**Domain Name Investigation Checklist**

**Basic Domain Information**

**· Identify the domain registration**

**Tools :- Namecheap WHOIS**

**Link :-- https://www.namecheap.com/domains/whois/lookup/**

**· Check domain creation, update, and expiration dates**

**Tools:- ViewDNS.info, DNSlytics**

**Link :--** [**https://viewdns.info/whois/**](https://viewdns.info/whois/)

[**https://dnslytics.com/**](https://dnslytics.com/)

**· Determine domain status (active, expired, clientHold, etc.)**

**Tools:-Censys, VirusTotal**

**Link :--**  [**https://censys.io/**](https://censys.io/)

[**https://www.virustotal.com/**](https://www.virustotal.com/)

**· Retrieve WHOIS information (registrant, organization, email)**

**Tools:- Whois.com, DomainTools**

**Link :--** [**https://whois.domaintools.com**](https://whois.domaintools.com/)

[**https://www.whois.com/**](https://www.whois.com/)

**· Check registration abuse contact details**

**Tools:-RDAP.org,AbuseIPDB, Spamhaus**

**Link :--** [**https://rdap.org/**](https://rdap.org/)

[**https://www.abuseipdb.com/**](https://www.abuseipdb.com/)

**https://check.spamhaus.org**

**Hosting & Infrastructure**

**· Identify associated IP addresses**

**Tools:- DNS Checker, Shodan**

**Link :--** [**https://dnschecker.org/**](https://dnschecker.org/)

[**https://www.shodan.io/**](https://www.shodan.io/)

**· Geolocate the IP(s)**

**Tools:- Ipinfo, ipapi**

**Link :--**  [**https://ipinfo.io/**](https://ipinfo.io/)

[**https://ipapi.co/**](https://ipapi.co/)

**· Perform reverse DNS lookup**

**Tools:- MXToolbox, DNSstuff**

**Link :--** [**https://mxtoolbox.com/ReverseLookup.aspx**](https://mxtoolbox.com/ReverseLookup.aspx)

[**https://www.dnsstuff.com/**](https://www.dnsstuff.com/)

**· Check hosting provider and AS number (Autonomous System)**

**Tools:- WhoisXML API, MaxMind**

**Link :--**

**· Check for shared hosting or other hosted domains on same IP**

**DNS Records**

**· Retrieve A, AAAA, MX, TXT, NS, SOA, and CNAME records**

**Tools:- Google Dig, DigWebInterface**

**Link :--** [**https://digwebinterface.com/**](https://digwebinterface.com/)

[**https://toolbox.googleapps.com/apps/dig/**](https://toolbox.googleapps.com/apps/dig/)

**· Check SPF, DKIM, DMARC configurations**

**Tools:- MXToolbox SPF Check, DKIMCore**

**Link :--** [**https://mxtoolbox.com/spf.aspx**](https://mxtoolbox.com/spf.aspx)

[**https://dkimcore.org/tools/keycheck.html**](https://dkimcore.org/tools/keycheck.html)

|  |
| --- |

|  |
| --- |

**· Check for recent DNS changes (passive DNS history)**

**Tools:- SecurityTrails, Robtex**

**Link :--**  [**https://securitytrails.com/**](https://securitytrails.com/)

[**https://www.robtex.com/**](https://www.robtex.com/)

**· Identify any dynamic DNS usage**

**Tools:- DynDNS, No-IP**

**Link :--** [**https://dyn.com/**](https://dyn.com/)

[**https://www.noip.com/**](https://www.noip.com/)

**Domain Reputation & Threat Intelligence**

**· Check domain reputation (VirusTotal, Cisco Talos, IBM X-Force, etc.)**

**Tools:- Cisco Talos Intelligence, IBM X-Force Exchange**

**Link :--** [**https://talosintelligence.com/**](https://talosintelligence.com/)

[**https://exchange.xforce.ibmcloud.com**](https://exchange.xforce.ibmcloud.com/)

**· Lookup in threat intelligence feeds (AlienVault OTX, AbuseIPDB)**

**Tools:- AbuseIPDB, ThreatMiner**

**Link :--**  [**https://www.abuseipdb.com/**](https://www.abuseipdb.com/)

[**https://www.threatminer.org/**](https://www.threatminer.org/)

**· Check for blacklisting (Spamhaus, SURBL, Google Safe Browsing)**

**Tools:- SURBL, MultiRBL Check**

**Link :--**  [**http://www.surbl.org/**](http://www.surbl.org/)

[**https://multirbl.valli.org**](https://multirbl.valli.org/)

**· Investigate if used in phishing, malware, or spam campaigns**

**Tools:- PhishTank, URLhaus**

**Link :--**  [**https://www.phishtank.com/**](https://www.phishtank.com/)

[**https://urlhaus.abuse.ch**](https://urlhaus.abuse.ch/)

**Website Content & Technology**

**· Analyze live website content (homepage, source code)**

**Tools:- HTTrack, Netcraft Site Report**

**Link :--**  [**https://www.httrack.com/**](https://www.httrack.com/)

[**https://sitereport.netcraft.com**](https://sitereport.netcraft.com/)

**· Use site capture tools (Wayback Machine, Archive.today)**

**Tools:- Wayback Machine, Archive.today**

**Link :--**  [**https://archive.org/web**](https://archive.org/web)

[**https://archive.today/**](https://archive.today/)

**· Identify CMS and technologies (Wappalyzer, BuiltWith)**

**Tools:- Wappalyzer, Netcraft**

**Link :--** [**https://www.wappalyzer.com/**](https://www.wappalyzer.com/)

[**https://sitereport.netcraft.com**](https://sitereport.netcraft.com/)

**· Check for malicious scripts or redirects**

**Tools:- VirusTotal URL Scanner, URLScan.io**

**Link :--**  [**https://www.virustotal.com/**](https://www.virustotal.com/)

[**https://urlscan.io/**](https://urlscan.io/)

**· Take screenshots for documentation**

**Tools:- PageCapture.io, Screenshot Guru**

**Link :--**  [**https://www.pagecapture.io/**](https://www.pagecapture.io/)

[**https://screenshot.guru/**](https://screenshot.guru/)

**Historical Data**

**· Review historical WHOIS records (Domaintools, SecurityTrails)**

**Tools:-** Spyse , **ViewDNS.info WHOIS History**

**Link :--** [**https://censys.io/**](https://censys.io/)

**https://viewdns.info/**

**· Analyze past hosting records and IP changes**

**Tools:- DomainTools Hosting History, IPinfo**

**Link :--**  [**https://whois.domaintools.com**](https://whois.domaintools.com/)

[**https://ipinfo.io/**](https://ipinfo.io/)

**· Check for prior uses or associations (business, personal, cybercrime)**

**Tools:- ThreatMiner, AlienVault OTX**

**Link :--** [**https://www.threatminer.org/**](https://www.threatminer.org/)

[**https://otx.alienvault.com**](https://otx.alienvault.com/)

**Email Associations**

**· Identify registrant email (if public)**

**Tools:- SecurityTrails, WhoisXML API**

**Link :--** [**https://whois.whoisxmlapi.com**](https://whois.whoisxmlapi.com/)

[**https://securitytrails.com/**](https://securitytrails.com/)

**· Check if email was used for registering other domains**

**Tools:- WhoisXML Reverse WHOIS, DomainTools Reverse WHOIS**

**Link :--**  [**https://reverse-whois.whoisxmlapi.com**](https://reverse-whois.whoisxmlapi.com/)

[**https://research.domaintools.com/reverse-whois**](https://research.domaintools.com/reverse-whois)

**· Check if email is leaked in breaches**

**Tools:- HaveIBeenPwned, LeakCheck**

**Link :--** [**https://haveibeenpwned.com/**](https://haveibeenpwned.com/)

[**https://leakcheck.io/**](https://leakcheck.io/)

**· Look for email patterns across other domain registrations**

**Tools:- DomainTools Iris Investigate, ThreatCrowd**

**Link :--**  [**https://www.domaintools.com/products/iris/**](https://www.domaintools.com/products/iris/)

[**https://www.threatcrowd.org/**](https://www.threatcrowd.org/)

**Registrant & Organization Links**

**· Map out registrant and organization connections**

**Tools:- SpyOnWeb, Farsight DNSDB**

**Link :--** [**http://spyonweb.com/**](http://spyonweb.com/)

[**https://www.farsightsecurity.com/tools/dnsdb/**](https://www.farsightsecurity.com/tools/dnsdb/)

**· Investigate linked domains, aliases, and IP ranges**

**Tools:- VirusTotal Graph, GreyNoise**

**Link :--**  [**https://www.virustotal.com/graph**](https://www.virustotal.com/graph)

[**https://www.greynoise.io/**](https://www.greynoise.io/)

**· Correlate with other known threat actors or campaigns**

**Tools:- MITRE ATT&CK, Maltego**

**Link :--**  [**https://attack.mitre.org**](https://attack.mitre.org/)

[**https://www.maltego.com/**](https://www.maltego.com/)

**Email Address Investigation Checklist**

**Basic Information**

**· Identify the email service provider (Gmail, Yahoo, ProtonMail, custom domain)**

**Tools:- EmailHippo, MailTester**

**Links:-**  [**https://mailtester.com/**](https://mailtester.com/)

[**https://tools.emailhippo.com**](https://tools.emailhippo.com/)

