

Why Joshua Wright loves Windows Vista ?

And why you should be glad you're not
running it.

Zoher Anis
Sr. Security Engineer

Agenda

- Who is this dude ? – Joshua Wright
- Background
- Vista Command line Kung-fu
- Demo
- A new and powerful feature
 - Questions ?

Basics

- Wireless Network Interface Controller modes
 - Infrastructure / Master Mode
 - Managed Mode / Client Mode
 - Ad-Hoc Mode / Peer – to - Peer
 - Monitor Mode / Passive Mode

Wireless Stack in Windows Vista – NDIS 6

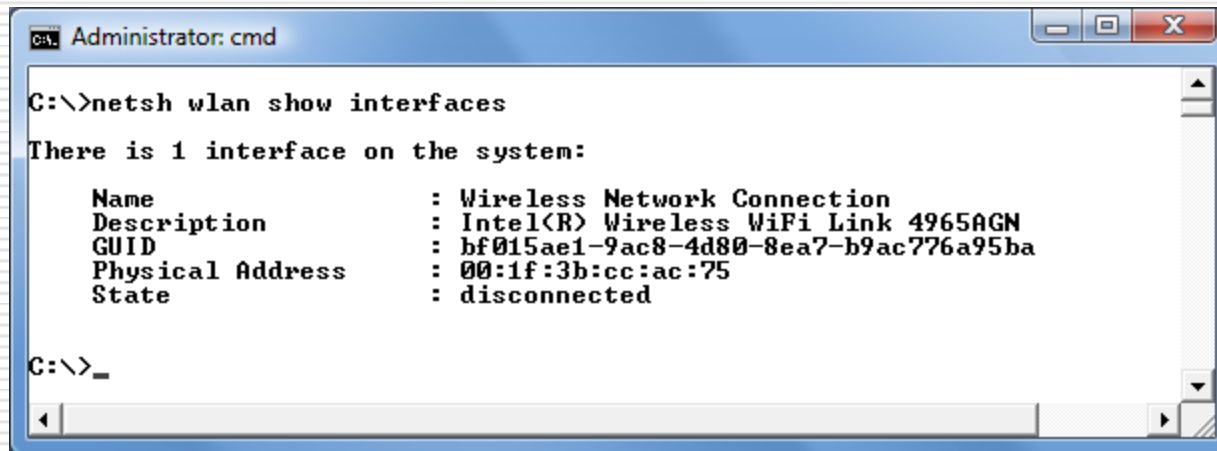
- With NDIS 6 model driver developers
 - Have standard set of APIs with Native Wifi Miniport Driver
 - Easy access to information for developing Wireless Analysis Tools via native Wifi API functions

- Penetration Testers can use accessible command- line tools to
 - Establish Ad-hoc Networks
 - Establish Bridge infrastructure over unauthenticated wireless networks
 - Explore other near by networks
 - Capture 802.11 wireless frames for further analysis

