INFORMATION TECHNOLOGY

Comparison of programs for traffic analysis

Y. V. Skoryk, V. A. Vlasova, B. G. Knabe

Kharkov National University of Radio Electronics, Kharkov, Ukraine
Corresponding author. E-mail: yuliia.skoryk@nure.ua, viktoriia.vlasova@nure.ua, bogdan.knabe1@gmail.com

Paper received 01.02.20; Accepted for publication 17.02.20.

https://doi.org/10.31174/SEND-NT2020-224VIII27-08

Abstract. The paper considered the theoretical and practical features of the following programs for monitoring traffic: Observium, Nagios, tcpdump, NetworkMiner, WireShark, Cain and Abel, Zabbix, Network Olympus, and also analyzes the characteristic features of programs for analyzing network traffic. Based on the research, it is shown which programs are most suitable for analyzing network traffic.

Keywords: *traffic analysis, monitoring, program, network traffic.*

Introduction. Network monitoring software is an indispensable tool for every system administrator. They allow you to quickly respond to abnormal activities within the local network, to be aware of all network processes and, thus, automate part of the administrator's routine activities: primarily those related to network security. These tools provide convenient means of visualizing the volumes of outgoing and incoming traffic, allow you to keep statistics, measure speed, monitor the activity of network users and the like. The most relevant programs for monitoring the local network are Observium, Nagios, tcpdump, NetworkMiner, WireShark, Cain and Abel, Zabbix, Network Olympus, which will be analyzed in this paper.

A Brief Review of Related Publications. In [1], the features of the Observium program were considered. In [2], the features of Nagios and Zabbix programs were considered, and their comparison was also carried out. In [3], the tcpdump program is considered. The work [4] describes the NetworkMiner program. The work [5] examined in detail the functionality and operability of the WireShark program. In [6], an introduction to the Cain and Abel program is given. The work [7] describes the Zabbix program, and also describes the network model used in Zabbix. The work [8] describes the functionality of the Network Olympus program.

However, not one of these works compares these programs.

Purpose. To compare programs for traffic analysis, and also on the basis of the analysis to show which traffic analyzers are most suitable for monitoring network traffic.

Analysis of traffic analyzer programs. The Observium program, whose work is based on the use of the SNMP protocol, allows not only to examine the state of a network of any scale in real time, but also to analyze the level of its performance. This solution integrates with hardware from Cisco, Windows, Linux, HP, Juniper, Dell, FreeBSD, Brocade, Netscaler, NetApp and other vendors. Thanks to a perfectly developed graphical interface, these programs provide system administrators with a ton of options for tuning - from ranges for auto-detection to SNMP protocol data needed to collect information about the network. All reports that are generated using the analysis of the event log, the Observium can present in the form of charts and graphs, clearly demonstrating the "weak" side of the network. Observium, as the slogan on the main site says, is a system for monitoring and monitoring network devices and servers. Moreover, the list of supported devices is huge and is not limited only to network devices, the main condition is that the device supports SNMP. But besides SNMP, the information collected can be supplemented by other methods and protocols, for example, syslog, rancid, unix-agent [1]. Message log shown in Fig. 1.

Advantages of the program: a free version is available for a short time; convenient and beautiful interface; it is possible to monitor services such as Apache, Nginx, Mysql, Bind and others, through unix-agent; there are functions of automatic detection; monitoring of some virtualization systems is supported; there is the possibility of building graphs and charts.

Disadvantages: it is installed only on linux systems, there is no version for windows; It is used for large, large networks.

Nagios is a monitoring solution based on a web interface. It is quite difficult to master, however, thanks to its sufficiently co-operation and well-developed documentation, it can be mastered in a few weeks. Nagios is not just a solution for monitoring networks, it is also a solution for monitoring operating networks, individual applications, databases, individual servers, logs [2]. Nagios dashboard shown in Fig. 2.

Advantages of the program: using Nagios, system administrators are able to remotely adjust the amount of load; integration with other applications; it is possible to view the degree of load of memory reserves in databases, for physical indicators of parts of network equipment; there is support for all modern operating systems; convenient to use; colorful interface.

