TCP/IP Protocols and Investigative Tools

Gary C. Kessler
Gary Kessler Associates
Vermont Internet Crimes Task Force

Overview

- Internet structure
- TCP/IP protocol suite
  - » IP addressing
  - » TCP/UDP ports
- Higher layer applications and tools
  - » DNS
  - » World Wide Web
  - » E-mail and BASE64
  - » Social networks and finding people

The Internet

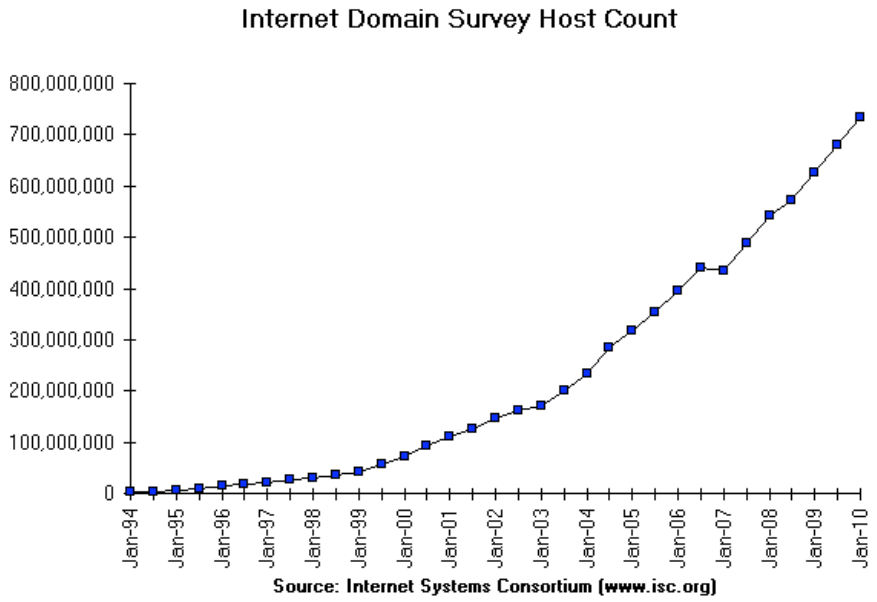
What does the 'Net look like, anyway?

The Internet

- The Internet is a network of networks
  - » Magic
  - » "...big. Really big. ...vastly hugely mind-bogglingly big..." (D. Adams, *The Hitchhiker's Guide to the Galaxy*)
  - » Owned by everyone, owned by no one
    - Anarchy, but not that well organized
- All hosts use the TCP/IP protocol suite

The Size of the Internet

- The Internet began in 1969 (4 nodes)
  - » Since 1990, it has grown and gained acceptance faster than anything else in human history
  - » User/host was doubling rate ~9-10 months
    - Rate finally started to slow in the U.S. in 2000
- 758.1M hosts in the DNS (4/2010)
  - » 1.03M are named *www* (#1, not counting *www1*, *www2*, *web*, and other variants)
  - » 924K are named *mail* (#2, not counting *mx*, *smtp*, *pop*, *mailer*, and other variants)



Internet User Demographics

WORLD INTERNET USAGE AND POPULATION STATISTICS

World Regions	Population (2009 Est.)	Internet Users Dec. 31, 2000	Internet Users Latest Data	Penetration (% Population)	Growth 2000-2009	Users % of Table
Africa	991,002,342	4,514,400	**86,217,900**	8.7 %	1,809.8 %	4.8 %
Asia	3,808,070,503	114,304,000	**764,435,900**	20.1 %	568.8 %	42.4 %
Europe	803,850,858	105,096,093	**425,773,571**	53.0 %	305.1 %	23.6 %
Middle East	202,687,005	3,284,800	**58,309,546**	28.8 %	1,675.1 %	3.2 %
North America	340,831,831	108,096,800	**259,561,000**	76.2 %	140.1 %	14.4 %
Latin America/Caribbean	586,662,468	18,068,919	**186,922,050**	31.9 %	934.5 %	10.4 %
Oceania / Australia	34,700,201	7,620,480	**21,110,490**	60.8 %	177.0 %	1.2 %
WORLD TOTAL	6,767,805,208	360,985,492	**1,802,330,457**	**26.6 %**	399.3 %	100.0 %

NOTES: (1) Internet Usage and World Population Statistics are for December 31, 2009. (2) CLICK on each world region name for detailed regional usage information. (3) Demographic (Population) numbers are based on data from the US Census Bureau . (4) Internet usage information comes from data published by Nielsen Online, by the International Telecommunications Union, by GfK, local Regulators and other reliable sources. (5) For definitions, disclaimer, and navigation help, please refer to the Site Surfing Guide. (6) Information in this site may be cited, giving the due credit to www.internetworldstats.com. Copyright © 2001 - 2010, Miniwatts Marketing Group. All rights reserved worldwide.

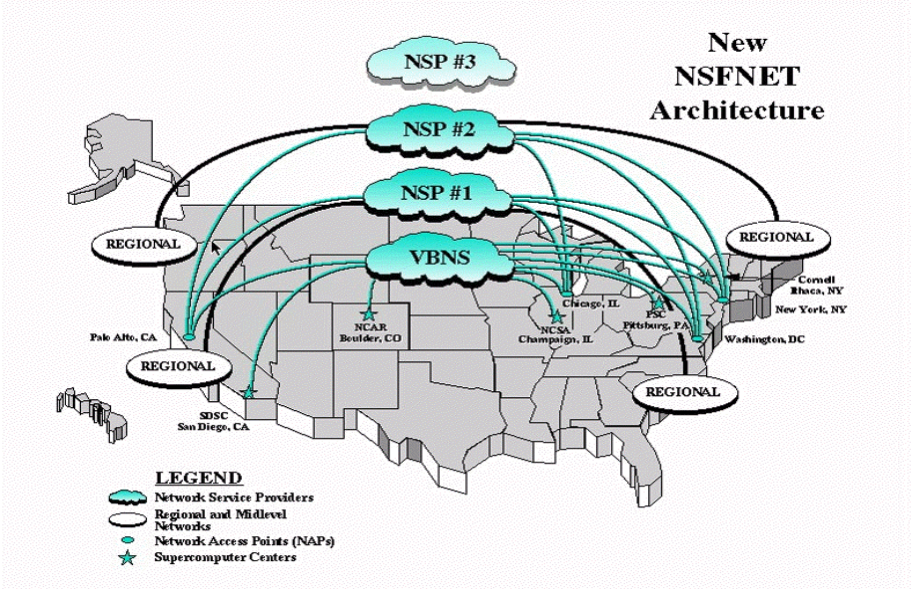
Source: ***http://www.internetworldstats.com/stats.htm***

Internet Administration

- Internet Society (ISOC)
- Internet Engineering Task Force (IETF)
- Internet Assigned Numbers Authority (IANA)
- The Internet Corporation for Assigned Names and Numbers (ICANN)
  - » Name registries include VeriSign Global Registry Services (.com, .net) and the Public Interest Registry (.org)
  - » Not to mention over 100 registrars (e.g., Domain Bank, Register.com, Tucows)
- Regional Number Registries
  - » American Registry for Internet Numbers (ARIN)
  - » Asia-Pacific NIC (APNIC)
  - » Réseaux IP Européen (RIPE)
  - » Latin American and Caribbean NIC (LACNIC)
  - » African NIC (AfriNIC)

Internet Documentation

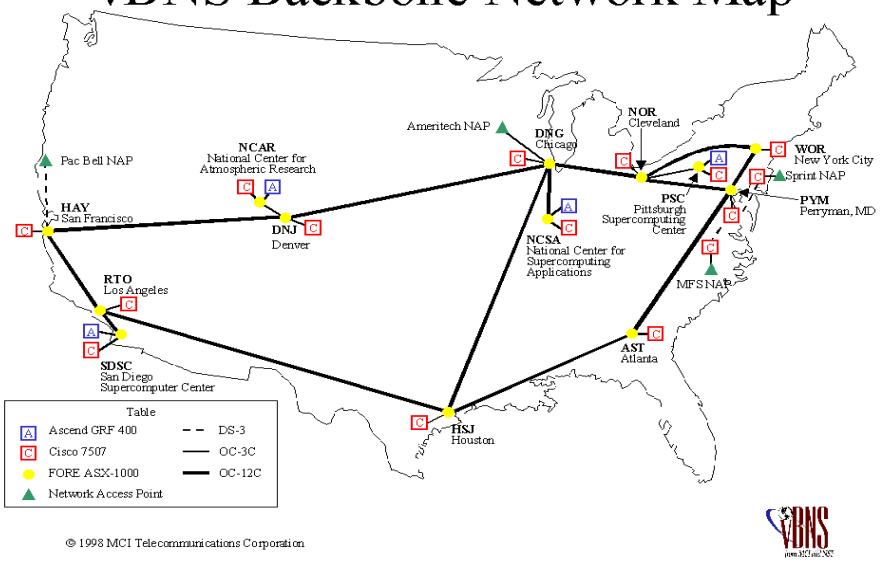
- Policies, standards, protocols, humor, tutorials, and more are documented in papers called Request for Comments (RFC)
  - » RFCs are numbered, and most are published in ASCII
  - » Almost all are available via anonymous FTP, WWW, or e-mail
  - » *http://www.rfc-editor.org/rfc.html*

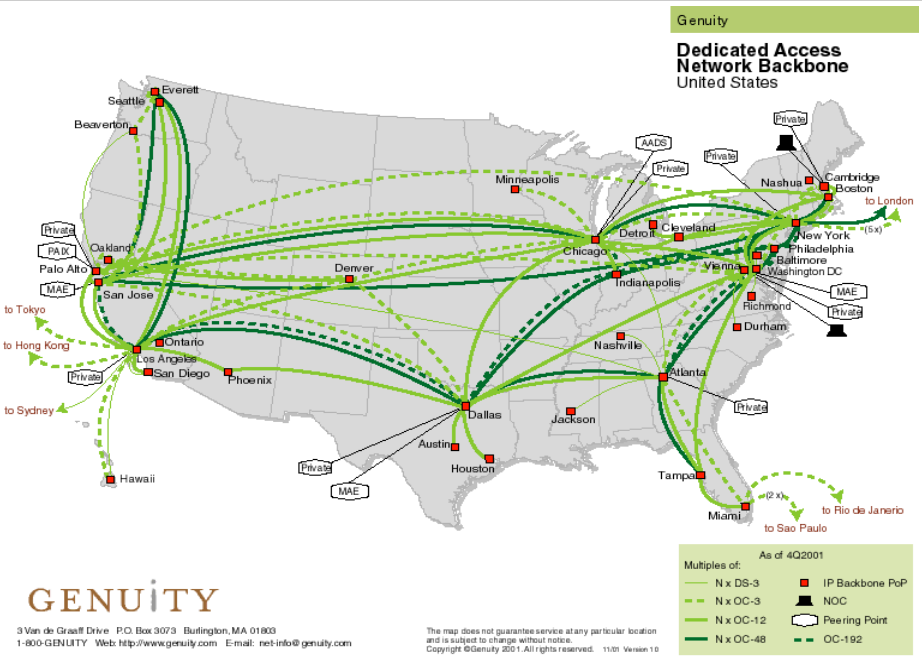


More Terms: Tier 1, 2, and 3

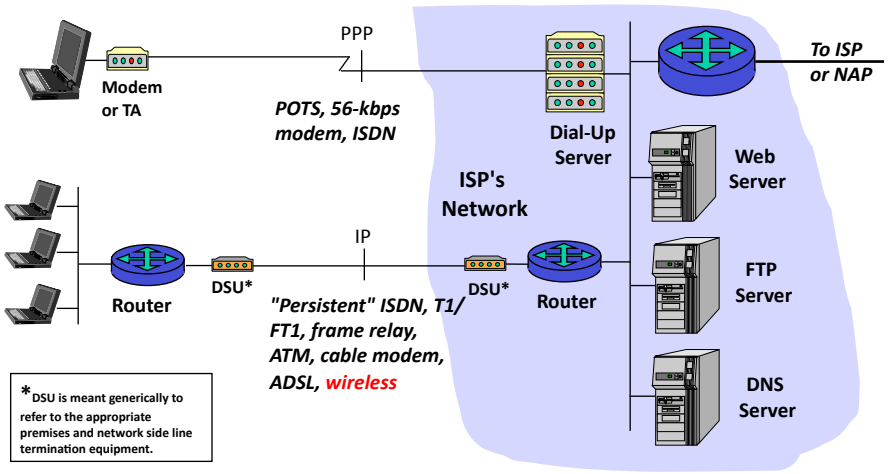
- Tier 1 (National ISP)
  - » Connects to multiple NAPs
  - » Tier 1s generally have bilateral peering
  - » National/global access
- Tier 2 (Regional ISP)
  - » Connects to 1 (or maybe 2) NAPs
- Tier 3 (Local ISP)
  - » Has no direct NAP connection
  - » Usually has two "upstream" (Tier 1?) ISPs for reliability