Vista Wireless Command line kung-fu

- ❑ ipconfig ..
- ❑ Identifying Wireless Interfaces

C:\>netsh wlan show interfaces

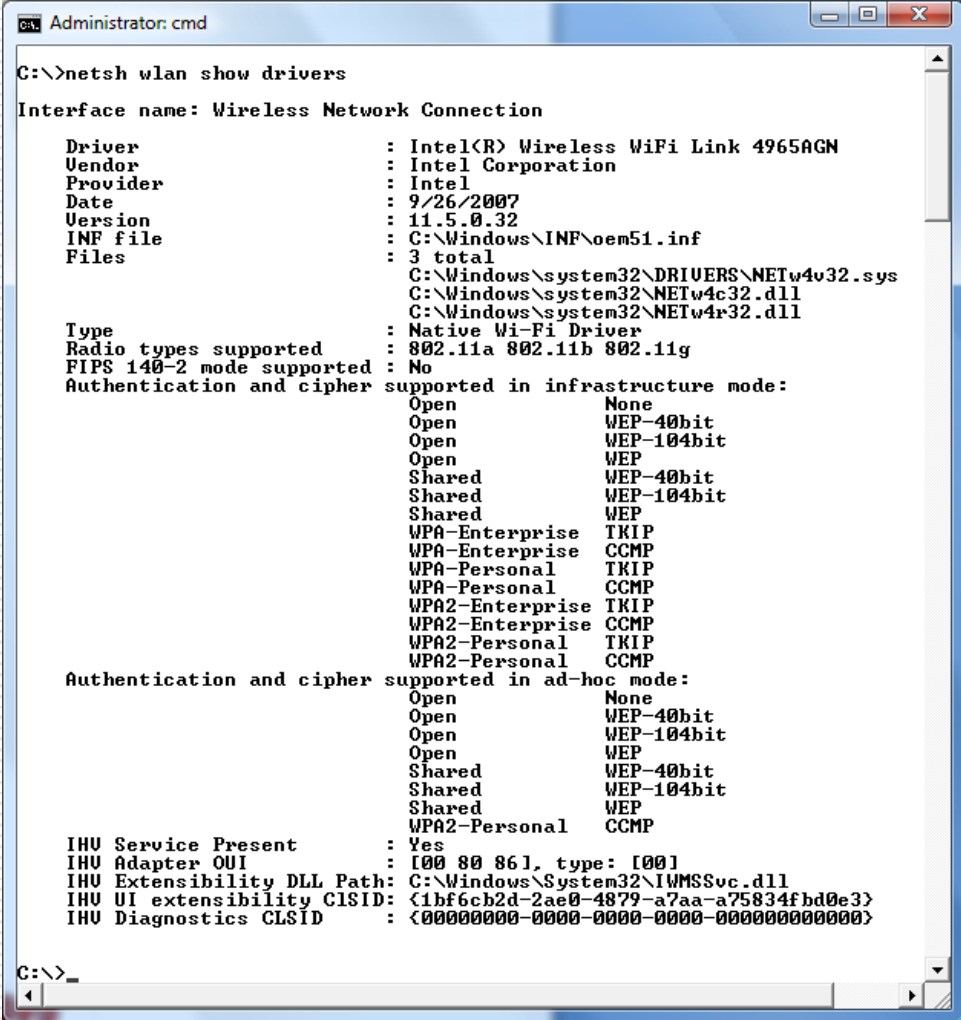


```
Administrator: cmd
C:\>netsh wlan show interfaces
There is 1 interface on the system:
Name                : Wireless Network Connection
Description         : Intel(R) Wireless WiFi Link 4965AGN
GUID                : bf015ae1-9ac8-4d80-8ea7-b9ac776a95ba
Physical Address    : 00:1f:3b:cc:ac:75
State                : disconnected
C:\>_
```

