**Lab 6 Name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**MCSE 1 DNS Name Resolution**

**Objective:**

In this lab you will:

- configure the client to use a DNS server

- use Wireshark to observe the DNS traffic

- access DNS cache

- configure the hosts file

**Procedure:**

\_\_\_ Start Hamilton (Windows 8) and Calgary (Server 2008 R2). Log into the Administrator’s account on each computer.

We want Calgary to be a domain controller. A server becomes a domain

controller when you add Active Directory to the server. The next part of the lab

will step you through the process of adding Active Directory.

**Calgary:**

\_\_\_ Click on **Start** and **Run**. Type **dcpromo**.

**Dcpromo** stands for **D**omain **C**ontroller **promo**tion.

The following screen shots will help you make the correct choices:

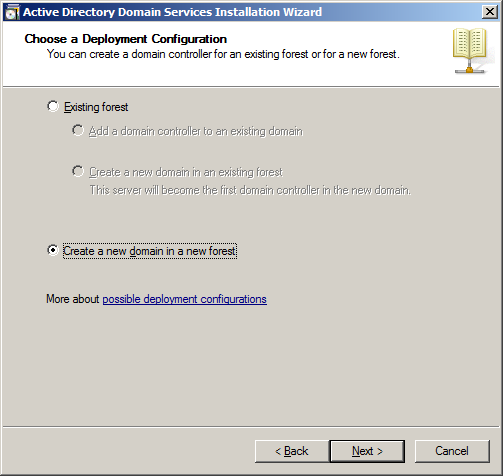


Fig. 1 Creating a domain controller

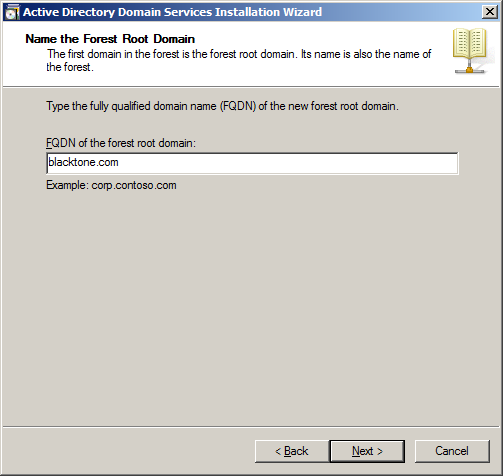


Fig. 2 The forest root domain is **blacktone.com**

\_\_\_ On the NetBIOS name page, click **Next** to accept the default.

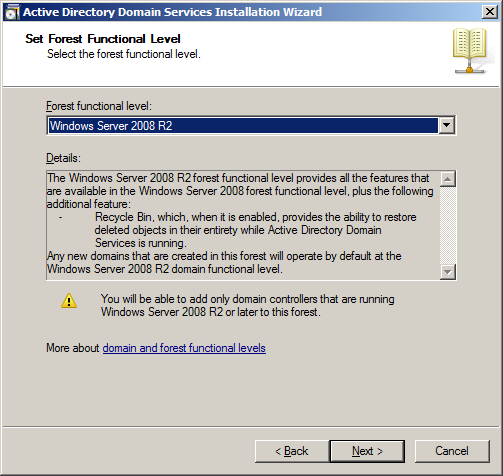
****

Fig. 3 Set the Forest Functional level to **Windows Server 2008 R2**

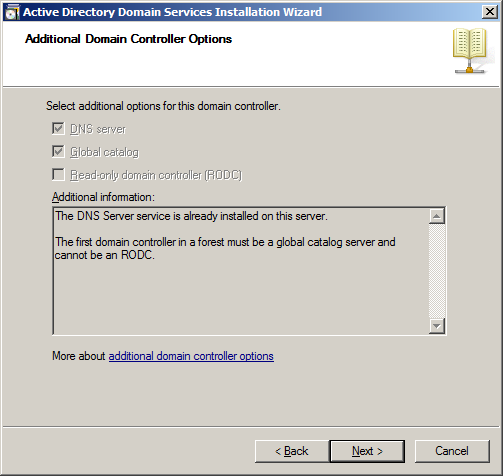


Fig. 4 Accept the default for DNS and Global Catalog

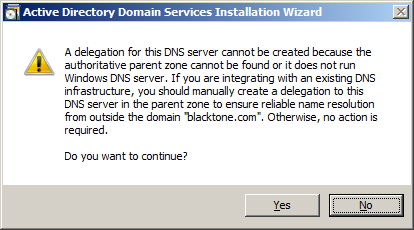


Fig. 5 click on “Yes”