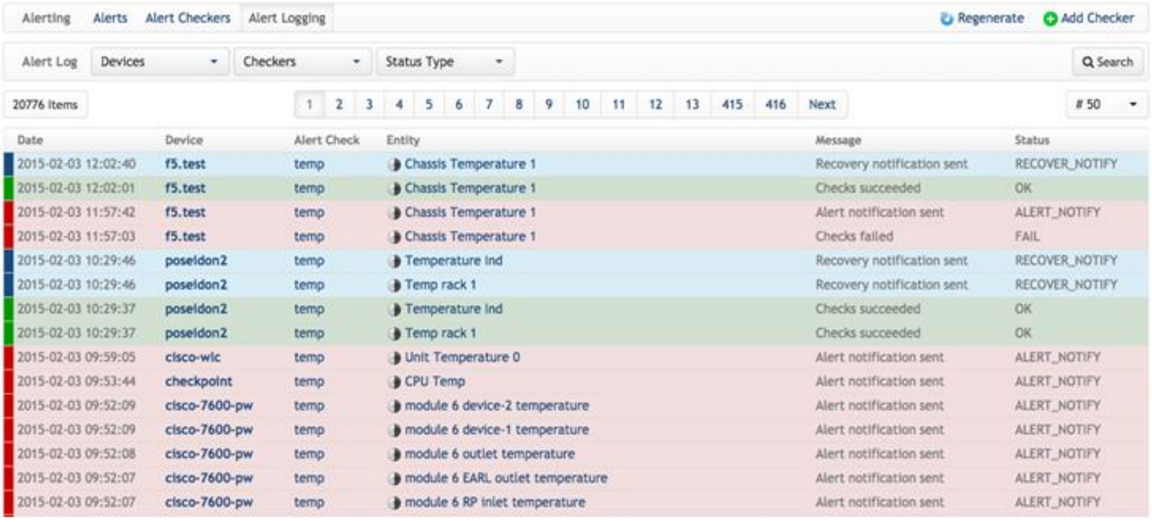
Disadvantages: the program is intended for small organizations; the system is not fault tolerant and is scaled by transferring part of the checks to separate servers; The interval between checks and parameter measurements is too long.

The tcpdump traffic analyzer looks like some kind of outdated tool, and from the point of view of functionality it works as well. Despite the fact that he copes with his work and copes well, using a minimum of system resources for this, it will be difficult for many modern specialists to understand a huge number of data tables. But there are situations when the use of solutions so circumcised and unpretentious to resources can be useful [3].

Advantages of the program: simple program to install; it is possible to install on linux and windows; It has all the basic functionality that you expect to see in any traffic analyzer - capture, recording, etc.

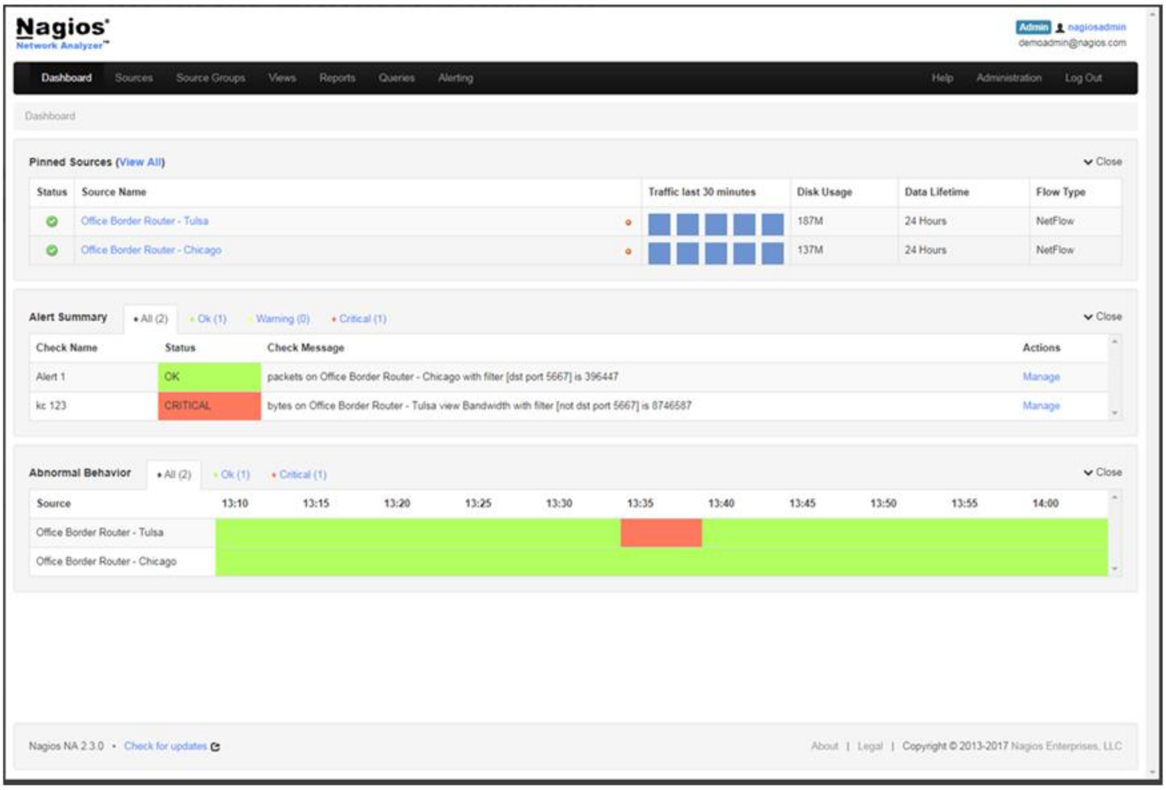
Disadvantages: inconvenient interface; missing graphical interface.

