CEIC 2011

Tracing IP Addresses

Gary C. Kessler
Vermont Internet Crimes Against Children Task Force
Gary Kessler Associates/Norwich University

Overview

CEIC 2011

- 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

CEIC 2011

What does the 'Net look like, anyway?

CEIC 2011

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

CEIC 2011

- 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 2000
- 768.9M hosts in the DNS (7/2010)
  - 1.02M are named *www* (#1, not counting *www1*, *www2*, *web*, and other variants)
  - 928K are named *mail* (#2, not counting *mx*, *smtp*, *pop*, *mailer*, and other variants)

Internet User Demographics

CEIC 2011

WORLD INTERNET USAGE AND POPULATION STATISTICS

World Regions	Population (2010 Est.)	Internet Users Dec. 31, 2000	Internet Users Latest Data	Penetration (% Population)	Growth 2000-2010	Users % of Table
Africa	1,013,779,050	4,514,400	110,931,700	10.9 %	2,357.3 %	5.6 %
Asia	3,834,792,852	114,304,000	825,094,396	21.5 %	621.8 %	42.0 %
Europe	813,319,511	105,096,093	475,069,448	58.4 %	352.0 %	24.2 %
Middle East	212,336,924	3,284,800	63,240,946	29.8 %	1,825.3 %	3.2 %
North America	344,124,450	108,096,800	266,224,500	77.4 %	146.3 %	13.5 %
Latin America/Caribbean	592,556,972	18,068,919	204,689,836	34.5 %	1,032.8 %	10.4 %
Oceania / Australia	34,700,201	7,620,480	21,263,990	61.3 %	179.0 %	1.1 %
WORLD TOTAL	6,845,609,960	360,985,492	1,966,514,816	28.7 %	444.8 %	100.0 %

NOTES: (1) Internet Usage and World Population Statistics are for June 30, 2010. (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 © 2000 - 2010, Miniwatts Marketing Group. All rights reserved worldwide.

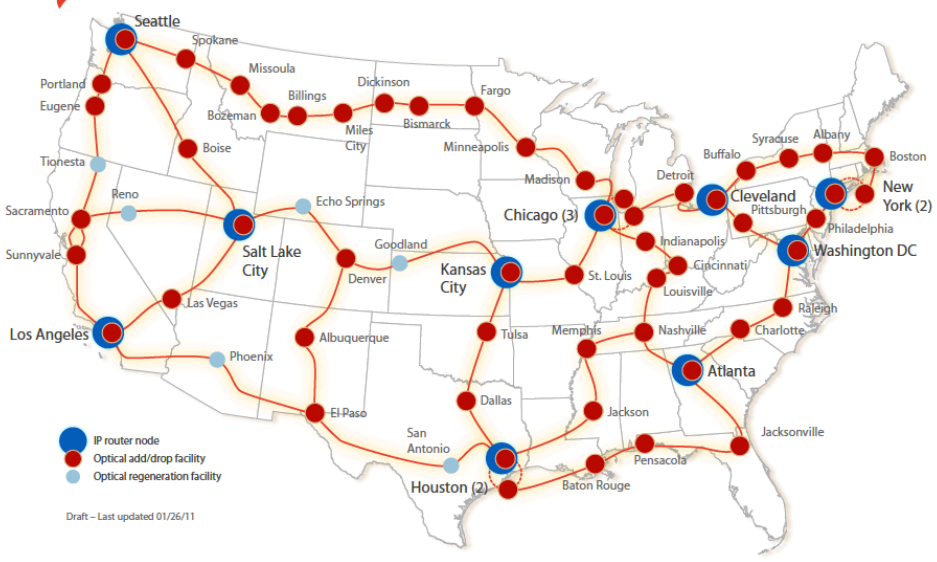
Source: *http://www.internetworldstats.com/stats.htm*

Internet Administration

CEIC 2011

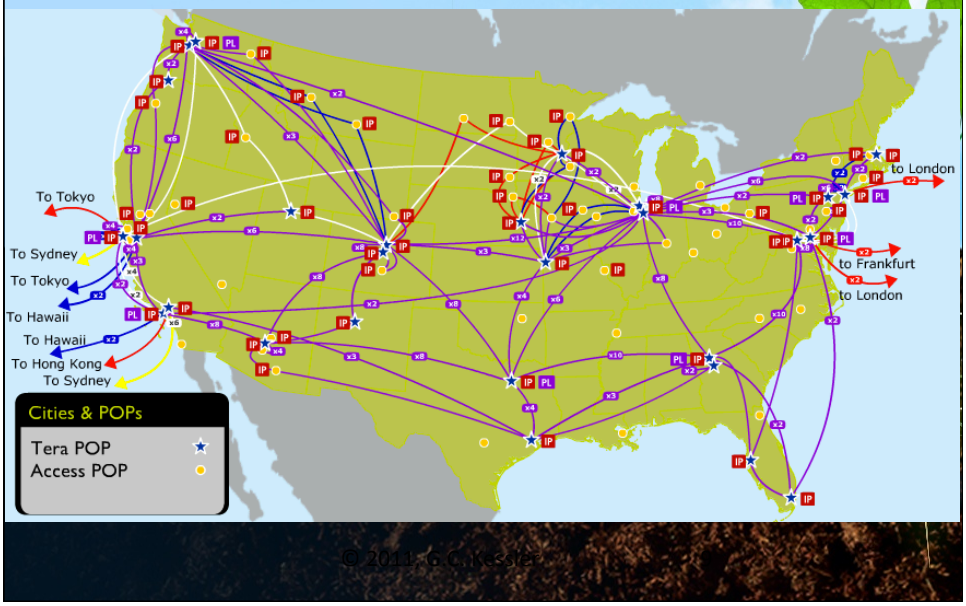
- Internet Society (ISOC)
- Internet Engineering Task Force (IETF)
- Internet Assigned Numbers Authority (IANA)
- The Internet Corporation for Assigned Names and Numbers (ICANN)
  - Name registries include VeriSign Global Registry Services (.com, .net) and the Public Interest Registry (.org)
  - Not 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)

Internet2 Planned 100 Gigabit Infrastructure Topology (DRAFT)



CEIC 2011

Qwest IP Network Backbone



CEIC 2011

The Communications Language of the Internet

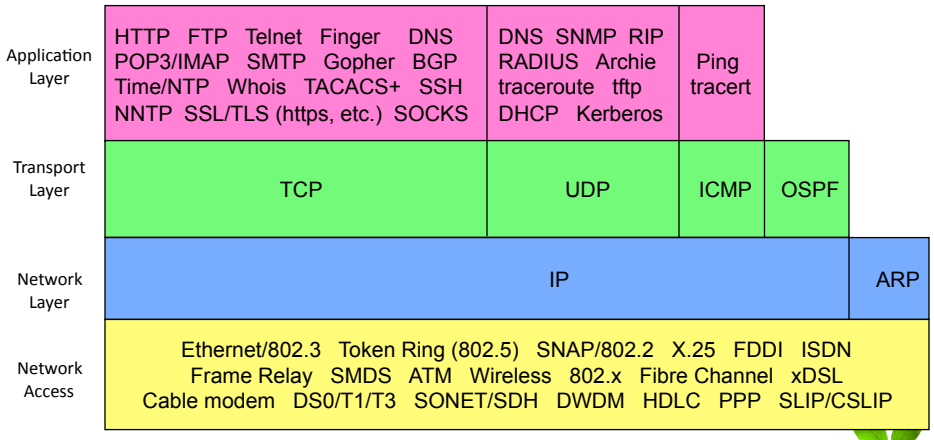
The Internet and TCP/IP

CEIC 2011

- 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??*

The TCP/IP Protocol Suite

CEIC 2011



Internet Protocol

CEIC 2011

- 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

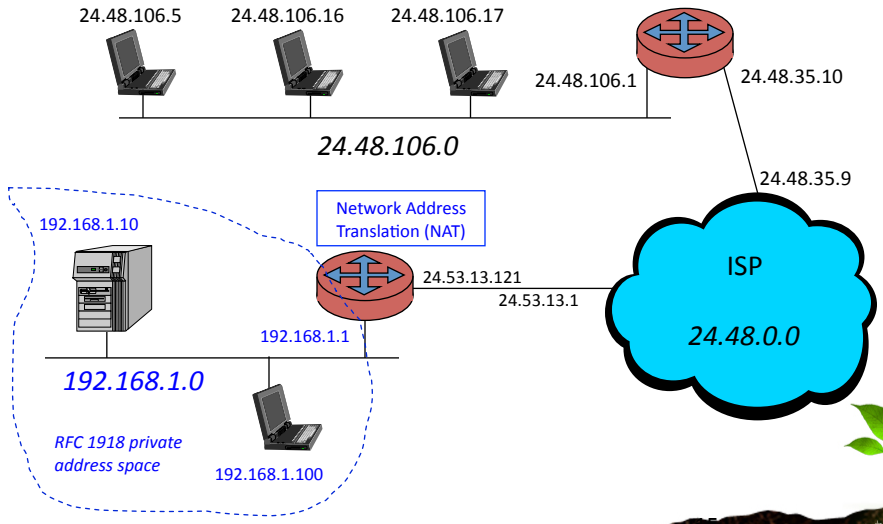
CEIC 2011

- IP version 4 (IPv4) addresses are 32 bits (4 bytes) 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

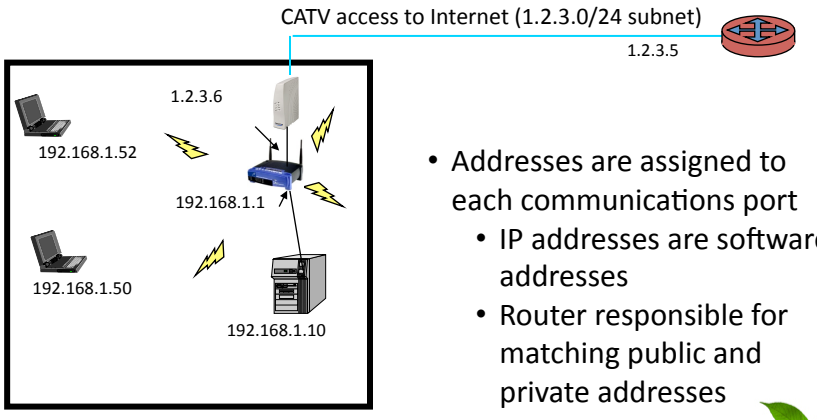
IP Addressing

CEIC 2011



IP Addressing and NAT

CEIC 2011



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

IP version 6 Addressing

CEIC 2011

- IP version 6 (IPv6) addresses are 128 bits (16 bytes) 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 as 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
  - IPv4 mapped addresses -- ::ffff:0:0/96

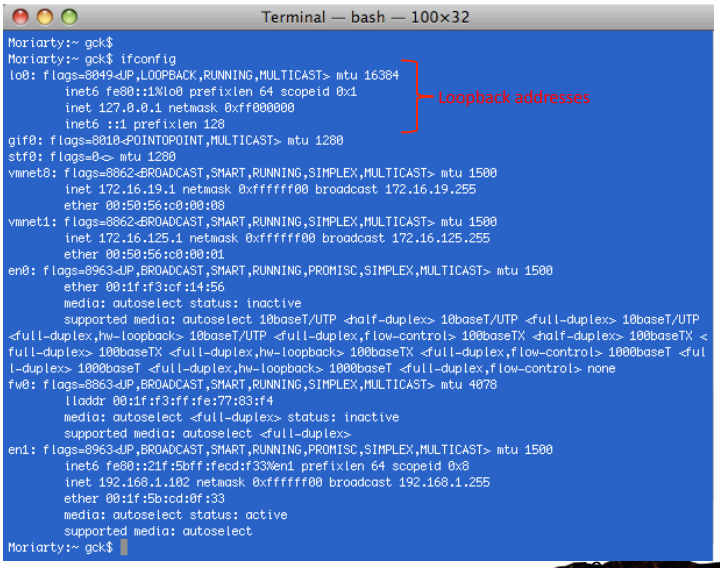
See http://en.wikipedia.org/wiki/IPv6#Addressing and http://www.tcpipguide.com/free/t_IPv6Addressing.htm

ipconfig (DOS/Windows)

CEIC 2011

```
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)



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

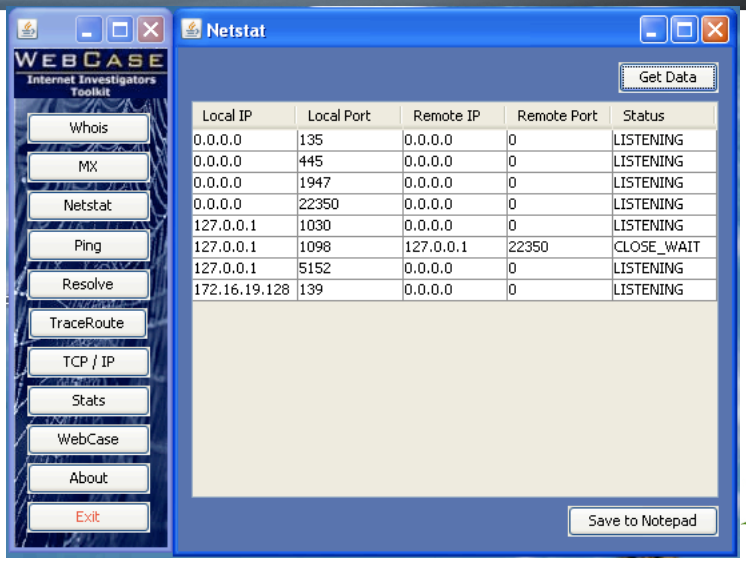
Port No.	Protocol	Application	Port No.	Protocol	Application
7	UDP	echo	80	TCP	http
13	TCP	daytime	110	TCP	pop3
19	UDP	chargen	111	TCP	sunrpc
20	TCP	ftp-data	113	TCP	auth
21	TCP	ftp-control	119	TCP	nntp
22	TCP	ssh	123	UDP	ntp
23	TCP	telnet	137	UDP	netbios-ns
25	TCP	smtp	138	UDP	netbios-dgm
37	UDP	time	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

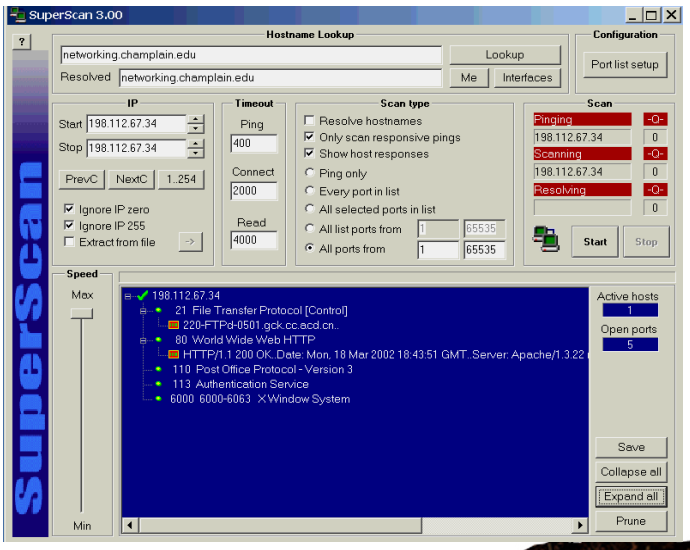
```
[gck@networking gck]$ netstat -atu
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 *:x11                   *:*                     LISTEN
tcp        0      0 *:http                  *:*                     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
```


And tools to examine TCP/IP and Internet information

Internet Domain Names

CEIC 2011

- 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!!

CEIC 2011

- 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!!

CEIC 2011

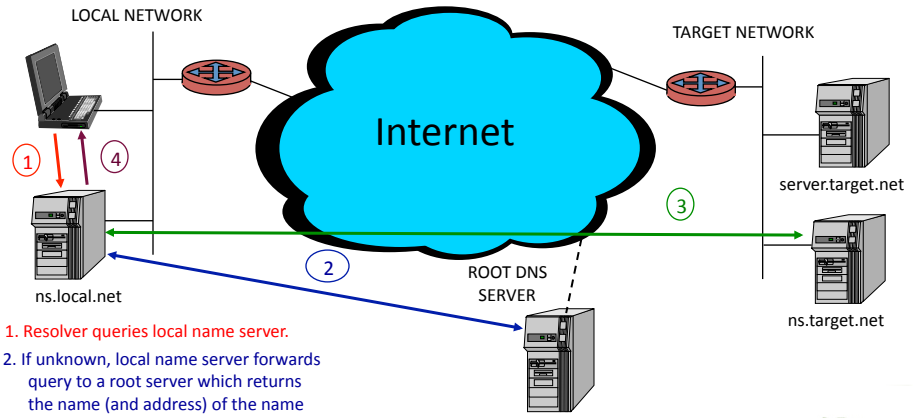
- ICANN approved Internationalized Domain Names (IDNs) as ccTLDs in May 2010:
  - Egypt: مصر (MaSr)
  - Saudi Arabia: السعودية (Al Saudiah)
  - Russian Federation: .pф
  - United Arab Emirates: امارات (Emaarat)

DNS

CEIC 2011

- 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

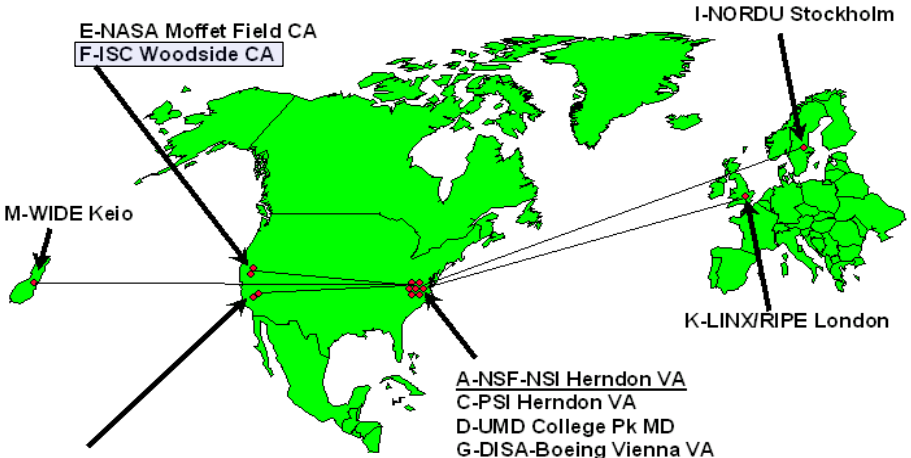


1. Resolver queries local name server.
2. If unknown, local name server forwards query to a root server which returns the name (and address) of the name server for the target domain.
3. Target network's name server replies to local name server.
4. Local name server responds to resolver.

DNS Root Servers

1 Feb 98

Designation, Responsibility, and Locations



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

DNS Resource Records

CEIC 2011

```
example.com.   IN SOA  ns.example.com.
     hostmaster.example.com.  (
   2011021416   ; serial # (YYYYMMDDHH 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
www.example.com.          IN  AAAA 2001:468:d01:3c::80df:3c15
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.
```


IP Addresses and Domain Names

CEIC 2011

- IP address and domain name ownership are 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

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 <<<
```

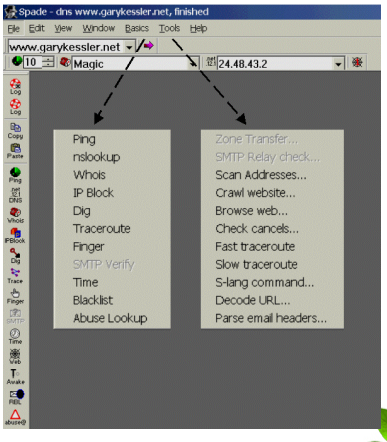
Some versions of *nix (e.g., RedHat, FreeBSD) will automatically redirect the query…

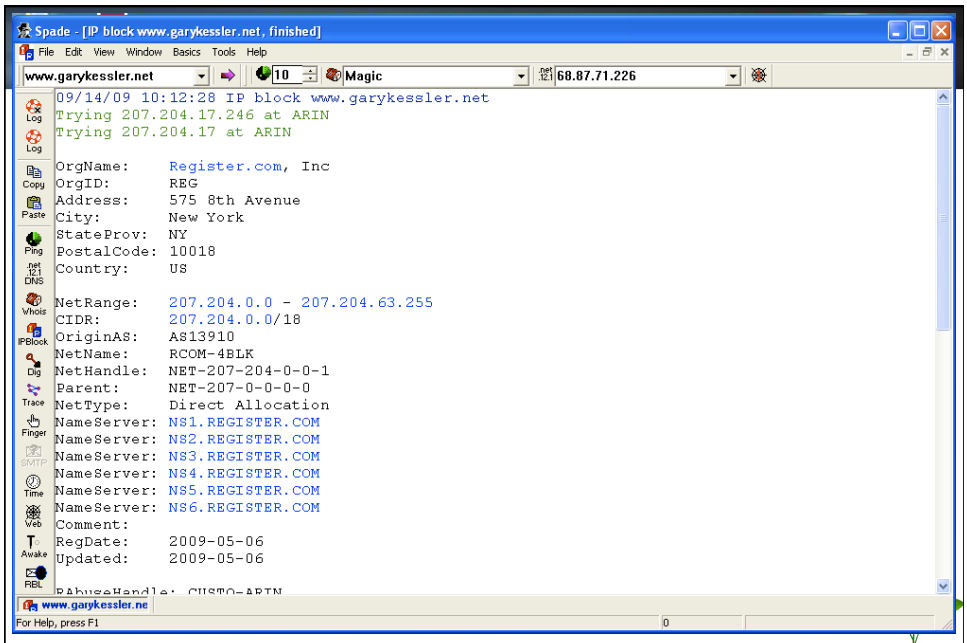

```
                :
    Registrant:
    Gary Kessler Associates
    Gary Kessler
    2 Southwind Drive
    Burlington, VT 05401
    US
    Email: gck@garykessler.net

  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$
```

