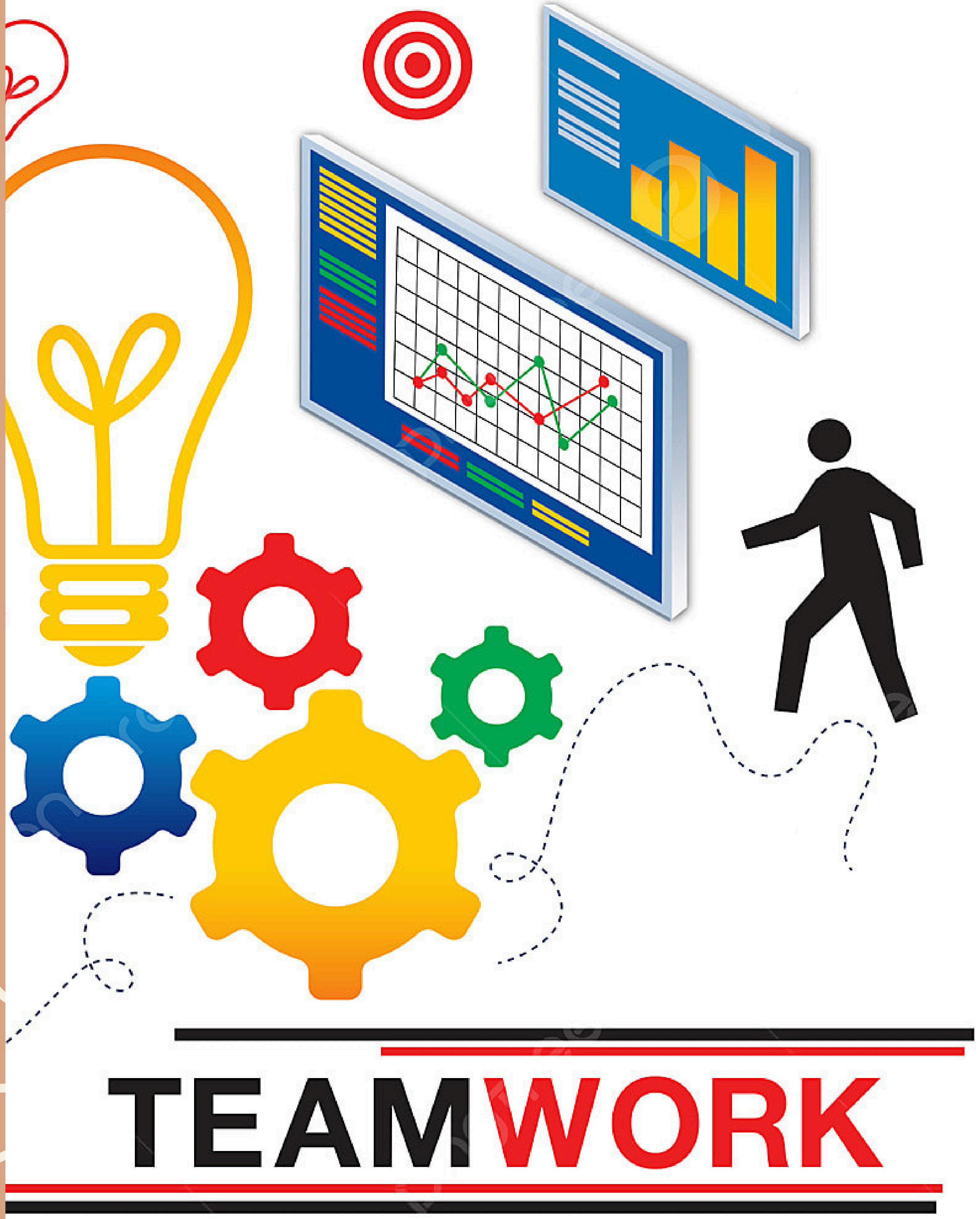
VIT® BHOPAL
www.vitbhopal.ac.in

ADVANCED RECONNAISSANCE & VISUALIZATION TOOL

REVIEW-2

Presented To: Dr.Ajay Kumar Phulre Sir



Team Members

1. 20BCY10102
G.Sharan Raghav

2. 20BCY10176
Sai Maneesh CH

3. 20BCY10181
S.Hareshwara Reddy

4. 20BCY10186
B.Shiva Sai

Introduction

- The Advanced Reconnaissance and Visualization Tool (ARVT) is a comprehensive solution designed to gather intelligence, visualize data, and facilitate decision-making in cybersecurity, military intelligence, and business intelligence domains.
- With advanced reconnaissance capabilities and intuitive visualization features, ARVT empowers users to identify threats, analyze trends, and mitigate risks effectively.
