International Journal of Internet, Broadcasting and Communication Vol.8 No.4 26-38 (2016)
http://dx.doi.org/10.7236/IJIBC.2016.8.4.26

IJIBC 16-4-x

Android Network Packet Monitoring & Analysis Using Wireshark and Debookee

Mi-Hwa Song

Division of Information and communication technology, Semyung University, Jechon, Korea
e-mail: mhsong@semyung.ac.kr

Abstract

Recently, mobile traffic has increased tremendously due to the deployment of smart devices such as smartphones and smart tablets. Android is the world's most powerful mobile platform in smartphone. The Android operating system provide seamless access to many applications and access to the Internet. It would involve network packet sharing communicated over the network. Network packet contains a lot of useful information about network activity that can be used as a description of the general network behaviours. To study what is the behaviours of the network packet, an effective tools such as network packet analyzers software used by network administrators to capture and analyze the network information. In this research, more understanding about network information in live network packet captured from Android smartphone is the target and identify the best network analyzer software.

Keywords: *Network Packet Monitoring, Android Network Monitoring, Network Packet Analysis Software, Android Platform.*

1. Introduction

Smartphones are steadily gaining popularity, creating new application areas as their capabilities increase in terms of computational power, sensors and communication. Smartphone traffic shows increased tremendously share of Internet traffic. Cellular traffic is projected to grow 10 times faster than fixed Internet traffic and most of this traffic is generated by smartphones. Android is one of the newer operating systems targeting smartphones but have lead to explosive growth in traffic over cellular networks. Mobile devices are used for various applications usually to browsing the Internet due to popularity of applications like Facebook, Skype, Online banking, email clients etc which keeps exchanging data with corresponding server. In cellular networks, mobile devices are communicating to share resources and data through a network. Network packets are units of data travelling in these networks and they carry all the important information from its source to its final destination. When we are browsing an Internet using a web browser like Google or Naver search portal using Android device, we just click the link and within a second the website will appear. We

Manuscript Received: Sep. 22, 2016 / Revised: Sep.26, 2016 / Accepted: Oct. 4, 2016
Corresponding Author: mhsong@semyung.ac.kr
Tel:+82-43-645-1645, Fax: +82-43-649-1747
Division of Information and communication technology, Semyung University, Jechon, Korea

don't know there are packet and protocols exchanges and many processes occurred behind that. How we use those packets to understand what's happening in the network?

To study all the processes occurred behind the network live packet, we need a specific software to capture and analysis the network packets. There are many network packet analyzer available but we don't know yet what are the best softwares that can give optimum performances in network packets capture and analysis. We also don't know what are the information that can be retrieved from network packet capture and analysis from live network on Android device.

Based on the above problem stated, the objectives of this research are:

1) To study the information on live network packet retrieved from network analyzer
2) To determine what are the best network packet analyzer
3) To make a comparison between at least two different network packet analyzer.

To explore and understand the information on the analysis on network packet that being captured by network analyzer software. This research will focus on:

- Network packet analysis on Android
- Debokee and Wireshark (network packet analyzer software)
- Analysis on captured network packets

2. Background

This topic is a review of the past and progressing research. It includes a review on packet analysis, packet analyzer softwares, network packet analyzer for Android, Android based smartphone and all reviews that are related to the research.

2.1 Packet Analysis

A packet analysis, also known as protocol analysis, network analysis, traffic analysis, packet sniffing, eavesdropping and others is the process of capturing network packet and learn from network information to determine what is happening on the network. It also involved monitoring process on a selected communication being conducted with a predetermined protocol by the exchange of protocol data units between two entities over a data network. According to Spangler and Ryan, packet sniffing is a technique of monitoring every packet that crosses the network [1].

2.2 Packet Analyzer

A packet analyzer or also can be identified as protocol analyzer or packet sniffer or packet analyzer is a program/ software that monitors data packets traveling over a network. The software will decode the data packets of common protocols in network traffic to readable format of network information. The protocol analyzer of the present invention is capable of displaying station level statistics, network statistics, real-time event information, and protocol distribution. It also for calculating and displaying protocol distribution in real-time in connection with monitoring data frames carried on a digital transmission network [2]. A packet sniffer is a piece of hardware or software that monitors all network traffic and can be operated in both switched and non-switched environment [3].

