Web Services and the LAMP Stack

GTFO Security

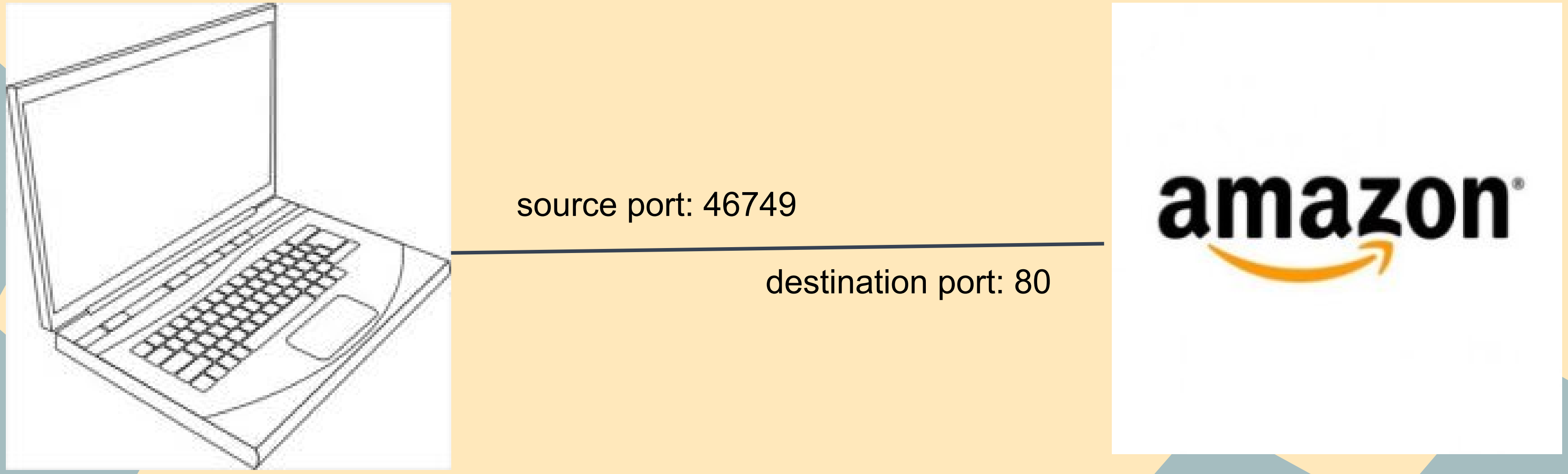
Agenda

- The stack
    - Web server
    - Database
    - Application
- LAMP
    - Components
    - Monitoring
        - Processes
        - Files
        - Network

How the Web Works

Connecting to Web Sites

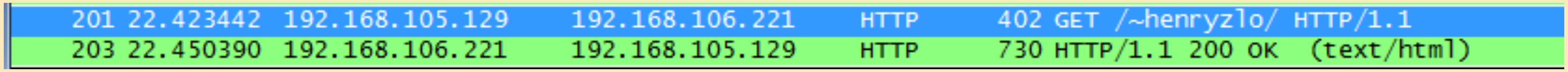
- Recall that when you navigate to a web site, you form a connection.
- The protocol for this connection is either HTTP or HTTPS (encrypted connections).



