



SVUIS
Syrian Virtual University



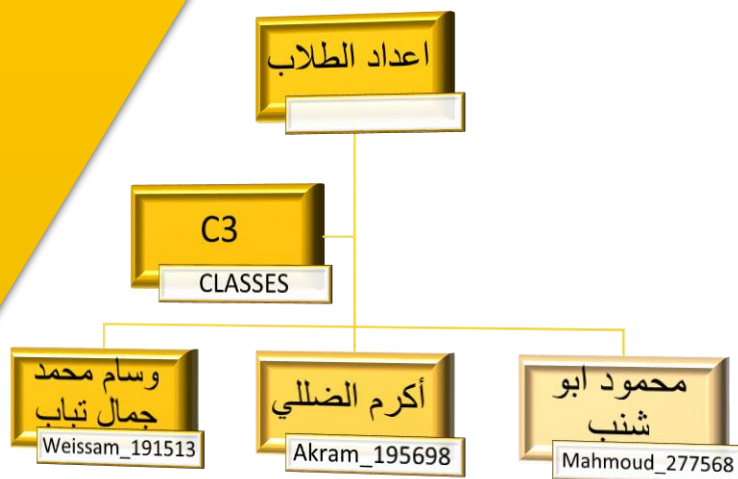
خدمات الشبكات

F23

INT202

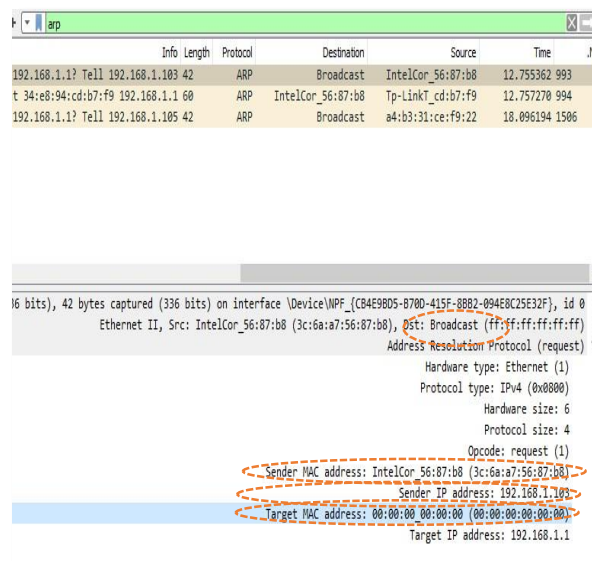
أشراف الدكتور

فراس
عيسى



1. Run Wireshark and start capturing packets
2. Go to cmd
3. Type: arp -a
4. Type: arp -d *
5. Go to Wireshark, stop capturing and filter packet using arp filter

Question	Answer
What is Packet's type and numbers?	Broadcast 2 packets
What is Sender MAC Address?	3c:6a: a7:56:87: b8
What is Sender IP address?	192.168.1.103
What is destination MAC address?	00:00:00: 00:00:00
What is Destination MAC address Type?	Broadcast
What is Target IP address?	192.168.1.1
What is Sender MAC Address (Response packet)?	34: e8:94:cd: b7: f9
What is Sender IP address (Response packet)?	192.168.1.1
What is destination MAC address (Response packet)?	IntelCor_56:87: b8 (3c:6a: a7:56:87: b8)
What is Target IP address (Response packet)?	192.168.1.103
What is the value of Opcode?	2





السؤال الثاني:

حذف معلومات الذاكرة الخابية من الحاسب.

٢- حذف معلومات الذاكرة الخابية من متصفح الإنترنت.

٣- شغل Wireshark.

٤- أطلب العنوان <https://arabic.rt.com> :

٥- أوقف التقاط الطرود.

سنحاول الآن التقاط طرود HTTP التي تحدث أثناء تصفح الإنترنت بدون تدخل المستخدم.

Question	Answer
IP address for https://arabic.rt.com/ ?	34.246.219.147
Request Packet Host	arabic.rt.com
Destination Port?	443
HTTP version	HTTP/1.1
Response status?	200 OK
Last-Modified?	Mon, 01 Apr 2024 1:31:22 GMT
Server Type?	nginx
How many TCP segments are used to carry the response?	TCP segment data (22 bytes)
Content Length	2638
Does server use cookies?	Yes



توثيق عمليات التقاط طرود HTTP التي تحدث أثناء تصفح الإنترنت بدون تدخل المستخدم بالصور.

