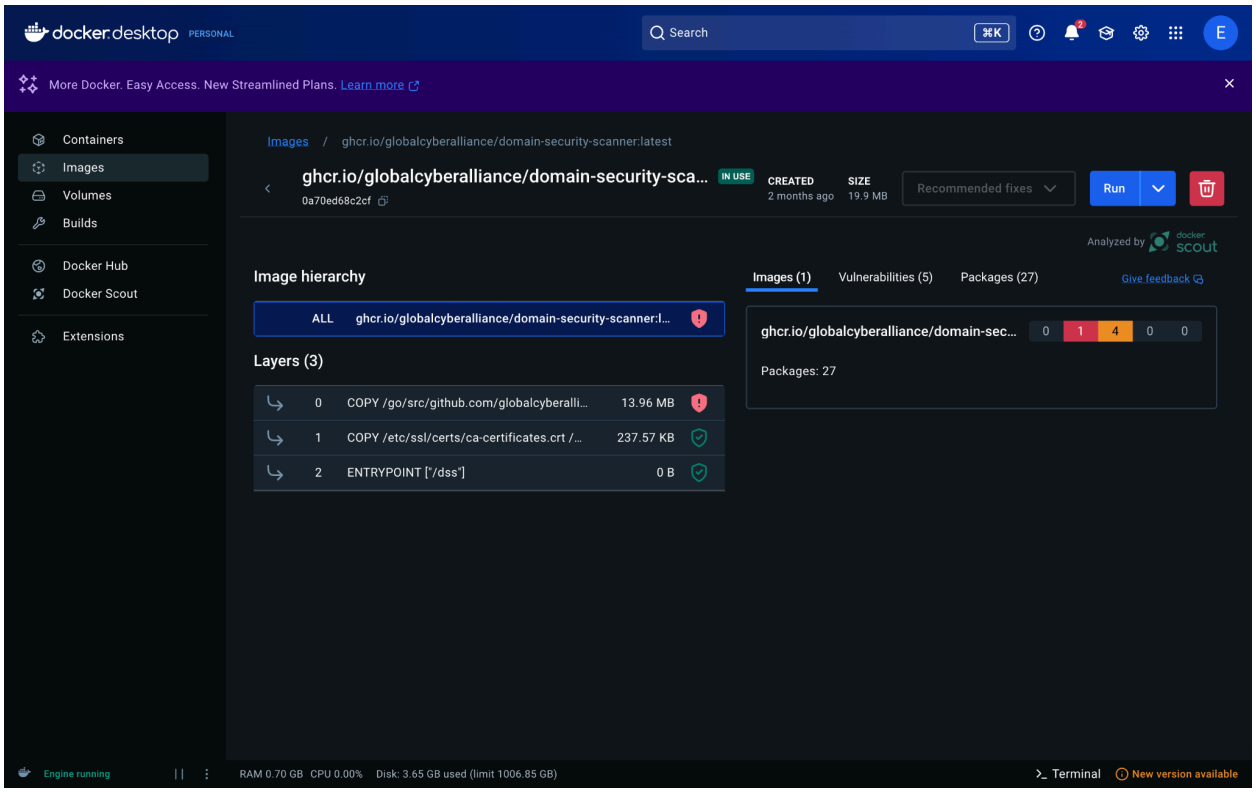
Domain-Security-Scanner: ([GitHub Page])
This open-source program by *Global Cyber Alliance* can be used to perform scans against domains for DKIM, DMARC, and SPF DNS records. Making it an ideal comparison for Spoofy.

