Washington State Gambling Commission

Internet Gambling & Cyber Crime Investigations

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



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

Internet Mining – Digging for Data

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

Internet Mining – Digging for Data

Transmission Control Protocol & Internet Protocol

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

- <u>TCP</u> divides data into packets containing information for error control and reassembly
- <u>*IP*</u> 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

Internet Mining – Digging for Data

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

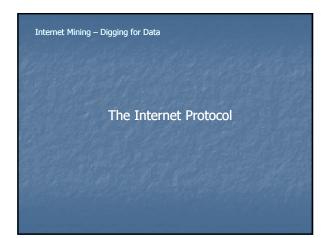
Internet Mining – Digging for Data

TCP Sequence Tracking

- Sequence number in the TCP header keeps track of the sent /received byte counts for the hosts $% \left({{{\rm{A}}_{\rm{B}}} \right)$
- 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

1	- Alter		all and and and		
Bit Offset	Bits 0-3	4.7	8-15	16-31	
0		Source		Destination Port	
32	Sequence Number				
64	Acknowledgment Number			it Number	
96	Data Offset		Reserved	Flags Window	
128		Check	sum	Urgent Pointer	
160		Options + Padding			
160/192+			Data		





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"

Internet Mining – Digging for Data

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

Internet Mining – Digging for Data

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

ModelsProtocols

Internet Mining – Digging for Data

Models:

- A concept of how something should work
- Let **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 <u>does</u> provide a solution
- A 'Ford Mustang' is an example of working solution

Internet Mining – Digging for Data

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

Upper Layers:

- Application specific functions (data format, encryption, connection management)

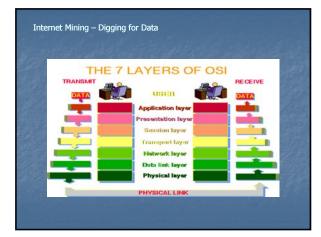
 - 7. Application
 6. Presentation
 5. Session

Internet Mining – Digging for Data

Lower Layers:

- Network specific functions (routing, addressing)
 4. Transport
 3. Network

 - 2. Data link
 - 1. Physical





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

(DSI Model	TCP/IP Model			
Арр	lication		нттр	FTP	
Pres	entation	Application	HILE	FIF	
Sess	ion		Sockets		
Trar	nsport	Transport	TCP	UDP	
Net	work	Internet	ICMP I	ARP	
Data	i Link	Network Interface			
Phys	ical	Hethork interface	╔┲╪╤╤┲┹┙		
12					
		OSI and TCP/IP			



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

Internet Mining – Digging for Data

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.

Internet Mining – Digging for Data

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"

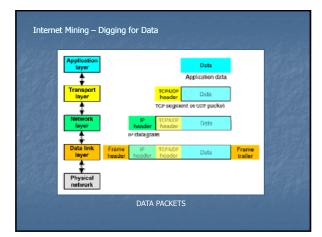
Internet Mining – Digging for Data

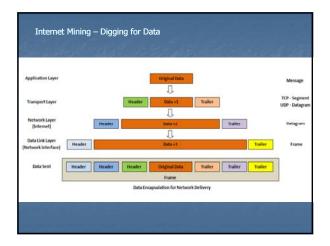
How does a Protocol Stack Work?

- 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 is a packet-switched network
- Information transmitted via data packetsLong 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"

Step 1:

A document is prepared

Receiving host reassembles fragmented datagram in correct order.

Internet Mining – Digging for Data

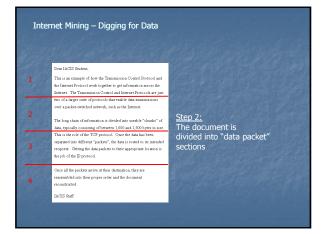
Dear IACIS Student,

Dear JACRS Swaterst. This is an example of how the Transmission Control Protocol and the Internet Protocol work cognitient to get information across the Internet. The Transmission Control and Internet Protocols are just two of a larger rule of protocols that anothe data transmissions over a padoet-switched network, such as the Internet.

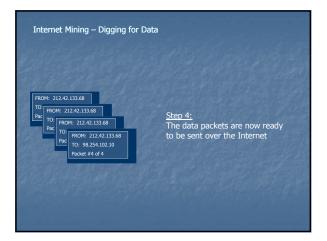
The long chain of information is divided into usuable "chouds" of data, typically consisting of between 1,000 and 1,500 bytes in size. This is the role of the TOP protocol. Once the data has been reparated into different "packets", the data is round to its intended required. Getting the data packets 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.

LACIS Staff



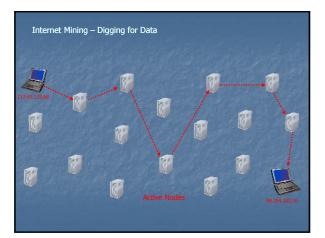


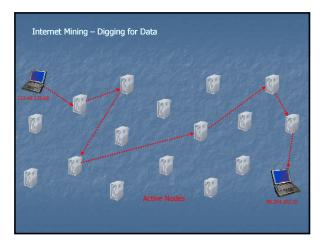


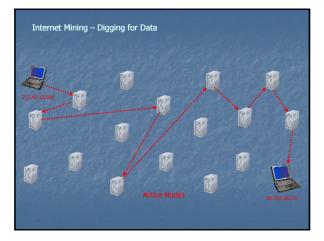
Packet transmission route is dependant upon:

