TM

TrustedMARC

DMARC Report Parser — User Manual

Version 2.0 · trustedmarc.co.uk

This manual covers installation, activation, operation, and troubleshooting of TrustedMARC on macOS and Windows. It is intended for IT administrators, security analysts, MSPs, and anyone responsible for monitoring email authentication for their domain.

1. Overview

1.1 Background

Mail providers — including Google, Microsoft, Amazon SES, Zoho, and Yahoo — send automated DMARC aggregate reports to domain owners every day. These reports arrive as compressed XML attachments (.zip or .gz) and contain detailed records of every email observed claiming to originate from the monitored domain, along with the authentication results applied to each message.

Without dedicated tooling, these reports are effectively unreadable. They accumulate in an inbox as cryptic attachments that most recipients never open. This tool processes an entire folder of reports in a single operation and transforms the data into an actionable HTML dashboard.

1.2 What the tool does

TrustedMARC is distributed as a single self-contained desktop application (trustedmarc.py, packaged as TrustedMARC.app on macOS and TrustedMARC.exe on Windows). It provides a graphical interface for selecting report folders, configuring options, and running the parser — no command line required.

The parser performs the following operations on each report batch:

- **Parsing.** Unpacks .zip, .gz, and .xml files, reads the XML, and extracts all authentication records including source IP, message count, SPF result, DKIM result, and disposition.
- **Alignment checking.** Evaluates SPF and DKIM alignment properly under both relaxed and strict modes — checking whether the authenticated domain matches the visible From header, which is the actual DMARC requirement.
- **Multi-domain support.** Processes report files covering multiple domains in a single run. When no domain filter is set, the tool identifies and reports on every domain found across all report files simultaneously. A domain tab selector in the IP Detail tab allows switching between domains. This means a single folder of reports can reveal authentication data for every domain your organisation sends from.
- **Sender identification.** Matches each IP address against a database of known sending services (Google Workspace, SendGrid, Amazon SES, Microsoft 365, Mailchimp, Zoho, and over 30 others) using geolocation and reverse DNS data.
- **Geolocation.** Queries ip-api.com to determine the country, city, and ISP for each sending IP. Batched to 100 IPs per request with rate limiting. No API key required.
- **Reverse DNS.** Resolves each IP to a hostname where available, which helps confirm whether traffic is coming from a known service's infrastructure.
- **DNS record retrieval.** Fetches the live SPF and DMARC TXT records for the monitored domain via Google's public DNS API, so the report reflects the current state of the domain's configuration.
- **Suspicious IP flagging.** Automatically marks IPs meeting defined criteria: high failure rate (>50%), total failure (100% fail, >10 messages), single-day spike (one date, >100 messages), and multi-domain sending (>3 domains).
- **Recommendations.** Generates prioritised, actionable recommendations covering policy level, failing known senders, alignment rates, SPF record health, and missing records.

> *Nothing is transmitted externally except IP addresses for geolocation lookup (ip-api.com) and DNS queries (dns.google). All processing and report generation occurs locally on the machine running*

the script.

1.3 Output

The tool produces a single self-contained HTML file. No server or internet connection is required to view it. The report contains the following sections:

- An executive summary paragraph with a plain-English verdict and key statistics.
- Eight summary stat cards covering total messages, pass/fail counts, alignment counts, unique IPs, identified senders, and suspicious IP count.
- Six charts: DMARC pass/fail donut, SPF alignment donut, DKIM alignment donut, reporting organisations bar, message timeline (stacked bar, pass vs fail per day), and top sending IPs by volume.
- **Senders tab.** IPs grouped by identified sending service. Each sender shows total message count, pass rate, IP count, and category. Clicking a sender expands to show individual IPs with counts, pass/fail, location, and flags.
- **IP Detail tab.** Full sortable, filterable table of every sending IP. Clicking any row expands a drilldown panel showing identity, network, authentication detail, and a per-IP activity timeline chart.
- **Health & Actions tab.** Policy journey indicator, live DNS records for the domain, and a prioritised recommendation list.
- CSV export of all IP data including geolocation, accessible via a button in the report header.
- Print stylesheet for clean PDF generation via the browser print function.

