# Unveiling The Malicious Users Behind the Anonymity Networks

DR. SUBBARAO KOLAVENNU[1], MUKESH GILDA[2], SHAIK ASIF[3], T. P. TEJASWINI[4], G. RAGHAVENDRA[5]

[1] *Head of The Dept, Dept of CSE [Cyber Security], Sphoorthy Engineering College, Hyderabad, India*

[2] *Assistant Professor, Dept of CSE [Cyber Security], Sphoorthy Engineering College, Hyderabad, India*

[3, 4, 5] *Dept of CSE [Cyber Security], Sphoorthy Engineering College, Hyderabad, India*

***Abstract*— This project addresses the issue of detecting intruders from hiding behind privacy-protecting anonymity networks. Today's incident handlers and IT/Security professionals face many challenges in securing their networks and enforcing company policies that protect those networks. A growing concern is the use of anonymous proxy services. However, recent security breaches reveal that SSH and HTTPS have been used to launch attacks by malicious users by taking advantage of these services to hide their identities. They do this for legitimate reasons that include preventing hostile work environments for their users, protecting network assets and data from malicious code or theft, and complying with regulations and company policies. We evaluate our approaches with SSH and HTTPS connections and show that they achieve high performance for both applications. Our detection algorithms are based on the extra latency delays introduced by the presence of the anonymity networks. Since the latency disparity is sensitive to the location of the anonymity network, our algorithms must be evaluated in the most challenging scenarios. This paper explores methods organizations may use to detect and prevent anonymous proxy usage. To demonstrate the robustness of our approach in the Tor case, we tested our method in multiple Tor circuit node selection strategies. The approach can be applied to other applications meeting the same criteria.***

***Index Terms*- Network security, intrusion detection, anonymous proxies, anonymity networks, VPNs, potential security threats.***

## I. INTRODUCTION

Internet users are facing an unprecedentedly high risk of being tracked and monitored. Technologies exist to assist online users in concealing their identities by using anonymous connections. With anonymous proxies, a user accesses an anonymous proxy website and selects an intended website (such as one that is blocked for the user) that the proxy will retrieve and display within its own page. However, the use of an anonymity network to protect a user's privacy comes with a cost. The extra hops will undoubtedly slow down the communication between the user and the server. More frequently, obfuscation techniques are used to hide the destination website, transmitted to the proxy server from the user via a parameter in the URL, making detection extremely difficult.

Many existing solutions rely almost entirely on blacklisting undesirable web sites, with the result being that many users learn that anonymous proxies allow them to easily bypass this filtering. While blacklists serve a purpose, how do you know if users are circumventing your policies and your blacklists? One answer is to focus on detecting access to anonymous proxies. This paper will focus on techniques for detecting access to anonymous proxy services which are Detecting Known Proxies – will focus on known proxy services that can be blacklisted as well as TOR (The Onion Router), Identifying and Detecting Popular Proxy Systems – will focus on the popular proxy packages such as PHPPRoxy, CGI Proxy, and Glype and Detecting Proxied Access to Your Website –will discuss the challenges of detecting proxied access by Internet users to web sites that you host.

## II. DETECTING KNOWN PROXIES

### 2.1 Blacklists

Blacklists are not generally effective at preventing new or previously unknown proxy sites because the proxy sites must be known before, they can be added to a blacklist. Blacklists can prevent already known proxies from being reused, leaving only newly created

or renamed sites accessible. Blacklists are relatively "low cost" in that using them in blocking rules or log searches does not severely impact system performance. In some cases, you may know something is a proxy but not have a way to readily detect it, so including it on a list of blocked sites gets the job done. There are some free proxy lists that people have compiled, but all seem to suffer from lack of attention; someone started the blacklist with good intentions and then ran out of time to keep it updated. If you run across a good blacklist, it may prove a valuable resource, but keep in mind that it is likely not the owner's top priority.