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

"Like electricity – takes the path of least resistance"







- 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

+ Bits	0-3	4-7	8-15	16-18	19-31
0 Ver	sion	Header Length	Type of Service		Total Length
32	_	Identific	ation	Flags	Fragment Offset
64	Time to Live Protocol		Header Checksum		
96	Source			Address	
128	Destina			n Address	
160	Options				
160 or 92+	Data				



- 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 %

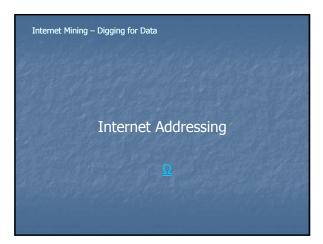
+	Bits 0-3	4-11	12-15	16-23	24-31	
0	Version	Traffic Class		Flow Label		
32		Payload Length		Next Header	Hop Limit	
64						
96		Source Address				
128			Source	Address		
160						
192						
224			Destination			
256			Destination	Address		
288						
-	-	The second second second	and the states of	to a setter country		

- Internet Addressing Comparison: Internet Act • IPv4 - Sample address construction • 32 bit - 206.32.114.68 - Maximum addresses • 4,294,967,296
- - 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	232	2128
Address Capacity	4.3 Billion	340 Undecillion
Addressing Type	Decimal	Hexadecimal
Network Address Translation	Required	Not Required

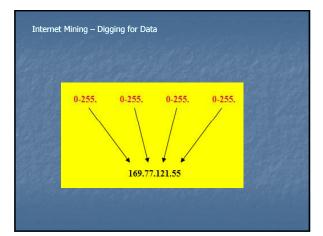
IPv4 = 4,294,967,296
IPv6 = 340,282,366,920,938,463,463,374,607,431,768,211,456

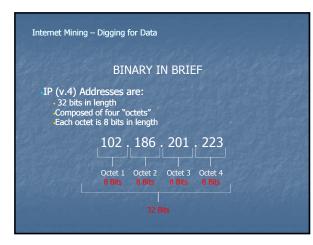


- Internet Addressing (IPv4)
 - Systems connected to the Internet must have unique addresses
 - Internet Protocol requires 4 byte numerical address (IP address) referred to as "dotted decimal method" or an "octet"
 - Four-byte address comprised of two components:
 - Network component
 - Host component

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 (2⁸)
 Normally written in a dotted quad notation
 Some values are reserved





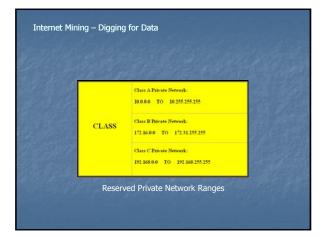
Network	Class:		
Class A	1 – 126	N.H.H.H	16.777.216
Class B	128 - 191	N.N. 8. 8	65.536
Class C	192 - 223	N.N.N.	254
Class D	224 - 239	multicasting	A the
Class E	240 - 255	experimental	

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

	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







So who is responsible for the management of Internet numbers?

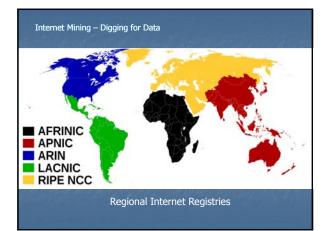
Regional Internet Registry

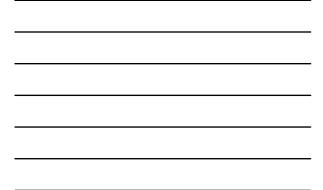
 Manages the allocation and registration of Internet number resources within a particular region of the world.

Internet Mining – Digging for Data

Regional Internet Registries:

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





Internet Assigned Numbers Authority (IANA)

Responsible for global coordination of: DNS Root Zone

- Global IP Address Allocations
- Internet Protocol Name & Number Registries

- 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 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

Internet Mining – Digging for Data

Addressing Schemes Dynamic Host Configuration Protocol (DHCP)

- Automated Assignment of

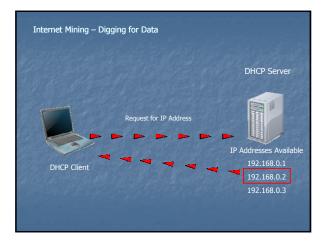
 - IP Addresses
 Subnet Masks
 Default Gateway
 - Other IP Parameters

Internet Mining – Digging for Data

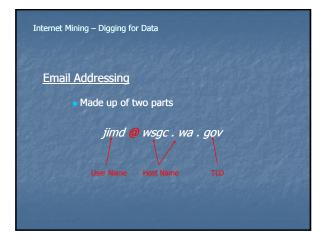
Dynamic Host Configuration Protocol (DHCP)

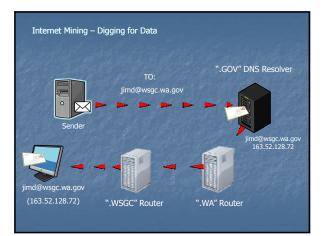
- 3 Allocation Modes

 - Dynamic "Leased"
 Automatic (DHCP Reservation)
 - Manual









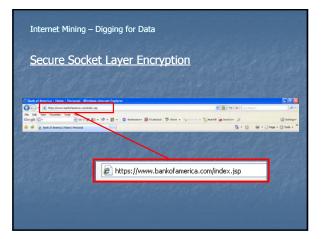


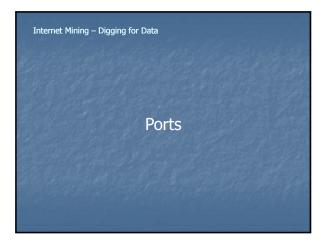
Secure Socket Layer Encryption

- 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





Ports

- Similar to doors in a building
- Different doors used for different purposes Ports:
- 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

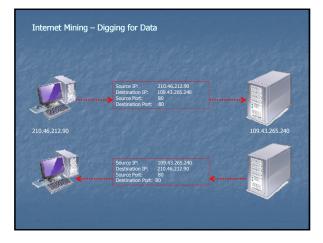
TCP/IP utilizes a port numbering convention to separate each network function, such as e-mail and web browsing.

