http://www.oxygen-forensic.com
+1 877 9 OXYGEN
+44 20 8133 8450
+7 495 222 9278

Oxygen Agent Application Approach

OxyAgent is a small forensically designed application for the complete data extraction from the smartphones

- Drawbacks of the standard approaches. Physical analysis of gigabyte hex dumps takes a lot of time. At the same time all logical protocols were developed for sync purposes, thus they can only extract a top of the iceberg and do not guarantee the data invariability. For example, SyncML protocol has no access to the log records of the mobile device. While examination process it uses phone memory a lot and above all it requires mobile device firmware updates for the up-to-date work. Most of the known protocols generate synchronization log files and leave some traces of the synchronization process and moreover - in many cases phone requires the extra add-ons to be installed during the acquisition process. Besides that a lot of forensically important information is still not accessible. These are not forensically designed applications so they are out of full control from examiner.

- Oxygen Agent application approach. The Agent application approach, introduced by Oxygen Software in 2004, almost achieves the completeness of data extracted by physical methods without expensive equipment or plenty of time for investigations. Using low-level protocols allows the program to get maximum data. At the same time it works via standard cables and adaptors and allows to present the extracted data in readable and user-friendly format that is more peculiar to logical analysis.
  Agent is always up-to-date and ready to extract the complete data. API for data access changes less frequently than binary formats for the information storage.
  Oxygen Forensic Suite guarantees the analyzed mobile phone data invariability while accessing it from the program. The Agent application uses Oxygen Software proprietary protocol and is fully write-protected. It does not change any user data in the mobile device. This can be easily proved by hash. Like all other applications including preinstalled ones which utilize "standard" protocols the Agent uses the mobile device's internal memory which can't stay unchanging in any case. Standard smartphone can have dozens of processes to be launched at the same time (even if they were not started manually) and all of them use the mobile device's internal memory constantly changing it. The memory can't be "frozen" if the phone is turned on.
  The Agent application is used for Symbian OS, Android, Windows Mobile and BlackBerry platforms. All other platforms (including Apple devices) do not require the Agent installation. All information about the Agent application installation and removal is documented for Symbian, Android and BlackBerry platforms by their Application Managers and can be easily viewed in the mobile device.

- OxyAgent for smartphones based on Symbian OS.
  - Certified Agent. Certification allows to escape problems and excessive questions during installation. Current certified Agent (v. 3.24) is valid from 14.10.2009 to 15.10.2019.
  - Installation. Agent can be copied to the mobile device using Oxygen Connection Wizard. Due to the Symbian OS features you must complete the installation process manually. Agent can be installed either to phone memory or flash card according to your needs. All the facts of the Agent installation process can be verified in App Manager log of the mobile device.
  - Uninstallation. All the facts of the Agent uninstallation process can be verified in App Manager log of the mobile device. You can uninstall the Agent manually immediately after you detached the phone from the PC or finished working with Oxygen Forensic Suite 2010.
  - Using Symbian Agents if you have a phone with date in the past (earlier than 14.10.2009). In some cases the phone's date needs to be turned back to preserve Event Log records. For such a case Oxygen Forensic Suite 2010 offers a set of self-signed Agents which are stored in Oxygen Forensic Suite 2010\Agent\SymbianOldCert folder.

- OxyAgent for smartphones based on Windows Mobile OS.
  - Auto-installation. While using USB connection Oxygen Forensic Suite 2010 installs the Agent automatically. Only in case of Bluetooth connection you need to copy the Agent manually via OBEX. Agent can be installed either to phone memory or flash card according to your needs.
    As Windows Mobile platform allows to copy application files and start application right from the flash card, you can change the phone owner's flash card to the flash card which is used for forensic investigations. This operation will prevent changes in the device memory. If the original phone owner's card is used only free clusters can be lost (which potentially can contain previously deleted data) but no existing information will be modified.
    Using the Agent allows to bypass ActiveSync for Windows Mobile phones by connecting directly to the device via Bluetooth.
  - Auto-uninstallation. While using USB connection Oxygen Forensic Suite 2010 uninstalls the Agent automatically. Only in case of Bluetooth connection you need to remove the Agent manually.

- OxyAgent for smartphones based on Android OS.
  - Auto-installation. Oxygen Forensic Suite 2010 installs the Agent automatically right to the mobile device. All the facts of the Agent installation process can be verified in App Manager log of the mobile device. All the installation, start-up and uninstallation procedures are fully controlled by Oxygen Forensic Suite 2010. Android platform allows an indirect data exchange and can use files stored on the flash card. Oxygen Forensic Suite 2010 uses a flash card to store temporary files with the results of the data reading from the mobile device. You can change the phone owner's flash card to your own flash card which is used for forensic

investigations. This operation will prevent changes in the device memory. If the original phone owner's card is used only free clusters can be lost (which potentially can contain previously deleted data) but no existing information will be modified.

- Auto-uninstallation. Oxygen Forensic Suite 2010 uninstalls the Agent automatically. All the facts of the Agent uninstallation process can be verified in App Manager log of the mobile device.

- OxyAgent for Blackberry smartphones
  - Auto-installation. Oxygen Forensic Suite 2010 installs the Agent automatically right to the mobile device. All the facts of the Agent installation process can be verified in App Manager log of the mobile device.
  - Uninstallation. All the facts of the Agent uninstallation process can be verified in App Manager log of the mobile device. You can uninstall the Agent manually immediately after you detached the phone from the PC or finished working with Oxygen Forensic Suite 2010.

- Benefits of the Agent approach
  Oxygen Forensic Suite 2010 with its Agent approach use the same scheme like standard methods for data extraction do – PC-client which requests information from server inside the mobile device by using a protocol. But unlike standard methods the Oxygen proprietary protocol and the Agent take into account the forensic specifics and provide full control over the server inside the mobile device and its data invariability and give an access to the maximum of forensically important data.