

PacketMaze Lab(wireshark)

一家公司的內部伺服器被標記存在異常網路活動，存在多個指向未知外部 IP 的出站連線。初步分析顯示可能存在資料外洩。請調查提供的網路日誌，以確定入侵來源和方法。

Tools:

Brim
suricatarunner
suricata.rules
NetworkMiner
Wireshark
MAC lookup

FTP 密碼是什麼？

找FTP

UNODC-GPC-001-003-JohnDoe-NetworkCapture-2021-04-29.pcapng

Wireshark - Follow TCP Stream (tcp.stream eq 10) - UNODC-GPC-001-003-JohnDoe-NetworkCapture-2021-04-29.pcapng

File Edit View Go Cap

tcp.stream eq 10

No.	Time
492	35.840412653
493	35.840472212
494	35.840523520
495	35.840527861
496	35.851219261
497	35.851494469
498	35.851516416
499	35.851521941
500	35.851770445
501	35.851835155
502	35.881821765
503	35.881904802
504	35.882780006
505	35.882924904
506	35.883091900
507	35.883100972

220 Welcome to Hacker FTP service.
AUTH TLS
530 Please login with USER and PASS.
AUTH SSL
530 Please login with USER and PASS.
USER kali
331 Please specify the password.
PASS AfricaCTF2021
230 Login successful.
SYST

AfricaCTF2021

第二季

使用的 DNS 伺服器的 IPv6 位址是什麼192.168.1.26 ?

Kali Linux 2023

UNODC-GPC-001-003-JohnDoe-NetworkCapture-2021-04-29.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
51	2.262634313	192.168.1.26	192.168.1.10	DNS	84	Standard query 0xa2ec A fp.msedge.net OPT
64	2.454518557	192.168.1.10	192.168.1.26	DNS	289	Standard query response 0xa2ec A fp.msedge.net
140	5.466737896	192.168.1.26	192.168.1.10	DNS	88	Standard query 0x3b76 A l-ring.msedge.net OPT
141	5.535145587	192.168.1.10	192.168.1.26	DNS	191	Standard query response 0x3b76 A l-ring.msedge
171	6.050208984	192.168.1.26	192.168.1.10	DNS	98	Standard query 0x303d A fp-vs-nocache.azureedge
172	6.131427861	192.168.1.10	192.168.1.26	DNS	421	Standard query response 0x303d A fp-vs-nocache
201	6.716987654	192.168.1.26	192.168.1.10	DNS	97	Standard query 0xd289 A a-ring-fallback.msedge
203	6.850862235	192.168.1.10	192.168.1.26	DNS	212	Standard query response 0xd289 A a-ring-fallback
238	8.767159684	192.168.1.26	192.168.1.10	DNS	111	Standard query 0x3800 A a-0001.a-afddentry.net
239	8.864876339	192.168.1.10	192.168.1.26	DNS	273	Standard query response 0x3800 A a-0001.a-afdd
464	20.373968341	192.168.1.26	192.168.1.10	DNS	88	Standard query 0x6820 A t-ring.msedge.net OPT
474	25.432264559	fe80::b011:ed39:866..	fe80::c80b:adff:fea:1db7	DNS	108	Standard query 0x6820 A t-ring.msedge.net OPT
475	25.539326475	fe80::c80b:adff:fea:..	fe80::b011:ed39:8665:3b0a	DNS	197	Standard query response 0x6820 A t-ring.msedge
11844	75.330610869	fe80::b011:ed39:866..	fe80::c80b:adff:fea:1db7	DNS	120	Standard query 0x2a59 A connectivity-check.ubuntu
11845	75.353487745	fe80::c80b:adff:fea:..	fe80::b011:ed39:8665:3b0a	DNS	168	Standard query response 0x2a59 A connectivity
11859	79.870010218	fe80::b011:ed39:866..	fe80::c80b:adff:fea:1db7	DNS	123	Standard query 0x7670 A geo.prod.do.dsp.mp.microsoft
11860	80.217965943	fe80::c80b:adff:fea:..	fe80::b011:ed39:8665:3b0a	DNS	547	Standard query response 0x7670 A geo.prod.do.d

