IJSER PUBLICATIONS

International Journal of Scientific and Engineering Research

Volume 8, Issue 3, March 2017

ISSN 0222-9552

Website : www.ijser.org
Email: ijser.editor@ijser.org

Journal Information

SUBSCRIPTIONS

The International Journal of Scientific and Engineering Research (Online at www.ijser.org) is published monthly by IJSER Publishing, Inc., France/USA/India

Subscription rates for academic Institutes:
Print: $150 per issue.
To subscribe, please contact Journals Subscriptions Department, E-mail: sub@ijser.org

SERVICES

Advertisements
Advertisement Sales Department, E-mail: service@ijser.org

Reprints (minimum quantity 100 copies)
Reprints Co-ordinator, IJSER Publishing.
E-mail: ijser.editor@ijser.org

COPYRIGHT

PRODUCTION INFORMATION

For manuscripts that have been accepted for publication, please contact:
E-mail: ijser.secretary@ijser.org

Potential Threat Analysis Hypertext Transfer Protocol and Secure Hypertext Transfer Protocol of Public WiFi Users (Batam Case)

CosmasEkoSuharyanto, PastimaSimanjuntak

Abstract—Computer network security has became an international issue in the last decade. We can not deny the ability of a network administrator is increasingly needed to secure the system. One of the important skills that must be possessed is able to read the data packets in computer network traffic. Protocol analysis needed to monitor and analyze information from any data packets that are sent or received on the network. From the user side, are required to have knowledge of information security, especially if accessing via free public wifi. The purpose of this study is to provide and analizethe captured HTTP and HTTPS packets using a network packet analyzer tool. The Object of this research is user of public wifi in the city of Batam, Indonesia. The study resulted a comprehensive analysis of data packets, we obtained user behavior when accessing information via public wifi. Despite many sites have been using secure protocols such as HTTPS but there are still using standard protocols resulting information open to hackers.

Index Terms—packet sniffer, sniffing, internet security, public wifi, man in the middle (MITM)

1 Introduction

Wireless technologies have become increasingly popular in our everyday business and personal lives[1]. Various types of wireless networks and technologies allow devices to speak (send data) to each other and to the web (TCP/IP Networks) without cables.Wireless technologies promise to offer even more features and functions in the next few years, especially Wireless Fidelity (WiFi). WiFi uses radio waves (RF) to allow two devices to communicate with one another. The technology is most commonly used to connect Internet routers to devices like computers, tablets and phones; however, it can be used to connect together any two hardware components.Smart phones are now heavily used for data communications, such as messaging, browsing web sites, and even streaming audio and video files.

Indonesian's Internet Service Providers Association (APJII) recently released a survey about internet users in Indonesia year 2016. According the survey, from 92.8 millions users; 17.7 millions (13.3%) access internet from their home, 14.9 millions (11.2%) access from their office, 2.9 millions access from their campus, 2.1 millions access from Paid Internet Café and 1.2 millions (0.9%) access from free public wifi (internet park, free internet café)[2].Still from the survey, about 20.8% or 27.6 millions usethe internet related to their work and 47.6% or 63.1 millions use smartphone to access the internet.

Based on the survey, therefore, wireless network security systems are increasingly required at this time along with the increasing use of smartphones to access a lot of information from the internet.

2 Network Protocols

2.1 Hypertext Transfer Protocol

The Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems. HTTP has been in use by the World-Wide Web global information initiative since 1990. The first version of HTTP, referred to as HTTP/0.9, was a simple protocol for raw data transfer across the Internet[3], [4]. The current version of the protocol is HTTP/1.1, which adds a few extra features to the previous 1.0 version. HTTP provides a general framework for access control and authentication, via an extensible set of challenge-response authentication schemes, which can be used by a server to challenge a client request and by a client to provide authentication information[5].

HTTP defines methods to indicate the desired action to be performed on the identified resource. What this resource represents, whether pre-existing data or data that is generated dynamically, depends on the implementation of the server.The HTTP/1.0 specification[6] defined the GET, POST and HEAD methods and the HTTP/1.1[7] specification added 5 new methods: OPTIONS, PUT, DELETE, TRACE and CONNECT.

2.2 Hypertext Transfer Protocol Secure

HTTP (RFC2616) was originally used in the clear on the Internet. However, increased use of HTTP for sensitive applications has required security measures. SSL, and its successor TLS (RFC2246) were designed to provide channel-oriented security. This document describes how to use HTTP over TLS[8] or HTTP Secure (HTTPS).HTTPS connections were primarily used for payment transactions on the World Wide Web, e-mail and for sensitive transactions in corporate information systems[9]. In the late 2000s and early 2010s, HTTPS began to see widespread use for protecting page authenticity on all types of websites, securing accounts and keeping user communications, identity and web browsing private.In order to create an HTTPS message, then, the sender integrates the sender's preferences with the receiver's preferences. The result of this is a list of cryptographic enhancements to be applied and keying material to be used to apply them. This may require some user intervention[9].