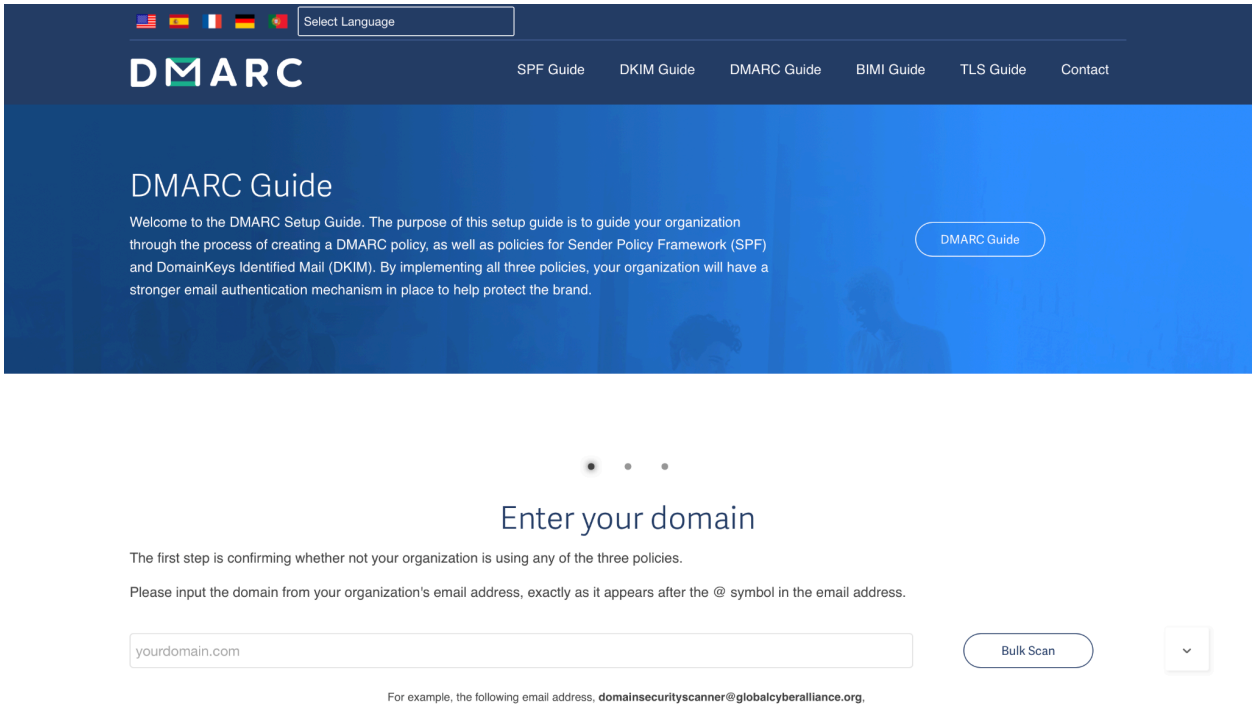
Something about this program is very bizarre. I don't really understand why it refuses to work. This program is intended for Docker. I have gotten this Docker running, however, you can see that this program refuses to work inside of Docker. I will launch it and it immediately closes, additionally I don't have Docker premium. Setting it up on a macOS machine with Go is also impossible because the program can't access Python script. Maybe a bug? Whatever.

You can see here an analysis of the vulnerabilities in this program; none of them are very significant with the exception of [CVE-2025_22869] for DDoS attacks. This is not very important, just a note about the status of the program, there is no fix for this CVE.



You can see the intended tool usage here. A user can use the ‘dss’ command to check any domain similarly to Spoofy. You can see that Domain-Security-Scanner has some additional functionality in the form of the ‘-a’ and ‘--checkTLS’ functions. Spoofy has no ability to advise potential fixes; it only gives basic information about the DKIM, DMARC, and SPF DNS records. Additionally, Spoofy has no TLS analysis functions which would be a significant boon for the platform. Potentially, something we can consider adding to Spoofy in the future. Unfortunately, I can’t run any tests based on the status of the program in Docker.

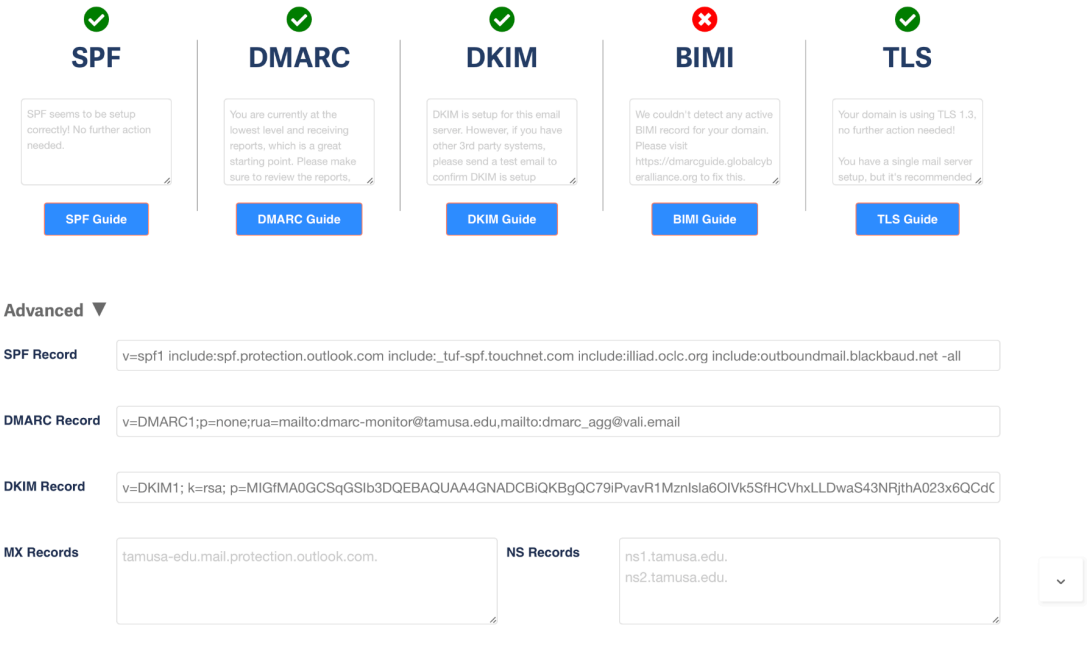
Thankfully this program can be run in a browser. Mind you with significantly less features than its Docker counterpart. We will run our comparison test through this platform (Webpage for Domain-Security-Scanner).



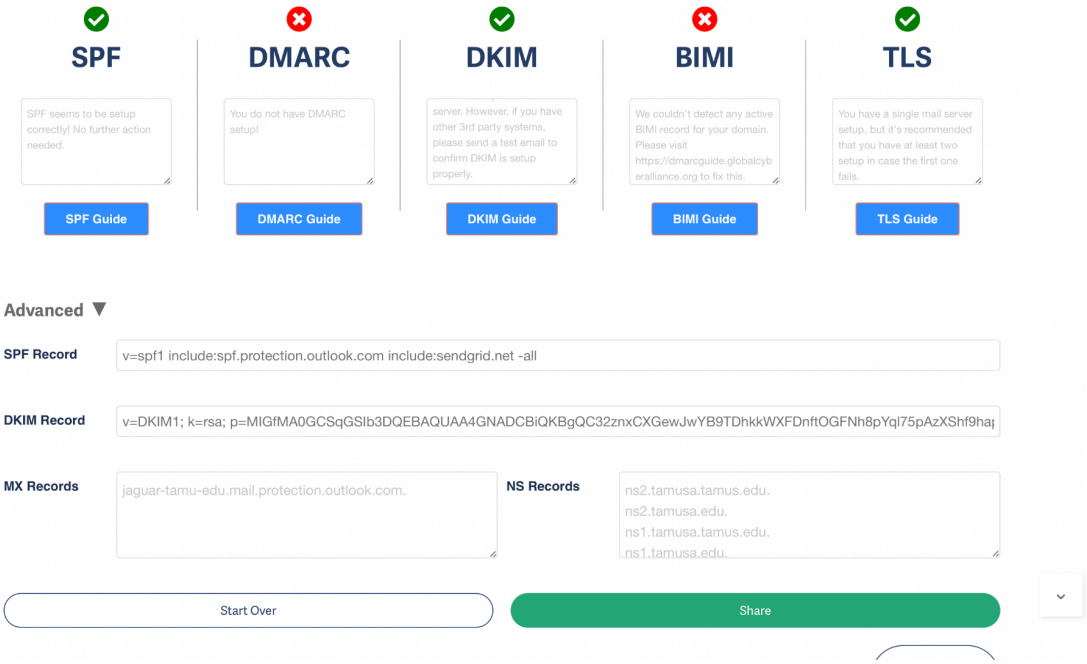
You can see the webpage here. It's fairly straightforward, the top of the page has some links to pages that explain SPF, DKIM, DMARC, BIMI, and TLS accordingly. You also have the options for a simple scan and a bulk scan (for checking multiple domains). The results for my tests on the webpage can be seen below. I did a very simple test on the TAMUSA domains.

