**Actividad Análisis Disco Windows**



Daniel Escaño Hernández CET Ciberseguridad

# **1. Índice:**

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

[**2. Cuestiones**](#_g59i8ewd3ed3) **3**

[**2.1 ¿Cuál es el código MD5, SHA1 y SHA256 de la fuente de evidencia proporcionada?**](#_5d38uxjyswtl) **3**

[**2.2 ¿Cuál es el usuario primario del sistema?**](#_shtyqoc7kn2j) **3**

[**2.3 ¿Cuándo fue la última vez que este usuario hizo login en el sistema?**](#_r3fob9ymcy1g) **3**

[**2.4 ¿Cuál es el password de este usuario?**](#_sjjmfdoahpe7) **4**

[**2.5 ¿Qué usuarios hay registrados en el sistema?**](#_cd7kyt3rktmj) **4**

[**2.6 ¿El sistema tiene aplicaciones de la Microsoft Store instaladas? Si las tiene indique al menos 3.**](#_z8vw7tsuq4r3) **4**

[**2.7 ¿A qué aplicaciones se tenía acceso directo desde el escritorio si miramos en el árbol de directorios?**](#_hg5a6b48h61r) **6**

[**2.8 ¿A qué aplicaciones se tenía acceso directo desde el escritorio si miramos en el registro del usuario principal? ¿Se corresponde esto con lo comentado en el punto anterior?**](#_twwvlqadjdge) **6**

[**2.9 ¿Podrías averiguar qué programa se ejecutó en el sistema, por parte del usuario principal, el 17 de marzo de 2019 a las 20:56?**](#_y00kccuz7o1e) **7**

[**2.10 ¿Cuándo es la última vez que se abrió el bloc de notas?**](#_3fcc1wux5lqx) **7**

[**2.11 ¿Qué programa se usaba por defecto para abrir archivos con extensión .docx?**](#_2awss0y2d8zl) **8**

[**2.12 Si nos fijamos en los archivos abiertos recientemente…¿Qué archivo fue abierto mediante cuadro de diálogo desde el Dropbox del usuario principal?**](#_ljn3cdbg0932) **8**

[**2.13 ¿Con qué programa se abrió un archivo de extensión .webp mediante cuadro de diálogo? ¿En qué directorio estaba?**](#_ynfo5bbbx4v2) **9**

[**2.14 ¿Qué archivos, directorios o aplicaciones se abrieron mediante la caja de ejecutar (windows+R)**](#_rfj7ufe2keu5) **9**

[**2.15 Lista los archivos, con sus rutas completas, que fueron abiertos con Microsoft Word, así como la fecha en que estos fueron abiertos.**](#_1icv1shd0nxo) **9**

[**2.16 Indica con qué finalidad se escribió por última vez en la barra de direcciones de Windows Explorer.**](#_pz7sd0sks1r5) **10**

[**2.17 ¿En qué fecha fue abierto por última vez un archivo de extensión .dotx?¿Cuál era su nombre?**](#_vvz0ofgb3c4s) **10**

[**2.18 Lista los programas que se ejecutan al inicio de sesión del usuario principal y el directorio donde se encontraban.**](#_dxlozwp58hoh) **11**

[**2.19 ¿Cuáles son las letras de los dispositivos montados en el sistema?**](#_svkbt012pdgl) **11**

[**2.20 Indica el modelo de tarjeta de red que tenía el equipo del que fue obtenida la fuente de evidencia con la que estamos trabajando.**](#_6f0oo3o27jej) **12**

[**2.21 ¿Cuándo fue la última vez, y la primera, que se inició sesión correctamente en una cuenta del sistema? Indicar fecha y hora.**](#_ncvoc7jydyar) **12**

[**2.22 ¿Qué nombre tenía el equipo en cada uno de estos eventos anteriores?**](#_ez8gzgh0hqn0) **13**

[**2.23 ¿Cuál es el primer evento con nivel de error registrado en los eventos del sistema?**](#_5z662fystt02) **14**

[**2.24 Dentro del directorio que almacena los ficheros con los que el usuario ha interactuado recientemente, encuentra el link que apunta a un fichero accedido el 09/02/2019 a las 21:09:41 que no sea un template.**](#_hlv95tolvctb) **14**

[**2.26 Si nos fijamos en los Jumplist del equipo del que se tomó la muestra, ¿Cuáles son los archivos que tenían acceso rápido para la aplicación Microsoft Word 16?**](#_uoq550rced5j) **15**

[**2.27 Usando la misma información que en el punto anterior, ¿Cuáles serían los accesos rápidos que tendría el usuario principal en el explorador de Windows?**](#_cswrwf8183to) **15**

[**2.28 ¿Qué URL tenía como acceso directo en el navegador Edge y que fue modificada por última vez el 19 de febrero de 2019?**](#_kp4rpz38mfow) **16**

[**2.29 ¿Cuándo fue creado el archivo “Get Started with Dropbox Paper.url” que se encuentra en el directorio Dropbox del usuario principal del sistema?**](#_2zyf8btpikfc) **16**

[**2.30 ¿Cuál es el tamaño lógico y físico del archivo alpy.png?**](#_efwenufm8jh4) **17**

[**2.31 Cuándo fué la última vez que el usuario principal hizo login en github?**](#_pi5qj9yf0p3g) **17**

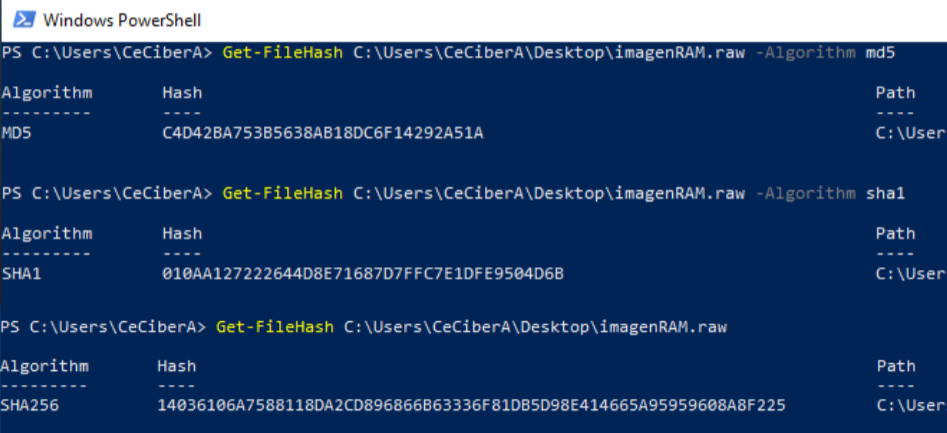
[**2.32 Parece que al usuario principal le preocupaba la seguridad de su equipo. ¿De qué web se descargó un aintimalware para tratar este problema?**](#_9pay08t3bnyd) **18**