- 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)





Ports

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

C:∖>netstat_

Internet Mining – Digging for Data

QUESTIONS?





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

	Version/IHL	Type of Service	Length
Header	Identific		Flags et offset CRC
	Time To Live (TTL)	Protocol Source IP Address	CRC
	Destination IP Address		
	Type of Message	Code	CRC
Payload		Quench	
		Data (Optional)	
	32 Bit `	'PING" packet	

 _
 _

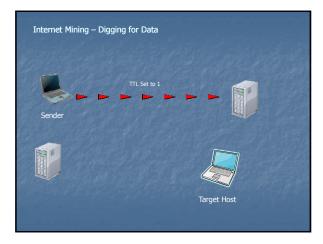
Traceroute

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

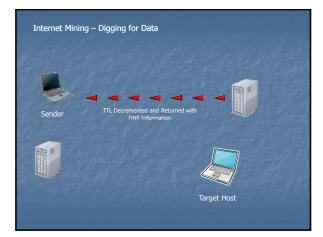
Internet Mining – Digging for Data

Traceroute

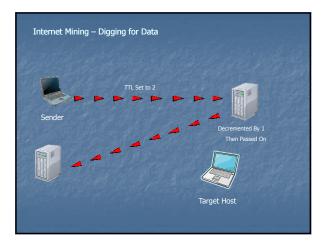
- Time To Live (TTL)
 - Number of Routers A Data Packet May Traverse
 - As Data Packet Traverses a Router
 - TTL Count is Decremented by 1
 - When Count Reaches Zero Data Packet is Discarded
 Error Message Sent to Sender

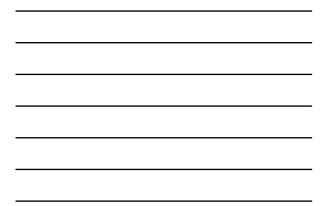


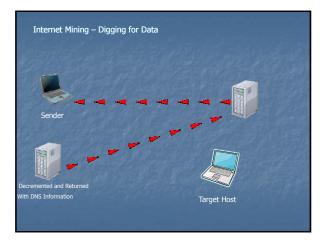




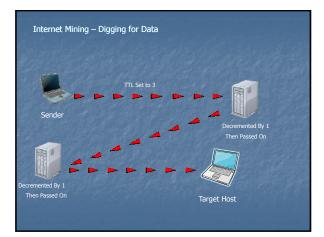




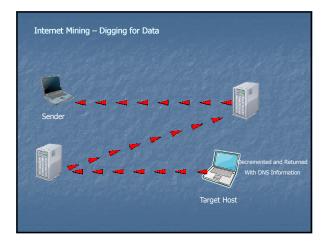














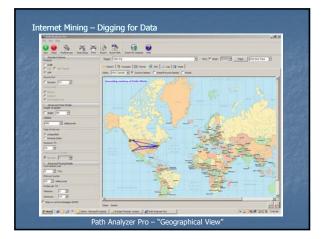
Traceroute Tools

- TraceRoute

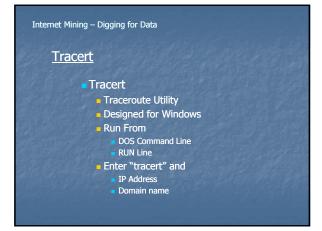
 http://www.brothersoft.com/internet/miscellaneous /traceroute_10678.html
- VisualRoute
 http://www.visualroute.com/
- Path Analyzer Pro
 http://www.pathanalyzer.com/

Real Andrew Pro											-
	S B COST	10. O									
the line induces further to	Tates a	HT Caste									
C. Device Links		[reprint g			*	no U	Sand Free	÷.	ter 115		1
C 104	1	1.0.0	3 (here 9 (here 11 (h	1-1-							
P to Farmer	1000	1.3 2499 13	Contract de las las se	108.0	and I						-
laura feit							P	-			
F April 10 11				-				-			
Tang Sub				-		- 1		-		_	
# Salar						\pm		-			
P rotates in				-				-			
Adverse mide factor		In assess	Index	famil		1.0		1000	1	1000	and the second
C test [rs = +1]	100	108 178 174 101	100.210.220.200	****	Interest Name	4.44	0.44	- James	- Ingine	1.44	
Links		10110-0020	147.03.246.020	430	NACCONT.		. 18	A	3.0	1.9	2.1
fee Historia	1.1	107.10.246.2	54735.54.5 (71.)A (0.1)	400	84.00 MT	6.00	16.15	1	18.42	71.11	- 2
Tax of Dente	100	175 17 366 227	175.17.306.107			10	14.76	-	18.76	8.0	
a second	1.00	106.107.6.2 206.104.106.01	101.0073.0 (1073+04.00.000.000.000	1446	INTERACTORY AND A	1.00	8.0		26.45	20.00	100
C reana tear	128	205.104.08.8	2000 1 1001 (pt () () () () (pt ())	-	WHAT PART	100	21.86		N.M.	21.00	1
Reptile 11.		108.20E.4.(19	An U.Y. official Continues		175-05-01	100	84	1.1	4 10.17	10.40	
1 2	- 12	10,000,000,000	and () Looped Links	1041	1079-029-030	-18-	10.00		COLUMN TAXABLE	10.0	
P	118	100,000,00	ar 12/11-mp all also.	-	NT16 525 216 NT16 128 210	1.00	18.14		10.3	35.54	÷
attended have breek	- 6	100.45.05.20	print Mattillergraftin		TO DRIVE	10	10.0		Canal:	10.00	
NUM BARLING	100	100-200-27-012	ode ad	26.04	122.08.08	14	10.00		Contraction.	20.8	
1 32 754											
Henry Links											
a di site per											
Andread and The											
Name (1 d)											
Parameter 1 w 121											
a bell in comparison brand	at in										

