Forensic Analysis of I2P Activities

Maxim Wilson
Department of Computing
Staffordshire University
Beaconside ST18 0AD, Stafford, UK
m.wilson@out-of-hours.it

Behnam Bazli
Department of Computing
Staffordshire University
College Road, Stoke-On-Trent ST4 2DE, UK
behnam.bazli@staffs.ac.uk

***Abstract* – file sharing applications that operate as form of peer-to-peer (P2P) networks have been popular amongst users and developers for their heterogeneity and easy deployments features. However, they have been used for illegal activities online. This brings new challenges to forensic investigations in detecting, retrieving and analysing the P2P applications. We investigate the characteristics of I2P network in order to outline the problems and methods in detection of I2P artefacts. Furthermore, we present new methods to detect the presence of I2P using forensically approved tools and reconstruct the history of I2P activity using artefacts left over by I2P router software.**

Keywords; P2P, I2P artefacts, Detection methods, Forensics Analysis, Security

I. INTRODUCTION

The self-organising overlay networks that are distributed on IP networks are called P2P networks. P2P file-sharing networks reflect the Internet of Things (IoT) paradigm with autonomous networked devices within distributed and decentralised systems. P2P networks are managed by protocols implemented at the application level. They are implemented on top of the User Datagram Protocol (UDP) or Transmission Control Protocol (TCP). Furthermore, P2P overlays provide support for scalability within dynamic and decentralised systems. The nodes within a P2P system act in a self-managing manner in contrast to the client-server model. Such overlay networks go beyond the services offered by conventional client-server systems [1]. P2P systems are popular and pervasive, and largely used for file sharing and data communication.

While the rapid growth and ubiquitous use of file sharing applications is generally positive for users, they introduce many challenges in forensic investigations. The dynamic change of membership, the geopolitical stance on copyright materials, legal and ethical issues in dealing with file sharing applications are some examples to include. However, the most challenging issue is overcoming the misuses provoked by capabilities of P2P network. Many law enforcement agencies struggle to keep up with the new tools and techniques which are misused by P2P users, who contribute to and facilitate illegal activities online.

In this work we examine the characteristics of I2P networks or related applications which attract illegal activities and may pose a problem for the forensic analyst. Furthermore, we propose a number of alternative approaches to identify or reconstruct the suspect's activity on I2P network and analyse the remaining artefacts using a mix of custom made and industry approved forensic tools.

The rest of the paper is organised in the following structure; Section two introduces the I2P network, its current developments and the challenges it presents in forensic investigations. Section three outlines solution design and description of forensic procedures in I2P investigations. Section four includes related works and section five provides discussion and future direction of the research.

II. Network Overlay

Network overlay provides support for scalability within a dynamic and decentralised system with self-managing nodes. This means they can take advantage of the available resources, content and traffic stability independent of central servers. Nodes have dual client and server roles, meaning they can both initiate and listen for incoming connections.

A. P2P Networks

A network overlay is a solution to address scalability issues within distributed systems. It is a virtual network of nodes and logical links built on top of the existing network. It can therefore be used to deliver additional services and functionalities which are not offered by the base network. Since overlay network avoids direct interaction with underlying infrastructure, it can be easily deployed without costly upgrades or interruptions to the base network services. Furthermore, it does not require modification of existing software or protocols in order for new nodes to join the overlay network.

A P2P overlay provides support for scalability within a dynamic and decentralised system with self-managing nodes. This means all nodes contribute to and benefit from shared pool of network resources and content, without being reliant on any central server.

There are many P2P networks with diverse properties classified based on different methods such as performance metrics, topology, protocol and structure [4]. P2P overlays are popular amongst users for file sharing and communication such as Skype, BitTorrent and Freenet. Each class of the system has its own advantages and disadvantages, but we will focus on P2P overlays that offer some degree of anonymity to their users. Anonymity is the main attribute that provides user privacy. But this feature is for incriminating activities from sharing copyrighted materials and cybercrimes to illegal transactions.

