

ДОДАТОК А
ТЕЗИ ДОПОВІДІ

ВІЙСЬКОВА АКАДЕМІЯ ЗБРОЙНИХ СИЛ
АЗЕРБАЙДЖАНСЬКОЇ РЕСПУБЛІКИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
"ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ДП "ПІВДЕННИЙ ДЕРЖАВНИЙ ПРОЕКТНО-
КОНСТРУКТОРСЬКИЙ ТА НАУКОВО-ДОСЛІДНИЙ
ІНСТИТУТ АВІАЦІЙНОЇ ПРОМИСЛОВОСТІ"
УНІВЕРСИТЕТ МІСТА ЖИЛІНА

СУЧАСНІ НАПРЯМИ РОЗВИТКУ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ
ТЕХНОЛОГІЙ ТА ЗАСОБІВ УПРАВЛІННЯ

Тези доповідей одинадцятої міжнародної
науково-технічної конференції

8 – 9 квітня 2021 року

Том 1: секції 1, 2



Баку – Харків – Київ – Жиліна – 2021

**ВІЙСЬКОВА АКАДЕМІЯ ЗБРОЙНИХ СИЛ
АЗЕРБАЙДЖАНСЬКОЇ РЕСПУБЛІКИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
"ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ДП "ПІВДЕННИЙ ДЕРЖАВНИЙ ПРОЕКТНО-
КОНСТРУКТОРСЬКИЙ ТА НАУКОВО-ДОСЛІДНИЙ
ІНСТИТУТ АВІАЦІЙНОЇ ПРОМИСЛОВОСТІ"
УНІВЕРСИТЕТ МІСТА ЖИЛІНА**

СУЧАСНІ НАПРЯМИ РОЗВИТКУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЗАСОБІВ УПРАВЛІННЯ

**Тези доповідей одинадцятої міжнародної
науково-технічної конференції**

8 – 9 квітня 2021 року

Том 1: секції 1, 2

Баку – Харків – Київ – Жиліна – 2021

сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління

| | | | | | |
|-------------------------|-----|------------------------|-----|-----------------------|-----|
| Кременчуцький М.О. | 15 | Міхаль О.П. | 58 | Смідович Л.С. | 10 |
| Кузьмін Ю.О. | 87 | Можаяв О.О. | 60 | | 102 |
| Кузьома Т.М. | 56 | | 83 | | 103 |
| Кулак Г.К. | 106 | Молчанов Г.І. | 109 | Соболь В.В. | 112 |
| Кулак С.В. | 56 | | 113 | Судаков В.О. | 73 |
| Кулик Ю.О. | 10 | | 114 | Ткаленко О.В. | 39 |
| | 102 | Морозова Н.В. | 25 | Томах В.В. | 55 |
| Купіков О.В. | 61 | Настенко О.С. | 71 | Тройно Т.В. | 81 |
| Куров А.М. | 74 | Новікова К.А. | 37 | Трофіменко М.О. | 60 |
| Кучеренко Ю.Ф. | 19 | Носик А.М. | 19 | Туровський І.І. | 62 |
| Кучук Г.А. | 62 | | 46 | Удалов Д.В. | 94 |
| | 121 | Ольшанська Т.І. | 40 | Федоров О.В. | 94 |
| Лабєцький О.Д. | 47 | Онищенко О.І. | 64 | Федорович О.С. | 11 |
| Ламанов С.В. | 63 | Оніщенко Д.П. | 111 | | 12 |
| Лебедєв В.О. | 33 | Осіка К.С. | 118 | Філімончук Т.В. | 40 |
| Лебедєв О.Г. | 33 | Остапенко О.В. | 105 | | 52 |
| | 56 | Панченко В.І. | 115 | | 65 |
| | 57 | Партика С.О. | 122 | | 66 |
| Лебедєва М.В. | 58 | Пашенко Г.І. | 69 | | 67 |
| Лещенко О.Б. | 99 | Писаренко О.С. | 100 | | 68 |
| | 100 | Пісклова Т.С. | 3 | | 69 |
| | 101 | Пліта Л.Л. | 18 | | 70 |
| Лисенко А.А. | 57 | Подорожняк А.О. | 108 | | 71 |
| Лисенко В.О. | 99 | | 111 | | 72 |
| Лифар Д.С. | 68 | | 112 | | 73 |
| Лолєнко А.А. | 108 | Пономаренко П.М. | 6 | Філіппенко І.В. | 78 |
| Луїчкін О.Г. | 77 | Приходько Д.С. | 70 | | 106 |
| Лугай Л.М. | 12 | Прончаков Ю.Л. | 11 | Харченко Н.А. | 91 |
| Любченко Н.Ю. | 111 | Разінькова Є.О. | 72 | | 92 |
| Ляшенко Г.С. | 84 | Рєва О.А. | 103 | | 93 |
| Ляшенко О.С. | 20 | Рєва К.В. | 85 | Цяпа Т.В. | 101 |
| | 82 | Росінський Д.М. | 50 | Чеботарьова Д.В. | 79 |
| | 83 | Рощупкін Є.С. | 17 | | 85 |
| | 84 | Русанова Є.В. | 24 | Черкашина Т.О. | 109 |
| Маковейчук О.М. | 59 | Сєвостьянова К.А. | 34 | Черних О.П. | 123 |
| Малохвій Є.Є. | 113 | Сєвостьянова О.М. | 71 | Чернявський І.О. | 82 |
| | 114 | | 72 | Шведко О.О. | 83 |
| Марговицький В.О. | 25 | Сємихат В.В. | 110 | Шєвєль А.В. | 16 |
| | 42 | Скидан Д.В. | 54 | Шємякін Є.Ю. | 116 |
| | 43 | Склярєв А.С. | 64 | Шилова Т.М. | 107 |
| | 45 | Скорик Ю.В. | 86 | Ширяєв А.В. | 89 |
| | 47 | | 87 | Юрченко Ю.Б. | 117 |
| Маруніч І.М. | 53 | | 105 | Янковський О.А. | 51 |
| Мєзєнцєв М.В. | 15 | Скрильєв О.В. | 58 | Ярошєвич Р.О. | 36 |
| Мірошничєнко Р.О. | 76 | Скринник Г.Ю. | 59 | Яшина О.С. | 104 |

