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

ŽILINSKÁ UNIVERZITA
V ŽILINE

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

ПОРІВНЯЛЬНИЙ АНАЛІЗ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ІНЖИНІРИНГУ ТРАФІКУ

Скорик Ю.В., Кузьмінов Ю.О.
Харківський національний університет радіоелектроніки, Харків, Україна

На сьогоднішній день темпи розвитку галузі телекомунікацій є одними з ...йшвидших. Поряд зі зниженням темпів зростання клієнтської бази опера...рів зв'язку, спостерігається зростання трафіку за рахунок впровадження ...вих технологій і збільшення частки послуг на базі IP-технологій. З огляду ...а 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 телеко...мунікаційних мереж. Виникає необхідність виконання вимог якості обслуго...вання - Quality of Service (QoS), які для різних класів трафіку часто не тіль...ки відрізняються, але й суперечать один одному. Для одночасного забезпе...чення різних вимог QoS в систему зв'язку потрібно впроваджувати системи ...жинірингу трафіку, які в свою чергу повинні враховувати особливості різ...них класів трафіку і забезпечувати ефективний перерозподіл ресурсів мережі [2, 3].

Метою доповіді є аналіз програмних продуктів, призначених для аналі...зу та моніторингу мережного трафіку. Були обрані наступні програми, які ...опомагають 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 користува...цький інтерфейс і набагато більше можливостей із сортування та фільт...рації інформації. Ця програма, «знає» структуру самих різних мережних про...толів, і тому дозволяє розібрати мережний пакет, відображаючи значення ...жного поля протоколу будь-якого рівня. Tcpdump в свою ж чергу працює в ...нсолі, відкладає мережу і мережну конфігурацію в цілому. NetFlow Traffic Analyzer ідентифікує користувачів і додатки, які споживають найбільше тра...фіку, 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. СниффферWireshark[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.

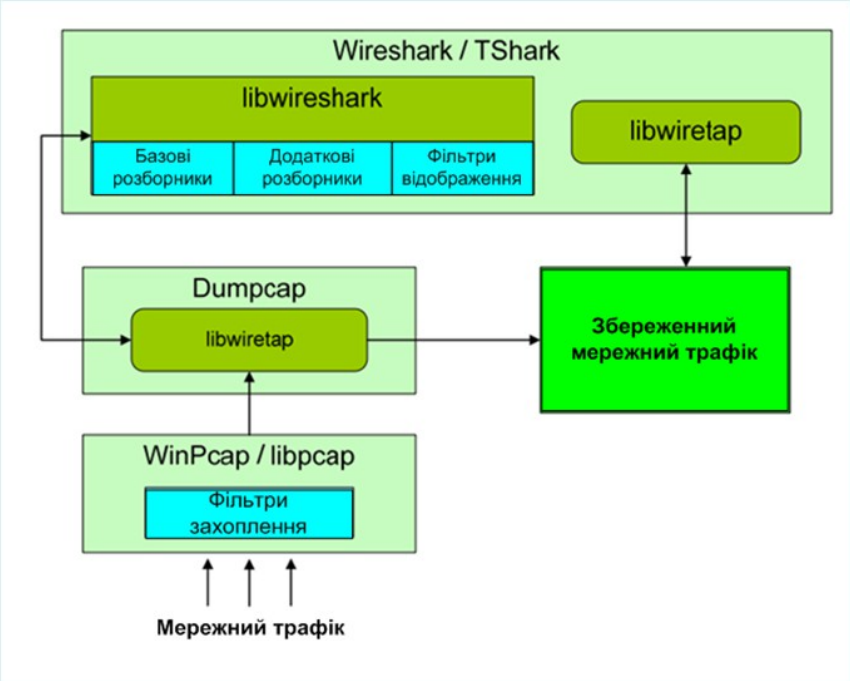
2

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.

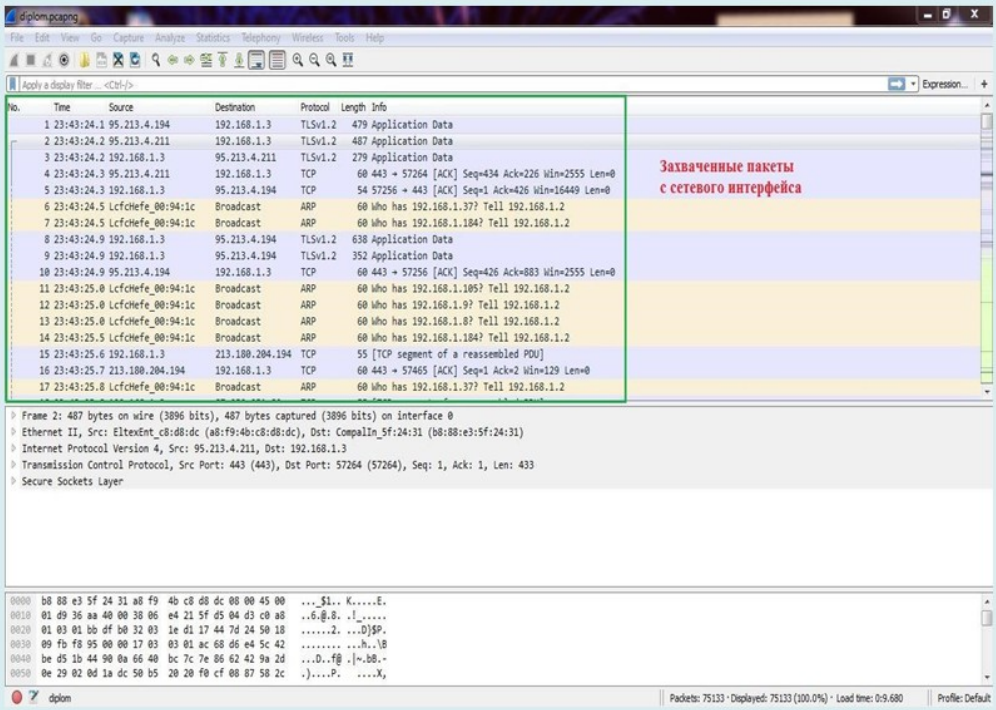
3

Wireshark



4

Wireshark. Відображення захоплених пакетів



5

Wireshark. Статистичні дані захопленого трафіку

Характеристика	Значення
First packet/Початок захвату	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%