**· Extract domain from email and investigate domain reputation**

**Tools:- VirusTotal, Cisco Talos Intelligence**

**Links:-** [**https://www.virustotal.com/**](https://www.virustotal.com/) [**https://talosintelligence.com/**](https://talosintelligence.com/)

**· Check if it's disposable, temporary, or anonymous email provider**

**Tools:- MailCheck.ai , EmailListVerify**

**Links:-** [**https://mailcheck.ai/**](https://mailcheck.ai/) [**https://emaillistverify.com/**](https://emaillistverify.com/)

**· Assess format (e.g., firstname.lastname, numeric suffixes, random strings)**

**Tools:- Hunter Email Finder, LinkedIn**

**Links:-**  [**https://www.linkedin.com/**](https://www.linkedin.com/) [**https://metricsparrow.com/tool/email-permutator/**](https://metricsparrow.com/tool/email-permutator/)

**Breach and Leak Exposure**

**· Search for email in breach databases**

**HaveIBeenPwned** [**https://haveibeenpwned.com/**](https://haveibeenpwned.com/)

**Firefox Monitor** [**https://monitor.firefox.com**](https://monitor.firefox.com/)

**· Look for associated credentials (username/password dumps)**

**LeakCheck.io**  [**https://leakcheck.io/**](https://leakcheck.io/)

**GhostProject.fr**  [**https://ghostproject.fr/**](https://ghostproject.fr/)

**· Identify reuse in known data leaks or darknet dumps**

**IntelX**  [**https://intelx.io/**](https://intelx.io/)

**Ahmia.fi**  [**https://ahmia.fi/**](https://ahmia.fi/)

**· Check if exposed in paste sites (e.g., Pastebin, Ghostbin)**

**Pastebin**  [**https://pastebin.com/**](https://pastebin.com/)

**Scylla.sh**  [**https://scylla.sh/**](https://scylla.sh/)

**Email Reputation & Threat Intelligence**

**· Check if email is reported in spam or phishing campaigns**

**EmailRep.io**  [**https://emailrep.io/**](https://emailrep.io/)

**Spamhaus Lookup** [**https://check.spamhaus.org**](https://check.spamhaus.org/)

**· Search for presence in threat intelligence platforms (e.g., VirusTotal, AbuseIPDB, OTX)**

**VirusTotal**  [**https://www.virustotal.com/**](https://www.virustotal.com/)

**AbuseIPDB**  [**https://www.abuseipdb.com/**](https://www.abuseipdb.com/)

**· Determine associations with malware delivery or scam campaigns**

**PhishTank**  [**https://www.phishtank.com/**](https://www.phishtank.com/)

**ThreatMiner** [**https://www.threatminer.org/**](https://www.threatminer.org/)

**· Look for abuse reports or fraud listings**

**FraudWatch** [**https://fraudwatch.com/**](https://fraudwatch.com/)

**DeHashed**  [**https://www.dehashed.com/**](https://www.dehashed.com/)

**Reverse Lookup & Identity Correlation**

**· Perform reverse email lookup (LinkedIn, Hunter.io, Pipl, Social Searcher)**

**Pipl** [**https://pipl.com/**](https://pipl.com/)

**Social Searcher**  [**https://www.social-searcher.com/**](https://www.social-searcher.com/)

**· Check if used in social media accounts (Facebook, Twitter, Instagram)**

**KnowEm** [**https://knowem.com/**](https://knowem.com/)

**Facebook Search**  [**https://www.facebook.com/**](https://www.facebook.com/)

**· Identify name, phone numbers, photos, or aliases linked to email**

**DeHashed** [**https://www.dehashed.com/**](https://www.dehashed.com/)

**IntelX**  [**https://intelx.io/**](https://intelx.io/)

**· Correlate email with known threat actor profiles (e.g., MISP, APT notes)**

**AlienVault OTX** [**https://otx.alienvault.com**](https://otx.alienvault.com/)

**Malpedia** [**https://malpedia.caad.fkie.fraunhofer.de**](https://malpedia.caad.fkie.fraunhofer.de/)

**Domain Analysis (for custom domains)**

**· Investigate domain ownership (WHOIS)**

**Whois Lookup by ICANN** [**https://lookup.icann.org**](https://lookup.icann.org/)

**WhoisXML API**  [**https://www.whoisxmlapi.com/**](https://www.whoisxmlapi.com/)

**· Check domain’s mail configurations (SPF, DKIM, DMARC)**

**MXToolbox Email Health Check** [**https://mxtoolbox.com/emailhealth**](https://mxtoolbox.com/emailhealth)

**DMARC Analyzer**  [**https://www.dmarcanalyzer.com/**](https://www.dmarcanalyzer.com/)

**· Look up domain DNS records (MX, TXT)**

**DNS Checker** [**https://dnschecker.org/**](https://dnschecker.org/)

**IntoDNS** [**https://intodns.com/**](https://intodns.com/)

**· Analyze hosting and IP geolocation**

**IPinfo.io**  [**https://ipinfo.io/**](https://ipinfo.io/)

**IP2Location** [**https://www.ip2location.com/demo**](https://www.ip2location.com/demo)

**· Review history of domain usage (legitimate or malicious)**

**Wayback Machine**  [**https://archive.org/web**](https://archive.org/web)

**VirusTotal**  [**https://www.virustotal.com/**](https://www.virustotal.com/)

**Technical Header Analysis (if email message available)**

**· Analyze "Received" headers to trace mail path**

**Header Analyzer Pro**  [**https://www.header-analyzer.com/**](https://www.header-analyzer.com/)

**MxToolbox Email Header Analyzer** [**https://mxtoolbox.com/EmailHeaders.aspx**](https://mxtoolbox.com/EmailHeaders.aspx)

**· Identify originating IP address and geolocation**

**IPinfo.io**  [**https://ipinfo.io/**](https://ipinfo.io/)

**WhatIsMyIPAddress Lookup** [**https://whatismyipaddress.com/ip-lookup**](https://whatismyipaddress.com/ip-lookup)

**· Check sending MTA (mail transfer agent) and mail client**

**Header Analyzer Pro** [**https://www.header-analyzer.com/**](https://www.header-analyzer.com/)

**Microsoft Message Header Analyzer** [**https://mha.azurewebsites.net/**](https://mha.azurewebsites.net/)

**· Detect signs of spoofing or forged headers**

**Google Header Analyzer** [**https://toolbox.googleapps.com/apps/messageheader/**](https://toolbox.googleapps.com/apps/messageheader/)

**Mailhardener Email Validator** [**https://www.mailhardener.com/emailtools/email-analyzer**](https://www.mailhardener.com/emailtools/email-analyzer)

**· Correlate timestamp, timezone, and relay chain**

**Header Analyzer Pro**  [**https://www.header-analyzer.com/**](https://www.header-analyzer.com/)

**MxToolbox Email Headers** [**https://mxtoolbox.com/EmailHeaders.aspx**](https://mxtoolbox.com/EmailHeaders.aspx)

**Behavioral Analysis**

**· Check if email is used in online scams, fraud, or impersonation**

**Scamwatch**  [**https://www.scamwatch.gov.au/**](https://www.scamwatch.gov.au/)

**FraudWatch**  [**https://www.fraudwatch.com/**](https://www.fraudwatch.com/)

**· Look for patterns in subject lines, writing style, grammar (for phishing emails)**

**PhishTool**  [**https://www.phishtool.com/**](https://www.phishtool.com/)

**Mailsploit Checker**  [**https://mailsploit.com/**](https://mailsploit.com/)

**· Assess tone and urgency tactics in message body**

**CheckPhish.ai**  [**https://checkphish.ai/**](https://checkphish.ai/)

**· Detect any embedded links, malicious attachments, or obfuscation**

**Any.Run**  [**https://any.run/**](https://any.run/)

**Web Presence & Footprint**

**· Google search the email (in quotes for exact match)**

**Google Search**  [**https://www.google.com/**](https://www.google.com/)

**· Search in forums, blogs, shopping sites, or comment sections**

**Scylla.sh**  [**https://scylla.sh/**](https://scylla.sh/)

**Google Blog Search** [**https://www.google.com/search?q="email@example.com"+blog**](https://www.google.com/search?q=%22email@example.com%22+blog)

**· Use username/email correlation tools (e.g., Sherlock, Maigret)**

**WhatsMyName Tool** [**https://github.com/WebBreacher/WhatsMyName**](https://github.com/WebBreacher/WhatsMyName)

**· Look up Gravatar or avatar images associated with the email**

**Have I Seen This Gravatar?** [**https://gravatar-profile-viewer.vercel.app**](https://gravatar-profile-viewer.vercel.app/)

**Email Header Spoof Detection (if phishing suspected)**

**· Compare "From" and "Return-Path" fields**

**Header Analyzer Pro**  [**https://www.header-analyzer.com/**](https://www.header-analyzer.com/)

**· Analyze SPF/DKIM/DMARC results for delivery authenticity**

**Mailhardener Email Analyzer** [**https://www.mailhardener.com/emailtools/email-analyzer**](https://www.mailhardener.com/emailtools/email-analyzer)

**· Investigate sending domain's legitimacy**

**Whois Lookup** [**https://lookup.icann.org**](https://lookup.icann.org/)

**IP Address Investigation Checklist**

**Basic Information**

**· Identify IP version (IPv4 / IPv6)**

[**https://ipinfo.io/**](https://ipinfo.io/) [**https://whatismyipaddress.com/**](https://whatismyipaddress.com/)

