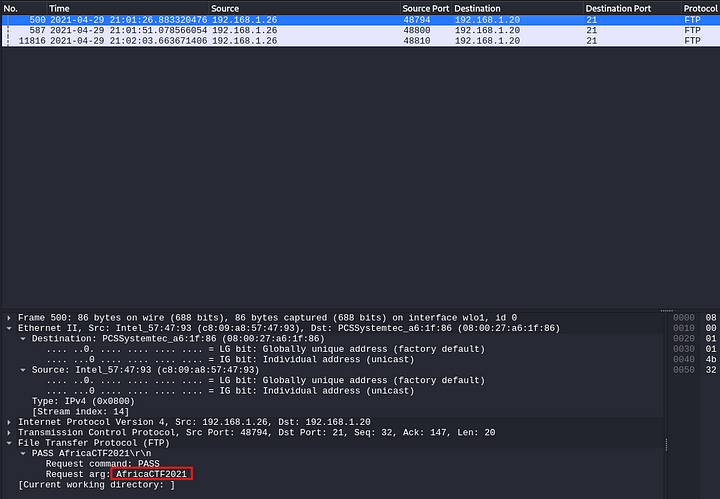
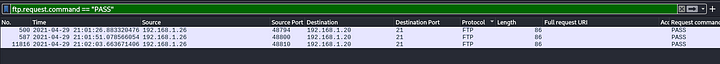
### **PacketMaze — CyberDefenders**

**Scenario:** A company’s internal server has been flagged for unusual network activity, with multiple outbound connections to an unknown external IP. Initial analysis suggests possible data exfiltration. Investigate the provided network logs to determine the source and method of compromise.

#### **Tasks:**

1. **What is the FTP password?**

Filter: ftp.request.command == “PASS”

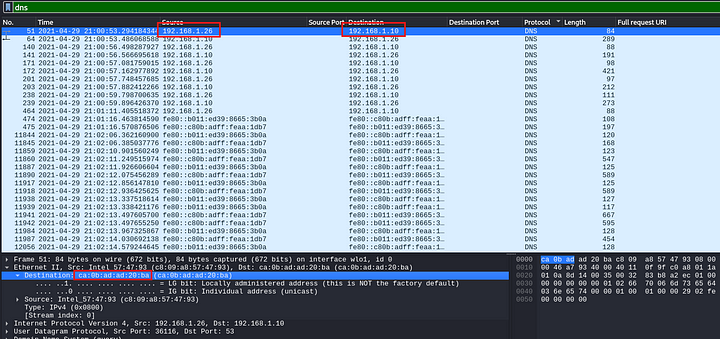


**Answer:** AfricaCTF202

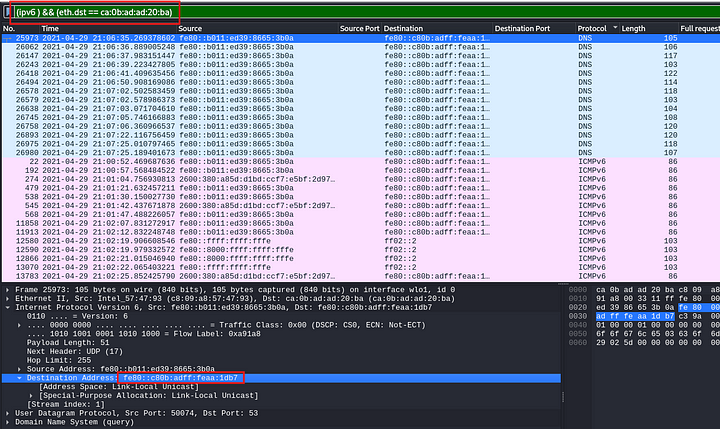
**2. What is the IPv6 address of the DNS server used by 192.168.1.26?**

