Washington State Gambling Commission

Internet Gambling
&
Cyber Crime Investigations

Jim Dibble, CFCE, CEECS, SCERS, DFCP, CFE
Special Agent, Criminal Intelligence Unit

Internet Mining - Digging for Data

Ω

Objectives

At the end of this lesson you will be able to:

- Understand basic Internet technology
- Understand how TCP/IP works
- Understand what an IP address is
- Understand the basic technical procedures used during Internet communication

Internet Technology

What is the Internet?

- No centralized management exists
- Collection of networks and organizations
- Common procedures and protocols
- Guided by different groups
  - Internet Society
  - Internet Architecture Board (IAB)
  - Internet Engineering Task Force (IETF)
  - World Wide Web Consortium (W3C)
  - Private "registrar" companies
- Regional & Local Networks
  - Internet Backbones

Transmission Control Protocol
&
Internet Protocol

Internet Mining – Digging for Data

Transmission Control Protocol / Internet Protocol

- Suite of communications protocols used to connect hosts on the Internet.
- The defacto standard for sending data over the networks.
- A set of protocols - not a single protocol
- Developed by Department of Defense Advanced Research Projects Agency (DARPA) in 1969
- Protocols are mapped to a four layer model known as the DARPA or DOD model

Internet Mining – Digging for Data

Transmission Control Protocol / Internet Protocol

...not just one protocol, but a full protocol suite, which includes:

- *Transmission Control Protocol – TCP*
- *Internet Protocol – IP*
- *File Transfer Protocol – FTP*
- *Terminal Emulation – Telnet*
- *Internet Control Message Protocol – ICMP*
- *Address Resolution Protocol - ARP*
- *User Datagram Protocol - UDP*
- ..... and others

Internet Mining – Digging for Data

TCP divides data into packets containing information for error control and reassembly

IP places header on each packet and directs packets via most efficient route.

At destination:

- IP header is removed.
- The TCP attached to the packet is examined to ensure no packets were lost or corrupted.
- If lost/damaged, sender requested to resend packet.

Transmission Control Protocol

Transmission Control Protocol (TCP)

- Defined as a "*reliable connection-oriented transport mechanism*"
- Verifies that data delivered across a network is done accurately and in the proper sequence

TCP Sequence Tracking

- Sequence number in the TCP header keeps track of the sent /received byte counts for the hosts
- Host tracks and acknowledges the number of packets received by including the byte count in the TCP header
- As data is sent and received, the byte count and sequence numbers increase incrementally
- Error control generates and sends a request for missing and/or damaged packets

Bit Offset	Bits 0-3	4-7	8-15	16-31
0	Source Port			Destination Port
32	Sequence Number			
64	Acknowledgment Number			
96	Data Offset		Reserved Flags Window	
128	Checksum			Urgent Pointer
160	Options + Padding			
160/192+	Data			

TCP Header Format

The Internet Protocol

The Internet Protocol (IP):

- Responsible to get packets from one system to another
- IP address uniquely identifies host on a given network
- No error control provided at this level

TCP/IP is:
a suite of "**protocols**"
based on an "**architectural model**"

What is an Architectural Model?

- Provides a common frame of reference for Internet communications
- Used to explain communication protocols and develop them
- Separates functions performed by communication protocols in layers
- Each layer in the stack performs a specific function in network communication

Required Elements

- Pathway
  - A way to get information from one place to another
- Rules
  - Defined set of rules to facilitate communication
- Connection
  - Communication between devices

Rules, Rules, Rules…..defined as

- Models
- Protocols

Models:

- A concept of how something should work
- It **does not** provide a solution
- A 'car' is an example of concept

Protocols:

- Actually provide a working solution for concepts identified in a model
- It **does** provide a solution
- A 'Ford Mustang' is an example of working solution

Open System Interconnection (OSI) Model

- An essential component of network design since 1984
- Is an ***abstract model*** – not strictly adhered to
- Effort by International Standards Organization (ISO) to standardize network design
- Divides complex host-to-host networking into layers
- Layers ordered from lowest to highest in "*stack*"
- Stack contains seven layers in two groups
  - Upper Layers
  - Lower Layers

Internet Mining – Digging for Data

Upper Layers:

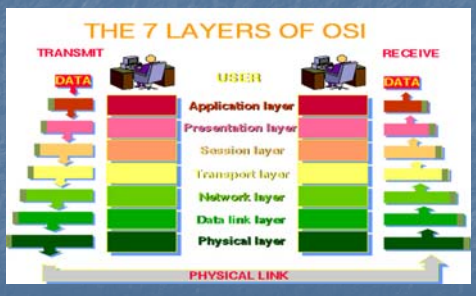
- *Application specific functions* (data format, encryption, connection management)
  7. Application
  6. Presentation
  5. Session

Internet Mining – Digging for Data

Lower Layers:

- *Network specific functions* (routing, addressing)
  4. Transport
  3. Network
  2. Data link
  1. Physical

Internet Mining – Digging for Data



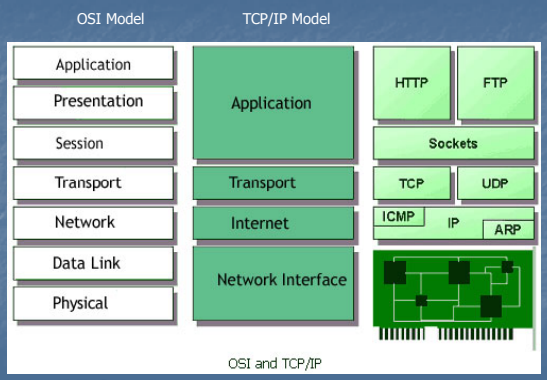
Internet Mining – Digging for Data

The TCP/IP Architectural Model*

- Consists of four (4) layers
  - Application Layer
  - Transport Layer
  - Internet Layer
  - Network Interface Layer

Each layer corresponds to one or more layers of the OSI Model

** DOD Model*



Internet Mining – Digging for Data

NETWORK LAYER

- Contains protocols to deliver data to other devices attached to the network
- Three distinct functions:
  - Defines how to transmit a frame (data unit passed across the physical connection)
  - Exchanges data between computer and physical network over physical link
  - Delivers data between devices on same network

(Responsible for placing TCP/IP packets on and receiving them from the network)

INTERNET LAYER

- Defines IP Address
- Manages addressing of packets and delivery between networks

TRANSPORT LAYER

- Where flow-control and connection protocols exist
- Manages the transfer of data via TCP (connection-oriented) and UDP (connectionless) transport protocols
- Opens and maintains connections ensuring packets are received.

APPLICATION LAYER

- Provides applications the ability to access the services of the other layers
- Defines protocols the applications use to exchange data
- Where "higher level" protocols operate:
  - Simple Mail Transfer Protocol (SMTP)
  - File Transfer Protocol (FTP)
  - Secure Shell (SSH)
  - Hyper Text Transfer Protocol (HTTP)

How does a Protocol Stack Work?

- Data passed down from one layer to another until transmitted over network
- Each layer determines how data is handled at that level
- Each layer adds control data (address, routing controls, checksum) to ensure proper delivery

Internet Mining – Digging for Data

How does a Protocol Stack Work?