There are many packet analyzers available to help administrator's works become more easier. A simple search on the Internet shows number of analyzers available whether for Windows OS or Mac OS. Packet

analyzers can also be installed and accessed directly on some smartphones itself. Some of the most prominent are:

- **Wireshark**
  Wireshark is one of the best sniffers available and is being developed as a free, commercial-quality sniffer. It has numerous features, a nice graphical user interface (GUI), decodes over 400 protocols, and is actively being developed and maintained. It runs on UNIX-based systems, Mac OS X, and Windows. This is a great sniffer to use in a production environment.

- **Debookee**
  Debookee is a packet analyzer for OS X which has the ability to intercept network traffic through a Man-in-the-middle attack. Debookee will intercept traffic from any device on a network, including iPhone, iPad, Android, Blackberry, PC, Mac, and others. This enables users to analyze the traffic of devices that cannot support packet-capture, such as mobile, tablets, etc. With no network interruption, Debookee can complete a scan of your network and display IP addresses, MAC addresses, and vendors associated to discovered devices.

- **PRTG Network Monitor**
  PRTG network monitor is network monitoring software from Paessler AG. PRTG runs on Windows and monitors network availability and network usage using SNMP, Packet Sniffing, WMI, IP SLAs and Netflow and various other protocols. Since the release of PRTG 9, the software supports the monitoring of IPv6 devices. A web-based interface is available, as well as dedicated apps for iOS and Android

- **Ettercap**
  Ettercap was specifically designed to sniff a switched network. It has built-in features such as password collecting, OS fingerprinting and character injection, and runs on several platforms including Linux, Windows, and Solaris. It is actively maintained at ettercap.sourceforge.net.

- **Tcpdump**
  Tcpdump is the oldest and most commonly used network sniffer, and was developed by the Network Research Group (NRG) of the Information and Computing Science Division (ICSD) at Lawrence Berkeley National Laboratory (LBNL). It is command line-based and runs on UNIX-based systems, including Mac OS X. It is actively developed and maintained at www. Tcpdump.org.

According to ibm.com, Wireshark is by far the best GUI based open source packet analyzer [4]. This tool is extremely helpful for network administrators to know details like which all computers are trying to communicate with a machine. Wireshark also in the list of best free network analysis tools [5]. In fact, Wireshark is often considered the de facto standard among the industry.

Debookee delivers real-time packet capture analysis in a friendly graphical user interface. Instead of overwhelming the user with RAW packets, Debookee displays only the most important and vulgarized information usually found in the packet flow. As a result, Debookee supports extraction of requests details from HTTP, HTTPS, DNS, TCP, DHCP, SIP, and RTP protocols. Debookee analyzes the network traffic of any device in three easy steps [6]. First, Debookee scans the network and identifies the devices in use. The user then selects the device, or target, that they would like to be analyzed. With a simple click, Debookee provides a comprehensive report so users can analyze the traffic.

2.3 Monitor network packet for Android device

Nowadays, the operating system for mobile devices Android is taking a leading position within the world of smartphones and tablets. Android is Google's operating system for mobile devices. One of the most used features in this sense is the ability to transmit data between two devices through an internet connection.

2.3.1 Analysis and interpretation of emulated data traffic in Android platform [7]

The final goal is to find out how Android manages sending and receiving packets. To do this, after performing all the necessary tests, the results are deeply analyzed to empirically conclude which is the most appropriate connection type for the transmission of different traffic types, being Wi-Fi the best choice to transmit them. In the near future, applications will be able to optimize its performance by taking advantage of this knowledge. From the results obtained in the real tests, conclusions are going to be extracted about how Android treats the transmission and reception of packets. These conclusions will be targeted in each connection type, analyzing separately the emulator, Wi-Fi and 3G .

2.3.2 Monitoring network traffic for Android devices [8]

The same principles that organizations use to monitor network traffic go into their networks must be applied to the network traffic originating from mobile devices. This means that the techniques and tools, which would normally be used to collect and analyze network activity, can also be used to detect anomalous network traffic or network intrusions related to smartphones.

2.3.3 Android Malware Behaviors for Android Platform Using Interactive Labs

Alongside the growth of the operating system, malware for Android has increased tremendously. Currently, few strategies are available to identify and detect malware on this platform. It is included network packet analysis strategy it can help to identify possible attacks or malicious activity or finding unsecured and bloated applications. This paper discusses in detail four labs that have been developed by the author to familiarize the students with the Android platform and dynamic malware analysis technique.

As a conclusion, network packet analysis method is widely used in previous experiments to monitor the packet activities that travel over the network. The method also help to identify malware behaviours or any possible attacks activities that happen in the network. There are many network packet analyzers that can help to implement the network packet analysis. According to many reviews, Wireshark is the best and commonly used network analyzers nowadays.

3. Research Methodology

3.1 Analysis Framework for Packet analysis on Android

As packet analysis was performed, usually a good portion of the analysis will happen after the capture. Sometimes several captures need to be performed to get the better observation. There are few processes need to be done from the first to start to capture the network packets until the analysis results are obtained. Figure 1 shows how packet analyzer's processes are being done. There are two packet analyzers are used in this research which are Wireshark and Debookee. The processes in both softwares of network packet analysis are same as shown in Figure 1.

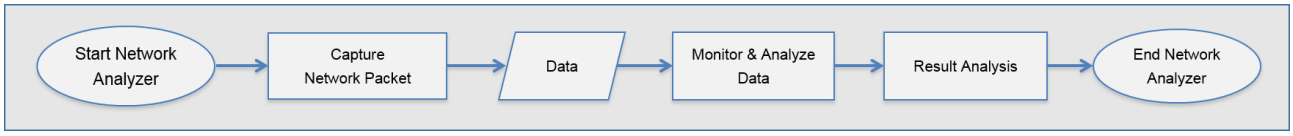

Figure 1. Analysis Flow Chart

3.2 System Architecture

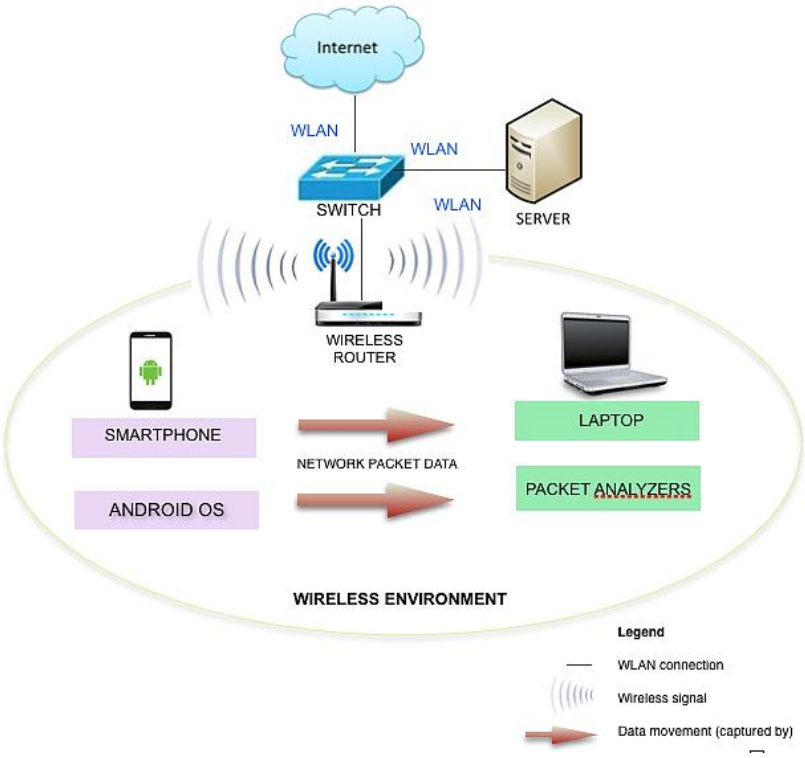

Figure 2. Android Network Packet Analysis System Architecture

Figure 2 shows network packet analysis in Android smartphone system architecture. The figure shows all components and connections involved in the analysis process. The connection used in this research is wireless connection which smartphone and laptop are connected in the same wireless network. The wireless connection is established from wireless router that is connected to the main source, the Internet. Two packet analyzers which are Wireshark and Debokee are installed in laptop to capture, monitor and analyze network packet from smartphone. The analyzers will capture network packet data coming from the smartphone.

3.3 Hardware and Software

This research requires some softwares and hardwares in order to get research objectives achieved. There are list of softwares and hardwares required:

Software	Wireshark, Debookee, Android Operating System
Hardware	Android Smartphone, Laptop, Wireless router

3.4 Setting up process

Figure 3. Set up process

The set up process in this research is simple as shown in Figure 3. Wireless router is used to distributes wireless connection to laptop and Android smartphone. The SSID (Service Set Identifier) name of wireless router is 'TPLINK'. Then, laptop and Android smartphone are connected to same wireless connection from the wireless router. The smartphone will browsing the Internet activities such as sending email, online banking, social networking and others and network analyzers which are Wireshark and Debookee that being installed in laptop will capture and monitor the network packet data that coming from the smartphone. Lastly, the network analyzers will do the analysis and retrieve network information from the packet data.