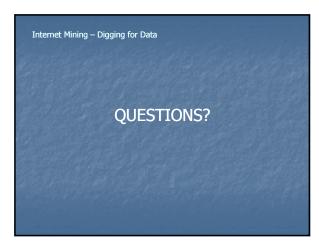




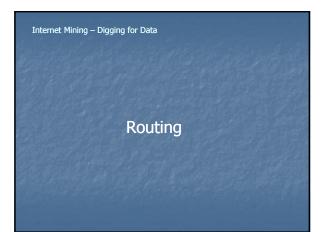




60 Co	mmar	nd Pre	ampt				
C:\>t	race	rt c	ops.o	rg			
Traci over						198.	186.27.1821
123		ns ns		ns ns	<1 # 52	ns.	192.168.1.1 Request timed out. spkn-ds1-gw04-196.spkn.gwest.net [207.225.41.19
1							
4	52 53	PIG PIG	52 52	PIG PIG		RS DS	spkn-agw1.inet.quest.net [207.225.41.125] spk-core-01.inet.guest.net [205.171.153.33]
6	53	115	52	ms	52	115	spk-core-02.inet.gwest.net [205.171.153.14]
2	61	n=	62				tuk-core-01.inet.quest.net [205.171.8.90]
8	29 29	ns ns	79 80	PIS DIS		R 5	sip-brdr-02.inet.quest.net [67.14.32.10]
10		PIG N				RS RS	53.146.26.54
4567898111		ns.	80	ns	81		ae-2.r20.snjsca04.us.hb.gin.ntt.net [129.250.3.
12	169	ns	168	F10	173	85	as-1.r20.asbnva81.us.bb.gin.ntt.net [129.250.4.
13	149	ns	147	ns	149	ns	xe-1-1.r01.stngva01.us.bb.gin.ntt.net [129.250.
14	149	ns.	148	ns:	178	ns	ge-0-0.r00.stngva01.us.wh.verio.net [129.250.
15	155	ns	152	ns	168	ns	ge-0-25.a1033.stngva01.us.wh.verio.net [198.65.
16	176	115	168	ns:	171	R S	cops.org [198.186.27.182]







How Computers Send Data Across the Internet

- Important hardware components

 - Hubs
 Link groups of computers
 - Eink 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?

Internet Mining – Digging for Data

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.

Internet Mining – Digging for Data

Routing

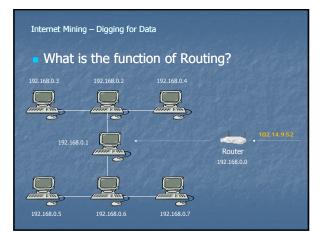
Switch

- 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.

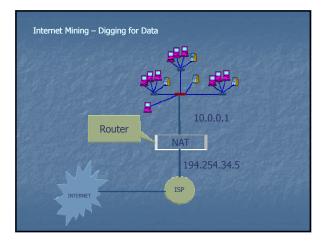
Routing

Router

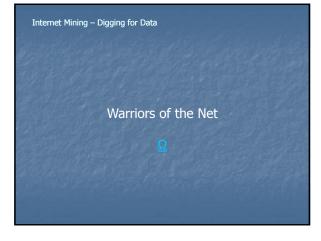
- Device that forwards <u>data packets</u> along networks.
- Connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP.s network.
 Located at gateways, the places where two or more networks connect.
- Use headers and forwarding tables to determine the best path for forwarding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

