

Assignment - A Deeper Look at DNS

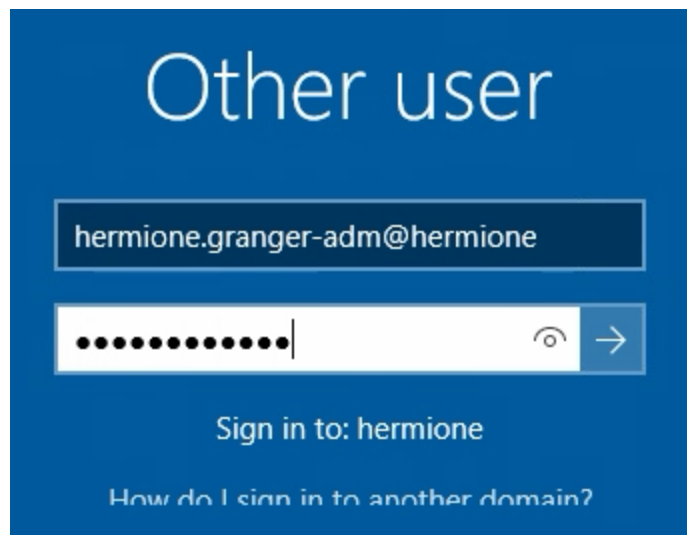
💡 Networking is key to systems administration. In your previous classes (Network Fundamentals), you should have learned a bit about how DNS works and had the opportunity to use Wireshark. These skills should be part of your systems administration toolkit. It's hard to debug a networking problem if you don't know what is going on under the hood.

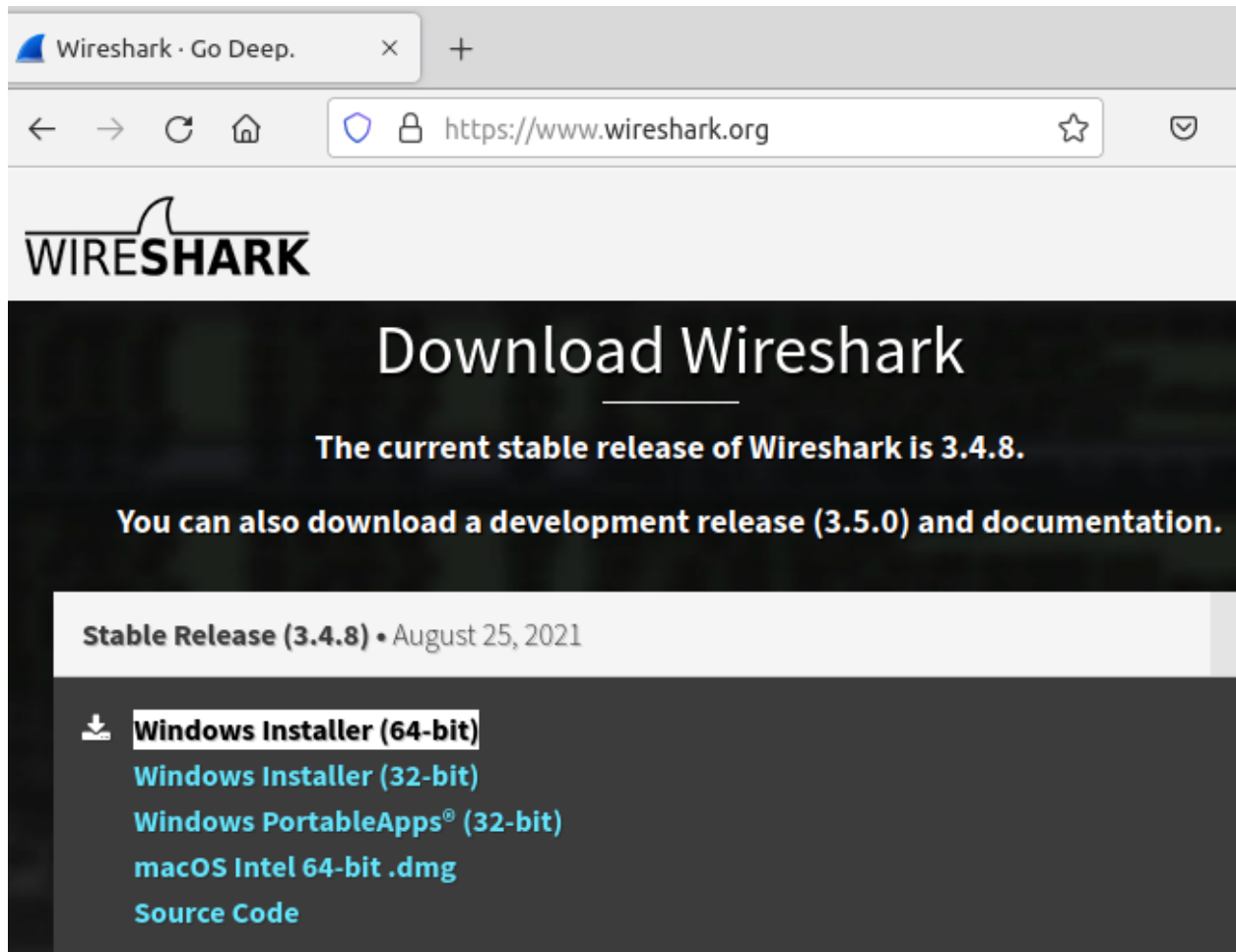
DNS problems are the root of many systems administration challenges. You may have experienced this when trying to join WKS01 to the domain.

