**Report**

Saad 43973

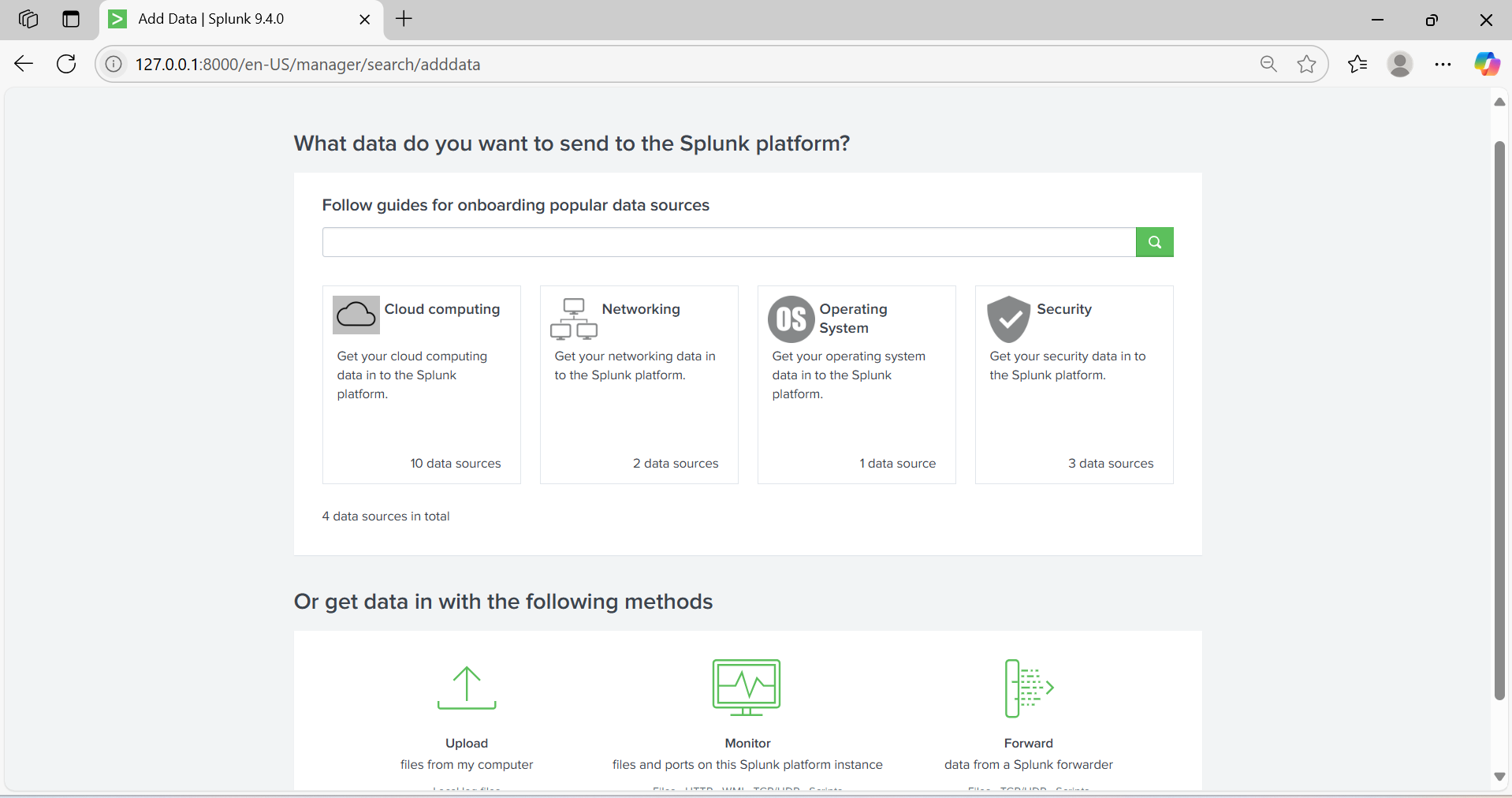
Investigation Report:

