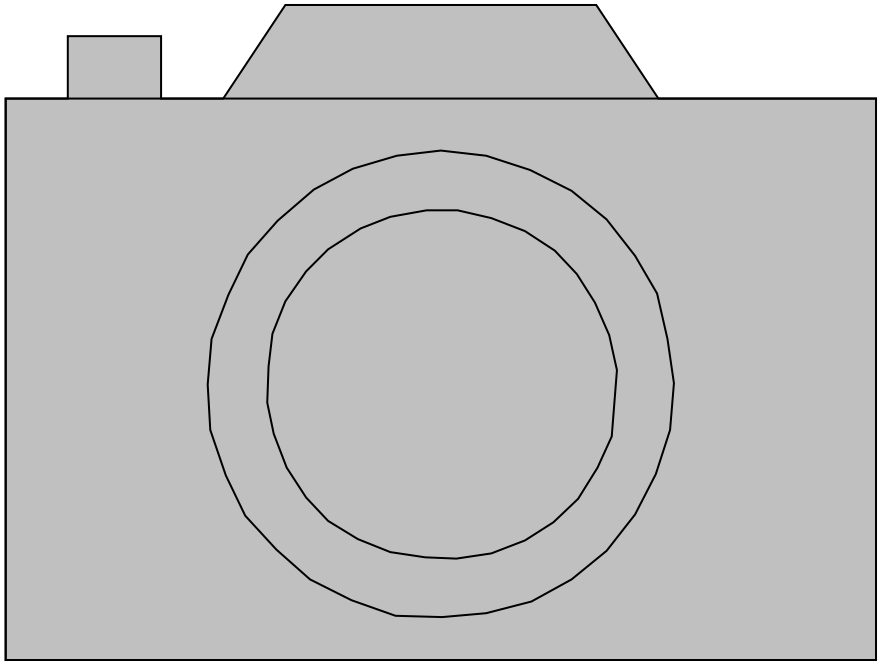
WiFi Related Registry Keys

What Can we Discover

- Whether the user's AP was open or secured
- What different APs the user has been connecting to
- The date and times the user has been connected to their AP and the Internet
- Whether the user was using a different adapter

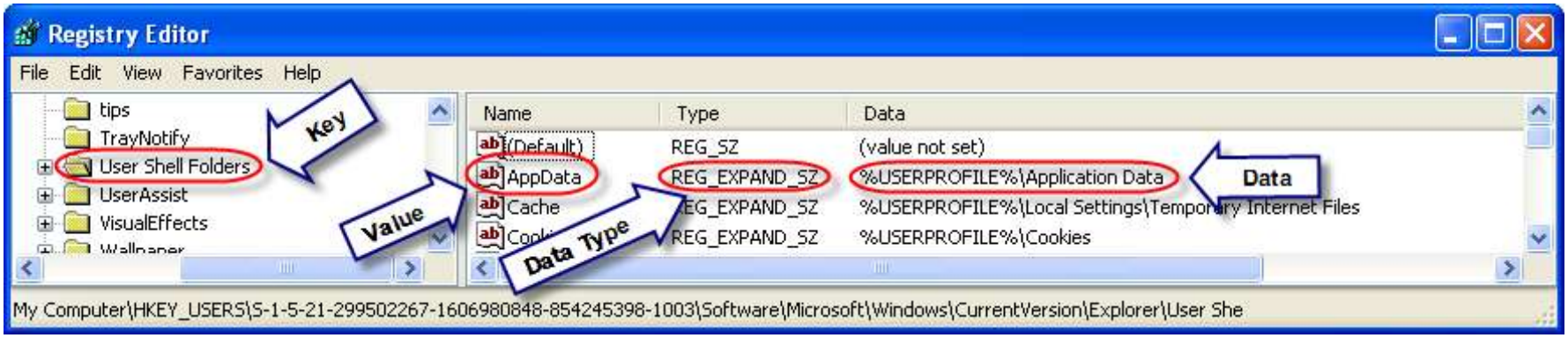
The Big Picture



THE BASICS

The Windows Registry

- Repository for **system settings**
- Repository for **user settings**
- Stored on the **hard disk** as well as in **memory** (RAM)
- Organized into:
  - **Keys**
  - **Values**
  - **Data**


Registry Editor
File Edit View Favorites Help
tips
TrayNotify
User Shell Folders
UserAssist
VisualEffects
Key
Value
Data Type
Data
Name
Type
Data
(Default)
REG_SZ
(value not set)
AppData
REG_EXPAND_SZ
%USERPROFILE%\Application Data
Cache
%USERPROFILE%\Local Settings\Temporary Internet Files
REG_EXPAND_SZ
%USERPROFILE%\Cookies
My Computer\HKEY_USERS\S-1-5-21-299502267-1606980848-854245398-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\User She

Files Containing the Registry

System Information

%SystemRoot%\System32\config

- Default, SAM, SECURITY, Software, System, Userdiff, etc...

default	256 KB	File	16/09/2009 2:34 PM
SAM	256 KB	File	16/09/2009 2:34 PM
SECURITY	256 KB	File	16/09/2009 2:34 PM
software	23,040 KB	File	16/09/2009 2:34 PM
system	7,168 KB	File	16/09/2009 2:51 PM
userdiff	256 KB	File	07/08/2004 1:52 AM

User Specific Information

%SystemRoot%\Documents and Settings\<username>

- NTUSER.DAT

NTUSER.DAT	1,280 KB	DAT File	16/09/2009 3:13 PM

Date & Time Stamps

- Registry Key **time stamps** are in the system's **UTC**
- **When a Key is created**, an initial time stamp is placed on it
- Every time a Key's Values or Data are **changed**, the **time stamp** on the **Key** is **updated**

❖ It may not be possible to tell which value or data changed

AccessData Registry Viewer - [NTUSER.DAT]

File Edit Report View Window Help

File Name MRU
View
Save As
File Name MRU
View

Name	Type	Data
Value	REG_MULTI_SZ	O:\Courses and Workshops\NIT\2009\0902\NITC 0902 Grades.xlsx...
Maximum Ent...	REG_DWORD	0x0000000A (10)

Key Properties

Last Written Time	29/08/2009 15:52:08 UTC

```
000  4f 00 3a 00 5c 00 43 00-6f 00 75 00 72 00 73 00  O·:·\·C·o·u·r·s·
010  65 00 73 00 20 00 61 00-6e 00 64 00 20 00 57 00  e·s· ·a·n·d· ·W·
020  6f 00 72 00 6b 00 73 00-68 00 6f 00 70 00 73 00  o·r·k·s·h·o·p·s·
030  5c 00 4e 00 49 00 54 00-5c 00 32 00 30 00 30 00  \·N·I·T·\·2·0·0·
040  39 00 5c 00 30 00 39 00-30 00 32 00 5c 00 4e 00  9·\·0·9·0·2·\·N·
050  49 00 54 00 43 00 20 00-30 00 39 00 30 00 32 00  I·T·C· ·0·9·0·2·
```

NTUSER.DAT\Software\Microsoft\Office\12.0\Common\Open Find\Microsoft Office Excel\Settings\Save Offset: 0

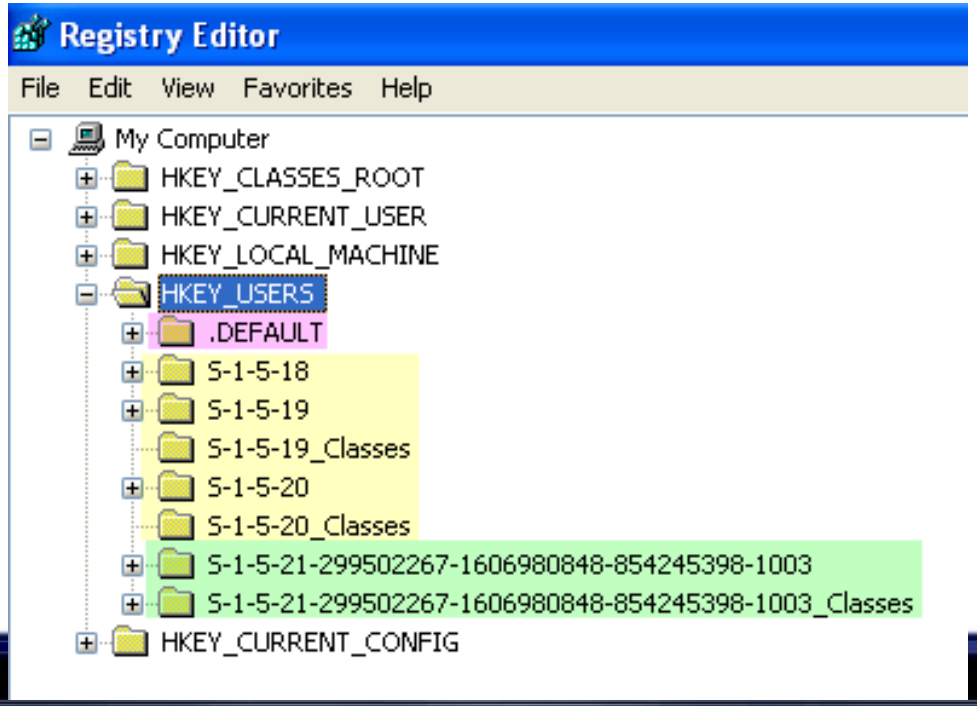
Security Identifiers (SID)

- ***Unique*** names
- Identify **users** or **groups of users**
- Assigned by a Windows Domain Controller
- Not portable to other networks

S-<SID_Version>-<Identifier_authority>-<Domain_Identifier>-<Relative_Identifier>

S-1-5-21-299502267-1606980848-854245398-1003

- **S-1-5-18** – LocalSystem
- **S-1-5-19** – NT Authority, local service.
- **S-1-5-19_Classes -** NT Authority local service classes.
- **S-1-5-20** – NT Authority, network service
- **S-1-5-20-Classes** – NT Authority, network service classes.



