WINDOWS COMMAND LINE

```
C:\Users\nagalman>taskkill /IM notepad.exe
SUCCESS: Sent termination signal to the process "notepad.exe" with PID 1392.

C:\Users\nagalman>
```

Outline

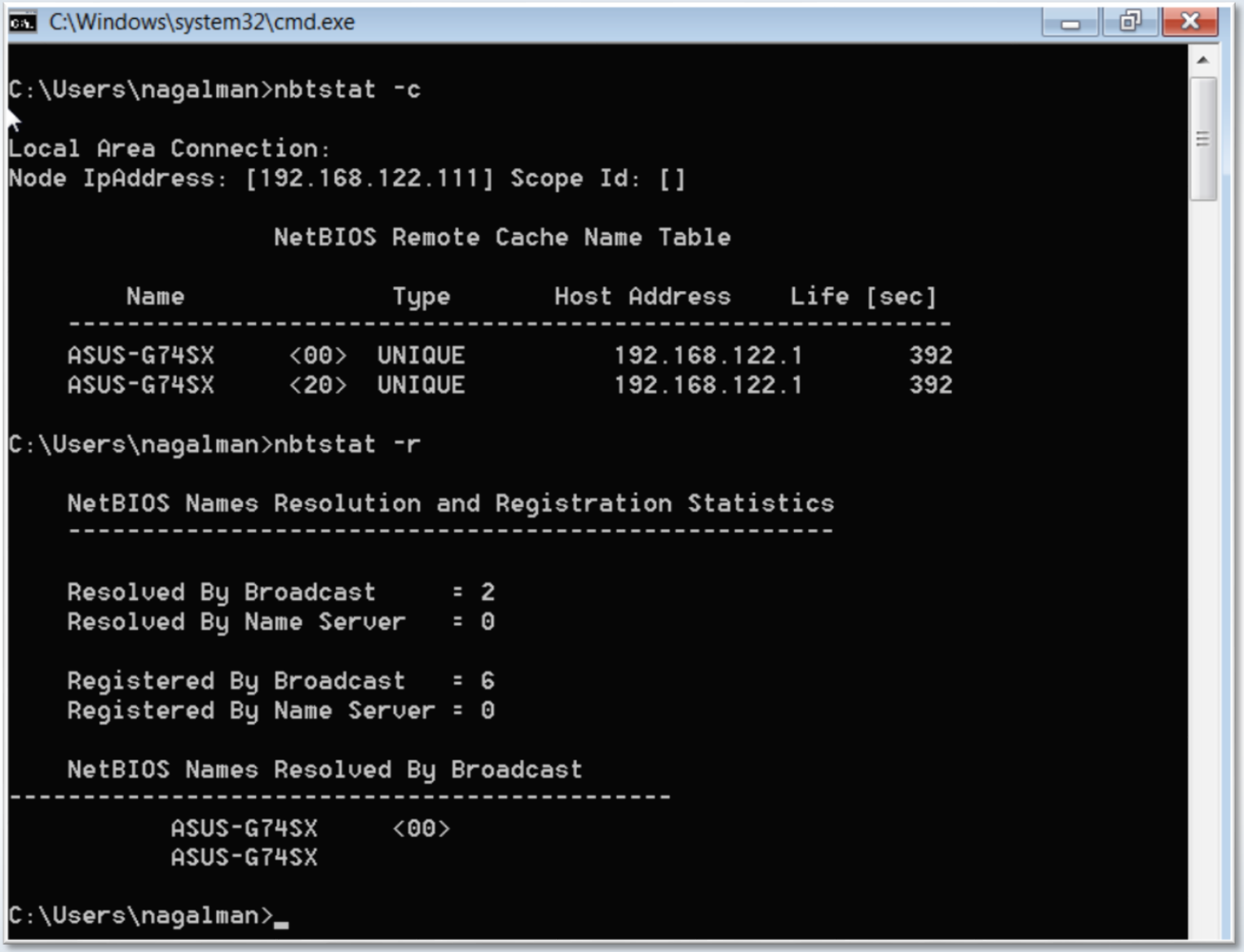
- Windows Command Line
- nbstat
- Taskkill
- bootrec
- fixboot
- fixmbr
- shutdown
- tasklist
- md
- rd