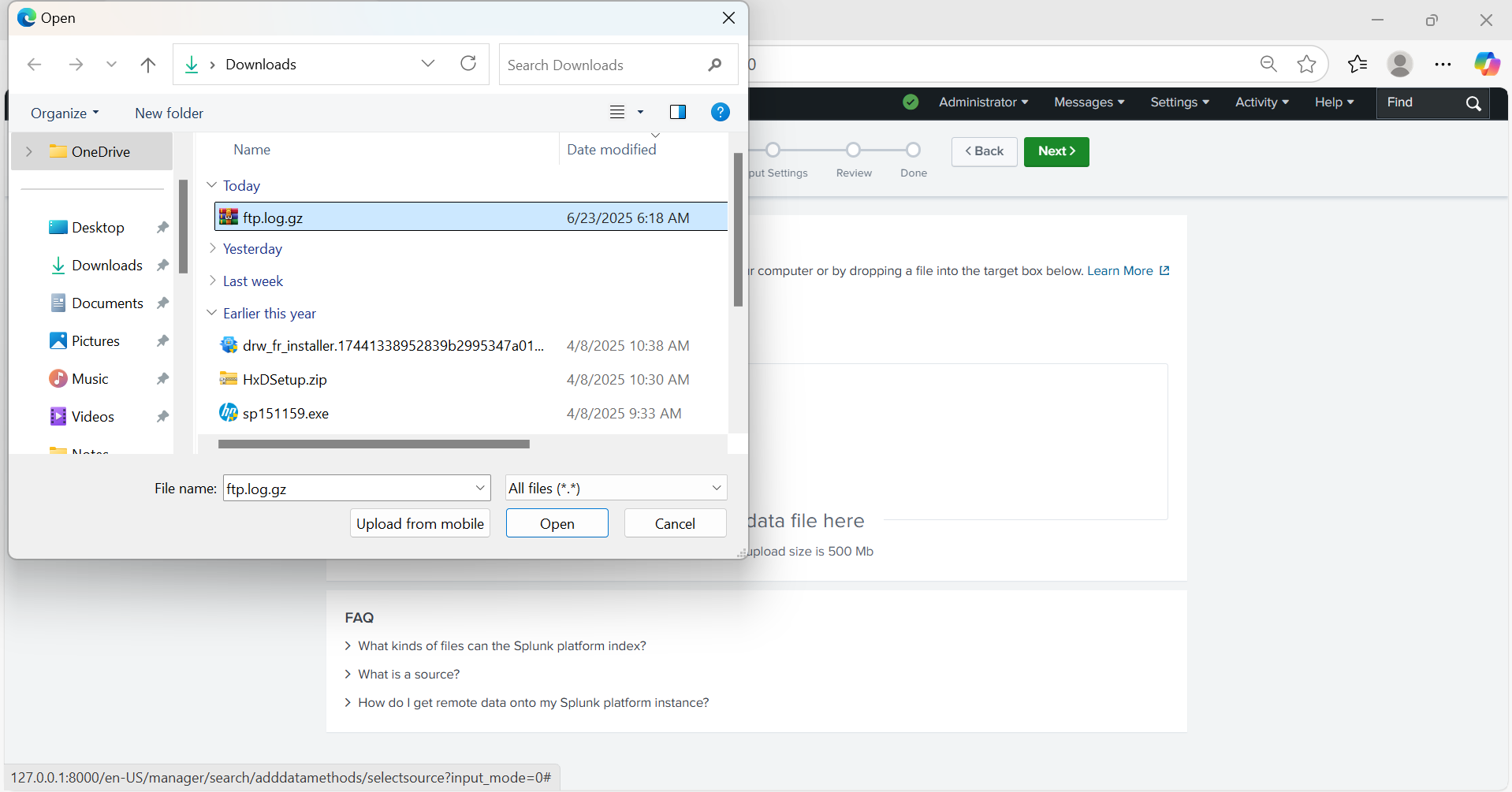
Unauthorized FTP Access Attempts on Host DESKTOP-JE26QMA