**· Check IP type (Public, Private, Reserved, Loopback, etc.)**

**Whois Lookup Tools like ARIN**

**· Determine if static or dynamic IP**

[**https://whatismyipaddress.com/**](https://whatismyipaddress.com/)

**Geolocation and Ownership**

**· Geolocate the IP (country, region, city)**

**IPgeolocation.io**  [**https://ipgeolocation.io/**](https://ipgeolocation.io/)

**· Check ISP / hosting provider**

**WhatIsMyIPAddress**  [**https://whatismyipaddress.com/**](https://whatismyipaddress.com/)

**· Identify ASN (Autonomous System Number) and AS owner**

**BGPView.io**  [**https://bgpview.io/**](https://bgpview.io/)

**· Determine if the IP belongs to a VPN, proxy, TOR exit node, or mobile network**

**IPQualityScore**  [**https://www.ipqualityscore.com/**](https://www.ipqualityscore.com/)

**Reverse DNS and Hostname**

**· Perform reverse DNS lookup**

**MXToolbox Reverse Lookup**  [**https://mxtoolbox.com/ReverseLookup.aspx**](https://mxtoolbox.com/ReverseLookup.aspx)

**· Identify associated domain name(s)**

**ViewDNS Reverse IP Lookup**  [**https://viewdns.info/reverseip/**](https://viewdns.info/reverseip/)

**· Check hostname patterns (e.g., dynamic, VPN, ISP-assigned)**

**Whois (IP)**  [**https://whois.domaintools.com**](https://whois.domaintools.com/)

**Blacklist and Threat Intelligence**

**· Check IP reputation**

**VirusTota** [**https://www.virustotal.com/**](https://www.virustotal.com/)**l**

**· Lookup in blocklists and RBLs**

**Spamhaus** [**https://www.spamhaus.org/**](https://www.spamhaus.org/)

**· Check for associations with malware, phishing, botnets, or brute-force activity**

**VirusTotal**  [**https://www.virustotal.com/**](https://www.virustotal.com/) **AbuseIPDB**  [**https://www.abuseipdb.com/**](https://www.abuseipdb.com/)

**· Look up in public threat feeds**

**AlienVault OTX** [**https://otx.alienvault.com**](https://otx.alienvault.com/)

**Port Scanning and Services (if authorized)**

**· Perform basic port scan**

**Shodan**  [**https://www.shodan.io/**](https://www.shodan.io/)

**Identify open ports and exposed services**

**ZoomEye**  [**https://www.zoomeye.org/**](https://www.zoomeye.org/)

**· Analyze banners for version info and misconfigurations**

**Netcat** [**https://nmap.org/ncat/**](https://nmap.org/ncat/)

**· Check for vulnerabilities on exposed services**

**OpenVAS** [**https://www.greenbone.net/en/**](https://www.greenbone.net/en/)

**Passive DNS and Historical Data**

**· Lookup passive DNS history**

**SecurityTrails** [**https://securitytrails.com/**](https://securitytrails.com/)

**· Identify previously resolved domains**

**RiskIQ Community**  [**https://community.riskiq.com**](https://community.riskiq.com/) **Robtex**  [**https://www.robtex.com/**](https://www.robtex.com/)

**· Check IP address history (hosting, ownership changes)**

**ViewDNS - IP History** [**https://viewdns.info/iphistory/**](https://viewdns.info/iphistory/)

**Web and Internet Presence**

**· Search IP in Google, forums, paste sites, and OSINT platforms**

**Google Dorking**  [**https://www.google.com/**](https://www.google.com/)

**· Check if used in spam campaigns or phishing kits**

**AbuseIPDB**  [**https://www.abuseipdb.com/**](https://www.abuseipdb.com/)

**· Investigate use in previous cyberattacks or coordinated infrastructure**

**GreyNoise**  [**https://www.greynoise.io/**](https://www.greynoise.io/)

**Behavioral and Traffic Analysis (if internal)**

**· Correlate with firewall and SIEM logs**

**Splunk**  [**https://www.splunk.com/**](https://www.splunk.com/) **Elastic SIEM**  [**https://www.elastic.co/siem**](https://www.elastic.co/siem)

**· Check connection frequency, data volume, and destinations**

**Wireshark**  [**https://www.wireshark.org/**](https://www.wireshark.org/)

**· Look for suspicious behavior (beacons, lateral movement, scanning)**

**Darktrace**  [**https://www.darktrace.com/**](https://www.darktrace.com/)

**· Link with internal alerts or incidents (EDR, NDR, IDS)**

**Suricata**  [**https://suricata.io/**](https://suricata.io/)

**Correlation & Attribution**

**· Correlate with domains, email addresses, file hashes, or user accounts**

**AlienVault OTX** [**https://otx.alienvault.com**](https://otx.alienvault.com/)

**· Look for related IOCs across threat campaigns**

**MITRE ATT&CK Navigator** [**https://attack.mitre.org**](https://attack.mitre.org/)

**· Assess links to APT groups, botnets, or cybercriminal forums**

**ThreatMiner**  [**https://www.threatminer.org/**](https://www.threatminer.org/)

**· Evaluate potential spoofing or NAT usage**

**GreyNoise**  [**https://www.greynoise.io/**](https://www.greynoise.io/)

**Phone Number Investigation Checklist**

**Basic Number Details**

**· Identify country code and carrier prefix**

**Tool :- Twilio Lookup**

**Link :- twilio.com/lookup**

**· Determine if number is mobile, landline, VoIP, or toll-free**

**Tool :- TrueCaller**

**Link :-** [**https://www.truecaller.com/**](https://www.truecaller.com/)

**· Check if number is from a disposable or virtual phone service**

**Tool :- TextNow**

**Link :-** [**https://www.textnow.com/**](https://www.textnow.com/)

**· Validate number format using tools like**

**Tool :- PhoneInfoga**

**Link :-** [**https://phoneinfoga.net/**](https://phoneinfoga.net/)

**Carrier & Geolocation**

**· Identify telecom operator or virtual provider**

**Tool :- Nexmo**

**Link :-**  [**https://www.nexmo.com/**](https://www.nexmo.com/)

**· Approximate geolocation (city, state, or country-level)**

**Tool :- IPQualityScore**

**Link :- ipqualityscore.com**

**· Determine portability (has number been moved across carriers?)**

**Tool :- Telesign**

**Link :-** [**https://www.telesign.com/**](https://www.telesign.com/)

**Spam, Scam, and Abuse Reports**

**Check phone reputation (e.g., TrueCaller, WhoCallsMe,)**

**Tool :- TrueCaller**

**Link :-** [**https://www.truecaller.com/**](https://www.truecaller.com/)

**Tool :-WhoCallsMe**

**Link :-** [**http://whocallsme.com**](http://whocallsme.com/)

**· Search for user complaints, fraud, or harassment reports**

**Tool :- WhoCallsMe**

**Link :-** [**https://whocallsme.com/**](https://whocallsme.com/)

**· Look for listings on fraud watchlists, robocall databases, or scam-reporting forums**

**Tool :- ScamNumbers.info**

**Link :-** [**https://scamnumbers.info/**](https://scamnumbers.info/)

**Reverse Lookup & OSINT**

**· Perform reverse phone lookup (e.g., TrueCaller)**

[**Tool :-**](https://www.truecaller.com/) **TrueCaller**

**Link :-**  [**https://www.truecaller.com/**](https://www.truecaller.com/)

**· Search in Google, social media, data breach repositories, and paste sites**

**Tool :- Google Dorks**

**Link :-** [**https://www.google.com/**](https://www.google.com/)

**· Check if phone number appears in online ads, marketplaces, or classifieds (e.g., OLX)**

**Tool :- OLX**

**Link :-** [**https://www.olx.in/en-in**](https://www.olx.in/en-in)

**· Look up in people search engines (BeenVerified)**

**Tool :- BeenVerified**

**Link :-** [**https://www.beenverified.com/**](https://www.beenverified.com/)

**Social Media & Messaging Apps**

**Check if number is registered on:**

**Tool :- Signal**

**Link :-** [**https://signal.org/**](https://signal.org/)

**Tool :--WhatsMyName**

**Link :-** [**https://github.com/WebBreacher/WhatsMyName**](https://github.com/WebBreacher/WhatsMyName)

**Tool :- Telegram API**

**Link :-** [**https://telegram.org/**](https://telegram.org/)

**· Save or screenshot profile pictures, statuses, names, and bios**

**Tool :- Webperserver**

**Link :-** [**https://www.webpreserver.com/**](https://www.webpreserver.com/)

**· Use apps like GetContact to identify crowdsourced tags and labels**

**Tool :-- GetContact**

**Link :-**  [**https://www.getcontact.com/**](https://www.getcontact.com/)

**Tool :--TrueCaller**

**Link :-** [**https://www.truecaller.com/**](https://www.truecaller.com/)

**Breached Data and Leaks**

**· Check if number appears in data breaches**

**Tool :- BreachDirectory**

**Link :-** [**https://breachdirectory.org/**](https://breachdirectory.org/)

**· Correlate number with leaked email addresses or usernames**

**Tool :- DeHashed**

**Link :-** [**https://www.dehashed.com/**](https://www.dehashed.com/)

**Call & SMS Behavior (If Access Permitted)**

**· Analyze logs for frequency, pattern, and timestamp of interactions**

**Tool :--Splunk**

**Link :-** [**https://www.splunk.com/**](https://www.splunk.com/)

**Tool :- Graylog**

**Link :-**  [**https://www.graylog.org/**](https://www.graylog.org/)

**· Determine if OTP-based fraud or impersonation has occurred**

**Tool :- Zimperium**

**Link :-** [**https://www.zimperium.com/**](https://www.zimperium.com/)

***Digital Currency (Cryptocurrency) Investigation* Checklist**

**Basic Cryptocurrency Identification**

**· Identify the type of cryptocurrency**

**Tool :--Bitcoin**

**Link :--** [**https://www.blockchain.com/explorer**](https://www.blockchain.com/explorer)

**Tool :-- Ethereum**

**Link :-**  [**https://etherscan.io/**](https://etherscan.io/)

**Tool :-- Monero**

**Link :-** [**https://moneroblocks.info/**](https://moneroblocks.info/)

**· Determine the blockchain platform**

**Tool :- ERC-20**

**Link :-**  [**https://etherscan.io/**](https://etherscan.io/)

**Tool :- BEP-20**

**Link :-** [**https://bscscan.com/**](https://bscscan.com/)

**· Note address format and length to validate legitimacy**

**Tool :- BitcoinAddressValidator**

[**Link :- https://tools.bitcoin.com/address-validator**](https://tools.bitcoin.com/address-validator)