актуальні напрями розвитку інформаційно-комунікаційних технологій та засобів управління

ПОРІВНЯЛЬНИЙ АНАЛІЗ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ІНЖИНІРИНГУ ТРАФІКУ

Скорик Ю.В., Кузьмін Ю.О.

Харківський національний університет радіоелектроніки, Харків, Україна

На сьогоднішній день темпи розвитку галузі телекомунікацій є одними з найвищих. Поряд зі збільшенням темпів зростання клієнтської бази операторів зв'язку, спостерігається зростання трафіку за рахунок впровадження нових технологій і збільшення частки послуг на базі IP-технологій. З огляду на зазначені тенденції, оператори зв'язку, впроваджують нові послуги, що призводить до переходу телекомунікаційних мереж до мультисервісності [1].

У свою чергу це накладає деякі обмеження на функціонування телекомунікаційних мереж. Виникає необхідність виконання вимог якості обслуговування - Quality of Service (QoS), які для різних класів трафіку часто не тільки відрізняються, але й суперечать один одному. Для одночасного забезпечення різних вимог QoS в систему зв'язку потрібно впроваджувати системи інжинірингу трафіку, які в свою чергу повинні враховувати особливості різних класів трафіку і забезпечувати ефективний перерозподіл ресурсів мережі [2, 3].

Метою доповіді є аналіз програмних продуктів, призначених для аналізу та моніторингу мережного трафіку. Були обрані наступні програми, які допомагають відслідковувати і аналізувати дані мережного трафіку: Wireshark, tcpdump, NetFlow Traffic Analyzer.

Можна сказати, що функціональність, яку надає Wireshark, дуже схожа з можливостями програми tcpdump, однак Wireshark має графічний користувацький інтерфейс і набагато більше можливостей із сортування та фільтрації інформації. Ця програма, «знає» структуру самих різних мережних протоколів, і тому дозволяє розібрати мережний пакет, відображаючи значення кожного поля протоколу будь-якого рівня. Tcpdump в свою ж чергу працює в консолі, відкладає мережу і мережну конфігурацію в цілому. NetFlow Traffic Analyzer ідентифікує користувачів і додатки, які споживають найбільше трафіку, і дозволяє вам точно знати, як використовується мережа; захоплює дані про потоках з безперервного мережного трафіку, перетворює їх в графіки і таблиці, що легко читаються.

Список літератури

1. Олифер В. Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы, 4-е издание – СПб.: Питер, 2010. – 944 с.
2. Мониторинг сети. СнифферWireshark[Электронный ресурс]. – Режим доступа: URL: <http://www.4stud.info/networking/work2.html>
3. Tcpdump&libpcap[Электронный ресурс]. – Режим доступа: URL: <http://www.tcpdump.org/#documentation>

ДОДАТОК Б
СЛАЙДИ ПРЕЗЕНТАЦІЇ

Харківський національний університет радіоелектроніки
Кафедра Інформаційно-мережної інженерії

Кваліфікаційна робота на тему:

Дослідження програм з інжинірингу трафіка

Виконав студент групи ІМІзм-19-2
Кузьмінов Юрій
Керівник: доц.Скорик Ю.В.

1

Мета роботи – дослідити та провести порівняльний аналіз програм з інжинірингу трафіку: Wireshark, Iris Network traffic Analyzer, NetFlow Traffic Analyzer, Bro Network Security Monitor, Snort, ClearSight Analyzer, CommView.

