Wireless Router Interrogation

July 26, 2012

D. Matthew Powell

Webinar Information

- All attendees will be muted.
- If you desire to ask a question, please use the questions section of the GoToWebinar dialog box, typically in the upper right corner of the screen.
- Please do not raise your hand for questions since we cannot unmute you.
- The questions will either be answered directly by a panelist or asked to the presenter who will answer.

Webinar Information

- Poll questions may be asked during the webinar. They will be left open only a short period of time so please respond promptly.

QUICKPOLL

Which best describes your role?

Select one of the following:

○ Investigator
○ Forensic Examiner
○ Prosecutor
○ Other

Poll in progress for attendees only

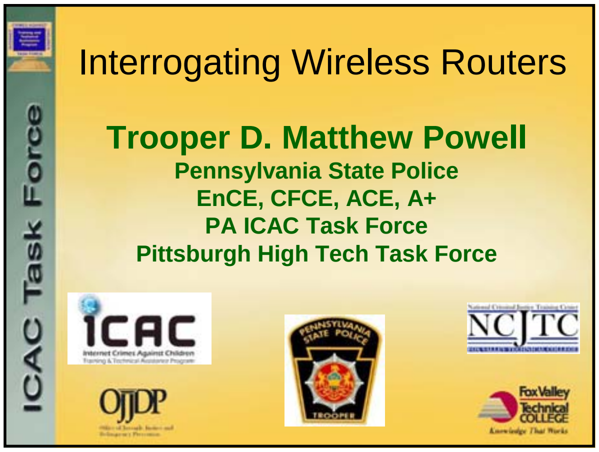
ICAC Task Force

Webinar Information

- At the conclusion of the webinar a short survey will appear. Please complete it before signing off.
- A link to view the recorded webinar and the Powerpoint slides will be provided to you via email after the webinar.

OJJDP

Fox Valley Technical College Knowledge That Works



ICAC Task Force

Interrogating Wireless Routers

Trooper D. Matthew Powell
Pennsylvania State Police
EnCE, CFCE, ACE, A+
PA ICAC Task Force
Pittsburgh High Tech Task Force

ICAC Internet Crimes Against Children Training & Technical Assistance Program

Pennsylvania State Police Trooper

NCJTC

OJJDP

Fox Valley Technical College Knowledge That Works

ICAC Task Force

Examples of Wireless Routers

ICAC Task Force

MAC Addresses

The MAC address is a unique value associated with a network adapter/device. MAC addresses are also known as hardware or physical addresses. They uniquely identify an adapter/device on a LAN.

MAC addresses are 12-digit hexadecimal numbers (48 bits in length). By convention, MAC addresses are usually written in one of the following two formats:

MM:MM:MM:SS:SS:SS or MM-MM-MM-SS-SS-SS

e.g.: 60:33:4b:2a:cf:d1

The first half of a MAC address contains the ID number of the adapter manufacturer. These IDs are regulated by an Internet standards body.

The second half of a MAC address represents the serial number assigned to the adapter by the manufacturer.

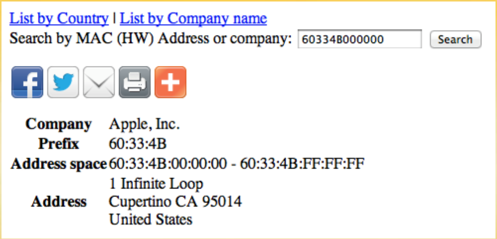
OJJDP

Fox Valley Technical College
Knowledge That Works

ICAC Task Force

MAC Addresses

If you do a Google search for the MAC address or visit hwaddress.com
You can enter the MAC address and you will be provided with the Manufacturer of that device.



Search by MAC (HW) Address or company: 60334B000000

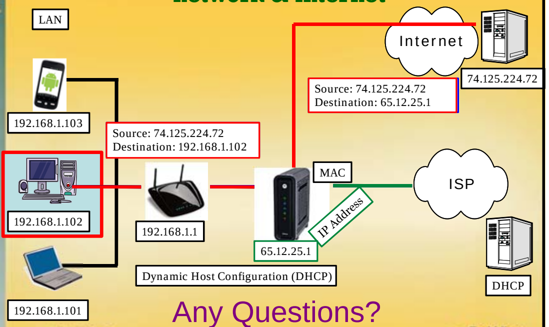
Company	Apple, Inc.
Prefix	60:33:4B
Address space	60:33:4B:00:00:00 - 60:33:4B:FF:FF:FF
Address	1 Infinite Loop Cupertino CA 95014 United States

OJJDP

Fox Valley Technical College
Knowledge That Works

ICAC Task Force

How the router is used to communicate on the network & internet



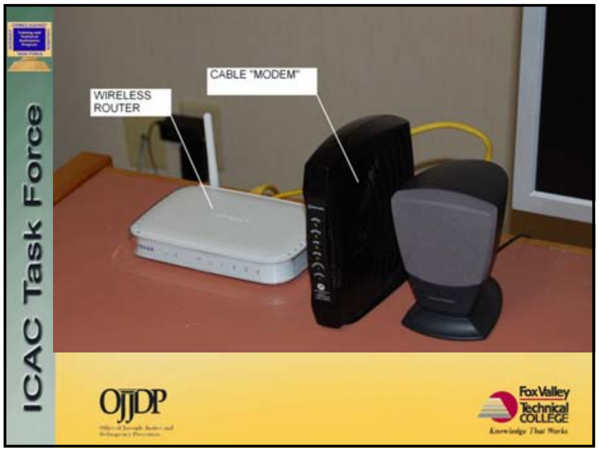
Any Questions?
Poll Question #2

OJJDP

Fox Valley Technical College
Knowledge That Works

ICAC Task Force

THE SEARCH



ICAC Task Force

OJJDP

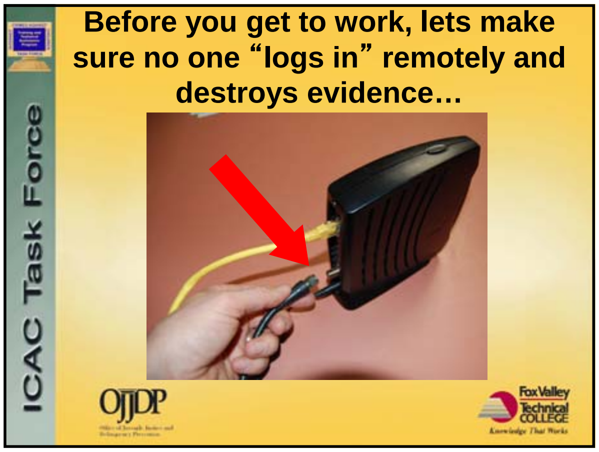
Fox Valley Technical College
Knowledge That Works

ICAC Task Force

Once you find your device… remember that digital photos and videos are FREE.

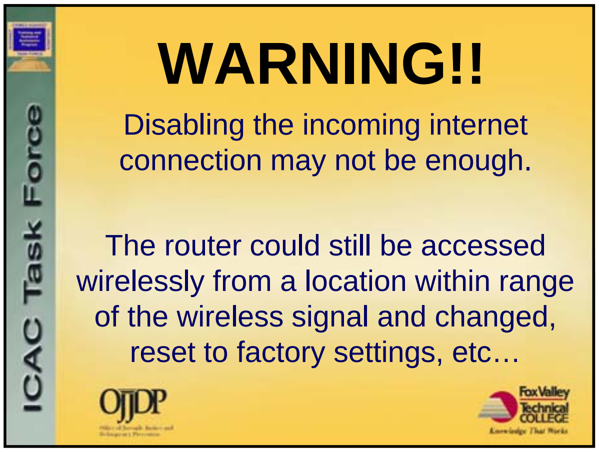
OJJDP

Fox Valley Technical College
Knowledge That Works



Before you get to work, lets make sure no one “logs in” remotely and destroys evidence…

YOU REALLY DIDN’T JUST TOUCH YOUR SUSPECT’S PROPERTY WITH OUT GLOVES ON…. RIGHT?



WARNING!!

Disabling the incoming internet connection may not be enough.