Outline

- cd
- del
- format
- copy
- xcopy
- robocopy
- diskpart
- sfc
- chkdsk

- A command-line interface (CLI) is a way to interact with a computer by issuing commands to the computer in the form of successive lines of text (command lines)
- All desktop OSs have a CLI
- Very powerful and fast for experienced users
- Very low resource interface
- Biggest disadvantage is having to learn and remember all the commands

- a diagnostic tool for NetBIOS over TCP/IP to help troubleshoot NetBIOS name resolution problems
- nbtstat -c
- -c: displays the contents of the NetBIOS name cache, the table of NetBIOS names and their resolved IP addresses.
- -n: displays the names that have been registered locally on the system.
- -r: displays the count of all NetBIOS names resolved by broadcast and querying a WINS server.
- -R: purges and reloads the remote cache name table.
- -RR: sends name release packets to WINs and then starts Refresh.
- -s: lists the current NetBIOS sessions and their status, including statistics.
- -S: lists sessions table with the destination IP addresses.
- nbtstat help


C:\Windows\system32\cmd.exe
C:\Users\nagalman>nbtstat -c
Local Area Connection:
Node IpAddress: [192.168.122.111] Scope Id: []
NetBIOS Remote Cache Name Table
Name Type Host Address Life [sec]
ASUS-G74SX <00> UNIQUE 192.168.122.1 392
ASUS-G74SX <20> UNIQUE 192.168.122.1 392
C:\Users\nagalman>nbtstat -r
NetBIOS Names Resolution and Registration Statistics
Resolved By Broadcast = 2
Resolved By Name Server = 0
Registered By Broadcast = 6
Registered By Name Server = 0
NetBIOS Names Resolved By Broadcast
ASUS-G74SX <00>
ASUS-G74SX
C:\Users\nagalman>

Taskkill

- Terminates a process (program, application) by process ID or name
- taskkill /IM cmd.exe
- Taskkill /?