3.4.1 Installing Wireshark

In this research wireshark is one of the network analyzer that being used to capture and analyze network packets data. Wireshark is one of useful packet tool. Some of the features that Wireshark have:

- It has an easy-to-read and configurable GUI
- It can capture data from the network or read from a capture file
- It has rich display filter capabilities

Wireshark can be installed on Windows and Mac operating system. First, download the Wireshark software from its official website (www.Wireshark.org) [9]. Then, follow the all the installation instructions to install it in the laptop until the installation is finish. There are few interfaces of Wireshark below in Figure 4.

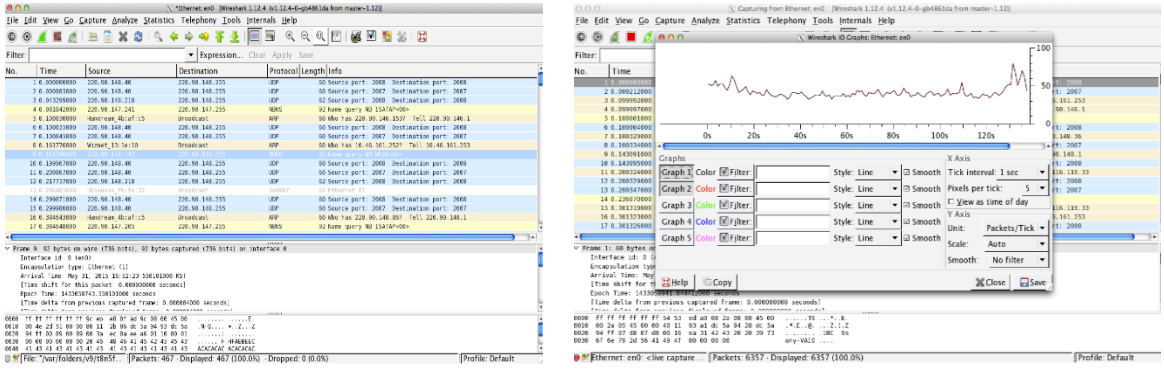

Figure 4. Wireshark network packet capture interface (left), IO Graphs (right)

3.4.2 Installing Debookee

Debookee is another network analyzer used in this research. Debookee is packet analyzer designed only for Mac OS X. It is still new in network analyzer software. The use of Debookee software is because want to explore its features and comparison of its performance with Wireshark will be made. Debookee provides some of the features which are:

- Scan and discover all devices currently active on a network
- Real time packet capture analysis of following protocols such as HTTP, HTTPS, DNS, TCP, DHCP and SIP.

Debookee only can be installed on Mac OS X operating system. First, download the Debookee software from its official website (ww.iwaxx.com) [10]. Then, follow the all the installation instructions to install it in the laptop until the installation is finish. There are few interfaces of Debookee below in Figure 5 and Figure 6.

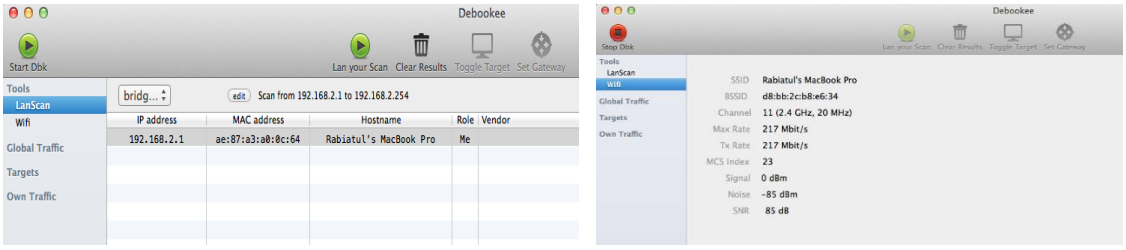

Figure 5. Debookee's start interface (left), Debookee's Wifi interface (right)