The router could still be accessed wirelessly from a location within range of the wireless signal and changed, reset to factory settings, etc…

ICAC Task Force
OJJDP
Fox Valley Technical College

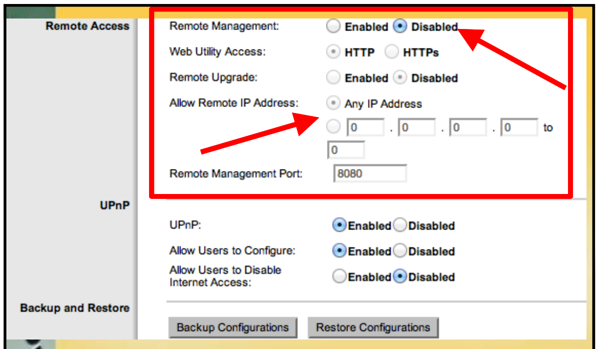
ICAC Task Force

Remote access is unlikely, but… not impossible.

- By default, most wireless routers DO NOT allow “admin access” via wireless means.
- Furthermore, most people running a wireless network do not enable this “admin access” via wireless means (likely because they do not know how).

OJJDP

Fox Valley Technical College Knowledge That Works



Remote Access

Remote Management: ○ Enabled ● Disabled

Web Utility Access: ● HTTP ○ HTTPs

Remote Upgrade: ○ Enabled ● Disabled

Allow Remote IP Address: ● Any IP Address

○ 0 . 0 . 0 . 0 to 0

Remote Management Port: 8080

UPnP

UPnP: ● Enabled ○ Disabled

Allow Users to Configure: ● Enabled ○ Disabled

Allow Users to Disable Internet Access: ○ Enabled ● Disabled

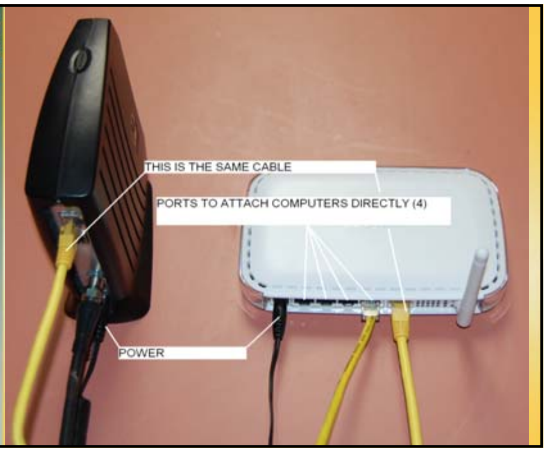
Backup and Restore

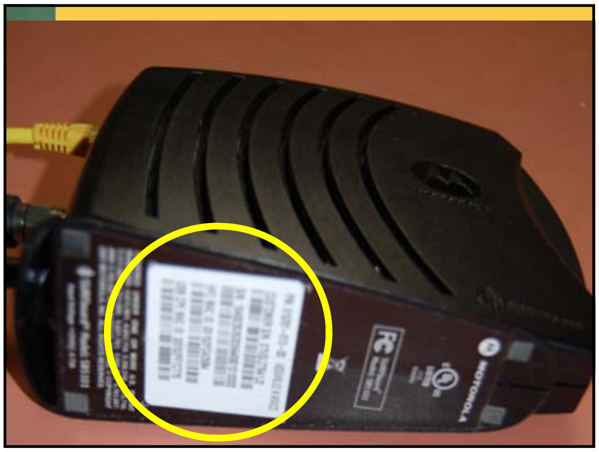
ICAC

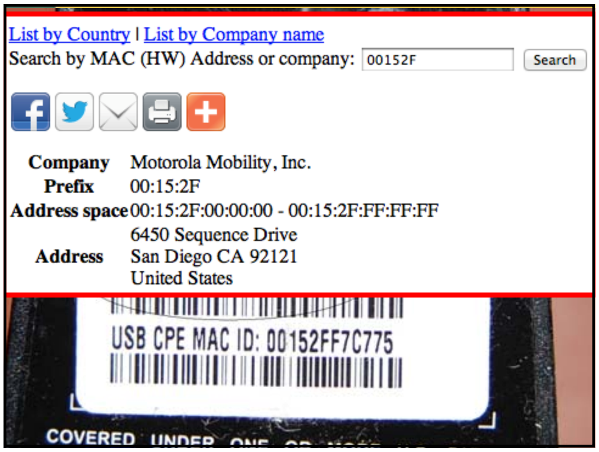
OJJDP

Fox Valley Technical College Knowledge That Works

ICAC Task Force



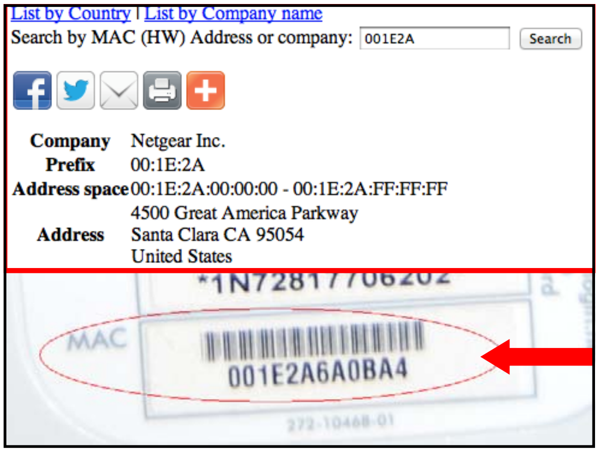




List by Country | List by Company name

Search by MAC (HW) Address or company: 00152F Search

Company	Motorola Mobility, Inc.
Prefix	00:15:2F
Address space	00:15:2F:00:00:00 - 00:15:2F:FF:FF:FF
Address	6450 Sequence Drive San Diego CA 92121 United States



List by Country | List by Company name

Search by MAC (HW) Address or company: 001E2A Search

Company	Netgear Inc.
Prefix	00:1E:2A
Address space	00:1E:2A:00:00:00 - 00:1E:2A:FF:FF:FF
Address	4500 Great America Parkway Santa Clara CA 95054 United States

ICAC Task Force

REFRESHER COURSE

MAC Address (Media Access Control): Hardware/Physical Address that uniquely identifies a device (or a node) on a network.

Node: A processing location on a network. A node can be a computer (laptop/desktop), a wireless printer, smartphone, tablet computer or more specifically the Network Interface Card (network card) within the device.

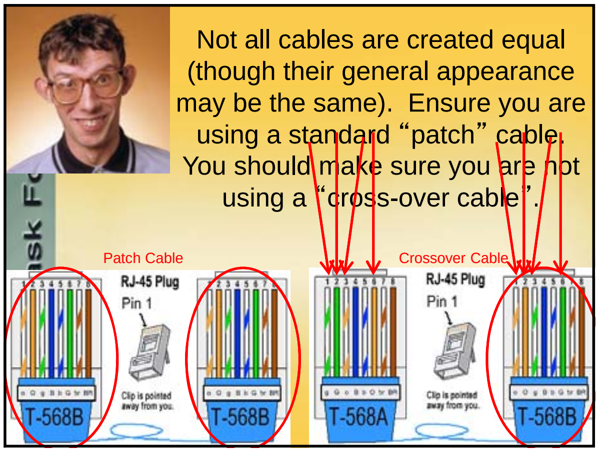
It would be beneficial to know your MAC address… this will be shown later.

Any Questions?

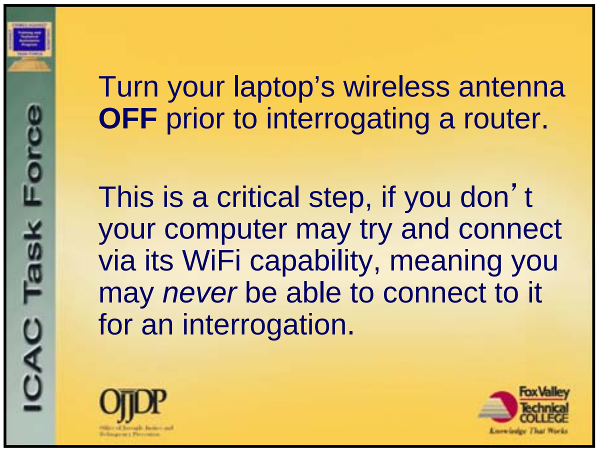
TIME FOR THE ROUTER INTERROGATION

Poll Question #3

GEEK COFFEE



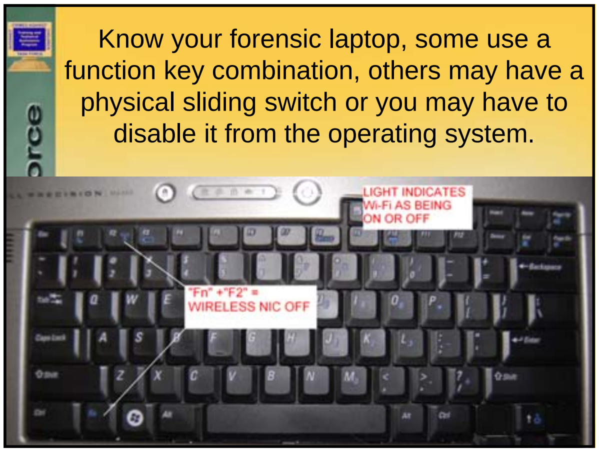
Not all cables are created equal (though their general appearance may be the same). Ensure you are using a standard “patch” cable. You should make sure you are not using a “cross-over cable”.