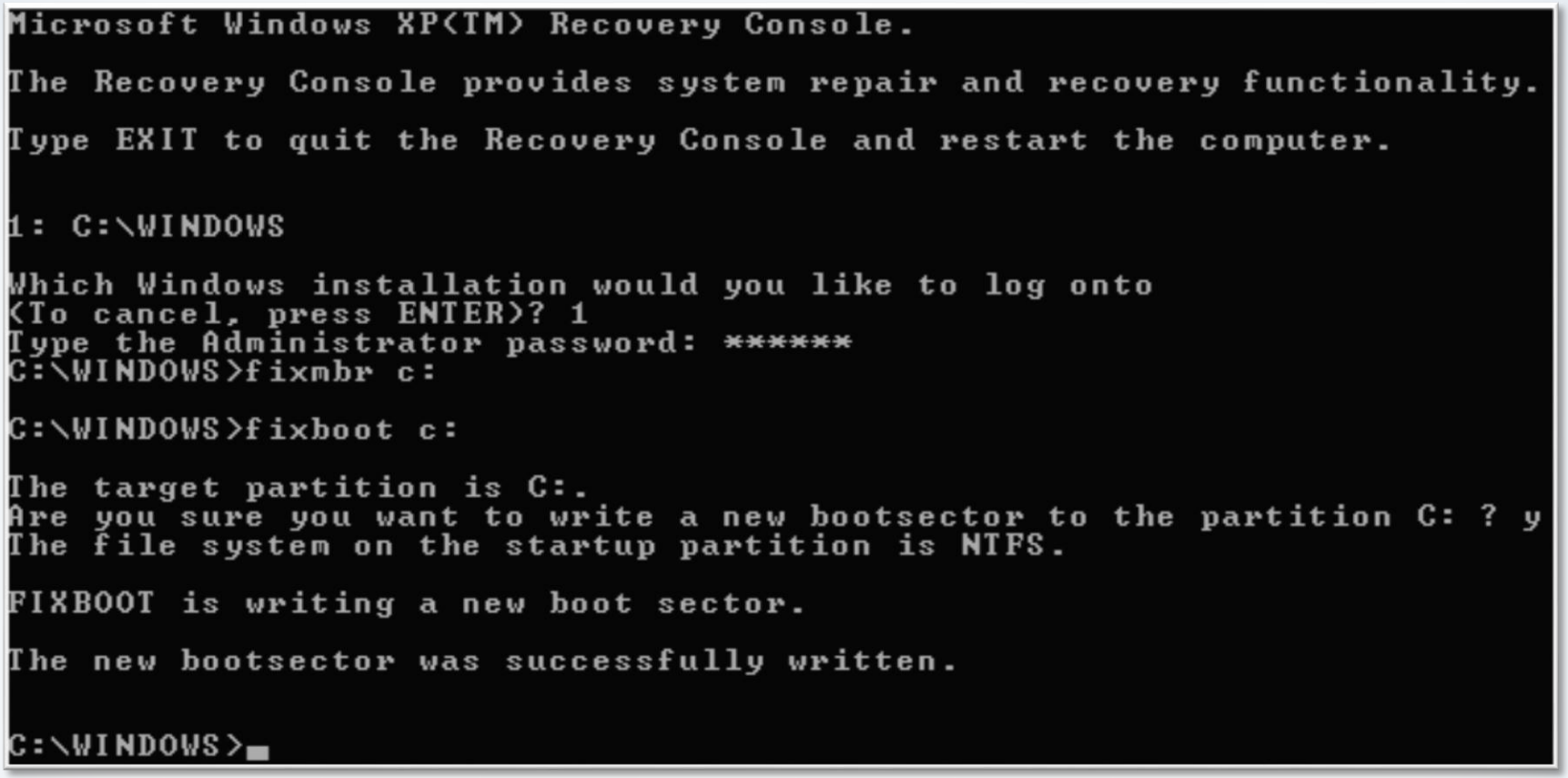
- Used in the Windows Recovery Environment to troubleshoot and repair the following in Windows Vista or Windows 7:
  - A master boot record (MBR)
  - A boot sector
  - A Boot Configuration Data (BCD) store
- Bootrec.exe /fixmbr

```
DISKPART> exit

Leaving DiskPart...

X:\Sources>bootrec.exe /fixmbr
The operation completed successfully.

X:\Sources>bootrec.exe /fixboot
The operation completed successfully.

X:\Sources>bootrec.exe /RebuildBcd
Scanning all disks for Windows installations.

Please wait, since this may take a while...

Successfully scanned Windows installations.
Total identified Windows installations: 1
[1]  C:\Windows
Add installation to boot list? Yes(Y)/No(N)/All(A):Y
The operation completed successfully.

X:\Sources>exit_
```

- Used in the Windows Recovery Environment to write a new partition boot sector to the system partition
- fixboot c:


Microsoft Windows XP(TM) Recovery Console.
The Recovery Console provides system repair and recovery functionality.
Type EXIT to quit the Recovery Console and restart the computer.
1: C:\WINDOWS
Which Windows installation would you like to log onto
(To cancel, press ENTER)? 1
Type the Administrator password:
C:\WINDOWS>fixboot
The target partition is C:.
Are you sure you want to write a new bootsector to the partition C: ? y
The file system on the startup partition is NTFS.
FIXBOOT is writing a new boot sector.
The new bootsector was successfully written.
C:\WINDOWS>

- Repairs the master boot record of the boot disk
- fixmbr\Device\HardDisk0


Microsoft Windows XP(TM) Recovery Console.
The Recovery Console provides system repair and recovery functionality.
Type EXIT to quit the Recovery Console and restart the computer.
1: C:\WINDOWS
Which Windows installation would you like to log onto
(To cancel, press ENTER)? 1
Type the Administrator password: ******
C:\WINDOWS>fixmbr c:
C:\WINDOWS>fixboot c:
The target partition is C:.
Are you sure you want to write a new bootsector to the partition C: ? y
The file system on the startup partition is NTFS.
FIXBOOT is writing a new boot sector.
The new bootsector was successfully written.
C:\WINDOWS>

shutdown

- Allows you to shutdown or restart a local or remote computer
- shutdown /?

