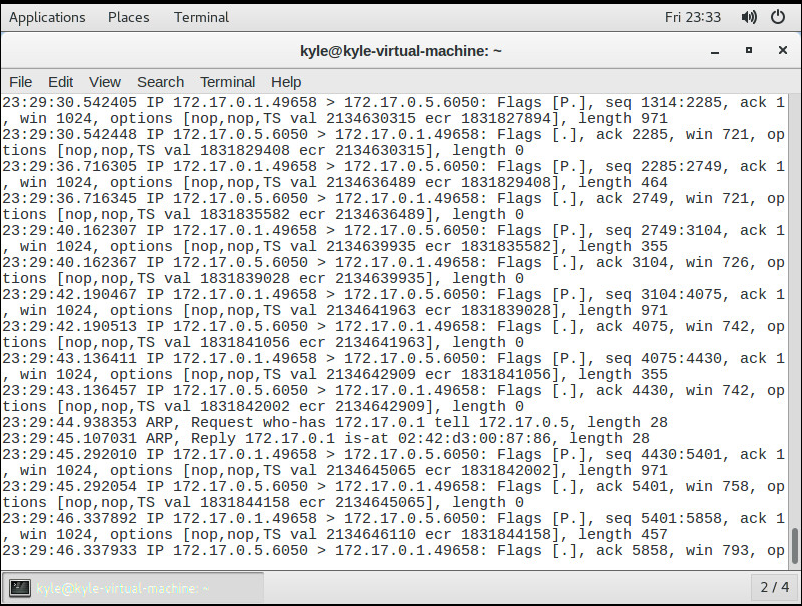
Project 3-1: SO

Kyle M. Stecki

University of Advancing Technology

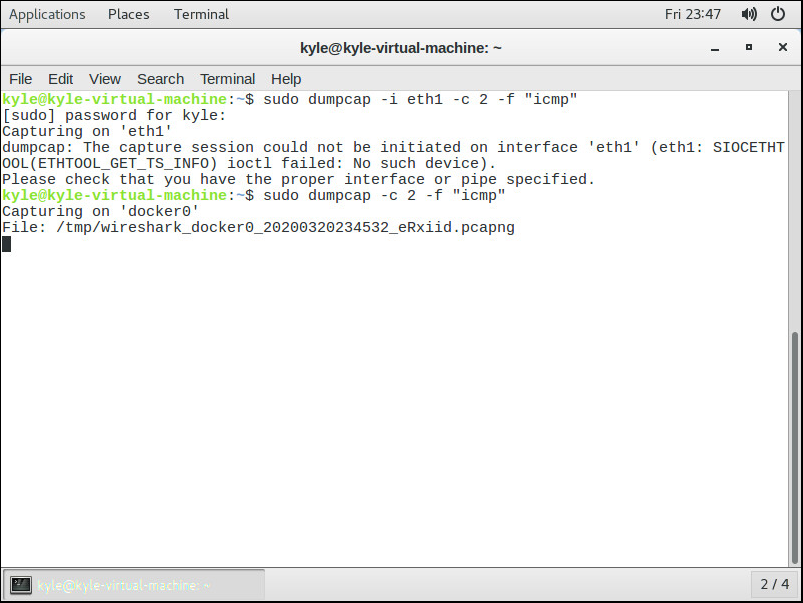
Tcpdump:

Tcpdump is a tool that analyzes network traffic packets with a various amount of features that can be applied to the search. A nice feature of Tcpdump is being able to take that captured traffic and saving it to a file for later review. For my test of the tool I decided to keep it simple and my tests only constricted it down further. I started with ‘tcpdump -n -w -C’ and soon realized I needed to input a file size but didn’t know the parameters in which the size was. I then tried to run just ‘tcpdump -n -w’ without a file setup and with the slowness of the vm over the vpn, in interest of time, I shortened it once again. Finally I got to just ‘tcpdump -n” which finally started to pan out results. This is what I found from the results of the test.