Turn your laptop’s wireless antenna **OFF** prior to interrogating a router.

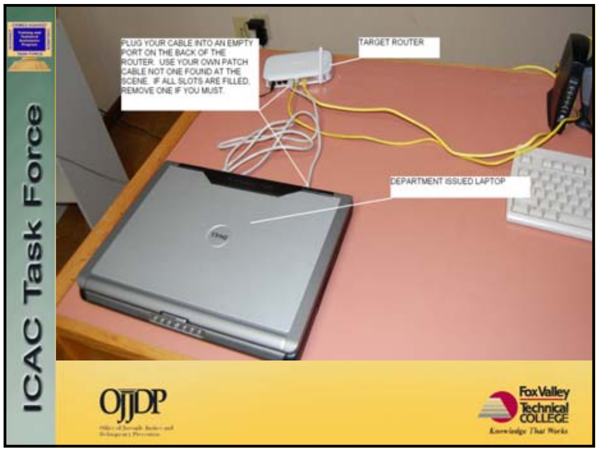
This is a critical step, if you don’t your computer may try and connect via its WiFi capability, meaning you may *never* be able to connect to it for an interrogation.

ICAC Task Force
OJJDP
Fox Valley Technical College
Knowledge That Works

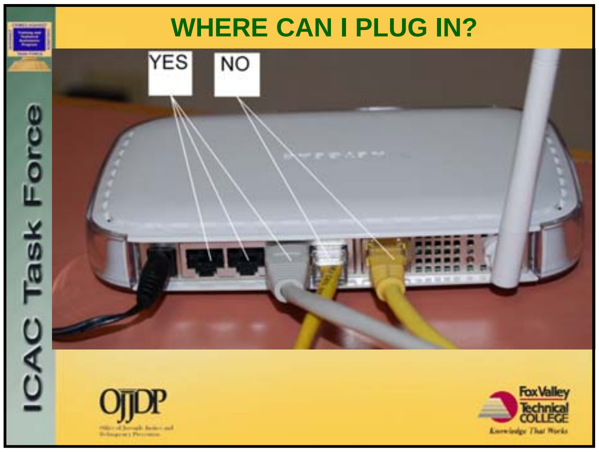


Know your forensic laptop, some use a function key combination, others may have a physical sliding switch or you may have to disable it from the operating system.

LIGHT INDICATES Wi-Fi AS BEING ON OR OFF
"Fn" +"F2" = WIRELESS NIC OFF



ICAC Task Force
PLUG YOUR CABLE INTO AN EMPTY PORT ON THE BACK OF THE ROUTER. USE YOUR OWN PATCH CABLE NOT ONE FOUND AT THE SCENE. IF ALL SLOTS ARE FILLED, REMOVE ONE IF YOU MUST.
TARGET ROUTER
DEPARTMENT ISSUED LAPTOP
OJJDP
Fox Valley Technical College
Knowledge That Works



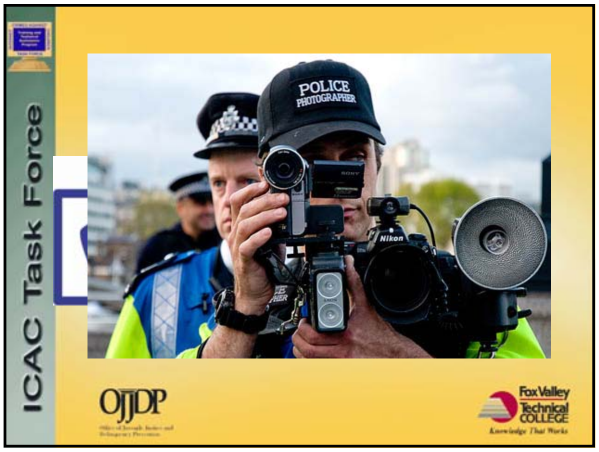
WHERE CAN I PLUG IN?

ICAC Task Force

OJJDP

Fox Valley Technical College

Knowledge That Works

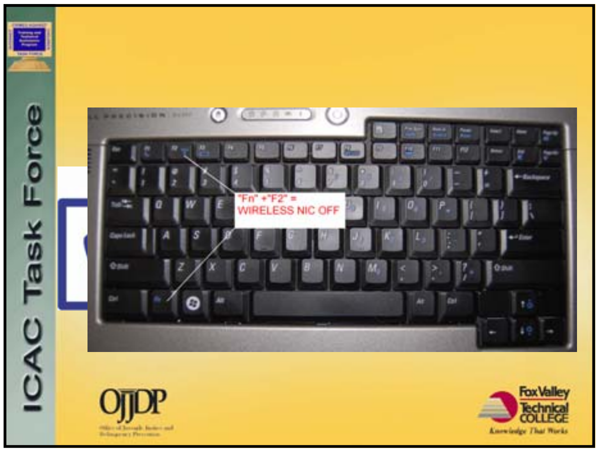


ICAC Task Force

OJJDP

Fox Valley Technical College

Knowledge That Works

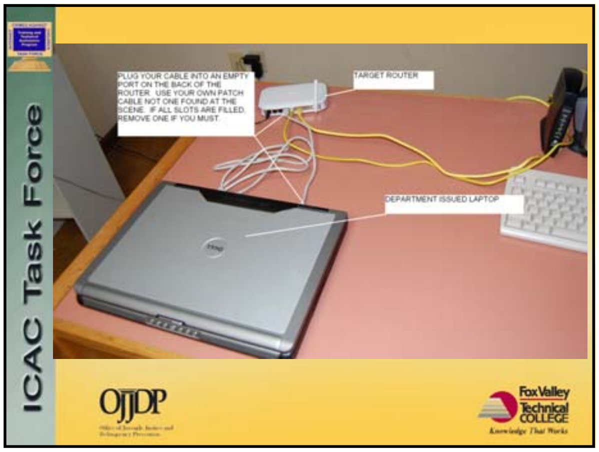


ICAC Task Force

OJJDP

Fox Valley Technical College

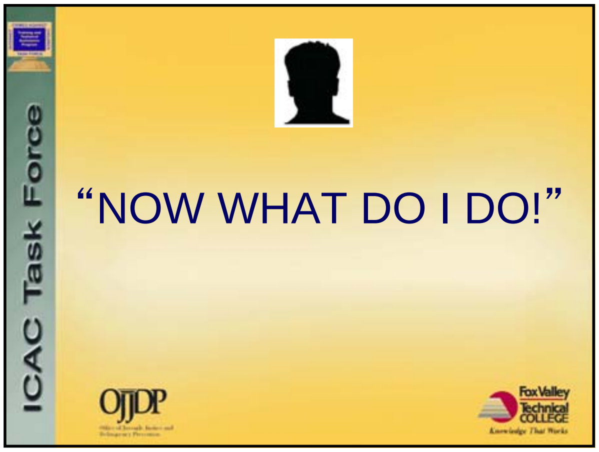
Knowledge That Works



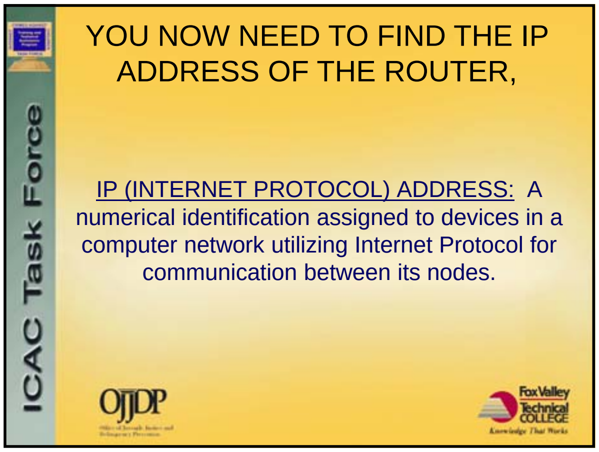
PLUG YOUR CABLE INTO AN EMPTY PORT ON THE BACK OF THE ROUTER. USE YOUR OWN PATCH CABLE NOT ONE FOUND AT THE SCENE. IF ALL SLOTS ARE FILLED, REMOVE ONE IF YOU MUST.