2. Getting Started

TrustedMARC is delivered as a self-contained desktop application. No Python installation, no terminal, and no additional software is required. Simply download the application for your platform and double-click to launch.

2.1 macOS — TrustedMARC.app

1. Download TrustedMARC-Mac.zip from trustedmarc.co.uk and unzip it.
2. Move TrustedMARC.app to your Applications folder, or run it from any location.
3. **First launch — Gatekeeper warning.** macOS may display a security warning because the application is not signed with an Apple Developer certificate. Right-click (or Control-click) the app, choose Open, then click Open again. This is a one-time step.
4. The licence activation screen appears. Enter your licence key and click Activate. An internet connection is required for first activation.
5. The main application window opens. You are ready to use TrustedMARC.

After the first activation your licence is stored on this machine. You will not be asked again unless you move to a new machine or use File then Deactivate Licence.

2.2 Windows — TrustedMARC.exe

6. Download TrustedMARC-Windows.zip from trustedmarc.co.uk and unzip it.
7. Run TrustedMARC.exe from the unzipped folder.
8. **First launch — SmartScreen warning.** Windows may display a SmartScreen warning. Click More info, then Run anyway. This is a one-time step.
9. The licence activation screen appears. Enter your licence key and click Activate. An internet connection is required for first activation.
10. The main application window opens. You are ready to use TrustedMARC.

3. Licence Activation

TrustedMARC requires a valid licence key to run. This section covers how to activate your licence, what happens if you go offline, and how to move to a new machine.

3.1 First launch — activating your licence

When you launch the application for the first time, a licence activation screen appears. Enter the licence key you received by email and click Activate.

11. Ensure you have an internet connection before your first launch.
12. Open dmarc_app-2.0.py as described in Section 2.
13. The licence activation screen appears. Enter your key exactly as provided — copy and paste is recommended.
14. Click Activate. The application contacts the licence server and verifies your key.
15. On success, the main application window opens immediately. Your licence is stored on this machine and you will not be asked again.

> *Your licence key is tied to this machine. To move it to a new machine, use File then Deactivate Licence on the old machine first. If the old machine is unavailable, contact support@trustedmarc.co.uk.*

3.2 Normal use after activation

After the first activation, the application validates your licence automatically on every launch. You do not need to enter your key again. The validation takes less than a second and requires an internet connection.

3.3 Using the application offline

If you launch TrustedMARC without an internet connection, it will check when your licence was last successfully validated online. The following rules apply:

- **Within 3 days of last validation:** The application launches normally. A yellow warning banner is shown at the top of the window indicating you are running offline and how many days of the grace period remain.

- **Beyond 3 days of last validation:** The application cannot launch. Connect to the internet and relaunch — validation takes place automatically and the application opens as normal.

> *The 14-day grace period is designed to cover short-term connectivity issues such as travel or temporary outages. It is not intended for permanent offline use.*

3.4 Moving to a new machine

Your licence is activated on one machine at a time. The easiest way to move it is to deactivate on the old machine before setting up the new one.

Option 1 — Deactivate yourself (recommended)

16. On the old machine, open TrustedMARC.
17. Go to File then Deactivate Licence.
18. Confirm the dialog. The licence is removed from this machine immediately.
19. On the new machine, launch TrustedMARC and enter your licence key when prompted.

Option 2 — Contact support (if the old machine is unavailable, lost, or broken)

If you no longer have access to the old machine and cannot self-deactivate, contact support@trustedmarc.co.uk with your licence key. We will reset the activation manually, usually within one business day.

3.5 Licence errors

Licence suspended	Your licence has been suspended. Contact support@trustedmarc.co.uk.
Licence expired	Your licence has expired. Contact support to renew.
Already active on another machine	The key is registered to a different machine. Contact support for a transfer.
Key not found	Check the key was entered correctly. Copy and paste from the original email.
Grace period expired	Connect to the internet and relaunch. Validation is automatic.