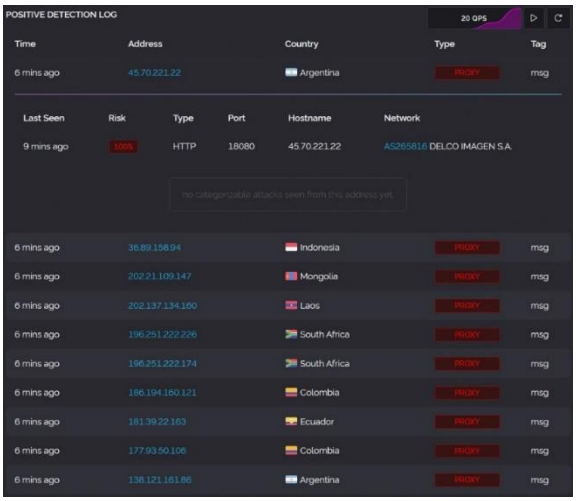

FIGURE 1. BLACKLISTS of the malicious proxies.

2.2 TOR

TOR, or The Onion Router, is a project to provide free software and volunteered network infrastructure (TOR nodes) to provide anonymity online. While preventing someone who is monitoring your Internet connection from learning what sites you visit has positive connotations for free speech in many parts of the world, it presents a problem for corporate and educational environments where identification and control of sites accessed is necessary to enforce acceptable use policies, minimize data leakage, and stop users from accessing harmful content. To test for TOR detection methods, I first installed the Vidalia package, a free multi-platform suite of TOR tools containing TOR, a GUI for TOR called Vidalia, Privoxy (a TOR add-on which filters out ads, banners, and pop-ups), and Tor button, the Firefox add-on that allows one button enabling and disabling of TOR sessions within Firefox. I then used Wireshark to capture network traffic as I initiated a TOR session.

## III. IDENTIFYING AND DETECTING POPULAR PROXY SYSTEMS

3.1 SSL Proxies

Anonymous proxies can employ digital certificates to make detection more difficult as all traffic passed will be encrypted. Except where self-issued (in which case they are not trusted by default browsers) SSL certificates are expensive from both a monetary and CPU (as the server handles the encryption) standpoint. The free, advertised anonymous proxies discussed here are unlikely to pay these premiums, especially when digital certificates get tied to a fully qualified domain name and many anonymous proxies come and go or change names week by week. For these reasons, SSL proxies are generally represented by commercial offerings. they are commercial entities advertising their names and paying for commercial digital certificates, these proxies are easy to find and easy to block; they will not be changing their domain names frequently, if at all. This is not surprising since their model is to provide anonymous browsing services to customers looking for anonymous browsing, not trying to circumvent filtering. These services can be blocked with a blacklist or a filtering rule as described in the blacklisting section.

## IV. ANONYMOUS CONNECTION

The goal of establishing an anonymous connection is to allow users to communicate with a remote server while concealing their identities. However, anonymity may also be used by attackers to protect them. In the past, hackers often take advantage of several intermediate hops to hide their identities before launching an attack. One example of such attacks is the SSH stepping-stone attack, by which the attacker gains access to a remote server with previously compromised accounts. With a chain of stepping-stones, the attacker has established a secure connection to a server anonymously. Therefore, Tor is the common tool for proxying the traffic to the Clearnet with low-latency anonymity. To launch an attack via Tor, the attacker can route their traffic through a preconfigured circuit with a high anonymity level. Furthermore, continuous development and research keep improving the performance and

anonymity of the existing Tor framework.

4.1 Detecting Anonymous Connections

As we stated, hackers have been widely abusing anonymity technologies to hide their identity. Previous research has studied stepping-stone detection techniques, and researchers. propose various algorithms to detect incoming SSH connections through stepping-stones. The algorithm based on association rule mining to detect stepping-stone SSH attacks achieves relatively high accuracy even with chaffed or jittered network traffic. A neural network-based algorithm to detect stepping-stone attacks and prove that the method can even predict the number of stepping stones in the chain. A novel approach that can identify long stepping-stone connection chains from short chains by comparing connections to a pre-computed short-chain profile. However, these algorithms rely on the timing information extracted from many SSH connections data packets, results in late detection that hinders the victim server from taking any effective security measure.

## V. CONNECTING THROUGH PROXY

Proxies are widely used in both building Internet firewalls and anonymizing connections. In general, proxies can operate at either the application layer or the session layer of the OSI model. A SOCKS proxy can be placed in the middle of the connection to conceal the client's identity to the server. After the SOCKS protocol handshake, the proxy forwards all the sub sequent data packets on the client's behalf to the destination server. One of the principal objectives of an adversary attacking a remote server is to make identity tracing extremely difficult. With multiple proxies available, the attacker can chain them together in the connection. The process of establishing a proxy chain is to perform the protocol handshakes incrementally from the client to the subsequent proxies in the chain.