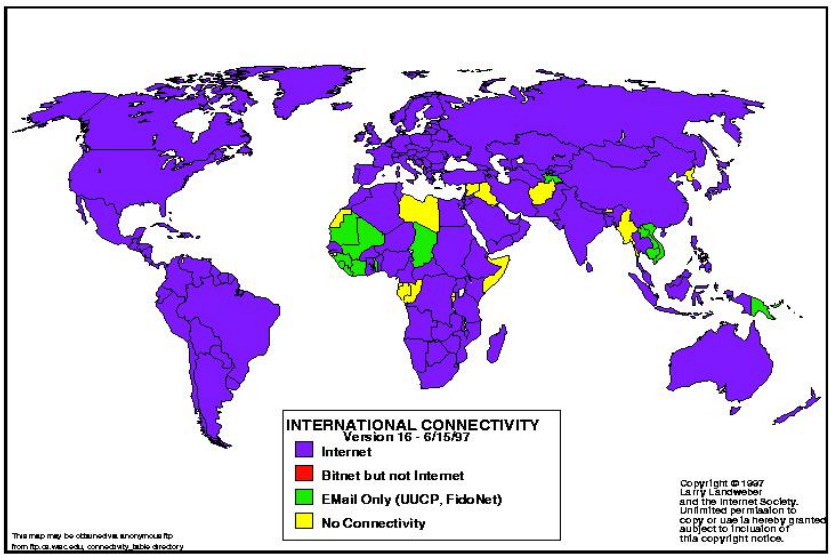
vBNS Backbone Network Map





Access Option Summary





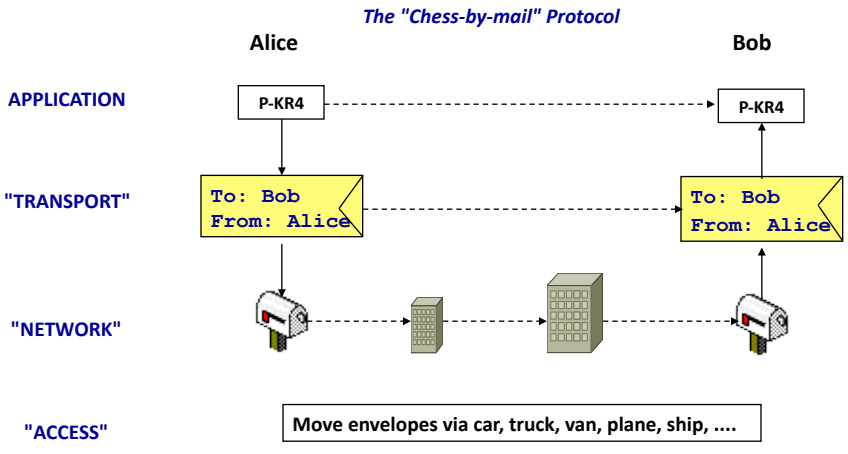
TCP/IP

The Communications Language of the Internet

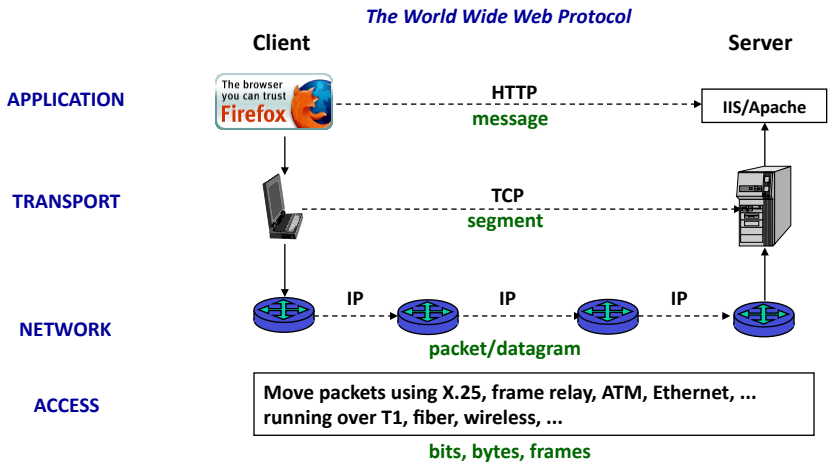
The Internet and TCP/IP

- TCP/IP is
  - » The communications protocol suite that holds the Internet together
  - » Non-proprietary; supported by all vendors on all software platforms
  - » *"We reject kings, presidents, and voting. We believe in rough consensus and running code."* (D. Clark, about the IETF)
  - » *The future protocol for voice and video??*

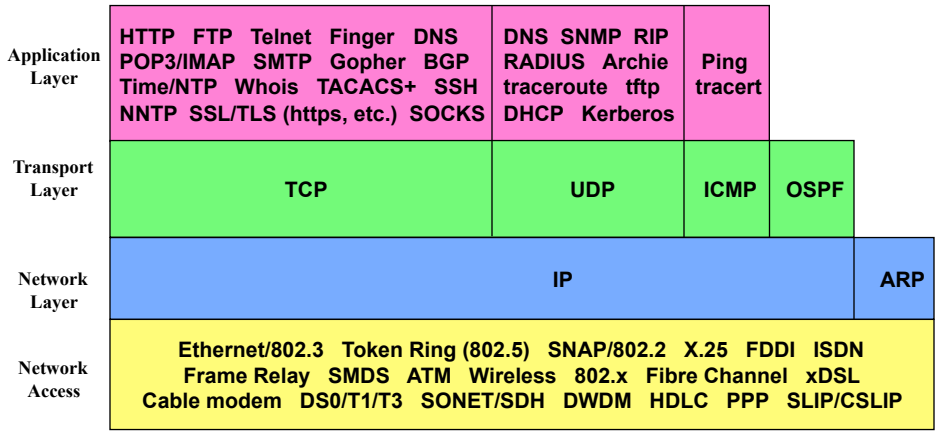
A Layered Protocol



Another Layered Protocol



The TCP/IP Protocol Suite



Internet Protocol

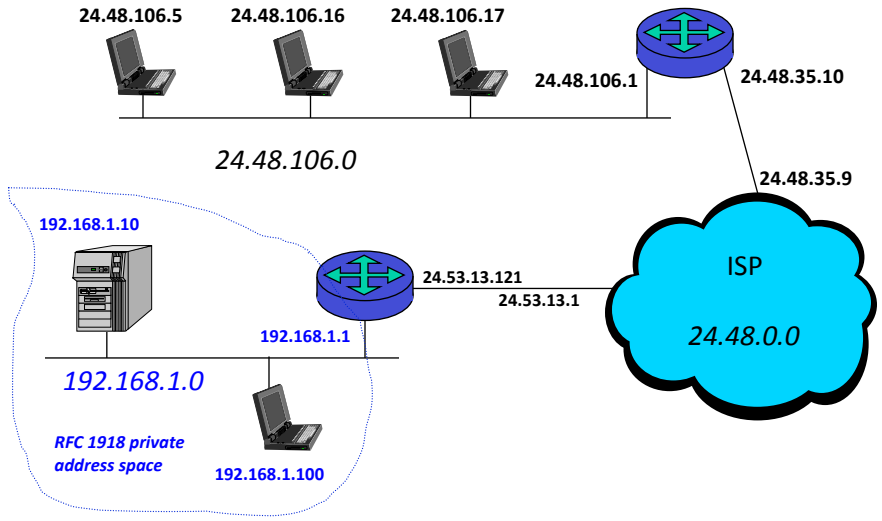
- Communication between host and router, or router-to-router
  - » Connectionless, unreliable datagram service
- Responsible for:
  - » Host addressing
  - » Error notification
  - » Fragmentation/reassembly
  - » Software/hardware address resolution
  - » Routing
- Operates over any underlying network

IP version 4 Classful Addressing

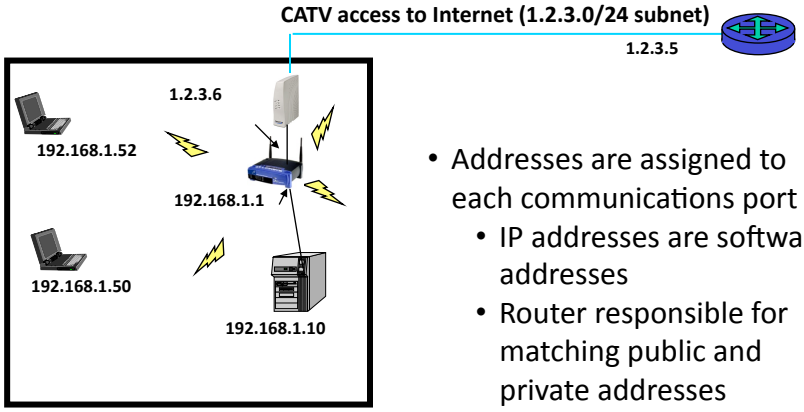
- IP version 4 (IPv4) addresses are 32 bits in length
  - » *Dotted decimal* notation: e.g., 208.162.106.17
- Addresses have NETID and HOSTID
  - » Class A (1-126): 8-bit NETID; very large networks
  - » Class B (128-191): 16-bit NETID; moderate size networks
  - » Class C (192-223): 24-bit NETID; small networks
  - » Class D (224-239): Multicast
  - » Class E (240-255): Experimental
- RFC 1918 private address space
  - » 10.0.0.0/8 (10.0.0.0-10.255.255.255)
  - » 172.16.0.0/12 (172.16.0.0-172.31.255.255)
  - » 192.168.0.0/16 (192.168.0.0-192.168.255.255)

REF: http://www.iana.org/assignments/ipv4-address-space

IP Addressing



IP Addressing and NAT



- Addresses are assigned to each communications port
  - IP addresses are software addresses
  - Router responsible for matching public and private addresses

Special Purpose IPv4 Addresses

Address Block	Present Use	Reference
0.0.0.0/8	"This" Network	RFC 1122, §3.2.1.3
10.0.0.0/8	Private-Use Networks	RFC 1918
127.0.0.0/8	Loopback	RFC 1122, §3.2.1.3
169.254.0.0/16	Link Local	RFC 3927
172.16.0.0/12	Private-Use Networks	RFC 1918
192.0.0.0/24	IETF Protocol Assignments	RFC 5736
192.0.2.0/24	TEST-NET-1	RFC 5737
192.88.99.0/24	6to4 Relay Anycast	RFC 3068
192.168.0.0/16	Private-Use Networks	RFC 1918
198.18.0.0/15	Network Interconnect Device Benchmark Testing	RFC 2544
198.51.100.0/24	TEST-NET-2	RFC 5737
203.0.113.0/24	TEST-NET-3	RFC 5737
224.0.0.0/4	Multicast	RFC 3171
240.0.0.0/4	Reserved for Future Use	RFC 1112, §4
255.255.255.255/32	Limited Broadcast	RFC 919, §7 RFC 922, §7

Source: RFC 5735

IP version 6 Addressing

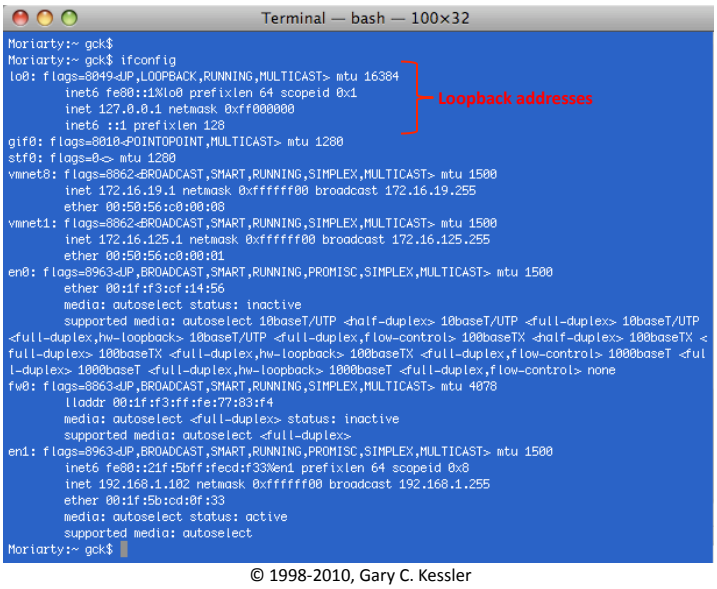
- IP version 6 (IPv6) addresses are 128 bits in length
  - *Hex group* notation: e.g., 2001:0db8:3241:0000:0000:9a8f:00c9:951e
- Addressing rules
  - Leading zeroes within a group do not have to be written
  - One or more consecutive all-zero groups can be replaced with a "::" (only one time in an address)
  - Address above could be written – 2001:db8:3241::9a8f:c9:951e
- Reserved addresses
  - Loopback – ::1/128 (127.0.0.1 in IPv4)
  - Link-local prefix – fe80::/10 (169.254.0.0/16 in IPv4)
  - Multicast addresses – ff00::/8 (224.0.0.0/7 in IPv4)
  - Documentation – 2001:db8::/32 (TEST-NET blocks in IPv4)
  - IPv4 mapped addresses -- ::ffff:0:0/96

See http://en.wikipedia.org/wiki/IPv6#Addressing and http://www.tcpipguide.com/free/t_IPv6Addressing.htm

ipconfig (DOS/Windows)

```
C:\> ipconfig /all
Windows 2000 IP Configuration

        Host Name . . . . . . . . . . . . : Altamont
        Primary DNS Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : sbtnvt.adelphia.net

Ethernet adapter Local Area Connection 3:

        Connection-specific DNS Suffix. . : sbtnvt.adelphia.net
        Description . . . . . . . . . . . : ORiNOCO PC Card (5 Volt)
        Physical Address. . . . . . . . . : 00-02-2D-67-4F-44
        DHCP Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.1.101
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1
        DHCP Server . . . . . . . . . . . : 192.168.1.1
        DNS Servers . . . . . . . . . . . : 68.168.96.162
                                            68.168.96.165
        Lease Obtained. . . . . . . . . . : Tuesday, July 27, 2004 15:33:08
        Lease Expires . . . . . . . . . . : Thursday, July 29, 2004 15:33:08

C:\>
```


ifconfig (Unix/Linux)




```
Moriarty:~ gck$
Moriarty:~ gck$ ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
vmnet8: flags=8862<BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        inet 172.16.19.1 netmask 0xffffff00 broadcast 172.16.19.255
        ether 00:50:56:c0:00:08
vmnet1: flags=8862<BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        inet 172.16.125.1 netmask 0xffffff00 broadcast 172.16.125.255
        ether 00:50:56:c0:00:01
en0: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        ether 00:1f:f3:cf:14:56
        media: autoselect status: inactive
        supported media: autoselect 10baseT/UTP <half-duplex> 10baseT/UTP <full-duplex> 10baseT/UTP
<full-duplex,hw-loopback> 10baseT/UTP <full-duplex,flow-control> 100baseTX <half-duplex> 100baseTX <
full-duplex> 100baseTX <full-duplex,hw-loopback> 100baseTX <full-duplex,flow-control> 1000baseT <ful
l-duplex> 1000baseT <full-duplex,hw-loopback> 1000baseT <full-duplex,flow-control> none
fw0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 4078
        lladdr 00:1f:f3:ff:fe:77:83:f4
        media: autoselect <full-duplex> status: inactive
        supported media: autoselect <full-duplex>
en1: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        inet6 fe80::21f:5bff:fecd:f33%en1 prefixlen 64 scopeid 0x8
        inet 192.168.1.102 netmask 0xffffff00 broadcast 192.168.1.255
        ether 00:1f:5b:cd:0f:33
        media: autoselect status: active
        supported media: autoselect
Moriarty:~ gck$
```

