ANÁLISIS FORENSE

Unidad 1. Actividad 8

22 DE ENEROE DE 2023

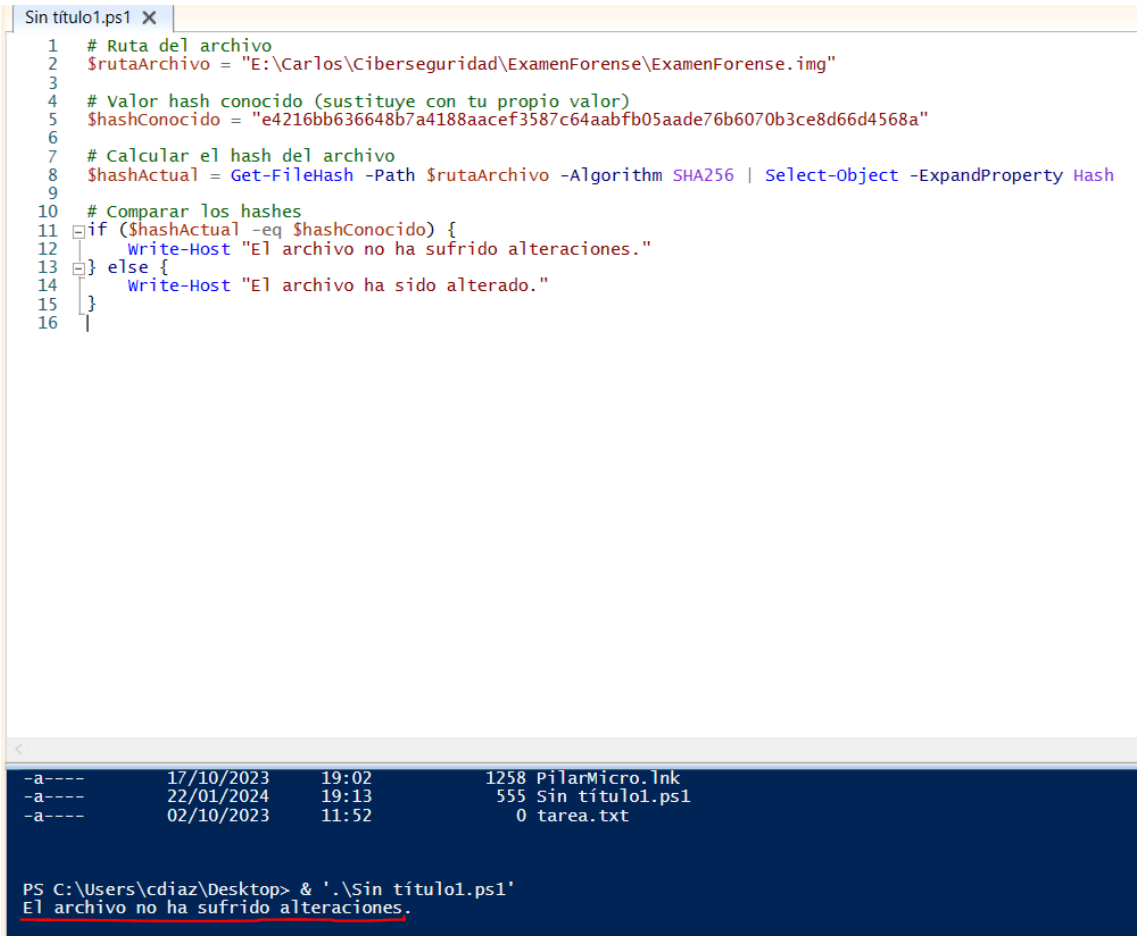
CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

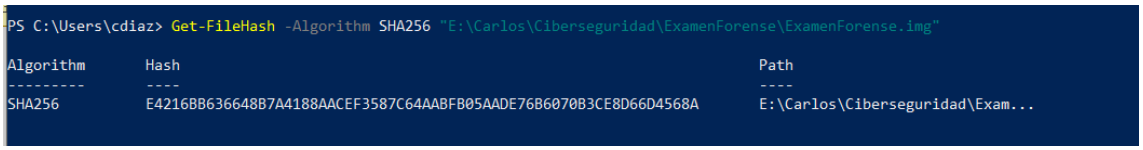
Driver Game Quiz.

