Opsporing verzocht

Bij het bedrijf XIsupport hebben ze het vermoeden dat binnen het bedrijf ongewenste contacten zijn met Rusland. Ze hebben jou een pcap-file gegeven en vragen je uit te zoeken of dit het geval is. Zoals vaak in dit soort gevallen: veel verdere informatie is er niet, je mag het allemaal zelf uitzoeken. Maar je bent een handige Python programmeur en met de standaard Python libraries kom je er wel.

Pcap

https://en.wikipedia.org/wiki/Pcap Pcap is een formaat dat gebruikt wordt om opgenomen netwerk-pakketten te schrijven naar een file en deze verder te analyseren. In de les is behandeld hoe je een pcap-file kunt lezen en de code van hva_pcap moet je gebruiken. De code is beschikbaar in `hva_pcap.py`

Pckt

In de les is behandeld hoe je een Ethernet, IP-packet en TCP-packet moet decoderen. De code is beschikbaar in `hva_pckt.py` . Je moet deze code gebruiken om een netwerk-packet te decoderen. https://en.wikipedia.org/wiki/Ethernet_frame https://en.wikipedia.org/wiki/Transmission*Control*Protocol https://en.wikipedia.org/wiki/Transmission*Control*Protocol

Tld

In de les is behandeld hoe de tld.csv file eruit ziet en hoe je hierin snel kunt zoeken. Gebruik het Object `TldDb` om de Tld van een IP-address te vinden. Dit object wordt in `hva_tld.py` beschreven.

Aanpak

Met boven genoemde libraries kun je een pcap-file lezen. Het packet eerst coderen als Eth en vervolgens de layload als Ip en daar de payload als Tcp. Nu kun je het `destination ip-address` opzoeken in Tld en vaststellen of deze verbinding naar Rusland gaat. Zo ja, print de kenmerken van de verbinding af (tijdstip, src-ipaddr, src-ipport, dst-ipaddr, dst-ipport)