Vista Wireless Command line kung-fu

❑ Evaluating Interface Capabilities

```
C:\>netsh wlan show drivers
```



```
Administrator: cmd
C:\>netsh wlan show drivers

Interface name: Wireless Network Connection

Driver           : Intel(R) Wireless WiFi Link 4965AGN
Vendor           : Intel Corporation
Provider         : Intel
Date             : 9/26/2007
Version          : 11.5.0.32
INF file         : C:\Windows\INF\oem51.inf
Files            : 3 total
                  C:\Windows\system32\DRIVERS\NETw4v32.sys
                  C:\Windows\system32\NETw4c32.dll
                  C:\Windows\system32\NETw4r32.dll
Type             : Native Wi-Fi Driver
Radio types supported : 802.11a 802.11b 802.11g
FIPS 140-2 mode supported : No
Authentication and cipher supported in infrastructure mode:
  Open           None
  Open           WEP-40bit
  Open           WEP-104bit
  Open           WEP
  Shared         WEP-40bit
  Shared         WEP-104bit
  Shared         WEP
  WPA-Enterprise TKIP
  WPA-Enterprise CCMP
  WPA-Personal   TKIP
  WPA-Personal   CCMP
  WPA2-Enterprise TKIP
  WPA2-Enterprise CCMP
  WPA2-Personal  TKIP
  WPA2-Personal  CCMP
Authentication and cipher supported in ad-hoc mode:
  Open           None
  Open           WEP-40bit
  Open           WEP-104bit
  Open           WEP
  Shared         WEP-40bit
  Shared         WEP-104bit
  Shared         WEP
  WPA2-Personal  CCMP

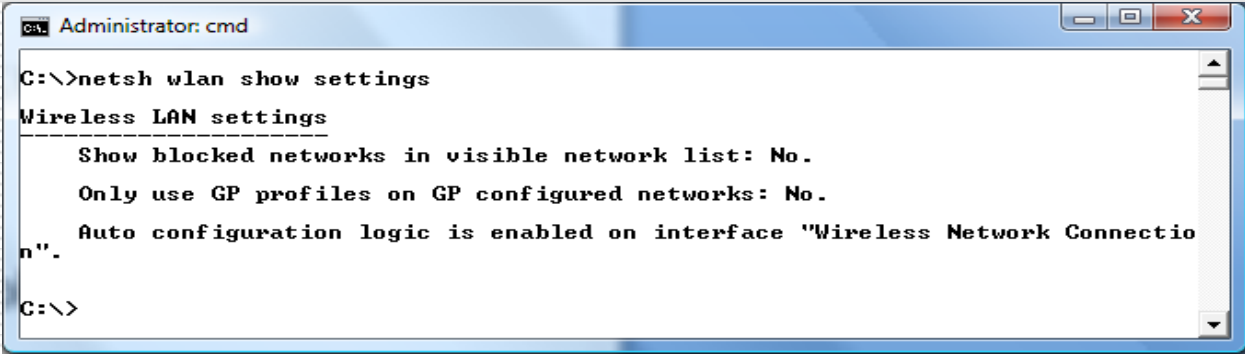
IHU Service Present : Yes
IHU Adapter OUI     : [00 80 86], type: [00]
IHU Extensibility DLL Path: C:\Windows\System32\IWMSsvc.dll
IHU UI extensibility CLSID: {1bf6cb2d-2ae0-4879-a7aa-a75834fbd0e3}
IHU Diagnostics CLSID : {00000000-0000-0000-0000-000000000000}

C:\>_
```

Vista Wireless Command line kung-fu

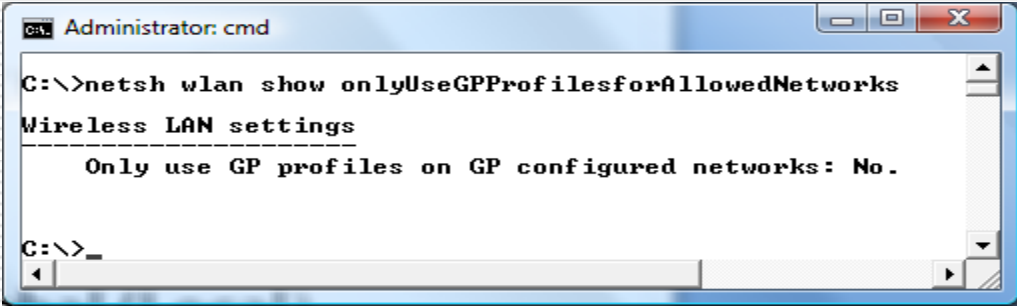
- ❑ Identifying configuration Method (Global/Local)

C:\>netsh wlan show settings



```
Administrator: cmd
C:\>netsh wlan show settings
Wireless LAN settings
-----
Show blocked networks in visible network list: No.
Only use GP profiles on GP configured networks: No.
Auto configuration logic is enabled on interface "Wireless Network Connection".
C:\>
```