1. A fin de que los abogados de la mafia no puedan alegar que se ha roto la cadena de custodia, comprueba que la evidencia no ha sufrido alteraciones. Haz esto tanto con PowerShell como con Autopsy.

Con powershell:



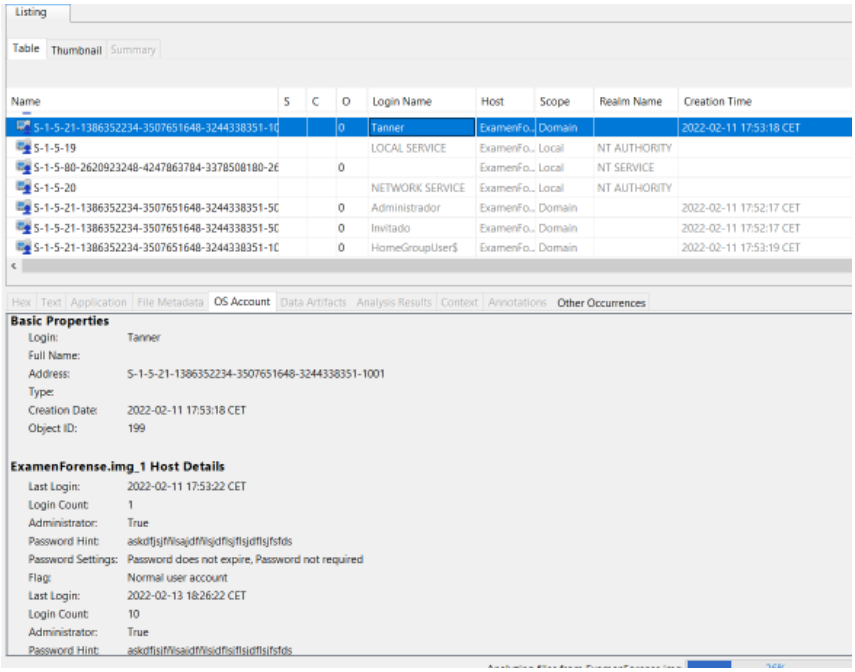
Otra forma de hacerlo:



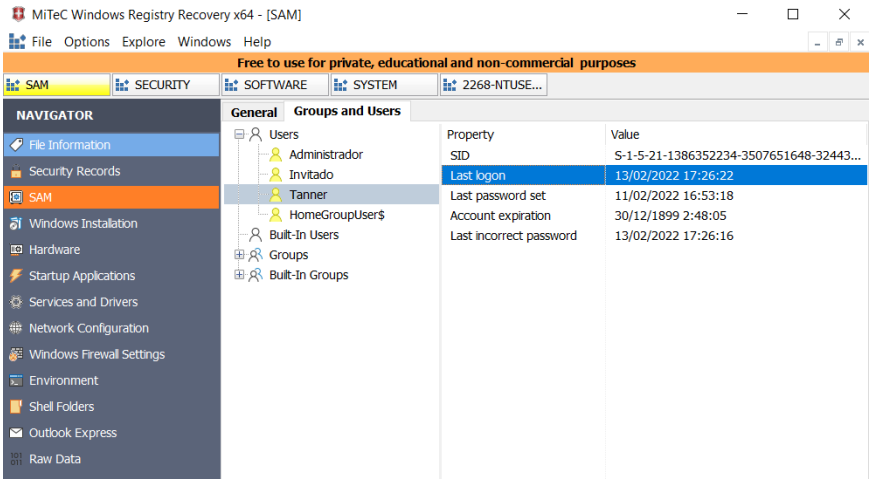
Con autopsy:

2. Comprueba que Tanner tiene un usuario en el equipo, y cuándo hizo login por última vez. Haz esto tanto en Autopsy como en Windows Registry Recovery.

