YAHOS – Yet Another HOst Sentinel

A process monitoring tool for both network-based and host-based signatures.

- Primarily designed for Windows systems running on x86 architecture.
- Continuously monitors running processes and their open ports to log any network activity.

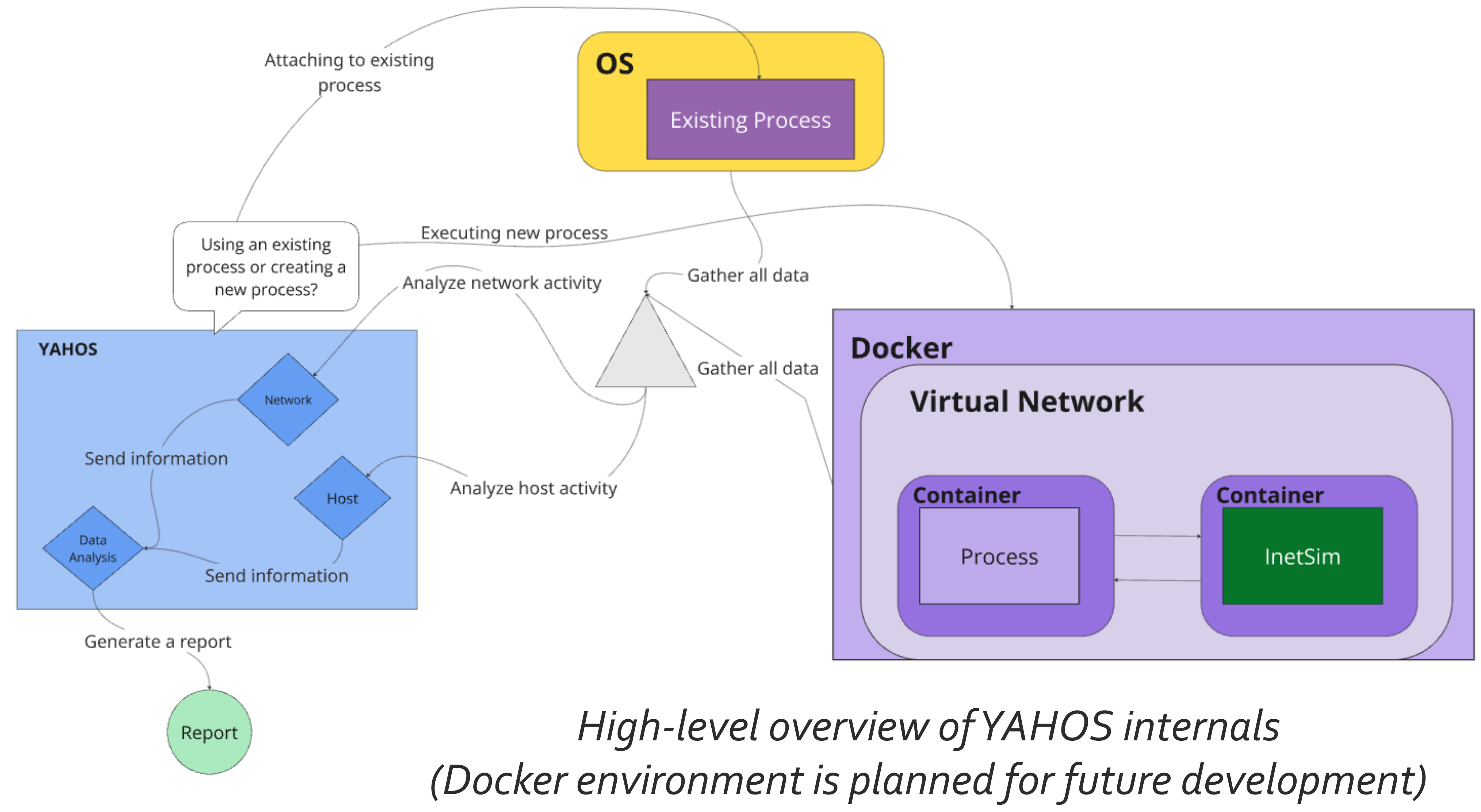
The goal of this tool is to enhance system security by offering monitoring and analysis capabilities.

Guillermo Rached – Computer Science

Thomas McCoy – Computer Science

Project Advisor: Giovani Abuaitah

Design



High-level overview of YAHOS internals (Docker environment is planned for future development)

Intended Uses

YAHOS is intended to be useful for assisting in the reverse engineering of malware and overall system monitoring.

Systems administrators, security analysts, and malware analysts can use YAHOS to help improve the overall safety of the digital landscape.