Determining Specific User's SIDs

- **SAM file**:
  - **\SAM\Domains\Account\Users**
- SOFTWARE file:
  - **\Microsoft\WindowsNT\CurrentVersion\ProfileList**

- Contains the user name and SID in Hex.
- You must convert the last three hex numbers to decimal to determine the decimal version of the SID that is used in the Recycler and System Volume Information Folder

- **FTK Registry Viewer** does much of this for you

AccessData Registry Viewer - [SAM]

File Edit Report View Window Help

- SAM
  - SAM
    - Domains
      - Account
        - Aliases
        - Groups
        - Users
          - 000001F4
          - 000001F5
          - 000003EA
          - 000003EB
          - 000003EC
          - 000003F0
          - 000003F1
          - Names
      - Builtin

Name	Type	Data
F	REG_BINARY	02 00 01 00 00 00 00 00 54 55 A3 AB FA 36 CA 01 0
V	REG_BINARY	00 00 00 00 D4 00 00 00 02 00 01 00 D4 00 00 00 0

Key Properties

Last Written Time	16/09/2009 18:22:38 UTC
SID unique identifier	1009
User Name	Mary
Full Name	Mary
Logon Count	1
Last Logon Time	16/09/2009 18:22:38 UTC
Last Password Change Time	11/09/2009 12:32:00 UTC
Expiration Time	Never
Invalid Logon Count	0
Last Failed Login Time	13/09/2009 12:34:06 UTC
Account Disabled	false
Password Required	true
Country Code	0 (System Default)
Has LAN Manager Password	true
Has NTLMv2 Password	true

```
00 | 02 00 01 00 00 00 00 00-54 55 a3 ab fa 36 ca 01 | ........TU£
10 | 00 00 00 00 00 00 00 00-76 50 d8 db db 32 ca 01 | ........vPØ
20 | ff ff ff ff ff ff ff 7f-48 2d 31 7c 6e 34 ca 01 | ÿÿÿÿÿÿÿ·H-1
30 | f1 03 00 00 01 02 00 00-10 02 00 00 00 00 00 00 | ñ··· ··· ··· ···
40 | 00 00 01 00 00 00 00 00-00 00 ff ff db 01 91 7c | ··· ··· ··· ··ÿÿ
```

SAM\SAM\Domains\Account\Users\000003F1

Offset: 0

Canada

AccessData Registry Viewer - [software]

File Edit Report View Window Help

- Ports
- Prefetcher
- Print
- ProfileList
  - S-1-5-18
  - S-1-5-19
  - S-1-5-20
  - S-1-5-21-930212210-811250829-2050355374-1008
  - S-1-5-21-930212210-811250829-2050355374-1009
  - S-1-5-21-930212210-811250829-2050355374-500
- related.desc
- SeCEdit
- Setup

Name	Type	Data
ProfileImagePath	REG_EXPAND_SZ	%SystemDrive%\Documents and Settings\Mary
Sid	REG_BINARY	01 05 00 00 00 00 00 05 15 00 00 00 72 E9 71 37 8D B4 ...
Flags	REG_DWORD	0x00000000 (0)
State	REG_DWORD	0x00000004 (4)
CentralProfile	REG_SZ	(value not set)
ProfileLoadTimeLow	REG_DWORD	0xAC53C358 (2891170648)
ProfileLoadTimeHigh	REG_DWORD	0x01CA36FA (30029562)
RefCount	REG_DWORD	0x00000000 (0)
RunLogonScriptSync	REG_DWORD	0x00000000 (0)

Key Properties

Last Written Time	16/09/2009 18:32:02 UTC

```
00 25 00 53 00 79 00 73 00-74 00 65 00 6d 00 44 00 %·S·y·s·t·e·m·D·
10 72 00 69 00 76 00 65 00-25 00 5c 00 44 00 6f 00 r·i·v·e·%·\·D·o·
20 63 00 75 00 6d 00 65 00-6e 00 74 00 73 00 20 00 c·u·m·e·n·t·s· ·
30 61 00 6e 00 64 00 20 00-53 00 65 00 74 00 74 00 a·n·d· ·S·e·t·t·
40 69 00 6e 00 67 00 73 00-5c 00 4d 00 61 00 72 00 i·n·g·s·\·M·a·r·
50 79 00 00 00                                      y···
```

software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-930212210-811250829-2050355374-1009

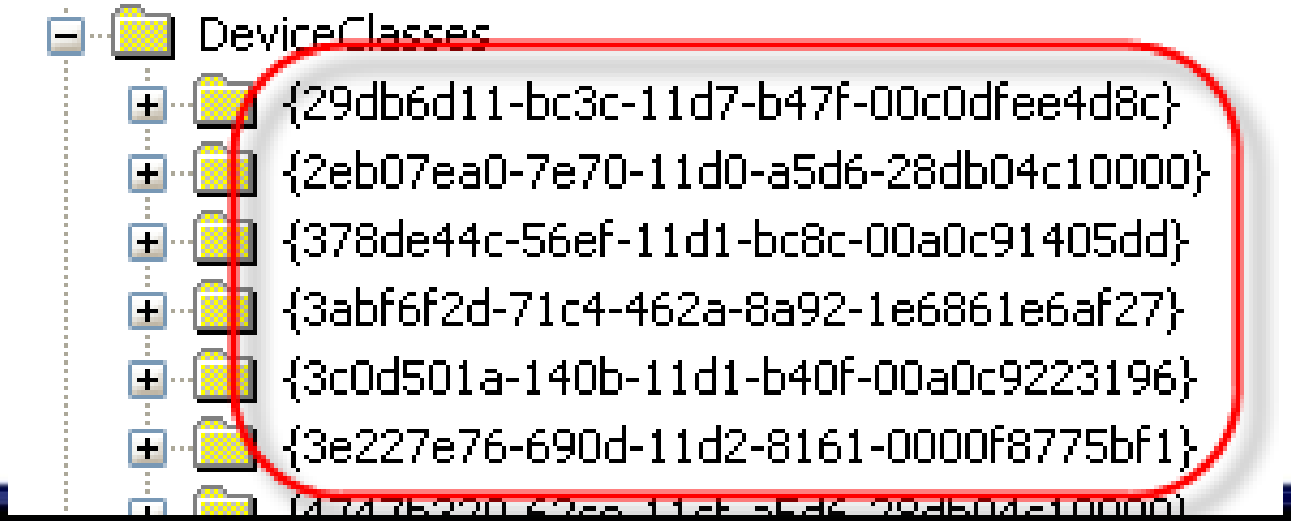
Offset: 0

_REGISTRY_USER_NTUSER_S-1-5-18
_REGISTRY_USER_NTUSER_S-1-5-19
_REGISTRY_USER_NTUSER_S-1-5-20
_REGISTRY_USER_NTUSER_S-1-5-21-930212210-811250829-2050355374-500
_REGISTRY_USER_NTUSER_S-1-5-21-930212210-811250829-2050355374-1008
_REGISTRY_USER_NTUSER_S-1-5-21-930212210-811250829-2050355374-1009
_REGISTRY_USER_USRCLASS_S-1-5-18
_REGISTRY_USER_USRCLASS_S-1-5-19
_REGISTRY_USER_USRCLASS_S-1-5-20
_REGISTRY_USER_USRCLASS_S-1-5-21-930212210-811250829-2050355374-500
_REGISTRY_USER_USRCLASS_S-1-5-21-930212210-811250829-2050355374-1009
ComDb.Dat
domain.txt

Globally Unique Identifiers (GUID)

