CNT 4603: System Administration
Spring 2015

Project Seven – PowerShell Scripting And Digitally Signing Scripts

Instructor : Dr. Mark Llewellyn

Email: markl@cs.ucf.edu
Office: HEC 236, 407-823-2790
Office Hours: M&W 1:00-3:00pm, T&Th 10:30am-12:30pm

Department of Electrical Engineering and Computer Science
Computer Science Division
University of Central Florida

Project Seven

- **Title:** "Project Seven: PowerShell Scripting And Digitally Signing Scripts"
- **Points:** 50 points
- **Due Date:** April 19, 2015 by 11:59 pm WebCourses time.

- **Objectives:** To create a PowerShell script using best standards and practices for script creation and to digitally sign the script.
- **Deliverables:**
  1. Screen shots as shown on pages 6, 7, 8, 9, 10, and 11.
  2. The digitally signed source code for your script.

Project Seven – Background

- We'll focus on PowerShell scripting for this assignment. While we haven't dealt with all of the various aspects of PowerShell scripting, we have covered enough in the lecture notes for you to be able to create a useful system administrator script.

- In keeping with the discussions in PowerShell – Parts 3 and 5 lecture notes, that dealt with best practices and standards for scripting, you will need to follow these principles for this project. Namely, in the overall layout of the script, naming conventions, and appending a digital signature to your script.

- Use either your `Mark-Server1` or `Mark-Server2` for this project. You'll need PowerShell Version 2.

Project Seven – Background

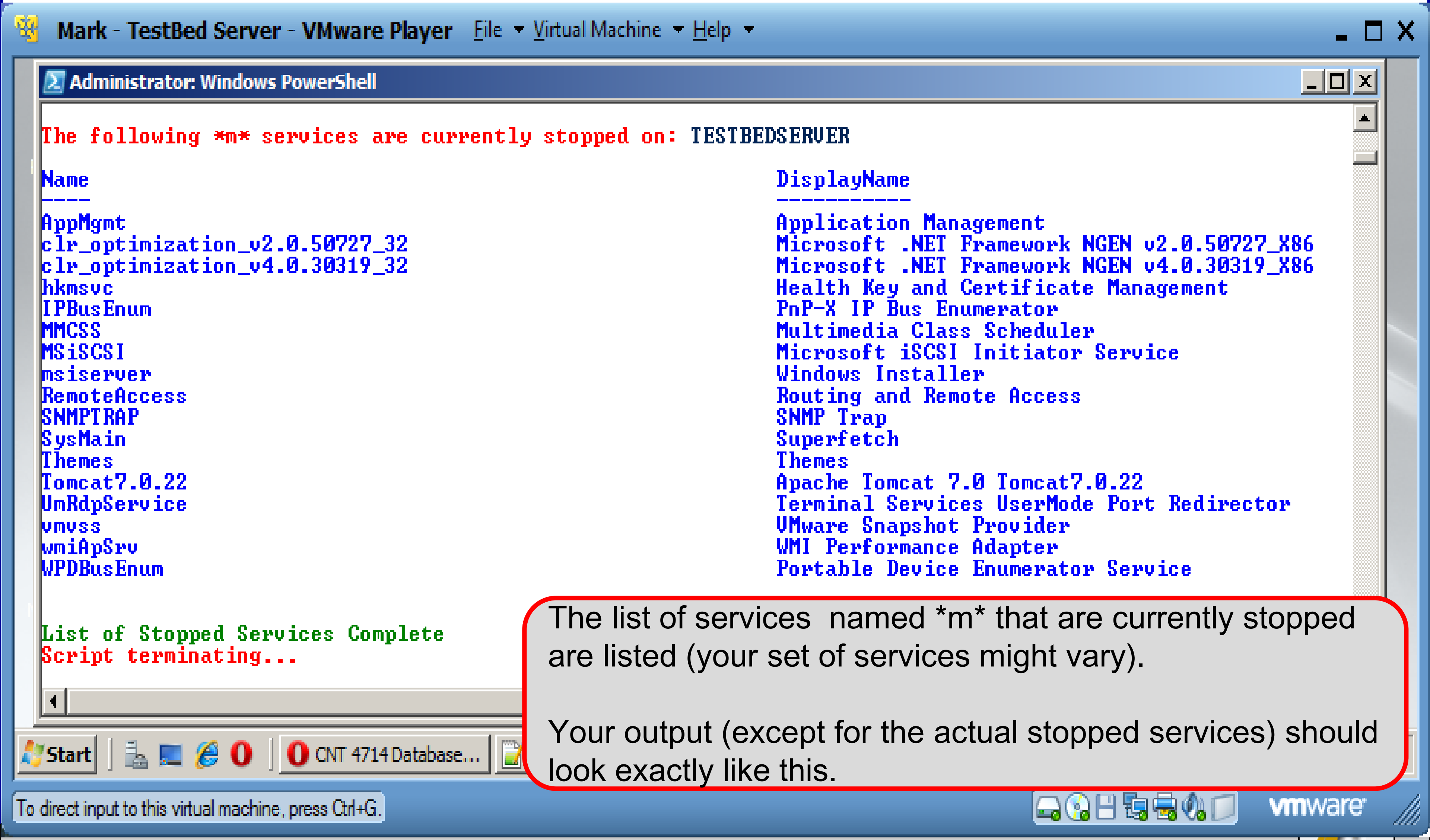
- The script you will create will list all of the currently stopped , on the server where the script is executed, that begin with a certain, user supplied (an input parameter to the script), prefix (e.g., A*, *c*, m*, A*, or some variation).

