[Windows 7 / 8 / 10] Web Browser Artifacts – Internet Explorer and Edge Browser

Contact: junhyeong.lee@plainbit.co.kr, http://maj3sty.tistory.com

Information	Type	Path	Comments
Website URI **Access Time** **Cache Filename** **Cache File Local Full Path**	Cache	- *%UserProfile%*\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat - *%UserProfile%*\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\<Random>*	- ~ IE9
Website URI **Access Time** **Visit Count** **Web Page Title** **HTTP Header**	History	- *%UserProfile%*\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat - *%UserProfile%*\AppData\Local\Microsoft\Windows\History\History.IE5\<period>\index.dat	- 로컬 파일의 열람 기록도 기록되어 있음(파일 실행 기록 X)
Website Domain **Access Time** **Cookie Name/Value** **Cookie Expire Time** **Cookie Created Time**	Cookie	- *%UserProfile%*\AppData\Roaming\Microsoft\Windows\Cookies\index.dat - *%UserProfile%*\AppData\Roaming\Microsoft\Windows\Cookies*	- ~ IE9
Download URI **Download Filename** **Download File Local Full Path** **Download File Size**	Download	- *%UserProfile%*\AppData\Roaming\Microsoft\Windows\IEDownloadHistory\index.dat	- IE9 ~

[Cache] Website URI Access Time Cache Created Time Cache Modified Time at Server Cache Expire Time Cache Sync Time Cache Filename Cache File Local Full Path Cache File Size **[History]** Website URI Access Time History Expire Time HTTP Response Header **[Cookie]** Website Domain Access Time Cookie Name/Value Cookie Created Time at Local-Filesystem Cookie Expire Time Cookie Filename Cookie Local Full Path **[Download]** Download URI Download Time Download Filename Download File Local Full Path HTTP Response Header	Cache History Cookie Download	- *%UserProfile%*\AppData\Local\Microsoft\Windows\WebCache\WebCacheV(01|16|24).dat	- IE10 ~, Edge - 온라인 수집 시 Clean Shutdown 상태에서 수집해야 함 - History Expire Time의 기본 설정은 20일 - Cookie Expire Time의 기본 설정은 20일 - 로컬 파일의 열람 기록도 기록되어 있음(파일 실행 기록 X)

[Windows 7 / 8 / 10] Web Browser Artifacts – Chrome Browser (version 67.0.3396.99)

Contact: junhyeong.lee@plainbit.co.kr, http://maj3sty.tistory.com

Information	Type	Path	Comments
Website URI **First Access Time** **Last Access Time** **Visit Count** **Cache Filename** **Cache File Local Full Path** **Cache Expire Time** **HTTP Response Header**	Cache	- *%UserProfile%*\AppData\Local\Google\Chrome\User Data\Default\Cache\data_[0-4] - *%UserProfile%*\AppData\Local\Google\Chrome\User Data\Default\Cache*	
Website URI **First Access Time** **Last Access Time** **Web Page Title** **Visit Count** **Visit Duration Time** **Search Keyword**	History	- *%UserProfile%*\AppData\Local\Google\Chrome\User Data\Default\History	- 로컬 파일의 열람 기록도 기록되어 있음(파일 실행 기록 X) - urls 테이블과 visits 테이블을 id 필드를 통해 join하여 분석하면 웹사이트 URL의 전체 접속 이력(타임라인)을 확인할 수 있음 - urls 테이블과 keyword_search_terms 테이블을 id 필드를 통해 join하여 분석하면 어떤 웹사이트에서 어떤 검색어를 입력했는지 알 수 있음

Website URI **Cookie Name/Value** **Cookie Expire Time** **Cookie Last Access Time** **Secure Cookie Flag** **HttpOnly Flag** **Expire Flag**	Cookie	- *%UserProfile%*\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Download URI **Download Start Time** **Download End Time** **Download Filename** **Download Local Full Path** **Download File Size** **Received Data Size** **Download Complete Flag** **Download File Last Modified-Time at Local Filesystem**	Download	- *%UserProfile%*\AppData\Local\Google\Chrome\User Data\Default\History	- downloads 테이블과 downloads_url_cahins 테이블을 id 필드를 통해 join하여 분석하면 Download URL Chain을 확인할 수 있음
Website URI **URL Rank** **Web Page Title** **Redirect URL** **Last Updated Time**	Top Sites	- *%UserProfile%*\AppData\Local\Google\Chrome\User Data\Default\Top Sites	
Shortcuts Keyword **Number of Uses** **Last Used Time**	ShortCuts	- *%UserProfile%*\AppData\Local\Google\Chrome\User Data\Default\Shortcuts	
Login URI **Login Credential(ID/PW)** **Credential Store Time**	Login Data	- *%UserProfile%*\AppData\Local\Google\Chrome\User Data\Default\Login Data	- 비밀번호는 암호화되어 있음
Bookmark URI **Bookmark Add Time** **Bookmark Name**	Bookmark	- *%UserProfile%*\AppData\Local\Google\Chrome\User Data\Default\Bookmarks	
Website URI **Tab Type** **Tab Order(index)** **Tab Add Time**	Last Tabs	- *%UserProfile%*\AppData\Local\Google\Chrome\User Data\Default\Last Tabs	- 파일이 별도의 파일 포맷을 사용 (No SQLITE)

[Windows 7 / 8 / 10] Web Browser Artifacts – Firefox Browser (version 61.0.1)

Contact: junhyeong.lee@plainbit.co.kr, http://maj3sty.tistory.com

Information	Type	Path	Comments
Website URI **Last Access Time** **Last Modified Time** **Visit Count** **Cache Filename** **Cache File Local Full Path** **Cache Expire Time** **HTTP Response Header**	Cache	- *%UserProfile%*\AppData\Local\Mozilla\Firefox\Profiles\<Random>\cache2\index - *%UserProfile%*\AppData\Local\Mozilla\Firefox\Profiles\<Random>\cache2\entries*	
Website URI **Last Access Time** **Web Page Title** **Visit Count** **Search Keyword**	History	- *%UserProfile%*\AppData\Roaming\Mozilla\Firefox\Profiles\<Random>\places.sqlite	- 로컬 파일의 열람 기록도 기록되어 있음 (파일 실행 기록 X) - moz_places 테이블과 moz_keywords 테이블을 place_id 필드를 통해 join하여 분석하면 어떤 웹사이트에서 어떤 검색어를 입력했는지 알 수 있음
Website URI **Cookie Name/Value** **Cookie Create Time** **Cookie Expire Time** **Cookie Last Access Time** **Secure Cookie Flag** **HttpOnly Flag**	Cookie	- *%UserProfile%*\AppData\Roaming\Mozilla\Firefox\Profiles\<Random>\cookies.sqlite	

Download URI **Download Start Time** **Download End Time** **Download Filename** **Download Local Full Path** **Download File Size** **Received Data Size** **Download Complete Flag** **Download File Last Modified-Time at Local Filesystem**	Download	- *%UserProfile%*\AppData\Roaming\Mozilla\Firefox\Profiles\<Random>\places.sqlite	- moz_annos 테이블과 moz_anno_attributes 테이블을 id 필드로 join하여 분석하면 Download URL Chain을 확인할 수 있음
Web Page Title **Bookmark Add Time** **Last Modified Time**	Bookmark	- *%UserProfile%*\AppData\Roaming\Mozilla\Firefox\Profiles\<Random>\places.sqlite	- 삭제된 Bookmark 기록을 알 수 있음
Form Value **Form Field Name** **Used Count** **First Used Time** **Last Used Time**	Form history	- *%UserProfile%*\AppData\Roaming\Mozilla\Firefox\Profiles\<Random>\formhistory.sqlite	- 삭제된 폼 입력 기록을 알 수 있음

[Windows 7 / 8 / 10] Web Browser Artifacts – Opera Browser (version 54.0.2952.54)