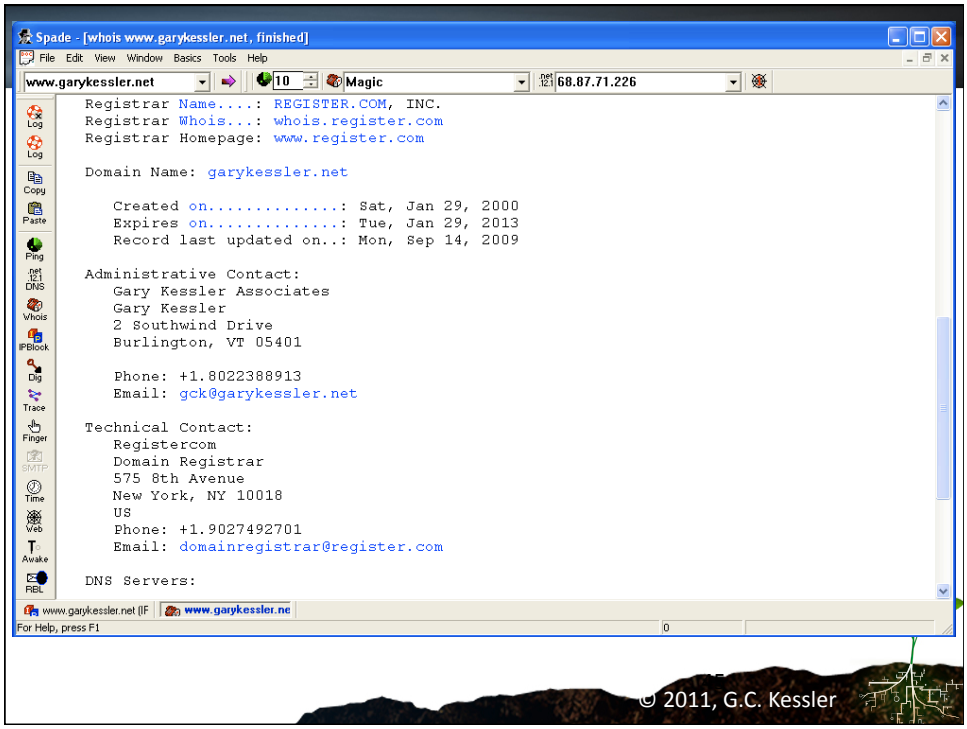
Sam Spade

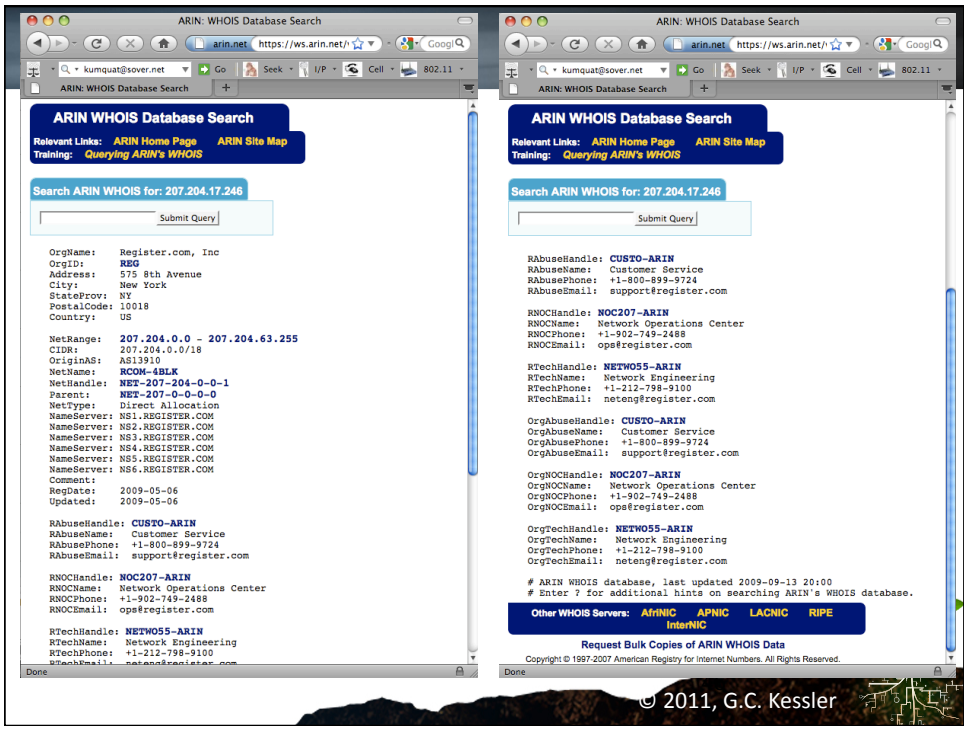
CEIC 2011

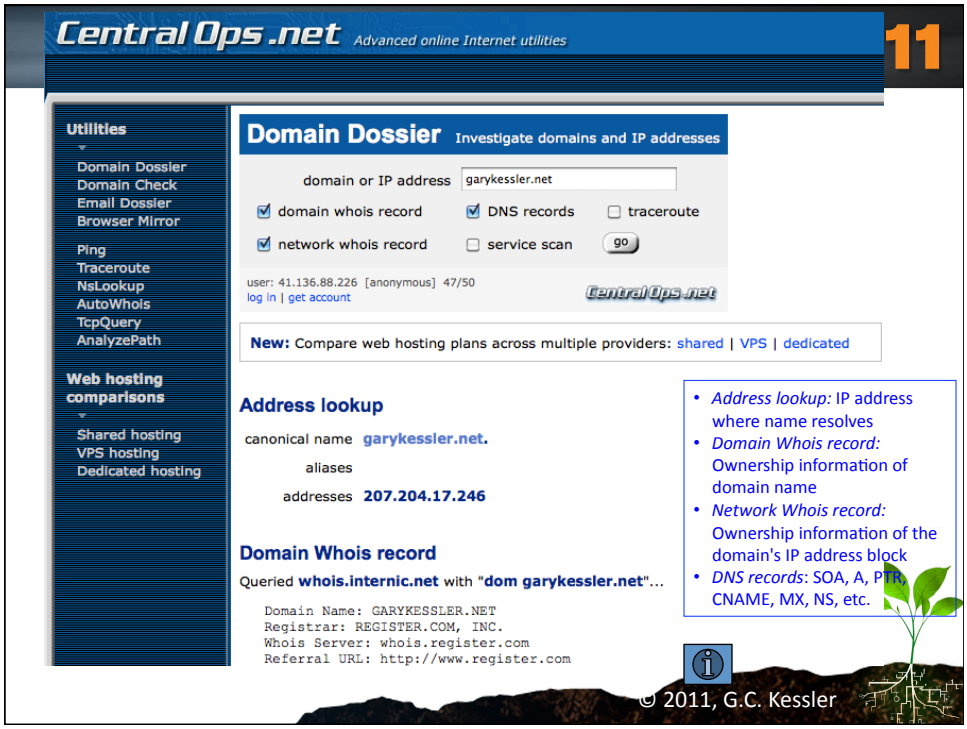
- Provides wide range of information gathering functions
- Run or download from *www.samspade.org*







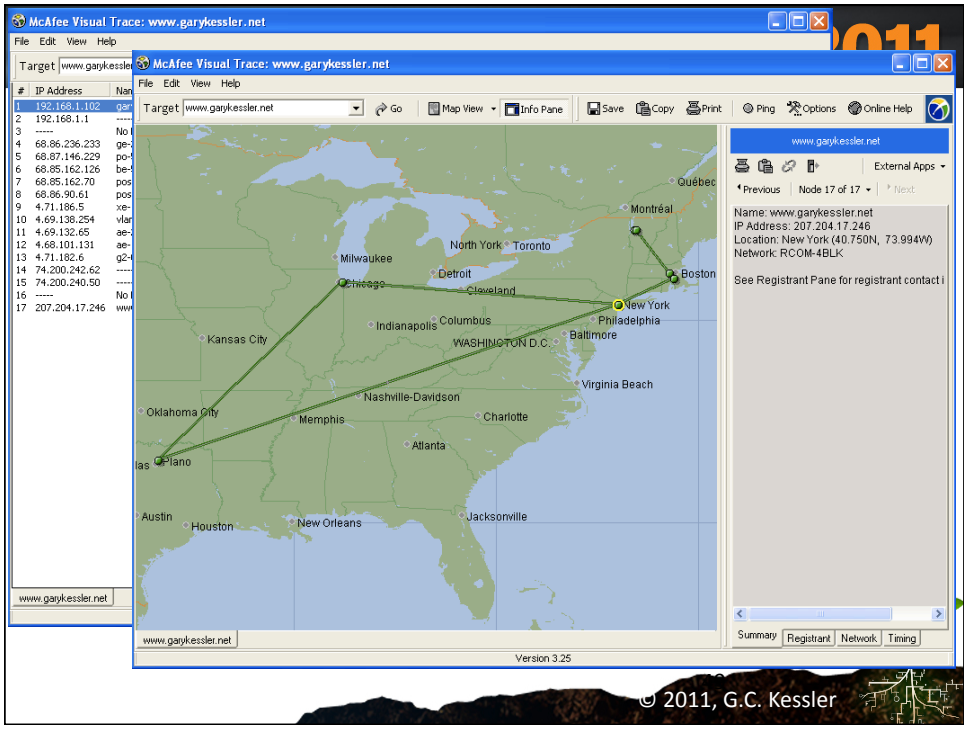




Traceroute

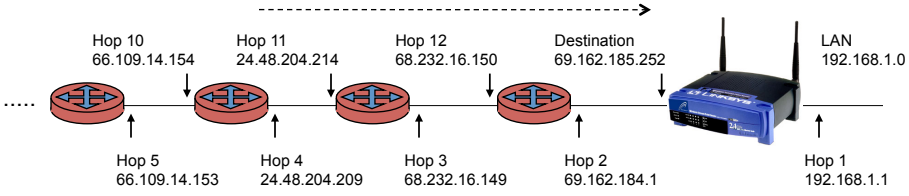
CEIC 2011

```
Moriarty:~ gck$ traceroute www.garykessler.net
traceroute to www.garykessler.net (207.204.17.246), 64 hops max, 40 byte packets
 1  10.0.1.1 (10.0.1.1)  3.390 ms  0.782 ms  0.683 ms
 2  10.1.11.1 (10.1.11.1)  3.403 ms  2.006 ms  2.104 ms
 3  204-13-47-117-dsl.burlingtontelecom.net (204.13.47.117)  1.896 ms  2.427 ms  1.854 ms
 4  bt-btv-core-g01.burlingtontelecom.com (204.13.40.35)  2.007 ms  3.229 ms  2.249 ms
 5  border7.ge1-9.burlingtontel-3.bsn.pnap.net (66.151.237.209)  10.052 ms  9.883 ms  17.214 ms
 6  core5.te6-1-bbnet1.bsn.pnap.net (63.251.128.17)  11.209 ms
    core5.te6-2-bbnet2.bsn.pnap.net (63.251.128.81)  10.066 ms
    core5.te6-1-bbnet1.bsn.pnap.net (63.251.128.17)  10.755 ms
 7  te4-1.ccr01.bos06.atlas.cogentco.com (38.104.252.69)  210.327 ms  172.247 ms  97.722 ms
 8  te0-4-0-4.ccr22.bos01.atlas.cogentco.com (66.28.4.253)  32.877 ms  32.871 ms  33.311 ms
 9  te0-5-0-5.ccr22.ord01.atlas.cogentco.com (154.54.43.73)  32.424 ms
    te0-1-0-7.ccr21.ord01.atlas.cogentco.com (154.54.43.193)  32.971 ms
    te0-4-0-7.ccr22.ord01.atlas.cogentco.com (154.54.43.205)  33.529 ms
10  te0-1-0-3.ccr22.ord03.atlas.cogentco.com (154.54.1.2)  32.952 ms  33.379 ms
    te0-5-0-3.ccr22.ord03.atlas.cogentco.com (154.54.43.234)  32.940 ms
11  38.104.102.102 (38.104.102.102)  33.253 ms  49.915 ms  32.746 ms
12  border5.po1-bbnet1.chg.pnap.net (64.94.32.10)  33.138 ms  33.093 ms  33.861 ms
13  layeredtech-6.border5.chg.pnap.net (74.217.8.10)  33.353 ms  42.694 ms  33.018 ms
14  74.200.240.14 (74.200.240.14)  33.076 ms  33.363 ms  32.861 ms
15  207.204.17.246 (207.204.17.246)  33.334 ms  32.884 ms  32.697 ms
Moriarty:~ gck$
```



Traceroute's Different Views...

