

[Get started](#)[Open in app](#)

wondersmith_rae

724 Followers

[About](#)[Follow](#)

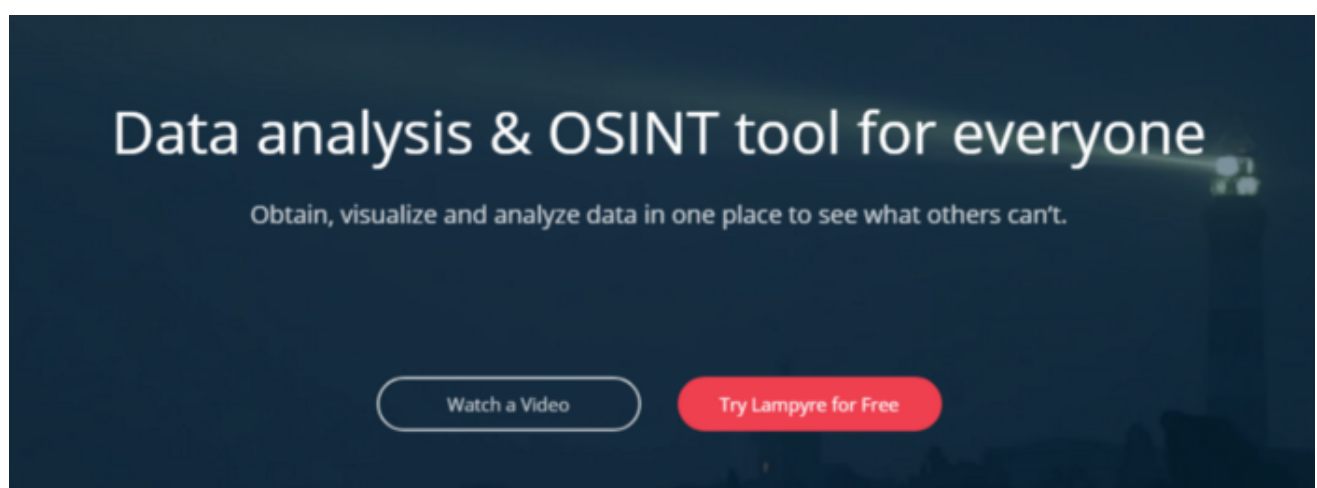
OSINT Quick Guide: Running a Domain Scan in Lampyre

***Due to recent findings by @MwOsint I can no longer endorse Lampyre as a trusted tool <https://keyfindings.blog/2020/03/23/be-careful-what-you-osint-with/>

