

**SI430: Lab 05 --- Raw Sockets and Packet Sniffing**

Names: Chris Paris and Meris Larkins

Alphas: 264845, 253486

External source(s)   
N/A

Honor

We wrote the code on our 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: \_CPP\_\_\_ and \_\_MEL\_\_

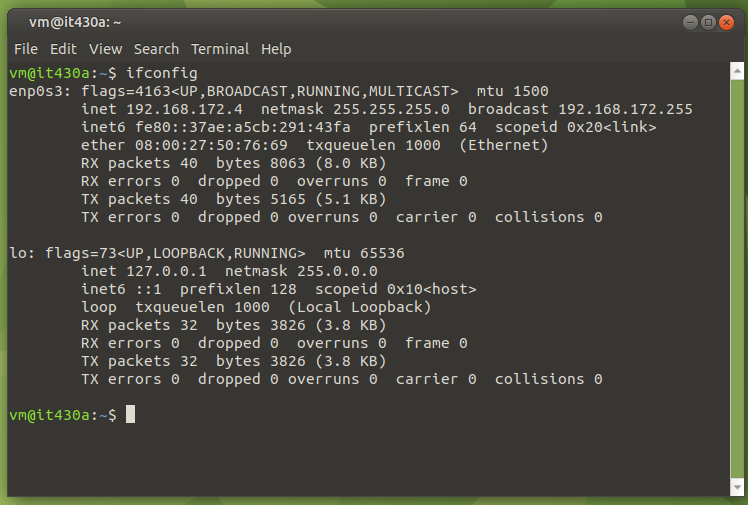
Challenges

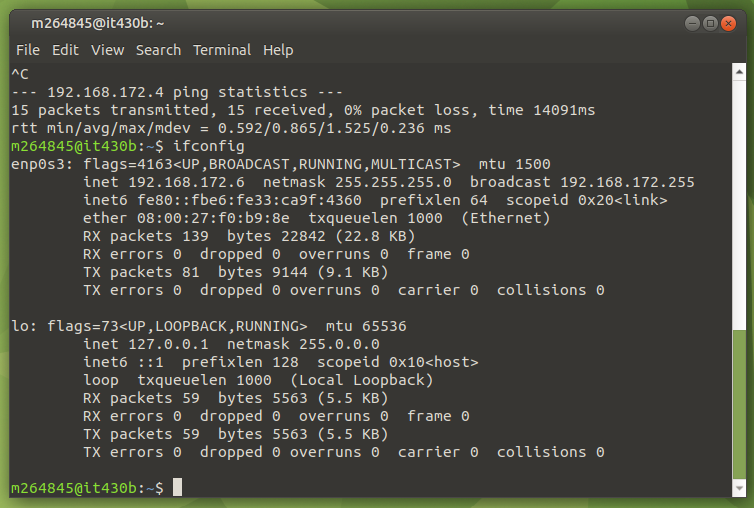
It was long

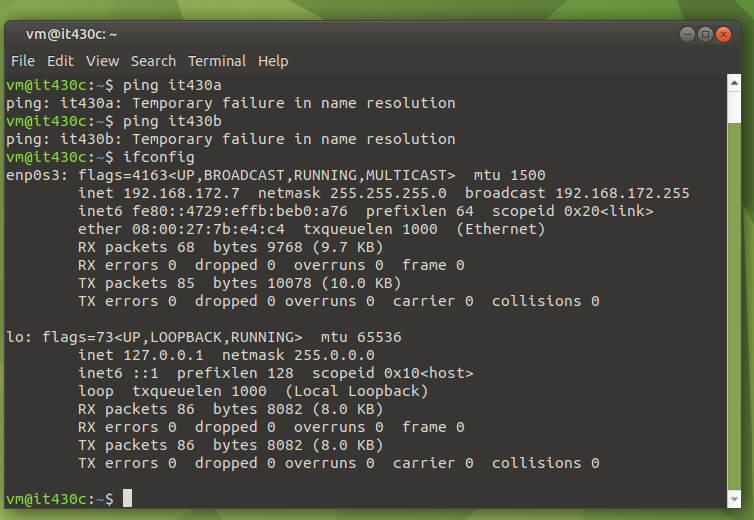
What we learned and what was interesting to us

