Task List

- What operating system and type of device is on 10.11.11.94?
  - HonHaiPrecis 38:b1:db:d0:91:9d (Honhai device)
  - Chrome OS

- What operating system and type of device is on 10.11.11.121?
  - MurataManufa b8:d7:af:37:20:9c (Murata device)
  - Linux OS

- Based on the MAC address for 10.11.11.145, who is the manufacturer or vendor?

  - Based on the MAC address for 10.11.11.145, (bc:ff:eb:bc:2d:98), Motorola is the manufacturer.

- What operating system and type of device is on 10.11.11.179?
  - Apple device a8:bb:cf:52:d9:32
  - Mac OS

- What version of Windows is being used on the host at 10.11.11.195?
  - Windows NT (yikes) (Windows NT 10.0)

- What is the user account name used to log into the Windows host at 10.11.11.200?
  - Used kerberos lookup to find brandon.gilbert is the user.

- What operating system and type of device is on 10.11.11.217?
  - Apple device e8:b2:ac:ac:b2:49
  - Mac OS

- What IP is the Windows host that downloaded a Windows executable file over HTTP?
  - 10.11.11.203 is the host that downloaded the executable from 188.95.248.71.

- What is the URL that returned the Windows executable file?
  - acjabogados.com/40group.tiff

- What is the SHA256 file hash for that Windows executable file?
  - 8d5d36c8ffb0a9c81b145aa40c1ff3475702fb0b5f9e08e0577bdc405087e635

- What is the detection rate for that SHA256 hash on VirusTotal?
  - 58/72 vendors flagged this file as malware.

- What public IP addresses did that Windows host attempt to connect over TCP after the executable file was downloaded?
  - 138.201.6.195 , 5.188.108.58

- What is the host name and Windows user account name used on that IP address?
  - Host: Tucker-Win7-PC
  - User: candice.tucker