3 Packet Sniffer

Packet sniffer is a program running in a network attached device that passively receives all data link layer frames passing through the device's network adapter[10], [11]. It is also known as Network or Protocol Analyzer or Ethernet Sniffer.Packet sniffing or packet analysis is the process of capturing the information transmitted across network. Packet Sniffing mainly used in network management, monitoring and ethicalhacking[4], [12], [13].

Wireshark,is the world's foremost and widely-used network protocol analyzer.Wireshark development thrives thanks to the volunteer contributions of networking experts around the globe and is the continuation of a project started by Gerald Combs in 1998[14].Wireshark excels in the number of protocols that it supports. These range from common ones like IP and DHCP to more advanced proprietary protocols like AppleTalk and BitTorrent. And because Wireshark is developed under an open source model, new protocol support is

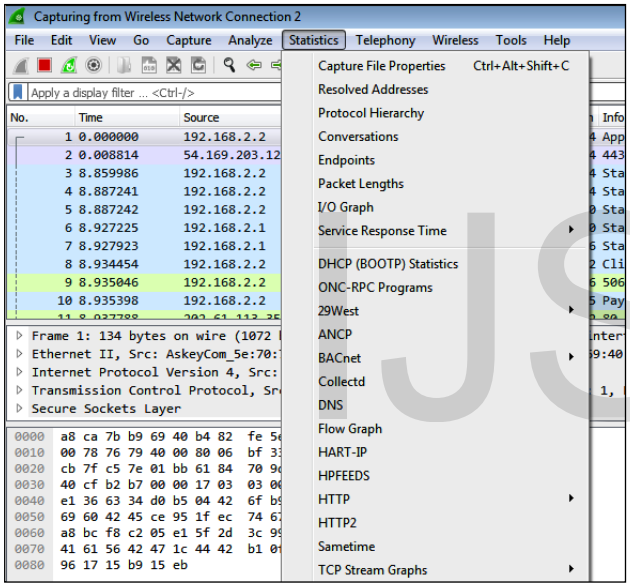

Figure 1.Wireshark Interface

added with each update.Wireshark has two filtering languages: one used when capturing packets, and one used when displaying packets. Display filters allow to concentrate on the packets that the administrator is interested in, while hiding the currently uninteresting ones. Packets can be selected on the basis of protocol, the presence of a field, the values of fields, comparison between fields etc[13].

Ettercap,is an open source Unix tool licensed under the GNU General Public License. It can be used for security checking and network analysis. It can stop the traffic in a part of the network, capture passwords and peform a man in the middle attack[15], [16]. There are many useful features included in the Ettercap that enables it to recognize the OS, open ports, IP and MAC addresses on the other computers in the network.Since it incorporates a variety of features necessary for working in switched environments, ettercap has evolved into a powerful tool that allows the user to launch several different types of man-in-the-middle (MITM) attacks. In addition, ettercap makes available many separate classic attacks and reconnaissance techniques within its interface[17].Ettercap works by putting the network interface into promiscuous mode and by

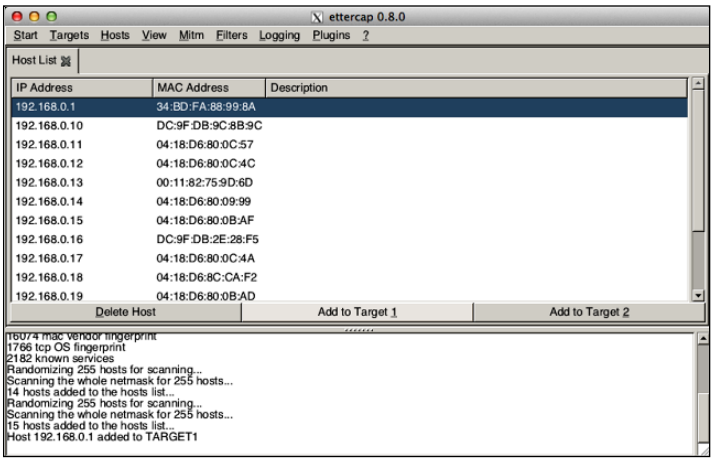

Figure 2.Ettercap Interface

ARP poisoning the target machines. Thereby it can act as a MITM and unleash various attacks on the victims. Ettercap has plugin support so that the features can be extended by adding new plugins[18].

4 Network Traffic Capturing Method

Network traffic analysis could be defined as: "the inference of information from observation of the network traffic data flow". Analysis in general, and hence network traffic analysis, can be categorized by time (or frequency) criteria and by the purpose of the analysis. Time based analysis categorization regarding time and frequency criteria, any network traffic analysis can be classified in one of the following three categories: real-time analysis, batched analysis and forensics analysis[10].

