How the Internet works

Jessica McKellar
You type **http://python.org** into your browser bar and press Enter. What happens?
Python Programming Language – Official

Python is a programming language that lets you work more quickly and integrate your systems more effectively. You can learn to use Python and see almost immediate gains in productivity and lower maintenance costs.

Python runs on Windows, Linux/Unix, Mac OS X, and has been ported to the Java and .NET virtual machines.

Python is free to use, even for commercial products, because of its OSI-approved open source license.
Questions

What  is python.org?

Where  is python.org?

How  does my computer talk to python.org?

What  does my computer say to python.org?
Protocol

A format and rules for exchanging information
Internet protocols are \textit{layered}, one protocol per task.
What is python.org?

Domain Name Service (DNS) translates hostnames to IP addresses

python.org → 82.94.164.162
Where is python.org?

Internet Protocol (IP) handles addressing and routing
Your packets of data hop from router to router through the Internet to their destination
scapy demo!
>>> res, _ = traceroute("python.org")
Begin emission:************
  82.94.164.162:tcp80
1  192.168.1.1  openwrt.lan
2  96.120.66.81  96.120.168.1.1
3  68.85.160.37  cambridge.ma.boston.comcast.net
4  68.85.106.29  needham.ma.boston.comcast.net
5  68.86.90.57   newyork.ny.ibone.comcast.net
6  68.86.85.22   111eighthave.ny.ibone.comcast.net
7  75.149.228.126 nyk-s2-rou-1001.us.eurorings.net
8  134.222.226.154 ldn-s2-rou-1101.uk.eurorings.net
9  134.222.231.148 ldn-s1-rou-1021.uk.eurorings.net
10 134.222.231.156 asd2-rou-1022.nl.eurorings.net
11 134.222.229.113 asd2-rou-1044.nl.eurorings.net
12 134.222.97.18  134.222.97.18
13 194.109.5.82   xr4.1d12.xs4all.net
14 194.109.12.34  swcolo2.3d12.xs4all.net
15 82.94.164.162  dinsdale.python.org

>>> res.graph(target="> traceroute.svg")
traceroute_ips = 
96.120.66.81
68.85.160.37
68.85.106.29
68.86.90.57
68.86.85.22
75.149.228.126
134.222.226.154
134.222.231.148
134.222.231.156
134.222.229.113
134.222.97.18
194.109.5.82
194.109.12.34
82.94.164.162

"".strip().split("
")
import pygeoip

gi = pygeoip.GeoIP("GeoLiteCity.dat")

for ip in traceroute_ips:
    record = gi.record_by_addr(ip)
    print ip.ljust(15),
    print record["country_name"],
    if record["time_zone"]:  
        print record["time_zone"],
    print ""
$ python geolocate.py

96.120.66.81    United States    Boston
68.85.160.37     United States    Boston
68.85.106.29     United States    Boston
68.86.90.57      United States    New_York
68.86.85.22      United States    New_York
75.149.228.126   United States    New_York
134.222.226.154  United Kingdom   London
134.222.231.148  United Kingdom   London
134.222.231.156  Netherlands      Amsterdam
134.222.229.113  Netherlands      Amsterdam
134.222.97.18    Netherlands      Amsterdam
194.109.5.82     Netherlands      Amsterdam
194.109.12.34    Netherlands      Amsterdam
82.94.164.162    Netherlands      Amsterdam
Where is python.org?

Internet Protocol (IP)
IP handles addressing and routing
How does my computer talk to python.org?

Transmission Control Protocol (TCP)

TCP reliably delivers data
Application-layer protocols that use TCP

web: HTTP
chat: IRC, XMPP/Jabber
e-mail: SMTP, POP3, IMAP

Each application uses a different “port” number, so many different applications can use TCP to talk to an IP address at the same time.
How does my computer talk to python.org?

Transmission Control Protocol (TCP)

TCP reliably delivers data
What does my computer say to python.org?