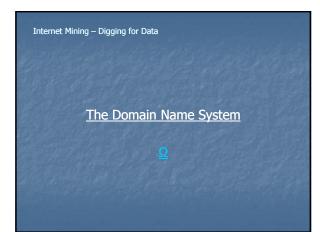












The Domain Name System

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

- 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

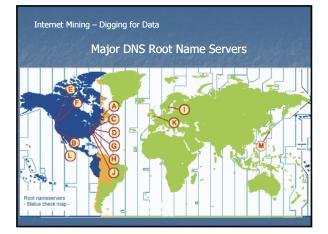
http://72.1.4.101 = http://iacis.com

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







- 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

Server	Operator	Locations	IP Addresses	AS Numb
A	VeriSign, Inc.	Sites: 4 Genet 4 Lond 4 Lond 5 Los Angeles, CA, US, New York, NY, US *; Palo Alto, CA, US *; Athlore, VA, US *	IP+4: 198.41.0.4 IP+6: 2001:503 BA3E-2:30	19836
В	Information Sciences Institute	Sites: 1 Grout 1 Local 1 Earth	IPv4: 192.228.79.201 IPv6: 2001:478:65:53	1057
2	Cognit Communications	Silenes 6 Chebd 8 Lood 0 Herrados, V.A., US, Los Angeles, C.A., US, New York, NY, US, Chicago, IL, US, Frankført, DE, Madrid, ES	IPv4: 192 33.4.12	2149
D	University of Maryland	IPv4: 128.8-10.90	27	
E	NASA Ames Research Center	Sites: 1 Grobal : Leoil 3 Mountain View, CA, US	IPv4: 192 203 230.10	297



_		장소가 그렇는 것 옷을 내 좋아요? 가지 못	Section and a section of the	
E	Internet Systems Consortium, Inc.	Sines: 40 Gold 2 Lond 7 Onema, Canada *, Palo Alin, CA, US *, San Jose, CA, US, New York, NY, US *, San Francisco, CA, US *, Madda ES, Hong Kong, JK, Lu Angdrei, CA, US *, Sonen, July *, Andrain, X.Y. *, Sao Pando, S.B. Briging, CN, Sond, KR *, Macrow, RJ *, Tapier, TW, Dohi, AL Pani, F. *, Sanguere, S.G., Binhara, A.Y. *, Transien, CA *, Matterny, MY, Labou, PT *, Johannesherg, ZA, Tel Avie, Li, Jakara, D, Manish, De Narich, KE: Common N, London, UK *, Santano A, Chal, CL, Dhaka, BD, Karach, PK, Torion, TD, Nadon, UK *, Santano A, Chal, CL, Dhaka, BD, Karach, PK, Cohno, D, London, UK *, Santano A, Ara, AR (Santan, WC, Gab, Yo, *, Panna, PA, Queda, EC, Kuaha, Languer, Malgrain *, Son, Fig. Care, Egypt, Adanta, GA, US, Podgerien, ME; S. Materna, MY	Dv4:192.5.5.241 Dv6:2001500.2Ff	3557
Q	U.S. DOD Network Information Center	Sites: 6 Goold 5 Lead 9 Load 9 Sturtgart Valdingen, DE, Najdes, IT JP, Sturtgart Valdingen, DE, Najdes, IT	IPv4: 192 112 36.4	5927
Н	U.S. Anny Research Lab	Sites: 1 Gabat 1 Leek 9 Aberdeen Proving Ground, MD, US *	IP+4 128 63 2 53 IP+6 2001:500.1:803/235	13



Autonomica	Sites: 34	IPv4: 192.36.148.17	29216
	Stockhan, S.F. Holiak, T. Man, T. London, T.K. Gorres, C.L. Kanorkow, N., Ook, N.D. Bandon, T.H. Hou Kon, R.K. Burnoto, B.E. Franker, D.E. Andone, T.R. Bucharer, R.D. Cheng, E., U.S. Walkagno, D.C.U.S. 75, 609, J. Kunki Langer, A.Y. Perk Abe, C.A. U.S. Jakars, D. Wangano, N.Z. Jahanesherz, Z.A. Ferli, A.U. San Francisco, C.A. U.S. Singarov, S. O. Mana, F.J. U.S. Adam, Y.A. U.S. Manthai, N.J. Boling, C.N. Manh, FH, Daha, Q.A. Colondo, L.K. Yenna, A.T. Fan, J.R. Tang, T.W.		
VerSign, Iac	Ster, 70 Gate at Lond 7. Daller, VA, US (2 alres); Daller, VA, US (1 alres); Askhure, VA, US "A Maniel, FL, US, VE, Ster, KA, US, Serfael, WA, US, Changa, E, US (2) alres); A matter Merr, AC, US (1 alres); San Francisco, CA, US (3 alres); Dallar, TX, US, Anterefans, NL, Landes, TK, Sternickall, GJ (2 alres); Tabox, PS, Benly, CC, Michael Perril, AU; Syshery, AK, Caris, EG, Caso, LO, Wortzer, PL, G alres); Benna, CA, Benna, Alexa, AE, San KA, Ballar, CA, San Perril, AU; Syshery, AK, Caris, EG, Caso, LO, Wong, CA, Hang, KK, Ballar, Danna, Alexa, AR, Matrid, JS, Fridward, CA, Hang, KK, Ballar, Danna, Alexa, AR, Matrid, JS, Fridward, CA, Hang, KK, Ballar, Danna, AR, San Kan, BA, San, CA, Son, No, No, Benna, LE, Tapier, WK, Norko, NY, San San, Alexa, Ballar, VA, Mian, TE, Fange, TK, and Nork, PH, Kalalarappe, MY, Landwardge (C), UL, Conn, CS, Vancerver, AC, Wellington, MY, Landward (C), MA, Conn, CS, Vancerver, AC, Wellington, MY, Landward (C), MA, Conn, CS, Wallerger, CA, Wellington, MY, Landward, CA, Wallerger, CA, Wellington, CA, Wellington, CA, Wellington, MY, Landward, CH, MA, Cann, CS, Wallerger, CA, Wellington, MY, Landward, CH, MA, Cann, CS, Wallerger, CA, Wellington, MY, Landward, CH, MA, Cann, CS, Wallerger, CA, Wellington, MY, Landward (C), MA, Canna, CS, Wallerger, CA, Wellington, MY, Landward, CH, MA, Canna, CS, Wallerger, MA, Wallerger, MA, Landward, CH, Wellington, CS, Wallerger, CH, Wellington, CH, Changer, CH, CH, Changer, CH, CH, Changer, CH, CH, CH,	IPv6 192 55 125 30 IPv6 2001503 C27:230	26415



