AMERICAN JOURNALS
Open Access, Peer Reviewed Journals

American Journal of Research in Humanities and Social Sciences
ISSN (E): 2832-8019 Volume 11, | April, 2023

ANALYSIS Of NETWORK TRAFFIC USING WIRESHARK SOFTWARE

Adkham Bozorov Norqabil ogli
Graduate Student of the National University of Uzbekistan
named after Mirzo Ulugbek

ABSTRACT	KEYWORDS
This paper discusses the process analysis of how wireshark analyzes Ethernet computer networks.	computer network, protocol analyzer, cloud technologies, network protocols, Sniffers.

Introduction

Wireshark is a traffic analyzer for Ethernet computer networks and more. It has a graphical user interface. The project was originally called Ethereal, but due to trademark issues, the project was renamed Wireshark in June 2006. The functionality that Wireshark provides is very similar to that of tcpdump, but Wireshark has a graphical user interface and more sorting and filtering capabilities. The program allows the user to view all traffic passing through the network in real time, puts the network card into promiscuous mode. The program is distributed under the free GNU GPL license and uses the cross-platform GTK+ library to build the graphical interface (a transition to Qt[8] is planned). There are versions for many UNIX-like systems, including GNU/Linux, Solaris, FreeBSD, NetBSD, OpenBSD, macOS, and Windows. Wireshark is a program that "knows" the structure of various network protocols, so it allows you to analyze a network packet, showing the value of each field of the protocol at any level.

MAIN PART

First of all, you need to install it on the system. Since one of the most used Linux distributions is Ubuntu, all examples will be shown on it. To install, enter the command in the console: sudo apt-get install wireshark After that, the program will appear in the main menu. You can run it from there. But it's best to do it from the terminal, because it needs superuser rights. You can do it like this: Appearance The program has a convenient graphical interface. The user is presented with a friendly window divided into 3 parts. The first is directly related to capture, the second is related to opening files and samples, and the third is help and support. The Capture block contains a list of network interfaces available for capture. If you select eth0, for example, and click Start, the capture process will begin. The window with received data is also logically divided into several parts. At the top there is a control panel with various elements. This is followed by a list of packages. It is presented in the form of a table. Here you can see the serial number of the package, its holding time, and the shipping and receiving address. You can also delete information about used protocols, length and other useful information. Below the list there is a window with the content of technical data of the selected package.

And even below there is a display in the hexadecimal system. Each view can be expanded in a large window to make the data easier to read. Applying filters Dozens or even hundreds of packages are constantly running in front of the user during the program's operation. Removing them manually is very difficult and time consuming. Therefore, the official guide recommends using WireShark filters. There is a special field for them in the program window - Filter. There is an Expression button to fine-tune the filter. But in most cases, a standard set of filters will suffice:

ip.dst is the destination IP address of the packet;

ip.src is the address of the sender;

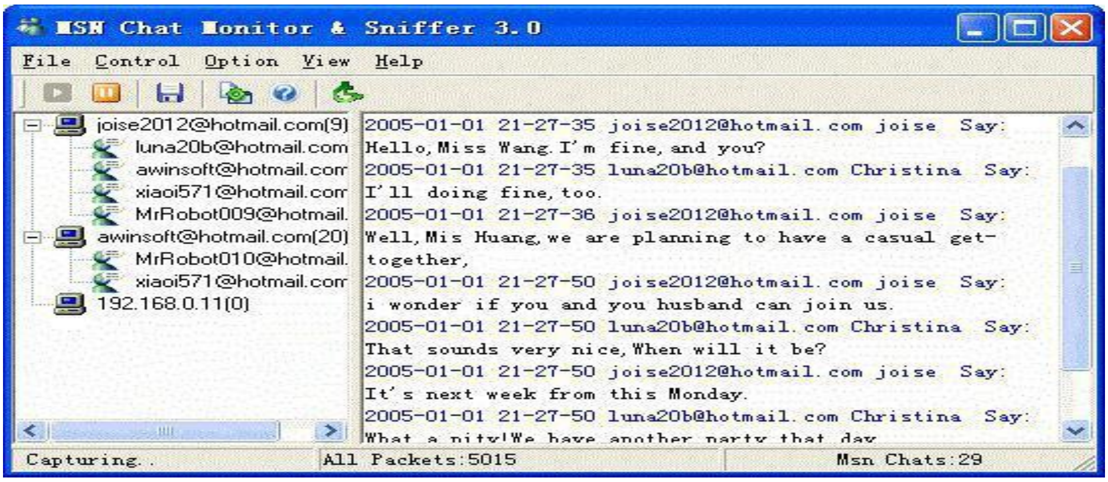
ip.addr - any ip; ip.proto is the protocol.