- Control data placed in front is called a "header"
- Control data placed at rear is called a "trailer"
- All information passed down is treated as data
- Each layer places its "header" and/or "trailer" around previous layer's "data"
- Wrapped messages then passed to lower layer
- Wrapping known as "encapsulation"

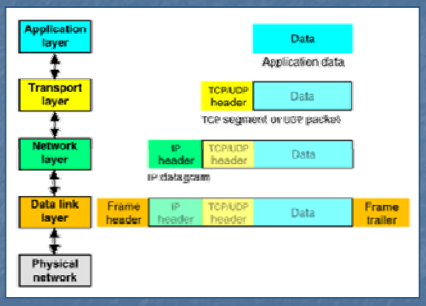
Internet Mining – Digging for Data

How does a Protocol Stack Work?

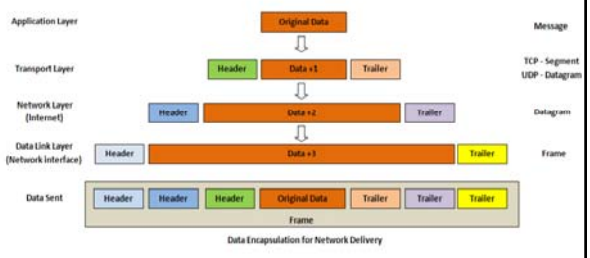
- When data is received by receiver:
  - Each layer strips off its header and/or trailer
  - Data passed up to the next layer
  - Information passed up the "stack" is interpreted as data and header/trailer
  - Process of removing headers and trailers is "decapsulation"

How does a Protocol Stack Work?

- Each layer in transmitting computer is enabled to communicate with the corresponding layer in the receiving computer
  - Known as "peer-to-peer communication"



DATA PACKETS



Internet Mining – Digging for Data

Data Packets

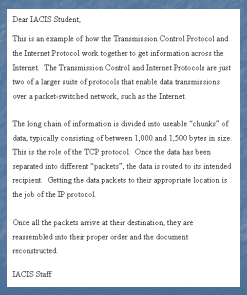
- Internet is a packet-switched network
- Information transmitted via data packets
- Long chains of data are susceptible to loss/corruption
- TCP breaks the long chains of data into a useable series of packets
- Typical packet is between 1,000 – 1,500 bytes in size

Internet Mining – Digging for Data

Data Packet vs. Datagram

- Often used interchangeably to refer to a "chunk" of data
- When Network's layer size for datagrams exceeds the limits of the physical link (Maximum Transmission Unit):
  - Network layer breaks large datagrams into packet-sized chunks
  - Data link layer and physical layer process and transmit packets
  - Process called "fragmentation"
- Receiving host reassembles fragmented datagram in correct order.

Internet Mining – Digging for Data



Dear IACIS Student,

This is an example of how the Transmission Control Protocol and the Internet Protocol work together to get information across the Internet. The Transmission Control and Internet Protocols are just two of a larger suite of protocols that enable data transmissions over a packet-switched network, such as the Internet.

The long chain of information is divided into useable "chunks" of data, typically consisting of between 1,000 and 1,500 bytes in size. This is the role of the TCP protocol. Once the data has been separated into different "packets", the data is routed to its intended recipient. Getting the data packets to their appropriate location is the job of the IP protocol.

Once all the packets arrive at their destination, they are reassembled into their proper order and the document reconstructed.

IACIS Staff

Step 1:
A document is prepared

Internet Mining – Digging for Data

1

Dear IACIS Student,

This is an example of how the Transmission Control Protocol and the Internet Protocol work together to get information across the Internet. The Transmission Control and Internet Protocols are just

2

two of a larger suite of protocols that enable data transmissions over a packet-switched network, such as the Internet.

The long chain of information is divided into useable "chunks" of data, typically consisting of between 1,000 and 1,500 bytes in size.

3

This is the role of the TCP protocol. Once the data has been separated into different "packets", the data is routed to its intended recipient. Getting the data packets to their appropriate location is the job of the IP protocol.

4

Once all the packets arrive at their destination, they are reassembled into their proper order and the document reconstructed.

IACIS Staff

Step 2:
The document is divided into "data packet" sections

Internet Mining – Digging for Data

1

2

3

4

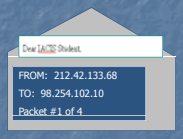
two of a larger suite of protocols that enable data transmissions over a packet-switched network, such as the Internet.

The long chain of information is divided into useable "chunks" of data, typically consisting of between 1,000 and 1,500 bytes in size.

This is the role of the TCP protocol. Once the data has been separated into different "packets", the data is routed to its intended recipient. Getting the data packets to their appropriate location is the job of the IP protocol.

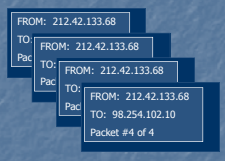
Once all the packets arrive at their destination, they are reassembled into their proper order and the document reconstructed.

IACIS Staff



Step 3:
Each section is enclosed in a data packet with source address, destination addresses, and packet number

Internet Mining – Digging for Data



Step 4:
The data packets are now ready to be sent over the Internet

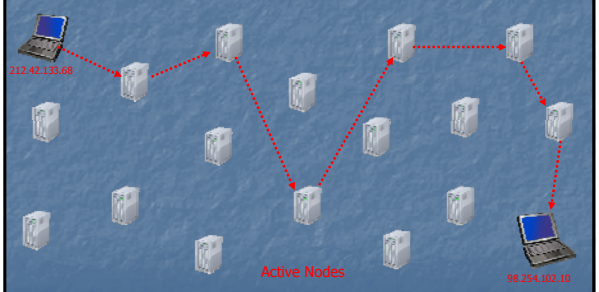
Internet Mining – Digging for Data

Packet transmission route is dependant upon:

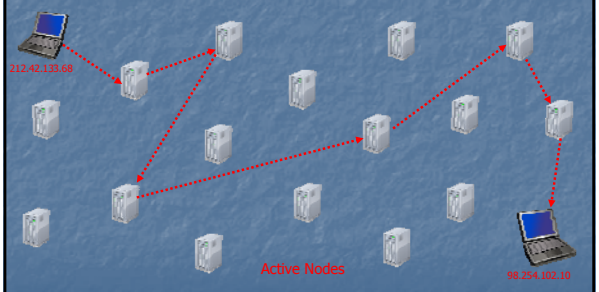
- Best available route
- Bandwidth available – Network traffic
- Node availability
  - May use same or different routes

"Like electricity – takes the path of least resistance"

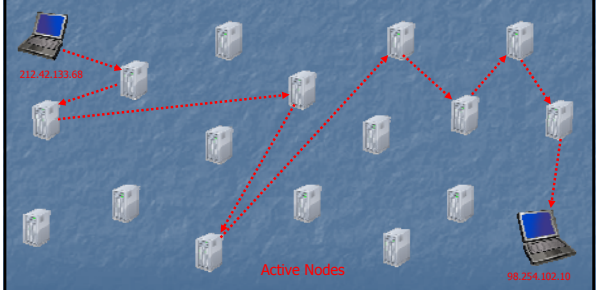
Internet Mining – Digging for Data



Internet Mining – Digging for Data



Internet Mining – Digging for Data



Internet Mining – Digging for Data

- IP version 4 (IPv4):
  - Fourth revision in IP development
  - The first widely deployed version
  - Provides data integrity via packet checksums
  - A "*Best Effort Delivery*" protocol - does not
    - guarantee data packet delivery
    - assure proper data packet sequencing
    - prevent duplicate packet delivery