	RIPE NCC	Ster: 18 Ook of 3 Landes, UK *, Amsterdan, NL *, Frankfurt, DE, Aftens, GR *, Doha, OA, Milan, T *, Roykjark, IS *, Holiniki, FF *, Genera, CH *, Penam, PL, Badgerst HU *, Abn Doha, KL Tadya, JP, Beitham, AU *, Miani, FL, US *, Delih, NJ, Novebrick, RJ, Dare Shan, TZ	IPv4: 193.0.14.129 IPv6: 2001.768:1	25152
-	ICANN	Sites: 3 Gobd: 1 Local 9 Los Angeles, CA, US *; Minni, FL, US *; Prague, CZ *	IPv4: 199.7.83.42 IPv6: 2001:500:3:42	20144
U	WIDE Project	Sites: 6 Galad: 5 Lond 1 Tokyo, JP (3 sites) *; Soud, KR; Paris, FR *; San Francisco, CA, US *	IPv4: 202.12.27.33 IPv6: 2001:dc3::35	7500



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

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

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

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

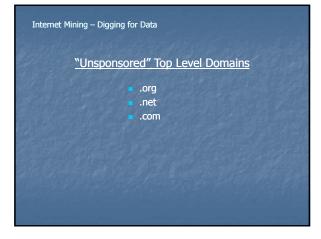
Top Level Domains

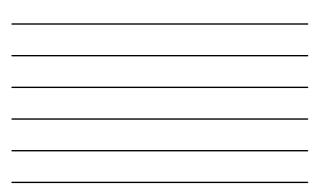
- "Sponsored" TLDs are assigned a sponsor representing the community most affected by the TLD
- "Unsponsored" TLD's operate under policies established by the global Internet community directly through the ICANN process.

Internet Mining – Digging for Data

"Sponsored" Top Level Domains

aero	 .mobi
.travel	.museum
.cat	.post
.XXX	int .
coop	• .edu
.info	.post
 .jobs 	.travel





Current List of Authorized TLD's

<u>http://www.icann.or_g/registries/top-level</u> domains.htm**.**

Internet Mining – Digging for Data

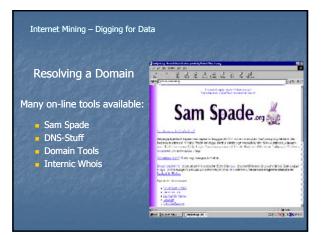
Top Level "Country Code" (cc) Domains

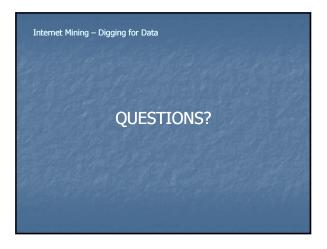
- .us United States
- .fr France
- au Australia
- .cz Czech Republic
- .ca Canada

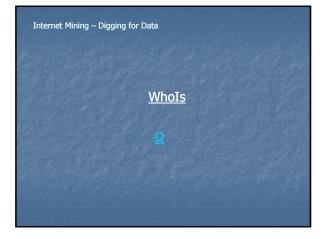
More than 230 country codes

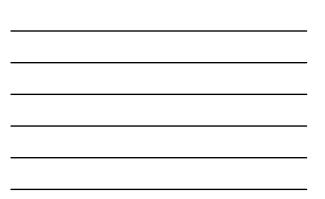












WhoIs

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

Internet Mining – Digging for Data

<u>WhoIs</u>

Problems

- Privacy
 False Registrations
- False Registration Information
- Uncooperative Registrars
- Information Timeliness & Inaccuracy
- Historical Information OverwrittenGlobalization

30 · x - treating	State (1971) All State States
File 621 New Facebox Socia Nels 2 Ar Mitchen Con Socia (2011) (March New Profile	No. None Cancer Hill Nove . (2 + 12 + 16, 16, 12 + 7 22)
👷 Fauritan 🦷 🗿 Sugarad Star. I 🚇 Qualities on 🖉 Pauritade 3978 Ø Sarliade og	the Pinn Pinn Pinn has been Pinn been by the the Carlo Alter \cdot , $b_{i} \in \underline{\mathbb{C}} 0 \Rightarrow b_{i} + b_{i} + b_{i} + b_{i}$
Whois	Spade.org
heljenaca certi	
Status	
We're running a new code bane, wik Bile code skared with the previous how Need to make DNS quester? Check smal Mackkes? Take a look of <u>emakte</u>	entrins. You night see perfolions: If so, you can probably work out where to report them to films



(Asked whois safenames net 43	about betjamaica.com)
18163	
Safenames Whois Server	
[REGISTRANT]	ALCON
	Olympic Sports Data Services
Contact Name:	Sr. Webmaster
Address Line 1:	1 Mangrove Way
Address Line 2:	and the second
City / Town:	Montego Bay
State / Province:	
Bip / Postcode: Country:	11111
	1 (876) 9536182
Pax:	1 (0)
Email:	webmaster-os8jadigiport.com
(ADMIN)	
Organisation Name:	
	International Domain Administrator
Address Line 1:	PO Box 5085
Address Line 2:	
	Milton Reynes MLO
	Bucks
Zip / Postcode:	MK6 32E
Country:	UK 44 (19082) 00022
Telephone: Fax:	44 (19082) 00022 44 (19083) 25192
Fax: Enail:	<pre>44 (19083) 20192 hostmaster@safenames.net</pre>