Technology Used

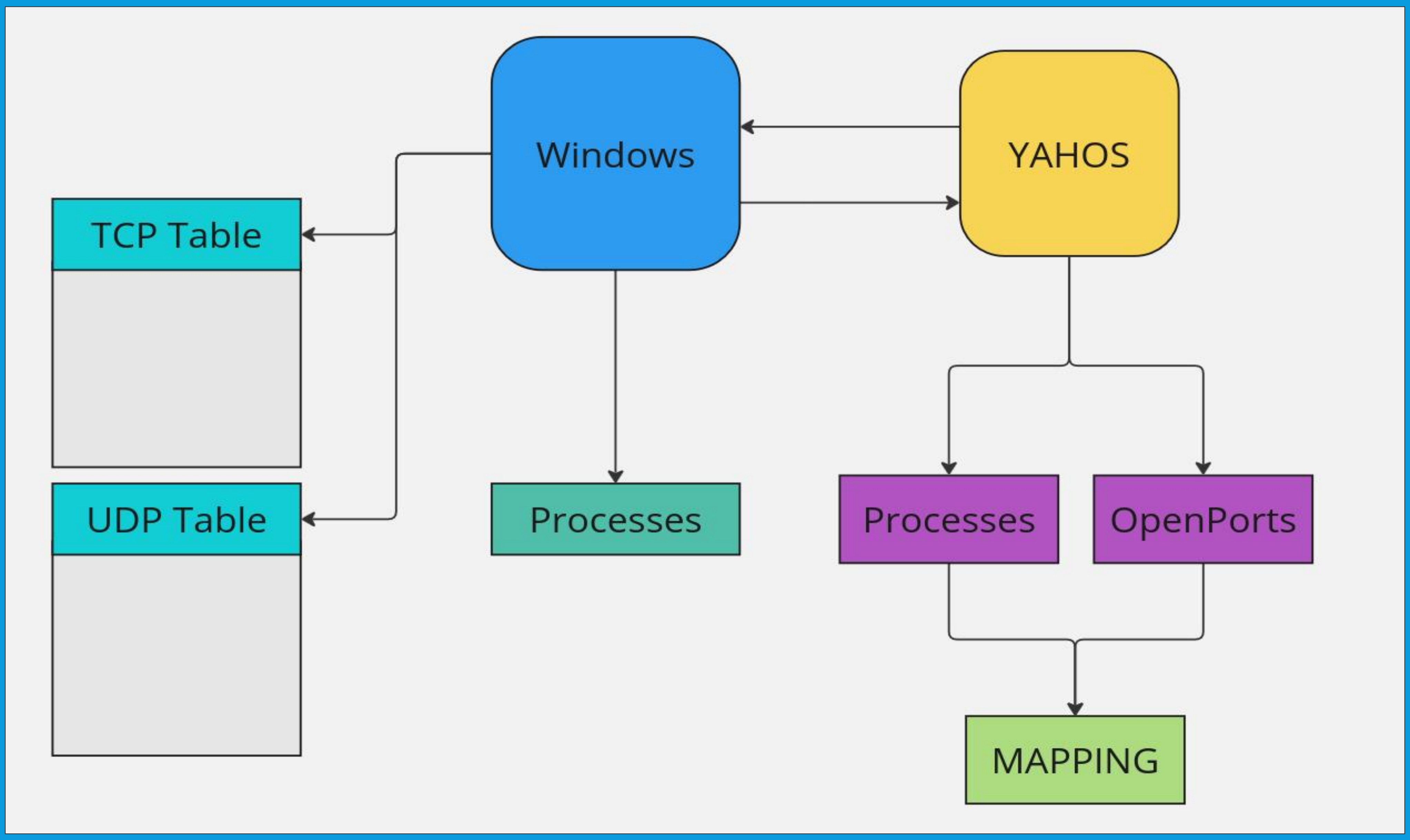
Qt

Windows API

Technical Details

Query Windows for active connections on both TCP and UDP protocols, then map these to known active processes.

This allows to initiate a network capture based on the obtained mapping and its interface.