- Displays a list of applications and services with their Process ID (PID) for all tasks running on either a local or a remote computer

tasklist

```
C:\Users\nagalman>tasklist

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0         24 K
System                           4 Services                   0        588 K
smss.exe                       264 Services                   0        832 K
csrss.exe                      344 Services                   0      4,084 K
wininit.exe                    392 Services                   0      3,692 K
csrss.exe                      404 Console                    1      4,864 K
winlogon.exe                   440 Console                    1      6,384 K
services.exe                   484 Services                   0     10,636 K
lsass.exe                      508 Services                   0      8,916 K
lsm.exe                        516 Services                   0      3,704 K
svchost.exe                    616 Services                   0      7,348 K
svchost.exe                    716 Services                   0      6,632 K
svchost.exe                    832 Services                   0     15,596 K
svchost.exe                    864 Services                   0     87,276 K
svchost.exe                    904 Services                   0     15,216 K
svchost.exe                    936 Services                   0     31,596 K
svchost.exe                    300 Services                   0      5,856 K
svchost.exe                   1016 Services                   0     21,852 K
spoolsv.exe                   1188 Services                   0      9,024 K
svchost.exe                   1240 Services                   0     13,488 K
armsvc.exe                    1340 Services                   0      3,392 K
mDNSResponder.exe             1408 Services                   0      4,504 K
EloSrvce.exe                  1464 Services                   0      4,116 K
svchost.exe                   1504 Services                   0     13,344 K
sqlservr.exe                  1540 Services                   0     15,324 K
QBCFMonitorService.exe        1736 Services                   0     11,204 K
sqlbrowser.exe                1924 Services                   0      3,424 K
sqlwriter.exe                 1956 Services                   0      5,244 K
TeamViewer_Service.exe        2000 Services                   0      7,504 K
QBDBMgrN.exe                  2884 Services                   0     15,084 K
taskhost.exe                  3056 Console                    1      9,388 K
dwm.exe                       2468 Console                    1      5,080 K
explorer.exe                   712 Console                    1     52,216 K
```

- Make directory – creates a folder, directory, or subdirectory
- md \School\UMBC
- Can substitute mkdir for md

```
c:\Users\nagalman>md School

c:\Users\nagalman>cd School

c:\Users\nagalman\School>mkdir UMBC

c:\Users\nagalman\School>dir
 Volume in drive C has no label.
 Volume Serial Number is D8A7-740C

 Directory of c:\Users\nagalman\School

07/22/2013  01:46 PM    <DIR>          .
07/22/2013  01:46 PM    <DIR>          ..
07/22/2013  01:46 PM    <DIR>          UMBC
               0 File(s)              0 bytes
               3 Dir(s)   6,096,531,456 bytes free

c:\Users\nagalman\School>
```

- Remove directory – deletes a folder, directory, or subdirectory
- rd \School\UMBC
- Can substitute rmdir for rd

```
c:\Users\nagalman\School>dir
 Volume in drive C has no label.
 Volume Serial Number is D8A7-740C

 Directory of c:\Users\nagalman\School

07/22/2013  01:46 PM    <DIR>          .
07/22/2013  01:46 PM    <DIR>          ..
07/22/2013  01:46 PM    <DIR>          UMBC
               0 File(s)              0 bytes
               3 Dir(s)   6,096,703,488 bytes free

c:\Users\nagalman\School>rd UMBC

c:\Users\nagalman\School>dir
 Volume in drive C has no label.
 Volume Serial Number is D8A7-740C

 Directory of c:\Users\nagalman\School

07/22/2013  01:59 PM    <DIR>          .
07/22/2013  01:59 PM    <DIR>          ..
               0 File(s)              0 bytes
               2 Dir(s)   6,096,703,488 bytes free

c:\Users\nagalman\School>
```

- Change directory – displays the name of the current directory or changes the current folder
- cd \School\UMBC
- Can substitute chdir for cd

```
c:\Users\nagalman>dir
 Volume in drive C has no label.
 Volume Serial Number is D8A7-740C

 Directory of c:\Users\nagalman

07/22/2013  01:46 PM    <DIR>          .
07/22/2013  01:46 PM    <DIR>          ..
12/14/2012  02:21 AM    <DIR>          .gimp-2.8
12/14/2012  02:18 AM    <DIR>          .thumbnails
05/19/2013  02:44 AM    <DIR>          Contacts
07/21/2013  08:04 PM    <DIR>          Desktop
06/07/2013  05:17 AM    <DIR>          Documents
07/02/2013  06:42 PM    <DIR>          Downloads
05/19/2013  02:44 AM    <DIR>          Favorites
05/19/2013  02:44 AM    <DIR>          Links
05/19/2013  02:44 AM    <DIR>          Music
05/19/2013  02:44 AM    <DIR>          Pictures
05/19/2013  02:44 AM    <DIR>          Saved Games
07/22/2013  01:59 PM    <DIR>          School
05/19/2013  02:44 AM    <DIR>          Searches
05/19/2013  02:44 AM    <DIR>          Videos
               0 File(s)              0 bytes
              16 Dir(s)   6,096,179,200 bytes free

c:\Users\nagalman>cd School

c:\Users\nagalman\School>
```