TARGET ROUTER

DEPARTMENT ISSUED LAPTOP


ICAC Task Force

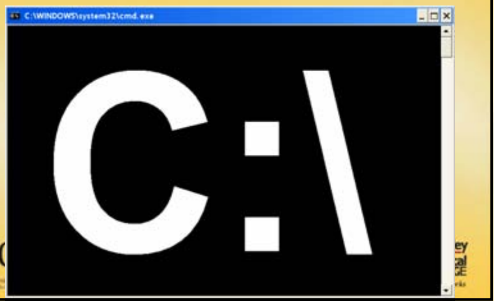
“NOW WHAT DO I DO!”


ICAC Task Force

YOU NOW NEED TO FIND THE IP ADDRESS OF THE ROUTER,

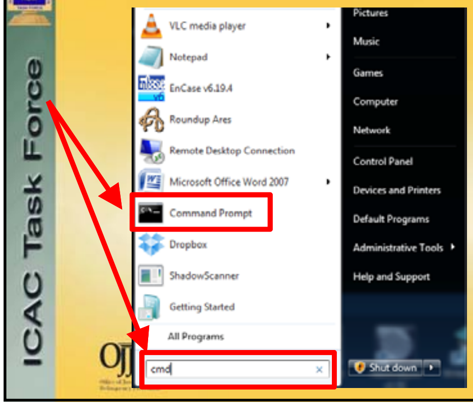
IP (INTERNET PROTOCOL) ADDRESS: A numerical identification assigned to devices in a computer network utilizing Internet Protocol for communication between its nodes.

TIME TO VISIT THE GHOST OF OPERATING SYSTEMS PAST….. DOS!!!



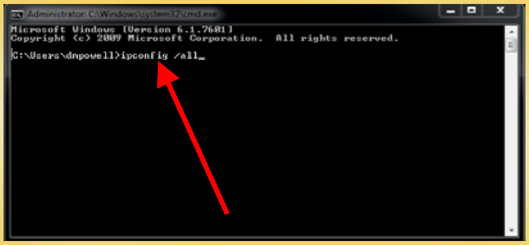
```
C:\
```

ROADMAP TO DOS

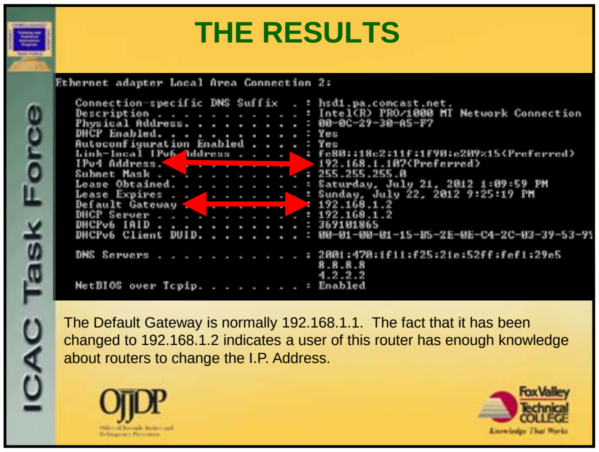


DOS COMMAND PROMPT

Type “IPCONFIG /ALL” (without the quotes… and there is a space after “ipconfig”…and no, it’s not case sensitive)
Then press Enter



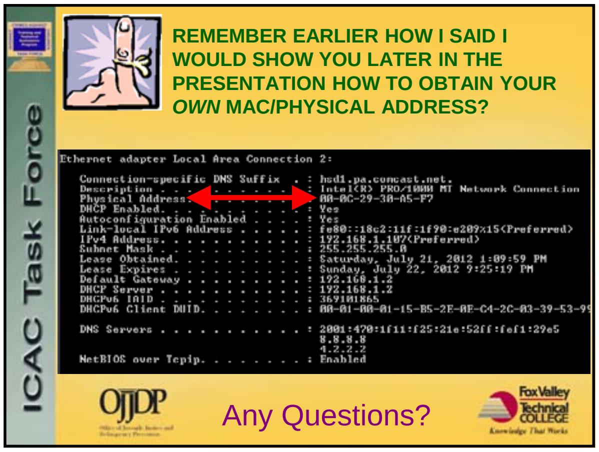
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\dnpowell>ipconfig /all_
```



THE RESULTS

```
Ethernet adapter Local Area Connection 2:

   Connection-specific DNS Suffix  . : hsd1.pa.comcast.net.
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Network Connection
   Physical Address. . . . . . . . . : 00-0C-29-30-A5-F7
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::18c2:11f:1f90:e209%15(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.107(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Saturday, July 21, 2012 1:09:59 PM
   Lease Expires . . . . . . . . . . : Sunday, July 22, 2012 9:25:19 PM
   Default Gateway . . . . . . . . . : 192.168.1.2
   DHCP Server . . . . . . . . . . . : 192.168.1.2
   DHCPv6 IAID . . . . . . . . . . . : 369101865
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-15-B5-2E-0E-C4-2C-03-39-53-9

   DNS Servers . . . . . . . . . . . : 2001:470:1f11:f25:21e:52ff:fef1:29e5
                                       8.8.8.8
                                       4.2.2.2
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

The Default Gateway is normally 192.168.1.1. The fact that it has been changed to 192.168.1.2 indicates a user of this router has enough knowledge about routers to change the I.P. Address.



