Law enforcement, financial institutions and corporations do not need to get their hands dirty by digging into the dark web to look for stolen or hidden data to locate digital fingerprints. This is a game-changer for companies concerned about advanced risk-management and will be useful for core investigation compliance.

**Introducing the ATII Darkweb Intelligence Platform**

**Project Hades**

**Delivering Darknet Secrets**

---

**We Do This**  →  **So That**  →  **You Can Do This**

- Scrape darweb sites for:
  - IP & Email Addresses
  - Keywords & Meta Tags
  - Etags, Favicon, Javascript
  - Google Analytics ID’s
  - SSH Keys, PGP Keys

- Monitor for Threats
- Filter & Pivot Through Queries
- Perform Risk & Link Analysis
- Map Out Organized Criminal Networks

Financial institutions can no longer ignore the links to financial crime on the darkweb. We would love to give you and your team a demo to show you its capabilities (which includes understanding your organization and your clients’ reputational risk on the dark-web).

Apply for a Demo & License

This is a game-changer for companies concerned about advanced risk-management and will be useful for core investigation compliance.
Hear what our digital data partners are saying about the Hades platform

“**We are incredibly proud to partner with and support the Anti-Human Trafficking Intelligence Initiative through their efforts in building tools and techniques for a cause which should be paramount to any organization in the cyber and crypto sphere. Their ability to timely extricate sensitive data from darknet markets such as IP addresses, usernames, e-mail addresses, and many other identifiers are oftentimes the crucial pieces of the puzzle critical to advancing investigations. There aren’t many players in this space who have dedicated themselves to this very important mission and we are incredibly grateful of their team who have made anti-human trafficking their life’s focus.**”

Shaun MaGruder
Founder & CEO at Blocktrace

“**The Attribution and Investigations teams at CipherTrace appreciate Project Hades vast array of indexed data from onion sites. The scraped onion site data provides the title of the sites as well as categories and keyword analysis. Investigations uses Project Hades data to identify crypto addresses which may be re-used i.e. multiple sites/scams using one BTC address. This provides CipherTrace with critical insights on relationships between entities and scam types, and any potential connections to CSAM/sexploitation.**”

Jonelle Still
Cryptocurrency Forensics Analyst at CipherTrace

Apply for a Demo & License

www.FollowMoneyFightSlavery.org