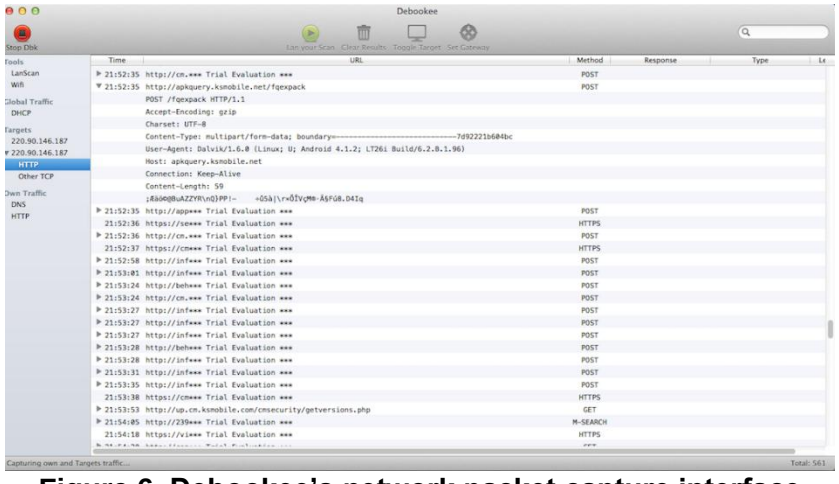

Figure 6. Debookee's network packet capture interface

4. Result and Analysis

This chapter discusses results and analysis from network packet data that being captured from both network analyzers, Wireshark and Debookee. There will be explanations on every network information retrieved. The analysis is made to study what is the best network analyzer between Wireshark and Debookee and their comparison.

4.1 Wireshark analysis

1) Browsing video (www.youtube.com)

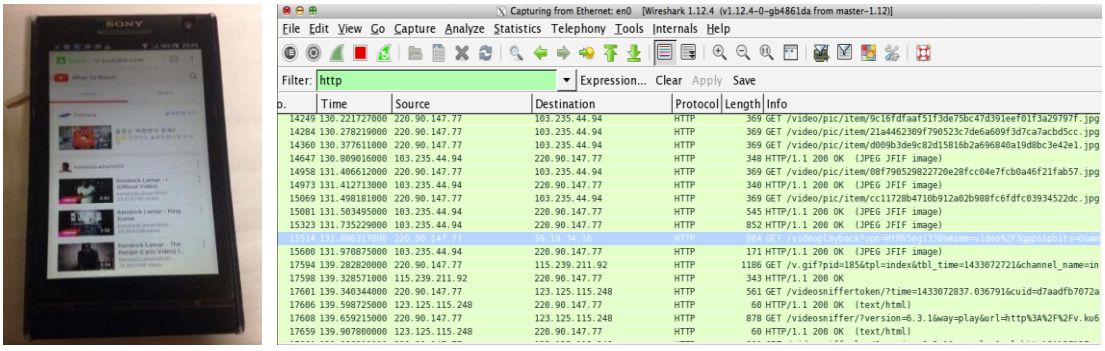

Figure 7. Watching video on youtube (left), Wireshark's packet list watching video from youtube (right)

Wireshark start to capture the network packet data coming from watching a video from youtube. Figure 8 may display the summary of table containing all packets in the current capture file, packet number, relative time the packet was captured, source and destination of the packet and packet's protocol.

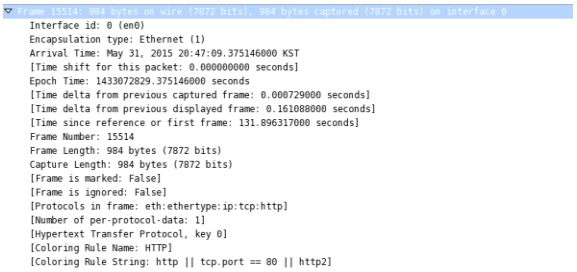

Figure 8. Packet details (frame details)

Summary of information retrieved from Figure 8 are :

- Number of packet frame :15514
- Protocol : HTTP
- Interface id: 0
- Encapsulation type : Ethernet
- Arrival time of packet frame : May 31, 2015, 20:47
- Time shift for this packet : 0.000000000 seconds
- Packet frame length : 984 bytes