del

- Deletes files
- del grade.txt
- Can substitute erase for del

del

```
c:\Users\nagalman\School>dir
 Volume in drive C has no label.
 Volume Serial Number is D8A7-740C

 Directory of c:\Users\nagalman\School

07/22/2013  02:06 PM    <DIR>          .
07/22/2013  02:06 PM    <DIR>          ..
07/22/2013  02:06 PM                 5 grades.txt
               1 File(s)              5 bytes
               2 Dir(s)   6,095,650,816 bytes free

c:\Users\nagalman\School>del grades.txt

c:\Users\nagalman\School>dir
 Volume in drive C has no label.
 Volume Serial Number is D8A7-740C

 Directory of c:\Users\nagalman\School

07/22/2013  02:07 PM    <DIR>          .
07/22/2013  02:07 PM    <DIR>          ..
               0 File(s)              0 bytes
               2 Dir(s)   6,095,650,816 bytes free

c:\Users\nagalman\School>_
```

- Formats the disk in the specified volume to accept Windows files
- format a:
- format /?

- Copies one or more files from one location to another
- copy Members.xls Cancel
- copy /?

```
c:\Users\nagalman\School>dir
 Volume in drive C has no label.
 Volume Serial Number is D8A7-740C

 Directory of c:\Users\nagalman\School

07/22/2013  02:18 PM    <DIR>          .
07/22/2013  02:18 PM    <DIR>          ..
07/22/2013  02:18 PM                 5 grades.txt
07/22/2013  02:18 PM    <DIR>          UMBC
               1 File(s)              5 bytes
               3 Dir(s)   6,095,650,816 bytes free

c:\Users\nagalman\School>copy grades.txt UMBC
        1 file(s) copied.

c:\Users\nagalman\School>cd UMBC

c:\Users\nagalman\School\UMBC>dir
 Volume in drive C has no label.
 Volume Serial Number is D8A7-740C

 Directory of c:\Users\nagalman\School\UMBC

07/22/2013  02:19 PM    <DIR>          .
07/22/2013  02:19 PM    <DIR>          ..
07/22/2013  02:18 PM                 5 grades.txt
               1 File(s)              5 bytes
               2 Dir(s)   6,095,650,816 bytes free

c:\Users\nagalman\School\UMBC>
```

- Copies files and directories, including subdirectories.
- xcopy Members.xls Cancel
- xcopy /?

```
c:\Users\nagalman\School>dir
 Volume in drive C has no label.
 Volume Serial Number is D8A7-740C

 Directory of c:\Users\nagalman\School

07/22/2013  02:18 PM    <DIR>          .
07/22/2013  02:18 PM    <DIR>          ..
07/22/2013  02:18 PM                 5 grades.txt
07/22/2013  02:19 PM    <DIR>          UMBC
               1 File(s)              5 bytes
               3 Dir(s)   6,095,650,816 bytes free

c:\Users\nagalman\School>xcopy UMBC \Users\nagalman\Upload
UMBC\grades.txt
1 File(s) copied

c:\Users\nagalman\School>dir \Users\nagalman\Upload
 Volume in drive C has no label.
 Volume Serial Number is D8A7-740C

 Directory of c:\Users\nagalman\Upload

07/22/2013  02:35 PM    <DIR>          .
07/22/2013  02:35 PM    <DIR>          ..
07/22/2013  02:18 PM                 5 grades.txt
               1 File(s)              5 bytes
               2 Dir(s)   6,095,650,816 bytes free

c:\Users\nagalman\School>
```

- Robust file copy - Copies files and directories, including subdirectories.
- Much more capable than copy
- Enables copying of files based on specific criteria
- ROBOCOPY source destination [file [file]...] [options]
- robocopy /?

