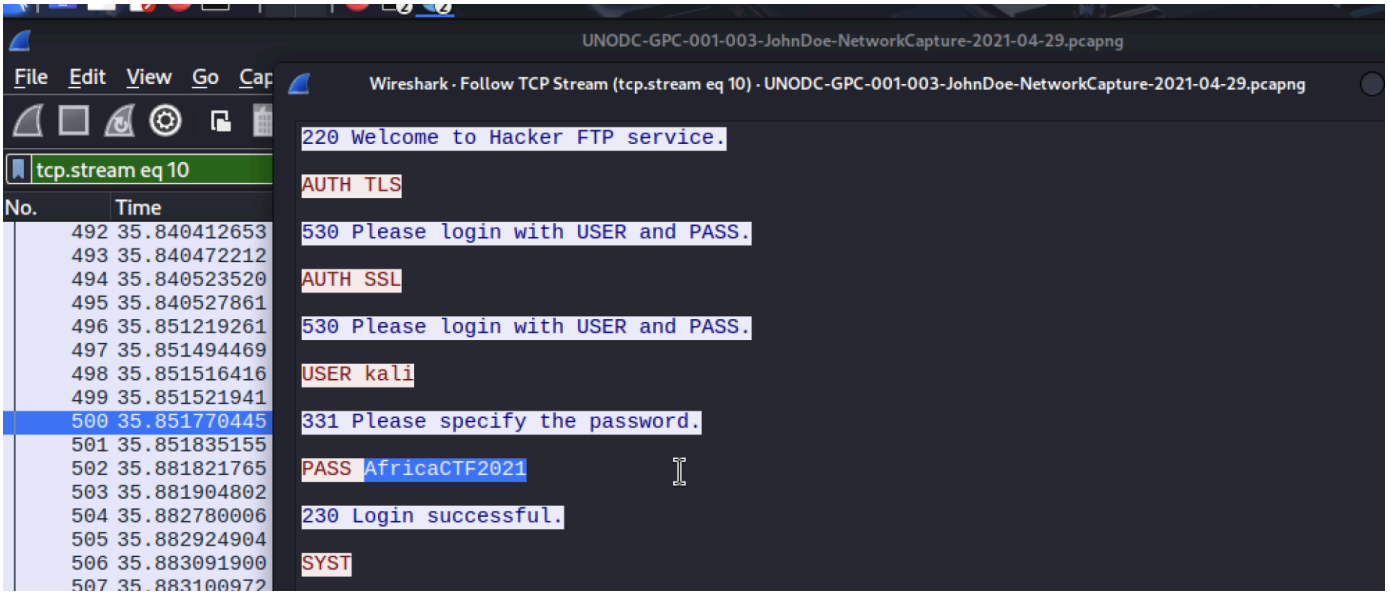
PacketMaze Lab(wireshark)