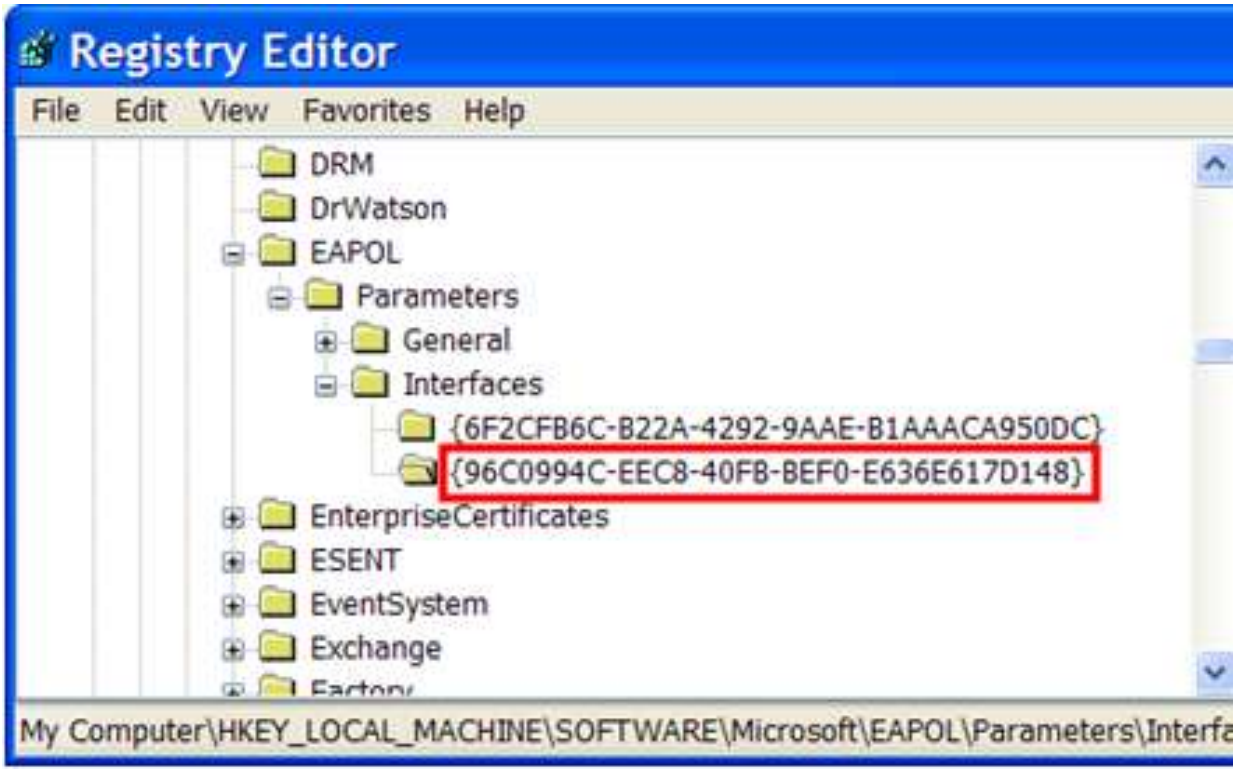
- **Identify devices**
- 16 Byte name
  - Hexadecimal notation
  - 8-4-4-4-12

5583FF01-9690-120C-A326-00AB003F549A

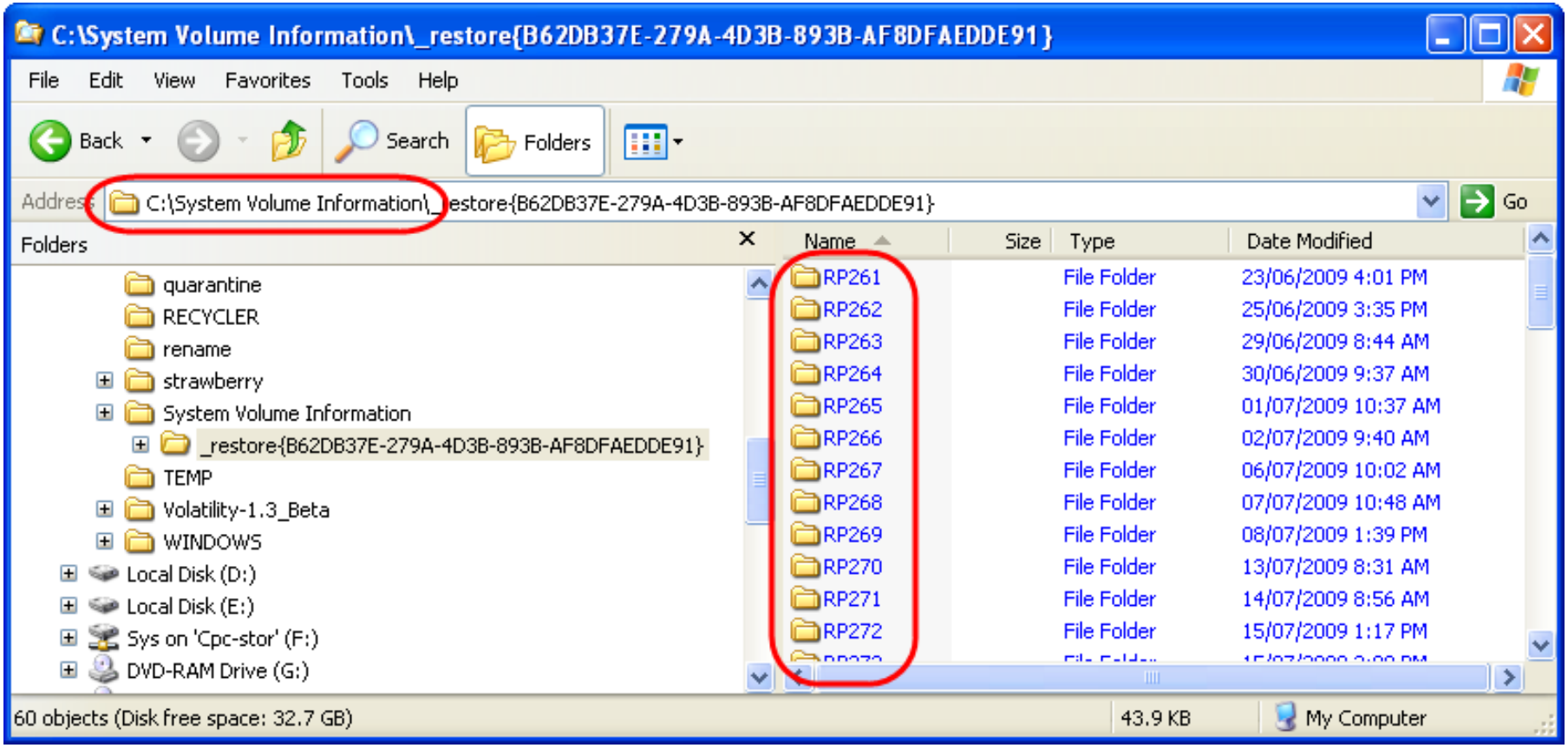


Globally Unique Identifiers (GUID)

- All Wireless Adapters are given a unique GUID



Restore Points



Restore Points

C:\System Volume Information_restore{B62DB37E-279A-4D3B-893B-AF8DFAEDDE91}\RP262\snapshot

File Edit View Favorites Tools Help

Back Search Folders

Address C:\System Volume Information_restore{B62DB37E-279A-4D3B-893B-AF8DFAEDDE91}\RP262\snapshot Go

Folders

- quarantine
- RECYCLER
- rename
- strawberry
- System Volume Information
  - _restore{B62DB37E-279A-4D3B-893B-AF8DFAEDDE91}
    - RP261
    - RP262
      - snapshot
    - RP263
    - RP264
    - RP265
    - RP266
    - RP267
    - RP268
    - RP269
    - RP270
    - RP271

Name

- Repository
- _REGISTRY_MACHINE_SAM
- _REGISTRY_MACHINE_SECURITY
- _REGISTRY_MACHINE_SOFTWARE
- _REGISTRY_MACHINE_SYSTEM
- _REGISTRY_USER_.DEFAULT
- _REGISTRY_USER_NTUSER_S-1-5-18
- _REGISTRY_USER_NTUSER_S-1-5-19
- _REGISTRY_USER_NTUSER_S-1-5-20
- _REGISTRY_USER_NTUSER_S-1-5-21-1214440339-790525478-839522115-500
- _REGISTRY_USER_NTUSER_S-1-5-21-1214440339-790525478-839522115-1003
- _REGISTRY_USER_USRCLASS_S-1-5-19
- _REGISTRY_USER_USRCLASS_S-1-5-20
- _REGISTRY_USER_USRCLASS_S-1-5-21-1214440339-790525478-839522115-500
- _REGISTRY_USER_USRCLASS_S-1-5-21-1214440339-790525478-839522115-1003
- ComDb.Dat
- domain.txt

17 objects (Disk free space: 32.7 GB) 44.6 MB My Computer

WiFi Concepts

- **SSID** – Service Set Identifier (i.e. Network name)
- **BSSID** – Basic Service Set Identifier (i.e. MAC address)
- **Encryption**
  - WEP (Wired Equivalent Privacy)
  - TKIP (Temporal Key Integrity Protocol)
  - AES (Advanced Encryption Standard)
- **Authentication**
  - WPA (WiFi Protected Access – AES)
  - WPA-PSK (Pre-Shared Key)