Frame 51: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface wl01, id 0x0000 ca 0b ad ad 20 ba 08 09 a8 57 47 93 08 08
 Ethernet II, Src: Intel_57:47:93 (c8:09:a8:57:47:93), Dst: ca:0b:ad:ad:20:ba (ca:0b:ad:ad:20:ba)
 Destination: ca:0b:ad:ad:20:ba (ca:0b:ad:ad:20:ba)
 Source: Intel_57:47:93 (c8:09:a8:57:47:93)
 Type: IPv4 (0x0800)
 [Stream index: 0]
 Internet Protocol Version 4, Src: 192.168.1.26, Dst: 192.168.1.10
 User Datagram Protocol, Src Port: 36116, Dst Port: 53
 Domain Name System (query)

Source Hardware Address (eth.src), 6 byte(s) | Packets: 45024 · Displayed: 163 (0.4%) | Profile: Default

c8:09:a8:57:47:93 <=ipv4的mac

Wireshark - Conversations · UNODC-GPC-001-003-JohnDoe-NetworkCapture-2021-04-29.pcapng

Conversation Settings

- Name resolution
- Absolute start time
- Limit to display filter

Ethernet · 1 IPv4 · 1 IPv6 · 1 TCP UDP · 81

Address A	Address B	Packets	Bytes	Stream ID	Total Packets	Percent Filtered	Packets A → B	Bytes A → B
c8:09:a8:57:47:93	ca:0b:ad:ad:20:ba	163	40 kB	0	33,552	0.49%	82	10 kB

Wireshark - Conversations · UNODC-GPC-001-003-JohnDoe-NetworkCapture-2021-04-29.pcapng

Conversation Settings

- Name resolution
- Absolute start time
- Limit to display filter

Ethernet · 1 IPv4 · 1 IPv6 · 1 TCP UDP · 81

Address A Address B Total Packets Percent Filtered Packets A → B Bytes A → B

c8:09:a8:57:47:93 ca:0b:ad:ad:20:ba 33,552 0.49% 82 10 kB

Apply as Filter Prepare as Filter Find Selected A ↔ B
 Not Selected A → B
 ...and Selected B → A
 ...or Selected A ↔ Any
 ...and not Selected A → Any
 ...or not Selected Any → A
 Any ↔ B
 Any → B
 B → Any

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

Packet list Display filter eth.addr==c8:09:a8:57:47:93 & eth.addr==ca:0b:ad:ad:20:ba

