CS 145 Lab Exercise 13
Wireshark Lab: TOR and the Dark Web
A.Y. 2016-2017, 2nd Semester

1 Introduction

In this laboratory exercise you are going to what TOR traffic looks like at the packet level, as well as visit a Dark Web website. As such, it would be helpful for you to review Lecture 15 (as well as Laboratory Exercise 1) before doing the laboratory exercise.

2 Restrictions

For this laboratory exercise the following restrictions apply:

- Trace generation and analysis may be done in any machine with the Wireshark software installed. However, the machine must have the TOR browser installed.

3 Instructions: Trace Generation

For this laboratory exercise, you would need to generate four tracefiles.

3.1 Facebook.com, TOR browser

1. Start up the Wireshark software.
2. Select the appropriate interface and begin packet capture.
3. Make sure that no other browser is open as it could complicate your tracefile. Open the TOR browser.
4. Enter the URL `www.facebook.com` and have the web page displayed in the TOR browser. Wait for the entire web page to load completely before proceeding to the next step.
5. Stop packet capture.

6. Save the packet trace file as `labexercise15A.pcapng`. You can use this if you wish to work on the laboratory report at a later time. Make sure that you do not turn off the Wireshark software or the TOR browser.

3.2 Inquirer.net, TOR browser

1. Begin a new packet capture.
2. Enter the URL `www.inquirer.net` and have the web page displayed in the TOR browser. Wait for the entire web page to load completely before proceeding to the next step.
3. Stop packet capture.
4. Save the packet trace file as `labexercise15B.pcapng`. You can use this if you wish to work on the laboratory report at a later time. Make sure that you do not turn off the Wireshark software or the TOR browser.

3.3 NL Growers, TOR browser

Warning: It is usually considered good practice when surfing Dark Web web sites to cover your laptop's or PC's webcam.

1. Begin a new packet capture.
2. Enter the URL `http://25ffhnaechrbzwf3.onion/` and have the web page displayed in the TOR browser. Wait for the entire web page to load completely before proceeding to the next step.
3. Stop packet capture.
4. Save the packet trace file as `labexercise15C.pcapng`. You can use this if you wish to work on the laboratory report at a later time.
5. Turn off your TOR browser and Wireshark software.

3.4 NL Growers, ordinary browser

1. Start up a web browser, which will display your selected homepage.
2. Clear the browser's history - I assume that you already know how to do this. Also, throughout the exercise, avoid using multiple tabs, even if your browser is capable of tabbed browsing. That is, while doing the laboratory exercise, do **not** surf any other websites, as that would affect the trace that you would generate.
3. Enter the URL `http://25ffhnaechrbzwf3.onion/`, press Enter, and observe what happens.

4 What to hand in

Answer the following questions in the laboratory report, based on your Wireshark experimentation:

1. Based on `labexercise15A.pcapng`, what is the IP address of the computer from/through which your computer got the packets for the Facebook webpage? You can use the volume of packets to deduce the identity of the computer in your tracefile. Include an annotated screenshot supporting your answer.

2. Compare the IP address in [1] with the IP address of the Facebook web server in `labexercise14.pcapng` (generated for the previous lab exercise). Are they the same? Include annotated screenshot(s) supporting your answer.

3. Using an online WHOIS service (`https://www.ultratools.com/tools/ipWhoisLookup`), determine the owner of the IP address in [1]. Is the IP address or computer/server owned by Facebook? Include an annotated screenshot supporting your answer.

4. If you are just looking at the tracefile and you did not know how the tracefile was generated, would you be able to deduce that it was generated by a browser surfing or loading the Facebook web page? Why or why not?

5. Look at `labexercise15B.pcapng` and `labexercise15C.pcapng`, generated by loading the web pages for Inquirer.net and NL Growers, respectively. What can you say about the identity of the computer from/through which your computer got the packets for the Facebook webpage? TOR works with *circuits*. For the very first computer in the circuit at least, does it change as you surf different web sites? Include annotated screenshot(s) supporting your answer.

6. Can your non-TOR browser load `http://25ffhnaechrbzwf3.onion/`? Why or why not? If it cannot be loaded, what error is returned? Include an annotated screenshot supporting your answer.

5 Submission

The laboratory report is due on Sunday, April 30, 2017, 2359 hours. You can submit the laboratory report via UVLE.