Content of WMI Image_Load Query.vbs (Site 1)

```
On Error Resume Next

Const wbemFlagReturnImmediately = &h10
Const wbemFlagForwardOnly = &h20

arrComputers = Array(".")
For Each strComputer In arrComputers
   WScript.Echo
   WScript.Echo "=========================================="
   WScript.Echo "Computer: " & strComputer
   WScript.Echo "=========================================="

   Set objWMIService = GetObject("winmgmts:\\" & strComputer & "\root\WMI")
   Set colItems = objWMIService.ExecQuery("SELECT * FROM Image_Load", "WQL", _
                                          wbemFlagReturnImmediately + wbemFlagForwardOnly)

   For Each objItem In colItems
      strEventGuid = Join(objItem.EventGuid, ",")
         WScript.Echo "EventGuid: " & strEventGuid
      WScript.Echo "EventSize: " & objItem.EventSize
      WScript.Echo "EventType: " & objItem.EventType
      WScript.Echo "FileName: " & objItem.FileName
      WScript.Echo "Flags: " & objItem.Flags
      WScript.Echo "ImageBase: " & objItem.ImageBase
      WScript.Echo "ImageSize: " & objItem.ImageSize
      WScript.Echo "InstanceId: " & objItem.InstanceId
      WScript.Echo "KernelTime: " & objItem.KernelTime
      WScript.Echo "MofData: " & objItem.MofData
      WScript.Echo "MofLength: " & objItem.MofLength
      strParentGuid = Join(objItem.ParentGuid, ",")
         WScript.Echo "ParentGuid: " & strParentGuid
      WScript.Echo "ParentInstanceId: " & objItem.ParentInstanceId
      WScript.Echo "ProcessId: " & objItem.ProcessId
      WScript.Echo "ReservedHeaderField: " & objItem.ReservedHeaderField
      WScript.Echo "ThreadId: " & objItem.ThreadId
      WScript.Echo "TimeStamp: " & objItem.TimeStamp
      WScript.Echo "TraceLevel: " & objItem.TraceLevel
      WScript.Echo "TraceVersion: " & objItem.TraceVersion
      WScript.Echo "UserTime: " & objItem.UserTime
      WScript.Echo
   Next
Next
```