Internet Mining – Digging for Data

+	Bits 0-3	4-7	8-15	16-18	19-31
0	Version	Header Length	Type of Service	Total Length	
32	Identification			Flags	Fragment Offset
64	Time to Live		Protocol	Header Checksum	
96	Source Address				
128	Destination Address				
160	Options				
160 or 192+	Data				

IPv4 Header Format

- IP version 6 (IPv6):
  - Developed in 1998 by Internet Engineering Task Force (IETF)
  - The next generation IP protocol for the Internet
  - Uses 128 bit addressing
  - Eliminates need for Network Address Translation
  - As of 2008 less than 1% penetration in any country
    - MAC OS X - 2.44%
    - Linux - 0.93%
    - Windows Vista – 0.32 %

IPv6 Header Format

Internet Addressing Comparison:

- IPv4
  - Sample address construction
    - 32 bit - 206.32.114.68
  - Maximum addresses
    - 4,294,967,296
- IPv6
  - Sample address construction
    - 128 bit - 2001:0f68:0000:0000:0000:0000:1986:69af
  - Maximum addresses
    - 340,282,366,920,938,463,463,374,607,431,768,211,456

Simple Comparison of IPv4 and IPv6:

Category	IPv4	IPv6
Worldwide Deployment	99% +	1% -
Addressing Space	32 bit	128 bit
Mathematical Expression	2^{32}	2^{128}
Address Capacity	4.3 Billion	340 Undecillion
Addressing Type	Decimal	Hexadecimal
Network Address Translation	Required	Not Required

- IPv4 = 4,294,967,296
- IPv6 = 340,282,366,920,938,463,463,374,607,431,768,211,456

Internet Addressing

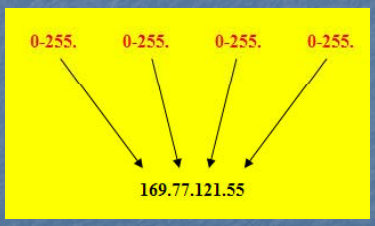
Ω

- Internet Addressing (IPv4)
  - Systems connected to the Internet must have unique addresses
  - Internet Protocol requires 4 byte numerical address (IP address) - referred to as "dotted decimal method" or an "octet"
  - Four-byte address comprised of two components:
    - Network component
    - Host component

192.168.040.10

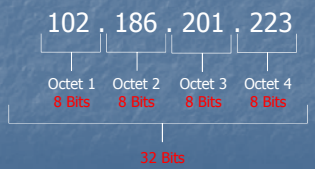
AAA.BBB.CCC.DDD

- 4 groups of 3 digits (32 bit addressing)
- Each group from 0 to 255
- Each group called an Octet (2^8)
- Normally written in a dotted quad notation
- Some values are reserved



BINARY IN BRIEF

- IP (v.4) Addresses are:
  - 32 bits in length
  - Composed of four "octets"
  - Each octet is 8 bits in length



Internet Mining – Digging for Data

Network Class:			
Class A	**1 – 126**	N.H.H.H	16.777.216
Class B	**128 - 191**	N.N.H.H	65.536
Class C	**192 - 223**	N.N.N.H	254
Class D	**224 - 239**	multicasting	
Class E	**240 - 255**	experimental	

NETWORK ADDRESSING

Internet Mining – Digging for Data

- Three major network classes:
  - **Class A** 1-126 1.0.0.0 – 126.0.0.0
    - 16.7 million addresses (hosts) per network.
  - **Class B** 128-191 128.0.0.0 – 191.255.0.0
    - 65,546 addresses (hosts) per network.
  - **Class C** 192-223 192.0.0.0 – 223.255.255.0
    - 254 addresses (hosts) per network

Internet Mining – Digging for Data

	Octet 1	Octet 2	Octet 3	Octet 4
Class A	001-126	0-255	0-255	0-255
Class B	128-191	0-255	0-255	0-255
Class C	192-223	0-255	0-255	0-255

NETWORK ADDRESSING

Indicates the identity of the network
Indicates the identity of a machine (Host) on that network

Reserved Private Network Ranges

So who is responsible for the management of Internet numbers?

Regional Internet Registry

- Manages the allocation and registration of Internet number resources within a particular region of the world.

Regional Internet Registries:

- African Network Information Centre (AfriNIC) for Africa
- American Registry for Internet Numbers (ARIN) for Canada, several parts of the Caribbean region, and the United States.
- Asia-Pacific Network Information Centre (APNIC) for Asia, Australia, and neighboring countries
- Latin American and Caribbean Internet Addresses Registry (LACNIC) for Latin America and parts of the Caribbean region
- RIPE NCC for Europe, the Middle East, and Central Asia

Internet Mining – Digging for Data

Regional Internet Registries

Internet Mining – Digging for Data

Internet Assigned Numbers Authority (IANA)

- Responsible for global coordination of:
  - DNS Root Zone
  - Global IP Address Allocations
  - Internet Protocol Name & Number Registries

Internet Mining – Digging for Data

So what's the relationship between IANA and the Regional Internet Registries?

- IANA delegates Internet resources to the RIR
- RIR's develop regional policies & delegate resources to their customers:
  - Internet Service Providers
  - End-user Organizations.

Addressing Schemes

- Static & Dynamic IP Addresses
  - Static IP Address
    - Never Changes
    - Used for Dedicated Connections
  - Dynamic IP Address
    - Assigned at Connection
    - From Available IP Pool
    - Remains "Static" until Disconnection
    - Obtained via Dynamic Host Configuration Protocol

Addressing Schemes

- Dynamic Host Configuration Protocol (DHCP)
  - Automated Assignment of
    - IP Addresses
    - Subnet Masks
    - Default Gateway
    - Other IP Parameters

Dynamic Host Configuration Protocol (DHCP)

- 3 Allocation Modes
  - Dynamic – "Leased"
  - Automatic *(DHCP Reservation)*
  - Manual

Internet Mining – Digging for Data

Internet Mining – Digging for Data

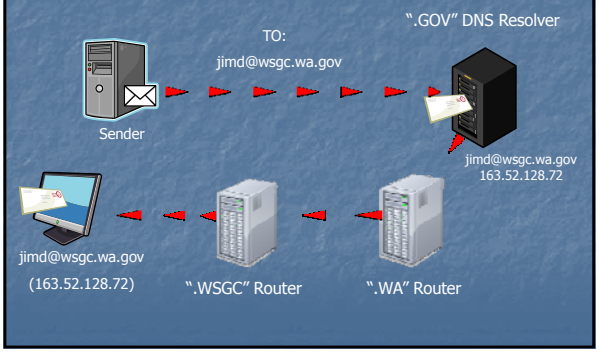
Email Addressing

- Made up of two parts

jimd @ wsgc . wa . gov

User Name Host Name TLD

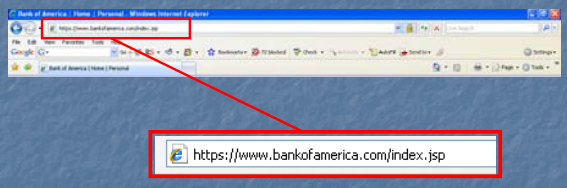
Internet Mining – Digging for Data



Secure Socket Layer Encryption

- Secure Socket Layer Encryption (SSL)
  - Message Transmission Security Protocol
  - Included in Internet Explorer and Netscape
  - Uses RSA Encryption & Authentication System
- Encryption
  - Occurs to two levels
    - Low – 40 – 56 bits
    - High – 128 to 256
    - Depends on client system and SSL Certificate