- Built with scalability, adaptability, and security in mind, ARVT offers a versatile platform for navigating the complexities of modern data-driven environments.

Challenges faced in ARVT

Data Integration Complexity: Integrating data from diverse sources such as APIs, OSINT, and network scans can be complex due to differences in formats, structures, and access methods.
Scalability and Performance Optimization:

Visualization of Complex Data: Visualizing complex reconnaissance data, such as network topologies or threat intelligence feeds, in a meaningful and actionable format presents challenges in design and implementation.

Adapting to Emerging Threats: The cybersecurity landscape is constantly evolving, requiring the ARVT to adapt to emerging threats, new attack techniques, and evolving adversary tactics through continuous updates and improvements.

Security and Compliance Considerations: Ensuring that the ARVT meets stringent security requirements and complies with regulatory standards for handling sensitive data presents challenges in encryption, access control, and audit trail implementation.

Findings

Increased Integration: ARVTs are integrating with machine learning and AI algorithms for predictive analysis and threat detection.

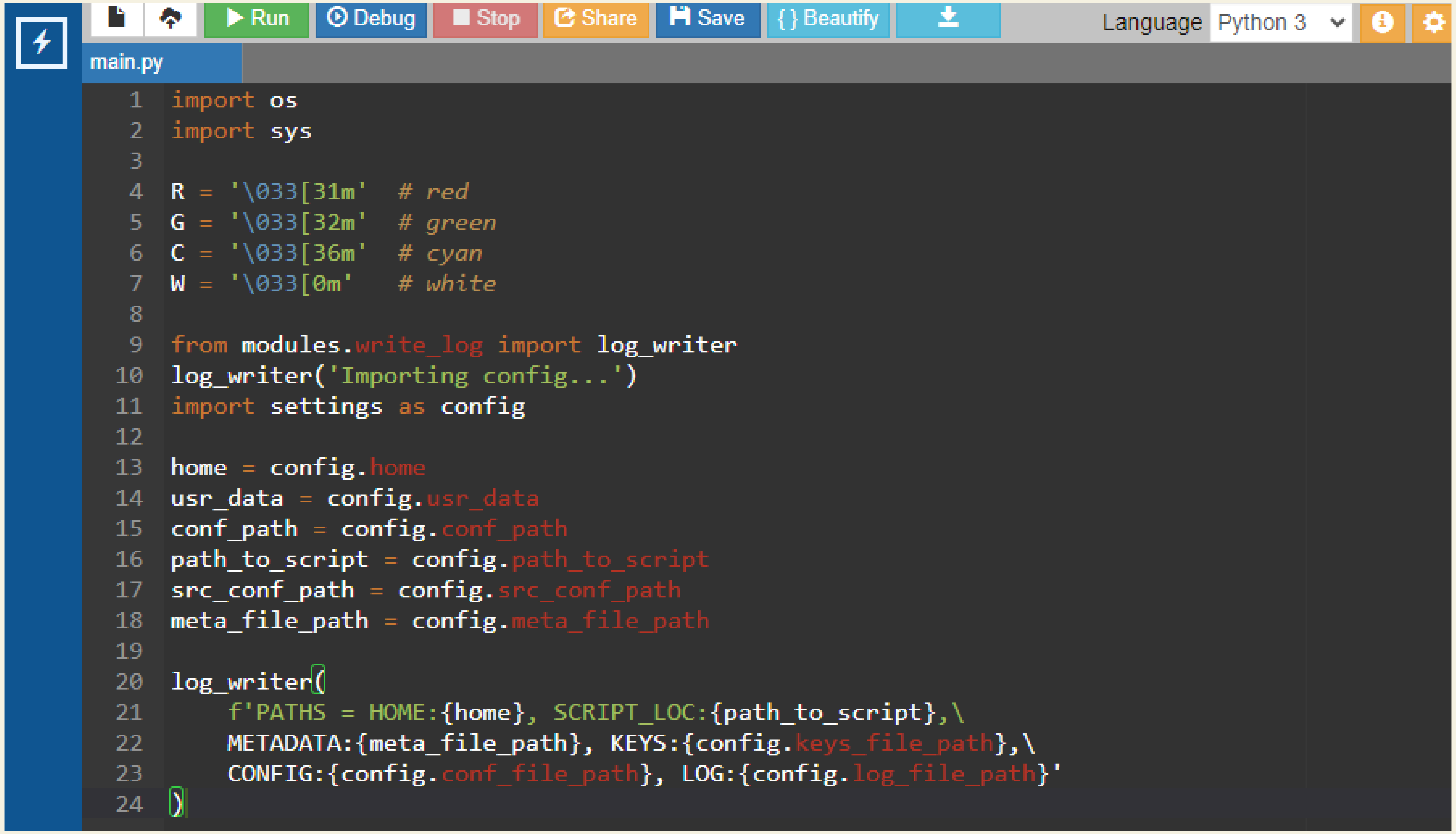
Cloud Adoption: Many ARVTs are shifting towards cloud-based solutions for scalability and accessibility.