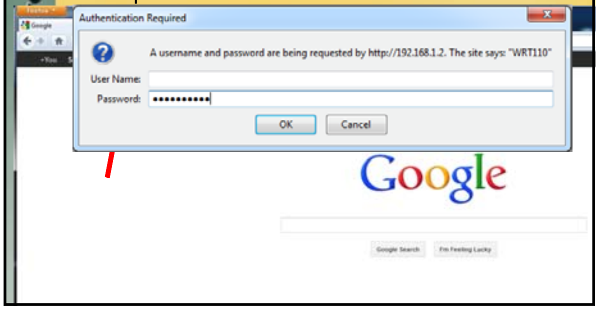
REMEMBER EARLIER HOW I SAID I WOULD SHOW YOU LATER IN THE PRESENTATION HOW TO OBTAIN YOUR *OWN* MAC/PHYSICAL ADDRESS?

```
Ethernet adapter Local Area Connection 2:

   Connection-specific DNS Suffix  . : hsd1.pa.comcast.net.
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Network Connection
   Physical Address. . . . . . . . . : 00-0C-29-30-A5-F7
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::18c2:11f:1f90:e209%15(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.107(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Saturday, July 21, 2012 1:09:59 PM
   Lease Expires . . . . . . . . . . : Sunday, July 22, 2012 9:25:19 PM
   Default Gateway . . . . . . . . . : 192.168.1.2
   DHCP Server . . . . . . . . . . . : 192.168.1.2
   DHCPv6 IAID . . . . . . . . . . . : 369101865
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-15-B5-2E-0E-C4-2C-03-39-53-9

   DNS Servers . . . . . . . . . . . : 2001:470:1f11:f25:21e:52ff:fef1:29e5
                                       8.8.8.8
                                       4.2.2.2
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Any Questions?

CHOOSE YOUR TOOL WITH WHICH TO INTERROGATE THE TARGET ROUTER

- Next enter the Router’s IP address in the URL bar… in our example it was 192.168.1.2, and press Enter.
- You should then be prompted for a username and password



Authentication Required

A username and password are being requested by http://192.168.1.2. The site says: "WRT110"

User Name:

Password: ••••••••••

ICAC Task Force

NOTE: The dialog box is a result of your browser looking for login credentials, not the router. A lot of Linksys/Cisco routers do NOT have a username, only a password.

There are different ways to obtain the router’s login credentials.

1. They may be written on the router itself by the suspect.

1. They may have never been changed from the default credentials… Google is your friend here… look them up (we will get to this)

1. If the router was provided by the ISP, the credentials may be imprinted on the bottom of the device.

2. Last, but definitely not least, ASK THE SUSPECT. Worst case scenario he says he won’t tell you, but usually, they tell you.

OJJDP

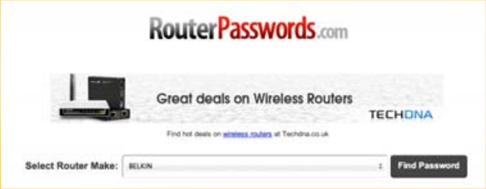
Fox Valley Technical College Knowledge That Works

ICAC Task Force

Linksys/Cisco likes using “admin” for the password (remember, usually there is no username with Linksys/Cisco routers)

Netgear likes using “admin” and “password” or “admin” and “1234” for defaults.

Visit “routerpasswords.com” for a list of common router makes/models for a complete list.
Just choose your router’s manufacturer from the dropdown list and click “Find Password”.



RouterPasswords.com

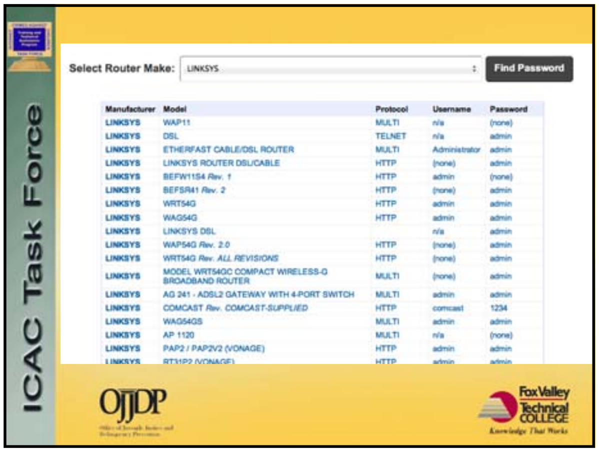
Great deals on Wireless Routers TECHDNA

Find hot deals on wireless routers at Techdna.co.uk

Select Router Make: BELKIN

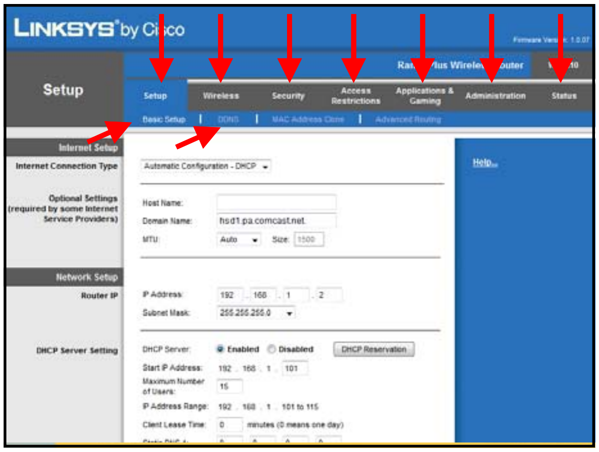
OJJDP

Fox Valley Technical College Knowledge That Works



Select Router Make: LINKSYS

Manufacturer	Model	Protocol	Username	Password
LINKSYS	WAP11	MULTI	n/a	(none)
LINKSYS	DSL	TELNET	n/a	admin
LINKSYS	ETHERFAST CABLE/DSL ROUTER	MULTI	Administrator	admin
LINKSYS	LINKSYS ROUTER DSL/CABLE	HTTP	(none)	admin
LINKSYS	BEFW11S4 *Rev. 1*	HTTP	admin	(none)
LINKSYS	BEFSR41 *Rev. 2*	HTTP	(none)	admin
