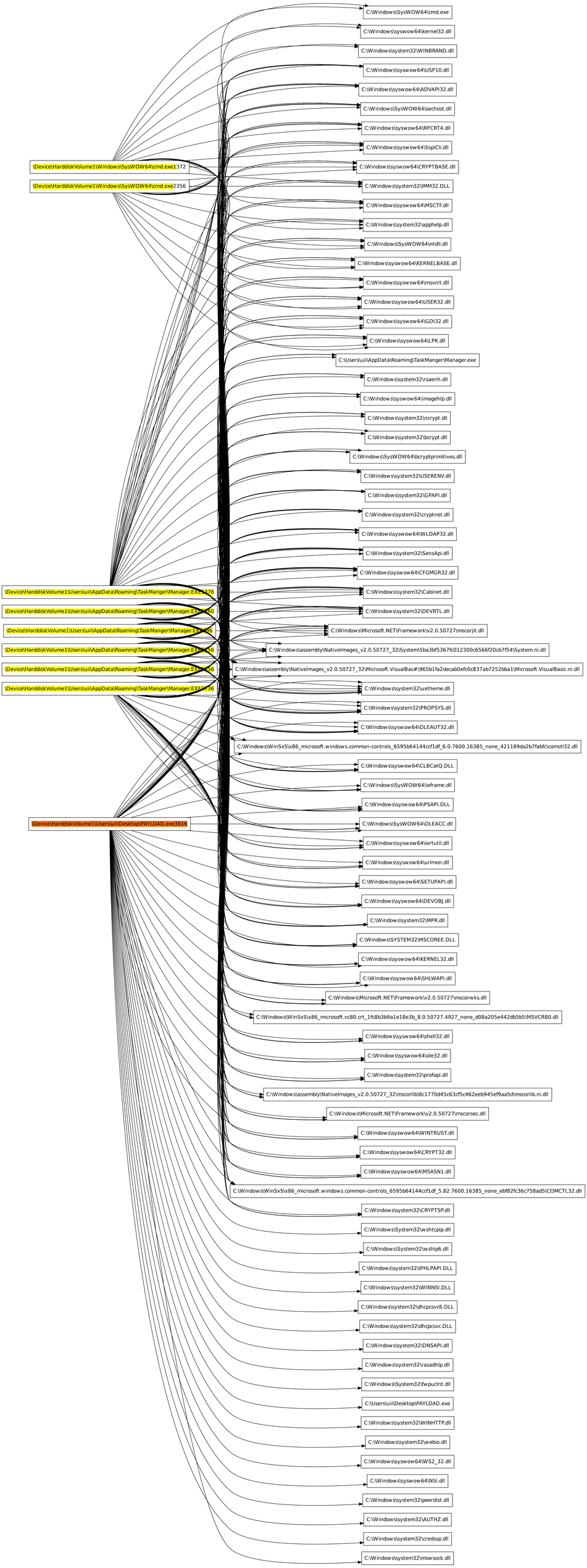
\Device\HarddiskVolume1\Windows\SysWOW64\cmd.exe1372
\Device\HarddiskVolume1\Windows\SysWOW64\cmd.exe2356
\Device\HarddiskVolume1\Users\uii\AppData\Roaming\TaskManger\Manager.EXE1276
\Device\HarddiskVolume1\Users\uii\AppData\Roaming\TaskManger\Manager.EXE1360
\Device\HarddiskVolume1\Users\uii\AppData\Roaming\TaskManger\Manager.EXE1356
\Device\HarddiskVolume1\Users\uii\AppData\Roaming\TaskManger\Manager.EXE1356
\Device\HarddiskVolume1\Users\uii\AppData\Roaming\TaskManger\Manager.EXE1356
\Device\HarddiskVolume1\Users\uii\AppData\Roaming\TaskManger\Manager.EXE1356
\Device\HarddiskVolume1\Users\uii\Desktop\PAYLOAD.exe3016
C:\Windows\SysWOW64\cmd.exe
C:\Windows\syswow64\kernel32.dll
C:\Windows\system32\WINBRAND.dll
C:\Windows\syswow64\USP10.dll
C:\Windows\syswow64\ADVAPI32.dll
C:\Windows\SysWOW64\sechost.dll
C:\Windows\syswow64\RPCRT4.dll
C:\Windows\syswow64\SspiCli.dll
C:\Windows\syswow64\CRYPTBASE.dll
C:\Windows\system32\IMM32.DLL
C:\Windows\syswow64\MSCTF.dll
C:\Windows\system32\apphelp.dll
C:\Windows\SysWOW64\ntdll.dll
C:\Windows\syswow64\KERNELBASE.dll
C:\Windows\syswow64\msvcrt.dll
C:\Windows\syswow64\USER32.dll
C:\Windows\syswow64\GDI32.dll
C:\Windows\syswow64\LPK.dll
C:\Users\uii\AppData\Roaming\TaskManger\Manager.exe
C:\Windows\system32\rsaenh.dll
C:\Windows\syswow64\imagehlp.dll
C:\Windows\system32\ncrypt.dll
C:\Windows\system32\bcrypt.dll
C:\Windows\SysWOW64\bcryptprimitives.dll
C:\Windows\system32\USERENV.dll
C:\Windows\system32\GPAPI.dll
C:\Windows\system32\cryptnet.dll
C:\Windows\syswow64\WLDAP32.dll
C:\Windows\system32\SensApi.dll
C:\Windows\syswow64\CFGMGR32.dll
C:\Windows\system32\Cabinet.dll
C:\Windows\system32\DEVRTL.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorjit.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System\5ba3bf5367fc012300c6566f20cb7f54\System.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\965b1fa2decab0efc0c837ab7252bba1\Microsoft.VisualBasic.ni.dll