source port: 46749

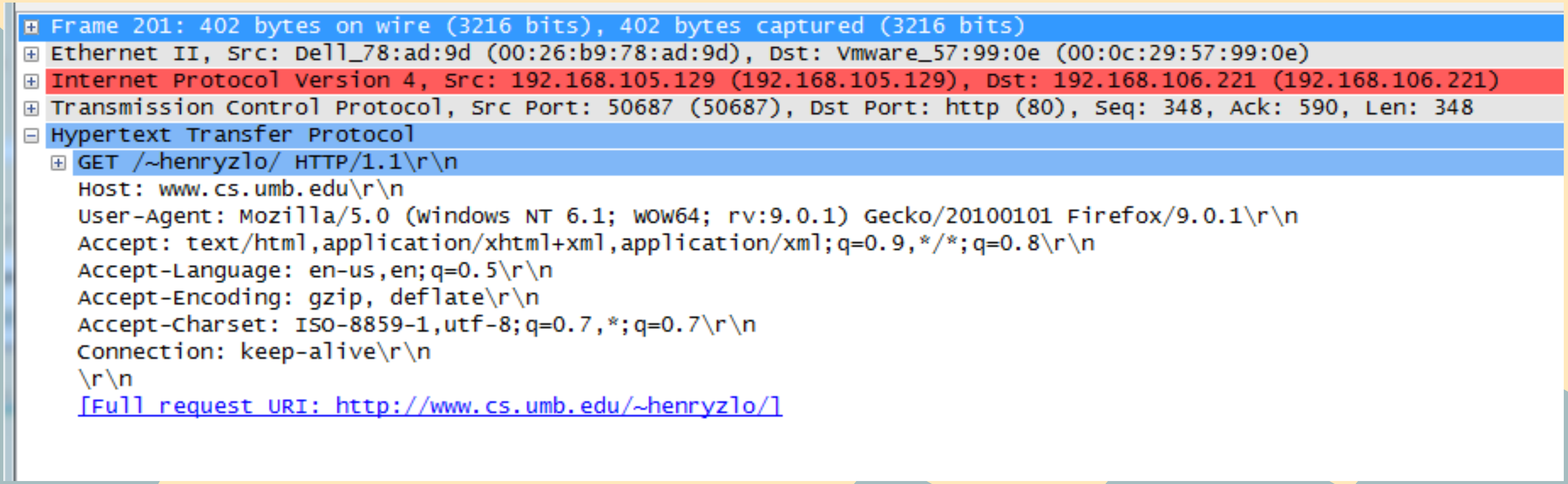
destination port: 80

HTTP Request



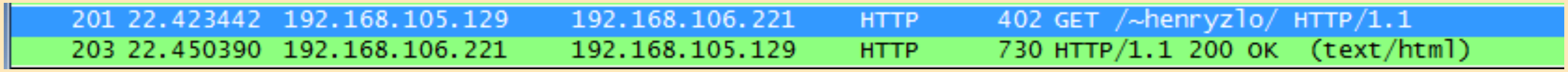
```
201 22.423442  192.168.105.129   192.168.106.221   HTTP    402 GET /~henryzlo/ HTTP/1.1
203 22.450390  192.168.106.221   192.168.105.129   HTTP    730 HTTP/1.1 200 OK  (text/html)
```

The GET command requests a web page



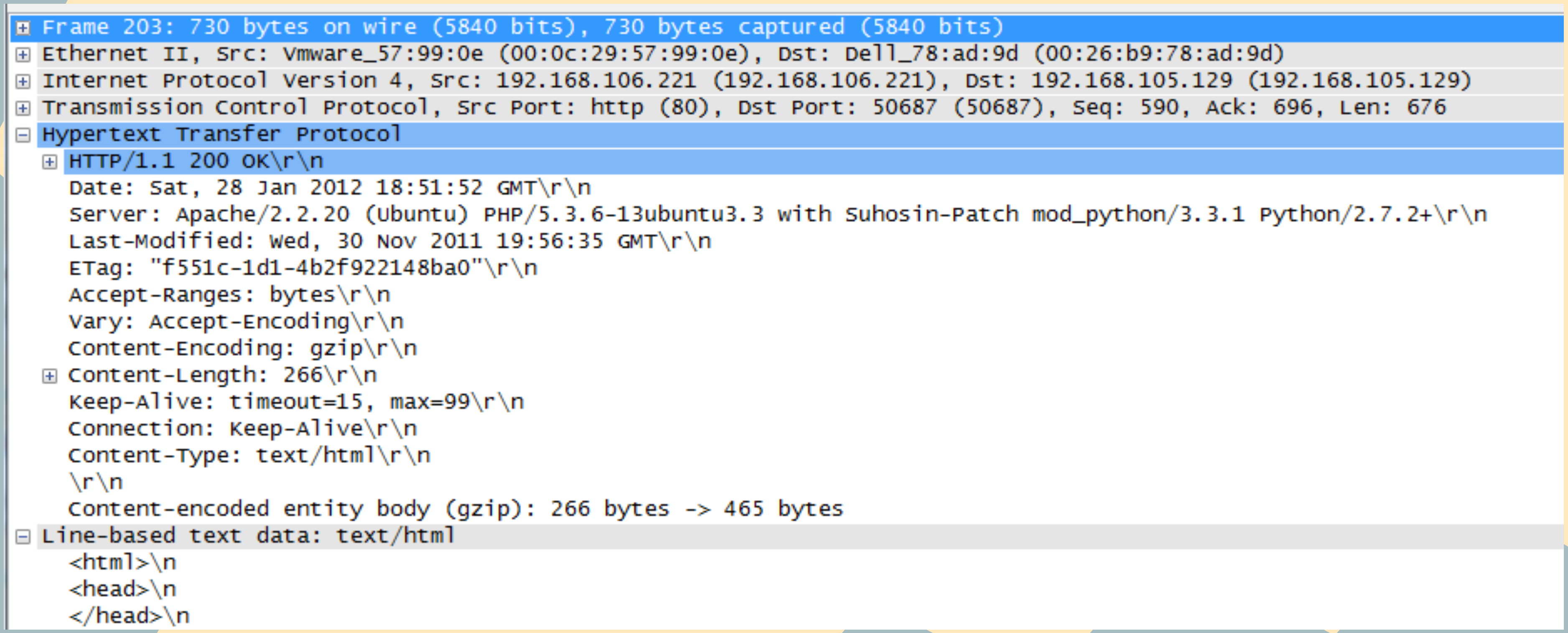
```
⊞ Frame 201: 402 bytes on wire (3216 bits), 402 bytes captured (3216 bits)
⊞ Ethernet II, Src: Dell_78:ad:9d (00:26:b9:78:ad:9d), Dst: Vmware_57:99:0e (00:0c:29:57:99:0e)
⊞ Internet Protocol Version 4, Src: 192.168.105.129 (192.168.105.129), Dst: 192.168.106.221 (192.168.106.221)
⊞ Transmission Control Protocol, Src Port: 50687 (50687), Dst Port: http (80), Seq: 348, Ack: 590, Len: 348
⊟ Hypertext Transfer Protocol
  ⊞ GET /~henryzlo/ HTTP/1.1\r\n
    Host: www.cs.umb.edu\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:9.0.1) Gecko/20100101 Firefox/9.0.1\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://www.cs.umb.edu/~henryzlo/]
```