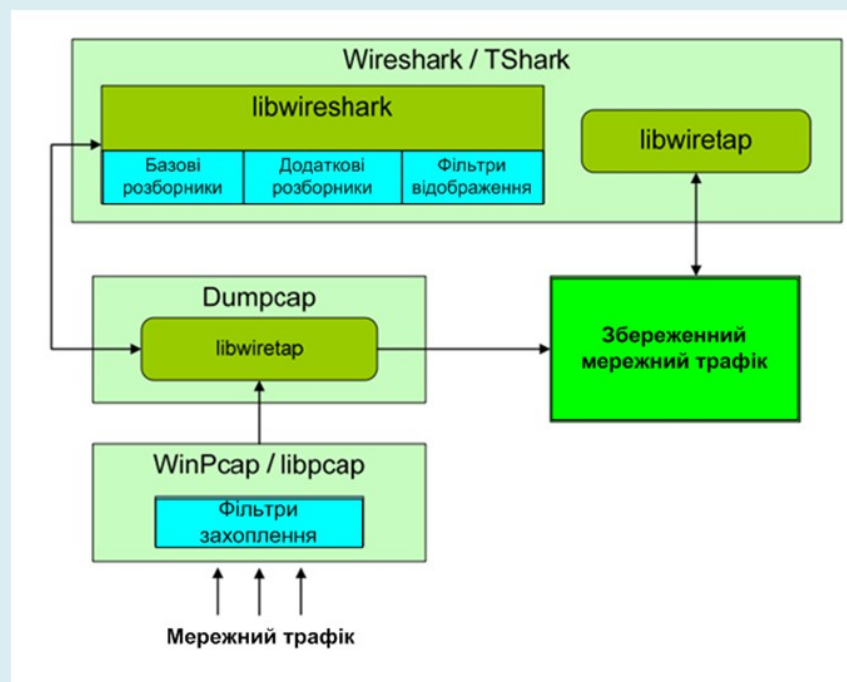
2

Захоплення трафіку здійснюється за допомогою аналізаторів трафіку(сніферів). У загальному випадку, сніфер - це програма, яка призначена для перехоплення і подальшого аналізу, або тільки аналізу мережного трафіку. В рамках конкретних продуктів можуть бути реалізовані додаткові можливості, наприклад, розбір заголовків мережних протоколів, фільтрація за заданими критеріями, відновлення сесій.

На даний час можна нарахувати не один десяток програмних продуктів, призначених для аналізу та моніторингу мережного трафіку, кожен з яких має свої достоїнства і недоліки, тому актуальною є тема роботи, яка присвячена программам аналізаторам.

3

Wireshark



4

Wireshark. Відображення захоплених пакетів

The screenshot shows the Wireshark interface with a list of captured packets. A red box highlights a specific packet (No. 2) with the text "Захваченные пакеты с сетевого интерфейса" (Captured packets from the network interface). The interface shows various protocols like TLSv1.2, TCP, and ARP.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|------------|-------------------|-----------------|----------|--------|--|
| 1 | 23:43:24.1 | 95.213.4.194 | 192.168.1.3 | TLSv1.2 | 479 | Application Data |
| 2 | 23:43:24.2 | 95.213.4.211 | 192.168.1.3 | TLSv1.2 | 487 | Application Data |
| 3 | 23:43:24.2 | 192.168.1.3 | 95.213.4.211 | TLSv1.2 | 279 | Application Data |
| 4 | 23:43:24.3 | 95.213.4.211 | 192.168.1.3 | TCP | 60 | 443 → 57264 [ACK] Seq=434 Ack=226 Win=2555 Len=0 |
| 5 | 23:43:24.3 | 192.168.1.3 | 95.213.4.194 | TCP | 54 | 57256 → 443 [ACK] Seq=1 Ack=426 Win=16449 Len=0 |
| 6 | 23:43:24.5 | Lcfciefe_00:94:1c | Broadcast | ARP | 60 | who has 192.168.1.3?? Tell 192.168.1.2 |
| 7 | 23:43:24.5 | Lcfciefe_00:94:1c | Broadcast | ARP | 60 | who has 192.168.1.184? Tell 192.168.1.2 |
| 8 | 23:43:24.9 | 192.168.1.3 | 95.213.4.194 | TLSv1.2 | 638 | Application Data |
| 9 | 23:43:24.9 | 192.168.1.3 | 95.213.4.194 | TLSv1.2 | 352 | Application Data |
| 10 | 23:43:24.9 | 95.213.4.194 | 192.168.1.3 | TCP | 60 | 443 → 57256 [ACK] Seq=426 Ack=883 Win=2555 Len=0 |
| 11 | 23:43:25.0 | Lcfciefe_00:94:1c | Broadcast | ARP | 60 | who has 192.168.1.185? Tell 192.168.1.2 |
| 12 | 23:43:25.0 | Lcfciefe_00:94:1c | Broadcast | ARP | 60 | who has 192.168.1.9? Tell 192.168.1.2 |
| 13 | 23:43:25.0 | Lcfciefe_00:94:1c | Broadcast | ARP | 60 | who has 192.168.1.8? Tell 192.168.1.2 |
| 14 | 23:43:25.5 | Lcfciefe_00:94:1c | Broadcast | ARP | 60 | who has 192.168.1.184? Tell 192.168.1.2 |
| 15 | 23:43:25.6 | 192.168.1.3 | 213.180.204.194 | TCP | 55 | [TCP segment of a reassembled PDU] |
| 16 | 23:43:25.7 | 213.180.204.194 | 192.168.1.3 | TCP | 60 | 443 → 57465 [ACK] Seq=1 Ack=2 Win=129 Len=0 |
| 17 | 23:43:25.8 | Lcfciefe_00:94:1c | Broadcast | ARP | 60 | who has 192.168.1.3?? Tell 192.168.1.2 |

Frame 2: 487 bytes on wire (3896 bits), 487 bytes captured (3896 bits) on Interface 0
 Ethernet II, Src: EltexEnt_c8:d8:dc (a8:f9:4b:c8:d8:dc), Dst: Compalln_5f:24:31 (b8:88:e3:5f:24:31)
 Internet Protocol Version 4, Src: 95.213.4.211, Dst: 192.168.1.3
 Transmission Control Protocol, Src Port: 443 (443), Dst Port: 57264 (57264), Seq: 1, Ack: 1, Len: 433
 Secure Sockets Layer