C:\Windows\system32\uxtheme.dll
C:\Windows\system32\PROPSYS.dll
C:\Windows\syswow64\OLEAUT32.dll
C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.16385_none_421189da2b7fabfc\comctl32.dll
C:\Windows\syswow64\CLBCatQ.DLL
C:\Windows\SysWOW64\ieframe.dll
C:\Windows\syswow64\PSAPI.DLL
C:\Windows\SysWOW64\OLEACC.dll
C:\Windows\syswow64\iertutil.dll
C:\Windows\syswow64\urlmon.dll
C:\Windows\syswow64\SETUPAPI.dll
C:\Windows\syswow64\DEVOBJ.dll
C:\Windows\system32\MPR.dll
C:\Windows\SYSTEM32\MSCOREE.DLL
C:\Windows\syswow64\KERNEL32.dll
C:\Windows\syswow64\SHLWAPI.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
C:\Windows\WinSxS\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4927_none_d08a205e442db5b5\MSVCR80.dll
C:\Windows\syswow64\shell32.dll
C:\Windows\syswow64\ole32.dll
C:\Windows\system32\profapi.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\mscorlib\8c1770d45c63cf5c462eeb945ef9aa5d\mscorlib.ni.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorsec.dll
C:\Windows\syswow64\WINTRUST.dll
C:\Windows\syswow64\CRYPT32.dll
C:\Windows\syswow64\MSASN1.dll
C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7600.16385_none_ebf82fc36c758ad5\COMCTL32.dll
C:\Windows\system32\CRYPTSP.dll
C:\Windows\System32\wshtcpip.dll
C:\Windows\System32\wship6.dll
C:\Windows\system32\IPHLPAPI.DLL
C:\Windows\system32\WINNSI.DLL
C:\Windows\system32\dhcpcsvc6.DLL
C:\Windows\system32\dhcpcsvc.DLL
C:\Windows\system32\DNSAPI.dll
C:\Windows\system32\rasadhlp.dll
C:\Windows\System32\fwpuclnt.dll
C:\Users\uii\Desktop\PAYLOAD.exe
C:\Windows\system32\WINHTTP.dll
C:\Windows\system32\webio.dll
C:\Windows\syswow64\WS2_32.dll
C:\Windows\syswow64\NSI.dll
C:\Windows\system32\peerdist.dll
C:\Windows\system32\AUTHZ.dll
C:\Windows\system32\credssp.dll
C:\Windows\system32\mswsock.dll