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？

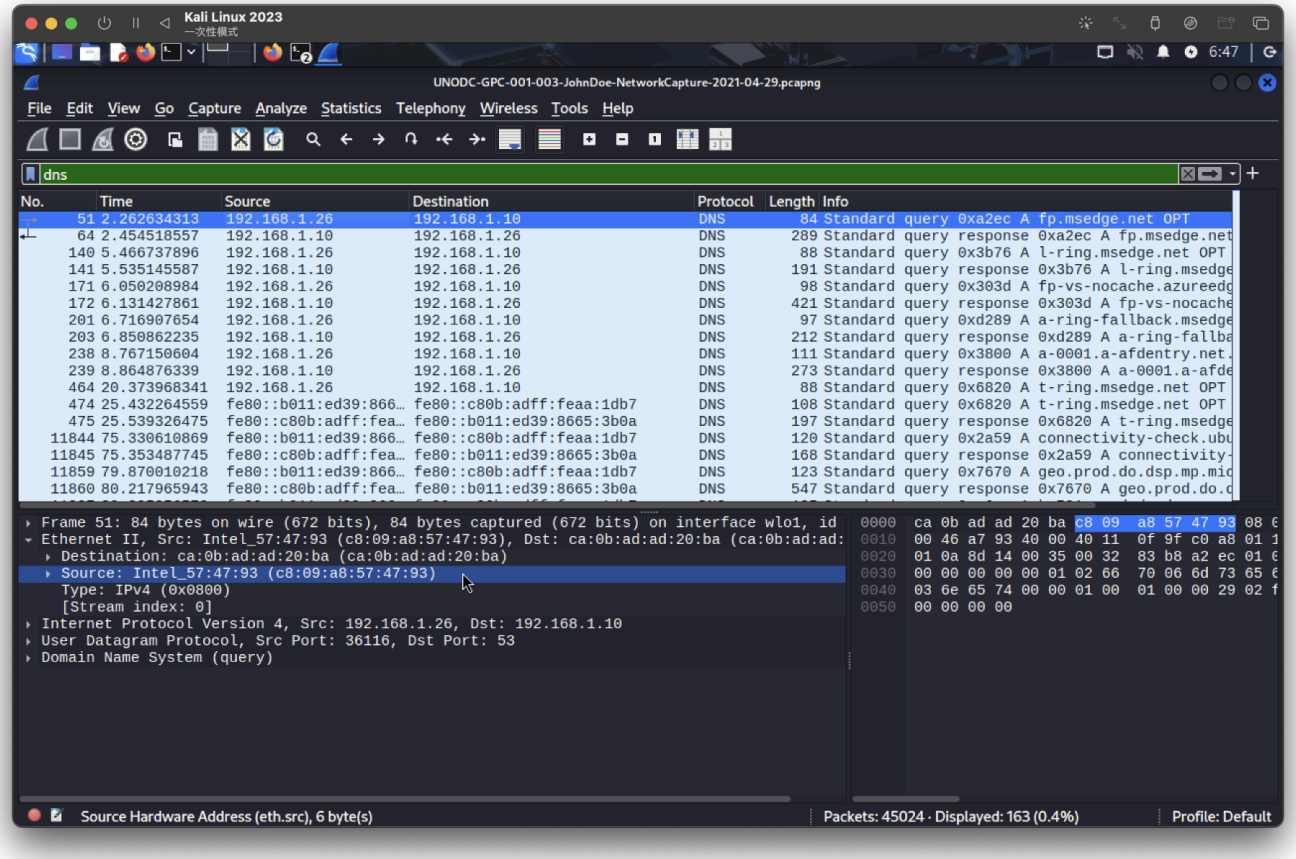
找FTP



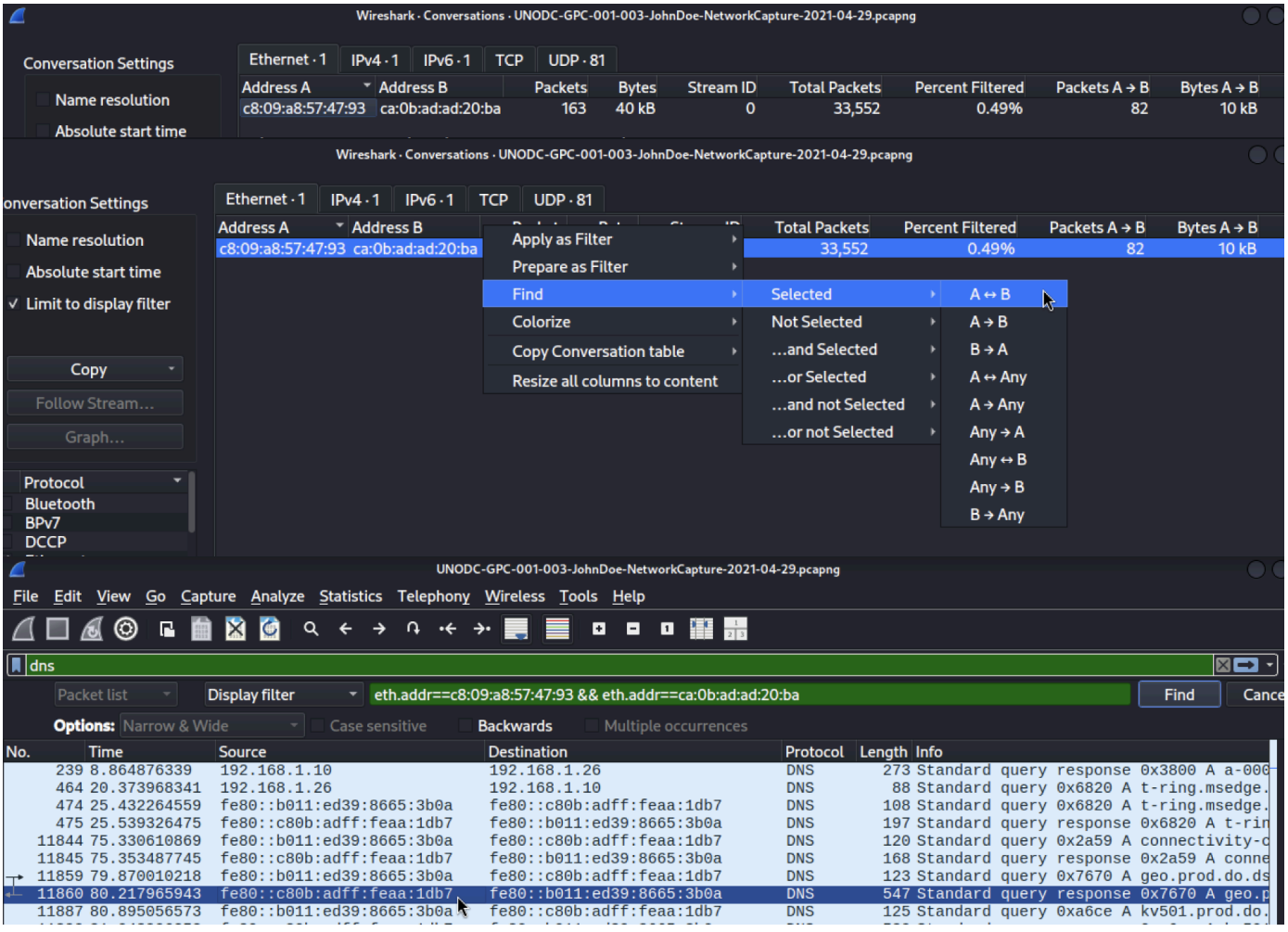
`AfricaCTF2021`

第二季

使用的 DNS 伺服器的 IPv6 位址是什麼192.168.1.26？



`c8:09:a8:57:47:93` <=ipv4的mac

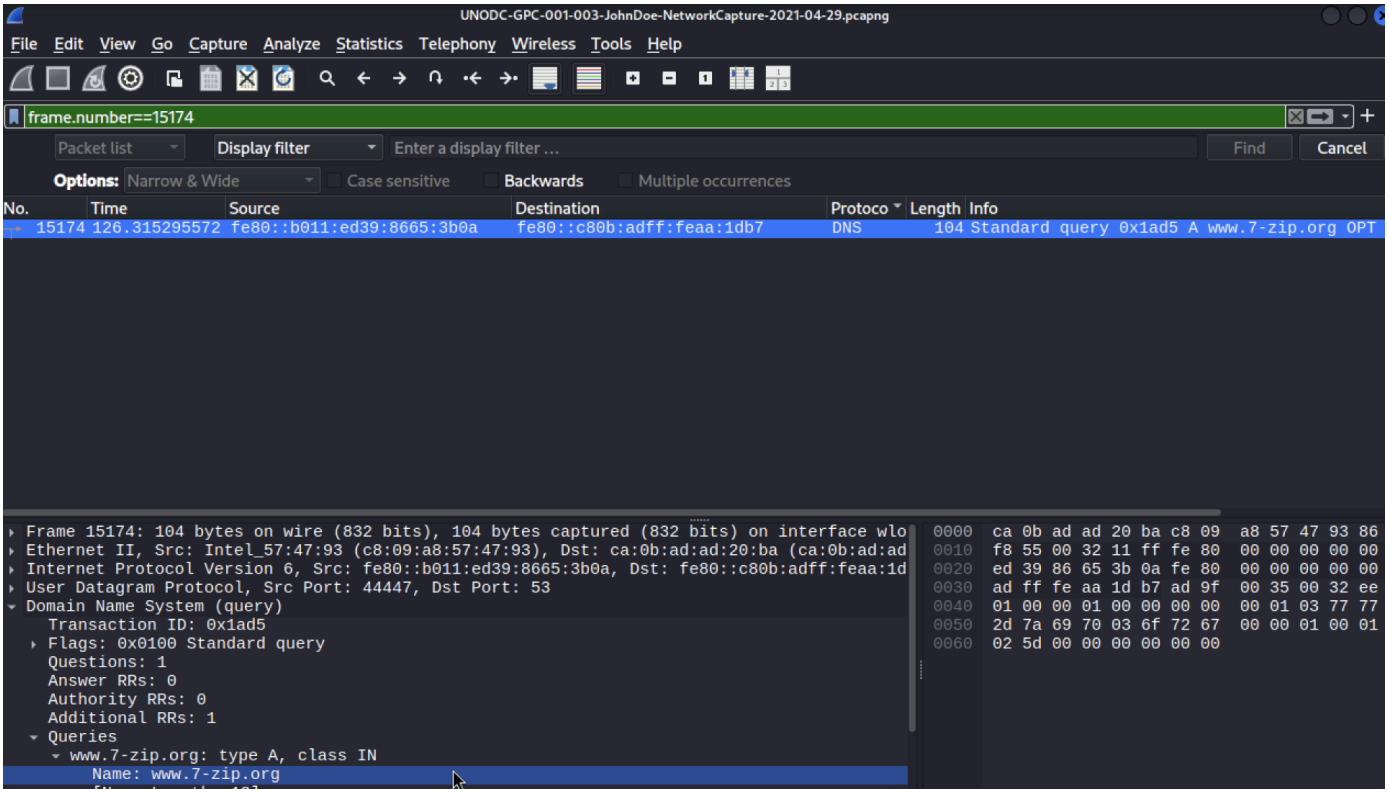


