Friend or Foe?
How Anti-Digital Forensics vs. Digital Forensics Make or Break a Case

Nancy Scheidt
https://orcid.org/0000-0001-7653-1711
Independent Researcher, UK

EXECUTIVE SUMMARY

In this day and age, it is difficult to imagine technology not being part of our everyday life. However, such can also hold the power to be used for activities that an average consumer may not partake in. This chapter focuses on anti-digital forensics and digital forensics methods. Hence, it examines detection avoidance strategies and establishes current investigation and prevention methods when a crime is committed with the help of technologies within cyberspace, reaching from device forensics to data hiding. The cases of the San Bernardino shooting, hacktivist group 'Anonymous,' EncroChat, and the Shadowz Brotherhood are discussed, examining how offenders utilise technologies such as encryption and data wiping to try to 'outrun' authorities as well as methods authorities implement to keep up with technological advances to prevent and detect these criminal activities.

INTRODUCTION: DEFINITION AND STATE OF ART

Historically, technology can be defined rather broadly. In modern society people often connect the word 'technology' with mobile phones, computer as well as the internet, which is a logical verdict, however, 'technology' is more extensive than initially thought. Looking at the origins and the compounds of the term 'technology', the Greek

word ‘techne’ can be defined as art and craft whereas the Greek word ‘logos’ can be defined as word and speech. Having said that, if researchers are looking at this area from the point of view of applied science as well as the application of knowledge, the definition of technology transforms further into the understanding ‘of everyday used items’ which, as stated above, are often linked to internet connectable devices (Buchanan, 1998). These developments provided society with a rather new crime scene environment, the cyberspace, as well as devices which can be connected to it. Lippert & Cloutier (2021, p. 1) establish the cyberspace to be “a digital ecosystem, the next generation of Internet and network applications, promising a whole new world of distributed and open systems that can interact, self-organize, evolve, and adapt”. It is a network or platform which is made of a number of systems allowing to store, access and / or use data of any kind, at any time and from almost anywhere in the world. Clark (2010) established there to be four cyberspace layers to categories the different entities which use, create or are part of the cyberspace:

1. **Physical Layer**

The Physical Layer is the most commonly used and referred to cyberspace area by society. To provide real-life examples, this layer consists of a variety of digital devices such as PCs, smartphones, networks, wires and routers, to name a few.

2. **Logic Layer**

This Logic Layer refers to the world wide web. Hence, it is looking at the internet as a platform and components that provide a variety of services for different users as well as their interests. These include but are not limited to social media, content focused platforms as well as shopping platforms.

3. **Information Layer**

The focus of the Information Layer is the creation and distribution of any kind of data as well as the interactions between cyberspace users. Hence, this layer looks at a variety of material such as books, educational sources, videos, pictures, and documents which users can create, access as well as share with one another.

4. **Personal Layer**

The category of the Personal Layer refers to society, in particular individuals, who navigate in cyberspace for different reasons and purposes. More specifically