TCP and UDP

- TCP/IP's Transport Layer protocols provide end-to-end (host-to-host) communication
  - » Transmission Control Protocol (TCP)
  - » User Datagram Protocol (UDP)
- Host address provided by IP; the process (i.e., application or service) is identified by port numbers

Ports

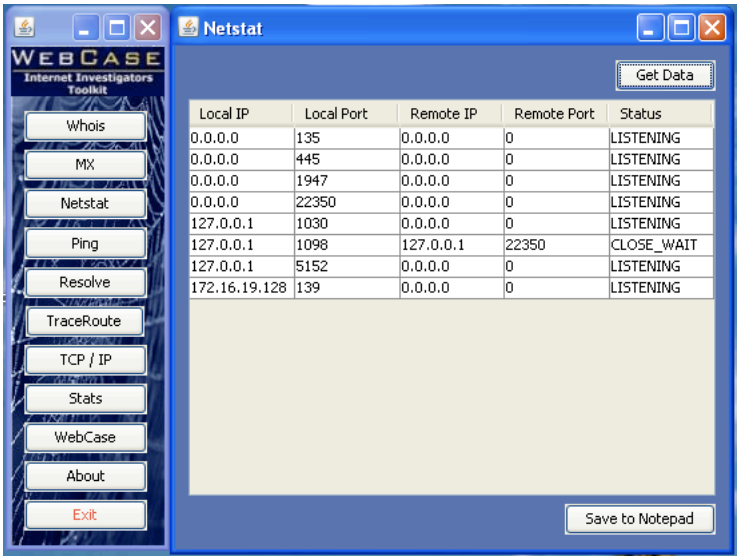
Port No.	Protocol	Application	Port No.	Protocol	Application
7	UDP	echo	80	TCP	http
13	TCP	daytime	110	TCP	pop3
19	UDP	chargen	111	TCP	sunrpc
20	TCP	ftp-data	113	TCP	auth
21	TCP	ftp-control	119	TCP	nntp
22	TCP	ssh	123	UDP	ntp
23	TCP	telnet	137	UDP	netbios-ns
25	TCP	smtp	138	UDP	netbios-dgm
37	UDP	time	139	TCP	netbios-ssn
43	TCP	whois	143	TCP	imap
53	TCP/UDP	dns	161	UDP	snmp
67	UDP	bootps	162	UDP	snmp-trap
68	UDP	bootpc	179	TCP	bgp
69	UDP	tftp	443	TCP	https (http/ssl)
70	TCP	gopher	514	UDP	syslog
79	TCP	finger	520	UDP	rip

Netstat (Unix)

```
[gck@networking gck]$ netstat -h
usage: netstat [-veenNcCF] [<Af>] -r         netstat {-V|--version|-h|--help}
       netstat [-vnNcaeol] [<Socket> ...]
       netstat { [-veenNac] -i | [-cnNe] -M | -s }

        -r, --route              display routing table
        -i, --interfaces         display interface table
        -g, --groups             display multicast group memberships
        -s, --statistics         display networking statistics (like SNMP)
        -M, --masquerade         display masqueraded connections

        -v, --verbose            be verbose
        -n, --numeric            dont resolve names
        --numeric-hosts          dont resolve host names
        --numeric-ports          dont resolve port names
        --numeric-users          dont resolve user names
        -N, --symbolic           resolve hardware names
        -e, --extend             display other/more information
        -p, --programs           display PID/Program name for sockets
        -c, --continuous         continuous listing

        -l, --listening          display listening server sockets
        -a, --all, --listening   display all sockets (default: connected)
        -o, --timers             display timers
        -F, --fib                display Forwarding Information Base
(default)
        -C, --cache              display routing cache instead of FIB

  <Socket>={-t|--tcp} {-u|--udp} {-w|--raw} {-x|--unix} --ax25 --ipx --netrom
  <AF>=Use '-A <af>' or '--<af>' Default: inet
  List of possible address families (which support routing):
    inet (DARPA Internet) inet6 (IPv6) ax25 (AMPR AX.25)
    netrom (AMPR NET/ROM) ipx (Novell IPX) ddp (Appletalk DDP)
    x25 (CCITT X.25)
```


Netstat

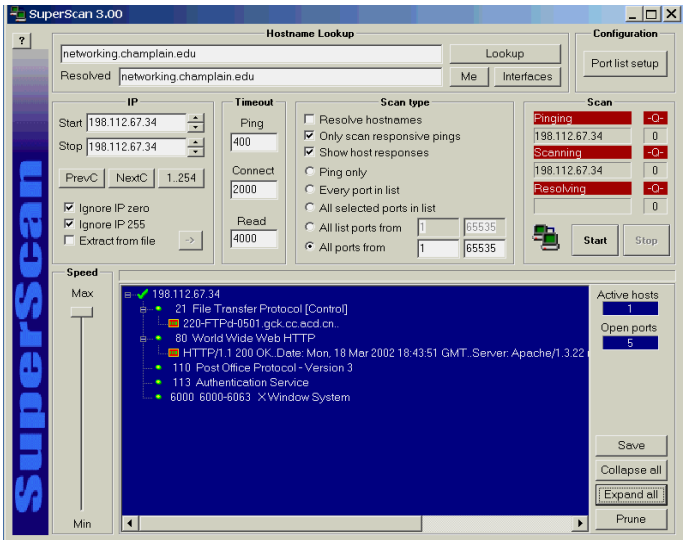
```
[gck@networking gck]$ netstat -atu
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 *:x11                   *:*                     LISTEN
tcp        0      0 *:http                  *:*                     LISTEN
tcp        0      0 *:auth                  *:*                     LISTEN
tcp        0      0 *:ftp                   *:*                     LISTEN
tcp        0      0 *:ssh                   *:*                     LISTEN
tcp        0      0 34-67.champlain.edu:ssh vt-lakechamplain2b:1568 ESTABLISHED
[gck@networking gck]$ netstat -atun
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:6000            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:113             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 198.112.67.34:22        24.50.101.21:1568       ESTABLISHED
[gck@networking gck]$ netstat -i
Kernel Interface table
Iface   MTU Met    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0   1500   0   507304      0      0      0   443753      0      0      0 BRU
lo    16436   0       47      0      0      0       47      0      0      0 LRU
```

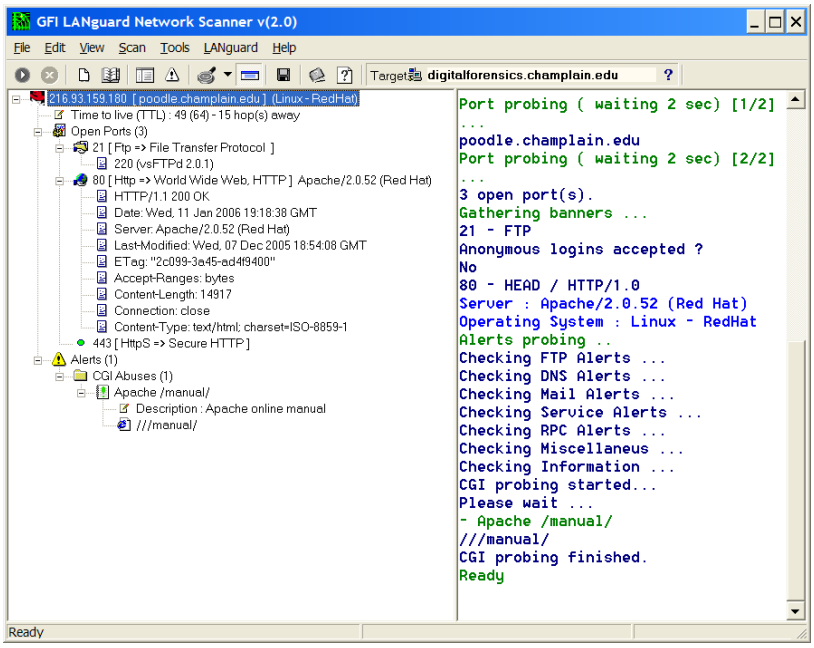


Finger

```
[gck@networking gck]$ finger @shell.sover.net
[granite.sover.net]
Login    Name                 Tty   Idle  Login Time   Office     Office Phone
betonica Allison Turner       *p2     19  Feb 15 20:16
dracofyl Aaron D Murphy       *p1   1:37  Feb 15 18:59
erikl    Erik R. Leo          *p4    24d  Jan 15 13:15 23         +1(802)463-2111
kessfam  Gary Kessler          p3        Feb 15 20:36
merriam  Bill Merriam          p8     46  Feb 15 19:38
tlongtin Tom Longtin           pb     41  Feb 15 09:16
vanslett                       p0   3:38  Feb 15 16:58
[gck@networking gck]$ finger kessfam@shell.sover.net
[granite.sover.net]
Login: kessfam                          Name: Gary Kessler
Directory: /home/k/e/kessfam            Shell: /bin/bash
On since Fri Feb 15 20:36 (EST) on ttyp3 from 24.50.101.21
No Plan.
[gck@networking gck]$
```


Port Scanning - Windows





nmap

```
[root@networking gck]# nmap -O foo.example.net
Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Interesting ports on foo.example.net (192.168.167.3):
(The 1518 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
22/tcp     open        ssh
80/tcp     open        http
113/tcp    open        auth
6000/tcp   open        X11
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=146832 (Good luck!)
No OS matches for host
[root@networking gck]# nmap -O baz.example.net
Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Interesting ports on baz.example.net (192.168.167.4):
(The 1516 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
80/tcp     open        http
135/tcp    filtered    loc-srv
137/tcp    filtered    netbios-ns
138/tcp    filtered    netbios-dgm
139/tcp    filtered    netbios-ssn
1031/tcp   open        iad2
TCP Sequence Prediction: Class=trivial time dependency
                         Difficulty=2 (Trivial joke)
Remote operating system guess: Windows NT4 / Win95 / Win98
```


Higher Layer Applications

And tools to examine TCP/IP and Internet information

Internet Domain Names

- Host names are in form: *host.domain.global-top-level-domain*
- Examples include:

www.cisco.com	tick.usno.navy.mil	www.itu.int
www.isoc.org	www.ed.gov	clover.sover.net
campus.champlain.edu	mail.cc.duq.edu	www.garykessler.net
cnri.reston.va.us	cms.csd.k12.vt.us	dps.state.vt.us

www.udg.mx	www.iso.ch
reduno.reduno.com.mx	www.netvision.net.il
www.iss.u-tokyo.ac.jp	www.yell.co.uk

- Notes
  - *.ws* **not** Web Site; it belongs to Samoa
  - *.tv* **not** television; it belongs to Tuvalu
  - See ***http://www.norid.no/domenenavnbaser/domreg.html***

Late Flash: *New* TLDs!!

- ICANN approved new TLDs in November 2000:
  - *.aero* - Aviation industry
  - *.biz* - Businesses
  - *.coop* - Business cooperatives
  - *.info* - General use
  - *.museum* - Museums
  - *.name* - Individuals
  - *.pro* - Professionals
- *.mobi* - Mobile Internet (July 2005)

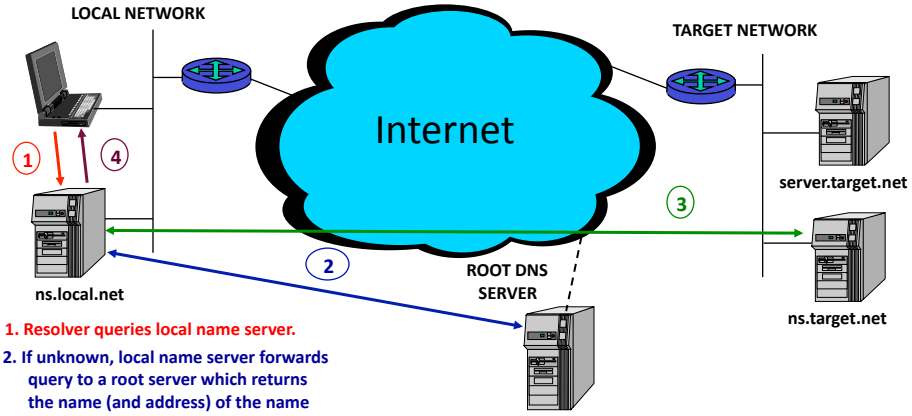
Late Flash: *Newer* TLDs!!