4. Using the Application

4.1 Launching the application

macOS

Double-click TrustedMARC.app in your Applications folder, or wherever you saved it. The application opens directly with no terminal required.

Windows

Double-click TrustedMARC.exe from the folder you unzipped it into. The application opens directly with no terminal required.

4.2 Preparing report files

Save all DMARC report email attachments from your inbox into a single folder. The files may be a mix of .zip, .gz, and .xml formats and do not need to be renamed. Subfolders within the reports folder are scanned automatically.

In Outlook, the most efficient method is to select all DMARC report emails, right-click an attachment in the reading pane, and choose Save All Attachments. Direct the save dialog to your reports folder.

4.3 Generating a report

20. Click Browse next to Reports Folder and select the folder containing your DMARC files.
21. The Output Report path is set automatically to a timestamped file in the same folder. Adjust it if required.
22. Optionally enter a domain in the Domain filter field (e.g. spiderdomain.com). Leave blank to include all domains found in the reports.
23. Adjust the option checkboxes if needed (see Section 4.4).
24. Click Generate Report. The log area shows progress in real time.
25. When processing is complete the report opens automatically in your default browser. Click Open Report in the status bar to reopen it.

4.4 Options

Geolocation	When enabled, each IP address is looked up via ip-api.com to retrieve country, city, and ISP information. Requires an active internet connection — if offline this option will silently produce no results and senders may appear as Unknown. Adds a few seconds for large IP sets.
Reverse DNS	When enabled, each IP is resolved to a hostname. Requires an active internet connection — if offline hostnames will not be resolved. Adds a few seconds per batch of IPs.
DNS records	When enabled, the live SPF and DMARC records for the filtered domain are fetched via Google DNS and displayed in the Health tab. Requires an active internet connection and a domain filter to be set. If offline or no domain is specified, the Health tab will not show live DNS records and some recommendations may not fire.
Domain filter	Limits the report to records for a specific domain. If left blank all domains in the reports folder are included. Required for DNS record lookup.

Geolocation, Reverse DNS, and DNS record lookup all require an active internet connection. If you are working offline, untick these options before generating a report — the report will still be produced but without IP location data, hostnames, or live DNS records. Sender identification may be less accurate without geolocation data as the tool uses ISP information to identify known services.

5. The Dashboard

The output HTML file opens in any modern browser. No internet connection is required to view it once generated.

5.1 Summary card

A plain-English paragraph at the top of the page states the period covered, total message volume, DMARC pass rate, SPF and DKIM alignment rates, identified sender count, and any suspicious IP findings. It opens with a verdict indicator reflecting the overall pass rate: Excellent (>=95%), Good (>=80%), Needs Attention (>=60%), or Action Required (<60%).

5.2 Stat cards

Eight cards display the headline figures: total messages, DMARC pass, DMARC fail, SPF aligned, DKIM aligned, unique IPs, senders identified, and suspicious IP count.

5.3 Charts

DMARC Pass / Fail	Donut chart of overall DMARC result.
SPF Alignment	Donut showing the proportion of messages with proper SPF alignment to the From header domain.
DKIM Alignment	Donut showing DKIM alignment rate.
Reporting Orgs	Horizontal bar of the top reporting organisations by message volume. Label width adjusts automatically to prevent clipping.
Message Timeline	Stacked bar chart of pass and fail volumes for each date in the reporting period.
Top Sending IPs	Stacked horizontal bar of the 15 highest-volume sending IPs, showing pass and fail portions.

5.4 Senders tab

IPs are grouped by identified sending service. Each sender card shows the service name, emoji, category badge, IP count, total message volume, and pass rate with a visual bar. Clicking any card expands it to list the individual IPs, their hostnames, message counts, pass/fail breakdown, country, and any flags.

Services are identified by matching the geolocation ISP name, organisation name, ASN, and reverse DNS hostname against a database of over 30 known senders including Google Workspace, Microsoft 365, SendGrid, Amazon SES, Mailchimp, Zoho Mail, Mailgun, HubSpot, Salesforce, Klaviyo, and others. Unidentified senders fall back to their ISP name.