Focus on User Experience: ARVTs are prioritizing intuitive interfaces and customizable dashboards for enhanced user experience.

Collaboration Features: ARVTs are incorporating collaboration features to facilitate information sharing and team collaboration.

CODE DEMO

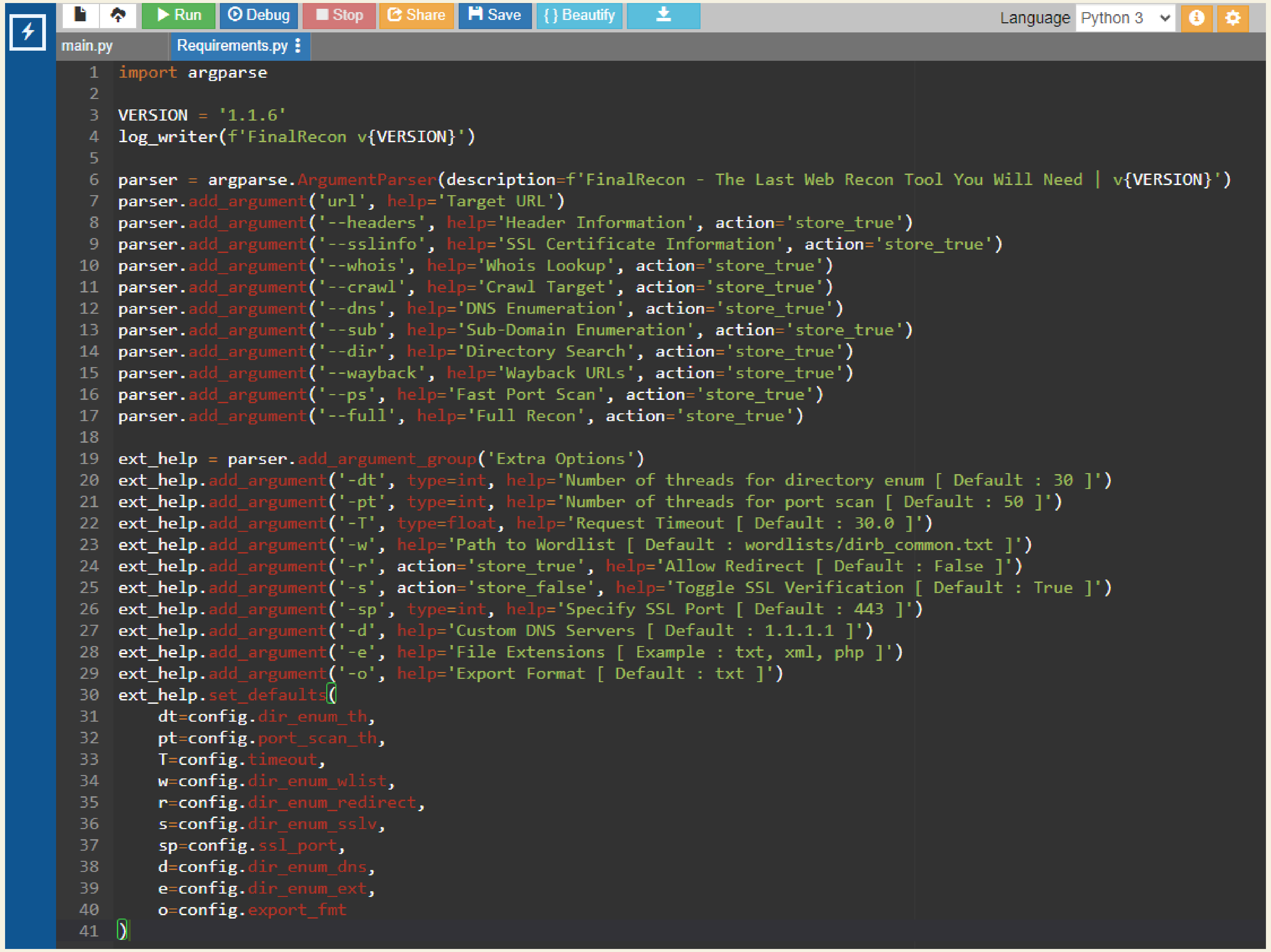
Main.py



```python
import os
import sys

R = '\033[31m'  # red
G = '\033[32m'  # green
C = '\033[36m'  # cyan
W = '\033[0m'   # white

from modules.write_log import log_writer
log_writer('Importing config...')
import settings as config

home = config.home
usr_data = config.usr_data
conf_path = config.conf_path
path_to_script = config.path_to_script
src_conf_path = config.src_conf_path
meta_file_path = config.meta_file_path

log_writer(
    f'PATHS = HOME:{home}, SCRIPT_LOC:{path_to_script},\
    METADATA:{meta_file_path}, KEYS:{config.keys_file_path},\
    CONFIG:{config.conf_file_path}, LOG:{config.log_file_path}'
)
```

