

Wi-Fi Security Level Analysis for Minimizing Cybercrime

By Imam Riadi

Wi-Fi Security Level Analysis for Minimizing Cybercrime

Anis Susila Abadi
Islamic University Indonesia
Yogyakarta, Indonesia

Imam Riadi
Ahmad Dahlan University
Yogyakarta, Indonesia

Yudi Prayudi
Islamic University of Indonesia
Yogyakarta, Indonesia

ABSTRACT

The increasing human need for Internet access requires Internet access service that is easy to do as the availability of Wi-Fi hotspot. Among the many Wi-Fi hotspots in public service locations in Yogyakarta is still very little attention to the security of data communications on the wireless network. This makes the hacker be interested to discover his ability to perform various activities of cybercrime. This study aims to analyze and test the Wi-Fi network security contained in locations of public services in Yogyakarta. The method used in this study is a qualitative method that consists of five main steps, namely the study of literature, the issue of criteria Wi-Fi, research instruments, data collection, and analysis. The location of public services, Wi-Fi hotspot providers selected in three categories: hotel, restaurant / cafe, and educational institutions. Each public service category taken sample 5 different locations. Testing is done with action that leads to crime by type of action such as sniffing, DNS spoofing and hijacking. The results showed that the majority of Wi-Fi located at the location of public service vulnerable to criminal attack. Wi-Fi throughout the studied (100%) are not secure against sniffing activities, 80% are not secure against DNS spoofing activities, and 66.6% are not secure against hijacking action.

General Terms

Wifi Security Attack

Keywords

Wi-Fi security, cybercrime, sniffing, DNS spoofing, hijacking

1. INTRODUCTION

Technological innovation is now growing more rapidly. Everyone in all that is associated with the technology. In harmony with the development of these communities have high mobility want to find a service that is flexible, easy-paced and satisfying and pursue efficiency in all aspects. One technology that able to provide those needs is the technology of Wi-Fi (Wireless Fidelity). The penetration of the internet and computer networks is rapidly increasing in addition to providing ease but also has security concerns for companies and individual database users [1] [2].

Wi-Fi network actually has more weaknesses than wired networks. Some disadvantages of Wi-Fi security issue that is still vulnerable than wired technology [3], the rate is influenced by environmental conditions, Bandwidth required larger, some electronic devices may weaken the signal Wi-Fi, Cost components of Wi-Fi is big enough and network capacity is quite limited.

In this era, the availability of mobile services has increased significantly due to many important applications provided by mobile device manufacturers. A variety of mobile device security issues and data privacy threat that challenges both manufacturers and users. Therefore, the mobile device is an ideal target for a wide range of issues of security and privacy threats [4].

In Yogyakarta, there are currently many services such as Wi-Fi hotspot commercial, ISP, Internet Cafe, campuses and offices are using Wi-Fi network on each, but very little attention to the security of data communications on the wireless network. This makes the hacker be interested in exploration ability to perform various activities that are usually illegal through a Wi-Fi network.

From the facts above and the number of Wi-Fi, especially in Yogyakarta, there is no research or testing in locations that provide Wi-Fi in Yogyakarta. Therefore we need research or testing in locations specific Wi-Fi to see the level of network security that uses Wi-Fi proficiency level. By knowing the security level Wi-Fi and the possibility of criminal activities that can be done, it can be done precautions to avoid or minimize crime activities on the Wi-Fi service.

2. CURRENT RESEARCH

In general, there have been previous studies that discuss the safety of Wi-Fi and cybercrime attack. This study focuses on the analysis of Wi-Fi security level that existed at the location of public services in the Yogyakarta area. Other studies related to Wi-Fi security level is done by Hamid and Fietyata Yudha, which has analyzed the security level Wi-Fi network FTI-UIL. In the study Wi-Fi network in UIL was very vulnerable to attacks ARP Poisoning and all the existing network successfully attacked by ARP Poisoning attacks [5].

Another study was conducted by Mekhaznia T [6], entitled Wi-Fi Security Analysis. This study aims to determine the system's security protocol by using FMS Attcak wifi. The results showed that the security protocol with WEP and WPA wifi is not completely secure and can be assault with a key recovery attack.

Research conducted by Jindal P entitled Quantitative analysis of the security performance in wireless LANs [7]. This study aims to determine how the security system on a Wi-Fi network. The results showed that the different security protocols will have different security levels. Knowing this, it can have a security protocol that has a strong resistance.