- Your script should be named according to the verb-noun conventions we discussed (see page 38 – part 3 notes).

- Your script should follow a professional format (see pages 12-on in part 5 notes).

- The pages that follow explain the details of the project, stepping you through the actions. In the various callouts, the items that appear in **bold green** text require you to do screen captures and/or answer questions. These screen captures and answers will constitute your submission for this project. Be sure that your server's name is visible in all screenshots.

Project Seven – Output of the Script



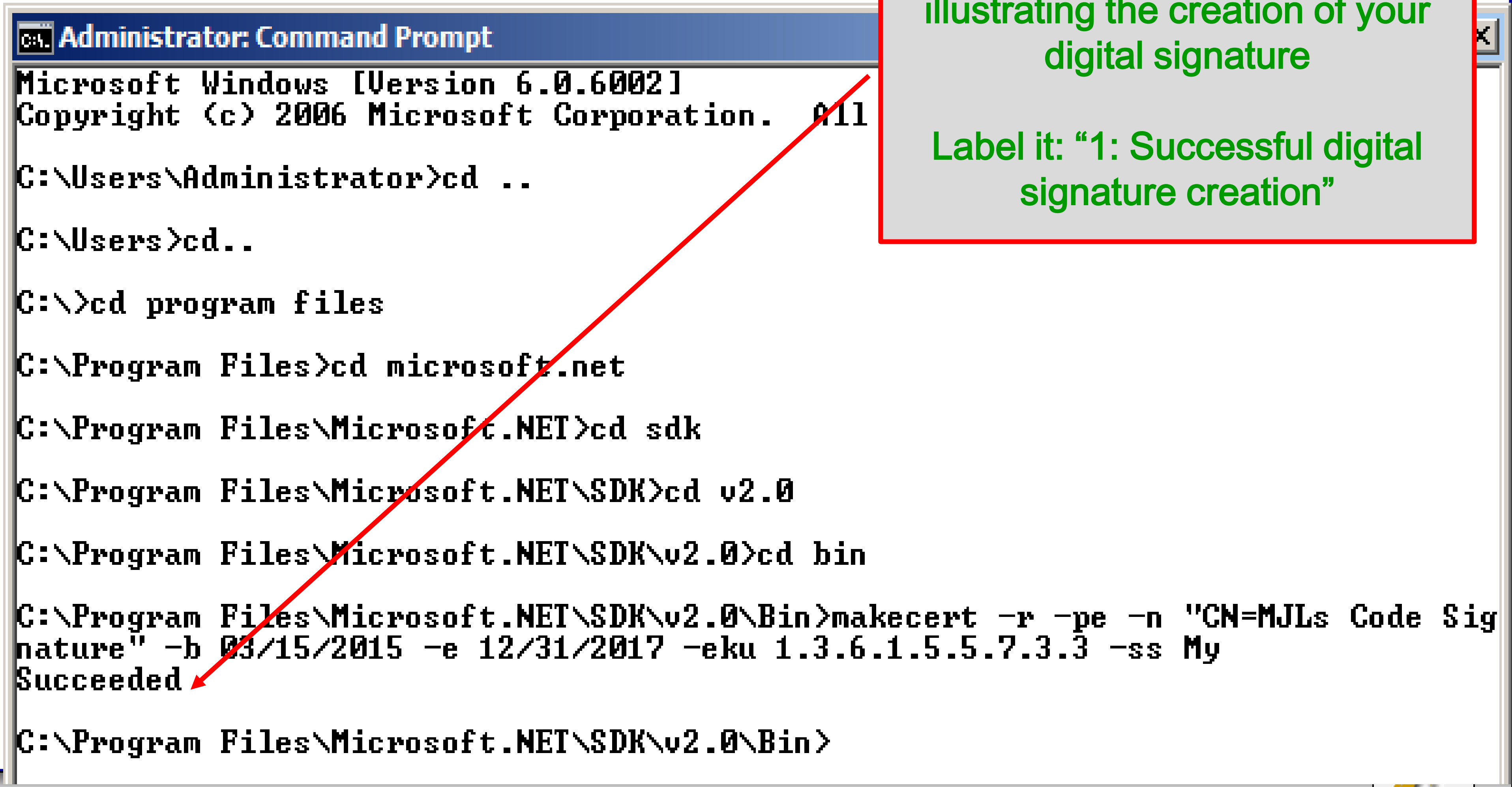
Mark - TestBed Server - VMware Player
File
Virtual Machine
Help
Administrator: Windows PowerShell
Start
CNT 4714 Database...
To direct input to this virtual machine, press Ctrl+G.
vmware

```
The following *m* services are currently stopped on: TESTBEDSERVER

Name                                                       DisplayName
----                                                       -----------
AppMgmt                                                    Application Management
clr_optimization_v2.0.50727_32                             Microsoft .NET Framework NGEN v2.0.50727_X86
clr_optimization_v4.0.30319_32                             Microsoft .NET Framework NGEN v4.0.30319_X86
hkmsvc                                                     Health Key and Certificate Management
IPBusEnum                                                  PnP-X IP Bus Enumerator
MMCSS                                                      Multimedia Class Scheduler
MSiSCSI                                                    Microsoft iSCSI Initiator Service
msiserver                                                  Windows Installer
RemoteAccess                                               Routing and Remote Access
SNMPTRAP                                                   SNMP Trap
SysMain                                                    Superfetch
Themes                                                     Themes
Tomcat7.0.22                                               Apache Tomcat 7.0 Tomcat7.0.22
UmRdpService                                               Terminal Services UserMode Port Redirector
vmvss                                                      VMware Snapshot Provider
wmiApSrv                                                   WMI Performance Adapter
WPDBusEnum                                                 Portable Device Enumerator Service


List of Stopped Services Complete
Script terminating...
```