**· Detect if address is exchange-generated, mixer/tumbler, or privacy coin**

**Tool :- WalletExplorer**

**Link :-**  [**https://www.walletexplorer.com/**](https://www.walletexplorer.com/)

**Address Ownership & Profiling**

**· Perform basic blockchain lookup**

**Tool :- Blockchair**

**Link :-** [**https://blockchair.com/**](https://blockchair.com/)

**Tool :- Etherscan**

**Link :-**  [**https://etherscan.io/**](https://etherscan.io/)

**· Check if wallet is associated with:**

**· Known exchange**

**Tool :- WalletExplorer**

**Link :-**  [**https://www.walletexplorer.com/**](https://www.walletexplorer.com/)

**· Scam or ransomware address**

**Tool :- ChainAbuse**

**Link :- https://www.chainabuse.com/**

**· Mixer or darknet market**

**Tool :- CipherTrace**

**Link :-** [**https://ciphertrace.com/**](https://ciphertrace.com/)

**· Look up address in Open Source Intelligence (OSINT) tools:**

**Tool :- WalletExplorer**

**Link :-**  [**https://www.walletexplorer.com/**](https://www.walletexplorer.com/)

**Tool :- CipherTrace**

**Link :-** [**https://ciphertrace.com**](https://ciphertrace.com/)

**Tool :- Chainalysis Reactor (if available)**

**Link :-** [**https://www.chainalysis.com/products/reacto**](https://www.chainalysis.com/products/reacto)

**· Scam alert platforms**

**Tool :- BitcoinAbuse**

**Link :-** [**https://www.bitcoinabuse.com/**](https://www.bitcoinabuse.com/)

**Tool :- Bitquery**

**Link :-** [**https://bitquery.io/**](https://bitquery.io/)

**Transaction History & Pattern Analysis**

**· Review full transaction history (incoming, outgoing, timestamps)**

**Tool :- Etherscan**

**Link :-** [**https://etherscan.io/**](https://etherscan.io/)

**· Identify transaction volume and frequency**

**Tool :- Bitquery Explorer**

**Link :-**  [**https://explorer.bitquery.io**](https://explorer.bitquery.io/)

**· Analyze transaction behavior (e.g., round numbers, small splits, common mixer patterns)**

**Tool :- Crystal Blockchain**

**Link :-** [**https://crystalblockchain.com/**](https://crystalblockchain.com/)

**· Trace flow of funds to/from known services (exchanges, marketplaces)**

**Tool :- AMLBot**

**Link :-**  [**https://amlbot.com/**](https://amlbot.com/)

**Cluster & Network Analysis**

**· Group related wallet addresses (heuristic or clustering tools)**

**Tool :- CipherTrace**

**Link :-**  [**https://ciphertrace.com/**](https://ciphertrace.com/)

**· Detect linked addresses or services by transaction patterns**

**Tool :- GraphSense**

**Link :-**  [**https://graphsense.info/**](https://graphsense.info/)

**· Map fund movements using visualizers**

**GraphSense, Bitquery, Breadcrumbs)**

**· Follow the chain of transactions (peel chains, layering, mixing)**

**Tool :- Tokenview**

**Link :-** [**https://tokenview.io/**](https://tokenview.io/)

**Exchange & Service Attribution**

**· Check if the address or transaction involves:**

**· Centralized exchanges (Binance)**

**Tool :- Binance**

**Link :-** [**https://www.binance.com/**](https://www.binance.com/)

**· P2P platforms (LocalBitcoins)**

**Tool :- LocalBitcoins**

**Link :-** [**ttps://localbitcoins.com**](https://localbitcoins.com/)

**· Review AML/KYC possibilities for identified platforms**

**Tool :- Coinfirm**

**Link :-**  [**https://www.coinfirm.com/**](https://www.coinfirm.com/)

**· Contact platform for logs, KYC info (if LEA)**

**Tool :- BitGo**

**Link :-** [**https://www.bitgo.com/**](https://www.bitgo.com/)

**Threat & Scam Association**

**Search address on:**

**· Check reports of scams, fraud, ransomware, darknet usage**

**Tool :- Elliptic**

**Link :-**  [**https://www.elliptic.co/**](https://www.elliptic.co/)

**· Search for ransom notes or phishing campaigns linking to the address**

**Tool :- HaveIBeenPwned**

**Link :-**  [**https://haveibeenpwned.com/**](https://haveibeenpwned.com/)

**De-anonymization & Identity Correlation**

**· Check for reused wallet address across forums, marketplaces**

**Tool :- CryptoSearch**

**Link :-**  [**https://www.cryptosearch.com/**](https://www.cryptosearch.com/)

**· Investigate any public exposure on Reddit, Twitter, or GitHub**

**Tool :-Reddit Search**

**Link :-**  [**https://www.reddit.com/**](https://www.reddit.com/)

**· Look for associated email, phone, or username**

**Tool :- Hunter**

**Link :-** [**https://hunter.io/**](https://hunter.io/)

**Privacy Coin Considerations**

**· Identify if the currency is privacy-focused (e.g., Monero, Dash)**

**Tool :- Monero**

**Link :-** [**https://www.getmonero.org/**](https://www.getmonero.org/)

**Tool :- Dash**

**Link :-** [**https://www.dash.org**](https://www.dash.org/)

**· Understand limitations of tracking these coins**

**Tool :- Chainalysis**

**Link :-**  [**https://www.chainalysis.com/**](https://www.chainalysis.com/)

**· Look for exchange entry/exit points or off-ramps**

**Tool :- CipherTrace**

**Link :-**  [**https://ciphertrace.com/**](https://ciphertrace.com/)

**Cross-Chain Analysis (if involved)**

**· Look into cross-chain swaps or use of DeFi services**

**Tool :- DeFiLlama**

**Link :-** [**https://defillama.com/**](https://defillama.com/)

**· Analyze synthetic or mirrored tokens (e.g., wBTC, renBTC)**

**Tool :- wBTC**

**Link :-** [**https://wbtc.network**](https://wbtc.network/)

**Tool :- renBTC**

**Link :-** [**https://renproject.io/**](https://renproject.io/)

**File Analysis Checklist**

**(*Covers: Document Files, Multimedia, APK, IPA, Windows & Mac Executables, Database Files*)**

**🔹 1. General File Identification (All File Types)**

**· Identify file type using file header (magic bytes) — not just extension**

**Tool :- Detect It Easy**

**Link :-**  [**https://ntinfo.biz/**](https://ntinfo.biz/)

**· Confirm actual file type using tools like file, TrID, or Detect It Easy (DIE)**

**Tool :- Binwalk**

**Link :-**  [**https://github.com/ReFirmLabs/binwalk**](https://github.com/ReFirmLabs/binwalk)

**· Extract hash values (MD5, SHA1, SHA256)**

**Tool :- HashCalc**

**· Analyze file metadata (creation, author, timestamps)**

**Tool :- Metadata2Go**

**Link :-**  [**https://www.metadata2go.com/**](https://www.metadata2go.com/)

**· Check digital signatures (if present) and certificate details**

**Tool :- PEStudio**

**Link :-**  [**https://www.winitor.com/**](https://www.winitor.com/)

**· Determine if the file is compressed, encrypted, or obfuscated**

**Tool :- Binwalk**

**Link :-**  [**https://github.com/ReFirmLabs/binwalk**](https://github.com/ReFirmLabs/binwalk)

**🔹 2. Document File Analysis (.docx, .xls, .ppt, .pdf, etc.)**

**Check for:**

**· Embedded macros or scripts (VBA, XLM)**

**Tool :- ViperMonkey**

**Link :-**  [**https://github.com/decalage2/ViperMonkey**](https://github.com/decalage2/ViperMonkey)

**· External references/links (web-based payloads)**

**Tool :- Oleob**

**Link :-**  [**https://github.com/decalage2/oletools/wiki/oleobj**](https://github.com/decalage2/oletools/wiki/oleobj)

**· Auto-executing elements (e.g., AutoOpen)**

**Tool :- Olevba**

**Link :-** [**https://github.com/decalage2/oletools/wiki/olevba**](https://github.com/decalage2/oletools/wiki/olevba)

**Extract and review:**

**· OLE objects**

**Tool :- OfficeMalScanner**

**Link :-** [**https://github.com/Tib3rius/OfficeMalScanner**](https://github.com/Tib3rius/OfficeMalScanner)

**· Embedded files**

**Tool :- Binwalk**

**Link :-** [**https://github.com/ReFirmLabs/binwalk**](https://github.com/ReFirmLabs/binwalk)

**· Metadata (e.g., last modified by, company)**

**Tool :- Oletools(Olemata)**

**Link :-** [**https://github.com/decalage2/oletools/wiki/olemeta**](https://github.com/decalage2/oletools/wiki/olemeta)

**Tool :- Didier Stevens Tools**

**Link :- https://github.com/DidierStevens/DidierStevensSuite**

**Tool :- Olevba**

**Link :- https://github.com/decalage2/oletools/wiki/olevba**

**🔹 3. Multimedia File Analysis (.jpg, .png, .mp4, .mp3, etc.)