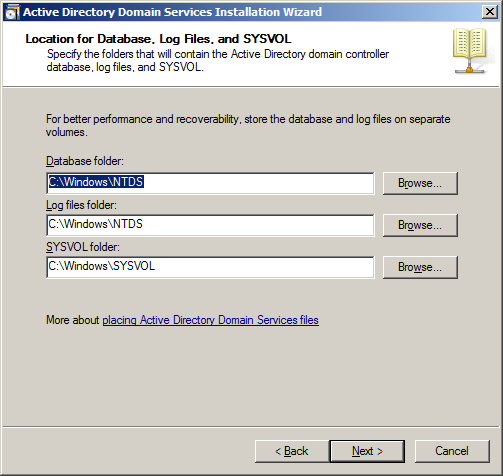


Fig. 6 Accept the defaults

\_\_\_ Use the password **P@ssw0rd**.

\_\_\_ On the **Summary**  page click on **Next**.

\_\_\_ Click on **Finish**.

\_\_\_ While Active Directory is installing, make sure you can ping by IP address between Hamilton and Calgary.

\_\_\_ Restart Calgary when Active Directory installation finishes.

**Hamilton:**

\_\_\_ Open the properties page of the NIC on Hamilton and configure the preferred DNS server so it points to Calgary.

**1. Capture the NIC property page on Hamilton showing that you have configured Calgary as the preferred DNS server.**

\_\_\_ Clear the DNS cache on Hamilton by typing **ipconfig /flushdns**.

\_\_\_ Clear the DOS window by typing **cls**.

\_\_\_ Display the DNS cache on Hamilton. To do this type

**ipconfig /displaydns**.

**2. Capture the display of the DNS cache on Hamilton.**

\_\_\_ Start Wireshark on Hamilton.

If the Wireshark display looks like figure 7, turn off Windows updates on Hamilton. To turn off Windows updates, follow these steps:

\_\_\_ From the Windows 8 Start screen, type **control panel**.

\_\_\_ Click on **System and Security**.

\_\_\_ Click on **Windows Update**.

\_\_\_ On the left-hand side, click on **Change Settings**.