The list of services named *m* that are currently stopped are listed (your set of services might vary).

Your output (except for the actual stopped services) should look exactly like this.

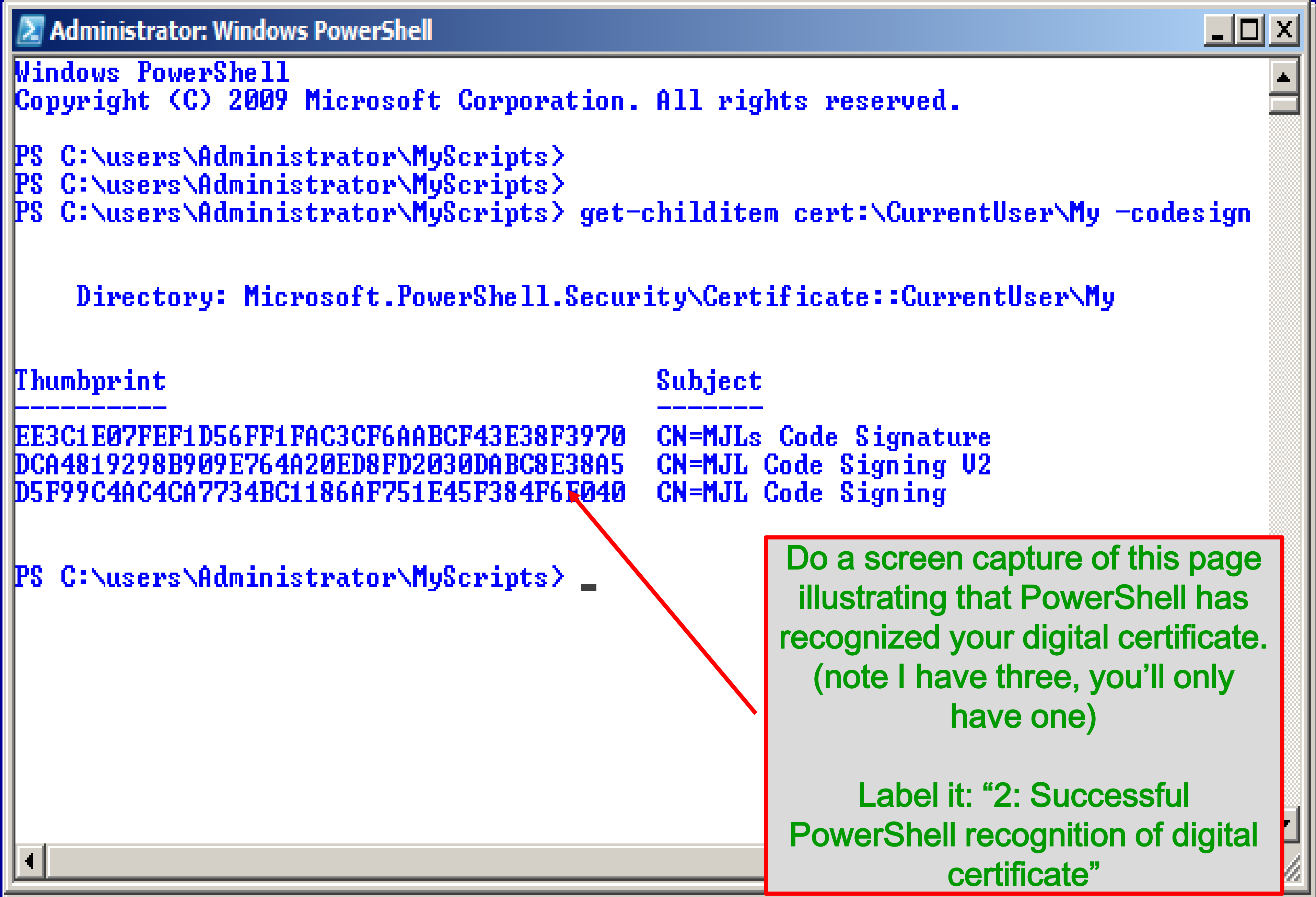
Project Seven – Creating The Digital Signature



```
Microsoft Windows [Version 6.0.6002]
Copyright (c) 2006 Microsoft Corporation.  All

C:\Users\Administrator>cd ..

C:\Users>cd..

C:\>cd program files

C:\Program Files>cd microsoft.net

C:\Program Files\Microsoft.NET>cd sdk

C:\Program Files\Microsoft.NET\SDK>cd v2.0

C:\Program Files\Microsoft.NET\SDK\v2.0>cd bin

C:\Program Files\Microsoft.NET\SDK\v2.0\Bin>makecert -r -pe -n "CN=MJLs Code Sig
nature" -b 03/15/2015 -e 12/31/2017 -eku 1.3.6.1.5.5.7.3.3 -ss My
Succeeded

C:\Program Files\Microsoft.NET\SDK\v2.0\Bin>
```

