Chap 24 – IP Addresses

- Often gathered as part of an investigation
  - Legal processes / LEA
  - Using Domain search techniques from chapter 23
  - Various OSINT tools

viewdns.info

- Reverse IP - Shows all other domains hosted from the same server. Useful for finding phishing sites or identifying other sites on the same shared hosting server.
- IP Location - Displays geographic information about an IP,
- Port Scan - Test whether common ports are open on a server.
- Whois - Displays owner/contact information for a domain name or IP address
- Traceroute - Trace the servers that data traverses from the ViewDNS server to the specified domain name or IP address
- Reverse DNS - Find the reverse DNS entry (PTR) for a given IP, generally the server or host name.

Other Sites

- Bing – Supposedly can look up websites hosted on an IP, example didn’t work.
- IPLocation – Returns a lot of info and it’s free
- That’s Them – More invasive searches, results based on marketing data, can reveal person’s name, address, etc.
- I Know What You Download – Shows torrent downloads
- Wigle – Crowd source database for wireless access points, didn’t seem to work very well.

Other Sites

- Shodan – Standard, maps, images
- Zoomeye – Shodan competitor but sometimes provides different results
- Threat Crowd – Is an IP malicious?
- Censys – Collects data on hosts and sites
- Ip2location – Takes email header
- Iplogger – Create a link or image and will gather info on an IP that clicks on it
  - Blocked by most email providers

IP Logging

- Iplogger – Create a link or image and will gather info on an IP that clicks on it
  - Blocked by most email providers
- Canary Tokens – Also provides tracking tokens
  - Blocked by most email providers
- Roll your own to prevent email provider interference (pg 509)
- URL Biggy – Obfuscate the link even more to a ‘urlbiggy.com/’

Other Tools

- Get Notify – tracks if an email was opened and provides connection info
- HTML page with a these and more tools:
  - file:///home/osint/osint_files/tools/IP.html
  - Dependent on local paths
  - Need to enable popups from the location