NetworkMiner is another software solution whose functionality goes beyond the usual traffic analysis. While other traffic analyzers focus on sending and receiving packets, NetworkMiner keeps track of those directly sending and receiving packets. This tool is more suitable for identifying problem computers or users than for general diagnostics or network monitoring. NetworkMiner is designed for Windows. Sniffer supports FTP, HTTP and SMB. Also retrieving user data "logins and passwords." The program can be used both for sniffing and for parsing WLAN traffic (IEEE 802.11). The most important feature of this traffic analyzer is the ability to extract files and certificates that are transmitted over the network. This function can be used to intercept and save all kinds of audio and video files [4]. An example of packet capture in NetworkMiner is shown in Fig. 3.



Date	Device	Alert Check	Entity	Message	Status
2015-02-03 12:02:40	f5.test	temp	Chassis Temperature 1	Recovery notification sent	RECOVER_NOTIFY
2015-02-03 12:02:01	f5.test	temp	Chassis Temperature 1	Checks succeeded	OK
2015-02-03 11:57:42	f5.test	temp	Chassis Temperature 1	Alert notification sent	ALERT_NOTIFY
2015-02-03 11:57:03	f5.test	temp	Chassis Temperature 1	Checks failed	FAIL
2015-02-03 10:29:46	poseidon2	temp	Temperature Ind	Recovery notification sent	RECOVER_NOTIFY
2015-02-03 10:29:46	poseidon2	temp	Temp rack 1	Recovery notification sent	RECOVER_NOTIFY
2015-02-03 10:29:37	poseidon2	temp	Temperature Ind	Checks succeeded	OK
2015-02-03 10:29:37	poseidon2	temp	Temp rack 1	Checks succeeded	OK
2015-02-03 09:59:05	cisco-wlc	temp	Unit Temperature 0	Alert notification sent	ALERT_NOTIFY
2015-02-03 09:53:44	checkpoint	temp	CPU Temp	Alert notification sent	ALERT_NOTIFY
2015-02-03 09:52:09	cisco-7600-pw	temp	module 6 device-2 temperature	Alert notification sent	ALERT_NOTIFY
2015-02-03 09:52:09	cisco-7600-pw	temp	module 6 device-1 temperature	Alert notification sent	ALERT_NOTIFY
2015-02-03 09:52:08	cisco-7600-pw	temp	module 6 outlet temperature	Alert notification sent	ALERT_NOTIFY
2015-02-03 09:52:07	cisco-7600-pw	temp	module 6 EARL outlet temperature	Alert notification sent	ALERT_NOTIFY
2015-02-03 09:52:07	cisco-7600-pw	temp	module 6 RP inlet temperature	Alert notification sent	ALERT_NOTIFY

Figure 1. Message log



Pinned Sources (View All)

