**Phishing Analysis Tools and Resources**

**Free Online Email Header Analyzers**

**1. MXToolbox Email Header Analyzer**

* **URL**: <https://mxtoolbox.com/EmailHeaders.aspx>
* **Features**:
  + RFC 822 compliant parsing
  + Authentication results (SPF, DKIM, DMARC)
  + Hop analysis with delays
  + IP blacklist checking
* **Best for**: Comprehensive header analysis
* **Usage**: Paste full email headers and click analyze

**2. Trustifi Email Analyzer**

* **URL**: <https://trustifi.com/email-analyzer/>
* **Features**:
  + Security protocol analysis
  + Delay identification
  + Authentication verification
  + User-friendly interface
* **Best for**: Security-focused analysis
* **Usage**: Paste headers or upload .eml file

**3. Mailmodo Email Header Analyzer**

* **URL**: <https://www.mailmodo.com/tools/email-header-analyzer/>
* **Features**:
  + Common header breakdown
  + Authentication headers
  + Server path analysis
  + Mobile-friendly interface
* **Best for**: Quick analysis with clear results
* **Usage**: Copy headers from various email clients

**4. Zoho Email Header Analyzer**

* **URL**: <https://www.zoho.com/toolkit/email-header-analyzer.html>
* **Features**:
  + Three-section analysis (message, hop, other details)
  + Sender information analysis
  + Spam/phishing identification
  + Route tracking
* **Best for**: Detailed hop analysis
* **Usage**: Paste original message content

**5. WhatIsMyIP Email Header Analyzer**

* **URL**: <https://www.whatismyip.com/email-header-analyzer/>
* **Features**:
  + IP address extraction
  + Location identification
  + Simple interface
  + Fast analysis
* **Best for**: Quick IP and location checks
* **Usage**: Paste header and click analyze

**URL and Link Analysis Tools**

**1. VirusTotal**

* **URL**: <https://www.virustotal.com/gui/home/url>
* **Features**:
  + Multi-engine scanning
  + Reputation checking
  + Historical data
  + Community comments
* **Usage**: Submit suspicious URLs for analysis

**2. URLVoid**

* **URL**: <https://www.urlvoid.com/>
* **Features**:
  + Multiple blacklist checks
  + Website reputation
  + IP information
  + Domain details
* **Usage**: Enter URL for reputation check

**3. Hybrid Analysis**

* **URL**: <https://www.hybrid-analysis.com/>
* **Features**:
  + Behavioral analysis
  + Malware detection
  + Detailed reports
  + Free tier available
* **Usage**: Submit URLs/files for sandbox analysis

**4. Any.run**

* **URL**: <https://any.run/>
* **Features**:
  + Interactive sandbox
  + Real-time analysis
  + Network traffic monitoring
  + Screenshot capture
* **Usage**: Submit URLs for live analysis

**Domain and IP Analysis Tools**

**1. WHOIS Lookup**

* **URL**: <https://whois.net/> or <https://www.whois.com/>
* **Features**:
  + Domain registration details
  + Registrar information
  + Creation/expiration dates
  + Contact information
* **Usage**: Search domain name for ownership details

**2. DNS Lookup Tools**

* **URL**: <https://dnschecker.org/>
* **Features**:
  + Multiple DNS record types
  + Global DNS propagation
  + Mail server information
  + IP resolution
* **Usage**: Check DNS records for domains

**3. IP Geolocation**

* **URL**: <https://whatismyipaddress.com/ip-lookup>
* **Features**:
  + Geographic location
  + ISP information
  + Organization details
  + Threat intelligence
* **Usage**: Enter IP address for location data

**4. Shodan**

* **URL**: <https://www.shodan.io/>
* **Features**:
  + Internet-connected device search
  + Service identification
  + Vulnerability information
  + Historical data
* **Usage**: Search IP addresses for exposed services

**Email Header Extraction Guides**

**Gmail (Web)**

1. Open email
2. Click three vertical dots (⋮)
3. Select "Show original"
4. Copy full content

**Outlook (Web)**

1. Open email
2. Click three horizontal dots (•••)
3. Choose "View message source"
4. Copy header section

**Outlook (Desktop)**

1. Open email in Outlook
2. Click "File" → "Properties"
3. Copy "Internet headers" content

**Apple Mail**

1. Open email
2. View → Message → All Headers
3. Copy displayed headers

**Thunderbird**

1. Open email
2. View → Message Source (Ctrl+U)
3. Copy header portion

**Browser-Based Tools**

**1. Browser Developer Tools**

* **Access**: F12 or right-click → Inspect
* **Usage**: Analyze suspicious websites (if safe to visit)
* **Features**:
  + Network traffic monitoring
  + Script analysis
  + Resource inspection

**2. Browser Extensions**

* **Netcraft Extension**: Website reputation and phishing protection
* **Web of Trust (WOT)**: Community-based website ratings
* **uBlock Origin**: Block malicious content and tracking

**Command Line Tools (Advanced)**

**1. Dig Command**

dig domain.com MX  
dig domain.com TXT

* **Purpose**: DNS record lookup
* **Usage**: Check SPF, DMARC records

**2. Nslookup**

nslookup domain.com  
nslookup -type=MX domain.com

* **Purpose**: Name server lookup
* **Usage**: Resolve domains to IP addresses

**3. Whois Command**

whois domain.com

* **Purpose**: Domain registration information
* **Usage**: Get ownership and registration details

**Mobile Apps**

**1. Email Header Analyzer (Android/iOS)**

* **Features**: Mobile-friendly header analysis
* **Usage**: Analyze emails on mobile devices

**2. Network Analyzer (iOS/Android)**

* **Features**: Network diagnostics
* **Usage**: Check connectivity and DNS resolution

**Creating Test Environment**

**1. Virtual Machine Setup**

* **Software**: VirtualBox, VMware
* **Purpose**: Safe environment for malware analysis
* **Usage**: Isolate suspicious content analysis

**2. Isolated Network**

* **Setup**: Separate network segment
* **Purpose**: Contain potential threats
* **Usage**: Advanced malware analysis