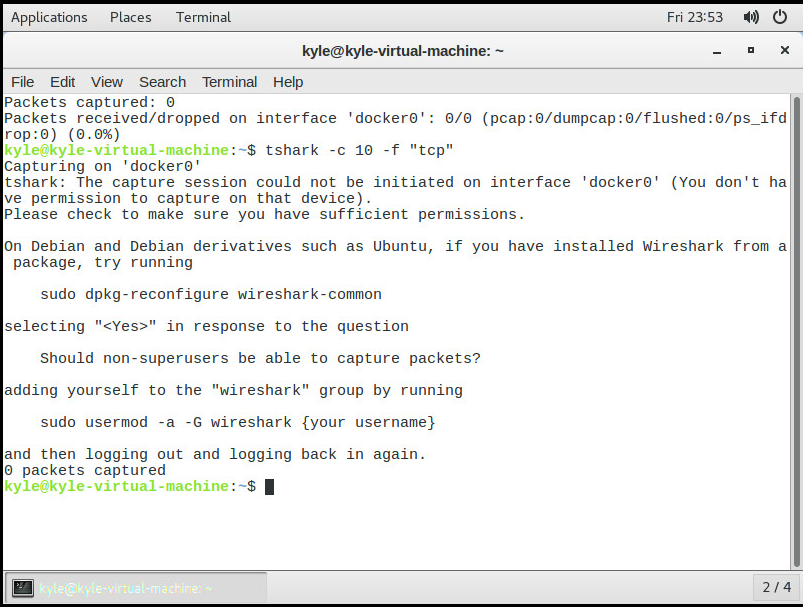


DumpCap and Tshark:

Next is dumpCap and Tshark which further cover more traffic analyzing, with a few differences. For instance, Tshark is a similar product to wireshark, but runs within the CLI and has a strong protocol analysis, with hundreds of protocols that it understands. Both DumpCap and Tshark depend on libpcap traffic capture library to access the packets they are sniffing. Again I had a little trouble with the commands arguments and had to shorten the arguments for DumpCap and used ‘sudo dumpcap -c 2 -f “icmp”’ this capture was for 2 packets of icmp and saved to a file automatically

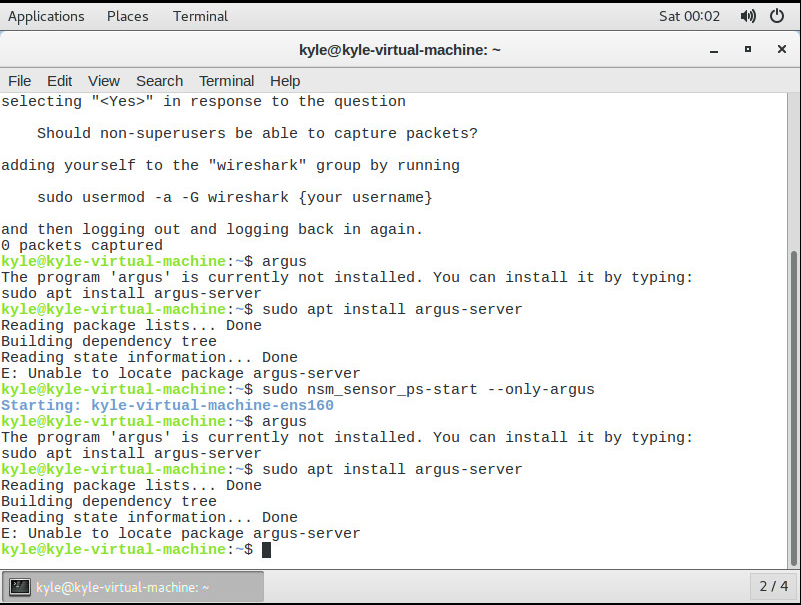


After reviewing Tshark, it really made me realize that I need to learn arguments better and what their parameters would pertain too. I tried to test it with ‘tshark -c 10 -f “tcp”’ with no success because it did not have permission to initiate with docker0. It came back with the following message.