In this research, first step, we run an ARP-Poisonning to the

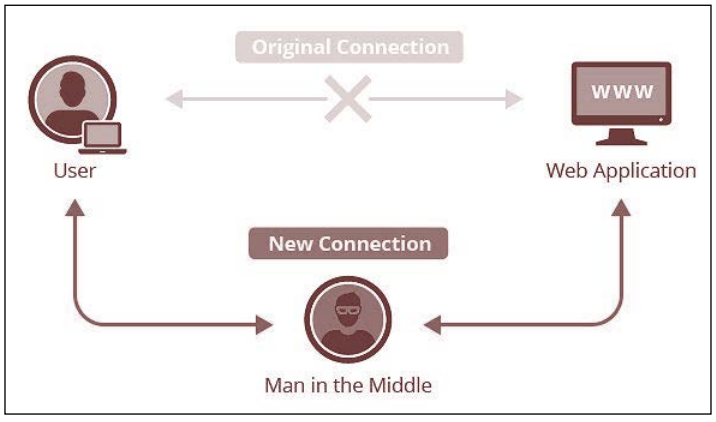

Figure 3. MITM Attack Scheme

target Router-Accespointthen capture the packets using Wireshark. By manipulating the ARP cache on each victim host, it is possible to change the normal direction of traffic between two hosts, and redirect it to flow through our machine instead.

Network data inspection techniques obtain information of network data by inspecting network header fields of each packet, compute them and produce outputs or results. Packets are decoded and presented in a human readable way.

5 Public Wifi in Batam, Indonesia

Batam is small island located between the waters of the Straits of Malacca and Singapore Straits. Batam serve as regional free trade zone (FTZ) then made famous Batam in terms of industrial development. Batam as a major city in western Indonesia that has become a Smart City. The application of information technology has also greatly expanded rapidly. Even been proposed since a few years ago Batam as Digital Island[19].

In terms of telecommunications infrastructure, the government of Batam provides free internet hotspots in some strategic places, called Taman Internet (Internet Park).In addition, Batam also has many shopping centers that provide free hotspots. With a lot of consideration on a representative sample based on research prinsiples, we decided to conduct this study in seven shopping centers and five internet parks.

6 Result and Analysis

Total packet data we captured are around 2,868,880 packets. We merge the packet as necessary to facilitate the analysis process.

Table 1
Captured Packets

Shopping Centers (Mall)		Internet Parks	
BCS Mall	203.130	Engku Putri	392.500
DC Mall	65.155	Sagulung	222.269
Kepri Mall	176.284	Taman Makam Pahlawan	218.343
Mega Mall	106.809	Tiban	11.080
Nagoya Hill	623.199	Lubuk Baja	118.824
Panbil Mall	26.291		
Top 100 Tembesi	693.916		

6.1 TCP Protocol Hierarchy

Hierarchy Protocol analysis was conducted to see the complete protocol hierarchy along with the total package of the data it contains. The Transmission Control Protocol (TCP) is one of the main protocols of the Internet protocol suite.Based on **Figure 4** it can be seen that the total of TCP protocol is 56.48%. As a protocol stack, TCP consists of several protocols. HTTP (Hypertext Transfer Protocol) consisting of 2.0% smaller than the secure protocol (HTTPS) with 22.63%.In general most free publicwifi' user in Batam use the Internet to access the encrypted content. These findings will be explored further in the analysis of the HTTP and HTTPS on further discussion.

Display filter: none

Protocol	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Transmission Control Protocol	1620438	1500735971	0.007	903994	585795929	0.003
Hypertext Transfer Protocol	57495	57892799	0.000	47277	52377506	0.000
Secure Sockets Layer	649288	855618924	0.004	640988	846254723	0.004
Data	8633	922270	0.000	8633	922270	0.000
XMPP Protocol	30	5934	0.000	30	5934	0.000
Domain Name Service	837	470822	0.000	822	468572	0.000
Socks Protocol	87	10579	0.000	87	10579	0.000
Remote Procedure Call	2	220	0.000	0	0	0.000
Session Initiation Protocol	1	289	0.000	1	289	0.000
TURN Channel	46	6874	0.000	0	0	0.000
Malformed Packet	1	65	0.000	1	65	0.000
GSM over IP protocol as used by ip.access	2	164	0.000	0	0	0.000
Short Message Peer to Peer	16	10336	0.000	15	10170	0.000
DG Gryphon Protocol	3	264	0.000	0	0	0.000
REsource LOcation And Discovery Framing	3	502	0.000	3	502	0.000
User Datagram Protocol	26600	5392305	0.000	0	0	0.000
Internet Control Message Protocol	10592	957134	0.000	10592	957134	0.000
Internet Group Management Protocol	1925	101612	0.000	1925	101612	0.000
Address Resolution Protocol	191874	8150840	0.000	191874	8150840	0.000
Internet Protocol Version 6	1845	199966	0.000	0	0	0.000

Figure 4. TCP Protocol Hierarchy

6.2 IP Conversation Analisys

Conversation analysis is used to look at the specifics of traffic between the two endpoints. Conversation analysis will be divided into two categories of objects of research; Shopping Centers (Mall) and Internet Parks.

