



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...



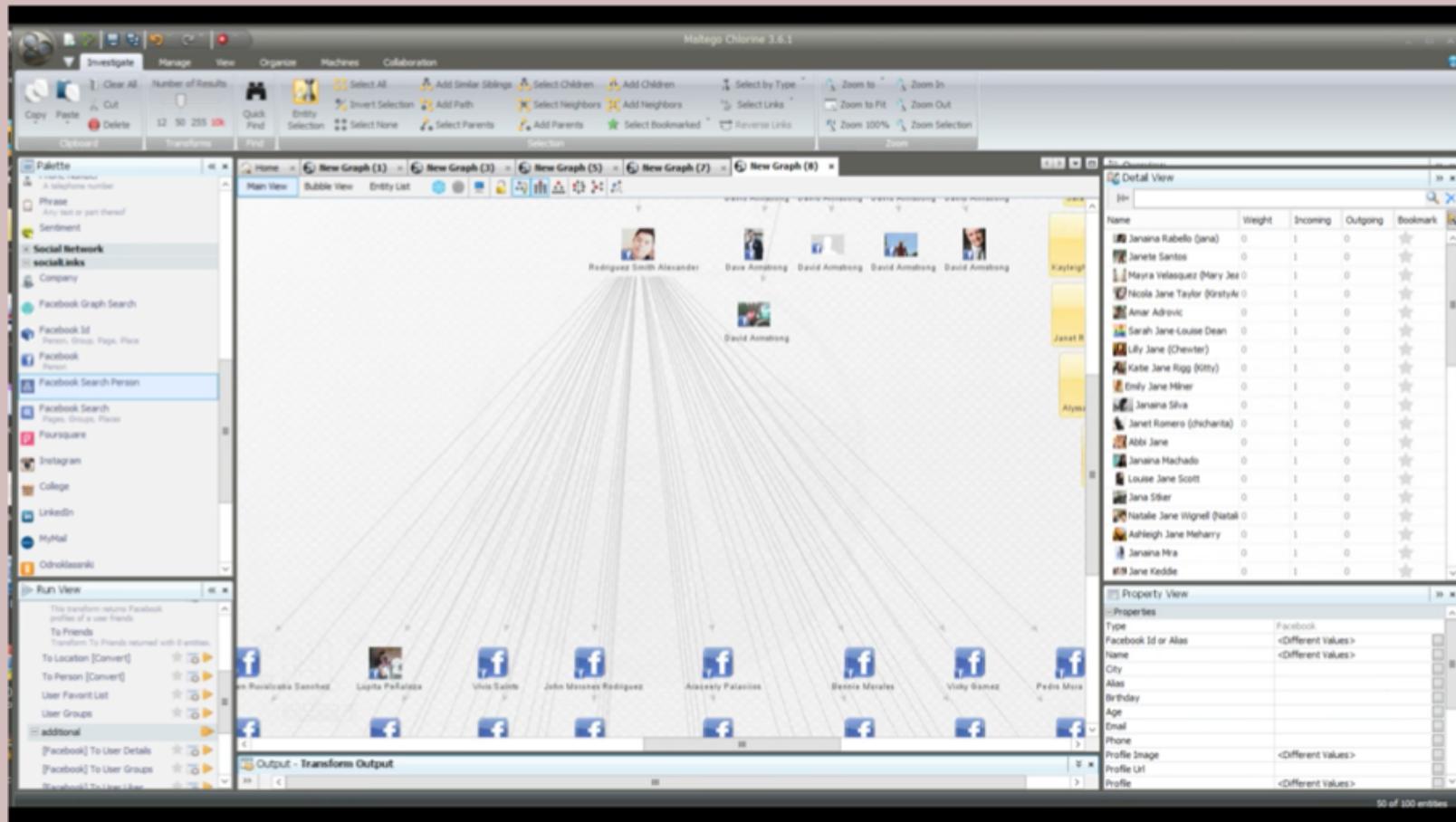
Information Aggregation

- 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



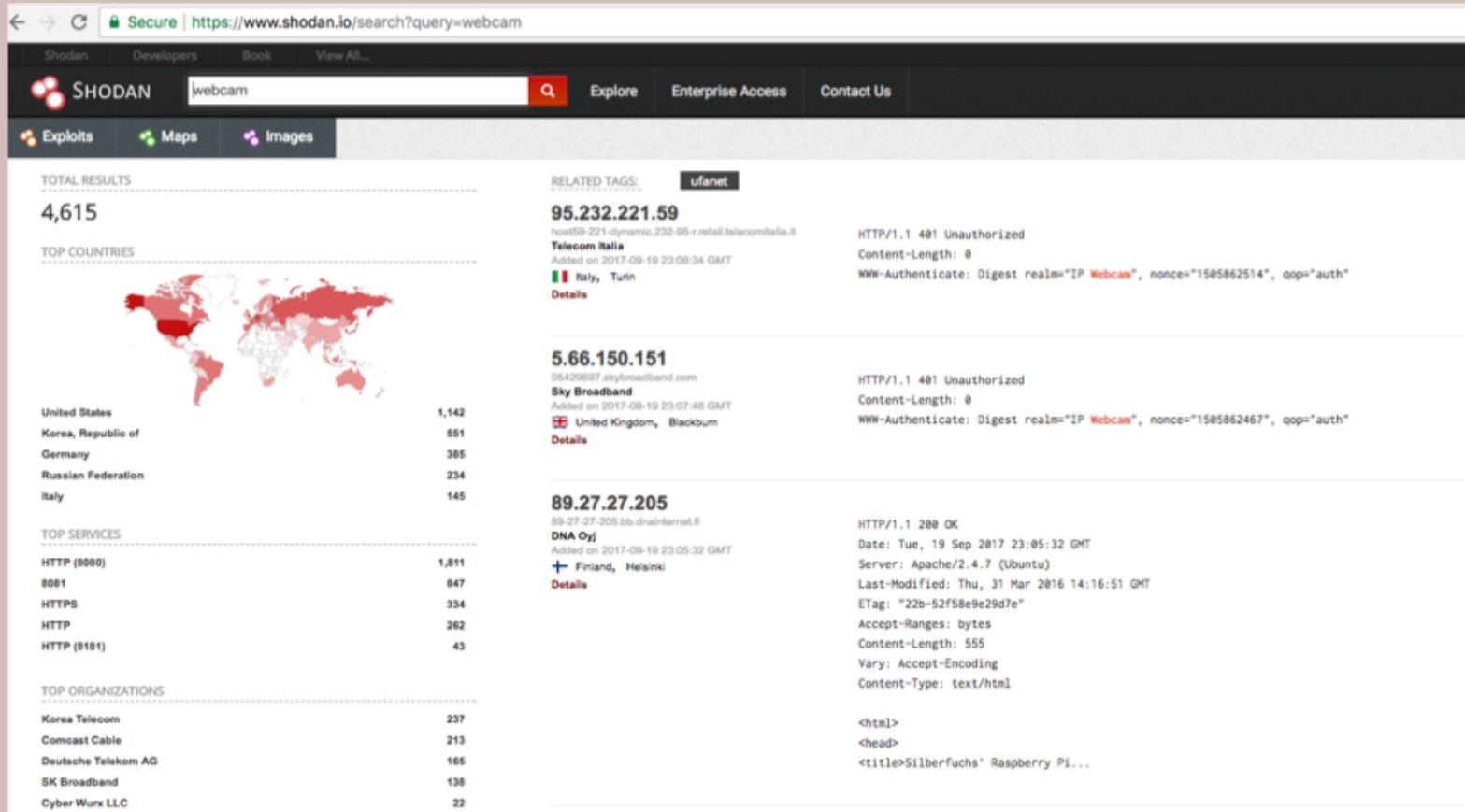
Maltego

- Builds relationship maps between people and resources



Shodan

- Search engine for internet-connected devices and their vulnerabilities



Secure | https://www.shodan.io/search?query=webcam

Shodan Developers Book View All...

SHODAN

Explore Enterprise Access Contact Us

Exploits Maps Images

TOTAL RESULTS 4,615

TOP COUNTRIES



Country	Count
United States	1,142
Korea, Republic of	551
Germany	385
Russian Federation	234
Italy	145

TOP SERVICES

Service	Count
HTTP (8080)	1,811
8081	847
HTTPS	334
HTTP	262
HTTP (8191)	43

TOP ORGANIZATIONS

Organization	Count
Korea Telecom	237
Comcast Cable	213
Deutsche Telekom AG	165
SK Broadband	138
Cyber Wurx LLC	22

RELATED TAGS: ufanet

