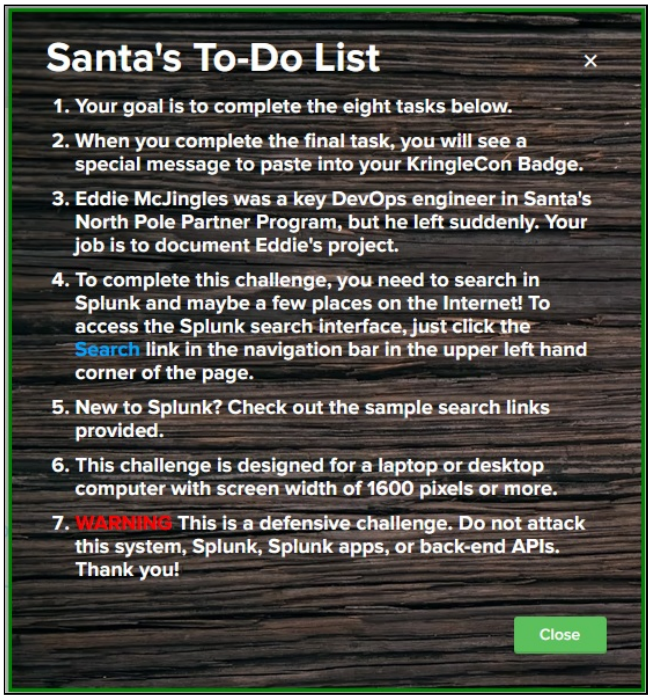
KringleCon 4: Calling Birds!

The Great Room

1. Click to talk to `Angel Candysalt`

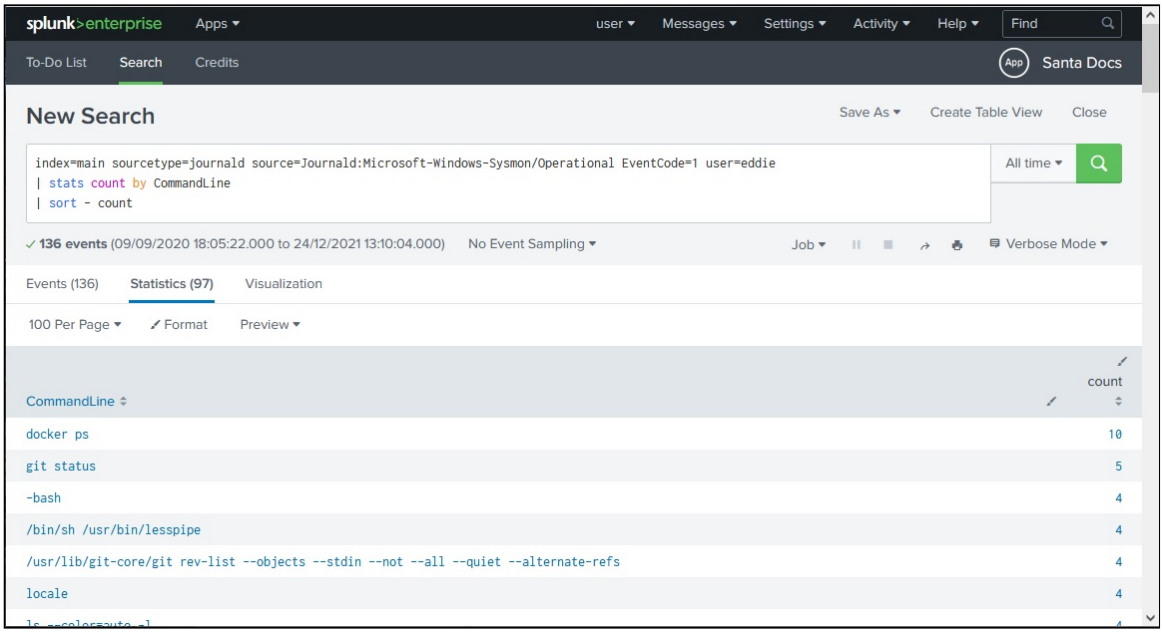
```
Greetings North Pole visitor! I'm Angel Candysalt!

A euphemism? No, that's my name. Why do people ask me that?

Anywho, I'm back at Santa's Splunk terminal again this year.

There's always more to learn!

Take a look and see what you can find this year.

With who-knows-what going on next door, it never hurts to have sharp SIEM skills!
```