C:\>netsh wlan show onlyusegppprofilesforallowednetworks

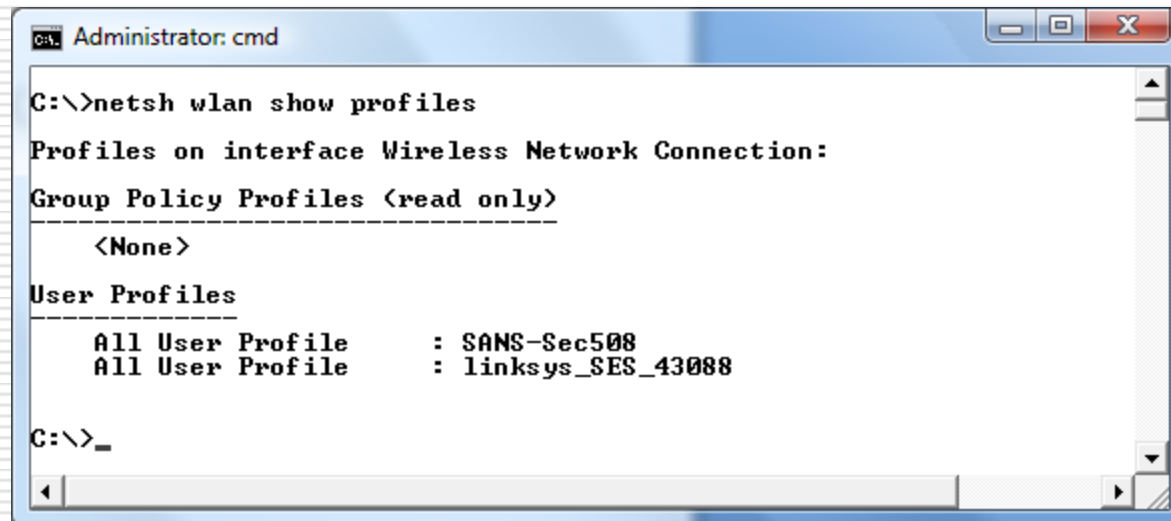


```
Administrator: cmd
C:\>netsh wlan show onlyUseGPPProfilesforAllowedNetworks
Wireless LAN settings
-----
Only use GP profiles on GP configured networks: No.
C:\>_
```

Vista Wireless Command line kung-fu

❑ Examining Preferred Networks

C:\>netsh wlan show profiles



```
Administrator: cmd
C:\>netsh wlan show profiles
Profiles on interface Wireless Network Connection:
Group Policy Profiles <read only>
-----
<None>
User Profiles
-----
    All User Profile      : SANS-Sec508
    All User Profile      : linksys_SES_43088
C:\>_
```

Vista Wireless Command line kung-fu

□ Analyzing Wireless Profiles

C:\>netsh wlan show profile name="xxxxx"

```
Administrator: cmd
C:\>netsh wlan show profile name="SANS-Sec508"
Profile SANS-Sec508 on interface Wireless Network Connection:
-----
Applied: All User Profile
Profile Information
-----
Version           : 1
Type              : Wireless LAN
Name              : SANS-Sec508
Control options   :
  Connection mode : Connect automatically
  Network broadcast : Connect only if this network is broadcasting
  AutoSwitch      : Switch to more preferred network if possible
Connectivity settings
-----
Number of SSIDs   : 1
SSID name        : "SANS-Sec508"
Network type     : Infrastructure
Radio type       : [ Any Radio Type ]
Vendor extension  : Not present
Security settings
-----
Authentication    : Open
Cipher            : None
Security key      : Absent
Key Index         : 1
C:\>
```

```
Administrator: cmd
C:\>netsh wlan show profile name="linksys_SES_43088"
Profile linksys_SES_43088 on interface Wireless Network Connection:
-----
Applied: All User Profile
Profile Information
-----
Version           : 1
Type              : Wireless LAN
Name              : linksys_SES_43088
Control options   :
  Connection mode : Connect manually
  Network broadcast : Connect only if this network is broadcasting
  AutoSwitch      : Do not switch to other networks
Connectivity settings
-----
Number of SSIDs   : 1
SSID name        : "linksys_SES_43088"
Network type     : Infrastructure
Radio type       : [ Any Radio Type ]
Vendor extension  : Not present
Security settings
-----
Authentication    : WPA-Personal
Cipher            : CCMP
Security key      : Present
C:\>
```