[**2.33 A estas alturas ya nos habremos dado cuenta de que al usuario principal le gustan las Alpacas, pero ¿que parte de este animal quería saber si era suave? ¿Cómo lo podemos saber?**](#_uw5gp58ag7ds) **19**

[**2.34 Si nos fijamos en la papelera de reciclaje de la unidad externa de la fuente de evidencia, indica toda la información que puedas sobre lo que encuentres.**](#_n5ojfa50c9ly) **20**

# **2. Cuestiones**

### **2.1 ¿Cuál es el código MD5, SHA1 y SHA256 de la fuente de evidencia proporcionada?**



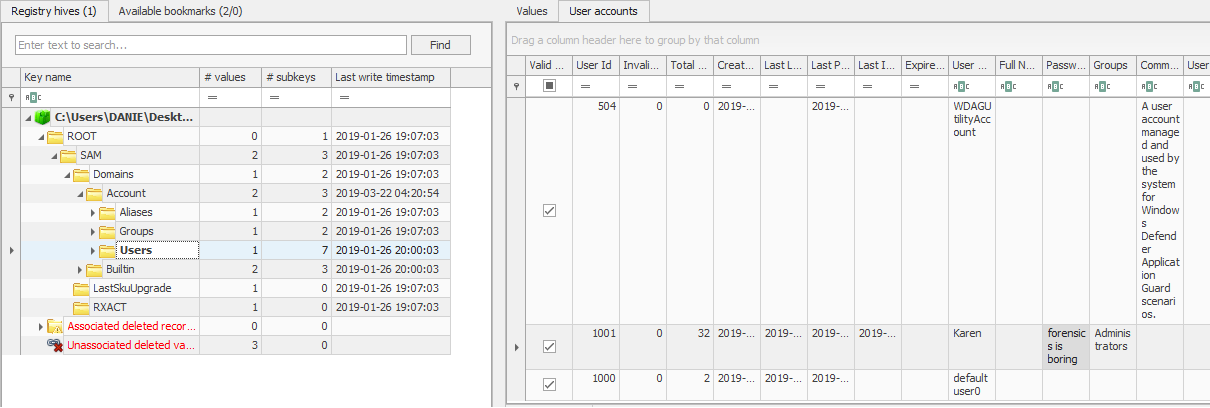
### **2.2 ¿Cuál es el usuario primario del sistema?**

Karen

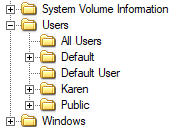
### **2.3 ¿Cuándo fue la última vez que este usuario hizo login en el sistema?**



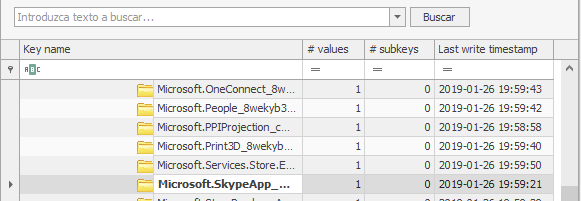
### **2.4 ¿Cuál es el password de este usuario?**

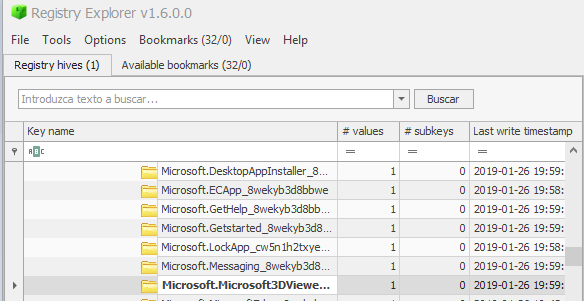


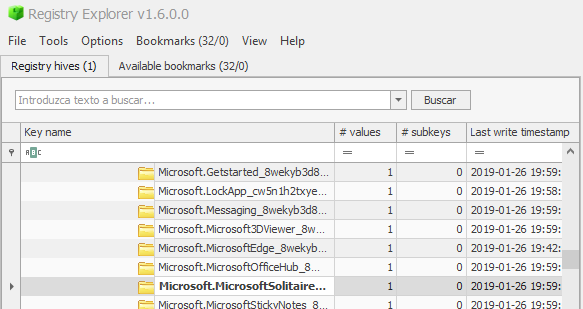
### **2.5 ¿Qué usuarios hay registrados en el sistema?**



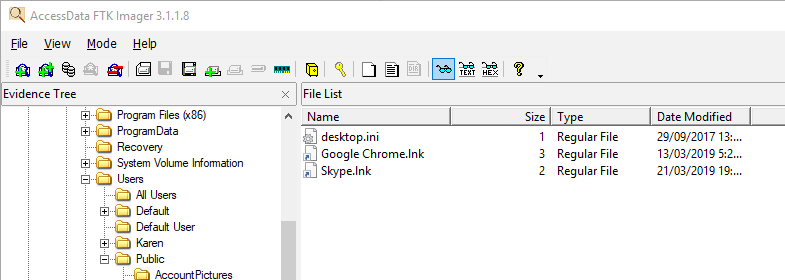
### **2.6 ¿El sistema tiene aplicaciones de la Microsoft Store instaladas? Si las tiene indique al menos 3.**



