

**SI430: Lab 04 --- PCAP Data Analysis II**

Names: Meris Larkins and Chris Paris

Alphas: 253486, 264845

External source(s)

Honor

We wrote the code on my own except the help from the external source(s) listed above. Moreover, we didn’t copy any part of the code from other midshipmen.

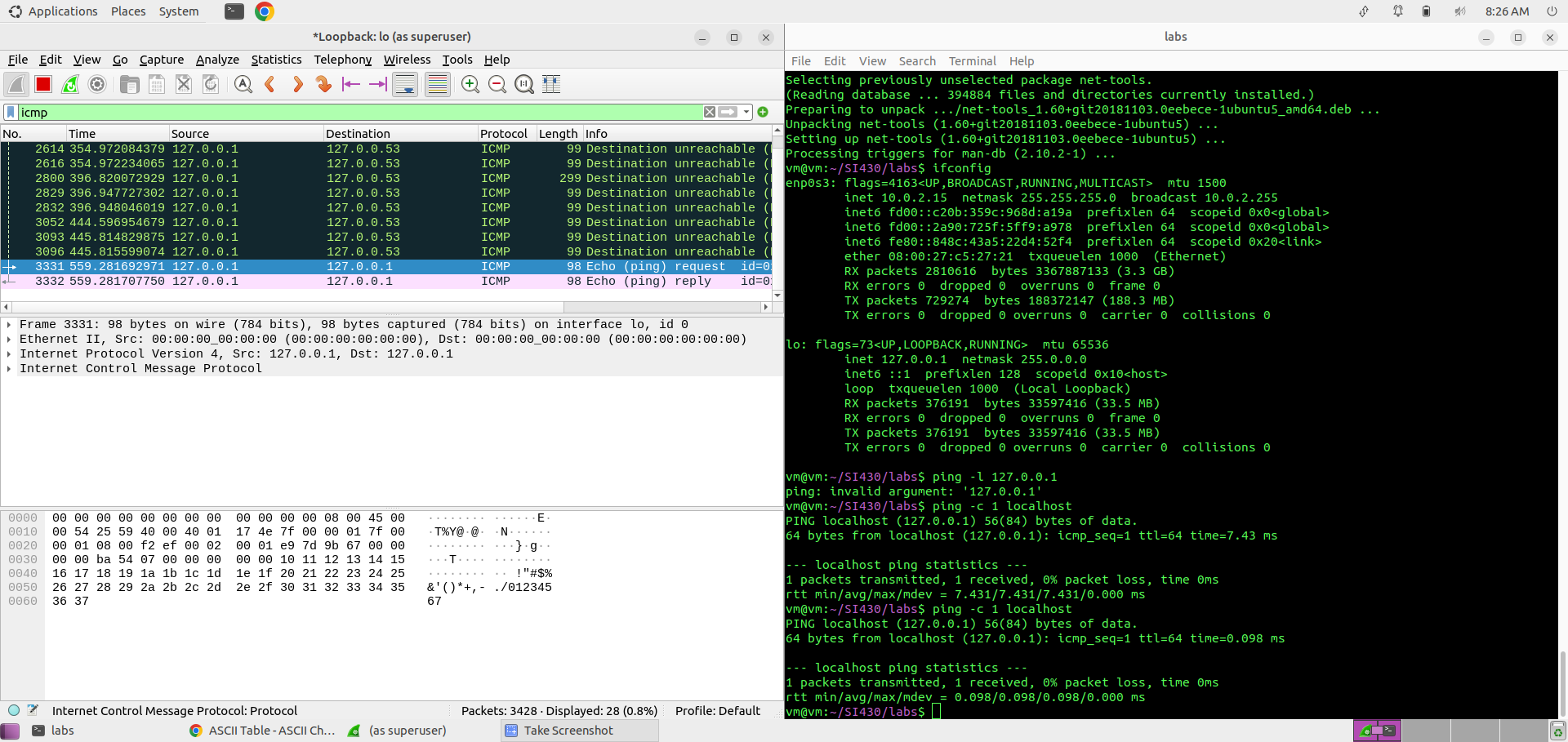
Initials: MEL and CPP

Challenges

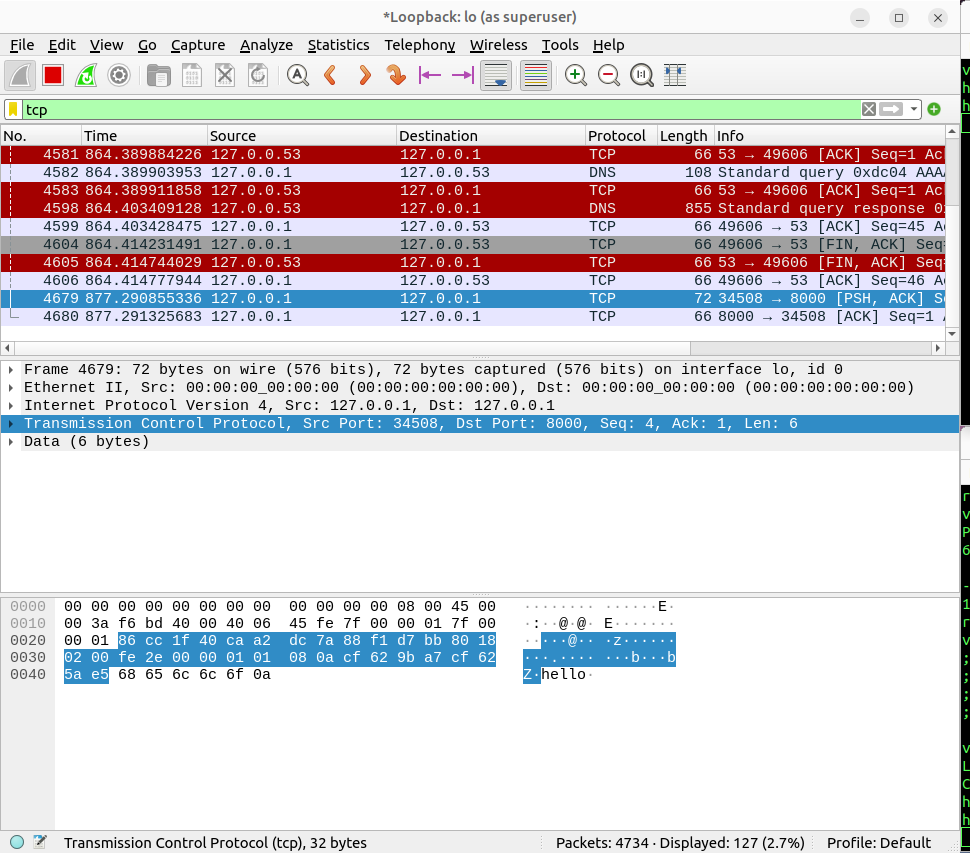
This lab was less challenging and more tedious

What we learned and what was interesting to us

# **Part 1:**



# 



# **Part 4:**

Many countries around the world have become players in the cyber game. The most notable contenders are China and Russia, although there is a difference in their motivations. China is more focused on developing their cyber infrastructure and using any attacks as a means of surveillance, not necessarily denial of service. It follows a doctrine known as “Peaceful Rise,” which says China will not focus on attacking its adversaries until it becomes an equal. An example of China’s cyber exploits is the Tibetan mail server attack conducted in 2008. It originated with a phishing email sent to a Tibetan monk; the monk clicked on the link, thinking it was from a colleague, and his machine became infected, eventually spreading to the server it was running on located outside the country.  
Russia, on the other hand, tends to be more destructive in its cyber exploits. Russia feels “encircled” by the rest of the world powers and does not have as robust of a technological infrastructure as China does. Therefore, Russia relies on lashing out