HTTP Request



```
201 22.423442 192.168.105.129    192.168.106.221    HTTP     402 GET /~henryzlo/ HTTP/1.1
203 22.450390 192.168.106.221    192.168.105.129    HTTP     730 HTTP/1.1 200 OK  (text/html)
```

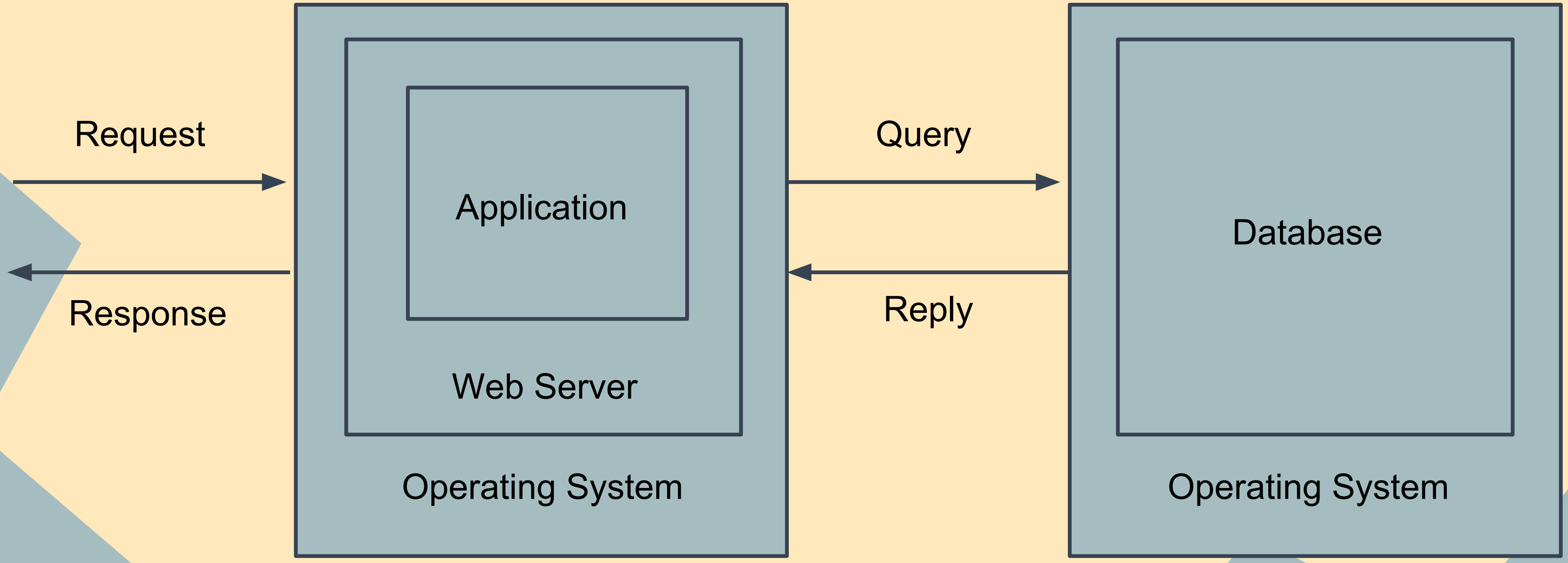
The response contains the web page



```
⊞ Frame 203: 730 bytes on wire (5840 bits), 730 bytes captured (5840 bits)
⊞ Ethernet II, Src: Vmware_57:99:0e (00:0c:29:57:99:0e), Dst: Dell_78:ad:9d (00:26:b9:78:ad:9d)
⊞ Internet Protocol Version 4, Src: 192.168.106.221 (192.168.106.221), Dst: 192.168.105.129 (192.168.105.129)
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: 50687 (50687), Seq: 590, Ack: 696, Len: 676
⊟ Hypertext Transfer Protocol
  ⊞ HTTP/1.1 200 OK\r\n
    Date: Sat, 28 Jan 2012 18:51:52 GMT\r\n
    Server: Apache/2.2.20 (Ubuntu) PHP/5.3.6-13ubuntu3.3 with Suhosin-Patch mod_python/3.3.1 Python/2.7.2+\r\n
    Last-Modified: Wed, 30 Nov 2011 19:56:35 GMT\r\n
    ETag: "f551c-1d1-4b2f922148ba0"\r\n
    Accept-Ranges: bytes\r\n
    Vary: Accept-Encoding\r\n
    Content-Encoding: gzip\r\n
  ⊞ Content-Length: 266\r\n
    Keep-Alive: timeout=15, max=99\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html\r\n
    \r\n
    Content-encoded entity body (gzip): 266 bytes -> 465 bytes
⊟ Line-based text data: text/html
    <html>\n
    <head>\n
    </head>\n
```

Behind the Scenes

- Requests are handled by the application.
- Application sits on top of the web server and the OS.
- Application communicates with database.



Behind the Scenes

- Web servers
  - Apache
  - IIS (Windows Server)
- Applications are written in
  - PHP
  - Perl
  - Python
  - ASP.NET
  - Any other language
- Databases
  - MySQL
  - Microsoft Access

Databases

- Stores data in tables.
- Applications use SQL queries to communicate.
- Queries must be authenticated (there are permissions in the database).
- Example of SQL:
  - INSERT INTO My_table (field1, field2, field3) VALUES ('test', 'N', NULL);
  - SELECT title, price FROM Book WHERE price > 1.0;

command attributes table

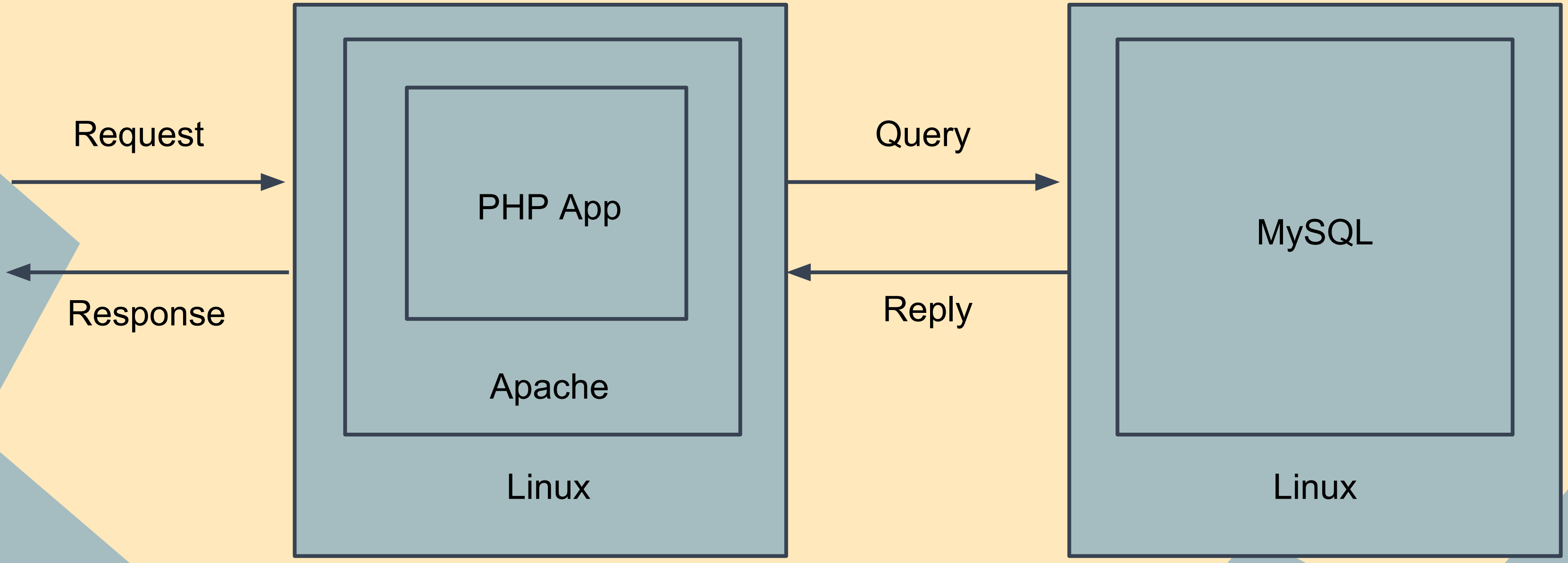
Application

- Written in various languages.
- Handles the requests, responses, communicates with database.
- More on this later.

LAMP

LAMP

- Linux, Apache, MySQL, PHP.
- Most popular web application stack.
- Free and open source.

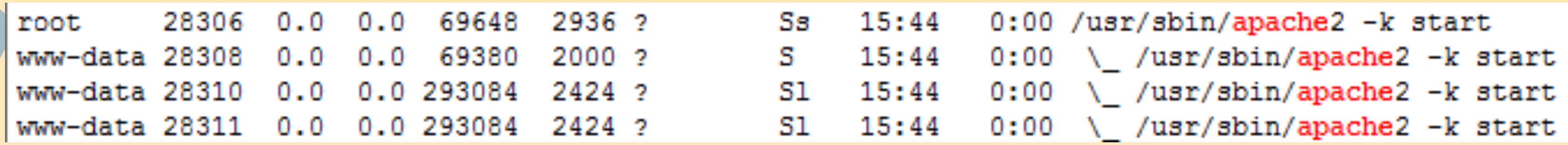


LAMP Components

- Apache runs a PHP application, which listens on port 80 for requests.
- PHP takes in the request data, constructs an HTTP response, and queries database if necessary.
- The Apache server should listen on port 80 (no restrictions.)
- The database should **only** listen to the web server.

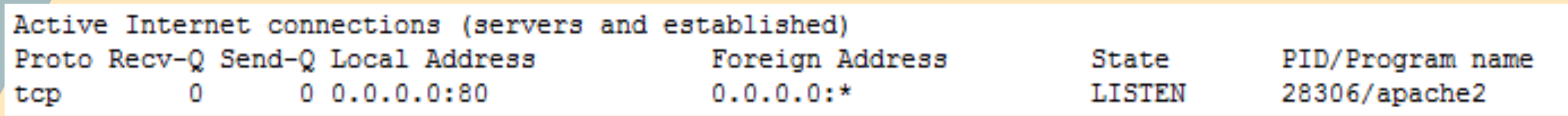
Apache Process Profile

- Apache runs as root and spawns off "worker threads" owned by www-data.



```
root      28306  0.0  0.0  69648  2936 ?        Ss   15:44   0:00 /usr/sbin/apache2 -k start
www-data 28308  0.0  0.0  69380  2000 ?        S    15:44   0:00  \_ /usr/sbin/apache2 -k start
www-data 28310  0.0  0.0 293084  2424 ?        Sl   15:44   0:00  \_ /usr/sbin/apache2 -k start
www-data 28311  0.0  0.0 293084  2424 ?        Sl   15:44   0:00  \_ /usr/sbin/apache2 -k start
```

- By default, listens on port 80 on every interface.

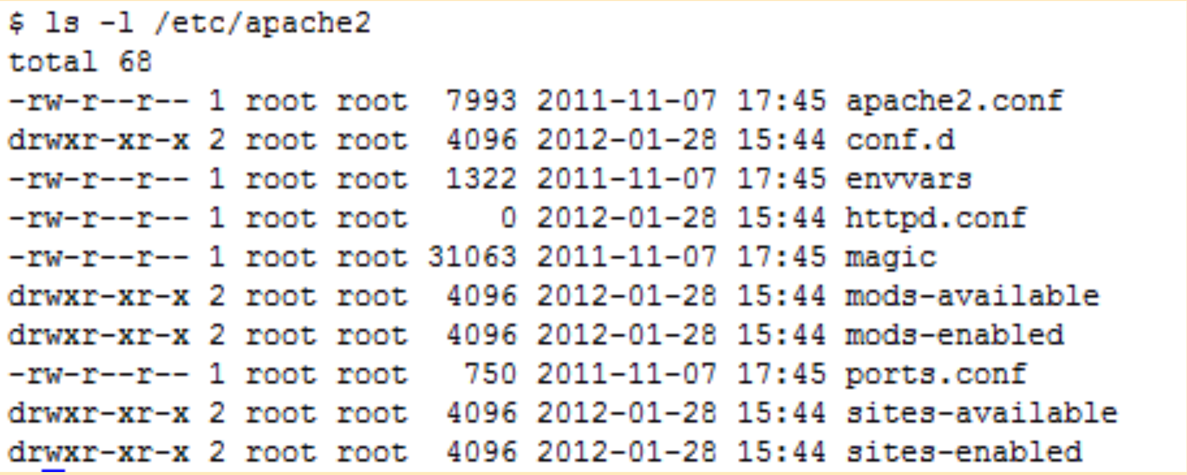


```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      28306/apache2
```

- Port 443 for HTTPS.

Apache Filesystem Profile

- Configuration files in /etc/apache2.

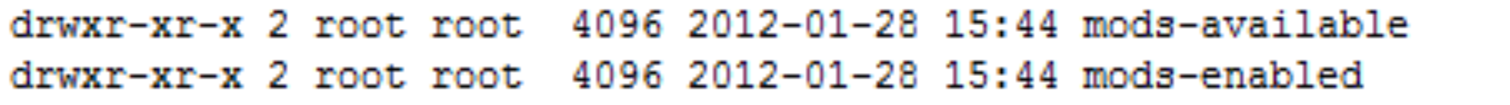


```
$ ls -l /etc/apache2
total 68
-rw-r--r-- 1 root root  7993 2011-11-07 17:45 apache2.conf
drwxr-xr-x 2 root root  4096 2012-01-28 15:44 conf.d
-rw-r--r-- 1 root root  1322 2011-11-07 17:45 envvars
-rw-r--r-- 1 root root     0 2012-01-28 15:44 httpd.conf
-rw-r--r-- 1 root root 31063 2011-11-07 17:45 magic
drwxr-xr-x 2 root root  4096 2012-01-28 15:44 mods-available
drwxr-xr-x 2 root root  4096 2012-01-28 15:44 mods-enabled
-rw-r--r-- 1 root root   750 2011-11-07 17:45 ports.conf
drwxr-xr-x 2 root root  4096 2012-01-28 15:44 sites-available
drwxr-xr-x 2 root root  4096 2012-01-28 15:44 sites-enabled
```

- sites-available contains web site configurations (NOT data!).
- *conf* are config files and folders.

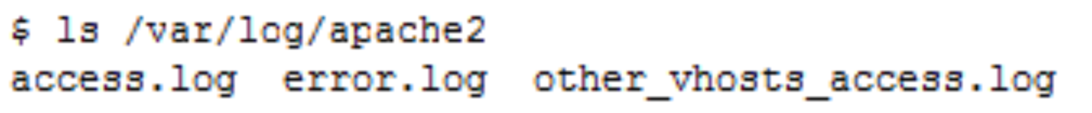
Apache Filesystem Profile

- Apache uses mods to support functionality such as PHP, MySQL.



```
drwxr-xr-x 2 root root  4096 2012-01-28 15:44 mods-available
drwxr-xr-x 2 root root  4096 2012-01-28 15:44 mods-enabled
```

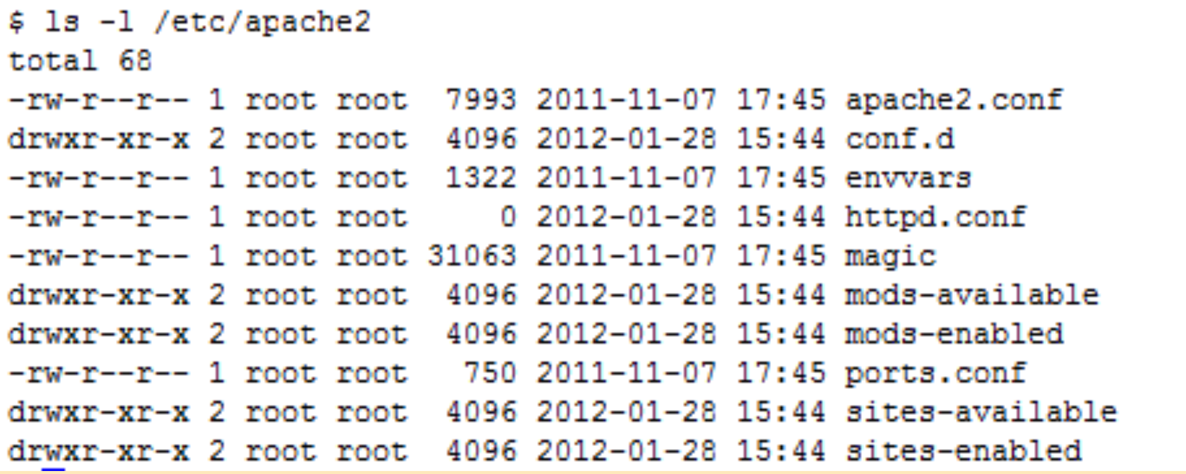
- Logs are in /var/log/apache2.



```
$ ls /var/log/apache2
access.log  error.log  other_vhosts_access.log
```

Apache Filesystem Profile

- Configuration files in /etc/apache2.

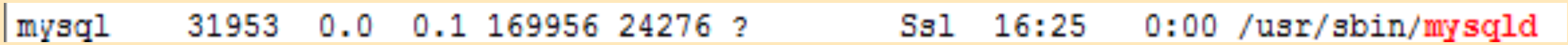


```
$ ls -l /etc/apache2
total 68
-rw-r--r-- 1 root root  7993 2011-11-07 17:45 apache2.conf
drwxr-xr-x 2 root root  4096 2012-01-28 15:44 conf.d
-rw-r--r-- 1 root root  1322 2011-11-07 17:45 envvars
-rw-r--r-- 1 root root     0 2012-01-28 15:44 httpd.conf
-rw-r--r-- 1 root root 31063 2011-11-07 17:45 magic
drwxr-xr-x 2 root root  4096 2012-01-28 15:44 mods-available
drwxr-xr-x 2 root root  4096 2012-01-28 15:44 mods-enabled
-rw-r--r-- 1 root root   750 2011-11-07 17:45 ports.conf
drwxr-xr-x 2 root root  4096 2012-01-28 15:44 sites-available
drwxr-xr-x 2 root root  4096 2012-01-28 15:44 sites-enabled
```

- Sites-available contains web site configurations.
- *conf* are config files and folders.

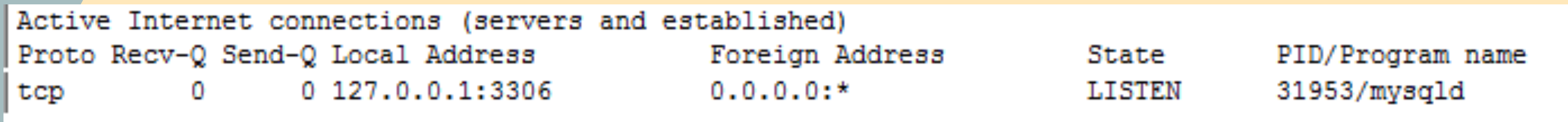
MySQL

- Runs as mysql user.
- MySQL has its own users and permissions - there is a 'root' user inside MySQL.



```
mysql     31953  0.0  0.1 169956 24276 ?        Ssl  16:25   0:00 /usr/sbin/mysqld
```

- Listens on port 3306, by default only to requests from localhost.



```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             State       PID/Program name
tcp        0      0 127.0.0.1:3306              0.0.0.0:*                   LISTEN      31953/mysqld
```

PHP

- Config file is php.ini
  - Usually resides in /etc/php5/apache2/php.ini

- Error messages go to /var/log/apache2/error.log by default

Live Demo

- Installing a LAMP server.
- Configuring a LAMP server.