First, on the object Shopping Centers,look at he**Figure 5**, user with IP address 192.168.43.64 communicated with the IP Address 114.4.4.207 with the highest total data packets (85,503 packets), using IP Lookup facility it can be recognized that the IP Address 114.4.4.207 is hostname *cache.google.com*, the ISP location in Jakarta, PT IndosatTbk.Next, the user with the IP

IPv4 Conversations

Address A	Address B	Packets	Bytes	Packets A→B	Bytes A→B
114.4.4.207	192.168.43.64	85 503	124 183 657	85 503	124 183 657
74.125.171.220	192.168.3.45	21 058	30 523 922	21 058	30 523 922
173.194.51.199	192.168.3.45	20 214	29 118 130	20 214	29 118 130
173.194.49.44	192.168.3.94	16 788	23 477 712	16 788	23 477 712
192.168.3.77	219.83.126.59	11 022	13 070 836	0	0
114.4.39.200	192.168.43.218	9 781	14 125 790	9 781	14 125 790
192.168.21.20	192.168.21.254	9 673	5 709 248	3 485	363 656
192.168.3.139	192.168.3.254	9 037	5 200 982	4 446	480 574
192.168.41.194	219.83.126.59	9 003	12 389 747	0	0
31.13.79.208	192.168.43.218	8 275	9 405 510	8 275	9 405 510
173.194.49.47	192.168.3.99	8 210	11 968 244	8 210	11 968 244
13.107.4.50	192.168.3.53	7 990	9 898 452	7 990	9 898 452
192.168.41.194	219.83.126.58	7 427	8 582 599	0	0
74.125.171.202	192.168.3.60	7 236	10 441 660	7 236	10 441 660
74.125.200.141	192.168.41.190	7 140	10 238 921	7 140	10 238 921
107.155.58.70	192.168.41.212	6 940	10 500 612	6 940	10 500 612
74.125.130.132	192.168.3.94	6 145	6 731 400	6 145	6 731 400
192.168.3.53	219.83.126.59	6 050	7 095 662	0	0

Figure 5. IP Conversations (Object Shopping Centers)

address 192.168.3.45 that perform data communications with the IP Address 74.125.171.220 (21,058 packets), IP Lookup facility did not mention the hostname of the IP Address yet, this IP geographically located in North America and owned by Google Inc.In the next dominant position is the communication between the IP address 192.168.3.45 with 173.194.51.199 (20,214 packets), same with the previous IP Address, IP is also owned by Google Inc.

Second, on the object Internet Park, in this analysis we conducted a check list 'name resolution' on the Wireshark interface that can instantly known owner of the IP address.As shown in **Figure 6**, users with IP address 192.168.1.6 communicated with the IP address 74.125.102.28 (googlevideo.com). IP address 192.168.1.103 communicated with the IP Address 118.98.36.145 (googlevideo.com). Furthermore, the IP address 192.168.1.106 with 58,961 packets to communicate with IP Ad-

dress 31.13.79.227 (fbcdn.net).

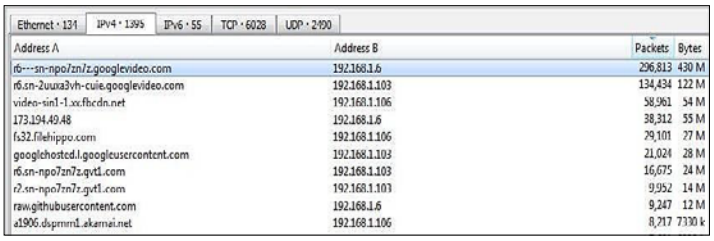

Figure 6. IP Conversations (Object Internet Parks)

6.3 Hypertext Transfer Protocol (HTTP) Analysis

Each protocol in the network, work together, in real time, therefore, has a track each, or in terms of computer science is called as port. The HTTP protocol occupy port 80 in the computer system, and on this analysis, we will analyze user behavior when they surf the Internet, so we will find relevance to the security of the information that will be discussed here.

The total packets of data we filtered in particular on the HTTP protocol with research object Shopping Center (Malls) 15,392 packets, or 0.8% of the total data packet.Then we rank top 10 destination website based on highest total packets.