Do a screen capture of this page illustrating the creation of your digital signature

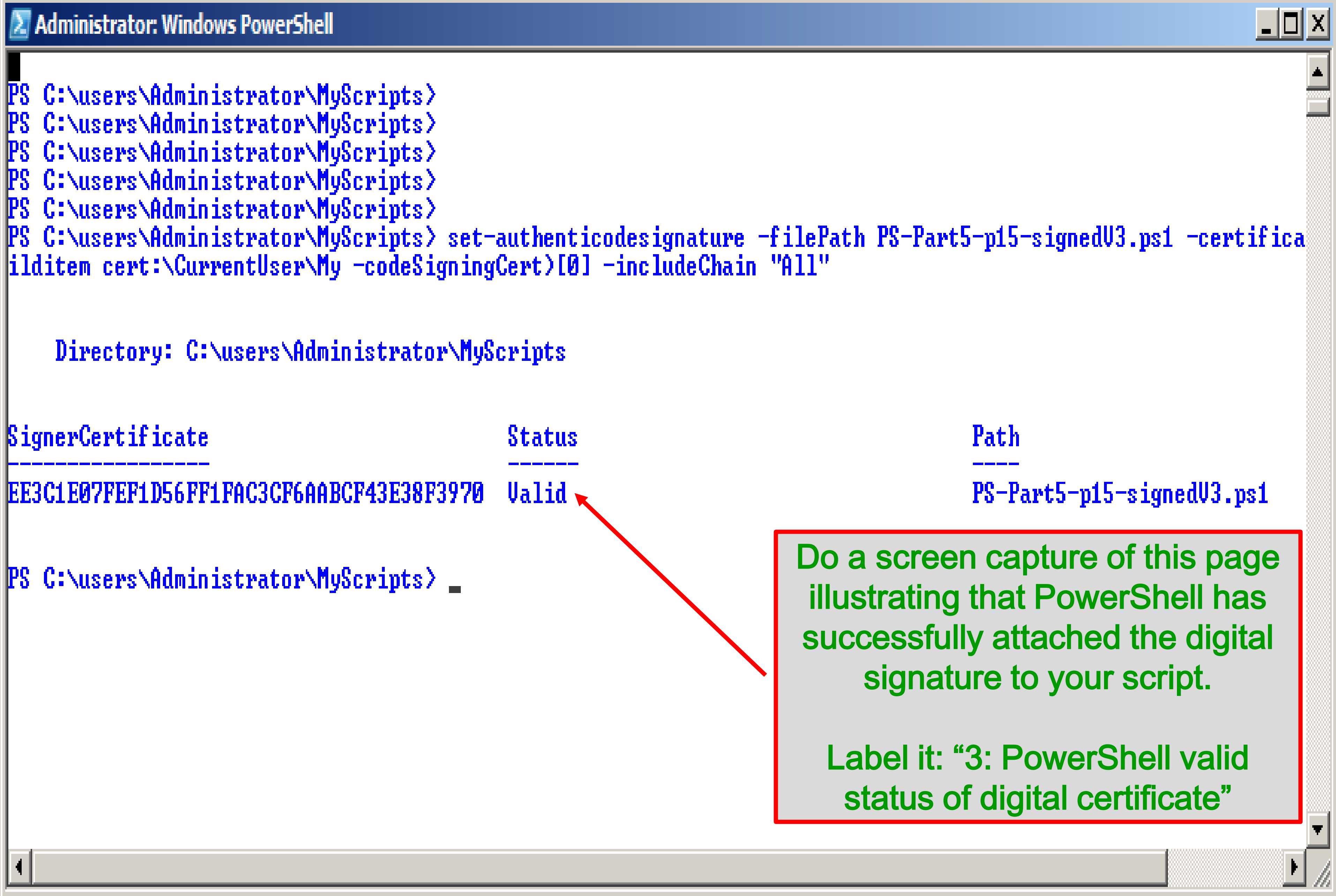
Label it: “1: Successful digital signature creation”



```
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\users\Administrator\MyScripts>
PS C:\users\Administrator\MyScripts>
PS C:\users\Administrator\MyScripts> get-childitem cert:\CurrentUser\My -codesign


    Directory: Microsoft.PowerShell.Security\Certificate::CurrentUser\My


Thumbprint                                Subject
----------                                -------
EE3C1E07FEF1D56FF1FAC3CF6AABCF43E38F3970  CN=MJLs Code Signature
DCA4819298B909E764A20ED8FD2030DABC8E38A5  CN=MJL Code Signing V2
D5F99C4AC4CA7734BC1186AF751E45F384F6F040  CN=MJL Code Signing


PS C:\users\Administrator\MyScripts> _
```