95.232.221.59
host59-221-dynamic.232-95-r.retail.telecomitalia.it
Telecom Italia
Added on 2017-09-19 23:08:34 GMT
Italy, Turin
[Details](#)

HTTP/1.1 401 Unauthorized
Content-Length: 0
WWW-Authenticate: Digest realm="IP Webcam", nonce="1505862514", qop="auth"

5.66.150.151
05429697.skybroadband.com
Sky Broadband
Added on 2017-09-19 23:07:46 GMT
United Kingdom, Blackburn
[Details](#)

HTTP/1.1 401 Unauthorized
Content-Length: 0
WWW-Authenticate: Digest realm="IP Webcam", nonce="1505862467", qop="auth"

89.27.27.205
89-27-27-205.bb.dnainet.fi
DNA Oyj
Added on 2017-09-19 23:05:32 GMT
Finland, Helsinki
[Details](#)

HTTP/1.1 200 OK
Date: Tue, 19 Sep 2017 23:05:32 GMT
Server: Apache/2.4.7 (Ubuntu)
Last-Modified: Thu, 31 Mar 2016 14:16:51 GMT
ETag: "22b-52f58e9e29d7e"
Accept-Ranges: bytes
Content-Length: 555
Vary: Accept-Encoding
Content-Type: text/html

<html>
<head>
<title>Silberfuchs' Raspberry Pi...

