From there, visual inspection is a good idea, **aquatone** (https://github.com/michenriksen/aquatone) is a great tool, however most people don't realise it will also accept endpoints and files, not just domains, so it's sometimes worth looking for everything and then passing it all into aquatone: cat domains-endpoints.txt | aquatone

To discover files and directories, **FFuF** (https://github.com/ffuf/ffuf) is by far the fastest and most customisable, it's worth reading all the documentation, however for basic usage: ffuf -ac -v -u https://domain/FUZZ -w wordlist.txt.

Wordlists – Every hacker needs a wordlist and luckily Daniel Miessler has provided us with "SecLists" (https://github.com/danielmiessler/SecLists/) which contains wordlists for every type of scanning you want to do. Grab a list and start scanning to see what you can find. As you continue your hunting you'll soon realize that building your own lists based on keywords found on the program can help aid you in your hunting. The Pentester.io team released "CommonSpeak" which is also extremely useful for generating new wordlists, found here: https://github.com/pentester-io/commonspeak. A detailed post on using this tool can be found at https://pentester.io/commonspeak-bigquery-wordlists/

Custom Tools – Hunters with years of experience typically create their own tools to do various tasks, for example have you checked out TomNomNom's GitHub for a collection of random yet useful hacking scripts? https://github.com/tomnomnom. I can't speak on behalf of every researcher but below are some custom tools I have created to aid me in my research. I will regularly create custom versions of these for each website i'm testing.

WaybackMachine scanner – This will scrape /robots.txt for all domains I provide and scrape as many years as possible. From here I will simply scan each endpoint found via BurpIntruder or FFuF and determine which endpoints are still alive. A public tool can be found here by @mhmdiaa – https://gist.github.com/mhmdiaa. I not only scan /robots.txt but also scrape the main homepage of each subdomain