Cheatography

Test Cheat Sheet

by cdefreit via cheatography.com/32722/cs/10131/

Network

Display Message - Execute with PSEXEC

```
MSG * /TIME:120 "Test Message"
```

Find Mail Server

```
nslookup -q=mx microsoft.com
```

PowerShell equivilant

```
Resolve-DnsName google.com -Type MX
```

Identify PDC/Schema Master

```
netdom query fsmo
```

Repair trust relationship to the domain

```
Test-ComputerSecureChannel [-Repair]
```

Track down process trying to get out

```
netstat -ano 1 | findstr 443
```

```
netsh -r COMPUTERNAME interface ip set dns "Local Area Connection" static x.x.x.x
```

```
netsh -r COMPUTERNAME interface ip add dns name="Local Area Connection" addr=x.x.x.x
```

```
Set-DnsClientServerAddress -ServerAddresses x.x.x.x,y.y.y.y
```

or...

```
Set-DnsClientSer<Tab> -ser x.x.x.x,y.y.y.y
```

Misc.

Set Command Prompt window size on the fly

```
mode 150, 40
```

(width, Height)

Output results to clipboard

```
 |Clip
```

```
Example: ipconfig /all | clip
```

Combining Commands

```
ipconfig /release && ipconfig /renew
```

```
gpresult /f /h %temp%\result.html && %temp%\result.html
```

Find Large Files

```
robocopy /XJD /L /E /NDL /B /min:100000000 c:\ c:\dummyfolder
```

Search current path for files containing text:

```
for /f %i in ('findstr /I /S /C:"connectionstring" *')
```

easily delete files containing specific text

```
for /f %i in ('findstr /M /I /S /C:"virus.dat" *.eml') do @del "%i"
```

Control IP for outgoing connections

```
netsh int ipv4 add address "Local Area Connection" 172.16.0.22 255.255.255.0 skipassource=true
```

RDP

```
"qwinsta" shows RDP sessions on a computer.
"rwinsta 1" logs off user with ID of 1.
```

Test

This is text.

This is 'code'

or

This is `code'

or

This is `code`

It was that last one! cool.

ok, so here we go:

Find large files on a drive (e.g. finding logs to clean up to get some free space:

```
robocopy /XJD /L /E /NDL /B /min:100000000 c:\ c:\dummyfolder
```

By **cdefreit**

cheatography.com/cdefreit/

Not published yet.

Last updated 7th December, 2016.