B. I2P Network

I2P (Invisible Internet Project) is an adaptation of Kademlia [3] developed to go a step further than just anonymity and enables users to access an isolated '*darknet'*. I2P provides P2P communication channel along with various protocols and encryption standards to maintain user anonymity. The end-to-

end communication between two users is not globally advertised and fully encrypted. I2P improves on standard TCP/IP communication model by ensuring that IP (Internet Protocol) packets exchanged between participating hosts always contain encrypted data. Instead of relying on IP addresses to uniquely identify hosts and route traffic, I2P introduces its own identifiers and routing logic at higher layer of the protocol stack. As long as Layer 4 network connectivity exists between hosts, I2P is able to operate in complete isolation from the rest of the public Internet infrastructure. These improvements aim to improve anonymity of network users by reducing the risk of malicious third party (such as a compromised Internet service provider) intercepting or altering the network traffic.

a. *I2P Routers*

I2P nodes communicate through a set of peer-to-peer tunnels facilitated by I2P router software. The nodes follow "garlic" routing logic, which requires use of separate tunnels for inbound and outbound traffic. Every transmitted message is relayed through chain of third-party I2P routers many times hiding the user identity completely. The communication between peers has no defined exit point from I2P to normal Internet, therefore avoiding issues seen within similar systems like Tor [6].

b. *I2PSnark*

I2PSnark is the default torrent client for I2P network and is distributed as part of I2P router software. As a native I2P application, I2PSnark cannot understand IP addresses and is therefore unable to communicate over normal Internet. This limitation is intentional and ensures that no personally identifying P2P traffic can leak outside of encrypted I2P tunnel. Security and ease of use ensure continued popularity of I2PSnark with I2P network users. I2PSnark user base is larger than that of all other I2P torrent clients combined, with I2PSnark being responsible for one-third of total I2P network traffic [5].

P2P (BitTorrent) clients operating over normal Internet provide any member of the torrent swarm with information about all other peers. Forensic examiner can therefore obtain torrent creator's IP address, which may then be checked via Internet Service Provider to determine the identity of illegal filesharer. Applying this method to I2PSnark yields only a list of peers' I2P network identifiers, which have no forensic value.

c. *Domain name resolution*

The I2P project considers public Internet DNS (Domain Name Service) infrastructure to be unsuitable for use in anonymizing distributed overlay network. Internet's DNS is seen as highly hierarchical structure, susceptible to both technical failure and takeover of domain names by malicious third parties. For these reasons, I2P network implements its own system for resolving short, human-readable domain names.

As part of this system, every node in I2P network is expected to keep a local *"addressbook"*. The *addressbook* is a file which stores associations between an I2P domain name and I2P network identifier (instead of IP address). The concept is similar to use of hosts file by nodes of early Internet before the invention of DNS.

To reduce the need for manual editing of hosts file, I2P implements a name record update mechanism known as "subscriptions". I2P node user can specify several other nodes on the I2P network to be "subscription sources", which will then be regularly polled for their copies of the addressbook. Any entries for domain names which are not present in the subscribed node addressbook are merged with current copy.

The aim of described I2P system is to keep all information required for resolving domain names within secure I2P network, preferably on the local I2P node. Therefore, a forensic analyst who manages to obtain name resolution query logs from I2P user's Internet Service Provider or DNS caching server on local network is unlikely to find any entries related to I2P.

d. *Darknets (eepsites)*

I2P uses its own domain name service which enables the existence of '*eepsites'*, hidden websites that can only be accessed by users connected to I2P overlay network. Eepsites are hosted directly on I2P nodes and are accessed via names ending in '*.i2p'* top-level domain as shown in Fig 1.

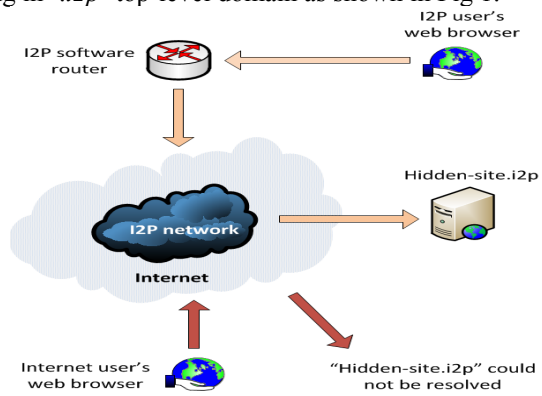

Fig 1. Eepsites Cannot be Accessed from Normal Internet

Within an investigation of a normal Internet website, the domain registration records and copy of DNS zone file can provide several key pieces of forensically valuable information. These include contact details of the registrar, personal details of the domain owner and *resource records* providing IP addresses of the host. In this way, the identity of the website owner can be identified and the host device seized for further investigation by the forensic analyst.