The study titled Cyber Security Challenges within the Connected Home Ecosystem Futures conducted by Arabeo [8]. In this study aims to determine how the security of the connection is made via a smart home.

The study, entitled Detection and analysis of eavesdropping in anonymous communication networks by Chakravarty et al. [9]. The purpose of this study is to analyze crime anonymous tapping in a network. The focus of research by implementing a prototype using the IMAP protocol, SMTP, and HTTP. These results indicate that the encrypted using SSL security can not guarantee a person of the man in the middle of the attack.

The study, entitled Performance evaluation of laboratory Wi-Fi IEEE 802.11a wpa point-to-multipoint links by Carvalho et al. [10]. This study focuses on the evaluation of the

performance of IEEE 802.11a permagkat wifi with WPA security links point to multipoint.

The study, entitled Security Concerns with Open Research Issues of Present Computer Network by Rathee G. And Saini H. [3]. This study proposes a method of Wireless Mesh Networking security system to deal with wiretapping attacks, attacks on the network layer, and an attack against the service.

The study, titled reviews on Cybercrime Affecting Portable Devices by safavi et al. [11]. This study aims to determine bagaimana security for data probadi available on mobile devices android smartphone operating system from cyber attacks such as data theft and phishing.

The study, entitled Performance Evaluation of IEEE 802.15.4 Protocol Under Coexistence of 802.11b by wagh et al. [12]. This study aims to simulate the frequency of wifi 802.11b protocols (ZigBee) to prevent coexistence in a wireless network.

In this study the author elaborates on earlier research with a focus test the level of network security or network using Wi-Fi in Yogyakarta, such as in environmental education, hotel and restaurant / cafe. Testing is done with some form of crime sniffing, DNS spoofing and hijacking. The test results then analyzed to determine how the security conditions. Objectives and methods contained in this study is different from the studies conducted earlier. This study aims to test and analyze the security level Wi-Fi contained on the location of public services in Yogyakarta to attack by sniffing, DNS spoofing and hijacking.

3. METODOLOGY

The method used in this study consists of five main steps, namely literature, identification, determine research instruments, data collection, and analysis. Fig. 1 shows the design was made in several steps in this study.

3.1 Literature Study

At this stage of data collection by literature related to the Wi-Fi network security and cybercrime. A literature study began by gathering various information materials from books, proceedings, journals, articles and links from web pages that are relevant to the issues to be investigated. A literature study was also conducted to understand the theories of the fundamental concepts of computer networking technology, Wi-Fi and interception of communications networks as well as a discussion on research or scientific work earlier in order to avoid duplication or repetition that makes research ineffective.

3.2 Identification

Phase identification is done by identifying the Wi-Fi security criteria and identification of cybercrime activities through Wi-Fi network.

Identification of existing security criteria Wi-Fi on the location of public services in the Yogyakarta area is the identification of criteria for Wi-Fi is identifying the type of security applied to a Wi-Fi hotspot service. There are several criteria that can be used by a hotspot Wi-Fi is open, wireless key, and web authentication login.

Identification of cybercrime activities is the identification of the types of attacks that lead to cybercrime through Wi-Fi network. There are three activities that can be done is sniffing, DNS spoofing and hijacking.

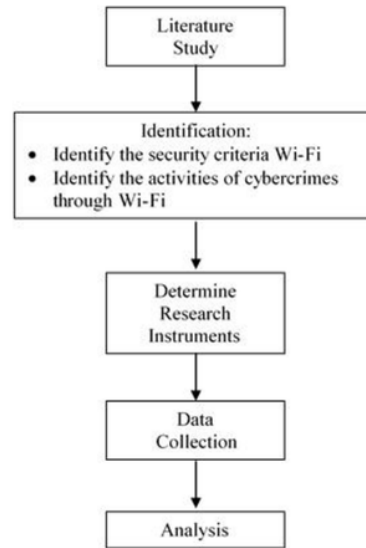


Fig 1: Draft grooves research

3.3 Research Instruments

In this study have some Wi-Fi hotspot locations that are in the public service. The location of public services in question is the location that provides services to the user in general so that anyone can use the Wi-Fi hotspot without having registered permanently. In this study selected three categories namely the location of public services institutions, hotel and restaurant / cafe. Each category of public service locations are randomly selected five samples at a different location but still in the region of Yogyakarta area.

