JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Info Gathering and Aggregation

THREAT MANAGEMENT

Information Gathering

- Can be done using packet captures
- Requires an intruder to breach a company's network to gather this info
- Treasure trove of information
  - What hosts are on the network
  - What operating systems are the running
  - What shares are available
- This is done using tools like Wireshark
  - Beyond the scope of this lesson…

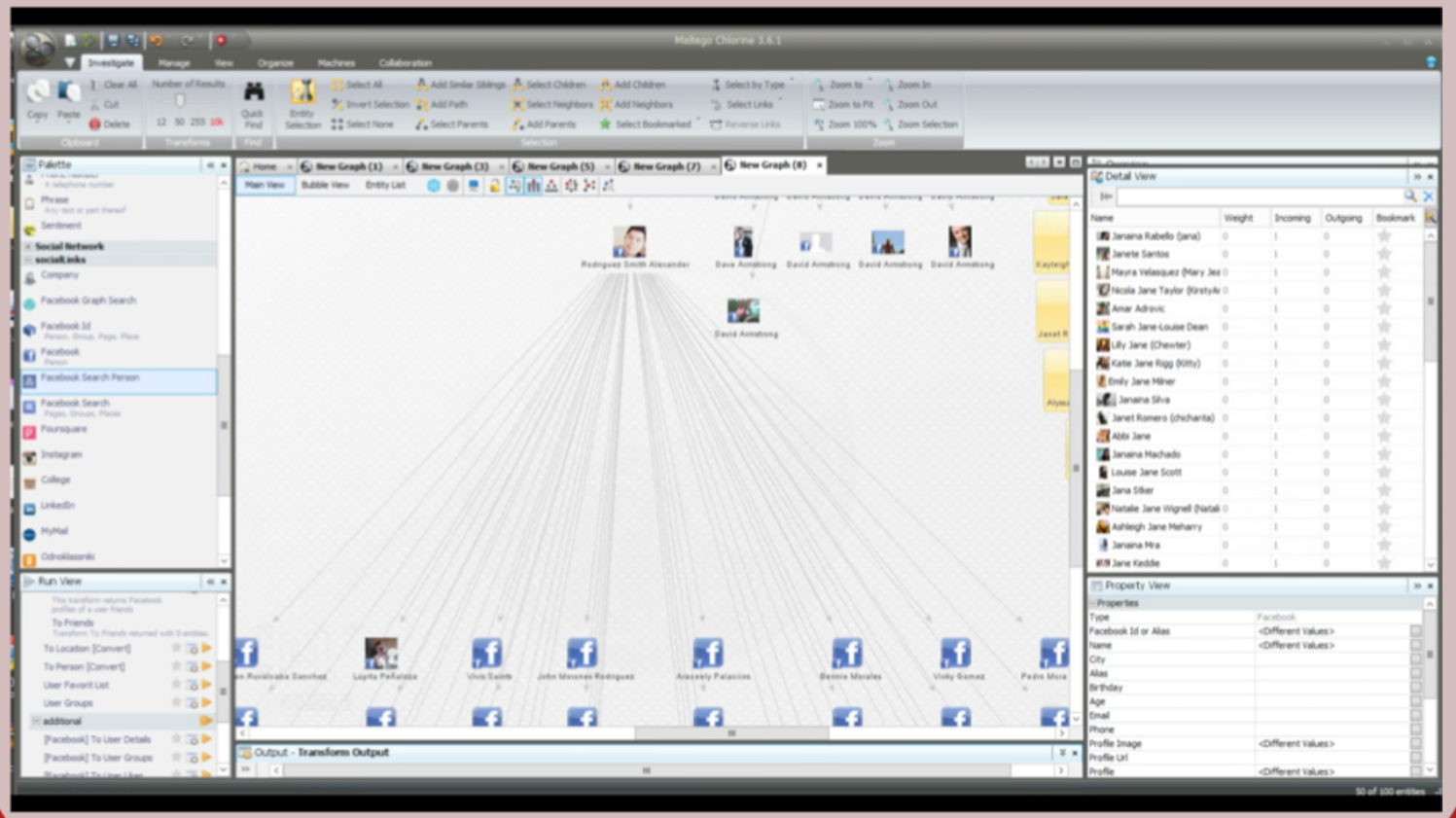
Information Aggregation

- Gathering information from various platforms for analysis with a single tool

- theHarvester
  - Gathers emails, domains, hostnames, employee names, open ports, banners, etc.
  - Text-based tool installed in Kali