Overall, I think this tool is useful but its implementation is bad unfortunately. It's good inspiration but it's awful to use. This website has terrible ping and some errors when loading webpages. Maybe I would have liked this tool more if it worked in Docker.

TAMUSA.EDU:

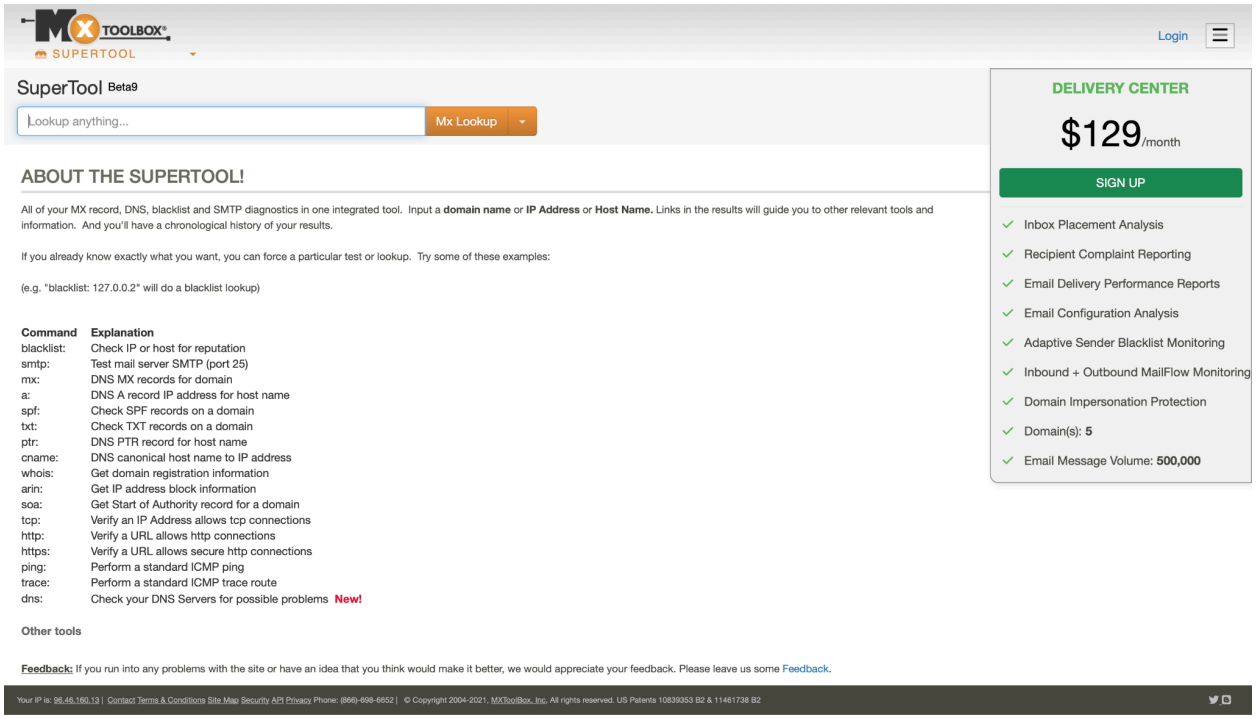


JAGUAR.TAMU.EDU:



MXToolBox Network Tools (Website):

MXToolBox is an online diagnostic tool used for email and network troubleshooting. It has a suite of utilities including Email and DNS troubleshooting, network diagnostics, performance and security analysis. These use cases make it an ideal comparison for Spoofy. Specifically for its capability to check SPF, DKIM, and DMARC records for email security settings. These settings, as established, allow us to determine the spoofability of a domain. Additionally the MX check and Blacklist Check functions can give us a better idea of how the domain functions. Specifically, what IPs the chosen domain is blacklisting. For the majority of blocked domains you'll notice they present critical vulnerabilities that need to be avoided.