HyperText Transfer Protocol (HTTP)

Clients use HTTP to request resources from servers
Resources

http://python.org

- HTML
- images
- textual or binary data
- dynamically-generated query results
How to be a web browser
telnet demo!
$ telnet python.org 80
Trying 82.94.164.162...
Connected to python.org.
Escape character is '^]'.
GET / HTTP/1.1
Host: python.org
<head>
  <title>
    Python Programming Language &ndash; Official Website
  </title>
</head>
Python Programming Language – Official Website
<head>
  <title>
    Python Programming Language &ndash; Official Website
  </title>
</head>
<head>
    <title>
        Python Programming Language &ndash; Official Website
    </title>
</head>
HTTP/1.1 200 OK
Date: Mon, 04 Mar 2013 00:22:30 GMT
Server: Apache/2.2.16 (Debian)
Last-Modified: Fri, 01 Mar 2013 22:31:40 GMT
Content-Type: text/html

<head>
  <title>
    Python Programming Language
    &ndash; Official Website
  </title>
</head>
import urllib2
urllib2.urlopen( "http://python.org" ).read()
How to be a web server
class HTTPProtocol(basic.LineReceiver):
    def __init__(self):
        self.lines = []

    def lineReceived(self, line):
        self.lines.append(line)
        if not line:
            self.sendResponse()

    def sendResponse(self):
        self.sendLine("HTTP/1.1 200 OK")
        self.sendLine(""")
        for line in self.lines:
            self.sendLine(line)
        self.transport.loseConnection()

reactor.listenTCP(80, HTTPFactory())
reactor.run()
class HTTPProtocol(basic.LineReceiver):
    def __init__(self):
        self.lines = []

    def lineReceived(self, line):
        self.lines.append(line)
        if not line:
            self.sendResponse()

    def sendResponse(self):
        self.sendLine("HTTP/1.1 200 OK")
        self.sendLine(""")
        for line in self.lines:
            self.sendLine(line)
        self.transport.loseConnection()

reactor.listenTCP(80, HTTPFactory())
reactor.run()
What does my computer say to python.org?

HyperText Transfer Protocol (HTTP)

Clients use HTTP to request resources from servers
You type `http://python.org` into your browser bar and press Enter. What happens?
IP addressing and routing
requesting resources
reliable delivery
addressing and routing

hostnames → IP addresses
DNS

TCP
IP
HTTP
DNS
HTTP
TCP
IP
<wireshark demo>
### Surfing the web

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Destination IP</th>
<th>Protocol</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.1</td>
<td>192.168.1.127</td>
<td>DNS</td>
<td>Standard query response Ox119e CNAME <a href="http://www.meetup.com">www.meetup.com</a> A 38.123.132.30</td>
</tr>
<tr>
<td>192.168.1.1</td>
<td>192.168.1.127</td>
<td>DNS</td>
<td>Standard query response Ox16f8 A 38.123.132.30</td>
</tr>
<tr>
<td>192.168.1.127</td>
<td>38.123.132.30</td>
<td>TCP</td>
<td>60546 &gt; http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=16</td>
</tr>
<tr>
<td>192.168.1.127</td>
<td>38.123.132.30</td>
<td>TCP</td>
<td>60547 &gt; http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=16</td>
</tr>
<tr>
<td>38.123.132.30</td>
<td>192.168.1.127</td>
<td>TCP</td>
<td>http &gt; 60547 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460</td>
</tr>
<tr>
<td>192.168.1.127</td>
<td>38.123.132.30</td>
<td>TCP</td>
<td>60547 &gt; http [ACK] Seq=1 Ack=1 Win=65535 Len=0</td>
</tr>
<tr>
<td>192.168.1.127</td>
<td>38.123.132.30</td>
<td>HTTP</td>
<td>GET /bostonpython/ HTTP/1.1</td>
</tr>
<tr>
<td>38.123.132.30</td>
<td>192.168.1.127</td>
<td>TCP</td>
<td>http &gt; 60546 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460</td>
</tr>
<tr>
<td>192.168.1.127</td>
<td>38.123.132.30</td>
<td>TCP</td>
<td>60546 &gt; http [ACK] Seq=1 Ack=1 Win=65535 Len=0</td>
</tr>
<tr>
<td>38.123.132.30</td>
<td>192.168.1.127</td>
<td>TCP</td>
<td>http &gt; 60547 [ACK] Seq=1 Ack=1127 Win=7882 Len=0</td>
</tr>
<tr>
<td>192.168.1.127</td>
<td>74.125.226.214</td>
<td>TCP</td>
<td>[TCP segment of a reassembled PDU]</td>
</tr>
<tr>
<td>192.168.1.127</td>
<td>74.125.226.214</td>
<td>TCP</td>
<td>[TCP segment of a reassembled PDU]</td>
</tr>
</tbody>
</table>
## Lonely printers

