**Footprinting**

## Alumno 1: Marco Batista Calado

## Alumno 2: Enrique González de Anleo Aliaga

**Definición:** es la técnica utilizada para recopilar información sobre los sistemas informáticos y las entidades a las que pertenecen. (Wikipedia)

La información a recopilar deberá estar abierta al público salvo que exista un acuerdo o contrato con la empresa objetivo a fin de poner a prueba su seguridad.

**Ejercicios:**

1. Buscar un contrato de Hacking Ético en inglés o español

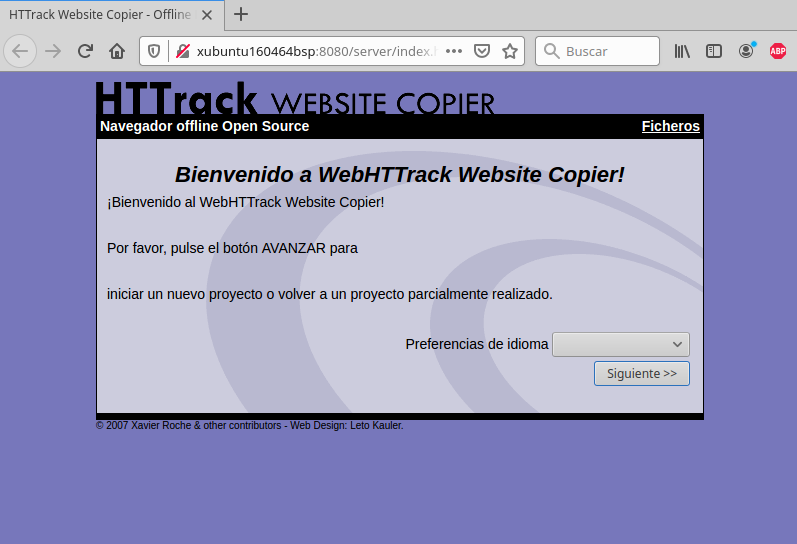
[***https://www.uslegalforms.com/forms/us-02478bg/ethical-hacking-agreement-for-external-network***](https://www.uslegalforms.com/forms/us-02478bg/ethical-hacking-agreement-for-external-network)

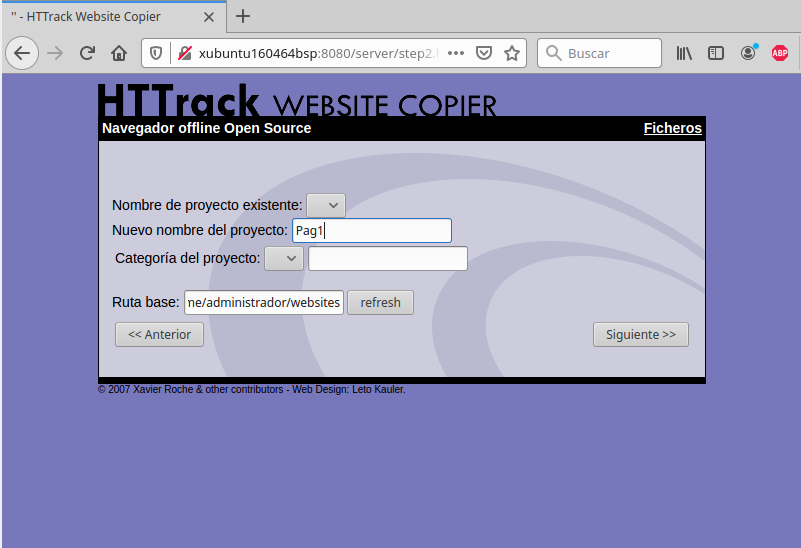
***A partir de Network Mapping, aparecen las cláusulas.***

2. Descargar un sitio web con la herramienta HTTrack y filtrar sus páginas web para encontrar URL’s o direcciones de email.