For our example we're going to do an analysis on the TAMUSA domains, similarly to the previous tool. This should give us a good point of reference for our discussion of MXToolBox. What's especially curious in comparison to the previous test you'll notice is that this website states that tamusa.edu does not have a DMARC policy. Further analysis points to the DMARC policy being p=none. This leads me to believe that the tool we previously tested could potentially be inaccurate. You'll notice looking at the previous images that tamusa.edu's DMARC policy is confirmed by the other tool to also be p=none. Meaning there is no DMARC security. For security, this DMARC policy should be p=quarantine, but it is not so we should state that there is no DMARC policy. That is misleading, because though the domain has a DMARC policy because mail domains are required to list a policy to be legitimate that does not necessarily mean the policy is secure. Especially considering that with Gmail and Yahoo domains they're making a move away from zero policy.

mx:tamusa.edu Find Problems | Solve Email Delivery Problems | mx

Pref	Hostname	IP Address	TTL	
10	tamusa-edu.mail.protection.outlook.com	52.101.10.10 Microsoft Corporation (AS8075)	60 min	Blacklist Check SMTP Test
10	tamusa-edu.mail.protection.outlook.com	2a01:111:f403:c946::6	60 min	Blacklist Check

	Test	Result	
!	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled	More Info
✓	DMARC Record Published	DMARC Record found	
✓	DNS Record Published	DNS Record found	

Your email service provider is "Microsoft Office" Need Bulk Email Provider Data?

dns lookup | dns check | dmarc lookup | spf lookup | dns propagation

Reported by **ns1.tamusa.edu** on 3/20/2025 at **9:29:31 PM (UTC -5)**, just for you. Transcript

dmarc:tamusa.edu Solve Email Delivery Problems | dmarc


```
v=DMARC1;p=none;rua=mailto:dmarc-monitor@tamusa.edu,mailto:dmarc_agg@vali.email
```

Tag	TagValue	Name	Description
v	DMARC1	Version	Identifies the record retrieved as a DMARC record. It must be the first tag in the list.
p	none	Policy	Policy to apply to email that fails the DMARC test. Valid values can be 'none', 'quarantine', or 'reject'.
rua	mailto:dmarc-monitor@tamusa.edu,mailto:dmarc_agg@vali.email	Receivers	Addresses to which aggregate feedback is to be sent. Comma separated plain-text list of DMARC URIs.

	Test	Result	
!	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled	More Info
✓	DMARC Record Published	DMARC Record found	
✓	DMARC Syntax Check	The record is valid	
✓	DMARC External Validation	All external domains in your DMARC record are giving permission to send them DMARC reports.	
✓	DMARC Multiple Records	Multiple DMARC records corrected to a single record.	

dns lookup | dns check | mx lookup | spf lookup | dns propagation

Reported by **ns2.tamusa.edu** on 3/20/2025 at **9:31:25 PM (UTC -5)**, just for you. Transcript

Tool	SPF Support	DKIM Support	DMARC Support	TLS Support	Notes
Spoofy	✅ Yes	❌ No	✅ Yes	❌ No	CLI tool that checks SPF & DMARC only. Outputs spoofability score based on 198 DNS policy combinations. No DKIM/TLS functionality included.
MXToolbox	✅ Yes	✅ Yes	✅ Yes	✅ Yes	Web-based suite with tools for DNS, email, blacklist checks, and TLS diagnostics. Accurate SPF, DKIM, and DMARC analysis with enforcement status.
Domain-Security-Scanner	✅ Yes	✅ Yes	✅ Yes	✅ Yes	Open-source CLI and web tool. Supports `--checkTLS`. Web version is limited and slow; Docker implementation has reliability issues.