Maltego

* According to a professional in this industry, this is the best tool available for this sort of work
* OSINT tool
* $999 for a year subscription [Maltego for Professional Investigators and Small Teams - Maltego](https://www.maltego.com/maltego-for-pro/)
* [Product Features - Maltego](https://www.maltego.com/product-features/)
* Trace IP addresses, ID networks and servers
* Graph and map making tools -- can put in tons of data points in an easy-to-read layout
* “Integrations reach from data for threat intelligence and network footprinting to social media and crypto forensics”
* Data sources: [Data at your fingertips - Maltego](https://www.maltego.com/transform-hub/)

Metasploit

* Pentesting tool
* There’s a free version
* Similar to Maltego in some capabilities
* Similar to Wireshark in ability to listen to incoming connections
* [Metasploit | Penetration Testing Software, Pen Testing Security | Metasploit](https://www.metasploit.com/)
* [Nightly Installers · rapid7/metasploit-framework Wiki · GitHub](https://github.com/rapid7/metasploit-framework/wiki/Nightly-Installers)

Harvester

* Open Source Hyper Converged Infrastructure Software
* Linux based, get email addresses, domain info, etc from the email sender
* [GitHub - rancher/harvester: Open source hyperconverged infrastructure (HCI) software](https://github.com/rancher/harvester)

Recon-ng

* open source recon tool
* Target specific data -- i.e. the sender’s email address; give a granular view of servers, emails, IP, lots of data
* Python
* [GitHub - lanmaster53/recon-ng: Open Source Intelligence gathering tool aimed at reducing the time spent harvesting information from open sources.](https://github.com/lanmaster53/recon-ng)
* [Recon-ng | Penetration Testing Tools (kali.org)](https://tools.kali.org/information-gathering/recon-ng)