Do a screen capture of this page illustrating that PowerShell has recognized your digital certificate. (note I have three, you'll only have one)

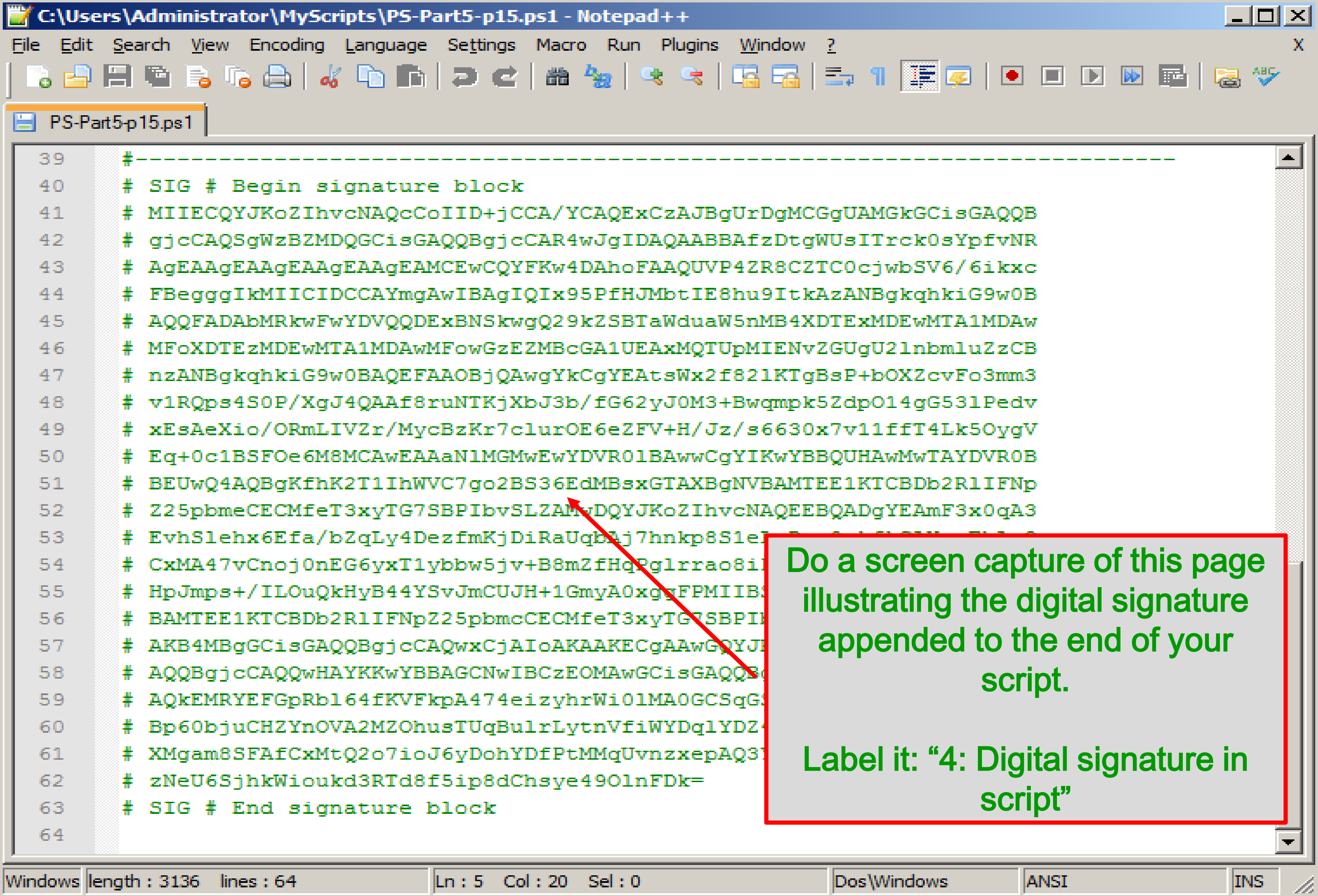
Label it: "2: Successful PowerShell recognition of digital certificate"



```
PS C:\users\Administrator\MyScripts>
PS C:\users\Administrator\MyScripts>
PS C:\users\Administrator\MyScripts>
PS C:\users\Administrator\MyScripts>
PS C:\users\Administrator\MyScripts>
PS C:\users\Administrator\MyScripts> set-authenticodesignature -filePath PS-Part5-p15-signedV3.ps1 -certifica
ilditem cert:\CurrentUser\My -codeSigningCert)[0] -includeChain "All"


    Directory: C:\users\Administrator\MyScripts


SignerCertificate                         Status                                      Path
-----------------                         ------                                      ----
EE3C1E07FEF1D56FF1FAC3CF6AABCF43E38F3970  Valid                                       PS-Part5-p15-signedV3.ps1


PS C:\users\Administrator\MyScripts> _
```

