

**SI430: Lab 03 --- PCAP Data Analysis I**

Names: Meris Larkins and Chris Paris

Alphas: 253486, 264845

External source(s)

Referred to GeeksForGeeks page on python enumerate function

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

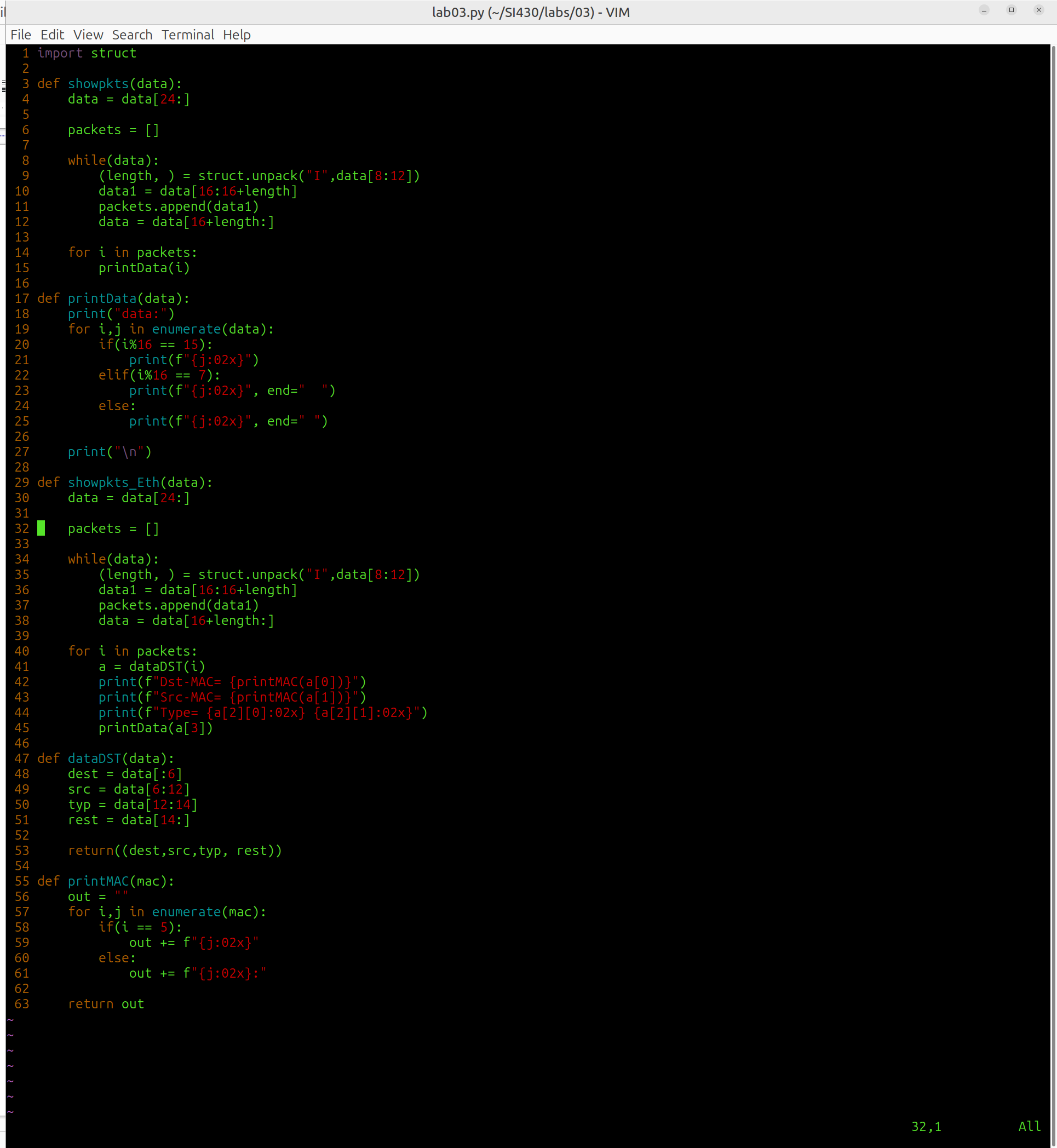
This lab was less challenging and more tedious

What we learned and what was interesting to us

We learned about the python enumerate function, which is very helpful for counting in a for-each loop.

It was interesting to hear about the Ed Snowden treason from the perspective of someone in industry gradually finding out it happened. The effect the breach had on the relationship between corporate entities and the government is not widely talked about.

# **Part 1 & 2**

****

Wrote in a semi-object-oriented manner, making functions, especially printing, that were good at doing that without cluttering the main functions.

# **Part 3:**

In the early days of the Internet, people didn’t have to worry about the security of their devices. The only “hackers” were essentially pranksters who just wanted to prove they could break into their school’s network or send funny messages over dial-up. It wasn’t until the late 1980’s that real problems started to arise, such as PC viruses, the Internet worm, DDoS attacks, and underground markets. Once the 2000s hit, governments started using the existing digital infrastructure to collect data from suspects on a large scale. The NSA unwittingly gave the world a look at how they accomplish this through Ed Snowden, a whistleblower who divulged NSA collection methods to journalists in Hong Kong. Those papers made their way to some of the most well-known news providers, and companies like Google, Microsoft, and Facebook discovered their data was being breached, inciting a rift between digital corporations and government actors.

Given Snowden’s act of treason, the world now has an idea of how several pieces of NSA software work and are used to collect information. Prism is an access channel that allows the FBI to conduct wiretaps if they have a warrant to do so. Tempora collects intelligence from fiber-optic cables; at the time of Snowden, 200 cables were tapped, and the NSA could collect from 46 cables at a time. An especially frustrating piece of technology to corporations was Muscular, which targets data freely flowing between centers and undoes the SSL encryption protecting it so it can be analyzed. The Special Collection Service (SCS) uses Tempest monitoring to collect information from electromagnetic emissions as well as a program called Bullrun/Edgehill to tamper with the digital supply chain. Then there’s Xkeyscore, a piece of software used to conduct queries on data using selectors to narrow down searches. Many exploits have been conducted using Xkeyscore, including the Logjam attack, used to break the Diffie-Hellman encryption used by many VPNs and TLS connections, and Quantum, which was used to tap Internet endpoints. On the military side, the Stuxnet attack was able to take down Iran’s uranium enrichment centrifuges. Since then, monitoring data and the conduction of attacks by government entities have continued to scale up, with some entities, like vendors and mercenaries, starting to act independently of their governments.