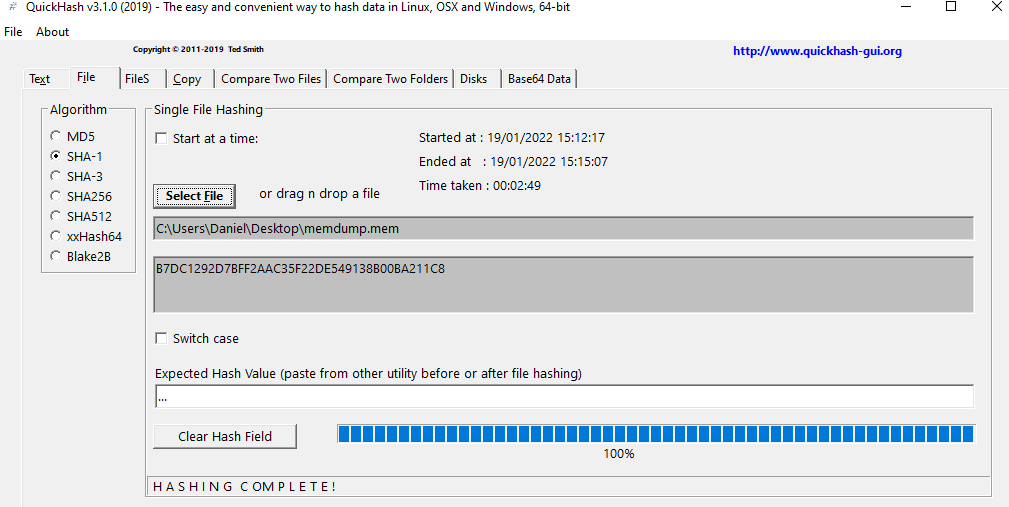
Obtener, con el software FTK Image, la imagen de la memoria volátil en formato RAW. Con extensión “.mem”.