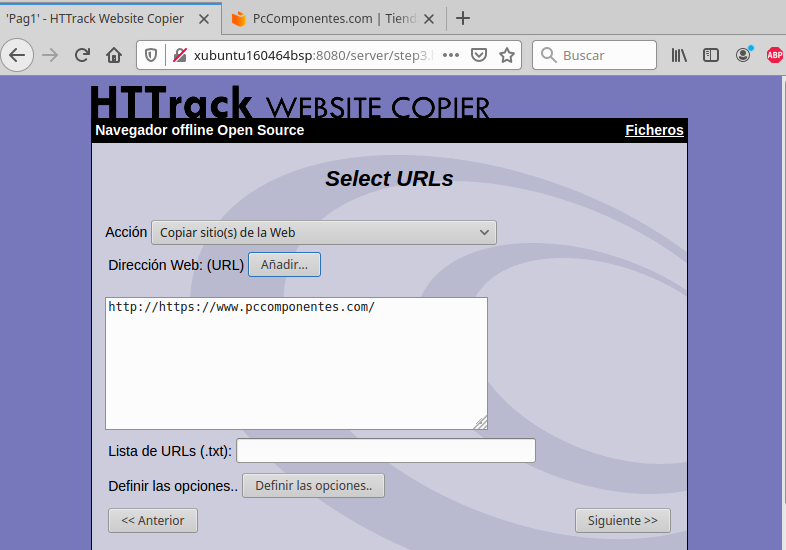
ej. http://www.webscantest.com

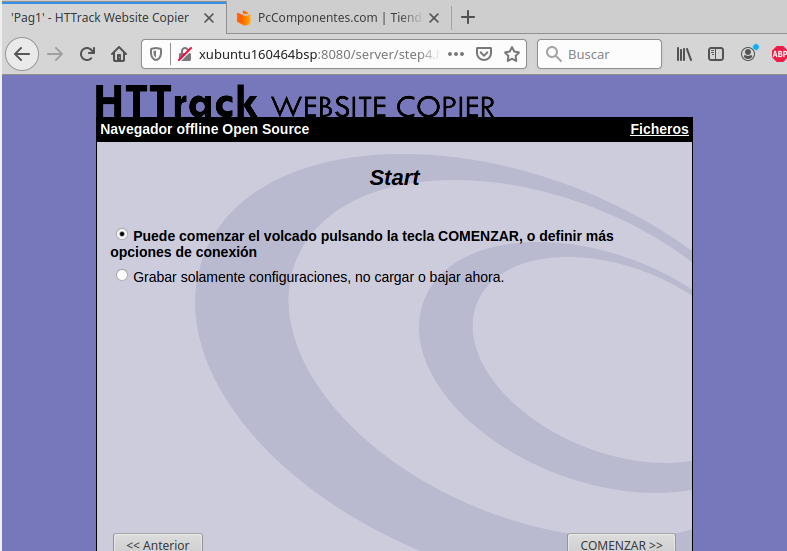
**sudo apt-get install webhttra**

**en ubuntu es por página aunque instale**

****

****

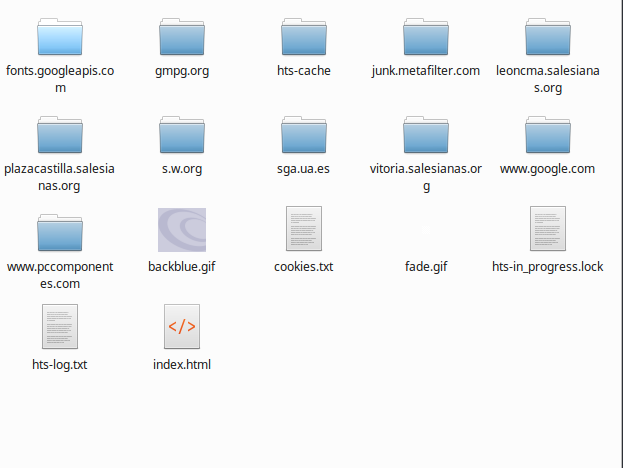
****

****

**Al final lo hicimos con la página del cole:**

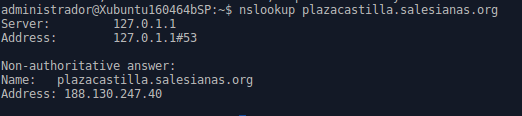
****

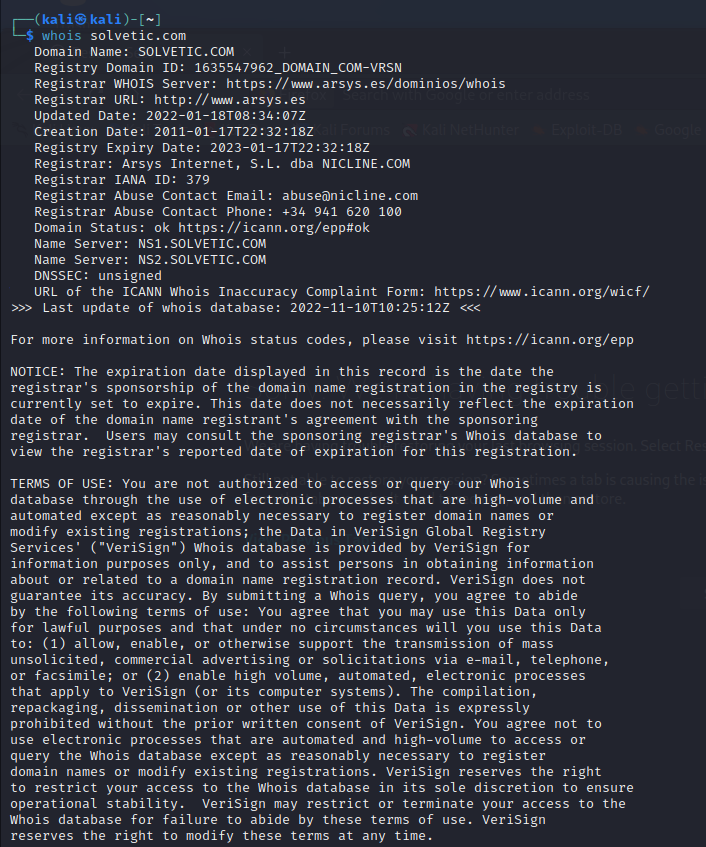
****

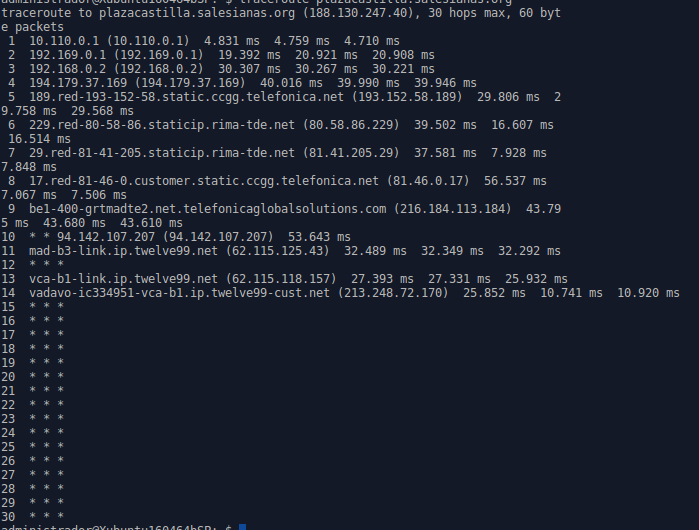
****

3. Conseguir las direcciones IP’s de una empresa y su localización mediante comandos, repositorios de información pública o herramientas gráficas.

