AHAЛИЗ ТРАФИКА В WIRESHARK

Работу выполнил:

И.О. Фамилия А.Г. Саргсян

студбилет: 1032201740

Группа: НПИбд-02-20

ЦЕЛЬ РАБОТЫ

Изучение посредством Wireshark кадров Ethernet, анализ PDU протоколов транспортного и прикладного уровней стека TCP/IP.

```
C:\WINDOWS\system32>ping mail.ru
Обмен пакетами с MAIL.ru [94.100.180.200] с 32 байтами данных:
Ответ от 94.100.180.200: число байт=32 время=53мс TTL=56
Ответ от 94.100.180.200: число байт=32 время=55мс TTL=56
Ответ от 94.100.180.200: число байт=32 время=57мс TTL=56
Ответ от 94.100.180.200: число байт=32 время=51мс TTL=56
Статистика Ping для 94.100.180.200:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 51мсек, Максимальное = 57 мсек, Среднее = 54 мсек
C:\WINDOWS\system32>_
```

IIIU	Intu						
).	Time	Source	Destination	Protocol	Length	Info	
	600 8.064243	172.16.36.180	188.184.103.157	HTTP		601 GET /topics/birth-web HTTP/1.1	
	622 8.150599	188.184.103.157	172.16.36.180	HTTP		173 HTTP/1.1 302 Found	
	7029 31.815903	172.16.36.180	93.184.220.29	HTTP		286 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBQS14tALDViBvqCf47YkiQRtKz1BAQUpc436uuwdQ6UZ4i0RfrZJBCHlh8CEAebp5W0VNX9V1EL	
	7037 31.882749	93.184.220.29	172.16.36.180	OCSP		601 Response	
	7129 32.123965	172.16.36.180	104.18.32.68	HTTP		287 GET /MFIwUDBOMEwwSjAJBgUrDgMCGgUABBQh80WaEMqmyEvaHj1isSfVM4p8SAQUF9nWJSdn%2BTHCSUPZMDZEjGypT%2BsCEQCTzO2d5Q5Z	
	7138 32.203710	104.18.32.68	172.16.36.180	OCSP		1046 Response	
1	11219 114.995577	172.16.36.180	188.184.103.157	HTTP		590 GET /about HTTP/1.1	
1	11238 115.064823	188.184.103.157	172.16.36.180	HTTP		162 HTTP/1.1 302 Found	
1	12119 119.548964	172.16.36.180	172.16.37.116	HTTP		350 GET /ws/app/YouTube HTTP/1.1	
1	12121 119.665177	172.16.37.116	172.16.36.180	HTTP/XML		478 HTTP/1.1 200 OK	

✓ Wireshark · Пакет 600 · 3.4.pcapng _ _ > Frame 600: 601 bytes on wire (4808 bits), 601 bytes captured (4808 bits) on interface \Device\NPF_{C11EDED0-90E6-4F5E-BA1F-D2CB81CF24CC}, id 0 v Ethernet II, Src: IntelCor_67:eb:02 (40:ec:99:67:eb:02), Dst: Cisco_60:9c:d2 (70:18:a7:60:9c:d2) v Destination: Cisco_60:9c:d2 (70:18:a7:60:9c:d2) Address: Cisco_60:9c:d2 (70:18:a7:60:9c:d2)0. = LG bit: Globally unique address (factory default)0 = IG bit: Individual address (unicast) Source: IntelCor 67:eb:02 (40:ec:99:67:eb:02) Address: IntelCor_67:eb:02 (40:ec:99:67:eb:02)0. = LG bit: Globally unique address (factory default)0 = IG bit: Individual address (unicast) Type: IPv4 (0x0800) ✓ Internet Protocol Version 4, Src: 172.16.36.180, Dst: 188.184.103.157 0100 = Version: 4 0101 = Header Length: 20 bytes (5) > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 587 Identification: 0x384e (14414) > Flags: 0x40, Don't fragment ...0 0000 0000 0000 = Fragment Offset: 0 Time to Live: 128 Protocol: TCP (6) Header Checksum: 0x0000 [validation disabled] [Header checksum status: Unverified] Source Address: 172.16.36.180

вывод

- 1. Я научился захватывать пакеты с помощью Wireshark
- 2. Научился найти нужную информацию из них
- 3. Проанализировал PDU протоколы транспортного и прикладного уровней TCP/IP