Table 2
Top 10 Destination Website (Object Shopping Centers)

No	*Websites*	*Packets*	*Packets (bytes)*	*Note*
1	http://indosat.net.id/	4403	6361	Internet Services Provider
2	http://microsoft.com/	1501	2196	Microsoft
3	http://akamaitechnologies.com/	1402	2117	*content delivery network provider*
4	http://indosat.net.id/	1164	1673	Internet Services Provider
5	http://indosat.net.id/	841	1184	Internet Services Provider
6	http://indosat.net.id/	843	898	Internet Services Provider
7	http://akamaitechnologies.com/	608	864	*content delivery network provider*
8	http://indosat.net.id/	769	828	Internet Services Provider
9	http://buanalintas.co.id	525	784	Internet Services Provider
10	http://aws.amazon.com	474	678	cloud computing provider

Based on the data obtained on **Table 2**, it can be concluded that users who take advantage of free wifi internet connection at the location of shopping centers (malls) are more inclined to open up business sites. This is understandable because when a team of researchers conducted observations directly to the location of shopping centers, most users take advantage of wifi cafes are generally dominated by business people.

On Internet Park, we obtained 10,768 packets or 1.1% of total packets. Based on the data we presented clearly on **Table 3**, it can be foundthe behavior of Internet users on location of Internet Park in Batam. Most users are more likely to use it to search for information, such as www.google.com as a popular search sites, software center www.fillehippo.com. It can also be observed that the subsequent tendency to get information about education, for example online bookstore, online journals, etc. This is confirmed that most users of free wifi in the park are students.

Table 3
Top 10 Destination Website (Object Internet Parks)

No	*Websites*	*Packets*	*Packets (bytes)*	*Note*
1	www.google.com	369	302	Search engine
2	http://adskom.com/	467	294	Digital Advertisment publisher
3	http://filehippo.com/	298	256	Download center
4	http://library.binus.ac.id/	273	224	University
5	http://swiftserve.com/	262	205	Multimedia
6	http://bukukita.com/	255	193	Online bookstore
7	http://alfaonline.com/	283	182	mall online
8	http://www.doubleclickbygoogle.com/	240	178	Digital service provider
9	http://akamai.com/	256	166	Content Delivery Network
10	http://andipublisher.com	202	129	Online book publisher

6.4 Hypertext Transfer Protocol Secure Analysis

Compared with HTTP packets, https have larger percentage. Total HTTPS packet in Shopping Centers is 131,353 packets or 6.9%.

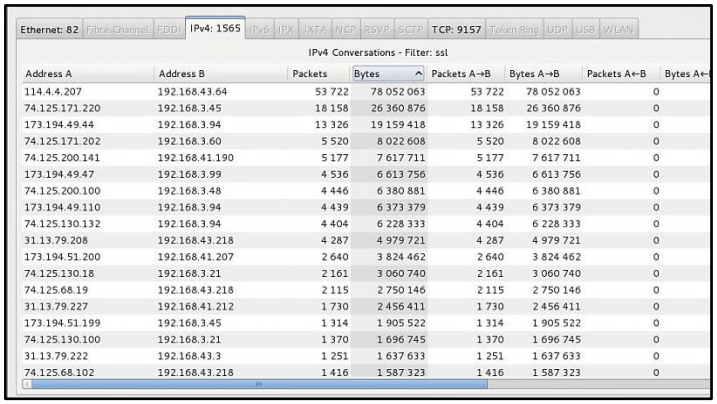

Figure 7. IP Conversation HTTPS (Object Shopping Centers)

Basen on **Figure 7**, we obtained information of the sites with highest data communications activity (in bytes), and to

easily find what sites are most total bytes of data, we also includes the hostname of the IP Address (**Table 3**).**Table 3** shows us that Google dominates the data communications activity in the object Shopping Center then followed by Facebook.

Table 4
Top 10 Websites Destination

No.	*Nama Situs*	*Packet*	*Packets (Bytes)*	*Note*
1	114.4.4.207 (https://google.com)	53722	78052	Google Inc
2	74.125.171.220 (https://google.com)	18158	26360	Google Inc
3	173.194.49.44 (https://google.com)	13326	19159	Google Inc
4	74.125.171.202 (https://google.com)	5520	8022	Google Inc
5	74.125.200.141 (https://google.com)	5177	7617	Google Inc
6	173. 194.49.47 (https://google.com)	4536	6613	Google Inc
7	74.125.200.100 (https://google.com)	4446	6380	Google Inc
8	173. 194.49.110 (https://google.com)	4439	6373	Google Inc
9	74.125.130.132 (https://google.com)	4404	6228	Google Inc
10	31.13.79.208 (https://facebook.com)	4287	4979	Social Media

Now, we look at Internet Park data, total packet is 974,096 or 27.4%. Based on **Figure 8**, we obtained information of the sites with highest data communications activity (in bytes), and to easily find what sites are most total bytes of data, we also includes the hostname of the IP Address in **Table 4**.