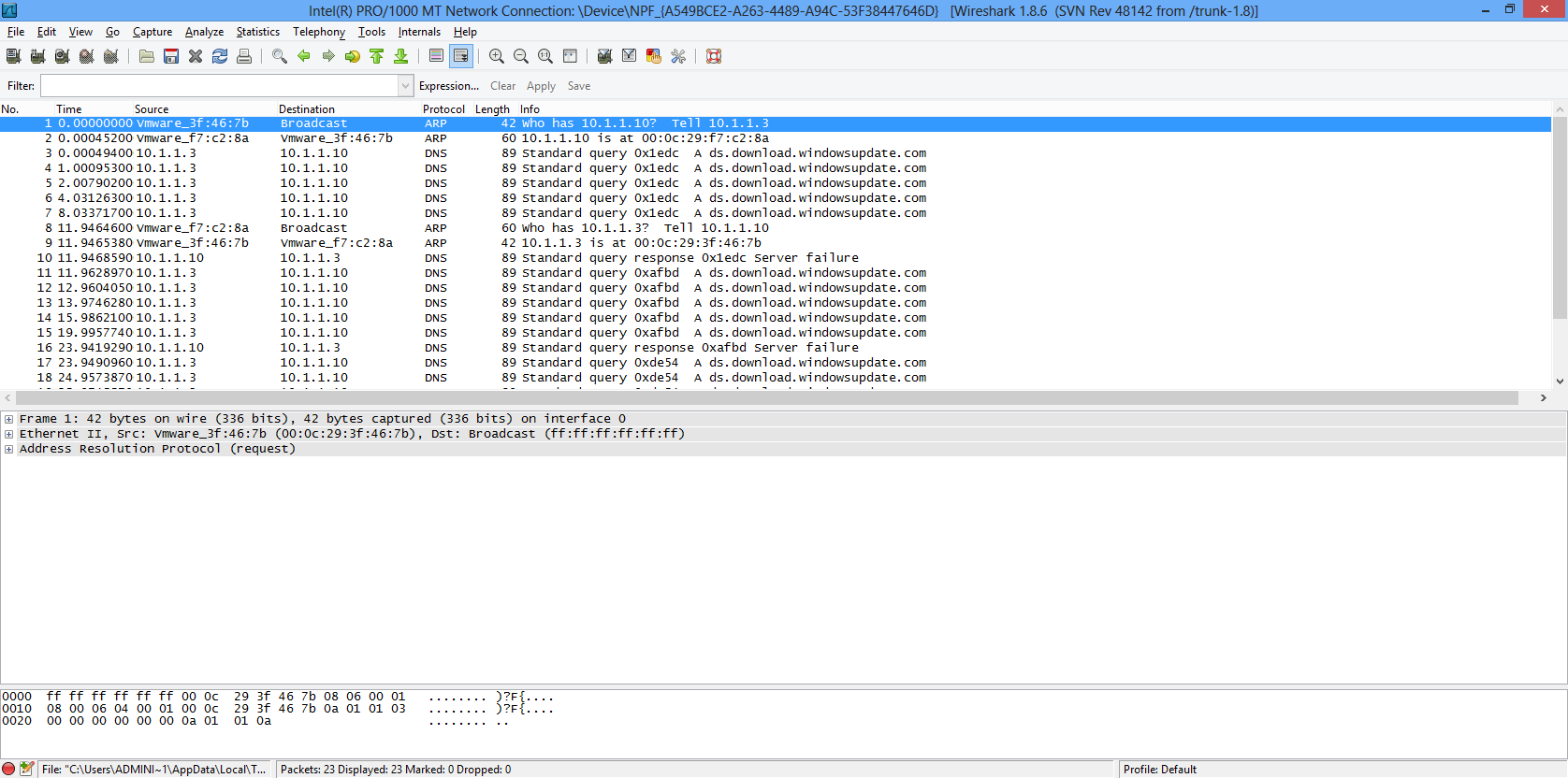


Fig. 7 Wireshark displays a lot of annoying standard query frames Windows update

\_\_\_ Make the selections shown in figure 8, to turn off Windows updates. Click on OK and close the Windows update screens.

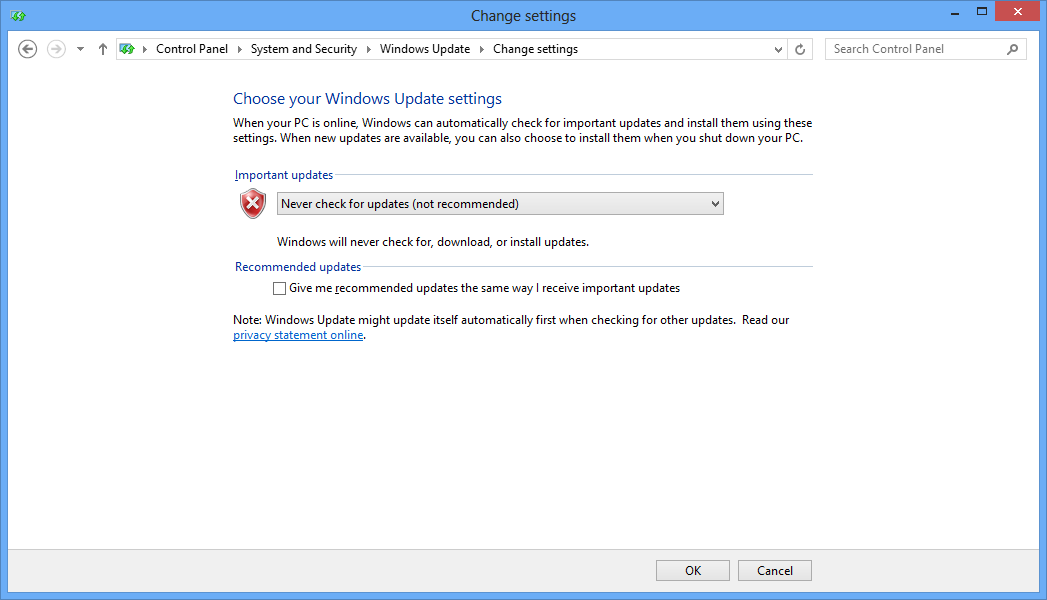


Fig. 8 Turning off Windows updates

\_\_\_ Clear the netbios cache by typing **nbtstat –R**.

\_\_\_ Clear the ARP cache by typing **arp –d \*** .

\_\_\_ Ping Calgary from Hamilton, by typing **ping Calgary**.

\_\_\_ Stop Wireshark when the pings end.

