The National Cyber-Forensics and Training Alliance (NCFTA) is a U.S. based nonprofit corporation founded in 2002, with focused on identifying, mitigating, and neutralizing cyber crime threats globally. The NCFTA was intentionally created by industry, academia, and law enforcement for the sole purpose of establishing a neutral, trusted environment that enables two-way information sharing with the ultimate goal to identify, mitigate, disrupt, and neutralize cyber threats. Through the NCFTA, private industry and government are able to both physically and virtually work together in this neutral, trusted environment. As such, the NCFTA is one of the only non-governmental entities in the world that maintains such a unique relationship with both national and international law enforcement entities, and private sector companies.

The NCFTA is headquartered in Pittsburgh, PA, with branch offices in New York and Los Angeles. Each location has the following model: permanently embedded law enforcement, both national and international, and industry representatives sitting amongst NCFTA personnel in NCFTA controlled spaces. The purpose is to maximize information sharing and analytic support in a neutral, collaborative and trusted environment with the ultimate goal of supporting law enforcement in case development and threat attribution that leads to prosecution; while these cases are being developed, we also support industry in developing countermeasures and thus mitigating the ongoing threats posed by criminal actors.

Under contract, the NCFTA provides direct analytical services to law enforcement in support of criminal investigations and thus access to WHOIS information is invaluable (if not critical) in our support with helping law enforcement determine attribution, along with connecting seemingly disparate criminal activities to individual actors. Additionally, we work very closely (and confidentially) with brand and intellectual property protection programs within our various industry partners. These partners regularly see criminal activity, to include spoofing brand names in domain registration for the purpose of counterfeiting or brand protection hijacking, spoofing domains in targeted spear phishing attacks, etc. As such, most of our partners do not have the technical skill sets or manpower to identify each one of the domains and who the registrant is and thus rely on NCFTA analysts to help identifying the nefarious actors behind any criminal activity. Once we identify the actors and the activity they are conducting, we then connect our law enforcement and industry partners (victims) to help determine how best to proceed.

The NCFTA conducts our mission for the greater good and not for commercial purposes. We strictly adhere to not commercializing our work and every partner must adhere to a strict confidentiality and terms of use protocol.

The NCFTA has assisted with numerous large scale disruption activities against a well funded and determined criminal infrastructure. Most recently, in just the first quarter of 2018, our partnerships with industry and law enforcement have contributed to:

- $14,400,000 in law enforcement seizures
- 111 cases referred to or supported with law enforcement
- 14 arrests
- $74,328,496 in LOSS AVOIDANCE

For the period of 2015-2017, the impact has been even more impressive:

- $118,898,269 in law enforcement seizures
- 1,068 cases referred to or supported with law enforcement

- 489 arrests
- $1,669,893,849 in LOSS AVOIDANCE

This work for the greater good would not have been as productive and successful without NCFTA involvement and contributions through analytical research. A great deal of that research includes having access to domain registrants to support legitimate research and investigations. Prohibiting organizations like NCFTA from having legitimate access to this data would have a dramatic, negative impact on the cyber super heroes out there who are trying to protect our citizens and companies from those who have no other goal than to inflict harm, disrupt our social fabric, and exploit otherwise well intentioned protocols intended to promote “privacy”.