Options: Narrow & Wide Case sensitive Backwards Multiple occurrences

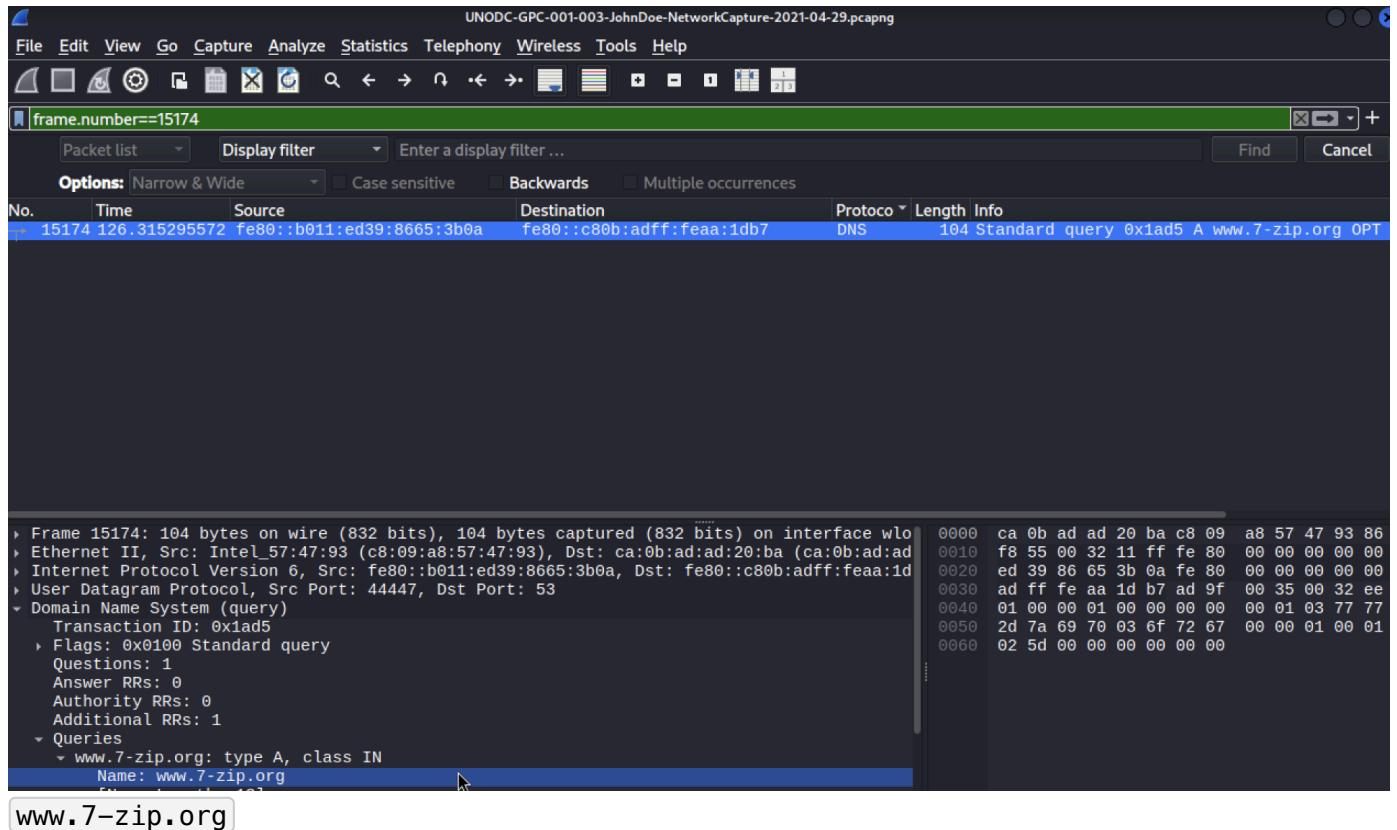
No.	Time	Source	Destination	Protocol	Length	Info
239	8.864876339	192.168.1.10	192.168.1.26	DNS	273	Standard query response 0x3800 A a-0001.a-afddentry.net
464	20.373968341	192.168.1.26	192.168.1.10	DNS	88	Standard query 0x6820 A t-ring.msedge.net
474	25.432264559	fe80::b011:ed39:8665:3b0a	fe80::c80b:adff:fea:1db7	DNS	108	Standard query 0x6820 A t-ring.msedge.net
475	25.539326475	fe80::c80b:adff:fea:1db7	fe80::b011:ed39:8665:3b0a	DNS	197	Standard query response 0x6820 A t-ring.msedge
11844	75.330610869	fe80::b011:ed39:8665:3b0a	fe80::c80b:adff:fea:1db7	DNS	120	Standard query 0x2a59 A connectivity-check.ubuntu
11845	75.353487745	fe80::c80b:adff:fea:1db7	fe80::b011:ed39:8665:3b0a	DNS	168	Standard query response 0x2a59 A connectivity
11859	79.870010218	fe80::b011:ed39:8665:3b0a	fe80::c80b:adff:fea:1db7	DNS	123	Standard query 0x7670 A geo.prod.do.dsp.mp.microsoft
11860	80.217965943	fe80::c80b:adff:fea:1db7	fe80::b011:ed39:8665:3b0a	DNS	547	Standard query response 0x7670 A geo.prod.d
11887	80.895056573	fe80::b011:ed39:8665:3b0a	fe80::c80b:adff:fea:1db7	DNS	125	Standard query 0xa6ce A kv501.prod.d

fe80::c80b:adff:fea:1db7

第三季

使用者在資料包中尋找哪個網域15174 ?

參數 : frame.number==15174



第四季

192.168.1.26從到 總共發送了多少個 UDP 封包24.39.217.246 ?

參數 : udp and ip.src 192.168.1.26 and ip.dst_host 24.39.217.246

UNODC-GPC-001-003-JohnDoe-NetworkCapture-2021-04-29.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp and ip.src==192.168.1.26 and ip.dst_host==24.39.217.246

Packet list Display filter Enter a display filter ...

Options: Narrow & Wide Case sensitive Backwards Multiple occurrences

No.	Time	Source	Destination	Protocol	Length	Info
15806	128.281136434	192.168.1.26	24.39.217.246	UDP	94	53638 → 54150 Len=52
15808	128.283606894	192.168.1.26	24.39.217.246	UDP	94	51601 → 54150 Len=52
15825	130.239091258	192.168.1.26	24.39.217.246	UDP	94	53638 → 54150 Len=52
15851	132.241685345	192.168.1.26	24.39.217.246	UDP	94	53638 → 54150 Len=52
15865	135.324998370	192.168.1.26	24.39.217.246	UDP	94	53638 → 54150 Len=52
15942	137.223543961	192.168.1.26	24.39.217.246	UDP	94	53638 → 54150 Len=52
16095	139.223629695	192.168.1.26	24.39.217.246	UDP	94	53638 → 54150 Len=52
16695	143.331929739	192.168.1.26	24.39.217.246	UDP	94	53638 → 54150 Len=52
16810	145.217958711	192.168.1.26	24.39.217.246	UDP	94	53638 → 54150 Len=52
16955	147.222253195	192.168.1.26	24.39.217.246	UDP	94	53638 → 54150 Len=52

