

Automation & Recon Frameworks

Recon Frameworks

- [SpiderFoot](#) — Automated reconnaissance with 200+ modules
- [Recon-ng](#) — Open-source recon framework
- [Maltego](#) — Link analysis and visualization platform
- [theHarvester](#) — Harvest emails, hosts, subdomains
- [datasploit](#) — OSINT automation toolset

Browser Extensions and Utilities

- [Mitaka](#) — IOC investigation from the browser
- [Shodan Plugin](#) — Shodan search extension
- [Wappalyzer Extension](#) — Detect web technologies directly in browser

Emulators Android

- [Amiduos](#) - Android Emulator for Windows
- [Android x86](#) - Repo of Android VDI-images
- [Bluestacks](#) - Android App player for Windows & Mac
- [BigNox](#) - Another Android Emulator, lots of options
- [Genymotion](#) - Cloud bases Android devices

Metadata and Document Analysis

- [Metagoofil](#) — Metadata extraction from public documents
- [FOCA](#) — Document metadata collection and analysis
- [Bulk Extractor](#) — Forensic tool for extracting digital artifacts

Self-hosted and Modular Platforms

- [Cortex](#) — Observable analysis and enrichment framework
- [OpenCTI](#) — Threat intelligence platform with enrichment modules
- [IntelOwl](#) — API-driven threat intel and OSINT automation
- [Kali Linux](#) — Linux distribution with OSINT and recon tools included

From:

<https://wiki.fortier-family.com/> - **Warnaud's Wiki**

Permanent link:

https://wiki.fortier-family.com/cybersecurity/osint/docs_automation-recon

Last update: **2026/08/07 11:49**