Status	Source Name	Traffic last 30 minutes	Disk Usage	Data Lifetime	Flow Type
✓	Office Border Router - Tulsa		187M	24 Hours	NetFlow
✓	Office Border Router - Chicago		137M	24 Hours	NetFlow

Alert Summary

Check Name	Status	Check Message	Actions
Alert 1	OK	packets on Office Border Router - Chicago with filter [dst port 5667] is 396447	Manage
kc 123	CRITICAL	bytes on Office Border Router - Tulsa view Bandwidth with filter [not dst port 5667] is 8746587	Manage

Abnormal Behavior

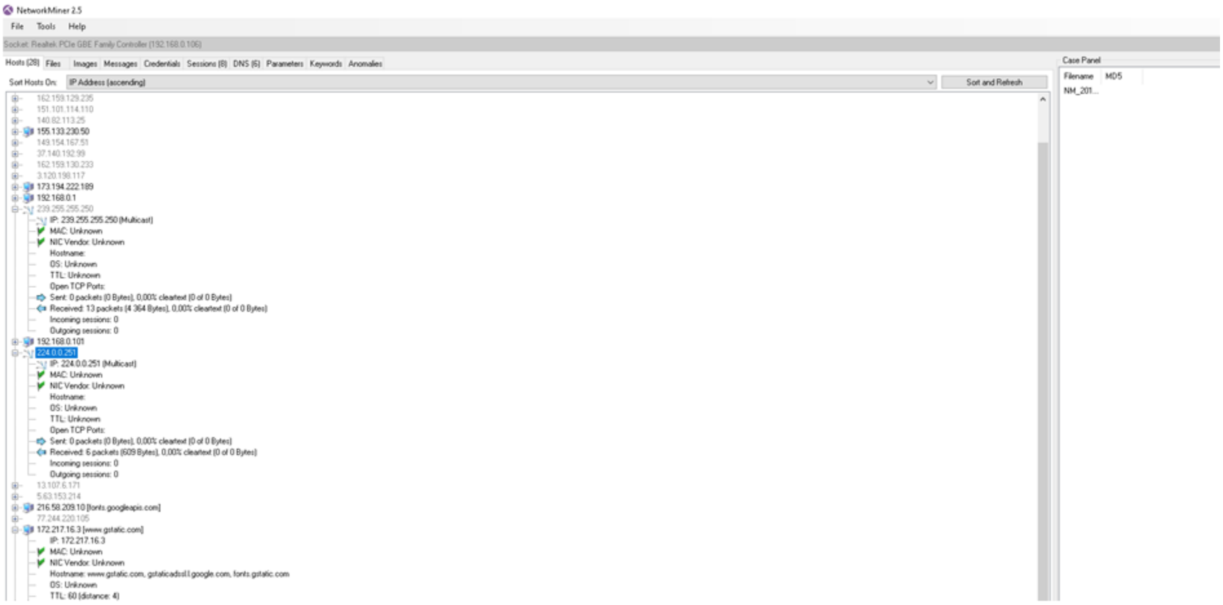
Source	13:10	13:15	13:20	13:25	13:30	13:35	13:40	13:45	13:50	13:55	14:00
Office Border Router - Tulsa	🟩	🟩	🟩	🟩	🟩	🟥	🟩	🟩	🟩	🟩	🟩
Office Border Router - Chicago	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩

Figure 2. Nagios dashboard

Advantages of the program: quick and easy installation; there is a graphical interface; there is visualization and classification of data into groups - which simplifies the analysis of traffic and makes it fast.

Disadvantages: not suitable for corporate solutions; In the evaluation version, some functions are limited.

The WirelessShark program is a relatively new tool in the solution for network diagnostics, but during this time it has already managed to gain recognition and respect from IT professionals. WireShark handles traffic analysis perfectly, doing its job perfectly. The developers were able to find a middle ground between the source data and the visual representation of this data, therefore, in WireShark there are no distortions in one direction or another, which are in most other programs for analyzing network traffic. WireShark is simple, compatible and portable. Using WireShark, you can get exactly what you need. WireShark has an excellent user interface, many options for filtering and sorting.


NetworkMiner 2.5
File Tools Help
Socket: Realtek PCIe GBE Family Controller (192.168.0.106)
Hosts (28) Files Images Messages Credentials Sessions (8) DNS (6) Parameters Keywords Anomalies
Sort Hosts On:
Sort and Refresh
Case Panel
Filename MD5
NM_201...