Secure Socket Layer Encryption



Ports

Internet Mining – Digging for Data

Ports

- Similar to doors in a building
- Different doors used for different purposes
- Ports:
  - identify which application the data is destined for and which application sent the data
  - allow different applications on the same computer to utilize network resources without interfering with each other
- There are 65,536 ports (0 thru 65,535)

Internet Mining – Digging for Data

Ports

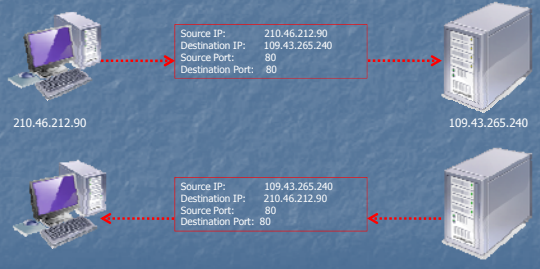
- TCP/IP utilizes a port numbering convention to separate each network function, such as e-mail and web browsing.
- Port numbering:
  - placed inside every IP packet
  - used by the sending and receiving systems to determine the packet destination.
- An IP address and port number together are referred to as a "socket"
  - Example – 210.125.105.226:80

Internet Mining – Digging for Data

Some common application ports:

Port 21 – File Transfer Protocol (FTP)
Port 22 – Secure Shell Protocol (SSH)
Port 25 – Simple Mail Transfer Protocol (SMTP)
Port 57 – Mail Transfer Protocol (MTP)
Port 80 – Hyper Text Transfer Protocol (HTTP)
Port 53 – Domain Name System (DNS)

Internet Mining – Digging for Data



Internet Mining – Digging for Data

Ports

- NETSTAT Command Line Utility
  - Displays which ports are open
  - Displays current connection

```
C:\>netstat_
```

Internet Mining – Digging for Data

QUESTIONS?

Time for a
Practical Demonstration

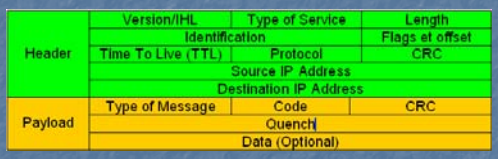
TCP/IP Utilities

Ω

- TCP/IP Utilities
  - Packet Inter-Network Groper (PING)
    - Used to test if Host is reachable
    - Sends *ICMP "echo request"
      - data packets sent to requested host
    - Listens for ICMP "echo response"
      - data packets returned from host

*Internet Control Message Protocol

Internet Mining – Digging for Data



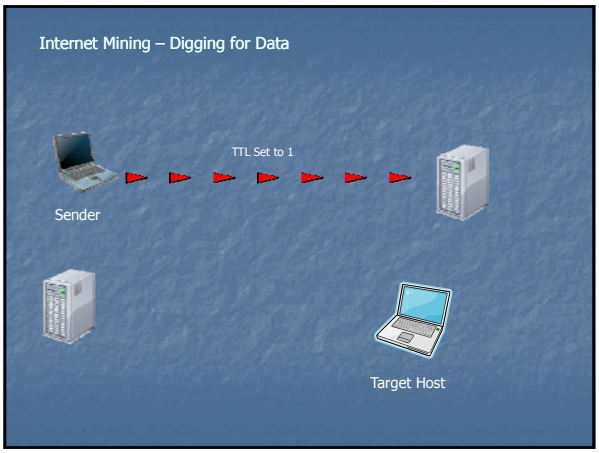
32 Bit "PING" packet

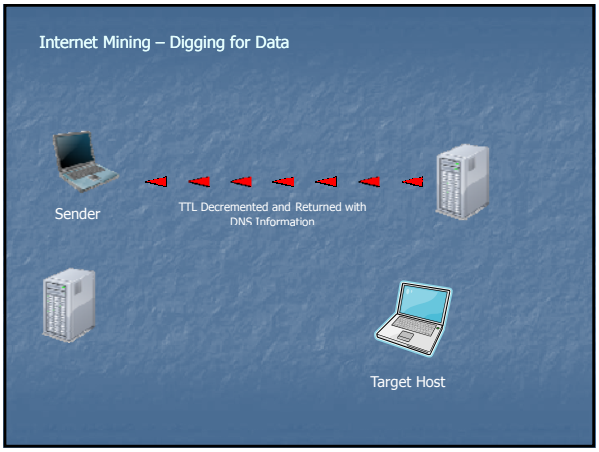
Internet Mining – Digging for Data

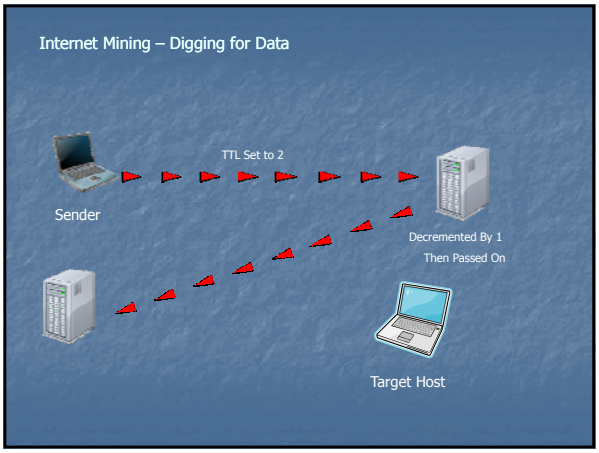
- Traceroute
  - Traces Data Packet Route
  - Internet Debugging Tool
  - Information Provided:
    - Number of Nodes/Routers Enroute
    - Time Between Nodes/Routers
    - Provides DNS Information