- ICANN approved Internationalized Domain Names (IDNs) as ccTLDs in May 2010:
  - » Egypt: مصر (MaSr)
  - » Saudi Arabia: السعودية (Al Saudiah)
  - » Russian Federation: .pф
  - » United Arab Emirates: امارات (Emaarat)

DNS

- The Domain Name System is a distributed database that is used to
  - » Resolve host name to an IP address (A)
  - » Resolve an IP address to a host name (PTR)
  - » Find the mail server(s) for a given domain (MX)
  - » Find the name server(s) for a given domain (NS)

DNS Name Resolution Process

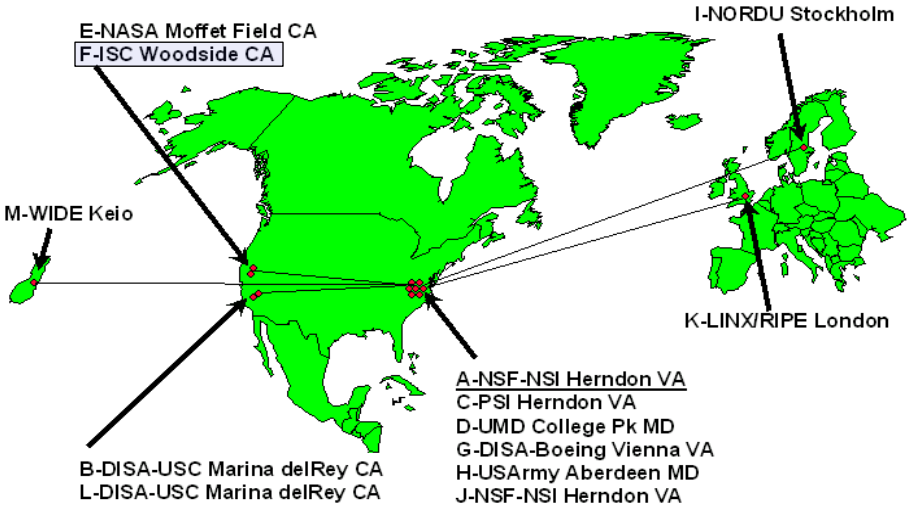


1. Resolver queries local name server.
2. If unknown, local name server forwards query to a root server which returns the name (and address) of the name server for the target domain.
3. Target network's name server replies to local name server.
4. Local name server responds to resolver.

DNS Root Servers

1 Feb 98

Designation, Responsibility, and Locations



REF: http://www.root-servers.org/

DNS Resource Records

```
example.com.  IN SOA  ns.example.com.
     hostmaster.example.com.  (
     20081005   ; serial # (date format)
        10800   ; refresh (3 hours)
         3600   ; retry (1 hour)
       604800   ; expire (1 week)
        86400)  ; TTL (1 day)
www.example.com.          IN  A   10.1.2.129
ns.example.com.           IN  A   10.1.2.130
mail.example.com.         IN  A   10.1.2.130
example.com.              IN  NS  ns.example.com.
example.com.              IN  NS  name.exampleisp.net.
example.com.              IN  MX  10 mail.example.com.
syrup.example.com.        IN  CNAME  www.example.com.
129.2.1.10.in-addr.arpa.  IN  PTR  www.example.com.
```


nslookup (1)

```
Moriarty:~ gck$ nslookup
> www.garykessler.net
Server:     216.93.145.253
Address:    216.93.145.253#53

Non-authoritative answer:
Name:   www.garykessler.net
Address: 207.204.17.246
> set type=mx
> garykessler.net
Server:     216.93.145.253
Address:    216.93.145.253#53

Non-authoritative answer:
garykessler.net         mail exchanger = 0 mx01.register.com.
garykessler.net         mail exchanger = 10 mx03.register.com.

Authoritative answers can be found from:
garykessler.net         nameserver = dns055.b.register.com.
garykessler.net         nameserver = dns211.c.register.com.
garykessler.net         nameserver = dns223.a.register.com.
garykessler.net         nameserver = dns249.d.register.com.
dns055.b.register.com   internet address = 216.21.232.55
dns211.c.register.com   internet address = 216.21.235.211
dns223.a.register.com   internet address = 216.21.231.223
dns249.d.register.com   internet address = 216.21.236.249
```

nslookup (2)

```
> set type=soa
> garykessler.net
Server:     216.93.145.253
Address:    216.93.145.253#53

Non-authoritative answer:
garykessler.net
            origin = dns223.a.register.com
            mail addr = root.register.com
            serial = 2009082818
            refresh = 28800
            retry = 7200
            expire = 604800
            minimum = 14400

Authoritative answers can be found from:
garykessler.net         nameserver = dns223.a.register.com.
garykessler.net         nameserver = dns249.d.register.com.
garykessler.net         nameserver = dns055.b.register.com.
garykessler.net         nameserver = dns211.c.register.com.
dns055.b.register.com   internet address = 216.21.232.55
dns211.c.register.com   internet address = 216.21.235.211
dns223.a.register.com   internet address = 216.21.231.223
dns249.d.register.com   internet address = 216.21.236.249
> exit
> Moriarty:~ gck$
```


dig (1)

```
Moriarty:~ gck$ dig www.garykessler.net

; <<>> DiG 9.4.3-P3 <<>> www.garykessler.net
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28510
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 4

;; QUESTION SECTION:
;www.garykessler.net.               IN          A

;; ANSWER SECTION:
www.garykessler.net.    14043       IN          A           207.204.17.246

;; AUTHORITY SECTION:
garykessler.net.        93761       IN          NS          dns223.a.register.com.
garykessler.net.        93761       IN          NS          dns249.d.register.com.
garykessler.net.        93761       IN          NS          dns055.b.register.com.
garykessler.net.        93761       IN          NS          dns211.c.register.com.

;; ADDITIONAL SECTION:
dns055.b.register.com.  167131      IN          A           216.21.232.55
dns211.c.register.com.  93761       IN          A           216.21.235.211
dns223.a.register.com.  93761       IN          A           216.21.231.223
dns249.d.register.com.  73468       IN          A           216.21.236.249

;; Query time: 1 msec
;; SERVER: 216.93.145.253#53(216.93.145.253)
;; WHEN: Mon Sep 14 09:45:26 2009
;; MSG SIZE  rcvd: 221

Moriarty:~ gck$
```

dig (2)

```
Moriarty:~ gck$ dig www.garykessler.net mx

; <<>> DiG 9.4.3-P3 <<>> www.garykessler.net mx
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1887
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.garykessler.net.               IN          MX

;; Query time: 42 msec
;; SERVER: 216.93.145.253#53(216.93.145.253)
;; WHEN: Mon Sep 14 09:47:39 2009
;; MSG SIZE  rcvd: 37

Moriarty:~ gck$ dig www.garykessler.net soa

; <<>> DiG 9.4.3-P3 <<>> www.garykessler.net soa
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52050
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.garykessler.net.               IN          SOA

;; Query time: 20 msec
;; SERVER: 216.93.145.253#53(216.93.145.253)
;; WHEN: Mon Sep 14 09:48:55 2009
;; MSG SIZE  rcvd: 37

Moriarty:~ gck$
```


whois

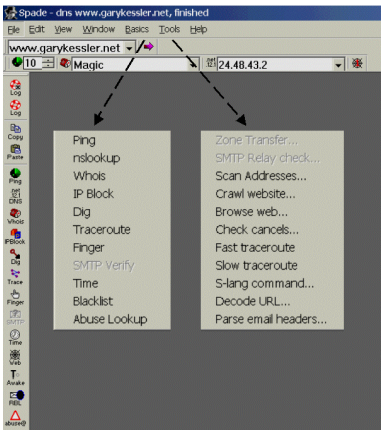
```
Moriarty:~gck$ whois garykessler.net

Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

   Domain Name: GARYKESSLER.NET
   Registrar: REGISTER.COM, INC.
   Whois Server: whois.register.com
   Referral URL: http://www.register.com
   Name Server: DNS055.B.REGISTER.COM
   Name Server: DNS211.C.REGISTER.COM
   Name Server: DNS223.A.REGISTER.COM
   Name Server: DNS249.D.REGISTER.COM
   Status: clientTransferProhibited
   Updated Date: 28-aug-2009
   Creation Date: 29-jan-2000
   Expiration Date: 29-jan-2013

>>> Last update of whois database: Mon, 14 Sep 2009 13:53:41 UTC <<<
```

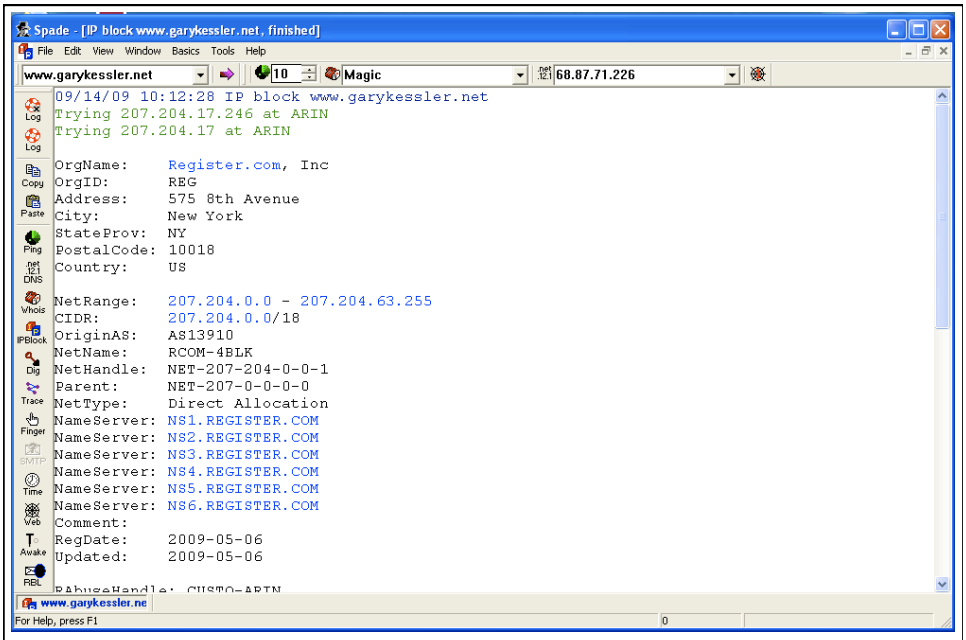
Some versions of *nix (e.g., RedHat, FreeBSD) will automatically redirect the query...

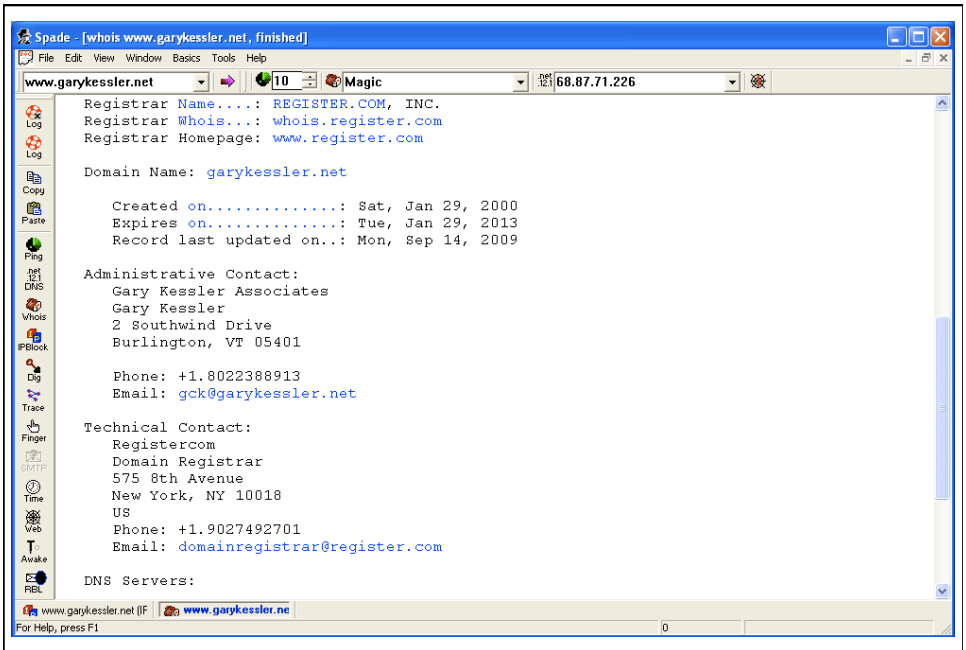
```
                :
     Registrant:
     Gary Kessler Associates
     Gary Kessler
     2 Southwind Drive
     Burlington, VT 05401
     US
     Email: gck@garykessler.net

   Registrar Name....: REGISTER.COM, INC.
   Registrar Whois...: whois.register.com
   Registrar Homepage: www.register.com

   Domain Name: garykessler.net

      Created on..............: Sat, Jan 29, 2000
      Expires on..............: Tue, Jan 29, 2013
      Record last updated on..: Mon, Sep 14, 2009

   Administrative Contact:
      Gary Kessler Associates
      Gary Kessler
      2 Southwind Drive
      Burlington, VT 05401
      US
      Phone: +1.8022388913
      Email: gck@garykessler.net

   Technical Contact:
      Registercom
      Domain Registrar
      575 8th Avenue
      New York, NY 10018

      Phone: +1.9027492701
      Email: domainregistrar@register.com

   DNS Servers:

   dns211.c.register.com
   dns249.d.register.com
   dns223.a.register.com
   dns055.b.register.com

Visit AboutUs.org for more information about garykessler.net
<A HREF="http://www.aboutus.org/garykessler.net">AboutUs: garykessler.net</A>

115-152:~ gck$
```