0000 b8 88 e3 5f 24 31 a8 f9 4b c8 d8 dc 00 00 45 00 ..._51.. K.....E.
 0010 01 09 36 aa 40 00 30 06 e4 21 5f 05 04 d3 c0 a8 ...6.#.8. .!_.....
 0020 01 03 01 bb df b0 32 03 1e d1 17 44 7d 24 50 182. ...D)\$.P.
 0030 09 fb f8 95 00 00 17 03 03 01 ac 68 06 e4 5c 42h..|B
 0040 be d5 1b 44 90 0a 66 40 bc 7c 7e 86 62 42 9a 2d ...D..# .|~.bb.-
 0050 0e 29 02 0d 1a dc 50 b5 20 20 f0 cf 08 07 58 2cP.X,

5

Wireshark. Статистичні дані захопленого трафіку

| Характеристика | Значення |
|---|---------------------|
| First packet/Початок захопту | 2020-05-19 23:23:24 |
| Last packet/ Останній захоплений пакет | 2020-05-19 23:59:51 |
| Elapsed/ Час захоплення, хв | 00:36:27 |
| Packets/Захоплені пакети | 75133 |
| Packets size/ Розмір всіх пакетів, Мбайт | 68 Mb |
| Average kbytes/s Середня швидкість пакетів | 67 kbytes/s |
| Average kbits/s / Середня швидкість | 538 kbit/s |

6

Wireshark. Використані протоколи в захоплених пакетах

| Protocol /Протокол | Packets/Пакети, kbit | Packets size byte/Розмір усіх пакетів | Average kbits/s / Середня швидкість | Packets/Пакети, % |
|--------------------|----------------------|---------------------------------------|-------------------------------------|-------------------|
| Ipv6 | 796 | 72940 | 591 | 1.1 |
| Ipv4 | 60635,7 | 6600731 | 534 | 62.4 |
| UDP | 678 | 107824 | 873 | 3.4 |
| DNS | 504 | 99700 | 808 | 0.7 |
| TCP | 16426,3 | 63665319,17 | 534 | 24.5 |
| HTP | 820 | 548548 | 444 | 0.9 |
| ARP | 5273 | 315822 | 456 | 7 |
| ВСЬОГО | 75133 пакетів | 71303168 Byte | 608 kbits/s | 100% |