This method is not effective against I2P eepsites. Normal Internet registrars are part of DNS hierarchy and therefore encouraged to cooperate with law enforcements under the Internet Corporation for Assigned Names and Numbers (ICANN) scheme. I2P domain name registrars are anonymous, have no governing body and incur no penalty for ignoring laws, regulations or requests from law enforcement agencies. The process of eepsite name registration further

ensures that no personal information or IP addresses are stored by registrar.

The lack of access to hidden eepsites from Internet makes them invisible to Wayback Machine and search engine caches. These are frequently relied on by forensic analysts to prove the content of suspect website at certain point in time. Eepsites therefore are less consistent as evidence compared to normal websites because no backup copy of an *eepsite* can be located if it is shut down by its owner.

e. Discovering an I2P installation

The possible misuses of I2P network are less known among law enforcement agencies and forensic analysts. This may lead to I2P installation on seized machine not being discovered or not recognized as source of valuable forensic artefacts.

The industry approved software such as EnCase and FTK has no analysis or detection functionality for I2P. As such they do not provide any insight into data left over by I2P software.

I2P can be installed in one of the two modes on a Windows machine; either as an application or as a system service. The system service installations of I2P have more value to forensic analyst. This is due to the fact that I2P installation as service is preferred by users who require permanent connection to I2P network - for hosting of *eepsite*s or sharing content. However, I2P installed as a system service is harder to discover due to lack of entries in Start Menu, Desktop and Most Recently Used (MRU) software lists.

III. Forensic analysis of I2P

I2P router software focuses strongly on security of network traffic rather than the data stored locally on participating I2P nodes. As a result, the local data is stored without encryption and can be of use to forensic analyst investigating a seized device. We conducted the following experiments in order to forensically evaluate the I2P network and assess how it can be used for illegal activities. Furthermore, we highlight how the functionalities and flaws within the network should be considered in forensic investigations.

a. Investigation of I2P installers

I2P installers for Windows family of operating systems contain several layers. The outer layer is a self-extracting archive of 7-Zip format, used to distribute the installer components in a single file and reduce the file size. Inner layer is a '*PACK'* file created by *IzPack* installer generator for applications written in Java. Although there is no official unpacker for files made by *IzPack*, the structure of package file slightly resembles that of a forensic image and can therefore be reversed. *IzPack* package file contains a general file header, which is followed by files belonging to individual components of I2P router software. Individual component files within the package are designated by header and footer signatures, which also list the component file name, type and intended installation path.

These component files can be extracted with a single script written in a programing language such as Python which is compatible with most forensic tools, and then used to either construct a hash set library or in manual comparison by forensic analyst.

a. *Detection via known hash set library*

The individual I2P components extracted from installer files can be used to produce hash set libraries. These libraries can be imported into approved forensic software that is currently unable to identify the presence of I2P within evidence. EnCase suite by Guidance Software is one example of forensic tool which is approved for generating legally valid forensic reports, but cannot detect I2P in its default configuration. EnCase, however, supports use of hash libraries containing *MD5* and *SHA1* hashes of known software. These hash libraries are used by forensic labs to either filter out known good software[1] or detect known bad content such as illegal images or software with dubious uses.

EnCase can therefore be equipped for detection of I2P by importing a legacy hash library containing *MD5* hashes of I2P components. Some components of I2P are more suitable for this detection that others due to their unchanging nature. For example, I2P application itself is not a good candidate for hash library, as the hash changes with frequent releases of I2P. However, the digital certificates of I2P developer eepsites are good candidates, since these are present in every I2P node installation and remain unaffected across multiple version releases for years.

b. *Comparison of addressbooks*

One of the components of the I2P which can be extracted from I2P installer is the copy of the default *addressbook*. Every new I2P node is provided with the same copy of this addressbook during installation, so that it can access a basic minimal set of trustworthy eepsites. The I2P node is then expected to expand on this minimal addressbook by importing information from its own set of subscription sources and manual addition of eepsite domain name entries.