REGISTRY, NETWORKS & WIFI

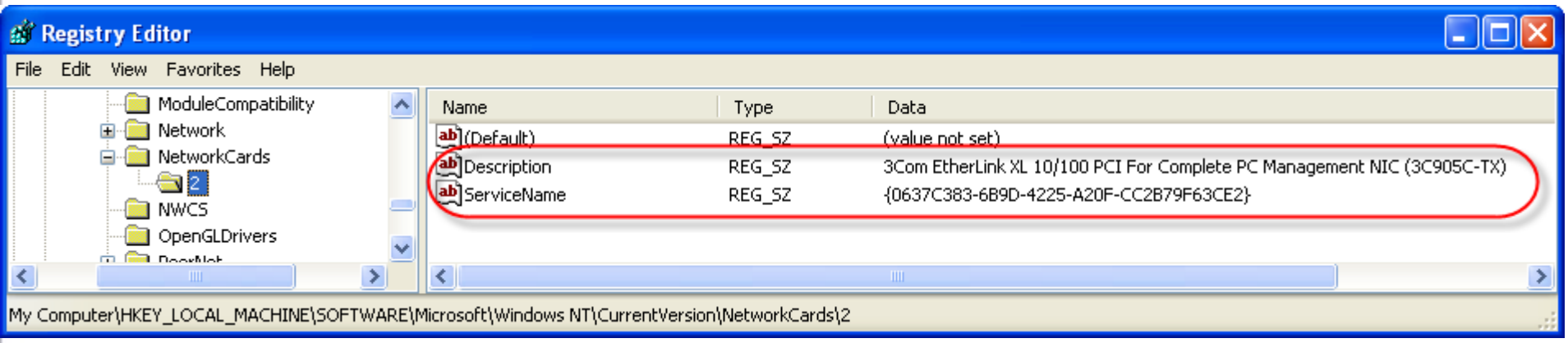
Network Cards

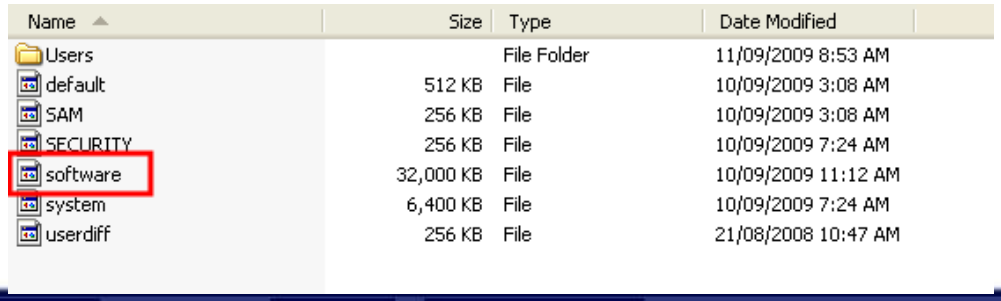
- If a computer contains multiple network cards (e.g. an Ethernet NIC as well as a Wi-Fi card), there will be **Registry keys** created **for each card**

- When a network card is removed from a computer, the Registry entry for it is **not deleted**.

Network Cards & Wireless Adapters

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkCards





Name	Size	Type	Date Modified
Users		File Folder	11/09/2009 8:53 AM
default	512 KB	File	10/09/2009 3:08 AM
SAM	256 KB	File	10/09/2009 3:08 AM
SECURITY	256 KB	File	10/09/2009 7:24 AM
software	32,000 KB	File	10/09/2009 11:12 AM
system	6,400 KB	File	10/09/2009 7:24 AM
userdiff	256 KB	File	21/08/2008 10:47 AM

- The “Last Written Time” will usually represent the date and time that the adapter was ***first installed***

AccessData Registry Viewer - [software]

File Edit Report View Window Help

31
32
34
NWCS
OpenGLDrivers
PeerNet
Perflib

Key Properties

Last Written Time	12/08/2009 18:55:13 UTC

Name	Type	Data
ServiceName	REG_SZ	{ED25DA33-CB0D-4365-9A0D-4D933B84BF2D}
Description	REG_SZ	NETGEAR WG111v3 54Mbps Wireless USB 2.0 Adapter

```
00 4e 00 45 00 54 00 47 00-45 00 41 00 52 00 20 00 N·E·T·G·E·A·R· ·
10 57 00 47 00 31 00 31 00-31 00 76 00 33 00 20 00 W·G·1·1·1·v·3· ·
20 35 00 34 00 4d 00 62 00-70 00 73 00 20 00 57 00 5·4·M·b·p·s· ·W·
30 69 00 72 00 65 00 6c 00-65 00 73 00 73 00 20 00 i·r·e·l·e·s·s· ·
```

software\Microsoft\Windows NT\CurrentVersion\NetworkCards\34

Offset: 0

WiFi Connections

Keys of Interest:

- **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EAPOL\Parameters\Interfaces\{GUID}**
- **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WZCSVC\Parameters\Interfaces**
- **HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces**

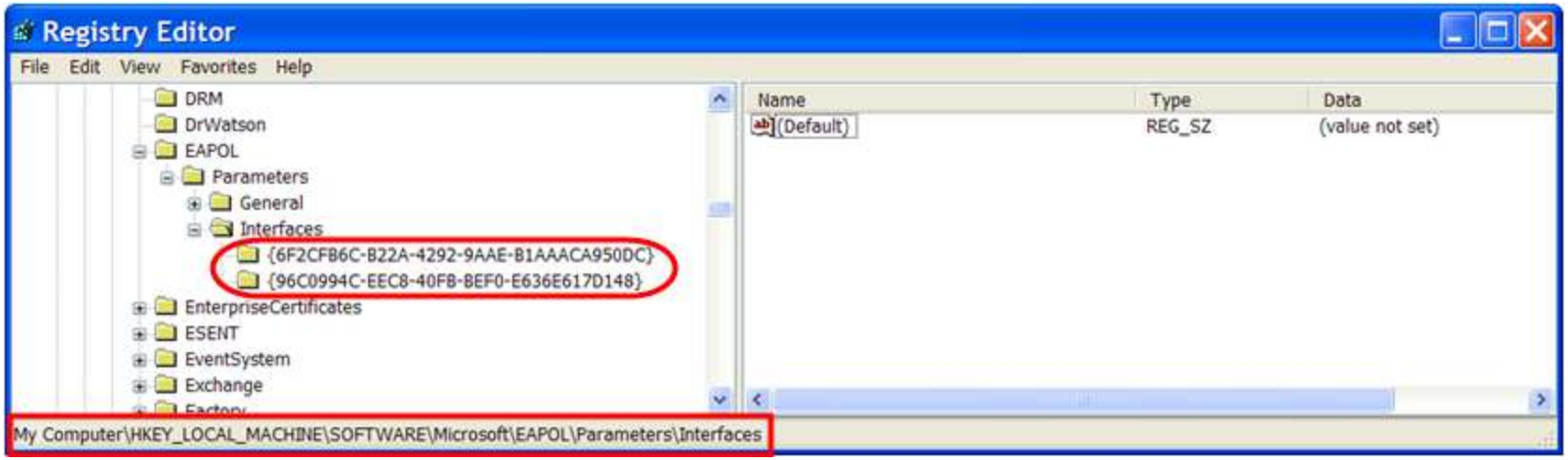
EAPOL = Extensible Authentication Protocol over LAN

WZCSVC = Wireless Zero Configuration Service

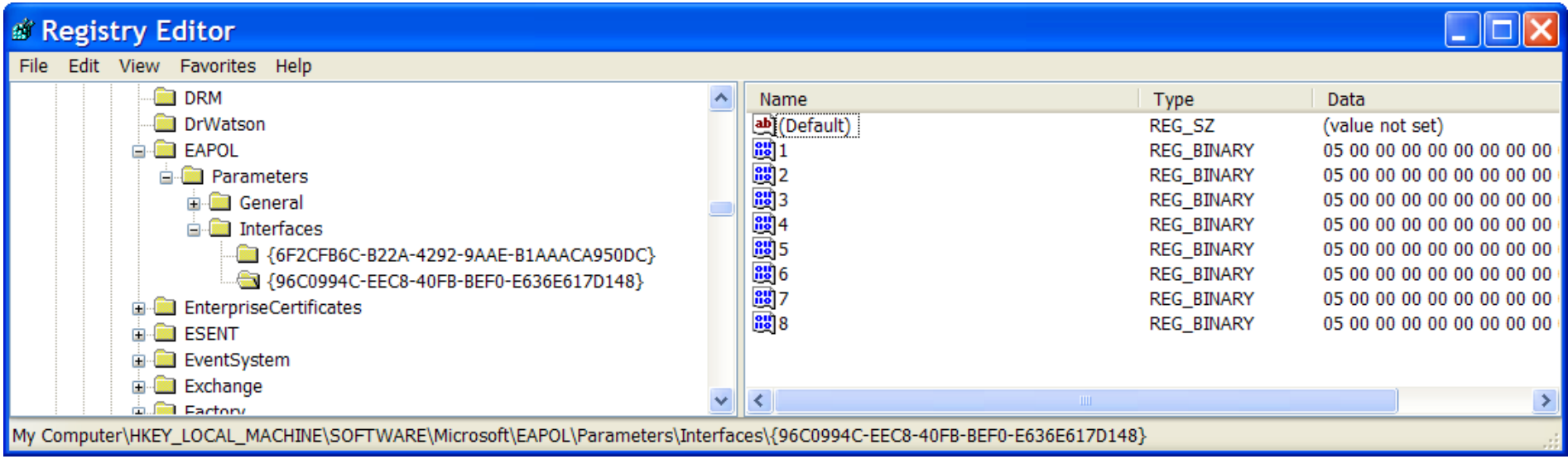
The registry keeps a list of the different wireless interfaces that have been used on the computer. These can be found under the following key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EAPOL\Parameters\Interfaces