Contact: junhyeong.lee@plainbit.co.kr, http://maj3sty.tistory.com

Information	Type	Path	Comments
Website URI **First Access Time** **Last Access Time** **Visit Count** **Cache Filename** **Cache File Local Full Path** **Cache Expire Time**	Cache	- *%UserProfile%*\AppData\Local\Opera Software\Opera Stable\Cache* - *%UserProfile%*\AppData\Local\Opera Software\Opera Stable\Media Cache*	
Website URI **First Access Time** **Last Access Time** **Web Page Title** **Visit Count** **Visit Duration Time** **Search Keyword**	History	- *%UserProfile%*\AppData\Roaming\Opera Software\Opera Stable\History	- 로컬 파일의 열람 기록도 기록되어 있음(파일 실행 기록 X) - urls 테이블과 visits 테이블을 id 필드를 통해 join하여 분석하면 웹사이트 URL의 전체 접속 이력(타임라인)을 확인할 수 있음 - urls 테이블과 keyword_search_terms 테이블을 id 필드를 통해 join하여 분석하면 어떤 웹사이트에서 어떤 검색어를 입력했는지 알 수 있음

Website URI **Cookie Name/Value** **Cookie Expire Time** **Cookie Last Access Time** **Secure Cookie Flag** **HttpOnly Flag** **Expire Flag**	Cookie	- *%UserProfile%*\AppData\Roaming\Opera Software\Opera Stable\Cookies	
Download URI **Download Start Time** **Download End Time** **Download Filename** **Download Local Full Path** **Download File Size** **Received Data Size** **Download Complete Flag** **Download File Last Modified-Time at Local Filesystem**	Download	- *%UserProfile%*\AppData\Roaming\Opera Software\Opera Stable\History	- downloads 테이블과 downloads_url_cahins 테이블을 id 필드를 통해 join하여 분석하면 Download URL Chain을 확인할 수 있음
Website URI **URL Rank** **Web Page Title** **Redirect URL** **Last Updated Time**	Top Sites	- *%UserProfile%*\AppData\Roaming\Opera Software\Opera Stable\Top Sites	
Shortcuts Keyword **Number of Uses** **Last Used Time**	ShortCuts	- *%UserProfile%*\AppData\Roaming\Opera Software\Opera Stable\Shortcuts	
Login URI **Login Credential(ID/PW)** **Credential Store Time**	Login Data	- *%UserProfile%*\AppData\Roaming\Opera Software\Opera Stable\Login Data	- 비밀번호는 암호화되어 있음
Bookmark URI **Bookmark Add Time** **Bookmark Name**	Bookmark	- *%UserProfile%*\AppData\Roaming\Opera Software\Opera Stable\Bookmarks	
Website URI **Tab Type** **Tab Order(index)** **Tab Add Time**	Last Tabs	- *%UserProfile%*\AppData\Roaming\Opera Software\Opera Stable\Last Tabs	- 파일이 별도의 파일 포맷을 사용 (No SQLITE)

[Windows 7 / 8 / 10] Web Browser Artifacts – Whale Browser (version 1.3.49.6)

Contact: junhyeong.lee@plainbit.co.kr, http://maj3sty.tistory.com

Information	Type	Path	Comments
Website URI **First Access Time** **Last Access Time** **Visit Count** **Cache Filename** **Cache File Local Full Path** **Cache Expire Time**	Cache	- *%UserProfile%*\AppData\Local\Naver\Naver Whale\User Data\Default\Cache\data_[0-4] - *%UserProfile%*\AppData\Local\Naver\Naver Whale\User Data\Default\Cache*	
Website URI **First Access Time** **Last Access Time** **Web Page Title** **Visit Count** **Visit Duration Time** **Search Keyword**	History	- *%UserProfile%*\AppData\Local\Naver\Naver Whale\User Data\Default\History	- urls 테이블과 visits 테이블을 id 필드를 통해 join하여 분석하면 웹사이트 URL의 전체 접속 이력(타임라인)을 확인할 수 있음 - Urls 테이블과 keyword_search_terms 테이블을 id 필드를 통해 join하여 분석하면 어떤 웹사이트에서 어떤 검색어를 입력했는지 알 수 있음
Website URI **Cookie Name/Value** **Cookie Expire Time** **Cookie Last Access Time** **Secure Cookie Flag** **HttpOnly Flag** **Expire Flag**	Cookie	- *%UserProfile%*\AppData\Local\Naver\Naver Whale\User Data\Default\Cookies	

