Timeline Example

Mon Nov 26 2012 23:01:53,macb,"[ENG IEHISTORY] **explorer.exe->Visited: callb@http://58.64.132.8/download/Symantec-1.43-1.exe** PID: 284/Cache type ""URL "" at 0x2895000“

Mon Nov 26 2012 23:01:54,macb,"[ENG MFT FILE_NAME] **WINDOWS\Prefetch\SYMANTEC-1.43-1[2].EXE-3793B625.pf** (Offset: 0x17779800)“

Mon Nov 26 2012 23:01:54,.acb,"[ENG MFT FILE_NAME] **WINDOWS\system32\6to4ex.dll** (Offset: 0x324c800)“

Mon Nov 26 2012 23:01:55,m...,"[ENG Registry] **$$$PROTO.HIV\ControlSet001\Services\6to4“**

Mon Nov 26 2012 23:01:58,.acb,"[ENG THREAD] **svchost.exe** PID: 1024/TID: 804“

Timeline Example (cont)

Mon Nov 26 2012 23:03:10,macb,"[ENG MFT FILE_NAME] **WINDOWS\webui** (Offset: 0x1bc21000)“

Mon Nov 26 2012 23:06:47,macb,"[ENG MFT FILE_NAME] **WINDOWS\webui\gs.exe** (Offset: 0x16267c00)“

Mon Nov 26 2012 23:11:58,macb,"[ENG MFT FILE_NAME] **WINDOWS\Prefetch\GS.EXE-3796DDD9.pf** (Offset: 0x311800)“

Mon Nov 26 2012 23:11:58,m...,"[ENG Registry] **SECURITY\Policy\Secrets“**

Mon Nov 26 2012 23:11:58,.a..,"[ENG MFT STD_INFO] **WINDOWS\system32\samsrv.dll** (Offset: 0x329f000)"

Mon Nov 26 2012 23:11:58,.a..,"[ENG MFT STD_INFO] **WINDOWS\system32\cryptdll.dll** (Offset: 0x3329c00)"