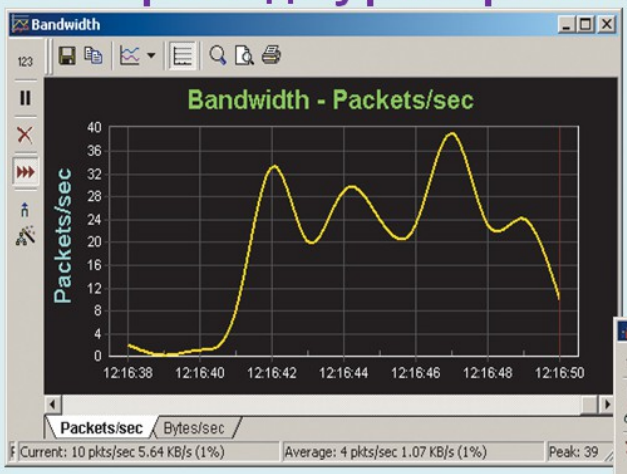
7

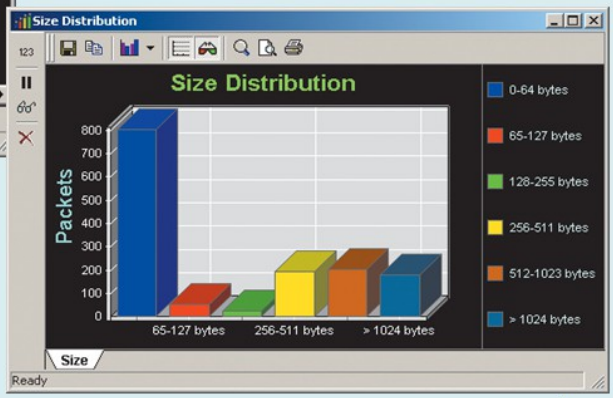
Iris Network Traffic Analyzer

Figure 1: IrisNet Architecture

8

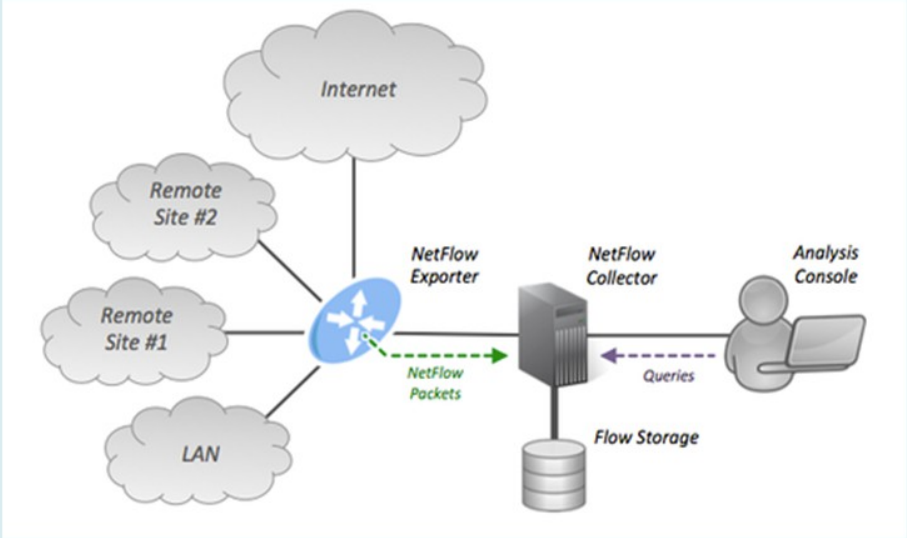
Iris Network Traffic Analyzer. Графік швидкості передачі пакетів в аналізаторі Iris та діаграма розподілу розмірів пакетів в аналізаторі Iris