Internet Mining – D	igging for Data	
No. State of State	Sale and	Traceroute Traces the route packets take to this host. Enter P Enter a Timeout
URIL Deobhuscator De-obhuscates confusing URLs	ONS Traversal verify all DNS servers are reporting the same results	
free (R)	Enter somen an heat name	DNS Lookup Look up a DNS record (A, MX, NS, SOA, etc.) Enter domain or host name
CIDR/Netmask Calculates CIDR ranges (e.g. 192 198, 192 294) Itmr CDR range or P	IP Information Shrives into about an IPv4, including city and country Draw P	Select a record type A V Optional Server and view Select additional deplay type Pretty V
Abuse Lookup Finds abuse contact for a domain Enter domain name	Decimal IPs Converts a decimal IP (e.g. 2130706433) into an IP. Enter tecner IP or IP Total Converts on the IP of IP Total Converts on the IP Total Converts o	Ping Shows duration for packets to reach a host. Enter host name (or P)
	http://www.dnsstuff.com	



hanced Tools					
op Level Domain Lookup	٢	SSL Examination	۲	Web Site HTTP Headers	۲
Enter Dimain		Enter Donain or P		Enter Watada URL	
Contraction of the Contraction	Aur -	Child Contail in P	(he -	Line website one	Ren D
SN Information	۲	Find Nearby IPs	•	SPE	٢
Siter Name, ASN or IP		Error P.		E-mail Address(or domain or SPF string)	
	Arr. (*)	1	(Aut)	P nails carrieg from	Rin •
IAC Address	۲	Zone File Dump	۲	RFC4193 Local IPv6 Range Gene	
Inter MAC address		Enter Donas		Generates an 'almost unique' local IP range, per RFC4193	v6 address
THE DAL BOURSE	(Ref.)	Enter Jonan	(Ret O		Bet (+)
					- C
		and the second second		1	



Internet Mining – Digging for Data	Creation Date: 21-Feb-2000 Expiration Date: 21-Feb-2016
Registration Service Provided By: DOMAINCLIP Contact: +1.6046388501 Website: http://www.domainclip.com Domain Name: BODOG.COM	Domain servers in listed order: any cast.bit2host.co.uk any cast.bit2host.org any cast.bit2host.ord any cast.bit2host.com ns0.bit2host.com
Registrant: PrivacyProtect.org Domain Admin ************************************	Administrative Contact: PrivacyProtect.org Domain Admin *******@privacyprotect.org) P.O. Box 97 Note - AI Postal Mails Rejected, visit Privacyprotect.org Moergestel null,5062 ZH NL Tel. +45.36946676
www.dnss	tuff.com







Whois: Bot	log.com				Acquire the	s Domain Name		
	Search little	a Records			Search		Thumbnail:	2000-01-0
Whois Record	Site Profile	Registration	Server Stats	my Wheth				-
My Whois Vi	***						X	
OstsCompar	ains For Sale or ad.com (\$1,076 ostrunet (Bid)	BoDog	hePola.net (Bid) Ia.com (\$1,695)		E E E +	8 Mark +		
		ay of workin				HideHelp		
Add to M Roll your category	y Whois mouse over an	Whois result da		to My Whole" ici	ou want to see. on. Click the icon to add or My Whois page in the		Gueve the Do	@
Once you			ty included in My are Vilhola search		appear and the My Who	s tab will	CHED CONTRACT	
Dontnee			our My Whois tab Ne icon to remove		over the category to see		Par robusta Register	neral ILDs
	hange the order				category and look for th ap or down the list.	e up and		Ber







Internet Mir	ing – Digging for Data
/hois Record Site	Profile Registration Server Stats My Whois
Vhois Record	
Related Domains For	Sale or At Auction
OddsCompared.com BoDogLifeRegistry.ne	
Registrant Search:	"PrivacyProtect.org" owns about 3,004 other domains
Email Search	contact@privacyprotect.org is associated with about 1,106,903 domains
Registrar History	3 registrars
NS History:	8 changes on 5 unque name servers over 6 years.
P History:	5 changes on 4 unique name servers over 5 years.
Whois History:	1.259 records have been archived since 2003-01-21.
Reverse IP:	4 other sites hosted on this server.
A	Montor This Domain Name
	www.domaintools.com

