

3234



Google Dorking

Explaining how Search Engines work and leveraging them into finding hidden content!

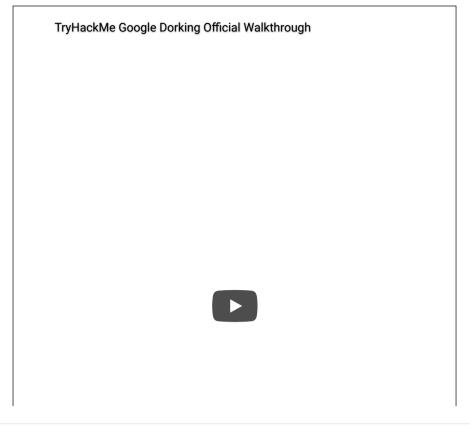


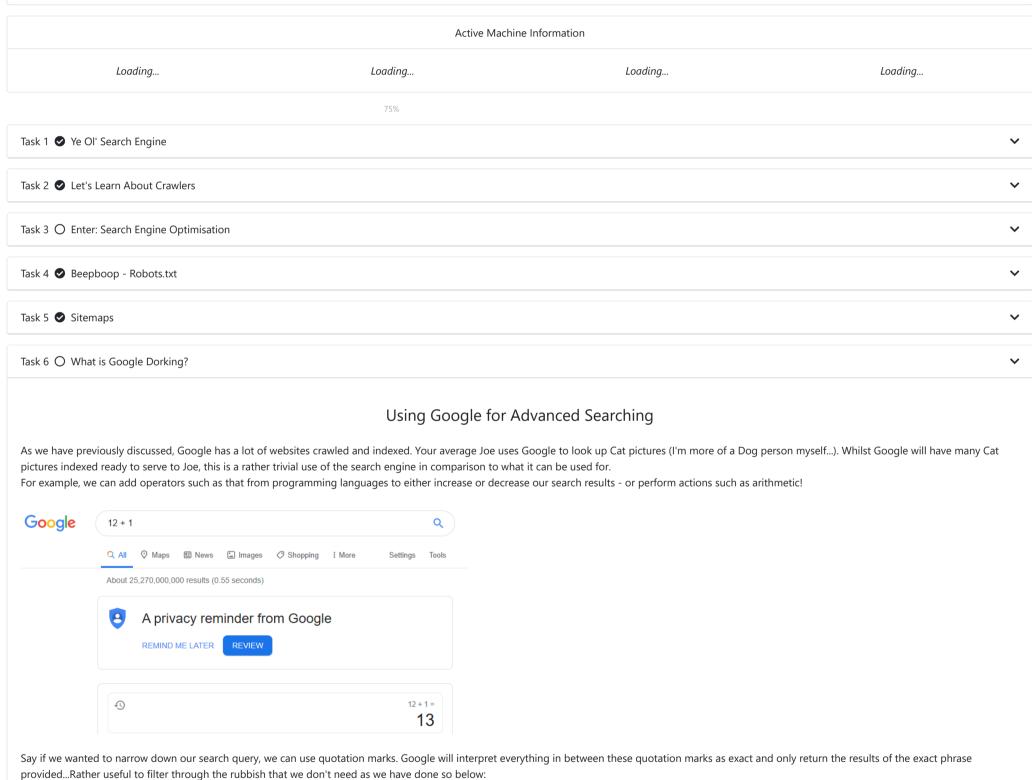
Start AttackBox

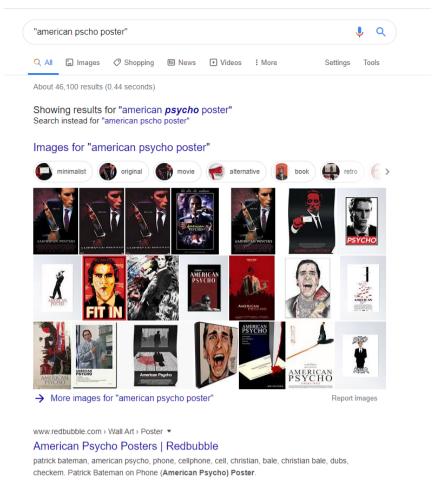
Show Split View

名 Cloud Details

Awards Help 🕸



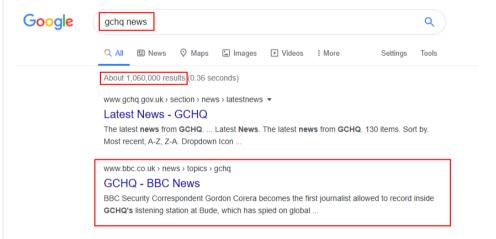




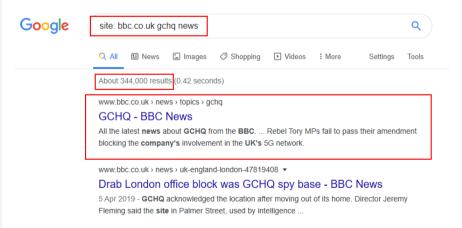
Refining our Queries

We can use terms such as "site" (such as bbc.co.uk) and a query (such as "gchq news") to search the specified site for the keyword we have provided to filter out content that may be harder to find otherwise. For example, using the "site" and "query" of "bbc" and "gchq", we have modified the order of which Google returns the results.

In the screenshot below, searching for "gchq news" returns approximately 1,060,000 results from Google. The website that we want is ranked behind GCHQ's actual website:



But we don't want that...We wanted "bbc.co.uk" first, so let's refine our search using the "site" term. Notice how in the screenshot below, Google returns with much fewer results? Additionally, the page that we didn't want has disappeared, leaving the site that we did actually want!



Of course, in this case, GCHQ is quite a topic of discussion - so there'll be a load of results regardless.

So What Makes "Google Dorking" so Appealing?

First of all - and the important part - it's legal! It's all indexed, publicly available information. However, what you do with this is where the question of legality comes in to play...

A few common terms we can search and combine include:

Term	Action
filetype:	Search for a file by its extension (e.g. PDF)
cache:	View Google's Cached version of a specified URL
intitle:	The specified phrase MUST appear in the title of the page