5.5 IP Detail tab

A full table of every sending IP with columns for IP address, hostname, identified sender, message count, DMARC pass count, DMARC fail count, SPF alignment badge, DKIM alignment badge, disposition, pass rate bar, location, ISP, reporting organisation, date range, and flags.

Filtering and search

The IP Detail table has four controls that can be used individually or in combination:

- **Text search.** The search box in the top-left filters across all columns simultaneously — IP address, hostname, sender name, country, ISP, and flags. Type any part of any value to narrow the list. The row count updates in real time.
- **Date range picker.** The From and To date fields filter to IPs that were active within the selected period. An IP is shown if its activity overlaps the selected range at all — so an IP that sent across January to March will still appear if you filter to February. Use this to isolate activity from a specific incident or time period.
- **Flag filter dropdown.** Filters to IPs matching a specific suspicious flag: All IPs (no filter), Suspicious only (any flag), High Fail (more than 50% failure rate), Total Fail (100% failure), or Spike (single-day high volume). Use this to quickly focus on the IPs most likely to need attention.
- **Column sorting.** Click any column header to sort ascending; click again to sort descending. Sorting by Pass Rate ascending quickly surfaces the worst-performing senders.

Drilldown panel

Clicking any row in the IP Detail table expands a drilldown panel below it showing:

- **Identity detail.** Header-from domain, envelope-from domain, and DKIM selectors used by this IP.
- **Network detail.** Fully resolved hostname, ISP name, ASN, and geolocation.
- **Authentication counts.** Exact pass and fail counts for SPF and DKIM alignment.
- **Per-IP activity chart.** A small bar chart showing pass and fail volumes for each date this IP appeared in the reports. Useful for spotting whether a problem started on a specific date.

5.6 Health and Actions tab

Three sections are presented:

- **Policy Journey.** A visual step indicator showing the current DMARC policy (p=none, p=quarantine, or p=reject) and the remaining steps towards full enforcement. The policy is read from the live DNS record where available, not from the XML report files, so it always reflects the current state of your DNS configuration.
- **Live DNS Records.** The current SPF and DMARC TXT records fetched at report-generation time. Allows immediate comparison between what the records say and what the traffic data

shows. These are only fetched when a domain filter is specified and DNS lookup has not been disabled.

- **Recommendations.** A prioritised list of actionable findings. Red (priority 1) items require immediate attention. Yellow (priority 2) items should be addressed in the near term. Blue (priority 3) items are advisory and represent improvements rather than problems.

How recommendations are generated

The recommendation engine applies the following logic:

- **Policy level.** Read from the live DNS DMARC record. If p=none is detected, a priority 1 alert is raised. If p=quarantine is detected, a priority 3 advisory suggests moving to p=reject — this is intentionally low priority because quarantine is a valid and effective configuration, not a problem.
- **Failing known senders.** A sender is only flagged if the majority of its messages (more than 50%) are failing DMARC and there are at least 10 failing messages. Services such as Google Workspace and Microsoft 365 appear in reports both as senders of your mail and as reporters who received mail and filed the report. The tool distinguishes between these: a cloud provider is only flagged if its failures outnumber its passes. If passes dominate, the service is almost certainly reporting rather than sending as your domain and failing.
- **SPF and DKIM alignment rates.** If fewer than 80% of messages have SPF or DKIM alignment, a recommendation is raised.
- **SPF record health.** If the live SPF record has more than 8 includes (approaching the DNS lookup limit of 10), or uses +all (which authorises any server to send as your domain), a recommendation is raised.
- **Missing records.** Missing SPF or DMARC records are only flagged when DNS lookup was actually run and returned a definitive answer. If DNS lookup was disabled with --no-dns, or no domain filter was specified, these warnings are suppressed to avoid false positives.