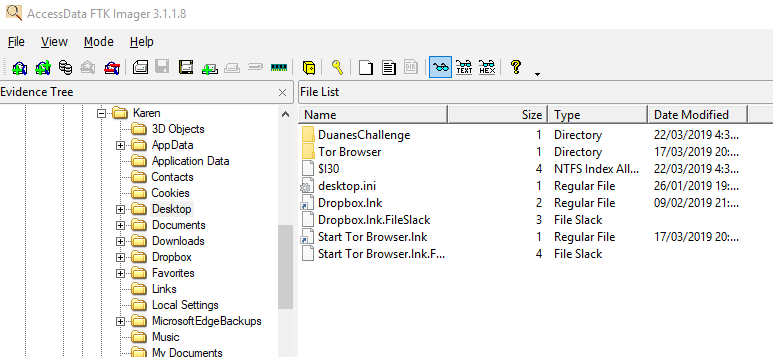




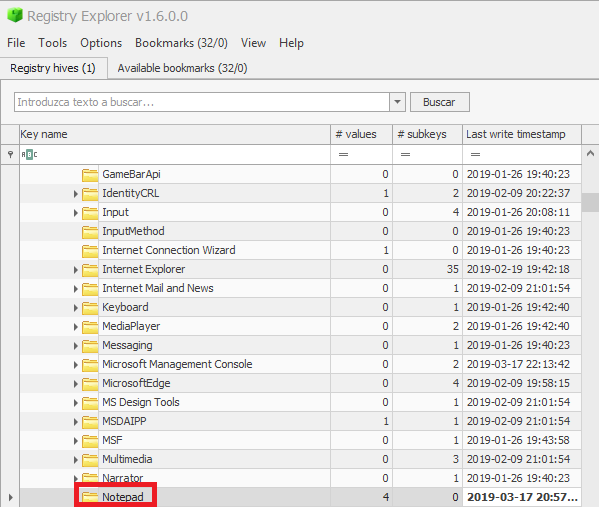
### **2.7 ¿A qué aplicaciones se tenía acceso directo desde el escritorio si miramos en el árbol de directorios?**



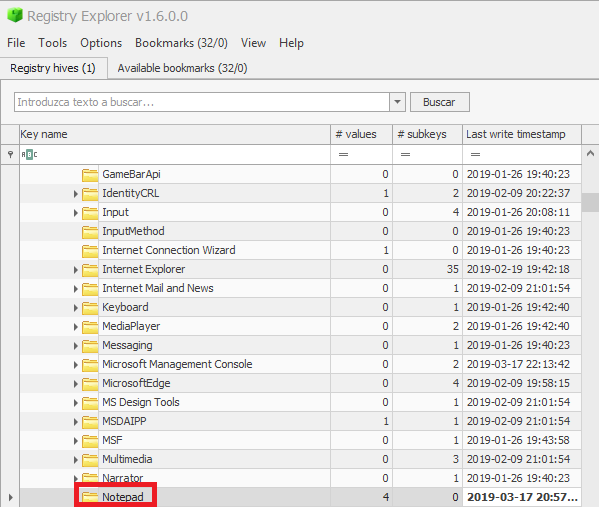
### **2.8 ¿A qué aplicaciones se tenía acceso directo desde el escritorio si miramos en el registro del usuario principal? ¿Se corresponde esto con lo comentado en el punto anterior?**



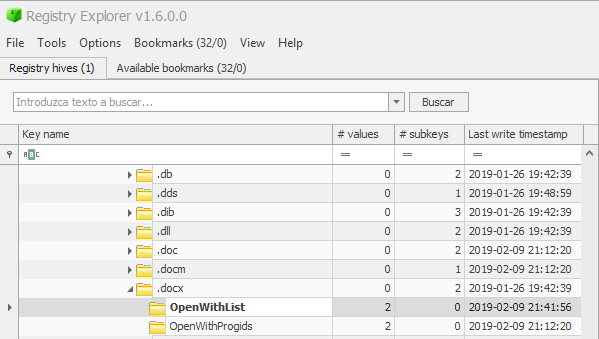
### **2.9 ¿Podrías averiguar qué programa se ejecutó en el sistema, por parte del usuario principal, el 17 de marzo de 2019 a las 20:56?**



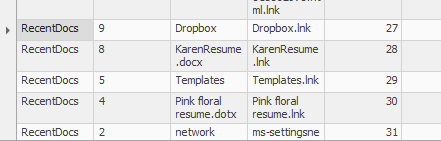
### **2.10 ¿Cuándo es la última vez que se abrió el bloc de notas?**



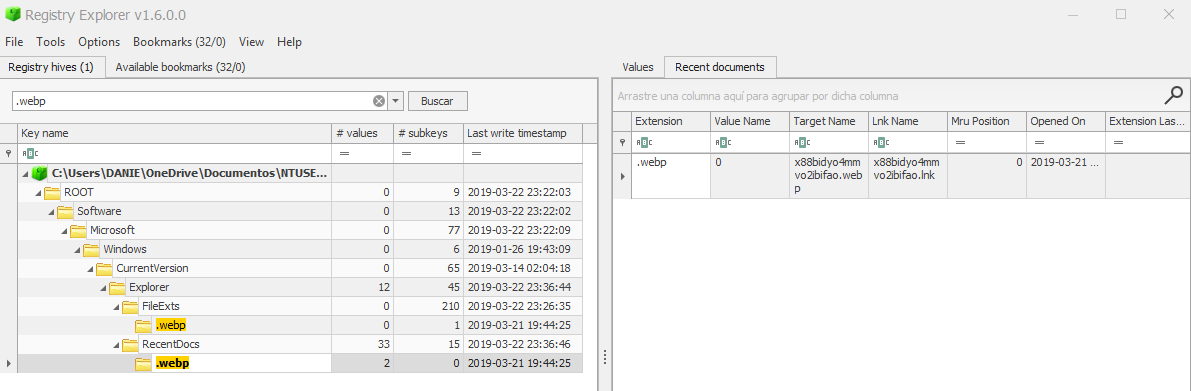
### **2.11 ¿Qué programa se usaba por defecto para abrir archivos con extensión .docx?**