Forensic analyst can use this minimal default *addressbook* as a reference to be compared against *addressbook* found on the seized machine. Entries which are not found in the default *addressbook* have either been imported via subscription updates or added manually by I2P node owner. Eepsite records originating from subscription can be further eliminated from this list via inspection of subscription update log[2] entries such as update timestamp, source and domain name of imported record. Through this process of elimination, the addressbook from seized computer can be reduced to set of domain records which are highly likely to have been added by I2P node owner manually for his personal eepsite browsing. This information can be especially useful if the suspect has taken anti-forensic steps to eliminate browsing history and artefacts from his local machine.

c. *Takeover of existing registrars*

---

[1] National Software Reference Library (NSRL) hash sets are produced for this purpose.

[2] Present in the 0.9.25 version of I2P

Registrars in I2P network do not have to pass through any kind of accreditation or approval process. This makes it possible for any interested party to operate their own I2P domain name registrar node. Although it is possible for law enforcement or forensic analyst to setup their own new registrars on I2P network, some of existing known good registrars may also become vulnerable to takeover. The primary candidate for takeover would be registrar known as *'NO.i2p'*. *NO* is a small registrar compared to developer operated ones like '*Stats.i2p*', but still occupies a special position in I2P name resolution system.

NO does not share permissive policy operated by '*rogue'* registrars such as *INR*. Instead, *NO* shares same version of registration policy as developer-owned registrars, disallowing illegal or questionable content. Since there are no policy disagreements, *NO* is one of the few registrars considered "trusted" by I2P project team. As a trusted registrar, it is one of only four service choices shown to each I2P user who tries to access sites not known to local addressbook.

As of early 2016, the *NO* registrar appears to have been abandoned by its owner. New domain requests can still be submitted by users through *NO* site, but are not reviewed by its operator. The database of the existing domains has not been purged or screened for content violations, with *NO* retaining name entries for resources which violate its own terms of registration, such as I2P mirror of *Silk Road Reloaded* website.

The lack of maintenance together with the trusted status should make *NO* an attractive target for both law enforcement and malicious parties. Due to the lack of maintenance, *NO* is currently not receiving security updates for its I2P router software or the web server. An attacker with ability of compromising *NO* can gain control over a critical part of I2P infrastructure.

The alternative option would be to wait until the failure of *NO* or its I2P server and resort to social engineering. Most of I2P registrars including *NO* are running name resolution software known as *Py-I2PHosts*, which is available for download from its developer *eepsite* on I2P network. It is therefore possible to recreate *NO* after its failure, but on different *B32* and *eepsite* addresses. The recreated registrar can be then advertised on I2P community resources as resumed after hardware failure.

Success of this method is possible due to the decentralised structure of I2P registrars, which offers no control over the membership. Any user can setup a high-value network service with minimal resources. Registrar *'RUS.i2p'* was known for hosting I2P documentation and *eepsite* entries for users located in ex-CIS countries. After several extended outages and restorations of services, this registrar succumbed to a server hardware failure and is no longer available. Another of I2P registrars *'NIC.i2p'* lost ownership of its original *eepsite* domain name and can be reached only through its full network address. Several I2P operators found this incident suspicious and questioned[3] the operator's ability to run a critical network service. Despite this, the registrar remains operational at the time of this report and is included on unofficial "known good" registrar lists circulating in I2P user community.

d. *Mirroring of eepsites*

The non-hierarchical model of I2P name resolution system makes it possible for the forensic analyst to create own mirror of suspect website and register it under the same domain name. Domain names in I2P are guaranteed to be unique only per each registrar, but may not be unique for the entire I2P network. This makes it possible for the same I2P domain name to be associated with more than one host at the same time.