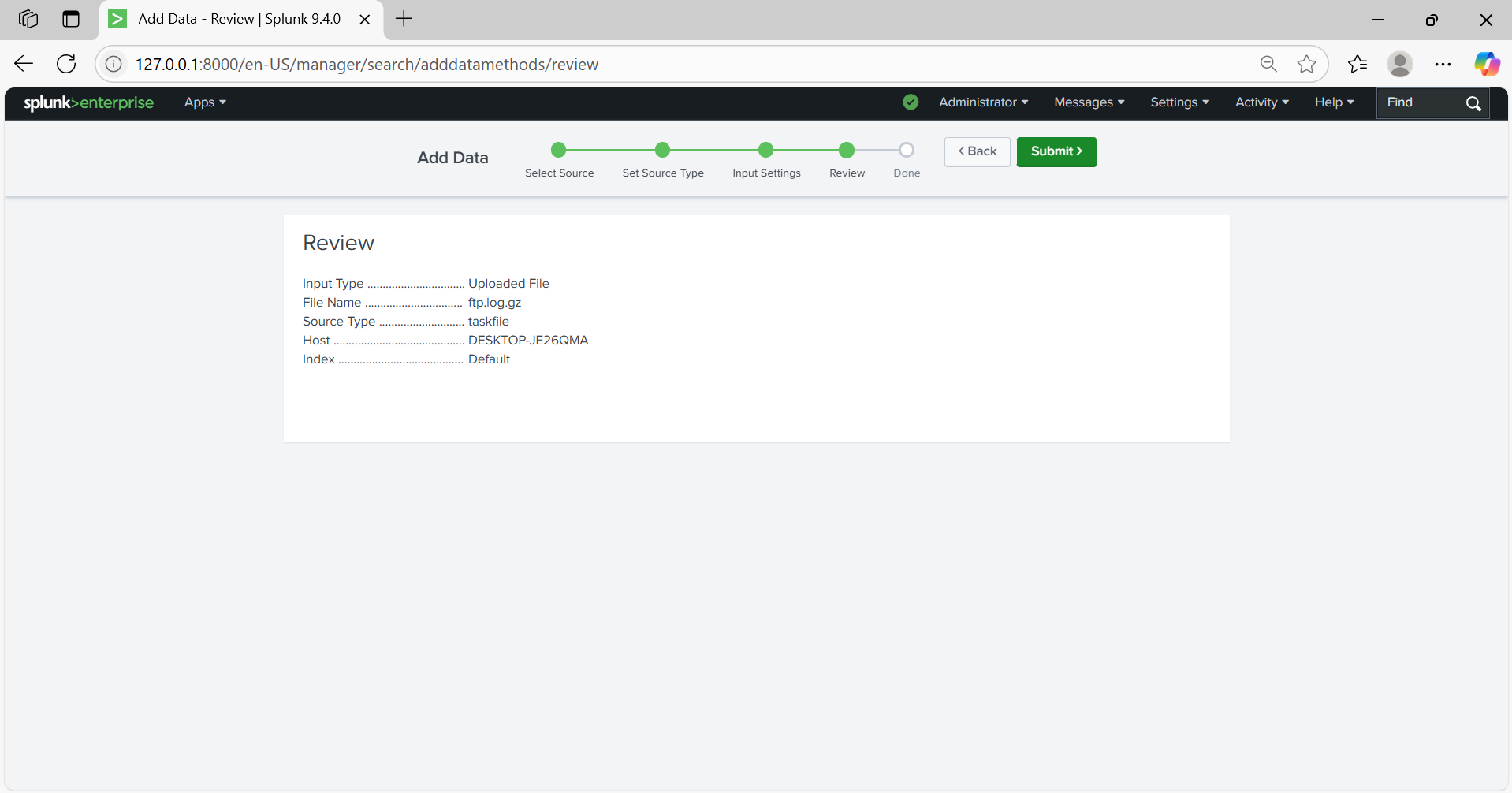
Date: 23rd June 2025