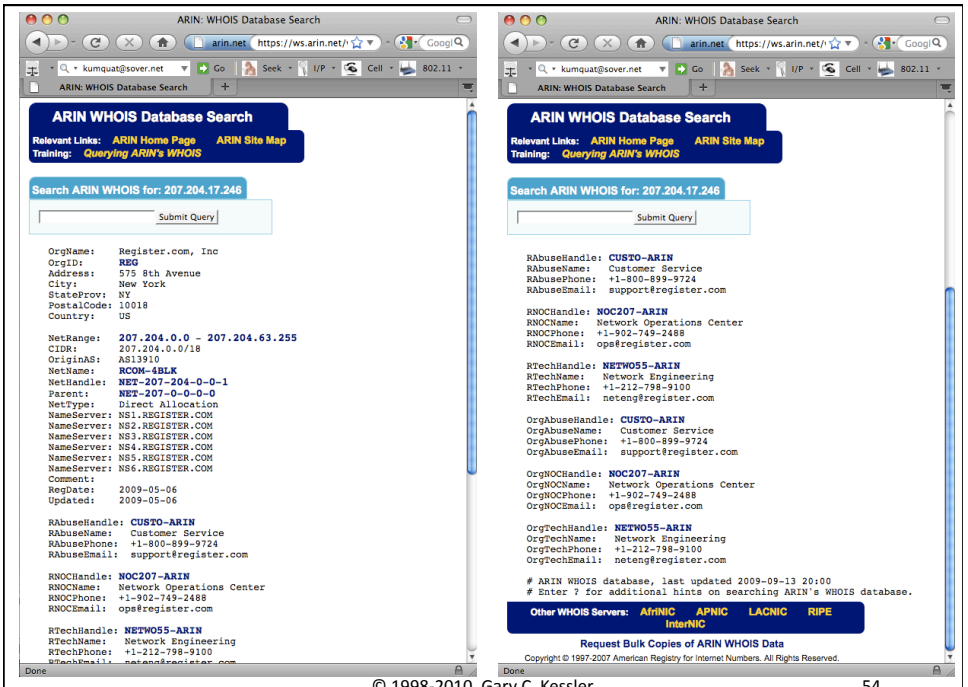

Sam Spade

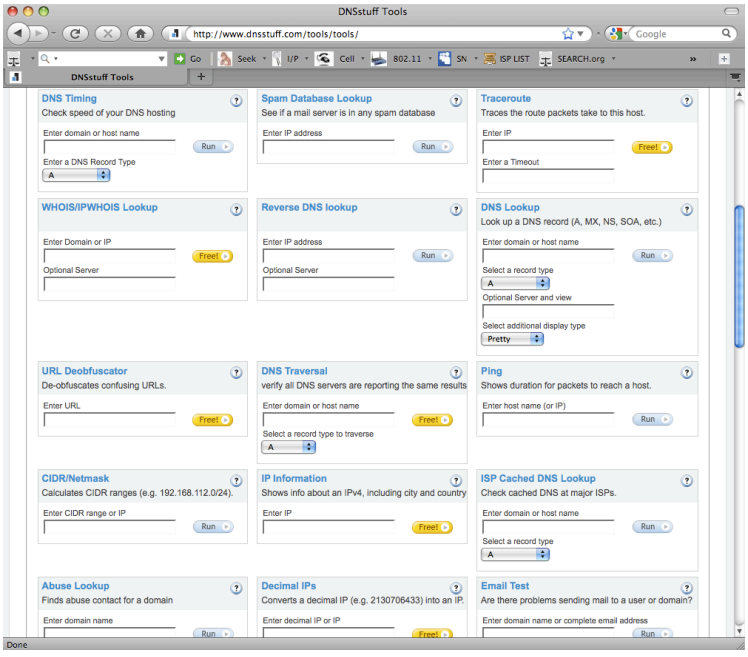
- Provides wide range of information gathering functions
- Run or download from *www.samspade.org*

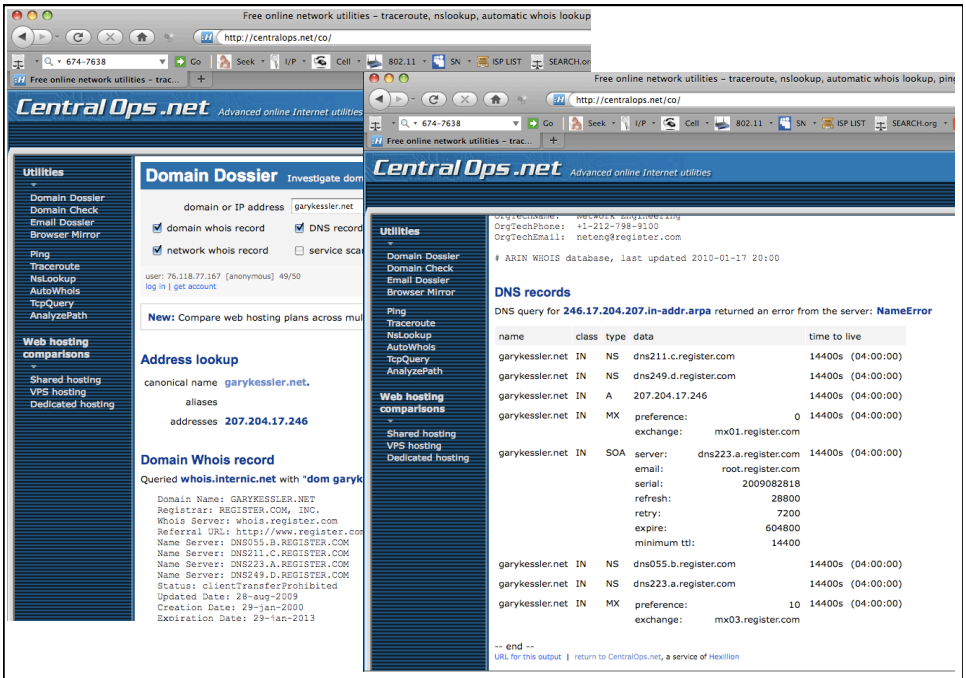



Spade - [IP block www.garykessler.net, finished]
File Edit View Window Basics Tools Help
www.garykessler.net
10
Magic
68.87.71.226
09/14/09 10:12:28 IP block www.garykessler.net
Trying 207.204.17.246 at ARIN
Trying 207.204.17 at ARIN
OrgName: Register.com, Inc
OrgID: REG
Address: 575 8th Avenue
City: New York
StateProv: NY
PostalCode: 10018
Country: US
NetRange: 207.204.0.0 - 207.204.63.255
CIDR: 207.204.0.0/18
OriginAS: AS13910
NetName: RCOM-4BLK
NetHandle: NET-207-204-0-0-1
Parent: NET-207-0-0-0-0
NetType: Direct Allocation
NameServer: NS1.REGISTER.COM
NameServer: NS2.REGISTER.COM
NameServer: NS3.REGISTER.COM
NameServer: NS4.REGISTER.COM
NameServer: NS5.REGISTER.COM
NameServer: NS6.REGISTER.COM
Comment:
RegDate: 2009-05-06
Updated: 2009-05-06
For Help, press F1


Spade - [whois www.garykessler.net, finished]
File Edit View Window Basics Tools Help
www.garykessler.net
10
Magic
68.87.71.226
Registrar Name....: REGISTER.COM, INC.
Registrar Whois...: whois.register.com
Registrar Homepage: www.register.com
Domain Name: garykessler.net
Created on..............: Sat, Jan 29, 2000
Expires on..............: Tue, Jan 29, 2013
Record last updated on..: Mon, Sep 14, 2009
Administrative Contact:
Gary Kessler Associates
Gary Kessler
2 Southwind Drive
Burlington, VT 05401
Phone: +1.8022388913
Email: gck@garykessler.net
Technical Contact:
Registercom
Domain Registrar
575 8th Avenue
New York, NY 10018
US
Phone: +1.9027492701
Email: domainregistrar@register.com
DNS Servers:
For Help, press F1

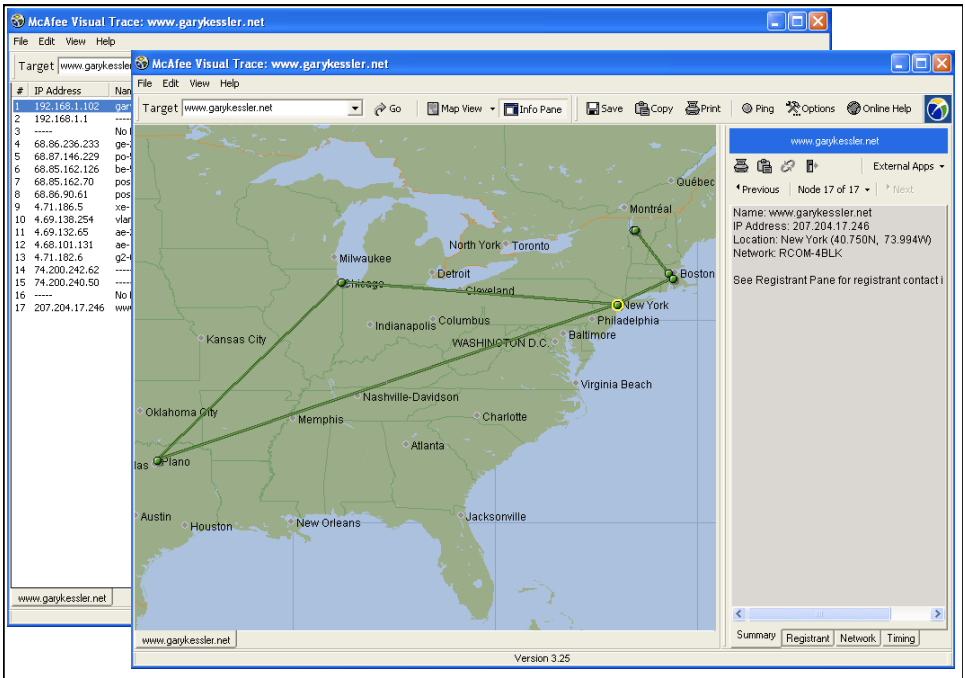

ARIN: WHOIS Database Search
ARIN WHOIS Database Search
Relevant Links: ARIN Home Page ARIN Site Map
Training: Querying ARIN's WHOIS
Search ARIN WHOIS for: 207.204.17.246
Submit Query
OrgName: Register.com, Inc
OrgID: REG
Address: 575 8th Avenue
City: New York
StateProv: NY
PostalCode: 10018
Country: US
NetRange: 207.204.0.0 - 207.204.63.255
CIDR: 207.204.0.0/18
OriginAS: AS13910
NetName: RCOM-4BLK
NetHandle: NET-207-204-0-0-1
Parent: NET-207-0-0-0-0
NetType: Direct Allocation
NameServer: NS1.REGISTER.COM
NameServer: NS2.REGISTER.COM
NameServer: NS3.REGISTER.COM
NameServer: NS4.REGISTER.COM
NameServer: NS5.REGISTER.COM
NameServer: NS6.REGISTER.COM
Comment:
RegDate: 2009-05-06
Updated: 2009-05-06
RAbuseHandle: CUSTO-ARIN
RAbuseName: Customer Service
RAbusePhone: +1-800-899-9724
RAbuseEmail: support@register.com
RNOCHandle: NOC207-ARIN
RNOCName: Network Operations Center
RNOCPhone: +1-902-749-2488
RNOCEmail: ops@register.com
RTechHandle: NETWO55-ARIN
RTechName: Network Engineering
RTechPhone: +1-212-798-9100
Done
ARIN: WHOIS Database Search
ARIN WHOIS Database Search
Relevant Links: ARIN Home Page ARIN Site Map
Training: Querying ARIN's WHOIS
Search ARIN WHOIS for: 207.204.17.246
Submit Query
RAbuseHandle: CUSTO-ARIN
RAbuseName: Customer Service
RAbusePhone: +1-800-899-9724
RAbuseEmail: support@register.com
RNOCHandle: NOC207-ARIN
RNOCName: Network Operations Center
RNOCPhone: +1-902-749-2488
RNOCEmail: ops@register.com
RTechHandle: NETWO55-ARIN
RTechName: Network Engineering
RTechPhone: +1-212-798-9100
RTechEmail: neteng@register.com
OrgAbuseHandle: CUSTO-ARIN
OrgAbuseName: Customer Service
OrgAbusePhone: +1-800-899-9724
OrgAbuseEmail: support@register.com
OrgNOCHandle: NOC207-ARIN
OrgNOCName: Network Operations Center
OrgNOCPhone: +1-902-749-2488
OrgNOCEmail: ops@register.com
OrgTechHandle: NETWO55-ARIN
OrgTechName: Network Engineering
OrgTechPhone: +1-212-798-9100
OrgTechEmail: neteng@register.com
ARIN WHOIS database, last updated 2009-09-13 20:00
Enter ? for additional hints on searching ARIN's WHOIS database.
Other WHOIS Servers: AfrNIC APNIC LACNIC RIPE InterNIC
Request Bulk Copies of ARIN WHOIS Data
Copyright © 1997-2007 American Registry for Internet Numbers. All Rights Reserved.
Done


DNSstuff Tools
http://www.dnsstuff.com/tools/tools/
DNS Timing
Check speed of your DNS hosting
Spam Database Lookup
See if a mail server is in any spam database
Traceroute
Traces the route packets take to this host.
WHOIS/IPWHOIS Lookup
Reverse DNS lookup
DNS Lookup
Look up a DNS record (A, MX, NS, SOA, etc.)
URL Deobfuscator
De-obfuscates confusing URLs.
DNS Traversal
verify all DNS servers are reporting the same results
Ping
Shows duration for packets to reach a host.
CIDR/Netmask
Calculates CIDR ranges (e.g. 192.168.112.0/24).
IP Information
Shows info about an IPv4, including city and country
ISP Cached DNS Lookup
Check cached DNS at major ISPs.
Abuse Lookup
Finds abuse contact for a domain
Decimal IPs
Converts a decimal IP (e.g. 2130706433) into an IP.
Email Test
Are there problems sending mail to a user or domain?
Done