As reported by TRACEROUTE
Moriarty (204.13.42.115) -> Residential LAN (69.162.185.252)



As reported by TRACERT
Residential Host (192.168.1.101) -> Moriarty (204.13.42.115)

NOTES:
Moriarty is on the Burlington Police Department network which is part of the Burlington Telecom address block (204.13.40.0/21)
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)

© 2011, G.C. Kessler

Ping

CEIC 2011

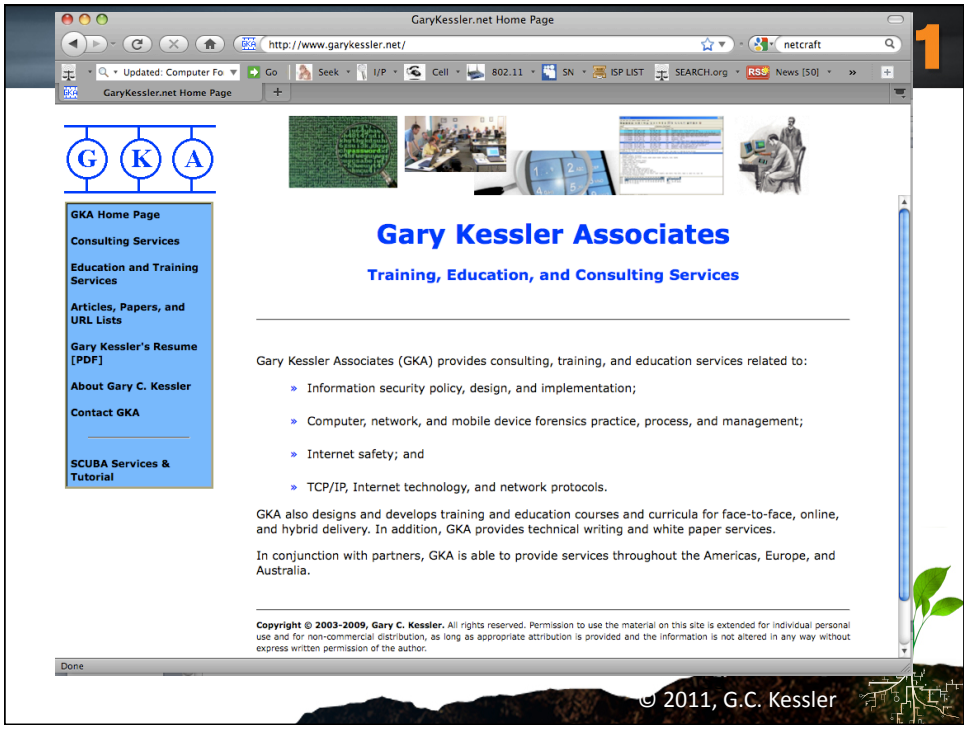
- The single most useful TCP/IP troubleshooting tool

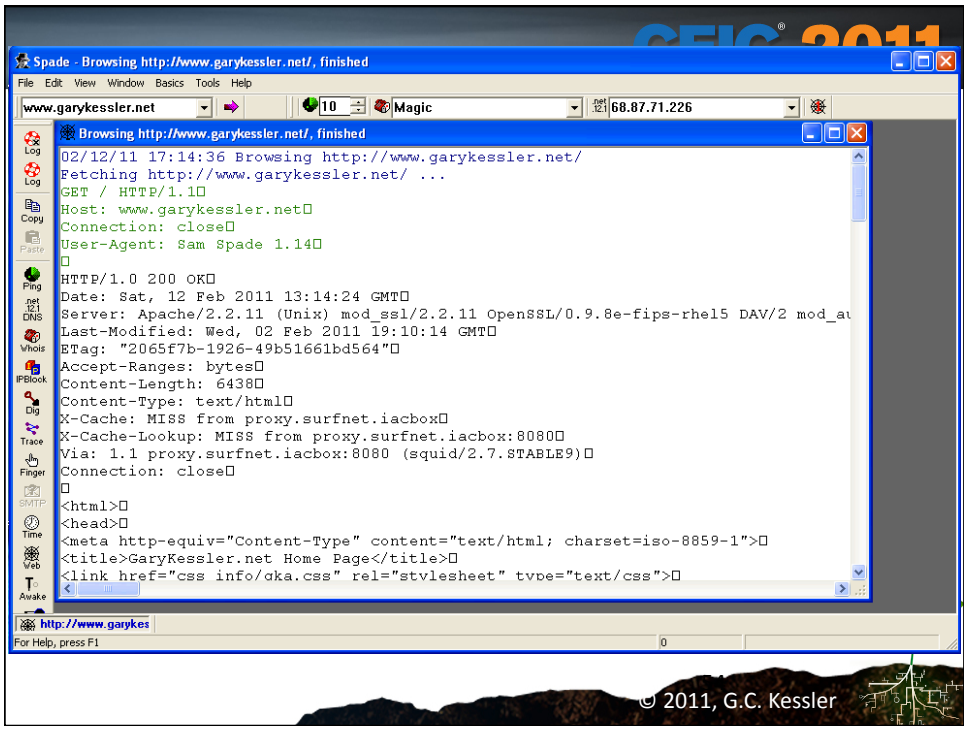
```
C:\> ping granite.sover.net
Pinging granite.sover.net [209.198.87.33] with 32 bytes of data:

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:\>
```