Do a screen capture of this page illustrating that PowerShell has successfully attached the digital signature to your script.

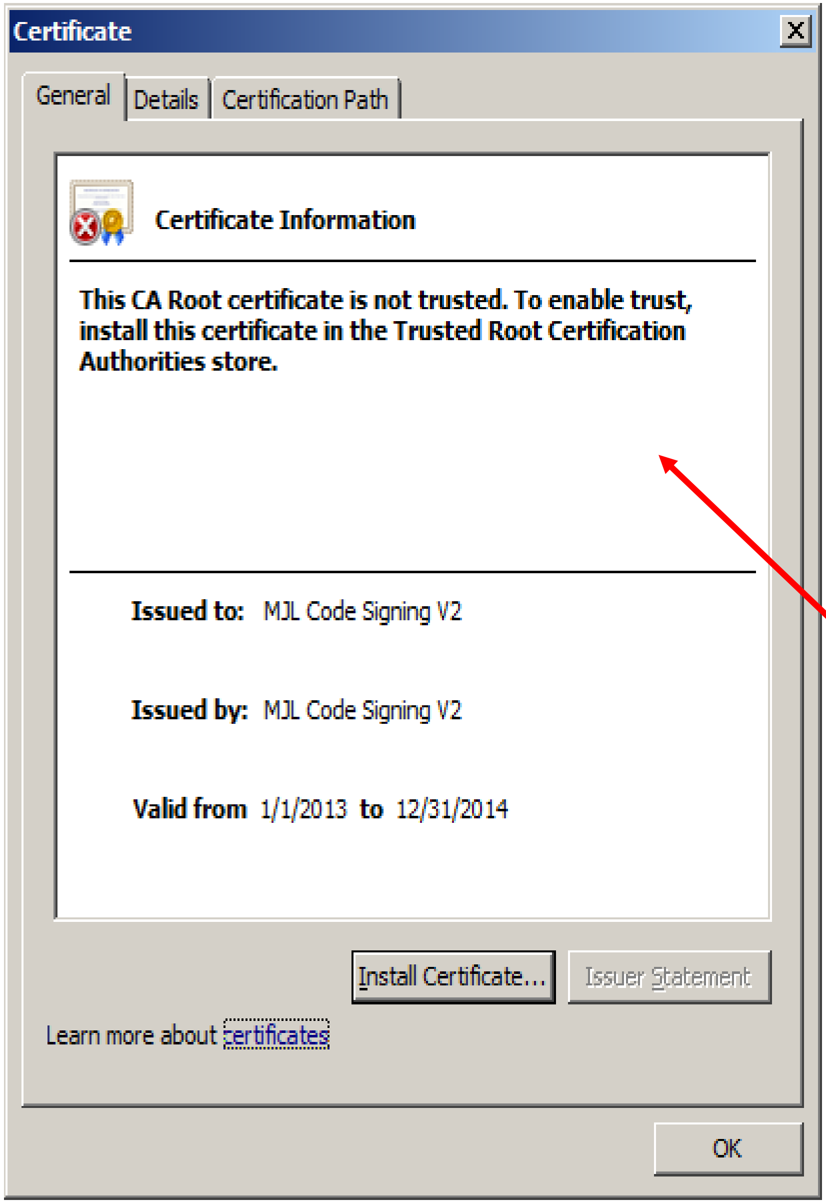
Label it: “3: PowerShell valid status of digital certificate”