Table 4 provides information that Google is still the dominant sites**,** nextis the social media sites Facebook and internet service provider Telkom.This is not surprising because social media users in Indonesia is very high compared to countries

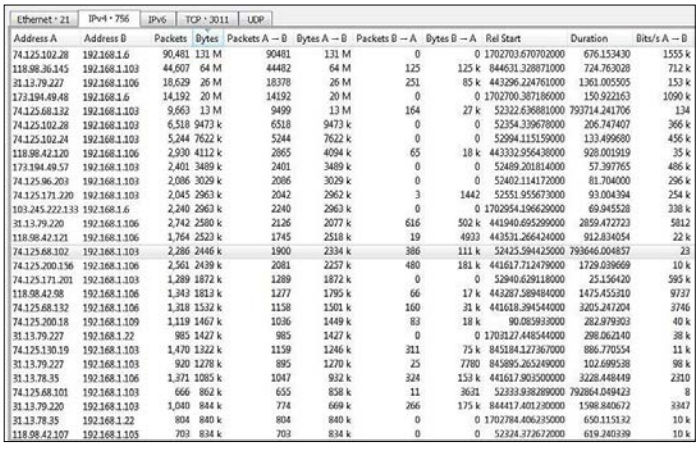

Figure 8. IP Conversations HTTPS (Object Internet Park)

in Southeast Asia. We were lucky because all social media websites are now using a secure protocol.

Table 5
Top 10 Website

No.	*Nama Situs*	*Paket*	*Bytes*	*Keterangan*
1	https://google.com/ (74.125.102.28)	90.481	131.000	Google Inc
2	https://www.telkom.net.id/ (118.98.36.145)	44.604	64.000	Internet Service Provider
3	https://facebook.com/ (31.13.79.227)	18.629	26.000	Social Media
4	https://google.com/ (173.194.49.48)	14.192	20.000	Google Inc
5	https://google.com/ (74.125.68.132)	9.663	13.000	Google Inc
6	https://google.com/ (74.125.102.28)	6.518	9.473	Google Inc
7	https://google.com/ (74.125.102.24)	5.244	7.622	Google Inc
8	https://www.telkom.net.id/ (118.98.42.120)	2.930	4.112	Internet Service Provider
9	https://google.com/ (173.194.49.57)	2.401	3.489	Google Inc
10	https://google.com/ (74.125.96.203)	2.086	3.029	Google Inc

We can also show the comparison between HTTP and HTTPS in the following diagram (Figure 9 and 10).

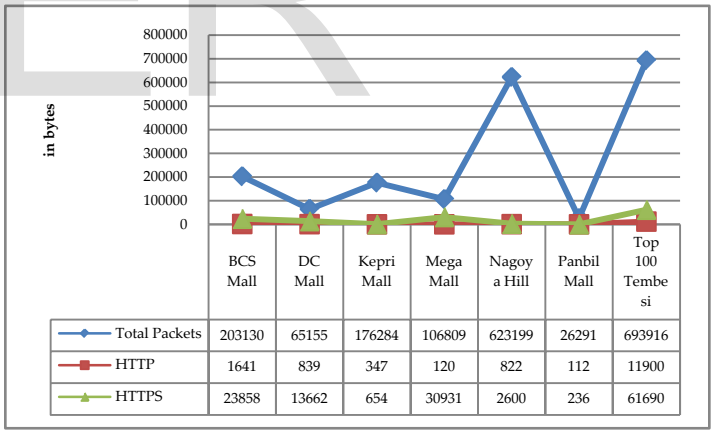

Figure 9. HTTP and HTTPS Packets (Object Shopping Centers)

Figure 9 illustrates a comparison of the data packets of HTTP and HTTPS protocols in Shopping Centers and **Figure 10** describes a comparison of the data packets of HTTP and HTTPS protocols in Internet Park.

Based on these findings, we can study the behavior of people of the city of Batam when accessing the internet in public wifiplaces.Yes, the percentage of users who access theencrypted sites is much higher thanunencrypted one, but we also found some potential risks should be of concern when accessing information in public wifi places.