Frame 15806: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface wlo1,
Ethernet II, Src: Intel_57:47:93 (c8:09:a8:57:47:93), Dst: ca:0b:ad:ad:20:ba (ca:0b:ad:ad:
Internet Protocol Version 4, Src: 192.168.1.26, Dst: 24.39.217.246
User Datagram Protocol, Src Port: 53638, Dst Port: 54150
Data (52 bytes)

0000 ca 0b ad ad 20 ba c8
0010 00 50 4f 3a 00 00 7f
0020 d9 f6 d1 86 d3 86 00
0030 3b 15 20 01 00 00 34
0040 27 b7 20 01 00 00 28
0050 26 09 01 04 00 00 00

UNODC-GPC-001-003-JohnDoe-NetworkCapture-2021-04-29.pcapng Packets: 45024 · Displayed: 10 (0.0%)

10

問5

PCAP 檔案中被調查系統的 MAC 位址是什麼？

同上，我們要調查src ip

c8:09:a8:57:47:93

問6

用來拍照的相機型號是什麼20210429_152157.jpg ?

參數 : ftp contains "20210429_152157.jpg" , 確定為FTP抓此檔案

UNODC-GPC-001-003-JohnDoe-NetworkCapture-2021-04-29.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ftp contains "20210429_152157.jpg"

Packet list Display filter Enter a display filter ...

Options: Narrow & Wide Case sensitive Backwards Multiple occurrences

No.	Time	Source	Destination	Protocol	Length	Info
7070	65.244555975	192.168.1.26	192.168.1.20	FTP	92	Request: STOR 20210429_152157.jpg

File **Edit** **View** **Go** **Capture** **Analyze** **Statistics** **Telephony** **Wireless**

- Open** Ctrl+O
- Open Recent**
- Merge...**
- Import from Hex Dump...**
- Close** Ctrl+W
- Save** Ctrl+S
- Save As...** Ctrl+Shift+S
- File Set**
- Export Specified Packets...**
- Export Packet Dissections**
- Export Packet Bytes...** Ctrl+Shift+X
- Export PDUs to File...**
- Strip Headers...**
- Export TLS Session Keys...**
- Export Objects**
- Print...** Ctrl+P
- Quit** Ctrl+Q

▶ **File Transfer Protocol (FTP)**
[Current working directory: /home/kali/]

Wireshark - Export · FTP-DATA object list

Text Filter: Content Type:

Packet	Hostname	Content Type	Size	Filename
512	192.168.1.26	FTP file	8,519 kB	20210429_152321.jpg
7076	192.168.1.26	FTP file	8,018 kB	20210429_152157.jpg
1837	192.168.1.20	FTP file	239 bytes	accountNum.zip

