Chapter 8
Cryptopometry as a Methodology for Investigating Encrypted Material

Niall McGrath
University College Dublin, Ireland

Pavel Gladyshev
University College Dublin, Ireland

Joe Carthy
University College Dublin, Ireland

ABSTRACT

When encrypted material is discovered during a digital investigation and the investigator cannot decrypt the material then he or she is faced with the problem of how to determine the evidential value of the material. This research is proposing a methodology titled Cryptopometry. Cryptopometry extracts probative value from the encrypted file of a hybrid cryptosystem. Cryptopometry also incorporates a technique for locating the original plaintext file. Since child pornography (KP) images and terrorist related information (TI) are transmitted in encrypted formats, the digital investigator must ask the question Cui Bono?—who benefits or who is the recipient? By following Cryptopometry, the scope of the digital investigation can be extended to reveal the intended recipient. The derivation of the term Cryptopometry is also described and explained.

INTRODUCTION

Law enforcement agencies (LEA) encounter encryption in relation to the distribution of KP (Carter, 2007) and of TI (Shahda, 2007) offences. For example a KP distributor encrypts the KP material with PGP and posts it into a newsgroup or interest group via anonymous re-mailer or via an instant messenger system. The accomplice who is subscribed to that group receives encrypted material and can decrypt it. The anonymity of all involved parties is preserved and the content cannot be decrypted by bystanders. The use of PGP encryption in general has been cited (Sieg-

DOI: 10.4018/978-1-4666-1758-2.ch008

fried, Siedsma, Countryman, & Hosmer, 2004) as a major hurdle in these investigations. In addition, during digital investigations evidence is often discovered which extends the scope of the investigation. These are compelling reasons for the computer forensic investigator to be able to identify encrypted material, examine it and finally extract evidential value from it. This paper presents *Cryptopometry* which is a methodology that was experimentally formulated and it facilitates the identification of the recipient of PGP encrypted material. As an adjunct to this, a technique that identifies the plaintext file that was encrypted is presented. Subsequently a technical evaluation was carried out in a case study to validate the methodology. Following this, the performance and error-rate of *Cryptopometry* were evaluated through experimental means and finally the future work items are outlined.

1 RESEARCH CONTRIBUTION

The *Cryptopometry* methodology has been formulated for the investigation of encrypted material. This methodology extracts evidential value from the encrypted material to enable the identification of the recipient of the encrypted material. The incorporated search technique correlates the ciphertext file under investigation with the original plaintext file. The methodology has been validated and its performance has been evaluated to a high degree of success. In addition the error-rate of identifying the wrong file has been determined to be low. In general *Cryptopometry* reduces the investigation time by systematically carving the data under investigation into a significantly reduced file set. *Cryptopometry* is an entirely novel approach to investigating encrypted material and it is fully automated.

2 PROBLEM DESCRIPTION

The investigation of subject A is initiated and a forensic image of the hard disk drive (HDD) is taken. Analysis is carried out and it is found that there is a significant amount of ciphertext files and plaintext files containing evidence. Subject A is a suspected distributor/seller of KP and subject B whose identity is unknown is the recipient of the encrypted material. The objective of this research is to establish an evidential link between the encrypter and the recipient of PGP encrypted material and subsequently identify the plaintext file that was encrypted. In this scenario subject A must have had subject B's public key (PK_B) and PGP encrypted the plaintext material (M) to form the ciphertext (C_B). Subject B can decrypt the ciphertext when he receives it with his private key (PVK_B), please see Figure 1. PGP is a hybrid cryptosystem where the ciphertext created by it follows the OpenPGP message format specified in Callas et al. (2007). A hybrid cryptosystem is a combination of symmetric and asymmetric encryption. A symmetric key is session generated and then this is used to encrypt data. The symmetric key is then encrypted using the recipient's public key. The public key can be stored and distributed by a key server. The symmetrically encrypted data and the asymmetrically encrypted symmetric key are the major components of a PGP ciphertext data-packet. PGP also compresses data before encryption for added security because this helps remove redundancies and patterns that might facilitate cryptanalysis, compression is only applied to the symmetrically encrypted data-packet. PGP uses the Deflater (zip) algorithm for compression.

2.1 Methodology

The methodology which facilitates the investigation of PGP encryption is outlined in Figure 2 and consists of a number of steps that are described in the following sections. In order to carry out this research a framework of Java classes was created