### **2.12 Si nos fijamos en los archivos abiertos recientemente…¿Qué archivo fue abierto mediante cuadro de diálogo desde el Dropbox del usuario principal?**



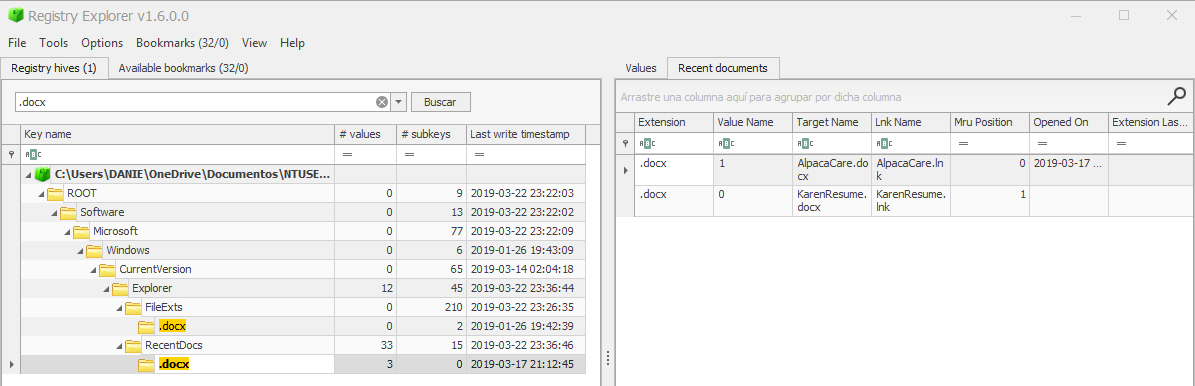
### **2.13 ¿Con qué programa se abrió un archivo de extensión .webp mediante cuadro de diálogo? ¿En qué directorio estaba?**



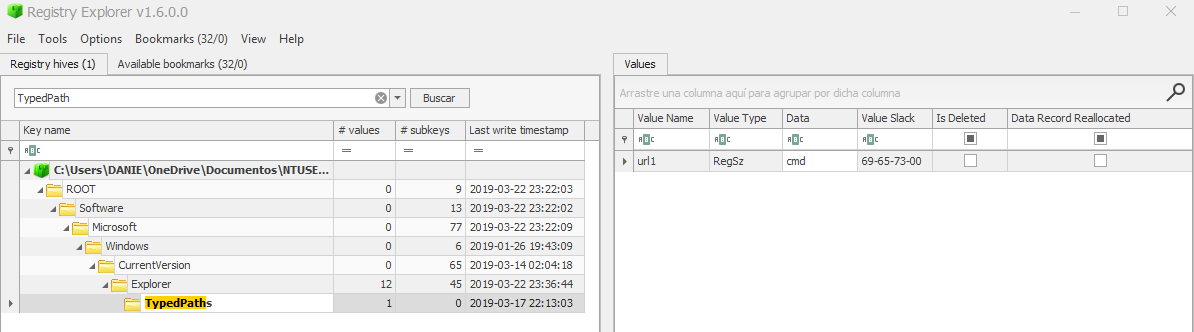
### **2.14 ¿Qué archivos, directorios o aplicaciones se abrieron mediante la caja de ejecutar (windows+R)**

### 

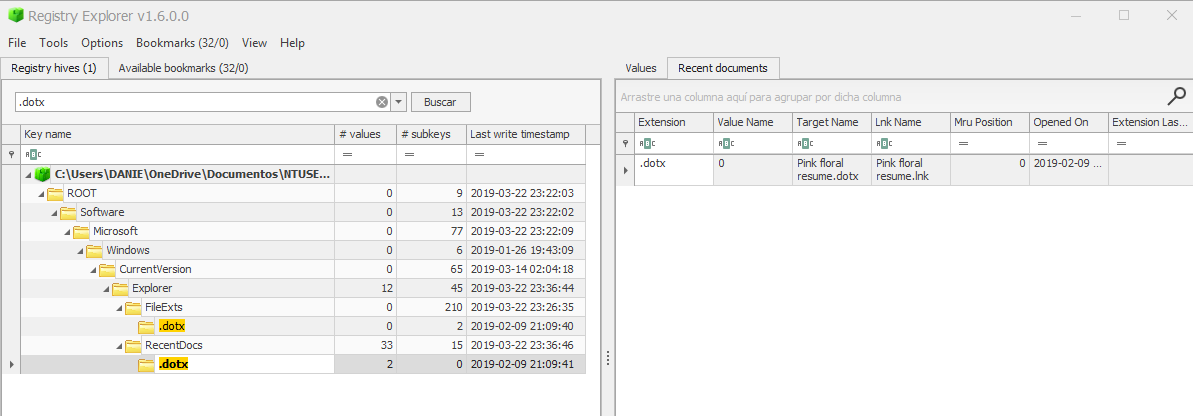
### **2.15 Lista los archivos, con sus rutas completas, que fueron abiertos con Microsoft Word, así como la fecha en que estos fueron abiertos.**