2. Click `splunk >` terminal



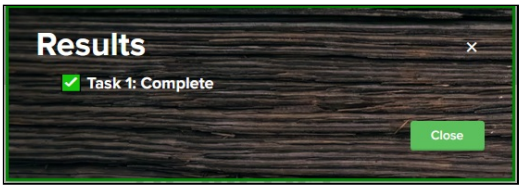
3. Click the `Close` button

4. Click the `Sysmon for Linux - Using Splunk stats and sort commands to find most/least common value of a field.` link

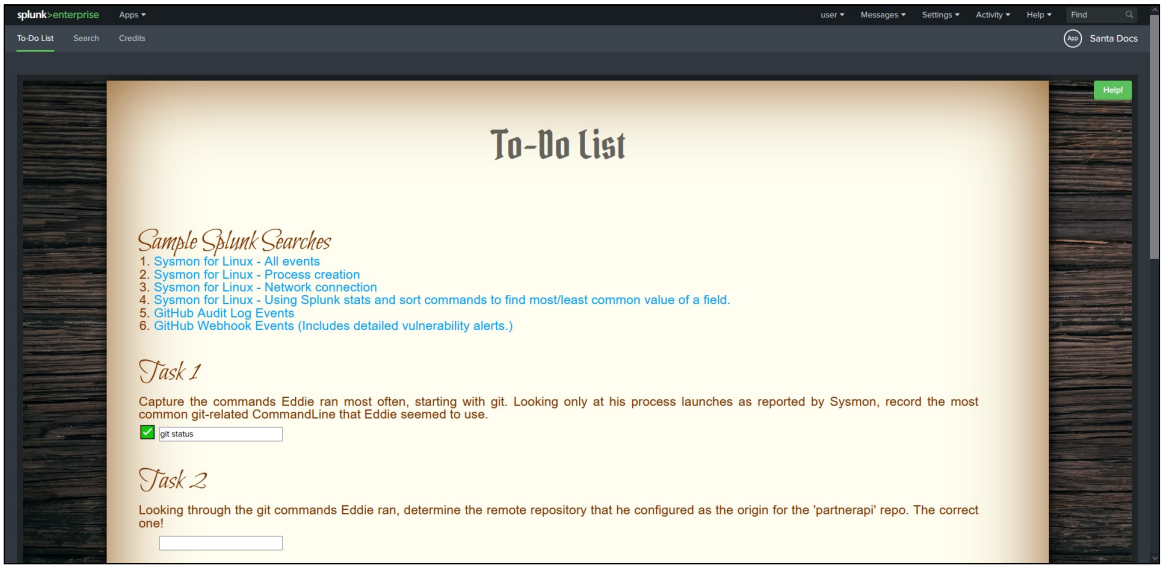


5. Click the `Second` tab and then click the `Task 1` text-box

6. Type `git status`

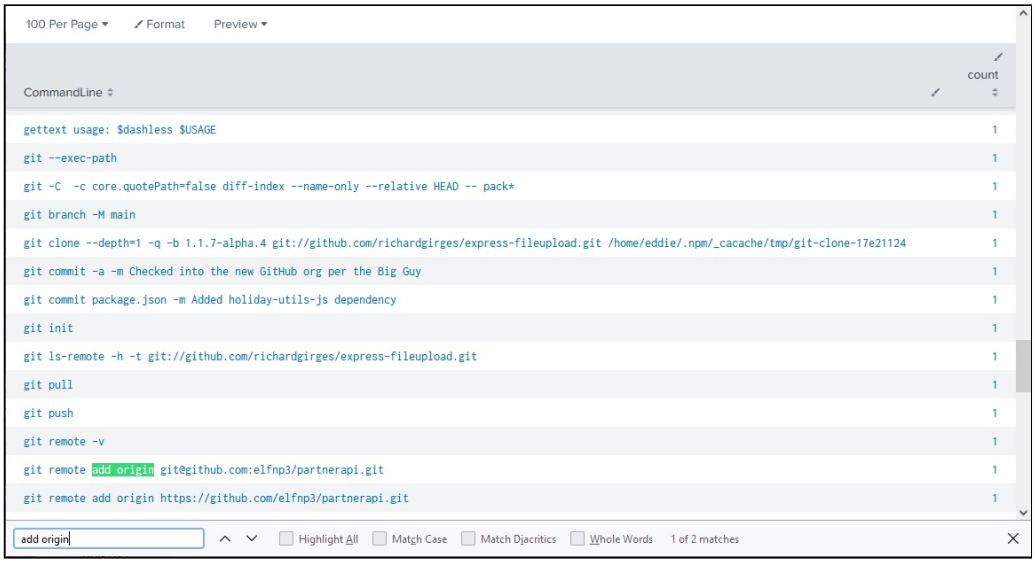


7. Click the `Close` button



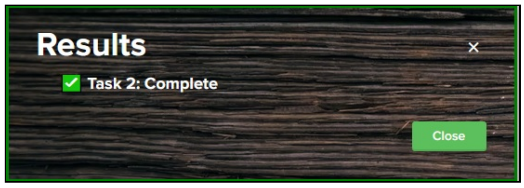
8. Click the `Third` tab and then press `CTRL + F`

9. Type `add origin`



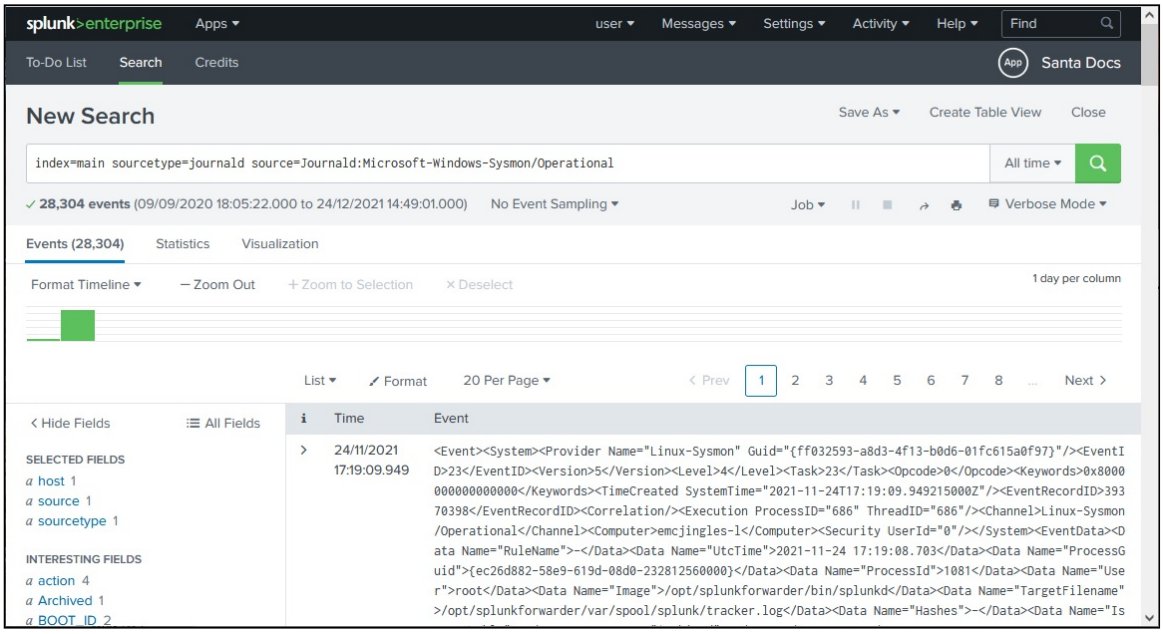
10. Click the `Second` tab and then click the `Task 2` text-box