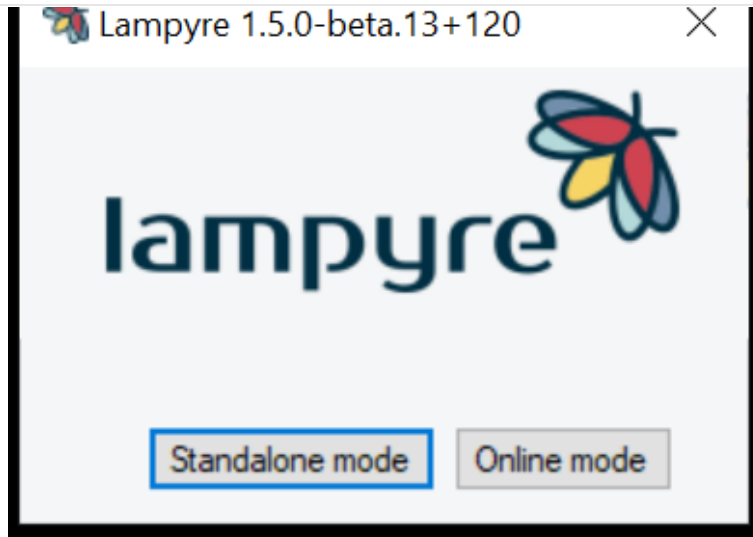


wondersmith_rae Feb 9, 2020 · 4 min read

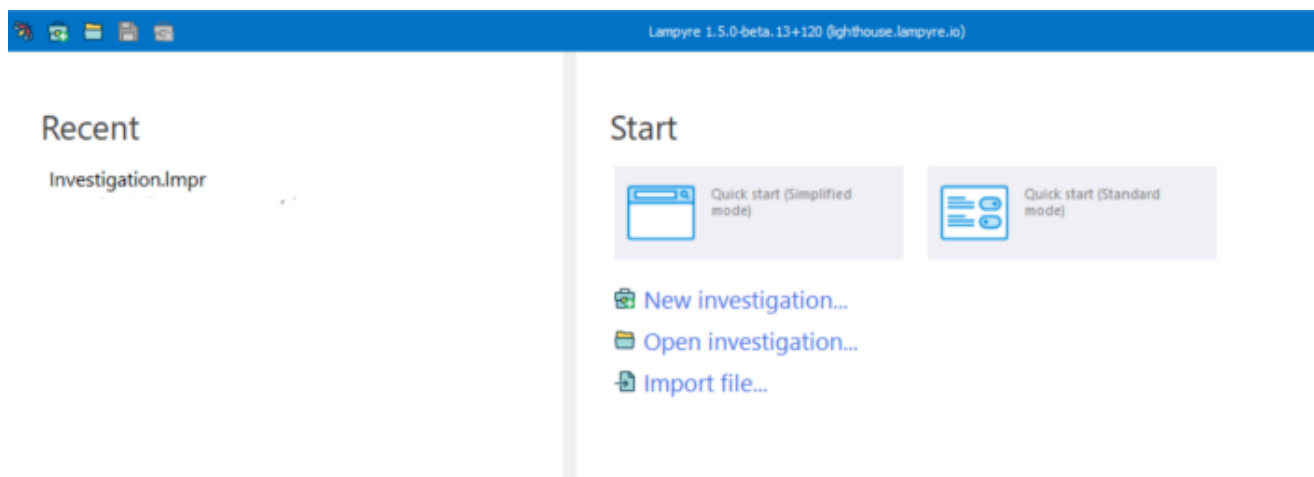
Lampyre is a windows-based tool that I like to use for some quick OSINT research. Previously, I wrote a blog on [Basic Email and Phone Number recon](#) but Lampyre has since upgraded and now has an exciting new beta version with a more simple layout and new tools. If you don't already have Lampyre, you can go to their website www.lampyre.io and click Try Lampyre for Free.



Once Lampyre is installed, activate it through their website and then open the program. This demo will be run in online mode, I have found it to be less buggy overall. It is my understanding that Standalone mode is just a way to isolate your search data from the internet and since we won't be doing anything secret in nature it shouldn't matter.

[Get started](#)[Open in app](#)