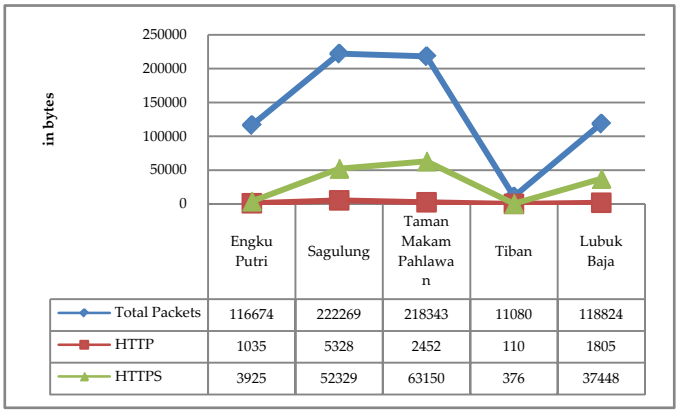

Figure 10. HTTP and HTTPS Packets (Internet Parks)

6.5 Potential Threats Found

The next analysis is to look at the association between the userbehaviorandthe potential threats to information security. This step conducted by analyzing the HTTP POST method, because this method is a method of sending databetween host and servers or destination websites.

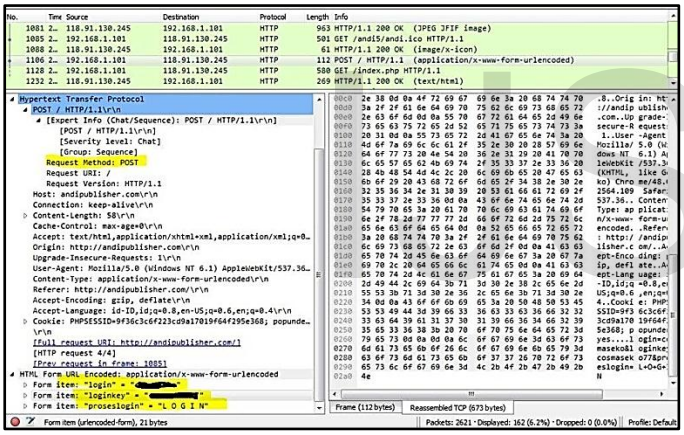

Figure 11. Login Account Information

This method is often the entry point for the sniffer to intercept the information as shown in **Figure 11**.Based on the findings of the research team, although the percentage is very small,the following is some information that is harmful to user and should not be accessed from free public wifi.

Table 6.
Website with Login Information

No	*Websites*	*HTTPS*	*Note*
1	https://ibank.klikbca.com/	✓	Bank Account
2	http://sia.upbatam.ac.id/siad/login.php	×	Campus login/ LMS
3	https://google.co.id	✓	Google account
4	http://www.bukukita.com/	×	Online Bookstore
5	https://ssl.olx.co.id/masuk/	✓	Ecommerce
6	https://www.telkom.net.id/	✓	ISP
7	http://belbuk.com/	×	Online Bookstore
9	https://facebook.com	✓	Social Media
10	https://www.amazon.com/	✓	Ecommerce
	ap/signin?		
11	http://library.binus.ac.id/	×	Login campus library
12	http://andipublisher.com/	×	Publisher
13	http://elsevier.com/	✓	Journal
14	http://sekolahkoding.com/	×	LMS
15	http://lppm.itb.ac.id/	×	LMS
17	http://www.alfaonline.com/	×	Ecommerce
18	https://login.kompas.com/	✓	Login to Sites
19	http://scopus.com/	✓	Journal

7 Conclussion

Based on the findings of the research presented in the discussion and analysis above, we conclude that the users of public wifi in Batam accessed an encrypted site is greater than the unencrypted sites. However, we also found some users still access the information that is risky (such as Login account) in free public wifi areas. Although some websites with a 'login account' has been using a secure protocol, we were advised to remain cautious when accessing via publicwifi.

Reference

[1] T. Karygiannis and L. Owens, "Wireless network security 802.11, bluetooth and handheld devices," *NIST Spec. Publ.*, vol. 128, pp. 800–48, 2002.

[2] APJII, "Penetrasi & Perilaku Pengguna Internet Indonesia," Jakarta, 2016.

[3] G. Sadasivan, J. Brownlee, B. Claise, and J. Quittek, "Architecture for IP flow information export." [Online]. Available: https://tools.ietf.org/html/rfc7235. [Accessed: 11-Mar-2017].

[4] C. Sanders, *PR AC T I C A L PAC K E T A N A LY S I S WIRESHARK TO SOLV E RE A L-WORLD*, 2nd ed. San Francisco: William Pollock, 2011.

[5] R. Fielding *et al.*, "RFC 2616 - Hypertext Transfer Protocol - HTTP/1.1," *Internet Soc.*, no. 2616, pp. 1–114, 1999.

[6] R. T. Fielding, T. Berners-Lee, and H. Frystyk, "Hypertext Transfer Protocol -- HTTP/1.0." [Online]. Available: https://tools.ietf.org/html/rfc1945. [Accessed: 11-Mar-2017].

[7] P. J. Leach, T. Berners-Lee, J. C. Mogul, L. Masinter, R. T. Fielding, and J. Gettys, "Hypertext Transfer Protocol -- HTTP/1.1." [Online]. Available: https://tools.ietf.org/html/rfc2616#section-9. [Accessed: 11-Mar-2017].