`fe80::c80b:adff:feaa:1db7`

第三季

使用者在資料包中尋找哪個網域15174？

參數：frame.number==15174

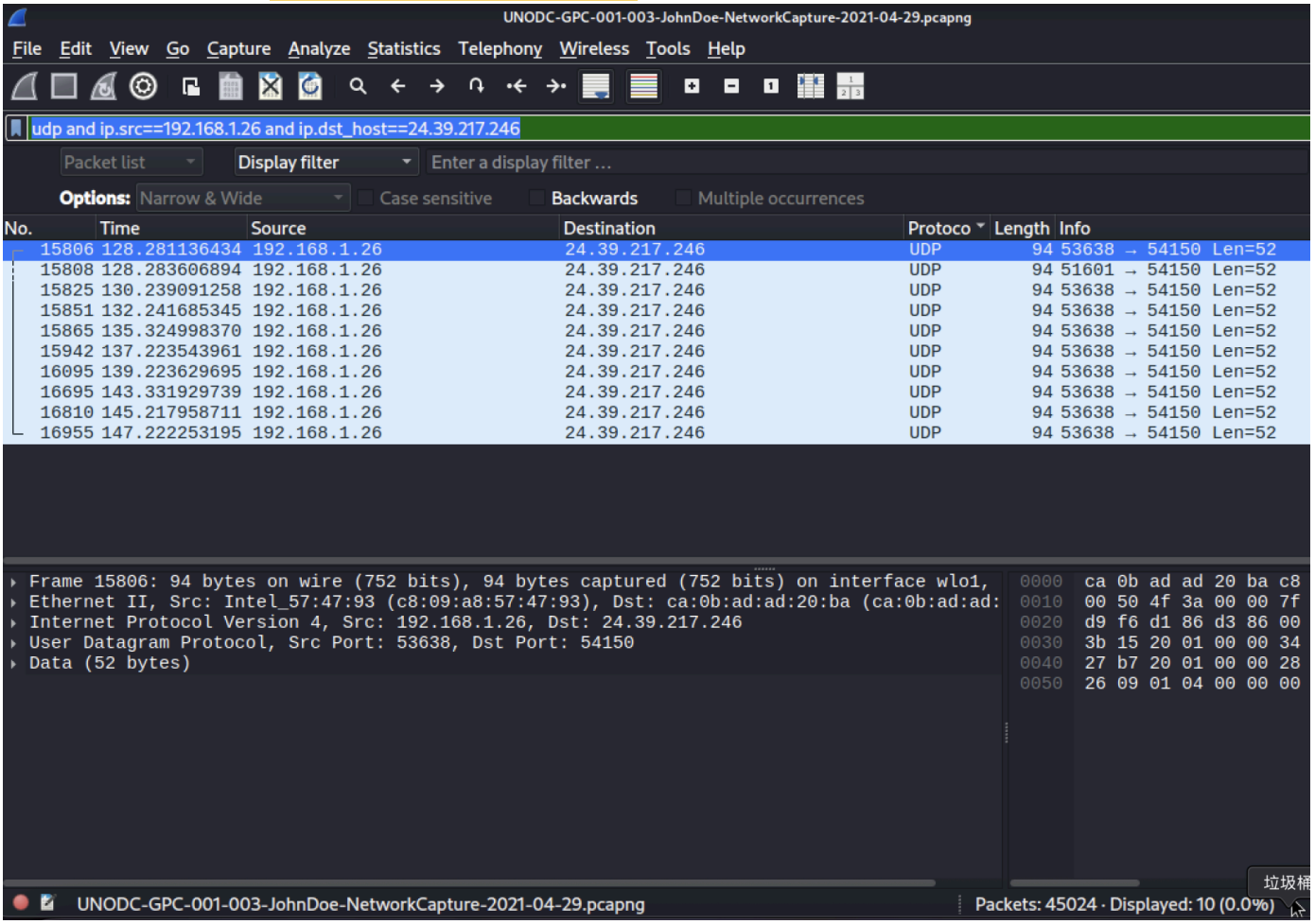


`www.7-zip.org`

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.src192.168.1.26 and ip.dst_host24.39.217.246