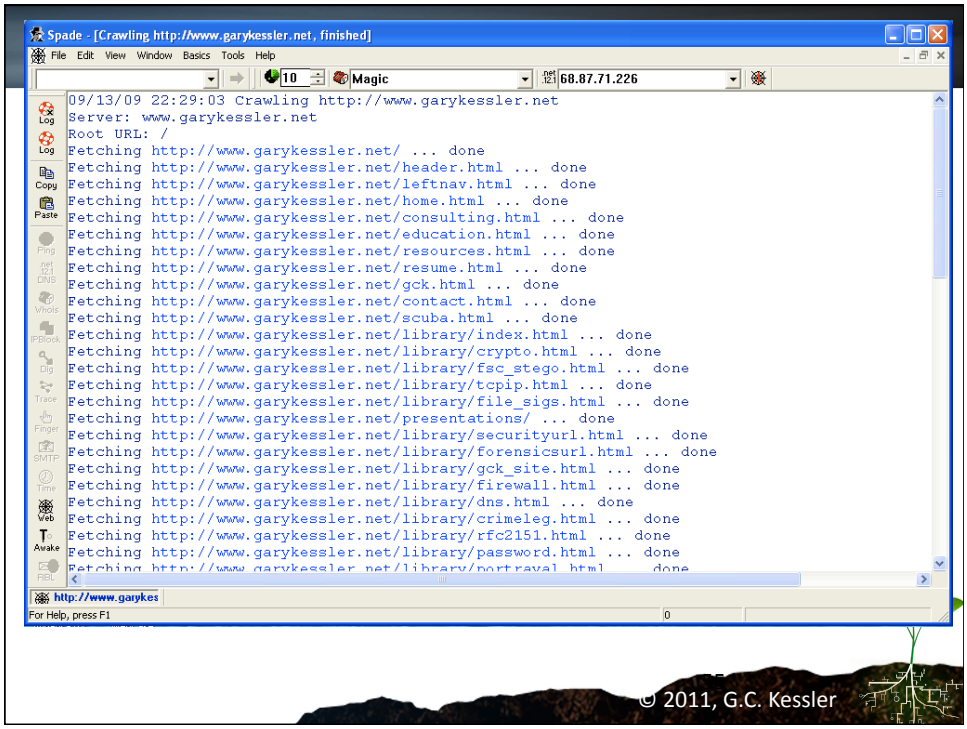
The World Wide Web

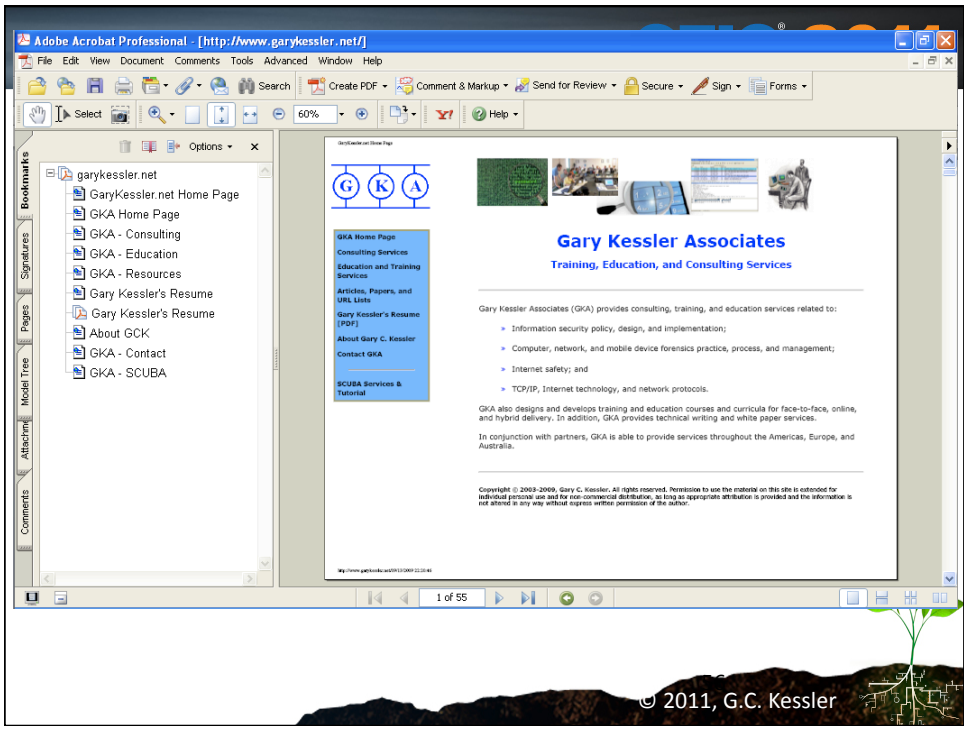
CEIC 2011

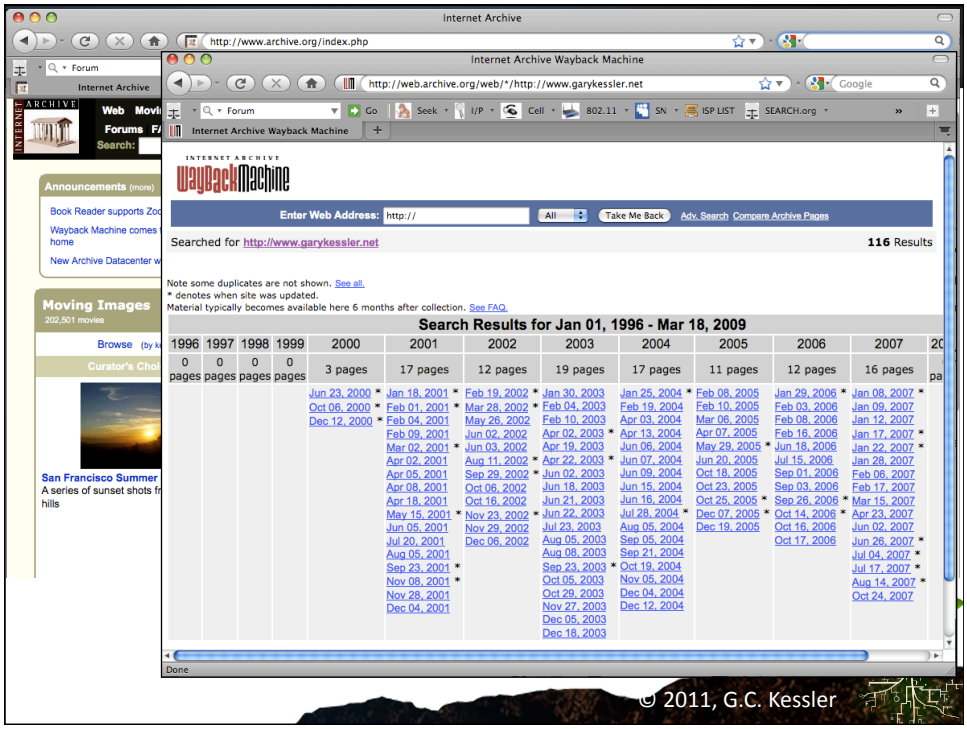
- *Not* a synonym for Internet!!
  - But accounts for ~65% of all Internet traffic
- HTTP is used for client-server communication
  - Common servers: Apache, IIS
- Web pages are written in HTML
  - Java, JavaScript, ActiveX, CGI, Perl, ASPs, ...
- Over 8B Web pages cataloged by Google (2005)
  - 100-200% annual growth


GaryKessler.net Home Page
http://www.garykessler.net/
GaryKessler.net Home Page
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.
Done
1
© 2011, G.C. Kessler


Spade - Browsing http://www.garykessler.net/, finished
File Edit View Window Basics Tools Help
www.garykessler.net
Magic
68.87.71.226
Browsing http://www.garykessler.net/, finished
02/12/11 17:14:36 Browsing http://www.garykessler.net/
Fetching http://www.garykessler.net/ ...
GET / HTTP/1.1
Host: www.garykessler.net
Connection: close
User-Agent: Sam Spade 1.14
HTTP/1.0 200 OK
Date: Sat, 12 Feb 2011 13:14:24 GMT
Server: Apache/2.2.11 (Unix) mod_ssl/2.2.11 OpenSSL/0.9.8e-fips-rhel5 DAV/2 mod_au
Last-Modified: Wed, 02 Feb 2011 19:10:14 GMT
ETag: "2065f7b-1926-49b51661bd564"
Accept-Ranges: bytes
Content-Length: 6438
Content-Type: text/html
X-Cache: MISS from proxy.surfnet.iacbox
X-Cache-Lookup: MISS from proxy.surfnet.iacbox:8080
Via: 1.1 proxy.surfnet.iacbox:8080 (squid/2.7.STABLE9)
Connection: close
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<title>GaryKessler.net Home Page</title>
<link href="css info/gka.css" rel="stylesheet" type="text/css">
http://www.garykes
For Help, press F1
© 2011, G.C. Kessler







But Aren't These All "Hacker Tools"?

CEIC 2011

ANALYSIS: Site Enumeration

ANALYSIS: Investigating Phishing

E-mail

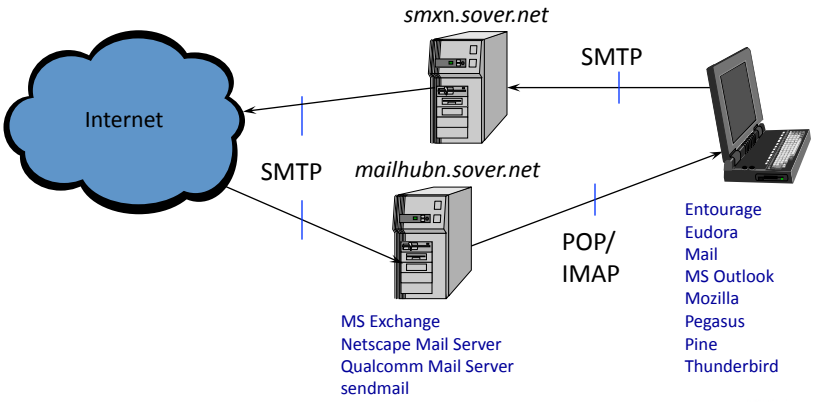
CEIC 2011

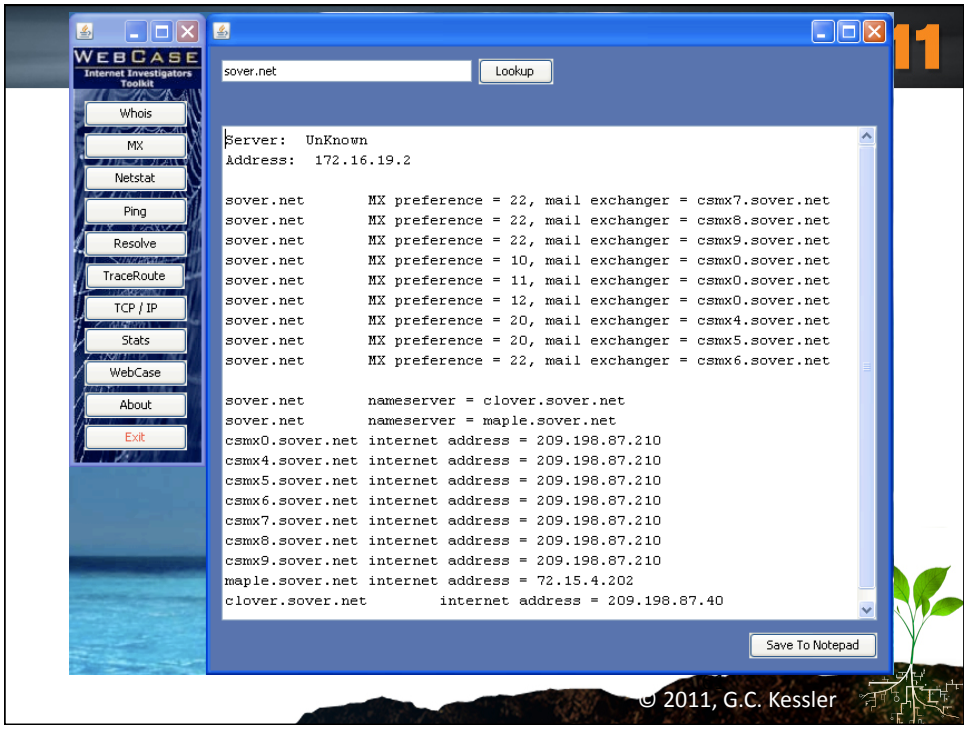
- Most widely used Internet application
- E-mail protocols
  - SMTP: Used between mail servers to forward mail, and from client to mail server to send mail
  - POP3 and IMAP: Used by client to download e-mail and manage mailbox
- DNS MX records identify the mail server(s) for a given domain
  - Lowest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

E-Mail Operation and Protocols

CEIC 2011

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





An SMTP Session

CEIC 2011

```
Moriarty:~ gck$ telnet mail.sover.net 25
220 mail.sover.net ready...
HELO moriarty.garykessler.net
250 mailgate8.sover.net Hello [41.136.88.226], pleased to meet you...
MAIL FROM:<gck@garykessler.net>
250 2.1.0 <gck@garykessler.net>... Sender OK
RCPT TO:<kumquat@sover.net>
250 2.1.5 <kumquat@sover.net>... Recipient OK
DATA
354 Enter mail, end with "." on a line by itself
HI!
.
250 2.0.0 p1B6Ndwk089903 Message accepted for delivery
quit
221 2.0.0 mailgate8.sover.net closing connection
Moriarty:~ gck$
```