CODE DEMO

Requirements.py



```python
import argparse

VERSION = '1.1.6'
log_writer(f'FinalRecon v{VERSION}')

parser = argparse.ArgumentParser(description=f'FinalRecon - The Last Web Recon Tool You Will Need | v{VERSION}')
parser.add_argument('url', help='Target URL')
parser.add_argument('--headers', help='Header Information', action='store_true')
parser.add_argument('--sslinfo', help='SSL Certificate Information', action='store_true')
parser.add_argument('--whois', help='Whois Lookup', action='store_true')
parser.add_argument('--crawl', help='Crawl Target', action='store_true')
parser.add_argument('--dns', help='DNS Enumeration', action='store_true')
parser.add_argument('--sub', help='Sub-Domain Enumeration', action='store_true')
parser.add_argument('--dir', help='Directory Search', action='store_true')
parser.add_argument('--wayback', help='Wayback URLs', action='store_true')
parser.add_argument('--ps', help='Fast Port Scan', action='store_true')
parser.add_argument('--full', help='Full Recon', action='store_true')

ext_help = parser.add_argument_group('Extra Options')
ext_help.add_argument('-dt', type=int, help='Number of threads for directory enum [ Default : 30 ]')
ext_help.add_argument('-pt', type=int, help='Number of threads for port scan [ Default : 50 ]')
ext_help.add_argument('-T', type=float, help='Request Timeout [ Default : 30.0 ]')
ext_help.add_argument('-w', help='Path to Wordlist [ Default : wordlists/dirb_common.txt ]')
ext_help.add_argument('-r', action='store_true', help='Allow Redirect [ Default : False ]')
ext_help.add_argument('-s', action='store_false', help='Toggle SSL Verification [ Default : True ]')
ext_help.add_argument('-sp', type=int, help='Specify SSL Port [ Default : 443 ]')
ext_help.add_argument('-d', help='Custom DNS Servers [ Default : 1.1.1.1 ]')
ext_help.add_argument('-e', help='File Extensions [ Example : txt, xml, php ]')
ext_help.add_argument('-o', help='Export Format [ Default : txt ]')
ext_help.set_defaults(
    dt=config.dir_enum_th,
    pt=config.port_scan_th,
    T=config.timeout,
    w=config.dir_enum_wlist,
    r=config.dir_enum_redirect,
    s=config.dir_enum_sslv,
    sp=config.ssl_port,
    d=config.dir_enum_dns,
    e=config.dir_enum_ext,
    o=config.export_fmt
)
```

Testing

Regression Testing: Conduct regression testing to ensure that recent changes and updates to the ARVT have not introduced any new defects or regressions. This includes retesting previously validated features and functionalities to validate their continued functionality.

User Acceptance Testing (UAT): Involve end-users in user acceptance testing to validate that the ARVT meets their requirements, expectations, and use cases. This includes gathering feedback, addressing user concerns, and ensuring alignment with user needs.

Accessibility Testing: Evaluate the accessibility of the ARVT to ensure it is usable by individuals with disabilities. This includes testing for compliance with accessibility standards such as WCAG (Web Content Accessibility Guidelines) and ensuring compatibility with assistive technologies.