HTTP/1.1 GET REQUEST ^	200 RESPONSE ^
METHOD: GET +	STATUS: 200OK +
URL	HEADERS
+ https://arabic.rt.com/static/img/recaptcha.svg	+ Accept-Ranges: bytes
HEADERS	+ Cache-Control: public, max-age=31536000, proxy-revalidate
+ Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8	+ Connection: keep-alive
+ Accept-Encoding: gzip, deflate, br, zstd	+ Content-Encoding: gzip
+ Accept-Language: ar,en-US;q=0.9,en;q=0.8	+ Content-Length: 2638
+ Connection: keep-alive	+ Content-Security-Policy: upgrade-insecure-requests
+ Cookie: _ym_uid=1719592101487477763; _ym_d=1719592101; _ym_visorc=b; _ym_isad=1; _ga=GA1.2.2074170931.1719592108; _gid=GA1.2.2131167200.1719592108	+ Content-Type: image/svg+xml
+ Host: arabic.rt.com	+ Date: Fri, 28 Jun 2024 16:28:53 GMT
+ Referer: https://arabic.rt.com/	+ ETag: W/"660a9b0a-1c6a"
sec-ch-ua: "Google Chrome";v="123", "Not:A-Brand";v="8", "Chromium";v="123"	+ Expires: Fri, 28 Jun 2024 16:28:54 GMTSat, 28 Jun 2025 16:28:54 GMT
sec-ch-ua-mobile: ?0	+ Last-Modified: Mon, 01 Apr 2024 11:31:22 GMT
sec-ch-ua-platform: "Windows"	+ Server: nginx
+ Sec-Fetch-Dest: image	+ Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
+ Sec-Fetch-Mode: no-cors	+ Vary: Accept-Encoding
+ Sec-Fetch-Site: same-origin	x-4fna: 3brfna
+ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36	X-4vcta: H20459R
	+ X-Content-Type-Options: nosniff
	+ X-XSS-Protection: 1; mode=block



DNS: السؤال الثالث

1. عنوان IP للخوادم:

Host	IP address
www.shamra.sy	185.216.135.10
www.w3schools.com	112.221.133.221

```
C:\Windows\system32\cmd.exe
C:\Users\DELL 3576>nslookup www.shamra.sy
Server: UnKnown
Address: 192.168.1.1

Non-authoritative answer:
Name:   shamra.sy
Address: 185.216.135.10
Aliases: www.shamra.sy
```

```
C:\Windows\system32\cmd.exe
C:\Users\DELL 3576>nslookup www.w3schools.com
Server: UnKnown
Address: 192.168.1.1

Non-authoritative answer:
Name:   cs837.wac.edgecastcdn.net
Address: 192.229.133.221
Aliases: www.w3schools.com
```


2. معرفة أسماء مخدمات الأسماء وعناوين IP لها:

Host Name	Server IP address
ns-130.awsdns-16.com	205.251.195.56
ns-824.awsdns-39.net	205.251.196.120
ns-1144.awsdns-15.org	205.251.199.229
ns-2021.awsdns-60.co.uk	225.251.112.132

```
C:\Windows\system32\cmd.exe
C:\Users\DELL 3576>nslookup -type=Ns www.amazon.com
Server: UnKnown
Address: 192.168.1.1

Non-authoritative answer:
www.amazon.com canonical name = tp.47cf2c8c9-frontier.amazon.com
tp.47cf2c8c9-frontier.amazon.com canonical name = d3ag4hukkh62yn.cloudfront.net
d3ag4hukkh62yn.cloudfront.net nameserver = ns-130.awsdns-16.com
d3ag4hukkh62yn.cloudfront.net nameserver = ns-824.awsdns-39.net
d3ag4hukkh62yn.cloudfront.net nameserver = ns-1144.awsdns-15.org
d3ag4hukkh62yn.cloudfront.net nameserver = ns-2021.awsdns-60.co.uk

ns-130.awsdns-16.com internet address = 205.251.192.130
ns-824.awsdns-39.net internet address = 205.251.195.56
ns-1144.awsdns-15.org internet address = 205.251.196.120
ns-2021.awsdns-60.co.uk internet address = 205.251.199.229
ns-130.awsdns-16.com AAAA IPv6 address = 2600:9000:5300:8200::1
ns-824.awsdns-39.net AAAA IPv6 address = 2600:9000:5303:3800::1
ns-1144.awsdns-15.org AAAA IPv6 address = 2600:9000:5304:7800::1
ns-2021.awsdns-60.co.uk AAAA IPv6 address = 2600:9000:5307:e500::1
```

