

Content of WMI Image_V0_Load Query.js (Site 1)

```
var wbemFlagReturnImmediately = 0x10;
var wbemFlagForwardOnly = 0x20;

var arrComputers = new Array("");
for (i = 0; i < arrComputers.length; i++) {
    WScript.Echo();
    WScript.Echo("=====");
    WScript.Echo("Computer: " + arrComputers[i]);
    WScript.Echo("=====");

    var objWMIService = GetObject("winmgmts:\\\\" + arrComputers[i] + "\\root\\WMI");
    var collItems = objWMIService.ExecQuery("SELECT * FROM Image_V0_Load", "WQL",
        wbemFlagReturnImmediately | wbemFlagForwardOnly);

    var enumItems = new Enumerator(collItems);
    for (; !enumItems.atEnd(); enumItems.moveNext()) {
        var objItem = enumItems.item();

        WScript.Echo("BaseAddress: " + objItem.BaseAddress);
        try { WScript.Echo("EventGuid: " + (objItem.EventGuid.toArray().join(", ")); }
        catch(e) { WScript.Echo("EventGuid: null"); }
        WScript.Echo("EventSize: " + objItem.EventSize);
        WScript.Echo("EventType: " + objItem.EventType);
        WScript.Echo("Flags: " + objItem.Flags);
        WScript.Echo("ImageFileName: " + objItem.ImageFileName);
        WScript.Echo("InstanceID: " + objItem.InstanceID);
        WScript.Echo("KernelTime: " + objItem.KernelTime);
        WScript.Echo("ModuleSize: " + objItem.ModuleSize);
        WScript.Echo("MofData: " + objItem.MofData);
        WScript.Echo("MofLength: " + objItem.MofLength);
        try { WScript.Echo("ParentGuid: " + (objItem.ParentGuid.toArray().join(", ")); }
        catch(e) { WScript.Echo("ParentGuid: null"); }
        WScript.Echo("ParentInstanceID: " + objItem.ParentInstanceID);
        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);
    }
}
```