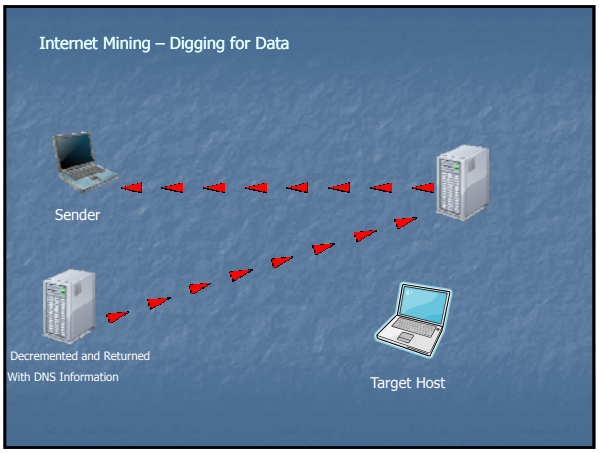
Internet Mining – Digging for Data

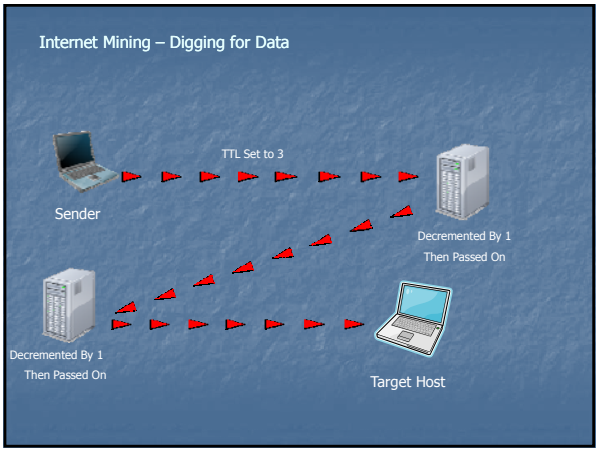
- Traceroute
  - Time To Live (TTL)
    - Number of Routers A Data Packet May Traverse
    - As Data Packet Traverses a Router
      - TTL Count is Decremented by 1
      - When Count Reaches Zero – Data Packet is Discarded
      - Error Message Sent to Sender

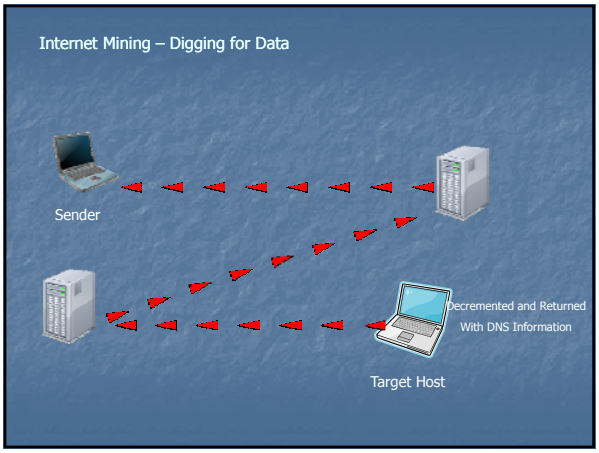

Internet Mining – Digging for Data
TTL Set to 1
Sender
Target Host


Internet Mining – Digging for Data
Sender
TTL Decremented and Returned with
DNS Information
Target Host


Internet Mining – Digging for Data
TTL Set to 2
Sender
Decremented By 1
Then Passed On
Target Host


Internet Mining – Digging for Data
Sender
Decremented and Returned
With DNS Information
Target Host


Internet Mining – Digging for Data
TTL Set to 3
Sender
Decremented By 1
Then Passed On
Decremented By 1
Then Passed On
Target Host

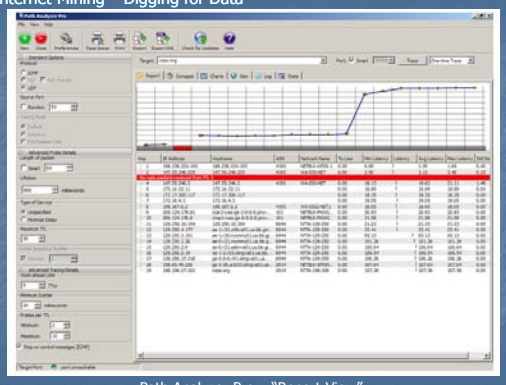

Internet Mining – Digging for Data
Sender
Decremented and Returned
With DNS Information
Target Host

Internet Mining – Digging for Data

Traceroute Tools

- TraceRoute
  - http://www.brothersoft.com/internet/miscellaneous/traceroute_10678.html
- VisualRoute
  - http://www.visualroute.com/
- Path Analyzer Pro
  - http://www.pathanalyzer.com/

Internet Mining – Digging for Data



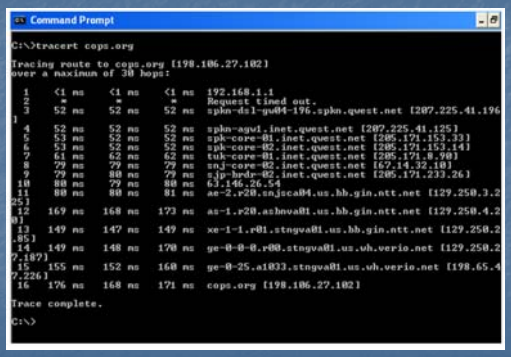
Path Analyzer Pro – "Report View"

Internet Mining – Digging for Data

Path Analyzer Pro – "Geographical View"

Tracert

- Tracert
  - Traceroute Utility
  - Designed for Windows
  - Run From
    - DOS Command Line
    - RUN Line
  - Enter "tracert" and
    - IP Address
    - Domain name



QUESTIONS?

Time for a
Practical Demonstration

Routing

How Computers Send Data Across the Internet

- Important hardware components
  - *Hubs*
    - Link groups of computers
  - *Bridges*
    - Link Local Area Networks (LAN)
  - *Gateways*
    - Translate data between networks
  - *Repeaters*
    - Amplify data traveling great distances
  - *Routers*
    - Ensure data packets arrive at destination

Routing

What's the difference between a Hub, Switch and Router?

Routing

- Hub
  - Connection point for devices in a network.
  - Commonly used to connect segments of a LAN.
  - Contains multiple ports.
    - When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets.

Routing

- Switch
  - Device that filters and forwards packets between LAN segments.
  - Keeps a record of the MAC addresses of all the devices connected to it.
  - Can identify which system is sitting on which port.
    - When a frame is received, it knows exactly which port to send it to without significantly increasing network response times.

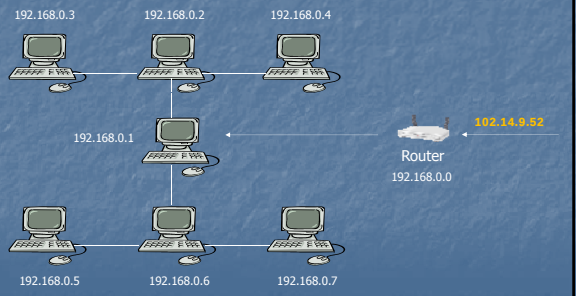
Internet Mining – Digging for Data

Routing

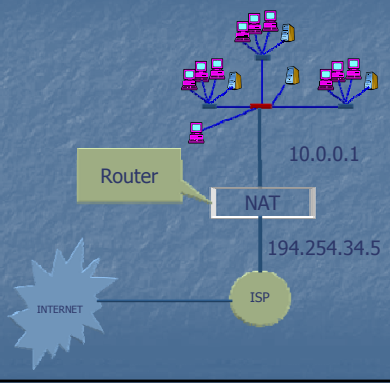
- Router
  - Device that forwards data packets along networks.
  - Connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP.s network.
  - Located at gateways, the places where two or more networks connect.
  - Use headers and forwarding tables to determine the best path for forwarding the packets
  - Use protocols to communicate with each other and configure the best route between any two hosts.

Internet Mining – Digging for Data

- What is the function of Routing?