**3. Capture the Wireshark display. It should look like figure 9.**

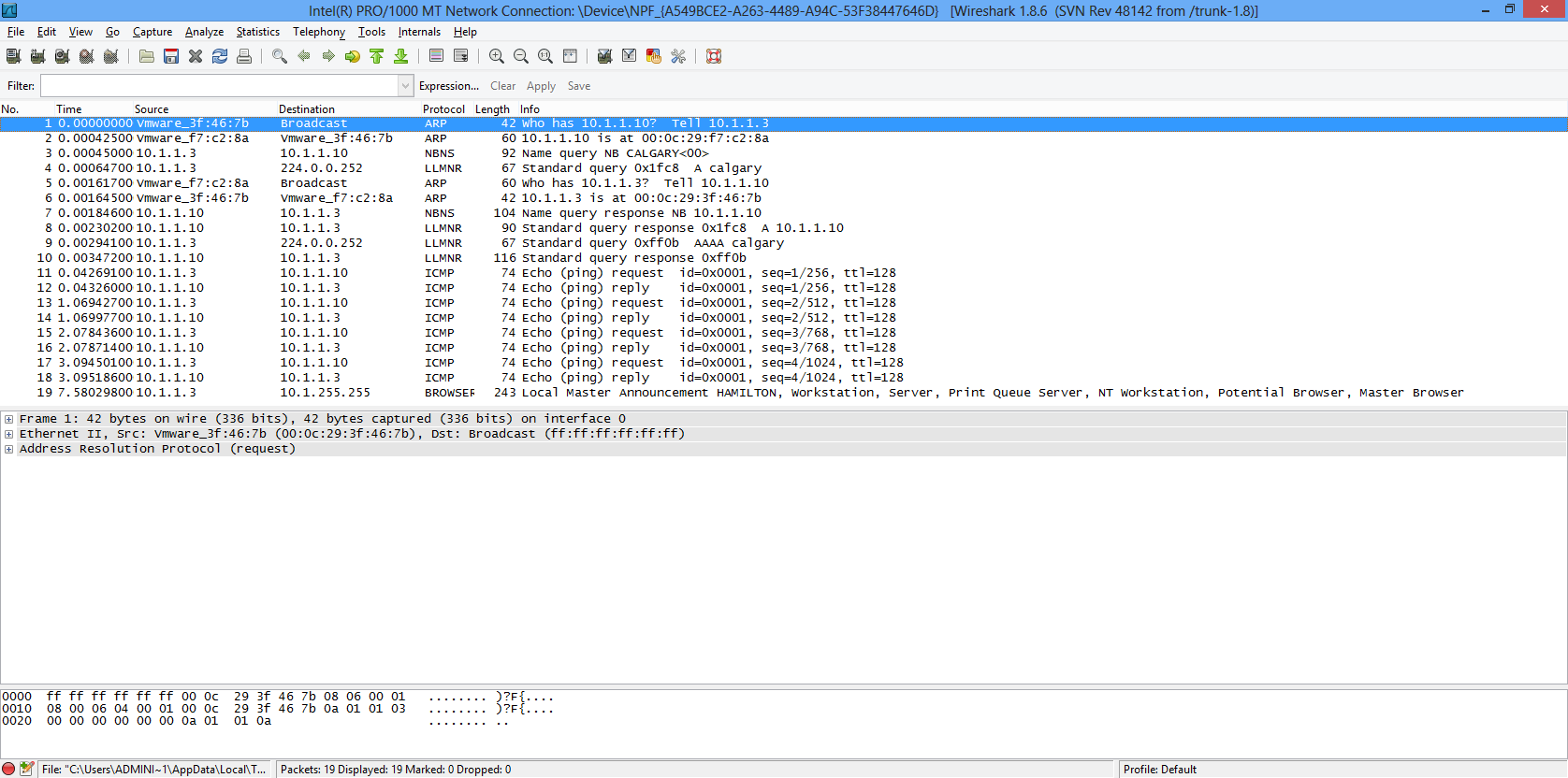


Fig. 9 The results of Hamilton pinging Calgary

Wireshark shows us the name Calgary was resolved by NetBIOS rather than DNS. In frame #3, Hamilton is sending the request for resolution to the WINS server (10.1.1.10) that you configured in the last lab.

The lecture notes say the host should try to send the query to the DNS server before it tries NetBIOS. Why didn’t Hamilton try to use DNS? (Think about it, don’t actual answer the question in your word document).

**client**

**DNS DNS NetBIOS**

**cache server**

Fig. 10 A host tries DNS before it tries NetBIOS

Hamilton is not joined to a domain and it therefore has no DNS suffix to tack on the end of the host name, Calgary. Therefore, Hamilton did not use DNS. Let’s try pinging Calgary with a DNS suffix and see if DNS is used.

\_\_\_ Start a fresh Wireshark capture on Hamilton.

\_\_\_ From Hamilton, ping **Calgary.blacktone.com**.