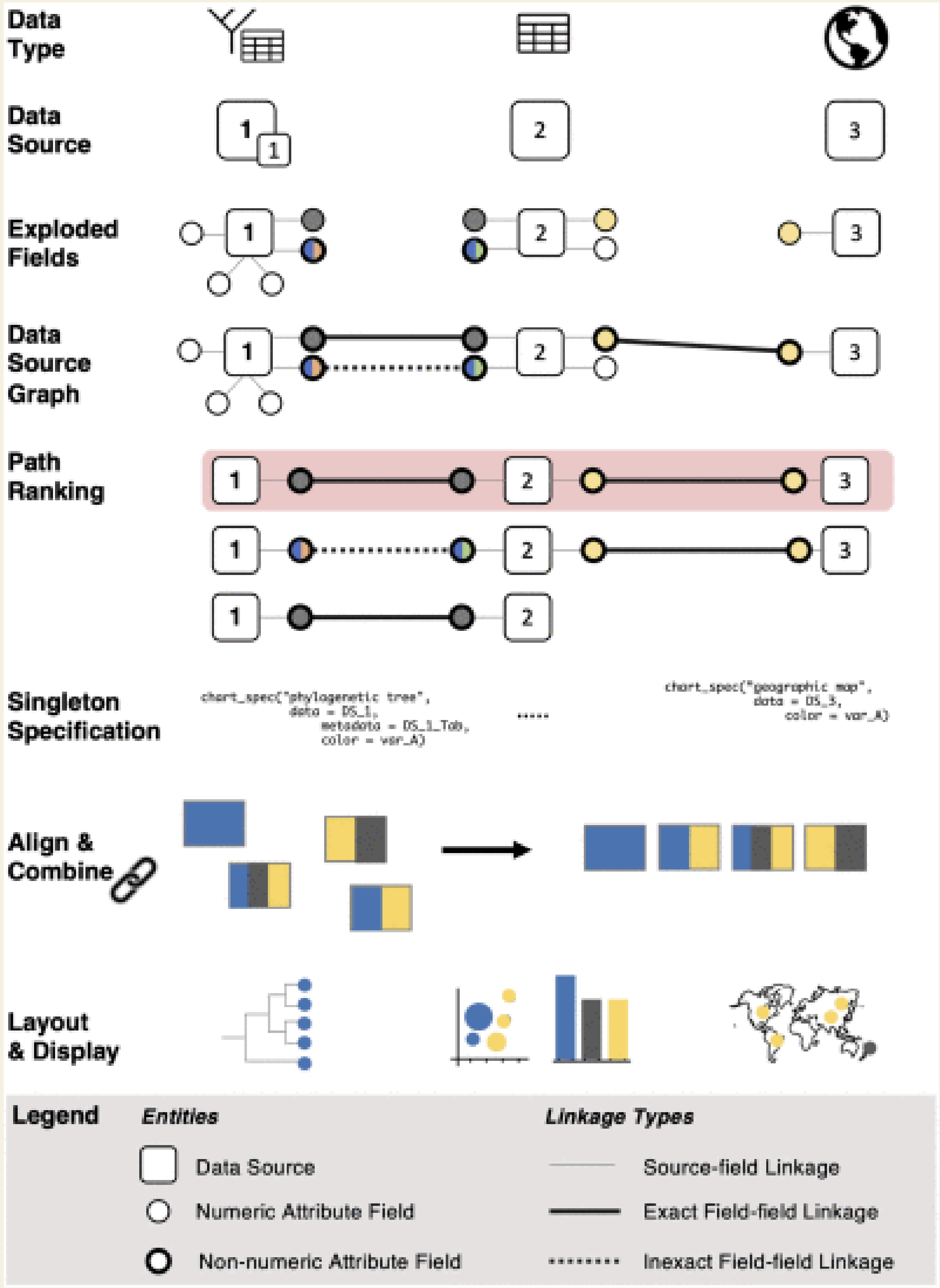
Validation

Requirement Validation: Verify that the ARVT meets all specified requirements, including functional, performance, security, and usability requirements. This involves comparing the features and functionalities of the tool against the documented requirements.

User Feedback Validation: Gather feedback from end-users, stakeholders, and domain experts to validate that the ARVT effectively addresses their needs and use cases. This involves conducting user surveys, interviews, and usability testing sessions to assess user satisfaction and identify areas for improvement.

Data Validation: Validate the accuracy, completeness, and reliability of the data processed and visualized by the ARVT. This involves comparing the output of the tool against known sources of truth and conducting data validation checks to ensure data integrity.