**

**· Validate format and integrity (ExifTool, MediaInfo)**

**Tool :- ExifTool**

**Link :- https://exiftool.org/**

**Tool :- MediaInfo**

**Link :- https://mediaarea.net/en/MediaInfo**

**· Check for steganography (e.g., using stegsolve, zsteg, steghide)**

**· Scan for:**

**· Hidden payloads or scripts (e.g., polyglot files)**

**· File manipulation (EXIF anomalies)**

**Tool :- ExifTool**

**Link :-**  [**https://exiftool.org/**](https://exiftool.org/)

**· Look for embedded malicious code or LSB encoding**

**Tool :- Oletools**

**Link :-**  [**https://github.com/decalage2/oletools**](https://github.com/decalage2/oletools)

**Review for use in phishing (e.g., QR codes in images)**

**🔹 4. Android Package (APK) File Analysis**

**· Decompile using**

**Tool :- JADX**

**Link :-**  [**https://github.com/skylot/jadx**](https://github.com/skylot/jadx)

**· Review:**

**· AndroidManifest.xml (permissions, services)**

**Tool :- Apktool**

**Link :-** [**https://github.com/iBotPeaches/Apktool**](https://github.com/iBotPeaches/Apktool)

**· Hardcoded IPs, URLs, keys, or credentials**

**Tool :- Frida**

**Link :-**[**https://www.frida.re/**](https://www.frida.re/)

**· Suspicious APIs (e.g., SMS, camera, dynamic code load)**

**Tool :- Portswigger**

**Link :-** [**https://portswigger.net/burp**](https://portswigger.net/burp)

**· Check:**

**· App signing certificate**

**Tool :- Apksigner**

**Link :-** [**https://developer.android.com/studio/command-line/apksigner**](https://developer.android.com/studio/command-line/apksigner)

**· Presence of native libraries (lib/)**

**Tool :- Apktool**

**Link :-** [**https://github.com/iBotPeaches/Apktool**](https://github.com/iBotPeaches/Apktool)

**· Broadcast receivers or background services**

**Tool :- Wireshark**

**Link :-** [**https://www.wireshark.org/**](https://www.wireshark.org/)

**· Behavior analysis (in emulator or MobSF sandbox)**

**Tool :- MobSF sandbox**

**Link :-** [**https://github.com/MobSF/Mobile-Security-Framework-MobSF**](https://github.com/MobSF/Mobile-Security-Framework-MobSF)

**🔹 5. iOS App File (IPA) Analysis**

**· Unzip and inspect the IPA file structure**

**Tool :- 7-Zip**

**Link :-**  [**https://www.7-zip.org/**](https://www.7-zip.org/)

**· Analyze:**

**o Info.plist file for app metadata**

**Tool :-OfficialAppleDeveloperDocumentation(.plist)**

**Link :-**[**https://developer.apple.com/documentation/foundation/formatting\_plist\_data**](https://developer.apple.com/documentation/foundation/formatting_plist_data)

**o Embedded provisioning profiles or certificates**

**Tool :-** [**ldid**](https://github.com/xerub/ldid)

[**https://github.com/xerub/ldid**](https://github.com/xerub/ldid)

**o Binary with tools like class-dump, otool, strings**

**Tool :- class-dump**

**Link :-** [**https://github.com/nygard/class-dump**](https://github.com/nygard/class-dump)

**· Scan for**

**o Jailbreak detection**

**o Obfuscation, anti-analysis techniques**

**o Network connections or dynamic code execution**

**Tools for all three(MobSF, objection)**

**Tool :- MobSF**

**Link :-**[**https://github.com/MobSF/Mobile-Security-Framework-MobSF**](https://github.com/MobSF/Mobile-Security-Framework-MobSF)

**Tool :- Objection**

**Link :-** [**https://github.com/sensepost/objection**](https://github.com/sensepost/objection)

**· Optional: Use Frida, Objection for dynamic analysis**

**Tool :- Frida**

**Link :-** [**https://frida.re/**](https://frida.re/)

**🔹 6. Windows Executable Analysis (.exe, .dll, .scr, etc.)**

**Check:**

**PE headers and sections**

**Tool :- PIEDS**

**Link :-** [**https://pieds-bitspilani.org/**](https://pieds-bitspilani.org/)

**Packers (UPX, Themida, etc.)**

**Tool :- UPX**

**Link :-**[**https://upx.github.io/**](https://upx.github.io/)

**Tool :- Themida**

**Link :-** [**https://www.oreans.com/Themida.php**](https://www.oreans.com/Themida.php)

**Tools:**

**PEStudio, CFF Explorer, Detect It Easy, Exeinfo PE**

**Sandbox test (Any.Run)**

**Tool :- Any.Run**

**Link :-** [**https://any.run/**](https://any.run/)

**Analyze behavior:**

**File, registry, network changes**

**Tool :- OSSEC**

**Link :-** [**https://www.ossec.net/**](https://www.ossec.net/)

**Persistence mechanisms (scheduled tasks, registry keys)**

[**Tool :- Wireshark**](https://www.wireshark.org/)

**Link :-** [**https://www.wireshark.org/**](https://www.wireshark.org/)

**🔹 7. Mac Executables (.dmg, .pkg, .app, Mach-O)**

**Validate Mach-O binary format**

**Use tools:**

**Tool :- otool**

**Tool :- codesign**

**Tool :- class-dump**

**Link :-**[**https://developer.apple.com/xcode/**](https://developer.apple.com/xcode/)

[**Link :-https://developer.apple.com/documentation/security/notarizing\_macos\_software\_before\_distribution/customizing\_the\_notarization\_workflow**](https://developer.apple.com/documentation/security/notarizing_macos_software_before_distribution/customizing_the_notarization_workflow)

**Link :-** [**https://github.com/nygard/class-dump**](https://github.com/nygard/class-dump)

**Inspect:**

**· Code signatures and entitlements**

**Tool :-AppleEntitlementsReference(entitlements.plist)**

[**https://opensource.apple.com/source/libsecurity\_codesigning/libsecurity\_codesigning-36860/lib/entitlements.plist.auto.html**](https://opensource.apple.com/source/libsecurity_codesigning/libsecurity_codesigning-36860/lib/entitlements.plist.auto.html)

**· Analyze dynamic behavior (on isolated macOS VM or with Frida)** [**Tool :- Virtual Box**](https://www.virtualbox.org/)

**Link :-** [**https://www.virtualbox.org/**](https://www.virtualbox.org/)

**🔹 8. Database Files (.db, .sqlite, .mdb, .accdb, etc.)**

**Look for:**

**o Embedded scripts or queries**

**Tool :- DB Browser for SQLite**

**Link :-** [**https://sqlitebrowser.org/**](https://sqlitebrowser.org/)

**o Links to external resources**

**Tool :- Microsoft(Strings)**

**Link :-**[**https://learn.microsoft.com/en-us/sysinternals/downloads/strings**](https://learn.microsoft.com/en-us/sysinternals/downloads/strings)

**o Hidden tables or malicious triggers**

**Tool :- SQL suspect**

**Link :-** [**https://www.sqlsuspect.com/**](https://www.sqlsuspect.com/)

**· Dump and analyze contents for:**

**o Credential storage**

**Tool :- FTkImager**

**Link :-**[**https://apps.microsoft.com/store/detail/hex-editor-neo/9NBLGGH42THS**](https://apps.microsoft.com/store/detail/hex-editor-neo/9NBLGGH42THS)

**o Keylogging or C2 data exfiltration**

**Tool :- Microsoft(Strings)**

**Link :-**[**https://docs.microsoft.com/en-us/sysinternals/downloads/strings**](https://docs.microsoft.com/en-us/sysinternals/downloads/strings)

**o Metadata manipulation**

**Tool :- Exiftool**

**Link :-** [**https://exiftool.org/**](https://exiftool.org/)

**🔹 9. Network or Dynamic Behavior (if applicable)**

**· Observe:**

**· DNS requests**

**Tool :- Wireshark**

**Link :-** [**https://www.wireshark.org/**](https://www.wireshark.org/)

**· HTTP/HTTPS or FTP calls**

**Tool :- Tcpdump**

**Link :-** [**https://www.tcpdump.org/**](https://www.tcpdump.org/)

**· Analyze with:**

**Tool :- Wireshark**

**Link :-** [**https://www.wireshark.org/**](https://www.wireshark.org/)

**Tool :-Procmon**

**Link :-**[**https://learn.microsoft.com/en-us/sysinternals/downloads/procmon**](https://learn.microsoft.com/en-us/sysinternals/downloads/procmon)

