Chapter 4: Analyzing “Badness”

“The world is full of *good* people who do *bad* things, mon ami.”

Hecure Poirot, Agatha Christie’s Poirot: The Clocks, 2009

“Sometimes, bad is bad.”

Huey Lewis & The News, Sports, Chrysallis Records, 1983

This chapter will continue the exploration of the AlienVault IP Reputation database that began in Chapter 3 and assumes the reader is familiar with the description of the data set and has followed along with the preliminary analyses.

Dissecting The “IP Address”

32-bit integer (“how does your computer see an IP address?”) + machine info

Part of a subnet / logical layout / MAC addresses, perhaps has a hostname (DNS)

Larger context: part of a global network organized by ASNs (BGP)

Lager context: Has a physical location

Mapping Outside the Continents

USE CASE: Visualizing AlienVault ASN data (force-directed network graphs of malhost ASN groupings)