7

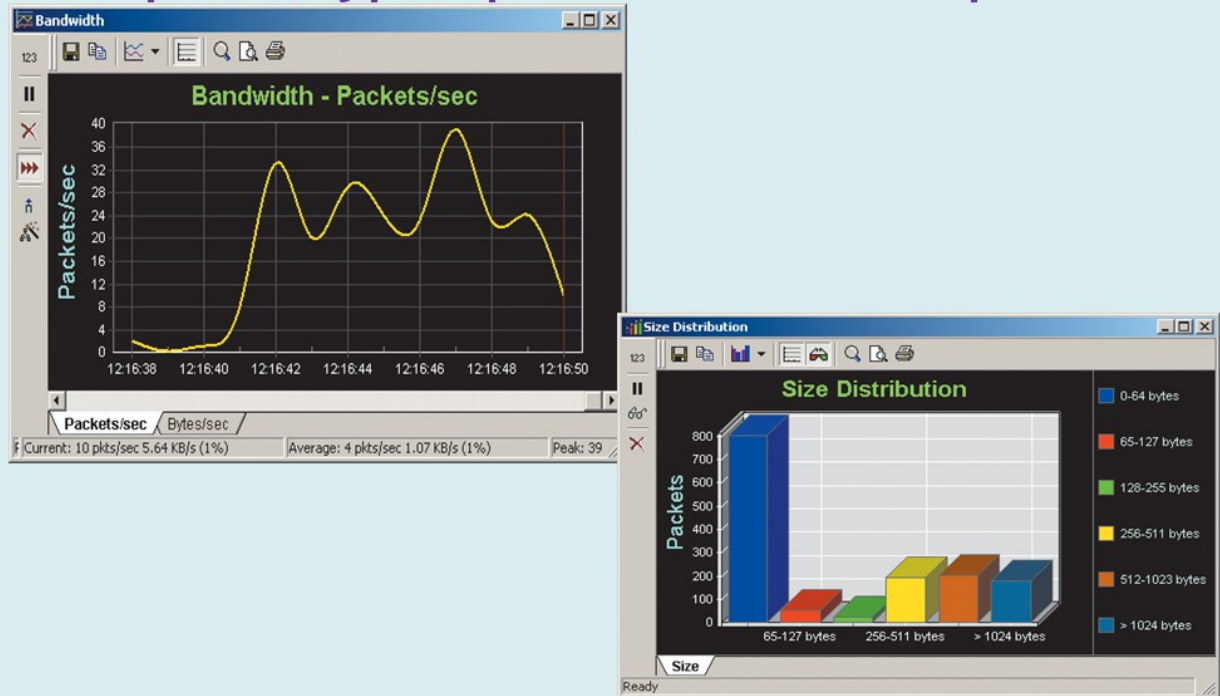
Iris Network Traffic Analyzer



Figure 1: IrisNet Architecture

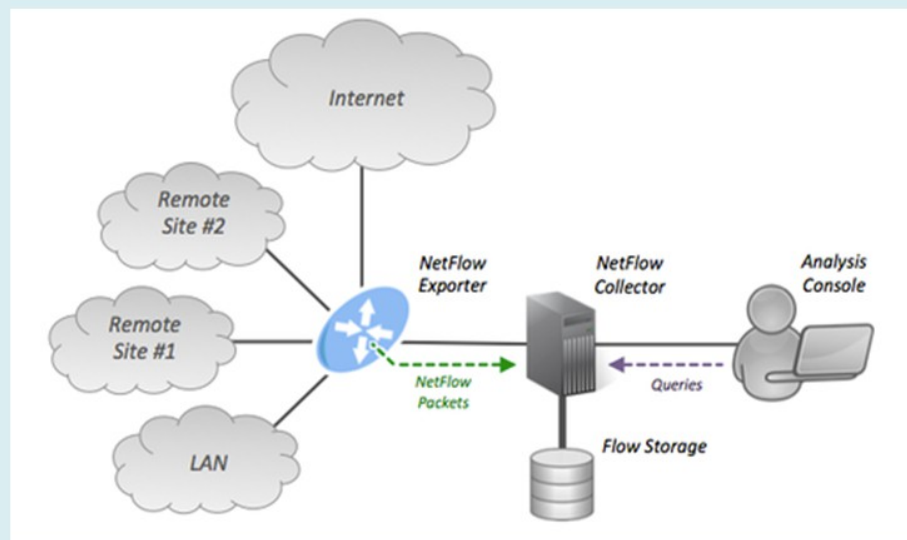
8

Iris Network Traffic Analyzer. Графік швидкості передачі пакетів в аналізаторі Iris та діаграма розподілу розмірів пакетів в аналізаторі Iris