11. Type `git@github.com:elfnp3/partnerapi.git`



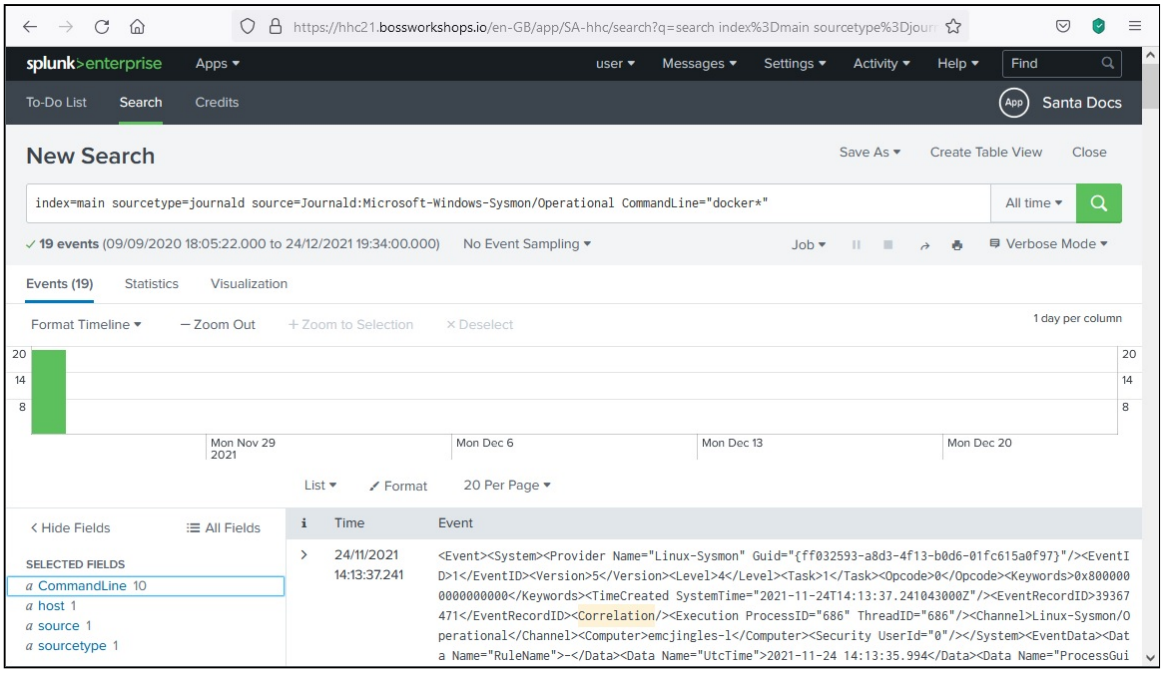
12. Click the `Close` button

13. Close the `Third` tab and then click the `Sysmon for Linux - All events` link

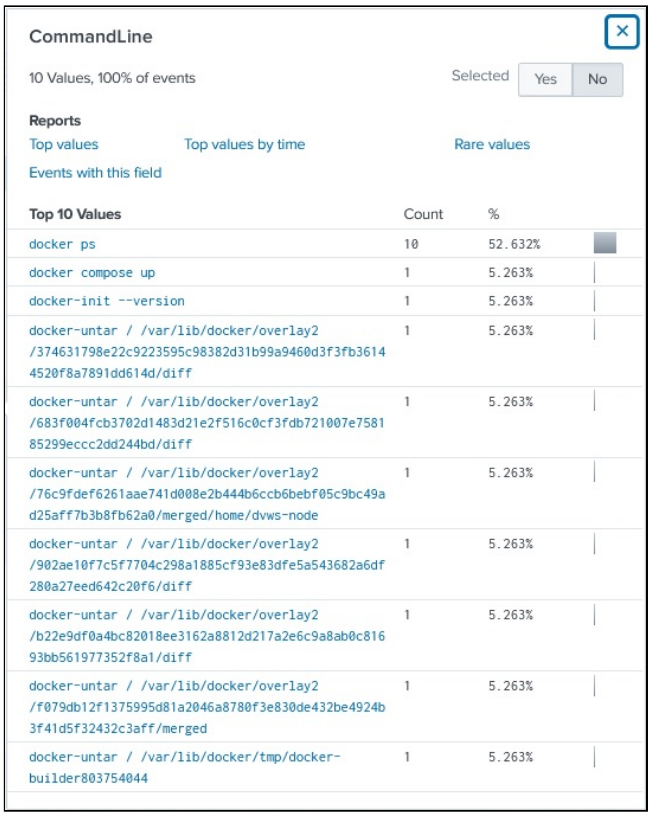


14. Add `CommandLine="docker*"` to the end of the Search

15. Click the `Search` button

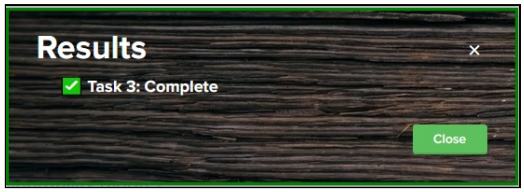


16. Click `CommandLine`

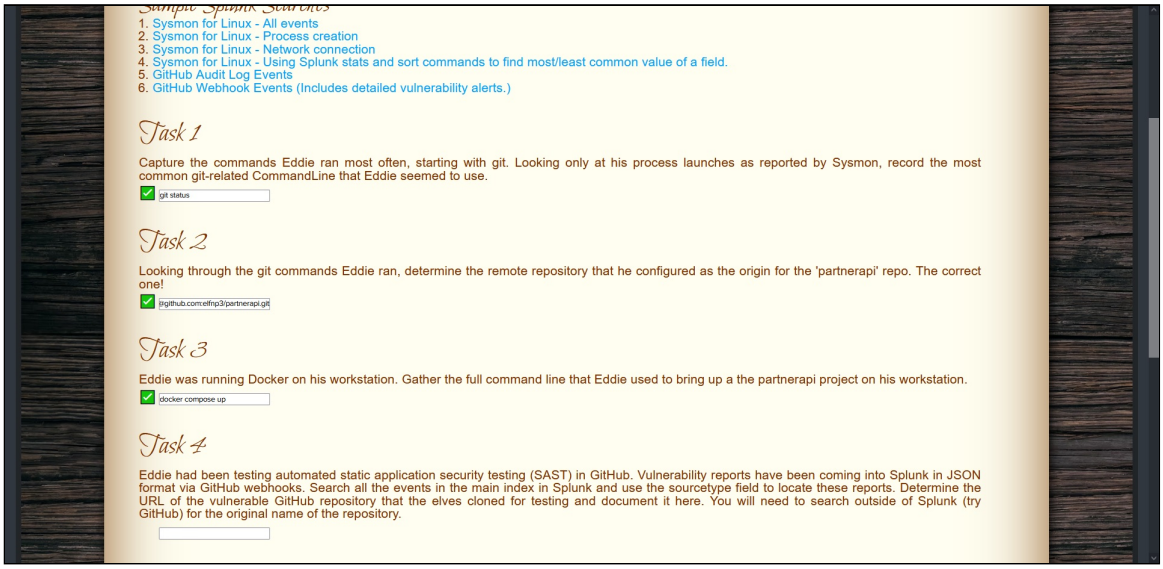


17. Click the `Second` tab and then click the `Task 3` text-box

18. Type `docker compose up`

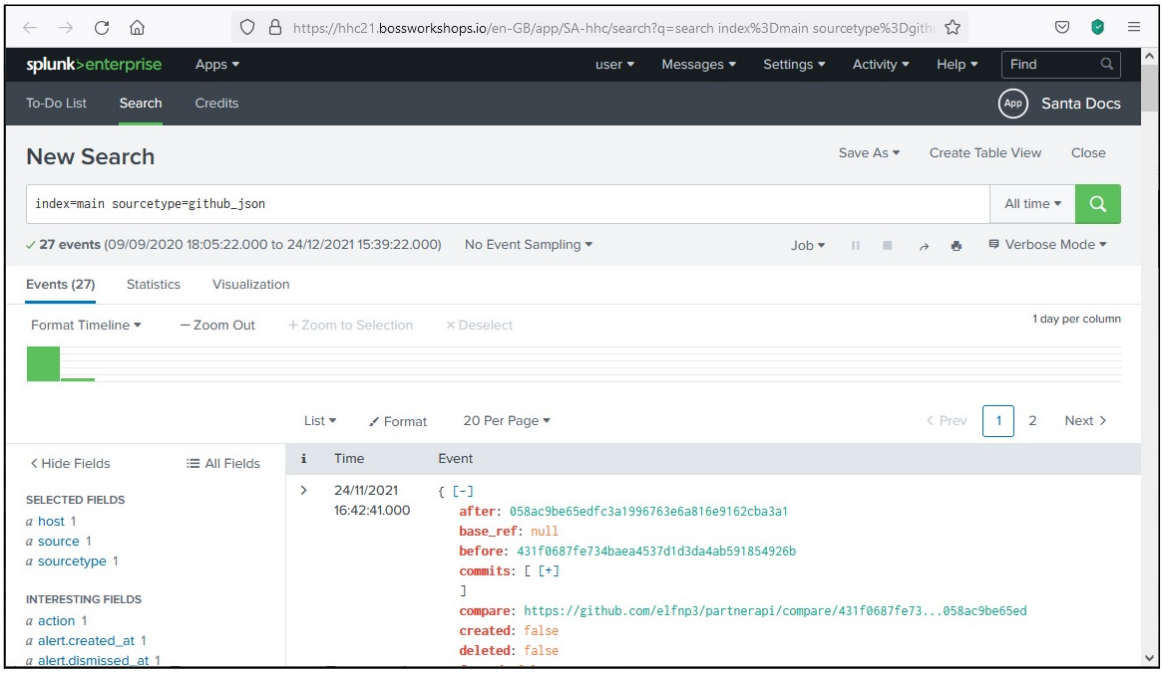


19. Click the `Close` button



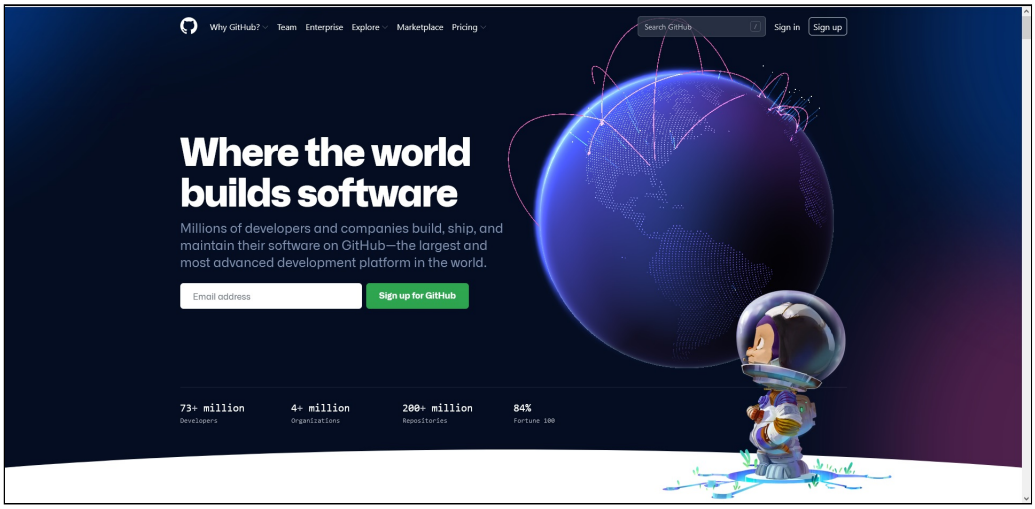
20. Close the `Third` tab

21. Click the `GitHub Webhook Events (Includes detailed vulnerability alerts.)` link

