Most common operating system and browser combination

You work for a large retailer that relies on Apache servers to support its ecommerce. Your corporate website team currently tests new deployments with the Chrome browser running on Windows. With limited resources, they need to focus their validation on the most common browser and operating system combination.

As an analyst, it's your job to help them reach a decision by supplying data on the most common operating system and browser combination used by people browsing the corporate website.

Data required

Web server data

Procedure

1. Search by values in the host field. For example, on Apache servers, enter this search:

   host=apache*

2. Enter a time range appropriate to your search. For this investigation it might make sense to look over a long period of time as well such as the last 24 hours, the last 7 days, or the last month.

3. Click Search.

4. After you start seeing results, check the Fields pane on the left-hand side of the screen and scroll down until you see the http_user_agent field. This field is logged by almost every type of webserver and describes the type of browser and device the user was using while navigating the site. Click the field to open the field dialog box.
5. In the field dialog box, click **Top values**. This shows you the most frequently seen values for that field.

Your search should look like this:

```
host=apache* top limit=20 http_user_agent
```

6. Check the data, for example, by clicking on the pie chart to visualize your results. It might be that the `http_user_agent` command on its own doesn't provide you with what you're looking for, so you can take extra steps to enrich the data.

7. Use the lookup command in your search to add a new set of fields that start with `ua_<something>`. These fields are retroactively applied to all events, so you can continue to add context, massage, and enrich data directly from your search in order to answer new questions of your data very quickly.

```
host=apache* | lookup user_agents http_user_agent
```

8. Add the eval command to join the operating system and browser fields together, add your top values limit back in, and re-run your search. You should now see device fields in the fields pane.

```
host=apache* | lookup user_agents http_user_agent | eval device=ua_os_family. "-" .ua_family | top limit = 20
```

---

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
9. You can also visualize your search, for example, by using a bar chart. You can now see the top OS and browser combination and supply this information to your website team.

Next steps

These additional Splunk resources might help you understand and implement these recommendations:

- Blog: Launching websites rapidly, without compromise
- Blog: A fast lane to value: Introducing IT Essentials Apps
- Blog: IT Essentials Work: A centralized app for all things IT Ops
- Tech Talk: Splunk Fundamentals: Working with web server data Part 1
- Tech Talk: Splunk Fundamentals: Working with web server data Part 2

Finally, you might be interested in other processes associated with the Managing web server performance use case.