The hardware used ³ this study are two laptops with specs Pentium Dual Core 1.8 GHz, 3 GB RAM, 320 GB Hard Disk, with Linux OS Backtrack, which serves as a Linux-based computer hacker. In addition to the hardware and software is also used which consists of the Linux operating system, the Windows operating system, Apache web server, browser, wireshark, and ettercap.

3.4 Data Collection

In this study, data was collected by means of observation and literature. The observations were made with the review directly to the location of the study and then make observations, take notes, and evaluate existing network location. Literature is a literature study to find materials from the Internet and read books that match the observed object.

3.5 Analysis

The analysis was conducted to test the security system of the wireless network or to identify possible values where unauthorized access can be obtained. The purpose of this test is to find vulnerabilities every point in the wireless network security system installed at certain locations that serve as the test object. Tests conducted with various activities that lead to internet crime (cybercrime) using the technique of sniffing, DNS spoofing, and Hijacking.

4. DISCUSSION

4.1 Testing Mechanism

In testing the security of a Wi-Fi hotspot locations that are in public services such as hotel, restaurant / cafe, and educational institutions is necessary to determine the exact mechanism so as not to be a crime and violating the privacy of other users. In doing Wi-Fi network security testing on the location of public services in Yogyakarta, researchers using two computers. The first computers used for users who access the internet through Wi-Fi networks that existed at the location of public services. The second computer is used as the attacker to commit the crime to the first computer. Two computers used by researchers connected in a network Wi-Fi.

4.2 Sniffing

The term is an act of sniffing capture data packets passing on a network. In this study, sniffing activities carried out to capture the data packets that pass through the Wi-Fi networks in public services. The captured data packets can then be analyzed and used for specific purposes.

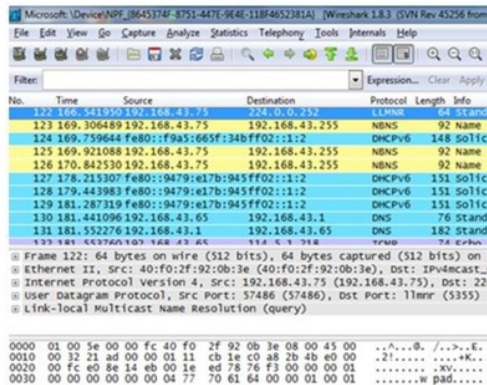


Figure 2 shows a Wireshark packet capture of network traffic. The packet list on the left shows several DNS queries and responses. The packet details pane on the right shows the structure of a DNS packet, including the header, questions, answers, and authority sections. The packet bytes pane at the bottom shows the raw hexadecimal and ASCII data of the captured packet.

No.	Time	Source	Destination	Protocol	Length	Info
122	166.541950	192.168.43.75	224.0.0.252	LLMNR	64	Standard query query
123	169.306489	192.168.43.75	192.168.43.255	NBNS	92	Name service
124	169.759644	fe80::f9a5:665f:34b:ff02::1:2		DHCPv6	148	Solicit
125	169.921088	192.168.43.75	192.168.43.255	NBNS	92	Name service
126	170.842530	192.168.43.75	192.168.43.255	NBNS	92	Name service
127	178.215307	fe80::f9a5:665f:34b:ff02::1:2		DHCPv6	151	Solicit
128	179.443983	fe80::f9a5:665f:34b:ff02::1:2		DHCPv6	151	Solicit
129	181.287319	fe80::f9a5:665f:34b:ff02::1:2		DHCPv6	151	Solicit
130	181.441096	192.168.43.65	192.168.43.1	DNS	76	Standard query query
131	181.552276	192.168.43.1	192.168.43.65	DNS	182	Standard query response

Fig 2: An example of a data packet sniffing by using the results of wireshark

Sniffing is done in this study is the packet capture data that pass through the network. In doing activities sniffing, computer attack using wireshark application. Target computer online activity where this activity will be captured by the attacker's computer. Fig. 2 below is an example of a data packet sniffing by using the results of wireshark. In this figure, there is information on the data packets passing through the network. The data includes time, source, destination, protocol, data length, and information about the package.

