



МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ННК «ІПСА» НТУУ «КПІ ІМ. ІГОРЯ СІКОРСЬКОГО»
КАФЕДРА ММСА

Лабораторна робота № 1

З дисципліни: Комп'ютерні мережі

Основи захоплення та аналізу пакетів

Виконала:

Студентка III курсу

Групи КА-71

Кічангіна О.Є.

Перевірив: Кухарєв С. О.

Київ 2020

Мета роботи: оволодіти методами роботи в середовищі захоплення та аналізу пакетів.

Хід виконання роботи

Відсилки першого пакету із запитом сторінки

No.	Time	Source	Destination	Protocol	Length	Info
297	6.442813	192.168.134.198	128.119.245.12	HTTP	463	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
344	7.147854	128.119.245.12	192.168.134.198	HTTP	504	HTTP/1.1 200 OK (text/html)
415	8.194542	192.168.134.198	17.253.55.201	HTTP	357	GET /ocsp04-aaica02/ME4wTKADAgEAMEUwQzBBMAKGBSs0AwIaBQAEFNqvF%2BZa6oA4ceFRLsAWwEInjUhJBBQx6napI3S139T9...
481	8.720499	17.253.55.201	192.168.134.198	OCSP	308	Response
610	9.717687	192.168.134.198	17.253.55.207	HTTP	357	GET /ocsp04-aaica02/ME4wTKADAgEAMEUwQzBBMAKGBSs0AwIaBQAEFNqvF%2BZa6oA4ceFRLsAWwEInjUhJBBQx6napI3S139T9...
714	10.821951	17.253.55.207	192.168.134.198	OCSP	290	Response

▶ Frame 297: 463 bytes on wire (3704 bits), 463 bytes captured (3704 bits) on interface en0, id 0
▶ Ethernet II, Src: Apple_70:4e:e0 (60:30:d4:70:4e:e0), Dst: ASUSTekC_67:19:61 (00:18:f3:67:19:61)
▶ Internet Protocol Version 4, Src: 192.168.134.198, Dst: 128.119.245.12
▶ Transmission Control Protocol, Src Port: 64852, Dst Port: 80, Seq: 1, Ack: 1, Len: 397
▼ Hypertext Transfer Protocol
▶ GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\nHost: gaia.cs.umass.edu\r\nUpgrade-Insecure-Requests: 1\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\nUser-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15\r\nAccept-Language: ru\r\nAccept-Encoding: gzip, deflate\r\nConnection: keep-alive\r\n\r\n[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
[HTTP request 1/1]
[Response in frame: 344]

Отримання першого пакету із відповіддю сервера

No.	Time	Source	Destination	Protocol	Length	Info
297	6.442813	192.168.134.198	128.119.245.12	HTTP	463	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
344	7.147854	128.119.245.12	192.168.134.198	HTTP	504	HTTP/1.1 200 OK (text/html)
415	8.194542	192.168.134.198	17.253.55.201	HTTP	357	GET /ocsp04-aaica02/ME4wTKADAgEAMEUwQzBBMAKGBSs0AwIaBQAEFNqvF%2BZa6oA4ceFRLsAWwEInjUhJBBQx6napI3S139T9...
481	8.720499	17.253.55.201	192.168.134.198	OCSP	308	Response
610	9.717687	192.168.134.198	17.253.55.207	HTTP	357	GET /ocsp04-aaica02/ME4wTKADAgEAMEUwQzBBMAKGBSs0AwIaBQAEFNqvF%2BZa6oA4ceFRLsAWwEInjUhJBBQx6napI3S139T9...
714	10.821951	17.253.55.207	192.168.134.198	OCSP	290	Response

▶ Frame 344: 504 bytes on wire (4032 bits), 504 bytes captured (4032 bits) on interface en0, id 0
▶ Ethernet II, Src: ASUSTekC_67:19:61 (00:18:f3:67:19:61), Dst: Apple_70:4e:e0 (60:30:d4:70:4e:e0)
▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.134.198
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 64852, Seq: 1, Ack: 398, Len: 438
▼ Hypertext Transfer Protocol
▶ HTTP/1.1 200 OK\r\nDate: Tue, 03 Mar 2020 13:39:37 GMT\r\nServer: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3\r\nLast-Modified: Tue, 03 Mar 2020 06:59:03 GMT\r\nETag: "51-59fedd6cb932e"\r\nAccept-Ranges: bytes\r\nContent-Length: 81\r\nKeep-Alive: timeout=5, max=100\r\nConnection: Keep-Alive\r\nContent-Type: text/html; charset=UTF-8\r\n\r\n[HTTP response 1/1]
[Time since request: 0.705041000 seconds]
[Request in frame: 297]

Контрольні питання

1. Які протоколи відображалися в вікні лістингу протоколів до включення фільтрації?
MDNS, TCP, HTTP, DNS, TLSv1.2, ARP, DHCP, ICMPv6, SSDP
2. Які протоколи використовувалися в збережених пакетах запиту та відповіді?
HTTP
3. Який період часу пройшов з часу відсилки першого пакету із запитом сторінки до отримання першого пакету з відповіддю сервера?
Пройшло 0,705941000 с.
4. Якими були вихідна та цільова адреси пакетів із запитом та із відповіддю?
Запит:
Вихідна: 192.168.134.198
Цільова: 128.119.245.12
Відповідь:
Вихідний: 128.119.245.12
Цільовий: 192.168.134.198
5. Яким був перший рядок запиту на рівні протоколу HTTP?
GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
6. Яким був перший рядок відповіді на рівні протоколу HTTP?
HTTP/1.1 200 OK (text/html)

Висновок

В ході виконання даної лабораторної роботи, були набуті навички використання програми Wireshark для захоплення пакетів. Було проаналізовано час за який було відправлено перший запит та отримано першу відповідь, а також було розглянуто протоколи HTTP.