Download URI **Download Start Time** **Download End Time** **Download Filename** **Download Local Full Path** **Download File Size** **Received Data Size** **Download Complete Flag** **Download File Last Modified-Time at Local Filesystem**	Download	- *%UserProfile%*\AppData\Local\Naver\Naver Whale\User Data\Default\History	- downloads 테이블과 downloads_url_cahins 테이블을 id 필드를 통해 join하여 분석하면 Download URL Chain을 확인할 수 있음
Website URI **URL Rank** **Web Page Title** **Redirect URL** **Last Updated Time**	Top Sites	- *%UserProfile%*\AppData\Local\Naver\Naver Whale\User Data\Default\Top Sites	
Shortcuts Keyword **Number of Uses** **Last Used Time**	ShortCuts	- *%UserProfile%*\AppData\Local\Naver\Naver Whale\User Data\Default\Shortcuts	
Login URI **Login Credential(ID/PW)** **Credential Store Time**	Login Data	- *%UserProfile%*\AppData\Local\Naver\Naver Whale\User Data\Default\Login Data	- 비밀번호는 암호화되어 있음
Bookmark URI **Bookmark Add Time** **Bookmark Name**	Bookmark	- *%UserProfile%*\AppData\Local\Naver\Naver Whale\User Data\Default\Bookmarks	
Website URI **Tab Type** **Tab Order(index)** **Tab Add Time**	Last Tabs	- *%UserProfile%*\AppData\Local\Naver\Naver Whale\User Data\Default\Last Tabs	- 파일이 별도의 파일 포맷을 사용 (No SQLITE)

[Windows 7 / 8 / 10] Web Browser Artifacts – Swing Browser (version 4.2.4.0(18.2.21.0))

Contact: junhyeong.lee@plainbit.co.kr, http://maj3sty.tistory.com

Information	Type	Path	Comments
Website URI **First Access Time** **Last Access Time** **Visit Count** **Cache Filename** **Cache File Local Full Path** **Cache Expire Time**	Cache	- *%UserProfile%*\AppData\Local\SwingBrowser\User Data\Default\Cache\data_[0-4] - *%UserProfile%*\AppData\Local\SwingBrowser\User Data\Default\Cache*	
Website URI **First Access Time** **Last Access Time** **Web Page Title** **Visit Count** **Visit Duration Time** **Search Keyword**	History	- *%UserProfile%*\AppData\Local\SwingBrowser\User Data\Default\History	- urls 테이블과 visits 테이블을 id 필드를 통해 join하여 분석하면 웹사이트 URL의 전체 접속 이력(타임라인)을 확인할 수 있음 - Urls 테이블과 keyword_search_terms 테이블을 id 필드를 통해 join하여 분석하면 어떤 웹사이트에서 어떤 검색어를 입력했는지 알 수 있음
Website URI **Cookie Name/Value** **Cookie Expire Time** **Cookie Last Access Time** **Secure Cookie Flag** **HttpOnly Flag** **Expire Flag**	Cookie	- *%UserProfile%*\AppData\Local\SwingBrowser\User Data\Default\Cookies	

Download URI **Download Start Time** **Download End Time** **Download Filename** **Download Local Full Path** **Download File Size** **Received Data Size** **Download Complete Flag** **Download File Last Modified-Time at Local Filesystem**	Download	- *%UserProfile%*\AppData\Local\SwingBrowser\User Data\Default\History	- downloads 테이블과 downloads_url_cahins 테이블을 id 필드를 통해 join하여 분석하면 Download URL Chain을 확인할 수 있음
Website URI **URL Rank** **Web Page Title** **Redirect URL** **Last Updated Time**	Top Sites	- *%UserProfile%*\AppData\Local\SwingBrowser\User Data\Default\Top Sites	
Login URI **Login Credential(ID/PW)** **Credential Store Time**	Login Data	- *%UserProfile%*\AppData\Local\SwingBrowser\User Data\Default\Login Data	- 비밀번호는 암호화되어 있음
Bookmark URI **Bookmark Add Time** **Bookmark Name**	Bookmark	- *%UserProfile%*\AppData\Local\SwingBrowser\User Data\Default\Bookmarks	
Website URI **Tab Type** **Tab Order(index)** **Tab Add Time**	Last Tabs	- *%UserProfile%*\AppData\Local\SwingBrowser\User Data\Default\Last Tabs	- 파일이 별도의 파일 포맷을 사용 (No SQLITE)