**Phishing Email Analysis Procedure**

**Step 1: Check Email Headers**

* Examine the email headers to identify the sender's IP, routing information, and any anomalies.
* Look for inconsistencies in the "From," "Reply-To," and "Received" fields.

**Step 2: Check Authentication Protocols**

* Verify that the email passes all three key authentication protocols: SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting, and Conformance).
* Check for "Pass" status in each. Failures may indicate spoofing.

**Step 3: Analyze File/Attachment Information**

* Identify any attachments, such as PDF or ZIP files.
* Decode attachments if encoded (e.g., Base64).

**Substep 3.1: Decode Base64 PDF to Hex Using CyberChef**

* Use CyberChef (an online tool for data transformation) to decode the Base64-encoded PDF attachment into hexadecimal format.
* Compare the decoded hex values against expected or known values.
* **Outcome Note:** If hex values do not match, proceed with caution as this may indicate tampering.

**Substep 3.2: Create and Extract ZIP File from CyberChef Output**

* Save the CyberChef output as an "attach.zip" file.
* Extract the contents of the ZIP file for further inspection.

**Substep 3.3: Verify ZIP File Contents**

* Install GHex if not available: Run sudo apt install ghex (on Ubuntu-based systems).
* Scan all metadata at once using ExifTool: Run exiftool -u PuzzleToCoCanDa/\* (replace "PuzzleToCoCanDa" with the actual extracted directory).
* Check hex values of individual documents using GHex.
  + **File 1: DaughtersCrown** - Hex value: Match (verified).
  + **File 2: GoodJobMajor** - Hex value: Match (verified).
  + **File 3: Money.xlsx** - Hex value: Mismatch (potential issue; investigate further).

**Substep 3.4: Open and Analyze Spreadsheet**

* Open the mismatched spreadsheet (e.g., Money.xlsx) in Google Sheets using a fake or disposable Gmail account to avoid risks.
* Inspect all sheets for hidden content.
* **Finding:** Hidden message found in Sheet 3.

**Substep 3.5: Decode Hidden Message**

* Extract the hidden message from Sheet 3 (likely Base64-encoded).
* Decode it using CyberChef to reveal the content (e.g., a location or IP address).
* **Finding:** Decoded message reveals a location or relevant data.

**Step 4: Further Network Checking**

* Use the decoded information (e.g., IP address from the hidden message) for network investigations.

**Substep 4.1: Traceroute to IP**

* Run traceroute 93.99.104.210 to trace the route to the IP and identify hops or geolocation.
* Analyze for suspicious routes or origins.

**Substep 4.2: Nmap Scan**

* Perform a stealth SYN scan: Run nmap -sS 93.99.104.210.
* Check for open ports, services, and vulnerabilities.
* **Note:** Ensure legal compliance; scanning without permission may violate laws.