**CJ 530 / CJ 603 – Internet Vulnerabilities & Criminal Behavior**

**Internet Forensics Assignment #1**

February 1, 2010

**Internet Protocol Number Databases**

IP Numbers uniquely identify every computer network on the Internet. Numbers are assigned to individuals and groups using a hierarchical structure

**IP Number Assignment**

**IANA** – *Internet Assigned Numbers Authority* – assigns large blocks of numbers to RIRs, Regional Internet Registries - <http://www.iana.org/>

**RIRs** - *Regional Internet Registries* – Four groups that assign sub blocks of IP numbers to large networks and to ISPs , Internet Service Providers, within the group’s geographic domain.

**ARIN** – *American Registry for Internet Numbers* –North America, parts of the Caribbean, and South Africa - <https://www.arin.net/>

063.x.x.x – 072.x.x.x

199.x.x.x

204.x.x.x – 209.x.x.x

216.x.x.x

**APNIC** – *Asia Pacific Network Information Centre* – Asia, the Pacific Rim, And Australia - <http://www.apnic.net/>

058.x.x.x – 061.x.x.x

202.x.x.x – 203.x.x.x

210.x.x.x – 211.x.x.x

218.x.x.x – 222.x.x.x

**RIPE** – *Réseaux IP Européens* *Network Coordination Center* – Europe, the Middle East, Northern Africa, and parts of Asia - <http://www.ripe.net/>

062.x.x.x

081.x.x.x – 088.x.x.x

193.x.x.x – 195.x.x.x

212.x.x.x – 213.x.x.x

217.x.x.x

**LACNIC** – *Latin American and Caribbean IP Address Regional Registry* – Latin America and the Caribbean - <http://www.lacnic.net/>

200.x.x.x – 201.x.x.x

---------------------------------------------------------------------------

001.x.x.x = 256 x 256 x 256 = 16,777,216 addresses

---------------------------------------------------------------------------

**Domain Names**

**ICANN** – *Internet Corporation of Assigned Names and Numbers* – assigns top-level domains and controls domain name registry, arbitrates domain name disputes - <http://www.icann.org/>

---------------------------------------------------------------------------

**Top-Level Domains** - .com, .net, .edu, .org, .biz, etc.

---------------------------------------------------------------------------

**Domain Name Registrars** – approved by ICANN to register domain names to hosts; individuals, groups, businesses, and so on. Each registrar maintains a database of domain names and contract information. Verification of this information is not always performed. Privacy services will register domain names for clients who wish to remain anonymous.

**Canonical name** – primary name for a host

**Alias** – a name that points to the same machine

**Internet Address Tools**

Query IP number and domain name registrar databases and return results.

**dig** (Mac OS, Unix) and **nslookup** – finds IP number for domain name and domain name for IP number.

---------------------------------------------------------------------------

After performing an IP number lookup, doing a reverse look up of the IP number can yield information about the canonical name of the host.

---------------------------------------------------------------------------

**whois** – queries the domain registration databases for contact and ownership information; whois of an IP number will return the subnets of which the IP number is part of.

---------------------------------------------------------------------------

Information returned by a whois query depends upon the registrars database that matches the host searched for. Some registrars will return all domains that use the searched host as a prefix; See microsoft.com

---------------------------------------------------------------------------

**traceroute** – shows the path between two addresses on the Internet. The IP address of each router on the path is captured and a reverse lookup is performed. Provides information on the connectivity of a host, type of network they are part of, who their ISP is, and how they are connected to the Internet. Uses ICMP, Internet Control Message Protocol.

---------------------------------------------------------------------------

Not all routers will return information and not all routers have a hostname.

-------------------------------------------------------------------------

**Assignment #1**

Select a web site that you would like to investigate. (Select one with a TLD of .com, .net, or .org) Use the tools described above to find out as much information as you can about the site. For example: what is the IP number of the site, who is the domain registered to, who is the ISP, what country is the IP number found in, does the information match up, and so on. Be sure to try a whois of the IP number to get information on what possible subnets the domain is in.

Once you have gotten all of the information you can using the Internet tools described above, use a search engine, such as Google or Bing, to see what other information you can find about the individual or company that runs the site. Also, try using one of the Internet Map services to see if you can get a map and an actual image of site’s location.

Prepare a Power Point presentation of your findings to share with the rest of the class.