`10`

問5

PCAP 檔案中被調查系統的 MAC 位址是什麼？

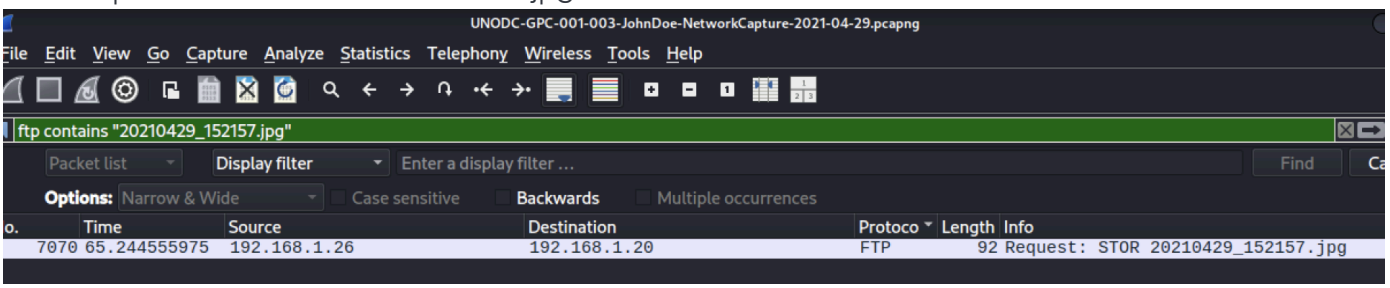
同上，我們要調查src ip

`c8:09:a8:57:47:93`

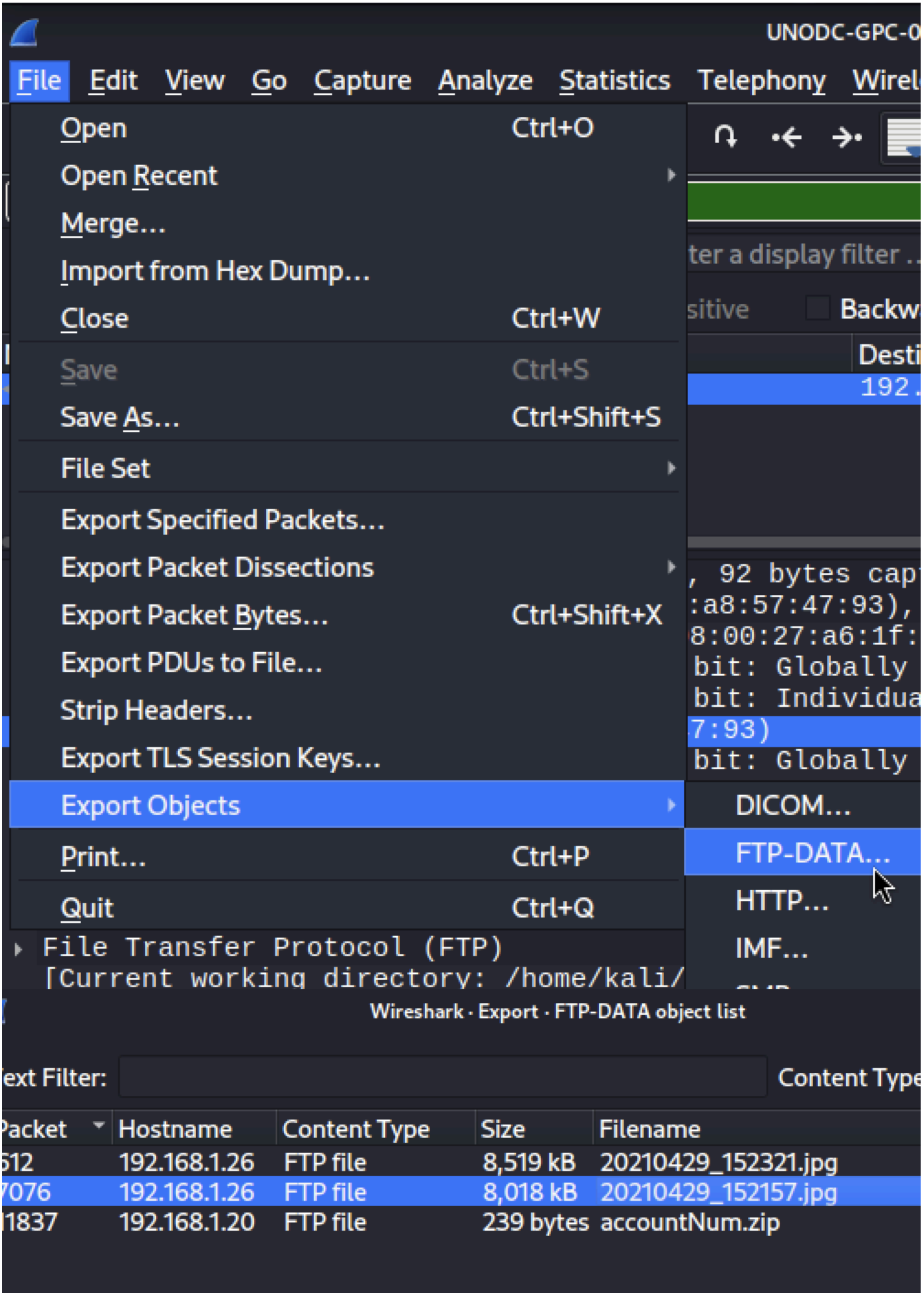
問6

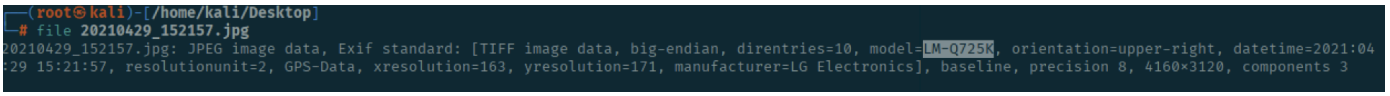
用來拍照的相機型號是什麼20210429_152157.jpg？

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



匯出FTP

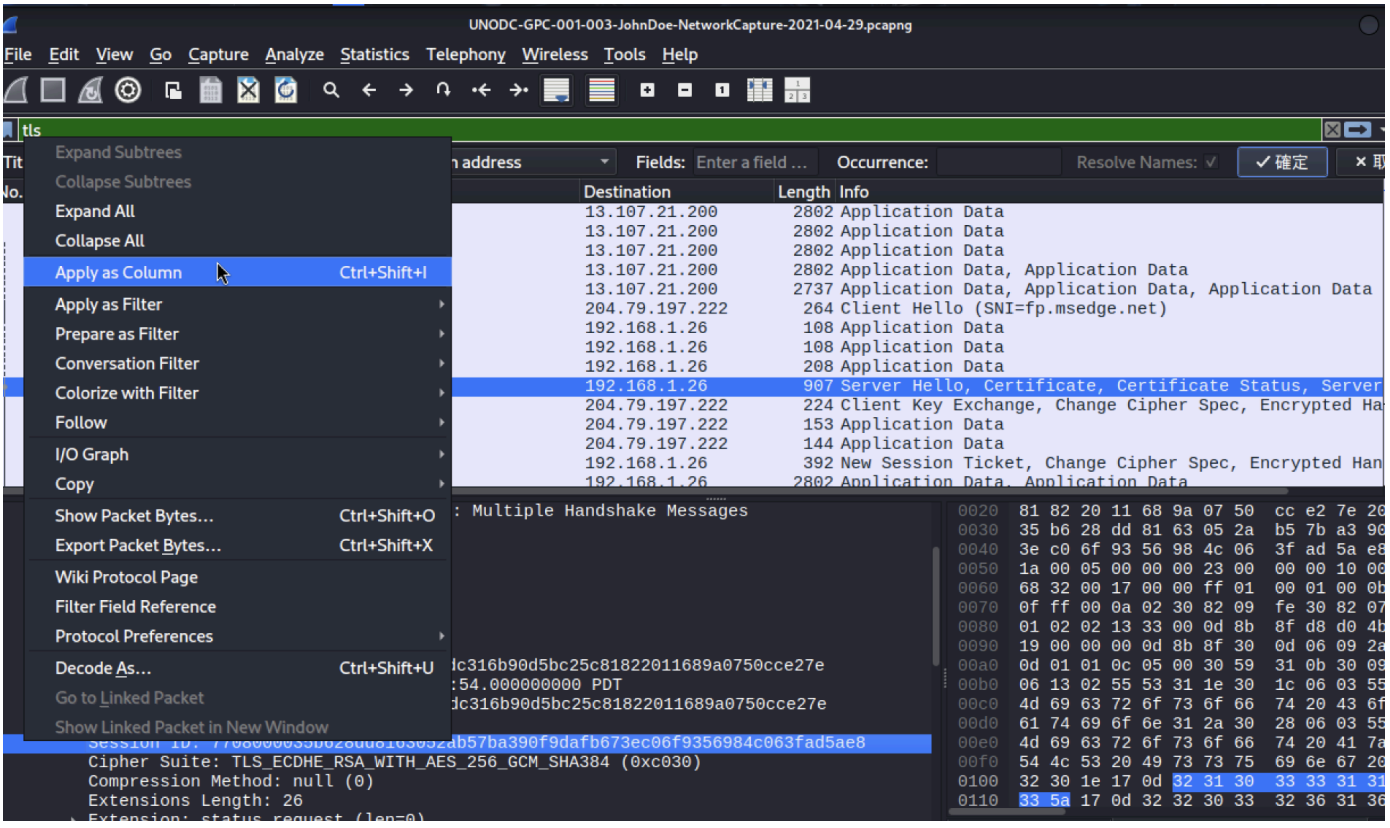

UNODC-GPC-0
File Edit View Go Capture Analyze Statistics Telephony Wirel
Open Ctrl+O
Open Recent
Merge...
Import from Hex Dump...
Close Ctrl+W
Save Ctrl+S
Save As... Ctrl+Shift+S
File Set
Export Specified Packets...
Export Packet Dissections
Export Packet Bytes... Ctrl+Shift+X
Export PDUs to File...
Strip Headers...
Export TLS Session Keys...
Export Objects
Print... Ctrl+P
Quit Ctrl+Q
DICOM...
FTP-DATA...
HTTP...
IMF...
File Transfer Protocol (FTP)
[Current working directory: /home/kali/
Wireshark · Export · FTP-DATA object list
ext 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
11837 192.168.1.20 FTP file 239 bytes accountNum.zip



