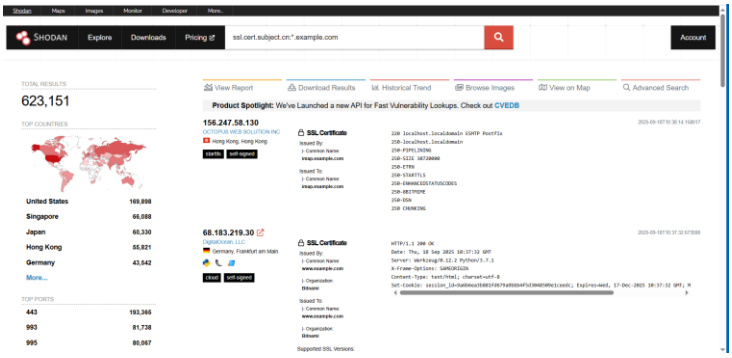
M1-A1: OSINT con Shodan y theHarvester

Objetivo: recolectar información pública sobre un dominio y analizar riesgos potenciales.

1. Accede a *Shodan.io*.
   - Realiza una query avanzada sobre un dominio de laboratorio (ej. `example.com`).
   - Ejemplo de query:

     ```
     ssl.cert.subject.cn:*.example.com
     ```

   - Identifica qué subdominios aparecen en los certificados SSL.



2. Ejecuta theHarvester sobre el mismo dominio:

   ```
   theHarvester -d example.com -b all -l 300 -f
   ```

   - Guarda el resultado en XML y JSON.
   - Anota correos y subdominios descubiertos.
3. Correlaciona los resultados de Shodan y theHarvester.

Entregar Informe breve (1–2 páginas) que incluya:

   - Capturas de pantalla de Shodan y theHarvester.
   - Lista de subdominios y correos encontrados.
   - Análisis: ¿qué servicios o usuarios parecen más expuestos?