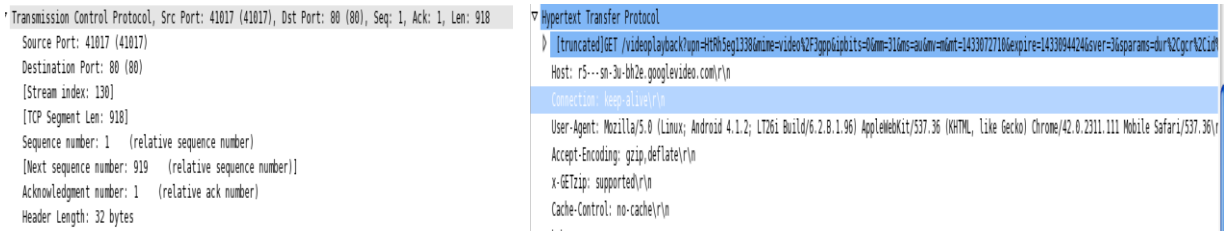

Figure 9. Packet details (TCP details) and Packet details (HTTP details)

Summary of information retrieved from Figure 9 (TCP details) are :

- Number of source port : 41017
- Number of destination port : 80
- Acknowledgement number : 1
- Sequence number : 1
- Header length : 32 bytes

Summary of information retrieved from Figure 9 (HTTP details) are :

- Method: GET (requests data from a specified resource)
- Connection: keep-alive (persistent connection)
- User- agent : Mozilla/5.0 (Linux; Android 4.1.2)

2) Online Banking (www.cimbclicks.com.my)

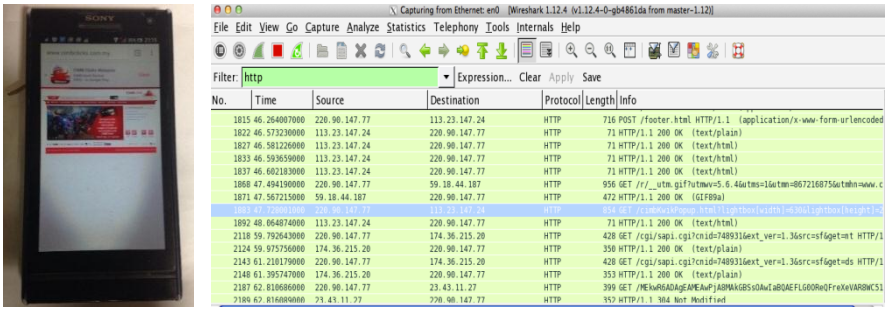

Figure 10. CIMB Online Banking service (left), Wireshark's packet list CIMB online banking (right)

Wireshark start to capture the network packet data coming from online banking service.

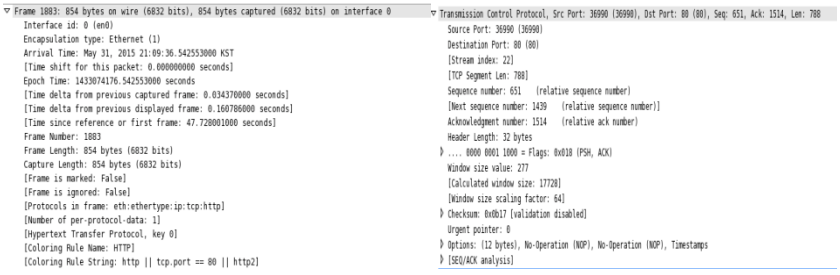

Figure 11. Packet details (frame details) and Packet details (TCP details)

Summary of information retrieved from Figure 11 (frame details) are :

- Number of packet frame : 1883
- Protocol : HTTP
- Interface id : 0
- Encapsulation type : Ethernet
- Arrival Time of packet: May 31, 2015, 21:09

- Time shift of this packet: 0.00000000 seconds
- Packet frame length: 854 bytes

Summary of information retrieved from Figure 11 (TCP details) are :

- Number of source port : 36990
- Number of destination port : 80
- Acknowledgement number : 1514ß
- Sequence number : 651
- Header length : 32 bytes
- TCP segment length : 788

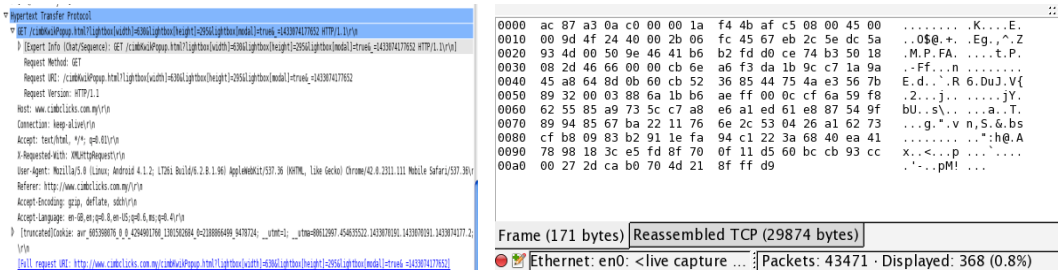

Figure 12. Packet details (HTTP details) (left) and Packet bytes (right)