One of the main factors that need the client's careful consideration is the connection speed. Because proxies in a chain might have different available bandwidths and latencies according to their configurations and network environments, the low performance proxies can compromise the overall connection speed from the client to the destination.

Besides, the proxy chain itself does not encrypt the network flows, results in possible eavesdropping along the chain. In other words, a client must trust every proxy in a proxy chain for a private and anonymous connection.

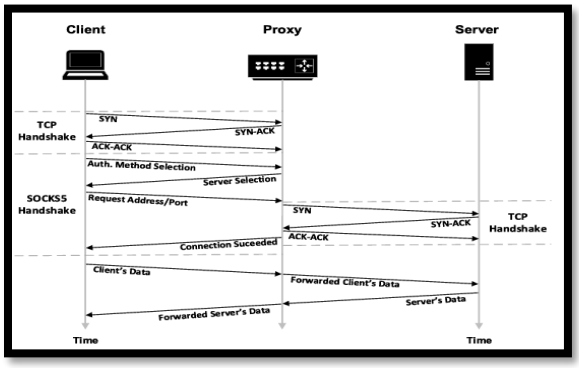


FIGURE 2. A depiction of how a client connect to a server via a SOCKS proxy server.

## VI. PROPOSED SOLUTION

Deploy intrusion detection systems (IDS) and intrusion prevention systems (IPS) to monitor network traffic and detect any suspicious activities. Utilize network forensics tools to analyze captured network data and identify potential threats. Implement threat intelligence platforms to gather information about known malicious users and their tactics. Utilize advanced malware analysis tools like Honeypot, Proton VPN, Canary Token, and IP Checker to identify and mitigate any malware threats within the network. Employ user behavior analytics (UBA) tools to detect anomalous user activities and identify potential malicious users. Implement strong authentication mechanisms, such as multi-factor authentication, to prevent unauthorized access. Continuously update and patch software and systems to protect against known vulnerabilities. By using these cyber security tools, we can enhance the security of anonymity networks and effectively unveil and prevent malicious users.

## VII. SCOPE

The scope of the project "unveiling and preventing malicious users behind anonymity networks" is mainly to create a comprehensive solution that tackles the challenges posed by these networks. The project aims

to conduct thorough research on anonymity networks and their vulnerabilities. It will then develop advanced cyber security tools and algorithms to detect and prevent malicious activities within these networks. The implementation of these tools will involve monitoring network traffic, identifying suspicious patterns, and ultimately unveiling the identities of malicious users. Collaboration with relevant stakeholders will be crucial for information sharing and coordinated efforts. Additionally, user education will play a vital role in raising awareness about the risks and responsible usage of anonymity networks. Continuous updates and improvements will be made to adapt to emerging threats, while ensuring compliance with legal and regulatory requirements for investigation and prosecution. Overall, the project seeks to enhance the security of anonymity networks and safeguard against malicious users.

### 7.1 SOFTWARE AND HARDWARE REQUIREMENTS

SOFTWARE REQUIREMENTS:
- Network Traffic Analysis Tools
- Machine Learning and AI Algorithms
- Data Visualization and Reporting Software
- Collaboration and Information Sharing Platforms
- Legal and Regulatory Compliance Software
- User Education and Awareness Platforms

HARWARE REQUIREMENTS:
- High-performance servers or cloud infrastructure for processing and analyzing network traffic data.
- Powerful CPUs and GPUs to handle complex machine learning algorithms. Sufficient storage capacity to store and process large datasets.
- Reliable network infrastructure to handle the incoming and outgoing traffic.
- Secure data backup and disaster recovery systems to ensure data integrity.

## VIII. PROBLEM STATEMENT

The main problem in detecting malicious users behind anonymity networks is the inherent challenge of tracing and identifying their activities due to the cloak of anonymity these networks provide. The very nature of anonymity networks makes it difficult to directly link actions to specific individuals, as they operate through encrypted channels and IP masking techniques. This makes it challenging for traditional detection methods to pinpoint the true identities of malicious users. Additionally, the vast amount of network traffic and the constant evolution of anonymity tools further complicate the detection process. Overcoming these obstacles requires the development of advanced techniques, algorithms, and collaboration among stakeholders to effectively unveil and prevent malicious activities within anonymity networks.