LINKSYS	WRT54G	HTTP	admin	admin
LINKSYS	WAG54G	HTTP	admin	admin
LINKSYS	LINKSYS DSL		n/a	admin
LINKSYS	WAP54G *Rev. 2.0*	HTTP	(none)	admin
LINKSYS	WRT54G *Rev. ALL REVISIONS*	HTTP	(none)	admin
LINKSYS	MODEL WRT54GC COMPACT WIRELESS-G BROADBAND ROUTER	MULTI	(none)	admin
LINKSYS	AG 241 - ADSL2 GATEWAY WITH 4-PORT SWITCH	MULTI	admin	admin
LINKSYS	COMCAST *Rev. COMCAST-SUPPLIED*	HTTP	comcast	1234
LINKSYS	WAG54GS	MULTI	admin	admin
LINKSYS	AP 1120	MULTI	n/a	(none)
LINKSYS	PAP2 / PAP2V2 (VONAGE)	HTTP	admin	admin
LINKSYS	RT31P2 (VONAGE)	HTTP	admin	admin



Internet Setup

Internet Connection Type: Automatic Configuration - DHCP

Optional Settings (required by some Internet Service Providers)

Host Name:

Domain Name: hsd1.pa.comcast.net

MTU: Auto Size: 1500

Network Setup

Router IP

IP Address: 192 . 168 . 1 . 2

Subnet Mask: 255.255.255.0

DHCP Server Setting

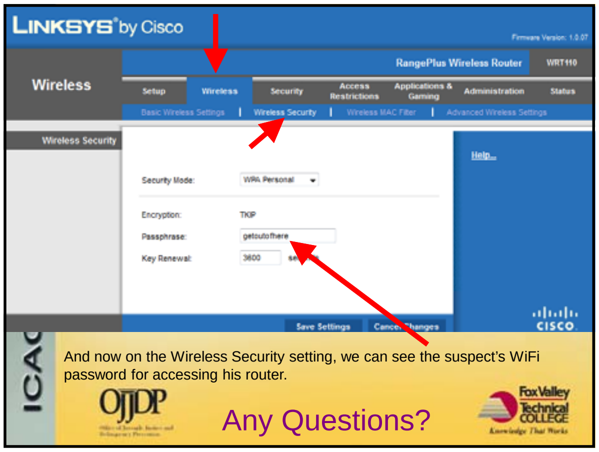
DHCP Server: ● Enabled ○ Disabled

Start IP Address: 192 . 168 . 1 . 101

Maximum Number of Users: 15

IP Address Range: 192 . 168 . 1 . 101 to 115

Client Lease Time: 0 minutes (0 means one day)



Wireless Security

Security Mode: WPA Personal

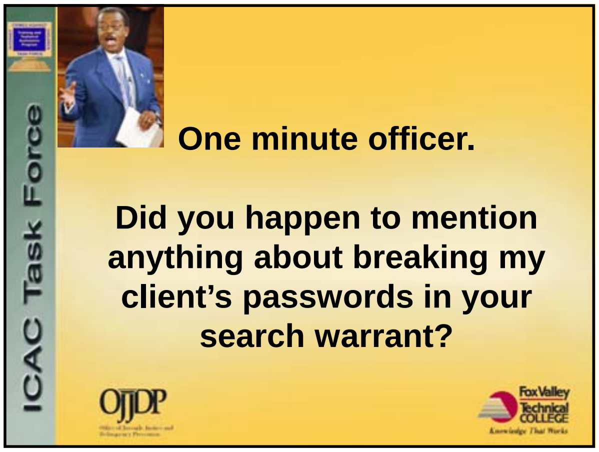
Encryption: TKIP

Passphrase: getoutofhere

Key Renewal: 3600 seconds

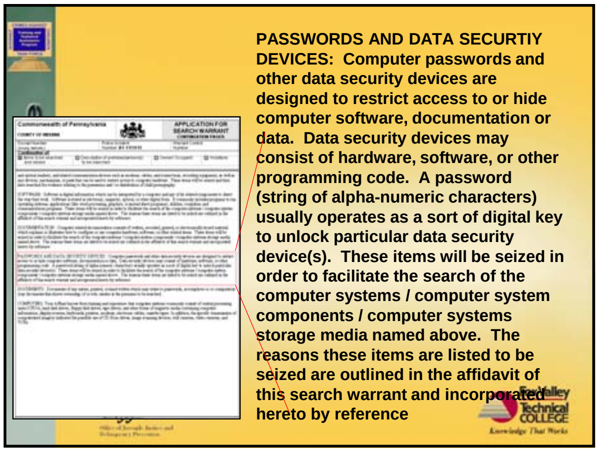
And now on the Wireless Security setting, we can see the suspect's WiFi password for accessing his router.

Any Questions?

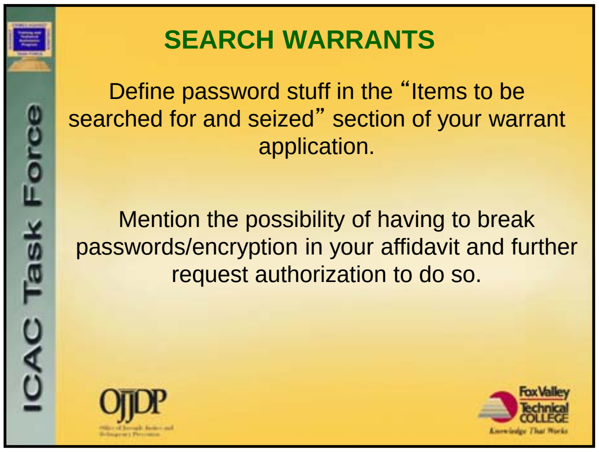


One minute officer.

Did you happen to mention anything about breaking my client’s passwords in your search warrant?


Commonwealth of Pennsylvania
APPLICATION FOR SEARCH WARRANT
Fox Valley Technical College
Knowledge That Works

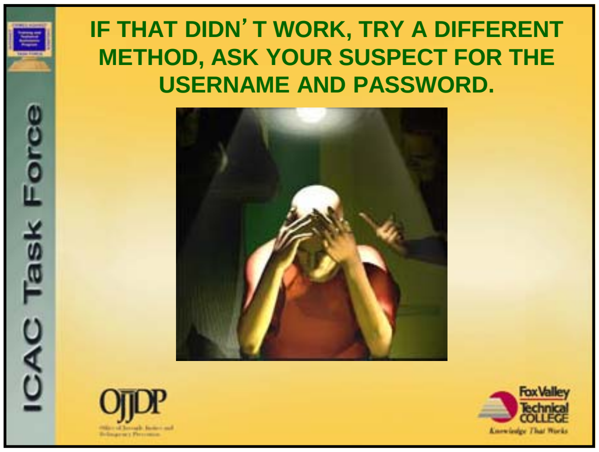
PASSWORDS AND DATA SECURTIY DEVICES: Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation or data. Data security devices may consist of hardware, software, or other programming code. A password (string of alpha-numeric characters) usually operates as a sort of digital key to unlock particular data security device(s). These items will be seized in order to facilitate the search of the computer systems / computer system components / computer systems storage media named above. The reasons these items are listed to be seized are outlined in the affidavit of this search warrant and incorporated hereto by reference



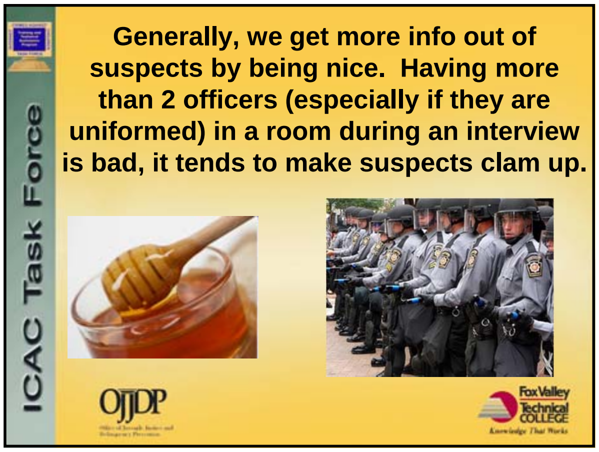
SEARCH WARRANTS

Define password stuff in the “Items to be searched for and seized” section of your warrant application.

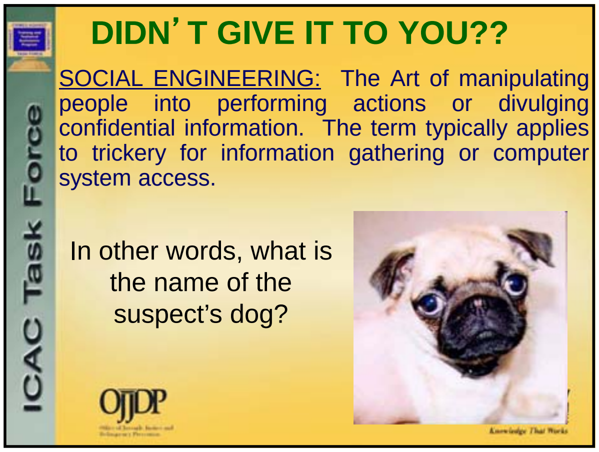
Mention the possibility of having to break passwords/encryption in your affidavit and further request authorization to do so.



IF THAT DIDN'T WORK, TRY A DIFFERENT METHOD, ASK YOUR SUSPECT FOR THE USERNAME AND PASSWORD.



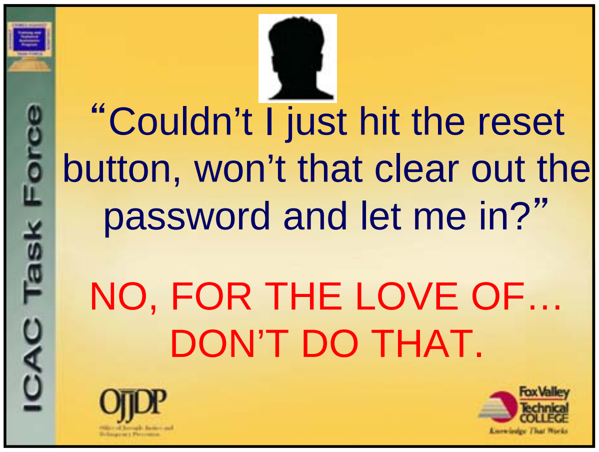
Generally, we get more info out of suspects by being nice. Having more than 2 officers (especially if they are uniformed) in a room during an interview is bad, it tends to make suspects clam up.



DIDN'T GIVE IT TO YOU??

SOCIAL ENGINEERING: The Art of manipulating people into performing actions or divulging confidential information. The term typically applies to trickery for information gathering or computer system access.

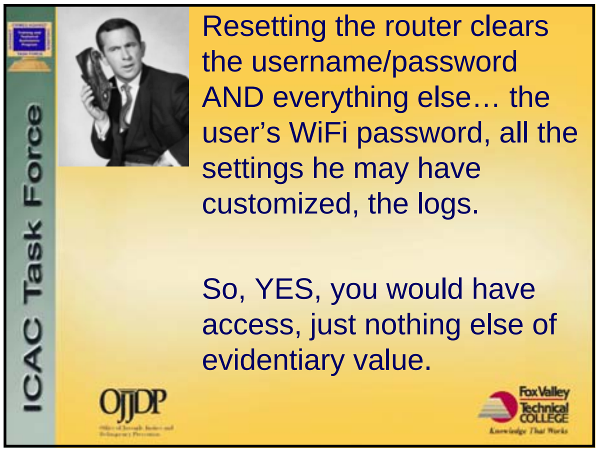