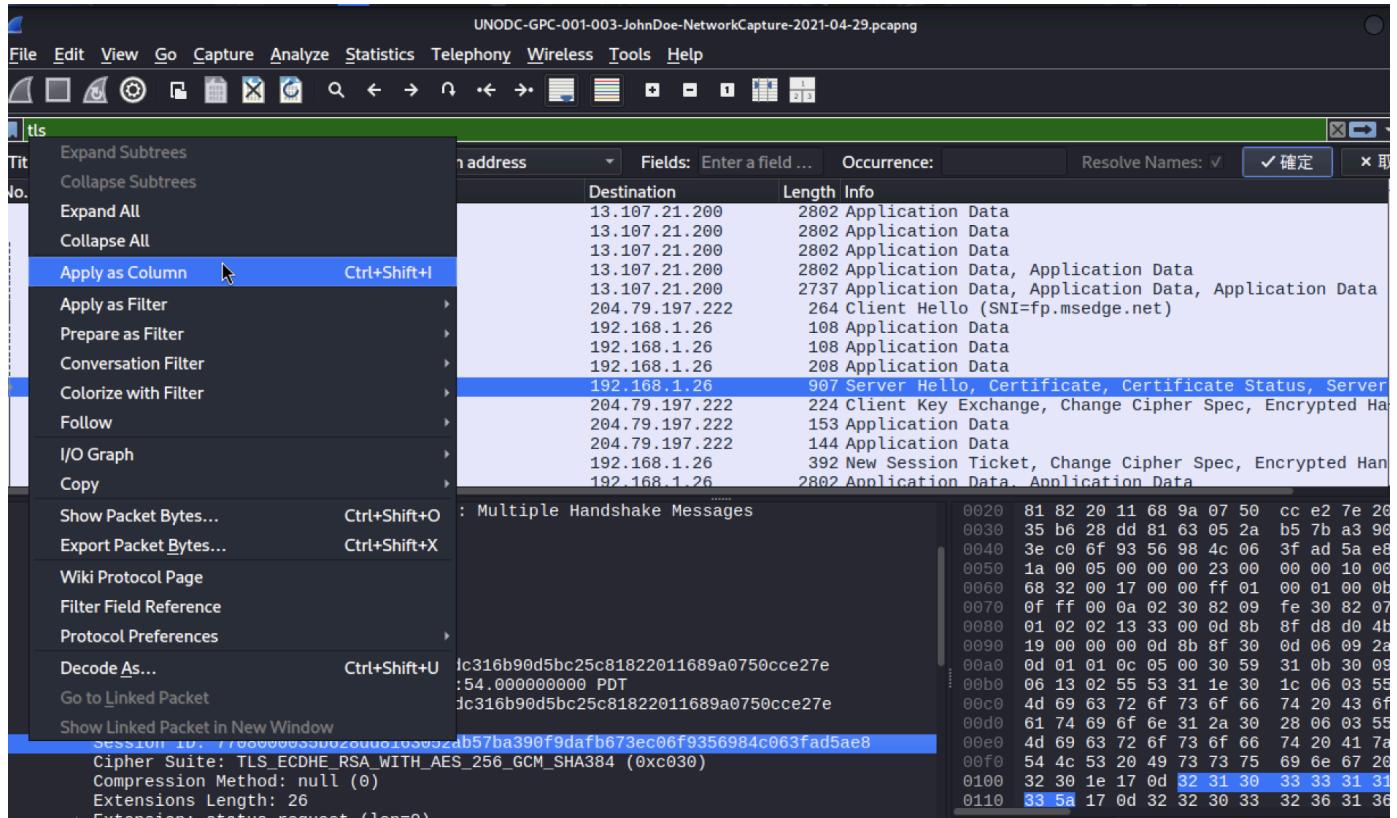
```
(root@kali:[/home/kali/Desktop]
# file 20210429_152157.jpg
20210429_152157.jpg: JPEG image data, Exif standard: [TIFF image data, big-endian, direntries=10, model=LM-Q725K, orientation=upper-right, datetime=2021:04:29 15:21:57, resolutionunit=2, GPS-Data, xresolution=163, yresolution=171, manufacturer=LG Electronics], baseline, precision 8, 4160x3120, components 3
```

LM-Q725K

問7

在會話 ID 為 的會話中，伺服器在 TLS 握手期間提供的臨時公鑰是什麼

da4a0000342e4b73459d7360b4bea971cc303ac18d29b99067e46d16cc07f4ff ?



看起來是 tls 第 2 次交握所會帶出 session id

參數 : tls.handshake.type == 2

UNODC-GPC-001-003-JohnDoe-NetworkCapture-2021-04-29.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tls.handshake.type==2