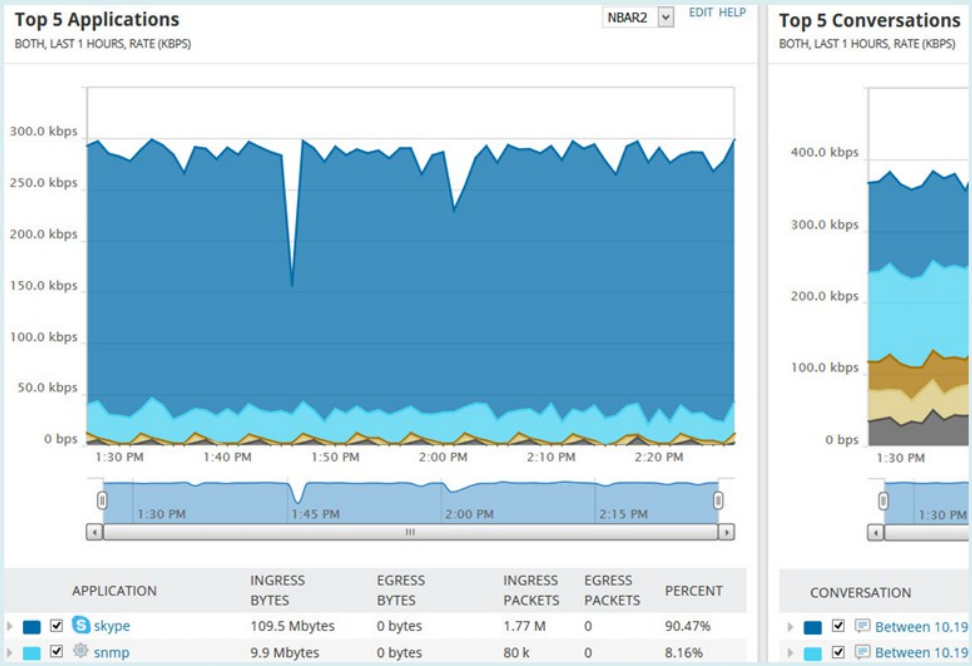
9

NetFlow traffic analyzer



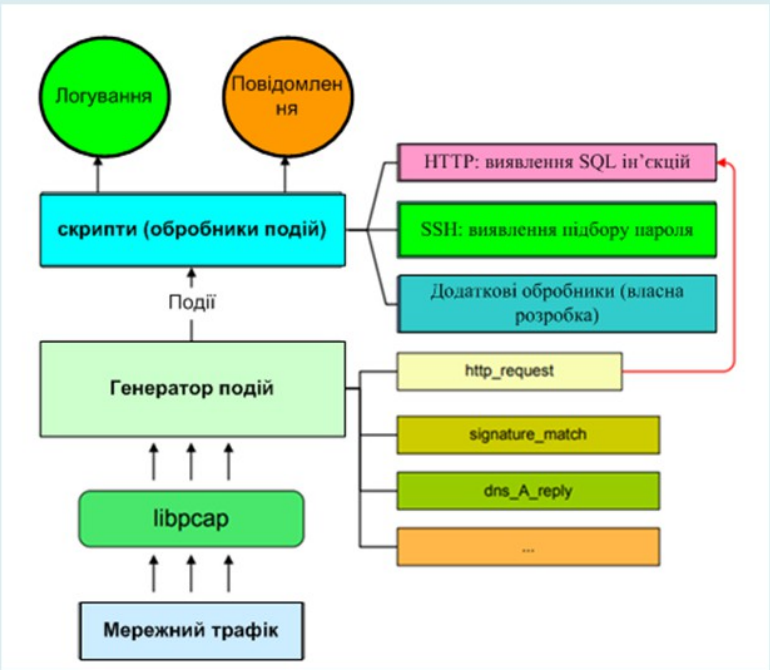
10

NetFlow traffic analyzer. Аналіз роботи програми