Internet Mining – Digging for Data



Warriors of the Net

Ω

The Domain Name System

Ω

The Domain Name System

- Domain Name System (DNS)
  - Allows Use of Alphanumeric Characters
  - Known as "*Domain Name*"
  - www.cops.org is seen as 198.106.27.102
  - A "*mnemonic*" device
  - Distributed Database Contains
    - Host Name
    - IP Address
    - Routing Information

Internet Mining – Digging for Data

- Domain Name System (DNS)
  - *"Resolves"* Domain Names
  - Allows Users to Reach IP Addresses Using Domain Name
  - Is built on a hierarchical structure
  - Service is automatically provided during your login
  - Replaces an IP-address with a name for easy addressing

http://72.1.4.101 = http://iacis.com

Internet Mining – Digging for Data

Domain Name System

- Distributed Database
  - Originally consisted of 13 Root Servers
  - Now replicated over 200 Root Servers
    - Located Around The World
    - Spread Workload
    - Provide Data Redundancy
    - Contain IP addresses of all TLD Registries and Global Registries

Internet Mining – Digging for Data

Major DNS Root Name Servers

Internet Mining – Digging for Data

Current Root Server Locations

Internet Mining – Digging for Data

Root Server Operators

- A VeriSign Global Registry Services
- B Information Sciences Institute
- C Cogent Communications
- D University of Maryland
- E NASA Ames Research Center
- F Internet Systems Consortium, Inc.
- G U.S. DOD Network Information Center
- H U.S. Army Research Lab
- I Autonomica/NORDUnet
- J VeriSign Global Registry Services
- K RIPE NCC
- L ICANN
- M WIDE Project

Internet Mining – Digging for Data

Server	Operator	Locations	IP Addresses	AS Numbe
A	VeriSign, Inc.	**Sites: 4** Global: 4 Local: 0 **Los Angeles, CA, US; New York, NY, US *; Palo Alto, CA, US *; Ashburn, VA, US ***	IPv4: 198.41.0.4 IPv6: 2001:503:BA3E::2:30	19836
B	Information Sciences Institute	**Sites: 1** Global: 0 Local: 1 Earth	IPv4: 192.228.79.201 IPv6: 2001:478:65::53	none
C	Cogent Communications	**Sites: 6** Global: 6 Local: 0 **Herndon, VA, US; Los Angeles, CA, US; New York, NY, US; Chicago, IL, US; Frankfurt, DE; Madrid, ES**	IPv4: 192.33.4.12	2149
D	University of Maryland	**Sites: 1** Global: 1 Local: 0 **College Park, MD, US**	IPv4: 128.8.10.90	27
E	NASA Ames Research Center	**Sites: 1** Global: 1 Local: 0 **Mountain View, CA, US**	IPv4: 192.203.230.10	297

DNS Root Name Servers

Internet Mining – Digging for Data

F	Internet Systems Consortium, Inc.	**Sites: 49** Global: 2 Local: 47 Ottawa, Canada *; **Palo Alto, CA, US** *; San Jose, CA, US; New York, NY, US *; **San Francisco, CA, US** *; Madrid, ES; Hong Kong, HK; Los Angeles, CA, US *; Rome, Italy; Auckland, NZ *; Sao Paulo, BR; Beijing, CN; Seoul, KR *; Moscow, RU *; Taipei, TW; Dubai, AE; Paris, FR *; Singapore, SG; Brisbane, AU *; Toronto, CA *; Monterrey, MX; Lisbon, PT *; Johannesburg, ZA; Tel Aviv, IL; Jakarta, ID; Munich, DE *; Osaka, JP *; Prague, CZ *; Amsterdam, NL *; Barcelona, ES *; Nairobi, KE; Chennai, IN; London, UK *; Santiago de Chile, CL; Dhaka, BD; Karachi, PK; Torino, IT; Chicago, IL, US *; Buenos Aires, AR; Caracas, VE; Oslo, NO *; Panama, PA; Quito, EC; Kuala Lumpur, Malaysia *; Suva, Fiji; Cairo, Egypt; Atlanta, GA, US; Podgorica, ME; St. Maarten, AN *	IPv4: 192.5.5.241 IPv6: 2001:500:2f::f	3557
G	U.S. DOD Network Information Center	**Sites: 6** Global: 6 Local: 0 **Columbus, OH, US**; **San Antonio, TX, US**; **Honolulu, HI, US**; **Fussa, JP**; **Stuttgart-Vaihingen, DE**; **Naples, IT**	IPv4: 192.112.36.4	5927
H	U.S. Army Research Lab	**Sites: 1** Global: 1 Local: 0 **Aberdeen Proving Ground, MD, US ***	IPv4: 128.63.2.53 IPv6: 2001:500:1:803f:235	13

DNS Root Name Servers

Internet Mining – Digging for Data

I	Autonomica	**Sites: 34** Stockholm, SE; Helsinki, FI; Milan, IT; London, UK; Geneva, CH; Amsterdam, NL; Oslo, NO; Bangkok, TH; Hong Kong, HK; Brussels, BE; Frankfurt, DE; Ankara, TR; Bucharest, RO; Chicago, IL, US; Washington, DC, US; Tokyo, JP; Kuala Lumpur, MY; Palo Alto, CA, US; Jakarta, ID; Wellington, NZ; Johannesburg, ZA; Perth, AU; San Francisco, CA, US; Singapore, SG; Miami, FL, US; Ashburn, VA, US; Mumbai, IN; Beijing, CN; Manila, PH; Doha, QA; Colombo, LK; Vienna, AT; Paris, FR; Taipei, TW	IPv4: 192.36.148.17	29216
J	VeriSign, Inc.	**Sites: 70** Global: 63 Local: 7 **Dulles, VA, US (2 sites)**; Dulles, VA, US (1 sites); **Ashburn, VA, US ***; **Miami, FL, US**; **Atlanta, GA, US**; Seattle, WA, US; Chicago, IL, US; **New York, NY, US ***; **Honolulu, HI, US**; **Mountain View, CA, US (1 sites)**; Mountain View, CA, US (1 sites); **San Francisco, CA, US (2 sites) ***; **Dallas, TX, US**; **Amsterdam, NL**; **London, UK**; **Stockholm, SE (2 sites)**; **Tokyo, JP**; **Seoul, KR**; Beijing, CN; **Singapore, SG**; **Dublin, IE**; **Kaunas, LT**; Nairobi, KE; **Montreal, CA**; **Perth, AU**; **Sydney, AU**; **Cairo, EG**; Cairo, EG; **Warsaw, PL (2 sites)**; **Brasilia, BR**; **Sao Paulo, BR**; **Sofia, BG**; **Prague, CZ**; **Johannesburg, ZA**; **Toronto, CA**; **Buenos Aires, AR**; **Madrid, ES**; **Fribourg, CH**; **Hong Kong, HK (2 sites)**; **Turin, IT**; **Mumbai, IN**; **Oslo, NO**; **Brussels, BE**; **Paris, FR (2 sites)**; **Helsinki, FI**; **Frankfurt, DE**; **Riga, LV**; **Milan, IT**; **Rome, IT**; **Lisbon, PT**; **San Juan, PR**; **Edinburgh, UK**; **Tallin, EE**; **Taipei, TW**; **New York, NY, US ***; **Palo Alto, CA, US ***; **Anchorage, US**; **Moscow, RU**; **Manila, PH**; **Kuala Lumpur, MY**; **Luxembourg City, LU**; **Guam, US**; **Vancouver, CA**; **Wellington, NZ**	IPv4: 192.58.128.30 IPv6: 2001:503:C27::2:30	26415