Internet Mining – Digging for Data	
Registration Service Provided By: DOSLDELIF Conterl: -L.844381601 Westle: http://www.dosuiclip.com	Technical Contact: FrivasyFrotect.org Domain Admin (contactContwasyDistectorg)
Domain Hame: B0000-CDH Hegistrast: FriveryTyconst.org Domain Admin (contact@programst.org)	7.0. Box 97 Note - All Postal Mails Rejected, visit Frivacyprotect.or Mocrestel null.5046 20
<pre>contain and itypicage(representation); P.0. Star P. Star Provide the Star Privacy protect.org Receptors:</pre>	HL Tel:+45.36946676 Billing Contact: PrivacyProtect.org Domain Amin (cirtuat@privacyprotect.org.)
Constant Dense: 32-Mex-2018 Departmention Dense: 31-Mex-2018 Departmention Dense: 31-Mex-2018 Anyment: 31:22-Mext, comp Anyment: 31:22-Mext, comp Anyment: 31:22-Mext, comp Anyment: 31:32-Mext, comp Anyl-31:22-Mext, com	P.O. Not 97 Note - All Datal Mails Rejected, visit Frivacyprotect.ory Moscrpatel mail.006 CH R. Tel 45.3654676 Status:ACTVM
Additionation Contact Principlement-op Densis Admin (<u>ContactGeneratoristics</u>)) 7.4. Dos 7 Note - All Portal Halls Reported, visit Privacyprotect.org Margueral Mail.1064 28 72 40.3044474	www.domaintools.com







Internet M	ining – Digging for Data
AboutUs:	Wiki article on Bodog.com
Related Sites:	belus.com, vegasinsider.com, therxforum.com, sportsinteraction.com, sportsbook.com, sbrforum.com, covers.com, bookmaker.com, bodoglife.com, wagerweb.com
Similar Domains:	Bo Doq - Casino Bo Doq - Sports Book Bo Doq - Sports Bo Doq Affiliate Bo Doq - Affiliates Bo Doq Baccarsi Bo Doq - Poker - Downloa Bo Doq - Uk Bo Doq Affiliate Life Bo Doq Affiliates Life Bo Doq Baduqi
DMOZ:	1 listings
DMOZ Title:	Bodog
DMOZ Description:	Casino and sportsbook providing lines on most major sports.
DMOZ Category:	/ Games / Gambling / Sports / Online / B /
Wikipedia:	9 pages
Visitors by Country:	Inited States 82.8%
Visitors by City:	I Los Angeles 7.2% I Boston 4% I New York 6% I Dalas-Fort Worth 3.8% San Francisco 6% I Chicago 2.8%
Alexa Trend/Rank:	#5,821: for the last three months.
Compete Rank:	1 #4.287 with 442,279 U.S. visitors per month
ing the second	www.domaintools.com





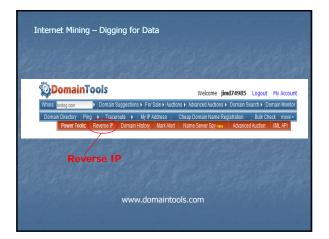


	Site Profile	Registration	Server Stats	My Whois	
Server Data					
Related Domain	s For Sale or A	t Auction		1 2 3 4 5	More >
OddsCompared BoDogLifeReals					
Server 1	ype: Apache				
				Ping, 1 DNS Lookup, 1 Traceroute,	
		bec - Kahnawak	e - Digital Media		
Response 0					
		LCOM expires in			
Domain St	atus. Registere	ed And Active W	Vebsite		

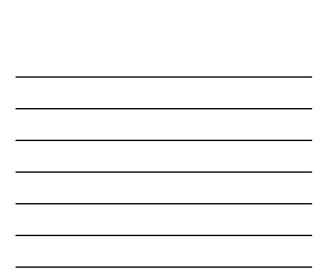


Internet	Mining –	Digging fo	r Data	Mala side ada di
Whois Record	Site Profile	Registration	Server Stats	My Whois
My Whois Vi	ew			
OddsCompar	ains For Sale or ed.com (\$1,076 oistry.net (Bid) Compete) <u>BeDoeld</u> PriceOdd		2 2 4 6 Mere > <u>BoCool lineRecots nel (Biol)</u> <u>Odds Tradina com (\$1,889)</u> 2,279 U.S. visitors per month
		-	AINCLIP DOM	IAINS, INC hnawake - Digital Media
			w.domaint	



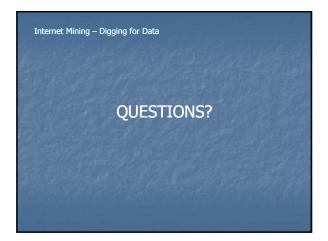






	ain Search + E	omain Montor
eap Comain Name Regi	Advanced Auction	XML API
		10
en II		
CH I		
og.com]		
38.209		
	DMOZ	Yahoo
	2 listings	6 listirugs
	Name Berver Sby own	ek 99_com] 238-209





Time for a *Practical Demonstration*



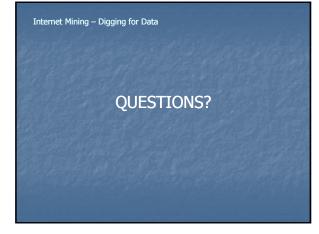
Diagnostic Utilities

Ipconfig

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

con Con	nmand Prompt _
C:∖>ip	config /all
Window	s IP Configuration
Ethern	Host Name : dibbles-7dbcla3 Prinary Dn: Suffix
	Connector-specific DNS Suffix : : domain.actdSleng Phopiski Marcess
м	Lease Expires





Time for a *Practical Exercise*

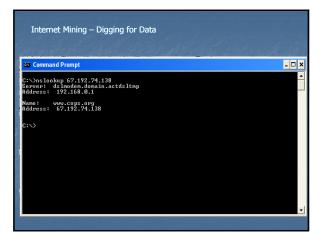
Internet Mining – Digging for Data

Diagnostic Utilities

NSLookup

MS-DOS Utility

- Look Up Domain/Host IP Address
- External DOS Command







Internet Technology Video