Vista Wireless Command line kung-fu

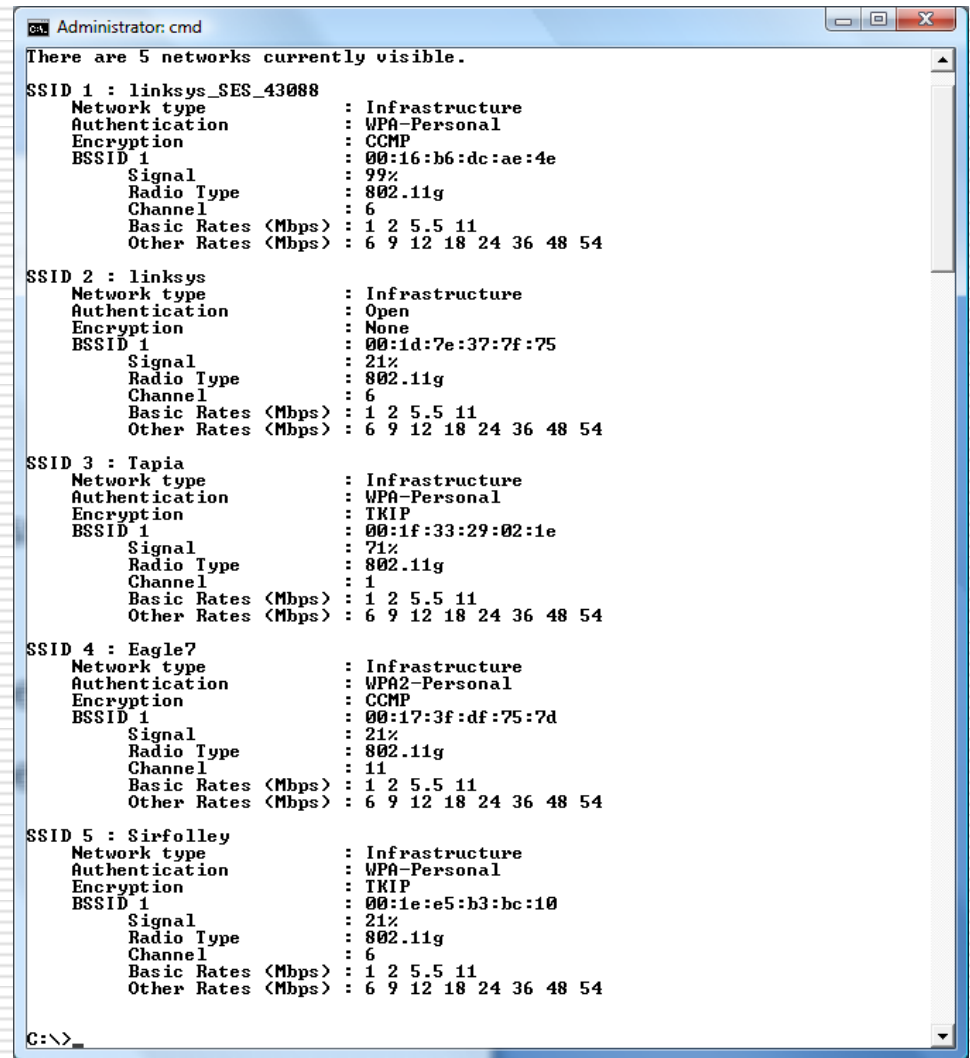
- Enumerating Networks

```
C:\>netsh wlan show networks mode=bssid
```