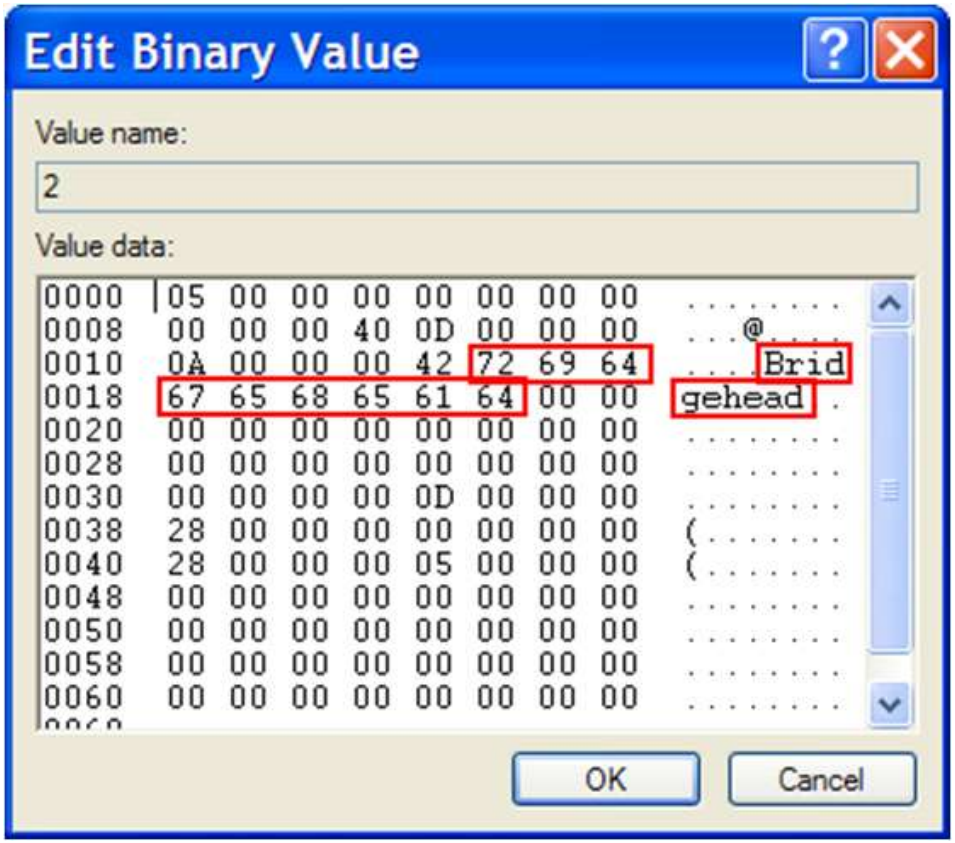
Two wireless adapters have been used on this computer:



- If you click on one of the interfaces keys, you will see a list of numbered values.
- Each one of these represents a **different wireless network** that the adapter has connected to



- The data in each of these values contains the **SSID** of the network



HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WZCSVC\Parameters\Interfaces

Value: **Static#0000, Static#0002, ...**

The **Data** for these **Values** contains:

- The **BSSID** of the network that the adapter has connected **0x08**
- The **SSID** of the network that the WAP has connected to **0x14**
- The type of **encryption** used **0x34**
- The **authentication** method / protocol **0x94**

AccessData Registry Viewer - [software]

File Edit Report View Window Help

- Wisp
- Works
- WZCSVC
  - Parameters
    - Interfaces
      - {24E2DF49-403A-47BA-9653-A6FEA1317B46}
      - {554C6A98-C8E0-4984-B112-C34DD22B746C}
      - {E869C63D-B1F9-4F32-B603-13D5CADB5E5E}
- MicroVision
- Mozilla

Name	Type	Data
LayoutVersion	REG_DWORD	0x00000007 (7)
ControlFlags	REG_DWORD	0x0BD18002 (198279170)
ActiveSettings	REG_BINARY	C8 02 00 00 00 40 00 00 00 13 46 C1 1F 72 00 00 0C 00 ...
Static#0000	REG_BINARY	C8 02 00 00 00 40 00 00 00 13 46 C1 1F 72 00 00 0C 00 ...
Static#0001	REG_BINARY	C8 02 00 00 00 40 00 00 00 19 CB 9E 72 FE 00 00 0A 00 ...

Key Properties

Last Written Time	16/09/2009 19:33:43 UTC

```
000 c8 02 00 00 00 40 00 00-00 13 46 c1 1f 72 00 00  È····@····FÁ·r··
010 00 00 00 00 4a 6f 6e 65-73 20 46 61 6d 69 6c 79  ····Jones Family
020 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
030 00 00 00 00 01 00 00 00-d3 ff ff ff 01 00 00 00  ........Óÿÿÿÿÿ····
040 20 00 00 00 64 00 00 00-00 00 00 00 88 2f 25 00   ···d·····/%·
050 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
060 01 00 00 00 82 84 8b 96-00 00 00 00 00 00 00 00  ................
070 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
080 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
090 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
0a0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
```

BSSID

SSID

Encryption

Authentication

software\Microsoft\WZCSVC\Parameters\Interfaces\{24E2DF49-403A-47BA-9653-A6FEA1317B46}

Offset: 0

Was the Access Point Secured? (WEP, WPA, WPA2, etc.)

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WZCSVC\Parameters\Interfaces

Hex Offset	Information
0x08	**BSSID**
0x10	**Length of SSID**
0x14	**Start of SSID string**
0x34	**Data Encryption type used** (TKIP, AES, WEP, Disabled)
0x94	**Network Authentication used** (WPA-PSK, WPA, Shared, Open)

Encryption Type 0x34	
WEP	00
Disabled	01
TKIP	04
AES	06

Network-Authentication 0x94	
WPA-PSK	04
WPA	03
Shared	01
Open	00

***** This is an incomplete list of values**

- **This WiFi network did not require authentication**
- **Encryption was disabled**

AccessData Registry Viewer - [software]

File Edit Report View Window Help

Works
WZCSVC
Parameters
Interfaces
{24E2DF49-403A-47BA-9653-A6FEA1317B46}
{554C6A98-C8E0-4984-B112-C34DD22B746C}
{E869C63D-B1F9-4F32-B603-13D5CADB5E5E}
MicroVision
Mozilla

Name	Type	Data
LayoutVersion	REG_DWORD	0x00000007 (7)
ControlFlags	REG_DWORD	0x0BD18002 (198279170)
ActiveSettings	REG_BINARY	C8 02 00 00 00 40 00 00 00 13 46 C1 1F 72 00 00 0C 00 ...
Static#0000	REG_BINARY	C8 02 00 00 00 40 00 00 00 13 46 C1 1F 72 00 00 0C 00 ...
Static#0001	REG_BINARY	C8 02 00 00 00 40 00 00 00 19 CB 9E 72 FE 00 00 0A 00 ...

Key Properties

Last Written Time	16/09/2009 19:33:43 UTC

```
000 c8 02 00 00 [illegible] 00-00 13 46 c1 1f 72 00 00  È····@····FÁ·r··
010 0[illegible] 4a 6f 6e 65-73 20 46 61 6d 69 6c 79  ····Jones Family
020 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
030 [illegible] 01 00 00 00-d3 ff ff ff 01 00 00 00  ........Óÿÿÿ····
040 20 00 00 00 64 00 00 00-00 00 00 00 88 2f 25 00   ···d·......../%·
050 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
060 01 00 00 00 82 84 8b 96-00 00 00 00 00 00 00 00  ................
070 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
080 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
[illegible] 00 00 00 00-00 00 00 00 00 00 00 00  ................
```

BSSID
SSID
Encryption disabled
Open network

software\Microsoft\WZCSVC\Parameters\Interfaces\{24E2DF49-403A-47BA-9653-A6FEA1317B46} Offset: 0

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces

- Interface configuration information
  - IP Address
  - Subnet Mask
  - DHCP lease obtained time (epoch time)
  - DHCP Server address
- Only the **most recent** configuration information
- **Previous configuration information** may be found in **restore points**.
- ***DHCP lease obtained time*** to pinpoint the date & time of the last connection

AccessData Registry Viewer - [_REGISTRY_MACHINE_SYSTEM]

File Edit Report View Window Help

- SysmonLog
- TapiSrv
- Tcpip
  - Linkage
  - Parameters
    - Adapters
    - DNSRegisteredAdapters
    - Interfaces
      - {0AB14DE1-88CC-443E-8B86-B9266B4C9C64}
      - {24E2DF49-403A-47BA-9653-A6FEA1317B46}
      - {27AA1DB8-FA9B-43D2-9593-DD61UB1A45BB}
      - {52826762-41E9-450C-BAEA-A10A822479BE}
      - {554C6A98-C8E0-4984-B112-C34DD22B746C}
      - {6A6596E3-D4E7-4225-92D7-6F7E28F3A2B0}
      - {6D30E2B9-6206-4644-8CC0-E60BFE71CEC1}
      - {F2B985F2-FD9B-4E37-A1B4-175FC795AF56}
    - PersistentRoutes
    - Winsock
  - Performance
  - Security
  - ServiceProvider
- TDPIPE
- TDTCP
- TermDD
- TermService
- Themes
- tifm21
- TlntSvr