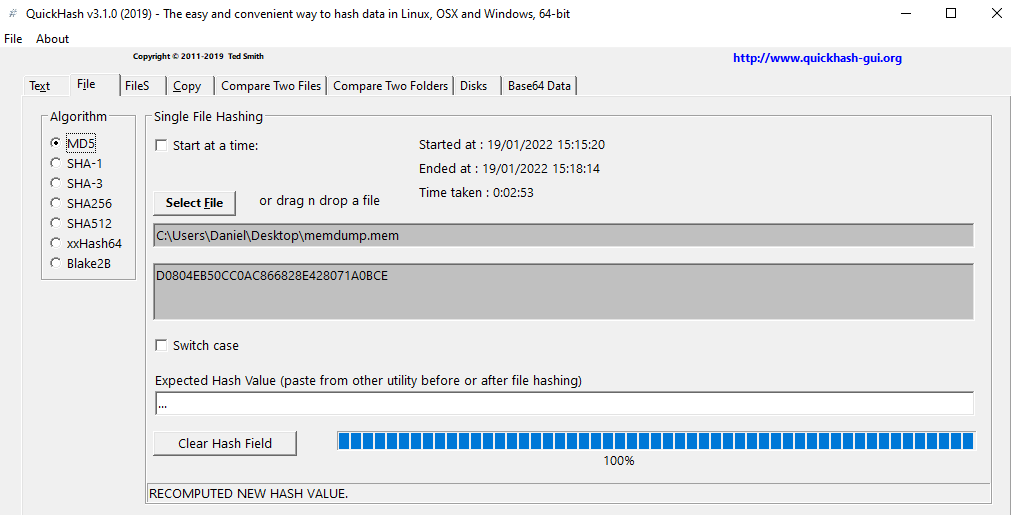


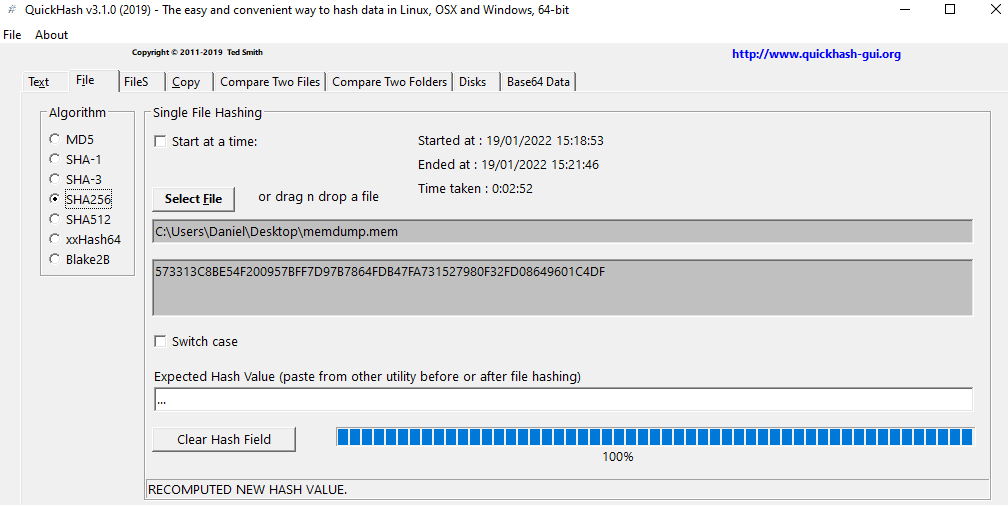


### **2.2 QuickHash:**

Calculamos los códigos MD5, SHA-1 y SHA-256 con la herramienta gráfica QuickHash.