Title: Destination	Type: Destination address	Fields: Enter a field ...	Occurrence:	Resolve Names: ✓ 確定
Source	Destination	Length Session ID		Info
185.70.41.35	192.168.1.26	1444 b8837ec96878f68edd37f11c4fcac5772e0438040d5dc3c821cb70ef6c76f58		Server Hello,
35.186.220.63	192.168.1.26	1444 be2b5593998b8f9c1e98d177ef6b65c5864a179ba2c7668bb92cd661ef853100		Server Hello,
172.217.4.74	192.168.1.26	3096 beb0370a47d6b8e1ab7780c68bef381f1270fed49e564d0ec91e6785085c03a		Server Hello,
13.107.21.200	192.168.1.26	138 c00a0000eaafb1a223f424f99fa526054fef67e01cef7a9b514065d95c0ae8		Server Hello,
52.137.103.130	192.168.1.26	1121 c21f00001011e860af1247c935def2ce870d2466145dd7625763e04562bf4100		Server Hello,
185.70.41.35	192.168.1.26	4162 c69f5a3378dd9306bf9722d5049de6ec368a797b0c63194d35342ebdc24abd7e		Server Hello,
52.137.103.130	192.168.1.26	2498 cc160000ea178d72508e3380b84b5486b28a2a62767e3e9c6f93eccc70897eec		Server Hello,
52.162.219.173	192.168.1.26	1707 da4a0000342e4b73459d7360b4bea971cc303aca18d29b99067e46d16cc07f4aff		Server Hello,
20.54.89.15	192.168.1.26	2521 dc3500000b3990ec96d1d6bb7ef79834bb804a88a6c83ef03bf532cf681544		Server Hello,
185.70.41.35	192.168.1.26	1444 dd56dd029abe832cdd2b3005b5d3b2db52f47cf5f14f7336dc5584e7179ca517		Server Hello,
52.114.75.149	192.168.1.26	1376 e10e0000099d357c67bc682e2cb9bd356ca2f15ca8ae8d942b5b3d1ea832ea3		Server Hello,
52.183.220.149	192.168.1.26	3759 e62900004683716008b97b10a1ff329haada31e7e50849fee88e36ed3fafaf6bf		Server Hello,

```

    ▶ Certificate [...]: 308205f3308204dba00302010202100c6ae97cced599838690a00a9ea53214300d06092a864886f70d0...
    ▶ Handshake Protocol: Certificate Status
      Handshake Type: Certificate Status (22)
      Length: 1767
      Certificate Status Type: OCSP (1)
      OCSP Response Length: 1763
    ▶ OCSP Response
    ▶ Handshake Protocol: Server Key Exchange
      Handshake Type: Server Key Exchange (12)
      Length: 361
    ▶ EC Diffie-Hellman Server Params
      Curve Type: named_curve (0x03)
      Named Curve: secp384r1 (0x0018)
      Pubkey Length: 97
      Pubkey: 04edcc123af7b13e90ce101a31c2f996f471a7c8f48a1b81d765085f548059a550f3f4f62ca1f0e8f74d727053074...
    ▶ Signature Algorithm: rsa_pkcs1_sha256 (0x0401)
      Signature Length: 256
      Signature [...]: 11914710183397b395995313bea183e0abc19619361016080bff249af9c5d88e7f2b8e44a161d5e2630673...
    ▶ Handshake Protocol: Server Hello Done
      Handshake Type: Server Hello Done (14)

```

04edcc123af7b13e90ce101a31c2f996f471a7c8f48a1b81d765085f548059a550f3f4f62ca1f0e8f74d
727053074a37bceb2cbdc7ce2a8994bcd76dd6834eefc5438c3b6da929321f3a1366bd14c877cc83e5d0
731b7f80a6b80916efd4a23a4d

問8

TLS 1.3用於建立連線的第一個客戶端隨機數是什麼protonmail.com ?

UNODC-GPC-001-003-JohnDoe-NetworkCapture-2021-04-29.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tls contains "protonmail.com"

No.	Time	Source	Destination	Length Session ID
17992	218.650666933	192.168.1.26	185.70.41.35	583 b8837ec96878f68edd37f11c4fcac5772e0438040d5dc3c821cb70ef6c76f58
17997	218.653798207	192.168.1.26	185.70.41.35	583 dd56dd029abe832cdd2b3005b5d3b2db52f47cf5f14f7336dc5584e71
18000	218.656063594	192.168.1.26	185.70.41.35	583 682b7e4bddfe48f8877b6c37cff8f3c6fbc51039b606076ff413bd6e22
18144	221.568712151	192.168.1.26	185.70.41.35	583 b70b4dd7f88b0795d10d44a43ee6091a54837eefcf42bec9f3584e71
18145	221.568886553	192.168.1.26	185.70.41.35	583 fbe0efc2a817d470164fe3b77db29f1abe411ff75403cb77c9dc2a10
18146	221.569250726	192.168.1.26	185.70.41.35	583 c69f5a3378dd9306bf9722d5049de6ec368a797b0c63194d35342ebdc
19069	224.846867048	192.168.1.26	185.70.41.130	583 48f384fd31ebc37e63e6c523906902b5183875d0e38b66094a5853f18
19070	224.847052741	192.168.1.26	185.70.41.130	583 5b6684c265b9f9e3765f3dbef480f83767aa4e1afe485811b830ba
19993	224.847594162	192.168.1.26	185.70.41.130	583 2f84dd39e4c50a32d2b8064a015f00a0192588f96e9dcfacc947e18
20350	231.204618948	192.168.1.26	185.70.41.130	583 4a18ac4fc355981a688b09ee3cf6a4997ee86507ccbf566265d2d91c1

```

    ▶ TLSv1.3 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 512
    ▶ Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 508
    ▶ Version: TLS 1.2 (0x0303)
      [Expert] Info (Chat/Deprecated): This legacy_version field MUST be ignored. The supported_versions exten...
      Random: 24e92513b97a0348f733d16996929a79be21b0b1400cd7e2862a732ce7775b70
      Session ID Length: 32
      Session ID: b8837ec96878f68edd37f11c4fcac5772e0438040d5dc3c821cb70ef6c76f58
      Cipher Suites Length: 32
      Cipher Suites (16 suites)
      Compression Methods Length: 1

