DESKTOP WEB BROWSER DATA

Web browsers have always been a goldmine of digital evidence. Oxygen Forensic® Detective already includes powerful support from over 30 unique iOS and Android mobile web browsers extracting and decoding a tremendous amount. Now, in Oxygen Forensic® Detective 11.4 we introduce the innovative ability to extract web browser data from Windows PCs.

Acquiring valuable web browser data from the target PC is simply a matter of launching our included Oxygen Forensic® KeyScout. The utility, when launched on the target PC, will collect a user’s complete browsing history, saved bookmarks, autofill data and cookies from the currently supported web browsers including Google Chrome, Mozilla Firefox, Microsoft Edge, and more. The evidence set might slightly vary depending on the browser type.

Once the browser data is collected it will be saved to our new file-type .odb file. This file can then be imported into Oxygen Forensic® JetEngine using the Oxygen Desktop Backup option. The web browser data will be parsed and ready for analysis within the Applications and Analytical sections of JetEngine. This new feature, built into the Oxygen Forensic® software, will definitely help investigators with PC internet artifact discovery.

ICLOUD KEYCHAIN EXTRACTION

The iOS Keychain is the password management system in Apple Mac OS and iOS devices that securely stores the most sensitive user data to include passwords and tokens. Obtaining access to the keychain should be of great importance for any for investigator. Oxygen Forensic® Detective 11.4 now arms the investigator with the ability to extract keychain data not only from an Apple iOS device directly, but also from iCloud.

Our current Oxygen Forensic® Cloud Extractor offers Keychain iCloud extraction only with a known login and password. However, token support will be added in an upcoming version.

Please note, the Keychain is available for collection in iCloud only if its synchronization is selected within the device settings by the user and only when an Apple iOS device has a screen lock PIN set.

The extracted Keychain data set includes the iCloud account details, a list of trusted devices, and the keychain data itself that contains passwords, logins and tokens as well as the credit card details, Wi-Fi data and other valuable investigative information.
PARROT DRONE DUMPS

With every new software release we make our Parrot drone support more robust and complete. Oxygen Forensic® Detective 11.4 now allows investigators to import and parse the binary logs of Parrot Bluegrass drones. These valuable files contain the detailed information about the flight that includes not only geo coordinates and time stamps but also velocity, attitude, ground speed, battery level, Wi-Fi signal and other parameters. We also support Parrot drone data that has been extracted from mobile apps, flight logs and cloud services.

WICKR ME MESSENGER DATA

Wickr Me is one of the most secure instant messaging apps and allows users to exchange end-to-end encrypted and content-expiring messages, including photos, and videos. Oxygen Forensic® Detective already supports Wickr Me data decryption from Android devices and in our new 11.4 release we also acquire this secure messenger data from the cloud service using the login/password or token extracted from a PC or a mobile device. The collected evidence includes contacts, chats, calls and account information.

ENHANCED EDL METHOD

Oxygen Forensic® Detective currently offers physical data extraction and screen lock bypass for over 500 Android devices based on various Qualcomm chipsets. In the 11.4 release we’ve added support for over 70 Android devices that have the MSM8939 chipset. Moreover, new investigators can upload and use a third-party bootloader files to perform a physical extraction of Qualcomm-chipset Android devices that are not officially supported by the current software version.

JETENGINE IMPROVEMENTS

Our Oxygen Forensic® JetEngine built in module is continually updated and with every release receives over 20 new innovative features. In this 11.4 release we are introducing the ability to export Oxygen Forensic® Detective extraction to JetEngine simply right-clicking it in the device list within Oxygen Forensic Detective and choosing the “Export to JetEngine” option. Other new features include parsing of KeyScout extractions, new Android backup types, enhanced analytics and more.