E-mail and Headers

CEIC 2011

```
Return-Path: <gck@garykessler.net>
Received: from smx84.sover.net (smx84.sover.net [207.136.194.24])
     by spot.sover.net (8.14.2/8.14.2) with ESMTP id p1B6OutI042831
     for <kumquat@mailhub2.sover.net>; Fri, 11 Feb 2011 01:24:56 -0500 (EST)
     (envelope-from gck@garykessler.net)
Received: from mailgate8.sover.net (mailgate8.sover.net [207.136.194.50])
     by smx84.sover.net (8.14.3/8.14.3) with ESMTP id p1B6OujH009562
     for <kumquat@mailhub2.sover.net>; Fri, 11 Feb 2011 01:24:56 -0500 (EST)
     (envelope-from gck@garykessler.net)
Received: from moriarty.garykessler.net ([41.136.88.226])
     by mailgate8.sover.net (8.14.3/8.14.3) with SMTP id p1B6Ndwk089903
     for <kumquat@sover.net>; Fri, 11 Feb 2011 01:24:44 -0500 (EST)
     (envelope-from gck@garykessler.net)
Date: Fri, 11 Feb 2011 01:23:39 -0500 (EST)
From: gck@garykessler.net
Message-Id: <201102110624.p1B6Ndwk089903@mailgate8.sover.net>


HI!
```

A POP3 Session

CEIC 2011

```
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

CEIC 2011

```
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//8AALgAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAA6AAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1v
ZGUuDQ0KJAAAAAAAAACu45jY6oL2i+qC9ovqgvaLaZ74i/CC9osCnfyLm4L2i7yd5YvngvaL6oL2
i+mC9ovqgveLZ4L2i4id5YvngvaLAp39i/OC9otSaWNo6oL2iwAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAFBFAABMAQMA+w7FPgAAAAAAAAA4AAPAQsBBgAAwAAAABAAAAAAAQCAygEAABABAADQAQAA
AEAAABAAAAACAAAEAAAAAAAAAAQAAAAAAAAAOABAAAQAAAAAAAAgAAAAAEAAAEAAAAAQAAAQ
AAAAAAAAEAAAAAAAAAAAAAAAAANABANABAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

