Incident Response Report

Incident ID: IR-20210430-001
Date: February 24, 2026
Analyst: Ruslan
Incident Type: Suspicious Network Activity, Internal Reconnaissance, and Potential Data Exfiltration
Status: Action Required

1. Executive Summary

On April 30, 2021, network traffic monitoring captured suspicious activity originating from an internal workstation (IP: 192.168.1.26). The user of this system interacted with an internal FTP server and multiple external web services in a manner suggesting possible unauthorized data gathering and exfiltration.

The initial compromise or insider activity involved successful authentication to the internal FTP server (192.168.1.20) using the credentials kali / AfricaCTF2021. The user transferred a media file (a JPEG image taken by an LG smartphone camera). Following the internal data transfer, the host queried the domain for archiving software (www.7-zip.org), sent anomalous UDP traffic to an external IP, and established encrypted TLS 1.3 communications with protonmail.com.

Forensic analysis of the FTP server revealed a non-standard folder created days prior, indicating potential staging. The combination of archiving tool queries, internal file access, and connections to external encrypted email services strongly points towards a data exfiltration attempt.

2. Timeline

Timestamp (UTC)	Event Category	Event Description	MITRE ATT&CK ID
01:01:26	Authentication	**Valid Accounts:** Successful FTP login to 192.168.1.20 using user kali and password AfricaCTF2021.	T1078 (Valid Accounts)
01:01:56	File Transfer	**Data Transfer:** Media file 20210429_152157.jpg was transferred via the unencrypted FTP session.	T1048 (Exfiltration Over Alternative Protocol)
01:02:57	Tool Acquisition	**DNS Query:** Host queried IPv6 DNS for www.7-zip.org (Packet 15174), likely to download compression tools.	T1071.004 (Application Layer Protocol: DNS)
01:02:59 – 01:03:18	Network Activity	**Outbound Traffic:** 10 UDP packets (Len=52) sent to external IP 24.39.217.246 on port 54150.	T1071 (Application Layer Protocol)
01:04:29	External Connection	**Encrypted Channel:** TLS 1.3 handshake initiated with protonmail.com (IP: 185.70.41.35).	T1071.001 (Web Protocols)
01:06:39	Web Browsing	**HTTP Traffic:** Unencrypted GET request to external site http://dfir.science/ (IP: 104.21.89.171).	T1071.001 (Web Protocols)

3. Technical Details

3.1. Investigated Asset (Client Workstation)

- **Internal IP:** 192.168.1.26
- **MAC address:** c8:09:a8:57:47:93 (Network card: IntelCor)
- **IPv6 DNS Server:** fe80::c80b:adff:feaa:1db7

3.2. Compromised Asset (FTP Server)

- **Internal IP:** 192.168.1.20
- **MAC address:** 08:00:27:a6:1f:86
- **Hardware Manufacturer Country:** United States (PCS Systemtechnik GmbH)
- **Staging Discovery:** A non-standard directory named ftp was discovered on the server. Directory metadata shows it was created prior to the main incident window, specifically on **April 20 at 17:53**, indicating persistent unauthorized access or staging activity.

3.3. Network Activity & Data Exfiltration Analysis

The activity utilized both plain-text internal protocols and encrypted external channels:

1. **Internal Authentication & Transfer:** The attacker/insider logged into the internal FTP server using the password AfricaCTF2021. The file 20210429_152157.jpg was interacted with. File metadata indicates the picture was taken using an LG camera, model **LM-Q725K**.
2. **Tooling:** Shortly after accessing internal files, a DNS lookup for www.7-zip.org was captured, indicating the user's intent to acquire an archiving tool to compress the gathered files.
3. **Encrypted External Comms (ProtonMail):** To bypass network inspection, the user established a secure TLS 1.3 session with ProtonMail.
    - *First TLS 1.3 Client Random:* 24e92513b97a0348f733d16996929a79be21b0b1400cd7e2862a732ce7775b70
4. **Advanced Cryptography:** Deep packet inspection of TLS traffic (Session ID: da4a00...) revealed the ephemeral public key provided by the server during the handshake:
    - *Key:* 04edcc123af7b13e90ce101a31c2f996f471a7c8f48a1b81d765085f548059a550f3f4f62ca1f0e8f74d727053074a37bceb2cbdc7ce2a8994dcd76dd6834eefc5438c3b6da929321f3a1366bd14c877cc83e5d0731b7f80a6b80916efd4a23a4d

4. IoCs

Type	Value	Description	Recommended Action
Credentials	kali : AfricaCTF2021	Compromised FTP account credentials.	**Reset / Disable**
IPv4	24.39.217.246	Target of suspicious outbound UDP traffic (10 packets).	**Block / Investigate**
Domain	www.7-zip.org	Archiving tool domain (used for	**Monitor**

		staging).	
URL	http://dfir.science/	Unencrypted HTTP site visited by the user.	**Monitor**
Filename	20210429_152157.jpg	Media file involved in internal data transfer.	**Analyze Content**
Folder Path	/ftp (created Apr 20, 17:53)	Suspicious directory created on the FTP server.	**Investigate**

5. Containment & Remediation

To prevent further data loss and secure the internal infrastructure, the following steps must be taken:

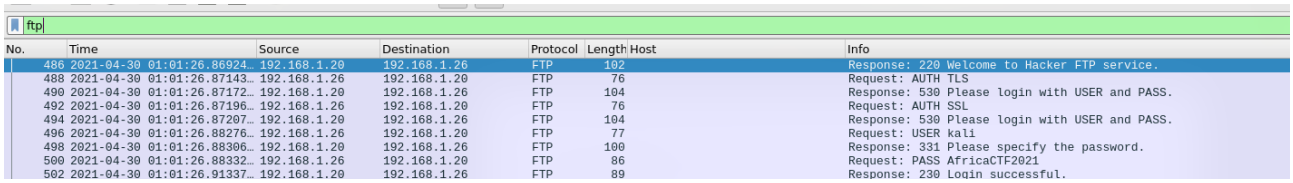
Immediate Actions (Containment):

1. Physically or logically disconnect workstation 192.168.1.26 from the corporate network to prevent further outbound data exfiltration.
2. Immediately disable the kali account on the FTP server (192.168.1.20) and rotate passwords for all other FTP user accounts.
3. Add the external IP 24.39.217.246 to the firewall Deny List.

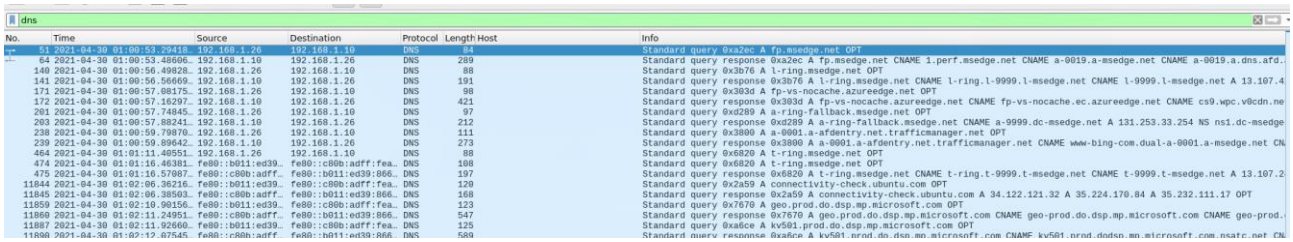
Short-term actions (Elimination):
4. Perform host-based forensics on the FTP server to analyze the contents of the /ftp directory created on April 20 at 17:53.
5. Review the contents of the 20210429_152157.jpg (LM-Q725K) image to determine if sensitive physical site information or documents were leaked.
6. Check the endpoints to confirm whether 7-Zip was successfully downloaded and installed, and look for .zip or .7z archive artifacts that may contain staged data.

Long-term actions (Improving security architecture):
7. Deprecate the use of unencrypted FTP (port 21) within the internal network. Migrate to secure alternatives such as SFTP (SSH File Transfer Protocol) or FTPS.
8. Implement strict firewall rules regarding which internal workstations are allowed to connect to external personal webmail services (e.g., ProtonMail), as these are common vectors for data exfiltration.

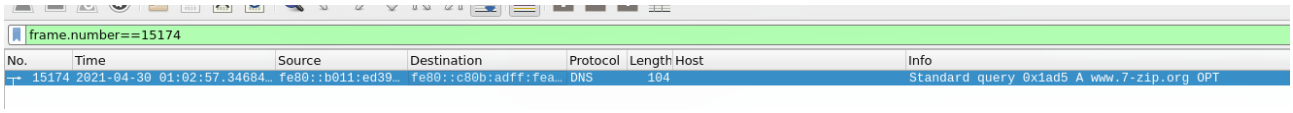
1. What is the FTP password?
- AfricaCTF2021

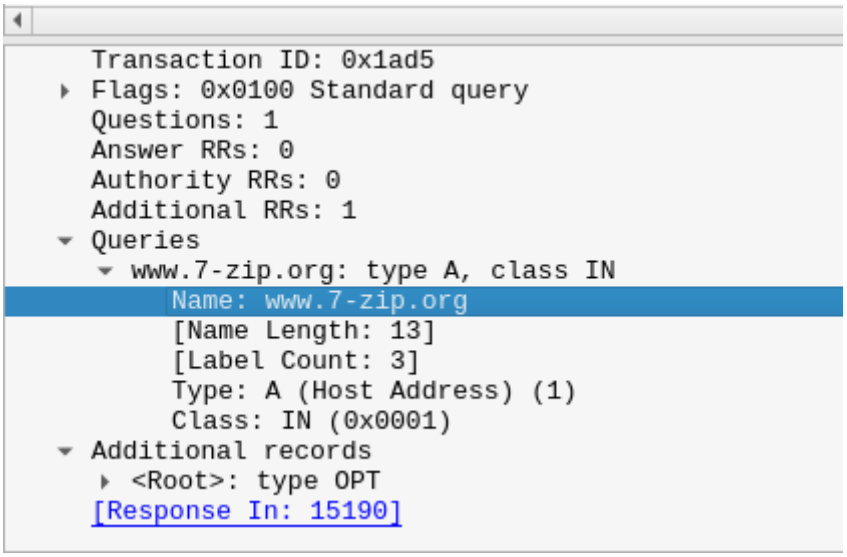


2. What is the IPv6 address of the DNS server used by 192.168.1.26?
- fe80::c80b:adff:feaa:1db7

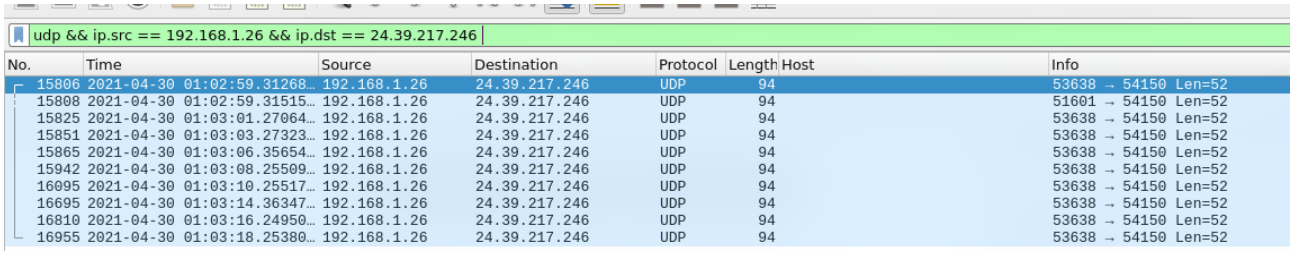


3. What domain is the user looking up in packet 15174?
- www.7-zip.org





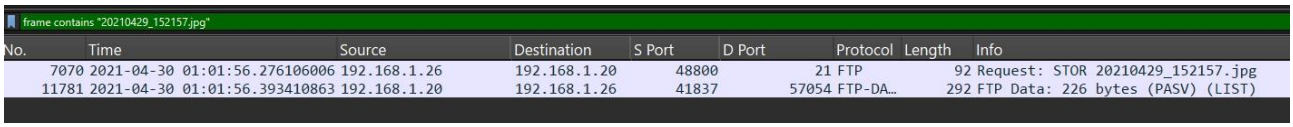
4. How many UDP packets were sent from 192.168.1.26 to 24.39.217.246?
- 10

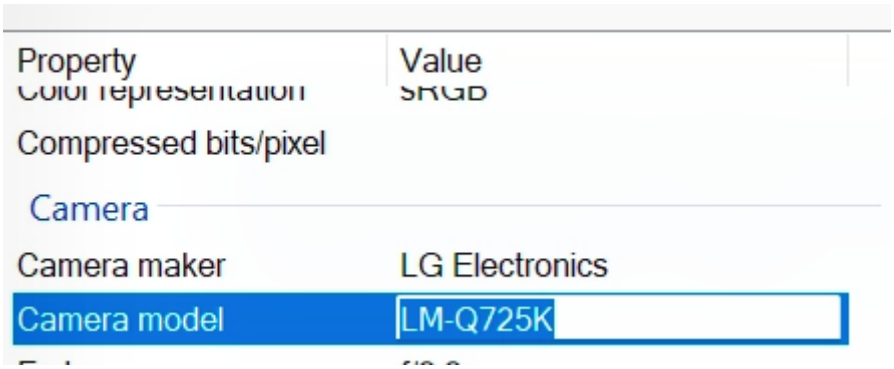


5. What is the MAC address of the system under investigation in the PCAP file?
- c8:09:a8:57:47:93

```
▸ Frame 15806: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface wlo1, id 0
▾ Ethernet II, Src: IntelCor_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: IntelCor_57:47:93 (c8:09:a8:57:47:93)
    Type: IPv4 (0x0800)
▸ 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)
```

6. What was the camera model name used to take picture 20210429_152157.jpg?
- LM-Q725K





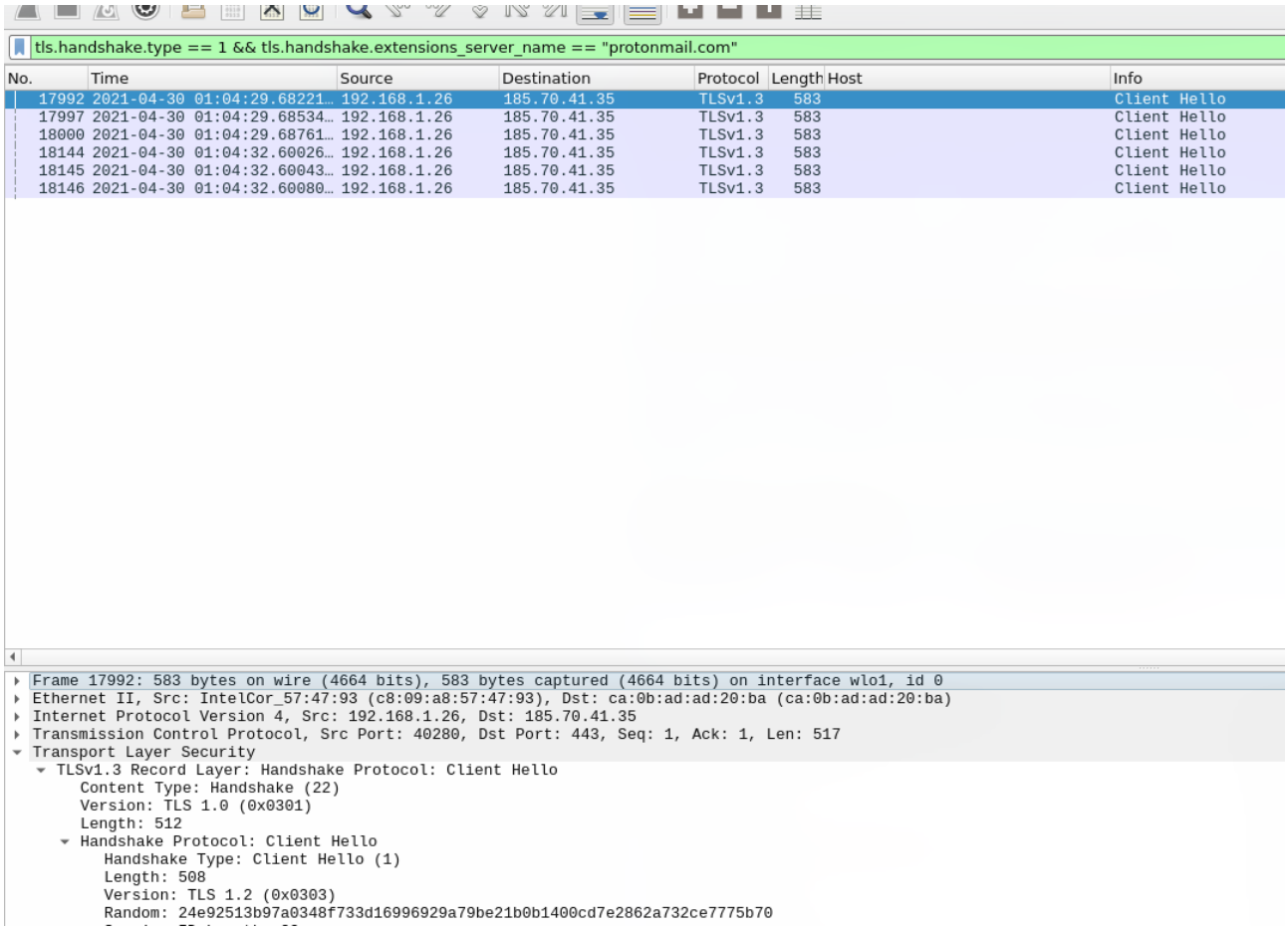
7. What is the ephemeral public key provided by the server during the TLS handshake in the session with the session ID: da4a0000342e4b73459d7360b4bea971cc303ac18d29b99067e46d16cc07f4ff?