Flow Chart

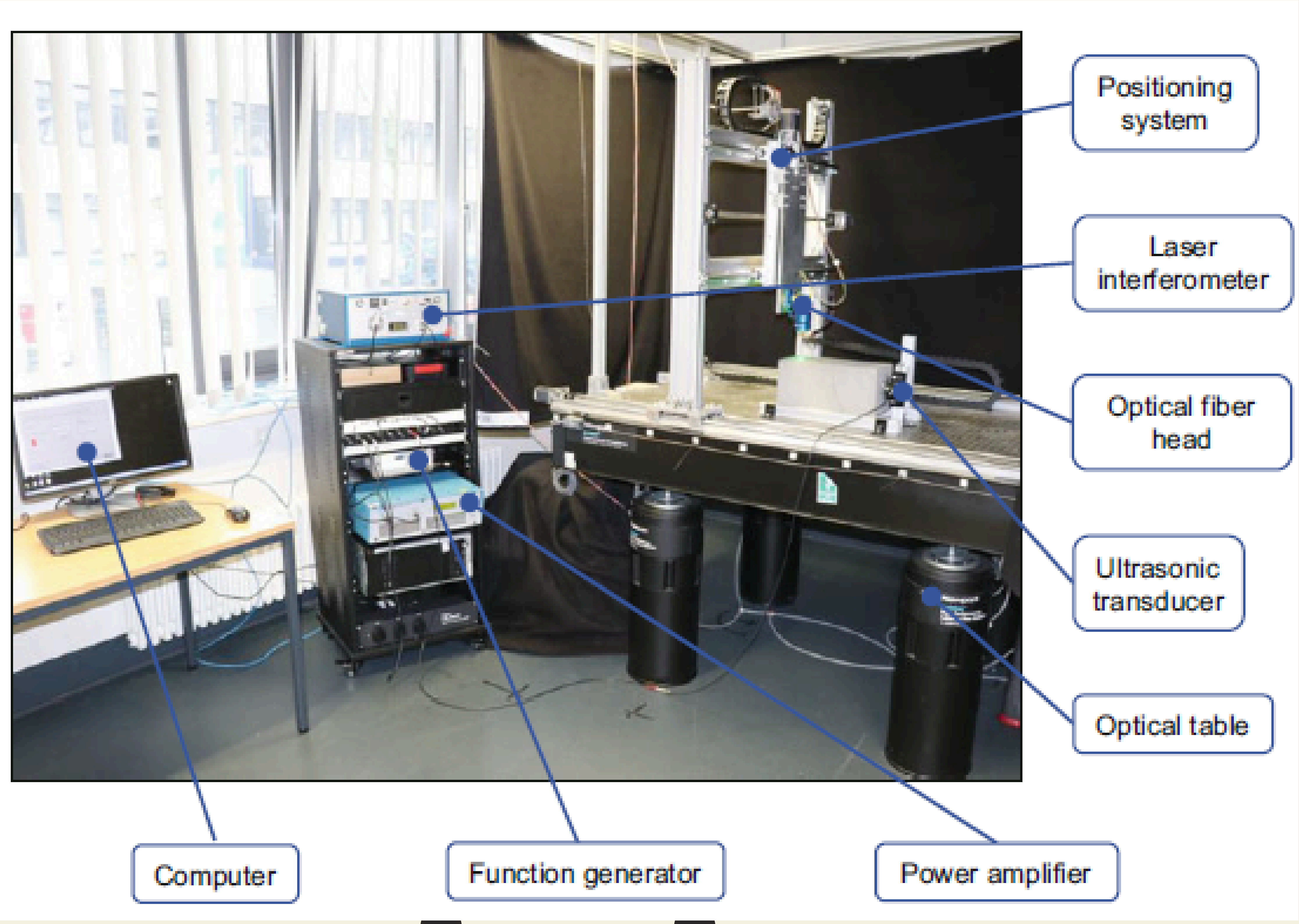


```
chart_spec("phylogenetic tree",
           data = DS_1,
              metadata = DS_1_Tab,
              color = var_A)
```

.....

```
chart_spec("geographic map",
           data = DS_3,
              color = var_A)
```

FLOW CHART


Positioning system
Laser interferometer
Optical fiber head
Ultrasonic transducer
Optical table
Computer
Function generator
Power amplifier

Results

Enhanced Threat Detection and Analysis: ARVTs enable cybersecurity professionals to detect and analyze threats more effectively by aggregating data from diverse sources, visualizing relationships and patterns, and identifying potential vulnerabilities and attack vectors.

Improved Situational Awareness: By providing comprehensive visualization of reconnaissance data, ARVTs enhance situational awareness for security teams, military personnel, and intelligence analysts, enabling them to make informed decisions and respond rapidly to emerging threats.

Faster Incident Response Times: ARVTs streamline reconnaissance workflows, automate repetitive tasks, and facilitate collaboration among cybersecurity teams, resulting in faster incident response times and reduced time-to-detection and time-to-remediation for security incidents.

Thank you for listening!

Don’t hesitate to ask any questions.