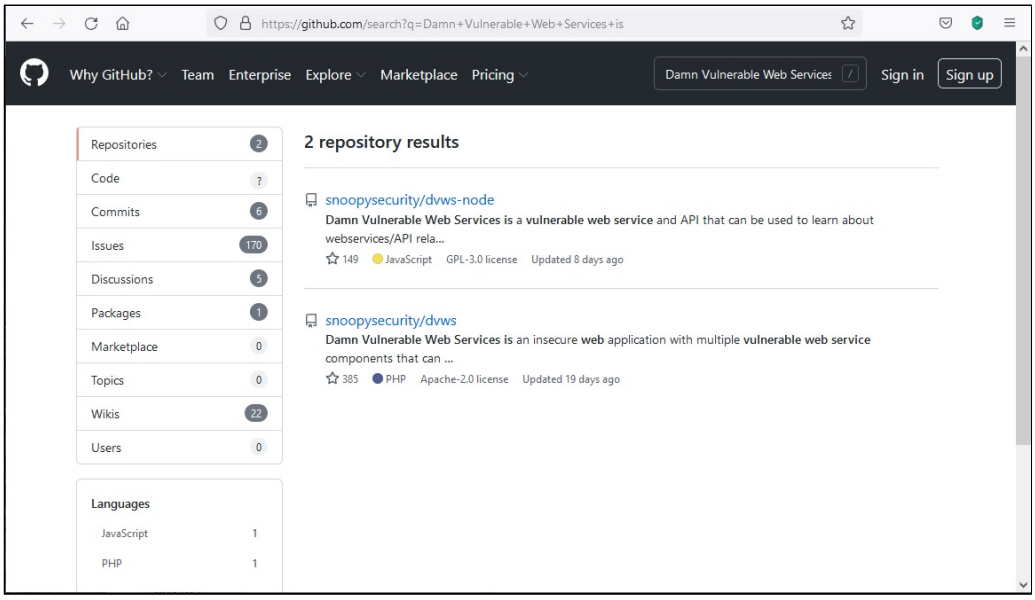


22. Scroll `Down` and then click `repository.description`

23. Open a `Fourth` tab and then navigate to `https://github.com/`



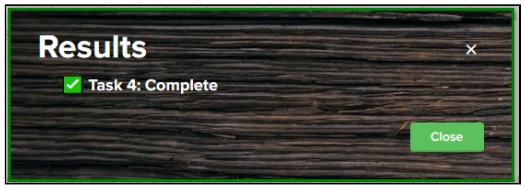
24. Type `Damn Vulnerable Web Services is` into the Search GitHub text-box



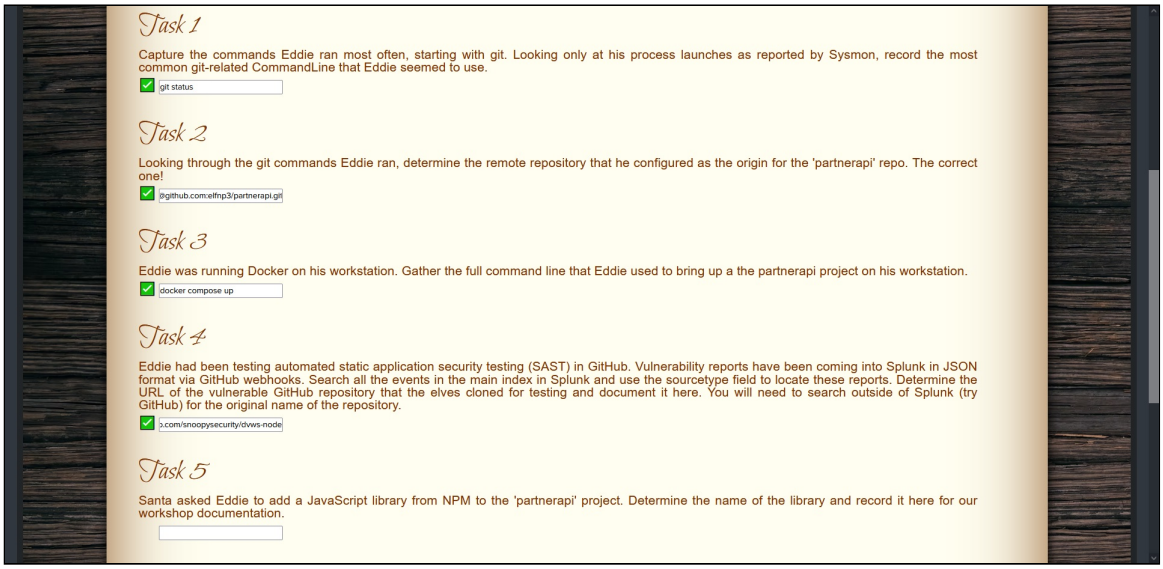
25. Click the `snoopysecurity/dvws-node` link and then scroll `Down`

26. Close the `Fourth` tab and then click the `Second` tab

27. Click the `Task 4` text-box and then type `dvws-node`



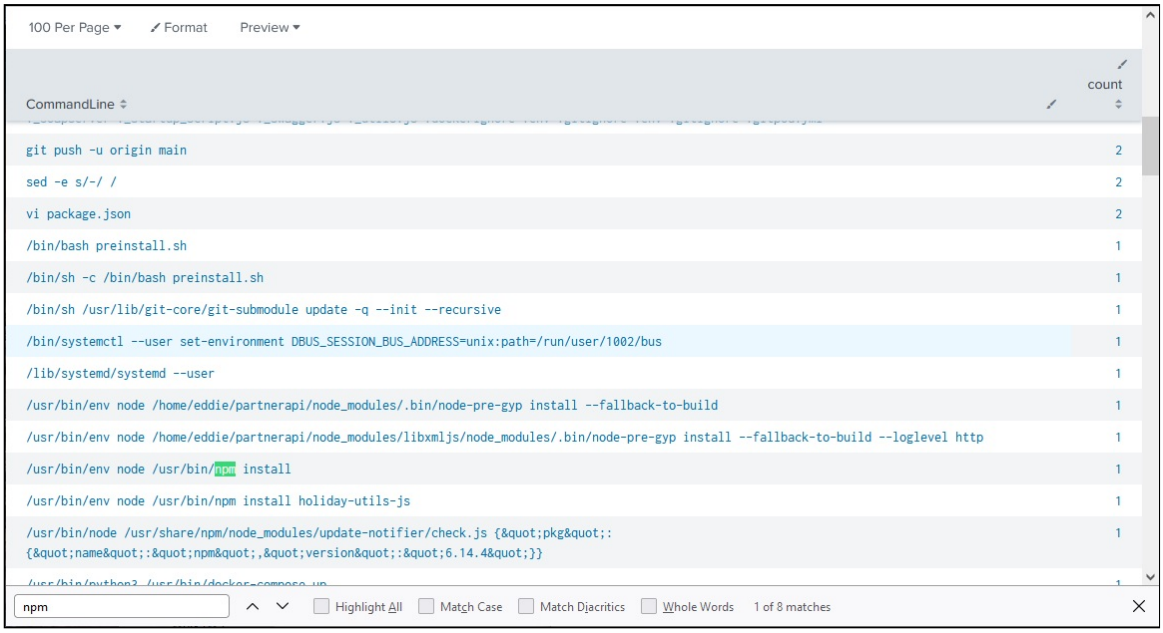
28. Click the `Close` button



29. Close the `Third` tab

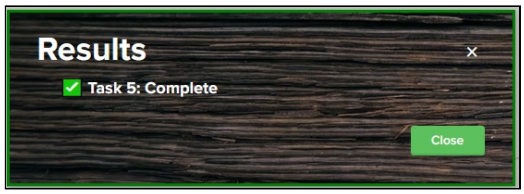
30. Click the `Sysmon for Linux - Using Splunk stats and sort commands to find most/least common value of a field.` link