> *If you believe a recommendation is incorrect — for example if it suggests a policy change you have already made — check that the DNS lookup ran successfully. The live DNS records are displayed in the same tab. If the DMARC record shown matches your actual configuration, the recommendation engine has read it correctly and the policy-level recommendation will not fire.*

5.7 Suspicious IP flags

high-fail	More than 50% of messages from this IP failed DMARC.
total-fail	Every message from this IP failed DMARC and there were more than 10 messages.
single-day-spike	This IP appeared on only one date but sent more than 100 messages.
multi-domain	This IP was sending on behalf of more than 3 different domains.

> *A flagged IP is not necessarily malicious. A misconfigured legitimate sender will also appear flagged. Use the ISP name, hostname, and geolocation data in the drilldown panel to determine whether the IP belongs to a known service.*

5.8 CSV export and printing

The Export CSV button in the report header downloads a spreadsheet containing every IP with all data columns including sender identification, geolocation, alignment counts, and flags. The Print / PDF button triggers the browser print dialog. A print stylesheet hides interactive elements and applies a clean white background suitable for PDF generation.

6. Making Sense of the Results

6.1 Understanding the pass/fail split

DMARC passes when either SPF or DKIM is aligned — meaning the authenticated domain matches the visible From header. A message can have SPF pass and DKIM fail and still pass DMARC if the SPF domain aligns. A message with both SPF and DKIM passing at the raw level can still fail DMARC if neither aligns with the From header. The dashboard reports alignment specifically, not raw pass/fail.

6.2 What to do when a known sender is failing

If a service such as SendGrid or Mailchimp appears in the Senders tab with a significant failure rate, the most likely cause is one of the following:

- The service is not included in the domain's SPF record. Add the relevant include statement.
- DKIM signing is not configured for the domain on that platform. Enable it in the platform's settings and add the provided CNAME or TXT record to DNS.
- The service is sending from a subdomain that is not covered by the DMARC record.

The recommendations in the Health tab will identify which of these applies and provide the specific action required.

6.3 What to do when an unknown IP is failing

An unidentified IP with a high or total failure rate is the primary indicator of spoofing. The appropriate response depends on the current DMARC policy:

- **p=none.** The domain is monitoring only. Spoofed messages are not being blocked. Use this data to confirm all legitimate senders are correctly configured, then move to p=quarantine.
- **p=quarantine.** Spoofed messages are being directed to spam. This is effective but not complete. Move to p=reject once the pass rate for legitimate traffic is consistently above 95%.
- **p=reject.** Spoofed messages are being refused entirely. This is the target state.

6.4 The policy journey

The recommended progression is p=none for at least four to six weeks of monitoring, then p=quarantine, then p=reject once confidence is established. Jumping directly to p=reject before all legitimate senders are properly authenticated will result in legitimate mail being rejected.

7. Reusing for Other Domains

No changes to either file are required to analyse a different domain. The tool is domain-agnostic. Simply point it at a folder of DMARC report files and optionally specify a domain filter.

If report files for multiple domains are stored in the same folder, the domain filter produces a separate focused report for each:

```
python3 dmarc_report-2.0.py ~/reports/ --domain spiderdomain.com --output
spider.html
python3 dmarc_report-2.0.py ~/reports/ --domain antdomain.com   --output
ant.html
```

Omitting the domain filter produces a single report covering all domains in the folder, with a domain tab selector appearing in the IP Detail tab when multiple domains are present.

8. Troubleshooting

8.1 Desktop application errors

Error / Symptom	Cause	Resolution
macOS — Gatekeeper blocks the app	macOS blocks apps not signed with an Apple Developer certificate.	Right-click the app, choose Open, then click Open again. One-time step.
Windows — SmartScreen warning	Windows flags software from publishers not in its database.	Click More info, then Run anyway. One-time step.
Licence key not found	The key was entered incorrectly or is missing the key/ prefix.	Copy and paste the full key directly from your purchase confirmation email.
Cannot reach licence server	No internet connection, or a VPN is blocking the connection.	Connect to the internet and try again. Disable VPN if one is active.
Licence registered to a different machine	The key is already activated on another machine.	Use File then Deactivate Licence on the old machine, or contact support@trustedmarc.co.uk to reset the activation.
Offline grace period expired	The app has not been able to validate online for more than 14 days.	Connect to the internet and relaunch. Validation is automatic.
Something went wrong	The report engine encountered an error. Check the log window for detail.	Most commonly caused by an empty folder, invalid files, or a domain filter with no matching records.
No records found for domain X	The domain filter did not match any records in the selected folder.	Check spelling matches exactly, or leave the filter blank to see all available domains.