IP Addresses and Domain Names

- IP address and domain name ownership are not related although not necessarily the same
  - » An IP address is assigned to a given Web site by the Web site hosting service provider
  - » A domain name is assigned by a name registry
- Tracing a Web site owner
  - » Hosting service requires a fee; follow the money
  - » Domain name registration requires a fee; follow the money
  - » A Web site needs to be maintained and updated; the server log will indicate how the Web manager accesses the site

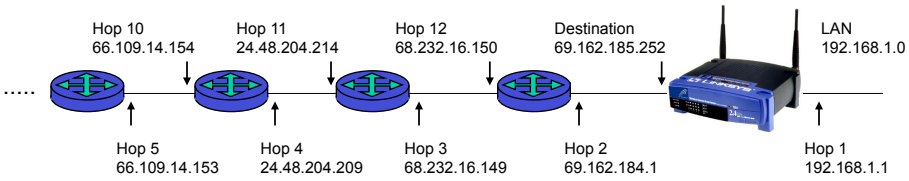


Traceroute

```
Moriarty:~ gck$ traceroute www.garykessler.net
traceroute to www.garykessler.net (207.204.17.246), 64 hops max, 40 byte packets
 1  251-152 (206.193.152.251)  1.123 ms  0.602 ms  0.442 ms
 2  ppp-64-25-209-166.teljet.com (64.25.209.166)  5.777 ms  6.827 ms  5.122 ms
 3  POS5-3.GW6.BOS4.ALTER.NET (208.192.181.193)  10.753 ms  15.142 ms  17.367 ms
 4  0.ge-3-3-2.XL4.BOS4.ALTER.NET (152.63.20.22)  14.460 ms  12.922 ms  11.625 ms
 5  0.so-6-3-0.XL4.NYC4.ALTER.NET (152.63.0.73)  19.330 ms  18.552 ms  21.431 ms
 6  0.xe-3-3-0.BR2.NYC4.ALTER.NET (152.63.3.122)  19.193 ms 0.xe-7-1-0.BR2.NYC4.ALTER.NET
(152.63.3.170)  18.154 ms 0.xe-11-0-0.BR2.NYC4.ALTER.NET (152.63.16.185)  47.632 ms
 7  4.68.110.105 (4.68.110.105)  19.542 ms te-7-1-0.edge2.NewYork2.level3.net
(4.68.127.21)  17.443 ms 4.68.110.105 (4.68.110.105)  17.495 ms
 8  vlan52.ebr2.NewYork2.Level3.net (4.69.138.254)  18.221 ms  19.836 ms  20.310 ms
 9  ae-2-2.ebr1.Chicago1.Level3.net (4.69.132.65)  42.911 ms  48.211 ms *
10  ae-12-51.car2.Chicago1.Level3.net (4.68.101.3)  41.283 ms  43.393 ms  45.052 ms
11  g2-0.gsr12008.sd.chgo.fastservers.net (4.71.182.6)  43.074 ms  52.553 ms  37.739 ms
12  74.200.242.62 (74.200.242.62)  36.307 ms  41.694 ms  37.140 ms
13  74.200.240.50 (74.200.240.50)  36.506 ms  45.658 ms  36.999 ms
14  * * *
15  www.garykessler.net (207.204.17.246)  34.835 ms  36.978 ms  37.555 ms
Moriarty:~ gck$
```


Traceroute's Different Views...

As reported by TRACEROUTE
Moriarty (206.193.152.115) -> Residential LAN (69.162.185.252)



As reported by TRACERT
Residential Host (192.168.1.101) -> Moriarty (216.93.152.115)

NOTES:
Moriarty is on the Champlain College network (216.93.144.0/20)
Residential Host is using RFC 1918 private addressing (192.168.1.0/24)
Residential LAN is on the Comcast network (69.162.128.0/18)

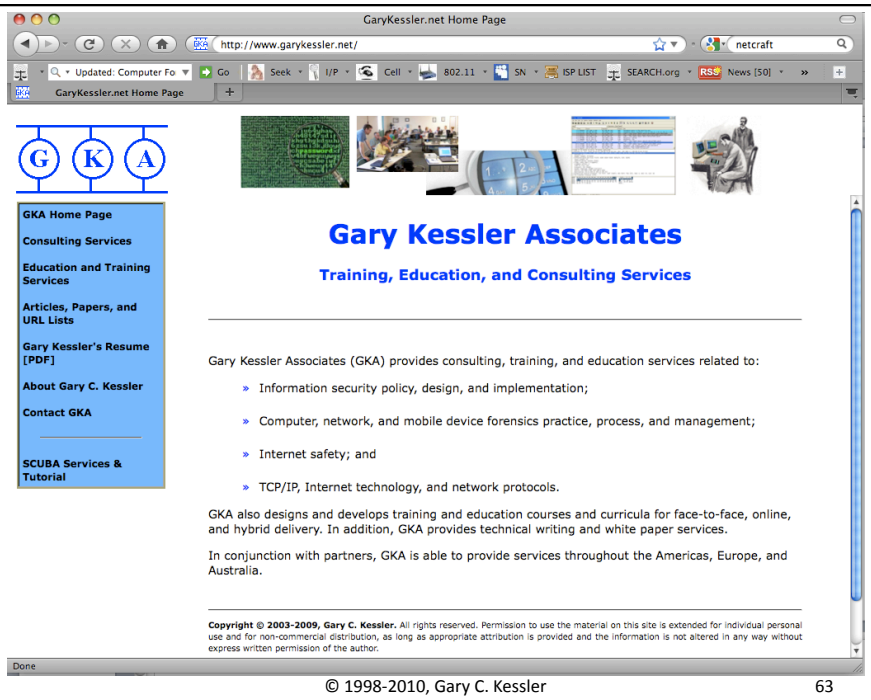
Ping

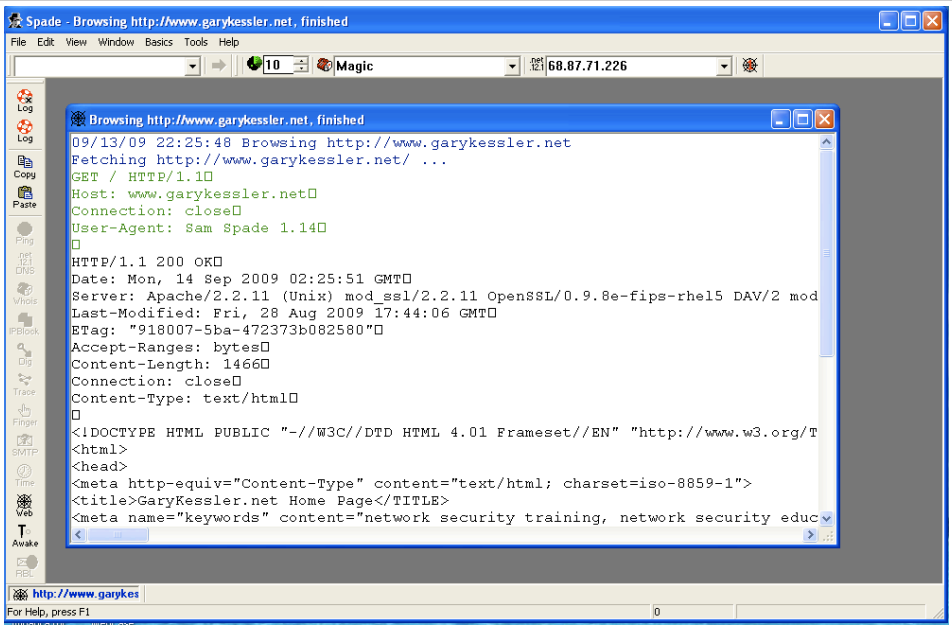
- The single most useful TCP/IP troubleshooting tool

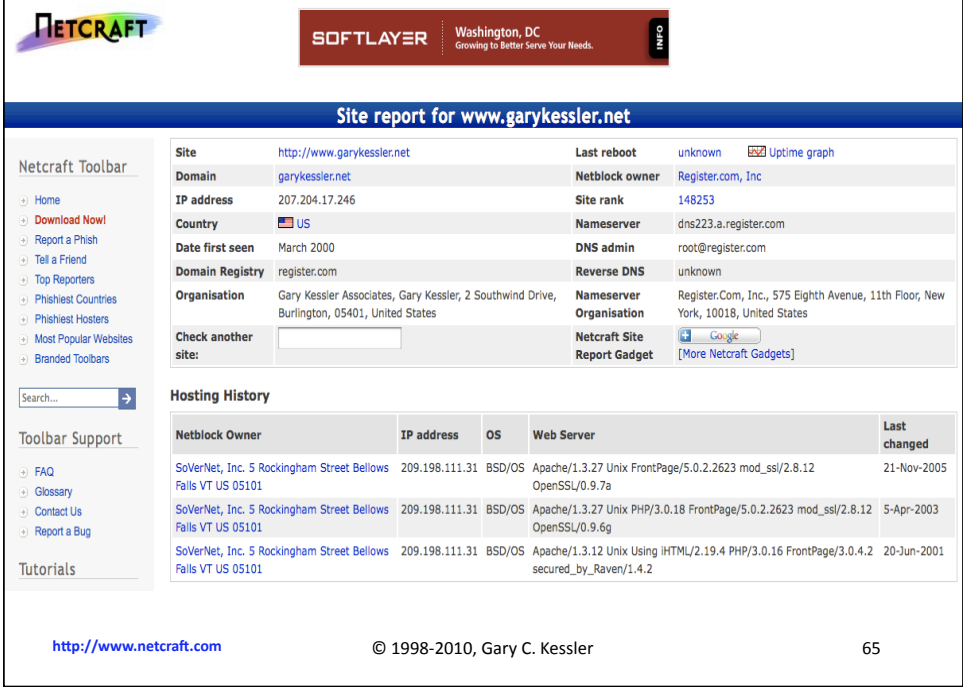
```
C:\> ping granite.sover.net
Pinging granite.sover.net [209.198.87.33] with 32 bytes of data:

Reply from 209.198.87.33: bytes=32 time=42ms TTL=247
Reply from 209.198.87.33: bytes=32 time=28ms TTL=248
Reply from 209.198.87.33: bytes=32 time=28ms TTL=248
Reply from 209.198.87.33: bytes=32 time=28ms TTL=248

Ping statistics for 209.198.87.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 28ms, Maximum =  42ms, Average =  31ms

C:\>
```

The World Wide Web

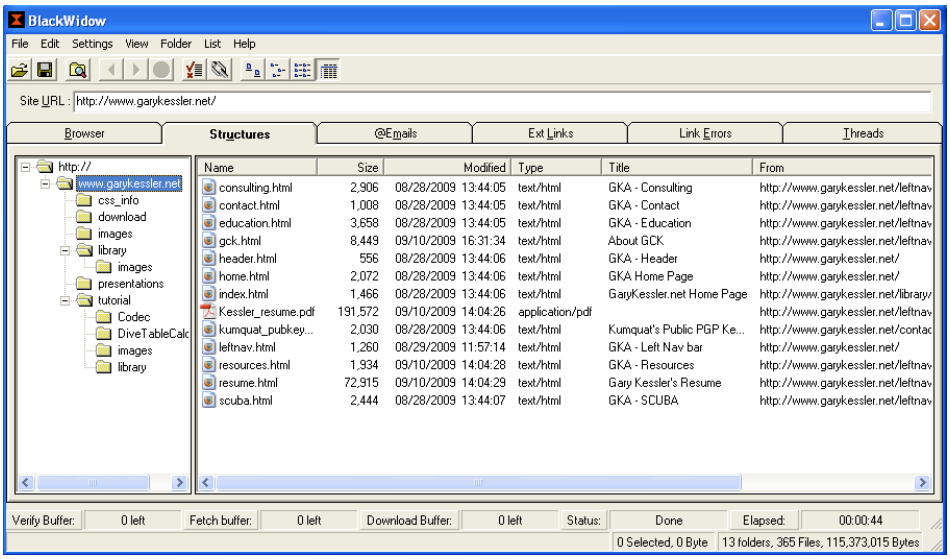
- *Not* a synonym for Internet!!
  - » But accounts for ~65% of all Internet traffic
- HTTP is used for client-server communication
  - » Common servers: Apache, IIS
- Web pages are written in HTML
  - » Java, JavaScript, ActiveX, CGI, Perl, ASPs, ...
- Over 8B Web pages cataloged by Google
  - » 100-200% annual growth