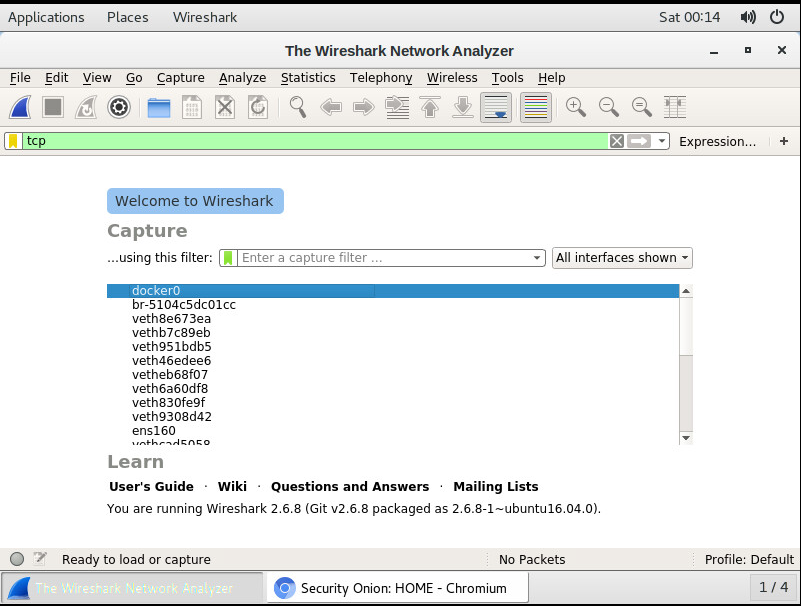
Argus:

Argus is primarily used to analyze session data and is done through the command line. A popular use for it is if you would like to look for specific information or script searches. When trying to use Argus, I got an error that it was not installed (which I had thought it was supposed to be install automatically with setup of SO). I promptly tried to install the apt package through the command line and it came back with a ‘unable to locate the package’ error. I tried the start command from the book and then tried to install the package again with no luck. I’m not sure what I’m doing wrong there, but I was unsuccessful in testing Argus.



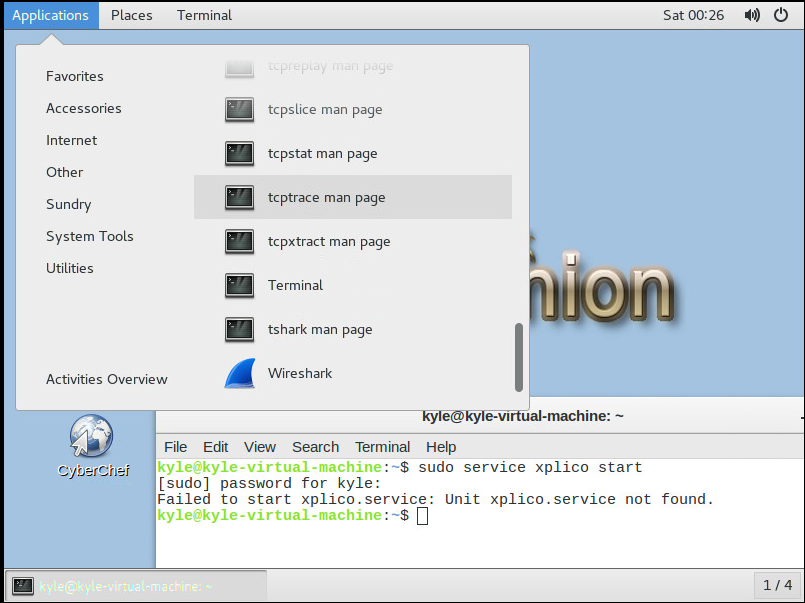
Wireshark:

Wireshark is the tool that we are all the most familiar with, as we have all have some experience with the program and have even had a past assignment to work with the tool. Wireshark is a packet capture tool that gives you many options on how to sort the packets and gives you a some-what friendly UI to work with. Unfortunately, I was pretty unsuccessful with getting a good session going with wireshark as there were so many interfaces to work with and I had no clue which one was actually being used to handle the traffic at that moment, but I have shown in a previous assignment that I can (some-what) work my way around wireshark and I know how it functions and what it is suppose to do. (I’m sorry for the bad work, but I just don’t know the how the network functions with security onion and I fear if I go in and start trying to figure out even the simplest task, I will end up getting lost and messing up any connection I currently have on the vm, here is a screenshot of my attempt to use the program, with the chromium window open as well to try and test the connection)