4.3 DNS Spoofing

DNS poisoning is a way to forge a host address that is accessible via a network. How this is done by submitting incorrect information about the IP address of a host. The goal is to divert traffic to packets of data from the actual host. This method can also be used to alter or destroy the contents of the DNS so that all access the DNS will be channeled to the wrong address or the address cannot be accessed. By doing DNS spoofing, an attacker could create a fake web that resembles the original. The attacker will direct users to a computer in the network when they want to access the original web. With this transition, the attacker has to fool the user to obtain information from those users.

DNS spoofing activity in this research is done by using time Linux operating system, Apache web server, and application

ettercap. Fig. 3 below is spoofing DNS activation using an application ettercap. In this figure, seen a few plugins that can be done one of which is DNS spoofing. The asterisk in the DNS Spoofing indicates that the plugin has been activated.

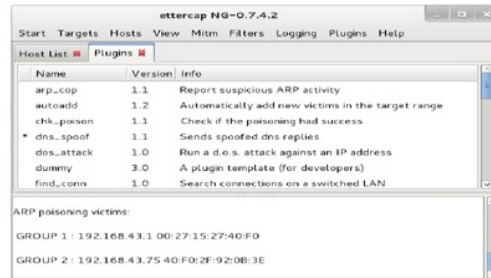


Fig 3: DNS spoof activity using an application ettercap

If the DNS spoofing activity is successfully done then the user will access a specific DNS will be directed to a local server belonging to the attacker. Fig. 4 below is a view of a DNS that have been successful in diverting.



Fig 4: View of a DNS that have been successful in diverting

4.4 Hijacking

Hijacking is an activity undertaken to enter a system through other and operating system. In this research, some measures to stop the activities of hijacking as a target connection, take a username and password the target or by taking session of the target computer. Fig 5 below is to stop the connection by using the application ettercap. In this figure, seen some connections host to host that was built over a network. to stop the connection can be made by selecting one connection and then disconnect the connection by clicking on the Kill Connection button.

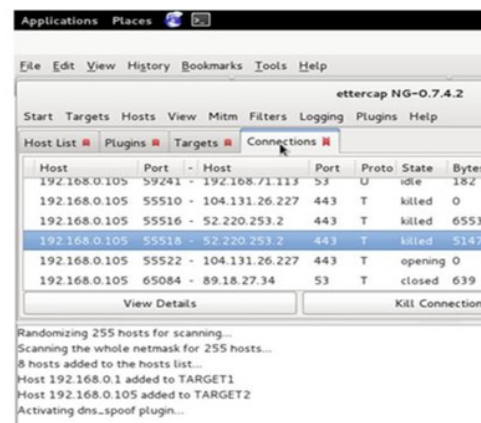


Fig 5: Kill connection to stop the connection by using the application ettercap

Another hijacking activity is by mac address spoofing. This activity is done by changing the mac address of the computer attackers with address mac computers have the target user. To do mac address spoofing used on Linux console applications. Fig 6 below is a command to change the mac address.

```

root@kali: ~
File Edit View Search Terminal Help

[....] Restarting web server: apache2
apache2: Could not reliably determine the server's full
using 127.0.0.1 for ServerName
. ok
root@kali:~# ifconfig wlan0 down
root@kali:~# ifconfig wlan0 hw ether 40:f0:2f:92:0b:3e
root@kali:~# ifconfig wlan0 up
root@kali:~#

```

Fig 6: Command to change mac address spoofing used on linux console applications

In addition to killing the connection, hijacking can also be done by entering the system by using session or user id belongs to another user. Session or user id can be obtained through the data packet sniffing using ²reshark application. Fig 7 the following are sniffing data packets containing the username and password.

```

68 74 74 70 3a 2f 2f 31 eferer: http://1
2e 31 2f 6c 6f 67 69 6e 92.168.1 .1/login
70 25 33 41 25 32 46 25 ?dst=htt p%3A%2F%
38 2e 32 30 30 2e 31 25 2F192.16 8.200.1%
70 74 2d 45 6e 63 6f 64 2F..Acce pt-Encod
70 2c 20 64 65 66 6c 61 ing: gzi p, defla
70 74 2d 4c 61 6e 67 75 te..Acce pt-Langu
49 44 2c 69 64 3b 71 3d age: id- ID,id;q=
53 3b 71 3d 30 2e 36 2c 0.8,en-U S;q=0.6,
0d 0a 0d 0a 75 73 65 72 en;q=0.4 ...user
73 26 70 61 73 73 77 6f name=agu s&passwo
36 30 65 36 62 62 39 35 rd=ebc0b 60e6bb95
34 34 65 61 64 36 31 39 f63b1c1a 44ead619
68 74 74 70 25 33 41 25 b6e&dst= http%3A%
2e 31 36 38 2e 32 30 30 2F%2F192 .168.200
70 75 70 3d 74 72 75 65 .1%2F&po pup=true