Summary of information retrieved from Figure 12 (HTTP details) are :

- Method : GET (requests data from a specified resource)
- Host : www.cimbclicks.com.my
- Connection : keep-alive (persistent connection)
- Accept: text/html
- User-agent : Mozilla/5.0 (Linux; Android 4.1.2)

Packet bytes (Figure 12 (right)) displays a packet in its raw, unprocessed form. The right section of Figure 12(right) shows the contents of each of the packets in ASCII characters

4.2 Debookee's Analysis

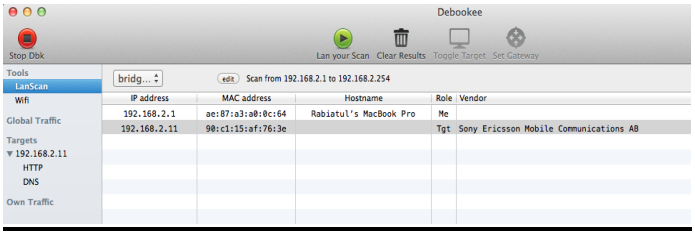

Figure 13. Debookee's list of devices in the active network

Figure 13 shows list of devices that are active in the same network. There are two devices which is Android smartphone is one of them. The interface displays IP address of the devices, MAC address, hostname and vendor. The smartphone's IP address is 192.168.2.11 and the name of vendor is Sony Ericsson Mobile Communication AB.

1) Browsing video (www.youtube.com)
The figure of smartphone browsing a youtube.com is same as figure above. (Refer figure 4.0)

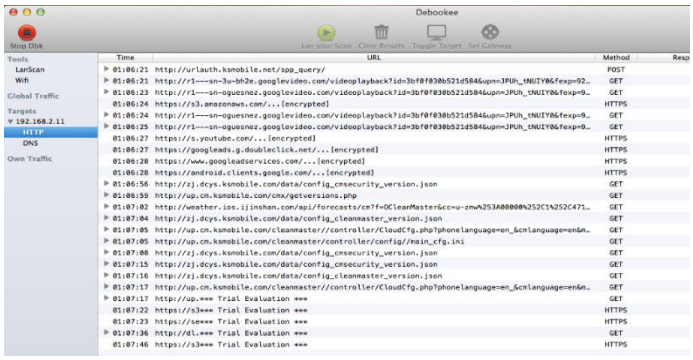

Figure 14. Debookee's packet list

Figure 14 may display the summary of time of packet, URL, method, response, type and length. There are few methods that being captured from browsing youtube.com from the smartphone. The methods are:

- **POST method (HTTP request method)** : to request that a web server accepts the data enclosed in the request message's body for storage. It is often used when uploading a file or submitting a completed web form
- **GET method (HTTP request method)** : intended to retrieve some data and can only send limited amounts of parameter data to the server.
- **HTTPS (Hyper Text Transfer Protocol Secure)** : the secure version of **HTTP**, the protocol over which data is sent between your browser and the website that you are connected to.

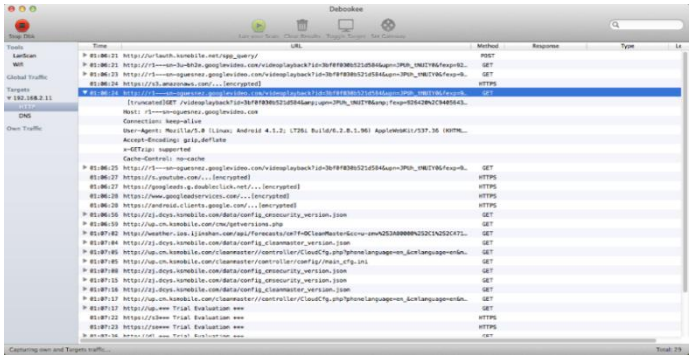

Figure 15. youtube.com packet details

Figure 15 may display the summary of :