against other countries to project power. For example, the NotPetya worm Russia launched in 2017 affected large corporations around the world, such as Maersk, Mondelez, and FedEx, costing them millions. It encrypted their data and asked for bitcoin to unlock it, but in reality, the encryption was irreversible, and the solution offered in exchange for bitcoin was a false promise.

Other countries have been making waves in the cyber realm on a smaller scale, but certain attacks have been no less notable. Saudi Arabia exposed that Jeff Bezos, the owner of the Washington Post, was having an affair, leading to his divorce. Syrian police used brutality tactics and spear-phishing during their civil war, threatening female family members of suspects with rape unless they disclosed passwords that could be used against them. Iran has gone through with both surveillance and offensive cyber actions, monitoring the emails of dissidents in the Netherlands and launching attacks on Aramco and Israeli water treatment plants. North Korea’s Wannacry worm was a repeat of NotPetya, targeting car companies, a chip manufacturer in Taiwan, and the British National Health Service. Then there are the attacks that can’t necessarily be attributed to one cause or source, like the 2009 Copenhagen Climate Summit email scandal, which was likely either an internal actor or a mistake, or the highly-preventable Equifax breach, in which the stolen data was never actually misused. The ethical boundary in terms of cyber becomes more blurry as technology and the political climate continue to evolve.