31. Press `CTRL + F` and then type `npm`

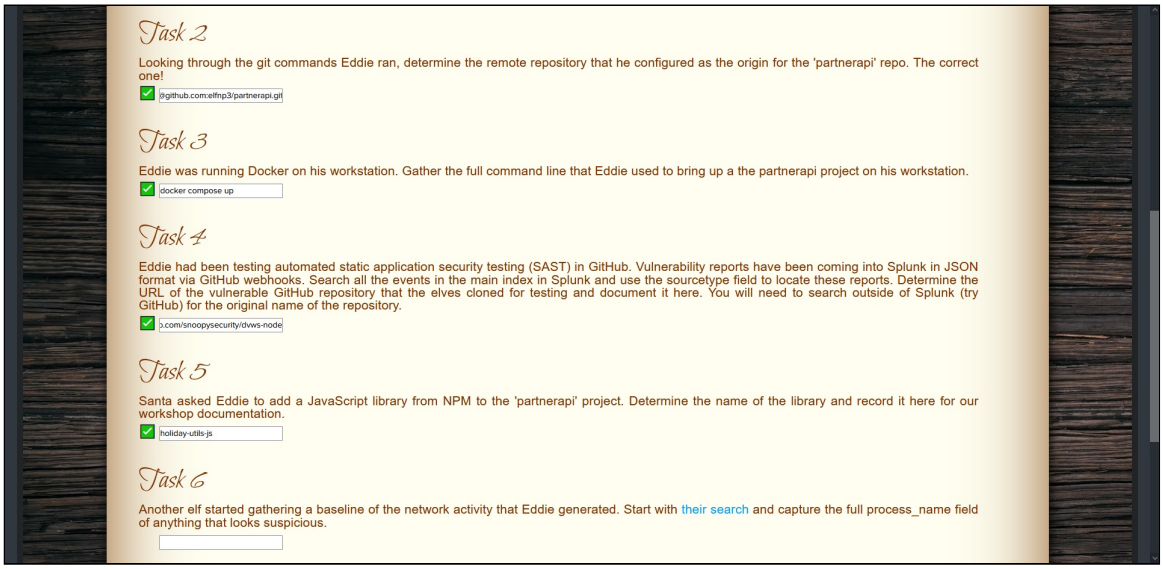


32. Close the `Third` tab and then click the `Task 5` text-box

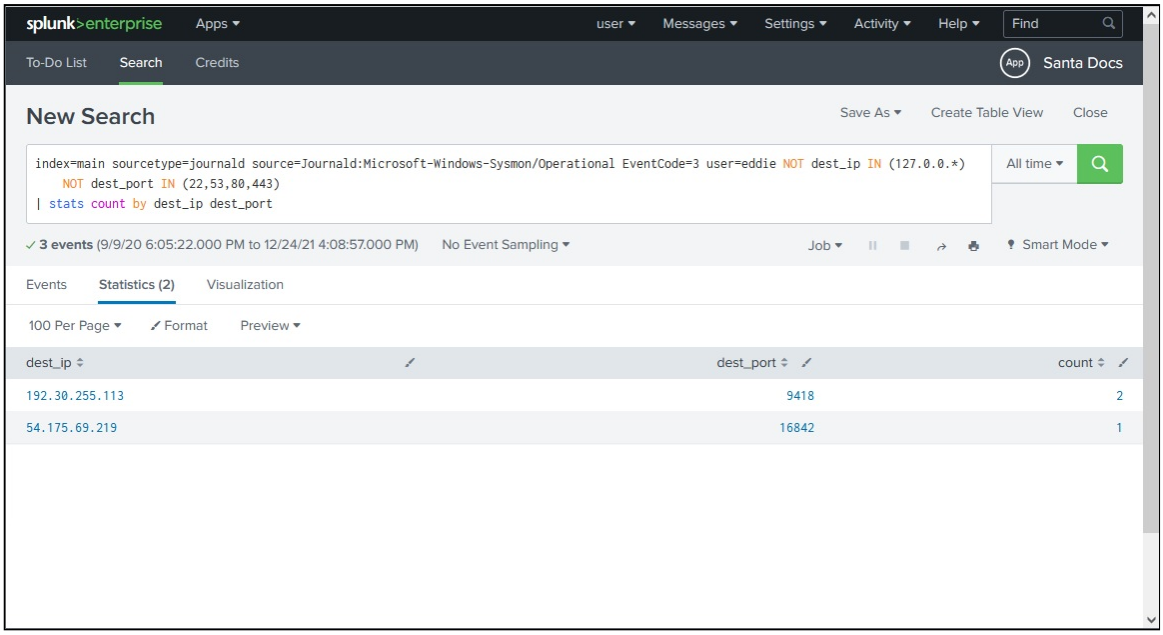
33. Type `holiday-utils-js`



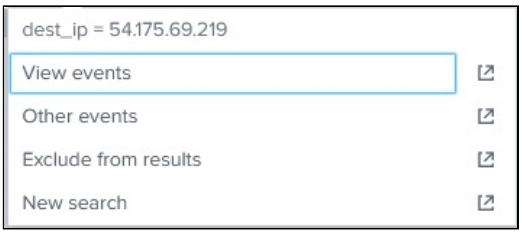
34. Click the `Close` button



35. Click `their search`

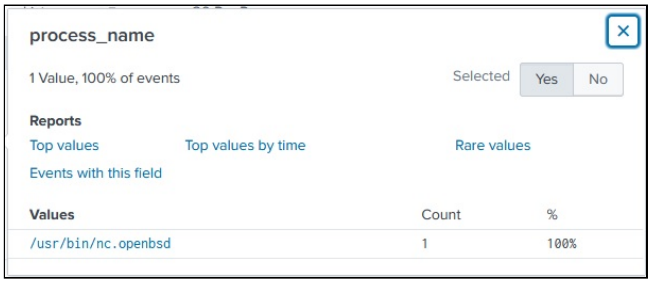


36. Click `54.175.69.219`



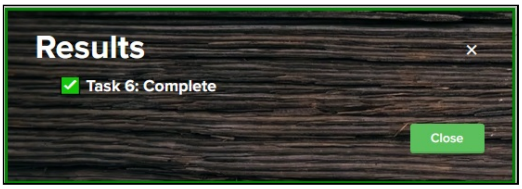
37. Click `View event`

38. Scroll `Down` and then click `process_name`

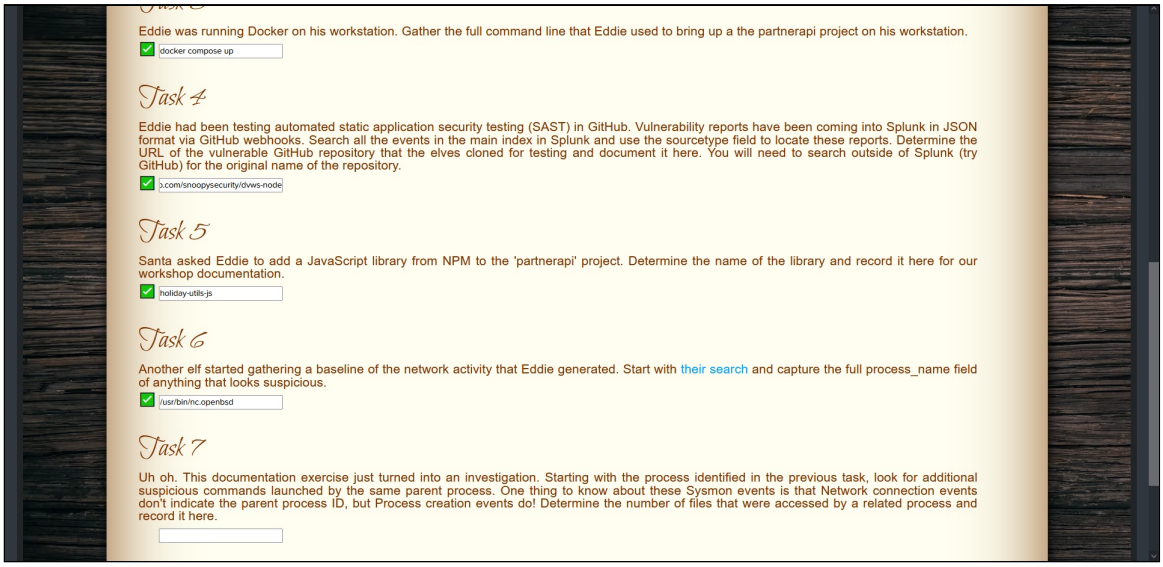


39. Click the `Second` tab and then click the `Task 6` text-box

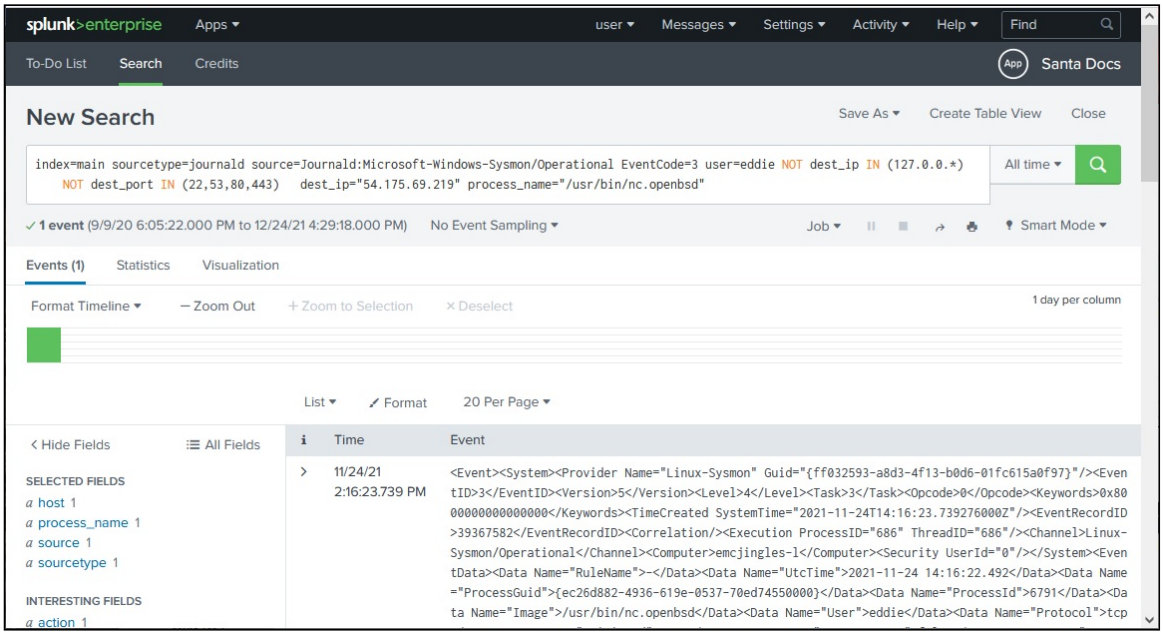
40. Type `/usr/bin/nc.openbsd`