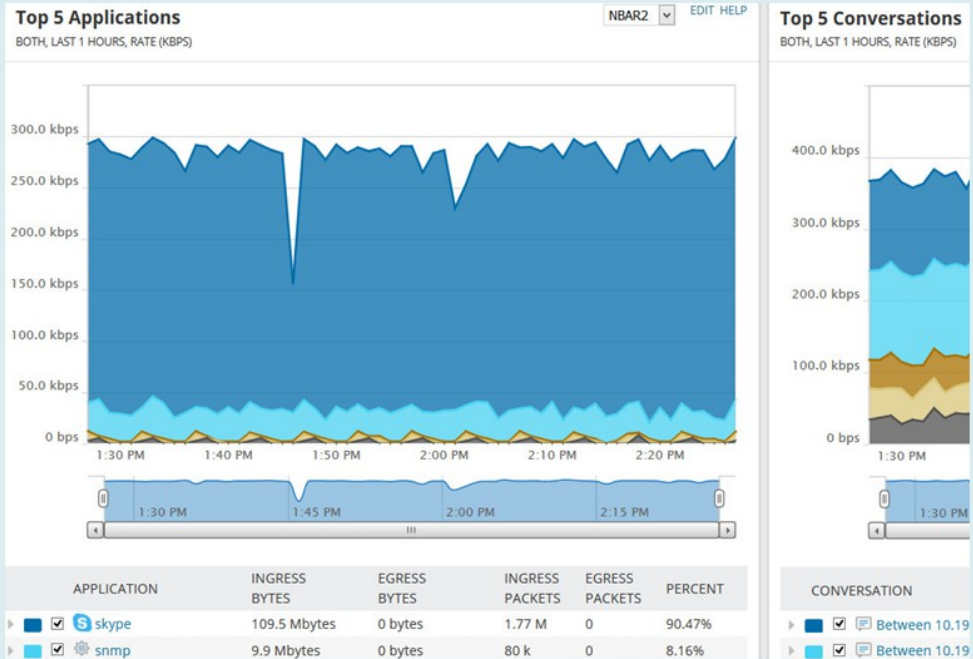
9

NetFlow traffic analyzer



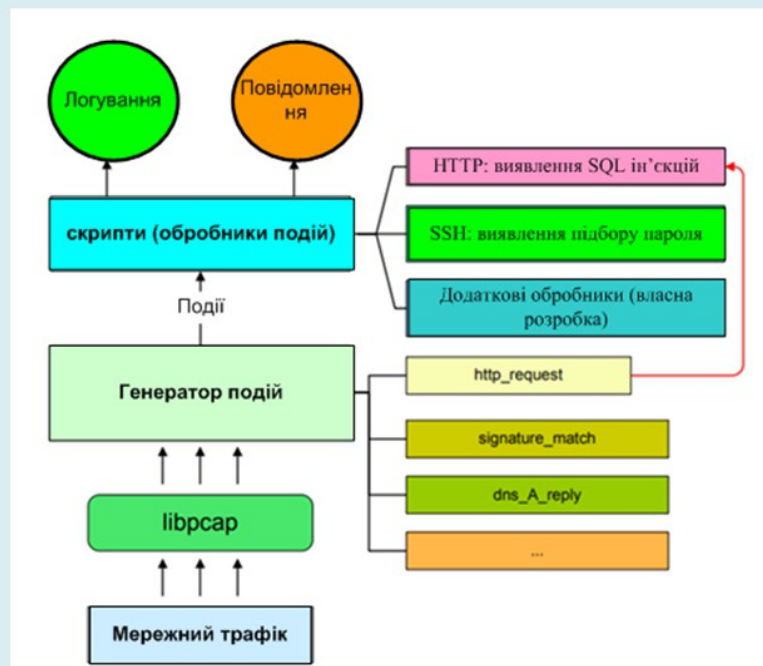
10

NetFlow traffic analyzer. Аналіз роботи програми



11

Bro Network Security Monitor



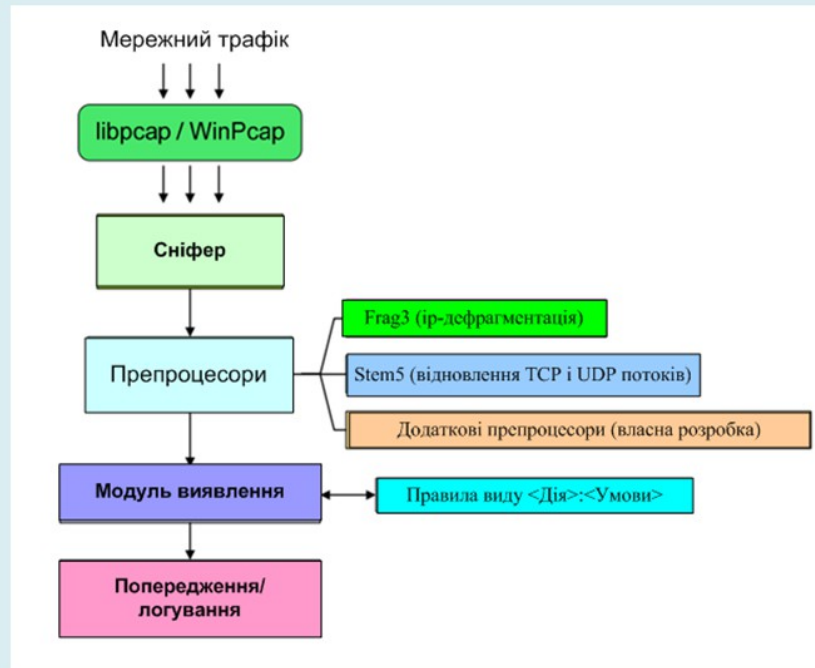
12

Bro Network Security Monitor. Аналіз трафіку за допомогою Bro

The screenshot displays the Sematext dashboard interface. At the top, there's a navigation bar with 'Dashboards' and 'Services' tabs. Below this, a search bar and a 'Query' input field are visible. The main area is a table of log entries with columns for 'host', 'answers', 'id_orig_h', 'id_orig_p', 'id_resp_h', 'logSource', 'rx_bytes', 'service', and 'severity'. A sidebar on the right contains 'Fields & Filters' and a 'Field stats' section. The bottom of the dashboard includes version information and a footer with 'Sematext Group, Inc. All Rights Reserved'.

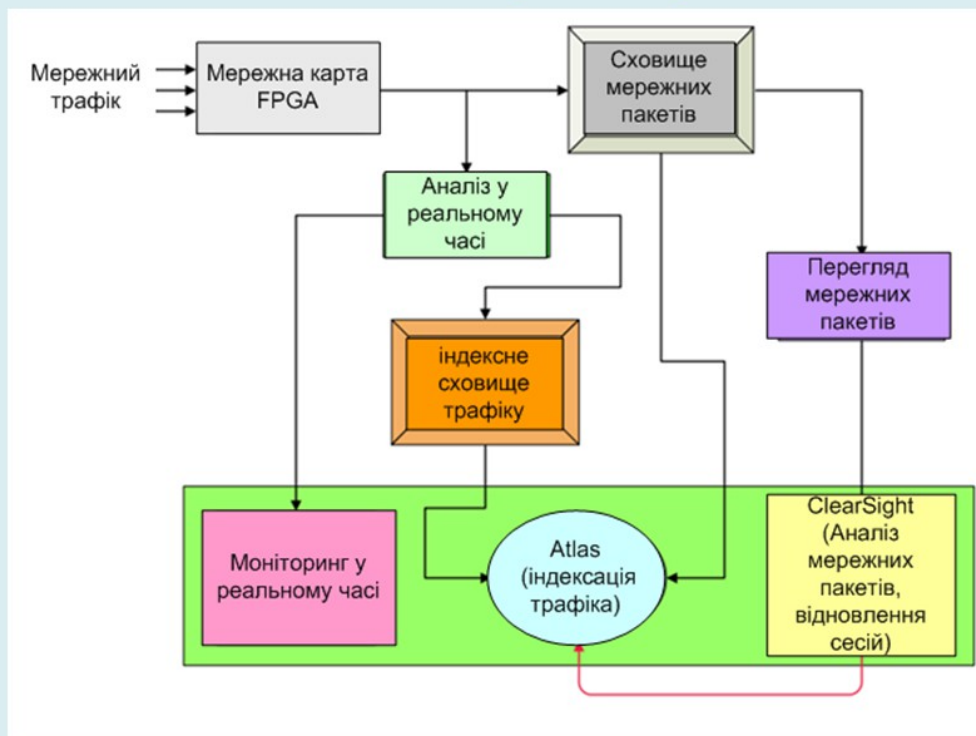
| host | answers | id_orig_h | id_orig_p | id_resp_h | logSource | rx_bytes | service | severity |
|-------------|---|---------------|-----------|----------------|----------------|----------|---------|----------|
| ipsec.local | | 192.168.1.20 | 52540 | 107.20.222.136 | ArgoBroker.log | | | info |
| ipsec.local | | 192.168.1.20 | 52539 | 107.20.222.136 | ArgoBroker.log | | | info |
| ipsec.local | | 188.166.94.17 | 9993 | 192.168.1.20 | ArgoBroker.log | | | info |
| ipsec.local | | 48.101.160.24 | 9993 | 192.168.1.20 | ArgoBroker.log | | | info |
| ipsec.local | | 52.7.133.188 | 2164 | 192.168.1.20 | ArgoBroker.log | | | info |
| ipsec.local | | 192.168.1.20 | 52596 | 192.209.67.196 | ArgoBroker.log | | | info |
| ipsec.local | | 192.168.1.20 | 52598 | 192.209.67.196 | ArgoBroker.log | | | info |
| ipsec.local | | 192.168.1.20 | 60249 | 148.62.0.29 | ArgoBroker.log | | | info |
| ipsec.local | | 192.168.1.20 | 17604 | 192.168.1.1 | ArgoBroker.log | | | info |
| ipsec.local | ipsec:ob-stark.com 192.209.67.196 148.62.0.29 148.62.1.66 66.214.66.35 148.62.3.88 168.78.45.16 192.237.193.126 192.237.192.132 148.62.0.31 174.143.166.88 148.62.3.119 | | | | ArgoBroker.log | | | info |