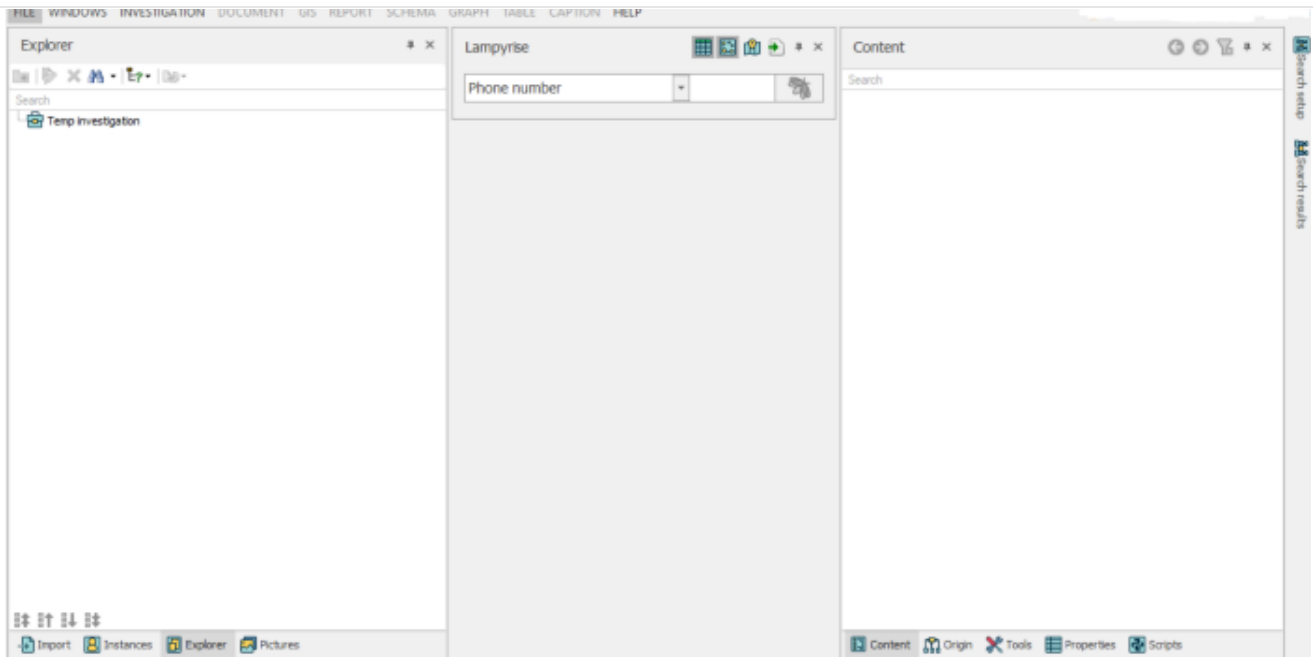
A window will open to start a new investigation. I prefer setting the layout to Simplified Mode since it has fewer options that will confuse me. Click on that option and windows will open for the new investigation.



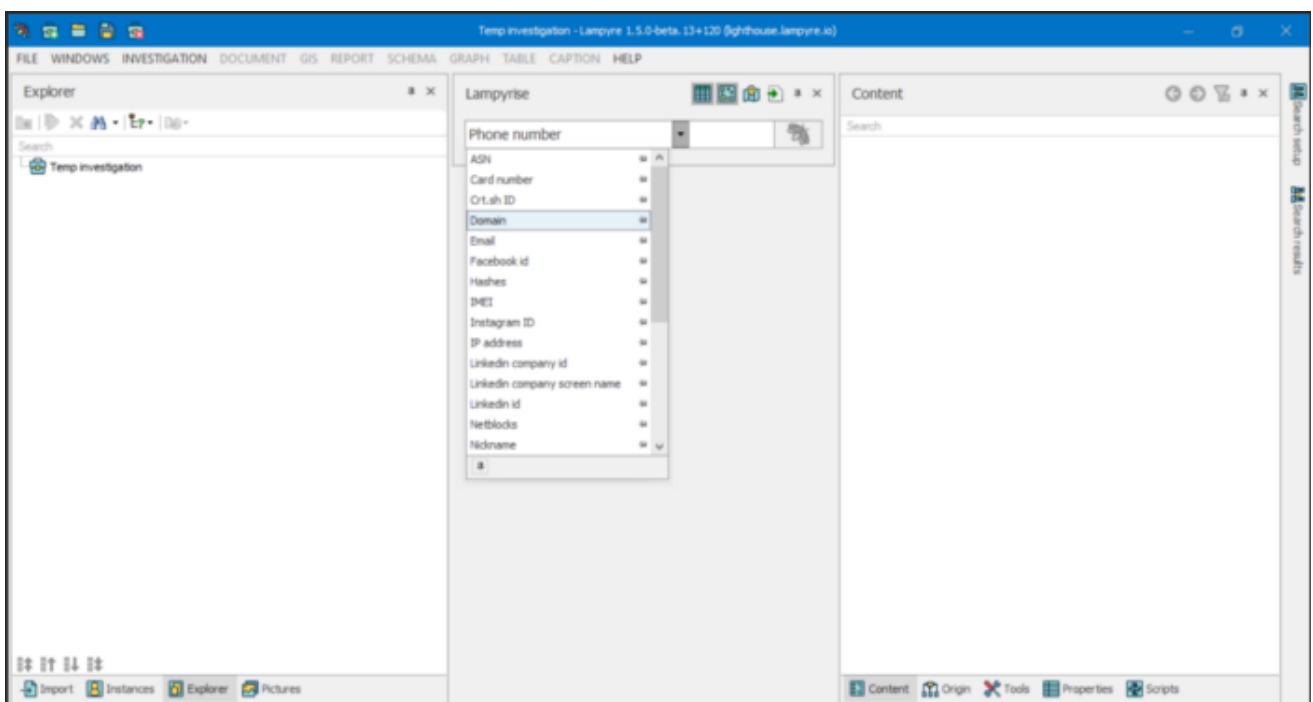
One of the cool new things in the beta is the Lampyrise tool. It makes it super easy to search for things by selecting them from the drop-down.

Get started

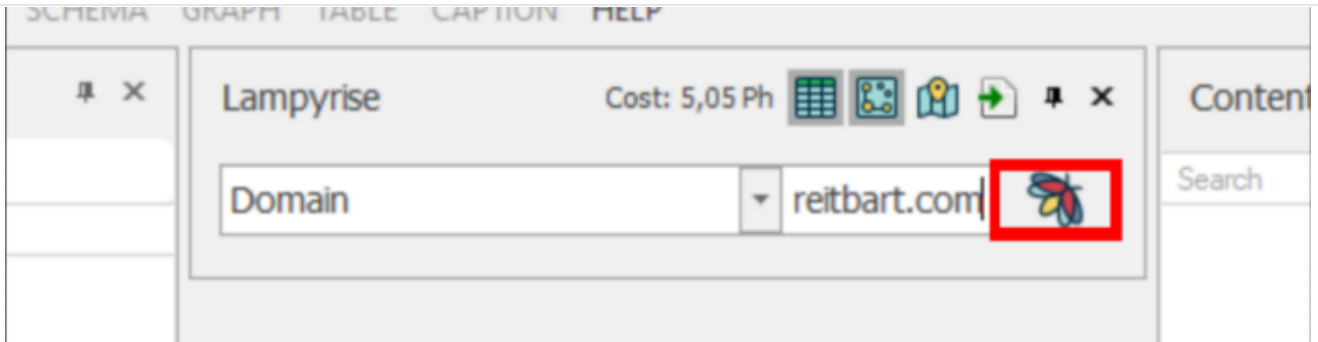
Open in app



You can see I chose **Domain** in the Lampyrise drop-down menu below. In the field next to Domain is where the search criteria will go.

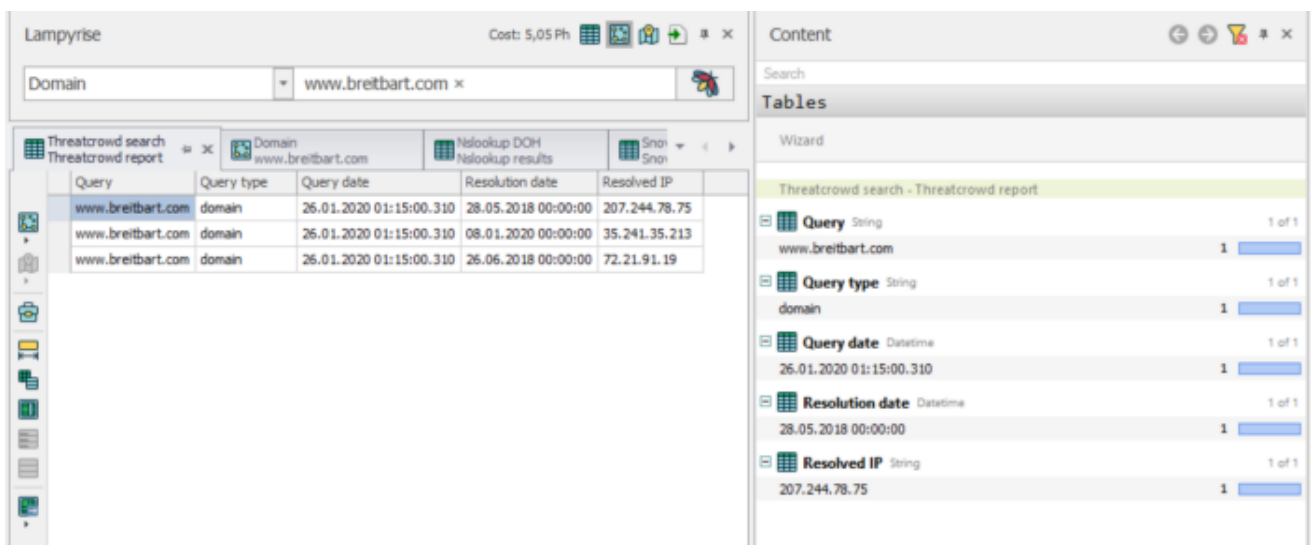


Out of sheer curiosity, I searched for Breitbart dot com and then clicked the Lampyre logo next to the box which starts the search.

[Get started](#)[Open in app](#)

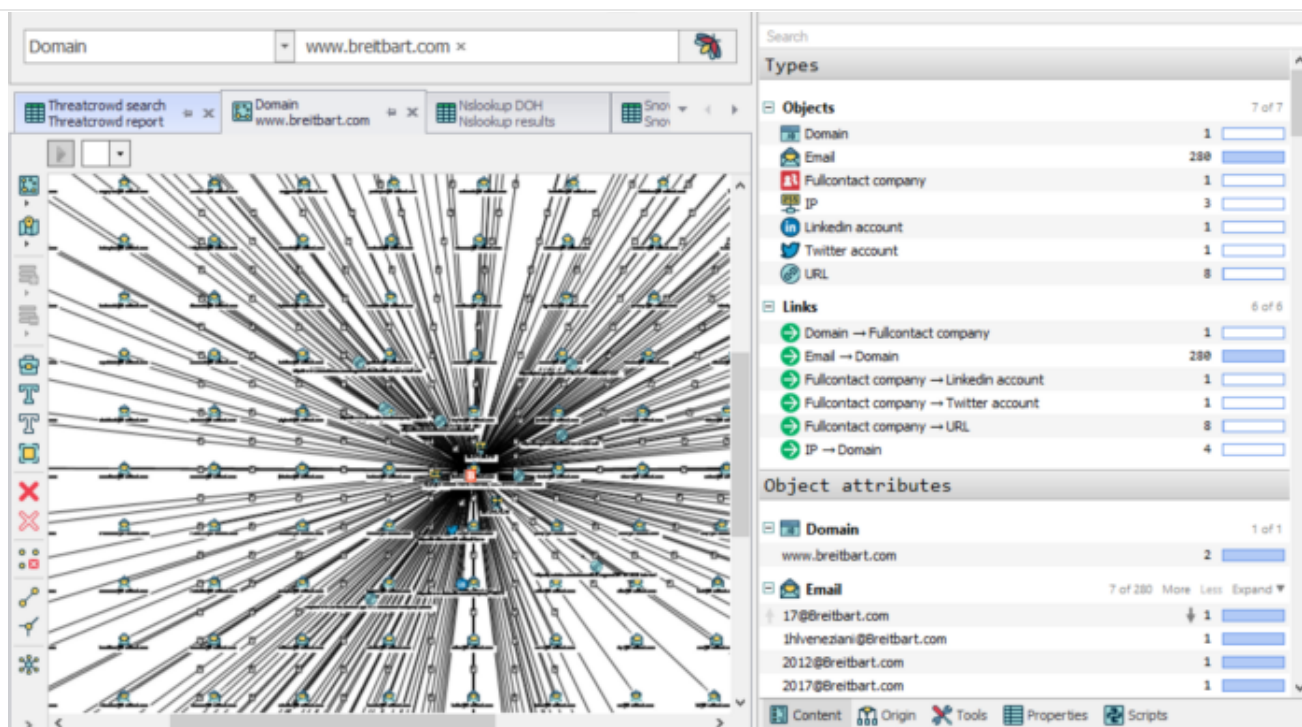
Another fun thing about Lampyre is there is no real need to mess with installing API keys. Their website claims to have over 100 regularly updated data sources. If you are a person who struggles with API keys in Maltego this might be where Lampyre can help.