```

參數 : tls contains "protonmail.com"

24e92513b97a0348f733d16996929a79be21b0b1400cd7e2862a732ce7775b70

問9

該地址的製造商FTP server's MAC註冊於哪個國家？

Frame 11810: 104 bytes on wire (832 bits), 104 bytes captured (832 bits) on interface wlo1, id 0
Ethernet II, Src: PCSSystemtec_a6:1f:86 (08:00:27:a6:1f:86), Dst: Intel_57:47:93 (c8:09:a8:57:47:93)
Destination: Intel_57:47:93 (c8:09:a8:57:47:93)
....0..... = LG bit: Globally unique address (factory default)
....0..... = IG bit: Individual address (unicast)
Source: PCSSystemtec_a6:1f:86 (08:00:27:a6:1f:86)
....0..... = LG bit: Globally unique address (factory default)
....0..... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
[Stream index: 14]

mac查詢

<https://maclookup.app/search/result?mac=c8:09:a8:57:47:93>

MAC Address Lookup
Find the vendor name of a device by entering an OUI or a MAC address
MAC c8:09:a8:57:47:93

Check an OUIs or a MAC address and display details like vendor name, location, MAC details, and more... [Search by Vendor Name?](#)

[Home](#) / [Search](#) / [Result \(C8:09:A8\)](#)

Intel Corporate

[Vendor](#) [Details](#)

MAC address prefix **C8:09:A8** is registered to **Intel Corporate**, located at Lot 8Jalan Hi-Tech 2/3Kulim Kedah 09000M

This registration is classified as **MA-L** (Mac Address Block Large) containing approximately 16 million MAC addresses

The prefix was registered on **09 August 2019**, and no subsequent updates have been recorded.

OUI: [C8:09:A8](#)

位置在美國



英特爾

公司：

英特爾是世界上第二大的半導體公司，也是首家推出x86架構中央處理器的公司，總部位於美國加利福尼亞州聖塔克拉拉。由羅伯特·諾伊斯、高登·摩爾、安迪·葛洛夫，以「整合電子」之名在1968年7月18日共同創辦公司，將高階晶片設計能力與領導業界的製造能力結合在一起。

資料來源：[維基百科](#)

執行長：[陳立武](#) (2025年3月18日–)

財務長：[大衛·津斯納](#)

創辦人：[高登·摩爾](#)、[羅伯特·諾伊斯](#)

創立於：1968年7月18日，美國加利福尼亞山景城

總部：[美國加利福尼亞聖塔克拉拉](#)

產品：中央處理器；微處理器；圖形處理器；存儲器；閃存；固態硬盤及其主控（已被SK海力士收購）；主板及其芯片組；網絡接口卡；Wi-Fi與藍牙芯片；移動電話調製解調器（已被蘋果公司收購）；晶圓代工服務

股票代號：[NASDAQ : INTC](#)；道瓊斯工業平均指數成分股；納斯達克100指數成份股；標準普爾500指數成分股

Q10

non-standard folder 4月20日什麼時間在FTP伺服器上建立？

The screenshot shows the Wireshark interface with a context menu open over a selected FTP packet. The menu path is: **Mark/Unmark Selected** → **Follow** → **TCP Stream**. The TCP Stream option is highlighted in blue.