**Tool :- Sysmon**

**Link :-** [**https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon**](https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon)

**· Look for dropped files, registry keys, or process injection**

**Tool :- Volatility Foundation**

**Link :-** [**https://www.volatilityfoundation.org/**](https://www.volatilityfoundation.org/)

**🔹 10. Threat Intelligence & Reporting**

**· Submit hash to:**

**Tool :-VirusTotal**

**Link :-**  [**https://www.virustotal.com/**](https://www.virustotal.com/)

**Tool :- Hybrid Analysis**

**Link :-**  [**https://www.hybrid-analysis.com/**](https://www.hybrid-analysis.com/)

**Tool :-ThreatFoxorMalShare**

**Link :-** [**https://github.com/Neo23x0/ThreatFox**](https://github.com/Neo23x0/ThreatFox)

**· Correlate behavior with known malware families or campaigns**

**Tool :- Cuckoosandbox**

**Link :-** [**https://cuckoosandbox.org/**](https://cuckoosandbox.org/)

**· Extract IOCs: IPs, domains, hashes, file paths, registry keys**

**Tool :- Fortify-IOC-Parser**

**Link :-** [**https://github.com/welchesd/Fortify-IOC-Parser**](https://github.com/welchesd/Fortify-IOC-Parser)

**· Document findings with screenshots and technical summaries**

**Tool :- Maltego**

**Link :-** [**https://www.maltego.com/**](https://www.maltego.com/)

**Device Investigation Checklist**

**🔹 1. Windows Devices**

**Acquire forensic image Tools (FTK Imager, Magnet ACQUIRE)**

**Tool :- FTK Imager**

**Link :-** [**https://accessdata.com/product-download/ftk-imager-version-4-7-1**](https://accessdata.com/product-download/ftk-imager-version-4-7-1)

**Tool :- Magnet ACQUIRE**

**Link :-** [**https://www.magnetforensics.com/products/magnet-acquire/**](https://www.magnetforensics.com/products/magnet-acquire/)

**Examine:**

**Tool :- Windows event logs (Application, Security, System)**

**Link :-**[**https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event- viewer**](https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-%20viewer)

**Registry Tools (e.g., Run Keys, USB history, network settings)**

**Tool :- RegRipper**

**Link :-** [**https://github.com/keydet89/RegRipper**](https://github.com/keydet89/RegRipper)

**Installed applications, startup items**

**Tool :- Microsoft**

**Link :-**[**https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns**](https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns)

**User activity: browser history, downloads, MRU**

**Tool :- Evidor**

**Link :-** [**https://github.com/SwiftOnSecurity/Evidor**](https://github.com/SwiftOnSecurity/Evidor)

**Analyze:**

**· Pagefile.sys and hiberfil.sys**

**Tool :- Sleuth Kit**

**Link :-** [**https://www.sleuthkit.org/**](https://www.sleuthkit.org/)

**· Security artifacts (AV logs, firewall)**

**Tool :- Microsoft**

**Link :-**[**https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-viewer**](https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-viewer)

**· Check for malware, persistence mechanisms, encrypted volumes**

**Tool :- Raptor**

**Link :-** [**https://github.com/rsmudge/raptor**](https://github.com/rsmudge/raptor)

**· Review attached devices, mounted shares**

**Tool :- Wireshark**

**Link :-** [**https://www.wireshark.org/**](https://www.wireshark.org/)

**2. macOS Devices**

**Acquire image using dd, Autopsy, or MacQuisition**

**· Collect live memory (if accessible)**

[**Tool :- Volatility Foundation**](https://www.volatilityfoundation.org/)

**Link :-** [**https://www.volatilityfoundation.org/**](https://www.volatilityfoundation.org/)

**· Analyze:**

**· System logs (/var/log/, unified logs)**

**Tool :- Logtail**

**Link :-** [**https://github.com/StefanKert/Logtail**](https://github.com/StefanKert/Logtail)

**· Plist files for app config and persistence**

**Tool :- plisteditorn**

**Link :-** [**https://www.plisteditorn.com/**](https://www.plisteditorn.com/)

**· LaunchAgents, LaunchDaemons, Login Items**

**Tool :- Etrecheck**

**Link :-** [**https://www.etrecheck.com/**](https://www.etrecheck.com/)

**· Examine:**

**· Spotlight, Quarantine logs**

**Tool :- Logkext**

**Link :-** [**https://github.com/stevenmichaeldavis/logkext**](https://github.com/stevenmichaeldavis/logkext)

**· Safari/Chrome browsing history**

**Tool :- ChromeForensics**

**Link :-** [**https://github.com/MooseDojo/ChromeForensics**](https://github.com/MooseDojo/ChromeForensics)

**· TCC.db for privacy and access control settings**

**Tool :- tcc-tools  
Link :-** [**https://github.com/micahflee/tcc-tools**](https://github.com/micahflee/tcc-tools)

**· Review Time Machine backups, APFS snapshots, and Disk Images**

**Tool :- GAM  
Link :-** [**https://github.com/jay0lee/GAM**](https://github.com/jay0lee/GAM)

**🔹 3. iOS Devices (iPhone/iPad)**

**Perform logical or full file system extraction (via Cellebrite, GrayKey, Elcomsoft)**

**· Collect:**

**· Messages (iMessage, SMS)**

**Tool :- iMazing**

**Link :-** [**https://imazing.com/**](https://imazing.com/)

**· Call logs, contacts, photos**

**Tools:- X1 Social Discovery**

**· Safari history, app usage logs**

**Tool :- iMazing**

**Link :-** [**https://imazing.com/**](https://imazing.com/)

**· Analyze:**

**· Installed apps and permissions**

**Tool :- Mobileverify  
Link :-** [**https://www.mobileverify.com/**](https://www.mobileverify.com/)

**· Location history (GPS logs, Apple Maps cache)**

**Tool :- iMazing**

**Link :-** [**https://imazing.com/**](https://imazing.com/)

**· iCloud synchronization artifacts**

**Tools:- ElcomSoft iOS Forensic Toolkit**

**· Investigate:**

**· Jailbreak indicators**

**Tool :- Checkra  
Link :-** [**https://checkra.in/**](https://checkra.in/)

**· Backup files or encrypted containers**

**Tools:- Cellebrite UFED**

**· Security and biometrics settings**

**Tool :-MVT**

**Link :-** [**https://github.com/mvt-project/mvt**](https://github.com/mvt-project/mvt)

**🔹 4. Android Devices**

**Acquire using ADB, Magnet AXIOM, Cellebrite UFED**

**Extract:**

**· SMS, call logs, contacts**

**Tools:- Autopsy**

**Link :-** [**https://www.autopsy.com/**](https://www.autopsy.com/)

**· WhatsApp, Telegram, Signal data (with root/access)**

**Tool :-MobSF**

**Link :-** [**https://github.com/mobsf/mobsf**](https://github.com/mobsf/mobsf)

**· App list, usage stats**

**Tool :- MobSF**

**Link :-** [**https://github.com/mobsf/mobsf**](https://github.com/mobsf/mobsf)

**· System logs (logcat, dmesg)**

**Tool :- LogCat**

**Link :-** [**https://developer.android.com/studio/command-line/logcat**](https://developer.android.com/studio/command-line/logcat)

**🔹 5. Removable Devices (USB, SD cards, External HDDs)**

**Create sector-level image (write-blocked mode)**

**Extract:**

**· File system structure and metadata**

**Tool :- Sleuth Kit**

**Link :-** [**https://www.sleuthkit.org/**](https://www.sleuthkit.org/)

**· Deleted files (recover with PhotoRec, Autopsy)**

**Tool :- R-studio**

**Link :-** [**https://www.r-studio.com/**](https://www.r-studio.com/)

**· LNK files, timestamps (creation/accessed)**

**Tool :- Sleuth Kit**

**Link :-** [**https://www.sleuthkit.org/**](https://www.sleuthkit.org/)

**Analyze:**

**· Hidden partitions or volumes**

**Tool :- DiskGenius  
Link :-** [**https://www.diskgenius.com/**](https://www.diskgenius.com/)

**· Embedded malware or scripts**

**Tool :- MiniTool  
Link :-** [**https://www.minitool.com/**](https://www.minitool.com/)

**· Encrypted containers Tools:- (e.g., VeraCrypt, BitLocker To Go)**

**🔹 6. IoT Devices (CCTV, Smart Speakers, Routers, etc.)**

**Analyze:**

**· Log files (if accessible)**

**Tool :- Microsoft**

**Link :-**[**https://www.microsoft.com/en-us/download/details.aspx?id=24659**](https://www.microsoft.com/en-us/download/details.aspx?id=24659)

**· Default credentials or open ports**

**Tool :- Nmap**

**Link :-** [**https://nmap.org/**](https://nmap.org/)

**· Configuration files (network, DNS, cloud services)**

**Tool :- CSPM Cloudsploit  
Link :-** [**https://cloudsploit.com/**](https://cloudsploit.com/)

**Investigate:**

**· Data exfiltration or command relays**

**Tool :- Zeek**

**Link :-** [**https://zeek.org/**](https://zeek.org/)

**· Evidence of botnet or malware infections**

**Tool :- Cuckoosandbox  
Link :-** [**https://cuckoosandbox.org/**](https://cuckoosandbox.org/)

**· Linked mobile apps or cloud accounts**

**Tool :- MobSF**

**Link :-**[**https://github.com/MobSF/Mobile-Security-Framework-MobSF**](https://github.com/MobSF/Mobile-Security-Framework-MobSF)