In other words, what is the name of the suspect's dog?



ICAC Task Force

“Couldn’t I just hit the reset button, won’t that clear out the password and let me in?”

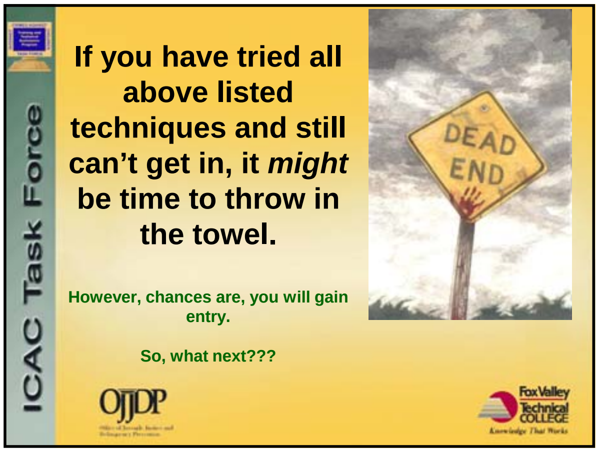
NO, FOR THE LOVE OF… DON’T DO THAT.



ICAC Task Force

Resetting the router clears the username/password AND everything else… the user’s WiFi password, all the settings he may have customized, the logs.

So, YES, you would have access, just nothing else of evidentiary value.



ICAC Task Force

If you have tried all above listed techniques and still can’t get in, it *might* be time to throw in the towel.

However, chances are, you will gain entry.

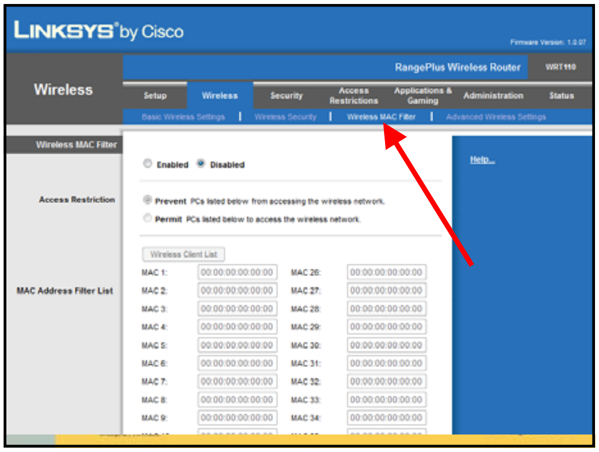
So, what next???

ICAC Task Force

DHCP lease tables, router logs, MAC filter lists and the like are a treasure trove of important information, let' s examine its contents…

Any Questions?

Poll Questions # 4 & 5



Wireless MAC Filter

○ Enabled ● Disabled

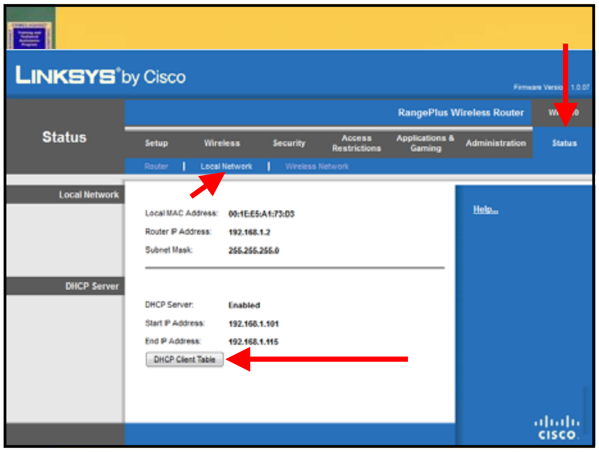
Access Restriction

● Prevent PCs listed below from accessing the wireless network.

○ Permit PCs listed below to access the wireless network.

MAC Address Filter List

MAC 1:	00:00:00:00:00:00	MAC 26:	00:00:00:00:00:00
MAC 2:	00:00:00:00:00:00	MAC 27:	00:00:00:00:00:00
MAC 3:	00:00:00:00:00:00	MAC 28:	00:00:00:00:00:00
MAC 4:	00:00:00:00:00:00	MAC 29:	00:00:00:00:00:00
MAC 5:	00:00:00:00:00:00	MAC 30:	00:00:00:00:00:00
MAC 6:	00:00:00:00:00:00	MAC 31:	00:00:00:00:00:00
MAC 7:	00:00:00:00:00:00	MAC 32:	00:00:00:00:00:00
MAC 8:	00:00:00:00:00:00	MAC 33:	00:00:00:00:00:00
MAC 9:	00:00:00:00:00:00	MAC 34:	00:00:00:00:00:00



Local Network

Local MAC Address: 00:1E:E5:A1:73:D3

Router IP Address: 192.168.1.2

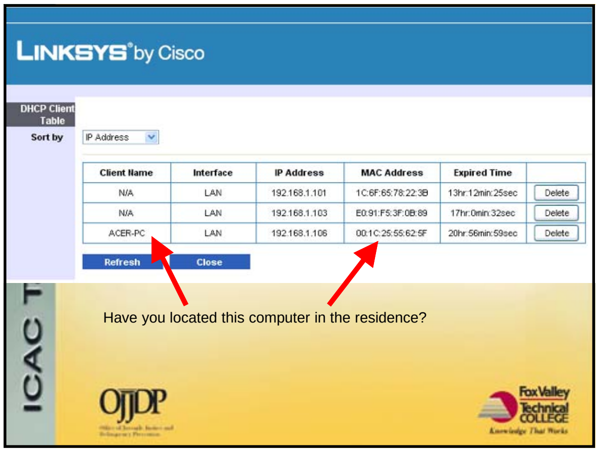
Subnet Mask: 255.255.255.0

DHCP Server

DHCP Server: Enabled

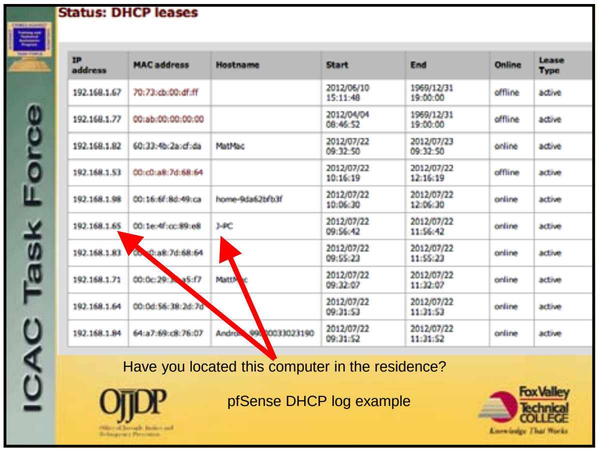
Start IP Address: 192.168.1.101

End IP Address: 192.168.1.115



Client Name	Interface	IP Address	MAC Address	Expired Time	
N/A	LAN	192.168.1.101	1C:6F:65:78:22:3B	13hr:12min:25sec	Delete
N/A	LAN	192.168.1.103	E0:91:F5:3F:0B:89	17hr:0min:32sec	Delete
ACER-PC	LAN	192.168.1.106	00:1C:25:55:62:5F	20hr:56min:59sec	Delete

Have you located this computer in the residence?

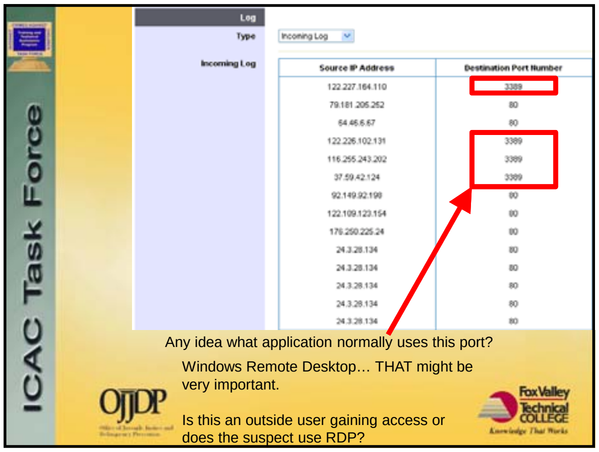


Status: DHCP leases

IP address	MAC address	Hostname	Start	End	Online	Lease Type
192.168.1.67	70:73:cb:00:df:ff		2012/06/10 15:11:48	1969/12/31 19:00:00	offline	active
192.168.1.77	00:ab:00:00:00:00		2012/04/04 08:46:52	1969/12/31 19:00:00	offline	active
192.168.1.82	60:33:4b:2a:cf:da	MatMac	2012/07/22 09:32:50	2012/07/23 09:32:50	online	active
192.168.1.53	00:c0:a8:7d:68:64		2012/07/22 10:16:19	2012/07/22 12:16:19	offline	active
192.168.1.98	00:16:6f:8d:49:ca	home-9da62bfb3f	2012/07/22 10:06:30	2012/07/22 12:06:30	online	active
192.168.1.65	00:1e:4f:cc:89:e8	J-PC	2012/07/22 09:56:42	2012/07/22 11:56:42	online	active
192.168.1.83	00:c0:a8:7d:68:64		2012/07/22 09:55:23	2012/07/22 11:55:23	online	active
192.168.1.71	00:0c:29:[illegible]:a5:f7	MattMac	2012/07/22 09:32:07	2012/07/22 11:32:07	online	active
192.168.1.64	00:0d:56:38:2d:7d		2012/07/22 09:31:53	2012/07/22 11:31:53	online	active
192.168.1.84	64:a7:69:c8:76:07	Android_99[illegible]0033023190	2012/07/22 09:31:52	2012/07/22 11:31:52	online	active