-
04edcc123af7b13e90ce101a31c2f996f471a7c8f48a1b81d765085f548059a550f3f4f62ca1f0e8f74d727053074a37bceb2cbdc7ce2a8994dcd76dd6834eefc5438c3b6da929321f3a1366bd14c877cc83e5d0731b7f80a6b80916efd4a23a4d

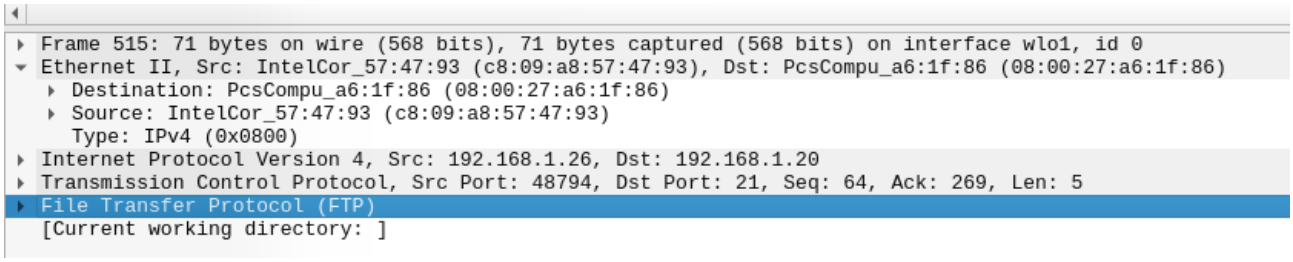
```
    ▸ Handshake Protocol: Certificate
    ▸ Handshake Protocol: Certificate Status
    ▾ Handshake Protocol: Server Key Exchange
        Handshake Type: Server Key Exchange (12)
        Length: 361
      ▾ EC Diffie-Hellman Server Params
          Curve Type: named_curve (0x03)
          Named Curve: secp384r1 (0x0018)
          Pubkey Length: 97
          Pubkey: 04edcc123af7b13e90ce101a31c2f996f471a7c8f48a1b81d765085f548059a550f3f4f6…
        ▸ Signature Algorithm: rsa_pkcs1_sha256 (0x0401)
          Signature Length: 256
          Signature: 11914710183397b395995313bea183e0abc19619361016080bff249af9c5d88e7f2b8e44…
    ▾ Handshake Protocol: Server Hello Done
        Handshake Type: Server Hello Done (14)
        Length: 0
```

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

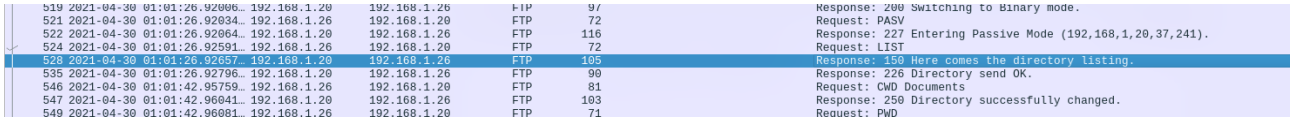
- 24e92513b97a0348f733d16996929a79be21b0b1400cd7e2862a732ce7775b70

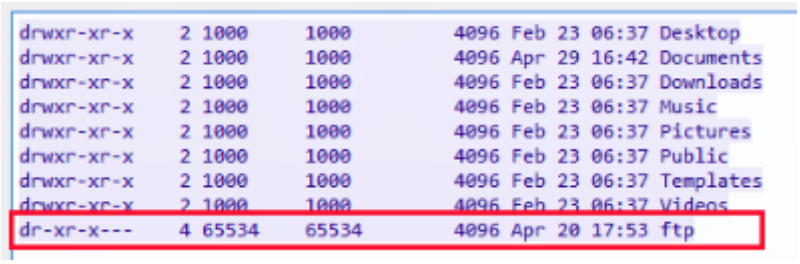


9. Which country is the manufacturer of the FTP server's MAC address registered in?
- United States



10. What time was a non-standard folder created on the FTP server on the 20th of April?
-17:53





11. What URL was visited by the user and connected to the IP address 104.21.89.171?
- http://dfir.science/