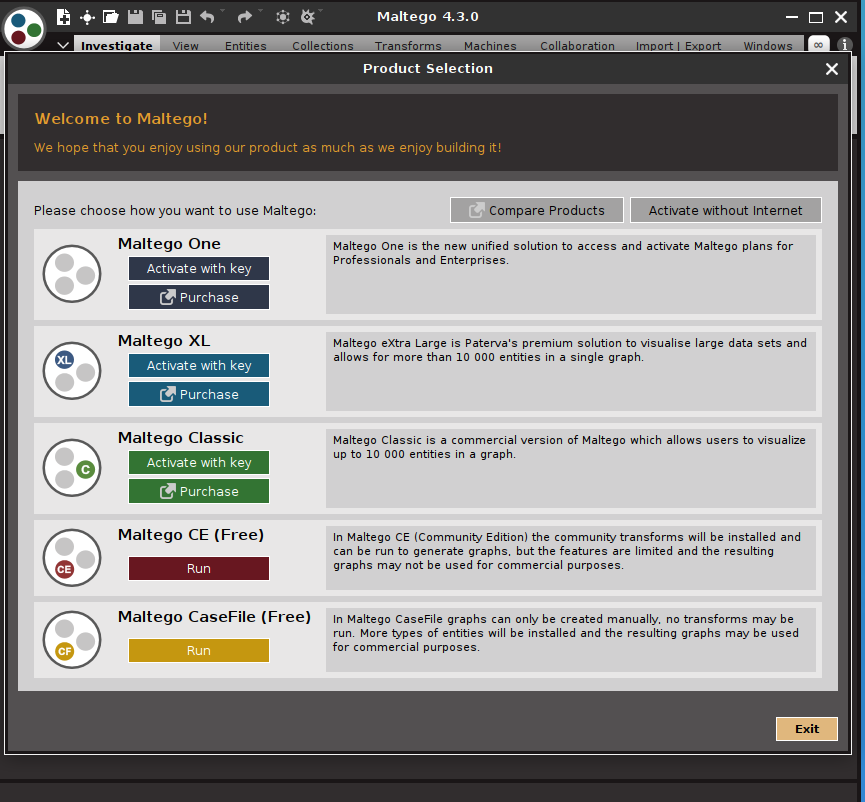
ej. nslookup, whois, http://ipv4info.com/, traceroute (<http://en.dnstools.ch/visual-traceroute.html>), <https://www.cual-es-mi-ip.net/geolocalizar-ip-mapa>

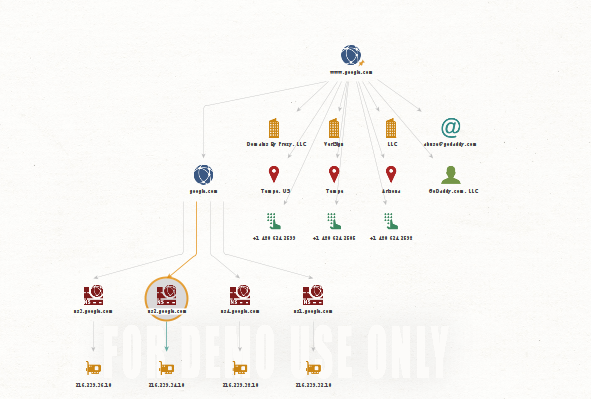






4. Footprinting con Maltego. Visualizar las direcciones IP del domino google.com







5. Rastrear un email hasta su origen, obtener la dirección IP del remitente consultando las cabeceras del correo.

ej. sender-ip, original-ip, originating-ip, …