Fresh Scan

```
C:\>netsh interface set interface "Name" disabled
```

```
C:\>netsh interface set interface "Name" enabled
```



```
Administrator: cmd
There are 5 networks currently visible.
SSID 1 : linksys_SES_43088
Network type      : Infrastructure
Authentication    : WPA-Personal
Encryption        : CCMP
BSSID 1          : 00:16:b6:dc:ae:4e
Signal           : 99%
Radio Type       : 802.11g
Channel          : 6
Basic Rates <Mbps> : 1 2 5.5 11
Other Rates <Mbps> : 6 9 12 18 24 36 48 54

SSID 2 : linksys
Network type      : Infrastructure
Authentication    : Open
Encryption        : None
BSSID 1          : 00:1d:7e:37:7f:75
Signal           : 21%
Radio Type       : 802.11g
Channel          : 6
Basic Rates <Mbps> : 1 2 5.5 11
Other Rates <Mbps> : 6 9 12 18 24 36 48 54

SSID 3 : Tapia
Network type      : Infrastructure
Authentication    : WPA-Personal
Encryption        : TKIP
BSSID 1          : 00:1f:33:29:02:1e
Signal           : 71%
Radio Type       : 802.11g
Channel          : 1
Basic Rates <Mbps> : 1 2 5.5 11
Other Rates <Mbps> : 6 9 12 18 24 36 48 54

SSID 4 : Eagle7
Network type      : Infrastructure
Authentication    : WPA2-Personal
Encryption        : CCMP
BSSID 1          : 00:17:3f:df:75:7d
Signal           : 21%
Radio Type       : 802.11g
Channel          : 11
Basic Rates <Mbps> : 1 2 5.5 11
Other Rates <Mbps> : 6 9 12 18 24 36 48 54

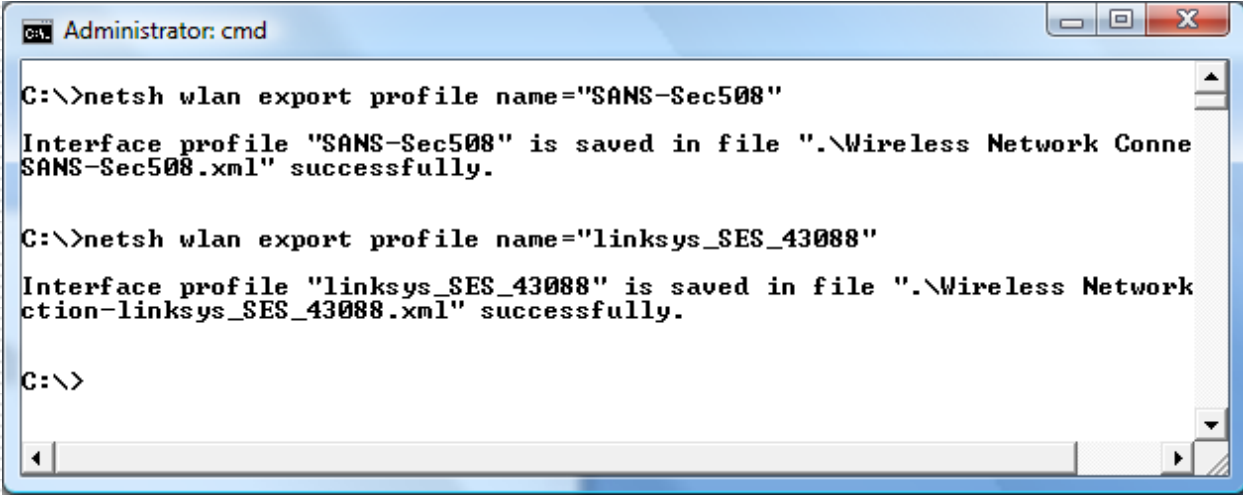
SSID 5 : Sirfolley
Network type      : Infrastructure
Authentication    : WPA-Personal
Encryption        : TKIP
BSSID 1          : 00:1e:e5:b3:bc:10
Signal           : 21%
Radio Type       : 802.11g
Channel          : 6
Basic Rates <Mbps> : 1 2 5.5 11
Other Rates <Mbps> : 6 9 12 18 24 36 48 54

C:\>
```