Con autopsy:

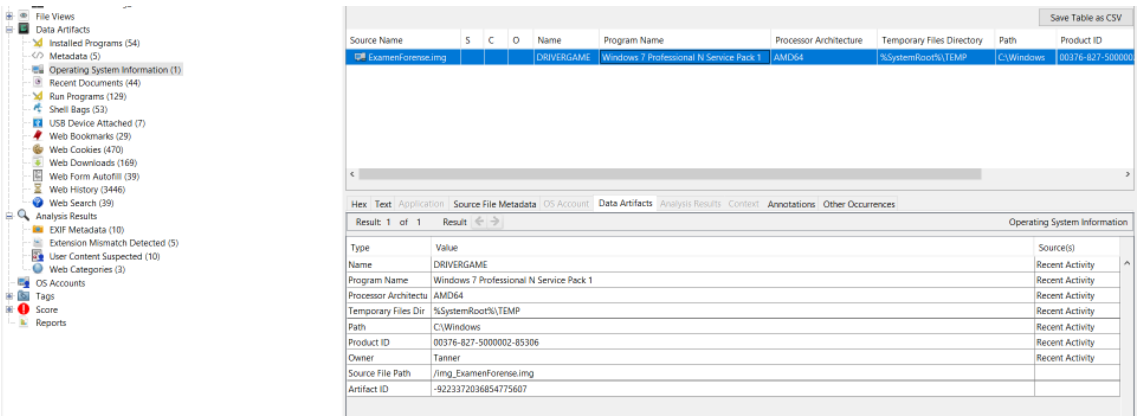


Con WRR:

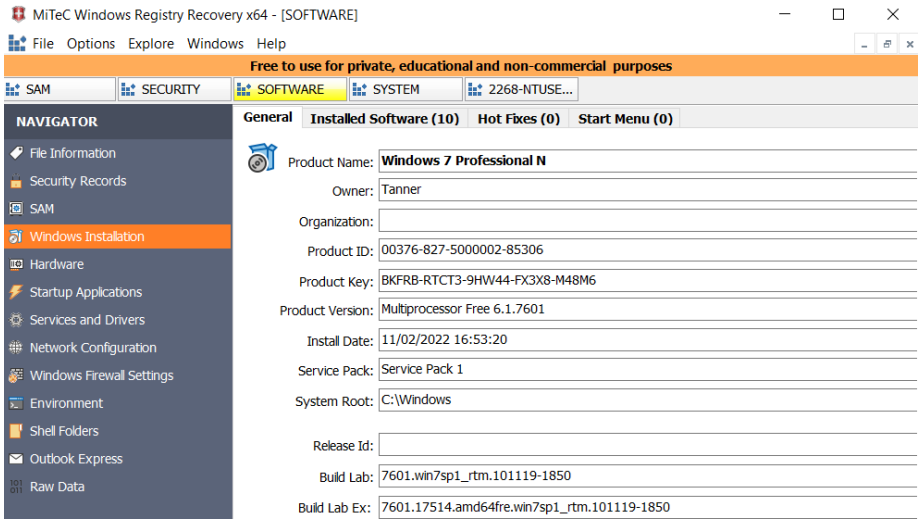


3. Comprueba la versión del Sistema Operativo. Haz esto tanto en Autopsy como en Windows Registry Recovery.

Esto se encuentra en Operating system Information:

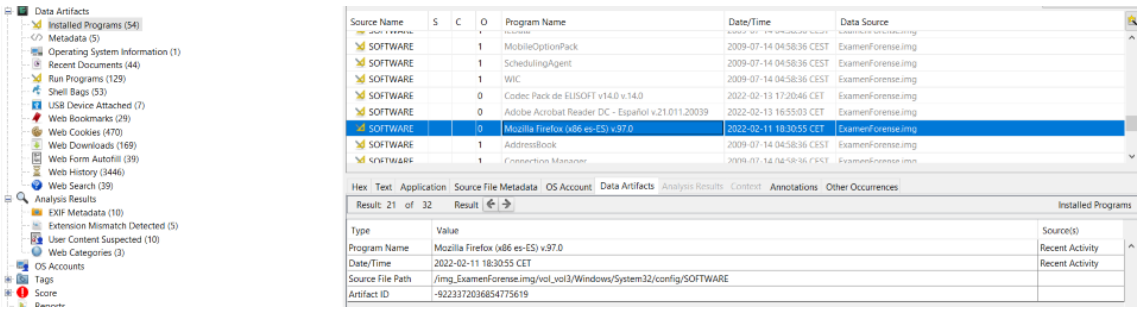


Con WRR:

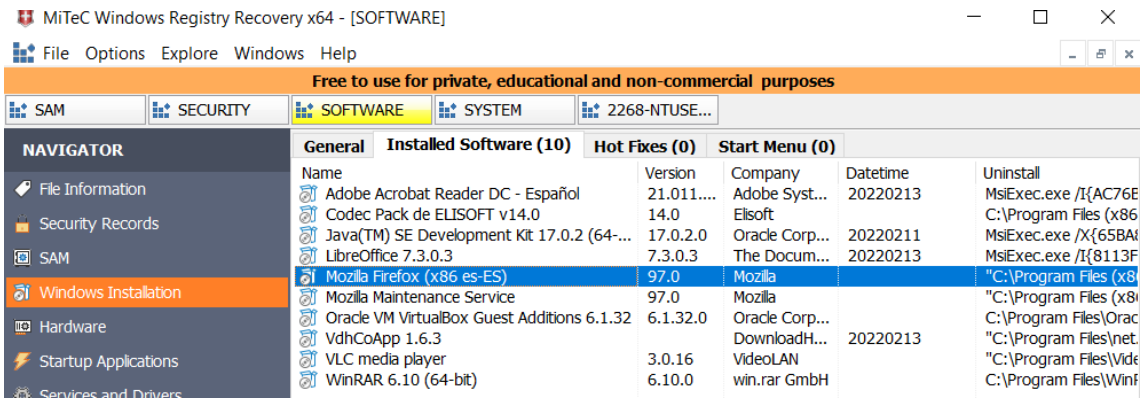


4. Por seguridad, Tanner ha instalado en el sistema un navegador web que no es de Microsoft. Consigue pruebas de cuál es y de que ha sido instalado. Haz esto tanto en Autopsy como en Windows Registry Recovery.

Esto se encuentra en el apartado de installer programs:

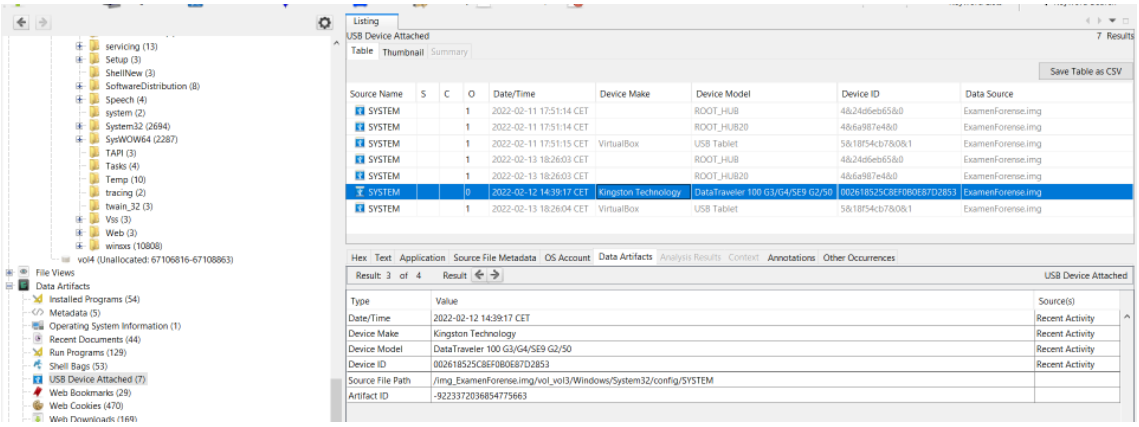


Con WRR:

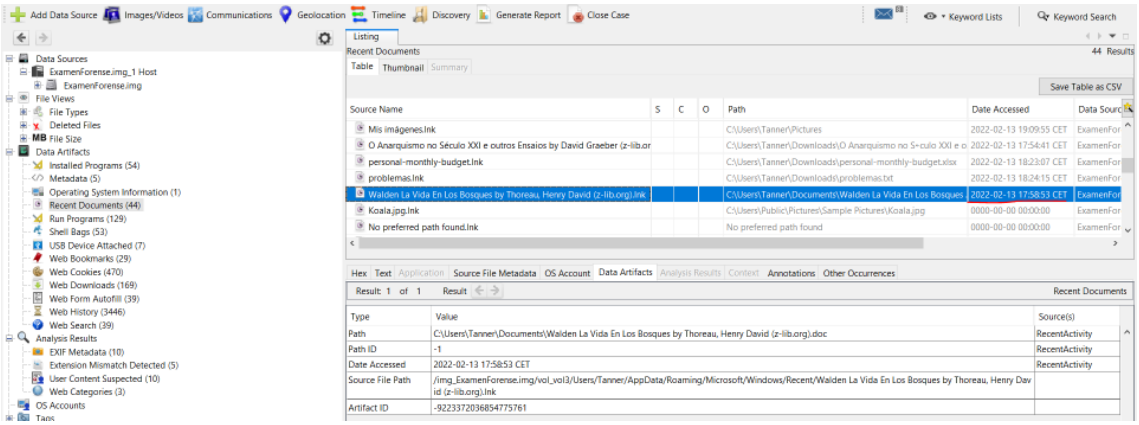


5. Comprueba que Tanner sólo introdujo un pendrive en el equipo, porque debería ser el pendrive en el que se creó la imagen de memoria con DumpIt. ¿Cuál es dicho pendrive y a qué hora lo introdujo?

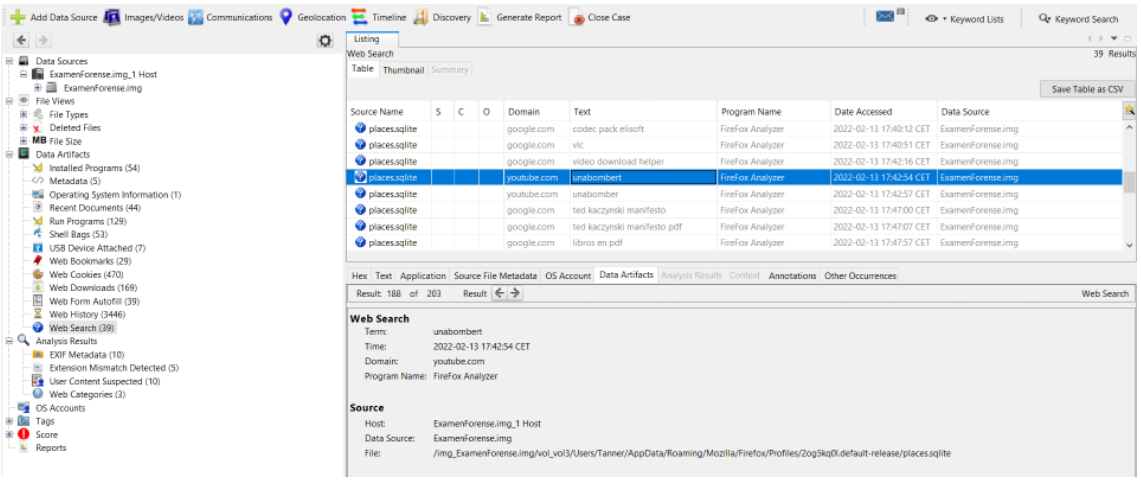
Con Autopsy:



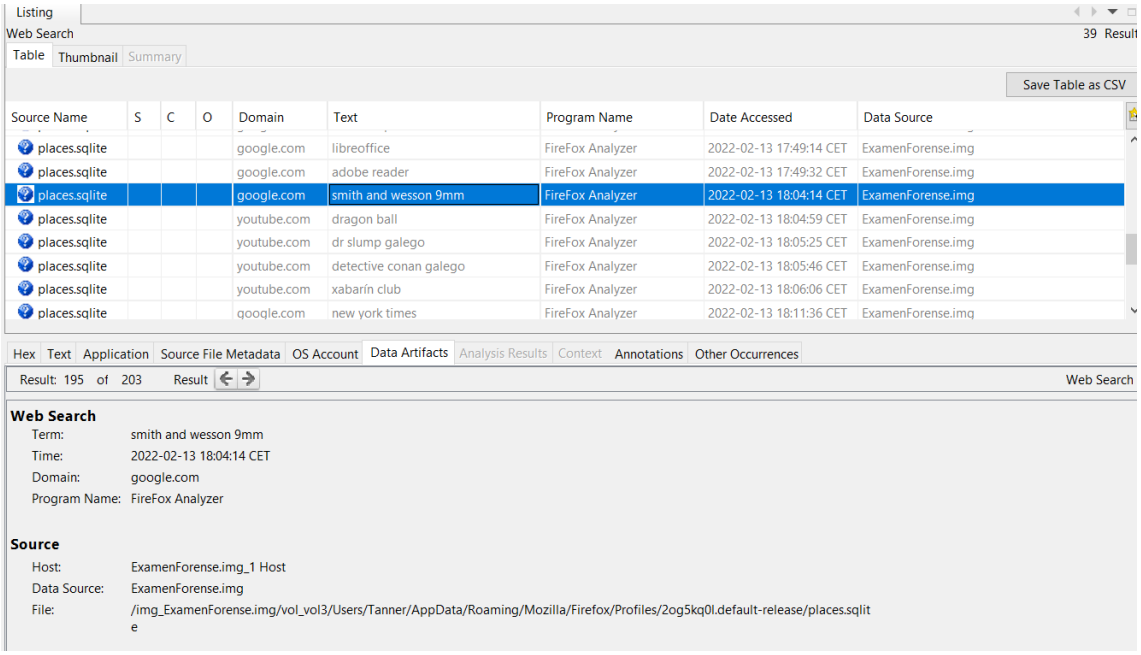
6. Tanner ha accedido a un fichero con extensión .doc recientemente ¿En qué fecha y hora fue accedido?