Key Properties

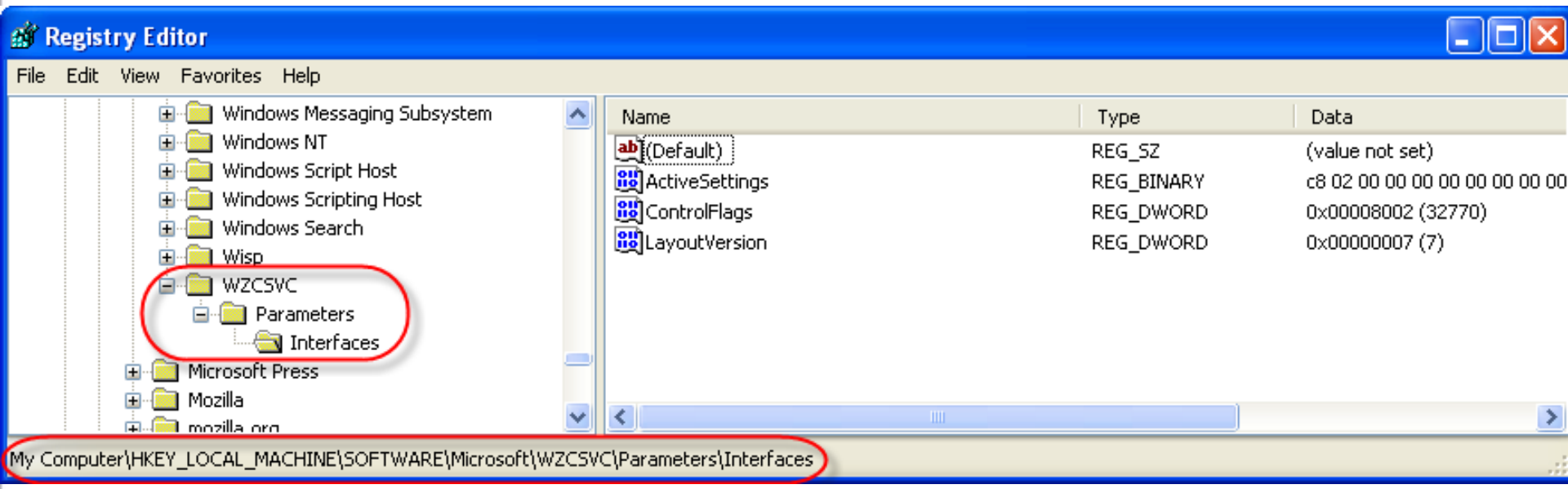
Last Written Time	16/09/2009 18:18:04 UTC

Name	Type	Data
UseZeroBroadcast	REG_DWORD	0x00000000 (0)
EnableDeadGWDetect	REG_DWORD	0x00000001 (1)
EnableDHCP	REG_DWORD	0x00000001 (1)
IPAddress	REG_MULTI_SZ	0.0.0.0
SubnetMask	REG_MULTI_SZ	0.0.0.0
DefaultGateway	REG_MULTI_SZ	(value not set)
DefaultGatewayMetric	REG_MULTI_SZ	(value not set)
NameServer	REG_SZ	(value not set)
Domain	REG_SZ	(value not set)
RegistrationEnabled	REG_DWORD	0x00000001 (1)
RegisterAdapterName	REG_DWORD	0x00000000 (0)
TCPAllowedPorts	REG_MULTI_SZ	0
UDPAllowedPorts	REG_MULTI_SZ	0
RawIPAllowedProtocols	REG_MULTI_SZ	0
NTEContextList	REG_MULTI_SZ	(value not set)
DhcpClassIdBin	REG_BINARY	(value not set)
DhcpIPAddress	REG_SZ	192.168.0.101
DhcpSubnetMask	REG_SZ	255.255.255.0
DhcpServer	REG_SZ	192.168.0.1
Lease	REG_DWORD	0x00093A80 (604800)
LeaseObtainedTime	REG_DWORD	0x4AAD23B3 (1252860851)
T1	REG_DWORD	0x4AB1C0F3 (1253163251)
T2	REG_DWORD	0x4AB536E3 (1253390051)
LeaseTerminatesTime	REG_DWORD	0x4AB65E33 (1253465651)
IPAutoconfigurationAddress	REG_SZ	0.0.0.0
IPAutoconfigurationMask	REG_SZ	255.255.0.0
IPAutoconfigurationSeed	REG_DWORD	0x58B74440 (1488405568)
AddressType	REG_DWORD	0x00000000 (0)
IsServerNapAware	REG_DWORD	0x00000000 (0)

_REGISTRY_MACHINE_SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{24E2DF49-403A-47BA-9 Offset: 0

If the computer has **never connected** to a wireless network, no keys with GUIDs should show up

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WZCSVC\Parameters\Interfaces



Following the GUID

- You can follow the globally unique identifier through the different registry keys to get a clearer picture of where and when a user was connecting with a particular adapter.

- You can also look through the computer's restore points to gain a historical perspective.

AccessData Registry Viewer - [software]

File Edit Report View Window Help

31
32
34
NWCS
OpenGLDrivers
PeerNet
Perflib

Key Properties

Last Written Time	12/08/2009 18:55:13 UTC

Name	Type	Data
ServiceName	REG_SZ	{ED25DA33-CB0D-4365-9A0D-4D933B84BF2D}
Description	REG_SZ	NETGEAR WG111v3 54Mbps Wireless USB 2.0 Adapter

```
00 4e 00 45 00 54 00 47 00-45 00 41 00 52 00 20 00 N·E·T·G·E·A·R· ·
10 57 00 47 00 31 00 31 00-31 00 76 00 33 00 20 00 W·G·1·1·1·v·3· ·
20 35 00 34 00 4d 00 62 00-70 00 73 00 20 00 57 00 5·4·M·b·p·s· ·W·
30 69 00 72 00 65 00 6c 00-65 00 73 00 73 00 20 00 i·r·e·l·e·s·s· ·
```

software\Microsoft\Windows NT\CurrentVersion\NetworkCards\34

Offset: 0

AccessData Registry Viewer - [software]

File Edit Report View Window Help

- WZCSVC
  - Parameters
    - Interfaces
      - {554C6A98-C8E0-4984-B112-C34DD22B746C}
      - {B647E28F-CD10-4022-9F7F-02CA2799DA06}
      - {E869C63D-B1F9-4F32-B603-13D5CADB5E5E}
      - {ED25DA33-CB0D-4365-9A0D-4D933B84BF2D}
- MicroVision
- Mozilla
- mozilla.org
- NETGEAR
- Network Associates
- Novell
- ODBC

Key Properties

Last Written Time	12/08/2009 18:59:10 UTC

Name	Type	Data
LayoutVersion	REG_DWORD	0x00000007 (7)
ControlFlags	REG_DWORD	0x03818002 (58818562)
ActiveSettings	REG_BINARY	C8 02 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 ...
Static#0000	REG_BINARY	C8 02 00 00 00 42 00 00 00 13 46 C1 1F 72 00 18 07 00 ...

```
000  c8 02 00 00 00 42 00 00-00 13 46 cl 1f 72 00 18  È····B····FÁ·r··
010  07 00 00 00 64 65 66 61-75 6c 74 00 00 00 00 00  ···default·····
020  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ··————————————··
030  00 00 00 00 01 00 00 00-c5 ff ff ff 03 00 00 00  ————————Åÿÿÿ————
040  20 00 00 00 64 00 00 00-00 00 00 00 88 2f 25 00  ···d————————/%·
050  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ··————————————··
060  01 00 00 00 82 84 8b 96-0c 12 18 24 00 00 00 00  ————————————$———
070  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ··————————————··
080  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ··————————————··
090  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ··————————————··
0a0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ··————————————··
0b0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ··————————————··
0c0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ··————————————··
```

software\Microsoft\WZCSVC\Parameters\Interfaces\{ED25DA33-CB0D-4365-9A0D-4D933B84BF2D}

Offset: 0

AccessData Registry Viewer - [system]

File Edit Report View Window Help

- Interfaces
  - {27AA1DB8-FA9B-43D2-9593-DD610B1A45BB}
  - {52826762-41E9-450C-BAEA-A10A822479BE}
  - {554C6A98-C8E0-4984-B112-C34DD22B746C}
  - {6A6596E3-D4E7-4225-92D7-6F7E28F3A2B0}
  - {6D30E2B9-6206-4644-8CC0-E60BFE71CEC1}
  - {B647E28F-CD10-4022-9F7F-02CA2799DA06}
  - {BD54E24F-24DB-4934-8B20-E8F391E93225}
  - {ED25DA33-CB0D-4365-9A0D-4D933B84BF2D}
  - {F2B985F2-FD9B-4E37-A1B4-175FC795AF56}
- PersistentRoutes
- Winsock
- Performance
- Security
- ServiceProvider
- TDPIPE
- TDTCP
- TermDD
- TermService
- Themes
- tifm21
- TlntSvr
- TosIde
- TrkWks
- TSDDD
- Udfs
- ultra
- UMWdf