C:\Users\Administrator\MyScripts\PS-Part5-p15.ps1 - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
PS-Part5-p15.ps1
Windows length : 3136 lines : 64 Ln : 5 Col : 20 Sel : 0 Dos\Windows ANSI INS

```
#------------------------------------------------------------------------------
# SIG # Begin signature block
# MIIECQYJKoZIhvcNAQcCoIID+jCCA/YCAQExCzAJBgUrDgMCGgUAMGkGCisGAQQB
# gjcCAQSgWzBZMDQGCisGAQQBgjcCAR4wJgIDAQAABBAfzDtgWUsITrck0sYpfvNR
# AgEAAgEAAgEAAgEAAgEAMCEwCQYFKw4DAhoFAAQUVP4ZR8CZTC0cjwbSV6/6ikxc
# FBegggIkMIICIDCCAYmgAwIBAgIQIx95PfHJMbtIE8hu9ItkAzANBgkqhkiG9w0B
# AQQFADAbMRkwFwYDVQQDExBNSkwgQ29kZSBTaWduaW5nMB4XDTExMDEwMTA1MDAw
# MFoXDTEzMDEwMTA1MDAwMFowGzEZMBcGA1UEAxMQTUpMIENvZGUgU2lnbmluZzCB
# nzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAtsWx2f821KTgBsP+bOXZcvFo3mm3
# v1RQps4S0P/XgJ4QAAf8ruNTKjXbJ3b/fG62yJ0M3+Bwqmpk5ZdpO14gG531Pedv
# xEsAeXio/ORmLIVZr/MycBzKr7clurOE6eZFV+H/Jz/s6630x7v11ffT4Lk5OygV
# Eq+0c1BSFOe6M8MCAwEAAaN1MGMwEwYDVR01BAwwCgYIKwYBBQUHAwMwTAYDVR0B
# BEUwQ4AQBgKfhK2T1IhWVC7go2BS36EdMBsxGTAXBgNVBAMTEE1KTCBDb2RlIFNp
# Z25pbmeCECMfeT3xyTG7SBPIbvSLZAMwDQYJKoZIhvcNAQEEBQADgYEAmF3x0qA3
# EvhSlehx6Efa/bZqLy4DezfmKjDiRaUqbAj7hnkp8S1e
# CxMA47vCnoj0nEG6yxT1ybbw5jv+B8mZfHqPglrrao8il
# HpJmps+/ILOuQkHyB44YSvJmCUJH+1GmyA0xggFPMIIB
# BAMTEE1KTCBDb2RlIFNpZ25pbmcCECMfeT3xyTG7SBPI
# AKB4MBgGCisGAQQBgjcCAQwxCjAIoAKAAKECgAAwGQYJ
# AQQBgjcCAQQwHAYKKwYBBAGCNwIBCzEOMAwGCisGAQQB
# AQkEMRYEFGpRbl64fKVFkpA474eizyhrWi01MA0GCSqG
# Bp60bjuCHZYnOVA2MZOhusTUqBulrLytnVfiWYDqlYDZ
# XMgam8SFAfCxMtQ2o7ioJ6yDohYDfPtMMqUvnzxepAQ3
# zNeU6SjhkWioukd3RTd8f5ip8dChsye49OlnFDk=
# SIG # End signature block
```

Do a screen capture of this page illustrating the digital signature appended to the end of your script.

