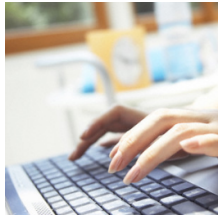


4 April 2008

By: Marius Oiaga, Technology News Editor



[Download Free Tools Designed to Analyze Internet Traffic from Vista](#)

Straight from Microsoft

At the end of March, Microsoft made available a couple of tools designed to enable analysis of Internet traffic from Windows Vista. But it is not just the latest Windows client that the Redmond company is focusing on, as the Windows XP and Windows 2000 operating systems are also supported. STRACE and HTTPREPLAY are both available as free downloads straight from Microsoft. Via STRACE, Internet Explorer LOG will be generated as the tool acts as a socket/SSL tracer. With HTTPREPLAY, users will be able to perform an extensive analysis and even to replay HTTP traffic. The HTTPREPLAY acts like a SOCKTRC plugin. "STRACE is a socket/SSL tracer that is based on the 'detours' utility. The tool has been specifically designed to generate LOG for Internet Explorer but it can be used with many other applications. Using STRACE with Internet Explorer is equivalent to use a (non full) debug build of WININET.DLL to generate a WININET LOG. The STRACE LOG contains clear text HTTP traffic (with socket information) and encrypted/decrypted SSL data. From the STRACE LOG, you can 'replay' a full navigation scenario using the HTTPREPLAY tool. This can be useful to reproduce a problem or browse web sites offline," reads Microsoft's overview of STRACE. When it comes down to HTTPREPLAY, things are a tad more complicated. The SOCKTRC plugin is intimately connected with STRACE or WININET logs. HTTPREPLAY essentially lets the user not set up an Internet Information Services, and still analyze HTTP traffic as well as replay a web server. In the eventuality that a repro scenario is not available, one can be built via HTTPREPLAY. "HTTPREPLAY reads the log file using a single ReadFile operation. (...) HTTPREPLAY first tries to send back the largest HTTP 200 OK response found. If such response is not available, the tool will send back the first response found for the URL requested. This method allows to replay HTTP traffic even if 401 or 407 responses are used. HTTPREPLAY is now able to replay STRACE log containing SSL (HTTPS) traffic," Microsoft informed. HTTPREPLAY is available [here](#). STRACE can be downloaded from this [link](#).