### **2.16 Indica con qué finalidad se escribió por última vez en la barra de direcciones de Windows Explorer.**



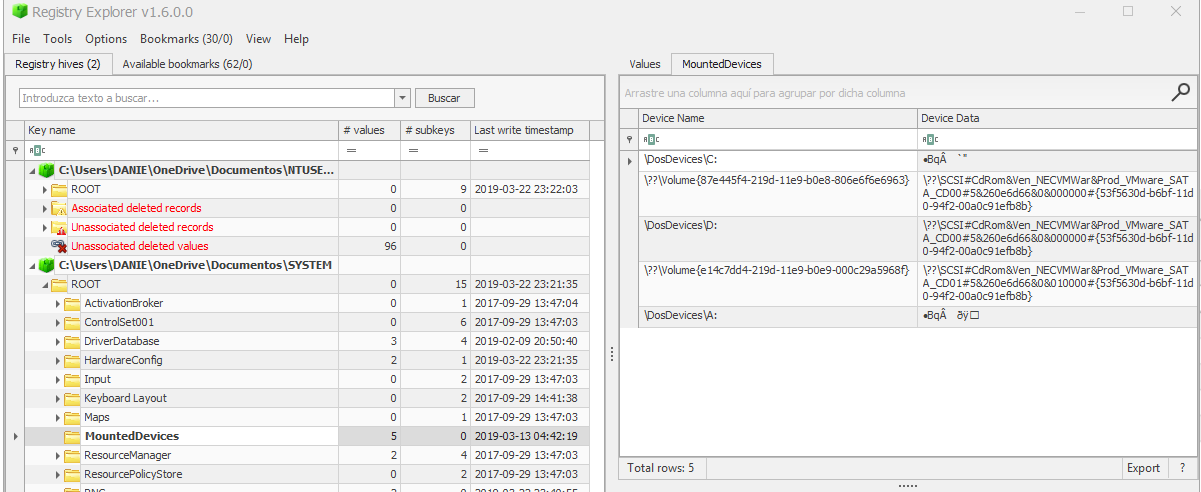
### **2.17 ¿En qué fecha fue abierto por última vez un archivo de extensión .dotx?¿Cuál era su nombre?**



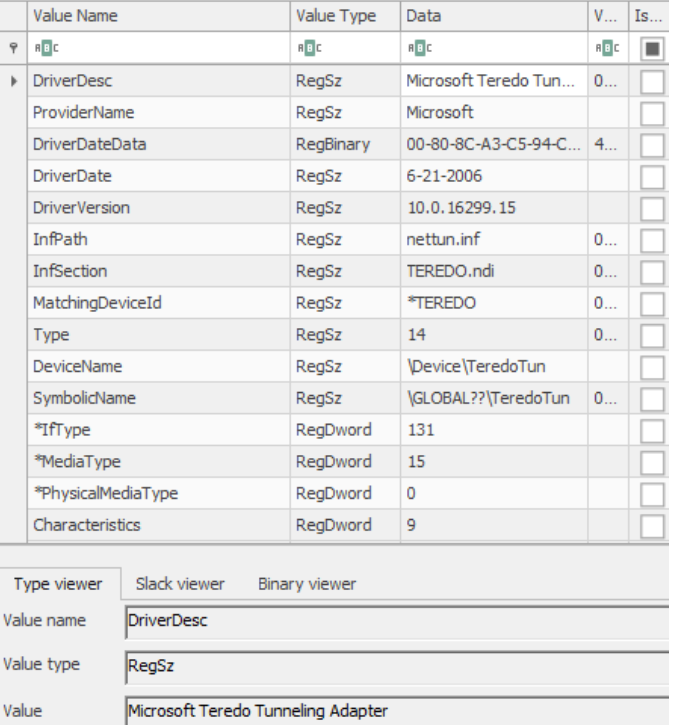
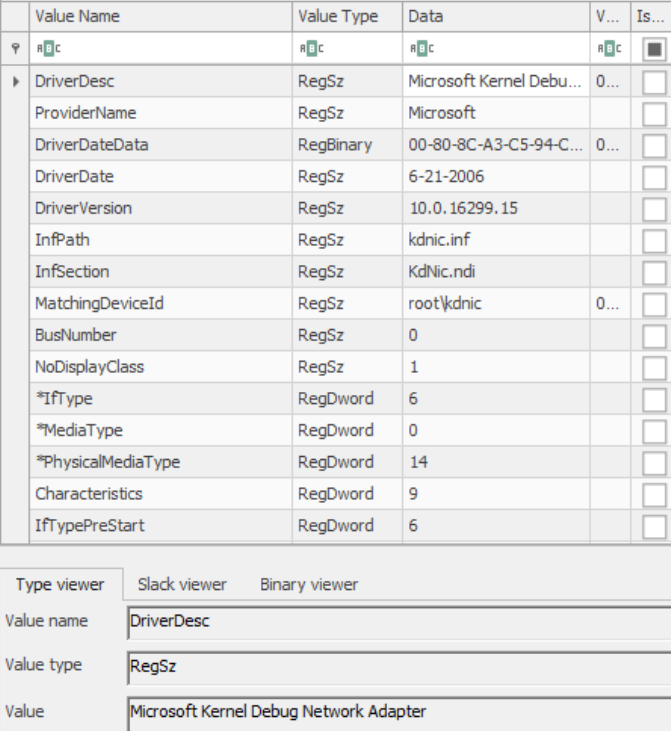
### **2.18 Lista los programas que se ejecutan al inicio de sesión del usuario principal y el directorio donde se encontraban.**

### 

### **2.19 ¿Cuáles son las letras de los dispositivos montados en el sistema?**

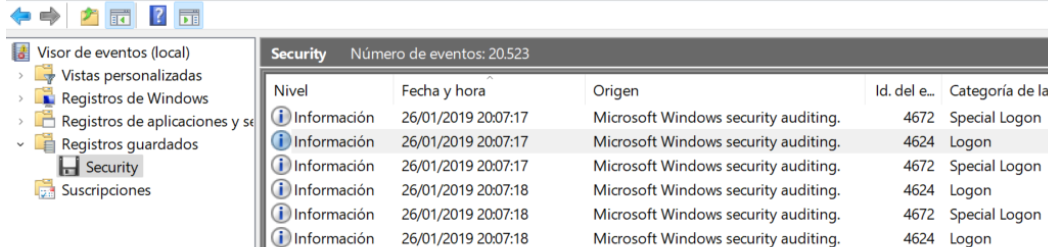


### **2.20 Indica el modelo de tarjeta de red que tenía el equipo del que fue obtenida la fuente de evidencia con la que estamos trabajando.**

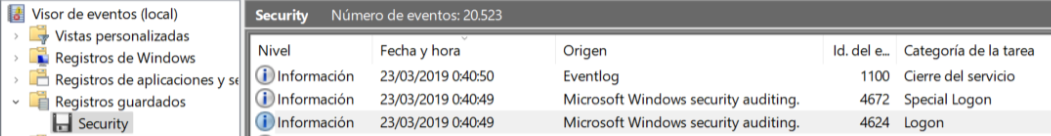


### **2.21 ¿Cuándo fue la última vez, y la primera, que se inició sesión correctamente en una cuenta del sistema? Indicar fecha y hora.**