Selected packet details:

- No. 11810 2021-04-30 01:02:03.659278789 192.168.1.20
- Type: Destination address
- Source: 192.168.1.20
- Destination: 192.168.1.26
- Length: 104
- Record Layer: Info
- Info: Response: 530 Please

Packet details pane:

- Frame 11810: 104 bytes on wire (832 bits), 104 b
- Ethernet II, Src: PCSSystemtec_a6:1f:86 (08:00:2
- Destination: Intel_57:47:93 (c8:09:a8:57:47:93)
- ...0. = LG bit: Glob
- ...0. = IG bit: Ind
- Source: PCSSystemtec_a6:1f:86 (08:00:27:a6:1f:86)
- ...0. = LG bit: Glob
- ...0. = IG bit: Ind
- Type: IPv4 (0x0800)
- [Stream index: 14]
- Internet Protocol Version 4, Src: 192.168.1.20, Dst: 192.168.1.26
- Transmission Control Protocol, Src Port: 21, Dst Port: 48810, Seq: 75, Ack: 21, Len: 38
- File Transfer Protocol (FTP)
- [Current working directory:]

Selected bytes pane:

Hex	Dec	ASCII
0000	c8 09 a8 5	
0010	00 5a a8 1	
0020	01 1a 00 1	
0030	01 fa cc 0	
0040	04 7d 35 3	
0050	69 6e 20 7	
0060	20 50 41 5	

逐一檢查流表

The screenshot shows the Wireshark interface with the **Follow TCP Stream** dialog open. The stream number is set to 11. The results pane displays a list of files in the /Desktop directory:

File	Size	Last Modified
Desktop	1000	Feb 23 06:37
Documents	1000	Apr 29 16:42
Downloads	1000	Feb 23 06:37
Music	1000	Feb 23 06:37
Pictures	1000	Feb 23 06:37
Public	1000	Feb 23 06:37
Templates	1000	Feb 23 06:37
Videos	1000	Feb 23 06:37
ftp	65534	Apr 20 17:53

Selected packet details:

- No. 525 2021-04-30 01:01:26.920
- Type: Destination address
- Source: 192.168.1.20
- Destination: Intel_57:47:93 (c8:09:a8:57:47:93)
- ...0. = LG bit: Glob
- ...0. = IG bit: Ind
- Source: PCSSystemtec_a6:1f:86 (08:00:27:a6:1f:86)
- ...0. = LG bit: Glob
- ...0. = IG bit: Ind
- Type: IPv4 (0x0800)
- [Stream index: 14]
- Internet Protocol Version 4, Src: 192.168.1.20, Dst: 192.168.1.26
- Transmission Control Protocol, Src Port: 21, Dst Port: 48810, Seq: 75, Ack: 21, Len: 38
- File Transfer Protocol (FTP)
- [Setup frame: 522]
- [Setup method: PASV]
- [Command: LIST]
- Command frame: 524
- [Current working directory: /home/kali]

Selected bytes pane:

0 client pkt(s), 1 server pkt(s), 0 turn(s).

Entire conversation (584 bytes) Show as ASCII No delta times Stream 11

Find: Filter Out This Stream Print Save as... Back × 關閉 說明

17:53

問11

使用者造訪了哪個 URL 並與 IP 位址關聯 104.21.89.171 ?

參數 : http and ip.addr ==104.21.89.171

檢查劉表

The screenshot shows a Wireshark capture window. A single HTTP stream is selected, labeled 'tcp.stream eq 224'. The details pane displays an incoming GET request from 'dfir.science' to the local host (127.0.0.1). The request includes various headers such as Host, Connection, Upgrade-Insecure-Requests, User-Agent, Accept, Accept-Encoding, and Accept-Language. The response pane shows a 301 Moved Permanently status with a Location header pointing to 'https://dfir.science/'. The raw pane shows the full HTTP exchange. The bottom pane shows the raw bytes of the selected frame.

```
GET / HTTP/1.1
Host: dfir.science
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

HTTP/1.1 301 Moved Permanently
Date: Fri, 30 Apr 2021 01:06:39 GMT
Transfer-Encoding: chunked
Cache-Control: max-age=3600
Expires: Fri, 30 Apr 2021 02:06:39 GMT
Location: https://dfir.science/
cf-request-id: 09c1e9541a00006140f92cc000000001
Report-To: {"endpoints": [{"url": "https://a.cloudflare.com/report?s=xTgjSVvc474GwLozCU6lCwMS0iq2X8UrFp%2B0p4tk2QkIULcn0ccwfbb%2FagmhV9cZtz%2FQ%2Bnc10E6%2FTJXjTUddDwfEL%2For%2FQjQ75Rpg%3D"}], "max_age": 604800, "group": "cf-nel"}
NEL: {"max_age": 604800, "report_to": "cf-nel"}
X-Content-Type-Options: nosniff
Server: cloudflare
CF-RAY: 647cde668b296140-ORD
alt-svc: h3-27=:443; ma=86400, h3-28=:443; ma=86400, h3-29=:443; ma=86400
```

<http://dfir.science/>