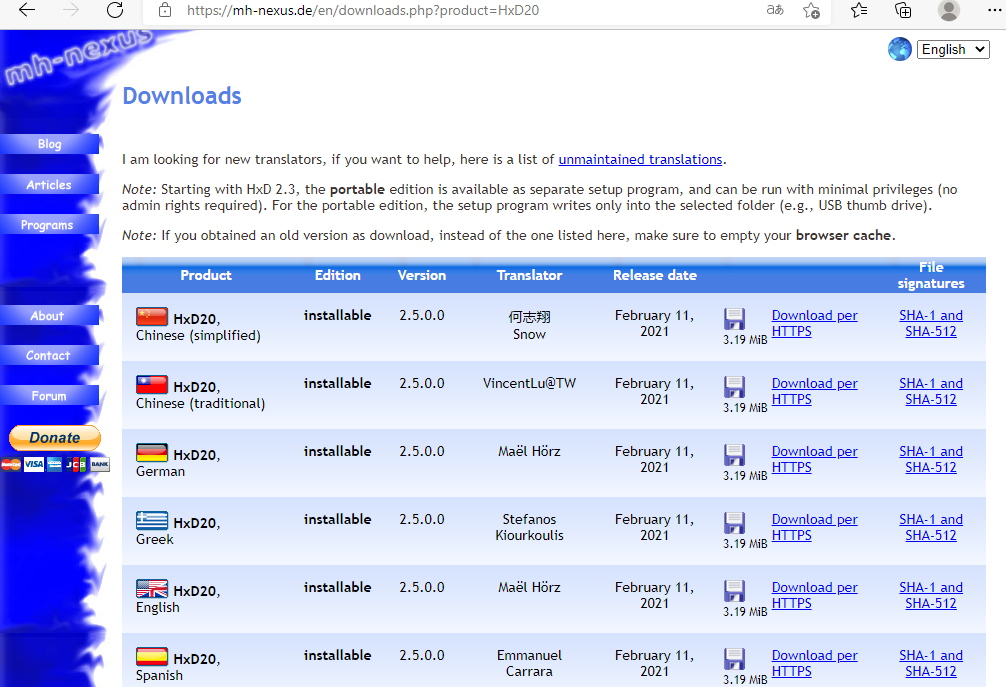


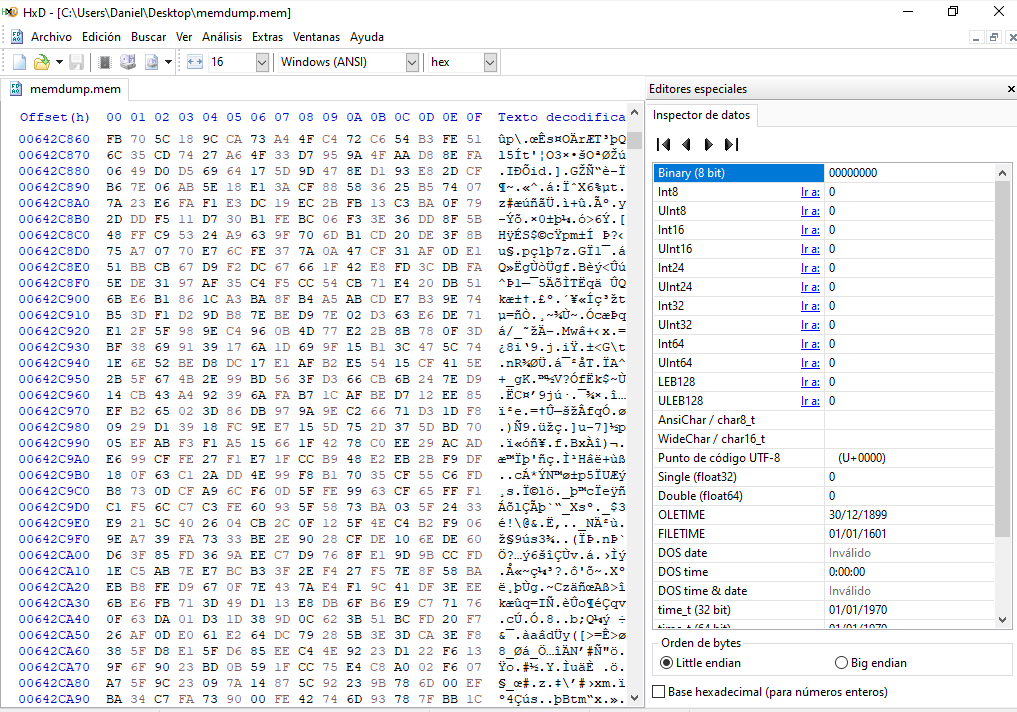




### **2.3 HxD:**

Visualizamos el contenido de la imagen de la memoria volátil obtenida con un visor hexadecimal gráfico.