If you've forgotten some of these techniques, some self study will be required to get on track.

Install Wireshark

Log off and login to wks01 again as a named domain admin user, and install Wireshark on WKS01.





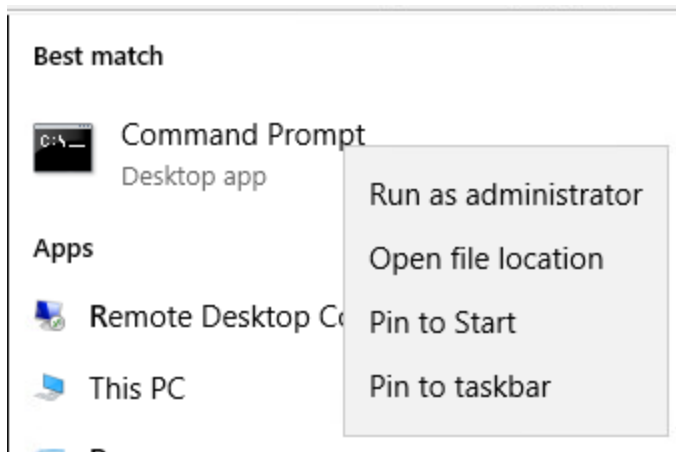
Capture DNS Traffic

1. Open Wireshark

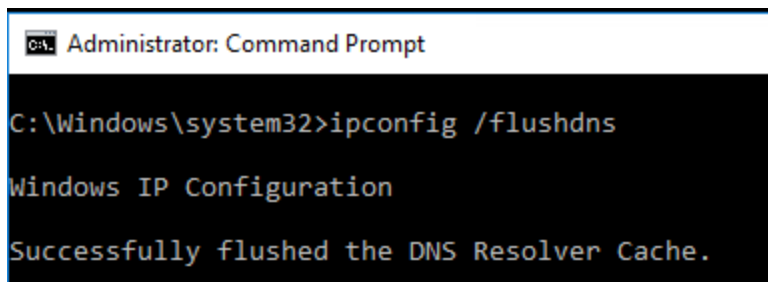


LET US DARE

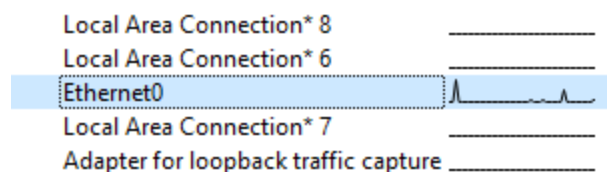
2. Open an elevated command prompt on wks01 (right-click over Command Prompt or Powershell App)



3. Release any Cached DNS records




4. Begin a Capture in Wireshark on Ethernet0
 - Hint: Look for the connection with network activity -



- Use Case 1: Ping a non-existent site (yourname_abc.edu)
- Use Case 2: Ping an existing local host (fw01-yourname)
- Use Case 3: Ping an existing remote site (champlain.edu)

5. Stop and save the Capture.

 Reminder: This is an assignment, so you are on your own for answering the deliverables section.



LET US DARE

Deliverables

1. In your capture, what are the destination IP addresses, ports and protocols for DNS traffic?
2. Perform some basic research. Does DNS ever use a protocol different than the one found in Deliverable 1? If so, why?
3. Figure out how to create a display filter showing only DNS traffic, provide a screenshot that shows at least six DNS packets.
4. For use case 1, what are the authoritative name servers for the .edu top level domain?
5. For use case 1, Provide a screenshot that shows the reply code from your .edu lookup (note this will be part of the flags field)
6. For use case 2, provide a screenshot showing the Answer's section of the DNS response for the fw01-yourname query.
7. For use case 3, what server responds to the dns request for champlain.edu, & is it authoritative?
8. What are the different types of DNS Records? Provide a brief description of each in your own words. There are dozens of DNS record types, so discuss the more common ones (< 10 of them) but more than (CNAME,A,PTR) discussed in class.
9. Your deliverable meets the submission [guidelines](#).



LET US DARE