МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАВЧАЛЬНО-НАУКОВИЙ КОМПЛЕКС
«ІНСТИТУТ ПРИКЛАДНОГО СИСТЕМНОГО АНАЛІЗУ»
НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»
КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ СИСТЕМНОГО АНАЛІЗУ

Практична робота №1
з курсу «Комп'ютерні мережі»

Виконав: студент 3 курсу
групи КА-74
Королюк Д.О.
Прийняв: Кухарєв С.О.

Київ – 2020р.

Запит:

Frame 91: 558 bytes on wire (4464 bits), 558 bytes captured (4464 bits) on interface \Device\NPF_{02DF4F74-5D72-4C21-BA18-F120F10D4FED}, id 0
Ethernet II, Src: CyberTAN_c2:ea:a9 (60:14:b3:c2:ea:a9), Dst: 66:c2:de:fb:31:14 (66:c2:de:fb:31:14)
Internet Protocol Version 4, Src: 192.168.43.213, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 49964, Dst Port: 80, Seq: 1, Ack: 1, Len: 504
Hypertext Transfer Protocol
GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
DNT: 1\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7,uk;q=0.6\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
[HTTP request 1/2]
[Response in frame: 95]
[Next request in frame: 97]

Відповідь:

Frame 95: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{02DF4F74-5D72-4C21-BA18-F120F10D4FED}, id 0
Ethernet II, Src: 66:c2:de:fb:31:14 (66:c2:de:fb:31:14), Dst: CyberTAN_c2:ea:a9 (60:14:b3:c2:ea:a9)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.43.213
Transmission Control Protocol, Src Port: 80, Dst Port: 49964, Seq: 1, Ack: 505, Len: 438
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Wed, 26 Feb 2020 09:47:56 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Wed, 26 Feb 2020 06:59:03 GMT\r\n
ETag: "51-59f7523c53b13"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 81\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 1/2]
[Time since request: 0.183360000 seconds]
[Request in frame: 91]
[Next request in frame: 97]
[Next response in frame: 98]
[Request URI: http://gaia.cs.umass.edu/favicon.ico]
File Data: 81 bytes
Line-based text data: text/html (3 lines)

Повторний запит:

Frame 97: 490 bytes on wire (3920 bits), 490 bytes captured (3920 bits) on interface \Device\NPF_{02DF4F74-5D72-4C21-BA18-F120F10D4FED}, id 0
Ethernet II, Src: CyberTAN_c2:ea:a9 (60:14:b3:c2:ea:a9), Dst: 66:c2:de:fb:31:14 (66:c2:de:fb:31:14)
Internet Protocol Version 4, Src: 192.168.43.213, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 49964, Dst Port: 80, Seq: 505, Ack: 439, Len: 436
Hypertext Transfer Protocol
GET /favicon.ico HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36\r\n
DNT: 1\r\n
Accept: image/webp,image/apng,image/*,*/*;q=0.8\r\n
Referer: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7,uk;q=0.6\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/favicon.ico]
[HTTP request 2/2]
[Prev request in frame: 91]
[Response in frame: 98]

Відповідь:

Frame 98: 538 bytes on wire (4304 bits), 538 bytes captured (4304 bits) on interface \Device\NPF_{02DF4F74-5D72-4C21-BA18-F120F10D4FED}, id 0
Ethernet II, Src: 66:c2:de:fb:31:14 (66:c2:de:fb:31:14), Dst: CyberTAN_c2:ea:a9 (60:14:b3:c2:ea:a9)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.43.213
Transmission Control Protocol, Src Port: 80, Dst Port: 49964, Seq: 439, Ack: 941, Len: 484
Hypertext Transfer Protocol
HTTP/1.1 404 Not Found\r\n
Date: Wed, 26 Feb 2020 09:47:57 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3\r\n
Content-Length: 209\r\n
Keep-Alive: timeout=5, max=99\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=iso-8859-1\r\n
\r\n
[HTTP response 2/2]
[Time since request: 0.182835000 seconds]
[Prev request in frame: 91]
[Prev response in frame: 95]
[Request in frame: 97]
[Request URI: http://gaia.cs.umass.edu/favicon.ico]
File Data: 209 bytes
Line-based text data: text/html (7 lines)

Контрольні запитання:
1. Які протоколи відображалися в вікні лістингу протоколів до включення фільтрації?
MDNS, SSDP, ICMPv6, DNS, ICMP, TCP, IGMPv2

In computer networking, the multicast Domain Name System (mDNS) resolves host names to IP addresses within small networks that do not include a local name server. It is a zero-configuration service, using essentially the same programming interfaces, packet formats and operating semantics as the unicast Domain Name System (DNS).

The Simple Service Discovery Protocol (SSDP) is a network protocol based on the Internet Protocol Suite for advertisement and discovery of network services and presence information. It accomplishes this without assistance of server-based configuration mechanisms, such as the Dynamic Host Configuration Protocol (DHCP) or the Domain Name System (DNS), and without special static configuration of a network host. SSDP is the basis of the discovery protocol of Universal Plug and Play (UPnP) and is intended for use in residential or small office environments.

Internet Control Message Protocol version 6 (ICMPv6) is the implementation of the Internet Control Message Protocol (ICMP) for Internet Protocol version 6 (IPv6) defined in RFC 4443.[1] ICMPv6 is an integral part of IPv6 and performs error reporting and diagnostic functions (e.g., ping), and has a framework for extensions to implement future changes.

The Domain Name System delegates the responsibility of assigning domain names and mapping those names to Internet resources by designating authoritative name servers for each domain.

The Internet Control Message Protocol (ICMP) is one of the main protocols of the internet protocol suite. It is used by network devices, like routers, to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached. ICMP can also be used to relay query messages. It is assigned protocol number 1. ICMP differs from transport protocols such as TCP and UDP in that it is not typically used to exchange data between systems, nor is it regularly employed by end-user network applications (with the exception of some diagnostic tools like ping and traceroute).

The Transmission Control Protocol provides a communication service at an intermediate level between an application program and the Internet Protocol. It provides host-to-host connectivity at the Transport Layer of the Internet model.

The Internet Group Management Protocol (IGMP) is a communications protocol used by hosts and adjacent routers on IPv4 networks to establish multicast group memberships. IGMP is an integral part of IP multicast. IGMP can be used for one-to-many networking applications such as online streaming video and gaming, and allows more efficient use of resources when supporting these types of applications. IGMP is used on IPv4 networks. Multicast management on IPv6 networks is handled by Multicast Listener Discovery (MLD) which uses ICMPv6 messaging in contrast to IGMP's bare IP encapsulation.

2. Які протоколи використовувалися в збережених пакетах запиту та відповіді?
Ethernet II, Internet Protocol Version 4, Transmission Control Protocol

3. Який період часу пройшов з часу відсилки першого пакету із запитом сторінки до отримання першого пакету з відповіддю сервера?
0.183360000 seconds

4. Якими були вихідна та цільова адреси пакетів із запитом та із відповіддю?
192.168.43.213 128.119.245.12
128.119.245.12 192.168.43.213

5. Яким був перший рядок запиту на рівні протоколу HTTP?
GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n

6. Яким був перший рядок відповіді на рівні протоколу HTTP?
HTTP/1.1 200 OK\r\n

Висновок: на цій роботі я навчився використовувати програму Wireshark та за допомогою неї виловлювати пакети з даними.