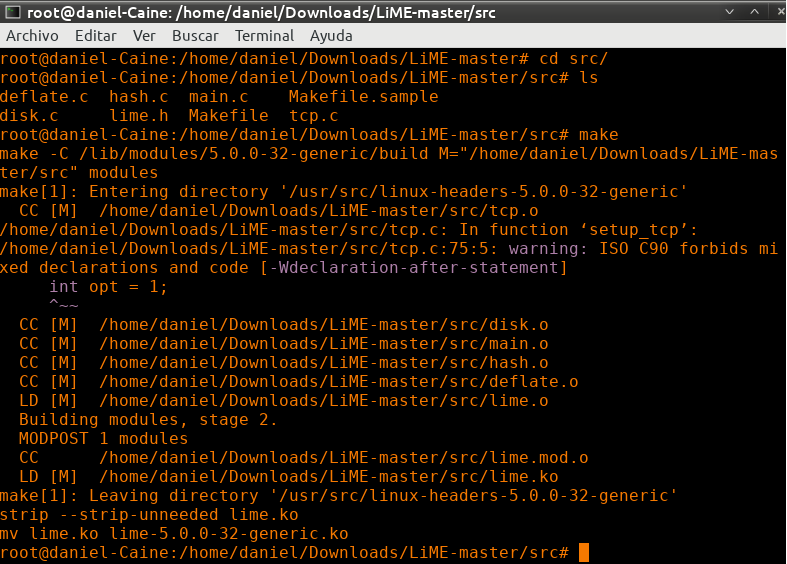


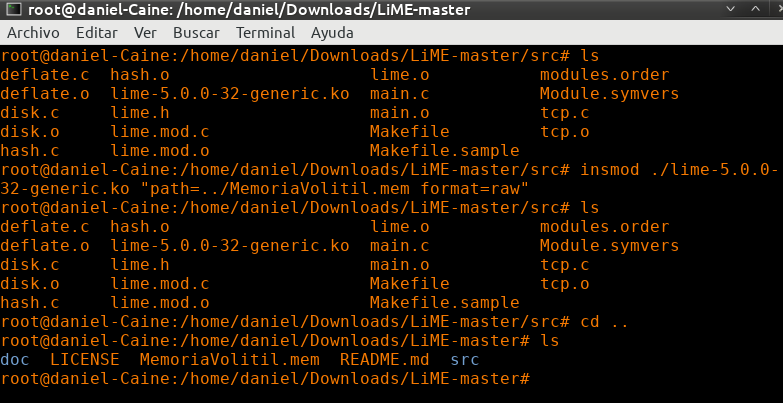


# **3. Linux**

### **3.1 LiME:**

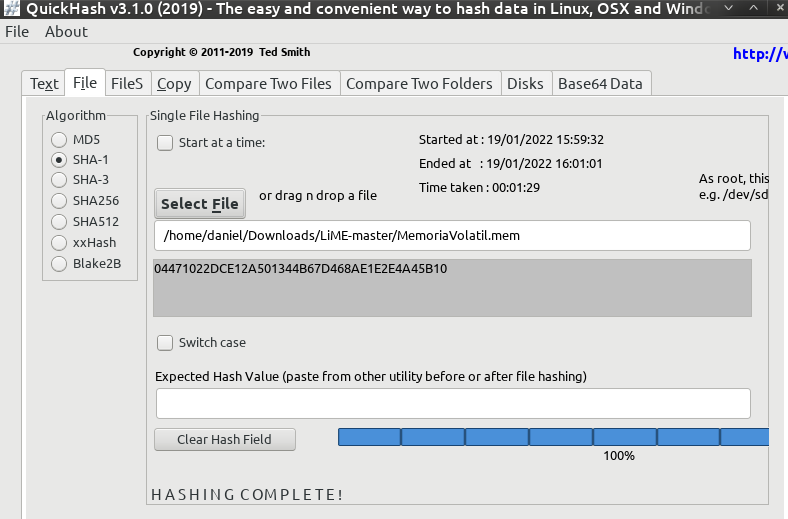
Obtener, con el programa LiME, la imagen de la memoria volátil en formato RAW. Con extensión “.mem”.