### 8.1 DEPLOYMENT DIAGRAM

In this deployment design, the project involves multiple components. The anonymity network is the target of the project, where malicious users operate. The monitoring system is responsible for capturing and analyzing network traffic within the anonymity network. It feeds the data to the detection algorithms, which use advanced techniques to identify suspicious patterns and activities. The identification techniques are then employed to unveil the true identities of the malicious users. Finally, a collaboration platform is established to facilitate information sharing and coordination among stakeholders involved in combating malicious activities within anonymity networks.

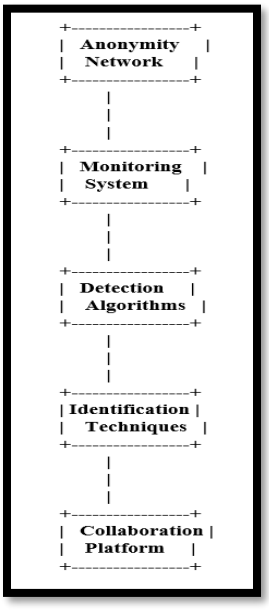


FIGURE 3. Deployment diagram of proposed system.

8.2 IMPLEMENTATION PLAN

8.1.1 HONEYPOT SETUP

Honeypot tools are cybersecurity tools that trick hackers by imitating vulnerable systems or services. They help organizations gather information about their tactics and intentions. Popular honeypot tools include Kippo, Dionaea, Cowrie, Honeyd, and Glastopf. Kippo and Cowrie focus on emulating SSH services, while Dionaea captures malware samples.
Honeyd is versatile, allowing emulation of various network services, and Glastopf specializes in emulating vulnerable web applications. Honeypots can be deployed in networks or on cloud infrastructure. However, it is important to configure and monitor them carefully to avoid security risks. Consulting cybersecurity professionals is recommended before deploying honeypot tools.

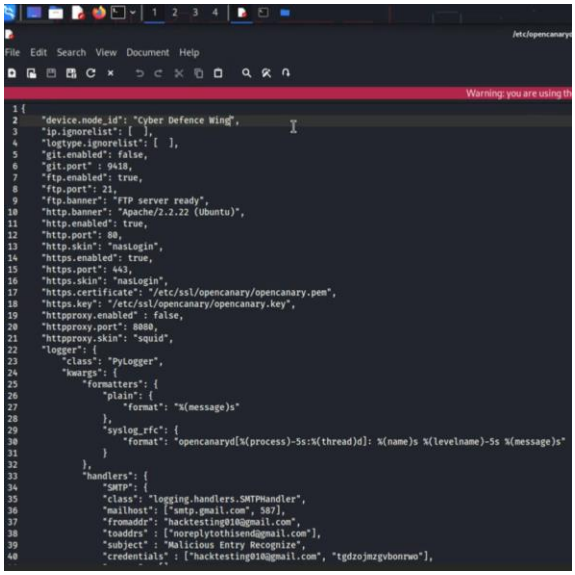


FIGURE 4. Honey pot setting up program

8.2.2 PROTON VPN

ProtonVPN is a powerful cybersecurity tool that helps protect your online privacy and security. It creates a secure, encrypted connection between your device and the internet, preventing others from intercepting your data. ProtonVPN offers a wide range of features, including a strict no-logs policy, strong encryption, and a large network of servers across the globe. It also has a user-friendly interface and supports multiple platforms. Whether you're browsing the web, streaming content, or accessing public Wi-Fi, ProtonVPN keeps your online activities private and secure. It's a great choice for anyone looking to enhance their online privacy and security.


FIGURE 5. Proton VPN setting up for anonymizing the identity.

7.4.3 IP CHECKER

An IP Checker tool is a handy online tool that allows you to check the IP address associated with your internet connection. It provides information about your IP address, such as your location, internet service provider, and other details. This tool can be useful for various reasons, such as troubleshooting network issues, verifying your online privacy, or identifying potential security threats. By knowing your IP address, you can have a better understanding of how your internet connection is being used and take necessary precautions to protect your privacy. It's a straightforward and helpful tool for anyone curious about their IP address.