LM-Q725K

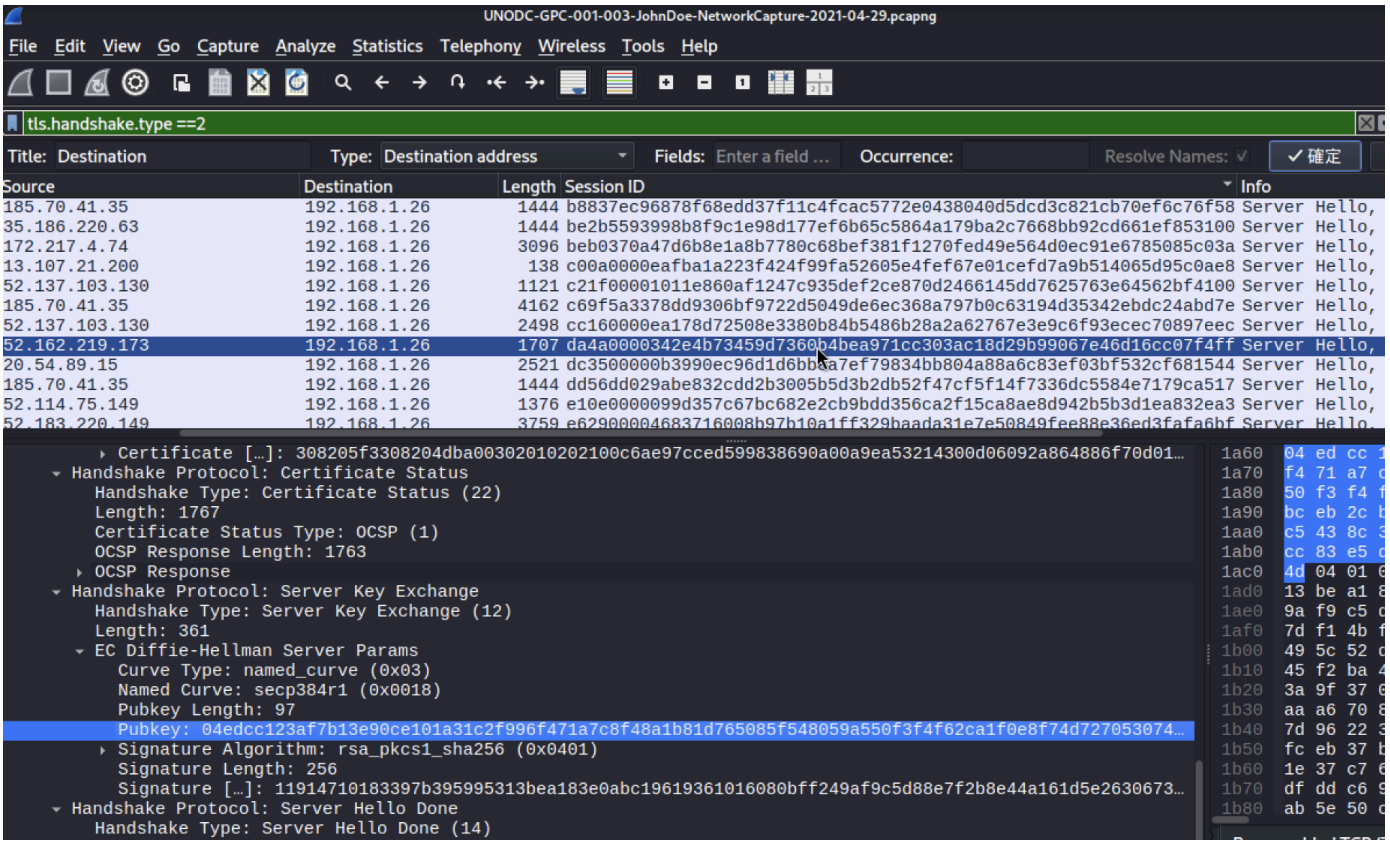
問7

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

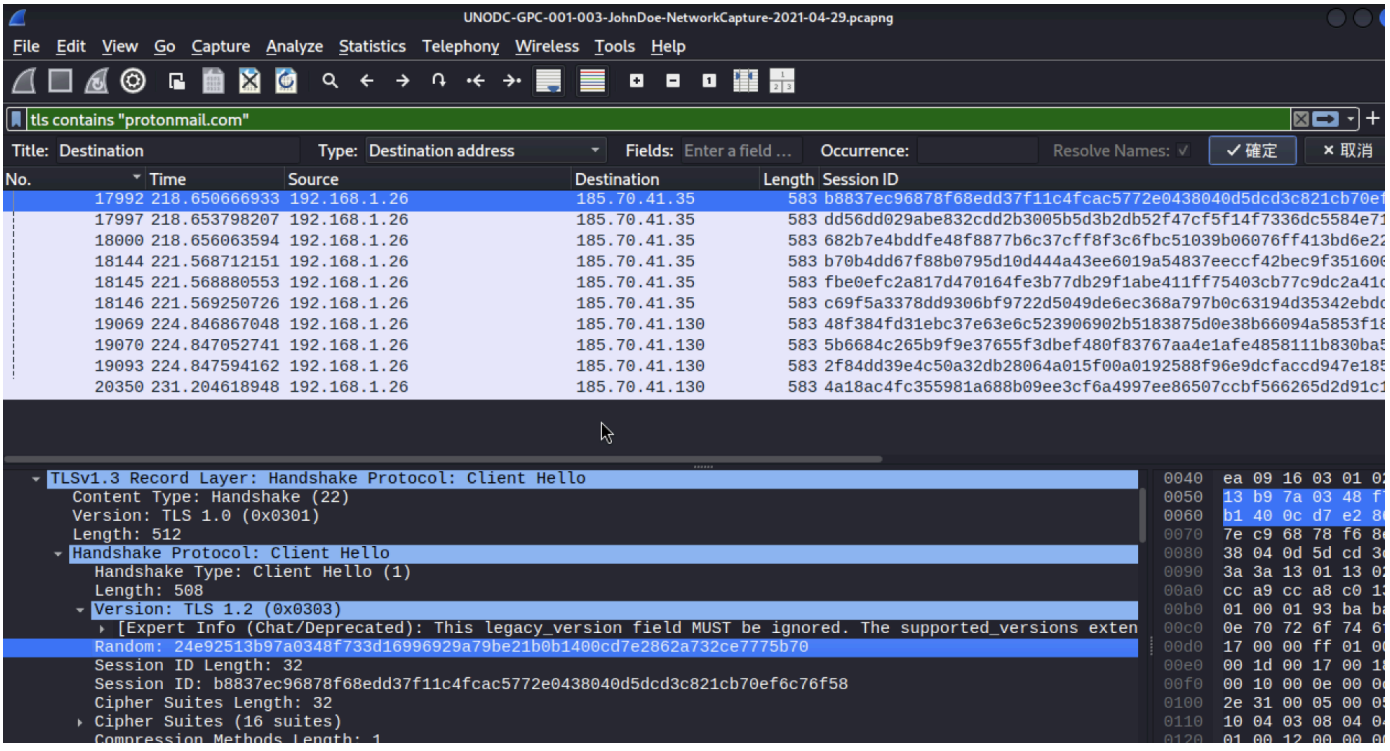
參數：tls.handshake.type ==2



`04edcc123af7b13e90ce101a31c2f996f471a7c8f48a1b81d765085f548059a550f3f4f62ca