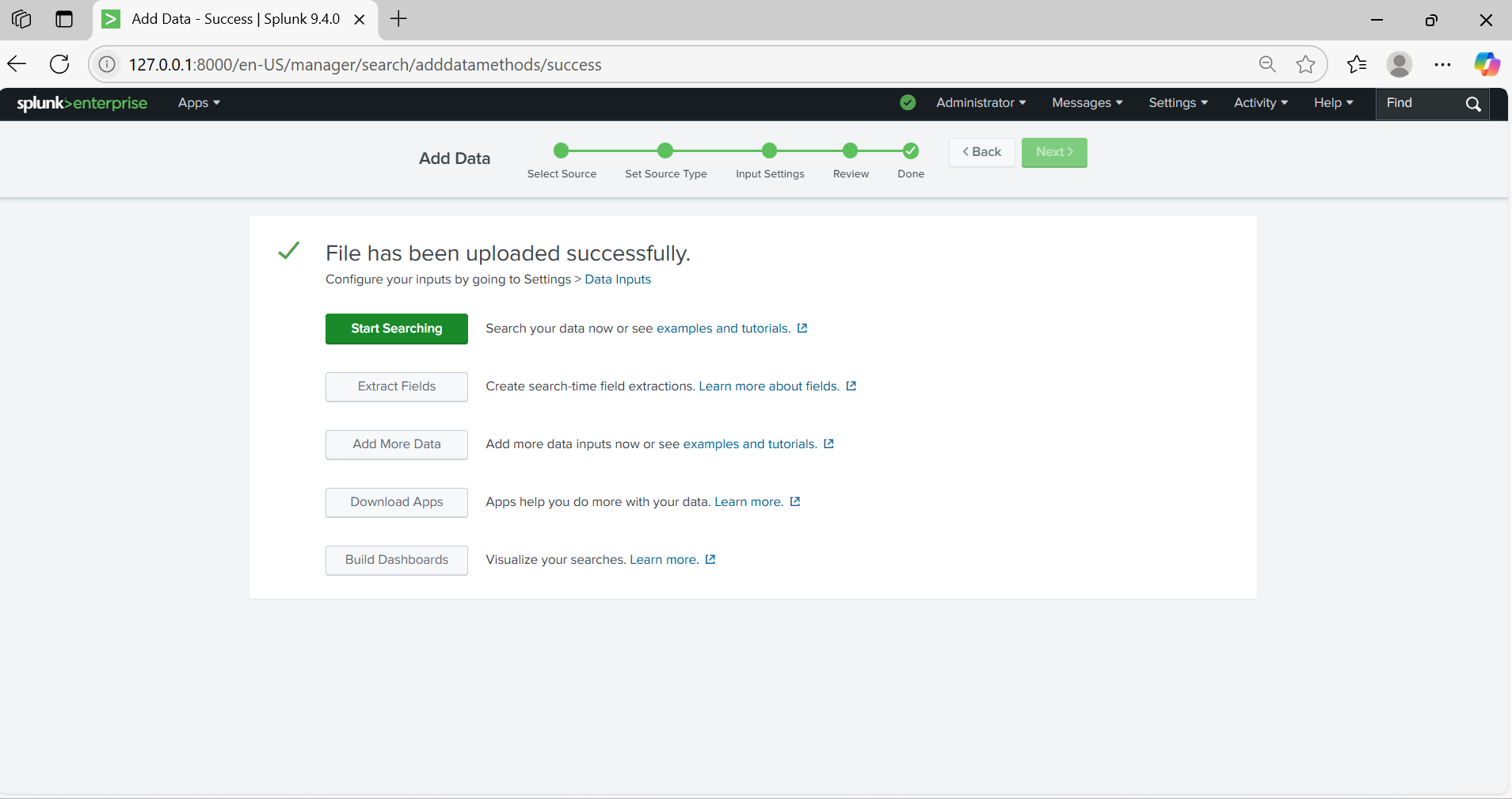
Follow Steps:

Open splunk and upload evidence file.

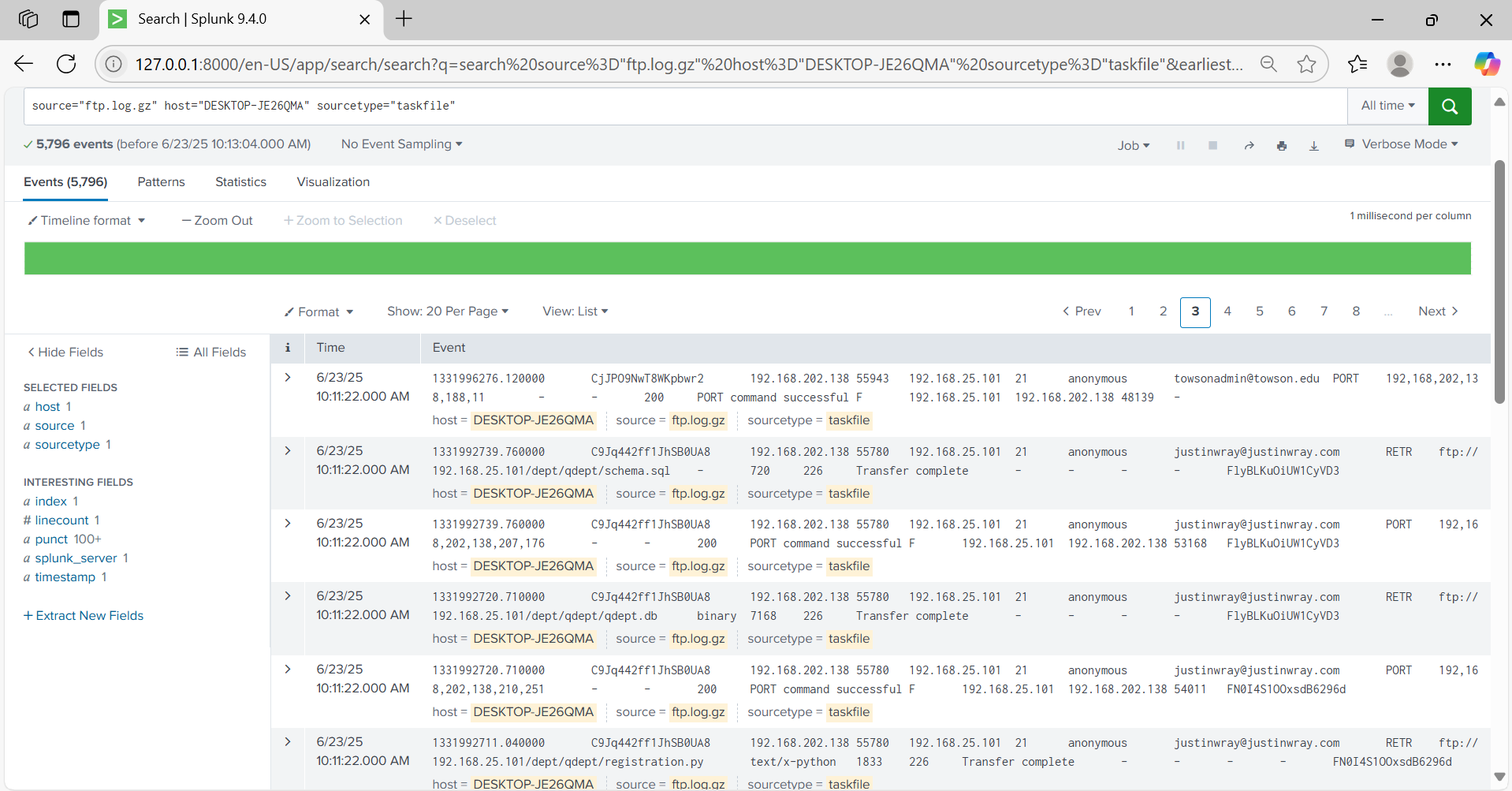


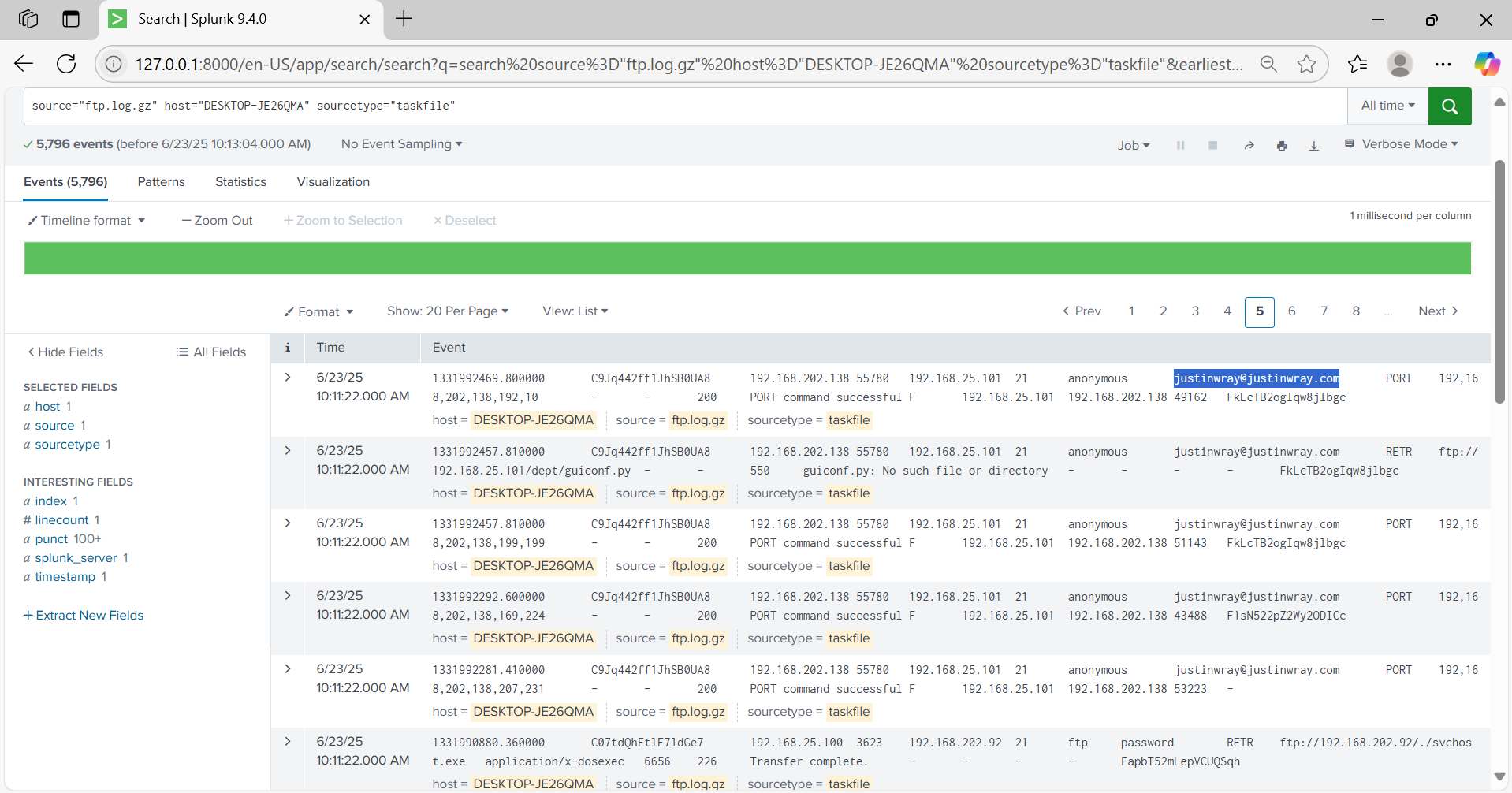


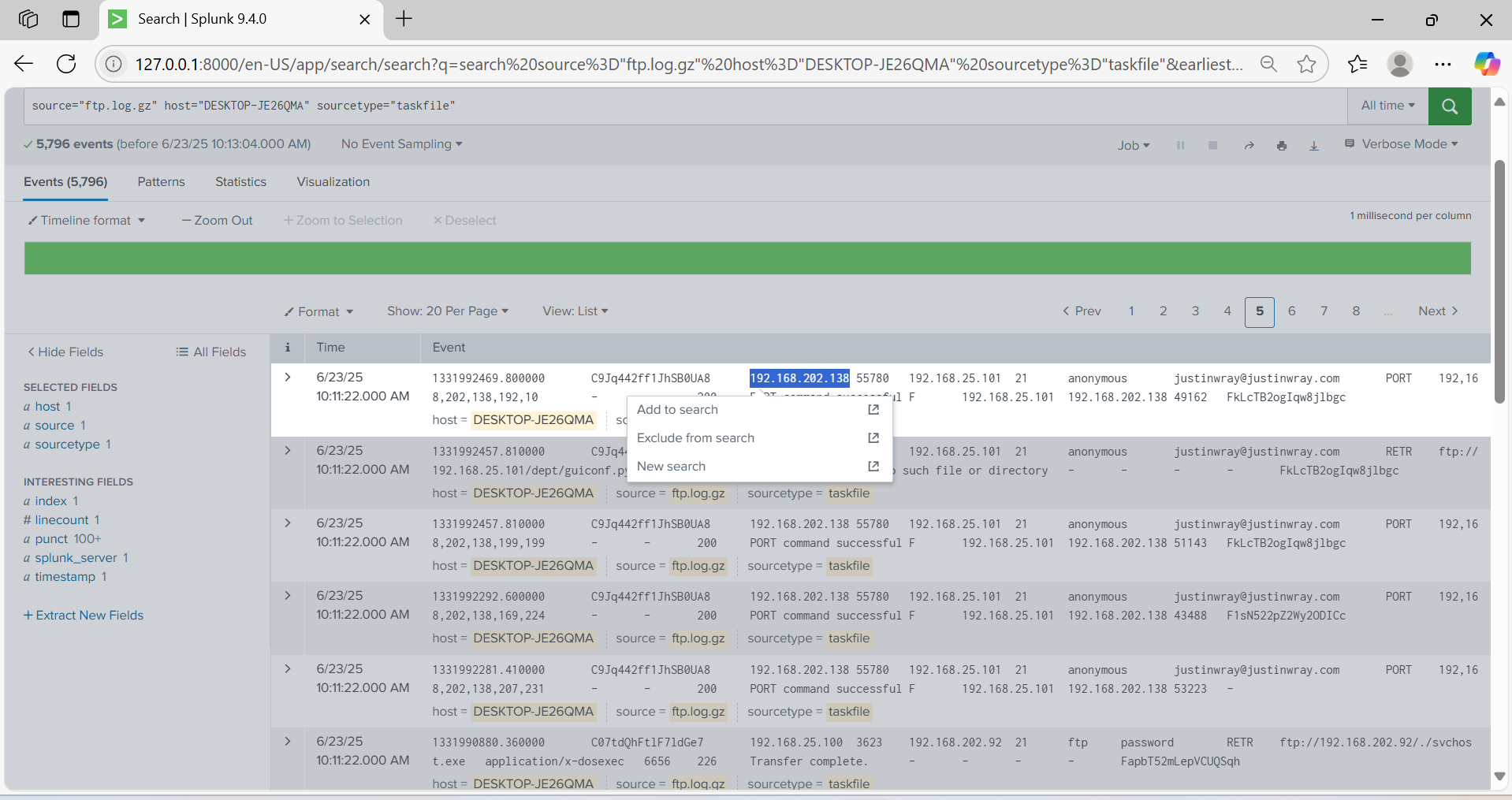




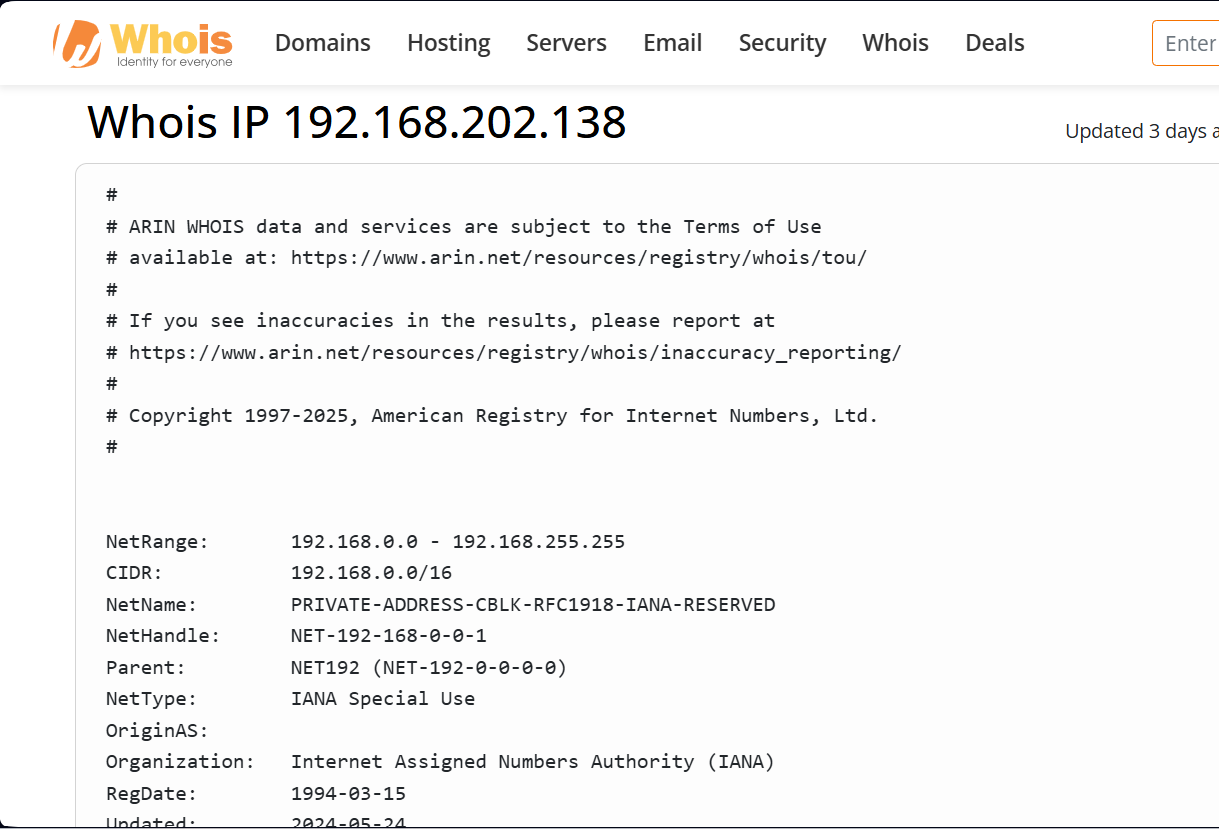
source="ftp.log.gz" host="DESKTOP-JE26QMA" sourcetype="taskfile"

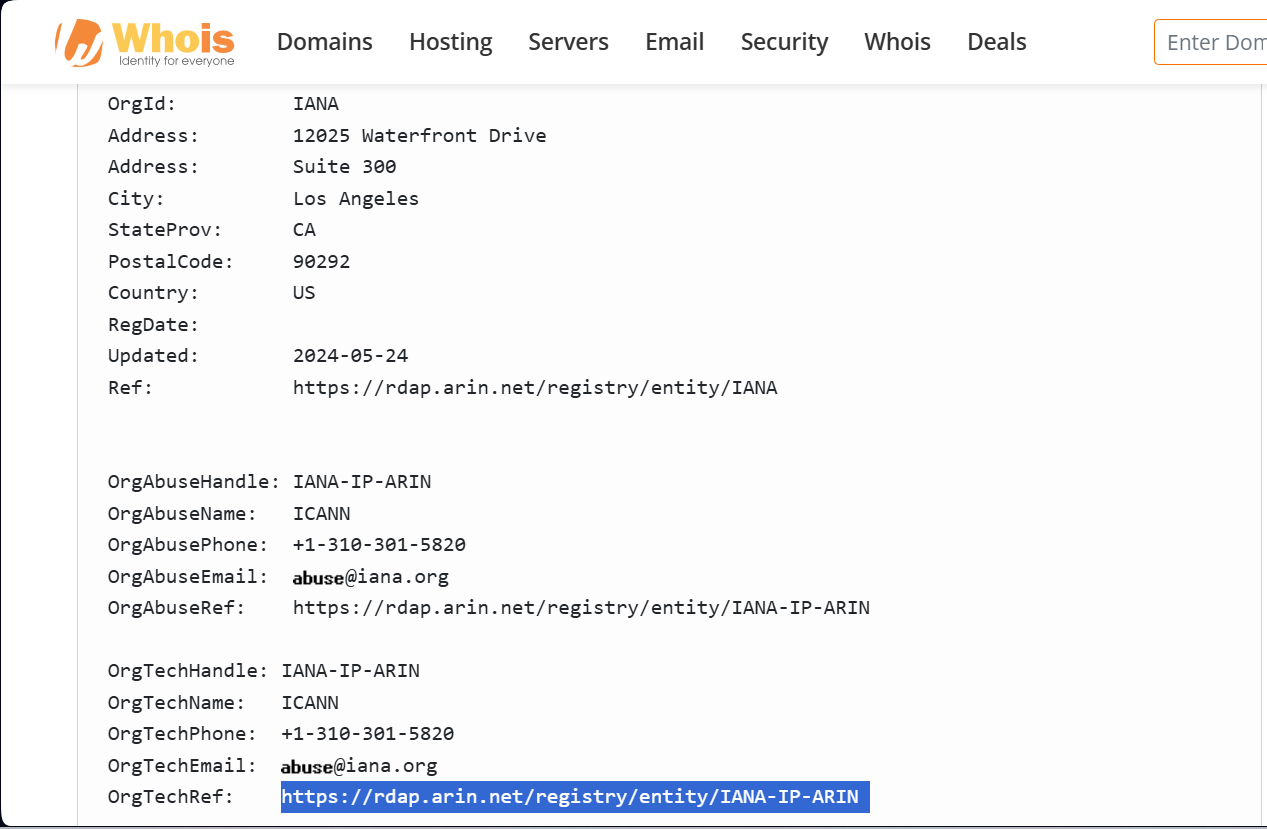






**Go to Whois Lookup and enter the IP address.**

****



**Summary:**

This report explains the investigation of FTP logs that were downloaded from a GitHub repository for analysis practice. Using Splunk 9.4.0, the goal was to find any unusual or suspicious activity in the logs.

During the analysis, we found several attempts to upload and delete files using fake or unauthorized usernames like password@example.com and anonymous. All of these actions failed because the system did not allow them. However, we also noticed some successful file transfers and commands involving files like vchost.exe, which can sometimes be used by malware. The use of passive and active FTP modes (PASV and PORT) also suggests that someone might have been trying to send or receive files in a hidden way.

**Key Observations:**

|  |  |
| --- | --- |
| Attribute | Details |
| Date | 23rd June 2025 |
| Time | 8:30:00 AM – 8:30:12 AM |
| Host | DESKTOP-JE26QMA |
| Log Source | ftp.log.gz |
| Sourcetype | task |
| Protocol | FTP (Port 21) |
| Usernames Used | password@example.com, anonymous |
| Commands Used | STOR, DELE, RETR, PORT, PASV |
| Activity Status | Some failed (Operation not permitted), some successful (Transfer complete) |

**Types of Suspicious FTP Behavior:**

#### A. ****Unauthorized File Actions****

* Multiple STOR (upload) and DELE (delete) commands were attempted using password@example.com.
* All these actions were **denied** (Operation not permitted), suggesting possible brute-force or enumeration.

#### B. ****Malware-like Behavior****

* Files executed like vchost.exe and /dosxec (suspicious binaries).
* Transfer commands (RETR) and use of passive mode PASV point to data exfiltration or malware command/control behavior.

#### C. ****Anonymous Access Attempts****

* Use of anonymous login with FTP is a red flag.
* Login attempts from 192.168.202.94 to internal host 192.168.25.101.

**Conclusion:**

This report confirms suspicious FTP activity indicating a potential security breach attempt. While some actions were blocked, others such as file retrieval and passive mode access were successful. This highlights the urgent need for response and tighter network security controls.