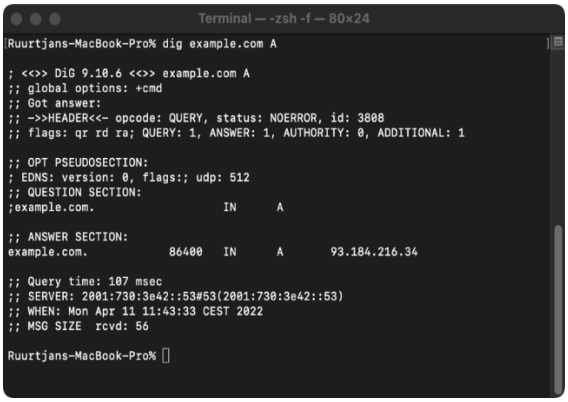


FIGURE 6. Revealing the IP Address of the Attacker.

7.4.4 CANARY TOKEN

A Canary Token is a nifty cybersecurity tool that helps detect unauthorized access or suspicious activity on your systems. It works by creating a digital trap that, when triggered, alerts you to potential breaches. These tokens can be embedded in various files, such as documents, emails, or even web pages. When an attacker interacts with the token, it sends an alert to your security team, allowing them to investigate and respond promptly. Canary Tokens are an effective way to monitor and detect potential threats, providing an extra layer of security to your digital assets. It's like having a canary in a coal mine, warning you of danger in your cybersecurity landscape.

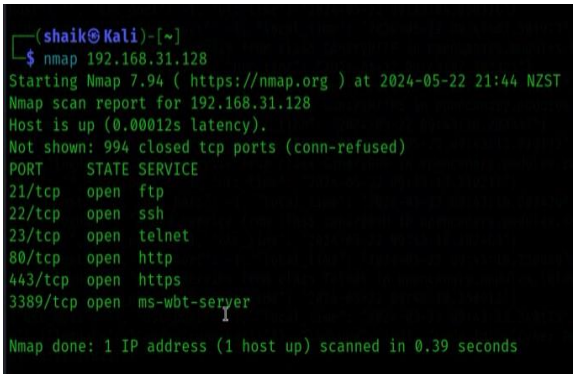


FIGURE 7. Implementation of Honey Pot using Canary Token and opening all the ports created through Honey Pot.

## IX. KEY FEATURES

- Helps gather information about hackers' tactics and intentions. Popular tools include Kippo, Dionaea, Cowrie, Honeyd, and Glastopf.
- Can be deployed in networks or on cloud infrastructure. Requires careful configuration and monitoring.
- Protects online privacy and security. Creates a secure, encrypted connection between your device and the internet. Offers a strict no-logs policy and strong encryption.
- User-friendly interface and supports multiple platforms. Allows you to check your IP address and associated details. Helps troubleshoot network issues and verify online privacy.
- Can be used to identify potential security threats. Simple and helpful tool for understanding your internet connection. Creates digital traps to detect unauthorized access or suspicious activity.
- Alerts you when the token is triggered, indicating potential breaches. Tokens can be embedded in files like documents, emails, or web pages.
- Provides an extra layer of security to monitor and detect threats. Allows for prompt investigation and response by security teams.


FIGURE 8. KALI LINUX Application

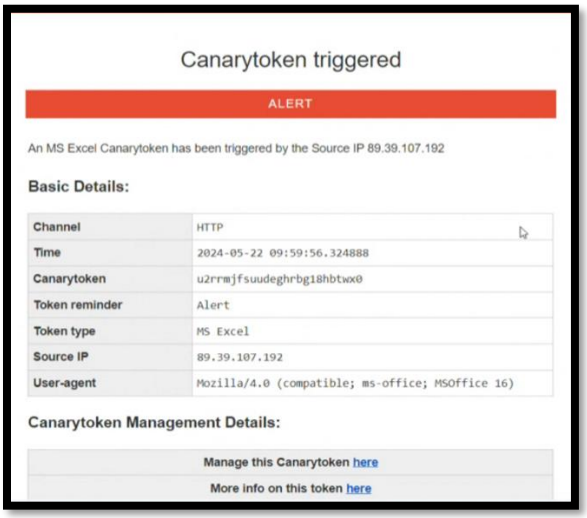


FIGURE 9. Detected malicious IP address of the attacker.

## CONCLUSION

Although there is no single, easy way to unveil and prevent the malicious users behind the anonymous networks, I have reviewed several techniques that can detect or block many proxies. Blacklists are a good starting point, especially if you can automate the updating of them by utilizing proxy-advertising sites. Honeypot rules can trick hackers by imitating vulnerable systems or services. They help organizations gather information about their tactics

and intentions, for the advanced ProtonVPN creates a secure, encrypted connection between your device and the internet, preventing others from intercepting your data. IP Checker users, may be used to access and check the IP addresses. Combined, these tools and techniques can help us stay on top of anonymous proxy usage in your environment.