- Method : GET
- Host : googlevideo.com
- Connection : keep-alive
- User-Agent : Mozilla/5.0 (Linux; Android 4.1.2)
- Accept-Encoding : gzip (file format and a software application used for file compression and decompression)

2) Online Banking (www.cimbclicks.com.my)

The figure of smartphone browsing a cimbclicks is same as figure above. (figure 15)

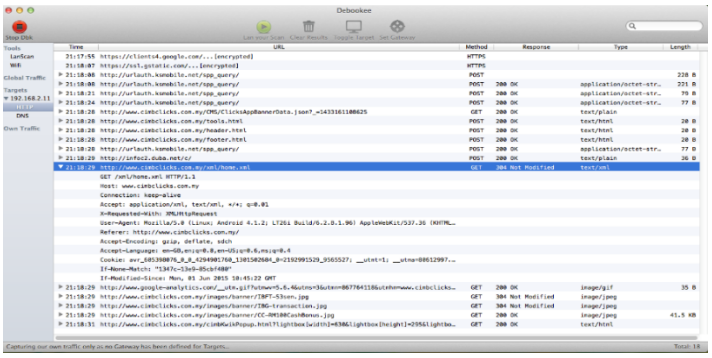

Figure 16. cimbclicks.com.my packet details

Figure 16 may display the summary of :

- Method : GET
- Response : 304 Not Modified (indicates that the resource for the requested URL has not changed since last accessed or cached).
- Host : www.cimbclicks.com.my
- Connection : keep-alive
- Accept : application/xml, text/xml
- User-Agent: Mozilla/5.0 (Linux; Android 4.1.2
- Accept-Encoding : gzip
- Accept-Language: en-GB (Great Britain English language), en (English), en-US (United States English Language)

4.3 Comparison between Wireshark and Debookee

Table 1. Comparison table between Wireshark and Debookee

	Wireshark	Debookee
Interface	Crowded, But user-friendly	Simple
Compatibility	Windows, Mac X OS	Mac X OS
Consistency	Widely used, best network analyzer	Not commonly used, new packet analyzer
Cost	Free(open source)	Free for the limited functions, $30 for full version
Functionality	Many functions, more details on network information	Less functions, less network information

5. Conclusion

Network analyzer is the best tool to capture network packet that coming from various devices in the same network. Then, the network packet need to be analyzed to understand what are the information contain in that. The use of best network analyzer is very important to get more details of network information.

From the analysis, both network analyzers which are Wireshark and Debookee produce information on captured network packet. But Wireshark analyze more details of capture network packets compare to Debookee. For example, the analysis are very details on frame packet section, Transmission Control Protocol(TCP) section, Hypertext Transfer protocol and many more can be explored. The functions provided in Wireshark is more rather than functions in Debookee. For example, Wireshark also provides IO Graph, protocol filter, telephony and others. Debookee only provides basic function but it is still useful but not detailed as in Wireshark.

The analysis shows many network information involved in packet data and help users to understand what method being used, arrival time of packet, length of packet, who is user-agent and can see throughly what really happen in network packet processes. The analysis helps the users to understand the flow of network packet process.

References

[1] Spangler, R. "Packet sniffer detection with antisniff". University of Wisconsin - Whitewater. Department of Computer and Network Administration, 2003.
[2] Anderson, C. D., Anderson, M. B., Cookmeyer, E. N., Daniels, R. A., Wheat, L. E., & Lingle, R. A.. U.S. Patent No. 5,850,388. Washington, DC: U.S. Patent and Trademark Office., 1998.
[3] Rupam, Atul Verma, Ankita Singh. "An Approach to Dectect Packets Using Packet Sniffing", *International Journal of Computer Science & Engineering Survery(IJCSES)*, Vol 4, No. 3., 2013.
[4] Wireshark is best GUI packet analyzer, *http://ibm.com*, 2012.
[5] Wireshark tool – best free network analyzer , *http://techsupportalert.com*, 2015.
[6] Debookee analyzer, http://prmac.com, 2014.
[7] Arias, A. C. "Analysis and interpretation of emulated data traffic in Android platform", *Vienna University of Technology, Department of Electrical Engineering*, 2011.
[8] Parrizas, A. A. "Monitoring network traffic for Android device", GIAC(GCIA) Gold Certification, SANS Institute InfoSec Reading Room., 2013.
[9] Wireshark, *http://www. wireshark.org*
[10] Debookee, *http://www. iwaxx.com*