\_\_\_ Stop Wireshark when the pings end.

**4. Capture the Wireshark display. It should look like figure 11.**

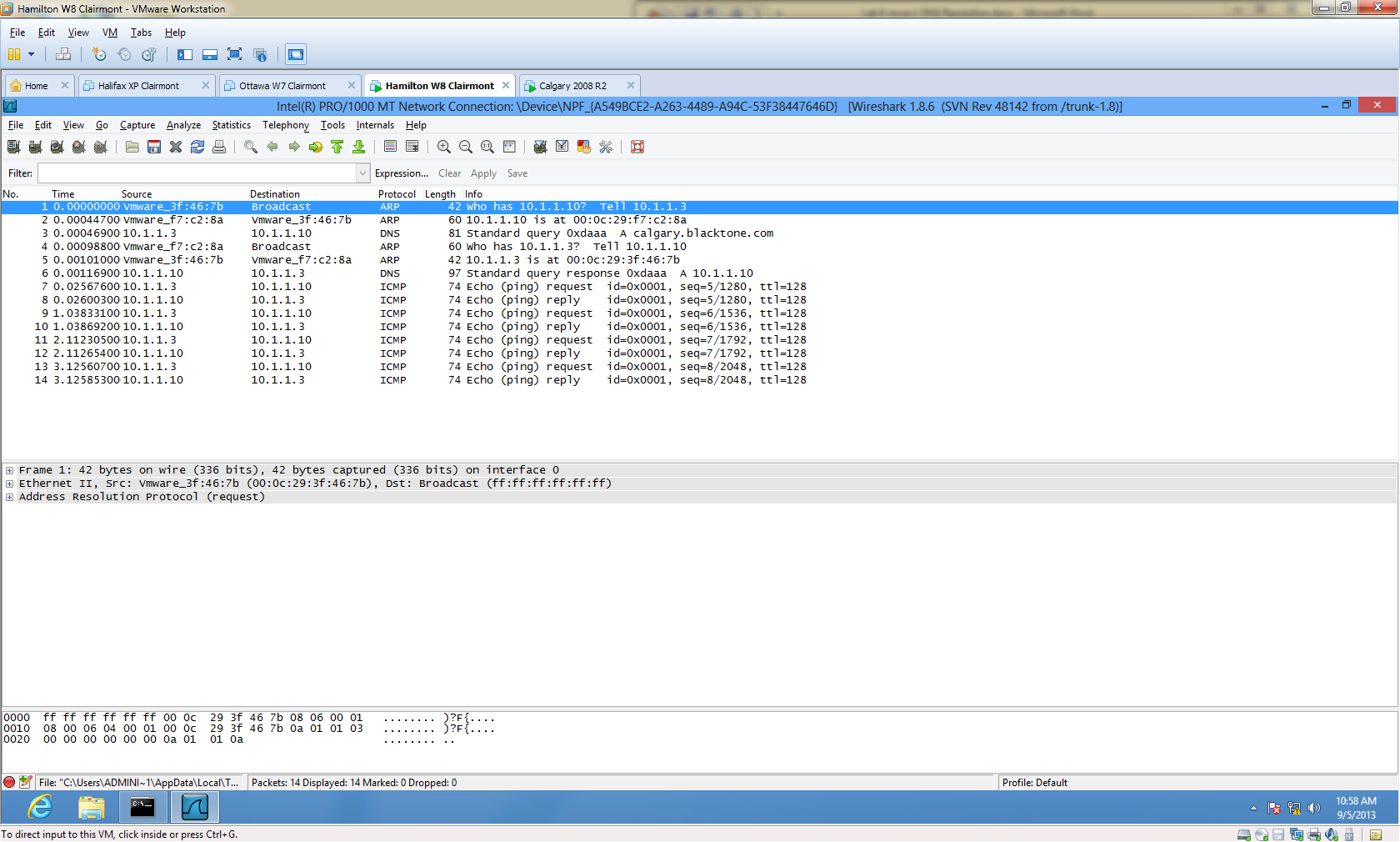


Fig. 11 The results of pinging Calgary.blacktone.com

Figure 11 shows us that this time Hamilton has directed its query to the DNS server as evidenced by frame #3.

\_\_\_ Clear the DOS window and then display the DNS cache on Hamilton.

**5. Capture the DNS cache on Hamilton.**

\_\_\_ From Hamilton, ping **Calgary.blacktone.com**.

\_\_\_ Start a fresh Wireshark capture on Hamilton.

\_\_\_ Ping **Calgary.blacktone.com** again.