8.2 Report content issues

Error / Symptom	Cause	Resolution
`No records found`	No matching DMARC files were found, or the domain filter excluded all records.	Check the folder path. If using a domain filter, confirm it matches the domain in the report files exactly (e.g. spiderdomain.com not www.spiderdomain.com).
`0 record(s) per file`	The XML inside the archive could not be parsed. Usually an expat issue on macOS.	Resolve the expat library issue first. Test with: python3 -c "import xml.etree.ElementTree as ET; ET.fromstring('<x/>')". If this raises an error, the expat fix is needed.
`All IPs show as Unknown sender`	Geolocation was disabled or returned no results, so sender identification has no ISP data to match against.	Run with geolocation enabled (the default). Ensure internet access is available. Sender identification requires ISP/org data from the geo API.
`Geolocation returns partial data`	The ip-api.com rate limit (45 requests/minute) was hit during a large batch.	This is handled automatically with a 1.5-second delay between batches. For very large IP sets the process simply takes longer — this is expected.
`DNS records show as missing`	DNS lookup was skipped (--no-dns flag or no domain filter set), or the records genuinely do not exist.	Ensure --domain is specified and DNS lookup is enabled. Verify the records exist using: nslookup -type=TXT _dmarc.yourdomain.com

9. Advanced — Python Script Usage

This section is for users who wish to run TrustedMARC from the Python source scripts rather than the desktop application. If you are using TrustedMARC.app or TrustedMARC.exe, you do not need this section.

> *The desktop application is self-contained and is the recommended option for all users. The Python scripts require Python 3.13 and additional dependencies described below.*

9.1 Requirements

For users who wish to run the application from source, the Python scripts dmarc_app-2.0.py and dmarc_report-2.0.py are provided. This requires the following to be installed:

Homebrew (macOS only)	Mac package manager. Required to install Python and expat. Install from brew.sh if not already present.

Python 3.13	Installed via Homebrew on macOS, or downloaded from python.org on Windows. Python 3.14 has a known incompatibility on macOS and should be avoided.
expat (macOS only)	XML parsing library. The macOS system version is outdated. Homebrew version must be used.
Tkinter	Required for the GUI. Not bundled with Homebrew Python — install with: brew install python-tk@3.13
Python packages	None. The script uses Python standard library only.

9.2 Installation — macOS

> *This section applies only if you are running the Python scripts directly. If you are using the standalone TrustedMARC.app, skip to Section 5.*

9.2.1 Install Homebrew

Open Terminal (Applications → Utilities → Terminal) and run:

```
/bin/bash -c "$(curl -fsSL
https://raw.githubusercontent.com/Homebrew/install/HEAD/install.sh)"
```

Follow the on-screen prompts. Homebrew will install the Xcode Command Line Tools if they are not already present. This may take several minutes.

9.2.2 Install Python 3.13 and expat

```
brew uninstall python@3.14    # remove if present — it has a known bug on macOS
brew install python@3.13
brew install python-tk@3.13   # install because it isn't bundled with Homebrew
Python
brew install expat
```

9.2.3 Configure your shell

These three lines configure Terminal to use the correct Python and expat library every time it opens. Run them once:

```
echo 'export PATH="/opt/homebrew/opt/python@3.13/bin:$PATH"' >> ~/.zshrc
echo 'export DYLD_LIBRARY_PATH="/opt/homebrew/opt/expat/lib:$DYLD_LIBRARY_PATH"'
>> ~/.zshrc
echo 'alias python3="python3.13"' >> ~/.zshrc
source ~/.zshrc
```

9.2.4 Verify

```
python3 --version    # should print: Python 3.13.x
```

If the version shown is still 3.9.6 or 3.14.x after running the above, open a new Terminal window and try again. The source ~/.zshrc command applies the changes to the current session only.