The program examines the content of data packets passing through the network. No special knowledge is required to start and use the results of Sniffer's work, just open it in the "Start" menu or click on the icon on the desktop (its launch is no different from other Windows programs). The utility's special function allows it to receive data packets, carefully unpack their contents, and present them to the user for analysis. After starting Wireshark, you will see the main program menu on the screen at the top of the window. With its help, the utility is controlled. If you need to download files that store information about packets captured in previous sessions, as well as save information about other packets captured in a new session, you will need the File tab for this. Sniffer: What is a sniffer in terms of English and computer technology? In fact, if you only translate the term, it is not difficult to determine the essence of such a software or hardware-software complex. This name comes from the English word sniff (sniff). This is where the meaning of the Russian term "sniffer" comes from. What is a smeller in our understanding? A "sniffer" capable of monitoring the use of network traffic, or in other words, a spy who interferes with the operation of local or Internet-oriented networks, releases the information he needs based on access through TCP / IP data transmission. protocols.

To test how the program works with filters, you need to enter a certain command. For example, a set like this – ip.dst == 172.217.23.131 – shows all packets going to the Google site. To see all traffic - incoming and outgoing - you can combine two formulas - ip.dst == 172.217.23.131 || ip.src == 172.217.23.131. Thus, it became possible to use two conditions at the same time in one line. Other conditions can be used, for example ip.ttl< 10. Dannaya command vyvedet vse pakety s dlitelnostyu jizni menshe 10. Chtoby vybrat dannye po ix razmeru, mojno primenit takoy podkhod — http.content_length > 5000.

Information _ _ from catching how protection .

This Wi - Fi sniffer or another analyzer without permission _ _ _ traffic from scanning protection who does systems yet too there is There is only one condition: they should be installed only with full confidence in "wiretapping".



```
joise2012@hotmail.com(9)
    luna20b@hotmail.com
    awinsoft@hotmail.com
    xiaoi571@hotmail.com
    MrRobot009@hotmail.
awinsoft@hotmail.com(20)
    MrRobot010@hotmail.
    xiaoi571@hotmail.com
192.168.0.11(0)
```

```
2005-01-01 21-27-35 joise2012@hotmail.com joise  Say:
Hello,Miss Wang.I'm fine, and you?
2005-01-01 21-27-35 luna20b@hotmail.com Christina  Say:
I'll doing fine, too.
2005-01-01 21-27-36 joise2012@hotmail.com joise  Say:
Well,Mis Huang,we are planning to have a casual get-
together,
2005-01-01 21-27-50 joise2012@hotmail.com joise  Say:
i wonder if you and you husband can join us.
2005-01-01 21-27-50 luna20b@hotmail.com Christina  Say:
That sounds very nice,When will it be?
2005-01-01 21-27-50 joise2012@hotmail.com joise  Say:
It's next week from this Monday.
2005-01-01 21-27-50 luna20b@hotmail.com Christina  Say:
What a pity!We have another party that day
```

Such software is often called "anti-sniffers". But if you think about it, these are the same sniffers that analyze traffic, but block other programs that try to get it. Therefore, the legitimate question is: is it worth installing such software? Maybe hacking it will do more damage or is it blocking what it's supposed to do? In the simplest case with Windows systems, it is better to use the built-in firewall (firewall) as protection. Sometimes there may be conflicts with the built-in antivirus, but this often only applies to free packages. There are no such flaws in the professionally purchased or monthly activated versions. That's all the concept of "Snaffer" instead of the next word. It seems that most people already understand what a sniffer is.

References

1. Rahim R. et al. Prototype file transfer protocol application for LAN and Wi-Fi communication //Int. J. Eng. Technol. – 2018. – T. 7. – №. 2.13. – C. 345-347.
2. Badea A., Croitoru V., Gheorghica D. Computer network vulnerabilities and monitoring //2015 9th International Symposium on Advanced Topics in Electrical Engineering (ATEE). – IEEE, 2015. – C. 49-54.
3. Han J. et al. Secure file transfer method and forensic readiness by converting file format in network segmentation environment //Journal of The Korea Institute of Information Security & Cryptology. – 2019. – T. 29. – №. 4. – C. 859-866.