\_\_\_ Stop Wireshark when the pings end.

**6. Explain why there is no request to a DNS server or WINS server in the Wireshark display, yet the name has been resolved.**

When you ping a host, it is easy to tell if the name was resolved by DNS or NetBIOS. Figure 12 shows how to recognize the distinction. If the name is resolved by DNS the FQDN (Fully Qualified Domain Name) appears in the first line of the output of the ping command. If NetBIOS resolves the name, only the host name shows up in the output of the ping command.

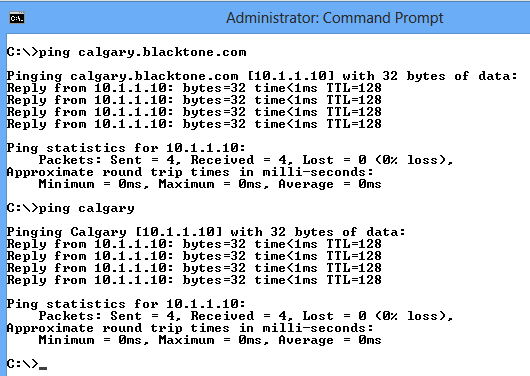


Fig. 12 How to tell whether DNS or NetBIOS did the resolving

Calgary is **Authoritative** for the domain **Blacktone.com**. This means it should contain a DNS record for every host that belongs to the Blacktone.com domain. When the clients turn on, they register themselves with the DNS server in their domain. The DHCP server will have configured the clients with the IP addresses of the DNS servers that they should be using.

If you try to reach a host in the domain and there is no record for it on the DNS server, the Authoritative DNS server sends back a negative cache entry so if you try the same host again the negative cache entry will be found in the DNS cache. The host will not bother sending requests out its NIC since it already knows that host does not exist. This saves bandwidth and CPU cycles.

\_\_\_ Start Wireshark on Hamilton.

\_\_\_ On Hamilton, ping **kalgary.blacktone.com**. Since there is no Kalgary

record, we should get a negative cache entry.

\_\_\_ Stop Wireshark when the pings are done.