- Enables management of disks, partitions, and volumes
- Diskpart is its own command interpreter
  - You enter commands much like cmd.exe
- Diskpart
- create partition primary size=10240 ID=[GUID]
- help

```
Microsoft DiskPart version 6.1.7601
Copyright (C) 1999-2008 Microsoft Corporation.
On computer: KVM-W7-64

DISKPART> help

Microsoft DiskPart version 6.1.7601

ACTIVE       - Mark the selected partition as active.
ADD          - Add a mirror to a simple volume.
ASSIGN       - Assign a drive letter or mount point to the selected volume.
ATTRIBUTES   - Manipulate volume or disk attributes.
ATTACH       - Attaches a virtual disk file.
AUTOMOUNT    - Enable and disable automatic mounting of basic volumes.
BREAK        - Break a mirror set.
CLEAN        - Clear the configuration information, or all information, off the
               disk.
COMPACT      - Attempts to reduce the physical size of the file.
CONVERT      - Convert between different disk formats.
CREATE       - Create a volume, partition or virtual disk.
DELETE       - Delete an object.
DETAIL       - Provide details about an object.
DETACH       - Detaches a virtual disk file.
EXIT         - Exit DiskPart.
EXTEND       - Extend a volume.
EXPAND       - Expands the maximum size available on a virtual disk.
FILESYSTEMS  - Display current and supported file systems on the volume.
FORMAT       - Format the volume or partition.
GPT          - Assign attributes to the selected GPT partition.
HELP         - Display a list of commands.
IMPORT       - Import a disk group.
INACTIVE     - Mark the selected partition as inactive.
LIST         - Display a list of objects.
MERGE        - Merges a child disk with its parents.
ONLINE       - Online an object that is currently marked as offline.
OFFLINE      - Offline an object that is currently marked as online.
RECOVER      - Refreshes the state of all disks in the selected pack.
               Attempts recovery on disks in the invalid pack, and
               resynchronizes mirrored volumes and RAID5 volumes
               that have stale plex or parity data.
REM          - Does nothing. This is used to comment scripts.
REMOVE       - Remove a drive letter or mount point assignment.
REPAIR       - Repair a RAID-5 volume with a failed member.
RESCAN       - Rescan the computer looking for disks and volumes.
RETAIN       - Place a retained partition under a simple volume.
SAN          - Display or set the SAN policy for the currently booted OS.
SELECT       - Shift the focus to an object.
```

- System file checker – scan and verifies the versions of all protected system files after a system restart
- Must be in an administrator command prompt
- sfc /scannow
- Sfc /?

```
C:\Windows\system32>sfc

Microsoft (R) Windows (R) Resource Checker Version 6.0
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

Scans the integrity of all protected system files and replaces incorrect version
s with
correct Microsoft versions.

SFC [/SCANNOW] [/VERIFYONLY] [/SCANFILE=<file>] [/VERIFYFILE=<file>]
    [/OFFWINDIR=<offline windows directory> /OFFBOOTDIR=<offline boot directory>
]

/SCANNOW        Scans integrity of all protected system files and repairs files
with
                problems when possible.
/VERIFYONLY     Scans integrity of all protected system files. No repair operati
on is
                performed.
/SCANFILE       Scans integrity of the referenced file, repairs file if problems
 are
                identified. Specify full path <file>
/VERIFYFILE     Verifies the integrity of the file with full path <file>.  No re
pair
                operation is performed.
/OFFBOOTDIR     For offline repair specify the location of the offline boot dire
ctory
/OFFWINDIR      For offline repair specify the location of the offline windows d
irectory

e.g.

        sfc /SCANNOW
        sfc /VERIFYFILE=c:\windows\system32\kernel32.dll
        sfc /SCANFILE=d:\windows\system32\kernel32.dll /OFFBOOTDIR=d:\ /OFFWINDI
R=d:\windows
        sfc /VERIFYONLY

C:\Windows\system32>_
```

- Check disk – display a status report and lists and correct disk errors
- chkdsk c:
- chkdsk /?

THANK YOU