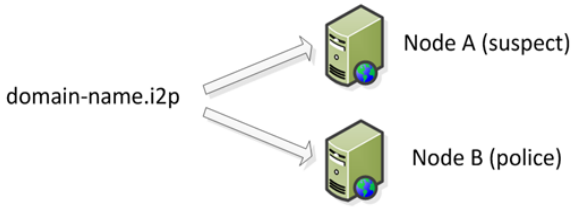

Fig. 2 I2P Short Domain Names Are Unique per Registrar

Due to complex propagation of I2P name updates, it is possible for the existing domain name to remain available on different registrars. For example, domain names registered via I2P registrar known as *INR* do not always propagate to other registrars due to *INR's* untrusted status.

This method of data collection should also be considered in relation to one peculiarity of I2P's naming system - persistence of name records. Once the I2P node *addressbook* entry is stored, it never expires. The registrar from which this *eepsite* information was originally retrieved may have since updated the information or purged the domain from its database entirely. However, none of these events will affect an existing addressbook entry. The owner, staff and regular visitors of mirrored I2P site will therefore remain unaffected by intelligence gathering carried out on the false mirror site.

The persistent *addressbook* entries work in favour of a forensic analyst or law enforcement agency. *Eepsite* owner and regular visitors are more likely to be security-conscious and very familiar with the "look and feel" of the compromised eepsite. This knowledge increases the risk of one of the visitors detecting inconsistencies in the false mirror site and alarming other users. In comparison, new or occasional visitors are less likely to be alarmed, since they do not have a reference to compare the mirror *eepsite* with.

The resulting benefit is that false mirror *eepsite* can remain undetected for a long period of time, constantly gathering information about activity of new visitors. The longer false *eepsite* stays operational, the higher is the chance of it trapping one of the regular visitors. This may occur through migration to new device (e.g. to secure virtual machine or a machine with full-disk encryption) without adequate preparation or release of incompatible update to I2P, therefore requiring user to repopulate his *addressbook* entries.

e. *Locating I2P Node by Network Performance*

[3] 'Nic.i2p' – a real DNS provider for I2P- I2P Forum

The use of denial-of-service attacks against I2P network has been proposed by Christopher Kack [7]. In attack known as "*darkloris*", the malicious I2P nodes keep cyclically opening a large number of connections to service provided by target I2P node. These connections are initiated with the sole purpose of consuming the resources of target I2P node, but are never properly used or terminated by the malicious nodes.

Kack successfully demonstrated the effectiveness of this attack against Jetty web server used by default in new installations of I2P router software. Despite Kack running his attack from a single malicious I2P node, the target node could not handle any more incoming connections to its web server, which resulted in all new eepsite visitors receiving an error page as shown in Fig 3.

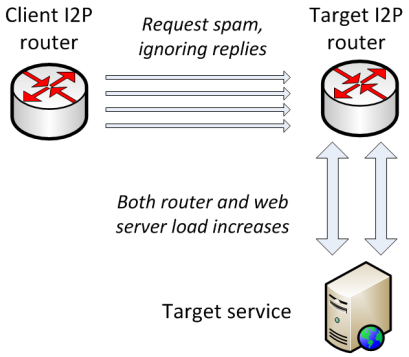

Fig 3. Kack's Generates Unused Connections to Target I2P Node

The original version of denial-of-service attack used by Kack was mitigated with introduction of request rate limiter in I2P router software. However, this mitigation is not complete and does not protect I2P nodes against other varieties of denial-of-service attacks. Instead of web server domain, the attack may instead focus on saturating the I2P encrypted tunnel limit, bandwidth or other resources of I2P node. The request rate limiter can be bypassed due to its reliance on I2P network identifier of the attacking node, which is not permanently assigned and can be changed by attacker every time one of his controlled nodes becomes blacklisted.

After the initial denial-of-service attack on I2P service node, the expected response of its operator was to increase the ratio of system resources available on I2P. This includes increasing the total bandwidth permitted, tunnel limit and memory size within I2P router configuration. However, this allows I2P router to accommodate an even larger denial of service attack, capable of having an impact on the I2P router. Network equipment used by the host is the first candidate for failure. The P2P aspect of I2P means that an active I2P router will be constantly receiving a large number of inbound TCP and UDP packets from a similarly large pool of unique remote IP addresses. The self-hosted I2P nodes running behind NAT may stop responding altogether, both on I2P network and the Internet. If the I2P router is monitored, the change in network performance or availability can be linked to denial of service attack.