Primera vez: 26/1/2019



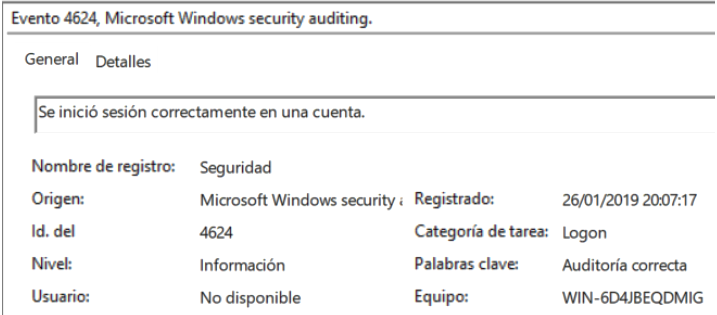
Última vez: 23/3/2019



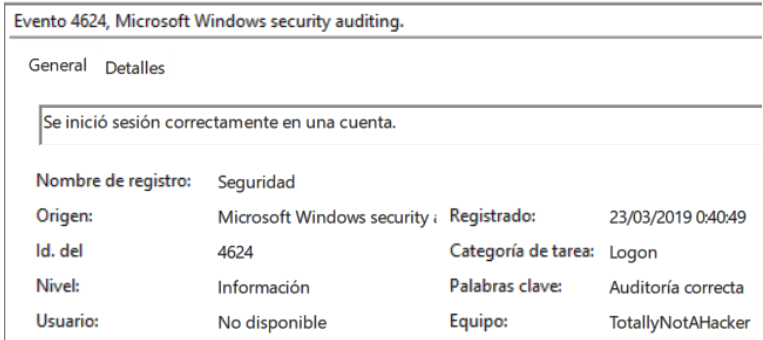
### 

### **2.22 ¿Qué nombre tenía el equipo en cada uno de estos eventos anteriores?**

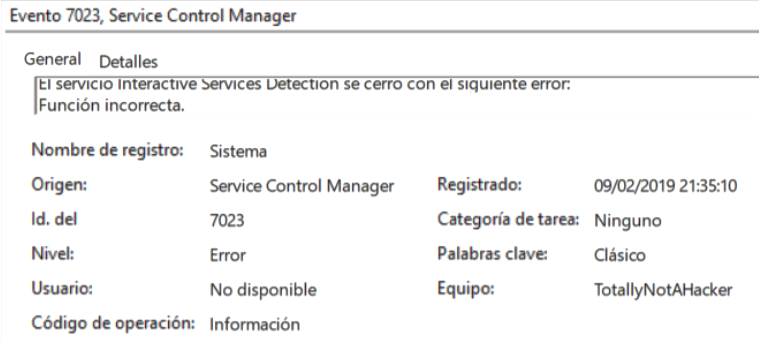
Primer:



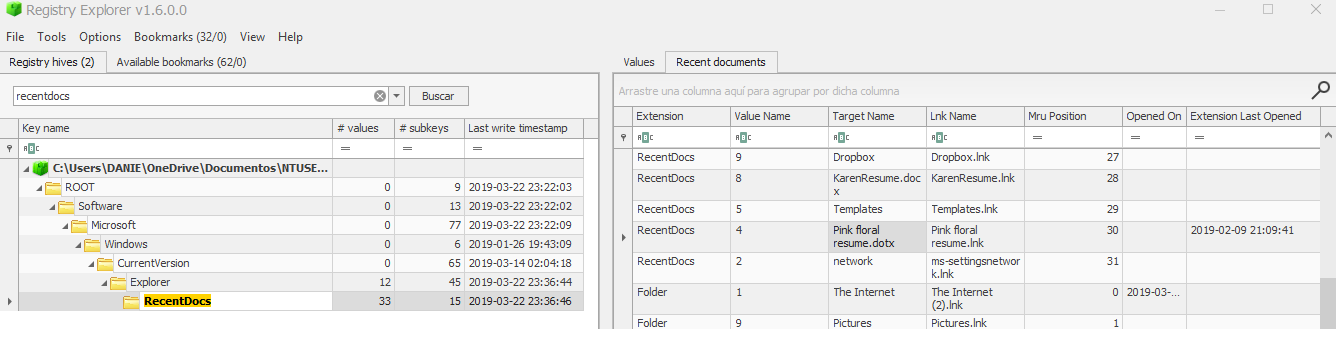
Último:



### **2.23 ¿Cuál es el primer evento con nivel de error registrado en los eventos del sistema?**

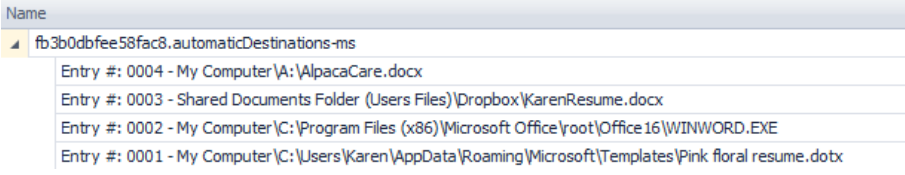


### **2.24 Dentro del directorio que almacena los ficheros con los que el usuario ha interactuado recientemente, encuentra el link que apunta a un fichero accedido el 09/02/2019 a las 21:09:41 que no sea un template.**