filter: dns

Identify the MAC address of the IP address to which DNS request is sent



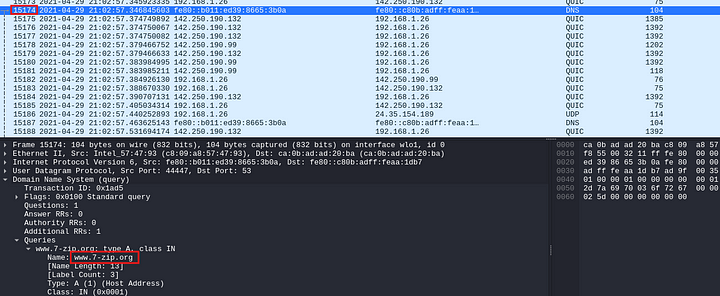
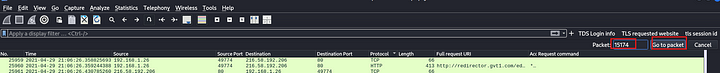
Filter: ipv6 && eth.dst ==ca:0b:ad:ad:20:ba



**Answer:** fe80::c80b:adff:feaa:1db7

**3. What domain is the user looking up in packet 15174?**

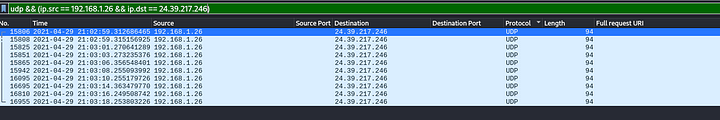
Use the Go feature in Wireshark. Go -> Go To Packet



**Answer:** [www.7-zip.org](http://www.7-zip.org)

**4. How many UDP packets were sent from 192.168.1.26 to 24.39.217.246?**

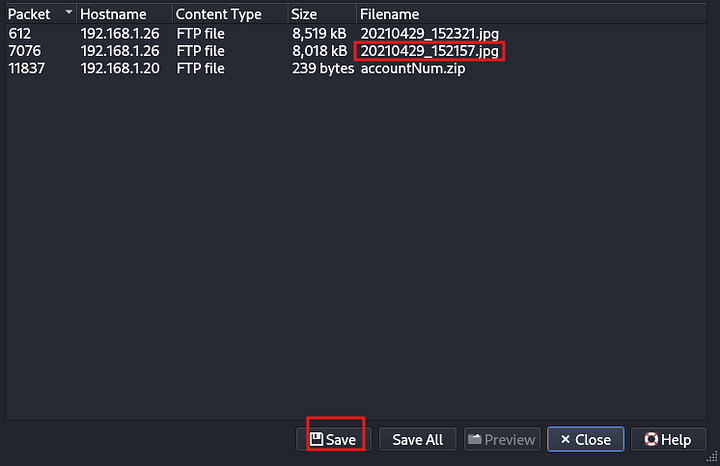
Filter: udp && (ip.src == 192.168.1.26 && ip.dst == 24.39.217.246)



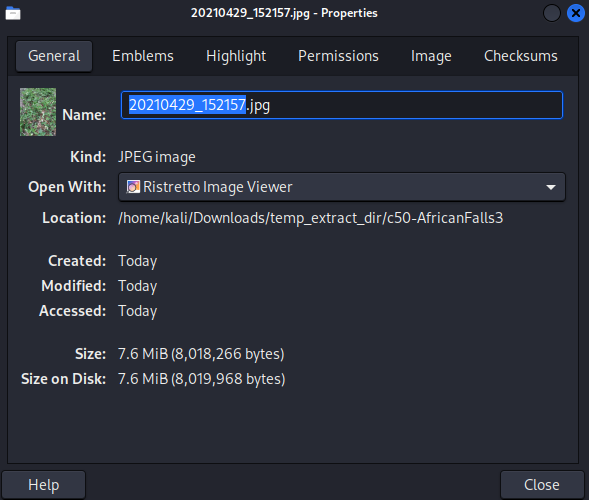
**Answer:** 10

**5. What was the camera model name used to take picture 20210429\_152157.jpg**

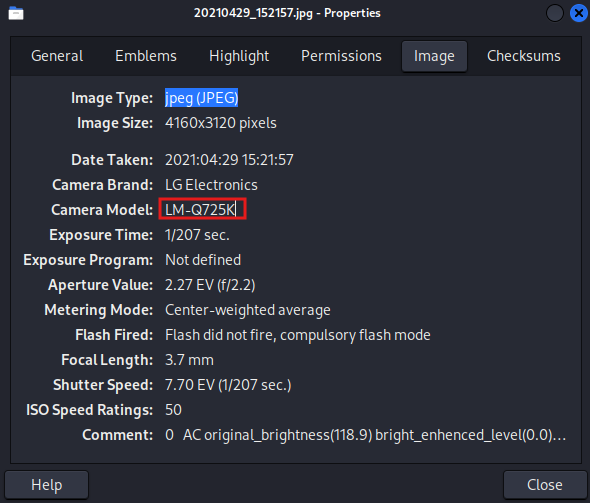
Download the image by going to File -> Export Objects -> FTP-DATA



Then right click the downloaded image, and click properties.



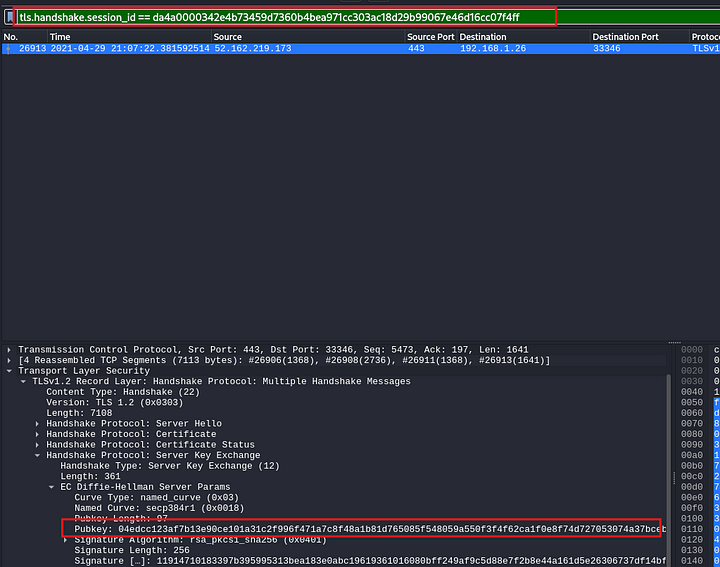
Then go to Image tab



**Answer:** LM-Q725K

**7. What is the ephemeral public key provided by the server during the TLS handshake in the session with the session ID: da4a0000342e4b73459d7360b4bea971cc303ac18d29b99067e46d16cc07f4ff?**

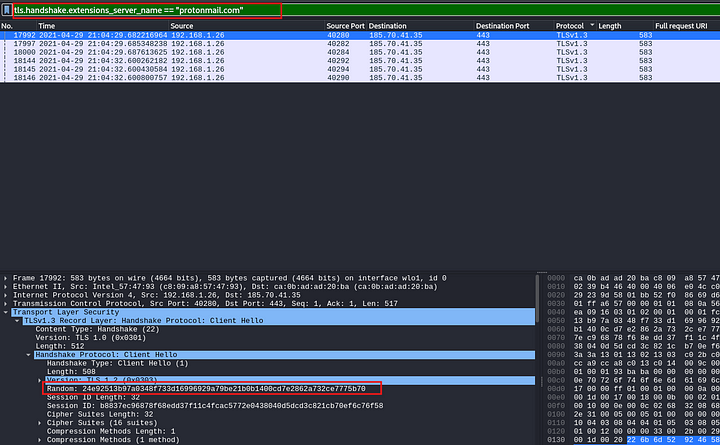
Filter: tls.handshake.session\_id == da4a0000342e4b73459d7360b4bea971cc303ac18d29b99067e46d16cc07f4ff



**Answer:** 04edcc123af7b13e90ce101a31c2f996f471a7c8f48a1b81d765085f548059a550f3f4f62ca1f0e8f74d727053074a37bceb2cbdc7ce2a8994dcd76dd6834eefc5438c3b6da929321f3a1366bd14c877cc83e5d0731b7f80a6b80916efd4a23a4d