remainder of e-mail deleted
```


Understanding BASE64

CEIC 2011

- 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

CEIC 2011

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

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

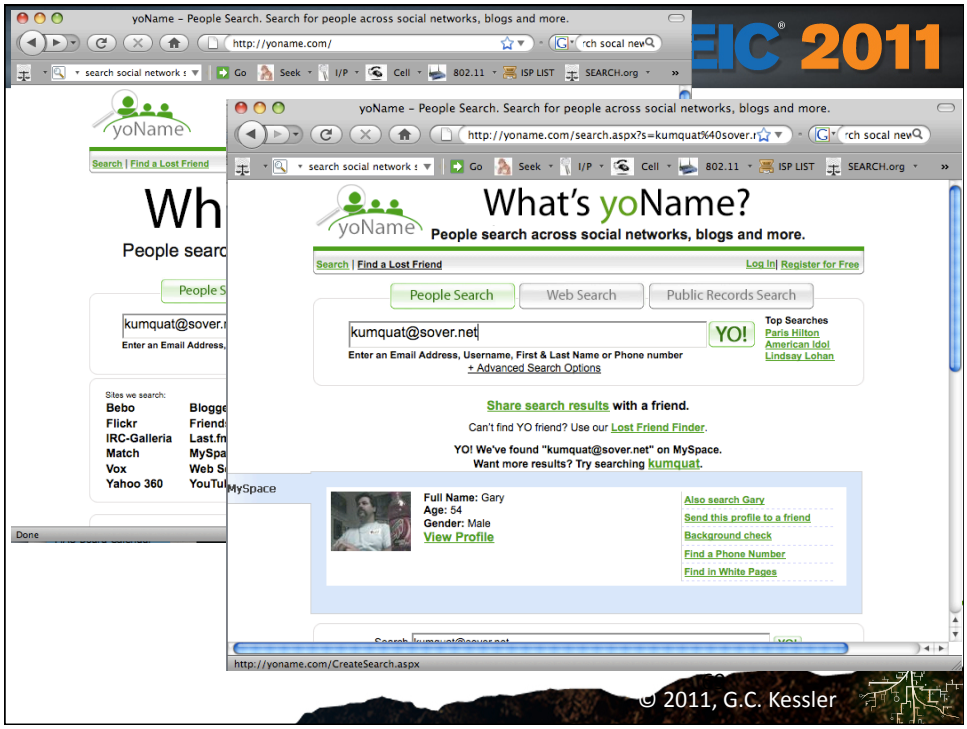
File signature for Windows executable file

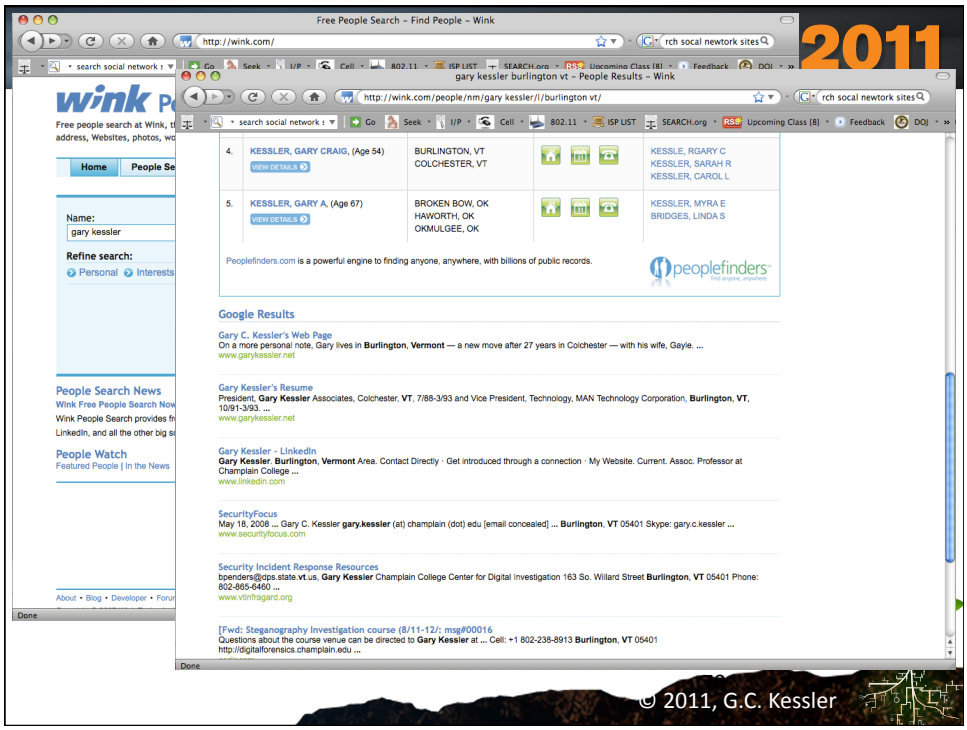
How can a bunch of ASCII characters hurt us? Remember that BASE64 encoding was specifically designed to transport a bit stream without appearing like a bit stream. The TVqQ string appears to be a set of four ASCII characters but it is actually a representation of 6-bit blocks which must be translated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

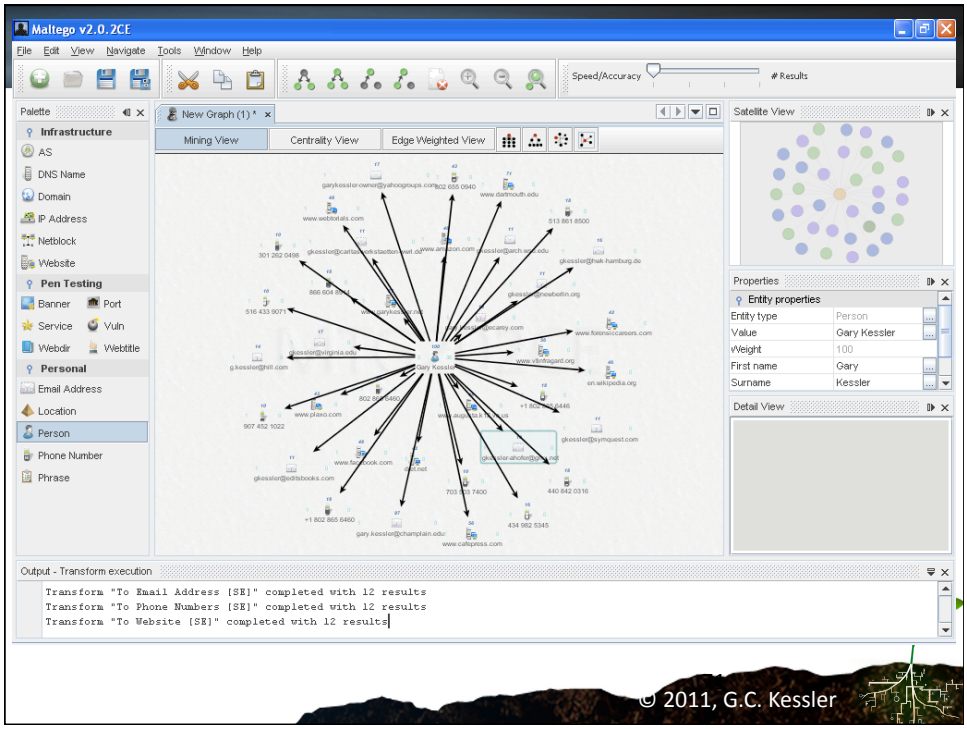
Social Networks (Web 2.0)

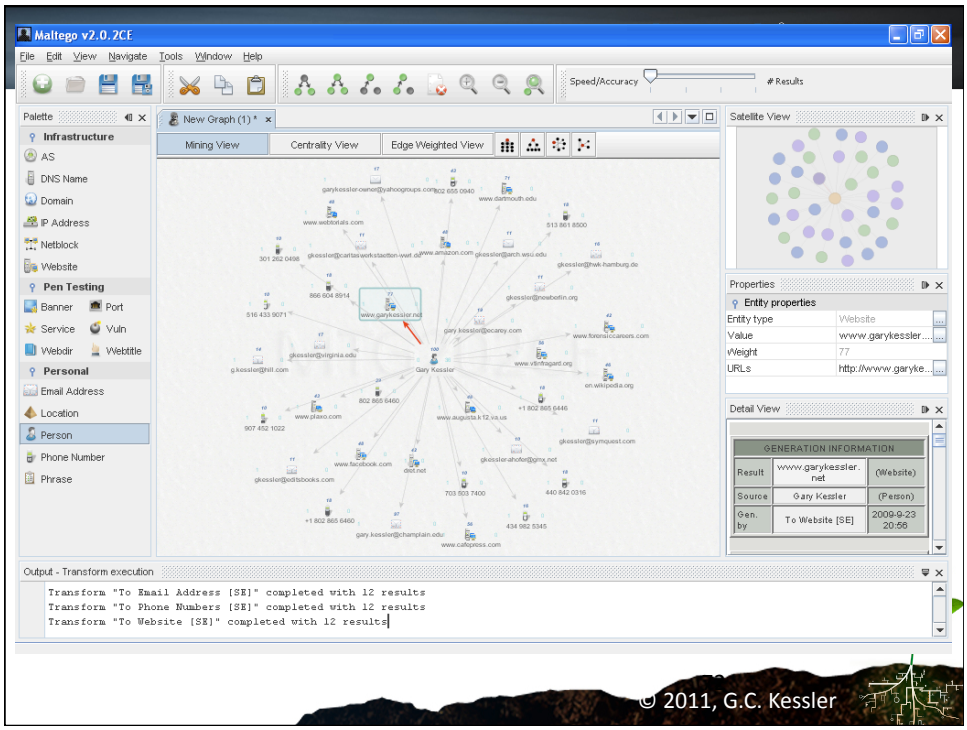
CEIC 2011

- Social networks
  - 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


yoName – People Search. Search for people across social networks, blogs and more.
http://yoname.com/
EIC 2011
yoName – People Search. Search for people across social networks, blogs and more.
http://yoname.com/search.aspx?s=kumquat%40sover.r
What's yoName?
People search across social networks, blogs and more.
Search | Find a Lost Friend
Log In| Register for Free
People Search
Web Search
Public Records Search
kumquat@sover.net
YO!
Enter an Email Address, Username, First & Last Name or Phone number
+ Advanced Search Options
Top Searches
Paris Hilton
American Idol
Lindsay Lohan
Share search results with a friend.
Can't find YO friend? Use our Lost Friend Finder.
YO! We've found "kumquat@sover.net" on MySpace.
Want more results? Try searching kumquat.
MySpace
Full Name: Gary
Age: 54
Gender: Male
View Profile
Also search Gary
Send this profile to a friend
Background check
Find a Phone Number
Find in White Pages
http://yoname.com/CreateSearch.aspx
© 2011, G.C. Kessler


Free People Search – Find People – Wink
http://wink.com/
2011
gary kessler burlington vt – People Results – Wink
http://wink.com/people/nm/gary kessler/l/burlington vt/
Name:
gary kessler
Refine search:
Personal
Interests
4. KESSLER, GARY CRAIG, (Age 54) VIEW DETAILS
BURLINGTON, VT
COLCHESTER, VT
KESSLE, RGARY C
KESSLER, SARAH R
KESSLER, CAROL L
5. KESSLER, GARY A, (Age 67) VIEW DETAILS
BROKEN BOW, OK
HAWORTH, OK
OKMULGEE, OK
KESSLER, MYRA E
BRIDGES, LINDA S
Peoplefinders.com is a powerful engine to finding anyone, anywhere, with billions of public records.
peoplefinders
Google Results
Gary C. Kessler's Web Page
On a more personal note, Gary lives in Burlington, Vermont — a new move after 27 years in Colchester — with his wife, Gayle. ...
www.garykessler.net
Gary Kessler's Resume
President, Gary Kessler Associates, Colchester, VT, 7/88-3/93 and Vice President, Technology, MAN Technology Corporation, Burlington, VT, 10/91-3/93. ...
www.garykessler.net
Gary Kessler - LinkedIn
Gary Kessler. Burlington, Vermont Area. Contact Directly · Get introduced through a connection · My Website. Current. Assoc. Professor at Champlain College ...
www.linkedin.com
SecurityFocus
May 16, 2008 ... Gary C. Kessler gary.kessler (at) champlain (dot) edu [email concealed] ... Burlington, VT 05401 Skype: gary.c.kessler ...
www.securityfocus.com
Security Incident Response Resources
bpenders@dps.state.vt.us, Gary Kessler Champlain College Center for Digital Investigation 163 So. Willard Street Burlington, VT 05401 Phone: 802-865-6460 ...
www.vtinfragard.org
[Fwd: Steganography Investigation course (8/11-12/: msg#00016
Questions about the course venue can be directed to Gary Kessler at ... Cell: +1 802-238-8913 Burlington, VT 05401
http://digitalforensics.champlain.edu ...
© 2011, G.C. Kessler


Maltego v2.0.2CE
File Edit View Navigate Tools Window Help
Speed/Accuracy
Results
Palette
Infrastructure
AS
DNS Name
Domain
IP Address
Netblock
Website
Pen Testing
Banner
Port
Service
Vuln
Webdir
Webtitle
Personal
Email Address
Location
Person
Phone Number
Phrase
New Graph (1) *
Mining View
Centrality View
Edge Weighted View
Satellite View
Properties
Entity properties
Entity type Person
Value Gary Kessler
Weight 100
First name Gary
Surname Kessler
Detail View
Output - Transform execution
Transform "To Email Address [SE]" completed with 12 results
Transform "To Phone Numbers [SE]" completed with 12 results
Transform "To Website [SE]" completed with 12 results
© 2011, G.C. Kessler


Maltego v2.0.2CE
File Edit View Navigate Tools Window Help
Speed/Accuracy
Results
Palette
Infrastructure
AS
DNS Name
Domain
IP Address
Netblock
Website
Pen Testing
Banner
Port
Service
Vuln
Webdir
Webtitle
Personal
Email Address
Location
Person
Phone Number
Phrase
New Graph (1) *
Mining View
Centrality View
Edge Weighted View
Satellite View
Properties
Entity properties
Entity type Website
Value www.garykessler...
Weight 77
URLs http://www.garyke...
Detail View
GENERATION INFORMATION
Result www.garykessler.net (Website)
Source Gary Kessler (Person)
Gen. by To Website [SE] 2009-9-23 20:56
Output - Transform execution
Transform "To Email Address [SE]" completed with 12 results
Transform "To Phone Numbers [SE]" completed with 12 results
Transform "To Website [SE]" completed with 12 results
© 2011, G.C. Kessler

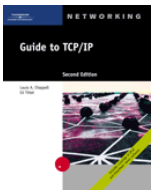
Summary

CEIC 2011

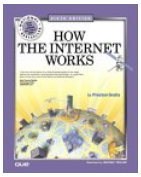
- Internet structure
- TCP/IP protocol suite
  - IP addressing
  - TCP/UDP ports
- Higher layer applications and tools
  - DNS
  - World Wide Web
  - E-mail and BASE64
  - Social networks and finding people

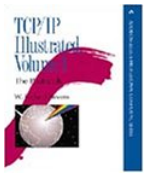
For More Information...

CEIC 2011



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





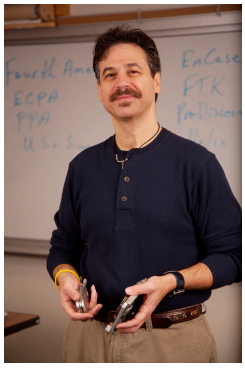
- "An Overview of TCP/IP Protocols and the Internet" (*www.garykessler.net/library/tcpip.html)*
- "TCP/IP and tcpdump Pocket Reference Guide" (*www.garykessler.net/download/tcpip/tcpip_prg.pdf*)

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@garykessler.net
gkessler@bpdvt.org
gkessle1@norwich.edu
Skype: gary.c.kessler

http://www.garykessler.net
http://www.vtinternetcrimes.org
http://infoassurance.norwich.edu



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?

CEIC 2011