1f0e8f74d727053074a37bceb2cbdc7ce2a8994dcd76dd6834eefc5438c3b6da929321f3a1366bd14c877cc83e5d0731b7f80a6b80916efd4a23a4d`

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？

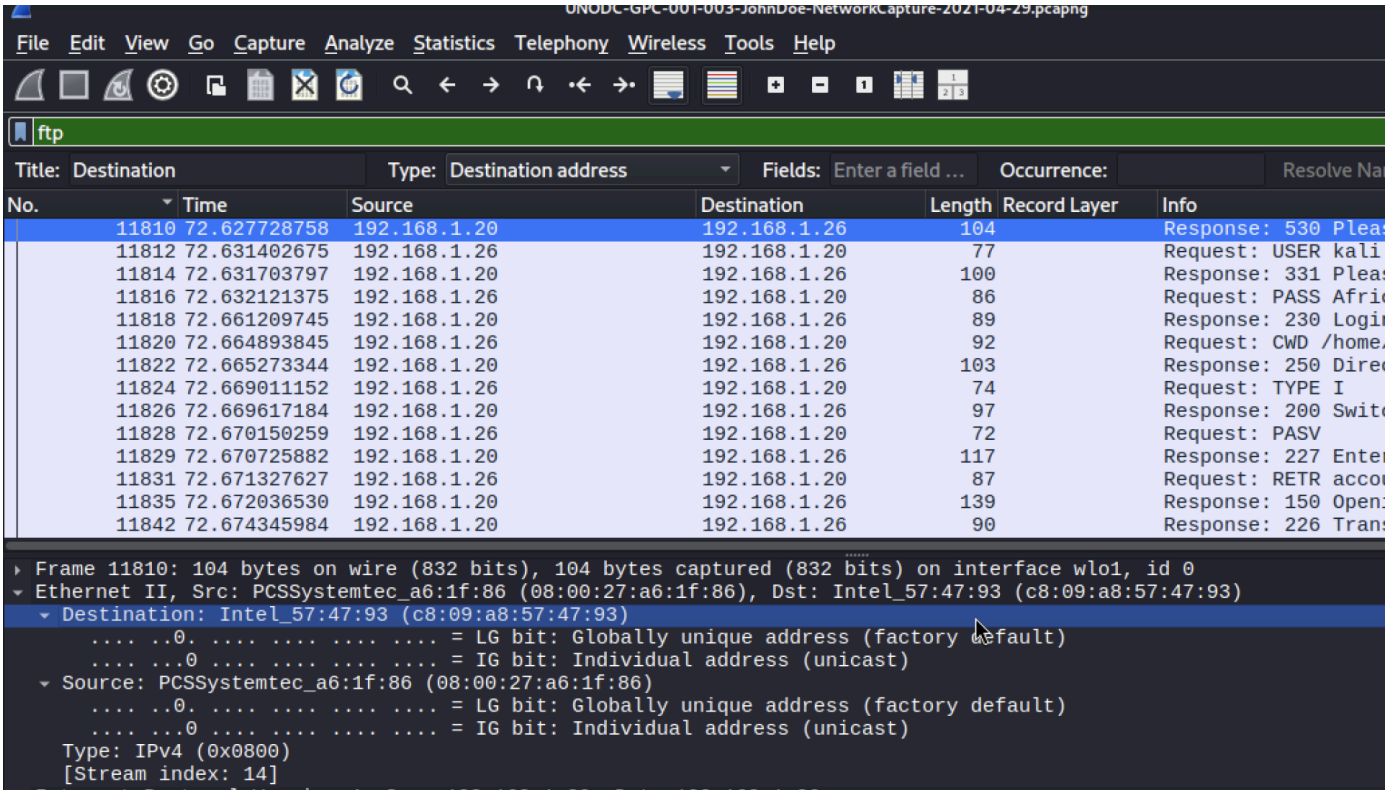


參數：tls contains "protonmail.com"