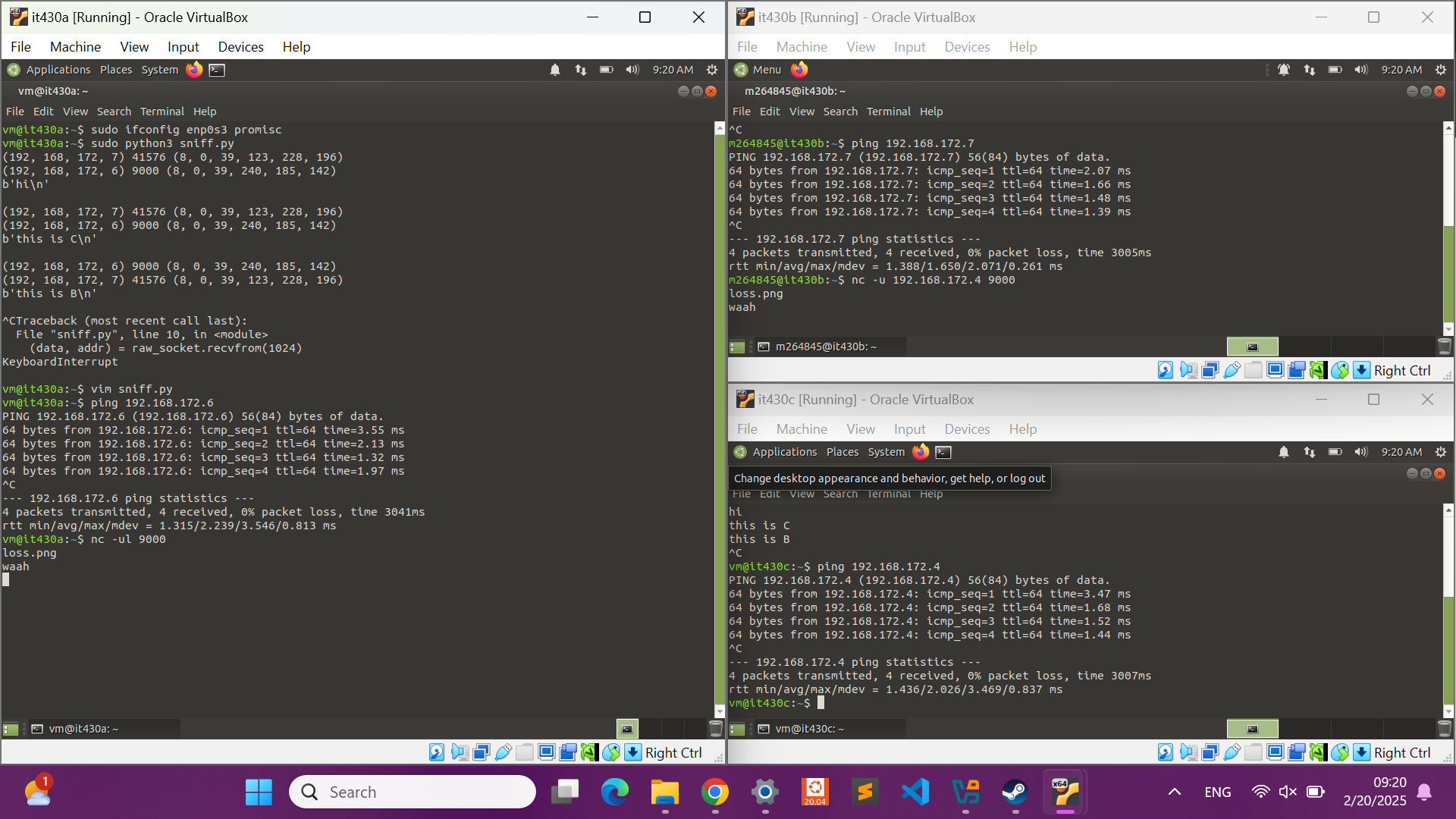
Raw Sockets read all traffic

# **Part 1**

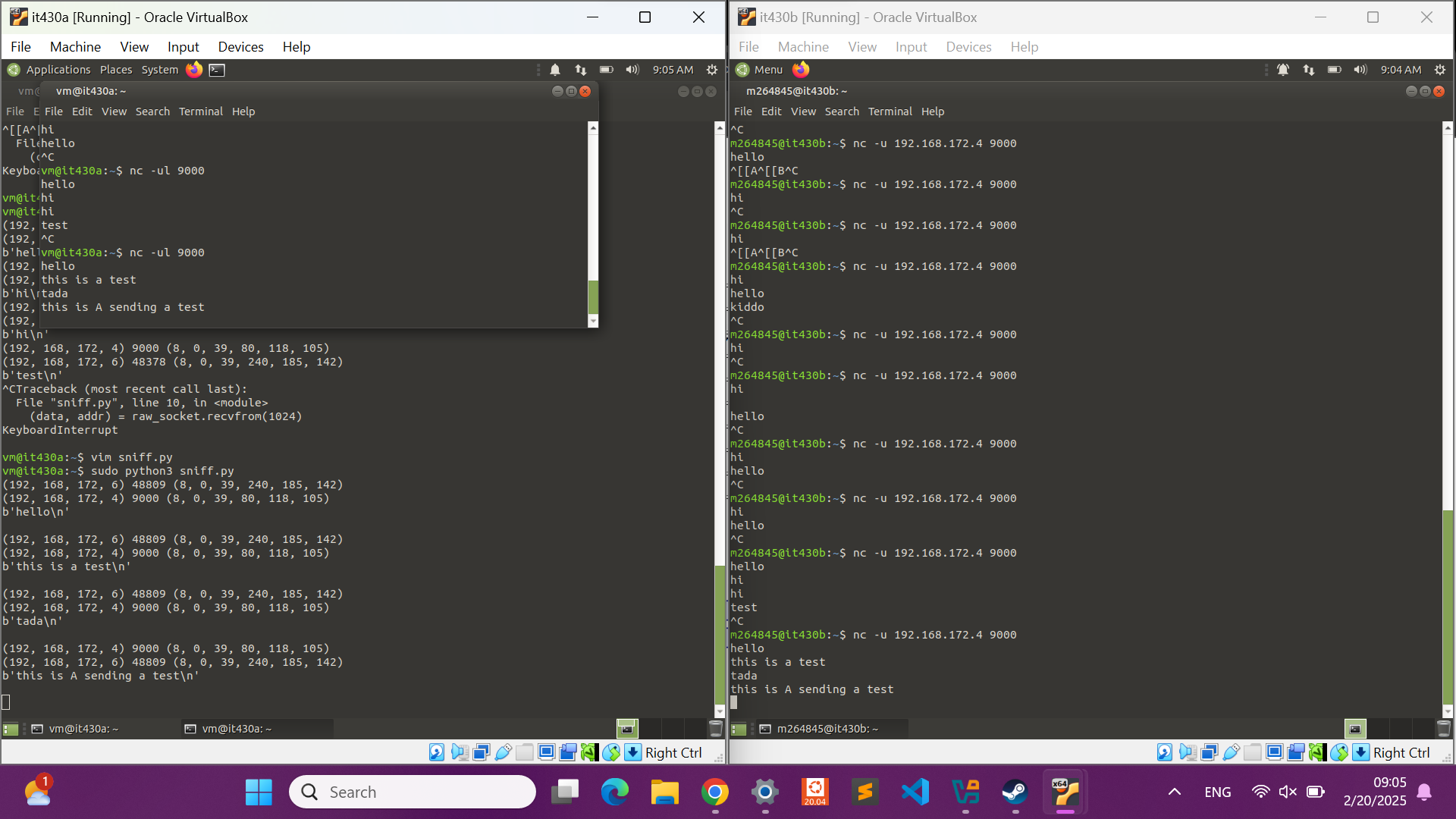




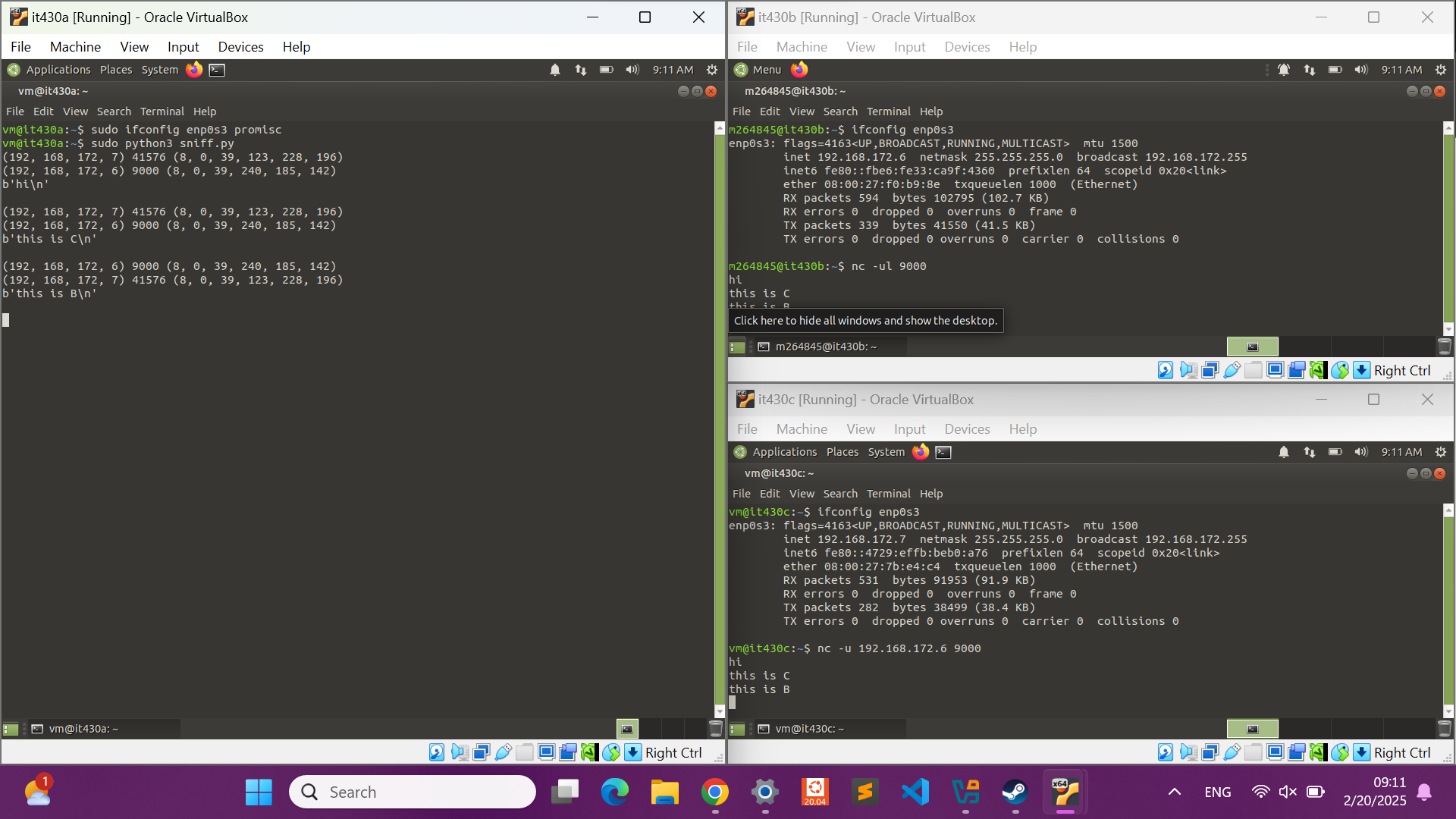




# **Part 2**

****

# **Part 3**

****

# **Part 4**

**Cybercrime has become increasingly prevalent in recent years as physical crime rates have dropped and criminals can use computers to fly under the radar. In fact, cybercrime makes up about half of all crime, even though it’s not caught as frequently or even considered crime in some cases. Cybercriminals can take a variety of forms. Botnet herders have been around since the late ‘90s, and their craft has evolved since their beginnings. It started with spam attacks like SYN floods, migrated to peer-to-peer botnets in which machines would infect each other, moved on to domain generation worms, and has become the exploitation of IoT devices. There are also cybercriminals writing malware; programs range from binary exploits to Trojans to mobile OS vulnerability attacks. Although there are many filters that now work against the industry, spammers are still alive and well, constantly finding ways to evade the walls built before them. Those who compromise accounts by cracking credentials tell a similar tale; they still exist, but they have become creative with their phishing lures. Other cybercriminal types include attackers who go after specific targets, cashout gangs who steal credit card information (or compromise bankers’ accounts via email), and those who develop ransomware that threatens the integrity of the cryptocurrency industry.**

In addition to outside actors, businesses have also fallen victim to internal actors. For example, the CEOs of Volkswagen and Audi found themselves in hot water after engineering their products to avoid running efficiently in favor of cleaner emissions if the cars detected typical emission testing conditions. The cars otherwise ran efficiently, intentionally circumventing compliance with green energy initiatives. Another example comes in the form of a company in China that created SIM cards to perform man-in-the-middle attacks on SIM cards in phones to lower roaming charges. Finally, there is the complicated issue of whistleblowers; many of them want to do the right thing by divulging information to authorities, but in cases like the Ed Snowden incident, whistleblowing can lead to grave consequences on the other side.