Key Properties

Last Written Time	12/08/2009 18:59:10 UTC

Name	Type	Data
UseZeroBroadcast	REG_DWORD	0x00000000 (0)
EnableDeadGWDetect	REG_DWORD	0x00000001 (1)
EnableDHCP	REG_DWORD	0x00000001 (1)
IPAddress	REG_MULTI_SZ	0.0.0.0
SubnetMask	REG_MULTI_SZ	0.0.0.0
DefaultGateway	REG_MULTI_SZ	(value not set)
DefaultGatewayMetric	REG_MULTI_SZ	(value not set)
NameServer	REG_SZ	(value not set)
Domain	REG_SZ	(value not set)
RegistrationEnabled	REG_DWORD	0x00000001 (1)
RegisterAdapterName	REG_DWORD	0x00000000 (0)
TCPAllowedPorts	REG_MULTI_SZ	0
UDPAllowedPorts	REG_MULTI_SZ	0
RawIPAllowedProtocols	REG_MULTI_SZ	0
NTEContextList	REG_MULTI_SZ	(value not set)
DhcpClassIdBin	REG_BINARY	(value not set)
DhcpIPAddress	REG_SZ	192.168.0.106
DhcpSubnetMask	REG_SZ	255.255.255.0
DhcpServer	REG_SZ	192.168.0.1
Lease	REG_DWORD	0x00093A80 (604800)
LeaseObtainedTime	REG_DWORD	0x4A83108D (1250103437)
T1	REG_DWORD	0x4A87ADCD (1250405837)
T2	REG_DWORD	0x4A8B23BD (1250632637)
LeaseTerminatesTime	REG_DWORD	0x4A8C4B0D (1250708237)
IPAutoconfigurationAddress	REG_SZ	0.0.0.0
IPAutoconfigurationMask	REG_SZ	255.255.0.0
IPAutoconfigurationSeed	REG_DWORD	0x00000000 (0)
AddressType	REG_DWORD	0x00000000 (0)
IsServerNapAware	REG_DWORD	0x00000000 (0)

system\ControlSet001\Services\Tcpip\Parameters\Interfaces\{ED25DA33-CB0D-4365-9A0D-4D933B

Offset: 0

Tracking User Activity

- **TypedURLS** (Internet Explorer)
  - HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs
  - HKEY_USERS\<*SID*>\Software\Microsoft\Internet Explorer\TypedURLs
- **MRU Lists**
- **Adobe**
  - \Software\Adobe\AcrobatReader\8.0\AVGeneral\cRecentFiles\c*n*
- **Remote Desktop Connections**
  - \Software\Microsoft\Terminal Server Client\Default

Example: Internet Explorer Typed URLs

AccessData Registry Viewer - [_REGISTRY_USER_NTUSER_S-1-5-21-930212210-811250829-2050355374-1008]

File Edit Report View Window Help

- SearchScopes
- SearchUrl
- Security
- Services
- Settings
- TabbedBrowsing
- Toolbar
- TypedURLs
- URLSearchHooks
- Zoom
- Keyboard
- MediaPlayer
- MessengerService

Name	Type	Data
url1	REG_SZ	http://nytimes.com/
url2	REG_SZ	http://reddit.com/
url3	REG_SZ	http://cnn.com/
url4	REG_SZ	http://slashdot.org/
url5	REG_SZ	http://digg.com/
url6	REG_SZ	http://cbc.ca/
url7	REG_SZ	http://www.fbi.gov/
url8	REG_SZ	http://www.csis.gc.ca/
url9	REG_SZ	http://www.rcmp-grc.gc.ca/
url10	REG_SZ	http://www.rcmp.com/
url11	REG_SZ	http://go.microsoft.com/fwlink/?LinkId=69157

Key Properties

Last Written Time	16/09/2009 18:21:52 UTC

```
00 68 00 74 00 74 00 70 00-3a 00 2f 00 2f 00 6e 00 h·t·t·p·:·/·/·n·
10 79 00 74 00 69 00 6d 00-65 00 73 00 2e 00 63 00 y·t·i·m·e·s·.·c·
20 6f 00 6d 00 2f 00 00 00-                        o·m·/···
```

_REGISTRY_USER_NTUSER_S-1-5-21-930212210-811250829-2050355374-1008\Software\Microsoft\Internet I | C | Offset: 0

Tracking User Activity

- If the user has logged on multiple times you may only get the most recent session's information
- Going back in time by using restore points can give you snapshots of Data from specific points in time

CORROBORATING REGISTRY DATA

Corroborating registry information with Wireless Access Point Information

- Manufacturer
- SSID
- BSSID
- Encryption & Authentication
- DHCP log file
- Activity log files
- System log files

AccessData Registry Viewer - [software]

File Edit Report View Window Help

- Wisp
- Works
- WZCSVC
  - Parameters
    - Interfaces
      - {24E2DF49-403A-47BA-9653-A6FEA1317B46}
      - {554C6A98-C8E0-4984-B112-C34DD22B746C}
      - {E869C63D-B1F9-4F32-B603-13D5CADB5E5E}
- MicroVision

Name	Type	Data
LayoutVersion	REG_DWORD	0x00000007 (7)
ControlFlags	REG_DWORD	0x03818002 (58818562)
ActiveSettings	REG_BINARY	C8 02 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 ...
Static#0000	REG_BINARY	C8 02 00 00 03 00 00 00 00 1A 70 6E 72 73 00 00 0C 00 ...
Static#0001	REG_BINARY	C8 02 00 00 00 40 00 00 00 13 46 C1 1F 72 00 00 07 00 ...

Key Properties

Last Written Time	16/09/2009 19:11:08 UTC

```
000  c8 02 00 [BSSID] 00-00 1a 70 6e 72 73 00 00  È·····pnrs··
010  0c 00 00 00 53 6d 69 74-68 20 46 61 6d 69 [SSID] ··Smith Family
020  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ······· ·····
030  00 [TKIP] 04 00 00 00-ea ff ff ff 03 00 00 00  ·····êÿÿÿ····
040  20 00 00 00 64 00 00 00-00 00 00 00 88 2f 25 00   ···d·····/%·
050  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ····· ·····
060  01 00 00 00 82 84 8b 96-24 30 48 6c 00 00 00 00  ·····$0Hl····
070  20 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00   ····· ·····
080  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ····· ·····
090  [WPA] 04 00 00 00-00 00 00 00 00 00 00 00  ····· ·····
```

software\Microsoft\WZCSVC\Parameters\Interfaces\{554C6A98-C8E0-4984-B112-C34DD22B746C} Offset: 0

LINKSYS®
A Division of Cisco Systems, Inc.

Firmware Version : v4.30.7

Wireless-G Broadband Router | Smith Family

Status

Setup | Wireless | Security | Access Restrictions | Applications & Gaming | Administration | Status

Router | Local Network | Wireless

Wireless

MAC Address :	00:1A:70:6E:72:73
Mode :	Mixed
SSID :	Smith Family
DHCP Server :	Enabled
Channel :	6
Encryption Function :	Enabled

MAC Address. This is the Router's MAC Address, as seen on your local, wireless network.

Mode. As selected from the Wireless tab, this will display the wireless mode (Mixed, G-Only, or Disabled) used by the network. **More...**

Refresh

CISCO SYSTEMS

LINKSYS®
A Division of Cisco Systems, Inc.

Firmware Version : v4.30.7

Wireless-G Broadband Router | Smith Family

Wireless

Setup | Wireless | Security | Access Restrictions | Applications & Gaming | Administration | Status

Basic Wireless Settings | Wireless Security | Wireless MAC Filter | Advanced Wireless Settings

Wireless Security

Security Mode :	WPA Personal
WPA Algorithms :	TKIP
WPA Shared Key :	Natal Brazil
Group Key Renewal :	3600 seconds

Security Mode : You may choose from Disable, WEP, WPA Pre-Shared Key, WPA RADIUS, or RADIUS. All devices on your network must use the same security mode in order to communicate.
More...