`24e92513b97a0348f733d16996929a79be21b0b1400cd7e2862a732ce7775b70`

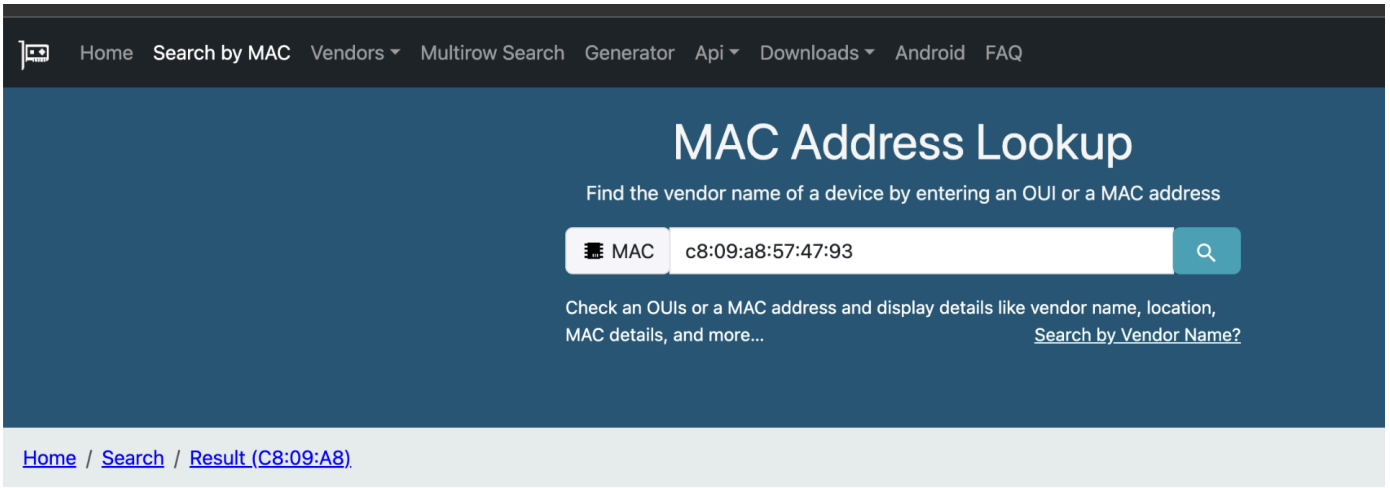
問9

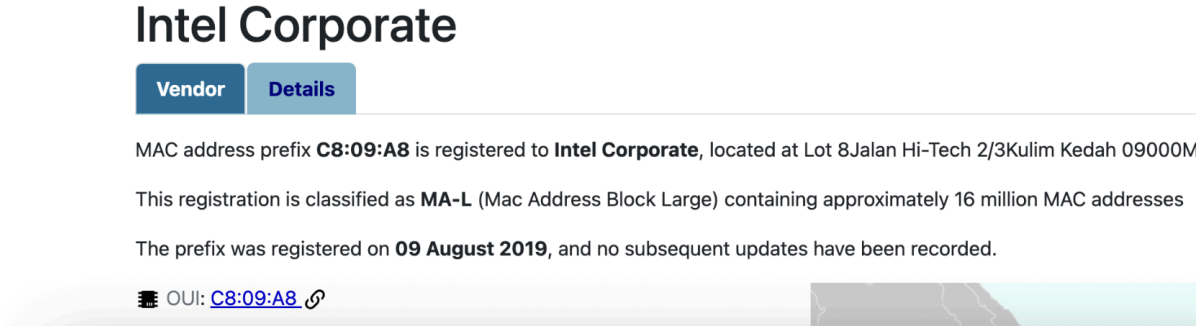
該地址的製造商FTP server's MAC註冊於哪個國家？



mac查詢

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





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

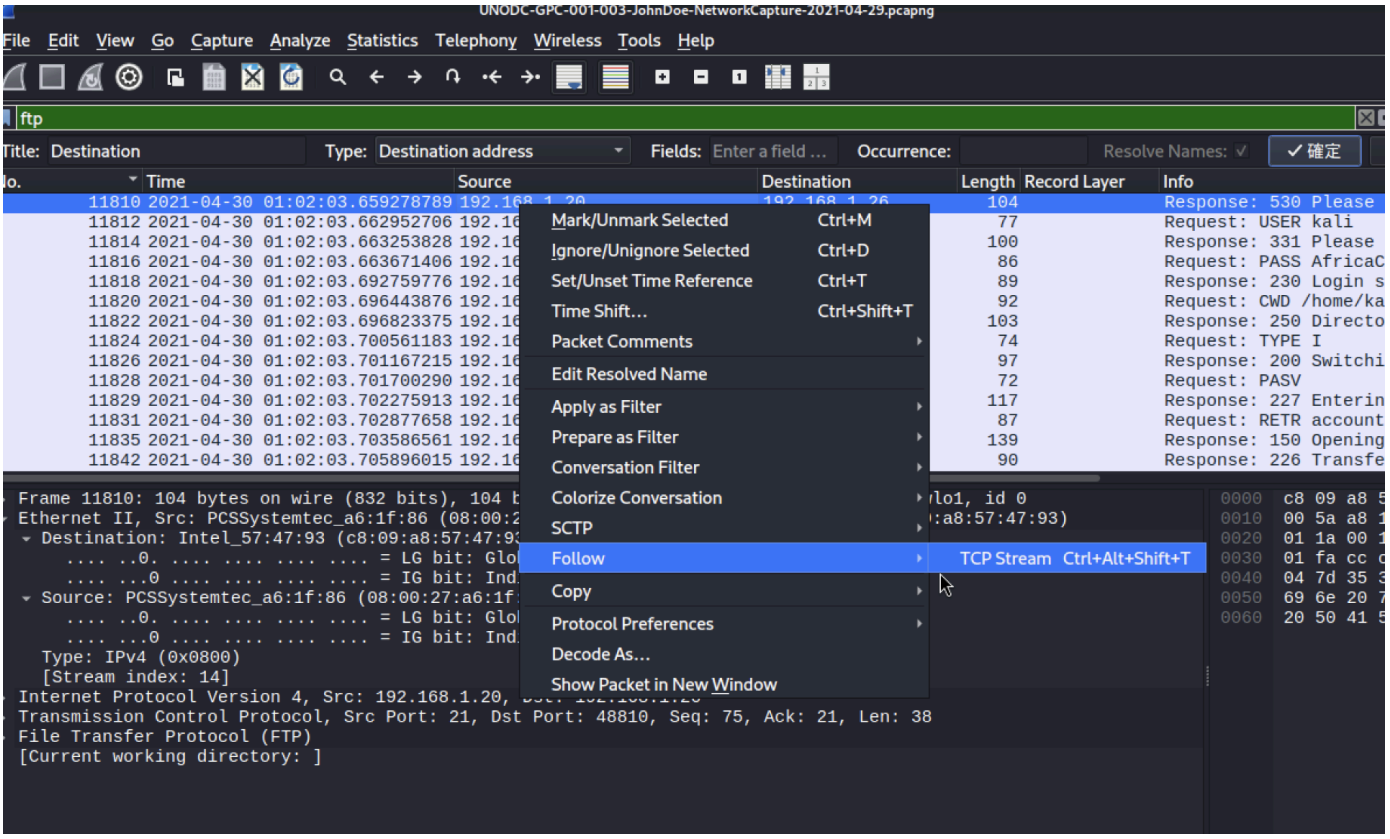
產品： 中央處理器; 微處理器; 圖形處理器; 存儲器; 閃存; 固態硬盘及其主控（已被SK海力士收購）; 主板及其芯片組; 網絡接口卡; Wi-Fi與藍牙芯片移動電話調製解調器（已被蘋果公司收購）; 晶圓代工服務