Have you located this computer in the residence?

pfSense DHCP log example

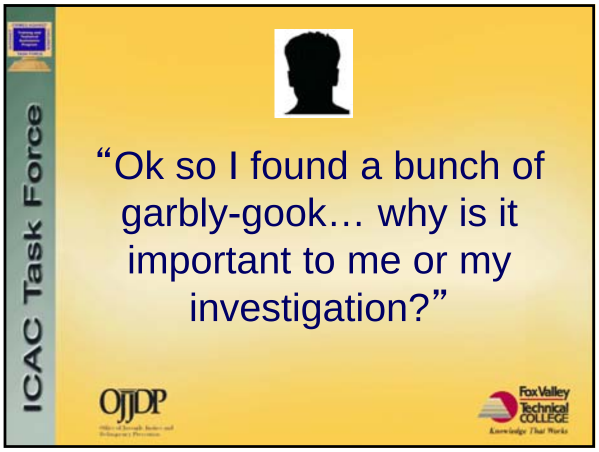


Source IP Address	Destination Port Number
122.227.164.110	3389
79.181.205.252	80
64.46.6.67	80
122.226.102.131	3389
116.255.243.202	3389
37.59.42.124	3389
92.149.92.198	80
122.109.123.154	80
178.250.225.24	80
24.3.28.134	80
24.3.28.134	80
24.3.28.134	80
24.3.28.134	80
24.3.28.134	80

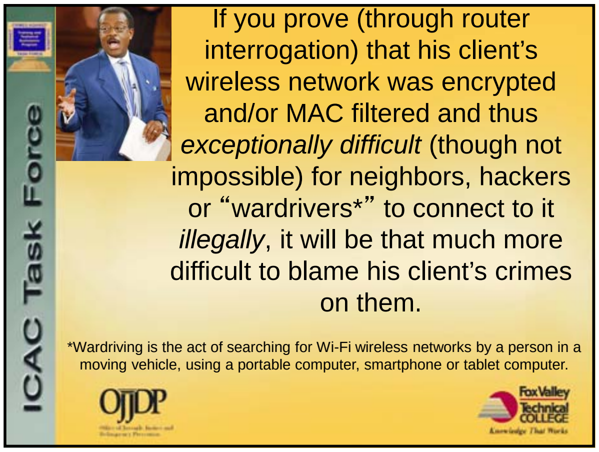
Any idea what application normally uses this port?

Windows Remote Desktop… THAT might be very important.

Is this an outside user gaining access or does the suspect use RDP?

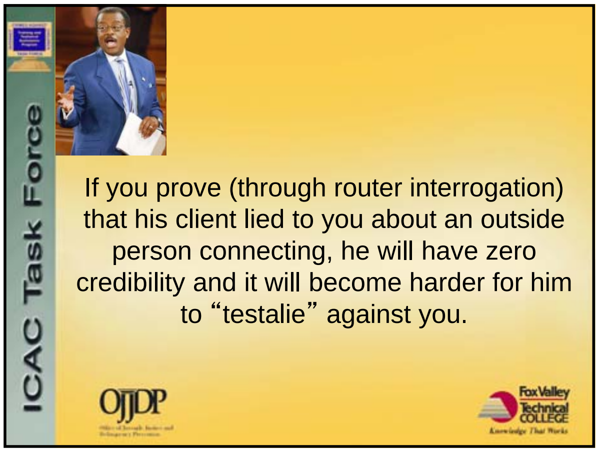

ICAC Task Force

"Ok so I found a bunch of garbly-gook… why is it important to me or my investigation?"

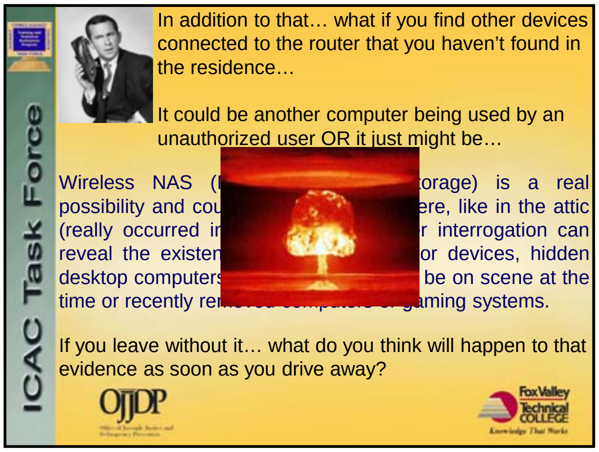

ICAC Task Force

If you prove (through router interrogation) that his client's wireless network was encrypted and/or MAC filtered and thus *exceptionally difficult* (though not impossible) for neighbors, hackers or "wardrivers*" to connect to it *illegally*, it will be that much more difficult to blame his client's crimes on them.

*Wardriving is the act of searching for Wi-Fi wireless networks by a person in a moving vehicle, using a portable computer, smartphone or tablet computer.


ICAC Task Force

If you prove (through router interrogation) that his client lied to you about an outside person connecting, he will have zero credibility and it will become harder for him to "testalie" against you.

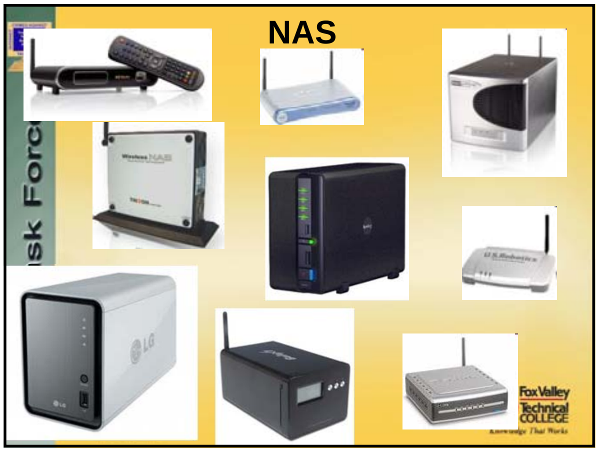

ICAC Task Force
OJJDP
Fox Valley Technical College
Knowledge That Works

In addition to that… what if you find other devices connected to the router that you haven't found in the residence…

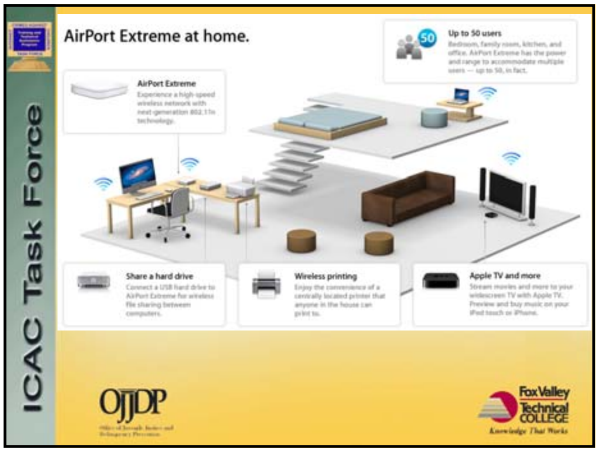
It could be another computer being used by an unauthorized user OR it just might be…

Wireless NAS (
torage) is a real
possibility and cou
ere, like in the attic
(really occurred in
r interrogation can
reveal the existen
or devices, hidden
desktop computers
be on scene at the
time or recently re
gaming systems.

If you leave without it… what do you think will happen to that evidence as soon as you drive away?



NAS



AirPort Extreme at home.

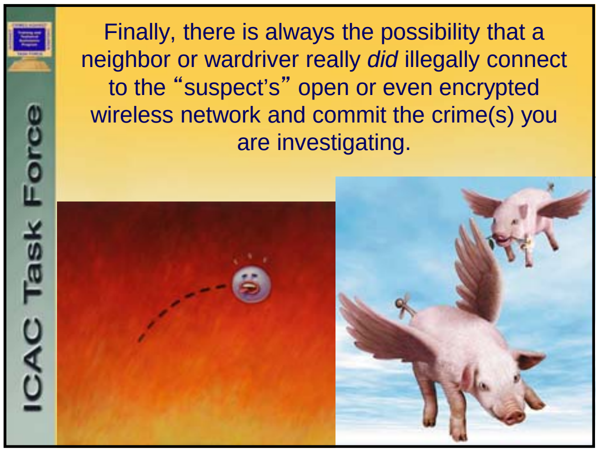
Up to 50 users
Bedroom, family room, kitchen, and office. AirPort Extreme has the power and range to accommodate multiple users — up to 50, in fact.

AirPort Extreme
Experience a high-speed wireless network with next-generation 802.11n technology.

Share a hard drive
Connect a USB hard drive to AirPort Extreme for wireless file sharing between computers.

Wireless printing
Enjoy the convenience of a centrally located printer that anyone in the house can print to.

Apple TV and more
Stream movies and more to your widescreen TV with Apple TV. Preview and buy music on your iPod touch or iPhone.



Finally, there is always the possibility that a neighbor or wardriver really *did* illegally connect to the “suspect’s” open or even encrypted wireless network and commit the crime(s) you are investigating.

OTHER DECENT TOOLS

Directional Antennas

WiFi Detectors

and probably the most widely used these days… the iPhone or an Android phone – using apps like Fing, WiFi Radar, WiFi Analyzer, etc…

Ponch and I are now open for any last questions you may have.