**🔹 7. Wireless Devices & Access Points**

**Identify connected wireless devices (using Wireshark, Kismet)**

**Tool :- Kismet**

**Link :-** [**https://www.kismetwireless.net/**](https://www.kismetwireless.net/)

**Extract:**

**· SSID, MAC, encryption type**

**Tool :- Kismet**

**Link :-** [**https://www.kismetwireless.net/**](https://www.kismetwireless.net/)

**· DHCP leases and logs**

**Tool :- Tcpdump**

**Link :-** [**https://www.tcpdump.org/**](https://www.tcpdump.org/)

**· ARP/NAT tables**

**Tool :- Nmap**

**Link :-** [**https://nmap.org/**](https://nmap.org/)

**Analyze:**

**· Admin panel logs (login attempts, config changes)**

**Tool :- Splunk**

**Link :-** [**https://www.splunk.com/**](https://www.splunk.com/)

**· Wi-Fi probe requests and beacon frames**

**Tool :- Aircrack  
Link :-** [**https://www.aircrack-ng.org/**](https://www.aircrack-ng.org/)

**· Possible rogue AP or Evil Twin activity**

**Tool :- RogueAP-Detector**

**Link :-** [**https://github.com/anotherik/RogueAP-Detector**](https://github.com/anotherik/RogueAP-Detector)

**🔹 8. Cross-Device Correlation**

**· Correlate:**

**· MAC addresses**

**Tool :- Kismet**

**Link :-** [**https://www.kismetwireless.net/**](https://www.kismetwireless.net/)

**· Timestamps**

**Tool :- Sleuth Kit**

**Link :-** [**https://www.sleuthkit.org/autopsy/**](https://www.sleuthkit.org/autopsy/)

**· Credentials and session cookies**

**Tool :- Keychain Access**

**Link :-** [**https://support.apple.com/guide/keychain-access/welcome/mac**](https://support.apple.com/guide/keychain-access/welcome/mac)

**· Location or geotagged data**

**Tool :- ExifTool**

**Link :-** [**https://exiftool.org/**](https://exiftool.org/)

**· Identify common cloud accounts, synced data, or shared devices**

**Tool :- Magnet AXIOM  
Link :-** [**https://www.magnetforensics.com/products/magnet-axiom/cloud/**](https://www.magnetforensics.com/products/magnet-axiom/cloud/)

**🔹 9. Reporting & Evidence Handling**

**· Hash and validate all acquired images**

**Tool :- Nirsoft  
Link :-** [**https://www.nirsoft.net/utils/hash\_my\_files.html**](https://www.nirsoft.net/utils/hash_my_files.html)

**· Maintain chain of custody**

**Tool :- CaseGuard**

**Link :-** [**https://caseguard.com/**](https://caseguard.com/)

**· Document:**

**· Device info, serial numbers, OS version**

**Tool :- Belarc  
Link :-** [**https://www.belarc.com/products\_belarc\_advisor**](https://www.belarc.com/products_belarc_advisor)

**· User accounts and roles**

**Tool :- IOC Bucket  
Link :-** [**https://iocbucket.com/**](https://iocbucket.com/)

**· Extracted artifacts and IOCs**

**Tool :- Volatility Foundation  
Link :-** [**https://www.volatilityfoundation.org/**](https://www.volatilityfoundation.org/)

**· Preserve volatile data (if applicable) and encrypt reports securely**

**Tool :- AxCrypt**

**Link :-** [**https://www.axcrypt.net/**](https://www.axcrypt.net/)

**Social Media Investigation**

**Facebook**

**Account Identification: Collect the target account name, email address, phone number, profile URL.**

**Tool :- WhatsMyName**

**Link :-**  [**https://whatsmyname.app/**](https://whatsmyname.app/)

**Profile Review: Check public profile details (location, bio, posts, photos).**

**Tool :- Maltego  
Link :-**  [**https://www.maltego.com/**](https://www.maltego.com/)

**Timeline Analysis: Review posts, comments, photos, and videos shared by the user.**

**Tool :- Hunchly**

**Link :-** [**https://www.hunch.ly/**](https://www.hunch.ly/)

**Messages: Investigate private messages (inbox and archived), including group messages.**

**Tool :- Cellebrite**

**Link :-**  [**https://www.cellebrite.com/**](https://www.cellebrite.com/)

**Friends & Connections: Analyze the user's friend list and interactions.**

**Tool :- Maltego**

**Link :-**  [**https://www.maltego.com/**](https://www.maltego.com/)

**Event Participation: Investigate events the user is invited to or attending.**

**Tool :- Social Links Pro**

**Link :-**  [**https://www.sociallinks.io/**](https://www.sociallinks.io/)

**Geotagging & Check-ins: Extract geotagged data from posts and check-ins.**

**Tool :- ExifTool**

**Link :-**   [**https://exiftool.org/**](https://exiftool.org/)

**Third-party Apps: Review any linked third-party applications and permissions.**

**Tool :-MobSF**  [**Link :-https://github.com/MobSF/Mobile-Security-Framework-MobSF**](https://github.com/MobSF/Mobile-Security-Framework-MobSF)

**IP & Device Logs: Collect IP addresses and device logs to trace login activity.**

**Tool :- Takeout  
Link :-**  [**https://takeout.google.com/**](https://takeout.google.com/)

**Deleted Content: Investigate any deleted posts, comments, or messages (via cached versions or third-party tools). NetClean Analyze netclean.com**

**Instagram**

**Account Details: Retrieve username, email, bio, followers/following count.**

**Tool :- Maigret  
Link :-**  [**https://github.com/soxoj/maigret**](https://github.com/soxoj/maigret)

**Profile Review: Analyze posts (photos, captions, hashtags) and stories.**

**Tool :- Maltego**

**Link :-**  [**https://www.maltego.com/**](https://www.maltego.com/)

**Messages (DMs): Review direct messages (including group chats).**

**Tool :- Elcomsoft  
Link :-**  [**https://www.elcomsoft.com/**](https://www.elcomsoft.com/)

**Followers & Interactions: Look into followers and who the target interacts with.**

**Tool :- Phantombuster**

**Link :-** [**https://phantombuster.com/**](https://phantombuster.com/)

**Hashtags & Mentions: Analyze hashtags and tagged photos in the user’s feed.**

**Tool :- Hashtagify**

**Link :-** [**https://hashtagify.me/**](https://hashtagify.me/)

**Location Tags: Examine posts with geotagging (locations and timestamps).**

**Tool :- ExifTool**

**Link :-**  [**https://exiftool.org/**](https://exiftool.org/)

**Third-Party Apps: Review connected apps and granted permissions.**

**Tool :-MobSF**  [**Link :-https://github.com/MobSF/Mobile-Security-Framework-MobSF**](https://github.com/MobSF/Mobile-Security-Framework-MobSF)

**Deleted Posts: Search for removed posts using cached data or third-party tools.**

**Tool :- Archive.today**

**Link :-**  [**https://archive.today/**](https://archive.today/)

**Security & Login History: Review login history and security settings (two-factor authentication, device logins).**

**Tool :- Cellebrite  
Link :-**  [**https://www.cellebrite.com/**](https://www.cellebrite.com/)

**Twitter (X)**

**Account Overview: Collect username, display name, bio, email (if available).**

**Tool :- Tinfoleak   
Link :-**  [**https://github.com/vaguileradiaz/tinfoleak**](https://github.com/vaguileradiaz/tinfoleak)

**Tweets & Retweets: Review recent tweets, retweets, and replies.**

**Tool :- TweetBeaver**

**Link :-**  [**https://tweetbeaver.com/**](https://tweetbeaver.com/)

**Followers & Following: Investigate follower/following list and their interactions.**

**Tool :- Twint**

**Link :-**  [**https://github.com/twintproject/twint**](https://github.com/twintproject/twint)

**Private Messages: Investigate direct messages (including media shared).**

**Tool :- Magnet AXIOM**

**Link :-**  [**https://www.magnetforensics.com/**](https://www.magnetforensics.com/)

**Hashtags & Mentions: Review any hashtags and mentions related to the user.**

**Tool :- Hashtagify**

**Link :-**  [**https://hashtagify.me/**](https://hashtagify.me/)

**Geo-Tagged Tweets: Analyze geolocation data from tweets with location tags.**

**Tool :- GeoSocial**

**Link :-** [***https://www.geosocialfootprint.com/***](https://www.geosocialfootprint.com/)

**Suspicious Activity: Look for bot-like activity (e.g., automated tweets, unusual engagement).**

**Tool :- Tinfoleak**

**Link :-**  [**https://github.com/vaguileradiaz/tinfoleak**](https://github.com/vaguileradiaz/tinfoleak)

**Deleted Content: Search for deleted tweets through third-party tools (e.g., Wayback Machine).**

**Tool :- Archive.today**

**Link :-**  [**https://archive.today/**](https://archive.today/)

**Login & Device Logs: Gather device and IP information (using advanced tools or platform APIs).**

**Tool :- Oxygen Forensics  
Link :-** [**https://www.oxygen-forensic.com/**](https://www.oxygen-forensic.com/)

**LinkedIn**

**Profile Review: Collect account details such as job title, company, connections, skills, and endorsements.**

**Tool :- Phantombuster**

**Link :-**  [**https://phantombuster.com/**](https://phantombuster.com/)

**Activity Feed: Investigate recent activity, including posts, shared content, comments, and articles.**

**Tool :- CrowdTangle**

**Link :-**  [**https://www.crowdtangle.com/**](https://www.crowdtangle.com/)

**Connections & Recommendations: Review connections and recommendations from others.**

**Tool :- Phantombuster**

**Link :-**  [**https://phantombuster.com/**](https://phantombuster.com/)

**Private Messages: Analyze LinkedIn messages and any attachments.**

**Tool :- Oxygen Forensic Detective**

**Link :-**  [**https://www.oxygen-forensic.com/**](https://www.oxygen-forensic.com/)

**Groups & Interests: Investigate groups the user is a part of and professional affiliations.**

**Tool :- Phantombuster**

**Link :-** [**https://phantombuster.com/**](https://phantombuster.com/)

**Location Tags: Review work history or events that have geolocation information.**

**Tool :- ExifTool**

**Link :-**  [**https://exiftool.org/**](https://exiftool.org/)

**Shared Media: Analyze shared articles, videos, and documents for metadata.**

**Tool :- LinkedIn Settings**

**Link :-** [**https://www.linkedin.com/settings**](https://www.linkedin.com/settings)

**Account & Device Logs: Review account security settings, login history, and device logs.**

**Tool :- Cellebrite**

**Link :-** [**https://www.cellebrite.com/**](https://www.cellebrite.com/)

**Snapchat**

**Account Information: Retrieve username, display name, associated email/phone number.**

**Tool :- PhoneInfoga**

**Link :-**  [**https://github.com/PhoneInfoga/PhoneInfoga**](https://github.com/PhoneInfoga/PhoneInfoga)

**Snaps & Stories: Investigate shared photos, videos, and ephemeral stories.**

**Tool :- ExifTool**

**Link :-**  [**https://exiftool.org/**](https://exiftool.org/)

**Chats & Group Messages: Review chats, including temporary messages.**

**Tool :- Magnet AXIOM**

**Link :-**  [**https://www.magnetforensics.com/**](https://www.magnetforensics.com/)

**Friends & Interactions: Look at friends list, and analyze interactions through direct messages and shared snaps.**

**Tool :- Social Links**

**Link :-** [**https://www.sociallinks.io/**](https://www.sociallinks.io/)

**Snap Map: Extract geolocation data from Snaps and Stories shared via Snap Map.**

**Tool :- Creepy**

**Link :-**  [**https://github.com/ilektrojohn/creepy**](https://github.com/ilektrojohn/creepy)

**Memory Content: Analyze saved Snaps (in Memories) for metadata.**

**Tool :- PhoneRescue**

**Link :-**  [**https://www.iphone-data-recovery.com/**](https://www.iphone-data-recovery.com/)

**Security Settings: Check for two-factor authentication, linked apps, and privacy settings.**

**Tool :- iMazing**

**Link :-**  [**https://imazing.com/**](https://imazing.com/)

**Deleted Snaps: Use forensic tools to recover deleted snaps if applicable.**

**Tool :- Cellebrite**

**Link :-**  [**https://www.cellebrite.com/**](https://www.cellebrite.com/)

**WhatsApp**

**Account Overview: Retrieve phone number, profile name, and status.**

**Tool :-WhatsAppWebScraper**  [**Link :-https://github.com/whatsappruby/whatsapp-web-scraper**](https://github.com/whatsappruby/whatsapp-web-scraper)

**Chats: Analyze individual and group chat messages (including timestamps, text, media).**

**Tool :- iMazing**

[**Link :- https://imazing.com/**](https://imazing.com/)

**Media Files: Investigate shared media (images, videos, documents) for metadata.**

**Tool :- ForensicExplorer**

**Link :-** [**https://www.forensicexplorer.com/**](https://www.forensicexplorer.com/)

**Group Involvement: Review group chats the user is involved in.**

**Tool :- Cellebrite  
Link :-** [**https://www.cellebrite.com/**](https://www.cellebrite.com/)

**Call Logs: Check for call records (voice, video), including durations and timestamps.**

**Tool :- iMazing**

**Link :-**  [**https://imazing.com/**](https://imazing.com/)

**Backup Data: Retrieve WhatsApp backups (local/cloud) if available.**

**Tool :- Oxyzen Forensics**

**Link :-** [**https://www.oxygen-forensic.com/**](https://www.oxygen-forensic.com/)

**Security Settings: Check encryption, two-factor authentication, and linked devices.**

**Tool :- Whatsapp BackUp Extractor**

**Link :-** [**https://whatsapp-backup-extractor.com/**](https://whatsapp-backup-extractor.com/)

**Deleted Messages: Investigate deleted messages or media (recovered from backups or forensic tools**

**Tool :- Cellebrite**

**Link :-**  [**https://www.cellebrite.com/**](https://www.cellebrite.com/)**).**

**IP Logs: Investigate connection logs from the IP addresses used for login.**

**Tool :- Magnet Forensics**

**Link :-** [**https://www.magnetforensics.com/**](https://www.magnetforensics.com/)

**Telegram**

**Account Details: Retrieve username, phone number, associated contacts.**

**Tool :- PhoneInfoga**

**Link :-** [**https://github.com/PhoneInfoga/PhoneInfoga**](https://github.com/PhoneInfoga/PhoneInfoga)

**Chats: Investigate all personal and group chats, including private and public channels.**

**Tool :- Oxygen Forensics**

**Link :-** [**https://www.oxygen-forensic.com/**](https://www.oxygen-forensic.com/)

**Media Files: Review shared media files and investigate timestamps, geolocation (if available).**

**Tool :- Maltego**

**Link :-** [**https://www.maltego.com/**](https://www.maltego.com/)

**Group & Channel Activity: Review the user’s involvement in any groups or public channels.**

**Tool :- PhantomBuster**

**Link :-**  [**https://phantombuster.com/**](https://phantombuster.com/)

**Bots: Investigate any bots the user is interacting with (if applicable).**

**Tool :- Maltego**

**Link :-** [**https://www.maltego.com/**](https://www.maltego.com/)

**Backup & Cloud: Access Telegram’s cloud backup for data recovery (if possible).**

**Tool :- iMazing**

**Link :-** [**https://imazing.com/**](https://imazing.com/)

**Deleted Messages: Recover deleted messages or media using forensic tools or backups.**

**Tool :- Oxygen Forensics**

**Link :-** [**https://www.oxygen-forensic.com/**](https://www.oxygen-forensic.com/)

**IP & Device Logs: Gather login details, device information, and IP address records.**

**Tool :- Magnet Forensics**

**Link :-** [**https://www.magnetforensics.com/**](https://www.magnetforensics.com/)

**iMessage**

**Account Info: Retrieve associated Apple ID, phone number, email.**

**Tool :- PhoneInfoga**

**Link :-**  [**https://github.com/PhoneInfoga/PhoneInfoga**](https://github.com/PhoneInfoga/PhoneInfoga)

**Message Review: Analyze message history (SMS, iMessages, multimedia).**

**Tool :- iMazing**

**Link :-**  [**https://imazing.com/**](https://imazing.com/)

**Group Chats: Investigate group chats and shared media.**

**Tool :- X1 Social Discovery**

**Link :-**  [**https://www.x1.com/**](https://www.x1.com/)

**iCloud Sync: Check for synchronization with iCloud (if accessible).**

**Tool :- Elcomsoft iOS Forensic Toolkit**

**Link :-**  [**https://www.elcomsoft.com/**](https://www.elcomsoft.com/)

**Media & Attachments: Examine shared images, videos, and other file types for metadata.**

**Tool :- Forensic Explorer**

**Link :-**  [**https://www.forensicexplorer.com/**](https://www.forensicexplorer.com/)

**Deleted Messages: Investigate any deleted iMessages (via backups or forensic tools).**

**Tool :- iMazing**

**Link :-**  [**https://imazing.com/**](https://imazing.com/)

**iCloud Backup: Check for available backups on iCloud, including encrypted message data.**

**Tool :- Elcomsoft iOS Forensic Toolkit**

**Link :-** [**https://www.elcomsoft.com/**](https://www.elcomsoft.com/)

**Signal**

**Account Information: Retrieve associated phone number, display name, and profile information.**

**Tool :- Signal Export Tool**

**Link :-**  [**https://signal.org/**](https://signal.org/)

**Message History: Review individual and group chat messages, including media shared.**

**Tool :- Oxygen Forensic Detective**

**Link :-**  [**https://www.oxygen-forensic.com/**](https://www.oxygen-forensic.com/)

**Media Files: Investigate shared media (photos, videos, audio messages) for metadata.**

**Tool :- Forensic Explorer**

**Link :-**  [**https://www.forensicexplorer.com/**](https://www.forensicexplorer.com/)

**Encryption & Security: Analyze encryption settings and any possible weak points.**

**Tool :- Wireshark**

**Link :-**  [**https://www.wireshark.org/**](https://www.wireshark.org/)

**Backup Data: Check for any local backups of Signal messages or media.**

**Tool :- iMazing**

**Link :-**  [**https://imazing.com/**](https://imazing.com/)

**Deleted Content: Investigate deleted messages using forensic tools if available.**

**Tool :- X1 Social Discovery**

**Link :-**  [**https://www.x1.com/**](https://www.x1.com/)

**Call Logs: Check for call logs (audio and video) with timestamps.**

**Tool :- Cellebrite**

**Link :-**  [**https://www.cellebrite.com/**](https://www.cellebrite.com/)