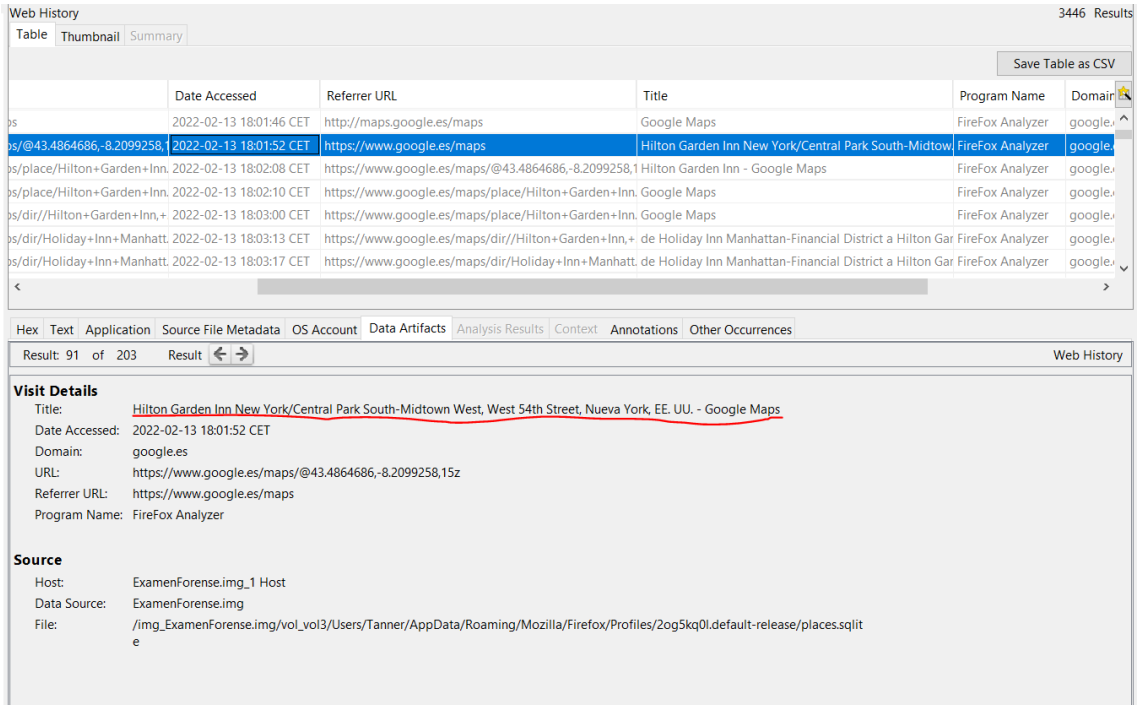
7. Tanner ha estado buscando información sobre un afamado terrorista. En concreto, ha estado viendo vídeos sobre él en una plataforma online. ¿Quién es dicho terrorista?



8. Para acabar con Jean Paul, Tanner ha adquirido un arma. ¿Sobre qué arma en concreto ha buscado información?



9. Tanner se aloja en el Holiday Inn Manhattan Financial District, pero Jean Paul está alojado en otro hotel diferente. Tanner tiene planeado ir a buscarlo en su coche. ¿En qué hotel se aloja Jean Paul?



10. Tras acabar la misión, Tanner tiene pensado ir a otro lugar. ¿Cuál es dicho lugar y cómo tiene pensado ir?

Esta buscando un vuelo de New York a Cancun: