Digital Investigator

Recap on IP, whois and nslookup

Wayback Engine

Introduction to Archiving Sites
Digital Investigator

Recap on IP, whois and nslookup

Recap on Networking
Bob

Network Address

Physical Address

IP Address: 192.168.0.2

Physical Address: C8-F7-33-4B-82-37

Alice

Network Address

Physical Address

Router

Switch

Author: Prof Bill Buchanan
Basic Connections
Net. Fun.
Author: Prof Bill Buchanan

Static Address Allocation
Router
Switch
Bob
Network
Address
Physical
Address
Physical Address: C8-F7-33-4B-82-37
DNS 
Server
IP Address: 192.168.0.10

IP Address: 192.168.0.10
Physical Address: C8-F7-33-4B-82-37

Author: Prof Bill Buchanan
Basic Connections
Net. Fun.
Author: Prof Bill Buchanan

Static/Dynamic Address Allocation

Router
Switch
Bob
Network Address
Physical Address

IP Address: 192.168.0.10
Physical Address: C8-F7-33-4B-82-37

# ifconfig eth0 192.168.0.10 netmask 255.255.255.0
# ifconfig eth0 down
# ifconfig eth0 up

# route add default gw 192.168.0.1

# nameserver 192.168.1.100
# cat /etc/resolve.conf
$ route
Kernel IP routing table

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>Genmask</th>
<th>Flags</th>
<th>Metric</th>
<th>Ref</th>
<th>Use</th>
<th>Iface</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.1</td>
<td>*</td>
<td>255.255.255.0</td>
<td>U</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>eth0</td>
</tr>
</tbody>
</table>

DHCP
Server

# dhclient eth0 -r
# dhclient eth0

LINUX
LINUX

Author: Prof Bill Buchanan
C:\>ipconfig

Windows IP Configuration

Wireless LAN adapter Wireless Network Connection:

Connection-specific DNS Suffix . : Home
Link-local IPv6 Address . . . . : fe80::445:2b39:27ab:99d6%12
IPv4 Address . . . . . . . . . . . : 192.168.0.2
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 192.168.0.1

$ ifconfig

eth0 Link encap:Ethernet  HWaddr C8-F7-33-4B-82-37
    inet addr:192.168.0.2  Bcast:192.168.0.2  Mask:255.255.255.0
    inet6 addr: fe80::445:2b39:27ab:99d6%12 Scope:Link
    UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
    RX packets:913240 errors:230 dropped:0 overruns:0 frame:230
    TX packets:663990 errors:7 dropped:0 overruns:0 carrier:12
    collisions:0 txqueuelen:1000
    RX bytes:179148797 (170.8 MiB) TX bytes:53220450 (50.7 MiB)
    Interrupt:9 Base address:0xb000
Dynamic Address Allocation

Bob

DNS Server

Network Address

IP Address, Subnet Mask, Default Gateway and DNS Server allocated from DHCP Server

IP Address: 192.168.0.10
Physical Address: C8-F7-33-4B-82-37

DHCP Server

Author: Prof Bill Buchanan
Author: Prof Bill Buchanan

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

Host Name . . . . . . . . . . . . . : bill-PC
Primary Dns Suffix . . . . . . . . . . . . . : 
Node Type . . . . . . . . . . . . . . . . . . . . . . : Peer-Peer
IP Routing Enabled . . . . . . . . . . : No
WINS Proxy Enabled . . . . . . . . . : No
DNS Suffix Search List . . . . . . . : Home

Wireless LAN adapter Wireless Network Connection:

Connection-specific DNS Suffix . . . : Home
Description . . . . . . . . . . . . . . . . : Intel(R) Centrino(R)
Advanced-N 6235
Physical Address . . . . . . . . . : C8-F7-33-4B-82-37
DHCP Enabled . . . . . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . . . : Yes
Link-local IPv6 Address . . . . . . . . : fe80::445:2b39:27ab:99d6%12(Preferred)
   IPv4 Address . . . . . . . . . . . . . : 192.168.0.2(Preferred)
   Subnet Mask . . . . . . . . . . . . . : 255.255.255.0
   Lease Obtained . . . . . . . . . . . . : 14 August 2013 09:53:53
   Lease Expires . . . . . . . . . . . . . : 15 August 2013 19:02:42
   Default Gateway . . . . . . . . . . . : 192.168.0.1
   DHCP Server . . . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . . . : 298383155
   DHCPv6 Client DUID . . . . . . . . : 00-01-00-01-19-87-34-5D-C8-F7-33-4B-82-37
   DNS Servers . . . . . . . . . . . . . : 192.168.0.1
   NetBIOS over Tcpip . . . . . . . . : Enabled
```

IP Address: 192.168.0.2
Physical Address: C8-F7-33-4B-82-37
Basic Connections

Net. Fun.

Author: Prof Bill Buchanan

nslookup

Root

ORG GOV COM

MICROSOFT IBM

$TTL 86400 ; 24 hours could have been written as 24h or 1d
$ORIGIN noname.com.

@ IN SOA ns1.noname.com. Host.noname.com (2002011887 ; serial
21600 ; refresh every 6 hours
3600 ; retry after 1 hour
604800 ; expire after 1 week
86400 ) ; minimum TTL of 1 day

IN NS ns1.noname.com. ; Name Server
IN MX 10 mail.noname.com. ; mail server
IN A 10.0.0.1 noname.com. IN A 10.0.0.1
fred IN A 10.0.0.2 ; maps a domain name to an IP address
www IN CNAME noname.com. ; define a common name of a host
ftp IN CNAME noname.com.
smt p IN CNAME noname.com.

Www.noname.com
Smtp.noname.com
Fred.noname.com (10.0.0.2)

Author: Prof Bill Buchanan
**Basic Connections**

**Net. Fun.**

**Author:** Prof. Bill Buchanan

---

**C:**> `nslookup`  
`> set type=soa`  
`> microsoft.com`

**Non-authoritative answer:**

- `microsoft.com`  
  - primary name server = `ns1.msft.net`
  - responsible mail addr = `msnhst.microsoft.com`
  - `serial` = 2011042301
  - `refresh` = 300 (5 mins)
  - `retry` = 600 (10 mins)
  - `expire` = 2419200 (28 days)
  - default TTL = 3600 (1 hour)

`> set type=mx`  
`> microsoft.com`

**Non-authoritative answer:**

- `microsoft.com`  
  - MX preference = 10, mail exchanger = `mail.messaging.microsoft.com`
- `microsoft.com`  
  - MX preference = 20, mail exchanger = `mail.messaging.microsoft.com`

**Physical Address:**

- `microsoft.com`  
  - nameserver = `ns5.msft.net`
- `microsoft.com`  
  - nameserver = `ns1.msft.net`
- `ns1.msft.net`  
  - internet address = 65.55.37.62
Basic Connections
Net. Fun.

Author: Prof Bill Buchanan

Whois

Registrar Query
Searches for registry information:
- ICANN.
- Regional Internet Registries:
  - ARIN. North/South America.
  - APNIC. Asia and Pacific.
  - LACNIC. Latin America and Caribbean.
  - AfriNIC. Africa.

Domain Name: cisco.com
Creation Date: 1987-05-14
Registration Date: 2011-04-06
Expiry Date: 2012-05-16
Organisation Name: Cisco Technology, Inc.
Organisation Address: 170 W. Tasman Drive
Organisation Address: San Jose
Organisation Address: 95134
Organisation Address: CA
Organisation Address: UNITED STATES
Admin Name: InfoSec
Admin Address: 170 West Tasman Drive
Admin Address: San Jose
Admin Address: 95134
Admin Address: CA
Admin Address: UNITED STATES
Admin Email: MBITtransferadmin@melbourneitdbs.com
Admin Phone: +1.4085273842

IP Address: 192.168.0.2
Physical Address: C8-F7-33-4B-82-37

www.microsoft.com
Archiving
Net. Fun.
Author: Prof Bill Buchanan
Introduction to Archiving

Laptop (146.176.164.40/24)
Virtual Machine (172.16.121.129/24)
Amazon Instance (54.81.219.235)
Gateway (146.176.164.254/24)
NAT (146.176.164.41/24)
Web log
Web Target of Interest
192.168.0.1
192.168.0.2
192.168.0.3/24

Author: Prof Bill Buchanan
Archiving Net. Fun.

Author: Prof Bill Buchanan

Introduction to Archiving

Laptop (146.176.164.40/24)

Virtual Machine (172.16.121.129/24)

Amazon Instance (54.81.219.235)

Gateway (146.176.164.254/24)

Amazon Instance (10.72.47.6)

Web Target of Interest

Snapshots of Web site

Web log

Author: Prof Bill Buchanan
Archiving

Web Target of
Interest

Web log

Robot.txt
User-Agent: *
Disallow: /buyer.dat
Disallow: /buyer.txt
Disallow: /log.dat
Disallow: /log.txt
Disallow: /error.txt
Disallow: /hand/
Disallow: /log/
Allow: /

Recording method

Crawl download
Using Website Copier (WinHTTrack)

Dynamic Analysis (Fiddler/Chrome)
  - Automated/Manual

Archive

Google Search/Google Hack

Off-line analysis

Introduction to Archiving

Author: Prof Bill Buchanan
Lab 2.1: Introduction to Archiving

Recap on IP, whois and nslookup

Wayback Engine
Examining HTTP Request/Response

Digital Investigator

Fiddler Session
Frame 3 (74 bytes on wire, 74 bytes captured)
Internet Protocol, Src: 192.168.75.1 (192.168.75.1), Dst: 192.168.75.132 (192.168.75.132)
Transmission Control Protocol, Src Port: abatemgr (3655), Dst Port: ftp (21), Seq: 0, Len: 0

Frame 4 (78 bytes on wire, 78 bytes captured)
Internet Protocol, Src: 192.168.75.132 (192.168.75.132), Dst: 192.168.75.1 (192.168.75.1)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: abatemgr (3655), Seq: 0, Ack: 1, Len: 0

Frame 5 (66 bytes on wire, 66 bytes captured)
Internet Protocol, Src: 192.168.75.1 (192.168.75.1), Dst: 192.168.75.132 (192.168.75.132)
Transmission Control Protocol, Src Port: abatemgr (3655), Dst Port: ftp (21), Seq: 1, Ack: 1, Len: 0

3-way handshake
GET / HTTP/1.1
User-Agent: Opera/9.80 (Windows NT 6.0; U; en) Presto/2.2.15 Version/10.01
Host: 192.168.75.132
Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*;q=0.1 Accept-Language: en-GB, en;q=0.9
Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1
Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0
Connection: Keep-Alive

HTTP/1.1 200 OK
Content-Length: 2606
Content-Type: text/html
Content-Location: http://192.168.75.132/iisstart.htm
Last-Modified: Sun, 13 Dec 2009 15:16:14 GMT
Accept-Ranges: bytes ETag: "fc31243677ccal:745" Server: Microsoft-IIS/6.0 X-Powered-By: ASP.NET
Date: Sat, 02 Jan 2010 22:33:01 GMT

<HTML> <HEAD> <TITLE>SFC (Final Test)</TITLE> </HEAD> <META http-equiv=Content-Type content="text/html; charset=iso-8859-1"> <LINK href="2.css" type=text/css rel=stylesheet> <style type="text/css"> ...
Digital Investigator

Archiving and Analysing Sites

Web site analysis

Off-line analysis
Web structure

**Wide and shallow**

- Index.html
- Page1.html
- Page2.html
- Page3.html

**Narrow and deep**

- Index.html
- Page1.html
- Page2.html
- Page3.html

**Linkfarm**

- Index.html
  - → External links
  - ← Internal links

**Popular site?**

- Index.html
  - ← Internal links
  - → External links

**Site A**

- External links

**Site B**

- Internal Reputation Builder

**Site C**

**Author:** Prof Bill Buchanan
Archiving
Net. Fun.

Author: Prof Bill Buchanan

A Risky Page

Broken Image

Unfocused advert

Advertising different products

FSA

Staticly defined APRs

Link farms

Great value life insurance

£100,000 cover from just
Archiving
Net. Fun.
Author: Prof Bill Buchanan
A Risky Page
Bad English
Broken Links
Missing content
Text heavy
URL tricker (gogle.com)
Skim site
Repeated content
Unfocused material
Scam
Digital Inv.
Author: Prof Bill Buchanan

You are accused of viewing/storage and/or dissemination of banned pornography (child pornography/zooophilia/rape etc.) You have violated World Declaration on non-proliferation of child pornography. You are accused of committing the crime envisaged by Article 161 of the Kingdom of Great Britain criminal law.

Article 161 of the Kingdom of Great Britain criminal law provides for the punishment of deprivation of liberty for terms from 5 to 11 years.

Also, you are suspected of violation of "Copyright and Related rights Law" (downloading of pirated music, video, warez) and of use and/or dissemination of copyrighted content. Thus, you are suspected of violation of Article 148 of the Kingdom of Great Britain criminal law.

Article 148 of the Kingdom of Great Britain criminal law provides for the punishment of deprivation of liberty for terms from 3 to 7 years or 150 to 550 basic amounts fine.

It was from your computer that unauthorized access had been stolen to information of State

Author: Prof Bill Buchanan
409. Integrating ASPX with HTML

Here's one of my routing challenges, which integrate ASPX files with an HTML page. For this I've used an IFRAME such as with:

<iframe src="http://networksims.com/security52.aspx" scrolling="no" frameborder="0" style="width:800px; height:350px"></iframe>

Content taken from another site

<i>Author: Prof Bill Buchanan</i>
Lab 2.3: Archiving and Analysing Web Site

Digital Investigator

Web site analysis

Off-line analysis
Google hacking. Advanced search methods such as:
- Filetype: xls
- Inurl: search-text
- Link: www.test.com
- Intitle: "Company records"

EDGAR Database. Contains information on publicly trading companies.

Alternative Sites. This can relate to information leaked from disgruntled employees, or for searching for information on employees.