

Week 17 Workshop

TW: Due to the lack of monitoring done on the contents on the dark web, depending on the search queries you use in this session you may encounter disturbing sites, images or markets that may be distressing for some participants (not Brandon though, obviously)

Justifications for this topic:

- Monitoring for zero-day exploits
- Incident response to data-breeches
- Law-enforcement and cybercrime investigation

To Proceed

- If you don't have it already, install TOR on your personal laptops
 - You may need to hotspot from your phone
- Firstly, navigate to [Ahima.fi](https://ahima.fi)
- Try different search queries of illicit (but not abuse) material to get a feel for the sorts and the abundance of content that can be found in these spaces.
- Below I have attached a list of dark-web OSINT tools, I have not tested them because everything takes a fucking eternity to load through onion networks but I suggest each participant chooses a different tool and we all explore the depths together :)

<https://infosecwriteups.com/top-12-osint-tools-for-the-dark-web-cfcf88c8fbe0>