**7. Capture the output of Wireshark. It should look like figure 13.**

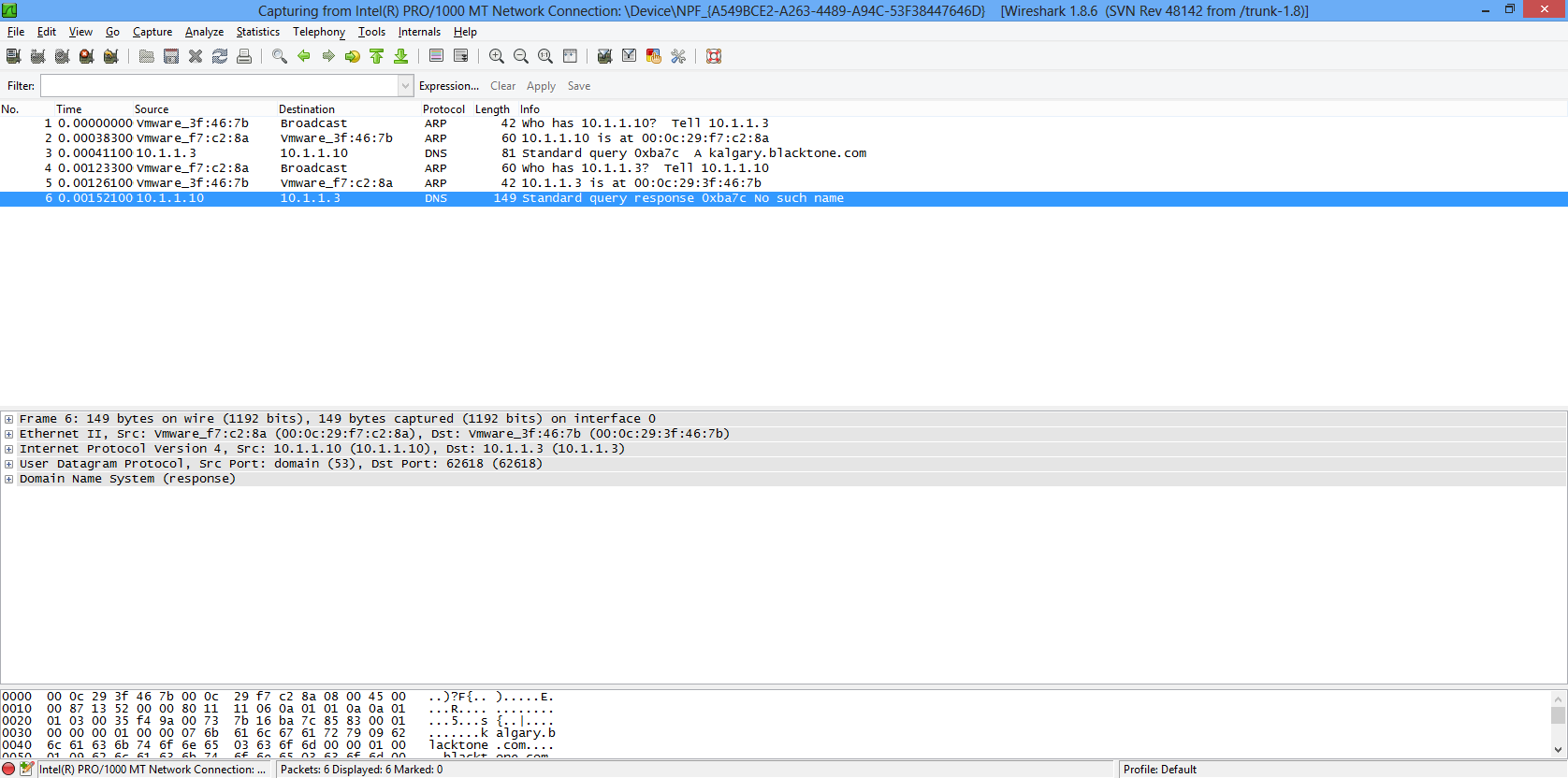


Fig. 13 DNS has been queried but it says the there is “no such name”

\_\_\_ Display the DNS cache on Hamilton. You should have a negative cache entry for Kalgary.Blacktone.com.

**8. Capture the DNS cache on Hamilton showing the negative cache entry.**

\_\_\_ Start Wireshark on Hamilton.

\_\_\_ On Hamilton, ping **kalgary.blacktone.com** again.

.

\_\_\_ Stop Wireshark when the pings are done.

**9. Explain why there are no frames in Wireshark, this time. (You may get some IPv6 and other frames showing up but none of the frames have anything to do with the ping).**

It is good practice to have multiple DNS servers for redundancy and load balancing. If one DNS server goes down the alternate DNS server will be tried.

Let’s assume we have a preferred DNS server at 10.1.1.250. Calgary at 10.1.1.10 will become our alternate DNS server. We will point Hamilton to 10.1.1.250 as the preferred DNS server. This server does not exist which is the same thing as saying the server failed. When Hamilton does not get a response from the preferred DNS server, it should try the alternate DNS server.

\_\_\_ Configure the NIC on Hamilton so 10.1.1.250 is the preferred DNS server and 10.1.1.10 is the alternate DNS server.

\_\_\_ Type **ipconfig /all** to display the changes.

**10. Capture the output of the ipconfig /all display showing the two DNS server addresses.**

\_\_\_ Start Wireshark on Hamilton.

\_\_\_ On Hamilton, ping **calgary.blacktone.com** again.

.

\_\_\_ Stop Wireshark when the pings are done.

