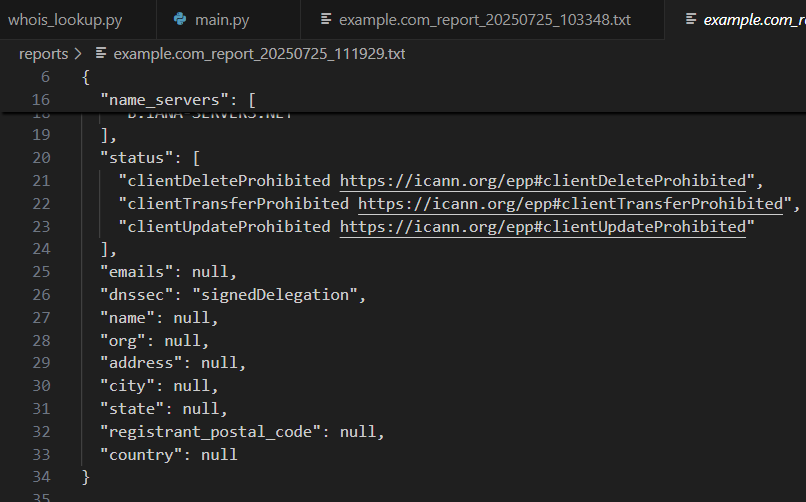


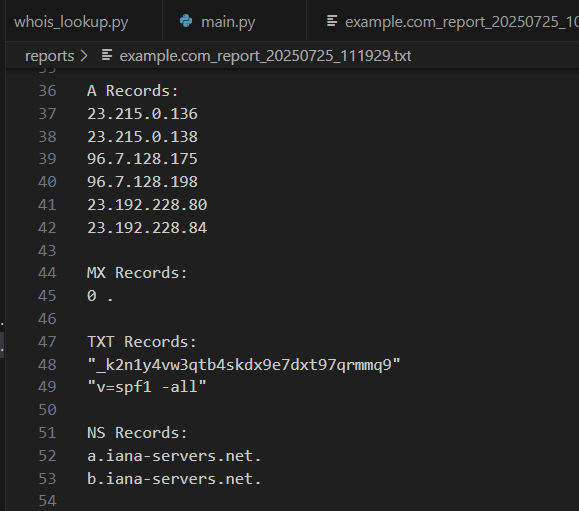
WHOIS is used in **passive recon** to know who owns the site, when it was made, registrar info, etc.

Report of Domain + Date & Time of Generation



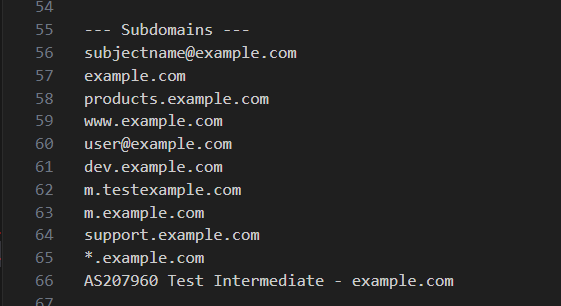
 Status flags (e.g., domain cannot be transferred or deleted)

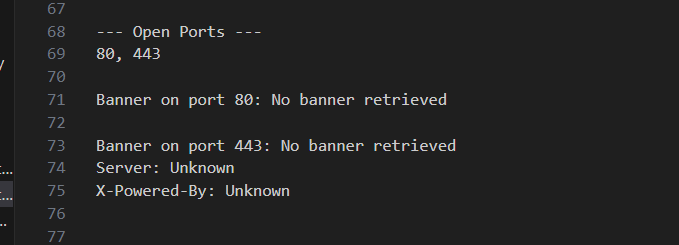
 Email and organization name if available



These records help understand how the domain is structured and which services are running.

| **Record Type** | **Description** |
| --- | --- |
| A Records | Maps domain to IPv4 address (server location) |
| MX Records | Mail Exchange servers (used for email delivery) |
| TXT Records | Text data like SPF (used for email security), verification keys |
| NS Records | Name servers that manage the domain’s DNS |





Identifies which ports on the server are open and potentially running services.

Open ports can be entry points into a server. This is part of ***active reconnaissance***.