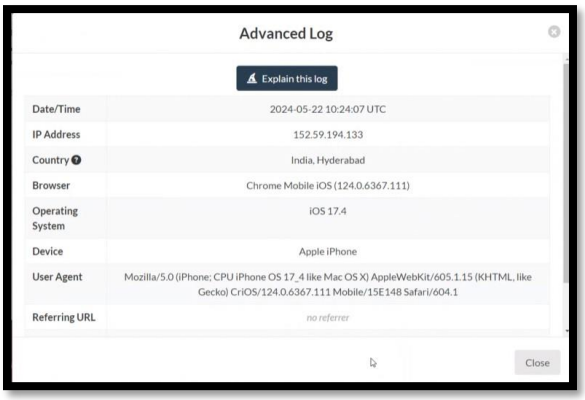


FIGURE 10. Advance Enhancement of the Project

## FEATURES OF UNVEILING AND THE MALICIOUS USERS BEHIND THE ANONYMOUS NETWORKS

Thinkst Canary is a security solution that helps detect attackers on a network before they can cause damage. It has the following features:

Setup: Takes only three minutes to set up.
No ongoing overhead: Has almost no false positives and no ongoing overhead.
Hosted management console: Customers receive a few events per year. Cloud-based deployment: Can be deployed in the cloud. Thinkst Canary can be used to: Order, configure, and deploy Canaries across a network. Drop fake AWS-API keys on every enterprise laptop. Increase the time it takes for attackers Thinkst Canaries are available in packs of five or more, and can be hardware, virtual, or cloud-based.

There is no limit to the number of Canarytokens, and both Canaries and Canarytokens can be created in groups called Flocks. Some of the new features in the Canary V3.x.5 release include:
Windows file shares
File share structures
Personalities for SAP NetWeaver, SolarWinds, and Sophos AWS Canaries. Thinkst Canary is an advanced security solution that helps detect attackers on your network before they can do any damage. With just 3 minutes of setup, no ongoing overhead, and nearly 0 false positives, you can detect attackers long before they dig in.

## REFERENCES

[1] BBC News. Coronavirus: Cyber-Attacks Hit Hospital Construction Com panies. Accessed: May 13, 2020. [Online]. Available: https://www.bbc.com/news/technology-52646808

[2] N.E.WeissandR.S.Miller, Thetargetandother nancial data breaches: Frequently asked questions, in Proc. Congressional Res. Service, Pre pared Members Committees Congr., vol. 4, Feb. 2015.

[3] L. Matsakis and I. Lapowsky. (Sep. 2018). Everything we Know About Facebooks Massive Security Breach. Wired. Accessed: Oct. 3, 2020. [Online]. Available: https://www.wired.com/story/facebook-security breach-50-million-accounts/

[4] J. McKeague and K. Curran, Detecting the use of anonymous proxies, Int. J. Digit. Crime Forensics, vol. 10, no. 2, pp. 7494, Apr. 2018, doi: 10.4018/IJDCF.2018040105.

[5] E. D.Zwicky, S. Cooper, and D. B. Chapman, Building Internet Firewalls: Internet and Web Security, 2nd ed. Sebastopol, CA, USA: OReilly & Associates, Inc., 2000.

[6] Zoica, Remus. New Threat That Can Be Used to Divert Web Traffic Through a Malicious Proxy Server. 31 March 2007. Accessed 28 August 2008 at <www.torproject.org>

[7] Tor project staff. Tor: anonymity online. Unknown. Accessed 30 May 2008 at http://wiki.noreply.org/noreply/TheOnionRouter/TorFAQ#headc7d58fb7afe0df2e76a50a288f3c6777d6a4adda

[8] Tor project staff. TorFAQ. Accessed 30 May 2008 at Key fingerprint = AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46

[9] Bianco, David. Detecting Tor on your network. 25 January 2005. Accessed 30 May 2008 at

http://blog.vorant.com/2005/01/detecting-tor-on-your-network.html

[10] Anonymous. How does Base 64 Encoding Work? 12 September 2007. Accessed on 20 June 2008 at http://www.hcidata.info/base64.htm.