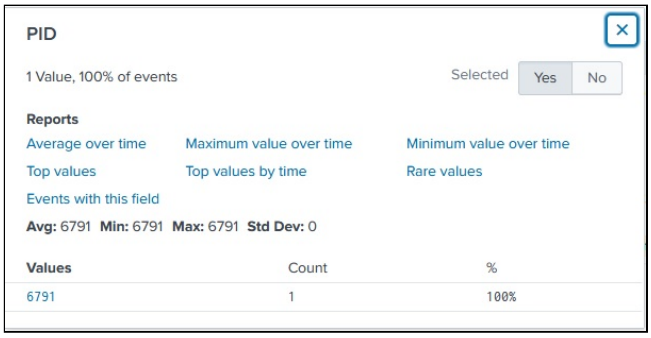
41. Click the `Close` button



42. Click the `Third` tab and then click `/usr/bin/nc.openbsd`

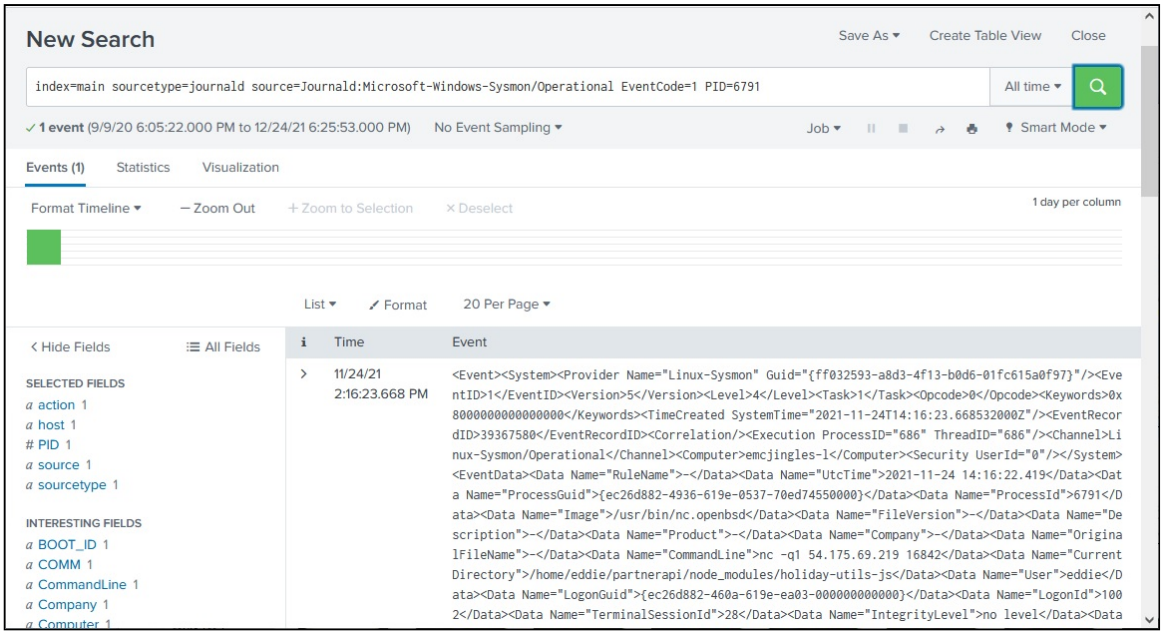


43. Scroll `Down` and then click `PID`

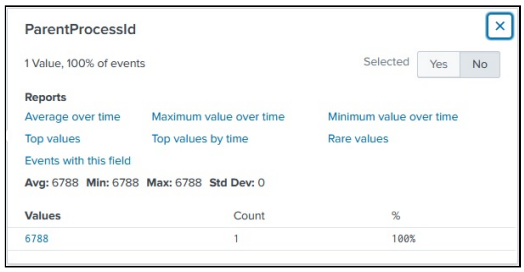


44. Modify the Search to `index=main sourcetype=journald source=Journald:Microsoft-Windows-Sysmon/Operational EventCode=1 PID=6791`

45. Click the `Search` button

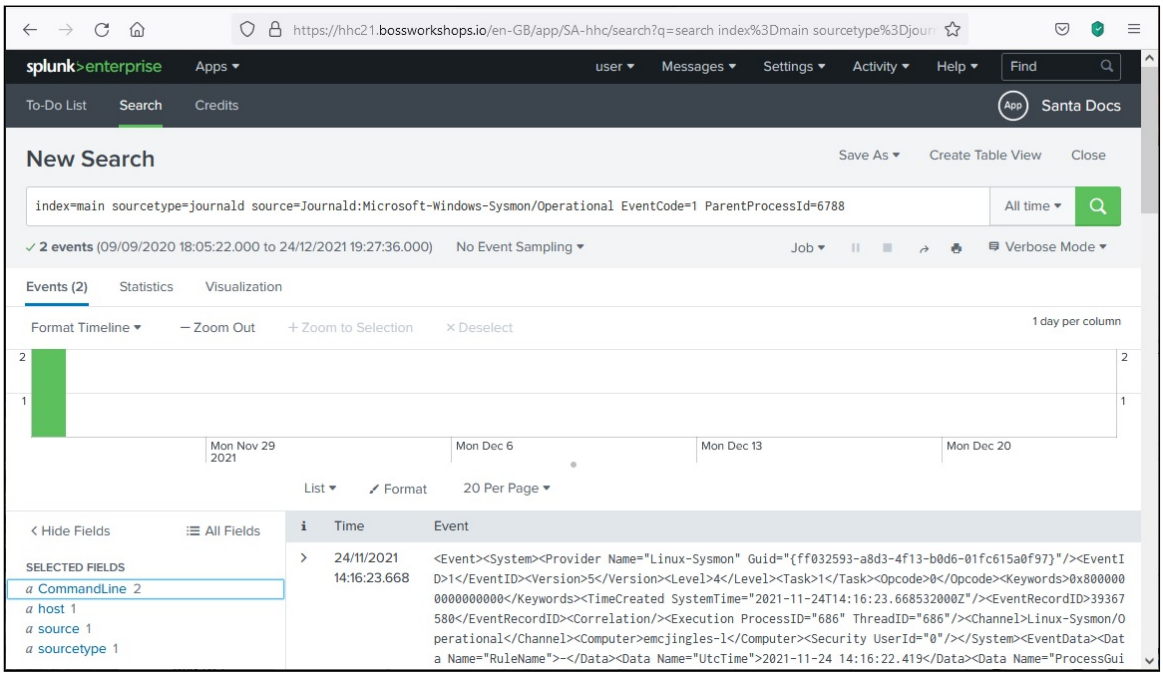


46. Scroll `Down` and then click `ParentProcessId`

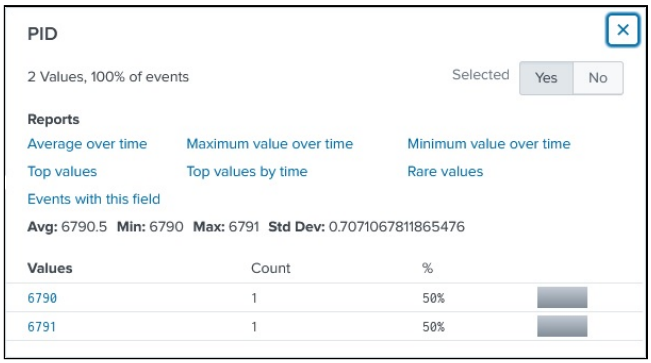


47. Modify the Search to `index=main sourcetype=journald source=Journald:Microsoft-Windows-Sysmon/Operational EventCode=1 ParentProcessId=6788`