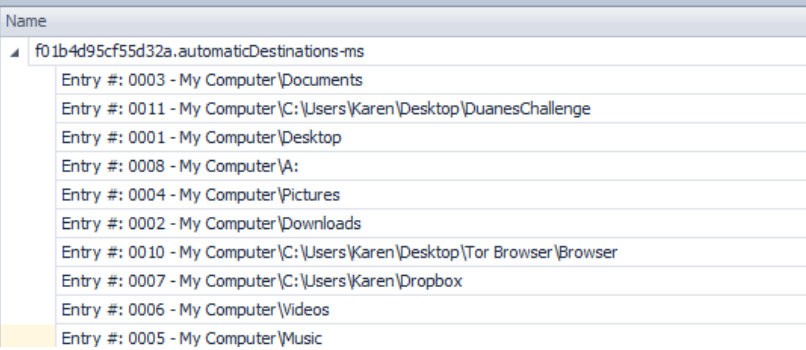


### 

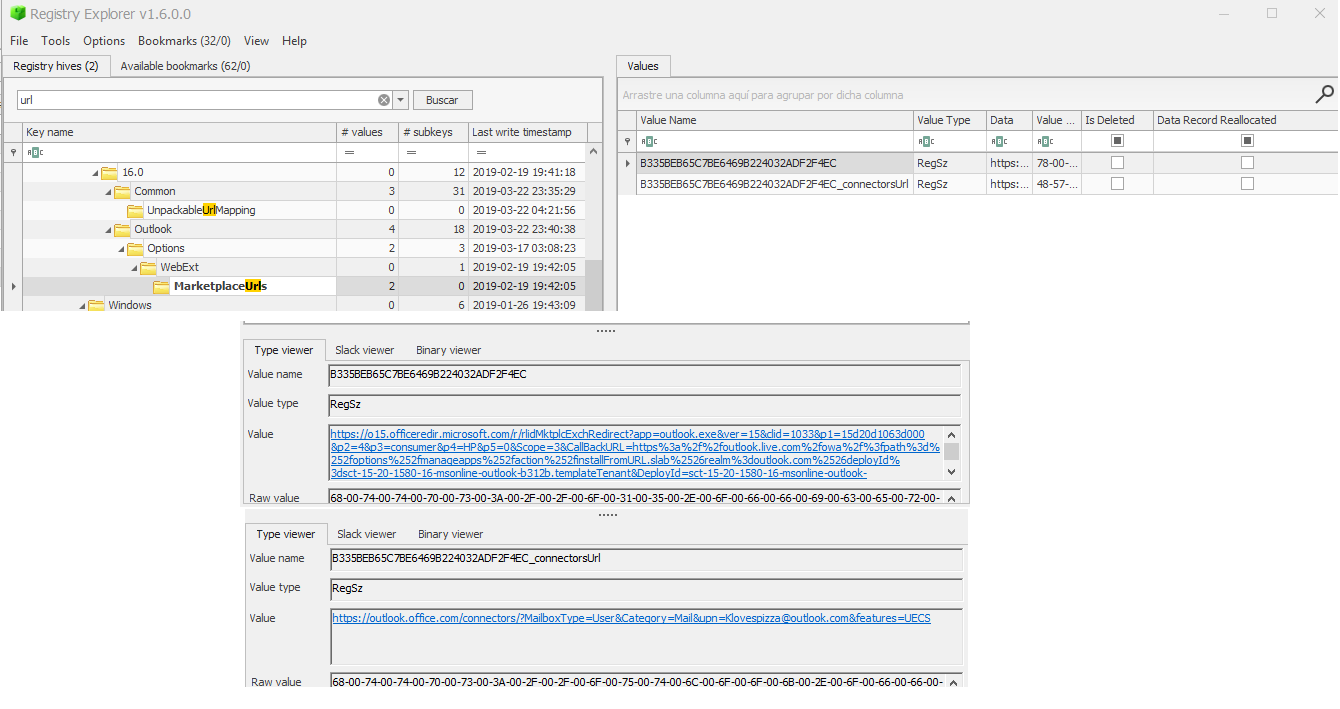
### **2.26 Si nos fijamos en los Jumplist del equipo del que se tomó la muestra, ¿Cuáles son los archivos que tenían acceso rápido para la aplicación Microsoft Word 16?**



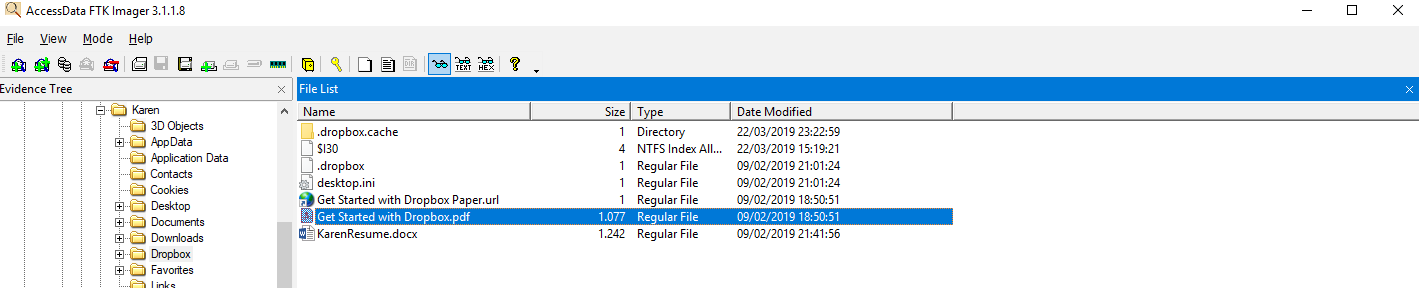
### **2.27 Usando la misma información que en el punto anterior, ¿Cuáles serían los accesos rápidos que tendría el usuario principal en el explorador de Windows?**



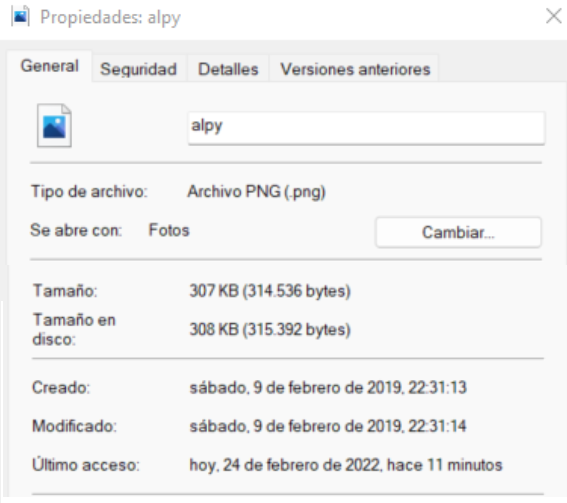
### **2.28 ¿Qué URL tenía como acceso directo en el navegador Edge y que fue modificada por última vez el 19 de febrero de 2019?**