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Destination IP</th>
<th>Protocol</th>
<th>Protocol Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.127</td>
<td>192.168.1.255</td>
<td>BJNP</td>
<td>Printer Command: Discover</td>
</tr>
<tr>
<td>192.168.1.127</td>
<td>224.0.0.1</td>
<td>BJNP</td>
<td>Printer Command: Discover</td>
</tr>
</tbody>
</table>
Lonely TiVos

9753 260.151096 192.168.1.127 72.21.91.111 TCP 60642 > https [ACK] Seq: 0; Ack: 0
9754 260.759240 192.168.1.143 192.168.1.255 TiVoConnect Discovery Beacon fizzig
9755 261.377265 54.243.101.69 192.168.1.127 TCP http > 60646 [FIN, ACK]

Frame 9754: 195 bytes on wire (1560 bits), 195 bytes captured (1560 bits)
Ethernet II, Src: Tivo_38:b9:db (00:11:d9:38:b9:db), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
User Datagram Protocol, Src Port: tivoconnect (2190), Dst Port: tivoconnect (2190)
TiVoConnect Discovery Protocol, fizzig (7460001908A9F7D)
  Flavor: 1
  Version: 20.2.2.1-01-2-746
  Method: broadcast
  Identity: 7460001908A9F7D
  Machine: fizzig
  Platform: tcd/Series4
  Services: TiVoMediaServer:80/http
Errors