**11. Capture the output of the Wireshark program. Your display should look like figure 14.**

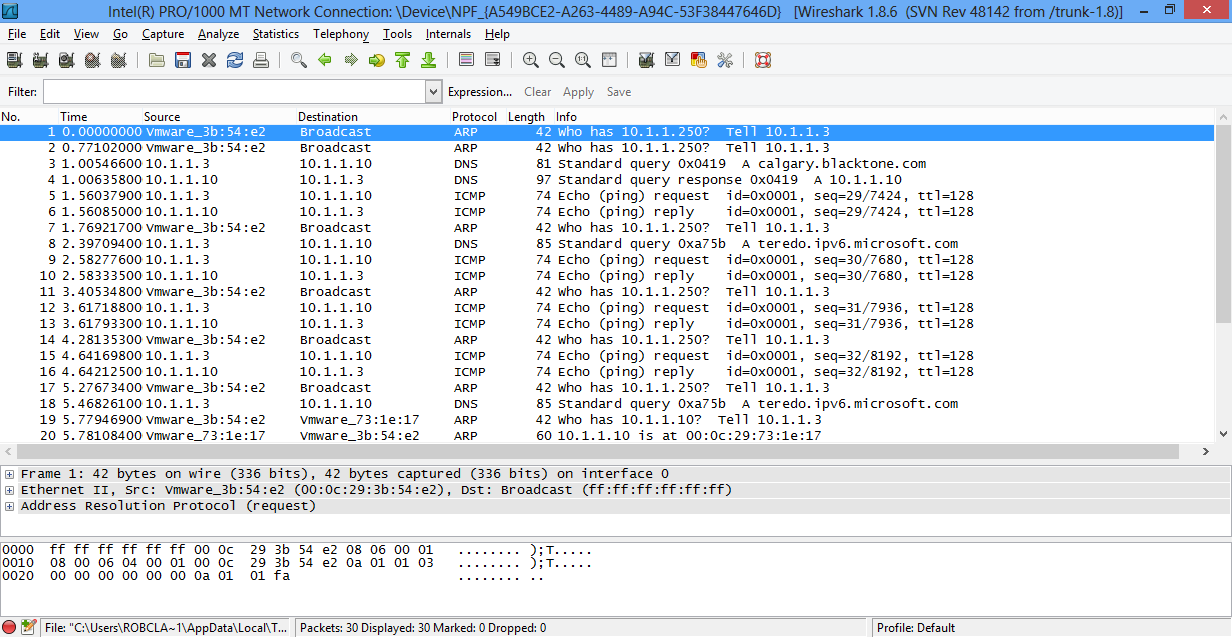


Fig. 14 Both the preferred and alternate DNS servers where tried to resolve the name.

In figure 14, you can see in frame #1 and frame #2 are ARPs sent by Hamilton to obtain the MAC address of the preferred DNS server at 10.1.1.250. Since the preferred DNS server did not reply, Hamilton tried the alternate DNS server as evidenced by frame #3.

\_\_\_ Configure Hamilton’s NIC so the preferred DNS server is Calgary and there is no alternate DNS server.

**Hosts file**

If you have sites that you frequently go to, you can configure the hosts file with

static entries for these popular sites. The advantage here is, every time you

reference one of the sites, the host will find a mapping in its DNS cache. This

saves, bandwidth and CPU cycles.

\_\_\_ Click on the Windows key to get to the Start window.

\_\_\_ Type **Notepad**. Click on **File** and **Open**. Locate the hosts file and open it in NotePad. Display all Files (\*.\*) and click on the **hosts** file to open it.

\_\_\_ Add the following line to the bottom of the file:

**157.16.178.9** [**www.youtube.com**](http://www.youtube.com)

**12. Capture the contents of the hosts file on Hamilton.**

\_\_\_ Save the file.

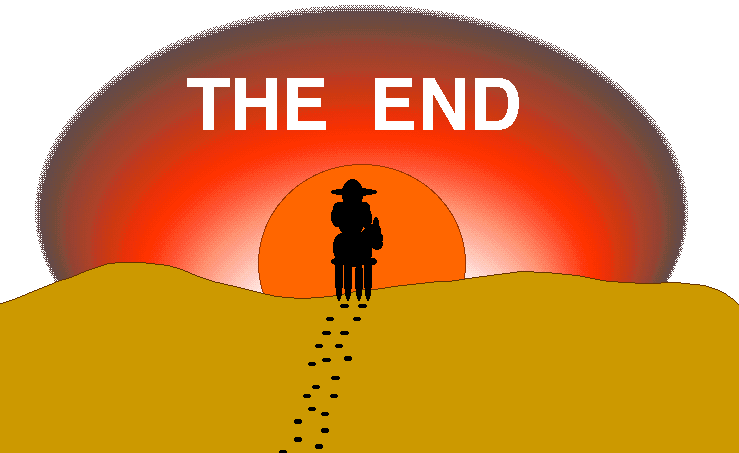
\_\_\_ Display the DNS cache on Hamilton. You should have an entry for youtube.

**13. Capture the contents of the DNS cache on Hamilton.**

\_\_\_ On Hamilton, ping www.youtube.com. The pings will not be successful since we can’t reach that network, but the name will be translated into its IP address.

\_\_\_ Remove the entry from the hosts file on Hamilton.

**14. Capture the contents of the DNS cache on Hamilton showing there are no entries.**

[](http://www.google.ca/url?sa=i&rct=j&q=&esrc=s&frm=1&source=images&cd=&cad=rja&docid=CT2JBoY4djRxNM&tbnid=V3ZA-eAnrfZbXM:&ved=0CAUQjRw&url=http://gridironglamourgirl.wordpress.com/2010/11/09/this-cowboy-is-riding-off-into-the-sunset-finally/&ei=TTqRUafiO8TerAGVjoD4Bw&bvm=bv.46340616,d.aWc&psig=AFQjCNF5DpaJMX76U8fEzxhiwLiBYC6NAQ&ust=1368558450220005)