An investigation of I2P network found that approximately half of total I2P network nodes do not stay connected for longer than a week [8]. This behaviour suggests presence of large number of nodes that are running over residential DSL or mobile broadband connections, which would be unable to properly handle large number of P2P packets and therefore vulnerable to this kind of attack.

The initial sample of IP addresses which need monitoring can be obtained by parsing I2P's floodfill database, a copy of which is kept by every I2P floodfill router. Adrian Crenshaw's research into identification of remote eepsites has produced a set of Python scripts for extracting this information [9].

Ordinary nodes which are not floodfill routers can be removed from candidate list, therefore reducing total list of candidates to a manageable number (several hundred). This is due to the way I2P determines promotion of ordinary routers to floodfill nodes. As of version 0.9.23, any I2P router which allows sufficient bandwidth to be shared by network is allowed to switch into floodfill node. A node which managed to remain available after the first denial-of-service attack is therefore highly likely to be a floodfill node and present on the extracted list.

If required, candidate list can be reduced further by continuous monitoring of floodfill nodes' availability and geolocation by IP. Any node that becomes unreachable while the targeted I2P service is still online is no longer a candidate. Geographic filtering becomes possible if some information about targeted node operator is known from other sources: social engineering, timestamps or accidental posting of information. All floodfill router records in NetDB have their IP addresses stored and therefore can be mapped [5].

The remaining suspect node IP addresses can then be monitored for signs of change in network performance such as dropped packets and increased round-trip times. The attacking nodes on I2P network can be commanded to cyclically connect and disconnect from suspect eepsite or other resource in order to produce a more visible pattern of changes over longer period of time.

IV. Related Works

Freenet [3] is an unstructured P2P system that has been designed to exchange information between users. It allows content to be published and retrieved in an anonymous way. Both the source and destination of the information are withheld from third parties and even from the system servers. Peers joined to the network participate in queries, data storage and retrieval of data items.

Freenet does not assign responsibility for documents to specific nodes and instead allows lookups to be carried out by searching for cached copies. Freenet aims to provide a flat Internet topology. In other words, you can communicate with an IP address next door, the same way you would communicate with another IP on the other side of the planet, without being discovered. It was first used by a large community of online users to distribute copyrighted materials on the Internet without being discovered. Clarke [3] claims that this was not the purpose of the project, which was

originally set up to counter rogue governments' attempts to impose censorship on the flow of information in the press, broadcasts and printed materials. Freenet nodes are encrypted and routed through other nodes to make it extremely difficult to determine its originator as well as content [3]. A request for key is passed along peers using flooding algorithm, which returns the corresponding data. These keys are location-independent. If a node received a request and knows the location of the file, it forwards it to the destination, which holds the information. If the node does not know the destination address, it forwards it to a node, which might hold the information or is likely to know the whereabouts of the resource.

To make the routing more efficient and smart, Freenet uses historical information and statistics from previous routing experiences to make a decision-based estimate of the time it might take to reach the destination. Caching based on specialisation of the nodes accumulated cache of the information resulted in Freenet failing to cope with overwhelming requests and collapsing in July 2003. It was then that the designer addressed the load balancing issues by ensuring the uniform load distribution and constraining queries to maintain the defined quota. Considering this approach has addressed the problem and works effectively, but it may lead to functionality issues by limiting incoming requests to retrieve resources. This means that individual nodes behaving other than anticipated may affect load balancing and increase request failure rate. Therefore, the challenge in terms of scalability and performance still persists within the Freenet structure. Like any other P2P system, nodes in Freenet can have a dual role and are not distinguishable by name. This component of the system improves the anonymity. However, an adversary can still identify the traffic load and distinguish server nodes using a packet analyser. Having said that, Freenet remains one the important systems in providing user anonymity.