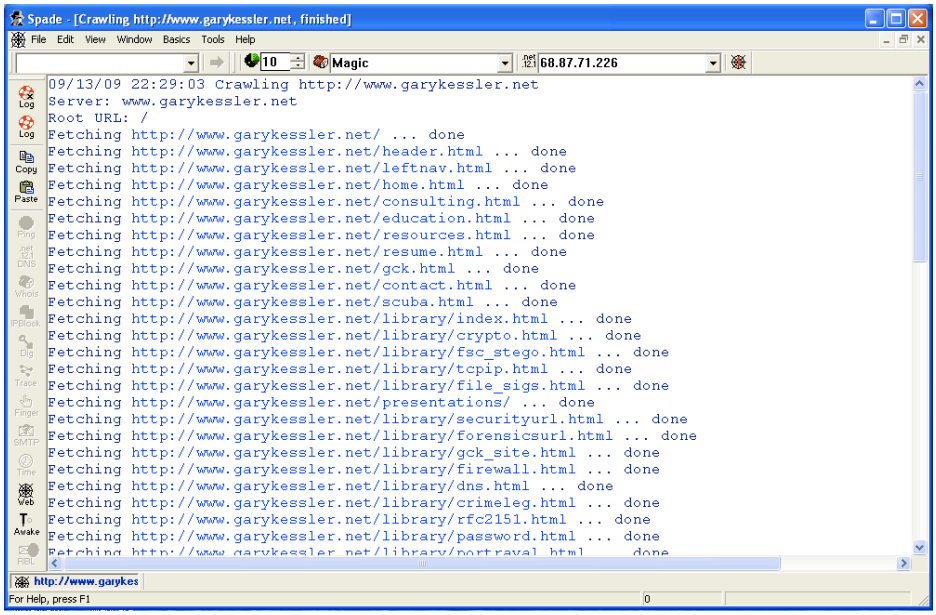




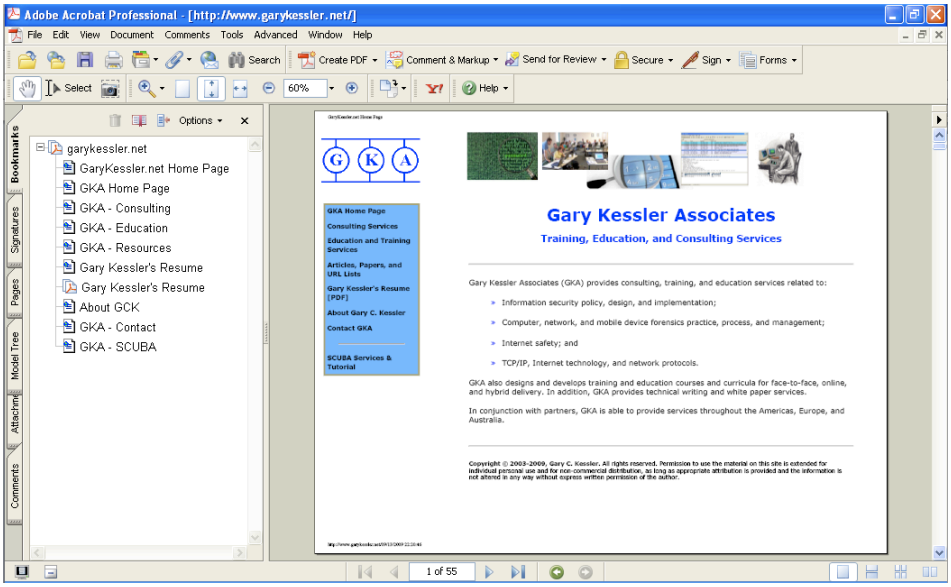
http://www.netcraft.com

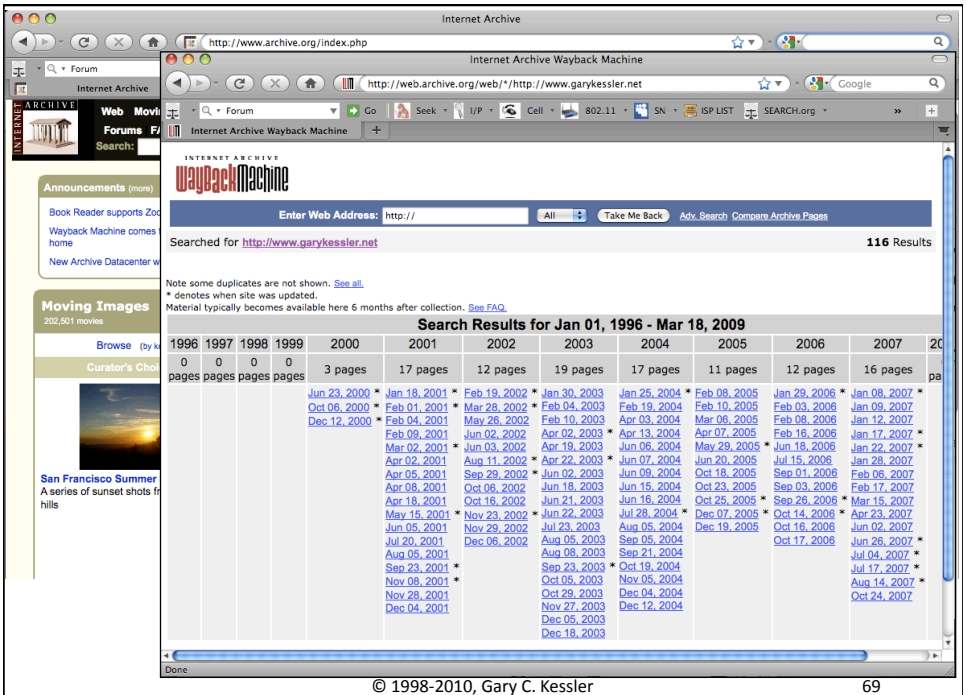


 66



 67


Adobe Acrobat Professional - [http://www.garykessler.net/]
File Edit View Document Comments Tools Advanced Window Help
Search Create PDF Comment & Markup Send for Review Secure Sign Forms
Select 60% Help
Options
garykessler.net
GaryKessler.net Home Page
GKA Home Page
GKA - Consulting
GKA - Education
GKA - Resources
Gary Kessler's Resume
Gary Kessler's Resume
About GCK
GKA - Contact
GKA - SCUBA
Bookmarks Signatures Pages Model Tree Attachments Comments
G K A
GKA Home Page
Consulting Services
Education and Training Services
Articles, Papers, and URL Lists
Gary Kessler's Resume (PDF)
About Gary C. Kessler
Contact GKA
SCUBA Services & Tutorial
Gary Kessler Associates
Training, Education, and Consulting Services
Gary Kessler Associates (GKA) provides consulting, training, and education services related to:
Information security policy, design, and implementation;
Computer, network, and mobile device forensics practice, process, and management;
Internet safety; and
TCP/IP, Internet technology, and network protocols.
GKA also designs and develops training and education courses and curricula for face-to-face, online, and hybrid delivery. In addition, GKA provides technical writing and white paper services.
In conjunction with partners, GKA is able to provide services throughout the Americas, Europe, and Australia.
Copyright © 2003-2009, Gary C. Kessler. All rights reserved. Permission to use the material on this site is extended for individual personal use and for non-commercial distribution, as long as appropriate attribution is provided and the information is not altered in any way without express written permission of the author.
1 of 55


Internet Archive
http://www.archive.org/index.php
Internet Archive Wayback Machine
http://web.archive.org/web/*/http://www.garykessler.net
Internet Archive Wayback Machine
WaybackMachine
Enter Web Address: http://
All
Take Me Back
Adv. Search Compare Archive Pages
Searched for http://www.garykessler.net
116 Results
Note some duplicates are not shown. See all.
* denotes when site was updated.
Material typically becomes available here 6 months after collection. See FAQ.
Search Results for Jan 01, 1996 - Mar 18, 2009
1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007
0 pages 0 pages 0 pages 0 pages 3 pages 17 pages 12 pages 19 pages 17 pages 11 pages 12 pages 16 pages
Announcements
Moving Images
San Francisco Summer
Done

But Aren't These All "Hacker Tools"?

ANALYSIS: Site Enumeration

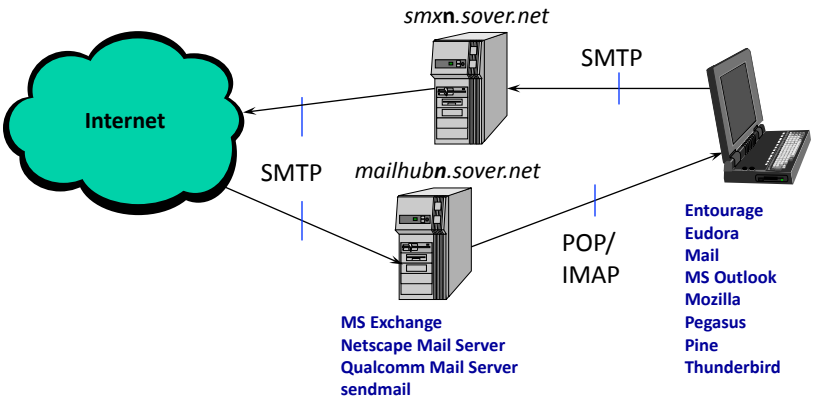
ANALYSIS: Investigating Phishing

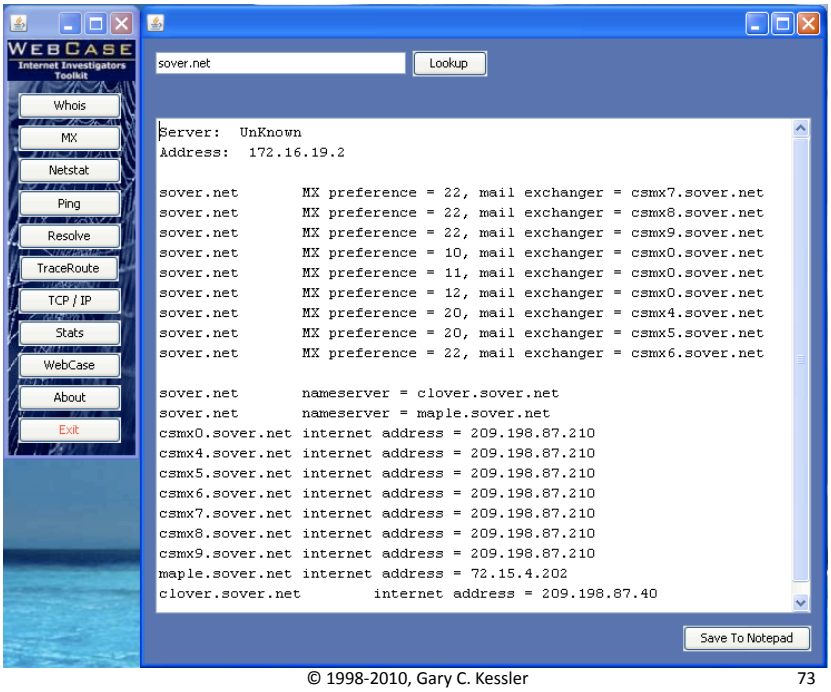
E-mail

- Most widely used Internet application
- E-mail protocols
  - » SMTP: Used between mail servers to forward mail, and from client to mail server to send mail
  - » POP3 and IMAP: Used by client to download e-mail and manage mailbox
- DNS MX records identify the mail server(s) for a given domain
  - » Lowest preference is preferred server

E-Mail Operation and Protocols

What happens to mail to/from *kumquat@sover.net?*





An SMTP Session

```
Moriarty:~ gck$ telnet mail.sover.net 25
220 mail.sover.net ready...
HELO networking.champlain.edu
250 Pleased to meet you...
MAIL FROM:<kesslerg@champlain.edu>
250 Sender OK
RCPT TO:<kumquat@sover.net>
250 Recipient OK
DATA
354 Start mail input; end with <CRLF>.<CRLF>
HI!
.
250 Message accepted for delivery
quit
221 Closing connection
Moriarty:~ gck$
```


E-mail and Headers

```
Return-Path: <kesslerg@champlain.edu>
Received: from mailgate0.sover.net (mailgate0.sover.net [209.198.87.43])
        by mailhub1.sover.net (8.11.6/8.11.6) with ESMTP id g39FNQv14867
        for <kumquat@mailhub1.sover.net>; Tue, 9 Apr 2002 11:23:26 -0400 (EDT)
Received: from networking.champlain.edu (34-67.champlain.edu [198.112.67.34])
        by mailgate0.sover.net (8.11.6/8.11.6) with SMTP id g39FMO713863
        for kumquat@sover.net; Tue, 9 Apr 2002 11:22:59 -0400 (EDT)
Date: Tue, 9 Apr 2002 11:22:59 -0400 (EDT)
From: kesslerg@champlain.edu
Message-Id: <200204091522.g39FMO713863@mailgate0.sover.net>
Status: RO

HI!
```

A POP3 Session

```
Moriarty:~ gck$ telnet pop3.example.com 110
+OK POP3 server ready pop3.example.com
USER gck
+OK Hello gck
PASS secret
+OK You are so in
LIST
+OK 2 messages (320 octets)
1 120
2 200
.
RETR 1
+OK 120 octets
<the POP3 server displays message 1>
.
DELE 1
+OK message 1 deleted
RETR 2
+OK 200 octets
<the POP3 server displays message 2>
.
DELE 2
+OK message 2 deleted
QUIT
+OK Sayonara

Moriarty:~ gck$
```


A Suspect Attachment

```
This is a multipart message in MIME format
--CSmtpMsgPart123X456_000_001DA0A7
Content-Type: text/plain;
        charset="iso-8859-1"
Content-Transfer-Encoding: 7bit
All information is in the attached file.
--CSmtpMsgPart123X456_000_001DA0A7
Content-Type: application/octet-stream;
         name="password.pif"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
         filename="password.pi"
TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAA6AAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1v
ZGUuDQ0KJAAAAAAAAACu45jY6oL2i+qC9ovqgvaLaZ74i/CC9osCnfyLm4L2i7yd5YvngvaL6oL2
i+mC9ovqgveLZ4L2i4id5YvngvaLAp39i/OC9otSaWNo6oL2iwAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAFBFAABMAQMA+w7FPgAAAAAAAAA4AAPAQsBBgAAwAAAABAAAAAAAQCAygEAABABAADQAQAA
AEAAABAAAAACAAAEAAAAAAAAAAQAAAAAAAAAAOABAAAQAAAAAAAAgAAAAAAEAAAEAAAAAAQAAAQ
AAAAAAAAEAAAAAAAAAAAAAAAAAANABANABAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

remainder of e-mail deleted
```

Understanding BASE64

- BASE64 is a special encoding scheme to allow the transfer of bit/byte/octet-streams in e-mail
- The bit stream appears as a string of ASCII characters
  - » One byte (8 bits) can take on a value between 0 & 255
  - » BASE 64 (6 bits) contains only: A-Z a-z 0-9 + /
  - » See *http://www.garykessler.net/library/base64.html*
- Three bytes (24 bits) in the octet stream are converted into four BASE64 characters (24 bits)

