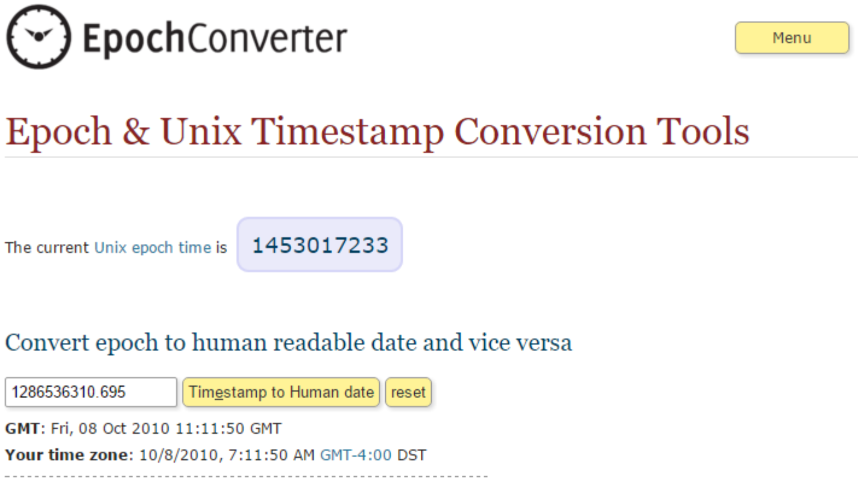
Log Analysis

Squid (Hard)

This challenge evaluates the contestant’s ability to analyze a Squid proxy log. Basic scripting knowledge is necessary to complete the challenge in a reasonable amount of time.

Question 1 can be solved by taking any of the Epoch timestamps and converting it into a human-readable date. An online tool, such as Epoch Converter, can be used to do this.



Epoch & Unix Timestamp Conversion Tools

The current Unix epoch time is 1453017233

Convert epoch to human readable date and vice versa

1286536310.695

GMT: Fri, 08 Oct 2010 11:11:50 GMT
Your time zone: 10/8/2010, 7:11:50 AM GMT-4:00 DST

Questions 2 and 3 can be solved by parsing the log using this Linux command to sort based on response time:

```
cat data.log | awk '{print $2}' | sort -n
```

Question 4 can be solved by parsing the log using this Linux command to find the unique IP addresses in the log:

```
cat data.log | awk '{print $3}' | sort | uniq
```

Questions 5 and 6 can be solved by parsing the log using this Linux command to find the number of times each HTTP method was requested:

```
cat data.log | awk '{print $6}' | sort | uniq -c
```

Questions 7 and 8 can be solved by searching for the string “192.168.0.224” and looking for URLs with any mention of antivirus.

Question	Answer
In what year was this log saved?	2010
How many milliseconds did the fastest request take?	5
How many milliseconds did the longest request take?	41762
How many different IP addresses did the proxy service in this log?	4
How many GET requests were made?	35
How many POST requests were made?	78
What company created the antivirus used on the host at 192.168.0.224?	Symantec
What URL is used to download an antivirus update?	http://liveupdate.symantecliveupdate.com/streaming/norton$202009$20streaming$20virus$20definitions_1.0_symalllanguages_livetri.zip