Vista Wireless Command line kung-fu

□ Analyzing Wireless Profiles

C:\>netsh wlan export profile name="xxxxx"



```
Administrator: cmd
C:\>netsh wlan export profile name="SANS-Sec508"
Interface profile "SANS-Sec508" is saved in file ".\Wireless Network Connection-SANS-Sec508.xml" successfully.

C:\>netsh wlan export profile name="linksys_SES_43088"
Interface profile "linksys_SES_43088" is saved in file ".\Wireless Network Connection-linksys_SES_43088.xml" successfully.

C:\>
```

Vista Wireless Command line kung-fu

- Adding Wireless profiles

```
C:\>netsh wlan add profile filename="xxxxx.xml"
```

Note: An existing (copied .xml file from other machine) or custom profile (modified .xml file) can be added.

- This can be also useful if you want to see the configuration settings for a Network.

Just copy to your machine and open through GUI.

Vista Wireless Command line kung-fu

- Starting a wireless Profile

```
C:\>netsh wlan connect name="xxxxx"
```



```
Administrator: cmd
C:\>netsh wlan connect name="linksys_SES_43088"
Connection request is received successfully.
C:\>netsh wlan disconnect interface="Wireless Network Connection"
Disconnection request is received successfully.
C:\>
```

Or you can add the script to the startup to start automatically.

And there is more

- Connecting to the network without saved profile
 - Tool – wlsample.exe (included in Windows SDK)

wlsample help can always be useful

wlsample ei shows interface details including GUID

wlsample disc [GUID] SSID i u

SSID ssid of the network

i/a infrastructure /ad-hoc

u/s unsecure/secure

Bridging Wired and Wireless Networks

- Add ad-hoc connection
- Create a bridge between wired and wireless connection
 - Unfortunately this can be only accomplished using Vista GUI.

- But wait
 - We have command line tools to do this nethelper.exe by mkreddy....

Vista Monitor Mode

- ❑ Mandatory requirement to support of extensible station and monitor mode
- ❑ This mode allows to capture all frames in the network
- ❑ Only supported using cmdline utility
- ❑ Vistarfmon
 - Written by Joshua Wright

```
C:\>vistarfmon.exe 1 mon
```