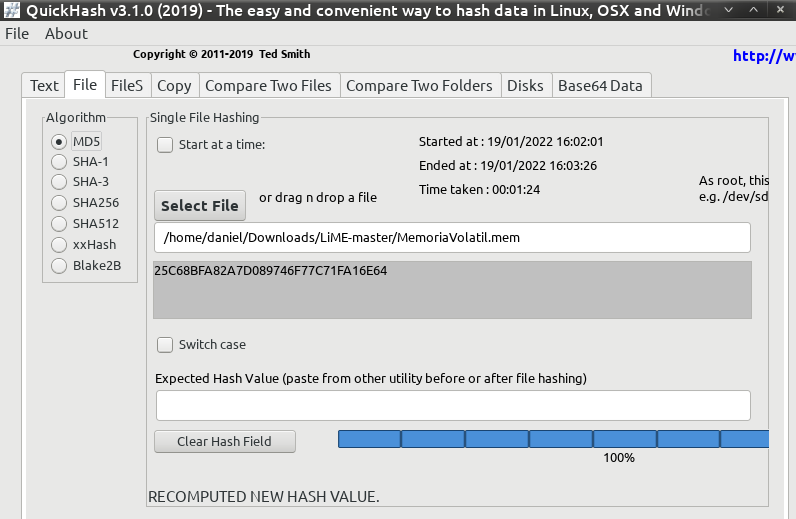


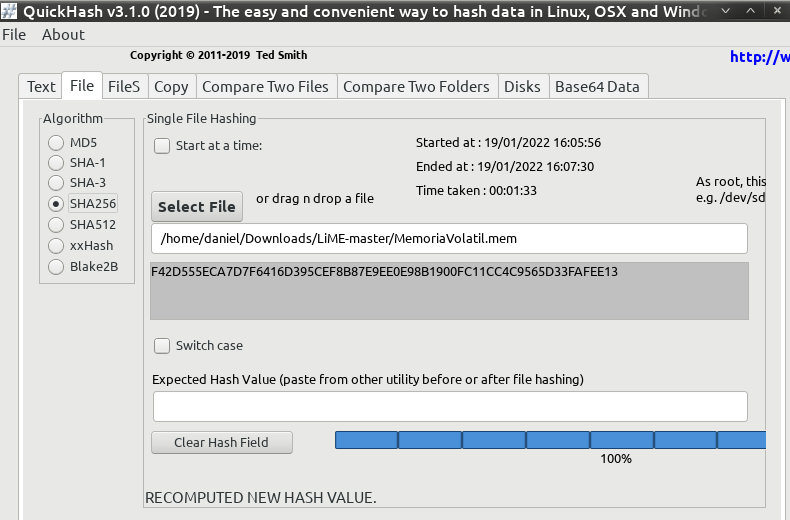


### **3.2 QuickHash (LiME):**

Calculamos los códigos MD5, SHA-1 y SHA-256 con la herramienta gráfica QuickHash.