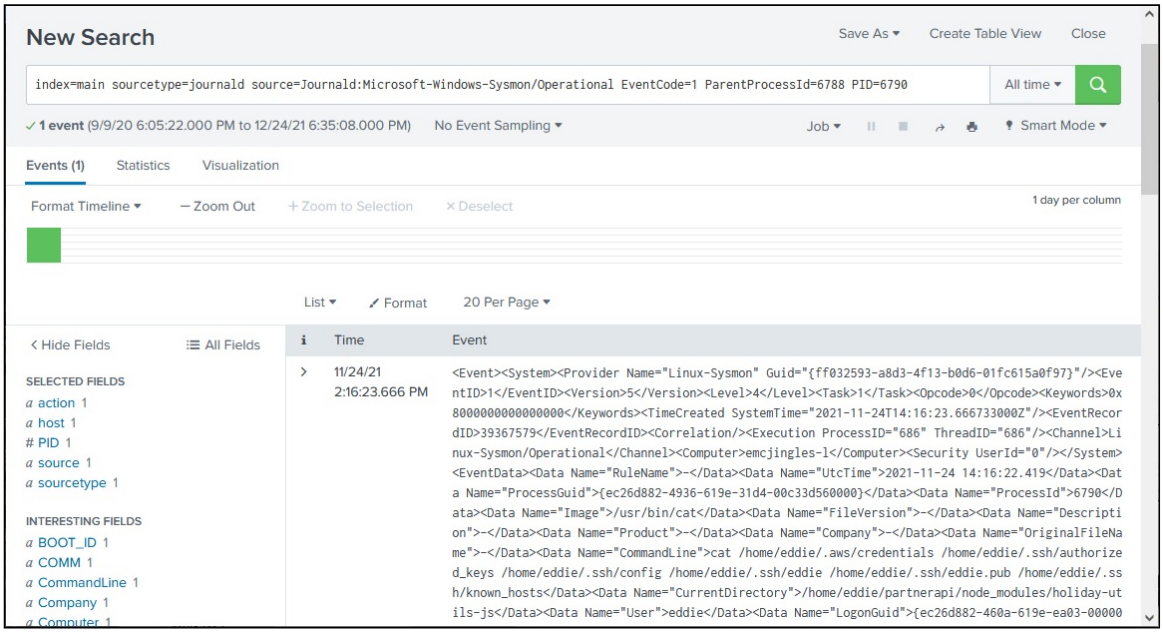
48. Click the `Search` button



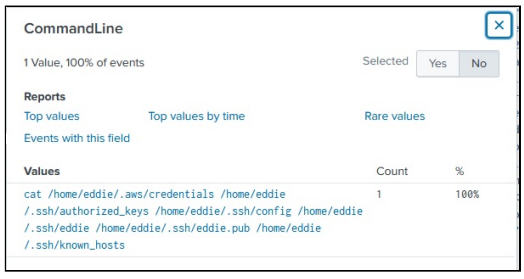
49. Scroll Down and then click PID



50. Click 6790

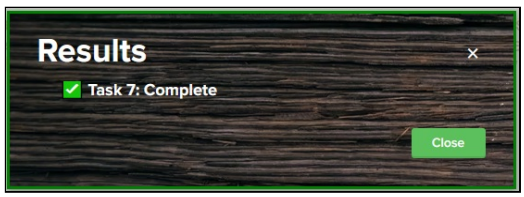


51. Click CommandLine

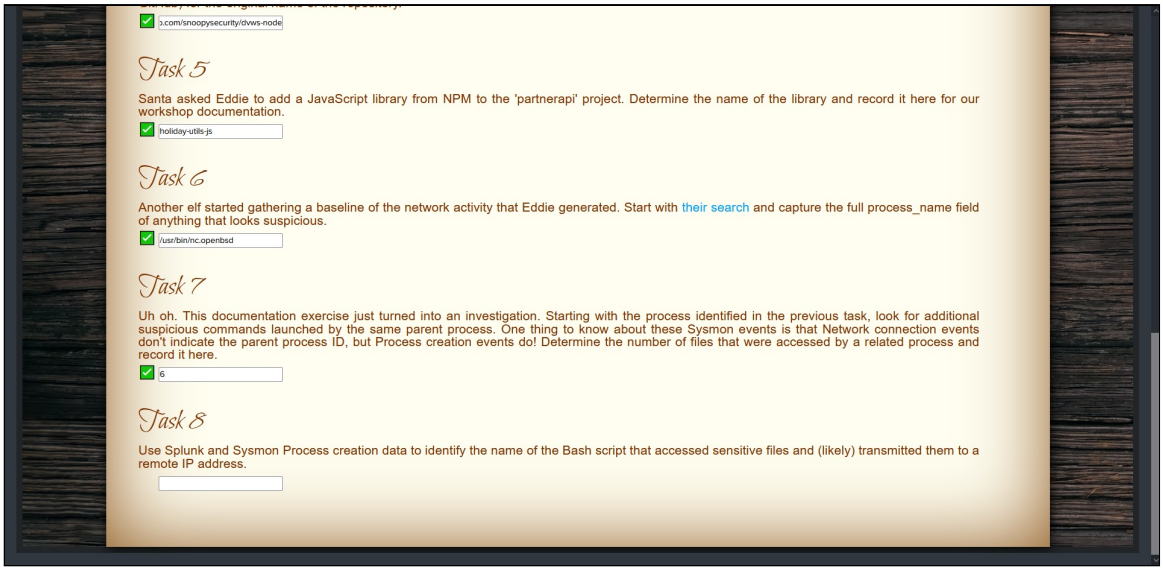


52. Click the Second tab and then click the Task 7 text-box

53. Type 6



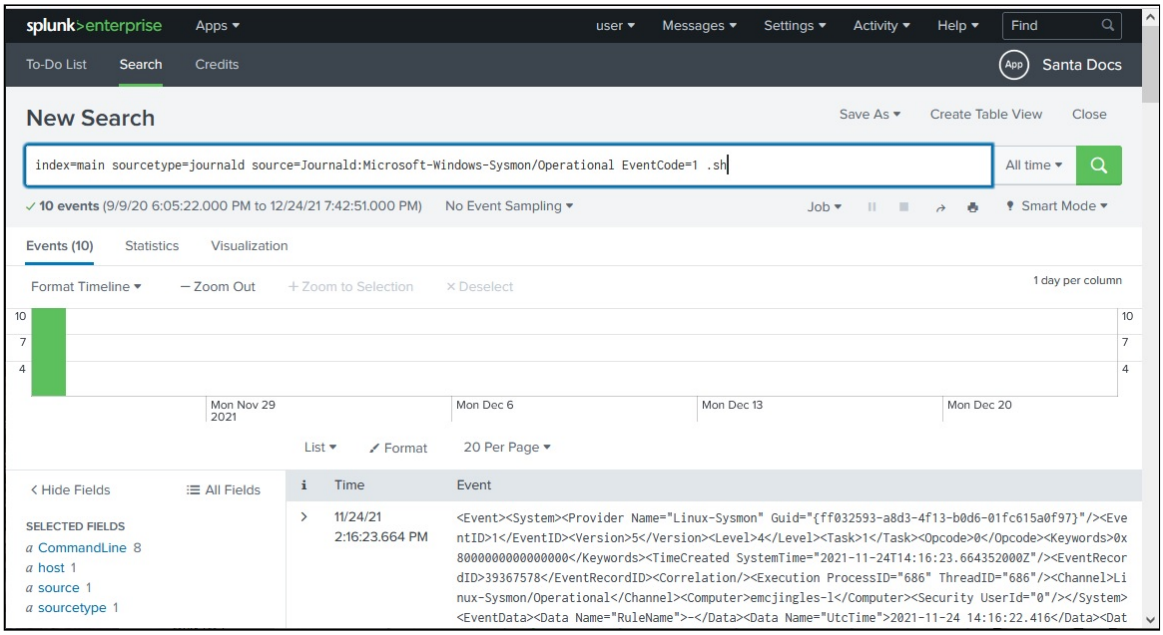
54. Click the `Close` button



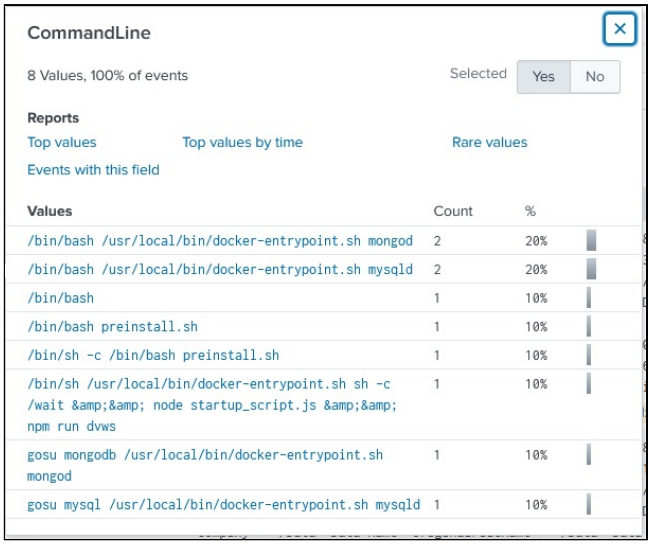
55. Click the `Third` tab

56. Modify the Search to `index=main sourcetype=journald source=Journald:Microsoft-Windows-Sysmon/Operational EventCode=1 .sh`