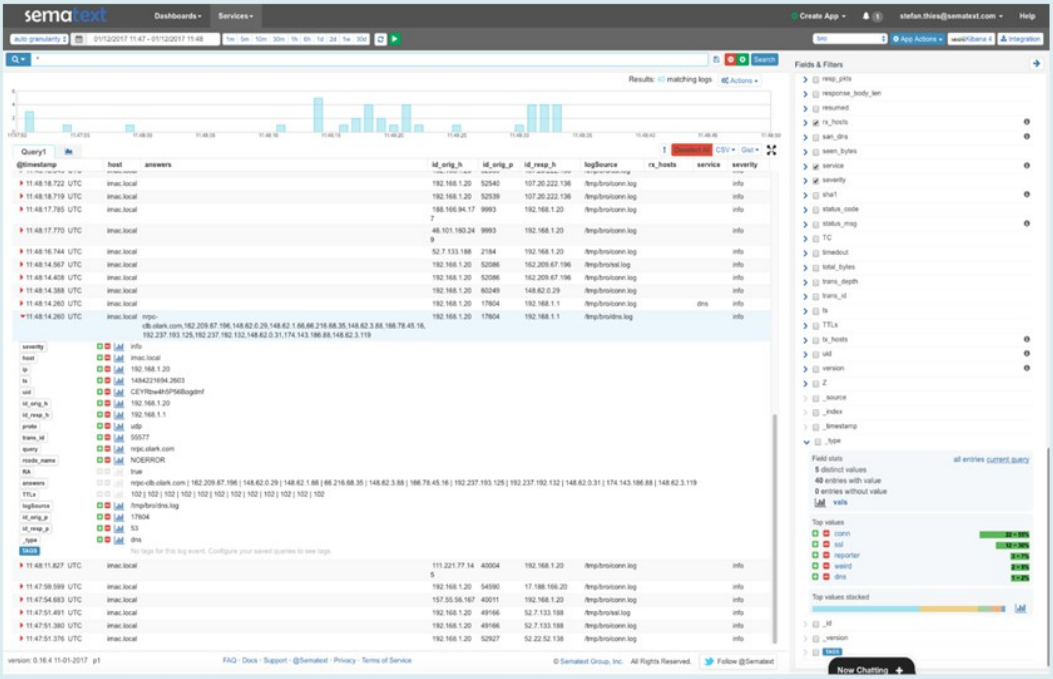
11

Bro Network Security Monitor



12

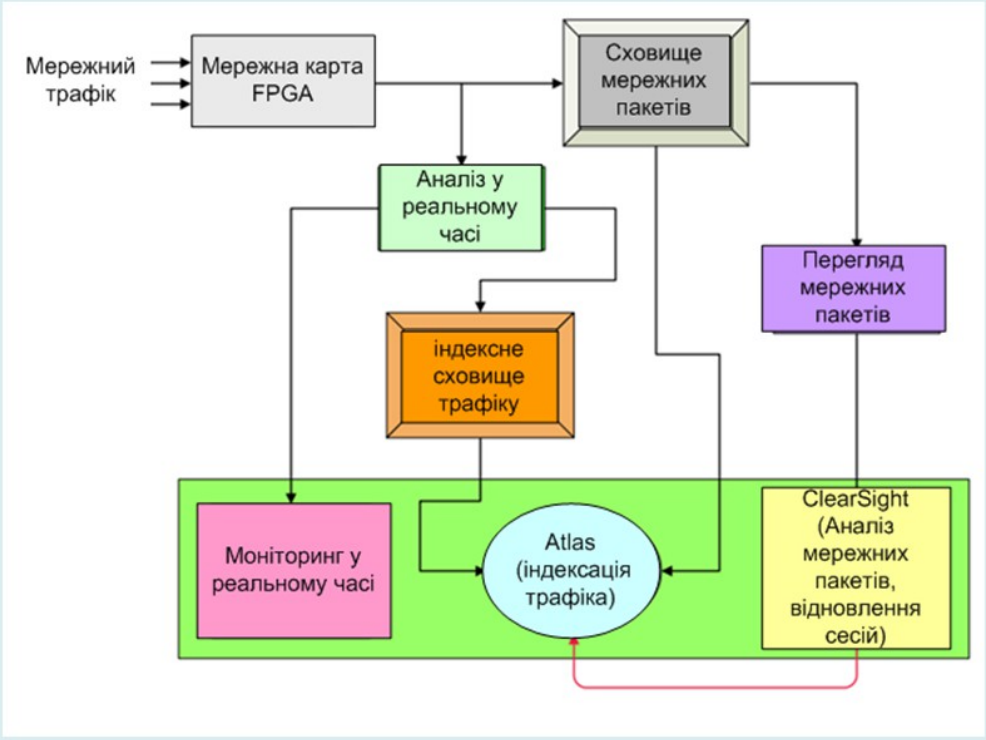
Bro Network Security Monitor. Аналіз трафіку за допомогою Bro