As this scan runs you can see it tabs pop up for Threatcrowd, NSLookup, Snov.io and Full Contact of objects and social networks with the domain. Additionally, I am able to choose whether I want to run data in a table, schema, map, or all three. Who doesn't love a good schema amirite?










Each tab shown here offers different data to parse through. The ThreatCrowd tab shows us all of the resolved IPs associated with our domain. ThreatCrowd is great at finding entities alone but requires something like Lampyre to help visualize all of the data.

In my initial scan, I ran all visualization options (table, schema, map). Below we can see the graph of all the entities associated with the domain. We can also open the Timeline (Window > Timeline) to focus in on just one section of the schema. Furthermore, we can grab an entity on the schema and open it into its own investigation.

[Get started](#)[Open in app](#)

Many of the entities found in this scan were emails. I found these two emails below interesting.



Content			
Search			
 Email: login	7 of 280	More	Less Expand ▼
↑ 17	↓ 1	<input type="text"/>	
1hlveneziani	1	<input type="text"/>	
2012	1	<input type="text"/>	
2017	1	<input type="text"/>	
40145_still_more_overtly_racist_comments	1	<input type="text"/>	
42057_pamela_geller_spreads_hatred_and_lies	1	<input type="text"/>	
a	1	<input type="text"/>	
 Email: domain	1 of 1		
breitbart.com	280	<input type="text"/>	
 Bio	1 of 1		
Syndicated news and opinion website providing continuously ...	1	<input type="text"/>	
 Company name	1 of 1		
Breitbart News Network, LLC.	1	<input type="text"/>	
 IP address	3 of 3		
↑ 207.244.78.75	↓ 1	<input type="text"/>	
35.241.35.213	1	<input type="text"/>	
72.21.91.19	1	<input type="text"/>	
 IP address: IP	3 of 3		
↑ 207.244.78.75	↓ 1	<input type="text"/>	
35.241.35.213	1	<input type="text"/>	
72.21.91.19	1	<input type="text"/>	
 URL	7 of 9	More	Less Expand ▼
↑ https://www.linkedin.com/company/140373	↓ 2	<input type="text"/>	

I obviously couldn't let it go without trying to validate them but they were undeliverable.

Validation summary

Input data: **42057_pamela_geller_spreads_hatred_and_lies@Breitbart.com**

Classification: ■ Undeliverable

Status: Invalid email address, the mailbox for the email address does not exist.

Status code: MailboxDoesNotExist [\(What's this?\)](#)

Another tab shows NSlookup, or Name Server Lookup results. This is used for querying the Domain Name System to gather the domain name, IP, or other DNS records. In this instance, NSlookup provided most of the same data as Threatcrowd.

The screenshot shows the Lampyrise interface with two main panels. The left panel displays the 'Threatcrowd search' results for the domain 'www.breitbart.com'. The right panel displays the 'NSlookup DOH' results for the same domain.

Threatcrowd search results:

Service	Query	Type	IP	Resolve date
Cloudflare	www.breitbart.com	A	35.241.35.213	26.01.2020 01:15:00.280
Google	www.breitbart.com	A	35.241.35.213	26.01.2020 01:15:00.280
jsondns.org	www.breitbart.com	A	35.241.35.213	26.01.2020 01:15:00.280

NSlookup DOH results:

Field	Value	Count
Service	String	3 of 3
Cloudflare		1
Google		1
jsondns.org		1
Query	String	1 of 1
www.breitbart.com		3
Type	String	1 of 1
A		3
IP	String	1 of 1
35.241.35.213		3
Resolve date	Datetime	1 of 1
26.01.2020 01:15:00.280		3

Lampyrise Osint Open Source Intelligence Cybersecurity Infosec We saw the schema, this below is the data in a table. We get all of the email addresses in an easy to export chart.



As you can see, using Lampyre is a simple way to start doing domain recon and practicing your OSINT skills. Generally, I do not stick to using just one method however and I would most likely pair this with searches from intelligence X, Whois, and RiskIQ just to name a few. Be sure to keep an eye out for more quick tips coming soon!