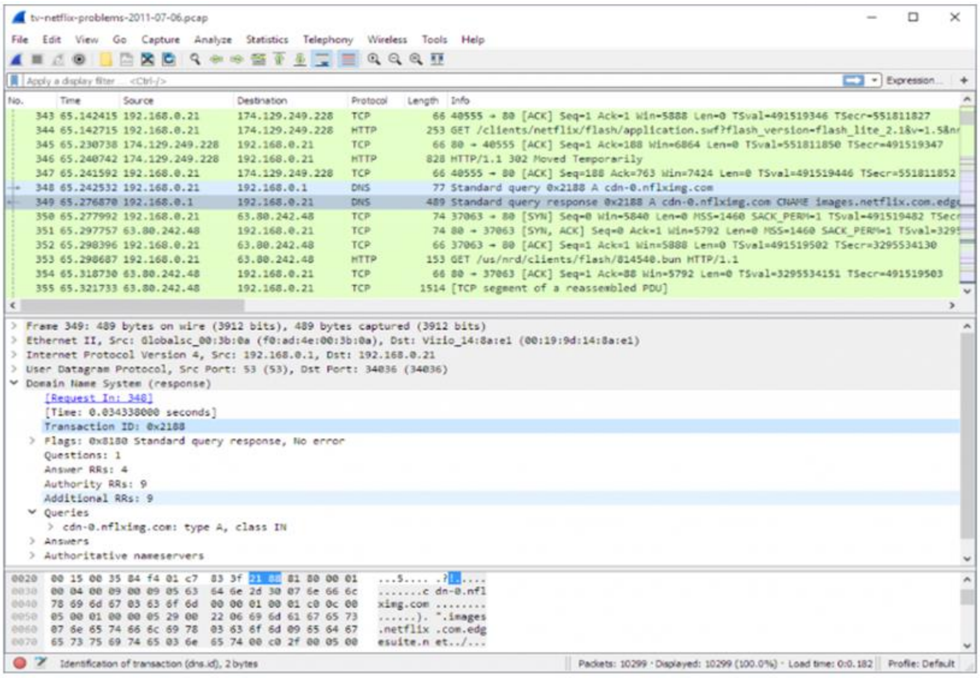
```
IP Address (ascending)
162.159.129.235
151.101.114.110
140.82.113.25
155.133.230.50
149.154.167.51
37.140.192.99
162.159.130.233
3.120.198.117
173.194.222.189
192.168.0.1
239.255.255.250
    IP: 239.255.255.250 (Multicast)
    MAC: Unknown
    NIC Vendor: Unknown
    Hostname:
    OS: Unknown
    TTL: Unknown
    Open TCP Ports:
    Sent: 0 packets (0 Bytes), 0,00% cleartext (0 of 0 Bytes)
    Received: 13 packets (4 364 Bytes), 0,00% cleartext (0 of 0 Bytes)
    Incoming sessions: 0
    Outgoing sessions: 0
192.168.0.101
224.0.0.251
    IP: 224.0.0.251 (Multicast)
    MAC: Unknown
    NIC Vendor: Unknown
    Hostname:
    OS: Unknown
    TTL: Unknown
    Open TCP Ports:
    Sent: 0 packets (0 Bytes), 0,00% cleartext (0 of 0 Bytes)
    Received: 6 packets (609 Bytes), 0,00% cleartext (0 of 0 Bytes)
    Incoming sessions: 0
    Outgoing sessions: 0
13.107.6.171
5.63.153.214
216.58.209.10 [fonts.googleapis.com]
77.244.220.105
172.217.16.3 [www.gstatic.com]
    IP: 172.217.16.3
    MAC: Unknown
    NIC Vendor: Unknown
    Hostname: www.gstatic.com, gstaticadssl.l.google.com, fonts.gstatic.com
    OS: Unknown
    TTL: 60 (distance: 4)
```

Figure 3. An example of traffic capture in NetworkMiner

WireShark traffic analyzer works great with any of the three most popular operating system families - * NIX, Windows, and macOS. WireShark is an open source software product and is distributed free of charge, and it is an excellent tool for conducting quick network diagnostics [5]. An example of packet capture in the WireShark program is shown in Fig. 4.