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

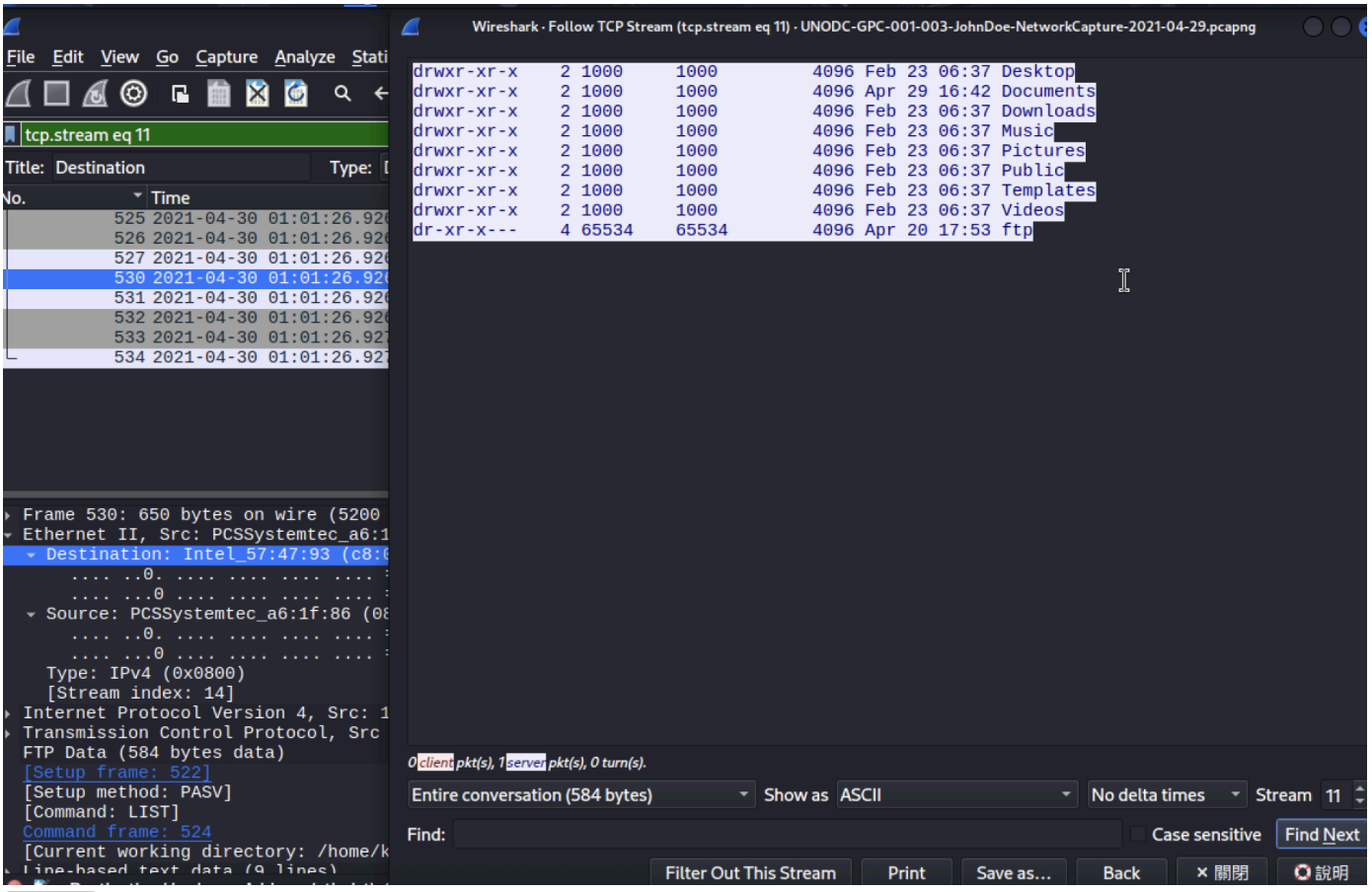
United States

Q10

non-standard folder4 月 20 日什麼時間在 FTP 伺服器上建立？



逐一檢查流表

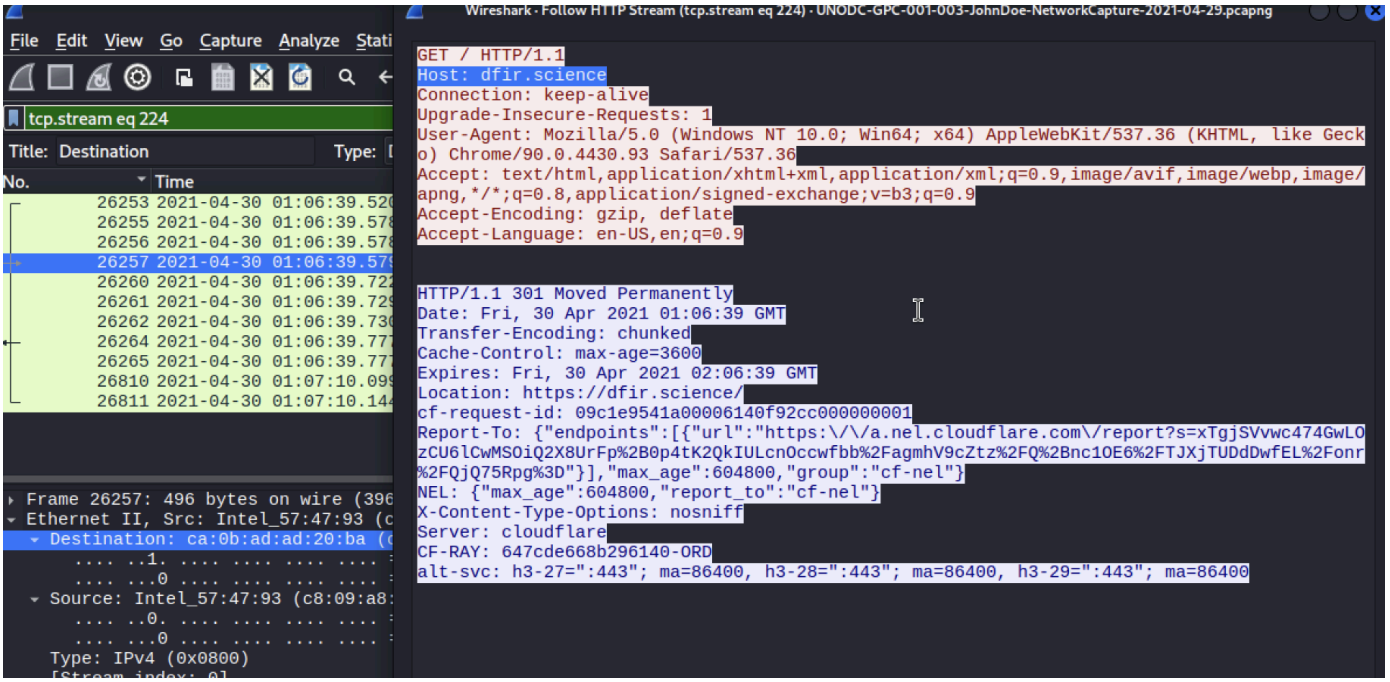


17:53

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



`http://dfir.science/`