57. Click the `Search` button

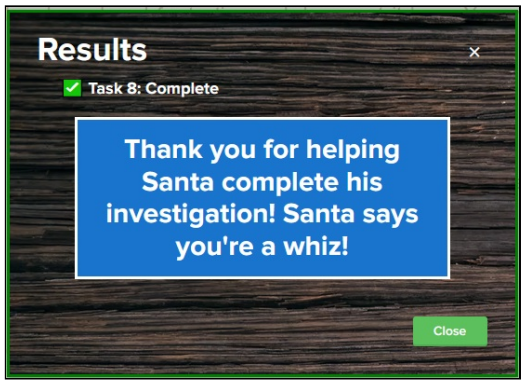


58. Click `CommandLine`

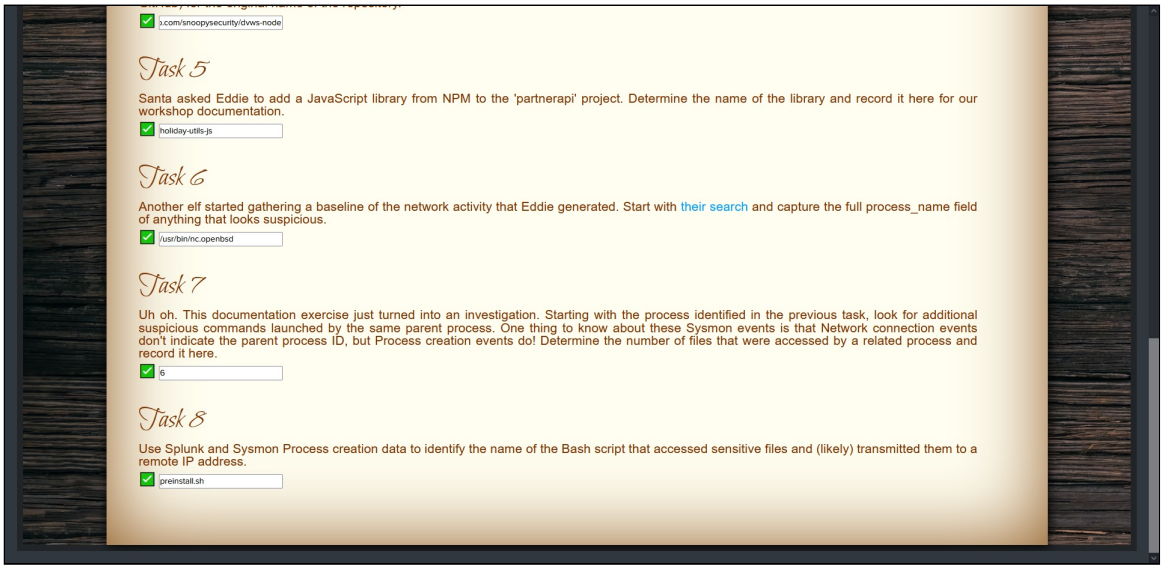


59. Close the `Third` tab

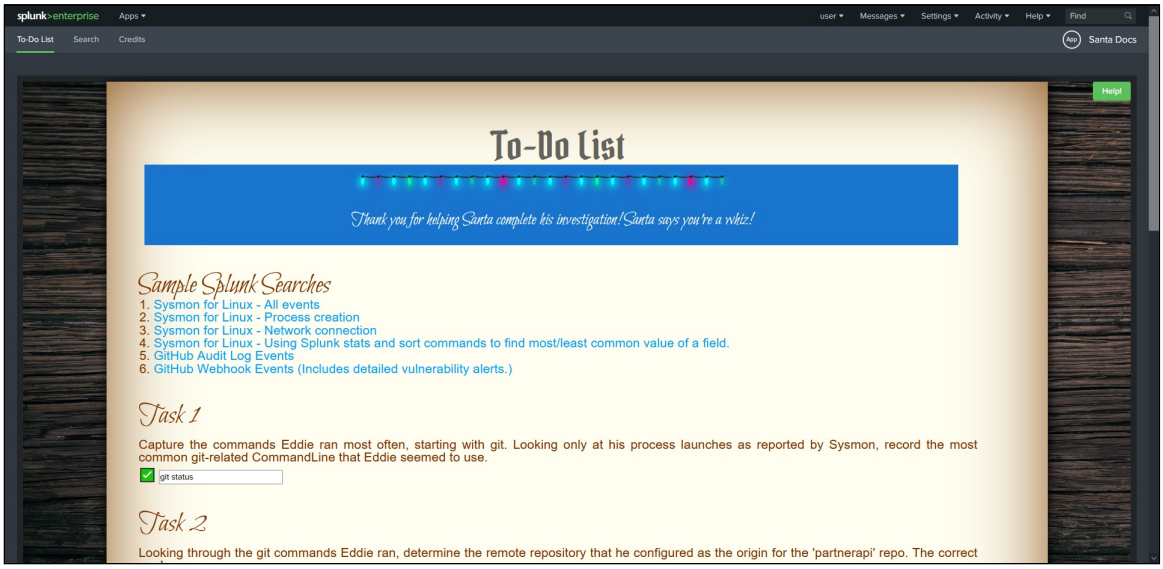
60. Type `preinstall.sh`



61. Click the `Close` button



62. Scroll to the `Top` of the window

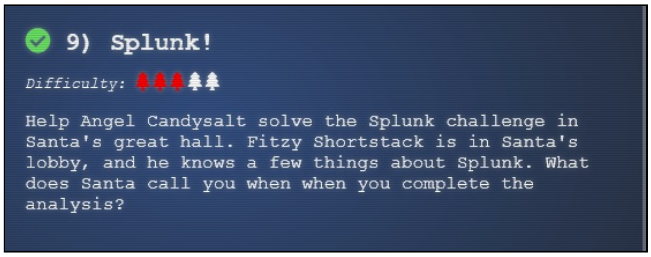


63. Close the `Second` tab

64. Click the `Tick` (Objectives) icon and then click `9) Splunk!`

65. Type `whiz`

66. Click the `Submit` button



67. Click `[Exit]`

68. Move `Left` to enter the `Kitchen`