Advantages of the program: WireShark has a good user interface; there are many options for filtering and sorting; The program works with any of the three most popular families of operating systems - * NIX, Windows and macOS; WireShark is an open source software product and is distributed free of charge.

Disadvantages: not for large companies; Used only for current traffic sniffing; when capturing packets online, a large number of unnecessary packets are stored on the computer.


tv-netflix-problems-2011-07-06.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

```
No.  Time      Source          Destination     Protocol Length Info
343 65.142415 192.168.0.21    174.129.249.228 TCP        66 40555 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519346 TSecr=551811827
344 65.142715 192.168.0.21    174.129.249.228 HTTP      253 GET /clients/netflix/flash/application.swf?flash_version=flash_lite_2.1&v=1.5&nr
345 65.230738 174.129.249.228 192.168.0.21    TCP        66 80 → 40555 [ACK] Seq=1 Ack=188 Win=6864 Len=0 TSval=551811850 TSecr=491519347
346 65.240742 174.129.249.228 192.168.0.21    HTTP      828 HTTP/1.1 302 Moved Temporarily
347 65.241592 192.168.0.21    174.129.249.228 TCP        66 40555 → 80 [ACK] Seq=188 Ack=763 Win=7424 Len=0 TSval=491519446 TSecr=551811852
348 65.242532 192.168.0.21    192.168.0.1     DNS        77 Standard query 0x2188 A cdn-0.nflximg.com
349 65.276870 192.168.0.1     192.168.0.21    DNS       489 Standard query response 0x2188 A cdn-0.nflximg.com CNAME images.netflix.com.edge
350 65.277992 192.168.0.21    63.80.242.48    TCP        74 37063 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=491519482 TSecr
351 65.297757 63.80.242.48    192.168.0.21    TCP        74 80 → 37063 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=3295
352 65.298396 192.168.0.21    63.80.242.48    TCP        66 37063 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519502 TSecr=3295534130
353 65.298687 192.168.0.21    63.80.242.48    HTTP      153 GET /us/nrd/clients/flash/814540.bun HTTP/1.1
354 65.318730 63.80.242.48    192.168.0.21    TCP        66 80 → 37063 [ACK] Seq=1 Ack=88 Win=5792 Len=0 TSval=3295534151 TSecr=491519503
355 65.321733 63.80.242.48    192.168.0.21    TCP      1514 [TCP segment of a reassembled PDU]

> Frame 349: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)
> Ethernet II, Src: Globalsc_00:3b:0a (f0:ad:4e:00:3b:0a), Dst: Vizio_14:8a:e1 (00:19:9d:14:8a:e1)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.21
> User Datagram Protocol, Src Port: 53 (53), Dst Port: 34036 (34036)
v Domain Name System (response)
    [Request In: 348]
    [Time: 0.034338000 seconds]
    Transaction ID: 0x2188
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 4
    Authority RRs: 9
    Additional RRs: 9
  v Queries
    > cdn-0.nflximg.com: type A, class IN
  > Answers
  > Authoritative nameservers

0020  00 15 00 35 84 f4 01 c7  83 3f 21 88 81 80 00 01   ...5.... .?!.....
0030  00 04 00 09 00 09 05 63  64 6e 2d 30 07 6e 66 6c   .......c dn-0.nfl
0040  78 69 6d 67 03 63 6f 6d  00 00 01 00 01 c0 0c 00   ximg.com ........
0050  05 00 01 00 00 05 29 00  22 06 69 6d 61 67 65 73   ......). ".images
0060  07 6e 65 74 66 6c 69 78  03 63 6f 6d 09 65 64 67   .netflix .com.edg
0070  65 73 75 69 74 65 03 6e  65 74 00 c0 2f 00 05 00   esuite.n et../...

Identification of transaction (dns.id), 2 bytes    Packets: 10299 · Displayed: 10299 (100.0%) · Load time: 0:0.182    Profile: Default
```