Snort



14

ClearSight Analyzer

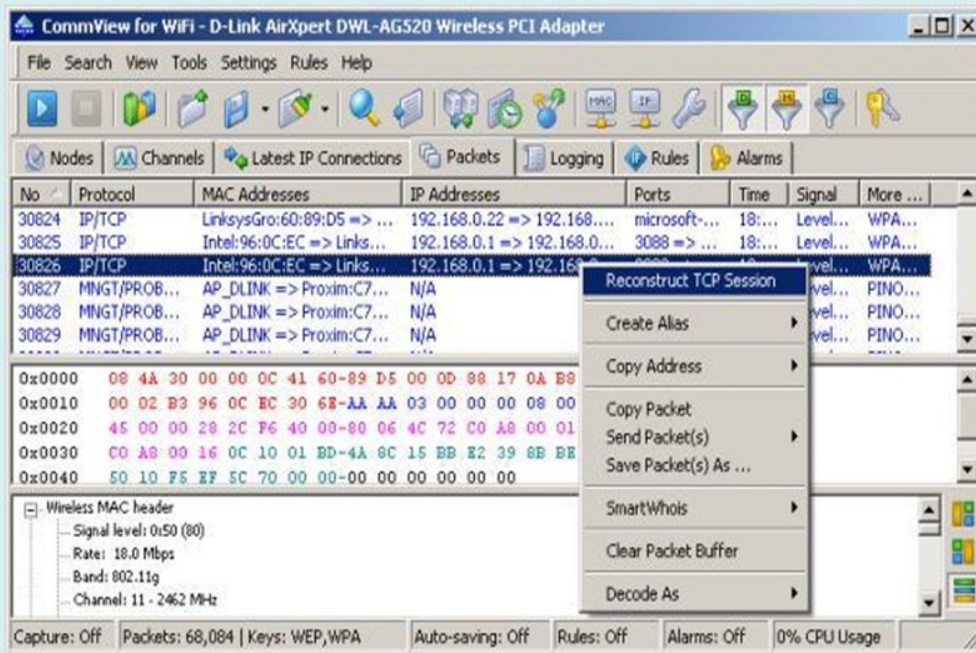


15

ClearSight Analyzer. АКТИВНІСТЬ В МЕРЕЖІ

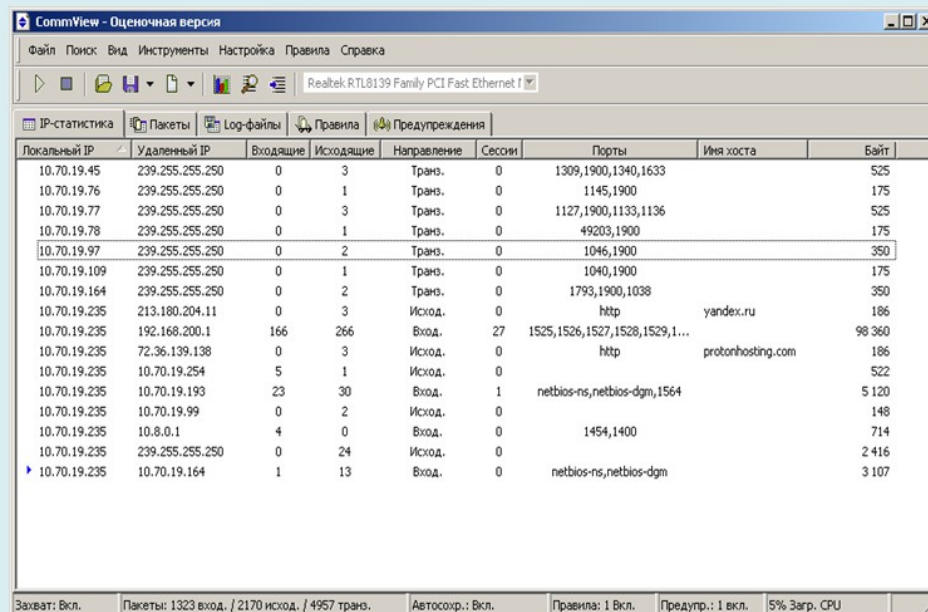


CommView



17

CommView. Мережна статистика пакетів



18

Аналіз мережного трафіку на базі відновлення TCP-сесій та розпізнавання протоколів

