主題論文
© 臺大法學論叢 NTU Law Journal
第 52 卷特刊/Vol.52, Special Issue (11. 2023)

The Decryption of Encrypted Files in Criminal Procedure

Rong-Geng Li[*]

Abstract

Computers have become an integral and essential part of our daily lives. A huge amount of digital data is exchanged among devices and stored in various storage types. With this increased reliance on technology comes the growing concern for data security and privacy. In this digital age, where personal and sensitive information is constantly being transmitted and stored, it becomes imperative to protect this data from unauthorized access. One way to achieve this is through the use of encryption technology. Encryption is the process of converting plain text into a code to prevent unauthorized access. This technology is widely used to secure data, but unfortunately, it can also be exploited by criminals to hide illegal activities and information. This makes it even more challenging for law enforcement agencies to carry out criminal investigations. While encryption provides a certain level of security, it does not automatically grant individuals privacy rights. In fact, the use of probability theory is not a suitable explanation for privacy. Encrypted files should not be equated with locked containers such as rooms or suitcases. The contents of encrypted files may be visible, but their meaning may not be understandable. Decrypting encrypted files is similar to interpreting a conversation in a foreign language or searching bags with sniffer dogs. Moreover, encrypting files does not provide absolute privacy protection. Law enforcement agencies are allowed to decrypt encrypted files that have been legally obtained, without obtaining a warrant in advance. In conclusion,

[*] Professor of Law, National Taipei University.
E-mail: ronggengli@gmail.com

while encryption technology is an effective tool for securing data, it does not provide complete privacy protection. It is important for individuals to be aware of the limitations and to adopt a multi-layered approach to data security and privacy. This may include using encryption technology, implementing strong passwords, and regularly updating software to stay ahead of potential security threats.

Keywords: privacy, encryption, decryption, crack, reasonable expectation of privacy, search, warrant requirement