DNS Root Name Servers

Internet Mining – Digging for Data

K	RIPE NCC	**Sites: 18** Global: 6 Local: 12 **London, UK ***; **Amsterdam, NL ***; **Frankfurt, DE**; Athens, GR *; Doha, QA; Milan, IT *; Reykjavik, IS *; Helsinki, FI *; Geneva, CH *; Poznan, PL; Budapest, HU *; Abu Dhabi, AE; **Tokyo, JP**; Brisbane, AU *; **Miami, FL, US ***; **Delhi, IN**; Novosibirsk, RU; Dar es Salaam, TZ	IPv4: 193.0.14.129 IPv6: 2001:7fd::1	25152
L	ICANN	**Sites: 3** Global: 3 Local: 0 **Los Angeles, CA, US ***; **Miami, FL, US ***; **Prague, CZ ***	IPv4: 199.7.83.42 IPv6: 2001:500:3::42	20144
M	WIDE Project	**Sites: 6** Global: 5 Local: 1 **Tokyo, JP (3 sites) ***; Seoul, KR; **Paris, FR ***; **San Francisco, CA, US ***	IPv4: 202.12.27.33 IPv6: 2001:dc3::35	7500

DNS Root Name Servers

Internet Mining – Digging for Data

What do Root Name Servers do?

- Publish the "root zone file"
  - Root Zone File created & edited by the Internet Assigned Numbers Authority (IANA)
  - Contains names and numeric IP addresses of authoritative DNS servers for all TLDs
  - The Root Zone File is at the apex of the hierarchical DNS distributed database

Example - in 2004 there were 258 TLDs supported by 773 different authoritative servers

Internet Mining – Digging for Data

Remember…

- No Internet traffic passes through Root Name Servers
- Most DNS information is cached in DNS servers
- When DNS servers do not have the requested cached DNS information, the Root Name Server is queried

122

Internet Mining – Digging for Data

Top Level Domains

- Internet Corporation for Assigned Names & Numbers (ICANN)
  - Responsible for assigning Internet Domain Names and web address since 1997
  - Ensures Universal Resolvability
  - Ensures Correct Name – IP Mapping
  - Accredits Domain name Registrars

Internet Mining – Digging for Data

ICANN

- Regulated by US Department of Commerce – National Telecommunications and Information Administration
- US will relinquish administrative oversight
- Seeking "multi-stakeholder" to assume oversight
- Contract expires September 2015

Internet Mining – Digging for Data

Top Level Domains

- Top Level Domain (TLD) Registry Organizations
  - Information About Domain Names Within TLD

Example:
http://www.cops.org – ".org" is the TLD

Internet Mining – Digging for Data

Top Level Domains

- .COM - Commercial organization
- .EDU - Educational site in the U.S.
- .GOV - Government agency in the U.S.
- .MIL - Military site in the U.S.
- .NET - Network site
- .ORG - Nonprofit organization

Internet Mining – Digging for Data

Top Level Domains

- TLDs with three or more characters are referred to as "generic" TLDs, or "gTLDs
- gTLD Types
  - Sponsored
  - Unsponsored

Internet Mining – Digging for Data

Top Level Domains

- "Sponsored" TLDs are assigned a sponsor representing the community most affected by the TLD
- "Unsponsored" TLD's operate under policies established by the global Internet community directly through the ICANN process.

Internet Mining – Digging for Data

"Sponsored" Top Level Domains

- .aero
- .travel
- .cat
- .xxx
- .coop
- .info
- .jobs
- .mobi
- .museum
- .post
- .int
- .edu
- .post
- .travel

Internet Mining – Digging for Data

"Unsponsored" Top Level Domains

- .org
- .net
- .com

Internet Mining – Digging for Data

Current List of Authorized TLD's

http://www.icann.or g/registries/top-level-domains.htm.

Internet Mining – Digging for Data

Top Level "Country Code" (cc) Domains

- .us United States
- .fr France
- .au Australia
- .cz Czech Republic
- .ca Canada

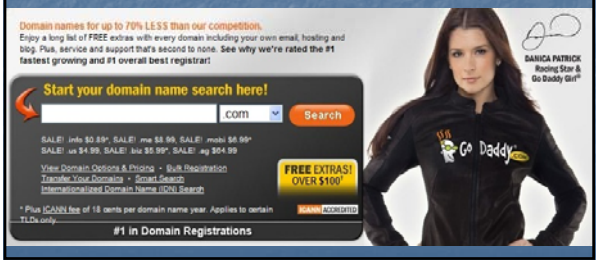
More than 230 country codes

Internet Mining – Digging for Data

How are domain names acquired?

Buy on-line:

www.godaddy.com – www.register.com – www.active-domain.com



Internet Mining – Digging for Data

Resolving a Domain

Many on-line tools available:

- Sam Spade
- DNS-Stuff
- Domain Tools
- Internic Whois

Internet Mining – Digging for Data

QUESTIONS?

Internet Mining – Digging for Data

WhoIs

Ω

Internet Mining – Digging for Data

- WhoIs
  - Internet-Based Utility
  - Provides Domain Record
    - Domain Owner's Name
    - DNS Information
    - Administrative Contacts
    - Technical Contacts

Internet Mining – Digging for Data

WhoIs

- Problems
  - Privacy
  - False Registrations
  - False Registration Information
  - Uncooperative Registrars
  - Information Timeliness & Inaccuracy
  - Historical Information Overwritten
  - Globalization

Internet Mining – Digging for Data

http://www.samspade.org

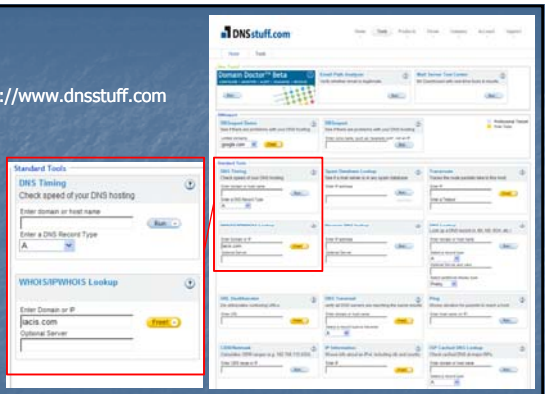
Internet Mining – Digging for Data

(Asked whois.safenames.net:43 about *betjamaica.com*)