Snort

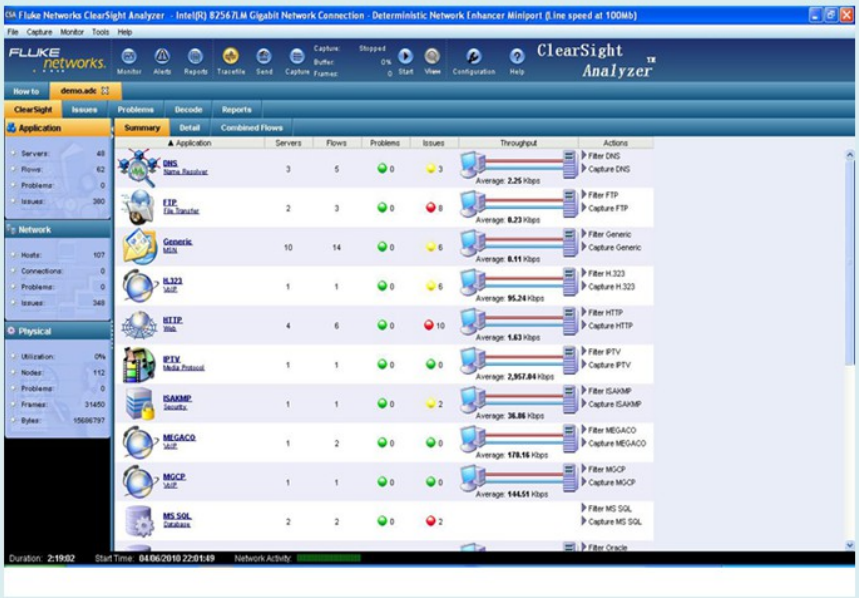
14

ClearSight Analyzer

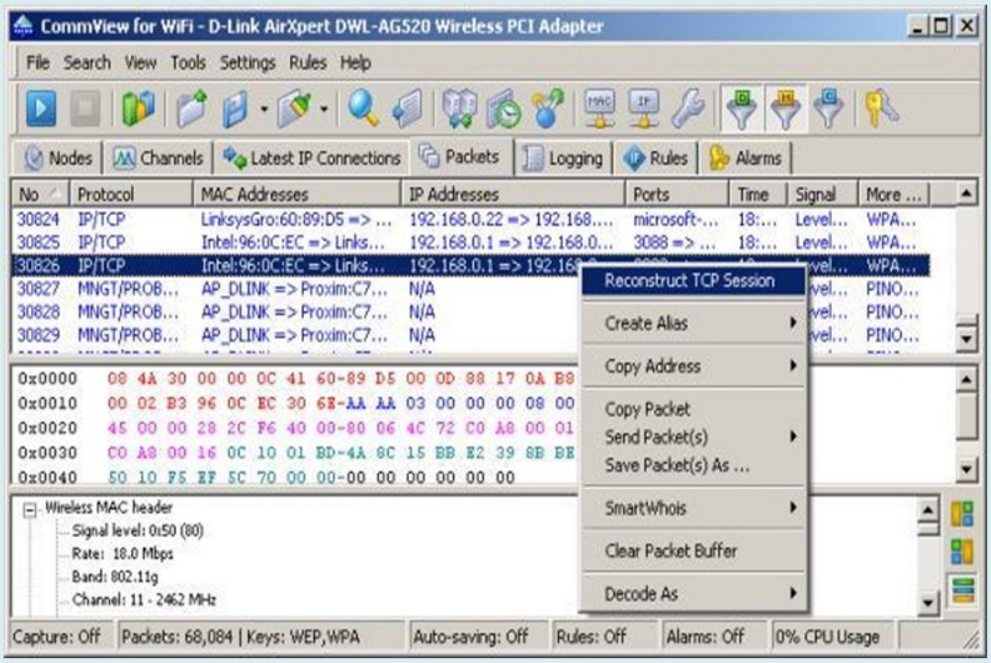


15

ClearSight Analyzer. Активність в мережі

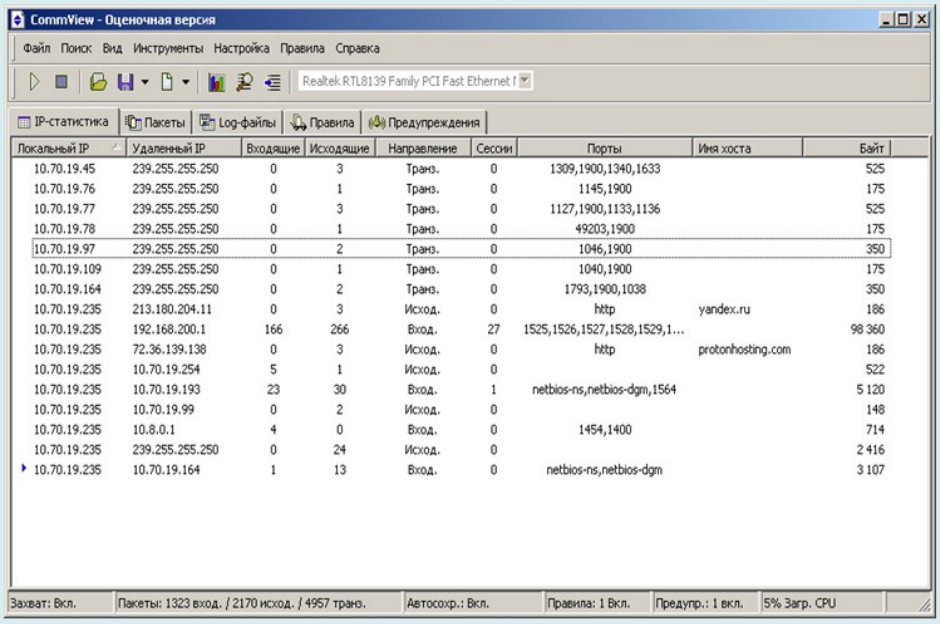


CommView



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-потоку). 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 відкинуті 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	-	-	-	-	-	-
Min крок між звітами	0,001 с.	1 с.	1 с.	1 с.	0,001 с	1 с.
Зміна min 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 легкісті 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.

Позначення	Найменування	Дод. відомості
	Текстові документи	
1.	Пояснювальна записка	76с.

Змін.	Арк.	Номер докум.	Підпис	Дата
Розроб.		Кузьмінов		
Перевір.		Скорик		
Н. контр.		Скорик		
Затв.		Безрук		

Дослідження програм з інжинірингу трафіка
Відомість кваліфікаційної роботи

Літ.	Аркуш	Аркушів
У	1	1

ХНУРЕ
кафедра ІМІ