Figure 4. An example of traffic capture in WireShark

Cain and Abel Program. With this software, the ability to analyze traffic is more of an auxiliary function than the main one. If you need to perform more functions than just analyze traffic, you can use this tool. With it, you can recover passwords for Windows, carry out attacks to obtain lost credentials, examine VoIP data on the network, analyze packet routing and much more. This is a really powerful tool for a system administrator with wide permissions. It works only in a Windows environment. Cain & Abel password recovery tool for Microsoft operating systems. It allows you to easily recover various types of passwords by analyzing network traffic, cracking encrypted passwords, and cryptanalysis. Allows you to record conversations via VoIP, decode secure passwords, recover wireless network keys, open password fields, open cached passwords and analyze routing protocols. The latest version is faster and contains many new features, such as ARP (Arp Poison Routing), which allows you to analyze traffic on switched LANs. In this version, the analyzer (sniffer) can also analyze encrypted protocols, such as SSH-1 and HTTPS, and contains filters for capturing credentials for a wide range of authentication mechanisms [6].

Advantages of the program: password recovery is very fast.

Disadvantages: it takes a lot of time to install; must have access to another administrator account on the computer.

Zabbix monitoring system is a universal open source network monitoring solution that can be configured for individual network models. Basically, it is intended for systems that have a server architecture. This application allows you to simultaneously manage hundreds of network nodes, which makes it an extremely effective tool in organizing the work of administrators working in large-scale enterprises. To deploy Zabbix on your local network, you will either need to run software agents, or use the SNMP protocol for management. In addition, this program provides a complete set of tools for monitoring the status of the network hardware. Note that in order to fully experience all the advantages of this solution, you will have to have at least basic knowledge of some programming languages that can be shared with Zabbix [2, 7].

Advantages of the program: free; the entire configuration is stored in the database, controlled via the web-interface; minimum interval between measurements - 1 second; easy to install.

Disadvantages: no version for Windows; all data is stored in the database, which is inefficient and limits scalability; fault tolerance is not provided; complex cumbersome interface.

Network Olympus. The program works as a service and has a web interface, which gives much greater flexibility and ease of use. The main feature - the script designer, allows you to move away from performing simple checks that do not allow you to take into account certain circumstances of the operation of the devices. With its help, you can organize monitoring schemes of any complexity to accurately identify problems and malfunctions, as well as automate the process of eliminating them. The script is based on a sensor, from which logical chains can be built, which, depending on the success of the test, will generate various alerts and actions aimed at solving problems. Each element of the chain can be edited at any time and immediately applicable to all devices with which the script is attached. All network activity will be monitored using the activity log and special reports [8].

Advantages of the program: free version of the program up to 100 devices; easy to configure and use, there is a designer of monitoring scripts.

Disadvantages: it is installed only under Windows.

Results and its discussion. Traffic monitoring is essential for effective network management. It is a source of information on the functioning of enterprise applications. This information is taken into account when allocating funds, planning computing power, identifying and localizing failures, and resolving security issues. The work considers 8 programs for traffic analysis. After conducting an analysis for each program, we can say that each program has its own advantages and disadvantages, and for each particular case, when choosing a program, this must be taken into account. We can distinguish the WireShark program, this program is most suitable for analysis, research, traffic monitoring. This program allows you to quickly diagnose the network.

Conclusions. In this work, we analyzed such programs for traffic analysis: Observium, Nagios, tcpdump, NetworkMiner, WireShark, Cain and Abel, Zabbix, Network Olympu. We can say that for most home users there will be enough opportunities that tcpdump, Wireshark, NetworkMiner provides. Among the reviewed network traffic analyzers, I would like to single out Zabbix, Observium, Nagios, which have more functionality and are free. Network Olympus can also be distinguished due to its convenient web interface, clear settings, convenient installation, free version, graphical display of requests and scanning. The monitoring system WireShark and NetworkMiner maximally meets the high requirements that are imposed in the case of a study of network traffic.

LITERATURE

1. https://habr.com/ru/post/249623/
2. http://www.netping.ru/Blog/sravnenie-sistem-monitoringa-zabbix-vs-nagios
3. http://blog.sedicomm.com/2017/05/30/tcpdump-poleznoe-rukovodstvo-s-primerami/
4. http://www.spy-soft.net/networkminer/
5. https://habr.com/ru/post/436226/
6. https://www.softsalad.ru/software/bezopasnost/zashchita-paroley/cain-abel
7. https://habr.com/ru/post/73338/
8. https://www.softinventive.ru/network-olympus/