Save Settings | Cancel Changes

CISCO SYSTEMS

System Log File

DHCP Active IP Table - Mozilla Firefox

http://10.22.33.1/DHCPTable.htm

DHCP Active IP Table

Refresh

DHCP Server IP Address: 10.22.33.1

Client Hostname	IP Address	MAC Address	Delete
CPC-5982375	10.22.33.100	00-1A-92-5A-5C-78	☐
ROWE-CPC	10.22.33.101	00-17-A4-CD-FF-0C	☐
ROWE-CPC	10.22.33.102	00-11-A3-BB-10-3C	☐

Done

Activity Log File

Outgoing Log Table - Mozilla Firefox

http://10.22.33.1/outLogTable.htm

Refresh

Outgoing Log Table

LAN IP	Destination URL/IP	Service/Port Number
10.22.33.100	static.cache.l.google.com	HTTP
10.22.33.100	safebrowsing.clients.google.com	HTTP
10.22.33.100	news.bbc.co.uk	HTTP
10.22.33.100	en-gb.fxfeeds.mozilla.com	HTTP
10.22.33.100	forensic.tech.googlepages.com	HTTP
10.22.33.100	pv-mirror01.mozilla.org	HTTP
10.22.33.100	forensic.tech.googlepages.com	HTTP
10.22.33.100	download.mozilla.org	HTTP

Done

System Log File

System Log - Mozilla Firefox

http://10.22.33.1/SysLogTable.htm

System Log

System Up Time: 0 days 00:11:25

ALL | Clear | Refresh

```
00:00:00 [10.22.33.1] : System is ready
00:00:00 System is cold start
00:00:00 Firmware Version : 1.45.3, Sep 26 2003
00:00:03 3/ICMP to 192.168.0.1 Dropping ICMP error message.
00:00:09 WAN(DHCP) IP is 192.168.3.221
00:01:55 TCP from 10.22.33.100:1903 to download.mozilla.org(63.245.209.58):80
00:01:55 TCP from 10.22.33.100:1904 to forensic.tech.googlepages.com(74.125.47.118):80
00:01:55 TCP from 10.22.33.100:1905 to pv-mirror01.mozilla.org(204.152.184.196):80
00:01:55 TCP from 10.22.33.100:1906 to forensic.tech.googlepages.com(74.125.47.118):80
00:02:00 TCP from 10.22.33.100:1907 to en-gb.fxfeeds.mozilla.com(63.245.209.45):80
00:02:00 TCP from 10.22.33.100:1908 to news.bbc.co.uk(212.58.226.29):80
00:02:11 Web login successfully from 10.22.33.100
00:02:37 TCP from 10.22.33.100:1914 to safebrowsing.clients.google.com(66.102.1.100):80
00:03:43 TCP from 10.22.33.100:1919 to static.cache.l.google.com(74.125.165.94):80
```

Clear | Refresh

Done

BSSID / MAC Address

BSSID = MAC Address = Adapter Hardware Address

Organizationally Unique Identifier (OUI)

- First three octets / Six hexadecimal characters
- E.g. **<u>00 1a 70</u> 5e 72 73**

- 0x10 **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WZCSVC\Parameters\Interfaces\Static#xxxx**
- Kismet, NetStumbler

- Can be looked up on Internet to determine the Access Point or adapter manufacturer

http://standards.ieee.org/regauth/oui/index.shtml

IEEE HOME | SEARCH IEEE | SHOP | WEB ACCOUNT | CONTACT IEEE

Membership Publications Services Standards Conferences Careers/Jobs

IEEE Standards Association

IEEE-SA Global Communities Text Size: A A A

PRODUCTS & SERVICES | IEEE-SA MEMBERSHIP | STANDARDS DEVELOPMENT | NEWS

Products & Services Home

Products
- ShopIEEE
- IEEE Standards Press

Services
- Standards Online Subcriptions
- Get IEEE 802®
- Get IEEE/ANSI N42™
- OUI, MAC or Ethernet and Other Registration

Reference Materials
- Interpretations
- Errata and Corrections
- Downloadable Documents

IEEE OUI and Company_id Assignments

The below public listings should be searched prior to applying for an OUI or IAB. Searching the list will allow you to determine whether your company or any parent/subsidiary companies already own an assignment. When searching the public listings, addresses should be entered as XX-XX-XX.

Your attention is called to the fact that the firms and numbers listed may not always be obvious in product implementations, as some manufacturers subcontract component manufacture and others include registered firm OUIs in their products.

Search the public OUI listing . . .

Search for: 001a70

Search! clear field

00-1A-70	(hex)	Cisco-Linksys, LLC
001A70	(base 16)	Cisco-Linksys, LLC 121 Theory Drive Irvine California 9261 UNITED STATES

Identifying WiFi Clients (Kismet)

Client List (Latest Seen)

!	MAC	Manuf	Data	Crypt	Size	IP Range	Sgn	Nse
! S	00:50:E8:06:03:D0	Unknown	25124	0	19M	10.0.0.139	0	0
! T	00:16:CF:73:28:29	Unknown	5225	0	818k	10.0.0.164	0	0
T	00:1F:3A:19:31:7C	Unknown	1289	0	159k	10.0.0.145	0	0
T	00:1A:73:BB:8B:70	Unknown	793	0	207k	10.0.0.151	0	0
T	00:16:44:6D:20:0A	Unknown	565	0	82k	10.0.0.147	0	0
T	00:90:4B:CD:5A:1E	Unknown	60	0	7k	10.0.0.139	0	0
T	00:1D:4F:21:D2:B7	Unknown	5522	0	764k	10.0.0.114	0	0

00-1D-4F (hex) Apple Computer Inc.
001D4F (base 16) Apple Computer Inc.
1 Infinite Loop
Cupertino California 95014
UNITED STATES

A FINAL NOTE:
WIFI AD-HOC NETWORKS

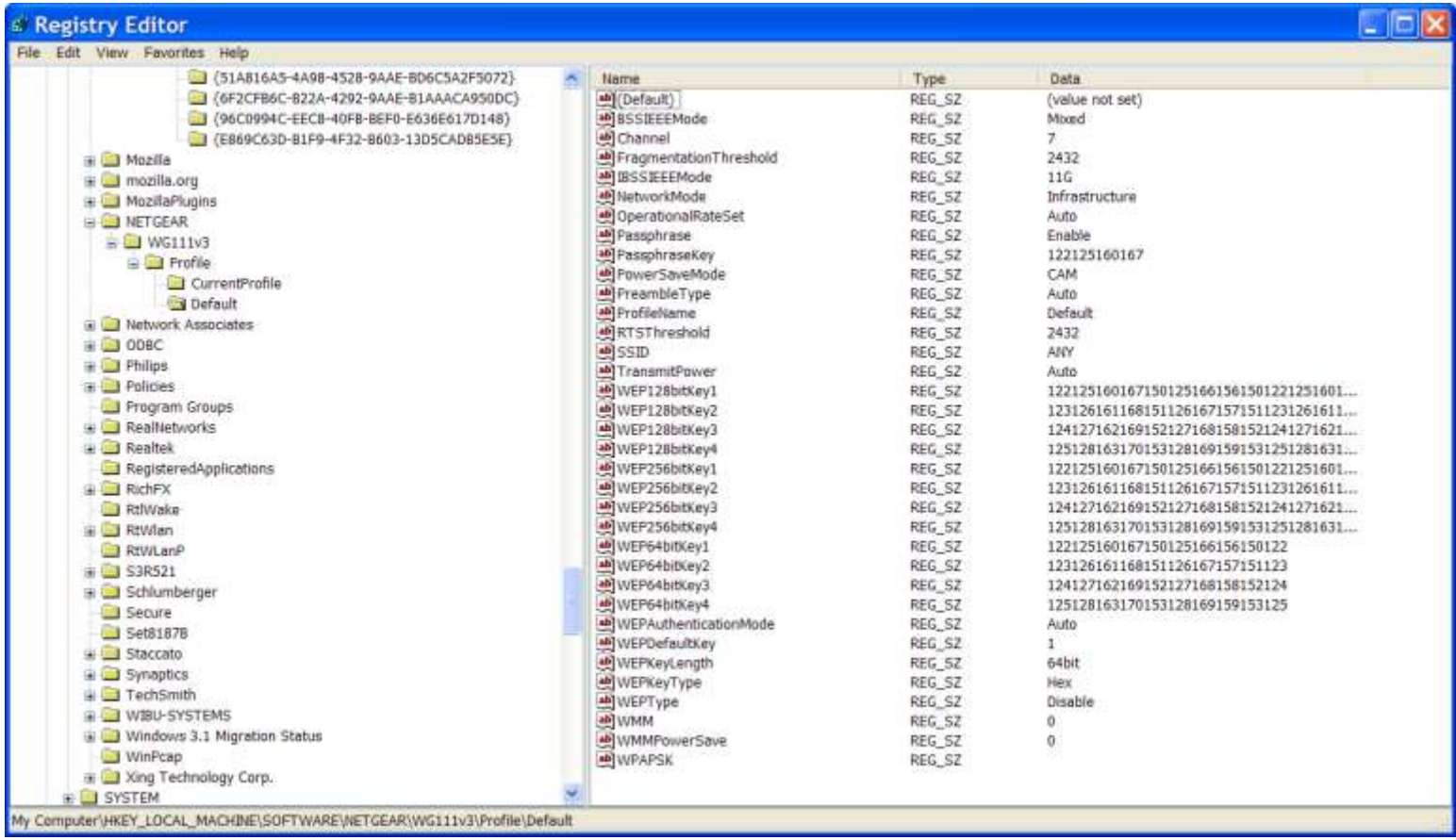
WiFi Ad-hoc Networks

Keys of Interest:

HKEY_LOCAL_MACHINE\SOFTWARE\...

- Was an independent ad/hoc network set up by the user, and if so what were its settings?
- The answer to this question may be found in the Registry under the **WiFi adapter's software settings**

HKEY_LOCAL_MACHINE\SOFTWARE\NETGEAR\WG111V3\Profile\Default



Thank you

Eric Rowe

Royal Canadian Mounted Police

Canadian Police College

erowe@cpc.gc.ca