**8. What is the first TLS 1.3 client random that was used to establish a connection with protonmail.com**

Filter: tls.handshake.exxtension\_server\_name == “protonmail.com”

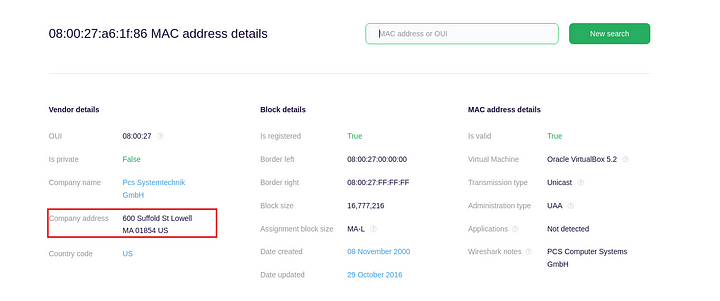
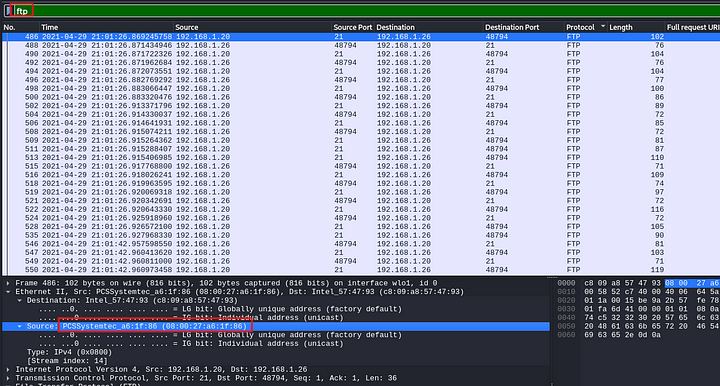


**Answer:** 24e92513b97a0348f733d16996929a79be21b0b1400cd7e2862a732ce7775b70

**9. Which country is the manufacturer of the FTP server’s MAC address registered in?**

Filter: ftp

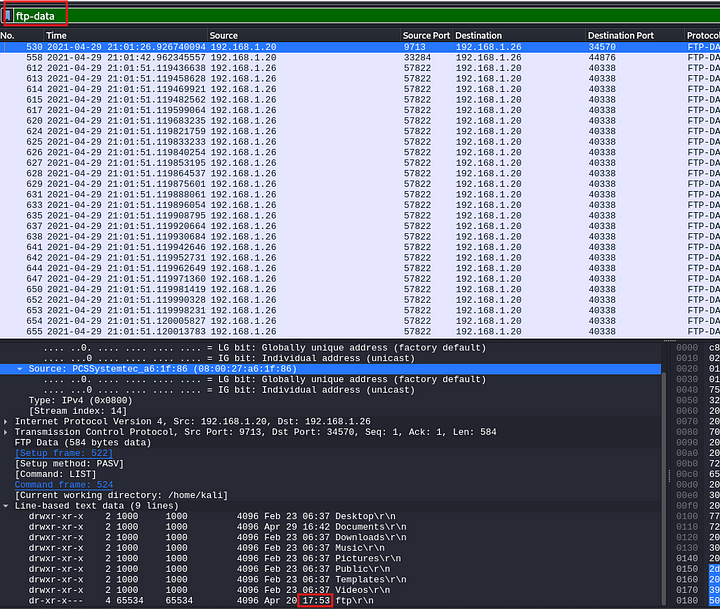
Select the first displayed packet, and copy its source mac address. Then paste this mac address in an online MAC lookup tool.



**Answer:** United States

**10. What time was a non-standard folder created on the FTP server on the 20th of April?**

Filter: ftp-data



**Answer:** 17:53

**11. What URL was visited by the user and connected to the IP address 104.21.89.171**

Filter: http && (ip.src == 192.168.1.26 && ip.dst == 104.21.89.171)



**Answer:**<http://dfir.science/>

This is the end of his walkthrough.