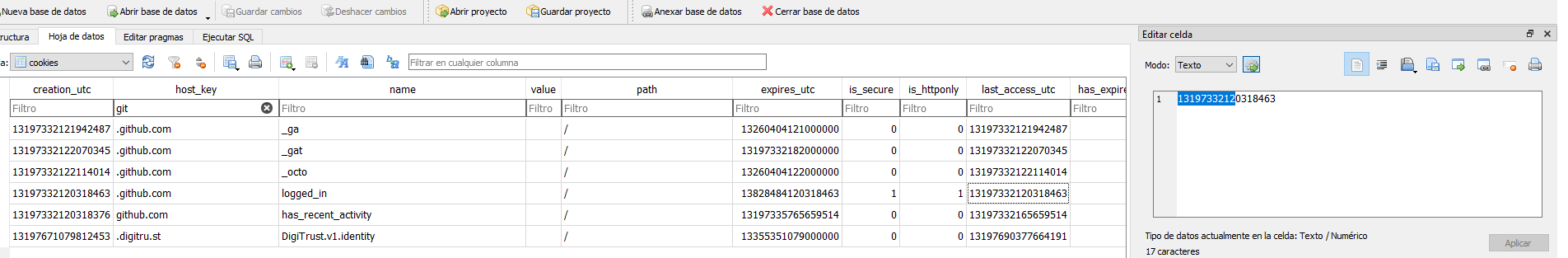
### **2.29 ¿Cuándo fue creado el archivo “Get Started with Dropbox Paper.url” que se encuentra en el directorio Dropbox del usuario principal del sistema?**

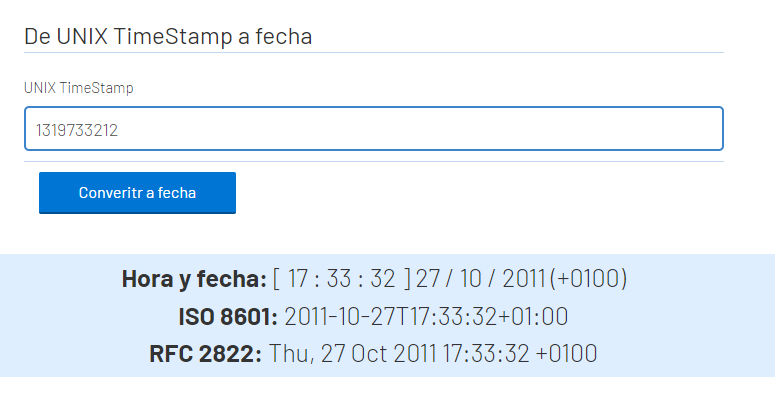


### **2.30 ¿Cuál es el tamaño lógico y físico del archivo alpy.png?**

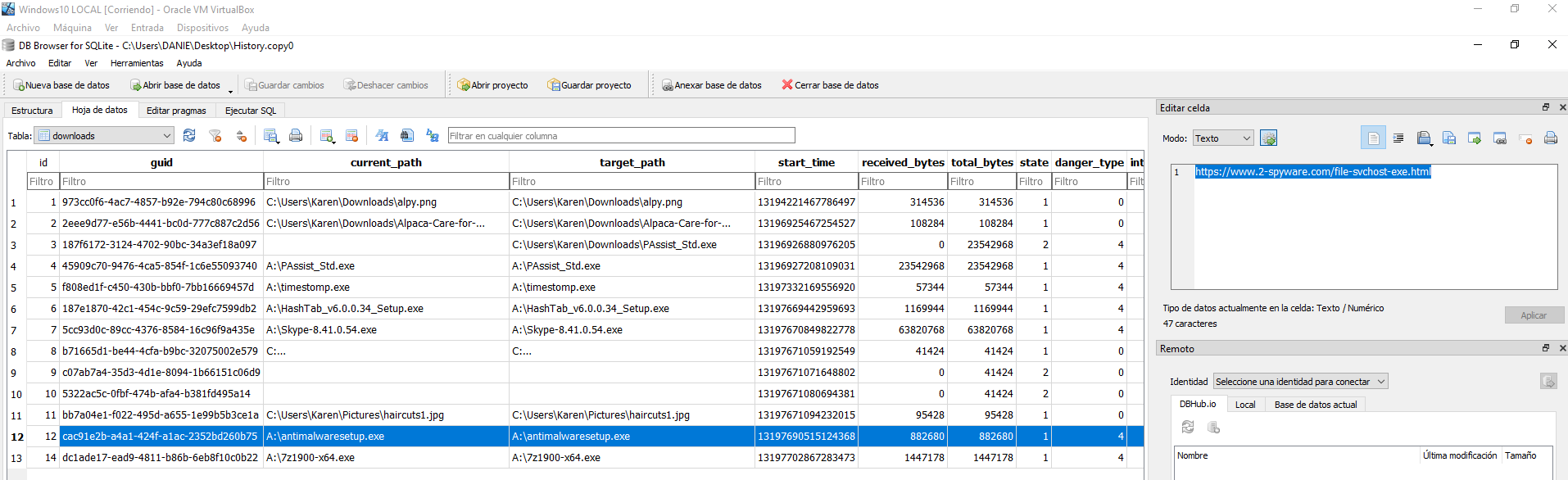


### **2.31 Cuándo fué la última vez que el usuario principal hizo login en github?**





### **2.32 Parece que al usuario principal le preocupaba la seguridad de su equipo. ¿De qué web se descargó un aintimalware para tratar este problema?**



### **2.33 A estas alturas ya nos habremos dado cuenta de que al usuario principal le gustan las Alpacas, pero ¿que parte de este animal quería saber si era suave? ¿Cómo lo podemos saber?**



### **2.34 Si nos fijamos en la papelera de reciclaje de la unidad externa de la fuente de evidencia, indica toda la información que puedas sobre lo que encuentres.**