| № | Кінцеві точки | Розмір відновленої сесії | | | |
|------------------------|--|--------------------------|--------|--------|---------------------|
| | | Wireshark | Snort | Bro | ClearSight Analyzer |
| google-http.pcap | | | | | |
| 1 | 192.168.0.105:25162 - 74.125.19.104:80 | 22925 | 22925 | - | 22925 |
| 2 | 192.168.0.105:25161 - 74.125.19.104:80 | 1216 | 1216 | | 1216 |
| 3 | 192.168.0.105:25160 - 68.142.205.139:80 | 1897 | 1897 | | 1897 |
| 4 | 192.168.0.105:25168 - 74.125.19.104:80 | 20125 | 20125 | 20125 | 20125 |
| 5 | 192.168.0.105:25175 - 68.142.205.139:80 | 6515 | 6515 | 6515 | 6515 |
| 6 | 192.168.0.105:25180 - 68.142.205.139:80 | 7087 | 7087 | 7087 | 7087 |
| google-https.pcap | | | | | |
| 7 | 192.168.0.105:24044 - 74.125.205.113:80 | 10480 | 10527 | 10480 | 10527 |
| 8 | 192.168.0.105:24053 - 68.142.205.139:80 | 6515 | 6515 | 6515 | 6515 |
| 9 | 192.168.0.105:24060 - 68.142.205.139:80 | 6797 | 6797 | 6797 | 6797 |
| 10 | 192.168.0.105:24089 - 68.142.205.139:80 | 123832 | 123832 | 123832 | 123832 |
| http-google.pcap | | | | | |
| 11 | 192.168.0.115:37927 - 74.125.19.106:80 | 31166 | 3166 | - | 31166 |
| 12 | 192.168.0.115:37903 - 74.125.19.106:80 | 15207 | 15207 | - | 15207 |
| 13 | 192.168.0.115:37979 - 74.125.36.37:80 | 0 | 0 | - | 0 |
| 14 | 192.168.0.115:37905 | ??? | ??? | ??? | ??? |
| http-googlesearch.pcap | | | | | |
| 15 | 24.6.173.220:49771 - 74.125.224.105:80 | 13244 | 13244 | - | 13244 |
| 16 | 24.6.173.220:49795 - 74.125.224.83:80 | 0 | 0 | - | 0 |
| 17 | 24.6.173.220:49831 - 63.245.209.93:80 | 0 | 0 | - | 0 |
| 18 | 24.6.173.220:49832 - 96.17.148.90:80 | 0 | 0 | - | 0 |

Аналіз показав наступне:

- Bro починає відновлювати дані з'єднання з моменту його встановлення, а Wireshark, Snort і ClearSight - з моменту виявлення першого TCP-сегмента між даними парами адрес- порт. З'єднання з номерами 11, 11 - 18 були встановлені до початку запису відповідної траси. Тому Bro не зміг їх відновити;
- кожне із з'єднань 4 - 6, 8 - 10 має по 2 сегмента, які потрапили в трасу в неправильному порядку (з точки зору збирання TCP-поток). При розборі інструменти Bro і Wireshark вірно додали дані цих сегментів в правильному порядку. Snort і ClearSight додали дані в тому порядку, в якому вони прийшли;
- з'єднання 7 має сегмент повторної передачі. Дані цих сегментів були відкинута Wireshark і Bro, але додані Snort і ClearSight;
- тестування показало, що інструменти Wireshark і Bro найбільш точно відновлюють дані TCP-з'єднань. Однак Bro не відновлює (хоча б частково) з'єднання, встановлені до моменту початку перехоплення трафіку. Snort і ClearSight не виробляють необхідного перепорядкування даних, додаючи їх в порядку приходу, а також не відкидають сегменти, передані повторно.

19

Порівняльна таблиця характеристик розглянутих програм-аналізаторів мережного трафіку

| | Wireshark | Iris | NetFlow | Bro | ClearSight | Comm View |
|----------------------------------|-----------|---------|---------|---------|------------|-----------|
| Розмір файлу | 17,4 МБ | 5,04 МБ | 20,6 Мб | 17,7 Мб | 18,1 Мб | 29,9 Мб |
| Мова інтерфейсу | англ. | рос. | англ. | англ. | англ. | англ. |
| Графік швидкості | + | + | + | - | + | + |
| Графік трафіку | + | + | + | - | + | - |
| Експорт, Імпорт | + | + | - | - | - | + |
| Запуск моніторингу | - | - | - | - | - | - |
| Мінімум крок між звітами | 0,001 с. | 1 с. | 1 с. | 1 с. | 0,001 с | 1 с. |
| Зміна мінімуму кроку між звітами | + | + | + | - | + | - |

20

ВИСНОВКИ

В роботі було розглянуто і проаналізовано програми з інжинірингу мережного трафіку: Wireshark, Iris Network traffic Analyzer, NetFlow Traffic Analyzer, Bro Network Security Monitor, Snort, ClearSight Analyzer, CommView. Для кожної з програм зроблено опис архітектури і основних переваг та недоліків з функціональності та легкості у використанні.

Досліджено основні можливості програм з висновками їх переваг і недоліків. Результати досліджень наведено у таблицях.

З найпопулярніших програм є Wireshark. Ця програма дає змогу зробити розбір та провести розпізнавання більш ніж 1000 мережних протоколів. Стосовно інших програм, вони не мають таку кількість підтримуваних протоколів.

Wireshark має більш ефективний засіб перегляду, збору та аналізу статистики трафіку.