[8] E. Rescorla, "HTTP Over TLS." [Online]. Available: https://tools.ietf.org/html/rfc2818. [Accessed: 12-Mar-2017].

[9] E. Rescorla and A. Schiffman, "The Secure HyperText Transfer Protocol." [Online]. Available:

https://tools.ietf.org/html/rfc2660. [Accessed: 12-Mar-2017].

[10] H. P. Pallavi Asrodia, "Network Traffic Analysis Using Packet Sniffer," *Int. J. Eng. Res. Appl.*, vol. 2, no. 3, pp. 854–856, 2012.

[11] M. A. Qadeer, M. Zahid, A. Iqbal, and M. R. Siddiqui, "Network Traffic Analysis and Intrusion Detection Using Packet Sniffer," *Commun. Softw. Networks, 2010. ICCSN '10. Second Int. Conf.*, pp. 313–317, 2010.

[12] P. Asrodia and V. Sharma, "Network Monitoring and Analysis by Packet Sniffing Method," *Int. J. Eng. Trends Technol.*, vol. 4, no. May, pp. 2133–2135, 2013.

[13] U. Banerjee, A. Vashishtha, and M. Saxena, "Evaluation of the Capabilities of WireShark as a tool for Intrusion Detection," *Int. J. Comput. Appl.*, vol. 6, no. 7, pp. 975–8887, 2010.

[14] Gerald Combs, "Wireshark · Go Deep." [Online]. Available: https://www.wireshark.org/. [Accessed: 12-Mar-2017].

[15] M. V. Alberto Ornaghi, "Ettercap Home Page." [Online]. Available: https://ettercap.github.io/ettercap/index.html. [Accessed: 12-Mar-2017].

[16] R. Wagner, "Address Resolution Protocol Spoofing and Man-in-the-Middle Attacks," 2003.

[17] M. Dunker, "ettercap Primer," 2004.

[18] G. Kaur, "Comparative Investigation of ARP Poisoning Mitigation Techniques using Standard Testbed for Wireless Networks," *Int. J. Comput. Appl.*, vol. 121, no. 13, pp. 15–19, 2015.

[19] Ahmad Dahlan, "Wujudkan Batam sebagai The Smart City." [Online]. Available: https://kominfo.go.id/index.php/content/detail/4800/Wujudkan+Batam+sebagai+The+Smart+City/0/sorotan_media. [Accessed: 12-Mar-2017].

AUTHOR

CosmasEkoSuharyanto

■Master of Information System Management, Bina Nusantara University, Jakarta 2015
■Certified Cisco CCNA Instructor, Electrical Engineering and Information Technolgy Dept. GadjahMada University 2016
■Lecturer of Computer Science at PuteraBatamUniversity, Batam-Indonesia
■ Email: costmust@gmail.com

PastimaSimanjuntak

■Master of Information System, STMIK PuteraBatam 2012
■Secretary of Research Department of PuteraBatam University
■Lecturer of Computer Science at PuteraBatam University, Batam-Indonesia
■ Email: p.lastria@gmail.com

CERTIFICATE *of* PUBLICATION

THIS ACKNOWLEDGES THAT

Cosmas Eko Suharyanto

HAS SUCCESSFULLY PUBLISHED RESEARCH PAPER

Potential Threat Analysis Hypertext Transfer Protocol and Secure Hypertext Transfer Protocol of Public WiFi Users (Batam Case)

MARCH
2017

Dr. Alex R. Mathews | John Britto

Members | IJSER Review Board Panel | www.ijser.org

IJSER
WWW.IJSER.ORG

International Journal of Scientific and Engineering Research (IJSER)

ACCEPTANCE LETTER

Paper Number: I097306
Paper Title: Potential Threat Analysis Hypertext Transfer Protocol and Secure Hypertext Transfer Protocol of Public WiFi Users (Batam Case)
Authors: Cosmas Eko Suharyanto, Pastima Simanjuntak

Type of the paper: (Please highlight)

☐ Research ☐ Application ☐ Case Study ☐ Survey ☐ On-going ☐ Other

Evaluation: (Please highlight)

	Low				High
Significance of Contribution:	1	2	3	4	5
Originality of Content:	1	2	3	4	5
Technical Quality:	1	2	3	4	5
Clarity of Presentation:	1	2	3	4	5

Overall recommendation (Please highlight)

Accept in current state
Accept with minor revision
Major Revision needed, recommend resubmission
Reject

Any additional comments: Paper Published in IJSER Volume 8, Issue3, March 2017 Edition (ISSN 2229-5518).

IJSER

Digitally signed by IJSER
DN: cn=IJSER, c=FR, o=IJSER Publishing, ou=Research, email=ijser.editor@ijser.org