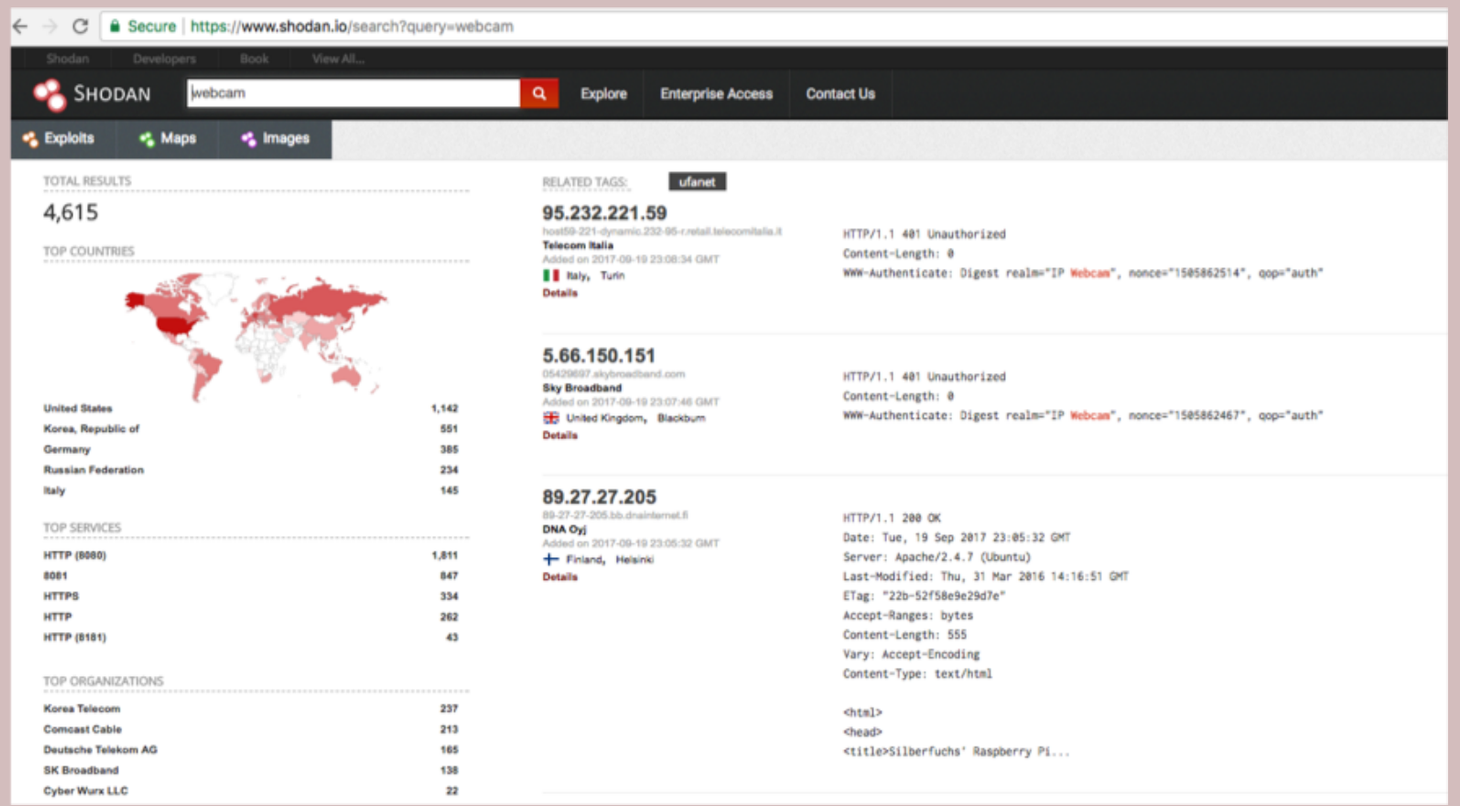
Maltego

- Builds relationship maps between people and resources



Shodan

- Search engine for internet-connected devices and their vulnerabilities



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE