I used this resource to help me understand the logs: <http://httpd.apache.org/docs/2.2/logs.html>

1. What type of log file is it?

**Answer:** There are 5 access logs, 5 error logs (6 in the file you shared, but “error\_log-20131201” seems to have a duplicate), a security log (authentication?), and a message log.

1. What are the dates which are represented by the logs?

**Answer:**

access\_log/error\_log (20131117): **10/Nov/2013** to 17/Nov/2013

access\_log/error\_log (20131124): 17/Nov/2013 to 24/Nov/2013

access\_log/error\_log (20131201): 24/Nov/2013 to 01/Dec/2013

access\_log/error\_log (20131208): 01/Dec/2013 to 08/Dec/2013

access log/errorlog: 08/Dec/2013 to **10/Dec/2013**

1. How many unique users appear?

**Answer:** There is a lot of different IPs. I am not really sure if you wanted us to count one by one or if you just wanted us to take a look and see there are a lot of users making requests to this server. I would think the second option is the most reasonable one. I would imagine there is an easier way to find out the number of users other than counting one by one (I don’t think in a real life situation one would count IPs one by one. Facebook, for instance, would bankrupt if they had to perform such task “by hand“ (so to say) on a regular basis).

1. What was the largest data export? and does it look out of the ordinary?

On access\_log, there are some images that seem rather large:

i.e.

- 71.47.54.177 requested some images, some of which were large: /themes/danland/images/**slideshow-shadow.gif** HTTP/1.1" 200 **45611**

- /themes/danland/images/slideshows/**snow.jpg** HTTP/1.1" 200 **43274**

These files seem to be large for .gif and .jpeg extensions but I don’t know what kind of image these are (I would guess they are high resolution images or they were not properly compressed for the web). I tried to open the pages to see the pictures but an error occurred.

1. What is the most common error found in the error logs?

**Answer:** The most common error was “File does not exist.” “Script not found or unable to stat“ was a recurrent one as well.

1. Do you see anything that is out of the ordinary?

**Answer:** On access\_log, user IP 89.248.160.192 was very active on 02/Dec/2013 and made a lot of requests to the phpMyAdmin. I did a research on “ZmEu“ (which was part of the log) and found out that this is a bot that “tries to find vulnerabilities in the phpMyAdmin“ (source: [http://ensourced.wordpress  
.com/2011/02/25/zmeu-attacks-some-basic-forensic/](http://ensourced.wordpress.com/2011/02/25/zmeu-attacks-some-basic-forensic/)).

Apparently, the attacks were not successful because all requests returned a 404 error. See a log line: 89.248.160.192 - - [02/Dec/2013:13:18:13 +0000] "GET /phpMyAdmin/scripts/setup.php HTTP/1.1" **404** 306 "-" "**ZmEu**"

This is probably not out of the ordinary butI learned about the baiduspider, the Chinese crawler bot. I did some research and fund funny that a lot of people were concerned that this bot was crawling their site, as if there was an ill intention behind it.

1. Write a short synopsis of what you found in each file.

Access logs:

* + IP addresses
  + User login names
  + Dates and times of requests
  + Type of requests (mostly HTTP)
  + Resource requested
  + Browser being used for the request
  + Web site on which the request was made
  + If the request was successful or not (numbers at the end of the log starting with 2, 3, 4, or 5 provide this information).
  + Size of the requested file (in b)

Error logs:

* + IP addresses
  + Dates and times of requests
  + If there was an error (error, notice, warning)
  + Type of error (i.e. “File does not exist”)
  + The requested address ( i.e. /var/www/cgi-bin/php5)

Authentication logs:

* + Date and time the log was created
  + The sshd (solid-state hybrid drives) – not really sure what it does
  + Type of authentication and if it was successful or if it failed (i.e.)
  + If there was an error
  + What port the request was made from
  + The type of secure shell used in the transfer of data (SSH or SSH2)