The Onion Router (Tor) is a distributed overlay network to anonymise TCP-based applications such as instant messaging, web applications and secure shell [10]. Each node in Tor chooses a path, builds a circuit with its neighbours known as successor and predecessor. The traffic is relayed through fixed-sized circuits and unwrapped by symmetric key at each node similar to layers of an onion. Tor uses the incremental relay of messages provides complete anonymity. The use of encryption at each layer provides data integrity. In order to avoid alteration by nodes, Tor encrypts the messages before they leave the source node.

However, there are some weaknesses that have been found within Tor [6], [11]. Adversaries can also target single points of failure within Tor network, such as exit and directory nodes.

Like I2P, Tor is vulnerable against CPU-consumed denial of service attacks. However, Tor provides low latency and high bandwidth which makes it attractive for users who share instant messages and large size files. The issues found in Tor can be used to de-anonymise the users or decrypt the transmitted messages. However, this is beyond the scope of this paper. Nonetheless, like any other anonymity service online, Tor remains a challenge in any forensic investigation.

V. Conclusion and Future Works

While the anonymity systems maintain user privacy, promote free speech and facilitate free flow of information, they may be misused for illegal and questionable activities. Because of technological, geopolitical and legal challenges identifying and accessing such activities is an issue for forensic analyst and law enforcement agencies. We studied some security issues and core functions of I2P through an experiment to improve its detection by well established forensic software. We analysed different features and characteristics of I2P network that can be used for illegal activities online. Our analysis and experiments show that privacy model offered by I2P is comprehensive, but still leaves forensically valuable artefacts that can be extracted by custom written tools. Such solutions can be integrated within the industry approved forensic tools to promote better practice in I2P investigations within law enforcement and to enhance the continuity of the evidence.

For the future works, we will investigate the security flows of I2P in more details in order to provide a better understanding of the system. This will contribute to effective and efficient investigation of I2P activities.

References

[1] Y. Wei, C. Wang, Y. Chu and R. Chang, R, “A Secure and Stable Multicast Overlay Network with Load Balancing for Scalable IPTV Services,” Int. J. Digit. Multimedia. Broadcast. pp. 1–12.B. 2012

[2] Zantout, Bassam, and Ramzi Haraty. "I2P data communication system." Proceedings of ICN. 2011.

[3] I. Clarke, ”Freenet: A Distributed Anonymous Information Storage and Retrieval System” 1999, [available at http://freenetproject.org/freenet.pdf]

[4] M. Jawad, P. Serrano-alvarado, and P. Valduriez, “Supporting Data Privacy in P2P Systems”, Table of Contents,” pp. 1–51, 2013.

[5] C. Timpanaro, I. Chrisment and O. Festor, “A bird’s eye view on the I2P anonymous file-sharing environment”, online at: https://hal.inria.fr/hal-00744919/PDF, 2012.

[6] D. McCoy, K. Bauer, D. Grunwald, T. Kohno and D. Sicker. Shining Light in Dark Places: Understanding the Tor Network. In Proc. of Privacy Enhancing Technologies Symposium (PETS), Leuven, Belgium, 2008.

[7] C. Kack, “Layer 7 DOS against I2P darknet”, 2012 [available from http://blog.kejsarmakten.se/all/projects/2012/09/11/dark-loris.html]

[8] P. Liu, L.Wang, Q.Tan, Q.Li, X.Wang, J.Shi, “Empirical Measurement and Analysis of I2P Routers”, 2014 [Available from: https://pdfs.semanticscholar.org/3e5f/2b136df32beef1281b6b2f206093806c57f6.pdf]

[9] A. Crenshaw, “Darknets and hidden servers: Identifying the true IP/network identity of I2P service hosts”, 2011 [Available from: http://www.irongeek.com/downloads/Identifying%20the%20true%20IP%20of%20I2P%20service%20hosts.pdf]

[10] R. Dingledine, N. Mathewson, and P. Syverson. Tor: The second-generation Onion router. In Proc. 13th USENIX Security Symposium, 2004.

[11] M.Ehlert, “I2P usability vs. Tor usability: a bandwidth and latency comparison” [Online] Available from: http://userpage.fu-