Examine the each of the logs and answer the following questions:

1. What type of log files are they?

Access Log, Error Log, System Messages, and Secure log

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

November 17, 2013; November 24, 2013; December 1, 2013; December 8, 2013; December 9, 2013; December 10, 2013

1. How many unique users appear?

One user: root

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

Dec 8 04:45:24 clinical-security-lamp kernel: IN=eth0 OUT= MAC=40:40:7c:01:70:3c:d0:d0:fd:6d:b5:bf:08:00 SRC=141.212.121.83 DST=209.20.69.216 LEN=40 TOS=0x00 PREC=0x00 TTL=244 ID=54321 PROTO=TCP SPT=40549 DPT=443 WINDOW=65535 RES=0x00 SYN URGP=0

Nothing looks out of the ordinary

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

File does not exist

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

In the secure log user: root tried to authenticate unsuccessfully several times over and over and over. Perhaps a hack attempt?

1. Write a short synopsis of what you found.

These are the logs from a Linux Server running PHP 5.3.3 and Apache2. Both the error logs and access logs are available along with the security log and system message log.