TCP protocol, retransmitting lost data
## Encrypted communication

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Destination IP</th>
<th>Protocol</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.127</td>
<td>199.59.148.10</td>
<td>TLSv1</td>
<td>Client Hello</td>
</tr>
<tr>
<td>199.59.148.10</td>
<td>192.168.1.127</td>
<td>TLSv1</td>
<td>Server Hello</td>
</tr>
<tr>
<td>199.59.148.10</td>
<td>192.168.1.127</td>
<td>TLSv1</td>
<td>Certificate, Server Hello Done</td>
</tr>
<tr>
<td>192.168.1.127</td>
<td>199.59.148.10</td>
<td>TLSv1</td>
<td>Client Key Exchange, Change Cipher Spec,</td>
</tr>
<tr>
<td>199.59.148.10</td>
<td>192.168.1.127</td>
<td>TLSv1</td>
<td>New Session Ticket, Change Cipher Spec,</td>
</tr>
<tr>
<td>192.168.1.127</td>
<td>199.59.148.10</td>
<td>TLSv1</td>
<td>Application Data</td>
</tr>
<tr>
<td>192.168.1.127</td>
<td>199.59.148.10</td>
<td>TLSv1</td>
<td>Application Data</td>
</tr>
<tr>
<td>199.59.148.10</td>
<td>192.168.1.127</td>
<td>TLSv1</td>
<td>Application Data</td>
</tr>
<tr>
<td>199.59.148.10</td>
<td>192.168.1.127</td>
<td>TLSv1</td>
<td>Application Data</td>
</tr>
<tr>
<td>199.59.148.10</td>
<td>192.168.1.127</td>
<td>TLSv1</td>
<td>Application Data</td>
</tr>
<tr>
<td>199.59.148.10</td>
<td>74.125.226.214</td>
<td>TLSv1.1</td>
<td>Application Data</td>
</tr>
<tr>
<td>192.168.1.127</td>
<td>74.125.226.214</td>
<td>TLSv1.1</td>
<td>Application Data</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP Address</td>
<td>Protocol</td>
<td>Request (CAP)</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------</td>
<td>----------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>192.168.1.127</td>
<td>82.96.64.4</td>
<td>IRC</td>
<td>Request (NICK) (USER)</td>
</tr>
<tr>
<td>192.168.1.127</td>
<td>82.96.64.4</td>
<td>IRC</td>
<td>Response (NOTICE)</td>
</tr>
<tr>
<td>192.168.1.127</td>
<td>82.96.64.4</td>
<td>IRC</td>
<td>Response (NOTICE) (NOTICE) (CAP)</td>
</tr>
<tr>
<td>192.168.1.127</td>
<td>82.96.64.4</td>
<td>IRC</td>
<td>Request (CAP)</td>
</tr>
<tr>
<td>192.168.1.127</td>
<td>82.96.64.4</td>
<td>IRC</td>
<td>Response (001)</td>
</tr>
<tr>
<td>192.168.1.127</td>
<td>82.96.64.4</td>
<td>IRC</td>
<td>Response (002) (003) (004) (005)</td>
</tr>
<tr>
<td>192.168.1.127</td>
<td>82.96.64.4</td>
<td>IRC</td>
<td>Response (2) (250) (375) (372) (372)</td>
</tr>
<tr>
<td>192.168.1.127</td>
<td>82.96.64.4</td>
<td>IRC</td>
<td>Response (372) (372) (372) (372)</td>
</tr>
<tr>
<td>192.168.1.127</td>
<td>82.96.64.4</td>
<td>IRC</td>
<td>Response (372) (372) (376) (MODE)</td>
</tr>
<tr>
<td>192.168.1.127</td>
<td>82.96.64.4</td>
<td>IRC</td>
<td>Response (NOTICE)</td>
</tr>
<tr>
<td>192.168.1.127</td>
<td>82.96.64.4</td>
<td>IRC</td>
<td>Request (NICKSERV)</td>
</tr>
<tr>
<td>192.168.1.127</td>
<td>82.96.64.4</td>
<td>IRC</td>
<td>Response (NOTICE)</td>
</tr>
<tr>
<td>192.168.1.127</td>
<td>82.96.64.4</td>
<td>IRC</td>
<td>Request (JOIN)</td>
</tr>
<tr>
<td>192.168.1.127</td>
<td>82.96.64.4</td>
<td>IRC</td>
<td>Response (JOIN)</td>
</tr>
<tr>
<td>192.168.1.127</td>
<td>82.96.64.4</td>
<td>IRC</td>
<td>Response (MODE) (353) (366)</td>
</tr>
<tr>
<td>192.168.1.127</td>
<td>82.96.64.4</td>
<td>IRC</td>
<td>Request (WHO)</td>
</tr>
<tr>
<td>192.168.1.127</td>
<td>82.96.64.4</td>
<td>IRC</td>
<td>Response (352)</td>
</tr>
<tr>
<td>192.168.1.127</td>
<td>82.96.64.4</td>
<td>IRC</td>
<td>Response (315)</td>
</tr>
</tbody>
</table>
IRC

 IRC server prompting for a password.
### IRC

Frame 70: 97 bytes on wire (776 bits), 97 bytes captured (776 bits)

- Internet Protocol Version 4, Src: 192.168.1.127 (192.168.1.127), Dst: 82.96.64.4
- Transmission Control Protocol, Src Port: 61339 (61339), Dst Port: 6667

**Internet Relay Chat**

- Request: NICKSERV IDENTIFY django4life

---

My password, django4life
<wireshark demo>
One last demo

How to propose marriage on your local network using Scapy and ARP-cache poisoning
Lonely printers

Address Resolution Protocol (ARP) maps hardware (MAC) addresses to IP addresses
When nerds get married

Universal logic gate rings
NAND = me
NOR = him
What next?

• Twisted
• Scapy
• wireshark
Twisted
Glasgow Haskell Compiler
PyPy
LLVM
Bash
Berkley DB

ZeroMQ
Git
nginx
Mercurial

CC BY 3.0
All proceeds to Amnesty International
Hot off the press!
Thank you!

@jessicamckellar
http://jesstess.com
A map of the entire Internet in 1977

ARPANET LOGICAL MAP, MARCH 1977

(O IMP △ PLURIBUS IMP
□ TIP ~ SATELLITE CIRCUIT)

(PLEASE NOTE THAT WHILE THIS MAP SHOWS THE HOST POPULATION OF THE NETWORK ACCORDING TO THE BEST INFORMATION OBTAINABLE, NO CLAIM CAN BE MADE FOR ITS ACCURACY)

NAMES SHOWN ARE IMP NAMES, NOT (NECESSARILY) HOST NAMES