Label it: “4: Digital signature in script”



This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: MJL Code Signing V2

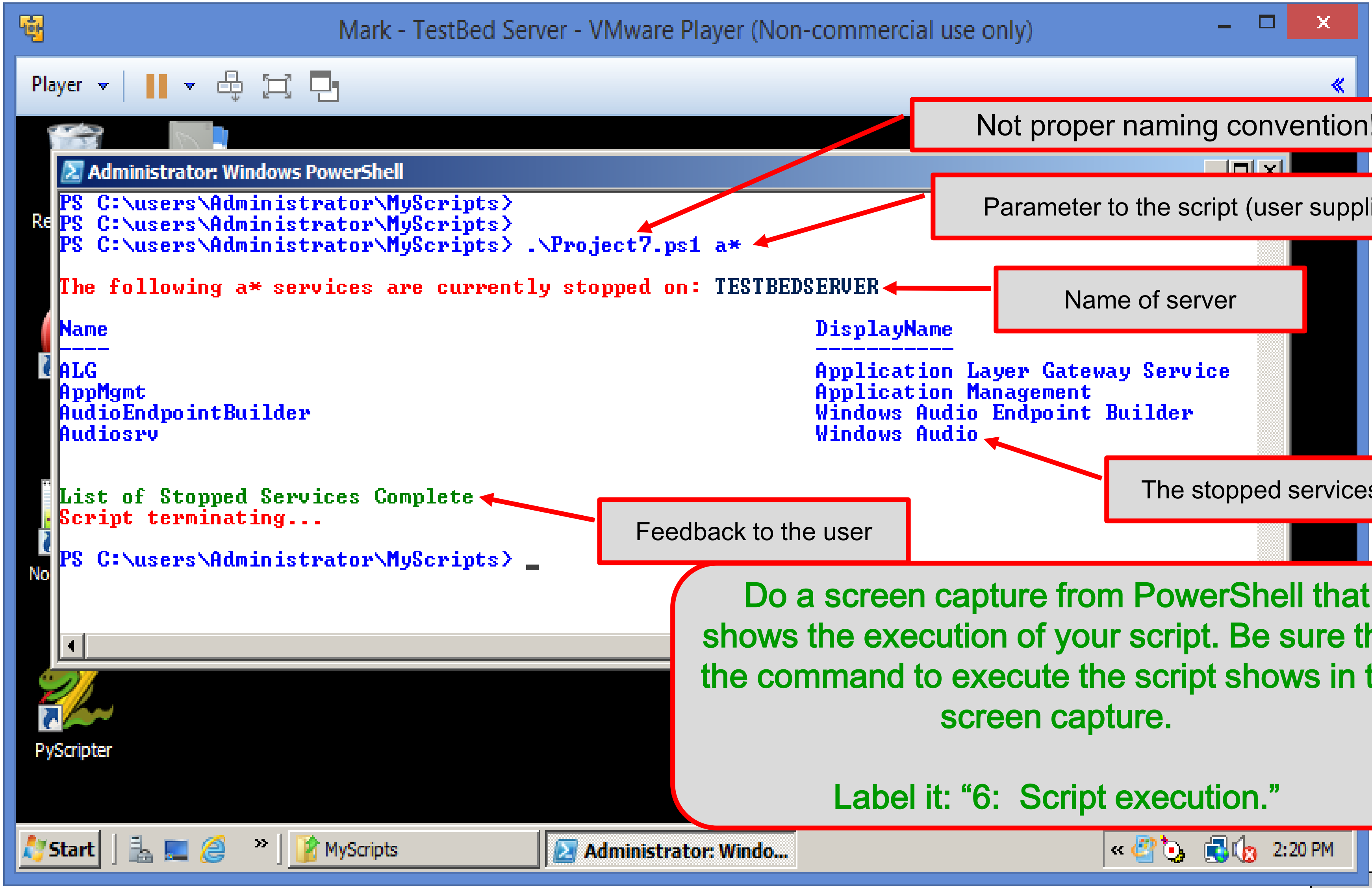
Issued by: MJL Code Signing V2

Valid from 1/1/2013 to 12/31/2014

Do a screen capture of this dialog that appears during the process of registering your CA.

Label it: “5: Preparing to install certificate.”

Project Seven – Output of the Script



Mark - TestBed Server - VMware Player (Non-commercial use only)
Player
Administrator: Windows PowerShell
PyScripter
Start
MyScripts
Administrator: Windo...
2:20 PM

```
PS C:\users\Administrator\MyScripts>
PS C:\users\Administrator\MyScripts>
PS C:\users\Administrator\MyScripts> .\Project7.ps1 a*

The following a* services are currently stopped on: TESTBEDSERVER

Name                                                        DisplayName
----                                                        -----------
ALG                                                         Application Layer Gateway Service
AppMgmt                                                     Application Management
AudioEndpointBuilder                                        Windows Audio Endpoint Builder
Audiosrv                                                    Windows Audio


List of Stopped Services Complete
Script terminating...

PS C:\users\Administrator\MyScripts> _
```

Not proper naming convention!

Parameter to the script (user supplied)

Name of server

The stopped services

Feedback to the user

Do a screen capture from PowerShell that shows the execution of your script. Be sure that the command to execute the script shows in the screen capture.

Label it: “6: Script execution.”