3. معرفة name canonical للمخدم:

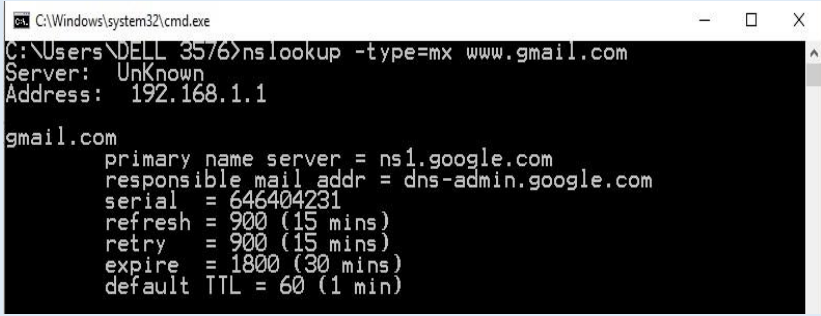
Host	Canonical name
www.svuonline.org	<p>svuonline.org</p> <pre>C:\Users\DELL 3576>nslookup -type=cname www.svuonline.org Server: UnKnown Address: 192.168.1.1 Non-authoritative answer: www.svuonline.org canonical name = svuonline.org</pre>

4. معرفة الاسم المقابل للعنوان التالي:

IP address	Name
213.178.227.252	<p>Non-existent domain</p> <pre>Microsoft Windows [Version 10.0.15053] (c) 2017 Microsoft Corporation. All rights reserved. C:\Users\DELL 3576>nslookup 213.178.227.252 Server: UnKnown Address: 192.168.1.1 *** UnKnown can't find 213.178.227.252: Non-existent domain C:\Users\DELL 3576>_</pre>



5. معرفة مخدم البريد الإلكتروني للموقع:

Name	Mail Server
www.gmail.com	<p>ns1.google.com</p> 

تنفيذ الأوامر التالية:

1. Run Wireshark and start capturing packets
2. Go to cmd
3. Type: nslookup www.mit.edu
4. Stop capturing packets
5. Click on the last DNS request query and fill the following table:

Question	Answer
What is DNS source and destination port for DNS request and response query?	Source: 192.168.1.6 Destination: 192.168.1.1 Req= 64277 53 Res= 64277 53
What is the type of DNS query Message?	Type= A
How many Answers in DNS query message?	0
DNS Flags value for the response?	0x8180
How many answers in DNS Response Message?	3
The content of each answer?	في الباكت
What is Authoritative name-servers?	dscb.akamaiedge.net



www.mit.edu 71	DNS	192.168.1.1	192.168.1.6	0.324245 5
akamaiedge.net AAA 203	DNS	192.168.1.6	192.168.1.1	0.751755 6

captured (568 bits) on interface \Device\NPF_{CB4E9BD5-B70D-415F-8BB2-094E8C25E32F}, id 0 <
II, Src: IntelCor_56:87:b8 (3c:6a:a7:56:87:b8), Dst: D-LinkIn_5a:1a:90 (74:da:da:5a:1a:90) <
Internet Protocol Version 4, Src: 192.168.1.6, Dst: 192.168.1.1 <
User Datagram Protocol, Src Port: 64277, Dst Port: 53 <
Source Port: 64277
Destination Port: 53
Length: 37
Checksum: 0x2e54 [unverified]
[Checksum Status: Unverified]
[Stream index: 1]
[Timestamps] <
UDP payload (29 bytes)
Domain Name System (query) <
Transaction ID: 0x0002
Flags: 0x0100 Standard query <
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries <
www.mit.edu: type A, class IN <
Name: www.mit.edu
[Name Length: 11]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)

www.mit.edu 71	DNS	192.168.1.1	192.168.1.6	0.324245 5
akamaiedge.net AAA 203	DNS	192.168.1.6	192.168.1.1	0.751755 6

Answers <
www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net <
Name: www.mit.edu
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 1800 (30 minutes)
Data length: 25
CNAME: www.mit.edu.edgekey.net
www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net <
Name: www.mit.edu.edgekey.net
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 60 (1 minute)
Data length: 24
CNAME: e9566.dscb.akamaiedge.net
e9566.dscb.akamaiedge.net: type A, class IN, addr 23.210.114.10 <
Name: e9566.dscb.akamaiedge.net
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 20 (20 seconds)
Data length: 4
Address: 23.210.114.10