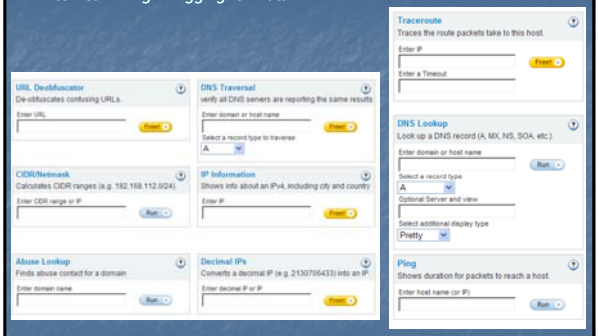
```
Safenames Whois Server Version 2.0
 Domain Name: BETJAMAICA.COM
   [REGISTRANT]
     Organisation Name: Olympic Sports Data Services
     Contact Name:      Sr. Webmaster
     Address Line 1:    1 Mangrove Way
     Address Line 2:
     City / Town:       Montego Bay
     State / Province:
     Zip / Postcode:    11111
     Country:           JM
     Telephone:         1 (876) 9536182
     Fax:               1 (0)
     Email:             webmaster-os@jadigiport.com

   [ADMIN]
     Organisation Name: Safenames Ltd
     Contact Name:      International Domain Administrator
     Address Line 1:    PO Box 5085
     Address Line 2:
     City / Town:       Milton Keynes MLO
     State / Province:  Bucks
     Zip / Postcode:    MK6 32E
     Country:           UK
     Telephone:         44 (19082) 00022
     Fax:               44 (19083) 25192
     Email:             hostmaster@safenames.net
```

http://www.dnsstuff.com



Internet Mining – Digging for Data



http://www.dnsstuff.com/

Internet Mining – Digging for Data

http://www.dnsstuff.com/

Internet Mining – Digging for Data

Registration Service Provided By: DOMAINCLIP
Contact: +1.6046388501
Website: http://www.domainclip.com

Domain Name: BODOG.COM

Registrant:
PrivacyProtect.org
Domain Admin ********@privacyprotect.org)
P.O. Box 97
Note - All Postal Mails Rejected, visit Privacyprotect.org
Moergestel
null,5066 ZH
NL
Tel. +45.36946676

Creation Date: 21-Feb-2000
Expiration Date: 21-Feb-2016

Domain servers in listed order:
anycast.bit2host.co.uk
anycast.bit2host.org
anycast.bit2host.net
anycast.bit2host.com
ns0.bit2host.com

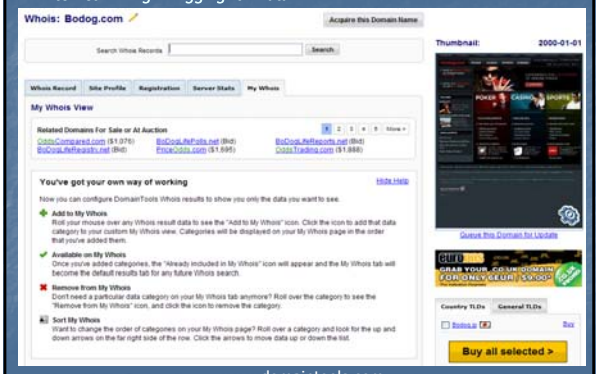
Administrative Contact:
PrivacyProtect.org
Domain Admin ********@privacyprotect.org)
P.O. Box 97
Note - All Postal Mails Rejected, visit Privacyprotect.org
Moergestel
null,5066 ZH
NL
Tel. +45.36946676

www.dnsstuff.com

Internet Mining – Digging for Data

www.domaintools.com

Internet Mining – Digging for Data



www.domaintools.com

Internet Mining – Digging for Data

www.domaintools.com

Internet Mining – Digging for Data

www.domaintools.com

Internet Mining – Digging for Data

www.domaintools.com

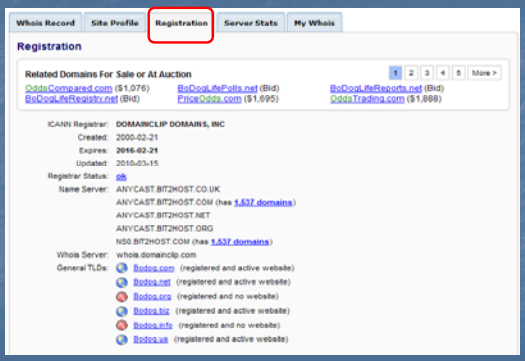
Internet Mining – Digging for Data

www.domaintools.com

Internet Mining – Digging for Data

www.domaintools.com

Internet Mining – Digging for Data

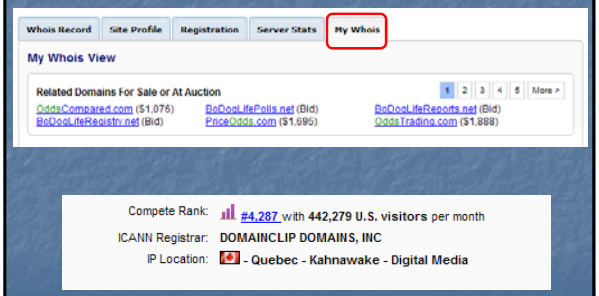


www.domaintools.com

Internet Mining – Digging for Data

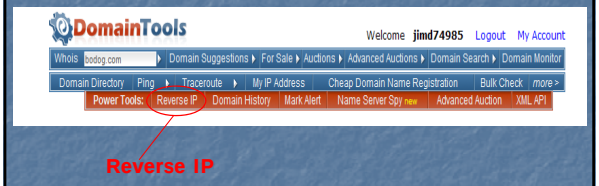
www.domaintools.com

Internet Mining – Digging for Data



www.domaintools.com

Internet Mining – Digging for Data



www.domaintools.com

Internet Mining – Digging for Data

www.domaintools.com

Internet Mining – Digging for Data

www.domaintools.com

Internet Mining – Digging for Data

QUESTIONS?

Internet Mining – Digging for Data

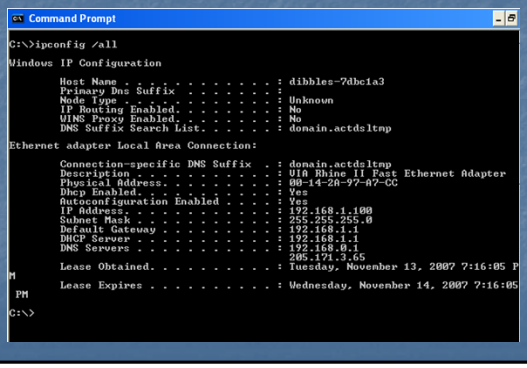
Time for a
Practical Demonstration

Diagnostic Utilities

Ω

Diagnostic Utilities

- Ipconfig
  - Command Line Interface
    - Displays TCP/IP Network Configuration Values
    - Refreshes DHCP Settings
    - Refreshes DNS Settings



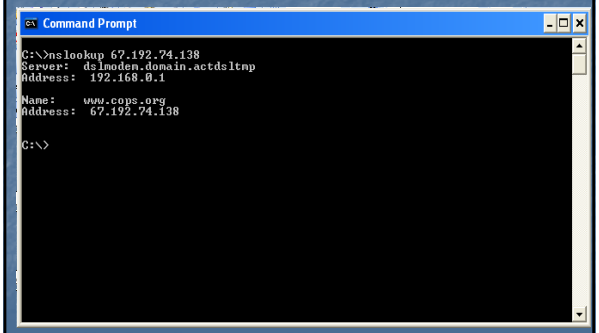
QUESTIONS?

Time for a
Practical Exercise

Diagnostic Utilities

- NSLookup
  - MS-DOS Utility
    - Look Up Domain/Host IP Address
    - External DOS Command

Internet Mining – Digging for Data



Internet Mining – Digging for Data

Time for a

Practical Demonstration

Internet Mining – Digging for Data

Internet Technology Video

Ω

QUESTIONS?