```

Fig 7: Sniffing data packets containing the username and password

5. ANALYSIS

Testing is done to see the level of security of Wi-Fi network by using DNS Poisoning techniques, sniffing and hijacking. In this research has been some hotspot Wi-Fi available in public services such as restaurant or cafes, hotels, and educational institutions. Each of these types of public service has taken several samples at different locations. The Wi-Fi hotspot then tested do the activities that led to the Internet crimes are sniffing, DNS Poisoning, and hijacking.

The test results on the security level of existing Wi-Fi hotspot in the public service are presented in Table 2. The data shows that overall the Wi-Fi hotspots are meticulous in status is not secure. The whole Wi-Fi studied (100%) are not safe against sniffing activities. Sniffing activities undertaken in this study is an event to view the data packets that pass through a Wi-Fi network. Tools used are Wireshark and Ettercap. Wireshark is software that can be used as network analysis tool. By using this tool one can analyze the condition of a network including a look at the data packets passing through the network. By looking at the data packets passing one can retrieve the data, analyze, and use it for specific purposes including crimes.

Network administrators can solve crimes sniffing by using network analysis software either similar or not to do an analysis on incoming network packets out over the network. If it finds any discrepancy traffic to the source and destination of suspicious, administrators can terminate connections to the computer that is suspected.

DNS spoofing action was successfully performed on most of the Wi-Fi hotspot. 80% Wi-Fi hotspot locations that are in the public service can attack with DNS spoofing activity. The success of spoofing action is performed using software Ettercap. DNS spoofing DNS done on Google.co.id belongs or belonged Microsoft.com DNS. DNS spoofing activity used to trick other users when accessing a domain address. With DNS spoofing someone can create a fake web page that is used to capture information from the user targets such as web login or authentication pages. By obtaining this information, then one can use the data to crime.

A user can avoid crime such as DNS spoofing action by way of caution when accessing a web page. Users need to check the authenticity of the DNS IP address to be accessed. Usually DNS spoofing IP address will point to the destination IP local address. The local IP address usually is 192.168.X.X.

Hijacking actions undertaken to enter into a system using other systems. By hijacking a person can pretend to be someone else and use existing resources to crime. The results of this study showed that 66.6% of the sample studied can be attacked with actions hijacking. Hijacking is done in this study is hijacking the mac address by spoofing or session hijacking.

The act of hijacking the mac address spoofing can be overcome by applying routing and restriction system client with the IP address listed and the mac address filtering. Hijacking with the web login session can be overcome by using a login page that is encrypted on the client side rather than on the server side so that data packets sent over the network is a packet of data that has been encrypted.

Internet users to exercise caution in making Internet access through a Wi-Fi hotspot that exist in the public service. Ensure kept up-to logout after accessing the web using a login system.

Table 2. The results of the security testing on wifi hotspot network

Wi-Fi Location	Wi-Fi Security	Testing			Status
		S	D	H	
Cafe 1	Wireless key	✓	✓	✓	Not Secure
Cafe 2	Wireless key	✓	✓	X	Not Secure
Cafe 3	Wireless key	✓	✓	✓	Not Secure
Cafe 4	Wireless key	✓	✓	✓	Not Secure
Cafe 5	Wireless key	✓	X	X	Not Secure
Hotel 1	Wireless key	✓	✓	✓	Not Secure
Hotel 2	Web login	✓	✓	✓	Not Secure
Hotel 3	Wireless key	✓	✓	✓	Not Secure
Hotel 4	Wireless key	✓	✓	✓	Not Secure
Hotel 5	Web login	✓	X	X	Not Secure
Campus 1	Wireless key	✓	✓	✓	Not Secure
Campus 2	Web login	✓	X	X	Not Secure
Campus 3	Web login	✓	✓	X	Not Secure
Campus 4	Wireless key	✓	✓	✓	Not Secure
Campus 5	Wireless key	✓	✓	✓	Not Secure

Description:

S: Sniffing; D: DNS Spoofing; H: Hijacking

6. CONCLUSION

After a test on Wi-Fi hotspot located at the location of public services and analyzing the test results, the conclusions presented in this section that the authors get based on existing data.