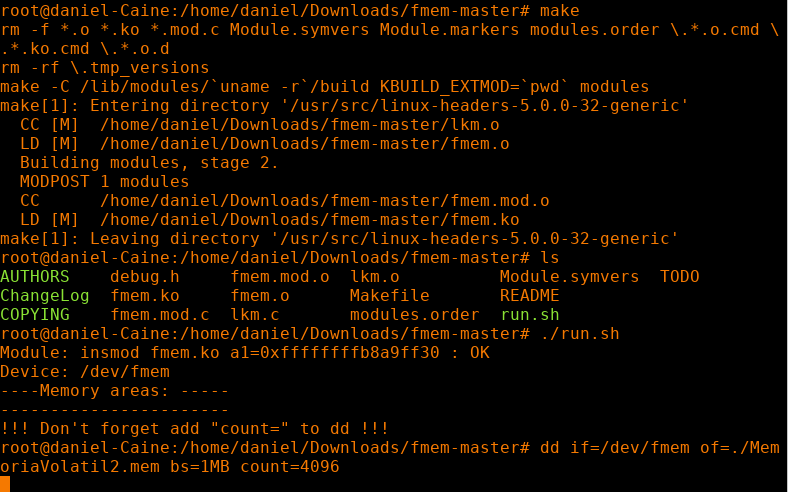


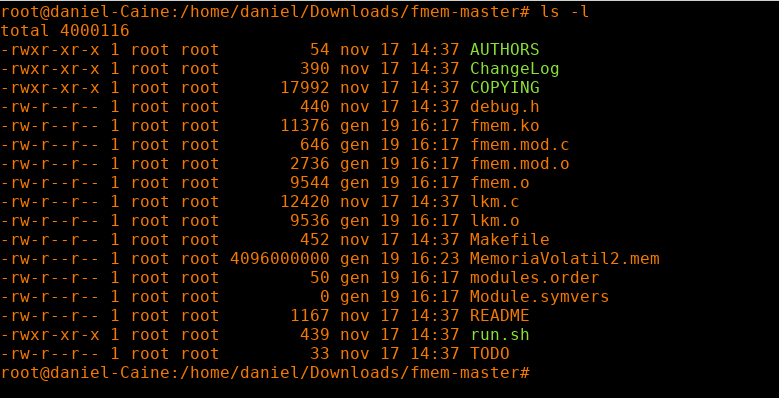




### **3.3 Fmem:**

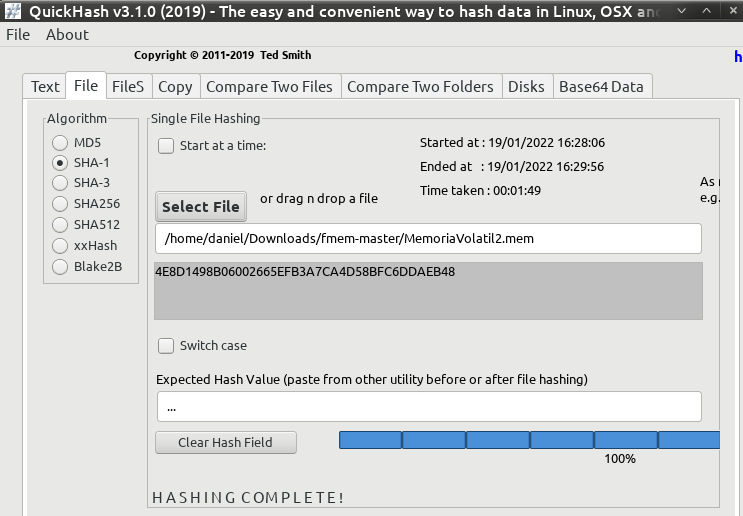
Obtener, con el programa Fmem, la imagen de la memoria volátil en formato RAW. Con extensión “.mem”.

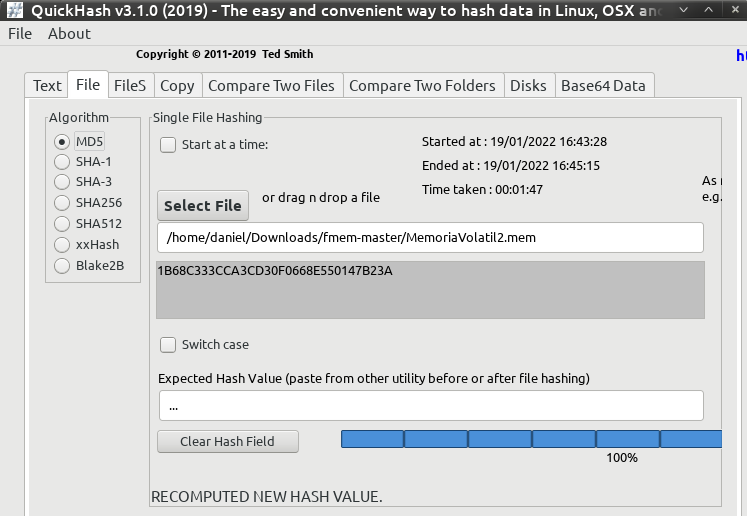


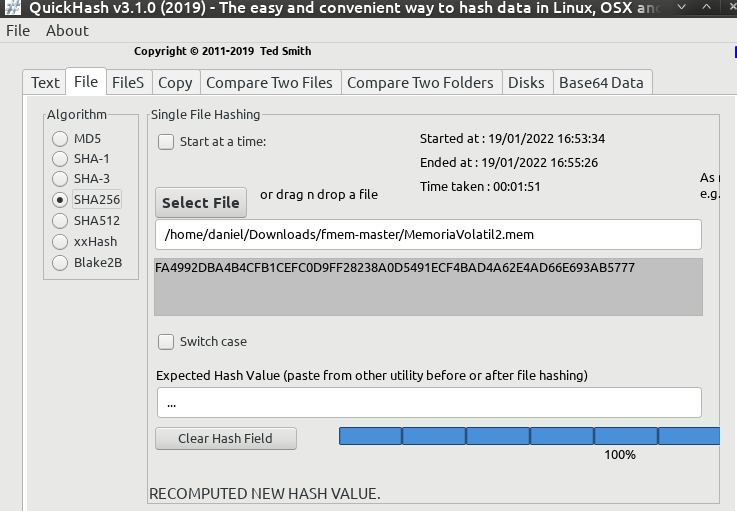


### **3.4 QuickHash (Fmem):**

Calculamos los códigos MD5, SHA-1 y SHA-256 con la herramienta gráfica QuickHash.







### **3.5 010 Editor:**

Visualizamos el contenido de la imagen de la memoria volátil obtenida con un visor hexadecimal gráfico, en este caso 010 Editor.