Deciphering the Attachment

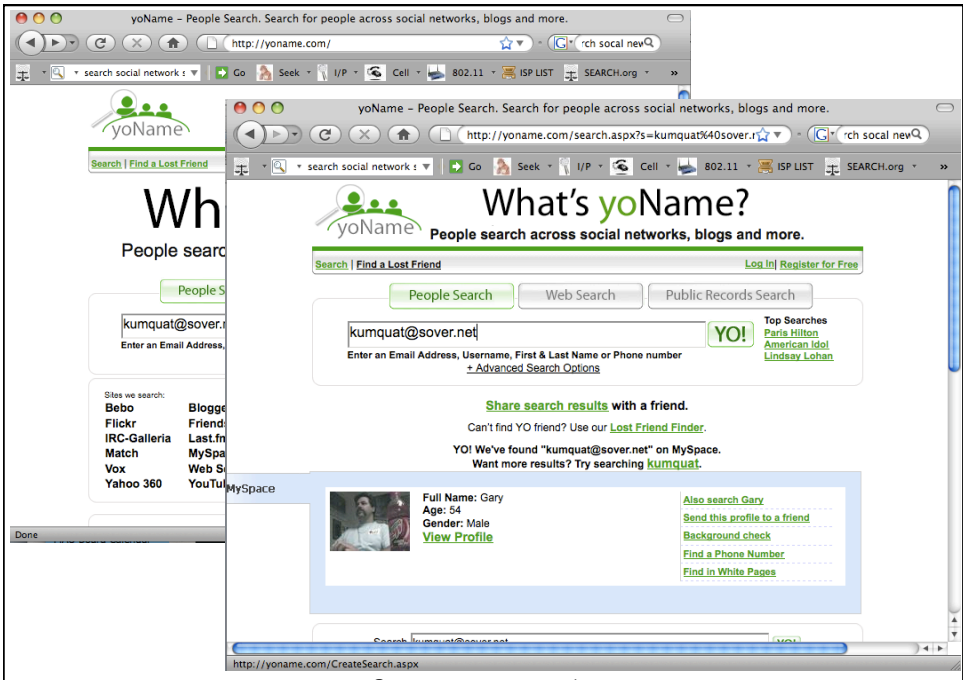
```
BASE64:   T      V      q      Q
          0x13   0x15   0x2A   0x10
          010011 010101 101010 010000

Regroup:  01001101 01011010 10010000
          0x4D     0x5A     0x90
ASCII:    M        Z        0x90
```

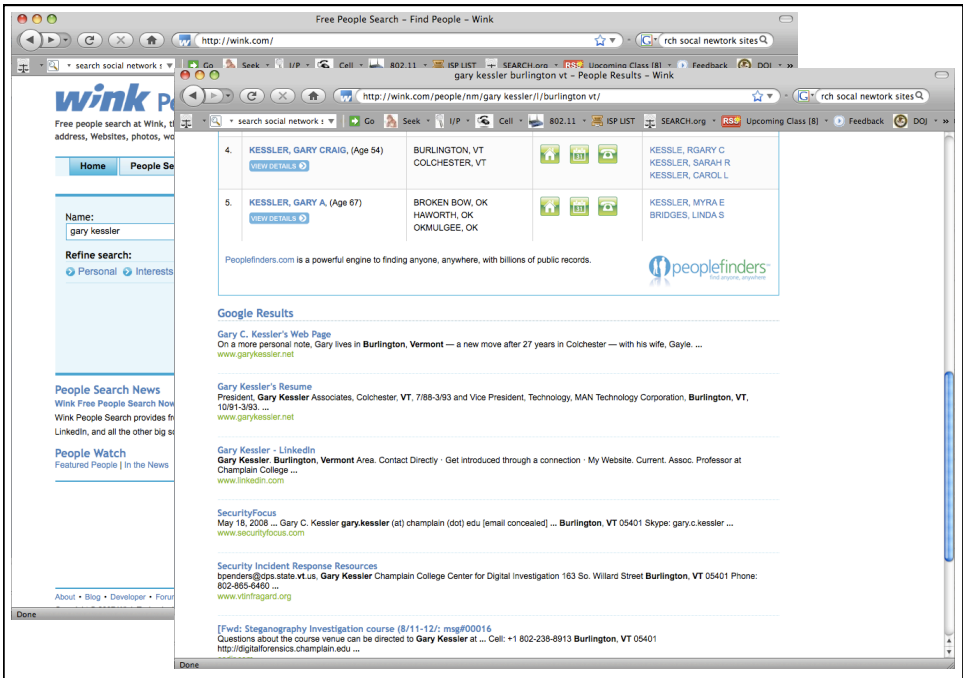
File signature for Windows executable file

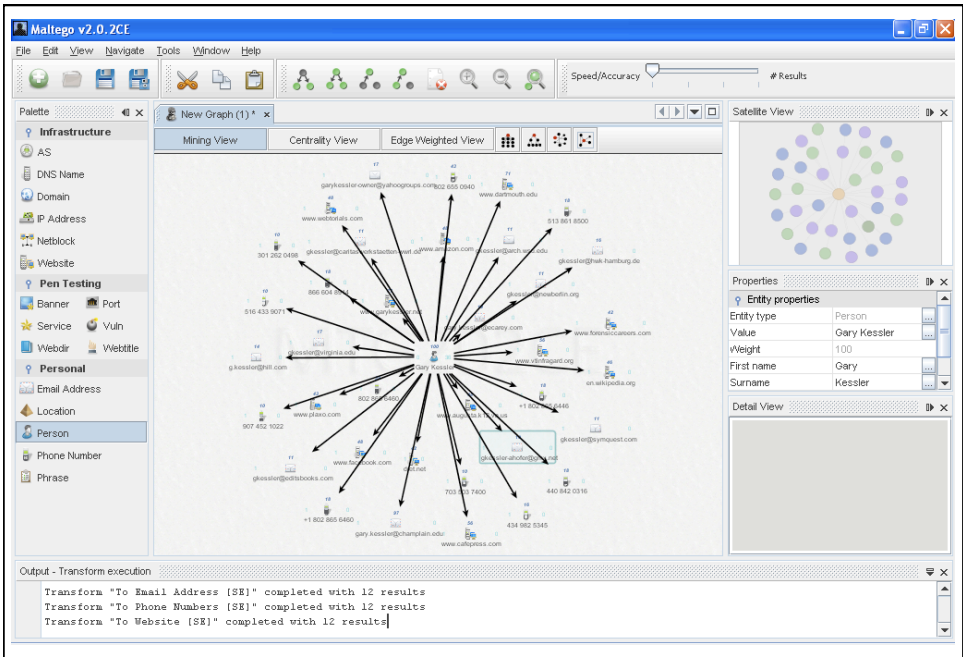
How can a bunch of ASCII characters hurt us? Remember that BASE64 encoding was specifically designed to transport a bit stream without appearing like a bit stream. The TVqQ string appears to be a set of four ASCII characters but it is actually a representation of 6-bit blocks which must be translated into the 8-bit byte (octet) stream... and now appears to be something much different!!

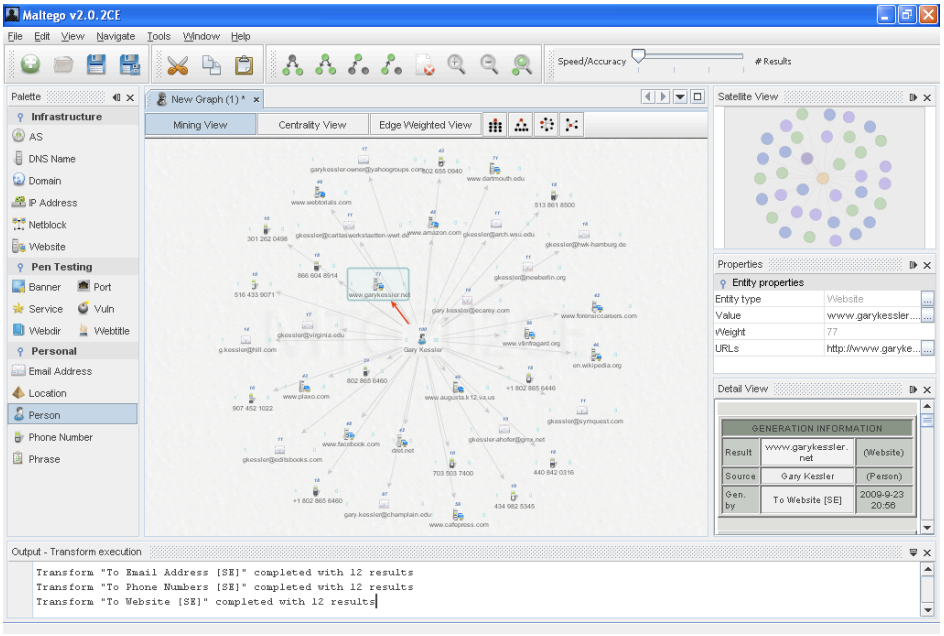
Social Networks (Web 2.0)

- Social networks (Web 2.0)
  - » Wikipedia lists >125 *notable, well known* social networking sites
    - Sites include Adult FriendFinder, Bebo, Facebook, Flickr, LinkedIn, MySpace, Plaxo, and Playboy U
    - *http://en.wikipedia.org/wiki/List_of_social_networking_websites*
  - » Other sites help you search across social networks (your mileage may vary)
    - http://yoname.com/
    - http://wink.com/
- Finding people
  - » Several sites help you find people, particularly for LE
  - » Maltego is very powerful open source sofware





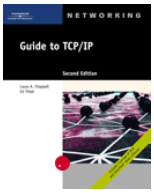




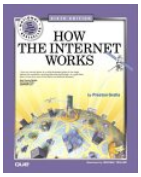
Summary

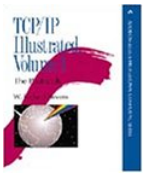
- Internet structure
- TCP/IP protocol suite
  - » IP addressing
  - » TCP/UDP ports
- Higher layer applications and tools
  - » DNS
  - » World Wide Web
  - » E-mail and BASE64
  - » Social networks and finding people

For More Information...



- *Guide to TCP/IP*, Chappell & Tittell
- *How the Internet Works,* Gralla
- *TCP/IP Illustrated, Vol. 1*, Stevens





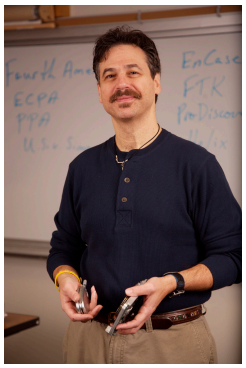
- "An Overview of TCP/IP Protocols and the Internet" (*www.garykessler.net/library/tcpip.html)*
- "TCP/IP and tcpdump Pocket Reference Guide" (*www.garykessler.net/download/tcpip/tcpip_prg.pdf*)

Speaker Contact Information

Gary C. Kessler, Ph.D., CCE, CISSP
GARY KESSLER ASSOCIATES
2 Southwind Drive
Burlington, VT 05401

mobile: +1 802-238-8913
e-mail: gck@gary*kessler.net*
gkessler@bpdvt.org
Skype: *gary.c.kessler*

http://www.garykessler.net
http://www.vtinternetcrimes.org



Acronyms and Abbreviations

ADSL	Asymmetric Digital Subscriber Line
ARP	Address Resolution Protocol (IETF)
ASCII	American Standard Code for Information Interchange
ASP	Active Server Pages (MS)
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol (IETF)
CGI	Common Gateway Interface
CSLIP	Compressed SLIP
DHCP	Dynamic Host Configuration Protocol (IETF)
DNS	Domain Name System (IETF)
DSU	Data service unit
DWDM	Dense wave division multiplexing
FDDI	Fiber Distributed Data Interface
FTP	File Transfer Protocol (IETF)
gTLD	Global Top-Level Domain
HDLC	High-level Data Link Control
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol (IETF)
ICANN	Internet Corp. for Assigned Names and Numbers
ICMP	Internet Control Message Protocol (IETF)
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IIS	Internet Information Server (MS)
IMAP	Internet Message Access Protocol (IETF)
IP	Internet Protocol (IETF)
IPv4/IPv6	Internet Protocol version 4, version 6
ISDN	Integrated services digital network
ISP	Internet service provider
NAP	Network access point
NNTP	Network News Transport Protocol (IETF)
NTP	Network Time Protocol (IETF)
OSPF	Open Shortest Path First (IETF)
POP	Post Office Protocol (IETF)
POTS	Plain old telephone service
PPP	Point-to-Point Protocol (IETF)
RADIUS	Remote Authentication Dial-In User Service
RFC	Request for Comments (IETF)
RIP	Routing Information Protocol (IETF)
SDH	Synchronous Digital Hierarchy
SLIP	Serial Line IP (IETF)
SMDS	Switched Multimegabit Data Service
SMTP	Simple Mail Transfer Protocol (IETF)
SNAP	Subnetwork Access Protocol (IEEE)
SNMP	Simple Network Management Protocol (IETF)
SONET	Synchronous Optical Network
SSH	Secure Shell
SSL	Secure Sockets Layer (Netscape)
TA	Terminal adapter (ISDN)
TACACS+	Terminal Access Controller Access Control System plus
TCP	Transmission Control Protocol (IETF)
TFTP	Trivial File Transfer Protocol (IETF)
TLD	Top-level domain
TLS	Transport Layer Security (IETF)
UDP	User Datagram Protocol (IETF)
vBNS	Very high speed Backbone Network Service
xDSL	Digital Subscriber Line technology family
WWW	World Wide Web

Questions? Comments? Queries?