All existing Wi-Fi hotspot service at the location of public services is a network service that is not safe. The network is vulnerable to sniffing activity that allows others to sniff out user activities in the network. Data show that 100% of existing wifi hotspot can be attacked by sniffing.

Some have a Wi-Fi hotspot good enough level of security against DNS spoofing and hijacking attacks but remain vulnerable to sniffing activity. Activity sniffing the first step when a person who wants to commit a crime network. Data shows that 80% of existing wifi hotspot can be attacked with DNS spoofing and 66.6% can be attacked with the hijacking. Fig. 8 below shows the percentage of successful activity of the attacks made against a Wi-Fi hotspot.

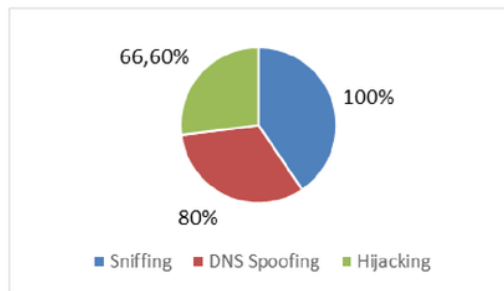


Fig 8: Percentage of successful activity of the attacks made against a Wi-Fi hotspot

7. REFERENCES

- [1] Bamrara A, "Evaluating Database Security and Cyber Attacks: A Relational Approach," *Journal of Internet Banking and Commerce An*, pp. 1-17, 2015.
- [2] D. Solak and M. Topaloglu, "The Perception Analysis of Cyber Crimes In View of Computer Science Students," *Procedia - Social and Behavioral Sciences* 182, p. 590-595, 2015.
- [3] G. Rathee and H. Saini, "Security Concerns with Open Research Issues of," *International Journal of Computer Science and Information Security (IJCSIS)*, Vol. 14, pp. 406-432, 2016.
- [4] J. Khan, H. Abbas and J. Al-Muhtadi, "Survey on Mobile User's Data Privacy Threats and Defense Mechanisms," *Procedia Computer Science* 56, p. 376-383, 2015.
- [5] Hamid and F. Yuda, "Studi Analisa Tingkat Keamanan Hotspot pada Jaringan FTI UII," *Universitas Islaman Indonesia*, 2013.
- [6] T. Mekhaznia and A. Zidani, "Wi-Fi security analysis," *Procedia Computer Science* 73, p. 172-178, 2015.
- [7] P. Jindal and B. Singh, "Quantitative analysis of the security performance in wireless LANs," *Journal of King Saud University - Computer and Information Sciences*, p. 23, 2015.
- [8] A. Arabo, "Cyber Security Challenges within the Connected Home Ecosystem Futures," *Procedia Computer Science* 61, p. 227 - 232, 2015.
- [9] S. Chakravarty, G. Portokalidis, M. Polychronakis and A. D. Keromytis, "Detection and analysis of eavesdropping in anonymous communication networks," *Int. J. Inf. Secur.*, p. 205-220, 2015.
- [10] J. A. R. P. d. Carvalho, H. Veiga, C. F. R. Pacheco and A. D. Reis, "Performance evaluation of laboratory wi-fi ieee 802.11a wpa point-to-multipoint links," *Procedia Technology* 9 (, p. 146-151, 2013.
- [11] S. Safavi, Z. Shukur and R. Razali, "Reviews on Cybercrime Affecting Portable Devices Seyedmostafa," *Procedia Technology* 11 (, p. 650-657, 2013.
- [12] S. S. Wagh, A. More and P. R. Kharote, "Performance Evaluation of IEEE 802.15.4 Protocol Under Coexistence of WiFi 802.11b," *Procedia Computer Science* 57, p. 745-751, 2015.

Wi-Fi Security Level Analysis for Minimizing Cybercrime

ORIGINALITY REPORT

1%

SIMILARITY INDEX

PRIMARY SOURCES

1	wirelesstradein.org Internet	34 words — 1%
2	Dale Liu Lead Author. "SSH Client Basics", Next Generation SSH2 Implementation, 2009 Crossref	12 words — < 1%
3	www.tehnoplus.me Internet	8 words — < 1%

EXCLUDE QUOTES OFF
EXCLUDE BIBLIOGRAPHY OFF

EXCLUDE MATCHES OFF