9.2.5 Place the files

Copy both files into a folder of your choice. A dedicated folder such as ~/Tools/dmarc is recommended.

- `dmarc_report-2.0.py` — the processing engine
- `dmarc_app-2.0.py` — the desktop application

Both files must be in the same folder. The app locates the engine by looking in its own directory. If they are separated it will display an error on launch.

9.3 Installation — Windows

This section applies only if you are running the Python scripts directly. If you are using the standalone TrustedMARC.exe, skip to Section 5.

9.3.1 Install Python

26. Open a browser and go to python.org/downloads
27. Download the latest Python 3.13.x installer (Windows installer 64-bit).
28. **Important:** On the first screen of the installer, tick the checkbox labelled **Add Python to PATH** before clicking Install Now.
29. Complete the installation. Restart any open Command Prompt windows afterwards.

9.3.2 Verify

Open Command Prompt (press Win+R, type cmd, press Enter) and run:

```
python --version    # should print: Python 3.13.x
```

On Windows the command is python (not python3). The app handles this automatically. If you see an error saying python is not recognised, Python was not added to PATH during installation. Uninstall and reinstall Python, ensuring the PATH checkbox is ticked.

9.3.3 Place the files

Copy both files into a folder such as C:\Tools\dmarc or your Desktop. Both files must be in the same folder.

9.4 Command-line usage

The parser can be run directly from the terminal without the GUI. This is useful for scripting, scheduled tasks, or server environments.

9.4.1 Basic usage

```
# macOS
python3 dmarc_report-2.0.py ~/Downloads/dmarc_reports/ --output report.html

# Windows
python dmarc_report-2.0.py C:\Users\John\Downloads\dmarc_reports --output
report.html
```

9.4.2 All options

--output / -o	Path and filename for the HTML report. Defaults to dmarc_report.html in the current directory.
--domain / -d	Filter to a specific domain. E.g. --domain spiderdomain.com
--no-geo	Skip IP geolocation. Faster and works without internet access.
--no-rdns	Skip reverse DNS lookups. Faster.
--no-dns	Skip live DNS record fetching. Use if no internet or no domain filter is set.

9.4.3 Examples

```
# Full run with domain filter
python3 dmarc_report-2.0.py ~/reports/ --domain spiderdomain.com --output
spider.html

# Fast offline run — no network lookups
python3 dmarc_report-2.0.py ~/reports/ --no-geo --no-rdns --no-dns

# Multiple domains — run separately
python3 dmarc_report-2.0.py ~/reports/ --domain spiderdomain.com --output
spider.html
python3 dmarc_report-2.0.py ~/reports/ --domain antdomain.com   --output
ant.html

# Open the report immediately (macOS)
python3 dmarc_report-2.0.py ~/reports/ --output r.html && open r.html

# Open the report immediately (Windows)
python dmarc_report-2.0.py C:\reports --output r.html && start r.html
```

10. Quick Reference

macOS — one-time setup

```
brew uninstall python@3.14
brew install python@3.13 expat
echo 'export PATH="/opt/homebrew/opt/python@3.13/bin:$PATH"' >> ~/.zshrc
echo 'export DYLD_LIBRARY_PATH="/opt/homebrew/opt/expat/lib:$DYLD_LIBRARY_PATH"'
>> ~/.zshrc
echo 'alias python3="python3.13"' >> ~/.zshrc
source ~/.zshrc
```

Launch the desktop app

```
python3 dmarc_app-2.0.py    # macOS
python  dmarc_app-2.0.py    # Windows
```

Standard command-line run

```
python3 dmarc_report-2.0.py ~/reports/ --domain yourdomain.com --output
report.html
open report.html    # macOS
start report.html   # Windows
```

Fast run — no network lookups

```
python3 dmarc_report-2.0.py ~/reports/ --no-geo --no-rdns --no-dns
```

If python3 breaks after opening a new terminal (macOS)

```
source ~/.zshrc
```