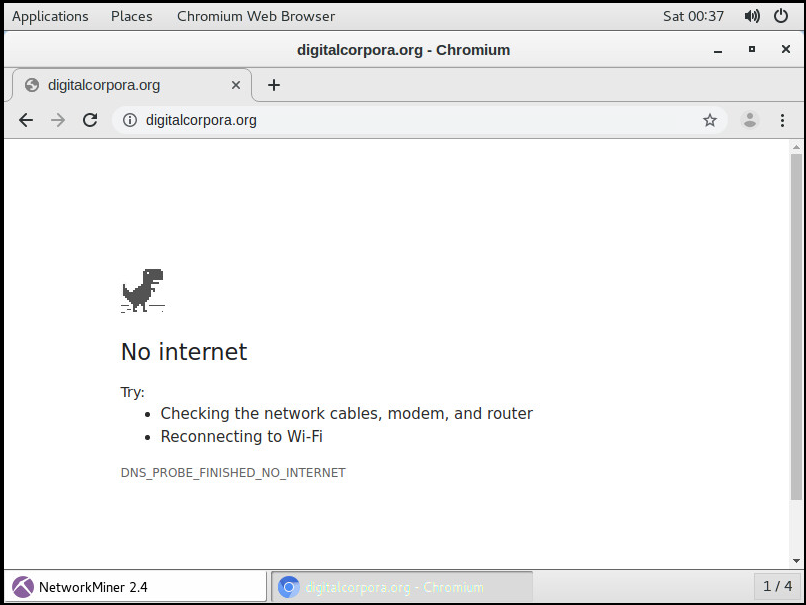
Xplico:

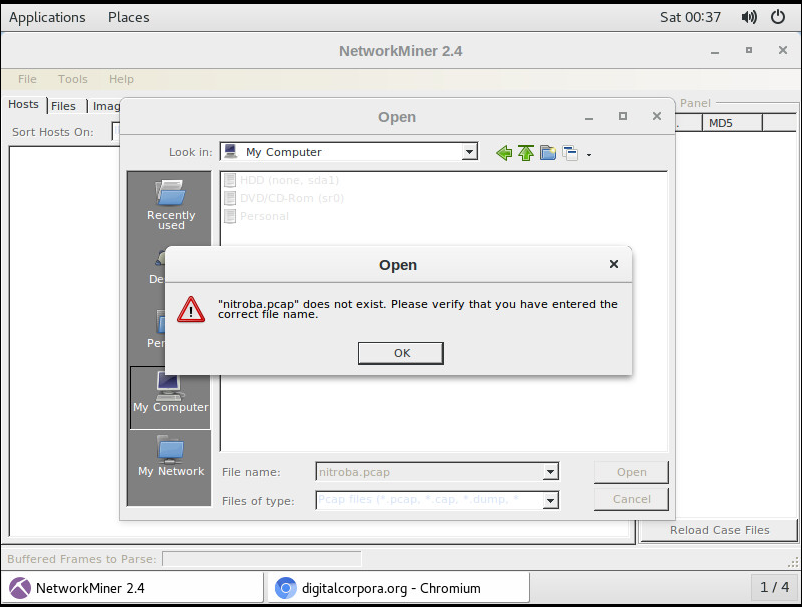
Xplico is a tool typically used against a saved trace file to extract and interpret the content and also can be used to sniff live traffic. As I’ve been doing for the previous tools, i’ve been following the guides in the book to properly try to start and use the tools. After reading through, I tried to start the service and got an error message ‘failed to start xplico.service: unit xplico.service not found’. I fear that my SO installation either went terribly wrong, or I am missing something entirely necessary to completing the installation and being able to properly use the tools. I would really like to get some experience (at least a little bit) as this is the first time being able to work with the product but I do not know how to go further without having the program installed. I searched the files in SO, under the applications tab at the top left of the machine and found nothing pertaining to Xplico. I know I am already late with the assignment and just telling you I can’t do it is not enough for the assignment, but I simply do not know what to do to get the tool running.



Network Miner:

Network Miner is a tool that is used to remote packet capture via Pcap-over-IP. It is another tool to further examine data on a trace file. Once again (I feel like a broken record) I was unable to follow along with the instructions in the book. I went to digitalcorpora.org on the vm and was met by ‘no internet’ error message within chromium. I feel I should know how to diagnose and fix the problem, but SO is just a foreign os to me and with all the different interfaces I just don’t know where to start.





References

For all of the above tools, I tried to follow the procedures given with the class book: The Practice of Network Security Monitoring.