Bring it all together

□ Demo

Volume Shadow copy feature

- ❑ Modified in Vista & Windows 2008
 - ❑ Does cluster diffing rather than file diffing
 - ❑ Can be very useful for Forensics
 - ❑ Uses 15% of the space by default
- C:\vssadmin.exe list shadows



```
Administrator: cmd

Contents of shadow copy set ID: {1f7b5045-d4aa-427d-b429-0b5161bb97e8}
  Contained 1 shadow copies at creation time: 2/17/2009 3:00:31 AM
  Shadow Copy ID: {a140f694-0ef3-466c-b1d6-29a445faa11c}
  Original Volume: (C:)\\?\Volume{25e43525-37c0-11dd-892f-806e6f6e6963}\
  Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy16
  Originating Machine: zoher-xpslap
  Service Machine: zoher-xpslap
  Provider: 'Microsoft Software Shadow Copy provider 1.0'
  Type: ClientAccessibleWriters
  Attributes: Persistent, Client-accessible, No auto release, Differential
1. Auto recovered

Contents of shadow copy set ID: {3593b496-1242-45d8-8b67-73e937097e03}
  Contained 1 shadow copies at creation time: 2/17/2009 6:55:42 PM
  Shadow Copy ID: {e3ad9651-88dc-4c72-aa8f-2422c2f548a0}
  Original Volume: (C:)\\?\Volume{25e43525-37c0-11dd-892f-806e6f6e6963}\
  Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy17
  Originating Machine: zoher-xpslap
  Service Machine: zoher-xpslap
  Provider: 'Microsoft Software Shadow Copy provider 1.0'
  Type: ClientAccessibleWriters
  Attributes: Persistent, Client-accessible, No auto release, Differential
1. Auto recovered

Contents of shadow copy set ID: {f89e5fcf-a314-4e15-a475-b6cfa7840b1b}
  Contained 1 shadow copies at creation time: 2/19/2009 7:44:20 PM
  Shadow Copy ID: {e1b28161-822f-4839-bb9e-766d864d4644}
  Original Volume: (C:)\\?\Volume{25e43525-37c0-11dd-892f-806e6f6e6963}\
  Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy18
  Originating Machine: zoher-xpslap
  Service Machine: zoher-xpslap
  Provider: 'Microsoft Software Shadow Copy provider 1.0'
  Type: ClientAccessibleWriters
  Attributes: Persistent, Client-accessible, No auto release, Differential
1. Auto recovered

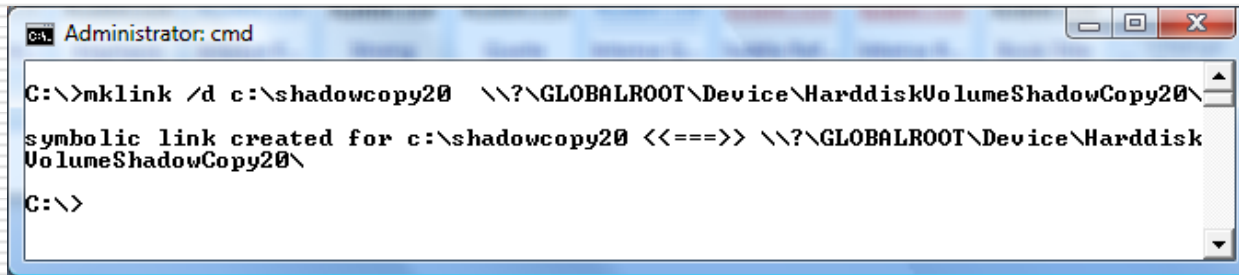
Contents of shadow copy set ID: {af4bf96c-87af-4d99-9a19-d20049cb8869}
  Contained 1 shadow copies at creation time: 2/21/2009 10:00:14 AM
  Shadow Copy ID: {04bd4abf-4677-45cf-ba65-23d3c8c5fe24}
  Original Volume: (C:)\\?\Volume{25e43525-37c0-11dd-892f-806e6f6e6963}\
  Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy19
  Originating Machine: zoher-xpslap
  Service Machine: zoher-xpslap
  Provider: 'Microsoft Software Shadow Copy provider 1.0'
  Type: ClientAccessibleWriters
  Attributes: Persistent, Client-accessible, No auto release, Differential
1. Auto recovered

Contents of shadow copy set ID: {daac9e8e-ecf8-4d1a-aacf-dbb7b07b55d4}
  Contained 1 shadow copies at creation time: 2/22/2009 2:22:01 AM
  Shadow Copy ID: {9ddadf7f-caf9-4995-84c4-16fa580876f6}
  Original Volume: (C:)\\?\Volume{25e43525-37c0-11dd-892f-806e6f6e6963}\
  Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy20
  Originating Machine: zoher-xpslap
  Service Machine: zoher-xpslap
  Provider: 'Microsoft Software Shadow Copy provider 1.0'
  Type: ClientAccessibleWriters
  Attributes: Persistent, Client-accessible, No auto release, Differential
1. Auto recovered

C:\>
```

Volume Shadow copy feature

❑ Creating link



```
Administrator: cmd
C:\>mklink /d c:\shadowcopy20 \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy20\
symbolic link created for c:\shadowcopy20 <<===>> \\?\GLOBALROOT\Device\Harddisk
VolumeShadowCopy20\
C:\>
```

❑ Imaging the shadow volume

❑ C:\> dd.exe if=\\.\HarddiskVolumeShadowCopy#
of=f:\sanp#.img --localwrt

❑ --localwrt allows output to local mounted drive

Acknowledgements

- The presentation is based on paper by Joshua Wright

http://www.inguardians.com/pubs/Vista_Wireless_Power_Tools-Wright.pdf

- Questions ?