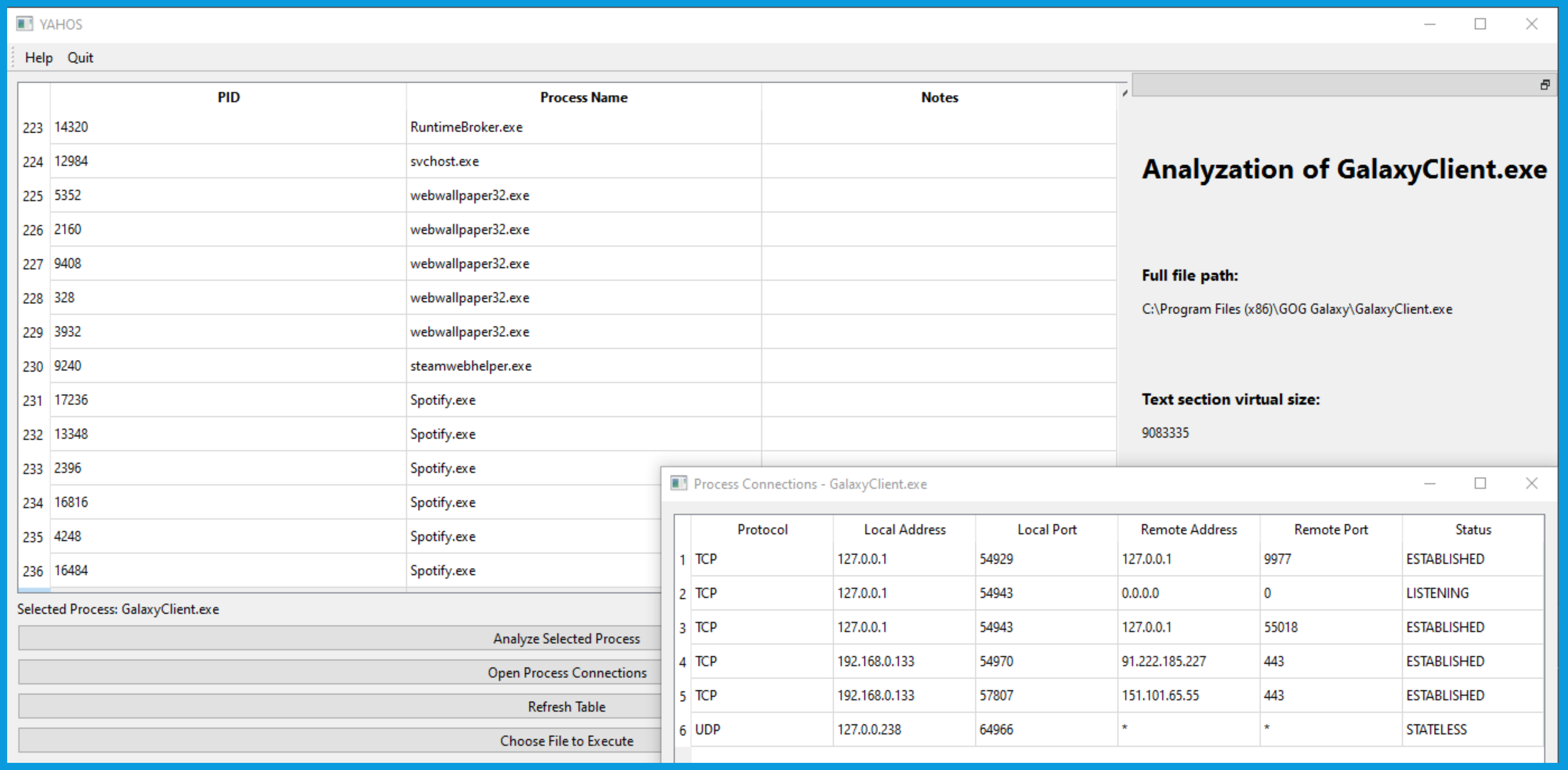
High-level overview of YAHOS interaction with the operating system and processes utilizing the information

Achievements

- View all running processes
- Analyze selected process, including text section virtual size and actual size as well as imports
- Network capture based on active process port

Challenges

- Working with the Win32 API
- Implementing Qt Framework for the UI
- Mapping running processes to open ports



	PID	Process Name	Notes
223	14320	RuntimeBroker.exe	
224	12984	svchost.exe	
225	5352	webwallpaper32.exe	
226	2160	webwallpaper32.exe	
227	9408	webwallpaper32.exe	
228	328	webwallpaper32.exe	
229	3932	webwallpaper32.exe	
230	9240	steamwebhelper.exe	
231	17236	Spotify.exe	
232	13348	Spotify.exe	
233	2396	Spotify.exe	
234	16816	Spotify.exe	
235	4248	Spotify.exe	
236	16484	Spotify.exe	

Selected Process: GalaxyClient.exe

Analyzation of GalaxyClient.exe

Full file path:

C:\Program Files (x86)\GOG Galaxy\GalaxyClient.exe

Text section virtual size:

9083335

Process Connections - GalaxyClient.exe

	Protocol	Local Address	Local Port	Remote Address	Remote Port	Status
1	TCP	127.0.0.1	54929	127.0.0.1	9977	ESTABLISHED
2	TCP	127.0.0.1	54943	0.0.0.0	0	LISTENING
3	TCP	127.0.0.1	54943	127.0.0.1	55018	ESTABLISHED
4	TCP	192.168.0.133	54970	91.222.185.227	443	ESTABLISHED
5	TCP	192.168.0.133	57807	151.101.65.55	443	ESTABLISHED
6	UDP	127.0.0.238	64966	*	*	STATELESS

YAHOS displaying enumerated process and active ports for selected process